WHITE PAPER
MOBILE PAYMENTS
2nd edition

Abstract	The 2nd edition of the White Paper includes an additional analysis of mobile remote payments and a section on mobile wallets.
Document Reference	EPC492-09
Issue	Version 3.0
Date of Issue	February 7th 2012

Table of Contents

List of Figures

List of Tables

Executive Summary

The role of the EPC is to contribute to the evolution of an integrated market for payments in Europe through helping in or facilitating in the development and promotion of standards, best practices and schemes. Mobile phones have achieved full market penetration and rich service levels making this the ideal channel for promoting the use of SEPA (Single Euro Payments Area) payment instruments.

This "white paper" endeavours to:

- Inform stakeholders of the EPC's commitment to mobile payments in SEPA;
- Describe some elements of the business rationale for payment service providers (PSPs) wishing to enter the mobile payment services market;
- Demonstrate the consumer adoption potential of mobile payments by presenting several realistic and illustrative scenarios for the use of mobile payments;
- Collect stakeholder views and feedback.

The white paper has been written in a non-technical style to inform PSPs, their customers and all the stakeholders involved in the payments value chain about the EPC's views for mobile payments in SEPA. The EPC would welcome all interested stakeholders' input on the information presented in this white paper.

When starting this work, the EPC analysed the different payment categories and has given prioritisation to mobile contactless SEPA card payments (MCPs) and mobile remote SEPA card and SCT payments. For each of the prioritised categories of mobile payments, the document provides a more detailed analysis through the specification of key use-cases, a description of the ecosystem, the high level architecture and the most important infrastructure aspects. Also the concept of mobile wallets is introduced.

The main conclusions of the document are as follows.

- For mobile contactless SEPA card payments, the choice of Secure Element (SE) has a major impact on the service model and the roles of the different stakeholders.
- For mobile remote payments, three primary challenges have been identified:
    - Convenience of transaction initiation and beneficiary identification for payments initiated by the payer;
    - Certainty of fate of the payment for the beneficiary;
    - Immediate (or very fast) payments.

While many of the identified challenges are not specific to the mobile channel, an early and definitive resolution is key if SEPA payment instruments are to become prevalent in the mobile channel. For interested readers requiring more detail on MCPs, the EPC has compiled implementation interoperability guidelines covering service, technical and security aspects (see [5]). The EPC intends to assist in specifying further implementation guidance on mobile remote payments in a forthcoming document which will be published for public consultation.

Although, it is up to the individual stakeholders in the mobile payments ecosystem to decide if and when they will implement their services in this area, the EPC aims, with the publication of this document, to pave the way for efficient launches of mobile SEPA payments.

0 Document information

0.1 Structure of the document

This section describes the structure of the white paper. Section 0 provides the references, definitions, and abbreviations used in this document. General information about the EPC and its vision may be found in section 1. Section 2 contains an introduction to SEPA, mobile payment services and related business rationale aspects. The next section portrays a number of mobile payments scenarios which are introduced via the description of the daily life of a consumer. It further contains a general overview on mobile payments and its categorisation and prioritisation as proposed by the EPC. Section 4 is devoted to mobile contactless card payments (MCPs). It includes a more detailed description of use-cases and a high level overview of the MCP ecosystem and architecture. In analogy, section 5 provides similar information for mobile remote payments (MRPs) whereby both mobile remote card payments and mobile remote credit transfers are covered. Section 6 illustrates how subscription to mobile payment services can be conveniently and easily achieved. The different infrastructure components used both for MCPs and MRPs are described in section 7. Section 8 introduces the usage of mobile wallets and the influence on consumer experience. The next section provides an overview of the most relevant standards and industry bodies in the mobile ecosystem. General conclusions, gaps and forthcoming work may be found in the final section 10. Finally, an introduction to SEPA payment instruments and a high level analysis on Secure Elements are provided in annexes.

0.2 References

[1]	Arthur D. Little Global M-Payment Report Update - 2009
[2]	EMVCo http://www.emvco.com/
[3]	European Payment Council EPC397-08 Customer-to-Bank Security Good Practices Guide
[4]	European Payments Council EPC 020-08 SEPA Cards Standardisation (SCS) Volume - Book of Requirements
[5]	European Payments Council EPC 178-10 Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines
[6]	European Payments Council – GSM Association EPC 220-08 Mobile Contactless Payments Service Management Roles - Requirements and Specifications
[7]	European Telecommunications Standards Institute http://www.etsi.org/
[8]	European Telecommunications Standards Institute TS 102 221, TS 102 223, TS 102 22 and TS 102 226.
[9]	Global Platform http://www.globalplatform.org/
[10]	GSM Association http://www.gsmworld.com/

[11]	IDC Press release Jul 30th 2009 Smartphone Growth Encouraging, Yet the Worldwide Mobile Phone Market Still Expected To Shrink in 2009. http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS21950309&sectionId=null&elementId=null&pageType=SYNOPSIS
[12]	International Organisation for Standardisation http://www.iso.org
[13]	Internet Engineering Task Force http://www.ietf.org/
[14]	International Telecommunication Union World Telecommunication/ICT Indicators Database 2010 (15th Edition) http://www.itu.int/ITU-D/ict/publications/world/world.html
[15]	Mobey Forum http://www.mobeyforum.org/
[16]	Mobey Forum Alternatives for Banks to offer Secure Mobile Payments (version 1.0) http://www.mobeyforum.org/Press-Documents/Press-Releases/Alternatives-for-Banks-to-offer-Secure-Mobile-Payments
[17]	Mobey Forum Mobile wallet –Definition and vision - Part 1 http://www.mobeyforum.org/Press-Documents/Press-Releases/Mobey-Forum-White-Paper-Provides-a-New-Perspective-on-Market-Development
[18]	NFC Forum http://www.nfc-forum.org/home
[19]	Payment Services Directive Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.
[20]	SD Card Association https://www.sdcard.org/developers

Table 1: Bibliography

0.3 Definitions

Term	Description
Acquirer	A PSP enabling the processing of the merchant's transaction with the issuer through an authorisation and clearing network. In the context of this document, it effectively means accepting mobile payments.
Alias (Unique Identifier)	For remote payments, an alias is basically a pseudonym for the beneficiary that can be uniquely linked to the beneficiary’s name, BIC and IBAN in case of remote SCT and to the identification of the beneficiary's payments account in case of remote SCP. The usage of an alias as identification of the payer may also be used.
Beneficiary	A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction. [19]

Cardholder	A consumer which has an agreement with an issuer for MCP service. He/she needs to be an MNO (or an MVNO) subscriber which has an NFC-enabled mobile equipment.
Card Not Present	A transaction that occurs when the card is used remotely which means there is no physical interaction between the physical card and a POI at the time of the transaction.
Confirmation of Payment Service	In the context of this document, it refers to a service which offers a sufficient degree of assurance for the beneficiary that the payment will be or has been executed (ranging from a simple confirmation to actual receipt of funds).
Consumer	A natural person who, in payment service contracts covered by the [19], is acting for purposes other than his trade, business or profession (as defined in [19]).
3-corner model	Both the payer and the beneficiary are customers of the same PSP which operates under a given payment scheme.
4-corner model	The payer and the beneficiary are customers of different PSPs. Both PSPs can operate under one and the same payment scheme or under different payment schemes.
Customer	A payer or a beneficiary which may be either a consumer or a business.
e-Payment Service	In the context of this document, it is a remote payment service based on the SCT instrument offering confirmation of payment to the beneficiary (who needs to be a registered e-Payment Service participant).
Identification of beneficiary	A mean of uniquely identifying the beneficiary and its underlying account. Examples are the usage of IBAN / BIC, an alias, card number, dedicated credentials, …
Issuer	A PSP providing the payment account and, in the context of this document, the mobile payment application to the customer.
Merchant	The acceptor within an MCP scheme for payment of the goods or services purchased by the consumer (cardholder in the context of the document). Also known as attendant in case of attended POIs. The merchant is a customer for its acquirer.
Mobile Contactless Card Payment (MCP)	A mobile phone initiated payment where the cardholder and the merchant (and/or his/her equipment) are in the same location and communicate directly with each other using contactless radio technologies, such as NFC, for data transfer (also known as contactless payments). In the context of this document, all mobile contactless payments are mobile contactless card payments.
MCP application	An application residing on a Secure Element performing the payment functions related to an MCP, as dictated by the MCP issuer.
MCP application user interface	The mobile phone application executing the user interactions related to the MCP application, as permitted by the MCP issuer.
MCP issuer	A PSP providing the MCP application to the consumer.
Mobile Network Operator (MNO)	A mobile phone operator that provides a range of mobile services, potentially including facilitation of NFC services. The MNO ensures connectivity Over the Air (OTA) between the payer (consumer) and its PSP using its own or leased network (the latter are sometimes referenced as MVNOs - Mobile Virtual Network Operators).

Mobile Remote Payment (MRP)	A payment initiated by a mobile phone or similar device whereby the transaction is conducted over a mobile telecommunication network (e.g. GSM, mobile Internet, …) and which can be made independently from the payer's location (and/or his/her equipment).
Mobile wallet	A digital wallet which is a service allowing the wallet holder to securely access, manage and use identification and payment instruments in order to initiate payments residing on the mobile phone.
MRP application	An application residing on an SE performing the payment functions related to an MRP, as dictated by the MRP issuer.
MRP application user interface	The mobile phone application executing the user interactions related to the MRP application, as permitted by the MRP issuer.
MRP issuer	A PSP providing the MRP application to the consumer
NFC (Near Field Communication)	A contactless protocol specified by ISO/IEC 18092.
Payer	A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order ([14]).
Payment account	Means an account held in the name of one or more payment service users which is used for the execution of payment transactions [19].
Payment scheme	A technical and commercial arrangement setup to serve one or more payment systems and which provides the organisational, legal and operational framework rules necessary for the payment services marketed (e.g. card scheme, e-Payment service …)
Payment Service Provider (PSP)	The bodies referred to in Article 1 of the [19] and legal and natural persons benefiting from the waiver under Article 26 of the [19].
Payment system	A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions (as defined in [14]).
Payment transaction	An act, initiated by the payer or by the beneficiary, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the beneficiary (as defined in [19]).
POI device	Point of interaction device (e.g. POS, vending machine, ATM, …)
Purchase context	Different ways offered by a merchant to their customers to make purchases (e.g. SMS, mobile website, dedicated mobile application, pre-registered alias).
Secure Element (SE)	A certified tamper-resistant platform (device or component) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. Examples include UICC, embedded Secure Elements, chip cards and SD cards.
Secure Element issuer (SE issuer)	A trusted third party responsible for the issuance and maintenance of an SE. Typical examples are MNOs and card manufacturers.
Trusted Service Manager (TSM)	A trusted party acting on behalf of the SE issuer and/or the MRP application issuer in case an SE is involved to host the MRP application(s).

Trusted Third Party (TTP)	This is an entity which facilitates interactions between stakeholders of the ecosystem who all trust this third party (examples are SE issuer, TSM, common infrastructure manager…).

Table 2: Definitions

0.4 Abbreviations

Term	Definition
AAUI	Application Activation User Interface
B2B	Business to Business
B2C	Business to Consumer
C2B	Consumer to Business
C2C	Consumer to Consumer
CAP	Chip Authentication Program
CNP	Card Not Present
CSM	Clearing and Settlement Mechanism
CVM	Cardholder Verification Method
DPA	Dynamic Passcode Authentication
ETSI	European Telecommunications Standards Institute
GP	GlobalPlatform
GSMA	The GSM Association
ID	Identifier
ISO	International Organisation for Standardisation
MCP	Mobile Contactless Payment
MNO	Mobile Network Operator
MRP	Mobile Remote Payment
MVNO	Mobile Virtual Network Operator
NFC	Near-Field Communications
POI	Point of Interaction
PSD	Payment Services Directive
PSP	Payment Service Provider
SCF	SEPA Card Framework
SCP	SEPA Card Payment
SCT	SEPA Credit Transfer
SDD	SEPA Direct Debit
SE	Secure Element
TEE	Trusted Execution Environment
TSM	Trusted Service Manager
TTP	Trusted Third Party
UICC	Universal Integrated Circuit Card
uSCT	Urgent SEPA Credit Transfer

Table 3: Abbreviations

1 General

1.1 About EPC

The European Payments Council (EPC, see http://www.europeanpaymentscouncil.eu/index.cfm) is the coordination and decision-making body of the European banking industry[1] in relation to payments. The purpose of the EPC is to support and promote the Single Euro Payments Area (SEPA). The EPC contributes to the development of the payment schemes and frameworks necessary to realise an integrated euro payments market. In particular, the EPC elaborates on common positions of PSPs[2] for the cooperative space of payment services, assists in standardisation processes, formulates best practices and supports and monitors the implementation of decisions taken. This is done in such a way that PSPs can maintain self-regulation and meet regulators' and stakeholders' expectations as efficiently as possible.

The EPC consists of 74 members representing banks, banking communities and payment institutions. More than 360 professionals from 32 countries are directly engaged in the EPC's work programme, representing organisations of all sizes and sectors of the European banking industry. The European Central Bank acts as an observer in all EPC working and support groups and in the EPC Plenary (the Plenary is the decision-making body of the EPC). The EPC is a not-for-profit organisation which makes all of its deliverables, including the SEPA Scheme Rulebooks and adjacent documentation, available to download free of charge on the EPC Website. Note that the EPC does not supply technology, goods or services.

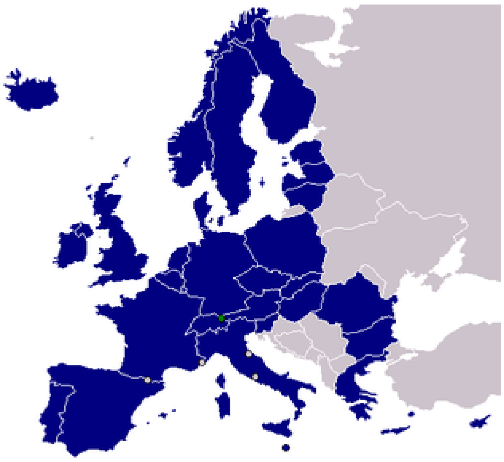


Figure 1: SEPA coverage

A more detailed introduction to SEPA payment instruments can be found in Annex I – SEPA Payment Instruments.

1.2 Vision

The vision of the EPC is to contribute to the evolution of an integrated market for payments through helping in or facilitating the development and promotion of standards, best practices and schemes. Following this line, the EPC has been chartered by its member banks and payment institutions to partner with other stakeholders for the practical deployment of mobile payments in SEPA.

The payment transactions enabled by mobile devices and services could build on existing SEPA Rulebooks and SEPA Cards Framework and (global) standards as far as possible. Therefore, the EPC intends to assist in specifying standards and guidelines to create the necessary environment so

[1] the banking industry is including banks, banking communities and payment institutions

[2] any reference to banks within this document is not intended to limit the provision of mobile payment services solely to banks but is meant to refer to PSPs

that payment service providers can deliver secure, efficient and user-friendly mobile solutions to access the SEPA payment instruments.

Cross-industry cooperation, especially between the payment sector and mobile network operators (MNOs), has been identified as a critical success factor. Therefore the EPC commits itself to help facilitate cross-industry cooperation on rules, standards and best practices in this area. Consumers (see section 0.3 for the definition) should not be bound to a specific MNO or a particular mobile equipment, and should retain their current ability to switch between payment service providers.

1.3 Scope and objectives

The purpose of this white paper is to present an overview on mobile payments for SEPA. This means the usage of the mobile channel for the initiation of SEPA payment instruments. This second edition of this document includes detailed analyses for both contactless and remote payments, according to the priorities set by the EPC (see section 3.2.2).

With the publication of this white paper, the EPC has the following objectives:

- Inform stakeholders about the EPC's commitment to mobile payments in SEPA and the potential of the mobile channel to build on SEPA payment instruments;
- Inform on the new convenient, homogenous and seamless services access and new business opportunities enabled by the mobile channel;
- Outline the prioritised categories for mobile payments;
- Analyse mobile contactless card payments and mobile remote payments;
- Provide other information and examples of existing mobile payment deployments.

1.4 Out of scope and future documents

This document is intended to be self-contained. It should be noted that it is not meant to be an exhaustive introduction to all aspects of mobile payment services but rather focuses on the initiation of payments via the mobile channel leveraging existing SEPA payment instruments (SCT, SDD and SEPA for Card Payments). The reader is referred to the EPC standards and rulebooks (www.europeanpaymentscouncil.eu) for the general aspects of the transaction leg in mobile payments.

This white paper may not remain a standalone document but its purpose is to provide a view on the context as it stands now. This by no means prejudges a future approach by EPC neither in terms of work that may or may not be performed nor of any process that may or may not be proposed to this effect.

The document does not contain market research since numerous studies are already available.

Although this document describes some elements for the business rationale for payment service providers wishing to enter the mobile payments market, more details are provided in the Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines document [5] and forthcoming Mobile Remote Payments Interoperability Implementation Guidelines document to be issued by the EPC. These guidelines focus on interoperability between the different stakeholders involved in the mobile ecosystems such as the SE issuer, the MCP issuer, the MNO, the TSM, etc.

in the co-operative space. Furthermore, technical and security aspects related to the mobile payment application life cycle management and the mobile payment transaction, are addressed.

1.5 Audience

The document is primarily intended for payment service providers as listed in the Payment Services Directive (PSD) [19], such as banks and payment institutions, and card schemes.

In addition, the document may also provide valuable information to other parties involved in implementations and deployment of mobile payments, such as:

- Mobile Network Operators (MNOs);
- Trusted Service Managers (TSMs);
- Equipment manufacturers;
- Merchants and merchant organisations;
- Consumers;
- Application developers;
- Public administrations;
- Regulators;
- Standardisation and industry bodies; and
- Other interested stakeholders

2 Introduction

2.1 Evolution of mobile-based services in SEPA

According to [14] the current penetration of mobile phones in the developed economies is close to saturation. Most consumers are already using mobile phones for services beyond the traditional voice calls and short messaging services (SMS). These services have been greatly facilitated by the current MNO infrastructure supporting packet-oriented Internet access through GPRS and 3G technologies through virtually full geographic network coverage. Recently, consumer expectations for mobile phone functionality have increased dramatically. This is signalled by the fact that the smart phones' market segment is growing more strongly, and at a much higher rate than any other segment [11]**.** Consumers are assuming this trend will continue and are eager to embrace new service solutions based on this delivery platform which may ease their daily lives in a convenient way. Clearly financial services are recognised as most important among these new mobile services, hereby setting high expectations. Moreover, the migration to mobile payments may reduce the cash and cheque usage. The EPC, together with PSPs, believe that mobile-phone initiated payments will be very well received by their customers.

Merchants demand that new technology solutions provide a direct improvement to the efficiency of their operations, ultimately resulting in cost savings and in an increase in business volume. Merchants also expect that new technology reduces exposure to security issues (such as cash theft) and liability (such as illicit payments). Finally, merchants expect that new service offerings introduce new opportunities for marketing, value-added services and increased brand strength. The EPC believes that mobile-phone based payments, in particular those using the contactless approach, are very well positioned to achieve all these benefits for merchants and other stakeholders who are directly providing services to consumers.

In relation to the personal consumer space, the availability of practical SEPA consumer-to-consumer mobile payments, either payment account or card-based, would provide new electronic payment means.

Finally, according to [1], many PSPs have already identified mobile payments as their target for their new growth opportunities. Different mobile payment pilots and commercial deployments are conducted in SEPA and elsewhere, where stakeholder feedback has been consistently very positive. Therefore the SEPA marketplace is clearly set for an immediate uptake of mobile payment services.

2.2 Business rationale

By definition, the ecosystem for mobile payments, whatever form it may take, will provide in its value chain a role for PSPs that hold payment accounts (banks, payment institutions or e-money institutions). This white paper is not intended to build a business case for payments institutions in mobile payments (since this lies in the competitive space, see section 2.4). It rather aims to describe some elements of the business rationale for PSPs who wish to enter the mobile payments market.

PSPs need to anticipate and adapt to future customer behaviour. The mobile channel offers a huge opportunity for PSPs to extend and enrich the payment services offered to their customers. It is very important that this opportunity is grasped, because of a new generation of consumers which rely to a large extent on mobile phones in their daily life. Consumers are increasingly performing financial services via their mobile phone and mobile payments appear to be the next logical step.

The proliferation of mobile devices throughout Europe (and the wider availability of smart phones with multiple applications) and their potential for the initiation of mobile payments, offer a major opportunity to increase the usage of SEPA payment instruments. The usage of the mobile channel may further provide opportunities for additional services such as mandate signing or delivery for direct debits.

As expressed in its vision and roadmap, one of the objectives of the EPC is to stimulate the development and implementation of mobile payments. At this early stage, with the large number of stakeholders involved, alignment around key aspects of the ecosystem is crucial to move from fragmentation to standardisation and to enable the development of SEPA-wide service offerings. An example of such alignment is the ability to associate aliases with payment accounts for MRPs.

As previously stated, the document does not include any market data or research. The reader is invited to consult the numerous market studies available, which show that, besides strong market potential, mobile payments are already taking off. Each PSP should, however, individually determine if it has a business case based on market research, potential revenues and estimated investments and costs. It should further define its position, the resources it is prepared to invest and the role it wants to play in the value chain. Clearly this business case will differ for each PSP, depending on its customer base, its business strategy and objectives, its geographical environment, the technical infrastructure and resources employed.

The major elements supporting a business rationale are the following:

- strong penetration of mobile phones: in the last couple of decades the number of mobile phones has by far exceeded the number of payment cards worldwide, and more and more consumers are ready and willing to use the mobile channel for payments;
- the potential of the recent SEPA payment schemes and framework investments in relation to mobile phone initiated payments;
- provide user convenience by meeting proven needs of both consumers and merchants;
- the need to foster innovation with competitive offerings to the consumer's benefit in a more complex ecosystem including new stakeholders, in line with the EPC SEPA vision; thereby growing the market for payments and migrating consumers to faster, more efficient and more convenient means of payments.

As mentioned above, it is neither the purpose of this paper nor the purpose of EPC to discuss the strategy for which a PSP may enter the market and the concrete service models including the various interactions among the different stakeholders in the value chain. However, a high level description of various service models is presented for both mobile contactless (see section 4) and mobile remote payments (see section 5). These models are analysed in further detail in [5] for MCPs and will be further investigated for MRPs in forthcoming interoperability implementation guidelines.

The main drivers for the stakeholders involved in the ecosystem for a swift adoption of mobile payments are the following:

Consumers’ expectations and demands

- Efficiency: speed of payment initiation;
- Convenience and mobility : make cashless payments anywhere, anytime;

- Confidence and trust;
- Immediacy of payment / confirmation of payment: real time assurance for the beneficiary/merchant of payment execution which allows immediate release of goods or services to the consumer (payer);
- Reachability by payers / consumers of beneficiaries / merchants.

Beneficiaries / merchants

- Cost efficiency (e.g. for merchants**);**
- Confidence and trust;
- Immediacy of payment / confirmation of payment: real time assurance for the beneficiary of payment execution (e.g. merchants, consumers);
- Desire for cash displacement and in some countries cheque displacement;
- Reachability of beneficiaries / merchants by payers / consumers;
- Provision of related additional services such as cross-selling and/or geo-based marketing;
- Low implementation effort.

PSPs

- Customer retention/acquisition;
- Cost efficiency;
- Risk reduction / improved monitoring;
- Provision of related additional services such as mandate management, pre-populated beneficiary details in case of remote payment;
- Desire for cash displacement and, in some countries, cheque displacement;
- Regulators’ expectations.

Clearly the mobile phone will be an additional payment initiation channel co-existing with other channels and means of payment. Other alternatives exist and the payments business is not limited to SEPA frontiers.

2.3 Security aspects

One of the key factors for the proliferation of mobile payments is the "trust" that consumers and merchants have in these payment means. The perception of security in mobile payment transactions is an important aspect in building this trust; other aspects include the contractual relationship between the customers and their PSPs and the transparency of the underlying processes. If there is any doubt about this, the relationship between a PSP and its customers and, even worse, the whole reputation of the PSPs, their services and technologies used could be severely damaged.

To maintain a similar trust and transparency towards customers for mobile payments as for the existing payment initiation channels, it is fundamental to establish a secure, homogeneous ecosystem also encompassing the new stakeholders where it can easily be understood that:

- responsibilities are assigned;
- security issues are consistently governed by the involved stakeholders;

- payment transactions are secured, comprehensible and reliable;
- privacy is respected.

This indicates that an overall security architecture needs to be established that covers all security aspects of the mobile payments ecosystem following reputable international standards. This security architecture should cover at least the following aspects:

- Process level

  Every stakeholder (e.g. PSP, MNO and TSM) in the mobile payments ecosystem must ensure that an appropriate information security management system is in place. Each service provider must be able to either state this in a suitable way to auditors or to define it in terms of security service level agreements in the applicable contractual relationships.

  The information security management system contains at least methods and procedures to monitor and manage relevant risks, and assigns the appropriate resources and responsibilities to mitigate these risks. Every participating party has to define their responsibilities and the valuable assets to protect in their sphere of responsibility.

- Application level

  For any use-case there has to be a security concept documented. On this level the applications and work flows are known. The abstract components in terms of used devices, consumer behaviour, attack surfaces, application environments, etc. can be described and used to analyse the threats and risks. This applies for the whole supply chain and can be broken down into the different perspectives of the customer, service providers, and contractual partners respectively.

- Implementation level

  At the implementation level, the choice of which security controls and measurements should be in place depends mainly on the technical solutions used to implement the services and the associated environment.

  By analysing the specific implementation, the security attack surface can be identified and the appropriate countermeasures, both technical and organisational, can be taken. As an example, for MCP the most salient countermeasure identified is the “Secure Element”, which is introduced later in this document (see also [5]).

