Document EPC163-13
Version 2.0
Date: 21 January 2014

WHITE PAPER
MOBILE WALLET PAYMENTS

Abstract	This document describes the concept of a mobile wallet which provides an intuitive interface to the user of a mobile device to manage his/her portfolio of mobile payments next to other mobile services.
Document Reference	EPC 163-13
Issue	Version 2.0
Date of Issue	21 January 2014
Reason for Issue	Updated version based on comments received through public review
Produced by	EPC Secretariat

European Payments Council

Table of Contents

List of tables

List of figures

Executive Summary

The overall role of the EPC is to contribute to the promotion of the Single Euro Payments Area (SEPA) and to the evolution of an integrated market for payments in Europe, through helping in or facilitating the development and promotion of standards, best practices and schemes (see http://www.europeanpaymentscouncil.eu).

Since mobile devices have achieved full market penetration and rich service levels they are an ideal channel for SEPA payment instruments. The usage of the mobile device is hereby primarily considered for the payment initiation whereas the underlying payments are based on existing SEPA instruments as described in the white paper on mobile payments published by the EPC (see [1]).

Creating ease, convenience and trust for end-customers (payers/consumers and beneficiaries/merchants) is regarded as critical for the further development of mobile payments. Since a mobile wallet may be regarded as a key tool to address these challenges, the EPC has decided to devote a white paper to this concept.

This white paper primarily focuses on mobile wallets as an enabler for mobile payments. The document first describes a number of use cases of mobile wallets for financial services as an introduction to the subject. Next it explains how mobile wallets may be regarded as a facilitator for mobile payments while the mobile wallet ecosystem is analysed. This white paper further describes various mobile wallet models enabling mobile payments which may be identified in the market today. It contains also a high level overview of some technical and life cycle management aspects and provides a list of the main industry and standardisation bodies involved.

This white paper endeavours to:

- 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[1];
- Inform on the new convenient, homogenous and seamless service access and new business opportunities enabled by the usage of a mobile wallet to perform mobile payment transactions;
- Provide examples of the usage of a mobile wallet for mobile payments;
- Outline the mobile wallet ecosystem and the different existing models for mobile wallets.

Today, mobile wallets are in their early stages of development. No one in the payment ecosystem knows exactly how the mobile wallet marketplace will evolve in the coming years. But the offering of additional mobile services (such as ticketing, loyalty, couponing, etc...) next to financial services appears to be important drivers for the value proposition.

In addition, to enable a cost-effective approach for all stakeholders involved in the mobile wallet payments ecosystem, a number of key challenges remain to be addressed in the future regarding this topic:

- Harmonisation of user interfaces to enable a consistent user experience (easy to use, intuitive, etc...);
- Co-existence of payment with other mobile services in a mobile wallet;
- Co-existence of multiple mobile wallets on or accessed through a single mobile device;
- Linkage of mobile wallets in the payer's space with merchant wallets;

[1] Note that the concepts described in this white paper may also be applied outside SEPA.

- Interoperability of mobile wallet interfaces;
- Execution of proximity payments with remote mobile wallets;
- Alignment of mobile wallet security aspects (including authentication) with existing and forthcoming requirements for mobile payments[2] related to mobile wallet interfaces and infrastructure;
- Coordination amongst various industry initiatives on mobile wallets.

This white paper has been written in a non-technical style to inform PSPs, their customers and all stakeholders involved in the payments value chain about the EPC's views on the usage of mobile wallets as an enabler for mobile payments in SEPA[3]. The EPC encourages an open dialogue and a collaboration of all relevant stakeholders to combine future efforts so that these issues are adequately addressed while contributing to the success of mobile (payment) services through mobile wallets.

[2] See for example the SecuRe Pay *"Recommendation for the security of internet payments" and the draft* SecuRe Pay *"Recommendation for the security of mobile payments"* published by the European Central Bank.

[3] Note that the concepts described in this white paper may also be applied for payments outside SEPA.

0 Document information

0.1 Structure of the document

This section describes the structure of this white paper. Section 0 provides the references, definitions, and abbreviations used in this document. General information about the European Payments Council (EPC) and its vision may be found in section 1. Section 2 contains an introduction to mobile wallets and the services they could support. Section 3 portrays a number of scenarios whereby a mobile wallet is used for financial services which are introduced via the description of the daily life of a consumer. In section 4, a high level overview is provided of the mobile wallet ecosystem and the stakeholders involved. Section 5 is devoted to an overview of the mobile wallet components and the most relevant models that appear in the market today to support mobile payments. Section 6 introduces the (technical) interfaces of mobile wallets. Different aspects of the life cycle management of mobile wallets are highlighted in section 7. Section 8 lists the most relevant standards and industry bodies involved with mobile wallets. General conclusions may be found in the final section 9. Annex 1 describes the SEPA payment instruments. A few illustrations through detailed descriptions of mobile wallet use cases for contactless and remote payments may be found in Annex 2. Annex 3 provides some examples of combinations of mobile wallet components.

0.2 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.

Ref.	Title
[1]	European Payments Council EPC492-09 White Paper Mobile Payments http://www.europeanpaymentscouncil.eu
[2]	European Payments Council EPC 178-10 Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines http://www.europeanpaymentscouncil.eu
[3]	European Payments Council EPC020-08 SEPA Cards Standardisation "Volume" Book of Requirements http://www.europeanpaymentscouncil.eu
[4]	Global Platform TEE System Architecture http://www.globalplatform.org/
[5]	GSMA White Paper: The Mobile Wallet http://www.gsm.org
[6]	GSMA NFC Core Wallet Requirements http://www.gsm.org
[7]	ISO/IEC 18092: Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1) http://www.iso.org

[8]	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 http://www.mobeyforum.org
[9]	Payment Services Directive Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

Table 1: References

0.3 Definitions

The following terminology is applied in this document. The abbreviations used may be found in section 0.4.

Term	Definition
Alias	For remote payments, an alias is basically a pseudonym (e.g., mobile phone number) for the beneficiary that can be uniquely linked to the beneficiary's payment account (e.g., IBAN or payment card number).
Authentication	The provision of assurance of the claimed identity of an entity or of data origin.
Authentication application	A dedicated application residing in a secure environment to support the authentication process in a payment transaction.
Authentication method	The method used for the authentication of an entity or data origin.
Authenticator	A security factor used in an authentication method. Typical examples are tokens, mobile codes/passcodes, etc.
Beneficiary	A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction. [9]
Cardholder verification	Function used to evaluate whether the person "presenting" the card is the legitimate cardholder.
Consumer	A natural person who, in payment service contracts covered by the [9], is acting for purposes other than his trade, business or profession (as defined in [9]).
Customer	A payer or a beneficiary which may be either a consumer or a business.
Credential(s)	Payment/banking account related data that may include a passcode (mobile code, on-line passcode, etc.), provided by the PSP (issuer) to its customer, which is provided via his/her mobile device for identification/authentication purposes in the context of the document.
Credentials manager UI	A dedicated user interface that enables the consumer/payer to manage a set of credentials for mobile payment service(s).
Digital wallet	A service accessed through a device (e.g., a PC) which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications. A digital wallet is sometimes also referred to as an e-wallet.
Dynamic authentication	Authentication method that uses cryptography or other techniques to create a one-per-transaction random authenticator (a so-called dynamic authenticator).
Financial services	Any service of banking, credit, insurance, personal pension, investment or payment nature (see ec.europa.eu/internal_market/financial-markets).
Hardware Security Module (HSM)	Specialised hardware device designed to protect cryptographic keys and the use of those keys in executing cryptographic functions. An HSM provides security services in support of payments.
Merchant	The beneficiary within a mobile payment scheme for payment of goods or services purchased by the consumer/payer. The merchant is a customer of its PSP.
Merchant wallet	A type of wallet where the payment gateway and the mobile wallet gateway are integrated services at the merchant's website.
Mobile code	A user verification method used for mobile card payments. It is a code entered via the keyboard of the mobile device to verify the cardholder's identity as a cardholder verification method.
Mobile Contactless Payment (MCP)	A mobile device initiated payment where the cardholder and the merchant (and/or his/her equipment) are in the same location and communicate directly with each other using contactless radio technologies, such as NFC, for data transfer (also known as contactless payments).

MCP application	An application residing in a secure environment performing the payment functions related to a Mobile Contactless Payment, as specified by the Mobile Contactless Payment application issuer in accordance with the payment scheme.
Mobile device	Personal device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth … 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 its PSP using its own or leased network (the latter are sometimes referenced as MVNOs - Mobile Virtual Network Operators).
Mobile payment service	Payment service made available by software/hardware through a mobile device.
Mobile payment service issuer	A PSP providing the mobile payment application (Mobile Contactless Payment or Mobile Remote Payment), authentication application and/or credentials to the consumer/payer.
Mobile proximity payment	A mobile payment where the communication between the mobile device and the Point of Interaction device takes place through a proximity technology (e.g., NFC, QR code, 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, etc.) and which can be made independently from the payer's location (and/or his/her equipment).
Mobile Remote Payment (MRP) application	An application residing in a secure environment performing the payment functions related to a Mobile Remote Payment, as specified by the Mobile Remote Payment application issuer in accordance with the payment scheme.
Mobile service	Service such as identification, payment, ticketing, loyalty, etc., made available through a mobile device.
Mobile service issuer	The provider of a mobile service.
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.
Mobile wallet gateway	A service operated by the mobile wallet issuer or a trusted third party acting on its behalf, which establishes for mobile transactions a link between the consumer/payer and its mobile wallet and between the mobile wallet and the payment gateways. During the payment transaction, it allows the payment gateway to receive authentication data directly from the mobile wallet. For life cycle management, it establishes a link between the mobile wallet and the mobile wallet issuer to download credentials, payment and/or authentication applications from the PSP.
Mobile wallet issuer	The service provider that issues mobile wallet functionalities to the customer (consumer or merchant).

Mobile wallet passcode	A code entered by the consumer/payer[4] via his/her mobile device that may be required to activate a mobile wallet. It is sometimes referred to as "mobile wallet credentials".
Network operator	The provider of data connectivity to the consumer and potentially other services. MNOs and ISPs are examples of network operators.
NFC (Near Field Communication)	A contactless protocol specified by ISO/IEC 18092 [7].
On-line passcode	Secret data known by the consumer/payer and used for remote financial services, such as on-line banking, SCT payments, etc., to verify its identity.
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. [9].
Payment account	Means an account held in the name of one or more payment service users which is used for the execution of payment transactions. [9].
Payment component	Either a dedicated mobile payment/authentication application and/or a set of credentials.
Payment component User Interface (UI)	Enables the consumer/payer to manage a specific mobile payment service through a dedicated user interface. Depending on the payment component type, it may be a mobile payment/authentication application UI (provided by the PSP) or a credentials manager UI.
Payment gateway	A service operated by a beneficiary's PSP or a trusted third party that manages the authorisation of payments for merchants. It facilitates the transfer of information between the payment portal (such as a website or mobile device) and the beneficiary's PSP.
Payment scheme	A single set of rules, practices, standards and/or implementation guidelines agreed between PSPs for the execution of payment transactions and which is separated from any infrastructure or payment system that supports its operation
Payment Service Provider	The bodies referred to in Article 1 of the [9] and legal and natural persons benefiting from the waiver under Article 26 of the [9].
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 [9]).
Payment transaction	An act, initiated by the payer or by the beneficiary, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the beneficiary (as defined in [9]).
POI device	"Point of Interaction" device; the initial point where data is read from a consumer device (such as a PC or mobile phone) or where consumer data is entered. 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 Point of Sale (POS), vending machine, Automated Teller Machine (ATM) or merchant website (a so-called "virtual POI").

[4] Not to be confused with the mobile code or cardholder verification method (CVM).

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 environment	A system which implements the controlled storage and use of information. A secure environment is used to protect personal and/or confidential data. It may be located in the mobile device, such as a Secure Element or a Trusted Execution Environment, or located in a remote Secured Server.
Secured Server	A web server with secure remote access that enables the secure storage and processing of payment related data.
Static authentication	An authentication method that uses always the same authenticator (e.g., card data).
Strong authentication	A dynamic authentication method which involves at least two independent authenticators. This means that at least one of them is dynamic.
Trusted Execution Environment (TEE)	An execution environment (as defined by Global Platform, see [4]) 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 Service Manager (TSM)	A trusted third party acting on behalf of the secure element issuers and/or the mobile payment/authentication application issuers in the case where a secure element is involved, or on behalf of the mobile wallet issuers.
Trusted Third Party (TTP)	An entity which facilitates interactions between stakeholders of the ecosystem who all trust this third party. Examples of TTPs include TSMs and payment gateway providers.
Umbrella UI	Mobile wallet user interface component managing the portfolio of mobile payment services accessed through the mobile device. The umbrella UI is located in the mobile device.
User Interface (UI)	An application enabling the user interactions. Examples are umbrella UI, mobile payment/authentication application UI and credentials manager UI.
User Verification Method	A method for checking that a user (consumer) is the one claimed.

Table 2: Terminology

0.4 Abbreviations

Abbreviation	Term
C2B	Consumer-to-Business
C2C	Consumer-to-Consumer
CSM	Clearing and Settlement Mechanism
CVM	Cardholder Verification Method
ETSI	European Telecommunications Standards Institute
GP	GlobalPlatform
GSMA	The GSM Association
HSM	Hardware Security Module
IBAN	International Bank Account Number
ISP	Internet Service Provider
MCP	Mobile Contactless Payment
MNO	Mobile Network Operator
MRP	Mobile Remote Payment
MVNO	Mobile Virtual Network Operator
NFC	Near-Field Communications
OS	Operating System
OTA	Over the Air
PAN	Primary Account Number
PC	Personal Computer
POI	Point of Interaction
PSD	Payment Services Directive
PSP	Payment Service Provider
QR code	Quick Response code
SCP	SEPA Card Payment
SCT	SEPA Credit Transfer
SDD	SEPA Direct Debit
SE	Secure Element
TEE	Trusted Execution Environment
TSM	Trusted Service Manager
TTP	Trusted Third Party
UI	User Interface

Table 3: Abbreviations

1 General

1.1 About EPC

The European Payments Council (EPC, see http://www.europeanpaymentscouncil.eu/index.cfm) is the coordination and decision-making body of the European banking industry[5] in relation to payments. The purpose of the EPC is to support and promote the Single Euro Payments Area (SEPA). The EPC contributes to the development of the payment schemes and frameworks necessary to realise an integrated euro payments market. In particular, the EPC elaborates on common positions of payment service providers (PSPs)[6] for the cooperative space of payment services, assists in standardisation processes, formulates best practices and supports and monitors the implementation of decisions taken.

The EPC consists of 68 members representing banks, banking communities and payment institutions. More than 360 professionals from 28 countries are directly engaged in the EPC's work programme, representing organisations of all sizes and sectors of the European banking industry. The European Central Bank acts as an observer in all EPC working and support groups and in the EPC Plenary (the Plenary is the decision-making body of the EPC). The EPC is a not-for-profit organisation which makes all of its deliverables, including the SEPA Scheme Rulebooks and adjacent documentation, available to download free of charge on the EPC Website. Note that the EPC does not supply technology, goods or services.

