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

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

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

© ISO 2017

STANDARDSISO.COM : Click to view the full PDF of 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

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

Foreword

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

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

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

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

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

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

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

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

 © ISO 2017 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

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*

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

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).

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

 © ISO 2017 – All rights reserved

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);

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

— 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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

 © ISO 2017 – All rights reserved

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).

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

 © ISO 2017 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

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

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).

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

 © ISO 2017 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

 © ISO 2017 – All rights reserved

7.1.2.1 Online transactions — No UVM

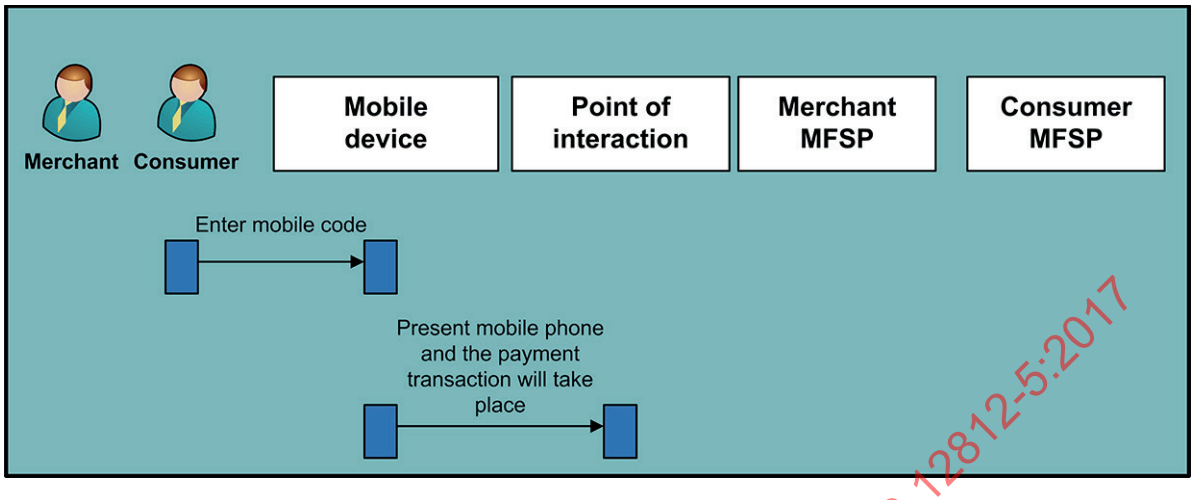


Figure 1 — Online/no UVM transaction flow

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

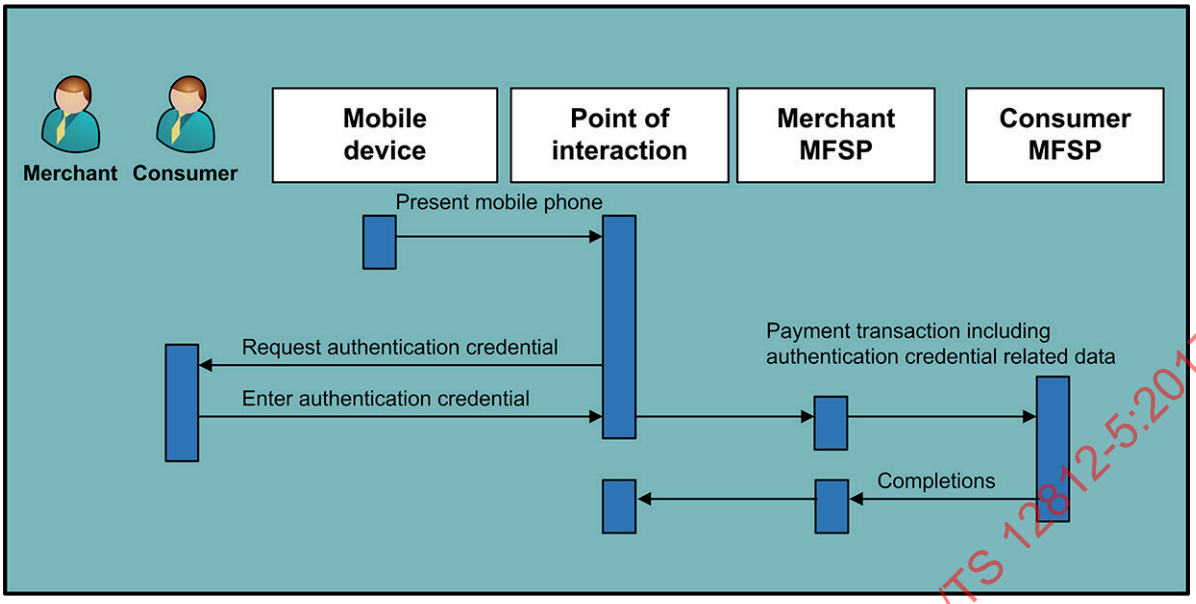


Figure 2 — Online/online UVM transaction flow

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

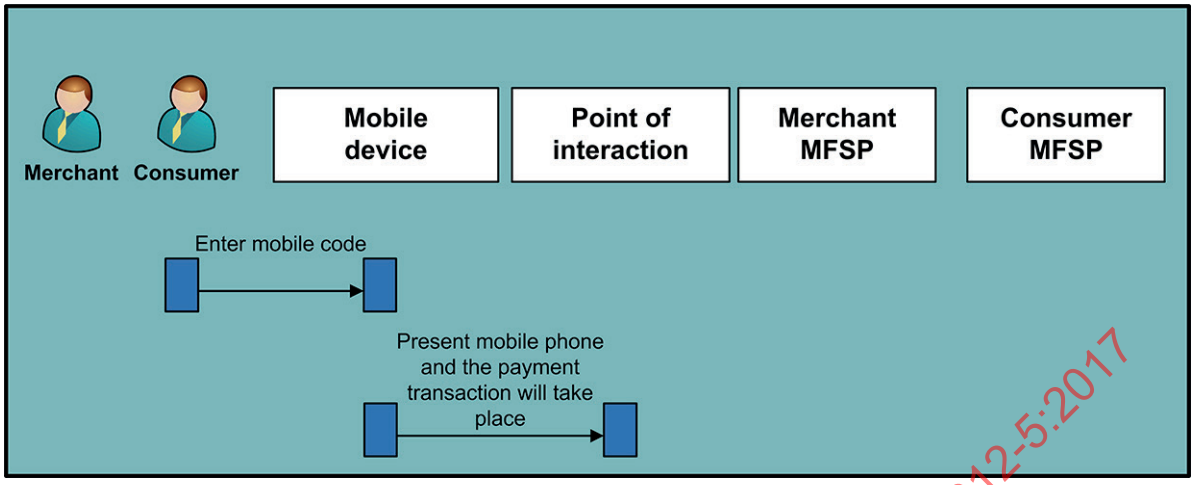


Figure 3 — Online/off-line UVM transaction flow

Again, with the completion in step 5, the dedicated response message will not be forwarded to the MCP application on the mobile device.

7.1.2.4 Off-line transactions — No UVM

This MPP method is typically intended for low value payments. The following steps will take place after the risk analysis (see steps 1 to 4 in 7.1.2.3):

5) off-line MCP application authentication/authorization;

6) transaction completion.

In this case, the transaction flow is identical to an off-line MCP without UVM, where a single tap transfers data between the mobile device and the POI.

7.1.2.5 Off-line transactions — Off-line UVM

Similar to 7.1.2.3, an off-line UVM is entered by the consumer via the keyboard of the mobile device. For security reasons, this UVM is a dedicated mobile code issued by the 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 (see Figure 4), this mobile code is entered before the tap, so that the result of the mobile code verification can be forwarded to the POI with 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 (MCP);

3) application selection (MCP application);

4) MCP data retrieval;

5) off-line MCP application authentication/authorization;

6) transaction completion.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

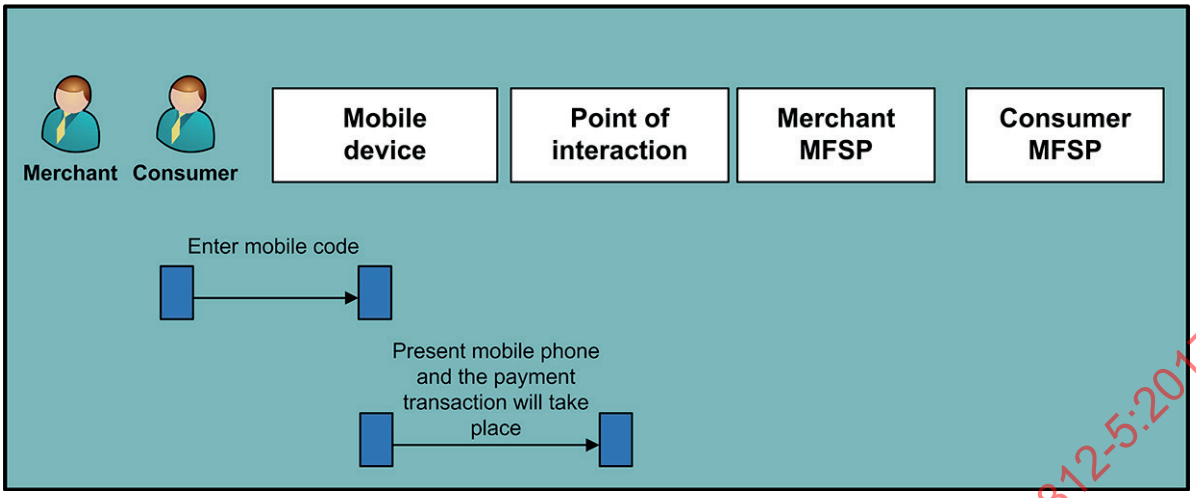


Figure 4 — Off-line/off-line UVM transaction flow

7.1.3 Double tap: Analysis of UVMs

7.1.3.1 Online transactions — Off-line UVM

In this MPP case (see Figure 5), an off-line UVM is entered by the consumer via the keyboard of the mobile device. For security reasons, this UVM is a dedicated mobile code issued by the 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 double tap, this mobile code is entered after the first tap and the result of the mobile code verification is forwarded in the online authentication/authorization message to the consumer MFSP via the POI through the second tap.

The following steps will be executed after the risk analysis (see steps 1 to 4 in 7.1.2.5):

5) confirmation of payment details, received from the POI, by the consumer via the off-line cardholder verification with mobile code entry on the mobile device;

6) online MCP application authentication/authorization;

7) transaction completion.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

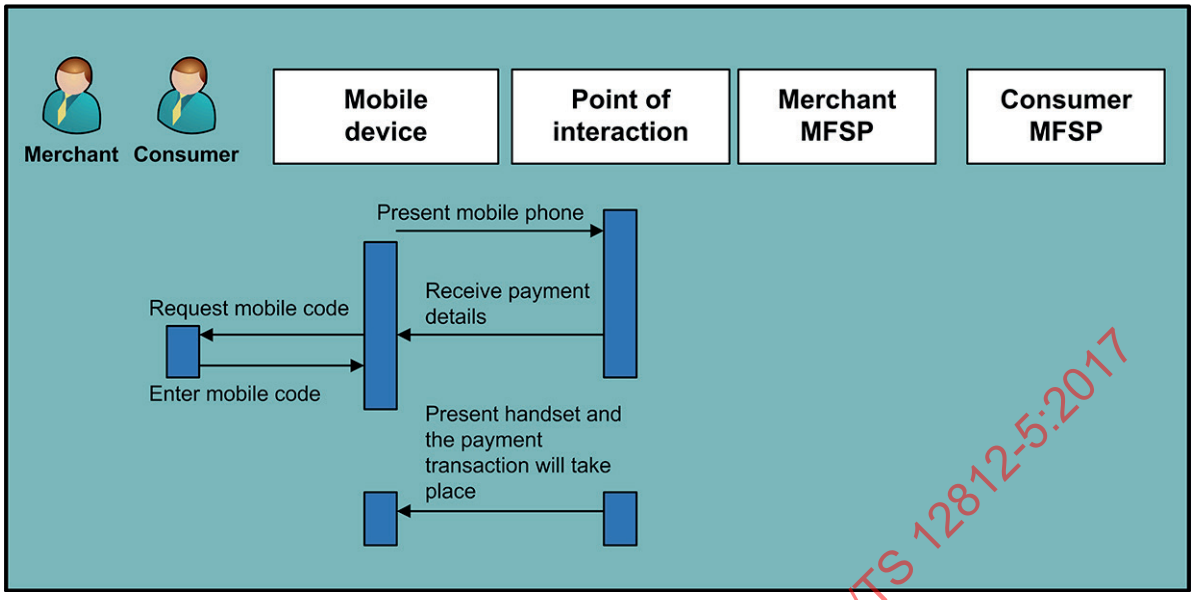


Figure 5 — Double tap online/off-line UVM transaction flow

Again, with the completion of step 5, the dedicated message will not be forwarded to the MCP application in the mobile device.

