



大容量 USIM 智能卡技术及应用

董双赫,严斌峰,胡 博,郭晓花

(中国联合网络通信有限公司研究院 北京 100032)

摘 要:对新型大容量 USIM 智能卡进行了详细介绍和深入探讨。介绍了高速 IC-USB 机卡通道、集成 NAND flash 闪存芯片等大容量卡的关键技术。对比传统智能卡,新型大容量 USIM 智能卡具有更高传输速率、更大存储空间、数据安全存储等优点。探讨了大容量 USIM 卡配套的管理客户端及业务管理平台的架构及功能,分析了该技术可能造成的影响,并给出了对未来业务模式和应用场景的建议和规划。

关键词:大容量 USIM 智能卡;业务模式;应用场景

doi: 10.11959/j.issn.1000-0801.2015075

Technology and Application of High-Capacity USIM Card

Dong Shuanghe, Yan Binfeng, Hu Bo, Guo Xiaohua

(China Unicom Research Institute, Beijing 100032, China)

Abstract: A new high-capacity USIM card was introduced and discussed in detail and depth. Its key technology (IC-USB interface, integrated NAND flash chips) was introduced. Compared to traditional SIM card, the high-capacity USIM card has higher transmission rates, larger storage space, and data security storage. The structure and functions of supporting client and management platform were discussed. The influence of this technology may have caused was analyzed. Appropriate suggestions and plantings to the future of business model and application scenario were given.

Key words: high-capacity USIM card, business model, application scenario

1 引言

20 世纪 80 年代之后,数字无线通信技术引入了 SIM (subscriber identity module, 客户识别模块)卡的概念。SIM 卡实际上是一张内含大规模集成电路的智能卡,用来登记用户的重要数据和信息,通过鉴权来防止未经授权的无线接入,保护网络运营商和用户身份不被假冒;通过对传输加密防止在无线信道上被窃听,保护用户隐私;实现了移动通信终端的机卡分离,大大增强了各终端设备的共享性。如今,电信智能卡已经普遍应用于各种具有无线通

信需求的终端中,如手机、平板、汽车、家电等。电信智能卡作为独立的安全硬件具备用户身份鉴权、个人数据(短信、通讯录)存储、运行智能卡应用等功能。随着电信智能卡技术的发展,在智能卡上承载的业务越来越多,而智能卡自身又是用户手中唯一完全由运营商掌控的元素,这使得智能卡成为运营商发展业务的有力武器。

但是近年来移动互联网发展迅速,作为移动互联网的载体和入口,智能终端的种类和功能也有了突飞猛进的发展。在用户眼中智能终端品牌已经显得更为重要,而网络运营商的品牌及其所提供的服务往往被忽略掉了。与智能

收稿日期:2015-02-05;修回日期:2015-03-03

论文引用格式:董双赫,严斌峰,胡博等. 大容量 USIM 智能卡技术及应用. 电信科学, 2015075

Dong S H, Yan B F, Hu B, *et al.* Technology and Application of High-Capacity USIM Card. Telecommunications Science, 2015075



终端的快速进化相比,电信智能卡诞生至今发展却一直非常缓慢。从 2G 卡到 3G 卡再到 LTE 卡,卡的功能一直相对单一,只有通信鉴权等简单功能;卡容量从最初的 8 KB 到现在的 512 KB,一直没有大的提升,使得向卡内存储多个应用或内容时空间十分紧张;同时智能卡与终端的数据传输接口仍然沿用最古老的通信接口,数据传输速率十分有限。传统智能卡的数据传输速率、数据存储容量等的限制已成为运营商发展智能卡新业务的瓶颈。

中国联合网络通信集团有限公司(以下简称中国联通)在传统电信智能卡基础上正在研发并推出具备 GB 级存储能力的新型大容量 USIM(universal subscriber identity module,全球用户身份模块)电信智能卡(以下简称大容量卡),以提升智能卡基础硬件能力,打造智能卡新型业务模式,建立移动互联网时代新的用户入口。

