TECHNICAL SPECIFICATION

ISO/TS 12812-4

First edition
2017-03

Core banking — Mobile financial services —

Part 4: Mobile payments-to-persons

Opérations bancaires de base — Services financiers mobiles —

Partie 4: Paiements mobiles à personnes

Reference number
ISO/TS 12812-4:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

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

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

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

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

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

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

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

Introduction

The ISO 12812 series is a multi-part standard addressing interoperable and secure systems for the provision, operation and management of Mobile Financial Services (MFSs).

This document addresses how a payer interacts with a person to initiate and complete a mobile payment. A "person" can be either a natural individual or a small business entity legally recognized as a "person" but where the payment is casual in nature (e.g. where the purpose is to transfer funds between people who know each other, such as family members, friends or neighbours, or where the relationship between two people is casual, such as to pay the babysitter, nanny, handyman, etc.).

Payment instruments used for mobile payments-to-persons are rendered by appropriate MFS applications that are available in or accessed through a mobile device. This mobile device, using an appropriate secure environment, stores or provides access to sensitive data. Such sensitive data include application configuration information, personal account data and user authentication data (authentication credentials), including cryptographic keys.

This document includes a set of requirements and some recommendations intended to facilitate the interoperability of mobile payments-to-persons. This document also outlines the need for consumer protection mechanisms (e.g. including fair contract terms, rules on transparency of charges, clarification of liability, complaints mechanisms and dispute resolution).

The objective of this document is to provide MFSPs with technical provisions to enable the development of interoperable mobile payments-to-persons services, where either the payer or the payee uses a mobile device to transact a payment to a person.

Mobile payments-to-persons may require the payer to input a unique identifier of the payee. The payee of a mobile payments-to-persons transaction (e.g. family member, friend) should be able to verify the received amount and the reason for the payment. Although the standard focuses on mobile payments-to-persons resulting in account-to-account payments, mobile payments-to-persons systems have also been deployed in scenarios where payer and/or payee are unbanked. From a wider perspective, then mobile payments-to-persons and especially remittances may facilitate later financial inclusion (see Annex A).

This document differentiates between proximate mobile payments-to-persons and remote mobile payments-to-persons:

— Proximate mobile payments-to-persons refers to a payment conveyed from one mobile device to another mobile device, where the payer and the payee are physically present in the same location. In this document, such mobile devices are assumed to enable a contactless or other communication channel to be established. One example is the Near Field Communication Interface (see ISO 18092), present on an NFC-enabled Mobile Device. NFC technology in the mode called peer-to-peer establishes such a contactless channel between the two communicating devices. This document does not preclude the use of other proximity technologies like (e.g. bluetooth low energy, QR codes).

— Remote mobile payments-to-persons refers to payments in which both the payer and the payee may be not physically present at the same location, meaning that the mobile device establishes a communication channel using a wireless network.

Regarding the implementation of mobile payments-to-persons, the following factors should be considered:

— Technology innovation is dynamic, especially for mobile devices and their operating systems, mobile wallets and payment infrastructures. Thus, requirements should be flexible to handle current and future technologies.

— Regulatory and policy issues should be addressed for the operation of payment systems by ensuring conformance with national and multi-national legislation and regulation, (e.g. Know Your Customer (KYC), Anti-Money Laundering (AML), the U.S. Office of Foreign Assets Control (OFAC) and Combating the Financing of Terrorism (CFT), data protection/privacy and customer protection).

— Global utilization of mobile payments-to-persons in the two following areas:

a) The deployment of mobile devices in developing countries that are often challenged by geographical boundaries, a lack of a centralized banking infrastructure, and a need for the provision of MFS to under-banked and/or unbanked individuals.

b) Social networks are used by millions or even billions of people in systems relying on interpersonal services (e.g. music, games, relationships). Many of these services generate direct payments-to-persons relationships which may involve the use of mobile payments-to-persons.

Mobile payments-to-persons constitute one type of MFS. The contents of this document are closely related with other parts of the standard. Potential implementers of mobile retail payment solutions should look at part 5. Both parts 4 and 5 of ISO 12812 seek to support all possible technologies and are not intended to favour any specific technology. Therefore, individual implementations of a mobile payments-to-persons service may be highly dependent upon or require the application of other parts of the ISO 12812 standard. In particular:

— ISO 12812-1 describes the general framework and definitions for the standard;

— ISO 12812-2 specifies requirements and recommendations for security and data protection;

— ISO 12812-3 specifies requirements and recommendations for the management of mobile financial applications.

Figures 1 to 6 or part thereof are courtesy of the European Payments Council.

Core banking — Mobile financial services —

Part 4: Mobile payments-to-persons

1 Scope

This document provides comprehensive requirements and recommendations, as well as specific use cases for implementation of interoperable mobile payments-to-persons.

The emphasis is placed on the principles governing the operational functioning of mobile payments-to-persons systems and processes, as well as the presentation of the underlying technical, organizational, business, legal and policy issues, leveraging legacy infrastructures of existing payment instruments (see ISO 12812-1:2017, Annex C).

This document includes the following items:

a) requirements applicable to mobile payments-to-persons;

b) recommendations regarding mechanisms involved in the operation of interoperable mobile payments-to-persons;

c) a description of the different use cases for mobile payments-to-persons;

d) a generic interoperability model for the provision of different mobile payments-to-persons;

e) recommendations for the technical implementation of the generic architectures for the mobile payments-to-persons program;

f) recommendations for mobile remittances;

g) use cases with the corresponding transaction flows;

h) discussion of the financial inclusion of unbanked and underbanked persons (Annex A);

i) some legal aspects to consider for mobile payments-to-persons (Annex B).

The document is structured as follows:

— Clause 6 sets forth the requirements that a mobile payments-to-persons program must comply with.

— Clauses 7, 8 and 9 provide the different levels of implementation for the interoperability of mobile payments-to-persons.

— Clause 7 describes the interoperability principles for mobiles payments-to-persons.

— Clause 8 describes:

  1) a three-layer high-level architecture for mobile payments-to-persons programs;

  2) payments instruments sustained by these programs;

  3) processing details for a series of significant use cases of mobile payments-to-persons using these payment instruments.

— Clause 9 provides a step-by-step data flow description for different mobile payments-to-persons implementations: bank-centric, non-bank centric and card-centric. They can be mapped into the

processing use cases of Clause 8, where abstraction is made in the nature of the payment service providers.

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 12812–2:2017, *Core banking — Mobile financial services — Part 2: Security and data protection for mobile financial services*

ISO 12812–5, *Core banking —Mobile financial services — Part 5: Mobile payments to businesses*

3 Terms and definitions

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

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

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

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

3.1
agent
entity that transfers funds to an MFSP on behalf of the payer or disburses funds from an MFSP to the payee

Note 1 to entry: The definition applies especially to remittance and covers both three- and four-corner systems.

3.2
mobile payments to person
mobile payment where the payee is a person

3.3
mobile remittance
transfer of money through mobile device between two persons located or not in the same country

3.4
mobile remittance service provider
entity that provides a mobile remittance service

3.5
mobile payments-to-persons program
operational network, governed by laws, rules and technical specifications, standards, providing mobile payments-to-persons services

3.6
payee identifier
information enabling a MFSP to identify the beneficiary of a mobile payments-to-person

3.7
unbanked
individual who does not have access to a bank account or who has no contract with a financial institution for banking services

4 Abbreviated terms

ACH	Automatic Clearing House
AML	Anti-Money Laundering
BIC	Business Identifier Code
CFT	Combating the Financing of Terrorism
CI	Consumers International
CSM	Clearing and Settlement Mechanism
IBAN	International Bank Account Number
KYC	Know Your Customer
MFS	Mobile Financial Service
MFSP	Mobile Financial Service Provider
MNO	Mobile Network Operator

5 Specific characteristics for mobile payments-to-persons

5.1 General

The content in this clause is generic in nature and can be applied across a wide variety of mobile payments-to-persons. The objective is to contribute to a common understanding on how the various mobile payments-to-persons programs work.

Together, the different sections of this clause propose a flexible framework for mobile payments-to-persons programs which includes:

— functional and technical commonalities between different mobile payments-to-persons as classified in Clauses 8 and 9;

— functional architectures suitable to mobile payments-to-persons;

— provisions to cover regional requirements and/or constraints, in particular, those of a legal or regulatory nature.

5.2 Mobile payments-to-persons concepts

Depending upon the nature of the mobile payments-to-persons system, the transfer may involve any combination of:

— a deposit account or a credit account associated with the payer and/or the payee;

— an agent accepting from the payer or disbursing to the payee funds through a variety of methods, including cash;

— electronic money held by the payer or payee, either resident in a server or stored in a mobile device using an appropriate secure environment (see ISO 12812-2).

5.3 User expectations

The next list (not exhaustive) precises some expectations of users (payers and payees) of mobile payments-to-persons systems:

a) payee availability of funds at all times;

b) easy to use service;

c) quick transfer and confirmation;

d) increasingly seek transferability of funds with persons enrolled by different MFSPs;

e) resistance against attacks (theft, skimming, etc.);

f) transparency of charges;

g) clarification of liability;

h) availability of complaint and dispute resolution mechanisms.

