European
Payments Council

[ ] Public – [ ] Internal Use – [x] Confidential – [ ] Strictest Confidence
Distribution: N/A

FINAL DRAFT

Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines

Abstract	This document provides guidance for the implementation of Mobile Contactless SEPA Card Payments
Document Reference	EPC144-17
Issue	Version 0.8
Date of Issue	6 October 2017
Reason for Issue	EPC Board approval for 3-months public consultation on the document

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.

This document defines the implementation guidelines for mobile contactless SEPA card payments (MCPs). It aims to reflect the current state of the art at the time of writing. However, it needs to be recognised that the MCP ecosystem is rapidly evolving with lots of new entrants in the market. Some of these solutions are proprietary today. Clearly, market adoption will determine the success of each of these new entrants.

Cross-industry cooperation on specifications, guidelines and best practices has been identified as a critical success factor in this area. Therefore, the EPC has facilitated the setting-up of a multi-stakeholder group covering the various sectors involved in the mobile payment ecosystem to develop this document.

It is recognised that MCPs are only covering a specific type of mobile proximity payments which are defined as *"A mobile payment where the consumer and the merchant (and/or their equipment) are in the same location and where the communication between the mobile device and the point of interaction device (POS terminal, vending machine, ATM, …) takes place through a proximity technology (e.g., NFC, 2D barcodes including QR codes, BLE, etc.)"*. However, as already mentioned in the ERPB report (see [25]), the European market is currently much less mature with respect to the usage of non-NFC based technologies for mobile payments and also the related standardisation efforts towards interoperability of these solutions are in their early days. As a consequence the current version of the document only covers MCPs[1], whereby SEPA card payments based on NFC technology, as specified in the Cards Standardisation Volume (see [4]), are the underlying SEPA payment instrument[2].

The guidelines focus on interoperability between the different stakeholders involved in the MCP ecosystem. In particular, they address the interoperability aspects related to the MCP application life cycle management. Furthermore, they cover some aspects of the technical interoperability of an MCP transaction, including a number of options, which are at the discretion of the MCP issuers and acquirers.

In this document, in order to reduce duplication and prevent conflicting requirements, the work produced by other standard and industry bodies in this area is extensively leveraged and referenced. The present document covers three types of Secure Elements

---

[1] Future work is planned by the multi-stakeholder group to deal with non-NFC mobile proximity card payments.

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

(SEs) in the mobile phone to store the MCP application, namely the UICC, the embedded SE and embedded UICC, in addition to HCE-based solutions.

The document endeavours to:

- Enable the quick development and implementation of mobile solutions.
- Avoid further fragmentation of the market for MCPs and promote SEPA reach.
- Provide transparency to market participants for MCPs by describing the roles of the stakeholders involved.

It is important to notice that the document only addresses the aspects of MCPs that reside in the co-operative space amongst the multi-stakeholder group. As such, the specification of business cases and a detailed analysis of the MCP value chain fall outside the scope of this document.

While producing this document, the multi-stakeholder group still noticed a number of remaining gaps and challenges that are existing today and if properly addressed could even further encourage the market take up of MCPs. Those include:

- Various standardisation and industry bodies have been involved in defining the appropriate specifications for MCPs but further standardisation is needed for HCE-based solutions to support the cloud-based models as well as for security requirements for new POI terminals such as PDAs, mobile phones, etc.

- One of the main challenges for MCP issuers remains the support of the different mobile platforms. Mobile devices have different operating systems with different execution environments which directly impacts the "secure" communication between different components in the device. Therefore, the development of specifications of a framework, referenced as a "Smart Secure Platform" (enabling the provision of value-added services relying on authentication of the user, regardless of the mobile device, communication channel and underlying technology) taking into account the requirements for mobile payments, hereby leveraging work already done by EMVCo and Global Platform, as requested to ETSI in [25] is of utmost importance.

- The adoption of contactless payments by certain sectors (e.g. mass transit) has proven to be an important catalyst and is even critical for their general take-up in various countries. The take-up of contactless payments in some sectors such as public administrations and the transport sector as recommended in [25] has been lacking behind in some countries.

- The dependency of the consumer on the type of mobile device with respect to the choice of MCP services. Therefore, access to the mobile device contactless interface in order to ensure that the consumer can have a choice amongst payment applications from different mobile payment providers, independently of the mobile device and the operating system used, should be ensured by all handset manufacturers and mobile OS developers (see [25]).

- The impact of the revised Payment Services Directive (PSD2) [2] with the RTS on strong customer authentication (see [6] in Annex A: Overview regulatory documents) and the IF Regulation (see [3] in Annex A: Overview regulatory documents) related to MCPs on the customer experience.

Although some of the issues mentioned above have already been identified in the ERPB report in 2015 [25], the multi-stakeholder group recognises that further work is needed as follow-up on the recommendations made in the report.

By developing these implementation guidelines, the multi-stakeholder group aimed to contribute to a competitive MCP market by providing the different stakeholders with an insight into the different service, technical and security aspects involved. The document could serve as a reference basis for making certain implementation choices.

In light of major new trends, and the rapidly changing market, it is recommended for the present document to be regularly updated. Therefore, the multi-stakeholder group aims to maintain the document to reflect the state of the art in light of major new trends and developments related to MCPs and to keep it aligned with the various documents referenced.

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 Contactless Card Payments (MCPs) related to the SEPA card payment instrument as well as the scope and the objectives of this document.
- Chapter 2 defines the high-level principles.
- Chapter 3 provides a short description of MCPs while introducing the different participants in the ecosystem. Additionally, it gives a high-level overview of the different phases involved in an MCP.
- Chapter 4 describes the different service models, along with their advantages and main challenges. The analysis takes into account the stakeholders involved in MCPs.
- Chapter 5 provides a description of the required processes for the life cycle management of an MCP.
- Chapter 6 is devoted to different aspects of the MCP application itself such as authentication, authorisation, cardholder verification and risk management. It also includes detailed descriptions of MCP use cases.
- Chapter 7 provides an overview on the overall MCP architecture and the different standard and industry bodies involved in the MCP ecosystem. Furthermore, it gives an insight into the technical infrastructure needed, including the different components in the MCP architecture.
- Overall conclusions on MCPs are made in chapter 8.
- Annexe A provides an overview of the relevant regulatory documents.
- Annexe B gives examples of MCP life cycle management for a number of models
- Annexe C describes examples of MCP life cycle use cases based on the process specified in section 5.
- Annexe D illustrates via an example the construction of the PPSE.
- Annexe E 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.

N°	Title	Issued 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 payments services in the internal market, amending Directives 2002/65/EC, 2009/110/EC	EC

	and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC	
[3]	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
[4]	ECSG 001-17 – SEPA Cards Standardisation Volume v8.0	ECSG
[5]	EMV Integrated Circuit Card Specifications for Payment Systems	EMVCo
[6]	EMV Contactless Specifications for Payment Systems, Books A-D	EMVCo
[7]	EMV Mobile Contactless Payment Technical Issues and Position Paper	EMVCo
[8]	The Role and Scope of EMVCo in Standardising the Mobile Payments Infrastructure (White Paper)	EMVCo
[9]	EMV Contactless Communication Protocol Specification	EMVCo
[10]	EMV Handset Requirements for Contactless Mobile Payment	EMVCo
[11]	EMV Contactless Mobile Payment Architecture Overview	EMVCo
[12]	EMV Contactless Mobile Payment – EMV Profiles of GlobalPlatform UICC Configuration	EMVCo
[13]	EMV Contactless Mobile Payment – Application Activation User Interface – Overview, Usage Guidelines and PPSE Requirements	EMVCo
[14]	EMV Contactless Mobile Payment – Software-based Mobile Payment Security Requirements	EMVCo
[15]	EMV Contactless Mobile Payment – PPSE and Application Management for Secure Element	EMVCo
[16]	EMVCo White Paper on Contactless Mobile Payment	EMVCo
[17]	EMVCo Security Evaluation Process	EMVCo
[18]	EMV Payment Tokenisation Specification version 2.0	EMVCo
[19]	EMV Contactless Mobile Payment - Payment Card Management (White paper)	EMVCo
[20]	EMVCo Contactless Symbol Reproduction Requirements	EMVCo

[21]	EPC 220-08: Mobile Contactless Payments Service Management Roles - Requirements and Specifications	EPC-GSMA
[22]	EPC 492-09: White paper Mobile Payments	EPC
[23]	EPC 178-10: Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines – edition 2011	EPC
[24]	EPC 163-13: White Paper Mobile Wallet Payments	EPC
[25]	ERPB Final report on Mobile and card-based contactless proximity payments	ERPB
[26]	ETSI TS 102 588: Technical Specification Smart Cards; Application invocation API by a UICC Web Server for Java Card Platform	ETSI
[27]	ETSI TS 102 622: Smart Cards; UICC – Contactless Front-end (CLF) interface; Host Controller Interface (HCI)	ETSI
[28]	ETSI TS 102 613: Smart Cards; UICC-CLF Interface; Physical and Data Link Layer Characteristics	ETSI
[29]	ETSI EN 301549: Accessibility requirements suitable for public procurement of ICT products and services in Europe	ETSI
[30]	Accepting contactless payments – A Guide for retailers	Eurocommerce
[31]	Towards a better payment experience	Eye Association Netherlands
[32]	GPC_SPE_034: Card specification + Amendments	GlobalPlatform
[33]	Confidential Card Content Management – Card Specification - Amendment A	GlobalPlatform
[34]	UICC Configuration	GlobalPlatform
[35]	Messaging Specification for Mobile NFC Services	GlobalPlatform
[36]	Card Specification - Amendment C Defines a mechanism for an end user to activate a contactless services when the card support multiple contactless applications	GlobalPlatform
[37]	Proposition for NFC Mobile: Secure Element Management and Messaging – White Paper	GlobalPlatform
[38]	GPC_SPE_031: Card – Composition Model	GlobalPlatform
[39]	GPD_SPE_009: TEE System Architecture	GlobalPlatform
[40]	GPS_GUI_006: End-to-End Simplified Service Management Framework for payment	GlobalPlatform

[41]	White paper: Ensure interworking between multiple Contactless Card Emulation Environments	ETSI - GlobalPlatform - NFC Forum
[42]	GPC_SPE_114: Multiple Contactless Card Emulation Environments – Managing Entity	GlobalPlatform
[43]	Pay-Buy-Mobile Initiative: Requirements for Single Wire Protocol NFC Handsets	GSMA
[44]	Mobile NFC Services White Paper	GSMA
[45]	NFC Technical Guidelines White Paper	GSMA
[46]	Pay-Buy-Mobile Initiative: Business Opportunity Analysis – Public White Paper.	GSMA
[47]	HCE and Tokenisation for Payment Services - Discussion paper	GSMA / Consult Hyperion
[48]	The Mobile Economy 2017	GSMA
[49]	SGP.02 V3.2: Remote Provisioning Architecture for Embedded UICC Technical Specification	GSMA
[50]	World Telecommunication/ICT Indicators Database 2015 (19th Edition)	ITU
[51]	White Paper - Alternatives for Banks to offer Secure Mobile Payments	Mobey Forum
[52]	White Paper - Business models for NFC payments.	Mobey Forum
[53]	Mobile wallet – Parts 1-5	Mobey Forum
[54]	The Host Card Emulation in Payments - Options for Financial Institutions	Mobey Forum
[55]	ISO 12812: Core banking - Mobile financial services - Parts 1-5	ISO
[56]	ISO/IEC 7812: Identification cards - Identification of issuers	ISO
[57]	ISO/IEC 7816-4: Identification cards — Integrated circuit cards, Part 4: Organisation, security and commands for interchange	ISO
[58]	ISO/IEC 14443: Identification cards - Contactless integrated circuit cards - Proximity cards - Parts 1-4.	ISO
[59]	ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems -- Near Field Communication - Interface and Protocol (NFCIP-1).	ISO
[60]	NFC Activity Technical Specification	NFC Forum
[61]	NFC Digital Protocol Technical Specification.	NFC Forum

[62]	NFC Controller Interface (NCI) Specifications	NFC Forum
[63]	Digital Payments Solutions Industry Considerations	The UK Cards Association

Table 1: Bibliography

0.3 Definitions

Throughout this document, the following terms are used. Their definitions are based on [2], [4] and [55].

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: - Something you know, such as a password, PIN or passphrase - Something you have, such as a token device or smart card - Something you are, such as a biometric.
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 data consists of the PAN and other data elements.
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 Security Code (CSC)	A data element that protects the integrity of the card data.

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.
Contactless Technology	A radio frequency technology operating at very short ranges so that the user has to perform a voluntary gesture in order that a communication is initiated between two devices by approaching them. It is a (chip) card or mobile payment acceptance technology at a POI device which is based on ISO/IEC 14443 (see [58]).
Customer	A payer or a beneficiary which may be either a consumer or a business (merchant).
Credential(s)	Payment account related data that may include a code (e.g., mobile code), provided by the PSP to their customer for identification/authentication purposes.
2D barcodes	A two dimensional barcode is a machine-readable optical label that contains digital information. They are also referred to as matrix barcodes. Examples include QR codes and tag barcodes.
Digital wallet	A service accessed through a consumer device which allows the wallet holder to securely access, manage and use a variety of services/applications including payments, identification and non-payment applications (e.g., value added services such as loyalty, couponing, etc.). A digital wallet is sometimes also referred to as an e-wallet.
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.
Merchant	The beneficiary within a mobile payment scheme for payment of the goods or services purchased by the consumer. The merchant is a customer of their PSP.
Mobile code	An authentication credential used for user verification and entered by the consumer via the keyboard of the mobile device.
Mobile Contactless Payment (MCP)	A mobile proximity payment where the payer and the payee communicate directly using contactless technologies.
Mobile device	Personal device with mobile communication capabilities such as a telecom network connection, Wi-Fi, Bluetooth, etc. Examples of mobile devices include mobile phones, smart phones, tablets.
Mobile equipment	The mobile phone without the UICC (also referred to as mobile handset).
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 Contactless Payment (MCP) Application	A set of modules (application software) and/or data (application data) needed to provide functionality for a mobile contactless payment service as specified by the mobile contactless payment application issuer in accordance with the Card scheme.
Mobile Payment Application user interface	The user interface of a mobile payment application.
Mobile Proximity Payment (MPP)	A mobile payment where the consumer and the merchant (and/or their equipment) are in the same location and where the communication between the mobile device and the Point of Interaction device takes place through a proximity technology (e.g., NFC, 2D barcodes, BLE, etc.).
Mobile 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 specified by ISO/IEC 18092 [59].
Payment Application Selection User Interface	The mobile phone user interface (component) enabling the consumer to • Access the MCP application User Interface on the mobile phone • Select the preferred payment application.
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 device	"Point of Interaction" device; the initial point where data is read from a consumer device or where consumer data is entered in the merchant's environment. As an electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a consumer to perform a payment transaction. The merchant controlled POI may be attended or unattended. Examples of POI devices are POS, vending machine, ATM.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC and which allows, when enabled, the access to a specific mobile network infrastructure.
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 [56].
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 three different form factors of SE: Universal Integrated Circuit Card (UICC), embedded SE (including eUICC) and microSD. Both the UICC and microSD are removable.
Secure Element (SE) Provider	A TTP which owns the original access rights to the SE. Typical examples are MNOs and mobile device manufacturers.
(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. Examples include the EMVCo Token, see [18].
(Payment) Token Requestor	An entity requesting a token to the Token Service
(Payment) Token Service	A system comprised of the key functions that facilitate generation and issuance of payment tokens, and maintain the established mapping of payment tokens to the payer account related data when requested by the token requestor. It may also include the capability to establish the token assurance level to indicate the confidence level of the payment token to the payer account related data / payer / merchant / device / environment binding. The service also provides the capability to support token processing of payment transactions submitted using payment tokens by de-tokenising the payment token to obtain the actual account related data.
(Payment) Token Service Provider (TSP)	An entity that provides a Token Service.
Security Domain	On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the MCP issuer, the MNO or a third party.
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]).
Third Party	This is an entity in the ecosystem that is different from an MNO or an MCP issuer (e.g. TSM, card manufacturer, …).
Trusted Execution Environment (TEE)	A separate execution environment (as defined by Global Platform, see [27]) that runs alongside, but isolated from the main operating system. A TEE has security capabilities and meets certain security-related requirements: it protects TEE assets from general software attacks, defines rigid safeguards

	as to data and functions that a program can access, and resists a set of defined threats.
Trusted Platform Module (TPM)	A secure crypto processor (which is a dedicated microprocessor) that securely stores features used to authenticate a computer platforms such as PC, laptop, or mobile device. These features can include passwords, certificates, or encryption keys. The TPM can also help to ensure that the platform remains trustworthy.
Trusted Service Manager (TSM)	A trusted third party acting on behalf of the SE provider and/or the MCP application issuer in case an SE is involved to host the MCP application(s).
Trusted Third Party (TTP)	An entity which facilitates interactions between stakeholders of the ecosystem who all trust this third party (examples are SE provider, TSM, common infrastructure manager…).
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.
UICC	Universal Integrated Circuit Card - A generic and well standardised SE owned and issued by the MNOs.

Table 2: Terminology

0.4 Abbreviations

Abbreviation	Term
AAM	Active Account Management
API	Application Programming Interface
ATC	Application Transaction Counter
ATM	Automated Teller Machine
BIN	Bank Identification Number
BLE	Bluetooth Low Energy
CASD	Controlling Authority Security Domain
CBP	Cloud-based Payments
CBPP	Cloud-based Payments Platform
CDA	Combined Data Authentication
CDCVM	Consumer Device CVM
CVM	Cardholder Verification Method
2D barcode	Two dimensional barcode

DAP	Data Authentication Pattern
DCS	Domestic Card Scheme
DDA	Dynamic Data Authentication
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
FCI	File Control Information
FIDO Alliance	Fast IDentity Online Alliance
GDPR	General Data Protection Regulation
GP	Global Platform
GSMA	The GSM Association
HCE	Host Card Emulation
ICS	International Card Scheme
IF regulation	Interchange Fee regulation
IIN	Issuer Identification Number
IPR	Intellectual Property Rights
ISD	Issuer Security Domain
ISO	International Organization for Standardization
LCM	Lifecycle Management
MA	Mobile Application
MACP	Mobile Application Cloud Platform
MCP	Mobile Contactless Payment
ME	Mobile Equipment
MNO	Mobile Network Operator
NFC	Near-Field Communication
OS	Operating System
OTA	Over the Air
PAN	Primary Account Number
PAR	Payment Account Reference
PCM	Payment Card Manager

POI	Point of Interaction
POS	Point of Sale
PPSE	Proximity Payment System Environment
PSD	Payment Services Directive
PSP	Payment Service Provider
QR code	Quick Response code
REE	Rich Execution Environment
RFID	Radio Frequency Identification
RTS	Regulatory Technical Standard
SD	Security Domain
(micro) SD (card)	micro Secure Digital card
SE	Secure Element
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMR	Service Management Role
SPA	Smart Payment Association
SSD	Supplementary Security Domain
SP	Service Provider
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
TSM	Trusted Service Manager
TSP	Token Service Provider
TP	Third Party
TTP	Trusted Third Party
UI	User Interface
UICC	Universal Integrated Circuit Card

Table 3: Abbreviations

0.5 Maintenance Process

The EPC has established a dedicated multi stakeholder group (see Annex E: The multi-stakeholder group) for the development of this document. This multi stakeholder group aims to regularly update the document to reflect the state of the art in light of major

new trends and developments related to MCPs and to keep it aligned with the various documents referenced.

1 General

1.1 Introduction

In March 2017, the EPC published the last edition of a white paper [22], which provides a high-level description of mobile payments in general covering mobile proximity and mobile remote payments.

This document is aimed at readers who require more detail on implementation guidance for mobile contactless card based payments (MCPs) covering business, technical, security and legal aspects.

This current document, defining the implementation guidelines for MCPs aims to reflect the current state of the art at the time of publication. However, it needs to be recognised that the MCP ecosystem is rapidly evolving with a lot of new entrants in the market. New developments include Android Pay, ApplePay, Samsung Pay, PayPal, social platforms such as Twitter and its Twitpay linked to PayPal, etc.. Nevertheless many of these solutions are proprietary today. Clearly, market adoption will determine the success of each of these new entrants.

Cross-industry cooperation on specifications, guidelines and best practices has been identified as a critical success factor in this area. Therefore the EPC has 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 this document, while leveraging the relevant documentation developed in standardisation and industry bodies.

This document replaces EPC 178-10v2.0 [23].

1.2 Vision

This document subscribes to the vision specified in the ERPB report on Mobile and card-based contactless proximity payments (see [25]) 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, user-friendliness, better integration of value added services with payment – and to cost-effectiveness for society.

The guidelines aim to contribute to the creation of the necessary environment so that service providers, cards schemes, manufacturers and other stakeholders involved in the mobile ecosystem can deliver secure, efficient and user-friendly MCP solutions, in an integrated market.

The document contributes to the development of this integrated market for payments through the development and promotion of standards and guidelines.

1.3 Scope

The guidelines focus on interoperability between the different stakeholders involved in the MCP ecosystem in the co-operative space. In particular, they address the interoperability aspects related to the MCP application life cycle management. Furthermore, they cover some aspects of the technical interoperability of an MCP transaction, including a number of options, which are at the discretion of the MCP issuers and acquirers.

It is recognised that MCPs are only covering a specific type of mobile proximity payments which are defined as "A mobile payment where the consumer and the merchant (and/or their equipment) are in the same location and where the communication between the mobile device and the point of interaction device (POS terminal, vending machine, ATM, …) takes place through a proximity technology (e.g., NFC, 2D barcodes including QR codes, BLE, etc.)". However, as already mentioned in the ERPB report (see [25]), the European market is currently much less mature with respect to the usage of non-NFC based technologies for mobile payments and also the related standardisation efforts towards interoperability of these solutions are in their early days. As a consequence the current version of the document only covers MCPs[3], whereby SEPA card payments based on NFC technology, as specified in the Cards Standardisation Volume (see [4]), are the underlying SEPA payment instrument[4].

More specifically, the document aims to provide information related to the following points:

- A description of MCP use cases;

- The roles for the main stakeholders in the MCP ecosystem;

- The service model alternatives for MCPs;

- How can interoperability between the various stakeholders, within the same service model, be ensured?

- The main architectures for MCP.

---

[3] Future work is planned by the multi-stakeholder group to deal with non-NFC mobile proximity card payments.

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

- How to implement MCP applications on the same mobile device – mobile wallet concept and what are the technical solutions available?

- The impact of new rules and regulations (PSD2 and RTS, GDPR, IF Regulation). What does the collective industry (existing incumbents) expect with respect to a consistent customer experience?

- The main technical and security issues and the related dependencies impacting the service model.

- Some aspects for the evaluation and certification processes.

- The main industry/standardisation bodies involved and their focus.

Finally, it is important to notice that the document only addresses the aspects of MCPs, which reside in the co-operative space of the stakeholders in the MCP value chain. As such, the specification of business cases and a detailed analysis of the MCP value chain fall outside the scope of the document.

1.4 Objectives

The purpose of this document is to provide interoperability implementation guidelines for MCPs.

In order to achieve this the document will

- Provide guidelines so that all deployed operational and transactional processes directly related to MCPs can be implemented while facilitating compliance with the relevant legal regulations (e.g., PSD2, IF Regulation, GDPR, etc.).

- Describe how all deployed MCPs can be implemented while maintaining appropriate methodologies for risk management, supporting adaption to prevent fraud.

- Ensure that MCPs achieve an adequate level of interoperability.

- Enable a harmonised consumer experience across Europe for MCPs at the POI.

- Provide guidance for the implementation of MCPs which is complementary to the existing technical specifications and standards developed by standardisation and industry bodies in the NFC ecosystem, especially to the SEPA Cards Standardisation Volume (see [4]).

1.5 Audience

The document is primarily intended for the payment industry. It aims to create awareness amongst this industry about the various aspects to be considered in the

development of MCP solutions. The aim is also to help new entrants to understand where are the risks, which aspects may become problematic in order to create / maintain an adequate level of trust in MCPs. It could further be used as a reference by the payment industry to address users (consumers and merchants) for a cohesive payment experience.

It aims to provide information to stakeholders involved in implementations and deployment of MCPs, including:

- Payment Service Providers;

- Card schemes;

- Other service providers such as (TSMs, MNOs, EMV Payment Tokenisation Providers, etc.);

- Equipment manufacturers;

- Merchants and merchant organisations;

- Consumers;

- MCP application developers;

- Regulators;

- Standardisation and industry bodies.

2   High-level principles

The following high-level principles have been employed for the specification of these guidelines. They represent a more elaborate version of those contained in the EPC's White paper Mobile payments (see [22]) with a special emphasis on MCPs.

1. To support the need for European and global interoperability, the usage of SEPA cards as specified in the SEPA Cards Standardisation Volume (see [4]) is assumed.

2. The service models and infrastructures used for SEPA card payments should be leveraged as much as appropriate.

3. 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.

4. Creating ease, convenience and trust for end-customers (consumers and merchants), using a mobile device to initiate an MCP, is regarded as critical for the further development within this area.

5. Consumers shall be able within SEPA wide schemes to make MCPs throughout SEPA, regardless of the original country where the MCP application was subscribed to and / or issued.

6. A consumer using a specific card product should have a similar experience at the POI throughout SEPA. However, this experience may slightly differ depending on the existing infrastructure or other relevant environmental conditions (e.g., influenced by the risk management or POI type).

7. Stakeholder (including consumers and merchants) payment liabilities should be clear, and in line with applicable regulations (see Annex A: Overview regulatory documents.

8. PSPs should have the possibility to develop MCP services on all the common mobile platforms[5] in the market openly (see [25]).

9. The mobile device interface / wallet provider should enable the PSP to define the graphical interface to the consumer for its MCP service, including brands and logos, card scheme brands, payment type, etc. as appropriate.

10. Consumers should have the possibility for their MCP services to switch mobile devices[6] and should not be bound to a specific MNO.

---

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

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

11. Consumers should be able to use all the MCP services offered by multiple PSPs using their mobile device[7].

12. Consumers should be able to select the relevant MCP service to be used for a particular contactless payment transaction.

13. All stakeholders involved in the MCP ecosystem should comply with the applicable regulations (see Annex A: Overview regulatory documents).

---

[7] subject to appropriate agreements.

EPC144-17 v0.8 Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines

3   MCP Overview

3.1   Introduction

This section provides a short, high-level description of an MCP, which is defined as a Contactless SEPA Card Payment (see [4]) executed by a cardholder over NFC using a dedicated MCP application accessed via a mobile device.

As illustrated in the following figure, the main parties involved in an MCP do not differ from when a physical contactless card is used to perform a SEPA card payment. The payment transaction is performed by reusing the existing SEPA contactless card payments accepting devices and transaction infrastructure. When the MCP application is an SE-based application, the back-end will be that already used for SEPA card payments (blue shaded), while for HCE based implementations, the issuers back end systems will be required to support cloud-based functions (as described in section 4). Note however that the latter is transparent for all other stakeholders in the MCP ecosystem.

As illustrated in the figure below, the following participants are involved in the MCP ecosystem:

- The acquirer is a payment service provider enabling the processing of the merchant's transaction to the MCP issuer through an authorisation and clearing network.

- The card payment scheme is 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 (an MCP in the context of this document).

- The consumer has an agreement with an MCP issuer for MCP services. The consumer is required to have an NFC-enabled mobile device.

- The (MCP) issuer, is a payment service provider providing the MCP service to the consumer in compliance with regulatory / security requirements. The issuer is responsible for the provisioning of the MCP application (directly or indirectly) and the personalisation of the application with consumer's data. Furthermore, the issuer is also responsible for other MCP application life cycle management aspects.

- The merchant is accepting an MCP transaction for the goods or services purchased by the consumer; the merchant has an agreement with an acquirer and shall be equipped with a contactless Point of Interaction (POI) device.

- The MNO offers data connectivity to the consumer and potentially other services.

Further participants in the MCP ecosystem are discussed in section 3.4.
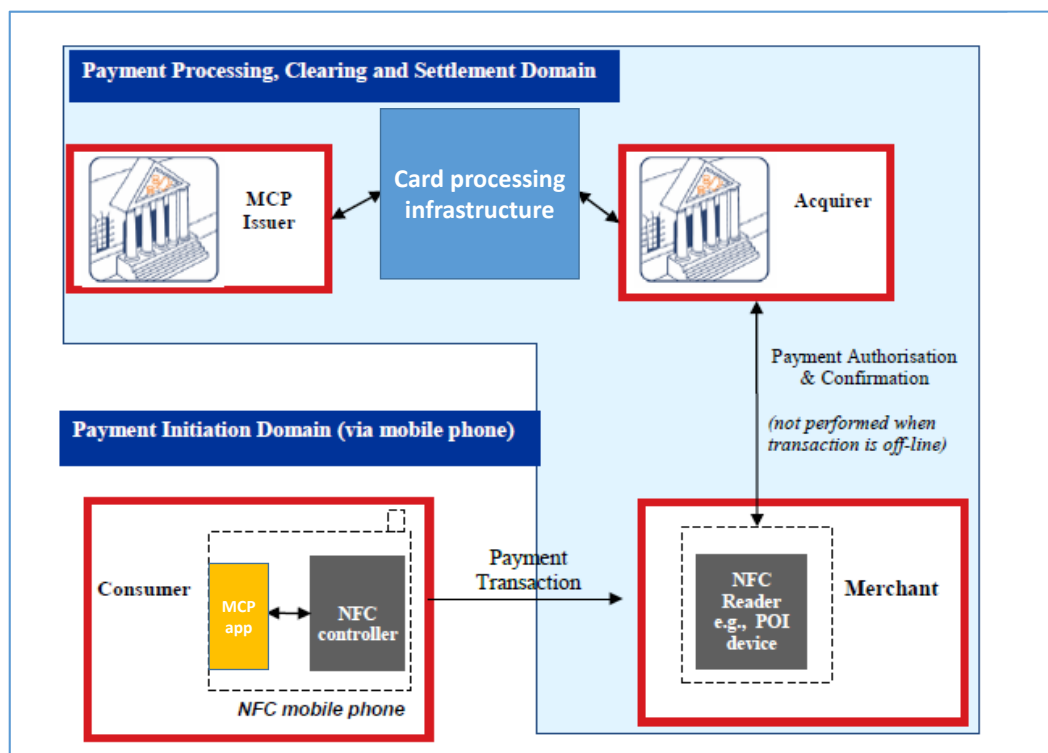
Figure 1: MCP Transaction

Notes:
- Components within the blue shaded area are similar to contactless card payments.
- Parts of the MCP application may reside in the cloud (see chapters 4, 5 and 7).

For a proper MCP service management it is important to distinguish between the following two phases related to an MCP:

- The provisioning and life cycle management of the MCP application.
- The MCP transaction.

A short description of each of these phases is provided below.

3.2 Provisioning and life cycle management

The MCP application is defined as a set of modules (application software) and /or data (application data) needed to provide functionality for an MCP service as specified by the MCP issuer in accordance with the card scheme. The MCP application is accessed via the mobile device. This implies that dedicated processes need to be defined for the provisioning and management of the MCP application, which may vary depending on service model chosen (e.g., SE-based, HCE-based, see section 4). Although, the provisioning of the MCP application represents a change to the issuer's value chain,

existing card data preparation systems can be leveraged for the personalisation of the MCP application.