2 大容量卡的关键技术

2.1 整体架构

智能卡(CPU 卡)是一种镶嵌集成电路芯片并且芯片中带有微处理器、存储单元以及芯片操作系统的卡片,具有数据存储、命令处理和数据安全保护等功能。传统电信智能卡大部分采用 8 管脚或 6 管脚设计,内部模块包括 CPU(8 bit)、ROM(3~8 kbit)、RAM(6~16 kbit)、EEPROM(128~512 kbit)和串行通信单元,与终端的接口只有标准的 ISO 7816 接口。

大容量卡与传统电信智能卡采用了不同的封装工艺,在原有卡片结构基础上集成了 NAND flash(2~16 GB)闪存芯片,用于扩展数据存储容量;采用了新的 IC-USB 接口取代传统的 ISO 7816 接口作为新的数据传输通道;将客户端形式作为新的交互界面,大容量卡架构如图 1 所示。

2.2 IC-USB 高速机卡接口

传统智能卡与智能终端的接口(C7 触点)根据 ISO/IEC 7816 系列规范定义,通过 APDU(application protocol data unit,应用协议数据单元)交换数据,实际数据传输速率非常慢(14 KB/s),这导致终端与卡只能进行简单的命令交互,无法快速传输大量数据。

大容量卡采用了新的 IC-USB 接口,该接口在 TS 102 600 规范中定义,用于在芯片间通过 USB2.0 协议进行数据传输。该接口使用卡片预留的 C4、C8 接口作为数据 I/O 通道,终端则复用原有的 USB2.0 驱动即可实现与大容量卡的数据交互。

USB 技术的实现包含了 USB 主机和 USB 设备两个方面,但是在原有终端上,终端对于 USB 技术的实现是基于 USB 设备的,而不是基于 USB 主机的,这两者在实现技术上有比较大的区别。中国联通与终端设备厂商经过共同努力,克服了大量困难,在终端上实现了从 USB 设备向 USB 主机的转化,包括集成 USB 主机芯片、改造 BASE BAND 设计、改造传统 SIM 卡电气部分接口(C4、C8)、添加 USB 系统管理软件等。目前已有多家芯片厂商具备了成熟的大

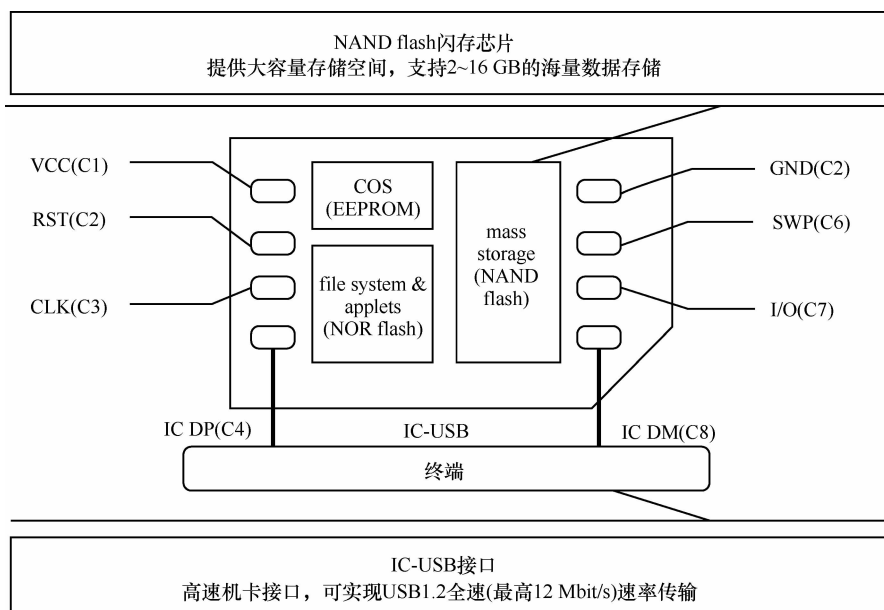


图 1 大容量卡架构

容量卡芯片技术,多款终端能实现大容量卡配套功能。

IC-USB 接口支持 APDU over USB 模式,即通过 USB 协议发送 APDU 指令,使其在功能上能够完全取代原有的 ISO 7816 接口,同时该接口还支持 mass storage(大容量存储)模式,能够进行较大数据和多媒体文件的传输;IC-USB 接口使得智能卡与终端的数据传输速率有了质的提升,目前支持 USB2.0 全速模式(12 Mbit/s),未来还将支持 USB2.0 高速(HSIC)模式。

