Mobile NFC Infrastructure
Version 1.0
30th July 2012

Security Classification – NON CONFIDENTIAL

Table of Contents

1 Introduction

1.1 Overview

With an increased activity in the Mobile Near Field Communication (NFC) ecosystem, a need for a global and standardised set of specifications and processes has arisen to address and guide UICC based implementations of NFC services.

This document outlines the existing and/or planned GSMA component specifications and processes, and defines where and how these interconnect within the overall mobile NFC infrastructure. These documents are not standards, but guidelines which may refer to other existing industry standards.

Its aim is to provide a common Mobile Network Operator (MNO) vision of Universal Integrated Circuit Cards (UICC) based NFC service application, promoting a stable, efficient and interoperable ecosystem development and reduced market fragmentation.

This Mobile NFC Infrastructure document will better enable professionals and organizations in the mobile NFC ecosystem to:

- Facilitate technical development with harmonized MNO processes and aid commercial deployment of Mobile NFC Services;
- Develop common specifications for interoperability and industry wide support.

1.2 Scope

This document presents an overview of the NFC ecosystem and presents, in that context, references to additional technical documents published, or planned to be published, through the GSMA:

- NFC Handset APIs Requirements Specification
- NFC UICC Requirements Specification
- Multi Protocols for Contactless Interoperability
- MNO - SP interface : Business Process Implementation Guidelines using the GlobalPlatform protocols

1.3 Definition of Terms

Term	Description
API	Application Programming Interface
AFSCM	Association Française du Sans Contact Mobile
CLF	ContactLess Front-end
CLT	ContactLess Tunnelling
ETSI	European Telecommunications Standards Institute
GCF	Global Certification Forum
GP	Global Platform
HCI	Host Controller Interface
HW	Hardware
IEC	International Electrotechnical Commission
IS	Information System
ISD	Issuer Security Domain
ISO	International Organization for Standardization
MNO	Mobile Network Operator

MSISDN	Mobile Station Integrated Services Digital Network
NFC	Near Field Communication
OS	Operating System
OTA	Over The Air
PoS	Point-Of-Sale
RF	Radio Frequency
SD	Security Domain
SSD	Supplementary Security Domain
SE	Secure Element
TSM	Trusted Service Manager
SP	Service Provider
STK	SIM (Subscriber Identity Module) Tool Kit
SWP	Single Wire Protocol
UI	User Interface
UICC	Universal Integrated Circuit Card – This is the technically correct name for a 'SIM card'

1.4 Document Cross-References

Ref	Title
[1]	[1] [ETSI TS 102 613 Smart Cards; UICC – Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics v 7.8.0 (2010-04)
[2]	[2] ETSI TS 102 622 Smart Cards; UICC – Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) v 7.8.0 (2011-01)
[3]	[3] Global Platform Card Specifications v 2.2.1
[4]	[4] Global Platform Card Specification v 2.2, Amendment C: Contactless Services Version v.1.0
[5]	[5] Global Platform Card Specification Version 2.2, Amendment A: Confidential Card Content Management v 1.0
[6]	[6] GP System Messaging Specification for management of mobile-NFC Services v 1.0
[7]	[7] AFSCM "Introduction to AFSCM Mobile NFC Service Specifications" release 1.0
[8]	[8] GSMA Mobile Ticketing White Paper, v1.0, February 2011
[9]	[9] GSMA Handset APIs & Requirements v2.0
[10]	[10] GSMA UICC Requirements Specification v2.0
[11]	[11] GSMA Multi Protocols for Interoperability (to be published, 2012)
[12]	[12] GSMA MNO – SP Interface: Business Process Implementation Guidelines using GP protocols
[13]	[13] INTERFACE SPECIFICATION Between Telecom Operators and NFC Service Providers, 09/09/2011

2 Overview of the relevant documents

2.1 Handset Requirements Specification

The purpose of this document, GSMA Handset Requirements Specification [9] is to provide handset manufacturers with a set of common NFC handset requirement specifications that an NFC handset shall fulfil to participate in the NFC ecosystem. It also defines the application architecture required to fulfil the secured NFC use cases and the handset Application Programming Interfaces (APIs) for Operating Systems (OSs).

Its scope is restricted to software platforms/application frameworks that are supported by handset manufacturers and defines at a high level the application architecture required to

fulfil the *secured* NFC use cases. It further expands upon this, by detailing the particular handset APIs per OS to enable a *secured* service use case and the atomic requirements necessary to fulfil the NFC software architecture.

2.2 UICC Requirements Specification

This document, GSMA UICC Requirements Specification [10] sets out a common framework of requirements for Universal Integrated Circuit Cards (UICCs) to support UICC-based NFC services, selecting options among those allowed by existing standards to ensure interoperability.