As an example, the figure below provides an overview for the provisioning and maintenance of an MCP application on an SE residing on a mobile device. Although this figure depicts a TSM (see section 3.4), this entity might be omitted from these processes depending on the actual implementation. The MCP issuer may use fulfilment methods that do not require TSM services, and use in-house or third party systems for certain services.
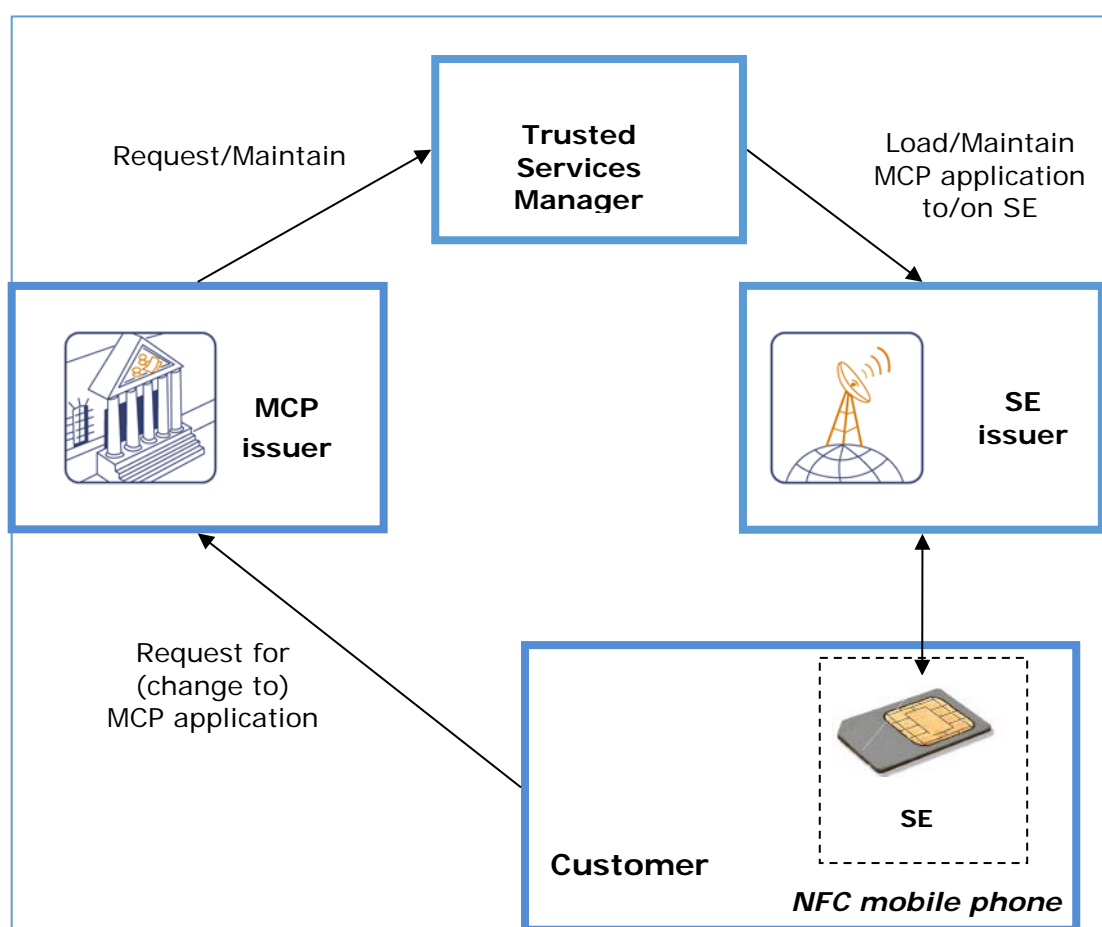
Figure 2: Provisioning/maintenance of MCP application on an SE

Further guidance on the different processes involved in the provisioning and maintenance of the MCP application is provided in section 5.

3.3 MCP Transaction

MCP transactions are designed to use the existing EMV contactless card payment infrastructure, emulating EMV contactless card transactions. However, there are some differences in the MCP implementation, examples of which include the support of CDCVM, or the use of the mobile device screen to display the transaction amount. Therefore, the document will mainly focus on the interaction between the mobile device and the POI device (see yellow area in the figure below).
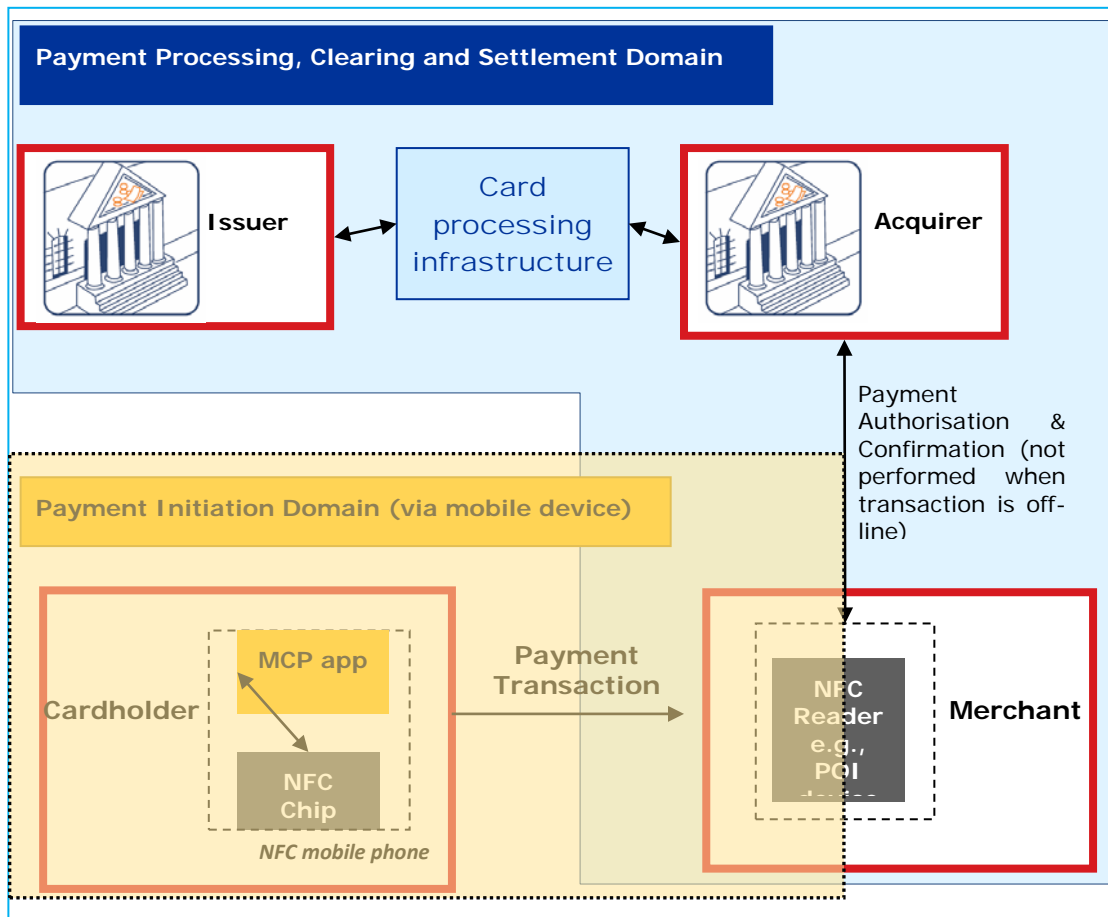
Figure 3: MCP Transaction

Further details on the different aspects of an MCP transaction are provided in section 6.

3.4 The stakeholders in the MCP ecosystems

MCPs alter existing ecosystems involving some new stakeholders in the value chain compared to physical card payments. Although the main participants involved in an MCP transaction do not differ from those in a physical card payment, MCPs need to rely on a series of technical infrastructure elements that are unique to the mobile environment.

Some years ago, specific guidance has been developed for the roles covering the functions related to MCPs. In order to facilitate the introduction of an interoperable ecosystem of service providers performing TSM functions, the EPC and the GSMA had jointly developed requirements and specifications for the MCP service management roles for MCP applications residing on a UICC, see [21]. Many service models are possible by delegating combinations of the different roles (technical and commercial) to one or more TSMs. The service management roles for other types of SEs (see Annex II in [22]) and their related service models are described in section 5 and Annex B: Overview life cycle management processes for MCP models.

However, due to the introduction of HCE based solutions and tokenisation during recent years, new stakeholders have been introduced in the MCP ecosystem which fulfil specific roles in the provisioning and life cycle management of an MCP application. More guidance on these new models are provided in sections 4 and 5 and in [18], [47] and [54] .

The following stakeholders, in addition to the ones described in section 3.1 may be involved:

- The SE provider is a key stakeholder in the ecosystem if the MCP application is stored in an SE on the mobile device. This is the MNO in case of a UICC, the mobile equipment manufacturer, the MCP issuer or a third party in case of an embedded SE, (see section 4).

- The Trusted Service Manager (TSM) is a TTP acting on behalf of the SE providers and/or the MCP application issuers to facilitate an open ecosystem where an SE is involved in hosting the MCP application(s). As illustrated in the figure above, MCP issuers, TSMs and SE providers collaborate to perform the provisioning and management of the MCP application(s). Several TSMs may co-exist offering competing services both to the SE and MCP issuers.

- The Token Service Provider (TSP) is a TTP who is involved if payment tokens are used in MCPs as surrogate values for the PANs (see [18]). The TSP manages the generation and issuance of payment tokens, and maintains the established mapping of payment tokens to the payer account related data when requested by the token requestor. The TSP service may also include the capability to establish the token assurance level to indicate the confidence level of the payment token to the payer account related data / payer / merchant / device / environment binding. The TSP also provides the capability to support token processing of payment transactions submitted using payment tokens by de-tokenising the payment token to obtain the actual account related data.

- The Mobile Wallet Issuer is a service provider that issues mobile wallet functionalities to the customer (consumer or merchant).

- Other relevant new stakeholders include for example:
  - SE manufacturers,

- Cloud service providers (which may be the MCP issuer themselves or the issuer may delegate this service to a TPP),
- Application developers (MCP application, AAUI, mobile wallet …),
- Mobile Operating System suppliers,
- Mobile equipment manufacturers,
- Organisations performing infrastructure certification (e.g., SEs, MCP applications, POI, etc.).

At this stage, with the large number of stakeholders involved, alignment around key aspects of the ecosystem is crucial to move from fragmentation to harmonisation and to enable the development of SEPA-wide service offerings.

Numerous market studies available show that, besides strong market potential, mobile payments have really taken off (see for instance [48]). The major elements supporting a rationale for service providers to enter the mobile payments market include the following:

- Strong penetration of mobile devices: mobile phones have achieved full market penetration[8] with enriched technology and service levels. More in particular in Europe, nowadays, "smart phones" have become a commodity[9]. Therefore, they are an ideal channel for increasing the usage of SEPA payment instruments. Moreover, more and more consumers are ready and are willing to use the mobile device for payments.
- The usage of the mobile device for payments allows to enhance the consumer purchase experience through value-added services such as loyalty, couponing, e-receipts, etc.
- Provisioning of user convenience by meeting proven needs of both consumers and merchants.
- The quick evolution and adoption of technology during the recent years.
- The need to foster innovation with competitive offerings to the customer's benefit in a more complex ecosystem including new stakeholders, thereby growing the market for non-cash payments and migrating consumers to faster, more efficient and more convenient means of payments.

As mentioned above, it is not the purpose of this paper to discuss the strategy for which a service provider may enter the market and the concrete service models including the various interactions among the different stakeholders in the value chain. However, a high-level description of various service models is presented in chapter 4.

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

---

[8] The number of active mobile devices and human beings crossed over somewhere around the 7.19 billion mark (see http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html)

[9] See https://www.statista.com/statistics/494554/smartphone-users-in-western-europe/

Consumers' expectations and demands

- Efficiency: speed of payment initiation, frictionless;
- Convenience and mobility: make cashless payments anywhere, anytime;
- Consistent consumer experience;
- Simplicity for enrolment and to conduct a payment;
- Confidence and trust;
- Privacy and data protection;
- Wide merchant acceptance of MCPs.

Note that value added services such as special offers or loyalty points are also part of consumers' expectations but are out of the scope of this document according to the focus on the payment transaction. However, for illustrative purposes a dedicated use case is described in chapter 6.

Merchants' expectations

- Quick, efficient and secure process at point of payment;
- Resilience (zero downtime);
- Cost effective;
- Consumer focused: The payment process needs to be a convenient, simple process, easily understood by consumers who can see the benefits and "want to use it";
- Confidence and trust in the end to end process by both consumers and merchants;
- Guarantee of payment: Either immediate payment or confirmation and/or assurance of payment to enable immediate release of goods or services to the consumer;
- Desire for cash displacement and in some countries paper cheque displacement;
- Reachability of consumers through any mobile device (interoperability);
- Easy to implement and quick to market;
- Optionally, subject to consumer consent, the provision of related additional services through consumer payment data collection to enable cross-selling and geo-based marketing services.

Service providers' expectations

- Customer retention/acquisition;
- Cost efficiency;
- Risk reduction / improved monitoring;
- Provision of related additional services;
- Desire for "cash displacement" and, in some countries, "cheque displacement";
- Compliance with regulations.

Card scheme expectations

- Equivalent levels of security compared to contactless card transactions;

- Adoption of the current acceptance infrastructure;
- Maintain the speed and convenience of the contactless card experience for consumers.

Clearly, the mobile device will be an additional payment initiation channel co-existing with other channels and means of payment. Other alternatives exist and the payments business is not limited to SEPA's geographical scope.

4   Service Models

This chapter provides an overview on the service models for the provisioning and life cycle management of the MCP applications. Hereby a distinction is made between SE-based and cloud-based models.

4.1   SE-based MCP Applications

The Service models for the provisioning and life cycle management of the MCP applications depend on the type of SE that the MCP issuer implements. As previously mentioned, three alternatives for SEs are being adopted by the market to host the MCP application:

- The removable UICC, which contains an SE;
- The embedded SE (eSE), a secure component which is integrated in the mobile phone at the time of manufacturing;
- The embedded UICC (eUICC) - which is integrated in the mobile phone at the time of manufacturing – and contains an SE;

The removable UICC

The removable UICC or SIM is present in almost every mobile phone in the world. The UICC contains the MNO operator profile which is used to connect the phone to the network. This MNO profile is created at the factory and cannot be changed. In this model, in addition to the MNO profile, an SE element is also located on the UICC. This SE is capable of secure application management and may host applications from other service providers such as the MCP application.

The embedded SE (eSE)

The embedded SE is a specific hardware component that is embedded in a mobile device by the manufacturer (OEM), and can hold applications in secure domains like e.g., the MCP application. The control of the SE initially lies with the manufacturer. In most cases the eSE exists besides a (removable) UICC.

The embedded UICC (eUICC)

As of mid-2017 a new form factor of the UICC has become available. The embedded UICC (eUICC), specified by the GSMA (see [49]) is a new hardware version of the traditional UICC, which may also contain an SE. The main difference with the traditional UICC is that this eUICC is not provided in advance with an MNO profile. The MNO of choice is selected by the consumer at the time of purchasing the mobile phone, after which the specific MNO profile is loaded over the air. The same also applies for the SE. An eUICC can even hold multiple MNO profiles at a time, with only one single MNO profile being active at any point in time. This active profile determines the behavior of the eUICC and thus the mobile phone.

It is expected that the eUICC will eventually replace the UICC but both are likely to co-exist for a number of years.

For a period of time the industry trialled the use of a removable micro SD card to house an SE. They appeared to be a good technical "bridging" solution because of their quick time to market and straightforward business model. However, other challenges, such

as cost, lack of standards and specifications, reliance on availability of specific mobile hardware, as well as technical issues impacting performance has meant that this type of implementation has not proven to be popular. Because of this, this type of SE will not be discussed further.

Although multiple SEs (of various types) may be present in the mobile phone (see [19] and section 7.3.2), for simplicity the presence of only one SE that hosts (an) MCP application(s) will be considered in this chapter.

In view of the control that the issuer of the SE has in the ecosystem, the choice of the SE has an impact on the roles and responsibilities of the various stakeholders.
Based on the type of SE chosen by the MCP issuer, the Service Models are defined below, focusing on the co-operative domain.

Four business scenarios have been selected based on the three different SE types.

Scenario	SE Type	SE issuer	MCP issuer
1	UICC	MNO	Issuing PSP
2a 2b	Embedded SE (eSE)	Mobile equipment manufacturer Third party (e.g. TSM or other TP including MNO)	Issuing PSP Issuing PSP
3	eUICC	MNO[10]	Issuing PSP

Table 4: SE types

For each of the four selected service scenarios in this chapter, it is intended to:

- Define the roles and responsibilities of the stakeholders. The main interactions between them are represented by the arrows in the figures below.
- Define the basic principles;
- Define the necessary processes to issue the MCP application[11];
- Analyse and evaluate the service model.

In every scenario, the TSM(s) could be non-existent, could have pure technical roles, or could, in addition, also have commercial roles [21]. Clearly the TSM can facilitate the development of the mobile ecosystem involving other service providers and allows an

---

[10] After provisioning, the MNO profile and the SE (with its Security Domains) are managed by the MNO in the same way as a removable UICC.

[11] based on the processes specified in [21] and section 5.

easy connection between different MNOs and different MCP issuers. Commercial agreements between stakeholders directly or indirectly involved in MCPs are out of scope.

4.1.1 Scenario 1: the MNO provides the UICC

4.1.1.1 *Introduction*

In this scenario, the SE is the UICC which is provided by the MNO while the MCP issuer is responsible for the issuance and life cycle management of the MCP application. The following services could be provided by the TSM either to the MCP issuer or to the MNO:

- OTA-services, e.g. provisioning and MCP application life cycle event (see chapter 5).
- Procuring space on the UICC on behalf of the MCP issuer.
- Facilitating business (e.g. renting space) on the UICC on behalf of the MNO.

Figure 4: The MCP application resides on the UICC provided by the MNO

4.1.1.2 *Analysis*

The main advantages of this scenario for MCP issuers are the following:

- The distribution of the UICC to the consumers is the responsibility of the MNO.
- The UICC has already good market penetration.
- The UICC has a good reachability.
- Most of the necessary technical and security standards have already been developed.

- Each Service Management Role is described in terms of requirements from the MNO and the MCP issuer domains of responsibility in [21]; therefore there is mutual understanding of the processes between MNOs and MCP issuers.
- The impact on issuing systems is less important for MCP issuers who have already implemented cards. The main change is that the current connection to the card personalisation is replaced by the connection to the entity in charge of these Service Management roles.

The main challenges to face in this scenario for MCP issuers are the following:

- The interoperability between different MCP issuers using different TSMs, i.e. interoperability capability to the newly deployed TSMs
- The set-up of the necessary SLAs between the MCP issuers and the MNOs/TSMs. For example, the agreement on the user MCP interface or the achievement of the MCP issuer's security requirements might be challenging subjects to cover.

This scenario is suitable for hosting multiple payment applications from the same MCP issuer or even from multiple MCP issuers. The model even allows for the hosting of applications from other service providers such as ticketing, loyalty, etc..

4.1.2 Scenario 2a: the mobile equipment manufacturer (OEM) provides the eSE

4.1.2.1 Introduction

In this scenario, the SE is an embedded SE (eSE) in a mobile equipment which is provided by the mobile equipment manufacturer while the MCP issuer is responsible for the issuance and life cycle management of the MCP application. The mobile device also includes a UICC for the mobile subscription.

The following services could be provided by the TSM either to the MCP issuer or to the mobile equipment manufacturer:

- MCP services, e.g. provisioning and MCP application life cycle event (e.g. via mobile internet).
- Procuring space on the SE on behalf of the MCP issuer.
- Facilitating business (e.g. renting space) on the SE on behalf of the mobile equipment manufacturer.
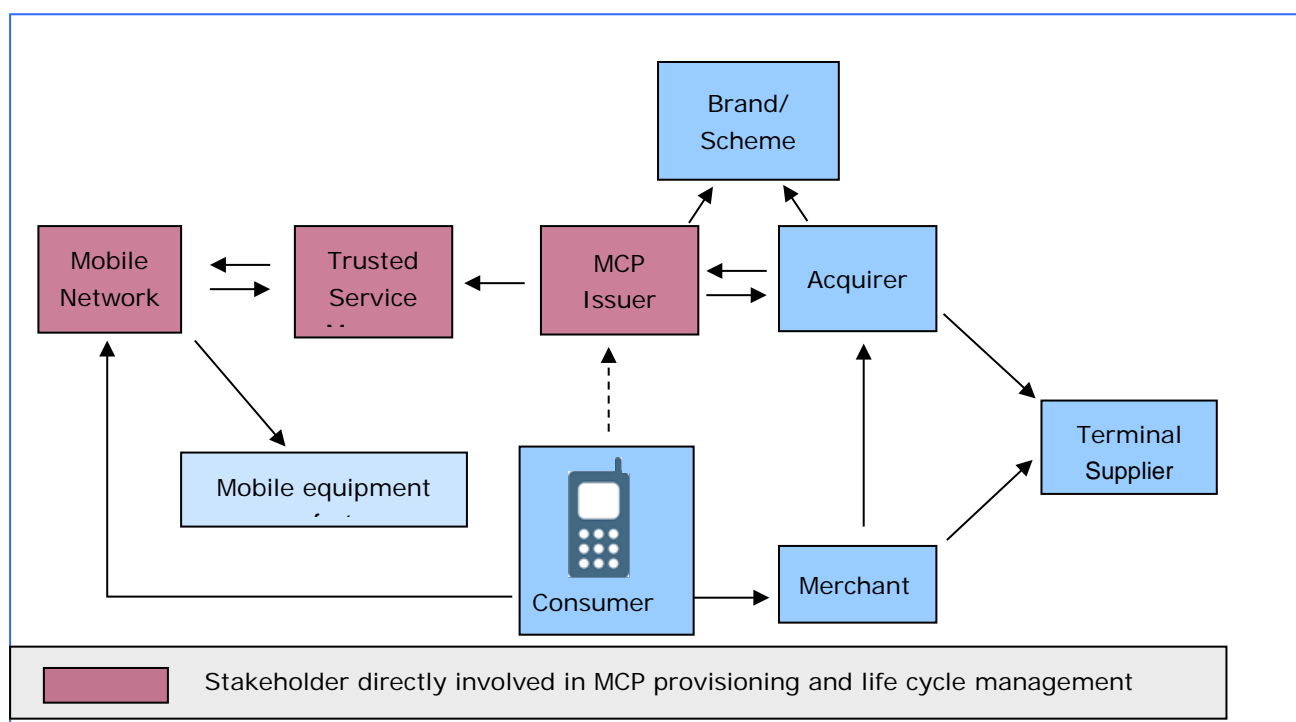
Figure 5: The MCP application resides on the eSE provided by the mobile equipment manufacturer

4.1.2.1 *Analysis*

The main advantages of this scenario for the MCP issuers are the following:

- This scenario is prepared for a mobile ecosystem involving other service providers.
- It allows direct connection of mobile equipment manufacturers, as the SE issuer, with multiple MCP issuers.
- The distribution of the eSE to the consumers is the responsibility of the mobile equipment distributors.
- There is a possible advantage with respect to the processes involved in the certification of the chipset.
- From a security point of view, an eSE offers the potential for a simpler environment.

The main challenges to face in this scenario for MCP issuers are the following:

- The interoperability between different MCP issuers using different TSMs, i.e. interoperability capability to the newly deployed TSMs.
- The MNOs will have to support mobile equipments with eSEs.
- Agreement on one common process for MCP application provisioning and maintenance to be followed by all different mobile equipment manufacturers.
- The timely delivery of appropriate technical/security standards needed e.g. by Global Platform and NFC Forum[12].

---

[12] Note that for certain aspects, proprietary solutions are not necessarily a blocking factor as the SE will only need to work with the mobile equipment in which it is embedded.

This scenario is suitable for hosting multiple payment applications from the same MCP issuer or even from multiple MCP issuers. The model even allows for the hosting of applications from other service providers such as ticketing, loyalty, etc.

4.1.3 Scenario 2b: a third party provides the eSE

4.1.3.1 Introduction

In this scenario, the SE is an embedded chip in a mobile equipment which is provided by a third party which can be a TSM or another third party, while the MCP issuer is responsible for both issuance and life cycle management of the MCP application. The mobile device also includes a UICC for the mobile subscription.

The following services could be provided by the TSM to either the MCP issuer or the third party:

- MCP services, e.g., provisioning and MCP application life cycle event (e.g. via mobile internet).
- Procuring space on the SE on behalf of the MCP issuer.
- Facilitating business (e.g. renting space) on the SE on behalf of the third party.
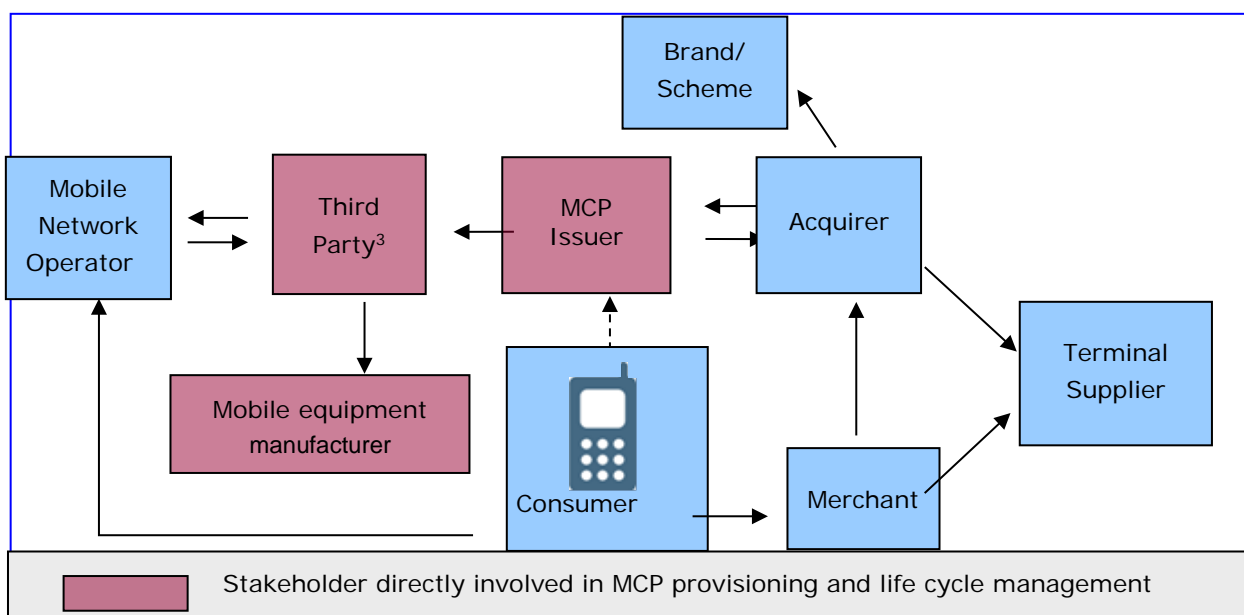
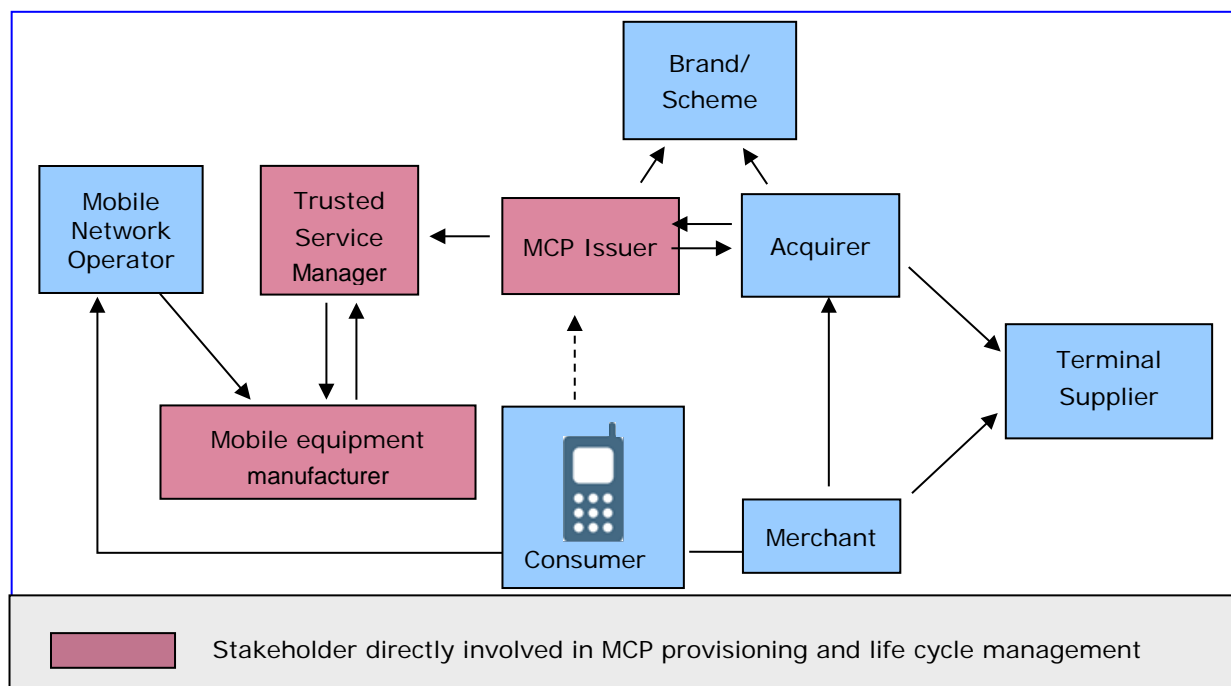**Figure 6: The MCP application resides on the eSE provided by a third party**

---

[13] The third party can be a TSM or another third party.

4.1.3.2 *Analysis*

The main advantages of this scenario for MCP issuers are the following:

- This scenario is prepared for a mobile ecosystem involving other service providers.
- The distribution of the eSE to the consumers is the responsibility of the mobile equipment distributors.
- There is a possible advantage with respect to the processes involved in the certification of the chipset with the MCP application.
- From a security point of view, an eSE offers the potential for a simpler environment.

The main challenges to face in this scenario for MCP issuers are the following:

- The interoperability between different MCP issuers using different TSMs, i.e. interoperability capability to the newly deployed TSMs.
- Establishment of appropriate third parties and their relationship with TSMs.
- The SE is not provided by the mobile equipment manufacturer but by a third party. The installation of this eSE in the mobile device requires an agreement between the mobile equipment manufacturer and the SE issuer.
- Agreement between third parties and mobile equipment manufacturers for the embedding in mobile equipments.
- The MNOs will have to support mobile equipments with eSEs.
- The switch between one mobile equipment to another one is more inconvenient for the consumer because a re-enrolment process is needed.
- The timely delivery of appropriate technical/security standards needed, provided e.g. by Global Platform and NFC Forum.