7.1.3.2 Off-line transactions — Off-line UVM

As discussed in 7.1.3.1, an off-line UVM is entered by the consumer via the keyboard of the mobile device. For security reasons, this UVM is a dedicated mobile code issued by the 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 double tap, this mobile code is entered after the first tap and the result of the mobile code verification is forwarded in the off-line authentication message to the POI with the second tap.

The following steps (see Figure 6) will be executed after the risk analysis (see steps 1 to 4 in 7.1.2.5):

5) confirmation of payment details received from the POI by the consumer via the off-line cardholder verification with mobile code entry on mobile device;

6) off-line MCP application authentication/authorization;

7) transaction completion.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

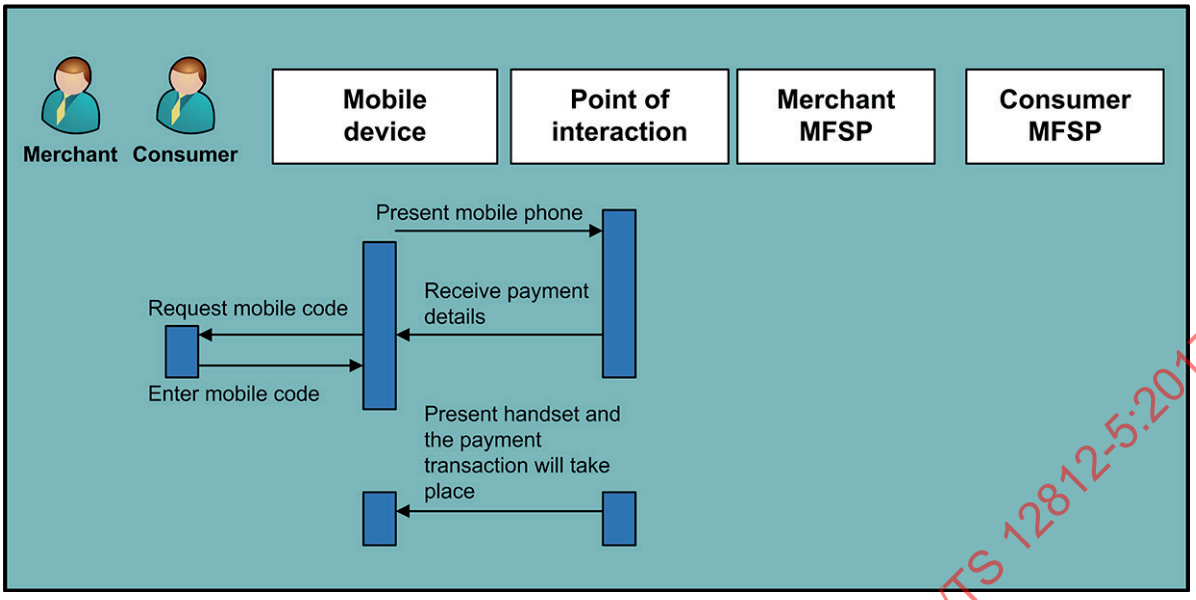


Figure 6 — Double tap off-line/off-line UVM transaction flow

7.1.3.3 Additional remarks

If the result of the completion of an MPP transaction needs to be transmitted to the mobile device, an additional tap would be required or the mobile device would need to be kept on the POI.

The same is valid for any life cycle management (e.g. risk management parameters) executed via automated processing from the MFSP to the MCP application.

NOTE 1 The consumer can be given the option to decide to always use a mobile code before the first tap, if supported by the MCP issuer.

NOTE 2 In each of the above scenarios, the mobile code could be replaced by another off-line UVM, such as biometrics.

Alternatively, some MFSPs might support the usage of a so-called “confirmation button” on the mobile device for payments without UVM to allow the consumer to acknowledge that a transaction is taking place.

7.1.4 Mobile contactless payment transaction

Table 2 shows a matrix of the possible MCP transaction types which could be carried out between a mobile device and the POI. Implementers interested in how EPC handles use cases for various types of MCP transactions should refer to the EPC Document 492.09 Version 4.0.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

Table 2 — Overview of transaction types versus UVM usage

	Transaction			
	Off-line		Online	
UVM	Single tap	Double tap	Single tap	Double tap
Online UVM (Pin on the POI)	—	—	X	—
Off-line UVM (Mobile code on the mobile phone)	X[a]	X[b]	X[a]	X[b]
No UVM	X	—	X	—

[a] Pior to tap.

[b] Between two taps.

7.1.4.1 Single tap — Off-line transaction flow — No UVM (optionally off-line UVM)

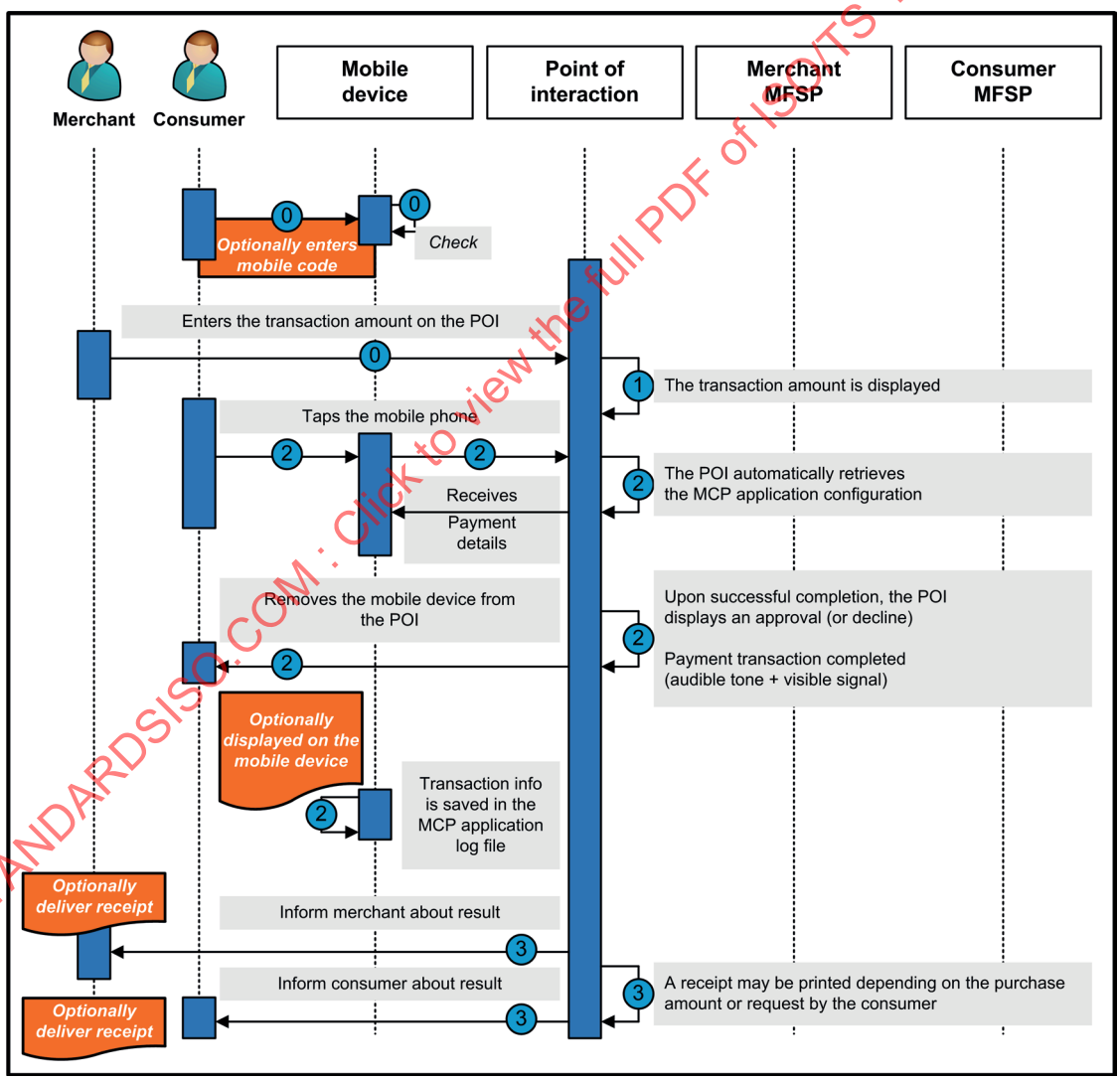


Figure 7 — Single tap — Off-line transaction flow/no UVM (optionally off-line UVM)

Step 0 (Pre-requisite)

— As an option, the consumer enters his/her mobile code to "open" the MCP application on the mobile device before starting the transaction (known as manual mode).

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

— Otherwise, the MCP application is chosen without any mobile code entry (known as automatic mode).

— The merchant enters the transaction amount on the POI.

Step 1

— The transaction amount is displayed on the POI.

— The POI requests a card payment.

Step 2

— The consumer taps his/her mobile device on the contactless reader area. (The consumer holds the mobile device close to the contactless reader area until an audible tone and/or a visible signal takes place.)

— The POI selects the contactless technology.

— The POI checks the available applications and selects the appropriate MCP application through the MPP's secure environment.

— The contactless reader and MCP application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to UVM, it is determined that no UVM is required.

— An audible tone and/or visible signal then indicate that the mobile device to contactless reader exchange is completed. After this, the mobile device can be removed from the contactless reader area.

NOTE Transaction processing at the POI might still continue.

— An off-line MCP application authentication/authorization is performed by the POI.

— After processing the off-line authorization, the POI displays an approval or decline message.

— Information about the current transaction (e.g. transaction amount) is saved in the MCP application log file and optionally displayed on the mobile device.

Step 3

— The merchant is informed about the result of the transaction.

— The consumer is informed about the result of the transaction.

— Depending on the purchase amount, the POI features and consumer choice, a transaction receipt may be printed.

