WHITE PAPER
Non-NFC based Mobile SEPA Card Proximity Payments

EPC109-19 / Version 1.0 / Date of publication: 7 June 2019

WHITE PAPER

Non-NFC based Mobile SEPA Card Proximity Payments

EPC109-19
2019 Version 1.0
Date issued: 7 June 2019
Reason for issue: Publication on EPC website

Abstract

This document provides insights into non-NFC based Mobile SEPA Card Proximity Payments (MCPPs).

Table of Contents

List of tables

List of figures

Executive Summary

Mobile devices have achieved full market penetration and rich service levels in most, if not all, EU Member States, making the mobile channel ideal for leveraging and promoting the use of SEPA payment instruments.

In 2017, the EPC facilitated the setting-up of a multi-stakeholder group covering the various sectors involved in the mobile payment ecosystem. The group developed a new version of the interoperability implementation guidelines for mobile contactless card based payments (MCPs) based on NFC-technology, covering business, technical, security and legal aspects, which was published in July 2018 (see [12]).

In recent years, non-NFC proximity technologies (e.g. QR-codes, BLE) have been introduced in the market for various mobile payment services to enhance the consumer experience and to bring additional functionality and services to the customer (e.g. integration of payment with loyalty) and to overcome the lack of accessibility to the NFC antenna on some mobile operating systems.

However, in comparison to MCPs, the European market is currently much less mature with respect to the usage of these non-NFC based technologies for mobile payments. Also, standardisation efforts aiming at interoperability of these solutions are in their early days.

In order to create awareness on these mobile card payment solutions, the same multi-stakeholder group (see Annex B), agreed to develop a white paper to provide a high level overview of non-NFC based mobile card proximity payments (MCPPs), utilising SEPA cards (as specified in the Cards Standardisation Volume - see [5]) as the underlying payment instrument[1]. In view of the current market deployments, the document has been restricted to proximity payments based on QR-codes and Bluetooth-Low-Energy (BLE) technologies (see section 2.3). Note that although many QR-code solutions for non-card based mobile payment instruments already exist in the market today (such as SEPA Credit Transfer, Direct Debit or e-money based), they are out of scope of the current document, since other multi-stakeholder groups are covering these payments[2].

In addition to use cases, the document provides some insights into transaction characteristics and impacts on the POIs.

While producing this document, the multi-stakeholder group noticed some opportunities but also a number of gaps and challenges that are existing today and, if properly addressed, could encourage the market take-up of MCPPs (see chapter 6).

Therefore, the multi-stakeholder group wishes to promote the following guidelines:

[1] Note that the use cases and service models introduced in these guidelines may also be applied outside SEPA.

[2] See for instance https://www.europeanpaymentscouncil.eu/what-we-do/other-sepa-payments/sepa-goes-mobile/ad-hoc-multi-stakeholder-group-mobile-initiated and https://www.europeanpaymentscouncil.eu/what-we-do/other-sepa-payments/sepa-goes-mobile/ad-hoc-multi-stakeholder-group-mobile-initiated

- Existing QR-code card-based solutions should consider migrating to the EMVCo specifications (see [8], [9] and [10]) to enhance the interoperability of their solutions;
- New MCPP service providers should base their QR-code based developments on the EMVCo specifications (see [8], [9] and [10]);
- Standardisation and industry bodies should further analyse the usage of the BLE technology for card payments and develop the appropriate technical standards and implementation guidelines to contribute to an enhanced, secure and harmonised customer payment experience.

Moreover, to achieve full interoperability in an open model with merchant-presented QR-codes, the relevant market participants are encouraged to work together to develop a common standard for the implementation of these payments.

0 Document Information

0.1 Structure of the document

This document contains a number of chapters and annexes, as follows:

- Chapter 1 provides the vision on Mobile Card–based Proximity Payments (MCPPs) related to the SEPA card payment instrument as well as the scope and the objectives of this document.
- Chapter 2 provides a short overview of MCPPs and includes a detailed description of some MCPP use cases.
- Chapter 3 is devoted to different characteristics of the MCPP transaction itself such as authentication, authorisation, cardholder verification and risk management.
- Chapter 4 provides some insights into POI characteristics.
- Chapter 5 includes a short description of standardisation and industry bodies that develop specifications, guidelines and white papers related to MCPPs.
- Chapter 6 identifies some challenges and opportunities for the deployment of MCPPs.
- Overall conclusions on MCPPs are made in chapter 7.
- Annex A provides an overview of the relevant regulatory documents.
- Annex B gives an overview of the different organisations involved in the multi-stakeholder group that developed this document.

0.2 References

This section lists external references mentioned in this document. Square brackets throughout this document are used to reference documents in this list.

Ref	Document title	Developed by
[1]	Guideline for user-friendly payment terminals	Dutch National Forum on the Payment System
[2]	PSD2: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC	EC
[3]	Commission Delegated Regulation (EU) 2018/189 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as 'RTS')	EC
[4]	IF Regulation: Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions	EC
[5]	ECSG 001-17 – SEPA Cards Standardisation Volume v8.0	ECSG

[6]	EMV® Integrated Circuit Card Specifications for Payment Systems	EMVCo
[7]	EMV® Contactless Specifications for Payment Systems, Level 1 Specifications + Books A-D	EMVCo
[8]	EMV® QR code Specification for Payment Systems (EMV QRCPS) - Merchant - Presented Mode	EMVCo
[9]	EMV® QR code Specification for Payment Systems (EMV QRCPS) - Consumer - Presented Mode	EMVCo
[10]	EMV® Merchant-Presented QR Guidance and Examples	EMVCo
[11]	EPC492-09: White paper Mobile Payments	EPC
[12]	EPC144-17: Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines	EPC
[13]	EPC342-08: Guidelines on algorithms usage and key management	EPC
[14]	EPC163-13: White Paper Mobile Wallet Payments	EPC
[15]	ERPB Final report on Mobile and card-based contactless proximity payments	ERPB
[16]	Towards a better payment experience	Eye Association Netherlands
[17]	The Mobile Economy 2017	GSMA
[18]	IEEE 802.15.1: IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN)	IEEE
[19]	ISO/IEC 7812: Identification cards - Identification of issuers	ISO
[20]	ISO 12812: Core banking - Mobile financial services - Parts 1-5	ISO
[21]	ISO 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards – Parts 1-4	ISO
[22]	ISO/IEC 18004: Information technology -- Automatic identification and data capture techniques -- QR-code bar code symbology specification	ISO
[23]	ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems -- Near Field Communication - Interface and Protocol (NFCIP-1).	ISO
[24]	NFC Controller Interface (NCI) Specifications	NFC Forum

Table 1: References

0.3 Definitions

Throughout this document, the following terms are used. Their definitions are based on [2], [5] and [20].

Term	Definition
Acquirer	A PSP contracting with a payee to accept and process card-based payment transactions, which result in a transfer of funds to the payee.
Authentication	The provision of assurance that a claimed characteristic of an entity is correct. The provision of assurance may be given by verifying an identity of a natural or legal person, device or process.
Authenticator	A security factor used in an authentication method such as: • Knowledge, such as a password, PIN or passphrase • Possession, such as a token device or smart card • Inherence, such as a biometrics.
Bluetooth Low Energy (BLE)	A wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications including beacons. Compared to classic Bluetooth, BLE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.
Cardholder	A consumer who has an agreement with an issuer for a mobile card payment service.
Card account	An account held by a PSP which will be used for one or more card services and which is related to a specific cardholder. A card account is identified by card data.
Card data	A data set used to perform a card service that allows the identification of the cardholder and their account.
Card-on-File	A card acceptance technology where the PAN and expiry date have been provided prior to the transaction and stored securely for later use. It is used for Card-Not-Present transactions (see [5]).
Card scheme	A technical and commercial arrangement (often referred to as the "rules") between parties in the card value chain, resulting in a set of functions, procedures, arrangements, rules and devices that enable a cardholder to perform a payment transaction, and/or cash withdrawal or any other card service.
Card services	A process to perform or support financial transactions based on card data.
Card transaction	A transaction used to perform a card service.
Cardholder verification	Function used to verify whether the person using the card application is the legitimate cardholder.
Cardholder Verification Method (CVM)	A method used to perform cardholder verification. Examples include PIN, mobile code.

Consumer	A natural person who, in payment service contracts covered by the PSD2, is acting for purposes other than his or her trade, business or profession [2].
Consumer Device CVM (CDCVM)	A CVM entered by or captured from the consumer on the consumer device, i.e. a mobile device in the context of this document (e.g., mobile code, biometrics).
Contactless (NFC) technology	A radio frequency technology operating at very short ranges so that the user has to perform a voluntary gesture in order that a communication is initiated between two devices by approaching them. It is a (chip) card or mobile payment acceptance technology at a POI device, which is based on ISO/IEC 14443 (see [21]).
Customer	A payer or a beneficiary which may be either be a consumer or a business (merchant).
Credential(s)	Payment account related data that may include a code (e.g., mobile code), provided by the PSP to their customer for identification/authentication purposes.
2D barcode	A two dimensional barcode is a machine-readable optical label that contains digital information. They are also referred to as matrix barcodes. Examples include QR-codes and tag barcodes.
Digital wallet	A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
Dynamic authentication	An authentication method that uses cryptography or other techniques to create a one-per-transaction random authenticator (a so-called “dynamic authenticator”).
EMVCo	An LLC formed in 1999 by Europay International, MasterCard International and Visa International to enhance the EMV Integrated Circuit Card Specifications for Payments Systems. It manages, maintains, and enhances the EMV specifications jointly owned by the payment systems. It currently consists of American Express, Discover, JCB, MasterCard, Union Pay and VISA.
Host Card Emulation (HCE)	A technology that enables mobile devices to emulate a contactless card. HCE does not require the local usage of an SE on the mobile device for storage of sensitive data such as credentials, cryptographic keys, etc.
(Card) issuer	A PSP contracting to provide a payer with a payment instrument to initiate and process the payer's card-based payment transactions. Note: This PSP can be a member of a card payment scheme.
In-app payment	These are payments made directly from within a mobile application (e.g., a merchant app). The payment process is completed from within the app to enhance the consumer experience.

