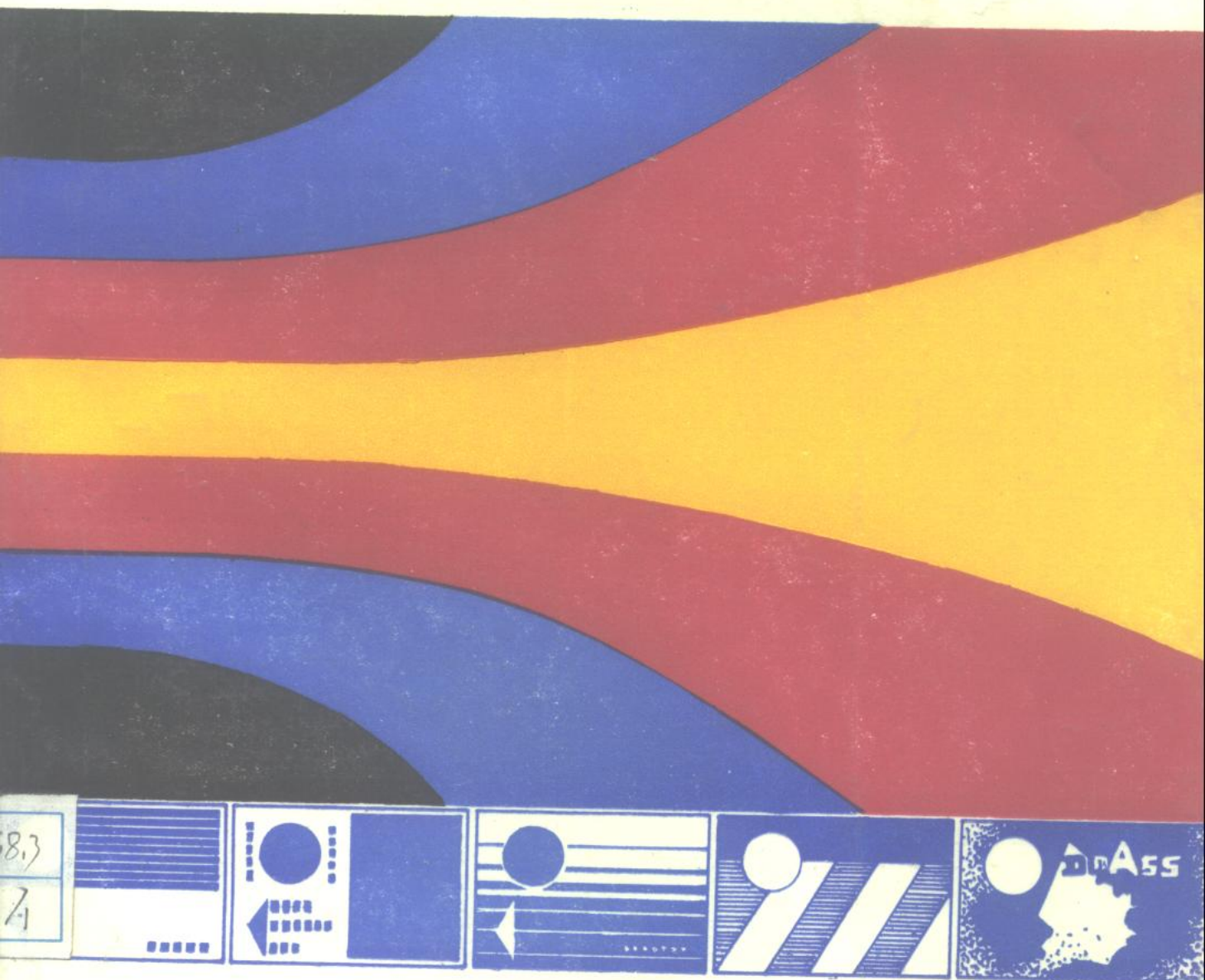
智能卡

最终的个人计算机

〔美〕 J.斯威格尔兹 著
中国工商银行科技部《智能卡》编译组 译



58.3
Z1

電子工業出版社

TP368.2
S107

智能卡

最终的个人计算机

〔美〕 J.斯威格尔兹 著

中国工商银行科技部《智能卡》编译组 译

电子工业出版社

021332

内 容 简 介

本书系统地介绍了金融交易卡从传统的冲压凸形字符的磁条卡到智能卡的发展过程，全面地讨论了智能卡的类型、构造、设计、标准、系统连接、测试及其各种应用，还分析了智能卡会给社会带来的影响及智能卡的安全防护问题。

