DEVICE REQUIREMENTS
NEAR FIELD COMMUNICATION (NFC)

VERSION 5.1

Issued: June 2013

Prepared For:	Prepared By:
Verizon Wireless	Device Evolution

[Device supplier should contact Device Marketing Product Development for Assistance]

Revision History

Rev.	Author	Description of Changes	Date
1.0	Yuk Li Saloni Pokharna Praveen Venkataramu Jim Xanthos	Initial release Last tag ID used: 137	March 2011
2.0	Yuk Li Jim Xanthos Manuel E. Caceres Hannah Moon	Updated following requirements: • entrance criteria • overview • card emulation – power modes • deployment plans • mobile payments use case • smart posters use cases • peer to peer use cases • user performance expectations • architecture • NFC • card emulation power modes • mode of operation • single SE • UICC based SE • embedded SE memory size • cryptographic • antenna • SW APIs for MIDP2 Java devices • SW APIs for Dalvik Java devices • Java card • SE key control • application security • logical channel support • user interaction • software • NFC performance Added following requirements: • user interface for Contactless Front End • Contactless Front End disabled mode •SE certification • embedded secure keys • SW APIs for all devices • Card Application Toolkit Deleted requirement for the following:	September, 2011

		• user usage statistical analysis • cryptographic performance Last tag ID used: 145	
3.0	Manuel Caceres Heather Vaughn Yuk Li	• Added NFC security Tag handling requirer • Modified SE API requirements • Updated/added UI images	January 2012
4.0	Yuk Li Manuel Caceres Heather Vaughn	-Added requirements for connection handover -Added Requirements for Google Access Control -Moving UI images into a separate package -Updates to Peer-to-Peer functional security requirements -minor updates to user experience use case section device evolution strategies	April 2012
4.1	Manuel Caceres Heather Vaughn	-Added requirements for Global Platform SE Access Control -Added requirements clarifications for Android Open SIM Alliance API mapping -Added Performance requirements for Open SIM Alliance APIs	July 2012
4.2	Manuel Caceres	-Removed P2P UI Prompting System menu requirement, as it is already covered by the UI/UX -Removed effective date for GP, as all devices sha Now comply	October 2012
5.0	Manuel Caceres Yuk Li Warren Uy	-Removed Embedded SE requirements, OEMs Must follow ISIS certification if applicable -Removed Marketing Architecture sections -Removed not applicable sections -Clarified Requirements regarding Mifare Classic -Removed duplicate requirements -All requirements match a test case -Removed Marketing tags, Req-Pro tags will Only be used going forward	February 2013
5.1	Manuel Caceres	-Added GPAC Mode 1 support and retrieval Behavior for unknown tlvs. -Changed OMAPI performance requirements -Removing Google Access Control in lieu of GPAC -Wifi handover support	June 2013

TABLE OF CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

This document describes the requirements to be met by a wireless device OEM for Near Field Communication (NFC).

All requirements generated, only apply to new product launches. Any running changes or field upgrades need to be handled as special cases under extraordinary circumstances involving coordination with VZW Device Marketing and Network.**GLOSSARY/DEFINITIONS**

This section defines acronyms and terms used throughout the document.

Term [Abbreviation (if Applicable)]	Definition
NFC	Near Field Communication. Close proximity wireless contactless technology at 13.56MHz.
MNO	Mobile network operators
OTA	Over the air
TSM	Trusted service manager – party who manages the deployment of mobile applications and account data OTA to the device
POS	Point of sale terminals
HCI	Host Controller Interface
SWP	Single Wire Protocol
SE	Secure Element
GP	Global Platform
AC	Access Control
OMAPI	Open Mobile API
API	Application Program Interface

1.2 APPLICABILITY TO EXISTING VZW DEVICE REQUIREMENTS AND COMPLIANCE TEST PLANS

Unless specifically identified in this document, the device shall comply with Verizon Wireless Device Feature Definition/Requirements and Verizon Wireless Device Testing Process.

