PD ISO/TS 12812-5:2017

BSI Standards Publication

Core banking — Mobile financial services

Part 5: Mobile payments to businesses

Documents
Document Sharing Hub

Full document details: PD ISO/TS 12812-5:2017

National foreword

This Published Document is the UK implementation of ISO/TS 12812-5:2017.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017.
Published by BSI Standards Limited 2017

ISBN 978 0 580 82899 7

ICS 03.060

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2017.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/TS 12812-5:2017

TECHNICAL SPECIFICATION

ISO/TS 12812-5

First edition
2017-03

Core banking — Mobile financial services —

Part 5: Mobile payments to businesses

Opérations bancaires de base — Services financiers mobiles —

Partie 5: Paiements mobiles à entreprises

Reference number
ISO/TS 12812-5:2017(E)

Documents
Document Sharing Hub

© ISO 2017

Full document details: PD ISO/TS 12812-5:2017

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

© ISO 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TS 12812-5:2017

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Requirements of a mobile payments-to-businesses system ... **2**
4.1 Device, network and application selection requirements ... 2
4.2 Security requirements ... 3
4.3 Logging requirements ... 3
4.4 Notice requirements ... 4
4.5 Receipt requirements ... 4
4.6 Data privacy requirements ... 4
5 Types of mobile payments ... **5**
5.1 Mobile proximate payments ... 5
5.2 Mobile remote payments ... 6
5.3 Other mobile payments technologies ... 6
5.3.1 Quick response (QR) based payments ... 6
5.3.2 Mobile payments through short messaging service (SMS) ... 6
5.3.3 Mobile payments through mobile airtime ... 6
5.3.4 Mobile wallet ... 6
6 Payment instruments ... **7**
6.1 Direct debit ... 8
6.2 Credit transfer ... 8
6.3 Payment card ... 8
6.4 Other payment instruments ... 8
6.4.1 Mobile bill account ... 9
6.4.2 Stored value account (SVA) ... 9
7 Use cases ... **9**
7.1 Proximate card payments use cases ... 9
7.1.1 User verification method ... 9
7.1.2 Single tap: Analysis of UVMs ... 10
7.1.3 Double tap: Analysis of UVMs ... 14
7.1.4 Mobile contactless payment transaction ... 16
7.1.5 Risk management in mobile proximate payments (MPPs) ... 26
7.1.6 Additional features ... 31
7.1.7 Interoperability and MPP service availability ... 32
7.2 Remote payments use cases ... 33
7.2.1 Mobile remote card payments ... 33
7.2.2 Mobile remote credit transfer ... 39
7.2.3 Mobile remote transactions using remote secured server ... 47
7.2.4 Interoperability model based on a centralized common infrastructure ... 49
7.2.5 Mobile remote payments using other payment instruments ... 50
7.2.6 Risk management in mobile remote payments (MRPs) ... 51
8 Requirements in the consumer environment ... **51**
8.1 General ... 51
8.2 Requirements in the consumer environment ... 52
Annex A (informative) **Host card emulation** ... **53**
Annex B (informative) **Procedures for redress and dispute resolution** ... **54**
Bibliography ... **55**

Documents
Document Sharing Hub

© ISO 2017 – All rights reserved

Full document details: PD ISO/TS 12812-5:2017

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
Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

Introduction

The use of mobile devices to conduct financial services is occurring following the steady rise of the number of customers using the Internet for these services. As an evolving market, mobile financial services (MFSs) are being developed and implemented on various bases throughout different regions of the world and also among the various providers of such MFSs (MFSPs). Given these conditions, then, the purpose of this document is to facilitate and promote interoperability, security and quality of MFSs, while providing an environment where all stakeholders can benefit from the evolution, and MFSPs remain as commercially free and competitive as possible to design their own implementations in pursuing their own business strategies.

The intentions of this document are:

a) to advance interoperability of MFSs globally by building an international vision of this environment and by defining requirements based on a common terminology and basic principles for the design and operation of MFSs (see ISO 12812-1:2017, Clause 5);

b) to define technical components and their interfaces, as well as roles that may be performed by different MFSPs (e.g. financial institutions, mobile network operators, trusted service managers). These components and their interfaces, as well as roles, are defined according to identified use cases, although future use cases may be considered during the maintenance of the standard;

c) to identify existing standards on which MFSs should be based, as well as possible gaps.

Standardization effort in this area is beneficial for a sound development of the MFSs market as it will:

— facilitate and promote interoperability between the different components or functions developing and/or providing MFSs (see ISO 12812-1:2017, 4.3 and 4.4), including consideration of the impact of new components and/or interfaces created by the introduction of a mobile device into the payment chain;

— build a secure environment so that payers and payees (see ISO/TS 12812-4) and consumers and merchants (this document) can trust MFSs and allow the MFSPs to manage their risks;

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

— enable the consumer to choose from different providers of devices or MFSs, including the possibility to contract with several MFSPs for services on the same device;

— enable the consumer to transfer MFSs from one device to another one (portability);

— promote a consistent consumer experience among various MFSs and MFSPs, with easy-to-use interfaces.

