MOBEY FORUM

Mobile Remote Payments

General Guidelines for Ecosystems

White Paper

June 2010

MOBEY FORUM

Mobile Financial Services

Edgar, Dunn & Company

Management Consultants

June 2010

Mobey Forum Remote Payments Task Force

Chair:

Jonathan Bye	Royal Bank of Scotland

Co-chairs:

Jonatan Evald Buus	CellPoint Mobile
Olivier Denis	SWIFT

Editorial Panel:

Samee Zafar	Edgar, Dunn & Company
Liisa Kanniainen	Mobey Forum
Ville Sointu	Tieto
Jonathan Bye	Royal Bank of Scotland
Jonatan Evald Buus	CellPoint Mobile
Olivier Denis	SWIFT

Contributors:

Bent Bensen	DnB NOR
Olivier Cognet	Nokia
Edna Cubillos	Redeban Multicolor
Valentin Echeverry	Redeban Multicolor
Viktoria Erngard	Telenor
Alistair Gates	Edgar, Dunn & Company
Gunilla Garpas	Nordea
Riekus Hatzmann	Atos Origin
Pekka Laaksonen	Nordea
Anne Lene Hvalen	BBS
Olli Jussila	TeliaSonera
Thomas Magin	Deutsche Bank
Jean-Luc Pellegrinelli	Caisse d'Epargne
Jack Robinson	VocaLink
Gerhard Romen	Nokia
Minh van Le	Atos Origin
Bernard van der Lande	Atos Origin
Olli Welin	TeliaSonera
Michael Whyte	SWIFT

Support:

Tanja Viskari	Mobey Forum
Ida Floor	Mobey Forum

Contents

Chairman's Foreword

When agreeing to chair the Mobey Forum's Remote Payments Task Force some 12 months ago it seemed a straight forward task to produce a White Paper on mobile remote payments.

However it soon became clear that this is a highly complex ecosystem with multiple stakeholders and a fast pace of technological development.

We quickly had to find a way to add value to the debate and utilise the extensive experience and resource available through the Mobey Forum membership.

One of the great strengths of Mobey is that it is possible to draw on a broad base of knowledge from the banking industry, payments processors and infrastructure providers, MNO's, handset manufacturers, systems integrators and consultancy firms.

This unique combination of members provides a perspective not available to many other groups that are focused around a single industry or interest. Of course it can also make consensus finding and decision making more challenging and along the way to producing this report we had some heated but highly productive discussions.

We also signed a cooperation agreement with the European Payments Council Mobile Channel Working Group (EPC M-CWG) which led to the sharing of early drafts and joint discussions that provided valuable feedback. I am grateful to Dag-Inge Flatraaker, chair of the M-CWG, and the team for their support.

There are a large number of reports on mobile payments and while these serve a valuable purpose we wanted to distinguish Mobey Forum's output. This report does not describe mobile pilots and implementations nor does it provide detailed technical implementation guidelines. Rather it describes business models and core processes required to ensure interoperability and start the market.

Mobey Forum is a global organisation hence the models are generic, designed to be adapted to local and regional market conditions.

Payment providers and other stakeholders will need to determine which models best suit their markets, whether they utilise centralised or decentralised common infrastructures or models that do away with such infrastructure and rely entirely on direct messaging between the transacting parties.

Finally I would like to thank Tanja Viskari of Mobey Forum for her support and coordination and Samee Zafar of Edgar, Dunn & Company for his insights and sterling work in pulling together inputs and editing skills.

Jonathan Bye

Royal Bank of Scotland & Chair, Mobey Forum Remote Payments Task Force

Executive Summary

With over 4 billion[1] mobile devices on a global basis, the mobile phone is perhaps the most successful consumer device in history in terms of consumer access, penetration, and usage. The mobile phone offers new possibilities and opportunities for offering a wide range of services to consumers and businesses including mobile payments.

The mobile phone can be used for making *physical* payments at a shop or some other physical location - or *remotely* where payments can be made irrespective of the location of the payer and the payee. This paper deals with remote payments only.

This paper suggests that the mobile phone number, and not any other specific code or identifier, should be used to identify the payer and payee in a mobile remote payment transaction. Using the mobile phone number will provide user convenience, ensure privacy and the security of payment information, and facilitate interoperability across stakeholders.

For mobile remote payments to achieve critical mass in the shortest possible timeframe and to minimise infrastructure investments, it is essential to leverage existing payment infrastructure as far as possible. The paper identifies guidelines for developing a payment "ecosystem" stressing the need for interoperability across different payment systems and stakeholders across the globe.

This paper discusses three potential ecosystem models based on varying levels of interoperability. These are summarised below:

- ❖ *Common Infrastructure Model* (CIM) suggests a central or distributed database which links the mobile phone number with existing payment instruments such as bank accounts, payment cards, or stored value accounts. The mobile phone number is then used as the "mobile identifier" or MID to identify the transacting parties

- ❖ *Intermediate Operability Model* includes the CIM model above and additional capabilities to facilitate mobile remote payments across systems that are currently not interoperable

- ❖ *Direct Interoperability Model* does not require common infrastructure but indicates that the payment transaction format is modified and adapted to facilitate mobile remote payments.

This paper discusses these models, identifies the requirements for implementing the models, and provides generic process flow diagrams for implementing secure and interoperable mobile remote payments.

[1] CIA World Factbook

Introduction

The Remote Payments Task Force of the Mobey Forum has developed this document for industry guidance and consultation.

Mobey Forum is a global non-profit organisation, driven by the finance industry. Mobey Forum has over 50 members; the member categories are banks, vendors, payment processors and MNOs. Its objective is to envision prosperous Mobile Financial Services (MFS) ecosystems.

The mission of the Mobey Forum is to facilitate banks to offer mobile financial services through sharing insight from pilots, cross-industry collaboration, analysis, experiments and co-operation and communication with relevant external stakeholders. The main focus is on building sustainable business model alternatives.

Mobey Forum Strategy is three-fold:

- Informational – industry insight, first-hand experience sharing, knowledge repositories, regular industry news and member updates
- Networking – Mobey Workshops connect the leaders cross industries to build new relationships
- Shaping the industry - creating the future: interaction and ongoing liaisons with standardisation organisations, analysts and industry influencers

Mobey Forum organises four two-day Workshops per year, each specially designed to address the most challenging current issues, facilitated by recognised leaders within the industry. Workshops are highly interactive with opportunities for strategic learning, networking and sharing of peer experiences. Additionally Mobey Forum fosters ongoing Workgroups and Task Forces in order to promote the exchange of expertise, insight and solutions.

Mobey Forum was founded in May 2000 and now it is an established industry body aiming to create the Mobile Financial Services ecosystem. Mobey Forum has become the leading source of independent cutting edge MFS market information.

The mobile phone and the services it offers have evolved remarkably over the last decade or so. Initially used mainly for voice communication, it is now being extensively relied upon for all types of communication messaging involving text and data exchange such as Short Messaging System (SMS), Multimedia Messaging Service (MMS) and internet browsing. Both voice and data communications are indispensible for consumers and generate billions of dollars for providers across the globe. Mobile phones vastly outnumber personal computers, televisions, or music players.

Another major triumph of the mobile phone is that it appeals to consumers across geographies transcending customer income and wealth profiles. One is just as likely to see a mobile phone being used on a yacht cruising in the Mediterranean as in the hands of a fruit picker in rural India.

Offering consumer services that can be delivered over a mobile device has the potential to reach an unprecedented proportion of global consumers and businesses like no other consumer device. With the growth of mobile broadband internet, the distinction between mobile communications and mobile computing devices is blurring.

Already the latest “smartphones” offer a vast array of applications, just like computers, ranging from practical programs such as spreadsheets to mobile television to all types of video games and entertainment packages. Tomorrow’s essential handheld device will communicate, compute, and connect in an all in one integrated and convenient manner acting as an indispensible personal assistant no matter what you do and where you live.

For institutions interested in providing mobile payments or financial services, the mobile phone represents new opportunities to access customers. The mobile channel can act as a virtual branch that can offer banking and payment services to the entire customer base.

In the physical world, a number of pilots and preliminary programmes have been rolled out where a mobile device is used to pay for goods and services by tapping, touching, or waving at a contactless point of sale (POS) terminal. These are called proximity of mobile contactless payments or NFC (Near Field Communication) payments. These payments are not within the scope of this document.

This paper is focused on mobile remote payments which enable two parties to send and receive payments or exchange funds using the mobile channel irrespective of where they are located. These are defined in more detail in a later section. The paper covers all types of remote payments for goods and services and those that simply transfer funds between two or more parties (commonly called mobile money transfers).

Background & Objectives

1. Background

In today's world, payments are made with various payment instruments, such as bank accounts[2], payment cards, and stored value accounts, using standardised "payment identifiers" (e.g., a bank account or credit card account number). When a person wants to pay or transfer funds to another person or business, they are able to do so by instructing their payment services provider, such as a bank or a card company, to transfer value from their account to that of the receiver or payee.

Advances in payment systems technology, infrastructure, and channels mean that such financial transactions can be made over a number of channels such as bank branches, POS terminals, automated teller machines (ATM's), the internet (directly or via internet banking), and now over mobile phones. These channels accommodate the commonly used payment instruments such as bank accounts, payment cards, and stored value accounts.

A key characteristic of a payment transaction is that it requires the payment identifiers of all parties to a payment transaction. In a bank account to bank account electronic payment, the payer provides the details of the recipient – account number and routing information – to their bank. Such payment identifiers, therefore, form the core mechanism over which the routing, clearing, and settlement of all payment transactions takes place.

In mobile communications, voice and data messaging are routed using a unique identifier - referred to in this document as the Mobile Identifier or MID - to identify the mobile subscriber. In such communications the mobile phone number[3] is used as the "mobile identifier" or MID.

To develop a framework for facilitating mobile remote payments that are efficient and convenient, the paper strongly suggests that the mobile phone number is used as the MID and not any other identifier for identifying, sending and receiving payments between transacting parties. In other words, when someone wants to initiate a mobile payment, they need to know only the phone number of the recipient and not the details of their bank account.

At the very minimum, there are three key reasons for using the mobile phone number as the MID - the primary identifier for mobile remote payments:

- *Convenience*: A new payment instrument, method, or channel must offer a compelling consumer experience based on added customer convenience to be attractive to users.

[2] Throughout this document, a bank account refers to the relevant payment instruments such as credit transfers, standing orders, and direct debits that access the account

[3] Mobile Subscriber Integrated Services Digital Network Number(MSISDN) in GSM standard terminology

People already communicate using phone numbers and are hardly likely to ask others the details of their bank accounts or payment card numbers in order to make payments.

- *Privacy and Security*: In addition to convenience, another key consideration for using the MID for mobile remote payments is that people, in general, are reluctant to share their financial details with others unless they trust them. In addition to identity theft, unauthorised access to bank account or payment card details can result in payment fraud and significant losses for all stakeholders. Using a payment mechanism that only requires the MID while keeping the payment details confidential ensures the integrity of a remote payment system and keeps financial information private.

- *Interoperability*: Not all payment systems are interoperable. The systems and protocols leveraged by Visa and MasterCard are to a large extent similar as they follow common technical standards (for example, to interface with point of sale (POS) terminals at merchants or cash machines) but they are not interoperable with each other (a payment on a Visa card can only be made to a merchant who accepts Visa card transactions. A Visa merchant will not accept payments made with a MasterCard card product). Mobile phone numbers, on the other hand, follow standardised topologies and are based on global routing and roaming standards. A mobile subscriber can identify and connect with another subscriber simply using the mobile phone number. To achieve critical mass for mobile payments, this standardisation of mobile subscriber identification can be leveraged, as far as practical to maximise interoperability across diverse mobile payment systems. The interoperability challenge of many mobile payment systems is, therefore, to leverage the flexibility of the mobile phone number to offer a high degree of interoperability in order to maximize the usage potential by consumers.

This paper also recognises that the MID is one of several possible identifiers and is itself not without challenges to implement, namely in terms of control and ownership, number recycling by MNO's and customer churn.

2. Objectives

In light of the above, this paper aims at providing the stakeholders of the mobile payment industry with indicative guidelines to develop "ecosystem(s)" for mobile remote payments that:

- Are open and interoperable[4]
- Offer convenience through the use of mobile identifiers or MID's (this paper suggests the MID is represented by the mobile phone number) for identifying the sending and receiving entities
- Leverage underlying infrastructures for existing payment instruments, such as a bank account, payment card, or stored value accounts. The paper does not envisage frameworks that require entirely new payment systems to be developed.

[4] For discussion on open and interoperable systems please refer to the next section

The “ecosystem” identifies the parties or stakeholders and their roles initiating, processing, and completing a mobile remote payment.