5.4 Stakeholders involved in a mobile payments-to-persons program

5.4.1 Mobile financial service provider

The MFSP contracts the customer for a mobile payments-to-persons service provided in the framework of an MFS program. An MFSP directly operates the mobile payments-to-persons service or may subcontract some elements of the program to a third party.

A primary role of the MFSP is the issuance of mobile payments-to-persons applications to be used during the transaction. The MFSP also implement risk prevention and technical controls that ensure the security of the transaction in conformance with the rules of the MFS program. In particular, the MFSP controls the access to mobile payments-to-persons services to their enrolled customers using authentication mechanisms.

An open MFS program involves at least one business agreement between two or more different MFSPs in order to offer customers services according to mutually contracted governance rules (see ISO 12812-1:2017, B.3).

NOTE In this document, the acronym MFSP refers to a “payments-to-persons MFSP”.

5.4.2 Mobile network operator

The MNO operates the wireless network that may be required to proceed to a mobile payments-to-person transaction. The MNO provides access to the network after authenticating the user. The MNO may also act as the distribution channel for the mobile device and associated authentication means.

5.4.3 Agent

The agent is the entity entitled by contract with an MFSP to disburse cash to the payee (cash-out) or to accept cash (cash-in) from a payer to proceed to a mobile payments-to-person to a designated payee. An agent may be a regulated entity.

5.4.4 Electronic money service provider

The electronic money service provider is an entity (that may be regulated based on national laws or regulations) that is authorized to issue and exchange electronic money between their customers.

6 Requirements for mobile payments-to-persons

6.1 General

This clause identifies a set of requirements that are common to both proximate and remote mobile payments-to-persons.

These requirements are similar to those covering the payments to a business environment. Where in particular receipt delivery is needed, printed or in electronic form, the requirements of ISO 12812-5 apply.

A mobile payments-to-person transaction involves typically an initial connection between the mobile device of the payer and an MFSP after the selection of an application by the payer. Upon the payer authentication and the retrieval of payee's routing information, the MFSP of the payer establishes a second connection with the MFSP of the payee to instruct the payment.

The requirements set out in this clause shall apply to:

— the implementation of the mobile payments-to-persons application;

— the protocols executed between the MFSPs involved in the transaction, as well as to the protocols between the payer/payee and their MFSP. In particular, these protocols shall convey data needed to conform to 6.3, 6.4 and 6.5.

NOTE Security and data protection requirements are addressed in ISO 12812-2.

6.2 Device, network, and application selection requirements

6.2.1 General

These requirements are intended to ensure that a customer has the freedom to choose under certain conditions the mobile device and MNO for access to MFSs that will be used.

6.2.2 Requirements

6.2.2.1 An MFSP shall permit customers (e.g. payer or payee) to select the mobile device they desire for the access to the mobile payments-to-persons service, provided that the mobile device supports a secure environment compatible with the MFSP requirements and is consistent with ISO 12812-2.

6.2.2.2 An MFSP shall facilitate the selection of the MNO which the customer desires to handle mobile communications services, provided that the MNO supports a secure environment compatible with the MFSP requirements.

6.2.2.3 A mobile device shall permit a customer to:

— select the appropriate mobile payments-to-persons application(s) including a mobile wallet, for handling any particular mobile payments-to-persons transaction;

— permit a customer to disable an MFS application (see ISO 12812-3:2017, 7.1).

6.2.2.4 An MFSP shall ensure that when a mobile wallet is used for mobile payments-to-persons, it is capable of providing, at least, the following functionality:

— a trusted user interface to:

a) manage (register, update, delete) data that may be used for the service;

b) allow the user to select and use the payments-to-persons service (can be one interface managing all payment means or different interfaces for different means);

— a data repository (on the mobile device or a secure remote server).

6.3 Logging requirements

6.3.1 General

These requirements are intended to facilitate the traceability of transactions and enable the customer to verify that these transactions have been performed correctly.

6.3.2 Requirements

6.3.2.1 An MFSP shall provide the means for a customer to view details of each mobile payment transaction. The transaction log shall, at a minimum, display the last 10 transactions handled by a mobile payments-to-persons application, or the recent transactions completed over the past 30-day period, whichever provides the most information. Beyond the immediate logging information, the MFSP shall arrange to provide additional information to a customer upon request under reasonable terms.

6.3.2.2 The transaction log shall make available the following data:

— transaction identifier;

— transaction date;

— transaction time;

— transaction amount(s);

— transaction currency code(s);

— transaction type (e.g. debit, credit);

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

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

NOTE A parallel requirement to provide a transaction log to a payee may not be practical because the payee can be a customer of a different MFSP.

6.4 Notice requirements

6.4.1 General

These requirements are intended to:

— reduce the risks and consequences of unauthorised or incorrectly executed payment transactions so that the payer and the payee may inform their MFSPs as soon as possible about any contestations concerning allegedly unauthorised or incorrectly executed payment transactions, and

— accelerate the availability of the funds by the payee.

6.4.2 Requirements

6.4.2.1 The payer MFSP shall notify a payer that a payment has been authorized, approved, or completed.

6.4.2.2 The payee MFSP shall notify the payee about the status of a payment (e.g. that a payment has been received into the payee's account).

6.4.2.3 The payee MFSP shall notify the payee about the ability to access the funds that were transferred into the payee's account.

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

6.5 Authentication and authorization requirements

6.5.1 General

These requirements are intended to reduce risks and consequences of unauthenticated or unauthorized payment transactions using preventive measures to authenticate and authorize the payer and the payee.

6.5.2 Requirements

6.5.2.1 The payer MFSP shall authenticate the payer to verify the identity of the payer and his/her mobile device and shall authorize the transaction after validating the availability of funds and according to its internal risk management procedures. For authentication and authorization methods, see ISO 12812-2. For payment-to-person transaction authentication, authorization and acceptance discussion and use cases, see 9.2, 9.3 and 9.4.

6.5.2.2 The payee MFSP shall authenticate the payee to verify the identity of the payee and his/her mobile device and shall authorize the transaction according to its internal risk management procedures. For authentication and authorization methods, see ISO 12812-2. For payment to person transaction authentication, authorization and acceptance discussion and use cases, see 9.2, 9.3 and 9.4.

7 Scenarios for interoperability

7.1 General

Interoperability of a mobile payments-to-persons program refers to the ability of a payer enrolled with an MFSP to execute a mobile payments-to-person transaction with a payee who is not necessary enrolled with the payer MFSP. Both MFSPs must have access to a mobile payments-to-persons system.

This document describes two interoperability scenarios:

— Scenario 1, where the transaction is processed within a single mobile payments-to-persons system;

— Scenario 2, where the transaction is processed through different mobile payments-to-persons systems and interoperability models for payment facilitation.

Implementers interested in specific examples of how interoperability between MFSP has been handled in SEPA/EPC situations may refer to documentation in EPC 492.09 version.

NOTE The figures in Clauses 7 and 8 are inspired from the EPC document.

7.2 Scenario for interoperability 1

7.2.1 General

In scenario 1, MFSP(s) are members of the same mobile payments-to-person system. This scenario covers two models described in 7.2.2 and 7.2.3.

In both models, the MFSP(s) participating in the transaction:

— implement common protocols to connect to the payment system for the execution of payments using a given payment instrument;

— have access to a common clearing and settlement facility;

— enrol their customers for a mobile payments-to-persons service;

— provide their customers with a mechanism (e.g. a mobile payments-to-persons application, a mobile wallet) to transmit payment orders through wireless communication networks.

7.2.2 Three-corner model

In a three-corner model, both the payer and the payee are customers of the same MFSP. The three-corner model is also called closed-loop or MFSP centric (see ISO 12812-1:2017, Annex B).

The fact that only one MFSP is involved may result in a simplified implementation of the use cases, such as the identification of the payee (which is known to the MFSP), the payment confirmation and the immediacy of the funds availability by the payee.

7.2.3 Four-corner model

In this model, the payer and the payee are customers of the different MFSPs. The four-corner model is also called open-loop or inter-MFSP collaborative (see ISO 12812-1:2017, Annex B).

In this model, MFSPs have implemented common protocols and access to shared system infrastructures for payment initiation, processing and settlement.

7.3 Scenario for interoperability 2 (cross-system payment)

Scenario 2 refers to interconnectivity options to enable a payer enrolled by an MFSP member of a system A to transfer funds to a payee enrolled with an MFSP of a different system B. The business rationale for scenario 2 is the need for a MFSP to boost the volume of transactions and to extend the mobile payments-to-persons service to a larger number of payees.

Possible solutions include:

— Bilateral or multilateral agreements between systems.

— The creation of a common infrastructure (e.g. a hub) to support cross-system payments-to-persons payments and develop a common directory shared between systems and similar in functionality to the one designed in 7.4. This cross-system directory may be implemented as the federation of existing common directories and be accessible using a common protocol.

