Requirements for Single Wire Protocol NFC Handsets
Version 2.0
November 20, 2008
Pay-Buy-Mobile Initiative

Security Classification: Restricted

Document History

Version	Date	Brief Description of Change
1.0	July 2008	Version 1.0 For comment
2.0	November 2008	Version 2.0 release

TABLE OF CONTENTS

TABLE OF FIGURES

1. GENERAL

1.1. Purpose and Overview

This document is in support of the GSM Association's mobile Near Field Communications (NFC) initiatives and is intended to facilitate the availability of the needed Single Wire Protocol (SWP) NFC-enabled handsets required by the mobile network operators (MNO).

Mobile network operators (MNO) are considering the deployment of NFC services in the 2009/2010 timeframe. Multi-NFC applications must be supported with these handsets. This includes, but are not limited to, credit/debit payment, public transport ticketing, loyalty and service initiation (through tag reading).

In order to meet the deployment objective for the mobile NFC services, it is critically important that UICC based NFC mobile handsets become commercially available in a timely fashion.

In addition to providing support for the above stated timeframe for the potential commercial NFC service deployments, the device requirements document is intended to ensure commonality of features and functionalities across handsets while ensuring an optimum user experience.

The aim of the document is to provide a set of operator-defined minimum common set of requirements that will provide the handset manufacturers with guidance in terms of the features and functionalities to be made available on the UICC-based NFC mobile phones in order to support the NFC services under consideration by the mobile operators.

By defining this minimum set of features and functionalities, the aim is to avoid further delay in the availability of the required handsets by providing the manufacturers with guidance on operator requirements.

While this document attempts to define a minimum set of requirements for the GSMA mobile operators, an appendix has been included to reflect requirements that are deemed optional as they may not meet all mobile operator strategic objectives or properly support regional differences.

The content of this document was developed by the mobile network operators within the GSMA and includes significant inputs and contributions from across the mobile and financial industries based on the previously published version of the document.

This document is non-binding. It is intended to be a reference document for mobile network operators when defining their NFC device requirements and for handset manufacturers when developing and manufacturing new handsets to support NFC services.

1.2. Scope

The primary objective of this document is *to provide a guide* for mobile network operators intending to specify handset requirements in support of mobile NFC services. The document covers key areas of functionality expected by GSMA operators and the specific requirements needed in devices to support NFC services.

The focus of the document will be solely on those aspects of the handset that involves supporting mobile NFC services based on the use of the Universal Integrated Circuit Card (UICC) as the secure element (SE). The NFC modes addressed by these requirements are covered in section 3 of the document.

Requirements relating to NFC services based on the use of non-UICC SE options are out of scope.

Requirements for non-NFC services are not impacted or affected by these NFC requirements. The content of this document will draw heavily on the NFC Technical Guidelines documents previously published by the GSMA (Ref. 1, 2).

The document is not intended to:

- Provide functional requirements to support non-NFC mobile services;
- Replace individual operator's specification, requirements and quality control levels for devices;
- Contractually bind handset manufacturers.

The intended audience for this document consists of the handset manufacturers, chipset manufacturers and mobile operators involved in enabling NFC mobile services.

This document covers the following areas:

- General Requirements;
- Handset Architecture;
- Single Wire Protocol Support;
- Host Controller Interface Support;
- Handset Browser;
- User Interface;
- Application Support;
- OTA Provisioning;
- Security Requirements;
- Handset Testing and Certification;
- Interoperability;
- Performance;
- Power Management.

