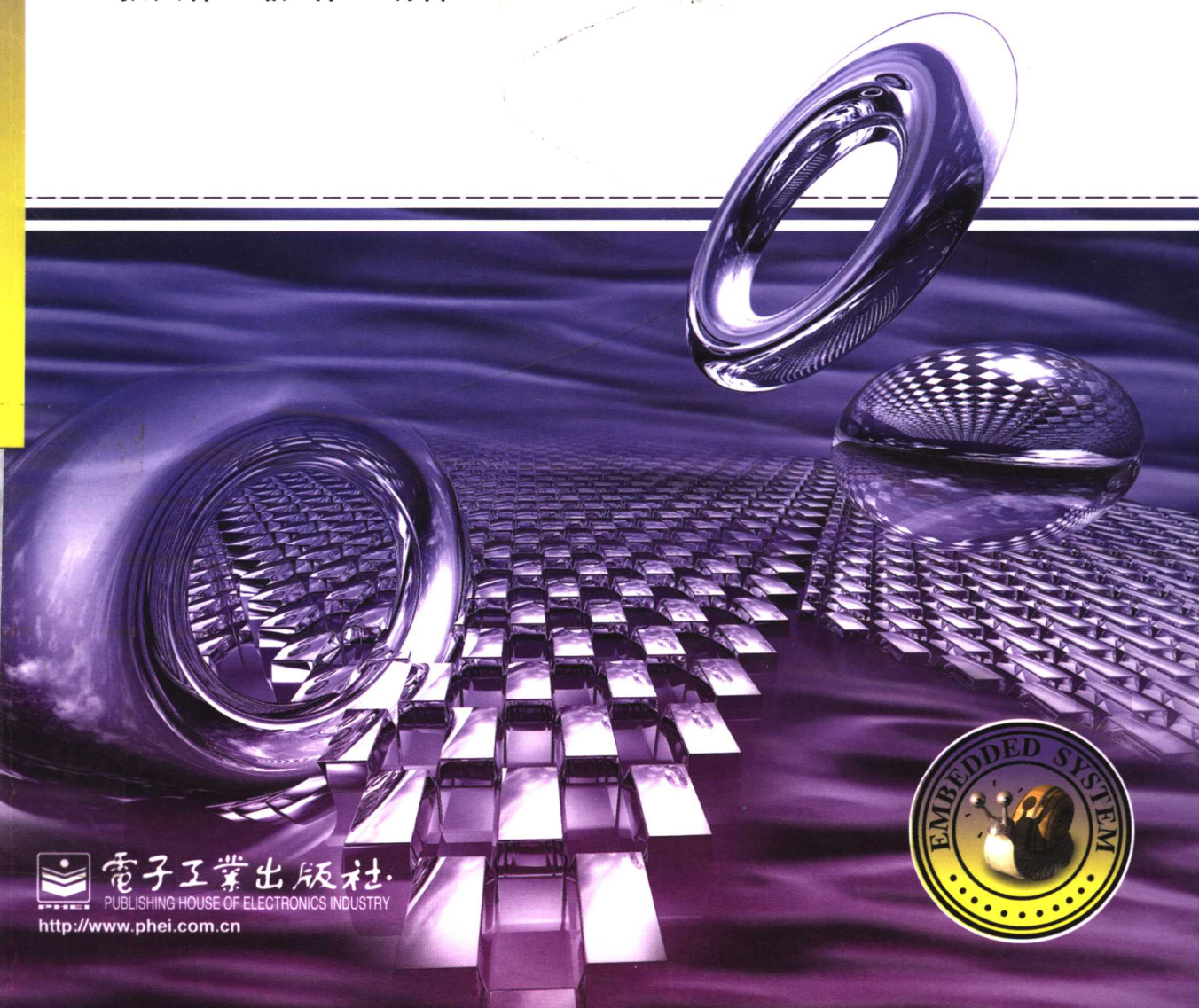
嵌入式技术与应用丛书

EMBEDDED SYSTEM

Java智能卡原理与应用开发

张大伟　靳伟　编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

嵌入式技术与应用丛书

Java 智能卡原理与应用开发

张大伟　靳　伟　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

随着互联网和移动通信技术的发展，Java 智能卡以其安全的多应用支持、主流的面向对象编程环境、应用程序动态下载等众多优点在产业界得到了广泛应用。本书在深入介绍 Java 智能卡原理的基础上，详细阐述了 Java 智能卡 Applet 的开发方法。全书分为两个部分，在第一部分编程基础中，详细介绍了 Java 智能卡的基本原理、开发环境配置、基本 Applet 的编写方法、异常机制、事务处理、共享接口等开发技术。在第二部分应用案例中，结合 Java 智能卡在电子政务、金融、移动增值业务方面的具体应用，详细阐述了身份认证与数字签名、PBOC 电子钱包/存折应用、SIM Toolkit 等应用的开发方法。

面向 Java 智能卡电子政务、电子商务、移动增值领域具体应用的开发讲解并提供了大量翔实的应用例程是本书最主要的特点。

本书可作为电子政务、金融、手机增值业务等方面 Java 智能卡应用开发人员的参考书籍和培训教材，也可作为高校 Java 智能卡教学的本科生和研究生教材。

图书在版编目（CIP）数据

Java 智能卡原理与应用开发/张大伟，靳伟编著. —北京：电子工业出版社，2008.5
（嵌入式技术与应用丛书）
ISBN 978-7-121-05692-5

Ⅰ. J… Ⅱ. ①张…②靳… Ⅲ. JAVA 语言—应用—智能卡 Ⅳ. TP391.4

中国版本图书馆 CIP 数据核字（2007）第 199775 号

责任编辑：高买花　　特约编辑：陈宁辉
印　　刷：北京天宇星印刷厂
