EPC492-09
Version 4.7.5
25 May 2016

WHITE PAPER
MOBILE PAYMENTS

Abstract	This new edition of the white paper contains various updates in different sections in view of the changed mobile payment ecosystems and the introduction of new technologies over the recent years.
Document Reference	EPC492-09
Issue	Version 4.7.5 edition 2016
Date of Issue	25 May 2016

Table of Contents

1 Document information 9
1.1 Structure of the document 9
1.2 References 10
1.3 Definitions 12
1.4 Abbreviations 18
2 General 20
2.1 About the EPC 20
2.2 Vision 20
2.3 Scope and objectives 20
2.4 Out of scope 20
2.5 Audience 21
3 Introduction 22
3.1 Evolution of mobile-based services in SEPA 22
3.2 Mobile ecosystem 22
3.3 Security aspects 24
3.4 Architecture for SEPA mobile payment services 25
3.5 High level principles 26
4 Mobile payments for SEPA 27
4.1 A day in the life of a mobile payments consumer 27
4.1.1 Pay for train to work 27
4.1.2 Mobile access to premium entertainment 28
4.1.3 Pay for a business lunch 28
4.1.4 Afternoon refreshment 28
4.1.5 Buy groceries 28
4.1.6 Remote subscription to an on-line family game 28
4.1.7 Ticket for a football match 28
4.1.8 Re-imbursement of a friend 29
4.2 General overview on mobile payments 29
4.2.1 Introduction 29
4.2.2 The mobile payment categories within EPC's focus 30
5 Mobile Proximity Payments 38
5.1 Introduction 38
5.2 Use-cases – Mobile Contactless SEPA Card Payments 38
5.2.1 MCP 1 - Mobile Contactless SEPA Card Payment - Tap and Go 38
5.2.2 MCP 2 - Mobile Contactless SEPA Card Payment - Double Tap with Mobile Code 40
5.2.3 MCP 3 - Mobile Contactless SEPA Card Payment - Single Tap and PIN 42
5.3 Use-cases – Mobile Proximity SEPA Credit Transfers 44
5.3.1 MPCT 1 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer 44
5.3.2 MPCT 2 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer 46
5.4 Ecosystem 49
5.4.1 Introduction 49

5.4.2 Stakeholders 49
5.4.3 Service models 50
6 Mobile Remote Payments 53
6.1 Introduction 53
6.2 Use-cases - Mobile Remote SEPA Card Payments 53
6.2.1 MRCP 1 - Consumer-to-Business Mobile Remote SEPA Card Payment - Basic 53
6.2.2 MRCP 2 - Consumer-to-Business Mobile Remote SEPA Card Payment - Mobile Wallet 55
6.2.3 MRCP 3 - Consumer-to-Business Mobile Remote SEPA Card Payment - Strong cardholder authentication 58
6.2.4 MRCP 4 - Consumer-to-Consumer Mobile Remote SEPA Card Payment ... 61
6.3 Use-cases - Mobile Remote SEPA Credit Transfers 64
6.3.1 MRCT 1 - Consumer-to-Consumer Mobile Remote SCT – Static authentication via mobile browser 65
6.3.2 MRCT 2 - Consumer-to-Consumer Mobile Remote SCT – Alias –Strong authentication via MRCT application in mobile wallet 67
6.3.3 MRCT 3 - Consumer-to-Business Mobile Remote SCT-Inst – QR code – Strong authentication via MRCT application 70
6.3.4 MRCT 4 - Consumer-to-Business – Mobile Remote SCT-Inst - Consumer redirection with strong authentication via mobile browser 73
6.4 Ecosystem 76
6.4.1 Introduction 76
6.4.2 Stakeholders 76
6.4.3 Service models 77
6.5 High level architecture 78
6.5.1 Introduction 78
6.5.2 Layer 1 revisited 79
6.5.3 Layer 2 revisited 81
7 Secure consumer subscription to mobile payment services 84
7.1 Remote subscription 84
7.2 Subscription with self-service device 86
7.3 Subscription at the PSP's branch 87
8 Infrastructure 89
8.1 Mobile devices 89
8.1.1 General 89
8.1.2 End-user interface 89
8.1.3 Secure Elements 90
8.1.4 Host Card Emulation 90
8.1.5 Trusted Execution Environment 91
8.1.6 Trusted Platform Module 91
8.2 Infrastructure for mobile payment transactions 91
8.2.1 Transaction infrastructure 91
8.2.2 Alias 92
8.2.3 Storage of mobile payment data and applications in the mobile device ... 93
8.2.4 Provisioning & management 93

8.2.5 Mobile payment application user interface 93
8.2.6 Tokenisation 94
8.2.7 Merchant interface 94
9 Mobile wallets 96
9.1 Definition 96
9.2 Usage of mobile wallets for mobile payments 96
10 Standardisation and industry bodies 97
11 Conclusions 99
Annex I – SEPA Payment Instruments 101
Annex II – Secure Elements in the mobile device 102
Annex III – Mapping the MRP use-cases on the infrastructure 103

List of Figures

Figure 1: A day in the life of Mr Garcia 27
Figure 2: MCP 1 - Mobile Contactless SEPA Card Payment - Tap and Go..... 39
Figure 3: MCP 2 - Mobile Contactless SEPA Card Payment - Double Tap with Mobile Code..... 41
Figure 4: MCP 3 - Mobile Contactless SEPA Card Payment - Single Tap and PIN... 43
Figure 5: MPCT1 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer 46
Figure 6: MPCT2 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer 48
Figure 7: MCP transaction 51
Figure 8: MRCP 1 - Consumer-to-Business Mobile Remote SEPA Card Payment -Basic 54
Figure 9: MRCP 2 - Consumer-to-Business Mobile Remote SEPA Card Payment - Mobile Wallet 57
Figure 10: MRCP 3 - Consumer-to-Business Mobile Remote SEPA Card Payment - Strong cardholder authentication..... 60
Figure 11: MRCP 4 - Consumer-to-Consumer Mobile Remote SEPA Card Payment 63
Figure 12: MRCT 1 - Consumer-to-Consumer Mobile Remote SCT – Static authentication via mobile browser 66
Figure 13: MRCT 2 - Consumer-to-Consumer Mobile Remote SCT– Alias - Strong authentication via MRCT application in mobile wallet..... 69
Figure 14: MRCT 3 - Consumer-to-Business Mobile Remote SCT-Inst - QR code – Strong authentication via MRCT application 72
Figure 15: MRCT 4 - Consumer-to-Business – Mobile Remote SCT-Inst -Consumer redirection with strong authentication via mobile browser..... 75
Figure 16: High level architecture for Mobile Remote Payments 78
Figure 17: The 3-corner model 79
Figure 18: The 4-corner model under a single payment scheme..... 80
Figure 19: The 4-corner model involving different payment schemes..... 80
Figure 20: Direct interoperability model..... 81
Figure 21: Centralised common infrastructure model..... 82
Figure 22: Example of remote subscription to mobile payment services..... 85
Figure 23: Example of ATM subscription to mobile payment services scenario 87
Figure 24: Example of in-person mobile payment service subscription use-case... 88

List of Tables

Table 1: Bibliography 11
Table 2: Definitions 17
Table 3: Abbreviations 19
Table 4: Illustration of mobile payments using SEPA instruments 30
Table 5: Mobile Proximity Payments: focus levels 31
Table 6: Mobile Contactless SEPA Card Payments: focus levels 32
Table 7: Mobile Proximity SEPA Credit Transfer Payments: focus levels 33
Table 8: Mobile Remote Payments: focus levels 34
Table 9: Mobile Remote SEPA Card Payments: focus levels 35
Table 10: Mobile Remote SEPA Direct Debit Payments: focus levels 36
Table 11: Mobile Remote SEPA Credit Transfer Payments: focus levels 37
Table 12: MCP 1 - Mobile Contactless SEPA Card Payment - Tap and Go 40
Table 13: MCP 2 - Mobile Contactless SEPA Card Payment - Double Tap with Mobile Code 42
Table 14: MCP 3 - Mobile Contactless SEPA Card Payment - Single Tap and PIN .. 44
Table 15: MPCT 1 – Consumer-to-Business Mobile Proximity Instant Credit Transfer 46
Table 16: MPCT 2 – Consumer-to-Business Mobile Proximity Instant Credit Transfer 49
Table 17: MRCP 1 - Consumer-to-Business Mobile Remote SEPA Card Payment - Core 55
Table 18: MRCP 2 - Consumer-to-Business Mobile Remote SEPA Card Payment - Mobile Wallet 58
Table 19: MRCP 3 - Consumer-to-Business Mobile Remote SEPA Card Payment - Strong cardholder authentication 61
Table 20: MRCP 4 -Consumer-to-Consumer Mobile Remote SEPA Card Payment - Core 64
Table 21: MRCT 1 - Consumer-to-Consumer Mobile Remote SCT – Static authentication via mobile browser 67
Table 22: MRCT 2 - Consumer-to-Consumer Mobile Remote SCT – Alias - Strong authentication via MRCT application in mobile wallet 70
Table 23: MRCT 3 - Consumer-to-Business - Mobile Remote SCT-Inst - QR code – Strong authentication via MRCT application 73
Table 24: MRCT 4 - Consumer-to-Business – Mobile Remote SCT-Inst –Consumer redirection with strong authentication via mobile browser 76
Table 25: Mapping of uses cases onto three layers MRP architecture 103

Executive Summary

The overall purpose of the EPC is to support and promote European payments integration and development, notably the Single Euro Payments Area (SEPA) (see http://www. www.epc-cep.eu). Therefore this white paper focuses on mobile payment ecosystems that are based on SEPA[1] payment instruments, hereby covering both four and three corner models.

Since mobile phones have achieved full market penetration and rich service levels they are an ideal channel for SEPA payment instruments. The usage of the mobile phone is hereby primarily considered for the payment initiation whereas the underlying payments are based on existing SEPA instruments. When starting this work, the EPC analysed the different payment categories and has given focus to mobile contactless SEPA card payments (MCPs) and mobile remote SEPA card and SCT payments.

The EPC published in 2010 its first edition of the white paper on mobile payments. While addressing both mobile contactless and mobile remote payments through a high-level overview, more attention was given to the first payment type.

Early 2012, the EPC published its second edition covering all its main focus areas for mobile payments while addressing also the comments received from various stakeholders through an open consultation.

With this new third edition the EPC has extended the scope to include new types of mobile proximity payments while addressing also the new stakeholders and technologies that entered the mobile ecosystem over the last years. As before, the EPC is now launching a three months public consultation on this document to collect further stakeholder's input.

For each focus area of mobile payments a detailed analysis through the specification of key use-cases is provided in the document. Furthermore a description of the ecosystem, the high level architecture and the most important infrastructure aspects are given. Also the concept of mobile wallets is briefly introduced.

This white paper endeavours to:

- Inform stakeholders of the EPC's commitment to an integrated market for mobile payments in SEPA;
- Describe some elements of the rationale for payment service providers (PSPs) and other interested parties 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 document 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 welcomes all interested stakeholders' input on the information presented in this white paper.

The main conclusions of this white paper are as follows:

- For mobile contactless SEPA card payments, the choice between an SE or an HCE approach has a major impact on the service model and the roles of the different stakeholders. For other mobile proximity payments, the lack of standardisation in the usage of the various proximity technologies is resulting in a very fragmented approach throughout Europe. A comprehensive and more detailed

[1] Note that the use cases and service models introduced in this white paper may also be applied to non SEPA areas.

analysis of the challenges for the mobile proximity payments may be found in the ERPB report [10]. The EPC has been significantly involved in this ERPB work.

- 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) transfer of funds.

While many of these identified challenges are not specific to the mobile channel, an early resolution is key if remote SEPA payment instruments are to become successful in this environment. With the specification of a SEPA Instant Credit Transfer Scheme the EPC is delivering a major contribution to address some of these challenges (see [8]).

Although, it is up to the individual stakeholders in the mobile payments ecosystem to decide if and when they will offer their services in this area, the EPC aims, with the publication of this document, to contribute to the harmonisation of mobile SEPA payments. It is further to be noted that various sections of the document can also be applied to non-SEPA based mobile payments.

Next to working with other stakeholders involved in the mobile ecosystem, the EPC further plans to engage with relevant industry bodies to contribute to the development of open specifications for the interoperability of mobile payments, which can be used by the payment industry and all interested parties.

1 Document information

1.1 Structure of the document

This section describes the structure of the white paper. Section 1 provides the references, definitions, and abbreviations used in this document. General information about the EPC and its vision may be found in section 2. Section 3 contains an introduction to SEPA, mobile payment services and related aspects of the mobile payment ecosystem. Section 4 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 the focus areas proposed by the EPC. Section 5 is devoted to mobile proximity payments (MPPs). It includes a more detailed description of use-cases and a high level overview of the ecosystem. By analogy, section 6 provides similar information for mobile remote payments (MRPs) whereby both mobile remote card payments and mobile remote credit transfers are covered. Section 7 illustrates how subscription to mobile payment services can be conveniently and easily achieved. The different infrastructure components used both for MPPs and MRPs are described in section 8. Section 9 briefly introduces the usage of mobile wallets. Section 10 provides an overview of the most relevant standards and industry bodies in the mobile ecosystem. General conclusions may be found in the final section 11. In addition, an introduction to SEPA payment instruments and a high level analysis on Secure Elements are provided in annexes, as well as a mapping of use-cases on mobile remote payments described in sections 6.2 and 6.3 on the three layer architecture introduced in section 6.5.

The main changes that have been applied to the document in comparison to the October 2012 edition are due to the changed mobile payment ecosystems involving new stakeholders, the introduction of new technologies over the recent years and the new Payment Service Directive (PSD2).

1.2 References

This section lists the references mentioned in this document. Square brackets throughout this document are used to refer to a document of this list.

[1]	EMVCO specifications
[2]	European Banking Authority EBA/GL/2014/12_Rev1: Guidelines on the security of internet payments
[3]	European Payments Council EPC 397-08: Customer-to-Bank Security Good Practices Guide
[4]	European Payments Council EPC 020-08 SEPA Cards Standardisation (SCS) "Volume" Book of Requirements Book 1: General Book 2: Functional Requirements Book 3: Data Elements Book 4: Security Book 5: Conformance Verification Procedures Book 6: Implementation Guidelines Book 7: Card Processing Framework
[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 Payments Council EPC 163-13: White Paper Mobile Wallet Payments
[8]	European Payments Council EPC 269-15: Proposal for the design of an optional euro SCT Instant scheme
[9]	Euro Retail Payments Board Pan-European instant payments in euro: definition, vision and way forward
[10]	Euro Retail Payments Board Final report on Mobile and card-based contactless proximity payments
[11]	Global Platform GPD_SPE_009: TEE System Architecture
[12]	GSM Association / Consult Hyperion HCE and Tokenisation for Payment Services - Discussion paper
[13]	GSMA Association The Mobile Economy Report 2015
[14]	International Telecommunication Union World Telecommunication/ICT Indicators Database 2015 (19th Edition)
[15]	Mobey Forum Alternatives for Banks to offer Secure Mobile Payments
[16]	Mobey Forum

	Mobile wallet Part 1 - Definitions and Visions Part 2 - Control Points in the Mobile Wallet Part 3 - The Hidden Controls Part 4 - Structure and Approaches Part 5 – Strategic Options for Banks –Parts 1-5
[17]	Mobey Forum The Host Card Emulation in Payments – Options for Financial Institutions
[18]	ISO 12812: Core banking – Mobile financial services – Parts 1-5 (under finalisation)
[19]	ISO/IEC 14443: Identification cards -- Contactless integrated circuit cards -- Proximity cards – Parts 1-4.
[20]	ISO/IEC 18092: Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1).
[21]	Payment Services Directive 2 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payments services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
[22]	IF Regulation Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions

Table 1: Bibliography

1.3 Definitions

Throughout this document, the following terms are used.

Term	Definition
Account Servicing Payment Service Provider (ASPSP)	A PSP providing and maintaining an account for a payer (see [21]).
Acquirer	A PSP or one of their agents whom enters into a contractual relation with a merchant and an issuer via a card payment scheme, for the purpose of accepting and processing card transactions.
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 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.
(Payment) Application	A set of modules (application software) and/or data (application data) needed to provide functionality for a mobile payment service as specified by the mobile payment application issuer in accordance with the payment scheme (see also [18]).
(Payment) Application user interface	The mobile phone application executing the user interactions related to the mobile payment application, as permitted by the mobile payment application issuer.
Authentication	The provision of assurance of the claimed identity of an entity or of data origin.
Bluetooth low energy (BLE)	A wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications including beacons. Compared to classic Bluetooth, BLE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.
Beneficiary	See Payee
Cardholder	A consumer which has an agreement with an issuer for a mobile card payment service.
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.
Consumer	A natural person who, in payment service contracts covered by the PSD2, is acting for purposes other than his or her trade, business or profession [21].
Consumer Verification Method	A method for checking that a consumer is the one claimed.
3-Corner model	Both the payer and the beneficiary hold their payment accounts with the same PSP which operates under a given payment scheme.

4-Corner model	The payer and the beneficiary hold their payment accounts with different PSPs. Both PSPs can operate under one and the same payment scheme or under different payment schemes.
Contactless Technology	A radio frequency technology operating at very short ranges so that the user has to perform a voluntary gesture in order that a communication is initiated between two devices by approaching them. It is a (chip) card or mobile payment acceptance technology at a POI device which is based on ISO/IEC 14443 (see [19]).
Customer	A payer or a beneficiary which may be either a consumer or a business (merchant).
Credential(s)	Payment account related data that may include a code (e.g., mobile code), provided by the PSP to their customer for identification/authentication purposes.
Credit transfer	A payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer [21].
2D barcodes	A two dimensional barcode is a machine-readable optical label that contains digital information. They are also referred to as matrix barcodes. Examples include QR codes and tag barcodes.
Digital wallet	A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
Direct debit	A payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's PSP or to the payer's own PSP [21].
EMVCo	An LLC formed in 1999 by Europay International, MasterCard International and Visa International to enhance the EMV Integrated Circuit Card Specifications for Payments Systems. It manages, maintains, and enhances the EMV specifications jointly owned by the payment systems. It currently consists of American Express, Discover, JCB, MasterCard, Union Pay and VISA (see [1]).
Host Card Emulation (HCE)	A technology that enables mobile devices to emulate a contactless card. HCE does not require the local usage of a secure element on the mobile device for storage of sensitive data such as credentials, cryptographic keys, etc.
Identification of beneficiary	A mean of uniquely identifying the beneficiary and their underlying account. Examples are the usage of IBAN, an alias, card number, dedicated credentials, …
(Card) Issuer	A PSP or one of their agents that supplies the card payment account and, in the context of this document, the mobile card payment application (including card data) to the

	customer (cardholder), and whom is a member of a card payment scheme. The Issuer enters into a contractual relationship with a consumer (cardholder) and guarantees payment to the acquirer for transactions that are in conformity with the rules of the relevant card payment scheme.
Instant payment	Electronic retail payment solutions available 24/7/365 and resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation). This is irrespective of the underlying payment instrument used (credit transfer, direct debit or payment card) and of the underlying clearing and settlement arrangements that make this possible (see [9]).
Merchant	The beneficiary within a mobile payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP.
Mobile code	An authentication credential used for consumer verification and entered by the consumer via the keyboard of the mobile device
Mobile Contactless Payment (MCP)	A mobile proximity payment where the payer and the payee communicate directly using contactless technologies.
Mobile device	Personal device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth, etc., which offers connections to internet. Examples of mobile devices include mobile phones, smart phones, tablets.
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 consumer and their PSP using their own or leased network.
Mobile Proximity Payment (MPP)	A mobile payment where the consumer and the merchant (and/or their equipment) are in the same location and where the communication between the mobile device and the Point of Interaction device takes place through a proximity technology (e.g., NFC, 2D barcodes, BLE, etc.).
Mobile Remote Payment (MRP)	A payment initiated by a mobile 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 payment service	A payment service made available by software/hardware through a mobile device.
Mobile service	A service such as identification, payment, ticketing, loyalty, etc., made available through a mobile device.
Mobile wallet	A digital wallet accessed through a mobile device. This service may reside on a mobile device owned by the consumer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a combination thereof) or on a merchant website. Typically, the so-called mobile wallet

	issuer provides the wallet functionalities but the usage of the mobile wallet is under the control of the consumer. Multiple mobile wallets might coexist in a mobile device.
Mobile wallet issuer	The service provider that issues mobile wallet functionalities to the customer (consumer or merchant).
NFC (Near Field Communication)	A contactless protocol specified by ISO/IEC 18092 [20].
Payee	A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction [21].
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 [21].
Payment account	An account held in the name of one or more payment service users which is used for the execution of payment transactions [21].
Payment scheme	A technical and commercial arrangement (often referred to as the "rules") between parties in the payment value chain, which provides the organisational, legal and operational framework rules necessary to perform a payment transaction.
Payment Service Provider (PSP)	A body referred to in Article 1(1) of [21] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of [21].
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 [21]).
Payment transaction	An act, initiated by the payer or on his behalf or by the payee (beneficiary), of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee (as defined in [21]).
POI device	"Point of Interaction" device; the initial point where data is read from a consumer device or where consumer data is entered in the merchant's environment. As an electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a consumer to perform a payment transaction. The merchant controlled POI may be attended or unattended. Examples of POI devices are 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).
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 universal integrated circuit cards (UICC),

	embedded secure elements, chip cards and secure digital cards.
Secure Element issuer (SE issuer)	A TTP responsible for the issuance and maintenance of an SE. Typical examples are MNOs and card manufacturers.
Secured Server	A web server with secure remote access that enables the secure storage and processing of payment related data.
Third Party Payment Service Provider (TPP)	A third party that offers payment services which are different to the Account Servicing PSP (ASPSP) such as a Payment Initiation Service Provider (PISP), Account Information Service Providers (AISP) and Trusted Party Payment Instrument Issuer (TPII) (see [21]).
(Payment) Tokenisation	The usage of payment tokens instead of real payer related account data in payment transactions
(Payment) Token	Payment Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payer account related data (e.g., the PAN for card payments, the IBAN for SCTs). Payment Tokens must not have the same value as or conflict with the real payment account related data. Examples include the EMVCo Token, see [1].
(Payment) Token Requestor	An entity requesting a token to the Token Service
(Payment) Token Service	A system comprised of the key functions that facilitate generation and issuance of payment tokens, and maintain the established mapping of payment tokens to the payer account related data when requested by the token requestor. It may also include the capability to establish the token assurance level to indicate the confidence level of the payment token to the payer account related data / payer / merchant / device / environment binding. The service also provides the capability to support token processing of payment transactions submitted using payment tokens by de-tokenising the payment token to obtain the actual account related data.
(Payment) Token Service Provider (TSP)	An entity that provides a Token Service.
Trusted Execution Environment (TEE)	An execution environment (as defined by Global Platform, see [11]) that runs alongside, but isolated from a main operating system. A TEE has security capabilities and meets certain security-related requirements: it protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats.
Trusted Platform Module	A secure cryptoprocessor (which is a dedicated microprocessor) that securely stores features used to authenticate a computer platforms such as PC, laptop, or mobile device. These features can include passwords, certificates, or encryption keys. The TPM can also help to ensure that the platform remains trustworthy.