全书共分十六章：第一章为概论；第二、三章对金融交易卡作了一般介绍；第四、五、六、七、八章讨论了智能金融交易卡的设计、构造、应用、系统连接和现场测试情况，其中对智能卡交易起保证作用的信息协议作了专门的叙述；第九章给出了智能卡设计中应考虑的人的因素；第十、十一章讨论了智能卡的安全及其防护措施；第十二章是对智能卡的经济因素的分析；第十三章介绍了其它有关的卡片技术；第十四章给出了智能卡的标准；第十五、十六章分析讨论了智能卡的发展策略和对社会带来的影响；最后是有关名词、术语解释的附录。

本书可供从事金融业务、银行电子化和信息处理工作的广大科技和管理人员使用，也可供有关专业的大专院校、中专学校的师生参考。

JS402/25

Jerome Svigals
SMART CARDS
The Ultimate Personal Computer
Macmillan Publishing Company, 1985
智能卡　最终的个人计算机
J. 斯威格尔兹　著
中国工商银行科技部《智能卡》编译组　译
责任编辑　吴明卒
电子工业出版社出版　（北京市万寿路）
电子工业出版社发行　各地新华书店经销
人民卫生出版社印刷厂印刷
*
开本：787×1092毫米 1/16 印张：8.75字数：221千字
1990年11月第1版　1990年11月第1次印刷
印数：4000册　　定价：6.20元
ISBN7-5053-1063-1/TP·176

译 者 的 话

近30年来，在金融领域内，随着电子技术的不断进步，自动柜员机（ATM）已越来越普及，金融交易卡(一种可存储数据的塑料磁卡)的使用已深入到社会的各个阶层，使人们的经济活动方式发生了很大的变化。在金融行业的带动下，这种塑料磁卡技术已在销售、保安、通信和交通等行业得到了广泛的应用。小小的卡片对人们的生活产生了重大的影响。尤其是近十年来，随着超大规模集成电路和大容量存储芯片的出现和应用，人们开始考虑塑料磁卡的换代产品——智能卡（Smart Card）的研制、生产、应用和标准化等有关方面的问题。我们相信，智能卡技术的应用将对促进人类未来的消费方式的进步起着巨大的推动作用。

今天，在发达的资本主义国家中，智能卡技术的发展已得到了广泛的重视。那么，什么是智能卡？它有哪些技术要求和用途？它将在哪些领域内使用？尤其是对金融行业的发展有何重大的影响？等等，就是这本书要回答的问题。为了使更多的人能很快地了解这方面的内容，我们翻译了这本书。对于广大的金融工作者来说，应该特别关注先进的电子技术对金融行业的变革带来的影响。《智能卡》一书值得广大金融工作者一读。

为了尽快地将这本书与同志们见面，我们组织了编译组，负责该书的翻译和出版工作。参加翻译工作的有朱宏岳、单怀光、陈天晴、章鸿猷和吴晓东等五位同志，其中朱宏岳同志对全书进行了总纂和审校。在审校过程中，杭州金融管理干部学院的奚利强和范乃敏同志在译稿的誊写和制图方面做了大量的工作。在此，特向对本书的出版给过帮助和支持的所有同志表示衷心的感谢。

