# Table of Contents

1. **Purpose and Scope** 3  
   1.1 Out of Scope 3  
2. **Definition of Terms** 4  
3. **Document Cross-References** 4  
4. **Mobile NFC Service Concept** 5  
   4.1 The benefits of a mobile wallet 5  
   4.2 Concept of Service Operation in a mobile wallet 6  
   4.2.1 The benefits of a Common Services platform 7  
5. **Overview of the Mobile NFC Service Model** 7  
   5.1 Relationship between NFC Mobile Stakeholders 7  
   5.2 Mobile NFC Service Model 8  
6. **Another NFC Service Model** 9  
   6.1 Trusted Service Management roles General and Logical architecture 9  
   6.1.1 3-Party Issuing and Lifecycle Model 9  
   6.1.2 4-Party Issuing and Lifecycle Model 10  
   6.1.3 Combination of 3 and 4 Party Models 11  
   6.1.4 Multi-TSM Model 11  
   6.2 MCP Lifecycle management 12  
   6.2.1 Customer Inquiry 12  
   6.2.2 Subscription to MCP Application 12  
   6.2.3 Installation of the MCP Application 13  
   6.2.4 Usage of the MCP Application 13  
   6.2.5 Termination of the MCP Application 14  
7. **MNO and SP Responsibilities** 15  
   7.1 MNO Responsibilities 15  
   7.2 Service Provider Responsibilities 19  
8. **Conclusion** 23  
Document Management 24  
Document History 24
1 Purpose and Scope

Deployment of Near Field Communications (NFC) Universal Integrated Circuit Card (UICC, also known as the “SIM-card”) -based mobile payment services is a multi-industry effort requiring collaboration amongst many different players who are the key players in their respective industries. In order to encourage this, GSMA has produced many different guidelines from both a Mobile Network Operator (MNO) perspective and a collaborative perspective covering a range of topics, such as:

- The Mobile NFC Ecosystem [1];
- Technical Requirements for Handsets [2];
- Business Opportunity Analysis [3];
- Mobile Contactless Payments: Service Management Roles, Requirements and Specifications [4].

A good understanding and clarity in service operations is essential to the successful deployment of NFC services. This document provides an overview of the key concepts for Services Operations for mobile NFC services. It also proves operational guidelines for MNOs and Service Providers (SPs) to successfully deploy mobile NFC services in their markets.

The intended audience for this paper are MNOs, including other key NFC eco-system players, for example: SPs, handset manufacturers and system vendors.

This document is intended to provide guidelines for GSMA MNOs developing service operation specifications for commercial deployment of UICC-based mobile NFC services. It also provides guidance to MNOs seeking to achieve consensus in collaborating with other ecosystem players in their respective markets.

This document should also help key mobile NFC ecosystem players (such as, SPs, handset manufacturers and system vendors) to understand the role of the MNO in the ecosystem and importance of service operations in creating a successful mobile NFC ecosystem.

Chapters 4 and 5 describe a service operation model that has been commercially deployed in Japan. Another example is developed in Europe and this is described in chapter 6. Chapter 7 describes the operational responsibilities of MNOs and SPs.

1.1 Out of Scope

This document does not provide operational specifications for mobile NFC services but describes high level operational concepts. These concepts can be used to design operational specifications.
2 Definition of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPC</td>
<td>European Payments Council</td>
</tr>
<tr>
<td>MCP</td>
<td>Mobile Contactless Payment</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>OTA</td>
<td>Over The Air</td>
</tr>
<tr>
<td>SE</td>
<td>Secure Element</td>
</tr>
<tr>
<td>SM</td>
<td>Service Management</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>TSM</td>
<td>Trusted Service Manager</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal Integrated Circuit Card (also known as the “SIM card”)</td>
</tr>
</tbody>
</table>

3 Document Cross-References

<table>
<thead>
<tr>
<th>Ref</th>
<th>Document Number</th>
<th>Title</th>
<th>Title</th>
</tr>
</thead>
</table>
4  Mobile NFC Service Concept

This chapter provides a conceptual overview of mobile NFC services. The mobile NFC handset can provide a range of services for the customer. For example, payment, ticketing and access control. Furthermore, the mobile NFC handset can be considered to be a replacement of a customer’s physical wallet. This “virtual wallet” can support a number of “virtual cards” (e.g. credit, debit and loyalty). Hence, the mobile wallet is effectively providing contactless card services via the mobile phone (this concept is shown in Figure 4-1).