It is important to note that the aim of this paper is to provide guidance and a more informed understanding of commercially and operationally viable mobile remote payment models. While the paper describes the core elements of an ecosystem, it does not recommend or in any way prescribe an ideal mobile payments environment for a specific marketplace or payment service. It is up to the individual mobile payment providers to develop their own business models with pricing structures that reflect their business strategies and competitive strengths.

Core operational processes described and analysed in this paper are for illustrative purposes only. These incorporate the minimum process requirements to ensure that mobile remote payment transactions are initiated securely and accurately and are completed efficiently. These process descriptions do not entail any recommendations nor any proposals for standardisation of operational processes.

Important Note: The paper focuses on mobile payments only. Other applications such as mobile banking or using the mobile device solely for identification, validation, or verification purposes are beyond the scope of this paper.

Mobile Remote Payments

1. Overview

Mobile remote payments refer to payments that are ***initiated*** using a mobile communications device ***irrespective of the location*** of the payer or the payee.

For the purposes of this document, these do not include proximity (contactless) payments, where a mobile phone is used as a point-of-sale terminal, or where the mobile phone is used purely for the purposes of authorising a transaction.

Mobile remote payments can be classified into several "use cases", some of which are identified below for illustrative purposes[5]. The key criteria for such classification is based on the transacting parties involved and the reasons for undertaking the transaction.

- Person-to-Person (P2P): Transfer of funds from one individual to another using a mobile device also referred to as mobile money transfers (MMT). These include social payments (e.g., paying for shared expenses etc).

- International Remittances: A person-to-person / mobile money transfer across international borders considered a separate category due to the relatively higher payment value, possible foreign exchange requirement, and regulatory complexity.

- Person-to-Small Business (P2SB): Payments made by individuals for informal services (e.g., payments for babysitting or second hand items) or to formal sellers on a small scale (e.g., self employed plumbers). These are more akin to person-to-person payments.

- Person-to-Business (P2B): Payments to businesses for goods and services. This includes all physical goods and services but excludes digital goods such as ring tones and bill payments (considered separately). Conversely, also covered are business-to-person payments such as those for disbursement of salaries and wages or reimbursement of employee expenses.

- Mobile Bill Payments: Payments usually made for utilities such as those for gas, electricity, and water and other similar services normally, but not always, incurred on a recurring basis. Bill payment is related to but different from bill presentment where a bill is presented over a mobile device for approval or acceptance upon which a payment may be initiated using an existing arrangement such as a standing order.

[5] Various alternative terms are also used: such as consumer in place of person, merchant in place of business

- M-Commerce: Payments for digital goods such as ringtones and software applications that are downloaded directly onto the mobile device. A significant proportion of such payments are billed by the mobile operator(s) providing the service.

- Business-to-Business (B2B): Payments or funds transfers between two businesses. These could be payments for supply of goods and services and are usually large in value relative to retail payments.

Important Notes:

- The purpose of the list above is to identify broad mobile remote payment categories. Certain items and terms above may be used or interpreted differently in different markets (such as the definition of a small business). The list is not meant to be exhaustive.

- To accommodate the rapid advancements taking place such as the expected convergence between mobile computing and mobile communications, payment categories are described in a generic sense and are not intended to be precise.

2. Ecosystem Stakeholders – Definitions and Roles

There are various stakeholders involved and their roles and responsibilities are described in this paper. The core stakeholder list includes:

2.1 Primary Stakeholders

- Payer (or Sender): The payer uses a mobile device to initiate the payment transaction which is processed through a “payment provider”.
- Payer’s (or Sender’s) payment provider (PP): A payment provider such as a bank, a card issuer, a remittance agent, or a provider of stored value accounts who offers the mobile payment service to the payer. The payee's PP is responsible for authenticating the payer and complying with all relevant and applicable Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.
- Payee (or Receiver): The payee can be an individual, a business whether informal, small, large, or a regular merchant who accepts payments over various channels including mobile channels.
- Payee’s (or Receiver’s) payment provider: A payment provider such as a bank, remittance agent, card issuer, merchant acquirer, or a provider of stored value accounts who provides the mobile payment service to the customer. The payee's PP would usually be providing the customer account to the receiver to which the incoming payment will be credited.

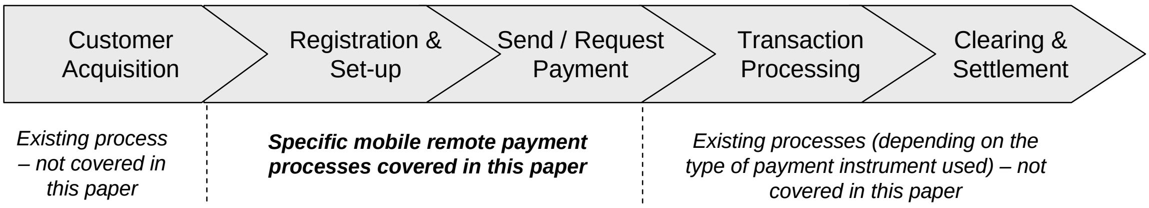
2.2 Enabling Stakeholders

These are stakeholders who do not necessarily have a direct relationship with customers but provide the enabling infrastructure over which a mobile remote payment is initiated, processed, and completed.

- Mobile Network Operator (MNO): The operator will provide the messaging infrastructure for text messages or other communication protocols that support mobile remote payments. MNO's are also referred to as wireless carriers.
- Central Infrastructure Manager (CIM): In certain situations where a centralised directory service is used to enable mobile remote payments, the directory provider will link a customer's (a) mobile identifier or MID (normally the mobile phone number) and (b) their default payment instrument such as a credit card or a bank account. This will enable the mobile identifier to act as a proxy or pseudonym for the card or account number to facilitate payments over existing networks. This role can also be fully or partially undertaken by a third party technology provider or a mobile operator. The CIM can also offer and operate customer authentication services.
- Payment Network: An existing payment system over which a payment transaction is completed such as an Automated Clearing House (ACH) or a bilateral clearing service for moving funds across bank accounts or payment card networks such as Visa or MasterCard.
- Handset Manufacturer: Handset manufacturers also play a significant role in the ecosystem by developing handsets that are designed to facilitate mobile payments and also through relevant value added services such as application pre-loading where relevant.
- Application Providers and Others: Mobile applications are fast emerging on the scene. They have generated a phenomenal level of demand from users of smart phones. Payment providers will be able to design creative remote payment applications for their customers. Application design and ease of use will serve as significant competitive features. Other stakeholders, for example, Secure Element (SE) manufacturers may also provide relevant services such as secure application storage.
- Government or Regulatory Entities: Government organisations and regulatory bodies aim to have relevant rules and regulations in place that keep payment systems secure and ensure that the interests of consumers and other payment system users are safeguarded and protected.

2.3 Process Value Chain

A series of core processes enable a mobile remote payment to be initiated and completed. At a high level, relevant processes of the value chain are described below.


Customer Acquisition
Registration & Set-up
Send / Request Payment
Transaction Processing
Clearing & Settlement
Existing process – not covered in this paper
Specific mobile remote payment processes covered in this paper
Existing processes (depending on the type of payment instrument used) – not covered in this paper

Customer Acquisition: This is an existing process within a payment provider. This relates to marketing and campaign management in order to acquire new customers. Though part of the overall value chain, it is relevant to all types of transactions and not just mobile remote payments. It is not covered in this paper.

Customer Registration & Account Set-up: A customer after signing up for the service will need to provide additional details for the customer record to be set-up for the service on the payment provider's systems. This process is explained later in this paper.

Send / Request Payment: This process is defined separately for sending and requesting a payment. This process forms the core of this paper in terms of suggested guidelines.

Transaction Processing; Clearing and Settlement: These are essential processes for any payment transaction. The paper envisages mobile remote payment services to leverage existing payment infrastructure. Therefore, these processes are those utilised in existing payment systems and not covered here.

There are certain additional supporting process that are listed below:

Customer support: The essential minimum level of customer support that should be provided is suggested in this paper.

Risk Management; Legal & Regulatory Compliance: Critical to any payment system but as risk management policies as well as legal and regulatory guidelines and regulations are different across markets, these are out of the scope of this paper.

3. Mobile Remote Payments Ecosystem

This section lays out an overview of a framework for enabling mobile remote payments over open and secure environments that leverage existing payments infrastructures offering a quick and pragmatic route to mass market acceptance of mobile remote payments.

3.1 Proprietary Payment Systems

Proprietary payment systems usually require both the payer and the payee to have accounts with the same payment provider. These are also called “closed loop” or “three party” payment systems.

Proprietary payment systems deal directly with end-customers. PayPal, for example, requires senders and receivers of funds to be registered with PayPal. Western Union, despite its wide global reach, is a proprietary payment system as it deals directly with end-customers and only supports transfers within a network of certified Western Union agents.

These systems are generally not interoperable with other payment systems. However, a proprietary system can interface with other proprietary systems on a bilateral basis or, more importantly, with an open payment system (see below) complying with standards and formats prescribed by that system. PayPal, a proprietary system interfaces with open banking systems for the purposes of depositing and withdrawing funds.

3.2 Open Payment Systems

An "open" payment system does not generally deal directly with end-customers or offer them payment accounts. Payment providers who participate in an open payment system offer interoperable payment services to their end users These payment providers are separate commercial entities and deal directly with their own end-customers.

Card payment networks such as Visa and MasterCard are examples of open payment systems because they do not deal directly with end-customers but enable participating financial institutions to offer payment services to their end-customers so that these customers can make payments wherever Visa or MasterCard payments are accepted.

Similarly, an ACH using SWIFT global messaging standard based on ISO20022 for authorising, clearing and settling account-to-account credit transfer between banks is an example of an open payment system. The ACH executes the credit transfer between banks without dealing with end-customers and uses a standardised messaging infrastructure for payments instructions referred to as the interbank payment interoperability domain.

Important Notes:

- Mobile remote payment ecosystem models described in this document relate to *open* payment systems which allow multiple entities to transact with each other.

- It is important to indicate here that payment systems may follow industry accepted formats and technology standards but may still opt to remain proprietary. Such systems will find it relatively easier to become interoperable with other systems at a later stage when they choose to do so compared to systems developed on unique proprietary standards.

4. ECOSYSTEM REQUIREMENTS

There are certain key requirements that are integral to a mobile remote payment ecosystem irrespective of the marketplace or geographic region of activity.

Please note that proprietary payment systems are also considered and discussed in this paper to the extent that an open payment ecosystem is able to provide an interoperability bridge across such systems (See Level 2 - Intermediate level below).

1. INTEROPERABILITY

For the development of an open mobile remote payment environment, it is important for stakeholders to review different available interoperability options.

This document envisages three interoperability options. Each market may follow its own approach that best suits its needs. The operational processes described later in this paper focus on different interoperability options in order to provide helpful and pragmatic implementation suggestions for developing mobile payment services.

The three broad interoperability options described below link to the three operating models described later in this document:

- ***Level 1 - Existing***: This relates to payment ecosystems that operate within existing levels and limitations of current payment systems

- ***Level 2 - Intermediate***: An expanded level of interoperability that provides a "bridge" between two or more payment systems that are presently not interoperable. For example: Payment from a customer of a payment system to a customer of another system where the two systems are not presently interoperable

- ***Level 3 – Direct or Extended***: A level of interoperability where mobile remote payments are undertaken in agreed transaction formats and in compliance with open and shared standards. Whether a payment between a payer and payee is completed directly or facilitated by one or more entities, under this interoperability option, a payment transaction is generated, received, processed and completed using common standards that are universally accepted irrespective of technology or underlying processes.