— The hub may offer different levels of service, depending in the investment effort decided. For instance, the hub may:

a) provide a service for protocol conversion, or

b) require the implementation of a specific protocol to be supported for the PSPs, or

c) provide APIs for the service to be offered (e.g. access to a Common Directory).

NOTE Future versions of the standard can provide technical solutions for cross-system interoperability.

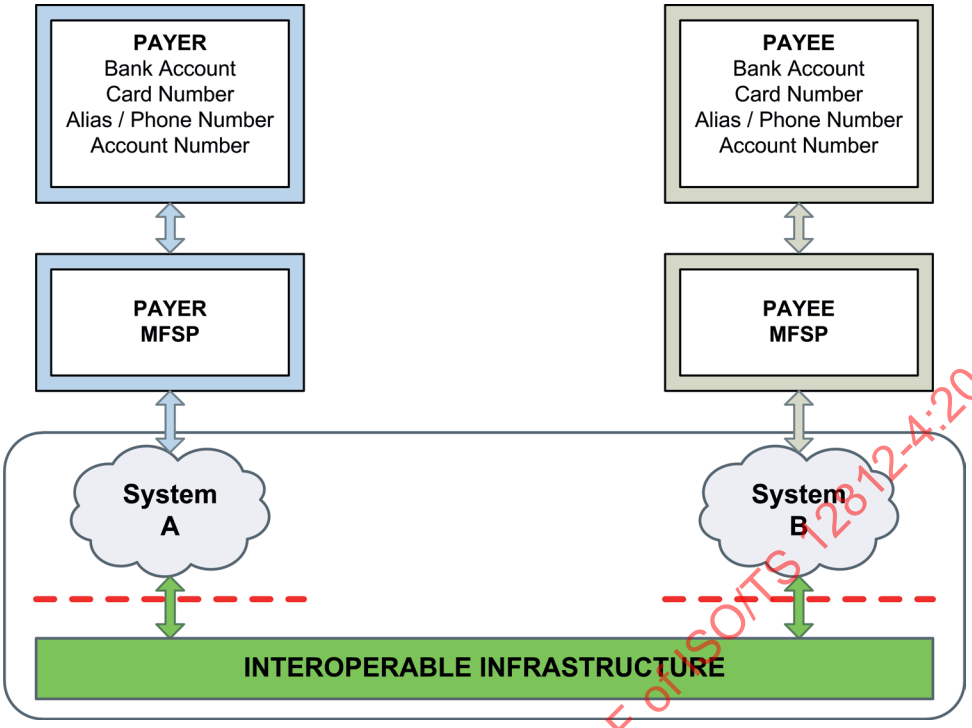

Figure 1 — Interoperability model for scenario 2

Figure 1 describes the interfaces required for the transmission of the payment instructions between the different stakeholders. For scenario 2, the routing of the payment instruction requires that both systems implement an interface for access of the respective system's MFSP to a common infrastructure.

7.4 Interoperability models for payment facilitation

7.4.1 General

A first concern for the mobile payments-to-persons program is to facilitate the initiation of the payment using an identifier (e.g. alias) of the payee easy to handle by the payer, but sufficient to retrieve the payee routing information.

This document proposes two interoperability models for the facilitation of payments to persons:

— The direct interoperability model, where the payer provides to his/her MFSP the information needed to route the payment instruction to the payee MFSP. It is based on the use of existing infrastructure and delivers direct interoperability between payers and payees, as described in 7.4.2.

— The common infrastructure model, which involves the implementation of a common infrastructure (CI) to which each MFSP participating in a system has access to. The payer MFSP sends a request to the CI using the payee identifier provided by the payee (e.g. an alias) and receives as a response the appropriate routing information for the payment transaction (e.g. to the payee's payment account through IBAN/BIC for credit transfers/ACH transactions). This model is described in 7.4.3.

NOTE Multiple versions of the common infrastructure model exist.

7.4.2 Direct interoperability model

The direct interoperability model is dependent on the payer's/payee's ability to forward all relevant payment information (BIC, IBAN, PAN, name, address, etc.) to his/her MFSP. The information for the payment transaction is directly provided by the payer to its MFSP. Implementing the direct

interoperability model in a mobile payments-to-persons system means that the payer MFSP does not need to collect additional information in order to generate the payment instruction.

In this way, the mobile payments-to-persons transaction may be performed in four steps:

— payment initiation by the payer including payee information;

— generation of the payment instruction by the payer MFSP;

— debit of the payer account and credit of the payee account;

— notification to the payee of the funds availability.

7.4.3 Common infrastructure

In this model, interoperability is achieved by the usage of a centralized common infrastructure which may have many shapes and purposes and which could even be implemented in a distributed way. The primary purpose of this infrastructure is to act as a directory service or switch for routing purposes as described in Figure 2. This centralized infrastructure could also offer various value added services such as delivery services which are, however, beyond the scope of the ISO 12812 standard.

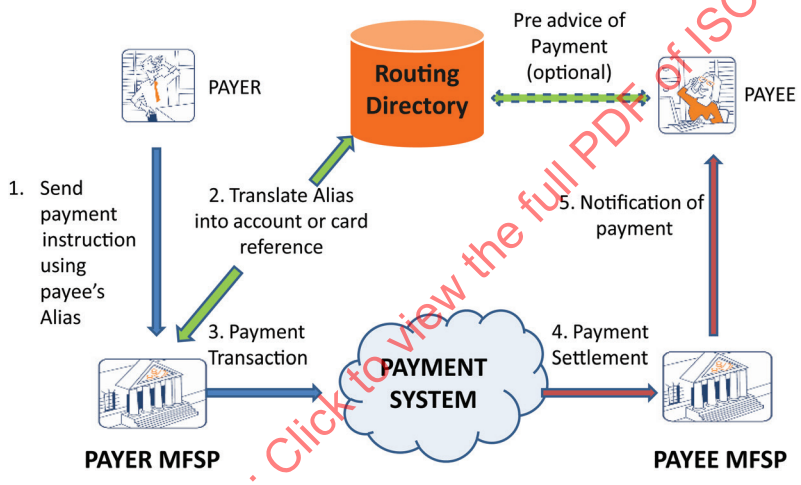

Figure 2 — Common infrastructure model

Figure 2 adds an additional step prior to the generation by the payer's MFSP of the payment instruction. The information for the payment transaction is to be retrieved by the payer's MFSP from a central data server based on the payee's alias provided by the payer to its MFSP.

The common interoperability model presents two advantages compared with the direct interoperability model:

— it avoids the inconvenience to payers of having to obtain the payee's account information;

— it avoids the payee to disclose his/her own account information to the payer.

The model relies on the enrolled users trusting the CI directory. In particular, the CI directory management shall comply with the data protection requirements set out in ISO 12812-2:2017, 6.3.

8 Implementation models

8.1 General

A mobile payments-to-persons program' refers to a formal arrangement between MFSPs either members or having access to payment systems on common governance rules for the processing, clearing and/or settlement of mobile payments-to-persons.

A great number of mobile payment programs exist in the marketplace having in common the use of the mobile device to initiate a payment from payer to payee, regardless of whether the payer and the payee are present in the same location or not.

This diversity of models for the provision of mobile payments-to-persons may be considered as the result of three different market trends:

— the emergence of new technologies enhancing the ability of the individuals to communicate;

— the need to provide methods to enable better control by users of their account balances (bank and non-bank accounts);

— the openness of the mobile payment market to new stakeholders.

In a consistent way with the other parts of this document, this clause uses the term MFSP for the entity directly in relationship with either the payer or the payee. However, in the real world, the information exchanges between the entities participating in a mobile payments-to-persons program will actually depend on the nature of the MFSPs involved (e.g. if the MFSP is a financial institution or not). Therefore, when required by a specific mobile payments-to-persons scenario, the nature of the MFSP is to be specified.

This document proposes a high-level architecture for the provision of mobile payments-to-persons using three functional layers.

8.2 High-level architecture and network technologies

8.2.1 Layer 1: Infrastructure used to convey payment initiation and authorization messages

Layer 1 refers to the transport level networks required for the users of the mobile payments-to-persons system, the payers and the payees, to agree, initiate and confirm the payment using mobile devices. For example, users of the 3G+ or 4G mobile networks have access to connectivity functionalities characterized by:

— a relatively fast establishment of data connection;

— relatively higher data speeds, dependent on the technical implementation, available QoS and the availability of the network service (or a fall-back access);

— capability of being constantly connected, without the need to re-establish the connection;

— capability to use voice and data connections simultaneously;

— fast speed and safe download for mobile payments-to-persons applications and services.

Depending on the mobile device technology and the payer's contractual relationship with the MFSP, layer 1 may be implemented over different wireless carriers.

Regardless of the carrier communication technology used (e.g. wireless, Internet), the messaging between the various parties to a remote payment transaction is crucial. The payee should also be notified to know that he/she has access to the transferred funds. Requirements regarding notice are set out in 6.4.