This scenario is suitable for hosting multiple payment applications from the same MCP issuer or even from multiple MCP issuers. The model even allows for the hosting of applications from other service providers such as ticketing, loyalty, etc.

However, this scenario, compared to scenario 2a, holds an increased complexity due to the fact that the stakeholders responsible for the SE and for the mobile equipment are different entities. A number of aspects, such as the responsibility for the SE certification, the mobile equipment certification and the support for the SE by the mobile equipment, are additional challenges that are an extra burden for implementations of this service model. As a conclusion, nowadays, this scenario appears to be much more challenging than the previous one.

4.1.4 Scenario 3: the mobile equipment manufacturer (OEM) provides the eUICC

4.1.4.1 *Introduction*

When a consumer purchases a mobile device that contains an eUICC there is no MNO profile available yet. The eUICC is more or less empty. To get a connection to a selected network operator the consumer has to select a subscription to an MNO, and download

the MNO profile to their new mobile device. The download of the necessary files is under control of the selected MNO and it prepares the eUICC for holding the MNO profile and SE structure. After provisioning of the eUICC, the eUICC is also prepared to manage SE applications like the MCP application.

As the SE is part of the MNO profile, changing the MNO by the consumer will automatically also imply a change in the SE and its applications. This can be compared with removing a traditional SIM and replacing this with a SIM of another operator.

The scenario below has the prerequisite that a remote UICC / SIM provisioning process has taken place and the accompanied SE is under control of the MNO.

The SE on the eUICC is provisioned by the MNO while the MCP issuer is responsible for the issuance and life cycle management of the MCP application. The following services could be provided by the TSM either to the MCP issuer or to the MNO:

- OTA-services, e.g. provisioning and MCP application life cycle event (see chapter 5).
- Procuring space on the UICC on behalf of the MCP issuer.
- Facilitating business (e.g. renting space) on the UICC on behalf of the MNO.
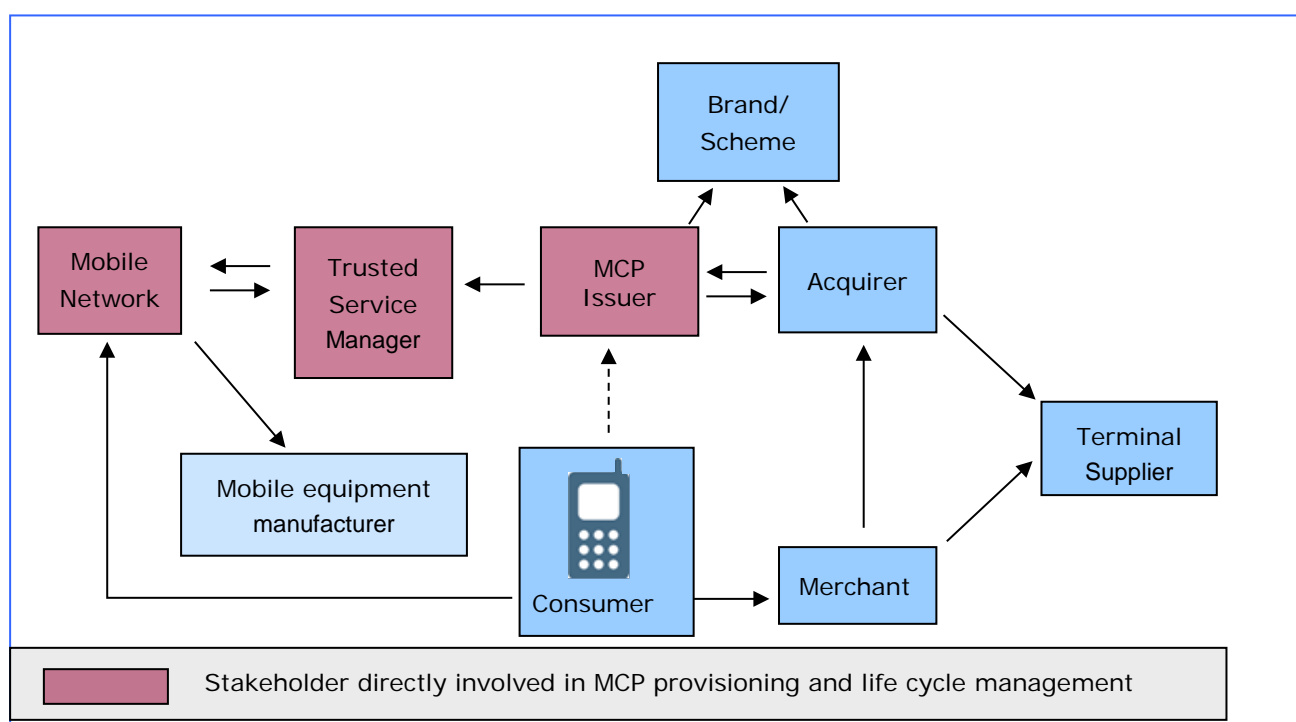
Figure 7: The MCP application resides on the eUICC provided by the mobile equipment manufacturer

4.1.4.2 *Analysis*

The main advantages of this scenario for MCP issuers are the following:

- The provisioning of the network operator profile and functional Secure Domains on the eUICC to the consumers is the responsibility of the MNO.
- The eUICC technology is comparable with the traditional UICC.
- The eUICC has a good reachability.

- Most of the necessary technical and security standards have already been developed (see for instance [49]).
- Each Service Management Role is described in terms of requirements from the MNO and the MCP issuer domains of responsibility in [21]; therefore there is mutual understanding of the processes between MNOs and MCP issuers.
- The impact on issuing systems is less important for MCP issuers who have already implemented cards. The main change is that the current connection to the card personalization is replaced by the connection to the entity in charge of these Service Management roles.

The main challenges to face in this scenario for MCP issuers are the following:

- The interoperability between different MCP issuers using different TSMs, i.e. interoperability capability to the newly deployed TSMs.
- The set-up of the necessary SLAs between the MCP issuers and the MNOs/TSMs. For example, the agreement on the user MCP interface or the achievement of the MCP issuer's security requirements might be challenging subjects to cover.

This scenario is suitable for hosting multiple payment applications from the same MCP issuer or even from multiple MCP issuers. The model even allows for the hosting of applications from other service providers such as ticketing, loyalty, etc.…

The use of an eUICC gives the consumer the opportunity to easily switch from one MNO to another without any physical interaction. The MNO profile (including the MNO Secure Domain and underlying service provider secure domains) can be downloaded over the air (OTA) to the device. When switching MNOs the existing MNO profile and accompanied applications residing on the eUICC (e.g., the MCP application) will be deactivated and exchanged with the new selected MNO profile.

4.2 Cloud-based MCP Applications

4.2.1 Introduction

An alternative approach to SE-based MCP Applications has been the introduction of Cloud-Based Payments (CBP) using Host Card Emulation (HCE) supported by the Android mobile phone operating system. Other mobile phone operating systems may also support HCE.

There are multiple paths that an issuer can take for their proposition to market depending on:

- Internal IT resource
- Budget
- Ongoing management of mobile applications, cloud and mobile platforms
- Existing relationships with processing partners
- Required time to market.

Deployment options include:

- In house development;

o Hosted by the Issuer
- Vendor Solution
  o Hosted by the Issuer
  o Hosted by a third party.

For cloud-based MCPs, the following components are involved:

- A Cloud-Based Payments Platform (CBPP) performs core functions that provision and manage consumer accounts according to issuer predefined preferences.
- A Mobile Application (MA) provides consumers with the tools necessary to manage the cloud-based payments experience including enrolment, provisioning, lifecycle management, and payment
- A Mobile Application Cloud Platform (MACP) securely brokers messages in support of enrolment, provisioning, active account management, and other use cases between the CBPP and the MA.

For these models, the MCP application consists of a part referred to as the Mobile Application (MA) residing on the mobile device and a part implemented in the Mobile Application Cloud Platform (MACP) (see Figure 9 in section 5.3).
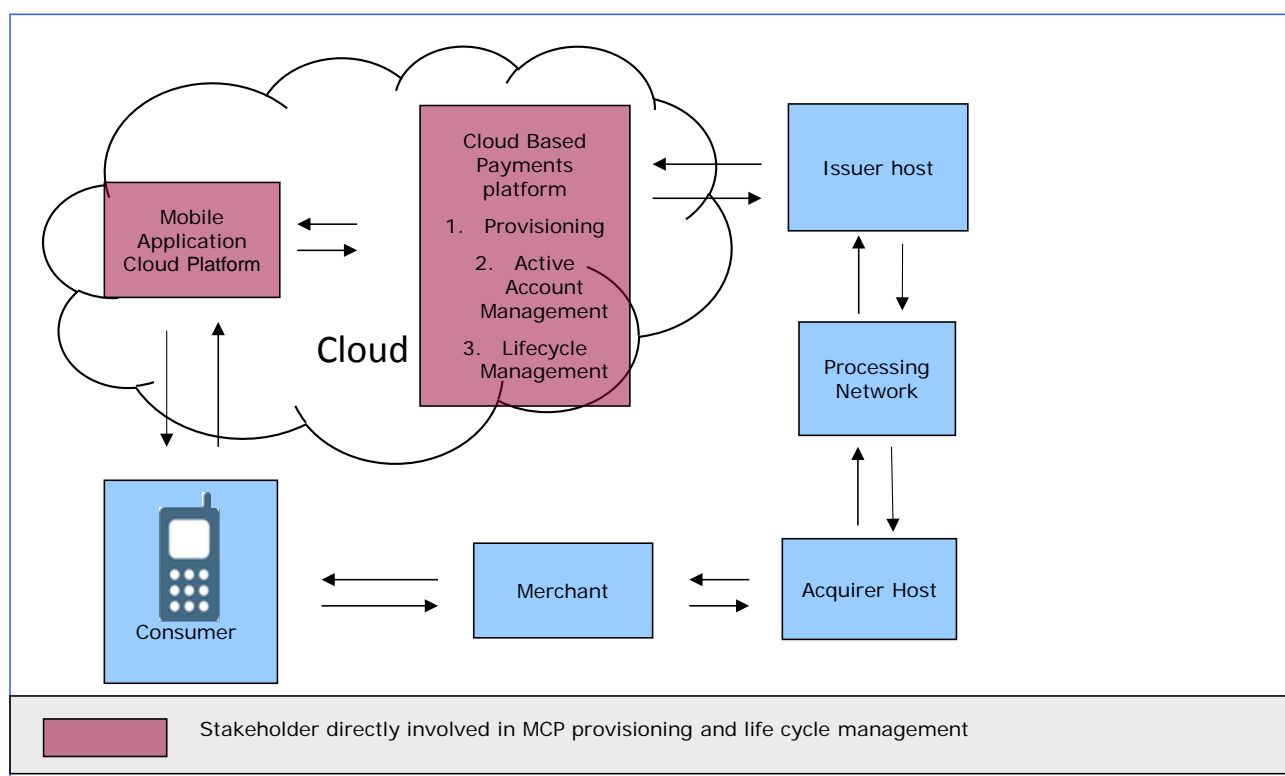
Figure 8: The cloud-based MCP ecosystem

4.2.2 Analysis

The main advantages of CBP for MCP issuers are the following:

- The simplification of the overall ecosystem.
- Can leverage issuers existing apps (e.g. mobile banking, Issuer wallets).

- Issuers able to create product differentiation with their offerings.
- No SE is required, consumers just download an app and enrol.
- Scalability, straightforward coverage of different mobile platforms.

The main challenges of CBP for MCP issuers are:

- Must meet additional security requirements due to no SE.
- Predominantly on-line only transactions.

In addition, hardware and software protection features can be combined with those of the CBP.

4.3 Conclusions

The table below provides a brief overview on the different stakeholders involved in the MCP ecosystem, dependent on the model used.

Entity	SE-based ecosystem	Cloud-based ecosystem
MCP Issuer	x	x
SE Issuer	x	
SE manufacturer	x	
Service provider TSM	x	
MNO TSM	x	
OS provider		x
Cloud-based platform		x
Handset manufacturer	x	x

Table 5: Stakeholders involved in SE-based versus cloud-based MCP ecosystem

From a technical perspective, the UICC-based solution offers a straightforward deployment in view of the maturity of available standards and the existing infrastructure. However, the complexity of the business model and the relationships between the relevant parties have proven to be challenging. The introduction of the eUICC in the market may provide a new approach to overcome some of these challenges.

Likewise, the usage of eSEs; the model based on a third party as SE issuer, appears to encompass too many challenges to offer an immediate solution (see section 4.1.3). These challenges as of today, have only been resolved by the major players in the mobile ecosystem. In the case of the mobile equipment manufacturer being responsible for the supply of the eSE (together with the mobile equipment), there may be additional issues related to the implementation of certain new roles as defined through the processes described in chapter 5.

For Cloud-based Payments, MCP issuers need to understand the different approaches to security that are utilised in CBP solutions and have in place the necessary security requirements for their own organisation as well as for any partners involved in their offerings. However, given the simplicity of the ecosystem and the associated commercial benefits, speed and simplicity of deployment, and the ability to integrate them within the issuers existing applications, CBP have proven in recent years to become a popular method of deploying MCPs.

This document aims to reflect the current state of the art at the time of release. Major new developments have been announced during the past years by various players on one hand or by technology providers on the other hand. Cloud-based payments using host card emulation is an obvious example. Since MCP issuers are free to implement their model of choice, the market will determine the success of each of the models described.

5 MCP application management

5.1 Introduction

The management of the MCP applications depends on the type of service model that the MCP issuer will choose. It is assumed that the consumer has a subscription with an MNO for mobile network services, including facilitation of NFC services.

This chapter provides an overview of the different processes related to the management of an MCP application between the different parties involved as described in the previous chapter.

In Annex B: Overview life cycle management processes for MCP models, a more detailed description of the procedures for the consumer during the life cycle of the MCP application and the information flows between the different participants are illustrated for some SE-based models, namely when the SE is a UICC or an eSE.

Note that for the management of the processes the appropriate Service Level Agreements (SLAs) between the stakeholders shall be put in place. Even if detailed terms and conditions mostly depend on bi-lateral specific deals between these parties, typical topics to be addressed in the SLAs should cover:

- Customer care;
- Consumer enquiries;
- Scalability;
- Operational aspects such as technical processes, security, incidents and fraud;
- Real-time (or "near-real-time") interaction management.

5.2 SE-based MCP Application life cycle: functions and processes

5.2.1 Functions

Functions for application lifecycle management are triggered by one or several possible situations and require actions from the MNO and/or the MCP Issuer and/or a third party (e.g., a TSM or SE issuer). In some cases actions may be required from the customer. The protocols used to execute the functions for MCP application lifecycle management will typically encompass acknowledgement/confirmation of the actions. This subclause provides the following non-exhaustive list of functions based on [21] and [55]:

1. *Eligibility request:* The MCP Issuer requests an eligibility report from the MNO or a third party to ascertain that the customer's mobile device is technically capable of hosting the MCP application and operating the related MCP service;

2. *Installation of MCP application:* The installation of the MCP application in the SE on the mobile device;

3. *Installation of MCP application user interface: The installation of the mobile equipment application executing the user interactions related to the MCP application, as permitted by the MCP issuer. Depending on the implementation*

this might require user interaction. This function may also include the personalisation and activation[14] of the MCP application.

4. *Update of MCP application parameters:* The update of MCP application parameters and counters (e.g., for risk management) during the lifecycle of the application;

5. *Deletion of MCP application:* The removal of the MCP application and related data from the SE on the mobile device;

6. *Deletion of MCP application user interface:* The removal of the MCP application user interface and related data from the mobile device;

7. *Blocking of MCP application:* The issuer instructs the MCP application to block itself in the SE either locally or remotely;

8. *Unblocking of MCP application:* The issuer unblocks remotely the MCP application in the SE;

9. *Blocking of mobile network connectivity:* The MNO blocks the network connectivity of the mobile device at the MNO server-side.

10. *Unblocking of mobile network connectivity:* The MNO re-installs the network connectivity of the mobile device at the MNO server-side.

11. *Audit of MCP application:* The MCP issuer retrieves MCP application data from the MCP application (e.g.; via OTA, NFC).

12. *Audit of SE:* The MCP issuer may request the SE issuer information about the SE resources, state of their MCP application(s), etc..

5.2.2 Processes

Each phase of the MCP application lifecycle (subscription, installation, usage and termination) is carried out by the execution of the processes listed hereafter. A process may be covered by functions described in section 5.2.1.

- *Subscription*

1. Inquiry to MCP issuer
2. Inquiry to SE issuer
3. Subscription to MCP service (application);
4. Renewal of MCP service (application);
5. Eligibility check;

- *Installation*

---

[14] Note however that different implementations may exist where this is to be considered as a separate function.

6. Installation of MCP application;
7. Installation of MCP application user interface;

- *Usage*

8. Audit MCP application;
9. Update MCP application parameters;
10. Change SE (if applicable);
11. Change mobile phone number;
12. Change mobile equipment;
13. Lost/stolen mobile device –contact MNO;
14. Lost/stolen mobile device –contact MCP issuer;
15. Recovery of mobile device (contact MNO/MCP issuer);
16. New mobile device after lost/stolen;
17. Change MNO;
18. Temporary mobile services suspension;
19. Resume mobile services;
20. Temporary MCP application suspension;
21. Resume MCP application;
22. MCP issuer customer relationship management;
23. MNO customer relationship management;

- *Termination*

24. Mobile service termination by consumer;
25. Mobile service termination by MNO;
26. MCP application termination by consumer;
27. MCP application termination by the MCP issuer.

5.3 HCE Based Application life cycle: functions and processes

In this section the functions and processes involved for the lifecycle management, including provisioning, of an MCP application for cloud-based models is described. For these models, the MCP application consists of a part referred to as the Mobile Application (MA) residing on the mobile device and a part implemented in the Mobile Application Cloud Platform, as illustrated in the figure below.
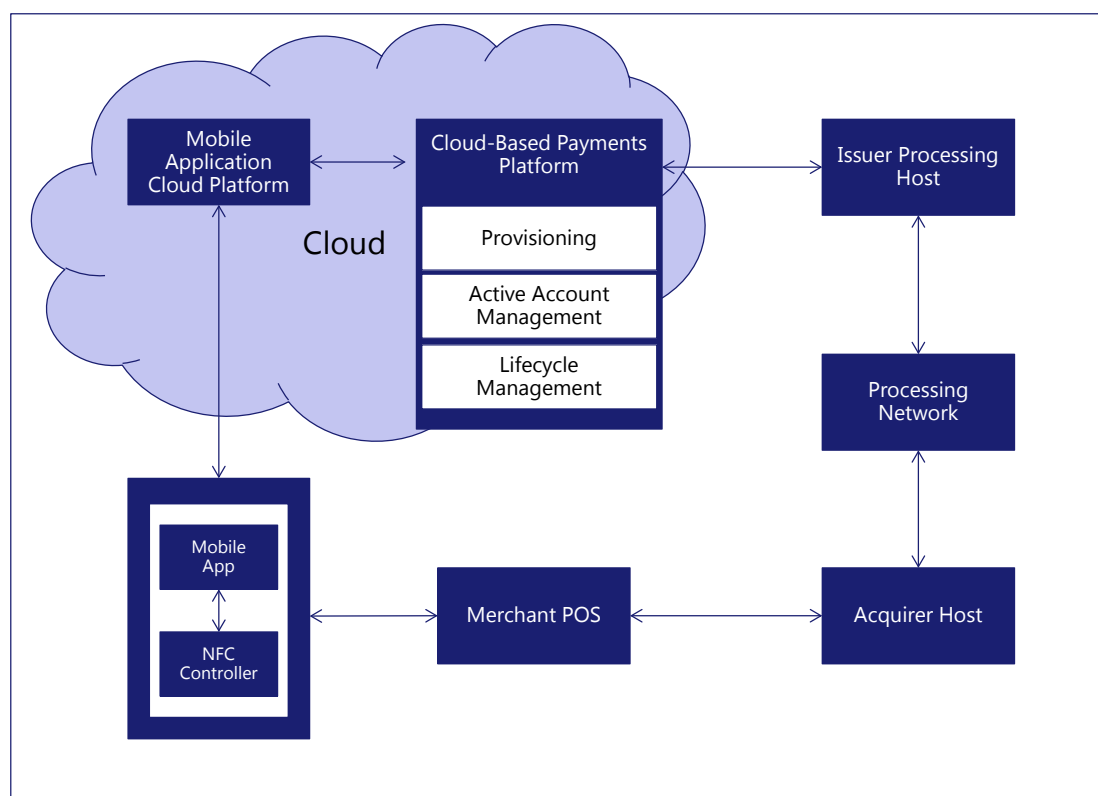
Figure 9: Cloud-based MCP architecture

5.3.1 Provisioning

This process generates account configuration data that is used to provision account on mobile applications for cloud-based payments. It generates an initial set of account parameters deployed to the mobile application. These parameters may include the PAN (or token), issuer risk parameters, and may also include triggers for refreshing account parameters on the mobile device.

Provisioning flow:

1. The consumer downloads the Mobile Application MA and after being authenticated, chooses the card to provision to the MA;

2. The MA communicates to Mobile Application Cloud Platform (MACP);

3. The MACP communicates with the Cloud-Based Payments Platform (CBPP);

4. The CBPP enables the account and sends account parameters and configuration data to the MACP;

5. The MACP sends provisioning payload to the MA on the mobile device;

6. The MA provisions the account on the mobile device using configuration data from the CBPP.

5.3.2 Active Account Management

Active Account Management (AAM) is a process that replenishes account parameter dynamic data based on the MCP issuer preferences.

AAM Flow:

- **Use Case 1 – Processing Host – Initiated**

  1. Consumer initiates the payment;

  2. Business as usual transaction processing flow;

  3. Transaction flows from the acquirer to the issuer processing host who checks if account parameters (dynamic data) need to be replenished;

  4. AAM will generate new account parameters and push to the MA on the mobile device.

- **Use Case 2 – Cloud-based payments platform – Initiated**

  1. Based on account parameters, the cloud-based payments platform initiates AAM;

  2. The cloud-based payments platform pushes new account parameters to the MA on the mobile device.

- **Use Case 3 – Mobile Application – Initiated**

  1. On-device account thresholds indicate account parameter replenishment is needed; the MA sends a request to cloud-based payment platform via the MACP;

  2. The cloud-based payment platform will either replenish account parameters or deny request. If honouring request, it sends new account parameters to the MA on the mobile device.

5.3.3 Lifecycle Management

Lifecycle Management (LCM) is a process that manages the lifecycle of an account (e.g. delete, suspend, resume triggered by the consumer or the MCP issuer).

Lifecycle Management Flow:

- **Use Case 1: Consumer – initiated LCM**

  1. Consumer initiates LCM;

  2. Request is sent via MACP to the cloud-based payments platform;

  3. The cloud-based payments platform performs LCM in coordination with the MCP issuer.

- **Use Case 2: MCP issuer – initiated LCM**

1. The MCP issuer initiates LCM and sends a request to the cloud-based payments platform;

2. The cloud-based payments platform performs LCM;

3. The cloud-based payments platform updates account via MACP.

6   MCP Application

This chapter aims to provide a high-level overview of the different transaction flows involved in MCPs. This includes on-line and off-line payments and the optional execution of a Cardholder Verification Method (CVM) (off-line or on-line). Section 6.2 provides details on the CVM with the introduction of CDCVMs. With the taps described in section 6.5, an MCP application authentication/authorisation are executed according to the corresponding card authentication/authorisation specifications in the SEPA Cards Standardisation Volume [4]. An MCP application risk management is treated in section 6.6. Finally, some additional features are handled in section 6.7. Section 6.8 illustrates a number of MCP use cases. However, it is up to the card schemes and the MCP issuers and acquirers involved to decide which transaction flows will be applied.

6.1   Performing an MCP

Prior to performing an MCP, consumers, dependent on the mobile device model, wallet configuration and/or operating system, may have to perform, or can choose to perform, some additional steps which are described in section 7.5. These additional steps will largely be driven by the consumer preference and will not be further discussed in this document.

However, the initial stages of the actual MCP transaction at the POI are identical to those using a physical contactless card. The following steps are executed and further details can be found in the references given:

1. Transaction initialisation (see section 4.2.3.1 in Book 2 of [4]);
2. Language selection (see section 4.2.3.2 in Book 2 of [4]);
3. Technology selection (see section 4.2.3.3 in Book 2 of [4]);
4. Selection of the Application (see section 4.2.3.4 in Book 2 of [4]);
5. MCP application data retrieval (see section 4.2.3.5 in Book 2 of [4]).

6.2   Cardholder Verification Methods

6.2.1   Introduction

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

For MCPs, the following cardholder verification methods may be used[15] (see also [4], Book 4):

- **On-line CVM:** PIN entered on the POI and verified on-line by the MCP issuer;
- **Off-line CVM:** a CDCVM, which is entered by or captured from the consumer on the mobile device. Typical methods used include

---

[15] Although a "signature" is allowed as fall-back for MCPs in the SEPA Cards Standardisation Volume (see [4]), it will not be considered in this document.

- Biometrics, verified by an application on the mobile device. Hereby a distinction may be made depending on the method for capturing
  o Active – which requires a consumer interaction; e.g., fingerprint;
  o Passive – no user interaction is needed; e.g., vein recognition by a wrist band or smart watch.

- Mobile code[16]: entered on the mobile device.
  o The verification of the mobile code is done by the MCP application in the SE on the mobile device;
  or
  o Implicit validation of the correct entry of the mobile code through a cryptographic derivation, verified on-line by the MCP issuer.

- **No CVM required.**

On a mobile device, a distinction may be made between a CDCVM verified by the MCP 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 MCP issuer. Functional and security requirements for "platform shared authentication" mechanisms are currently being developed by EMVCo. In the remainder of this document we will refer to "CDCVM" instead of an "off-line CVM".

As with contactless card payments, a distinction is made between on-line and off-line transactions as follows:
- **Off-line transaction:** Off-line authorised MCP transaction between POI and MCP Application (this means without on-line communication to the MCP issuer);
- **On-line transaction:** On-line authorised MCP transaction via the POI by the MCP issuer.

The transaction types versus the CVMs which can be supported are represented in the table below.

---

[16] 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.

	No CVM	On-line CVM	CDCVM
On-line transaction	X	X	X
Off-line transaction	X		X

<div align="center">**Table 6: Transaction types and CVMs**</div>

The usage of a CVM is often linked to the transaction risk management and is to be applied by the MCP 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 section 6.4 and Annex A: Overview regulatory documents). Typically, lower value transactions are exempted of the usage of a CVM (see section 6.4). For MCPs, other factors, such as the consumer choice, may influence the usage of a CVM (see for instance section 6.2.2.5).

Note: In the remainder of this document each of the combinations of this table will be further analysed. The figures provided only focus on the processing of the CVM and do not include the transaction processing (on- or off-line transaction).

6.2.2 Single tap: analysis of CVMs

With this payment method, the consumer performs a single tap with their mobile device to conduct the MCP transaction. The interaction between the mobile device and the POI during the single tap is the exchange of all information needed to perform the transaction. No further interaction is required. Based on the MCP/POI risk analysis, an on-line or off-line transaction will take place which might involve a CVM.

6.2.2.1   *On-line transactions - no CVM*

This payment method is typically used for low value payments (see section 6.4).

The following steps will take place after the risk analysis:
6. On-line MCP application authentication/authorisation (see sections 4.2.3.6 and 4.2.3.8 in Book 2 of [4]);
7. Transaction completion (see section 4.2.3.10 in Book 2 of [4]).

In this case the transaction flow is identical to an on-line contactless card payment without CVM, whereby a single tap is used between the mobile device and the POI for the data transfer between the mobile device and the POI. With the completion in step 7, the dedicated response message will not be transferred to the MCP application (on the mobile device).

6.2.2.2 *On-line transactions - on-line CVM*

In this case, the POI will request the consumer to enter their PIN on the POI. The PIN used is the classical PIN issued by the MCP issuer, not any PIN the consumer may have set up on their mobile device.

The following steps will be executed after the risk analysis:

6. On-line cardholder verification with PIN entry at POI (see section 4.2.3.7 in Book 2 of [4]);
7. On-line MCP application authentication/authorisation (see sections 4.2.3.6 and 4.2.3.8 in Book 2 of [4]);
8. Transaction completion (see section 4.2.3.10 in Book 2 of [4]).
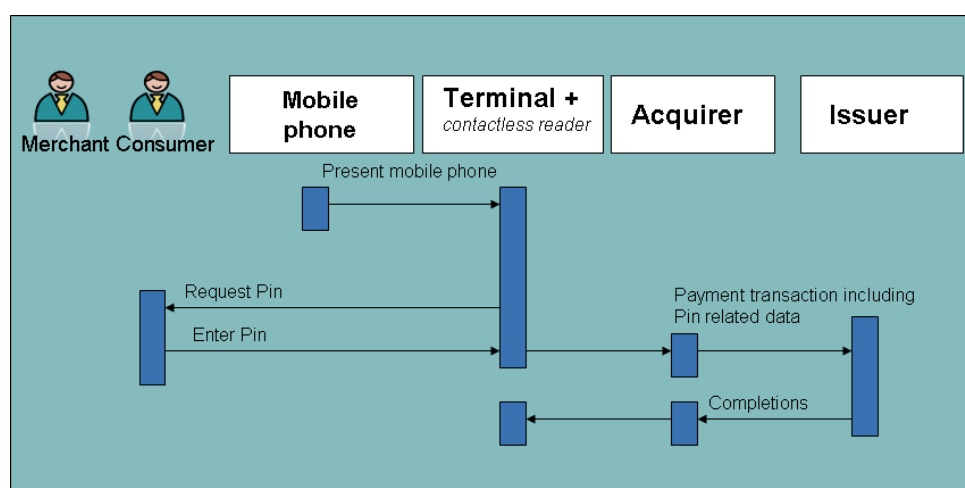
Figure 11: On-line transaction - on-line CVM

In this case the transaction flow is identical to an on-line contactless card payment with on-line CVM, whereby a single tap is used between the mobile device and the POI for the data transfer between the mobile device and the POI. With the completion in step 8, the dedicated response message will not be transferred to the MCP application (on the mobile device).

6.2.2.3 *On-line transactions - CDCVM*

In this case, a CDCVM is used which is performed by the consumer on the mobile device (e.g., as illustrated in the figure below, a mobile code verified by the MCP application on the mobile device).

The CDCVM is performed before the tap. The result of the CDCVM verification is transferred in the on-line authentication/authorisation message to the MCP issuer via the POI through the tap.

