Global Handset Requirements for CDMA - NFC for CDMA Terminals

CDG Document 206

Version 1.0

May 2012

CDMA Development Group
575 Anton Boulevard, Suite 560
Costa Mesa, California 92626
PHONE +1 888 800-CDMA
+1 714 545-5211
FAX +1 714 545-4601
http://www.cdg.org
cdg@cdg.org

Contents

Revision History

Date	Version	Description
May 2011	1.0	Initial Release

1. Introduction

1.1 Purpose

The purpose of this document is to specify the requirements for NFC (Near Field Communications) on a CDMA terminal. Near Field Communication is a wireless communication technology also known as short distance radio communication that permits the data transfer of small data amounts over short distances. It is a wireless connectivity technology that enables simple two-way interactions between devices, allowing consumers to perform contactless transactions, access digital content, and connect electronic devices with a single tap. Requirements will be specified for different NFC modes of operation on a CDMA handset. There will be no requirements defined for various applications that might be used during NFC operation. The requirements are mostly based on industry standards as defined by ECMA (European Computer Manufacturers Association), ISO/IEC, (International Organization for Standardization/ International Electrotechnical Commission) NFC Forum and Global Platform, as well as specific operator requirements needed to ensure proper NFC operation.

1.2 Scope

The scope of the document is to outline a set of requirements and functionalities which are required to be supported for a CDMA device with NFC. Requirements will cover areas that include operating range, data rates, modes of operation that include card emulation, read/write and peer to peer, security (embedded/non-embedded) and interoperability. Specific requirements around the use and management of Secure Elements will also be covered. Finally a detailed set of software and hardware requirements, security requirements and guidelines for design of the NFC device are provided.

1

2 *1.3 Reference Documents*

Ref	Document Title	Author	Version	Date
1.	ISO/IEC 14443 Identification Cards – Contactless Integration Circuit Cards – Proximity Cards			
2.	ISO/IEC 18443 Information Technology – telecommunication and information Exchange Between Systems – Near Field Communication			
3.	ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation			
4.	ISO 8583			
5.	ISO 18092			
6.	ETSI 102 221 – UICC Terminal Interface			
7.	ETSI TS 102 225, Secured packet structure for UICC applications			
8.	ETSI TS 102 613, UICC - Contactless Front End (CLF) Interface, Part 1: Physical and data link layer characteristics			
9.	ETSI TS 102 622, UICC - Contactless Front End (CLF) Interface: Host Controller Interface (HCI)			
10.	ECMA 340 – Near Field Communication Interface and Protocol (NFCIP-1)			
11.	ECMA 356 – NFCIP-1 RF Interface Test Methods			
12.	NFCForum-TS-DigitalProtocol			
13.	NFC Forum Type 1 Tag Operation Specification			
14.	NFC Forum Type 2 Tag Operation Specification			
15.	NFC Forum Type 3 Tag Operation Specification			
16.	NFC Forum Type 4 Tag Operation Specification			
17.	Global Platform Card Specification v 2.2			
18.	GlobalPlatform Card Confidential Card Content Management Card Specification			
19.	GlobalPlatform Card Remote Application Management over HTTP			
20.	GlobalPlatform Card Contactless Services Card Specification			

Ref	Document Title	Author	Version	Date
21.	GlobalPlatform Card Technology Secure Channel Protocol 03 Card Specification			
22.	GlobalPlatform Card UICC Configuration			
23.	NFC Logical Link Control Protocol Technical Specification			

1

2 *1.4 Acronyms and Abbreviations*

3 ***Table 1: Acronyms and Abbreviations***

Acronym / Abbreviation	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
APDU	Application Protocol Data Unit
ASK	Amplitude Shift Keying
BIP	Bearer Independent Protocol
BIST	Built In Self Test
DASM	Device Application Security Management
DMA	Digital Management Access
ECMA	European Computers Manufacturers Association
ECDH	Elliptic Curve Diffie-Hellman
EMVco	Europay Mastercard Visa Company
ETSI	European Telecommunications Standards Institute
ISO	International Standards Organization
IEC	International Electrotechnical Commission
JCB	Japan Credit Bureau
MSL	Master Subsidy Lock
NFC	Near Field Communication
NDEF	NFC Data Exchange Format
NFCIP	Near Field Communication Interface and Protocol
NFC LLCP	NFC Logical Link Control Protocol