8.2.2 Layer 2: Common infrastructure used for payment facilitation

The payment facilitation component is intended to:

— identify the payment instruments used by the two parties. Various models are available. The two parties may voluntarily disclose payment instrument details (e.g. account references) to each other; they may rely on some form of linkage (through a shared common infrastructure) between mobile identifiers and payment instruments belonging to the MFSPs handling the transaction;

— establish unambiguously the identifiers required for the routing of the mobile payments-to-persons transaction to the payee designated by the payer;

— establish the corresponding payment instruction order by the payer's MFSP.

8.2.3 Layer 3: Value transfers and funds movement

The actual transfer of value or movement of funds will take place using existing payment instruments.

Both the payer and the payee MFSPs are assumed to have access to clearing and settlement facilities (CSM) of a payment system, either directly or indirectly (through a bank having direct access to CSM). CSMs support functionalities such as:

— receiving transactions for clearing from the payer MFSP, either directly or indirectly;

— clearing and forwarding them to the payee MFSP ensuring that all transaction data transmitted by the payer MFSP are transmitted in full and without alteration;

— exception handling (e.g. returns, rejects and recalls);

— making arrangements such that settlement can be achieved between the MFSPs;

— providing any required risk management procedures and other related services.

NOTE The term CSM does not necessarily connote one entity (e.g. it is possible that the clearing function and the settlement functions are performed by separate entities).

8.3 Classification of mobile payments-to-persons

8.3.1 General

The principles governing this classification are the following:

— The classification of mobile payments-to-persons is not exhaustive;

— Mobile payments-to-persons in this document rely on the use of three existing payment instruments: credit transfers, cards and electronic money. Therefore existing payment systems can be used for the processing of mobile payments-to-persons;

— The exact transaction flows for these payment instruments may vary in different world regions, but they share a common set of messages to provide the core functionalities;

— Mobile payments-to-persons can be made in either proximate (physical proximity between the payer and the payee using, e.g. mobile devices with a contactless interface type NFC) or remote modes;

— A given MFSP may offer several mobile payments-to-persons services which may differ, amongst other factors, in terms of (1) settlement immediacy, (2) control by the payer of the debit on his/her account, (3) the fact that the funds to be transferred are in some time in possession of the MFSP or not and (4) in the security policy;

— The mobile remittance case has been addressed as a separate subclause (8.4) because of their specificities in terms of payment processing. Remittances are often intermediated by specific agents not found in other categories of mobile payments-to-persons.

8.3.2 Mobile credit transfer payment

The payer uses his/her mobile device to initiate a credit transfer to the payee account. This mode is also known as a "push" process. Once the credit transfer is authorized, the payer account is instantly debited and the payee account is credited and therefore given access to the funds transferred. These accounts may be a bank account or a payment account held by an MFSP, which is not necessary a financial institution. The funds transfer between the bank accounts of the MFSPs are usually settled later.

8.3.3 Mobile card payment

The customer uses his/her mobile device to initiate a card payment to another person's card account and the transaction is transmitted over a card network. The specific processing modalities may depend on the type of card (debit, credit, prepaid) used to fund the payment. Depending on the business model involved, the payer is required to furnish the card details to make the payments or the payer's card details are registered with the MFSP upfront.

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

8.3.4 Electronic money transfer

The electronic money amount to be sent may be either:

— locally stored in the mobile device of the payer, or

— stored in a prepaid account held by the MFSP. The issuance and operation of electronic money may be operated by specific institutions that may be the object of specific regulatory provisions.

8.4 Mobile remittances

A specific scenario of mobile remote transfer, frequently cross-border and recurrent, is where the payer is often a migrant worker. Unlike domestic remittances, cross-border remittances usually involve a currency conversion that is executed by transferring either script or electronic money between the accounts of the payer and the payee. The conversion issue (e.g. devaluation and currency convertibility) means that specific risks are associated with these remittances.

The flow of funds from persons living in two different countries impact the MFS in both countries. The importance of remittances, and the difficulties that can be associated with them, have been increasingly recognized in recent years. Traditionally, remittance services have been provided by specific MFSPs making up a market independent of traditional payment networks; however, additional business models have been identified in recent years which involve the use of new financial instruments.

There are a number of reasons why mobile remittances have taken on a significant role, as well as provide important features in their use:

— The remittance payment market is global in scope;

— Remittances are large in aggregate volume;

— They are the largest single source of external financing in many developing countries;

— They are counter-cyclical, and lend themselves to a wide variety of uses. They are better targeted to the needs of some individuals than official aid or foreign direct investment;

— Individual business cases can provide services useful to the development of emerging economies;

— The market opportunity for MFSPs is increasing as the flows are shifting from informal to formal channels, and in the long-run, international migration, trade and investment flows also are likely to increase;

— Besides providing remittance services for unbanked or under banked persons on an international or domestic basis, MFSPs can also provide remittance services for casual transfers (e.g. payments among individuals who know each other or for casual services);

— Providing remittances may attract new customers for other services (e.g. deposit, loan and insurance products). At the same time, this process will encourage account-to-account transfers rather than cash-to-cash transfers. This process could encourage increased customer savings;

— There is a need for transparency in the advance disclosure of all charges to customers, whenever such charges occur in the chain, including variable exchange levels at both ends of the transaction. For additional information, see Annex A.

8.5 High-level description for significant use cases

8.5.1 General

This clause provides some general information on the transaction flow for some significant use cases for mobile payments-to-persons. While these use cases have been inspired from regional specifications (e.g. published by the European Payments Council), they are generic enough to be considered as representative of similar payment methods used in other world regions. This clause covers two types of payments instruments used for mobile payments-to-persons: cards and credit transfers. Implementers interested in a specific example of how these use cases have been implemented in EPC/SEPA situations may refer to documentation in EPC Document EPC 492.09 Version 4.0.

A more complete detailed description including requirements and recommendations is available in Clause 9.

8.5.2 Mobile payments-to-persons by card

Figure 3 illustrates an example of user experience for a mobile payments-to-persons initiated by a mobile device where a customer (payer) wants to make a personal payment to a second customer (payee) using his/her mobile device and a card.

In this use case, the primary difference between this mobile payments-to-persons and a regular card payment is that the transaction is initiated by the payer, rather than by the payee. The payment is processed over the card network(s) and charged to the payer's payment card account in accordance with the terms of the customer's arrangement with the card issuers. The payee will typically (but not necessarily) be identified by his/her payment card details and the proceeds of the payment will be applied to the relevant underlying payment account. Depending on card program rules, there may be scope to use an alias (e.g. mobile phone number) and there may also be alternative options to identify and pay a payee (e.g. payment account).

A prerequisite for this scenario is that the payer has subscribed to a (possibly, but not necessarily, mobile specific) payments-to-persons card system with his/her card issuer. Many of the major card programs already offer some proprietary mobile payments-to-persons services, but these would need to achieve open program interoperability for generalized acceptance.

In Figure 3, the following steps are illustrated:

a) The payer decides upon the amount to be paid.

b) The payer selects his/her card mobile payments-to-persons application.

c) Payment data retrieval:

   1) The payer enters the amount.

   2) The payer enters the unique identifier of the payee (i) manually or (ii) in proximate mode the identifier may be automatically retrieved using a contactless or other local interfaces or (iii) the identifier may be stored in the mobile device or in a wallet.

3) The payer confirms the card number to be used.

d) The payer resolves the payee's identification details based upon the unique payee identifier.

e) The payer sends the payment to the payee's MFSP.

f) The payee then applies the payment to the underlying payee's payment account (optionally with a notification).

Another variation or extension of this use case would feature the ability to send an 'urgent' or 'fast' payment and would support the following scenarios:

— The payee needs use of funds for an emergency.

— The payee needs certainty of receipt to proceed with an underlying transaction (e.g. a sale of goods or rendering of services between persons with no formal relationship).

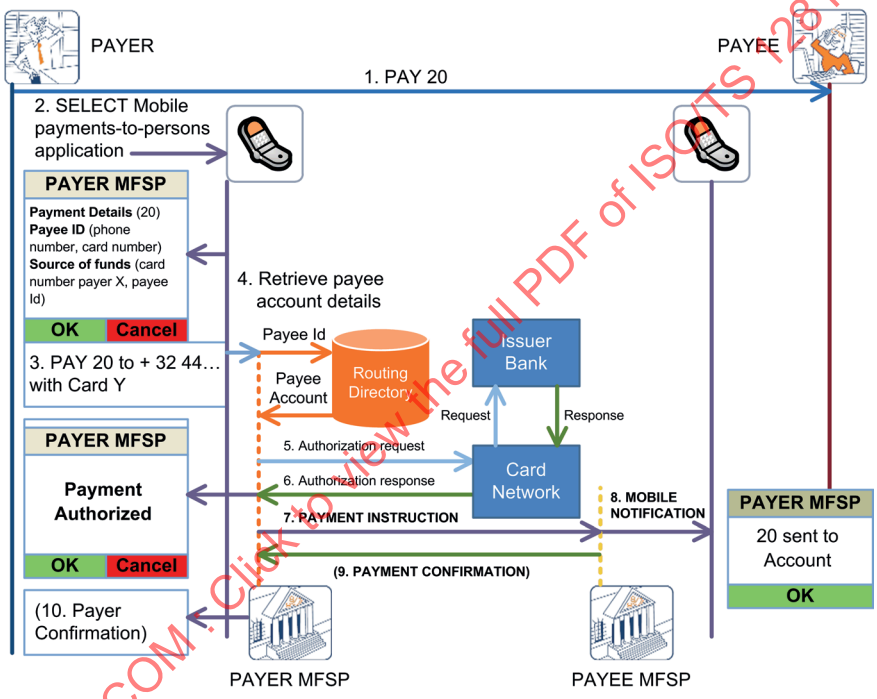

Figure 3 — (Urgent) card payment scenario

Table 1 — Mobile payments-to-persons by card

Payments to persons by card	
Category	Primarily payments-to-persons and some scenarios for payments to a casual business setting (e.g. small business or sole proprietary). Message flow according to Figure 3.
Communication type	Remote
Payment instrument	Payment card
Prerequisites	— Payee is identifiable with a unique identifier, generally, but not necessarily, a payment card. — The payee or the payee's MFSP has registered his/her identification account details in a common infrastructure (e.g. routing directory). — Payer has a payment card and is subscribed to a mobile payments-to-person card program by his/her MFSP (card issuer).

