王晓华　编著

NFC技术基础篇

· NFC移动支付从业人员的案头书

· 恩智浦、小米、易宝支付、京东商城
移动支付领域专家推荐

北京航空航天大学出版社
BEIHANG UNIVERSITY PRESS

NFC 技术基础篇

王晓华　编著

北京航空航天大学出版社

内 容 简 介

本书主要介绍 NFC 的基本协议，内容包括主机端与 NFC 控制器之间的通信协议、NFC 控制器与 eSE & SWP SIM 之间的协议、外部 POS 或者 READER 与 NFC 之间的射频协议。

本书适合 NFC 移动支付开发人员阅读。

图书在版编目(CIP)数据

NFC 技术基础篇 / 王晓华编著. -- 北京 : 北京航空航天大学出版社，2017.6

ISBN 978-7-5124-2444-9

Ⅰ. ①N… Ⅱ. ①王… Ⅲ. ①超短波传播—无线电技术—基本知识 Ⅳ. ①TN014

中国版本图书馆 CIP 数据核字(2017)第 133390 号

NFC 技术基础篇

王晓华 编著

责任编辑 胡晓柏 张 楠

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(邮编 100191) http://www.buaapress.com.cn

发行部电话：(010)82317024 传真：(010)82328026

读者信箱：emsbook@buaacm.com.cn 邮购电话：(010)82316936

涿州市新华印刷有限公司印装 各地书店经销

*

开本：710×1 000 1/16 印张：9.75 字数：174 千字

2017 年 6 月第 1 版 2017 年 6 月第 1 次印刷 印数：3 000 册

ISBN 978-7-5124-2444-9 定价：39.00 元

前　言

一个偶然的机会通过 Lucy 同学认识了胡老师，恰恰自己在这个时间点也想比较系统地总结一下 NFC 的相关技术，并尽可能多地分享一些自己的经验。在胡老师以及家人朋友的鼓励支持下，我也决定试一试。

之前自己并没有过写书的经历，对一些创作过程以及格式排版也比较陌生，比如这个前言我就不是很清楚是怎样的创作过程，是说写好前言之后一直往下写呢还是说等把书都写完了，然后在后来的某一天再把自己出书的心声写上去。为此特意咨询过胡老师，他给我的指导性的回复是不用让别的东西束缚，按自己的想法来写就可以了。这样对一些篇幅格式等之类的问题我也就知道该怎么做了。我比较喜欢把东西想好再往下写，所以大家翻开书后看到的这个排版顺序几乎也就是我的写作顺序。

近年来由于智能机的快速普及给人们带来一个思考，那就是出门是否还有必要带上一个钱包，里面装上现金和琳琅满目的卡片？而且现在支付宝、微信支付已经成了人们生活中必不可少的支付方式。写这本书之前，心里也会经常问自己一个问题，就是市面上真的还缺少一种需要特别硬件来支持的支付方式吗？

对于这两个问题，前者显然这是一个趋势性的东西，而且目前在实体店里能看到越来越多的人在使用手机进行消费和支付，大家也在享受这个技术带来的便捷性。

后面这个问题比较多的还是在实际体验上面，以支付宝为主的移动支付基于 QR 条码技术，对于用户来讲只需要一个客户端就可以解决问题，实体店只需要安装一套扫码枪接入服务即可以马上完成一个闭环支付体系，对于支付双方的学习成本是很低的。而对于 NFC 支付，就需要用户去购买特别带了 NFC 的支付设备，需要安装和激活卡片到手机上，带 NFC 支付的手机在市面上存量是一个问题，而且当手机导向市场后其实是没有一个真正意义上的运营主体的。这其实是一个巨大的问题，也就是说，没人会对用户体验进行直接负责。手机厂家对于 SWP-SIM 方案确实在商业利益考量上面来讲是没有动力的，运营商在实施 SWP-SIM 方案时大量的工作又是需要手机厂家和卡商去配合完成的。所以这一套方案玩下来，以 Android 手机为例，里面光要考量的各种软件版本就有 Android 版本、客户端钱包版本、NFC 协议栈版本、NFC 控制器固件版本、COS 版本、Applet 版本，里面还没有包括使用的硬件模块的版本等，只技术这一个环节就有大量繁琐的工作。NFC 基于的是一个射频通信技术，一旦铺向市场后就涉及需要和各种设备进行适配兼容性的工作，这个工作量也是巨大和难以想象的。