![Figure 4-1: Mobile Wallet Replacement Concept](image)

4.1 The benefits of a mobile wallet

Today, the mobile phone has become a necessity. Customers tend to have their mobile phone within reach. By adding a mobile wallet to the mobile phone, the phone becomes even more indispensable and increases the ease and convenience for the customer. This diminishes the customer’s dependency on the physical wallet.

Another benefit of a mobile wallet (beyond that of a physical wallet) is it can be expanded to include a number of other services, such as keys (for access control to homes, offices, cars etc.) and coupons. These additional services do not expand the physical size of the mobile phone, unlike the case with a physical wallet. Each customer can customise the number and types of services in their mobile wallet.

Today, there is an increasing trend for customers to purchase digital content from their mobile phones (e.g. applications, games and ring tones). This trend can be leveraged with mobile NFC handsets to allow customers to purchase physical items with their mobile wallet. This increases convenience for the customer and creates new business opportunities for MNOs and SPs.
### 4.2 Concept of Service Operation in a mobile wallet

Outside of the mobile phone environment, SPs will have their own set of business rules as to how each of their services operates. The mobile wallet can support a number of services. Moving all of these services to a mobile phone environment requires an additional set of business rules so that each of these services can co-exist and can operate successfully.

Mobile NFC services can run on a Secure Element (SE, i.e. the UICC). Where the SE is the UICC, there will be a basic set of business rules coming from the MNO (who owns the UICC). The MNO business rules need to be factored in with the SPs business rules for Service Operation. Where there is a common set of business rules agreed by the MNOs and key SPs, this can be considered to be a Common Services platform (this is shown in figure 4-2). Examples of services in a Common Services platform include E-Money, Membership cards, Coupons, Loyalty cards, Credit Cards and Transport cards.

![Figure 4-2: Diagrammatic Business View of Service Platform Categories (ideal scenario)](image)

Where some SPs cannot agree to comply with the business rules defined for the Common Services platform, then these services can reside in an additional Specific Services platform (see figure 4-3). Examples of services that could reside in a Specific Services platform include Government services and Military services (e.g. as realised in Japan).

![Figure 4-3: Diagrammatic Business View of Service Platform Categories (alternative scenario)](image)
4.2.1 The benefits of a Common Services platform

A Common Services platform is essential because once a common set of business rules are defined, new SPs can easily add their services in this framework without having to redefine the business rules. Furthermore, it streamlines business operations between the MNOs and the SPs. This has an additional benefit as it provides a consistent user experience in terms of customer care.

The Specific Services platform, however, adds additional complexity to business rules and service operations for the MNOs and SPs. Therefore the Specific Services platform should be considered optional.

5 Overview of the Mobile NFC Service Model

This chapter provides an overview of the Mobile NFC ecosystem focusing on the key players that are essential in any NFC ecosystem, the user, the MNO and the SP. It explains the importance of the division of responsibility between the MNO and SP, and why the MNO is best positioned to manage the SE. Finally, it explains the service model, which shows the relationship between the user, the MNO and the SP.

The GSMA has published a number of white papers regarding the benefits of UICC based NFC enabled M-Payment. For example, see reference documents [1] and [3].

5.1 Relationship between NFC Mobile Stakeholders

Figure 5-1 shows how the MNO provisions the basic mobile telecommunications services (i.e. voice and data services on to a Telecom Services Platform). The MNO also provisions the mobile NFC wallet on to the mobile NFC phone (i.e. on the Multi-service SE platform) and acts the SE (i.e. UICC) manager. The SP provisions the mobile NFC service in to the mobile wallet (i.e. on the Multi-service SE platform).