Table 1 *(continued)*

Payments to persons by card	
Payment initiator	Payer: steps 1 to 3
Payment facilitated by	Payer and Payee MFSPs: steps 4 to 5 and 7 to 10. Card Issuer: step 6. Optional payment confirmation determined by the payee MFSP to the payer MFSP: steps 9 to 10.
Payment settlement	See 9.5.

8.5.3 Payments-to-persons by credit transfer

8.5.3.1 General

Throughout this sub-clause, the term "credit transfer" refers to any such transaction (e.g. SEPA Credit Transfer, ACH). Three modalities for credit transfer, "core" (8.5.3.2), "urgent" (8.5.3.2) and "alias" (8.5.3.3), are differentiated. The mapping of these credit transfer modalities into detailed transaction flows resulting in the payee payment account settlement is described in Clause 9.

8.5.3.2 Credit transfer — Core

Figure 4 illustrates a possible core example of a user experience for a payment initiated using a mobile device where a customer (payer) makes a payment from his/her own payment account to the payment account of another customer (payee). Payer and payee may be, and frequently are, customers of different MFSPs (four-corner model).

This use case does not assume upfront confidence between payer and payee. Both payer and payee will receive the same level of services from their respective MFSP. In many circumstances, this use case is applicable for payments-to-persons where small business entities are involved or where the individuals have a casual working relationship (e.g. paying a babysitter, a handyman). Figure 4 illustrates the following steps:

a) The payee provides all the necessary account information to the payer; in proximate mode, this information may be automatically retrieved using a contactless or other local interfaces;

b) The payer provides all the payee account information to his/her MFSP via his/her mobile device. This information can be input by the payer in full or by accessing a pre-registered payee. This is typically done by using a specific application or by accessing a mobile browser;

c) The payer, once authenticated by his/her MFSP, authorizes the payment instruction in compliance with the usual security requirements set out by that MFSP;

d) The payer's MFSP then processes and submits the credit transfer to the payee's MFSP which in turn credits the payee;

e) Optionally, the payee's MFSP sends a payment confirmation message to the payer MFSP. This fact is indicated by putting this message between brackets in Figure 4.

NOTE In some implementations, the immediate payment confirmation to the payer may not be possible.

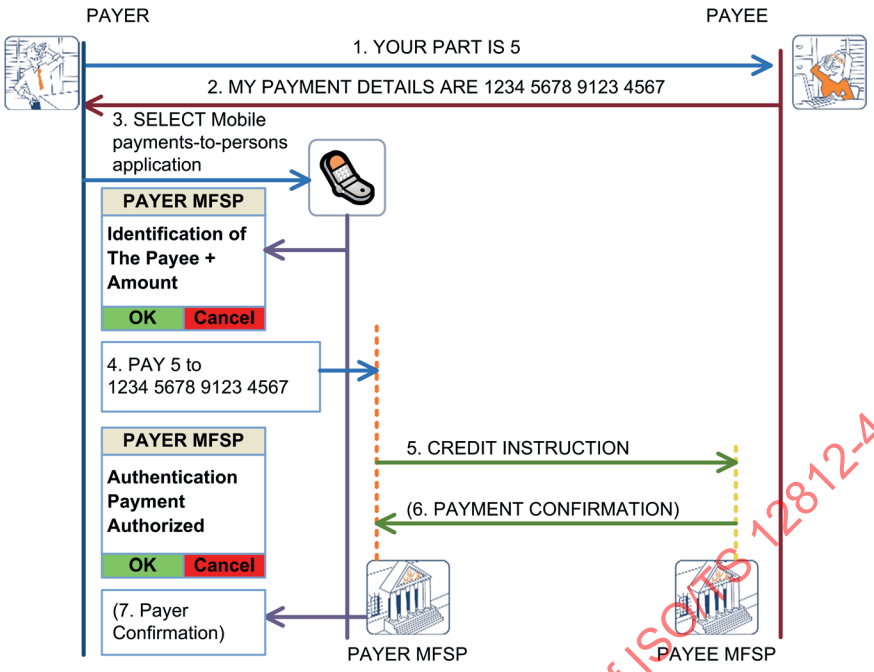

Figure 4 — Mobile payments-to-persons credit transfer

Table 2 — Mobile payments-to-persons credit transfer – core

Payments-to-persons Credit transfer – core	
Category	Payments-to-persons NOTE This method of transfer could also be applicable to other message flows according to Figure 4.
Communication type	Remote
Payment instrument	Credit transfer
Prerequisites	Payer subscribes to mobile remote payment service
Payment initiation by	Payer: steps 1,3 to 4 . Payee: step 2.
Payment facilitated by	Payer and Payee MFSP: step 5. Optional payment confirmation by the payee MFSP: steps 6 to 7. For details, refer to Clause 9. The detailed data flow may depend on the model followed by the system (bank-centric or non-bank-centric).
Payment settlement	See 9.3 and 9.4.

8.5.3.3 Credit transfer — Urgent

This document recognizes a variant of the credit transfer that may be implemented in mode "urgent transfer":

a) The payee provides all the necessary account information to the payer.

b) The payer provides all the payee account information to his/her MFSP via his/her mobile device. This information can be input by the payer in full or by accessing a pre-registered payee. This is typically done by using a specific application or by accessing a mobile browser.

c) The payer, once authenticated by his/her MFSP authorizes the credit transfer instruction in compliance with the usual security requirements set out by that MFSP.

d) The payer's MFSP then processes and submits the urgent payment to the payee's MFSP which in turn will credit the payee.

e) The payee will be able to confirm with his/her MFSP (almost instantly) that the payment has been received (e.g. mobile notification) and have access to the funds.

f) Optionally, the payee's MFSP sends a payment confirmation message to the payer MFSP. This fact is indicated by putting this message between brackets in Figure 5.

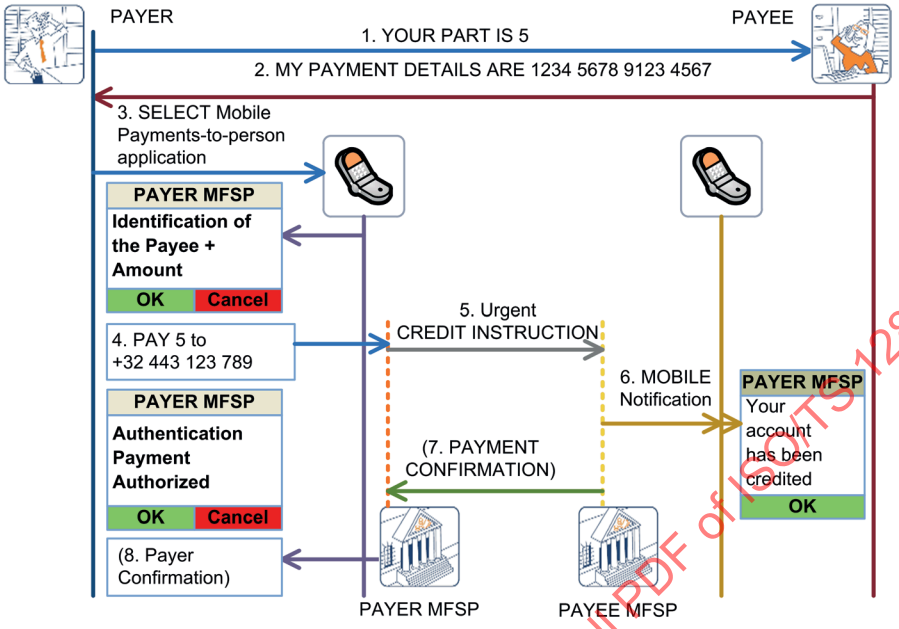

Figure 5 — Payments-to-persons urgent credit transfer

Table 3 — Payments-to-persons urgent credit transfer

Payments-to-persons urgent credit transfer	
Category	Payments-to-persons, also applicable to payments to small business
Communication type	Remote
Payment instrument	Credit transfer
Prerequisites	The establishment of an urgent credit transfer system
Payment Initiated by	Payer: steps 1, 3 to 4. Payee: step 2.
Payment facilitated by	Payer and payee MFSPs: steps 5 to 6. Optional payment confirmation: steps 7 to 8 by the payee MFSP. For details, refer to Clause 9. The detailed data flow may depend on the model followed by the system (bank-centric or non-bank-centric).
Payment settlement	See 9.3 and 9.4.

