

手机支付双界面卡的接触式与非接触式接口标准的研究

刘瑞玲, 李代平

(广东工业大学 计算机学院, 广东 广州 510090)

摘要: 针对双界面卡实现手机支付涉及接触式和非接触式两种相异的通信方式, 目前尚没有形成关于双界面卡开发的统一标准的问题, 通过对 SIMpass 方案的介绍, 以及对双界面卡中用到的 ISO/IEC7816 和 ISO/IEC14443 标准的详细分析, 得到在双界面卡的设计过程中应依据的标准和规范。指出当前双界面卡发展存在的问题, 为下一步双界面卡的设计实现做好了理论准备。

关键词: 手机支付; 双界面卡; 接触式; 非接触式

中图分类号: TP391.4

文献标识码: B

文章编号: 1674-7720(2010)14-0069-03

The study about the contact and non-contact mode interface's standard of mobile-payment's combi-SIM

LIU Rui Ling, LI Dai Ping

(School of Computer Science, Guangdong University of Technology, Guangzhou 510090, China)

Abstract: The double-interface card includes contact mode and non-contact mode, which are different in communication form. And nowadays, this profession hasn't unified standards for the double-interface card. Through to the SIMpass plan's introduction, and the multianalysis about ISO/IEC7816 and the ISO/IEC14443 which use in the combi-SIM, obtains the basis standard which will be used in the designing process for the double-interface card. At last, point out some questions coming from the double-interface card development, and makes the theory preparation for the combi-SIM's design and realization.

Key words: mobile-payment; combi-SIM; contact mode; non-contact mode

随着通信技术的发展, 手机功能日益增强, 各运营商为了提高市场占有率和效益最大化, 纷纷开发多种增值业务。随着 3G 技术的发展和成熟, 手机支付受到各运营商青睐, 以手机支付来代替生活中流通的各种卡, 不仅能够方便消费者, 也能为商家节约购卡投资。

手机支付的方式有两种: 第一种是从用户手机绑定的银行账户或信用卡账户中扣除费用, 如在手机支付业务合作商家(超市、餐饮、公交系统等)消费时, 只需在阅读器上刷手机, 即可完成款项支付。在此过程中, 手机只起到把用户银行帐户或信用卡帐户与终端机连接起来的作用; 第二种是通过用户支付其手机账单时支付费用, 由于行业间业务的限制, 该方式目前仅应用于手机铃声下载等有限业务。本文讨论的是第一种支付方式。

1 手机支付

1.1 手机支付概述

手机支付系统包括移动运营商、支付服务商(如银行)、应用提供商(如公交车、学校等)、设备提供商(终端厂商)、系统集成商、商家和终端用户。当前业内手机支付的主流技术实现方案有两种, 分别是 NFC^[1]方案和 SIMpass 方案^[2]。手机支付示意图如图 1 所示。

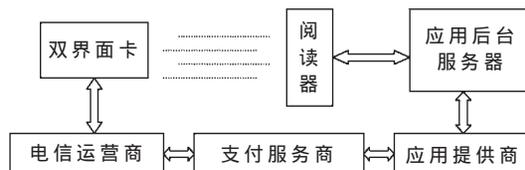


图 1 手机支付示意图

近距离无线通信 NFC(Near Field Communication)是由飞利浦、诺基亚、索尼等著名厂商联合主推的一项无线

技术与方法 Technique and Method

技术。NFC 由非接触式射频识别(RFID)和互联互通技术集中在单一芯片上,可在有限距离内(10 cm)与相关设备进行识别和数据交换。

SIMpass 方案融合了 DI 卡技术和 SIM 卡技术,称为双界面 SIM 卡,支持接触与非接触两个工作接口,接触界面实现 SIM 功能,非接触界面实现支付功能,兼容多个智能卡应用规范。利用 SIMpass 技术,可在无线通信网络及相应的手机支付业务服务平台的支持下,开展各种基于手机的现场移动支付服务。使用 SIMpass 的用户只需在相应的消费终端前挥一下,即可安全、轻松地完成支付过程。

1.2 SIMpass 方案

SIMpass 是一张双界面的多功能应用智能卡,集非接触式和接触式两个操作界面于一体。工作时,对芯片的访问可以通过接触界面实现,也可以由非接触式以射频方式实现。两个界面分别遵循两个不同的标准,接触界面符合 ISO/IEC 7816,非接触符合 ISO/IEC 14443。

双界面卡可分为以下三种:

(1)接触式智能卡系统与非接触式智能卡系统仅仅是物理地组合到一张卡片中,存在两个 EEPROM,两套系统互相独立。

(2)接触式智能卡系统与非接触式智能卡系统彼此操作独立,但共享卡内部分存储空间。

(3)接触式智能卡系统与非接触式智能卡系统完全融合,接触式与非接触式运行状态相同,共用一个 CPU 管理。

三种双界面 IC 卡中,只有最后一种双界面 IC 卡才是真正意义上的非接触式双界面 CPU 卡。

双界面 SIM 卡包括一个微处理器芯片和一个与微处理器芯片相连的天线线圈,由读写器产生的电磁场提供能量,能通过射频方式实现能量供应和数据传输。在 SIM 卡中加入非接触式界面,而用于提供电能和数据传输的天线集成在手机中或者印刷在塑料膜上,作为独立的一个部件存在,通过接触式界面处理传统的 GSM 命令,采用非接触式界面解决支付问题。其系统结构图如图 2 所示。