Trusted Service Manager (TSM)	A trusted third party acting on behalf of the SE issuer and/or the MCP application issuer in case an SE is involved to host the MCP application(s).
Trusted Third Party (TTP)	An entity which facilitates interactions between stakeholders of the ecosystem who all trust this third party (examples are SE issuer, TSM, common infrastructure manager…).
User Interface (UI)	An application enabling the user interactions.

Table 2: Definitions

1.4 Abbreviations

Throughout this document, the following abbreviations are used.

Abbreviation	Term
AAUI	Application Activation User Interface
AISP	Account Information Service Provider
ASPSP	Account Servicing PSP
ATM	Automated Teller Machine
B2B	Business to Business
B2C	Business to Consumer
BLE	Bluetooth Low Energy
C2B	Consumer to Business
C2C	Consumer to Consumer
CAP	Chip Authentication Program
CNP	Card Not Present
CSM	Clearing and Settlement Mechanism
CVM	Consumer Verification Method
2D barcode	Two dimensional barcode
DPA	Dynamic Passcode Authentication
EPC	European Payments Council
ERPB	Euro Retail Payments Board
ETSI	European Telecommunications Standards Institute
GP	GlobalPlatform
GSMA	The GSM Association
HCE	Host Card Emulation
HSM	Hardware Security Module
IBAN	International Bank Account Number
ID	Identifier
ISO	International Organisation for Standardisation
MCP	Mobile Contactless Payment
MNO	Mobile Network Operator
MPP	Mobile Proximity Payment
MRP	Mobile Remote Payment
MRCP	Mobile Remote SCP
MRCT	Mobile Remote SCT
NFC	Near-Field Communications
OS	Operating System
OTA	Over the Air
PISP	Payment Initiation Service Provider
POI	Point of Interaction
POS	Point of Sale
PSD	Payment Services Directive

PSP	Payment Service Provider
QR code	Quick Response code
REE	Rich Execution Environment
SCP	SEPA Card Payment
SCT	SEPA Credit Transfer
SDD	SEPA Direct Debit
SE	Secure Element
TEE	Trusted Execution Environment
TPII	Trusted Party Payment Instrument Issuer (e.g., wallet issuer)
TPM	Trusted Platform Module
TTP	Trusted Third Party
TPP	Third Party Payment Service Provider
TSP	Token Service Provider
UI	User Interface
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
SCT-Inst	Instant SCT

Table 3: Abbreviations

Note: In the sequel of this document no further distinction will be made between an ASPSP (as defined in [21]) and a PSP. If for instance reference is made to a payer's PSP, the payer's ASPSP is meant.

2 General

2.1 About the EPC

The European Payments Council (EPC), representing payment service providers, supports and promotes European payments integration and development, notably the Single Euro Payments Area (SEPA). The EPC is committed to contribute to safe, reliable, efficient, convenient, economically balanced and sustainable payments, which meet the needs of payment service users and support the goals of competitiveness and innovation in an integrated European economy. It pursues this purpose through the development and management of pan-European payment schemes and the formulation of positions and proposals on European payment issues in constant dialogue with other stakeholders and regulators at the European level and taking a strategic and holistic perspective. The primary task of the EPC is to manage the SEPA Credit Transfer and SEPA Direct Debit Schemes in close dialogue with all stakeholders. The EPC is an international not-for-profit association which makes all of its deliverables available to download free of charge on the EPC Website. Further information may be obtained from www.epc-cep.eu.

2.2 Vision

The vision of the EPC is to contribute to the evolution of an integrated market for payments. The payment transactions enabled by mobile devices and services could build on existing SEPA Scheme Rulebooks, the SEPA Cards and (global) standards as far as possible. Therefore, the EPC may assist in specifying standards and guidelines to create the necessary environment so that PSPs can deliver secure, efficient and user-friendly mobile solutions to access the SEPA payment instruments.

Cross-industry cooperation between all the different stakeholders in the mobile payment ecosystem could be a critical success factor. Consumers on the other hand should not be bound to a specific MNO or particular mobile equipment, and should retain their ability to switch between PSPs.

2.3 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 new edition of the document includes detailed analyses for both mobile proximity and remote payments, according to the focus areas set by the EPC (see section 4.2.2).

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 services access and business opportunities enabled by the mobile channel;
- Outline the categories for mobile payments;
- Provide examples of mobile payment use cases;
- Analyse mobile proximity and remote payments.

2.4 Out of scope

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 it rather focuses on the initiation of payments via the mobile channel using existing SEPA payment instruments (SCT, SDD and SEPA for Card Payments). The reader is referred

to the EPC rulebooks (www.epc-cep.eu) for the general aspects of the transaction leg in mobile payments.

The EPC recognises that there is also an increased usage during the last years of the mobile phone as customer device of the beneficiary (e.g., tax refunds, vouchers, etc.). However these use cases have not yet been considered in the current version of this document.

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 should by no means prejudge a future approach by EPC or other stakeholders 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. It focuses on areas that form the basis for interoperability in the co-operative space between PSPs. As such the specification of business cases and detailed analyses of mobile payment value chains are outside the scope of the present document.

2.5 Audience

The document is intended for PSPs as well as for other interested parties involved in mobile payments, such as:

- Mobile Network Operators (MNOs);
- Trusted Service Managers (TSMs);
- Third Party Payment Service Providers (TPPs)
- Token Service Providers;
- Equipment manufacturers (handsets, POIs, etc.);
- Merchants and merchant organisations;
- Consumers;
- Application developers;
- OS developers;
- Public administrations;
- Regulators;
- Standardisation and industry bodies;
- Card schemes;

and

- Other interested stakeholders.

3 Introduction

3.1 Evolution of mobile-based services in SEPA

According to [13], smart phone adoption is already reaching critical mass in developed markets, with these devices now accounting for 60% of the connections. During the last decade, most consumers have been using mobile phones beyond the traditional services of voice calls and SMS. The new services including mobile internet and a wide variety of dedicated apps have been greatly facilitated by the new MNO infrastructure including UMTS and 4G technologies through virtually full geographic network coverage. As an example, mobile devices accounted already for 31,2 % of all website traffic worldwide[2] in Q1 2014. The consumer expectations for mobile device functionality have increased dramatically which is reflected in the rapid uptake of the smart phones' market segment. Consumers are eager to embrace new services based on this delivery platform which thanks to their convenience may ease their daily lives. Clearly financial services are recognised as important among these new mobile services, hereby setting high expectations with respect to availability and trust. Recent figures show that about 56% of smart phone owners purchased a product using a mobile app transaction in 2015[3]. Also mobile banking transactions via apps are on the rise.

Merchants expect to get valuable data and get direct communication and more information on their customer's needs and preferences, subject to their consent. They also 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 are very well positioned to achieve all these benefits for merchants and other stakeholders who are directly providing services to consumers. In addition, the migration to mobile payments may reduce the cash and cheque usage.

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

During the last years, many PSPs and other market participants have already identified mobile payments as a target for new growth opportunities. Different mobile payment pilots and commercial deployments are already conducted in SEPA and elsewhere.

However, the market is fragmented in terms of maturity of mobile payments adoption and the related technical standards implementations. Likewise, the mobile payments environment shows strong complexities, mainly related to the usage of different technologies and the large number of business stakeholders involved in the mobile ecosystem.

3.2 Mobile ecosystem

An open approach for the ecosystem for mobile payments is important for the society and will involve, whatever form it may take, a number of different stakeholders in its value chain. This white paper aims to describe the rationale for the different stakeholders to enter the mobile payments market.

---

[2] See http://www.statista.com/statistics/284202/mobile-phone-internet-user-penetration-worldwide/

[3] According to The Paypers, 18 January 2016.

There is 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 remote registration for financial services or mandate signing for direct debits.

At this 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 interested service provider 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 service provider, depending on its customer base, its business strategy and objectives, its geographical environment, the technical infrastructure and resources employed.

The major elements supporting a rationale for service providers to enter the mobile payments market include the following:

- Strong penetration of mobile phones: in the last 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. More in particular in Europe a steady rise in the number of “smart phones” is to be noted during the last years.
- The potential of the recent SEPA payment schemes investments in relation to mobile phone initiated payments;
- Provisioning of user convenience by meeting proven needs of both consumers and merchants;
- The need to foster innovation with competitive offerings to the customer’s benefit in a more complex ecosystem including new stakeholders, thereby growing the market for non-cash 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 service provider 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 proximity (see section 4) and mobile remote payments (see section 5).

The main drivers identified for some of the stakeholders involved in the ecosystem for a potential adoption of mobile payments include the following:

Consumers’ expectations and demands

- Efficiency: speed of payment initiation, frictionless;
- 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 (interoperability).

Note that value added services such as special offers or loyalty points are also part of consumers' expectations but are out of scope of the document according to the focus on the payment feature.

Beneficiaries / merchants' expectations

- Efficiency: speed of payment (e.g., for 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 (interoperability)
- Data collection from consumers, subject to their consent, and provision of related additional services such as cross-selling and/or geo-based marketing;
- Low implementation effort.

Service providers' expectations

- 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.

3.3 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; this should imply consistent governance and a strong cooperation between stakeholders to deal with the potential security issues; 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 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 addressed 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, TSM or TPP) in the mobile payments ecosystem would need to ensure that an appropriate information security management system is in place. Each service provider would need to 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 security measures identified include the “Secure Element” or “Tokenisation” which are introduced later in this document (see also [5]).

3.4 Architecture for SEPA mobile payment services

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 of payments through mobile phones. Mobile payments will need to comply with the PSD2 [21] 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. This remains a decision by each scheme and / or individual PSP.

The documents developed by the EPC are made publicly available to market participants and providers within the mobile channel value chain in order to contribute to 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 the latter 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 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 customer experiences wherever risk management policies allow. In that respect, the EPC contributes in defining security requirements, recommendations and guidelines with the appropriate bodies in this area.

3.5 High level principles

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

1. In order to assist in the development of an integrated market for mobile payments, EPC promotes SEPA payment instruments as a basis[4];
2. PSPs should be able to differentiate 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 should be clear, and in line with applicable regulations;
6. The PSP should be able to define the graphical interface to the consumer for its mobile payment service, including brands and 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 device.[5]
8. The consumer shall be able to use all their mobile payment services offered by multiple PSPs using his/her mobile device[6]. Furthermore, he/she shall be able to select the relevant mobile payment service to be used for a particular payment transaction;
9. Mobile payments should, as much as possible, use 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 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, within the boundaries of the payment scheme, 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) (see also [10]).

[5] Obviously, the mobile device for payments will need to meet the appropriate technical requirements (e.g., NFC).

[5] Obviously, the mobile device for payments will need to meet the appropriate technical requirements (e.g., NFC).

[6] Subject to appropriate commercial and technological relationships.

4 Mobile payments for SEPA

4.1 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.

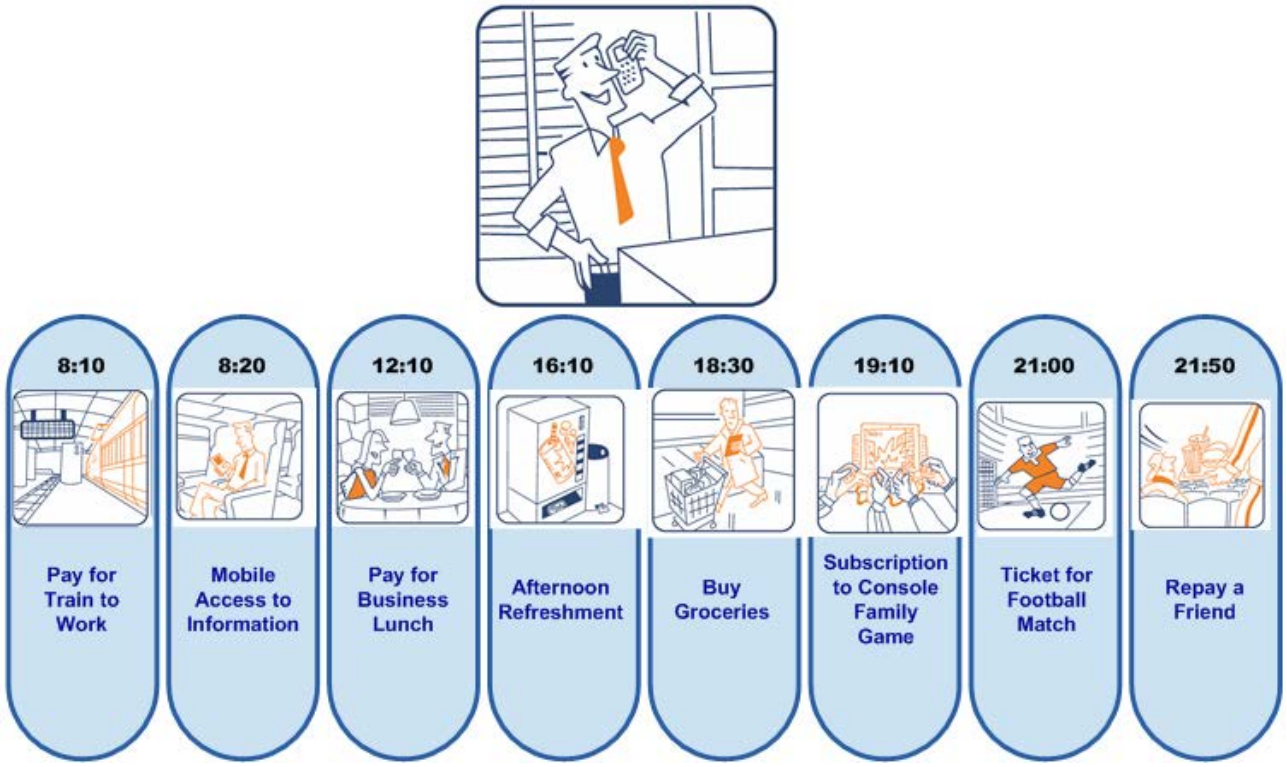

Figure 1: A day in the life of Mr Garcia

4.1.1 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 using a dedicated ticketing app on his mobile phone. He opens the ticketing app, which holds his credentials for remote payment, using a passcode and selects "the ticket renewal". He is invited to authorise the payment. Subsequently, the validity period of his ticket is updated and he can tap his mobile phone at the gate to access the train platform and, due to the speedy process, still catches his usual 8:15 train.

4.1.2 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. He is requested to login to the website using his personal credentials. Some details of his credit card (last digits of the PAN and validity period) are displayed to him and his is requested to enter the corresponding CVC value. His payment is confirmed and he subsequently obtains access to the requested movie.

4.1.3 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.

4.1.4 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 selects his preferred payment card from the menu option on his mobile phone display and swiftly taps the vending machine with his mobile phone to perform the transaction with this 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.

4.1.5 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.

4.1.6 Remote subscription to an on-line family game

While browsing 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 authorisation by Mr Garcia for direct debit payment. By accepting the request, Mr Garcia selects his current payment account as the target of the charges. His daughter can then start playing right away while Mr Garcia leaves for a football match.

4.1.7 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 opens a dedicated payment app linked to his account and scans the QR code which corresponds with his seat preference. He is invited to authorise the credit transfer. He receives confirmation of the payment and the ticket on his mobile phone. He enters the stadium by tapping his mobile phone at the entry gate.

4.1.8 Re-imbursement of 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.

4.2 General overview on mobile payments

4.2.1 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 "proximity" or "remote" payments. For "proximity payments" the consumer and the merchant (and/or his/her equipment) are in the same location and communicate directly using a proximity technology (e.g., NFC, 2D barcodes, BLE, etc.). 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 their equipment).

Note that the boundaries between these two categories are becoming blurred e.g., when information for the transaction (e.g. the beneficiary) gathered via a proximity technology through a POI, but the actual payment initiation is done remotely via the mobile device.

Depending on the nature of the payer and beneficiary being a consumer[7] 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 concerned. Moreover, since only a few use-cases have been provided in section 3.1, not all categories represented in Table 4 have been covered.

[7] According to [21], "consumer" means a natural person who, in payment service contracts covered by [21], 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.

		SEPA Credit Transfer	SEPA Direct Debit (Mandate)	SEPA Card Payments
Proximity	**C2C**			
	C2B	Ticket for a football match		Buy groceries Afternoon refreshment
	B2C			
	B2B			Pay for a business lunch
Remote	**C2C**	Re-imbursement of 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

4.2.2 The mobile payment categories within EPC's focus

To maximise the potential and overall benefits of mobile payments, the EPC is committed to facilitate market adoption. As a part of this strategy, the EPC commissioned an external market study for the first edition of this document, to prioritise its work in the mobile payments area. An analysis of mobile payment use scenarios based on the SEPA payment instruments (SCT, SDD and SEPA Cards) was conducted for the different market segments: Consumer-to-Business (C2B) and vice versa, Consumer-to-Consumer (C2C, often referred to as P2P) and Business-to-Business (B2B), both from a consumer and business (merchant) perspective. This analysis has proven to be very useful when describing scenarios for use-cases and for identifying gaps that may be barriers to the full deployment of SEPA in the mobile channel. The different scenarios adhered 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, or more generally speaking risk management, are a matter for each PSP and/or payment 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.

As a result of this market study and based on the following evaluation criteria:

- Business and economic aspects;
- Infrastructure and go to market;
- Market potential;

the EPC originally decided to focus on mobile contactless SEPA card payments (MCPs) and mobile remote SEPA card and SCT payments for the first releases of this document. In view of the market evolution during the last years and the recent ERPB report on mobile proximity payments (see [10]), the EPC has decided to enlarge the first category to mobile proximity payments with the new edition of the document. For both categories, proximity and remote payments, a selection of use cases will be described in sections 4 and 5 of this document based on a high level analysis made below.

4.2.2.1 Mobile Proximity Payments (MPP) analysis

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

	SEPA Cards	SDD	SCT
C2C			
C2B			
B2C			
B2B			

	Low Focus
	Medium Focus
	High Focus

Table 5: Mobile Proximity Payments: focus levels

The following sections provide a high level view on each of these three payment types.

Mobile Proximity SEPA Card Payments

The SEPA Card Payment scenarios were analysed and two key focus areas emerged i.e. Consumer-to-Business (C2B) and Consumer-to-Consumer (C2C).

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 based on NFC technology (see [4]). This allows the cardholder to simply wave or tap 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 offers a great opportunity for the development of interoperable mobile contactless payments for SEPA. The survey conducted in the context of the ERPB report (see [10]) has shown that for proximity payments whereby cards are the underlying payment instrument, the NFC technology is by far the one with the best market take-up.

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 market evolutions during recent years have shown that the opportunity has sufficient potential to merit special focus on 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 like 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.

As a result of the analysis above, the rest of the document will in the context of mobile proximity payments whereby the underlying payment instrument is a SEPA card, only focus on mobile contactless payments (MCPs).

SEPA Card	Consumer	Business
Consumer	**C2C** • Offers a practical service for personal payments, including cheque and cash displacement • Needs support from card schemes to achieve wider cross-border 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 offers opportunities to grow and develop the contactless SEPA Card Payments market and also facilitates value added services by card issuers
Business	**B2C** • Even if the card were a business or a purchasing card, the cardholder acts as a consumer • Therefore this scenario is no different to the 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 the C2B scenario • No need for distinct use-cases

Table 6: Mobile Contactless SEPA Card Payments: focus levels

Mobile Proximity 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 on a proximity basis and are therefore out of scope for this section. Hence, no further focus will be given to these payments.

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 Proximity SEPA Credit Transfer Payments

The potential use-cases for mobile proximity payments were analysed for the purpose of this document. Although already available in some countries, the take up of this category is expected to be accelerated with the availability of an instant SCT-based payment scheme "SCT-Inst" (see [9]).

One of the technologies that is used in several countries for mobile proximity payments based on SCT are QR-codes. Typical transactions include for example ticketing but also pilots for in-shop purchases have been launched during the past years. However, in most cases the SEPA Credit Transfer is initiated through proximity technology but authorised remotely, thus facilitating the subsequent transaction.

If a C2C scheme for SCT-Inst was developed it could be enhanced to allow mobile proximity technology to identify the beneficiary, but the instruction and authorisation by the payer is still likely to be done remotely.

SCT	Consumer	Business
Consumer	**C2C** • Offers a practical service for personal payments, including cheque and cash displacement • Certainty of fate would increase proposition, e.g., instant SCT scheme • "Viral" growth opportunity	**C2B** • Offers a practical service for payments, including cheque and cash displacement • Certainty of fate for SCT payments would increase merchant proposition, e.g., instant SCT scheme
Business	**B2C** • Unlikely to be used by businesses and large corporates • Using the mobile channel to initiate SCTs, a business would be acting like a consumer • Therefore the scenario is no different to the C2C scenario	**B2B** • Unlikely to be used by businesses and large corporates • Using the mobile channel to initiate SCTs, a business would be acting like a consumer • Therefore the scenario is no different to the C2B scenario

Table 7: Mobile Proximity SEPA Credit Transfer Payments: focus levels

4.2.2.2 Mobile Remote Payments (MRP) analysis

Enhancements with respect to customer authentication and transaction risk management for remote payments have been continuously addressed during the last years (see for instance [2]) and are expected to further evolve in view of PSD2 (see [21]). There is potential for some mobile-specific enhancements, which could help to develop this channel for SEPA payments.

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

	SEPA Cards	SDD	SCT
C2C			
C2B			
B2C			
B2B			

	Low Focus
	Medium Focus
	High Focus

Table 8: Mobile Remote Payments: focus levels

The following sections provide a high level view on each of these three payment types.

Mobile Remote SEPA Card Payments

Card transactions tend to be made by consumers (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. Therefore there is no need to develop distinct use-cases for such scenarios.

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

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. However, a mass-market cross-border acceptance will largely depend 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.

A typical example of a Business-to-Consumer (B2C) transaction is a refund.