Local (card) payment	A card payment initiated at the merchant's (physical) POI and processed as an EMV-based card transaction. This concept is the opposite of a remote (card) payment (see [5]).
Merchant	The beneficiary within a mobile payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP.
Mobile Card-based Proximity Payment (MCPP)	A mobile card payment where the consumer and the merchant (and/or their equipment) are in the same location and where the communication between the mobile device and the Point of Interaction device takes place through a non-NFC proximity technology (e.g., QR-codes, BLE, etc.).
MCPP app(lication)	A set of modules (application software) and/or data (application data) needed to provide functionality for an MCPP service as specified by the MCPP provider in accordance with the Card scheme.
Mobile code	An authentication credential used for cardholder verification and entered by the consumer via the keyboard of the mobile device.
Mobile Contactless Payment (MCP)	A mobile proximity payment where the payer and the payee communicate directly using contactless NFC technology.
Mobile device	Personal device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth, etc. Examples of mobile devices include mobile phones, smart phones, tablets.
Mobile Network Operator (MNO)	A mobile phone operator that provides a range of mobile services, potentially including facilitation of NFC services. The MNO ensures connectivity Over the Air (OTA) between the consumer and their PSP using their own or leased network.
Mobile payment service	A payment service made available by software/hardware through a mobile device.
Mobile service	A service such as identification, payment, ticketing, loyalty, etc., made available through a mobile device.
Mobile wallet	A digital wallet accessed through a mobile device. This service may reside on a mobile device owned by the consumer (i.e. the holder of the wallet) or may be remotely hosted on a secured server (or a combination thereof) or on a merchant website. Typically, the so-called mobile wallet issuer provides the wallet functionalities but the usage of the mobile wallet is under the control of the consumer.
Mobile wallet issuer	The service provider that issues mobile wallet functionalities to the customer (consumer or merchant).
NFC (Near Field Communication)	A contactless protocol for mobile devices specified by the NFC Forum for multi-market usage and by EMVCo [7] for mobile card payment applications. NFC Forum specifications (see [24]) are based on ISO/IEC 18092 [23] but have been extended for harmonisation with EMVCo and interoperability with ISO/IEC 14443 [21] infrastructures.

Payment Service Provider (PSP)	A body referred to in Article 1(1) of [2] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of [2].
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 [2]).
POI	"Point of Interaction", the initial point in the merchant's environment where data is exchanged with the mobile device or where consumer data is entered (e.g. physical POI, QR-code on a poster).
Physical POI	A POI that is a physical device and consists of hardware and software, hosted in acceptance equipment to enable a cardholder (consumer) and/or merchant to perform a local card payment. The merchant controlled POI may be attended or unattended. Examples of POI include POS, vending machine (see [5]).
QR-code	A two-dimensional code consists of black modules arranged in a square pattern on a white background. A Quick Response (QR)-code is an example of a two-dimensional code as specified in ISO/IEC 18004 [22].
Primary Account Number (PAN)	A series of digits that identify a customer card account or relationship. This number contains a maximum of 19 digits according to ISO/IEC 7812 [19].
Remote (card) payment	A transaction initiated by the consumer (cardholder) using a customer device (i.e. a mobile device in the context of this document) to buy products and services using mobile internet. The concept is the opposite of a local (card) payment (see [5]).
Remote POI	The initial point where card data enters the merchant's domain for remote transactions. It exists in a variety of technical platforms which enable a cardholder (consumer) and/or a merchant to generate a remote payment (e.g. a payment page accessed via a merchant website or via a mobile app) (see also [5]).
Secure Element (SE)	A tamper-resistant platform (typically a one chip secure microcontroller) 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. There are different form factors of SE including Universal Integrated Circuit Card (UICC), embedded SE (including eUICC and iSE) and microSD. Both the UICC and microSD are removable.
Static Authentication	An authentication method that always uses the same authenticator.
(Payment) Tokenisation	The usage of payment tokens instead of real payer related account data in payment transactions
(Payment) Token	Payment Tokens can take on a variety of formats across the payments industry. They generally refer to a surrogate value for payer account related data (e.g., the PAN for card payments). Payment Tokens must

	not have the same value as or conflict with the real payment account related data.
Strong customer authentication	An authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (see Article 4 in [2]).
User Interface (UI)	An application or part of an application enabling the user interactions, as permitted by the application issuer. It allows to provide information to the consumer (such as payment amount) and enables the consumer to interact in order to change preferences, perform queries, enter credentials, etc.

Table 2: Terminology

0.4 Abbreviations

Throughout this document, the following abbreviations are used.

Abbreviation	Term
BLE	Bluetooth Low Energy
CDCVM	Consumer Device CVM
CNP	Card-Not-Present
CVM	Cardholder Verification Method
2D barcode	Two dimensional barcode
EBA	European Banking Authority
EC	European Commission
EPC	European Payments Council
ERPB	Euro Retail Payments Board
ECSG	European Cards Stakeholders Group
ETSI	European Telecommunications Standards Institute
FIDO Alliance	Fast IDentity Online Alliance
GDPR	General Data Protection Regulation
GSMA	The GSM Association
HCE	Host Card Emulation
IEEE	Institute of Electrical and Electronics Engineers
IF Regulation	Interchange Fee Regulation
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
MA	Mobile Application
MCP	Mobile Contactless Payment
MCPP	Mobile Card-based Proximity Payment

MNO	Mobile Network Operator
NFC	Near-Field Communication
OS	Operating System
OTA	Over the Air
PAN	Primary Account Number
PCI	Payment Card Industry
POI	Point of Interaction
POS	Point of Sale
PSD	Payment Services Directive
PSP	Payment Service Provider
QR-code	Quick Response code
RFID	Radio Frequency Identification
RTS	Regulatory Technical Standard
SE	Secure Element
SEPA	Single Euro Payments Area
SP	Service Provider
TSM	Trusted Service Manager
TSP	Token Service Provider
TP	Third Party
UI	User Interface
URL	Uniform Resource Locator

Table 3: Abbreviations

1 General

1.1 Introduction

In March 2017, the EPC published the latest edition of a white paper [11], which provides a high-level description of mobile payments in general, covering mobile proximity and mobile remote payments. The EPC also facilitated the setting-up of a multi-stakeholder group covering the various sectors involved in the mobile payment ecosystem to develop a new version of the implementation guidance for mobile contactless card based payments (MCPs) based on NFC-technology, covering business, technical, security and legal aspects (see [12]).

The present document, developed by the same multi-stakeholder group (see Annex B), provides an overview of card-based mobile proximity payments (MCPPs) using non-NFC based technologies.

1.2 Vision

This document subscribes to the vision specified in the ERPB report on Mobile and card-based contactless proximity payments (see [15]) which reads as follows:

"To ensure over time, across Europe, a secure, convenient, consistent, efficient and trusted payment experience for the customer (consumer and merchant) for retail transactions at the Point of Interaction (POI), based on commonly accepted and standardised contactless and other proximity payment technologies."

This vision is based on the following guiding principles:

- Technical interoperability of contactless and other proximity transactions across Europe (based on common technical, functional and security standards and a common certification and evaluation framework) both for consumer devices (cards, mobile devices, wearables, …) and POIs;
- Wide availability and usability of appropriate POI equipment and consumer devices;
- Appropriate security and privacy to build and maintain trust.

The aim is to lead to an enhanced payment experience – faster check out, improved user-friendliness, better integration of value added services with payment – and to increased cost-effectiveness for society.

This white paper aims to contribute to the creation of awareness on non-NFC based mobile card proximity payments amongst the various stakeholders involved in the mobile ecosystem in order to deliver efficient and user-friendly MCPP solutions, in an integrated market.

1.3 Scope

The European market is currently much less mature with respect to the usage of non-NFC based technologies for mobile payments compared to MCPs. Also the related standardisation efforts towards interoperability of these solutions are in their early days. Therefore this document is conceived as a white paper to provide a high level overview of non-NFC based mobile card proximity payments (MCPPs), whereby SEPA cards as specified in the Cards Standardisation Volume (see [5]) are the underlying payment instrument[3]. In view of the current market deployments, the document has been restricted to proximity payments based on QR-codes and Bluetooth-Low-Energy (BLE) technologies (see section 2.3). Note that although many non-card

[3] Note that the use cases and service models introduced in these guidelines may also be applied outside SEPA.

based QR-code solutions already exist in the market today (such as SEPA Credit Transfer, Direct Debit or e-money based), they are out of scope of the current document, since other multi-stakeholder groups are covering these payments[4].

Next to use cases, the document provides some insights into transaction characteristics, the technology and infrastructure used and tries to identify some of the opportunities and challenges posed by these solutions.

It is important to note that the document only addresses the aspects of MCPPs which reside in the interoperability space of the stakeholders in the MCPP value chain. As such, the specification of business cases and a detailed analysis of the MCPP value chain fall outside the scope of the document.

1.4 Objectives and rationale

Non-NFC proximity technologies (e.g. QR-codes, BLE) have been introduced in the market for various mobile services to enhance the consumer experience and to bring additional functionality at the check-out to the customer (e.g. integration of payment with loyalty).

The ERPB report on mobile and card-based contactless proximity payments (see [15]), published in 2015, identified some challenges to be addressed in the context of MCPs using NFC technology to meet the vision cited above. One of the main obstacles identified in section 5.2.4 of this report, is the lack of openness of some operating systems in the market which may be stifling innovation; e.g., the lack of open and free access to the mobile device capabilities (such as the NFC antenna). The report specified a dedicated recommendation in that respect (see ERPB/2015/rec 16[5]) on which, unfortunately not much progress was made during the last two years. In some markets, the lack of accessibility to the NFC antenna in some mobile operating systems, has given rise to the introduction of non-NFC based mobile proximity payments solutions to meet customer expectations.

The purpose of this document is to provide insights into these solutions and to identify some challenges with respect to achieving an adequate level of interoperability and enabling a harmonised customer experience across Europe for MCPPs at the POI.

1.5 Audience

The present document is primarily intended for the payment industry. It aims to create awareness amongst the industry about the development of non-NFC based MCPP solutions and to provide a common understanding of the MCPP landscape. It could further be used as a reference by the payment industry.

[4] See for instance https://www.europeanpaymentscouncil.eu/what-we-do/other-sepa-payments/sepa-goes-mobile/ad-hoc-multi-stakeholder-group-mobile-initiated and https://www.europeanpaymentscouncil.eu/what-we-do/other-sepa-payments/sepa-goes-mobile/ad-hoc-multi-stakeholder-group-mobile-initiated

[5] ERPB/2015/019: Statement following the fourth meeting of the Euro Retail Payments Board held on 26 November 2015.

2 Mobile card proximity payments overview

2.1 Introduction

In the context of this document, non-NFC Mobile SEPA Card Proximity Payments (MCPPs) are SEPA Card Payments (see [5]) which are initiated using a mobile device. The consumer and the merchant's POI are in the same location and the communication between the mobile device and the POI takes place through a non-NFC proximity technology (e.g., QR-code, BLE).

2.2 Different types of MCPPs

Mobile card payments may be categorised in different ways. The table below aims to provide an overview depending on the payment context. The blue shaded area marks the scope of the present document on non-NFC mobile SEPA card based proximity payments. Hereby two technologies are considered: QR-code and BLE. For QR-codes a distinction is made between merchant- and consumer-presented modes. Depending on the implementation, the transaction may be a "local" or a "remote" card transaction (see [5]).

