



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	EPC178-10
Issue	Version 1.0
Date of Issue	April 28 th 2011
Reason for Issue	Consultation
Produced by	EPC Secretariat
Circulation	Final draft version for consultation

Executive Summary

The role of the EPC is to ensure the evolution of an integrated market for payments in Europe through the development and promotion of standards, best practices and schemes. Mobile phones have achieved full market penetration and rich service levels in most, if not all, Member States, making the mobile channel ideal for leveraging and promoting the use of SEPA payment instruments.

The EPC, working together with other stakeholders, is in the process of establishing the necessary standards and business rules to leverage the full potential of the mobile channel for the initiation and receipt of SEPA payments in an interoperable environment. Currently, several individual pilots already exist across SEPA. However, a broad implementation of cross border interoperable mobile payment solutions is needed to avoid market fragmentation which would hinder the emergence of open, non-proprietary technology standards for user-friendly mobile payment services.

In July 2010, the EPC published the first edition of a white paper [\[EPC6\]](#) which offers an informative read to any party interested in mobile payments and aims to foster a common understanding between payment service providers and other stakeholders, including customers, by using non-technical language. The document predominantly focuses on Mobile Contactless (card) Payments (MCPs), where the mobile device needs to be in close proximity to a point-of-sale terminal, while also addressing some aspects of mobile remote payments, where two parties are able to send and receive funds irrespective of where they are located.

Furthermore, EPC and GSMA jointly developed a document [\[EPC3\]](#) which defines the requirements and specifications for the roles and responsibilities of MCP issuers and Mobile Network Operators (MNOs) involved in the provisioning and life cycle management of an MCP application residing on the UICC ¹.

The EPC has further built on these documents to specify the present Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines. It is also hereby leveraging the work done by other standard and industry bodies in this area. The present document covers three types of Secure Elements (SEs) in the mobile phone to store the MCP application, namely the UICC, the embedded Secure Element and the micro Secure Digital (SD) card. This is the result of a thorough analysis of different SE alternatives to ensure an adequate level of security and appropriate governance by payment service providers.

The document further endeavours to:

- Enable the quick development and implementation of mobile solutions.
- Avoid the development of proprietary solutions with limited (geographical) reach, leading to fragmentation market.
- Provide transparency to market participants for the Mobile Contactless SEPA Card payments by describing the roles of the large number of stakeholders involved.

¹ UICC refers to the Universal Integrated Circuit Card

- Clarify the position of the EPC to ensure the interests with regard to standardisation and industry bodies.
- Define the minimum level of security for the whole mobile payment value chain in order to establish confidence in this environment.

The document is structured as follows:

In the first section, the EPC provides its vision on MCPs related to SEPA payment instruments, as well as the scope and the objectives of this document.

This is followed by the definition of high-level business principles in section 2.

Section 3 provides a short description of MCPs while introducing the different participants in the ecosystem. Furthermore, it gives a high level overview of the different phases involved in an MCP.

In sections 4 and 5, the different service models and processes involved in the provisioning and the life cycle management of the MCP application residing on one of the SE types mentioned above, are described in detail. Each model is analysed, along with its advantages and main challenges.

Section 6 is devoted to different aspects of the MCP application. Firstly, a high level overview of the transaction flows involved in MCPs is provided, including on-line and off-line transactions with the optional execution of an appropriate Cardholder Verification Method (CVM). Next, the MCP application risk management is described, with examples of use cases to be found in Annex 9.1.

The next section provides an overview on the overall MCP architecture, as well as a mapping of standards and specifications defined by other standard and industry bodies in the mobile ecosystem. Furthermore, it specifies the technical infrastructure needed, as well as the security requirements, for the different components in the MCP architecture.

Overall conclusions on MCPs may be found in the final section 8.

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

In producing these implementation guidelines, EPC aims to support potential MCP issuers by providing an insight into the different service, technical and security aspects involved. The document should serve as a reference basis for making certain implementation choices.

Table of Contents

Executive Summary	2
0 Document Information	9
0.1 References	9
0.2 Definitions	12
0.3 Abbreviations	14
0.4 Stakeholder Consultation and Validation Process.....	15
1 General	16
1.1 Introduction	16
1.2 Vision	16
1.3 Scope and Objectives	16
1.4 Audience.....	17
2 High-level business principles for MCP	19
3 Mobile Contactless SEPA Card Payments Overview.....	20
3.1 Introduction	20
3.2 Provisioning and life cycle management.....	21
3.3 MCP Transaction.....	22
3.4 Basic MCP principles	23
3.5 The MCP ecosystem.....	24
4 Service Models.....	26
4.1 Scenario 1: the MNO provides the UICC	27
4.1.1 Introduction.....	27
4.1.2 Analysis.....	27
4.2 Scenario 2a: the mobile handset manufacturer provides the embedded chip.....	28
4.2.1 Introduction	28
4.2.2 Analysis.....	29
4.3 Scenario 2b: a third party provides the embedded chip	30
4.3.1 Introduction.....	30
4.3.2 Analysis.....	30
4.4 Scenario 3a: a third party provides the micro SD	31
4.4.1 Introduction.....	31
4.4.2 Analysis.....	32
4.5 Scenario 3b: the issuing bank provides the micro SD.....	33
4.5.1 Introduction.....	33
4.5.2 Analysis.....	34
4.6 Conclusions	34
5 Process-level guidelines	36
5.1 Processes overview of the MCP life cycle for scenario 1	36
5.2 Processes overview of the MCP life cycle for scenario 2a	40
5.3 Processes overview of the MCP life cycle for scenario 2b	44
5.4 Processes overview of the MCP life cycle for scenario 3a	48
5.5 Processes overview of the MCP life cycle for scenario 3b	53
6 Mobile Contactless Payment Application.....	59
6.1 Cardholder Verification Methods.....	59

6.1.1	Introduction.....	59
6.1.2	Single Tap: analysis of CVMs	60
6.1.3	Double Tap: Analysis of CVMs.....	63
6.2	MCP transaction	66
6.2.1	Single Tap - off-line transaction flow - no CVM (optionally off-line CVM).....	66
6.2.2	Single Tap - on-line transaction flow – no CVM.....	68
6.2.3	Double Tap - off-line transaction flow – off-line CVM	70
6.2.4	Double Tap - on-line transaction flow – off-line CVM	72
6.2.5	Single Tap - on-line transaction flow – on-line CVM	74
6.3	Risk management	75
6.3.1	Introduction.....	75
6.3.2	Form Factor.....	76
6.3.3	Parameters	76
6.3.4	Point Of Interaction Risk parameters.....	76
6.3.5	MCP risk parameters.....	77
6.3.6	Additional Remarks	80
6.4	Additional features	81
6.4.1	Transaction Logging	81
6.4.2	Receipts.....	82
6.5	Interoperability and MCP Service availability.....	82
7	Technical and Security Infrastructure	84
7.1	Overall MCP architecture.....	84
7.2	Mapping of standards and specifications	85
7.3	Mobile equipment.....	89
7.3.1	Introduction.....	89
7.3.2	Application Activation User Interface (AAUI)	90
7.4	Point of Interaction.....	91
7.4.1	Transaction initialisation.....	92
7.4.2	Technology selection	92
7.4.3	Application Selection.....	92
7.4.4	Card Authentication	92
7.4.5	Cardholder Verification	92
7.4.6	Authorisation.....	92
7.5	Secure Element.....	92
7.5.1	Introduction.....	93
7.5.2	Proximity Payment System Environment.....	93
7.5.3	Security Domains and GlobalPlatform Management Profiles.....	95
7.6	Back-end systems.....	97
7.6.1	Personalisation	98
7.6.2	Process to install the MCP application	99
7.6.3	MCP management systems	100
7.6.4	MCP authorisation systems.....	100
7.7	Security requirements and certification.....	101
7.7.1	SE and MCP application.....	101
7.7.2	MCP application life cycle management	107
7.7.3	Certification	108
7.8	Conclusions	108
8	Conclusions.....	110

9	Annexes.....	111
9.1	MCP Risk Management Use Cases.....	111
9.1.1	Introduction.....	111
9.1.2	Use Case Scenario 1: off-line transaction without CVM.....	111
9.1.3	Use Case Scenario 2: off-line transaction with off-line CVM.....	112
9.1.4	Use Case Scenario 3: On-line transaction without CVM	113
9.1.5	Use Case Scenario 4: on-line transaction with off-line CVM	114
9.1.6	Use Case Scenario 5: on-line transaction with on-line CVM.....	115
9.2	Example of AAUI implementation	115

DRAFT

List of tables

Table 1: References	11
Table 2: Terminology	13
Table 3: Abbreviations	14
Table 4: Secure Element types	26
Table 5: Transaction types and CVMs	59
Table 6: Overview matrix transaction types versus CVM usage.....	66
Table 7: CVM Usage.....	77
Table 8: CVM-based risk management	78
Table 9: On-line/ Off-line Risk management	80
Table 10: Example of management mode scenarios	97
Table 11: Security Requirements for Secure Elements and MCP applications.....	105
Table 12: Type of assurance augmentation	106
Table 13: Security requirements for Mobile equipment.....	107
Table 14: Security requirements for MCP application management.....	108
Table 15: Off-line transaction without CVM	111
Table 16: Off-line transaction with off-line CVM.....	112
Table 17: On-line transaction without CVM	113
Table 18: On-line transaction with off-line CVM.....	114
Table 19: On-line transaction with on-line CVM.....	115

DRAFT

List of figures

Figure 1: Mobile Contactless Card Payment Transaction	21
Figure 2: Provisioning/maintenance of MCP application on a Secure Element.....	22
Figure 3: MCP Transaction	23
Figure 4: Mobile Contactless SEPA Card Payments Business Ecosystem	25
Figure 5: The MCP application resides on the UICC provided by the MNO.....	27
Figure 6: The MCP application resides on the embedded chip provided by the mobile handset manufacturer	29
Figure 7: The MCP application resides on the embedded chip provided by the third party	30
Figure 8: The MCP application resides on the micro SD provided by a third party	32
Figure 9: The MCP application resides on the micro SD provided by the issuing bank.....	33
Figure 10: MCP life cycle overview for scenario 1	37
Figure 11: MCP life cycle overview for scenario 2a.....	41
Figure 12: MCP life cycle overview for scenario 2b.....	45
Figure 13: MCP life cycle overview for scenario 3a.....	49
Figure 14: MCP life cycle overview for scenario 3b.....	54
Figure 15: On-line transaction - no CVM.....	60
Figure 16: On-line transaction - on-line CVM.....	61
Figure 17: On-line transaction - off-line CVM.....	62
Figure 18: Off-line transaction - no CVM.....	62
Figure 19: Off-line transaction - off-line CVM.....	63
Figure 20: On-line transaction - off-line CVM.....	64
Figure 21: Off-line transaction - off-line CVM.....	65
Figure 22: Single Tap - off-line transaction flow - no CVM (optionally off-line CVM).....	66
Figure 23: Single Tap - on-line transaction flow – no CVM.....	68
Figure 24: Double Tap - off-line transaction flow – off-line CVM.....	70
Figure 25: Double Tap - on-line transaction flow – off-line CVM	72
Figure 26: Single Tap - on-line transaction flow – on-line CVM	74
Figure 27: The MCP System Architecture	84
Figure 28: Mapping of standards.....	89
Figure 29: Mobile equipment architecture	89
Figure 30: Location of the PPSE	94
Figure 31: Typical EMV smart card architecture	102
Figure 32: Example of an AAUI implementation	117

0 Document Information

0.1 References

This section lists external references mentioned in this document. Use of square brackets throughout this document is used to reference documents in this list.

N.º	Document Number	Title	Issued by:
[AEPM1]		Mobile Contactless Proximity Payment – Technical Specifications, v2.1	AEPM
[AFSCM1]	101203 AFSCM TECH _ LIVBL	Interface specification between Telecom Operators and NFC Service Providers release 1.2.1 – Dec.2010	AFSCM
[EC1]	Directive 2007/64/EC	Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market	EU Single Market
[EC2]	COM(2009) 324 final	White Paper – Modernising ICT Standardisation in the EU – The Way Forward	European Commission
[ECB1]	Single Euro Payments Area 2010	Seventh Progress Report – October 2010 section 3.3 Development of Mobile Payments	ECB
[EMV1]		EMV Mobile Contactless Payment Technical Issues and Position Paper, v1.0	EMVCo
[EMV2]		The Role and Scope of EMVCo in Standardising the Mobile Payments Infrastructure (White Paper), v1.0	EMVCo
[EMV3]		EMV Contactless Communication Protocol Specification, v2.0.1	EMVCo
[EMV4]		EMV Handset Requirements for Contactless Mobile Payment, v1.0	EMVCo
[EMV5]		EMV Contactless Mobile Payment Architecture Overview, v1.0	EMVCo
[EMV6]		EMV Contactless Mobile Payment – EMV Profiles of GlobalPlatform UICC Configuration, v1.0	EMVCo
[EMV7]		EMV Contactless Mobile Payment – Application Activation User Interface – Overview, Usage Guidelines and PPSE Requirements, v1.0	EMVCo
[EMV8]		Book A, EMV Contactless Specifications for Payment Systems, Architecture & General Remarks, v2.1	EMVCo
[EMV9]		Book B, EMV Contactless Specifications for Payment Systems, Entry Point Specification, v2.1	EMVCo
[EMV10]		Integrated Circuit Card Specifications for Payment Systems Book 3 Application Specification, v4.2	EMVCo

N.º	Document Number	Title	Issued by:
[EPC1]	EPC020-08	SEPA Cards Standardisation Volume	EPC
[EPC2]	EPC052-08	Customer-to-Bank Security Threat Assessment	EPC
[EPC3]	EPC220-08	Mobile Contactless Payments Service Management Roles – Requirements and Specifications	EPC-GSMA
[EPC4]	EPC342-08	Guidelines on Algorithms Usage and Key Management	EPC
[EPC5]	EPC397-08	Customer-to-Bank Security Good Practices Guide	EPC
[EPC6]	EPC492-09	White Paper Mobile payments	EPC
[EPC7]	EPC178-10	Mobile Contactless SEPA Card Payments Implementation Guidelines	EPC
[ETSI1]	ETSI TS 102 588	Technical Specification Smart Cards; Application invocation API by a UICC Web Server for Java Card Platform	ETSI
[ETSI2]	ETSI TS 102 622	Smart Cards; UICC – Contactless Front-end (CLF) interface; Host Controller Interface (HCI)	ETSI
[ETSI3]	ETSI TS 102 613	Smart Cards; UICC-CLF Interface; Physical and Data Link Layer Characteristics	ETSI
[GP1]	GPC_SPE_034	GlobalPlatform Card specification, v 2.2.1	GP
[GP2]		Confidential Card Content Management – Card Specification, v2.2–Amendment A, v1.0.1	GP
[GP3]		UICC Configuration, v1.0.1	GP
[GP4]		Messaging Specification for Mobile NFC Services, v1.0	GP
[GP5]		Card Specification, v2.2 Amendment C Defines a mechanism for an end user to activate a contactless services when the card support multiples contactless application	GP
[GP6]		Proposition for NFC Mobile: Secure Element Management and Messaging – White Paper (2009)	GP
[GP7]	GPC_SPE_031	GlobalPlatform Card – Composition Model, v0.0.106	GP
[GSMA1]	Pay-Buy-Mobile Initiative	Requirements for Single Wire Protocol NFC Handsets, v2.0 – Nov. 2008	GSMA
[GSMA2]		Mobile NFC Services White Paper -Feb 2007	GSMA
[GSMA3]		NFC Technical Guidelines V2 White Paper – Nov. 2007	GSMA
[GSMA4]	Pay-Buy-Mobile Initiative	Business Opportunity Analysis – Public White Paper – Nov. 2007	GSMA

N.º	Document Number	Title	Issued by:
[ISO1]	ISO/IEC 18092	Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)	ISO
[ISO2]	ISO/IEC 14443-3	Identification cards — Contactless integrated circuit(s) cards — Proximity cards 2001	ISO
[ISO3]	ISO/IEC 14443-4	Identification cards - Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol.	ISO
[ISO4]	ISO/IEC 7816-4	Identification cards — Integrated circuit cards Part 4: Organisation, security and commands for interchange	ISO
[MF1]		White Paper - Alternatives for Banks to offer Secure Mobile Payments, v1.0	Mobey Forum
[OMTP1]		Advanced Trusted Environment: OMTP TR1	OMTP
[OMTP2]		Security Threats on Embedded Consumer Devices	OMTP
[OMTP3]		Trusted Environment: TR0	OMTP
[OMTP4]		UICC recommendation	OMTP

Table 1: References

0.2 Definitions

Term	Definition
Acquirer	A payment service provider enabling the processing of a merchant's transaction with the MCP issuer through an authorisation and clearing network. In the context of this document it effectively means 'accepting mobile payments'.
Cardholder	A consumer who has an agreement with an MCP issuer for MCP Service. He/she needs to be an MNO subscriber which has an NFC-enabled mobile phone.
Card Scheme	A technical and commercial arrangement set up to serve one or more card brands and which provides the organisational, legal and operational framework rules necessary for the services marketed by the brand to function.
Consumer	In the context of the document, the consumer is a cardholder.
Customer	A customer can be either a consumer or a merchant.
Issuer (or Issuing bank)	A payment service provider providing the MCP application to the consumer (cardholder). In the context of this document, also referred to as MCP issuer.
MCP issuer	See Issuer.
Merchant	The acceptor within an MCP scheme for payment of the goods or services purchased by the consumer (cardholder in the context of the document). Also known as attendant in case of attended POIs. The merchant is a customer for its acquirer.
Mobile Contactless Payment (MCP)	A mobile phone initiated payment where the cardholder and the merchant (and/or his/her equipment) are in the same location and communicate directly with each other using contactless radio technologies, such as NFC (RFID), Bluetooth or Infrared for data transfer (also known as contactless payments). In the context of this document all Mobile Contactless Payments are Mobile Contactless SEPA Card Payments.
Mobile Contactless Payment (MCP) application	An application residing on a Secure Element performing the payment functions, as dictated by the MCP issuer, over NFC.
Mobile Contactless Payment (MCP) application User Interface	The mobile equipment application executing the user interactions related to the Mobile Contactless Payment application, as permitted by the MCP issuer.
Mobile equipment	Mobile phone without the Secure Elements such as the UICC (also referred to as mobile handset).

Mobile Network Operator (MNO)	A cell phone carrier offering a range of mobile services, potentially including facilitation of NFC services – such as MCPs. The MNO owns the UICC it provides to the customer and ensures connectivity Over the Air (OTA) between the customer and the issuing bank
Mobile phone	Mobile equipment with all Secure Elements, including the UICC (also referred to as Mobile Station).
Mobile wallet	A digital wallet which is a service allowing the wallet holder to securely access, manage and use identification and payment instruments in order to initiate payments residing on the mobile phone.
NFC	A contactless protocol specified by ISO/IEC 18092.
Payment Application Selection User Interface	The Mobile phone user interface (component) enabling the customer to <ul style="list-style-type: none"> • access the MCP application User Interface on the Mobile phone • select the preferred payment application.
Payment service provider	The bodies referred to in Article 1 of the Payment Service Directive [EC1] and legal and natural persons benefiting from the waiver under Article 26 of [EC1].
(Card) Payment Transaction	An act, initiated by the cardholder or by the merchant, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the cardholder and the merchant.
POI device	Point of Interaction device
Secure Element	A tamper-resistant platform (device or component) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. Examples include UICC, embedded Secure Elements, chip cards and SD cards.
Secure Element issuer	A trusted third party responsible for the supply and maintenance of a Secure Element. Typical examples are MNOs, third parties including TSMs or mobile handset manufacturers.
Security Domain	On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the issuing bank, the MNO or a third party).
Third party	This is an entity in the ecosystem that is different from an MNO or an issuing bank (e.g. card manufacturer, evaluation laboratory).
Trusted Service Manager (TSM)	A trusted party acting on behalf of the MNO and/or the issuing bank (see [EPC3] for more information)
UICC	Universal Integrated Circuit Card - A generic and well standardised Secure Element owned and issued by the MNOs.

Table 2: Terminology

0.3 Abbreviations

Term	Definition
AAUI	Application Activation User Interface
ATC	Application Transaction Counter
ATM	Automated Teller Machine
CASD	Controlling Authority Security Domain
CVM	Cardholder Verification Method
DAP	Data Authentication Pattern
ETSI	European Telecommunications Standards Institute
FCI	File Control Information
GP	Global Platform
GSMA	The GSM Association
IPR	Intellectual Property Rights
ISD	Issuer Security Domain
ISO	International Organisation for Standardisation
MCP	Mobile Contactless Payment
ME	Mobile Equipment
MNO	Mobile Network Operator
NFC	Near-Field Communication
OS	Operating System
OTA	Over the Air
POI	Point of Interaction
POS	Point of Sale
PPSE	Proximity Payment System Environment
RFID	Radio Frequency Identity
SD	Security Domain
SD (card)	Secure Digital card
SE	Secure Element
SEPA	Single Euro Payment Area
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMR	Service Management Role
SSD	Supplementary Security Domain
SP	Service Provider
TSM	Trusted Service Manager
TP	Third Party
UICC	Universal Integrated Circuit Card

Table 3: Abbreviations



0.4 Stakeholder Consultation and Validation Process

According to the roadmap approved by the EPC Plenary March 2009, this version of the Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines is provided for internal EPC and external stakeholder consultation with comments due by 17th June 2011. A final version is expected to be published by end of September 2011.

DRAFT

1 General

1.1 Introduction

In July 2010, the EPC published the first edition of a white paper [\[EPC6\]](#) which provides a high-level description of m-payments in general and, more specifically, of mobile contactless card payments.

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

1.2 Vision

The vision of EPC is to ensure the evolution of an integrated market for payments through the development and promotion of standards, best practices, and schemes.

Following this line, the EPC has been chartered by its member banks and payment institutions to leverage its existing leadership position for the practical deployment of mobile payments in SEPA.

The payment transactions enabled by mobile devices and services should build on existing SEPA Rulebooks and SEPA Cards Framework and (global) standards as far as possible. Therefore, EPC specifies rules, standards and guidelines to create the necessary environment so that payment service providers can deliver secure, efficient and user-friendly mobile solutions to access the SEPA payment instruments.

Cross-industry cooperation, especially between the banking sector and mobile network operators, has been identified as a critical success factor. Therefore EPC commits itself to help facilitate cross-industry cooperation on rules, standards and best practices in this area. Customers should not be bound to a specific mobile network operator or a particular mobile handset and should retain their current ability to switch between payment service providers.

1.3 Scope and Objectives

The purpose of this document is to provide interoperability implementation guidelines for Mobile Contactless Payments whereby SEPA card payments are the underlying SEPA payment instrument. The aim of the document is to

- Ensure that all deployed operational and transactional processes directly related to Mobile Contactless SEPA Card payments can be implemented while maintaining compliance with the [EC1] and all the other relevant regulations.
- Ensure that all deployed operational and transactional processes directly related to Mobile Contactless SEPA Card payments can be implemented while maintaining (at least) similar levels of risk management as for SEPA Contactless Card Payments.
- Ensure that all deployed operational and transactional processes directly related to Mobile Contactless SEPA Card Payments achieve an adequate level of interoperability.

- Provide guidance to payment service providers on Mobile Contactless Payments in addition to the existing technical standards developed by standardisation and industry bodies in the NFC ecosystem.

More specifically, the document aims to provide answers to the following questions:

- What are the roles for the main stakeholders in the Mobile Contactless SEPA Card Payment ecosystem?
- What are the service model alternatives for Mobile Contactless SEPA Card Payments?
- How is interoperability between the various stakeholders, within the same service model, ensured?
- What is the main architecture for Mobile Contactless SEPA Card Payments and how does it relate to SEPA Contactless Card Payments?
- What are the main technical and security issues?
- What are the main technical and security dependencies impacting the business?
- Who are the main industry/standardisation bodies involved and what is their focus?
- What are the remaining gaps for and the main challenges to market take-up on Mobile Contactless SEPA Card Payments?

1.4 Audience

The document is primarily intended for the following stakeholders:

- Payment service providers (banks and payment institutions).

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

- Trusted service managers (TSMs).
- Mobile network operators (MNOs).
- Equipment manufacturers.
- Merchants and merchant organisations.
- Consumers.
- MCP application developers.



- Regulators.
- Standardisation and industry bodies.

DRAFT

2 High-level business principles for MCP

The following high-level business principles have been employed for the specification of this guidelines document. They represent a more elaborate version of the guidelines contained in [\[EPC6\]](#) with a special emphasis on Mobile Contactless SEPA Card Payments.

1. MCPs shall be built on the SEPA Cards Framework.
2. Payment service providers should be able to diversify their services offer with enough leeway such that the current effective competitive marketplace for payments is not hampered.
3. Creating ease, convenience and trust for the end-customers, (consumers and merchants), using a mobile phone to initiate an MCP, is regarded as critical for the further development within this area.
4. Consumers shall be able to make MCPs throughout SEPA, regardless of the original country where the Mobile Contactless SEPA Cards application was issued.
5. Each individual consumer should have a similar experience when performing a MCP transaction. This includes the interaction with the accepting device (POI). However, this experience may slightly differ depending on the geographical location or other relevant environment conditions (e.g. influenced by the risk management).
6. Stakeholder (including consumers and merchants) payment liabilities will be no different to the ones valid for existing SEPA Card Payments deployments.
7. The payment service provider is responsible for the definition of its own graphical interface to the consumer, including brands & logos, card scheme brands, payment type, etc.... The mobile phone user interface (AAUI) shall be able to support this representation.
8. Consumers should not be bound to a specific mobile network operator or particular mobile equipment and should retain their current ability to switch between payment services providers. Note that the mobile phone will require NFC-capabilities.
9. Consumers shall be able to use MCP services issued by different payment service providers using a single mobile phone, and must be able to select the relevant MCP application to be used for a particular payment transaction.
10. MCPs should, as much as possible, leverage technologies which are already widely deployed in this sector. All referenced technologies and systems could however be subject to IPR rules.

3 Mobile Contactless SEPA Card Payments Overview

3.1 Introduction

This section provides a short description of Mobile Contactless SEPA Card Payments (MCP), which are defined as any Contactless SEPA Card Payment [\[EPC1\]](#) executed by a cardholder using a dedicated MCP application over NFC. The MCP application is provided by the issuing bank and is loaded onto the Secure Element, which is independently provided by the Secure Element issuer which may be the MCP issuer, the MNO or another third party. Regardless of which Secure Element is used, the introduction of the mobile contactless technology should aim to achieve the same security level as for the existing (contactless) SEPA card payments (see [\[EPC1\]](#)).

As illustrated in the following figure, the main parties involved in the MCP do not differ from a “classical” (contactless) SEPA card payment. The payment transaction is performed by reusing the existing SEPA contactless card payments accepting devices, while the back-end and transaction infrastructure will be those already used for SEPA card payments (blue shaded).

The participants in the MCP ecosystem illustrated in Figure 1 are as follows:

- The acquirer is a payment service provider enabling the processing of the merchant’s transaction to the issuing bank through an authorisation and clearing network.
- The card scheme is a technical and commercial arrangement setup to serve one or more card brands (in this document linked to MCP applications) and which provides the organisational, legal and operational framework rules necessary for the services marketed by the brand to function.
- The customer is an MNO subscriber (covering a variety of contractual relationships, e.g. pre-paid, post-paid) which has an agreement with an MCP issuer for MCP Service; the customer is required to have an NFC-enabled Mobile phone.
- The issuer (or issuing bank), is a payment service provider providing the MCP service to the consumer; the issuer is responsible for the provisioning of the MCP application to the Secure Element of the mobile equipment and the personalisation of the application with customer’s data. Furthermore, the issuer is also responsible for other life cycle management aspects. In the context of this document, it is also referred to as MCP (application) issuer.
- 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 device.
- The MNO offers data connectivity to the customer and potentially other services, including NFC-related services.
- The SE issuer is a trusted party responsible for providing the Secure Element for the storage of the MCP application in the mobile equipment. In case of a UICC, the SE issuer is the MNO (see [\[EPC3\]](#)).

- The Trusted Service Manager (TSM) is a trusted party acting on behalf of the SE issuers and/or the MCP issuers to facilitate an open ecosystem (see [EPC3] for more information). Several TSMs may co-exist offering mutually-competing services.