SEPA Card	Consumer	Business
Consumer	**C2C** • Offers a practical service for personal payments, including cheque and cash displacement • Needs cooperation for cross-border implementation 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 in recent years
Business	**B2C** • Very unlikely for a business to be paying a consumer by card unless a refund, which is similar to a C2B service • Even if the card is a business or purchasing card, the cardholder acts as a consumer • Therefore this scenario is no different to the C2C scenario	**B2B** • Even if the card is a business or purchase card, the cardholder acts as a consumer • Therefore this scenario is no different to the C2B scenario • Could be a very practical cheque displacement opportunity for small businesses

Table 9: Mobile Remote SEPA Card Payments: focus levels

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 10: Mobile Remote SEPA Direct Debit Payments: focus levels

Mobile Remote SEPA Credit Transfer Payments

The SCT offers the possibility for using SEPA payments in the mobile area. As the payment is a PSP-to-PSP transfer, it works equally well for consumer, business and government 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 and/or availability of funds is required in many situations;
- For payers, the use of a suitable beneficiary identifier is essential. In most circumstances it will not be practical for a payer to input the IBAN and other relevant information of the beneficiary while using a mobile device.

SCT	Consumer	Business
Consumer	**C2C** • Offers a practical service for spontaneous personal payments, including cheque and cash displacement • Needs a practical service for beneficiary ID (mobile number or other 'alias' could be a solution) • May require central repository function • Certainty of fate would increase proposition e.g., instant SCT scheme • "Viral" growth opportunity	**C2B** • Offers a practical service for personal payments, including cheque and cash displacement • Needs a practical service for beneficiary ID for smaller businesses • Certainty of fate for SCT payments would increase merchant proposition, e.g., instant SCT scheme
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 no different to the C2C scenario	**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 no different to the C2B scenario

Table 11: Mobile Remote SEPA Credit Transfer Payments: focus levels

5 Mobile Proximity Payments

5.1 Introduction

In the context of this document, Mobile Proximity Payments (MPPs) are SEPA payments (SCT, SDD, SCP) which are initiated using a mobile device where the consumer and the merchant (and/or their equipment) are in the same location and where the communication between the mobile device and the POI terminal takes place through a proximity technology (e.g., NFC, 2D barcodes, BLE, etc.). This means that the payment transaction is dependent on a physical contact with a POI such as a point of sale terminal.

5.2 Use-cases – Mobile Contactless SEPA Card Payments

This section provides a short description of Mobile Contactless SEPA Card Payments (MCPs), which are defined as any contactless SEPA Card payment executed by a cardholder (the consumer) using an NFC enabled mobile device. Regardless which technology (see section 7) 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 (see [4]).

It 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 device user interface are mentioned they are also purely illustrative.

Below, three generic Consumer-to-Business (C2B) SEPA MCPs are described, irrespective of the type of card used (credit, debit or prepaid). B2B is implemented if the consumer is a business.

5.2.1 MCP 1 - Mobile Contactless SEPA Card Payment - Tap and Go

The scenario presented in Figure 2 depicts a possible checkout procedure at a groceries store for a low value payment transaction.

Before the scenario commences, the consumer would need to subscribe first to the mobile payments service for their payment card. They further may select it as the default payment instrument within the mobile wallet configuration menu. As an option, the consumer enters their mobile code or fingerprint to “open” the MCP service before starting the transaction.

In the figure below, the following steps are illustrated:

1. The merchant starts by entering the transaction amount on the POI terminal.
2. The consumer either selects a payment card via a dedicated menu on the mobile device for the payment or the default payment card (preselected on the consumer’s mobile device) is automatically used for the payment. Therefore, to confirm the payment transaction, the consumer only needs to tap the mobile device 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.

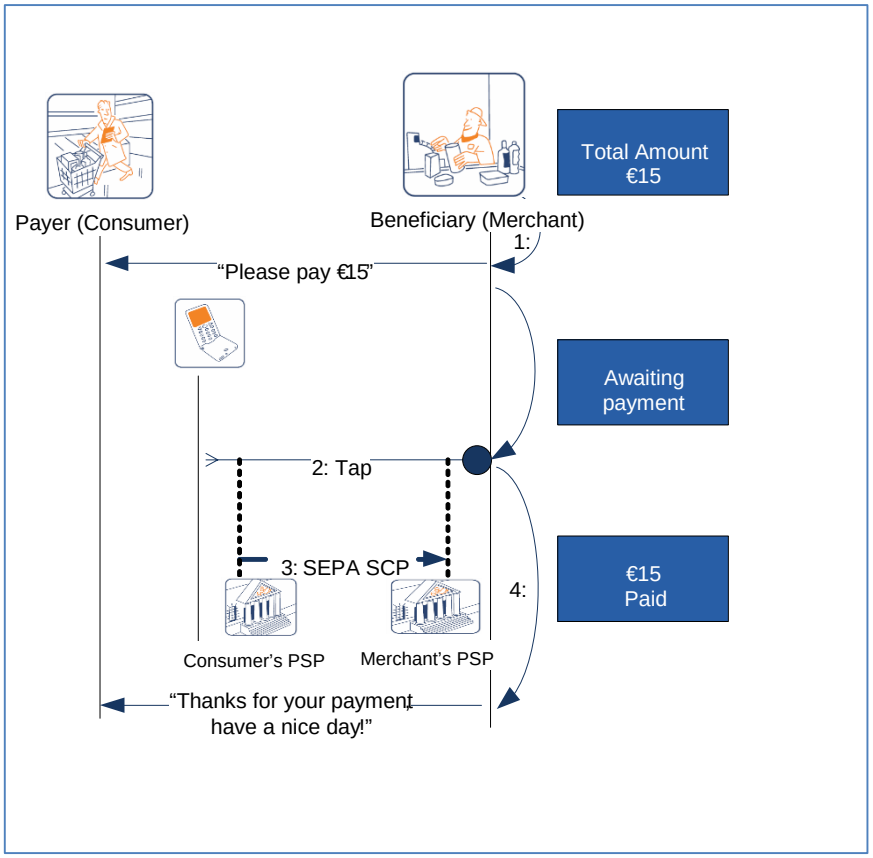

Figure 2: MCP 1 - Mobile Contactless SEPA Card Payment - Tap and Go

MCP 1 - Mobile Contactless SEPA Card Payment - Tap and Go	
Category	Consumer-to-Business (C2B). Also applicable to B2B.
Communication type	Contactless
Payment instrument	SEPA Card
Payment initiation by	Merchant
Prerequisites	• Consumer subscribed to MCP Service • Consumer pre-selected a payment card as default in their mobile device or selects a payment card on the mobile device at transaction time. As an option, the consumer enters their mobile code to "open" the MCP service before starting the transaction • Payment Token stored on mobile device as needed • Merchant with NFC-enabled POI terminal • Merchant agreement.
Payment authorisation mode by consumer	Tap at NFC enabled POI terminal
Merchant benefits	• Access to broader consumer base • Highly-efficient payment processing • Speed of transaction when the consumer chooses to "open" the MCP application before starting the transaction • Additional value added services such as loyalty, couponing, etc. • Cheque and cash displacement
Consumer benefits	• Convenience, mobility • Speed of transaction when the consumer chooses to "open" the MCP application before starting the transaction • Further reduction of cash handling • Reduced cash handling and cheque displacement • Smaller queues
Challenges	Transaction time[8]

Table 12: MCP 1 - Mobile Contactless SEPA Card Payment - Tap and Go

5.2.2 MCP 2 - Mobile Contactless SEPA Card Payment - Double Tap with Mobile Code

Figure 3 depicts a possible checkout procedure at a groceries store for a high value payment transaction where the consumer enters their mobile code on the mobile device.

Before the scenario commences, the consumer would need to subscribe first to the mobile payments service for their payment card. They further may select it as the default payment instrument within the mobile wallet configuration menu.

[8] A description of more general challenges related to mobile contactless payments may be found in [10].

In the figure below, the following steps are illustrated:

1. The merchant starts by entering the transaction amount on the POI terminal.
2. The consumer taps their mobile device on the NFC-enabled POI terminal area.
3. The consumer either selects a payment card via a dedicated menu on the mobile device for the payment or the default payment card (preselected on the consumer's mobile device) is automatically used for the payment. To confirm the payment transaction, the consumer only needs to enter their mobile code[9] onto the mobile device.
4. Next, the consumer taps the mobile device a second time on the NFC-enabled POI terminal area.
5. The transaction is then processed as a standard SEPA SCP transaction.
6. The merchant is able to check the payment.

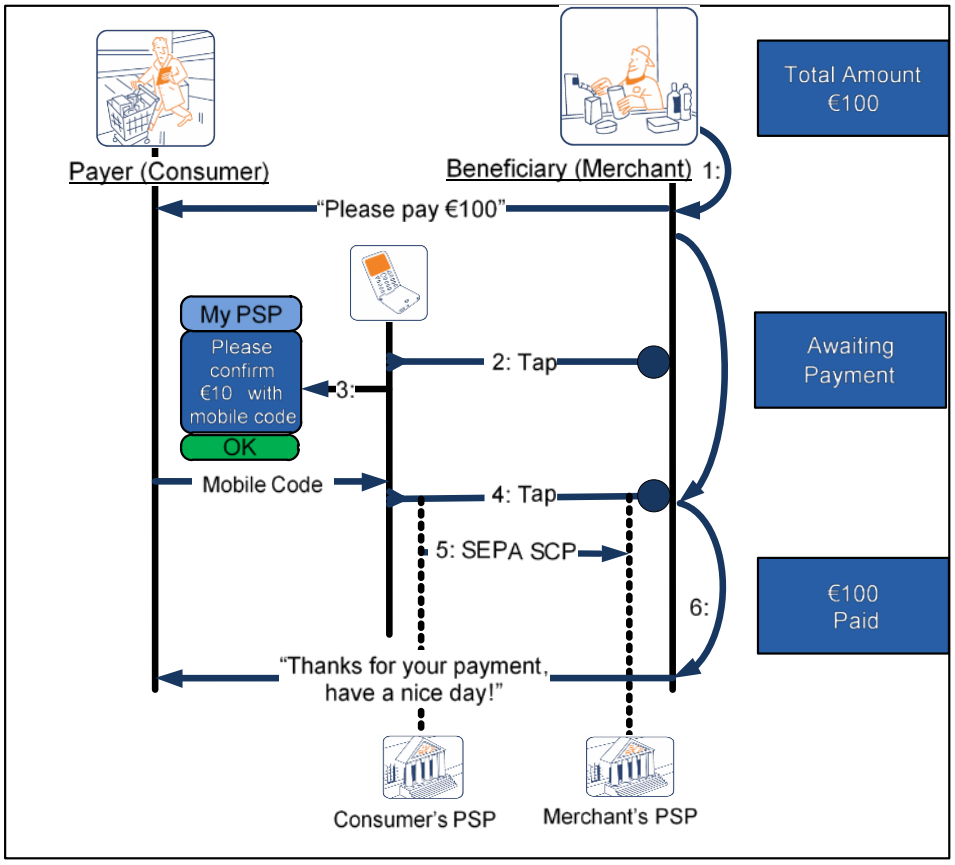

Figure 3: MCP 2 - Mobile Contactless SEPA Card Payment - Double Tap with Mobile Code

[9] For security reasons, it is strongly recommended that 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 information is provided in [4] and [5].

MCP 2 - Mobile Contactless SEPA Card Payment - Double Tap with Mobile Code	
Category	Consumer-to-Business (C2B). Also applicable to B2B.
Communication type	Contactless
Payment instrument	SEPA Card
Payment initiation by	Merchant
Prerequisites	• Consumer subscribed to MCP Service • Consumer pre-selected a payment card as default in their mobile device or selects a payment card on the mobile device at transaction time. • Payment Token stored on mobile device as needed • Merchant with NFC-enabled POI terminal. • Merchant agreement.
Payment authorisation mode by consumer	• 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. • Cheque and cash displacement
Consumer benefits	• Convenience, mobility • Further reduction of cash handling • Reduced cash handling and cheque displacement
Challenges	Education / acceptance of new payment experience by both the consumer and the merchant.[10]

Table 13: MCP 2 - Mobile Contactless SEPA Card Payment - Double Tap with Mobile Code

5.2.3 MCP 3 - Mobile Contactless SEPA Card Payment - Single Tap and PIN

The scenario presented in Figure 4 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 their PIN code on this POI terminal.

Before the scenario commences, the consumer would need to subscribe first to the mobile payments service for their payment card. They further may select 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 on the POI terminal.
2. The consumer taps their mobile device on the NFC-enabled POI terminal area.
3. The consumer either selects a payment card via a dedicated menu on the mobile device for the payment or the default payment card (preselected on the consumer's mobile device) is automatically used for the payment.

[10] A description of more general challenges related to mobile contactless payments may be found in [10].

4. The consumer is requested to enter their PIN code on the POI to complete the transaction. Information about the current transaction is optionally displayed on the mobile device.
5. The consumer enters their PIN code[11] on the POI terminal to confirm the payment transaction.
6. The transaction is then processed as standard SEPA SCP transaction.
7. The merchant is able to check the payment.

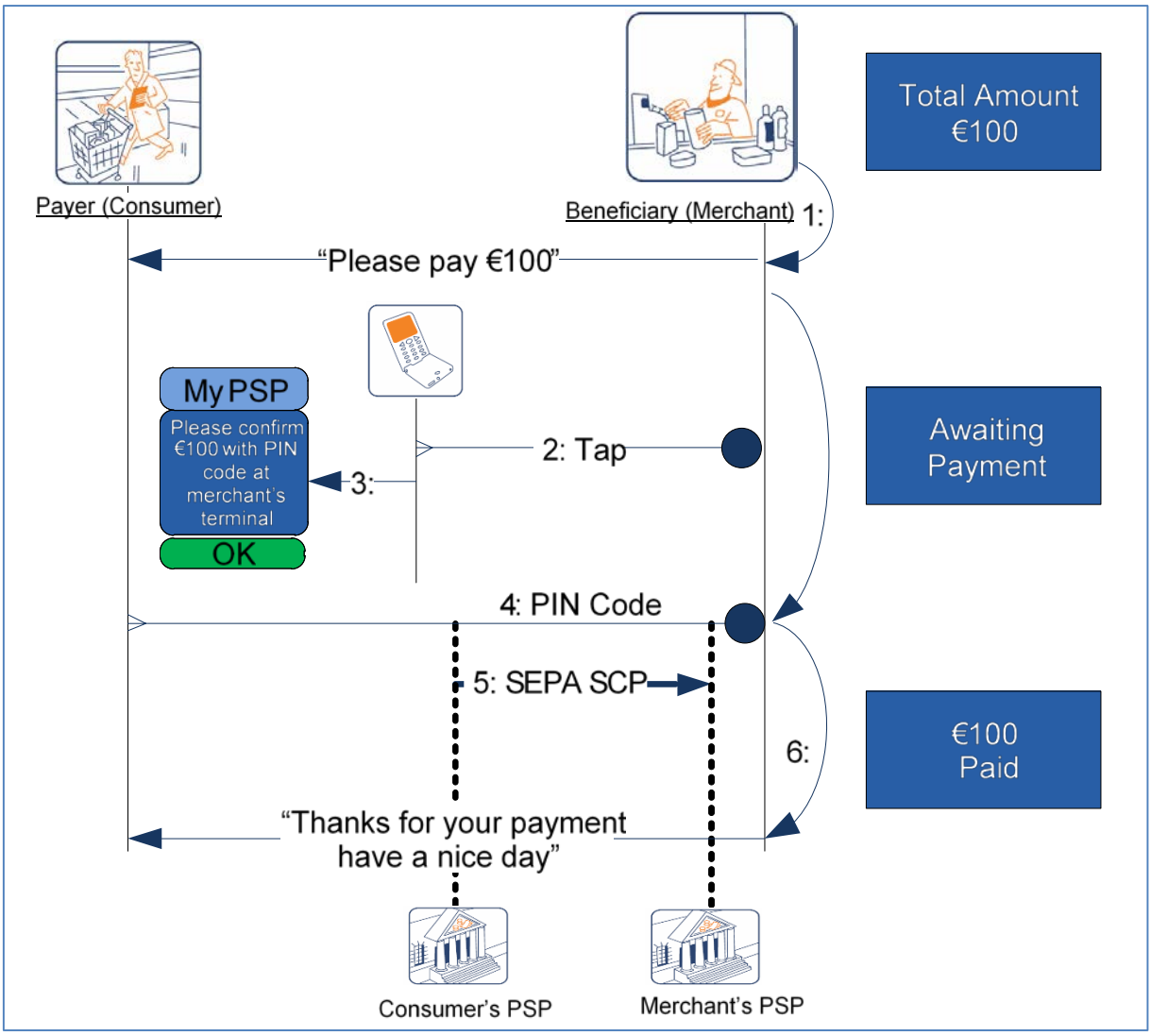

Figure 4: MCP 3 - Mobile Contactless SEPA Card Payment - Single Tap and PIN

[11] Same as the PIN used for conducting contact-based card payment transactions with a POI having an encrypted PIN pad.

MCP 3 - Mobile Contactless SEPA Card Payment - Single Tap and PIN	
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 MCP Service • Consumer pre-selected a payment card as default in their mobile device or selects a payment card on the mobile device at transaction time. • Payment Token stored on mobile device as needed • Merchant with NFC-enabled on-line POI terminal. • Merchant agreement.
Payment authorisation mode by consumer	PIN code entry on POI terminal
Merchant benefits	• Access to broader consumer base • Additional value added services such as loyalty, couponing, etc. • Cheque and cash displacement
Consumer benefits	• Convenience, mobility • Further reduction of cash handling • Reduced cash handling and cheque displacement
PSP benefits	This contactless payment service may also be used at ATMs
Challenges	No specific challenges in the mobile channel compared to card payments.[12]

Table 14: MCP 3 - Mobile Contactless SEPA Card Payment - Single Tap and PIN

5.3 Use-cases – Mobile Proximity SEPA Credit Transfers

5.3.1 MPCT 1 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer

The scenario presented in Figure 5 depicts a possible checkout procedure at a groceries store.

Before the scenario commences, the consumer would need to subscribe first to the mobile payments service and download the dedicated app linked to a specific account (IBAN) on their mobile device.

In the figure below, the following steps are illustrated:

1. The merchant starts by entering the transaction amount on the POI terminal which generates a QR code over the transaction amount and the merchant's IBAN.

[12] A description of more general challenges related to mobile contactless payments may be found in [10]

2. The consumer selects the MPP application on their mobile device and scans the QR code with their mobile device from the POI terminal.
3. To confirm the payment transaction the consumer enters their mobile code on their mobile device.
4. The MPP app initiates an SCT-Inst with the consumer's PSP.
5. The consumer's PSP then processes and submits the SCT-Inst to the merchant's PSP which in turn will credit the merchant.
6. The merchant will be able to get confirmation that the payment has been received and has access to the funds.

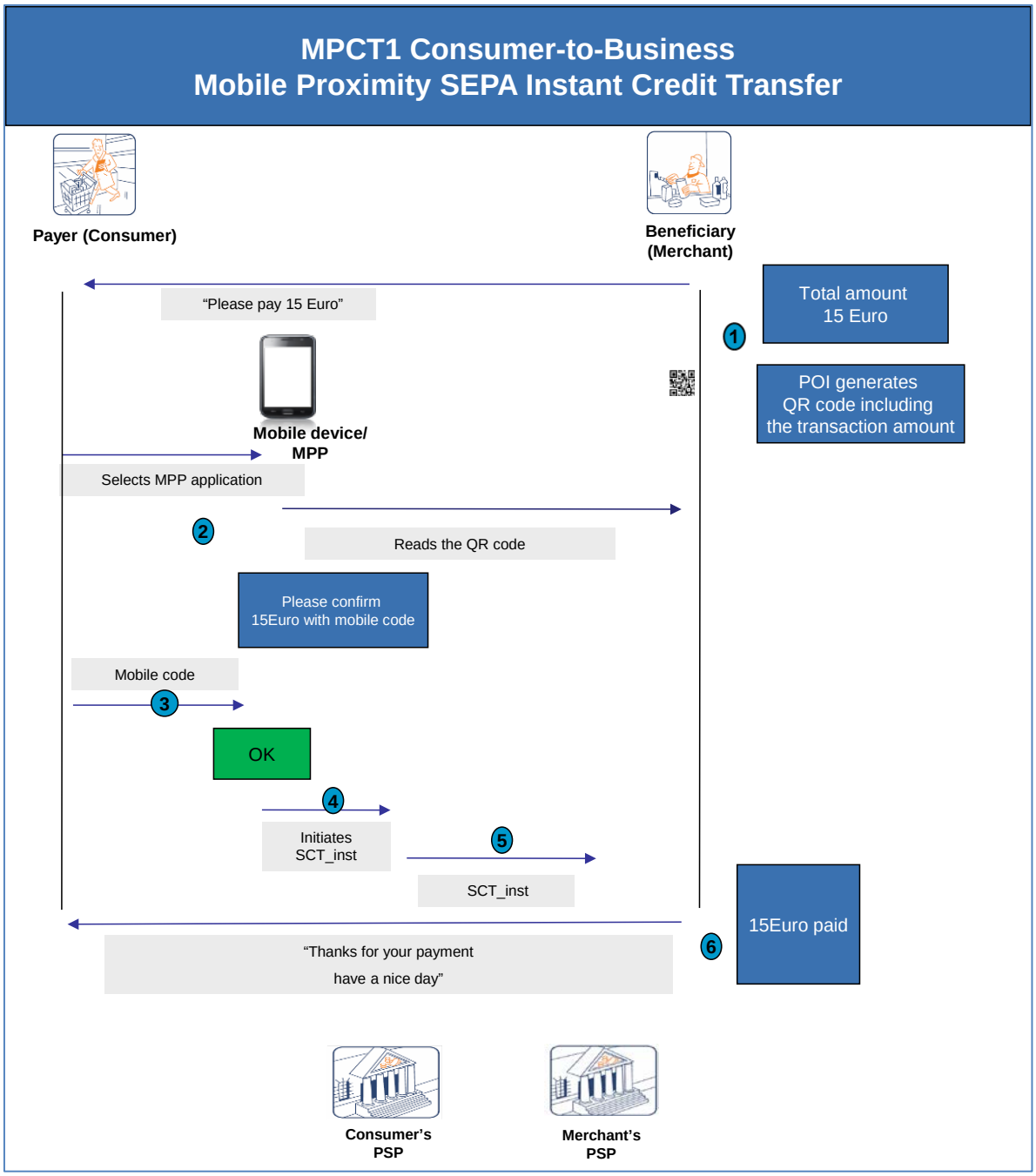

Figure 5: MPCT1 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer

MPCT 1 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer	
Category	Consumer-to-Business (C2B), also applicable to B2B
Communication type	Proximity, QR code
Payment instrument	SEPA Instant Credit Transfer
Payment initiation by	Merchant
Prerequisites	• The establishment of an Instant SEPA Credit Transfer scheme • Consumer subscribed to MPP Service • Consumer downloaded dedicated MPP app on mobile device • Consumer selects MPP app on mobile device • Merchant subscribed to MPP Service (depending on implementation) • Merchant with POI terminal with dedicated QR application.
Payment authorisation mode by consumer	Mobile code entry on mobile device
Merchant benefits	• Access to broader consumer base • Additional value added services such as loyalty, couponing, etc. • Cheque and cash displacement
Consumer benefits	• Convenience, mobility • Reduced cash handling and cheque displacement
PSP benefits	• Full control over the payment service ecosystem • Further reduction of cash handling
Challenges	• The set up and operation of the SCT-Inst scheme • Interoperability of MPP solutions based on QR codes

Table 15: MPCT 1 – Consumer-to-Business Mobile Proximity Instant Credit Transfer

5.3.2 MPCT 2 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer

The scenario presented in Figure 6 depicts a possible checkout procedure at a groceries store.