8.5.3.4 Credit transfer — Alias

A third scenario for payments-to-persons credit transfers makes use of a payee alias (e.g. payee mobile phone number) making the input of the payee details considerably more convenient for the payer.

It is assumed that:

— the payee shall have his/her identification details 'registered' against his/her alias;

— the payer's MFSP shall facilitate the use of aliases in its mobile payment instruction;

— the payer's MFSP shall be able to identify the payee's MFSP and payment account details from the payee's alias via a common infrastructure.

In Figure 6, the following steps are illustrated:

a) The payee provides his/her identification details to the payer, using a payee's alias.

b) The payer provides the necessary information (amount, payee's alias, etc.) to his/her MFSP via his/her mobile device. This is done by using a specific mobile application or by a mobile browser.

c) The payer, once authenticated by his/her MFSP, authorizes the credit transfer instruction in compliance with the usual security requirements set out by that MFSP.

d) The payer's MFSP establishes the payee's identification details and identifies the payee's MFSP using the payee's alias through a common infrastructure.

e) The payers MFSP submits the credit transfer to the payee's MFSP to credit the payee.

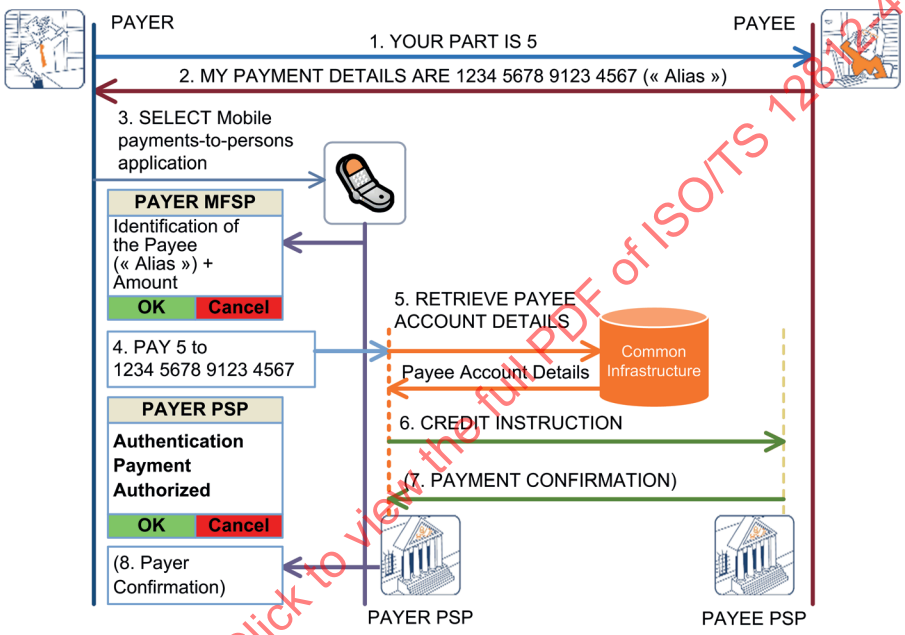

Figure 6 — P2P credit transfer – alias

NOTE In some implementations, the immediate payment confirmation to the payer may not be possible.

Table 4 — Mobile payments-to-persons credit transfer–alias

Payments-to-persons credit transfer–alias	
Category	Payments-to-persons
Communication type	Remote
Payment instrument	Credit transfer
Prerequisites	— The payee or the payee's MFSP has registered his/her identification details in a common infrastructure. — The payer's MFSP has access to the common directory infrastructure. — The payer's MFSP offers the alias-based mobile payment service.
Payment initiated by	Payer: steps 1, 3 to 4. Payee: step2.
Payment facilitated by	Payer and Payee MSFPs: steps 5 to 8. Optional payment confirmation by the payee MFSP: steps 7 to 8. For details, refer to Clause 9. The detailed data flow may depend on the model followed by the system (bank-centric or non-bank-centric).
Payment settlement	See 9.3 and 9.4.

9 Detailed payments-to-persons transaction flows

9.1 General

Clause 7 describes two high-level interoperability modes. Clause 8 provides some use cases for mobile payments-to-persons using credit transfers (both with direct and common infrastructure interoperability models) and cards as payment instruments and precising the basic messages to be exchanged. However, depending on the nature of the MFSP, a transaction generated with the same payment instrument (e.g. a credit transfer) may be processed in slightly different ways. This clause is intended to provide standard solutions for mobile payments-to-persons processing, by setting out transaction data flows for a series of payment models. As with Clause 8, the starting point is the payer having:

— enrolled a payment instrument with an MFSP, which may be a bank (bank-centric payments-to-persons model) or a non-bank institution (non-bank-centric payments-to-persons model);

— some sort of identifier of the account of the payee sufficient for the MFSP to routing the payment, possibly with the support of a common infrastructure (e.g. a common directory);

— the amount to be transferred, which may optionally be agreed and confirmed by the payee before the payment is executed.

In turn, the payee has been enrolled by an MFSP to collect valid payments which are transferred to the account designated by the payee, either a bank account or a payment account held by a non-bank institution.

For implementers interested in specific example of how these use cases have been implemented in the United States, see Reference [2].

9.2 Models for the processing of mobile payments-to-persons

Clause 9 differentiates three models for mobile payments-to-persons systems:

— bank-centric;

— non-bank-centric;

— card-centric.

Regardless of the model used by the mobile payments-to-persons transaction, a mobile payments-to-persons compliant with this document take place in three phases:

a) Initiation or setup phase: The payment instrument is selected by the payer (e.g. by selecting an application in a wallet), then the mobile device establishes a wireless communication with his/her MFSP to transfer a payment order along with an identifier of the beneficiary of the payment.

b) Payment facilitation phase: Authentication, authorization and optionally acceptance during which the payment instruction is processed. It includes:

   1) Specific authentication mechanisms to be implemented by the payer's MFSP (of the payment instrument, the payer and the payment data) are discussed in ISO 12812-2;

   2) Authorization of the payment results from the verification by the payer's MFSP of (i) the availability of funds in the payer's account and (ii) the existence of the payee's account possibly using a common directory.

c) Clearing and settlement phase: The MFSP proceeds to the transfer of funds between the payer account and the payee's account, using a clearing and settlement mechanism in one or more steps.

9.3 Bank-centric payments-to-persons models

Bank-centric mobile payments-to-persons allow for the transfer of funds from the bank account of the payer to the bank account of the payee over the ACH network. In bank-centric models, the customer is directly enrolled by a bank participating in the system. The payer initiates the payment by logging on to his/her bank's website or mobile payment application and opting to use the mobile payments-to-persons service. As in other methods, the payer provides the alias, email address or mobile phone number of the payee. The payment request is directly addressed by the payer to his/her bank. If the funds are available, the payer's bank forwards the payment request to an MFSP.

The MFSP verifies the existence of the payee's bank account (e.g. using a common infrastructure directory) and transmits the payment instruction message to the payee's bank. As an option, the payment may be subject to acceptance by the payee. In this case, the payee's bank transmits a payment confirmation back to the payer's bank through the MFSP.

After that point, the processing of the payment depends on how the payment is cleared and settled:

— through a split payment over the ACH system (see 9.3.1), or

— a single ACH payment from the payer to the payee (see 9.3.2).

9.3.1 Split payment over the ACH system

9.3.1.1 Main characteristics

The settlement takes place in two separate steps (also referred to as "legs"):

— In the first leg of the processing, the MFSP instructs its bank to pull funds from the payer's bank account using an ACH debit. The account information for the debit pull is provided to the payments-to-persons service by the payer at registration.

— In the second leg, the MFSP tells its bank to send funds to the payee's account using an ACH credit:

a) The account information for the credit push is provided to the MFSP by the payee at registration (if he has a registered account at a participating bank), or

b) It is obtained directly from the payee (if he does not have a registered account at a participating bank).

NOTE The ACH credit can sometimes be initiated before the ACH debit has been completed.

9.3.1.2 Detailed data flow description

The assumptions for this scenario are: (1) the payer uses the mobile device to send, e.g. 100 units to payee, (2) both the payer's bank and the payee's bank participate in the mobile payments-to-persons program and (3) both banks use the same clearing operator for their ACH processing.

Initiation or setup phase

a) The payer logs on to his/her bank's mobile website or activates bank mobile application to send 100 units to the payee using the payments-to-persons service and provides the payee's email address and/or mobile phone number.