NOTE See 4.4 and 4.5 for the requirements related to the issuance of receipts and notices to consumers, including notices about the legal status of a payment.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

7.1.4.2 Single tap — Online transaction flow — No UVM

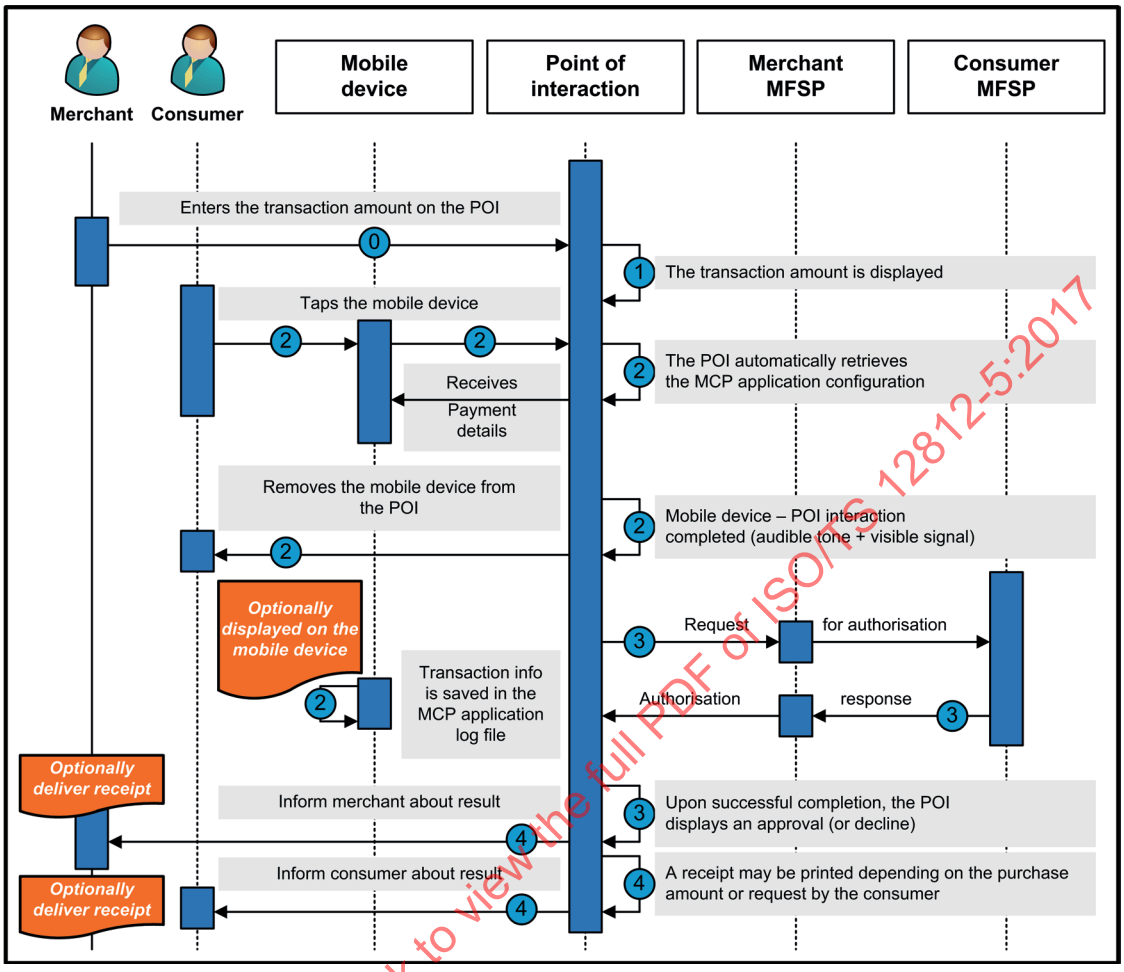


Figure 8 — Single tap — Online transaction flow/no UVM

Step 0 (Pre-requisite)

— The merchant enters the transaction amount on the POI.

Step 1

— The transaction amount is displayed on the POI.

— The POI requests a card payment.

Step 2

— The consumer taps his/her mobile device on the contactless reader area. (The consumer holds the mobile device close to the contactless reader area until an audible tone and/or visible signal take place.)

— The POI selects the contactless technology.

— The POI checks the available applications and selects the appropriate MCP application through the MPP application's secure environment.

— The contactless reader and MCP application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to UVM, it is determined that no UVM is required.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

— An audible tone and/or visible signal then indicate that the mobile device to contactless reader exchange is completed. After this, the mobile device can be removed from the contactless reader area.

NOTE Transaction processing at the POI might still continue.

— An off-line MCP application authentication is optionally performed by the POI.

— An online MCP application authorization is performed by the POI.

— The consumer then removes the mobile device from the contactless reader area.

— Information about the current transaction (e.g. online transaction requested for transaction amount) is saved in the MCP application log file and optionally displayed on the mobile device.

— The contactless reader transmits all transaction information to the POI.

Step 3

— After processing the online authorization, the POI displays an approval or decline message.

Step 4

— The merchant is informed about the result of the transaction.

— The consumer is informed about the result of the transaction.

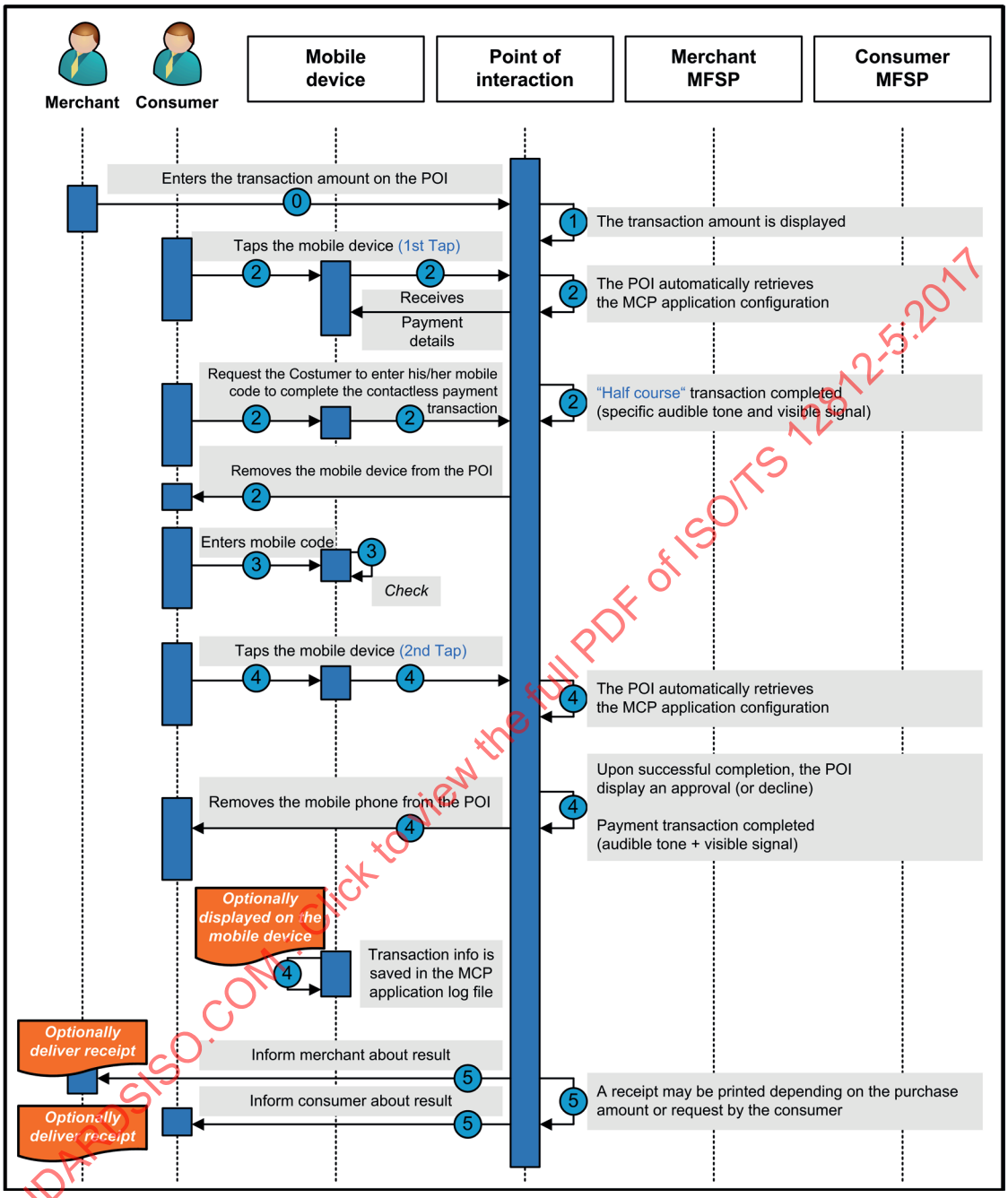
— Depending on the purchase amount, the POI features and consumer choice, a transaction receipt may be printed.

NOTE See 4.4 and 4.5 for the requirements related to the issuance of receipts and notices to consumers, including notices about the legal status of a payment.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

7.1.4.3 Double tap — Off-line transaction flow — Off-line UVM



STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

Figure 9 — Double tap — Off-line transaction flow/off line UVM

Step 0 (Pre-requisite)

— The merchant enters the transaction amount on the POI.

Step 1

— The transaction amount is displayed on the POI.

— The POI requests a card payment.

© ISO 2017 – All rights reserved

Step 2

— The consumer taps (first tap) his/her mobile device on the contactless reader area. (The consumer holds the mobile device close to the contactless reader area until an audible tone and/or visible signal takes place.)

— The POI selects the contactless technology.

— The POI checks the available applications and selects the appropriate MCP application through the MPP application's secure environment.

— The contactless reader and MCP application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to UVM, it is determined that an off-line UVM (mobile code) is required.

— A specific audible tone and/or visible signal indicate that "half-course" transaction is completed and that the consumer is prompted to enter his mobile code to complete the proximate payment transaction.

— The consumer then removes the mobile device from the contactless reader area.

Step 3

— The consumer checks the purchase amount and enters his/her mobile code on the mobile device.

— Upon successful verification of the mobile code, a message is displayed on the mobile device, requiring the consumer to again tap the mobile device on the contactless reader area.

Step 4

— The consumer taps again (second tap) the mobile device on the contactless reader area.

— An audible tone and/or visible signal then indicate that the mobile device to contactless reader exchange is completed. After this, the mobile device can be removed from the contactless reader area.

NOTE 1 Transaction processing at the POI might still continue.

— An off-line MCP application authentication/authorization is performed by the POI.

— After processing the off-line authorization, the POI displays an approval or decline message.

— Information about the current transaction (e.g. transaction amount) is saved in the MCP application log file and optionally displayed on the mobile device.

Step 5

— The merchant is informed about result of the transaction.

— The consumer is informed about result of the transaction.

— Depending on the purchase amount, the POI features and consumer choice, a transaction receipt may be printed.