Before the scenario commences, the consumer would need to subscribe first to the mobile payments service and download the dedicated app linked to a specific account (IBAN) on their mobile device. Both the payment app and the merchant's POI terminal are connected to a common infrastructure (see section 7). The merchant's POI terminal

has a unique identifier (POI_ID) in the payment system which is included in a unique QR code, displayed on the terminal.

In the figure below, the following steps are illustrated:

1. The merchant starts by entering the transaction amount on the POI terminal. The POI terminal reports to the common infrastructure that it is waiting for a payment confirmation on a given transaction (amount, POI_ID, etc.).
2. The consumer opens their mobile payment app in the mobile device and scans the QR code from the POI.
3. The mobile payment app retrieves the POI_ID from the QR code and communicates the POI_ID to the common infrastructure.
4. The common infrastructure connects the transaction from the POI terminal with the payment consumer's mobile payment app and transmits the necessary transaction information to the mobile payment app for confirmation.
5. The transaction details are displayed in the mobile payment app on the consumer's mobile device with a request for confirmation of the transaction.
6. The consumer enters their mobile code to confirm the transaction.
7. A transaction confirmation by the payer is returned to the common infrastructure and upon successful validation an SCT-Inst[13] is initiated (between the appropriate PSPs).
8. The common infrastructure sends a payment confirmation to the POI terminal.
9. Both the consumer (on their mobile device) and the merchant (at the POI terminal) receive notification of the transaction.

[13] Note that this use case is also applicable with a card payment as underlying payment instrument.

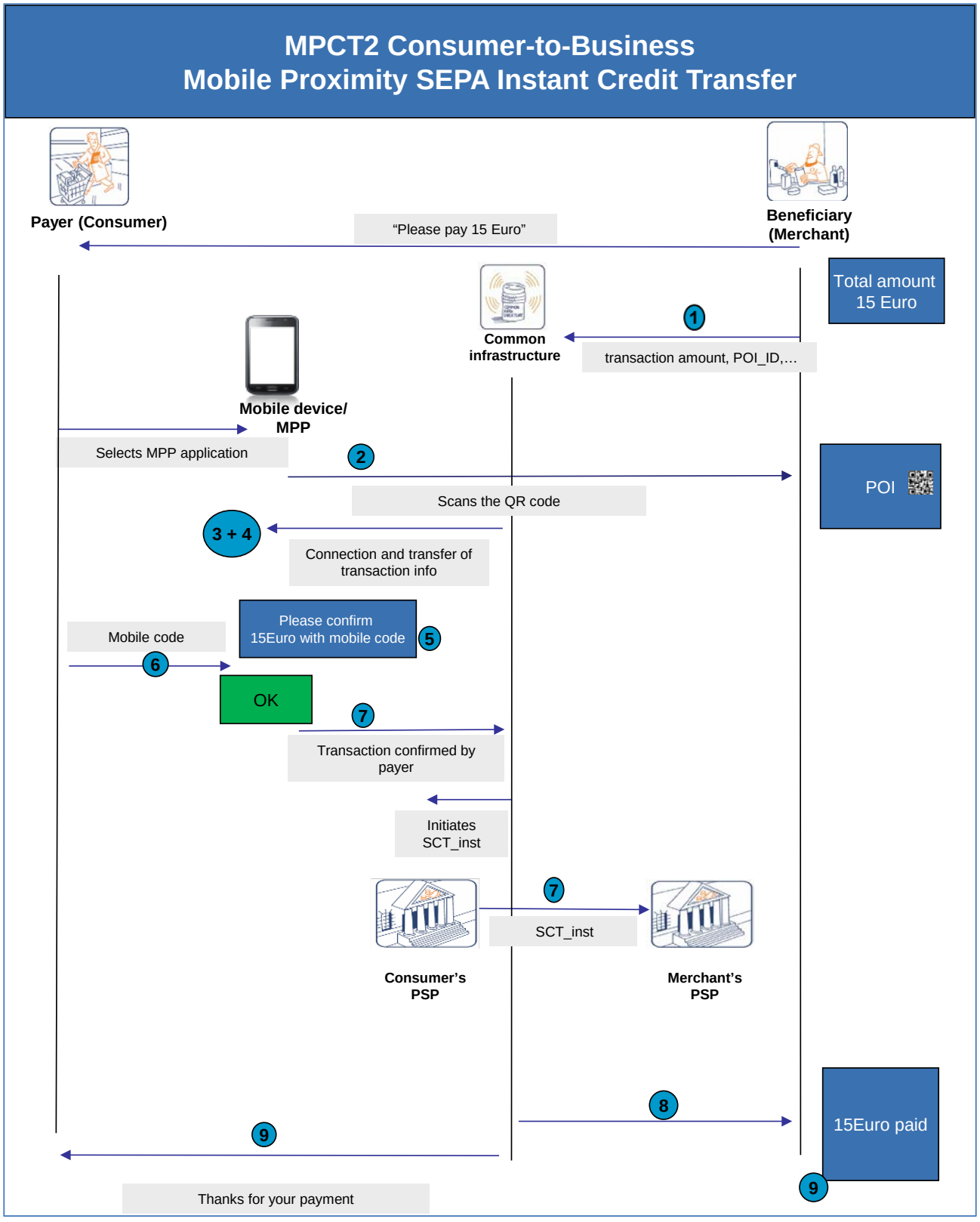

Figure 6: MPCT2 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer

MPCT2 – Consumer-to-Business Mobile Proximity SEPA Instant Credit Transfer	
Category	Consumer-to-Business (C2B), also applicable to B2B
Communication type	Proximity, QR code
Payment instrument	SEPA Instant Credit Transfer
Payment initiation by	Merchant
Prerequisites	• The establishment of an Instant SEPA Credit Transfer scheme • Consumer subscribed to MPP Service • Merchant subscribed to MPP Service • Consumer downloaded dedicated MPP app on mobile device • Consumer selects MPP app on mobile device • Merchant with POI terminal with dedicated QR code
Payment authorisation mode by consumer	Mobile code entry on mobile device
Merchant benefits	• Access to broader consumer base • Additional value added services such as loyalty, couponing, etc. • Cheque and cash displacement
Consumer benefits	• Convenience, mobility • Further reduction of cash handling • Reduced cash handling and cheque displacement
PSP benefits	Full control over the payment service ecosystem
Challenges	• The set up and operation of the SCT-Inst scheme • Implementation of common infrastructure • Interoperability of MPP solutions based on QR codes

Table 16: MPCT 2 – Consumer-to-Business Mobile Proximity Instant Credit Transfer

5.4 Ecosystem

5.4.1 Introduction

Mobile proximity payments (MPPs) introduce a new ecosystem involving new participants in the chain. Even if many of the stakeholders involved in the MPP transaction do not differ from those involved in a “classic” card or SCT payment, MPPs need to rely on a series of technical infrastructure elements that are unique to the mobile environment for the management of the MPP service life cycle processes.

5.4.2 Stakeholders

- The consumer is a natural person who makes the mobile payment; he/she owns a SEPA payment account or a SEPA compliant card, a mobile device and would need to hold an active subscription with an MNO;

- The merchant is the acceptor for payment of the goods or services purchased by the consumer;

- The PSP offers SEPA payment services compliant with regulatory/security requirements;
- The MNO is responsible for securely routing messages, operating the mobile network, issuing and recycling mobile phone numbers.
- The payment system functions are both provided by a SEPA compliant payment scheme and a clearing and settlement mechanism (CSM);
- The MCP/MPP issuer is the PSP responsible for provisioning the application to the consumer.
- The SE issuer is a key stakeholder in the ecosystem if the MCP/MPP application is stored in an SE on the mobile device. This is the MNO in case of a UICC, the mobile equipment manufacturer, the MCP/MPP issuer or a third party in case of an embedded SE, the MCP/MPP issuer or a third party in case of a secure micro SD card (see section 4 in [5]).
- The Trusted Service Manager (TSM) is a TTP acting on behalf of the SE issuers and/or the MCP/MPP application issuers to facilitate an open ecosystem in case an SE is involved to host the MCP/MPP application(s). As illustrated in the figure below, MCP/MPP issuers, TSMs and SE issuers collaborate to perform the provisioning and management of the MCP/MPP application(s). Several TSMs may co-exist offering mutually-competing services both to the SE and MCP/MPP issuers.
- The Token Service Provider (TSP) is a TTP which is involved if payment tokens are used in mobile proximity payments as surrogate values for payer account related data (e.g., the PAN for card payments, the IBAN for SCTs). The TSP manages the generation and issuance of payment tokens, and maintains the established mapping of payment tokens to the payer account related data when requested by the token requestor. The TSP service may also include the capability to establish the token assurance level to indicate the confidence level of the payment token to the payer account related data / payer / merchant / device / environment binding. The TSP also provides the capability to support token processing of payment transactions submitted using payment tokens by de-tokenising the payment token to obtain the actual account related data.
- The Mobile Wallet Issuer is a service provider that issues mobile wallet functionalities to the customer (consumer or merchant).
- Other relevant new stakeholders include for example:
  - SE manufacturers
  - Cloud service providers
  - Trusted Party Payment Instrument Issuer
  - Application developers (MPP/MCP application, AAUI, mobile wallet …).
  - Mobile equipment manufacturers.
  - Organisations performing infrastructure certification (e.g., SEs, MPP/MCP applications, POI, etc.).

5.4.3 Service models

Two main phases need to be distinguished for mobile proximity payments (MPPs): the payment transaction itself and the provisioning and life cycle management of the mobile

proximity application. The service models vary according to the phase as described below.

5.4.3.1 Payment transaction

An MPP does not in any way modify the underlying SEPA payment transaction. Therefore the service model of the latter remains unaffected. This is illustrated below in the case of a Mobile Contactless Payment (MCP).

As shown in Figure 7 below, the main parties involved in an MCP transaction 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]).

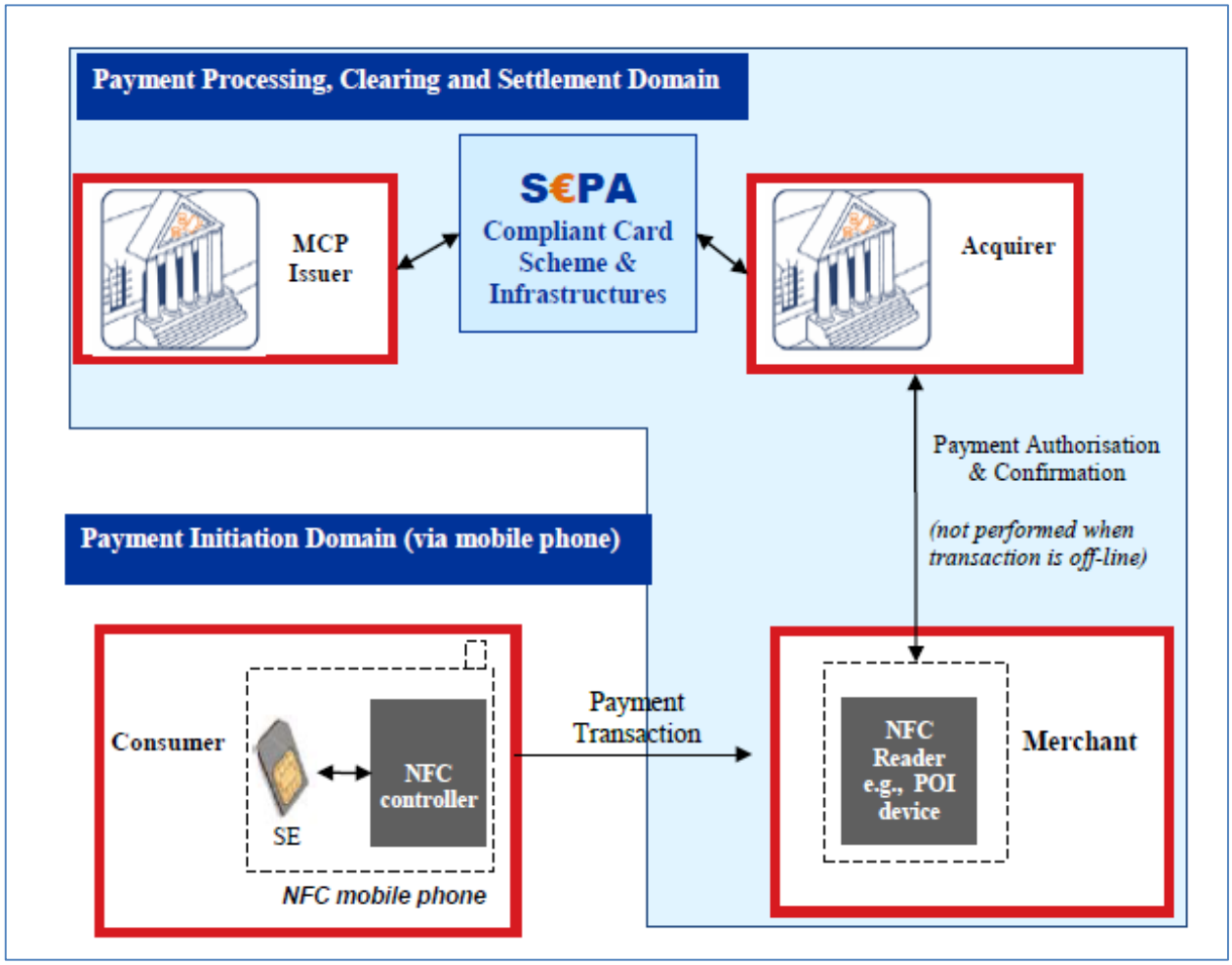

Figure 7: MCP transaction[14]

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

5.4.3.2 Provisioning and management

As defined in ISO 12812-Part 1 (see [18]), a mobile payment application is defined as a set of modules (application software) and/or data (application data) needed to provide functionality for a mobile payment service as specified by the mobile payment application issuer in accordance with the payment scheme. General guidelines on the life cycle management of mobile payment applications is provided in ISO 12812 - Part 3 (see [18]).

Some years ago, specific guidance has been developed for the roles covering the functions related to mobile contactless payment applications (MCPs). In order to facilitate the introduction of a rich ecosystem of service providers performing TSM functions, the EPC and the GSMA had jointly developed requirements and specifications for the MCP service management roles for MCP applications residing on a UICC [6]. Many service models are possible by delegating combinations of the different roles (technical and commercial) to one or more TSMs. The service management roles for other types of Secure Elements (see Annex II) and their related service models have subsequently been described in a document by the EPC (see [5]).

However, due to the introduction of HCE based solutions and tokenisation during recent years, many new stakeholders have been introduced in the MCP ecosystem which fulfil specific roles in the provisioning and life cycle management of an MCP application. More guidance on these new models are for instance provided in [1], [12] and [17].

6 Mobile Remote Payments

6.1 Introduction

In the context of this document, Mobile Remote Payments (MRPs) are SEPA payments (SCT, SDD, SCP) which are initiated using a mobile device 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 their equipment). This means that the payment transaction is not dependent on a physical contact with a POI such as a POS terminal.

6.2 Use-cases - Mobile Remote SEPA Card Payments

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

6.2.1 MRCP 1 - Consumer-to-Business Mobile Remote SEPA Card Payment - Basic

In this scenario, illustrated in Figure 8, the consumer uses their mobile device 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 their mobile device the consumer will start by navigating to the checkout section of the merchant's website[15];
2. The merchant's website will present the payment information on the consumer's mobile phone;
3. The consumer selects the "payment by card" option via internet and is redirected to the payment section under the control of a payment gateway to proceed with the transaction under a secure http connection (https). He/she enters their payment card details (card number, expiry date and card security code) and initiates a remote SCP transaction;
4. The transaction is then further processed as a basic[16] SEPA card m-commerce transaction (see [4]);

   The merchant releases the goods or services to the consumer.

[15] Alternatively the consumer may use a dedicated application in the mobile device.

[16] Basic m-commerce refers to a static card authentication (see [4]).

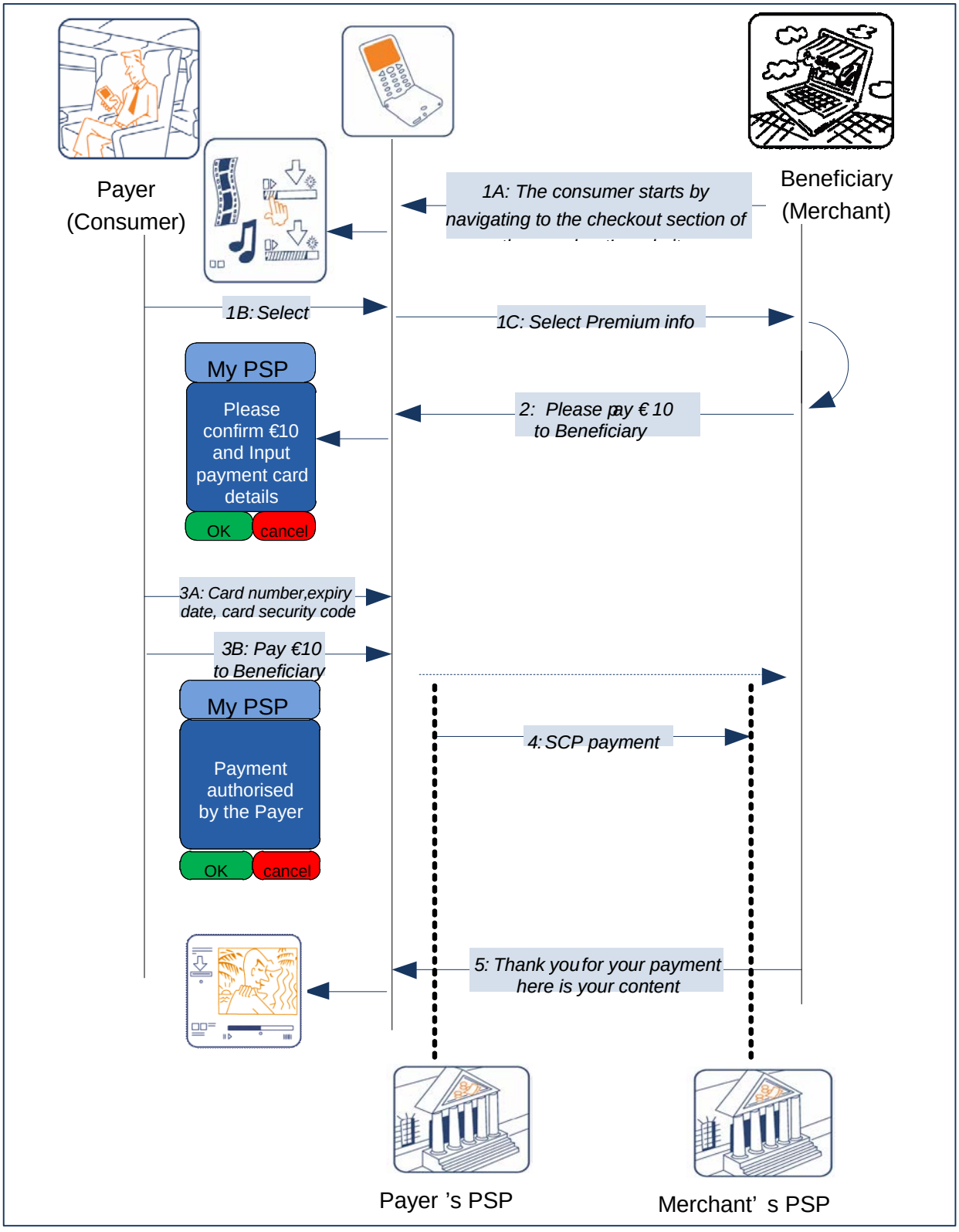

Figure 8: MRCP 1 - Consumer-to-Business Mobile Remote SEPA Card Payment -Basic

MRCP 1 - Consumer-to-Business Mobile Remote SEPA Card Payment – Basic	
Category:	Consumer-to-Business (C2B), also applicable to B2B
Communication type	Remote
Payment instrument	SEPA Card
Payment initiation by	Merchant
Prerequisites	• Merchant accepts remote card payments for a given card scheme • Consumer has a compliant card within the same card scheme
Payment authorisation mode by consumer	Determined by the PSP (card issuer) in accordance with the card scheme
Merchant benefits	• Access to broader consumer base • Merchant anytime accessible by the consumer • Cheque and cash displacement
Consumer benefits	• Convenience, mobility • Further reduction of cash handling • Reduced cash handling and cheque displacement
Challenges	• No specific challenges in the mobile channel compared to other remote card payments via internet • For the payer: inconvenience for the consumer to enter their credentials via the mobile device (could be solved by e.g., usage of a mobile wallet[17]) • For the beneficiary: since this is a CNP transaction, the merchant has no certainty about the payment (the issuer has chargeback rights)

Table 17: MRCP 1 - Consumer-to-Business Mobile Remote SEPA Card Payment - Core

6.2.2 MRCP 2 - Consumer-to-Business Mobile Remote SEPA Card Payment - Mobile Wallet

In this scenario, illustrated in Figure 9, the consumer uses their mobile device 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 consumer makes use of a mobile wallet[18] to access and retrieve their payment card details when making the payment to the merchant.

From the merchant's perspective, the scenario is very similar to MRCP 1.

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

[18] See also section 8 and [7] for more information on mobile wallets.

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

In the figure below, the following steps are illustrated:

1. While browsing the internet with their mobile device the consumer will start by navigating to the checkout section of the merchant's website[19];
2. The merchant's website will present the payment information on the consumer's mobile phone;
3. The consumer selects the "payment by card" option via internet and is redirected to the payment section under the control of a payment gateway to proceed with the transaction under a secure http connection (https). The consumer payment card details are provided through the use of a mobile wallet and the consumer's entry of the card security code, which initiates a remote SCP transaction;
4. The transaction is then further processed as a "basic" SEPA card m-commerce transaction (see [4]).
5. The merchant releases the goods or services to the consumer.