IC-USB 支持的智能卡—终端数据传输协议有 CCID (USB chip/smart card interface device,USB 芯片智能卡接口设备)和 ICCD(USB integrated circuit card device,USB 集成电路卡设备)两种。CCID 定义了智能卡读卡器接口规范,通过此规范终端可以与智能卡通信,智能卡集成了读卡器功能和 ICC 功能;ICCD 引用了 CCID 内容,并针对部分规则做了特殊定义,如端点配置了 bulk 传输和 control 传输(CCID 以 bulk 传输为主),支持 3 种报文(CCID 支持 14 种报文),使用 control 传输实现低速数据交互(CCID 支持全速及高速数据传输)。从目前技术支持和未来的发展情况看,CCID 协议具备更好的设备兼容性、更强大的速率支持和更好的可扩展性。因此,经过综合考虑,大容量卡的接口采用了 CCID 传输协议。

由于 IC-USB 接口承载了 APDU over USB 及 mass storage 等多个模式,智能卡需要具备处理通信中断和延时的逻辑,即 APDU 指令具备最高优先级。当多条数据并发时,要保证 APDU 优先发送,对其他数据进行延时处理;当正在进行 mass storage 传输,有电信业务需要与卡通信时,应中断 mass storage 传输,处理 APDU 命令,并在结束后恢复 mass storage 的数据传输。

IC-USB 接口实际传输速率(读速率为 700 KB/s,写速率为 500 KB/s)是传统接口的 40~50 倍,见表 1。这使得向卡内下载较大的应用程序无需长时间等待,读取卡内数据更为快捷,甚至播放卡内存储的 720 p 视频都十分流畅。

表 1 机卡速率对比

机卡接口类型	实际传输速率/(KB·s ⁻¹)
ISO 7816	14
IC-USB	500~700

2.3 大容量存储芯片

传统电信智能卡存储介质为 EEPROM 或 NOR flash。EEPROM 通过电子擦除,价格很高、写入时间长、写入速度慢;NOR flash 目前正在取代 EEPROM 成为主流的存储介

质,NOR 的特点是应用简单、无需专门的接口电路、传输效率高,属于芯片内执行(execute in place,XIP),这样应用程序可以直接在 NOR flash 内运行,不必再把代码读到系统 RAM 中。但是 NOR flash 只在 1~4 MB 的小容量时才具备较高的成本效益,很低的写入和擦除速度大大影响了它的性能。

与 NOR flash 相比,NAND flash 能提供极高的单元密度,并且写入和擦除的速度都很快,但是不支持在内部运行程序,是高数据存储密度的理想解决方案。因此大容量卡采用了全新的封装工艺,在不改变卡片尺寸的基础上封装了 NAND flash 大容量闪存芯片,使得大容量卡具备至少 2 GB 的数据存储容量,极大地扩展了电信智能卡的数据存储空间。

大容量卡采用双芯片设计,集成了智能卡芯片和闪存控制器。智能卡芯片实现传统电信智能卡的安全功能;闪存控制器控制 NAND flash 闪存芯片的数据 I/O。

扩展的大容量空间可用来存储用户私密数据(通讯录、短信、通话记录等),告别了传统电信智能卡只能存储几百条短信和通讯录的历史。同时,这部分空间还可用于存储各种应用程序、各类文档和多媒体文件等,极大地扩展了智能卡的应用场景。普通 SIM 卡和大容量卡存储空间见表 2。

表 2 普通 SIM 卡和大容量卡存储空间对比

智能卡种类	存储空间
普通 SIM 卡	128 KB/512 KB
大容量卡	2~16 GB

2.4 新型业务交互界面

传统电信智能卡的业务交互界面为基于 OTA 的动态 STK(SIM card tool kit,SIM 卡工具套件)菜单,它是一种小型编程语言的软件,可以固化在 SIM 卡中,为 SIM 卡的增值业务提供一个简单、易操作的开发平台。STK 能够接收和发送短信数据,起到 SIM 卡与短信之间的接口作用,同时还允许 SIM 卡运行自己的应用软件。这些功能经常被用在可通过软件激活的电话显示屏上,以文本菜单方式进行信息检索操作或交易。