由于时间仓促和我们的水平所限，书中一定存在不少的缺点和错误，切望读者批评指正。

《智能卡》编译组

一九九〇年五月六日

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

早期的动力设备

工业革命的兴起是以一些大型的、中心动力工厂为基础的。首先是采用水轮机，它通过一组转轴与皮带来传送动力。水轮机作为一种能源后来被蒸汽机所代替，蒸汽机又被电动机所代替。不管怎么样，它们都采用了类似的、以大型集中的能源来传送物理能的方法。

如大多数技术一样，动力的发展促进了经济的繁荣。老式的挂钟发展为精巧的手表，羽毛笔进化为圆珠笔，畜力驱动发展成小型能源，最终出现了小功率的电动机，这大大加速了工业生产率的提高。小功率电动机在历史上第一次能既容易又经济地满足人们对能量的需要。电动机可到处安装且能够提供各种特定应用所需要的功率。到二次大战时，小功率电动机的功能及其经济性已发展到能满足广泛的家庭使用的水平。今天，在一般中等经济收入的家庭内约使用着不少于100台电动机，例如钟表、冰箱、空调设备、加热器、洗衣机、烘干机、缝纫机、真空吸尘器、恒温箱等都离不开电动机。

对于信息处理系统来说，在很大程度上正在经历着相类似的发展过程。第二次世界大战后不久，推出了以真空管为基础的、体积庞大的数字计算机系统。由于技术发展非常迅速，从真空管到晶体管直到制成现代大型计算机系统用的集成电路芯片，仅仅用了不到20年的时间。随着数字技术的发展，开始生产一种“小功率”的计算机。技术发展是如此之快，今天已经处于单片式微型计算机的时代了。

芯片

什么是集成电路芯片呢？它是用电化学的方法把高密度的电子线路“刻”在硅基片上的一种电子组件。最近30年来的技术发展，使芯片上的电子线路集成密度骤增到令人难以置信的程度。事实上，1950年最早的电子数字计算机的体积竟是今天单片微机的200万倍（1000平方英尺比1¼平方英寸）。而且这种单片微机比起原始的电子管计算机来，其运算速度更快，容量更大，使用也更为灵活方便。

在现代化的家庭内，使用基于芯片的微处理机大约有20到30个左右。它们被安装在微波炉、手提式半导体、收音机、电视机、音响设备及家用汽车等设备中。正如小功率电动机在40年前为人口的激增作出能量的准备一样，今天的集成电路芯片也在作类似的准备。本书要讨论的是20年中人们会遇到的部分事情，它是一本研究关于芯片对我们日常生活所起的重要作用的教程。书中讨论并预测了单片微机的安装方法、个人化处理、如何根据不同的用户需要进行裁剪以及如何被大众所接受和使用等问题。

现在已经有不少产品将一些单片微机芯片组装成体积很小的计算机（个人计算机）。然而，历史表明所有伟大的发明创造都要经历一个初级阶段。新技术往往首先被用来替代老的技术，例如用火车和汽车来替代马匹。当今的个人计算机是一个最新的例子，它

此为试读，需要完整PDF请访问：www.ertongbook.com

表明了两个过渡性的概念。第一个是：要想有效地使用信息处理机，必须掌握计算机语言及程序设计知识。第二个是：培训信息处理设备的用户的最好方法是把他们当作键盘和计算机接口语言的操作员来训练。目前出售的个人计算机是以这些概念为基础的，它不能促进信息处理功能的广泛而普遍的应用。试想假如现代的电视机需要用户象使用目前的个人计算机那样复杂的操作的话，那么电视机还能达到今天普及使用的水平吗？

技术改变了我们的生活

幸运的是，我们现在已经有了一些更为成熟的新技术的例子。这些例子证明了人类与技术之间的界面被简化为允许在日常生活中直接使用时，这种新技术就将改变我们的生活方式。汽车就是一个很好的例子，今天的汽车导致了购物中心和超级市场的产生。它们的开设建立在家庭汽车的机动性的基础上。大家知道，驾驶家庭汽车并不需要理解内燃机的原理或汽化器的正确工作顺序。同样，自动柜员机（ATM）使安装在一个“箱子”内的计算机系统得到了公众普遍的使用。自动柜员机正在改变我们的生活方式，它能为社会提供每日24小时和每周七天的银行服务。这个例子又一次说明尖端技术只有在未受过专门训练的普通公众都能使用时，才能得到社会广泛的承认。

