CDMA 全球手机要求——CDMA 终端 NFC

CDG 第 206 号文件

1.0 版

2012 年 5 月

地址：加利福尼亚州科斯塔梅萨市
Anton 大道 575 号 560 室
CDMA 发展集团 邮编：92626
电话：+1 888 800-CDMA
+1 714 545-5211
传真：+1 714 545-4601
网址：http://www.cdg.org
电子邮箱：cdg@cdg.org

目录

1 版本历史

日期	版本	说明
2011 年 5 月	1.0	初版

1. 简介

1.1 目的

本文件的目的是规定 CDMA 终端的 NFC（近场通讯）要求。 近场通讯是一种无线通讯技术，也称短距离无线电通讯技术，允许短距离传输少量数据。这种无线连接技术支持设备之间简单的双向交互，消费者只需轻轻一按即可进行非接触式交易、访问数字内容和连接电子设备。本文件将规定 CDMA 手机上不同的 NFC 工作模式要求，但对 NFC 工作过程中可能使用的各种应用程序不作要求。这些要求主要根据 ECMA（欧洲计算机制造商协会）、ISO/IEC（国际标准化组织/国际电工委员会）、NFC 论坛和全球平台制定的行业标准以及运营商为确保 NFC 正常运行而提出的具体要求制定。

1.2 范围

本文件的范围是概述要求具有 NFC 功能的 CDMA 设备满足的一系列要求和功能。要求所涉及的方面将包括工作范围，数据速率，包括卡模式、读卡器模式、点对点模式在内的工作模式，安全（嵌入/非嵌入）和互操作性，还将涉及关于安全元件的使用和管理的具体要求；最后详述了软硬件要求、安全要求和 NFC 设备设计指南。

1

2 *1.3 参考文件*

序号	文件名	作者	版本	日期
1.	ISO/IEC 14443 识别卡——非接触式集成电路卡——邻近卡			
2.	ISO/IEC 18443 信息技术——系统间的远程通信和信息交换——近场通讯			
3.	ISO/IEC 15408，信息技术安全性评估通用准则			
4.	ISO 8583			
5.	ISO 18092			
6.	ETSI 102 221——UICC 终端接口			
7.	ETSI TS 102 225，UICC 应用程序的安全包结构			
8.	ETSI TS 102 613, UICC——非接触式前端 (CLF) 接口，第 1 部分：物理和数据链路层的特征			
9.	ETSI TS 102,622, UICC——非接触式前端 (CLF) 接口：主机控制器接口 (HCI)			
10.	ECMA 340——近场通讯接口和协议 (NFCIP-1)			
11.	ECMA 356 – NFCIP-1 射频接口测试方法			
12.	NFC 论坛——TS——数字协议			
13.	NFC 论坛 1 类标签操作规范			
14.	NFC 论坛 2 类标签操作规范			
15.	NFC 论坛 3 类标签操作规范			
16.	NFC 论坛 4 类标签操作规范			
17.	全球平台卡片规范 2.2 版			
18.	全球平台卡片 卡上机密内容管理 卡片规范			
19.	全球平台卡片 通过 HTTP 进行远程应用程序管理			
20.	全球平台卡片 非接触式服务卡片规范			
21.	全球平台卡片技术 安全通道协议 03 卡片规范			

序号	文件名	作者	版本	日期
22.	全球平台卡片 UICC 配置			
23.	NFC 逻辑链路控制协议技术规范			

1.4 缩略语和缩写词

表 1：缩略语和缩写词

缩略语/缩写词	说明
AES	高级加密标准
API	应用程序编程接口
APDU	应用协议数据单元
ASK	幅移键控
BIP	承载无关协议
BIST	内建自测试
DASM	设备应用程序安全管理
DMA	数字管理存取
ECMA	欧洲计算机制造商协会
ECDH	椭圆曲线密钥交换体制
EMVco	Europay、Mastercard、Visa 公司
ETSI	欧洲电信标准协会
ISO	国际标准化组织
IEC	国际电工委员会
JCB	日本信用会社
MSL	运营商补贴锁定
NFC	近场通讯
NDEF	NFC 数据交换格式
NFCIP	近场通讯接口与协议