1.3. References

1. GSM Association White Paper, Mobile NFC Services, Version 1.0, February 2007.
2. GSM Association White Paper, Mobile NFC Technical Guidelines, Version 1.0, April 2007.
3. GSM Association White Paper, Mobile NFC Technical Guidelines, Version 2.0, November 2007.
4. GSM Association White Paper, Pay-Buy-Mobile Business Opportunity Analysis, Version 1.0, November 2007.
5. ETSI TS 102 613 Release 7, Smart Cards; UICC-CLF Interface; Physical and Data Link Layer Characteristics.
6. ETSI TS 102 622 Release 7, Smart Cards; UICC – Contactless Front-end (CLF) interface; Host Controller Interface (HCI).
7. Open Mobile Alliance OMA-TS-Smartcard_Web_Server-V1.0, April 2008.
8. ISO/IEC 14443; Identification cards – Contactless integrated circuit(s) – Proximity cards.
9. Java Specification Request (JSR) 177: Security and Trust Services API (SATSA) for Java 2 Platform, Micro Edition (Final Release 3 September, 2004 and Maintenance Release 20 August, 2007).
10. Java Specification Request (JSR) 257: Contactless Communication API (Final Release 17 October, 2006).
11. ETSI TS 102 600 Smart Cards; UICC-Terminal interface; Characteristics of the USB interface (Release 7).
12. EMV Contactless Specifications for Payment Systems; EMV Contactless Communication Protocol Specification, Version 2.0, August 2007.
13. ETSI TS 102 484 Smart Cards; Secure channel between a UICC and an end-point terminal (Release7).
14. GSM Association Requirements for Single Wire Protocol NFC Handsets V1.0, July 2008.
15. GlobalPlatform Card Specification Version 2.2, March 2006.
16. ETSI TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics.
17. ETSI TS 102 223 Smart Cards; Card Application Toolkit (CAT).
18. NFC Forum Technical Specification Type 4 Tag Operation Specification, NFCForum-TS-Type-4-Tag_1.0; 2007-03-13.
19. Java Community Process (JCP), JSR 118: Mobile Information Device Profile 2.1,

1.4. Abbreviations

BIP	Bearer Independent Protocol
CAT	Card Application Toolkit
CLDC	Connected, Limited Device Configuration
CLF	ContactLess Frontend
ETSI	European Telecommunications Standards Institute
ETSI-SCP	ETSI Smart Card Platform
HCI	Host Controller Interface
IP	Internet Protocol
MMI	Man Machine Interface
MNO	Mobile Network Operator
NFC	Near Field Communications
OTA	Over the Air
OMA	Open Mobile Alliance
POS	Point of Sale
SATSA	Security and Trust Services API
SCWS	Smart Card Web Server
SE	Secure Element
STK	SIM Application Toolkit
SWP	Single Wire Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UICC	Universal Integrated Circuit Card
USB	Universal Serial Bus

1.5. Definition of Terms

For the purposes of the document, the following terms and definitions apply:

- A "**Device**" is the user's mobile phone that is normally used to provide mobile telephone service and in addition contains the NFC chip for support of the contactless services. The terms mobile device and handset are used interchangeably throughout the document;
- "**UICC**" is the smart card (defined in 3GPP TS102 221) which contains account information and memory that is used to enable GSM and UMTS cellular telephones;
- "**Secure Element**" is the smart card in the handset that will store and execute the contactless applications. In this document the focus is on the selection of the UICC as the secure element;
- "**Service Provider**" refers to the entity that provides the service that is utilised by the end user. In the case of proximity contactless mobile payment, this could be the card issuing bank and the transit authority in the case of contactless transit ticketing.

2. DEVICE OVERVIEW

The requirements defined in this document are based on the GSMA recommendation that the Universal Integrated Circuit Card (UICC) provides the most appropriate Security Element (SE) in the phone. The requirements do not however preclude the existence of additional Security Elements either embedded or removable within the handset. The UICC SE will be capable of securely storing and executing multiple contactless applications provided by different service providers.

The mobile device will be required to support multiple NFC payment applications as well as support for non-payment applications such as public transport ticketing and service initiation through tag reading. The Secure Element (UICC) may be shared by multiple applications provided by different service providers including the mobile network operator.

NFC M-Payment is defined as the combination of contactless payment services with mobile phones, based on NFC technology. The mobile phone with a hardware-based secure identity token (the UICC) can provide the ideal environment for NFC applications. The UICC can supplement the physical plastic credit or debit card, providing benefits for the service provider and offering users additional convenience and options when making payment at the point-of-sale (POS) terminals.

NFC M-Ticketing may be defined for the purpose of this document, as the combination of contactless transport services with mobile phones, based on NFC technology. In NFC M-Ticketing, the NFC mobile phone has to support the reader infrastructure of the public transport provider. Currently, most contactless smart card based transport systems use ISO/IEC 14443 or a proprietary variation of the standard. The NFC Forum also supports ISO/IEC 14443.