上述两个例子说明，产品和服务的开发者应掌握一个基本的目标。即不具备新技术知识的人要有能力去使用这种新技术。本书认为被称为智能卡的单片微型机的应用也具有相同的性质。书中将阐述智能卡的封装、在经济领域中的应用以及一些必要的用户操作技能。成功的开发和对各种因素的有效利用将对在日常生活中更好地使用各种类型的单片微机智能卡作出贡献。

芯片及其未来的发展

未来的基于芯片的设备，它的集成密度将更高、成本更低、功能更强且适应性更灵活。然而，我们如何去进一步丰富未来的基于芯片的信息处理功能呢？有趣的是，芯片的繁荣是在下列各方面十分短缺的时期出现的，它们是能量、政府费用、就业机会、空余时期、教育投资等的短缺以及第三世界经济增长缓慢和生产水平的低下。微机芯片的大量生产和广泛应用将对上述诸问题产生显著的影响。在描述了未来的智能卡——最基本的个人计算机之后，将讨论它对社会产生的影响。

智能卡不仅仅作为金融支付的工具。智能卡的许多概念是出自近20年来银行业务的电子化及自动服务化的发展。这些新的银行设备的成功引进及顾客的接受使用就好象是一个重要的课堂。银行家和设备研制专家对自动柜员机的用户如何使用这种机器作了细微的考察，他们花了大量的时间致力于产品的改进和市场的开拓，并从中获得了多年的发展经验。本书中采用的一些概念还受益于许多富有创新精神的智能卡发明者十多年来的研究成果。在此，我谨向他们表示衷心的感谢。

我还要特别感谢斯坦夫·维斯坦博士对本书的审查、建议及作出的许多贡献。他是美国运通公司（AEC）的首席科学家。维斯坦博士1984年2月在IEEE的《频谱(spectrum)》杂志上也是制定集成电路（智能）卡的新国际标准的主要参加者之一。

J·斯威格尔兹

第一章 概 论

1.1 什么是智能卡？

智能卡由一个或多个集成电路芯片所组成，并封装成便于人们携带的形式。它可以是带有内部集成电路芯片的银行卡，也可以是士兵身分标志牌的替代物。智能卡可以有任何的形状、大小和厚度，以方便使用者的携带、插入、取回以及与设备的连接。智能卡所采用的封装可从最简单的单张卡片变化到具有自己的键盘、显示器、电源和通信接口的工作站。事实上，它可能是一种具有适当的微芯片以实现智能卡功能的袖珍式计算机。

智能卡芯片具有多种功能，其中可包括遵循指令的执行作逻辑选择以及跟随不同的判定路线等逻辑功能，还有用于识别和响应外部提供的信息的逻辑。逻辑处理可在芯片内部执行，或者从外部向智能卡提供逻辑处理的结果。芯片可以是通用的，也可以是专门设计的。它可包含完整的微处理器，也可能是加密器那样的特殊处理用的芯片。简言之，在智能卡内可以使用任何为单片微机技术开发的逻辑功能。

智能卡芯片具有暂时的或永久的数据存储能力。智能卡存储器中的内容可以供外部读取，或供内部信息处理和判定之用。芯片中还可具有可破坏的或不可逆的以及可变的记录项或存储线路。例如，有的存储器当数据写入存储区后，写入线路随即被破坏（可以利用烧断所连接的熔丝来实现）。这将防止已写入数据的改变。智能卡也可设计成能有选择地破坏所存的数据。例如，在使用预付款的、可多次使用的电话卡来通电话时，每打通一次电话就消耗掉卡中的一个增量单位，就是利用了这种功能。