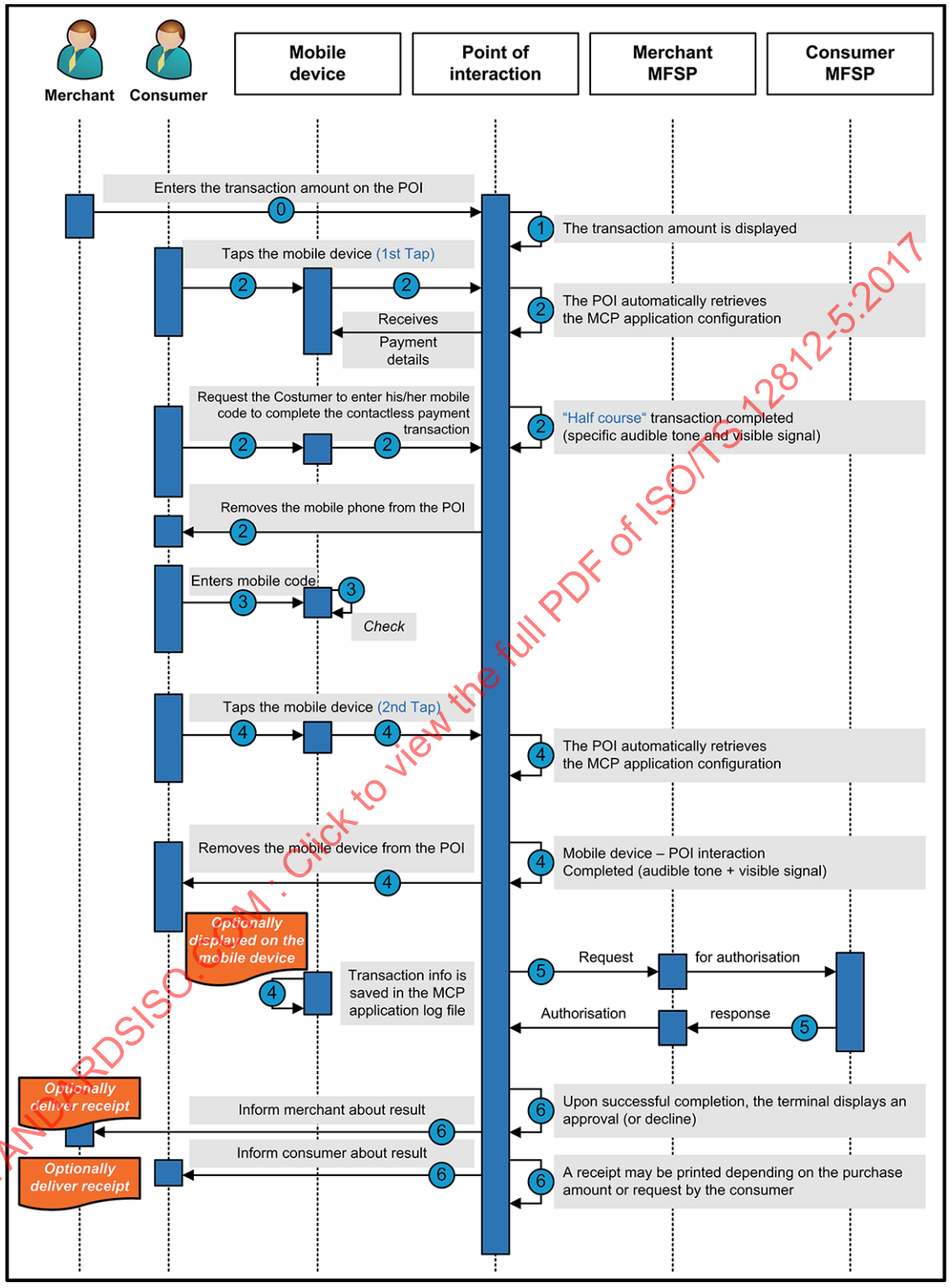
NOTE 2 See 4.4 and 4.5 for the requirements related to the issuance of receipts and notices to consumers, including notices about the legal status of a payment.

NOTE 3 Double tap is implementation dependent. It can be considered as a two-step transaction or two transactions, one as the initialization transaction and one as a payment transaction.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

7.1.4.4 Double tap — Online transaction flow — Off-line UVM



STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

Figure 10 — Double tap — Online transaction flow/off-line UVM

Step 0 (Pre-requisite)

— The merchant enters the transaction amount on the POI.

© ISO 2017 – All rights reserved

Step 1

— The transaction amount is displayed on the POI.

— The POI requests a card payment.

Step 2

— The consumer taps (first tap) the mobile device on the contactless reader area. (The consumer holds the mobile device close to the contactless reader area until the audible tone and/or visible signal occurs.)

— The POI selects the contactless technology.

— The POI checks the available applications and selects the appropriate MCP application through the MPP application's secure environment.

— The contactless reader and MCP application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to UVM, it is determined that an off-line UVM (mobile code) is required.

— A specific audible tone and/or visible signal indicate that "half-course" transaction is completed.

— The consumer is prompted to enter the mobile code in response to the UVM condition.

— The consumer enters his code (on the mobile device or on the POI in response to the prompt to complete the transaction.

— The consumer then removes the mobile device from the contactless reader area.

Step 3

— The consumer checks the purchase amount and enters his/her mobile code on the mobile device.

— Upon successful verification of the mobile code, a message is displayed on the mobile device, requiring the consumer to tap again the mobile device on the contactless reader area.

Step 4

— The consumer taps again (second tap) the mobile device on the contactless reader area.

— An audible tone and/or visible signal then indicates that the mobile device to contactless reader exchange is completed. After this, the mobile device can be removed from the contactless reader area.

NOTE 1 Transaction processing at the POI might still continue.

— An off-line MCP application authentication is optionally performed by the POI.

— An online MCP application authorization is performed by the POI.

— Information about the current transaction (e.g. transaction amount) is saved in the MCP application log file and optionally displayed on the mobile device.

Step 5

— After processing the online authorization, the POI displays an approval or decline message.

Step 6

— The merchant is informed about result of the transaction.

— The consumer is informed about result of the transaction.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

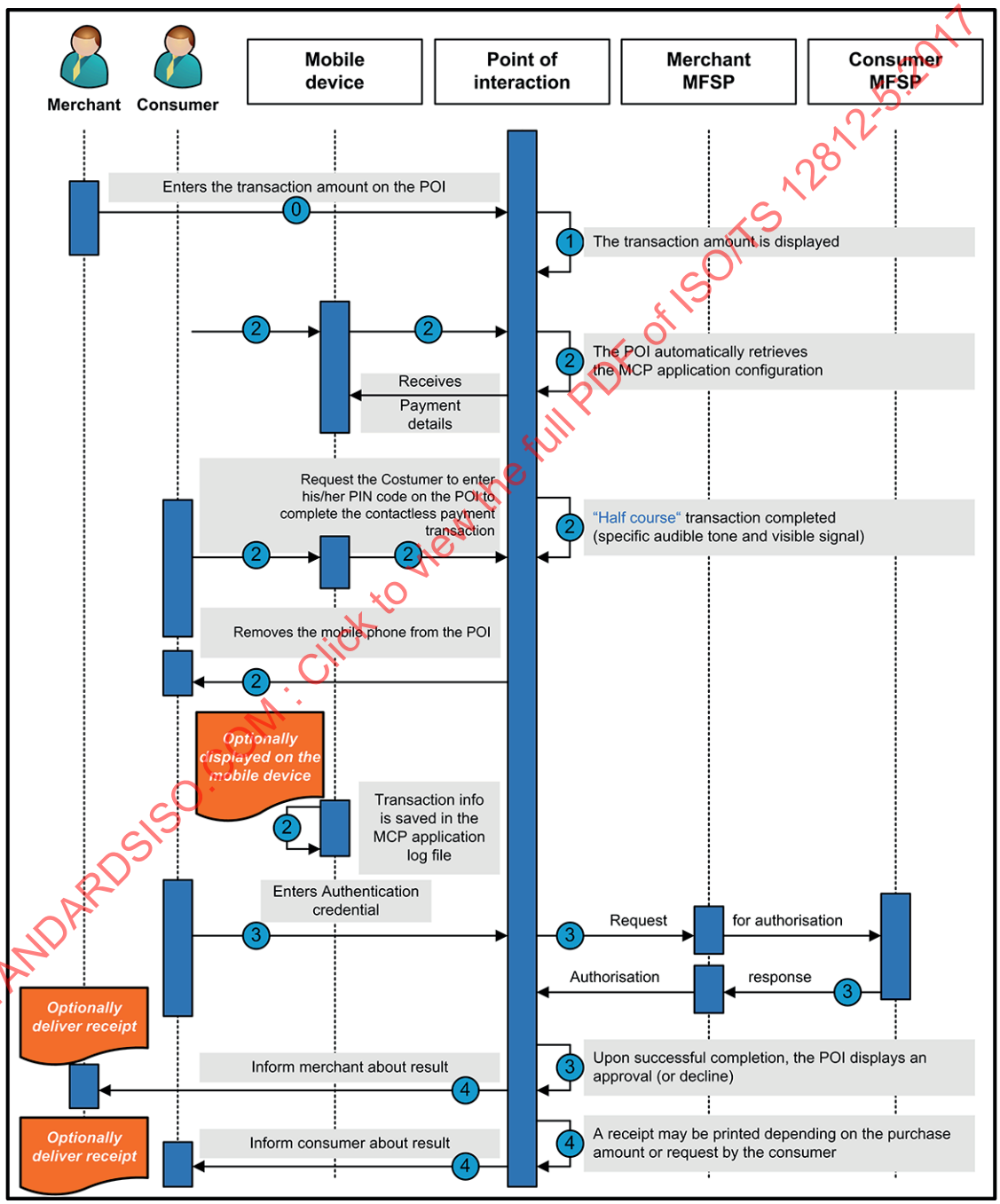
 © ISO 2017 – All rights reserved

— Depending on the purchase amount, the POI features and consumer choice, a transaction receipt may be printed.

NOTE 2 See 4.4 and 4.5 for the requirements related to the issuance of receipts and notices to consumers, including notices about the legal status of a payment.

NOTE 3 Double tap is implementation dependent. It can be considered as a two-step transaction or two separate transactions, namely, an initialization transaction followed by the payment transaction.

7.1.4.5 Single tap — Online transaction flow — Online UVM



STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

Figure 11 — Single tap — Online transaction flow/online UVM

Step 0 (Pre-requisite)

— The merchant enters the transaction amount on the POI.

© ISO 2017 – All rights reserved

Step 1

— The transaction amount is displayed on the POI.

— The POI requests a card payment.

Step 2

— The consumer taps the mobile device on the contactless reader area. (The consumer holds the mobile device close to the contactless reader area until an audible tone and/or visible signal occurs.)

— The POI selects the contactless technology.

— The POI checks the available applications and selects the appropriate MCP application through the MPP application's secure environment.

— The contactless reader and MCP application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to UVM, it is determined that an online UVM is required.

— A specific audible tone and/or visible signal indicate that "half-course" transaction is completed.

— The consumer is prompted to enter his/her mobile code in response to the UVM condition.

— The consumer enters a mobile code (on the mobile device or on the POI in response to the prompt to complete the transaction; see 4.2.7).

— The consumer then removes the mobile device from the contactless reader area.

— An off-line MCP application authentication is optionally performed by the POI.

— An online MCP application authorization is performed by the POI.

— Information about the current transaction (e.g. online transaction requested for transaction amount) is saved in the MCP application log file and optionally displayed on the mobile device.

— The contactless reader transmits all transaction information to the POI.

Step 3

— The consumer checks the purchase amount and enters a mobile code on the POI (see 4.2.7).

— After processing the online authorization, the POI displays an approval or decline message.

Step 4

— The merchant is informed about result of the transaction.

— The consumer is informed about result of the transaction.

— Depending on the purchase amount, the POI features and consumer choice, a transaction receipt may be printed.

NOTE See 4.4 and 4.5 for the requirements related to the issuance of receipts and notices to consumers, including notices about the legal status of a payment.

7.1.5 Risk management in mobile proximate payments (MPPs)

The mobile environment offers a number of additional features which can be exploited for mobile proximate card payments with respect to the transaction amount, compared with contactless card payments using "physical" plastic chip cards. In particular, the mobile environment provides a user interface (e.g. keyboard, screen) that enables the verification method (UVM), enabling transactions that require the usage of a UVM (e.g. a customer verification method such as used by various card brands or in EMV). In this latter situation, the UVM is referred to as the cardholder verification method (CVM);

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

 © ISO 2017 – All rights reserved

some of the controls described in this clause relate specifically to CVM examples, but the generic term UVM is used. Similarly, over-the-air (OTA) is an additional channel available to the MFSP for managing the application, including the risk parameters, which reduces its dependency on the POI capabilities.