Payment context	Mobile card-based payments

Person to Person (P2P)
• Mobile banking
  o Browser
  o Banking app
• MCPP (P2P) app
	• Push and pull models
	• Different technologies including NFC, QR-codes, BLE
	
	Reference:
	EPC White paper mobile payments (EPC492-09v5.0, [11])

m-Commerce • Browser • MCPP app • In-app	*References:* EPC White paper mobile payments, [11] SEPA Cards Standardisation Volume, [5]
In-store (cash register) • NFC	*References:* EPC White paper mobile payments, [11] SEPA Cards Standardisation Volume, [5] Mobile Contactless SEPA Card Interoperability Implementation Guidelines, [12]
• QR-codes	**Merchant-presented (attended / unattended)** • QR-code scanned by the consumer's mobile device from a merchant presented QR-code (e.g., QR-code on physical POI, poster, webpage, etc) including the merchant data • Static or dynamic QR-code • Initiated by the consumer

	• Remote card transaction[6] (see section 3.6) *Reference:* EMV QR-code Specification for Payment Systems (EMV QRCPS) – Merchant-Presented Mode, [8] **Consumer-presented mode** • QR-code presented by the consumer's mobile device to the merchant's POI including card data • Static or dynamic QR-code • Initiated by the merchant • Depending on the implementation (see section 3.6): o local card transaction based on EMV-QR- code (QR-code with chip data) o remote card transaction with stored card data (card-on-file) (QR-code with cardholder identifier) *Reference:* EMV QR-code Specification for Payment Systems (EMV QRCPS) - Consumer-Presented Mode, [9]
• BLE technology	**Connection via Bluetooth Low Energy Technology (BLE) (attended / unattended)** • Merchant initiated transaction • Remote card transaction[7] (see section 3.6)

Table 4: Overview Mobile Card Payments

2.3 Proximity technologies

The non-NFC based proximity technologies considered in this document are QR-codes and BLE, which are briefly described below.

QR-code

A two-dimensional code consisting of black modules arranged in a square pattern on a white background. A Quick Response (QR) code is an example of a 2D code as specified in ISO/IEC 18004 [22]. In the context of mobile card proximity payments, the QR-code is used as a means of payment initiation, in one of two modes;

[6] Note that this mechanism could also initiate non-card based remote transaction which however fall outside the scope of this document.

[7] Technically the transaction could also be implemented as a local transaction, processed in a similar way as an NFC-based mobile card transaction. However, no such implementations were identified in the European market today.

1. Merchant-presented QR-code - where the code contains data to identify the merchant and transaction or
2. Consumer-presented QR-code – where the code contains data to identify the customer.

In the case of a merchant-presented QR-code, the consumer needs to have a mobile application on their mobile device that has the capability of scanning the QR-code of the merchant and initiating a mobile card payment transaction. Merchant-presented QR-codes have been specified by EMVCo in [8].

In the case of a consumer-presented QR-code, the consumer can make purchases using data associated with themselves or their card and previously provisioned to their mobile device. This data may range from cardholder identification data, over credentials to chip card data which are used to calculate a QR-code (static or dynamic). The consumer typically has to select the QR option for card payment within their mobile card application, which will result in the display of the QR-code on the mobile device. The QR-code is scanned by the merchant at the time of payment to complete the purchase. Consumer-presented QR-codes have been specified by EMVCo in [9].

Bluetooth and Bluetooth Low Energy

Bluetooth

Bluetooth is an industry standard according to IEEE 802.15.1 for bidirectional data transmission between devices over relatively short distances using radio technology. They may be operated worldwide without approval but robustness against interference (e.g., by WLANs or cordless telephones) needs to be implemented[8]. The actual achievable range depends not only on the transmission power but also on several further parameters such as for example, the sensitivity of a receiver and the designs of the transmitting and receiving antennas used by radio communication modules, or obstacles between transmitter and receiver. There are different range classes: Class 1 (max. 100 m), Class 2 (max. 10 m), Class 3 (max. 1 m).

Pairing

The establishment of a connection always takes place under the protocol architecture according to the specifically supported Bluetooth release version. A connection can originate from any Bluetooth enabled device. As soon as Bluetooth devices are put into operation, the individual Bluetooth controllers identify themselves within two seconds. Since this connection time for payment application at the POI is much too long, currently only the variant "Bluetooth Low Energy (BLE)" is applied in payment contexts.

Bluetooth Low Energy

Bluetooth Low Energy (BLE), is a radio technology with which devices in an environment up to about 10 meters can be networked. Compared to "classic" Bluetooth, BLE offers significantly shorter connection times. Based on the protocol Bluetooth version Low Energy V4.0 (and later) a “connectionless” (non-statically paired) operation can be established in only 3 ms and data transmission can be completed after 6 ms.

[8] To achieve robustness against interference, frequency hopping is used, in which the frequency band is divided into 79 channels at 1 MHz intervals, which are changed up to 1600 times per second.

It should be noted that currently EMVCo is considering the inclusion of BLE technology in their 2nd Generation Specifications.

2.4 MCPP use cases

Introduction

The following use cases for non-NFC mobile card-based proximity payments (MCCPs) will be described in this document through a figure with a description of the different steps involved. Note that these use cases are presented for illustrative purposes only, the list is not meant to be exhaustive.

Use case #	Description
Use case 1	Merchant-presented QR-code at POI in-store, including transaction amount, – remote card transaction - customer authentication using fingerprint
Use case 2	Merchant-presented QR-code on a poster – consumer entry of transaction amount – remote card transaction - customer authentication with mobile code
Use case 3	Consumer-presented QR-code including chip card data – local transaction – transaction amount entered by merchant and added in authorisation message – local card transaction - customer authentication using mobile code
Use case 4	Consumer-presented QR-code including cardholder identifier – low value transaction amount entered by merchant and added in authorisation message – remote card transaction with stored card data
Use case 5	Merchant initiated BLE-based at POI in-store - remote card transaction - customer authentication using mobile code

Table 5: Overview MCPP Use cases

Use case 1: Merchant-presented QR-code at POI – customer authentication using fingerprint

In this use case, both the consumer and the merchant / acquirer participate in an MCPP service. An MCPP transaction is described, which is performed with a mobile device via the scanning of a QR-code, containing the transaction amount, on the payment terminal in a store. The transaction is a remote card transaction with an on-line authorisation to the issuer whereby a fingerprint is used as a CDCVM.

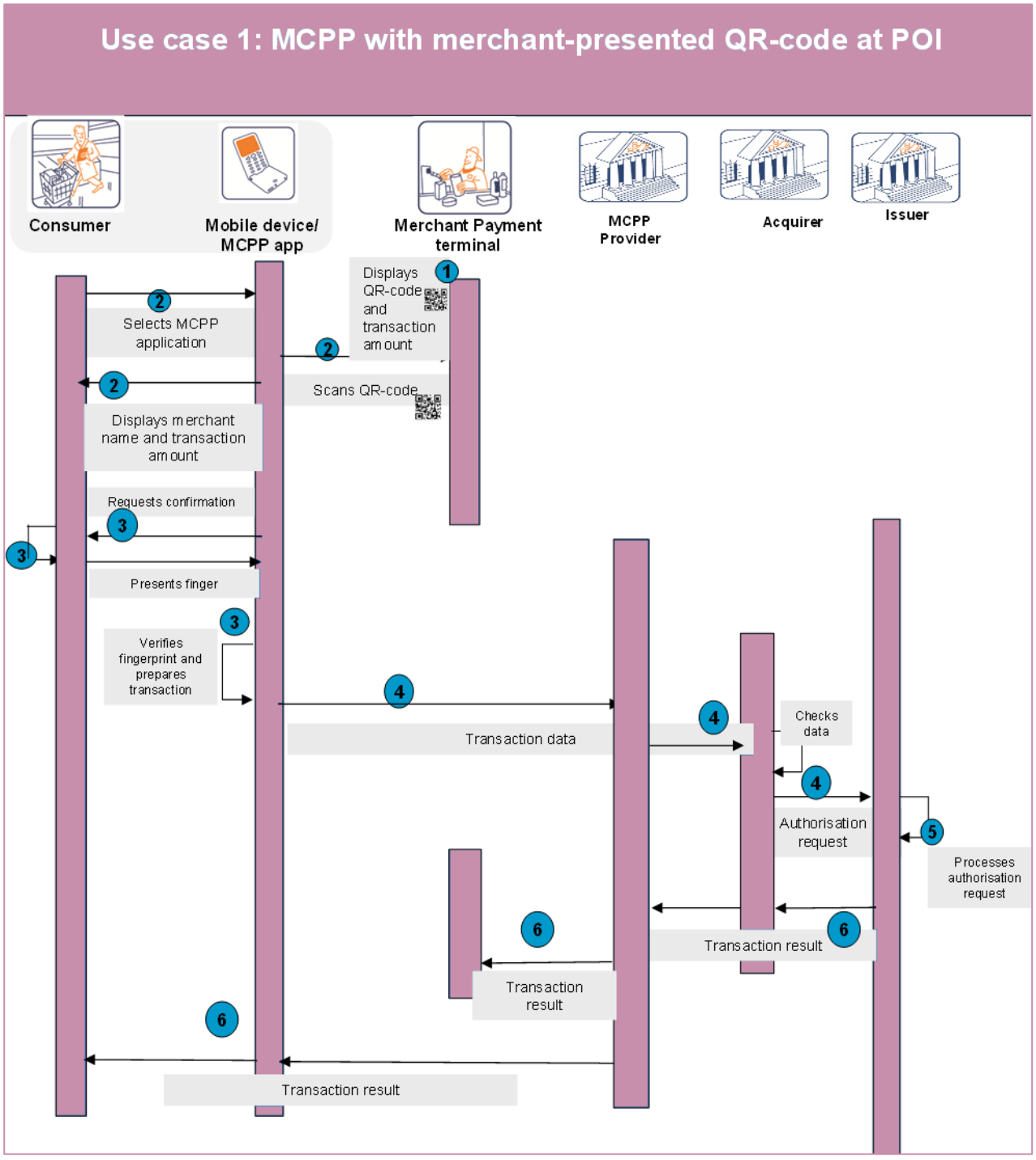

Figure 1: MCPP with merchant-presented QR-code at POI

In the figure above the following steps are illustrated:

- As a prerequisite, the consumer would need to first subscribe to the MCPP service and download an MCPP app from an MCPP service provider on their mobile device, linked to a specific card account.
- The merchant and the acquirer need to participate in the MCPP service.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The consumer scans their groceries at an unattended terminal in a department store and confirms to proceed to payment.
- The transaction amount is displayed on the payment terminal with a QR-code, which is generated by the payment terminal and includes the transaction amount, the merchant's identifier and merchant name.