An important requirement of electronic ticketing systems for public transport is the speed of a transaction. The card emulation mode in the NFC mobile phone / UICC should be comparable or better in performance to that of a contactless smart card.

If a transport ticketing application can communicate with the electronic ticketing application, then all types of added value functions can be offered. The evolution of the mobile device can now provide a rich and dynamic user interface along with an ever increasing faster internet connection speed. This enables the development of advanced applications to support the NFC services, for example, in the Java environment. The mobile operator may also choose alternatively, to present the user interface for NFC services from the UICC utilizing the OMA Smart Card Web Server (SCWS). With the SCWS, the UICC user interface evolves from text based (STK) to a multi-media rich experience.

3. DEVICE REQUIREMENTS

As identified in the Scope section, the requirements for the mobile device included in this document are incremental to existing handset requirements and are intended to only address the features and functionalities necessary to support the enablement of mobile NFC services and applications.

Wherever possible the requirements in this document are based on existing approved NFC-related standards for the mobile phone.

This document captures requirements relating to the following areas:

3.1. General Requirements

[3.1-1] The addition of these capabilities based on the identified requirements should not negatively impact the use of the phone for the basic telecom services such as voice and data; and vice-versa. For instance, during a transaction it shall be possible for the end user to receive voice or data communications without disruption of the NFC service transaction. In addition it shall be possible to perform an NFC transaction while in voice or data communication mode.

3.2. Architecture Requirements

[3.2-1] A handset supporting NFC based applications shall at a minimum incorporate the following components:

- An RF proximity antenna;
- An NFC controller/chipset connected to the UICC and also to the RF antenna and baseband controller;
- A standardized connection between the UICC and the NFC controller;
- The baseband processor with the supporting functions needed for the NFC applications. Examples of such functions would include the browser, the man-machine interface (MMI), etc.

Other components of relevance in supporting the NFC services include:

- the browser;
- the modem required to access the mobile network; and
- the man-machine interface (MMI).

Where necessary, requirements affecting these components will be identified throughout the document.