上面这些已知的难度是不是说 NFC 没有了机会，还有人会说 NFC 是十几年设计的技术框架、已经跟不上现在的节奏。显然这些质疑是站不住脚的。比如同样的

无线连接技术 Wi-Fi 和蓝牙，仔细去查看它们的发明时间和普及时间点出现，它们都是经历过一段漫长的静默期，再到后面的某一时间节点某一个事件，此项技术才成为了标准配置。现在 Wi-Fi 技术就是一个随处可见、人人在用的东西，蓝牙也在连接耳机和汽车电子等领域发挥很大的作用，而且 Wi-Fi 和蓝牙的版本还在不停地迭代和演进，我们又有什么理由不去相信 NFC 不会成为标准配置的那一天。基础性技术确实在发展过程中会显现出上面提到的各种问题，但是所有这种类似的技术都是有一个自身发展的规律，不可能一蹴而就，也不可能像某些应用技术一样通过一个后台优化在短暂的一段时间内就做到质的飞跃。我时刻提醒自己保持一个积极乐观的心态去面对这些问题，也时刻提醒自己保持一个虔诚和敬畏的心态去面对技术。

既然我认可它是一门基础技术，也就是说这种东西是不会过时的，假如这个技术在若干年后不复存在，我也十分有理由相信本书里面的一些技术将会在别的一个什么技术或产品上灵魂附体开出美丽的花朵。

NFC 技术支持三种工作模式：读/写器模式、点对点模式和卡模拟模式，其实这三种功能属性都基于很相似的底层射频技术。如果能把这些底层比较相似的标准和规范进行收缩归置，再把上层数字协议的一些东西进行抽丝剥茧展现给大家，这也就给我写这本书带来了可能性，否则 NFC 的各种标准和规范之多、之复杂，我是万万不敢下笔的。

此书编写的另外一个目的就是因为在市面找不到一本比较全面介绍 NFC 技术的书。我的观点是应用级的东西写成的书其实时效性是不强的，而且应用技术本身发展得快去得也快。现在这种技术是一个流行的前沿尖端的技术，过个二三年可能整个架构都变了，而且这种技术在网络上的资源也十分丰富，但是协议性的东西在一个较长的时间段里不会发生一个质的变化，经常变化的就是扩充了协议子集，但新出来的版本还是会向下向前兼容的，所以有一本归置完整便捷、能供工程师案头查阅协议的工具类书就变得很有意义。

王晓华 2017/4/15　晴

于北京市海淀区牡丹园

目　　录

1 简 介

近场通信(Near Field Communication,NFC)是一种近距离基于 13.56 MHz 频率通信的无线电技术。NFC 是一种非接触式技术,主要应用的领域有标签信息交互、门禁系统、卫生保健、优惠券、公交地铁、支付和消费电子产品等等。

资料显示一些前瞻性的 NFC 技术研究于 2002 年就已经开始了,但是正式的 NFC 概念于 2004 年 3 月 18 日由飞利浦半导体(现为恩智浦半导体公司)、诺基亚和索尼三家公司共同宣布研制开发,并同时成立了非营利性行业协会 NFC 论坛。NFC 技术规范定义的 NFC 本身的底层技术并没有说从零开始去设计和规划,而是基于现已有的 13.56 MHz 非接触式射频识别(RFID)技术演进变种而来,并且也做到了真正意义上的技术向下向前兼容,通用和适配性上面也做到了兼容市面上尽可能多的一些技术和已有产品,例如支持读取市面上已有的一些逻辑加密卡片,如 Mifare Ultralight、Topaz、Mifare Desfire、Felica 等,也支持读取基于标准 GP 规范的 JAVA 卡(CPU 卡片)。

从 2004 年论坛成立到现在,NFC 技术已经走过了十几个年头。这期间行业经历了各种起伏,有来自 IP 技术竞争方面的,也有来自商业竞争方面的,在此我们有必要回顾一下 NFC 的前世今生。下面罗列几个 NFC 的标志性大事件和时间节点。