缩略语/缩写词	说明
NFC LLCP	NFC 逻辑链路控制协议
NFC SEC	NFC 安全
OMA	开放移动联盟
OTA	空中下载
PID	参数 ID
PKI	公钥基础设施
POS	销售点
RTD	记录类型定义
SMS	短信息服务
SNEP	简易 NDEF 交换协议
SSL	安全套接层
SWP	单线协议
TEE	可信执行环境
TLS	传输层安全协议
UICC	通用集成电路卡

1.5 术语和定义

要求可分为三类：

(M) 强制要求	手机**必须**支持这一特征，以完成批准程序。
(HD) 高度需求	强烈要求或建议手机支持这一特征。该特征可在文件的后续版本中转变为强制要求。对这一特征的支持在终端商业推广中具有重要价值。
(O) 可选	由制造商决定终端是否支持这一特征。手机**可**支持这一特征。

1.6 运营商验收

如果运营商要求，制造商**应**提供下列文件和证书用于对设备进行技术评估：

1.6.1 文件

要求编号 #	要求	终端	备注	参考	PRI 的可设置性
1.6.1.1	GHRC 合规报告，详述 GHRC 本文件各个相关部分的合规或不合规	M			不适用
1.6.1.2	EMVCo 或通用准则认证	HD	Visa、万事达卡 (Master Card)、美国运通(American Express) 和 JCB 要求。 支持与否由运营商决定		不适用
1.6.1.3	EMVCo 1 类批准	HD	Visa、万事达卡 (Master Card)、美国运通 (American Express) 和 JCB 要求。 支持与否由运营商决定		不适用
1.6.1.4	NFC 论坛第 1 波认证	M	第 1 波包括较低等级的数字协议测试，特别是标签操作、数字协议和行为规范		不适用
1.6.1.5	NFC 论坛第 2 波认证	HD	第 2 波增加了物理层和选定的较高等级的数字协议的测试，包括射频模拟和点对点		不适用
1.6.1.6	Isis 1 级认证	O	ISIS 是 Verizon Wireless、AT&T 和 T-Mobile 共同建立的合资企业 支持与否由运营商决定		

CDMA 手机的 NFC 要求

要求编号 #	要求	终端	备注	参考	PRI 的可设置性
1.6.1.7	Isis 2 级认证	O	ISIS 是 Verizon Wireless、AT&T 和 T-Mobile 共同建立的合资企业 支持与否由运营商决定		不适用
1.6.1.8	全球平台合规	HD	合规关注的是安全芯片上内嵌的应用程序的功能和安全性。 本要求对于移动支付应用程序是强制性要求。		不适用

1

2. 要求

本部分阐述的是对 NFC 设备的最低要求。

2.1 最低标准支持

下列要求适用于支持 CDMA 终端上的 NFC 功能的设备。

2.1.1 协议支持

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.1.1.1	遵守 ISO/IEC 14443 规范	M	提供关于非接触式卡间通信的 4 部分基本标准		不适用
2.1.1.2	支持 A 类和 B 类卡	M			不适用
2.1.1.3	遵守 ISO/IEC 18092/ECMA-340 近场通讯接口和协议——1 (NFCIP-1)	M			不适用
2.1.1.4	遵守 ISO/IEC 21481/ECMA-352 近场通讯接口和协议——2 (NFCIP-2)	M			不适用
2.1.1.5	遵守 ISO/IEC 7816	M			
2.1.1.6	支持 NFC 逻辑链路控制协议 (LLCP) 技术规范	M	定义 OSI 第 2 层协议，以支持两个具有 NFC 功能的设备之间的点对点通信。这对于任何涉及双向通信的 NFC 应用程序都必不可少。	http://www.nfc-forum.org	不适用
2.1.1.7	支持 NFC 数字协议技术规范	M	解决具有 NFC 功能的设备通信的数字协议问题，提供一个以 ISO/IEC 18092 和 ISO/IEC 14443 标准为基础的执行规范。	http://www.nfc-forum.org	不适用
2.1.1.8	支持 NFC 行为技术规范	M	本规范阐述了如何	http://www.nfc-	不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
			使用 NFC 数字协议规范设置另一个 NFC 设备或 NFC 论坛标签的通信协议。	forum.org	
2.1.1.9	支持 NFC 简易 NDEF 交换协议 (SNEP) 规范	M	以 NFC 论坛点对点模式工作时，简易 NDEF 交换协议 (SNEP) 允许具有 NFC 功能的设备上的应用程序与另一个 NFC 论坛设备交换 NFC 数据交换格式 (NDEF) 消息。	http://www.nfc-forum.org	不适用
2.1.1.10	支持 EMV 非接触式通信协议	HD	基于 EMVCo 的支付服务的必需符合该要求	http://www.emvco.com/specifications.aspx	不适用

