IC卡的技术与应用

王卓人　邓晋钧　刘宗祥　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

内 容 简 介

IC 卡技术正迅猛的普及到国民经济和人民生活的各个领域，成为科技开发人员瞩目的焦点。

本书分二篇。基础篇有：绪论、IC 卡的基本物理特性、IC 卡芯片技术、IC 卡的用卡过程、IC 卡的数据元与命令、IC 卡的安全性、IC 卡的操作系统、IC 卡应用设备及其开发系统。应用篇有：IC 卡应用编制一般考虑、IC 卡在支付系统的应用、GSM 系统中的用户识别模块(SIM 卡)、IC 卡在劳动保险中的应用等。

本书内容全面、深入浅出，适合从事 IC 卡开发设计人员及教学人员参考。

IC 卡的技术与应用

王卓人　邓晋钧　刘宗祥　编著

责任编辑　王惠民

*

电子工业出版社出版(北京市 173 信箱)

电子工业出版社总发行　　各地新华书店经销

华南师范大学印刷厂印刷

*

开本：787 × 1092 毫米　1/16　　印张：29.75　　字数：600 千字

1999 年 2 月第一版　　1999 年 2 月第一次印刷

印数：1 ~ 3000 册　　定价：40.00 元

ISBN7 - 5053 - 4400 - 5/TP·2034

前　言

从开始动笔写这本书，到如今完成它，已经是易两春秋的时光，大部份的内容都是在头一年完成的。但，由于种种原因以后的工作时停时续，至今才得以付印。

在这段时间里，从开始动笔时尚未见到一本有关这一方面的图书，到本书付印前至少已经有三本类似的书了（也许还更多，作者寡闻未得一睹）。报刊、杂志上不断发表的有关论著，以及常有的金卡工程新进展的报导，这些都令人深受鼓舞。在我们这样一个超过 10 亿人口的大国里，就同一个命题写上 3～5 本书，也许不算多，但愿这本书能对读者有用，值得在案头备上一本以便参考查阅。

作者们从已经有的几本书中学得了不少东西。为了和那几本书不完全雷同，首先，我们希望本书尽可能地比较详尽、实用。为此，除了各章写的比较细致、具体外，还专门编写了“IC 卡的操作系统”和“IC 卡应用系统的开发工具”两章（第七章和第八章）。为了避免空洞、不着实际，这两章是以国内开发的 TimeCOS 操作系统（由握奇数据系统公司开发）和相应的开发工具为范例写成的。如果读者不嫌苦燥，能耐心读下去，作者确信对理解 IC 卡的工作过程和应用系统的设计，以及开发工具的掌握会有较大的收益。其中还包括了一些应用实例，有了这样的范例，就能比较快地上手了。

其次，在应用方面，我们的打算是既要尽可能地多讨论一些应用的范围，也要把应用中的具体问题叙述深入透彻些。由于 IC 卡日益扩大其应用领域，深入到日常生活、社会活动的各个方面，作者既无能力，也无可能都涉及到。实际上只讲了金融交易处理，GMS 系统中的用户识别和社会劳动保险三个方面应用的 IC 卡，并以支付系统的 IC 卡为主，详细地叙述了金融交易处理中 IC 卡的工作过程，也许对理解与实施各种支付卡的规范，组成应用系统和 IC 卡的发行会有所帮助。

作者们就是抱着上述愿望合三人之力来从事这一工作的。本书由王卓人主编并编写了第 1,4,5,6,7,10,11 章，第 2,3,8,9,12 章由邓晋钧编写，第 12 章由刘宗祥编，而后再由王卓人修改定稿。作者限于水平和条件，书中定有不少错误或疏漏之处敬请读者和专家指正。

还要说明的是，IC 卡技术仍正在迅速发展之中。例如，非接触 IC 卡就是一个引人注目的方面，一些和 IC 卡应用有关的技术和产品，如生物识别技术和激光存储卡等也都在迅猛发展、日益扩大其应用范围，限于各种原因，未能在本书中一一述及读者们只有从未来的出版物（相信不会有多久）中搜集资料了。

另外，本书在写作中得到了不少同志的帮助和指导，广州华南计算机金卡工程有限公司，握奇数据系统公司给予技术资料方面；电子工业出版社广州科技公司给予出版方面的支持；广州金融电子化公司的罗小姐帮助打印整理了部份手稿，在此一并表示谢意。