Acronym / Abbreviation	Description
NFC SEC	NFC Security
OMA	Open Mobile Alliance
OTA	Over The Air
PID	Parameter ID
PKI	Public Key Infrastructure
POS	Point of Sale
RTD	Record Type Definition
SMS	Short Messaging Service
SNEP	Simple NDEF Exchange Protocol
SSL	Secure Socket Layer
SWP	Single Wire Protocol
TEE	Trusted Execution Environment
TLS	Transport Layer Security
UICC	Universal Integrated Circuit Card

1.5 Terms and Definitions

Three categories of requirements are established:

(M) Mandatory	The handset **must** support that characteristic in order to achieve approval.
(HD) Highly Desirable	It is highly desirable and recommended that the handset supports this characteristic. This feature may become Mandatory in subsequent versions of the document. Supporting this characteristic will be valued in the commercial promotion of the device.
(O) Optional	It is left up to the manufacturer whether or not the device supports this characteristic. The handset **may** support this characteristic.

1.6 Carrier Acceptance

If required by the operator, the following documents and certifications **SHALL** be provided by the manufacturer for technical evaluation of the device:

1.6.1 Documentation

Req. #	Requirement	Terminal	Remarks	References	PRI Configurable
1.6.1.1	GHRC compliance report detailing compliance or non-compliance to each of the relevant sections of this document	M			N/A
1.6.1.2	EMVCo or Common Criteria certification	HD	Required by Visa, Master Card, American Express & JCB. Support is dependent on carrier		N/A
1.6.1.3	EMVCo Type1 Approval	HD	Required by Visa, Master Card, American Express, & JCB. Support is dependent on carrier		N/A
1.6.1.4	NFC Forum Wave 1 Certification	M	Wave 1 includes testing for the lower level digital protocols, specifically tag operations, digital protocol, and activity specifications		N/A
1.6.1.5	NFC Forum Wave 2 Certification	HD	Wave 2 adds testing for the physical layer and selected upper level digital protocols, including RF analog and peer-to-peer.		N/A
1.6.1.6	Isis Level 1 Certification	O	ISIS is joint venture between Verizon Wireless, AT&T &		

Req. #	Requirement	Terminal	Remarks	References	PRI Configurable
			T-Mobile. Support is dependent on carrier		
1.6.1.7	Isis Level 2 Certification	O	ISIS is joint venture between Verizon Wireless, AT&T & T-Mobile. Support is dependent on carrier		N/A
1.6.1.8	Global Platform Compliance	HD	Compliance is focused on functional & security aspects of embedded applications on secure chips. For Mobile Payments Applications this requirement is Mandatory		N/A

2. Requirements

This section states minimum requirements for a NFC device.

2.1 Minimum Standards Support

The following requirements apply to devices supporting NFC on a CDMA terminal

2.1.1 Protocol Support

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.1.1.1	Comply to ISO/IEC 14443 Specifications	M	Provides the 4 part baseline standards for communication between contactless cards		N/A
2.1.1.2	Support both Type A and Type B Cards	M			N/A
2.1.1.3	Comply to ISO/IEC 18092 / ECMA-340 Near Field Communication Interface and Protocol – 1 (NFCIP-1)	M			N/A
2.1.1.4	Comply to ISO/IEC 21481 / ECMA-352 Near Field Communication Interface and Protocol – 2 (NFCIP-2)	M			N/A
2.1.1.5	Comply to ISO/IEC 7816	M			
2.1.1.6	Support NFC Logical Link Control Protocol (LLCP) Technical Specification	M	Defines an OSI layer-2 protocol to support peer-to-peer communication between two NFC-enabled devices, which is essential for any NFC applications that involve bi-directional communications.	http://www.nfc-forum.org	N/A
2.1.1.7	Support NFC Digital Protocol Technical	M	Addresses the digital protocol for	http://www.nfc-forum.org	N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
	Specification		NFC-enabled device communication, providing an implementation specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards.		
2.1.1.8	Support NFC Activity Technical Specification	M	The specification explains how the NFC Digital Protocol Specification can be used to set up the communication protocol with another NFC device or NFC Forum tag.	http://www.nfc-forum.org	N/A
2.1.1.9	Support NFC Simple NDEF Exchange Protocol (SNEP) specification	M	The Simple NDEF Exchange Protocol (SNEP) allows an application on an NFC-enabled device to exchange NFC Data Exchange Format (NDEF) messages with another NFC Forum device when operating in NFC Forum peer-to-peer mode.	http://www.nfc-forum.org	N/A
2.1.1.10	Support EMV Contactless Communication Protocol	HD	Required for Payment Services based on EMVCo	http://www.emvco.com/specifications.aspx	N/A