Figure 1: SEPA coverage

1.2 Vision

The vision of the EPC is to contribute to the evolution of an integrated market for payments through helping in or facilitating the development and promotion of standards, best practices and schemes.

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

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

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

PSPs can deliver secure, efficient and user-friendly mobile solutions to access the SEPA payment instruments[7] which may coexist with other payments instruments.

Cross-industry collaboration between all the different stakeholders in the mobile payment ecosystem could be a critical success factor. Different mobile payment solutions from multiple PSPs should be able to coexist in a same mobile device. Consumers should not be bound to a specific network operator or particular mobile equipment; they should also retain their ability to switch between PSPs. Clearly, interoperability is "the" feature needed to achieve these goals.

Creating ease, convenience and trust for end-customers (payers/consumers and beneficiaries/merchants) is regarded as critical for the further development of mobile payments. Since a mobile wallet may be regarded as a key tool to address these challenges, the EPC has decided to devote a white paper to it.

1.3 Scope and Objectives

The purpose of this white paper is to describe the concept of a mobile wallet which provides an intuitive interface to consumers/payers to manage their portfolio of mobile payment services next to other mobile services. It further allows PSPs to create a simple and easy experience for their customers.

The paper presents a general overview of mobile wallets with an emphasis on its usage for mobile payments in the SEPA area[8]. It includes a detailed analysis of the usage of mobile wallets for both mobile contactless and mobile remote payments initiation, according to the focus areas set by the EPC [1].

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 instruments9;
- Inform on the new convenient, homogenous and seamless service access and new business opportunities enabled by the usage of a mobile wallet to perform mobile payment transactions;
- Provide examples of the usage of a mobile wallet for mobile payments;
- Outline the mobile wallet ecosystem and the different existing models for mobile wallets supporting payments.

1.4 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 wallets but it rather focuses on the initiation and authentication of payments via the mobile wallet. It aims to provide a high level overview on different aspects of payments performed through mobile wallets while avoiding detail of implementation specifics.

The document does not contain market research since a number of studies are already available. As such the specification of business cases and detailed analyses of mobile wallet value chains are outside the scope of the present document.

[7] See Annex 1 for more information.
[8] Note that the concepts described in this white paper may also be applied outside SEPA.
[9] See Annex 1 for more information.

1.5 Audience

This document aims to handle the concept of mobile wallets at a non-technical level. It is intended for PSPs as well as for other interested parties involved in mobile payments, such as:

- Mobile wallet issuers;
- Equipment manufacturers/vendors;
- Application developers;
- Consumers;
- Merchants and merchant organisations;
- Public administrations;
- Regulators;
- Standardisation and industry bodies;
- Payment schemes;
- (Mobile) Network Operators;
- Trusted Service Managers;
- Trusted Third Parties;

and

- Other interested parties.

2 Introduction

Similar to the physical world, a "digital wallet" acts as a digital organiser[10] and typically contains identification information on the wallet holder, on payments instruments accessible to the wallet holder and optionally personal information items belonging to the holder (e.g., pictures, documents, etc.). This may include information related to eIDs, 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 is based on technical infrastructures (hardware and software) allowing the secure storage, processing and communication of the information described above provided by the wallet holder, the wallet issuer and the application/service providers. There exists a wide variety of different implementations for these infrastructures ranging from full implementation in the equipment of the wallet holder to remote implementations (as a remote wallet in a "Software as a Service") accessed through the wallet holder's equipment.

Mobile wallets are digital wallets which are accessed through a mobile device (e.g., mobile phone, tablet, etc....). In the context of this document it is a service allowing the wallet holder to access, manage and use mobile payment services, possibly, next to non-payment applications. As said before, 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.

Although different mobile wallets have been launched in the market in recent years, they are still in their early stages of development. However, a variety of services are already offered to customers. Where originally the penetration of mobile wallets was more focused on coupon deployment and loyalty management, more recently, the mobile wallet presents diverse capabilities extending well beyond these services such as the management of mobile financial services including mobile banking and payment opportunities.

As an illustration, a mobile wallet may include (but is not limited to) the following features:

- Management by the consumer/payer of a broad portfolio of mobile payment services from different providers (e.g., prioritisation or default selection) including sensitive data to be protected;
- Facilitation of the payments (selection and authentication) for goods or services or person-to-person payments;
- Storage of tickets, boarding passes that can be presented at a checkpoint;
- Offering of a single storage place for loyalty programs and coupons;
- Storage of credentials for easy and convenient identification and authentication (e.g., for access control);
- Storage of personal information such as delivery address to facilitate on-line shopping experience, …

[10] Also referred to as a "digital container" by Mobey Forum (see [8])

In addition, mobile wallets may facilitate the set-up of value added services for service providers or merchants. As an example of such a value-added service, a merchant may make a special offer to customers who are in the vicinity of its outlet. Another example is the pop-up of the entrance ticket on the mobile device screen when approaching a movie theatre.

This white paper will focus on mobile payment services presented via a mobile wallet which is hosted on, or accessed via, a mobile device. Appropriate technical and security requirements will need to be fulfilled by mobile wallets in order to support payment services. In addition, ownership of and responsibilities for the mobile wallet need to be clarified and will be implementation dependent.

As illustrated in Figure 2, one or multiple mobile wallets may coexist and be accessed through a mobile device; hereby each mobile wallet may contain one or multiple applications/services[11].This figure is used only as an example of mobile wallets in a mobile device. Additional configurations may exist which involve different mobile wallets, each managing multiple mobile financial services.

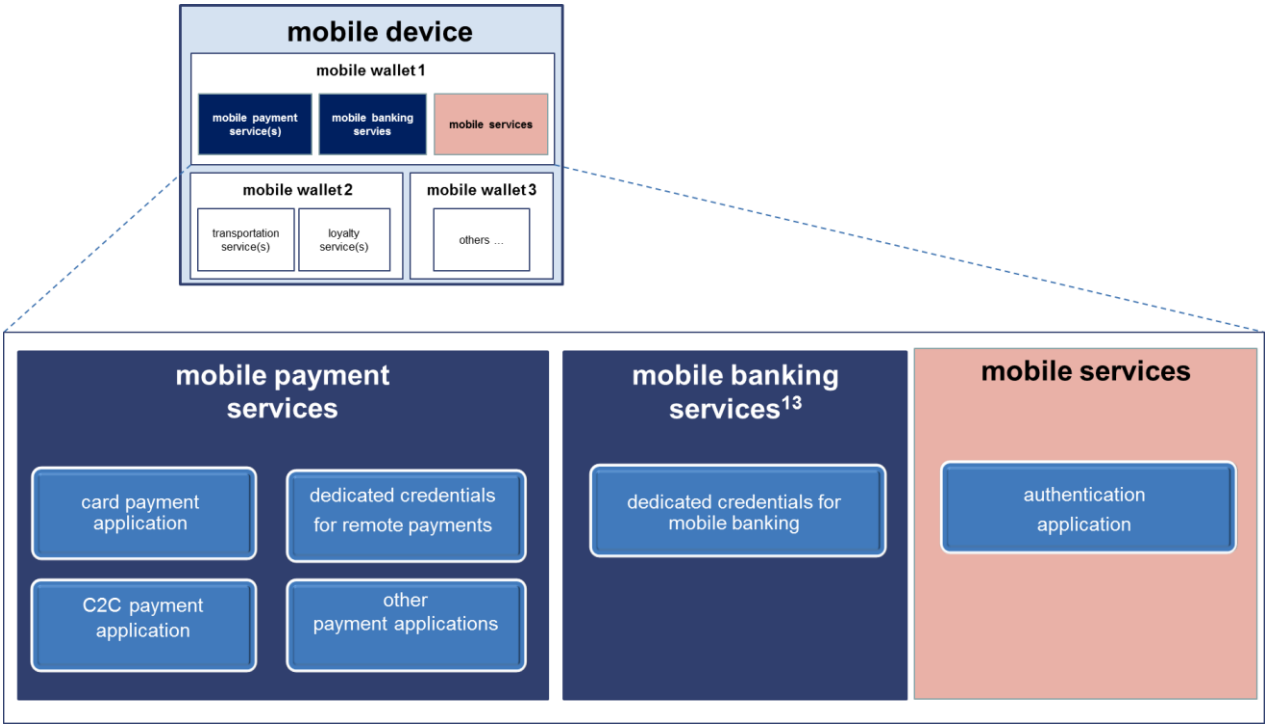

Figure 2: Example of multiple mobile wallets accessed through a mobile device

[11] Note that mobile payment/authentication applications installed on a mobile device may be also directly accessed without the usage of a mobile wallet.

[12] Note that mobile payment services may be accessed through mobile banking services.

3 Mobile wallet for mobile financial services

3.1 A day in the life of a mobile wallet holder

This section demonstrates how the daily life of a consumer can be enhanced by using a mobile wallet accessed via his/her mobile device for the execution of mobile financial services. 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 wallet initiated payment services.

Mr Garcia, a regular mobile phone user with a very busy life, particularly enjoys using his mobile phone beyond just browsing, 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, including payments. As a customer of different PSPs, he has a mobile wallet installed on his mobile phone to facilitate his mobile financial services. Amongst others, his mobile wallet contains a payment card application, a C2C card-based application and dedicated credentials for remote card and SCT payments as well as mobile banking. If more than one payment application of a certain type is available in the wallet, it is assumed that he would have set a prioritisation list.

The following figure depicts a day in his life.

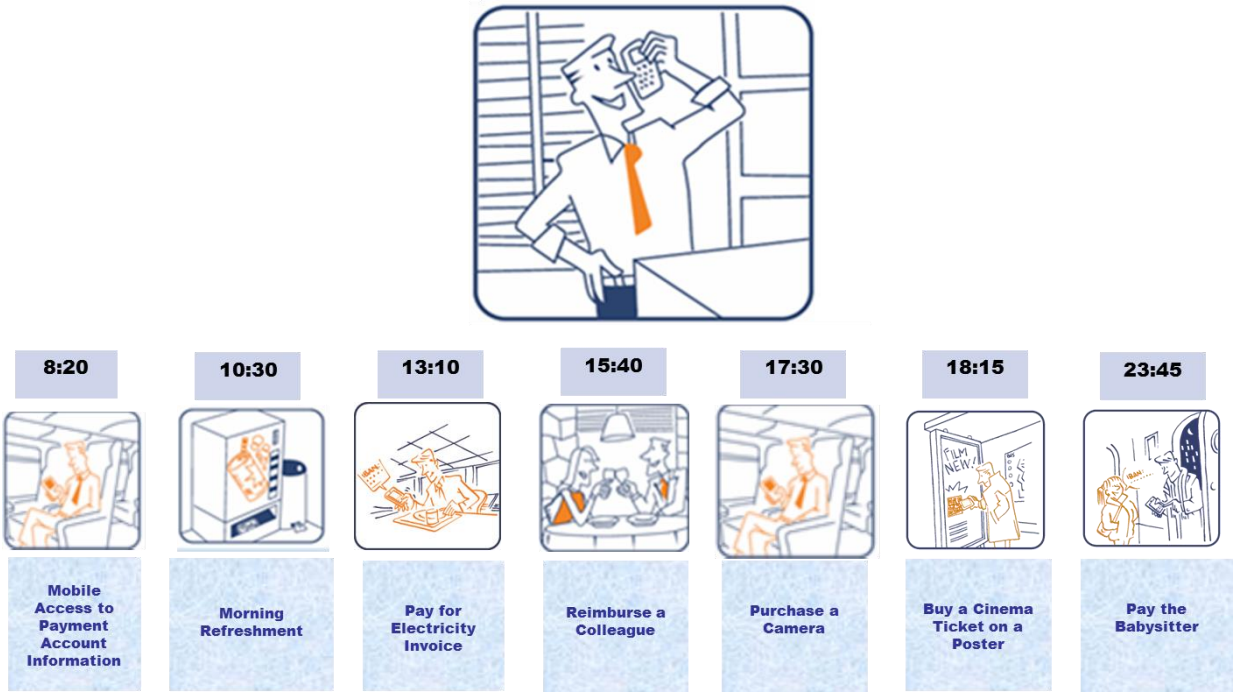

Figure 3: A day in the life of Mr Garcia

3.1.1 Mobile access to payment account information

Next week, Mr Garcia's family will be celebrating their daughter's birthday and therefore he bought gifts for her yesterday. Comfortably seated in the train on his way to the office, he decides to check the status of his banking account via his mobile phone. Mr Garcia enters his mobile wallet passcode to open the wallet which contains the credentials and the related on-line passcode for the on-line banking service from his PSP. After an automatic verification of this on-line passcode, he gets access to his account balance, the list of the last (e.g., ten) transactions as well as the list of scheduled financial transactions. Mr Garcia is now reassured about the correct payment of his purchases, logs off his banking application and starts reading the news on his mobile device.

3.1.2 Morning refreshment

By mid-morning, Mr Garcia takes a short break. Just outside his office there is a small food parlour with several vending machines. After selecting a cappuccino, he opens his mobile wallet and presents his mobile phone to the contactless reader of the vending machine. An MCP application in his mobile wallet will be used to pay for this drink (see section 4.2.1 in [1]). With the payment, the vending machine (recognising that a mobile phone has been used for the payment) shows the website of the cappuccino brand for a special offer. Next, Mr Garcia downloads a reduction coupon on his mobile phone for usage with his next purchase.

3.1.3 Payment of the electricity invoice

During lunch break, Mr Garcia is checking his e-mails on his mobile phone. He received this morning a message from his electricity supplier presenting his bimonthly invoice to be paid. Mr Garcia opens his mobile wallet which contains the credentials for the on-line banking service from his PSP. Mr Garcia selects his preferred payment account and the IBAN of his electricity supplier from a list of registered beneficiaries. Mr Garcia is invited to enter the amount and optionally, a reference for the transaction for identification in his future statement. After checking, he confirms the payment transaction through an authentication process involving his on-line passcode. In return, he receives an SMS from his PSP that the SCT will be processed with the amount and the appropriate reference (see section 5.3. in [1]).

3.1.4 Reimbursement of a colleague

In the afternoon, Mr Garcia wants to reimburse a colleague who paid an earlier restaurant bill. In order to do so, Mr Garcia opens his mobile wallet and selects the C2C payment application. Since he intends to use his corporate payment card instead of his preferred (personal) payment card, he has to explicitly select it in his mobile wallet. He is subsequently invited to enter the amount and a unique identifier of his colleague (e.g., mobile phone number) and to confirm the transaction by entering his mobile code. His colleague will receive a confirmation of the transaction while Mr Garcia will receive a message on his mobile wallet informing that his card account has been debited (see section 5.2.4 in [1]).