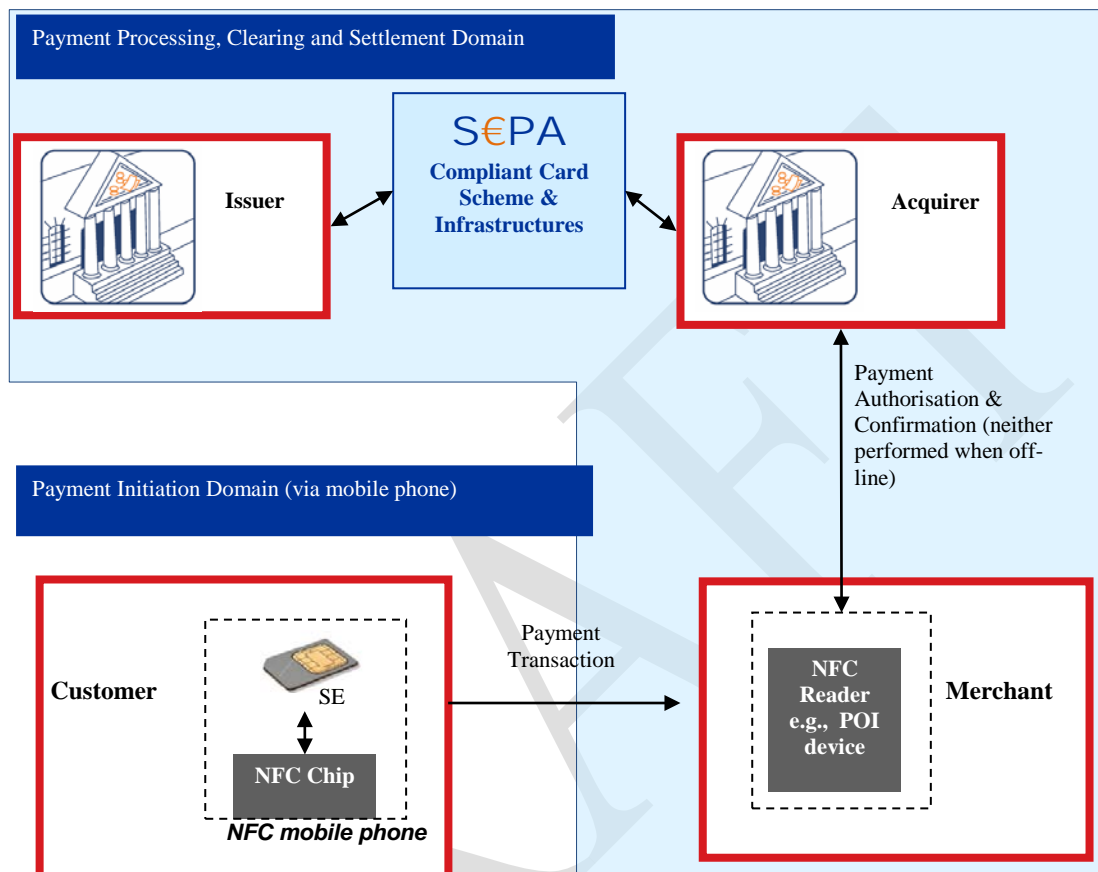


Figure 1: Mobile Contactless Card Payment Transaction

For the execution of a risk assessment it is important to distinguish between the following two phases related to MCP:

- The provisioning and life cycle management of the MCP application.
- The mobile contactless card payment transaction.

A short description of each of these phases is provided.

3.2 Provisioning and life cycle management

The MCP application is to be installed on a Secure Element in the mobile phone. This implies that dedicated processes need to be defined for the provisioning and management of the MCP application, which may vary depending on the Secure Element chosen. 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 such as TSMs, or MNOs in the case of the Secure Element (SE) being a UICC [EPC3].

The figure below provides an overview for the provisioning of an MCP application on a Secure Element and for its maintenance. Although this figure depicts a TSM, this entity might be omitted from these processes depending on the actual implementation. In this case, the issuing bank will be directly involved with the SE issuer.

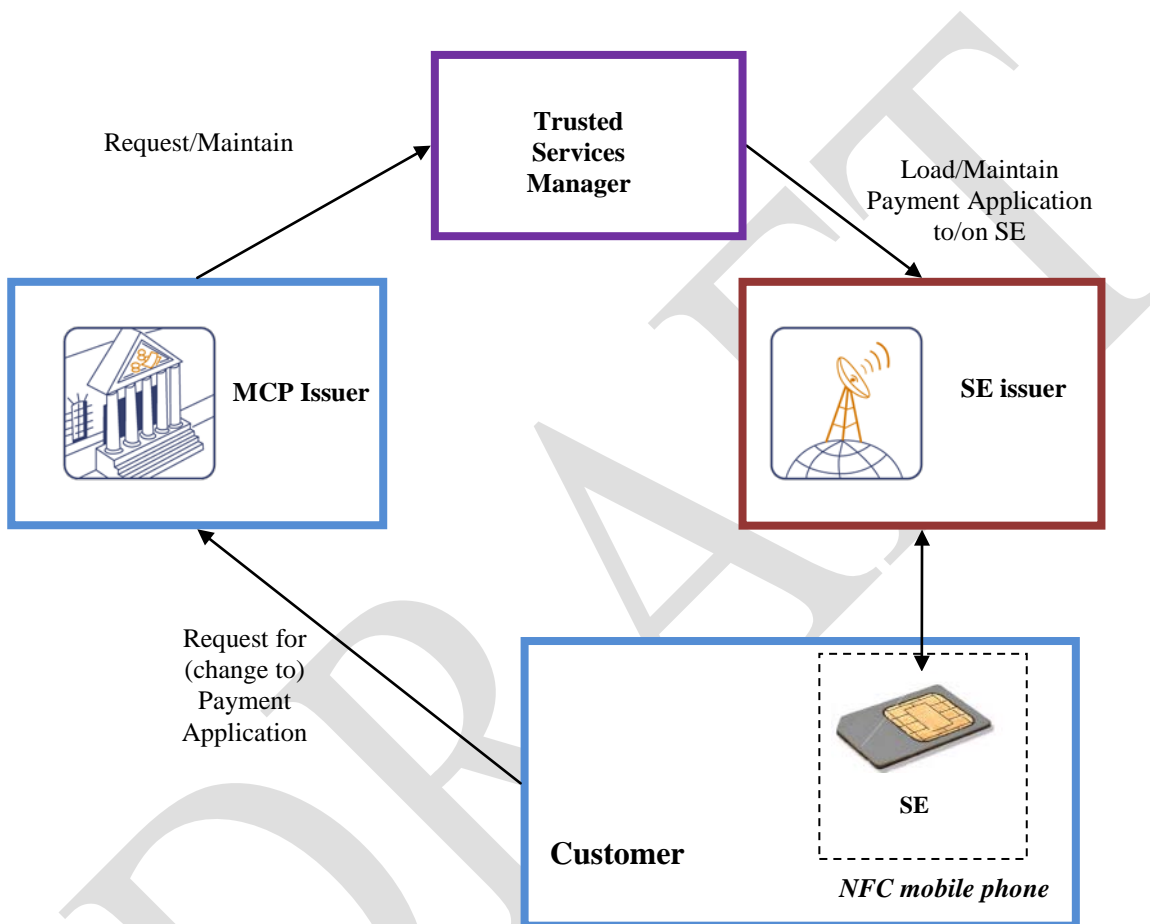


Figure 2: Provisioning/maintenance of MCP application on a Secure Element

3.3 MCP Transaction

The aim is that MCP transactions are expected to work with the existing contactless card payment terminal infrastructure on the basis that they will emulate card-based contactless applications. Generally speaking, these use EMV-style security processes. However, there may be business, functional or security reasoning for POI devices to have specific functionality to support MCP implementations e.g. the display of the transaction amount on the mobile phone. Also the authentication/authorisation of the payment transaction will be similar to (contactless) card payments [EPC1]. Therefore the document will mainly focus on the interaction between the mobile phone and the POI device. (See grey area in Figure 3)

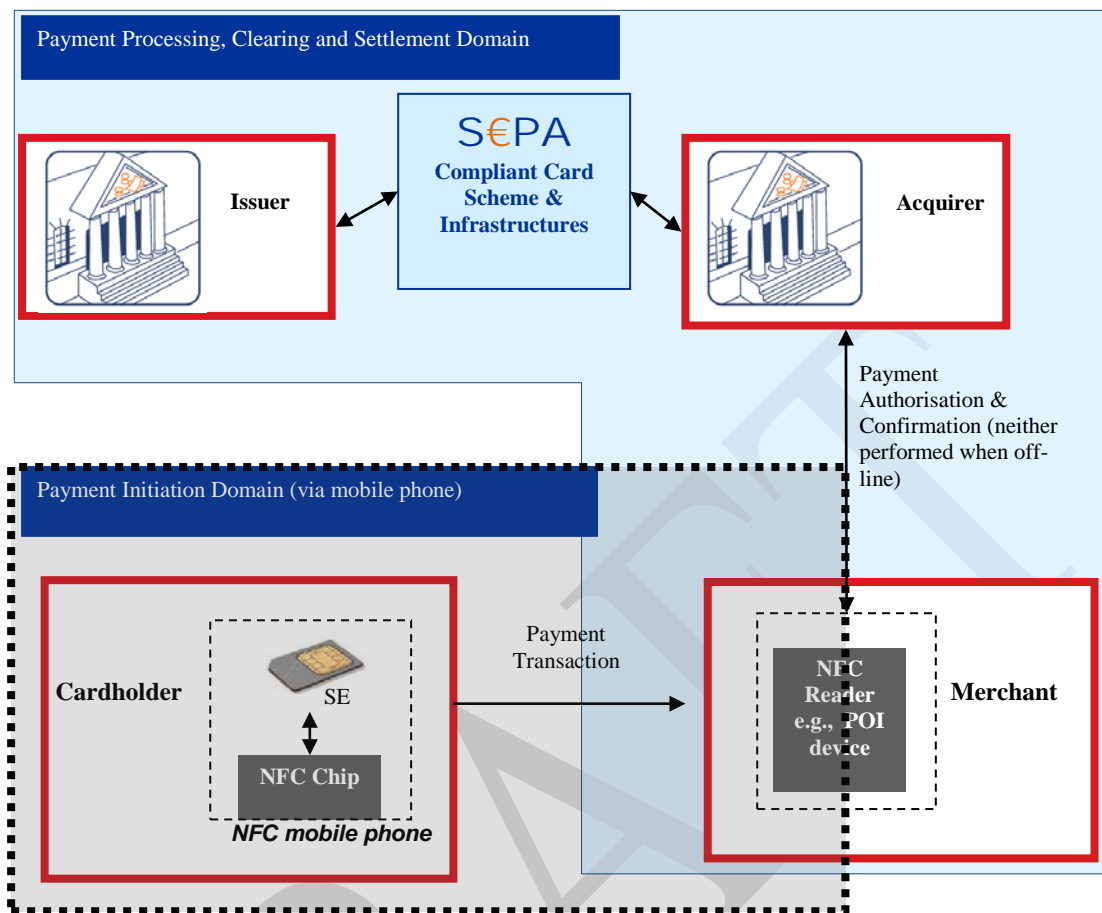


Figure 3: MCP Transaction

3.4 Basic MCP principles

The EPC Mobile Contactless SEPA Card Payments model defined in [EPC6] is based on the following principles:

- The MCP application is stored on a Secure Element in the Mobile phone.
- Three types of Secure Elements are considered:
 - UICC.
 - Embedded chip.
 - Secure micro SD card.
- The issuing bank is responsible for the life cycle management of the MCP application.
- The MNO is responsible for providing the data connectivity.

3.5 The MCP ecosystem

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

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

The main structure of the new ecosystem is depicted in Figure 4.

In addition to the main participants introduced in section 3.1, a number of additional new stakeholders may be identified:

- Secure Element manufacturers.
- MCP application developers.
- Mobile equipment manufacturers.
- NFC equipment manufacturers.
- Organisations performing certification for Secure Elements and MCP applications.

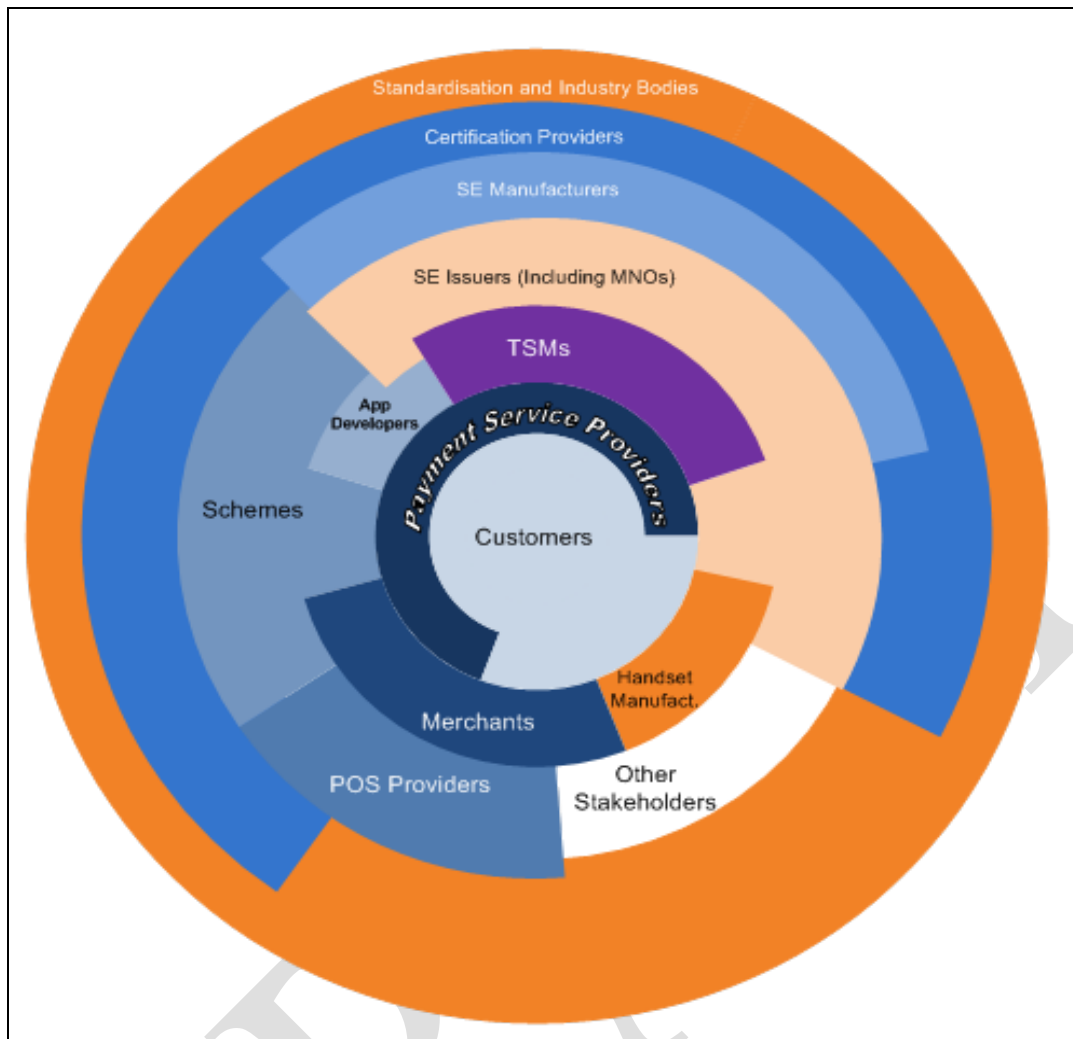


Figure 4: Mobile Contactless SEPA Card Payments Business Ecosystem

Contact points in the figure depict major business relationships between participants. The Mobile Contactless SEPA Card Payments Business Ecosystem is customer centric. The latter is not only a customer to the payment service provider but also to the merchant, the mobile handset manufacturer and, potentially, the SE issuer.

The Trusted Service Manager is a set of roles building the bridge between SE issuers (including MNOs) and issuing banks. Several companies may be involved to assume these roles.

Mobile Contactless SEPA card Payments interoperability is required and should be ensured by Standardisation and Industry Bodies as follows:

- Any MCP application can be stored and executed in any SE.
- Any NFC-enabled mobile phone can interact with any POI.
- Any MCP application can interact with any AAUI (see section 7.3.2) on the mobile phone.

4 Service Models

The Service Models for the provisioning and life cycle management of the MCP applications depend on the type of Secure Element (SE) that the MCP issuer will choose. As mentioned before, three alternatives for SEs are considered appropriate by the EPC to host the MCP application:

- The UICC, a generic and well standardised component.
- The embedded chip, a secure component which is integrated in the mobile phone at the time of manufacturing.
- The secure micro SD. There are two types of micro SD cards, one with and one without an NFC antenna. Both should be considered. The assumptions are the following:
 - A micro SD with NFC antenna will be used only in a mobile handset without NFC capabilities to avoid radio frequency issues and conflict.
 - A micro SD without NFC antenna will be used only in a mobile handset with NFC capabilities.

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 issuing bank, the Service Models are hereafter defined focusing on the co-operative domain.

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

Scenario	SE Type	SE issuer	MCP issuer
1	UICC	MNO	Issuing bank
2a	embedded chip	Mobile handset manufacturer	Issuing bank
2b		Third party (e.g. TSM or other TP)	Issuing bank
3a	micro SD	Third party (e.g. TSM or other TP)	Issuing bank
3b		Issuing bank	Issuing bank

Table 4: Secure Element types

For each of the five selected service scenarios in this section, it is intended to:

- Define the roles and responsibilities of the stakeholders.
- Define the basic principles.
- Define the necessary processes to issue the MCP².
- 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 [[EPC3](#)].

² based on the processes specified in [[EPC3](#)]

The existing agreements between the stakeholders directly involved and the other stakeholders, or agreements between the latter, are out of scope.

4.1 Scenario 1: the MNO provides the UICC

4.1.1 Introduction

In this scenario, the Secure Element 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 issuing bank or to the MNO:

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

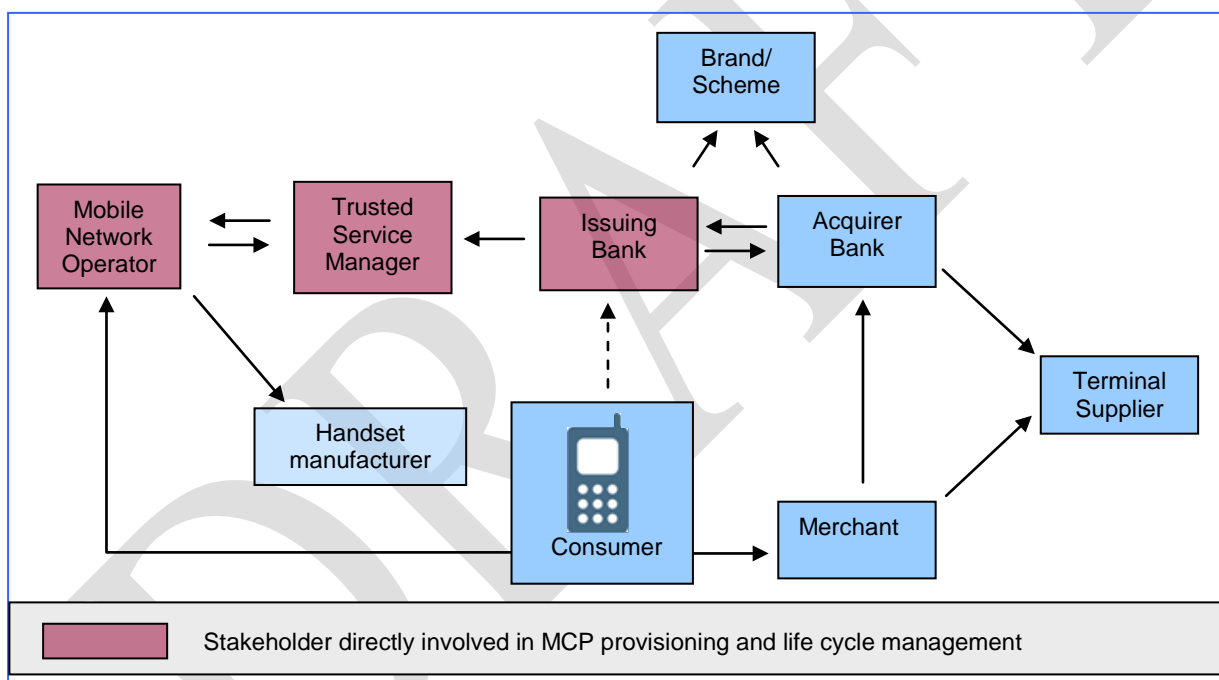


Figure 5: The MCP application resides on the UICC provided by the MNO

4.1.2 Analysis

The main advantages of this scenario are the following:

- This scenario facilitates the development of the mobile ecosystem involving other service providers.
- It allows easy connection between different MNOs and different MCP issuers.
- The distribution of the UICC to the end users is the responsibility of the MNO.

- The UICC has a 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 [EPC3]; therefore there is mutual understanding of the processes between MNOs and MCP issuers.
- The impact on issuing systems is less important for issuing banks 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 are the following:

- Interoperability between existing 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 meets the MCP business requirements specified by the EPC and 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....

4.2 Scenario 2a: the mobile handset manufacturer provides the embedded chip

4.2.1 Introduction

In this scenario, the Secure Element is an embedded chip in a mobile handset which is provided by the mobile handset manufacturer 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 issuing bank or to the mobile handset manufacturer:

- MCP services, e.g. provisioning and MCP application life cycle event (e.g. via mobile internet).
- Procuring space on the Secure Element on behalf of the issuing bank.
- Facilitating business (e.g. renting space) on the Secure Element on behalf of the mobile handset manufacturer.

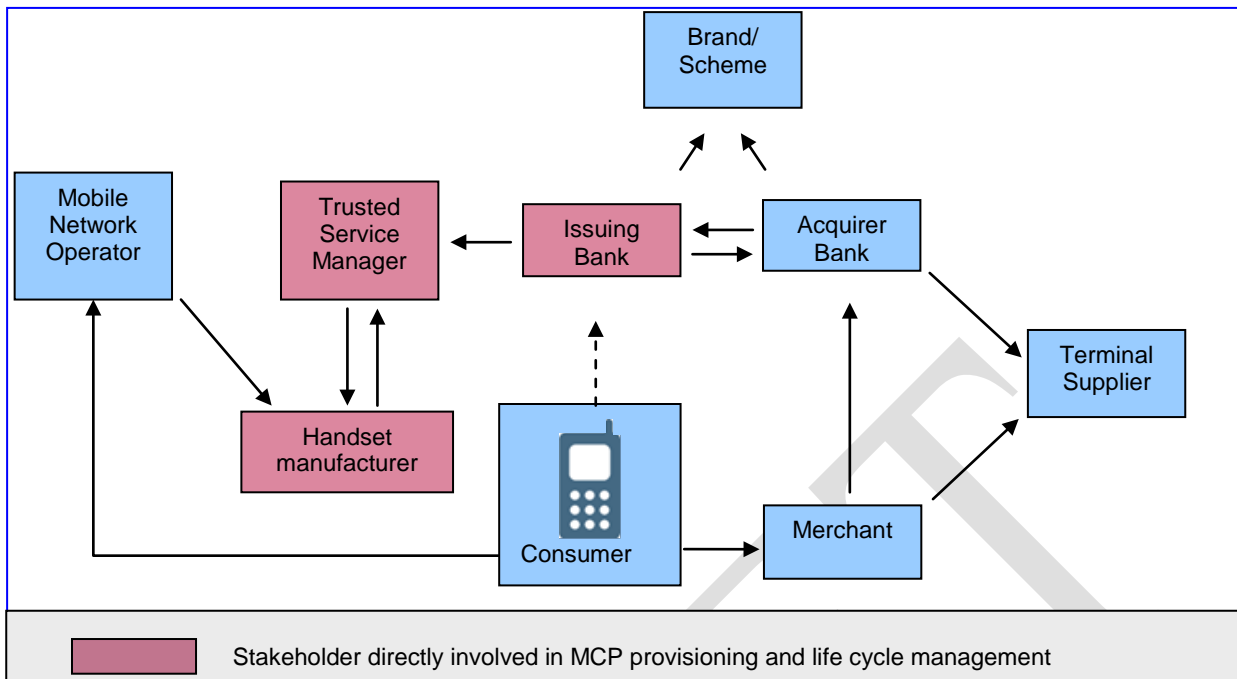


Figure 6: The MCP application resides on the embedded chip provided by the mobile handset manufacturer

4.2.2 Analysis

The main advantages of this scenario are the following:

- This scenario is prepared for a mobile ecosystem involving other service providers.
- It allows direct connection of multiple mobile handset manufacturers with multiple MCP issuers.
- Distribution of embedded chips is the responsibility of the mobile handset manufacturer.
- There is a possible advantage with respect to the certification of the chipset and the MCP application.
- From a security point of view, an embedded Secure Element offers the potential for a simpler environment (e.g. the choice of the secure chip, the co-existence with non-payment applications).

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

- Interoperability between existing TSMs.
- The MNOs to distribute and support mobile handsets with embedded chips.
- Agreement on one common process to be followed by all different mobile handset manufacturers.
- The timely delivery of appropriate technical/security standards needed e.g. by Global Platform and NFC Forum.

This scenario meets the MCP business requirements specified by the EPC and 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.

4.3 Scenario 2b: a third party provides the embedded chip

4.3.1 Introduction

In this scenario, the Secure Element is an embedded chip in a mobile handset 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 following services could be provided by the TSM to either the issuing bank or the third party:

- MCP services, e.g. provisioning and MCP application life cycle event (e.g. via mobile internet).
- Procuring space on the Secure Element on behalf of the issuing bank.
- Facilitating business (e.g. renting space) on the Secure Element on behalf of the third party.

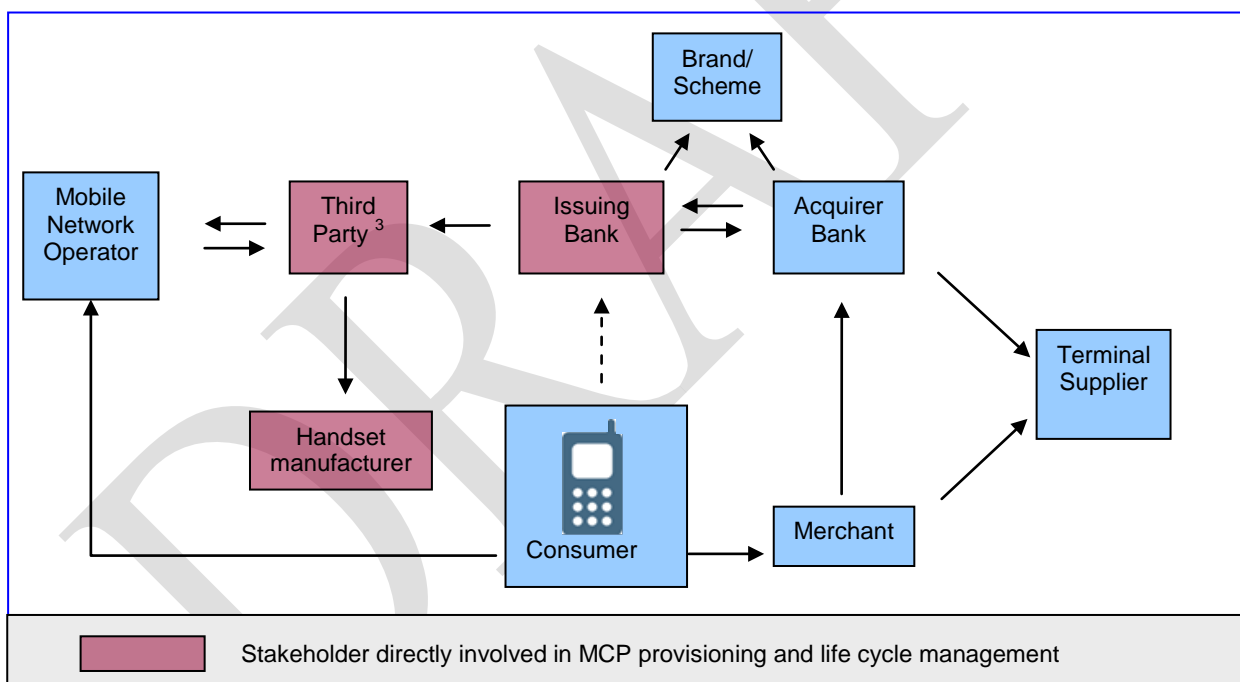


Figure 7: The MCP application resides on the embedded chip provided by the third party

4.3.2 Analysis

The main advantages of this scenario are the following:

³ The third party can be a TSM or another third party

- This scenario is prepared for a mobile ecosystem involving other service providers.
- There is a possible advantage with respect to the certification of the chipset with the MCP application.
- From a security point of view, an embedded SE offers the potential for a simpler environment (e.g. the choice of the secure chip and the co-existence with non-payment applications).