Step 2

- The consumer selects their MCPP app in their mobile wallet and scans the QR-code from the POI;
- The mobile device displays the transaction amount and the merchant name and requests a consumer confirmation.

Step 3

- The consumer confirms the payment transaction by having their fingerprint read by the mobile device.
- The fingerprint is verified by the mobile device.

Step 4

- Upon successful fingerprint verification, the MCPP app sends the details of the transaction, including the transaction amount and merchant account data to the MCPP service provider.
- The MCPP provider forwards this data to the acquirer who checks the data and initiates an on-line card authentication / transaction authorisation to the issuer.

Step 5

- The issuer processes the authorisation request.

Step 6

- The merchant is informed about the result of the transaction by the MCPP service provider.
- The consumer is informed about the result of the transaction and may optionally receive an e-receipt from the MCPP service provider.

Notes:

- The presentation of the QR-code by the merchant could also be done for example on a webpage on a merchant tablet, the transaction flow however would remain the same.

- A variant to this example exists with respect to the processing of the transaction data. However, the consumer experience remains the same. The transaction information could be sent from the mobile device to the MCPP service provider which associates the transaction information received from the MCPP app with information received from the merchant's POI (see section 3.6).

Use case 2: Merchant-presented QR-code on a poster – customer authentication with mobile code

This use case presents an MCPP transaction which may be used for a donation for charity. It is performed with a mobile device via the scanning of a QR-code on a poster. The transaction information is entered by the consumer on the mobile device. The transaction is a remote card transaction with an on-line authorisation to the issuer whereby a mobile code is used as CDCVM.

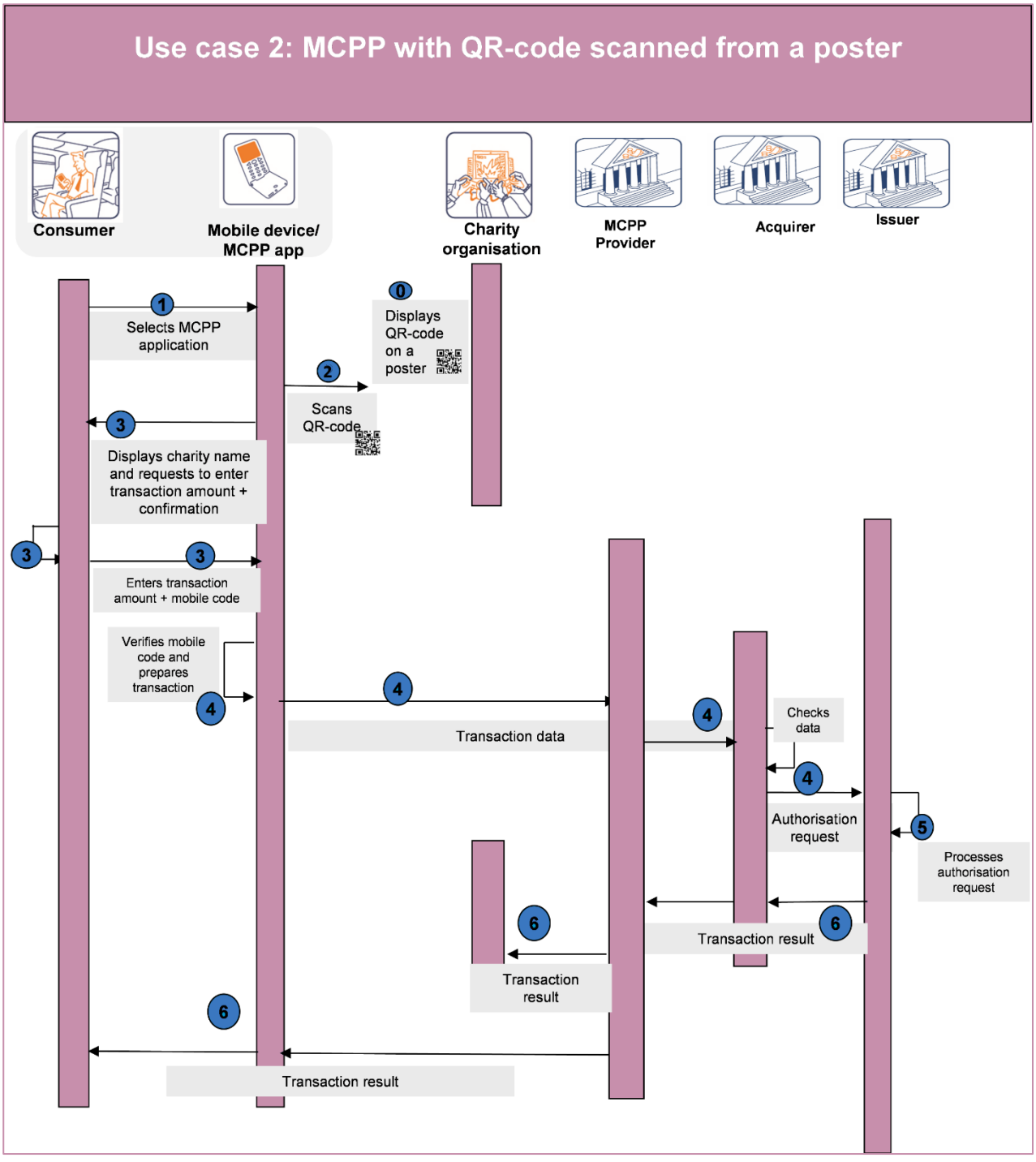

Figure 2: MCPP with QR-code scanned from a poster

In the figure above the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MCPP service and download an MCPP app from an MCPP service provider on their mobile device, linked to a specific card account.
- The merchant and the acquirer need to participate in the MCPP service.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The consumer wishes to donate for a charity seeing a dedicated poster.
- The consumer selects their MCPP app in their mobile wallet and opens the app.

Step 2

- A message is displayed on the mobile device inviting the consumer to scan the QR-code.

Step 3

- The MCPP app scans the QR-code and retrieves the merchant identifier and name.

  The consumer is invited to enter their donation amount and to confirm the transaction by entering their mobile code.

Step 4

- Upon successful verification of the mobile code by the MCPP app, the transaction information (including the merchant identifier and transaction amount) is sent to the MCPP service provider.
- The MCPP provider forwards this data to the acquirer who checks the data and initiates an on-line card authentication / transaction authorisation to the issuer.

Step 5

- The issuer processes the authorisation request.

Step 6

- The merchant is informed about the result of the transaction;
- The consumer is informed about the result of the transaction and may optionally receive an e-receipt.

Use case 3: Consumer-presented QR-code including chip card data – customer authentication with mobile code

This use case presents an MCPP transaction, which is performed via the presentation of a QR-code, which includes chip card data, by the customer on their mobile device to the merchant's POI. The transaction is processed as a local card transaction with on-line authorisation to the issuer whereby a mobile code is used as CDCVM.

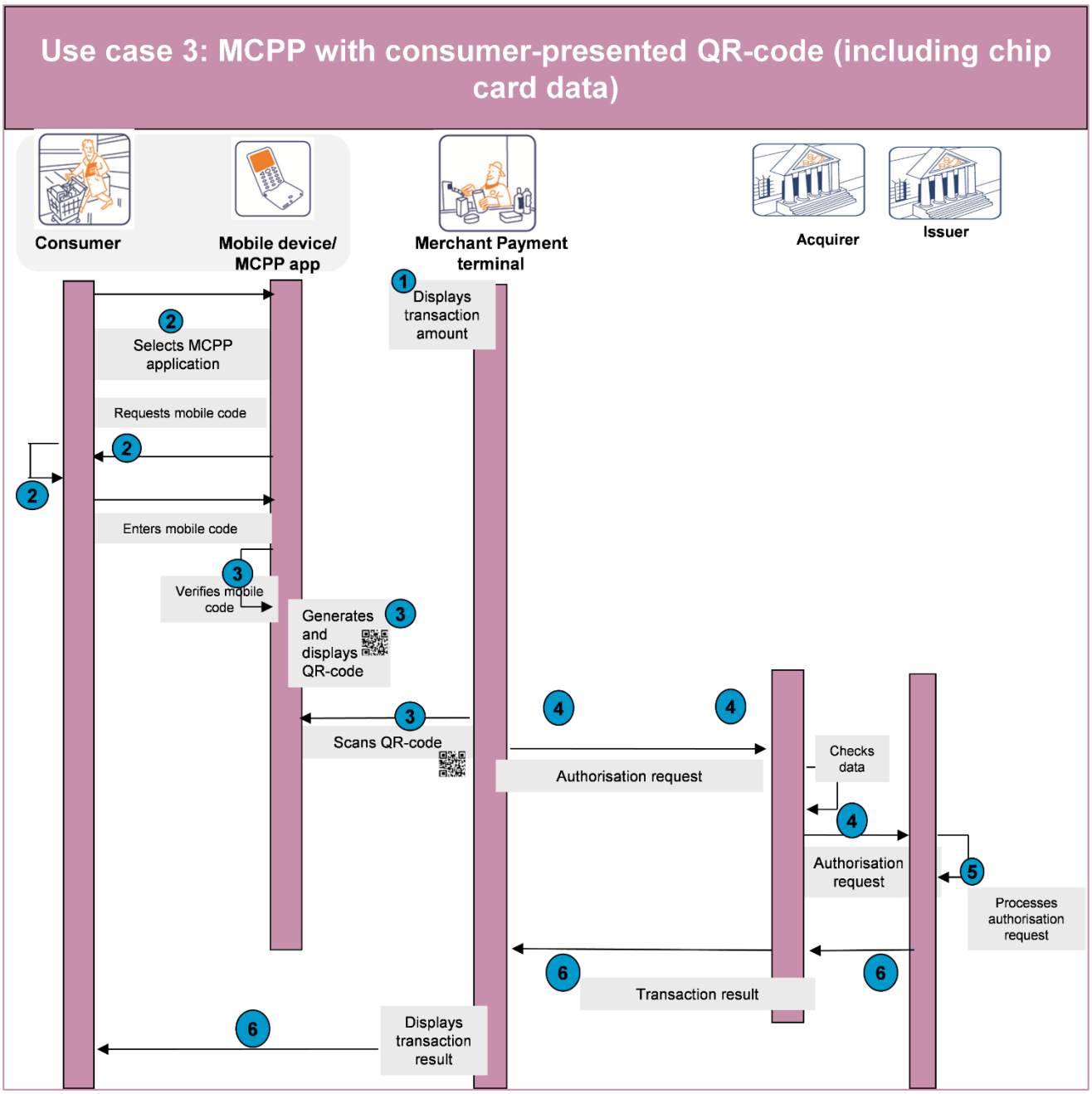

Figure 3: MCPP with consumer-presented QR-code (including chip data)

In the figure above the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MCPP service, including the registration of their card account.
- They also need to download an MCPP app on their mobile device from the MCPP service provider that can generate and display a QR-code that contains chip card data linked to their card account.