2.1.2 NFC Data Exchange Formats

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.1.2.1	Support NFC Data Exchange Format (NDEF) Technical Specification	M	Specifies a common data format for NFC Forum-compliant devices and NFC Forum-compliant tags.	http://www.nfc-forum.org	N/A

2.1.3 NFC Tag Types

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.1.3.1	Support NFC Forum Type 1 Tag Operation Specification	M	Type 1 Tag is based on ISO/IEC 14443A. Tags are read and re-write capable; users can configure the tag to become read-only. Memory availability is 96 bytes and expandable to 2 kbyte.	http://www.nfc-forum.org	N/A
2.1.3.2	Support NFC Forum Type 2 Tag Operation Specification	M	Type 2 Tag is based on ISO/IEC 14443A. Tags are read and re-write capable; users can configure the tag to become read-only. Memory availability is 48 bytes and expandable to 2 kbyte.	http://www.nfc-forum.org	N/A
2.1.3.3	Support NFC Forum Type 3 Tag Operation Specification	O	Type 3 Tag is based on the Japanese Industrial Standard (JIS) X 6319-4, also known as FeliCa. Tags are pre-configured at manufacture to be either read and re-writable, or read-only. Memory availability is variable, theoretical memory limit is 1 MByte per service.	http://www.nfc-forum.org	N/A
2.1.3.4	Support NFC Forum Type 4 Tag Operation Specification 2.0	M	Type 4 Tag is fully compatible with the ISO/IEC 14443 standard series. Tags are pre-configured at manufacture to be either read and re-writable, or read-only. The memory availability is variable, up to 32 KBytes per service; the communication	http://www.nfc-forum.org	N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
			interface is either Type A or Type B compliant.		

1

2 2.1.4 NFC Record Type Definitions

3

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.1.4.1	Support NFC Record Type Definition (RTD) Technical Specification	M	Specifies the format and rules for building standard record types used by NFC Forum application definitions and third parties that are based on the NDEF data format.	http://www.nfc-forum.org	N/A
2.1.4.2	Support NFC Text RTD Technical Specification	M	Provides an efficient way to store text strings in multiple languages by using the RTD mechanism and NDEF format.	http://www.nfc-forum.org	N/A
2.1.4.3	Support NFC Smart Poster RTD Technical Specification	M	Defines an NFC Forum Well Known Type to put URLs, SMSs or phone numbers on an NFC tag, or to transport them between devices.	http://www.nfc-forum.org	N/A
2.1.4.4	Support NFC Generic Control RTD Technical Specification	M	Provides a simple way to request a specific action (such as starting an application or setting a mode) to an NFC Forum device (destination device) from another NFC Forum device, tag or card (source device) through NFC communication.	http://www.nfc-forum.org	N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.1.4.5	Support NFC Signature RTD Technical Specification	M	Specifies the format used when signing single or multiple NDEF records. Defines the required and optional signature RTD fields, and also provides a list of suitable signature algorithms and certificate types that can be used to create the signature.	http://www.nfc-forum.org	N/A

2.1.5 NFC Connection Handovers

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.1.5.1	Support NFC Forum Connection Handover Technical Specification	M	Defines the structure and sequence of interactions that enable two NFC-enabled devices to establish a connection using other wireless communication technologies. Connection Handover combines the simple, one-touch set-up of NFC with high-speed communication technologies, such as WiFi or Bluetooth.	http://www.nfc-forum.org	N/A

