EPC – GSMA
Mobile Contactless Payments Service Management Roles Requirements and Specifications

Doc: EPC 220-08, Version 2.0
October 2010

Contents

EXECUTIVE SUMMARY

The concept of using Mobile Phones to make Mobile Contactless Payments (MCP) in a secure and convenient manner is considered to be the next logical step in the development of mobile applications and payment services.

MCP, as described in this document, refers to a payment application residing in the Universal Integrated Circuit Card (UICC) (also known as the "SIM Card") within the mobile phone that employs Near Field Communication (NFC) technology.

Realising this opportunity requires a close collaboration between the key players in Mobile Communications, Payments and NFC (Near Field Communication) business ecosystems, in particular between the Payment Services Providers acting as Issuers and the Mobile Network Operators (MNOs).Therefore, in 2008, the GSMA, the global trade body for the mobile industry, and the European Payments Council (EPC), which represents 8000 banks in the European Union and EEA and Switzerland decided to work together to accelerate the deployment of services that enable consumers to pay for goods and services in shops, restaurants and other locations using their mobile phones. Both the GSMA and the EPC envisage that this cross-industry cooperation will enable Issuers to deliver better mobile payments services to their customers, supported by mobile operators' infrastructure.

This document has been jointly developed by both organisations for the European (SEPA) market and focuses on the different roles and processes involved in provisioning and lifecycle management of the MCP Application on the UICC.

This document describes the main processes between Issuers and MNOs necessary to load and manage the MCP Application(s) on the UICC (note that the payment transaction itself is out of scope of this document). These processes are defined in terms of Service Management Roles (SMRs).

Responsibility and ownership of the SMRs falls entirely within the MNO and Issuer domains. Where the MNO or Issuer decides to delegate some SMRs to a third party, this third party is known as a Trusted Service Manager (TSM). One or more TSMs can be selected by MNOs and Issuers to implement SMRs. The document includes a description of a number of business models that support the implementation of these SMRs.

In order to accommodate the freedom of choice for the customer while supporting a level-playing field in the MCP, UICC-based ecosystem, Issuers and MNOs should have freedom of choice in selecting TSM(s) for implementing SMRs.

Each SMR is described in terms of technical requirements from the MNO and Issuer domains of responsibility. The objective of this document is to provide these SMR/TSM requirements to the key stakeholders involved in the MCP ecosystem. This should facilitate the establishment of commercial relationships between the MNOs, Issuers and TSMs; thereby expediting the potential deployment and commercialisation of MCP around the world.

The main purpose of this document is to serve as a reference basis for actual implementations of MCPs and the different actors involved. The reader is also advised to consult the respective websites of EPC and GSMA for further detailed documentation.

This report has been produced by the European Payments Council (EPC) and the GSM Association (GSMA).
For further information on their respective roles see sections 1.4 & 1.5 on pages 7 & 8 of this document.

1 Introduction

1.1 Background

The concept of using Mobile Phones to make Mobile Contactless Payments (MCP) in a secure and convenient manner is considered to be the next logical step in the development of mobile applications and services. Since Mobile Phones have become a pervasive commodity today, the consumers will clearly benefit from the ease and convenience of paying for goods and services using this new payment channel. In the context of the present document, the MCPs using the Mobile Phone are based on Near Field Communication (NFC) technology while the payment application(s) are resident on the Universal Integrated Circuit Card (UICC). Although the payment application may reside on other types of Secure Element in the Mobile Phone these fall outside the scope of the present document. Those alternatives will be further dealt with by EPC (see [12]).

Realising this opportunity requires a tight collaboration between the key players in Mobile Communications, Payments and NFC business ecosystems, in particular between the Mobile Network Operators (MNOs) and the Issuers (representing the Payment Services Providers). This is a prerequisite to establish a stable ecosystem while resulting in a "win-win" business model for all parties involved.

The notion of the Trusted Service Manager (TSM) was originally introduced by Global System for Mobiles Association (GSMA) to achieve technical and business scalability in this new ecosystem. Thereafter, the European Payments Council (EPC) and the GSMA agreed to jointly work in refining the roles and requirements of the TSMs to facilitate a UICC-based MCP ecosystem.

1.2 Objective and Purpose of this document

This document contains requirements and specifications for the purpose of enabling UICC-based NFC-enabled Mobile Contactless Card Payments Application deployment and management interoperability across multiple Issuers and MNOs. The basic principle is that each sector keeps its own core business: payments for Banks/Payment Services Providers [9] and mobile services for MNOs so that existing business models can remain.

This is aimed at building an environment in which there are neither technical, legal nor commercial barriers which stand in the way of MNO subscribers, merchants, Issuers, Acquirers and MNOs to enable, select, accept, or support their preferred MCPs. Each of the parties should be able to make a specific choice of MCP(s) only based on value considerations.

In order to deliver the quality services that the market place is expecting, the existing payment and communication infrastructures should be leveraged as much as possible to support MCP. The Mobile Phone is to be considered as an additional access channel to SEPA payment schemes and infrastructure. However, there might be some required changes or additions to the infrastructure to be able to use the mobile devices at a Point-of-Sale environment (e.g., the installation of devices at the Point Of Interconnect (POI) for the acceptance of contactless payments).

To facilitate commercial and technical scalability across the SEPA market, this document also enables the establishment of commercial entities that fulfil the roles of the TSM by providing a formal set of requirements and specifications that need to be met by such entities, which cover business, technical and security aspects. This set shall serve as a common basis for the definition of a contractual TSM framework.

In particular, this document addresses the main technical and commercial processes between Issuers and MNOs necessary to load and manage the MCP Application(s) on the UICC. These processes are defined as Service Management Roles (SMR), which are composed of a consistent set of logical functions. Each SMR may be fulfilled by Issuers, MNOs and/or possibly one or more TSMs.

In order to accommodate the freedom of choice for the customer while supporting a level-playing field in the MCP, UICC-based ecosystem, Issuers and MNOs should have freedom of choice in selecting TSM(s) for fulfilling SMRs as deemed appropriate. This means that an MNO or an Issuer should have the ability to choose amongst multiple TSMs.

1 Introduction

The document is a cross-industry initiative to ensure that the market evolves efficiently with respect to the different SMRs that need to be assumed in the MCP ecosystem. An interoperability model is hereby recommended, which can be adopted by the market. However, if the model is adopted, the requirements associated with an SMR SHALL be mandatory/optional as stated in this document, whenever a party implements that SMR and the relevant corresponding SLA.

At the time of writing of this document, the EPC and GSMA are preparing supporting documentation that will need to be taken into account when implementing MCP services. The reader is referred to the respective web sites (www.europeanpaymentscouncil.eu, www.gsmworld.com) for further information. Further requirements are also specified by the Card Schemes (see www.emvco.com).

1.3 Intended audience

The document is primarily intended for the following stakeholders:

- TSMs
- Banks, other Payment Services Providers and Card Schemes.
- Mobile Network Operators.

In addition, the document may also provide valuable information for other parties involved in implementations and deployment of MCP services, such as

- Mobile Equipment manufacturers
- UICC manufacturers
- POI manufacturers
- Merchant Organisations
- Regulators.

1.4 Role of EPC

The EPC is the banking industry's decision-making and coordination body in relation to payments. The purpose of EPC is to support and promote a single harmonised, open and interoperable European domestic payments market achieved through industry self-regulation. The EPC now consists of 74 members comprising of banks and banking communities. More than 300 professionals from 31 countries are directly engaged in the work programme of the EPC, representing all sizes and sectors of the banking industry within Europe. The EPC schemes and standards have been defined in close dialogue with all stakeholders including representatives of the business community. Stakeholders are actively involved in the further development of the schemes and standards through participation in the EPC Customer Stakeholder Forum.

The EPC defines common positions for core payment services, provides strategic guidance for standardisation, formulates best practices and supports and monitors implementation of decisions taken. This is done in a way that enables banks to maintain self-regulation and meet regulators' and stakeholders' expectations as efficiently as possible.

The EPC M-Channel Working Group is focusing on the area of the initiation and receipt of credit and debit payments (including card payments) through mobile phones and defines the basic requirements, rules and standards for such payment initiation and receipt. It develops proposals that are mature for collaboration and standardisation and which form the basis for interoperability, rather than those lying in the competitive space. It further fosters cross-industry cooperation to enable the Mobile Phone to be an efficient channel to initiate payments (see www.europeanpaymentscouncil.eu).

The EPC also collaborates with Mobey Forum to analyse the different MCP business models.

1 Introduction

1.5 Role of GSMA

The GSMA is the global trade association representing over 750 GSM Mobile Network Operators across more than 200 countries and territories worldwide and over 200 manufacturers and suppliers. The primary goals of the GSMA are to ensure mobile and wireless services work globally and are easily accessible, enhancing their value to individual customers and national economies, while creating new business opportunities for operators and their suppliers. Hence the GSMA provides the ideal forum to represent the MNO community for the purposes of defining mobile NFC services (see www.gsmworld.com).

MNO collaboration in this area ensures a consistent approach in the development of mobile NFC services among mobile operators and other involved parties in the industry and hence promotes interoperability, leading to standardisation on a global scale and prevents market fragmentation.

At the time of writing this document, over 50 of the largest MNOs are working together in the GSMA's Pay-Buy-Mobile project to develop a common vision on UICC-based, NFC-enabled mobile payments. They represent over 50% of the worldwide GSM market and currently address over 1.4 billion customers.

1.6 Scope

"Mobile Payments" may cover a broad scope including any type of payment initiated through a Mobile Phone. For the purpose of this document, only Mobile Contactless Payments (MCPs), meaning the initiation of SEPA Contactless Card payments [14] at the Point-of-Interaction (POI) through NFC technology are considered.

MCPs require a Secure Element (SE) to store the Bank's payment applications and associated security credentials (see [1]). For this joint document EPC and GSMA have agreed to leverage the UICC as the Secure Element (see [7], [8] and [9]). The UICC represents a mobile network element and is owned by the MNO, who issues the UICC to the Customer. In case of UICC based NFC-enabled mobile services, parts of the UICC will be made available to the Banks to load their payment applications, either Over-The-Air (OTA), using the MNO's network or through other means such as preloading or NFC. To enable MCP, both the Mobile Equipment and the UICC need to be NFC compliant, as defined in [6] and [15].

This document has been jointly developed by EPC and GSMA for the European (SEPA) market and focuses on the different service management roles and lifecycle processes involved in provisioning and management of the MCP Application on the UICC. The payment transaction itself is not within the scope (see section 2.2).

Further guidance for the implementation of MCP applications and associated transactions will be provided by EPC in a separate document.

This document should facilitate the establishment of commercial relationships between the MNOs, Issuers and TSMs; thereby expediting the deployment and commercialisation of MCP around the world.

1.7 Document structure

This document is structured following a top-down approach as far as this was possible. Section 2 elaborates on the Mobile Contactless Payment. Section 3 introduces the main business rationale supporting the Service Management Roles (SMR). Section 4 is a high level overview on how the SMRs can be combined to achieve multiple possibilities of deployment and business models. Section 5 introduces the MCP Application management processes and associated functions. To facilitate comprehension, the interaction between processes is further illustrated through a set of examples in Annex I.

Sections 6 and 7 introduce the formal requirements for Issuers, MNOs and TSMs entities. Section 8 procures a base-line framework for the creation of the Service Level Agreements between the different business parties involved.

Finally, section 9 provides some overall conclusions related to the TSM and the associated Service Management Roles.

1 Introduction

1.8 Definitions

Acquirer
A Payment Service Provider enabling the processing of the merchant's transaction with the Issuer through an authorisation and clearing network.

Card Scheme
A technical and commercial arrangement setup 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.

Customer
An MNO subscriber (covering a variety of contractual relationships, e.g. pre-paid, post-paid) which has an agreement with an Issuer for MCP Service; the Customer is required to have an NFC enabled UICC and an NFC enabled Mobile Equipment.

Issuer
A Payment Service Provider providing the MCP Application to the Customer

MCP Service Management Information System

A backend database which records for each UICC which MCP services are installed and active.

Merchant
Is the acceptor within an MCP scheme for the payment of goods or services purchased by the Customer.

Mobile Contactless Payment (MCP)
Transaction (payment) at the POI (Point of Interaction) using a mobile NFC including a Mobile Contactless Payment Application (also referred to as Mobile Proximity Payment).

Mobile Contactless Payment Application
UICC Application performing the payment functions, as dictated by the Issuer, over NFC.

Mobile Contactless Payment (MCP) Application User Interface
The Mobile Equipment (ME) application executing the user interactions related to the Mobile Contactless Payment Application, as permitted by the Issuer.

Mobile Contactless Payment Service
The MCP Service comprises a number of applications. For example: the MCP payment application in the UICC and a User Interface application, a dedicated Customer help desk, etc….

Mobile Equipment (ME)
Mobile Phone without UICC (also referred to as Mobile Handset)

Mobile Phone
UICC + Mobile Equipment (ME) (also referred to as Mobile Station).

1 Introduction

Near Field Communication (NFC)
A contactless protocol specified by ISO/IEC 18092.

NFC Mobile Phone

A Mobile Phone including NFC functionalities.

Payment Application Selection User Interface
The Mobile Phone user interface (component) enabling the Customer to:

- Access the MCP Application User Interface on the Mobile Phone,
- Select the preferred payment application

Payment Service Provider
An entity offering online services for electronic payments by a variety of payment methods such as cards, bank-based payments and online banking, either a bank or a payment institution as defined by and licensed according to the Payment Services Directive [17].

Secure Element (SE)
A tamper-resistant platform (device or component) capable of securely storing and executing applications and their secrets (e.g. keys), in accordance to the rules and security requirements set forth by a set of well-identified trusted authorities. Examples are UICC, embedded Secure Elements, Chip Cards, SD Cards, etc.

Security Domain (SD)
On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the MNO, an Issuer or a TP).

Service Management Roles (SMR)
A set of roles that enable the lifecycle management of MCP whilst meeting security and quality of service requirements to the Issuer (MNO and Customer).

Supplementary Security Domain (SSD)
A Security Domain other than the MNO Security Domain.

Third Party (TP)
This is an entity in the ecosystem that is different from an MNO or Issuer (e.g. Card Manufacturer, Evaluation Laboratory).

Trusted Service Manager (TSM)
A third party that implements one or more Service Management roles.

1 Introduction

1.9 Normative text

In the context of this document, when used in upper case the following English words SHALL be interpreted as follows:

SHALL

This word means that the definition is an absolute requirement of the specification.

SHALL NOT

These words mean that the definition is an absolute prohibition of the specification.

SHOULD

This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. In the context of this document, if implemented, the item SHALL be implemented as specified.

MAY

This word means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

1 Introduction

1.10 Acronyms

Acronym	Meaning
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Program Interface
EMVCo	Company owned by American Express, JCB, MasterCard and Visa which manages, maintains and enhances the EMV Integrated Circuit Cards Specifications (see www.emvco.com)
EPC	European Payments Council
ETSI	European Telecommunications Standards Institute
ETSI-SCP	European Telecommunications Standards Institute-Smart Card Platform
GP	GlobalPlatform
GSM	Global System for Mobiles
GSMA	GSM Association
ISO	International Organisation for Standardisation
M	Mandatory, reflected as “SHALL” in this document
MCP	Mobile Contactless Payment
MNO	Mobile Network Operator
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
NFC	Near Field Communication
O	Optional, reflected as “SHOULD” in this document
OTA	Over the Air supporting protocols which enable to address the UICC using the handset as a transparent communication means, as defined in [2]
POI	Point of Interaction (e.g., POS, ATM, etc., see [14])
POS	Point of Sale
SD	Security Domain
SSD	Supplementary Security Domain
SE	Secure Element
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SM	Service Management
SMR	Service Management Role
SP	Service Provider
TSM	Trusted Services Manager
TP	Third Party
UI	User Interface
UICC	Universal Integrated Circuit Card
UPI	User Primary Interface
USIM	Universal Subscriber Identity Module

1 Introduction

1.11 Referenced Documents

#	Document Title	Reference
1	AEPM Book "0"	Payez Mobile: Mobile Contactless Proximity Payments Technical Specifications Book 0; General Description, Version 2.0, May 2009
2	AFSCM: Guidelines for Interconnection of Service Providers' and Mobile Network Operators' Information Systems	Release 1.0, 02/06/2009, Ref 090720 – AFSCM TECH LIVBL – Interconnection Guidelines – v1.doc www.afscm.org/en
3	EMV Mobile Contactless Payment - White Paper: The Role and Scope of EMVCo in Standardising the Mobile Payments Infrastructure - Version 1.0	EMVCo, October 2007 www.emvco.com
4	EMV Contactless Communication Protocol Specification - Version 2.0.1	EMVCo, July 2009 www.emvco.com
5	EMV Profiles of GlobalPlatform UICC Configuration	EMVCo www.emvco.com
6	ETSI TS 102.225 Smart Cards; Secured packet structure for UICC based applications	ETSI, April 2009 www.etsi.org
7	GlobalPlatform Card Specification V.2.2 + amendments	GlobalPlatform, http://www.globalplatform.org
8	GlobalPlatform UICC Configuration v1.0	GlobalPlatform, October 2008 http://www.globalplatform.org
9	GlobalPlatform Proposition for NFC Mobile: Secure Element Management and Messaging	GlobalPlatform, April 2009 www.globalplatform.org/documents/GlobalPlatform_NFC_Mobile_White_Paper.pdf
10	HCI	ETSI TS 102 622, Release 7 www.etsi.org
11	ISO/IEC 18092; Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)	www.iso.org
12	Mobile Contactless SEPA Card Payments Implementation Guidelines	EPC178-10 www.europeanpaymentscouncil.eu
13	Mobile NFC Services White Paper	GSMA, February 2007, http://www.gsmworld.com/documents/nfc_services_0207.pdf
14	Mobile Payments	EPC492-09 www.europeanpaymentscouncil.eu
15	NFC Technical Guidelines V2 White Paper	GSMA, November 2007, www.gsmworld.com/documents/nfc/gsma_nfc2_wp.pdf
16	Pay-Buy-Mobile Business Opportunity Analysis Public White Paper	GSMA, November 2007, www.gsmworld.com/documents/pbm/gsma_pbm_wp.pdf
17	Directive 2007/64/EC	European Parliament and Council of 13 November 2007 on Payment Services in the Internal Market. www.eur-lex.europa.eu

#	Document Title	Reference
18	SEPA Cards Framework	EPC027-05 www.europeanpaymentscouncil.eu
19	SEPA Core Direct Debit Scheme Rulebook	EPC016-06 www.europeanpaymentscouncil.eu
20	SEPA Credit Transfer Scheme Rulebook	EPC125-05 www.europeanpaymentscouncil.eu
21	SEPA Cards Standardisation "Volume"	EPC020-08www.europeanpaymentscouncil.eu
22	SWP	ETSI TS 102 613, Release 7 www.etsi.org

2 Mobile Contactless Payment Overview

2.1 What is an MCP?

In the context of this document a Mobile Contactless Payment (MCP) is any SEPA Card based payment executed by a Customer using a dedicated Mobile Contactless Payment Application provided by an Issuer and loaded onto the UICC (provided by an MNO) of a Customer's NFC enabled Mobile Phone.