The following steps are executed with the payment transaction:
0. Off-line cardholder verification with CDCVM performed on mobile device (see section 4.2.3.7 in Book 2 of [4]);

Steps 1 to 5 as described in section 6.1.
6. On-line MCP application authentication/authorisation (see sections 4.2.3.6 and 4.2.3.8 in Book 2 of [4]);
7. Transaction completion (see section 4.2.3.10 in Book 2 of [4]).
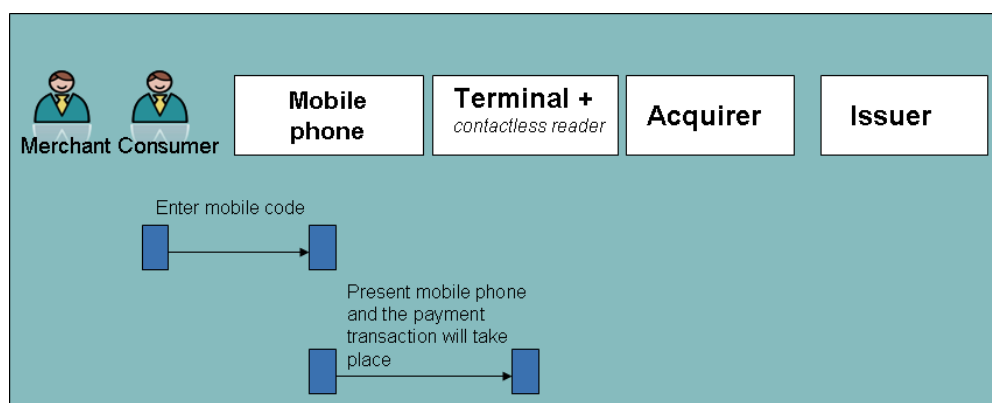
Figure 12: On-line transaction - CDCVM

Again, with the completion in step 7, the dedicated response message will not be transferred to the MCP application (on the mobile device).

6.2.2.4   *Off-line transactions - no CVM*
This payment method is typically intended for low value payments.

The following steps will take place after the risk analysis:
6. Off-line MCP application authentication/authorisation (see sections 4.2.3.6 and 4.2.3.8 in Book 2 of [4]);
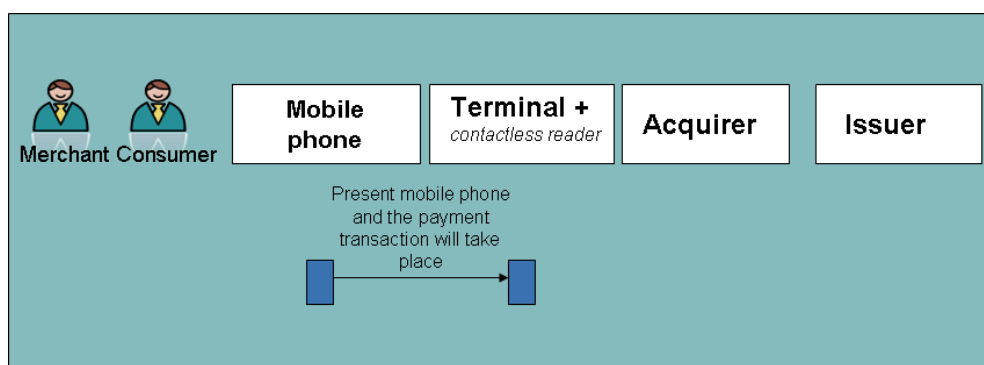7. Transaction completion (see section 4.2.3.10 in Book 2 of [4]).
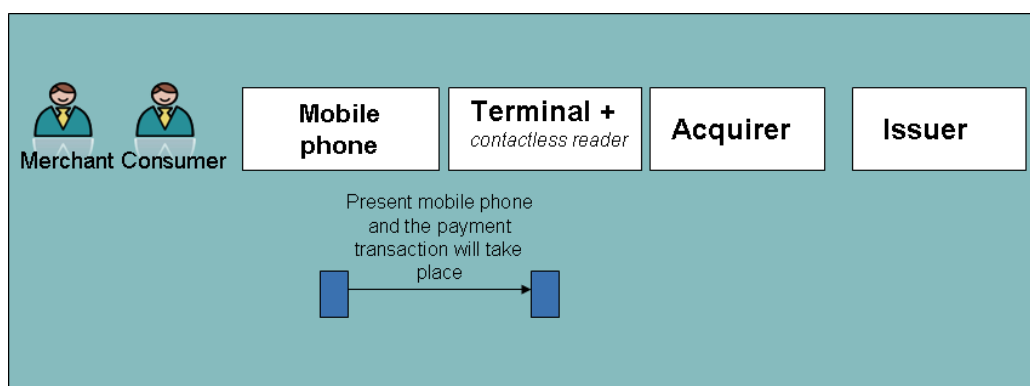
Figure 13: Off-line transaction - no CVM

In this case the transaction flow is identical to an off-line contactless card payment without CVM, where a single tap is used between the mobile device and the POI for the data transfer between the mobile device and the POI.

6.2.2.5 *Off-line transactions - CDCVM*

Similar to 6.2.2.3, a CDCVM is used which is performed by the consumer on the mobile device. The result of the CDCVM verification is transferred to the POI with the tap.

The following steps are executed with the payment transaction:

0. Off-line cardholder verification with CDCVM performed on mobile device (see section 4.2.3.7 in Book 2 of [4]);

Steps 1 to 5 as described in section 6.1.

6. Off-line MCP application authentication/authorisation (see sections 4.2.3.6 and 4.2.3.8 in Book 2 of [4]);

7. Transaction completion (see section 4.2.3.10 in Book 2 of [4]).
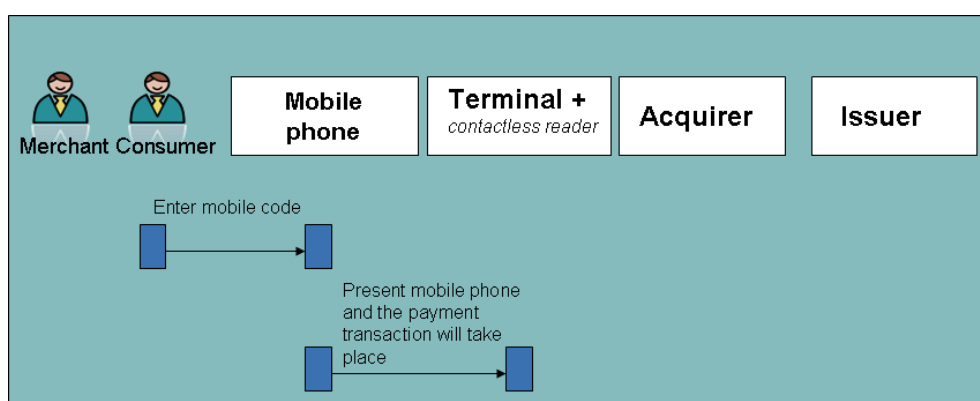
Figure 14: Off-line transaction - CDCVM

6.2.3 Double Tap: Analysis of CVMs

6.2.3.1 *On-line transactions - CDCVM*

Similar to 6.2.2.3, a CDCVM is used which is performed by the consumer on the mobile device. This CDCVM is performed after the 1st tap. The result of the CDCVM verification is transferred in the on-line authentication/authorisation message to the MCP issuer via the POI through the 2nd tap.

The following steps will be executed after the risk analysis:

6. Confirmation of payment transaction details, received from the POI, by the consumer via the CDCVM on the mobile device (see section 4.2.3.7 in Book 2 of [3]);
7. On-line MCP application authentication/authorisation (see sections 4.2.3.6 and 4.2.3.8 in Book 2 of [3]);
8. Transaction completion (see section 4.2.3.10 in Book 2 of [4]).
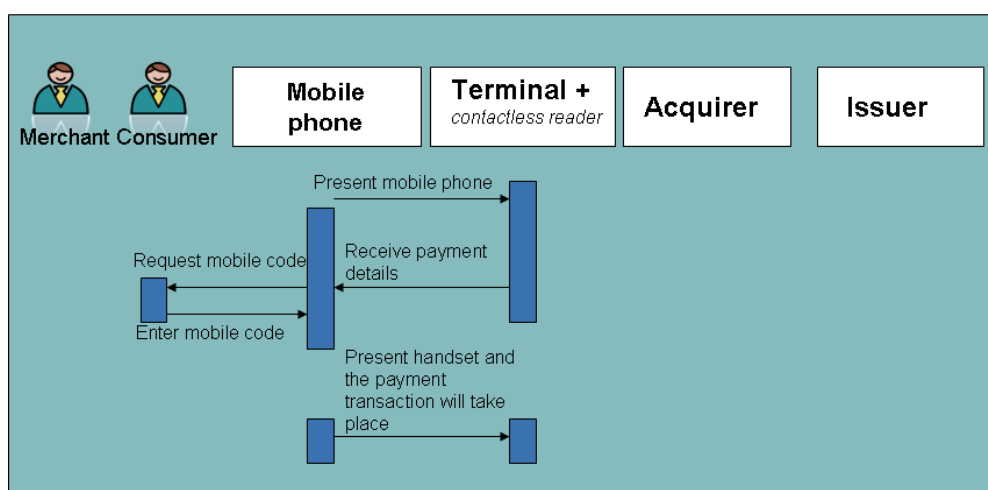
Figure 15: On-line transaction - CDCVM

Again, with the completion in step 8, the dedicated message will not be transferred to the MCP application (on the mobile device).

6.2.3.2   *Off-line transactions - CDCVM*

As in section 6.2.3.1, a CDCVM is used which is performed by the consumer on the mobile device. This CDCVM is performed after the 1st tap and the result of the verification is transferred in the off-line authentication message to the POI with the 2nd tap.

The following steps will be executed after the risk analysis:

6. Confirmation of payment transaction details, received from the POI, by the consumer via the CDCVM on the mobile device (see section 4.2.3.7 in Book 2 of [3]);
7. Off-line MCP application authentication/authorisation (see sections 4.2.3.6 and 4.2.3.8 in Book 2 of [3]);

8. Transaction completion (see section 4.2.3.10 in Book 2 of [4]).
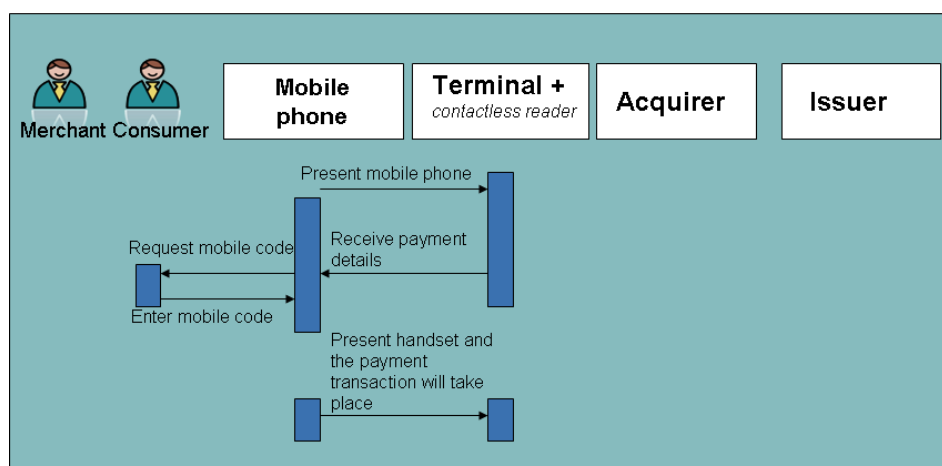
Figure 16: Off-line transaction - CDCVM

6.2.3.3   *Additional remarks*

Any flow requiring an additional tap is to be avoided in view of the consumer experience.

- If the result of the completion of the transactions needs to be transmitted to the mobile device, an additional tap would be required or, alternatively, the mobile device would need to be kept on the POI,
- Any life cycle management (e.g. risk management parameters) executed via script processing from the MCP issuer to the MCP application.

Alternatively, some MCP issuers might support, for payments without CVM, the usage of a so-called "confirmation button" on the mobile device to allow the consumer to acknowledge that a transaction is taking place.

6.3 Card Authentication

By this function the MCP application is authenticated by the POI (off-line data authentication) or by the MCP issuer (issuer authentication). For MCP transactions, a dynamic authentication is required according to section 2.2.2.1 in Book 4 of [4], which means that either Combined Data Authentication (CDA) or fast Dynamic Data Authentication (fDDA) is supported.

6.4 Strong Customer Authentication

Article 97 of the Payment Services Directive PSD2 [2] mandates the usage of strong customer authentication for MCP transactions, except for the exemptions (Article 98) defined in Article 11 of the draft Regulatory Technical Standards (RTS) for Strong Customer Authentication and Common and Secure Communication under PSD2 (see [3] in Annex A: Overview regulatory documents). Those exemptions currently read as follows[17]:

---

[17] This text will be updated as soon as the final RTS are published.

"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 transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication does not exceed five."

The combination of a dynamic card authentication (see section 6.3) with a CVM provided by the consumer (see section 6.2) creates a strong customer authentication method.

6.5 MCP transaction

The table below shows a matrix of the possible transaction types for the execution of an MCP transaction between a mobile device and a POI terminal:

Mobile device	MCP Transaction			
	Off-line		On-line	
CVM	Single tap	Double tap	Single tap	Double tap
On-line CVM	-	-	X	-
CDCVM	X[1]	X[2]	X [1]	X[2]
No CVM	X	-	X	-

Table 7: Overview transaction types versus CVM usage

[1] prior to tap

[2] between 2 taps

6.6 Risk management

6.6.1 Introduction

The mobile environment offers a number of additional features that may be utilised for MCPs with respect to the transaction amount, compared to contactless card payments using physical cards, including additional CVMs (see section 6.2 and [4]). In addition, "Over the Air" (OTA) is an additional channel available to the MCP issuer for managing

the MCP application, including issuer risk parameters, which reduces the dependency on the POI capabilities.

As with all other transactions, there are a number of risk parameters which may be set to control the behaviour of a transaction. For mobile transactions, they may be set either in the MCP application, on the POI, or more commonly, both. Issuers and acquirers configure their MCP applications and POI's based on their own risk appetite and according to the rules of the relevant card scheme. The actual risk parameters used in an individual transaction will vary, dependent on a number of factors such as:

- Whether the transaction is performed online;
- Whether a CVM was required;
- Whether the transaction is domestic/international;
- The time since the last online transaction;
- The cumulative amount spent since the last online transaction.

Note: This list is not exhaustive, and issuers may use any number of counters and limits made available by themselves, or the Card scheme of the MCP application they issue.

6.6.2 Form Factor

For certain purposes the identification of the form factor (e.g., physical card or mobile device) being used may be required. Therefore, the MCP applications shall have a dedicated data element indicating the form factor. In so far that this data element is not authenticated, it can only be used for information by the POI, the acquirer or the MCP issuer.

6.6.3 Parameters

When conducting an MCP transaction, typically the consumer presents their mobile device to the POI. The following steps are then executed:

1. Transaction initialisation (see section 4.2.3.1 in Book 2 of [4]);
2. Language selection (see section 4.2.3.2 in Book 2 of [4]);
3. Technology selection (see section 4.2.3.3 in Book 2 of [4]);
4. Selection of the Application (see section 4.2.3.4 in Book 2 of [4]);
5. MCP application data retrieval (see section 4.2.3.5 in Book 2 of [4]).

Based on the MCP/POI risk analysis, an on- or off-line transaction will take place which might involve a CVM.

6.6.4 Point Of Interaction Risk parameters

6.6.4.1 *Acquirer CVM Limit*

The *Acquirer CVM Limit* is a risk management parameter indicating the maximum value of a transaction which does not require a CVM.

Transactions for which the value is less than, or equal to, the *Acquirer CVM Limit* are typically low risk payments (e.g., low value) where convenience and speed are important and the usage of a CVM would not be appropriate. Transactions for which the value is greater than the *Acquirer CVM Limit* require the usage of a CVM (see 6.2).

The value of the *Acquirer CVM Limit* is set in the POI application and defined by the acquirer in accordance to the Card scheme (typically at country level). It takes into account the risk of fraudulent transactions (e.g., in case of loss or theft of the mobile device), while preferably using the same contactless *Acquirer CVM Limit*, independent of the form factor. In addition, for consistent consumer and merchant experience (and education), the contactless *Acquirer CVM Limit* should ideally be the same for all Card schemes in a certain geography.

An overview on the CVM usage is given in the table below.

Transaction Amount	≤ Acquirer CVM Limit	> Acquirer CVM Limit
CVM	Optional	Mandatory

<div align="center">**Table 8: CVM usage**</div>

Note: Optional in the context of this table means that the CVM may be used depending on the outcome of other CVM related risk management (see section 6.2).

6.6.4.2   *Floor Limit*

The *Floor Limit* is a parameter indicating the value of a transaction above which an on-line authorisation by the MCP issuer is required.

- Transactions for which the value is less than or equal to the *Floor Limit* may be approved off-line by the MCP application.
- Transactions for which the value is greater than the *Floor Limit* which are not authorised on-line by the MCP issuer are at the liability of the acquirer/merchant.

The value of the *Floor Limit* is set in the POI application and defined by the acquirer under the Card scheme rules (it may depend on different factors such as the merchant Category Code, etc., or the payment product).

Note: Even if the transaction value is less than the *Floor Limit*, the POI might require an on-line authorisation due to other risk management features such as the random on-line transaction selection by the POI set by the acquirer, if this option is supported by the POI.

6.6.4.3   *Transaction Limit*

The *Transaction Limit* is a parameter indicating the value of a transaction above which the MCP transaction is not allowed.

- Transactions for which the value is less than or equal to the *Transaction Limit* may be approved off-line by the MCP application or on-line by the MCP issuer.
- Transactions for which the value is greater than the *Transaction Limit* will be declined off-line.

The value of the *Transaction Limit* is set in the POI application and defined by the acquirer under the Card scheme rules (it may depend on different factors such as the merchant Category Code, etc., or the payment product).

6.6.5 MCP application risk parameters

The sections below provide a description of possible MCP risk parameters. It is at the discretion of the MCP issuer to make a choice on which parameters will be supported or to add any other risk parameter that seems to be appropriate.

6.6.5.1 *Mobile Code Try Limit and Counter*

The mobile code may be used as a CDCVM (see section 6.2). The *Mobile Code Try Limit* is a parameter indicating the maximum number of consecutive incorrect mobile code trials allowed.

The number of mobile code trials is recorded and the *Mobile Code Try Counter* represents the remaining number of trials allowed. The *Mobile Code Try Counter* is reset to the *Mobile Code Try Limit* after successful mobile code verification by the MCP application.

If the *Mobile Code Try Counter* is equal to zero, indicating no remaining mobile code trials are left, all further MCP transactions requiring a CVM and optionally all MCP transactions:

- are declined by the MCP application until the *Mobile Code Try Counter* is reset by the MCP issuer,

or

- are routinely sent on-line to the MCP issuer indicating that the *Mobile Code Try Counter* has reached zero, until the *Mobile Code Try Counter* is reset by the MCP issuer.

The value of the *Mobile Code Try Limit* is set in the MCP application and defined by the MCP issuer.

In case the mobile code is used as a CDCVM, it shall be used in conjunction with a *Mobile Code Try Limit* and *Counter* (see ReqS4 in Book 4 in [4]).

Note: In case biometrics are used this is typically a shared CDCVM, whereby a similar counter and limit exist; however, those are not managed by the MCP application.

6.6.5.2 *Consecutive No-CVM Limit and Counter*

The *Consecutive No-CVM Limit* is a parameter indicating the number of consecutive MCP transactions which can be performed before a CVM (typically a mobile code) is requested to protect against fraud.

The total number of No-CVM transactions is recorded in the *Consecutive No-CVM Counter* which is managed by the MCP application.

When a transaction is performed and the resulting *Consecutive No-CVM Counter* is greater than the *Consecutive No-CVM Limit*, then a CVM is required.

The *Consecutive No-CVM Counter* will be reset by the MCP application after the successful CVM verification.

The value of the *No-CVM Limit* is set in the MCP application and defined by the MCP issuer according to the Card scheme rules, taking into account:

- The risk of fraudulent transaction (e.g. in case of loss or theft of the mobile device).
- The convenience from the consumer perspective.

6.6.5.3 *Overview CVM-based risk management*

The next table provides an overview on the risk management related to the CVM as discussed above.

Transaction	Consecutive No-CVM Counter ≤ Consecutive No-CVM Limit	Consecutive No-CVM Counter > Consecutive No-CVM Limit
CVM	Optional	Mandatory

Table 9: CVM-based risk management

The *Consecutive No-CVM Limit* is the maximum number of consecutive transactions without CVM.

Note: Optional in the context of this table means that the CVM may be used depending on the outcome of other CVM related risk management (see section 6.6.4.1).

6.6.5.4 *Cumulative Off-line Limit and Amount Accumulator*

The *Cumulative Off-line Limit* is a parameter indicating the maximum total value of MCP transactions (amounts) which can be performed before an on-line authorisation request is required in order to protect against fraud or overdraft.

The total amount of off-line transactions is recorded in the *Cumulative Off-line Amount Accumulator* which is managed by the MCP application.

When an off-line transaction is performed and the resulting *Cumulative Off-line Amount Accumulator* reaches the *Cumulative Off-line Limit*, then an authorisation request is required.

The *Cumulative Off-line Amount Accumulator* may be reset per definition by the MCP issuer in one of the following ways:

- Via script processing performed Over the Air (OTA); here two modes exist, the so-called "push" (MCP issuer host initiated) and "pull" (MCP initiated) modes (see section 7.9.2). This reset may be optionally confirmed by the consumer (e.g., by entering a mobile code).
- Via script processing performed via the POI using NFC. This might require an additional tap or placing the mobile device on the NFC interface of the POI.

The value of the *Cumulative Off-line Limit* is set in the MCP application and defined by the MCP issuer according to the scheme rules, taking into account:

- The risk of fraudulent transaction (e.g. in case of loss or theft of the mobile device).
- The credit risk.
- The convenience from the consumer perspective.

Note that the MCP issuer may decide to use two different values, namely an Upper and a Lower Limit instead of the *Cumulative Off-line Limit*. In this case, if the total amount of off-line transactions is between the two values, an on-line transaction will be requested if possible. When the Upper Limit is reached, the transaction shall be processed on-line. If this is impossible because of an off-line POI, the transaction will be declined.

6.6.5.5   *Consecutive Off-line Limit and Counter*

The *Consecutive Off-line Limit* is a parameter indicating the number of consecutive off-line MCP transactions which can be performed before an on-line authorisation request is required in order to protect against fraud or overdraft.

The total number of off-line transactions is recorded in the *Consecutive Off-line Counter*[18] which is managed by the MCP application.

When an off-line transaction is performed and the resulting *Consecutive Off-line Counter* reaches the *Consecutive Off-line Limit*, then an authorisation request is required.

The *Consecutive Off-line Counter* may be reset per definition by the MCP issuer in one of the following ways:

- Via script processing performed Over the Air (OTA), hereby two modes exist, the so-called "push" (MCP issuer host initiated) and "pull" (MCP initiated) modes (see section 7.9.2). This reset may be optionally confirmed by the consumer.
- Via script processing performed via the POI using NFC. This might require an additional tap or placing the mobile phone on the NFC interface of the POI.

The value of the *Consecutive Off-line Limit* is set in the MCP application and defined by the MCP issuer according to the scheme rules, taking into account:
- The risk of fraudulent transaction (e.g. in case of loss or theft of the mobile device).
- The credit risk.
- The convenience from the consumer perspective.

Note: The MCP issuer may decide to use two different values, namely an upper and a lower limit instead of the *Consecutive Off-line Limit*. In this case, if the total number of off-line transactions is between the two values, an on-line transaction will be requested if possible. When the upper limit is reached, the transaction shall be processed on-line. If this is impossible because of an off-line POI, the transaction will be declined.

6.6.5.6   *Overview risk management off-line/on-line transactions*

The next table provides an overview on the risk management related to on-line and off-line transaction mode as discussed above.

---

[18] The consecutive off-line counter counts the number of transactions since the counter was explicitly reset by the MCP Issuer. An on-line transaction does not necessarily result in the counter being reset.

Transaction	Amount≤ Floor Limit	Cumulative Off-line Amount ≤ Cumulative Off-line Limit	Consecutive Off-line Counter ≤ Consecutive Off-line Limit	> Floor Limit or Cumulative Off-line Limit or Consecutive Off-line Limit
Mode	On-/Off-line	On-/Off-line	On-/Off-line	On-line

<p align="center">**Table 10: On-line/off-line risk management**</p>

Floor Limit is the maximum value of the Transaction Amount for an off-line transaction.

Cumulative Off-line Limit is the maximum amount of cumulative off-line transactions.

Consecutive Off-line Limit is the maximum number of consecutive off-line transactions.

In case of a reset, both *Cumulative Off-line Amount Accumulator* and *Consecutive Off-line Counter* will usually be reset together.

6.6.6 Additional Remarks

6.6.6.1 *Transaction currency*

If the transaction currency is different than the MCP application currency, an appropriate mechanism must be implemented in order to conduct the risk management related to off-line transactions. It is important to notice that in any case for each off-line transaction the MCP issuer risk is already limited by the maximum Floor Limit defined in 6.6.4.2.

Examples of mechanisms at the discretion of the MCP issuer to handle such transactions are:

- On-line authorisation request to the MCP issuer; which offers the most control but results in the declination of the transaction at an off-line only POI.
- Use of a currency conversion table in the MCP application, which offers a good control but introduces some overhead to the MCP issuer related to the management of the conversion table and which obviously can only support a limited number of currencies.
- Use of an alternative risk management which is not based on the transaction amount, e.g. by using the *Consecutive Off-line Limit*. However, this mechanism offers less control to the MCP issuer.

6.6.6.2 *Additional risk parameters*

Depending on the MCP product, additional risk parameters might need to be introduced, such as for prepaid, which are not further specified in this document.

6.6.6.3 *Parameters Update*

The POI parameters are updated by the acquirer. It should be possible to do this remotely.

The MCP application parameters are updated by the MCP issuer, typically using script processing. It might be executed using OTA.

6.7 Additional features

6.7.1 Transaction Logging

Each MCP application shall have its own transaction logging function. The MCP application shall store the transaction details in a dedicated log file in the MCP application. At a minimum, the last 10 transactions initiated shall be displayable[19] to the consumer while the number of transactions stored in the log file remains at the discretion of the MCP issuer. As on-line transactions may be declined by the MCP issuer, the transaction log may not match with the card statement. However, this transaction log allows at least the consumer to check independently the last 10 transactions initiated.

Every time a contactless transaction is initiated, a new record[20] is created and the transaction logging is updated in the MCP application. Afterwards the Payment Card Manager (PCM, see section 7.3.2) can retrieve the appropriate information from this log file to allow the consumer to view details of the transactions initiated. The PCM shall at a minimum display the last 10 transactions per MCP application.

The ordering of the transactions are recorded so Record #1 is the most recent transaction and Record #2 is the transaction prior to that, etc..

The MCP application updates the log file which should contain the following log data:

- Transaction Date and Time / Application Transaction Counter (ATC).
- Amount, Authorised.
- Amount, Other (i.e., cash-back).
- Transaction Currency Code.
- Cryptogram Information Data.
- Transaction Type.
- Merchant Name and Location.

Methods of presenting the transaction history within the PCM should be MCP issuer/application provider choice. The log should ideally enable to sort transactions by:

- Date (from most recent to oldest).
- Amount (ascending / descending).
- Transaction Type (debit / refund).

Depending on the MCP issuer's business requirements, an access control to this transaction logging display may be implemented (e.g., by requesting a mobile code verification). The MCP issuer may also choose to provide the consumers the ability to enable or disable this access control themselves.

6.7.2 Receipts

The transaction receipt is the payment receipt intended for the consumer. The handling of transaction receipts for MCP transactions is identical to the ones for transactions performed with physical cards. Section 4.2.3.10 in [4] provides further guidance. For

---

[19] The MCP application will always have an AAUI associated with it. The log data should be extracted from the MCP application and stored within the AAUI.

[20] Considering the integrity and security data aspect, the data within the MCP application's transaction log is not considered to be secure, i.e. there is no guarantee that EMV transaction logging data originated from a transaction with a genuine terminal.

POIs capable of printing a transaction receipt, it shall provide a receipt upon the consumer's request.

As mobile equipment offers additional capabilities, receipts may also be provided via other channels (e.g. electronic receipts).

6.8 MCP use cases

6.8.1 Introduction

The following use cases will be described in this document through a figure with a description of the different steps involved. Note that the use cases are presented for illustrative purposes, the list is not meant to be exhaustive.

Use case #	Description
Use case 1	Mobile phone - Payment transaction with single tap – off-line transaction – with CDCVM (mobile code) + variant on-line transaction
Use case 2	Mobile phone - Payment transaction with single tap - on-line transaction flow – on-line CVM (PIN at POI)
Use case 3	Mobile phone – Payment transaction with single tap - on-line transaction flow – no CVM
Use case 4	Mobile phone - Payment transaction with double tap - off-line transaction flow – CDCVM (biometrics)
Use case 5	Mobile phone - Payment transaction with double tap - on-line transaction flow – CDCVM (mobile code)
Use case 6	Wearable - Payment transaction with single tap - off-line transaction – no CVM
Use case 7	Mobile phone – Public transport
Use case 8	Mobile phone – Parking
Use case 9	Mobile phone - Payment transaction combined with loyalty card
Use case 10	Mobile phone – Cancellation of an MCP transaction
Use case 11	Mobile phone – Refund of an MCP transaction

Table 11: Overview MCP uses cases

The table below represents a mapping of the MCP use cases 1 through 6 on the MCP transaction table (see Table 7: Overview transaction types versus CVM usage).

Mobile device	MCP Transaction			
	Off-line		On-line	
CVM	Single tap	Double tap	Single tap	Double tap
On-line CVM	-	-	Use case 2	-
CDCVM	Use case 1	Use case 4	Use case 1 variant	Use case 5
No CVM	Use case 6	-	Use case 3	-

Table 12: Overview MCP uses cases versus MCP transaction types

6.8.2 Use case 1: Mobile phone - single tap – off-line transaction – CDCVM

This use case presents an MCP transaction, which is performed with a mobile phone via a single tap with an off-line authorisation and a mobile code.

Figure 17: Off-line transaction – single tap - CDCVM

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)

- The consumer either selects a payment card via a dedicated menu on their mobile phone for the payment or the default payment card (preselected on the consumer's mobile phone) is automatically used for the payment.
- The consumer enters their mobile code which is verified by the MCP Application.
- The merchant enters the transaction amount on the POI.

Step 1

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

Step 2

- The consumer taps their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI uses the contactless technology and selects the appropriate MCP Application through the PPSE.
- The contactless reader and MCP application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters.
- The audible tone and/or visible signal mentioned above indicate that the mobile phone - contactless reader interaction is completed. After this, the mobile phone can be removed from the contactless reader area. Note, however, that the transaction processing at the POI might still continue.
- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the mobile phone.
- An off-line card authentication/ transaction authorisation is performed by the POI.
- After processing the off-line authorisation, the merchant's POI displays an approval or decline.

Step 3

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

Variant: on-line transaction

In this cases the Step 2 reads as follows:

- The consumer taps their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until an audible tone and/or visible signal occur).

- The POI uses the contactless technology and selects the appropriate MCP Application through the PPSE.

- The contactless reader and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters.

- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the mobile phone.

- The consumer can remove their mobile phone from the contactless reader area.

- An off-line card authentication is optionally performed by the POI.