2004 年　NFC 论坛正式成立;

2006 年　诺基亚公司发布第一款支持 NFC 的功能手机 (Nokia 6131i);

2010 年　Google 公司发布第一款支持 NFC 的智能手机 (Nexus S);

2010 年　默认在 Android 代码基线中集成 NFC 协议栈;

2011 年　Google 公司发布和运营基于 NFC 内嵌安全单元的谷歌钱包;

2013 年　Android 在 kitkat4.4 版本中使能基于主机端软件 (HCE) 的应用;

2014 年　Apple 公司发布的 iPhone6 等全线产品支持 NFC 技术;

2016 年　Apple 公司在中国发布了基于 NFC 技术的苹果支付 (Apple Pay)。

看上面的信息鲜有国内公司的影子,单纯从趋势影响力来看确实国内公司的身份主要还是一个跟随者。如果只是以这一点来评价国内的公司这肯定是不公平的。

在整个 NFC 移动支付行业的低迷期，移动运营商确实是在投入和付出的，特别是中国移动、联通和电信三家公司对 SWP-SIM 方案的 NFC 手机的持续供血。最终方案在实际市场的运营反响和体验度是另外一个故事，但是现在回顾来看来对整个行业起到了重要的作用，至少不至于产生断代式的后果；还有一个就是中国银行业确实是对 NFC 移动支付做了大量细致的工作。尽管大家在说 NFC 移动支付，但当前市面上其实并没一个能快速实施和落地的完整标准和解决方案，要做到能真正地用起来，这还需要有大量的调试和开发工作。在中国特别是以银联、招商银行等为主的公司其实是做了大量详实具体的贡献。

上面仅是把影响行业趋势的大事件大节点列出来了，参考上面的时间节点并对应市场上 NFC 设备的占用率和激活率数据，我们不难看出两个巨大的加速引擎分别是智能手机的到来和移动支付的落地。原因为前者简化 NFC 技术集成的难度，后者则从用户体验入手把现有的一些非接触的支付应用集成到了手机里面，比如集成平时使用率高的公交卡和芯片银行卡应用等。目前能看到的 NFC 技术在支持模拟卡片的功能对用户体验带来极大的方便，例如用户的公交卡开卡和充值都可以在手机应用中完成，而不需要去公交充值站点排队等待。带 NFC 的支付功能的手机是可以在线下实体店中的大部分 POS 机上的完成银行卡的非接触刷卡交易，并且支持的线上有卡交易也是一个集安全和体验为一体的有价值的应用。从目前看到的线上有卡交易数据量，未来这可能是一个体量巨大的应用分支。

NFC 论坛定义 NFC 设备的三个大块的属性分别为设备对外部卡片标签的读/写模式、设备与设备之间的点对点通信模式以及设备本身支持模拟卡片的模式。

在论坛定义的读/写模式中，目前只是定义了 4 类标签，市面上的 NFC 设备一般是不止支持这 4 类标签，实际上支持得更多。但不管如何这 4 类标签中 Tag1/2/4 的射频技术都是基于 ISO/IEC 14443 的，Tag3 则是一个主要应用于日本国内的一个技术，规范参考(JIS) X 6319-4。

点对点的工作模式需要参考的规范为 ISO/IEC 18092。其实底层参考的射频通信技术也还是把 ISO/IEC 14443 和(JIS) X 6319-4 做了一些细微改动然后把它们揉在了一起。工作原因有机会与当初参与过讨论定义这个规范的人员进行交流，大概当初飞利浦和索尼公司在为了找到一个双方都能相互紧密捆绑在一起的技术点，用于双方分别支持的 ISO/IEC 14443 和(JIS) X 6319-4 设备能更好地互连互通，后来点对点模式找到了这个切入点，技术本身上来讲其实点对点的底层射频技术还是那

两种。

关于卡模拟功能，标准上来讲就是根据各自的喜好或意愿，NFC 论坛本身不对此功能的具体技术进行定义和规范，所以想要了解更多的技术细节就需要去研究和学习 GP 规范和 JAVA 卡标准。根据这本书的市场反响我再考虑是否编写一本更多关于这个方面细节的书，这都是后话。不管你想模拟成一张什么样标准什么样技术的卡片，最终其实都是为了有更多用户能用起来刷起来，但是市面上已有的银行 POS、公交系统大部分都是基本 ISO/IEC 14443 的标准。