2.2 The MCP ecosystem

Mobile Contactless Payments introduce a new ecosystem involving new players in the chain.

The main actors involved in the transaction based on MCP do not differ from a "classical" payment as illustrated in Figure 1.

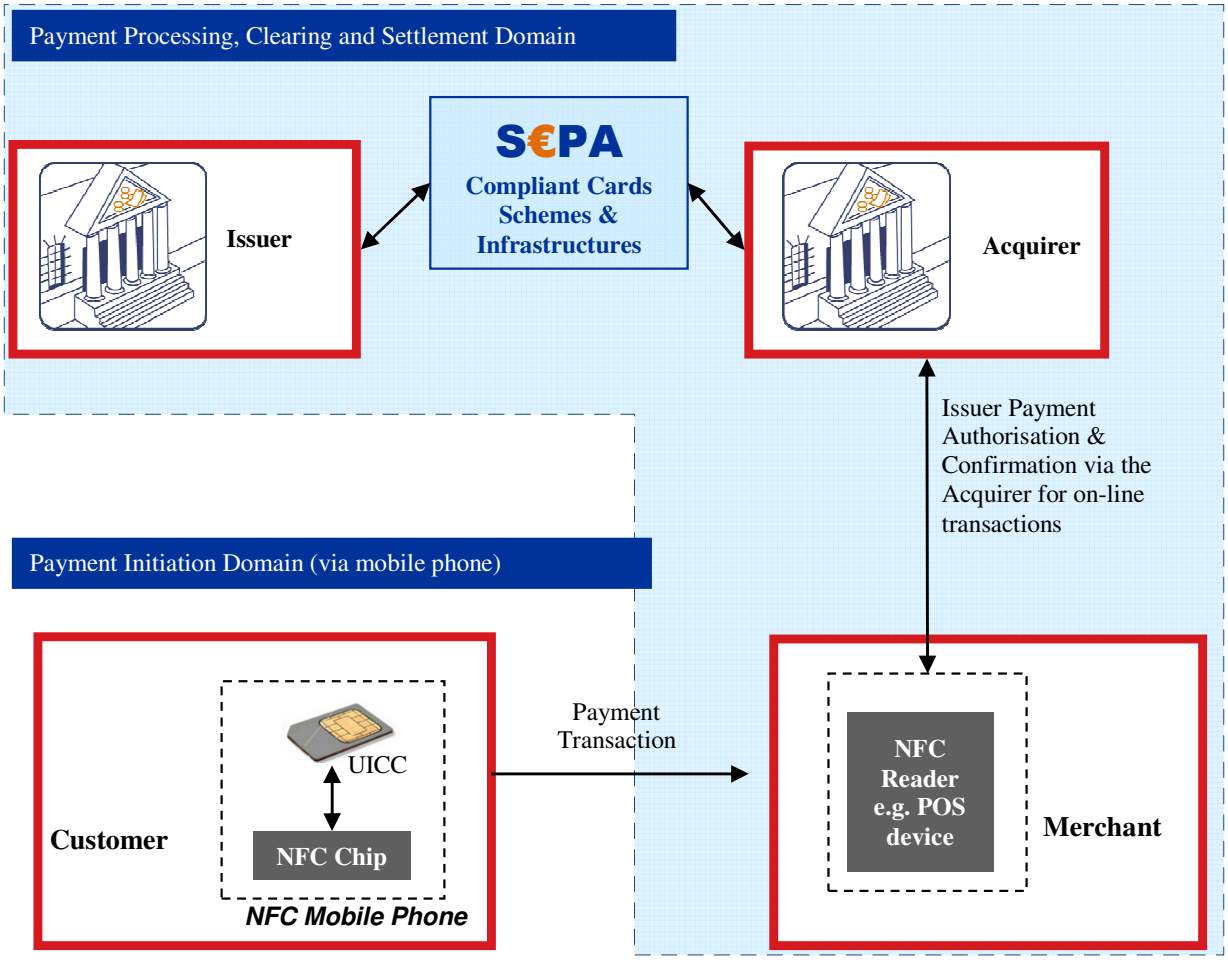


Figure 1: Initiation and Processing of an NFC enabled, UICC-based Contactless Payment

2 Mobile Contactless Payment Overview

The Customer is also a MNO subscriber and the MNO is involved as the owner of the UICC for the provisioning and management of the MCP Application as illustrated in Figure 2. Further guidance is provided in section 4.

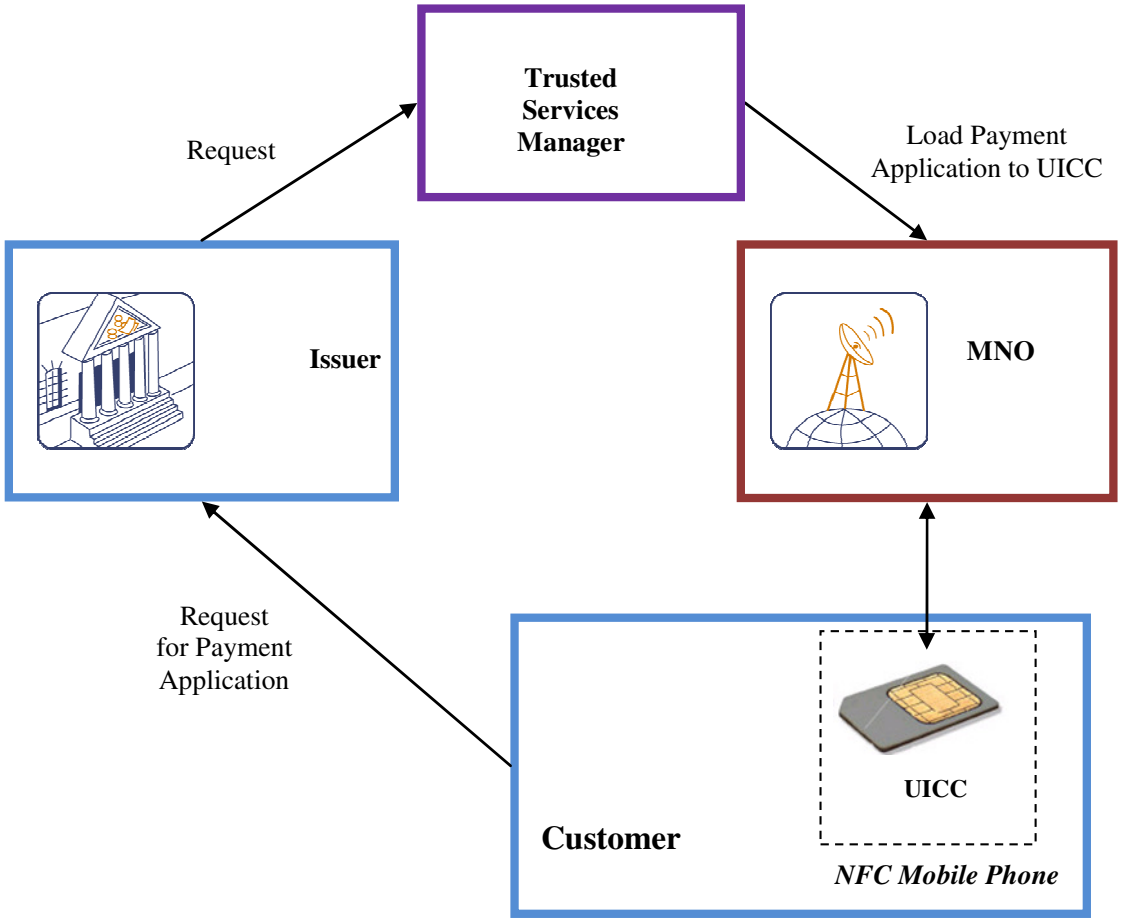


Figure 2: Provisioning of MCP Application to a UICC

2 Mobile Contactless Payment Overview

Therefore the actors in the MCP ecosystem illustrated in the figures above are as follows:

- **The Acquirer** is a Payment Service Provider enabling the processing of the merchant's transaction to the Issuer 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 Issuer for MCP Service; the Customer is required to have an NFC enabled UICC and an NFC enabled Mobile Equipment.
- **The Issuer** (in this document the term "Issuer" means "MCP Application Issuer") is a Bank (or Payment Service Provider) providing the MCP service to the Customer; the Issuer is responsible for the provisioning of the MCP Application to the UICC of the Mobile Equipment, and the personalization of the application with Customer's data. Furthermore, the Issuer is also responsible for other life cycle management aspects.
- **The Merchant** is accepting a MCP scheme for payment of the goods or services purchased by the Customer; the merchant has an agreement with an Acquirer and shall be equipped with a contactless Point of Interaction device.
- **The Mobile Network Operator (MNO)** offers a range of mobile services, 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 Issuer (or its TSM agent depending on market implementation).

The Service Management Roles (SMR) is a set of functions that will be executed by one or more parties to load, maintain and/or delete the MCP Application on the UICC. The implementation of these roles will be defined according to the requirements from both the Issuers and MNOs. These SMRs can be attributed to different physical entities, Issuers, MNOs, TSMs, etc. Parties performing SMR(s) typically have technical and/or commercial relationships with Issuers and/or MNOs.

Where the MNOs or Issuers decide to fully or partially sub-contract the implementation and/or operation of their Service Management Roles to a third party, this party is called a **Trusted Service Manager (TSM)** as depicted in Figure 2. Further information on the TSM is provided in section 4.

It is recognized that one or more TSMs are needed to support multiple Issuers and MNOs.

3 Guiding Principles for Service Management

The following reflects some high level guiding principles which might have an impact on the SMR and should be supported by the requirements and specifications laid down in the sequel of this document.

3.1 Portability

The Customer shall be able to switch from one MNO to another while keeping the possibility to use the MCP Application (provided the relevant arrangements between actors have been set up).

The Customer shall also be able to change the Mobile Equipment (provided the Mobile Equipment is NFC-compliant and enabled to support the MCP Application User Interface).

The Customer shall also be able to switch from one Issuer to another and thus replace his/her current MCP service by a new one (provided the relevant arrangements between actors have been set up).

These results in the following:

- Switching MNO implies issuing a new UICC (by the new MNO) and reload MCP Application (by the Issuer);
- Switching Issuers implies loading a new MCP Application by the new Issuer;
- Switching Mobile Equipment may only imply the download of a new MCP Application User Interface by the Issuer.

Further details on the required process are provided in Annex I and section 5.

3.2 Cross-border usage within SEPA

The Customer shall be able to use the MCP Application to make a payment transaction in any country independent of the one where he/she has an agreement with an MNO.

If OTA is used for the MCP Application management abroad, then any associated costs including any other potential costs shall be clear and visible to the Customer.

3.3 Certification / Type Approval

Standardized certification and type approval processes shall be performed independently by appropriate accredited bodies, for the following components:

- Secure Element (this work is focused on the UICC being the SE);
- Mobile Equipment with supporting technology (NFC enabled);
- Service Management processes (provisioning and personalization, data exchanges…);
- Every MCP Application preloaded to the Secure Element, or downloaded after issuance and certification of the Secure Element.

The certification/type approval of POI terminals is outside the scope of this Project.

3 Guiding Principles for Service Management

3.4 Security and Privacy

The specifications supported by this document should enable the secure deployment and operation of MCP Applications by Issuers.

Additional security requirements for MCP Applications and their execution environment based on a risk analysis and assessment may be applicable (see www.europeanpaymentscouncil.eu, www.emvco.com). These security requirements will typically address:

- UICC (hardware and operating system)
- MCP Application User interface (display and entry on the keyboard)
- Mobile Equipment,
- MCP Application and its management
- Point of Interaction

and further include the requirements for the appropriate key management needed.

The MNO will specify additional security requirements (see section 1.2)

- That enable MCP Applications to be securely stored on the UICC,
- That enable third party applications to be securely stored /downloaded on a UICC,
- That enable the security between each stored application,

which also include the requirements for the appropriate key management needed. Typically MNOs will comply to GP Card implementation 2.2 [3] and related amendments.

In addition, the MNOs and the Issuers need to comply with legal regulations regarding Customer privacy.

All parties involved in MCP Application Services shall conform to the security requirements stated in sections 6 and 7.

3.5 Branding

The Issuer brands shall be supported in user interfaces on the Mobile Phone. The Issuer is responsible for the definition of the Issuer's presentation (graphical interface) to the Customer including Issuer brands and logos, card scheme brands, payment type etc.

3.6 Support of Multiple MCP Applications

Several MCP Applications shall be supported (e.g., debit cards, credit cards, prepaid cards…), either alone or together, with an appropriate selection mechanism (mechanism for the end user/customer to select the preferred payment option – like a wallet). The Customer shall be in full control of which MCP services they subscribe to and shall be able to request the removal of MCP Applications from the UICC.

3 Guiding Principles for Service Management

3.7 Multiple Issuers

The Customer shall be able to have MCP Applications issued by different Issuers at the same time in the Mobile Phone (on the UICC), and shall be able to select the relevant MCP Application to be used for a payment transaction. The user interface that will enable the MCP Application will typically be provided by the MNO. The user interface for the selection of the MCP Application itself will typically be provided the Issuer.

A standardised data structure will be provided by the Issuer to represent the MCP Application in the MNO user interface. This data structure should contain at least:

- Issuer Name,
- MCP Application Name (this is typically the commercial name),
- Logo(s).

3.8 Requirements for the User Interface - unifying the Payment experience

The Customer should have a similar payment experience when performing a MCP transaction independent of the location where the transaction is executed. This includes the interaction with the accepting device (POI) (similar to the customer experience on ATM networks that is essentially the same anywhere in Europe).

The Customer shall have access to a user friendly and consistent mechanism through their Mobile Phone to select preferred MCP Applications between several Issuers.

More information on the User Interface is provided in Annex II

3.9 Customer care

Point(s) of contact for the Customer shall be clearly defined between actors, with an agreement of their respective roles (for example in case of loss, theft, or questions/support).

3.10 Service Level Agreements (SLAs)

SLAs have to be set up between Issuers, the entities performing the Service Management Roles and the MNOs (depending on the configuration and the market circumstances).

3.11 Common Interface

The Issuers and MNOs shall define a common interface between their respective service management information systems for MCPs to ensure synchronisation on the MCP Application status (e.g. active, blocked, etc.). The API shall cover the SM processes defined in section 5.3[1] .

[1] EPC and GSMA encourage international standardisation of such an API.
Some work in this area has already been done, for example in France with the AFSCM (see www.afscm.org/en). Furthermore, GlobalPlatform is currently developing the secure messaging specifications for these APIs (see www.globalplatform.org).

4 Service Management

4.1 Service Management Overview

Service Management Roles are defined in this document in order to:

- Provide a common vision from EPC and GSMA on the organization of remote management of UICC-based Mobile NFC contactless payment;
- Provide models for the implementation of the Service Management Roles;
- Define and clarify roles and responsibilities of the actors on the Service Management.

Service Management Roles shall comply with the requirements set forth in sections 6 and 7.