但是随着移动互联网的发展,用户交互界面也发展为以图形化界面为主的趋势,STK 菜单的交互模式已经变得陈旧和繁琐,STK 菜单只有文本的显示方式,且由多级构成,操作不便,同时无法展示卡内存储的数据内容。因此,中国联通开发了大容量卡管理客户端,以终端应用的形式管理大容量卡,展示卡内数据,提供各种服务。

大容量卡管理客户端基于智能终端应用实现,使得电



信智能卡具备了丰富多彩、方便友好的用户界面,同时功能上实现大容量卡的空间管理,包括卡存储内容的展示和管理、基于卡空间数据的服务和应用等,如图2所示。大容量卡管理客户端让智能卡管理具备了媲美互联网应用的用户体验,使其成为一个新的业务入口。



图2 大容量卡管理客户端界面

大容量卡管理客户端的主要功能如下。

- 文件管理:大容量存储区作为存储介质挂载,以文件形式管理大容量存储区,用户可进行文件的复制、粘贴、剪切、删除等操作,其他应用也可访问该存储区。
- 内容分类展示:客户端中视频、图片、文档、应用等都有单独的展示区域,用户可更方便地浏览各种内容,同时各种文件都可通过调用终端的相应程序打开。
- 智能卡服务入口:实现基于智能卡的业务和功能,包括内容定制、数据备份等,是运营商推广智能卡增值业务的重要途径。

3 大容量卡业务模式与应用场景

大容量卡通过一系列技术创新和硬件升级大幅度提升了电信智能卡的能力,更快的数据传输速率、更大的数据存储空间使其可以支撑更多的新型业务模式。目前,中国联通结合自身特点和移动互联网时代的用户需求探索出一套大容量卡业务体系,通过终端客户端、云平台、大容量电信智能卡和适配终端形成了闭环的业务流,同时开放接口让第三方智能卡应用开发者都可以使用大容量卡业务,以形成大容量卡业务生态系统。

3.1 业务模型

大容量卡业务模型包括手机管理客户端、应用管理平台、大容量卡及其适配终端,大容量卡业务架构如图3所示。

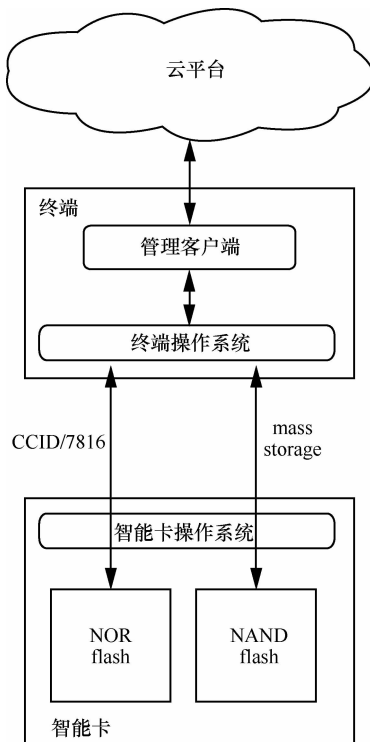


图3 大容量卡业务架构

管理客户端负责大容量卡内数据的呈现和使用,各种业务的展示和使用,是用户与运营商的接触点。

应用管理平台是大容量卡业务的承载和管理平台,实现的功能包括大容量卡客户端的下载和升级、大容量卡内应用和数据的管理、用户管理和信息统计等。

客户端、云平台、大容量卡及适配终端共同构成了大容量卡的业务链,在此基础上可以实现各种新的运营业务,包括数据安全、应用及内容的预置与分发、数据备份和还原等。

3.2 数据安全管理

随着技术的进步,网络对人们经济、社会活动的介入越来越深,信息和数据的收集也变得越来越便捷。一方面使相关行业能够利用信息和数据实现更大的价值创造,另一方面也给个人信息的保护带来了前所未有的挑战。用户信息不仅涉及个人隐私,更是一种重要的“数据资产”,特别是互联网经济的崛起使“大数据”带来的商业价值日益凸显。也正因为如此,相关行业的数据和信息被作为核心