2. EXISTING PAYMENTS INFRASTRUCTURE

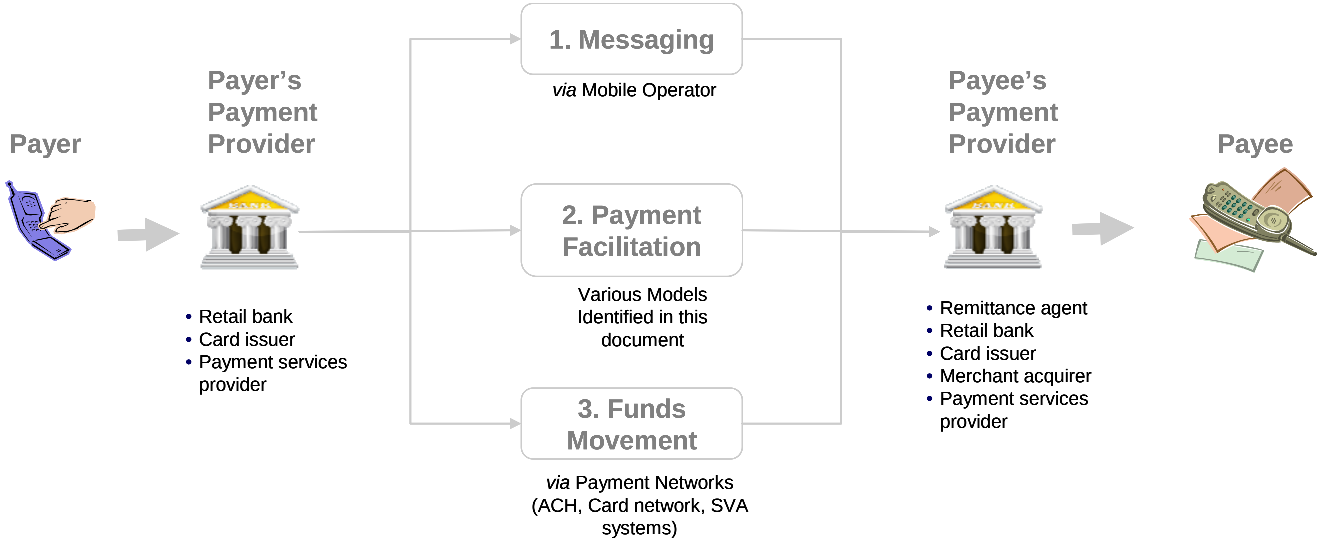
The general guidance supplied by this document stresses the importance of leveraging existing payment infrastructures. While this is not a mandatory requirement, quick time to market can only be achieved through utilising existing technology and underlying systems rather than creating entirely new structures for supporting mobile remote payments. This will also help minimise additional infrastructure investments to the extent possible.

3. Security

A foremost requirement for offering mobile remote payments is to ensure that all payment transactions are initiated and completed in a secure manner. Supporting systems and processes should be in place to mitigate operational and financial risks. Established payment systems have developed effective procedures relating to risk management such as fraud prevention and authentication processes. Authentication for authorised users is a key factor to assure customers and businesses that a mobile payment is not likely to be fraudulent and where relevant, to control non-repudiation and to establish defined liabilities in case of any claim.

5. Ecosystem Components

Three core components of a mobile remote payment ecosystem enable a payment transaction to be securely and successfully completed. These are discussed below:



- **Component 1: Messaging (or Communications)**

  Messages between the various parties to a payment transaction are crucial. A payer needs to know when a payment was authorised, approved, or completed For a receiver it is critical to know the status of a payment so that a decision can be made to release goods or acknowledge receipt to complete the transaction.

  For mobile remote payments, communications can take place utilising a variety of available technologies.

  It is highly likely that mobile network operators (MNO's) will provide the infrastructure for message transport.

- **COMPONENT 2: PAYMENT FACILITATION**

  The payment facilitation component assists in identifying the payment instruments used by the two parties to a payment transaction.

  Various models are available. The two parties may voluntarily disclose payment instrument details to each other; they may rely on some form of linkage (through a shared directory or some other facilitating asset) between mobile identifiers and payment instruments belonging to the transacting parties; or may deploy and / or comply with common mobile payment transaction standards to make payments to each other.

- **COMPONENT 3: FUNDS MOVEMENT**

  Actual transfer of value or movement of funds will take place using available payment networks. A majority of payments in any market are processed leveraging three widely used payment instruments:

  - Bank accounts – over ACH and other inter-bank payment systems
  - Payment cards (debit, credit, charge and others) – over global, regional, and local payment card networks
  - Stored value accounts (PayPal, Obopay etc.) – over proprietary networks that may or may not interface with banking and payment card networks.

Important Note: The guidance provided in this document stresses the importance of leveraging these existing payment instruments.

6. Initial Implementation Guidelines

For ease of planning and implementation, the following set of guidelines is provided for the initial stages of ecosystem development.

- Payment Instruments in Scope: There are three core payment instruments which are responsible for an overwhelming majority of global payments transactions. These are (a) Bank accounts (b) Payment cards such as credit, charge, debit or prepaid (c) stored value accounts such as PayPal. The ecosystem envisioned in this document takes these three instrument types into consideration.

  At this stage payments charged to a mobile operator bill or prepaid airtime account are excluded from the scope of this document.

- Default Payment Instrument (DPI): Some markets for commercial or legal reasons may require the customer to be able to set-up and select from multiple payment instruments. However, to achieve quick speed to market, it is expected that a customer will be able to set-up a single payment instrument as the default payment instrument, to send and receive funds. As services mature, there will be greater choice available to users in terms of the number and type of payment instruments (see next section on future guidelines).

  Please note that this guideline is included here for the sole purpose of facilitating quick implementations. Remote mobile payment ecosystems are free to select and implement services that allow the use of multiple payment instruments.

- Flexible User Interface (UI): The UI should be designed and developed by the payment provider and should serve as an area of competitive service differentiation.

- Communication Options: There are several technology options available to providers of mobile remote payments. This paper does not indicate or recommend in any form the type of communication protocol to be used.

- Payment Transactions Formats: Existing transaction formats should be deployed as far as practical. Ultimately as mobile remote payment volumes grow some form of common standards and payment transaction formats which preferably extend the existing formats may need to be agreed amongst stakeholders (see next section on future guidelines).

- Operational Rules and Regulations: The open ecosystem will leverage the operating rules and regulations of the payment networks that are used for mobile remote payments. For example, a mobile remote payment that uses a credit or debit card account will be subject to existing dispute management and chargeback rules of the payment scheme (such as Visa or MasterCard). Some payment instruments are preferred for certain use cases because of their key characteristics. For example, payment cards provide immediate payment guarantee to merchants so that goods and services can be released.

- Speed of Payment: The mobile ecosystem does not propose to develop a special purpose real time payment system or a new system that provides an immediate payment guarantee to the receiver. It is assumed that the payment guarantee procedures and payment settlement timeframes of the underlying payment network will govern when and how a mobile remote payment is completed. Depending upon the underlying payment system processes, a transaction could be settled in a matter of seconds (in case of near real time systems such as United Kingdom's Faster Payments service) or may take up to several days. It is important to note here that certain payment instruments are more suitable to specific payment categories (or use cases). For example, for person-to-business payments where goods or services are to be delivered, immediate settlement or a payment guarantee is usually preferred by the merchant so that delivery can be undertaken without risk. In such cases payment cards are more appropriate as these offer the merchant a guaranteed payment for the transaction.

  A market or a payment provider may provide additional value added services such as an immediate payment guarantee or near real time settlement. These would be considered in the competitive domain and beyond the scope of this paper.

7. Future Implementation Guidelines

As systems mature and mobile remote payment activity moves towards mass market adoption, additional features can be developed as necessary and in conjunction with customer demand.

- Multiple Payment Instruments: Customers will be able to select from a wide variety of payment instruments to send and receive funds using a mobile device. However, as stated earlier, this may be a day 1 requirement in some markets due to commercial or legal reasons

- Mobile Payment Transaction Formats: Standardisation will ensure that mobile remote payments are made in universally agreed transaction formats. This will also allow new players to enter the industry and offer new payment products and services using common and open standards

- Real / Near Real Time Payment: Developing additional infrastructure elements that will facilitate mobile remote payments to be completed in real or near real time. Such enhancements may be implemented for mobile payments only or for all electronic payments within a certain market as is the case with United Kingdom through the Faster Payments service.

Operating Models

1. OVERVIEW

This section identifies infrastructure components and technology elements that need to be in place for the development of a pragmatic and interoperable industry-wide approach to facilitate mobile remote payments.

2. MODEL 1: COMMON INFRASTRUCTURE MODEL

The model corresponds to Level 1 - existing interoperability. This model proposes the development of shared or common infrastructure (CI) that allows the routing of payment transactions based on the mobile identifier (MID). The mobile payment industry should aim at developing interoperable directory services that link a customer’s MID with the associated payment instrument registered by the customer. In a fully centralised environment (see centralised implementation scenario below), the directory service should support a query protocol to retrieve the payment instrument details using the MID of the parties registered for preparing payment instructions and submitting these for processing, clearing and settlement over, as far as applicable, existing payment systems such as ACH or card networks.

The retrieval and matching procedure in this model varies according to the implementation scenarios as explained below.

2.1 Implementation Scenarios

1. *Centralised*: A centralised implementation scenario refers to a system where mobile ecosystem stakeholders share a common infrastructure (CI) directory linking a payment instrument to a mobile identifier (MID)

2. *Distributed*: In this scenario, each payment provider (such as a bank) develops and maintains its own directory of registered customers. The centralised infrastructure only provides a link between bank identifier code (BIC) and the MID. Here, the confidential database containing payment instrument details is decentralised.

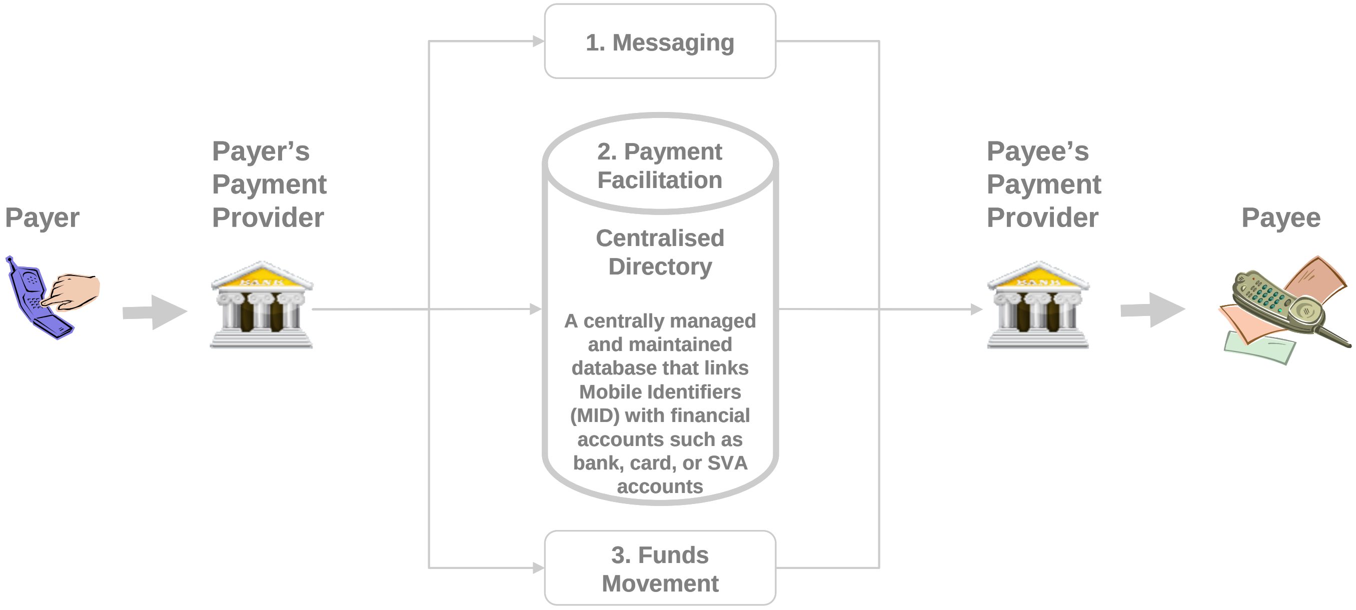
Common Infrastructure can also be expanded in terms of one or more international directory services linking national or regional directories that operate on a logic similar to the domain name service (DNS) on the internet for routing payment transactions across national or regional boundaries.

2.2 Centralised Implementation Scenario

This scenario envisages a database managed and maintained centrally. This could be set up and managed by an external entity, called the central infrastructure manager (CIM) on a commercial basis. The entity could be a payments infrastructure services provider operating on its own or on behalf of a competent authority such as a payment association or consortium of payment providers in a specific market.

The directory contains the MID's of customers of payment providers who have registered to use the mobile remote payment service and their default payment instrument (DPI) as supplied by those customers.

Initially it is suggested that the DPI should be a single payment instrument for the purposes of sending and receiving a mobile payment transaction or, alternatively, two instruments – one for sending and the another for receiving. At a later stage additional payment options may be added.


1. Messaging
Payer
Payer's Payment Provider
2. Payment Facilitation
Centralised Directory
A centrally managed and maintained database that links Mobile Identifiers (MID) with financial accounts such as bank, card, or SVA accounts
Payee's Payment Provider
Payee
3. Funds Movement

Advantages

Minimum investment for payment providers: In this model most of the upfront investment in terms of infrastructure development is undertaken by the CIM who also ensures that adequate procedures and processes are in place to ensure system availability, integrity, and security.