- An on-line card authentication / transaction authorisation is performed by the POI.

- After processing the on-line authorisation, the merchant's POI displays an approval or decline.

6.8.3 Use case 2: Mobile phone - single tap - on-line transaction – on-line CVM

This use case presents an MCP transaction, which is performed with a mobile phone via a single tap with an on-line authorisation and an on-line CVM (PIN at POI).
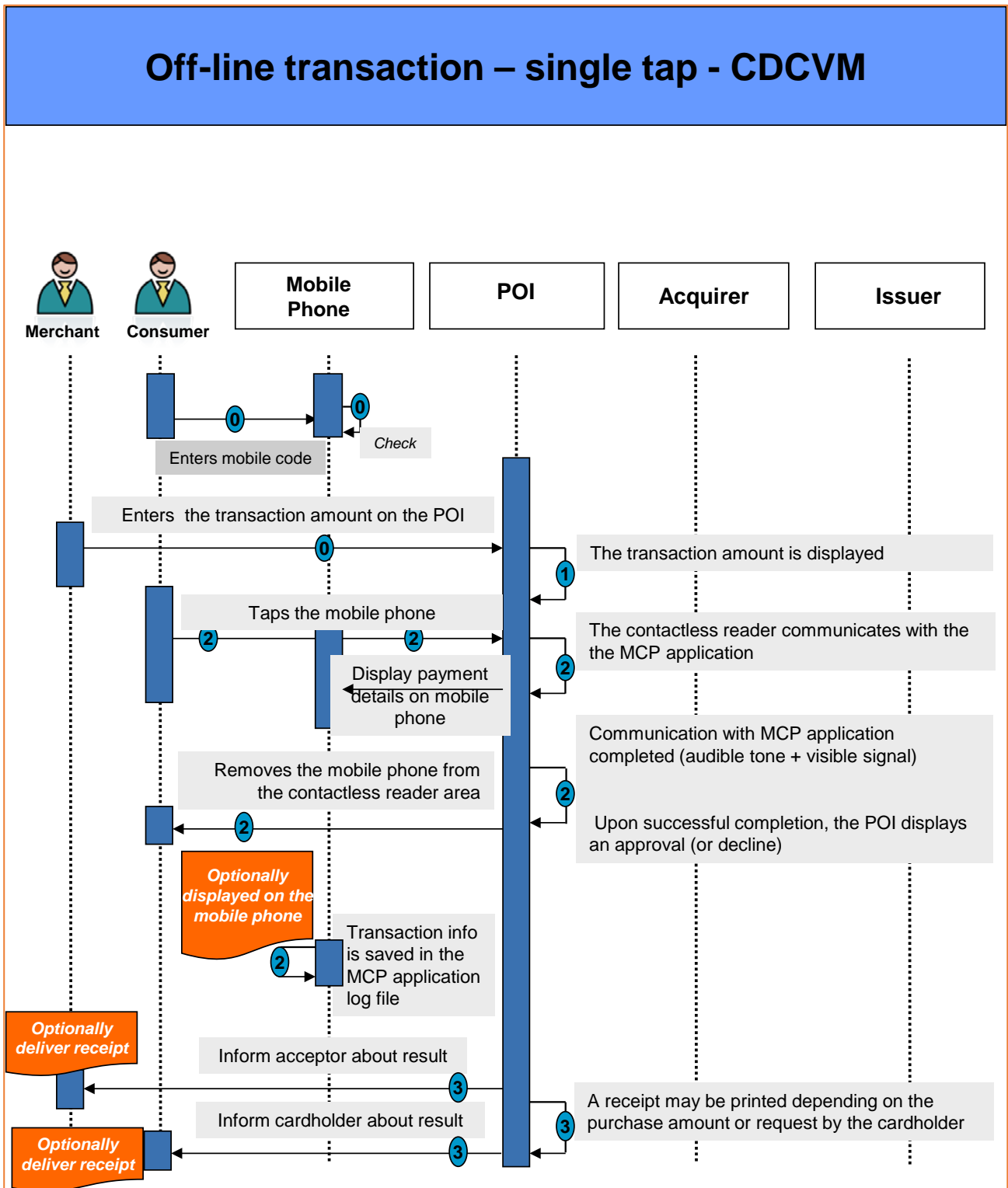

Figure 18: On-line transaction – single tap - on-line CVM

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)

- The consumer either selects a payment card via a dedicated menu on their mobile phone for the payment or the default payment card (preselected on the Consumer's mobile phone) is automatically used for the payment.

- The merchant enters the transaction amount on the POI.

Step 1

- The transaction amount is displayed on the merchant's POI.

- The POI requests for a card payment.

Step 2

- The consumer taps their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until an audible tone and/or visible signal occur).

- The POI uses the contactless technology and selects the appropriate MCP Application through the PPSE.

- The contactless reader and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to CVM, it is determined that an on-line CVM (PIN code on the POI) is required.

- The specific audible tone and/or visible signal mentioned above, indicate(s) that "half-course" transaction is completed and that the consumer is requested to enter their PIN code on the POI to complete the contactless payment transaction.

- The consumer can remove their mobile phone from the contactless reader area.

- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the mobile phone.

- An off-line card authentication is optionally performed by the POI.

Step 3

- The consumer checks the purchase amount and enters their PIN code on the merchant's POI.

- An on-line card authentication / transaction authorisation is performed by the POI.

- After processing the on-line authorisation, the merchant's POI displays an approval or decline.

Step 4

- The merchant is informed about result of the transaction.

- The consumer is informed about result of the transaction.

- Depending on the purchase amount, the merchant's POI features and consumer choice, a transaction receipt may be printed.

6.8.4 Use case 3: Mobile phone - single tap - on-line transaction – no CVM

This use case presents an MCP transaction, which is performed with a mobile phone via a single tap with an on-line authorisation without a CVM.
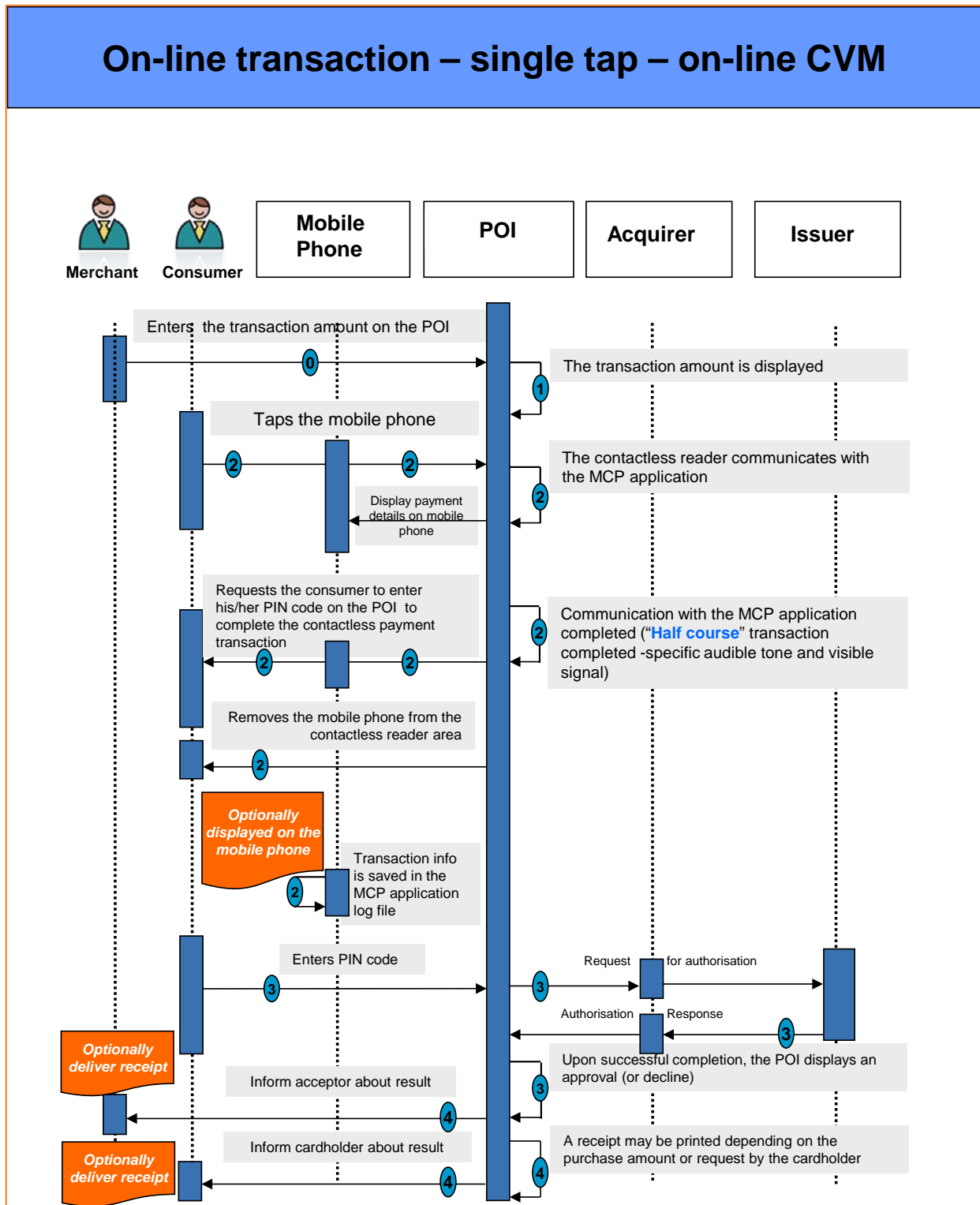

Figure 19: On-line transaction – single tap - no CVM

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)

- The consumer either selects a payment card via a dedicated menu on their mobile phone for the payment or the default payment card (preselected on the consumer's mobile phone) is automatically used for the payment.

- The merchant enters the transaction amount on the POI.

Step 1

- The transaction amount is displayed on the merchant's POI.

- The POI requests a card payment.

Step 2

- The consumer taps their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until audible tone and/or visible signal take place).

- The POI uses the contactless technology and selects the appropriate MCP Application through the PPSE.

- The contactless reader and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to CVM, it is determined that no CVM is required.

- The audible tone and/or visible signal mentioned baove, indicate(s) that the mobile phone - contactless reader interaction is completed. After this, subsequently, the mobile phone can be removed from the contactless reader area. Note however that the transaction processing at the POI might still continue.

- The consumer then removes their mobile phone from the contactless reader area.

- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the mobile phone.

- An off-line card authentication is optionally performed by the POI.

- An on-line card authentication / transaction authorisation is performed by the POI.

Step 3

- After processing the on-line authorisation, the merchant's POI displays an approval or decline.

Step 4

- The merchant is informed about the result of the transaction.

- The consumer is informed about the result of the transaction.

- Depending on the purchase amount, the merchant's POI features and consumer choice, a transaction receipt may be printed.

6.8.5 Use case 4: Mobile phone - double tap - off-line transaction – CDCVM

This use case presents an MCP transaction, which is performed with a mobile phone via a double tap with an off-line authorisation and a CDCVM (fingerprint).
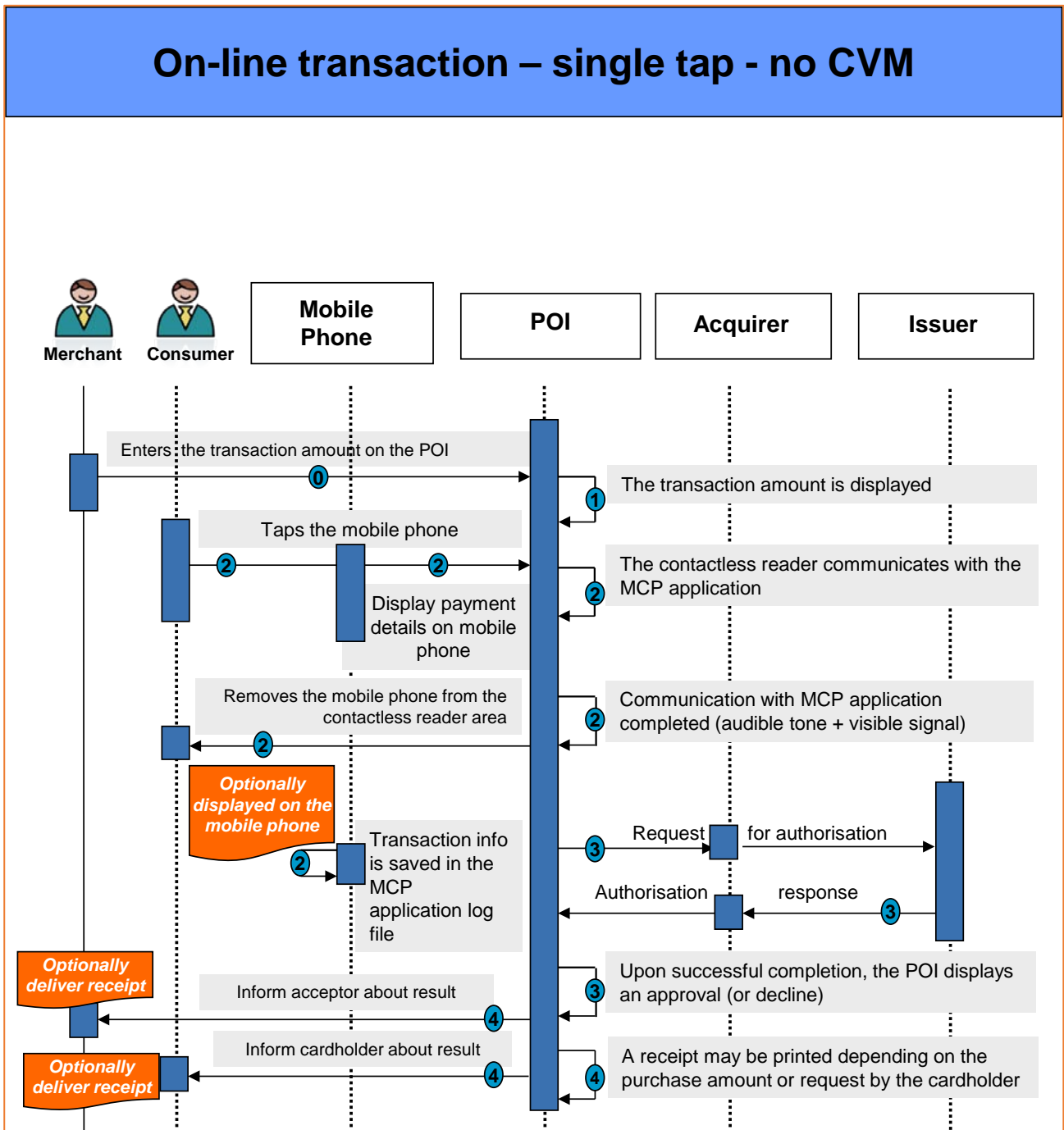

Figure 20: Off-line transaction – double tap – CDCVM

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)
The merchant enters the transaction amount on the POI.

Step 1
- The transaction amount is displayed on the merchant's POI.
- The POI requests for a card payment.

Step 2
- The consumer taps (1st tap) their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until audible tone and/or visible signal take place).
- The POI uses the contactless technology and selects the appropriate MCP Application through the PPSE.
- The contactless reader and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to CVM, it is determined that a CDCVM is required.
- The specific audible tone and/or visible signal mentioned above, indicate(s) that the first step of the transaction is completed and that the consumer is requested to enter their mobile code to complete the contactless payment transaction.
- The consumer then removes their mobile phone from the contactless reader area.

Step 3
- The consumer checks the purchase amount and presents their finger to the mobile phone.
- Upon successful verification of the fingerprint by the mobile phone, a message is displayed on the mobile phone requiring the consumer to tap again their mobile phone on the contactless reader area.

Step 4
- The consumer taps again (2nd tap) their mobile phone on the contactless reader area.
- An audible tone and/or visible signal then indicate that the mobile phone – contactless reader interaction is completed. After this the mobile phone can be removed from the contactless reader area. Note, however, that the transaction processing at the POI might still continue.
- Information about the current transaction (e.g. transaction amount) is saved in the MCP Application log file and optionally displayed on the mobile phone.
- An off-line MCP Application authentication / transaction authorisation is performed by the POI.

- After processing the off-line authorisation, the merchant's POI displays an approval or decline message.

Step 5

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

6.8.6 Use case 5: Mobile phone - double tap - on-line transaction — CDCVM

This use case presents an MCP transaction, which is performed with a mobile phone via a double tap with an on-line authorisation and a CDCVM (mobile code).
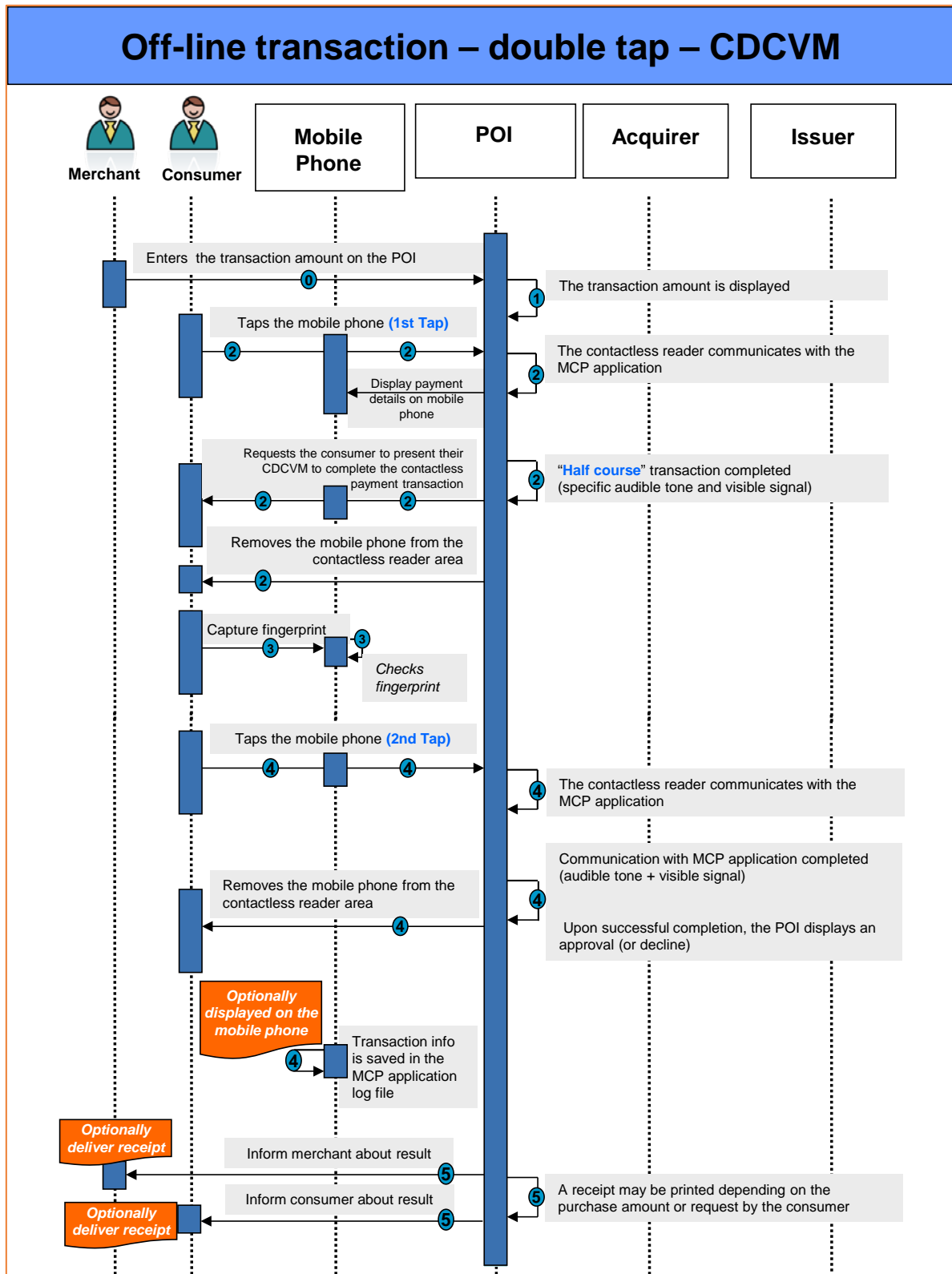
Figure 21: On-line transaction – double tap – CDCVM

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)
The merchant enters the transaction amount on the POI.

Step 1

- The transaction amount is displayed on the merchant's POI.

- The POI requests for a card payment.

Step 2

- The consumer taps (1st tap) their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until the audible tone and/or visible signal take place).

- The POI uses the contactless technology and selects the appropriate MCP Application through the PPSE.

- The contactless reader and MCP application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to CVM, it is determined that a CDCVM (mobile code) is required.

- The specific audible tone and/or visible signal mentioned above, indicate(s) that the first step of the transaction is completed and that the consumer is requested to enter their mobile code to complete the contactless payment transaction.

- The consumer then removes their mobile phone from the contactless reader area.

Step 3

- The consumer checks the purchase amount and enters their mobile code on the mobile phone.

- Upon successful verification of the mobile code, a message is displayed on the mobile phone requiring the consumer to tap again their mobile phone on the contactless reader area.

Step 4

- The consumer taps again (2nd tap) their mobile phone on the contactless reader area.

- An audible tone and/or visible signal then indicate that the mobile phone – contactless reader interaction is completed. After this the mobile phone can be removed from the contactless reader area. Note, however, that the transaction processing at the POI might still continue.

- Information about the current transaction (e.g. transaction amount) is saved in the MCP application log file and optionally displayed on the mobile phone.

- An off-line card authentication is optionally performed by the POI.

- An on-line MCP application authorisation / transaction authorisation is performed by the POI.

<u>Step 5</u>

- The merchant is informed about the result of the transaction.

- The consumer is informed about the result of the transaction.

- Depending on the purchase amount, the merchant's POI features and consumer choice, a transaction receipt may be printed.

6.8.7 Use case 6: Wearable - single tap - off-line transaction – no CVM

This use case presents an MCP transaction, which is performed using a wearable via a single tap with an off-line authorisation without a CVM.
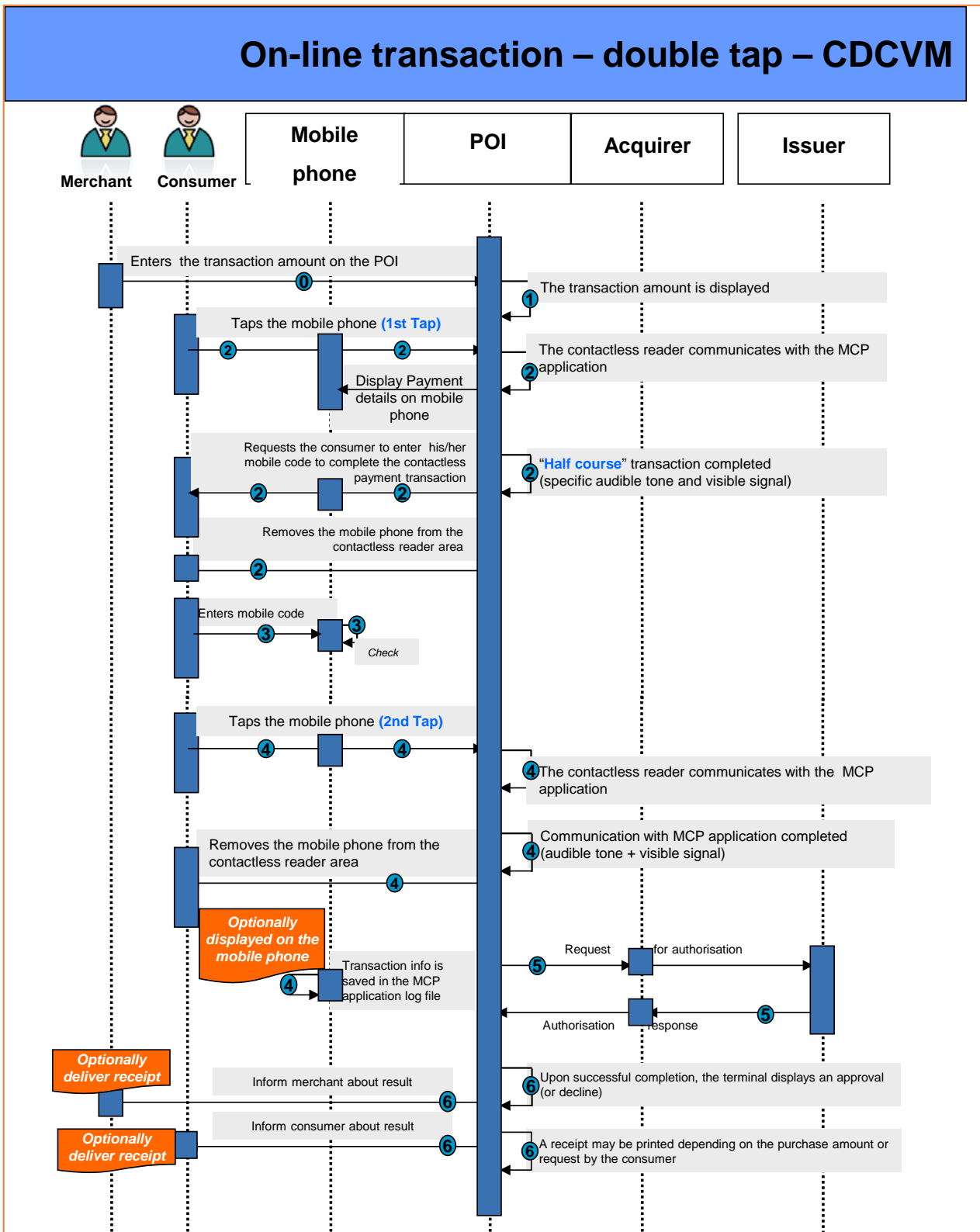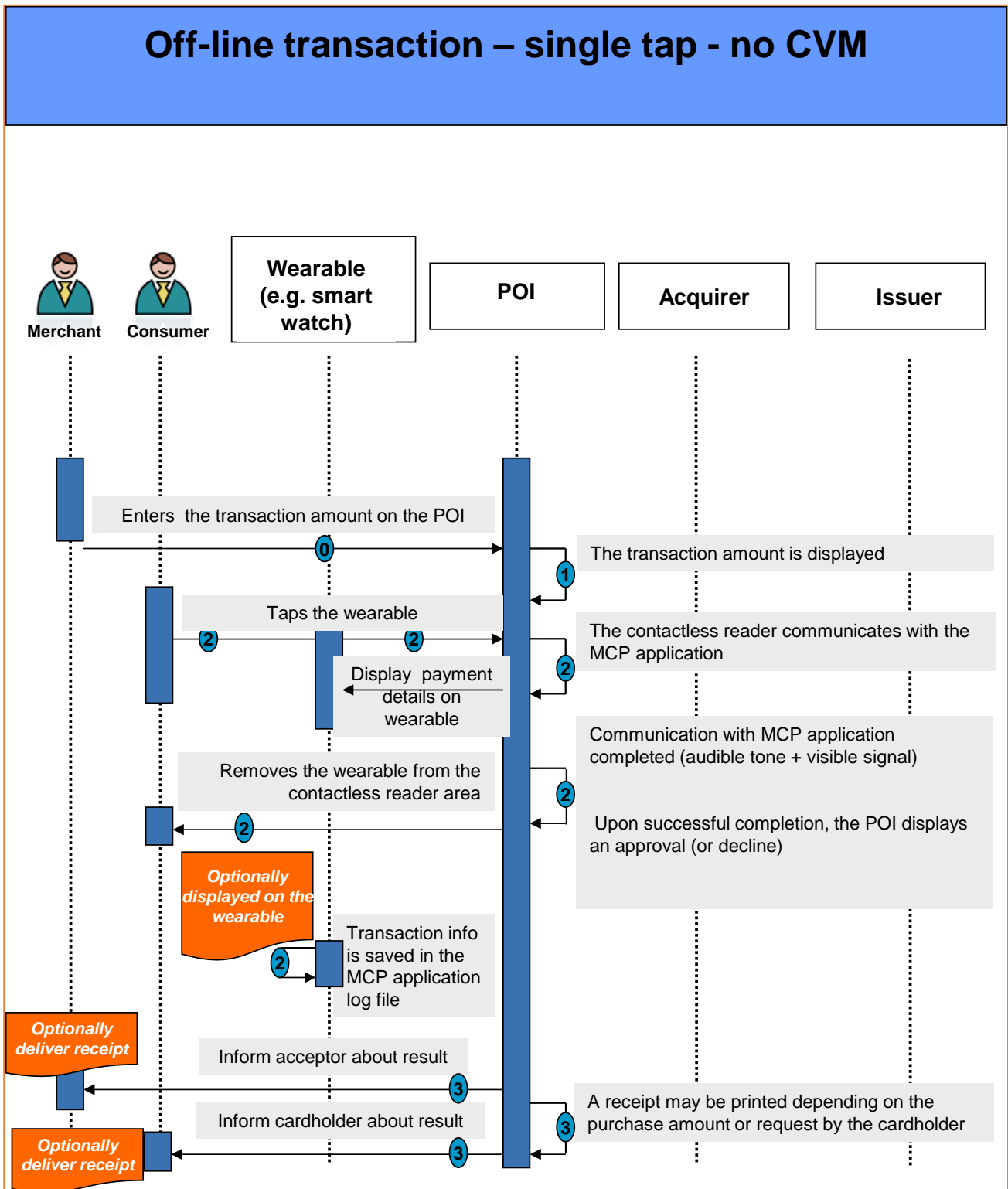

Figure 22: Wearable - on-line transaction – single tap – no CVM

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)

- The consumer either selects a payment card via a dedicated menu on their wearable for the payment or the default payment card (preselected on the consumer's mobile phone) is automatically used for the payment.
- The merchant enters the transaction amount on the POI.

Step 1

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

Step 2

- The consumer taps their wearable on the contactless reader area. (The consumer holds their wearable close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI uses the contactless technology and selects the appropriate MCP Application through the PPSE.
- The contactless reader and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to CVM, it is determined that no CVM is required.
- The audible tone and/or visible signal mentioned above, indicate(s) that the wearable - contactless reader interaction is completed. After this, the wearable can be removed from the contactless reader area. Note, however, that the transaction processing at the POI might still continue.
- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the wearable.
- An off-line card authentication/ transaction authorisation is performed by the POI.
- After processing the off-line authorisation, the merchant's POI displays an approval or decline.

Step 3

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

6.8.8 Use case 7: Mobile phone - Public transport - CDCVM

This use case presents an MCP transaction, which is performed using a mobile phone for the payment of public transport. It accommodates a variable fare with aggregation, based on the TfL (Transport for London) system.

Figure will be added in final version

Figure 23: Public transport — CDCVM

EPC144-17 v0.8 Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)

- The consumer either selects a payment card via a dedicated menu on their mobile phone for the payment or the default payment card (preselected on the consumer's mobile phone) is automatically chosen for used for the payment.

- The consumer enters their CDCVM (mobile code/ biometrics) which is verified by the MCP Application on the mobile phone.

Step 1

- The consumer taps their mobile phone on the contactless reader area (touch-in). (The consumer holds their mobile phone close to the contactless reader area until an audible tone and/or a visible signal takes place).