1.3 NEW VZW DEVICE COMPLIANCE TEST PLANS REQUIRED TO SUPPORT THESE DEVICE REQUIREMENTS

Any device that is NFC-enabled shall additionally comply with the VZW NFC Compliance Test Plan.

1.4 ENTRANCE CRITERIA

The vendor shall obtain the following certifications:

EMVCo Certification for Embedded SE (If applicable)

Isis Level 1 Certification
Isis Level 2 Certification

See the “Verizon Wireless Device Compliance Test Entrance Criteria” and reference [38] for additional information on the certification process.

If the OEM will introduce a wireless charger back-cover with the device at launch, it shall obtain ISIS Level 1 Certification with the wireless back-cover as entrance criteria.

Any accessory sold by the OEM which may impact the functionality of NFC (i.e front cover sleeves,etc) shall be first approved by VZW.

1.5 DEVICE APPLICABILITY

These requirements are applicable to all devices which include an NFC Contactless Front end and a NFC Antenna.

2 USER INTERFACE

2.1 NFC CONTACTLESS FRONTEND (CLF)

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

2.1.1 NFC CONTACTLESS FRONT-END (CLF) ON/OFF SETTING

The device shall have controls available to the user to turn NFC ON or OFF. The default setting shall be set to "OFF".

NFC Contactless Front-End (CLF) OFF Prompt
If the NFC CLF is turned OFF, applications needing to use the CLF shall prompt the user to turn the NFC CLF ON and link users directly to that setting so that users don’t need to find it themselves.

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.NFC Contactless Front-End (CLF) ON Indicator
If possible, when the NFC CLF is ON, the device should provide a visual indicator (e.g., Android Status Bar icon) that it is enabled and ready to process information.

2.2 NFC PLATFORM SECURITY REQUIREMENTS

While device is in a voice call, the device shall disable any audible NFC indications that can be coupled to the voice uplink.

2.2.1 NFC LOCKED AND SCREEN TURNED OFF PROMPTS

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens when device is off or locked.

2.2.2 NFC PROMPTS BY DEFAULT SCENARIOS

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

2.2.3 PEER-TO-PEER PROMPTS

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens for peer-to-peer device exchanges. When a user presents an NFC Peer-to-Peer device.

2.2.4 INPUT VALIDATION

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens related to the proper behavior when a malformed, or improperly formatted tag is presented to the device.

2.2.5 NFC ACTIONS THAT WILL ALWAYS PROMPT

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens related dialing or texting.

3 HARDWARE REQUIREMENTS

3.1 MECHANICAL/ELECTRICAL

3.1.1.1 NFC CLF

The NFC shall conform to ISO/IEC 14443A & B, ISO/IEC 18092, and ISO/IEC 7816-4.

3.1.1.1.1 Card Emulation Power Modes

The device shall wait and not interfere (i.e turn off the CLF during initialization) with NFC CLF and UICC card emulation initialization.

NFC CLF shall support high power mode and low power mode mode for card emulation.

NFC CLF shall not support “No Power Mode”.

In low power mode when the device is switched off due to low battery, the device shall provide sufficient power to perform 50 card emulation transactions for at least 24 hour period.

3.1.1.1.2 Modes Of Operation

NFC shall support all NFC modes of operation; Card Emulation, Tag, Reader/Writer, and Peer-To-Peer

.Peer-To-Peer mode shall support ISO 18092, NFC-IP1, and NFC Forum LLCP protocol.

3.1.1.1.3 Contactless Front End (CLF) Disabled Mode

There shall be a mode where the CLF can be disabled. In the disabled mode, the CLF shall not respond to or communicate with the application processor, the secure element, or any (future) elements that have connection to the CLF.

3.1.1.2 SECURE ELEMENT

3.1.1.2.1 Single Physical SE

The NFC-enabled handset shall support only a single physical secure element (i.e., no additional SEs are allowed). If the device supports a UICC based secure element, then the device shall not also include an embedded secure element.