Speed of transaction: With centralised infrastructure, transactions can be routed and processed quickly. A single database will complete transactions and deal with exception items quicker than one that is distributed and maintained by several entities.

Efficiency: Updates to the central database will be applied to the entire directory infrastructure with very little management and maintenance to be undertaken by individual participating payment providers.

Time to market: The time necessary to implement the centralised infrastructure and connect payment providers is expected to be less than the time required if all payment providers develop their own systems that match MID's with payment instruments.

Disadvantages

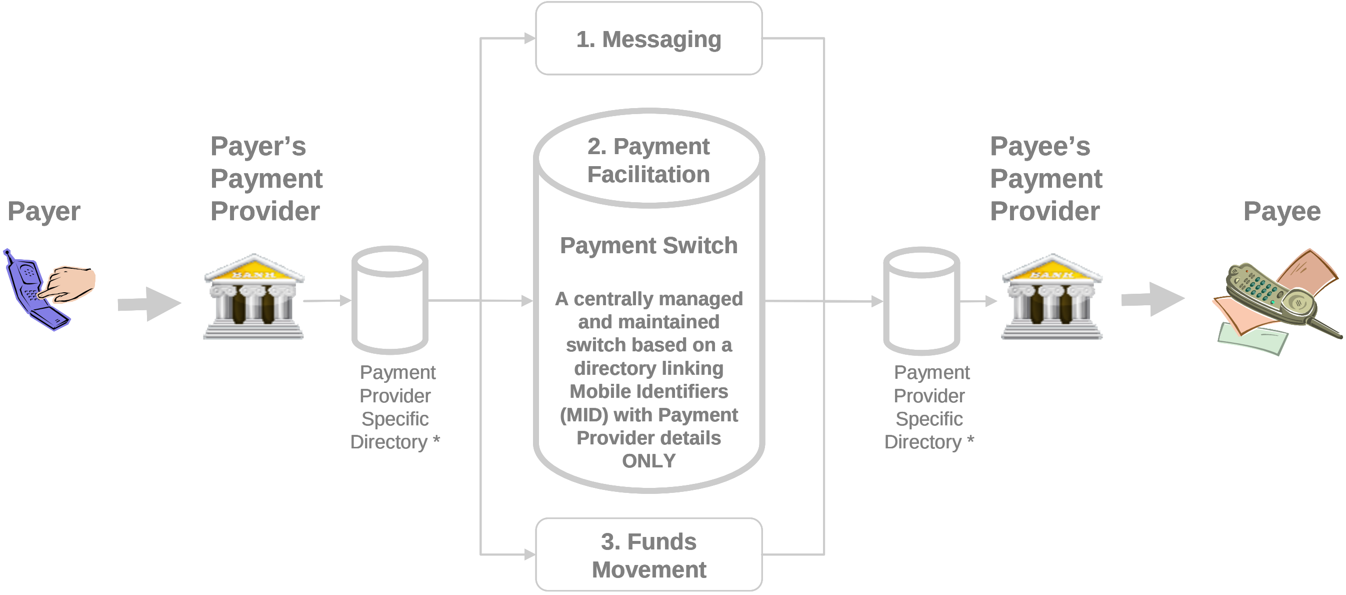
Security: The central database will store confidential customer financial information. This may create security related as well as consumer data protection issues in markets where there are strict privacy and data management regulations in force. It may also not be advisable in markets where storage of sensitive financial information at a central location and managed by a third party is considered a potential area of regulatory concern. The CIM will need to ensure suitable compliance with industry standards relating to stored bank account and payment card data.

Maintenance: Processes will have to be devised and operated to ensure that the central directory is kept up to date and available at all times. This will be a key challenge but may serve as a differentiating feature where there are competing CIM's in the marketplace. If customers change their MID, report their handsets stolen, or change payment providers, their details will need to be updated quickly and accurately so that the service remains effective.

2.3 Distributed Implementation Scenario

The distributed model provides a more decentralised approach with the central directory operating only as a “transaction switch”. The central directory in this case manages records that link MID’s with the name / detail of the customer’s payment provider and switches or routes payment transactions to the appropriate payment provider.

Each payment provider maintains and manages a separate directory database of MID’s and account data relating to their customers. Unlike the centralised model, confidential customer account data is kept confidentially by the customer’s payment provider and not by a separate entity.


1. Messaging
Payer
Payer’s Payment Provider
2. Payment Facilitation
Payment Switch
A centrally managed and maintained switch based on a directory linking Mobile Identifiers (MID) with Payment Provider details ONLY
Payee’s Payment Provider
Payee
Payment Provider Specific Directory *
Payment Provider Specific Directory *
3. Funds Movement

* Database that link Mobile Identifiers (MID) with financial accounts for the Payment Provider’s customers (maintained by the Payment Providers)

Advantages

Security and data protection: Payment providers will manage their own directories so that confidential information is retained by the them and not by a third party managing a centralised system. As such the CIM will only function as a payment transaction “switch”.

Control: Payment providers have control over their customer records in terms of how often these are updated and what steps are taken to remove, suspend, or modify records in case of de-registrations or terminations due to lost handsets.

Disadvantages

Additional investments: Payment providers in this scenario must set-up and maintain their own database directories and therefore this scenario requires upfront investment. Participating payment providers will need to implement supporting operational processes to ensure these records are updated in a timely manner. However it is expected that this level of customer data will already be available at many payment providers.

Efficiency: In a system where there are several hundred or several thousand payment providers participating, there are bound to be operational as well as other technical issues that will have to be addressed by individual entities. If these are not resolved in a timely and efficient manner, it is likely that this scenario may be relatively inefficient compared to the one above and result in a higher number of exception items.

Time to market: As every payment provider will need to develop their own confidential database linking MID's to payment instruments, the time required for an ecosystem to be implemented on a wide scale may be considerable.

3. Model 2: Intermediate Interoperability Model

This model relates to Level 2 - intermediate interoperability. The intermediate interoperability model is an extension of the model discussed above. In this model, the Common Infrastructure Manager (CIM) provides additional services to "bridge" the "interoperability gap" across different closed loop systems and across open systems that are currently not interoperable.

This model does not propose new transaction formats or make any standardisation recommendations. The actual framework or model design will depend on the CIM and may vary from market to market.

Examples (for illustrative purposes only):

- A customer with a Visa card making a payment to a cardholder / merchant with a MasterCard account
- A customer with, say a PayPal account, making a payment to a customer with say, an Obopay account

To keep the model simple without the need for developing new technology standards or infrastructure, one possible avenue is for the CIM to open and maintain accounts in each of the three party systems it aims to bridge. Under this arrangement, the CIM will open a control account with payment system A and a control account with payment system B where A and B are presently not interoperable payment systems. A customer of payment system A will be able to make a payment to a customer of payment system B by transferring funds to the CIM's control account with payment system A. The transaction will carry payment instructions along with beneficiary details. The CIM will in turn transfer the amount from its account to the beneficiary's account with payment system B. The CIM will internally make the necessary accounting entries to ensure completion of the transaction.

In this way, no additional infrastructure is required and the transaction can be completed using mechanisms within existing system capabilities. Additional technology elements, especially to accommodate payment messaging between the CIM, the payer, and the payee will have to be developed by the CIM.

Besides technology changes, it is possible that special negotiations and permissions from existing payment systems will be necessary to implement this model. In consequence, new operational procedures and regulations could appear as well.

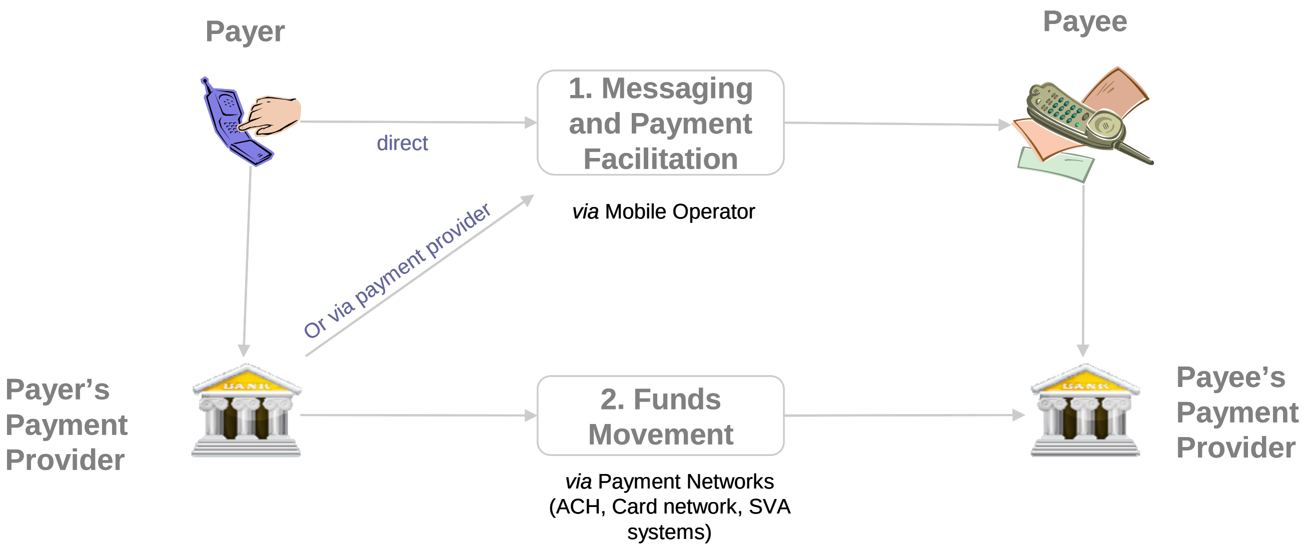
4. Model 3: Direct Interoperability Model

This model corresponds to Level 3 – direct interoperability. This model suggests direct payment messaging and facilitation between the payer and the payee without the need for any common infrastructure.

A key requirement of the model is that an open standardised mobile payment message format is agreed by all the stakeholders. The payment providers will then accordingly make system changes within their existing technology systems and develop suitable interfaces to process such payment messages.

A new interoperable messaging/transaction format will have to be developed or the existing messaging/transaction format will need to be enhanced in order to use the MID as payment instrument identifier for parties. Based on current thinking, the ISO20022 messaging standard for financial transactions in XML format supports multiple type of data fields for account identifiers and can be leveraged to include the MID as an account identifier. Older card payment messaging standard such as ISO8583 support the card number only as a payment instrument identifier and are not suitable for including MID as the payment instrument identifier.

The payer will use an application or an online site to prepare the payment instructions using an acceptable industry standard security arrangement such as Public Key Infrastructure (PKI) technology, and send the payment message to the receiver. The transaction format will need to be standardised and agreed. The receiver will forward the message to its payment provider, such as a bank or a card company, who will read the message and process it accordingly using existing payments infrastructure. For example, the payment instruction after receipt by the receiver's payment provider may be treated exactly as an ACH transaction for clearing, settlement, and completion.



There are a number of alternatives how the process may be implemented. In addition to the message sent by the payer directly to the payee, it may be possible for the payer to prepare and send a mobile message with instructions to initiate the transaction to its payment provider (see illustration above). This may be a better alternative from a security perspective. The payer's payment provider will then send the message directly to the receiver who will submit it to their payment provider.

Gap Analysis

1. OVERVIEW

A key point of consideration in envisioning a mobile remote payments ecosystem in this document is that such an ecosystem and all related operational models, as highlighted in previous sections, should ***leverage existing payment instruments and payment systems infrastructure networks*** used for facilitating electronic payments. This will ensure that mobile payments utilise existing investments and payment providers are able to design and launch mobile payment offerings in the most optimal timeframes possible. The ultimate industry objective is to ensure that payment systems are available that can handle mobile remote payments on a commercial scale in markets across the globe securely and efficiently.

The "gap" between today's payment systems and those envisioned in this document is discussed in this section. Additional elements and enhancements to the existing systems will need to be undertaken by some or all the stakeholders are discussed below.

2. COMMON INFRASTRUCTURE (CI)

Common infrastructure refers to models 1 and 2 (existing and intermediate interoperability) and consists of a directory service linking MID's to financial account data. Common Infrastructure Manager (CIM) entities will need to be set-up to manage / own the new assets.

To support such a directory, operational processes will have to be designed and implemented for customer registration, record retrieval, payment facilitation, and payment processing. Customer data is sensitive and, therefore, the design of the directory service should preserve the security and confidentiality of mobile ecosystems owners.

The sizing and the performance requirements for the registration and retrieval processes are critical where millions of customers might use the service across multiple countries.

The record data format should be based on international messaging standards for payments and enable unique mapping of the record data into instructions for payment messages (the ISO-200022 standard and the XML format/structure of the debtor/creditor account block are suggested as suitable for this purpose).