2.4 Architecture for mobile payment services

The EPC is proposing high level principles and an architecture for mobile payments in order to create the necessary standards and business rules for PSPs in this new area. Mobile payments constitute a new channel in which existing SEPA instruments, i.e. the SEPA schemes (SCT, SDD) and SEPA Cards (SCP), can be utilised. The main focus is in the area of initiation and receipt of credit and debit payments (including card payments) through mobile phones. Mobile payments will comply with the PSD [19] as well as with the existing rules for underlying SEPA instruments. As a result, the mobile channel does not put any constraint on the value or type of payments generated through it (all SEPA instruments are transaction amount-neutral). This remains a competitive decision by each scheme and / or individual PSP.

The high level principles and an architecture for mobile payments including (references to) standards rules and best practices developed by the EPC are made publicly available to market participants and providers within the mobile channel value chain in order to give the latter the opportunity to provide their input on the elaboration of any standards and business rules in this area. It will be the responsibility of each of them, or of any grouping thereof, to decide when and how to adopt these and, in particular, towards which segment or segments of the payments market their products and services will be geared. This could be e.g. the micro-payment segment, or any other segment.

One of the strongest business opportunities of mobile payments lies in introducing omnipresent services replacing cash. These services should speed up daily transactions and lower the general operational cost of business. The EPC is particularly concerned with facilitating this by enabling highly-streamlined user experiences wherever risk management policies allow. In that respect, the EPC and other bodies are suggesting minimum security requirements. However, the practical implementation of these remains in the competitive space.

The EPC focuses on the areas that form the basis for interoperability and not those lying in the competitive space. It will also foster cross-industry cooperation to enable the mobile phone to become an efficient channel to initiate payments.

The next figure illustrates the involvement of the EPC in the different layers within the scope of mobile payments.

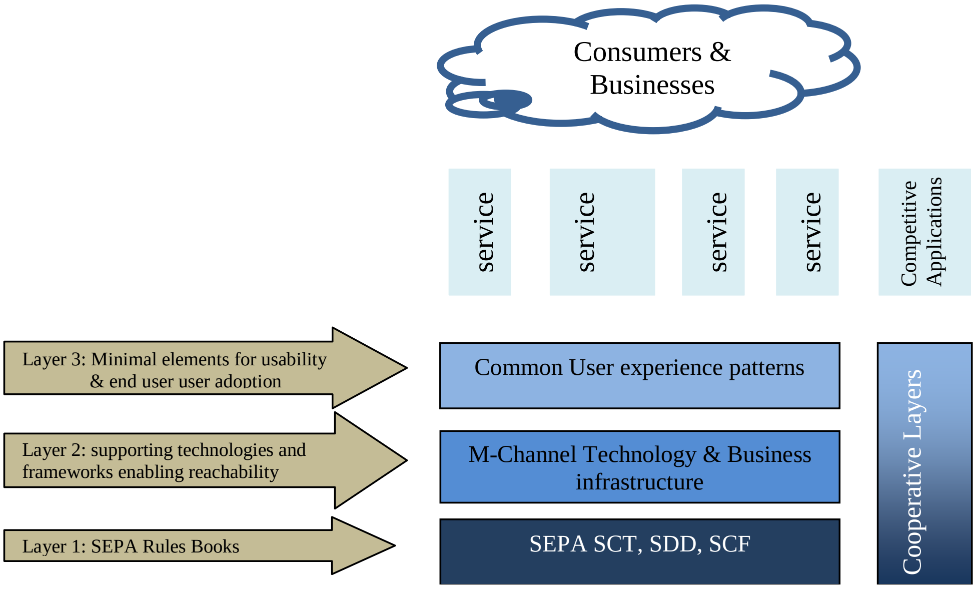

Consumers & Businesses
service
service
service
service
Competitive Applications
Layer 3: Minimal elements for usability & end user user adoption
Layer 2: supporting technologies and frameworks enabling reachability
Layer 1: SEPA Rules Books
Common User experience patterns
M-Channel Technology & Business infrastructure
SEPA SCT, SDD, SCF
Cooperative Layers

Figure 2: Scope of mobile payments

Note: The gradient of blue denotes the level of cooperation in each layer.

Layer 1 denotes the already existing SEPA Rules Books for SCT and SDD and the SEPA Cards Framework. This layer includes the underlying payment instruments for mobile payments.

Layer 2 covers the supporting technologies and frameworks enabling reachability into the SEPA payment instruments. A notable example in this area can be found within the EPC documents “Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines” [5] and “EPC-GSMA Mobile Contactless Payments Service Management Roles - Requirements and Specifications” [6] , which has been jointly developed by the EPC and the GSM Association (GSMA).

Layer 3 elements are, by default, mostly in the competitive space. But in order to overcome the potential complexity of the mobile phone user experience and to ensure reachability, minimal guidelines will be proposed. These guidelines will introduce behavioural patterns for a practical consumer experience and, when applicable, will define minimum security requirements to ensure the integrity of business chains to the benefits of customers. Examples of areas completely left open for competition between different PSPs are pricing, concrete user experiences, risk management, delegation with parental controls, reporting, co-marketing with merchants or other service providers, branding, etc.

2.5 High level guiding principles

The following high-level principles are considered by the EPC to support its vision for mobile SEPA payments.

1. In order to assist in the development of standards and rules for mobile payments, EPC uses existing SEPA payment instruments as a basis[3];

2. Payment service providers should be able to diversify their services offer with enough leeway such that the current effective competitive marketplace for payments is not hampered;

3. Creating ease, convenience and trust for end-customers, (payers / consumers and beneficiaries / merchants), using a mobile phone to initiate a mobile payment, is regarded as critical for the further development within this area;

4. Consumers shall be able to make mobile payments throughout SEPA, regardless of the original country where the SEPA mobile payment services were subscribed to;

5. Stakeholder (including payers / consumers and beneficiaries / merchants) payment liabilities will be no different to those valid for existing SEPA payment instruments;

6. The PSP is responsible for the definition of its own graphical interface to the consumer, including brands & logos, card scheme brands, payment type, etc. as appropriate. The mobile phone user interface shall be able to support this representation;

7. Consumers should not be bound to a specific MNO or particular mobile equipment and should retain their current ability to switch between PSPs;

[3] Note that this does not preclude other types of "mobile payments" which are not based on the SEPA instruments (see also sections 1.3 and 1.4);

8. If a Secure Element (SE) is involved in the mobile payment, which is supported by multiple PSPs, the consumer shall be able to use all their mobile payment services offered using a single mobile phone. Furthermore, he/she shall be able to select the relevant mobile payment application to be used for a particular payment transaction;

9. Mobile payments should, as much as possible, leverage technologies and infrastructure which are capable of being widely deployed in this area. All referenced technologies and systems could however be subject to intellectual property rights rules;

10. The existing service models and structures used for SEPA payments should be retained as much as possible as appropriate.

11. All PSP's personalisation data related to a customer for a mobile payment service in the course of mobile payments shall remain the property of the customer’s PSP.

12. For MCPs, customers should have the same payment experience when performing a mobile contactless SEPA card payment transaction independent of the location at which the transaction is executed. This includes the interaction with the accepting device (POI).

3 Mobile payments for SEPA

3.1 A day in the life of a mobile payments consumer

This section demonstrates how the daily life of a consumer can be enhanced by using his/her mobile phone for payments (so-called mobile payments). A few examples are presented to illustrate some use-cases. It should be noted that many other variations and use-cases exist for the deployment of mobile phone initiated payment services.

Mr Garcia, a regular mobile phone user with a very busy life, is an “assumed” customer of a given PSP. Mr Garcia particularly enjoys using his mobile phone beyond just phone calls and texting. The availability and convenience of this handy device at any time is attracting him to employ it for new types of services. In particular, his perception of having full control over the device creates for him an environment that he trusts to conduct payments. The following figure depicts a typical day in his life.

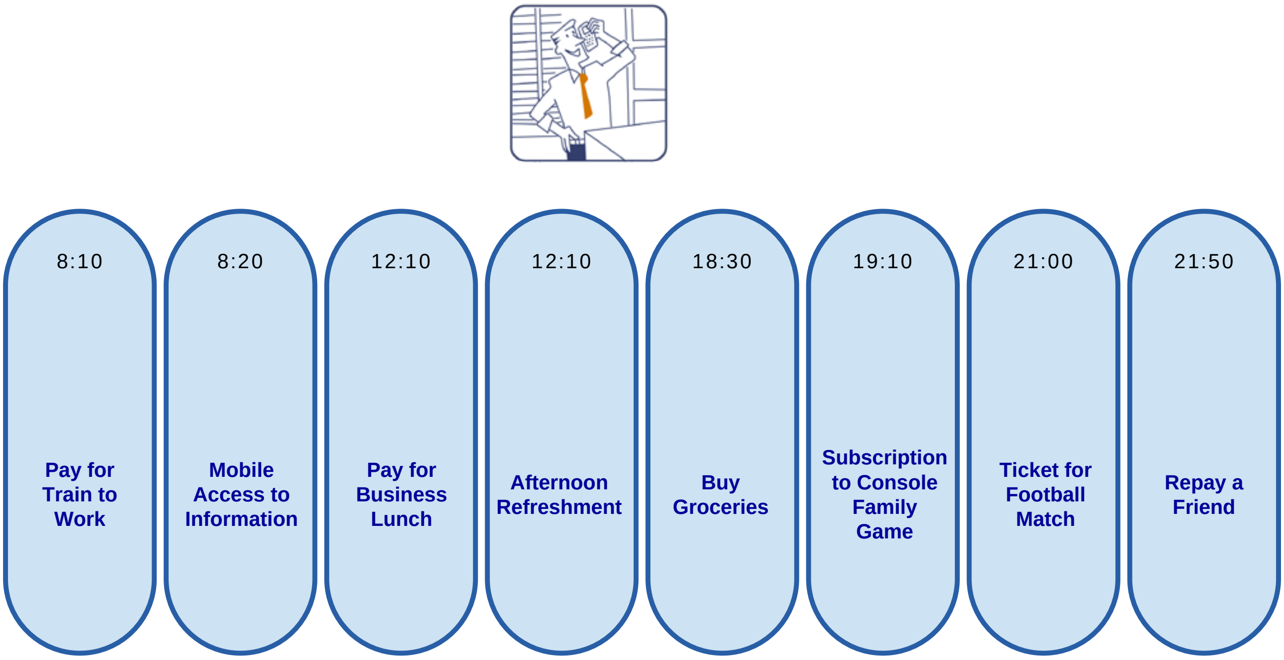


Figure 3: A day in the life of Mr Garcia

3.1.1 Pay for train to work

Mr Garcia arrives at 8:10 at the station to take the train to his office. When he reaches the entry gate to get to the platform, he tries to validate his monthly ticket by tapping his mobile phone on the gate’s sensor. Unfortunately he is informed that his ticket has expired. A specific message on his mobile phone display suggests purchasing a renewal. Mr Garcia then decides to step out of the queue and to purchase the renewal from the ticketing machine using his payment account. He does that by directly confirming the renewal on the mobile phone and subsequently by tapping the mobile phone to the ticketing machine. Back to the gate, he is now allowed to access the train platform and, due to the speedy process, still catches his usual 8:15 train.

3.1.2 Mobile access to premium entertainment

Once comfortably seated in the train, Mr Garcia uses his mobile phone for some entertainment during the journey by browsing a video on-demand website. However, the website informs him that this is a paying service. Through a simple menu option on his mobile phone display, Mr Garcia selects his credit card (for which the details are embedded in the mobile phone), to pay on the website. He subsequently obtains access to the requested movie.

3.1.3 Pay for a business lunch

At lunch time, Mr Garcia invites a prospective customer in a restaurant. After checking the bill, he decides to use the corporate card embedded in his mobile phone to pay. This is achieved by selecting the appropriate card from the menu option on his mobile phone display, enabling the payment transaction by entering his mobile code and simply tapping his phone on the POS terminal presented by the waiter.

3.1.4 Afternoon refreshment

By mid-afternoon, Mr Garcia takes a short break for some energy recharging. Just outside his office there is a small food parlour with several vending machines. After making the selection of his preferred soda, he swiftly taps the vending machine with his mobile phone to perform the transaction with his payment card. With the payment, the vending machine (recognising that a mobile phone has been used for the payment) shows the website of the soda brand for a special offer. Next, Mr Garcia downloads a reduction coupon on his mobile phone for usage with his next soda purchase.

3.1.5 Buy groceries

On the way back home, Mr Garcia stops at the local supermarket to buy a few groceries. At the cashier, he first taps the soda reduction coupon on his mobile phone to the POS terminal. Next he decides to use his debit card embedded in his mobile phone to pay the remaining amount. This is achieved by selecting this card from the options menu on the display of his mobile phone. He taps his mobile phone to the cashier's POS terminal a first time to obtain the payment details and enters his mobile code on the mobile phone. Finally, he taps again the POS terminal with his mobile phone to confirm the payment. Once paid, the POS terminal updates the loyalty card of Mr Garcia in his mobile phone with the points obtained with the purchase.

3.1.6 Remote subscription to an on-line family game

While browsing the Internet with the family's game console, Mr Garcia's daughter finds a new subscription-based multiplayer game she would like to buy. Mr Garcia agrees to pay for it and enters his mobile phone number on the console screen. Immediately afterwards, the mobile phone displays the request for direct debit authorisation. By selecting this, Mr Garcia authorises his payment account as the target of the charges. His daughter can then start playing right away while Mr Garcia leaves for a football match.

3.1.7 Ticket for a football match

Tonight Mr Garcia has an appointment with his friends at the stadium to support the local football team. At the stadium entrance, Mr Garcia pays again with his mobile phone. He first selects the appropriate payment card from the menu option on his mobile phone display. Then he taps his mobile phone on the ticketing terminal, which updates the mobile phone with the ticket for the football match. Subsequently, he enters the stadium by tapping his mobile phone at the entry gate.

3.1.8 Repay a friend

At the half-time break, one of Mr Garcia's friends offers to get fish and chips. Upon her return, Mr Garcia insists on reimbursing her. In order to do so, he first selects the mobile number of his friend from the contact list in his mobile phone. Then, by selecting his preferred payment account from the menu option on the display, Mr Garcia transfers the appropriate amount to his friend's account. Finally, his friend receives a message on her mobile phone display confirming the receipt of the credit transfer.

3.2 General overview on mobile payments

3.2.1 Introduction

As mentioned in section 2.2, "mobile payments" constitutes a new channel to re-use existing SEPA instruments.

Mobile payments are broadly classified as "contactless" (also known as "proximity") or "remote" payments. For "contactless payments" the consumer and the merchant (and/or his/her equipment) are in the same location and communicate directly with each other using contactless radio technologies, such as NFC for data transfer. For "remote payments" the transaction is conducted over telecommunication networks such as GSM or internet, and can be made independently of the payer's location (and/or his/her equipment). To leverage as much as possible the shared infrastructure for contactless SEPA card payments, mobile contactless payments are based only on the usage of NFC technology in card-emulation mode.

Depending on the nature of the payer and beneficiary being a consumer[4] or a business, mobile payments may be also classified as Consumer-to-Consumer (C2C), Consumer-to-Business (C2B), Business-to-Consumer (B2C) and Business-to-Business (B2B) payments.

The following table illustrates how the use-cases described in section 3.1 can be implemented using the existing SEPA instruments. It should be noted, however, that each use-case may be implemented by more SEPA instruments than the one presented. Therefore, a use-case listed in the table below should not be interpreted as the class-type representative of the mobile payment

[4] According to [19], "consumer" means a natural person who, in payment service contracts covered by [19], is acting for purposes other than his trade, business or profession. "Business" is therefore defined as any natural or moral person that is not a consumer.

concerned. Moreover, since only a few use-cases have been provided in section 3.1, not all categories represented in Table 1 have been covered.

		SEPA Credit Transfer	SEPA Direct Debit (Mandate)	SEPA Card Payments
Contactless	**C2C**			
	C2B			Ticket for a football match Buy groceries Afternoon refreshment
	B2C			
	B2B			Pay for a business lunch
Remote	**C2C**	Repay a friend		
	C2B	Pay for train to work	Remote subscription to an on-line family game	Mobile access to premium entertainment
	B2C			
	B2B			

Table 4: Illustration of mobile payments using SEPA instruments

3.2.2 The mobile payment categories prioritised by the EPC

To maximise the potential and overall benefits of mobile payments, the EPC is committed to facilitate a quick market adoption. As a part of this strategy, the EPC conducted a market study in 2008 to prioritise its work in the mobile payments area. Based on the following evaluation criteria: business and economic aspects, infrastructure and go-to-market, and, last but not least, market potential.

An analysis of the different payment types, SCT, SDD and SEPA Cards from the perspective of both consumers and businesses (merchants) is useful when prioritising scenarios for use-cases and for identifying gaps that may be barriers to the full deployment of SEPA in the mobile channel.

The use-cases will adhere to the following principles:

- There is no distinction between domestic and cross-border (within SEPA) transactions
- The nature of the underlying purchase is not within scope
- Transaction value and other limits are a matter for each payment service provider and/or scheme.

Additionally, for the purpose of preparing use-cases, as payment users will be initiating these payments with a 'personal' mobile device most payments will either be:

- consumer payments;
- or business (particularly small businesses) payments initiated by individuals behaving as consumers,

and can therefore generally be covered by the same use-cases.

3.2.2.1 Mobile Contactless Payments analysis

The following table is a summary of the levels of priority for each potential scenario for SEPA Mobile Contactless Payments.

	SEPA Cards	SDD	SCT
C2C	🟩	🟥	🟥
C2B	🟩	🟥	🟥
B2C	🟥	🟥	🟥
B2B	🟧	🟥	🟥

🟥	Low Priority
🟧	Medium Priority
🟩	High Priority

Table 5: Mobile Contactless Payments: priorities

The following sections look at each of the three payment types.

Mobile Contactless SEPA Card Payments

The SEPA Card Payment scenarios were analysed and two key priorities emerged i.e. Consumer-to-Business (C2B) and Consumer-to-Consumer (C2C, often referred to as P2P).

A typical payment card transaction is C2B, with the beneficiary usually being a merchant. In an effort to offer a viable alternative to cash for low value transactions, the payments card industry has been developing the concept of contactless cards. This allows the cardholder to simply wave or touch the card close to the merchant's payment terminal for the payment to proceed. Mobile devices are capable of supporting the same technology and therefore can be used by the cardholder instead of the physical card itself. This is therefore the greatest opportunity, and thus priority, for the development of mobile contactless payments for SEPA.

Mobile devices open up the possibility for contactless proximity Consumer-to-Consumer (C2C) card payments. Such developments are naturally dependent on the participation of the payment card schemes, but it was felt that the opportunity has sufficient potential to merit prioritisation for these use-cases.

Business-to-Business (B2B) SEPA Card Payments are a relatively small proportion of all card payments and are generally conducted using a business or a purchasing card. However, when these transactions take place, the "business" cardholder is effectively behaving as a consumer and the underlying payment process is identical to other SEPA Card Payments. As this document covers contactless SEPA Card Payments using a mobile device, this makes the behaviour even more 'consumer-like'. There is therefore no need to develop specific B2B scenarios for SEPA Card Payments.

Business-to-consumer (B2C) transactions are generally limited to refunds, and where these transactions do take place, they are extremely unlikely to be conducted by using mobile contactless technology and are therefore not prioritised.

SEPA Card	Consumer	Business
Consumer	**C2C** • Offers a practical solution for personal payments, including cheque and cash displacement • Needs support from card schemes to achieve wider reach	**C2B** • Technology available to use mobile devices instead of physical cards for contactless SEPA Card Payments • Merchants should not be impacted by the use of the mobile device rather than the physical card • Use of a mobile affords opportunities to grow and develop the contactless SEPA Card Payments market and also facilitates value added services by card issuers
Business	**B2C** • Very unlikely for a business to be paying a consumer by card, even less so using contactless and probably never using mobile contactless • Even if the card were a business or a purchasing card, the cardholder acts as a consumer, therefore would be the same as C2C scenario	**B2B** • Even if the card is a business or a purchasing card, the cardholder acts as a consumer • Therefore this scenario is no different to C2B above • No need for distinct use-cases

Table 6: Mobile Contactless SEPA Card Payments: definition and priorities

Mobile Contactless SEPA Direct Debit Payments

Direct Debits are originated by the PSP of the beneficiary and are debited to the account of the payer. SDDs cannot be made “contactlessly” and so therefore are out of scope for this section. Therefore, no further prioritisation is required.

In terms of using the mobile channel to help develop SDDs, there may be opportunities to develop value added services around mandates for direct debit users and even the possibility of establishing an SDD mandate using a mobile device.

Mobile Contactless SEPA Credit Transfer Payments

The potential use-cases for mobile contactless payments were analysed for the purpose of prioritisation in this document. In all cases where the payment is conducted using contactless technology, the underlying transaction is a SEPA Card Payment.

There are some possibilities where the underlying transaction, e.g. the renewal of a transport ticket is conducted with mobile contactless technology, as a result of a SEPA Credit Transfer. However, in most, if not all, cases the SEPA Credit Transfer is instructed and authorised remotely, thus facilitating the subsequent transaction.

There is the possibility that if a C2C scheme for SCT was developed it could be enhanced to allow the combination of mobile and contactless technology to identify the beneficiary, but the instruction and authorisation by the payer is still likely to be done remotely. As such a scheme does not exist, and as the payment itself would not technically be a contactless one, this was not prioritised. As mobile contactless SCTs effectively cannot be made, no further prioritisation is required.

3.2.2.2 Mobile Remote Payments analysis

The following table is a summary of the levels of priority for each potential scenario for SEPA MRPs according to the analysis performed by the EPC for its strategy on mobile payments.

	SEPA Cards	SDD	SCT
C2C	🟩	🟥	🟩
C2B	🟩	🟥	🟩
B2C	🟥	🟥	🟧
B2B	🟧	🟥	🟧

🟥	Low Priority
🟧	Medium Priority
🟩	High Priority

Table 7: Mobile Remote Payments: priorities

The following sections look at each of the three payment types.

Mobile Remote SEPA Card Payments

Card transactions tend to be made by consumer cardholders while the beneficiaries tend to be businesses. Although it is acknowledged that some transactions are made with purchasing cards and business/corporate cards, these transactions are still initiated and authorised in the same way as consumer transactions. There is therefore no need to develop distinct use-cases for such scenarios.

According to the current card payment processes, SEPA MRPs are regarded as "Card-Not-Present (CNP)" transactions. This means that all characteristics and challenges of CNP transactions remain valid.

Some enhancements, with respect to authorisation and greater payment certainty for the beneficiary, are needed to increase merchant adoption of this type of card payments. While these areas are being continually addressed, there is potential for some mobile-specific enhancements, which could help to develop this channel for SEPA card payments.

Consumer-to-consumer card-based payments do offer an opportunity in the mobile channel. Some payment schemes already provide such services on a proprietary basis, but mass-market acceptance is largely dependent on the interoperability of all participating card schemes.

As already identified, card payments by businesses are lower volume than those for consumer payments, but where they do occur, they will be covered by the ‘consumer’ use-cases.

In the case of refunds by merchants, these are not likely (though not impossible) to be initiated using a mobile device and therefore will not be covered in a use-case here.

SEPA Card	Consumer	Business
Consumer	**C2C** • Offers a practical solution for personal payments, including cheque and cash displacement • Needs cooperation of card schemes • Existing card number could serve as practical beneficiary IDs. • Viral growth opportunity	**C2B** • Already available through browsers and applications • Certainty of fate for CNP transactions would increase merchant proposition • Mobile channel specific developments are to be expected
Business	**B2C** • Very unlikely for a business to be paying a consumer by card • Even if the card is a business or purchasing card, its user acts as a consumer, therefore would be the same as C2C scenario • A small business that accepts mobile payments could possibly initiate a refund via mobile, but this is not likely in most cases	**B2B** • Even if the card is a business or purchase card, its user acts as a consumer • Therefore this scenario is no different to C2B above • Could be a very practical cheque displacement opportunity for small businesses

Table 8: Mobile Remote SEPA Card Payments: definition and priorities

Mobile Remote SEPA Direct Debit Payments

While SDD is not specifically excluded from the mobile channel, direct debits by their nature, are (almost universally) initiated by businesses and therefore use-cases with consumers as the originator would be of limited value.

Furthermore, businesses originating SDDs are not likely to do so using a mobile device, so use-cases depicting such scenarios would also be of little value.

In terms of using the mobile channel to help develop SDDs, there may be opportunities to develop value added services around mandates for direct debit users and even the possibility of establishing an SDD Mandate using a mobile device.

SDD	Consumer	Business
Consumer	**C2C** • Consumers do not (generally) originate SDDs • In the event that it should occur, the consumer is behaving like a business • Therefore see B2C scenario	**C2B** • Consumers do not (generally) originate SDDs • Even less likely for a consumer to originate a SDD on a business debtor • In the event that it should occur, the consumer is behaving like a business • Therefore see B2B scenario
Business	**B2C** • Most unlikely that a business would originate a SDD using a mobile device • Some potential to offer mandate services in the mobile channel	**B2B** • Most unlikely that a business would originate a SDD using a mobile device • Some potential to offer mandate services in the mobile channel

Table 9: Mobile Remote SEPA Direct Debit Payments: definition and priorities

Mobile Remote SEPA Credit Transfer Payments

The SCT offers the possibility for leveraging SEPA payments in the mobile arena. As the payment is a PSP-to-PSP transfer, it works equally well for consumer, business and government (state) payments. This category, if fully enabled, also offers the opportunity to migrate away from cheques, cash and other paper instruments in countries where these are still in use (in particular France, Ireland and the U.K.).

There are two obvious challenges for the enablement of the SCT in the mobile channel:

- For beneficiaries, particularly businesses (merchants) dealing with consumers, some form of immediate (or near-immediate) payment execution certainty, or a confirmation of payment, is required in many situations;

- For payers, particularly when making a payment to a merchant who is not pre-registered in an e-Payment service (see section 5.2.2.4), the use of a suitable beneficiary identifier is essential. In most circumstances it will not be practical for a payer to input the IBAN, BIC and other relevant information of the beneficiary while using a mobile device.