编者

1998 年 9 月

目　录

基础篇

应用篇

基础篇

第一章　绪论

以“三金工程”为代表的一批国家重大工程项目是加速我国国民经济信息化建设的重大措施。其中“金卡工程”是跨系统、跨地区、跨世纪的社会系统工程，与我国金融电子化建设和现代化支付系统的建设密切相关。“金卡工程”以计算机、通信等现代化科学技术为基础，通过计算机网络系统，并以银行卡等为介质，用电子信息转帐形式实现货币流通，它的实现必将大大加速我国金融现代化的步伐。

党中央、国务院的领导同志历来十分重视金融现代化和金融科技工作，江泽民总书记在93年6月1日曾说：“随着社会主义市场经济体制的建立，金融业在社会发展中的作用越来越显著，实现金融电子化，建设好金融信息网络，对于实现金融业的现代化，保证中央银行的宏观调控有着积极的作用。”因此，他题词指出：“实现金融电子化，为社会主义市场经济服务。”党的十四届三中全会通过的《中共中央关于建立社会主义市场经济体制若干问题的决定》中明确要求：“实现银行系统计算机网络化，扩大商业汇票和支票等结算工具的使用面，严格结算纪律，提高结算效率，积极推行信用卡，减少现金流通量。”

党中央的这些英明决策，完全符合改革开放，建设社会主义市场经济的需要，符合信息社会发展的需要。信息化是当今人类社会发展的最新生产力，正从总体上引导着全球经济和人类社会发展的进程。

1.1　信息和金卡工程

1.1.1　信息和信息社会

信息是什么？很难给出确切统一的定义，我们只能在各个不同的领域中，从不同的角度来理解其内含和外延。在计算机系统中，把信息定义为数据、消息中所包含的内容。在通信系统中，从产生信息的客观对象看来，信息是客观世界各种事物的变化和特征的反映，是事物运动状态和运动方式的表征，是事物的属性，是事物的内容、形式及其发展变化的反映；从接收信息的认识主体看来，信息是能够用来消除不确定性的东西，是收信者事先所不知道的内容，或者更抽象地说，信息是关于事物未知程度的度量。日常，人们把信息视作信号、数据、资料、情报、消息、新闻、知识等等，而信息则被包含在各种信号及其组合，如语言、文字、图形、图象等表达手段之中。或者更概括地说，信息被包含在音频、视频以及各种声、光、电、化、力学、热学等人们可以直接或间接感知的变化中。控制论奠基人 N. Wiener 在《人有人的用处》一书中认为：“信息这个名称的内容，就是我们对外界进行调节，并使我们的调节为外界所了解时而与外界交换来的东西”，“信息就是变异度”，“信息就是差异”，这类定义说明信息作为作用与反作用过程的表征存在于反映事物特性的相互联系之中。

从上面关于信息的含义可知信息具有客观性、普通性、无限性、动态性、依附性、计量性、变

换性、传递性、系统性等等特性。它是超物质的、可扩散的、能共享的。在人类认识和改造世界的斗争中起着十分巨大的作用。它是认识的依据，实践的指南，开发资源的条件，挖掘智慧的源泉。信息系统是信息“有序化”的过程，是系统组织化的重要因素。它作为“粘合剂”，“联系纽带”和“神经中枢”能对未来的发展和变化进行预测、干预和引导，从而使系统和客观事物，乃至社会和经济机体协调地发展。

显然，信息不是物质和能量。物质可以被加工成为材料，能源可以被转换成为动力，这是人类社会发展的有形资源或称第一资源。信息则可以被提练成为知识和智慧，为人类社会发展开发了无形的第二资源。信息、能量和物质三者就构成了支持人类社会发展的三大战略资源。

人类社会的发展在经历了茹毛饮血、穴居野处的上古时代之后，就进入了开发绿色资源的畜牧和耕耘的农业社会。而后则是开发钢铁、煤炭、石油等黑色资源的工业化社会。目前，正处于向“后工业化社会”演变的阶段之中。所谓“后工业化社会”，有的学者认为就是开发灰色资源(大脑皮层)的信息社会。这就是说：“古代人类主要仅能利用物质一种资源，近代人类能够利用物质和能量两种资源，现代人类正在学会综合利用物质、能量和信息三种资源，这种历史进步，分别导致了古代人力工具，近代动力工具和现代智能工具的出现。”(1996 年信息基础结构国际学术会议北京宣言——“信息时代宣言”)。

可以认为，信息社会的序幕是以二次世界大战的结束，人类社会中出现的所谓三大爆炸而拉开的。这三大爆炸就是核爆炸、人口爆炸和信息爆炸。正是这三大爆炸，特别是信息化，导致了对人类社会的“第三次浪潮”的冲击。“人们亲眼目睹：一场汹涌澎湃的信息化世纪风暴，正席卷着世界的每个角落，……信息化已成为不可逆转的历史进程。”(1996 年信息基础结构国际学术会议北京宣言——“信息时代宣言”)。