2.2 Hardware Requirements

The following requirements apply to devices supporting NFC on a CDMA terminal

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.2.1	Support an NFC Host Controller that manages the overall NFC operations between the terminal, UICC and 3rd party POS entity	M			N/A
2.2.2	Support a dedicated RF proximity antenna for NFC communication	M			
2.2.3	Support a Secure Element that is either embedded on the UICC or embedded in the NFC Chip or secure memory card and that is separate from the non-volatile memory of the terminal	M	The implementation is dependent on the Operator.		
2.2.4	Ability to support multiple Secure Elements	HD	There may be a requirement in some markets to have multiple secure elements co-exist on the terminal, ex: UICC, Secure SD, & embedded on terminal		N/A
2.2.5	For devices supporting UICC, be compliant to ETSI and 3GPP2 UICC Standards	M		http://www.etsi.org/WebSite/Technologies/Smartcards.aspx http://www.3gpp2.org/Public_html/specs/alltsgscfm.cfm	N/A
2.2.6	Support the ability to enable/disable NFC operation via a hard key that should work independently of the power on/off function of the terminal	M	This functionality is required to give the user control on NFC operation when the terminal is powered off		N/A
2.2.7	Support the use of a	HD	Operators may		N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
	Biometric reader on the device to authenticate the user prior to allowing a secure application session using NFC from proceeding		specify which applications (ex: payments) require biometric authentication		

2.3 Software Platform Requirements

The following requirements apply to devices supporting NFC on a CDMA terminal

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.3.1	Support providing APIs for the NFC Application to securely access the Secure Element on the UICC or terminal	M	Secure APIs provided can be part of the native or smart phone open OS environment or implemented via solutions such as Sim Alliance's Open Mobile API Specification		N/A
2.3.2	Support providing APIs for the NFC Application to access and make full use of the display and keypad/touch interfaces on the terminal	M			N/A
2.3.3	Support providing API's for NFC application to access audio controls on the device	M	This may be required if for example an audio confirmation is needed when an NFC transaction is successfully completed		N/A
2.3.4	Support providing API's for NFC application to access vibration controls on the device	M	This may be required if for example an vibration confirmation is needed when an NFC transaction is successfully completed in vibrate mode		N/A
2.3.5	Support API's for NFC	M			N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
	application to access telephony functionality (make call) on the device				
2.3.6	Support providing API's for NFC Application to access the Web Browser Client	M			N/A
2.3.7	Support providing API's for NFC Application to access the SMS Messaging Client	M			N/A
2.3.8	Support providing API's to access the battery power level of the terminal	M	The power level available will dictate the mode NFC will operate in. Ex: Card Emulation mode only if the battery power is not sufficient		N/A

2.4 Minimum Operating Requirements

The following requirements apply to devices supporting NFC on a CDMA terminal

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.4.1	Support operating at 13.56 MHz, with a bandwidth of +-7Khz	M	These standards form the baseline for NFC device requirements;		N/A
2.4.2	Support the capability to exchange data with another NFC device or tag over a distance of approximately 4 cm (not more than 2 inches).	M	These standards form the baseline for NFC device requirements;		N/A
2.4.3	Support the capability of enabling NFC and indication on the screen (logo, mark) when NFC is enabled	M	These standards form the baseline for NFC device requirements;		N/A
2.4.4	Support the capability of disabling NFC and the disappearance of the (logo, mark) from the screen	M	These standards form the baseline for NFC device requirements;		
2.4.5	Support the capability to communicate at data rates of 106kbps, 212kbps and 424 kbps	M	These standards form the baseline for NFC device requirements;		N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.4.6	Support the following modulations: Amplitude Shift Keying (ASK) (Polling Mode) and Load Modulation (Listening Mode)	M	These standards form the baseline for NFC device requirements;		N/A
2.4.7	Support Manchester Coding	M	These standards form the baseline for NFC device requirements;		N/A
2.4.8	Support a magnetic field strength, between 1.5A/m and 7.5A/m in operating volume	M	These standards form the baseline for NFC device requirements;		N/A
2.4.9	Support a RF field threshold of approximately HThreshold=0.187A/m	M	These standards form the baseline for NFC device requirements;		N/A