1.2 为什么需要智能卡？

集成电路芯片的功能和容量在不断地快速增长，其进展情况可估计如下：

年	每平方英寸芯片上的密度（元件个数）
1970	10,000
1980	150,000
1990	1,000,000
2000	2,000,000～4,000,000

芯片成本也在大幅度地下降。对功能或容量相等的芯片来说，其成本差不多每年下降20%到40%。用塑料封装芯片、芯片制造工艺的更新、功能与集成密度之间的综合，这一切都在快速地发展着（第十二章中将进一步讨论智能卡的价格变化）。卡片功能和芯片功能的结合打开了一个广阔的新市场，它的发展取决于智能卡的经济而又富有生命力的开发应用。单片微机的市场销售量正在成为信息处理工业的主要经济因素。这些芯片不仅包含逻辑功能也具有存储能力。表1·1为各种计算机产品的美元销售量。表中预测，到1995年，微型计算机的销售量将增加到3130亿美元总销售量的55%。

到80年代后期，单片微机将是计算机产品中的主要形式。当整个计算机工业增加24倍时，将会发生这种局面。单片微机占领市场的时间取决于芯片能够处理的信息宽度。此宽度以比特（bit）数（信息的位，其值为0或1）来量度。

表 1·1

年　份	总销售额（十亿美元	主机系统（%）	小型机(%)	微型机(%)	其　它
1975	13	83	10	0	7
1980	29	60	17	6	17
1985	63	36	21	20	23
1990	141	17	21	37	25
1995	313	6	16	55	23

推出年代	单片微机（以比特表示的信息宽度）
1978	16
1985	32
1992	64

单片微机将如何封装？大部分的单片微机将被安装在其它产品中，它们的功能能否为最大多数的用户所利用？这个问题是智能卡能否推广的焦点。回答是肯定的，但需要给出适当的封装、应用和使用的方法。现在，从电子手表到袖珍计算器的一般应用中，经济地封装芯片的能力已经得到证实。这些芯片的应用是预先精细地设计好的，虽然是多功能的，公众已乐于接受这种芯片应用的技术。那么，芯片更普遍的应用是什么样的呢？

1.3 发展智能卡的机会

发展智能卡的大好机会取决于能否把每一张智能卡的功能充分地开发出来，使它适用于一个特定的应用环境。智能卡比传统的计算机要便宜得多，使用起来也更为方便。除了外部设备之外，芯片的信息处理能力正在接近与完整的个人计算机相匹配的水平。关键的差别在于智能卡采用专门设计的芯片，而个人计算机则是通用的。专用芯片的设计与通用芯片的主要差别在于它允许压缩所需的逻辑线路和存储量、简化用户的交互操作、以及加快智能卡的响应速度。（后面还要介绍一些重要的差别）。因此，有了适当的应用和使用方法，采用智能卡是比较经济的。每一种智能卡当与适当的信息处理设备一道使用时，在经济上可与通用个人计算机或工作站及其所分摊到的资源支持和专用线路成本相竞争。每张智能卡的成本仅为数美元，却可包含与完整地设计的专用信息处理和应用系统相等效的功能。

那么，由一片或数片芯片组成的智能卡是否已具备个人计算机的全部能力了呢？不是的，它所具有的是能提供管理、控制以及与相连接的设备或系统进行交互操作的软件。通过对预先建立好的特定应用程序及系统响应的剪裁，用户携带的智能卡仅需最少的附加选择项或变量就能完成全部操作。因此，无论芯片是如何复杂，对用户的使用来说，却是非常简单的，磁条银行卡就是一个很好的例子。它控制着自动柜员机（ATM）的全部复杂动作，而不需要用户了解机器内部的工作原理。

对于广大群众来说，使用智能卡要比个人计算机方便得多。它没有一字一键的键盘，不需要计算机语言或过程，不需要编写程序，更无复杂的显示器交互操作，甚至连程序

的装入和存取过程也无需知道。智能卡将能达到象电视机那样被人们普遍接受和乐于使用的水平，很可能达到与直拨电话系统一样普遍使用的程度。事实上，智能卡和电话、电视联合起来，将会发现最重要的应用，且前途无量。

1.4 为什么智能卡更好?

