智 能 卡 技 术

—IC 卡—

(第 二 版)

王爱英　主编

清 华 大 学 出 版 社

(京)新登字 158 号

内 容 简 介

智能卡是一种集成电路卡(IC card),以电子货币形式流通于市场,也可用作身份证明或健康卡。它继承了磁卡以及其他 IC 卡的所有优点,并有极高的安全、保密、防伪能力。本书对三种 IC 卡(存储器卡、逻辑加密卡和智能卡)和磁卡的物理结构、逻辑特性、实现技术和应用系统等进行了较为全面的论述,较详细地阐明了有关的国际标准、安全保密体制和读写设备(读卡器)等,并以自动柜员机 ATM 和销售点终端 POS 为重点介绍了卡的应用技术和应用系统。

本书对从事 IC 卡及其配套设备的设计、维护、制造的工程技术人员,以及从事与卡有关的应用系统的开发工作人员很有帮助。本书编写简明、易懂,因此也可作为高等院校师生以及有关工程技术人员、金融界人士的学习参考书。

版权所有,翻印必究。
本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

智能卡技术: IC 卡/王爱英主编. —2 版. —北京: 清华大学出版社, 2000
ISBN 7-302-03971-2

Ⅰ. 智… Ⅱ. 王… Ⅲ. 集成电路-磁卡片 Ⅳ. TP333.3

中国版本图书馆 CIP 数据核字(2000)第 35189 号

出版者: 清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
印刷者: 印刷厂
发行者: 新华书店总店北京发行所
开 本: 787× 1092 1/16 印张: 23.25 字数: 536 千字
版 次: 2000 年 9 月第 2 版 2000 年 9 月第 1 次印刷
书 号: ISBN 7-302-03971-2/TP・2324
印 数:
定 价: 元

序

当今世界信息技术的发展日新月异，一个以采集、开发、利用信息资源为特征的信息技术革命正席卷全球，信息技术已广泛地渗透到社会各领域，在世界经济和社会发展中发挥着越来越重要的作用。目前各个发达国家都在致力于信息化建设，在美国提出“国家信息基础设施 NII(National Information Infrastructure)计划”之后，欧共体、日本、韩国、新加坡等国家也都相继制定了信息高速公路计划、以此来加速本国经济的发展。

中国是一个发展中的国家，作为加速发展国民经济的战略举措，中国政府正在致力于国民经济信息化的建设，以“金桥”、“金卡”、“金关”、“金税”工程为代表的“金系列”工程的实施，就是中国政府为推进国民经济信息化建设所采取的重要行动。这些工程的建成，将对中国国民经济发展和社会信息化水平的提高作出积极的贡献。

利用现代信息技术来改造和装备各个部门，逐步建设一个比较发达的信息社会，对发展中国家来说，是一场全新的技术革命和社会改革，我们需要在实践中努力探索和提高。发展信息业有许多关键的要素，如计算机、通信、集成电路、软件、数据库和信息服务业的建设等。但如何将人类的社会活动和生产活动与现代化的信息系统和流通手段联系在一起也是非常重要的，只有这样才能更好地发挥人们的聪明才智，才能使人类享受到信息化带来的高度精神文明和物质文明。

传统的联系人与信息系统的手段是利用计算机键盘输入信息，或通过电子扫描仪将整篇文稿输入计算机，现在又开发出了手写体输入设备和语音输入设备等。但在金融和商贸领域内，使用得最普遍和最方便的是磁卡和 IC 卡，磁卡是利用安装在卡上的磁条来记录和读出信息，IC 卡则利用安装在卡中的集成电路(IC)来记录和传递信息。智能卡是 IC 卡家族中功能最强、安全性最高的一个成员，它将中央处理器(CPU)、存储器、连同操作系统安装在卡中。IC 卡是一种将个人信息最有效地送入到先进的全球信息网络并获取所需结果的最有效的办法，被誉为人与信息系统连接的“接口”。