To achieve these objectives, each part of the ISO 12812 will specify the necessary technical mechanisms and, when relevant, refer to existing standards in the area of each part.

The ISO 12812 (all parts) provides a framework flexible enough to accommodate new mobile device technologies, as well as to allow various business models, while enabling compliance with applicable national regulations (e.g. data privacy, protection of personally-identifiable data, consumer protection, anti-money laundering and prevention of financial crime) (see ISO 12812-1:2017, 6.3.4).

It is not the intention of the ISO 12812 (all parts) to duplicate or to seek to replace any existing standard in the area of MFSs (e.g. communication protocols, mobile devices). It is also not the intention of the ISO 12812 (all parts) to drive technology to any specific application or to restrict the development of future technologies or solutions. The ISO 12812 (all parts) does not define messages and data elements to be exchanged at the interfaces between the different components or actors of the system; instead identified messages and data elements are already specified (e.g. ISO 8583, ISO 20022) and are referenced by the standard. Mobile devices have communication capabilities that are sufficient for exchanging transaction data conforming to appropriate ISO standards (e.g. ISO 8583, ISO 20022) as

© ISO 2017 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

well as delivering the required transaction authorization information to the POS via other formats (e.g. bar codes, SMS).

The ISO 12812 (all parts) recognizes the need for unbanked or under-banked consumers to access MFSs. It also recognizes that these services may be provided by MFSPs who are not financial institutions according to the applicable regulation(s).

NOTE For this document, the terms and definitions from ISO 12812-1 apply; where a term is abbreviated in this document, the abbreviation is associated with the initial use of the term.

Figures 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 and 18 or part thereof are courtesy of the European Payments Council.

© ISO 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

Core banking — Mobile financial services —

Part 5: Mobile payments to businesses

1 Scope

This document focuses on mechanisms by which a person ("consumer", "payer" or "business") uses a mobile device to initiate a payment to a business entity ("merchant" or "payee"). Such a payment may use the traditional merchant point of interaction (POI) system, where the manner of settling the payment follows well-established merchant services paradigms. Additionally, there are other ways for a consumer to make a payment to a merchant, using the mobile device to initiate, authorize and process transactions outside of traditional payment networks using secure payment instruments. Accordingly, this document supports both "push" and "pull" payments (i.e. transactions that are pushed or transmitted from a mobile device into a POI or pulled or received into a mobile device or POI), which are initiated and/or confirmed by a consumer to purchase goods and or services, including proximate payments, remote secure server payments, as well as mobile payments that leverage other technologies [e.g. cloud computing, quick response ("QR") codes, biometrics, geo-location and other methods to authenticate and authorize the transaction].

One of the most important aspects of the MFS environment is mobile payments to businesses. There are many ways a consumer, or a business as a consumer, can make a payment to a merchant. ISO 12812 provides a comprehensive standard for using the mechanisms involved in mobilizing the transfer of funds regardless of who is involved in the process. This document is intended to be used by potential implementers of mobile retail payment solutions, while ISO 12812-4 is intended for potential implementers of solutions for mobile payments to persons.

NOTE ISO 12812-1:2017, 5.4 explains the differences in the use of these terms. As such, the ISO 12812 (all parts) seeks to support all possible technologies and is not designed to highlight or endorse specific technologies in the competitive marketplace.

Although this document deals with mobile payments made by a consumer or a business acting as a consumer, which transactions are subject to a variety of consumer protection requirements, in terms of the relationship to the MFSP, the consumer (or business) is the customer of the MFSP. Nevertheless, this document will use the term "consumer."

2 Normative references

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

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

ISO/TS 12812-2, *Core banking — Mobile financial services — Part 2: Security and data protection for mobile financial services*

ISO/TS 12812-3, *Core banking — Mobile financial services — Part 3: Financial application lifecycle management*

ISO/IEC 18004, *Information technology — Automatic identification and data capture techniques — QR Code 2005 bar code symbology specification*

© ISO 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TS 12812-5:2017

ISO/IEC 18092, *Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)*

ISO/IEC 21481, *Information technology — Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol –2 (NFCIP-2)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12812-1 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

4 Requirements of a mobile payments-to-businesses system

This clause identifies a set of requirements that are common to the mobilization of any payment, regardless of whether such a transfer of funds represents a payment to a person or to a business, or whether it is a mobile proximate payment or a mobile remote payment. In other words, these requirements apply regardless of the nature of the parties involved in the transaction and whether those parties are physically present at the same or different locations.

NOTE Many of these essential requirements also are contained in ISO/TS 12812-4, although there are nuances in how they operate when the payment is to a person as compared with a payments-to-businesses system, which has its own set of operating rules and technical specifications developed by the MFSP.

4.1 Device, network and application selection requirements

4.1.1 An MFSP shall document its compatibility requirements for each MFS it offers with a mobile device and permits a consumer (i.e. payer) to select a compatible mobile device and compatible MFS application(s) for his/her use.