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

- Interoperability between existing TSMs.
- Establishment of appropriate third parties and their relationship with TSMs.
- Agreement between third parties and mobile handset manufacturers for the embedding and the distribution of embedded chips in mobile handsets.
- The MNOs will have to distribute and support mobile handsets with embedded chips.
- The timely delivery of appropriate technical/security standards needed, provided e.g. by Global Platform and NFC Forum.

This scenario meets the MCP business requirements specified by the EPC and 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 holds an increased complexity due to the different responsible stakeholders for the Secure Elements and the mobile handsets. A number of aspects, such as the responsibility for the Secure Element certification, the mobile handset certification and the support for the Secure Element by the mobile handset manufacturer are additional challenges that are an extra burden for implementations of this service model.

4.4 Scenario 3a: a third party provides the micro SD

4.4.1 Introduction

In this scenario, the Secure Element is a micro SD card in a mobile handset which is provided by a third party 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 issuing bank or to the third party:

- MCP services, e.g. provisioning and MCP application life cycle event (e.g. via mobile internet).
- Procuring space on the Secure Element on behalf of the issuing bank.
- Facilitating business (e.g. renting space) on the Secure Element on behalf of the third party.

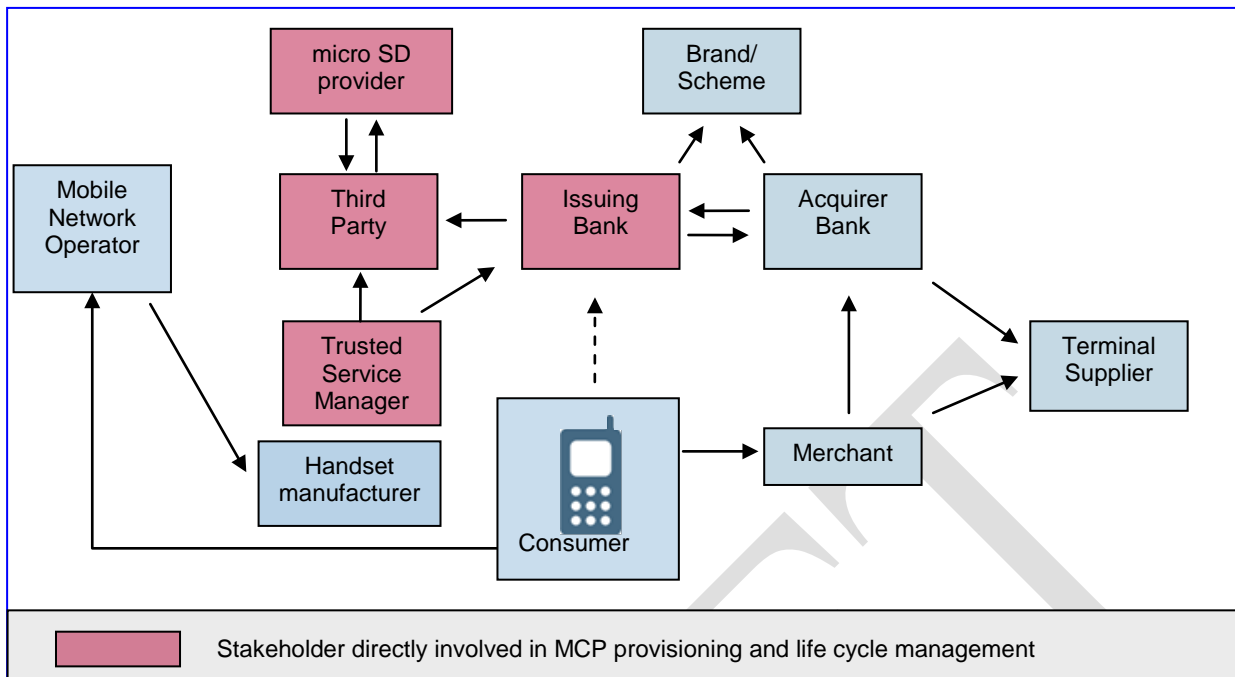


Figure 8: The MCP application resides on the micro SD provided by a third party

4.4.2 Analysis

The main advantages of this scenario are the following:

- It allows quick pilots by a single Issuing Bank to bridge technology.
- A micro SD is easy to distribute, analogous to the distribution of a physical plastic card.
- It facilitates portability in the case of a micro SD equipped with an NFC antenna, even if the set of APIs will have to be reloaded into the new mobile handset.

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

- For the moment, no standard exists by which the micro SD slot securely communicates with the user interface and the entity in charge of the Service Management roles. This means that “quick to market” efforts might be slowed down because of technical limitations.
- Interoperability between existing TSMs.
- The APIs used are not standardised:
 - Specific sets of APIs, to reach the mobile handset OTA, must be supported by the entity in charge of the service management roles for each new vendor.
 - Specific sets of APIs, to reach the micro SD, shall be supported by the AAUI.

Currently, there are no initiatives for standardisation in this area, even if there are some initial discussions within GlobalPlatform to issue a specification.

Moreover, the APIs also depend on the mobile handsets platform (java, android, etc.).

- There might be more potential technical barriers in case of micro SD with antenna, e.g. related to adequate testing and compatibility with the mobile handset.
- Establishment of appropriate Third Parties which link with multiple MCP issuers.

- Today, it is more appropriate for single MCP application than for multiple MCP applications issuing.

From a pure technical perspective, this scenario could meet the MCP business requirements specified by the EPC since it is suitable for hosting multiple payment applications. However, there are other important obstacles which might be very challenging to be addressed such as the MCP application selection in the user interface and possible security aspects related to hosting multiple applications on a micro SD card.

4.5 Scenario 3b: the issuing bank provides the micro SD

4.5.1 Introduction

In this scenario, the Secure Element is a micro SD card in a mobile handset which is provided by the MCP issuer who is also responsible for the issuance and life cycle management of the MCP application.

The following services could be provided by the TSM to the issuing bank:

- MCP services, e.g. provisioning and MCP application life cycle event (e.g. via mobile internet).
- Procuring space on the Secure Element on behalf of the issuing bank.
- Facilitating business (e.g. renting space) on the Secure Element on behalf of the third party.

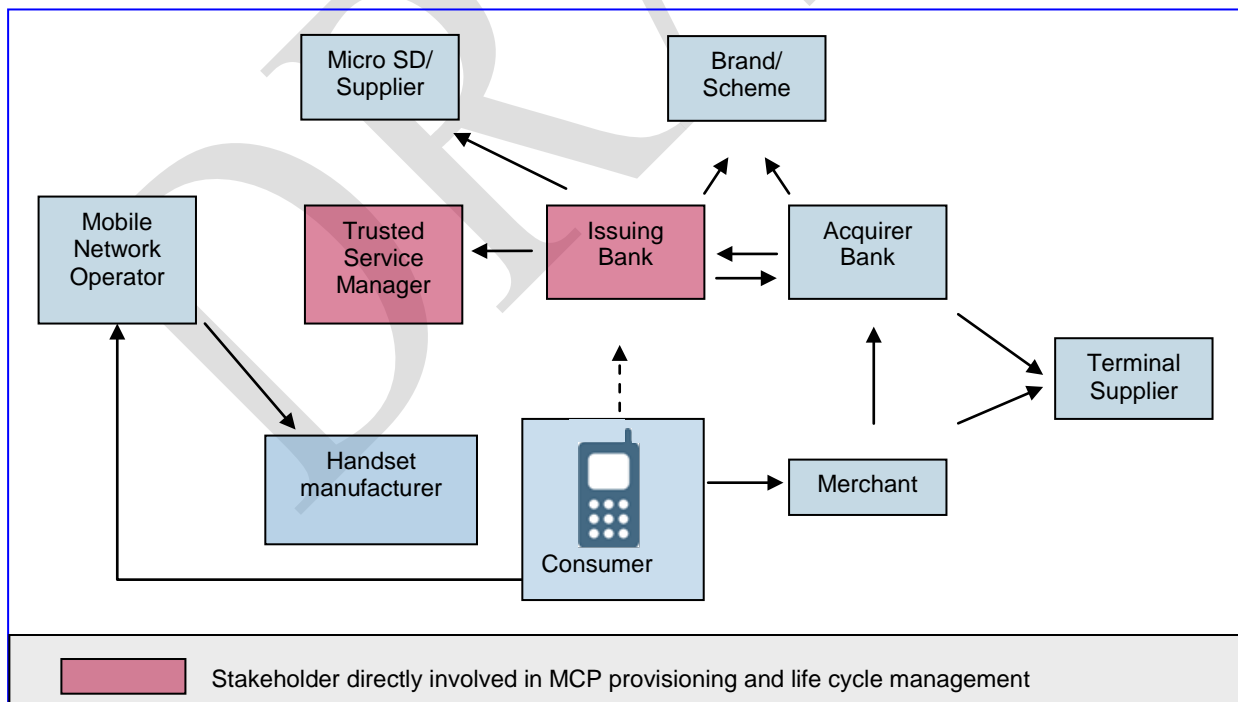


Figure 9: The MCP application resides on the micro SD provided by the issuing bank

4.5.2 Analysis

The main advantages of this scenario are the following:

- It allows quick pilots by a single issuing bank to bridge technology.
- A micro SD is easy to distribute, analogous to the distribution of a physical plastic card.
- It facilitates portability in the case of a micro SD equipped with an NFC antenna, even if the set of APIs will have to be reloaded into the new mobile handset.

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

- Interoperability between existing TSMs.
- For the moment, no standard exists by which the micro SD slot securely communicates with the user interface and the entity in charge of the Service Management roles. This means that “quick to market” efforts might be slowed down because of technical limitations.
- There might be more potential technical barriers in case of micro SD with antenna, e.g. related to adequate testing and compatibility with the mobile handset.
- The APIs used are not standardised:
 - Specific sets of APIs, to reach the mobile handset OTA, must be supported by the entity in charge of the service management roles for each new vendor.
 - Specific sets of APIs, to reach the micro SD, shall be supported by the AAUI.Currently, there are no initiatives for standardisation in this area, even if there are some initial discussions within GlobalPlatform to issue a specification. Moreover, the APIs also depend on the mobile handsets platform (java, android, etc.).
- Today, it is more appropriate for a single MCP application than for multiple MCP applications issuing.

This scenario meets the MCP business requirements specified by the EPC and is suitable for hosting multiple payment applications, but from the same MCP issuer only.

Note that in this scenario, multiple payment applications from multiple MCP issuers are unlikely.

4.6 Conclusions

From a pure technical perspective, the UICC-based solution offers the most straightforward deployment in view of the maturity of available standards and the existing infrastructure. However, some business-related aspects, such as the three or four corner model [[EPC3](#)], the business model as well as the specification of the appropriate SLAs might prove to be challenging.

Until now, with respect to the usage of embedded SEs, the model based on a third party as SE issuer appears to encompass too many challenges to offer an immediate solution (see section 4.3). These challenges appear only to be resolvable by big market players in the mobile ecosystem. In the case of the mobile handset manufacturer being responsible for the supply of the embedded SE (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 section 5.

In view of the analyses above, it becomes obvious that the usage of micro SD cards might be a good approach as a bridging technology because of its quick time to market and straightforward business model, at least in the case whereby the issuing bank provides the micro SD card. In this case, it could even be targeted towards multi-applications from the same issuing bank. However, other challenges might need to be faced, such as the lack of adequate interoperable standards and specifications (see section 7.8) and the availability of a wide range of appropriate mobile handsets. Moreover the usage of micro SD cards provided by individual issuing banks may also lead to a higher market fragmentation.

DRAFT

5 Process-level guidelines

The Service Models for the provisioning and life cycle management for the MCP applications depend on the type of Secure Element (SE) that the issuing bank will choose.

This section provides an overview of the different processes involved in the management of an MCP application between the different participants: MCP issuers, SE issuers, MNOs and customers.

It contains:

- The procedures that a customer shall follow during the life cycle of the MCP application.
- The information flows between the different participants.

The processes are described for the three SE alternatives which host the MCP application: the UICC, the embedded chip and the secure micro SD with their specific details depending on the issuance of the SE (see section 4 for a comprehensive description).

The process flow specified in section 5 in [EPC3] is used as a skeleton for the MCP life cycle overview in the sequel of this section. However, a split is made for the MNO between its roles as SE issuer and as mobile network provider.

5.1 Processes overview of the MCP life cycle for scenario 1

In this scenario, the Secure Element is the 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.

Figure 10 provides an overview of the processes which are subsequently specified below.

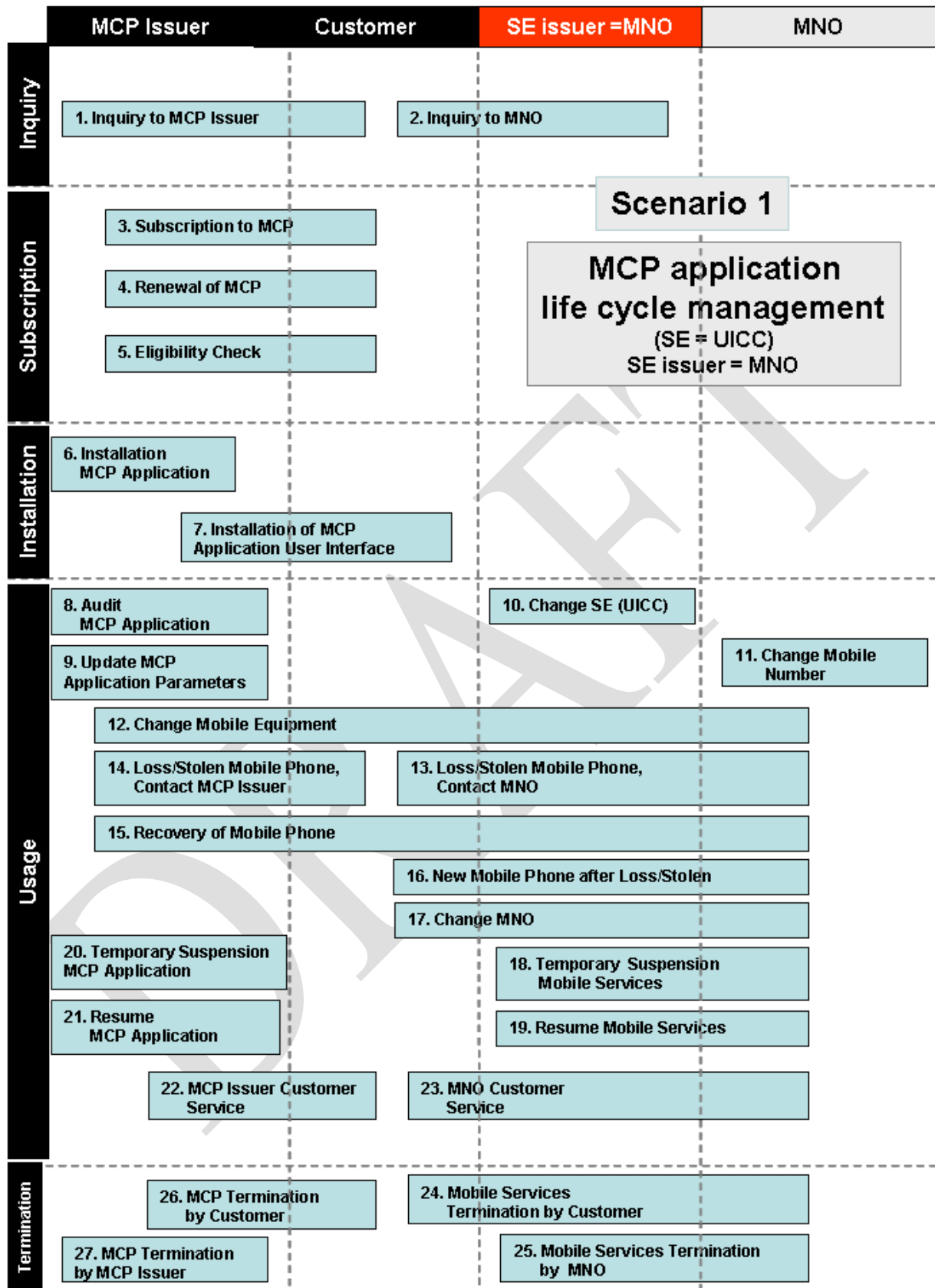


Figure 10: MCP life cycle overview for scenario 1

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 I of [EPC3].

Step 1: Customer Inquiry

The customer discovers the MCP services, typical examples are:

- **Process 1:** The customer requests information regarding MCP Services/Applications from the issuing bank.
- **Process 2:** The customer requests information regarding MCP Services/Applications from the SE issuer (MNO). The MNO refers the customer to the issuing bank.

Step 2: Subscription to MCP application

- **Process 3:** The customer subscribes to a MCP application with the issuing bank.
 - Use case 1 – The customer subscribes to a first MCP application from a given issuing bank for a given Secure Element.
 - Use case 2 – The customer subscribes to the addition of a new MCP application to the Secure Element from the same issuing bank.
- **Process 4:** The customer replaces/renews the current MCP application with a new one on the same Secure Element. The issuing bank proposes to renew the customer's existing application or proposes a new one.
- **Process 5:** The issuing bank checks the eligibility of the customer with the MNO and takes appropriate action as necessary with respect to the customer.

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

Step 3: Installation of the MCP application

- **Process 6:** The issuing bank installs the MCP application on the Secure Element in the Customer's mobile phone.
- **Process 7:** The issuing bank installs the MCP application User Interface. This might involve the customer.

Step 4: Usage of the MCP application

- **Process 8:** The issuing bank checks the status of the MCP application on the Secure Element.

- **Process 9:** The issuing bank updates the MCP application (parameters).
- **Process 10:** The customer changes the Secure Element.
- **Process 11:** The customer changes mobile phone number but keeps the same Secure Element and MNO. The end user has an operational mobile-NFC service deployed and activated (or locked). This change results in a change of the end user identifier and potentially in the way to reach the mobile phone via OTA channel. The MNO notifies the other participants of the ecosystem that the customer has changed his/her mobile phone number and, in particular, the issuing bank or TSM as appropriate. All participants of the ecosystem need to update their information systems with this change. The mobile equipment and the Secure Element are accessible through a new mobile phone number.
- **Process 12:** The customer changes his/her mobile equipment.
 - Use case 1: The new mobile equipment is unable to work with the Secure Element. The customer contacts the MNO's help desk.
 - Use case 2: The new mobile equipment works with the Secure Element. The MNO, once informed about the new mobile equipment (via any technical means), informs the issuing bank accordingly.
 - Use case 2a: The new mobile equipment detects the MCP application on the Secure Element and triggers the download of the MCP application User Interface by the issuing bank.
 - Use case 2b: The new mobile equipment is unable to identify the MCP application and therefore cannot download the MCP application User Interface. The customer contacts the issuing bank's help desk.
- **Process 13:** The customer's mobile phone is lost or stolen. The customer contacts the MNO's help desk.
- **Process 14:** The customer's mobile phone is lost or stolen. The customer contacts the issuing bank's help desk.
- **Process 15:** Following the loss (or theft) of the mobile phone, the customer recovers the mobile phone and contacts the MNO or the issuing bank as appropriate.
- **Process 16:** Following the loss (or theft) of the mobile phone, the customer gets new mobile equipment and a new Secure Element.
- **Process 17:** The customer changes MNO (typically retaining the number) and wishes to extend the MCP application to the new MNO.
- **Process 18:** The MNO temporarily suspends the mobile services.
- **Process 19:** Following the suspension of the mobile services, the MNO resumes the mobile services.

- **Process 20:** The issuing bank temporarily suspends the MCP service.
- **Process 21:** Following the suspension of the MCP application, the issuing bank resumes the MCP application.
- **Process 22:** The customer contacts the issuing bank's help desk.
- **Process 23:** The customer contacts the MNO's help desk.

Step 5: Termination of the MCP application

- **Process 24:** The customer terminates the mobile services with the MNO.
- **Process 25:** The MNO terminates the customer's mobile services.
- **Process 26:** The customer requests the termination of the MCP application.
- **Process 27:** The issuing bank terminates the MCP application.

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

In this scenario, the Secure Element is an embedded chip in a mobile handset which is supplied by the mobile handset manufacturer while the MCP issuer is responsible for the issuance and life cycle management of the MCP application.

Figure 11 provides an overview of all the processes in this scenario.

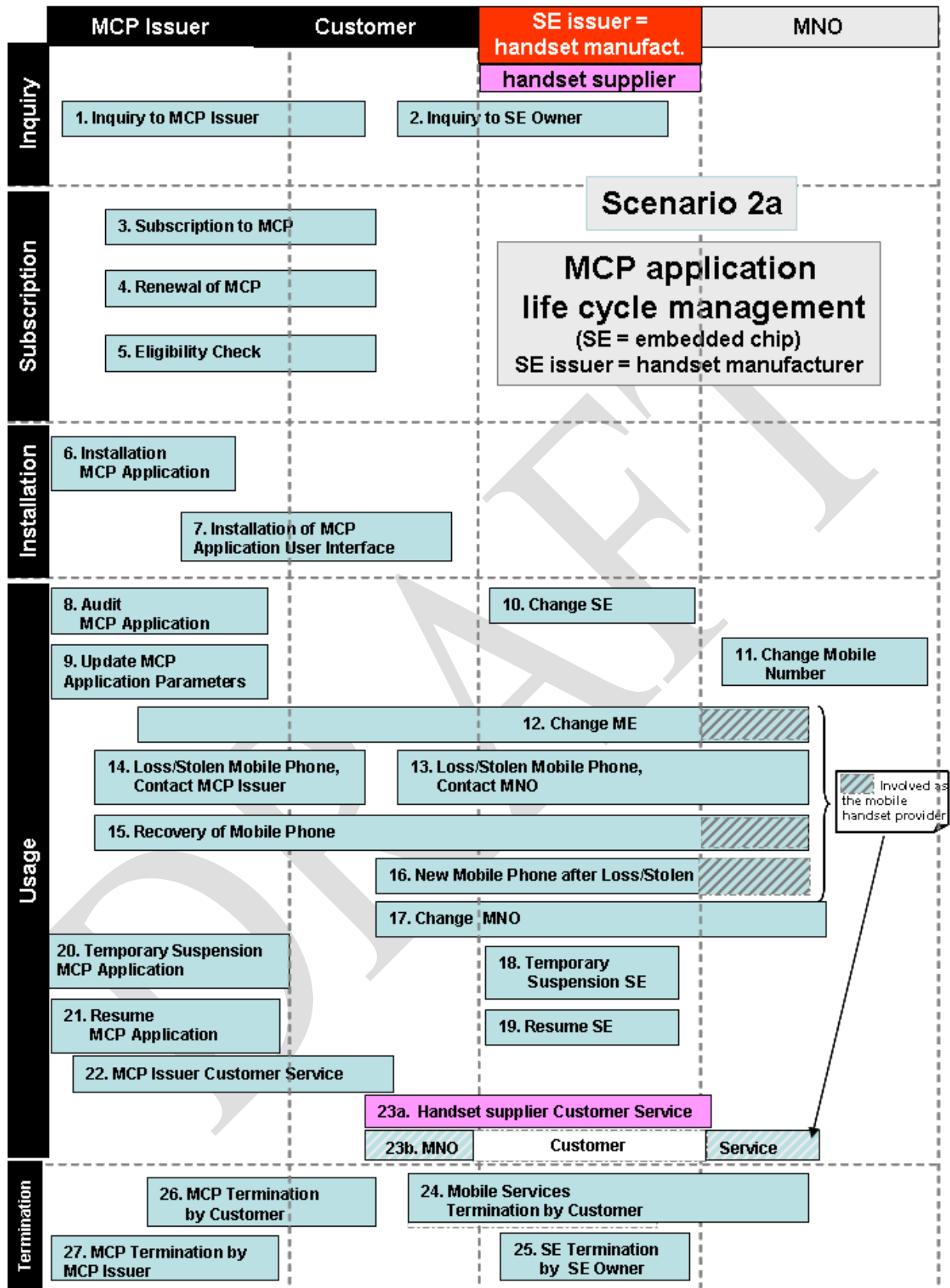


Figure 11: MCP life cycle overview for scenario 2a

Step 1: Customer Inquiry

The customer discovers the MCP services, typical examples are:

- **Process 1:** The customer requests information regarding MCP Services/Applications from the issuing bank.
- **Process 2:** The customer requests information regarding MCP Services/Applications from the SE issuer (mobile handset manufacturer). The mobile handset manufacturer refers the customer to the issuing bank.

Step 2: Subscription to MCP application

- **Process 3:** The customer subscribes to a MCP application with the issuing bank.
 - Use case 1 – The customer subscribes to a first MCP application from a given issuing bank for a given Secure Element.
 - Use case 2 – The customer subscribes to the addition of a new MCP application to the Secure Element from the same issuing bank.
- **Process 4:** The customer replaces/renews the current MCP application with a new one on the same Secure Element. The issuing bank proposes to renew the customer's existing application or proposes a new one.
- **Process 5:** The issuing bank checks the eligibility of the customer with the MNO and takes appropriate action as necessary with respect to the customer.

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

Step 3: Installation of the MCP application

- **Process 6:** The issuing bank installs the MCP application on the Secure Element in the Customer's mobile phone.
- **Process 7:** The issuing bank installs the MCP application User Interface. This might involve the customer.

Step 4: Usage of the MCP application

- **Process 8:** The issuing bank checks the status of the MCP application on the Secure Element.
- **Process 9:** The issuing bank updates the MCP application (parameters).

- **Process 10:** The customer changes the Secure Element. As the Secure Element is an embedded chip, to change the Secure Element also implies a change of ME. (See Process 12).
- **Process 11:** The customer changes mobile phone number but keeps the same Secure Element and MNO. The end user has an operational mobile-NFC service deployed and activated (or locked). This change results in a change of the end user identifier and potentially in the way to reach the mobile phone via OTA channel. The MNO notifies the other participants of the ecosystem that the customer has changed his/her mobile phone number and, in particular, the issuing bank or TSM as appropriate. All participants of the ecosystem need to update their information system with this change. The mobile equipment and the Secure Element are accessible through a new mobile phone number.
- **Process 12:** The customer changes his/her mobile equipment. As the Secure Element is an embedded chip, to change ME also implies a change of the Secure Element (see Process 10). The new mobile equipment works with the Secure Element. The MNO being informed about the new mobile equipment (via any technical means), informs the issuing bank accordingly. The new mobile equipment is unable to identify the MCP application and therefore cannot download the MCP application User Interface. The customer contacts the issuing bank's help desk.
- **Process 13:** The customer's mobile phone is lost or stolen. The customer contacts the MNO's help desk.
- **Process 14:** The customer's mobile phone is lost or stolen. The customer contacts the issuing bank's help desk.
- **Process 15:** Following the loss (or theft) of the mobile phone, the customer recovers the mobile phone and contacts the MNO or the issuing bank as appropriate.
- **Process 16:** Following the loss (or theft) of the mobile phone, the customer gets new mobile equipment and a new Secure Element.
- **Process 17:** The customer changes MNO (typically retaining the number) and wishes to extend the MCP application to the new MNO.
 - Use case 1: If the customer keeps his/her ME, he also keeps his/her Secure Element with the MCP application and AAUI on the mobile phone. The new entity in charge of the Service Management role must register the new customer and his/her ME in its database to offer the MCP service.
 - Use case 2: If the customer gets a new ME from the new MNO (typically retaining the number), he asks the new MNO to extend the MCP application.
- **Process 18:** The MNO temporarily suspends the mobile services.
- **Process 19:** Following the suspension of the mobile services, the MNO resumes the mobile services.