装　　订：北京鼎盛东极装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：20.25　字数：518 千字
印　　次：2008 年 5 月第 1 次印刷
定　　价：45.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

出 版 说 明

嵌入式技术是 21 世纪最具生命力的新技术之一，经过近几年的快速发展，已经成为电子信息产业中最具增长力的一个分支。随着手机、掌上电脑、GPS、机顶盒等新兴产品的大量应用，嵌入式系统的设计正成为软硬件工程师越来越关心的话题。面对不断涌现的技术需求和发展机遇，各大嵌入式系统开发商、各科研院所的研发人员都急需一套全方位、针对性强，且具有实际指导意义的嵌入式技术类书籍；各高等院校相关专业的本科生、研究生也迫切希望了解、掌握嵌入式系统的开发技巧，以推动嵌入式技术在各领域的广泛应用和快速发展。

《嵌入式技术与应用丛书》正是针对当前技术与市场需求，由国内站在 IT 业前沿并有实践开发经验的嵌入式系统专家，以实用技术为主线，理论联系实际，将他们在理论研究与实践工作中积累的大量经验和体会有机地融于一体，以丛书的形式奉献给广大读者！

本丛书由基础理论类、硬件设计类、软件开发类、综合应用类书籍组成，立足当前嵌入式技术的发展趋势、核心技术及其主要应用领域，将技术热点与实践应用紧密结合，以实际应用为主线，融合关键性嵌入式设计技术，围绕嵌入式设计理论、开发流程、嵌入式软件验证及测试、代码可重构以及代码优化等方面进行深入浅出的讲解和论述。

读者群定位于高等院校相关领域的高年级学生，科研、开发人员，嵌入式相关领域设计人员等，本丛书可作为嵌入式领域学习、开发人员的参考资料，也可作为高等院校相关专业师生的教学参考书。

本丛书的出版得到了业界许多专家、学者的鼎力相助，对此表示衷心的感谢！同时，热切欢迎广大读者提出宝贵意见，或者推荐更多优秀选题（gmholife@hotmail.com），共同为嵌入式技术的发展添砖加瓦！