Figure 3 shows:

- The domains of responsibility;
- The Service Management technical roles;
- The commercial relations that can be put in place between MNOs and Issuers

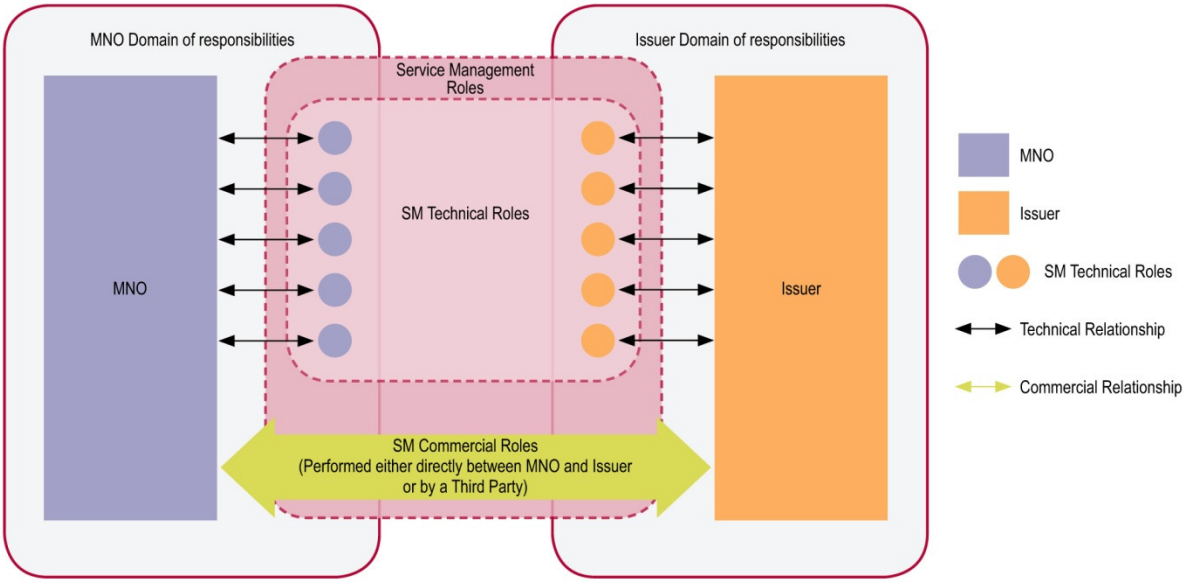


Figure 3:
Service Management General Overview

4 Service Management

4.2 Service Management Roles

Service Management (SM) is primarily a set of technical and commercial roles implemented to load maintain and delete the MCP Application on the UICC. The implementation of these roles is defined according to the requirements from both the Issuers and MNOs.

SM technical Roles are divided in two responsibility areas, according to the principle that responsibility areas cannot be shared by multiple actors:

1. The MNO domain of responsibility: The MNO is the owner of the UICC. Their responsibility is to provide the "secure management framework" in alignment with the Issuers and Card Schemes (i.e. for secure storage and execution of applications within the UICC) to the Issuer and Customers of the MCP Applications. In order to achieve this, the MNO needs to:

- Manage the UICC lifecycle (e.g. issuance, eligibility, memory management, SD management – see section 5.1, etc.),
- Manage the UICC security framework,
- Manage the Customer lifecycle,
- Provide support to Customers.

2. The Issuer domain of responsibility: The Issuer is the owner of his MCP Application. Their responsibility is to deliver and to operate the MCP Application for the Customer. In order to achieve this, the Issuer needs to:

- Manage his MCP Application lifecycle (i.e. development, download, personalization, activation, operational management, deletion), with the required level of security and compliance,
- Manage the Customer lifecycle,
- Provide support to Customers.

Issuers and MNOs will need to establish the appropriate SLAs related to these SMRs. Section 8 provides further guidance on this matter.

4.2.1 Technical and Security Roles

In order to deliver the mobile NFC-services value propositions to Customers, the following technical roles shall be implemented:

- **The MNO SM technical roles**: These technical roles are under the responsibility of MNOs. These technical roles cover the technical and security functions that are necessary to MNOs for implementing their offer to Issuers and Customers. They are actually implemented by MNOs or subcontractors appointed by MNOs. The technical roles & associated requirements for MNOs are formally introduced in section 6.
- **The Issuer SM technical roles:** These roles are under the responsibility of Issuers. These technical roles cover the technical and security functions that are necessary for Issuers to implement their service offering to Customers. They are actually implemented by Issuers or subcontractors appointed by Issuers. The technical roles & associated requirements for Issuers are formally introduced in section 7.

4 Service Management

4.2.2 Commercial Roles

In addition to the aforementioned technical roles, there is also a commercial relationship between Issuers and MNOs. This commercial relationship covers areas such as general Terms & Conditions, business models, Service Level Agreements, etc.

The commercial relationship between the MNO and the Issuer can be implemented either directly or indirectly:

- A **direct relationship** means that the MNO and the Issuer connect directly to each other, and sign a contract between themselves.
- An **indirect relationship** means that "commercial actors" stand between the MNO and the Issuer. The MNO and Issuer need to sign contracts with these commercial actors. The commercial actors can take on various levels of responsibilities depending on the activities that they intend to take (e.g. broker, commercial agent, supplier, central purchasing etc). Commercial actors are likely to be needed when:
- MNOs want to grant their Customers access to banking services without having to deal directly with Issuers.
- Issuers want to offer their services to their Customers without having to manage deals directly with MNOs.

An MNO can be connected or not to one or several commercial actors. An Issuer can be connected or not to one or several commercial actors

Direct and Indirect commercial relationships can coexist. The implementation of these combinations of models depends on market conditions as well as the preferred commercial strategy of the respective MNOs and Issuers (see section 4.3).

The minimal scope of the Service Level Agreements between commercial actors is introduced in section 8.

The commercial roles implemented through indirect relationships are introduced in the following subsections.

4.2.2.1 Brokerage

The commercial relationship for the exploitation of the UICC is in principle established between the Issuer and the MNO. In most markets there are many Issuers and MNOs active, and as a consequence there is a risk that each Issuer would have to negotiate a commercial agreement with each MNO.

One role of the TSM could be to act as a 'B2B broker' in this situation, performing the following functions:

- Buying (wholesale) services from MNOs.
- Packaging and pricing these services towards Issuers.
- Managing (as intermediary) the SLAs between Issuers and MNOs.

In this way the Issuer would only have to deal with one selected TSM to access the customer base of multiple MNOs, and reciprocally, for a MNO to access the customer base of multiple Issuers.

4 Service Management

4.2.2.2 B2B Marketing

In addition to the Brokerage role, a further role of the TSM could be to market the NFC payment service to Issuers and MNOs. Functions:

- Promote the NFC payment service to prospect MNOs and Issuers (seminars etc)
- Acquire MNOs to make their services available for NFC payments
- Market the services to prospect Issuers.

4.2.2.3 B2B Helpdesk

It is recommended that the support functions towards the Customer (consumer) are managed directly by Issuers and MNOs. However the TSM could offer a B2B support desk to:

- Second line support for issues related to the MCP Application lifecycle management (like activation/de-activation, application reloading). Support for Issuers and MNOs e.g., to enrol Customers.

4 Service Management

4.3 Service Models for SMR

This section introduces several examples from the possible MCP management services business models implemented through combinations of SMR distributed through Issuers, MNOs and third party service providers. More information on business aspects of service models related to MCP is provided in [10].

4.3.1 The 3 Party Model

The 3 parties are the Customer, the MNO and the Issuer (see Figure 4).

Service Management technical roles are the set of technical functions performed on behalf of the MNO and/or the Issuer. They are fully or partly fulfilled by TSMs.

In this model there is a direct business contract between Issuers and MNOs. In other words, TSM companies are not involved in the commercial relationship between Issuers and MNOs.

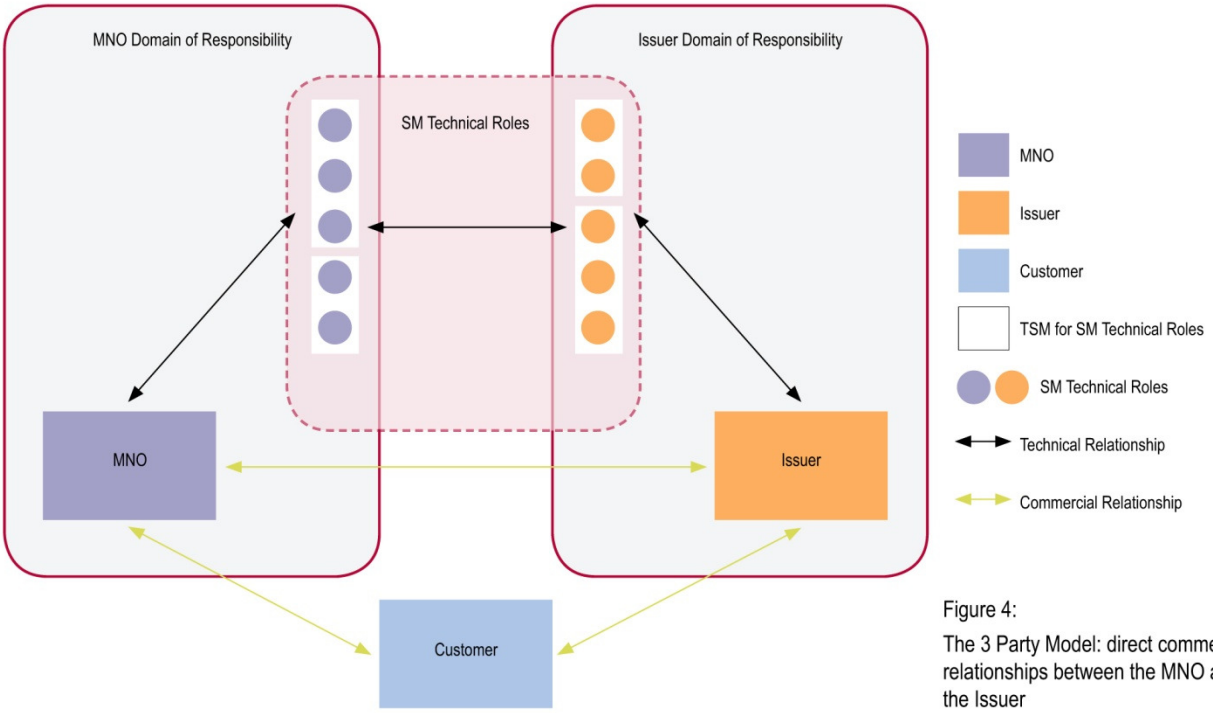


Figure 4:
The 3 Party Model: direct commercial relationships between the MNO and the Issuer

4 Service Management

4.3.2 The 4-Party Model

Where the MNOs or Issuers decide to fully or partially sub-contract the implementation and/or operation of their Service Management Roles to a third party, this party is called a **Trusted Service Manager (TSM).**

The 4 parties are the User, the MNO, the Issuer, and the TSM. In this model the TSM fulfils the technical roles as well as the commercial roles of the Service Management. This means that the TSM actors have commercial relationships with Issuers and MNOs, in this model there is NO direct commercial contract between Issuers and MNOs.

A general picture for this model is provided in Figure 5.

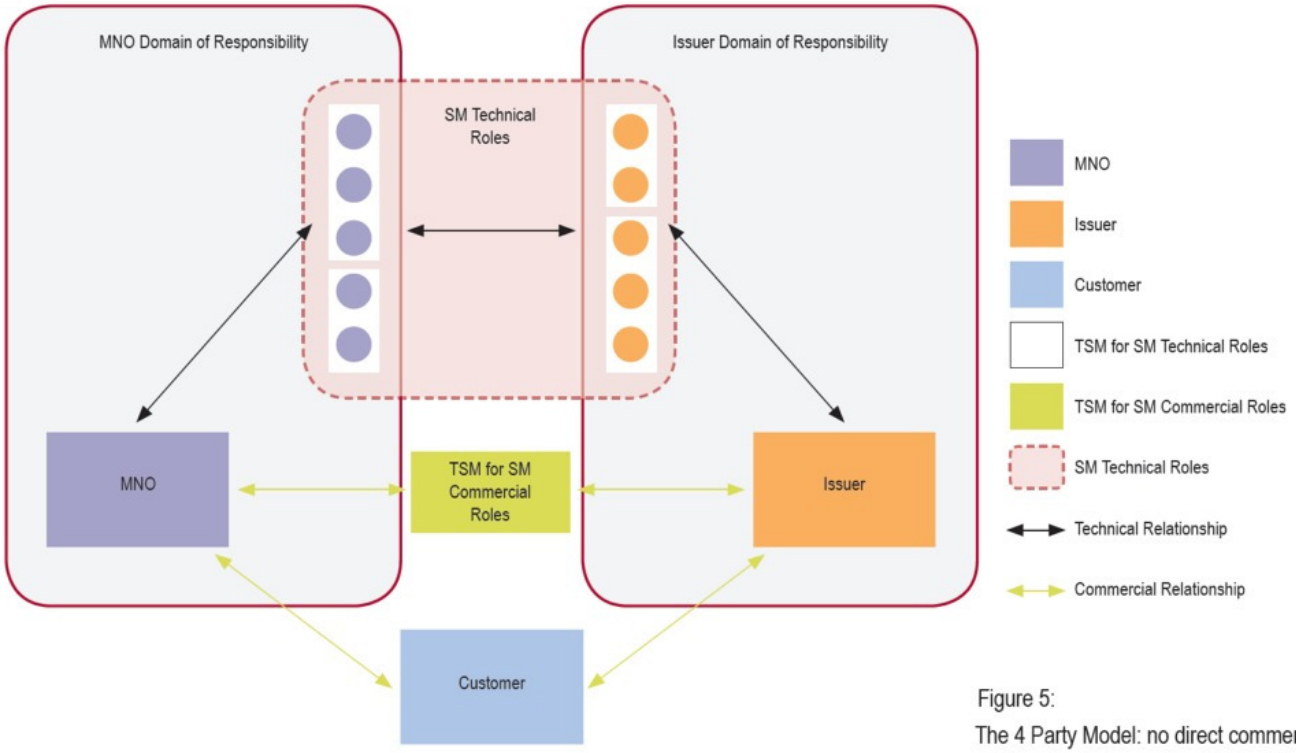


Figure 5:
The 4 Party Model: no direct commercial relationship between the MNO and the Issuer

4 Service Management

Hereunder are three examples of 4-Party models.

4.3.2.1 Example 1

In this example (see Figure 6), the same TSM fulfils technical and commercial roles for the Issuer. In the general case, several TSM companies may be involved.

This model implies that the TSM implementing commercial roles is selected by the Issuers and accepted by the MNOs.

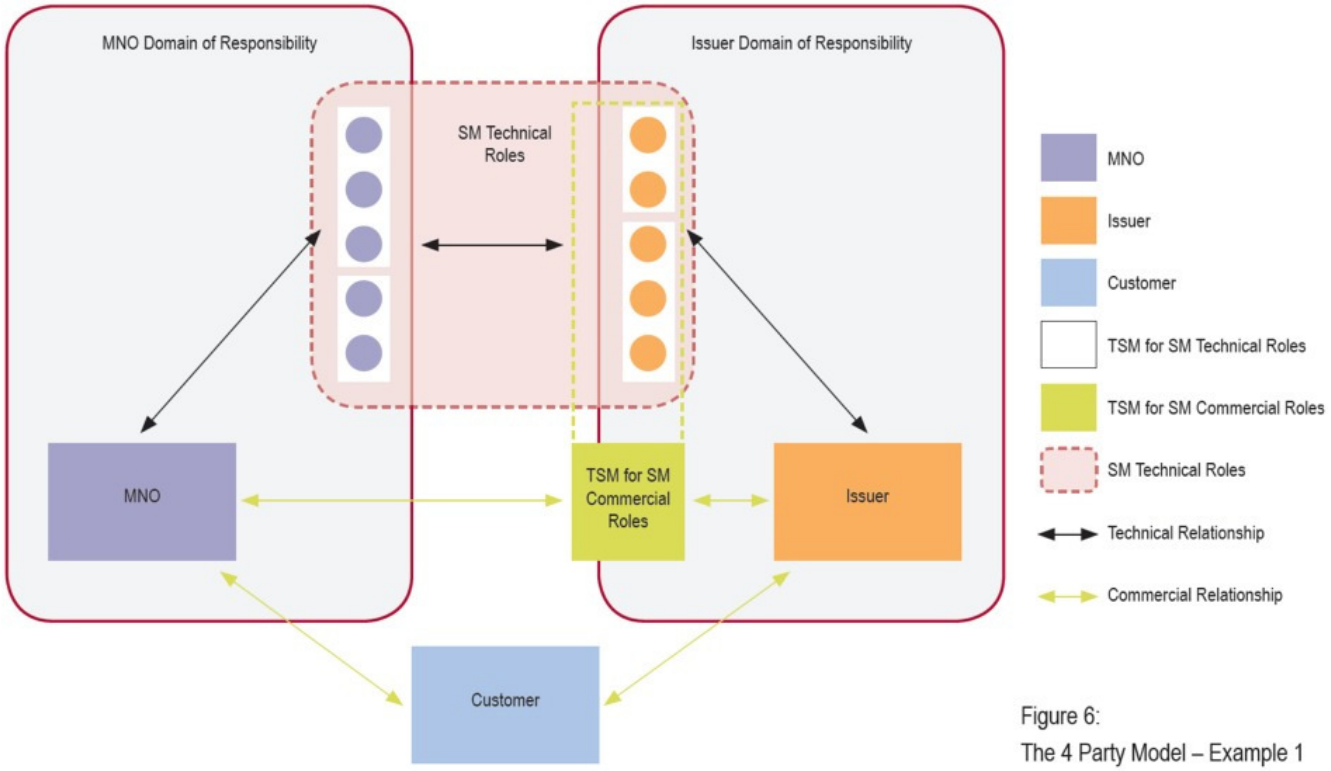


Figure 6:
The 4 Party Model – Example 1

4 Service Management

4.3.2.2 Example 2

In this example (see Figure 7), the TSM fulfils technical and commercial roles for the MNOs. In the general case, several TSM companies may be involved.