3.1.1.2.2 SE Interface

The interface to the UICC-based SE shall conform to ETSI 102 221 UICC terminal Interface, ETSI 102 613 Release 9 Single Wire Protocol (SWP), and ETSI 102.622 Release 7 Host Controller Interface (HCI) Protocol.
The device shall support Contactless Tunneling (CLT) mode for SWP as defined in ETSI TS 102.613.

3.1.1.2.3 Logical Channel Support

The device shall support all regular logical channels and all extended logical channels (3-19).

Secure element shall support multiple logical channels on external interfaces, including at least one channel on the contactless interface. Secure element shall have the capability to differentiate requests coming from the NFC antenna and requests from the mobile device. All SE shall have the ability to communicate with an external reader and with an application on the mobile device.

3.1.1.2.4 Embedded Secure Keys

The OEM shall provide the ISD keys for the embedded SE to Verizon. The device shall allow the ISD keys in the embedded SE to be changed by Verizon.

3.1.1.3 ANTENNA

There shall only be one active antenna on the device.

The device OEM shall indicate in a clear manner the location of the NFC antenna on the device. This will guide the user for the most optimal NFC place for transactions.

3.1.1.4 RF/MAGNETIC INTERFERENCE AND SUSCEPTIBILITY

During normal operations, the NFC circuit shall not cause interference with internal device circuit nor interfere with external devices. Similarly, the device shall not be negatively impacted by external devices with similar wireless coupling (i.e wireless charging) .

4 SOFTWARE SPECIFICATIONS

4.1 DEVICE BASED

4.1.1 SW APIs FOR ALL DEVICES

Except for MIDP2 Java Devices, OEMs shall provide SE APIs as defined in the SIMAlliance Open Mobile API (OMAPI) Specification version 2.03 or later.

The SE API shall only consist of the "Transport API" as defined in the OMAPI Specification version 2.03. The "Service Layer API" shall not be supported.

The device SE APIs shall establish a logical channel (i.e Session.OpenLogicalChannel) within an average of 150 milliseconds or less, and it shall not exceed 500 milliseconds. (Note: This includes Access Control enforcement).

The OMAPI shall define public APIs to allow consumer applications to define their UICC response timeouts per OMAPI Sessions. The default UICC response time out shall be set to 30 seconds.

4.1.1.1 SECURE ELEMENT ACCESS CONTROL

The device Secure Element APIs shall implement Access Control as specified by the Global Platform Access Control version 1.0, or greater. The Access Control module here forth shall be known as the "Enforcer".

The Enforcer shall support GET DATA Command in “Mode 1”, as specified in section "GET DATA Command".

When supporting "Mode 1" during handset bootup, the Enforcer shall not retrieve rules from the UICC unless all telecommunication processes have been completed or reached a state where the UICC SE is idle.

If the Enforcer fails to retrieve rules during boot up (i.e ARA-M not present, SE not present, etc), the Enforcer shall either fall back to Mode 2, Mode 3 or Mode 1. The refresh tag shall not be trusted.

Upon device reboot and/or SIM SE swap, all cached rules access control rules shall be purged.

The Enforcer shall at least support GET DATA Command in “Mode 2", as specified in section "GET DATA Command".

The Enforcer shall not generate or utilize any weak hashing algorithms (i.e MD5), currently all rules are defined as SHA-1 hashes in the ARA-M.

The Enforcer shall not interfere with any telecommunication activities (i.e dialing phone calls, sending SMS,etc).

The Enforcer shall validate the x509v3 certificate chain before calculating the Certificate Hash as defined in Section “Management of Certificate Chains“.

The Enforcer shall not make use of the Access Rule Files (ARF), it shall interface with the ARA-M.

The Enforcer shall deny access if the ARA-M is not found SE. It shall not fall back to Access Rule Files.

If no access rules are defined for a consumer application, access shall be denied (a rule must always exist for access).

The Enforcer shall ignore unknown TLVs within the ARA-M response.