Figure 5-1: Relationship between MNO, SP and users

The benefits of this approach are twofold; firstly, it allows the MNO to leverage its knowledge of provisioning mobile telecommunications services to develop an attractive and compelling mobile wallet service for the customer. Secondly, it allows the SP to develop and
optimize its NFC service without having to worry about the telecoms platform or the mobile wallet platform.

The MNO is best suited to be the SE manager because the MNO:
- Can manage the multiservice platform so that the NFC services can operate and co-exist successfully;
- Already provides end-to-end lifecycle support to customers (e.g. customer care);

5.2 Mobile NFC Service Model

Figure 5-2 depicts a successful service model in operation today.

There are three key players in this service model: the MNO, SP and User. The key relationships between these players are:

1. MNO – User relationship
   In this relationship the User requests to use the mobile wallet (assuming the User already has a subscription with the MNO for mobile telecommunication services). The MNO then provides the wallet, which allows the User to install, use or delete specific NFC services on their phone. The MNO is responsible for end-to-end lifecycle support to the Users (e.g. to deal with faults, change of handsets, change of subscription etc.).

2. MNO – SP relationship
   In this relationship the SP requests permission to develop NFC services for the MNOs mobile platform/wallet. The MNO can then grant permission to the SP to develop the NFC service for the mobile platform. The MNO can enable multiple SPs to co-locate their NFC services in the mobile wallet. This involves assuring SPs that their NFC services can be accessed by them alone (i.e. not by other SPs or the MNO).

3. SP- User contract relationship
   In this relationship, the User subscribes to the SPs NFC service. The SP provides that service on the User’s mobile wallet and is responsible for guaranteeing usage of that particular service. The SP is responsible for end-to-end lifecycle support to Users for their particular NFC service.

In order to realize this service model, it is important to have a clear division of responsibilities between User, SP and MNO.
6 Another NFC Service Model

The previous chapter details a service model that has been commercially deployed in e.g. Japan, another example has been developed in Europe, and this is described in this chapter.

The European MNOs working in the GSMA Pay-Buy-Mobile project have collaborated with the European Payment Council (EPC) to produce a common framework for UICC based Mobile Contactless Payments (MCP) and Service Management (SM) roles, see reference document [4] for details. An overview is provided below.

6.1 Trusted Service Management roles General and Logical architecture

Figure 6-1 provides an overview of Service Management for MCP. A set of SM roles exist in the MNO and Issuer (i.e. SP) domain. These SM roles can be performed in-house by the MNO/Issuer or they can be “out-sourced” to a third party (called the TSM).

Figure 6-1: Service Management General Overview

Different service models exist for MCP. For example 3-Party, 4-Party, combination and multi-TSM models. The salient features of each of these models are listed below, for more details please see reference document [4].

6.1.1 3-Party Issuing and Lifecycle Model

- Commercial actors are the Customer, the Issuer and the MNO.
- SM technical roles are the set of technical functions performed on behalf of the Issuer and/or the MNO.
• SM technical roles are fully or partly implemented by TSMs. TSMs are not involved in the commercial relationship between Issuers and MNOs.
• In this model there is a direct business relationship between Issuers and MNOs.

![Diagram of the 3-Party Model]

**Figure 6-2: The 3-Party Model**

### 6.1.2 4-Party Issuing and Lifecycle Model

- Commercial actors are the Customer, the Issuer, the MNO and the TSM performing SM commercial roles on behalf of Issuers and MNOs in addition to SM technical actors.
- In this model the TSM have commercial relationship with Issuers and MNOs.
- In this model there is no direct commercial relationship between Issuers and MNOs.
- In the general case, several TSM companies might be involved.
- This model implies that the TSM(s) implementing the SM commercial roles are accepted both by the Issuers and MNOs.
6.1.3 Combination of 3 and 4 Party Models

- “3-Party model” and “4-Party model” can coexist.
- In this case, some Issuers/MNOs have direct commercial relationships based on the 3-Party model while this relationship is managed by TSMs (implementing the commercial roles) for some others.
- The implementation of this combination of models depends on market conditions as well as Issuers and MNOs strategic choices.