电子工业出版社通信分社

2007 年 6 月

序

众所周知，Java 技术自从 1995 年 5 月正式推出以来，已经有了长足的进步和发展。在企业计算方面，基于 Java EE 的中间件解决方案是各大计算机公司、软件公司和系统集成公司最有力的武器，成为企业级应用必不可少的基础软件平台；在桌面计算领域，Java SE 是 PC 或个人电脑软件中不可缺少的部分，基于 Internet 的应用大量采用 Java SE 程序把应用与用户有机地联系起来，以安全、高效地提供网络服务。Java ME 已经是嵌入式领域的事实软件平台标准，无论是无线通信方面的手机软件平台，还是数字电视领域的机顶盒或数字电视机软件平台，都把 Java ME 技术作为其增值服务甚至基础支撑软件的发展方向；而在智能卡领域，Java Card 技术更是得到广泛应用，世界上已经发行了几十亿张支持 Java Card 技术的智能卡产品，如电信领域的 SIM 卡/R-UIM 卡/USIM 卡、金融领域的智能信用卡、政府/军队/企业的身份认证卡及居民身份证卡等。

为什么 Java 技术会得到这么广泛范围的接受呢？在我看来，主要有以下这么几点：

其一，Java 技术是开放技术。该技术标准由国际组织或企业联盟通过开放的程序和方法共同制定，包括标准的起草、确定、发布、修改及该标准未来的发展方向等。不论是商业合作伙伴还是竞争对手，都可以参加或引导标准的制定过程。开放技术能带来产品的公平竞争，并且用户可以从相互竞争的产品供应商那里选择所需要的符合开放标准的产品，今天对产品的选择并不影响明天选择不同来源的产品。其二，Java 技术的安全性。Java 的出现就是作为网络语言而诞生的，其安全设计的初衷就是认为从网络下载的程序都可能是不安全的，因此安全考虑和措施构成了 Java 架构的重要组成部分。其三，Java 技术的跨平台性。现在，几乎所有的操作系统平台都支持 Java 技术，所以用 Java 编写的程序可以运行在不同的软硬件平台上。

正是有了以上特点，Java 技术才能有今天的发展和普及，我们才能在这里讨论 Java Card 的技术和应用。

最近几年，Java Card 的发展在中国得到了长足的进步，研究和教学取得一定进展，在移动通信、金融、军队及企业身份卡等方面开始规模化应用。但是，在中国很难见到系统介绍 Java Card 技术与开发应用的中文书籍，这不能不说是一大遗憾。所幸，本书的出版可以部分满足在中国从事 Java Card 技术研究、教学、产品开发、产品推广、应用开发等方面人士的需要。本书作者几年来从事 Java Card 技术的研究和教学，有比较丰富的知识和经验。特别是本书包括了最新的 Java Card v.2.2.2 规范的内容，较详细地介绍了 Java Card 中的加密技术，给出了一些具体应用的代码例子，并介绍了 Java Card 应用开发工具的使用，这些都十分实用。望本书对于 Java Card 技术在中国的发展和应用能够起到较大的推动作用。

Sun Microsystems, Inc.

前　言

随着互联网和移动通信技术的发展，Java 智能卡以其多应用的支持、良好的安全特性、主流的面向对象编程环境、应用程序在线动态下载等众多优点在产业界得到了广泛应用。在智能卡应用的国际市场上，知名的智能卡厂商均支持 Java 技术，第三代移动通信技术（3G）已经完全使用 Java 卡技术作为 SIM 卡的应用规范以适应移动增值业务发展的需要。在教育领域，全球著名的智能卡厂商 Alaxto（即现在合并后的 Gemalto）已经组织了几届全球范围内面向高校的 Java 智能卡应用技术大赛，包括 MIT（美国麻省理工学院）在内的多所国际知名大学参加竞赛，推动了这一技术在高校中的普及与应用。

中国的智能卡市场在移动通信、银行、公众交通、有线电视、校园应用等方面迅猛发展，并且政府部门大力支持的多个大项目，如第二代身份证、社保卡等也将该趋势延续下来。特别是目前占市场份额 70%的手机 SIM 卡，《信息产业“十一五”规划》中表明，到 2010 年，中国移动电话用户总数将达 6 亿户。SIM 卡无论是目前的市场容量还是未来的发展潜力都是巨大的。2008 年的北京奥运会和 2010 年的上海世博会将进一步刺激市场对智能卡的需求。