“金卡工程”(即电子货币工程)是推进我国国民经济信息化的重大工程之一，它以磁卡或 IC 卡为媒介，利用邮电部、中国人民银行现有的网络资源，并通过“金桥”网构成经济信息系统，为银行、商贸和旅游等部门服务。它协助银行推广信用卡和现金卡，逐步实现现金存兑和支付的电子化；它为商贸和旅游等行业提供电子支付手段，以减少现金的流通量。随着互联网应用的日益普及，一个以电子商务为主要特征的网络经济时代即将来临，为此，各大商业银行已纷纷打算在互联网上开设电子银行，而 IC 卡将成为人们联网身份识别和实现电子支付的最好手段。此外，IC 卡还广泛应用于交通管理、医疗保险、身份证、电话付费、汽车加油付费、出租车付费等各个领域，其影响面之广是前所未有的。为此，熟

此为试读，需要完整PDF请访问：www.ertongbook.com

悉和了解智能卡及其相关设备对许多人来说都是十分重要的,“智能卡技术”一书的出版正是适应这一社会需求。它对培养和提高人们的信息化意识,推动智能卡的应用有积极意义,希望广大读者关心它、爱护它、不断提出建议,使之日趋完善,成为读者喜爱的一本技术工具书。

全国信息化技术标准委员会主任
中国软件行业协会理事长
杨天行
2000 年 4 月

前　　言

1995 年清华大学计算机科学与技术系师生在从事 IC 卡的集成电路设计和读写设备的设计制造过程中，深切感到国内这项工作尚处在起步阶段，无论是资料、设备和开发工具都很缺乏；另一方面又感到凭我们国内的计算机系统的设计制造水平和半导体工艺水平，完全能将 IC 卡及其配套设备的设计制造任务承担起来。“金卡工程”规划用 10 年左右时间，在全国 400 个城市的 3 亿人口中推广应用卡基支付系统，应用范围普及银行、商业、旅游、饭店以及各种预收费系统等，而且会永无止境地开发新的应用系统。因此，在全国将需要一大批有相应技术水平的人来从事各类卡及其配套设备和应用系统的设计、开发、制造、发行、维护和服务工作。为了适应这一需要，我们在收集资料的基础上经过消化、吸收、补充、提高，于 1996 年 1 月整理出版《智能卡技术》一书。后来用该书作为教材，为清华大学学生开了两次课，另外还向社会开办了两次培训班。

4 年过去了，IC 卡的应用无论在国外和国内都得到了前所未有的迅速发展，与此相适应的新的国际标准和国内标准不断涌现，作者通过几年的工作和学习，对 IC 卡的认识不断深入，于是萌发了修订《智能卡技术》一书的想法，在清华大学出版社的大力支持下，《智能卡技术》(第二版)终于与读者见面了。

清华大学计算机科学与技术系先后参与 IC 卡研制工作以及为本书原著出过力的研究生有张力同、孙军、陈华、汤斌浩和顾清等，现在他们都已奔赴各自工作岗位，这次修订工作主要由王爱英完成，但是没有他们的努力，原书的质量得不到保证，也就不会有第二版了。

本次修订工作除了对原书各章进行了修改和充实以外，还增加了三章，它们是非接触式集成电路(IC)卡的国际标准、IC 卡的测试标准和中国金融集成电路(IC)卡规范。这也反映了 IC 卡的发展动向，即 IC 卡从接触式向非接触式方向发展，金融卡由磁卡向 IC 卡过渡，同时随着应用的推广，测试标准也建立起来了。

由于使用 IC 卡具有流动性与全球性的特点，迫切要求实现开放性，相应的国际标准和国家标准也就显得特别重要，因此有关的标准在本书中占有大量篇幅。同时由于标准是可能修改的，例如本书第 3 章中的国际标准 ISO/ IEC 7816-3，已几经修改，这次本书按最新的版本进行了修改。

在编写本书过程中根据我们的学习、工作经验，力图全面反映智能卡技术各方面的知识、理论和实践经验，注意系统性和易读性，但由于作者知识的局限性，再加上技术发展快，又在一定程度上存在保密等原因，本书肯定会存在不少缺点，甚至错误，殷切希望领导、专家和广大读者提出宝贵意见和建议。