The retrieval protocol should be standardised, where possible in real-time, and efficient in terms of response time to a query. Standardised industry protocols for directory services such as LDAP could be used. Model 2 further requires the setting up of accounts with payment systems that are not currently interoperable. This would need to be supported by an enabling messaging and alert system to ensure automated communications of mobile remote payments.

It is intended that systems and processes already available for specific payment instruments to deal with customer service issues, dispute management, and exception item processing will continue to be used in a mobile environment. In other words, if a mobile remote payment is cleared and settled using an ACH payment system, the relevant rules and operating regulations of that system will also apply to the mobile transaction.

It is important to identify and monitor mobile transactions from traditional ones, in order to give all participants the possibility to control and develop specific actions to promote mobile payments. It is advisable to implement process such as transaction identifiers or flags to identify mobile payment transactions and develop reports to analyse transaction patterns etc.

Additionally, where certain payment providers such as banks, plan to integrate mobile payment systems within their mobile banking environments, they will require additional infrastructure development which is beyond the scope of this document.

3. Standardisation

The standardisation gap described here refers to Model 3 which facilitates direct messaging between two parties to a payment transaction – the payer and the payee using agreed and standardised message formats. Some form of client or server resident application or protocol will be required to prepare an encrypted payment message that will be sent to the receiver directly.

For this model to be implemented, agreement across industry stakeholders on common standards and transaction formats will be necessary. These include the standardisation of the following key transaction components. Please note this list is not exhaustive:

- Payment initiation or request message preparation
- Security and encryption formats to be used
- Transaction format that includes both the payment identifier and the mobile identifier
- Procedures and processes for processing or forwarding of encrypted messages to the payment provider for processing
- Procedures and processes for handling incomplete or failed transactions
- System of alerts and notifications for both the payer and payee

The effort towards standardisation, while necessary and optimal, generally requires significant time and effort for agreement and acceptance especially where standardisation is necessary on a global scale.

While detailed implementations will be solution specific, minimum standards will be required to be agreed and complied with.

Core Processes

1. Overview

Certain processes will have to be developed or enhanced by providers of mobile remote payments. These include, but are not limited to the following:

- Registration & set-up
- Send payments
- Request payments
- Customer support

Each process above is explained below at a high level together with guiding principles and, where applicable, suggested process steps. Process activities are presented at a generic level and individual market implementations may vary significantly from each other.

2. Registration & Set-up

Registration and set-up activities discussed in this section are prevalent primarily for models involving a common infrastructure. Where minimal or no common infrastructure is envisioned, as in model 3, different registration options will be applicable.

2.1 Description

Payment providers (PP's) must establish that a customer owns or has the appropriate rights to use the financial instruments to be used to either make or receive a mobile payment.

Customers should be able to register with multiple PP's to make payments. It is expected that customers will be automatically enabled to send and receive payments on initial registration. Additionally, nominating a default beneficiary may help to simplify and speed the payment process.

The customer's PP (sponsoring PP) should establish that the customer has correctly registered the MID of the mobile phone to be used to receive a payment. The customer's MID can be registered automatically from information sent by the MNO, when applicable.

Customer registration may be undertaken directly by a PP, or by an agent acting on their behalf.

The service requires that PP's obtain all the information from customers required in order to fully populate an entry on to the customer information (CI) database.

- Customer Name/Nickname
- Mobile number(s). Customers may register their mobile phone numbers to the Service using a full MID or a national-level number. However the number will always be stored on the CI database as a full MID
- Sponsoring PP name
- Payment instrument details
- Account name of the payment instrument, if applicable
- Customer identity code (allocated by the customer's sponsoring PP)

Customers may register in one of two modes:

- to receive payments only
- to send and receive payments

PP's undertake to populate the CI database with the details of every customer that they register to use the Service, whether or not they additionally operate a local database system.

2.2 Key Steps

(a) Sponsoring PP gathers data from customer wishing to register for the service. The sponsoring PP may enable a number of channels including, online banking, telephony and branch to collect data

(b) Sponsoring PP establishes that the customer has possession of the mobile phone to be used and is responsible for all KYC and regulatory checks

(c) Sponsoring PP sends data to CI database in real-time

(d) CI database undertakes validity check – e.g. is the mobile phone number already registered?

(e) If so, CI database advises Sponsoring PP. The PP may then reject entry and request new details, or ask customer to confirm that they wish to change existing associations or add a new association to another PP

(f) If not, CI database adds new entry and advises Sponsoring PP

(g) Sponsoring PP advises customer as appropriate and where applicable, sends customer authentication passcode via a secure delivery channel. The passcode can either be defined by the customer during the registration phase or be automatically generated by the sponsoring PP.

(h) Customer activates the mobile payment service using the supplied credentials.

2.3 Management and Maintenance

This section contains the process for updating customer records.

General principles

(a) All changes to CI database records take effect in real time
(b) Old records are retained for audit trail purposes
(c) All changes are authorised by the authenticated user

Option 1. Customer remains with original sponsoring PP

In cases where the customer wishes to amend details of their record, but otherwise the account remains with the original Sponsoring PP, the following process is suggested:

(a) Customer advises sponsoring PP of change of data
(b) Sponsoring PP establishes that the customer has possession of the mobile phone to be used
(c) Sponsoring PP sends data to CI database in real time
(d) CI database undertakes data validity checks
(e) If CI database rejects entry, Sponsoring PP is advised
(f) If CI database accepts entry, entry is updated [in real time] and Sponsoring PP is advised
(g) Sponsoring PP advises customer accordingly.

Option 2. Customer moves record to a new PP

In cases where the customer is moving the association for their mobile phone number from one PP to another, the PP to which the association is being moved to (the "New PP") takes precedence over the original sponsoring PP (the "Old PP"), as follows:

(a) Customer advises New PP that they wish to associate their mobile phone with an account at the New PP. New PP must fulfil all the requirements associated with an initial registration.
(b) New PP sends data to CI database in real time
(c) CI database identifies that a change in sponsoring PP is taking place and informs the Old PP
(d) CI database undertakes data validity checks
(e) If CI database rejects entry, New PP is advised
(f) If CI database accepts entry, entry is updated in real time, and New PP is advised
(g) New PP advises customer accordingly.

The key requirement is that changes in association from one PP to another should appear smooth and straightforward to the customer.

2.4 De-registration

This section contains the requirements and process for permanently removing customers from the Service.

General principles:

(a) Customers may choose to withdraw from the service
(b) PP's may de-register customers from the service, for example in cases of customer inactivity or misuse of service (or any illegal actions)
(c) Sponsoring PP's may wish to consider deactivating dormant / unused entries in order to mitigate the possibility that an unused mobile phone number has been re-allocated to another mobile phone customer by the Mobile Network Operator. In these cases Sponsoring PP's are encouraged to attempt to contact the customer prior to deactivation.
(d) When entries become dormant, the record is flagged as such on the CI database, and the sponsoring PP undertakes to inform the customer
(e) Deactivated records will be retained for audit purposes.
(f) Account deactivations will be reflected on the CI database in real time

3. Send Payments

3.1 Payment transaction with CI

Customers who have completed the registration process as defined in the discussion above are ready to make mobile remote payments. This section describes a generic payment process approach, individual service and market offers may differ as necessary.

As indicated earlier in this paper, when a payer makes a remote mobile payment to a known payee, the main identifier of the payee is a unique mobile ID which is typically the payee's phone number (MID) due to obvious usability benefits over other types of mobile IDs or account numbers.

The payment is made from payer's chosen payment instrument, which can be a bank account, credit/debit card or a stored value account (SVA). Payee's payment instrument can be any type, but the payer does not need to know what type payment instrument(s) is held by the payee.

When a customer starts a payment process, he/she will need the following:

- Payee's mobile identifier (MID).
- A connected mobile device that is registered to make payments with the payer's PP.
- A valid and authorised payment account.
- Sufficient amount of credit or value in the payment account to make the requested payment.

- Required credentials for authentication (e.g. PIN code, biometric ID, token)

Suggested process steps:

Step #	Description	Mandatory/ Optional
1	When starting a payment transaction the user might have configured his mobile device to require an unlock code to access the payment application. This step is not needed if payment is initiated by e.g. native SMS client of the mobile device. The unlock code can be validated either online or offline, depending on the underlying security solution.	Optional
2	Payer enters the minimum amount of payment information for payment initiation. This information includes (but might not be limited to): - Payee mobile identifier (MID) - Payment amount - Payment instrument to be debited (Optional) - Payment due date (immediate or future dated) - Message (optional)	Mandatory
3	Payer authorises the transaction with his/her credentials (e.g. PIN code). Actual authentication method is dependent on the underlying security solution. In practice this step can be combined with step 2 of this process if required for better usability.	Mandatory
4	Payment information and authentication information are sent to the payer's PP. Technical bearer is solution specific. It should be noted that sufficient level of encryption should be used when transmitting payment information from mobile device to the PP. Detailed encryption algorithm strength, non-repudiation and integrity requirements are solution specific.	Mandatory
5	Payer PP validates and authenticates the incoming request. Incoming payment request should be validated to have correct - Credentials (authentication) - Mandatory minimum payment information Additionally the payer PP can choose to validate whether the customer's payment instrument has sufficient credit to facilitate the transaction amount at this stage. Optionally the payment details can be validated only when executing the payment towards the payment network. It is also optional to validate limit amounts, accumulate amounts or number or payments, defined by the customer, the PP and/or regulations.	Mandatory

Step #	Description	Mandatory/ Optional
6	If payment is valid, process is continued in step 8. If not, process is terminated at step 7.	Mandatory
7	Payment transaction is terminated. User is informed of the reason for failing the initial validation.	Mandatory
8	Valid payment processing will start by requesting payee payment instrument information from the directory service (CIM).	Mandatory
9	CI checks whether the payee has registered his/her account instrument with the service. In case of a distributed scenario, this information might reside in another directory or region. It is the responsibility of the CI to take the necessary steps to check the registration status of any forwarded payee mobile identifier, regardless of payee's home directory location. If payee is registered (in any of the directories), process continues in step 11. If payee is not registered or his account instrument is not active, the process is terminated in step 10.	Mandatory
10	Payment process is terminated. Payer is informed of failed transaction and payee is optionally contacted to register for the service or activate his account instrument. It should be noted that a viral distribution process can be implemented in this stage. This would keep the payment process running, reserve the funds from payer's account and credit the payee account once the payee has registered for the service. Details of this process are not described in this white paper.	Mandatory
11	Payee's mobile identifier is mapped to a payment instrument routing information and a nickname.	Mandatory
12	Payer is asked for a payment confirmation based on given payment information and nickname received in step 11. Payer will not see the payee's full name or payment instrument information to avoid privacy issues.	Mandatory
13	If payer rejects the payment confirmation request, the process ends.	Mandatory
14	If payer approves the payment confirmation request, the payer PP starts the payment process. This process is dependent on what type of payment instrument is used on both sides.	Mandatory
15	If supported by the system, a real-time payment notification can be generated to notify the payee of incoming payment. Real-time payment notification is typically not needed if the chosen payment method and network supports real-time or near-real-time transactions (e.g. UK Faster Payments).	Optional

Step #	Description	Mandatory/ Optional
16	The optional real-time payment notification is generated by the Directory and sent to payee PP.	Optional
17	Payee PP can choose whether to route the notification to the payee or not. Typically this would be a value-added service for customer's who have requested to opt-in for payment notifications.	Optional
18	An optional notification can be sent to the payee on incoming payments. Notification can contain at least amount and payer information. If supported by the payment instrument used and the payment network, an estimated time for crediting the incoming funds should also be provided.	Optional
19	The payment process is executed by the rules and processes set by the used payment instruments. Details of this process by payment instrument are not in the scope of this white paper.	Mandatory
20	Once the payment process is complete, the payee's account is credited with the appropriate amount. Note that the amount credited may differ from the initial payment amount depending on the underlying business- and revenue sharing model.	Mandatory
21	If opted in by the payee, a notification can be sent to the payee once the funds are credited.	Optional
22	If supported by the system, a payment confirmation can be sent through to the payer PP once funds are credited to the payee payment instrument.	Optional
23	If opted in and supported by the system, a confirmation of completed payment can be shown to the payer.	Optional

3.2 Payment transaction without CI

Alternatively a payment transaction can be executed with a model that does not use a CI service for mapping mobile identifiers to payment instruments. In this model messages between payer / payer's PP and payee are sent through the operator network directly to the receiving mobile device based on the mobile identifier (MID).

This model requires that the payment instrument identifier or payer bank identifier (BIC) is sent with each payment message. In practice this sets limitations to the messaging layer, as clear text protocols like plain SMS using native messaging clients can not be used without harming the usability of the service.