As with other mobile contactless card payments, a distinction between online and off-line transactions needs to be considered from a risk management perspective. Therefore, a number of risk parameters are used. These parameters are set up by the MFSP or the acquirer according to the underlying MFS payment program.

In addition, the application has a set of features for risk management, such as counters and limits that will be used to make the decision for a particular transaction. The purpose of this subclause is to present these risk management parameters for MPPs.

Moreover, any limits set should take into account risks as they may be perceived by consumers and should therefore allow consumers to vary the limits downwards if they wish.

7.1.5.1 Form factor

Certain functions might require the identification of functionality that is linked to the type of form factor (e.g. physical card or mobile device) being used.

Therefore, the application will have a data element indicating this functionality and, as far as this indication impacts the transaction, the data element shall be reliable and therefore authenticated.

Independent of the functionality linked to specific form factors, the application may also include a data element indicating the form factor. In so far that these data are not authenticated, it can only be used for information (e.g. statistics) by the POI, the acquirer or the MFSP.

7.1.5.2 Point of interaction risk parameters

7.1.5.2.1 UVM limit

The UVM limit is a risk management parameter indicating the maximum value of a transaction which does not require a UVM.

Transactions for which the value is less than, or equal to, the UVM limit are typically low risk payment environments (e.g. low value) where convenience and speed are important and the usage of a UVM would not be appropriate. Transactions for which the value is greater than the UVM limit require the usage of a UVM. This can be an online PIN or an off-line mobile code (see 4.2.7).

The value of the UVM limit is set in the POI application and defined by the MFS payment program or scheme (at country/region/global level). It shall take into account the risk of fraudulent transactions (e.g. in case of loss or theft of the mobile device), while preferably using, within a program or scheme, the same contactless UVM limit, independent of the form factor. In addition, for consistent consumer and merchant experience (and education), the contactless UVM limit should ideally be the same for all programs/schemes in a certain geography (e.g. a country, SEPA area).

An overview on the UMV usage is given in Table 3 in the context of an EMV implementation (i.e. where use of the term CVM is appropriate).

Table 3 — UVM usage

Transaction amount	≤UVM limit	>UVM limit
UVM	Optional	Mandatory

NOTE Optional in Table 3 means that the UVM can be used, depending on the outcome of other UVM-related risk management.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

7.1.5.2.2 Floor limit

The floor limit is a parameter indicating the value of a transaction above which an online authorization by the MFSP is required.

— Transactions for which the value is less than or equal to the floor limit may be approved off-line by the MFS application.

— Transactions for which the value is greater than the floor limit which are not authorized online by the MFSP will be handled under applicable operating rules.

The value of the floor limit is set in the POI application and defined by the acquirer under the scheme rules (it may depend on different factors, such as the Merchant Category Code or the payment product).

NOTE 1 Information on the use of Merchant Category Codes is found in ISO 18245.

NOTE 2 Even if the transaction value is less than the floor limit, the POI might require an online authorization, due to the random online transaction selection by the POI set by the acquirer, if this option is supported by the POI.

7.1.5.3 MPP risk parameters

The following subclauses provide a description of possible MPP risk parameters. It is at the discretion of the MFSP to make a choice on which parameters will be supported or to add any other risk parameter that seems to be appropriate.

7.1.5.3.1 Mobile code try limit and counter

Mobile code try limit is not only a parameter to indicate the maximum number of consecutive incorrect mobile code trials allowed, but also is one to be determined considering entirely a type of transactions, value amount of transactions, and accumulated number of incorrect trials. As such, a mobile code may be used as a UVM.

The number of mobile code trials is recorded and the mobile code try counter represents the remaining number of trials allowed. The mobile code try counter is reset to the mobile code try limit after successful mobile code verification by the MFS application.

If the mobile code try counter is equal to zero, indicating no remaining mobile code trials are left, all further MPP transactions requiring a UVM, and optionally all mobile proximate transactions:

— are declined by the MFS application until the mobile code try counter is reset by the MFSP; or

— are routinely sent online to the issuing bank, indicating that the mobile code try counter has reached zero, until the mobile code try counter is reset by the MFSP.

The value of the mobile code try limit is set in the MFS application and defined by the MFSP.

7.1.5.3.2 Consecutive No-UVM Limit and Counter

The Consecutive No-UVM Limit is a parameter indicating the number of consecutive transactions which can be performed before a UVM (typically a mobile code) is requested to protect against fraud.

The total number of No-UVM transactions is recorded in the Consecutive No-UVM Counter, which is managed by the MFS application.

When a transaction is performed and the resulting Consecutive No-UVM Counter is greater than the Consecutive No-UVM Limit, then a UVM is required.

The Consecutive No-UVM Counter will be reset by the MFS application after the successful mobile code verification.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

The value of the No-UVM Limit is set in the MCP application and defined by the MFSP, according to the program/scheme rules, taking into account:

— the risk of fraudulent transaction (e.g. in case of loss or theft of the mobile device), and

— the convenience from the consumer perspective.

7.1.5.3.3 UMV-based risk management

Table 4 provides an overview on the risk management related to the UMV as discussed above in the context of an EMV or branded card transaction.

Table 4 — UVM-based risk management

Transaction	Consecutive No-UVM Counter ≤ Consecutive No-UVM Limit	Consecutive No-UVM Counter > Consecutive No-UVM Limit
UVM	Optional	Mandatory

The Consecutive No-UVM Limit is the maximum number of consecutive transactions without UVM.

NOTE Optional in Table 4 means that the UVM can be used depending on the outcome of other UVM-related risk management.

7.1.5.4 Cumulative Off-line Limit and Amount Accumulator

The Cumulative Off-line Limit is a parameter indicating the maximum total value of transactions (amounts) which can be performed before an online authorization request is required to protect against fraud or overdraft.

The total amount of off-line transactions is recorded in the Cumulative Off-line Amount Accumulator, which is managed by the MFS application.

When an off-line transaction is performed and the resulting Cumulative Off-line Amount Accumulator reaches the Cumulative Off-line Limit, then an authorization request is required.

The Cumulative Off-line Amount Accumulator may be reset per definition by the MFSP in one of the following ways:

— via automated processing performed OTA; here two modes exist, the so-called “push” (prompt initiated by a MFSP host) and “pull” (prompt initiated by the MPA) modes. This reset may be optionally confirmed by using the mobile code entered by the consumer;

— via automated processing of a message performed via the POI using NFC. This might require an additional tap or placing the mobile device on the NFC interface of the POI.

The value of the Cumulative Off-line Limit is set in the MFS application and defined by the MFSP according to the program/scheme rules, taking into account:

— the risk of fraudulent transaction (e.g. in case of loss or theft of the mobile device);

— the credit risk;

— the convenience of transaction processing from the consumer perspective.

The MFSP may decide to use two different values, namely an upper and a lower limit, instead of the Cumulative Off-line Limit. In this case, if the total amount of off-line transactions is between the two values, an online transaction will be requested, if possible. When the upper limit is reached, the transaction shall be processed online. If this is impossible because of an off-line POI, the transaction will be declined.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

7.1.5.4.1 Consecutive Off-line Limit and Counter

The Consecutive Off-line Limit is a parameter indicating the number of consecutive off-line transactions which can be performed before an online authorization request is required to protect against fraud or overdraft.

The total number of off-line transactions is recorded in the Consecutive Off-line Counter[1)] which is managed by the MFS application.

When an off-line transaction is performed and the resulting Consecutive Off-line Counter reaches the Consecutive Off-line Limit, then an authorization request is required.

The Consecutive Off-line Counter may be reset per definition by the MFSP in one of the following ways:

— via automated processing performed OTA; here two modes exist, the so-called "push" (prompt initiated by a MFSP host) and "pull" (prompt initiated by the application) modes. This reset may be optionally confirmed by using the mobile code entered by the consumer;

— via automated processing of a message performed via the POI using NFC. This might require an additional tap or placing the mobile device on the NFC interface of the POI.

The value of the Consecutive Off-line Limit is set in the application and defined by the MFSP according to the program/scheme rules, taking into account:

— the risk of fraudulent transaction (e.g. in case of loss or theft of the mobile device);

— the credit risk;

— the convenience of transaction processing from the consumer perspective.

The MFSP may decide to use two different values, namely an upper and a lower limit, instead of the Consecutive Off-line Limit. In this case, if the total number of off-line transactions is between the two values, an online transaction will be requested if possible. When the upper limit is reached, the transaction shall be processed online. If this is impossible because of an off-line POI, the transaction will be declined.

7.1.5.4.2 Overview risk management off-line/online transactions

Table 5 provides an overview of the risk management related to online and off-line transaction mode as discussed above.

Table 5 — Online/off-line risk management

Transaction	Amount ≤ Floor limit	Cumulative Off-line amount ≤ Cumulative off-line limit	Consecutive Off-line counter ≤ Consecutive off-line limit	> Floor limit or cumulative off-line limit or consecutive off-line limit
Mode	Online/off-line	Online/off-line	Online/off-line	Online

Floor limit is the maximum value of the transaction amount for an off-line transaction.

Cumulative off-line limit is the maximum amount of cumulative off line transactions.

Consecutive off-line limit is the maximum number of consecutive off line transactions.

In case of a reset, both the cumulative off-line amount accumulator and consecutive off-line counter will usually be reset together.

1) The consecutive off-line counter counts the number of transactions since the counter was explicitly reset by the MFSP. An online transaction does not necessarily result in the counter being reset.

© ISO 2017 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

7.1.6 Additional features

7.1.6.1 Transaction logging

Each application should have its own transaction logging function (see 4.3). While specific methods of conforming to that requirement are left to each individual MFSP, it may be useful to discuss how such functionality may operate.

The application should store the transaction details in a dedicated log file in the application. It is recommended that, at a minimum, the last 10 transactions initiated should be displayable[2)] to the consumer or transactions over a 30-day period whichever is the longer, although each MFSP has the discretion to determine the maximum number of transactions stored in the log file remains. Since online transactions may be declined by the MFSP, the transaction log may not match with the actual transaction statement. However, this transaction log allows the consumer to at least check independently the last 10 transactions initiated. As indicated in 4.3, the MFSP should adopt a procedure to give additional log information to a consumer upon request under reasonable terms.

Every time a proximate transaction is initiated, a new record[3)] can be created and the transaction logging is updated in the application. Then the user interface can retrieve the appropriate information from this log file to allow the consumer to view the details of the transactions initiated. The user interface shall, at a minimum, enable the mobile device to conform to the requirements of 4.4 (i.e. display the last 10 transactions per application, or the transactions over the past 30 days, whichever provides more information).

The ordering of the transactions are recorded so Record #1 is the most recent transaction and Record #2 is the transaction prior to that, etc.

The application updates the log file, which should contain the following log data, without which a consumer cannot adequately identify the specific transaction:

— transaction date and/or transaction time/application transaction counter (ATC);

— amount, authorized;

— amount, other (i.e. cash-back);

— transaction currency code;

— cryptogram information data (token information);

— transaction type;

— merchant name and location.

Methods of presenting the transaction history within the user interface should be the choice of the MFSP/MFSP. Transactions in the logging should be able to be sorted by:

— date (from most recent to oldest);

— amount (ascending/descending);

— transaction type (debit/refund).

Depending on the MFSP's business requirements, an access control for this transaction logging display may be implemented. This control is performed by requesting mobile code verification. The MFSP may also choose to provide the consumers the ability to enable or disable this access control themselves.