Depending on the nature of the relationship between the two parties, there are different practicalities to consider, based on the level of trust and the requirement for convenience. The following is a high-level summary of these:

1. High trust level, convenience not critical - here a regular SCT can be used. The payer is happy to enter full beneficiary details. The beneficiary does not require any immediate or advance confirmation;
2. High trust level, but convenience important – here the payer needs a solution to facilitate the entry of the information related to the beneficiary ID. No extra requirements for the beneficiary are needed;
3. Low trust levels and convenience important – here, in addition to payer’s requirements in (2), the beneficiary requires some certainty of execution or even a confirmation of payment execution.

In section 5, a use-case for each will be presented with additional reflections on the type of payer and beneficiary being it a consumer or a business. There will be some cases when businesses behave as consumers when initiating payments using the mobile channel (small businesses in particular) and also where, as beneficiaries, consumers behave as businesses i.e. require a confirmation of payment execution.

SCT	Consumer	Business
Consumer	**C2C** • Offers a practical solution for spontaneous personal payments, including cheque and cash displacement • Needs a practical solution for beneficiary ID (mobile number or other 'alias' could be a solution) • May require central repository function • Certainty of fate would increase proposition • "Viral" growth opportunity	**C2B** • Offers a practical solution for personal payments, including cheque and cash displacement • Needs a practical solution for beneficiary ID for smaller businesses • Certainty of fate for SCT payments would increase merchant proposition
Business	**B2C** • Unlikely to be used by businesses and large corporates, but may have considerable potential for small businesses • Using the mobile channel to initiate SCTs, a business would be acting like a consumer • Therefore the scenario would be the same as C2C	**B2B** • Unlikely to be used by businesses and large corporates, but may have considerable potential for small businesses • Using the mobile channel to initiate SCTs, a business would be acting like a consumer • Therefore the scenario would be the same as C2B

Table 10: Mobile Remote SEPA Credit Transfer Payments: definition and priorities

4 Mobile Contactless Card Payments

4.1 Introduction to Mobile Contactless Card Payments

This section provides a short description of Mobile Contactless SEPA Card Payments (MCPs), which are defined as any contactless SEPA Card [5] payment executed by a cardholder (the consumer) using a dedicated MCP application over NFC. The MCP application is provided by the issuer and is loaded onto a Secure Element (SE), which is independently provided by the SE issuer which may be the MCP issuer, the MNO or another trusted third party (TTP). Regardless of which SE is used, the introduction of the mobile contactless technology should aim to achieve the same security level as for the existing (contactless) SEPA card payments [5].

4.2 Use-cases Mobile Contactless SEPA Cards

This section further elaborates on the use-cases for MCPs introduced in the section 3.1. It should be noted that the user experience described is only an illustrative example since many different implementations are possible for each use-case. Wherever aspects of the mobile phone user interface are mentioned they are also purely illustrative.

This section describes three generic Consumer-to-Business (C2B) SEPA mobile contactless card payments, irrespective of the type of card used (credit, debit or prepaid). B2B is implemented if the consumer is a business.

4.2.1 MCP 1 Tap and Go

The scenario presented in Figure 4 depicts a possible checkout procedure at a groceries store for a low value payment transaction.

Before the scenario commences, the consumer must have subscribed to the mobile payments service for his/her payment card, and selected it as the default payment instrument within the mobile wallet configuration menu. As an option, the consumer enters his/her mobile code to “open” the MCP application before starting the transaction (known as manual mode).

In the figure below, the following steps are illustrated:

1. The merchant starts by entering the transaction amount to the POI terminal.
2. The payment card, which is preselected on the consumer’s mobile phone, is automatically used for the payment. Therefore, to confirm the payment transaction, the consumer only needs to tap the mobile phone on the NFC-enabled POI terminal area.
3. Thereafter, the transaction is processed as a standard SCP transaction.
4. The merchant is able to check the payment.

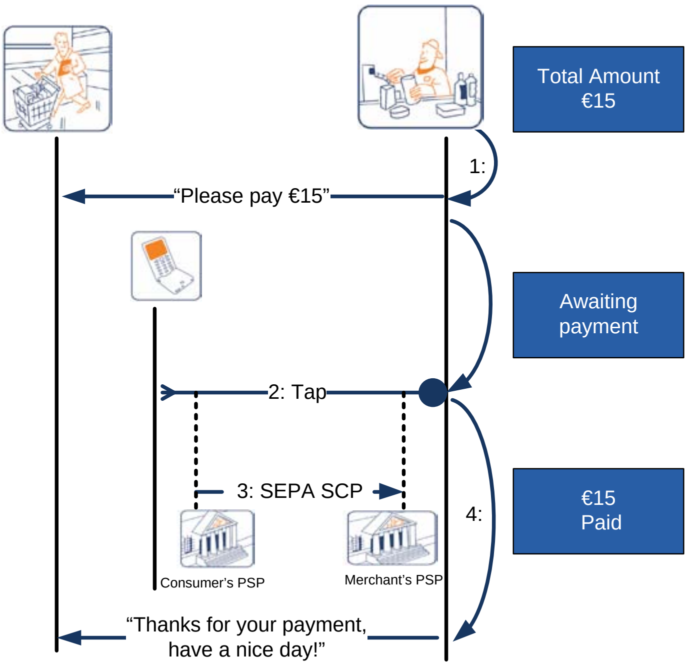


Figure 4: MCP 1 Tap and Go

MCP 1 Tap and Go – Characteristics	
Category	Consumer-to-Business (C2B). Also applicable to B2B.
Communication type	Contactless
Payment instrument	SEPA Card - any type (SCF)
Payment initiation by	Merchant
Prerequisites	• Consumer subscribed to Mobile Contactless Payment Services. • Consumer pre-selected a payment card as default in his/her mobile. As an option, the consumer enters his/her mobile code to "open" the MCP application before starting the transaction (known as manual mode). • Merchant with NFC-enabled POI terminal. • Merchant agreement.
Payment confirmation mode	Tap at NFC enabled POI terminal
Merchant Benefits	• Access to broader consumer base • Highly-efficient payment processing • Additional value added services such as loyalty, couponing, etc.
Consumer Benefits	• Convenience, mobility • Further reduction of cash handling • Cheque (or cash) displacement • Smaller queues
Challenges	No specific challenges in the mobile channel compared to contactless card payments

Table 11: MCP 1 Tap and Go

4.2.2 MCP 2 Double Tap

The scenario presented in **Figure 5** depicts a possible checkout procedure at a groceries store for a high value payment transaction where the consumer enters his/her mobile code on the mobile phone.

Before the scenario commences, the consumer must have subscribed to the mobile payments service for his/her usual payment card and selected it as the default payment instrument within the mobile phone wallet configuration menu.

In the figure below, the following steps are illustrated:

1. The merchant starts by entering the transaction amount to the POI terminal.
2. The consumer taps his/her mobile phone on the NFC-enabled POI terminal area.
3. The payment card which is pre-selected on the consumer's mobile phone is automatically used for the payment. Therefore, to confirm the payment transaction, the consumer only needs to enter his/her mobile code[5] onto the mobile phone.
4. Next, the consumer taps the mobile phone a second time on the NFC-enabled POI terminal area.
5. The transaction is then processed as standard SEPA SCP transaction.
6. The merchant is able to check the payment.

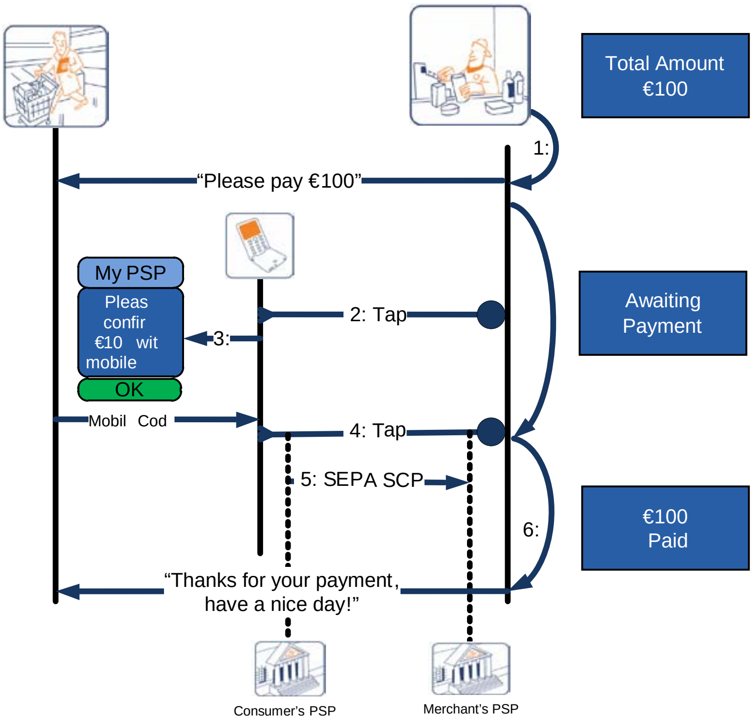


Figure 5: MCP 2 Double Tap

[5] For security reasons the consumer's authentication code denoted as "mobile code" shall not be the same as the card PIN used for conducting contact-based card payment transactions. Further guidance is provided in [5].

MCP 2 Double Tap – Characteristics	
Category	Consumer-to-Business (C2B). Also applicable to B2B.
Communication type	Contactless
Payment instrument	SEPA Card - any type (SCF)
Payment initiation by	Merchant
Prerequisites	• Consumer subscribed to Mobile Contactless Payment Services. • Consumer pre-selected a payment card as default in his/her mobile. • Merchant with NFC-enabled POI terminal. • Merchant agreement.
Payment confirmation mode	• Mobile code with confirmation tap at NFC-enabled POI terminal
Merchant Benefits	• Access to broader consumer base • Efficient payment processing • Additional value added services such as loyalty, couponing, etc.
Consumer Benefits	• Convenience, mobility • Further reduction of cash handling • Cheque (or cash) displacement
Challenges	Education / acceptance of new payment experience by both the consumer and the merchant.

Table 12: MCP 2 Double Tap

4.2.3 MCP 3 Single Tap and PIN

The scenario presented in Figure 6 depicts a possible checkout procedure at a groceries store for a high value payment transaction whereby the merchant’s POI is an on-line terminal and the consumer enters his/her PIN code on this POI.

Before the scenario commences, the consumer must have subscribed to the mobile payments service for his/her usual payment card, and selected it as the default payment instrument within the mobile wallet configuration menu.

In the figure below, the following steps are illustrated:

1. The merchant starts by entering the transaction amount to the POI terminal.
2. The consumer taps his/her mobile phone on the NFC-enabled POI terminal area.
3. The payment card, which is preselected on the consumer's mobile phone, is automatically used for the payment. The consumer is requested to enter his/her PIN code on the POI to complete the transaction. Information about the current transaction (e.g. on-line transaction requested for given transaction amount) is optionally displayed on the mobile phone.
4. The consumer enters his/her PIN code[6] on the POI terminal to confirm the payment transaction.
5. The transaction is then processed as standard SEPA SCP transaction.
6. The merchant is able to check the payment.

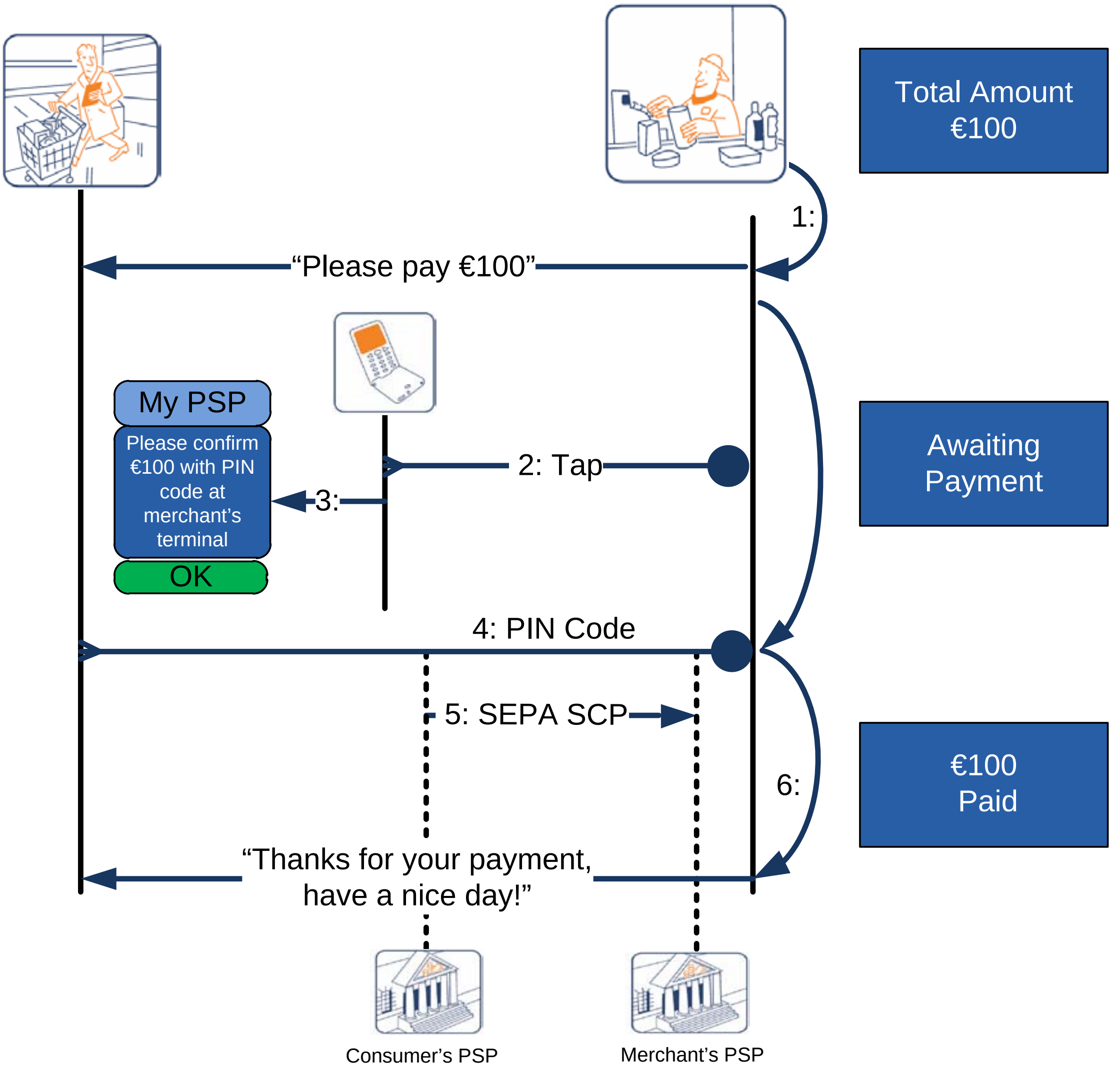


Figure 6: MCP 3 Single Tap and PIN

[6] Same as the PIN used for conducting contact-based card payment transactions.

MCP 3 Single Tap and PIN – Characteristics	
Category	Consumer-to-Business (C2B). Also applicable to B2B
Communication type	Contactless
Payment instrument	SEPA Card - any type (SCF)
Payment initiation by	Merchant
Prerequisites	• Consumer subscribed to Mobile Contactless Payment Services. • Consumer pre-selected a payment card as default in his/her mobile. • Merchant with NFC-enabled POI terminal. • Merchant agreement.
Payment confirmation mode	PIN code entry on POI terminal
Merchant Benefits	• Access to broader consumer base • Additional value added services such as loyalty, couponing, etc.
Consumer Benefits	• Convenience, mobility • Further reduction of cash handling • Cheque (or cash) displacement
PSP Benefits	This contactless payment solution may also be used at ATMs
Challenges	No specific challenges in the mobile channel compared to card payments

Table 13: MCP 3 Single Tap and PIN

4.3 Ecosystem

4.3.1 Introduction

By definition the ecosystem for mobile payments, whatever form it may take, will provide in its value-chain for a role for PSPs that hold payment accounts. Although this document is not intended to build a business case for PSPs in mobile payments (since this lies in the competitive space) it aims to demonstrate that a powerful business rationale to do so exists.

MCPs introduce a new ecosystem involving new participants in the chain. Even if the main participants involved in the transaction based on MCP do not differ from a “classical” payment, MCPs need to rely on a series of technical infrastructure elements that are unique to the mobile environment. Of particular interest are the mobile phones, the SEs and the back-ends to manage the MCP life cycle processes.

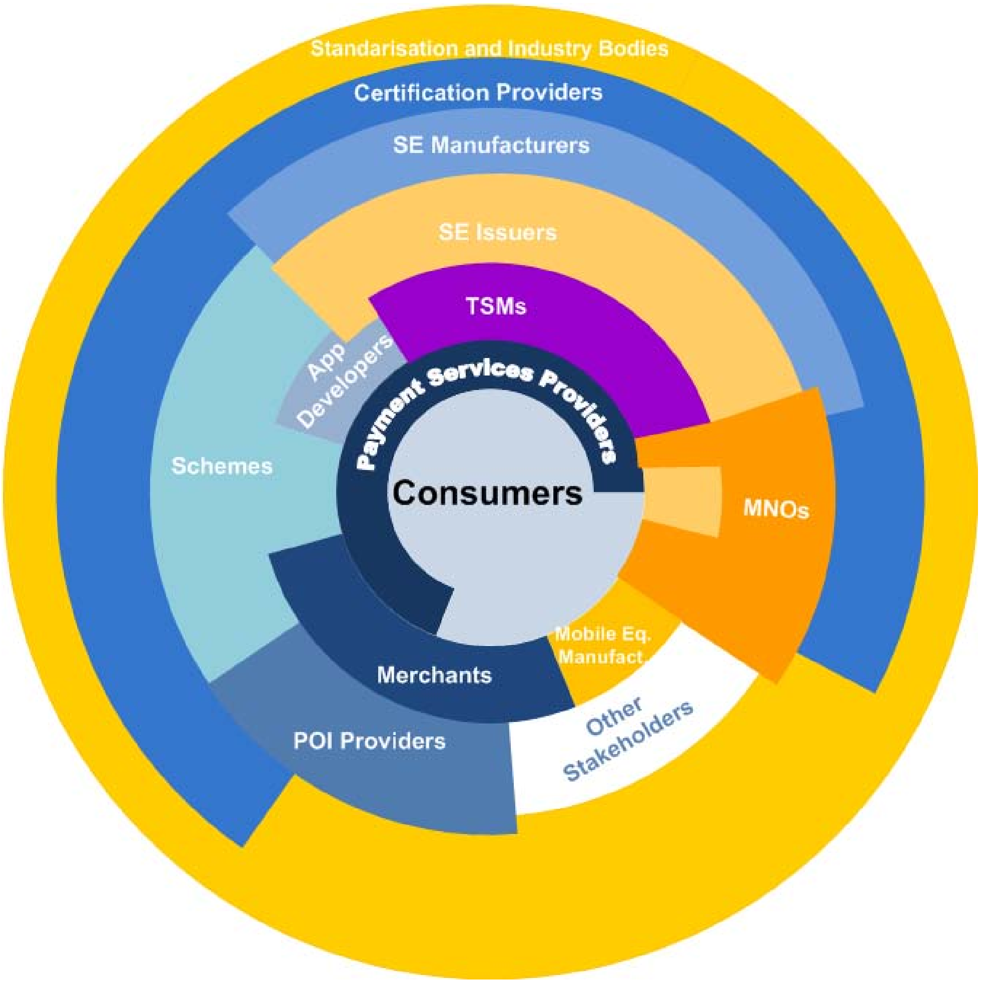


Figure 7: MCP business ecosystem

Due to the complexity of the ecosystem, only the most important business relationships in the figure above are depicted through the contact points. The MCP business ecosystem is consumer centric. The latter is not only a consumer to the payment service provider but also to the merchant, the MNO, the mobile equipment manufacturer and, potentially, the SE issuer.

4.3.2 New stakeholders

As introduced above, the most salient stakeholder in the MCP ecosystem is the SE issuer. This is the MNO in case of a UICC, the handset manufacturer or MCP issuer in case of an embedded SE (see section 4 in [5]), etc. In any case, the MCP issuer may optionally use a so-called Trusted Service Manager (TSM) for the lifecycle management of its application. The TSM is a trusted third party (TTP) introduced to provide for better scalability when several MCP issuers must undertake commercial and technical interactions with several SE issuers. As illustrated in Figure 8, MCP issuers, TSMs and SE issuers collaborate to perform the provisioning and management of the MCP application(s).

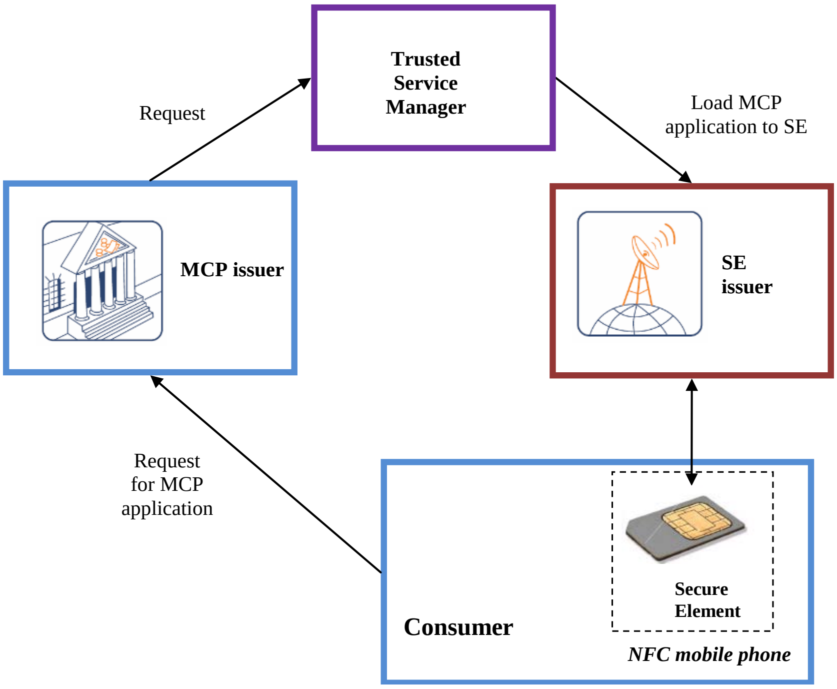


Figure 8: Provisioning of MCP applications to an SE

To facilitate an open ecosystem, many TSMs may exist that offer mutually-competing services to both SE and MCP issuers.

Other relevant new stakeholders are:

- SE manufacturers.
- Application developers (MCP application, AAUI, mobile wallet …).
- Mobile equipment manufacturers.
- Organisations performing infrastructure certification (e.g., SEs, MCP applications, POI, etc.).

4.3.3 Service models

4.3.3.1 Payment transaction

An MCP does not in any way modify the underlying SEPA card payment transaction. Therefore the service model of the latter remains unaffected (see also section 4.4).

4.3.3.2 Provisioning and management

In order to facilitate the introduction of a rich ecosystem of service providers performing TSM functions, the EPC and the GSMA have jointly developed requirements and specifications for the MCP service management roles for applications residing on a UICC [6]. Subsequently, the EPC has extended these requirements and specifications to two further types of SEs: embedded SE and removable SE (such as secure micro SD card) [5].

A high-level summary of the partitioning of MCP service management roles is illustrated in Figure 9 below.

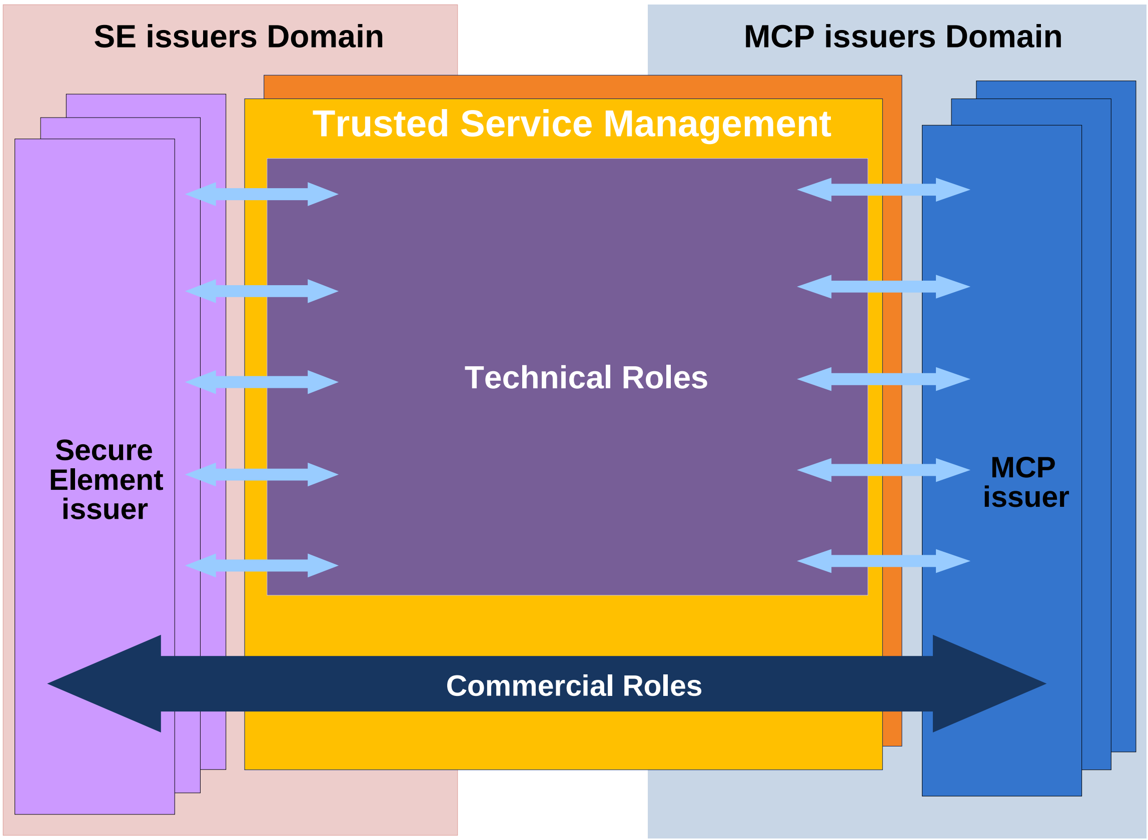


Figure 9: Provisioning and management overview for MCPs

Many services models are possible by delegating combinations of the different technical and commercial roles to one or more TSMs, including three and four-party service models, please refer to [5] and [6] for more details.