Step 1

- The merchant enters the transaction amount on the POI.
- The transaction amount is displayed on the merchant's POI.
- The POI requests for a card payment.

Step 2

- The consumer selects the MCPP app on their mobile device and opens the MCPP app by presenting their mobile code to the mobile device.
- The mobile code is verified by the MCPP app on mobile device.

Step 3

- Upon successful mobile code verification, the MCPP app generates a QR-code which contains chip card data and a dynamic element.
- The consumer presents the QR-code to the POI to confirm the payment transaction.
- The POI scans the QR-code and retrieves the cardholder data from the QR-code.
- The merchant includes the transaction amount with the retrieved card data into the authorisation request message.

Step 4

- A local transaction is initiated by the merchant and an on-line transaction authorisation is performed to the issuer via the acquirer.

Step 5

- The issuer processes the authorisation request.

Step 6

- The merchant is informed about the result of the transaction via their acquirer.
- The consumer is informed about the result of the transaction via the POI.
- Depending on the purchase amount, the merchant’s POI features and consumer choice, a transaction receipt may be printed.

***Note**:* This solution enables an easy combination with a merchant loyalty application by using the consumer identification data from the scanned QR-code.

Use case 4: Consumer-presented QR-code including cardholder identifier – low value transaction

This use case presents an MCPP transaction, which is performed via the presentation of a QR-code, which includes a cardholder identifier, by the customer on their mobile device to the merchant's POI. The card data is collected by the merchant through the cardholder identifier retrieved from the scanned QR-code by the POI. The transaction is processed as a remote card transaction with stored card data (card-on-file CNP payment), whereby no customer authentication is performed in view of the low value transaction. It is typically used in "closed" systems.

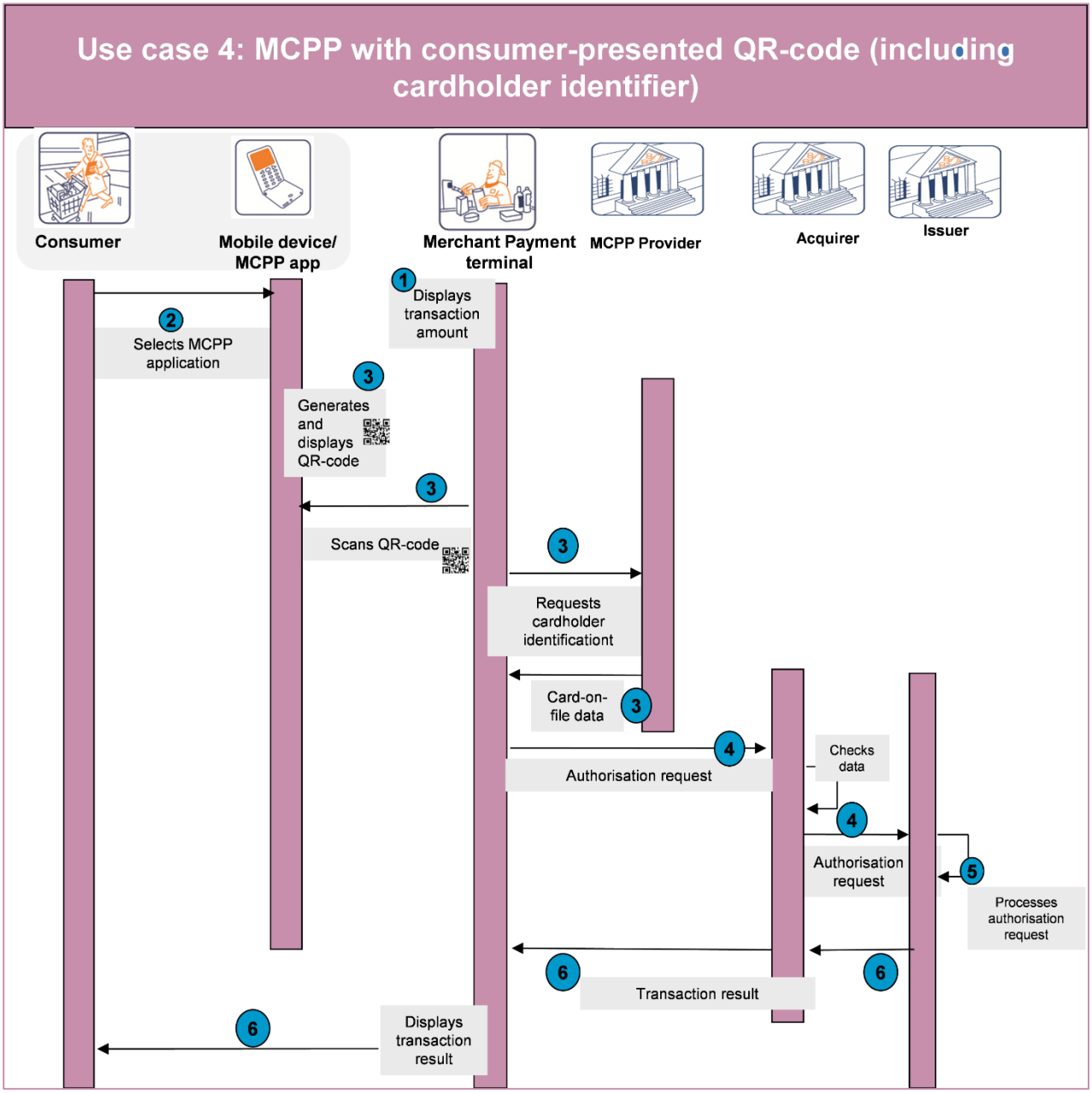

Figure 4: MCPP with consumer-presented QR-code (including cardholder identifier)

In the figure above the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MCPP service, including the registration of their card account with a corresponding cardholder identifier.
- They also need to download a dedicated MCPP app on their mobile device from the MCPP service provider that can generate and display a QR-code calculated on their identifier.
- The merchant needs to be subscribed to the MCPP service and needs to be connected to the MCPP service during the transaction.

Step 1

- The merchant enters the transaction amount on the POI.
- The transaction amount is displayed on the merchant's POI.
- The POI requests for a card payment.

Step 2

- The consumer selects and opens the MCPP app on their mobile device.

Step 3

- The MCPP app generates a QR-code which contains consumer identification data (e.g. cardholder identifier, including a dynamic element).
- The consumer presents the QR-code to the POI to confirm the payment transaction.
- The POI scans the QR-code and retrieves the consumer identification data from the QR-code.
- The merchant retrieves the card-on-file data related to the consumer identification data from the MCPP service and includes it with the transaction data, including the transaction amount, into the authorisation request message.

Step 4

- A remote card transaction is initiated by the merchant and an on-line authorisation is performed to the Issuer.

Step 5

- The issuer processes the authorisation request.

Step 6

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

Note: This solution enables an easy combination with a merchant loyalty application by using the consumer identification data from the scanned QR-code.

Use case 5: Merchant initiated BLE-based transaction at POI – customer authentication with mobile code

This use case presents an MCPP transaction, which is performed with a mobile device via a single tap using BLE technology with the POI in-store. The transaction is a remote card transaction with an on-line authorisation to the issuer whereby a mobile code is used as a CDCVM.

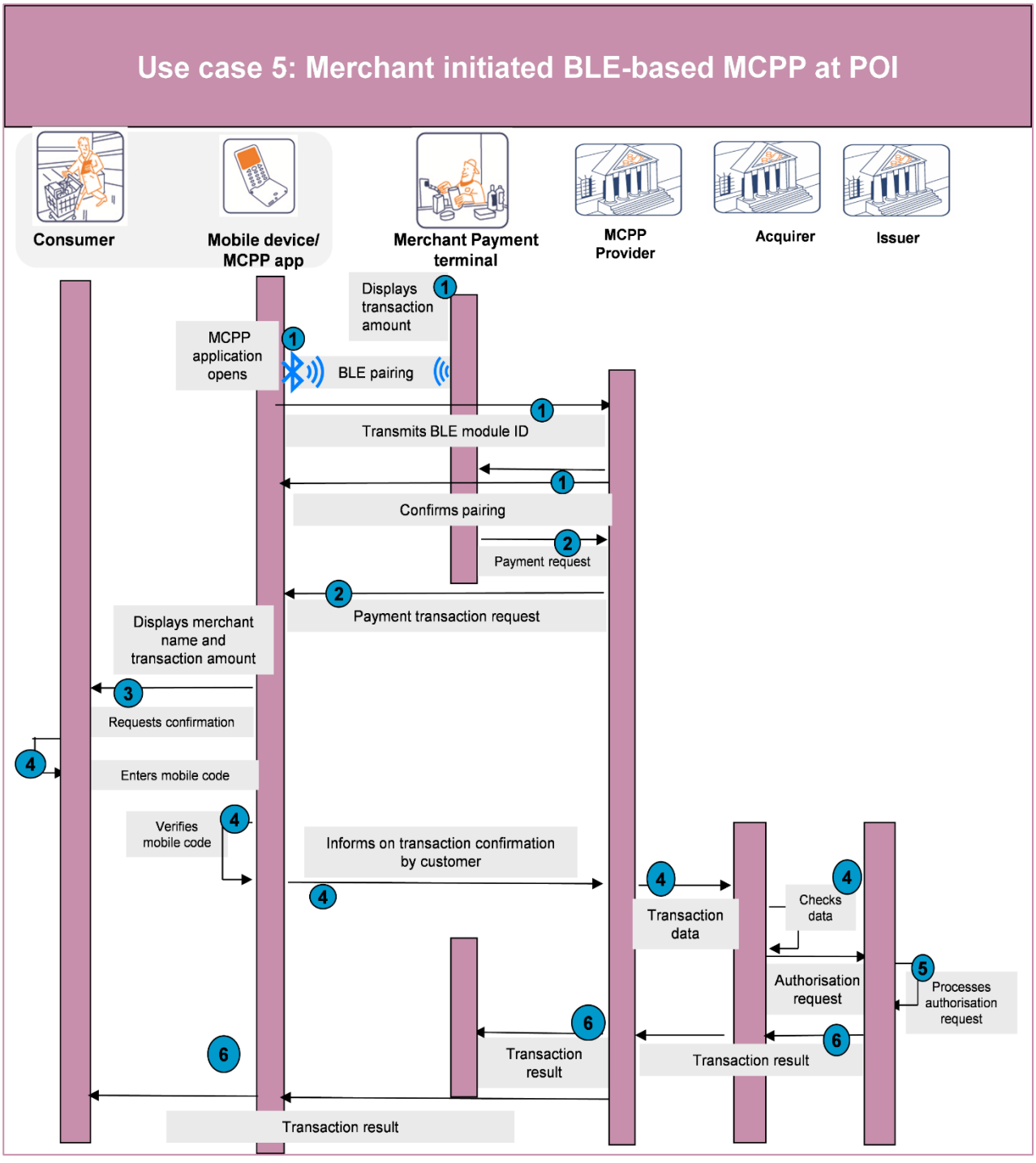

Figure 5: Merchant initiated BLE-based MCPP at POI

In the figure above the following steps are illustrated:

Step 0

- As a prerequisite, the consumer would need to first subscribe to the MCPP service and download a dedicated MCPP app on their mobile device from the MCPP service provider, linked to a specific card account.
- The merchant needs to be subscribed to the MCPP service and needs to be connected to the MCPP service during the transaction.
- During the payment transaction, a mobile internet connection is required.

