Contents

Executive Summary

1 Introduction
1.1 Purpose and scope of this document
1.2 Intended Audience
1.3 Mobile Wallet Stakeholders

2 Delivering mobile NFC services

3 The Mobile Wallet
3.1 The Core Wallet
3.1.1 Core features
3.1.2 Plastic card substitution
3.2 The Extended Wallet

4 Implementing mobile NFC Services
4.1 No UI App
4.2 Native UI app implementation
4.2.1 Native UI App development
4.2.2 Template-based UI App development
4.3 UI App implemented by the extended wallet

5 Annex
5.1 Definition of Terms
5.2 Service App Lifecycle
5.2.1 App Development
5.2.2 Registration
5.2.3 Test & Certification
5.2.4 Security
5.2.5 Publication
5.2.6 Discovery
5.2.7 Service Provider App Download
5.2.8 Service Provider App Installation
5.2.9 UICC Applet Installation
5.2.10 Display
5.2.11 Execution
5.2.12 Update
5.2.13 Removal
5.3 Framework Specifications

Document Management
References
Authors
Document History
Other Information
Executive Summary

Near Field Communication (NFC) technology enables devices within a few centimetres of each other to exchange information and data. Some plastic debit and credit cards now contain NFC chips, enabling people to pay for items by simply tapping the card against an NFC terminal. Mobile phones are also increasingly being equipped with NFC capabilities, opening up an opportunity to transform the consumer experience of payments in retail stores, ticketing, access control and other aspects of daily life.

In many cases, mobile NFC services will be presented via a “mobile wallet” – the subject of this white paper. A mobile wallet is a software application on a mobile handset that functions as a digital container for payment cards, tickets, loyalty cards, receipts, vouchers and other items that might be found in a conventional wallet. The mobile wallet enables the user to manage a broad portfolio of mobile NFC services from many different companies.

This document sets out a framework for service providers, such as banks, retailers and transport operators, and mobile operators to create a simple and easy experience for the customer for mobile NFC services. This standardised framework is also designed to enable a “develop once only” approach for service providers dealing with multiple mobile operators and vice versa.

This paper envisages that consumers will be able to access NFC services through a mobile wallet provided by their mobile operator. This mobile wallet should always include certain core features to ensure that a service provider’s NFC service is compatible with wallets from multiple mobile operators.

In many cases, the wallet will be able to launch a service provider application, which enables a user to manage a specific NFC service through a dedicated user interface (UI). In this paper, this application, which runs on the handset, is referred to as the “UI app”.

Figure 1: Delivering mobile NFC services
The mobile wallet may also contain other service provider features that are not related to NFC. In general, the UI app is the responsibility of the service provider. In some cases, all the functionality needed by a given service provider may be included in the mobile wallet itself, in which case a separate UI app is not needed.

This paper envisages that each NFC service will also be supported by an applet (a small application) within the handset’s universal integrated circuit card (UICC), commonly known as a SIM card, and optionally a service provider application running on a remote computer server, accessible via the mobile network. The applet on the UICC securely manages NFC transactions. It sits inside the secure domain on the UICC where it is isolated from other service providers’ applets – this architecture protects the user’s sensitive data and privacy by minimising the risk of interference or unauthorised access.

In addition to the required core wallet features, many mobile operators’ wallets may support generic functionality for specific use cases, such as payment, public transport ticketing and couponing. Mobile operators are also likely to make templates available that service providers can use to quickly produce their own UI apps for specific handset platforms.

The GSMA believes the mobile wallet architecture described in this paper will enable the efficient deployment of a wide range of compelling, secure and interoperable mobile NFC services, which will enrich the lives of individuals and create new business opportunities for a wide range of companies.
1 Introduction

Many of the world’s leading mobile network operators have committed to launch commercial mobile NFC services, secured by the UICC (commonly known as the SIM card) within mobile handsets. The GSMA is working with these operators, along with industry stakeholders and regulators, to stimulate the growth of a global ecosystem supporting the rollout of UICC-based NFC services.