王爱英

写于清华园

2000 年 4 月

目　　录

前言 …… Ⅲ
第 1 章　智能卡概论 …… 1
1.1　智能卡基础知识 …… 1
1.1.1　什么是智能卡 …… 1
1.1.2　IC 卡的接口设备 …… 3
1.2　金融卡的应用基础 …… 3
1.2.1　IC 卡提供的信息 …… 3
1.2.2　举例—— 在自动柜员机上实现取款 …… 3
1.2.3　IC 卡存储区的分配和功能简介 …… 4
1.2.4　接口设备存储器内容简介 …… 4
1.2.5　使用智能卡完成一次购物的操作过程 …… 5
1.2.6　发展智能卡与人有关的因素 …… 5
1.2.7　智能卡的种类 …… 6
1.3　智能卡的安全问题 …… 6
1.3.1　影响智能卡安全的若干基本问题 …… 6
1.3.2　安全措施 …… 7
1.3.3　密钥与认证 …… 7
1.3.4　卡片的作弊问题 …… 8
1.4　识别卡的国际标准 …… 8
1.4.1　磁卡的国际标准 …… 8
1.4.2　IC 卡的国际标准 …… 9
1.5　金卡工程(电子货币工程) …… 9
1.5.1　金卡工程的总体设想 …… 9
1.5.2　银行卡基本业务需求 …… 11
1.5.3　金卡工程总体结构 …… 12
1.5.4　应用软件设计要求和设备功能 …… 16
1.5.5　安全与保密 …… 19
1.5.6　技术标准与规范 …… 20
1.6　智能卡的诞生与发展 …… 20
1.7　本书内容简介 …… 21
思考题 …… 22
第 2 章　磁卡 …… 24
2.1　概述 …… 24

2.2 金融交易卡第1磁道的格式及内容 …… 29
2.3 金融交易卡第2磁道的格式及内容 …… 30
2.4 金融交易卡第3磁道的格式及内容 …… 31
2.5 主账号格式 …… 38
2.6 金融交易内容 …… 40
2.7 磁卡存在的问题 …… 42
2.8 与磁卡有关的国际标准 …… 43
思考题 …… 44
第3章 接触式集成电路(IC)卡国际标准(一) …… 45
3.1 ISO 7816-1,接触式集成电路卡的物理特性 …… 45
3.2 ISO 7816-2,接触式集成电路卡的触点尺寸和位置 …… 46
3.3 ISO/IEC 7816-3,接触式集成电路卡的电信号和传输协议 …… 46
3.3.1 操作条件 …… 47
3.3.2 触点的电压和电流值 …… 48
3.3.3 IC卡的操作过程 …… 50
3.3.4 卡的复位 …… 51
3.3.5 异步传输的复位应答(answer to reset) …… 53
3.3.6 协议和参数选择PPS(protocol and parameters selection) …… 58
3.3.7 异步半双工字符传输协议(T=0) …… 58
3.3.8 导步半双工分组传输协议(T=1) …… 60
3.4 ISO/IEC 7816-10接触式集成电路卡(同步卡)的电信号和复位应答 …… 64
3.4.1 触点的电特性 …… 64
3.4.2 卡的复位 …… 65
3.4.3 复位应答 …… 66
3.4.4 触点的释放 …… 67
思考题 …… 67
第4章 接触式集成电路(IC)卡国际标准(二) …… 69
4.1 ISO/IEC 7816-4(行业间交换用命令)规定的范围 …… 69
4.2 数据结构 …… 69
4.2.1 文件组织 …… 69
4.2.2 数据访问(存取)方式 …… 70
4.2.3 文件控制信息(FCI) …… 72
4.3 卡的安全结构 …… 73
4.3.1 安全状态 …… 73
4.3.2 安全属性 …… 74
4.3.3 安全机制 …… 74
4.4 应用协议数据单元(APDU)的信息结构 …… 74
4.4.1 命令APDU …… 75
4.4.2 应答APDU …… 76