4.1.2 To the extent that an MFS imposes specific requirements on a mobile network operator (MNO), the MFSP shall document those requirements and determine which MNOs support the MFS. An MFSP shall permit a consumer to select an MNO that supports the required mobile communications services for the MFS.

4.1.3 An MFSP shall permit a consumer to select or pre-configure (e.g. for low value transactions) the appropriate mobile application(s) and/or payment instrument(s), including a mobile wallet, for handling any particular mobile payment transaction(s).

4.1.4 An MFSP shall ensure that when a mobile wallet is used for mobile payments to a business, it shall be capable of providing, at a minimum, the following functionality:

— an interface to register personal and payment instruments data (on the mobile device);

— a data repository to store the data (on the mobile device or a secured server);

— an interface allowing the consumer to select the payment instrument;

— an interface allowing the consumer to use the selected payment instrument (can be one interface managing all payment means or different interfaces for different means);

— an interface for managing and updating stored data (e.g. update, cancellation).

© ISO 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

4.1.5 An MFSP shall provide a statement of account activity to the consumer, in a manner appropriate for the circumstances (e.g. mailing periodic paper statement, download file, online account).

NOTE In cases of billing accounts where the consumer has an obligation for regular payments, due dates can be displayed on the mobile device by use of pop-up warnings (e.g. information regarding consequences of non-payment).

4.2 Security requirements

4.2.1 A mobile device used for MFSs shall be able to store or provide access to applications within an appropriate secure environment (e.g. using supplementary software, SE, TEE) in accordance with ISO/TS 12812-2.

4.2.2 An application, as well as any associated credentials, resident on the mobile device or accessed through a mobile device, shall be managed in conformance with the requirements and/or guidance provided in ISO/TS 12812-3.

4.2.3 A mobile device shall be able to authenticate a consumer using a user verification method (UVM) established by the MFSP as suitable for the particular application.

NOTE For implementation of authentication mechanisms, refer to ISO/TS 12812-2.

4.2.4 A mobile device shall be equipped with a display and a keyboard (physical or virtual) and other equipment (e.g. a biometrics capture device) if needed, enabling the activation/selection of the payment instrument and the confirmation of the transaction by the payer using trusted paths.

4.2.5 A mobile device shall possess the capability to secure the communications channel used for the mobile payment transaction in a manner that has been determined to be sufficient by the MFSP.

4.2.6 A mobile device should enable the consumer to access a mutual authentication gateway for exchanging the mobile payment transaction. If the application does not provide mutual authentication, the MFSP should take alternative security measures in order to protect the communication channel against security attacks (e.g. man-in-the-middle, malware and viruses).

4.2.7 The MFSP shall ensure that, in establishing any mobile codes or similar authentication credential (see ISO 12812-1), any use it allows of a bank-issued PIN shall be done in conformance with the requirements of ISO 9564; a non-bank issued PIN/mobile code does not need to conform to these requirements.

4.3 Logging requirements

4.3.1 An MFSP shall provide the means for a consumer to view the details of each mobile payment transaction. The transaction log shall, at a minimum, display the last 10 transactions handled by an application or the recent transactions completed over the past 30-day period whichever provides the most information. When specifically requested by the customer and where it is possible and feasible, the MFSP shall make available additional information to supplement the immediately available information log of the transaction(s) under reasonable terms.

4.3.2 The transaction log should make available to a consumer the following data:

— transaction date;

— transaction time;

— transaction amount(s);

© ISO 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

— transaction currency code(s);

— transaction type;

— payee/payer information (e.g. name/device ID and location);

— transaction verification/integrity information (e.g. token, cryptogram).

4.4 Notice requirements

4.4.1 An MFSP shall notify a consumer that a payment has been authorized, approved and/or completed (see 4.4.4 for notice delivery methods).

4.4.2 The customer's MFSP, or in some cases the merchant's MFSP, shall inform the merchant about the status of a payment (e.g. that a payment has been received into the merchant's account).

4.4.3 An MFSP shall notify the merchant about the ability to access the funds that were transferred into its account.

4.4.4 An MFSP shall accomplish the notice required by this subclause through an appropriate method of communication (e.g. through pop-up notice in the application, by text, by email, by paper statement).

NOTE Such notices and related communications can include value-added services (e.g. on-demand payment verification services, fully electronic long-term transaction records, special records for visually impaired users).

4.5 Receipt requirements

4.5.1 A POI that is capable of printing a paper transaction receipt shall provide the consumer with a printed receipt upon request.

4.5.2 A POI that is capable of transmitting an electronic receipt (e.g. via email, text messaging or other means) shall provide the consumer with an electronic receipt upon request.

4.5.3 A POI that knows in advance that it cannot provide a transaction receipt should inform the consumer, to the extent it is physically capable of doing so, that no receipt can be printed or electronically transmitted and offer the consumer the choice to continue or to cancel the transaction.

In certain low-value transaction environments (e.g. toll roads, subways), it may not be feasible for the system to provide a receipt or to enable the consumer to cancel the transaction.

4.5.4 An MFSP shall notify a consumer about the legal status of different forms of transaction record required by the jurisdiction where the MFS is being used.