6.1.4 Multi-TSM Model

- Commercial actors are the Customer, the Issuer, the MNO and the TSM performing both SM commercial and technical roles.
- In this model multiple TSMs are involved.
- There is no direct commercial relationship between Issuers and MNOs.
6.2 MCP Lifecycle management

Five phases are defined in the customer life-cycle management:
1. Customer Inquiry
2. Customer subscription
3. Installation of Service
4. Customer Usage
5. Termination of Service

To support these different phases, 27 different processes have been defined. A listing of these processes is written below (further details can be found in reference document [4] see section 6.1.2).

6.2.1 Customer Inquiry

- 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.

6.2.2 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).

6.2.3 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.

6.2.4 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)

• Process 12: The Customer changes Mobile Equipment
  o Scenario 1: The new Mobile Equipment is unable to work with the UICC. The Customer contacts the MNO’s help desk.
  o 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.
  o 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.
  o 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.

6.2.5 **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.
7 **MNO and SP Responsibilities**

This chapter describes from an operational perspective the MNO and SP responsibilities. These responsibilities are not meant to be an exhaustive list but provide an overview of the key operational concepts.

### 7.1 MNO Responsibilities

<table>
<thead>
<tr>
<th>MNO Function</th>
<th>Definition</th>
<th>Significance from User Perspective</th>
<th>Significance from MNO Perspective</th>
<th>Significance from SP Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>(M-1) Post Issuance of services</td>
<td>Users are able to request issue of mobile NFC services into their NFC handsets after purchasing the handsets. Services issued are not restricted to services pre-installed in UICC.</td>
<td>Users should be free to dynamically register for NFC services they want to use, at the time and place they want to use them. This results in increased convenience to users.</td>
<td>MNO is able to market new types or varieties of NFC services to users even after deploying Mobile NFC handsets to users. This leads to an environment that is conducive to new business opportunities for the MNO. It also increases the appeal of the NFC service platform offered by the MNO to users.</td>
<td>Due to factors like timing of start of services and expansion of services (e.g. local to global), SPs who may not have the luxury of having their services be pre-installed in UICCs, and can provision even after the UICCs have been deployed. This results in increased business opportunities for the SPs.</td>
</tr>
<tr>
<td>(M-2) Issuance/Deletion of Services via mobile network</td>
<td>Users are able to request issuance/deletion of mobile NFC services into the SE of their NFC handsets via the mobile network</td>
<td>24hour accessibility and instant processing of registration increases convenience for users. Users can forgo hassle of registering services at service counter (which has limited opening hours), or using mail or web based application forms (which usually takes days to process)</td>
<td>24hour accessibility and instant processing of registration lowers barrier to entry for users to use NFC services. Results in more active NFC services users, which results in increased user loyalty to MNO.</td>
<td>SPs can quickly introduce new services or improvements to current services (e.g. conduct marketing campaigns, collect usage data for marketing purposes) even after NFC handsets and UICCs are deployed. This results in increased business opportunities for the SPs.</td>
</tr>
<tr>
<td>MNO Function</td>
<td>Definition</td>
<td>Significance from User Perspective</td>
<td>Significance from MNO Perspective</td>
<td>Significance from SP Perspective</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>(M-3) Issuance/Deletion of Services via contactless terminal (optional for future phases)</td>
<td>Users are able to request issuance/deletion of mobile NFC services into SE of their NFC handsets via the contactless terminal</td>
<td>Increased convenience when applying for an NFC service, as users can request issuance and use an NFC service immediately upon tapping their handsets on the contactless terminals. (Online registration and UI application download can be performed later at user’s convenience)</td>
<td></td>
<td>SPs can gain more users for their services by encouraging users to apply for and use the NFC service at the Point Of Sale.</td>
</tr>
<tr>
<td>(M-4) Local NFC Lock</td>
<td>Users are able to enable/disable the NFC functionality of their NFC handset, using a push of a button or via menu settings</td>