- **Process 20:** The issuing bank temporarily suspends the MCP service.
- **Process 21:** Following the suspension of the MCP application, the issuing bank resumes the MCP application.
- **Process 22:** The customer contacts the issuing bank's help desk.
- **Process 23a:** Depending on the business model, the customer contacts the respective help desk dependent on the supplier of the mobile handset. This might be for example the MNO.
- **Process 23b:** The customer contacts the MNO's helpdesk.

Step 5: Termination of the MCP application

- **Process 24:** The customer terminates the mobile services with the MNO.
- **Process 25:** The MNO terminates the customer's mobile services.
- **Process 26:** The customer requests the termination of the MCP application.
- **Process 27:** The issuing bank terminates the MCP application.

Note: for processes 18, 19, 23 and 24 corresponding to Suspension, Resume and Termination, the MCP service must be terminated prior to the suspension of the MNO subscription to avoid OTA problems.

5.3 Processes overview of the MCP life cycle for scenario 2b

In this scenario, the Secure Element is an embedded chip in the mobile handset, 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.

Figure 12 provides an overview of all the processes for this scenario.

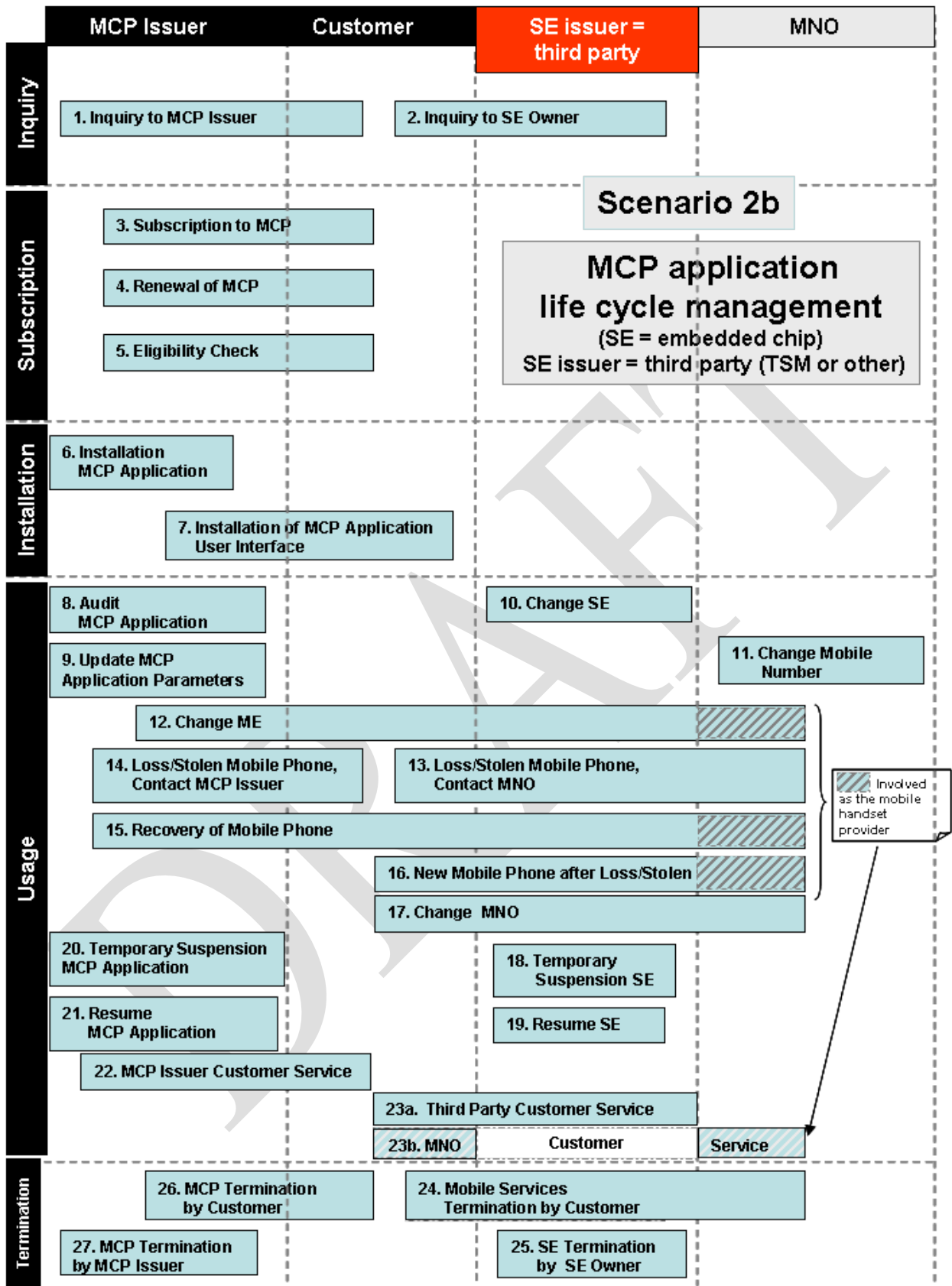


Figure 12: MCP life cycle overview for scenario 2b

Step 1: Customer Inquiry

The customer discovers the MCP services, typical examples are:

- **Process 1:** The customer requests information regarding MCP Services/Applications from the issuing bank.
- **Process 2:** The customer requests information regarding MCP Services/Applications from the SE issuer (third party). The third party refers the customer to the issuing bank.

Step 2: Subscription to MCP application

- **Process 3:** The customer subscribes to an MCP application with the issuing bank.
 - Use case 1 – The customer subscribes to a first MCP application from a given issuing bank for a given Secure Element.
 - Use case 2 – The customer subscribes to the addition of a new MCP application to the Secure Element from the same issuing bank.
- **Process 4:** The customer replaces/renews the current MCP application with a new one on the same Secure Element. The issuing bank proposes to renew the customer's existing application or proposes a new one.
- **Process 5:** The issuing bank checks the eligibility of the customer with the MNO and takes appropriate action as necessary with respect to the customer.

As a result of step 2 it is assumed that the customer is equipped with the appropriate MCP compatible mobile phone (mobile equipment + Secure Element).

Step 3: Installation of the MCP application

- **Process 6:** The issuing bank installs the MCP application on the Secure Element in the Customer's mobile phone.
- **Process 7:** The issuing bank installs the MCP application User Interface. This might involve the customer.

Step 4: Usage of the MCP application

- **Process 8:** The issuing bank checks the status of the MCP application on the Secure Element.
- **Process 9:** The issuing bank updates the MCP application (parameters).
- **Process 10:** The customer changes the Secure Element.

- **Process 11:** The customer changes mobile phone number but keeps the same Secure Element and MNO. The end user has an operational mobile-NFC service deployed and activated (or locked). This change results in a change of the end user identifier and potentially in the way to reach the mobile phone via OTA channel. The MNO notifies the other participants of the ecosystem that the customer has changed his/her mobile phone number and, in particular, the issuing bank or TSM as appropriate. All participants of the ecosystem need to update their information system with this change. The mobile equipment and the Secure Element are accessible through a new mobile phone number.
- **Process 12:** The customer changes his/her mobile equipment. As the Secure Element is an embedded chip, to change ME also necessitates a change of Secure Element. (See Process 10). The new mobile equipment works with the Secure Element. The MNO, once informed about the new mobile equipment (via any technical means), informs the issuing bank accordingly. The new mobile equipment is unable to identify the MCP application and therefore cannot download the MCP application User Interface. The customer contacts the issuing bank's help desk.
- **Process 13:** The customer's mobile phone is lost or stolen. The customer contacts the MNO's help desk.
- **Process 14:** The customer's mobile phone is lost or stolen. The customer contacts the issuing bank's help desk.
- **Process 15:** Following the loss (or theft) of the mobile phone, the customer recovers the mobile phone and contacts the MNO or the issuing bank as appropriate.
- **Process 16:** Following the loss (or theft) of the mobile phone, the customer gets new mobile equipment and a new Secure Element.
- **Process 17:** The customer changes MNO (typically retaining the number) and wishes to extend the MCP application to the new MNO.
 - Use case 1: If the customer keeps his/her ME, he also keeps his/her Secure Element with the MCP application and AAUI on the mobile phone. The new entity in charge of the Service Management role must register the new customer and his/her ME in its database to offer the MCP service.
 - Use case 2: If the customer gets a new ME from the new MNO (typically retaining the number), he asks the new MNO to extend the MCP application.
- **Process 18:** The MNO temporarily suspends the mobile services.
- **Process 19:** Following the suspension of the mobile services, the MNO resumes the mobile services.
- **Process 20:** The issuing bank temporarily suspends the MCP service.

- **Process 21:** Following the suspension of the MCP application, the issuing bank resumes the MCP application.
- **Process 22:** The customer contacts the issuing bank's help desk.
- **Process 23a:** The customer contacts the third party helpdesk responsible for the issuance of the SE.
- **Process 23b:** The customer contacts the MNO's helpdesk.

Step 5: Termination of the MCP application

- **Process 24:** The customer terminates the mobile services with the MNO.
- **Process 25:** The MNO terminates the customer's mobile services.
- **Process 26:** The customer requests the termination of the MCP application.
- **Process 27:** The issuing bank terminates the MCP application.

Note: for processes 18, 19, 23 and 24 corresponding to Suspension, Resume and Termination, the MCP service must be terminated prior to the suspension of the MNO subscription to avoid OTA problems.

5.4 Processes overview of the MCP life cycle for scenario 3a

In this scenario, the Secure Element is a secure micro SD card in a mobile handset which is provided by a third party while the MCP issuer is responsible for the issuance and life cycle management of the MCP application.

Figure 13 provides an overview of all the processes for this scenario.

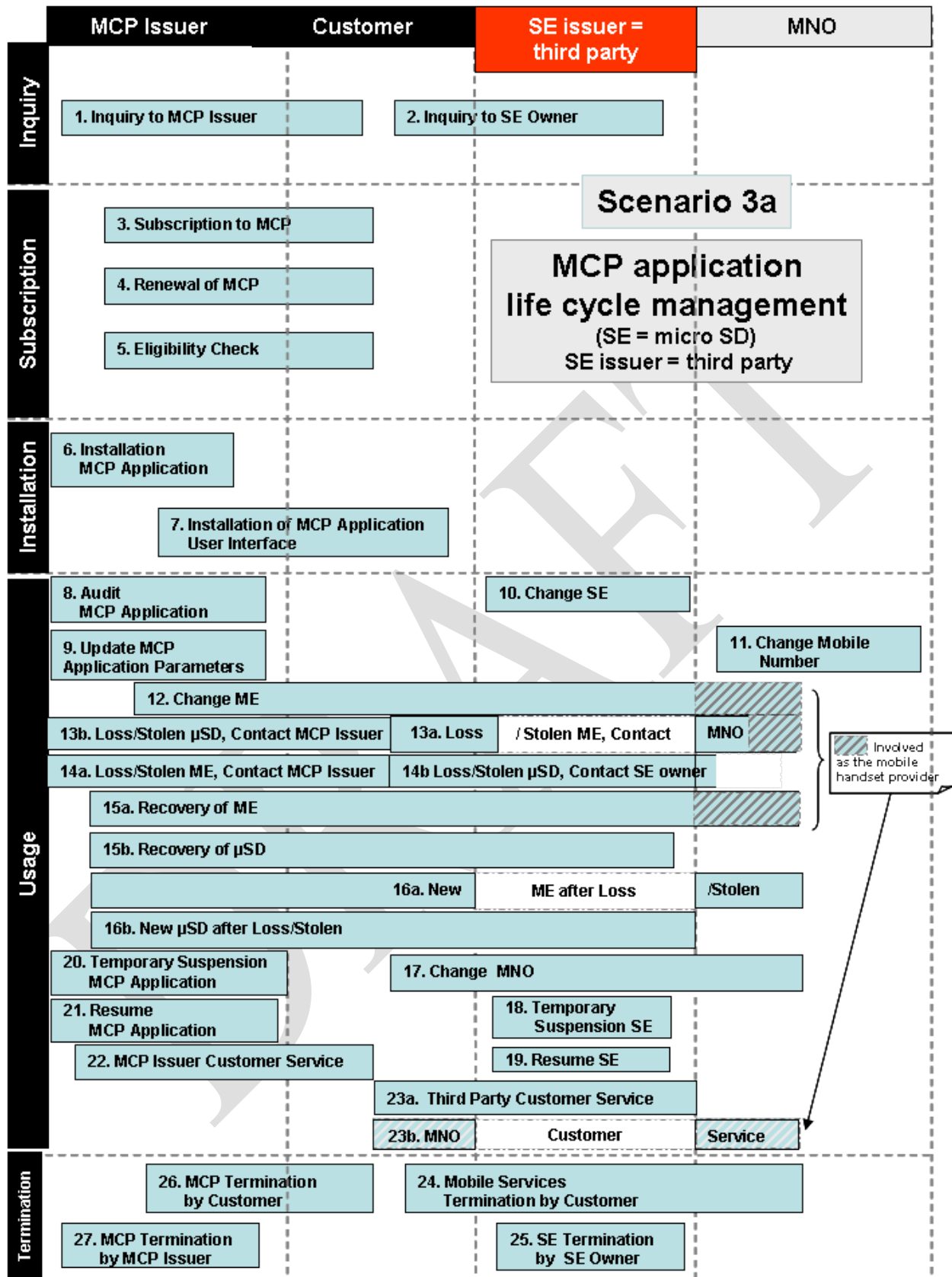


Figure 13: MCP life cycle overview for scenario 3a

Step 1: Customer Inquiry

The customer discovers the MCP services, typical examples are:

- **Process 1:** The customer requests information regarding MCP Services/Applications from the issuing bank.
- **Process 2:** The customer requests information regarding MCP Services/Applications from the SE issuer (third party). The third party refers the customer to the issuing bank.

Step 2: Subscription to MCP application

- **Process 3:** The customer subscribes to a MCP application with the issuing bank.
 - Use case 1 – The customer subscribes to a first MCP application from a given issuing bank for a given Secure Element.
 - Use case 2 – The customer subscribes to the addition of a new MCP application to the Secure Element from the same issuing bank.
- **Process 4:** The customer replaces/renews the current MCP application with a new one on the same Secure Element. The issuing bank proposes to renew the customer's existing application or proposes a new one.
- **Process 5:** The issuing bank checks the eligibility of the customer with the MNO and takes appropriate action as necessary with respect to the customer.

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

Step 3: Installation of the MCP application

- **Process 6:** The issuing bank installs the MCP application on the Secure Element in the Customer's mobile phone.
- **Process 7:** The issuing bank installs the MCP application User Interface. This might involve the customer.

Step 4: Usage of the MCP application

- **Process 8:** The issuing bank checks the status of the MCP application on the Secure Element.
- **Process 9:** The issuing bank updates the MCP application (parameters).
- **Process 10:** The customer changes the Secure Element.

- **Process 11:** The customer changes mobile phone number but keeps the same Secure Element and MNO. The end user has an operational mobile-NFC service deployed and activated (or locked). This change results in a change of the end user identifier and potentially in the way to reach the mobile phone via OTA channel. The MNO notifies the other participants of the ecosystem that the customer has changed his/her mobile phone number and, in particular, the issuing bank or TSM as appropriate. All participants of the ecosystem need to update their information system with this change. The mobile equipment and the Secure Element are accessible through a new mobile phone number.
- **Process 12:** The customer changes his/her mobile equipment.
 - Use case 1: The new mobile equipment is unable to work with the Secure Element. The customer contacts the MNO's help desk.
 - Use case 2: The new mobile equipment works with the Secure Element. The MNO, once informed about the new mobile equipment (via any technical means), informs the issuing bank accordingly.
 - Use case 2a: The new mobile equipment detects the MCP application on the Secure Element and triggers the download of the MCP application User Interface by the issuing bank.
 - Use case 2b: The new mobile equipment is unable to identify the MCP application and therefore cannot download the MCP application User Interface. The customer contacts the issuing bank's help desk.
- **Process 13:** Because the Secure micro SD and the mobile equipment can be lost or stolen independently of each other, process 13 is split into two different processes: lost or stolen mobile equipment, contact MNO (process 13a) and lost or stolen Secure Element, contact SE issuer (process 13b).
 - **Process 13a:** For the mobile equipment, the customer contacts the MNO's help desk.
 - **Process 13b:** For the secure micro SD card, the customer asks the MCP issuer for reissuing the MCP application on the new secure micro SD card.

Note that it is not possible to lock the MCP application on the lost or stolen secure micro SD card.
- **Process 14:** It is split into two different processes: lost or stolen mobile equipment, contact MCP issuer (process 14a) and lost or stolen Secure Element, contact SE issuer (process 14b).
 - **Process 14a:** The customer informs the MCP issuer he/she cannot use the MCP application anymore.
 - **Process 14b:** The customer asks for a new secure micro SD card.

- **Process 15:** It is split into two different processes: Recovery of ME (process 15a) and Recovery of secure micro SD card (process 15b).
 - **Process 15a:** The customer inserts the existing secure micro SD card into the recovered ME and asks the SE issuer to reactivate (unlock) the MCP application.
 - **Process 15b:** The customer inserts the recovered secure micro SD card into the ME and asks the SE issuer to reactivate (unlock) the MCP application.
- **Process 16:** It is split into two different processes: New ME after loss/stolen (process 16a) and new secure micro SD card after loss/stolen (process 16b).
 - **Process 16a:** The customer is in contact with the MNO and the MCP issuer to reload the AAUI into the new ME.
 - **Process 16b:** The customer is in contact with the MCP issuer and the SE issuer to reload the MCP application.
- **Process 17:** Change MNO. The customer keeps his/her SE with the MCP application.
 - The customer keeps his/her ME: he/she keeps the AAUI on the mobile phone. The new entity in charge of the service management role, depending on the MNO, must register the new customer and his/her ME in its database to offer the MCP service.
 - The customer gets a new ME from the new MNO. The new entity in charge of the service management role, depending on the MNO, must register the new customer in its database to offer the MCP service and then download the AAUI on the ME.
- **Process 18:** The MNO temporarily suspends the mobile services.
- **Process 19:** Following the suspension of the mobile services, the MNO resumes the mobile services.
- **Process 20:** The issuing bank temporarily suspends the MCP service.
- **Process 21:** Following the suspension of the MCP application, the issuing bank resumes the MCP application.
- **Process 22:** The customer contacts the issuing bank's help desk.
- **Process 23a:** The customer contacts the third party helpdesk responsible for the supply of the SE.
- **Process 23b:** The customer contacts the MNO's helpdesk.

Step 5: Termination of the MCP application

- **Process 24:** The customer terminates the mobile services with the MNO.
- **Process 25:** The MNO terminates the customer's mobile services.
- **Process 26:** The customer requests the termination of the MCP application.
- **Process 27:** The issuing bank terminates the MCP application.

Note: For processes 18, 19, 23 and 24 corresponding to suspension, resume and termination, the MCP service must be terminated prior to the suspension of the MNO subscription to avoid OTA problems.

5.5 Processes overview of the MCP life cycle for scenario 3b

In this scenario, the Secure Element is a secure micro SD card in a mobile handset which is provided by the MCP issuer who is also responsible for the issuance and life cycle management of the MCP application. Figure 14 provides an overview of all the processes for this scenario.

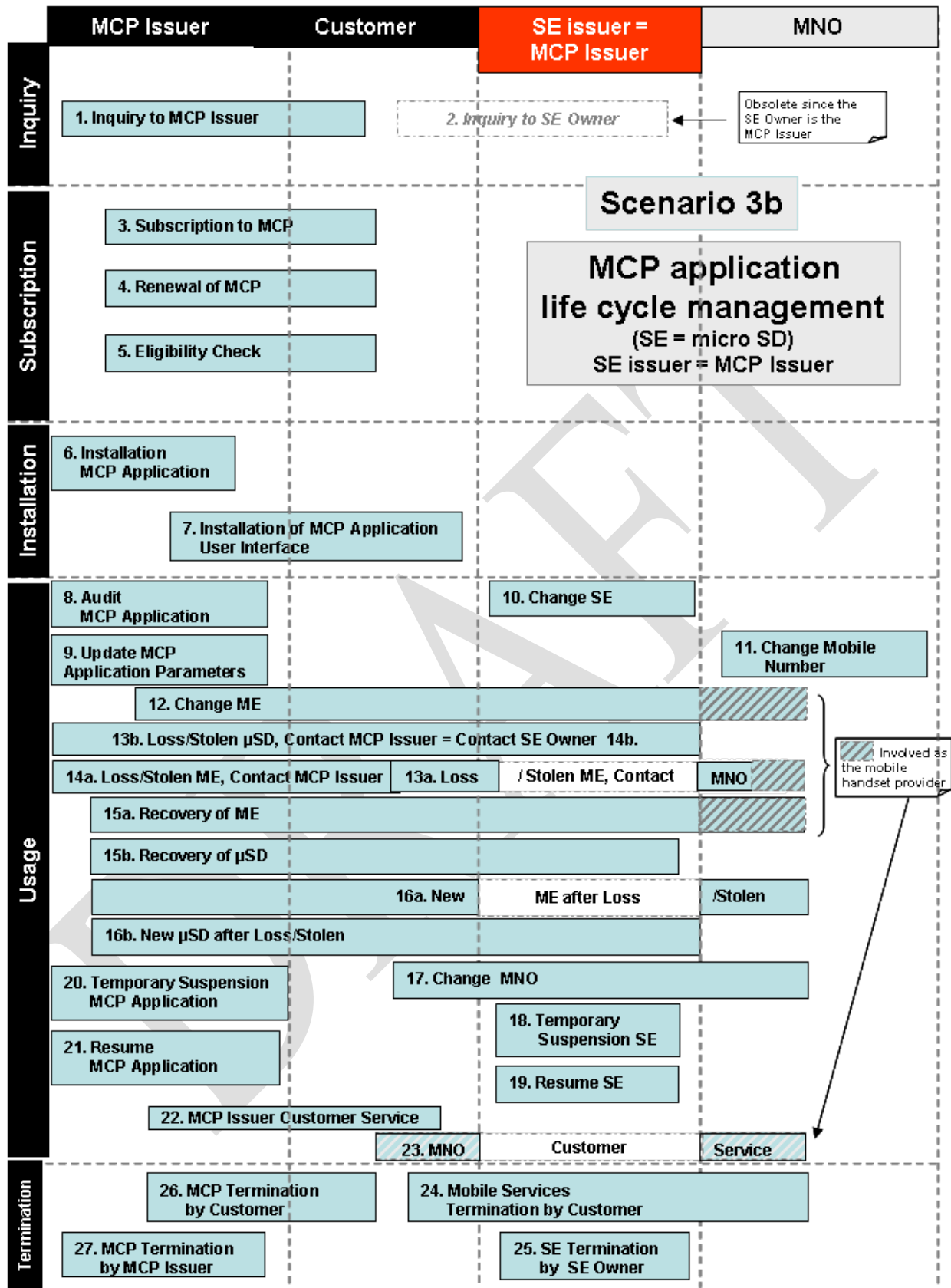


Figure 14: MCP life cycle overview for scenario 3b

Step 1: Customer Inquiry

The customer discovers the MCP services, typical examples are:

- **Process 1:** The customer requests information regarding MCP Services/Applications from the issuing bank.
- **Process 2:** Obsolete since the SE issuer is the MCP issuer.

Step 2: Subscription to MCP application

- **Process 3:** The customer subscribes to a MCP application with the issuing bank.
 - Use case 1 – The customer subscribes to a first MCP application from a given issuing bank for a given Secure Element.
 - Use case 2 – The customer subscribes to the addition of a new MCP application to the Secure Element from the same issuing bank.
- **Process 4:** The customer replaces/renews the current MCP application with a new one on the same Secure Element. The issuing bank proposes to renew the customer's existing application or proposes a new one.
- **Process 5:** The issuing bank checks the eligibility of the customer with the MNO and takes appropriate action as necessary with respect to the customer.

As a result of Step 2 it is assumed that the customer is equipped with the appropriate MCP compatible mobile phone (i.e. mobile equipment + Secure Element).

Step 3: Installation of the MCP application

- **Process 6:** The issuing bank installs the MCP application on the Secure Element in the Customer's mobile phone.
- **Process 7:** The issuing bank installs the MCP application User Interface. This might involve the customer.

Step 4: Usage of the MCP application

- **Process 8:** The issuing bank checks the status of the MCP application on the Secure Element.
- **Process 9:** The issuing bank updates the MCP application (parameters).
- **Process 10:** The customer changes the Secure Element.

- **Process 11:** The customer changes mobile phone number but keeps the same Secure Element and MNO. The end user has an operational mobile-NFC service deployed and activated (or locked). This change results in a change of the end user identifier and potentially in the way to reach the mobile phone via OTA channel. The MNO notifies the other participants of the ecosystem that the customer has changed his/her mobile phone number and, in particular, the issuing bank or TSM as appropriate. All participants of the ecosystem need to update their information system with this change. The mobile equipment and the Secure Element are accessible through a new mobile phone number.
- **Process 12:** The customer changes his/her mobile equipment.
 - Use case 1: The new mobile equipment is unable to work with the Secure Element. The customer contacts the MNO's help desk.
 - Use case 2: The new mobile equipment works with the Secure Element. The MNO, once informed about the new mobile equipment (via any technical means), informs the issuing bank accordingly.
 - Use case 2a: The new mobile equipment detects the MCP application on the Secure Element and triggers the download of the MCP application User Interface by the issuing bank.
 - Use case 2b: The new mobile equipment is unable to identify the MCP application and therefore cannot download the MCP application User Interface. The customer contacts the issuing bank's help desk.
- **Process 13:** Because the Secure micro SD and the mobile equipment can be lost or stolen independently of each other, process 13 is split into two different processes: lost or stolen mobile equipment, contact MNO (process 13a) and lost or stolen Secure Element, contact SE issuer (process 13b).
 - **Process 13a:** For the mobile equipment, the customer contacts the MNO's help desk.
 - **Process 13b:** For the Secure micro SD, the customer asks the MCP issuer for reissuing the MCP application on the new secure micro SD.

Note that it is not possible to lock the MCP application on the lost or stolen secure micro SD.
- **Process 14:** It is split into two different processes: lost or stolen mobile equipment, contact MCP issuer (process 14a) and lost or stolen Secure Element, contact SE issuer (process 14b).
 - **Process 14a:** The customer informs the MCP issuer that he/she cannot use the MCP application anymore
 - **Process 14b:** The customer asks for a new secure micro SD card.

In that case, process 14b and 13b are identical because the SE issuer is the MCP issuer.

- **Process 15:** It is split into two different processes: recovery of ME (process 15a) and recovery of secure micro SD (process 15b).
 -
 - **Process 15a:** The customer inserts the existing secure micro SD card into the recovered ME and asks the SE issuer to reactivate (unlock) the MCP application.
 - **Process 15b:** The customer inserts the recovered secure micro SD card into the ME and asks the SE issuer to reactivate (unlock) the MCP application.
- **Process 16:** It is split into two different processes: New ME after loss/stolen (process 16a) and new secure micro SD card after loss/stolen (process 16b).
 - **Process 16a:** The customer is in contact with the MNO and the MCP issuer to reload the AAUI into the new ME
 - **Process 16b:** The customer is in contact with the MCP issuer and the SE issuer to reload the MCP application.
- **Process 17:** Change MNO. The customer keeps his/her SE with the MCP application.
 - the customer keeps his/her ME : he/she keeps the AAUI on the mobile phone - The new entity in charge of the Service Management Role, depending on the MNO, must register the new customer and his/her ME in its database to offer the MCP service.
 - the customer receives a new ME from the new MNO. The new entity in charge of the Service Management Role, depending on the MNO, must register the new customer in its database to offer the MCP service and then download the AAUI on the ME.
- **Process 18:** The MNO temporarily suspends the mobile services.
- **Process 19:** Following the suspension of the mobile services, the MNO resumes the mobile 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 customer contacts the issuing bank's help desk.
- **Process 23:** The customer contacts the MNO's help desk.

Step 5: Termination of the MCP application

- **Process 24:** The customer terminates the mobile services with the MNO.
- **Process 25:** The MNO terminates the customer's mobile services.

- **Process 26:** The customer requests the termination of the MCP application.
- **Process 27:** The MCP issuer terminates the MCP application.

Note: For Processes 18, 19, 23 and 24 corresponding to Suspension, Resume and Termination, the MCP service must be terminated prior to the suspension of the MNO subscription to avoid OTA problems.