资源广泛争夺。然而,一方面缺少监管,一方面又有利可图,使非法获取个人信息的行为获得了很大的操作空间。近年来,由于经济利益的驱使、行业生态的混乱、法律法规的缺失以及公民自身对个人信息保护意识的欠缺等原因,围绕个人信息的采集、加工、开发和销售正悄然变为一条“数据产业链”,信息泄露造成的“精准营销”和金融诈骗活动给人们的隐私和财产造成了难以估量的损失。

从互联网到移动互联网,智能终端功能越强大,安全隐患就越多。近年来愈演愈烈的手机病毒、木马、诈骗短信造成越来越多的信息泄露、电话短信骚扰甚至银行卡被盗刷等不安全因素。大容量卡作为独立于智能终端的独立硬件,具备独有的安全机制,配合管理客户端可以实现多种安全能力,使得用户数据得到更好地保护。

(1) 文件加密存储

大容量存储区可以进行文件的加密存储,支持多种加密算法,包括 IDEA、RSA、AES 等主流算法。用户的敏感数据可通过管理客户端加密后,存储在大容量卡的加密存储区内,而加密数据的读取也必须通过客户端进行,可以有效防止恶意程序非法访问用户的隐私数据。

(2) 访问控制机制

安全访问控制主要采取全局平台可信任框架的 GPAC(global platform access control,全局平台访问控制)机制。GPAC 由终端的访问控制模块与用户卡中的规则文件构成,可对手机应用访问大容量卡的权限进行控制和管理,以防止 SIM/SE 访问 API(application programming interface,应用程序编程接口)的非法使用给用户卡带来的危害。

通过多重安全保护机制,大容量卡能有效保护用户隐私数据的安全,同时能够安全存储支付证书、支付密钥、交易信息等信息,保证移动支付及金融应用的安全。

3.3 应用、内容的预置与分发

大容量卡的大容量存储空间可进行各种内容的预置,包括终端常用应用、热门视频、音乐、书籍、图片等,这些内容在制卡的时候进行预置,发卡时能够直接到达用户。预置内容不仅方便用户的直接使用,还是一种推广应用的天然渠道。

结合管理客户端和管理平台,大容量卡可以实现一种内容推送服务。例如,用户选择感兴趣的内容,在终端空闲时平台可以向用户卡内定向推送用户选择的内容。卡内内容由于是本地存储,使用时有比在线内容更流畅的用户体

验(如播放视频文件更为流畅,随意切换进度),在离线时也可使用多媒体内容。

3.4 卡内数据备份还原

智能卡作为用户通信的核心入口,保存着用户通讯录、短信、通话记录等重要信息。但是随着这些数据体积越来越大,传统的电信智能卡已经没有空间来进行存储,同时当终端需要读取这些信息时,受限于数据通道的速率限制,读取时间也相应越来越长。以至于近年来用户的通讯录、短信等都已经转移至终端上存储。但是当用户更换手机时,旧终端上的这些信息无法导入新的终端中,导致重要联系人的丢失、重要信息无法转移的问题。

大容量卡拥有很大的存储容量,使得存储通讯录和短信不再受到容量的限制,同时高速的 IC-USB 通道也解决了读取速率的瓶颈。这样用户可以将通讯录和短信全部存在大容量卡中,在更换终端时可以实现通讯录和短信的无缝迁移,不再丢失重要联系人或信息。

在大容量卡管理客户端内还提供了通讯录、短信的备份和还原服务,用户可以将终端内通讯录短信备份到卡(本地)或者管理平台(云平台)上,当使用新卡时可以及时恢复这些重要信息。

除了通讯录和短信,客户端配合云平台还可以提供卡内多种数据的备份还原服务,包括各类应用、视频、音乐等,让用户在换卡后能够还原数据,保证文件不丢失,体验无缝衔接。

4 未来技术演进及应用扩展

大容量卡技术已经具备了商用能力,但是与智能终端及其他存储设备相比还有一些不足之处,如机卡接口传输速率仍然较低,向卡内存储较大文件时时间较长;相比现在智能终端或其他存储设备的存储容量,大容量卡的存储容量较小;虽然在硬件上大容量卡已经有了质的提升,但在业务模式上的探索还处在不成熟的阶段。