4.4 High level architecture

As illustrated in Figure 10, the main parties involved in the transactions based on MCPs do not differ from a “classical” SEPA card payment. The payment transaction is performed by reusing the existing SEPA contactless card payments accepting devices, while the back-end and transaction infrastructure will be those already used for SEPA card payments (see [4]).

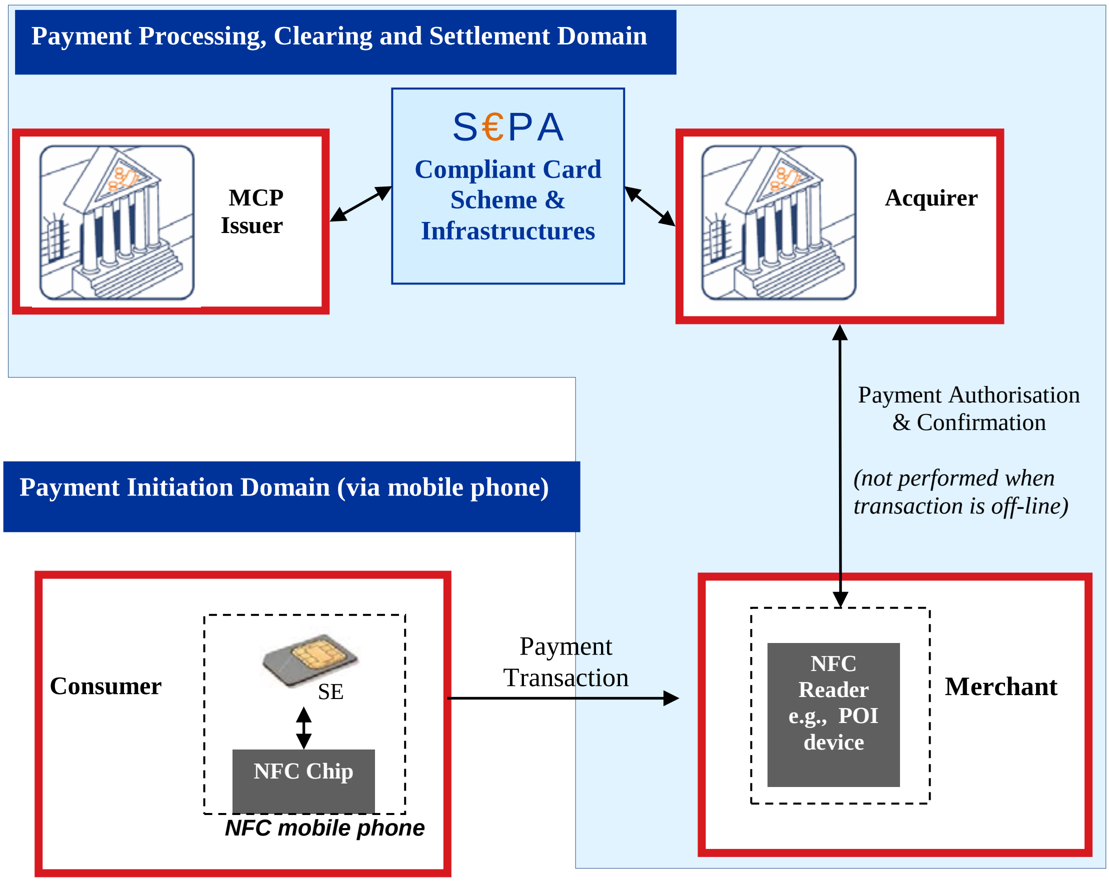

Payment Processing, Clearing and Settlement Domain
S€PA
Compliant Card Scheme & Infrastructures
MCP Issuer
Acquirer
Payment Authorisation & Confirmation
(not performed when transaction is off-line)
Payment Initiation Domain (via mobile phone)
Consumer
SE
NFC Chip
NFC mobile phone
Payment Transaction
NFC Reader e.g., POI device
Merchant

Figure 10: MCP transaction[7]

[7] Components within the blue shaded area are similar to contactless card payments

5 Mobile Remote Payments

5.1 Introduction to Mobile Remote Payments

In the context of this document, Mobile Remote Payments (MRPs) are SEPA payments (SCT, SDD, SCP) which are initiated using a mobile phone where the transaction is conducted over a mobile telecommunication network (e.g. GSM, mobile Internet, etc.) and which can be made independently from the payer's location (and/or his/her equipment). This means that the payment transaction is not dependent on physical contact with a POI such as a point of sale device.

5.2 Use-cases Mobile Remote Payments

5.2.1 Mobile Remote SEPA Card Payments

The following use-cases are based on an SCP as underlying SEPA payment instrument.

5.2.1.1 SCP 1 Consumer-to-Business SEPA Card Payment - Core (C2B)

In this scenario, illustrated in Figure 11, the consumer uses his/her mobile phone to conduct a payment to a merchant, which is providing goods or services (e.g. mobile content). B2B is implemented when the consumer is a business.

The flow of this example is similar to a remote SEPA Card Payment using a PC over the Internet.

In the figure below, the following steps are illustrated:

1. While browsing the Internet with his/her mobile phone (also known as mobile Internet) or through the use of a specific MRP application, the consumer will start by navigating to the checkout section of the merchant's website.
2. The merchant's website will present the payment information on the consumer's mobile phone.
3. The consumer inputs his/her payment card details (e.g. card number, expiry date and card security code) and initiates an SCP transaction
4. Once the payment is authorised, the SEPA Card Payment is processed.
5. The merchant releases the goods or services to the consumer.

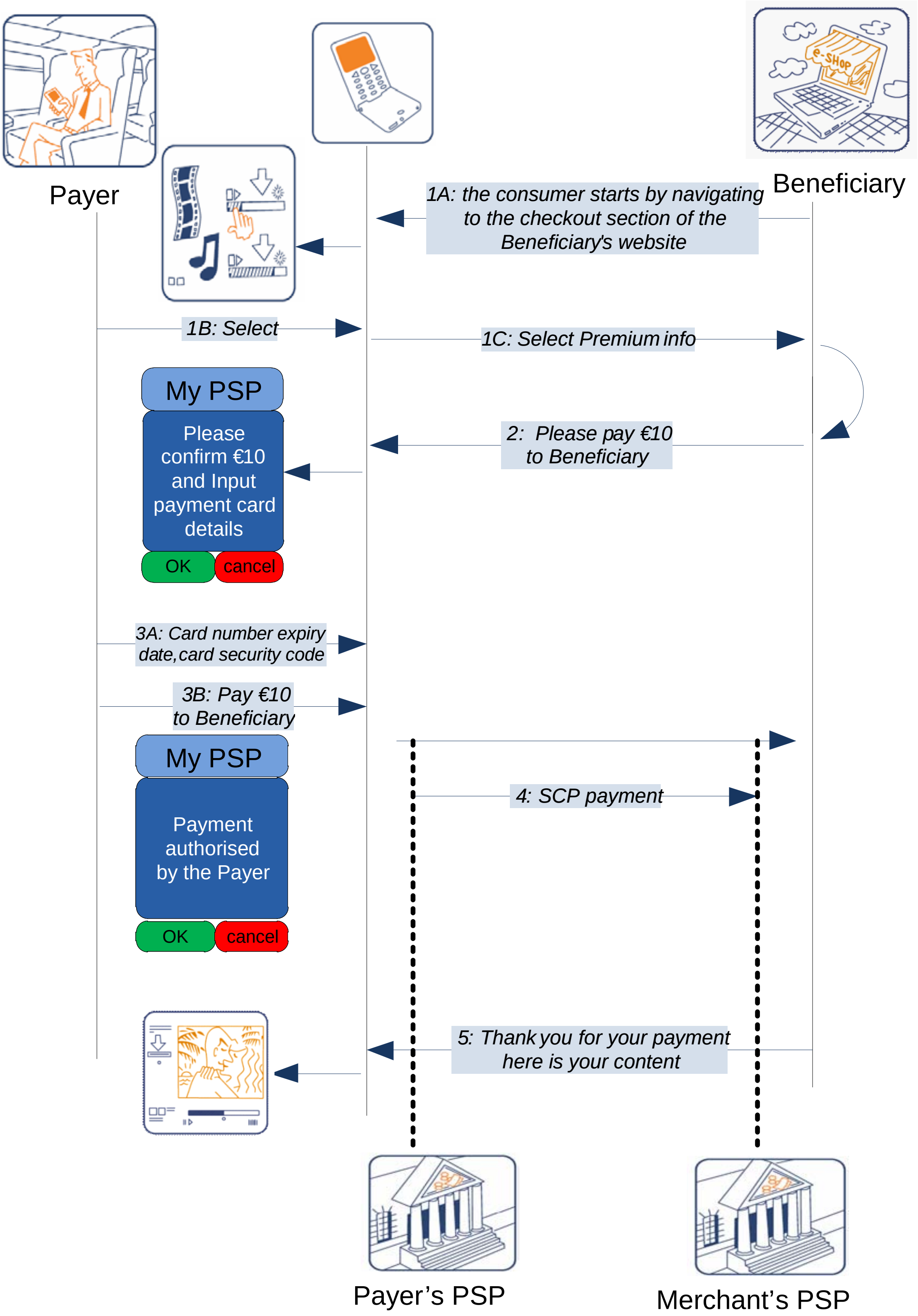

Payer
Beneficiary
1A: the consumer starts by navigating to the checkout section of the Beneficiary's website
1B: Select
1C: Select Premium info
My PSP
Please confirm €10 and Input payment card details
OK
cancel
2: Please pay €10 to Beneficiary
3A: Card number expiry date,card security code
3B: Pay €10 to Beneficiary
My PSP
Payment authorised by the Payer
OK
cancel
4: SCP payment
5: Thank you for your payment here is your content
Payer's PSP
Merchant's PSP

Figure 11: SCP 1 Consumer-to-Business SEPA Card Payment

SCP 1 Consumer-to-Business SEPA Card Payment – Core	
Category:	Consumer-to-Business (C2B), also applicable to B2B
Communication type	Remote
Payment instrument	SEPA Card - any type (SCF)
Payment initiation by	Merchant
Prerequisites	• Merchant accepts remote card payments for a given card scheme • Consumer has an SCF compliant card within the same card scheme
Payment confirmation mode	As with any other remote SEPA card transaction
Merchant Benefits	• Access to broader consumer base • Merchant anytime accessible by the consumer
Consumer Benefits	• Convenience, mobility • Further reduction of cash handling • Cheque (or cash) displacement
Challenges	• No specific challenges in the mobile channel compared to other remote card payments via Internet • Inconvenience for the consumer to enter his/her credentials into the mobile phone (could be solved by e.g. usage of a mobile wallet[8]) • Since this is a CNP transaction, the merchant has no certainty about the payment (the issuer has chargeback rights)

Table 14: SCP 1 Consumer-to-Business SEPA Card Payment - Core

5.2.1.2 SCP 2 Consumer-to-Business SEPA Card Payment - Mobile wallet (C2B)

In this scenario, illustrated in Figure 12, the consumer uses his/her mobile phone to conduct a payment to a merchant, which is providing services or goods (e.g. mobile content). B2B is implemented when the consumer is a business. The difference from the ‘core’ scenario above is that the paying consumer makes use of a mobile wallet to access and retrieve its payment card details when making the payment to the merchant.

From the merchant’s perspective, the scenario is very similar to SCP 1.

Before the scenario commences, the consumer should have enabled the card(s) for conducting remote payments within a mobile wallet configuration menu.

[8] Note that some practical evidence on mobile wallets may be found through specific initiatives launched in certain communities or regions.

In the figure below, the following steps are illustrated:

1. While browsing the Internet with his/her mobile phone (also known as mobile Internet) or through the use of a specific MRP application, the consumer will start by navigating to the checkout section of the merchant's website;
2. The merchant's website will present the payment information on the consumer's mobile phone;
3. The consumer payment card details are provided through the use of a mobile wallet and his/her entry of the card security code[9], which initiates an SCP transaction;
4. Once the payment is authorised, the SEPA Card Payment is processed;
5. The merchant releases the goods or services to the customer.

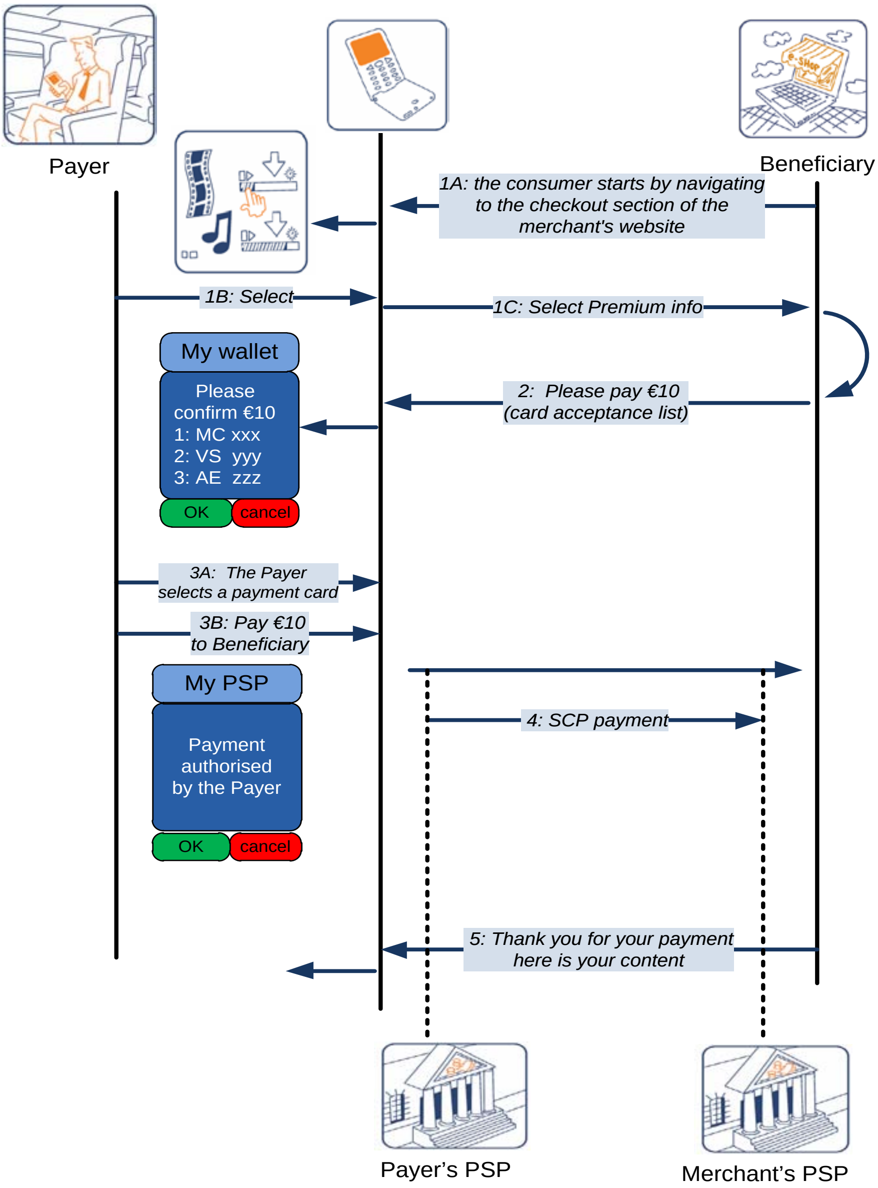

Payer
Beneficiary
1A: the consumer starts by navigating to the checkout section of the merchant's website
1B: Select
1C: Select Premium info
My wallet
Please confirm €10
1: MC xxx
2: VS yyy
3: AE zzz
OK
cancel
2: Please pay €10 (card acceptance list)
3A: The Payer selects a payment card
3B: Pay €10 to Beneficiary
My PSP
Payment authorised by the Payer
OK
cancel
4: SCP payment
5: Thank you for your payment here is your content
Payer's PSP
Merchant's PSP

Figure 12: SCP 2 Consumer-to-Business SEPA Card Payment - Mobile wallet

[9] For more details, see SEPA Cards Standardisation Volume [4].

SCP 2 Consumer-to-Business SEPA Card Payment - Mobile wallet	
Category:	Consumer-to-Business (C2B), also applicable to B2B
Communication type	Remote
Payment instrument	SEPA Card - any type (SCF)
Payment initiation by	Merchant
Prerequisites	• Merchant accepts remote card payments for a given card scheme • Consumer has an SCF compliant card within the same card scheme
Payment confirmation mode	As with any other remote SEPA card transaction
Merchant Benefits	• Access to broader cardholder base • Merchant anytime accessible by cardholder
Consumer Benefits	• Convenience, mobility • Convenience for the consumer to choose a payment card with associated credentials, using a mobile wallet. Further reduction of cash handling • Cheque (or cash) displacement
Challenges	• No specific challenges in the mobile channel compared to other remote card payments via Internet • User authentication: since he/she is not allowed to store the card security code, the customer normally still must enter this value to perform the transaction which is not very user-friendly.

Table 15: SCP 2 Consumer-to-Business SEPA Card Payment- Mobile wallet

5.2.1.3 SCP 3 Consumer-to-Business SEPA Card Payment - Strong cardholder authentication (C2B)

In this scenario, the difference with the SCP 2 scenario above is that the payer is required to take an extra authentication step. As a card-based authentication such as CAP (Chip Authentication Program) or DPA (Dynamic Passcode Authentication) may be used for remote card transactions, the usage of an SE in the mobile phone which hosts a (dedicated) authentication application could be a considerable enhancement with respect to consumer convenience. The usage of this authentication application must be subject to a mobile code entered by the consumer on the mobile phone and verified by the authentication application. This consumer authentication gives the merchant greater protection against fraudulent or repudiated transactions. Moreover, if the mobile phone already hosts an MCP application in an SE, this might be a cost-effective solution.

The card issuer(s) must have installed a (dedicated) authentication application in the SE of the consumer’s mobile phone. Furthermore, the consumer must have enabled the authentication application(s) for conducting remote payments e.g. within a mobile wallet configuration menu.

As another alternative, if the payer has both an NFC mobile phone and a contactless card including an authentication application such as CAP or DPA, he/she can authenticate by presenting the card to the NFC reader of the mobile phone. Again, the usage of this authentication method must be subject to a mobile code entered by the consumer on the mobile phone.

In the figure below, the following steps are illustrated:

1. While browsing the Internet with his/her mobile phone (also known as mobile Internet) or through the use of a specific MRP application, the consumer will start by navigating to the checkout section of the merchant's website;
2. The merchant's website will present the payment information on the customer's mobile phone;
3. The consumer payment card details are provided through the use of a mobile wallet and he/she initiates an SCP transaction. The payment card authentication application authenticates the consumer;
4. Subject to successful authentication, the payment is then authorised;
5. Once the payment is authorised, the SCP is processed;
6. The merchant releases the goods or services to the customer.

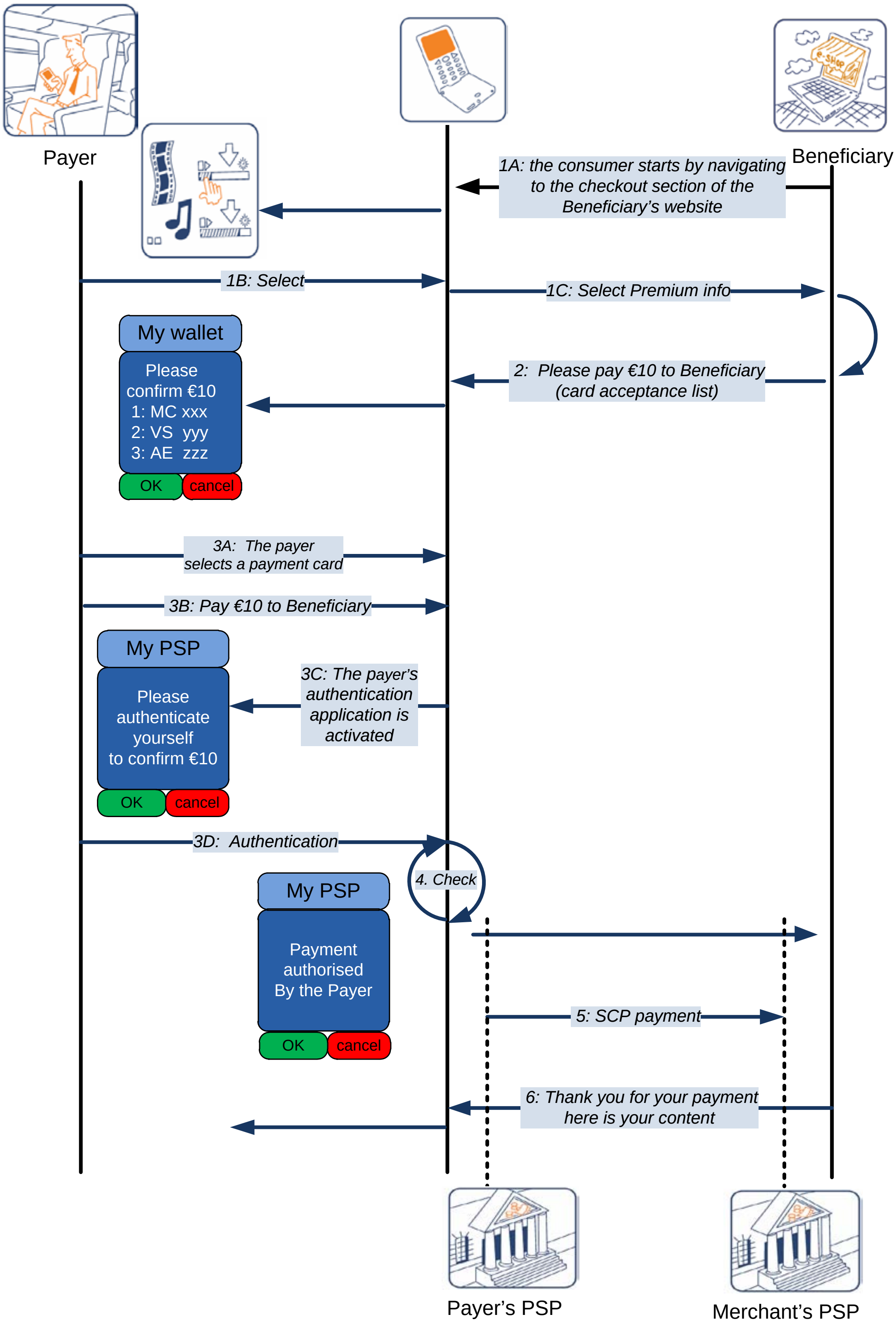

Payer
Beneficiary
1A: the consumer starts by navigating to the checkout section of the Beneficiary's website
1B: Select
1C: Select Premium info
My wallet
Please confirm €10
1: MC xxx
2: VS yyy
3: AE zzz
OK
cancel
2: Please pay €10 to Beneficiary (card acceptance list)
3A: The payer selects a payment card
3B: Pay €10 to Beneficiary
My PSP
Please authenticate yourself to confirm €10
OK
cancel
3C: The payer's authentication application is activated
3D: Authentication
4. Check
My PSP
Payment authorised By the Payer
OK
cancel
5: SCP payment
6: Thank you for your payment here is your content
Payer's PSP
Merchant's PSP

Figure 13: SCP 3 Consumer-to-Business SEPA Card Payment - Strong cardholder authentication

SCP 3 Consumer-to-Business SEPA Card Payment - Strong cardholder authentication	
Category:	Consumer-to-Business (C2B), also applicable to B2B
Communication type	Remote
Payment instrument	SEPA Card - any type (SCF)
Payment initiation by	Merchant
Prerequisites	• Merchant accepts remote card payments for a given Card scheme • Consumer has an SCF compliant card within the same Card scheme
Payment confirmation mode	As with any other remote SEPA card transaction
Merchant Benefits	• Access to broader cardholder base • Merchant anytime accessible by cardholder • Reduction of remote card payment fraud
Consumer Benefits	• Convenience, mobility • Convenience for the consumer: more automated handling of the authentication • Further reduction of cash handling • Cheque (or cash) displacement
Challenges	• No specific challenges in the mobile channel compared to other remote card payments via Internet

Table 16: SCP 3 Consumer-to-Business SEPA Card Payment - Strong cardholder authentication

5.2.1.4 SCP 4 Consumer-to-Consumer SEPA Card Payment – Core (C2C)

Figure 14 introduces a possible example of user experience for a consumer-to-consumer SEPA card payment initiated by a mobile phone where a consumer (payer) wants to make a personal payment to a second consumer (beneficiary) with his/her mobile phone.

In this use-case, the primary difference between this and a regular SEPA card payment is that the transaction is initiated by the payer, rather than by the beneficiary. The payment is processed over the card scheme network(s) and charged to the payer's payment card account in the normal way. The beneficiary will typically (but not necessarily) be identified by his/her payment card details and the proceeds of the payment will be applied to the relevant underlying payment account. Depending on card scheme rules, there may be scope to use an alias (e.g. mobile phone number) and there may also be alternative options to identify and pay beneficiaries (e.g. payment account).
This scenario may also be applicable for C2B payments where the beneficiary is a business (but behaving in the manner of a consumer and subject to card scheme rules). Payer and beneficiary may be customers of different PSPs.