此为试读,需要完整PDF请访问: www.ertongbook.com

4.4.3 命令头部、数据字段和应答尾部的代码约定 …… 76
4.5 基本行业间命令 …… 81
4.6 面向传输的行业间命令 …… 98
4.7 历史字节 …… 100
4.7.1 目的和一般结构 …… 100
4.7.2 类型指示符(必有的) …… 100
4.7.3 可选的 COMPACT-TLV 对象 …… 100
4.7.4 状态信息 …… 104
4.7.5 DIR 数据访问 …… 105
4.8 与应用无关的卡服务 …… 105
4.8.1 定义和范围 …… 105
4.8.2 卡识别服务 …… 105
4.8.3 应用选择服务 …… 106
4.8.4 数据对象检索服务 …… 106
4.8.5 文件选择服务 …… 106
4.8.6 文件 I/O 服务 …… 107
4.9 ISO/IEC 7816-5 应用标识符的编号系统和注册过程 …… 108
4.9.1 定义和缩写 …… 108
4.9.2 数据单元 …… 108
4.9.3 检索 ASN.1 对象 …… 110
4.9.4 数据单元的使用 …… 111
4.9.5 标识符的注册 …… 111
4.10 ISO/IEC 7816-6/7/8 的简介 …… 113
思考题 …… 113
第 5 章 非接触式 IC 卡国际标准 …… 115
5.1 ISO/IEC 14443-1 物理特性 …… 115
5.2 ISO/IEC 14443-2 射频能量和信号接口 …… 115
5.2.1 能量传送 …… 116
5.2.2 信号接口 …… 116
5.3 ISO/IEC 2nd CD 14443-3 初始化和防冲突 …… 119
5.3.1 登记(polling) …… 119
5.3.2 Type A——初始化和防冲突 …… 120
5.3.3 Type B——初始化和防冲突 …… 129
5.4 ISO/IEC 14443-4 选择应答和传输协议 …… 137
5.4.1 激活序列 …… 137
5.4.2 协议 T= CL 半双工分组传输协议 …… 141
5.4.3 专用接口参数 …… 144
5.4.4 协议操作 …… 144

5.4.5 多卡激活 …… 144
思考题 …… 147
第 6 章 IC 卡的测试标准 …… 148
6.1 IC 卡的一般特性测试 …… 148
6.2 接触式 IC 卡的物理和电气特性的测试方法 …… 149
6.3 接口设备(IFD)物理和电气特性的测试方法 …… 151
6.4 接触式 IC 卡逻辑操作的测试方法 …… 152
6.5 接口设备(IFD)逻辑操作的测试方法 …… 153
6.6 非接触式 IC 卡的测试方法 …… 154
6.6.1 静电测试 …… 154
6.6.2 功能测试 …… 155
思考题 …… 159
第 7 章 智能卡的安全和鉴别 …… 161
7.1 对智能卡安全的威胁 …… 161
7.2 物理安全 …… 161
7.3 逻辑安全 …… 162
7.3.1 用户鉴别 …… 162
7.3.2 存储区域保护 …… 164
7.3.3 智能卡的通信安全与保密 …… 165
7.4 密码技术 …… 167
7.4.1 对称密码体制 …… 169
7.4.2 非对称密码体制 …… 177
7.4.3 密钥管理 …… 181
7.5 智能卡的安全使用 …… 182
思考题 …… 184
第 8 章 IC 卡及其专用芯片 …… 185
8.1 IC 卡的存储器芯片 …… 185
8.2 IC 卡的逻辑加密芯片(接触式 IC 卡) …… 192
8.2.1 名词解释 …… 192
8.2.2 功能框图 …… 193
8.2.3 芯片内部存储区域分配(举例) …… 194
8.2.4 ATMEL 公司的逻辑加密卡芯片 …… 195
8.2.5 Siemens 公司的逻辑加密卡芯片 …… 202
8.2.6 几种典型电路分析 …… 209
8.3 非接触式 IC 卡 Mifare …… 211
8.3.1 Mifare standard …… 212
8.3.2 Mifare Pro …… 217
8.4 智能卡的硬件环境和芯片 …… 217