3.1.5 Purchase of a camera

While travelling back home, Mr Garcia navigates using his mobile device browser to a merchant's website via mobile internet and selects a camera he wants to purchase. He is subsequently invited to confirm the purchase. The checkout section of the merchant's website displays the transaction details and Mr Garcia selects the (corresponding) wallet payment method on the merchant's website. This selection triggers the opening of his mobile wallet and the selected card details are displayed. He subsequently validates the transaction by entering his mobile code. The mobile wallet will automatically complete the card transaction and will provide the merchant's website with the necessary information including the delivery details. The merchant's website will process the transaction and will inform Mr Garcia about the outcome via his mobile browser (see section 5.2.2 in [1]).

3.1.6 Purchase of a cinema ticket on a poster

After leaving the train, Mr Garcia walks down the main shopping street. He notices an advertising poster on a bus stop inviting him to scan a QR code to buy a "film premiere" ticket for the same evening. Since only the first 300 participants will have a chance to participate in this event, Mr Garcia opens his mobile wallet, selects the supported mobile remote payment application and scans the QR Code. The transaction information is displayed on his mobile device and he chooses to pay by SCT. Mr Garcia is invited to authenticate himself (involving his on-line passcode) to authorise the SCT transaction. The merchant then receives a notification that the payment is on its way and sends a voucher to Mr Garcia's mobile device, which is automatically stored in his mobile wallet to be used as a ticket when he arrives at the premiere event.

3.1.7 Payment of the babysitter

In the evening, Mr Garcia invites his wife to the film premiere and hires a new babysitter, Sonia. After an enjoyable evening, Mr Garcia needs to pay Sonia before taking her home. He requests Sonia's alias (e.g., mobile phone number) and opens his mobile wallet to select the C2C payment application from his PSP to make the credit transfer. He manually enters Sonia's alias as the beneficiary and enters the amount and optionally, a reference for the transaction (e.g., Sonia - June 2013) for identification in his future statement. Mr Garcia then checks the information and confirms the payment transaction involving his on-line passcode. In return, his PSP sends him an e-mail indicating that the SCT will be processed with the amount and the appropriate reference (see section 5.3.2 in [1]).

3.2 Mobile wallet and mobile payments

3.2.1 Mobile wallet usage for payments

As shown in the examples in the previous section, the mobile wallet may facilitate the payment initiation phase for the consumer/payer by supporting the selection of the payment instrument as well as the authentication process. Mobile wallets may support a variety of payment instruments with different authentication methods, including mobile proximity and remote payments. This may offer opportunities for both consumers and merchants if they understand in terms of security and convenience (such as using a mobile wallet for in-store remote payments). Optionally, a passcode could be used to open the mobile wallet (see section 6.3 for more details).

The following table illustrates how the payment use-cases can be implemented using the existing SEPA instruments. It should be noted, however, that some use-cases described in the previous section may be

implemented by other SEPA instruments than the one presented. Therefore, a use-case listed in Table 4 below should not be interpreted as the class-type representative of the mobile payment concerned.

		SEPA Credit Transfer	SEPA Card Payment
Mobile proximity payment (using contactless technology)	C2B		Morning refreshment
Mobile proximity payment (using another technology)	C2B	Purchase of a cinema ticket on a poster	
Mobile remote payment	C2B	Payment of the electricity invoice	Payment for a camera
	C2C	Payment of the babysitter	Reimbursement of a colleague

Table 4: Illustration of usage of a mobile wallet for payments based on SEPA instruments

Note that more details on the specific use cases described in sections 3.1.2, 3.1.5 and 3.1.7 may be found in Annex 2.

Depending on the payment services supported, the mobile wallet application can be very simple, when designed to manage information related to a single payment instrument, or, more complex, when different payment instruments are involved. However, in any case, it allows the wallet holder (consumer/payer) to select, at any given time, the payment instrument he/she wants to use for a particular transaction.

In addition, it is desirable that the mobile wallet will enable the consumer/payer to:

- Define a default payment instrument – one for all or even better, one for every type of payment situation (e.g., prepaid card X for contactless payments, SCT of bank Y for C2B remote payments, credit card Z for C2C remote payments, ...);

or

- Prioritise one mobile payment service over another, for example by selecting the payment card to be active.

3.2.2 High level principles

Conceptually, a mobile wallet may be provided by a PSP that issues a single or multiple payment instruments with the only aim being to manage these payment instruments[13]. Alternatively, the mobile wallet may be provided by a mobile wallet issuer or a trusted third party (TTP) acting on its behalf, and designed to manage payment instruments issued by multiple PSPs (see section 5 for more information).

It would be desirable that mobile wallet issuers ensure their mobile wallets follow some basic principles in support of mobile payment services based on SEPA instruments such as:

1. Consumers/payers should be able to use their mobile wallet(s) to make mobile payments throughout SEPA, regardless of the original country where the mobile wallet was issued and where the SEPA mobile payment services were subscribed to;

[13] Potentially next to other mobile financial services provided by the same PSP

2. The usage of a mobile wallet should not impact the security of the underlying payment instrument including the protection of personal data (see [1] and [2] for more details);
3. A mobile wallet should be able to support the easy recognition and selection by the consumer/payer of any mobile payment service defined by a PSP, including brands & logos, payment scheme brands, payment instrument, etc. as appropriate;
4. All PSP's proprietary personalisation data related to a customer for a mobile payment service (e.g., IBAN, PAN...) accessed through a mobile wallet in the course of mobile payments, should remain under the management of the payer's PSP;
5. A mobile wallet should enable mobile payment services by including core functionalities such as (but not limited to):
    - Selection and initiation of a mobile payment via the mobile device, from a list of mobile payment services supported by the mobile wallet;
    - Life cycle management of credentials and payment/authentication applications (installation, update, activation, deactivation, cancellation, etc.);
6. Mobile wallets should ensure a high availability of their services as expected by their holders.

4 Mobile wallet payments ecosystem

4.1 Introduction

The ecosystem for mobile wallet payments includes a variety of aspects such as the different stakeholders, their business models, the technical infrastructure and security measures and the legal framework. However this white paper will only focus on the stakeholders involved and on some technical and security aspects.

Mobile wallet payments introduce new stakeholders in the ecosystem in addition to the existing stakeholders for mobile payments as described in sections 4.3 and 5.4 in [1]. Since mobile wallets are dynamic and fast-developing, there is a potential for existing stakeholders in mobile payments to take on additional roles and/or for new players to enter the market. These new stakeholders may come from different backgrounds with a variety of motivations to offer robust, competitive and effective mobile wallet services for consumers.

4.2 Stakeholders of the mobile payments ecosystem

The following stakeholders in the *mobile payments* ecosystem which were already identified in [1] take also part in the *mobile wallet payments* ecosystem.

1. The consumer/payer 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 contractual relationships with a network operator (an MNO and/or an ISP) for mobile services; the consumer experience will be driven by convenience, cost and the offerings from the other stakeholders in the ecosystem. The consumer may control which mobile wallet he/she wants to use, and which content he/she wants in his/her mobile wallet by making the necessary arrangements with the mobile wallet issuer and mobile (payment) service providers.
2. The beneficiary owns a SEPA payment account or, where relevant, a SEPA compliant card.
    - In the case where the beneficiary is a merchant, the beneficiary is the acceptor of payments for goods or services purchased by the consumer/payer. A mobile wallet can offer a new way to interact with its customers. An added incentive may also come in the shape of the mobile wallet being an effective way to establish brand exposure and closer customer relationships by offering loyalty incentives, discounts and other marketing offers;
    - In the case where the beneficiary is a private customer/small business, there may be situations where it is very convenient for the beneficiary to own a mobile device in order to receive value added services like notifications.
3. The PSP offers SEPA payment services compliant with regulatory/security requirements. As a service provider that handles its customers' financial services through various channels, a PSP may aspire to take on a new role in mobile wallet services and position its brand in this new financial environment.
4. The network operator, an MNO and/or an ISP, is responsible for securely routing messages, operating the mobile and/or the internet network. Furthermore, an MNO has the capability to put the mobile wallet and mobile payment/authentication applications onto the consumer's mobile devices/UICC.
5. The payment system functions are both provided by a payment scheme based on a SEPA payment instrument (see Annex 1) and a clearing and settlement mechanism (CSM).

6. In the case where a dedicated payment application (MCP or MRP application), authentication application or credentials on the mobile device is/are involved, the mobile payment service issuer is the PSP responsible for provisioning the application or the credentials to the consumer/payer. The application or credentials is/are stored in a secure environment. This is typically in a Secure Element (SE) on the mobile device or on a remote Secured Server. This implies the involvement of additional stakeholders such as the SE issuer (see [1]). Optionally, the mobile payment service issuer may also use a so-called Trusted Service Manager (TSM) for the life cycle management of the application.
7. The Trusted Service Manager (TSM) is a TTP acting on behalf of the SE issuers and/or the mobile payment service issuers to facilitate an open ecosystem. Mobile payment service issuers, TSMs and SE issuers collaborate to perform the provisioning and management of the application(s) and/or credentials.
8. An optional TTP that operates an infrastructure that could facilitate increased convenience and/or trust for the parties involved (e.g., a common infrastructure when an alias is used for remote payments, see [1]);
9. A payment gateway provider is a TTP that facilitates the transfer of information between the payment portal (such as a website or mobile device) and the beneficiary's PSP. This service can be operated directly by the PSP.

Additional stakeholders include for example:

- Manufacturers in the case where a secure environment is involved (e.g., SE manufacturer);
- Application developers for MCP, MRP, authentication applications and mobile wallets with their dedicated user interfaces;
- Mobile device manufacturers/vendors;
- Organisations performing infrastructure evaluation/certification.

The reader is referred to [1] for further details on the roles of these stakeholders in mobile payments.

4.3 New stakeholders specific to the mobile wallet payments ecosystem

Next to the stakeholders described above, this section describes the new additional stakeholders identified in the mobile wallet payments ecosystem.

- The mobile wallet issuer delivers mobile wallet functionalities (see section 3.2) to the customer (consumer or merchant). For this purpose, new players may enter the market, or already existing stakeholders in the mobile (wallet) payments ecosystem, such as PSPs, TSMs, TTPs, MNOs, merchants, OS providers or payment schemes, may assume this role. Their motivation to do so may include enhancing support to their customers, widening their financial services business or strengthening their brand position in mobile services, mainly in the mass market. Note that in addition to its roles defined above, a TSM may also be involved to act on behalf of the mobile wallet issuer.
- The mobile wallet gateway provider operates the mobile wallet gateway service that establishes a link between the mobile wallet and a payment gateway for mobile payments transactions. This service may be operated directly by the mobile wallet issuer or by a TTP.

All the stakeholders described above will need to establish the appropriate contracts and service level agreements to agree on the functional and security requirements, liabilities, etc. However, as mentioned before, this is outside the scope of the current document.

Note that the figures used for illustrative purposes in the remaining sections of this document have been simplified and only present a high level view (of parts) of the mobile wallet payments ecosystem. As a consequence, they do not depict all stakeholders involved as outlined above.

5 Mobile wallet models for mobile payments

5.1 Introduction

This white paper assumes that consumers/payers will perform mobile payment services via a mobile wallet accessed through a mobile device. Depending on the type of mobile payment services covered and on the mobile wallet issuer, different mobile wallet models may be identified. Because of the variety of influencing factors ranging from pure business to more technical aspects, a categorisation of these models proves to be challenging. These main factors may include among others:

- The variety of mobile services covered, such as proximity or remote payment products from one or multiple PSPs, non-payment services, etc.;
- The mobile wallet issuer (e.g., an independent TTP or a mobile (payment) service issuer);
- The location of the mobile wallet.

However, in what follows an attempt is made to distinguish a few trends appearing in the market today:

- Vertical versus horizontal mobile wallets;
- Mobile wallet in the payer's space versus mobile wallet in the beneficiary's space;
- Mobile wallet located in the mobile device versus a remote Secured Server (also sometimes referred to as "in the cloud"), or a combination thereof.

Note that this list is not exhaustive and other models could emerge on the market in the future. In addition this categorisation is not exclusive in the sense that a given mobile wallet may belong to different categories (e.g., a horizontal wallet in the payer's space on a remote server accessed via a mobile device).

The following sections aim to provide a high level overview on some mobile wallet models while focusing on mobile payment services. A PSP can freely choose the models of mobile wallet it will support to provide its mobile payment services. However its choice should not conflict with existing terms and conditions to conduct mobile payments.

5.2 Vertical versus horizontal models

One way of categorising mobile wallets is by introducing the concept of a "vertical" versus "horizontal" mobile wallet as presented in the Mobey Forum work [8].

- A "*vertical*" mobile wallet is typically developed by a single service provider and is limited to hosting mobile services/applications from this provider only (see Figure 4). Although this could be considered as a rather closed approach, the vertical mobile wallet is assumed to be easier to manage, and is scalable in terms of costs, maintenance and operational models. Typically, a vertical mobile wallet is provided by the mobile wallet issuer with a number of preloaded services.

- A "*horizontal*" mobile wallet is designed to accommodate multiple mobile services developed by a number of different service providers (see Figure 4). It aims to offer an open wallet in terms of services to the customers. It allows customers to acquire and organise mobile services from different service providers.