国内的 Java 智能卡技术起步较晚，但发展很快。2005 年，北京握奇数据系统有限公司完成了国内首个具有完全自主知识产权的 Java 智能卡平台的研发，而后多家厂商也开始进入这一市场。随着整个行业的发展，对 Java 智能卡开发人员的需求也在快速增长。作者近年来一直从事于 Java 智能卡技术的研究，并参与了北京握奇首张 Java 智能卡的研发工作，也深切地感受到 Java 智能卡应用的快速发展和专业人才的紧缺。本书的出版正是希望能够为这一快速增长的人才需求市场提供一本具有实际应用价值的参考书。

全书分两个部分，共 13 章。第一部分为 Java 智能卡编程基础，包括第 1~10 章，第 1~3 章详细介绍智能卡和 Java 智能卡的基本原理、软硬件平台和总体结构。第 4 章详细讲述 Java 智能卡开发环境的配置方法。第 5~9 章为 Java 智能卡 Applet 编程的具体介绍，并在第 8 章、第 9 章深入阐述事务处理和应用防火墙机制的编程方法，这也是 Java 智能卡中所特有的嵌入式编程技术。在第 10 章，我们给出了一个综合上述章节内容的编程示例。第一部分适合于 Java 智能卡的初学者作为入门知识来学习。第二部分为 Java 智能卡应用案例，包括第 11~13 章，其中第 11 章详细阐述电子政务中的数字签名和身份认证机制在 Java 智能卡中的实现方法，第 12 章给出符合中国人民银行规范的电子钱包应用的开发设计方法，第 13 章详细描述 SIM Toolkit 的一个开发例程。第二部分主要面向于实际应用案例的开发讲解，适合于具有一定 Java 智能卡基础的中高级开发人员来学习。本书在每一章理论讲解之后都安排了一个示例程序和测试脚本的分析，以加深相关知识的理解，作为进一步开发的范例。

本书特点：面向 Java 智能卡电子政务、电子商务、移动增值领域具体应用的开发讲

解并提供了大量翔实的应用例程。

在全书的编写过程中，靳伟完成了第 7、8 章的编写，张红武完成了第 9 章的编写，李曦完成了第 3 章的编写，其余章节由张大伟编写完成。同时在编写过程中，还得到了胥怡心、李胜广在技术上的帮助和支持，在此也向他们表示诚挚的谢意。同时也要感谢北京握奇数据系统有限公司的大力支持和电子工业出版社高买花编辑对本书出版的精心指导和热情帮助。

由于 Java 智能卡是一门新兴的技术，并在不断地发展和完善，我们对它的理解仍欠全面。限于作者水平有限，书中不可避免存在缺点和不足，真诚地欢迎广大读者批评指正（dwzhang@bjtu.edu.cn 或 gmholife@hotmail.com），以利于我们纠偏补益于来时。