8.5 智能卡的操作系统——COS …… 220
8.5.1 COS 概述 …… 220
8.5.2 COS 的体系结构 …… 221
8.5.3 COS 的命令系统 …… 227
8.6 智能卡举例(MC68HC05SC 系列) …… 231
8.7 Java 智能卡(Java card) …… 239
8.7.1 Java 语言及简单程序举例 …… 239
8.7.2 Java 虚拟机 …… 240
8.7.3 Java 智能卡的应用程序 …… 242
思考题 …… 249
第 9 章 IC 卡接口设备技术 …… 250
9.1 IC 卡接口设备的组成 …… 250
9.2 IC 卡适配插座(IC 卡座) …… 251
9.2.1 IC 卡适配插座的结构形式 …… 251
9.2.2 选择 IC 卡适配插座时的几个重要的指标 …… 252
9.3 IC 卡的接口电路和读写控制 …… 252
9.3.1 接触式 IC 卡的接口电路 …… 252
9.3.2 接触式 IC 卡的控制与读写技术 …… 254
9.3.3 非接触式 IC 卡读写机具的现状 …… 262
9.4 IC 卡的应用设备 …… 263
9.4.1 专用的 IC 卡应用设备 …… 264
9.4.2 通用型 IC 卡应用设备 …… 266
9.5 读写器(接口设备)规范 …… 267
9.5.1 《集成电路(IC)卡读写机通用规范》(送批稿)简介 …… 267
9.5.2 《接口设备基本应用编程接口规范(暂定名)》(讨论稿)简介 …… 268
思考题 …… 269
第 10 章 中国金融集成电路(IC)卡规范 …… 271
10.1 机电接口 …… 271
10.2 卡片操作过程 …… 272
10.3 字符的物理传送 …… 272
10.4 复位应答 …… 273
10.5 传输协议 …… 274
10.5.1 物理层 …… 274
10.5.2 数据链路层 …… 274
10.5.3 传输层 …… 275
10.5.4 应用层 …… 276
10.6 数据元和命令 …… 277
10.6.1 文件 …… 277

10.6.2 命令 …… 277
10.7 应用选择 …… 279
10.7.1 应用标识符(AID)的编码 …… 280
10.7.2 支付系统环境(PSE)结构 …… 280
10.7.3 支付系统的目录编码 …… 280
10.7.4 终端的应用选择 …… 280
10.8 安全机制 …… 281
10.8.1 基本安全要求 …… 281
10.8.2 安全报文传送 …… 281
10.8.3 过程密钥的产生 …… 283
10.8.4 认可的加密算法 …… 283
10.9 电子存折/电子钱包(ED/EP)应用 …… 284
10.9.1 文件 …… 284
10.9.2 命令 …… 284
10.9.3 安全 …… 288
10.9.4 终端 …… 289
10.9.5 交易流程 …… 289
10.9.6 防拔 …… 295
10.10 磁条卡功能 …… 295
附录 10.A 数据元解释 …… 297
附录 10.B ED/EP 应用的密钥关系 …… 298
附录 10.C ED/EP 应用的基本数据文件(EF) …… 300
思考题 …… 301
第 11 章 自动柜员机 ATM 和销售点终端 POS …… 302
11.1 ATM 的功能和结构 …… 302
11.1.1 ATM 的硬件构成 …… 302
11.1.2 ATM 的软件 …… 306
11.1.3 ATM 的机械结构 …… 307
11.1.4 ATM 应用流程 …… 308
11.1.5 ATM 应用现状与前景 …… 309
11.2 POS 和 POS 系统 …… 309
11.2.1 POS 结构和功能 …… 309
11.2.2 POS 终端的三种类型 …… 310
11.2.3 POS 系统的构成与应用 …… 311
思考题 …… 313
第 12 章 IC 卡应用技术 …… 314
12.1 IC 卡的应用概况与技术优势 …… 314
12.2 IC 卡的应用模式与特点 …… 315

此为试读,需要完整PDF请访问: www.ertongbook.com

12.3 IC 卡的应用领域 …… 317
12.3.1 IC 卡在金融领域的应用 …… 317
12.3.2 IC 卡在非金融领域的应用 …… 320
12.3.3 一卡多用 …… 323
12.4 IC 卡应用系统的开发 …… 324
12.5 IC 卡应用系统的安全性和可靠性 …… 327
思考题 …… 328
附录 A 有关识别卡的国际组织及识别卡标准 …… 329
附录 B 集成电路卡注册管理办法 …… 333
附录 C T= 0 的 APDU 传输 …… 336
附录 D T= 1 的 APDU 传输 …… 342
附录 E RSA 密码算法的实现 …… 345
附录 F 智能卡的设计、制造、个人化和发行 …… 350
附录 G 英文缩写词 …… 355
参考文献 …… 358