基于 ISO/IEC 14443 规范理论上通信距离能做到 10 cm 左右，这是一个理论数据，基于的是一个自由开放的射频场。事实上市面上已有的 NFC 设备由于结构件的限制、整机射频的复杂度，最终出来产品的通信距离基本上是要小于这个理论值。市场上看到的 NFC 设备成功交易的通信距离在 2～4 cm 之间，能保持在 4 cm 之内也是 NFC 论坛比较推荐的一个参考范围。现有能看到所有的公交和银行应用的交易数据吞吐量最多都是在几百个字节之内，也就是说 POS 读头与 NFC 设备之间即使它们握手在最低的通信档位 106 kbps，一次完整的交易也是在毫秒级以内完成的。也正是这个范围的通信距离和交易速度对于非接触刷卡交易有了一个比较好的用户体验基础。

所以说其实这三种功能属性几乎都是基于很相似的底层射频技术，如果能把这些底层比较相似的标准和规范进行收缩归置，再把上层数字协议一些的东西进行抽丝剥茧展现给大家，这也是这本书在接下来重点介绍给大家的。

2 术语和缩略语

在任何行业都可能有一些术语之类的东西会让圈外人一头雾水拒之门外，但其实解释清楚后就本身来讲并没有那么难，并且一些必要的缩写能提高大家的沟通效率。所以在开始具体的技术章节之前，这里把一些符号、术语和缩写形式所代表的意思总结如下。

2.1 硬件部分

表 2.1 列出了硬件部分的术语及出处和解释。

表 2.1 硬件部分术语

标示	出处和解释
NFC	Near field communication 近场通信技术
NFCC	NFC Controller NFC 控制器
NFCEE	NFCExecution Environment NFC 运行环境（例如 UICC）
RFID	Radio Frequency Identification 无线射频技术
SE	Secure Element 安全单元
eSE	Embedded Secure Element 嵌入式安全单元
CLF	Contact less front-end 射频前端
CLT	Contact less Tunnel 接触通道
PBTF	Power By The Field (aka PBF) 射频场取电
NFC-WI	Near Field Communication-Wired Interface 近场通信技术 -接触接口（国际标准叫法）
S2C	SigIn-SigOut-Connection（aka NFC-WI）双线接口包括信号进和出（企业内部叫法）
DCLB	Digital Contactless Bridge 数字非接触式桥（企业内部叫法）
SWP	Single Wire Protocol 单线协议
SWIO	Single Wire protocol Input/Output（aka SWP）单线协议包括信号进和出
UICC	Universal Integrated Circuit Card 通用集成电路卡片
CICC	Close-coupledIntegrated Circuit Card 密耦合卡片
CCD	Close-coupled Device 密耦合读头

续表 2.1

标示	出处和解释
PICC	ProximityIntegrated Circuit Card 近耦合卡片
PCD	Proximity Coupling Device 近耦合读头
VICC	Vicinity Integrated Circuit Cards 疏耦合卡片
VCD	Vicinity Coupling Device 疏耦合读头
UID	Unique Identifier 唯一标示号码
AID	Application Identifier 应用标示号码
PMU	Power Management Unit 单元管理单元
CGU	ClockGeneration Unit 时钟发生器
CIU	Contactless Interface Unit 非接触接口单元
MAC	Media Access Control 介质访问控制
PHY	Physical Layer 物理层
AGC	Automatic Gain Control 自动增益控制

2.2 软件部分

表 2.2 列出了软件部分的术语及出处和解释。

表 2.2 软件部分术语

标示	出处和解释
JVM	Java Virtual Machine Java 虚拟机
JSR	Java Specification Requests Java 规范申请
JNI	Java Native Interface Java 原生接口
FRI	Forum Reference Implementation 论坛参考实现
NDEF	NFC Data Exchange Format NFC 数据交换格式
RTD	Record Type Definition 记录类型定义
HAL	Hardware Abstraction Layer 硬件抽象层
DAL	Data Access Layer 数据访问层
OSAL	Operating System Abstraction Layer 操作系统抽象层
HCI	Host Controller Interface 主机控制接口
LLC	Logical Link Control 逻辑链路控制
LLCP	Logical Link Control Protocol 逻辑链路控制协议