DRAFT

6 Mobile Contactless Payment Application

This section aims to provide a high level overview of the different transaction flows involved in Mobile Contactless Payments. This includes on-line and off-line payments and the optional execution of a Cardholder Verification Method (CVM) (off-line or on-line). Section 6.1 provides details on the CVM with the introduction of the mobile code as the off-line CVM. With the taps described in section 6.2, an MCP application authentication/authorisation is executed according to the corresponding card authentication/authorisation specifications in [EPC1, sections 4.3.2.5 and 4.3.2.7]. An MCP application risk management is treated in section 6.3, and examples of use cases may be found in Annex 9.1. Finally a number of additional features are handled in section 6.4.

6.1 Cardholder Verification Methods

6.1.1 Introduction

The mobile environment offers also a number of additional features which can be exploited for mobile contactless card payments with respect to Cardholder Verification Methods (CVMs) compared to contactless card payments using "physical" plastic chip cards. In the latter case, for security reasons, any CVM (such as "off-line PIN") requiring off-line verification using the contactless interface is not allowed at the Point of Interaction (POI) (see [EPC1]). With mobile payments, certain features of the mobile phone such as the keyboard could be used in the CVM process. The mobile phone is a "personal" device which is considered to be less vulnerable to certain types of physical attacks than a "public" terminal. However, their overall threats are becoming similar as the ones to personal computers including e.g. malware, phishing, etc..

As with other contactless card payments, also in the mobile environment, a distinction between on-line and off-line transactions needs to be considered leading to the following combinations which are represented in the table below.

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

Table 5: Transaction types and CVMs

The usage of a CVM is mostly linked to the transaction risk management and is currently for contactless card payments at the discretion of the card payment application issuer or underlying Card Scheme. Typically, only high value transactions require the usage of a CVM. For mobile contactless payments, other factors, such as the customer choice, may influence the usage of a CVM (see for instance section 6.1.2.5).

Note: In the sequel 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).

6.1.2 Single Tap: analysis of CVMs

With this payment method, the customer performs a so-called "single" Tap with his/her mobile phone to conduct the MCP transaction. The following steps are executed between the mobile phone and the POI:

1. Technology selection (see [EPCI] 4.3.2.2) (contactless card payment).
2. Application selection (see [EPCI] 4.3.2.3) (MCP application).
3. MCP data retrieval (see [EPCI] 4.3.2.4).

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

6.1.2.1 On-line transactions - no CVM

This payment method is typically intended for low value payments.

The following steps will take place after the risk analysis:

4. On-line MCP application authentication/authorisation (see [EPCI] 4.3.2.5.1).
5. Transaction completion (see [EPCI] 4.3.2.10).

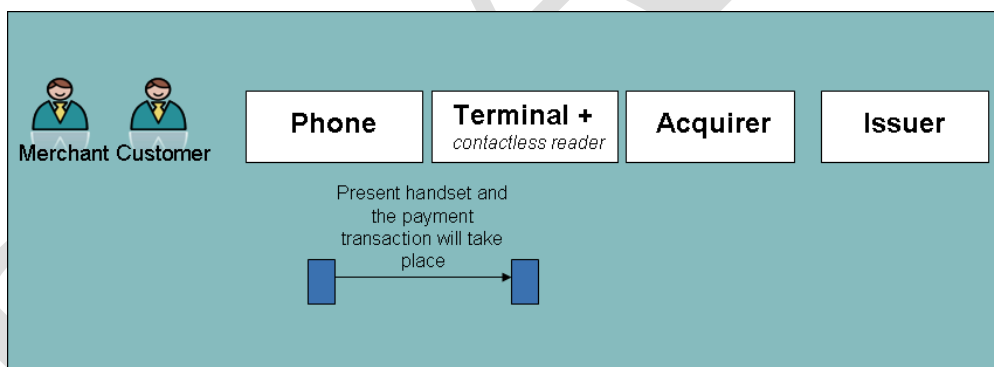


Figure 15: On-line transaction - no CVM

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 phone and the POI for the data transfer between the mobile phone and the POI. With the completion in step 5, the dedicated response message will not be transferred to the MCP application in the mobile phone.

6.1.2.2 On-line transactions - on-line CVM

In this case, the POI will request the customer to enter his/her PIN on the POI. The PIN used is the "classical" PIN code associated with the "card" application.

The following steps will be executed after the risk analysis:

4. On-line MCP application authentication/authorisation (see [EPCI] 4.3.2.5).
5. On-line cardholder verification with PIN entry at POI (see [EPCI] 4.3.2.6.1B).
6. Transaction completion (see [EPCI] 4.3.2.10).

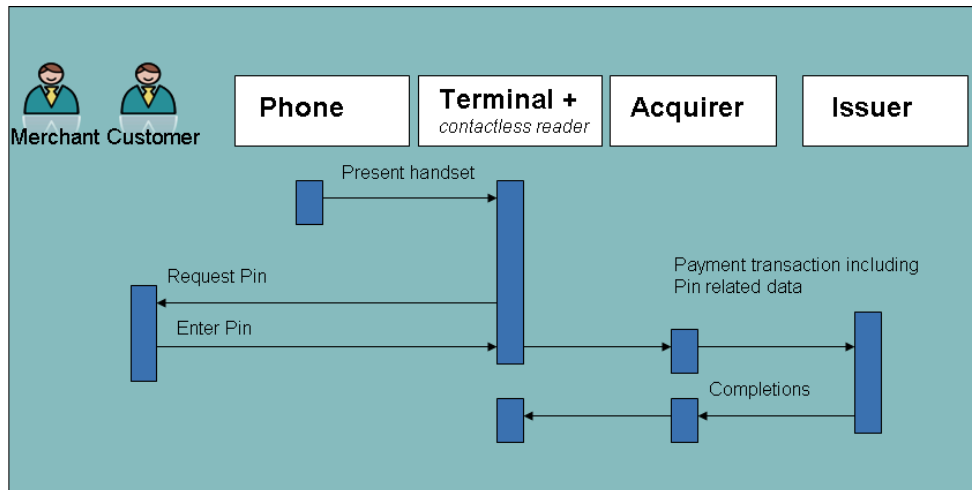


Figure 16: On-line transaction - on-line CVM

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 phone and the POI for the data transfer between the mobile phone and the POI. With the completion in step 5, the dedicated response message will not be transferred to the MCP application in the mobile phone.

6.1.2.3 On-line transactions - off-line CVM

In this case, an off-line CVM is used which is entered by the customer via the keyboard of the mobile phone. For security reasons, this CVM is a dedicated mobile code (also referred to as mobile PIN, mobile passcode, etc.) which differs from the "classic" card PIN. The verification of this mobile code is executed through the MCP application in the SE.

In the case of a single Tap, this mobile code is entered before the Tap. In this way, the result of the mobile code verification shall be transferred in the on-line authentication/authorisation message to the issuing bank via the POI through the Tap.

The following steps are executed with the payment transaction:

0. Off-line cardholder verification with mobile code entry on mobile phone (see [EPCI] 4.3.3.8).
1. Technology selection (see [EPCI] 4.3.2.2) (contactless card payment).
2. Application selection (see [EPCI] 4.3.2.3) (MCP application).
3. MCP data retrieval (see [EPCI] 4.3.2.4).
4. On-line MCP application authentication/authorisation (see [EPCI] 4.3.2.5.1).
5. Transaction completion (see [EPCI] 4.3.2.10).

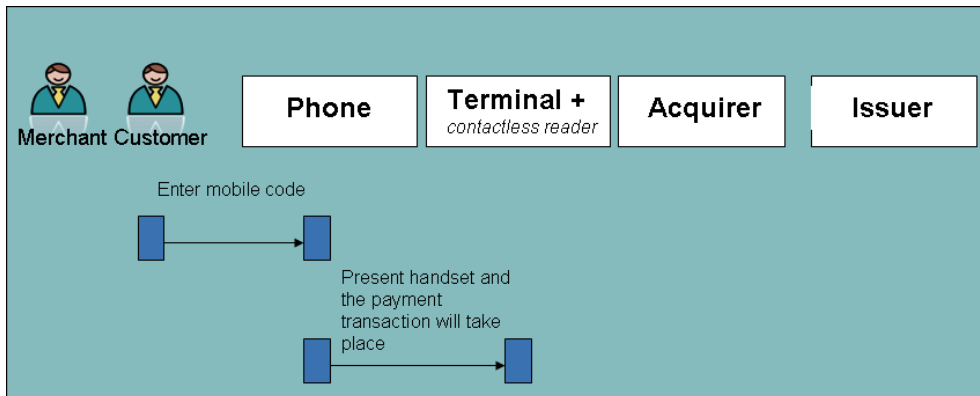


Figure 17: On-line transaction - off-line CVM

Again, with the completion in step 5, the dedicated response message will not be transferred to the MCP application in the mobile phone.

6.1.2.4 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:

4. Off-line MCP application authentication/authorisation (see [\[EPC1\] 4.3.2.5.2](#)).
5. Transaction completion (see [\[EPC1\] 4.3.2.10](#)).

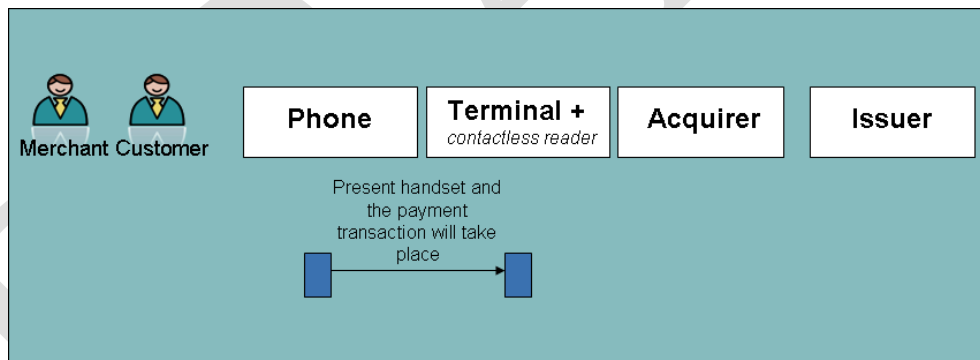


Figure 18: Off-line transaction - no CVM

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 phone and the POI for the data transfer between the mobile phone and the POI.

6.1.2.5 Off-line transactions - off-line CVM

Similar to 6.1.2.3, an off-line CVM is used which is entered by the customer via the keyboard of the mobile phone. This CVM is again a dedicated mobile code for which the verification is executed through the MCP application in the SE.

In the case of a "single" Tap, this mobile code is entered before the Tap such that the result of the mobile code verification can be transferred to the POI with the Tap.

The following steps are executed with the payment transaction:

0. Off-line cardholder verification with mobile code entry on mobile phone (see [EPCI] 4.4.3.3.8).
1. Technology selection (see [EPCI] 4.3.2.2) (contactless card payment).
2. Application selection (see [EPCI] 4.3.2.3) (MCP application).
3. MCP data retrieval (see [EPCI] 4.3.2.4).
4. Off-line MCP application authentication/authorisation (see [EPCI] 4.3.2.5.2).
5. Transaction completion (see [EPCI] 4.3.2.10).

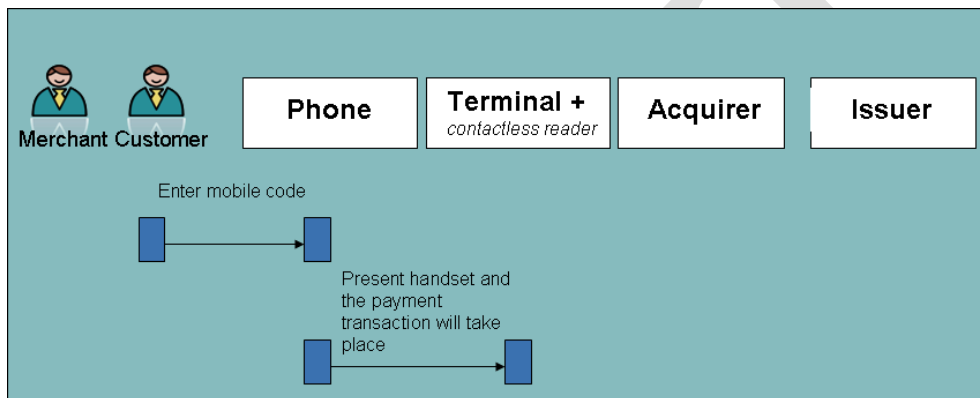


Figure 19: Off-line transaction - off-line CVM

6.1.3 Double Tap: Analysis of CVMs

6.1.3.1 On-line transactions - off-line CVM

In this case an off-line CVM is used which is entered by the customer via the keyboard of the mobile phone. For security reasons, this CVM is a dedicated mobile code (also referred to as mobile PIN, mobile passcode, etc.) which differs from the "classic" card PIN. The verification of this mobile code is executed through the MCP application in the SE.

In the case of a double Tap, this mobile code is entered after the 1st Tap and the result of the mobile code verification is transferred in the on-line authentication/authorisation message to issuing bank via the POI through the 2nd Tap.

The following steps will be executed after the risk analysis.

4. Confirmation of payment details, received from the POI, by the customer via the off-line cardholder verification with mobile code entry on mobile phone (see [EPCI] 4.4.3.3.8).
5. On-line MCP application authentication/authorisation (see [EPCI] [1] 4.3.2.5.1).
6. Transaction completion (see [EPCI] 4.3.2.10).

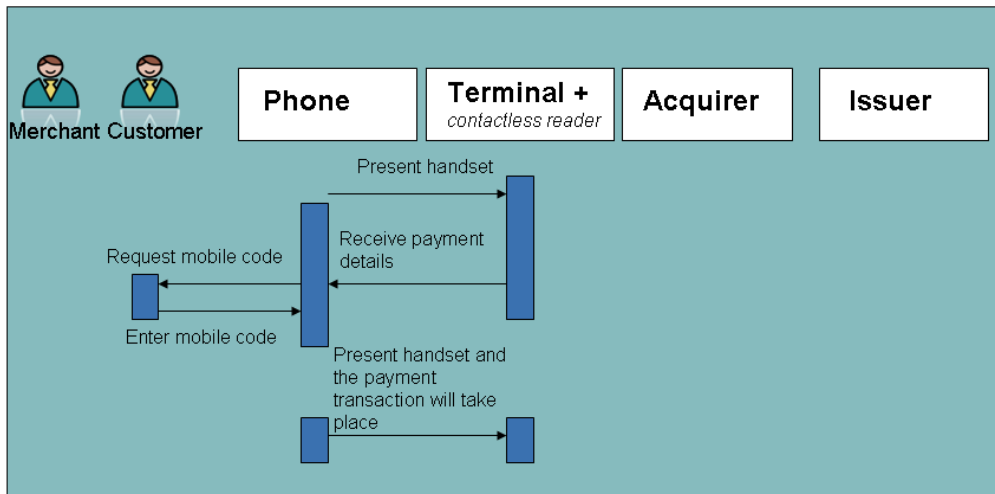


Figure 20: On-line transaction - off-line CVM

Again, with the completion of step 5, the dedicated message will not be transferred to the MCP application in the mobile phone.

6.1.3.2 Off-line transactions - off-line CVM

As in 6.1.3.1, an off-line CVM is used which is entered by the customer via the keyboard of the mobile phone. This CVM is again a dedicated mobile code for which the verification is executed through the MCP application in the SE.

In the case of a double Tap, this mobile code is entered after the 1st Tap and the result of the mobile code 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:

4. Confirmation of payment details received from the POI by the customer via the off-line cardholder verification with mobile code entry on mobile phone (see [\[EPCI\] 4.4.3.3.8](#)).
5. Off-line MCP application authentication/authorisation (see [\[EPCI\] 4.3.2.5.2, 4.3.2.7.2](#)).
6. Transaction completion (see [\[EPCI\] 4.3.2.10](#)).

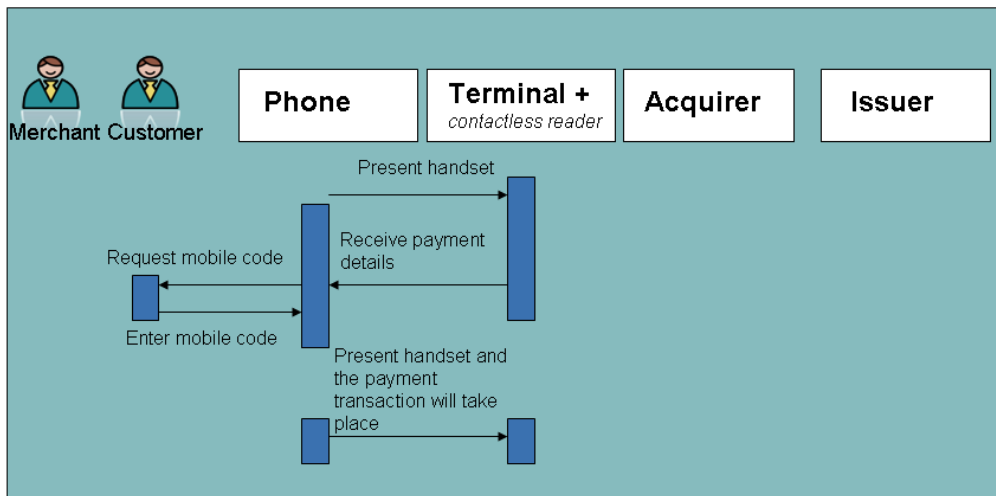


Figure 21: Off-line transaction - off-line CVM

6.1.3.3 Additional remarks

If the result of the completion of the transactions needs to be transmitted to the mobile phone, an additional Tap would be required or, alternatively, the mobile phone needs to be kept on the POI.

The same is valid for any life cycle management (e.g. risk management parameters) executed via script processing from the MCP issuer to the MCP application.

Optionally, the customer might decide to always use a mobile code before the 1st Tap if supported by the MCP issuer.

Note that the mobile code could be replaced by other off-line CVMs such as biometric verification.

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

6.2 MCP transaction

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

CVM	TRANSACTION ⁴			
	Off-line		On-line	
	Single Tap	Double Tap	Single Tap	Double Tap
On-line CVM (PIN on the POI)	-	-	X	-
Off-line CVM (Mobile Code on the Mobile Phone)	X ⁽¹⁾	X ⁽²⁾	X ⁽¹⁾	X ⁽²⁾
No CVM	X	-	X	-

⁽¹⁾ prior to Tap
⁽²⁾ between 2 Taps

Table 6: Overview matrix transaction types versus CVM usage

6.2.1 Single Tap - off-line transaction flow - no CVM (optionally off-line CVM)

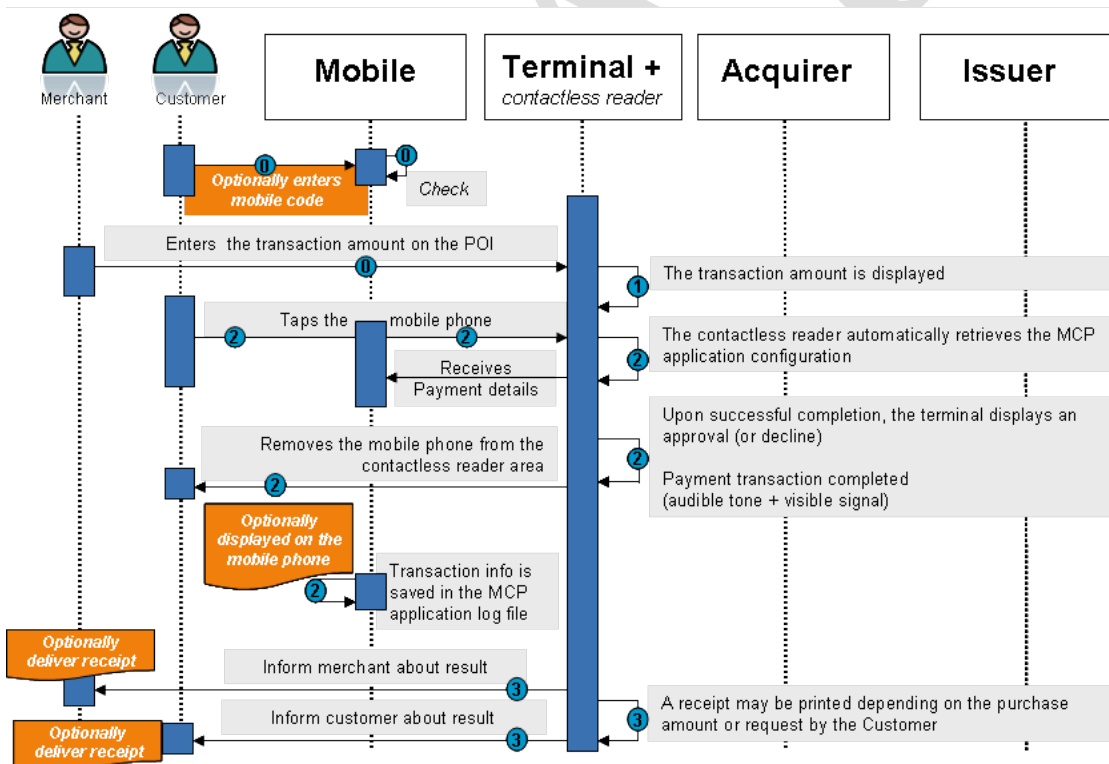


Figure 22: Single Tap - off-line transaction flow - no CVM (optionally off-line CVM)

⁴ Rows 1 and 2 apply for transactions requiring the presentation of a CVM as a result of the risk management. (See 6.3). Row 2 in addition applies in case a customer decides to pre-emptively enter his/her off-line CVM (mobile code).

Step 0 (Pre-requisite)

- As an option, the customer enters his/her mobile code to “open” the MCP application before starting the transaction (known as manual mode).
- Otherwise, the MCP application is selected without any mobile code entry (known as automatic mode).
- The merchant enters the transaction amount on the POI terminal.

Step 1

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

Step 2

- The customer taps his/her mobile phone on the contactless reader area. (The customer holds his/her mobile phone close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI selects the contactless technology.
- The POI checks the available applications and selects the appropriate MCP application through the PPSE.
- The contactless reader automatically retrieves the MCP application configuration including the CVM list (No CVM in this scenario).
- The contactless reader transmits all transaction information to the merchant’s POI terminal.
- 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 MCP application authentication/authorisation is performed by the POI.
- After processing the off-line authorisation, the merchant’s POI terminal displays an approval or decline.
- Information about the current transaction (e.g. transaction amount) is saved in the MCP application log file and optionally displayed on the mobile phone.

Step 3

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

6.2.2 Single Tap - on-line transaction flow – no CVM

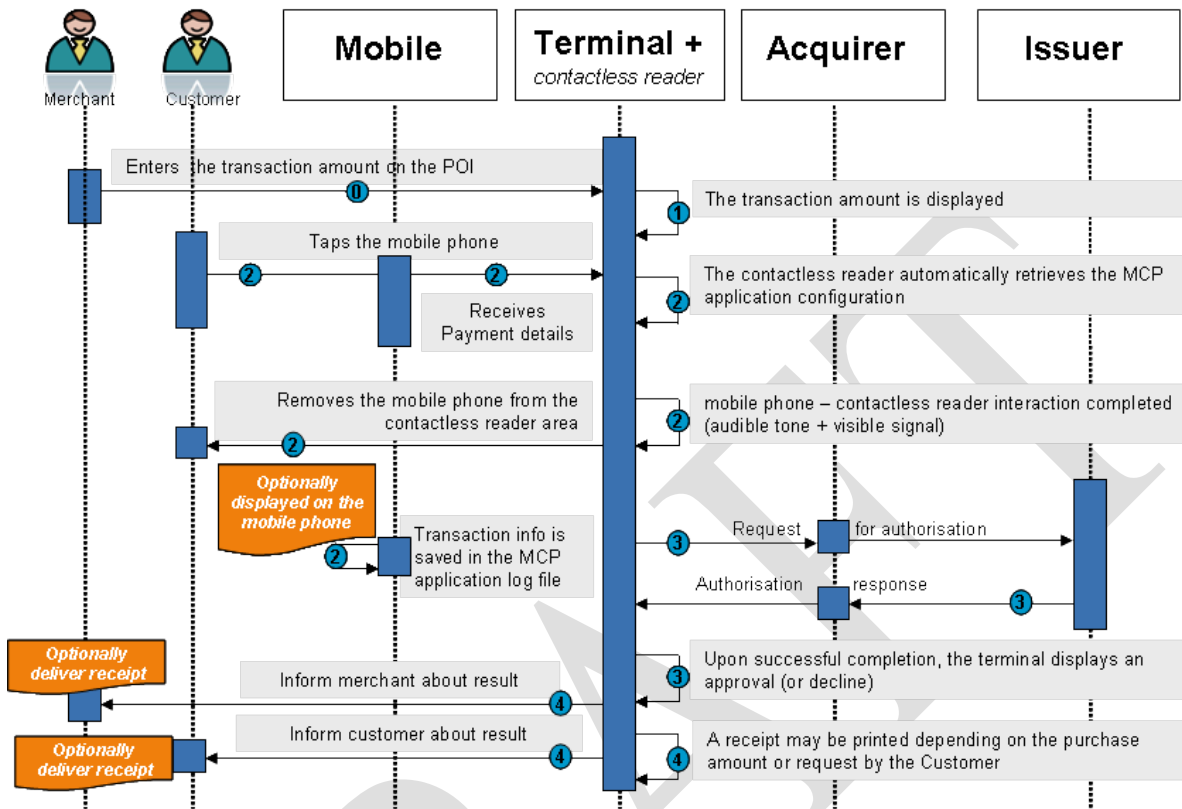


Figure 23: Single Tap - on-line transaction flow – no CVM

Step 0 (Pre-requisite)

- The merchant enters the transaction amount on the POI terminal.

Step 1

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

Step 2

- The customer taps his/her mobile phone on the contactless reader area. (The customer holds his/her mobile phone close to the contactless reader area until audible tone and/or visible signal take place).
- The POI selects the contactless technology.
- The POI checks the available applications and selects the appropriate MCP application through the PPSE.
- The contactless reader automatically retrieves the MCP application configuration including the CVM list (No CVM in this scenario).

- An audible tone and/or visible signal then 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.
- An off-line MCP application authentication is optionally performed by the POI.
- An on-line MCP application authorisation is performed by the POI.
- The customer then removes his/her mobile phone from the contactless reader area.
- Information about the current transaction (e.g. on-line transaction requested for transaction amount) is saved in the MCP application log file and optionally displayed on the mobile phone.
- The contactless reader transmits all transaction information to the merchant's POI terminal.