It lists for the NFC UICC a minimum set of requirements and the specification of technical gaps identified in order to ensure the efficient and consistent development and deployment of NFC services. In particular this document details references to the standard technical specifications, by mandating which optional requirements shall be considered mandatory for the NFC UICC for enabling interoperable solutions.

2.3 Multi Protocols for Interoperability

This document, GSMA Multi Protocols for Interoperability [11] makes recommendations to handset manufacturers and to Proximity Coupling Device (PCD) manufacturers to ensure their interoperability.

The NFC mobile handset and UICC combination needs to be compliant with several infrastructures (e.g. payment, access control, public transportation, etc.), whereas a contactless plastic card is compliant with only one single infrastructure.

ISO/IEC 14443 [2], [3], [4], [5] standards are composed of a set of parameters and options. The main objective of this document is to define a configuration in line with these standards that allows the UICC to host several types of data and applications.

2.4 MNO - SP Interface: Business Process Implementation Guidelines using GP protocols

This document, GSMA MNO – SP Interface: Business Process Implementation Guidelines using GP protocols [12] is concerned with the matter of interoperability between Service Provider Trusted Service Manager (TSM-SP) and Mobile Network Operator Trusted Service Manager (TSM-MNO) platforms in order to manage NFC services.

This document defines the implementation of AFSCM [7] [13] interaction processes using GlobalPlatform Messaging Specification for Mobile NFC services [6].

3 Mobile NFC Overview

3.1 NFC Mobile Handset

The NFC Mobile Handset is divided into three main components: the NFC controller, the UICC acting as a Secure Element (SE) and the User Interface.

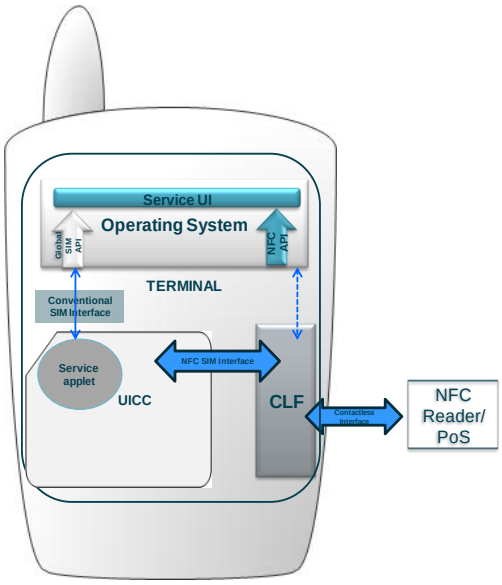

Figure 1: : NFC Mobile Handset

3.1.1 UICC as Secure Element

In its role as the UICC issuer, the MNO manages the UICC for enabling 3rd parties to securely store their NFC applications on the UICC – the MNO is therefore a key contributor to the provisioning and the security of UICC-enabled services. The detailed agreements depend on respective business models, commercial agreements and the chosen mode as specified by Global Platform (simple and delegated management mode described in the referenced documents).

The UICC provides both logical security (i.e. command encryption) and physical security (i.e. tamper proofing and copy protection) allowing Mobile NFC applications to be executed in a secure environment if applications comply with standardized security requirements.

Additional advantages using the UICC are that it is based on global and well-established standards (such as ETSI-SCP, 3GPP, Global Platform) covering application management, Over The Air (OTA) communication, and isolation.

Thus, the UICC provides the tools for:

- *Security between applications*: the UICC provides a firewall mechanism to ensure a total separation between the applications;
- *Secure communication channel*: The UICC offers a secure communication channel between the Service Provider's Platform and its application.

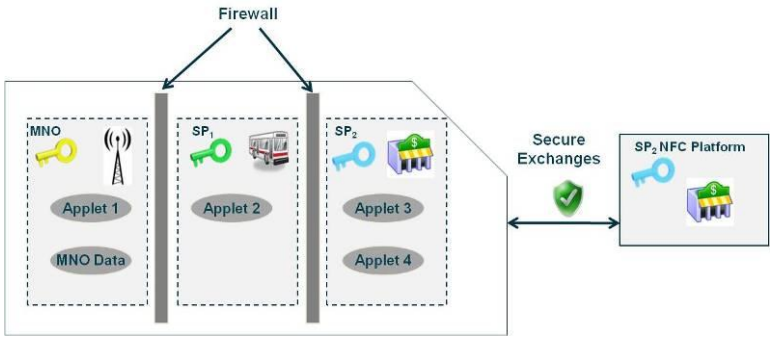

Figure 2: UICC as a Secure Element

A detailed description of the UICC and the requirements that must be fulfilled to be the Secure Element (SE) in the NFC ecosystem are described in the document ***"NFC UICC Requirements Specification***UICC Requirements Specification***"***.

The application developed in the UICC is called Applet and its development is well defined via Java Card technologies.