Step 1

- The merchant enters the transaction amount on the POI.
- The transaction amount is displayed on the merchant's POI.
- The consumer places their mobile device briefly next to the BLE module in the POI area which automatically opens the MCPP app (this assumes that the BLE is turned-on). The BLE module pairs with the MCPP app and transmits a BLE module ID.
- The MCPP app transmits the received BLE module ID to the MCPP service provider back-end system.
- The MCPP service provider back-end system identifies and associates the POI and the consumer's mobile device.
- Then, the back-end server returns a confirmation message to the mobile device which is shown in the MCPP app. At the same time, the POI learns from the MCPP service provider back-end system that a pairing has taken place.

Step 2

- The POI sends a payment request with the transaction amount to the MCPP service provider back-end.
- Because of the existing pairing, the consumer's mobile device is known on the back-end server and a corresponding message is sent to the MCPP app on the mobile device.

Step 3

- The consumer's MCPP app displays the transaction amount payable along with information about the merchant.
- The consumer is requested to enter a mobile code to confirm the payment[9].
- Upon successful verification of the mobile code by the MCPP app, the MCPP service provider back-end system is informed.

Step 4

- A remote card transaction with an on-line authorisation to the Issuer is performed by the MCPP service provider back-end system.

Step 5

[9] Even if it concerns a low value payment and a CDCVM is not performed, the explicit confirmation of the transaction by the consumer is required (e.g. a swipe or confirmation on mobile device display).

- The issuer processes the authorisation request.

Step 6

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

3 MCPP transaction characteristics

3.1 Introduction

This chapter aims to provide a high-level overview of the different transaction characteristics involved in MCPPs. However, it is up to the card schemes and the MCPP issuers and acquirers involved to decide which transaction flows will be applied.

3.2 Cardholder verification

The mobile environment already offers today a number of additional features which can be utilised for MCPPs with respect to Cardholder Verification Methods (CVMs) compared to physical contactless cards. This includes for example, the keyboard of the mobile device, a camera (iris scanning), or a dedicated biometric sensor (fingerprint).

For MCPPs, the cardholder verification method used is typically a CDCVM. It is entered by or captured from the consumer on the mobile device. Typical methods used include

- Biometrics, verified by the OS on the mobile device.
- Mobile code[10]: entered on the mobile device.
    - The verification of the mobile code is done by an MCPP application on the mobile device;

  or

    - Implicit validation of the correct entry of the mobile code through a cryptographic derivation, verified on-line by the MCPP issuer.

Note that a CDCVM authentication result may be used in a number of different ways as shown below. EMVCo is currently working on a more detailed document on this subject.

Instant (authentication/ verification)	Prompt for CDCVM for every transaction (e.g., mobile code, fingerprint)
Persistent (authentication/ verification)	Prompting for CDCVM is not necessary as long as certain conditions remain satisfied (for example consistent monitoring of the consumer presence) (e.g., vein recognition by wristband or smart watch).
Prolonged (authentication/ verification)	Prompt for CDCVM only if a CDCVM has not occurred within a pre-defined time-period.

Table 6: Overview CDCVM usage

On a mobile device, a distinction may be made between a CDCVM verified by the MCPP issuer, and a so-called “shared” CDCVM, which is shared amongst different mobile applications accessible via the mobile device. This “shared” CDCVM may be verified by another service provider than the

[10] For security reasons, in case of a mobile code, this is a dedicated mobile code (also referred to as mobile PIN, mobile passcode, etc.) which differs from the "classic" card PIN.

MCPP issuer. Functional and security requirements for "platform shared authentication" mechanisms are currently being developed by EMVCo.

The usage of a CVM is often linked to transaction risk management and is applied by the MCPP issuer in the context of strong customer authentication according to the Regulatory Technical Standards (RTS) for Strong Customer Authentication and Common and Secure Communication under PSD2 (see sections 3.4, 3.5 and Annex A: Overview regulatory documents). Typically, lower value transactions are exempted from the usage of a CVM (see section 3.4). For MCPPs, other factors, such as consumer choice, may influence the usage of a CVM.

3.3 Transaction authorisation

As with mobile contactless NFC-based card payments, a distinction could be made between on-line and off-line transactions with respect to the authorisation of the transaction by the issuer as follows:

- **On-line transaction:** MCPP transaction authorised via an on-line communication with the card issuer, see [5];
- **Off-line transaction:** Off-line authorised MCPP transaction by an MCPP Application on the mobile device (this means without on-line communication to the card issuer, see [5]).

However, since there do not seem to be solutions in the European market using off-line authorisations for non-NFC based mobile proximity card payments, the document will not further analyse this option.

The table below shows a matrix of the possible transaction types for the execution of an MCPP transaction between a mobile device and a POI for on-line authorisations.

MCPP transaction		
	On-line authorisation	
	Local card transaction	Remote card transaction
Merchant-presented QR-code	-	X
Consumer-presented QR-code	X QR-code includes chip card data	X QR-code includes only cardholder identifier Card-on-file transaction
BLE technology*	[X]**	X

Table 7: Overview MCPP transactions

*dependent on the implementation these transactions may be processed as local or remote card transactions

** since no actual implementations have been identified in Europe, this category is not further considered in this document

3.4 Strong customer authentication

Article 97 of the Payment Services Directive PSD2 [2] mandates the usage of strong customer authentication for transactions, except for the exemptions (Article 98) defined in Article 11 [Contactless payments at point of sale], Article 12 [Unattended terminals for transport fares and parking fees] and Article 13 [Trusted beneficiaries] of the Commission delegated regulation, supplementing PSD2, with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as 'RTS') (see [5] in : Annex A: Overview regulatory documents).

The most important exemptions read as follows:

Article 11:

"Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 of the RTS, where the payer initiates a contactless electronic payment transaction provided that the following conditions are met:

(a) the individual amount of the contactless electronic payment transaction does not exceed EUR 50; and

(b) the cumulative amount of previous contactless electronic payment transactions initiated by means of a payment instrument with a contactless functionality from the date of the last application of strong customer authentication does not exceed EUR 150; or

(c) the number of consecutive contactless electronic payment transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication does not exceed five."

Article 12:

"Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee."

3.5 Transaction authentication

Article 97(2) of the Payment Services Directive PSD2 [2] mandates *for electronic remote payment transactions, that payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee*[11], except for the exemptions (Article 98), defined in Article 16 [Low value transactions] and Article 18 [Transaction risk analysis] of the RTS (see [5] in Annex A: Overview regulatory documents)

The exemptions read as follows:

Article 16:

"Payment service providers shall be allowed not to apply strong customer authentication, where the payer initiates a remote electronic payment transaction provided that the following conditions are met:

[11] i.e. merchant in the context of this document.

(a) the amount of the remote electronic payment transaction does not exceed EUR 30; and

(b) the cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed EUR 100;

or (c) the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed five consecutive individual remote electronic payment transactions."

Article 18:

"1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.

2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:

(a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for 'remote electronic card-based payments' and 'remote electronic credit transfers' respectively;

(b) the amount of the transaction does not exceed the relevant exemption threshold value ('ETV') specified in the table set out in the Annex;

(c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:

(i) abnormal spending or behavioural pattern of the payer;

(ii) unusual information about the payer's device/software access;

(iii) malware infection in any session of the authentication procedure;

(iv) known fraud scenario in the provision of payment services;

(v) abnormal location of the payer;

(vi) high-risk location of the payee.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

(a) the previous spending patterns of the individual payment service user;

(b) the payment transaction history of each of the payment service provider's payment service users;

(c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;

(d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication."

3.6 Transaction processing

The different MCPP solutions in the market today use different models for the transaction processing. Below, the most common models will be briefly described.

Merchant-presented QR-code based MCPP solutions

Consumers are issued an MCPP application that has the capability to scan a merchant-Presented QR-Code and initiate a card payment transaction. This may be offered by the card issuer or a third party (MCPP service provider). In both cases, the request to process the card payment transaction is ultimately directed to the issuer that manages the consumer's card account from which the funds will be withdrawn.

The issuer receives the initial card payment transaction, and secures or withdraws the transaction amount from the consumer's account.

Upon receiving the card payment transaction, the acquirer checks the validity of the merchant account information and other merchant credentials and, when valid, credits the card payment transaction amount to the account associated with the merchant account information.

The merchant awaits notification of a successful transaction response before delivering the goods and services to the consumer.

The issuer or MCPP service provider issues a notification to the consumer (typically to their MCPP application).

The figure below illustrates the card transaction flow. Different message flows are possible between the entities involved, depending on type of MCPP application and/or wallet and the infrastructure supported by the card payment network. In the figure below, the combination of entities involved and the various message flows is jointly referred to as the "Network".