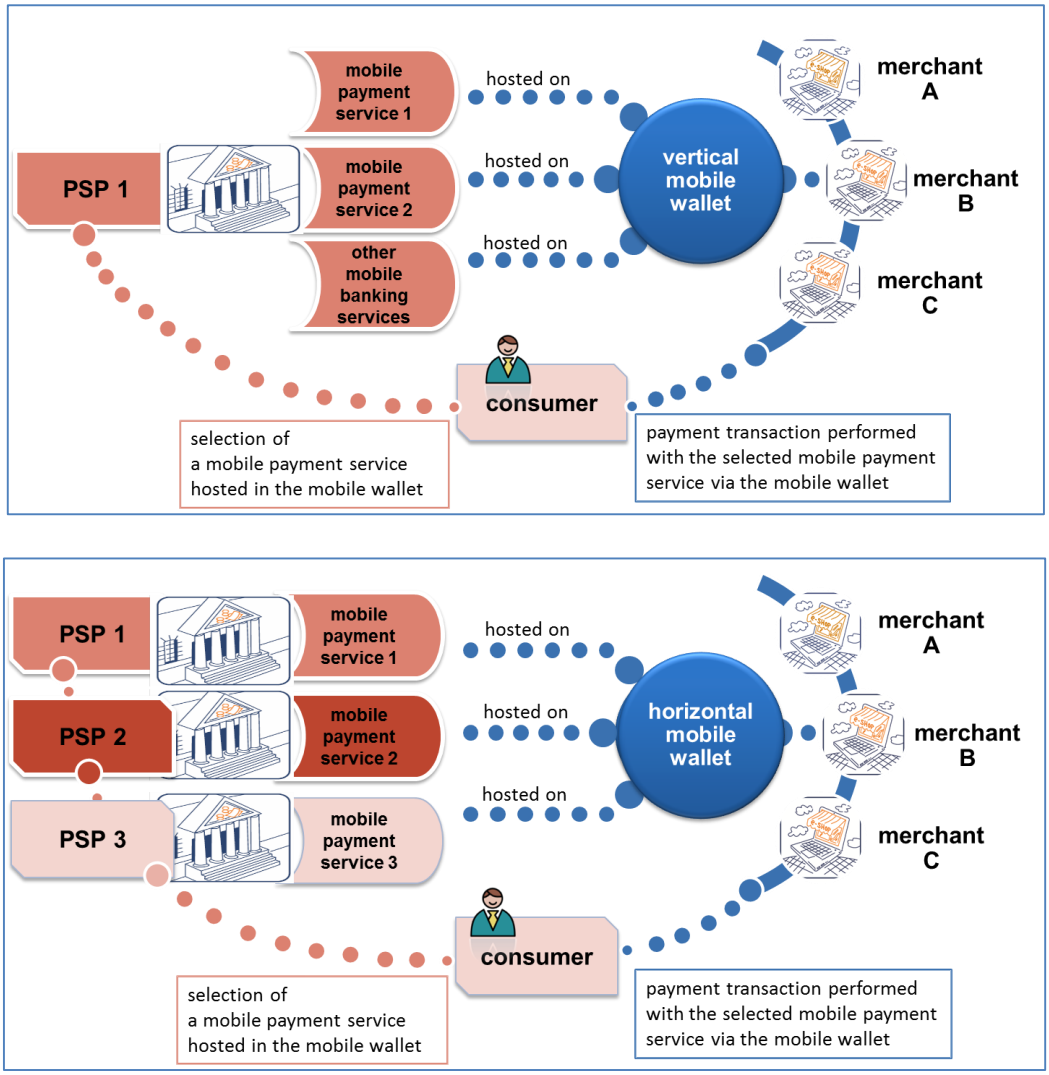

Figure 4: Vertical versus horizontal mobile wallet

Let us now focus on mobile wallets used for mobile payment services. Most of the solutions introduced on the market during the past years for the support of mobile payments were under the responsibility of the PSPs. This means that the PSP was solely responsible for the issuance and life cycle management of a mobile wallet containing its payment services.

But with the enhanced (security) technology offerings' appearing on the market today, a more open mobile wallet approach becomes feasible to support mobile payment services. The consumer/payer may decide him/herself on a preferred mobile wallet and the mobile payment/authentication applications he/she wants to access through this mobile wallet. As an example, the consumer/payer may directly add credentials issued by his/her PSP, or more generally mobile payment services to his/her mobile wallet,

possibly without direct interaction with his/her PSP[14] (as long as the underlying mobile payment service is covered by a contract with his/her PSP). However, this more open approach might require a contractual relationship between the mobile payment/authentication application issuer(s) and the mobile wallet issuer for inclusion of mobile payment services in the wallet. For illustration purposes an example is given in Figure 5 below.

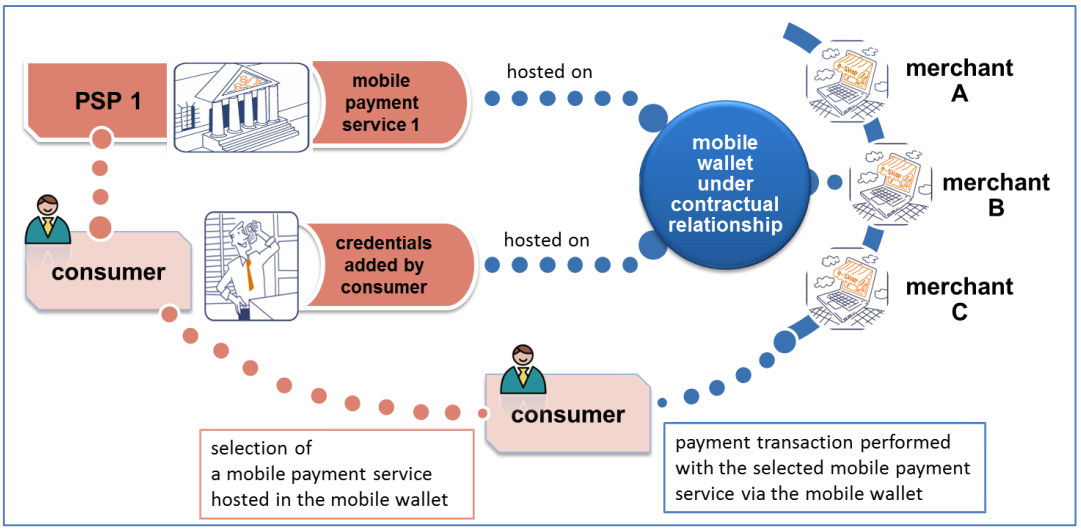

Figure 5: Example of a mobile wallet under contractual relationships between PSPs and a mobile wallet issuer

This open approach may offer the possibility to the mobile wallet issuer for aggregation of some payment services with other non-payment services (e.g., loyalty, transport, couponing …) in order to gain mass market attraction. On the other hand, there may be a number of challenges with this open approach including interoperability between different mobile service providers, mobile service life cycle management including customer support and the establishment of appropriate service agreements between the mobile wallet issuer and the multiple mobile service providers. Moreover, this model, where the consumer is given certain freedom to populate the mobile wallet, may require specifications of common interfaces between the mobile wallet and mobile service life cycle management infrastructures. Consequently, it might be more difficult to deploy these open models without the development of appropriate standards.

It should further be noted that the two models are not mutually exclusive and may co-exist within the same mobile device (e.g., a horizontal wallet model for loyalty programs and a vertical wallet model for mobile payment services).

[14] Note that with the introduction of smart phones, the consumer is already familiar with selecting and downloading services from dedicated web stores.

5.3 Payer's space versus beneficiary's space models

It is recognised that a mobile wallet may help to provide an improved payment experience to consumers/payers and merchants/beneficiaries:

- For consumers/payers, the mobile wallet could provide convenience and security;
- For merchants/beneficiaries, the mobile wallet could provide additional opportunities to attract new consumers and to enhance the relationships with existing consumers, e.g., by offering additional services around payment such as couponing or loyalty.

Another way of categorising mobile wallets is by introducing the two following mobile wallet types depending on the "spaces" where they are issued:

- The so-called *"payer's space mobile wallet"* where the mobile wallet issuer has "an agreement with" or "is" the consumer/payer's PSP. An example of the latter case is the vertical mobile wallet (see section 5.2). It can be hosted either on the mobile device of the payer or on a Secured Server or a combination thereof.
- The so-called *"beneficiary's space mobile wallet"* where the mobile wallet issuer has "an agreement with" or "is" the merchant or the merchant/beneficiary's PSP. When the issuer is the merchant, it is generally referred to as a *merchant wallet*[15]. Note that this wallet can be hosted either on the mobile device[16] of the payer, on a Secured Server (hosted by a TTP or a merchant).

Note that in both cases the mobile wallet issuer may be a new player or an existing stakeholder as described in section **Error! Reference source not found.**.

Let us focus now on the merchant wallet model related to the integration of specific services at the merchant's website. In this case, the mobile wallet issuer is the merchant.

As represented in Figure 6 (configuration 1), a merchant wallet could be for example a wallet issued by a merchant which is located on the merchant's website[17] and accessed via a dedicated application in the mobile device of the consumer/payer. Although different mobile payment services, potentially from different PSPs, may be registered in a merchant wallet, it usually only allows the consumer/payer to pay on the website of this specific merchant.

Alternatives may exist (configuration 2) whereby a merchant wallet allows payments on websites from different merchants but hosted on the same platform.

[15] Note that in the context of this document, it is just a subset of the general concept of a digital wallet issued by the merchant.
[16] The mobile wallet is hosted in the mobile device of the payer (for usage) but it remains a mobile wallet from the beneficiary's space (the mobile wallet issuer is in the beneficiary's space)
[17] In this case, there may be security concerns in terms of responsibility for the security of the mobile payment related data and, consequently, a secure environment is also needed for the remote storage of these mobile payment related data.

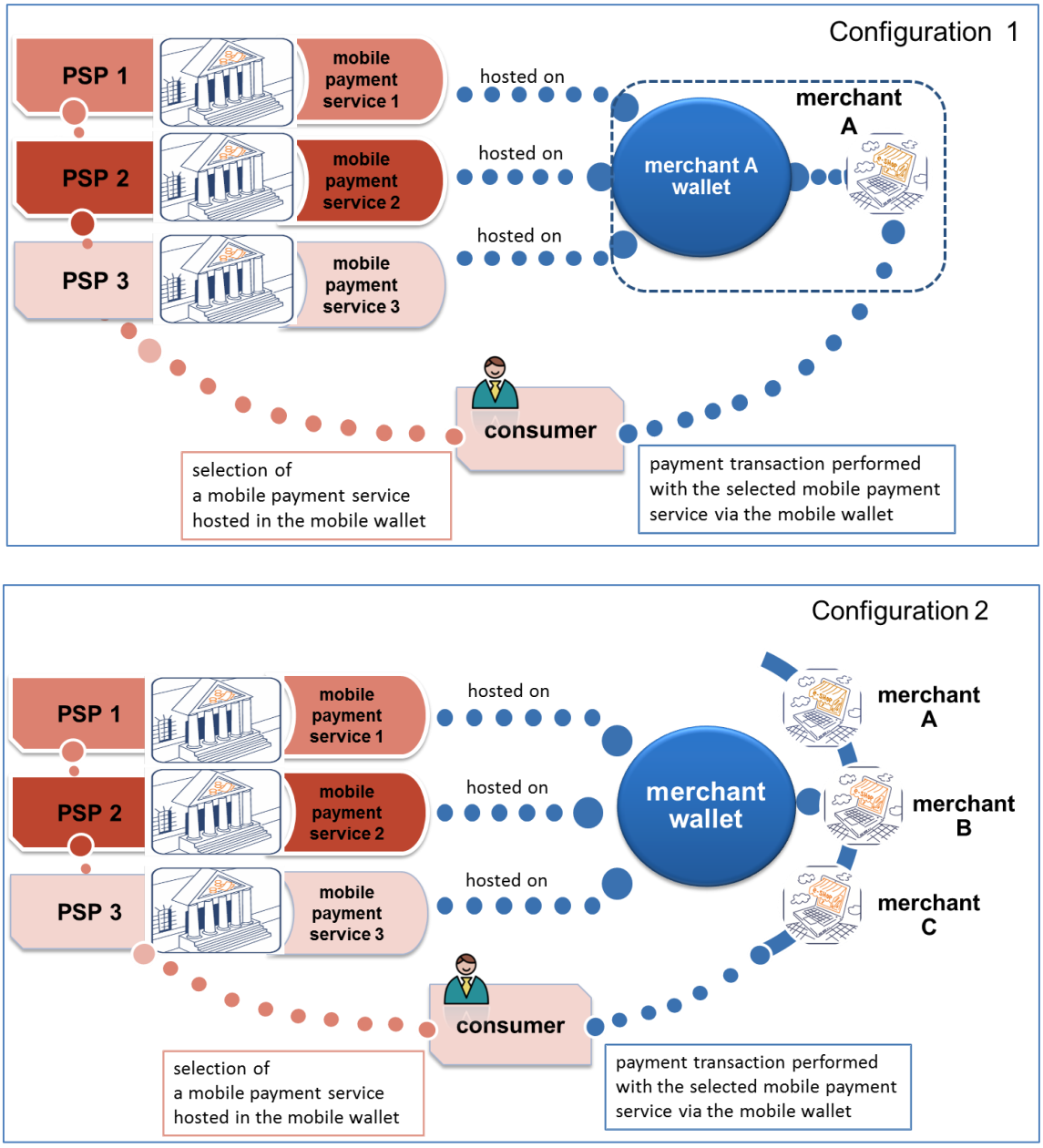

Figure 6: Merchant wallet

5.4 Location of the mobile wallet: from mobile device to Secured Server

A more technical approach for distinguishing a mobile wallet model is by analysing its location with respect to the mobile device. The mobile wallet may be hosted on a mobile device or (partly) stored remotely (also sometimes referred to as "*in the cloud*"). But in any case, the mobile wallet is always accessed via a user interface (e.g., the umbrella UI, see section 6.1) hosted on the mobile device, as shown in the figure below.

Figure 7: Locations of the mobile wallet

Note that multiple mobile wallets in different locations may co-exist and be hosted in or accessed through a single mobile device. As an example, Figure 19 in Annex 2 depicts a mobile device whereby two mobile wallets are managed through a common umbrella UI, one on the mobile device and one on a Secured Server.

In the case that a mobile wallet or parts thereof are stored remotely, an appropriate secure environment (e.g., a Secured Server) is needed (e.g. to store and process the mobile payment related data, see section 6.1). PSPs should consider that this model may offer certain advantages with respect to the accommodation of mobile services (e.g., fast technical integration process). In addition, it allows access from different mobile devices and it may ease the remote management of the mobile wallet, such as locking, disabling or resetting (see section 7), under control of the mobile wallet issuer who delivers mobile wallet functionalities.

In terms of availability, a key difference related to the location of the mobile wallet is the capability to (always) perform transactions. Indeed, a mobile wallet fully located on a mobile device may allow off-line transactions (e.g., contactless payments), while the one (partially) hosted on a remote server needs connection to this server to perform the transaction.

5.5 Conclusions

From the previous sections, it may be concluded that a variety of mobile wallet models are likely to coexist in the market. An important factor influencing the market take up of a mobile wallet model is the user experience. From a consumer perspective, the mobile wallet allows him/her to store, access and manage mobile services including payments. Therefore user friendliness, convenience, variety of services offered and trust are "key" for the consumer's choice of a particular model. Note in the context of trust, a distinction shall be made between a mobile wallet itself and a payment instrument (which is covered by a set of rules[18]) accessed through the mobile wallet. As such the mobile wallet model should not impact the security of the payment services covered.

It is noted that other factors may influence a mobile wallet model including:

- The ease of implementation of value added services around payments for merchants;
- The type of mobile payment services hosted in, or accessed through, the mobile wallet, and the number of different PSPs involved;
- The acceptance of a unified UI for mobile payment services offered by different PSPs;
- The coexistence of mobile payment services with other mobile services;
- The consumer awareness and education related to security and privacy aspects of the mobile wallet used for payment services. An example is the possible capture of purchase related data from mobile wallet payments and the subsequent (commercial) exploitation of such collected data without consent of the consumer;
- The type of secure environment and its location.

Open mobile wallets are considered to be important for the market take-up of mobile payments whereby the combination with mobile non-payment services will allow the critical mass to be reached.

As mentioned in section 2, multiple mobile wallets may coexist and may be accessed through a single mobile device (see Figure 2). Note that these mobile wallets may cover different models as described above.

[18] Typically specified by the payment scheme

6 Technical aspects

6.1 Mobile wallet components to support mobile payments

A mobile wallet supporting mobile payments may be viewed as a combination of the three following components:

- The payment component itself. This can be a dedicated payment/authentication application and/or a set of credentials; this component should reside inside a secure environment, such as a Secure Element (SE), or on a Secured Server (typically involving an HSM); its role is to securely execute mobile payment transactions. This component is under the responsibility of the payer's PSP.