---

2) The MPP application will always have a user interface associated with it. The log data should be extracted from the MPP application and stored within the user interface.

3) Considering the integrity and security data aspect, the data within the MPP application's transaction log is not considered to be secure (i.e. there is no guarantee that EMV transaction logging data originated from a transaction with a secure terminal).

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

7.1.6.2 Receipts

The transaction receipt is a requirement to provide a payment receipt intended for the consumer (see 4.5). While specific methods of conforming to that requirement are left to each individual issuer, it may be useful to discuss how such functionality may operate.

The handling of transaction receipts for MPP should be identical to the ones for transactions performed with physical cards. For POI capable of printing a transaction receipt, it provides a receipt upon the consumer's request. If the POI knows in advance that it cannot print a transaction receipt, it informs the consumer that no receipt can be printed and offers the consumer the choice to continue or abort the transaction.

Because mobile devices may offer additional capabilities, receipts may also be provided via other channels (e.g. electronic receipts) which are not yet defined. The MFSP should take reasonable steps to inform consumers about the different legal status of forms of transaction records (e.g. consumers may find that they need a digital receipt if one cannot be printed).

7.1.6.3 Data sharing between MPP applications from a single issuer

A given MFSP may want to provide multiple MFSs by loading different applications in an SE or other secure environment. Mechanisms may be available to allow the sharing of resources between these applications, such as risk management counters and limits, and mobile code. For example, this may be to address common business or security policies.

Data sharing may have advantages for both MFSPs and consumers. For example:

— sharing risk management counters and limits between MPP applications simplifies risk management of these MPP applications by the MFSP;

— sharing the mobile code and (some of) its attributes (mobile code try counter and limit and mobile code verification status) may improve the consumer experience;

— sharing MPP application state information (e.g. activated) may simplify administrative operations and life cycle management of the MCP applications by the MFSP and MFS application choice by the consumer.

7.1.7 Interoperability and MPP service availability

Some countries have chosen to systematically process payment transactions online, while other countries have opted for a mix of online and off-line transactions, depending on the acquirer and the MFSP risk management configuration.

As long as MPP transactions remain domestic transactions, interoperability could be ensured. But what will happen if a consumer who uses an application based on an "online" tries to make an MPP transaction at a merchant using an "off-line" program (e.g. in different countries)? A transaction that needs to go online in a pure off-line environment will be declined.

NOTE A similar problem exists for a physical card.

The card programs and the MFSPs should take appropriate actions to ensure the interoperability among all use cases, with minimal impact on the consumer side and maximizing the service availability.

One other aspect which might have an important impact on the consumer is the usage of the single or double tap. This situation might even get more complex if other contactless services, such as loyalty and couponing, are performed in conjunction with the MPP transaction. Therefore, MFSPs that develop and offer MPP applications are encouraged to ensure at least consistency among MFSPs in a given geography. Moreover, MFSPs using MPP applications should appropriately educate their consumers in this respect.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

7.2 Remote payments use cases

In the context of this document, the mobile remote payments (MRPs) are payments which are initiated using a mobile device where the transaction is conducted over a mobile telecommunication network (e.g. GSM, mobile Internet) and which can be made independently from the payer's location (and/or this means that the transaction is not dependent on physical contact with a POI, e.g. point of sale device).

7.2.1 Mobile remote card payments

7.2.1.1 Card payment without an MRP

The use case can be described as follows.

a) The consumer uses his/her mobile device to navigate to a merchant website via mobile Internet and selects the goods or services to be purchased.

b) After having accepted the merchant's general purchase conditions, the consumer is prompted to confirm the purchase.

c) The checkout section of the merchant website displays the transaction details, including the amount and the payment options, via the mobile device to the consumer.

d) The consumer is redirected to the payment section. Here, more than one alternative can be found depending on the implementation:

   1) the consumer enters the card details in the checkout section of the merchant website;

   2) the consumer enters the card details in the virtual POI (virtual POS in this case) of the merchant's acquirer; or

   3) the consumer selects a payment option base on a digital wallet that is a card container, where a card can be chosen from a menu or list (in most cases, the consumer shall subscribe the wallet service in advance).

e) The transaction summary is displayed on the mobile device indicating the date, the merchant reference, the amount and the selected payment card and the consumer is prompted to confirm the transaction.

f) The transaction is processed to obtain the authorization. Additional steps may be performed to satisfy requirements for strong authentication to prevent fraud. When both card and virtual POI require strong authentication, then a dynamic authentication method is executed.

g) Once the payment is authorized, the consumer is automatically redirected to the merchant website and receives a confirmation of the transaction, including transaction details.

h) A receipt is sent by the merchant to the consumer (see 4.5).

i) The merchant releases the goods or services to the consumer.

This use case is based on current infrastructure for card payments and follows the standard processes for card payments in a four-corner model with the consumer, the card issuer the merchant, and the acquirer.

— The consumer (cardholder) enters the PAN, expiry date and Card Security Check (CSC) (static authentication) onto the payment page (which is transmitted in the authorization message via the acquirer to the issuer), or

— the consumer is redirected to the MFSP's authentication server (or its agent) to perform a static or dynamic authentication (e.g. the so-called 3D Secure method).

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

7.2.1.2 Card payment with an MRP

This use case can also be performed using mobile internet browsing via a mobile device. However, it is often more convenient to use an MRP installed on the mobile device. The use case can be described as follows.

a) The consumer opens the MRP application of his/her MFSP on his or her mobile device. The application can be a stand-alone application, a widget in the mobile wallet or an MRP application that is accessed through the mobile browser on the mobile device. Within the MRP application, the consumer would have already configured a card as an active card to use for making transactions and by default, the transaction will be charged to that active card. The consumer can activate or deactivate cards anytime using the application settings.

b) The consumer authorizes the transaction according to the security policies of the MFSP.

c) Once the transaction is authorized, the merchant's account is credited.

d) The transaction is then confirmed and all transaction data are displayed on the mobile device screen.

e) The merchant optionally receives a message from its MFSP with a notification of the transaction (the consumer's card account has been debited).

In this use case, the following requirements may need to be supported:

— The consumer may have an MNO subscription for the MFS. In case that mobile phone number is used for identifying the merchant, then the merchant may also need to be subscribed to the MFS.

— In terms of interoperability, in early stages, the consumer and the merchant may use the same cards scheme/program because it may well be that the cross card schemes may not be supported.

— A platform is required to link the mobile phone number with the payment card details. This association allows the appropriate routing of the transaction. During the consumer/payer enrollment process of the service, this association of the mobile phone number and payment/card number is performed.

7.2.1.2.1 MRP with no UVM

In this scenario, illustrated in Figure 12, the consumer uses his/her mobile device to initiate a payment to a merchant for the purchase of goods or services (e.g. mobile content); however, no UVM is used. This scenario is also valid when the consumer is a business.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

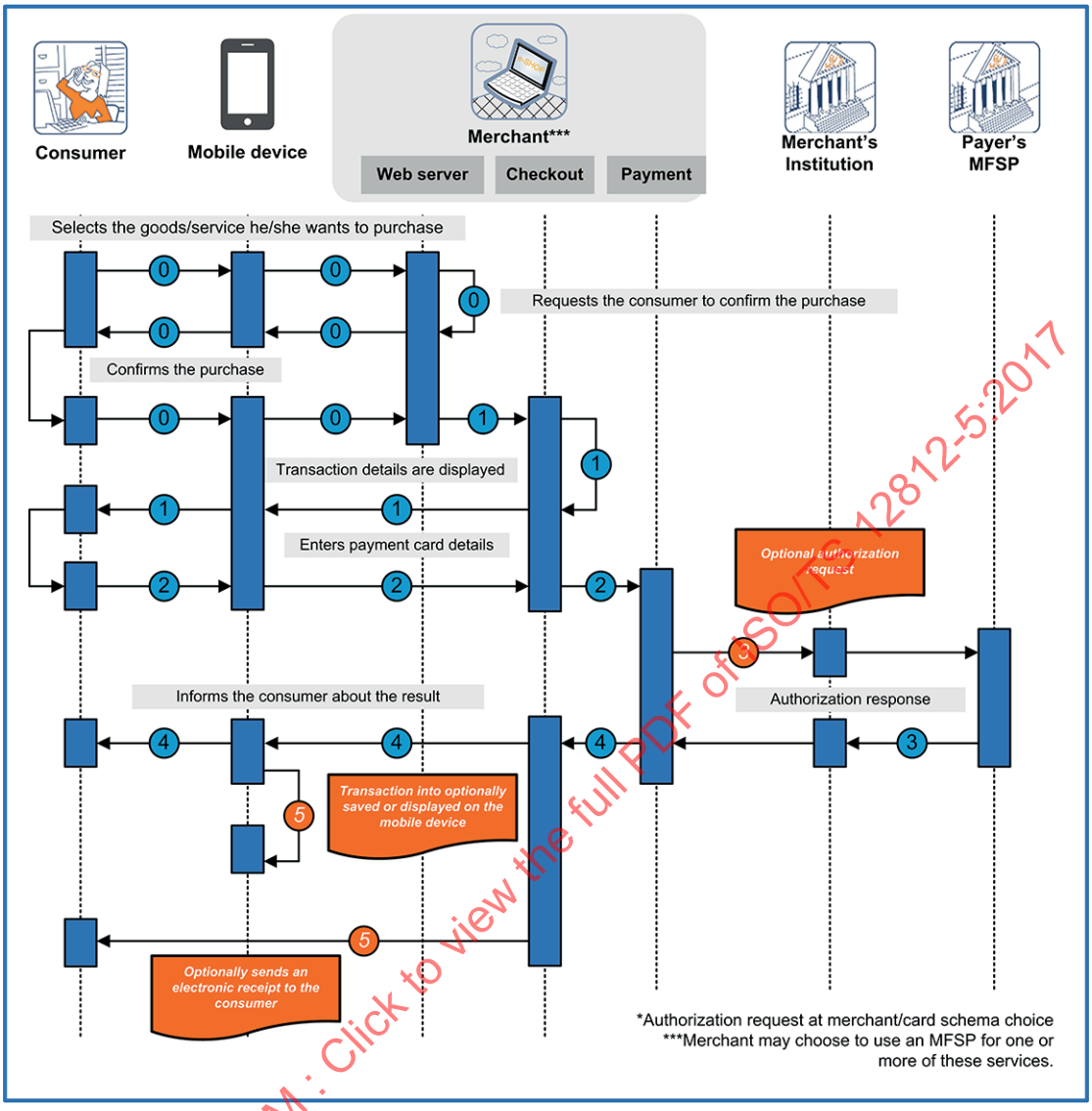


Figure 12 — MRP card/no UVM

In Figure 12, the following steps are illustrated:

Step 0 (Pre-requisite)

— The consumer navigates using his/her mobile device to a merchant website via mobile internet and selects the goods/service he/she wants to purchase.

— After accepting the general purchase conditions offered by the merchant, he/she is requested to confirm the purchase.

Step 1 (Transaction details displayed)

— The checkout section of the merchant website displays the transaction details including the amount and the payment options, via the mobile device to the consumer.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

Step 2 (Card payment selection)

— The consumer selects the “payment by card” option via mobile internet and is requested to enter his/her payment card details[4]. The consumer is redirected to the payment section under the control of a payment gateway to proceed with the transaction under a secure connection (e.g. TSL).

— As an alternative to the entry of the payment card details by the consumer, there may be an application stored in, or accessed through, the mobile device. The consumer is then redirected to the user interface of this application to select the payment card to be used and the card details are automatically transferred to the payment section.

— The transaction summary is displayed on the mobile device, typically including the date, the merchant reference, the amount and the selected payment card whereby the consumer is invited to confirm the transaction.