第 1 章　智 能 卡 概 论

1.1　智能卡基础知识

1.1.1　什么是智能卡

智能卡的名称来源于英文名词“smart card”，又称集成电路卡，即 IC 卡(integrated circuit card)。它将一个集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似。

IC 卡的概念是 20 世纪 70 年代初提出来的，法国布尔(BULL)公司于 1976 年首先创造出 IC 卡产品，并将这项技术应用到金融、交通、医疗、身份证明等多个行业，它将微电子技术和计算机技术结合在一起，提高了人们生活和工作的现代化程度。

IC 卡芯片具有写入数据和存储数据的能力，IC 卡存储器中的内容根据需要可以有条件地供外部读取，或供内部信息处理和判定之用。根据卡中所镶嵌的集成电路的不同可以分成以下三类：

1. 存储器卡　卡中的集成电路为 EEPROM(可用电擦除的可编程只读存储器，也可写作 E^2PROM。)

2. 逻辑加密卡　卡中的集成电路具有加密逻辑和 EEPROM。

3. CPU 卡　卡中的集成电路包括中央处理器 CPU、E^2PROM、随机存储器 RAM 以及固化在只读存储器 ROM 中的片内操作系统 COS(chip operating system)。

另外还有一种 ASIC(专用集成电路)卡，它是在逻辑加密卡基础上增加一些专用电路，例如完成加密/解密运算的电路等，但由于卡内设有 CPU，所以完成的功能是固定的，没有灵活性。在本书中对这种芯片没有进行专门讨论，因为在讨论了前面三种卡以后，ASIC 卡的结构与功能也就明确了。

严格地讲，只有 CPU 卡才是真正的智能卡，但在本书中，为了论述全面，更为了应用的需要，我们将研究讨论上述三种 IC 卡。

按应用领域来分，IC 卡有金融卡和非金融卡两种。金融卡又有信用卡(credit card)和现金卡(debit card)等。信用卡主要由银行发行和管理，持卡人用它作为消费时的支付工具，可以使用预先设定的透支限额资金。现金卡又称储蓄卡，可用作电子存折和电子钱包，不允许透支。非金融卡往往出现在各种事物管理、安全管理场所，如身份证明、健康记录和职工考勤等。另外一些预付费卡，例如用于公交系统中的交通卡和电表上的 IC 卡等，各由相应的管理单位发行(当然也可委托银行收费)。这种卡兼有一部分电子钱包的功能，在本书中我们仍将它列为非金融卡。

按卡与外界数据传送的形式来分，有接触式 IC 卡和非接触式 IC 卡两种。当前使用广泛的是接触式 IC 卡，在这种卡片上，IC 芯片有 8 个触点可与外界接触。非接触式 IC 卡的集成电路不向外引出触点，因此它除了包含前述三种 IC 卡的电路外，还带有射频收发电

路及其相关电路。非接触式卡出现较晚,但由于它具有一些接触式 IC 卡所不能替代的优点,因此在某些应用领域发展很快。

在 IC 卡推出之前,从世界范围来看,磁卡已得到广泛应用,为了从磁卡平稳过渡到 IC 卡,也是为了兼容,在 IC 卡上仍保留磁卡原有的功能,也就是说在 IC 卡上仍贴有磁条,因此 IC 卡也可同时作为磁卡使用,图 1.1 为 IC 卡的外观图,正面中左侧的小方块中有 8 个触点,其下面为凸型字符,背面有磁条。正面还可印刷各种图案,甚至人像。卡的尺寸、触点的位置与用途、磁条的位置及数据格式等均有相应的国际标准予以明确规定。