The widespread usage of UICC-based NFC services will lead to significant socio-economic benefits for individuals, governments, transportation authorities, retailers, banks, mobile operators and other stakeholders. Handsets equipped with NFC enable people to interact quickly and efficiently with the world around them, simply by tapping their device against a reader, thereby reducing the friction involved in everyday processes, such as making payments at point of sale or validating tickets.

The commitment of multiple mobile operators to UICC-based NFC services will ensure global interoperability, portability and bank-grade security for users worldwide. A standardised approach will also help the broader ecosystem to generate economies of scale, as well as enabling consumers to easily move their personal data from one device to another.

1.1 Purpose and scope of this document

This document describes the concept of a mobile wallet that will provide an intuitive interface to enable the user to manage their portfolio of mobile NFC services.

It sets out a framework that NFC service providers and mobile operators can use to create a simple and easy experience for the end customer.

The standardised framework, set out in this paper, is also designed to reduce costs and complexity for service providers by minimising the need to develop different apps for each mobile operator they partner with. Ideally, both service providers and mobile operators will be able to adopt a “develop once only” approach for mobile NFC-related apps and services for each mobile platform (handset operating system).

Detailed technical specifications and guidelines for app developers are not included. These are in the scope of parallel specification work, which will be published at a later stage (see Annex 5).

This document focuses on mobile wallets provided by mobile operators rather than other players. Other, non-SIM-based solutions are neither excluded nor in any way affected by these requirements.

1.2 Intended Audience

- This document discusses the concept of the mobile wallet on a non-technical level. It is intended for:
- Service providers wishing to deploy mobile NFC services on handsets. These service providers may be from:
  - Banking
  - Retail
  - Public transport
  - Other industries
- Mobile operators wishing to implement open mobile wallet specifications in their network and on their handsets.
- Handset vendors seeking to offer and distribute NFC-enabled devices.
- Independent app developers who wish to build NFC services or develop mobile wallets for mobile operators.
- Consumers who want to learn about how mobile NFC services will change their future mobile experience.

1 The SIM is an application, which authenticates subscribers on mobile networks, that resides on a universal integrated circuit card (UICC). The role of the UICC can be extended through the addition of other applications that be used to securely interact with NFC card readers.
1.3 Mobile Wallet Stakeholders

The following stakeholder requirements were a specific focus in the development of the framework described in this document:

Consumers will look for:
- A clear and simple way of managing the mobile NFC services installed on their handset.
- Services that are portable between different mobile operators.
- A consistent user experience for specific NFC services across mobile operators.
- A consistent mobile wallet user experience across service providers.

NFC service providers will look for:
- An environment that enables them to provide highly secure and user-friendly NFC services to large numbers of customers, regardless of their mobile operator.
- A framework that makes the development and management of NFC applications as simple as possible.

Mobile operators will look for:
- An efficient way to provide their customers with a wide selection of innovative mobile NFC services.
2 Delivering mobile NFC services

This paper envisions that consumers will access mobile NFC services through a mobile wallet provided by their mobile operator. The software applications that underpin this approach are described below:

The mobile wallet – this application manages the portfolio of mobile NFC services on the handset. It may also manage other services offered by mobile operators and their partners. The mobile wallet should always include some core features to support interoperability. The mobile wallet will also enable the user to prioritise one NFC service over another, for example selecting the active payment card. In general, this app is likely to be the responsibility of the mobile operator. (The mobile wallet is covered in more detail in section 3).

The service provider UI application – this application enables a user to manage a specific NFC service through a dedicated user interface (UI) and can also be launched by the mobile wallet. In this paper, this application, which runs on the handset, is referred to as the “UI app”. It may also contain other features that are not related to NFC. In general, the UI app is the responsibility of the service provider. In some cases, all the functionality needed by a given service provider may be included in the mobile wallet, in which case a separate UI app is not needed. (UI apps are covered in more detail in section 4).