2.5 Modes of Operation

The following requirements shall be supported for all modes of operation

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.5.1	Support card emulation mode	M			N/A
2.5.2	Support read/write mode	M			N/A
2.5.3	Support peer-to-peer mode (ISO-18092, NFC-IP1 and LLCP)	HD			N/A
2.5.4	Support reading Type 1 tag	M			N/A
2.5.5	Support reading Type 2 tag	M			N/A
2.5.6	Support reading Type 3 tag	O	Type 3 is for Felica and only required in devices that need to operate in certain countries		N/A
2.5.7	Support reading Type 4 tag	M			N/A
2.5.8	Support being able to write Type1 tag	M			N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.5.9	Support being able to write Type2 tag	M			N/A
2.5.10	Support being able to write Type3 tag	O	Type 3 is for Felica and only required in devices that need to operate in certain countries		N/A
2.5.11	Support being able to write Type4 tag	M			N/A
2.5.12	Support being able to poll all technologies like NFC-A, NFC-B and NFC-F	M	NFC-F is for Felica and not mandatory		N/A
2.5.13	Support being able to operate in Poll and Listen mode	M			N/A
2.5.14	Support active and passive mode(high, low and no battery power) while operating in Card Emulation	M			N/A
2.5.15	Support operating at bit rate of 106kbps while reading a Type1 tag	M			N/A
2.5.16	Support Operating at bit rate of 106kbps while reading a Type2 tag	M			N/A
2.5.17	Support a payload of 253 bytes at a bit rate of 212kbps while reading a Type3 tag	O	Type 3 is for Felica and only required in devices that need to operate in certain countries		N/A
2.5.18	Support a payload of 254 bytes at a bit rate of 106kbps and 424kbps while reading a Type4 tag	M			N/A
2.5.19	Be compliant to Type 4A Tag platform while emulating a card according to NFC-A	M			N/A
2.5.20	Be compliant to Type 4B Tag platform while emulating a card according to NFC-B	M			N/A
2.5.21	Be compliant to Type 3 Tag platform while emulating a card according to NFC-F	O	Type 3 is for Felica and only required in devices that need to operate in certain		N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
			countries		
2.5.22	Support communication at 106kbps, 212kbps and 424kbps while operating in peer to peer mode	HD			N/A
2.5.23	Support not taking more than 250 msecs to do a transaction in card emulation mode	M			N/A
2.5.24	Support RF Collision Avoidance (Listen before talk) while operating in peer to peer mode	M			N/A
2.5.25	Support payload size of up to 254 bytes while operating in peer to peer mode	HD			N/A
2.5.26	Support Negotiated Handover (Bluetooth/WiFi) while operating in peer to peer mode	HD			N/A
2.5.27	Support Static Handover (Bluetooth/WiFi) while operating in peer to peer mode	HD			N/A

2.6 Application support

The NFC enabled terminal **SHALL** support the following minimum application requirements:

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.6.1	Support an application capable of reading Smart posters with a web address (initiating browser)	M			N/A
2.6.2	Support an application capable of reading Smart posters with action to dial a number	M			N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.6.3	Support an application capable of reading Smart posters with plain text message	M			N/A
2.6.4	Support an application capable of reading Smart posters with SMS initiation	M			N/A
2.6.5	Support an application capable of writing Type 1 tag	M			N/A
2.6.6	Support an application capable of writing Type 2 tag	M			N/A
2.6.7	Support an application capable of writing Type 3 tag	O	Type 3 is for Felica and only required in devices that need to operate in certain countries		N/A
2.6.8	Support an application capable of writing Type 4 tag	M			N/A
2.6.9	Support an application in card emulation mode as a debit card	M			N/A
2.6.10	Support an application in card emulation mode as a credit card	M			N/A
2.6.11	Support an application in card emulation mode as a loyalty card	M			N/A
2.6.12	Support an application in card emulation mode as a gift card	M			N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.6.13	Support an application in card emulation mode for access control	HD			N/A
2.6.14	Support an application in card emulation mode for ticketing (event, concert, transport)	M			N/A
2.6.15	Support an application in peer-to-peer mode for data transfer of up to 1 kb (vCard)	HD			N/A
2.6.16	Support an application in peer-to-peer mode for data transfer of up to 1 kb (Contacts)	HD			N/A
2.6.17	Support a application in peer-to-peer mode for pairing using Bluetooth	HD			N/A
2.6.18	Support an application in peer-to-peer mode for pairing using Wi-Fi	HD			N/A
2.6.19	Support an application in peer-to-peer mode for data transfer of more than 1 kb using Bluetooth (Picture, music)	HD			N/A
2.6.20	Support an application in peer-to-peer mode for data transfer of more than 1 kb using Wi-Fi (Picture, music)	HD			N/A
2.6.21	Support an application selecting the NFC mode of operation automatically	M			N/A
2.6.22	Support only the installation of signed NFC Applications on a trusted domain (ex Operator)	M			N/A