To decrease the attack surface to the ARA-M (A00000015141434C00), the Enforcer shall hardcode the AID of the ARA-M, and shall not allow access to any consumer application.

The Enforcer shall support the NFC Event filtering as described in the Global Platform Access Control 1.0.

The Enforcer shall fully implement the GET-DATA-Next commands to retrieve all rules longer than 255 bytes. This shall apply to all retrieval modes and unknown TLVs.

4.1.1.1.1 Enforce on Session Class vs. Channel Class

The Enforcer shall retrieve all application relevant rules (i.e AR-DO-REFRESH, AR-DO) upon invocation of the OMAPI Session class. If Mode 2 is being utilized, the query results shall be cached for the duration of the Session Class Object. Security Exceptions shall be thrown at the OMAPI Channel Class as per the Global Platform Access Control version 1.0, or greater.

4.1.1.1.2 CLF Unknown TLV Pass through

The Enforcer shall forward all unknown TLV tags and values contained within APDU-AR-DO to the CLF stack/CLF chipset after retrieved from the ARA-M.

4.1.1.1.3 ARA-M Rule Change Events (For Future Study (FFS))

The Enforcer shall be able to receive rule change events originating from the ARA-M. Upon receiving such event, the ARA-M shall perform AR-DO-REFRESH query and update its rules cache (Mode 2 & 3) or retrieve all rules (Mode 1). All Enforcing security contexts must be refreshed upon receiving the update event.

4.1.2 SW APIS FOR MIDP2 JAVA DEVICES

The SW API to allow an application access to the NFC shall be compliant with JSR-177 and JSR-257 including optional parts NDEF, RF, and SC. The SW API to allow an application access to the SE shall be compliant with JSR-177 including optional parts APDU, JCRMI, PKI, and CRYPTO..

JSR-177 and JSR-257 shall be tested using the Java Device Test Suite (JDTS), which runs the Technology Compatibility Kit (TCK) for each JSR (or equivalent for non-Java Operating Systems).

4.1.3 SW APIS FOR DALVIK DEVICES (E.G., ANDROID)

The SW API to allow an application access to the NFC shall:

- Comply with Android 2.3 Compatibility Definition 2010, Release 2.3.3
- Implement NFC API for Android from:
http://developer.android.com/guide/topics/nfc/index.html
- Note: an earlier version of Android may be used as long as it complies with the above

SIMAlliance OpenMobile API for Dalvik Devices

The OEM shall ensure that the SE APIs packaged as “org.simalliance.openmobileapi” for application compatibility.
SEEK for Android version 2.2.2 or greater, is the preferred SE Access API implementation.

The SIMAlliance Open Mobile exception definitions do not fully adapt to Dalvik Devices Exceptions (i.e Android Exceptions). The OMAPI exceptions shall be defined as the following Android exceptions:

1. The **IllegalParameterError** exception shall be implemented as **IllegalArgumentException**.

2. The **IOError** exception shall be implemented as **IOException**.
3. The **OperationNotSupportedError** shall be implemented as **OperationNotSupportedError**.
4. The **SecurityError** shall be implemented as **SecurityException**.
5. The **NoSuchElementError** shall be implemented as java.util.**NoSuchElementException**.
6. The **IllegalStateError** shall be implemented as **IllegalStateException**.

4.1.3.1 NFC CLF Events

The device shall support the delivery of NFC CLF events to user space applications.

The device shall support transaction events originating from the SE, through the NFC CLF in accordance to ETSI – TS 102 705.

The ETSI – TS 102 705 events shall be mapped to a standard GSMA namespace while being delivered to consumer applications.

The ETSI – TS 102 705 events shall be delivered using the GSMA broadcast method. Unit cast event delivery shall not be implemented.

The GSMA APIs which allow the switch between unit-cast vs. broadcast shall not be implemented (this ensures that the events are delivered via broadcast).

4.1.3.2 Android NFCEE_ACCESS.XML file (DEPRECATED)

The device shall not interfere with the delivery of NFC CLF events. NFC CLF events shall only be controlled by the Global Platform Access Control.