The service provider applet – this small application, which sits inside a secure domain reserved for the service provider on the UICC, securely manages NFC transactions. This application does not have a user interface and is referred to in this paper as the “UICC applet”.

3 The Mobile Wallet

3.1 The Core Wallet

To provide both end-users and service providers with a consistent experience, mobile operators should ensure their mobile wallets adhere to the common set of basic principles and high level business requirements defined in this white paper – the core wallet functionality. The mobile wallet should also support interoperable standards defined by other standards bodies, where applicable.

The core wallet should enable users to discover, install, update, run and uninstall mobile NFC services. Some of these activities may be implemented on a remote computer server, accessed via a mobile network, for which the wallet serves as a user interface.

3.1.1 Core features

In particular, the core wallet is required to support the following functions:

- The ability to search for specific NFC services in a simple way.
- The ability to display the list of NFC services installed on the handset, displaying logos and static information, such as service details.
- The ability to trigger the installation of service provider apps from a variety of sources, such as an app store or a service provider web site.
- The ability to launch a service provider app on the handset from the list of NFC services in the wallet.
- The ability to activate and deactivate NFC services already on the UICC.
- The provision of links and access details, such as phone numbers, email addresses and web addresses for customer support for the app from the service provider.

3.1.2 Plastic card substitution

Mobile operators may also design their core wallets to support “card virtualisation”, enabling a service provider to substitute its physical plastic NFC card (sometimes called a contactless card) with a virtual card in the mobile wallet. For many, this approach provides consumers with a familiar experience, encouraging usage in the first stage of deployment of mobile NFC services.

As an option, and in order to improve the user experience, the mobile wallet could use a set of predefined commands to retrieve relevant information from the service provider’s UICC applet. This information is interpreted by the wallet and used to display end-user specific data within a virtual image of the consumer’s plastic card inside the wallet.

This approach would mean the service provider does not have to do any coding activities to create a user interface on the handset.
3.2 The Extended Wallet

Beyond the core wallet functionality proposed by this paper, each mobile operator decides what other features and services are included in their wallet. By implementing optional features, referred to as the “extended wallet”, a mobile operator can enable service providers to offer mobile NFC services from within the wallet, rather than through their own UI app.

The mobile operator can implement these extended functions in a generic way for specific services, such as payment, public transport ticketing, couponing, etc.

To provide such generic services, the extended wallet needs specific information from the service provider (see section 5.2.1 for more detail). The wallet dynamically interprets this information to offer the relevant NFC services and interacts directly with the corresponding UICC applet. This approach reduces the cost of testing NFC apps on the multitude of devices a mobile operator may have in its portfolio.

The generic services supported by the extended wallet could include:

- Payment card functions, such as making a contactless payment or reviewing the balance on a specific account.
- Coupon management: receiving, displaying, managing and redeeming coupons.
- Receiving and redeeming NFC tickets for transport and events etc.
- Enabling access to a building.
- Provide service parameters specific to the kind of service (e.g. payment, loyalty, couponing, ticketing, building access). For example, the account number of the associated bank, expiry dates etc. for a payment service.

Figure 2: Extending a core wallet to support more functionality
4 Implementing NFC Services

To roll-out an NFC service, a service provider may need to implement several applications:

- A "UICC applet", hosted on the handset’s UICC, which performs the secure transactions and stores the associated data. Typically written in the widely-used Java programming language, this application is deployed in the service provider’s dedicated secure area on the UICC. Service providers can deploy these applets “over the air” in a number of different ways, interacting with mobile operators directly or through third-parties (interfaces between service providers and mobile operators are covered in other GSMA papers). The GSMA expects this UICC applet to be compatible with any UICC (with sufficient resources available) from any mobile operator, and with any handset. More detail on the NFC UICC applet can be found in the NFC Service Provider Applets Development Guideline document.