This model implies that the TSM implementing the commercial role is selected by the MNO and accepted by the Issuers.

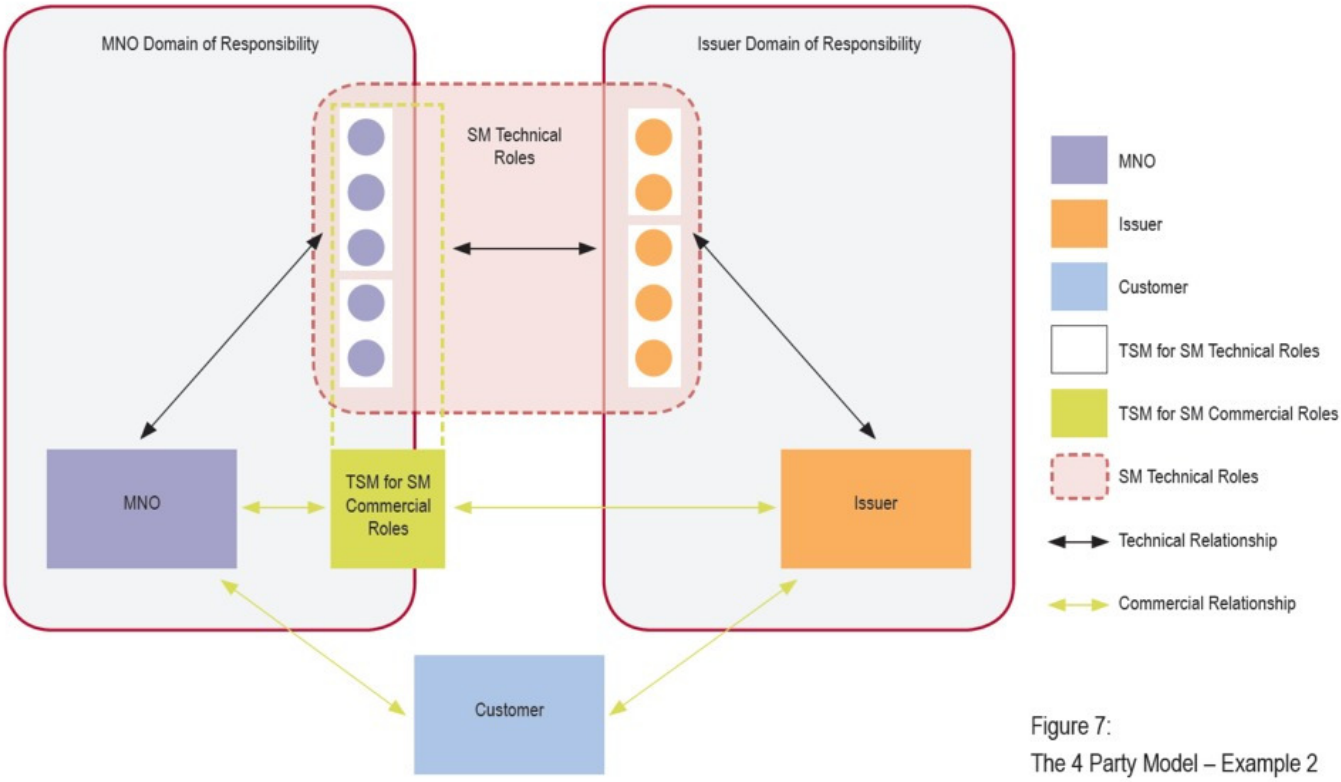


Figure 7:
The 4 Party Model – Example 2

4 Service Management

4.3.2.3 Example 3

In this example (see Figure 8), the TSM fulfils technical and commercial roles for both the Issuers and the MNOs. In the general case, several TSM companies may be involved.

This model implies that the TSM implementing the commercial role is an independent entity accepted by both the Issuers and the MNOs.

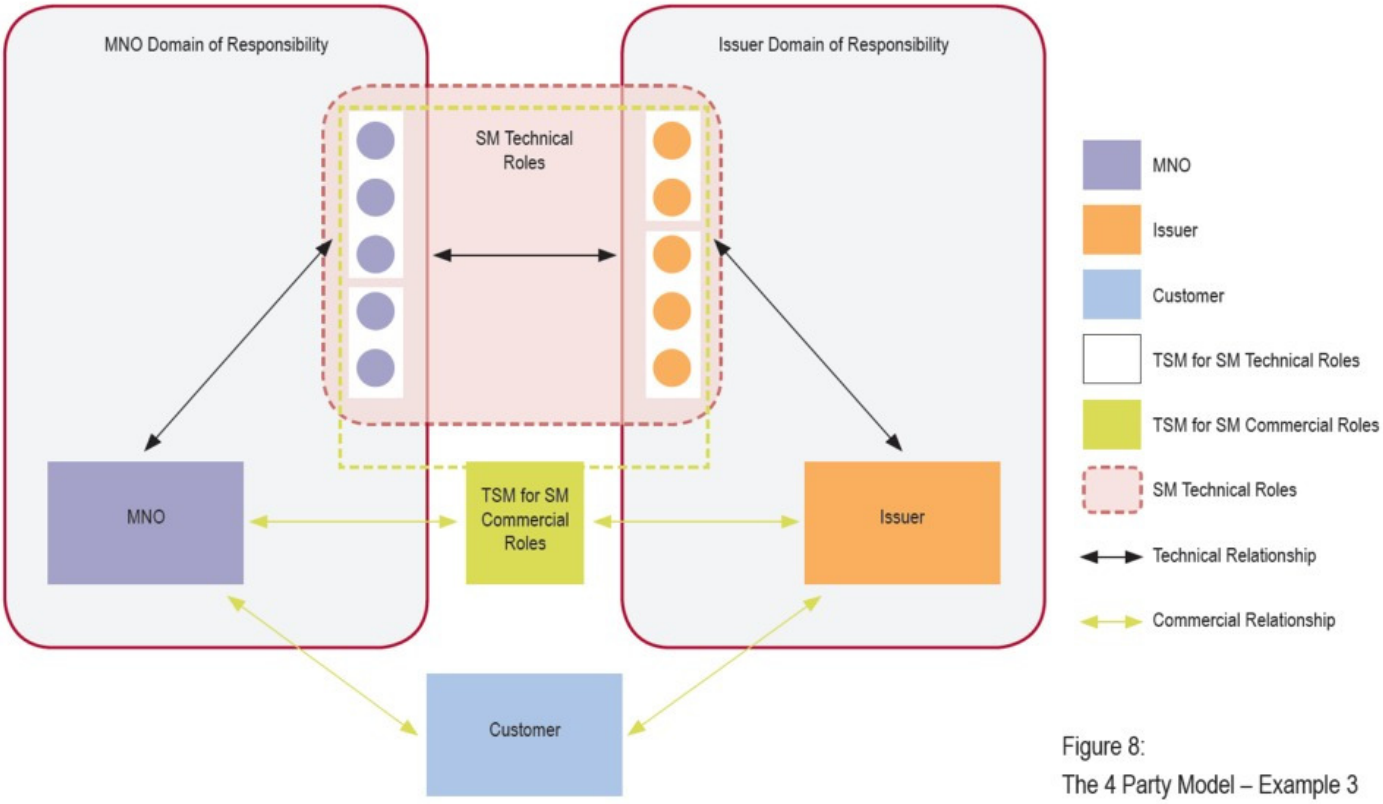


Figure 8:
The 4 Party Model – Example 3

4 Service Management

4.3.3 The Combination Model

The 3-party and 4-party models can co-exist. For instance, a MNO and a given Issuer may have a one-to-one commercial agreement (not involving any commercial TSM) while the same MNO may be connected to another Issuer via technical and commercial TSM.

4.3.4 Multiple TSM Model

The implementation of the MCP ecosystem in the real world will require the connection of multiple issuers with multiple MNOs which may involve multiple TSMs for both SM technical and/or commercial roles. This model is reflected in the following figure.

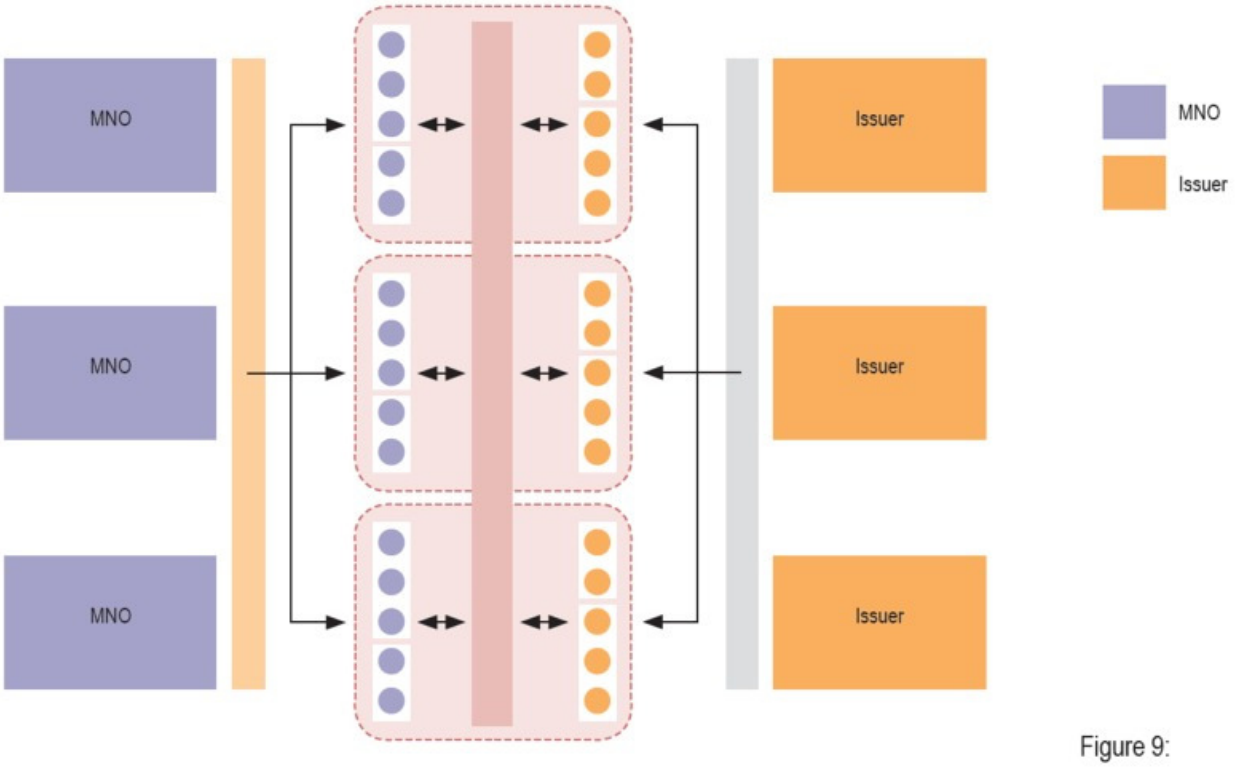


Figure 9:

Multiple TSM Model

In order to ensure interoperability between the different actors in the model depicted above a common API needs to be defined between the MNOs and the TSMs on one side, and the TSMs and the Issuers on the other side. The secure messaging specifications for these APIs are being developed by GlobalPlatform (www.globalplatform.org).

5 MCP Application Lifecycle Management

5.1 UICC management modes

In the MCP, UICC-based ecosystem, the MNO owns the UICC hosting the Issuers' MCP Application. Therefore, each MNO may choose an appropriate service model(s) and consequently select the personalisation features to be supported by the UICC and available to its partners (Issuers and TSMs). Today GlobalPlatform has specified UICC configuration scenarios that can be used to implement these service models (see [5]). These configuration scenarios address the Card Content Management which means the ability to control and manage the functions and the information on the UICC and its applications.

- Simple Mode: A MNO centric model, where Card Content Management is only performed by the MNO but can be monitored by the Issuer and/or TSM,
- Delegated Mode: Card Content Management can be delegated to an Issuer/TSM but each operation requires preauthorisation from the MNO,
- Authorised Mode: Card Content Management is fully delegated to an Issuer/TSM for a sub area of the UICC.

The requirements stated in this White Paper may change depending on which UICC management mode is being adopted. Any service management model constructed from these configuration modes shall provide the means for the MNOs to fulfil their SMRs including security and certification requirements. The delegation of some SMRs may vary according to the UICC management model chosen. The exact commands used to perform the functions will be implementation dependent.

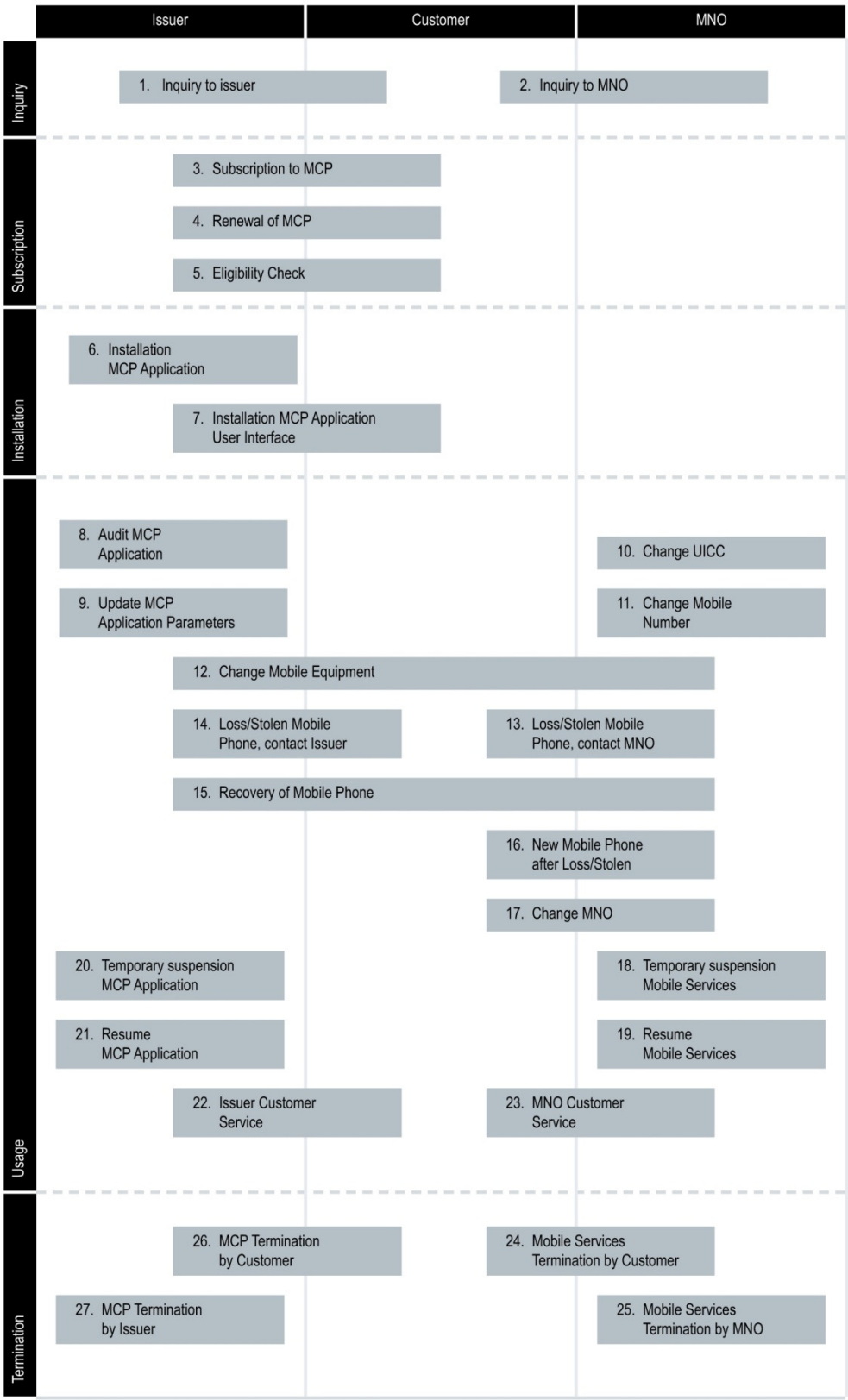
GlobalPlatform introduces the concept of Security Domains (SD) to support security services such as key handling, encryption, decryption, digital signature generation and verification for applications stored on the UICC. Supplementary Security Domains (SSD) are established on behalf of an Issuer to support the secure management of MCP applications (see [5]).

5.2 Functions

The following section describes the mainstream functions involved in an MCP Application lifecycle. The protocols used to execute the functions will typically encompass acknowledgement/confirmation on the actions.

Figure 10 provides an overview of these functions which are subsequently specified below.