目前，基于磁带和冲压凸形字符的塑料卡系统还存在着不少局限性。它们的存储容量有限；它们又是静态的，即内部没有对数据内容的安全控制或对读出、修改内容进行控制的逻辑线路。磁条所需的读取技术，主要是顺序的和机械性的。对智能卡来说，它将具有更大的存储容量、更严密的控制、更方便的连接方法以及对集成电路芯片内容直接用电子化方法读出的手段。这些问题将在以后的章节中再作深入的讨论。

1.5 使用智能卡的社会

试想象我们已经生活在一个智能卡的社会之中，每个人都有好几张智能卡，它们可以属于下面表中的任意类型。

智能卡类型	发行者
金融服务卡	金融机构
医疗病历和服务卡（可从你的医生那里得到健康状况的报告）	医疗保险机构
政府工作部门标识卡(例如相应部门颁发的许可证)	地方，州和国家政府
通信服务卡	通信服务公司
旅行服务卡	旅行服务公司
职业通行证	雇主
军事技能训练卡	军队
电子诊断卡	电子设备卖主
汽车公路通行卡	汽车协会
工作站个人化专用卡	雇主、计算机服务公司、终端和电缆服务公司
软件装入和保护卡	软件开发者或卖主

1.6 信息协议

每一类智能卡都是由一个“可以标识”的机构发行的，它具有国家注册机构指定的标识码。每张卡内具有标准的数据内容或称为信息协议。

信息协议提供如下的应用交易功能：

对卡片发行人和持有人的标识进行核对。

启动卡片持有者的个人标识号（PIN）输入卡片。

设置卡片持有者可使用的服务类别及其限制金额。

建立卡片的控制日期：启用日期、允许重新使用的日期和停止使用的日期。

记录访问用的参考信息，例如电话和通信网络的访问地址。

在内部交易日志中记录智能卡的使用细节。

建立个人数据库，例如财务数据和存取码。

信息协议是推广使用智能卡的基础。举例来说，假定每个电话或与电话有关的设备（例如，可视图文终端（videotex）、电子电话号码簿、本地到长途数据传输的入口设备）都有智能卡的接口和信息协议逻辑，则作为一个智能卡的用户，就可以走向任何地方的任何设备，实现范围广泛的、基于智能卡的各种活动。在智能卡社会中，许多地方

都设置有卡片的接口或供卡片插入的选件。这种接口和许多信息设备是装在一起的，例如：电话机、电视机、可视图文接收机、零售商店的结帐机、饭店登记台、出租汽车服务台、医生门诊台、家用汽车、电子邮件接收机、家庭饮食设备、卫星广播解码器、办公楼前厅中的证券市场交易机以及家庭中的电子期刊接收设备等，都将设置有智能卡的接口装置。

1.7 智能卡的使用

有了公用的信息协议后，便能允许每一种基于智能卡的应用采取以下相同的操作步骤：

插入用户智能卡；

键入个人标识号（PIN），通过与在智能卡内的标识号相比较以完成用户的身分验证；

从功能菜单上选择所需的服务；

输入最少的数据以满足交易的需要；

确认或接受设备所给出的结果或金额；

观察结果，作出最后的判定；

取走收据；

把作出的判定和执行过的操作记入智能卡；

最后取走智能卡。

上述操作顺序将是智能卡时代的基本使用模式。今天的自动柜员机正在使广大群众逐步适应这种方便的操作。因此，引入智能卡作为金融交易卡或其它的应用，既有很好的兼容性又符合发展的需要。可以预料，这将促进智能卡获得更广泛的应用。

1.8 智能卡的类型

在智能卡社会中，至少有三种类型的智能卡。第一种是用户携带的卡片，它包含着逻辑、数据和对上述信息协议的响应。第二种是作业卡或售货商使用的卡片，它包含了结构细节、数据以及特定的任务或作业所需的通信地址。第三种是设备卡，用来操纵所需任务的信息处理设备。