Payment facilitation phase: Authentication, authorization and acceptance

b) The payer's bank verifies that the payer has sufficient funds.

c) The payer's bank transmits payment information to the MFSP.

d) The MFSP ascertains from payee's email address or mobile phone number that he/she has a registered account at a participating bank, (e.g. using a common directory infrastructure). Then, it transmits the payment information to the payee's bank.

e) The MFSP sends an email or a text message to payee informing him/her of payment.

The protocol then proceeds as follows:

— If the payment does not require the acceptance by the payee to proceed, then step i) applies just after step e).

— If the payment requires the acceptance by the payee, then steps f) to h) apply.

f) The payee logs on to his/her bank's mobile website or an application on mobile device and is informed that payment is waiting. The payee agrees to receive payment and chooses which registered account to use for deposit.

g) The payee's bank tells the MFSP that the payee has accepted payment and indicates which registered account he wants to use for deposit.

h) The MFSP sends an email or a text message to payer telling him/her that the payee has accepted the payment.

Clearing and settlement phase: Payment from payer to MFSP

i) The MFSP informs its bank that it has been authorized to pull 100 units of currency rom payer's bank account at payer's bank.

j) The bank sends ACH file to operator with debit to payer's bank account, using account information provided by payer to the MFSP during the registration.

k) The operator sends the ACH file to the payer's bank with debit to payer's bank account.

l) The payer's bank posts debit to payer's bank account (could occur earlier).

m) The operator debits the reserve account of payer's bank and credits reserve account of the MFSP bank.

n) The MFSP bank posts credit on to the MFSP bank account.

Clearing and settlement: Payment from payments-to-persons provider to payee

o) The MFSP tells its bank that it has been authorized to push 100 units of currency to payee's bank account at payee's bank.

p) The MFSP bank posts debit on to the MFSP bank account.

q) The MFSP bank sends the ACH file to the operator with credit to payee's bank account, using account information provided by the payee to the MFSP during registration.

r) The clearing operator sends the ACH file to the payer's bank with credit to payee's bank account.

s) The clearing operator debits the reserve account of the MFSP bank and credits the reserve account of the payee's bank.

t) The payee's bank posts credit on to payee's bank account (could occur earlier).

Figure 7 illustrates the flow of messages to execute the mobile payments-to-person bank-centric in split mode.

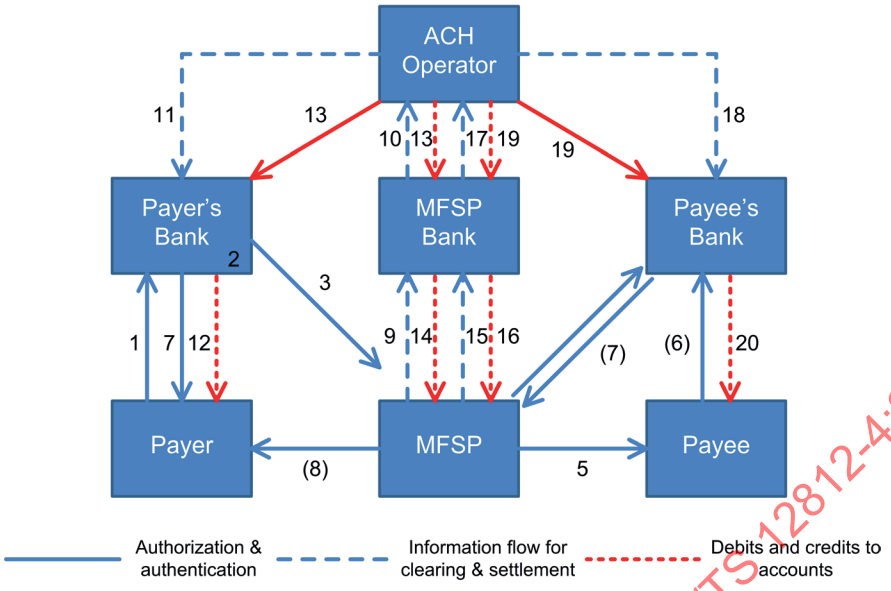

Figure 7 — Split bank-centric model

9.3.2 Bank-centric single payment over the ACH system consortium model

9.3.2.1 Main characteristics

In the second type of bank-centric mobile payments-to-persons, the funds are transferred by means of a single credit transfer from the payer's bank account to the payee's bank account. The service may be operated either by individual banks or by a consortium. The consortium refers to a multi-bank MFS program to provide mobile payments-to-persons services in one single payment. The payee's bank is not necessarily a member of the consortium.

— When the mobile payments-to-persons service is operated by an individual bank, the payee can receive the payment using an account at any bank. The bank operating the mobile payments-to-persons service sends the payee an email or text message informing him/her of the payment and asking for his/her bank account information. The bank uses the information to send an ACH credit to the payee's account if the account is held by another bank, or to make a book transfer to the payee's account if the account is also held by the payer's bank.

— When the mobile payments-to-persons are processed through a mobile payment bank consortium, a payee with an account at a member bank can go directly to his/her bank's website to receive the payment instead of providing his account information to the payments-to-persons service. Specifically, the consortium would use the payee email address or mobile phone number provided by the payer to determine if the payee was signed up for the mobile payments-to-persons service with a member bank:

a) If the payee was signed up, the consortium would transmit the payment information to the payee's bank, after which the payee optionally connects to his/her bank's website to accept the payment.

b) If the payee was not signed up with a consortium bank, he/she would be asked to go to the consortium's website to provide his/her account information.

Clearing and settlement would likely consist of a single ACH credit pushed from the payer's bank account to the payee's bank account. Two scenarios can be identified:

— If the payee was signed up with a member bank, he/she would indicate the account into which he/she wants the payment deposited. After the payee has made this choice, his/her bank would transmit the account information to the payer's bank through the consortium. Figure 8 provides the data flow for this case.

— If the payee was not signed up with a member bank, he would be asked to provide his account information on the mobile payment consortium website, and the consortium would pass the information on to the payer's bank. In both cases, the payer's bank would use the payee's account information to send him an ACH credit.

9.3.2.2 Detailed transaction flow

The assumptions for this scenario are:

— the payer uses a mobile device to send 100 units to the payee;

— both the payer's bank and the payee's bank belong to the consortium;

— they use the clearing operator for their credit/transfer/ACH processing.

Initiation Phase

a) The payer logs on to his/her bank's mobile website or selects a mobile application, indicates that he/she wants to pay 100 units of currency to the payee using the payments-to-persons service, and provides payee's email address or mobile phone number.

Payment facilitation phase: Authentication, authorization and acceptance

b) The payer's bank verifies that payer has sufficient funds.

c) The payer's bank transmits the payment information to consortium.

d) The consortium ascertains from the payee's email address or mobile phone number that he/she has an account at a member bank and transmits the payment information to the payee's bank.

e) The consortium sends an email or a text message to the payee informing him/her of the payment.

The protocol then proceeds as follows:

— If the payment does not require the acceptance by the payee to proceed, then step j) applies just after step e).

— If the payment requires the acceptance by the payee, then steps f) to i) apply.

f) The payee logs on to his/her bank's mobile website or mobile app and is informed that payment is waiting for approval. The payee agrees to receive payment and chooses which account to use for deposit.

g) The payee's bank sends a message to the consortium indicating that the payee has accepted the payment and providing the payee's account information.

h) The consortium passes the message from payee's bank to payer's bank.

i) The consortium sends an email or a text message to the payer informing her that the payee has accepted the payment.

Clearing and settlement

j) The payer's bank posts the debit to the payer's bank account.

k) The payer's bank sends an ACH file to the clearing operator with credit to payee's bank account, using account information sent by the payee's bank.

l) The clearing operator sends ACH file to payee's bank with a credit to payee's bank account.

m) The clearing operator debits the reserve account of the payer's bank and credits the reserve account of the payee's bank.

n) The payee's banks posts credit to payee's bank account.

NOTE Depending on the risk policy of the payee's bank (e.g. if urgent payments-to-persons service is provided), the payee's account could be credited earlier (after step f)).

Figure 8 illustrates the flow of messages to execute the single mobile payments-to-persons bank-centric.

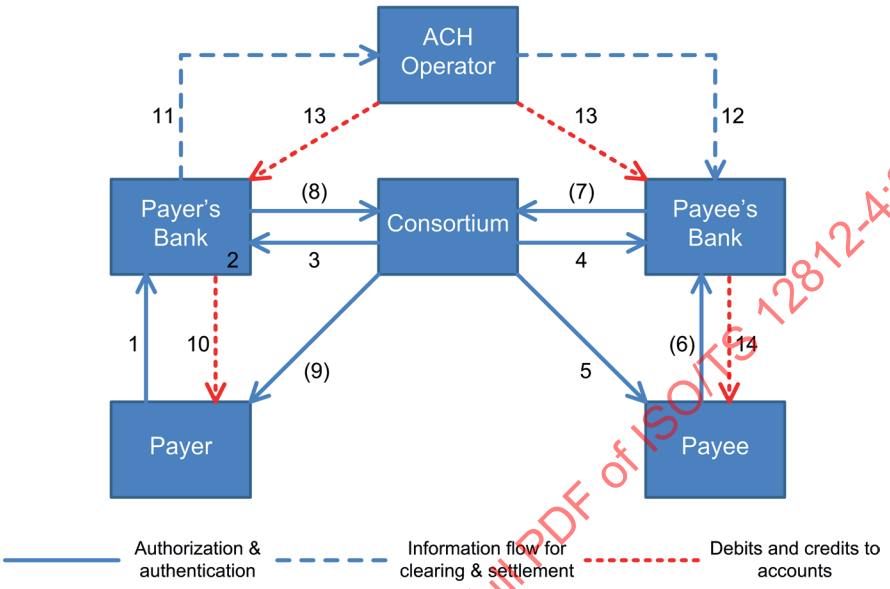

Figure 8 — Single bank-centric consortium model

9.4 Non-bank-centric models

9.4.1 General

The payer's MFSP often provides an application managing a payment instrument associated to a payer's payment account.