4.6 Data privacy requirements

4.6.1 An MFSP shall ensure that each MFS it offers conforms to the data protection laws and regulations of each jurisdiction in which the application is designed to operate (see related information in ISO/TS 12812-2:2017, 14.1) In the furtherance of this requirement, an MFSP should conduct a privacy impact assessment (see ISO/TS 12812-2:2017, 14.3).

4.6.2 An MFSP shall conform to the requirements and recommendations contained in ISO/TS 12812-2:2017, 14.2.

4.6.3 An MFSP shall ensure that parties involved in the processing of the mobile payment document and implement a security policy that addresses information security and acceptable uses.

© ISO 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

4.6.4 An MFSP shall ensure that third parties involve in the processing of mobile payments provide the appropriate legal notice to the consumer and/or the merchant that the execution of a transfer across borders entails transmission of the appropriate personal information according to their respective jurisdictions.

5 Types of mobile payments

In general terms, there are two major categories of mobile payments to a business: (1) proximate payments and (2) remote payments. Existing payment instruments may either be used in a proximate or remote manner, whether the technology employed is contactless or some other mobile payment technology, such as the QR-based mobile payments, mobile payments through mobile airtime, secured server-based payment authorizations, etc. (see ISO 12812-1:2017, 7.2, 7.3 and Annex C). All types of mobile payments rely on an application that either resides on the mobile device or is accessed through the mobile device. This clause identifies and describes such payment types as part of specific guidance and use cases.

In some implementations of mobile payments, the actual sensitive transaction data (e.g. the PAN) is replaced by a payment token, a temporary surrogate which may also possess same data structure as the original data. Tokens may also be used as a mechanism to handle the post-authorization storage of sensitive data for security purposes.

5.1 Mobile proximate payments

Mobile proximate payments to a business (MPPs) are consumer payments to a merchant that are made using a mobile device where both parties are in the same location. Such transactions, for example, may be initiated by placing the device very close to the merchant's POI equipment (i.e. in proximity to the reader) or by using a mobile payment app while the mobile device is located at the merchant retail location. These payments may rely on NFC technology (see ISO 12812-1); other methods are bluetooth and wireless (see IEEE 802.11). Although this document does not relate exclusively to NFC as the only possible technology for proximate payments, the document cites NFC uses cases as one illustration of this payment type, including the use of NFC operations in host card emulation mode (see Annex A). This approach permits potential implementers to better understand the issues faced by the current mobile payments ecosystem. Other technologies or methods are available for initiating a mobile payment transaction (see 5.2 to 5.3).

NFC technology has been included in some mobile devices. Although there are many ways to configure NFC communication protocols for various uses, a mobile device using NFC that conforms to this document shall follow ISO/IEC 18092 and ISO/IEC 21481 for communicating with the merchant POI device. When a mobile device communicates according to these standards, it is capable of exchanging the necessary transaction data to the POI so that a transaction is processed in a manner consistent with the processing of debit and credit cards in a card-emulation mode (e.g. ISO 8583, ISO 20022). Because use of the NFC protocol enables transactions to be processed quickly by bringing the mobile device in proximity to the POI ("touching", "waving" or "tapping" are terms that have been applied to this process), the result is an effective transaction processing and a streamlined user experience. It should be noted that in other MPPs, the payment might not be made in card-emulation mode and may require a different set of parameters for the transaction (e.g. bar codes, secured server-based transactions with or without the use of a token). In these latter situations, the mobile device is capable of exchanging transaction data in appropriate formats (e.g. bar codes).

MPP transactions require a secure environment that is capable of protecting all sensitive transaction and personally-identifiable data, as well as mitigating the risks usually handled by online risk management. Such secure environment shall conform to the requirements of ISO/TS 12812-2, and may take a variety of forms, including a supplementary software component ("security controls"), a secured server, a UICC (a SIM-based SE), an embedded SE or a microSD card. The MPP shall also conform to the requirements of 4.2 and 4.6. Additionally, in some NFC-based transactions, certain sensitive operations are directly performed within an SE on the mobile device (e.g. data encryption, transaction validation when the payment amount value is above a certain threshold amount).

© ISO 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

5.2 Mobile remote payments

Mobile remote payments to a business (MRPs) are non-face-to-face or online transactions, made using a mobile communications network or Internet browser, independent of the business location, where a consumer initiates a payment or transfer of monetary value that may or may not be card-based (e.g. payment account, scrip, electronic money) in exchange for goods or services being acquired from a merchant or other business entity. In a remote application on the mobile device, the most security-oriented operations are consumer authentication/transaction validation and authorization of the transaction.

Although it is acknowledged that some MRP transactions are made with purchasing cards and business/corporate cards, these transactions are nevertheless initiated and authorized in the same way as consumer card transactions; thus, there is no need to develop distinct use cases for such scenarios. Similarly, all MRPs shall employ a secure environment to protect all sensitive transaction and personally-identifiable data by conforming to the requirements of 4.2 and 4.6.