Figure 10 MCP lifecycle overview



5.2.1 Eligibility Request

Typically triggered by	The Issuer requests an eligibility report from the MNO to ascertain that the Customer's Mobile Phone is technically able to receive the payment service.	
Description	MNO	Provides the appropriate information to the Issuer, including: • MNO approval, in this case the MNO provides audit information including a Technical Identifier and all relevant UICC and available Mobile Equipment references. • MNO decline, in this case the MNO provides the reason for refusal (to the extent allowed by applicable privacy legislation), in which case the Issuer does not proceed to 5.2.2.
	Issuer	Informs the Customer about the new payment service acceptance or rejection (e.g., if the UICC is no longer certified, inform the Customer about the new payment service conditions).
	Customer	Contacts the MNO as appropriate in case of rejection

5.2.2 Installation of MCP Application

Typically triggered by	After confirmation of eligibility (5.2.1) in the following cases: • New contract subscription by the Customer with the Issuer. • Renewal (e.g., broken UICC, expired UICC certificate) or change (e.g., in case of change of MNO) of the UICC. • Renewal of outdated MCP Application (performed after 4.1.6)	
Description	Issuer	• Checks if it owns an SSD on the UICC. If not, the Issuer requests the MNO to create its dedicated SSD (see section 6, MR.4 and MR.5). • Loads the MCP Application via OTA, • Personalises the MCP Application for the Customer via OTA.

Other installation models might exist, such as preloading, or loading via another channel, e.g., Bluetooth, NFC, but the loading will always remain under the responsibility of the Issuer.

5 MCP Application Lifecycle Management

5.2.3 Installation of MCP Application User Interface

Typically triggered by	Finalisation of installation of MCP Application (see 5.2.2)	
Description	Issuer	Installs the MCP Application User Interface on the Mobile Equipment. This might require User interaction depending on the actual implementation.
	Customer	Requests the activation of the MCP Application, which is then operational.

5.2.4 Update of MCP Application Parameters

Typically triggered by	Issuer requests an update of MCP Application Parameters (e.g., update of internal parameters such as the application counters or an update (reload/upload) of the off-line balance value pre-authorised).	
Description	Issuer	Updates the MCP Application parameters via OTA or alternatively, via NFC (e.g., using an additional "tap" at POI).

5.2.5 Deletion of MCP Application

Typically triggered by	• The mobile service contract is terminated. • The MCP service contract is terminated. • The contract between Issuer and MNO is terminated. • The MCP Application is outdated. • The UICC is outdated. • The Customer requests the deletion of the MCP Application.	
Description	Issuer	Removes the payment application(s) and related data from the UICC via OTA.

5 MCP Application Lifecycle Management

5.2.6 Deletion of MCP Application User Interface

Typically triggered by	Deletion of MCP Application (see 5.2.5)	
Description	Issuer/ Customer	Depending on the actual implementation, the MCP Application User Interface is removed by the Issuer or Customer (e.g., in case of an Issuer midlet)

5.2.7 Block MCP Application

Typically triggered by	• The Customer's Mobile Phone has been stolen or lost. • The Issuer temporarily suspends the MCP service subsequent to for example:, - Fraudulent behaviour against the Issuer; - Reaching the upper bound for consecutive wrong MCP Personal Code entries by the Customer; - The suspension of the MNO mobile service.	
Description	Issuer	The Issuer instructs the MCP Application to block itself in the UICC: triggered either locally or remotely via OTA.

5.2.8 Unblock MCP Application

Typically triggered by	• The Customer has recovered the Mobile Phone or the UICC. • The MNO reactivates after a temporary mobile service suspension (e.g., subsequent to a Customer's request) (see 5.2.7). • The Issuer reactivates after a temporary mobile service suspension (e.g., subsequent to Customer's request) (see 5.2.7).	
Description	Issuer	Unblocks the MCP Application via OTA.

5 MCP Application Lifecycle Management

5.2.9 "Block Mobile Network Connectivity" Notification

Typically triggered by	• The Customer's Mobile Phone has been stolen or lost.. • The MNO temporarily suspends the mobile service (e.g., this might be subsequent to a Customer's request).	
Description	MNO	The MNO informs the Issuer in accordance with the SLA (see section 8). Blocks the network connectivity at the MNO server-side after the agreed time window with the Issuer (see 6.2.4 and 7.2.4). As a result OTA is no longer available to the Issuer for MCP Application management.

5.2.10 "Unblock Mobile Network Connectivity" Notification

Typically triggered by	• The Customer has recovered the Mobile Phone or the UICC. • The MNO reactivates after a temporary mobile service suspension (e.g., subsequent to a Customer's request) (see 5.2.9).	
Description	MNO	• Unblocks the network connectivity at the MNO server-side and as a result OTA is available to the Issuer for MCP Application management. • The MNO informs the Issuer in accordance with the SLA (see 6.2.4 and 7.2.4).

5.2.11 Audit MCP Application

Typically triggered by	• The Issuer's request, depending on its MCP security requirements (e.g., checking unexpected Customer behaviour, confirmation of update actions, MCP personalization error analysis) during the operational lifecycle of the MCP Application. • The Issuer requests information on MCP Application data (e.g., management of the "off-line balance" amount in case of pre-paid).	
Description	Issuer	Retrieves MCP Application data via OTA or, alternatively via NFC.

5 MCP Application Lifecycle Management

5.2.12 Audit UICC

Typically triggered by	Some UICC checks to be performed by the MNO may be required by the Issuer before the load of an MCP Application, after its removal, or to update or synchronise relevant UICC information with the information stored on a server.	
Description	Issuer	• Retrieves information about the state of all MCP Applications related to the Issuer, including SSDs on the UICC, in particular: - If the MCP Application is loaded (after MCP Application issuance); - If the MCP Application is not loaded (before MCP Application issuance or after removal); - If the Issuer SSD exists and is personalised, before MCP Application loading. • Retrieves information about the UICC resources: - The size of free memory on the UICC available to the Issuer for MCP Applications to be loaded on the UICC, before and after any operation that requires or de-allocates memory resources of the UICC.

5.3 MCP Application Lifecycle Procedures

This section provides an overview of the different processes involved in the management of an MCP Application between the different actors: 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 Issuers and MNOs.

The numbers of the processes described below refer to Figure 10.

5 MCP Application Lifecycle Management

In the following sub-sections the MCP life-cycle steps and process are generically described. Process numbers do not denote sequential order; actual order is in introduced in a per-scenario basis in Annex I (section 10) and summarized in section 5.4.

5.3.1 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 Issuer.
- **Process 2:** The Customer requests information regarding MCP Services/Applications from the MNO. The MNO refers the Customer to the Issuer.

5.3.2 Step 2: Subscription to MCP Application

- **Process 3:** The Customer subscribes to a MCP Application with the Issuer
  - **Scenario 1** – The Customer subscribes to a first MCP Application from a given Issuer for a given UICC.
  - **Scenario 2** – The Customer subscribes to the addition of a new MCP Application to the UICC form the same Issuer.
- **Process 4:** The Customer replaces/renews the current MCP Application with a new one on the same UICC. The Issuer proposes to renew the Customer's existing application or proposes a new one.
- **Process 5:** The Issuer 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 + UICC).

5.3.3 Step 3: Installation of the MCP Application

- **Process 6:** The Issuer installs the MCP Application on the Customer's Mobile Phone.
- **Process 7:** The Issuer installs the MCP Application User Interface. This might involve the Customer.

5.3.4 Step 4: Usage of the MCP Application

- **Process 8:** The Issuer checks the status of the MCP Application on the UICC.
- **Process 9:** The Issuer updates the MCP Application (parameters).
- **Process 10:** The Customer changes the UICC.
- **Process 11:** The Customer changes mobile phone number (the Customer keeps the same UICC and MNO)

5 MCP Application Lifecycle Management

- **Process 12:** The Customer changes Mobile Equipment

  - **Scenario 1:** The new Mobile Equipment is unable to work with the UICC. The Customer contacts the MNO's help desk.

  - **Scenario 2:** The new Mobile Equipment works with the UICC. The MNO being informed about the new Mobile Equipment (via any technical means), informs the Issuer accordingly.

  - **Scenario 2a:** The new Mobile Equipment detects the MCP Application on the UICC, and triggers the download of the MCP Application User Interface by the Issuer.

  - **Scenario 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 Issuer'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 Issuer'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 Issuer as appropriate.
- **Process 16:** Following the loss (or theft) of the Mobile Phone, the Customer gets a new Mobile Equipment and a new UICC.
- **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 Issuer temporarily suspends the MCP service
- **Process 21:** Following the suspension of the MCP Application, the Issuer resumes the MCP Application.
- **Process 22:** The Customer contacts the Issuer's help desk.
- **Process 23:** The Customer contacts the MNO's help desk.

5.3.5 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 Issuer terminates the MCP Application.

5 MCP Application Lifecycle Management

5.4 Mapping of MCP Lifecycle Processes versus MCP Application Functions

The following table maps the processes described in section 5.3. onto the functions provided in section 5.1. Functions & process mentioned between parentheses are optional. Next the process is introduced for reference purposes only; it depends on the actual scenario where the initiation process is inscribed.

Phase	Processes	Functions
Inquiry	1 Inquiry to Issuer	
	2 Inquiry to MNO	
Subscription	3 Subscription to MCP Application	
	4 Renewal of MCP Application	Audit MCP Application→ Audit UICC→ Deletion of MCP Application→ Installation of MCP Application
	5 Eligibility check	Eligibility Request
Installation	6 Install MCP Application	Installation of MCP Application
	7 Install MCP Application User Interface	Installation of MCP Application User Interface
Usage	8 Audit MCP Application	Audit MCP Application
	9 Update MCP Application Parameters	Update of MCP Application Parameters
	10 Change UICC	
	11 Change Mobile Number	
	12 Change Mobile Equipment	Eligibility Request
	13 Loss/Stolen Mobile Phone-contact MNO	
	14 Loss/Stolen Mobile Phone- contact Issuer	Block MCP Application
	15 Recovery of Mobile Phone	
	16 New Mobile Phone after loss/stolen	Eligibility Request
	17 Change MNO	
	18 Temporary Mobile Services suspension	"Block Mobile Network Connectivity" Notification
	19 Resume Mobile Services	"Unblock Mobile Network Connectivity" Notification
	20 Temporary MCP Application suspension	Block MCP Application
	21 Resume MCP Application	Unblock MCP Application
	22 Issuer Customer Service	
	23 MNO Customer Service	
Termination	24 Mobile Service Termination by Customer	
	25 Mobile Service termination by MNO	"Block Mobile Network Connectivity" Notification
	26 MCP Application termination by Customer	
	27 MCP Application termination by the Issuer	Deletion of MCP Application→ (Deletion of MCP Application User Interface)

6 Requirements for Service Management in the MNO Domain

Section 6.1 introduces the formal description of the SMR in the MNO domain. Thereafter, for each step of the MCP services lifecycle, three types of Requirements are defined:

- Functional & Technical Requirements
- Security Requirements
- Legal Requirements

For each SMR requirement, MNOs can decide to execute the related developments and operations themselves or to subcontract them to one or more TSMs.

6.1 Service Management Roles in the MNO domain

#	MR.1
Role name	UICC security policy definition
Definition	This UICC security policy is defined by the MNO in alignment with Issuers and Card Schemes. It includes the protection profile for the UICC based on security requirements specified by the MNO, Issuers and Card Schemes (see section 3.4). This protection profile defines the implementation rules of the UICC (Hardware and Software) to be done by the UICC manufacturers. It includes end-to-end security management (UICC input/output + UICC internal management).
Responsibility	Defined by the MNO
Triggered by	New threats, new security requirements, e.g., due to changed environment.
Functions	

6 Requirements for Service Management in the MNO Domain

#	MR.2
Role name	UICC certification & Mobile Equipment verification (standards and interoperability)
Definition	Steps: 1. UICC. Obtain and maintain the certification of the UICC platform. Usually, this is done by accredited independent entities (e.g. via the Common Criteria process and a defined Protection Profile, via the Card Schemes or via EMVCo) and is only done when a new UICC platform is released. 2. Mobile Equipment. Pass the Mobile Equipment through the usual GCF (Global Certification Forum) and MNO tests (including the NFC Interface).
Responsibility	The MNO is responsible. Tests performed by independent TPs (typically a certification lab that is independent from a TSM)
Triggered by	New UICC New Mobile Equipment.
Functions	

#	MR.3
Role name	Management of the list of Issuer MCP Applications stored on the UICC
Definition	The purpose is to handle on the MNO server the list of MCP Applications currently installed in any UICC (including data such as Issuer, AID, Version, and Status). This list is typically used for UICC re-issuance in case of loss and it is especially useful in case of multiple TSM doing the SMR for Issuers.
Responsibility	The MNO is responsible. Can be operated by the MNO or a TSM
Triggered by	Issuance
Functions	5.2.12

6 Requirements for Service Management in the MNO Domain

#	MR.4
Role name	Creation of the Issuer Supplementary Security Domain (SSD)
Definition	The Creation of the SSD is done by the UICC manufacturer, MNO or TSM. This entity generates the temporary SSD keysets after the SSD creation and pushes it onto the new SSD. For each SSD, only one entity (which could be the MNO or the TSM depending on the management model implemented) is able to manage the SSD (e.g., SSD deletion, blocking/unblocking, etc.).
Responsibility	The MNO is responsible. Can be operated by the MNO or a TP (e.g., a TSM or UICC manufacturer)
Triggered by	Issuance
Functions	5.2.2

#	MR.5
Role name	Management of Secure Keysets(for pre-created SSD keysets)
Definition	This role is linked to “Issuer SSD creation” and “SSD assignment” roles. The entity performing this role (e.g., UICC manufacturer) keeps secret keysets of pre-created SSDs(e.g., in factory) and provides these temporary keysets to the Issuer once this Issuer has a contract with the MNO so that the Issuer can change the keysets values making sure the MNO cannot access the final keysets values.
Responsibility	The MNO is responsible. It is operated by a TP (e.g., a UICC manufacturer)
Triggered by	Issuance
Functions	5.2.2

#	MR.6
Role name	Assignment of SSD
Definition	To link the SSD AID to an Issuer, the following steps are needed: 1.Transmit the temporary SSD keyset to the Issuer SSD Manager for its replacement (only in the dynamically created SSD case) 2. Link the SSD Application Identifier (AID) to the Issuer in the MNO information system. 3. Set the SSD privilege (Simple Mode, Delegated Mode, Authorised Mode – see 5.1)
Responsibility	The MNO is responsible Can be operated by the MNO or a TSM
Triggered by	Issuance
Functions	5.2.2

6 Requirements for Service Management in the MNO Domain

#	MR.7
Role name	Management of the UICC Memory
Definition	The MNO is the only entity with the overall mapping of the memory allocation on the UICC. For instance this feature can be used as criteria to perform an eligibility check on the memory status before a MCP Application download request is performed by the Issuer. Also, the MNO can trigger a remote UICC memory audit.
Responsibility	The MNO is responsible. Can be operated by the MNO or a TSM
Triggered by	Issuance or Customer preference.
Functions	5.2.1, 5.2.2, 5.2.12

#	MR.8
Role name	Contractual and technical pre-controls - eligibility of Issuer and Customers to the MNO service related to MCP.
Definition	Issuers' operations on the UICC may require that the MNO checks: 1. The contractual eligibility of Issuer and Customers to the MNO service. • If the contract established between the MNO and the Issuer and/or its subcontractors is still valid. • The target Customer has a valid mobile subscription (allowing the access to the MNO Service). 2. The technical eligibility of the Customer's Mobile Phone to the MNO service • The technical configuration of the UICC makes MCP possible (for instance if the UICC is a NFC UICC, free memory is sufficiently available, and the UICC certificate is valid). • The technical configuration of the Mobile Equipment makes it possible (NFC capabilities only). When contractual and technical eligibility pre-controls are satisfactory, the requested operation can be achieved.
Responsibility	The MNO is responsible. Can be operated by the MNO or a TSM
Triggered by	Issuance
Functions	5.2.1

6 Requirements for Service Management in the MNO Domain

#	MR.9
Role name	Management of the OTA NFC application on behalf of Issuers (Simple Mode)
Definition	In Simple Mode, the MNO implements the following functions on behalf of the Issuer in compliance with the security policy (see MR.1): 1. MCP Application approval control. 2. MCP Application load, install, activate, remove.
Responsibility	The MNO is responsible. Can be operated by the MNO or a TSM
Triggered by	Issuance and post-Issuance.
Functions	5.2.2, 5.2.4, 5.2.5, 5.2.7, 5.2.8, 5.2.11

#	MR.10
Role name	MNO hotline/customer service.
Definition	Performed by the MNO to support the Customer before and after sale. The MNO Customer Service is linked with the Issuer Customer Service in order to coordinate and synchronise answers to Customers, as appropriate.
Responsibility	The MNO is responsible. Can be operated by the MNO or a TSM
Triggered by	Issuance and post-Issuance
Functions	

#	MR.11
Role name	Management of Customer lifecycle events.
Definition	Recording of events and taking appropriate actions with the Issuer and Customer. • Termination / change – of mobile subscription – of MCP Services contract between the Issuer and Customer • Loss and theft of Mobile Phone • Mobile Equipment change • UICC change • Mobile suspension • Change of phone number (MSISDN) • Change of installed Issuer MCP Application
Responsibility	The MNO is responsible. Can be operated by the MNO or a TSM
Triggered by	Issuance and post-issuance
Functions	