- A mobile application (“UI app”), hosted on the mobile handset, can provide the user interface for accessing service features; The service provider will use appropriate tools (depending on the handset operating system) to develop the UI app. As with any mobile application, this UI app will be Operating System specific or may even be optimized for a specific handset, but should be compatible with any network operator.

- A remote software application running at a service provider’s data centre which communicates with the UI app. This application typically implements (or connects to) service provider’s business processes (such as payment or ticketing) to deliver the mobile NFC-enabled service.

The next section discusses the various options for service providers to implement a UI app, depending on the complexity of their application, their technical skills, the diversity of handsets to be supported and their resources.

4.1 No UI App

If a service provider only needs the handset to be able to activate or deactivate a NFC service (see chapter 3), it may not need a UI app. The core wallet is able to perform basic NFC application management. Some mobile operators’ core wallets will also be able to store a virtual version of a service provider’s existing NFC card, enabling a NFC handset to function in the same way as a NFC plastic card (see section 3.1.2).

4.2 Native UI app implementation

A service provider can implement their own native UI app (an application developed specifically for the mobile handset’s operating system), which can then be launched by the mobile wallet as a standalone app. This UI app provides a dedicated user-interface to the relevant service.

Service providers could develop a compliant UI app for mobile NFC services in several different ways, such as:

- Extend existing mobile apps (such as a banking app) with NFC functionality, i.e. add new code that can communicate with a payment app on the UICC.

- Develop a new NFC-enabled UI app from scratch.

- Use tools provided by a mobile operator or third party that generates a UI app based on service provider data captured in a template. (See section 4.2.1 for details).

4.2.1 Native UI App development

Service providers can implement a native UI app either by extending an existing mobile application or by developing a new application. They will typically need one version for each handset operating system they intend to support.
4.2.2 Template-based UI App development

Different mobile handsets may need different UI apps, depending on which operating system the handset uses. To reduce the complexity of producing UI apps that are compatible with a core wallet and the handset’s operating system, mobile operators are likely to make tailored tools and other support available for service providers in many industries. In many cases, a mobile operator could provide the full application on behalf of the service provider. Figure 3 shows how a service provider could combine basic icons and text with a template provided by a mobile operator to quickly and easily create a customised UI app.

With this approach, generic apps can be used by multiple service providers for the same kind of business function. For example, a generic app for loyalty cards can be customised and used by different service providers.

4.3 UI App implemented by the extended wallet

As discussed in chapter 3, some mobile operators may provide additional functionality in their mobile wallets that a service provider can use to implement NFC services, rather than developing their own UI app. In this case, the service provider would not need to develop their own UI app. But they will need to supply the mobile operator with additional information, such as the service name, necessary to customise the extended features.

Figure 3: Generating a UI app from a Template
5 Annex

This annex goes into more detail about the concepts described in this paper and how to implement them. Note, it uses more technical language than the main document. The following glossary defines the terms used.

5.1 Definition of Terms

<table>
<thead>
<tr>
<th>TERM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Android mobile operating system</td>
</tr>
<tr>
<td>API</td>
<td>App Programming Interface</td>
</tr>
<tr>
<td>Applet</td>
<td>Java program for execution on the UICC</td>
</tr>
<tr>
<td>GSMA</td>
<td>GSM Association</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>MNO TSM</td>
<td>Mobile Network Operator Trusted Service Manager</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station Integrated Services Digital Network</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>SIM</td>
<td>An subscriber authentication application that runs on a UICC</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SP_CP</td>
<td>Service Provider Core Package</td>
</tr>
<tr>
<td>TSM</td>
<td>Trusted Service Manager</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal Integrated Circuit Card (commonly known as the SIM card)</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
</tbody>
</table>
5.2 Service App Lifecycle

This section describes the different steps service providers, mobile operators, end users, and other ecosystem players need to take to develop and deploy service provider NFC applications into end users’ mobile wallets. Figure 4 illustrates how different elements of the ecosystem could interact to create and manage a NFC service app.