5.3 Other mobile payments technologies

Although other mobile payments technologies may be either mobile proximate or mobile remote payments, those technologies are significantly different from traditional card network or NFC mobile payments. Several mobile payments are discussed in this subclause, based on the use of non-payment network transaction processing or on the use of traditional payment networks in non-traditional ways (e.g. quick response, short messaging service, mobile airtime and wallet).

5.3.1 Quick response (QR) based payments

These are mobile payments which are initiated by a consumer using a QR code conforming to the requirements of ISO/IEC 18004. In some instances, the QR code is used through an application to obtain a traditional card payment authorization; in other situations, the QR code is used through an application to authenticate the consumer and provide the consumer with access to a payment instrument. QR codes may be displayed either on the screen of the mobile device or at the POI.

5.3.2 Mobile payments through short messaging service (SMS)

These mobile payments, or components of a payment transaction, are made through the use of an SMS text message. The text message may be used to confirm payment information, account information or consumer authentication sometimes through the use of a token. SMS does not use any data encryption.

This type of mobile payment is used in some parts of the world (e.g. Asia, Africa and United States) and may be used to transfer funds (both in payments to persons and payments to businesses environments).

5.3.3 Mobile payments through mobile airtime

This type of mobile payment is currently used in various parts of the world, especially in developing markets. Mobile airtime is often used to supplant a lack of banking infrastructure and to afford access to MFSs through specific applications enabling non-banked persons to gain access to financial services. A general scenario for the mobile payment through mobile airtime enables a consumer to pay for the goods or services using his/her mobile airtime units billed by the consumer's/customer's MNO, either as a pre-paid or as a post-paid monthly contractual plan. Settlement requires a business relationship between the MNO/MFSP and individual merchants.

5.3.4 Mobile wallet

A "mobile wallet" refers to use of a mobile device as a surrogate for a physical wallet. All relevant financial information (e.g. bank or non-bank issued account numbers, credit-card numbers) may be stored either on the actual mobile device or remotely (see ISO 12812-1); a consumer shall have the mobile device present for the transaction to occur and be able to perform all the necessary authentications required by the MFSP. Payments may be made using NFC technology embedded in the mobile device in card

© ISO 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

emulation mode; the device is waved over (tapped or touched to or passed over) a contact point-of-sale terminal at a retail business location for payment. Other technologies for mobile wallet applications are located remotely or cloud-based (i.e. using a secured server), where the application is accessed by the customer using the browser on the mobile device.

For a mobile wallet payment, the consumer launches an application that has been installed or downloaded to his/her mobile device, or accessed through the mobile Internet browser, when prompted to make a payment at a POS or remotely. The application on the device interfaces with the application that is preloaded with the consumer's account/payment information. The transaction is processed via a third-party MFSP/processor or merchant acquirer and settled over the respective payment network (e.g. credit, debit, ACH, prepaid, other).

A consumer then selects the desired form of payment (e.g. mobile money, card-based payment, secured server-based payment, including QR) from the various applications that have been previously loaded into the mobile device (or stored separately in the wallet in the mobile device), or which the consumer has arranged to access through the Internet browser. The selected app/applet then instructs the SE or the cloud provider to provide account information associated with that application accessible through his or her mobile device. In an NFC situation, when the consumer "taps" his/her mobile device on the POI, the device's NFC chipset enters a "secure card emulation mode", which is one of three operating modes supported by active chips. The NFC chipset then accesses the SE for the consumer-selected account information. The NFC chipset transmits payment information to the awaiting payment terminal, where it is then communicated to the card processing network. In all cases, the payment transaction is then recorded in the consumer's mobile device wallet application.

6 Payment instruments

From an "open" MFS program point of view, existing payment instruments available for use can be divided into the following three categories: direct debit, credit transfer (either bank or non-bank accounts) and card-based (e.g. credit, debit, stored-value).

NOTE All payment instruments discussed in this clause are existing forms of payment instrument that are not unique to the mobile payment environment (see ISO 12812-1:2017, Annex C).

From the other perspective, there are "closed" MFSs that use the same standard payment instruments, but are not interoperable with the open program options, unless two or more MFSPs contractually agree to cooperate and share their programs, which results in making them essentially "open" as between the participating MFSPs (see ISO/TS 12812-4, which encourages such agreements). Another form of payment instrument is the mobile wallet, which can function as its own payment instrument (i.e. mobile money) or be a container of any of the above payment instruments.

In the world of payment processing, the role of the data formats and messages used to exchange information between merchants, merchant acquirers and MFSPs can be compared with the role of language in communication between people. Every payment program contains a set of operating rules and technical standards for the execution of payment transactions established by a MFSP, which rules shall be followed by others who are part of or participating in the payment program. These rules can be regarded as instruction manuals which provide a common understanding on how to move funds (e.g. from account A to account B).