To reemphasise, multiple implementation scenarios are possible. The following is suggested for guidance only.

Main characteristics of the payment transaction are similar to the transaction with CI.

Suggested process steps:

Step #	Description	Mandatory/ Optional
1	When starting a payment transaction the user may have configured his mobile device to require an unlock code to access the payment application. This step is not needed if payment is initiated by e.g. native SMS client of the mobile device. The unlock code can be validated either online or offline, depending on the underlying security solution.	Optional
2	Payer enters the minimum amount of payment information for payment initiation. This information includes (but might not be limited to): - Payee mobile identifier (MID) - Payment amount - Payment instrument to be debited (Optional) - Payment due date (immediate or future dated) - Message (optional)	Mandatory
3	Payer authorises the transaction with his/her credentials (e.g. PIN code). Actual authentication method is dependent on the underlying security solution. In practice this step can be combined with step 2 of this process if required for better usability.	Mandatory
4	Payment information and authentication information are sent to the payer's PP. Technical bearer is solution specific. It should be noted that sufficient level of encryption should be used when transmitting payment information from mobile device to the PP. Detailed encryption algorithm strength, non-repudiation and integrity requirements are solution specific.	Mandatory
5	Payer PP validates and authenticates the incoming request. Incoming payment request should be validated to have correct - Credentials (authentication) - Mandatory minimum payment information Additionally the payer PP can choose to validate whether the customer's payment instrument has enough credit to facilitate the transaction amount at this stage. Optionally the payment details can be validated only when executing the payment towards the payment network.	Mandatory
6	Payment is validated and the payer PP sets up a payment instruction indicating that a payment is due from the payer's account. If payment is valid, the process is continued in step 8. If not, process is terminated at step 7.	Mandatory

Step #	Description	Mandatory/ Optional
7	Payment transaction is terminated. User is informed of the reason for failing the initial validation.	Mandatory
8	Payment message containing at minimum: - Payment amount - Payer mobile identifier - Payer bank identifier (BIC) is sent through the operator network to the payee's mobile device using the payee mobile identifier (MID).	Mandatory
9	Payee receives the payment message to his/her mobile device. After reviewing the received information, payment message is forwarded to the payee PP.	Mandatory
10	Payee PP validates whether the payee is subscribed to the mobile payment service or not and if his account instrument is active. If payee is mobile enabled, process continues in step 12. If payee is not mobile enabled, process continues in step 11.	Mandatory
11	Payee receives a message about not being enabled to receive mobile payments. Optionally, registration process is initiated to enrol the customer to mobile service (defined separately).	Mandatory
12	Payee PP constructs a payment request using payment amount and payer mobile identifier, and sends it to payer PP based on the BIC received in the original payment message.	Mandatory
13	Payment network processes the payment request and routes it to the payer PP based on BIC.	Mandatory
14	Payer PP receives the payment request and matches it to the payment instruction set up in step 6. If payment request is valid, payment confirmation request is sent to the payer.	Mandatory
15	Payer receives the payment confirmation request. If payer rejects the confirmation request, payment process is continued in step 16. If payer accepts the confirmation request, payment process is continued in step 17.	Mandatory
16	Process is terminated and payee is notified of cancelled payment.	Mandatory
17	Payment transaction is initiated and payer account is debited.	Mandatory
18	The payment process is executed by the rules and processes set by the used payment instruments. Details of this process by payment instrument are not	Mandatory

Step #	Description	Mandatory/ Optional
	in the scope of this white paper.	
19	Payment is received and payee's account is credited.	Mandatory
20	If opted in, payee is notified of received funds.	Optional

4. Request Payment

4.1 Payment Request with CI

Customers who have completed the registration process as defined in the discussion above are ready to request mobile remote payments. A payment request is a step preceding the actual payment process.

As indicated earlier in this document, when a payer approves / makes a remote mobile payment request to a payee, the main identifier of the payee is a unique mobile ID (MID), which is typically the payee's phone number due to obvious usability benefits over other types of mobile IDs or account numbers.

The payment is made from payer's chosen payment instrument, which can be a bank account, credit/debit card or a stored value account (SVA). Payee's payment instrument can be any of any type, but the payer does not need to know what type payment instrument(s) is held by the payee.

When payee customer starts/initiates a payment request, he/she will need the following:

- Payer's mobile identifier (MID)
- Payee's (own) mobile identifier that will be sent within the message
- Payee's BIC code (e.g. Bank Identification Code – in case of bank account to account payments) – where applicable
- A valid and authorised payment account

Payer will need the following to finish the payment process:

- Sufficient amount of credit or value in the payer's payment account to authorise the payment request
- Required credentials for authenticating the payment (e.g. PIN code, biometric ID, token)

Process steps:

Step #	Description	Mandatory/ Optional

1	When starting a payment request the payee might have configured his mobile device to require an unlock code to access the payment application. This step is not needed if payment is initiated by e.g. native SMS client of the mobile device. The unlock code can be validated either online or offline, depending on the underlying security solution.	Optional
2	Payee enters the minimum amount of payment request information for payment request initiation. This information includes (but might not be limited to): - Payee mobile identifier (MID) - Payer mobile identifier (MID) - Payment amount - Payee's BIC code (e.g. Bank Identification Code)- where applicable - Payment instrument to be credited (Optional) - Payment due date (immediate or future dated) - Message (optional)	Mandatory
3	Payee's PP validates and authorises the payment request i.e. validates the payee and checks the relevant payment request information that the message contains all the right fields or is in the right format.	Mandatory
4	Payee's PP directs the payment request to the CIM	Mandatory
5	CIM routes the payment request to Payer's PP based on mobile identifier of the payer.	Mandatory
6	Payer's PP receives the payment request and validates the payment request.	Mandatory
7	Payer approves / authorises the payment. Payer authorises the transaction with his/her credentials (e.g. PIN code). Actual authentication method is dependent on the underlying security solution.	Mandatory
8	See Payment process	Mandatory

4.2 Payment Request without CI

This section describes a generic payment request process in scope of mobile remote payment definition when there is not a common nominator i.e. CI within the process either centralised or de-centralised. The message structure should enable the minimum amount of information for the routing purposes. Payment message format should be standardised and applied by both of the PP's (Payee's PP and Payer's PP).

When a payer approves / makes a remote mobile payment to a known payee, the main identifier of the payee is a unique mobile ID which is typically the payee's phone number (MID) due to obvious usability benefits over other types of mobile IDs or account numbers.

The payment is made from payer's chosen payment instrument, which can be a bank account, credit/debit card or a stored value account (SVA). Payee's payment instrument can be of any type, but the payer does not need to know what type payment instrument(s) is held by the payee.

When payee customer starts/initiates a payment request, he/she will need the following:

- Payer's mobile identifier (MID).
- Payee's (own) mobile identifier that will be sent within the message
- Payee's BIC code (e.g. Bank Identification Code – where relevant)
- A connected mobile device that is registered to make payment requests with the payee's PP.

Payer will need the following to finish the payment process:

- A valid and authorised payment account.
- Sufficient amount of credit or value in the payment account to authorise the payment request.
- Required credentials for authentication (e.g. PIN code, biometric ID, token)

Process steps:

Step #	Description	Mandatory/ Optional
1	When starting a payment request the payee might have configured his mobile device to require an unlock code to access the payment application. This step is not needed if payment is initiated by e.g. native SMS client of the mobile device. The unlock code can be validated either online or offline, depending on the underlying security solution.	Optional
2	Payee enters the minimum amount of payment request information for payment request initiation. This information includes (but might not be limited to): - Payee mobile identifier (MID) - Payer mobile identifier (MID) - Payment amount - Payee's BIC code (e.g. Bank Identification Code) - Payment instrument to be credited - Payment due date (immediate or future dated) - Message (optional)	Mandatory
3	Payer approves / authorises the payment. Payer authorises the transaction with his/her credentials (e.g. PIN code).	Mandatory

	Actual authentication method is dependent on the underlying security solution.	
4	Payee's PP receives the payment approval / authorisation from the payer and validates the payment approval (including message structure, user etc).	Mandatory
5	See Payment process	Mandatory

5. Customer Service

5.1 Description

Customer support covers a range of different use scenarios. In general, support processes will vary, depending on the specific customer service needs. The payment provider is responsible towards its customers for all aspects of the service delivery (messaging, databases and funds transfer) and serves as the customer's primary point of contact.

In some cases the payment provider will direct the customer to contact the merchant, handset provider, or the mobile operator, as the case maybe. In each case, however, the relationship between the customer and the payment provider will be governed by the contract between the two parties.

5.2 Illustrative service scenarios

Selected service scenarios are listed for illustrative purposes only. This list is not meant to be exhaustive.

Service discovery

- Customer is unable to locate service registration information
- Customer is unable to locate service at Merchant

Service registration and activation

- Customer is not able to enter sufficient information to fulfil registration entry
- Customer receives error message stating MID entry exists
- Customer receives error message after registration entry
- Customer doesn't receive activation code
- Customer unable to activate DPI entry

End/change service

- Customer unable to end service
- Customer unable to change service

  - Change within existing payment provider
  - Change to new payment provider

Other

- Purchase ok, nothing happens after acquiring service initiated payment confirmation
- Payment confirmation ok, nothing happens at Merchant
- Payment initiation sent, confirmation not received
- Payment initiation & confirmation ok, nothing happens with payee
- Chargebacks

6. Areas Beyond Scope

6.1 Risk Management

Risk management is a primary consideration for development of any payment system. This document does not propose any specific guidelines on technology related risk mitigation matters such as for encryption or message transport.

For the purpose of development of operationally viable mobile remote ecosystems, it is essential that all aspects of risk are considered, evaluated, and taken into account when designing technology infrastructure or the supporting operational processes.

A detailed discussion on risk management is beyond the scope of this document.

6.2 Regulatory Compliance

Regulation and compliance are highly critical elements to be considered at the entity as well as national levels. Payment providers must ensure that the applicable regulatory requirements – such as KYC upon registration – are adequately complied with and that good practices of regular interface and continuing dialogue with regulators should be observed on all levels.

Mobey Forum understands that regulatory environments vary significantly across markets. As such regulatory perspectives are beyond the scope of this paper.

Appendix – Common Requirements

1. Overview

The ideas, options, and potential scenarios highlighted in this document are not meant to be prescriptive but provide indicative guidance to the various stakeholders in developing commercially viable mobile remote payment services.

The providers of mobile remote payment services will need to assess the needs of their customers in order to identify the business requirements for developing suitable products and services. There are, however, a set of general requirements for a service that can be considered “common” to all stakeholders.

Some requirements are necessary at start-up and many are needed as ongoing operational demands, in other cases there may be external requirements stemming from outside the immediate stakeholder environment. This is illustrated in the table in this section.

These are based on a set of universally accepted principles that must be considered and followed for the development of commercially viable and successful mobile payments.

Key Principles:

A mobile remote payment service offering must have:

- *A viable business case*: A remote payment offering, like any other, should have a positive business case where the benefits accrue directly (such as fees and commissions) or indirectly (such as strategic differentiation, reduction in churn, cross selling opportunities) to the service provider. On an overall industry basis, mobile payment ecosystems must provide the opportunity to generate acceptable and sustainable returns for all entities.
- *Clear liability protection*: Service provider should clearly communicate to payment service users the rules and regulations governing potential liabilities for events such as transaction failure, identity theft, fraud loss etc.
- *Security*: Generally accepted security standards must be followed under all circumstances. Risk management processes should be in place to ensure system integrity.
- *Usability / ease of use*: Mobile remote payment service offerings should be designed to deliver a positive customer experience.
- *Availability*: Service should be reliable and available with minimum acceptable downtime for maintenance and related matters.