<td>Increased security and protection of user services, as users are able to protect their services from being misused by unauthorised persons. Increased assurance to users, to comfortably use NFC services without fear of their services being misused. In general, this is also expected by users as a basic function, just as they are able to password lock their handsets to prevent unauthorised access to their phone address book, browser etc.</td>
<td>MNO is able to market this security feature to assure potential users and lower the barrier to entry for NFC services. This increases the possibility of users moving from non-active to active user state.</td>
<td>SP is able to market this security feature to assure potential users and reduce their worries over the possibility of their NFC handsets being misused. This increases the possibility of users moving from non-active to active user state.</td>
</tr>
<tr>
<td>MNO Function</td>
<td>Definition</td>
<td>Significance from User Perspective</td>
<td>Significance from MNO Perspective</td>
<td>Significance from SP Perspective</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>(M-5) Remote NFC Lock</td>
<td>Users are able to remotely enable/disable the NFC functionality of the NFC handset which is stolen or lost, by requesting to the MNO (e.g. online or calling in to the MNO’s call center)</td>
<td>Increased security and protection of user services, as users are able to protect their services from being misused by unauthorised persons. Increased assurance to users, to comfortably use NFC services without fear of their services being misused.</td>
<td>MNO is able to advertise this security feature to reassure potential users and lower the barrier to entry for NFC services. This is a clear advantage over the standard plastic contactless card.</td>
<td>SP is able to market this security feature to reassure potential users and reduce their worries over the possibility of their NFC handsets being misused.</td>
</tr>
<tr>
<td>(M-6) Remote Individual Service Lock</td>
<td>In the case of late payments or misuse of service by a particular user, SPs are able to remotely enable/disable their deployed mobile NFC service within an NFC handset belonging to that user, by requesting to the MNO (e.g. online or calling in to the MNO’s call center)</td>
<td>In cases like breaking of the service usage agreement, blacklisted users will be barred from using the service as SPs can remotely disable their NFC service via the MNO.</td>
<td>Due to the advantage this feature compared to the plastic card, an MNO could market this feature as a service to SPs which could lead to a new revenue source for the MNO. (For example, the SPs would pay according to the number of successful locks)</td>
<td>SPs have the right to remotely enable/disable their services for specific users. This means that there would be increased assurance for SPs to offer NFC mobile services to their current plastic card users. This also results in reduced risk of losses that could be incurred from misuse of their services.</td>
</tr>
<tr>
<td>MNO Function</td>
<td>Definition</td>
<td>Significance from User Perspective</td>
<td>Significance from MNO Perspective</td>
<td>Significance from SP Perspective</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>(M-7) Full Format</td>
<td>In the case of cancelled subscriptions, damaged UICCs, transfer of ownership of subscription etc., MNOs are able to format all NFC service related data in the SE of the affected UICC.</td>
<td>Increased convenience and reassurance to users as users have the capability to easily remove all NFC services and re-initialise their SE. In general, this is also expected by users as a basic function, just as they are able to remove all phonebook, image and application data through re-initialising their handset.</td>
<td>MNO is able to reduce risk of misuse of SE's that are sent in for repair or returned by the user. (at expiry of mobile subscription)</td>
<td>Reassures SP that risk of misuse is reduced through full format of SE’s when they are entrusted by the user to another party.</td>
</tr>
<tr>
<td>(M-8) Data Transfer</td>
<td>In the case of UICC change due to version up (Speed, Functionality, Memory etc.), all mobile NFC services data in can be transferred from the old UICC to the new UICC. This function may be carried out at the request of the user or MNO.</td>
<td>Increased convenience for users when wanting to move from one SE to another. It is terribly inconvenient for users to contact each SP to transfer each service one by one. (e.g. Users having several UICCs for different countries can easily move services from one UICC to the other)</td>
<td>Upon release of an updated UICC, it is easier for MNOs to encourage current users to move to the new UICC. For the division of responsibilities to be clear, it is fundamentally assumed that this function not be used or marketed for NFC services related purposes of backup etc. All SPs are to provide for data transfer of their services for purposes of, SE to SE service transfer, backup etc.</td>
<td></td>
</tr>
</tbody>
</table>
### Service Provider Responsibilities