Step 3

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

Step 4

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

6.2.3 Double Tap - off-line transaction flow – off-line CVM

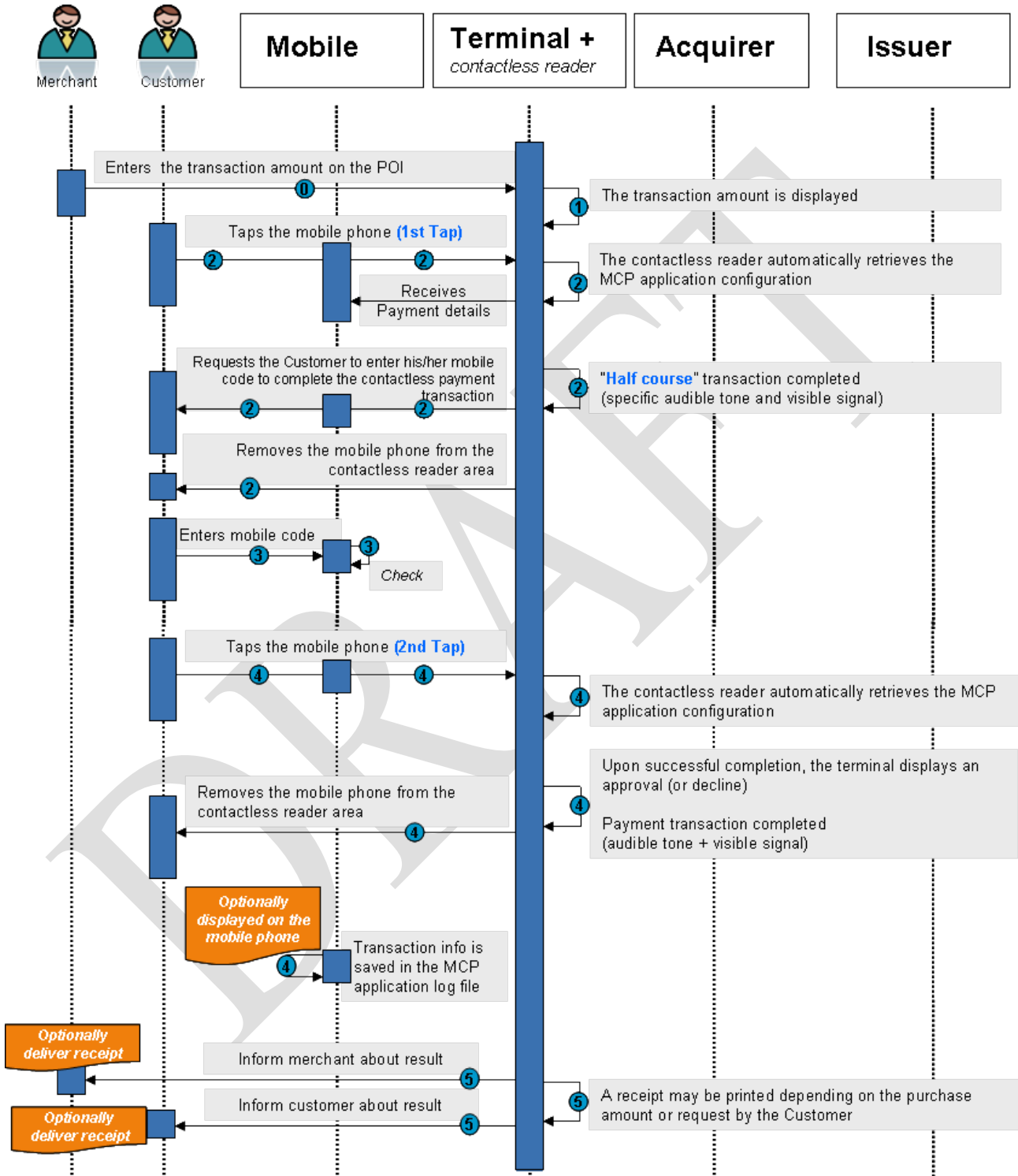


Figure 24: Double Tap - off-line transaction flow – off-line CVM

Step 0 (Pre-requisite)

- The merchant enters the transaction amount on the POI terminal.

Step 1

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

Step 2

- The customer taps (1st Tap) his/her mobile phone on the contactless reader area. (The customer holds his/her mobile phone close to the contactless reader area until audible tone and/or visible signal take place).
- The POI selects the contactless technology.
- The POI checks the available applications and selects the appropriate MCP application through the PPSE.
- The contactless reader automatically retrieves the MCP application configuration including the CVM list (off-line CVM in this scenario).
- A specific audible tone and/or visible signal indicate that "half-course" transaction is completed and that the customer is requested to enter his/her mobile code to complete the contactless payment transaction.
- The customer then removes his/her mobile phone from the contactless reader area.

Step 3

- The customer checks the purchase amount and enters his/her mobile code on the mobile phone.
- Upon successful verification of the mobile code, a message is displayed on the mobile phone requiring the customer to tap again his/her mobile phone on the contactless reader area.

Step 4

- The customer taps again (2nd Tap) his/her 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.
- An off-line MCP application authentication/authorisation is performed by the POI.
- After processing the off-line authorisation, the merchant's POI terminal displays an approval or decline message.
- Information about the current transaction (e.g. transaction amount) is saved in the MCP application log file and optionally displayed on the mobile phone.

Step 5

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

Note:

Double Tap is implementation dependent. It can be considered as a two-step transaction or two transactions, one as the initialisation transaction and one as a payment transaction.

6.2.4 Double Tap - on-line transaction flow – off-line CVM

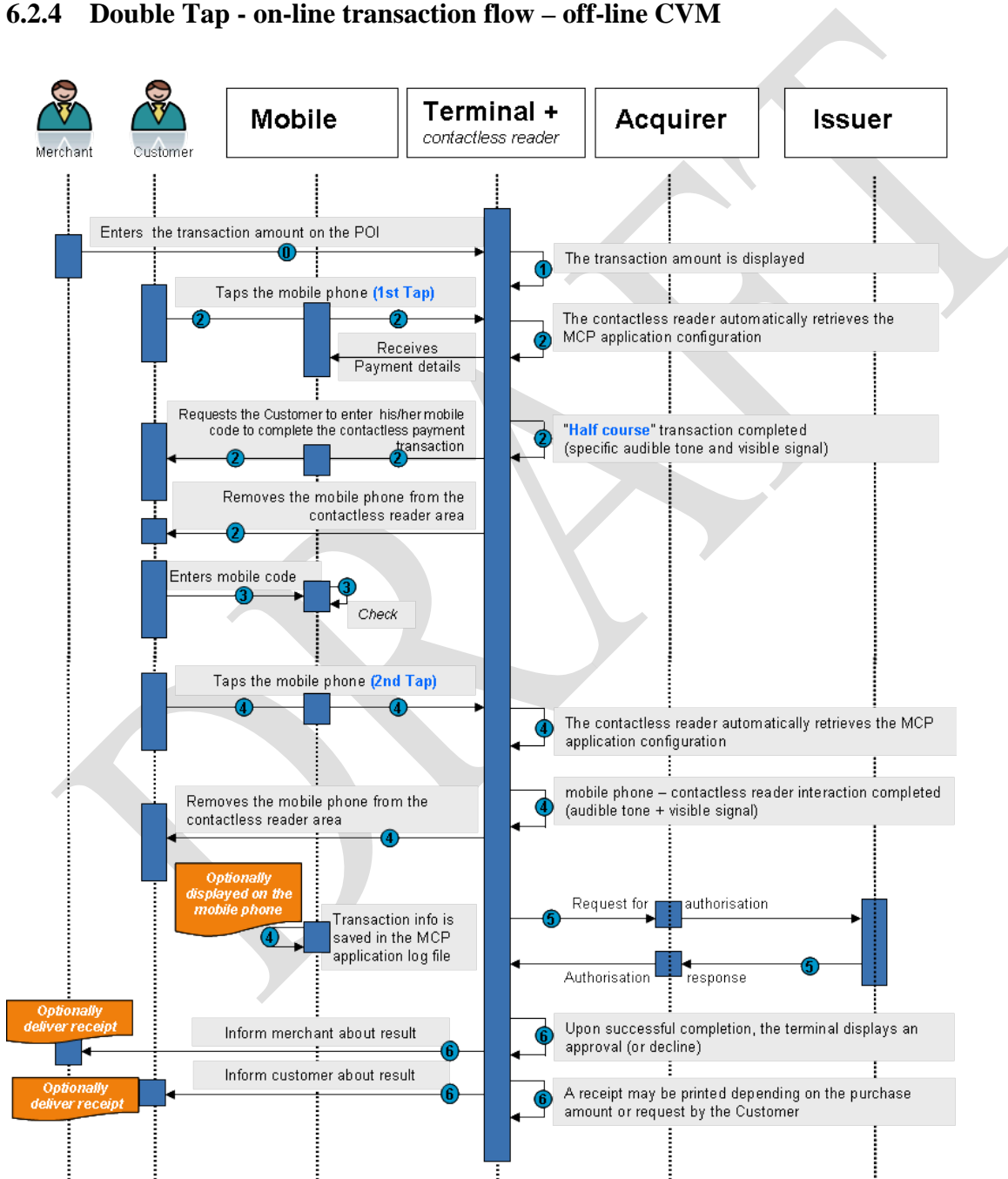


Figure 25: Double Tap - on-line transaction flow – off-line CVM

Step 0 (Pre-requisite)

- The merchant enters the transaction amount on the POI terminal.

Step 1

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

Step 2

- The customer taps (1st Tap) his/her mobile phone on the contactless reader area. (The customer holds his/her mobile phone close to the contactless reader area until the audible tone and/or visible signal occur).
- The POI selects the contactless technology.
- The POI checks the available applications and selects the appropriate MCP application through the PPSE.
- The contactless reader automatically retrieves the MCP application configuration including the CVM Method list (off-line CVM in this scenario).
- A specific audible tone and/or visible signal indicate that "half-course" transaction is completed and that the customer is requested to enter his/her mobile code to complete the contactless payment transaction.
- The customer then removes his/her mobile phone from the contactless reader area.

Step 3

- The customer checks the purchase amount and enters his/her mobile code on the mobile phone.
- Upon successful verification of the mobile code, a message is displayed on the mobile phone requiring the customer to tap again his/her mobile phone on the contactless reader area.

Step 4

- The customer taps again (2nd Tap) his/her 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.
- An off-line MCP application authentication is optionally performed by the POI.
- An on-line MCP application authorisation is performed by the POI.
- Information about the current transaction (e.g. transaction amount) is saved in the MCP application log file and optionally displayed on the mobile phone.

Step 5

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

Step 6

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

Note

Double Tap is implementation dependent. It can be considered as a two-step transaction or two separate transactions, namely an initialisation transaction followed by the payment transaction.

6.2.5 Single Tap - on-line transaction flow – on-line CVM

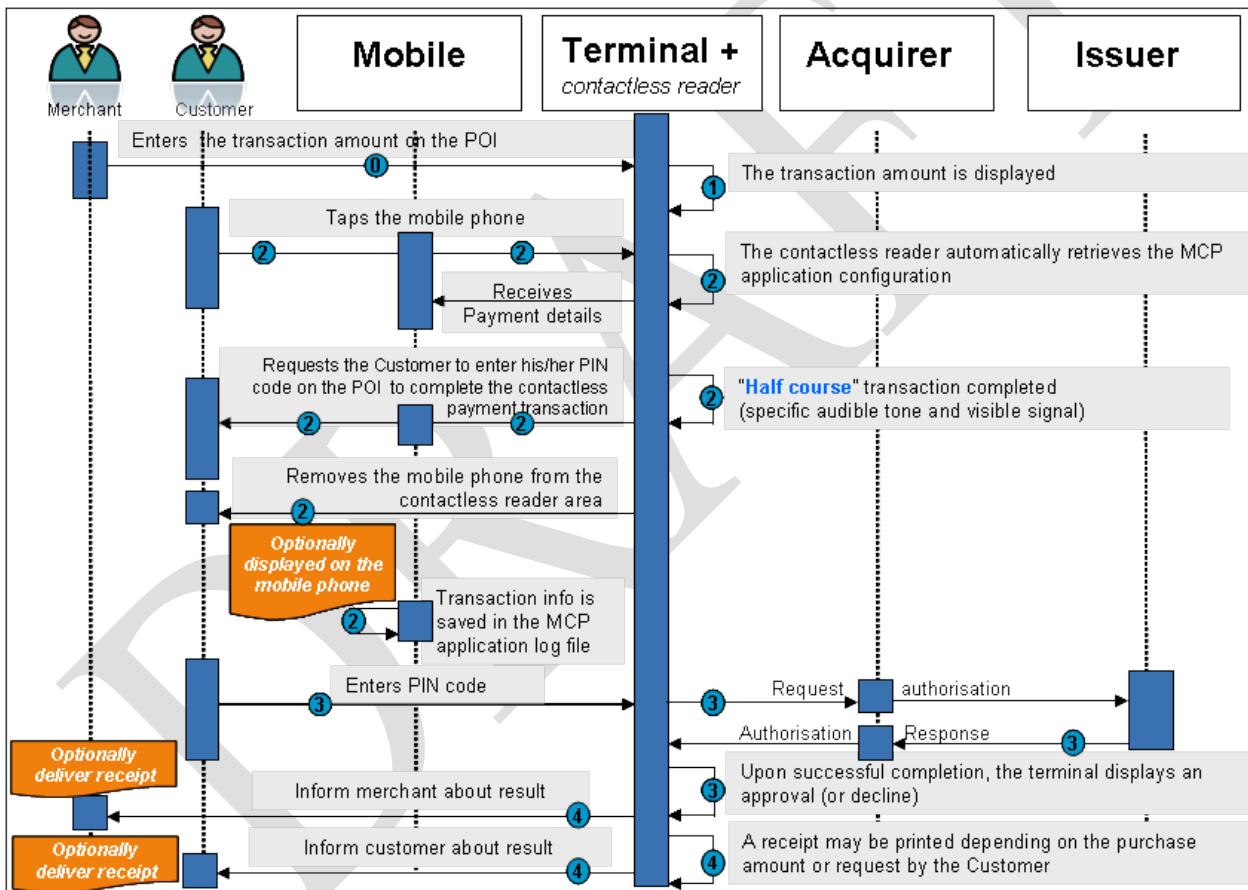


Figure 26: Single Tap - on-line transaction flow – on-line CVM

Step 0 (Pre-requisite)

- The merchant enters the transaction amount on the POI terminal.

Step 1

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

Step 2

- The customer taps his/her mobile phone on the contactless reader area. (The customer holds his/her mobile phone close to the contactless reader area until an audible tone and/or visible signal occur).
- The POI selects the contactless technology.
- The POI checks the available applications and selects the appropriate MCP application through the PPSE.
- The contactless reader automatically retrieves the MCP application configuration including the CVM list (on-line CVM in this scenario).
- A specific audible tone and/or visible signal indicate that "half-course" transaction is completed and that the customer is requested to enter his/her PIN code on the POI to complete the contactless payment transaction.
- The customer can remove his/her mobile phone from the contactless reader area.
- An off-line MCP application authentication is optionally performed by the POI.
- An on-line MCP application authorisation is performed by the POI.
- Information about the current transaction (e.g. on-line transaction requested for transaction amount) is saved in the MCP application log file and optionally displayed on the mobile phone.
- The contactless reader transmits all transaction information to the merchant's POI terminal.

Step 3

- The customer checks the purchase amount and enters his/her PIN code on the merchant's POI terminal.
- After processing the on-line authorisation, the merchant's POI terminal displays an approval or decline.

Step 4

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

6.3 Risk management

6.3.1 Introduction

The mobile environment offers a number of additional features which can be exploited for mobile contactless card payments with respect to the transaction amount compared to contactless card

payments using "physical" plastic chip cards. In particular, the mobile environment provides Cardholder Verification Methods (CVM) enabling transactions that require the usage of a CVM. CVMs for MCP are described in [EPC2]. In addition, Over the Air (OTA) is an additional channel available to the MCP issuer for managing the MCP application including the risk parameters which reduces its dependency on the POI capabilities.

As with other contactless card payments, also in the mobile environment, a distinction between on-line and off-line transactions needs to be considered from a risk management perspective. Therefore a number of risk parameters are used. These parameters are set up by the MCP issuer or the acquirer according to the underlying card scheme.

In addition, the MCP application has a set of features for risk management such as counters and limits that will be used to make the decision for a particular transaction. The purpose of this section is to present these risk management parameters for MCP. In the sequel of this document the risk parameters will be analysed and are grouped in POI risk parameters and MCP risk parameters.

6.3.2 Form Factor

Certain functions might require the identification of the type of form factor being used. Therefore the MCP applications shall have a data element indicating the form factor which could be used by the POI, the acquirer or the MCP issuer.

6.3.3 Parameters

When conducting an MCP, typically the customer presents his/her mobile phone to the Point of Interaction (POI). The following steps are then executed between the mobile phone and the POI:

1. Technology selection (see [EPC1] 4.3.2.1) (contactless card payment).
2. Application selection (see [EPC1] 4.3.2.3.1B) (MCP application).
3. MCP data retrieval (see [EPC1] 4.3.2.4.1).

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

6.3.4 Point Of Interaction Risk parameters

6.3.4.1 CVM Limit

The 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 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 CVM limit require the usage of a CVM as described in [EPC2]. This can be an on-line PIN or an off-line mobile code.

The value of the CVM Limit is set in the POI application and defined by the scheme (at country/region/global level). It must take into account the risk of fraudulent transactions (e.g. in case of loss or theft of the mobile phone), while preferably using, within a scheme, the same contactless CVM Limit, independent of the form factor. In addition, for consistent customer and merchant experience (and education), the contactless CVM Limit should ideally be the same for all Schemes in a certain geography (e.g. a country, SEPA area).

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

Transaction Amount	\leq CVM Limit	$>$ CVM Limit
CVM	Optional	Mandatory

Table 7: CVM Usage

6.3.4.2 Floor Limit

The *Floor Limit* is a parameter indicating the value of a transaction above which an on-line authorisation by the issuing bank 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 issuing bank 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 scheme rules (it may depend on different factors such as the merchant Category Code, etc., or the payment product).

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

6.3.5 MCP 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.

6.3.5.1 Mobile code Try Limit and Counter

The mobile code may be used as a CVM (see section 6.1). 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:

- 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 issuing bank 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.

6.3.5.2 Consecutive No-CVM Limit and Counter

The *Consecutive No-CVM Limit* is a parameter indicating the number of consecutive 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 mobile code verification.

The value of the *No-CVM 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 phone).
- The convenience from the customer perspective.

6.3.5.3 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 \leq Consecutive No-CVM Limit	Consecutive No-CVM Counter $>$ Consecutive No-CVM Limit
CVM	Optional	Mandatory

Table 8: CVM-based risk management

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

6.3.5.4 Cumulative Off-line Limit and Amount Accumulator

The *Cumulative Off-line Limit* is a parameter indicating the maximum total value of 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 7.6.3). This reset may be optionally confirmed by using the mobile code entered by the customer.
- Via script processing performed via the POI⁵ using NFC. This might require an additional Tap or placing the mobile phone 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 phone).
- The credit risk.
- The convenience from the customer 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.

6.3.5.5 Consecutive Off-line Limit and Counter

The *Consecutive Off-line Limit* is a parameter indicating the number of consecutive off-line transactions 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 *Consecutive Off-line Counter* 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 7.6.3). This reset may be optionally confirmed by using the mobile code entered by the customer.
- Via script processing performed via the POI⁶ using NFC. This might require an additional Tap or placing the mobile phone on the NFC interface of the POI.

⁵ Script processing via POI is currently not covered for contactless technology in [1=SEPA Cards Standardisation Volume – Book of Requirements].

⁶ Script processing via POI is currently not covered for contactless technology in [EPCI].

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 phone).
- The credit risk.
- The convenience from the customer perspective.

Note that 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.

6.3.5.6 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.

Transaction	Amount \leq Floor Limit	Cumulative Off-line Amount \leq Cumulative Off-line Limit	Consecutive Off-line Counter \leq 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

Table 9: On-line/ Off-line Risk management

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.

6.3.6 Additional Remarks

6.3.6.1 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 issuing bank risk is already limited by the maximum Floor Limit defined in 6.3.4.2.

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

- On-line authorisation request to the issuing bank; which offers the most control to the issuing bank 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 issuing bank 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 issuing bank control.

6.3.6.2 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 section.

6.3.6.3 Parameters Update

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

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

6.4 Additional features

6.4.1 Transaction Logging

Each MCP application shall have its proper 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 displayable⁷ to the consumer while the number of transactions stored in the log file remains at the discretion of the MCP issuer. For on-line transactions, not all transactions initiated are authorised by the issuing bank. Therefore the transactions log may not match with the card statement in view of the declined transactions.

Every time a contactless transaction is initiated, a new record⁸ is created and the transaction logging is updated in the MCP application. Afterwards the AAUI can retrieve the appropriate information from this log file to allow the customer to view details of the transactions initiated. The AAUI 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:

⁷ The MCP application will always have a AAUI associated with it. The log data should be extracted from the MCP application and stored within the AAUI.

⁸ 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.

- 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.

Further guidance on details for the data is provided in Annex D in [\[EMV10\]](#).

Methods of presenting the transaction history within the AAUI should be MCP issuer/application provider choice. Transactions in the logging should be able to be sorted 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. This control is performed by requesting a mobile code verification. The MCP issuer may also choose to provide the customers the ability to enable or disable this access control themselves.

6.4.2 Receipts

The transaction receipt is the payment receipt intended for the customer. The handling of transaction receipts for MCP is identical to the ones for transactions performed with physical cards. Section 4.4 of [\[EPCI\]](#) provides further guidance. For POIs capable of printing a transaction receipt, it shall provide a receipt upon the customer's request. If the POI knows in advance that it cannot print a transaction receipt, it shall inform the customer that no receipt can be printed and offer the choice to continue or abort the transaction.

As mobile equipment offers additional capabilities, receipts may also be provided via other channels (e.g. electronic receipts) which are not yet defined.

6.5 Interoperability and MCP Service availability

Some countries of the SEPA zone 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 issuing bank 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 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 customer side and maximizing the service availability.

DRAFT

7 Technical and Security Infrastructure

The infrastructure needed during the payment transaction for mobile contactless card payments fully leverages the transaction infrastructure already deployed for card payments. Mobile contactless SEPA card payments will further leverage the investments to be made for acceptance of contactless cards at POIs.

The technical and security infrastructure described below complies with the SEPA Cards Standardisation Volume Book of Requirements v5.0 [EPCI] and mobile payment documents edited by EMVCo:

- [EMV4] The mobile handsets requirements comply with EMVCo – Handset Requirements for Contactless Mobile Payment [v1.0 – June 2010].
- [EMV5] The overall MCP general architecture complies with EMVCo – Contactless Mobile Payment Architecture Overview [v1.0 – June 2010].
- [EMV7] The necessary components described to enable application activation comply with EMVCo - Application Activation User Interface – Overview, Usage Guidelines and PPSE Requirements [v1.0 – December 2010].

7.1 Overall MCP architecture

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

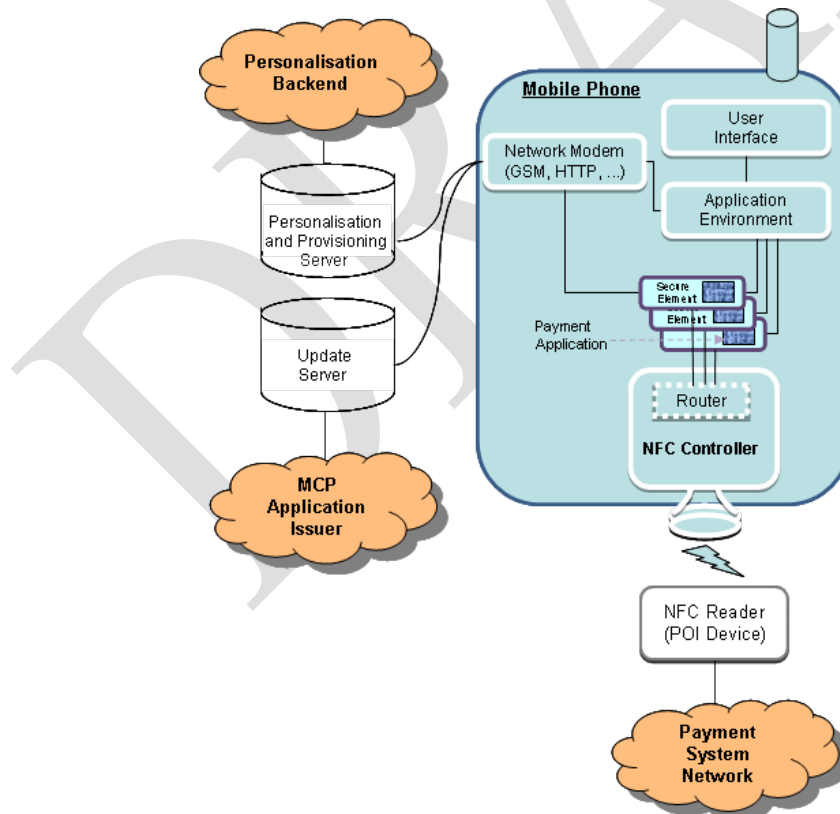


Figure 27: The MCP System Architecture

To be eligible to conduct a Mobile Contactless Payment, the mobile equipment should have the following components:

- An Application Environment in which applications may be loaded and run. This application environment may host User Interface applications which allow for communication between a MCP application and the user.
- A User Interface which displays necessary information and provides the input mechanism for user selection and payment functions.
- One (or more) Secure Element(s) which host one or more MCP applications.
- A NFC Controller which provides contactless capabilities.
- A Network Modem (standard networking protocols issued by ETSI and GSMA, or application-specific protocols built on top of standard Internet access protocols) which provides network connectivity for the Application Environment and for provisioning and personalisation of MCP application onto a Secure Element.

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

The MCP application is to be installed on a Secure Element by a personalisation and provisioning server which communicates with the Secure Element via the mobile network connection (e.g. OTA). This implies that dedicated processes need to be defined for the provisioning and management of the payment application, which may vary depending on the Secure Element form factor (UICC, embedded chip or secure micro SD). 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.

The Personalisation and Provisioning Server is connected to a personalisation backend, which allows the issuing bank to issue the MCP application to the mobile equipment.⁹

Once the MCP application is installed and provisioned, it may be updated via the Update Server. This allows application counters reset and parameters update. The Update Server also communicates with the Secure Element and the MCP application using the network connection.

7.2 Mapping of standards and specifications

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

- ISO

The International Organisation for Standards (ISO) is the world's largest developer and publisher of International Standards. ISO has different committees which specify technical standards used in mobile payments such as standards for integrated circuit cards,

⁹ The MCP application might also be preloaded on the Secure Element prior to its issuance.

communication protocols such as NFC, security mechanisms and is also involved with mobile payments in ISO TC68.

List of relevant ISO documents:

- ISO/IEC 18092 Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1) [\[ISO1\]](#).
- ISO/IEC 14443-3:2001: Identification cards - Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialisation and anti-collision [\[ISO2\]](#).
- ISO/IEC 14443-4:2001: Identification cards - Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol [\[ISO3\]](#).
- ISO/IEC 7816-4 Identification cards — Integrated circuit cards — Part 4: Organisation, security and commands for interchange [\[ISO4\]](#).

- 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.

List of relevant ETSI documents:

- ETSI TS 102 588, Technical Specification Smart Cards; Application invocation Application Programming Interface (API) by a UICC Web Server for Java Card Platform. [\[ETS11\]](#).
- ETSI TS 102 622, Smart Cards; UICC – Contactless Front-end (CLF) interface; Host Controller Interface (HCI). [\[ETS12\]](#).
- ETSI TS 102 613, Smart Cards; UICC-CLF Interface; Physical and Data Link Layer Characteristics. [\[ETS13\]](#).

- EMVCo

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

List of relevant EMV documents¹⁰ :

- EMV Mobile Contactless Payment Technical Issues and Position Paper, v1.0. [\[EMV1\]](#).
- The Role and Scope of EMVCo in Standardising the Mobile Payments Infrastructure (White Paper), v1.0 [\[EMV2\]](#).
- EMV Contactless Communication Protocol Specification, v2.0.1 [\[EMV3\]](#).
- EMV Handset Requirements for Contactless Mobile Payment, v1.0 [\[EMV4\]](#).

¹⁰ Some EMV documents may have a restricted access.

- EMV Contactless Mobile Payment Architecture Overview, v1.0 [\[EMV5\]](#).
 - EMV Contactless Mobile Payment - EMV Profiles of GlobalPlatform UICC Configuration, v1.0 [\[EMV6\]](#).
 - EMV Contactless Mobile Payment - Application Activation User Interface - Overview, Usage Guidelines and PPSE Requirements, v1.0 [\[EMV7\]](#).
 - Book A, EMV Contactless Specifications for Payment Systems, Architecture & General Remarks, v2.1 [\[EMV8\]](#).
 - Book B, EMV Contactless Specifications for Payment Systems, Entry Point Specification, v2.1 [\[EMV9\]](#).
 - Integrated Circuit Card Specifications for Payment Systems Book 3 Application Specification, v4.2 [\[EMV10\]](#).
- GlobalPlatform

GlobalPlatform (GP) is the leading international association focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-business model implementations, which delivers benefits to issuing banks, service providers and technology providers.

List of relevant GlobalPlatform documents¹¹:

- Card specification, v 2.2.1 [\[GP1\]](#).
 - Confidential Card Content Management – Card Specification, v2.2 – Amendment A, v1.0; [\[GP2\]](#).
 - UICC Configuration, v1.0.1 - Card Specification, v2.2 [\[GP3\]](#).
 - Messaging Specification for Mobile NFC Services, v1.0 [\[GP4\]](#).
 - Contactless Services, v1.0 – Card Specification, v2.2 – Amendment C, v1.0 [\[GP5\]](#).
 - Proposition for NFC Mobile: Secure Element Management and Messaging [\[GP6\]](#).
 - GlobalPlatform Card – Composition Model, v0.0.106 [\[GP7\]](#).
- 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 mobile handset manufacturers, 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.