2. Common Requirements

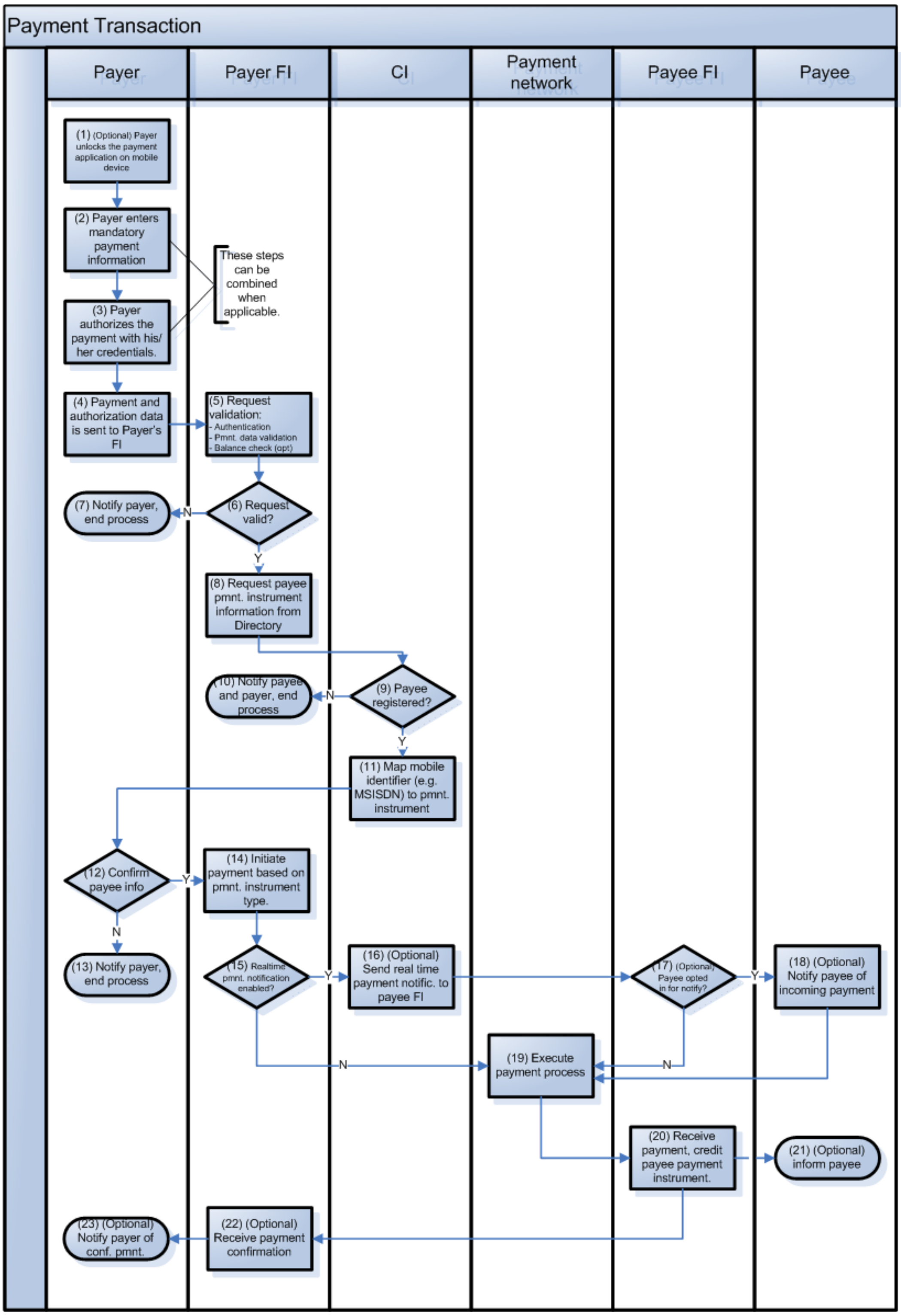
Based on the principles listed above, the minimum requirements that are common to all stakeholders are listed below:

Requirement	Initial	Operational	External
The instrument that holds monetary value in the system can be: • Credit / Debit card, Prepaid cards. • Bank account • Proprietary stored value account *(Frequent flyer club, PayPal etc.)*	X	X	
Payment network used to relay payment information can be: • Existing card networks *(Visa, MasterCard etc.)* • Existing clearing and payment networks (*SWIFT, Faster Payment etc.)* • Proprietary closed network *(PayPal, Western Union etc.)*	X	X	
Speed of payment to be based on capabilities of underlying payment instrument. For messaging, it's important to realise that using strong encryption will introduce a short delay of a few seconds that most likely needs to be communicated to the consumer.		X	
Customer enrolment process should be flexible and adapted to suit the type of service being offered.		X	
Remote mobile payment solutions must comply with all relevant payment regulations such as anti-money laundering and KYC.			X
Service pricing options must be transparent to all stakeholders in both domestic and international usage. Lack of transparency (such as MNO roaming charges in some cases) to the consumer may seriously impact the business case.		X	
Payment application must be available to the mass market and preferably not available only for selected handsets		X	
Liability / Risk framework must be clear for all parties involved with the service.		X	

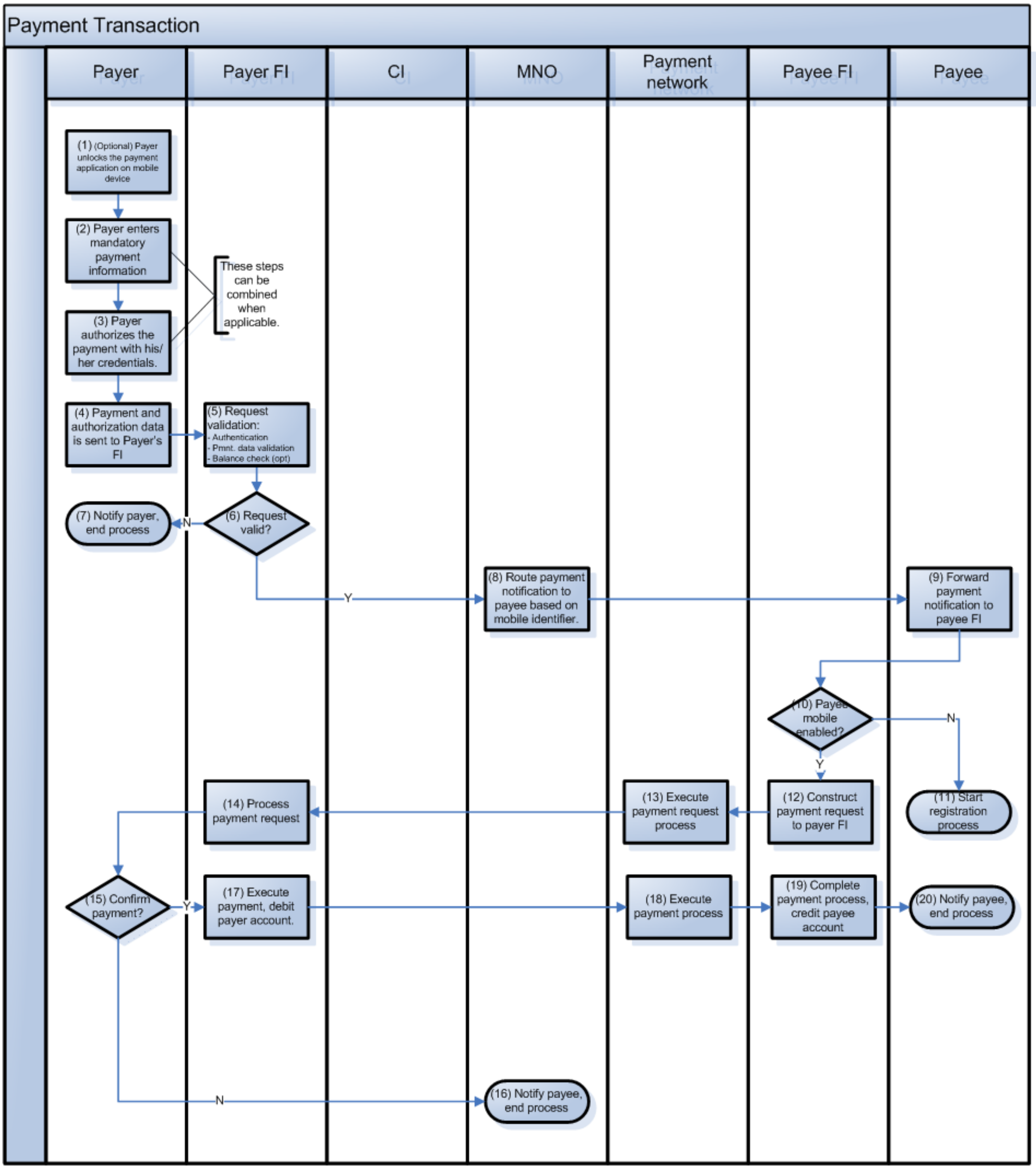
Appendix – Process Flowcharts

Process Flow Charts – Illustrative

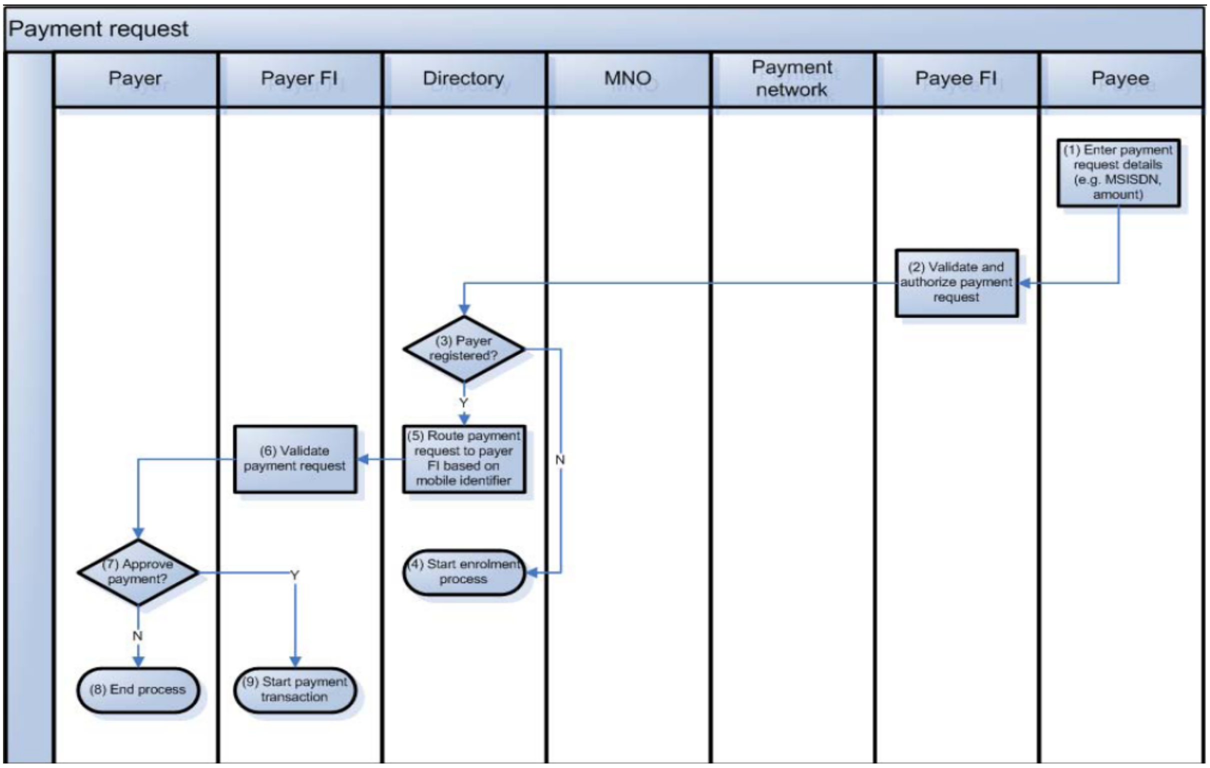
1. Send Payment With Central Infrastructure (ci) – Model 1


Payment Transaction
Payer
Payer FI
CI
Payment network
Payee FI
Payee
(1) (Optional) Payer unlocks the payment application on mobile device
(2) Payer enters mandatory payment information
(3) Payer authorizes the payment with his/ her credentials.
These steps can be combined when applicable.
(4) Payment and authorization data is sent to Payer's FI
(5) Request validation: - Authentication - Pmnt. data validation - Balance check (opt)
(6) Request valid?
N
(7) Notify payer, end process
Y
(8) Request payee pmnt. instrument information from Directory
(9) Payee registered?
N
(10) Notify payee and payer, end process
Y
(11) Map mobile identifier (e.g. MSISDN) to pmnt. instrument
(12) Confirm payee info
N
(13) Notify payer, end process
Y
(14) Initiate payment based on pmnt. instrument type.
(15) Realtime pmnt. notification enabled?
Y
(16) (Optional) Send real time payment notific. to payee FI
(17) (Optional) Payee opted in for notify?
Y
(18) (Optional) Notify payee of incoming payment
N
N
(19) Execute payment process
(20) Receive payment, credit payee payment instrument.
(21) (Optional) inform payee
(22) (Optional) Receive payment confirmation
(23) (Optional) Notify payer of conf. pmnt.