4.1.4 SW NFC Security

4.1.4.1 NFC HANDLING Behavior

When the device is locked (with or without a password/PIN), it shall not allow automatic NFC functions.

.The device shall not broadcast NFC WAKEUP (in reader mode), nor respond to a NFC WAKEUP (in tag emulation mode) command when the device is screen is powered off.

The device shall not truncate or any tag information and shall display the full tag information to the user.

The device shall fully warn the user when turning off prompting with the security concerns of automatic NFC action.

There shall be UI controls to enable/disable prompting.

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

4.1.4.1.1 CLF Service Filtering

The device NFC stack and CLF shall provide filtering capabilities which will allow the following:

1. Filter ISO 7816 card emulation commands for AID Selection. Apply enforcing rules based on the current device power state (i.e low power, no power, full power) and other enforcing contexts.
2. Filtering rules shall be dynamically updated through the use of GPAC (refer to unknown TLV)

4.1.4.1.2 Handling Actions that Modify Personal or System Settings

ny action derived from a NFC device (i.e smart tag) that could alter any device system settings, launch urls or personal settings shall first prompt the user with a clear description of the action to be taken.

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

4.1.4.1.3 Handling Actions for Dialing or Mobile Messaging

Any NFC action which dials or send SMS shall **always** first prompt the user for confirmation. The device may use the dialing or sms native applications as the prompt.

If the device is in an active call session while the NFC action is received, the current call shall not be interrupted.

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

4.1.4.1.4 Handling Actions in Peer-to-Peer mode

NFC device comes within range, the user shall be prompted before any action is taken. This shall not be applicable for Card Emulation mode.

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

4.1.4.1.5 Handling Actions for Connection Handover

By default, the device shall prompt the user with full connection information (i.e Bluetooth Address, Wifi SSID,etc) before the NFC handover takes place.

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

The OEM shall use a single UI menu element to control prompting for NFC connection handover (i.e Bluetooh, Wifi,etc).

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

4.1.4.2 NFC DATA TRANSFER VALIDATION

- The device (reader) shall validate all data from tags and peer-to-peer communications according to the NFC Forum - NFC Data Exchange Format (NDEF) Technical Specification 1.0 or greater:
- The URL, URI, and vCard message parsers shall be capable of rejecting oversized or malformed messages.

Please refer to VZW NFC Flow and UI Package for relevant interaction states or screens.

4.1.5 MOBILE APPLICATION FRAMEWORK

4.1.5.1 IMEI/MDN

The mobile application frame work shall include an API that allows mobile applications to retrieve the mobile device's IMEI or MEID as well as the MDN.

4.1.6 NFC

When an application requires use of Card Emulation mode, the device shall inform the application in the event that card emulation is turned off. This can be done in a similar fashion as described in "NFC Contactless Front-End (CLF) ON/OFF Setting".

4.1.6.1 USER INTERACTION

The handset should present an indication in the form of a system icon of the current ability to perform NFC transactions.

4.1.6.2 NFC DETECTION

In card emulation mode, the NFC stack shall trigger events when the mobile device enters into an RF field, when the mobile device is removed from an RF field.

4.1.6.3 NFC API

The device NFC stack shall include APIs for third party applications to receive NFC RF Field events.

4.1.7 CONNECTION HANDOVER

The device shall support connection handover features as specified in the sections below. The connection handover shall be compliant to the NFC Forum Connection Handover specification version 1.2 or newer.

4.1.7.1 STATIC HANDOVER

The device shall support the Static Handover as specified in the NFC Forum Connection Handover Specification version 1.2 or newer.

4.1.7.1.1 Bluetooth Out of Band (OOB) For Static Handover

The device shall be able to read and interpret an NFC Forum compliant tag for connection handover, in particular a tag that contains a Handover Select Record.

The device shall be able to scan and decode fields as defined in the Bluetooth SIG core specification Secure Simple Pairing Out Of Band (OOB) in the Bluetooth Core Specification version 4.0 or newer, including the mandatory OOB Tag fields as well as the optional OOB Tag fields.