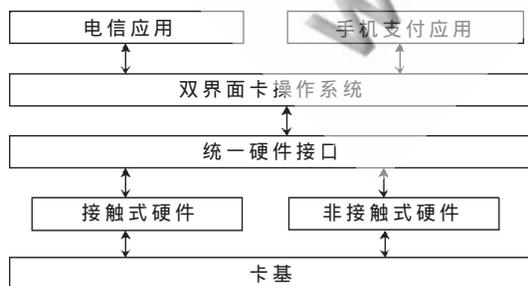


图 2 双界面卡 SIMpass 方案系统结构图

2 接触式系统和非接触式系统简介

2.1 接触式系统

双界面 SIM 卡的接触界面按 SIM 卡设计,其 IC 结

构包括:

- (1)SIM/UIM/USIM/PIM——用于储存用户数据、身份认证及为手机短信提供储存空间;
- (2)EEPROM——电可擦写存储器;
- (3)CPU——中央处理器;
- (4)ROM——只读存储器。

SIM 卡部分用于正常的手机移动通信、鉴权,因此,在实际设计时要符合电信业内相关规范和标准。接触式卡面的设计依据 ISO/IEC7816 系列规范。

2.2 非接触式系统

非接触式系统主要由射频识别 RFID(Radio Frequency Identification)技术实现^[2]。一般物理构成包括标签、阅读器和天线三部分。

RFID 技术分类如下:

- (1)按应用频率分为低频、高频、超高频和微波。
- (2)按能源的供给方式分为无源、有源和半有源。无源 RFID 读写距离近;有源 RFID 读写距离远,但需有电池供电。
- (3)按调制方式分为主动式和被动式。前者用自身的射频能量主动地发送数据给读写器;后者使用调制散射方式发射数据,必须利用读写器的载波来调制自己的信号。

RFID 技术工作原理(针对被动式而言)是,当阅读器遇见 RFID 标签时,发出电磁波,周围形成电磁场,标签从电磁场中获得能量激活标签中的微芯片电路,芯片转换电磁波,然后又发送给阅读器,阅读器把它转换成相关数据。

由于双界面卡中的手机支付使用范围小,所以在设计开发时,RFID 主要参照 ISO 14443A/B(ISO SC17/WG8)标准。

3 ISO/IEC7816 和 ISO14443

由上综述可知,SIMpass 方案中的双界面 SIM 卡接触式界面和非接触式界面的工作原理和设计依据标准互不相同。

3.1 ISO/IEC7816

ISO/IEC7816 是一套规范体系,它包括以下几部分:

- (1)ISO/IEC7816-1:接触式 IC 卡的物理特性;
- (2)ISO/IEC7816-2:接触式 IC 卡的触点尺寸和位置;
- (3)ISO/IEC7816-3:接触式 IC 卡(异步卡)的电信号和传输协议;
- (4)ISO/IEC7816-4:行业间交换命令;
- (5)ISO/IEC7816-5:应用标识符的编号系统和注册过程;
- (6)ISO/IEC7816-6:行业间数据元;
- (7)ISO/IEC7816-7:结构化卡查询语言的行业间命令;
- (8)ISO/IEC7816-8:安全有关行业间命令;
- (9)ISO/IEC7816-9:接触式卡管理命令;

技术与方法 Technique and Method

(10)ISO/IEC7816-10:接触式 IC 卡(同步卡)的电信号和复位应答。

其中 ISO/IEC7816 的第 4 至第 9 部分属于传输层及应用层标准,第 1 至 3 部分主要介绍了接触式集成电路卡的基本技术要求^[3]。

ISO/IEC7816-2 对该类 IC 卡的触点作了详细的规定,各触点及功能如表 1 所示。

表 1 接触式 IC 卡芯片触点的分配表

触点序号	功能	触点序号	功能
C1	电源电压 V_{CC}	C5	接地 GND
C2	复位信号 RST	C6	编程电压 V_{PP}
C3	时钟信号 CLK	C7	数据输入/输出接口 I/O
C4	保留	C8	保留

在设计双界面卡的 SIM 卡时,可以把 C4、C8 用于连接射频识别中的天线部分。

通过触点 V_{CC} ,接口设备应向卡提供两种电压支持,即 A 类(5 V)和 B 类(3 V),因此接口设备也相应地分为 A 类接口、B 类接口和 AB 类接口设备。两类卡和三类接口的对应关系如图 3 所示。