A prerequisite for this scenario is that the payer has subscribed to a (possibly, but not necessarily, mobile specific) C2C card payment system with his/her card issuer. Many of the major card schemes already offer some proprietary C2C services, but these would need to achieve interoperability for mass SEPA acceptance.

In the figure below, the following steps are illustrated:

1. The payer decides upon the amount to be paid.
2. The payer selects his/her MRP application.
3. The payer enters the amount and the unique identifier of the beneficiary, confirms the card number to be used for payment and authorises the transaction.
4. The payer's PSP resolves the beneficiary's identification details from the unique identifier.
5. The payer's PSP sends the payment to the beneficiary's PSP.
6. The beneficiary's PSP then applies the payment to the underlying beneficiary payment account (optionally with a notification).

A further enhancement of this use-case would be where an ‘urgent' or ‘fast' payment can be made ensuring immediacy. A ‘fast' SCP C2C service would cater for scenarios where:

- The beneficiary needs use of funds for an emergency;
- The beneficiary needs certainty of receipt to proceed with an underlying transaction e.g. a sale of goods or rendering of services between strangers.

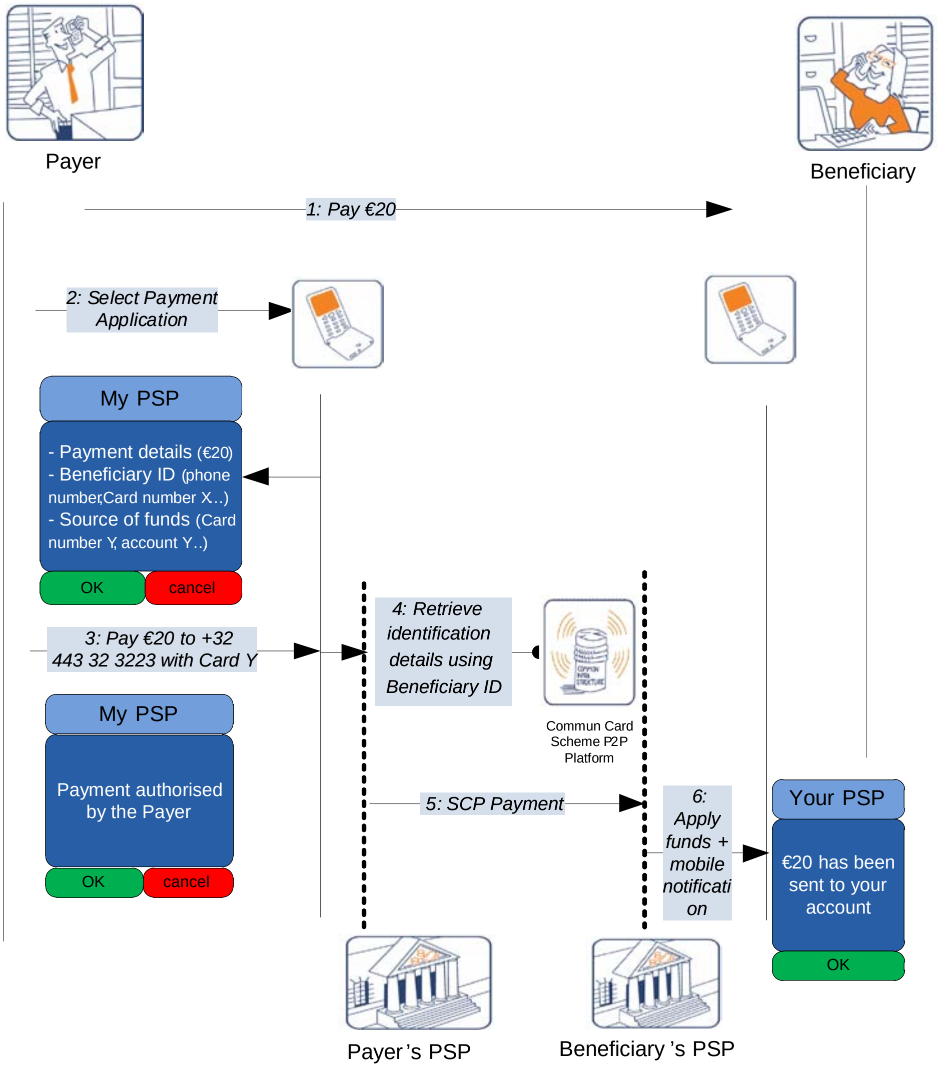

Payer
Beneficiary
1: Pay €20
2: Select Payment Application
My PSP
- Payment details (€20)
- Beneficiary ID (phone number,Card number X..)
- Source of funds (Card number Y, account Y..)
OK
cancel
3: Pay €20 to +32 443 32 3223 with Card Y
4: Retrieve identification details using Beneficiary ID
Commun Card Scheme P2P Platform
My PSP
Payment authorised by the Payer
OK
cancel
5: SCP Payment
6: Apply funds + mobile notificati on
Your PSP
€20 has been sent to your account
OK
Payer 's PSP
Beneficiary 's PSP

Figure 14: SCP 4 Consumer-to-Consumer SEPA Card Payment - Core

SCP 4 Consumer-to-Consumer SEPA Card Payment - Core	
Category	Primarily Consumer-to-Consumer (C2C), some scenarios for Consumer to (e.g. small) Business (C2B)
Communication type	Remote
Payment instrument	SEPA Card – any type (SCF)
Payment initiation by	Payer
Prerequisites	Beneficiary is identifiable with a unique identifier, generally, but not necessarily, a payment card Payer has an SCF compliant card and is subscribed to a mobile C2C card payment system by his/her PSP (card issuer)
Payment confirmation mode	Determined by the PSP (card issuer).
Customer Benefits	• Quick and easy for both consumers. • Access to non-card acquired beneficiary for payer • Allows payer to keep credentials private and avoids beneficiary having to disclose account details
Challenges	• Ensuring card scheme interoperability • Management and support of unique beneficiary identifier if required • Inconvenience for the cardholder to enter his/her credentials into the mobile phone (could be solved, for example, by the usage of a mobile wallet).

Table 17: SCP 4 Consumer-to-Consumer SEPA Card Payment - Core

5.2.2 Mobile Remote SEPA Credit Transfer

The following use-cases are based on an SCT as underlying SEPA payment instrument. Note that under the current SCT rules, the maximum processing time between PSPs for an SCT is one business day (D+1) under the PSD.

Independently of the initiation steps, the actual SCT transaction is always based on the usage of the IBAN and BIC[10].

5.2.2.1 SCT 1 Consumer-to-Consumer SEPA Credit Transfer – Core (C2C, SCT)

Figure 15 introduces a possible core example of a user experience for an SCT payment initiated using a mobile phone where a consumer (payer) makes a payment from his/her own payment account to the payment account of another consumer (beneficiary). Payer and beneficiary may be, and frequently are, customers of different payment service providers (PSPs) (4-corner model[11], see sections 5.4.3.2 and 5.4.3.3).

[10] According to the SEPA Regulation, the necessary usage of the BIC by consumers will be phased out by February 2016 at the latest and, in most cases, by February 2014 for domestic transactions.

[11] Any reference to the 4-corner model should not be interpreted as meaning that 3-corner models could not be benefiting from the developments considered here.

In this scenario no upfront confidence between payer and beneficiary is assumed. Both payer and beneficiary will receive the same level of services from their respective PSP as with any other SCT.

In many circumstances, this use-case is also applicable for C2B, B2C and B2B (particularly small businesses).

In the figure below, the following steps are illustrated:

1. The beneficiary provides all the necessary information, including IBAN and BIC to the payer;
2. The payer provides all the necessary information, including IBAN and BIC of the beneficiary to his/her PSP via his mobile phone. This information can be input by the payer in full or by accessing a pre-registered beneficiary. This is typically done by using a specific mobile phone PSP application or by accessing a mobile browser;
3. The payer, once authenticated by his/her PSP, authorises the SCT instruction in compliance with the usual security requirements set out by that PSP;
4. The payer's PSP then processes and submits the SCT to the beneficiary's PSP which in turn will credit the beneficiary.

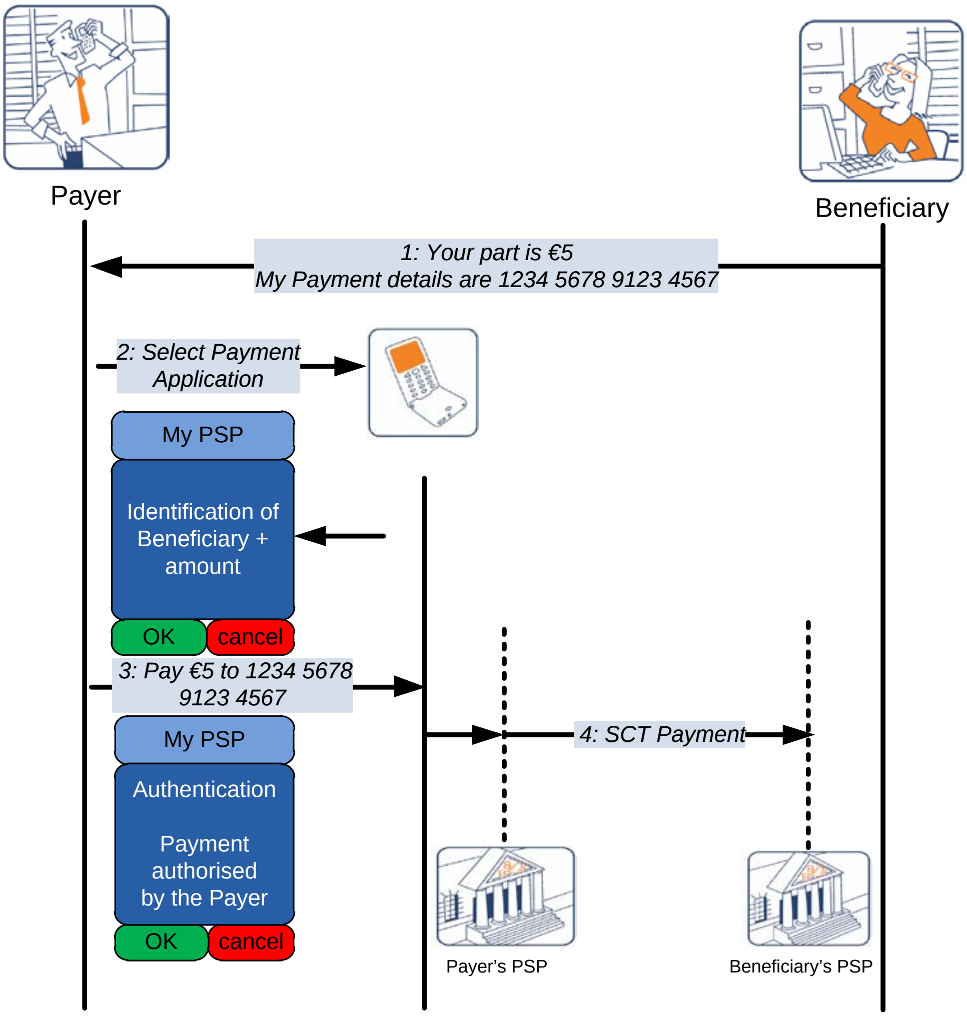

Payer
Beneficiary
1: Your part is €5
My Payment details are 1234 5678 9123 4567
2: Select Payment Application
My PSP
Identification of Beneficiary + amount
OK
cancel
3: Pay €5 to 1234 5678 9123 4567
My PSP
Authentication
Payment authorised by the Payer
OK
cancel
4: SCT Payment
Payer's PSP
Beneficiary's PSP

Figure 15: SCT 1 Consumer-to-Consumer SEPA Credit Transfer – Core

SCT 1 Consumer-to-Consumer SEPA Credit Transfer – Core	
Category	Consumer-to-Consumer (C2C), also applicable to C2B and B2B.
Communication type	Remote
Payment instrument	SEPA Credit Transfer
Payment initiation by	Payer
Prerequisites	Payer subscribes to Mobile Remote Payment service. (depends on how the PSP allows to receive instructions from the payer)
Payment confirmation mode	Determined by PSP
Customer Benefits	• Mobility for payer • Cheque (or cash) displacement
Challenges	• Inconvenience of importing credentials • Number and complexity of steps required to initiate the SCT • Potential for error • The beneficiary may find it inconvenient or undesirable to provide /reveal his/her IBAN and BIC. • The beneficiary has no immediate confirmation of irrevocability of payment • The beneficiary is dependent on SCT clearing cycle and services of his/her own PSP for execution of payment.

Table 18: SCT 1 Consumer-to-Consumer SEPA Credit Transfer – Core

5.2.2.2 SCT 2 Consumer-to-Consumer SEPA Credit Transfer – Alias (C2C, SCT)

Figure 16 introduces a possible example of a user experience for an SCT payment initiated by a mobile phone where a consumer (payer) makes a payment from his/her own payment account to the payment account of another consumer (beneficiary). Payer and beneficiary may be, and frequently are, customers of different PSPs (4-corner model[12], see sections 5.4.3.2 and 5.4.3.3).

In this scenario no upfront confidence between payer and beneficiary is assumed. A beneficiary alias (e.g. beneficiary mobile phone number) will be in place, making the input of the beneficiary details considerably more convenient for the payer.

In many circumstances, this use-case is also applicable for C2B, B2C and B2B (particularly small businesses).

The beneficiary must have his/her identification details 'registered' against his/her alias.
The payer's PSP must facilitate the use of aliases in its mobile SCT instruction acceptance process.

[12] Any reference to the 4-corner model should not be interpreted as meaning that 3-corner models could not be benefiting from the developments considered here.

The payer’s PSP must be able to identify the beneficiary’s PSP and payment account details from the beneficiary's alias via a common infrastructure (see section 5.4.2.3).

In the figure below, the following steps are illustrated:

1. The beneficiary provides his/her identification details to the payer, using a beneficiary's alias for convenience and/or security;
2. The payer provides the necessary information (amount, beneficiary’s alias, etc.) to his/her PSP via his/her mobile phone. This is typically done by using a specific mobile phone MRP application or by accessing a mobile browser;
3. The payer, once authenticated by his/her PSP, authorises the SCT instruction in compliance with the usual security requirements set out by that PSP;
4. The payer’s PSP establishes the beneficiary’s identification details and identifies the beneficiary’s PSP using the beneficiary’s alias through a common infrastructure;
5. The payers PSP then processes and submits the SCT to the beneficiary’s PSP which in turn will credit the beneficiary.

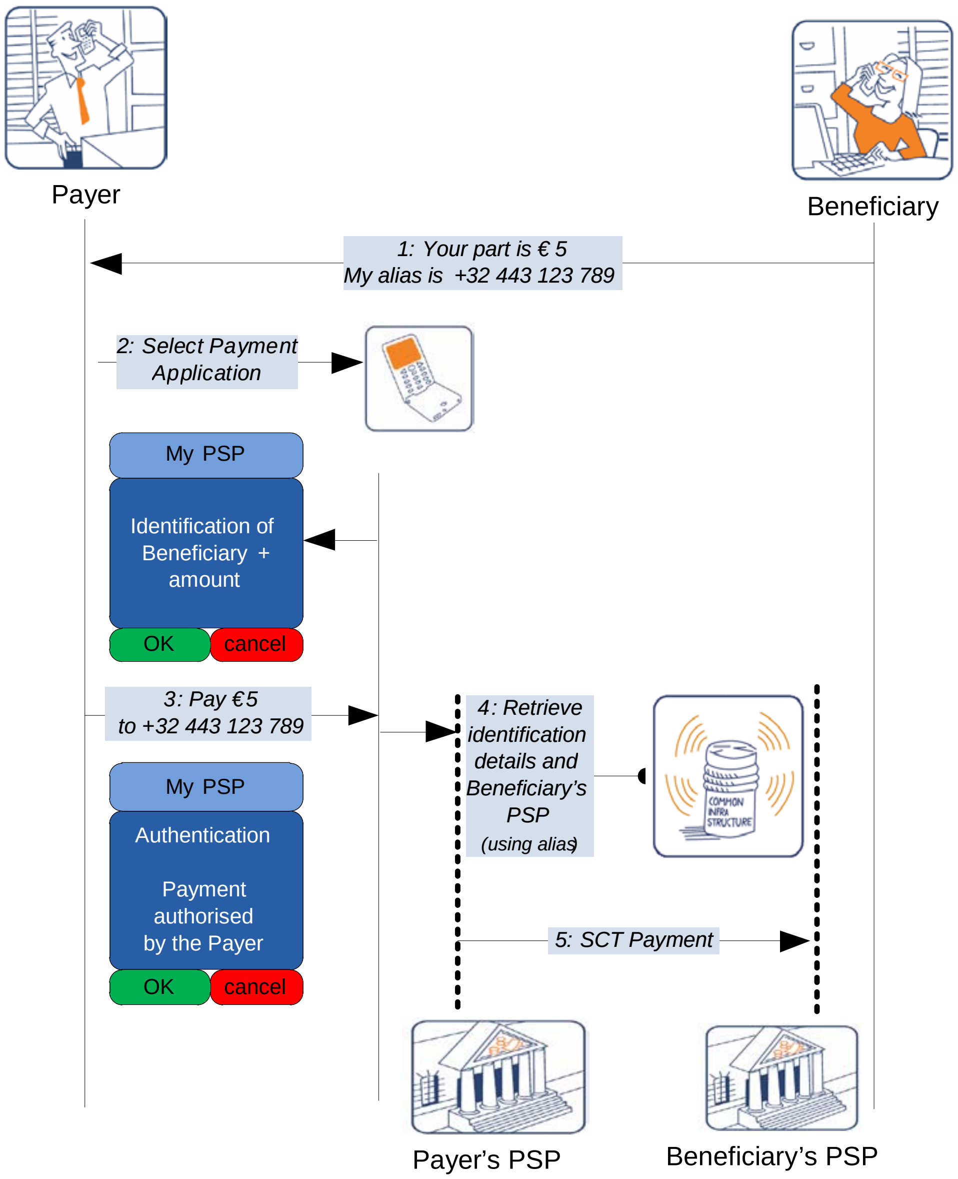

Payer
Beneficiary
1: Your part is € 5
My alias is +32 443 123 789
2: Select Payment Application
My PSP
Identification of Beneficiary + amount
OK
cancel
3: Pay €5 to +32 443 123 789
My PSP
Authentication
Payment authorised by the Payer
OK
cancel
4: Retrieve identification details and Beneficiary's PSP
(using alias)
COMMON INFRA STRUCTURE
5: SCT Payment
Payer's PSP
Beneficiary's PSP

Figure 16: SCT 2 Consumer-to-Consumer SEPA Credit Transfer– Alias

SCT 2 Consumer-to-Consumer SEPA Credit Transfer–Alias	
Category	Consumer-to-Consumer (C2C), also applicable to C2B and B2B
Communication type	Remote
Payment instrument	SEPA Credit Transfer
Payment initiation by	Payer
Prerequisites	• The beneficiary or the beneficiary's PSP has registered his/her identification details in a common infrastructure. • The payer's PSP must have access to the common infrastructure. • The payer's PSP must offer the alias-based mobile payment service.
Payment confirmation mode	Determined by PSP
Customer Benefits	• Convenience, mobility. • Beneficiary does not have to remember and reveal identification (IBAN, BIC) to the payer. • Cheque (or cash) displacement.
Challenges	• Agreement on alias format. • The set up and operation of the common infrastructure. • The beneficiary has no immediate confirmation of irrevocability of payment. • The beneficiary is dependent on SCT clearing cycle and services of his/her own PSP for execution of payment.

Table 19: SCT 2 Consumer-to-Consumer SEPA Credit Transfer– Alias

5.2.2.3 SCT 3A Consumer-to-Business SEPA Credit Transfer– Confirmation (C2B, C2C B2B SCT)

Figure 17 introduces a possible example of a user experience for an SCT payment initiated by a mobile phone where a consumer (payer) makes a payment from his/her own payment account to the payment account of a beneficiary. Payer and beneficiary may be, and frequently are, customers of different PSPs (4-corner model[13], see sections 5.4.3.2 and 5.4.3.3).

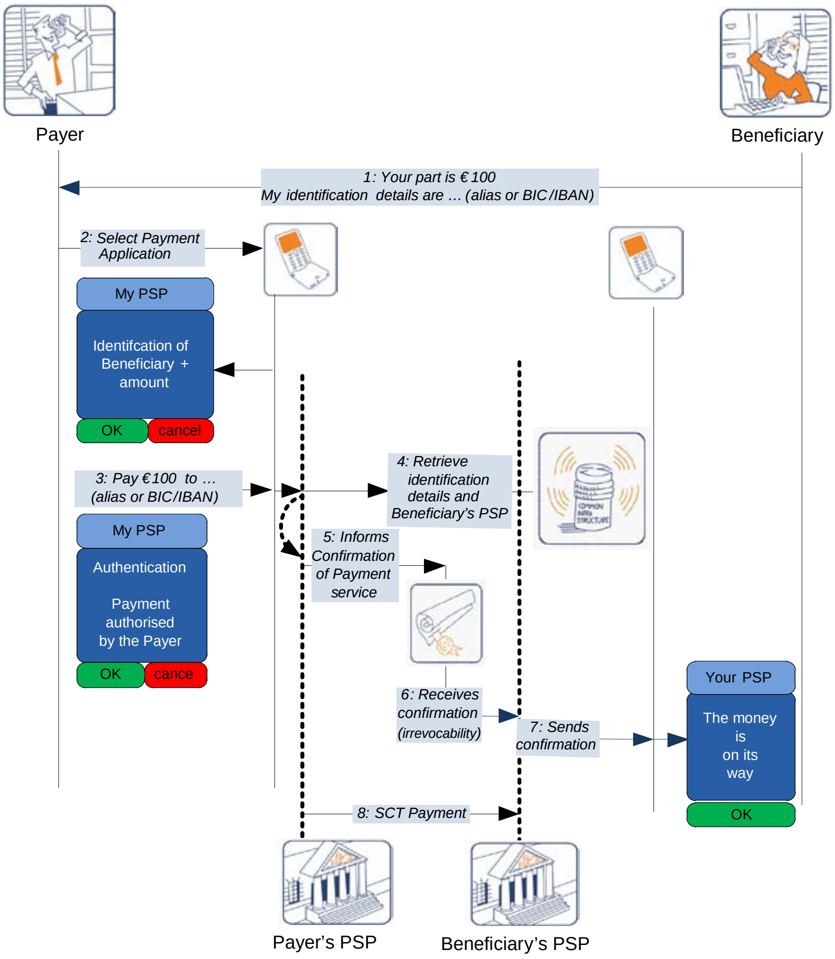
In this use-case, “Confirmation of payment” for the beneficiary is essential for SCT being an acceptable form of payment (e.g. a merchant needs a sufficient degree of assurance about the execution of the payment before delivering its goods or services). Typically, but not universally, this will be a consumer to business (merchant) C2B scenario. However, C2C situations (e.g. selling a car or other high value items) and B2B (e.g. between tradesmen) can be envisaged.

Ideally, but not necessarily, the beneficiary alias as defined in the previous scenario should be used. This use-case is also applicable for C2C, B2C and B2B (small businesses) subject to registration in a common shared "Confirmation of Payment" service.

[13] Any reference to the 4-corner model should not be interpreted as meaning that 3-corner models could not be benefiting from the developments considered here.

In the figure below, the following steps are illustrated:

1. The payer and the beneficiary agree upon the amount to be paid and the beneficiary provides his/her identification details to the payer possibly using an alias for convenience and/or security;
2. The payer provides the necessary information (amount, beneficiary's alias, etc.) to his/her PSP via his/her mobile phone. This is typically done by using a specific mobile phone MRP application or by accessing a mobile browser;
3. The payer, once authenticated by his/her PSP, authorises the SCT instruction in compliance with the usual security requirements set out by that PSP;
4. The payer's PSP establishes the beneficiary's identification details and identifies the beneficiary's PSP (e.g. using the beneficiary's alias) through a common infrastructure;
5. The payer's PSP informs the "Confirmation of Payment" service about the SCT payment including the beneficiary's identification details and corresponding PSP;
6. As a participant in the " Confirmation of Payment" service, the beneficiary's PSP receives confirmation that the SCT will be irrevocably made by the payer's PSP;
7. The beneficiary's PSP provides confirmation to the beneficiary;
8. The payers PSP then processes and submits the SCT to the beneficiary's PSP which in turn will credit the beneficiary.



Payer
Beneficiary
1: Your part is € 100
My identification details are … (alias or BIC/IBAN)
2: Select Payment Application
My PSP
Identifcation of Beneficiary + amount
OK
cancel
3: Pay €100 to … (alias or BIC/IBAN)
My PSP
Authentication
Payment authorised by the Payer
OK
cance
4: Retrieve identification details and Beneficiary's PSP
5: Informs Confirmation of Payment service
6: Receives confirmation (irrevocability)
7: Sends confirmation
Your PSP
The money is on its way
OK
8: SCT Payment
Payer's PSP
Beneficiary's PSP

Figure 17: SCT 3A Consumer-to-Business SEPA Credit Transfer– Confirmation

SCT 3A Consumer-to-Business SEPA Credit Transfer–Confirmation	
Category	Consumer-to-Business (C2B), also applicable to B2B.
Communication type	Remote
Payment instrument	SEPA Credit Transfer
Payment initiation by	Payer
Prerequisites	• A “Confirmation of Payment” service is established. • The payer's and the beneficiary's PSP must participate in the “Confirmation of Payment” service. • The beneficiary has registered to a notification service[14] with his/her PSP. • The payer must be enabled to instruct his/her PSP to avail of the “Confirmation of Payment” service.
Payment confirmation mode	Determined by PSP
Customer Benefits	• Convenience, mobility, speed • Cheque (or cash) displacement • The beneficiary has immediate confirmation of irrevocability of payment; this allows the beneficiary to release goods or services. Although the “Confirmation of Payment” service is immediate, the payment is not (necessarily).
Challenges	• The set-up and operation of the “Confirmation of Payment” service.