As discussed in 5.1, if the mobile device is exchanging transaction data to the POI so that a transaction is processed in a manner consistent with the processing of debit and credit cards in a card-emulation mode (e.g. ISO 8583, ISO 20022), the mobile device possesses the capability of handling the exchange of card transaction data. In the case of credit transfer or direct debit payment programs, some data formats/messages are based on ISO 20022, the data repository standard that covers numerous types of transaction messages in universal mark-up language (e.g. XML) for use in the financial supply chain, designed to enable communication between parties across all financial markets. For example, in the case of the European Union, the SEPA credit transfer (SCT) and SEPA direct debit data formats are based on ISO 20022. However, in the United States and elsewhere, these payments may require data and messages based on ISO 8583, or are transfers based on the NACHA Operating Rules governing the US ACH Network (hereafter collectively referred to as "credit transfers"). For card-based payments,

© ISO 2017 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

ISO 8583 and ISO 20022 specify the data/messages by which these transactions are authorized between a merchant, acquirer and card issuer. In the case of the United States, numerous card processing networks exist, some are open-loop systems (e.g. VisaNet, BankNet), closed-loop systems (e.g. American Express, Discover, individual stored value card systems). In Europe, the SEPA Cards Framework enables a consistent customer experience when making or accepting euro payments and cash withdrawals.

NOTE Open-loop systems are also referred to as "inter-MFS provider collaborative models" and closed-loop systems are also known as "centric models" (see ISO 12812-1:2017, Annex B).

This document leverages existing standards when defining procedures for mobile payments to a business. For each type of payment (e.g. a mobile proximate payment in a "brick and mortar" location, online purchases), this document identifies and describes interoperable, open systems using one or more standardized payments instruments (e.g. bank or non-bank account credit transfer, direct debit and credit, debit cards or prepaid cards).

NOTE Payment instruments are defined in ISO 12812-1; all references to that term in this document are consistent.

6.1 Direct debit

A direct debit program is based on the following concept: "I request money from someone else, with their prior approval, and credit it to myself." The payer (consumer) and the payee (business or merchant) shall each hold an account with an MFSP (which may be a different MFSP for the payer and for the payee), unless the transaction is really a credit transfer (see 6.2). The direct debit payment instrument allows a business to collect funds from a consumer's account, provided that the business obtains a digitally signed authorization granted by the consumer which authorizes the business to collect a payment. A consumer may instruct its MFSP not to accept any direct debit collections on his/her account.

6.2 Credit transfer

A credit transfer program (CTP) is based on the following concept: "I request money to be sent to someone, requesting money from myself and crediting it to the merchant." The CTP enables the MFSP to offer a core and basic credit transfer facilitating payment initiation, processing and reconciliation (e.g. SEPA CT, ACH). This scenario enables a consumer and a merchant to use different MFSPs to handle the transaction.

6.3 Payment card

Payments cards (e.g. debit, credit, prepaid, private account) enable a consumer (as the "payer" or "cardholder") to use general-purpose cards to make payments and withdraw cash and to enable a business to receive payments (as the "payee"). Consumers benefit from wider acceptance of cards and merchants benefit from a competitive acquiring market and are able to choose which card programs to accept and from which acquirer (an MFSP that acquires card transactions that services card-accepting merchants). MFSPs issue cards to consumers, host the cardholder database and authorize and handle the settlement of each transaction. MFSPs develop payment card programs based on various business models and also benefit from expanded service offerings.

6.4 Other payment instruments

There are available solutions in the market that use other payment instruments and usually use other communication channels and/or payment infrastructures. These solutions basically are based on mobile billing accounts (pre-paid or post-paid) or in stored value cards (SVCs) and/or stored value accounts (SVAs). Whether these solutions are interoperable depends on if they are part of an open or closed loop processing system, and the level of security and fraud protection usually depends on whether the particular payment instrument is identified with a specific consumer (e.g. if a gift card is registered to a consumer or not).

NOTE As noted above, all payment instruments discussed in this clause are existing forms of payment instrument that are not unique to the mobile payment environment (see ISO 12812-1:2017, Annex C).

AVA Documents
Document Sharing Hub

© ISO 2017 – All rights reserved

Full document details: PD ISO/TS 12812-5:2017

6.4.1 Mobile bill account

In the case of mobile bill accounts, the general business model is based on a consumer paying for goods or services using the same system he uses to pay for his mobile communications service (e.g. operator billing, carrier billing), although other similar business models may be offered by an MFSP to its subscribers. In these situations, the MFSP shall recognize the requirements for logging, notices and receipts (see 4.3, 4.4 and 4.5) to ensure that the consumer has access to all required information. Depending on the type of service subscription that the consumer has with the MNO or other MFSP, these payments can be either pre- or post-paid.

In the case of prepaid MFSs, the consumer is able to "top up" his account to continue to use the service. A consumer account can be topped up using various payment options available from the MFSP (e.g. cash, credit transfer).

In the case of post-paid MFSs, the MFSP periodically sends a bill to the consumer under the terms of the service subscription.

The MNO or other MFSP charges individual transactions to the consumer and settles with the merchant. The business model is determined by the MNO or MFSP. At this time, no settlement rules are contained in this document, although transparency requirements for consumers and merchants may suggest that this could be addressed in the future.