List of relevant GSMA documents:

- Requirements for Single Wire Protocol NFC Handsets, v2.0 - Nov 2008 [\[GSMA1\]](#).
- Mobile NFC Services White Paper (Feb 2007) [\[GSMA2\]](#).

¹¹ Some GP documents may have a restricted access.

- NFC Technical Guidelines, v2 White Paper (Nov 2007) [GSMA3].
- Pay-Buy-Mobile Business Opportunity Analysis Public White Paper (Nov 2007) [GSMA4].

- Mobey Forum

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

List of available Mobey Forum documents:

- White Paper - Alternatives for Banks to offer Secure Mobile Payments, v1.0 [MF1].

- NFC Forum

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

Figure 28 aims to synthesise which specification is relevant for each brick of architecture, e.g. mobile equipment, Secure Element, user application interface (AAUI), NFC controller, payment card and TSM.

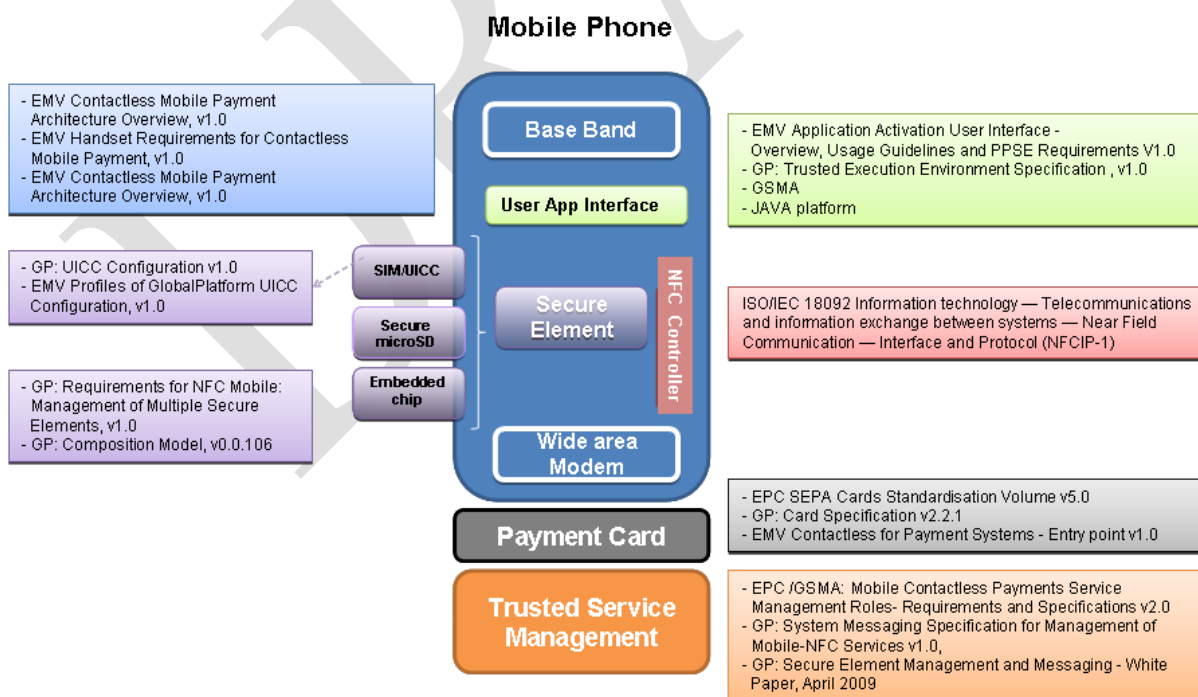


Figure 28: Mapping of standards

7.3 Mobile equipment

7.3.1 Introduction

The mobile equipment allows contactless communications by using NFC protocol (compliant with ISO14443 type A and B) with the means of a dedicated NFC controller embedded into the mobile equipment.

The NFC controller should be used in emulation mode to emulate a contactless card.

Figure 17 shows a mobile equipment architecture with alternative options for Secure Elements, and the interfaces which may be used between the internal components. The Application Environment, User Interface and the network modem described in Figure 16 are implemented by the Baseband and Application Processor.

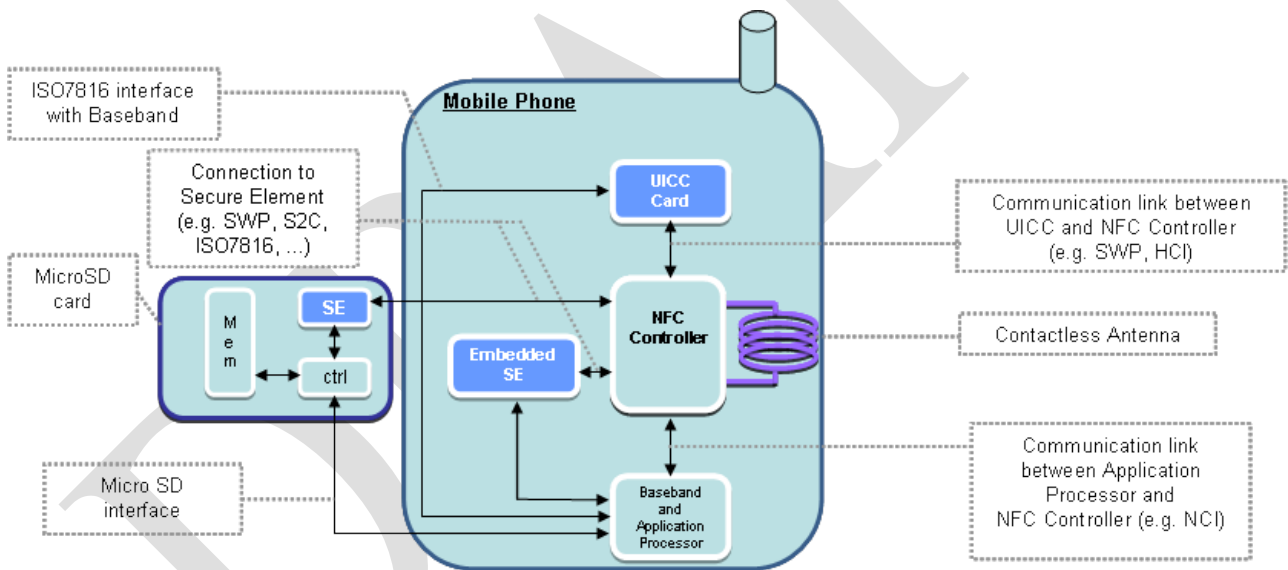


Figure 29: Mobile equipment architecture

Note:

Figure 29 is covering all three Secure Elements types, but only one is active as an SE in the sequel to the document.

The following requirements apply:

- Access to a Secure Element by mobile applications shall be limited to authorised mobile applications only.

- An authorised MCP application shall be able to interact with a Secure Element, i.e. an authorised mobile application must be able to address communication to any application on a Secure Element.
- An authorised MCP application shall be able to manage the accessibility state of the Secure Element (active or inactive) to the contactless interface (see chapter 7.3.2).

If a Secure Element is in the inactive state, communication received over the contactless interface shall not be routed to the Secure Element. An authorised MCP application shall still be able to route communication to the inactive Secure Element.

If a Secure Element is in the active state, communication received over the contactless interface shall be routed to the Secure Element.

7.3.2 Application Activation User Interface (AAUI)

The MCP application User Interface is dedicated to the management of the interaction with the customer, in connection with the MCP application located on the Secure Element.

This section elaborates on aspects of the MCP application User Interface, namely, representation, accessibility, presence of indicators showing the status of applications and how the AAUI is loaded into the mobile equipment. Finally, we illustrate with an example of a possible implementation.

7.3.2.1 Representation of the MCP application

The AAUI application should present information in an intuitive manner that is clearly recognisable and understandable to a typical consumer. When listing multiple applications, the list should be in the order chosen by the consumer. Each 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 unique dedicated Bank AAUI. An AAUI is then to be installed into the mobile equipment by the Bank AAUI Manager.

This AAUI is defined, developed and maintained under the responsibility of the MCP issuer. It should make use of the graphical capabilities of mobile equipment to display a specific bank graphical interface, including the issuing bank's logo.

Each application listed should contain the following:

- List the contactless applications related to the user interface application if there are more than one.
- Allow the customer to order the contactless applications within that list according to the consumers own preferences.
- Allow the consumer to prioritise the order in which a contactless terminal 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.¹²

7.3.2.2 Accessibility

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

- Deactivation without mobile code¹³.
- Activation with mobile code.

An example of a use case is when a customer wants to lend his/her mobile phone to somebody but he does not want to allow MCP application.

Note that the payment service shall not be available when the mobile equipment is turned off, nor when the mobile equipment battery level does not allow displaying the Bank GUI (battery low state).

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 a MCP transaction.

The POI application shall support application selection through the Proximity Payment System Environment (PPSE – see section 7.5.2).

A POI supporting MCPs shall be able:

- To identify cases where an off-line mobile code can be used (i.e. the customer uses an MCP application on the mobile phone).
- And to verify that the mobile code entry has been successfully performed.

¹² If the mobile equipment has the capability to support multiple Secure Elements and the AAUI is capable of managing the possibility of multiple contactless applications residing on these multiple Secure Elements, the Consumer could be provided with an indication as to which Secure Element each contactless application resides upon.

¹³ For security reasons, the Customer's authentication code denoted as "Mobile Code" shall not be the same as the card PIN used for conducting contact-based card payment transactions.

7.4.1 Transaction initialisation

For MCP transactions, the amount shall be available to the POI application at Transaction Initialisation.

The transaction shall be initiated (i.e. Card Service selection, amount availability and activation of the contactless reader) before presenting the mobile phone to the contactless reader of the POI.

7.4.2 Technology selection

The contactless chip processing shall be supported to perform a mobile contactless payment.

If a mobile phone is presented to the contactless reader of the POI and the reader has been activated during the Transaction Initialisation phase, the POI Application shall recognise this and shall initiate MCP application processing.

7.4.3 Application Selection

For MCP transactions, Application Selection shall follow the SEPA Card Standardisation Volumes [\[EPCI\]](#).

7.4.4 Card Authentication

The contactless POI Application shall support the off-line Card Authentication method as defined in [\[EPCI\]](#) when it is configured to perform off-line transactions. When the contactless POI application is configured to perform on-line only transactions, off-line Card Authentication¹⁴ is at the discretion of the Card Scheme.

7.4.5 Cardholder Verification

If the POI supports MCP, the POI application shall support mobile code management, i.e. the POI application user interface shall present a message inviting the customer to check the mobile phone and to follow up the instructions displayed¹⁵.

7.4.6 Authorisation

For on-line MCP transactions, if it is not possible to perform an on-line authorisation, the transaction shall be declined.

More detailed requirements on contactless POI can be found in the SEPA Cards Standardisation Volume [\[EPCI\]](#) section 4.4.3.

7.5 Secure Element

¹⁴ If the POI needs to trust data elements coming from the MCP application, the latter need to be secured within an off-line card authentication.

¹⁵ It is the mobile phone which displays the mobile code entry request and not the POI.

7.5.1 Introduction

A Secure Element (SE) is a tamper-resistant module capable of hosting applications in a secure manner. The Secure Element provides a protection of the applications including separation of the applications.

The Secure Element may appear in different form factors in the mobile equipment. In this document the following form factors are covered:

- A UICC.
- An embedded SE.
- A secure micro SD card.

Regardless of the form factor, a Secure Element 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:
 - A device or contact interface which enables commands and responses to be exchanged between the Secure Element and authorised mobile applications in the mobile equipment.
 - An antenna interface or contactless interface which enables the exchange of commands and responses between an application in the Secure Element 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 Secure Element, 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 Secure Element identifier (SEID¹⁶), regardless the type of SE (e.g., by using the UICC_ID, CUD (Card Unique Data) as defined by GP Card Specification 2.2¹⁷ ...).

7.5.2 Proximity Payment System Environment

7.5.2.1 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. In this architecture, the PPSE is depicted as an application on a Secure Element but it is feasible that it could be hosted elsewhere (e.g. within the mobile phone's Application Environment or within the NFC controller).

¹⁶ 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.

¹⁷ Card Unique Data is a data that uniquely identifies a card being the concatenation of the Issuer Identification Number (IIN) and the Card Image Number (CIN).

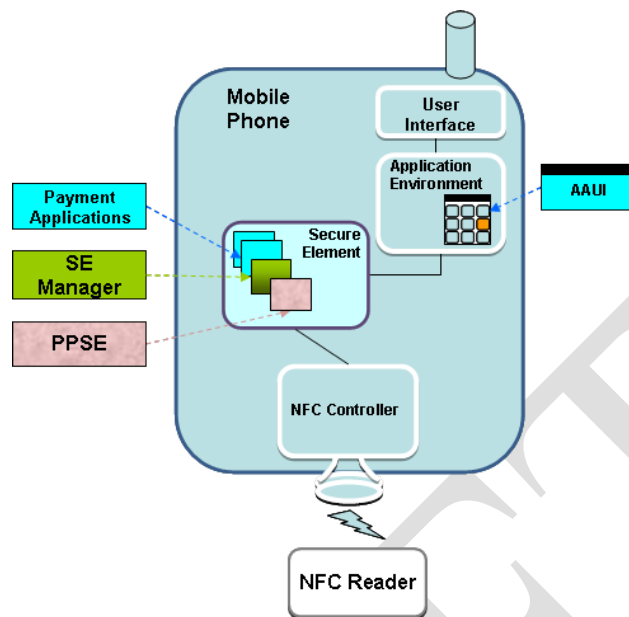


Figure 30: Location of the PPSE

There are two modes for the PPSE to receive and build the information that will be provided to the POI: External and Internal modes.

When External Mode is being used, the AAUI provides the PPSE with the details of the active applications that will be presented to the POI.

When Internal Mode¹⁸ is being used, the PPSE itself will, internally to the Secure Element, collect the details of the active applications from the Secure Element contactless manager¹⁹ and build the data to be presented to the contactless POI.

Note that there are two types of PPSE responses depending on whether the PPSE is being selected by the AAUI or whether the PPSE is being selected over the antenna interface.

7.5.2.2 Functionalities

The main purpose of any PPSE is to return a FCI (File Control Information) as a response to the selection of the PPSE application over an antenna interface. It contains the following information:

- Applications available for selection and use by the contactless POI.
- The priority of each application.
- The POI application used to interact with this application on the mobile phone.

¹⁸ Internal Mode can only be used when a single Secure Element is active.

¹⁹ A scheme employed by a Secure Element to manage the contactless applications thereon. The scheme could vary depending on the Secure Element implementation

7.5.2.3 Difference between a Contactless Card and an MCP application regarding the PPSE

- The PPSE in a card form factor has traditionally contained a static list of supported payment applications accessible over the contactless interface, personalised with an issuing bank defined prioritisation of each payment application.
- For mobile phones, the PPSE shall contain additional functionality that allows the applications that could potentially be returned to the contactless POI to be dynamically managed by the customer.

7.5.3 Security Domains and GlobalPlatform Management Profiles

7.5.3.1 Definition

Security Domains (SD) 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 a 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 (SSD) 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 the Security Domain it is in charge of. The SSD manager may have the capability to load, install, extradite or personalise applications on behalf of the service provider or the MCP issuer which granted the right for doing so.
- The controlling authority security domains (CASD) are a special type of Supplementary Security Domain. The controlling authority supports two responsibilities and can be performed by two different actors:
 - It controls a specific CASD which can enable confidential keys loading (confidential key loading authority) for setting up the initial keys of a SD.
 - It controls a specific SD used to enable mandated data authentication pattern (mandated DAP authority). The mandated DAP deployment model allows an actor to securely sign all application code before it is loaded in a GlobalPlatform card.

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

7.5.3.2 The key roles

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

- The MCP issuer procures the necessary components to load a complete payment application (i.e. application code, application data, application keys and/or certificates, and data belonging to a specific cardholder) onto a SE. The MCP issuer has a direct business relationship with and provides a SE-based service to the customer.
- 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 payment service providers.
- The Controlling Authority manages exchanges with an optional third party entity when required by the deployment model.
- The SE issuer holds ultimate 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 customers. The SE issuer is responsible for securely managing all the pre-issuance production processes culminating in an SE specifically prepared for a customer, 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 customer is the entity receiving the SE. He/she controls the download of MCP applications into the SE under the authorisation of the SE issuer.
- The SE issuer performs pre-personalisation functions, specifically the loading of the initial ISD, a CASD and, if any, application provider (i.e. MCP issuer) SD. Furthermore, the SE enabler should personalise the SD with SE issuer, controlling authority or application provider specific data. The SE enabler prepares the platform for subsequent application loading.

7.5.3.3 SE management modes

In the MCP, the SE issuer provides the SE and hosts the MCP issuer's application. GlobalPlatform has specified three different management modes to perform card content management (i.e. loading, installing, activating or removing the application) which means the ability to control and manage the functions and the information on the SE and its applications. The 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, i.e. SD creation.

- **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 security and business model between 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 controlling authority can be used. If the CASD does not exist, the MCP issuer and the SE issuer need to agree other process to ensure secure life cycle management processes for the MCP issuer.

7.5.3.4 Example of management mode scenarios

In these examples, the SE issuer such as MNO has provided the SE and controls the OTA platform to manage the SE. Only a few selected card content management functions are taken into the example. The table below shows some alternatives and, while not the full picture, it aims to highlight differences between different management modes.

	Simple mode using SE issuer OTA platform	Simple mode using SE issuer and TSM OTA platforms	Delegated mode with full/partial delegation to TSM	Authorised mode
APSD creation	TSM via SE issuer OTA platform	TSM via SE issuer OTA platform	TSM with SE issuer pre-authorisation via TSM OTA platform	TSM via TSM OTA platform
Application loading	TSM via SE issuer OTA platform	TSM via SE issuer OTA platform	TSM with SE issuer pre-authorisation via TSM OTA platform	TSM via TSM OTA platform
Personalisation	TSM via SE issuer OTA platform	TSM via TSM OTA platform	SP/TSM via TSM OTA platform	SP/TSM via TSM OTA platform

Table 10: Example of management mode scenarios

For more detailed information on that topic, please refer to the GlobalPlatform’s document [\[GP6\]](#).

7.6 Back-end systems

The MCP application interacts with a POI Device which is connected into the card payment acceptance infrastructure, responsible for authorisation, clearing and settlement.

The MCP application is to be installed on a SE by a personalisation and provisioning server which communicates with the SE via the mobile network connection (e.g. OTA). 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.

7.6.1 Personalisation

In traditional payment card production, the term “issuance” is used for the process of issuing a card to a cardholder and covers the steps:

- Pre-personalisation: preparing the card to receive personalised account data, including loading the application code onto the card and setting up any personalisation keys necessary to protect that account data.
- Personalisation: loading the personal account data into the application, including using the personalisation keys unique to the card to protect the confidential account data (mobile code, Keys).
- Fulfilment: physically dispatching the personalised card to the intended cardholder including sending the PIN by separate secure PIN mailer.
- Activation: the act of the cardholder contacting the issuing bank to notify that the card is now ready to be used.

For deployment of an MCP application to a mobile phone, the term “provisioning” is used to cover:

- Pre-personalisation: preparing the card to receive personalised account data, including loading the application code onto the card 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 customer, or may be done in a card bureau prior to physical dispatch to the customer.
- Personalisation: loading the personal account data over the air into the 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: parameters should be modified and usage of the MCP application should be controlled.

The personalisation and provisioning server is connected to a personalisation back-end, which allows the issuing bank to issue the MCP application to the mobile equipment.²⁰

The personalisation process is performed by the bank SSD manager of the issuing bank. All data preparations are realised by the same bank SSD manager.

²⁰ The MCP application might also be preloaded on the Secure Element prior to its issuance.

The bank SSD manager shall be capable of performing data preparation on all Secure Element regardless the SE profile of the end user.

The bank SSD manager receives EMV prepared data from the issuing bank and retrieves the card profile.

7.6.2 Process to install the MCP application

Several options could be chosen to install the MCP application on the secure element, such as remotely via OTA using e.g. SMS and data channel or preloaded in the factory before the supply.

- For the UICC secure element, the document on the "MCP Service Management Roles - Requirements and Specifications" [EPC3] provides guidance on the MCP application provisioning.
- For embedded chip secure element, there are two possible methods to deploy the MCP application and to perform personalisation:
 - Through OTA protocol so a remote access management over http protocol is performed through an administration agent (e.g. a mobile application: midlet, android application). Both push and pull mode are possible. In the case of push mode, an SMS is sent with a link to download the application (the so-called administration agent) to be installed on the mobile phone. The architecture for post issuance management is similar to provisioning methods described for UICC, via the OTA channel.
 - By pre-installation of the administration agent.
- For a secure micro SD Secure Element, in the case of a "built-in" antenna, APIs are required on the client side to enable OTA remote management via the admin. agent deployed on the mobile phone. These APIs are not standardised²¹ so specific sets of APIs, to reach the mobile handset OTA, must be supported by the entity in charge of the service management roles for each new vendor and specific sets of APIs to reach the micro SD shall be supported by the AAUI. Moreover, the APIs also depend on the mobile handsets platform (java, android, etc).

The difference between the secure micro SD, with and without NFC antenna, is in the tests performed during the eligibility phase. In the case of secure micro SD without NFC antenna, the mobile phone must contain a contactless front-end to be eligible.

If the secure micro SD contains an NFC antenna, the mobile phone contactless front-end presence will not be checked.

Eligibility check can be optionally performed at many occasions but is mandatory when:

²¹ Currently, there are no initiatives for standardisation in this area, even if there are some initial discussions within GlobalPlatform to issue a specification.

- Opening a new account.
- Renewing the Secure Element.
- Moving the Secure Element from a mobile phone to another.

Special care on the TSM side is required for the mobile change use case when the secure element is a removable device. The secure micro SD removal mechanism should be detected by a TSM to guaranty continuity of service (lock/unlock).

7.6.3 MCP management systems

Once the MCP application is installed and provisioned, it may be updated via the Update Server (see Figure 27). This allows application counters reset and parameters update, such as off-line balance value pre-authorized.

The MCP management is similar to cards but the OTA is an additional channel available for the Update Server to communicate with the Secure Element and the MCP application.

The counters may be reset by the MCP issuer via script processing performed OTA. Here 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 using the mobile code entered by the customer.

The counters may also be reset by the MCP issuer via script processing performed via the POI²² using NFC. This might require an additional Tap or placing the mobile phone on the NFC interface of the POI and may be considered as a drawback for the customer.

7.6.4 MCP authorisation systems

Authorisation messages for MCP transaction are similar to authorisation messages for transactions performed with a Card.

The only difference is the Form Factor (e.g. card, mobile phone) which should be managed by the issuing bank.

This identification should be performed in different ways depending on issuing bank implementation choices:

- using a dedicated parameter in a Data Element, including an indication of specific customer device features such as non card form factor, contactless only device with customer 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.

²² Script processing via POI is currently not covered for contactless technology in [1=SEPA Cards Standardisation Volume – Book of Requirements].

7.7 Security requirements and certification

This section deals with the security requirements of the different components in the MCP architecture. Here the main focus is on components which are different than the ones used within (contactless) card payment systems, namely the MCP application and the SE (as its carrier), the POI (with the contactless interface), the mobile handset and the MCP application life cycle management. Since only minor changes to the card back-end systems, with respect to the MCP transaction processing, are expected, (see section 7.6) no specific additional security requirements apply.

7.7.1 SE and MCP application

This section refers to what comprises the generic security requirements for Secure Element and the MCP application(s) stored on it.

The current section details the following:

- Scope of Evaluation, what parts & functions of the SE and MCP application are to be evaluated.
- Security Objectives & Assurance Level, an outline of the main security requirements.

7.7.1.1 Scope of the Evaluation

The Target of Evaluation, that is to say the object to be evaluated, is the payment functionality provided by MCP application stored on the Secure Element included in a mobile phone. It includes all hardware and software parts of the SE and MCP application needed to perform the payment functionality and to enforce its security.

SE and MCP application functionality, consisting mainly of transactions and possibly also of card management, is specified by each payment scheme. In this respect, it is assumed that the following basic capabilities are supported:

- Application Selection (at SE level).
- Initiate Application Processing.
- Off-line communication with the POI.
- Off-line Data Authentication (as described in [\[EPC1\]](#)).
- On-line authentication and communication with the MCP issuer (as described in [\[EPC1\]](#)).
- CVM (see section 6.2).
- MCP risk management (see section 6.3).
- Transaction Certification.
- Script processing (to update MCP application parameters and software).
- Internal State Management, ensuring that the above functions are performed in a coherent way.

The following security requirements can be used for any MCP applications on an SE that provides contactless payments via the NFC interface by supporting the basic capabilities listed above. It is an assumption that Secure Elements are either smart cards (e.g. UICCs) or share common technology

with smart cards (micro SD or embedded) such that evaluation services used for smart cards (e.g. payment cards) can be utilised. The figure below shows the architecture and components on a typical multiplicative smart card.

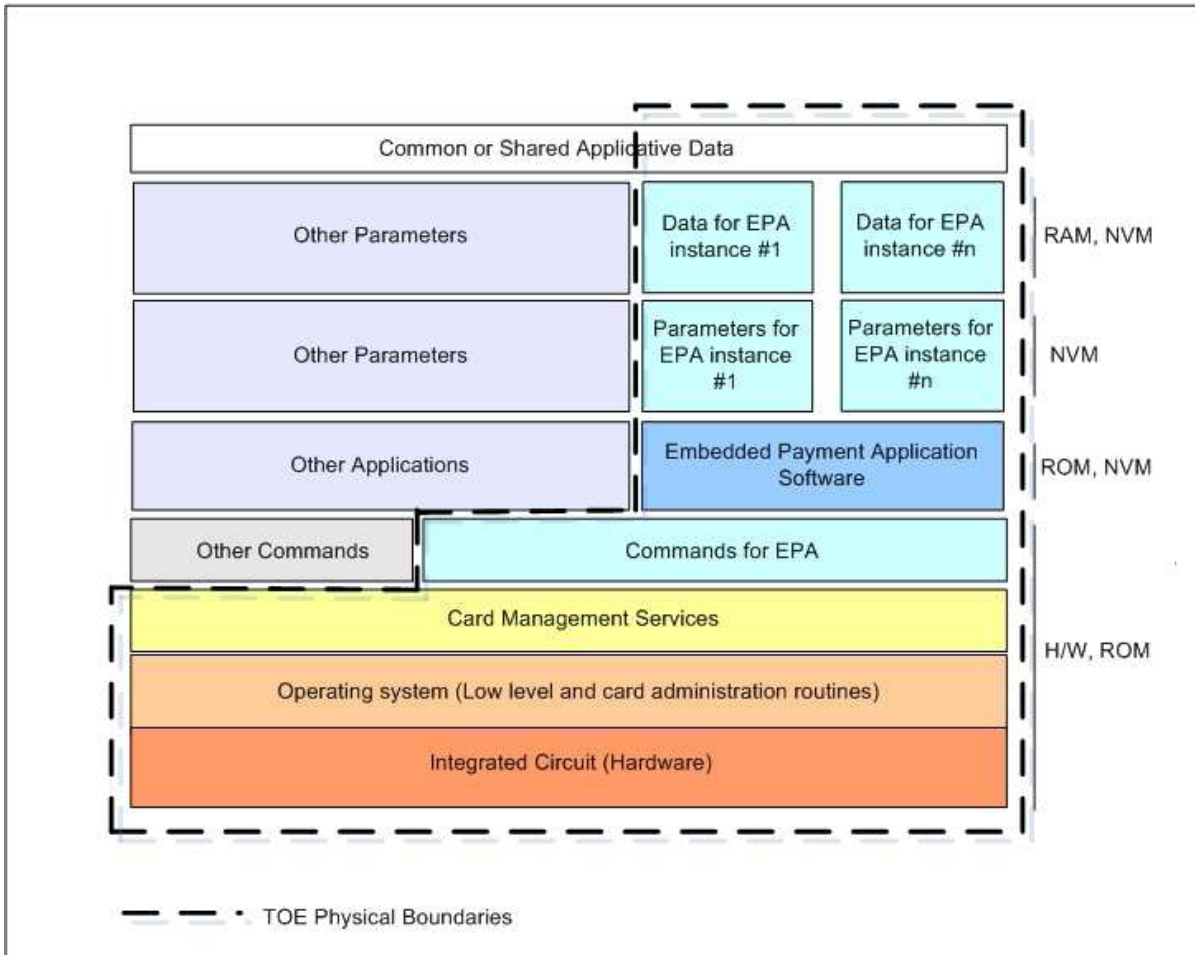


Figure 31: Typical EMV smart card architecture

In this figure, embedded payment application software and data parameters (the MCP application) are set on a platform comprising an MCP application command library, relying on low-level software and then IC hardware. Instances of MCP applications are defined by a set of personalisation data. Some MCP application data may be shared with other applications.