图 1.1　IC 卡的外观图

图 1.2　IC 卡应用过程

无论是磁卡还是IC卡,卡上都有唯一的发行人和持卡人的识别标志,这种卡称为“识别卡”。

1.1.2 IC卡的接口设备

为了使用卡片,还需要有与IC卡配合工作的接口设备IFD(inter face device),或称为“读写设备/读写器”。IFD可以是一个由微处理器、键盘、显示器与I/O接口组成的独立设备,该接口设备通过IC卡上的8个触点向IC卡提供电源并与IC卡相互交换信息。IFD也可以是一个简单的接口电路,IC卡通过该电路与通用微机相连接。无论是磁卡或IC卡,在卡上能存储的信息总是有限的,因此大部分信息需要存放在接口设备或计算机中。当用信用卡购物时,如在允许透支范围内,则可以先取走商品,事后再结算;如需一笔大款,则需经银行确认,授权于商店后,才能取走商品。由于银行、发放信用卡的公司以及商店不在同一处,因此需要经过通信线路和计算机(主机)联系才能实现上述过程。

图1.2(右半部)示出使用信用卡购物的过程,图1.2(左半部)是在ATM(自动柜员机)上自动取款(稍后说明)。

为了快速而又可靠地进行处理,计算机网络与通信线路的安全与响应时间是关键。

1.2 金融卡的应用基础

IC卡主要用作金融卡,金融卡的主要功能是存储数据和处理数据。

1.2.1 IC卡提供的信息

1. 印在卡上的可供人阅读的信息　用以标识卡发行人的标志、使用期限、客户姓名、账号和签名等,这些信息是卡能作为金融交易中的支付工具的基础。

2. 机器可读数据　卡上的凸出字符用于压印账单,以便向售货商和客户提供交易凭证。卡上还可提供金融交易的账目。

3. 提供机器可读的授权信息和数据收集系统的标识符。

1.2.2 举例——在自动柜员机上实现取款

下面以自动柜员机ATM为例进行说明。

自动柜员机是放在银行或商店大堂中供客户自动提款的机器(有的ATM还有自动存款功能)。执行从ATM提取现金的操作仅需十几秒钟,总共只需要做出4个输入动作:

1. 插入金融卡;
2. 输入个人标识码(PIN);
3. 选择交易类型(取款);
4. 给出申请提取的金额。

当ATM判别没有问题时,自动输出卡和现金,并打印凭证。由此可见,ATM是一种操作方便的信息处理系统,可以24小时提供服务。

ATM 是安装在柜里的计算机系统,它要处理卡片、货币、收据和信封(存款用)四种介质,并能与相连接的远程计算机相互通信。它的内部有严密的可靠的物理和逻辑安全措施。它的每一笔交易通常接受正确的授权和严格的控制,因此 ATM 系统既是一个操作简单的系统,又是一个构造复杂的系统。由于历史原因,目前 ATM 主要使用磁卡。

ATM 将磁条上(对磁卡)的数据,诸如发行人和客户账号识别码(用来获取自动授权信息的基础)通过通信线路与发卡单位的计算机及其账户数据库相连,用以检查金融卡的编号(查对黑名单),以防止他人使用已挂失的或偷窃来的金融卡,同时核对客户的账面记录,以查明可供支用的金额,并根据交易的金额随即更新账面记录,供金融卡下次使用。此外,为了避免某些可能发生的弊端(如已挂失但尚未列入黑名单),还要限制金融卡在一天内允许使用的次数和一天内允许提取现金的总金额。

绝大多数 ATM 机取款时还需输入个人标识符 PIN,并将 PIN 送到计算机,用来核对持卡人是否是卡的主人。如在通信线路上明文传送 PIN,存在被窃听的危险,为此有时需对 PIN 进行加密,这就要提供一个加密算法和“密钥”,让经过加密后的 PIN 在通信线路上传送,在接收端解密,因此在接收端提出了密钥的管理和保护的要求(参考第 7 章)。

1.2.3 IC 卡存储区的分配和功能简介

IC 卡的存储量比磁卡大得多,一般分四个存储区:

1. 公开的(不保密的)存储区　内含公用信息,诸如发行标识符、持卡人的账号等。

2. 外部不可读的存储区　存储的内容是供内部决策用的,如 PIN 值,该值是在卡片发行时进行个人化处理写入的,用户在输入正确的 PIN 值后,允许输入新 PIN 值进行修改,但在任何情况下,都不允许将存储在卡中的 PIN 值向外界传送。在本存储区内还可能存放密钥。

3. 保密存储区　内含账面余额、允许卡使用的服务类型及限额等。当持卡人输入正确的 PIN 值后,允许读取本存储区数据,进行交易,并根据应用情况写入正确数据(如修改余额)。

4. 记录区　内含每次交易细节,称为“日志”,可供查询。

除了存储器卡外,在其他 IC 卡中还有逻辑电路或微处理器,提供安全可靠的服务。

1.2.4 接口设备存储器内容简介

与智能卡配合使用的接口设备(或称为读写设备、读卡器)应该提供附加的存储器和逻辑电路,它本身可能就是一台微机。

用于商店中的接口设备的存储器中包含如下内容:

1. 交易数据　内含每次交易记录,一般于每天晚上将当天交易细节汇总后传送到开户银行或发卡银行,供转账和清算之用。银行应保证及时将应付款存入售货商账户。

2. 非法卡表(或称为黑名单、止付名单)　列出所有挂失、被窃或透支超过限额的账户清单,在每天向银行递交交易细节时,也递交此清单。同时银行经汇总后,应将修改后的黑名单提供给售货商。凡登在黑名单上的账户或透支超额的账户要进行交易时,须由售货商通过网络或用专用电话和银行进一步授权核实后,方可受理。也可拒绝处理,甚至可根

据实际情况将卡没收。

3. 保密数据　密钥和授权电话号码即属于保密数据,密钥用以生成校验码以防交易日志被修改。至于授权电话,在售货商希望成交某些超额交易时,用它接通用户银行,经银行授权后方可受理,如果电话通信线路很忙,那么等待授权的时间可能很长,甚至能让客户觉得无法容忍,这就会影响到金融卡的推广应用。较先进的系统应靠计算机网络和通信线路来完成授权功能。

1.2.5　使用智能卡完成一次购物的操作过程

操作顺序如下:

1. 客户拿着金融卡和购买的商品(或付款单)来到付款处。并将金融卡插入能输入PIN的小键盘设备中。

2. 售货员通过他本人工作的键盘输入交易金额。

3. 交易金融显示在小键盘设备的显示板上。

4. 客户在小键盘上按下某个指定键,表示对交易金额的认可。

5. 小键盘设备的显示板上指示客户输入PIN。然后客户输入PIN。输入后自动与卡中的PIN比较,如一致,就将金融卡自身打开,准备受理交易。

6. 接着接口设备内部进行一连串处理,如查对黑名单、核实资金是否够用、计算交易后的余额,将它登入交易日志记录里并计算出安全校验码加在日志记录中以保证数据的安全。同时把这笔交易记录也写到金融卡中,最后给客户打印收据。

7. 显示板指示交易结束,客户取走商品和卡。

1.2.6　发展智能卡与人有关的因素

参与智能卡操作的相关方面有:持卡人或用户,商店,卡片的发行者及销售部门,卡片的设计者、出售商及安全维护。

1. 持卡人或用户

用户要求:

(1) 使用方便:装置的地点、使用的时间和操作的步骤等力求方便。操作一学就会。

(2) 启用手续简易:发行和基于PIN号的卡片个人化处理手续简易。

(3) 加快交易时间:进行一次交易或授权等待时间尽量缩短。

(4) 安全可靠:每次交易正确无误,操作错误后的重新启动方便可靠,卡片的丢失、被窃和PIN值的更换等容易处理。

(5) 清楚简单的操作提示:卡片上清楚表明接口方向,显示屏幕清楚易读,避免使用计算机术语和复杂的交互式操作。

2. 商店

商店期望:

(1) 人员培养容易,操作过程和例外处理简单。

(2) 故障处理简单:故障处理包括出错后的重新启动、例外情况或交易被拒绝时的处理,以及在正常的解决办法失灵时,其他可供选择的措施。

此为试读,需要完整PDF请访问: www.ertongbook.com