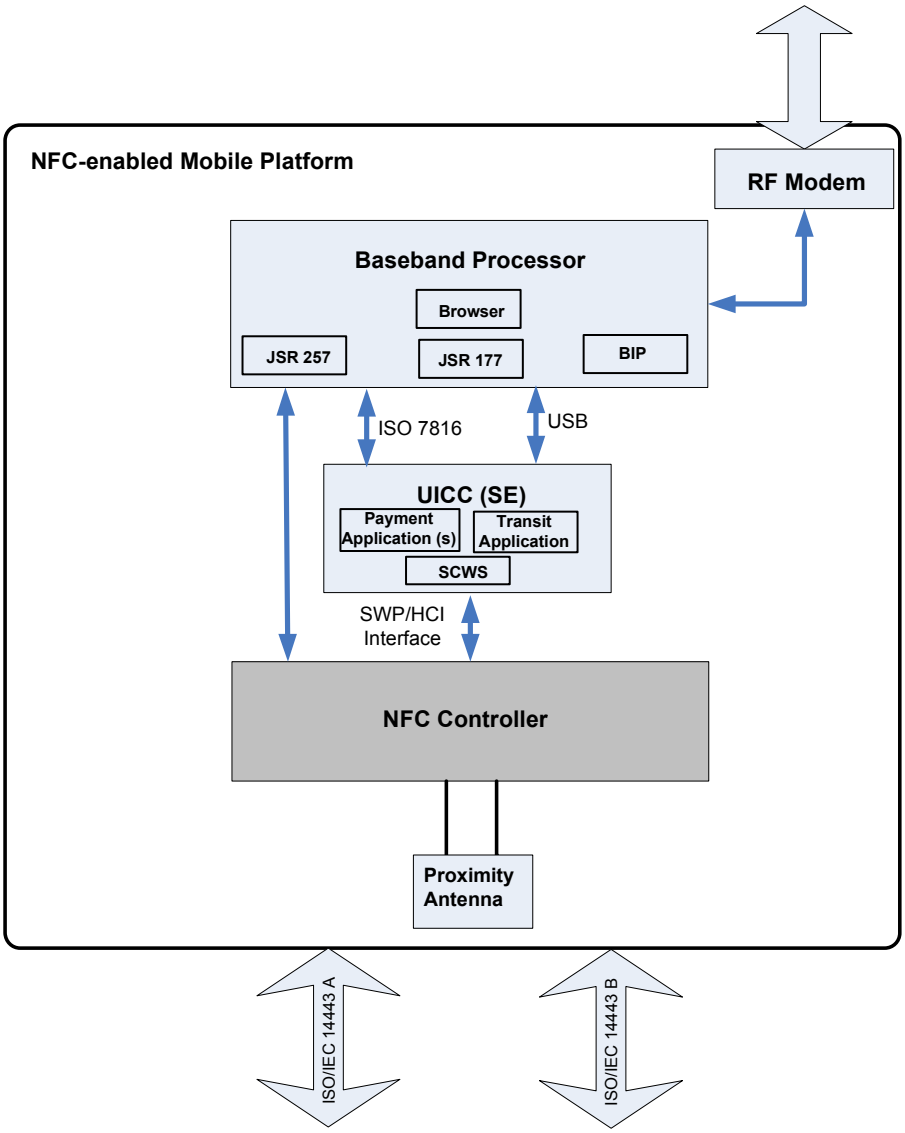

Figure 3-1: NFC Handset Functional Architecture.

Although a Payment application and Transit application is shown in the UICC, other applications for other NFC services can also run in the UICC

Figure 3-1 provides a high level architecture for the NFC mobile phone. The focus of the architecture as shown is on the key components for which requirements are being defined in this document. No new requirements are being specified for those components of the handset that are required for the support of existing services.

As shown above and as stated earlier, only the UICC SE is being addressed in this document. The requirement for a non-UICC SE is outside the scope of this document which focuses on a single-host architecture.

3.2.1 NFC Controller

[3.2.1-1] The NFC Controller/chipset shall support contactless communication in the following modes:

- Card emulation mode - supports at least both payments and ticketing (i.e. public transport); and
- Reader mode – supports NFC Forum Type 4 tag (ISO 14443-4 tag).
- Peer to peer application is outside the scope of this document as the necessary standards are not available at the time of writing.

[3.2.1-2] The handset is required to be fully interoperable with the existing contactless infrastructures being deployed for applications such as proximity payment, transport ticketing, etc. As a minimum therefore, the ISO 14443 Type A and Type B communication protocols must be supported, both in reader and card emulation modes.

[3.2.1-3] In addition to the requirements stipulated in this document, it is anticipated that mobile network operators will individually specify requirements for proprietary transport protocols based on ISO 14443 Type A and Type B to meet their own market needs in their own device requirements. Such protocols are outside the scope of this document and will not be addressed further.

3.2.2 The Proximity Antenna

[3.2.2-1] The proximity antenna provides the radio interface between the NFC handset and the NFC-compatible contactless point of sale reader or terminal. Implementation of the Technical interface for the proximity antenna should be based on the ISO 14443 standard.

[3.2.2-2] Additionally, for payment applications the proximity antenna implementation shall be based on the EMVCo's EMV Contactless Communication Protocol Specification [Ref. 12].

3.2.3 UICC/Handset Interfaces

[3.2.3-1] The NFC handset shall be capable of inter-working with any UICC smart card that complies with the ETSI technical specifications identified in the Reference section (Ref. 5 and 6) and conforms to the appropriate GlobalPlatform specification 2.2 and the latest Java card specification.

[3.2.3-2] Mobile network Operators (MNOs) have recommended the UICC as the most appropriate NFC Secure Element (SE) in mobile phones for card emulation and reader modes, offering many unique advantages for the customer, including: universal deployment, portability, remote management, standards based solution and a long operational lifecycle (Ref. 3). The interface between the UICC and the handset must be based on the approved standards as identified in this document.