6 Requirements for Service Management in the MNO Domain

6.2 Functional and Technical Requirements

6.2.1 Information Systems

#	Mandatory/ Optional	Requirement	Applies to Rules
M.1.1.1	M	The MNO MCP service management information system SHALL be connected to each individual Issuer MCP service management information system either directly or via the TSM(s).	MR.3, MR.4, MR.5, MR.6, MR.7, MR.9, MR.10, MR.11
M.1.1.2	O	The connection between the MNO and Issuer information systems for MCP service management SHOULD be done through an efficient integration process using common interfaces.	MR.4, MR.5, MR.6, MR.7, MR.9, MR.10, MR.11
M.1.1.3	M	The MNO SHALL provide an OTA to connect to the Customer and his/her Mobile Phone in support of MCP service management.	MR.10

6.2.2 MCP Services pre-issuance management

#	Mandatory/ Optional	Requirement	Applies to Rules
M.1.2.1	M	• The MNO SHALL provide the Issuers with the necessary information for the development of the MCP service, including the UICC MCP Application and the related Mobile Phone user interface application(s). More in particular, the requirements certification and interoperability SHALL be provided.	MR.1, MR.2
M.1.2.2	M	The MNO SHALL be responsible for the functional certification (type approval) of its UICC. The MNO SHALL be responsible for the security certification of its UICC. However, a process SHALL also be defined (e.g., Composite Evaluation) to ensure that the certification is maintained when applications are loaded post-issuance. At the time of writing this document, processes to certify UICCs for NFC services are being developed.	MR.1, MR.2
M.1.2.3	M	The MNO SHALL be responsible for certification of the following SM service processes: • MR.3 - Management of the list of Issuers MCP Applications stored on the UICC (server list) • MR.4 - Issuer Supplementary Security Domain (SSD) Creation • MR.6 - SSD Assignment • MR.7 - UICC Memory Management • MR.9 - OTA NFC application management on behalf of Issuers (simple mode)	MR.3, MR.4, MR.5, MR.6, MR.7, MR.9

#	Mandatory/ Optional	Requirement	Applies to Rules
M.1.2.4	M	The MNO SHALL be responsible that the usual GCF and MNO tests are passed by the Mobile Equipment manufacturer. This SHALL include the NFC interface.	MR.2
M.1.2.5	M	The MNO SHALL provide a list of supported NFC Mobile Equipment to the Issuers.	MR.2
M.1.2.6	M (in Simple Mode)	The MNO SHALL control the MCP Application approval on behalf of the Issuer in compliance with the security policy (see MR.1).	MR.9

6.2.3 MCP Service issuance management

#	Mandatory/ Optional	Requirement	Applies to Rules
M.1.3.1	M	The MNO SHALL provide the eligibility report regarding a customer upon request from the Issuer as specified in section 5.2.1.	MR.8
M.1.3.2	M	The MNO SHALL provide the MNO's customer technical ID to the Issuer for the MCP service as specified in section 5.2.1.	MR.8
M.1.3.3	M	The MNO SHALL be able to support at least one of the management modes as defined by the GlobalPlatform (see [4] and [5]) (see M.4.2) and supported by the Issuers.	MR.4, MR.5, MR.6, MR.8, MR.9, MR.11
M.1.3.4	M	The MNO SHALL enable the Issuer to load the MCP Application onto the Customer's Mobile Phone (function 5.2.2 in section 4).	MR.4, MR.5, MR.6, MR.9
M.1.3.5	M (in Simple Mode)	The MNO SHALL load, install and activate the MCP Application on behalf of the Issuer in compliance with the security policy (see MR.1).	MR.9
M.1.3.6	M	The MNO SHALL implement the necessary processes to maintain a customer's MCP service (e.g. for service improvement, bug correction, etc.)	MR.10, MR.11

6 Requirements for Service Management in the MNO Domain

6.2.4 MCP Service post-issuance management

#	Mandatory/ Optional	Requirement	Applies to Rules
M.1.4.1	M	The MNO SHALL be able to manage the memory of the UICC.	MR.7
M.1.4.2	M	The MNO SHALL be able to manage a list of all MCP Applications stored on the UICC.	MR.3
M.1.4.3.	M	The MNO SHALL enable the Issuer to manage the MCP Application onto the Customer's Mobile Phone (functions 5.2.4 through 5.2.11 in section 4).	MR.9
M.1.4.4	M (in Simple Mode)	The MNO SHALL remove the MCP Application on behalf of the Issuer in compliance with the security policy (see MR.1).	MR.9
M.1.4.5	M	The MNO SHALL inform the Issuer of the re-issuance of the UICC to a customer (e.g. after theft/loss of the mobile phone and UICC).	MR.11
M.1.4.6	M	The MNO SHALL inform the Issuer when a Customer's mobile service contract is terminated.	MR.11
M.1.4.7	M	The MNO SHALL enable the Mobile Equipment to display all MCP Applications with associated metadata (logo, status and label) to the Customer	MR.10
M.1.4.8	M	The MNO SHALL enable the Customer to activate and deactivate an MCP Application.	MR.10, MR.11
M.1.4.9	M	The MNO SHALL provide a mechanism to enable the MCP Application to remain active even if the MNO Network Connectivity has been blocked, subject to SLA6.	MR.10
M.1.4.10	M	The MNO SHALL enable the Customer to choose the MCP Application before payment.	MR.3
M.1.4.11	M	The MNO SHALL enable the Customer to manage the MCP Application preference list.	MR.3

6 Requirements for Service Management in the MNO Domain

6.3 Security Requirements

#	Mandatory/ Optional	Requirement	Applies to Rules
M.2.1	M	The MNO SHALL be responsible for compliance to the UICC security policy (see 6.1).	MR.2
M.2.2	M	The MNO SHALL be responsible for the creation of the Supplementary Security Domains (SSD) as appropriate.	MR.4
M.2.3	M	The MNO SHALL be responsible for establishing a process agreed with the Issuer whereby SSDs can be transferred to issuers with keysets that are not known to MNOs to allow Issuer to transfer and protect confidential data and code.	MR.5
M.2.4	M	The MNO SHALL ensure the security of the Customer information it has access to. The MNO SHALL ensure any information within the MCP Application and MCP Transaction SHALL NOT be visible or available to the MNO.	MR.4, MR.5, MR.6, MR.7, MR.8, MR.9, MR.10, MR.11
M.2.5	M	The MNO SHALL provide evidence that its security requirements that • enable MCP applications to be securely stored on the UICC, • enable third party applications to be securely stored /downloaded on a UICC, • enable the security between each stored application (i.e. no interference between applications stored on the UICC), are met, as described by its Security Policy.	MR.1

6.4 Legal Requirements

#	Mandatory/ Optional	Requirement	Applies to Rules
M.3.1	M	The MNO SHALL comply with the applicable laws and regulations with regards to data protection and privacy of the personal data corresponding to a Customer.	MR.3, MR.4, MR.5, MR.6, MR.7, MR.8, MR.9, MR.10, MR.11

7 Requirements for Service Management in the Issuer Domain

Section 7.1 introduces the formal description of the SMR in the Issuer domain. Thereafter, for each step of the MCP services lifecycle, three types of Requirements are defined:

- Functional & Technical Requirements (including security Requirements)
- Security Requirements
- Legal Requirements

For each SMR requirement, Issuers can decide to execute the related developments and operations themselves or to subcontract them to one or more TSMs.

7.1 Service Management Roles in the Issuer domain

#	IR.1
Role Name	Development of MCP Application
Definition	Development of the MCP Application to be stored and executed in the UICC according to technical, security and functional requirements provided by the Card Schemes & MNOs
Responsibility	The Issuer is responsible Can be operated by the Issuer or a TP
Triggered by	New UICC platform New MCP Application functionalities
Functions	

#	IR.2
Role Name	Development of MCP Application User Interface
Definition	Development of the MCP Application User Interface (see 3.8) according to technical and functional requirements. This User Interface could be stored in the Mobile Equipment (midlet) or in the UICC.
Responsibility	The Issuer is responsible Can be operated by the Issuer or a TP
Triggered by	New platform (Mobile Equipment) New functionalities
Functions	

7 Requirements for Service Management in the Issuer Domain

#	IR.3
Role Name	MCP Application approval
Definition	Obtain and maintain the approval of the MCP Application. Typically, this is done by accredited independent entities (e.g. via the Common Criteria process and a defined Protection Profile, via the Card Schemes or via EMVCo) and is only done when a new MCP Application is released. In case applications are loaded post-issuance, the process defined for composite evaluations needs to be applied.
Responsibility	The Issuer is responsible but the approval is operated by a TP (typically a certification lab that is independent from a TSM).
Triggered by	New platform; New functionalities
Functions	

#	IR.4
Role Name	Data Preparation (personalisation data)
Definition	Steps: 1. Logical Data Preparation: Generation of the personalisation profile is a compilation of all payment application data defined by the Issuer (Primary Account Number (PAN), Expiration Date, etc.) and related cryptographic data using payment application keys and Issuer certificates. 2. Physical Data Preparation: Generation and transmission of Application Packet Data Unit (APDU) blocks from the logical data to the Issuer Information System or TP operating the download and personalisation roles
Responsibility	The Issuer is responsible. Can be operated by the Issuer or a TP
Triggered by	Issuance, Update personalisation data
Functions	

7 Requirements for Service Management in the Issuer Domain

#	IR.5
Role Name	Issuer SSD key management (logical and physical secure storage and delivery)
Definition	Options: • For dynamically created SSDs the Issuer creates and installs the SSD keys. • For pre-created SSDs the Issuer connects to the entity that created the SSD in order to get the temporary SSD keys and renews them.
Responsibility	The Issuer is responsible. Can be operated by the Issuers or a TSM
Triggered by	Issuance
Functions	5.2.2

#	IR.6
Role Name	Download and Installation of MCP Application[2].
Definition	Downloading and Installing of the MCP Application onto the UICC after successful verifications, as appropriate. Options: • Simple mode. The MCP Application is first transmitted to the MNO, who then performs the download and install. • Authorised Management or Delegated Management The MCP Application is directly transmitted to the UICC (once the technical rights are granted by the MNO to the Issuer)
Responsibility	The Issuer is responsible. Can be operated by the Issuer or a TSM
Triggered by	Issuance
Functions	5.2.2

[2] The MCP Application can also be preloaded on the UICC

7 Requirements for Service Management in the Issuer Domain

#	IR.7
Role Name	Download of MCP Application User Interface
Definition	The MCP Application User Interface is downloaded and could be stored in the Mobile Equipment or on the UICC. The MCP Application User Interface download is not necessarily linked to the MCP Application download.
Responsibility	The Issuer is responsible. Can be operated by the Issuers or a TSM. This might involve the Customer.
Triggered by	Issuance
Functions	5.2.3

#	IR.8
Role Name	Personalisation of MCP Application
Definition	The Issuer personalises the MCP Application using the data defined by the Data Preparation role (IR.4).
Responsibility	The Issuer is responsible Can be operated by the Issuer or a TP
Triggered by	Issuance Update personalisation data
Functions	5.2.2, 5.2.4

#	IR.9
Role Name	Activation of MCP Application
Definition	The activation of the MCP Application is dependent on the UICC management mode chosen. Options: • Simple mode The Issuer requests the MNO to activate the MCP Application. • Delegated management or Authorised management The MCP Application is directly activated by the Issuer (once the technical rights are granted by the MNO)
Responsibility	The Issuer is responsible Can be operated by the Issuer or a TSM
Triggered by	Issuance
Functions	5.2.2

7 Requirements for Service Management in the Issuer Domain

#	IR.10
Role Name	OTA functional management of the MCP Application (including application download/update/deletion)
Definition	The OTA functional management of the MCP Application is dependent on the UICC management mode chosen. Options: • Simple mode. The Issuer requests the MNO to manage the application. • Delegated management or Authorised management The MCP Application is directly managed by the Issuer (once the technical rights are granted by the MNO)
Responsibility	The Issuer is responsible Can be operated by the Issuer or a TSM
Triggered by	Post Issuance events
Functions	5.2.2, 5.2.5, 5.2.11

#	IR.11
Role Name	OTA applicative management of the MCP Application (including application lock/unlock and excluding application download/update/deletion)
Definition	Initialising the payment application management operations (counter reset, script processing, application audit, etc.).
Responsibility	The Issuer is responsible Can be operated by the Issuer or a TSM
Triggered by	Post issuance events
Functions	5.2.4, 5.2.7, 5.2.8

#	IR.12
Role Name	Issuer Hotline/Customer service
Definition	Performed by the Issuer to support the Customer before and after issuing the MCP Application. The Issuer customer service is linked with the MNO customer service in order to coordinate and synchronise answers to Customers, as appropriate.
Responsibility	The Issuer is responsible Can be operated by the Issuer or a TSM
Triggered by	Issuance Post-issuance events
Functions	

7 Requirements for Service Management in the Issuer Domain

#	IR.13
Role Name	Management of Customer lifecycle events

Definition	The Issuer is responsible for taking the appropriate actions (including Customer care) after being informed by the MNO, as applicable.
	• Termination / change
	  – of mobile subscription
	  – of MCP Services contract between the Issuer and the Customer
	• Loss and theft of Mobile Phone
	• Mobile Equipment change
	• UICC change
	• Mobile services suspension
	• Change of phone number (MSISDN)
	• Change of MNO

Responsibility	The Issuer is responsible Can be operated by the Issuers or a TSM
Triggered by	Post issuance events
Functions	

7 Requirements for Service Management in the Issuer Domain

7.2 Functional and Technical Requirements

7.2.1 Information Systems

#	Mandatory/ Optional	Requirement	Applies to Rules
I.1.1.1	M	The Issuer MCP Service Management Information System SHALL be connected to each individual MNO MCP service management information systems either directly or via the TSM(s).	IR.5, IR.6, IR.7 IR.8, IR10, IR.11, IR.12, IR.13
I.1.1.2	O	The connection between MNO and Issuer information systems for MCP service management SHOULD be done through "fast integration processes" using common interfaces (see 3.11).	IR.5, IR.6, IR.7 IR.8, IR10, IR.11, IR.12, IR.13
I.1.1.3	M	The Issuer SHALL implement at least one of the following channels to connect to its Customer in support of MCP service management: • Mobile • Web • local (i.e. contactless)	IR.13

7 Requirements for Service Management in the Issuer Domain

7.2 Functional and Technical Requirements

7.2.2 MCP Services pre-issuance management

#	Mandatory/ Optional	Requirement	Applies to Rules
I.1.2.1	M	The Issuer SHALL be responsible for the development of its MCP services, including the MCP Application and the related MCP Application User Interface according to the information provided by the MNO.	IR.1, IR.2
I.1.2.2	M	The Issuer SHALL be responsible for the functional certification (type approval) of its MCP services. The Issuer SHALL be responsible for the security certification of its MCP UICC application. However, a process SHALL also be defined (e.g. composite Evaluation) to ensure that the certification is maintained when applications are loaded post-issuance. At the time of writing this document, processes to certify UICCs for NFC services are being developed.	IR.3
I.1.2.3	M	The Issuer SHALL be responsible for certification of the following SM service processes: • IR.4 - Data Preparation (personalization data) • IR.5 - Issuer SSD key management (logical and physical secure storage and delivery) • IR.6 - Issuer MCP Application installation (Download + instantiation) • IR.7 - Issuer MCP Application User Interface download • IR.8 – MCP Application personalization • IR.9 – MCP Application activation	IR.4, IR.5, IR.6, IR.7, IR.8, IR.9
I.1.2.4	M	The Issuer SHALL go through an MNO application validation process in order to guarantee that its applicative environment does not adversely impact the Mobile services and other NFC services.	IR.3

7 Requirements for Service Management in the Issuer Domain

7.2 Functional and Technical Requirements

7.2.3 MCP Service issuance management

#	Mandatory/ Optional	Requirement	Applies to Rules
I.1.3.1	M	The Issuer SHALL manage the association of the customer ID as provided by the MNO with the Customer ID assigned by the Issuer for the MCP service (this link shall be established at the time of the customer registration for the MCP service).	IR.4, IR.5, IR.6, IR.7, IR.8, IR.9, IR.10, IR.11, IR.12, IR. 13
I.1.3.2	M	The Issuer SHALL ensure that the following processes are performed in coordination with the MNO to place its MCP Application into the Customer's UICC: • Application provisioning • Application instantiation (optional) • Application personalization • Application activation The Issuer SHALL be able to support at least one of the management modes as defined by the GlobalPlatform White Paper and supported by the MNOs.	IR.8, IR.9, IR.10
I.1.3.3	M	The Issuer SHALL load its MCP Application Interface onto the Customer's Mobile Phone.	IR.7
I.1.3.4	M	The Issuer SHALL implement the necessary processes to maintain a customer's MCP service (e.g. for service improvement, bug correction, etc.)	IR.1, IR.2, IR.12

7 Requirements for Service Management in the Issuer Domain

7.2 Functional and Technical Requirements

7.2.4 MCP Service post-issuance management

#	Mandatory/ Optional	Requirement	Applies to Rules
I.1.4.1	M	The Issuer SHALL be able to remove a MCP Application from the UICC upon Customer's demand.	IR.12, IR.13
I.1.4.2	M	The Issuer SHALL be able to temporarily suspend a MCP service upon Customer's demand.	IR.12, IR.13
I.1.4.3	M	The Issuer SHALL be able to re-issue the MCP Application to a Customer in case of theft/loss of the mobile phone and UICC.	IR.4, IR.5, IR.6, IR.7, IR.8, IR.9 IR.12
I.1.4.4	M	The Issuer SHALL inform the MNO when a Customer's MCP service contract is terminated.	IR.13
I.1.4.5	M	The Issuer SHALL terminate the Customer's MCP service(s) associated with an MNO when the MNO informs the Issuer that the Customer's mobile subscription has been terminated.	IR.13