现在，人们把经济发达国家工业化和现代化的演变历史进程大致划分为工业化前期、中期(基本实现工业化)和后期(后工业化)三个阶段。工业化的前期可以英国为代表，主要工业为纺织和钢铁，钢铁工业搭起了“社会的骨骼”；中期以美国为代表，典型的工业包括了电力机械和内燃机等机械制造工业和汽车工业，由汽车工业支撑起来的高速公路布下了“社会的动脉”；后期可以日本的崛起为代表，关键工业就是以半导体为基础，计算机和通信为主体的电子工业，构成了“社会的神经和头脑”。这一演变进程可以形象地加以描述：英国人曾经乘着火车和轮船走向了世界霸主的地位；美国人在加快了节奏的时代，驾驶着福特的汽车和莱特兄弟的飞机称雄于一时；今天，以日本为代表的东方，正在发挥电子技术无可估量的作用，创造一个崭新的电子世界，努力实现世界经济重心东移的历史使命。

江泽民总书记在《论世界电子信息产业发展的新特点与我国信息产业的发展战略问题》一文中论述道：“电子信息产业的巨大发展，电子信息技术的广泛应用，正在把世界推向到一个所谓信息经济的时代，电子水准已成为进入后工业化时期发达国家最强大的生产力标志。”

比较起来，我国目前的情况与经济发达国家还有很大差距，商品经济不发达，生产力落后，工农业的劳动生产率相差几十倍，产品结构层次低。从总体上讲，尚处于工业化前期，邓小平同志指出：“中国社会过去闭塞，造成信息不通，是一个很大的弱点。”并提出了“开发信息资源，服务四化建设”的战略。江总书记进一步指出：“振兴我国经济，电子信息技术是一种有效的倍增器，是现实能够发挥作用最大、渗透性最强的新技术，要进一步把大力推广应用电子信息技术提到战略高度，充分发挥电子信息技术对经济的倍增作用，我们就能提高国民经济的效率，降低消耗，利用已形成的相当规模的钢铁、煤炭、电力、石油资源，创造出几倍于当前的国民经

济生产总值。"李鹏总理也指出:"电子和信息是一个新兴产业,代表了新一代的技术和新一代的生产力。它的发展和振兴必将对加快我国四个现代化的进程,振兴我国经济起到不可估量的重大作用。"

今天,大多数发达国家已跨入"后工业化社会",或称"信息化社会",第三产业(服务业)在国民经济中的比重已接近2/3。从前是"钢铁即国家",如今"半导体成了工业的粮食","电子即国家"。国内外的舆论指出:"在市场进一步全球化,竞争日益加剧的今天,企业靠什么取胜?靠信息取胜!信息已成为经济建设的战略资源,国民经济信息化所形成的综合性倍增效益,是当今社会发展的最新生产力。"所以纽约时报评论道:"今后大国对世界的控制主要是信息控制,大国之间的争夺主要是信息争夺。""冷战时代的核威胁,正被信息威胁所取代的看法"不无道理。

经济发达的国家现在都以信息产业,即由现代通信产业、计算机产业、集成电路产业和软件产业—以C^3S表示—所构成的新兴产业群,作为整个社会经济发展的基础。可以这样说,在人类有史以来所形成的各种产业中,没有哪一种能有这么迅猛发展的势头,没有哪一种能具有这么广泛的渗透性,没有哪一种能这么深入地改变与影响人们的生活乃至思维方式。信息产业,这是一座金山,它决定着下一世纪的力量对比,世界各国莫不向这个新的制高点发起全力的冲击。

1.1.2 金卡工程

正是在这种背景下,出于我国社会经济发展的客观而又迫切的需要,党中央、国务院做出了加快我国信息化进程的重大决策。而"三金工程"则是国家经济信息化的基础,它们的出台和实施标志着我国经济的信息化正走向一个新的高度。"三金工程"中,特别是"金卡工程",只有它是直接面向广大群众的,和亿万人民的生活息息相关的工程,它将影响和改变人们的传统观念和消费习惯,促进市场繁荣,极大地方便人们的生活和消费,未来将是"一卡在手,走遍天下"。

今天生活在地球上的人们,那怕他(她)生活在发展中国家,地处偏远的山区、荒芜的沙漠或寒冷的两极,他所处的社会也已经不再是鸡犬之声相闻、老死不相往来的自给自足的自然经济社会了。人们离不开市场、商品、流通、货币,……等等这些经济生活中的各个环节。但是市场、货币以及人们的交易行为和方式也在变化。我们之所以说金卡工程是直接面向广大群众和亿万人民的生活息息相关的工程,原因就在于它是对市场、商品、货币以及传统交易方式的变革。可以这样说,金卡工程也就是电子货币工程,目的是在无纸的、信息化的、商业行为的电子数据流通过程中,实现纸基货币(包括金属基硬币或代用品)的全部功能,完成一次消费或商品交易。