- The payment User Interface (UI) component. This component enables the consumer/payer to manage a specific mobile payment service through a dedicated user interface. Depending on the payment component type, i.e. dedicated application or credentials, this component may be a mobile payment/authentication application UI or a credentials manager UI (see Figure 8). In terms of security, TEE-enabled mobile devices may use the Trusted User Interface from the TEE to protect the sensitive operations such as the entry of the on-line passcode or mobile code. Depending on the implementation, various service providers might be responsible for this user interface (e.g., a mobile payment service provider in the case of a dedicated application or a mobile wallet issuer in the case of a credentials manager).

- The umbrella UI component. This component manages the portfolio of mobile payment services accessed through the mobile device. This may include services offered by different PSPs. Depending on the mobile payment services, the UI to the payment component may be launched through this umbrella UI (see Figure 15 and Figure 19 in Annex 3). The umbrella UI is located in the mobile device and aggregates multiple payment component UIs. This component is under the responsibility of the mobile wallet issuer. In terms of security, TEE-enabled mobile devices may use the Trusted User Interface from the TEE to protect the sensitive operations such as the entry of the mobile wallet passcode (see section 6.3).

It has to be noted that not all three components are necessarily present within the mobile wallet. As examples, the umbrella UI may be integrated with a payment component UI, a payment component (in the mobile wallet) may be directly accessed via its related UI, or a payment component may be residing outside but only accessed via the mobile wallet.

However, it is useful to consider a range of situations:

- From the simpler ones, where a single payment service is available on, or accessible via, the mobile device, next to other mobile services;
- To complex ones (as illustrated in Figure 8) where multiple mobile payment services of different nature (e.g., an SE with a MCP application, credentials for MRPs, etc.) are stored on, or accessed through, the mobile device, such as mobile financial services or authentication services, next to other mobile services. Moreover, the same set of credentials or authentication application may be shared by multiple mobile payment services.

In the case where multiple mobile payment services are managed by different mobile wallets in the same mobile device (such as presented in Annex 3), there is a challenge on how the user will select a specific mobile payment service.

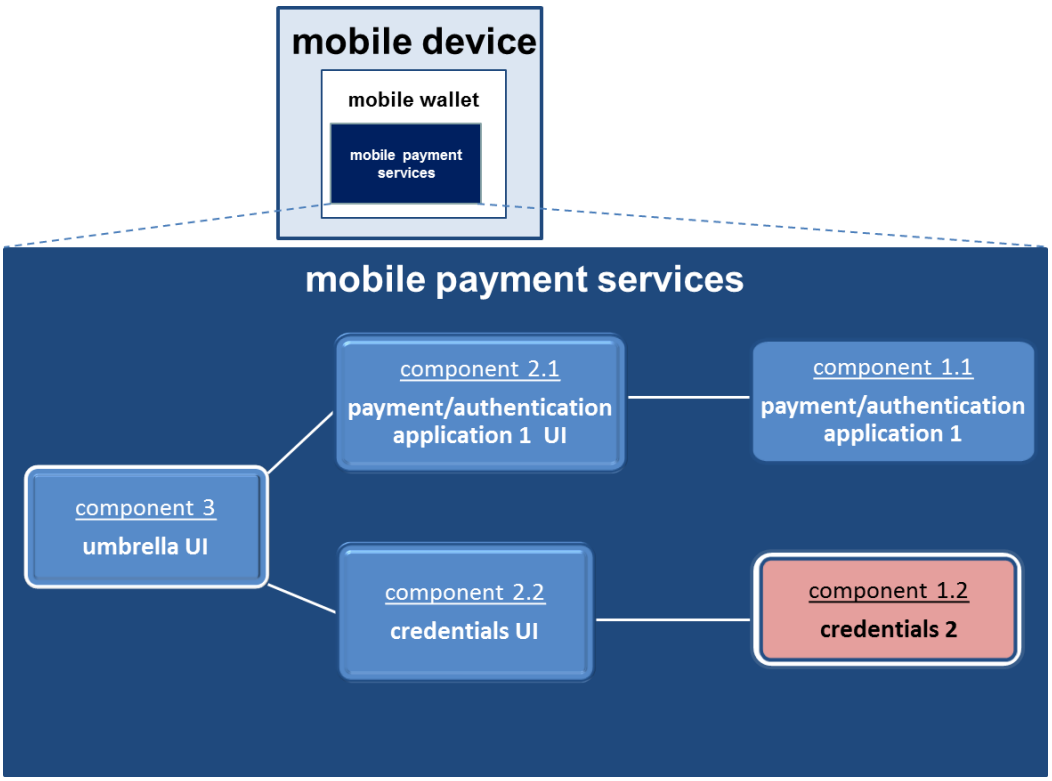

Figure 8: Example of a mobile wallet with two mobile payment services in a mobile device

6.2 From mobile device to Secured Server

Possible combinations of the mobile wallet components introduced above may result in a large variety of technical implementations which are further impacted by the location of these components (mobile device or Secured Server or a combination thereof).

One of the main challenges when performing a payment transaction is the access to the mobile payment service chosen by the consumer/payer especially when several mobile wallets are accessible and hosted either on the mobile device or in a Secured Server.

Different situations may appear:

- A unique umbrella UI may be shared by different mobile wallets;
- Dedicated umbrella UIs to mobile wallets may coexist on the mobile device;
- Mobile payment services may be directly accessible via their dedicated payment component UI hosted on the mobile device.

A few detailed examples of combinations of mobile wallet components for mobile payments are provided for illustrative purposes in Annex 3.

6.3 Mobile wallet passcode

When a consumer/payer wants to access a service via his/her mobile wallet such as the selection of a mobile payment instrument, he/she needs to open the mobile wallet via a user interface (for example the umbrella UI of the mobile wallet). This may require the entry of a mobile wallet passcode.

The verification of this mobile wallet passcode follows the same security recommendations as those applicable for payment components and therefore requires a secure environment.

The mobile wallet passcode is an optional[19] feature. It may enhance the security for accessing mobile payments instruments. Its usage is strongly recommended for the life cycle management of the mobile wallet (e.g., loading new mobile services). However its usage poses some challenges on the consumer/payer who has to remember an additional "secret" in addition to his/her mobile code and on-line passcode if required by the payment transaction.

6.4 Interfaces related to mobile payment

6.4.1 Introduction

A mobile wallet has a number of different interfaces[20] to:

- The payer and his/her mobile device;
- The beneficiary and his/her PSP's infrastructure (POI, payment gateway …);
- The mobile wallet issuer;
- The mobile payment/authentication application(s) and/or sets of credentials;

The mobile wallet could cover a variety of mobile payment instruments including both contactless and remote payments in the Customer-to-Business (C2B) and Consumer-to-Consumer (C2C) areas (see [1]).

The next sections provide some insight into these interfaces. However, since for mobile contactless transactions, a mobile wallet hosted on a Secured Server is unlikely, only the mobile wallet located on the mobile device is addressed in the current version of this document.

Even if the convenience for customers and the ease of use for mobile services are important for the market take up of mobile wallets, the creation of the envisaged interfaces should not impact the security of the payment services supported.

6.4.2 Mobile payment/authentication application(s) and/or sets of credentials

When mobile payment/authentication application(s) and/or sets of credentials are accessed through a mobile wallet but reside outside the mobile wallet, a variety of interfaces exists, depending on the configuration/implementation.

[19] The usage of a mobile wallet passcode is also related to the requirements for a TEE as specified by Global Platform (see [4]).

[20] Only interfaces impacted by the mobile wallet are considered. This means that interfaces involved in the processing of mobile payments between payer's/consumer's and beneficiary's/merchant's PSPs are out of scope.

For mobile contactless (proximity) C2B transactions with a mobile wallet hosted on the mobile device, the wallet directly interfaces with the payer via the umbrella UI and with a POI (e.g., via NFC, QR code, other 2D barcode such as Data Matrix, …) as depicted in Figure 9.

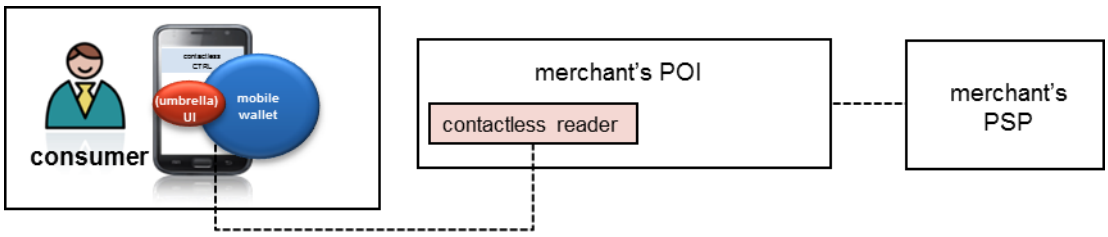

Figure 9: Interfaces - Face-to face C2B scenario

For mobile remote C2B payments, a merchant's website typically includes the following components as represented in Figure 10 below:

- The "shopping" pages;
- The checkout page, where the consumer/payer selects the payment method (e.g., through a logo or brand name) and provides the necessary information for delivery of the goods or services.
- The payment page where the consumer/payer provides the relevant mobile payment related data; this page is linked to or managed by a payment gateway. The payment page is often referred to as a "virtual POI". Note that the virtual POI may be residing on the merchant's website or in the payment gateway.

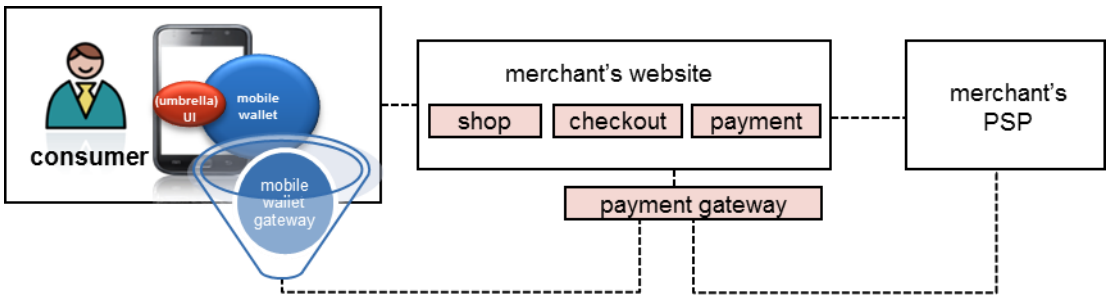

Figure 10: Interfaces - Remote C2B scenario

Depending on the location of the mobile wallet the following cases may be distinguished:

- If located on the mobile device, it directly interfaces with the consumer/payer via the umbrella UI, and with a virtual POI via a mobile wallet gateway which ensures the link with a payment gateway;
- If located on a Secured Server, both the consumer/payer and the virtual POI communicate with the mobile wallet via the mobile wallet gateway.

For remote C2C mobile payments (see Figure 11), the mobile wallet directly interfaces with the payer via the umbrella UI. Note that a common infrastructure might be needed for the retrieval of the identification details of the beneficiary from an alias populated via the mobile wallet (see [1]).

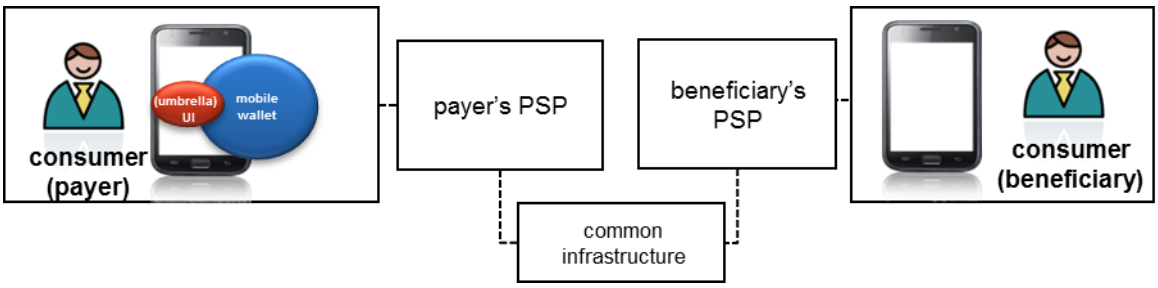

Figure 11: Interfaces - Remote C2C scenario

6.4.3 Mobile wallet issuer

Different interfaces may be considered between the mobile wallet and its issuer which are implementation dependent:

- If located remotely, a mobile wallet is typically hosted on a Secured Server and there may be a variety of interfaces depending on the implementation (e.g., web interface).
- If located on the mobile device, the interfaces are similar to those existing between mobile payment/authentication applications and their issuers. This means that several options are available to install the mobile wallet on the mobile device such as:
    - For the payment component: remotely via OTA using for example a data channel with a possible involvement of a TSM or preloaded by the manufacturer before the supply of the mobile device;
    - For the UI components (payment UI and/or umbrella UI): preloaded by the manufacturer or downloaded from the relevant application store.

These interfaces are not only used for the initial deployment of the mobile wallet components but also for its lifecycle management such as maintenance purposes and possible blocking in case of compromise of the mobile wallet or of its services.

6.4.4 Payment gateway

A payment gateway is a service operated under the control of a beneficiary's PSP (e.g., by a TTP) that manages the payments for merchants. It facilitates for remote mobile payments the transfer of information between the (virtual) POI (such as a website or apps on a mobile device) and the beneficiary's PSP. The communication between the consumer/payer's browser/mobile app and the payment gateway for remote payments is always protected using a secure protocol such as https.

6.4.5 Mobile wallet gateway

A mobile wallet gateway is a service operated by the mobile wallet issuer or a TTP acting on its behalf that establishes:

- For mobile remote payments a link between the consumer/payer and its mobile wallet and between the mobile wallet and the payment gateways used for the mobile payment transaction(s);
- For life cycle management a link between the mobile wallet and the mobile wallet issuer.

It enables:

- The triggering of the mobile wallet to open;
- The automatic transmission of data between the mobile wallet and the payment gateway in a payment transaction.
- A link between the mobile wallet and the mobile wallet issuer to download credentials, payment and/or authentication applications from the PSP, typically subject to mobile wallet passcode presentation and verification.

6.4.6 Umbrella UI

An umbrella UI is a unified payer's interface to the different payment components UIs; it acts as an aggregator of different payment means in a mobile wallet.

The umbrella UI resides on the mobile device and ensures:

- A unified access to the payment means whether residing in the mobile device or in a Secured Server;
- The management of the payment means such as priority settings, default, deletion, addition…

This component is under the responsibility of the mobile wallet issuer.

6.4.7 Interfaces and the mobile wallet ecosystem

The various interfaces allow the mobile wallet stakeholders to influence the mobile wallet ecosystem. A dedicated study has been undertaken by Mobey Forum to describe the potential roles of the different stakeholders through the introduction of so-called *"mobile wallet control points"* [8]. These control points enable mobile wallet stakeholders, via the appropriate interfaces, to take part in the development, maintenance and delivery of technology to consumers.