The fields shall be passed to the module responsible for Bluetooth OOB operation using NFC Connection Handover. Please refer to the Verizon Wireless Bluetooth Device Requirements for Bluetooth OOB requirements.

The static handover for Bluetooth shall follow the call flow in VZW NFC Flow and UI.

4.1.7.1.2 Wi-Fi Handover

4.1.7.1.2.1 Wi-Fi Sharing

The device shall be able to act as a NFC "static tag" (tag emulation) and provide Wi-Fi credentials to either share or proxy two NFC capable devices using data standards and protocols specified in the Wifi Simple configuration Technical Specification 2.0.2 or newer.

The device shall be able to provide its Mobile Hot Spot Wi-fi credentials through NFC either using a "tag emulation" or peer-to-peer mode by using data elements defined in the Simple Configuration Technical Specification 2.0.2 or newer.

The user shall be prompted before transferring Wi-fi credentials through NFC.

4.1.7.2 NEGOTIATED HANDOVER

The device shall be able to generate or receive and process a handover request message as specified in the NFC Forum Connection Handover Specification version 1.2 or newer.

The device shall be able to generate or receive and process a handover select message as specified in the NFC Forum Connection Handover Specification version 1.2 or newer.

4.1.7.2.1 Bluetooth OOB for Negotiated Handover

The device shall be able to generate or receive and process a handover request message with Bluetooth Carrier Type identification and Bluetooth specific mandatory and optional data records as defined by Bluetooth OOB as defined in Bluetooth SIG Bluetooth Core specification version 4.0 or newer. Both the mandatory fields and optional fields of the OOB fields shall be supported. If the intent is to use the Bluetooth as a possible connection, the Bluetooth shall be turned on and the message shall set Bluetooth power state as active or activating.

The device shall be able to generate or receive and process a handover select message with Bluetooth Carrier Type identification and Bluetooth specific mandatory and optional data records as defined by Bluetooth OOB as defined in Bluetooth SIG Bluetooth Core specification version 4.0 or newer. Both the mandatory fields and optional fields of the OOB fields shall be supported.

The Bluetooth NFC negotiated handover shall follow the call flow contained in VZW NFC Flow and UI Package.

4.2 DEVICE TO/FROM ACCESSORIES AND ASSOCIATED DEVICES

This NFC-enabled handset communicates with other NFC devices in accordance with ISO/IEC 14443 and ISO/IEC 18092.

NFC-enabled devices shall comply with the NFC Forum specifications related to the NFC Logical Link Control Protocol (LLCP), NFC Data Exchange Format (NDEF), and peer-to-peer operation.

The device shall support Simple NDEF Exchange Protocol (SNEP) as defined by NFC Forum.

The device shall support Reader/Writer mode for NFC forum defined tags type1, type 2, type 3 and type 4.

5 PERFORMANCE

5.1 MAJOR PERFORMANCE METRICS

5.1.1 NFC

The following performance benchmarks shall be met:

1. NFC MAXIMUM CARD EMULATION OPERATIONAL DISTANCE – The maximum card emulation operational distance required between two NFC-enabled devices before exchanging information is 4 cm.
2. CARD EMULATION MAXIMUM SESSION TIME – The maximum transaction time for the NFC-enabled handset to pass credit card information to a retailer POS reader in card emulation mode is 250ms. For UICC based SE, the SE shall at most consume 170ms of the 250ms.

5.2 VZW NFC COMPLIANCE TEST PLAN

Please reference VZW NFC Compliance Test Plan.