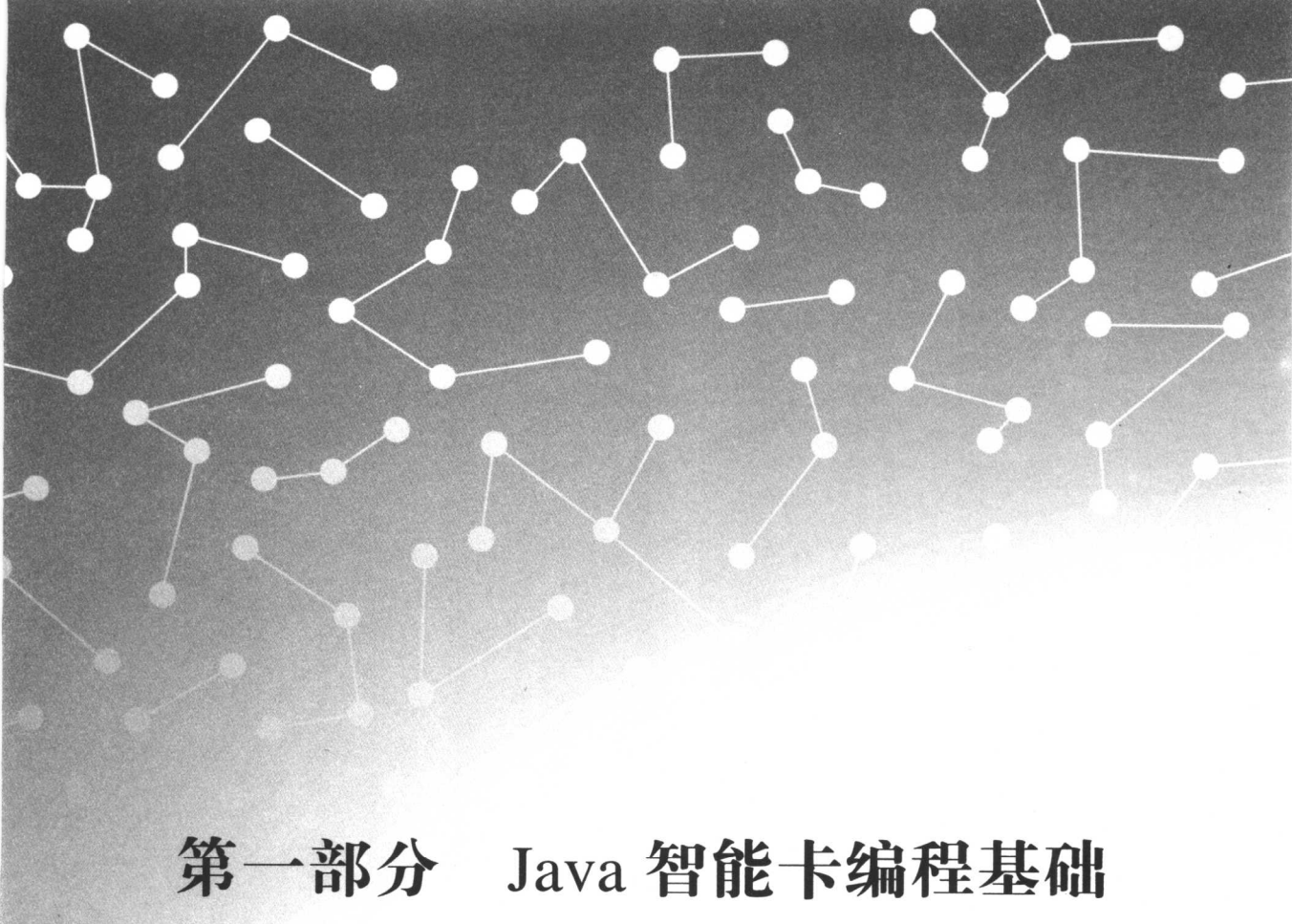
编著者

2007 年 12 月

目　录

第一部分　Java 智能卡编程基础

第二部分 Java 智能卡应用案例



第一部分　Java 智能卡编程基础

第1章 绪 言

随着科学技术的发展和社会的进步，人们在各项社会活动中的分工越来越细，相互之间的联系越来越频繁，依赖性也越来越强，第三产业在国民经济中所占的比重也越来越大。每天有许多人在各个方面为我们提供各项服务，我们也在某一方面为其他人提供服务。为了便于处理每天遇到的形形色色的多种事情，我们需要随身携带多种票证、卡片、单据等，例如现金、发票、收据、食堂饭票和公共交通车票等；还有证明身份用的身份证、工作证和看病用的医疗证等。携带现金，既不方便，又不安全，因此用卡来取代现金的计划就提到日程上来了。目前已发行的有银行信用卡、取款卡，日常生活中的电话卡、交通卡、预付费（水、电、煤气、用餐）卡和医疗卡等。并且随着智能卡技术的发展和智能卡应用领域的进一步规范化，今后我们使用的智能卡都将做到一卡多用，将众多应用集成在一张卡中，人们再也不必为找卡而烦心了。

目前，国际上智能卡的应用已经进入高峰发展时期，据统计，2000年全球智能卡市场为36亿张，2003年为63亿张。智能卡已经广泛应用在电信（SIM卡、USIM卡）、银行、医疗保健、娱乐、公交门票、门禁、识别、有线电视节目收视收费和顾客消费等领域。

1.1 智能卡简介

1. 智能卡概念

智能卡的名称来源于英文名词“Smart Card”，又称集成电路卡（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。由于智能卡都有唯一的发行人的识别标志，这种卡有时也被称为识别卡。