2.1.2 NFC 数据交换格式

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.1.2.1	支持 NFC 数据交换格式 (NDEF) 技术规范	M	为符合 NFC 论坛标准的设备和标签规定一个通用的数据格式	http://www.nfc-forum.org	不适用

2.1.3 NFC 标签类型

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.1.3.1	支持 NFC 论坛 1 类标签操作规范	M	1 类标签基于 ISO/IEC 14443A 标准。标签可读且可再次写入；用户可以配置标签，使之变为只读。内存为 96 字节，可以扩展到 2 千字节。	http://www.nfc-forum.org	不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.1.3.2	支持 NFC 论坛 2 类标签操作规范	M	2 类标签基于 ISO/IEC 14443A 标准。标签可读且可再次写入；用户可以配置标签，使之变为只读。内存为 48 字节，可以扩展到 2 千字节。	http://www.nfc-forum.org	不适用
2.1.3.3	支持 NFC 论坛 3 类标签操作规范	O	3 类标签基于日本工业标准 (JIS) X 6319-4，也称 FeliCa。标签在制造时已预先配置为可读且可再次写入或只读。内存大小不一，理论内存限值为 1 兆字节/服务。	http://www.nfc-forum.org	不适用
2.1.3.4	支持 NFC 论坛 4 类标签操作规范	M	4 类标签完全遵守 ISO/IEC 14443 标准系列。标签在制造时已预先配置为可读且可再次写入或只读。内存大小不一，最高 32 千字节/服务；通信接口遵守 A 类或 B 类标准。	http://www.nfc-forum.org	不适用

2.1.4 NFC 记录类型定义

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.1.4.1	支持 NFC 记录类型定义 (RTD) 技术规范	M	规定格式与规则，以便基于 NDEF 数据格式，为 NFC 论坛应用程序定义和第三方建立标准记录格式	http://www.nfc-forum.org	不适用
2.1.4.2	支持 NFC 文本 RTD 技术规范	M	使用 RTD 机制和 NDEF 格式，提供一种有效的多语种文本字符串存储方法。	http://www.nfc-forum.org	不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.1.4.3	支持 NFC 智能海报 RTD 技术规范	M	定义一种 NFC 论坛已知类，用以将 URL、SMS 或电话号码加入 NFC 标签中，或实现其在设备间的传输。	http://www.nfc-forum.org	不适用
2.1.4.4	支持 NFC 通用控制 RTD 技术规范	M	提供一种简易的方式，通过 NFC 通信，从一个 NFC 论坛设备、标签或卡（源设备）请求对一个 NFC 论坛设备（目标设备）执行规范（例如启动应用程序或设置模式）。	http://www.nfc-forum.org	不适用
2.1.4.5	支持 NFC 签名 RTD 技术规范	M	规定对单个或多个 NDEF 记录签名使用的格式。定义必填和可选签名 RTD 字段；提供一个合适的签名算法列表和可用于创建签名的证书类型。	http://www.nfc-forum.org	不适用

2.1.5 NFC 连接切换

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.1.5.1	支持 NFC 论坛连接切换技术规范	M	定义交互的结构和序列，令两个具有 NFC 功能的设备可以采用其他无线通信技术建立连接。连接切换结合了简单的一触式 NFC 设置和 WiFi 或蓝牙等高速连接技术。	http://www.nfc-forum.org	不适用