续表 2.2

标示	出处和解释
P2P	Peer to Peer 点对点
REQA,B	Request Command,Type A,Type B 请求命令类型 A 卡,请求命令类型 B 卡
ATQA,B	Answer To Request,Type A,Type B 应答请求类型 A 卡,应答请求类型 B 卡
SAK	Select AcKnowledge 选择应答
APDU	Application Protocol Data Unit 智能卡应用协议数据单元
C-APDU	Command APDU 命令型 APDU 数据
R-APDU	Response APDU 应答型 APDU 数据
ATR	Answer To Reset 复位应答命令
ATTRIB	PICC selection command,Type B 类型 B 卡选择命令
HLTA,B	Halt Command,Type A,Type B 停止命令类型 A 卡,停止命令类型 B 卡
SEL	SELect code,Type A 类型 A 卡选择代码
SELECT	Select Command,Type A 类型 A 卡选择命令
WUPA,B	Wake-UP Command,Type A,Type B 复位命令类型 A 卡,复位命令类型 B 卡
NfcA	ISO14443-3A ISO14443 第三层协议类型 A 卡
NfcB	ISO14443-3B ISO14443 第三层协议类型 B 卡
NfcF	JIS 6319-4 日本 Felica 标准的参考规范
NfcV	ISO 15693 近场耦合卡片的参考规范
IsoDep	ISO 14443-4 近场感应卡片的参考规范
CLT cmd	first byte is not 'E0(RATS)','50(HLTA)','93(ANTI-1)','95' or '97',第一条指令不为 E0/50/93 的命令
Tag 1	Topaz 企业内部商标卡片的叫法（T1T）
Tag 2	MIFARE Ultralight 企业内部商标卡片的叫法（T2T）
Tag 3	Felica 企业内部商标卡片的叫法（T3T）
Tag 4	MIFARE Desfire 企业内部商标卡片的叫法（T4T）

2.3 安全单元和认证部分

表 2.3 列出了安全单元和认证部分的术语及出处和解释。

表 2.3 安全单元和认证部分术语

标示	出处和解释
GCF	Global Certification Forum 全球认证论坛
PTCRB	PCS Type Certification Review Board 个人电脑类型认证审查委员会
CE	Conformite Europeenne 欧洲安全合格标示
FCC	Federal Communication Commission 美国联邦通信委员会
FCT	Forum Certificate Tests 论坛认证测试
PBOCx.x	People's Bank of China (aka JR/T 0025-2005) 中国人民银行支付规范标准
BCTC	Bank Card TestCenter (China) 银行卡检测中心(中国)
SCC	Standards Council of Canada (Canada) 加拿大标准委员会(加拿大)
CESTI	Centres d'Evaluation de la Sécurité des Technologies de l'Information (France) 技术安全信息评价中心(法国)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Germany) 德国联邦信息安全局(德国)
UKAS	United Kingdom Accreditation Service (UK) 英国认证服务局(英国)
NIST	National Institute of Standards and Technology (US) 国家标准与技术研究所(美国)
CC	Common Criteria 通用标准
EAL	EvaluationAssurance Level 评估保证级别
FIPS	Federal Information Processing Standards 联邦信息处理标准
EMV	Europay MasterCard and VISA 欧洲万事达和维萨组织
JCOP	Java Card Open Platform Java 卡开放平台
JCVM	Java Card Virtual Machine Java 卡虚拟机
JCRE	Java Card Runtime Environment Java 卡运行环境
GP	Global Platform 全球卡片平台标准
OP3	Open Platform Protection Profile 开放平台保护规范
TOE	Target Of Evaluation 目标评价
SFRs	Security Functional Requirements 安全功能要求
SARs	Security Assurance Requirements 安全保证要求
PP	Protection Profile 保护规范
ST	Security Target 安全目标
DAP	Data Authentication Pattern 数据认证模式
ACM	Access Condition Matrix 访问状态矩阵
EAC	Extended Access Control 扩展访问控制
LDS	Logical Data Structure 逻辑数据结构
CQM	Card Quality Management 卡片质量管理