[19] Alternatively, the consumer may use a dedicated application on the mobile device.

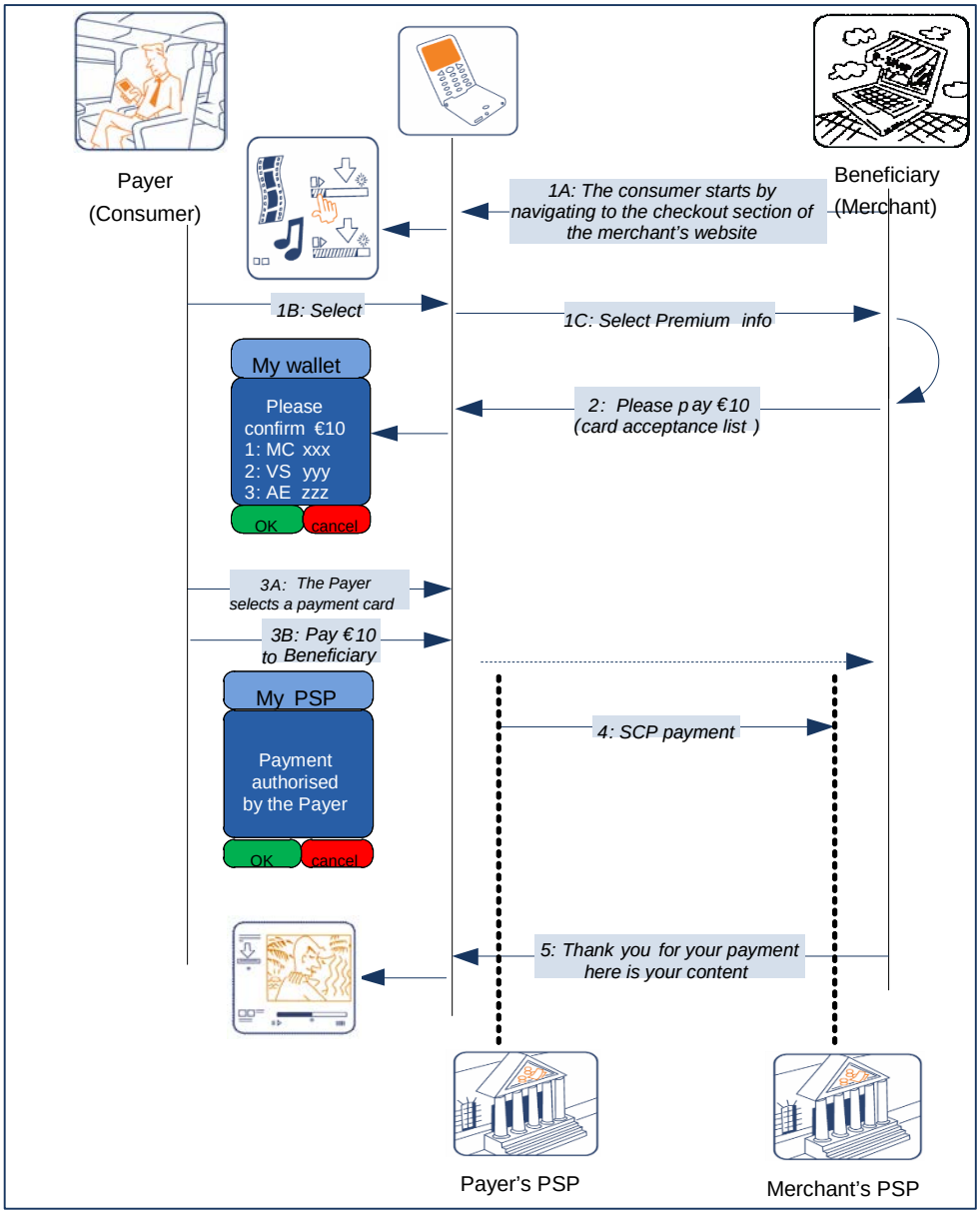

Figure 9: MRCP 2 - Consumer-to-Business Mobile Remote SEPA Card Payment - Mobile Wallet

MRCP 2 - Consumer-to-Business Mobile Remote SEPA Card Payment - Mobile Wallet	
Category:	Consumer-to-Business (C2B), also applicable to B2B
Communication type	Remote
Payment instrument	SEPA Card
Payment initiation by	Merchant
Prerequisites	• Merchant accepts remote card payments for a given card scheme • Consumer has a compliant card within the same card scheme
Payment authorisation mode by consumer	Determined by the PSP (card issuer) in accordance with the card scheme
Merchant benefits	• Access to broader cardholder base • Merchant anytime accessible by cardholder • Cheque and cash displacement
Consumer benefits	• Convenience, mobility • Convenience for the consumer to choose a payment card with associated credentials, using a mobile wallet. • Reduced cash handling and cheque displacement
Challenges	• No specific challenges in the mobile channel compared to other remote card payments via internet • Payer authentication: the consumer is not allowed to store the card security code, the consumer normally still would need to enter this value to perform the transaction which is not very user-friendly.

Table 18: MRCP 2 - Consumer-to-Business Mobile Remote SEPA Card Payment - Mobile Wallet

6.2.3 MRCP 3 - Consumer-to-Business Mobile Remote SEPA Card Payment - Strong cardholder authentication

The difference between this scenario and the MRCP 2 scenario described above, is that the payer is required to take an extra authentication step. As a dynamic card-based authentication such as CAP (Chip Authentication Program) or DPA (Dynamic Passcode Authentication) may be used for remote card transactions, the access via a mobile device to a secure environment which hosts a similar (dedicated) dynamic authentication application could be a considerable enhancement with respect to consumer convenience. The usage of this dynamic authentication application would typically need to be subject to a mobile code entered by the consumer on the mobile device and verified by the dynamic authentication application, resulting into a “strong customer authentication” in accordance to [21]. This authentication gives the merchant greater protection against fraudulent or repudiated transactions. Moreover, if the mobile device already provides an MCP service, this could also be leveraged for authentication purposes for remote card transactions.

The card issuer(s) would need to install a (dedicated) dynamic authentication application in a secure environment (e.g. in the SE of the consumer's mobile device or on a remote server). Furthermore, the consumer would need to enable the authentication application(s) for conducting remote payments e.g., within a mobile wallet configuration menu on their mobile device.

As another alternative, if the payer has both an NFC enabled mobile phone and a contactless physical card including a dynamic 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 would need to be subject to a mobile code entered by the consumer on their mobile phone.

In the Figure 10 below, the following steps are illustrated:

1. While browsing the internet with their mobile device, the consumer will start by navigating to the checkout section of the merchant's website[20];
2. The merchant's website will present the payment information on the consumer's mobile device;
3. The consumer payment card details are provided through the use of a mobile wallet and he/she initiates an SCP transaction. The dynamic authentication application authenticates the consumer. This involves the entry of a mobile code by the consumer on their mobile device;
4. The transaction is then further processed as a "secured" SEPA card m-commerce transaction (see [4]).
5. The merchant releases the goods or services to the consumer.

[20] Alternatively the consumer may use a dedicated application in the mobile device.

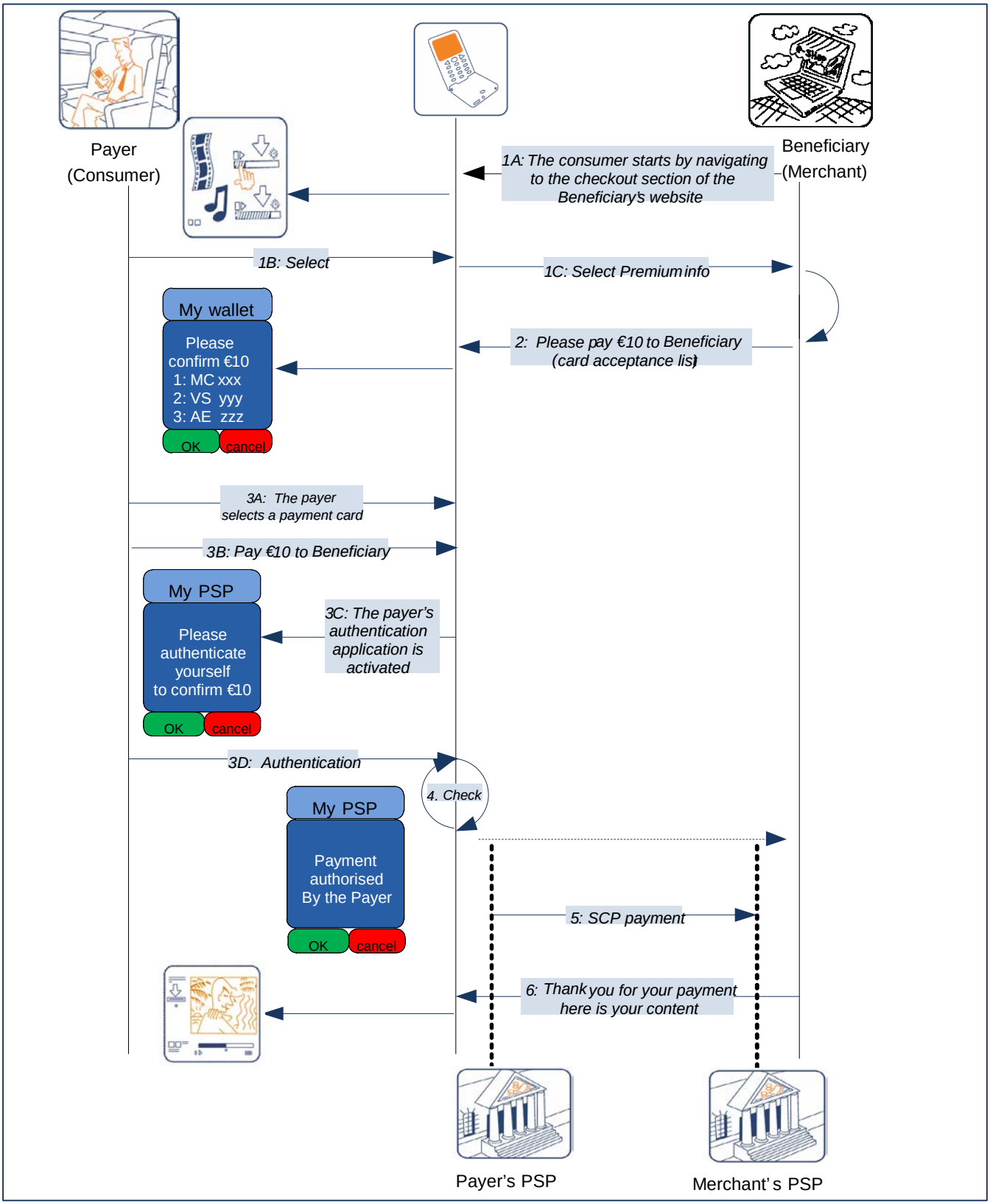

Figure 10: MRCP 3 - Consumer-to-Business Mobile Remote SEPA Card Payment - Strong cardholder authentication

MRCP 3 - Consumer-to-Business Mobile SEPA Card Payment - Strong cardholder authentication	
Category:	Consumer-to-Business (C2B), also applicable to B2B
Communication type	Remote
Payment instrument	SEPA Card
Payment initiation by	Merchant
Prerequisites	• Merchant accepts remote card payments for a given card scheme • Consumer has a compliant card within the same card scheme
Payment authorisation mode by consumer	Determined by the PSP (card issuer) in accordance with the card scheme
Merchant benefits	• Access to broader cardholder base • Merchant anytime accessible by cardholder • Reduction of remote card payment fraud • Cheque and cash displacement
Consumer benefits	• Convenience, mobility • Convenience for the consumer: more automated handling of the authentication • Further reduction of cash handling • Reduced cash handling and cheque displacement
Challenges	• No specific challenges in the mobile channel compared to other remote card payments via internet

Table 19: MRCP 3 - Consumer-to-Business Mobile Remote SEPA Card Payment - Strong cardholder authentication

6.2.4 MRCP 4 - Consumer-to-Consumer Mobile Remote SEPA Card Payment

Figure 11 introduces a possible example of user experience for a consumer-to-consumer SEPA card payment initiated by a mobile device where a consumer (payer) wants to make a personal payment to a another consumer (beneficiary) with their mobile device.

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 their 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). A prerequisite for this scenario is that the payer has subscribed to a (possibly, but not necessarily, mobile specific) C2C card payment system with their card issuer. Many of the major card schemes already offer some proprietary C2C services, but these would need to achieve cross-border 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 their 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 (e.g., via the entry of a mobile code).
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 instant use of funds;
- The beneficiary needs certainty of receipt to proceed with an underlying transaction e.g., a sale of goods or rendering of services between strangers.

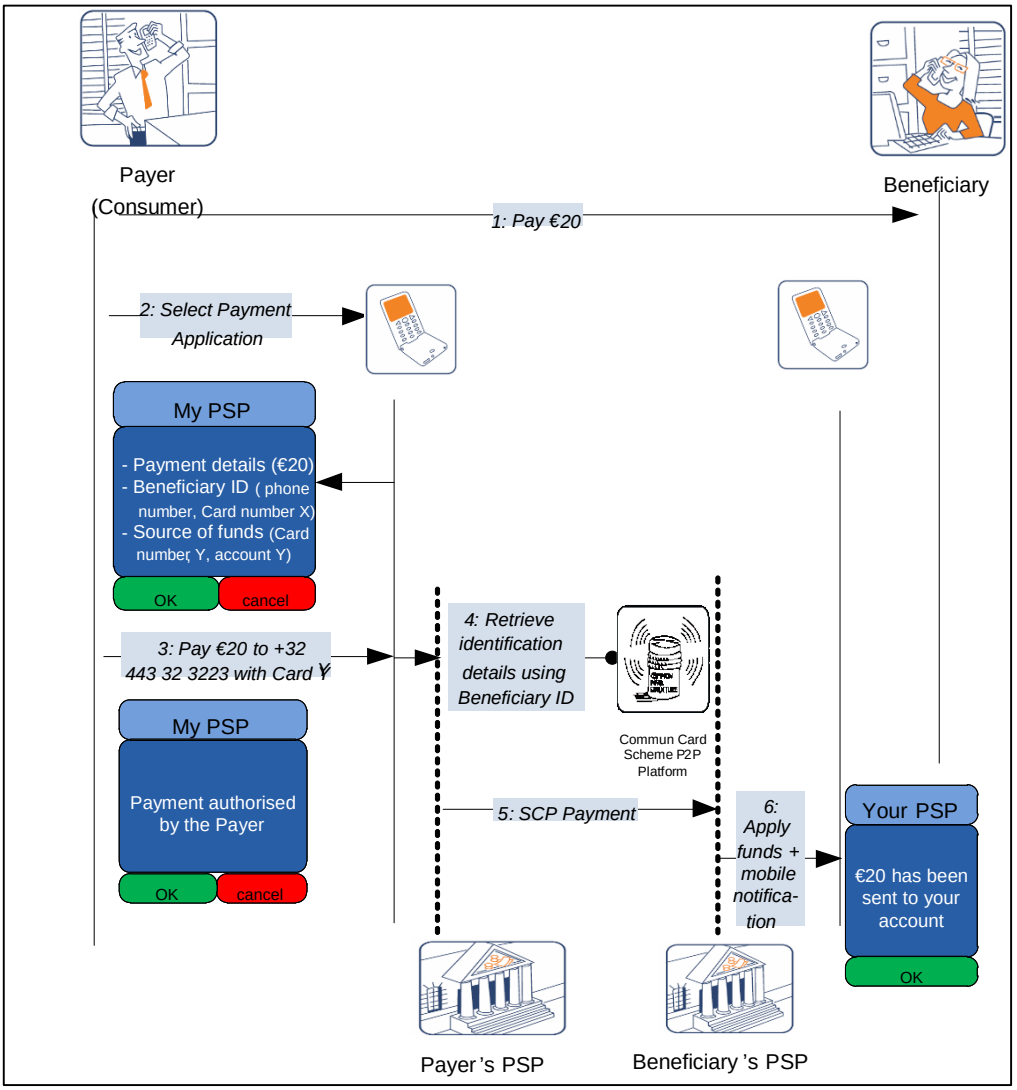

Figure 11: MRCP 4 - Consumer-to-Consumer Mobile Remote SEPA Card Payment

MRCP 4 - Consumer-to-Consumer Mobile Remote SEPA Card Payment	
Category	Primarily Consumer-to-Consumer (C2C), some scenarios for Consumer to (e.g., small) Business (C2B)
Communication type	Remote
Payment instrument	SEPA Card
Payment initiation by	Payer
Prerequisites	• Beneficiary is identifiable with a unique identifier, generally, but not necessarily, a payment card • Payer has a compliant card and is subscribed to a mobile C2C card payment system by their PSP (card issuer)
Payment authorisation mode by consumer	Determined by the PSP (card issuer) in accordance with the card scheme
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 • Cheque and cash displacement
Challenges	• Ensuring card scheme interoperability • Management and support of unique beneficiary identifier if required • For the payer: inconvenience to enter the beneficiary's identifier into the mobile phone (could be solved, for example, by the usage of stored beneficiaries in a mobile wallet)

Table 20: MRCP 4 -Consumer-to-Consumer Mobile Remote SEPA Card Payment - Core

6.3 Use-cases - Mobile Remote SEPA Credit Transfers

The use-cases described in this section are based on an SCT (SEPA Credit Transfer) as underlying SEPA payment instrument[21]. This means that, independently of the initiation steps, the actual SCT transaction is always based on the usage of the IBAN. Note also that under the current SCT rules, the maximum processing time between PSPs for an SCT is one business day (D+1). However, the EPC is in the process of specifying a new – optional – instant credit transfer scheme: SCT-Inst (see [8]) with immediate interbank clearing of the transaction and availability of the funds for the payee (within seconds of payment initiation).

[21] Note that the use cases presented may also be applied to non SEPA areas.

6.3.1 MRCT 1 - Consumer-to-Consumer Mobile Remote SCT – Static authentication via mobile browser

Figure 12 introduces a possible example of user experience whereby the consumer (payer) uses their mobile device to conduct an MRCT from their payment account to the payment account of another consumer (beneficiary) using a mobile browser.

Furthermore, it concerns a low value payment whereby a static authentication is applied (in accordance to [2]).

In many circumstances, this use-case remains valid for C2B, B2C and B2B (in particular for small businesses).

In the figure below, the following steps are illustrated:

0. The payer and the beneficiary agree upon the amount to be paid to the beneficiary (which is assumed to be low value). Subsequently, the beneficiary provides all the appropriate payment information to the payer, including IBAN as necessary.
1. The payer opens a mobile banking session with their PSP in accordance with the security policy of their PSP (e.g.; by entering user id and password) through their mobile device via a mobile browser and selects the MRCT service.
2. Next, the payer selects the account (IBAN_pay) he/she wants to use in case he/she holds several eligible payment accounts and enters the details of the transaction via their mobile device including at least:
    - The transaction amount,
    - The identification (IBAN_ben) of the beneficiary's account to be credited; this information can be input by the payer in full or by accessing a pre-registered beneficiary.
3. The payer enters an on-line static passcode[22] via their mobile device to authorise the credit transfer request.
4. The credit transfer request including the passcode is provided to the payer's PSP.
5. The payer's PSP checks the completeness of the transaction related data entries and verifies the on-line passcode and the data received.
6. The payer's PSP checks the availability of funds on the payer's account, prepares and submits the credit transfer instruction to the beneficiary's PSP.
7. The beneficiary's PSP credits the beneficiary's account with the transaction amount.
8. The beneficiary optionally receives a message from their PSP that their account has been credited. The payer optionally receives a message from their PSP informing them that the selected account has been debited.

[22] Typically the passcode used for on-line (internet) banking.

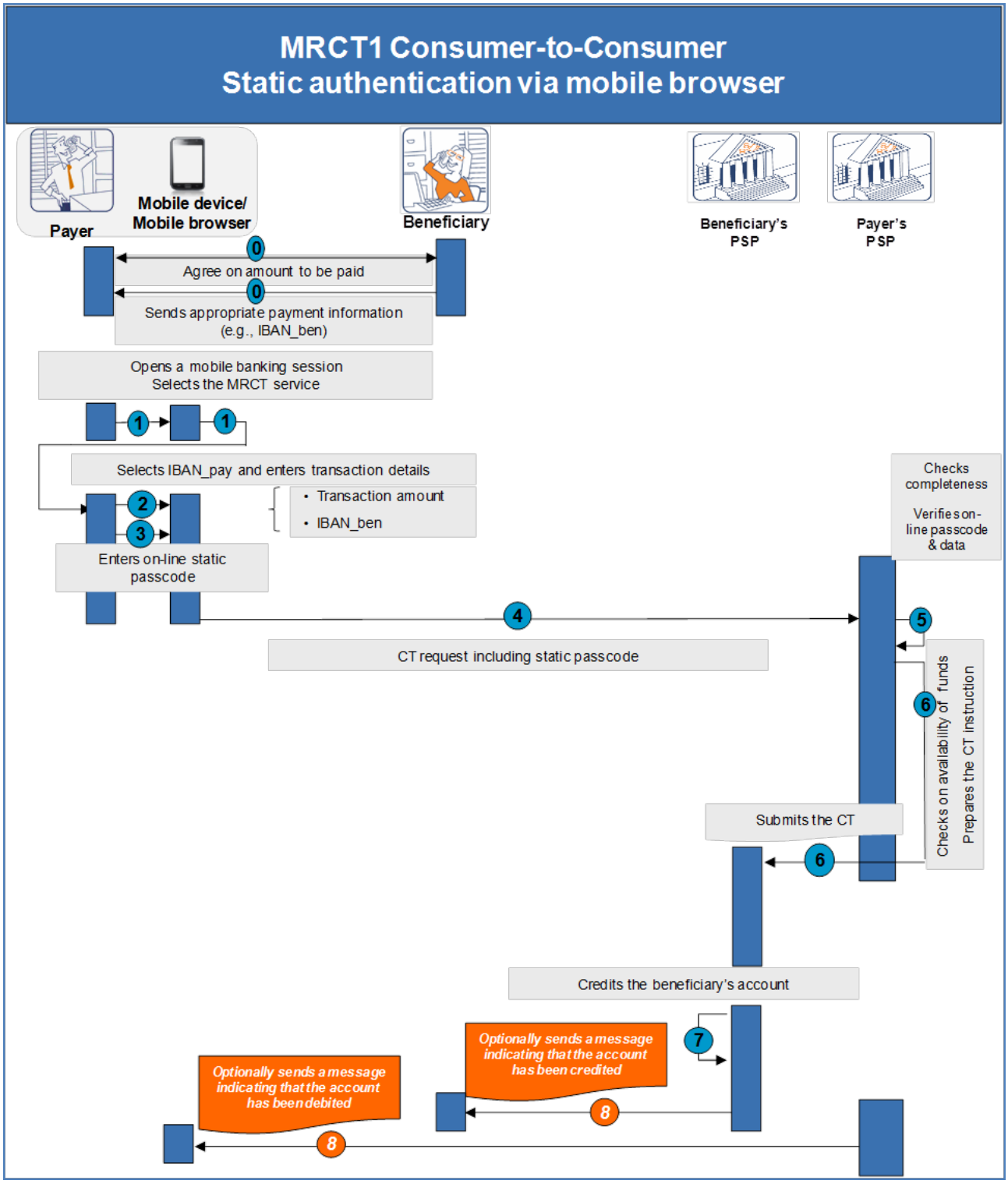

Figure 12: MRCT 1 - Consumer-to-Consumer Mobile Remote SCT – Static authentication via mobile browser

MRCT 1 - Consumer-to-Consumer Mobile Remote SCT – Static authentication via mobile browser	
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 authorisation mode by consumer	Determined by the payer's PSP in accordance with the remote payment scheme based on SCT
Customer benefits	• Mobility for payer • Cheque and cash displacement
Challenges	• For the payer: o Inconvenience of importing credentials o Number and complexity of steps required to initiate the SCT o Potential for error • For the beneficiary: o May find inconvenient or undesirable to provide /reveal their IBAN o No immediate confirmation of irrevocability of payment o Dependent on SCT clearing cycle and services of their PSP for execution of payment

Table 21: MRCT 1 - Consumer-to-Consumer Mobile Remote SCT – Static authentication via mobile browser

6.3.2 MRCT 2 - Consumer-to-Consumer Mobile Remote SCT – Alias –Strong authentication via MRCT application in mobile wallet

Figure 13 introduces a use case whereby the consumer (payer) uses their mobile device to conduct an MRCT from their own payment account to the payment account of another consumer (beneficiary) using an MRCT application (a so-called P2P application) accessed via a mobile wallet (see [7]). Payer and beneficiary may, and frequently will, hold their payment accounts with different PSPs (4-corner model[23]- see section 5.5.2).