实际应用时，并不是任何时候都需要这三种类型的卡片。某些情况下，可能只需要用户卡片，自动柜员机便是如此。这时，作业卡或设备卡的功能是以扩展的存储和逻辑功能的形式装配在该设备中的。在零售点结帐机中，则尚需使用作业卡。它包含了应用和保密、安全所需的逻辑以及一张非法卡表（"hot" card list），以代替验证授权的电话查询。作业卡内还将记录全部的交易细节。售货商可通过联机通信或人工传送作业卡的方法，把记录在作业卡上的批量交易数据送给他的开户银行进行结帐。在信息处理系统中，设备卡将提供设备配置的控制。它使一组同样的单元设备（例如显示器、输入/输出装置、通信接口等）能根据不同的应用需要，作多种方式的使用。

1.9 信息设备

智能卡的使用促使信息处理设备有了重大的发展。设想一下，在你的家庭里或办公

室中可能使用的信息处理设备，它们可以是一个平面型电视屏幕的显示器，并用触摸式的输入装置代替键盘，一个自动化的通信设备，一台打印机和适当容量的存储装置。信息处理设备应具有供三种智能卡插入的位置。作为金融应用时的操作步骤如下：

第一步，插入金融交易用户卡。

第二步，选择并插入现金流量管理应用卡或作业卡。此卡片包含财务数据库的电话号码和支持财务分析的程序。它还包含了保护你的设备与金融机构之间安全传送重要数据用的密钥。

第三步，插入设备卡。它将指定和控制本次应用所需的工作站或信息处理设备的配置。这些设备包含一台触摸式输入的显示器，一台通信设备，局部存储器，一台输出用的打印机和局部逻辑部件。

1.10 智能卡的应用实例：个人财务管理

在插入智能卡后，系统就立即进入自动做好处理准备的状态，在显示器上出现如下选择项的菜单：

1. 交易和帐单处理
2. 财务报表和查询
3. 现金收支分析
4. 财务决策和管理

首先选择“交易和帐单处理”，屏幕上随即出现最近通过电子邮件所接收到的帐单。你对每一张帐单要支付的金额和付款日期进行逐张确认或修改。如果出现一张新的付款单，则需进入付帐系统确认。这种新型的电子帐单包含了识别帐户所需的数据、付款期限的选择以及付款用的电子邮件地址等。

接着可选择“现金收支分析”，这时屏幕上显示出自你上次使用此应用之后的现金收支变化情况，包括现金支出、现金收入以及全部的交易，并根据最近 12 个月内的现金收支情况作出现金收支分析。得出的结论可能是现金短缺或是现金剩余。如果有盈余的现金，则要选择另一个菜单并进行相应的操作。首先，更新你的金融交易卡内的现金、透支限额和借方的内容。接着，可以验明通常被归入货币资金的少量多余现金，于是你就能作出各种决定。

最后，选择“财务决策和管理”，输入可用资金的金额和有效期限，屏幕上便显示出一张列出当前可选用的投资方案、期望的收益以及其它限制的表格。选择和输入你的投资决策，包括你所确认的资金额、投资的日期、限制条件以及其它的措施。至此，本次应用已告结束，你可以取走作业卡和设备卡了。如果该系统不再继续使用，便可关机，否则应使它处于接收电子邮件的工作模式。这需要把接收电子邮件用的作业智能卡和相应的设备配置卡插入系统，使它处于无人照管的自动操作状态。

1.11 智能卡与个人计算机的比较

你也许会有这样的想法，即智能卡主要应用于人们日常生活中的基本事务和特定的信息处理。然而，智能卡还将普及应用于更多专门的信息和决策处理。从种类繁多的作业卡和设备卡中选择出不同的卡片组合，将提供范围广泛的应用功能和设备。智能卡的

此为试读，需要完整PDF请访问：www.ertongbook.com