[3.2.3-3] There are two internal interfaces with the UICC that are required to be supported by the handset. These are:

- ISO 7816 (ETSI TS 102.221);
- Single Wire Protocol/Host Controller Interface (ETSI TS 102.613 and TS 102.622).

[3.2.3-4] The physical interface and the data link layer between the UICC and the NFC chip shall be based on the Single Wire Protocol specification as defined in ETSI TS 102 613.

[3.2.3-5] The logical interface between the UICC and the NFC chip shall be based on the Host Controller Interface (HCI) specification as defined in ETSI TS 102 622.

[3.2.3-6] Implementations of TS 102 221, TS 102 223 and TS 31.111 are required to support the proper operation of SWP / HCI and contactles applications in general (For example, HCI Connectivity Event).

3.2.4 Java ME Support

[3.2.4-1] The Handset shall provide support for Java ME MIDP 2.1 (JSR 118).

[3.2.4-2] JSR 177 Security and Trust Services API (SATSA) are required in order to provide secure communications between the MIDlets running in the handset and the Java Applets stored in the UICC. Access control as provided in the JSR 177 is required as a degree of protection of the secure element from attacks by malicious applications. Moreover, it is recommended to implement Appendix A (Recommended Security Element Access Control) to increase the level of security of the solution.

3.3. User Interface Requirements

The User Interface identifies the enabling technologies that are required on the handset to provide the user with the ability to control the payment, ticketing and any other NFC applications contained in the SE. This user control will be enabled through a User Interface application (referred to as the mobile wallet) that may optionally reside in the phone or in the secure element/UICC itself.

The mobile wallet is the software application that provides the user of the mobile phone with the necessary control over the NFC applications residing in the UICC. This control will largely depend on the user interface functionality. The choice and provisioning of the mobile wallet will be determined by the entity providing the wallet to the customer, which will depend on specific market situations. In this section, it is assumed however, that the operator will provide the wallet to the user.

This section details the user interface requirements to be enabled within the handset that are considered necessary to meet the needs of the user, the mobile operator and the service provider community.

The identification of requirements for and selection of, the wallet application itself is considered out of scope for this document.

3.3.1 General UI requirements

[3.3.1-1] The handset may support multiple user interfaces.

[3.3.1-2] The preferred user interface for payment service shall be based on a Graphical User Interface (GUI) interface. A GUI interface is considered essential in order to provide an optimum user experience as well as to support the branding requirements of the NFC service providers. The device should be capable of supporting such GUIs.

[3.3.1-3] Depending on the market in which the NFC handset will be utilized, the enabling technologies to be supported by the handset should include the following:

- SIM Tool Kit (STK);
- Smart Card Web Server (SCWS);
- Java-based handset middleware.

The choice of the above enabling technology to be utilized in the NFC handset will be at the discretion of the individual mobile network operator.

3.3.2 SIM Tool Kit (STK)

[3.3.2-1] The handset shall provide support for a text-based user interface based on the SIM Application Toolkit.

3.3.3 Smart Card Web Server (SCWS)

The Smart Card Web Server user interface option is a local web server residing on the UICC. The SCWS allows for the provisioning of on-card dynamic services and rich media presentation to the customer. Interaction within the user interface will occur utilizing the handset browser.

[3.3.3-1] Required handset support for the SCWS must be based on the OMA Smartcard Web Server technical specifications.

[3.3.3-2] Support for the SCWS will require the availability of a Bearer Independent Protocol (BIP) client and the BIP TCP server mode as described in ETSI TS 102 223.

3.3.4 Java-based Midlet

[3.3.4-1] The mobile operator will have the option to provide the user interface as a java based wallet application. This will be handset-based and will be installed, triggered and managed by the baseband controller.

[3.3.4-2] To ensure secure and trustworthy operation of the application, JSR 177 (SATSA) shall be utilized between the Java midlet and the Java applet in the UICC. Additional security around JSR 177 will be needed to prevent interception or manipulation of data between the MIDlet and the corresponding applet on the UICC, see section 3.6.2.

3.3.5 Handset Browser Requirement

[3.3.5-1] The browser provisioned in the handset shall be compliant with WAP 2.0 and HTTP 1.1.

[3.3.5-2] Local browsing shall be enabled.