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 and a strong authentication is performed (in accordance to [2]).

In view of the usage of an alias, a so-called "Common Infrastructure" (see section 7) needs to be established and operated (e.g., by the P2P Scheme) that enables the registration of the beneficiary aliases against their account details.

[23] 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 many circumstances, this use-case remains valid for B2B (in particular for small businesses).

In the figure below, the following steps are illustrated:

0. The payer and the beneficiary agree upon the amount to be paid to the beneficiary. Subsequently, the beneficiary provides their alias to the payer.
1. The payer opens the mobile wallet he/she wishes to use. This might involve the entry of a mobile wallet passcode (see [7]). Next the payer selects the MRCT (P2P) payment application in the mobile wallet.
2. Once the MRCT application is selected, the IBAN_pay is self-populated by the mobile wallet.

   The payer enters the details of the transaction via his mobile device:

   - The transaction amount,
   - The beneficiary's alias; this information may be manually entered by the payer on the mobile device or selected via the mobile wallet in case of a pre-registered beneficiary.
3. The credit transfer request is provided to the payer's PSP.
4. The payer's PSP checks the completeness of the transaction related data entries. The payer's PSP sends the beneficiary's alias to a common infrastructure which returns the appropriate payment information details of the beneficiary (e.g., account name and IBAN_ben) and their PSP to allow the correct routing of the payment transaction.
5. Subsequently, the payers' PSP sends an authentication request including the beneficiary's account name and a challenge to the MRCT application in the mobile device of the payer.
6. The authentication request is handled automatically by the MRCT application in the payer's mobile device. The beneficary's account name and the transaction amount payer are displayed on the mobile device while the payer is requested to enter his/her mobile code once during the transaction. If the mobile code verification is successfully performed by the MRCT application, it calculates an authentication response which is provided to the payer's PSP.
7. The payer's PSP verifies the authentication response and the data received.
8. The payer's PSP checks the availability of funds on the payer's account and prepares the credit transfer instruction. The payer's PSP submits the credit transfer instruction to the beneficiary's PSP.
9. The beneficiary's PSP credits the beneficiary's account with the transaction amount.
10. The beneficiary optionally receives a message from his/her PSP that their account has been credited. The payer optionally receives a message from his/her PSP informing that their account has been debited.

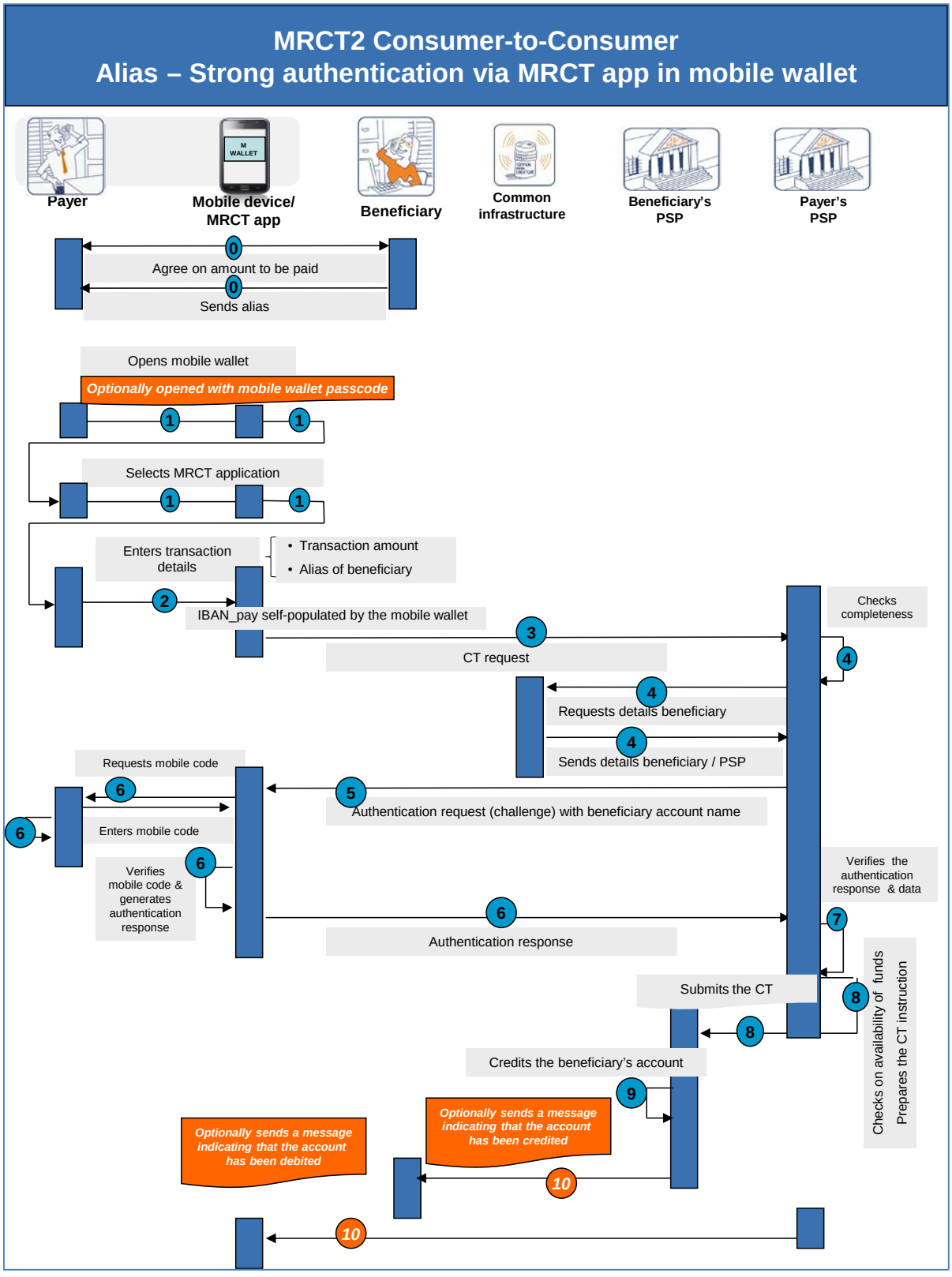

Figure 13: MRCT 2 - Consumer-to-Consumer Mobile Remote SCT– Alias - Strong authentication via MRCT application in mobile wallet

MRCT 2 - Consumer-to-Consumer Mobile Remote SCT–Alias – Strong authentication via MRCT application in mobile wallet	
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 the their identification details in a common infrastructure • The payer's PSP would need access to the common infrastructure • The payer's PSP would need to offer the alias-based mobile payment service
Payment authorisation mode by consumer	Determined by the payer's PSP in accordance with the remote payment scheme based on SCT
Customer benefits	• Convenience, mobility • Beneficiary does not have to remember and reveal their identification (e.g., IBAN) to the payer • Cheque and cash displacement
Challenges	• Agreement on alias format. • The set up and operation of the common infrastructure • For the beneficiary: o No immediate confirmation of irrevocability of payment o Dependent on SCT clearing cycle and services of their own PSP for execution of payment

Table 22: MRCT 2 - Consumer-to-Consumer Mobile Remote SCT – Alias - Strong authentication via MRCT application in mobile wallet

6.3.3 MRCT 3 - Consumer-to-Business Mobile Remote SCT-Inst – QR code – Strong authentication via MRCT application

In this use-case illustrated in Figure 14, a possible consumer experience is presented whereby he/she uses a mobile device to pay an invoice using an MRCT from their own payment account to the payment account of a merchant (beneficiary). Payer and beneficiary may, and frequently will, hold their payment accounts with different PSPs (4-corner model[24], section 5.5.2). Hereby a dedicated MRCT application on the mobile device is used.

Furthermore, a merchant QR code (including the name, the IBAN_ben of the merchant and the transaction amount) on the invoice will be in place, making the input of the

[24] 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.

merchant details considerably more convenient for the consumer. In this payment transaction a strong authentication is performed (in accordance to [21]).

In many circumstances, this use-case is also applicable for B2B (in particular for small businesses).

In the figure below, the following steps are illustrated:

0. The merchant sends an invoice to the consumer containing a QR code (which includes the merchant name, the transaction amount and the IBAN_ben).
1. The consumer selects and opens the MRCT application on their mobile device which possibly involves the entry of a password. Subsequently, the consumer scans the QR code from the merchant invoice using their mobile device.
2. Once the MRCT application is selected, the consumer selects the IBAN_pay he/she wants to use in case there are several eligible payment accounts, while the transaction amount and the IBAN_ben are automatically retrieved from the QR code.
3. The credit transfer request is provided to the consumer's PSP.
4. The consumer's PSP checks the completeness of the transaction related data entries and sends an authentication request including a challenge to the MRCT application in the mobile device of the consumer.
5. The authentication request is handled automatically by the MRCT application in the consumer's mobile device. The consumer is requested to enter their mobile code once during the transaction. If the mobile code verification is successfully performed by the MRCT application, it calculates an authentication response which is provided to the consumer's PSP.
6. The consumer's PSP verifies the authentication response and the data received.
7. The consumer's PSP checks on the availability of funds on the consumer's account, prepares and submits the credit transfer instruction to the merchant's PSP.
8. The merchant's PSP credits the merchant's account with the transaction amount.
9. The merchant optionally receives a message from his/her PSP that their account has been credited. The consumer optionally receives a message from their PSP informing that the selected account has been debited.

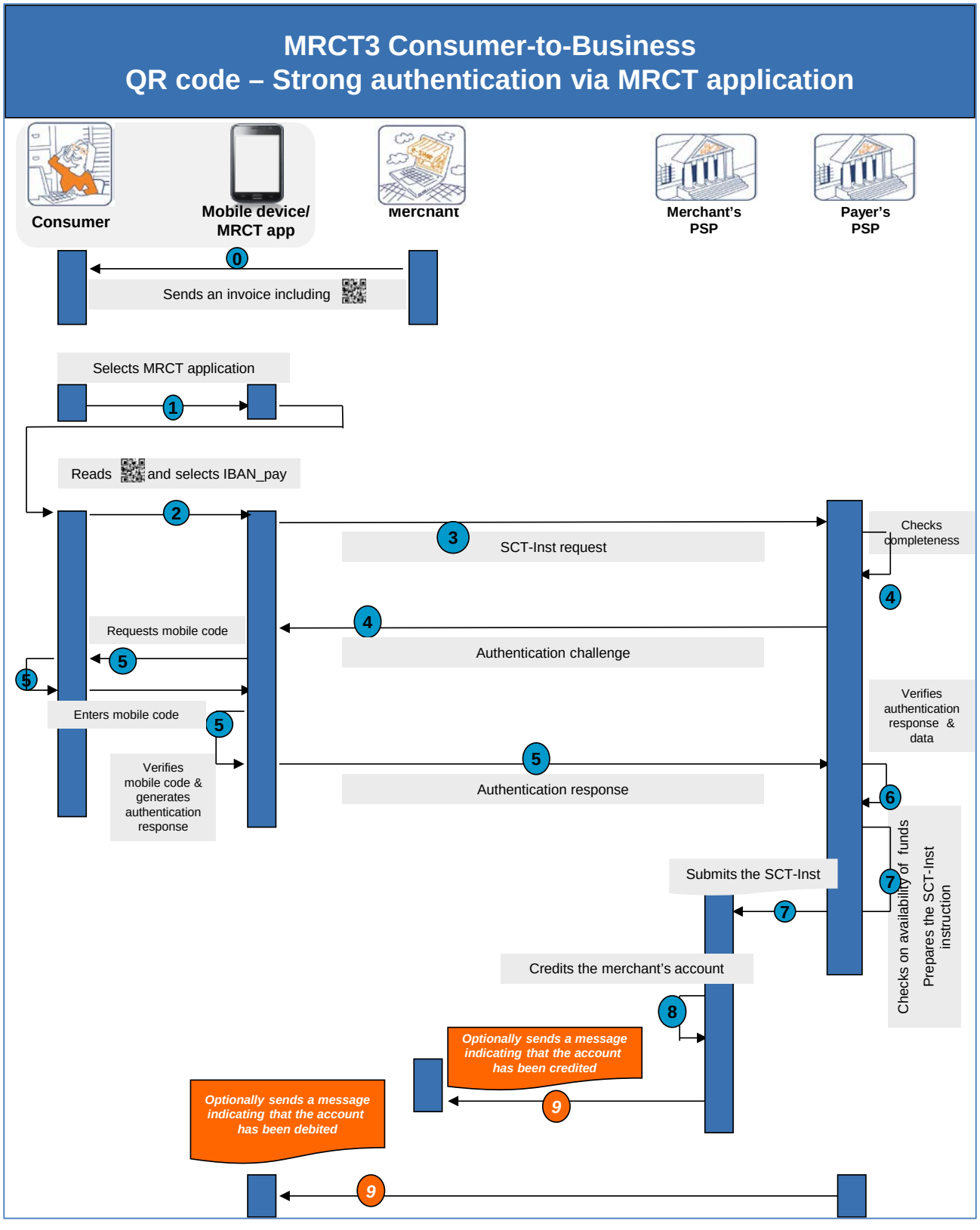

Figure 14: MRCT 3 - Consumer-to-Business Mobile Remote SCT-Inst - QR code – Strong authentication via MRCT application

MRCT 3 - Consumer-to-Business - Mobile Remote SCT-Inst - QR code – Strong authentication via MRCT application	
Category	Consumer-to-Business (C2B), also applicable to B2B.
Communication type	Remote
Payment instrument	SEPA Instant Credit Transfer
Payment initiation by	Payer
Prerequisites	• The payer's and the beneficiary's PSP would need to participate in the SCT-Inst scheme • The payer needs to download a dedicated MRCT app on their mobile device
Payment authorisation mode by consumer	Determined by the payer's PSP in accordance with the remote payment scheme based on SCT
Merchant benefits	• Convenience, mobility, speed • Cheque and cash displacement • Immediate confirmation of payment: this allows the beneficiary to release goods or services.
Consumer benefits	• Convenience, mobility, speed • Reduced cash handling and cheque displacement • Speed up the release of goods or services
Challenges	• The set-up and operation of a SCT-Inst scheme

Table 23: MRCT 3 - Consumer-to-Business - Mobile Remote SCT-Inst - QR code – Strong authentication via MRCT application

6.3.4 MRCT 4 - Consumer-to-Business – Mobile Remote SCT-Inst - Consumer redirection with strong authentication via mobile browser

In this use-case illustrated in Figure 15, a possible example of user experience is presented whereby the consumer (payer) uses their mobile device to pay for goods or services delivered by a merchant (beneficiary). Hereby an SCT-Inst is used from the consumer's payment account to the payment account of the merchant (beneficiary) which is initiated using a mobile browser. Payer and beneficiary may, and frequently will, hold their payment accounts with different PSPs.

Furthermore, the consumer is redirected from the merchant's website to their PSP's mobile service (e.g., a mobile banking system) where a strong authentication is performed (in accordance to [2]).

In the figure below, the following steps are illustrated:

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

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

1. The customer is redirected with the transaction details including the beneficiary's name, transaction amount and IBAN_ben to the TPP portal.
2. The consumer is invited to enter their preferred PSP on this portal for this transaction.

3. An instant credit transfer request including the transaction amount, the beneficiary's name and IBAN_ben are forwarded to the consumer's PSP.
4. The consumer is redirected with the instant credit transfer request reference by the e-payment scheme portal to the mobile service of their PSP.
5. The consumer is invited to enter their user-ID and identification data in accordance with the security policy of their PSP. After successful identification, the instant credit transfer reference with the transaction details including the transaction amount and merchant are displayed to the consumer.
6. The consumer's PSP sends an authentication request including a dynamic authenticator[25] (e.g., using a one-per-transaction number) via SMS to the consumer.
7. The consumer is subsequently requested to copy this dynamic authenticator into a dedicated authentication page to authorise the credit transfer request which is provided to their PSP.
8. The consumer's PSP verifies the dynamic authenticator and the data received.
9. The consumer is redirected based on previously received referral information by their PSP, via the TPP portal to the merchant.
10. The consumer's PSP checks the availability of funds on the consumer's account and sends a confirmation of credit transfer acceptance to the TPP.
11. The merchant is informed by the TPP about the payment confirmation which enables the release of the goods or services to the consumer.
12. The consumer receives confirmation from the merchant on the delivery of goods or services.
13. The consumer's PSP prepares and submits the SCT-Inst instruction to the merchant's PSP.
14. The merchant's PSP credits the merchant's account with the transaction amount.
15. The merchant optionally receives a message from his/her PSP that their account has been credited. The consumer optionally receives a message from their PSP informing that their account has been debited.

[25] Note that other dynamic authentication methods exist such as challenge/response based, which will be further elaborated in a forthcoming document.

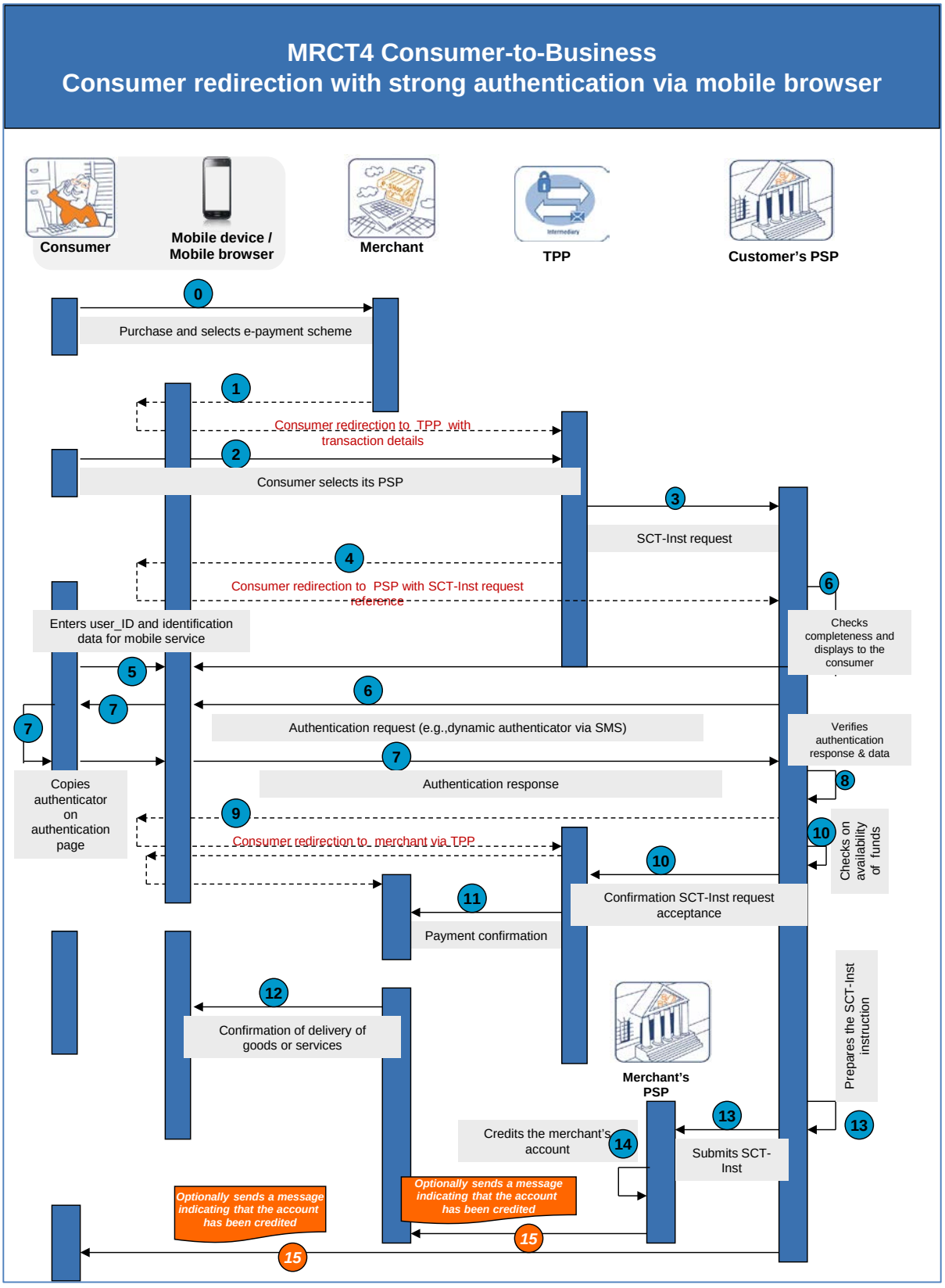

Figure 15: MRCT 4 - Consumer-to-Business – Mobile Remote SCT-Inst - Consumer redirection with strong authentication via mobile browser

MRCT 4 - Consumer-to-Business - Mobile Remote SCT-Inst- Consumer redirection with strong authentication via mobile browser	
Category	Consumer-to-Business (B2C)
Communication type:	Remote
Payment instrument	SEPA Instant Credit Transfer
Payment initiation by	Payer
Prerequisites	• The establishment of an Instant SEPA Credit Transfer scheme • The establishment of the TPP service
Payment authorisation mode by consumer	Determined by the payer's PSP in accordance with the remote urgent SCT scheme
Customer benefits	• Convenience, mobility, speed • Cheque and cash displacement • The beneficiary has immediate payment
Challenges	• The set up and operation of the SCT-Inst scheme • The set up and operation of the TPP service

Table 24: MRCT 4 - Consumer-to-Business – Mobile Remote SCT-Inst – Consumer redirection with strong authentication via mobile browser

6.4 Ecosystem

6.4.1 Introduction

As mentioned before, this white paper focuses on ecosystems that are based on SEPA[26] payment instruments. This covers both four and three corner models (see section 5.5.2) provided they use SEPA compliant formats. This also means that MRPs typically involve payment accounts.