2.2 硬件要求

下列要求适用于支持 CDMA 终端上的 NFC 功能的设备。

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.2.1	支持管理终端、UICC 和第三方 POS 实体间所有 NFC 操作的 NFC 主机控制器	M			不适用
2.2.2	支持 NFC 通信专用接近型射频天线	M			
2.2.3	支持内嵌在 UICC 上或 NFC 芯片或安全内存卡中的安全元件，元件与终端的非易失性内存分离	M	是否执行由运营商决定		
2.2.4	能支持多个安全元件	HD	有些市场可能要求终端有多个安全元件共存，例如：UICC、安全 SD 卡以及内嵌式终端		不适用
2.2.5	对于支持 UICC 的设备，遵守 ETSI 和 3GPP2 UICC 标准	M		http://www.etsi.org/WebSite/Technologies/Smartcards.aspx http://www.3gpp2.org/Public_html/specs/alltsgscfm.cfm	不适用
2.2.6	可通过独立于终端电源开关功能的硬键来启用/禁用 NFC 操作	M	如果用户想在终端关机时控制 NFC 操作，必须使用此功能		不适用
2.2.7	支持在允许使用 NFC 进行安全应用程序会话之前，使用设备上的生物识别设备进行用户验证	HD	运营商可规定哪些应用程序（例如：支付）要求生物验证		不适用

2.3 软件平台要求

下列要求适用于支持 CDMA 终端上的 NFC 功能的设备。

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.3.1	支持为 NFC 应用程序提供 API，以便安全访问 UICC 或终端上的安全元件	M	提供的安全 API 可以是 Native 终端或智能手机的开放式操作系统环境的一部分，或是通过 Sim Alliance 的开放移动 API 规范等解决方案执行		不适用
2.3.2	支持为 NFC 应用程序提供 API，以便访问并充分利用终端上的显示器、键盘/触控接口	M			不适用
2.3.3	支持为 NFC 应用程序提供 API，以便访问设备上的音频控制器	M	例如，在成功完成 NFC 交易需要音频确认时，可能需要此功能		不适用
2.3.4	支持为 NFC 应用程序提供 API，以便访问设备上的震动控制器	M	例如，在振动模式中，在成功完成 NFC 交易需要振动确认时，可能需要此功能		不适用
2.3.5	支持为 NFC 应用程序提供 API，以便访问设备上的电话功能（拨打电话）	M			不适用
2.3.6	支持为 NFC 应用程序提供 API，以便访问网络浏览器客户端	M			不适用
2.3.7	支持为 NFC 应用程序提供 API，以便访问 SMS 消息传送客户端	M			不适用
2.3.8	支持提供 API，以便查看终端的电池电量	M	可用电量将决定 NFC 的工作模式，例如：在电池电量不足时，只能在卡模式下工作		不适用

2.4 最低工作要求

下列要求适用于支持 CDMA 终端上的 NFC 功能的设备。

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.4.1	支持在频率为 13.56 MHz，带宽为 +-7Khz 的条件下工作	M	这些标准是 NFC 设备要求的基础标准；		不适用
2.4.2	可以在大约 4 cm（不超过 2 英寸）的距离内与另一个 NFC 设备或标签交换数据	M	这些标准是 NFC 设备要求的基础标准；		不适用
2.4.3	启用 NFC 功能时，能启动 NFC 并在屏幕上做出提示（徽标、标志）	M	这些标准是 NFC 设备要求的基础标准；		不适用
2.4.4	能禁用 NFC 并令其（徽标、标志）从屏幕上消失	M	这些标准是 NFC 设备要求的基础标准；		
2.4.5	支持 106kbps、212kbps 和 424 kbps 通讯数据速率	M	这些标准是 NFC 设备要求的基础标准；		不适用
2.4.6	支持下列调制： 幅移键控 (ASK)（轮询模式）和 负载调制（听取模式）	M	这些标准是 NFC 设备要求的基础标准；		不适用
2.4.7	支持曼彻斯特编码	M	这些标准是 NFC 设备要求的基础标准；		不适用
2.4.8	工作容积内支持 1.5A/m 到 7.5A/m 之间的磁场强度	M	这些标准是 NFC 设备要求的基础标准；		不适用
2.4.9	支持大约为 HThreshold=0.187A/m 的射频场阈值	M	这些标准是 NFC 设备要求的基础标准；		不适用