- The POI uses the contactless technology and selects the appropriate MCP Application through the PPSE.

- The contactless reader reads out the appropriate data from the MCP application.

- The card (MCP application) is checked against a deny list.

- The audible tone and/or visible signal mentioned above indicate(s) that the mobile phone - contactless reader interaction is completed and the gate opens. After this, the mobile phone can be removed from the contactless reader area. The consumer has entered the transit system.

- Information about the current transaction is saved in the MCP application log file and optionally displayed on the mobile phone.

Step 2

- The validated tap is collected in the transit operator's central back-office system.

- Where the card has not been seen by the transit operator in the previous 14 days a zero/nominal value on-line authorisation to the issuer is generated[21]. If the on-line authorisation is declined (statused /invalid card) it is added to the deny list.

Step 3

- When the consumer intends to leave the transit system, they tap their mobile phone on the contactless reader area (touch-out).

- An audible tone and/or visible signal/ gate opening indicate(s) that the mobile phone - contactless reader interaction is completed. After this, the mobile phone can be removed from the contactless reader area. The consumer has left the transit system.

---

[21] Note that on-line authorisation may not be immediate and in case of deny, the consumer can still leave the transit system.

Step 4

- The validated tap is collected in the transit operator's central back-office system.

Step 5

- At end of day, all the taps related to the same card (MCP applications) are aggregated and the applicable fare is calculated.

- Where an applicable authorisation trigger is reached an on-line authorisation for the value of the aggregated transactions is made.

- Depending on the authorisation response, transactions for settlement are submitted in accordance with agreed liability rules (e.g., liability for declined transaction less than a given amount may rest with the issuer).

6.8.9 Use case 8: Mobile phone - Parking — on-line transaction - no CVM

In the use case below, an MCP in a covered parking is described, which accommodates a fare based on the elapsed time between entering and leaving the parking. This use case is to be considered as an example for which multiple variants may exist.

Figure will be added in final version

Figure 24: Parking — no CVM

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)

The consumer either selects a payment card via a dedicated menu on their mobile phone for the payment or the default payment card (preselected on the consumer's mobile phone) is automatically chosen to be used for the payment.

Step 1

- The consumer taps their mobile phone on the contactless reader area (touch-in or check-in) at the parking meter.
- The POI uses the contactless technology and selects the appropriate MCP application through the PPSE.
- The contactless reader reads out the appropriate data from the MCP application.
- An audible tone and/or visible signal then indicate(s) that the mobile phone - contactless reader interaction is completed. After this, the mobile phone is removed from the contactless reader area.
- The validated tap is collected in the parking's central back-office system.

Step 2

- The parking's central back-office system checks the card validity/funds availability (e.g. *through a zero value on-line authorisation).*
- The parking's central back-office system sends the result back to the parking meter.
- The consumer is informed of the result via messaging on the parking meter's screen (allowed/not allowed).

Step 3

- When the consumer intends to leave the parking, they either select the same payment card via a dedicated menu on their mobile phone for the payment or the default payment card (preselected on the consumer's mobile phone) is automatically chosen to be used for the payment.
- The consumer taps their mobile phone on the contactless reader area (touch-out or check-out) at the parking meter.
- An audible tone and/or visible signal indicate(s) that the mobile phone - contactless reader interaction is completed. After this, the mobile phone is removed from the contactless reader area.
- Information about the initiation of the current transaction is saved in the MCP application log file and may be displayed on the mobile device.

Step 4

- The validated tap is collected in the parking's operator's central back-office system.
- The applicable fare is calculated.
- An on-line authorisation for the actual value of the fare is made.

Step 5

- The applicable fare and the result of the transaction are displayed on the screen of the parking meter.
- The consumer leaves the parking.

6.8.10 Use case 9: Mobile phone - Payment transaction with loyalty card — on-line transaction — no CVM

In the use case below, redemption from a loyalty application is used prior to an MCP transaction. For the MCP transaction, an on-line authorisation is performed. Subsequently, new points or rewards are collected on the loyalty application. This is to be considered as an example for which multiple variants may exist. The collection must happen after the actual payment in order to avoid the fraudulent accumulation of points.

Figure will be added in final version

Figure 25: MCP transaction with loyalty card

In the figure above the following steps are illustrated:

Step 0 (Pre-requisite)

- The merchant enters the transaction amount on the POI.
- The consumer selects a loyalty application in their mobile wallet and confirms the redemption amount by presenting a fingerprint to the mobile device.

Step 1

- The consumer taps their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI uses the contactless technology and reads out the loyalty related data from the selected loyalty application.
- The audible tone and/or visible signal mentioned above, indicate(s) that the mobile phone - contactless reader interaction is completed. After this, the mobile phone can be removed from the contactless reader area.

Step 2

- The merchant applies the redemption and the new transaction amount is displayed on the POI.
- If a balance payable is due, the POI requests a card payment.

Step 3

- The consumer selects a payment card in their mobile wallet.
- The consumer taps their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until audible tone and/or visible signal take place).
- The POI uses the contactless technology and selects the appropriate MCP application through the PPSE.
- The contactless reader and MCP application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to CVM, it is determined that no CVM is required.
- An audible tone and/or visible signal indicate that the mobile phone - contactless reader interaction is completed. After this, subsequently, the mobile phone can be removed from the contactless reader area. Note however that the transaction processing at the POI might still continue.
- Information about the current transaction is saved in the MCP application log file and, optionally, displayed on the mobile phone.

- An off-line card authentication is optionally performed by the POI.
- An on-line card authentication / transaction authorisation is performed by the POI.
- The consumer then removes their mobile phone from the contactless reader area.
- Loyalty collection, redemption points or rewards are updated within the loyalty application and optionally displayed on the mobile phone.

Step 4

After processing the on-line authorisation, the merchant's POI displays an approval or decline.

Step 5

- The merchant is informed about the result of the transaction.
- The consumer is informed about the result of the transaction.
- Depending on the purchase amount, the merchant's POI features and consumer choice, a transaction receipt may be printed.
- The consumer is able to check their new loyalty balance on-line via the dedicated loyalty application.

Note: If a decline is received by the merchant, the loyalty points will need to be adjusted.

6.8.11   Use case 10: Mobile phone - Cancellation of transaction

In the use case below, the off-line cancellation of an MCP transaction is described whereby the assumption is made that the original MCP transaction was authorised off-line and has not been captured yet by the Acquirer (based on SEPA Cards Standardisation Volume, Book 2, section 4.3.3) and the cancellation is performed according to the card scheme rules. This use case is to be considered as an example for which different variants exist depending on card scheme rules.

Step 0 (Pre-requisite)

- The consumer has just finished an MCP transaction at a merchant terminal which was authorised off-line using a given MCP application (selected payment card or default payment card on the mobile phone) and the cancellation of this transaction is requested.

- The consumer selects again the same payment card via a dedicated menu on their mobile phone for the payment or the default payment card (preselected on the consumer's mobile phone) is automatically chosen to be used for the cancellation.

- The merchant enters the information on the MCP transaction to be cancelled on the POI.

Step 1
- The cancellation of the transaction is displayed on the merchant's POI.
- The POI requests for the payment card[22].

Step 2
- The consumer taps their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until an audible tone and/or a visible signal takes place).

- The POI uses the contactless technology and selects the MCP application through the PPSE.

- The contactless reader reads out the appropriate data from the MCP application.

- An audible tone and/or visible signal then indicate that the mobile phone - contactless reader interaction is completed. After this, the mobile phone can be removed from the contactless reader area. Note, however, that the transaction processing at the POI might still continue.

- An off-line cancellation is performed which means that the original transaction is marked as cancelled in the POI.

- The merchant's POI displays the cancellation of the transaction.

Step 3

---

[22] With the sole purpose of retrieving card data.

- The merchant is informed about the result of the transaction.

- The consumer is informed about the result of the transaction.

- Depending on the purchase amount, the merchant's POI features and consumer choice, a transaction cancellation receipt may be printed.

6.8.12   Use case 11: Mobile phone - Refund

In the use case below, the refund of an MCP transaction with on-line authorisation is described (based on SEPA Cards Standardisation Volume, Book 2, section 4.3.2). This use case is to be considered as an example for which different variants exist depending on card scheme rules.

Step 0 (Pre-requisite)

- The consumer selects a payment card via a dedicated menu on their mobile phone for the payment or the default payment card (preselected on the consumer's mobile phone) is automatically used for the payment.

- The merchant enters the refund amount on the POI.

Step 1

- The refund amount is displayed on the merchant's POI.

- The POI requests for a payment card.

Step 2

- The consumer taps their mobile phone on the contactless reader area. (The consumer holds their mobile phone close to the contactless reader area until audible tone and/or visible signal take place).

- The POI uses the contactless technology and selects the appropriate MCP application through the PPSE.

- The contactless reader and MCP application mutually determine appropriate processing for the transaction. In this case, related to CVM, it is determined that no CVM is required.

- The audible tone and/or visible signal mentioned above, indicate(s) that the mobile phone - contactless reader interaction is completed. After this, subsequently, the mobile phone can be removed from the contactless reader area. Note however that the transaction processing at the POI might still continue.

- An on-line card authentication / transaction authorisation is performed by the POI.

- The consumer then removes their mobile phone from the contactless reader area.

- Information about the refund transaction is saved in the MCP application log file and optionally displayed on the mobile phone.

Step 3

- After processing the on-line authorisation, the merchant's POI displays a confirmation of the refund.

Step 4

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

6.9 Interoperability and MCP Service availability

Some countries in the SEPA area have chosen to systematically process payment transactions on-line, while other countries have opted for a mix of on- and off-line transactions, depending on the acquirer and the MCP issuer risk management configuration.

As long as MCP transactions remain domestic transactions, interoperability could be ensured. But what will happen if a consumer of an "on-line" country makes an MCP transaction in an "off-line" country? A transaction that needs to go on-line in pure off-line environment will be declined. Note that this is a similar problem to the physical cards world. The Card schemes and the payment service providers are encouraged to take appropriate actions to ensure the interoperability among all use cases with minimal impact on the consumer side and maximising the service availability.

One other aspect which might have an important impact on the consumer is the usage of the single or double tap. This situation might even get more complex if other contactless services such as loyalty, couponing are performed in conjunction with the MCP transaction. Therefore, stakeholders are encouraged to ensure at least consistency in a given geography. Moreover, they should appropriately educate their customers (both consumers and merchants) in this respect.

7 Technical and Security Infrastructure

MCPs fully leverage the infrastructure deployed for contactless SEPA card payments. The technical and security infrastructure described in this chapter complies with the SEPA Cards Standardisation Volume [4], while based on the MCP documents edited by EMVCo, see [6] to [16].

7.1 Introduction

This section provides a high-level overview of the technical and security infrastructure needed to support a contactless mobile payment transaction.

In order to conduct a payment transaction, the MCP application interacts with a contactless payment terminal (POI Device, see section 7.4), which is connected into the card payment acceptance infrastructure, responsible for authorisation, clearing and settlement.

The consumer selects and accesses the MCP application via the user interface (see section 7.5) of the mobile equipment (see section 7.3). Depending on the model, the MCP application is installed on an SE (see section 7.6) on the mobile device or is composed of an MA residing on the mobile device and a part implemented in the Mobile Application Cloud Platform (MACP). The processes for the provisioning and life cycle management of the MCP application, may vary depending on the model used (SE- or cloud-based, see sections 7.9 and 7.10). However, existing card personalisation systems can be leveraged for the personalisation of the payment application. In order to achieve this, third party providers might be involved. The authorisation of MCP transactions use the existing systems for cards (see section7.11).

7.2 MCP standards, specifications and white papers

MCPs 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:

- **ECSG**

The European Cards Stakeholders Group is a multi-stakeholder association supporting and promoting European card standardisation with market driven implementation. Its mission is to maintain and evolve the SEPA Cards Standardisation Volume [4] 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. Relevant EMVCo documents are listed in [5] through [18] (www.emvco.com).

- **ETSI**

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies, including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI defines GSM, UMTS telecommunication protocols and the UICC including all the access protocols. Moreover, ETSI is currently investigating the set-up of a new standardisation activity with appropriate stakeholders for a "Smart Secure Platform"[23]. Relevant ETSI documents are listed in [26] through [28] (www.etsi.org).

- **GlobalPlatform**

GlobalPlatform (GP) is an international association focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-service model implementations, which delivers benefits to issuers, service providers and technology suppliers. Relevant GlobalPlatform documents are listed in [32] through [39] (www.globalplatform.org).

- **GSMA**

The GSMA represents the interests of the worldwide mobile communications industry. Spanning more than 200 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, internet companies, and media and entertainment organisations. The GSMA is focused on innovating, incubating and creating new opportunities for its membership, all with the end goal of driving the growth of the mobile communications industry. Relevant GSMA documents are listed in [43] through [48] (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, communication protocols such as NFC, security mechanisms and is also is involved with mobile payments in ISO TC68 SC9. Relevant ISO documents are listed in [55] through [59] (www.iso.org).

- **Mobey Forum**

Mobey Forum is a global, financial industry driven forum, whose mission is to facilitate PSPs 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. Relevant Mobey Forum documents are listed in [51] through [54] (www.mobeyforum.org).

- **NFC Forum**

The Near Field Communication Forum is a non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices

---

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

and PCs. Relevant NFC Forum documents are listed in [60] and [61] (www.nfcforum.org).

- **PCI**

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

7.3 Mobile equipment

7.3.1 Introduction

The mobile equipment allows contactless communications by means of a dedicated NFC controller that is used in emulation mode to emulate a contactless card for MCPs. The next figure shows a mobile equipment architecture required to enable a POI to interact with the correct MCP applications based on the consumer's choice.
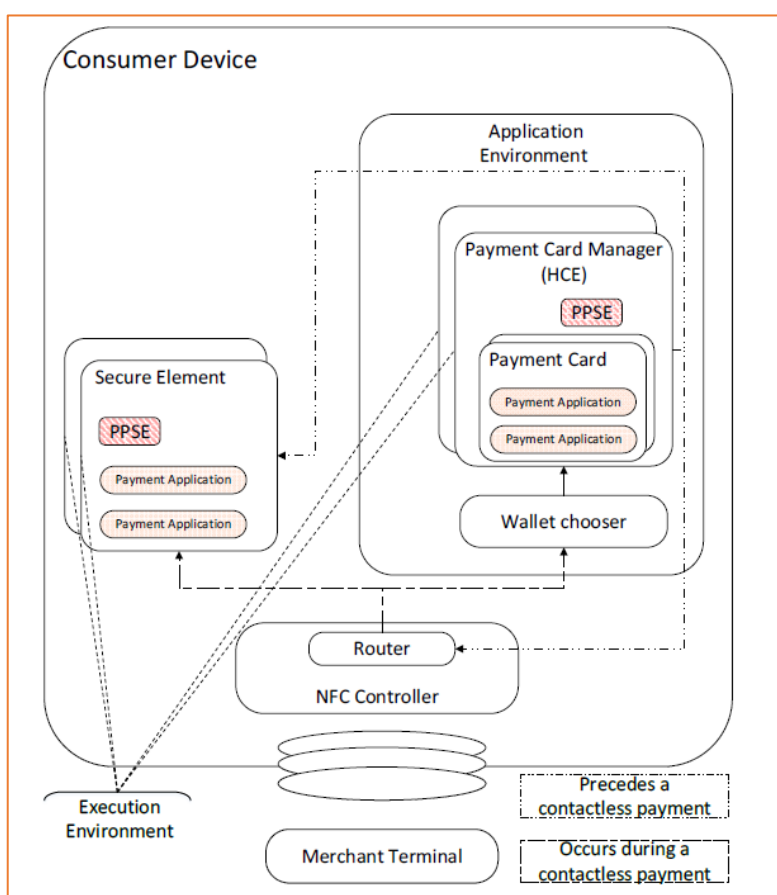

Figure 26: Mobile equipment architecture[24]

---

[24] This figure is courtesy of EMVCo, see [19].

The following components are represented in the figure:

- Payment Card Manager (PCM) – This component is a consumer visible mobile application (for example, a wallet app) resident within the mobile device application environment and used by the consumer to manage which Payment Card(s) will be used for conducting MCPs. More than one Payment Card Manager may be present on a mobile device.

- Payment Card – The consumer visible card(s) within a Payment Card Manager. This is typically the representation of a physical card product within a Payment Card Manager.

- Payment Application (MCP) – An application selectable over the contactless interface. The Payment Application could be present on an SE in the form of an applet or as a software card in the Payment Card Manager. There will be at least one Payment Application associated with a Payment Card, but depending on various factors, a Payment Card may be associated with multiple Payment Applications[25].

- Proximity Payment System Environment (PPSE) – An application selectable over the contactless interface. The primary responsibility of the PPSE is communicating the active Payment Application(s) and the respective priorities of the Payment Applications by responding to a POI. The Payment Applications are chosen by the consumer to be used for payment based on the selection of one or more Payment Card(s) within a Payment Card Manager. In this architecture, the PPSE is depicted as an applet on an SE or as a software card component of the Payment Card Manager.

- NFC Router – A component within the NFC Controller responsible for directing contactless communication to the correct execution environment on the mobile device.

- Wallet chooser – A platform may provide a feature to allow the consumer to set:
  - which Payment Card Manager(s) will interact with the consumer when a contactless payment transaction occurs;
  - [for HCE] which Payment Card Manager(s) will respond to commands received from the POI.

To enhance the user experience for MCPs, it is very important that consumer are aware of the exact location of the contactless NFC interface in their mobile equipment. Therefore mobile equipment manufacturers are strongly encouraged to clearly inform their customer about this and to strive for consistency amongst their different device models.

7.3.2 Payment Card Manager (PCM)

When EMVCo introduced in 2010 the concept of Application Activation User Interface (see [13]), most mobile devices that were enabled to process contactless payments were feature phones that did not specifically cater for a seamless experience when making a payment. Since then, the payment experience has improved significantly

---

[25] An an example, a Payment Card providing options for processing domestic or international transactions each being facilitated by a separately selectable MCP application.

based on a number of factors such as the improvements in mobile device processing power, incorporation of new biometric hardware and new means of user interaction (touchscreens), the adoption of the NFC Forum's NCI Specifications (see [62]) by most mobile device platforms and the adoption of relevant GlobalPlatform specifications (see section 7.6.2). These improvements allow a consumer to easily switch between multiple mobile applications on a device and between the choices offered by mobile applications. This has resulted in implementations that allow payments to be processed in less time and with less consumer interaction.

In addition, the support of HCE on the Android platform in conjunction with the support of Tokenisation (see section 7.8) and cloud-based based payment (see sections 7.7 and 7.10) by EMVCo and the Card schemes has resulted in a simplification of the provisioning process. This, along with the introduction of Apple Pay, has resulted in an increased adoption of mobile payment and provided an insight into where and how this space will progress.

Another important learning by EMVCo has been that in all cases, payment choice is performed by a wallet-type mobile application.

Taking the above into account, the original AAUI document has been split by EMVCo into a technical specification detailing both the requirements of a PPSE and the application management for SEs (see [13]) and a white paper which provides insight into the concept of a Payment Card Manager (see [19]).

The Payment Card Manager (PCM) is dedicated to the management of the interaction with the consumer, in connection with the MCP application located on the SE or as an HCE application. Hereby it is assumed that the Payment Cards is stored into one wallet (e.g. if a consumer has a Samsung phone with SamsungPay and AndroidPay, SamsungPay cannot see and manage the AndroidPay cards and vice versa).

7.3.2.1 *Representation of the MCP application*

The PCM should present information in an intuitive manner that is clearly recognisable and understandable to a typical consumer. Each MCP application in the list should have an equal amount of display real estate and a reasonable number of applications should be visible on any single screen.

Each MCP application is to be associated to a dedicated PCM which needs to be installed into the mobile equipment if not already present. The PCM is defined, developed and maintained under the responsibility of the MCP or wallet issuer. It should make use of the graphical capabilities of mobile equipment to display a specific PSP graphical interface, including the MCP issuer's logo.

Each PCM should contain the following:

- List the contactless applications related to the PCM if there are more than one;
- Allow the consumer to order the contactless applications within that list according to the consumers own preferences;
- Allow the consumer to prioritise the order in which a POI will interact with the contactless payment applications according to the consumer's own preferences.

In addition, contactless indicators should indicate to the consumer whether the device is capable of any communication over the contactless interface and should differentiate accessible and inaccessible applications.

Guidance on this topic may for instance be found in [22] and [63].

7.3.2.2 *Accessibility*

Consumers should have the capability to manage the accessibility status of their contactless applications. That is, the consumer should be able to set an application that is currently accessible to inaccessible and vice versa.

An example of a use case is when a consumer wants to lend their mobile phone to somebody but does not want to allow access to the MCP application.

7.3.3 Proximity Payment System Environment

7.3.3.1 *Definition*

The Proximity Payment System Environment (PPSE) is an application with the primary responsibility of communicating the active MCP applications and the respective priorities by responding to a contactless POI (see figure Figure 26).

The main purpose of any PPSE is to return an FCI (File Control Information) as a response to the selection of the PPSE application over an antenna interface. The content of the FCI contains a single MCP application directory entry or a list of MCP applications directory entries.

Each MCP application directory entry identifies the following information applicable to the entity selecting the PPSE (typically a POI):

- Applications available for selection and use by the contactless POI.
- The usage priority of each application.
- The specific POI application, i.e. the kernel, to be used to interact with this application on the mobile device.
- Other application-specific data.

7.3.3.2 *Functionalities*

For mobile devices, the PPSE typically contains additional functionality that allows the MCP application(s) reflected in the PPSE to be dynamically managed by the consumer through a Payment Card Manager. This mobile-specific functionality allows a Payment Card Manager to control the PPSE's response to the POI depending on the Payment Card choices of the consumer.

Additionally, MCP applications may be configured to be available (or not) when the mobile device is not switched on. Therefore, the response could depend on the PPSE's assumption related to whether or not the mobile device is switched on at the time it is presented to a POI.

There are three modes for the PPSE to receive and build the information that will be provided to the POI: External mode, Internal modes and Internal Mode with Mutual Exclusivity Rule.

- *External Mode:* In this mode, the PCM provides directly to the PPSE, the directory entry (see 7.3.3.2) of each MCP application that will be returned to the POI. External Mode is suitable for a single SE environment as well as when multiple Execution Environments (SE(s) and/or HCE) are active simultaneously.

- *Internal Mode*: In this mode, the PPSE itself will, internally to the SE, collect the details of the active applications from the SE contactless register services[26] and build the data to be presented to the POI. Internal Mode can only be used when a single SE is active

- *Internal Mode with Mutual Exclusivity Rule:* This mode is a variant of Internal Mode and is intended to ensure that no more than one Payment Card can be active at any time. When configured for this mode, the PPSE application behaves as if configured for Internal Mode, but over and above regular Internal Mode, it will deactivate any currently active MCP application when it is notified that a new MCP application has been activated.

For further information on the PPSE, the reader is referred to [13], [15] and [19].

7.4 Point of Interaction

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

A POI is capable of communicating with remote authorisation and clearing servers.

A contactless reader shall be connected to (or integrated with) this electronic device in order to carry out a contactless payment transaction and more specifically an MCP transaction.

The POI application shall support application selection through the Proximity Payment System Environment (PPSE – see section 7.3.3).

A POI supporting MCPs shall comply to the requirements specified in Books 2 and 4 of [4].

Visibility and transparency are key requirements for a good consumer experience on "where" and "how" to hold the mobile device to make a contactless payment. Therefore, manufacturers and retailers are encouraged to take the following guidelines into consideration.

POI Manufacturers
- Equip the POI with a clearly visible landing zone displaying the EMVCo Contactless Symbol, where the mobile device needs to be tapped by the consumer (see [20]);
- Standardise the "POI" look as much as possible for a given payment environment (e.g. shop, fuel station, vending machine, etc.). As an example vendors are encouraged to put the contactless antenna at the same location and to design equal access for terminals to the card slot for contact and the landing zone for contactless;
- Consider ergonomic optimisations (e.g., larger screens);
- MCP transaction steps should be accompanied by visuals, audible and messages – use clear picture language wherever possible;

---

[26] A register employed by an SE to manage the contactless applications thereon (see for instance [36]).

- Ensure accessibility for people with disabilities, as appropriate (e.g., see [1], [29] and [31]).

Retailers
- Clearly signpost that contactless payments are accepted, not only at the POI but as an example as soon as consumers enter the shop;
- Place the POI/contactless reader clearly facing and accessible to consumers;
- Educate their staff and ask them to promote MCPs. (see [30]).

It is further recognised that new types of POI terminals are entering the market such as mobile phones, tablets, PDAs, etc. They may introduce new risks which need to be appropriately addressed (e.g., entering a PIN on these devices). Security requirements for mobile POI devices are included in section 3.7 in Book 4 of [4].

7.5 Selection of the MCP application

Prior to performing an MCP, consumers, dependent on the mobile device model, wallet configuration and/or operating system, may have to perform, or can choose to perform, some additional steps:

- They may have to activate the mobile device screen to enable NFC payments.
- They can choose to have the NFC interface available for payments or not (regardless of the state of the screen).
- They may select a default payment card through the mobile phone operating system or through functionality provided by their wallet provider (i.e. the "card" that will be presented to the POI for payment)[27].
- They may choose to perform an identity verification step on their mobile device (e.g., enter a code, a biometric identifier, etc.) prior to every transaction regardless of whether the eventual transaction risk analysis requires a CVM (see section 6.2) or not.

The method for selecting an MCP application on a mobile device is an implementation option, and could vary dependant on a number of factors. These factors include the type of mobile device, the device operating system, the MCP architecture, wallet design, as well as a number of issuer and consumer preferences (settings).

Selecting payment applications on a mobile device will always result in either no payment application, a single payment application, or several payment applications available for selection by the POI, depending on which applications are supported by the POI. However, at this point application selection on the POI follows normal Application Selection rules (see [4]).

---

[27] For the selection of the application on the mobile device by the consumer, the reader is referred to section 7.5.

Use case 1: MCP application selection prior to payment

The consumer may select their preferred MCP application via a wallet in their mobile device prior to the payment. Note that a consumer may have several wallets in their mobile device. When tapping the mobile device to the POI, a single MCP application will be presented to the POI, which may be automatically selected.

Use case 2: Selection of application in case of multiple MCP applications

A mobile device may return several co-badged MCP applications in the PPSE to the POI in which case and additional selection of application by the consumer and the merchant needs to be performed on the POI. This second application selection on the POI will follow the normal application selection rules valid for cards (see section 2.2.21 in Book 6 in [4]). However, from a consumer perspective this should be avoided in view of a "simple" user experience.

Annex D: An example of construction of the PPSE, illustrates how the PSSE can response to the POI depending on the selection of the application by the consumer.

For further details on the selection of the application, the reader is referred to section 2.2 in Book 6 of [4].

7.6 Secure Element

7.6.1 Introduction

An SE is a tamper-resistant module capable of hosting applications in a secure manner. The SE provides a protection of the applications including separation of the applications. The SE may appear in different form factors in the mobile equipment.

In this document the following form factors are covered:

- A UICC
- An eSE
- An eUICC.

Regardless of the form factor, an SE shall contain:

- An Operating System which supports the secure execution of applications and secure storage of application data. The operating system may also support the secure loading of applications.
- Two communication interfaces:
    - o A device (contact) interface which enables commands and responses to be exchanged between the SE and authorised mobile applications in the mobile equipment.
    - o An antenna interface (contactless) interface which enables the exchange of commands and responses between an application in the SE and a contactless Point of Interaction via the NFC Controller of the mobile equipment.

- A Manager to maintain a list of contactless applications on the SE, the status of the applications and the associated data. The status of an application indicates if the application is available for selection on the contactless interface.

The SE is uniquely identified by the SE identifier (SEID[28]), regardless the type of SE (e.g., by using the UICC_ID, CUD (Card Unique Data) as defined by GP Card Specification, see [32]).

7.6.2 Security Domains and GlobalPlatform Management Profiles

This section provides a high-level overview of the concept of security domains and applicable management profiles. For more details, the reader is referred to [32] to [42].

7.6.2.1 *Definition*

Security Domains (SDs) act as the on-SE representatives of off-SE authorities. There are three main types of security domains, reflecting the three types of off-SE authority recognised by an SE:

- The issuer security domain (ISD) is the primary, mandatory on-SE representative of the SE administrator, typically the SE issuer.
- The supplementary security domains (SSDs) are additional, optional on-card representatives of application providers (e.g. MCP issuer) or their agents (e.g. TSM). The SSD manager is responsible for managing instantiated security domains on a card. It holds the secure channel protocol keys and/or certificates belonging to the security domain it is in charge of. It is also responsible for managing the secure communication to this security domain. As such, the SSD manager can load, install, extradite or personalise applications on the SD.
- The controlling authority security domains (CASDs) are a special type of SSD. The controlling authority supports the following responsibilities which may be performed by two different actors:
  - o It controls a specific CASD which can enable confidential key loading (confidential key loading authority) for setting up the initial keys of an SSD.
  - o It may also control a specific SD used to enable mandated data authentication pattern (mandated DAP authority). The mandated DAP deployment model allows an actor to securely verify on card all application code when it is loaded in a card.

In the present document, all three types are simply referred to as SD. SDs support security services such as key handling, encryption, decryption, digital signature generation, application loading and personalisation and their verification as needed. Each SD is established on behalf of an SE issuer, an MCP issuer or a controlling authority when these off-SE entities require the use of keys that need to be completely isolated from each other.

Note that also EMVCo has defined a profile for the configuration of a UICC supporting MCP (see [12]).

---

[28] There are standardisation activities ongoing in GlobalPlatform such as "Messaging configuration for management of mobile-NFC services" and "Secure Element Remote Application Management" which covers the different SE form factors and alternatives.

7.6.2.2 *The key roles*

The key roles for the MCP application life cycle management are described below:

- The controlling authority manages exchanges with an optional third party entity when required by the deployment model.

- The SE issuer holds the responsibility for the SE. An SE issuer may be the only authority to allow load, install, delete, extradition or personalisation of applications, or the SE issuer may delegate load, install, extradition or personalisation of the applications to a third party such as an MCP issuer, via the SSD manager. The SE issuer provides SEs to the consumers. The SE issuer is responsible for securely managing all the pre-issuance production processes culminating in an SE specifically prepared for a consumer, and for many post-issuance processes, including final decommissioning of an SE. The SE issuer determines a portfolio of applications to be supported and offered to its SE base.

   The SE issuer manages authorisation of applications permitted to reside on its SEs. The SE issuer performs pre-personalisation functions, specifically the loading of the initial ISD, a CASD and, if any, application provider's SD (i.e. MCP issuer's SD). Furthermore, the SD needs to be personalised with specific data related to the SE issuer, controlling authority or application provider.

- The SSD manager manages instantiated Security Domains on a card. If authorised by the SE issuer, the SSD manager is able to create other Security Domains to host multiple MCP issuers.

- The MCP issuer procures the necessary components to load a complete MCP application (i.e. application code, application data, application keys and/or certificates, and data belonging to a specific consumer) onto an SE. The MCP issuer has a direct business relationship with and provides an SE-based service to the consumer.