In this context it is assumed that the infrastructure and business processes of the current SEPA instruments are likely to be used. This means that the focus will be on how to use the mobile device 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.

MRPs introduce a new ecosystem involving new participants in the chain. Even if many of the stakeholders involved in the MRP transaction do not differ from those involved in a “classic” card or SCT payment, MPPs need to rely on a series of technical infrastructure elements that are unique to the mobile environment for the management of the MRP service life cycle processes.

6.4.2 Stakeholders

- The payer is a natural person who makes the mobile payment; he/she owns a SEPA payment account or a SEPA compliant card, a mobile phone and would need to have 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;

[26] Note that the use cases and service models introduced in this white paper may also be applied to non SEPA areas.

- The beneficiary owns a SEPA payment account and, where relevant, a SEPA compliant card. In case the beneficiary is a merchant, the beneficiary is the acceptor for payment of the goods or services purchased by the consumer. In case the beneficiary is a private customer / small business, there may be situations where it is very convenient 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;
- The MNO or other providers are 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, the MRP issuer is the PSP responsible for provisioning the application to the payer. The application is located in a secure environment, typically in an SE. In that case, the SE Issuer is a new stakeholder. This is the MNO in case of a UICC, the mobile equipment manufacturer or a third party in case of an embedded SE, the MRP issuer or a third party in case of a secure micro SD card (see section 4 in [5]). In any case, the MRP issuer may optionally use a so-called Trusted Service Manager (TSM) for the lifecycle management of its application.
- 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). The MRP issuers, TSMs and SE issuers collaborate to perform the provisioning and management of the MRP application(s). Several TSMs may co-exist offering mutually-competing services.
- The Mobile Wallet Issuer is a service provider that issues mobile wallet functionalities to the customer (consumer or merchant).
- An optional Third Party Payment Service Provider (TPP) such as a Payment Initiation Service Provider (PISP) which may facilitate the remote payment transaction (see [21]).
- An optional Trusted Third Party (TTP) that operates a common infrastructure[27] that could facilitate increased convenience and/or trust for the parties involved;

Other relevant new stakeholders include for example:

- SE manufacturers in case an SE is involved;
- Application developers (MRP application, AAUI, mobile wallet …);
- Mobile equipment manufacturers;
- Organisations performing infrastructure certification (e.g., MRP applications, etc.).

6.4.3 Service models

6.4.3.1 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.

[27] See section 5.5 Layer 2 for more information about common infrastructure

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 5.2.4). Although this TTP does not affect the underlying SEPA Card payment transactions, it might impact the service model.

The C2C mobile remote SCT payments introduced in section 5.3.1 do not modify in any way the underlying SCT payment transactions; hence the existing service model remains valid.

The use-case introduced in section 5.3.2 do not modify in any way the SCT payment transactions but the service model might be impacted by the introduction of a new stakeholder operating the common infrastructure.

The use-cases introduced in section 5.3.3 and 5.3.4 both require an instant SCT payment to cater for the immediacy while the latter use case also involves a new stakeholder which will impact the service model.

6.4.3.2 Provisioning and Management

Depending on the particular MRP, the payment data stored on the mobile device may range from pure payment credentials or tokens 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.

6.5 High level architecture

6.5.1 Introduction

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

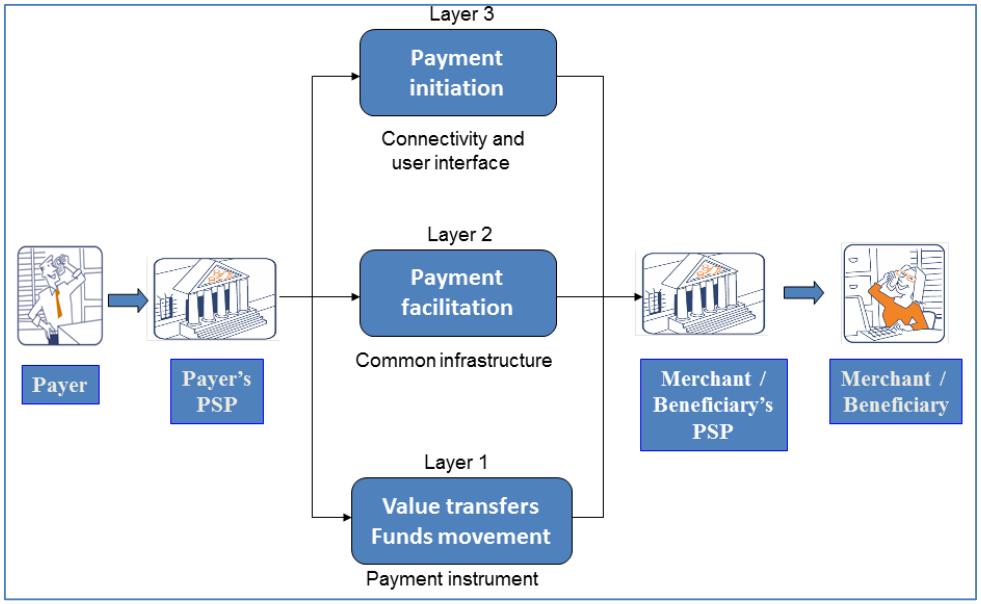

Figure 16: High level architecture for Mobile Remote Payments

In the figure above three layers may be distinguished:

- Layer 1: Payment instrument for value transfers and funds movement

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

- 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 to each other; they may rely on some form of linkage (through a shared common infrastructure operated by a TTP) between mobile identifiers and payment instruments belonging to the transacting parties.

- Layer 3: 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 whereby different approaches already exist in the market today, some of which involve a PISP.

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.

6.5.2 Layer 1 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.

6.5.2.1 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 sections 5.2 and 5.3, such as the identification of the beneficiary (which is known to the PSP), the confirmation of payment and the immediacy aspect.

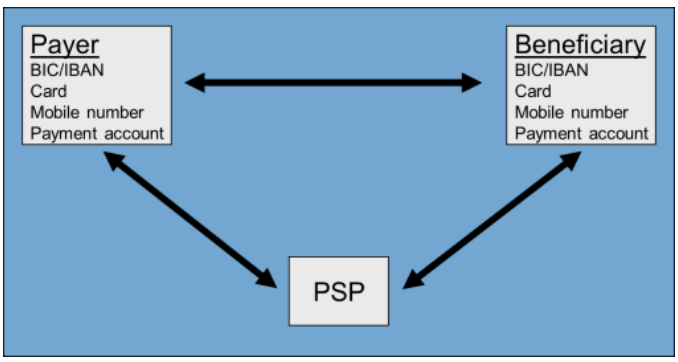

Figure 17: The 3-corner model

6.5.2.2 The 4-corner model under a payment scheme

In this model, the payer and the beneficiary hold their payment accounts with different PSPs. But the assumption is made that both PSPs operate under one and the same payment scheme (card scheme or any other payment scheme). This model might simplify again some aspects described in the use-cases provided in sections 5.2 and 5.3, such as the identification of the beneficiary through the alias, the confirmation of payment and the immediacy aspect.

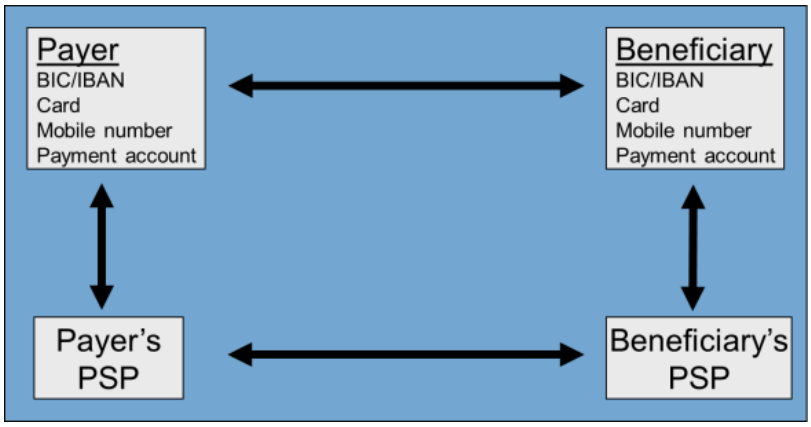

Figure 18: The 4-corner model under a single payment scheme

6.5.2.3 The 4-corner model involving different payment schemes

In this model, the payer and the beneficiary hold their payment accounts with different PSPs and both PSPs operate under different payment schemes. Clearly both schemes would need to adhere to a certain interoperability structure (implying that a business and technical agreement between the different payment schemes is in place). This is the most general model that may exist.

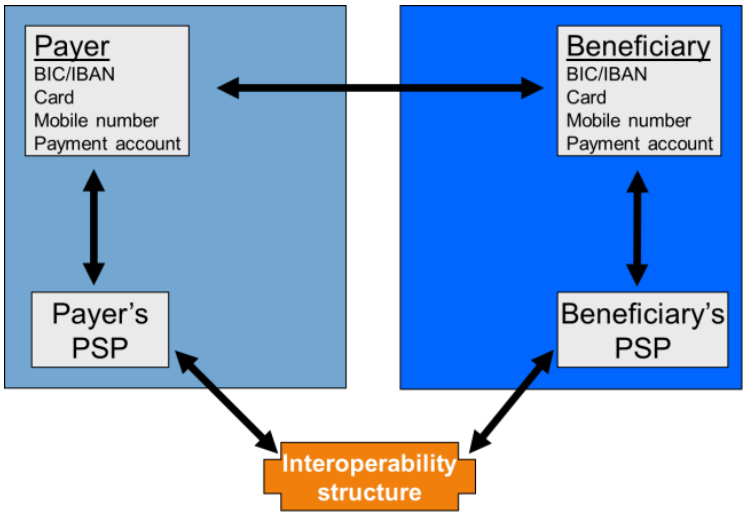

Figure 19: The 4-corner model involving different payment schemes

6.5.3 Layer 2 revisited

6.5.3.1 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 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 that may 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 payment before the shipment of the purchased goods or execution of services.

6.5.3.2 Direct interoperability model

The direct interoperability model is dependent on the payers/beneficiaries ability to forward all relevant payment information (IBAN, name, address, etc.) to their 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.

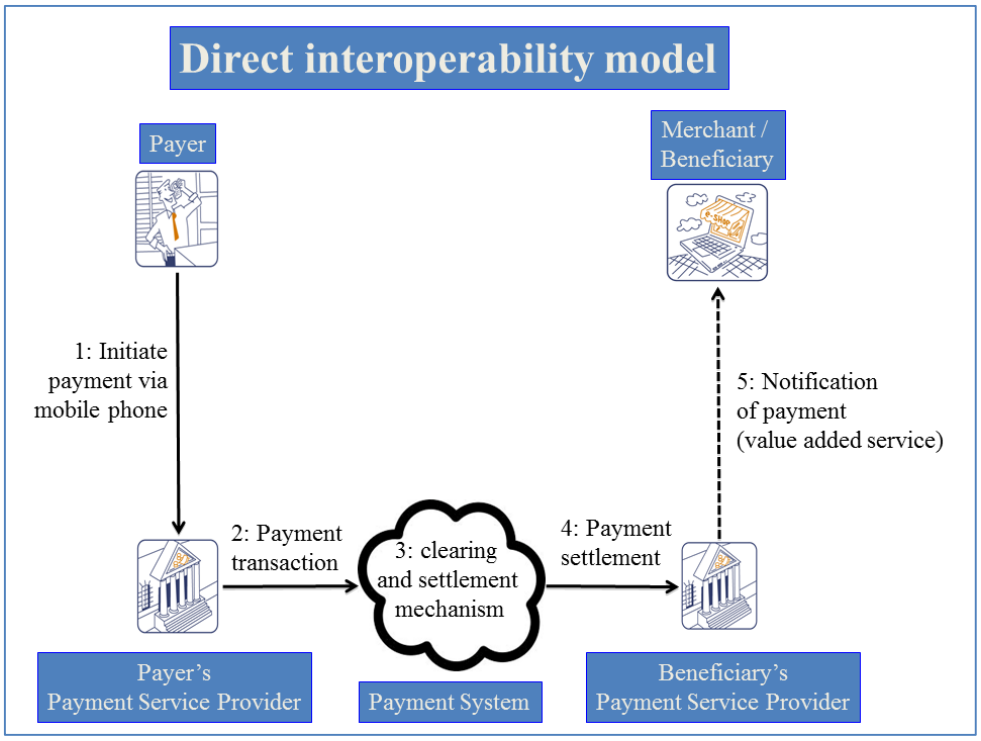

Figure 20: Direct interoperability model

The advantage of the direct interoperability model is the low implementation and operational cost as all transactions are directly routed into existing channels while the major disadvantage is the lack of convenience for the consumers[28].

There is room for supplementing the service model with value added services, e.g., notification services.

6.5.3.3 Interoperability model based on a centralised common infrastructure

In this model, interoperability is achieved by the usage of a centralised common infrastructure[29], typically operated by a TTP, which may have many shapes and purposes (see also section 7.3.1), and which could even be implemented in a distributed way[30]. 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.

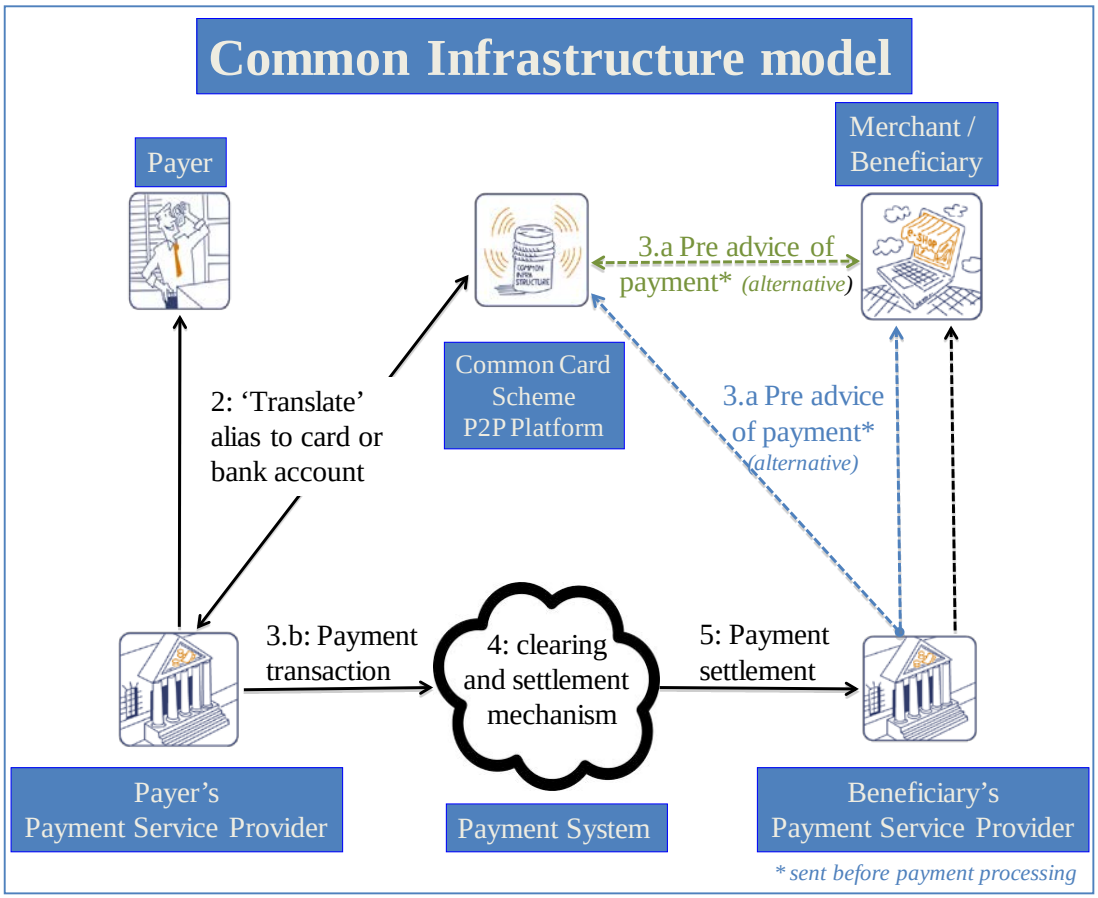

Figure 21: Centralised common infrastructure model

[28] Note that more complex scenarios may exist involving externalisation of "payment messaging".

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

[30] Note that more complex scenarios may exist involving externalisation of "payment messaging".

The advantages of the interoperability model based on a centralised common infrastructure are the following:

- The privacy, avoiding the two parties to disclose payment details to each other;
- The high convenience for the consumers to initiate the payment using an alias;
- The easy retrieval of the beneficiary's details;

while the major challenges are:

- The set-up of the infrastructure which needs to offer access control, confidentiality, integrity and availability;
- The maintenance to guarantee the accuracy and freshness of the information;
- The implementation cost.

7 Secure consumer subscription to mobile payment services

The use-cases specified through this section are introduced to demonstrate how secure consumer subscriptions to mobile payment services can be easily and conveniently achieved and should therefore be considered as 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 could 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.

7.1 Remote subscription

In this scenario, illustrated in Figure 22, a PSP's customer (the consumer) subscribes to mobile payment services via an existing payment service using the internet[31]. 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, containing a confirmation code such as a one-time password that is sent back for validation, 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 with the one-time password received in step 4, 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).

[31] Subscription through the mobile banking channel can be made in a similar approach.

SMS push is one option to install the application; alternatively the consumer can download the application from an application store. The process itself might be more complex and depends on the Secure Element chosen, i.e. the SE issuer.

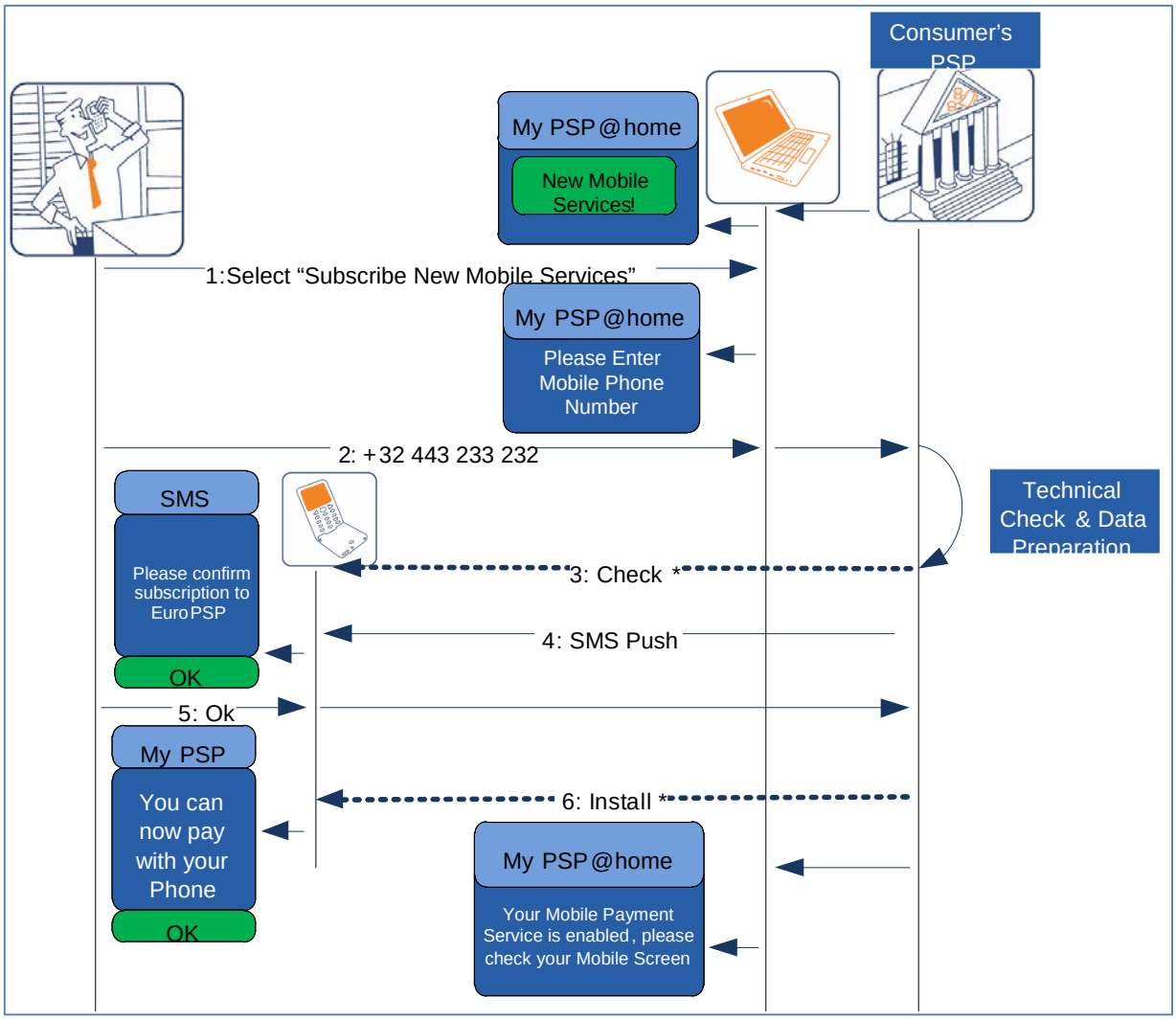

Figure 22: Example of remote subscription to mobile payment services

Note: Transactions marked with an asterisk may require further consumer interaction.