2.5 工作模式

所有工作模式皆需满足下列要求。

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.5.1	支持卡模式	M			不适用
2.5.2	支持读卡器模式	M			不适用
2.5.3	支持点对点模式（ISO-	HD			不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
	18092、NFC-IP1 和 LLCP）				
2.5.4	支持 1 类标签读取	M			不适用
2.5.5	支持 2 类标签读取	M			不适用
2.5.6	支持 3 类标签读取	O	3 类是针对 Felica 的，只有需在某些国家运行的设备需要		不适用
2.5.7	支持 4 类标签读取	M			不适用
2.5.8	支持 1 类标签写入	M			不适用
2.5.9	支持 2 类标签写入	M			不适用
2.5.10	支持 3 类标签写入	O	3 类是针对 Felica 的，只有需在某些国家运行的设备需要		不适用
2.5.11	支持 4 类标签写入	M			不适用
2.5.12	支持轮询所有技术，如 NFC-A、NFC-B 和 NFC-F	M	NFC-F 是针对 Felica 的，并非强制要求		不适用
2.5.13	支持在轮询、听取模式下工作	M			不适用
2.5.14	在卡模式下工作时，支持主动和被动模式（高、低、无电池电量）	M			不适用
2.5.15	读取 1 类标签时支持 106kbps 的工作比特率	M			不适用
2.5.16	读取 2 类标签时，支持 106kbps 的工作比特率	M			不适用
2.5.17	读取 3 类标签时，比特率为 212kbps，支持 253 字节的有效载荷	O	3 类是针对 Felica 的，只有需在某些国家运行的设备需要		不适用
2.5.18	读取 4 类标签时，比特率为 106kbps 和 424kbps，支持 254 字节的有效载荷	M			不适用
2.5.19	根据 NFC-A 执行卡模拟时，符合 4A 类标签平台要求	M			不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.5.20	根据 NFC-B 执行卡模拟时，符合 4B 类标签平台要求	M			不适用
2.5.21	根据 NFC-B 执行卡模拟时，符合 3 类标签平台要求	O	3 类是针对 Felica 的，只有需在某些国家运行的设备需要		不适用
2.5.22	在点对点模式下工作时，支持 106kbps、212kbps 和 424kbps 通信	HD			不适用
2.5.23	在卡模式下时，支持完成一个交易的时间不超过 250 毫秒	M			不适用
2.5.24	在点对点模式下工作时，支持射频碰撞避免（先听后说）	M			不适用
2.5.25	在点对点模式下工作时，支持高达 254 字节的有效载荷	HD			不适用
2.5.26	在点对点模式下工作时，支持协商式切换（蓝牙/WiFi）	HD			不适用
2.5.27	在点对点模式下工作时，支持静态切换（蓝牙/WiFi）	HD			不适用

2.6 应用程序支持

具有 NFC 功能的终端**应**支持下列最低应用程序要求：

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.6.1	支持能读取带网站地址的智能海报的应用程序（启动浏览器）	M			不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.6.2	支持能读取带拨号操作的智能海报的应用程序	M			不适用
2.6.3	支持能读取带纯文本消息的智能海报的应用程序	M			不适用
2.6.4	支持能读取带启动 SMS 功能的智能海报的应用程序	M			不适用
2.6.5	支持能写入 1 类标签的应用程序	M			不适用
2.6.6	支持能写入 2 类标签的应用程序	M			不适用
2.6.7	支持能写入 3 类标签的应用程序	O	3 类是针对 Felica 的，只有需在某些国家运行的设备需要		不适用
2.6.8	支持能写入 4 类标签的应用程序	M			不适用
2.6.9	在卡模式下，支持应用程序当做借记卡使用	M			不适用
2.6.10	在卡模式下，支持应用程序当做信用卡使用	M			不适用
2.6.11	在卡模式下，支持应用程序当做忠诚卡使用	M			不适用
2.6.12	在卡模式下，支持应用程序当做礼品卡使用	M			不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.6.13	在卡模式下，支持存取控制应用程序	HD			不适用
2.6.14	在卡模式下，支持票务应用程序（活动、音乐会、交通）	M			不适用
2.6.15	在点对点模式下，支持应用程序进行高达 1kb 的数据传输 (vCard)	HD			不适用
2.6.16	在点对点模式下，支持应用程序进行高达 1kb 的数据传输（接触)	HD			不适用
2.6.17	在点对点模式下，支持应用程序使用蓝牙配对	HD			不适用
2.6.18	在点对点模式下，支持应用程序使用 Wi-Fi 配对	HD			不适用
2.6.19	在点对点模式下，支持应用程序使用蓝牙进行超过 1kb 的数据传输（图片、音乐）	HD			不适用
2.6.20	在点对点模式下，支持应用程序使用 Wi-Fi 进行超过 1kb 的数据传输（图片、音乐）	HD			不适用
2.6.21	支持自动选择 NFC 工作模式的应用程序	M			不适用
2.6.22	支持只在可信域（例如运营商）安装已签名的 NFC 应用程序	M			不适用