2.7 UICC based Secure Element

The NFC enabled terminal **SHALL** support the following Secure Element requirements if the Secure Element is based within the UICC.

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.7.1	For Secure Elements embedded in the UICC, the terminal **SHALL** support Single Wire Protocol (SWP)	M		ETSI TS 102.613 ETSI TS 102.622	N/A
2.7.2	Support the terminal UICC interface as defined by ETSI TS 102.221	M		ETSI TS 102.221	N/A
2.7.3	Support the SWP Host Controller Interface	M		ETSI TS 102.613 ETSI TS 102.622	N/A
2.7.4	Support SWP Physical and Data Link Layer interface	M		ETSI TS 102.613	N/A
2.7.5	Support SWP Logical interface	M		ETSI TS 102.622	N/A
2.7.6	Support UICC Card Toolkits required for SWP Operation	M		ETSI TS 102.221 ETSI TS 102.223 ETSI TS 31.111	N/A
2.7.7	Support Bearer Independent Protocol (BIP) for communication between UICC and terminal	M		ETSI TS 102.223	N/A
2.7.8	Support OMA Smart Card Web Services for interfacing with UICC's that support a Smart Card Web Server	HD		http://www.openmobilealliance.org/technical/release_program/scws_v1_0.aspx	N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.7.9	Support the APDU data structure as the basis of communication between the Secure Element and NFC Application	M			
2.7.10	Support JSR 257 Contactless API, should the terminal suppoer a JavaME environment	HD			N/A
2.7.11	Support JSR 177: Secure Applications & Trusted Services API on Secure Elements supporting JavaCard & Smart Card Web Services	HD	Mandatory if SCWS is supported and Java based Midlet is used, such as an e-wallet		N/A

1

2

2.8 Management of Secure Elements

The NFC enabled terminal **SHALL** support the following requirements pertaining to the management of Secure Elements

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.8.1	Should multiple Secure Elements exist on the terminal, there **SHALL** be a mechanism for the user to select which one is to be used for the NFC transaction	M	Mandatory, only if multiple Secure Elements exist		N/A
2.8.2	Should multiple Secure Elements exist on the terminal, there **SHALL** be a mechanism for the user to retrieve which Secure Element is active at any given time	M	Mandatory, only if multiple Secure Elements exist		N/A
2.8.3	Support only one Secure Element being active in a transaction in any given time	M			N/A
2.8.4	The terminal **SHOULD** support a Secure Element Admin Agent that manages the operations of the various Secure Elements on the device	HD	Secure Element Admin Requirements can be found in the Global Platform Secure Element Remote Application Management Specification	http://globalplatform.org/specificationscard.asp	N/A
2.8.5	Support the ability to over the air (OTA) update and provision the Secure Element for new applications	M			N/A

2.9 Interoperability support

The NFC enabled terminal **SHALL** support the following Interoperability requirements:

NFC Requirements for CDMA Handsets

1

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.9.1	A terminal supporting NFC **SHALL NOT** impact with the CDMA functionality of the terminal	M			N/A
2.9.2	A terminal supporting NFC **SHALL NOT** impact with the CDMA functionality of non emergency call origination	M			N/A
2.9.3	A terminal supporting NFC **SHALL NOT** impact with the CDMA functionality of emergency call origination	M			N/A
2.9.4	A terminal supporting NFC **SHALL NOT** impact any of the supplementary CDMA services, such as Call Waiting, Call Forwarding, Call Blocking etc.	M			N/A
2.9.5	A terminal supporting NFC **SHALL NOT** impact with the CDMA functionality of sending or receiving an SMS	M			N/A
2.9.6	A terminal supporting NFC **SHALL NOT** impact with the CDMA functionality of sending or receiving an MMS	M			N/A
2.9.7	A terminal supporting NFC **SHALL NOT** impact with the CDMA functionality of originating a non tethered data call	M			N/A
2.9.8	A terminal supporting NFC **SHALL NOT** impact with the CDMA functionality of originating a tethered data call	M			N/A
2.9.9	A terminal supporting NFC **SHALL NOT** impact with the Bluetooth functionality of the terminal	M			N/A
2.9.10	A terminal supporting NFC **SHALL NOT** impact with the Wi-Fi functionality of the terminal	M			N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.9.11	A terminal supporting NFC **SHALL NOT** impact with the GPS functionality of the terminal	M			N/A
2.9.12	A terminal supporting NFC **SHALL** adhere to Airplane Mode requirements and disable the NFC functionality while in Airplane Mode	M			N/A
2.9.13	Support handling NFC transactions while on a voice or data call	M			N/A
2.9.14	A terminal supporting NFC **SHALLNOT** automatically disable NFC capabilities in battery low conditions	M			NA
2.9.15	Support operating the terminal in Card Emulation Mode even when the terminal is powered off	M			N/A

2.10 Security Requirements

The NFC device **SHALL** support the following security requirements. If additional security requirements are implemented by the OEM in conjunction with or in lieu of the following requirements, they shall be shared with the operator.

2.10.1 General Requirements

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.10.1.1	Support NFC-SEC's NFCIP-1 Security Services & Protocol (ECMA 385)	HD	This standard specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the PDUs and protocol for those services.	http://www.ecma-international.org/publications/standards/Ecma-385.htm	N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.10.1.2	Support NFC-SEC-01 NFC SEC Cryptography Standard using ECDH and AES (ECMA 386)	HD	This Standard specifies the message contents and the cryptographic methods for PID 01	http://www.ecma-international.org/publications/standards/Ecma-386.htm	N/A
2.10.1.3	Support the ability to perform NFC based transactions only after getting the user's consent	M	This may be achieved by notifying the user via the user interface whether to proceed with transaction or not. In the case of Card Emulation Mode, the user consent **SHALL** be achieved by the POS terminal	http://www.ecma-international.org/publications/standards/Ecma-386.htm	N/A
2.10.1.4	Support 2 factor authentication when allowing secure transactions over NFC	M			N/A
2.10.1.5	Support PKI based cryptography for secure applications sessions using NFC capabilities such as those defined by: GlobalPlatform Device Application Security Management (DASM) Key and Certificate Management Specification	M	If alternate PKI based solutions are implemented by the OEM, they shall be shared with the Operator.	http://globalplatform.org/specificationscard.asp	N/A
2.10.1.6	Support secure application provisioning such as those defined by: GlobalPlatform Device Application Security Management (DASM) Provisioning Specification	M	If alternate application security management and provisioning is implemented by the OEM, they shall be shared with the Operator.	http://globalplatform.org/specificationscard.asp	N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.10.1.7	Support a Trusted Execution Environment (TEE) separate and isolated from the standard application runtime environment on the terminal, such as those defined by: Global Platform Trusted Execution Environment (TEE) System Architecture Global Platform Trusted Execution Environment (TEE) Internal API Specification Global Platform Trusted Execution Environment (TEE) Client API Specification	M	This is especially applicable for transactions dealing with mobile payments If alternate trusted security environment is implemented by the OEM, they shall be shared with the Operator.	http://globalplatform.org/specificationscard.asp	
2.10.1.8	Support SSL 3.3 / TLS 1.2 for secure application sessions that are leveraging NFC capabilities between Secure Element and NFC application on terminal	M		RFC 5246	N/A
2.10.1.9	Access to any NFC specific Configurations **SHALL** be protected by MSL Code	M			N/A