6.4.2 Stored value account (SVA)

An SVA is a deposit of funds that a consumer uses to pay for transactions or transfer pre-paid funds, which deposit may be card-based, stored on the mobile device or stored in an account the consumer accesses through the mobile device. In this case, funds are transferred from the consumer's (payer's) account to the merchant's account, or to a MFSP's account, who then settles with the merchant. Several business models are available for the MFSP who issues and handles the SVA.

7 Use cases

Essentially, all payment instruments are potentially appropriate for use with all mobile proximate payments (MPP) types, as well as for use with all mobile remote payment (MRP) types. However, there may be factors that impact how an MFSP determines which payment instrument(s) are available for use in its payment program. Depending on the type of payment, one or another payment instrument may be more appropriate. An MFSP of MPPs and/or mobile remote payments (MRPs) shall recognize the requirements for logging, notices and receipts (see 4.3, 4.4 and 4.5), so that the consumer has access to all required information. Moreover, all of these requirements are potentially subject to national or local laws and/or regulations.

NOTE Use cases included in this document are for illustration purposes only and do not foreclose the potential to develop other feasible use cases. As noted in the Introduction, it is not the intention of this document to drive technology to any specific application or to restrict the development of future technologies or solutions.

7.1 Proximate card payments use cases

7.1.1 User verification method

In many cases of MPPs, cards are understood as the payment instrument. Thus, to the extent that proximate payments are card payments, including stored value and credit/debit cards, they are defined in this subclause as a "mobile contactless card payment" (MCP).

The MPP environment offers a number of additional features which can be exploited for mobile contactless card payments with respect to a user verification method (UVM), as compared with contactless card payments using "physical" integrated circuit "chip" cards. In the latter case, for security reasons, any UVM (such as "off-line PIN") requiring off-line verification using the contactless interface is not allowed at the POI. With mobile payments, certain features of the mobile device, such as the keyboard, could be used to enter the UVM.

© ISO 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

Many mobile devices are considered to be a "personal" device, which is considered to be less vulnerable to certain types of physical attacks than a "public" terminal. However, the overall security threats to any mobile device are nevertheless similar to personal computers, including threats from malware, phishing, etc. Accordingly, potential implementers of mobile payments-to-businesses solutions shall conform to the requirements of 4.2 and 4.6 and should review the requirements and guidance provided in ISO/TS 12812-2.

As with other, a distinction between online and off-line transactions needs to be considered, leading to the combinations which are represented in Table 1.

Table 1 — Distinction between an online and off-line transaction

	No UVM	Online UVM	Off-line UVM
Online transaction	Yes	Yes	Yes
Off-line transaction	Yes	No	Yes

The usage of a UVM as an authentication credential (see ISO 12812-1) is mostly linked to the transaction risk management and is currently for contactless card payments at the discretion of the card payment application MFSP or underlying card program/scheme. Typically, only high value transactions require the usage of a UVM. For MCPs, other factors such as consumer choice may impact the usage of a UVM. Implementers interested in how specific use cases are handled under SEPA/EPC and EMV settings may wish to review European Payments Council (EPC) Document 492.09 Version 4.0. Implementers interested in how specific use cases are handled in the United States may wish to review an article titled "New Person-to-Person Payment Methods: Have Checks Met Their Match" by S. Bradford and W. Keaton.

NOTE Each of the combinations of Table 1 will be analysed in 7.1.2 and 7.1.3. The figures provided only focus on the processing of the UVM and do not include the transaction processing (on- or off-line).

7.1.2 Single tap: Analysis of UVMs

With this MPP method, the consumer performs a so-called "single" tap with his/her mobile device to conduct the MCP transaction, consisting of the following steps:

1) technology selection (contactless card payment);

2) application selection (MCP application);

3) MCP data retrieval.

Based on the MCP/POI risk analysis, an online or off-line transaction will take place which might involve a UVM.