Step 3 (Payment process)

— The payment is processed as a remote card transaction. This may involve an online authorization request by the merchant (see 4.3.2.7.1 in EPC[10]).

Step 4 (Transaction finalization)

Once the payment is authorized:

— The consumer is automatically redirected to the merchant website and receives a confirmation of the transaction.

— The merchant releases the good/service to the consumer.

Step 5 (Transaction information)

— Transaction information (such as the transaction amount) may be saved in an MRCP application log file and/or optionally displayed on the mobile device.

— An electronic receipt may be sent by the merchant to the consumer.

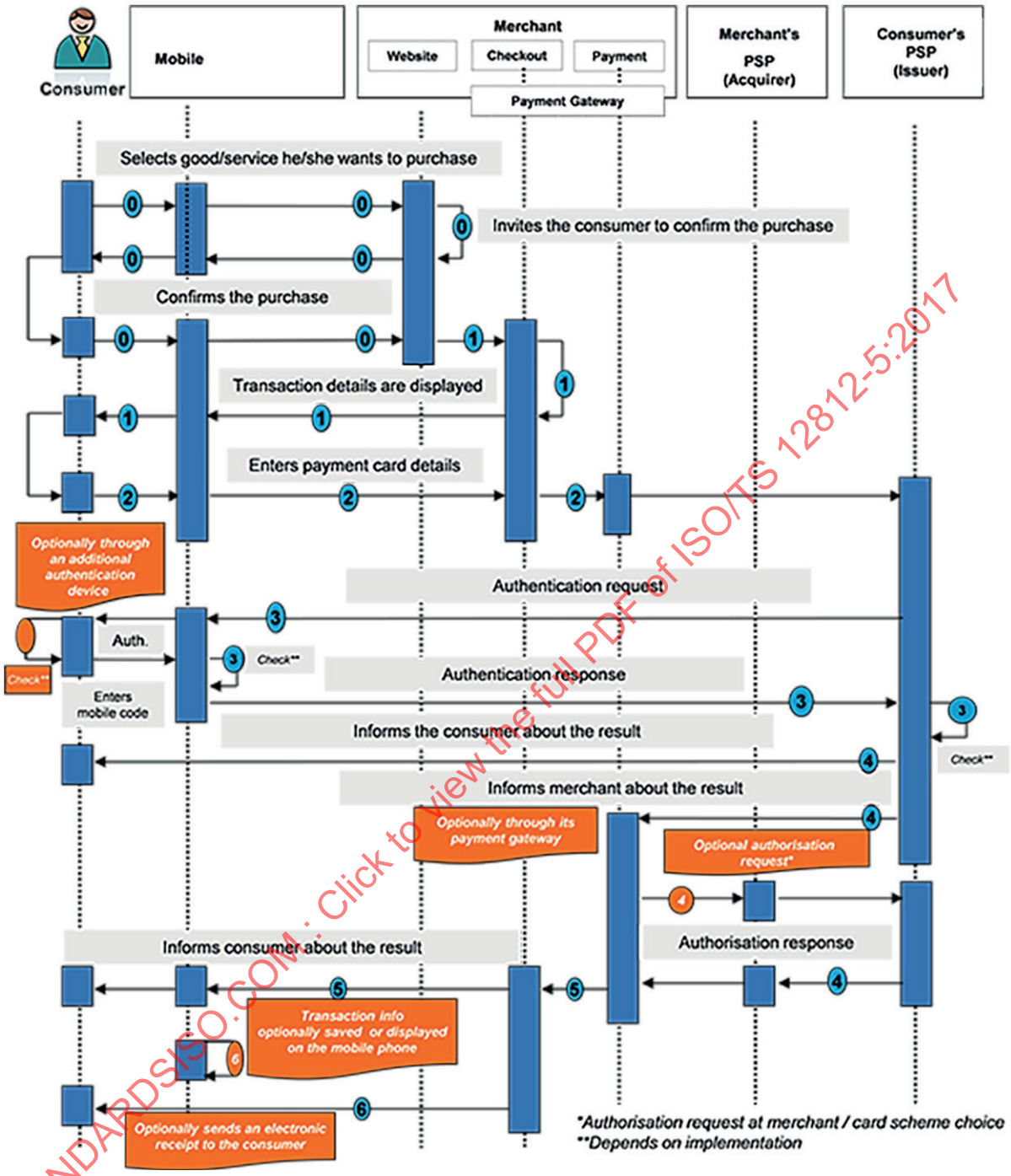
7.2.1.2.2 MRP with strong dynamic authentication

In this scenario, illustrated in Figure 13, the consumer uses his/her mobile device to conduct a payment to a merchant, which is providing goods or services (e.g. mobile content), using a “strong dynamic authentication method.” This scenario is also valid when the consumer is a business.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

4) Depending on the implementation, the card details may be entered in the checkout section of the merchant website or alternatively, by use of a third-party merchant MFSP.

© ISO 2017 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

Figure 13 — MRP (strong dynamic authentication)

In Figure 13, the following steps are illustrated:

Step 0 (Pre-requisite)

— The consumer navigates using his/her mobile device to a merchant website via mobile internet and selects the goods/service he/she wants to purchase.

— After having accepted the general purchase conditions, he/she is requested to confirm the purchase.

© ISO 2017 – All rights reserved

Step 1 (Transaction details displayed)

— The checkout section of the merchant website displays the transaction details including the amount and the payment options, via the mobile device to the consumer.

Step 2 (Card payment selection)

— The consumer selects the "payment by card" option via mobile internet and he/she is invited to enter his/her payment card details[5]. The consumer is redirected to the payment section under the control of a payment gateway to proceed with the transaction using a secure connection (e.g. TLS).

— As an alternative to the entry of the payment card details by the consumer, there may be an application stored in, or accessed through, the mobile device. The consumer is then redirected to the user interface of this application to select the payment card to be used and the card details are automatically transferred to the payment section.

— The transaction summary is displayed on the mobile device, typically including the date, the merchant reference, the amount and the selected payment card whereby the consumer is invited to confirm the transaction.

Step 3 (Authentication)

The consumer and the relevant data are subsequently authenticated[6] by his/her MFSP according to one of the following typical processes:

— In case of a payment card via mobile internet, the consumer and the relevant data are authenticated by its MFSP via a strong dynamic authentication method. Various methods may exist involving the usage of an additional authentication device. The consumer inserts his/her payment card into the additional device; the consumer's MFSP provides the consumer with a "challenge" to be entered/transmitted (on)to the additional device, followed by the consumer's mobile code entry. The authentication device then generates a "response" which the consumer is requested to enter at a given time during this process on his/her mobile device. The response is subsequently transmitted to the consumer's MFSP via the authentication response for verification[7].

— In case an authentication application is present on the mobile device, a dynamic authentication method (e.g. challenge/response method) is initiated by the consumer's MFSP and is handled automatically by the authentication application in a secure environment. The consumer is requested to enter his/her mobile code[8] (UVM) only once during the MRP transaction process. The mobile code is checked either locally (off-line UVM) by the authentication application or by the consumer's MFSP (online UVM).

Step 4 (Payment process)

— The consumer is informed by his/her MFSP about the result of its authentication.

— The merchant is informed (possibly involving its payment gateway) by the consumer's MFSP about the result of the authentication of the consumer.

— Subject to successful authentication by the consumer's MFSP, the payment is further processed as a MRP. This may involve[9] an online authorization request by the merchant to the consumer's MFSP (see 4.3.2.7.1 in EPC[10]).

5) Depending on the implementation, the card details may be entered in the checkout section of the merchant website or alternatively by use of a third-party merchant MFSP.

6) This authentication may involve transaction details.

7) The authentication process is very similar to the one used in a MRP.

8) Use of the mobile code in combination with the dynamic authentication effectively results into a strong dynamic authentication.

9) In particular cases, the authorization request could be optional, depending on the type of payment card and the merchant's decision. But, in any case, the capability to do an authorization request shall be present.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

Step 5 (Transaction finalization)

Once the payment is authorized:

— The consumer is automatically redirected to the merchant website and receives a confirmation of the transaction.

— The merchant releases the good/service to the consumer.

Step 6 (Transaction information)

— Transaction information (such as the transaction amount) may be saved in an MRP application log file and/or optionally displayed on the mobile device.

— An electronic receipt may be sent by the merchant to the consumer.

7.2.2 Mobile remote credit transfer

The following use cases are based on a credit transfer as the underlying payment instrument whereby funds are transmitted from the consumer's (payer's) account to the account of the merchant (payee). Mobile remote credit transfers (MRCTs) will use the same rules that are applied in current credit transfers via other channels (e.g. maximum processing time, account formats, etc.). The consumer and the merchant may be, and frequently are, customers of different MFSPs. Generally speaking, in the case of a credit transfer for a consumer to merchant payment, two categories may be considered:

— a first family whereby the merchant (business) requests the payment and the consumer is subsequently requested to confirm the payment according to the current credit transfer payment processes using their mobile device;

— a second family whereby the consumer initiates the payment to a merchant (business) using their mobile device (e.g. the payment of an invoice, possibly by scanning for instance a QR code).

For a payment to a business transaction, the "confirmation of credit transfer request acceptance" is important for the merchant to have a sufficient degree of assurance about the execution of the payment before delivering its goods or services.

In this clause, the following use cases are illustrated:

— a consumer to merchant MRCT whereby the consumer initiates the transaction for the payment of an invoice (see 7.2.2.1);

— a consumer to merchant MRCT whereby the merchant initiates the transaction and the consumer is redirected to their MFSP for the authentication (see 7.2.2.2);

— a consumer to merchant MRCT whereby the merchant initiates the transaction and the consumer is redirected to a TPP for the authentication (see 7.2.2.3).

The use cases remain also valid for business-to-business payments, in particular when the payer is a small business.

7.2.2.1 MRCT — Consumer payment of invoice to merchant

In this use case, illustrated in Figure 12, a consumer uses a mobile device to pay an invoice using an MRCT from his/her own payment account to the payment account of a merchant (payee). In these situations, a dedicated MRCT application on the mobile device is used.