2.7 基于 UICC 的安全元件

若安全元件位于 UICC 之内，则具有 NFC 功能的终端**应**支持下列安全元件要求。

要求编号 #	要求	类别	备注	参考	PRI 的可设置性

CDMA 手机的 NFC 要求

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.7.1	对于内嵌于 UICC 中的安全元件，终端**应**支持单线协议 (SWP)	M		ETSI TS 102.613 ETSI TS 102.622	不适用
2.7.2	支持 ETSI TS 102.221 规定的终端 UICC 接口	M		ETSI TS 102.221	不适用
2.7.3	支持 SWP 主机控制器接口	M		ETSI TS 102.613 ETSI TS 102.622	不适用
2.7.4	支持 SWP 物理和数据链路层接口	M		ETSI TS 102.613	不适用
2.7.5	支持 SWP 逻辑接口	M		ETSI TS 102.622	不适用
2.7.6	支持 SWP 运行所需的 UICC 卡工具组件	M		ETSI TS 102.221 ETSI TS 102.223 ETSI TS 31.111	不适用
2.7.7	支持 UICC 和终端之间的承载独立协议 (BIP)	M		ETSI TS 102.223	不适用
2.7.8	支持与支持智能卡网络服务器的 UICC 连接的 OMA 智能卡网络服务	HD		http://www.openmobilealliance.org/technical/release_program/scws_v1_0.aspx	不适用
2.7.9	支持 APDU 数据结构作为安全元件和 NFC 应用程序之间的通信基础	M			
2.7.10	若终端支持 JavaME 环境，支持 JSR 257 无接触式 API	HD			不适用
2.7.11	支持 JSR 177：支持 JavaCard 和智能卡网络服务的安全元件上的安全应用程序和可信服务 API	HD	若支持 SCWS 且使用基于 Java 的 Midlet，如电子钱包等，则为强制要求		不适用

1

2

2.8 安全元件管理

支持 NFC 功能的终端**应**支持下列关于安全元件管理的要求

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.8.1	若终端上有多个安全元件，则**应**有可令用户选择 NFC 交易使用哪个安全元件的机制	M	仅当存在多个安全元件时为强制要求		不适用
2.8.2	若终端上有多个安全元件，则**应**有可令用户检索任意给定时刻活动的安全元件的机制	M	仅当存在多个安全元件时为强制要求		不适用
2.8.3	任意给定时间的一次交易只能有一个活动的安全元件	M			不适用
2.8.4	终端**应**支持管理设备上各种安全元件运行的安全元件管理代理	HD	安全元件管理要求可参见全球平台安全元件远程应用程序管理规范	http://globalplatform.org/specificationscard.asp	不适用
2.8.5	可针对新的应用，空中 (OTA) 更新和提供安全元件	M			不适用

2.9 互操作支持

具有 NFC 功能的终端**应**支持下列互操作性要求：

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.9.1	支持 NFC 功能的终端**不得**影响终端的 CDMA 功能	M			不适用