用卡基支付的三个参与方是银行、商户和持卡人,这三者的业务关系如图1-1所示。

在这样的交易行为中;用到的媒介或设备有:信用卡、POS、ATM、网络及通信设备、计算机系统和相应的软件。要完成的功能有:授权、清算、资金的划转等。附带的功能有:信息的输入、输出操作、电子签名、查询、认证和鉴别等。涉及到的对象为:客户(持卡消费者),消费场所(商店、服务单位等特约商户),授权与结算机构(发卡者、银行等)。涉及到的金融计算机应用信息系统有:

·银行POS系统

·银行ATM

·储蓄通存通兑系统
·信用卡授权系统
·资金清算系统
·对公系统(会计核算系统)

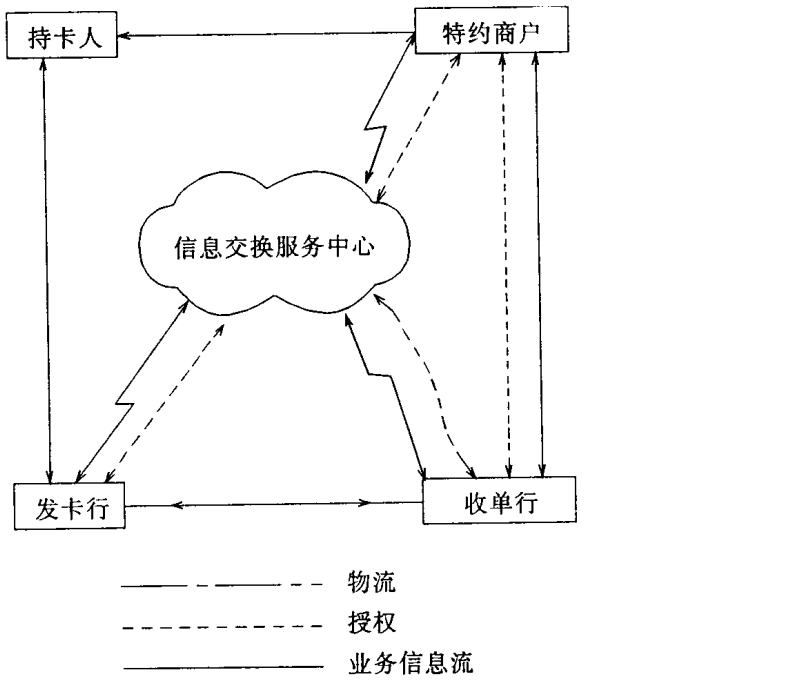

图 1-1　卡基支付业务关系图

在电子货币流通过程中,上述涉及到的系统间的关系可图示如下:

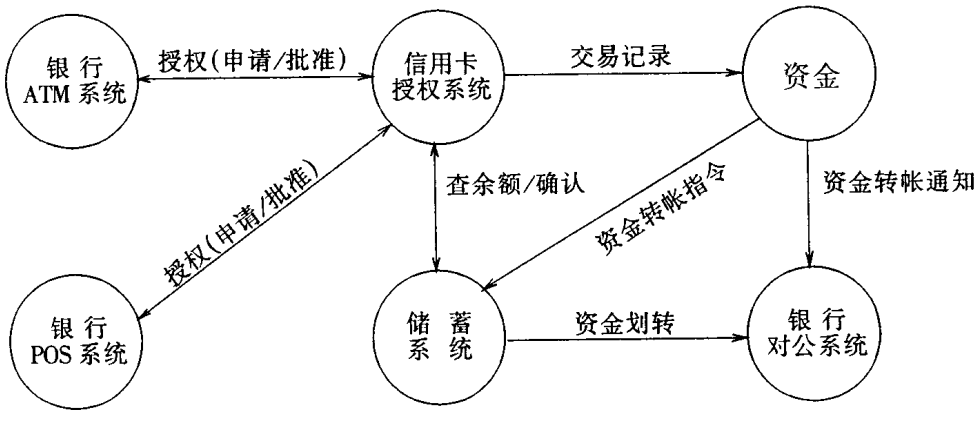

图 1-2　电子货币流通系统中各系统之间的关系

上图仅为同城消费时的示意图,有时可能涉及到异地(包括异国)和异行(开户行和收单行