The SE (smart card) encompasses all layers and embedded resources contributing to MCP application functionality. SEs may operate next to the MCP other applications. In this case, the latter applications fall outside the MCP application perimeter, but stay within the SE environment, so the evaluator can assess their impact on the MCP application security.

There is no restriction on SE technology provided that all security requirements expressed, and mainly focusing on MCP application functionality, are met. Those requirements are based on the requirements specified in chapter 5 of [\[EPC1\]](#).

Note that because chapter 5 of [\[EPC1\]](#) is under revision it might impact the present section. In this case, an appropriate revision of the text below will be made as soon as possible.

7.7.1.2 Security Requirements for Secure Elements and MCP applications

Security Objectives are high-level, free-text expression of main security requirements.

Assurance Level indicates the expected resistance of security features implemented by the SE in order to meet its security objectives.

TP	TRANSACTION PROTECTION The SE and MCP application enforces generation of unique certificates binding its users, following the transaction flow as defined by the MCP application specifications	
TP1	O.GENUINE_TRANSACTION_ONCE	The probability that two transaction certificates generated by a genuine MCP application, including authentication certificates, transaction certificates, and authorisation certificates are equal shall be very low. This is related to having genuine “unique” transactions.
TP2	O.TRANSACTION_BINDING	Genuine transactions shall bind the cardholder. Transactions cannot be modified at the advantage of an attacker; certified terms of the transactions shall not be modified, and transactions shall not be modified such they can be denied.
TP3	O.INTENDED_TRANSACTION_FLOW	The normal transaction flow as defined by the MCP application specifications shall be followed and no transaction steps shall be skipped.
TP4	O.EXHAUSTIVE_PARAMETERS	The SE shall be secure for all the possible values of parameters.
SUA	MCP APPLICATION AND USER AUTHENTICATION The MCP application provides means for its authentication and enforces authentication of some users in order to prevent forgery and identity usurpation.	
SUA1	O.AUTH	The SE services shall be protected from transaction forgery by ensuring MCP application authentication during the processing of each payment transaction.
SUA2	O.CH_AUTH	The MCP application shall ensure the authentication of the cardholder while processing any transaction: <ul style="list-style-type: none"> • Authentication failure systematic counting. • Secure authentication invalidation when CVM is blocked. • Secure authentication validation when CVM execution succeeds.
SUA3	O.ISSUER_AUTH	The MCP application shall ensure the authentication of the MCP issuer while

		<p>processing any on-line transaction:</p> <ul style="list-style-type: none"> • Non-repeatability of the authentication. • Systematic script and transaction rejected when issuer cryptogram is invalid. <p>Secure transaction validation when issuer cryptogram is valid, for both script processing (e.g. via OTA) and on-line authorisation processing.</p>
SUA4	O.CARD_MANAGER	Card Management processing is authorised to the authenticated MCP application Card Manager.
EP	EXECUTION PROTECTION The SE enforces protection of its services against service denial or corruption.	
EP1	O.OPERATE	The SE shall ensure the continued operation of its services: the MCP application shall be available under normal conditions of use of the SE.
EP2	O.ISOLATION	The SE shall ensure embedded application isolation through a secure data sharing mechanism. This means that no other application within this SE shall be able to access or modify MCP application data without authorisation by the data sharing mechanism.
DP	DATA PROTECTION The SE and MCP application protects sensitive data from corruption and disclosure when required.	
DP1	O.SECRECY	<p>The SE and the MCP application shall ensure that the storage and the manipulation of its sensitive information are protected against unauthorised disclosure:</p> <ul style="list-style-type: none"> • SE Management Keys. • MCP Management Keys. • MCP mobile code.
DP2	O.INTEGRITY	<p>The SE and the MCP application shall ensure that sensitive information managed or manipulated by the SE or MCP applications is securely protected against any corruption or unauthorised modification:</p> <ul style="list-style-type: none"> • SE configuration and management data. • MCP application PAN. • MCP application Keys. • MCP application Risk Parameters. • MCP Mobile Code. • MCP application Selection Parameters. • MCP application Transaction Parameters. • MCP application Transaction Data. • POI Transaction Data when operated by the MCP application.

DP3	O.CRYPTO	Cryptographic services, including keys provided by the SE, shall be protected from exploitation that would lead to confidential information being revealed or to incorrect operation of the cryptographic mechanism.
SP	SERVICES PROTECTION The SE enforces its own security policy to prevent provided services from being attacked.	
SP1	O.RISK_MNGT	The SE shall ensure that MCP application Risk Management features cannot be corrupted or manipulated: <ul style="list-style-type: none"> • System and security counters (e.g. ATC). • Risk parameters (limits and counters).
SP2	O.EPA_ISSUER	The SE shall ensure that the SE issuer is the only external user able to access and modify SE management features and data. The SE shall ensure that the MCP issuer is the only external user able to access and modify MCP application features and data.
SP3	O.DETECTION	The SE shall administrate the detection of security violations: corruption of sensitive content, access to restricted area, or improper conditions of use of the SE.

Table 11: Security Requirements for Secure Elements and MCP applications

Assurance is grounds for confidence that a product meets its security objectives. The evaluation methodology will provide assurance through an evaluation of the product in order to determine its security properties. Greater assurance results from a greater evaluation effort, through a broader scope, a greater attention to fine details or a more formal evaluation process.

The assurance level to be associated with the here above Security Objectives for SEs shall be equivalent to the assurance package defined as EAL4+ in the Common Criteria methodology²³.

Nevertheless an EAL4+ set of assurance requirements shall be augmented regarding the following criteria:

²³ Common Criteria Part 3 contains a catalogue of Security Assurance Requirements (SAR) and defines a set of Evaluation Assurance levels (EAL) numbered from 1 to 7, each level containing more or higher Security Assurance Requirements than the one before.

Type of assurance augmentation	Description
<i>Life Cycle Support – Sufficiency of security measures</i> ²⁴	The developer is required to take sufficient measures to ensure integrity and/or authenticity of the product at development time and throughout secure deliveries during product life cycle (e.g. to chip embedder, SE Issuer, MCP application loader).
<i>Vulnerability Analysis – Advanced Methodical Vulnerability Analysis</i> ²⁵ .	It is the highest possible level for vulnerability analysis and penetration testing. It requires the SE to resist all Common Criteria referenced attacks on smartcards, either through software, hardware or combination of both. It is traditionally labelled as " <i>highly resistant</i> ".

Table 12: Type of assurance augmentation

It is the responsibility of the SE and MCP application suppliers, together with their own suppliers higher up in the supply chain, to decide how the security requirements are best met.

They may choose to organise the evaluation as a composition, using a previously evaluated IC or software platform. They may choose to use protection profiles for ICs or software platforms. Here, the efficiency of composition, as for instance currently under development by GlobalPlatform (see [\[GP7\]](#)), is recognised. It is also appreciated that IC evaluation gives advanced notice on the capacity of IC state-of-the-art technology to defeat attackers. Therefore SE suppliers are encouraged to resort to it.

7.7.1.3 Security Requirements for Point Of Interaction

Currently, in addition to meeting the global card schemes security evaluation requirements, POI vendors wishing to sell devices throughout Europe shall also meet the security requirements of a number of local schemes, each of which have their own unique evaluation and approvals processes. It is the EPC’s goal to rationalise security evaluations such that a POI manufacturer will only need to carry out a single evaluation against a common set of security requirements for all Smart Card Framework compliant schemes. The security requirements for POIs accepting MCP are the same as for POIs including contactless technology for accepting contactless cards. Therefore the reader is referred to section 5.3 of [\[EPC1\]](#) for further guidance.

7.7.1.4 Security Requirements for Mobile equipment

Since various service providers will have applications residing on the mobile phone, the EPC decided to only specify the following generic security requirements.

Security requirements
MNOs, Issuers and TSMs shall monitor the market (app. stores, websites) if application malware is in circulation. They should inform each other and jointly take appropriate action. The service level agreements between these actors should cater for this

²⁴ ALC_DVS.2 (Life Cycle Support up to level 2)

²⁵ AVA_VAN.5 (vulnerability analysis up to level 5)

Only authorised applications/entities shall be able to access and communicate to the MCP application residing on the SE.
There should be generic enablers for Secure Mobile Environment (Trusted Execution Environment (TEE), secure storage, flexible secure boot, run-time integrity checking, firewalls, anti-virus software (for further guidance, see for instance [OMTP1] , [OMTP2] , [OMTP3] and [OMTP4]).
There shall be a mechanism which enables the cardholder to activate/deactivate the NFC interface (e.g. a dedicated button)
The MNOs, issuing banks and TSMs shall monitor the market (app. stores, websites) if application malware is in circulation. They shall inform each other and jointly take appropriate action. The service level agreements between these actors should cater for this.

Table 13: Security requirements for Mobile equipment

Clearly, meeting all these security requirements has a serious cost and time to market impact on the mobile equipment. Therefore MCP issuers should have a trade-off discussion between risks and costs with the mobile handset manufacturers and MNOs when implementing MCP. This should ensure that in the future appropriate mobile handsets are available in a timely manner with adequate security.

7.7.2 MCP application life cycle management

The document on the "MCP Service Management Roles - Requirements and Specifications" that EPC has jointly developed with GSMA [\[EPC3\]](#) provides further guidance on the security requirements for the different MCP application life cycle management roles involved in the process specified in chapter 5 of 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 embedded SE or micro SD card. Generic security requirements for the MCP issuer domain may be found in section 7.3.

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

Below an overview of the security requirements is provided.

The roles of all involved parties, their processes and responsibility shall be clearly defined and agreed by SLAs (Service Level Agreements).
A secure end-to-to end channel shall be established between the MCP Issuer and the MCP application residing on the Secure Element.
There shall be a mechanism that enables the MCP Issuer or TSM to suspend/block/terminate the MCP application residing on the mobile phone 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, cardholders will more easily detect abnormalities.
MNOs and MCP issuers should inform each other if a mobile phone 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 on the Secure Element.

Table 14: Security requirements for MCP application management

7.7.3 Certification

Since the EPC certification framework for physical card payments is still under development within the SEPA Cards Framework, additions to cover MCPs will be added at a later stage.

7.8 Conclusions

As market demands are growing, more and more mobile phones supporting different types of SEs will become available. From the analysis made in the foregoing sections it is clear that the choice of the type of SE has a major impact on the MCP service model.

Although various standardisation and industry bodies have been involved in defining the appropriate specifications for mobile contactless applications covering different SE types, it is obvious that for the UICC most maturity has been reached. There are indeed still missing standardised solutions for SD cards and also embedded SEs mostly rely on proprietary solutions.

GlobalPlatform has specified three different management modes to perform card content management (i.e. loading, installing, activating or removing the application) which means the ability to control and manage the functions and the information on the SE and its applications. The management modes may impact the service management roles (e.g. who manages the SSD) and therefore the security and business model between different stakeholders. The SE issuer may support all the management modes or only some of them. This might impact the choice of the MCP issuer.

As explained in section 4, a TSM might assume some MCP management roles on behalf of the SE or MCP issuer. In case MCP issuers have to deal with different TSMs, it is important to have a standardised interface available between them. GlobalPlatform has defined an API between TSMs and MNOs (in case the SE is the UICC) but the standardisation of an API between TSMs and MCP issuers (or mobile contactless application providers in a more general way) is still missing.

With respect to the mobile equipment, mobile devices have different operating systems with different execution environments. This has a direct impact on the "secure" communication between AAUI, SE and NFC controller. Therefore MCP issuers will have to deal with mobile specific implementations e.g., Java, Android

Most of the pilots are implemented using Java MIDP based applications and communicate through Java specific (JSR) interfaces but devices with NFC and without Java MIDP-support are entering the market. It can be assumed that most, if not all, major mobile platforms will support NFC sooner



or later including Symbian, Android, iOS, Windows Phone 7, Web OS, etc. The market take up on these offering will dictate the future evolution in the MCP area.

DRAFT

8 Conclusions

This document is aimed at defining the implementation guidelines for MCP. It mainly focuses on interoperability areas between the different stakeholders involved such as the SE issuer, the MCP issuer, the MNO, the TSM, etc. in the co-operative space.

The EPC has further built on the concepts introduced in its White paper on Mobile Payments [EPC6] and on the work undertaken with GSMA on the MCP Service Management Roles - Requirements and Specifications [EPC3]. It is further based on the SEPA Cards Standardisation Volume [EPC1], already published by EPC.

Next to defining the different models and processes related to the MCP life cycle management depending on the choice of the SE, namely the UICC, an embedded SE or a secure micro SD card, it addresses, in detail, MCP transaction aspects such as CVM, risk management and transaction flows. It further provides, as support to MCP implementations, an architectural overview and a description of the technical and security infrastructure needed. It also leverages, to a large extent, the work done by other standard and industry bodies and provides the appropriate references to the various documents produced by those. At the same time it also identifies the gaps where further standardisation would be needed by the appropriate technical bodies. In particular, the management of MCPs residing on secure micro SD cards suffer from a lack of standardisation in this area which imposes additional challenges to potential MCP issuers choosing this type of SE. Also, the absence of a standardised technical API between the TSMs and application service providers is an additional burden for MCP issuers that might have to interface with multiple TSMs in the future. It is hoped that new standard activities such as the one undertaken by ISO TC68 SC7 WG10 will deal with this.

It should also be noted that, because of EPC's scope, subjects such as business cases and revenue models for the MCP value chain, which are in the competitive space among payment service providers, are not being addressed in this document. However, existing business models should not be interfered with too much. Models where the MCP issuers rent space from the SE issuers to host their MCP application(s) will accommodate this.

In producing these implementation guidelines, EPC aims to support potential MCP issuers by providing an insight into the different service, technical and security aspects involved. The document should serve as a reference basis for making certain implementation choices.

9.1.3 Use Case Scenario 2: off-line transaction with off-line CVM

Settings
 CVM Limit 15 €
 Floor Limit 48 €

Counter/Accu exceeded

upper limit counted in

2	Counter _{Con, No-CVM}	see 6.3.5.2
150 €	Accu _{Off-line}	see 6.3.5.4
6	Counter _{Con, Off-line}	see 6.3.5.5

	Transaction		Counter _{Con, No-CVM}		Accu _{Off-line}		Counter _{Con, Off-line}		> CVM Limit	Mobile Code	> Floor Limit	On-line	Issuer Action (e.g. OTA)
	trx #	amnt	Value	Status	Value	Status	Value	Status					
initial values			2		24 €		2						
analysis after trans.	1	7 €	3	NOK	31 €	OK	3	OK	No	Yes	No	No	n/a
analysis after trans.	2	21 €	1	OK	52 €	OK	4	OK	Yes	Yes	No	No	n/a
			0		52 €		4						

Table 16: Off-line transaction with off-line CVM

In this scenario two different examples are presented for the mandatory request of a mobile code.

The first transaction for an amount of 7 euros will increase the *Consecutive No-CVM counter* to 3. Since this value is greater than the *Consecutive No-CVM limit*, the customer will be requested to present a CVM (i.e. a mobile code). Since the accumulator and counter related to on-line are not reached, an off-line transaction will take place. After the successful mobile code verification, the *Consecutive No-CVM counter* will be reset to 0 by the MCP application.

With the second transaction for an amount of 21 euros, the *Consecutive No-CVM counter* will be increased to 1, not reaching its limit yet but the transaction amount is greater than the CVM limit. Therefore the customer will be requested to present a CVM (i.e. a mobile code). Since the accumulator and counter related to on-line are not reached, an off-line transaction will take place. After the successful mobile code verification, again the *Consecutive No-CVM counter* will be reset to 0.

9.1.4 Use Case Scenario 3: On-line transaction without CVM

Settings
 CVM Limit 15 €
 Floor Limit 48 €

upper limit	counted in	Counter/Accu exceeded
3	Counter _{Con_No-CVM} see 6.3.5.2	
50 €	Accu _{Off-line} see 6.3.5.4	
3	Counter _{Con_Off-line} see 6.3.5.5	

	Transaction		Counter _{Con_No-CVM}		Accu _{Off-line}		Counter _{Con_Off-line}		> CVM Limit	Mobile Code	> Floor Limit	On-line	Issuer Action (e.g. OTA)
	trx #	amnt	Value	Status	Value	Status	Value	Status					
initial values			1		24 €		1						
analysis after trans.	1	13 €	2	OK	37 €	OK	2	OK	No	No	No	No	n/a
analysis after trans.	2	14 €	3	OK	51 €	NOK	3	OK	No	No	No	Yes	n/a ²⁵

initial values			1		24 €		2						
analysis after trans.	1	13 €	2	OK	37 €	OK	3	OK	No	No	No	No	n/a
analysis after trans.	2	12 €	3	OK	49 €	OK	4	NOK	No	No	No	Yes	n/a ²⁵

Table 17: On-line transaction without CVM

In this scenario, two different examples are presented in which the MCP transaction is mandated to go on-line.

In the first example, two payment transactions (transaction 1 and 2), each below the CVM limit, result in an overall amount in the *Cumulative Off-line Accumulator* which is greater than the *Cumulative Off-line Limit*. As a result, the second transaction will go on-line. Next, the *Cumulative Off-line Accumulator* and the *Consecutive Off-line Counter* will be reset by the MCP issuer according to 6.3.5.4.

In the second example, two payment transactions (transaction 1 and 2), each below the CVM limit, result in an overall value in the *Consecutive Off-line Counter* which is greater than the *Consecutive Off-line Limit*. As a result, the second transaction will go on-line. Again, the *Cumulative Off-line Accumulator* and the *Consecutive Off-line Counter* will be reset by the MCP issuer according to 6.3.5.4.

²⁶ The *Consecutive No-CVM Counter* is not reset by an OTA reset. It will be reset by the MCP application after the successful mobile code verification requested during the next MCP transaction.

9.1.5 Use Case Scenario 4: on-line transaction with off-line CVM

Settings
 CVM Limit 15 €
 Floor Limit 48 €

upper limit	counted in	Counter/Accu exceeded
2	Counter _{Con_No-CVM}	see 6.3.5.2
150 €	Accu _{Off-line}	see 6.3.5.4
3	Counter _{Con_Off-line}	see 6.3.5.5

	Transaction		Counter _{Con_No-CVM}		Accu _{Off-line}		Counter _{Con_Off-line}		> CVM Limit	Mobile Code	> Floor Limit	On-line	Issuer Action (e.g. OTA)
	trx #	amnt	Value	Status	Value	Status	Value	Status					
initial values			2		140 €		2						
analysis	1	14 €	3	NOK	154 €	NOK	3	OK	No	Yes	No	Yes	reset
after trans.			0		0 €		0						
analysis	2	50 €	1	OK	0 €	OK	0	OK	Yes	Yes	Yes	Yes	n/a
after trans.			0		0 €		0						

initial values			2		24 €		3						
analysis	1	51 €	3	NOK	24 €	OK	3	OK	Yes	Yes	Yes	Yes	n/a
after trans.			0		24 €		3						
analysis	2	26 €	1	OK	50 €	OK	4	NOK	Yes	Yes	No	Yes	reset
after trans.			0		0 €		0						

Table 18: On-line transaction with off-line CVM

In this scenario, two different examples are presented in which the MCP transaction is mandated to go on-line with the mandatory request for a mobile code.

In the first example, two payment transactions (transaction 1 and 2), are executed. In the first transaction the *Consecutive No-CVM counter* reaches 3 and the *Off-line Accumulator* is above its limit. Therefore a mobile code will be requested and the transaction goes on-line. After the successful mobile code verification, the *Consecutive No-CVM counter* will be reset to 0 by the MCP application. Next, the *Cumulative Off-line Accumulator* and the *Consecutive Off-line Counter* will be reset by the MCP issuer according to 6.3.5.

In the second transaction, the transaction amount is both above the CVM limit and the floor limit. Therefore a mobile code will be requested and the transaction goes on-line. After the successful mobile code verification, the *Consecutive No-CVM counter* will be reset to 0 by the MCP application. There is no impact on the *Cumulative Off-line Accumulator* and the *Consecutive Off-line Counter*.

In the second example, two payment transactions (transaction 1 and 2), are executed. In the first transaction, the *Consecutive No-CVM counter* reaches 3 and the transaction value is greater than the CVM limit and the floor limit. Therefore a mobile code will be requested and the transaction goes on-line. After the successful mobile code verification, the *Consecutive No-CVM counter* will be reset to 0 by the MCP application. There is no impact on the *Cumulative Off-line Accumulator* and the *Consecutive Off-line Counter*.

In the second transaction, the amount is greater than the CVM limit and the *Consecutive Off-line counter* is greater than its limit. Therefore a mobile code will be requested and the transaction goes on-line. After the successful mobile code verification, the *Consecutive No-CVM counter* will be reset to 0 by the MCP application. Next, the *Cumulative Off-line Accumulator* and the *Consecutive Off-line Counter* will be reset by the MCP issuer according to section 6.3.5.4.

9.1.6 Use Case Scenario 5: on-line transaction with on-line CVM

Settings
 CVM Limit 15 €
 Floor Limit 0 €



	Transaction		Counter _{Con_No-CVM}		Accu _{Off-line}		Counter _{Con_Off-line}		> CVM Limit	PIN on line	> Floor Limit	On-line	Issuer Action (e.g. OTA)
	trx #	amnt	Value	Status	Value	Status	Value	Status					
initial values			n/a		n/a		n/a						
analysis after trans.	1	10 €	n/a		n/a		n/a		No	No	Yes	Yes	n/a
analysis after trans.	2	50 €	n/a		n/a		n/a		Yes	Yes	Yes	Yes	n/a

Table 19: On-line transaction with on-line CVM

In this scenario, the floor limit is set to zero, so the transaction amount is always greater than the floor limit and the transaction systematically goes on-line.

In this case, the CVM is an on-line PIN keyboarded on the POI and all transactions have a single Tap.

If the transaction amount is greater than the CVM limit, then the on-line CVM is requested.

In this example, two payment transactions (transaction 1 and 2), are executed. In the first transaction, the transaction amount is below the CVM limit; therefore the transaction goes online without CVM.

In the second transaction, the transaction amount is above the CVM limit; therefore a PIN will be requested at the POI and the transaction goes on-line. After the successful PIN verification, the transaction is approved. Because transactions are systematically on-line, there are no counters that need to be managed.

9.2 Example of AAUI implementation

The MCP application AAUI should typically be interfaced to an NFC User Primary Interface under the responsibility of the MNO. As an example, Figure 32 provides a possible implementation of a

Mobile Wallet²⁷ (indicated by the orange key) which should manage the AAUI environment on the mobile equipment.

The NFC User Primary Interface should enable the customer to:

- Browse and access contactless applications, including MCP applications.
- Add new applications.
- Select the MCP application.
- Manage general NFC settings.

Two different implementations²⁸ of MCP application selection are possible:

- The ‘By default’ MCP application.
- The MCP application priority order.

In case of a ‘by default’ MCP application management, the PPSE indicates to the contactless POI which MCP application is accessible.

- Advantages:
 - the customer always knows what MCP application is used to perform a MCP transaction.
 - The customer can disable the MCP payment service if he/she does not specify any “by default” MCP application.
- Drawbacks:
 - Potential denial of service if the contactless POI interacting with the mobile phone does not know the default application.

In case of MCP application “priority order” management, the PPSE indicates to the contactless POI which MCP applications are accessible and in what priority order. The contactless POI will then interact with the highest priority application that is common to both the contactless POI and the mobile phone.

- Advantages:
 - It maximises the service availability.
- Drawbacks:
 - The customer does not control the MCP application that is used to perform a MCP transaction.

The MCP application AAUI should be downloaded and updated via OTA by the MCP issuer on the mobile equipment. Loading and updating of this AAUI shall be done under the agreement of the customer, as the owner of the mobile equipment. It should be removed from the mobile equipment either by the MCP issuer or the customer.

Several releases of the same AAUI should be defined and managed by the MCP issuer in order to propose a well-adapted AAUI to different mobile equipment man machine interface environments (e.g. different display sizes, navigation modes, other capabilities).

²⁷ A mobile wallet is a service allowing the wallet holder to securely access, manage and use identification and payment instruments in order to initiate payments.

²⁸ These implementations are not MCP specific and are available for the other applications managed by the PPSE.

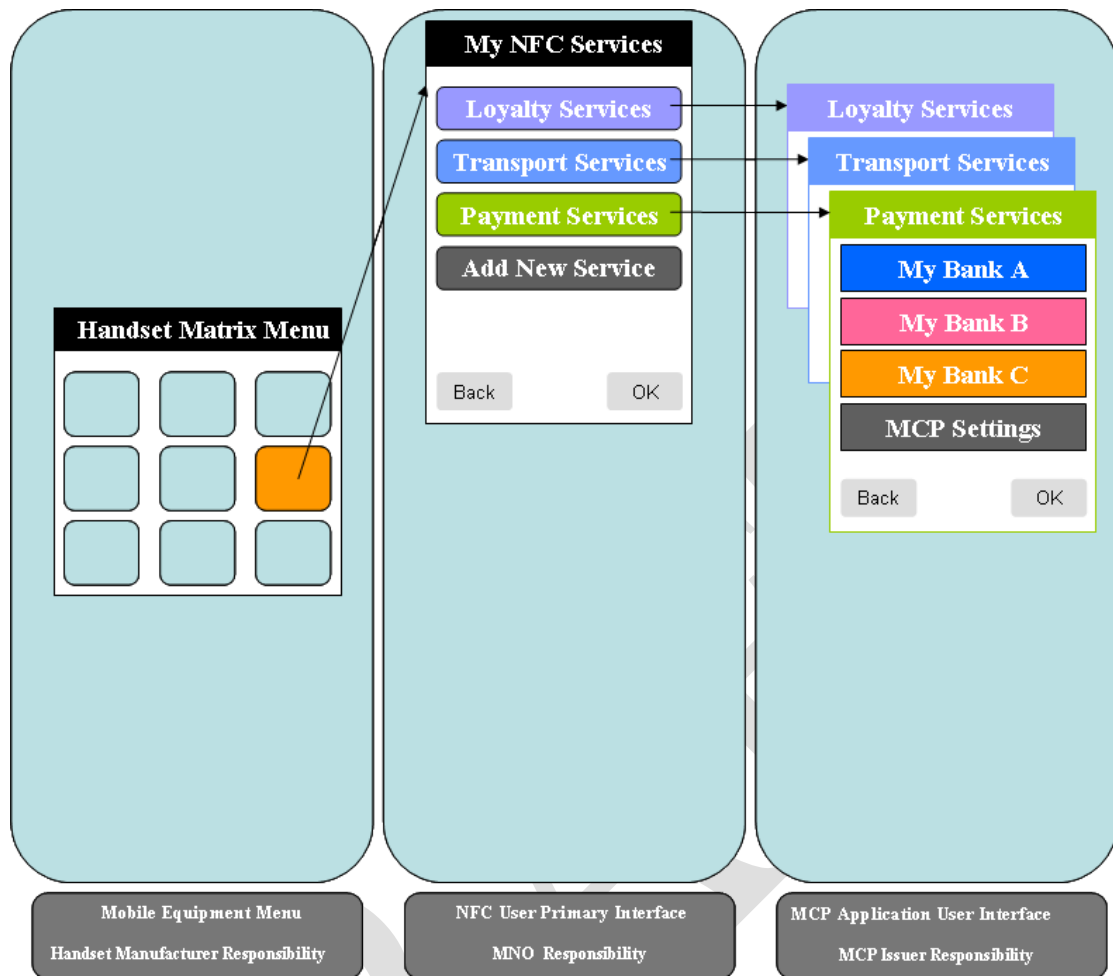


Figure 32: Example of an AAUI implementation

End of Document