7 Life cycle management

As described in section 6.1, a mobile wallet to support mobile payments may be viewed as a combination of the following three components:

- The payment component itself, which can be a dedicated payment/authentication application or credentials;
- The payment User Interface (UI) component, which may be a mobile payment/authentication application UI or a credentials manager UI;
- The umbrella UI component.

As described in section 5.4, the mobile wallet is always accessed via the mobile device, but some components may be located remotely on a Secured Server. Each component has its own life cycle management. Dedicated processes for the stakeholders involved need to be defined for this life cycle management, including the provisioning, of these components. These processes may vary depending on the location of these components. The mobile wallet components located in the mobile device need to be preinstalled or downloaded, while the components outside the mobile device need to be installed on a server. But in any case this should always be managed by the mobile wallet issuer. For some processes, a TTP (such as a TSM) may be involved.

As indicated in section 6, the life cycle management of the mobile wallet typically requires the entry of a mobile wallet passcode.

7.1 Mobile payment/authentication applications or credentials

A mobile payment/authentication application may be preinstalled or the consumer/payer may trigger the installation of a mobile payment/authentication application from a variety of sources, such as PSPs (e.g., via the PSP's website, an ATM …), application stores offered by other service providers or mobile wallet issuers.

An example of the installation of a mobile payment/authentication application from a PSP, assuming that an SE is involved for the hosting of a mobile payment/authentication application, may be found in the "MCP Interoperability Implementation Guidelines" document (see section 5 in [2]).

Credentials stored in a mobile wallet (application) are provided by the PSPs but may be managed (installed, updated or deleted) by the consumer/payer.

7.2 Mobile payment/authentication application UI and credentials manager UI

A mobile payment/authentication application UI may be preinstalled by, or downloaded from, the mobile application issuer or a TTP.

A credentials manager UI is typically preinstalled by, or downloaded from, the mobile wallet issuer.

The management of the mobile payment/authentication application UI and the credentials manager UI should include at a minimum the following functions:

- Update: there may be a need for an update of the UI;

- De-installation: a consumer/payer may want to remove a UI from his/her mobile wallet in which case all credentials/mobile applications are removed.

7.3 Umbrella UI

An umbrella UI is typically preinstalled by, or downloaded from, the mobile wallet issuer.

The management of the umbrella UI should include at a minimum the following functions:

- Update: there may be a need for an update of the umbrella UI;
- De-installation: a consumer/payer may want to remove an umbrella UI from his/her mobile wallet.

8 Standardisation and industry bodies

An open approach for mobile wallets requires consistency in specifications and guidelines defined by multiple standardisation and industry bodies.

At the time of publication, the most relevant bodies directly involved with mobile wallets are:

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

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

The work executed by the following bodies may indirectly influence the mobile wallet payments ecosystem:

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

- **GlobalPlatform**
  GlobalPlatform is a cross industry, non-profit association which identifies, develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology. Its proven technical specifications, which focus on the secure element (SE), trusted execution environment (TEE) and system messaging provide the tools that are regarded as the international industry standard for building a trusted end-to-end solution which serves multiple actors and supports several business models. (http://www.globalplatform.org/)

Note that other industry bodies might be indirectly involved with mobile wallets such as CSG [3] and PCI[21] for mobile card payments.

New bodies might become relevant in the future and will be added as appropriate in new releases of this document.

[21] Payment Card Industry Security Standards Council

9 Closing considerations

This white paper aims to provide an introduction to the concept of a mobile wallet as a facilitator for mobile payments next to other mobile services. A mobile wallet clearly offers the potential to bring convenience to the consumer/payer for the initiation and authentication for mobile payments while it allows the beneficiaries/merchants to enhance their offerings. Today, mobile wallets are in their early stages of development. However its potential success will very strongly depend on its value proposition to the consumers. No one in the payment ecosystem knows how exactly the mobile wallet marketplace will evolve in the coming years. But the offering of additional mobile services (such as ticketing, loyalty, couponing, etc.) next to financial services appears to be important drivers for the value proposition. Consumers need to be motivated to try mobile wallets so that they get convinced that it is secure[22] and ubiquitous.

However, to enable a cost-effective approach for stakeholders involved in the mobile wallet payments ecosystem, a number of key challenges remain to be addressed in the future regarding this topic:

- Harmonisation of user interfaces to enable a consistent user experience (easy to use, intuitive, etc...);
- Co-existence of payment with other mobile services in a mobile wallet;
- Co-existence of multiple mobile wallets on or accessed through a single mobile device;
- Linkage of mobile wallets in the payer's space with merchant wallets;
- Interoperability of mobile wallet interfaces;
- Execution of proximity payments with remote mobile wallets;
- Alignment of mobile wallet security aspects (including authentication) with existing and forthcoming requirements for mobile payments[23] related to mobile wallet interfaces and infrastructure;
- Coordination amongst various industry initiatives on mobile wallets.

The EPC encourages an open dialogue and a collaboration of all relevant stakeholders to combine efforts so that these issues are addressed adequately while contributing to the success of mobile (payment) services through mobile wallets.

[22] New threats on mobile devices (e.g., mobile malware) are factors which might impact mobile wallets.

[23] See for example the SecuRe Pay *"Recommendation for the security of internet payments" and the draft* SecuRe Pay *"Recommendation for the security of mobile payments"* published by the European Central Bank.

10 Annex 1: SEPA Payment Instruments

The payment instruments promoted by the EPC are:

- **SEPA Credit Transfer (SCT)**

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

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

- **SEPA Direct Debit (SDD)**

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

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

- **SEPA Cards Framework (SCF)**

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

Further information on the SEPA payment instruments may be obtained from the EPC website (http://www.europeanpaymentscouncil.eu).

11 Annex 2: Detailed description of mobile wallet payment use-cases

Different mobile payment use-cases involving a mobile wallet exist covering both contactless and remote payments. The following three use-cases based on SEPA payment instruments are described in this annex to illustrate the usage of a mobile wallet.

- Consumer-to-Business Mobile Contactless (SEPA) Card Payment;
- Consumer-to-Business Mobile Remote (SEPA) Card Payment;
- Consumer-to-Consumer Mobile Remote (SEPA) Credit Transfer.

11.1 Consumer-to-Business Mobile Contactless (SEPA) Card Payment

In this scenario, the consumer uses a mobile wallet accessed via his/her mobile device to conduct a contactless card payment to a merchant which is providing goods or services (e.g., mobile content) It is based on the MCP 1 use-case described in section 4.2 in [1]. Note that in this scenario, the mobile wallet passcode is being used to enable access to the MCP application through the mobile wallet - in most cases, this is an optional feature offered to the consumer.

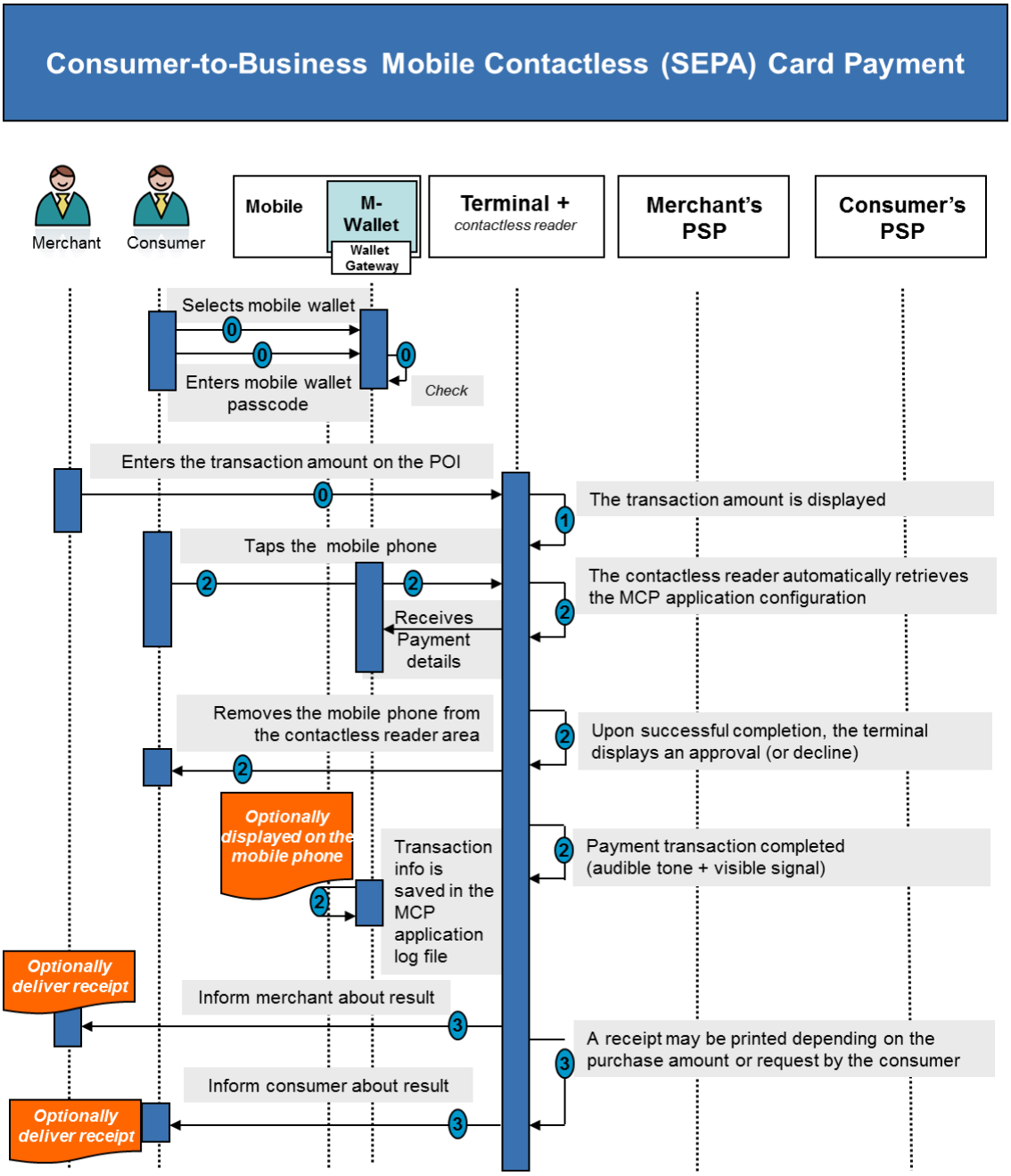

Figure 12: C2B Mobile Contactless (SEPA) Card Payment

Step 0 (Pre-requisite)

- The consumer selects his/her mobile wallet and enters his/her mobile wallet passcode to enable access to the MCP application before starting the transaction.
- The merchant enters the transaction amount on the POI terminal.

Step 1

- The transaction amount is displayed on the merchant's POI terminal.
- The POI selects the contactless technology and requests for a card payment.

Step 2

- The consumer taps his/her mobile phone on the contactless reader area. (The consumer holds his/her mobile phone close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI selects the MCP application.
- An audible tone and/or visible signal indicate that the mobile phone – contactless reader interaction is completed. After this, the mobile phone can be removed from the contactless reader area.
- An off-line MCP application authentication/authorisation is performed by the POI.
- After processing the off-line authorisation, the merchant's POI terminal displays an approval or decline.
- Information about the transaction (e.g., transaction amount) is saved in the MCP application log file and optionally displayed on the mobile phone.

Step 3

- The merchant is informed about the result of the transaction.
- The consumer is informed by the merchant about the result of the transaction.
- Depending on the purchase amount, the merchant's POI terminal features and consumer choice, a transaction receipt may be printed.

11.2 Consumer-to-Business Mobile Remote (SEPA) Card Payment

In this scenario, the consumer uses a mobile wallet accessed via his/her mobile device to conduct a payment to a merchant, which is providing goods or services (e.g., mobile content). Note that a "strong authentication method" is used in this scenario. This scenario is inspired by the MRCP 3 use case described in section 5.2.3 in [1].

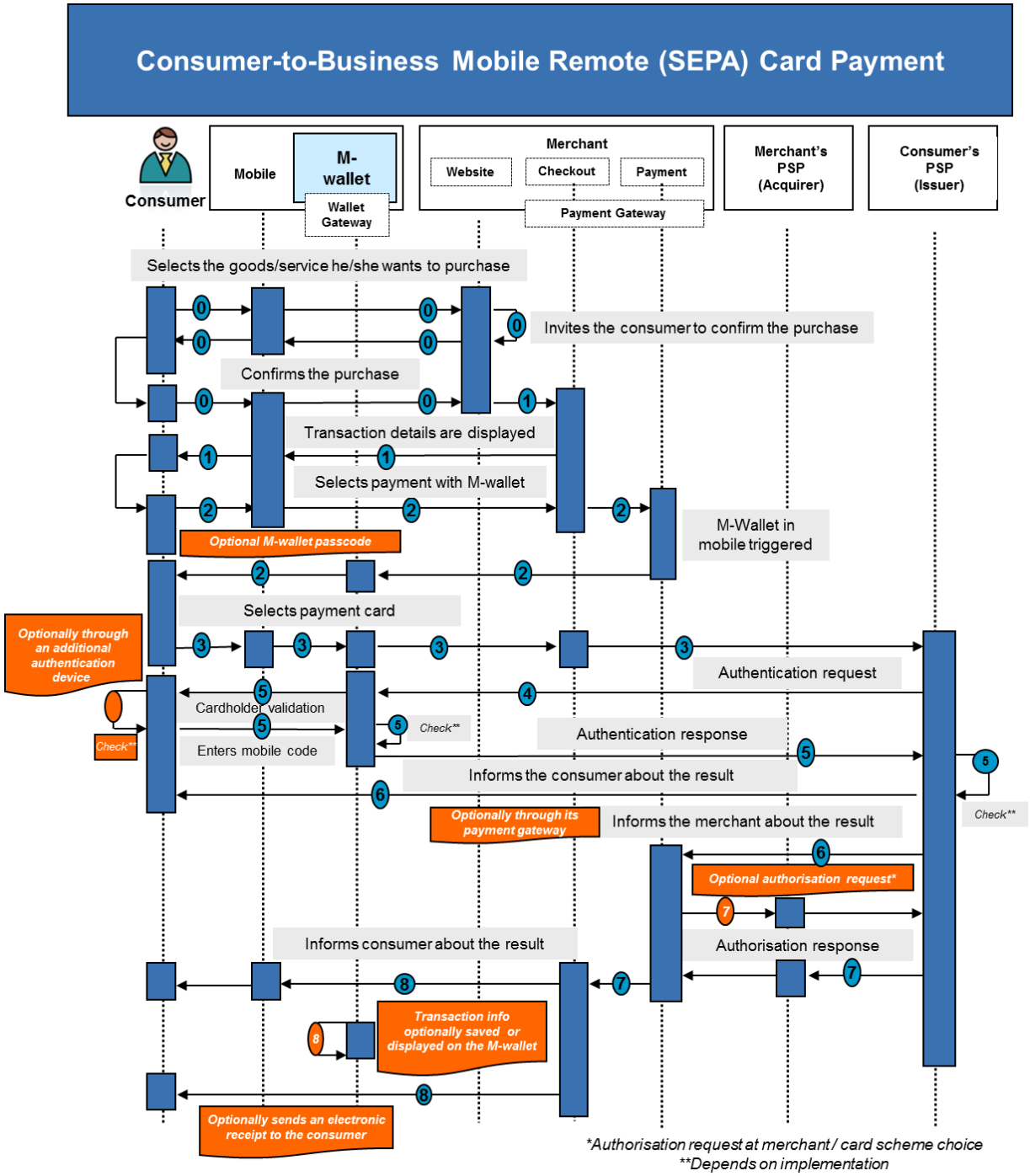

Figure 13: C2B Mobile Remote SEPA Card Payment transaction

In the figure above, the following steps are illustrated:

Step 0 (Pre-requisite)
The consumer navigates using his/her mobile device to a merchant website via mobile internet and selects the goods/service he/she wants to purchase.