CDMA 手机的 NFC 要求

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.9.2	支持 NFC 功能的终端**不得**影响非紧急呼叫发起端的 CDMA 功能	M			不适用
2.9.3	支持 NFC 功能的终端**不得**影响紧急呼叫发起端的 CDMA 功能	M			不适用
2.9.4	支持 NFC 功能的终端**不得**影响任何 CDMA 辅助服务，例如呼叫等待、呼叫转移、呼叫拦截等	M			不适用
2.9.5	支持 NFC 功能的终端**不得**影响发送或接收 SMS 的 CDMA 功能	M			不适用
2.9.6	支持 NFC 功能的终端**不得**影响发送或接收 MMS 的 CDMA 功能	M			不适用
2.9.7	支持 NFC 功能的终端**不得**影响发起非绑定数据呼叫的 CDMA 功能	M			不适用
2.9.8	支持 NFC 功能的终端**不得**影响发起绑定数据呼叫的 CDMA 功能	M			不适用
2.9.9	支持 NFC 功能的终端**不得**影响终端的蓝牙功能	M			不适用
2.9.10	支持 NFC 功能的终端**不得**影响终端的 Wi-Fi 功能	M			不适用
2.9.11	支持 NFC 功能的终端**不得**影响终端的 GPS 功能	M			不适用
2.9.12	支持 NFC 的终端**应**遵守飞行模式要求，在飞行模式时禁用 NFC 功能	M			不适用
2.9.13	支持在语音或数据呼叫过程中处理 NFC 交易	M			不适用
2.9.14	支持 NFC 功能的终端**不得**在电池电量低时自动禁用 NFC 功能	M			不适用
2.9.15	即使终端关机，也支持在卡模式下运行终端	M			不适用

2.10 安全要求

NFC 设备**应**支持下列安全要求。若 OEM 执行了其它安全要求和下述要求或取代下述要求，运营商**应**共享这些要求。

2.10.1 一般要求

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.10.1.1	支持 NFC-SEC 的 NFCIP-1 安全服务和协议 (ECMA 385)	HD	此标准规定了 NFCIP-1 的 NFC-SEC 安全信道和共享秘密服务以及这些服务的 PDU 和协议	http://www.ecma-international.org/publications/standards/Ecma-385.htm	不适用
2.10.1.2	支持使用 ECDH 和 AES (ECMA 386) 的 NFC-SEC-01 NFC SEC 加密标准	HD	此标准规定了 PID 01 的消息内容和加密方法	http://www.ecma-international.org/publications/standards/Ecma-386.htm	不适用
2.10.1.3	支持仅在征得用户的同意后才执行基于 NFC 的交易	M	可以通过用户界面询问用户是否继续执行交易来实现 在卡模式下，**应**通过 POS 终端获得用户的同意	http://www.ecma-international.org/publications/standards/Ecma-386.htm	不适用
2.10.1.4	通过 NFC 执行安全交易时，支持使用双重身份验证	M			不适用
2.10.1.5	支持使用如下述规范定义的 NFC 功能的基于 PKI 的安全应用程序会话加密： 全球平台设备应用程序安全管理 (DASM) 密钥和证书管理规范	M	若 OME 执行了基于 PKI 的替代解决方案，则运营商应共享这些方案。	http://globalplatform.org/specificationscard.asp	不适用
2.10.1.6	支持如下述规范定义的安全应用程序配置： 全球平台设备应用程序安全管理 (DASM) 配置规范	M	若 OME 执行了其他应用程序安全管理和配置，则运营商应共享这些方案。	http://globalplatform.org/specificationscard.asp	不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.10.1.7	支持独立于终端上标准应用程序运行时间环境的可信执行环境 (TEE)，如由下述规范定义的： 全球平台可信执行环境 (TEE) 系统架构 全球平台可信执行环境 (TEE) 内部 API 规范 全球平台可信执行环境 (TEE) 客户端 API 规范	M	尤其适用于用手机支付的交易 若 OME 执行了其他可信安全环境，则运营商应共享这些环境。	http://globalplatform.org/specificationscard.asp	
2.10.1.8	支持 SSL 3.3/TLS 1.2 进行利用终端上的安全元件和 NFC 应用程序之间的 NFC 功能的安全应用程序会话	M		RFC 5246	不适用
2.10.1.9	任何 NFC 专有配置的访问权皆**应**由 MSL 代码保护	M			不适用