未来大容量卡的技术演进及应用场景扩展可以从以下几方面入手。

(1) 提高大容量卡与终端接口的数据传输速率

目前采用的 IC-USB 接口最大传输速率为 USB2.0 全速(12 Mbit/s),未来可以升级为 HSIC 接口,实现 USB2.0 高速(480 Mbit/s)的传输速率。



(2)增大数据存储容量

随着封装技术的进步,未来大容量卡可集成更大容量的 NAND flash 芯片(2~16 GB),极大扩充智能终端的存储容量,同时为运营商开展业务提供更充足的空间。

(3)应用场景扩展

大容量卡的应用场景不仅限于运营商业,还可应用于多种场景。如大容量卡与 NFC 功能结合的复合型智能卡、行业应用(如对于个人数据需要加密存储、通信过程加密处理的行业)、物联网(利用大容量卡自身超大数据存储能力与通信能力的结合优势)等。未来的应用场景和业务模式还需要更多地被发掘。

5 结束语

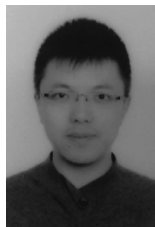
大容量 USIM 电信智能卡具备高速 IC-USB 接口、超大数据存储空间、新型的交互界面和业务模式,是中国联通推出的新一代电信智能卡,也是中国联通在移动互联网时代不断创新、寻求技术突破、探索新型业务模式的尝试。本文详细介绍了大容量卡的关键技术和架构、具体实现方法和未来演进路线,探讨了基于大容量卡的各种应用创新和业务模式,同时提出了对未来发展的建议。

参考文献

- 1 孙海涛,马久和,于春光等. USB 智能卡应用技术研究. 科学技术与工程, 2007(16): 4209~4211
Sun H T, Ma J H, Yu C G, et al. Research on application technology of USB smart card. Science Technology and Engineering, 2007(16): 4209~4211
- 2 李菲菲. USB 协议在智能卡上的多应用研究(硕士学位论文). 北京邮电大学, 2007
Li F F. Research on multi application of USB protocol in smart card (master dissertation). Beijing University of Posts and Telecommunications, 2007
- 3 蒲若崧. 高速、大容量新一代 SIM 卡. 信息安全与通信保密, 2010(7): 57~59
Pu R K. Next generation SIM card of high speed and mega-bit storage. Information Security and Communications Privacy, 2010(7): 57~59
- 4 ETSI TS 102 600. Smart Cards; UICC-Terminal Interface; Characteristics of the USB Interface, Release 10, 2010
- 5 Universal Serial Bus Specification Revision 2.0. USB Implementers Forum, 2000

- 6 Inter-Chip USB Supplement to the USB 2.0 Specification. The Universal Serial Bus Revision 2.0 Specification Package, 2006
- 7 Universal Serial Bus Mass Storage Class Specification Overview (Revision 1.2). USB Implementers Forum, Device Working Group: Mass Storage, 2010
- 8 Universal Serial Bus Mass Storage Class Bulk-Only Transport, Revision 1.0, 1999
- 9 Universal Serial Bus Device Class: Smart Card CCID Specification for Integrated Circuit(s) Cards Interface Devices, Revision 1.1, 2005
- 10 Global Platform Device Technology Secure Element Access Control Version 1.0, 2012

[作者简介]



董双赫,男,中国联合网络通信有限公司研究院终端与测试实验室工程师,主要研究方向为智能卡、智能终端、移动互联网应用等。



严斌峰,男,博士后,中国联合网络通信有限公司研究院终端与测试实验室主任、高级工程师,长期从事终端与智能卡相关研发工作,出版专著 1 部,在国内外期刊上发表论文 10 余篇,并申请了技术发明专利 10 余项,主要研究方向为移动增值业务、终端与智能卡相关技术、终端基础软件技术等。



胡博,男,中国联合网络通信有限公司研究院终端与测试实验室工程师,主要研究方向为智能卡、智能终端、移动互联网应用等。



郭晓花,女,中国联合网络通信有限公司研究院终端与测试实验室工程师,主要研究方向为智能卡、智能终端、移动互联网应用等。