续表 2.3

标示	出处和解释
PKI	Public Key Infrastructure 公共密钥
RNG	Random Number Generator 随机数发生器
SFI	Single Fault Injection 单一故障注入
AES	Advanced Encryption Standard 高级加密标准
DES	Data Encryption Standard 数据加密标准
RSA	Rivest,Shamir and Adleman asymmetric algorithm 不对称算法
IIN	Issuer Identification Number 发行识别号码
PIN	Personal Identification Number 个人识别号码
OID	Object Identifier 对象标示符
TLV	TagLength Value 标签 长度 键值
SMX	Smart MX 企业内部商标卡片的叫法
CM	Card Manager 卡片管理者
CVM	Cardholder Verification Methods 持卡人检验方法
ISD	Issuer Security Domain 主控安全域
SSD	Supplementary Security Domain 辅助安全域
TSM	Trusted Service Management 可信服务管理
HSM	Hardware Security Module 硬件加密机
SE	Secure Element 安全单元
eSE	embedded Secure Element 内置安全单元
SEI-TSM	Secure Element Issuer-Trusted Service Management 安全单元发行商可信服务管理
SP-TSM	Service Provider-Trusted Service Management 服务提供商可信服务管理
TEE	Trusted Execution Environment (ex. MobiCore) 可信赖执行环境
OP-TEE	Open Source Trust Execution Environment (https: //github.com/OP-TEE) TEE 开源社区操作系统
REE	Rich Execution Environment (ex. Android,iOS) 通用执行环境
TA	Trusted Application (ex. Alipay Wallet) 可信赖应用程序
TZ	TrustZone (ex.Cortex-A15,Cortex-A9,Cortex-A8,Cortex-A7,Cortex-A5,ARM1176) 信任区
TCM	Tightly Coupled Memory 紧耦合存储器
TZPC	TrustZone Protection Controller 信任区保护控制器
TZMA	TrustZone Memory Adapter 信任区存储适配器
TZASC	TrustZone Address Space Controller 信任区控制器地址空间
SMC	Secure Monitor Call 安全监控电话
SCR	Secure Configuration Register 安全配置登记
SE-Linux	Security Enhanced Linux 安全增强式 Linux
QRCode	Quick Response Code 二维码

3 通用无线连接技术

平时生活中接触得比较多的无线电连接技术有如用途广泛的移动电话、Wi-Fi和收音广播等，在把通信的距离缩小到半径200米左右以及通信支持上下行技术，我们就能看到下面这些已有的技术。

- **蓝牙无线技术**

当初设计该技术就是为了代替两台手机或电脑它们之间传送数据时使用线缆，现在它们之间的理论通信距离在半径10米左右，目前在蓝牙耳机、音响以及在车载电子上应用广泛。

- **Wi-Fi技术**

在一个相对比较固定的环境下使用该技术对于室内布线的复杂度能大大减低，例如宾馆、家庭、办公室等。该技术设计初衷也是为了能更好地优化局域网络(LAN)，在一个相对干净的自由场里通信距离能到达半径100米或更远。

- **ZigBee无线技术**

主要应用于组网规模相对大一些的工业自动化领域。该技术的通信范围也是可以做到在半径100米范围内，目前在餐馆使用的手持订单终端应用广泛。

- **红外无线技术(IrDA)**

是一个短程小于1米的通过光进行的交换数据的技术。红外线接口经常用于电脑、手机和数码产品之间。

- **无线射频识别(RFID)**

此技术本身的定义的概率比较宽泛，有高低频之分，有有源和无源通信之分。大概的工作原理为通过读头可以发起对外部的无线识别标签进行远程存储和检索数据。

- **非接触技术**

一般大家说的该技术都是约定俗成的ISO 14443和日本的FeliCa技术。该技术其实也是属于RFID中的一种，主机读头为有源工作，而卡片则是无源的。在工作时读头发起射频场强并且附加通信数据给卡片，卡片在收到无线射频场强时会把这