7.2 Subscription with self-service device

In this scenario, illustrated in Figure 23, 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, containing a confirmation code such as a one-time password that is sent back for validation, 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 with the one-time password received in step 4, 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).

SMS push is one option to install the application; alternatively the consumer can download the application from an application store. The process itself might be more complex and depends on the Secure Element chosen, i.e. the SE issuer.

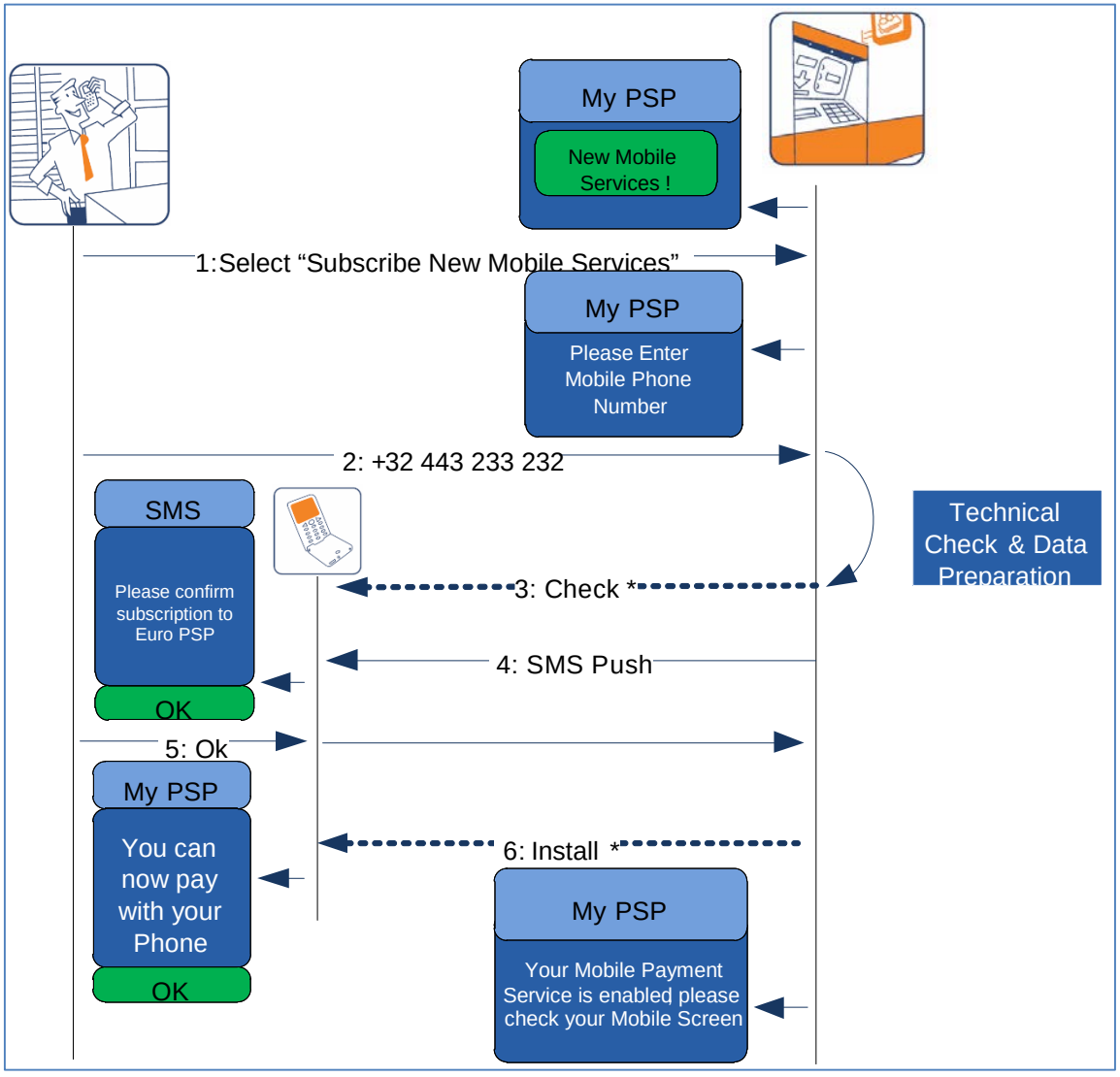

Figure 23: Example of ATM subscription to mobile payment services scenario

Note: Transactions marked with an asterisk may require further consumer interaction.

7.3 Subscription at the PSP's branch

In this scenario, illustrated in Figure 24, the subscription to mobile payment services is performed when the consumer visits their 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).

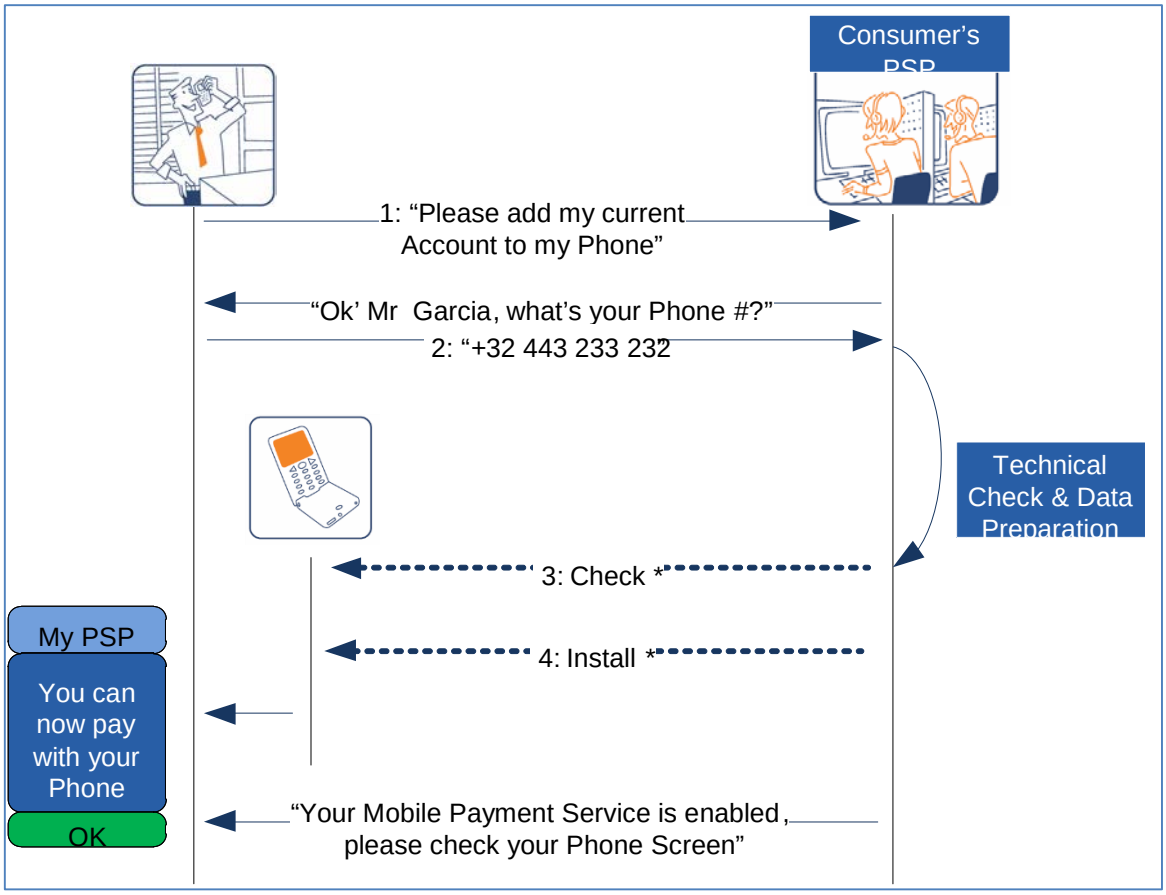

Figure 24: Example of in-person mobile payment service subscription use-case

Note: Transactions marked with an asterisk may require further consumer interaction.

8 Infrastructure

In this section the different infrastructure components are considered which are used for mobile payments.

8.1 Mobile devices

8.1.1 General

Within the SEPA region, most of the deployed general-purpose mobile phones are UMTS-based (also known as 4 and 5G) and therefore include the appropriate communication capabilities such as fast and reliable internet access to support mobile financial services. They use a so-called “UICC” (Universal Integrated Circuit Card), 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 mobile payment applications under the control of the PSPs.

A mobile phone may be used both for mobile proximity and mobile remote payments 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. For an MCP the requirements on mobile phones are more complex: the NFC controller, an SE or HCE and appropriate 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[32].

Mobile devices are constantly being enhanced and feature an ever-increasing number of capabilities. “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 [13].

NFC, used for mobile contactless payments, is compatible with contactless card protocols[33]. NFC-enabled phones can interact with standard NFC readers (e.g., POI) and with other NFC-enabled devices. Accordingly, they have the potential to re-use 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.

8.1.2 End-user interface

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 9) provide such an interface

[32] 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.

[33] 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.

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.

8.1.3 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 re-used for the SEs.

A number of alternatives exist for the deployment of SEs in the mobile device to support mobile payments. The main factors driving the choice of SE in this context could be:

- 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 until now 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 in [5]).

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

Most MCP implementations today make usage of an SE, although HCE-based solutions (see 7.1.4) are gaining momentum. For MRP, the payer directly authenticates to a payment server according to their 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.

More recently, also solutions based on a so-called SE in the cloud accessed via the mobile device have been introduced, for mobile payments. For MCPs they often come in combination with HCE-based solutions (see section 8.1.4) but also remote mobile payments based on a “SE in the cloud” gain momentum.

8.1.4 Host Card Emulation

Host Card Emulation (HCE) refers to an on-device technology that permits an NFC-enabled mobile device to perform card emulation without relying on access to an SE for

the storage of sensitive data such as credentials, cryptographic keys, etc. It is an architecture that provides exact virtual representation of a card using only software. HCE enables mobile applications running on supported operating systems with the ability to offer card solutions independently of third parties while leveraging cryptographic processes traditionally used by hardware-based SEs without the need for a physical SE. This technology enables the MCP issuers to offer mobile contactless payment solutions more easily.

To enhance the security, HCE-based solutions may be offered in combination with Tokenisation, see 8.2.6.

For further information on HCE the reader is referred to [12] and [17].

8.1.5 Trusted Execution Environment

In a mobile device, applications typically are executed in an environment provided and managed by a Rich OS, the so-called REE (Rich Execution Environment) This environment and applications running on it are considered un-trusted.

A Trusted Execution Environment (TEE) can be defined as a dedicated execution environment providing security features such as isolated execution, integrity of applications along with confidentiality of their assets for the deployment of sensitive services. The TEE runs alongside the Rich OS and provides security services to that rich environment and to the applications running inside this environment. It maybe be used for handling sensitive assets, it brings security to the interaction with the cardholder (e.g., the mobile code entry) and has the potential to control data flows in the consumer device. It is complimentary to the SE. For further information on TEE, the reader is referred to [11].

8.1.6 Trusted Platform Module

A Trusted Platform Module (TPM) is a computer chip (microcontroller) that can securely store features used to authenticate the platform. These features can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measures that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.

Trusted modules can be used in computing devices other than PCs, such as mobile phones or network equipment.

8.2 Infrastructure for mobile payment transactions

This section describes the different aspects of the infrastructure to support of mobile payment. As an illustration, Annex III provides a mapping of the use-cases described in sections 5.2 and 5.3 on the three layer architecture introduced in section 5.5.

8.2.1 Transaction infrastructure

The infrastructure needed during the payment transaction for mobile payments may fully re-use the infrastructure already deployed for the underlying payment instruments such as SEPA cards and SCTs. Moreover, the investments to be made for acceptance of contactless SEPA cards can also be used for mobile contactless SEPA card payments.

However, as identified in sections 5.2 and 5.3, 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 account 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 details (e.g. name and IBAN) of the beneficiary. 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 5.5.3 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 payment before the shipment of the purchased goods or execution of services. For both models, the MRP issuers have the responsibility to enrol consumers to the various MRP payment services. After subscription to the service ordered by the beneficiary to their PSP, the enrolment can be done either by the beneficiary's PSP or directly by the beneficiary him/herself. In any case, this might require a dedicated registration action by the beneficiary.

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 / payment account. In this way the payer's PSP is able to send the payment transaction to the beneficiary's PSP / payment 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/payment account and will then route the payment transaction to the beneficiary's PSP/payment 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 requirements related to e.g., privacy. Moreover, the common infrastructure needs to be reliably maintained in order to guarantee the accuracy and freshness of the information.

8.2.2 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 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.

8.2.3 Storage of mobile payment data and applications in the mobile device

In the following section, a distinction will be made between the storage of mobile payment related data/credentials, typically used in the context of remote mobile payments and the hosting of a mobile payment application on the mobile device. The storage of mobile payment related data is referring to the storage of data on the mobile device as a convenience to the consumer instead of entering it by hand at the transaction time. A mobile payment application is a dedicated software package residing on the mobile device (e.g. on a SE or HCE) that dynamically generates transaction data. In case of an MCP applications it has direct access to the NFC interface and therefore it communicates directly with the POI. Mobile payment applications are personalised and managed remotely by their issuer or a TSM on its behalf (see sections 5 and 6 in [5]). The issuers can compete in their service offerings by customising the mobile payment application, user-oriented configuration functions and the (remote) management operations.

8.2.3.1 Storage of mobile payment related data/credentials

The mobile phone can be used to store static data/credentials both for mobile payments. If there are security requirements for these data (integrity and/or confidentiality), the data needs to be stored in a trusted environment. These data may be stored by the payer or their 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.

8.2.3.2 Hosting of a mobile payment application

For mobile proximity payments and for some implementations of mobile remote payments, the hosting of a dedicated mobile payment application in the mobile device may be required. If this application has active security features, (e.g., cryptographic functions) the hosting shall be done in a secure environment such as an SE. A mobile payment application requires full life cycle management by the payer's PSP, including provisioning, activation, personalisation, etc. (see [5]).

The payer's PSP might delegate some of these functions to a TSM. Different requirements for the roles fulfilling the functions of mobile application life cycle management will apply (see [5] and [6]).

8.2.4 Provisioning & management

The mobile payment application is to be installed on the mobile device. 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 implementation chosen (e.g. SE- or HCE-based) chosen. It is expected that existing personalisation systems such as those employed for cards can be re-used for the personalisation of the payment application. In order to achieve this, TSMs might be involved. For further information on this topic the reader is referred to [5] and [6].

8.2.5 Mobile payment application user interface

A mobile payment application may be supported by complementary applications residing on the mobile device's "main memory", which are known as the mobile payment application user interface and which are dedicated to interact with the consumer (see for instance section 7.3 in [5] for further considerations on this subject).

The mobile payment application issuer is responsible for this application, its security characteristics and the secure communication with the mobile payment application.

8.2.6 Tokenisation

In order to enhance the security of mobile payment transactions, more in particular for HCE-based solutions, so-called payment tokens may be used. They generally refer to a surrogate value for consumer (payer) account related data (e.g., the PAN for card payments, the IBAN for SCTs) which is used for payment transactions. Payment Tokens must not have the same value as or conflict with the real payment account related data. Payment Tokens can take on a variety of formats across the payments industry. They are issued by Token Service Providers, typically in the context of mobile payments, on the request of the mobile payment service issuer or a TPP. Further information on the usage of tokenisation in the context of mobile contactless card payments may be found in [1].

8.2.7 Merchant interface

Since the merchant interface differs between mobile proximity and mobile remote payments, the topic is handled in separate sections below.

8.2.7.1 Mobile proximity payments

A Point of Interaction (POI) is a hardware and/or software component in merchant's point of sale equipment that enables a consumer to use a card to make a purchase at a merchant. The POI might be attended or unattended. POI systems have been further developed to allow other devices (e.g. mobile devices) and technologies (e.g. NFC, QR codes, etc..) to be used.

Today, in some SEPA countries a large part of the POI infrastructure is already NFC enabled (see [10] for more details) while in most others migration plans are put in place. This upgrade should include the potential requirements beyond those already defined for contactless SEPA card payments to maximise 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 MCPs.

Concerning other proximity technologies such as 2D barcodes, BLE, etc., it is to be noted that many different solutions exist which operate as "closed systems" and mostly do not offer cross-border interoperability. This leads to a very fragmented market throughout Europe, whereby there is a clear need for standardisation in the usage of the various proximity technologies for mobile payments.

8.2.7.2 Mobile remote payments

Generally, merchants have different ways for customers to make purchases which are referred to as "purchase contexts". For example, the merchant may offer the use of SMS, provide a mobile website, have a dedicated mobile remote application or accept a preregistered alias (e.g., a mobile phone number).

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 a mobile payment instrument and the mobile device are suitable for the particular purchase context.

A PSP will specify certain requirements on the consumer's mobile phone, based on the mobile financial service 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 (payment) application e.g., for payment instrument selection, authentication and other possible features.

9 Mobile wallets

9.1 Definition

Similar to the physical world, a "digital" wallet is basically holding identification information on the wallet holder, on payment 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 descriptions may be derived.

> *"A digital wallet is a service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services / applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc)[34]. 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 (or a combination thereof) but is anyway under the control of the holder. A digital wallet is sometimes referred to as an e-wallet."*
>
> *"A mobile wallet is a digital wallet which is accessed through a mobile device (e.g., phone, tablet,...)."*

A further vision and general reflection on mobile wallets may be found in [16].

9.2 Usage of mobile wallets for mobile payments

From a consumer perspective the mobile wallet is basically an application (or part of it) that allows them 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 EPC developed a dedicated White Paper on Mobile Wallet Payments to provide further guidance (see [7]).

---

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

10 Standardisation and industry bodies

Mobile SEPA payments require consistency in specifications and guidelines defined within several disciplines and issued by a heterogeneous group of standardisation and industry bodies.

The most relevant bodies in this area are:

- **ISO**

The International Organization for Standards (ISO) is a 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. Moreover, ETSI is currently investigating the set-up of a new standardisation activity with appropriate stakeholders for a “Smart Secure Platform”[35] . (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 has also published document sets on contactless payments, including mobile, and a framework for payment tokenisation. EMVCo also establishes and administers testing and approval processes to evaluate compliance with their specifications.(http://www.emvco.com/)

- **IETF**

The Internet Engineering Task Force (IETF) is an 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 an 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

[35] Enabling the provision of value-added services relying on authentication of the user, regardless of the mobile device, communication channel and underlying technology - taking into account the requirements for mobile payments.

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.gsma.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. It has established a Web Payments Interest Group whose aim is to develop a Web payment API for merchants. (www.w3.org)

11 Conclusions

Purpose of the EPC

The purpose of the EPC is to support and promote European payments integration and development, notably SEPA. 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 new edition of the white paper provides a high-level overview of mobile payments specifically dealing with:

- Mobile proximity payments
- Mobile remote payments.

The mobile phone is primarily used for the payment initiation while the EPC is promoting the usage of SEPA instruments for the underlying payments themselves.

Analysis and Focus

Having analysed many payment categories for both “proximity” and “remote” mobile payments, the following are viewed as EPC's focus areas for mobile payments:

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

Mobile Proximity Payments

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

For other mobile proximity payments, the lack of standardisation in the usage of the various proximity technologies is resulting in a very fragmented approach throughout Europe.

A comprehensive and more detailed analysis of the challenges for mobile proximity payments may be found in the ERPB report [10]. The EPC has been significantly involved in this ERPB work.

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 or the merchant;
- Immediate (or very fast) payments.

While many of these identified challenges are not specific to the mobile channel, an early resolution is key if remote SEPA payment instruments are to become successful in this environment. With the specification of a SEPA Instant Credit Transfer Scheme, the EPC is delivering a major contribution to address some of these challenges (see [8]).

Next Steps

Next to working with relevant stakeholders involved in the mobile ecosystem, the EPC further plans to engage with relevant industry bodies to contribute to the development

of open specifications for interoperability of mobile payments, which can be used by the payment industry and all interested parties.

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 PSPs executing the credit transfer would have to be scheme participants; i.e. both would have to formally adhere to the SCT Scheme. There is no limit on the amount of a payment carried out under the scheme.

The SCT Scheme Rulebook 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 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 and Business to Business (B2B) SDD Schemes apply to transactions in euro. The debtor and creditor each would need to hold an account with a PSP located within SEPA. The PSPs executing the direct debit transaction would have to be scheme participants; that is, both would have to formally adhere to the SDD Scheme. The scheme may be used for single (one-off) or recurrent direct debit collections; the amounts are not limited. The SDD B2B Scheme is available only to businesses.

SEPA Cards Standardisation Volume

The EPC together with the Cards Stakeholders Group (CSG) created the SEPA Cards Standardisation (SCS) Volume. This document defines a standard set of requirements to enable an interoperable and scalable card and terminal infrastructure across SEPA, based on open international card standards. The CSG is a multi-stakeholder body representing retailers, vendors, processors, card schemes and the EPC. Created in 2009, the CSG develops and maintains the SCS Volume, and focuses on a cards standardisation programme that will create a better, safer, more cost efficient and functionally richer card services environment, whatever the card product or scheme may be. The last version of the Volume (version 7.5) was published in May 2016 for public consultation.

Further information on the SEPA payment instruments may be obtained from the EPC website (www.epc-cep.eu).

Annex II – Secure Elements in the mobile device

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 with 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 or any other application provider 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 should ideally provide the platform for sharing resources between several application providers.

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 [15]. 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.

Annex III – Mapping the MRP use-cases on the infrastructure

In this annex, a mapping will be provided of the use-cases described in sections 6.2 and 6.3 on the three layer architecture introduced in section 6.5. Depending on the use-cases, the payment might be initiated in layer 3 through different ways (see section 6.5.1), such as via a browser or using a dedicated MRP application.

For each use-case, the following table lists the components to be added in layer 2 (e.g., common infrastructure) and the service in layer 1.

Three layers / Use Cases	Layer 3 payment initiation connectivity and user interface	Layer 2 payment facilitation common infrastructure	Layer 1 value transfers and funds movement payment instrument
MRCP 1	mobile browser	no	existing SCP
MRCP 2	mobile wallet	no	existing SCP
MRCP 3	dedicated MRCP application in a mobile wallet	no	existing SCP
MRCP 4	dedicated MRCP application, optional usage of mobile wallet	common infrastructure	existing SCP
MRCT 1	mobile browser	common infrastructure	existing SCT
MRCT 2	dedicated MRCT application	common infrastructure	existing SCT
MRCT 3	dedicated MRCT application		SCT-Inst
MRCT 4	mobile browser	TPP infrastructure	SCT-Inst

Table 25: Mapping of uses cases onto three layers MRP architecture

End of Document