The non-bank-centric mobile payments-to-persons models generally require the payer to have a payment account with the intermediary non-bank MFSP before initiating the payment. Many non-bank-centric solutions also require that the payee either already has an account or establishes an account to receive the payment (viral business model). Establishing an account in a non-bank MFSP generally entails:

— Creating a user ID and password and providing the non-bank MFSP personal details such as home address, email address and phone number. The nature of these data may be subject to local regulation;

— Designating a source from which payments can be funded, the main alternatives being a bank account or a payment card.

In all cases, the payer initiates the payment by logging on to the MFSP website or the mobile payment application of the non-bank intermediary. The payer's and the payee's MFSPs intermediate the overall transaction, using the bank system infrastructure when needed.

This document recognizes different scenarios for the processing of non-bank centric payments-to-persons, depending on whether:

a) the mobile payments-to-persons is funded using a bank account or an account held by the non-bank MFSP;

b) the MFSP stores value in an intermediate stage of the payment transaction;

c) the mobile payments-to-persons system follows a three-corner or a four-corner model;

d) the MFSP has direct or indirect access to clearing and settlement facilities.

How non-bank-centric payments are cleared and settled depends on a variety of factors, including the funding source used by the payer and the way funds are received by the payee. This standard differentiates four different scenarios, which are described in 9.4.2, 9.4.3, 9.4.4 and 9.5 respectively.

9.4.2 Three-corner non-bank-centric methods funded by non-bank account

9.4.2.1 Main characteristics

The payment is executed by account transfers on intermediary books. This method requires both the payer and the payee to hold a payment account with the same MFSP before initiating the mobile payments-to-person. The payer's account is to be prefunded before initiating the payment.

9.4.2.2 Detailed transaction flow

Initiation Phase

a) Payer logs on to MFSP's mobile website or an application, indicates he/she wants to pay 100 units of currency to the payee from his/her linked bank account and provides to the MFSP the payee's email address, text, or mobile phone number.

Payment facilitation phase: Authentication, authorization and acceptance

b) MFSP sends an email or a text message to the payee informing him of payment.

The protocol then proceeds as follows:

— If the payment does not require the acceptance by the payee to proceed, then step e) applies just after step b).

— If the payment requires the acceptance by the payee, then steps c) to e) apply.

c) The payee logs on to MFSP's mobile website or a downloadable application and indicates that he/she wants to receive the payment in his/her linked bank account.

d) The MFSP sends an email or a text message to the payer informing him/her that the payee has accepted the payment.

Settlement phase

e) MFSP debits 100 units of currency from the payer's payment account and credits 100 units of currency on to the payee's payment account.

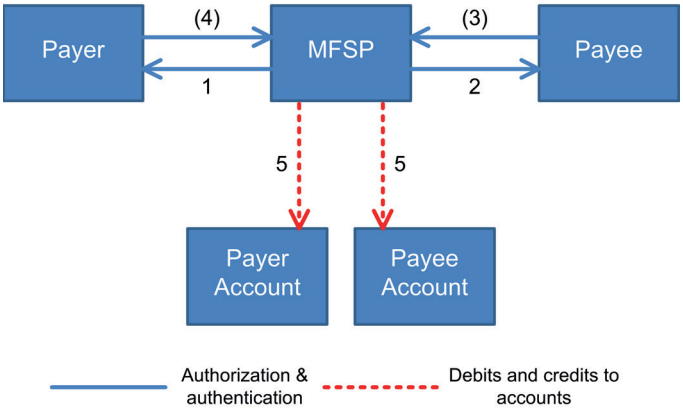

Figure 9 — Three-corner non-bank-centric model

9.4.3 Split non-bank centric model funded by bank account

9.4.3.1 Main characteristics

Split non-bank centric mobile payments-to-persons funded by bank account are processed in a way similar to bank-centric methods. The MFSP's bank transmits to the ACH two consecutive debit ("pull") and credit ("push") orders originated from the MFSP. The settlement takes place in two separate steps (also referred to as "legs"):

— In the first leg of the processing, the MFSP instructs its bank to pull funds from the payer's bank account via an ACH debit, using the account information provided by the payer. These funds are transferred to the payment account held by the payer in the MFSP.

— In the second leg which may begin before the first leg is completed, the MFSP instructs its bank to push funds to the payee's account via an ACH credit, using the payee bank account information available to the MFSP.

In most of these systems, both payments are executed over the ACH network.

9.4.3.2 Detailed transaction flow

Initiation Phase

a) The payer logs on to the MFSP's mobile website or an application, indicates he/she wants to pay to the payee from his/her linked bank account, and provides the payee's email address, text, or mobile phone number.

Payment facilitation phase: Authentication, authorization and acceptance

b) The MFSP sends an email or a text message to the payee informing him/her of the payment.

The protocol then proceeds as follows:

— If the payment does not require the acceptance by the payee to proceed, then step e) applies just after step b).

— If the payment requires the acceptance by the payee, then steps c) to e) apply.

c) The payee logs on to the MFSP's mobile website or an application and indicates that he/she wants to receive the payment in his/her linked bank account.

d) The MFSP sends an email or a text message to the payer informing him/her that the payee has accepted the payment.

Clearing and settlement phase: Payment from payer to MFSP

e) The MFSP tells its bank that it has been authorized to pull 100 units of currency from the payer's bank account.

f) The MFSP's bank sends the ACH file to the clearing operator with the debit to payer's bank account, using the account information provided by the payer to the MFSP.

g) The clearing operator sends an ACH file to payer's bank with debit to payer's bank account.

h) The payer's bank posts debit to payer's bank account.

i) The clearing operator debits the reserve account of the payer's bank and credits the reserve account of the MFSP bank.

j) The MFSP bank posts the credit to MFSP bank account.

Clearing and settlement: Payment from MFSP to payee

k) The MFSP tells its bank that it has been authorized to push 100 units of currency to payee's account at the payee's bank.

l) The MFSP bank posts debit to MFSP bank account.

m) The MFSP bank sends ACH file to the clearing operator with the credit to payee's bank account, using account the information provided by the payee to the MFSP during the registration.

n) The clearing operator sends the ACH file to payee's bank with the credit to payee's bank account.

o) The clearing operator debits the reserve account of the MFSP bank and credits the reserve account of the payee's bank.

p) The payee's bank posts the credit on to the payee's bank account.

NOTE Depending on the risk policy of the payee's bank (e.g. if urgent payments-to-persons service is provided), the payee's account could be credited earlier (after step c)).

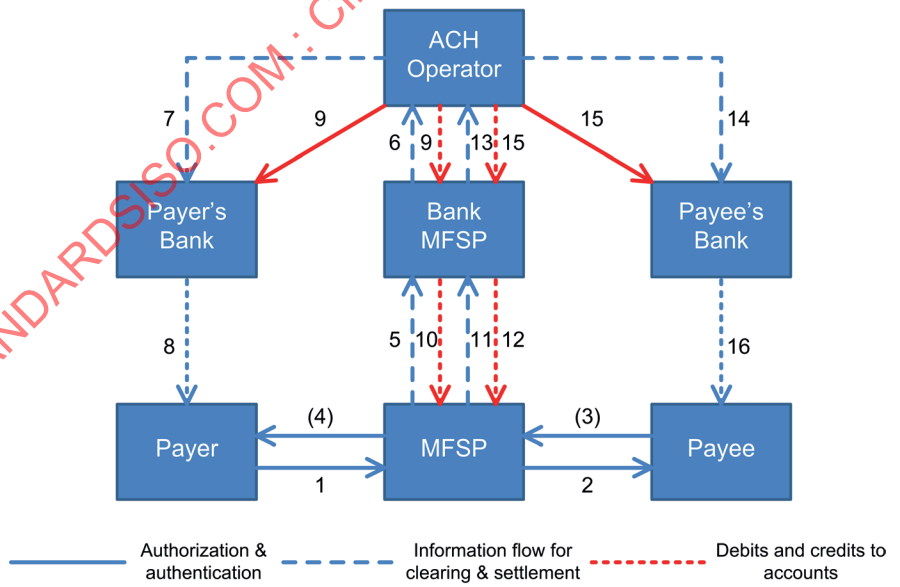

Figure 10 — Split non-bank-centric model funded by bank account