Table 20: SCT 3A Consumer-to-Business SEPA Credit Transfer– Confirmation

5.2.2.4 SCT 3B Consumer-to-Business SEPA Credit Transfer – Confirmation via e-Payment Service (C2B, SCT)

In this scenario, both the payer’s PSP and the beneficiary’s PSP belong to the same SCT based e-Payment Service which includes a “Confirmation of Payment” service. Moreover, the beneficiary is a registered merchant in the e-Payment Service. The payment flow is similar to an SCT transaction initiated via a PC or a tablet but here it is initiated via the mobile phone.

While this scenario requires the pre-registration of the beneficiary (merchant) to an e-Payment Service, it does have the advantage of the security for the beneficiary and convenience for the payer being provided as part of the same e-Payment Service.

Because the beneficiary (merchant) already has its PSP (or payment account) details registered with the e-Payment Service, the need for the use of aliases is eliminated. Also, as the e-Payment Service provides confirmation of payment to its registered merchants, the establishment of a separate “Confirmation of Payment” process for recipients becomes irrelevant.

When concluding a purchase through a mobile browser or an MRP application, the payer (consumer) simply selects the “e-Payment Service” option and his/her PSP from the list of

[14] A notification service is needed between the Beneficiary (merchant) and its PSP to receive confirmation of the payment from its PSP before releasing the goods or services to the payer.

participating PSPs. He/she will then be presented with a payment ‘instruction’ detailing the beneficiary and the amount, which is then authorised in accordance with his/her PSP’s normal requirements. In this use-case, both parties receive confirmation that the payment transaction has been executed.

In the figure below, the following steps are illustrated:

1. The payer, having made a purchase using a mobile device (mobile browser or application) selects the ‘e-payment’ option at the checkout;
2. A list of participating PSPs is then presented to the payer;
3. The payer selects his/her PSP from the list;
4. Through the e-Payment service, the payment details are ‘presented’ to the payer’s PSP. The payer is presented with a payment instruction from its PSP, outlining (at least) the name of the beneficiary and the amount of the payment to be made;
5. The payer, once authenticated by his/her PSP, authorises the SCT instruction in compliance with the usual security requirements set out by that PSP;
6. The payer’s PSP informs the e-Payment Service about the SCT payment including the beneficiary’s identification details and corresponding PSP. As a participant in the e-Payment Service, the beneficiary’s PSP receives confirmation that the SCT will be irrevocably made by the payer’s PSP;
7. The beneficiary’s PSP provides confirmation to the beneficiary;
8. The payers PSP then processes and submits the SCT to the beneficiary’s PSP which in turn will credit the beneficiary.

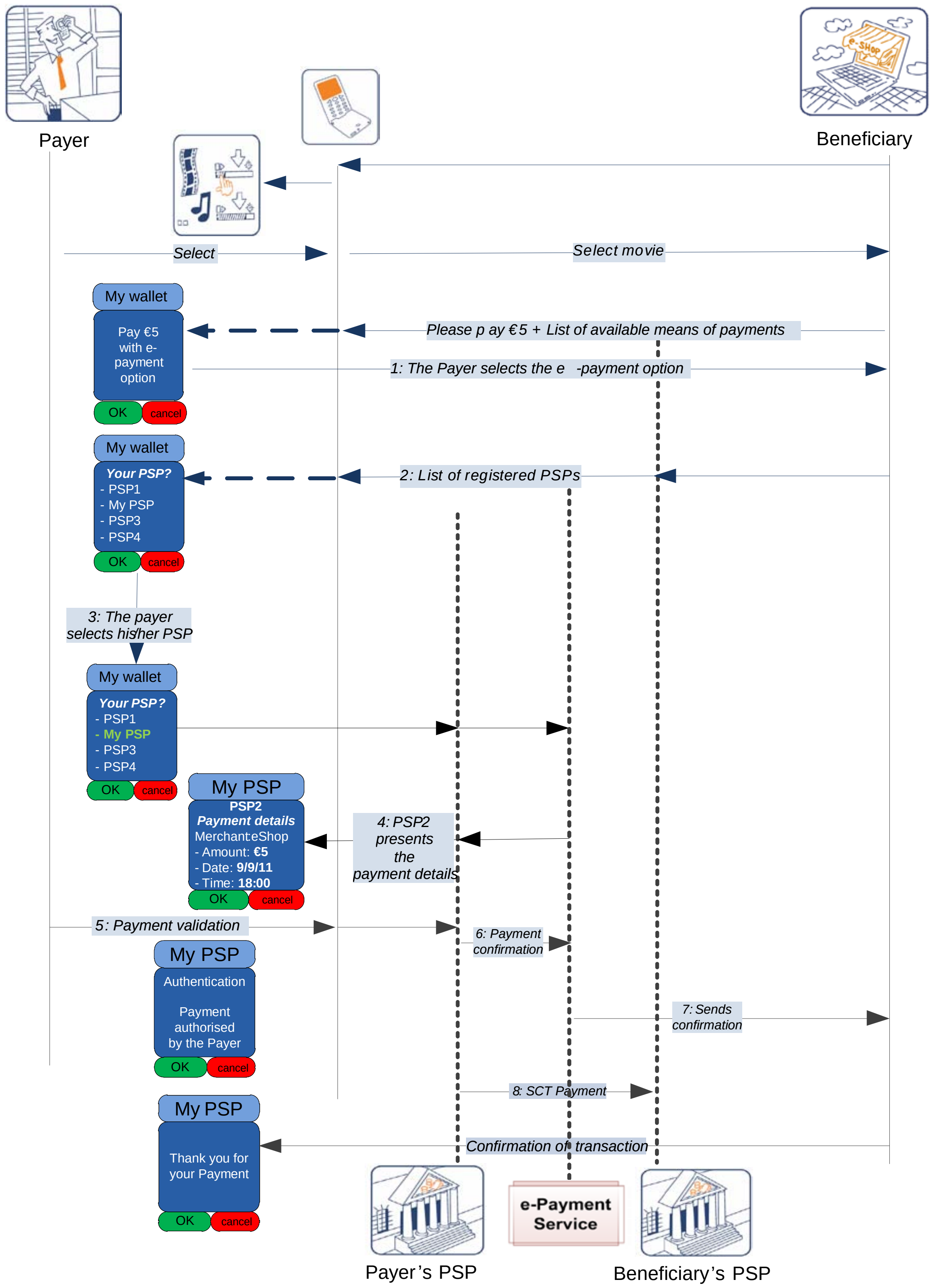


Figure 18: SCT 3B Consumer-to-Business SEPA Credit Transfer– Confirmation via e-Payment Service

SCT 3B Consumer-to-Business SEPA Credit Transfer - Confirmation via e-Payment Service	
Category	Consumer-to-Business (C2B)
Communication type	Remote
Payment instrument	SEPA Credit Transfer
Payment initiation by	Beneficiary (via e-Payment Service)
Prerequisites	An e-Payment Service is in place. Payer's and beneficiary's PSPs are registered within the same e-Payment Service. Beneficiary (merchant) is registered with the e-Payment Service.
Payment confirmation mode	Determined by e-Payment Service
Customer Benefits	• Convenience for the payer • Security for the beneficiary (merchant) • No need for the payer and the beneficiary to share credentials • e-Payment Service brings credibility and trust
Challenges	• Agreement on a "Confirmation of Payment" within an e-Payment Service (not mobile specific).

Table 21: SCT 3B Consumer-to-Business SEPA Credit Transfer – Confirmation via e-Payment Service

Note: In case the PSPs are registered with different e-Payment Services, there needs to be an interoperability structure (see also 5.4.3.3) defined to which both e-Payment Services adhere to. Moreover, in this case, this interoperability structure would also cater for a "Confirmation of Payment" Service.

5.2.2.5 SCT 4 Consumer-to-Consumer - u(rgent) SEPA Credit Transfer (C2C, uSCT)

Figure 19 introduces a possible example of a user experience for an 'urgent' SCT payment initiated using a mobile phone where a consumer (payer) makes a fast payment from his/her own payment account to the payment account of another consumer (beneficiary). Payer and beneficiary may be, and frequently are, customers of different PSPs. This scenario may also be particularly applicable for consumer-to-business transactions as the 'instant' nature of the transfer will allow the beneficiary to confirm receipt of funds with their PSP before 'releasing' the goods or services.

The SEPA SCT scheme does currently not offer a fast payment transfer. However, this does not preclude the development of a 'faster' or 'instant' service being provided by some or all SCT participants.

As more and more new entrants deliver greater choice to payment users, a demand for 'instant' execution of all transactions, particularly payments, is very likely. It is anticipated that PSPs will need to develop similar solutions if it is to remain competitive, particularly in the mobile space.

For the purpose of this scenario this concept is referred to as an "urgent" SEPA Credit Transfer (uSCT).

In many circumstances, this use-case is also applicable for C2B, B2C and B2B (particularly small businesses).

In the figure below, the following steps are illustrated:

1. The beneficiary provides his/her details to the payer, using a beneficiary's alias for convenience and/or security;
2. The payer provides the necessary information (amount, beneficiary's alias, etc.) to his/her PSP via his/her mobile phone. This is typically done by using a specific mobile phone PSP application or by accessing a mobile browser;
3. The payer, once authenticated by his/her PSP, authorises the SCT instruction in compliance with the usual security requirements set out by that PSP;
4. The payer's PSP then processes and submits the uSCT to the beneficiary's PSP which in turn will credit the beneficiary;
5. The beneficiary will be able to confirm with his/her PSP (almost instantly) that the payment has been received (e.g. mobile notification) and get access to the funds.

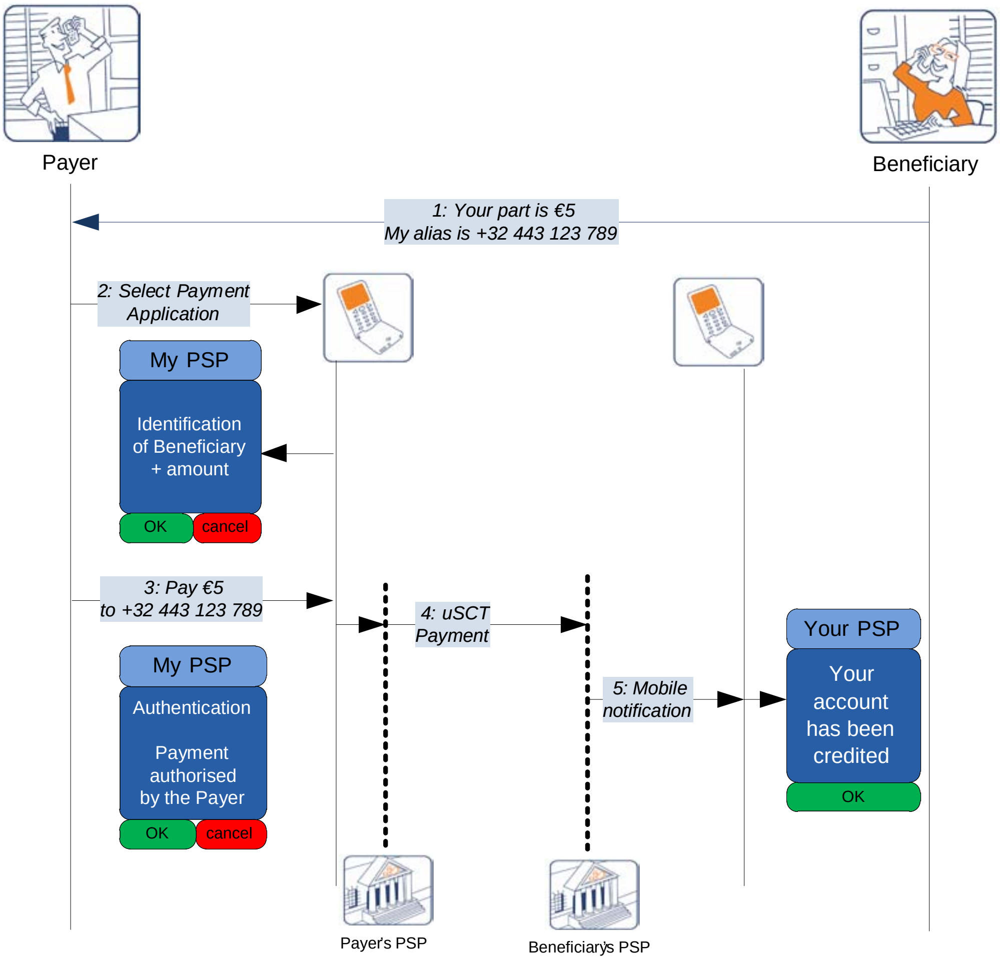

Payer
Beneficiary
1: Your part is €5
My alias is +32 443 123 789
2: Select Payment Application
My PSP
Identification of Beneficiary + amount
OK
cancel
3: Pay €5 to +32 443 123 789
My PSP
Authentication
Payment authorised by the Payer
OK
cancel
4: uSCT Payment
5: Mobile notification
Your PSP
Your account has been credited
OK
Payer's PSP
Beneficiarys PSP

Figure 19: SCT 4 Consumer-to-Consumer - u(rgent) SEPA Credit Transfer

Note: In this figure, the mechanism to retrieve the identification details of the beneficiary and his/her PSP from the mobile phone number is not represented.

SCT 4 Consumer-to-Consumer - u(rgent) SEPA Credit Transfer	
Category	Consumer-to-Consumer (C2C), also applicable to B2B, C2B and B2C.
Communication type:	Remote
Payment instrument	SEPA Credit Transfer
Payment initiation by	Payer
Prerequisites	The establishment of a SEPA uSCT
Payment confirmation mode	Determined by PSP
Customer Benefits	• Convenience, mobility, speed • Cheque (or cash) displacement • The beneficiary has immediate payment
Challenges	• The set up and operation of the uSCT

Table 22: SCT 4 Consumer-to-Consumer - u(rgent) SEPA Credit Transfer

This use-case corresponds in fact with the SCT 2 use-case whereby there is immediacy of payment using an urgent SEPA Credit Transfer (uSCT).

5.3 Ecosystem

5.3.1 Introduction

One of the purposes of the EPC is to promote the payment instruments of SEPA and therefore this white paper will only focus on ecosystems that comply with SEPA[15]. This covers both four and three corner models (see section 5.4.3) provided the latter use SEPA compliant formats. This also means that MRPs have to involve payment accounts.

It is desirable to reuse the infrastructure and business processes of the current SEPA instruments as much as possible. This means that the focus will be on how to use the mobile phone to initiate and feed SEPA transactions into the current payment infrastructures and then let those handle the payments according to the existing SEPA payment schemes.

5.3.2 Stakeholders

- The payer owns a SEPA payment account or a SEPA compliant card, and a mobile phone and must hold an active subscription with an MNO. Although this white paper focuses on payments initiated via the mobile phone, the conclusions may also apply to other mobile devices;
- The beneficiary owns a SEPA payment account and, where relevant, a SEPA compliant card. In case the beneficiary is a private customer / small business, there may be situations where it is beneficial for the beneficiary to own a mobile phone in order to receive value added services like notification;
- The PSP offers SEPA payment services compliant with regulatory/security requirements;

[15] Note that the use cases and service models introduced in this White Paper may also be applied to non SEPA areas.

- The MNO is responsible for securely routing messages, operating the mobile network, issuing and recycling mobile phone numbers which is important when the mobile numbers are used as alias;
- The payment system functions are both provided by a SEPA compliant payment scheme and a clearing and settlement mechanism (CSM);
- In case where a dedicated MRP application on the mobile phone is involved for the MRP, the MRP issuer is the PSP responsible for provisioning the application to the payer. Typically, the application is located in an SE in the mobile phone;
- An optional trusted third party (TTP) that operates a common infrastructure that could facilitate increased convenience and/or trust for the parties involved;
- The Trusted Service Manager (TSM) is a TTP acting on behalf of the SE issuers and/or the MRP application issuers to facilitate an open ecosystem in case an SE is involved to host the MRP application(s). Several TSMs may co-exist offering mutually-competing services.

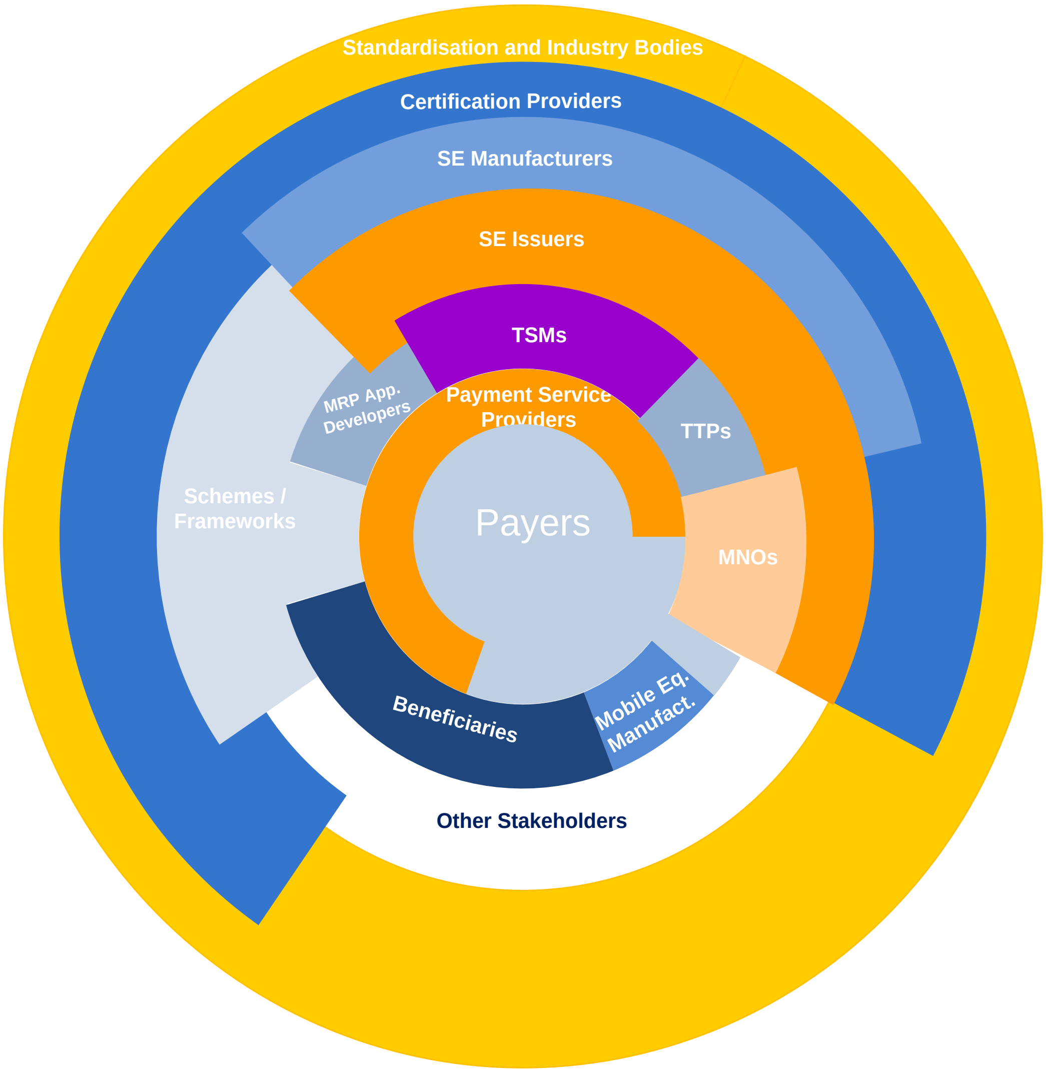


Figure 20: MRP business ecosystem

5.3.3 Service models

5.3.3.1 Payment Transaction

The C2B remote SEPA Card payments do not modify in any way the underlying SEPA Card payment transactions. Therefore, for these mobile remote SEPA Card payments, the service models of the SEPA Card payment transactions are unaffected.

For C2C remote SEPA Card payments, a new TTP operating the common card scheme P2P platform is needed for the retrieval of the identification details of the beneficiary (see 5.2.1.4). Although this TTP does not affect the underlying SEPA Card payment transactions, it might impact the service model.

The core C2C mobile remote SCT payments introduced in subsections 5.2.2.1 do not modify in any way the underlying SCT payment transactions; hence the existing service model remains valid.

The other use-cases introduced in subsections 5.2.2.2, 5.2.2.3 and 5.2.2.4 do not modify in any way the SCT payment transactions. However, the additional features introduced in these use-cases might impact existing SCT service models due to the introduction of new TTPs.

The final C2C use-case introduced in subsection 5.2.2.5 requires a change in the underlying SCT payment to cater for the immediacy. However, the SCT service model should remain unchanged.

5.3.3.2 Provisioning and Management

Depending on the particular MRP, the payment data stored on the mobile phone may range from pure payment credentials to a dedicated MRP application in an SE. Obviously, the provisioning and management of this payment data will vary accordingly. Some more information will be provided in section 7.3.

5.4 High level architecture

5.4.1 Introduction

For Mobile Remote Payments the following high level architecture may be considered independent whether the underlying payment instrument is SEPA Cards or SCT.

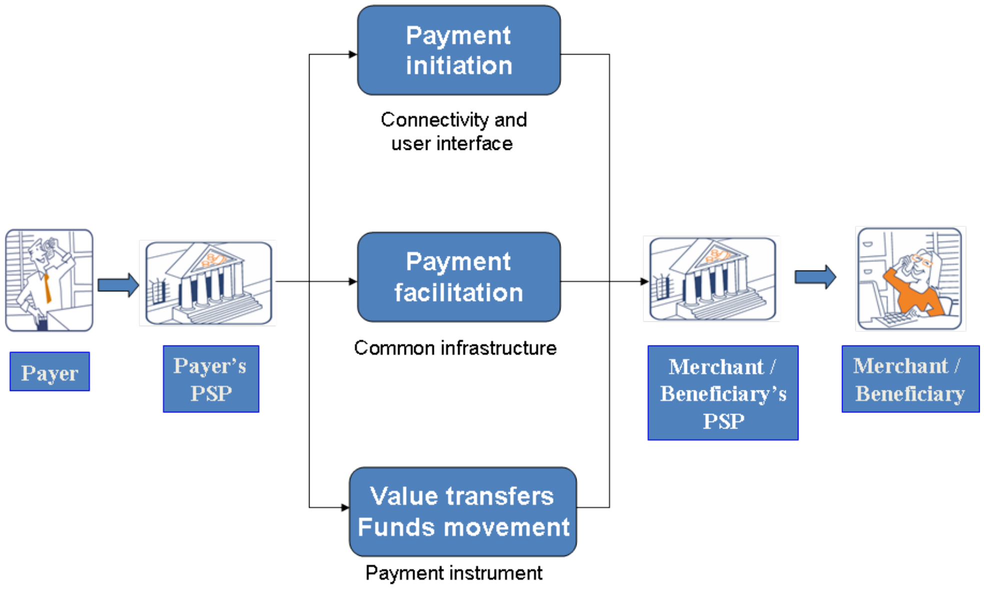


Figure 21: High level architecture for Mobile Remote Payments

In the figure above three layers may be distinguished:

- Layer 1: Connectivity and user interface used for payment initiation

  For the initiation of a Mobile Remote Payment, different means may be used such as a mobile browser, an SMS or a dedicated MRP application. Therefore, the connectivity and the user interface are critical components in ensuring a good user experience in this phase, but are in the competitive space.

  Also, further messages between the various parties to a remote payment transaction are crucial. For instance, a payer needs to know when a payment was authorised, approved, or completed while for the beneficiary it may be critical to know the status of a payment so that a decision can be made to release goods or services, or even acknowledge receipt to complete the transaction.

- Layer 2: Common infrastructure used for payment facilitation

  The payment facilitation component assists in identifying the payment instruments used by the two parties to a remote payment transaction. Various models are available. The two parties may voluntarily disclose payment instrument details (e.g. IBAN and BIC) to each other; they may rely on some form of linkage (through a shared common infrastructure) between mobile identifiers and payment instruments belonging to the transacting parties.

- Layer 3: Payment instrument for value transfers and funds movement

  Actual transfer of value or movement of funds will take place using existing SEPA payment instruments.

5.4.2 Layer 2 revisited

5.4.2.1 Introduction

The main purpose of the common infrastructure is to link the alias/unique identifier to the appropriate payment information details of the beneficiary to allow the appropriate routing of the payment transaction (e.g. to the beneficiary's payment account through IBAN/BIC for an SCT based transaction). It may be further used as a platform for value added services.

Depending on the usage of a common infrastructure (layer 2), there are two main models to be considered for Mobile Remote Payments in SEPA:

- The first model is based on the use of existing infrastructure and delivers direct interoperability between payers and beneficiaries;
- The second model is based on the establishment of a new centralised common infrastructure (in addition to the existing payment infrastructure). Note that some variations of the latter model may exist.

Both models invite the offering of value added services as mobile payment customers expect a fast and reliable service. Especially the notification process is considered valuable as e.g. merchants need confirmation of the payment before the shipment of the purchased goods or execution of services.

5.4.2.2 Direct interoperability model

The direct interoperability model is dependent on the payers/beneficiaries ability to forward all relevant payment information (BIC, IBAN, name, address, etc.) to his/her PSP or counterparty.
The only difference between this type of Mobile Remote SEPA Payment and a traditional SEPA payment is that the initiation of the payment is carried out via a mobile phone instead of for instance a PC or a paper form.