3.1.2 NFC Controller ContactLess Front-end

The NFC controller handles the physical transmission of data over the Radio Frequency (RF) interface allowing the mobile device to communicate via the NFC bearer using the three different modes: card emulation, reader/writer, and (optionally) peer to peer modes.

The ContactLess Front-end (CLF) must include a certain number of procedures that are needed in order to establish, configure, maintain and to react to certain events from the contactless interface (changes in the field, commands from the external device etc.) or from the service application inside the UICC (read tag, send event to the User interface in the handset etc.).

The following figure shows both interfaces:

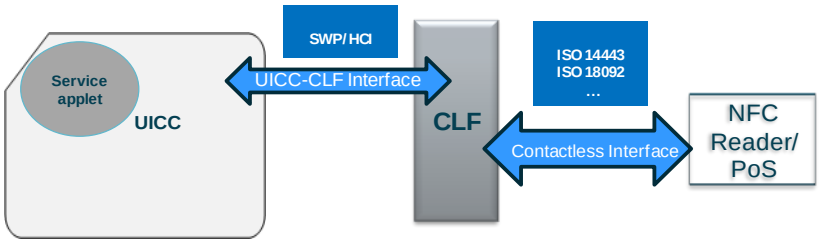

Figure 3: NFC Controller Interfaces

3.1.2.1 Contactless Interface: CLF-External Device

This interface, called Contactless Interface, supports all NFC technologies (ISO 14443 A & B contactless communication), as well as both reader/writer and card emulation modes.

As the NFC ecosystem will have several contactless technologies that directly affect the Mobile Handset, the CLF must switch to the different contactless technologies automatically. For example, the introduction of the Mobile Device (Handset+UICC combination) into the environment makes it necessary to add new specifications and new certification bodies and documents to ensure that every combination of reader and Mobile Device works in terms of range, speed and strength of field. An analysis of the contactless interoperability is described in the ***"Multi Protocols for Interoperability*Error! Reference source not found.*"*** document.

3.1.3 CLF-UICC Interface

The CLF must redirect the data enclosed towards the UICC which will store the actual NFC application waiting to receive the data. Thus, the data is sent through the UICC-CLF interface based on HCI and SWP protocols defined in ETSI specifications.

The SWP (Single Wire Protocol), ETSI TS 102 613 [1], supports the Physical and Data Link Layer of the communication between the CLF and the UICC in an NFC environment. It includes a ContactLess Tunnelling (CLT) mode that is used as a tunnelling procedure for protocols with stringent timing constraints and/or non-compliancy to ISO 14443 part 4. Whereas the HCI (Host Controller Interface), ETSI TS 102 622 [2], defines the logical interface that enables communication between UICC and CLF.

3.2 NFC Applications-User Interface

The User Interface (UI) is one of the key value propositions of Mobile NFC for the end customer, being a key element for the success of the Mobile NFC services. The UI application provides the interface to the customer by controlling the display keypad.

Currently there is a single approach promoted by GSMA to develop an efficient UI for Mobile NFC services: Android, J2ME, Web Application, etc.

Access control to the UICC and additional security steps are needed to guarantee secure and trustworthy operation of the application. For J2ME applications, the secure access to UICC is done via JSR177 Annex A mechanisms, however for other Smartphone OS (e.g. Android, WindowsPhone, etc.) UICC access and access-control are none existent. Thus there is a need to promote the availability of a Global UICC API and an Access Control policy that must be consistent throughout different Smartphone OSs (e.g. Android, J2ME, WP7, etc.). This topic is reflected in the ***"NFC Handset APIs Requirements Specification"***, with future versions planned to accommodate future releases of device Operating Systems.

3.2.1 Mobile Wallet

The Mobile Wallet can be considered as an "entry point" and "place" where customers can manage their NFC Services. The wallet enables and brings together a wide range of contactless applications: payments, m-commerce, ticketing [8], loyalty, advertising, e-couponing, etc. in one place.

3.3 TSM-MNO Platform

One of the main advantages of a Mobile NFC environment over traditional contactless cards is the ability to remotely and effectively deploy and manage content or services in the UICC

at a reduced cost and timescales, and in a dynamic manner in which any change is possible in a matter of minutes. For enabling SPs to remotely manage their applications, platforms using the mobile network and protocols to send commands to the handset and the UICC are specified and commercially available (TSM-SP).

Such TSM platform allows the SP to open a secure channel with its security domain and manage its application installation and lifecycle. To allow a mutual management of NFC services this TSM platform requires to be connected to the MNOs Platforms in charge of the UICC lifecycle management. Processes and interface are described in the ***MNO - SP Interface:*** **Business Process Implementation Guidelines using GP protocols*”*** document.

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	27/04/12	Document submitted to DAG & PSMC for approval, final approval date 30th July 2012	PSMC	Alicia Rodríguez de la Riva & Javier Ortuño Perez, Telefónica

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.