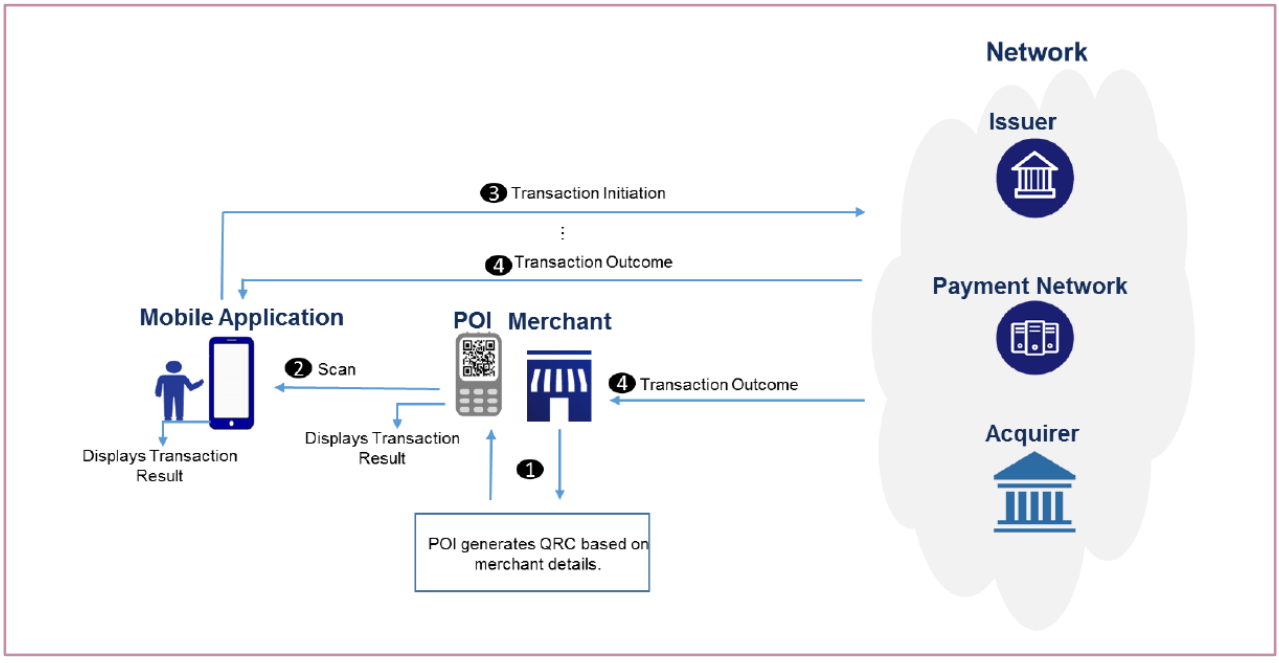

Figure 6: Merchant-presented mode transaction flow[12]

1. The merchant generates and displays a QR-code based on the merchant details.

[12] courtesy of EMVCo.

2. The consumer scans QR-code using an MCPP application on their mobile device to initiate the transaction, with CDCVM if required.
3. The MCPP application sends the transaction initiation request to the "Network".
4. The "Network" processes the transaction and informs the Merchant and the consumer of the transaction outcome.

Consumer-presented QR-code based MCPP solutions

In a Consumer-Presented Mode QR-code transaction, consumers can make purchases - using cardholder identification data or credentials associated with their card account and previously provisioned to their device - by selecting the QR-code option for payment within their MCPP application, which will result in the display of the QR-code, and having that QR-code scanned at the time of payment to complete the transaction.

These transactions are always authorised online and given that the scanning of the QR-code is a one-way transfer of data from the consumer's device to the POI, the payload of the QR-code does not contain any data from the POI.

While out of scope of this specification, in the event that any cardholder verification is required, it is envisaged that it would be performed through CDCVM. Thus, unlike typical EMV transactions, the requirement for CVM is never communicated, or delegated to the POI.

Note: Specific markets may have POI CVM requirements but those are out of scope of the present document (see also 3.2).

The processing of the transaction will depend on the content of the QR-code. If the QR-code only contains cardholder identification data, then the merchant will need to retrieve the card data using the cardholder identification and will process the transaction as a remote (card-on-file) transaction. If the QR-code contains chip card data, the transaction will be processed as an EMV on-line local card transaction (see [5]).

The figure below depicts the high-level solution architecture for QR-code payments processing. The components shown in the diagram are logical components that may map to different sets of implementation/physical components. The key objective of this diagram is to show the flow of QR-code data into the POI system and subsequently into the payment ecosystem. The diagram does not address other ecosystem components, such as provisioning of cardholder identification data or credentials, retrieving card data from cardholder identification data and consumer user interface/interactions on the mobile device before and at the time of checkout; or mobile platform, etc.

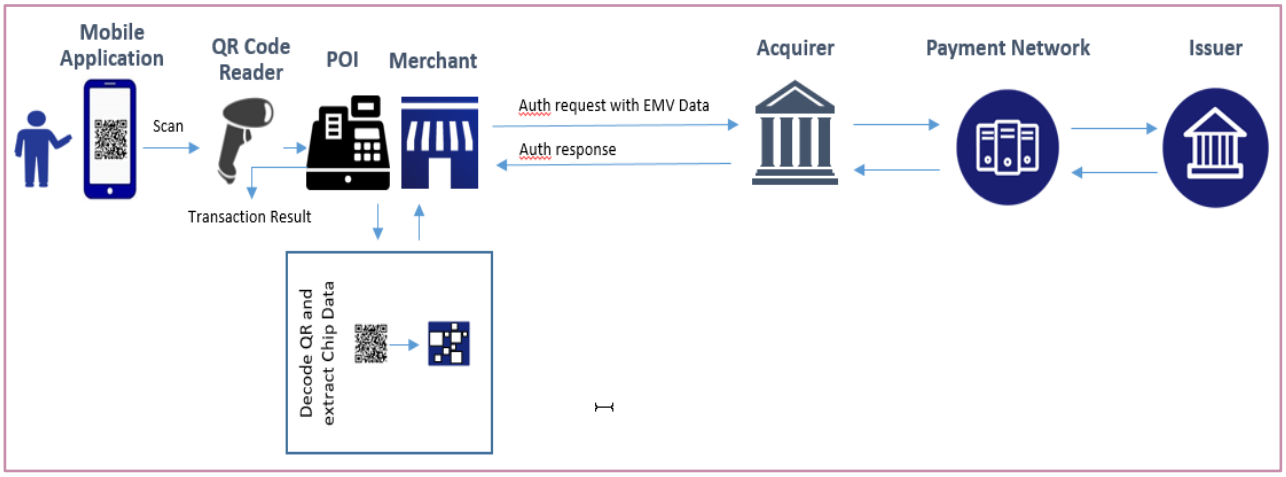

Figure 7: Consumer-presented mode transaction flow[13]

Merchant-presented QR-code and BLE based MCPP service provider solutions

This is a model based on a communication from both the MCPP app on the consumer's mobile device and the merchant's POI with the MCPP service provider back-end. Hereby both sides transfer dedicated transaction data to the MCPP service provider back-end system to enable the reconciliation of the transaction within this server.

Once the reconciliation has taken place and after the appropriate authentications, two options exist for the further processing of the remote card transaction:

- The MCPP service provider back-end system communicates the PAN and transaction data (including the transaction identifier) to the merchant's POI that initiates a card-on-file transaction or
- The MCPP service provider back-end system initiates an online authorisation to the issuer on behalf of the merchant / acquirer.

[13] courtesy by EMVCo.

4 POI characteristics

A “Point of Interaction” or POI is the initial point in the merchant’s environment where data is exchanged with the mobile device or where consumer data is entered (e.g. physical POI, QR-code on a poster, remote POI).

A physical POI consists of hardware and software which enables a consumer (cardholder) and/or a merchant to make a purchase involving a local card transaction. It is under the control of the merchant and may be attended or unattended. New generations of POI systems are designed to allow devices other than cards to be used to make payments (e.g. mobile phones or PDAs). A POI is capable of communicating with remote authorisation and clearing servers (see [5]).

The usage of proximity technologies such as QR-codes and BLE have an impact on the physical POIs.

For the usage of QR-codes in consumer-presented mode, there are two logical components needed on the merchant POI: the QR-code reader and the POI Application.

- The QR-code reader to scan the QR-code from the consumer’s mobile device, to decode the QR-code and to send the data recovered to the POI system. This data allows the identification of the consumer which is subsequently to be included in the authorisation request.
- The POI application to process the authorisation request. Its functions include decoding, parsing the data, checking content and format and transaction processing.

For the usage of QR-codes in merchant-presented mode, the merchant environment needs to generate and display a QR-code based on the merchant’s details. Those may also include transaction details such as the transaction identifier and transaction amount.

The QR-code may be static and shown on a poster or product. Dynamic QR-codes are typically generated and displayed by the POIs. They require a dedicated development by the POI vendor in the POI application to generate the QR-code at the time of the transaction. This QR-code is scanned by the consumer’s mobile device to initiate a card payment.

Contrary to the usage of QR-codes, the usage of BLE technology imposes both a hardware and/or software change to the POI for the integration of the BLE technology. To create a customer experience for BLE payments similar to that of NFC payments, the BLE transmission power at the POI must be extremely reduced to a power range of 5 cm - 10 cm. However, this relative strict restriction is not easy to achieve with standard BLE transmitter modules – such as those installed in POIs nowadays. Various boundary conditions, such as the concrete embedding of the modules and the integration environment of the POI strongly influence the field strength. As a result, power tuning must be controlled for a specific POI including its integration environment. A technical standardisation for such kind of BLE application is missing.

5 MCPP standards, specifications and white papers

MCPPs require the careful coordination of standards and specifications defined within several disciplines and issued by a heterogeneous group of industry bodies and global organisations. The most relevant are:

Bluetooth Special Interest Group (SIG)

The Bluetooth Special Interest Group (SIG) is a network of member organisations that are the caretakers and innovators of Bluetooth® technology. The standards organisation oversees the development of Bluetooth standards and the licensing of the Bluetooth technologies and trademarks to manufacturers. The SIG is a not-for-profit, non-stock corporation founded in September 1998 (www.bluetooth.com).

ECSG

The European Cards Stakeholders Group is a multi-stakeholder not-for-profit association supporting and promoting European card standardisation with market driven implementation. Its mission is to maintain and evolve the SEPA Cards Standardisation Volume [5] in line with market needs, reflecting the evolution of card payment technology, and to promote Volume conformance throughout the card payments value chain, to enable a more harmonised SEPA card payment ecosystem (www.e-csg.eu).

EMVCo

EMVCo exists to facilitate worldwide interoperability and acceptance of secure payment transactions. It accomplishes this by managing and evolving the EMV® Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Today there are EMV® Specifications based on contact chip, contactless chip, EMV® 2nd Generation, Common Payment Application (CPA), card personalisation, Payment Tokenisation, and 3-D Secure (www.emvco.com).

GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences (www.gsma.com).

ISO

The International Organization for Standardization (ISO) is a developer and publisher of International Standards. ISO has different committees which specify technical standards used in mobile payments such as standards for integrated circuit cards, QR-codes, communication protocols such as NFC, security mechanisms and is also is involved with mobile payments in ISO TC68 SC9 (www.iso.org).

PCI

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards,

including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. (www.pcisecuritystandards.org).

6 Challenges and opportunities

By analysing the different MCPP solutions that are currently available in the market, the following main challenges were identified. Here a special focus was given to both consumer and merchant experience. These challenges would need to be sufficiently addressed for a further SEPA-wide take-up of these solutions.