Figure 4: Service App Lifecycle
The following sections list key lifecycle activities along with some of the different options available to carry out those activities:

### 5.2.1 App Development

There are many different ecosystem players who could potentially develop mobile NFC apps. Regardless of who is actually developing the app, the service provider is eventually responsible for submission of the application to the mobile operator.

To this end, the service provider must compile a Core Package (SP_CP) zip file containing:

- Metadata that describes the whole package.
- Zero or more UI apps for specific mobile phone platforms.
- Graphics and artwork the core wallet can use to present information about the installed services to the end user.
- Applets for installation on the UICC.

### 5.2.2 Registration

Service provider packages are identified by a URL-based on a domain owned by the service provider. This guarantees that no conflict in package identification can occur. Conflicts within a service provider should be managed by the service provider itself.

### 5.2.3 Test & Certification

Service provider apps need to be tested and certified prior to deployment. The mobile operator will subject the core package to a certain number of manual checks and automatic tests before approval. Test and certification activities might be delegated by mobile operators to specialised external certification labs.

### 5.2.4 Security

The core package is signed by the service provider in order to guarantee integrity and non-repudiation of the provided metadata, service provider apps, and UICC applets and extended features (if the extended wallet is implemented). Security for the included apps will depend on the security guidelines of the corresponding platform. Android apps, for example, are self-signed by the developer of the app.

- The service provider UI app’s access to the corresponding UICC applet is controlled by the mobile wallet.
- The core wallet and the service provider apps can secure their interactions by mutually checking their signatures. The core wallet might only allow registered service provider apps access to its exposed APIs.

The GSMA expects similar security mechanisms will be implemented by other operating systems.

### 5.2.5 Publication

There are several options to make service provider apps available to end users:

- **Scenario 1**: publish to mobile operator-specific or generally accessible mobile wallet catalogue.
- **Scenario 2**: publish on an apps store (an operating system (OS) app shop, mobile operator shop or a third party app shop).

Additionally, UICC applets need to be submitted to a trusted service manager (TSM) if they are not managed directly by the mobile operator.

### 5.2.6 Discovery

In order to ensure widespread usage, it is of paramount importance that service providers enable consumers to discover their apps in multiple ways.

Here are several scenarios for the end user discovery of new services:

- **Scenario 1**: Discover from a mobile operator app catalogue or from the mobile wallet itself.
- **Scenario 2**: The user enters an app code into the mobile wallet to trigger a download process.
- **Scenario 3**: Discover in an application store (OS app shop, mobile operator’s shop or a third party app shop).
- **Scenario 4**: Any web site or app can contain a wallet link to enable a user to discover a service provider app.
5.2.7 Service Provider App Download

The app download process should facilitate the installation of the user interface component of the service on to the end user’s handset.

The download options largely depend on the discovery options described previously:

- **Scenario 1:** End user downloads service provider app from a website.
- **Scenario 2:** Push mode: A SMS message is sent to the device, which upon reception triggers the download from a download site. The push message could be triggered by the end user when entering his or her mobile phone number (Mobile Station Integrated Services Digital Network- MSISDN) into a service provider registration page.
- **Scenario 3:** Download from an applications store.
- **Scenario 4:** Download via a wallet link on a web site or another app.

5.2.8 Service Provider App Installation

The installation of a service provider app proceeds as with any other app, according to OS-specific installation mechanisms.

Note, that the app installation in itself does not render the service operable. An applet also needs to be installed on the UICC (see section 5.11). It may also be necessary to personalise the service applets on the UICC and the app on the handset (see section 5.12).

Depending on the mobile operating system, the core wallet might take actions during the installation process, e.g. display status information about the services currently being installed. The core wallet could, for example, employ iconographic methods or simple colour codes (such as the traffic light paradigm: red, orange, or green status) to indicate the progress of service installation to the user.

5.2.9 UICC Applet Installation

Installing the applet on the UICC makes the actual smartcard and NFC functionality available on the customer’s handset.