7.3 Security Requirements

#	Mandatory/ Optional	Requirement	Applies to Rules
I.2.1	M	The Issuer SHALL be responsible for the security of its MCP Application	IR.1, IR.2
I.2.2.	M	The Issuer SHALL ensure the security of the Customer mobile subscription related information that it can use and/or see. The Issuer SHALL ensure security of the data transmitted (for example via OTA) from its servers to the Customer mobile phone and UICC.	IR.4, IR.5, IR.6, IR.7, IR.8, IR.9, IR.10, IR.11, IR.12, IR.13

7.4 Legal Requirements

#	Mandatory/ Optional	Requirement	Applies to Rules
I.3.1	M	The Issuer SHALL comply with the applicable laws and regulations with regards to data protection and privacy of the personal data corresponding to a Customer.	IR.4, IR.5, IR.6, IR.7, IR.8, IR.9, IR.10, IR.11, IR.12, IR.13

8 Service Level Agreements for Service Management

In order to foster a market place with a rich set of commercial actors performing several SMRs, this document introduces a minimal scope for the SLAs between these commercial actors that can be used as common level-playing field. However, detailed terms and conditions mostly depend on bi-lateral specific deals between Issuers, MNOs and/or TSMs. Typical topics to be addressed in the SLAs should cover:

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

#	Mandatory/ Optional	Requirement	Applies to Rules
SLA.1	M	The Issuer and the MNO SHALL setup specific customer care processes in order to properly manage Customer support demand (e.g. handover to the MNO's customer care) as introduced in section 5.3.	IR.12, MR.11
SLA.2	M	The Issuer SHALL agree with the MNO which UICC Configuration Management modes are supported.	IR.1, IR.5, IR.6, IR.9, IR.10, IR.13, MR.4, MR.5, MR.6, MR.9, MR.10
SLA.3	M	The Issuer and the MNO SHALL setup the necessary information system scalability in order to deliver services to the customers under a commonly defined level of quality, which SHALL include availability, scalability and response time in accordance to section 5.1.	IR.4, IR.5, IR.6, IR.7, IR.8, IR.9, IR.10, IR.11, IR.12, IR.13, MR.3, MR.4, MR.5, MR.6, MR.7, MR.8, MR.9, MR.10, MR.11
SLA.4	M	The Issuer and the MNO SHALL mutually agree on a service model (see section 4.3). They SHALL be able to deliver, support and manage their services under a mutually defined level of agreement including liabilities.	IR.4, IR.5, IR.6, IR.7, IR.8, IR.9, IR.10, IR.11, IR.12, IR.13, MR.3, MR.4, MR.5, MR.6, MR.7, MR.8, MR.9, MR.10, MR.11,
SLA.5	M	The Issuer and the MNO SHALL set up systems allowing management of live & synchronous answers to Customers' requests (service inquiry, service provisioning request).	IR.4, IR.5, IR.6, IR.7, IR.8, IR.9, IR.10, IR.11, IR.12, IR.13, MR.3, MR.4, MR.5, MR.6, MR.7, MR.8, MR.9, MR.10, MR.11
SLA.6	M	The contract between the MNO and the Issuer SHALL address the policy for what shall happen in case of Mobile Service suspension/termination with respect to the usage of the MCP Application.	IR.13, MR.10

9 Conclusions

This document is aimed at defining the requirements and specifications for the various Service Management roles involved in the provisioning and lifecycle management of Mobile Contactless Payments (MCPs). It further provides a high-level description of the possible service models. The purpose is that it serves as a reference basis for actual implementations of MCPs and the different actors involved. The reader is also advised to consult the respective websites of EPC and GSMA for further detailed documentation related to these services.

10 Annex I - Examples of Scenarios Versus Processes

This section introduces several examples of MCP life-cycle scenarios build using the process introduced in section 5.3. For all scenarios the actual sequence of process may change in the final implementation according to the concrete Issuer's and MNO's business models.

- The scenario 10.1 introduces the standard case where a Customer enrols for the first time to the MCP Application.
- In scenario 10.2, the Customer decides to change MNO while keeping their MCP Application.
- In scenario 10.3, the Customer decides to change Mobile Equipment while keeping the MNO services and MCP Application.
- The Scenario 10.4 presents the case where a Customer loses and later recovers their Mobile Phone.
- The scenario 10.5 introduces the case where the Mobile Phone is stolen and never recovered.
- Finally scenario 10.6 an end of life-cycle example where the Customer decides to terminate the MCP Application.

10.1 A new Customer requests a new MCP Application

This is the standard scenario where a Customer requests to an Issuer to subscribe a MCP Application for the first time, the MCP Application is successfully installed, and then used for an undefined period of time. The scenario starts at process 1 or 2. During the standard usage of the MCP Applications, process 8 and 9 are executed as needed by the Issuer (see Figure 11).

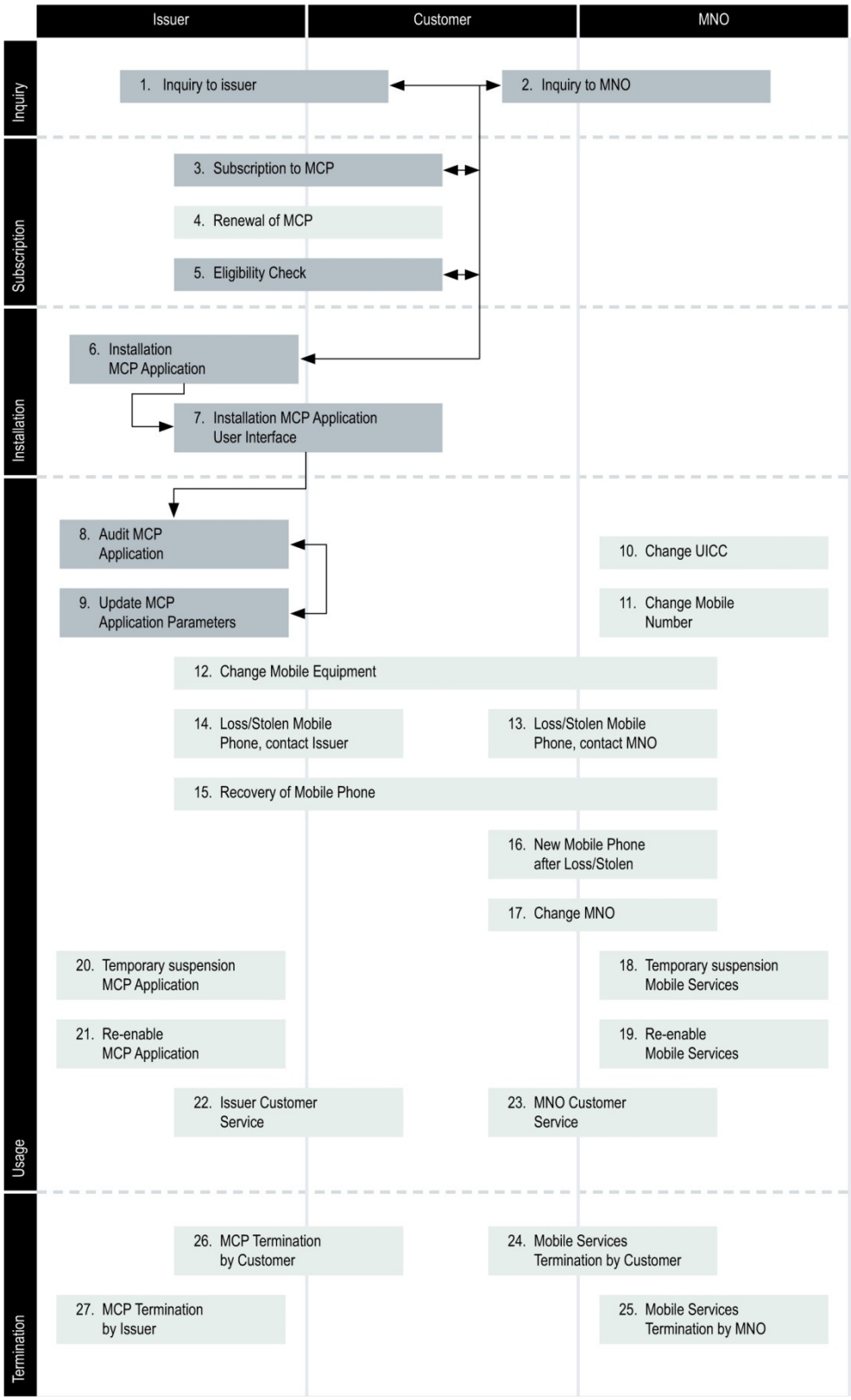


Figure 11
A new Customer requests a new MCP Application

10.2 Change by the Customer of the MNO

In this scenario the Customer decides to change MNO. The scenario starts at Process 17. Process 22 has no explicit flow arrows as it may be invoked by the Customer at any point during the scenario (see Figure 12).

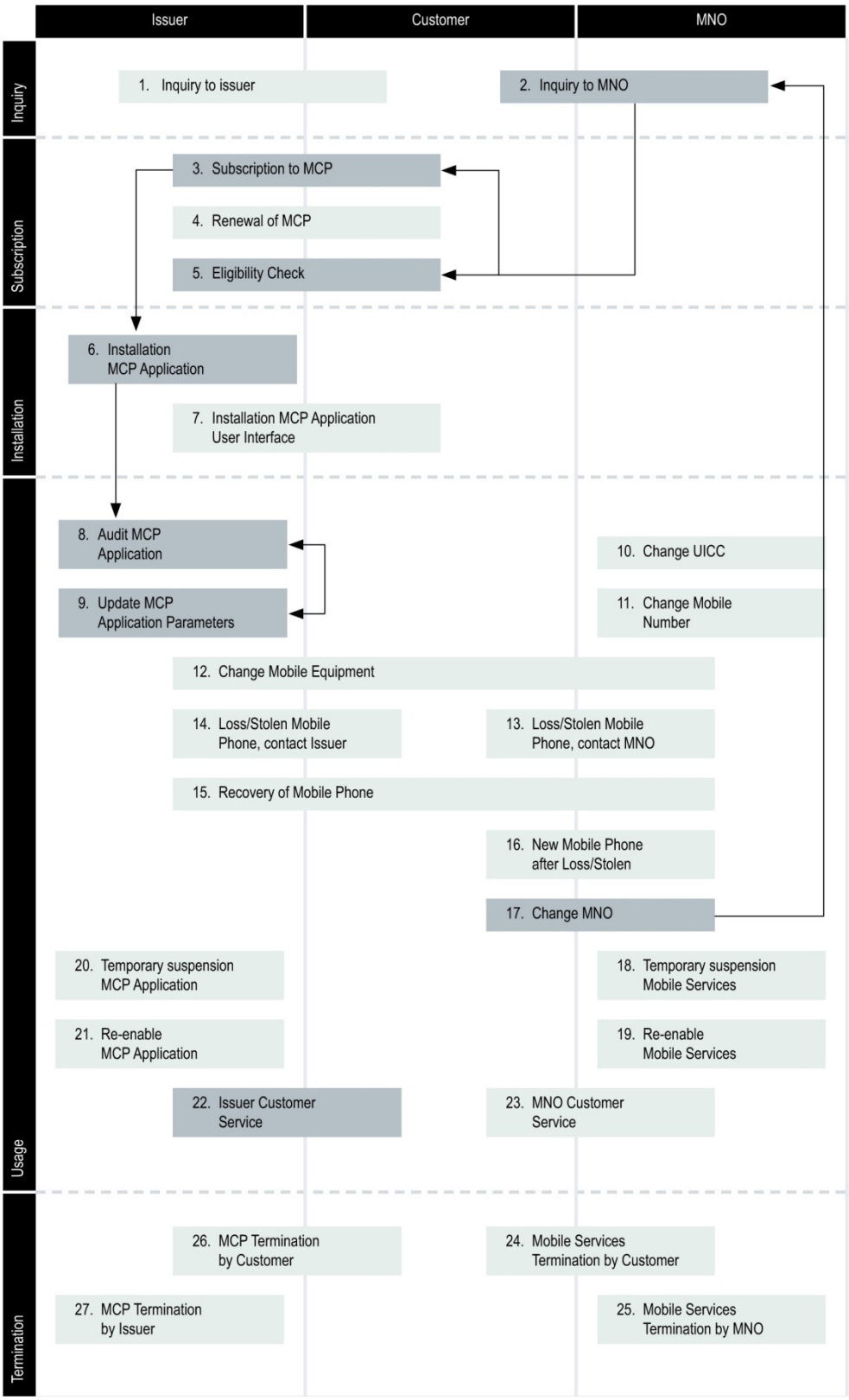


Figure 12 Change of the MNO by the Customer scenario

10.3 Change of Mobile Equipment by the Customer

In this scenario the Customer decides to update the Mobile Equipment. The scenario starts at process 12 (see Figure 13).

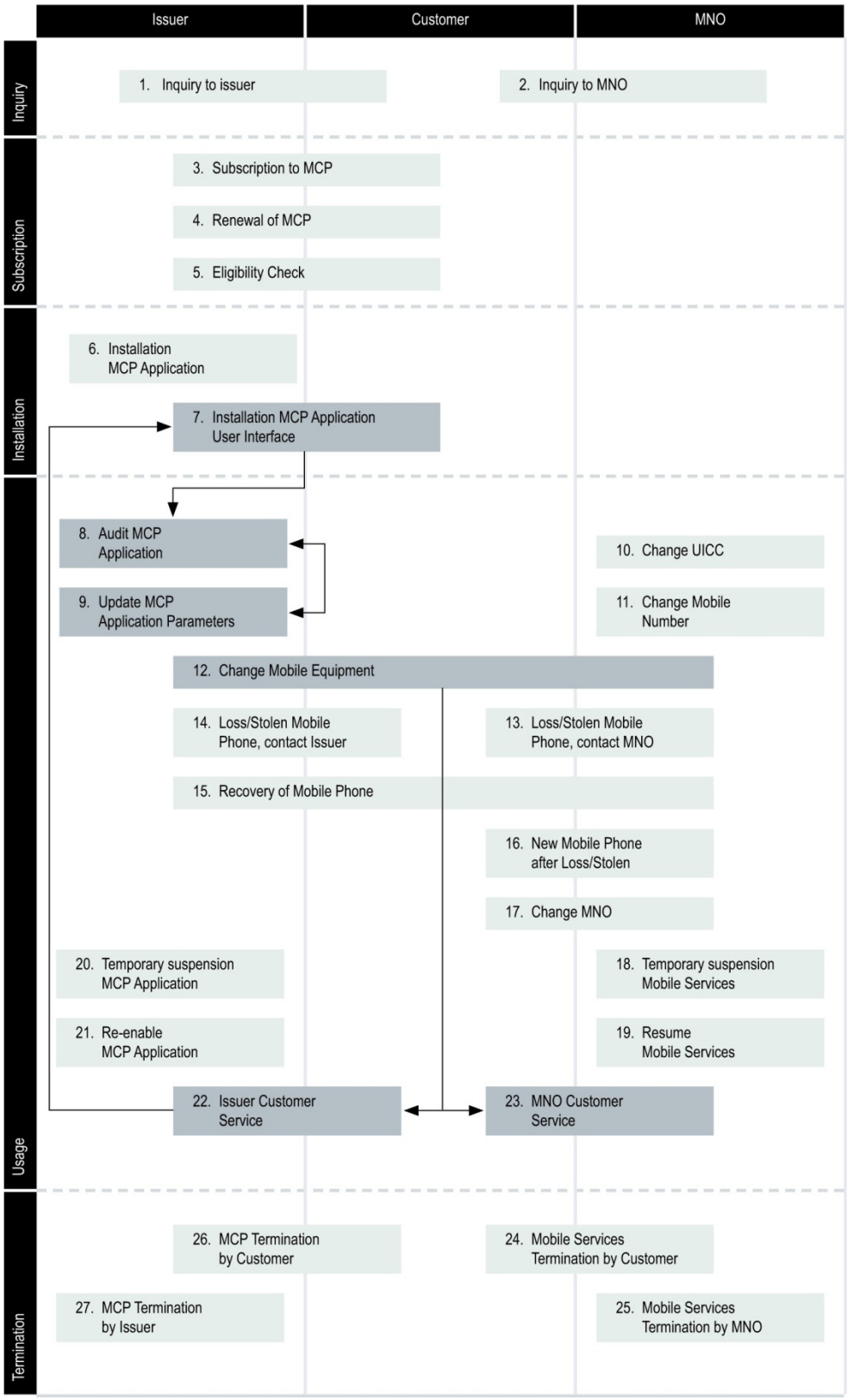


Figure 13 Change of Mobile Equipment by the Customer scenario

10.4 Loss and recovery of Mobile Phone

In this scenario the Customer first loses the Mobile Phone but later is able to recover it. In this particular case, when the Mobile Phone is lost the scenario starts at Processes 14. Thereafter, when the Mobile Phone is recovered the scenario re-starts at Process 15. Process 22 and 23 have no explicit flow arrows as they may be invoked by the Customer at any point during the scenario (see Figure 14).