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

Step 1 (Transaction details displayed)
The checkout section of the merchant website displays the transaction details including the amount and the payment options, via the browser of the mobile device, to the consumer.

Step 2 (Payment method selection)
The consumer selects the payment method (card (a) or mobile wallet (b)) on the merchant's website.

(a) In the case of the selection of a payment card, the consumer needs to open the mobile wallet him/herself via the mobile device;

(b) In the case of the selection of mobile wallet, the mobile wallet will be triggered to open via the mobile wallet gateway.

Step 3 (Payment card selection)
The consumer selects the payment card via the user interface of the mobile wallet.

Step 4 (Card details validation)
The payment gateway receives the selected card details in one of the following ways, depending on the payment method selected:

- via the mobile device (a);

or

- self-populated via the mobile wallet gateway (b);

and displays them to the consumer via the mobile device.

The consumer subsequently validates the card details with a visual check.

Step 5 (Transaction confirmation with authentication)

The consumer and the relevant data are subsequently authenticated[24] towards his/her PSP according to one of the following typical processes:

- In the case of a payment card via mobile internet, the consumer and the relevant data are authenticated by its PSP via a strong authentication method. Various methods may exist involving the usage of an additional authentication device. The consumer inserts his/her payment card into the additional device; the consumer's PSP provides the consumer with a "challenge" to be entered/transmitted (on)to the additional device, followed by the

[24] This authentication may involve transaction details.

consumer's PIN entry. The authentication device then generates a "response" which the consumer is requested to enter at a given time during this process on his/her mobile device. The response is subsequently transmitted to the consumer's PSP via the authentication response for verification.[25]

- In the case where an authentication application is present on the mobile device, a dynamic authentication method (e.g., challenge/response method) is initiated by the consumer's PSP and is handled automatically by the authentication application in a secure environment. The consumer is requested to enter his/her mobile code[26] (CVM) only once during the MRCP transaction process. The mobile code is checked either locally (off-line CVM) by the authentication application, or by the consumer's PSP (on-line CVM).

The presence of a mobile wallet does not affect the strong authentication process.

Step 6 (Payment process)
The consumer is informed by his/her PSP about the result of the authentication.

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

Subject to successful authentication by the consumer's PSP, the payment is further processed as a remote transaction. This may involve[27] an on-line authorisation request by the merchant to the consumer's PSP.

Step 7 (Transaction finalisation)
Once the payment is authorised,

- The merchant releases the good/service to the consumer.
- The consumer is automatically redirected to the merchant website and receives a confirmation of the transaction;

Step 8 (Transaction information)
Transaction information (such as the transaction amount) may be saved in an MRCP application log file/mobile wallet and/or optionally displayed on the mobile device.

An electronic receipt may be sent by the merchant to the consumer, possibly via the mobile device.

[25] The authentication process is very similar to the one used in a remote card payment.
[26] The usage of the mobile code in combination with the dynamic authentication effectively results into a strong authentication.
[27] In particular cases, authorisation request could be optional, depending on the type of payment card and the merchant's decision. But, in any case, the capability to do an authorisation request must be there.

11.3 Consumer-to-Consumer Mobile Remote (SEPA) Credit Transfer

In this scenario, the consumer (payer) uses a mobile wallet accessed via his/her mobile device to conduct a payment from his/her own payment account to the payment account of another consumer (beneficiary). It is based on the MRCT 2 use case described in section 5.3.2 in [1]. Hereby it is assumed that the beneficiary's alias (e.g., beneficiary mobile phone number) will be used, making the input of the beneficiary details considerably more convenient for the payer. This means that the beneficiary would need to "register" his/her identification details against his/her alias and the payer's PSP would need to facilitate the use of aliases in its mobile SCT instruction acceptance process. Moreover, the payer's PSP would need to be able to identify the beneficiary's PSP and payment account details from the beneficiary's alias e.g., via a "Common Infrastructure" (see section 5.5.3.3 in [1]) as illustrated in the example below.

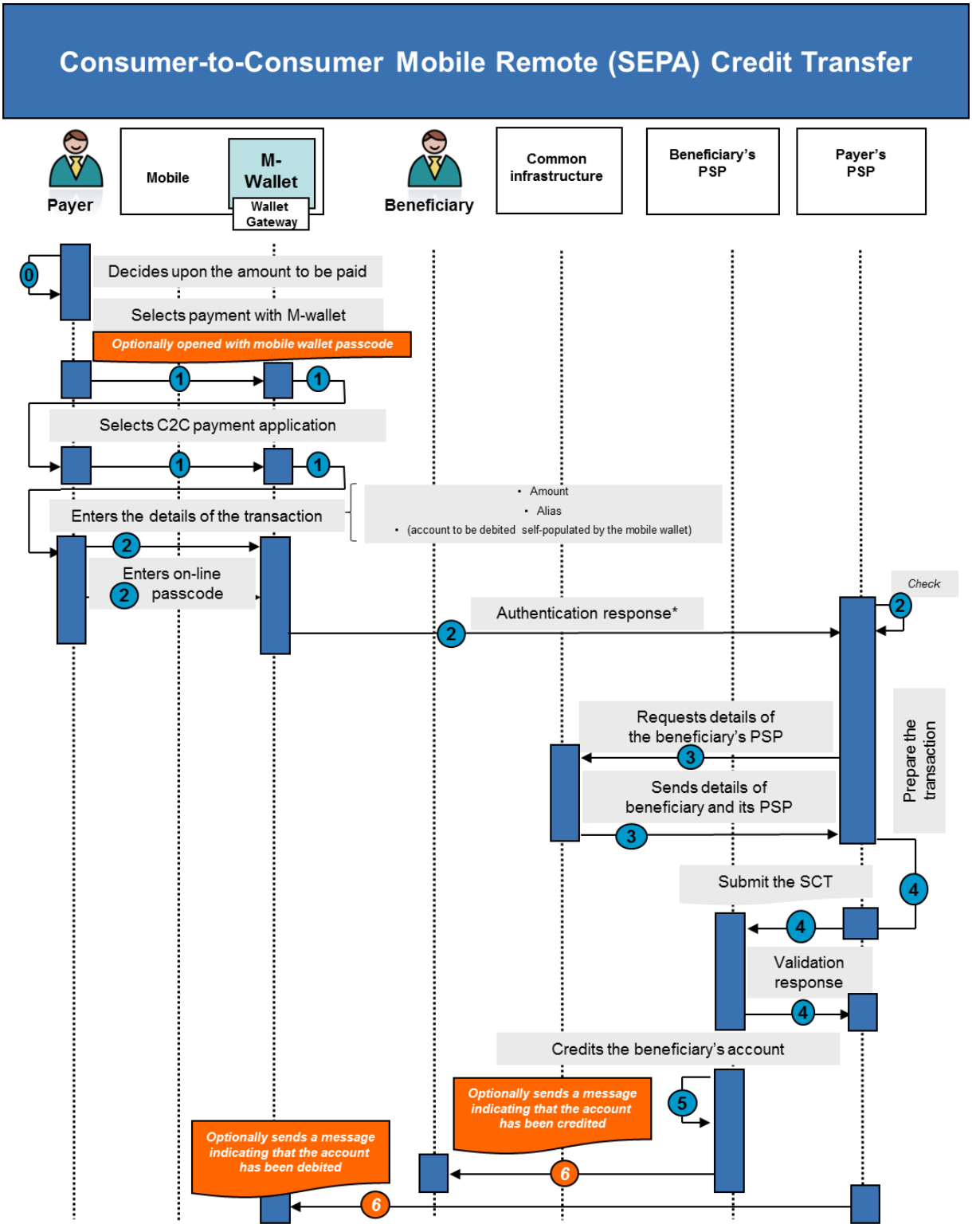

Figure 14: C2C Mobile Remote (SEPA) Credit Transfer

In the figure above, the following steps are illustrated:

Step 0 (Pre-requisite)
The payer decides upon an amount to be paid to a beneficiary.

Step 1 (C2C payment selection)

The payer selects the mobile wallet he/she wishes to use[28]. The payer is then redirected to the user interface of the mobile wallet to select the C2C payment application and the credentials (IBAN) he/she wants to use in the case where there are several eligible payment accounts;

Step 2 (Transaction details entry)
Once the C2C payment application is selected, the payer enters[29] the details of the transaction (amount, alias of the beneficiary) and confirms the transaction by entering the on-line passcode. These banking credentials are checked and the response is transferred on-line for verification to the payer's PSP.

Step 3 (Retrieve payment details and PSP of the beneficiary)
Next, the alias of the beneficiary is sent to a "common infrastructure" by the payer's PSP. The main purpose of this common infrastructure is to link the alias of the beneficiary to the payment information details of the beneficiary including his/her PSP in order to allow the appropriate routing of the payment transaction.

Step 4 (Payment process)
The payer's PSP initiates an SCT transaction.

Step 5 (Transaction finalisation)
The beneficiary's PSP credits the beneficiary's account with the transaction amount.

Step 6 (Transaction information)
The beneficiary optionally receives a message from his/her PSP that his/her account has been credited.

The payer optionally receives a message possibly on his/her mobile wallet from his/her PSP informing that his/her account has been debited.

[28] The "opening" of the mobile wallet may require a mobile wallet passcode entered by the payer via the mobile device.
[29] The payer can enter the details of the transaction either locally or remotely; in the latter case, the payer is directly connected via mobile internet to a dedicated server of his/her PSP.

12 Annex 3: Detailed examples of combinations of mobile wallet components

Possible combinations of the mobile wallet components introduced in section 6.2 may result in a large variety of technical implementations which are further impacted by the location of these components (mobile device or Secured Server or a combination thereof).

This annex provides five detailed examples of combinations of mobile wallet components for illustrative purposes:

- A first example in Figure 15 shows a common umbrella UI which is shared by different mobile wallets;
- A second example depicted in Figure 16 illustrates the case whereby each mobile wallet in a mobile device has its own umbrella UI;
- A third configuration in Figure 17 presents a mobile payment/authentication application within a mobile wallet which may be accessed either through the umbrella UI or outside the mobile wallet directly via the mobile payment/authentication application UI;
- Figure 18 provides an example where part of the mobile wallet is hosted on a Secured Server and accessed through an umbrella UI located on the mobile device.
- Finally Figure 19 represents a more complex example with two mobile wallets managed through a common umbrella UI, one mobile wallet is located on the mobile device and one is remotely hosted on a Secured Server.

Note that in the following detailed examples, a unique mobile payment/authentication application UI may be shared by multiple mobile payment/authentication applications. Moreover, the examples provided are not exhaustive, other combinations are possible.

Figure 15 shows two different mobile wallets for mobile payment services hosted in a mobile device. Each mobile wallet contains mobile payment/authentication applications possibly from different PSPs. The mobile wallets may be accessed via a common umbrella UI, provided by a Third Party.

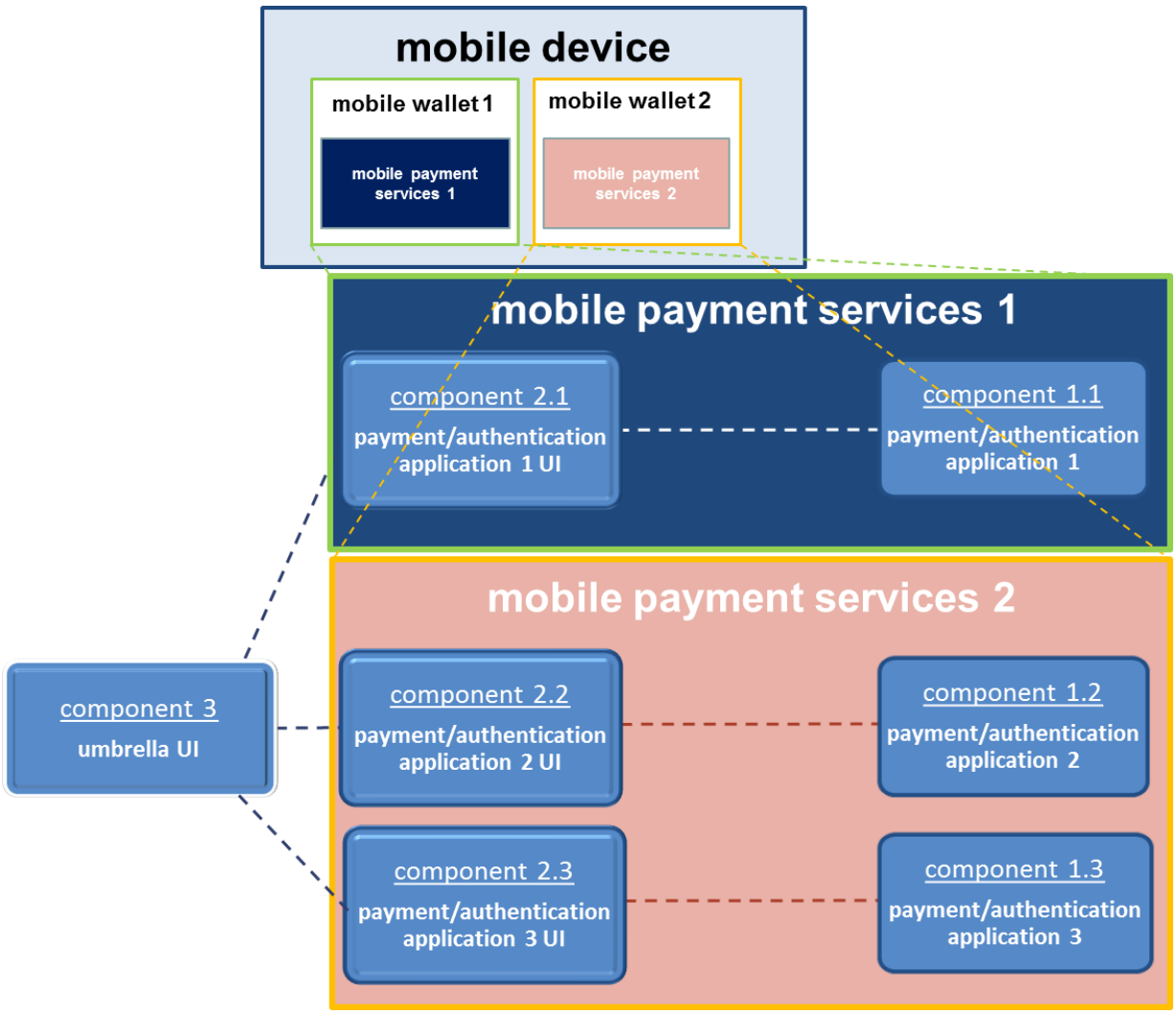

Figure 15: Example with two mobile wallets in a mobile device managed through a common umbrella UI

Figure 16 shows the case where each mobile wallet has its own umbrella UI.