6 REFERENCES

<Industry Standards References>

1. 3GPP TS 26.140 V5.1.0 (2002-06) Release 5
2. ISO/IEC 14443 Identification Cards – Contactless Integration Circuit Cards – Proximity Cards
3. ISO/IEC 18443 Information Technology – telecommunication and information Exchange Between Systems – Near Field Communication
4. ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation, Version 3.1. July 2009.
5. ISO 7816-4
6. ISO 8583
7. ISO 18092

8. ETSI – TS 102 705 – Smart Cards; UICC Application Programming Interface for Java Card for Contactless Applications, Version 9, January, 2011
9. ETSI 102 221 – UICC Terminal Interface
10. ETSI TS 102 225, Secured packet structure for UICC applications, Version 8.3.0.
11. ETSI TS 102 613, UICC - Contactless Front End (CLF) Interface, Part 1: Physical and data link layer characteristics, Version 9.1.0. April 2010.
12. ETSI TS 102 622, UICC - Contactless Front End (CLF) Interface: Host Controller Interface (HCI), Version 7.6.0. April 2010.ECMA-373, Near Field Communication Wired Interface (NFC-WI), Release 1. June 2006.
13. ECMA 340 – Near Field Communication Interface and Protocol (NFCIP-1) – 2nd Edition – December 2004
14. ECMA 356 – NFCIP-1 RF Interface Test Methods – 1st Edition – June 2004
15. ECMA 362 – NFCIP-1 Protocol Test Methods – 2nd Edition – December 2005
16. NFC Forum (http://www.nfc-forum.org/home/)
17. Global Platform Card Specification v 2.2 March 2006. (http://www.globalplatform.org/specificationscard.asp)
18. GlobalPlatform Card Confidential Card Content Management Card Specification v2.2 - Amendment A, Version 1.0. October 2007.
19. GlobalPlatform Card Remote Application Management over HTTP Card Specification v2.2 - Amendment B, Version 1.1. June 2009.
20. GlobalPlatform Card Contactless Services Card Specification v2.2 - Amendment C, Version 1.0. February 2010.
21. GlobalPlatform Card Technology Secure Channel Protocol 03 Card Specification v2.2 - Amendment D, Version 1.1. September 2009.
22. GlobalPlatform Card UICC Configuration, Version 1.0. 28 October 2008.
23. JSR-257: Contactless Communications API – Maintenance Release – July 2009 (http://www.jcp.org/en/jsr/detail?id=257)
24. JSR-177: Security and Trust Services for Java ME – Maintenance Release – August 2007(http://www.jcp.org/en/jsr/detail?id=177)
25. JSR-118. Mobile Information Device Profile 2.0 – Final Release 2 – June 2006.
26. JSR-139: Connected Limited Device Configuration 1.1 – Maintenance Release – November 2007.
27. Java Card Specifications, Classic Edition (JC Runtime Environment, JC Virtual Machine, JC API), Version 3.0.1. June 2009.
28. Java Card Specifications (JC Runtime Environment, JC Virtual Machine, JC API), Version 2.2.1. 2003.
29. Java Card Specifications (JC Runtime Environment, JC Virtual Machine, JC API), Version 2.2.2. March 2006.
30. Joint Interpretation Library - Application of Attack Potential to Smartcards, Version 2.5. April 2008.
31. BSI-PP-002, Smart Card IC Platform Protection Profile, Version 1.0. June 2001.
32. DCSSI-PP/9911, Smartcard Integrated Circuit with Embedded Software, Version 2.0. July 1999.
33. Java Card Protection Profile Collection, Version 1.1. May 2006.
34. NFC Forum Type 1 Tag Operation Specification 1.1
35. NFC Forum Type 2 Tag Operation Specification 1.1
36. NFC Forum Type 3 Tag Operation Specification 1.1

37. NFC Forum Type 4 Tag Operation Specification 2.0
38. Wi-Fi Simple Configuration Technical Specification, Version 2.0.2, Wi-Fi Alliance January 2012

<Verizon Specific Documentation References>

39. “Verizon Wireless Device Testing Process”
40. Verizon Wireless Device Compliance Test Entrance Criteria.
41. Verizon Wireless NFC Compliance Test Plan
42. Verizon Wireless SIM-Device Global Platform Access Control Test Plan

<Other Applicable References>

43. Isis Certification Process Specification, Version 1.0, March 14, 2011