© ISO 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

7.1.2.1 Online transactions — No UVM

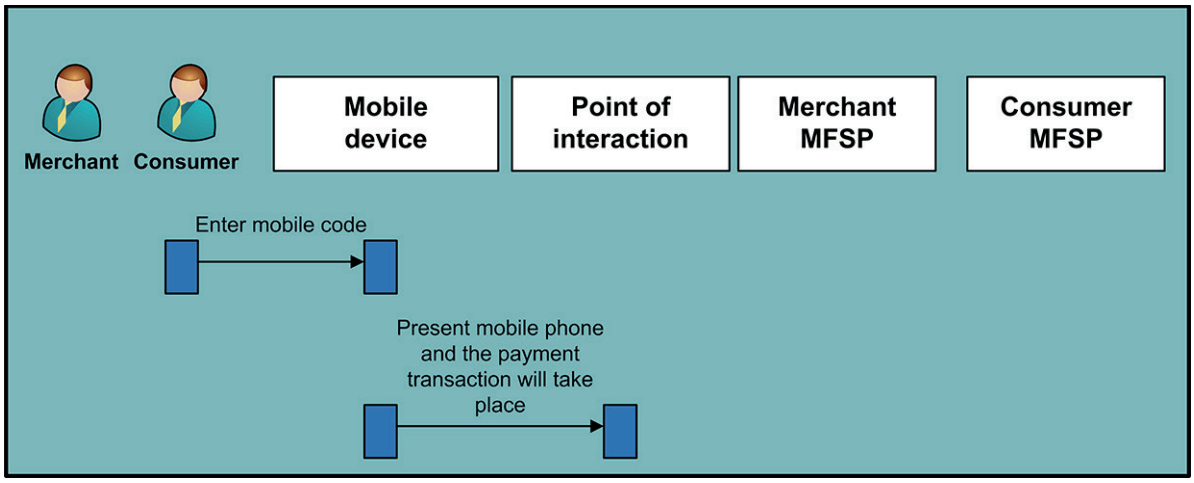

Figure 1 — Online/no UVM transaction flow

This payment method is typically intended for low value payments. The following steps will take place after the risk analysis (see steps 1 to 3 in 7.1.2):

4) online MCP application authentication/authorization; and

5) transaction completion.

In this case (see Figure 1), the transaction flow is identical to an online MCP without UVM, whereby a single tap transfers data between the mobile device and the POI. With the completion in step 5, the dedicated response message will not be forwarded to the MCP application in the mobile device.

7.1.2.2 Online transaction — Online UVM

In this MPP case, the POI will request the consumer to enter his/her mobile code (or any form of authentication credential as defined in ISO 12812-1) on the POI. The mobile code/PIN used is the PIN code associated with a "card" application (see 4.2.7).

The following steps will be carried out after the risk analysis (see steps 1 to 3 in 7.1.2):

4) online MCP application authentication/authorization;

5) online cardholder verification with mobile code entry at the POI;

6) transaction completion.

© ISO 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017

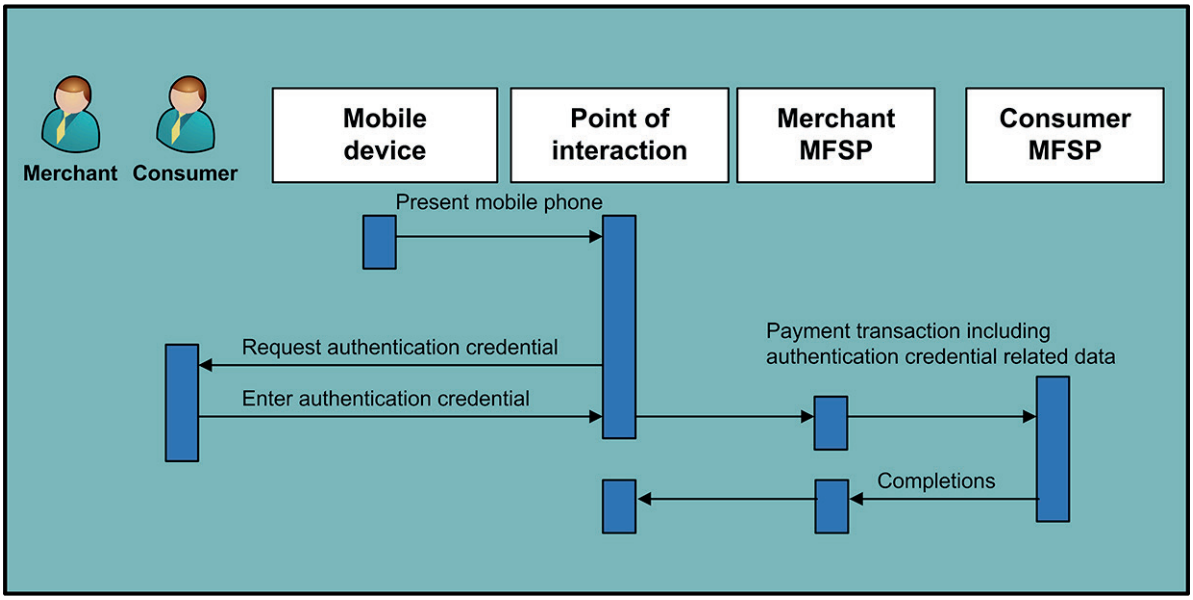

Figure 2 — Online/online UVM transaction flow

In this MPP case (see Figure 2), the transaction flow is identical to an online MCP with online UVM, whereby a single tap transfers data between the mobile device and the POI. With the completion in step 5, the dedicated response message will not be forwarded to the MCP application on the mobile device.

7.1.2.3 Online transactions — Off-line UVM

In this MPP case (see Figure 3), an off-line UVM is used which is entered by the consumer via the keyboard of the mobile device. For security reasons, this UVM is a dedicated mobile code issued by a MFSP, for which the verification is executed through the MCP application in the appropriate secure environment (see 4.2.7).

In the case of a single tap, this mobile code is entered before the tap. In this way, the result of the mobile code verification is forwarded in the online authentication/authorization message to the MFSP via the POI through the tap.

The following steps are executed with the payment transaction:

1) off-line cardholder verification with mobile code entry on mobile device;

2) technology selection;

3) application selection;

4) MCP data retrieval;

5) online MCP application authentication/authorization;

6) transaction completion.

© ISO 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TS 12812-5:2017