Challenges:

In various countries, the proximity solutions described in this document have been introduced by domestic card payment schemes, MCPP providers and retailers to be able to reach their consumers. However, because of the lack of standardisation, many different MCPP solutions exist in the market today. This means that consumers who would like to purchase across a range of merchants or cross-border may need to download many different MCPP applications on their mobile device in view of the proprietary implementations.

The usage of these proximity payment solutions also comes for the retailers with a cost for the adaptation of their card acceptance environment (e.g. the POI terminals). Here a distinction is to be made between the adoption of BLE technology at POIs that may require a hardware change versus the adoption of QR-codes which may only require a software update and, in case of support of the consumer-presented mode, a QR-code reader.

Recently, EMVCo has published dedicated specifications for the usage of QR-codes. However, it is to be noticed that many of the solutions available in the market today have a proprietary format. In view of the further take-up and interoperability of QR-code based mobile card payments, the migration to the EMVCo specifications needs to be addressed.

A QR-code code may be static, e.g., merchant account data and related payment details for a fixed transaction amount (typical use case of a transport ticket) or may be dynamic to initiate/identify a single mobile card transaction (e.g. at a POI).

Tampering QR-code data may lead to fraudulent transactions or data leakage. Therefore, the sensitive payment data in the QR-code should be adequately protected (e.g., through encryption and digital signature based on public-key cryptography, see [13]).

The integrity of the QR-code should always be checked if security mechanisms have been implemented (e.g. digital signature) and, if possible, the sensitive payment data retrieved could be checked against available data in the backend systems.

BLE is a potential alternative to NFC for electronic payments with mobile devices at the POI. Both transmission methods work bidirectional and have a sufficiently fast transmission rate.

BLE transmissions can be made secure against unauthorised intrusion if they are operated as a connection with multi-level dynamic key allocation. Static key assignment limits security. When the key is transmitted, exactly this part of the communication is particularly at risk, since only the successful exchange of the key protects a BLE connection.

Unlike NFC, with radio ranges of typically < 10 cm, BLE has ranges of many meters, depending on its range class. This causes practical problems for use at the POIs, as several mobile devices can be in the reception range of the POI. As a consequence, a card payment must be explicitly confirmed by the consumer on the mobile device once the connection has been successfully established – in other words, a "Tap & Go experience" is not possible. In comparison, NFC-based card payment avoids this problem because the connection and payment confirmation may be made by simply “tapping” the mobile device at the POI in a “single step”.

In analogy to NFC technology, the usage of the BLE technology for making proximity payments requires that the Bluetooth functionality on the consumer's mobile device is switched on, which should be handled by the MCPP app.

Finally, there is a lack of standardisation for the adoption of BLE technology for MCPPs (e.g. common specification for radio range on POI, transaction processing) and "common" customer experience guidelines.

Another challenge may occur when the POI supports multiple proximity technologies. In such an environment, the consumer's mobile device may perform a transaction over an unintended interface (e.g., consumer presented QR-code and in parallel an NFC-based transaction). However, this problem could potentially be avoided by appropriate implementation measures and will be further analysed by the ECSG.

Opportunities

Whilst there are challenges to implementing MCPP solutions as listed above, the introduction of these solutions also offers a number of opportunities to customers.

Since for some of these proximity payments, the initiation of the payment is based on data that allows the identification of the customer and reconciliation between the consumer and the merchant and/or the transaction may be done in a dedicated MCPP service provider backend system, an easy combination with a loyalty program or other services is made possible.

For some proximity payments, the initiation of the payment involves an exchange of data that allows the identification of a known customer with the merchant's backend system, allowing reconciliation with a merchant's loyalty program or other additional services.

The consumer identification can be used for instance to trigger the collection or redemption of loyalty points in combination with the payment transaction. This may provide value added benefits to retailers and their customer base.

The BLE technology is available on the majority of mobile phones. Almost all iOS and Android devices (as well as emerging platforms) support the technology. BLE also has the potential to eliminate line-ups at the check-out, giving customers the freedom to pay anywhere in-store.

As an example, a beacon could be installed at the entrance of a shop that identifies the consumer. If the consumer scans the goods they purchase using a dedicated MCPP app on their mobile device, the overall transaction amount could be displayed by the mobile device to the consumer once they have finished shopping. They could be subsequently invited on their mobile device to confirm the payment by entering a CDCVM. In addition, BLE beacons and sensors are able to form connections with more than one device at a time. Note however that the implementation of beacon-based solutions would need to take the GDPR requirements into account (see Annex A: Overview regulatory documents).

7 Conclusions

This document is conceived as a white paper providing a high level overview of non-NFC based mobile card proximity payments (MCPPs), whereby SEPA cards as specified in the Cards Standardisation Volume (see [5]) are the underlying payment instrument[14]. In view of the current market deployments, the document has been restricted to proximity payments based on QR-codes and Bluetooth-Low-Energy (BLE) technologies (see section 2.3). Next to use cases, the document provides some insights into transaction characteristics and the technology and infrastructure used for these payments.

Note that subjects such as business cases and revenue models for the MCPP value chain are in the competitive space and therefore are not addressed in this document.

While producing this document, the multi-stakeholder group noticed a number of gaps and challenges that are existing today and if properly addressed could encourage the market take-up of MCPPs (see section 6). Therefore, the multi-stakeholder group wishes to promote the following guidelines:

- Existing QR-based solutions should consider the migration to the EMVCo specifications (see [8], [9] and [10]) to enhance the interoperability of their solutions;
- New MCPP service providers should base their QR-based developments on the EMVCo specifications (see [8], [9] and [10]);
- Standardisation and industry bodies should further analyse the usage of the BLE technology for card payments and develop the appropriate technical standards and implementation guidelines to contribute to an enhanced, secure and harmonised customer payment experience.

Moreover, to achieve full interoperability in an open model with merchant-presented QR-codes, the relevant market participants are encouraged to work together to develop a common standard for the implementation of these payments.

The multi-stakeholder group further encourages MCPP service providers to take the following principles into account in their development to promote SEPA-wide non-NFC mobile card-based proximity payment solutions:

- To support European and even global interoperability, the usage of SEPA cards as specified in the SEPA Cards Standardisation Volume (see [5]) is recommended.
- The service models and infrastructures used for SEPA card payments should be leveraged as much as appropriate.
- Payment service providers (PSPs) should be able to differentiate their services offer with enough leeway such that the current effective competitive marketplace for payments is not hampered.
- Creating ease, convenience and trust for customers (consumers and merchants), using a mobile device to initiate an MCPP, should be regarded as critical for the further development within this area.

[14] Note that the use cases and service models introduced in these guidelines may also be applied outside SEPA.

- Consumers should be able to make MCPPs throughout SEPA, regardless of the original country where the MCPP service was subscribed to and/or issued.
- A consumer using a specific MCPP solution should have a similar experience at the POI throughout SEPA. However, this experience may slightly differ depending on the interface used (e.g., QR-code, BLE), existing infrastructure or other relevant environmental conditions (e.g., influenced by the risk management or POI type).
- Stakeholder (including consumers and merchants) payment liabilities should be clear, and in line with applicable regulations (see Annex A: Overview regulatory documents).
- PSPs should have the possibility to develop MCPP services on all the common mobile platforms[15] in the market openly (see [15]).
- The mobile device interface / wallet provider should enable the PSP to define the graphical interface to the consumer for its MCPP service, to support brands and logos, payment type, etc. as appropriate.
- Consumers should have the possibility for their MCPP services to switch mobile devices[16] and should not be bound to a specific MNO[17].
- Consumers should be able to use all the MCPP services offered by multiple PSPs using their mobile device[18].
- Consumers should be able to select the relevant MCPP service to be used for a particular proximity payment transaction, in line with the IF Regulation (see Annex A: Overview regulatory documents).
- All stakeholders involved in the MCPP ecosystem should comply with the mandatory provisions of relevant (EU) rules and regulations as applicable to them (see Annex A: Overview regulatory documents).

[15] Combination of different hardware and software on a mobile device.

[16] From different providers (including MNOs, handset manufacturers, OS providers, etc.) subject to appropriate agreements.

[17] Subject to appropriate agreements.

[18] Subject to appropriate agreements.

8 Annex A: Overview regulatory documents

The following regulatory documents apply in the context of MCPPs (non-exhaustive list):

[1]	Electronic Money Directive (EMD) Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision on the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=EN
[2]	4th Anti-Money Laundering Directive (AML4) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN
[3]	Interchange Fee Regulation (IF Regulation) Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=EN
[4]	Payment Services Directive (PSD2) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC	http://ec.europa.eu/finance/payments/framework/index_en.htm
[5]	Commission delegated regulation (EU) 2018/189 of 27 November 2017supplementing Directive (EU) 2015/2366 of the European Parliament and the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (also referred to as 'RTS')[19]	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC
[6]	General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection	http://ec.europa.eu/justice/data-protection/

[19] See also EBA-Op-2018-04: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, (https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf)

	of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC	
[7]	EBA/GL/2017/10 Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)	http://www.eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf
[8]	EBA/GL/2017/17 Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)	https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2/-/regulatory-activity/consultation-paper
[9]	EBA/GL/2018/05 Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2)	https://www.eba.europa.eu/documents/10180/2281937/Guidelines+on+fraud+reporting+under+Article+96%286%29%20PSD2+%28EBA-GL-2018-05%29.pdf/5653b876-90c9-476f-9f44-507f5f3e0a1e
[10]	ECB - Draft Recommendations for the security of mobile payments (draft document for public consultation)	https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf

Table 8: Overview regulatory documents

9 Annex B: The multi-stakeholder group

The following organisations have contributed to the update of this document through participation in the multi-stakeholder group

Banco Bilbao Vizcaya Argentaria (BBVA) - representing EPC
Bancontact on behalf of Febelfin - representing EPC
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR) - representing EPC
Cartes Bancaires - representing ECSG
Finance Denmark - representing EPC
Crédit Mutuel - representing EPC
DNB Bank - representing EPC
EMVCo
European Card Payment Association (ECPA)
IKEA - representing EuroCommerce
European Consumer Organisation (BEUC)
European Payment Institutions Federation (EPIF)
European Savings and Retail Banking Group (ESBG)
Eurosystem
Smart Payment Association (SPA) - representing ECSG
KPN
Mastercard
Verifone - representing ECSG
Visa

Table 9: The multi-stakeholder group

The multi-stakeholder group wishes to inform that this document is provided "as is" without warranty of any kind, whether expressed or implied, including, but not limited to, the warranties of merchantability and fitness for a particular purpose. Any warranty of non-infringement is expressly disclaimed. Any use of this document shall be made entirely at the user's own risk, and neither the multi-stakeholder group nor any of its members shall have any liability whatsoever to any implementer for any damages of any nature whatsoever, directly or indirectly, arising from the use of this document, nor shall the multi-stakeholder group or any of its members have any responsibility for identifying any IPR.

End of Document