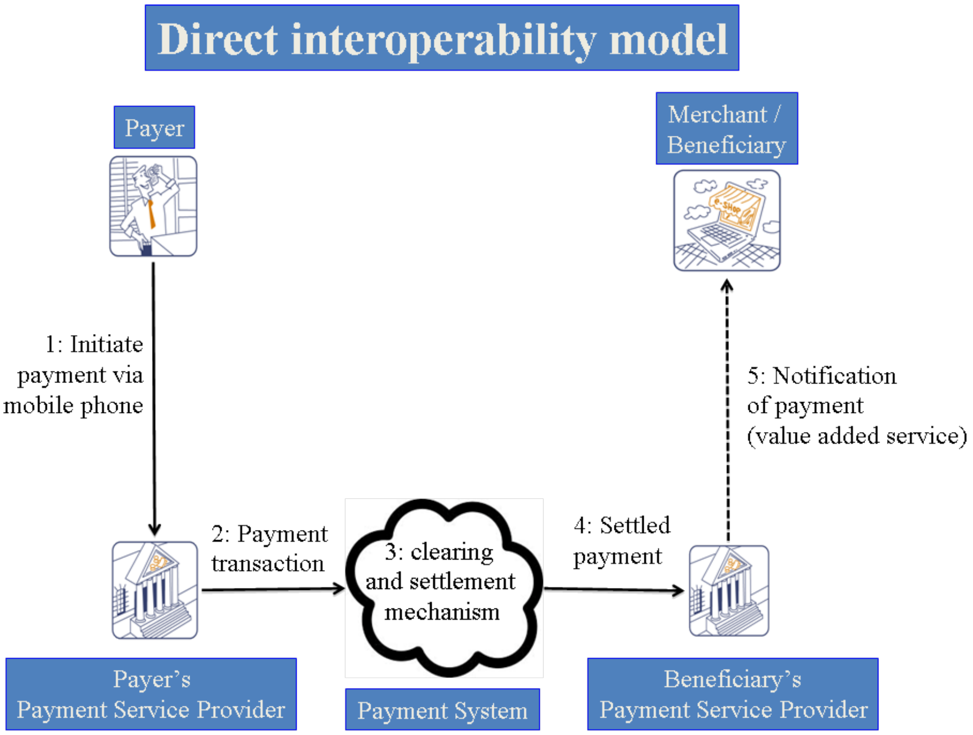

Direct interoperability model
Payer
Merchant / Beneficiary
1: Initiate payment via mobile phone
5: Notification of payment (value added service)
2: Payment transaction
3: clearing and settlement mechanism
4: Settled payment
Payer's Payment Service Provider
Payment System
Beneficiary's Payment Service Provider

Figure 22: Direct interoperability model

The advantages of the direct interoperability model are the low implementation and operational costs as all transactions are directly routed into existing channels, while the major disadvantage is the lack of convenience for the consumers. There is room for supplementing the service model with value added services, e.g. notification services.

5.4.2.3 Interoperability model based on a centralised common infrastructure

In this model interoperability is achieved by the usage of a centralised common infrastructure[16] which may have many shapes and purposes, and which could even be implemented in a distributed way. The primary purpose of this infrastructure is to act as a directory service or switch for routing purposes. Clearly this centralised infrastructure could also offer various value added services such as notification and delivery services which are, however, beyond the scope of this white paper.

[16] Note that common infrastructures could be proprietary (e.g., operated by card schemes).

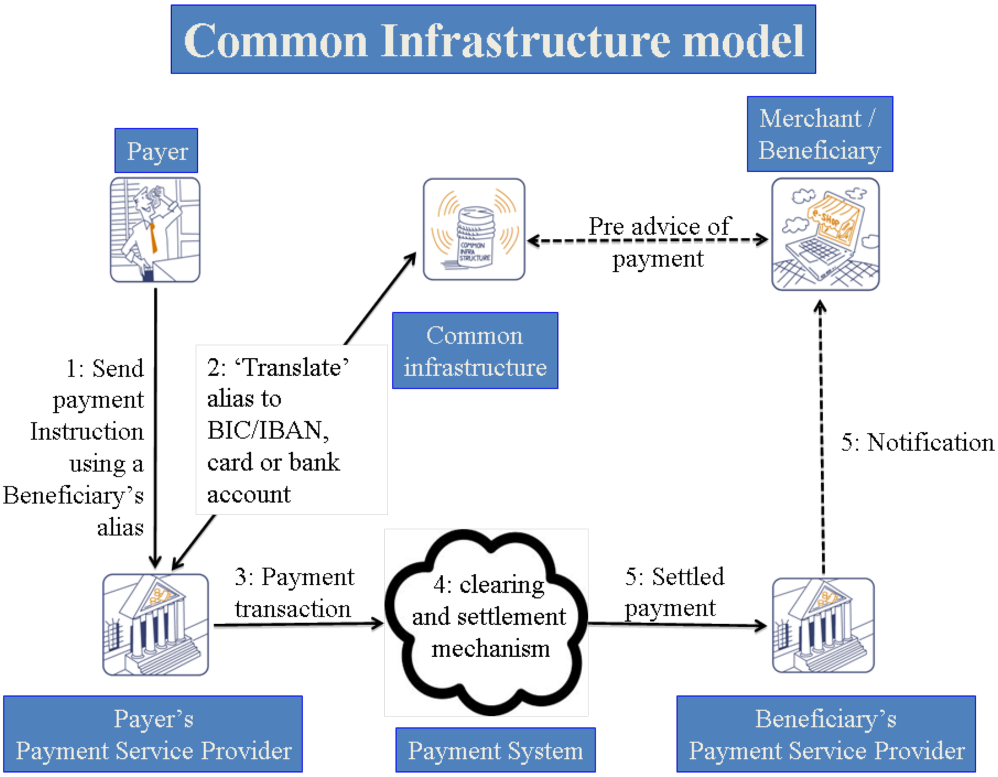

Common Infrastructure model
Payer
Merchant / Beneficiary
Pre advice of payment
Common infrastructure
1: Send payment Instruction using a Beneficiary's alias
2: 'Translate' alias to BIC/IBAN, card or bank account
5: Notification
3: Payment transaction
4: clearing and settlement mechanism
5: Settled payment
Payer's Payment Service Provider
Payment System
Beneficiary's Payment Service Provider

Figure 23: Centralised common infrastructure model

5.4.3 Layer 3 revisited

Based on this architecture, a number of different service models may be distinguished depending whether the payer and beneficiary do or do not belong to the same PSP and depending on whether the respective PSPs operate under the same or different payment schemes. In the next sections, the following models will be considered:

- The 3-corner model involving one single PSP;
- The 4-corner model involving different PSPs belonging to the same payment scheme;
- The 4-corner model involving different PSPs belonging to different payment schemes.

5.4.3.1 The 3-corner model

In this model, both the payer and beneficiary are customers of the same PSP which operates under a given payment scheme. The fact that only one PSP is involved might lead to simplifications in the implementation of the use-cases described in section 5.2, such as the identification of the beneficiary (which is known to the PSP), the payment confirmation and the immediacy aspect.

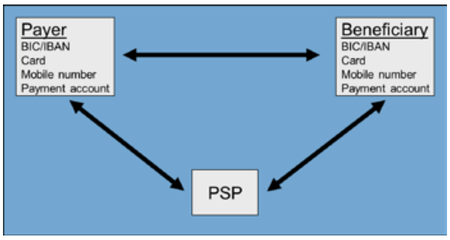


Figure 24: The 3-corner model

5.4.3.2 The 4-corner model under a payment scheme

In this model, the payer and the beneficiary are customers of different PSPs. But the assumption is made that both PSPs operate under one and the same payment scheme (card scheme or e-Payment service). This model might simplify again some aspects described in the use-cases provided in section 5.2, such as the identification of the beneficiary through the alias, the payment confirmation and the immediacy aspect.

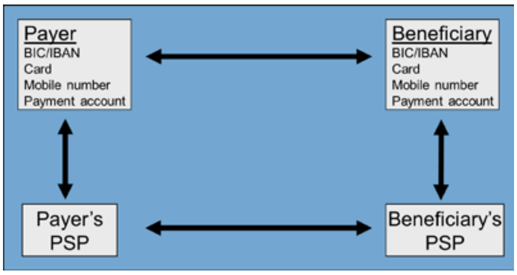


Figure 25: The 4-corner model under a single payment scheme

5.4.3.3 The 4-corner model involving different payment schemes

In this model, the payer and the beneficiary are customers of different PSPs and both PSPs operate under different payment schemes. Clearly both schemes need to adhere to a certain interoperability structure (implying that an agreement between the different payment schemes is in place). This is the most general model that may exist.

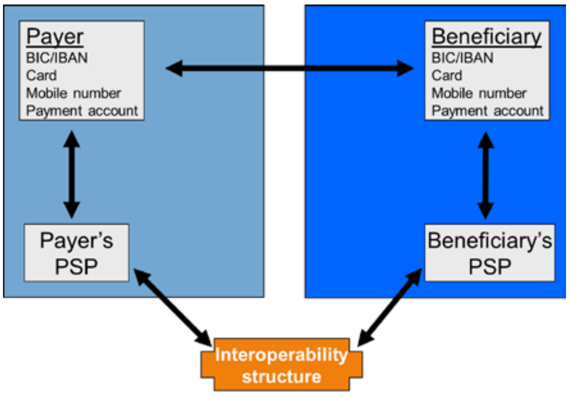


Figure 26: The 4-corner model involving different payment schemes

6 Secure subscription to mobile payment services

The use-cases for secure subscription to mobile payment services specified through this section are not based on the SEPA instruments and they are not subject to standardisation by the EPC. They are only introduced here to exhibit how subscriptions to mobile payment services can be easily and conveniently achieved and are illustrative examples only.

Mobile connectivity provides the potential for an almost immediate delivery of a new mobile payment service. However this "immediacy" is very much dependent on the elapsed time needed for the necessary checks and data preparation.

The registration and provisioning of a mobile payment application needs to be executed in a secure environment. Access to a mobile payment application would be easier for customers if they could use the existing trusted relationship between themselves and their PSP.

Please refer to [3] for concrete recommendations on implementing customer registration services while achieving compliance with the PSD [19].

6.1 Remote subscription

In this scenario, illustrated in

Figure 27, a PSP's customer (the consumer) subscribes to mobile payment services via an existing payment service using the web. In this way, the consumer is already authenticated and works within a secure environment.

This scenario makes the following assumptions:

- The current contract between the consumer and the PSP allows for a remote subscription (e.g. via e-banking) to new service extensions;
- The mobile phone has the necessary technical capabilities to conduct the desired type of mobile payment services.

The scenario could be conducted as follows:

1. The consumer first authenticates to the PSP as part of the usual remote session establishment.
2. Then the consumer initiates the mobile services subscription by entering his/her mobile phone number and indicating which particular service he/she wants to use.
3. Subsequently the PSP checks the technical eligibility of the mobile phone (including the UICC or/any other SE) directly or by using the services provided by a TSM.
4. The consumer then receives an SMS from the PSP on his/her mobile phone to signal this.
5. He/she opens the SMS and confirms he/she wants to start the service with the mobile phone receiving the message.
6. As soon as the consumer confirms, the service is fully provisioned and the mobile phone's display provides a confirmation to the consumer.

The provisioning of the service may include different features such as multiple applications which may be downloaded and installed in both the SE (e.g. payment application) and the mobile phone baseband (e.g. the end-user interface).

Further guidance will be provided in forthcoming implementation guidelines on mobile payments published by the EPC.

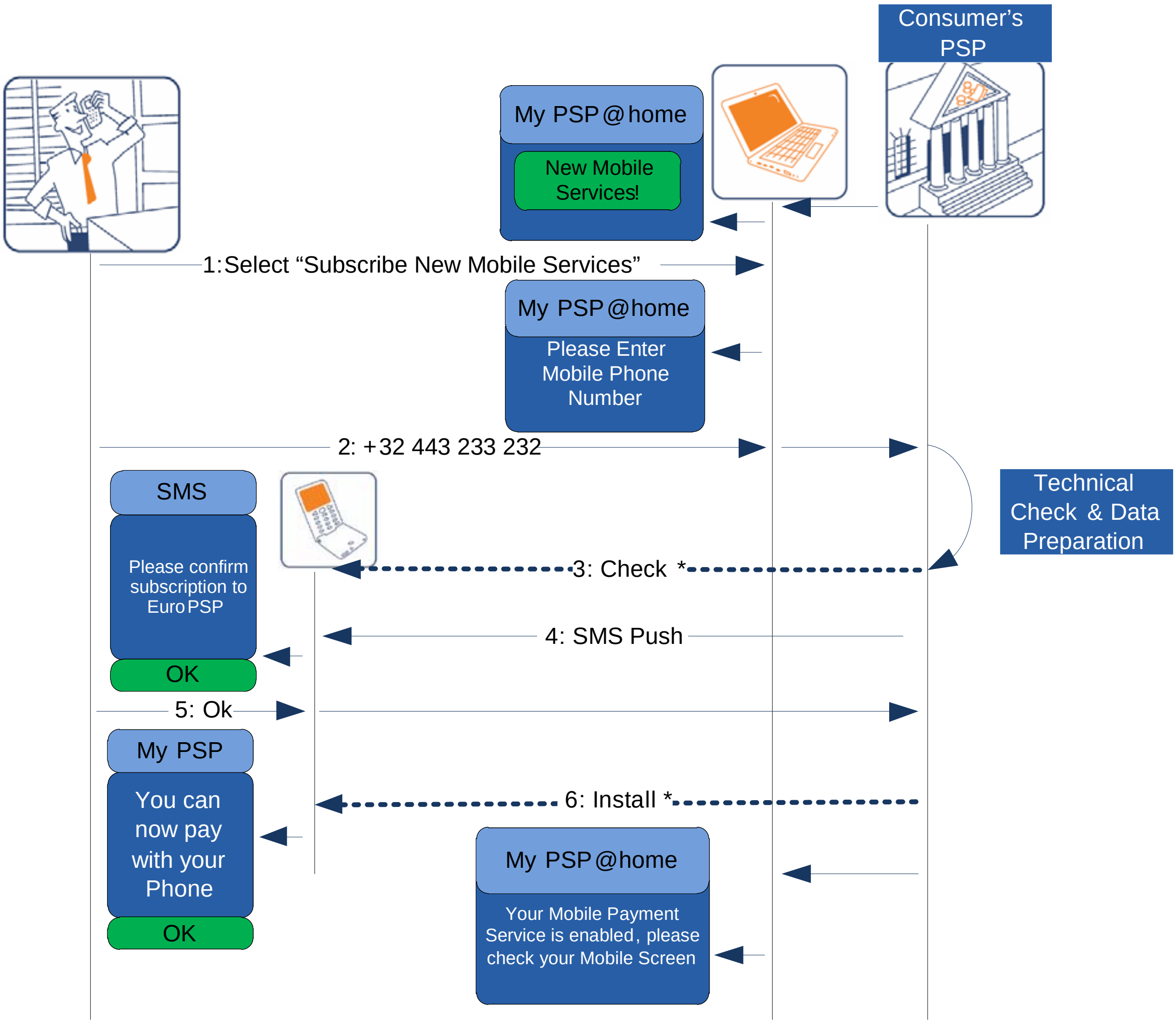

Consumer's PSP
My PSP@home
New Mobile Services!
1:Select "Subscribe New Mobile Services"
My PSP@home
Please Enter Mobile Phone Number
2: +32 443 233 232
SMS
Please confirm subscription to Euro PSP
OK
Technical Check & Data Preparation
3: Check *
4: SMS Push
5: Ok
My PSP
You can now pay with your Phone
OK
6: Install *
My PSP@home
Your Mobile Payment Service is enabled, please check your Mobile Screen

Figure 27: Example of remote subscription to mobile payment services

Note:

- Transactions marked with an asterisk may require further consumer interaction.

6.2 Subscription with self-service device

In this scenario, illustrated in Figure 28, a PSP’s customer (the consumer) subscribes to mobile payment services via a self-service device (e.g. an ATM). In this way, the consumer is already authenticated and works within a secure environment.

This scenario makes the following assumptions:

- The current contract between the consumer and the PSP allows for a self-service device - based subscription to new payment service extensions;
- The mobile phone has the necessary technical capabilities to conduct the desired type of mobile payment services.

The scenario is conducted as follows:

1. The consumer first authenticates to the ATM as part of the usual session establishment.
2. Then the consumer initiates the subscription by entering his/her mobile phone number and indicating which service he/she wants to use.
3. Subsequently the PSP checks the technical eligibility of the mobile phone (including the UICC or/any other SE) directly or by using the services provided by a TSM.
4. The consumer then receives an SMS from the PSP on his/her mobile phone to signal this.
5. He/she opens the SMS and confirms he/she wants to start the service with the mobile phone receiving the message.
6. As soon as the consumer confirms, the service is fully provisioned and the mobile phone’s display provides a confirmation to the consumer.

The provisioning of the service may include different features such as multiple applications which may be downloaded and installed in both the SE (e.g. payment application) and the mobile phone baseband (e.g. the end-user interface).

Further guidance will be provided in forthcoming implementation guidelines on mobile payments published by the EPC.

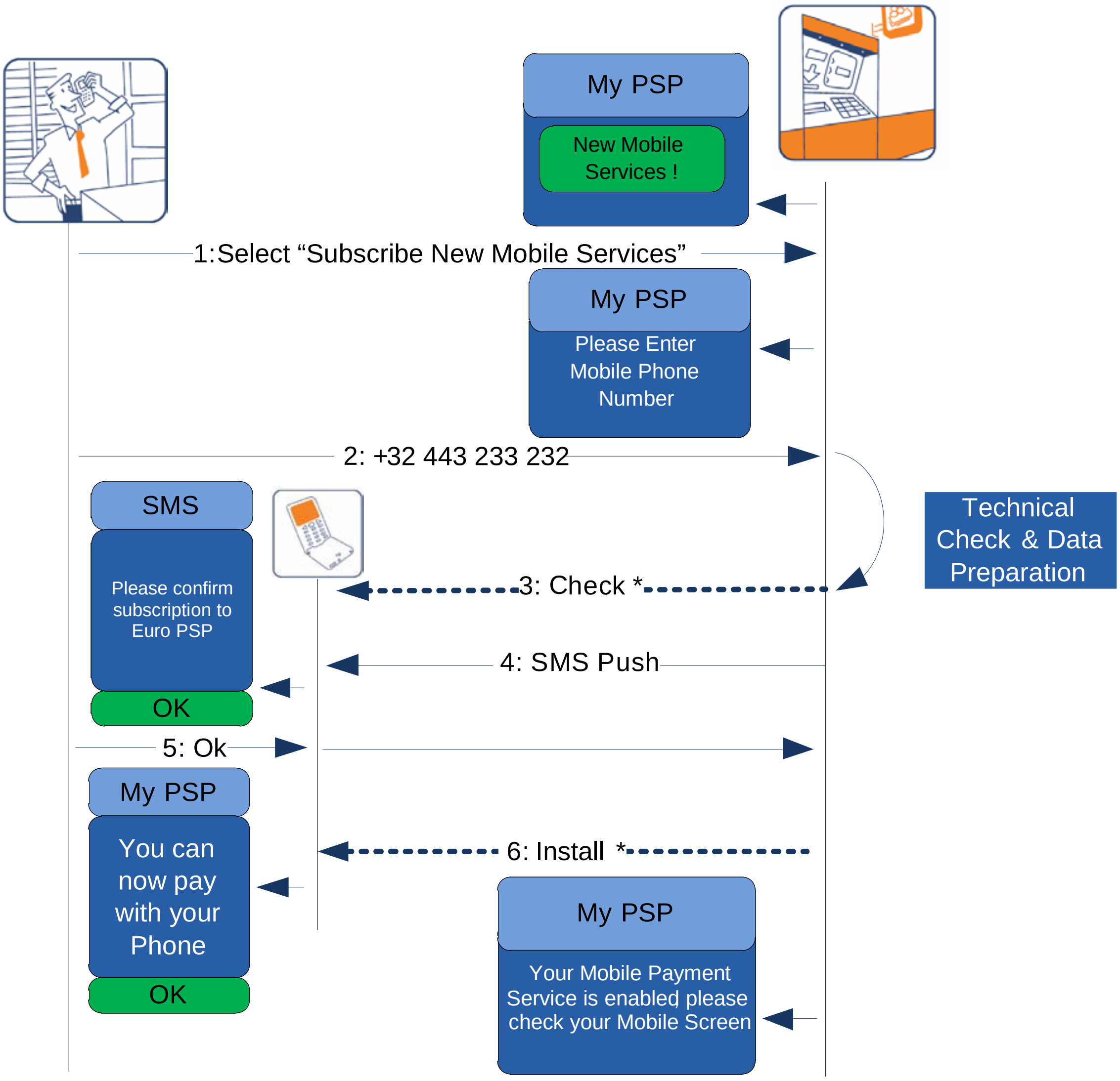

My PSP
New Mobile Services !
1:Select "Subscribe New Mobile Services"
My PSP
Please Enter Mobile Phone Number
2: +32 443 233 232
Technical Check & Data Preparation
SMS
Please confirm subscription to Euro PSP
OK
3: Check *
4: SMS Push
5: Ok
My PSP
You can now pay with your Phone
OK
6: Install *
My PSP
Your Mobile Payment Service is enabled please check your Mobile Screen

Figure 28: Example of ATM subscription to mobile payment services scenario

Note:

- Transactions marked with an asterisk may require further consumer interaction.

6.3 Subscription at the PSP's branch

In this scenario, illustrated in Figure 29, the subscription to mobile payment services is performed when the consumer visits his/her PSP's branch.

This scenario makes the following assumption:

- The mobile phone has the necessary technical capabilities to conduct the desired type of mobile payment services.

The scenario is conducted as follows:

1. The consumer notifies the branch clerk of his/her intention to subscribe to mobile payment services.
2. The customer then provides the mobile phone number to be enrolled as part of the registration information.
3. Subsequently the PSP checks the technical eligibility of the mobile phone (including the UICC or/any other SE) directly or by using the services provided by a TSM.
4. The new functionality is enabled remotely on the mobile phone and the consumer will simply discover a new payment application installed in his/her mobile phone.

The provisioning of the service may include different features such as multiple applications which may be downloaded and installed in both the SE (e.g. payment application) and the mobile phone baseband (e.g. the end-user interface).

Further guidance will be provided in forthcoming implementation guidelines on mobile payments published by the EPC.

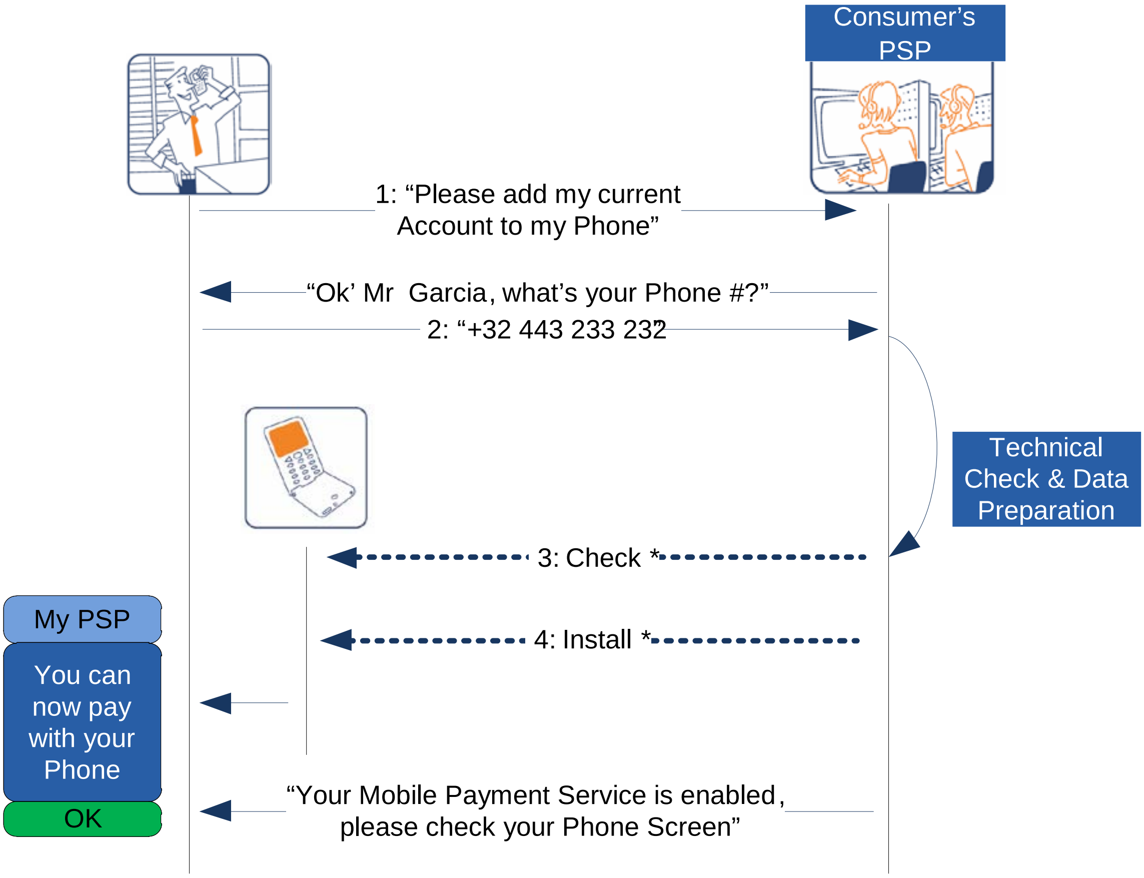

Consumer's PSP
1: "Please add my current Account to my Phone"
"Ok' Mr Garcia, what's your Phone #?"
2: "+32 443 233 232"
Technical Check & Data Preparation
3: Check *
4: Install *
My PSP
You can now pay with your Phone
OK
"Your Mobile Payment Service is enabled, please check your Phone Screen"

Figure 29: Example of in-person mobile payment service subscription use-case

Note:

- Transactions marked with an asterisk may require further consumer interaction.

7 Infrastructure

7.1 General

In this section the different infrastructure components are considered which are used for both MCPs and MRPs.

7.1.1 Mobile phones

Within SEPA, all deployed general-purpose mobile phones are either GSM or UMTS (also known as 3G). All UMTS mobile phones have mobile broadband capabilities, and virtually all new GSM mobile phones currently sold also support GPRS or EDGE, which also provide seamless access to Internet, albeit with a thinner bandwidth. These support the "UICC" (previously SIM), which is a tamper-resistant token, owned and provided by the MNOs, and fully standardised by ETSI. Whereas the UICC already manages the necessary confidential and cryptographic data to identify the user to the mobile network, the UICC can potentially also host MCP applications under the control of the PSPs.