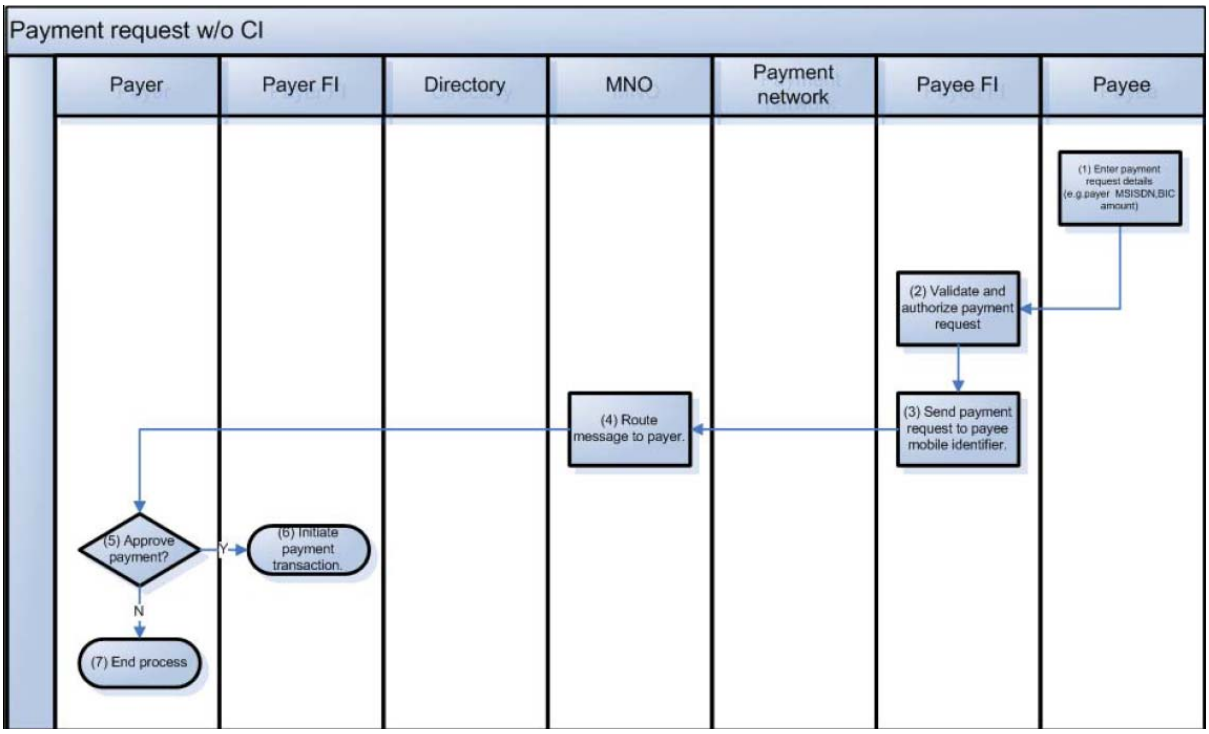
2. SEND PAYMENT WITHOUT CI - MODELS 2 & 3


Payment Transaction
Payer
Payer FI
CI
MNO
Payment network
Payee FI
Payee
(1) (Optional) Payer unlocks the payment application on mobile device
(2) Payer enters mandatory payment information
(3) Payer authorizes the payment with his/ her credentials.
These steps can be combined when applicable.
(4) Payment and authorization data is sent to Payer's FI
(5) Request validation:
- Authentication
- Pmnt. data validation
- Balance check (opt)
(6) Request valid?
N
(7) Notify payer, end process
Y
(8) Route payment notification to payee based on mobile identifier.
(9) Forward payment notification to payee FI
(10) Payee mobile enabled?
N
(11) Start registration process
Y
(12) Construct payment request to payer FI
(13) Execute payment request process
(14) Process payment request
(15) Confirm payment?
Y
(17) Execute payment, debit payer account.
(18) Execute payment process
(19) Complete payment process, credit payee account
(20) Notify payee, end process
N
(16) Notify payee, end process

3. Request Payment With CI[6] – Model 1


Payment request
Payer
Payer FI
Directory
MNO
Payment network
Payee FI
Payee
(1) Enter payment request details (e.g. MSISDN, amount)
(2) Validate and authorize payment request
(3) Payer registered?
Y
N
(4) Start enrolment process
(5) Route payment request to payer FI based on mobile identifier
(6) Validate payment request
(7) Approve payment?
Y
N
(8) End process
(9) Start payment transaction

4. Request Payment Without CI – Models 2 & 3


Payment request w/o CI
Payer
Payer FI
Directory
MNO
Payment network
Payee FI
Payee
(1) Enter payment request details (e.g.payer MSISDN,BIC amount)
(2) Validate and authorize payment request
(3) Send payment request to payee mobile identifier.
(4) Route message to payer.
(5) Approve payment?
Y
(6) Initiate payment transaction.
N
(7) End process

[6] Referred to as "Directory" service in the flowcharts

Glossary

Term	***Description***	***Source***
3G	Third generation (3G) is the generic term used for the next generation of mobile communications systems. These have been created to support the effective delivery of a range of multimedia services. In addition, they provide more efficient systems for the over-the-air transmission of existing services, such as voice, text and data that are available today.	GSMA
ACH - Automated Clearing House	Automated Clearing House (ACH) is an electronic network for financial transactions. ACH processes large volumes of credit and debit transactions usually in batches. ACH credit transfers include direct deposit payroll and vendor payments. ACH direct debit transfers include consumer payments on insurance premiums, mortgage loans, and other kinds of bills.	Wikipedia
Authentication, end-user	There are three universally recognised factors for authenticating individuals: ‘Something you know’, such as a password, PIN or an out of wallet response. ‘Something you have’, such as a mobile phone, credit card or hardware security token. ‘Something you are’, such as a fingerprint, a retinal scan, or other biometric. A system is said to leverage Two-factor authentication (T-FA) (or dual factor authentication) when it requires at least two of the authentication form factors mentioned above. This contrasts with traditional password authentication, which requires only one authentication factor (such as knowledge of a password) in order to gain access to a system.	Wikipedia

Term	***Description***	***Source***
Authentication, Two-way	Mutual authentication or two-way authentication refers to two parties authenticating each other suitably. In technology terms, it refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity. Typically, this is done for a client process and a server process without user interaction. Mutual SSL provides the same things as SSL, with the addition of authentication and non-repudiation of the client authentication, using digital signatures. However, due to issues with complexity, cost, logistics, and effectiveness, most web applications are designed so they do not require client-side certificates. This creates an opening for a man-in-the-middle attack, in particular for online banking. As the Financial Services Technology Consortium put it in its January 2005 report, "Better institution-to-customer authentication would prevent attackers from successfully impersonating financial institutions to steal customers' account credentials; and better customer-to-institution authentication would prevent attackers from successfully impersonating customers to financial institutions in order to perpetrate fraud."	Wikipedia
BIC	Bank Identifier Code – An 8 or 11 character ISO code assigned by SWIFT and used to identify a financial institution in financial transactions.	SWIFT
BIN	Bank Identification Number, A code that uniquely identifies a bank, and possibly a branch as part of a financial institution.	SWIFT

Term	*Description*	*Source*
Central Infrastructure Manager (CIM)	Central Infrastructure Manager (CIM): In certain situations where a centralised directory service is used to enable mobile remote payments, the directory provider will link a customer's (a) mobile identifier or MID (normally the mobile phone number) and (b) their default payment instrument such as a credit card or a bank account. This will enable the mobile identifier to act as a proxy or pseudonym for the card or account number to facilitate payments over existing networks. This role can also be fully or partially undertaken by a third party technology provider or a mobile operator. The CIM can also offer and operate customer authentication services.	Mobey Forum
IBAN	International Bank Account Number – An expanded version of the Basic Bank Account Number (BBAN) used internationally to uniquely identify the account of the customer at a financial institution.	SWIFT
Lightweight Directory Access Protocol (LDAP)	The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying data using directory services running over TCP/IP (Transmission Control Protocol / Internet Protocol)	Wikipedia

Term	***Description***	***Source***
Mobile Commerce	Mobile Commerce (also known as M-Commerce, mCommerce or U-Commerce, owing to the ubiquitous nature of its services) is the ability to conduct commerce, using a mobile device - e.g., a mobile phone (or cell phone), a PDA, a smart phone while on the move. Mobile commerce is currently mainly used for the sale of mobile phone ring-tones and games, although as 3G/UMTS services roll-out it is increasingly used to enable payment for location-based services such as maps, as well as video and audio content, including full length music tracks. Other services include the sending of information such as football scores via SMS. Currently the main payment methods used to enable mobile commerce are: • premium-rate calling numbers, • charging to the mobile telephone user's bill or • Deducting from their calling credit, either directly or via reverse-charged SMS.	Wikipedia
Mobile Ecosystem	A market environment in which the stakeholders achieve a good balance between competitive freedom and strategic dependencies, assuring easy uptake of mobile financial services by end-users and merchants through interoperability and freedom of choice.	Mobey Forum
Mobile Identifier (MID)	A number or code that is used as a "proxy" to identify a mobile subscriber and financial or other data linked to the subscriber	Mobey Forum
Money laundering	Money laundering, the metaphorical "cleaning of money" with regard to appearances in law, is the practice of engaging in specific financial transactions in order to conceal the identity, source and/or destination of money and is a main operation of underground economy. Encompasses any financial transaction which generates an asset or a value as the result of an illegal act, which may involve actions such as tax evasion or false accounting.	Wikipedia

Term	***Description***	***Source***
NFC	Near Field Communication (NFC) is a new, short-range wireless connectivity technology that evolved from a combination of existing contactless identification and interconnection technologies. Products with built-in NFC will dramatically simplify the way consumer devices interact with one another, helping people speed connections, receive and share information and even make fast and secure payments. NFC can be used with a variety of devices, from mobile phones that enable payment or transfer information to digital cameras that send their photos to a TV set with just a touch. The possibilities are endless, and NFC is sure to take the complexities out of today's increasingly sophisticated consumer devices and make them simpler to use.	NFC Forum
Non-repudiation	Non-repudiation is the concept of ensuring that a contract cannot later be denied by either of the parties involved. Non-repudiation is the opposite of plausible deniability. In regard to digital security, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of origin proves that data has been sent, and non-repudiation of delivery proves it has been received.	Wikipedia

Term	***Description***	***Source***
Open standards	An Open standard is a standard that is publicly available and has various rights to use associated with it. The term "open" is sometimes restricted to royalty-free technologies while the term "standard" is sometimes restricted to technologies approved by formalised committees that are open to participation by all interested parties and operate on a consensus basis. Some definitions of the term "open standard" permit patent holders to impose "reasonable and non-discriminatory" royalty fees and other licensing terms on implementers and/or users of the standard. For example, the rules published by the key standards bodies such as the ITU, ISO, and IEC permit requiring patent licensing fees for implementation. However, the definitions of the European Union and Danish government forbid open standards to require fees for use.	Wikipedia
PKI	In cryptography, a public key infrastructure (PKI) is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. This is carried out by software at a CA, possibly under human supervision, together with other coordinated software at distributed locations. For each user, the user identity, the public key, their binding, validity conditions and other attributes are made unforgettable in public key certificates issued by the CA.	Wikipedia
Secure Element	Is a platform where applications can be installed, personalised and managed preferably over-the-air. It is a combination of hardware, software, interfaces and protocols that enable secure storage and use of credentials for payments, authentication and other high end services.	Mobey Forum

Term	***Description***	***Source***
SEPA	Single Euro Payments Area - Customers can pay with euro cash anywhere in the euro area. But making cashless payments from one country to another is still not very smooth. SEPA will remove the technical, legal and commercial barriers. SEPA will make cashless paying with euro as easy, efficient and safe as it is today within one country. SEPA is a project of the market. Public authorities like the ECB and the European Commission play a supportive role.	ECB
Service Provider	The business entity providing the service in question either to end-user or to another business entity.	Wikipedia
SIM	A Subscriber Identity Module (SIM) is a removable smart card for mobile phones. SIM cards securely store the service-subscriber key used to identify a mobile phone. The SIM card allows users to change phones by simply removing the SIM card from one mobile phone and inserting it into another mobile phone. The use of SIM card is mandatory in the GSM world. The equivalent of a SIM in UMTS is called the Universal Integrated Circuit Card (UICC), whereas the Removable User Identity Module (RUIM) is more popular in CDMA phones.	Wikipedia
Smart Phone	A smart phone is a full-featured mobile phone with personal computer like functionality. Most smart phones are camera phones that support full featured email capabilities with the functionality of a complete personal organiser. An important feature of most smart phones is that applications for enhanced data processing and connectivity can be installed on the device[1], by contrast to regular phones which support sandboxed applications. These applications may be developed by the manufacturer of the device, by the operator or by any other third-party software developer. ”Smart” functionality includes any additional interface including a miniature QWERTY keyboard, a touch screen, or even just secure access to company mail, such as is provided by a BlackBerry.	Wikipedia