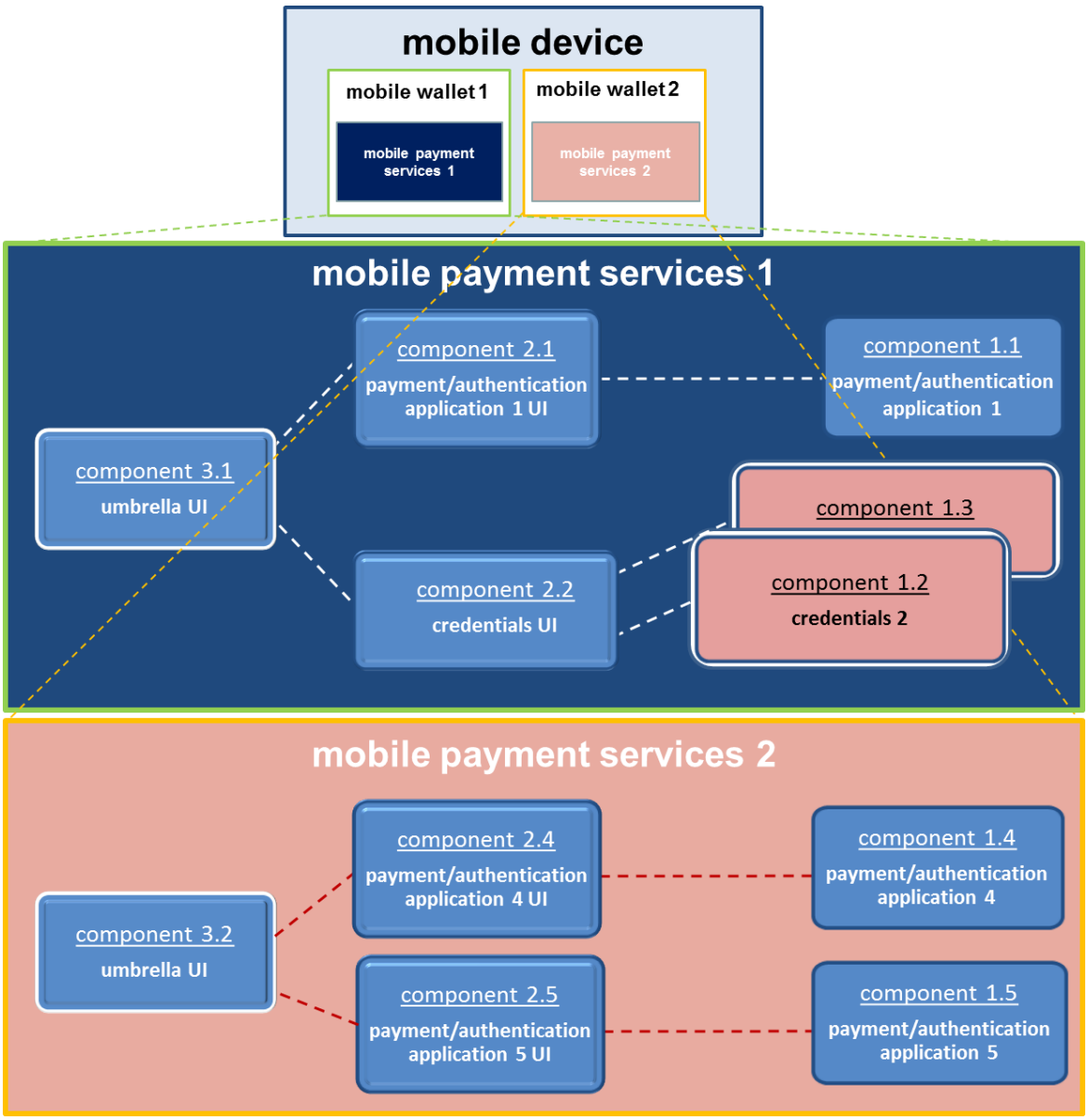

Figure 16: Example with two mobile wallets on a mobile device managed through their own umbrella UI

Figure 17 illustrates that, although a mobile payment service is accessed via a mobile wallet, it may remain directly accessible via a mobile payment UI hosted on the mobile device.

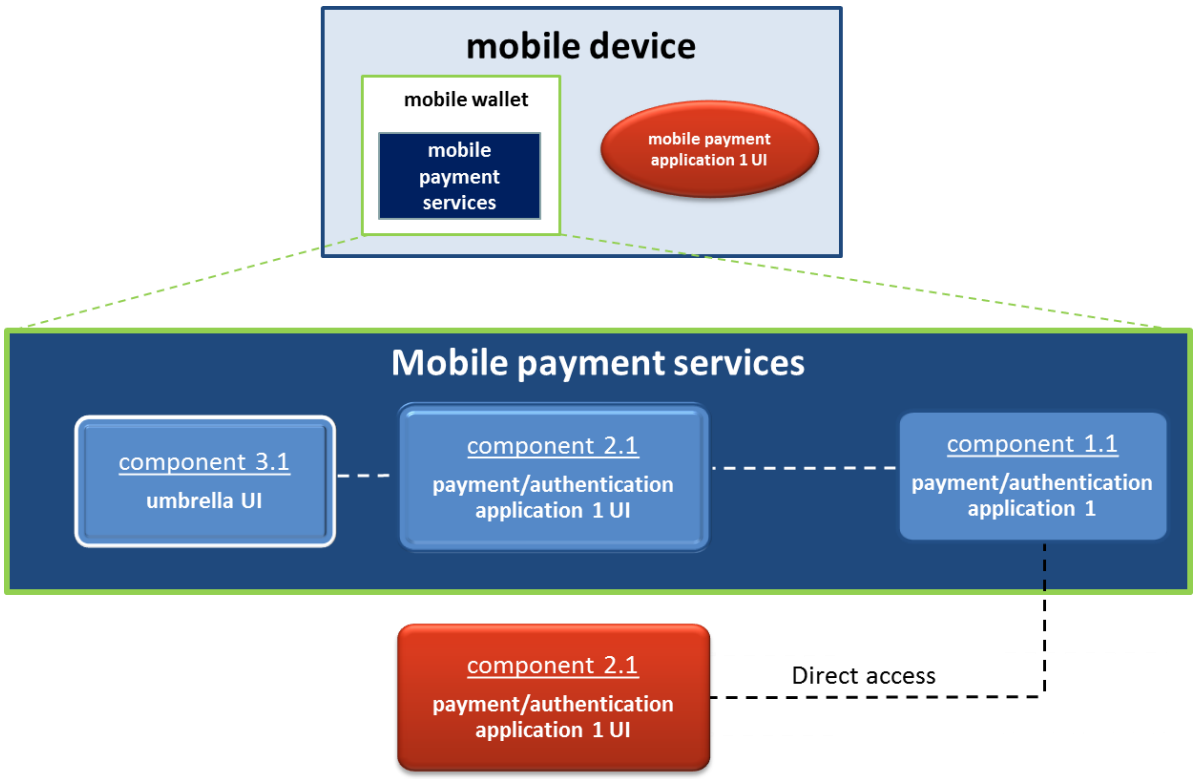

Figure 17: Example of a mobile payment service accessed via a mobile wallet or directly via a UI hosted on the mobile device

Figure 18 shows an example whereby part of the mobile wallet is hosted on a Secured Server. Mobile payment/authentication application 1 hosted on the Secured Server (component 1.1) is accessed via the mobile device through the umbrella UI.

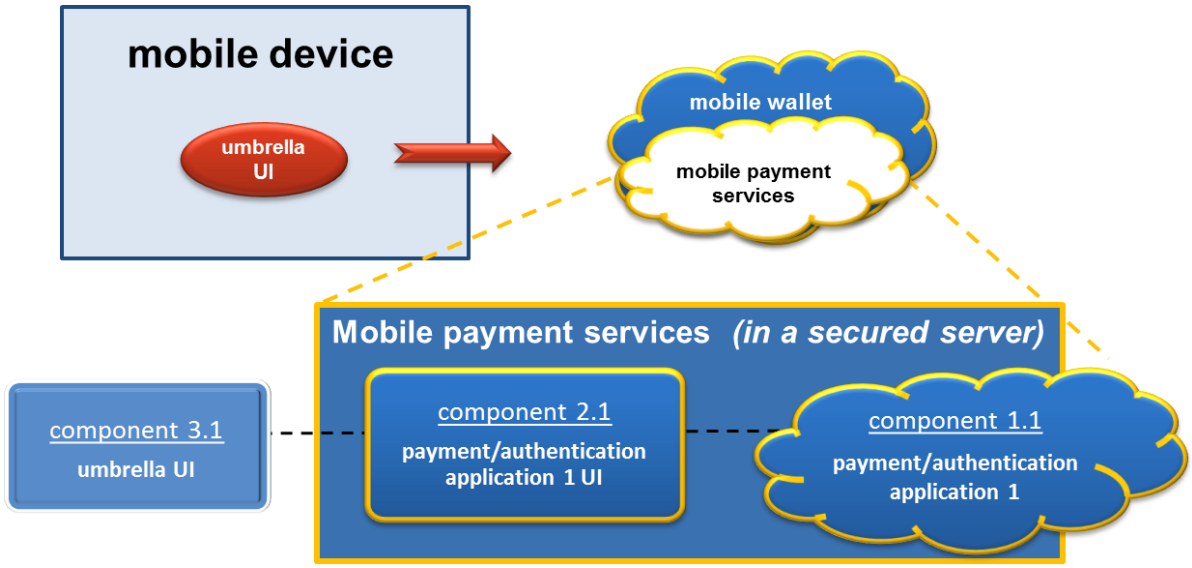

Figure 18: Example of a mobile wallet hosted on a Secured Server

Figure 19 shows a more complex example whereby two mobile wallets for mobile payment services, one on the mobile device and one on a Secured Server, are managed through a common umbrella UI.

The mobile wallet on the mobile device manages two different mobile payment/authentication applications and two sets of credentials, from different PSPs. Note that the credentials UI may manage different credentials issued by different PSPs. The umbrella UI on the mobile device also provides access to the mobile payment/authentication application 5 hosted on the Secured Server (component 1.5).

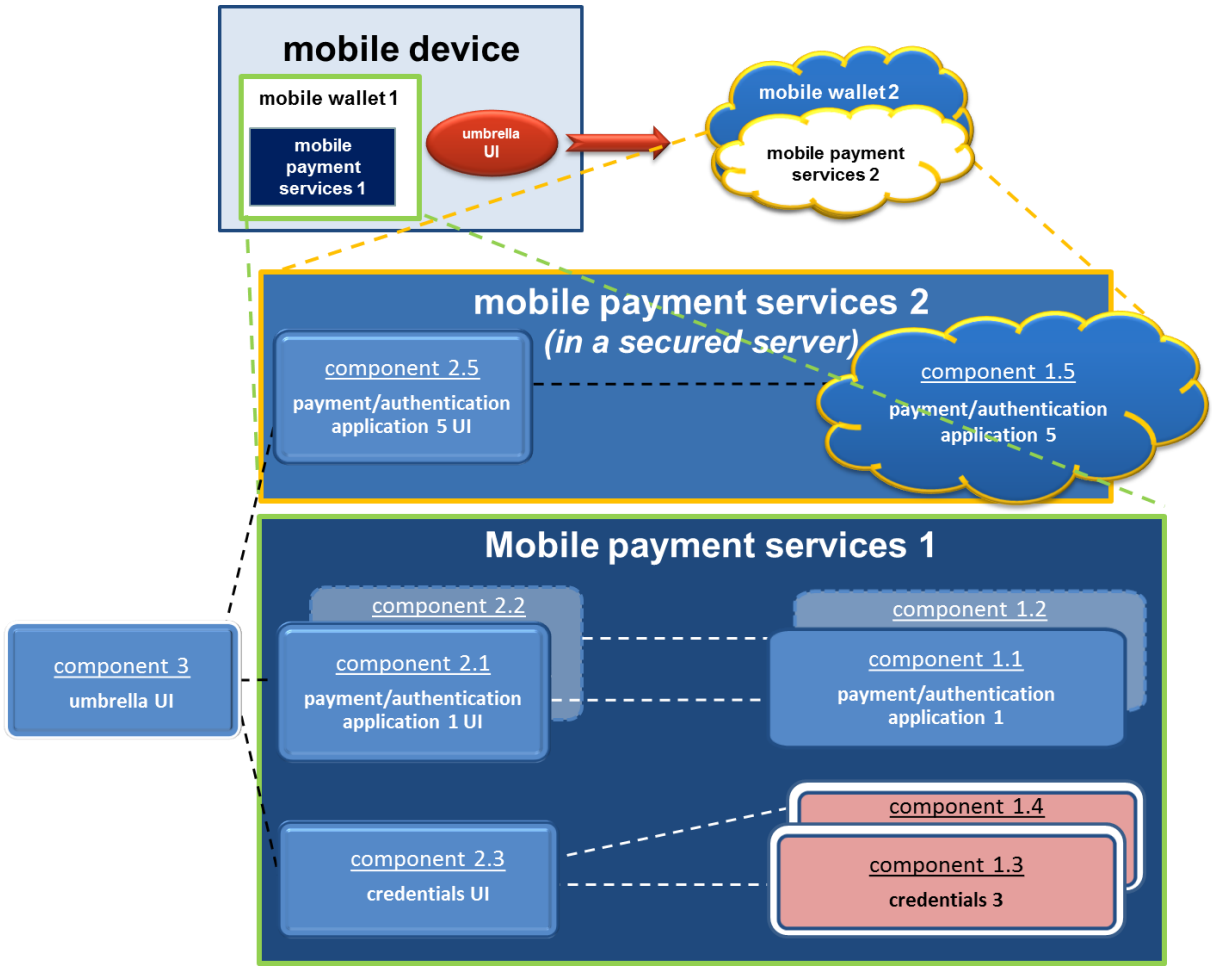

Figure 19: Example with two mobile wallets managed through a common umbrella UI, one on the mobile device and one on a Secured Server

End of Document