<table>
<thead>
<tr>
<th>SP Function</th>
<th>Definition</th>
<th>Significance from User Perspective</th>
<th>Significance from MNO Perspective</th>
<th>Significance from SP Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S-1) Offline Viewer</td>
<td>This function allows users to check their service information (e.g. E-money amount, ID number, coupons) without having to connect to the mobile network. (Advantage over current plastic card services)</td>
<td>Increased convenience and at times, necessary in cases of checking the e-money value or available coupons in the NFC handset before using them.</td>
<td>-</td>
<td>SPs can provide added value features of their services, using this function which allows users to use the features without having to connect to the mobile network. SPs can use this function as a backup feature, to check service related info like credit card numbers or ticket ID, when the contactless reader is unable to read such info from the NFC handset.</td>
</tr>
<tr>
<td>SP Function</td>
<td>Definition</td>
<td>Significance from User Perspective</td>
<td>Significance from MNO Perspective</td>
<td>Significance from SP Perspective</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>(S-2) Functionalities that handle case of change of user information in UICC</td>
<td>In cases like transferral of handset/UICC ownership or name change due to marriage, the user's mobile contract info changes. This could involve a change in owner info or a simple change in the family name of the user. This could involve the full formatting of the NFC services in the UICC. Service and operational design should be done taking the above cases into consideration.</td>
<td>In cases of change of UICC ownership where a user hands over ownership of UICC to another user, if the NFC services are left available in the UICC/NFC Handsets, there may be a risk of possible misuse of services by the new user. By employing methods like full formatting of NFC services in the UICC before transferring ownership, the original user is able to prevent such possible misuse.</td>
<td>It is possible for an MNO to change the ownership information of a UICC. From a privacy perspective, it is difficult for an MNO to release information related to ownership change to SPs. However, if privacy issues are overcome, it may be possible for an MNO to provide such information or limited version of such information to SPs as an option service.</td>
<td>In managing the users and UICC/NFC handsets, SPs need to be aware of the fact that users and the UICC/NFC handset are not permanently linked. It is advisable to have operations that deal with the case that users may not report that their mobile contact info (name change etc.) has changed.</td>
</tr>
<tr>
<td>SP Function</td>
<td>Definition</td>
<td>Significance from User Perspective</td>
<td>Significance from MNO Perspective</td>
<td>Significance from SP Perspective</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>------------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>(S-3) Functionalities that handle case of change of UICC</td>
<td>There are cases where users change their UICCs due to a damaged UICCs or UICC updates. Service and operational design should be done taking the above cases into consideration.</td>
<td>Users may be required to move from an old UICC to a new UICC due to damaged UICCs or UICC updates.</td>
<td>There should be means to ensure that the user’s ability to use NFC services should not be disrupted due to UICC change. A possible means is that the MNO provide a function where all NFC service related data could be transferred from old UICC to new UICC. If an MNO does not have the right to provide such a function, other means need to be implemented to deal with the NFC related data remaining in the old UICC. Also, such means should take into consideration the fact that the old UICC may not be able to be connected to the mobile network.</td>
<td>It is best that SPs deploy their services in such a way that allows for users to quickly continue using their NFC services even after a UICC change. For this to happen, SPs should have a mechanism in place that allows them to detect when a user changes their UICC.</td>
</tr>
<tr>
<td>(S-4) Functionalities that handle case of change of NFC handsets</td>
<td>There are cases where users change their NFC handsets due to damaged, lost or stolen handsets. Service and operational design should be done taking the above cases into consideration.</td>
<td>Although users have the freedom to switch handsets by reinserting their UICCs, they should be aware that the handset they switch to may not support the NFC functionality or NFC services.</td>
<td>As an MNO is unable to monitor when a user changes the handset (e.g. user may have multiple handsets or handsets could have changed ownership on an individual basis), it is impossible for the MNO to inform the SPs about the occurrence of such an event.</td>
<td>When users change their handsets and the handsets do not support either NFC functionality or services, then this could result in users not being able to use their NFC services. In this case, the SPs’ service operations should be designed taking into consideration the issue of educating users on procedures to follow prior to changing their handsets.</td>
</tr>
</tbody>
</table>
### Functionalities that handle case of suspension and resumption of mobile network access from UICC