Furthermore, a merchant QR code, including the name, an account identifier (e.g. routing number, IBAN) of the merchant and the transaction amount may be provided on the invoice, making the input of the merchant details considerably more convenient for the consumer.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved

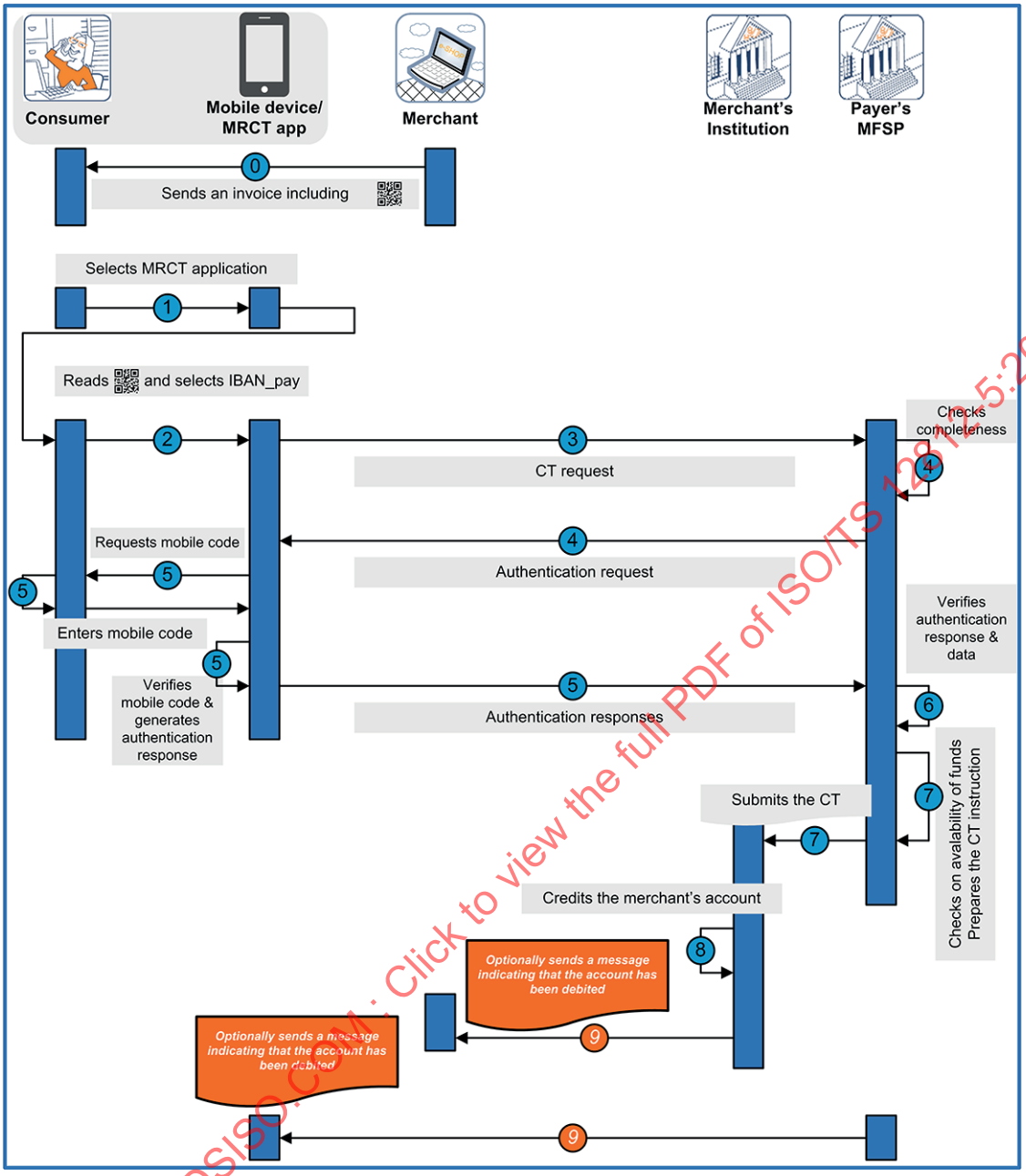


Figure 14 — Mobile remote credit transfer

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

In Figure 14, the following steps are illustrated:

Step 0 (Pre-requisite)

— The merchant sends an invoice to the consumer containing a QR code, which includes the merchant name, the transaction amount and the account identifier.

Step 1 (Payment application selection)

— The consumer selects and opens the MRCT application on his/her mobile device which possibly involves the entry of a mobile code. Subsequently, the consumer scans the QR code from the merchant invoice using his/her mobile device.

© ISO 2017 – All rights reserved

Step 2 (Transaction details entry)

— Once the MRCT application is selected, the consumer selects the account identifier he/she wants to use in case there are several eligible payment accounts, while the transaction amount and the merchant's account identifier is automatically retrieved from the QR code.

Step 3 (Credit transfer request)

— The credit transfer request is provided to the consumer's MFSP.

Step 4 (Authentication request)

— The consumer's MFSP checks the completeness of the transaction related data entries and sends an authentication request (possibly including a challenge) to the MRCT application in the mobile device of the consumer.

Step 5 (Authentication response)

— The authentication request is handled automatically by the MRCT application in the consumer's mobile device. The consumer is typically requested to enter his/her mobile code once during the transaction (see 4.2.7). If the mobile code verification is successfully performed by the MRCT application, it calculates an authentication response which is provided to the consumer's MFSP.

Step 6 (Authentication verification)

— The consumer's MFSP verifies the authentication response and the data received.

Step 7 (Payment process)

— The consumer's MFSP checks on the availability of funds on the consumer's account, prepares and submits the credit transfer instruction to the merchant's institution.

Step 8 (Transaction finalization)

— The merchant's Institution credits the merchant's account with the transaction amount.

Step 9 (Transaction information)

The merchant optionally receives a message from its institution that its account has been credited. The consumer optionally receives a message from his/her MFSP informing that the selected account has been debited. If such notification procedures are used, the following requirements shall be followed.

— A "Confirmation of Payment" service is established.

— The consumer's MFSP and the merchant's MFSP shall participate in the "Confirmation of Payment" service.

— The merchant has registered with a notification service with its MFSP.

— The consumer shall have the capability to instruct his/her MRSP to make the "Confirmation of Payment" service available.

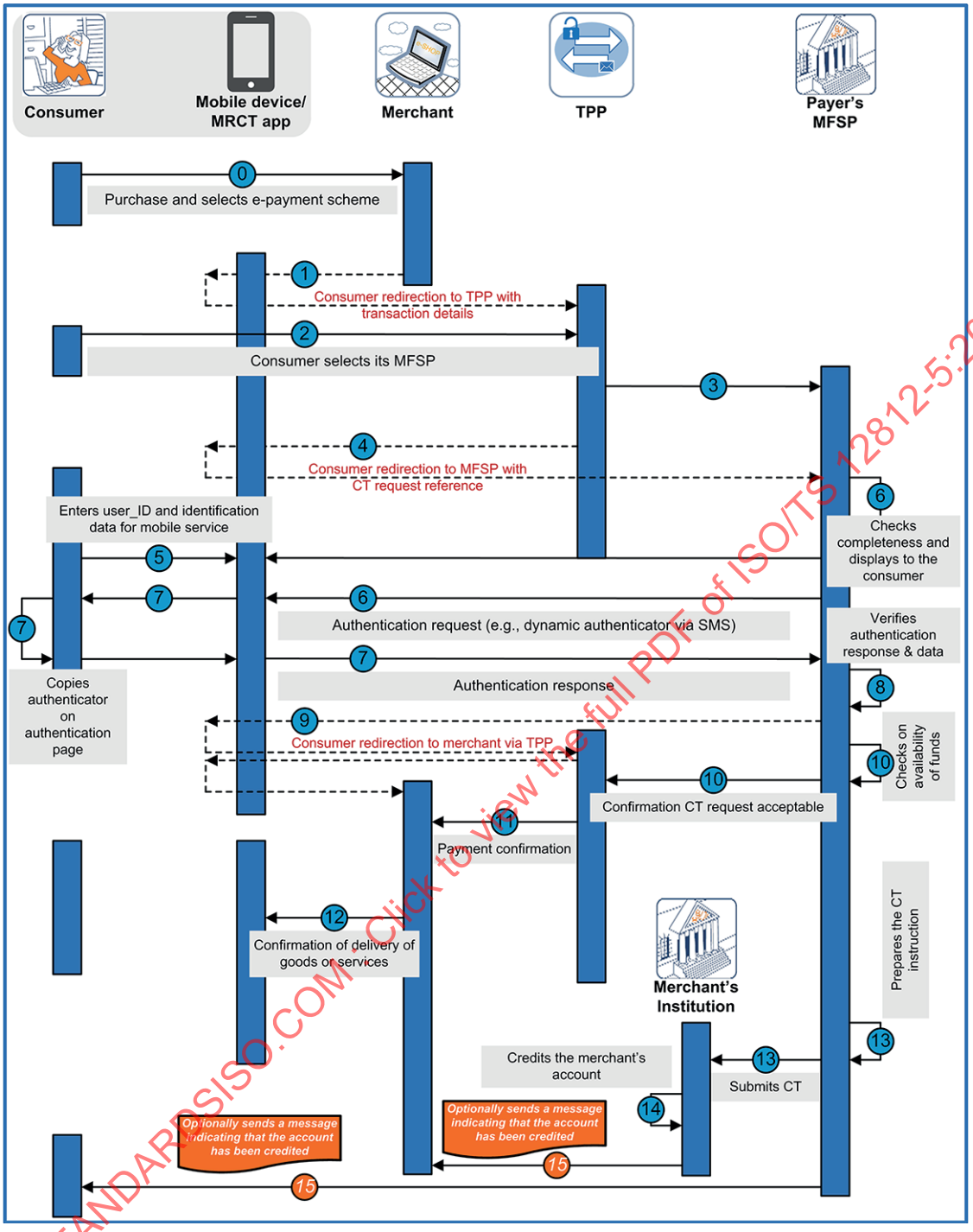
7.2.2.2 MRCT — Consumer to merchant transaction with consumer redirection to his/her MFSP for authentication

In this use case, illustrated in Figure 15, the consumer uses their mobile device to pay for goods or services delivered by a merchant (payee). An MRCT is used from the consumer's payment account to the payment account of the merchant using a mobile browser.

Furthermore, the consumer is redirected from the merchant's website to its MFSP's mobile service (e.g. a mobile banking system) where an authentication is performed.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

Figure 15 — Consumer to merchant transaction with consumer redirection to his/her MFSP for authentication

In Figure 15, the following steps are illustrated:

Step 0 (Pre-requisite)

— The consumer navigates using the browser of his/her mobile device to a merchant's website and selects the goods or services he/she wants to buy. After having accepted the general purchase conditions, he/she is requested to confirm the purchase.

© ISO 2017 – All rights reserved

— The checkout section of the merchant website displays the transaction details, including the amount and the payment options to the customer. The customer selects his/her preferred TPP in this checkout section.

Step 1 (Customer redirection to e-Payment Scheme)

— The customer is redirected with the transactions detail, including the beneficiary's name, transaction amount and account identifier to the e-commerce program/scheme/TPP portal.

Step 2 (Consumer selection of MFSP)

— The consumer is invited to enter his/her preferred MFSP on this portal for this transaction.

Step 3 (Credit transfer request)

— A credit transfer request including the transaction amount, the merchant's name and account identifier are forwarded to the consumer's MFSP.

Step 4 (Consumer redirection to their MFSP)

— The consumer is redirected with the credit transfer request reference by the e-payment program/scheme portal to the mobile service of his/her MFSP.

Step 5 (Consumer identification)

— The consumer is requested to enter his/her user ID and identification data in accordance with the security policy of his/her MFSP. After successful identification, the credit transfer reference with the transaction details, including the transaction amount and merchant information, are displayed to the consumer.

Step 6 (Authentication request)

— The consumer's MFSP sends an authentication request, possibly including a dynamic authenticator (e.g. using a one-per-transaction number) to the consumer (e.g. via SMS).

Step 7 (Authentication response)

— The consumer is subsequently requested to enter the authentication response (e.g. copy the dynamic authenticator) into a dedicated authentication page to authorize the credit transfer request which is provided to his/her MFSP.

Step 8 (Authentication verification)

— The consumer's MFSP verifies the authentication response and the data received.

Step 9 (Customer redirection to merchant)

— The consumer is redirected based on previously received referral information by his/her MFSP via the e-commerce program/scheme or the TPP portal to the merchant.

Step 10 (Credit transfer acceptance)

— The consumer's MFSP checks the availability of funds in the consumer's account and sends a confirmation of credit transfer acceptance to the e-payment scheme/TPP portal.

Step 11 (Payment confirmation to e-merchant)

— The merchant is informed by the e-commerce program/scheme or the TPP about the payment confirmation possibly by a forward of the MFSP's confirmation of credit transfer acceptance which enables the release of the goods or services to the consumer.

Step 12 (Delivery of goods or services)

— The consumer receives confirmation from the merchant on the delivery of goods or services.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 12812-5:2017

© ISO 2017 – All rights reserved