A mobile phone may be used both for MCPs and MRPs depending on the requirements set on the phone. For example, a PSP providing the MRP service may only require SMS support from a phone whereas another PSP may require the download of its payment application to the mobile phone with a specific platform. In MCP the requirements on mobile phones are more complex: the NFC controller, an SE and interfaces to enable secure MCP applications shall be in place. In the absence of an SE (see section 7.1.3), MRPs may make use of the security features within the mobile phones such as SIMs and TEEs[17]. It is currently thought that these will not be sufficiently secure for MCPs.

Mobile phones are constantly being developed and feature an ever-increasing number of capabilities. Modern phones, known as "smart-phones", are based on general-purpose (open) computing platforms capable of achieving very complex tasks, they support colour screens in an ever-increasing size, and allow for PC-like Internet access capabilities. Significantly, the smart-phone is the main category of mobile devices that is currently growing in market share, and at a remarkable pace [11].

NFC, used for mobile contactless payments, is compatible with contactless card protocols[18]. NFC-enabled phones can interact with standard NFC readers (e.g. POI) and with other NFC-enabled devices. Accordingly, they have the potential to leverage any existing infrastructure for card-based contactless payment services.

Therefore, it is reasonable to assume that, in SEPA, present and future payment applications can effectively rely on a wide deployed base of mobile phones featuring rich remote management capabilities, Internet access, and high resolution colour screens capable of sustaining an adequate user experience.

7.1.2 End-user interface

[17] TEE is a Trusted Execution Environment is a secure area that resides in the main processor of the phone and guarantees that sensitive data is stored, processed and protected in a trusted environment.

[18] The main difference is that a contactless card is said to communicate "passively" i.e. without needing its own power source, while an NFC-enabled mobile phone can use its batteries for extra functionality.

Mobile payments are managed with a user interface on the mobile device. This interface includes for example an SMS or USSD application, a browser or a downloadable client application provided by the PSP. Mobile wallets (see section 8) provide such an interface and might be managed by the PSP but could also be provided by a TTP in which case PSPs can have a presence through their payment application AAUIs.

Even if the most advanced smart phones boast “great” colour displays and touch-based interfaces, the user experience remains strongly challenged by the necessarily-small form factor. For example, the mobile phone form factor effectively limits the amount of information that can be displayed at any given time and the ability of the user to enter complex text. Therefore, it is important to provide easy-to-use mobile phone interfaces with consistent user experience across all the supported mobile phone implementations.

7.1.3 Secure Elements

Enhanced security is enabled by a so-called Secure Element (SE) (a certified, tamper-resistant, stand-alone integrated circuit, i.e. a “chip”) to store the consumer’s personal data and payment details. The experience from card payments shows that the chip technology is an efficient and cost effective way of achieving enhanced security. Moreover, the current infrastructure for the evaluation and certification practices for chips and cards may be leveraged for the SEs.

A number of alternatives exist for the deployment of SEs (see Annex II – The Secure Element) in the mobile phone to support mobile payments. The main factors driving the choice of SE in this context are:

- control and management of the SE;
- intrinsic security properties;
- eligibility for formal security certification;
- integration within the mobile phone and connections to external interfaces such as contactless or remote protocols;
- availability (timelines and geographical market);
- support infrastructure (personalisation tools);
- possibility of deployment within the existing commercial supply chains for mobile phones;
- cost-effectiveness and economies of scale.

The choice of the type of SE has an impact on the mobile payment service model. Therefore, the EPC has focused on three types of SEs: the UICC, an embedded SE and the removable SE such as the micro SD card and has made a detailed analysis on different aspects of the service model for each of them (see section 4 [5]).

To provide further support on this subject, a dedicated annex has been introduced, (see Annex II – The Secure Element.

As introduced in section 4, the sensitive operations involved with an MCP require the usage of an SE. For MRP, the payer directly authenticates to a payment server according to his/her PSP's selected authentication method and this does not necessarily require the usage of an SE. However, wherever an SE is already present to support MCPs, it may be useful for MRPs to enhance the consumer convenience. Additionally, the usage of an SE for MRP may increase the security.

7.2 Infrastructure for MCP

In this section the different infrastructure components are considered which are used for MCPs only.

7.2.1 Transaction infrastructure

The infrastructure needed during the payment transaction for MCPs fully leverages the infrastructure already deployed for card payments. The investments to be made for acceptance of contactless cards can also be used for mobile contactless SEPA card payments.

7.2.2 Provisioning & management

The mobile contactless SEPA cards payment application is to be installed on a SE (see section 7.1.3). This implies that dedicated processes need to be defined for the provisioning and management of the said payment application, which may vary depending on the SE chosen. It is expected that existing card personalisation systems can be leveraged for the personalisation of the payment application. In order to achieve this, TSMs might be involved. For further guidance on this topic the reader is referred to [5] and [6].

7.2.3 MCP application

The MCP application is the software residing on the SE which implements the payment card functionality within the mobile phone under the responsibility of the MCP issuer according to the SEPA Cards Framework. It has direct access to the NFC interface and therefore it communicates directly with the POI. MCP applications are personalised and managed remotely by the MCP issuer or a TSM on its behalf (see section 5 in [5]).

MCP issuers can compete in their service offerings by customising the MCP application, user-oriented configuration functions and the (remote) management operations.

Further guidance on the MCP application is provided in section 6 of [5].

7.2.4 MCP application user interface

An MCP application may be supported by complementary applications residing on the mobile phone’s “main memory”, which are known as the MCP application user interface (AAUI) and which are dedicated to interact with the consumer (see section 7.3 of [5] for further considerations on this subject). The MCP issuer is responsible for this application, its security characteristics and the secure communication with the MCP application.

7.2.5 Point of Interaction

A POI is a hardware and/or software component in point of sale equipment that enables a consumer to use a card to make a purchase at a merchant. The point of sale terminal might be attended or unattended. New generations of POI systems are designed to allow devices other than cards to be used to make payments (e.g. mobile phones or PDAs).

However, most of the POI infrastructure is not yet enabled for NFC and this will require further upgrading. This upgrade should include the potential requirements beyond those already defined for contactless SEPA card payments to maximize the effectiveness of those investments. For example, while the requirements for hardware components are expected to be identical, the embedded software may have to be updated for supporting e.g. the adequate handling of mobile codes. The EPC is already actively involved on this issue with all the relevant standardisation bodies and stakeholders.

7.3 Infrastructure for MRP

In this section the different infrastructure components are considered which are used for MRPs only.

7.3.1 Transaction infrastructure

Infrastructures needed for mobile remote payment transaction may utilise the infrastructure already deployed for remote card or SCT payments (e.g. merchant web browsers, 3D secure, remote wallets, etc.). However, as identified in chapter 5.2, certain use-cases involve the implementation of a common infrastructure.

As mentioned before, the main purpose of the common infrastructure is to link the alias/unique identifier to the appropriate payment information details of the beneficiary to allow the correct routing of the payment transaction. It may be further used as a platform for value added services.

Depending on the usage of a common infrastructure (layer 2), it is explained in section 5.4.2 that two main models could be considered for MRPs in SEPA. Both models invite the offering of value added services as mobile payment users expect a fast and reliable service. The notification process is considered especially valuable as e.g., merchants need confirmation of the payment before the shipment of the purchased goods or execution of services.

For both models the MRP issuers have the responsibility to enrol customers to the various MRP payment services.

The main purpose of the centralised common infrastructure is to link the alias/unique identifier to the appropriate payment information details of the beneficiary to allow the correct routing of the payment transaction. As a minimum the common infrastructure should store the alias/unique identifier and the name, IBAN and the BIC of the beneficiary. It may further be used as a platform for value added services.

This centralised common infrastructure might be implemented in different forms such as (but not limited to):

- As a central directory or database which allows the payer's PSP, having received the alias/ unique identifier of the beneficiary, to retrieve the corresponding details of the beneficiary's PSP / account / card (e.g. name, IBAN and/or BIC in case of SCT). In this way the payer's PSP is able to send the payment transaction to the beneficiary's PSP / account.

  The retrieval of the beneficiary's details might be implemented within two different options:
  - The alias/unique identifier of the beneficiary points to the URL of the PSP's beneficiary. In that case, the mapping between the alias/unique identifier and the details of the beneficiary is performed by the beneficiary's PSP.
  - The alias/unique identifier of the beneficiary directly points to the details of the beneficiary.

- As a central switch which allows the payer's PSP, having received the alias/unique identifier of the beneficiary, to send this information to the switch. The switch will link this information to the corresponding details of the beneficiary's PSP/account card (e.g. IBAN and/or BIC in case of SCT) and will then route the payment transaction to the beneficiary's PSP/account.

From a security perspective, it is clear that the common infrastructure needs to offer appropriate access control, confidentiality, integrity and availability. This may include meeting the legal regulations related to privacy. Moreover, the common infrastructure needs to be reliably maintained in order to guarantee the accuracy and freshness of the information.

7.3.2 Alias

The concept of an alias has been introduced in a number of use-cases in sections 4 and 5. It is basically a pseudonym that allows to uniquely identifying the beneficiary's payment account. In the case of SCT, it allows the link to the beneficiary's name, BIC and IBAN. For mobile remote card payments, it allows a unique identification of the beneficiary's payment account (e.g. using a mobile phone number). Note that an alias as identification of the payer may also be used.

7.3.3 Storage of MRP data and application in the mobile phone

In the following section, a distinction will be made between the storage of remote payment related data/credentials and the hosting of a remote payment application on the mobile phone. The storage of remote payment related data is referring to the storage of data on the mobile phone as a convenience to the consumer instead of entering it by hand at the transaction time. An MRP application is, in analogy with an MCP application, a dedicated software package that dynamically generates transaction data.

7.3.3.1 Storage of MRP related data/credentials

The mobile phone can be used to store static data/credentials both for remote SCT and SCP payments. If there are security requirements for these data (integrity and/or confidentiality), the data needs to be stored in a trusted environment, such as an SE. These data may be stored by the payer or his PSP. If stored in a trusted environment, it typically needs some access control, e.g. a form of authentication, such as a dedicated code by the payer or the PSP's MRP application management function.

7.3.3.2 Hosting of an MRP application

In some implementations of MRPs, the hosting of a dedicated MRP application in the mobile phone may be required. If this application has active security features, (e.g. cryptographic functions) the hosting shall be done in an SE. As with MCP, this MRP application requires full life cycle management by the payer's PSP, including provisioning, activation, personalisation, etc. (see [21]).

The payer's PSP might delegate some of these functions to a TSM. Similar to MCP, different requirements for the roles fulfilling these functions will apply (see [15] and [18].

7.3.3.3 Provisioning & management

The mobile remote SEPA payment might require the installation of a dedicated application on an SE (see section 7.1.3). This implies that dedicated processes need to be defined for the provisioning and management of the said payment application, which may vary depending on the SE chosen. In order to achieve this, TSMs might be involved. For further guidance on this topic the reader is referred to forthcoming MRP Interoperability Implementation Guidelines.

7.3.4 MRP application user interface

Even if the most advanced smart phones boast “great” colour displays and touch-based interfaces, the user experience remains strongly challenged by the necessarily-small form factor. For example, the mobile phone form factor effectively limits the amount of information that can be displayed at any given time and the ability of the user to enter complex text. Note that for the initiation for mobile remote payments different means may be used such as a mobile browser, an SMS or a dedicated AAUI.

The EPC will address this topic in more detail in forthcoming MRP Interoperability Implementation Guidelines.

7.3.5 Merchant interface

Generally, merchants have different ways for customers to make purchases which will be referred to as "purchase contexts" in this document. For example, the merchant may offer the use of SMS, provide a mobile website, have a dedicated mobile application (e.g. for games) or accept a preregistered alias (e.g. a mobile phone number) in a similar way to the traditional POI environment.

A basic requirement from both the merchant and the consumer perspective is that the purchase and payment processes provide a good user experience. In order to achieve this, it is important to ensure that the combination of an MRP instrument and the mobile phone are suitable for the particular purchase context.

A PSP will specify certain requirements on the consumer's mobile phone, based on the MRP implementation. In the simplest cases it is sufficient for the consumer to have SMS service availability, or to be able to use the Internet browser of the mobile phone (mobile browser). In other set-ups the PSP may require consumers to download a mobile application e.g. for payment instrument selection, authentication and other possible features.

7.3.6 Mapping the MRP use-cases on the infrastructure

In this section, a mapping will be provided of the use-cases described in section 5.2 on the three layer architecture introduced in section 5.4.1. Depending on the use-cases, the payment might be initiated in layer 1 through different ways (see section 5.4.1), such as mobile payment via a browser, mobile wallets, with or without strong authentication.

For each use-case, the following table lists the components to be added in layer 2 (e.g. common infrastructure) and the potential for new services in layer 3 (e.g. payment confirmation, immediacy of payment). Note that layers 2 and 3 are in the cooperative space, whereas layer 1 remains in the competitive space.

Three layers Use cases	Layer 1 payment initiation connectivity and user interface	Layer 2 payment facilitation common infrastructure	Layer 3 value transfers and funds movement payment instrument
SCT1	e.g. via mobile browser or via a dedicated MRP application	no	existing SCT
SCT2	e.g. via mobile browser or via a dedicated MRP application	yes common infrastructure	existing SCT
SCT3A	e.g. via mobile browser or via a dedicated MRP application	yes in case an alias is used	existing SCT + confirmation of payment service
SCT3B	e.g. via mobile browser or via a dedicated MRP application	yes in case an alias is used	existing SCT + confirmation of payment service via e-payment service
SCT4	e.g. via mobile browser or via a dedicated MRP application	yes in case an alias is used	existing SCT + Immediate payment
SCP1	e.g. via mobile browser	no	existing SCF
SCP2	via mobile wallet	no	existing SCF
SCP3	using strong authentication in payment initiation , e.g. by using a dedicated application through a mobile wallet	no	existing SCF
SCP4	optional usage of mobile wallet	yes common infrastructure	existing SCF

Table 23: Mapping of uses cases onto three layers MRP architecture

8 Mobile wallets

8.1 Definition

Similar to the physical world, a “digital” wallet is basically holding identification information on the wallet holder, on payments instruments accessible to the wallet holder and optionally personal information items belonging to the holder (e.g. pictures, documents, etc.). This may include information related to ID cards, digital signatures and certificates, logon information and billing and delivery addresses as well as payment instrument related information such as SCT and SDD products and payment cards (prepaid/purse, debit, credit). Furthermore it may also include other applications such as loyalty, transport or ticketing.

A “digital” wallet will be based on technical infrastructures (hardware and software) allowing the secure storage, processing and communication of the information described above provided by the wallet holder and/or the wallet provider and/or the (payment) application provider.

A “digital” wallet allows the holder to access the applications and the data without impacting their security and to maintain the various applications in the wallet. Moreover, the wallet holder expects a high availability of the wallet service.

The “digital” wallet will normally be implemented in the equipment used by the wallet holder. Thus the holder will have a direct control over his/her wallet. However a “digital” wallet could also be implemented as a remote wallet in a “Software as a Service” delivery scheme.

Besides the technical and security requirements that have to be fulfilled when using/offering wallets, the question of ownership of the wallet has to be clarified as it will be implementation dependent.

Therefore, the following definitions may be derived.

“A digital wallet is a service allowing the wallet holder to securely access, manage and use identification and payment instruments[19] *in order to initiate payments. This service may reside on a device owned by the holder e.g. a mobile phone or a PC or may be remotely hosted on a server but is anyway under the control of the holder.”*

“A mobile wallet is a digital wallet which resides on the mobile phone.”

A further vision and general reflection on mobile wallet may be found in [17].

8.2 Mobile wallets and mobile payments

In the context of this document the most relevant issue is the interaction between mobile wallets and mobile payments and, more specifically, the influence of mobile wallets on the user experience of a consumer.

[19] This definition allows to avoid confusion with electronic purses which are only one of the applications/payment instruments that could be contained in a digital wallet

Even still, in a starting phase for mobile payments, it is important to consider a range of situations: from the simpler ones, where a single payment application is available on the mobile phone, to complex ones, where more payment applications of different nature (SE with card information for NFC payments, card information for remote payments, virtual account, etc.) are stored on the mobile phone.

8.3 Usage of mobile wallets for mobile contactless and remote payments

From a consumer perspective the wallet is basically an application (or part of it) that allows him/her to securely access, manage or even register information relevant for payment(s) (basically personal information needed to identify the holder and information needed to identify and use payment instrument(s)), and to store this information in a secure way. The relevant information needs to be accessible anytime when the consumer wants to make a payment.

The wallet must, at least, cover the following functionality:

- An interface to register personal and payment instruments data (on the mobile)
- A data repository to store the data (on the mobile)
- An interface allowing user to select the payment instrument
- An interface allowing the user to use the payment instrument (can be one interface managing all payment means or different interfaces for different means)
- An interface for managing and updating stored data (update, cancellation, etc.).

As mentioned above, the mobile wallet application can be very simple, in the case of an application designed to store and manage information for a single payment instrument, or, more complex, in the case of different payment means. In case different payment means are stored in the wallet, it must, at least, allow the consumer to select, at any given time, the payment mean she/he wants to use.

On top of that, it is desirable that the wallet allows defining a default payment mean – one for all or even better, one for every type of payment situation (e.g. prepaid card X for contactless payments, credit card Y for remote payments, etc.).

Conceptually, a mobile wallet can be provided by the PSP that issues the payment means with the scope of managing only that specific payment means, or different payment means by the same PSP. Alternatively, the mobile wallet can be provided by a TTP but shall be conceived in to be able to manage payment means issued by multiple payment service providers.

Different possibilities can be expected: consumers that install on their mobile phone different apps in order to manage different payment means together with consumers that manage different payment means with a single application.

It would be desirable that the consumer has the freedom to choose how he/she prefers to organise and to use her/his wallet; payment service providers should allow consumers to manage (register and use) their payment means on every wallet[20].

The EPC plans further work on different aspects of mobile wallets.

[20] provided that the appropriate policies (e.g., security) are met.

9 Standardisation and industry bodies

Mobile SEPA payments require the careful coordination of standards and specifications defined within several disciplines and issued by a heterogeneous group of standardisation and industry bodies. Next to the EPC, the most relevant are:

- **ISO**

The International Organization for Standards (ISO) is the world's largest developer and publisher of International Standards. ISO has different committees which specify technical standards used in mobile payments such as standards for integrated circuit cards, communication protocols such as NFC, security mechanisms and is also is involved with mobile payments in ISO TC68 SC7 WG10. (http://www.iso.org/)

- **ETSI**

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies, including fixed, mobile, radio, converged, broadcast and Internet technologies. ETSI defines GSM, UMTS telecommunication protocols and the UICC including all the access protocols. (http://www.etsi.org)

- **EMVCo**

EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, MasterCard and Visa. (http://www.emvco.com/)

- **IETF**

The Internet Engineering Task Force (IETF) is a large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF defines the core for all Internet protocols. (http://www.ietf.org/)

- **GlobalPlatform**

GlobalPlatform (GP) is the leading, international association focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-service model implementations, which delivers benefits to issuers, service providers and technology suppliers. (http://www.http://www.globalplatform.org/)

- **GSMA**

The GSMA represents the interests of the worldwide mobile communications industry. Spanning more than 200 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organisations. The GSMA is focused on innovating, incubating and creating new opportunities for its membership, all with the end goal of driving the growth of the mobile communications industry. (http://www.gsmworld.com/)

- **Mobey Forum**

Mobey Forum is a global, financial industry driven forum, whose mission is to facilitate banks to offer mobile financial services through insight from pilots, cross-industry collaboration, analysis, experience-sharing, experiments and co-operation and communication with relevant external stakeholders. (http://www.mobeyforum.org/)

- **NFC Forum**

The Near Field Communication Forum is a non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs. (http://www.nfcforum.org/)

- **PCI**

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. (https://www.pcisecuritystandards.org)

- **W3C**

The World Wide Web Consortium (W3C) is an international community which develops Web standards. Its mission is to lead the Web to its full potential. (www.w3.org)

10 Conclusions

Role of EPC

The role of the EPC is to contribute to the evolution of an integrated market for payments in Europe through helping in or facilitating the development and promotion of standards, best practices and schemes. Mobile phones have achieved full market penetration and rich service levels making this the ideal channel for promoting the use of SEPA payment instruments.

This 2nd edition of the White Paper provides a high-level overview of mobile payments specifically dealing with:

- Mobile contactless payments
- Mobile remote payments.

The mobile phone is primarily used for the payment initiation while the EPC is using existing SEPA instruments for the underlying payments themselves.

Analysis and Prioritisation

Having analysed many payment categories for both “contactless” (proximity) and “remote” mobile payments, the following are viewed as EPC's priorities in the area of mobile payments:

- Mobile Contactless SEPA Card Payments;
- Mobile Remote SEPA Card Payments;
- Mobile Remote SEPA Credit Transfers.

Mobile Proximity Payments

For mobile contactless SEPA card payments, the choice of SE has a major impact on the service model and the roles of the different stakeholders.

The EPC has published MCP Interoperability Implementation Guidelines to support these stakeholders [5].

Mobile Remote Payments

Three primary challenges have been identified:

- Convenience of transaction initiation and beneficiary identification for payments initiated by the payer;
- Certainty of fate of the payment for the beneficiary;
- Immediate (or very fast) payments.

Next Steps

While many of the identified challenges are not specific to the mobile channel, an early and definitive resolution is key if SEPA payment instruments are to become successful in the mobile channel. In this regard, the EPC intends to focus on the development of Mobile Remote Payments Interoperability Guidelines.

Annex I – SEPA Payment Instruments

The payment instruments promoted by the EPC are:

- **SEPA Credit Transfer (SCT)**

The SCT Scheme enables payment service providers to offer a core and basic credit transfer service throughout SEPA, whether for single or bulk payments. The scheme's standards facilitate payment initiation, processing and reconciliation based on straight-through-processing. The scope is limited to payments in euro within SEPA countries, regardless of the currency of the underlying accounts. The credit institutions executing the credit transfer must be a Scheme participant; i.e. both must have formally adhered to the SCT Scheme. There is no limit on the amount of a payment carried out under the Scheme.

The SCT Scheme Rulebook [SCT] and the accompanying Implementation Guidelines are the definitive sources of information regarding the rules and obligations of the Scheme. In addition, a document entitled 'Shortcut to the SEPA Credit Transfer Scheme' is available which provides basic information on the characteristics and benefits of the SCT Scheme.

- **SEPA Direct Debit (SDD)**

The Core SDD Scheme - like any other direct debit scheme - is based on the following concept: "I request money from someone else, with their pre-approval, and credit it to myself".

The Core SDD Scheme [SDD] applies to transactions in euro. The debtor and creditor must each hold an account with a credit institution located within SEPA. The credit institutions executing the direct debit transaction must be scheme participants; that is, both must have formally adhered to the SDD Scheme. The Scheme may be used for single (one-off) or recurrent direct debit collections; the amounts are not limited.

- **SEPA Cards Framework (SCF)**

The SCF [SCF] developed by the EPC is a policy document which states how participants in the cards market such as card schemes, card issuers, payment card-accepting merchants and other service providers must adapt their current operations to comply with the SEPA vision for card payments in euro. While it is the choice of any participant in the cards market whether to become SCF-compliant or not, the EPC's members have pledged to conform to the conditions of the SCF in their capacities as issuers and acquirers.

Annex II – The Secure Element

A Secure Element is a certified tamper-resistant module (device or integrated circuit component) capable of securely storing and executing applications and their cryptographic data (e.g. keys), in accordance to the security policy and requirements set forth by the appropriate authorities (e.g. MCP application issuer, SE issuer). The SE provides a protection of the applications including separation of the applications.

Specific limitations introduced by the Mobile Phone form factor

Regardless of the final type of SE used, and in direct contrast to physical payment cards, specific provisions should be made to address the fact that, in most cases, PSPs of the mobile payment application will not be in charge of deploying mobile phones or SEs. The main reasons are:

- Only a limited number of SEs can be installed at any given time in a mobile phone. The user experience of swapping such SEs from a mobile phone is very often impractical.

- The mobile phone itself is not typically deployed by the PSPs and, contrary to the situation with payment cards, it is directly owned by the consumer. Selection of mobile phones by consumers is directly based on the features of the device (technical capabilities, design, cost, etc.), and not based on the requirements of the application providers. Therefore, an application provider attempting to deploy its own mobile phones will have no choice but to offer a wide selection of commonly available models from well-known mobile phone manufacturers (similarly as all MNOs already do for their sponsored devices), thereby incurring unreasonable operational costs.

- As any given consumer typically carries only one mobile phone, this phone must necessarily be shared between several application providers to allow for a competitive and fair market place for mobile services.

Secure Elements for mobile payments

The EPC contributed to the Mobey Forum document "*Alternatives for Banks to Offer Secure Mobile Payments*" which provides an overview of the current choices for SEs [16]. It covers the following types:

- Stickers
  Contactless cards, manufactured in the form of a sticker, which can be personalised and processed through the existing payment infrastructure. Consumers may place the sticker on their mobile phone for NFC payments.
- Secure Micro SD card
  Memory card products that hold an embedded chip which can be used as an SE (to be inserted in the mobile phone or embedded in a carrier, e.g. a sleeve). These secure micro SD cards may in addition hold an NFC antenna.
- Universal Integrated Circuit Card (UICC)
  A generic and well standardised SE owned and provided by the MNOs.
- Embedded SE

An SE embedded in a mobile phone at the time of its manufacturing.

- Trusted Mobile Base
  A secure isolated section on the core processors (CPU) of mobile phones which can store secure applications.

The EPC has further analysed these different types of SEs and has prioritised the following SE form factors:

- A UICC,
- An embedded SE,
- A removable SE such as a secure micro SD card,

in its further work (see [5]).

End of Document