<table>
<thead>
<tr>
<th>SP Function</th>
<th>Definition</th>
<th>Significance from User Perspective</th>
<th>Significance from MNO Perspective</th>
<th>Significance from SP Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S-5)</td>
<td>There are cases where the MNO suspends the right of a UICC to access its mobile network due to handset loss, theft, unpaid subscription fees etc.</td>
<td>Users must contact both the MNOs and various SPs of services that they are using, if they want to suspend both the mobile network service and NFC services.</td>
<td>It is possible for an MNO to suspend the mobile network service of a user. However, the reasons for suspension are many ranging from unpaid subscription to stolen and lost handsets. From a privacy perspective, it is difficult for an MNO to release such information to SPs.</td>
<td>Due to the suspension, users' UICC/NFC handset cannot be accessed via the mobile network. Thus, SPs should be aware that they are unable to access their NFC services on the users' UICC/NFC handset from their OTA servers. On the other hand, SPs should be aware of the possibility that just like the contactless cards, their NFC services can still be accessed via the NFC contactless interface by their contactless readers. Finally, SPs should also be aware that they may be able to resume access their NFC services on the users' UICC/NFC handset from their OTA servers, once their mobile network service suspension is lifted.</td>
</tr>
<tr>
<td>SP Function</td>
<td>Definition</td>
<td>Significance from User Perspective</td>
<td>Significance from MNO Perspective</td>
<td>Significance from SP Perspective</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>(S-6) Functionalities that handle case of cancellation of mobile contract</td>
<td>There are cases where the MNO cancels the mobile contract of a user thus resulting in terminating the UICC’s access its mobile network. This could occur from users wanting to terminate their contract or MNOs terminating contracts of blacklisted users who have violated the service agreements. Service and operational design should be done taking the above cases into consideration.</td>
<td>On cancellation of their mobile contract, users are unable to use NFC services via the mobile network. Thus, it is the responsibility of the users to inform SPs of this and to decide on the next course of action. (i.e. terminate or continue the NFC service)</td>
<td>It is possible for an MNO to terminate the mobile network contract of a user. From a privacy perspective, it is difficult for an MNO to release information related to termination (e.g. reasons for termination) to SPs. However, if privacy issues are overcome, it may be possible for an MNO to provide such information or limited version of such information to SPs as an option service.</td>
<td>Due to the termination, users’ UICC/NFC handset cannot be accessed via the mobile network. Thus, SPs should be aware that they are unable to access their NFC services on the users' UICC/NFC handset from their OTA servers. Service and operational design should be done taking the above points into consideration.</td>
</tr>
</tbody>
</table>

8 Conclusion

This document has provided an overview of the key concepts for Services Operations for mobile NFC services. It has also provided operational guidelines for MNOs and SPs to successfully deploy mobile NFC services in their markets. It is envisaged that the information and concepts described here will be extended and expanded, as the MNOs and other NFC ecosystem players build specific operational implementations in their respective markets.
Document Management

Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Brief Description of Change</th>
<th>Approval Authority</th>
<th>Editor / Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>16 March 2011</td>
<td>First Issue to DAG and EMC for approval</td>
<td>EMC</td>
<td>Kyoshi Mori (NTTDOCOMO)</td>
</tr>
<tr>
<td>1.0</td>
<td>18 March 2011</td>
<td>Updated to reflect DAG review comments</td>
<td>EMC</td>
<td>Kyoshi Mori (NTTDOCOMO) and Nav Bains (GSMA)</td>
</tr>
<tr>
<td>1.0</td>
<td>13 &amp; 14 April 2011</td>
<td>Submitted to EMC for approval</td>
<td>EMC</td>
<td>Kyoshi Mori (NTTDOCOMO) and Nav Bains (GSMA)</td>
</tr>
</tbody>
</table>

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org
Your comments or suggestions and questions are always welcome.