3.3.6 Usability Function

[3.3.6-1] The man-machine interface (MMI) in the handset shall allow the NFC applications to make full use of the display and keypad in support of the entry of PIN and Pass codes required by the NFC or user interface applications, the service provider or the MNO.

3.4. Transport Protocol/Application Management Requirements

The distribution of the application to the mobile phone, the subsequent personalization and the post-provisioning management of the NFC applications residing on the UICC will require the use of over-the-air (OTA) facilities. This will require the device to support specific transport protocols as identified below.

[3.4-1] For the download of Applets to the UICC, the handset will be required to support several concurrent high speed IP connections utilizing Bearer Independent Protocol Card Application Toolkit Transmission Protocol (BIP_CAT_TP) or Transmission Control Protocol/Internet Protocol (TCP/IP) transport protocols. Because of the file sizes involved, the SMS bearer may be utilized to provide application management (activation/lock/unlock) and personalization.

3.5. Power Management

This section defines requirements for the support of the NFC services under the conditions of low battery power or battery power off.

The regions of operation and significant threshold power levels were defined in the Mobile NFC technical guidelines whiter paper (version 1.0, April 2007, contained within [2]) and are illustrated in Figure 3-2.

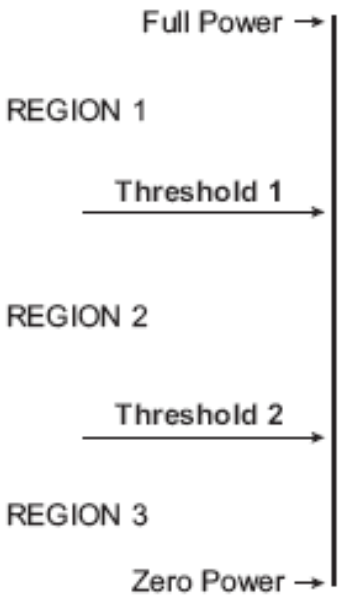

Figure 3-2: Power levels within the NFC phone

The regions are defined as follows:

- Region 1 (Full Power to Threshold 1): all functions are available in the mobile device;
- Region 2 (Threshold 1 to Threshold 2): all the functionalities of the mobile phone are shut down, except the clock module and a few other remaining functions;
- Region 3 (Threshold 2 to Zero Power): No functions are available in the mobile device.

[3.5-1] In order to ensure access to card emulation mode applications at all times, the NFC Controller shall be capable of operating in the Battery power On, Battery power Low and Battery power Off states.

[3.5-2] End users should be able to carry out an NFC transaction in a low battery power or battery power off situation where this is allowed by the service provider.

[3.5-3] To facilitate the above requirement, it shall be possible for the applications on the secure element to detect the current power state of the device.

[3.5-4] The ability to access transport ticketing in a low battery power or battery power off mode is seen as a key requirement by the end user and the transit operators.

[3.5-5] The RF power provided in the handset in the card emulation mode to support the transmission between the handset and the terminal shall be sufficient to enable a target operational range of 0 – 4 cm between the handset and the terminal.

[3.5-6] The handset shall support the capability to use the application in the power off mode as defined in the ETSI single wire protocol (SWP) specification (Ref. 5)

and where supported by the service provider. This is particularly desirable for such applications as ticketing and in some instances potentially, payment.

3.6. Security Requirements

This section identifies a set of requirements that are intended to ensure that the handset provides a highly secure and trusted environment as well as provide a barrier against possible malicious attacks and acts of fraud.

3.6.1 General Requirement

[3.6.1-1] The handset shall provide a simple mechanism for the user to ensure that NFC radio functions cannot be utilised without the user's awareness and explicit consent. This mechanism should be controllable from the user interface application.

3.6.2 UICC Handset Secure Channel

[3.6.2-1] Communication between the UICC applications and the handset shall be provided over a secure channel when required by the application.

[3.6.2-2] If a secure channel is required (e.g. for trusted display of payment amounts and personal assurance messages, capture of PIN without interception), then it should be conformant to ETSI TS 102 484.

[3.6.2-3] In the case of Midlets, this secure communication is facilitated by the use of JSR 177 (SATSA) as identified in the Architecture section.