Installation of the UICC applet on the UICC is normally carried out by a trusted service manager (TSM). In a case where the applet is provided in a core package, the mobile operator’s own TSM can provision that applet.

When it is installed on the UICC, the applet is personalised, i.e. user-specific data (such as account numbers or cryptographic secrets) is provisioned to the applet on the UICC. This personalisation process is implemented by the service provider or mobile operator TSM as outlined above.

5.2.10 Display

Finally, the service provider app’s graphical user interface (GUI) is presented to the end user. There are two possible variants for displaying the GUI:

- **Scenario 1:** Display the GUI within the wallet. The core wallet app includes an app manager from which the end user can view, configure, and execute his or her mobile NFC apps.
- **Scenario 2:** Display the GUI through the operating system (OS). A platform-specific app will be visible (typically with an icon) to the user through the phone OS user interface. Additional “shortcuts” may help organise the app’s visibility.
5.2.11 Execution

The options for executing an app on a handset are:

- **Scenario 1:** Execute from the wallet. If the end-user downloads an app through a wallet link in a web site or another app, the wallet’s NFC App manager will automatically execute the app.

- **Scenario 2:** Execute from the OS using the OS-specific app launcher.

- **Scenario 3:** Launch from another app and/or mobile web site by means of the “mwallet: schema”, i.e. a specially encoded URL requesting the wallet to perform a standardised action.

5.2.12 Update

There are several options for updating apps:

- **Scenario 1:** The package is versioned and the service provider can provide an updated package.

- **Scenario 2:** An update of the user interface can be also managed via: push through an apps store, push through an SMS or forced by the user interface itself.

- **Scenario 3:** Update of applet managed by TSM.

5.2.13 Removal

Applications can be removed from the wallet and handset by:

- **Scenario 1:** Removal can be triggered by the end user through the core wallet, which handles the removal of the service provider app and/or applet via calls to the TSM.

- **Scenario 2:** The service provider app is removed by the user using the OS-specific mechanisms.

- **Scenario 3:** The removal can be triggered by the core wallet and the TSM. For example, a service is discontinued due to a security concern when a phone is lost or stolen.

5.3 Framework Specifications

To support an interoperable framework for mobile wallets, the GSMA is publishing two sets of technical specifications.

1. **NFC Core Wallet Requirements and Core Package File Technical Proposal** – this document specifies the common requirements for a mobile wallet to ensure service providers apps can work across multiple operators. It specifies a format to be used by service providers to deliver information on their services to mobile operators. The specification also includes app programming interfaces (APIs) that could be used to exchange data with service provider apps in the future.

2. **NFC SP Applet Development Guideline** – this document specifies the implementation development guidelines for apps that reside on the UICC.
References

<table>
<thead>
<tr>
<th>Ref</th>
<th>Title</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>[B]</td>
<td>NFC Handset APIs &amp; Requirements</td>
<td>Version 2.0 (2011)</td>
</tr>
</tbody>
</table>

Authors

This document defines the mobile wallet requirements necessary to deliver mobile NFC Secure Services, and has been jointly developed by France Télécom, Telefónica, Telecom Italia, Deutsche Telekom and Vodafone. This white paper will be shared with other operators, device manufacturers, and with service providers and third party developers.

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>06/08/12</td>
<td>Document submitted to GSMA Document Approval Group (DAG) &amp; Products and Services Management Committee (PSMC) for approval, 3rd September 2012</td>
<td>PSMC and NFC</td>
<td>Peter Hofmann, Deutsche Telekom</td>
</tr>
</tbody>
</table>

Other Information

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 & questions are always welcome.

Security Classification

Non-Confidential GSMA White Paper

Antitrust Notice

The information contain herein is in full compliance with the GSM Association’s antitrust compliance policy.

Copyright Notice

Copyright © 2012 GSM Association

GSM and the GSM logo are the registered property of the GSM Association.
For further information please contact
prd@gsm.org
GSMA London Office
T +44 (0) 20 7356 0600
September 2012