2.10.2 应用程序的安全性和安全元件的访问控制

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.10.2.1	支持 NFC 应用程序安全元件访问控制政策	M	此政策由运营商制定，赋予某些 NFC 应用程序访问安全元件的某些功能的权力		不适用
2.10.2.2	访问控制政策**应**列出所有批准的 NFC 应用程序及其对安全元件的相关访问权	M			不适用
2.10.2.3	将访问控制政策存储在安全元件上任何第三方应用程序均无法访问的安全位置	M			不适用
2.10.2.4	访问控制政策对于安全元件**应**是唯一的。若存在多个安全元件，每个元件皆**应**有自己的访问控制政策	M			不适用
2.10.2.5	一个安全元件的数据**不得**与终端上其他安全元件有关联的应用程序共享	M			不适用

要求编号 #	要求	类别	备注	参考	PRI 的可设置性
2.10.2.6	如果访问控制政策中未注明相关 NFC 应用程序项目，则**应**禁止该 NFC 应用程序访问该安全元件	M			不适用
2.10.2.7	支持在赋予访问安全元件上某个小应用程序的权限之前，检查 NFC 应用程序的签名和应用程序 ID (AID)	M			不适用
2.10.2.8	若访问被拒绝，则**应**向用户显示对应的错误提示	M			不适用
2.10.2.9	支持使用证书链进行 NFC 应用程序签名	M	对于要接受的应用程序，必须拥有有效完整的证书链		不适用
2.10.2.10	证书**应**基于 X.509 方案	M			不适用

3. 附录 A：NFC 的安全措施

本附录收集了基于 NFC 的终端制造商在设计、制造其产品时应考虑的安全措施或指南。虽然它们并非执行 NFC 技术的明确要求，但在此以提供信息为目的将其列出，可以确保基于 NFC 的服务综合考虑安全问题。

3.1.1 软件威胁安全防护措施

#	安全措施	备注	参考
3.1.1.1	只允许从服务提供商授权的可信来源下载应用程序		
3.1.1.2	核准的 NFC 应用程序应进行某种形式的行业认可的认证，并在终端上正确签名和部署		
3.1.1.3	在终端内存或 UICC 中运行的 NFC 应用程序应有一个额外的安全层，将其与终端上的其他应用程序环境分隔开	通过按照全球平台的要求支持可信执行环境 (TEE) 来实现	
3.1.1.4	终端应在启动中或执行 NFC 交易之前执行检查，以确保系统的完整性（即文件加载器代码段无代码和静态变化）		
3.1.1.5	防止存储从设备安全检查中获取的日志。可以通过在安全检查过程中执行日志文件系统等方式来实现		
3.1.1.6	任何内建自测 (BIST) 功能只能经由 MSL/SPC 代码方式被用户访问		
3.1.1.7	任何可进行安全元件访问的 API 都必须是类型安全 API，从而防止错误的数据被发送到终端		
3.1.1.8	类型安全 API 和非类型安全 API 在相同的域边界中不得混用		

3.1.2 硬件威胁安全防护措施

#	安全措施	备注	参考
3.1.2.1	用硬件扩展（地址空间限制、微编程 DMA、MMU 平台扩展等）限制数字管理存取 (DMA) 系统可以访问的内存，使 DMA 无法用于将非授权数据从设备的安全框架内移出		
3.1.2.2	通过在 NFC 启用时锁定端口，确保调试端口不可用于访问关键安全资产		
3.1.2.3	使用安全代码或硬件允许或禁止 JTAG 访问设备	JTAG 可允许访问终端上的端口进行调试，因此可能被恶意利用	
3.1.2.4	使用运营商补贴锁定 (MSL) 代码等安全代码或硬件来允许或禁止串行端口访问安全代码空间		
3.1.2.5	在 PCB 的物理设计阶段，将跟踪通道子接口布置到 PCB，从而防止恶意实体访问物理探测	例如在带安全元件的设备被窃、被物理入侵时可能需要	
3.1.2.6	在 PCB 上加保护层，以抵御或显示连接此类探针的企图	例如在带安全元件的被盗设备被恢复时可能需要	

1