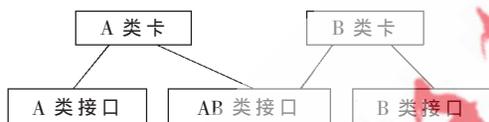


图 3 A、B 类卡与接口关系

只有当 IC 卡的触点与接口设备的触点被机械地连接时,电路被激活,即 RST 置为低电平状态,然后按照接口设备所选择的操作条件给 V_{CC} 通电(分 A 类、B 类),接口设备上的 I/O 应为接收状态,同时 CLK 提供时钟信号。电路被激活后,卡和接口设备之间进行信息交换,最后由接口设备释放电路。

接触式 IC 卡的信息传输协议分为异步半双工字符传输协议(T=0)和异步半双工块传输协议(T=1)。由于 T=0 传输协议应用广泛,目前国内外的接触式卡都支持 T=0 协议。双界面卡中接触式卡也应采用该协议。

3.2 ISO14443 标准

射频卡包括天线、防冲突环等。各部分在设计 and 制作过程中都分别遵照 ISO/IEC14443 相对应部分的要求^[4]。

(1)ISO/IEC14443-1:非接触式 IC 卡的物理特性;

(2)ISO/IEC14443-2:非接触式 IC 卡的射频能量和信号接口;

(3)ISO/IEC14443-3:非接触式 IC 卡的初始化和防冲突(Type A/Type B);

(4)ISO/IEC14443-4:非接触式 IC 卡的选择应答和传输协议(T=CL)。

3.3 双界面卡设计依据

由于双界面卡中的接触式与非接触式两部分物理

和电器特性方面互异,因此在设计开发时应合理规划,严格按照 ISO/IEC7816 和 ISO/IEC14443 协议标准。通过上述内容可知,这两个标准之间存在层次依附关系^[5],如图 4 所示。

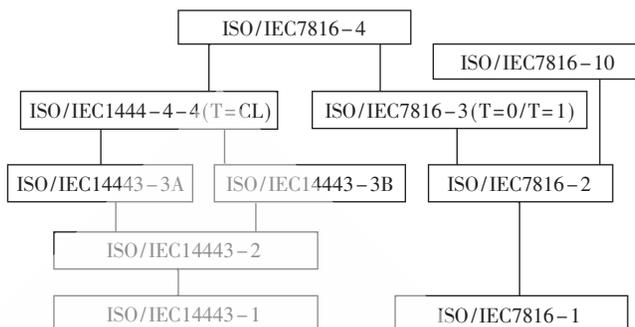


图 4 ISO/IEC1444 和 ISO/IEC7816 的关系

4 双界面卡评价

4.1 双界面卡的优势

(1)一卡多用

一张双界面卡能集成多个行业的不同应用。对于接触式应用,双界面卡正常进行;对于手机支付应用,根据应用条件和场合,可任选采用接触或非接触方式,能有效提高工作效率。

(2)高度安全

双界面卡卡基采用带随机数据发生器的芯片,能有效预防各种物理攻击;芯片的片内操作系统一次写成,从而保证了逻辑上的安全。在传输过程中,接触式和非接触式的数据都依据相关通信协议,而且其间运用了要求的加密算法,即使数据发生泄露也不会对安全造成危害。

4.2 双界面卡的不足

从技术角度看,业界尚没有关于双界面卡统一完善的设计、测试标准和依据,因此操作系统开发难度大、物理结构上的封装不易完成。双界面卡在某一具体行业或应用中如何规划才能达到最佳性价比,需要不断探索和改进。

从市场角度看,由于技术难度制约着双界面卡的价格,而且一卡多用的优势尚不明显,因此,在市场推广使用中有一定难度。

从安全角度看,人们对双界面卡认识不够,对其非接触式应用的安全性存在一定的顾虑。

从应用角度看,双界面卡的应用领域还要进一步拓宽,特别是其非接触式方面的应用,除手机支付外,还可以运用到身份识别或门禁功能。总之,尽可能充分发挥一卡多用、一卡通用的优势。

本文在分析手机支付常用的 SIMpass 方案的基础上,重点介绍了接触式和非接触式系统,以及通过分析两者的通信协议——ISO/IEC7816 和 ISO/IEC14443,得

出二者协议之间的相互依赖关系,对下一步双界面卡的研究和实现有一定的启发作用。另外,还指出了双界面卡目前存在的不足和有待改进的方面,希望对同行有所帮助。

参考文献

[1] 王翠玲.一种双界面多应用 SIM 卡的操作系统设计[D]. 厦门大学信息科学与技术学院,2008.
[2] 金倩,耿力.基于 RFID 的手机支付技术及标准[J].信息技术与标准化,2008,50(3):21.
[3] ISO 7816 Smart card standard[S].1999.

[4] ISO/IEC14443-2000 识别卡-非接触式集成电路卡-接近卡[S].2000.
[5] 中国电信 UIM 卡多应用框架需求规范[S].2009.
[6] 徐中华,刘玉珍,张焕国.一种新的“一卡多用”智能卡模型[J].计算机工程,2003,29(5).

(收稿日期:2010-02-28)

作者简介:

刘瑞玲,女,1982年生,硕士研究生,主要研究方向:3G 智能卡的开发、并行计算。

李代平,男,1955年生,教授,硕士生导师,主要研究方向:3G 智能卡研发、并行计算、体系结构等。