- The consumer is the entity receiving the SE. He/she controls the download of MCP applications into the SE under the authorisation of the SE issuer.

7.6.2.3 *SE management modes*

For MCPs, the SE issuer provides the SE which hosts the MCP application. GlobalPlatform has specified three different management modes to perform card content management (i.e. loading, installing, activating or removing the application). These modes are:

- Simple mode: an SE issuer centric model, where card content management is only performed by the SE issuer but can be monitored by the MCP issuer and/or a TSM. The SE issuer provides the MCP issuer with the SD.

- Delegated mode: card content management can be delegated to an MCP issuer and/or a TSM but each operation requires pre-authorisation from the SE issuer, e.g., MCP application loading.

- Authorised mode: card content management is fully delegated to an MCP issuer and/or a TSM for a sub-area of the SE.

The management modes may impact the service management roles (e.g., who manages the SSD) and therefore the business model between the different stakeholders. The SE issuer may support all the management modes or only some of them.

In all alternatives, the MCP issuer can manage the personalisation process itself or delegate it to a TSM. The security is guaranteed through the confidential set-up of initial secure channel keys, in which a controlling authority may be used.

7.6.2.4 *Example of management mode scenarios*

In these examples, different models of shared responsibility between the SE issuer such as the MNO or mobile equipment manufacturer and the MCP issuer to control, via the OTA platform, the management of the SE are presented. Only a few selected card content management functions are taken into the example. The table below shows some alternatives using a TSM and, while not the full picture, it aims to highlight differences between the various management modes.

SE Issuer	MNO	MNO	Mobile equipment manufacturer
Management mode	Simple mode using SE issuer OTA platform	Delegated mode with full/partial delegation to TSM	Authorised mode
MCP Issuer SD creation	TSM via SE issuer OTA platform	TSM with SE issuer pre-authorisation via TSM OTA platform	SE issuer
MCP application loading	TSM via SE issuer OTA platform	TSM with SE issuer pre-authorisation via TSM OTA platform	MCP Issuer or TSM via TSM OTA platform
Personalisation	TSM via SE issuer OTA platform	MCP issuer/TSM via TSM OTA platform	MCP issuer via TSM OTA platform

Table 13: Example of management mode scenarios

For more detailed information on this topic, the reader is referred to [37].

GlobalPlatform has released an End-to-End Simplified Service Management Framework for Payment [39] to streamline the service management process, by leveraging GlobalPlatform standards through the creation of simple end-to-end configurations specific to a vertical segment.

End-to-end configurations will enable providers to deploy services faster by starting with a basic template. This document covers a number of such end-to-end configurations by specifying:

- The workflows between the involved parties to ensure a proper user experience

- The overall architecture to provide clarity in the data flow and implementation

- The configurations and options for the various interfaces and devices to ensure interoperability.

Stakeholders may select their end-to-end configuration by answering a simple set of questions. The configurations selector will filter out the options. Each configuration is self-contained and describes an end-to-end system where each involved entity will be able to determine how to implement its own components.

The usage of this framework should considerably reduce the time needed to set-up an MCP ecosystem for SE-based models.

7.6.2.5 *Interworking Between Multiple Contactless Card Emulation Environments*

The arrival of the HCE and eSE in premium smart phones has raised multiple questions about the best way to manage multiple contactless environments. In 2016, the three main organisations ETSI, GlobalPlatform and NFC Forum decided to collaborate to solve this problem that is impacting the end user experience across different potential implementation in consumer devices and therefore slow down NFC services acceptance and deployment.

In March 2017, the three organisations have published a common white paper [35] to explain the solution selected and the details of the expected behavior of multiple NFC services hosted in the same consumer device on order to simplify the end user experience.

This covers services such as payment, transport, loyalty or access control. The approach will also be of interest to OEMs developing devices that support NFC services. For consumers, this clarity brings guarantee that services will work as advertised, regardless of the hosting contactless environment selected by the service provider.

As an umbrella approach, the GlobalPlatform Managing Entity Specification [41] ensures that multiple mobile contactless services may successfully coexist within a mobile device and that they will operate as intended, regardless of the hosting environment (eSE, HCE, UICC) selected by the service provider.

The "Managing Entity" offers an end user access to all contactless services in order to activate, de-activate and prioritise them. This specification is fully compatible with current contactless wallets offered by service providers or handset manufacturers. The "GlobalPlatform Managing Entity Specification" is supported by the latest versions of [27] and [62].

The GlobalPlatform Managing Entity Specification provides a mode that is backward compatible to all SEs already in the market. It supports the activation of multiple NFC services at the same time within a single mobile device independent of the hosting environment and has the ability to detect any potential conflicts. It also details how to simplify the end-user experience when selecting NFC services for entities such as mobile wallet providers.

7.7 Host Card Emulation (HCE)

Until recently, SE-based near-field communication (NFC) was the only practical and interoperable technology option to enable MCPs. Now, with major operating systems supporting Host Card Emulation (HCE), any application in the mobile device can directly access the NFC capabilities to communicate with a merchant's contactless POI. HCE eliminated any dependencies on having an SE. This provides a simpler option for the adoption of NFC by enabling MCP issuers, merchants, and third party application developers to provide consumer experiences for MCPs without the technical or commercial integrations required for the SE-based model.

Previously, an NFC application on a mobile device communicating with a contactless reader would have to be coded for and executed in an SE, but newer mobile device operating systems (OS) and implementations allow the application that receives and processes the payment transaction Application Protocol Data Unit (APDU) commands sent from the contactless reader to be coded for and executed in the application processor of the mobile device. As an example, this type of contactless payment was introduced by Google's introduction of the Host Card Emulation (HCE) in Android 4.4 KitKat and later versions.

To enhance the security, HCE-based solutions may be offered in combination with Tokenisation, see 7.8.

For further information on HCE the reader is referred to [47] and [54].

7.8 Tokenisation

In order to enhance the security of mobile payment transactions, more in particular for HCE-based solutions, so-called payment tokens may be used. They generally refer to a surrogate value for consumer (payer) account related data, which is used for payment transactions.

The EMV Payment Tokenisation Specification – Technical Framework v2.0 [18] describes the baseline requirements for the use of EMV Payment Tokens within the existing payment ecosystem through the establishment of a Token Programme. EMV Payment Tokens are surrogate values that can be used to replace the PAN in the payment ecosystem. EMV Payment Tokens are designed to provide transparency to payment ecosystem stakeholders when accepting and processing EMV Payment Tokens. EMV Payment Tokenisation is the process of replacing a Primary Account Number (PAN) with a unique EMV Payment Token that is restricted in its usage. They are issued by so-called "Token Service Providers", on the request of the issuer or a TPP.

An EMV Payment Token provides improved protection when its use is limited to a specific domain(s), such as a merchant, card / form factor (including mobile devices, wearables, etc.) or channel such as proximity payments. The application of these underlying usage controls, known as the Token Domain Restriction Controls, is a primary component and benefit of EMV Payment Tokens. The Token Domain Restriction Controls can be used to limit the use of an EMV Payment Token to its intended use (for example, prevention of the successful use of an EMV Payment Token outside of a specific channel).

EMV Payment Tokenisation can be used in many different usage scenarios within a payments ecosystem. The specific usage scenarios are implementation specific and could include, but are not limited to proximity payments. One of the example usage scenario referenced in the EMV Payment Tokenisation Specification – Technical Framework v2.0 is Use Case 1 - Mobile NFC at Point of Sale. This equates to an MCP that is using an EMV Payment Token. This example of EMV Payment Tokenisation uses an NFC-enabled mobile device at a contactless-enabled POI and communication is made using NFC. Cardholder experience may differ based on mobile device type. An EMV

Payment Token is stored within an NFC-enabled mobile device or alternatively in a remote server and delivered to the mobile device prior to commencing a transaction.

EMVCo has also introduced the EMV Payment Account Reference (PAR), which enables merchants, acquirers and payment processors to link together a cardholder's EMV payment token and PAN transactions. The new version 2.0 of the tokenisation specification (see [18]) clarifies this at a standards level and sets the rules for BIN controllers (such as an ISO IIN Card Issuer) to implement PAR for their BINs.

Further details on the usage of tokenisation in the context of MCPs may be found in [18].

7.9 Back-end systems for the life cycle management of SE-based MCPs

The MCP application interacts with a POI device that is connected to the card payment acceptance infrastructure, responsible for authorisation, clearing and settlement.

As a mobile phone has mobile network connection capabilities, an option to install the MCP application on an SE is to use a personalisation and provisioning server that communicates with the SE via this mobile network connection (e.g. OTA). In that case, dedicated processes need to be defined for the provisioning and management of the MCP application. They may vary depending on the SE form factor.

It is expected that existing card personalisation systems can be leveraged for the personalisation of the payment application. In order to achieve this, third party providers might be involved.
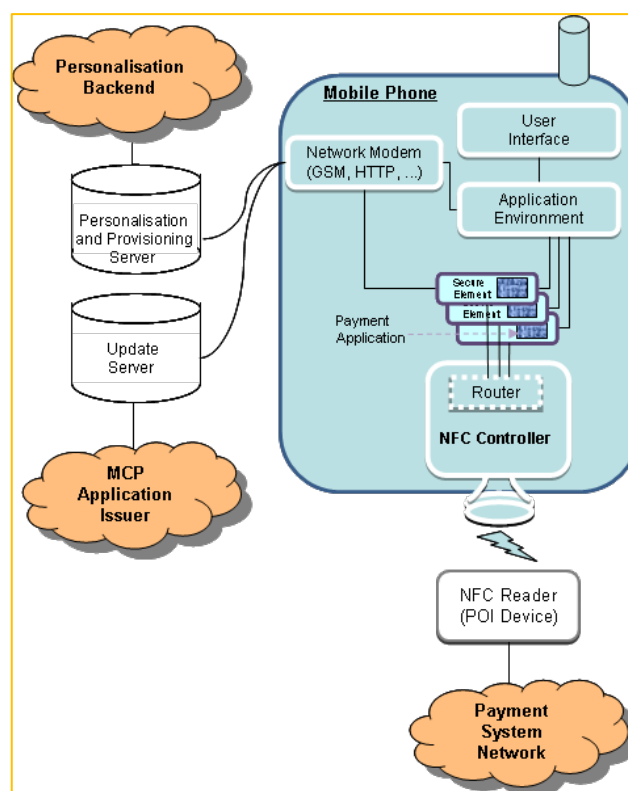

Figure 27: SE-based MCP lifecycle management back-end system

7.9.1 Provisioning

For deployment of an MCP application to a mobile device, the term "provisioning" is used to cover:

- Pre-personalisation: preparing the SE to receive personalised account data, including loading the application code onto the SE and setting up any personalisation keys necessary to protect that account data. This may be done over the air once the mobile phone is in the hands of the consumer, or may be done in a card bureau (for UICC or secure micro SD card) prior to physical dispatch to the consumer.
- Personalisation: loading the personal account data over the air into the MCP application, including using the personalisation keys unique to the card to protect the confidential account data (PIN, Keys).
- Activation: the cardholder confirms to the MCP issuer that the application has been personalised and is ready to use.
- Post-activation Management: loading of a new (version of the) or deleting an MCP application using OTA.

The personalisation and provisioning server is connected to a personalisation back-end, which allows the MCP issuer (or a third party) to issue the MCP application to the mobile equipment, hereby assuming the role of SSD manager (see section 7.6.2.1).[29]

Several options could be chosen to install the MCP application on the SE, such as remotely via OTA or preloaded in the factory before the supply.

- For the UICC SE, the document on the "MCP Service Management Roles - Requirements and Specifications" [21] provides guidance on the MCP application provisioning.
- For an eSE, there is a requirement for an administration agent (e.g., a mobile application: midlet, Android application) to provide connectivity between the SE and the provisioning service. The administration agent can be downloaded over the air (e.g., from App Store) or pre-installed.

Special care on the TSM side is required when the mobile equipment is changed in case the SE is a removable device, to guarantee continuity of service.

7.9.2 MCP management systems

Once the MCP application is installed and provisioned, it may be updated via the Update Server (see Figure 27). This allows the update of MCP application risk parameters and counters (see section 6.6.5).

The MCP management for SE-based models is similar to cards but the OTA is an additional channel available for the Update Server to communicate. The counters may be reset by the MCP issuer using OTA or via script processing.

For OTA two modes exist:

- The push mode where the reset is initiated by the MCP issuer host.
- The pull mode where the reset is initiated by the MCP. This reset may be optionally confirmed by the consumer (e.g. by entering a mobile code)

---

[29] The MCP application might also be preloaded on the SE prior to its issuance.

Script processing is performed via the POI using NFC. This might require an additional tap or placing the mobile device on the NFC interface of the POI.

7.10 Back-end systems for the life cycle management of cloud-based MCPs

7.10.1 Provisioning

How an installation of a cloud-based payments program is performed, and the associated roles and responsibilities, is an implementation decision. However, some of the major components and implementation considerations are given below.

A cloud-based payments program enables issuers to configure characteristics to provide a cloud-based payments experience desired for their accounts. Characteristics would include several risk parameters that manage the triggers for refreshing account parameters on a device.

The program is responsible for several core functions in the life of an account, these functions are provisioning, active account management, verification for payment, transaction processing, lifecycle management and post-payment activities.

Other functions to consider are the initial configuration process, billing, reporting and integration with enrolment and verification systems. How these are implemented and what each of the additional capabilities does is at the discretion of the program provider.

The major components are represented in the figure below.

Cloud-based Payments Platform
- Provisioning
- Active Account Management
- Verification for Payment
- Transaction Processing
- Lifecycle Management

Mobile Application Platform
- Application Management

Mobile Device
- App Environment (wallet or mobile app)
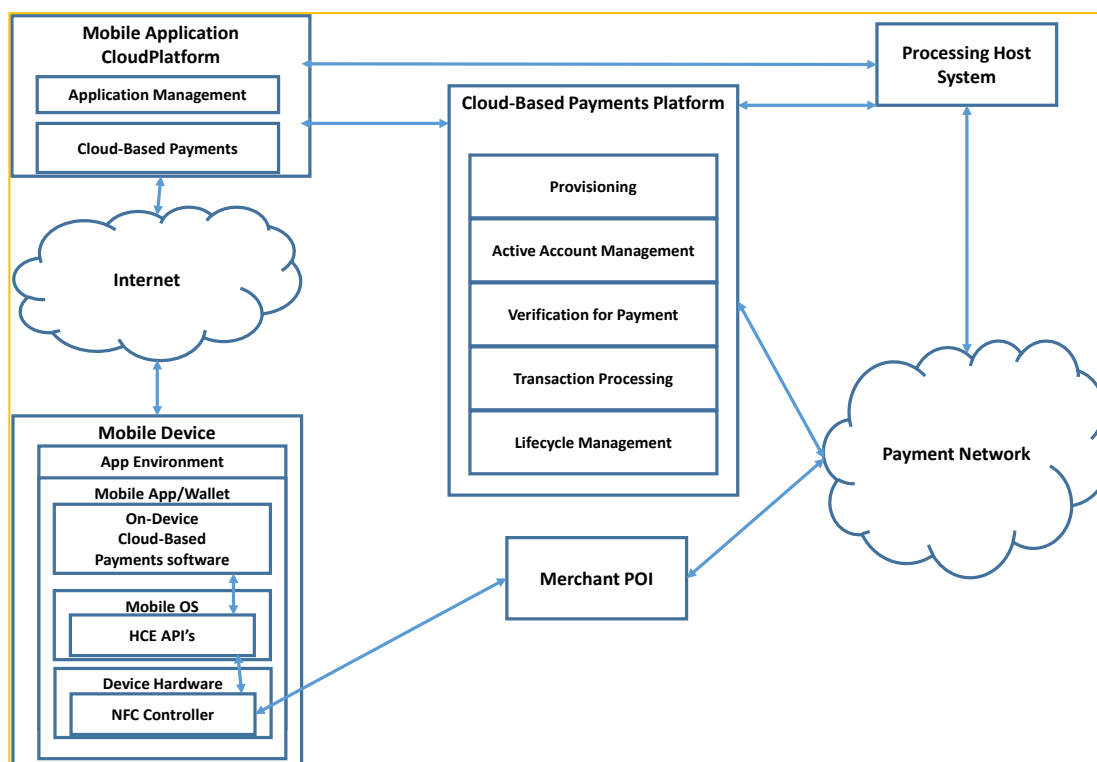- On-device cloud-based payments software

Figure 28: Cloud-based MCP lifecycle management back-end system

7.10.2   MCP management systems

After account provisioning, the cloud-based payments program performs active account management.   Active account management processes can also be initiated by transaction processing or by the mobile application on the consumers device.

During the account provisioning process, the active account management capability generates the initial set of account parameters to deploy to the mobile device. The account parameters consist of account information generated during provisioning, as well as any dynamic data needed to ensure the account parameters have only limited use after delivery to the device.

During transaction processing, if the profile indicates that account parameters must be replaced, the active account management capability recognises this and connects to the mobile device to replenish account parameters. Alternatively, the on-device service profile parameters indicate that account parameters need replenishing, then the mobile application can request account parameter replenishment.

7.11 MCP authorisation systems

Authorisation messages for MCP transaction are similar to authorisation messages for transactions performed with a physical card. The only difference is the form factor which should be managed by the MCP Issuer.

This identification could be performed in different ways including but not limited to:

- Using a dedicated parameter in a Data Element, including an indication of specific consumer device features (such as non-card form factor, contactless only device with consumer input capability and communication capability outside the existing financial infrastructure).

- Through an Application Identifier (AID). In this case, a dedicated AID range should be reserved for MCP applications.

Verification for Payment

- A cloud-based payments program may have the capability to provide on-device verification to the payment network prior to or during payment. The program enables Cardholder Verification Methods as verification for payment for provisioned accounts. As part of the service profile, specific rules for what can be used as CVM are established and shared with the provisioning, active account management and transaction processing capabilities.

Transaction processing for cloud-based payments

- After an account is provisioned the transaction processing service must be aware that the account in a cloud-based payments account. This is initiated by the provisioning capability and managed by the account management capability.

- When a cloud-based account is identified by the transaction processing service, the transaction processing capability of the cloud-based program ensures that the service profile parameters are verified, applied and communicated to the issuer.

7.12 Security and certification

It is critical to ensure that security for MCPs is fully addressed to maintain and enhance the customers (both consumers and merchants) trust in these payments and to comply with the relevant regulations and security standards. For the security requirements of the different components in the MCP architecture, the reader is referred to Book 4 (also including the PCI requirements for the POI) of [4].

For general information concerning evaluation, the reader is referred to Book 5 of [4]. The PPSE on the mobile device is certified by EMVCo under the level 2 testing. Additional guidance is also provided in the EMVCo security evaluation process (see [17]), in particular related to the platform security evaluation process. Further information on testing and evaluation may also be found on www.emvco.com.

The certification of the MCP applets is executed by the individual Card schemes.

It should further be noted that EMVCo, through a collaboration with FIDO, aims to develop a set of CDCVM related approval programs.

An issuer who intends to bring an MCP solution into the market, should ensure that it has been tested to be interoperable with a representative set of POIs, possibly restricted to the geographical region in which the issuer aims to deploy its services. On the other hand, POI manufacturers might want to verify independently that new MCP services are indeed interoperable with their POIs.

The document on the "MCP Service Management Roles - Requirements and Specifications" (see [21]) provides further guidance on the security requirements for the different MCP application life cycle management roles involved in the process specified earlier in the present document. It provides in section 6.3 security requirements in the MNO domain in case that the SE is a UICC. Obviously, similar security requirements will apply for any SE issuer in case of an eSE.

In such cases where the SE issuer (e.g. MNO) or MCP issuer decides to delegate some of the MCP service management roles to e.g., a TSM(s), the service level agreements with those parties should cover the appropriate security requirements. More guidance is given in section 8 in [21].

An overview of the security guidelines for MCP application management is provided below.

The roles of all involved parties, their processes and responsibility should be clearly defined and agreed by Service Level Agreements (SLAs).
A secure end-to-to end channel should be established between the MCP Issuer and the MCP application.
There shall be a mechanism that enables the MCP Issuer or TSM to suspend/block/terminate the MCP application in case of suspicious behaviour of the MCP application.
The processes to provision, to maintain and to use the MCP application shall be as far as possible consistent. In this way, consumers will more easily detect abnormalities.
MNOs and MCP issuers should inform each other if a mobile device has been stolen / lost.
The appropriate audits shall be conducted by all parties (e.g. MNOs, MCP issuers, TSMs) involved in the ecosystem related to the management processes of the MCP application.
Secure protocols shall be specified to ensure the authentication, integrity, and confidentiality in the processes related to the provisioning (including personalisation) and life cycle management of the MCP application.

Table 14: Security requirements for MCP application management

8   Conclusions

This document defines the implementation guidelines for MCP. It aims to reflect the current state of the art at the time of specification. However, it needs to be recognised that the MCP ecosystem is rapidly evolving with lots of new entrants in the market. Some of these solutions are proprietary today. Clearly, market adoption will determine the success of each of these new entrants.

The present guidelines focus on interoperability between the different stakeholders involved in the MCP ecosystem in the co-operative space. More in particular, it addresses the interoperability aspects related to the MCP application life cycle management. Furthermore, using a similar approach as in [4], it addresses the technical interoperability of an MCP transaction, hereby including a number of options, which are at the discretion of the MCP issuers and acquirers.

This document further builds on the concepts introduced in the EPC White paper on Mobile Payments [22] and on the joint EPC-GSMA work on the MCP Service Management Roles - Requirements and Specifications [21]. The document also aims to be aligned with the version 8.0 of the SEPA Cards Standardisation Volume [4], published by the ECSG.

Next to defining the different models and processes related to the MCP life cycle management it addresses, in detail, MCP transaction aspects such as CVM, risk management and transaction flows. Different MCP transactions are illustrated through an extensive set of use cases. As market demands are growing, more and more mobile devices supporting different MCP models will become available. From the analysis made in the document it is clear that the choice of the MCP model has a major impact on the MCP ecosystem and the different stakeholders involved.

The document further provides, as support to MCP implementations, an architectural overview and a description of the technical infrastructure needed. It also leverages, to a large extend, the work done by other standard and industry bodies and provides the appropriate references to the various documents produced by those.

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

While producing this document, the multi-stakeholder group still noticed a number of remaining gaps and challenges that are existing today and if properly addressed could even further encourage the market take up of MCPs. Those include:

- Various standardisation and industry bodies have been involved in defining the appropriate specifications for mobile contactless applications but further standardisation is needed for HCE-based solutions to support the cloud-based models as well as for security requirements for new POI terminals such as PDAs, mobile phones, etc.

- One of the main challenges for MCP issuers remains the support of the different mobile platforms. Mobile devices have different operating systems with different execution environments which directly impacts the "secure" communication between different components in the device. Therefore the development of specifications of a framework, referenced as a "Smart Secure Platform" (enabling the provision of value-added services relying on authentication of the user, regardless of the mobile device, communication channel and underlying technology) taking into account the requirements for mobile payments, hereby leveraging work already done by EMVCo and Global Platform, as requested to ETSI in [25] is of utmost importance.

- The adoption of contactless payments by certain sectors (e.g., mass transit) has proven to be an important catalyst and is even critical for their general take-up in various countries. The take-up of contactless payments in some sectors such as public administrations and the transport sector as recommended in [25] has been lacking behind in some countries;

- The dependency of the consumer on the type of mobile device with respect to the choice of MCP services. Therefore, access to the mobile device contactless interface in order to ensure that the consumer can have a choice amongst payment applications from different mobile payment providers, independently of the mobile device and the operating system used, should be ensured by all handset manufacturers and mobile OS developers (see also [25]).

- The impact of the new PSD2 [2] with the RTS on strong customer authentication (see [6] in Annex A: Overview regulatory documents) and the IF Regulation (see [3] in Annex A: Overview regulatory documents) related to MCPs on the customer experience.

Although some of the issues mentioned above have already been identified in the ERPB report in 2015 [25], the multi-stakeholder group recognises that further work is needed as follow-up on the recommendations made in the report.

By developing these implementation guidelines, the multi-stakeholder group aimed to contribute to a competitive MCP market, by providing the different stakeholders an insight into the different service, technical and security aspects involved. The document should serve as a reference basis for making certain implementation choices.

In light of major new trends, and the rapidly changing market, it is recommended for the present document to be regularly updated. Therefore, the multi-stakeholder group aims to maintain the document to reflect the state of the art in light of major new trends and developments related to MCPs and to keep it aligned with the various documents referenced.

9 Annex A: Overview regulatory documents

[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 payments services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC	http://ec.europa.eu/finance/payments/framework/index_en.htm
[5]	General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection 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	http://ec.europa.eu/justice/data-protection/
[6]	EBA/RTS/2017/02 Final Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under	www.eba.europa.eu

		Article 98 of Directive 2015/2366 (PSD2) amended by EBA, June 2017[30]	
[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]		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 15: Overview regulatory documents

---

[30] This reference will be updated as soon as the final document has been published.

10 Annex B: Overview life cycle management processes for MCP models

The process flow specified in section 5.2.2 is used as a skeleton for the MCP life cycle overview in the remainder of this Annex.

10.1 Processes overview of the MCP life cycle for scenario 1

In this scenario, the SE is the removable UICC which is supplied by the MNO (the SE issuer), while the MCP issuer is responsible for the issuance and life cycle management of the MCP application.

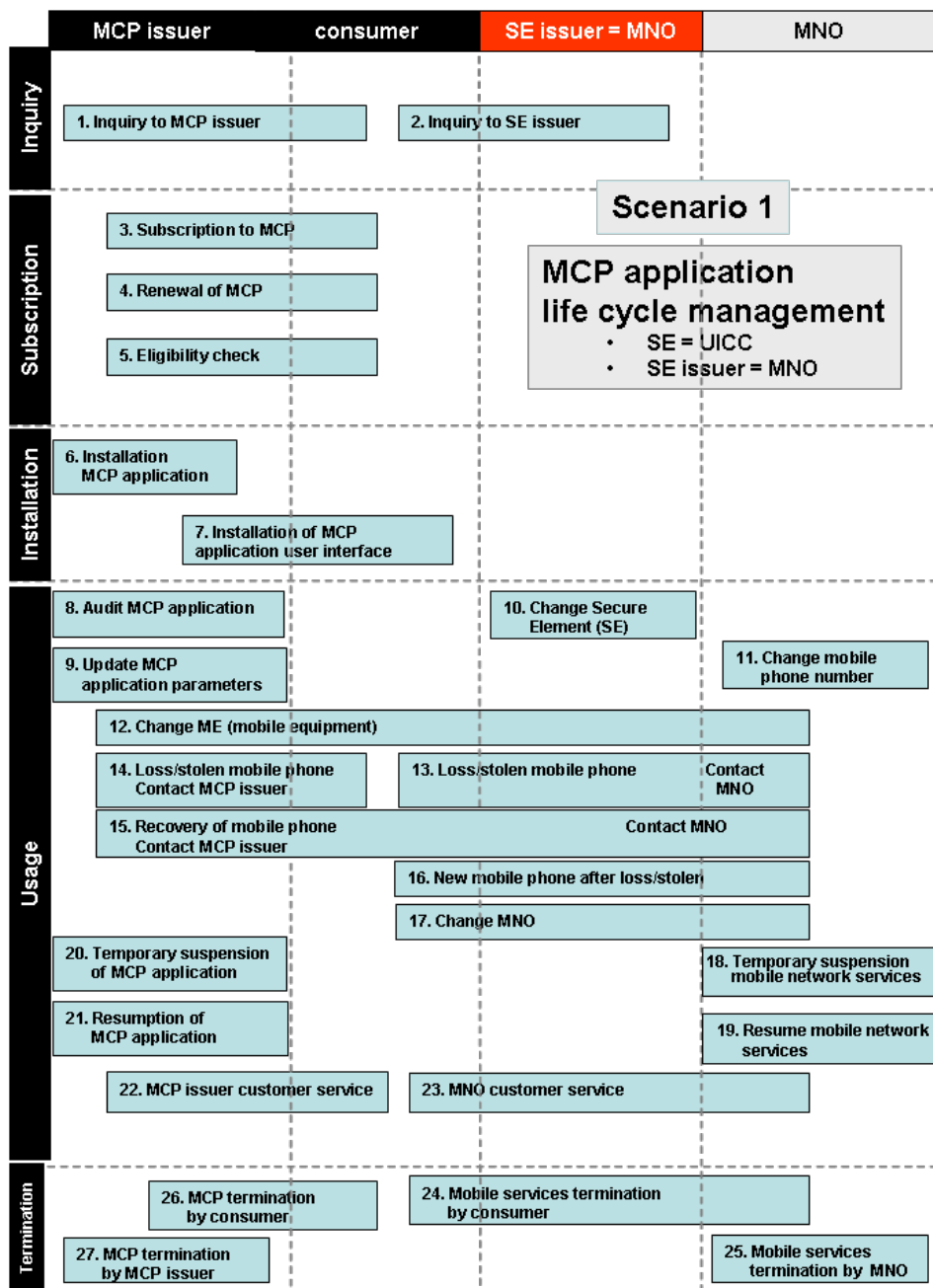The figure below provides an overview of the processes which are subsequently specified below.

Figure 29: MCP life cycle overview for scenario 1

In the following, the MCP life cycle steps and processes are generically described. Process numbering does not necessarily denote sequential order. An example for the actual order of processes is in Annex C: Examples of MCP life cycle use cases

Step 1: Consumer Inquiry

The consumer discovers the MCP services, typical examples are:

- **Process 1**: The consumer requests information regarding MCP services/applications from the MCP issuer.
- **Process 2**: The consumer requests information regarding MCP services/applications from the SE issuer (MNO). The MNO refers the consumer to the MCP issuer.

Step 2: Subscription to MCP application

- **Process 3**: The consumer subscribes to an MCP application with the MCP issuer.

    o Use case 1 – The consumer subscribes to a first MCP application from a given MCP issuer for a given SE.

    o Use case 2 – The consumer subscribes to the addition of a new MCP application to the SE from the same MCP issuer.

- **Process 4**: The consumer replaces/renews the current MCP application with a new one on the same SE. The MCP issuer proposes to renew the consumer's existing application or proposes a new one.

- **Process 5**: The MCP issuer checks the eligibility of the consumer with the MNO (both as the provider of mobile network services and as SE issuer) and takes appropriate action as necessary with respect to the consumer.

As a result of step 2, it is assumed that the consumer is equipped with the appropriate MCP compatible mobile phone (i.e. mobile equipment + SE).

Step 3: Installation of the MCP application

- **Process 6**: The MCP issuer is responsible for the installation of the MCP application on the SE in the consumer's mobile phone.

- **Process 7**: The MCP issuer (or a third party) installs the MCP application User Interface. This might involve the consumer.

Step 4: Usage of the MCP application

- **Process 8**: The MCP issuer checks the status of the MCP application on the SE.

- **Process 9**: The MCP issuer updates the MCP application (parameters).

- **Process 10**: The consumer changes the SE.