2.10.2 Application Security & Secure Element Access Control

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.10.2.1	Support an Access Control Policy to the Secure Element from NFC Applications	M	This policy is defined by the Operators, granting certain NFC applications certain rights and access to certain capabilities in the Secure Element		N/A
2.10.2.2	The Access Control Policy **SHALL** have listed all approved NFC applications and their associated rights to access the Secure Element	M			N/A

Req. #	Requirement	Category	Remarks	References	PRI Configurable
2.10.2.3	Storing the Access Control Policy on a secure location on the Secure Element not accessible by any 3rd party application	M			N/A
2.10.2.4	Access Control Policies **SHALL** be unique to the Secure Element. If multiple Secure Elements are present, each **SHALL** have its own Access Control Policy	M			N/A
2.10.2.5	Data from one Secure Element **SHALL NOT** be shared with Applications associated with other Secure Elements on the terminal	M			N/A
2.10.2.6	If the Access Control Policy does not include an entry for the NFC application in question, access to the Secure Element **SHALL** be prohibited to that NFC application	M			N/A
2.10.2.7	Support checking the Signature and Application ID (AID) of the NFC Application before granting access to the specific applet on the Secure Element	M			N/A
2.10.2.8	Should access be denied, an appropriate error message **SHALL** be displayed to the user	M			N/A
2.10.2.9	Support the use of a Certificate Chain for signing of NFC Applications	M	The full certificate chain has to be valid for the application to be accepted		N/A
2.10.2.10	Certificates **SHALL** be based on X.509 schema	M			N/A

3. Annex A: Security Considerations for NFC

This annex captures security considerations or guidelines that a manufacturer of NFC based terminals should take into account when designing and manufacturing their product. While they are not specifically a requirement to implement NFC technology, they are present here for informational purposes to ensure that security as a whole is considered for NFC based services.

3.1.1 Security Considerations against Software threats

#	Consideration	Remarks	References
3.1.1.1	Only permit download of applications from trusted sources that have been authorized by the service provider		
3.1.1.2	Approved NFC Applications should undergo some form of certification acceptable by the industry and be properly signed and provisioned on the terminal		
3.1.1.3	NFC Applications operating in either the terminal memory or UICC should have an extra layer of security separating them from other application environments on the terminal	This is achieved by supporting the Trusted Execution Environment (TEE) supported as per Global Platform requirements.	
3.1.1.4	The Terminal should perform checks during boot up or prior to execution of NFC transactions to ensure the integrity of the system (i.e. no code and static changes have been made to the File Loader piece of code)		
3.1.1.5	Prevent the storage of logs taken from security checks on the device. This can be done, as an example, by not implementing a journaling file system during security checks		
3.1.1.6	Any build in self test (BIST) functionality should be accessible by user only if available via MSL/SPC code		
3.1.1.7	Any APIS that are developed to allow access to Secure Element should be Type Safe APIs, such that malformed data cannot be sent to the terminal		
3.1.1.8	Type Safe APIs and non Type Safe APIs should not be mixed over the same domain boundary		

3.1.2 Security Considerations against Hardware threats

#	Consideration	Remarks	References
3.1.2.1	Restrict the memory the Digital Management Access (DMA) system can access with hardware extensions (address space limiters, micro-programmable DMA, MMU platform extensions, etc.) so that DMA cannot be used to move unauthorized data outside the secure framework of the device		
3.1.2.2	Ensure that the debug port cannot be used to access security critical assets, by locking the port while NFC is enabled		
3.1.2.3	Use security code or hardware to enable or disable JTAG for access to device.	JTAG can allow access to ports on the terminal for debug purposes and hence can be used for malicious use	
3.1.2.4	Use security code such as the Master Subsidiy Lock (MSL) code or hardware to enable or disable serial port for access to the security code space		
3.1.2.5	During physical design of PCB, route tracking channels sub-surface to the PCB such that access to physical probing by malicious entity is prevented	This may be needed, if for example, a device with secure element is stolen and physically hacked.	
3.1.2.6	Apply protective layers on the PCB to resist, or be indicative of, attempts to attach such probes	This may be needed, if for example, a stolen device with secure element is recovered	