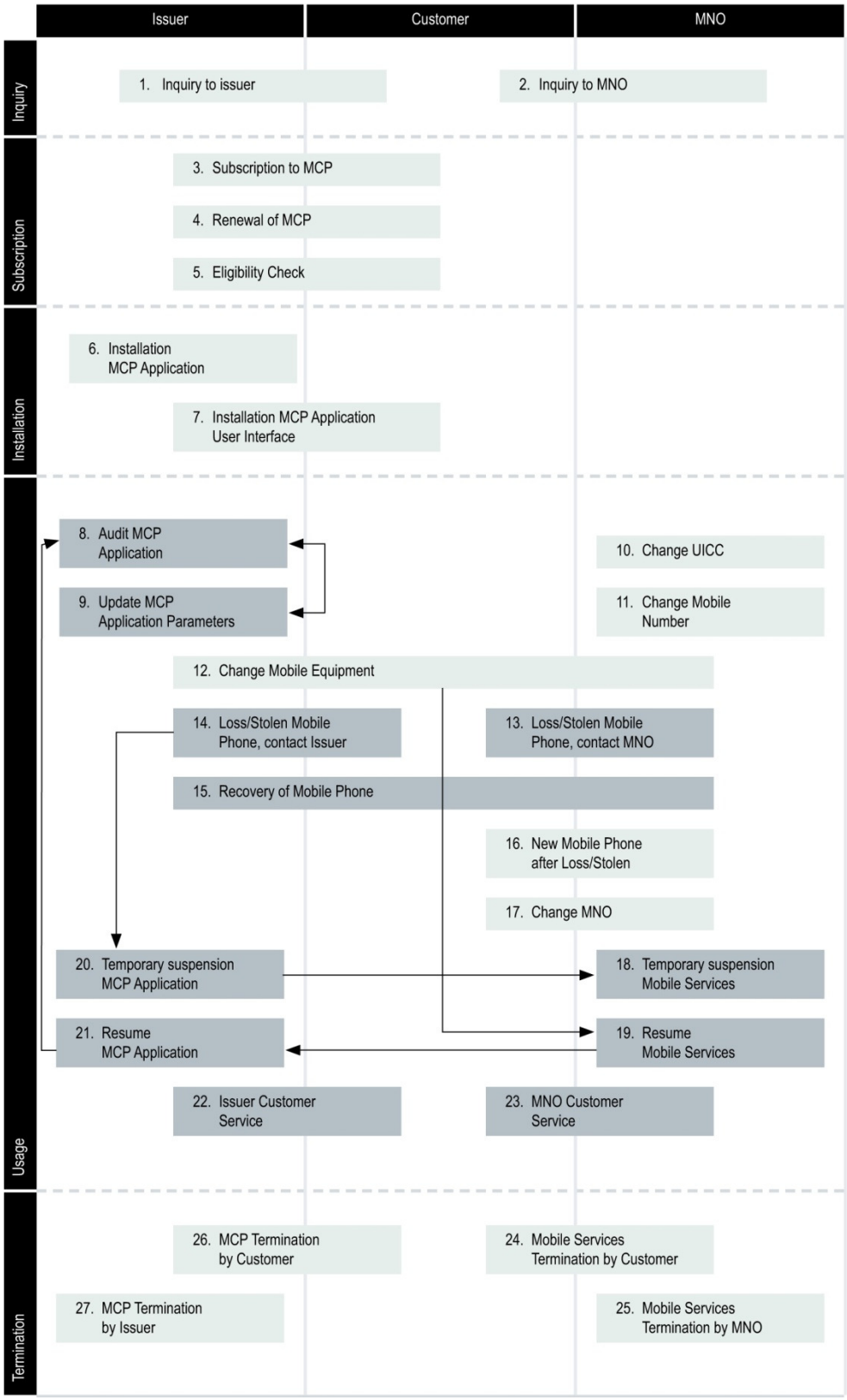


Figure 14 Loss and recovery of Mobile Phone scenario

10.5 Stolen Mobile Phone

In this scenario the Customers Mobile Phone is stolen and subsequently replaced. In this particular case, the scenario starts at Process 13. Process 22 and 23 have no explicit flow arrows as they may be invoked by the Customer at any point during the scenario (see Figure 15).

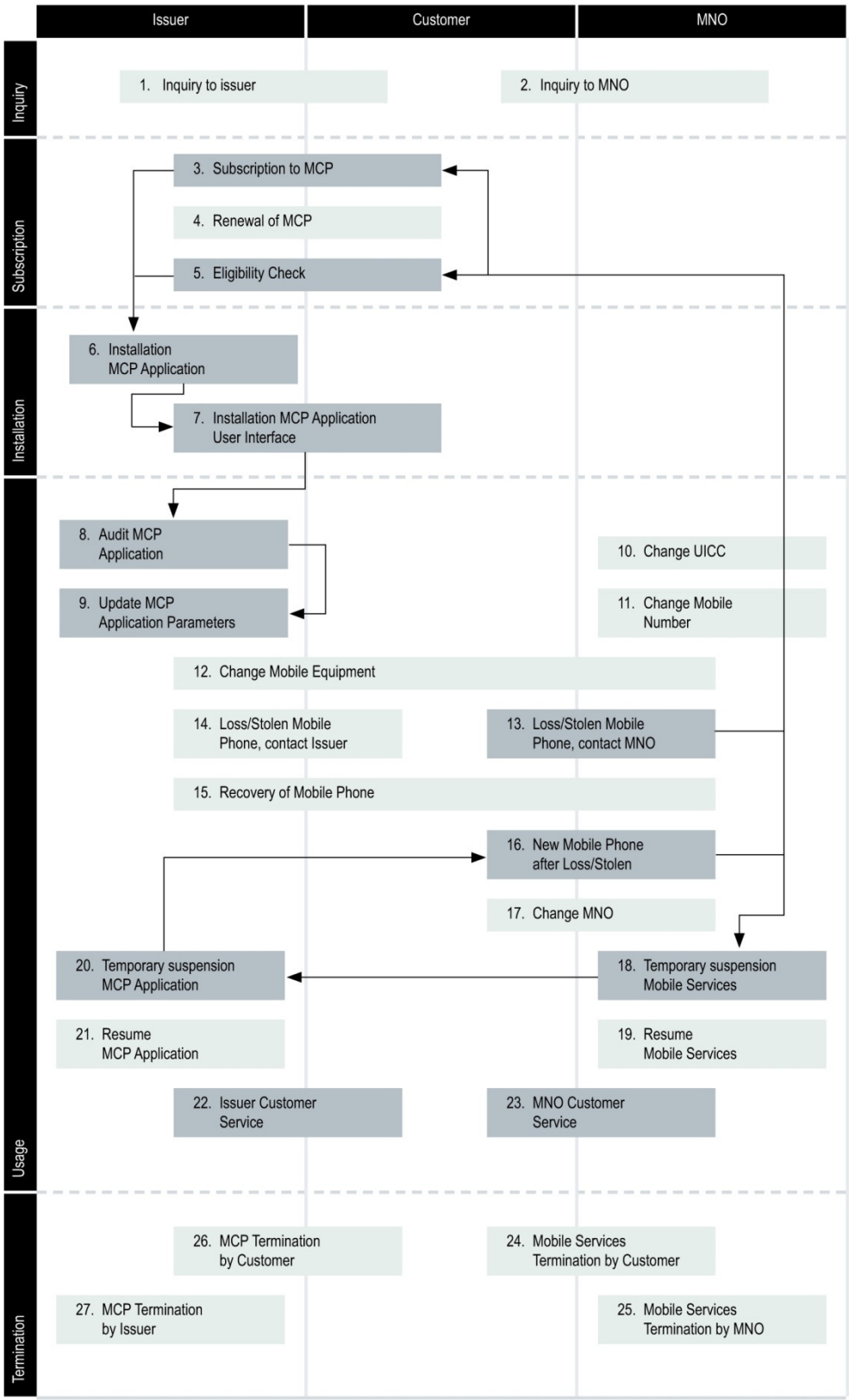


Figure 15
Stolen Mobile Phone scenario

10.6 Termination of MCP Application by Customer

In this scenario the Customer decides to terminate the MCP. In this particular case, the scenario starts at Process 22 (see Figure 16).

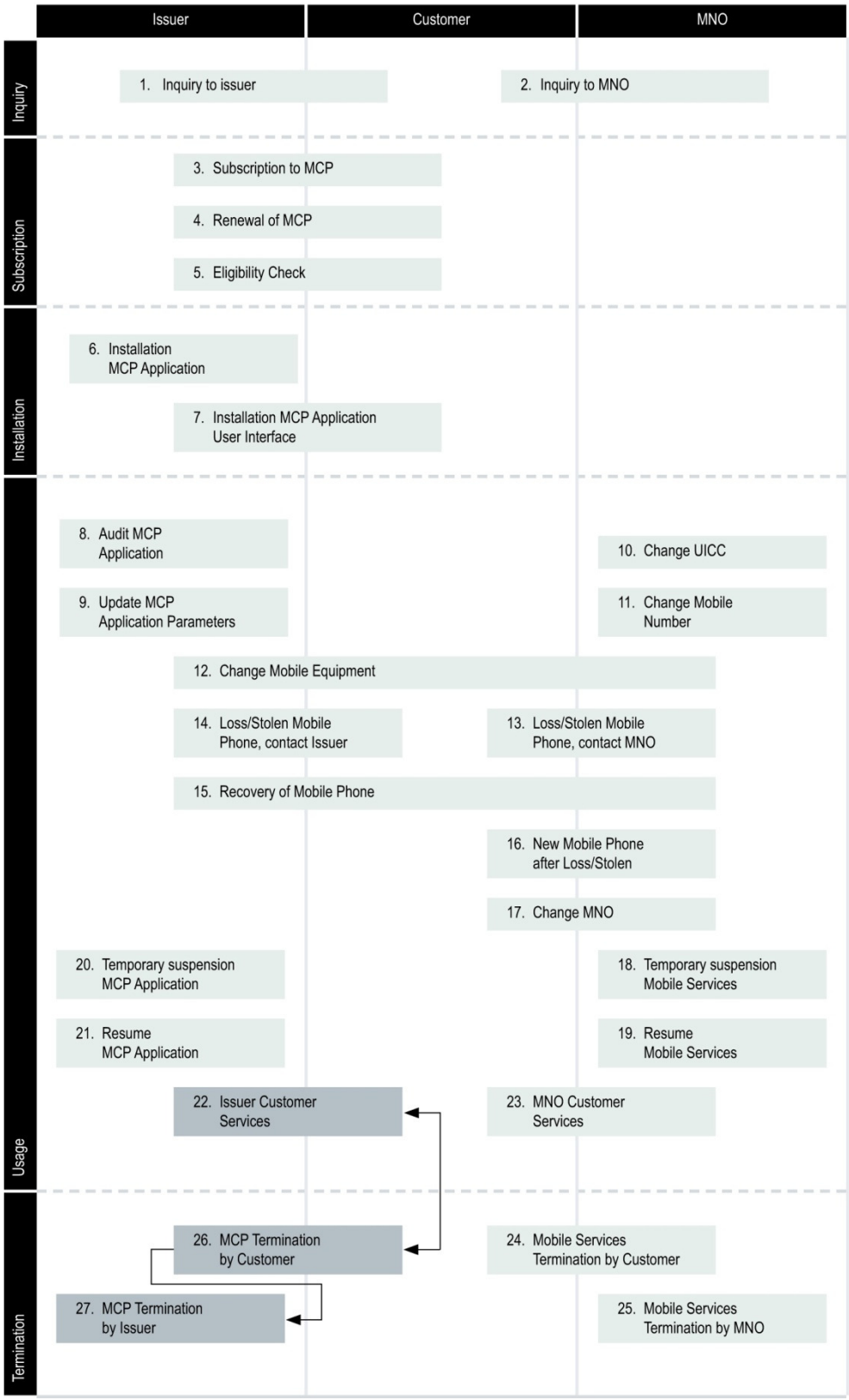


Figure 16 Termination of MCP Application by Customer Scenario

11 Annex II – MCP Application User Interface

This section elaborates on some aspects of the MCP Application User Interface.

The MCP Application User Interface (UI) is dedicated to the management of the interaction with the customer, in connection with the MCP Application located on the UICC.

This UI is defined, developed and maintained under the responsibility of the Issuer.

Primary functions linked to the MCP Application are:
- Personal code entry
- MCP Application configuration (e.g. new or updated parameters)

The MCP Application UI can typically be interfaced to an NFC User Primary Interface under the responsibility of the MNO (see Figure 17).

The NFC User Primary Interface enables the Customer to:
- browse and access MCP applications
- add new applications
- select the preferred MCP application (the 'by default' payment service)
- manage general NFC settings

The UI can be downloaded and updated via OTA by the Issuer on the Mobile Equipment. Loading and updating of the UI will be done under the agreement of the Customer (as owner of the Mobile Equipment). It can be removed from the Mobile Equipment by the Issuer or the Customer.

Several releases of the same UI may have to be defined and managed by the Issuer in order to propose a well adapted UI to different Mobile Equipment Man Machine Interface environments (e.g. different display sizes, different navigation modes, other capabilities).

As an example, figure 17 provides a possible implementation of the UI environment on Mobile NFC Equipment.

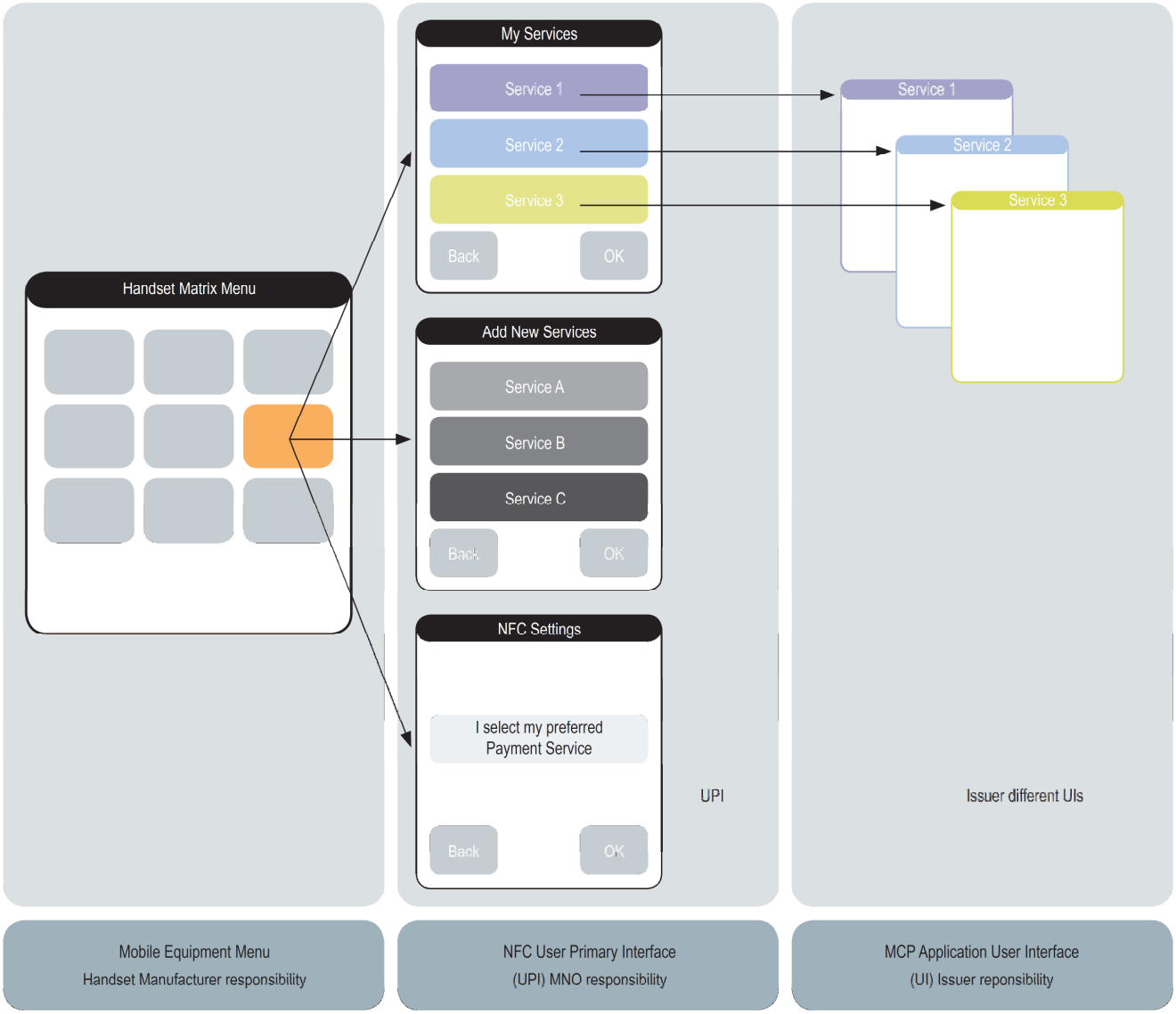


Figure 17:
One example of possible UI configurations on a Mobile Phone