- **Process 11**: The mobile phone number of the consumer changes but he/she keeps the same SE and MNO. The consumer has an operational mobile-NFC service deployed and activated (or locked). This change results in a change of the consumer identifier and potentially in the way to reach the mobile phone via OTA channel. The MNO notifies the MCP issuer that the mobile phone number of the consumer has changed. The MCP issuer needs to update its information system with this change. The mobile equipment and the SE are accessible through the new mobile phone number.

- **Process 12**: The consumer changes his/her mobile equipment.

  - o Use case 1: The new mobile equipment is unable to work with the SE. The consumer contacts the MNO's customer service.

  - o Use case 2: The new mobile equipment works with the SE. The MNO, once informed about the new mobile equipment (via any technical means), informs the MCP issuer accordingly.

    - ▪ Use case 2a: The new mobile equipment detects the MCP application on the SE and triggers the download of the MCP application User Interface by the MCP issuer or a third party.
    - ▪ Use case 2b: The new mobile equipment is unable to identify the MCP application and therefore cannot download the MCP application User Interface. The consumer contacts the MCP issuer's customer service.

- **Process 13**: The consumer's mobile phone is lost or stolen. The consumer contacts the MNO's customer service.

- **Process 14:** The consumer's mobile phone is lost or stolen. The consumer contacts the MCP issuer's customer service.

- **Process 15**: Following the loss (or theft) of the mobile phone, the consumer recovers the mobile phone and contacts the MNO or the MCP issuer as appropriate.

- **Process 16**: Following the loss (or theft) of the mobile phone, the consumer obtains a new mobile equipment and a new SE.

- **Process 17**: The consumer changes MNO (typically retaining the number) and wishes to extend the MCP application to the new MNO. He/she contacts his/her MCP issuer to re-provision the MCP application on the new UICC , and contacts the MCP issuer (or third party) to download the MCP application User Interface. The MNO registers the new consumer and his/her mobile phone in its information system to offer mobile network services.

- **Process 18**: The MNO temporarily suspends mobile network services.

- **Process 19**: Following the suspension, the MNO resumes mobile network services.

- **Process 20**: The MCP issuer temporarily suspends the MCP service.

- **Process 21**: Following the suspension of the MCP application, the MCP issuer resumes the MCP application.

- **Process 22**: The consumer contacts the MCP issuer's customer service (related to the MCP application).

- **Process 23**: The consumer contacts the MNO's customer service (related to the SE or mobile network services).

Step 5: Termination of the MCP application

Termination of the MCP service can be performed according to one of the following processes:

- **Process 24**: The consumer terminates the mobile network services with the MNO.

- **Process 25**: The MNO terminates the consumer's mobile network services.

- **Process 26**: The consumer requests the termination of the MCP application.

- **Process 27**: The MCP issuer terminates the MCP application.

Note: for processes corresponding to suspension, resumption and termination, the MCP service must be terminated prior to the suspension of the MNO subscription to avoid OTA problems.

Note: A similar process overview is valid for scenario 3, except for the following processes:

Process 12: The consumer changes their mobile equipment which is outfitted with an non removable eUICC. This implies the change of the SE and therefore also the MCP. The consumer contacts the MCP issuer's customer service. The change of the SE will trigger both a re-provisioning and a re-personalisation of

the MCP application. The process shall involve ensuring that the corresponding MCP application user interface is also available or is loaded.

Process 16: Following the loss (or theft) of the mobile phone, the consumer obtains a new mobile equipment with an eUICC that holds an SE. This leads to both a re-provisioning and a re-personalisation of the MCP application (see process 10).

However, a split is to be made for the MNO between its roles as the controlling entity for the SE (issuer and controlling eUICC) and as MNO.

10.2 Processes overview of the MCP life cycle for scenario 2a

In this scenario, the SE is an eSE in a mobile equipment which is supplied by the mobile equipment manufacturer while the MCP issuer is responsible for the issuance and life cycle management of the MCP application.

The figure below provides an overview of all the processes in this scenario.
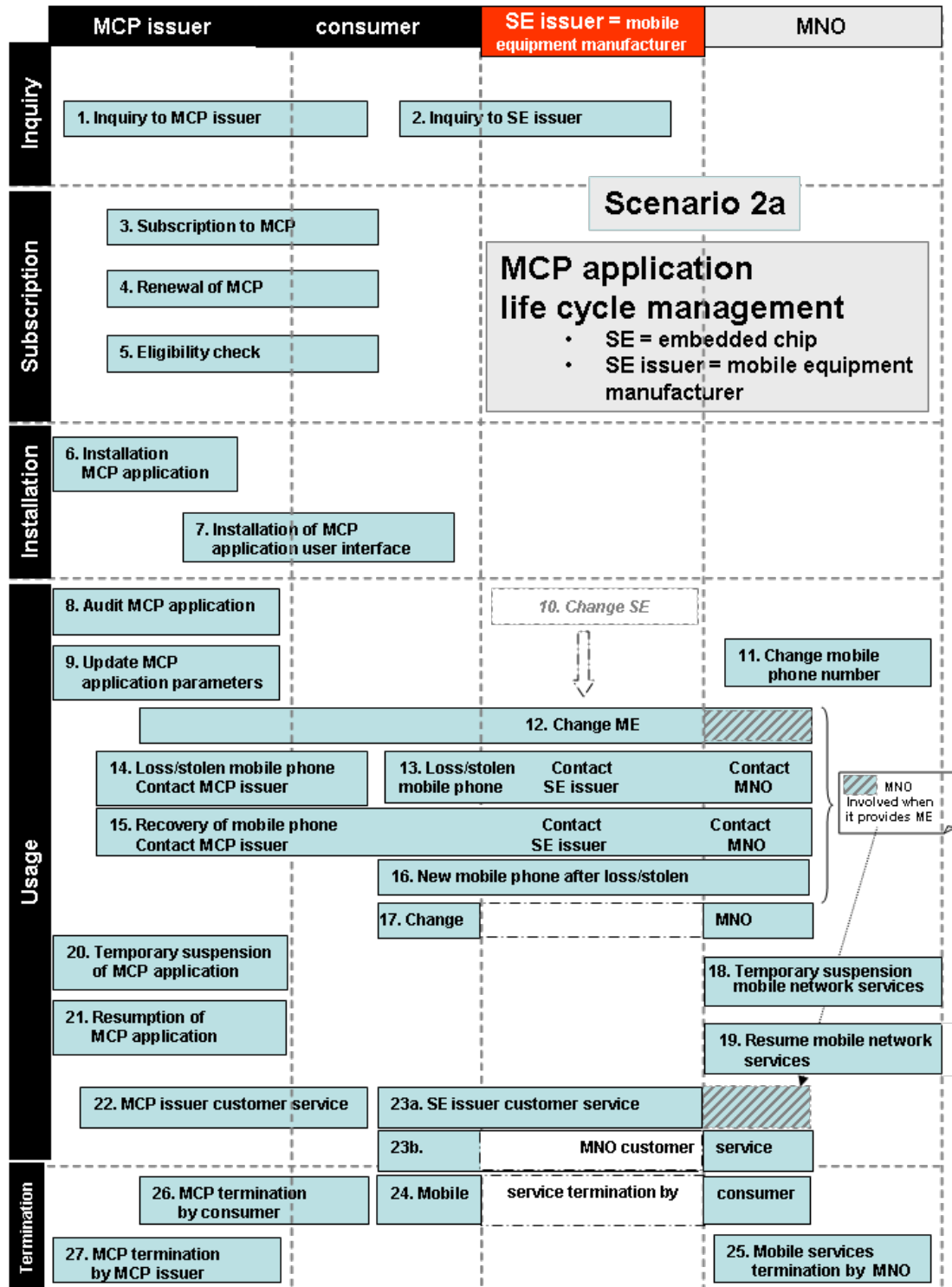

Figure 30: MCP life cycle overview for scenario 2a

Step 1: Consumer Inquiry

The consumer discovers the MCP services, typical examples are:

- **Process 1**: The consumer requests information regarding MCP services/applications from the MCP issuer.

- **Process 2**: The consumer requests information regarding MCP services/applications from the SE issuer (mobile equipment manufacturer). The mobile equipment manufacturer refers the consumer to the MCP issuer.

Step 2: Subscription to MCP application

- **Process 3**: The consumer subscribes to an MCP application with the MCP issuer.

  o Use case 1 – The consumer subscribes to a first MCP application from a given MCP issuer for a given SE.

  o Use case 2 – The consumer subscribes to the addition of a new MCP application to the SE from the same MCP issuer.

- **Process 4**: The consumer replaces/renews the current MCP application with a new one on the same SE. The MCP issuer proposes to renew the consumer's existing application or proposes a new one.

- **Process 5**: The MCP issuer checks the eligibility of the consumer with the MNO as the provider of mobile network services) and with the SE issuer, and takes appropriate action as necessary with respect to the consumer.

As a result of step 2 it is assumed that the consumer is equipped with the appropriate MCP compatible mobile phone (i.e. mobile equipment + SE).

Step 3: Installation of the MCP application

- **Process 6**: The MCP issuer is responsible for the installation of the MCP application on the SE in the consumer's mobile phone.

- **Process 7**: The MCP issuer (or a third party) installs the MCP application User Interface. This might involve the consumer.

Step 4: Usage of the MCP application

- **Process 8**: The MCP issuer checks the status of the MCP application on the SE.

- **Process 9**: The MCP issuer updates the MCP application (parameters).

- **Process 10**: This process is not applicable since the change of the SE is linked to the change of the mobile equipment (see process 12).

- **Process 11**: The mobile phone number of the consumer changes but he/she keeps the same SE and MNO. The consumer has an operational mobile-NFC service deployed and activated (or locked). This change results in a change of the consumer identifier and potentially in the way to reach the mobile phone via OTA channel. The MNO notifies the MCP issuer that the mobile phone number of the consumer has changed. The MCP issuer needs to update its information system with this change. The mobile equipment and the SE are accessible through the new mobile phone number.

- **Process 12**: The consumer changes his/her mobile equipment which implies the change of the SE. The consumer contacts the MCP issuer's customer service. The change of SE will trigger both a re-provisioning and a re-personalisation of the MCP application. The process shall involve ensuring that the corresponding MCP application user interface is also available or is loaded.

- **Process 13**: The consumer's mobile phone is lost or stolen. The consumer contacts the MNO's or the SE issuer's customer service as appropriate.

- **Process 14**: The consumer's mobile phone is lost or stolen. The consumer contacts the MCP issuer's customer service.

- **Process 15**: Following the loss (or theft) of the mobile phone, the consumer recovers the mobile phone and contacts the MNO, the SE issuer or the MCP issuer as appropriate.

- **Process 16**: Following the loss (or theft) of the mobile phone, the consumer obtains a new mobile equipment and a new SE.

- **Process 17**: The consumer changes MNO (typically retaining the number) and wishes to extend the MCP application to the new MNO.

    o   Use case 1: If the consumer keeps his/her mobile phone, he/she also keeps his/her SE with the MCP application and its User Interface on the mobile phone. The MNO registers the new consumer and his/her mobile phone in its information system to offer mobile network services.

    o   Use case 2: If the consumer obtains a new mobile phone (typically retaining the number), he/she contacts his/her MCP issuer to re-provision the MCP application on the new SE, and contacts the MCP issuer (or third party) to download the MCP application User Interface. The MNO registers the new consumer and his/her mobile phone in its information system to offer mobile network services.

- **Process 18**: The MNO temporarily suspends the mobile network services.

- **Process 19**: Following the suspension, the MNO resumes the mobile network services.

- **Process 20**: The MCP issuer temporarily suspends the MCP service.

- **Process 21**: Following the suspension of the MCP application, the MCP issuer resumes the MCP application.

- **Process 22**: The consumer contacts the MCP issuer's customer service (related to the MCP application).

- **Process 23a**: The consumer contacts the customer service related to the SE issuer. (Depending on the business model, this might be the mobile equipment supplier (e.g. MNO or other third party)).

- **Process 23b**: The consumer contacts the MNO's customer service (related to mobile network services).

Step 5: Termination of the MCP application

Termination of the MCP service can be performed according to one of the following processes:

- **Process 24**: The consumer terminates the mobile network services with the MNO.

- **Process 25**: The MNO terminates the consumer's mobile network services.

- **Process 26**: The consumer requests the termination of the MCP application.

- **Process 27**: The MCP issuer terminates the MCP application.

Note: for processes corresponding to suspension, resumption and termination, the MCP service must be terminated prior to the suspension of the MNO subscription to avoid OTA problems.

10.3 Processes overview of the MCP life cycle for scenario 2b

In this scenario, the SE is an eSE in the mobile equipment, supplied by a third party (e.g. TSM or other) while the MCP issuer is responsible for both issuance and life cycle management of the MCP application.

The figure below provides an overview of all the processes for this scenario.
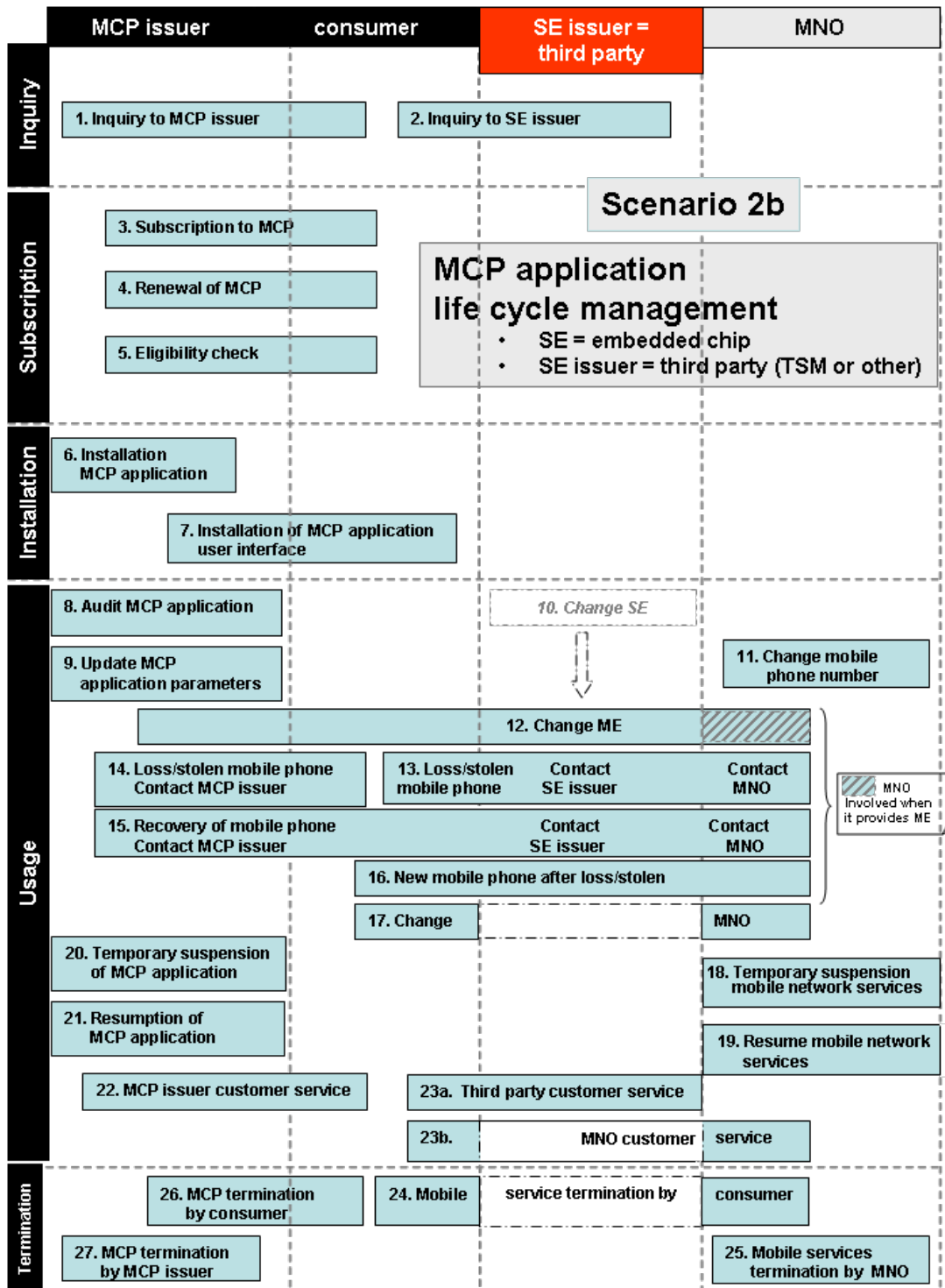

Figure 31: MCP life cycle overview for scenario 2b

Step 1: Consumer Inquiry

The consumer discovers the MCP services, typical examples are:

- **Process 1**: The consumer requests information regarding MCP services/applications from the MCP issuer.

- **Process 2**: The consumer requests information regarding MCP services/applications from the SE issuer (third party). The third party refers the consumer to the MCP issuer.

Step 2: Subscription to MCP application

- **Process 3**: The consumer subscribes to an MCP application with the MCP issuer.

    o Use case 1 – The consumer subscribes to a first MCP application from a given MCP issuer for a given SE.

    o Use case 2 – The consumer subscribes to the addition of a new MCP application to the SE from the same MCP issuer.

- **Process 4**: The consumer replaces/renews the current MCP application with a new one on the same SE. The MCP issuer proposes to renew the consumer's existing application or proposes a new one.

- **Process 5**: The MCP issuer checks the eligibility of the consumer with the MNO as the provider of mobile network services) and with the SE issuer, and takes appropriate action as necessary with respect to the consumer.

As a result of step 2 it is assumed that the consumer is equipped with the appropriate MCP compatible mobile phone (mobile equipment + SE).

Step 3: Installation of the MCP application

- **Process 6**: The MCP issuer is responsible for the installation of the MCP application on the SE in the consumer's mobile phone.

- **Process 7**: The MCP issuer (or a third party) installs the MCP application User Interface. This might involve the consumer.

Step 4: Usage of the MCP application

- **Process 8**: The MCP issuer checks the status of the MCP application on the SE.

- **Process 9**: The MCP issuer updates the MCP application (parameters).

- **Process 10**: This process is not applicable since the change of the SE is linked to the change of the mobile equipment (see process 12).

- **Process 11**: The mobile phone number of the consumer changes but he/she keeps the same SE and MNO. The consumer has an operational mobile-NFC service deployed and activated (or locked). This change results in a change of the consumer identifier and potentially in the way to reach the mobile phone via OTA channel. The MNO notifies the MCP issuer that the mobile phone number of the consumer has changed. The MCP issuer needs to update its information system with this change. The mobile equipment and the SE are accessible through the new mobile phone number.

- **Process 12**: The consumer changes his/her mobile equipment which implies the change of the SE. The consumer contacts the MCP issuer's customer service. The change of SE will trigger both a re-provisioning and a re-personalisation of the MCP application. The process shall involve ensuring that the corresponding MCP application user interface is also available or is loaded.

- **Process 13**: The consumer's mobile phone is lost or stolen. The consumer contacts the MNO's or the SE issuer's customer service as appropriate.

- **Process 14**: The consumer's mobile phone is lost or stolen. The consumer contacts the MCP issuer's customer service.

- **Process 15**: Following the loss (or theft) of the mobile phone, the consumer recovers the mobile phone and contacts the MNO, the SE issuer or the MCP issuer as appropriate.

- **Process 16**: Following the loss (or theft) of the mobile phone, the consumer obtains a new mobile equipment and a new SE.

- **Process 17**: The consumer changes MNO (typically retaining the number) and wishes to extend the MCP application to the new MNO.

    o Use case 1: If the consumer keeps his/her mobile phone, he/she also keeps his/her SE with the MCP application and its User Interface on the mobile phone. The MNO registers the new consumer and his/her mobile phone in its information system to offer mobile network services.

    o Use case 2: If the consumer obtains a new mobile phone (typically retaining the number), he/she contacts his/her MCP issuer to re-provision the MCP application on the new SE, and contacts the MCP issuer (or third party) to download the MCP application User Interface. The MNO registers the new consumer and his/her mobile phone in its information system to offer mobile network services.

- **Process 18**: The MNO temporarily suspends the mobile network services.

- **Process 19**: Following the suspension, the MNO resumes the mobile network services.

- **Process 20**: The MCP issuer temporarily suspends the MCP service.

- **Process 21**: Following the suspension of the MCP application, the MCP issuer resumes the MCP application.

- **Process 22**: The consumer contacts the MCP issuer's customer service (related to the MCP application).

- **Process 23a**: The consumer contacts the third party's customer service (related to the SE).

- **Process 23b**: The consumer contacts the MNO's customer service (related to mobile network services).

Step 5: Termination of the MCP application

Termination of the MCP service can be performed according to one of the following processes:

- **Process 24**: The consumer terminates the mobile network services with the MNO.

- **Process 25**: The MNO terminates the consumer's mobile network services.

- **Process 26**: The consumer requests the termination of the MCP application.

- **Process 27**: The MCP issuer terminates the MCP application.

Note: for processes corresponding to suspension, resumption and termination, the MCP service must be terminated prior to the suspension of the MNO subscription to avoid OTA problems.

11 Annex C: Examples of MCP life cycle use cases

The first example is a scenario where a consumer requests the MCP issuer to subscribe an MCP service for the first time[31]. The scenario starts at process 1.
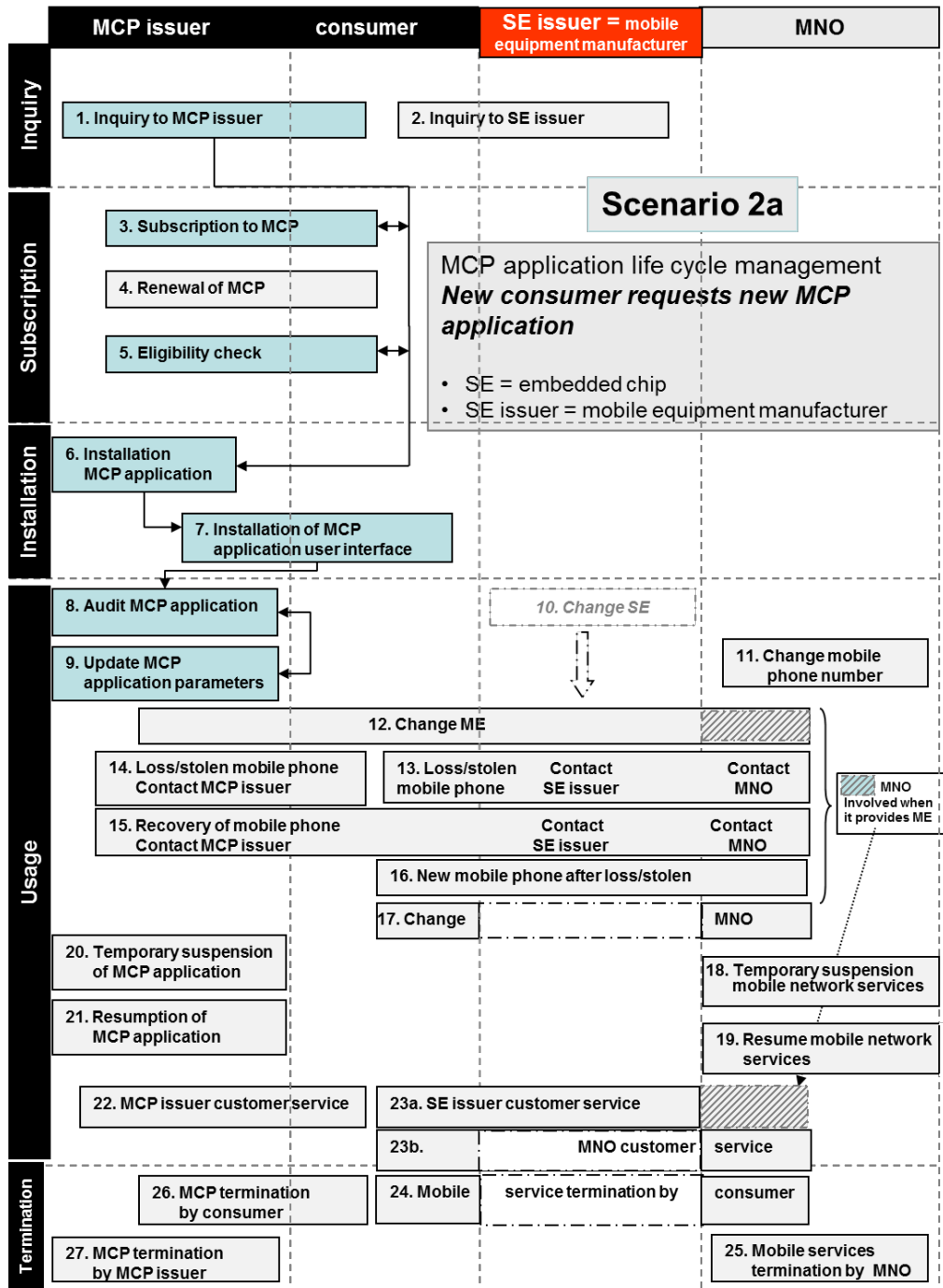

Figure 32: A new consumer requests a new MCP application

---

[31] Note that the actual sequence of process may change in the final implementation according to the concrete business models put in place.

In the next scenario, the consumer's mobile phone is stolen and subsequently replaced[32]. In this particular case, the scenario starts at process 13. Process 22 and 23a and 23b have no explicit flow arrows as they may be invoked by the consumer at any point during the scenario.
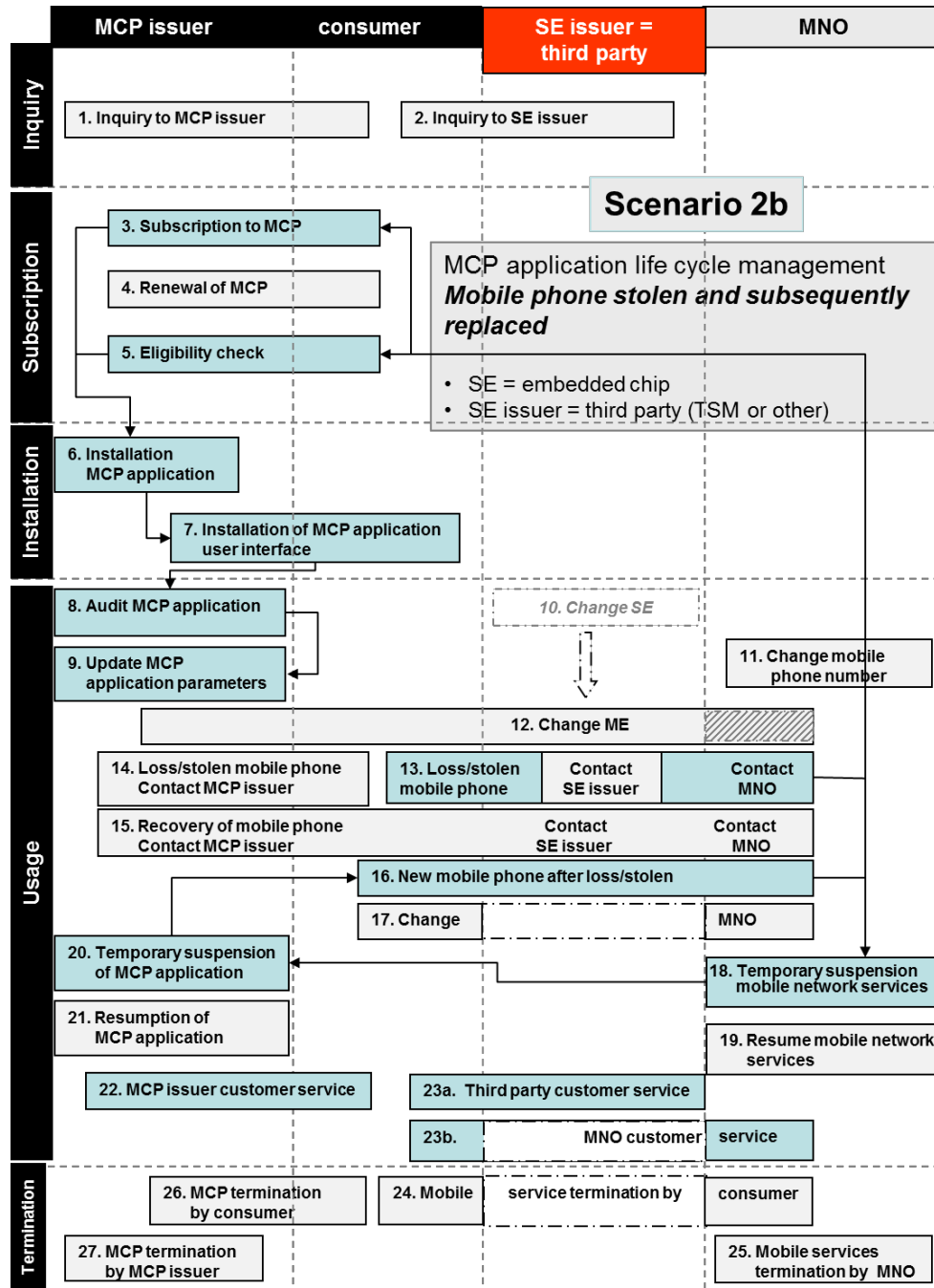

Figure 33: Consumer's mobile phone is stolen and subsequently replaced

_____

[32] Note that the actual sequence of process may change in the final implementation according to the concrete business models put in place.

12 Annex D: An example of construction of the PPSE

The figure below illustrates the response from the PPSE to the POI depending on the selection made by the consumer on the mobile device, in case both an international card scheme (ICS) and domestic card scheme (DCS) are present on the mobile device.
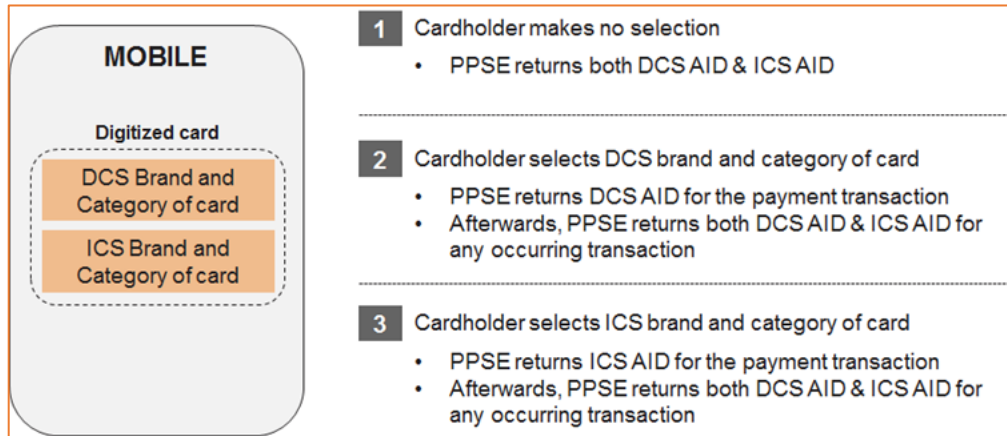

Figure 34: Selection of the application on the mobile device and PPSE

13 Annex E: 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 16: The multi-stakeholder group

The multi-stakeholder group wishes to thank GlobalPlatform for their contribution to section 7.6.2.

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