[3.6.2-4] In the case of the SCWS, TLS shall be used to secure the communication between the handset and the UICC.

[3.6.2-5] To ensure the needed security and avoid interoperability issues, TLS shall be implemented in the handset as specified in Section 6 of ETSI TS 102 484.

3.7. Handset Certification and Type Approval

Certification and testing requirements for the handset is currently being developed by the industry. It is anticipated that such requirements will have an impact on the NFC handsets as defined in these requirements. Once such requirements have been reviewed and agreed with the mobile operator community, they will be incorporated into subsequent versions of this document.

3.8. Handset Performance

[3.8-1] While in card emulation mode with battery on, the performance of the phone shall be such that the overall transaction duration time shall not be significantly different from the transaction duration time when contactless cards are used.

4. APPENDIX A: OPTIONAL NFC HANDSET FEATURES

4.1. Introduction

The requirements identified in this Appendix are considered beyond the minimal feature set but may be desired by individual mobile network operators.

4.2. UICC/Handset Interface

[4.2-1] Support for the USB High Speed Protocol (HSP) as defined in ETSI TS 102 600 should be considered. The addition of the USB high speed interface in the handset and UICC could greatly improve the speed of the network access for the application management.

[4.2-2] The use of the USB interface in support of the SCWS would greatly improve the user experience and should be considered.

4.3. Dedicated Icon and Sound

[4.3-1] The handset should provide an icon and a sound when a proximity credential has been successfully accepted by the POS terminal. If this feature is supported, the handset shall support an API that allows an NFC application to signal to the handset that proximity credentials have successfully been accepted.

[4.3-2] A vibration should be provided in place of the sound when the device is in the silent mode.

4.4. Secure Screen Display and Keyboard Entry

[4.4-1] Information presented to the user may be displayed either on the contactless reader or via the handset keyboard and screen. Where the handset is used for such information presentation, the integrity and non-repudiation of information presented to the user via the handset display or keyboard must be assured. To meet this requirement of a secure display of the information on the handset, the handset manufacturer should ensure that suitable methods are provided to guarantee the security of the display and keyboard device drivers.

4.5. Additional Usability Functions

<u>One button – Enable User Interface Application</u>

[4.5-1] Access to the NFC applications could be provided using a single soft key or button on the handset. This single key or button would then provide access to the user interface application [wallet] provided by the mobile network operator.

[4.5-2] A pass-code entered on the keypad to open the application may also be provided by the mobile operator to be activated at the discretion of the user.

Enable/Disable NFC Function

[4.5-3] The user should have the ability to enable or disable all NFC services with a minimum set of key strokes or by using a physical switch (see Security section).

Active application Notification

[4.5-4] It must be clearly identifiable to the user that the NFC functionality is switched on by the visibility of a specific icon on the screen of the handset.

4.6. Additional Power Management Function

[4.6-1] With battery off operation, the end user should have access to a “default” NFC application previously set by the user through the installed wallet application function.

4.7. Additional Security Requirements: NFC Enabling Button

[4.7-1] The NFC radio should normally operate in the ON-mode but may be left in the OFF-mode at the discretion of the user.

[4.7-2] The ON-OFF switch should work whether the handset is powered on or off.

4.8. Support for JSR 257

[4.8-1] JSR 257 (Contactless Communication API) provides a standardized API for supporting contactless communication such as NFC in J2ME applications. This API requires as a minimum, the J2ME Connected, Limited Device Configuration (CLDC). Where JSR 257 is supported, it is mandatory to implement the package Javax.microedition.contactless and the Secure Element Push mechanism (Appendix B of the JSR257). Communication between the installed third-party MIDlets and the NFC chipset should be supported based on the use of JSR 257.

4.9. Mode Switching

[4.9-1] The user shall be able to activate or de-activate the NFC Radio Frequency interface. If the NFC Radio Frequency interface is activated then the NFC Mode switching (i.e. polling between Card Emulation mode. Peer-to-Peer mode and Reader/Writer mode) shall be done automatically.

[4.9-2] It shall be possible for the NFC application to select the NFC mode automatically. For example this could be used to improve the performance of the NFC service.