智能卡是随着半导体技术的发展和社会对信息安全性等要求的日益提高应运而生的，它里面所包含的集成电路芯片具有微处理器及大容量存储器，具有存储、加密及数据处理能力，被公认为世界上最小的个人计算机。与目前仍在广泛应用的磁卡相比，智能卡具有安全性高、可靠性强、存储容量大等许多优点，它可承载比磁卡多达100倍的信息，并能与终端结合进行复杂的计算。这种既具有智能性，又便于携带的卡片，为现代信息的处理和传递提供了一种全新手段，它一出现就备受重视，并逐步在世界各国形成热点，风靡全球。

2. 智能卡发展进程

智能卡的概念最初由法国人罗兰德·莫瑞诺（Roland Moreno）在1972年提出，此后法国布尔（Bull）公司率先投入了对这一潜力无穷的高新技术产品的研究和开发。1976年

布尔公司高级研究员 Ugon 先生领导的研究小组首先研制成了世界上第一张由双晶片（微处理器和存储器）组成的智能卡，接着又于 1978 年制成了单晶片智能卡并取得了技术专利。

在 20 世纪 80 年代初期，法国和德国开始了最初的智能卡应用实验。除了法国的 Bull 以外，先后有 Motorola、Thomson、Hitachi、OKI、Toshiba、Sharp、Atmel、Gemplus、Schlumberger 等十几家公司相继投入智能卡芯片和卡片成品的开发与生产，形成了一个世界性的新兴技术产业。VISA 组织、MasterCard 组织、EuroPay 组织等三大国际信用卡组织相继推出了智能卡产品，在美洲、欧洲及亚洲的许多国家得到了推广和应用，并在当地的信用卡市场上占据了一定的份额。

智能卡的发展进步具体体现在结构、加密、通信接口、CPU 体系结构、安全性设计、功耗降低以及供电电压等方面，可概括为：

（1）结构的发展经历了从逻辑加密卡到智能卡的发展。

（2）加密算法经历了简单的硬件加密逻辑，即对称加密算法（DES、AES、3DES 等）到非对称式算法（RSA、ECC 等）的发展。

（3）接触卡接口、非接触卡接口、USB 接口，现阶段已经发展到一个芯片中集成了多种通信接口，形成所谓的双界面卡（接触/非接触、7816 接口/USB 接口等组合）。

（4）早期智能卡内的 CPU 与普通的嵌入式微控制器没有太多的区别，仅仅是一个 CPU 核而已。但是随着智能卡安全性、多用途等需求的不断提高，智能卡内 CPU 的体系结构也相应地发生了很大的变化。除了必须具有通用嵌入式微控制器的各种特性外，更多的是表现在安全性能方面逐步形成一个特定的、安全的智能卡 CPU 核。

（5）智能卡的安全性设计不仅仅表现在某一个部件方面，而是表现在整体方案方面，包括逻辑设计、物理实现都应该考虑。逻辑方面，各种加密算法、CPU 的状态设置及 MMU 实现、算法函数实现时间的随机化、具有真随机数发生器、频率检测、电压检测、温度检测等，都属于安全性设计的范畴。物理实现方面，防止各种物理解剖、探测都是安全性设计应该考虑的措施。

随着芯片技术和现代加密技术的发展进步，智能卡的发展更是日新月异。目前，智能卡已应用到银行、电信、交通、社会保险、电子商务等领域，IC 电话卡、金融智能卡、社会保险卡和手机中的 SIM 卡都属于智能卡的范畴。

3. 智能卡技术优势

相对于磁卡，智能卡在应用中的技术优势在于良好的机器读/写能力、共同认可的安全防范技术和相对较大的数据存储能力。

（1）良好的机器读/写性能便于人—机—卡之间的会话

智能卡是一种电路卡，它在机器读/写性能上远优于磁卡和光卡，无需往复的机械动作即可完成人—机—卡之间的多次会话过程,使卡在应用时更容易进行操作与相互通信，给卡的应用开发者和使用者都带来极大的便利。

（2）良好的安全技术使卡能够脱离网络使用

智能卡从硬件和软件等几个方面实施其安全策略，可以控制卡内不同区域的访问控制和存取特性。智能卡的安全可靠性使其在应用中对计算机网络的实时性、敏感性要求降低，

十分符合当前中国国情，有利于在网络质量不高的环境中应用。

（3）大容量的数据存储能力使智能卡成为数据载体

智能卡内部有 RAM、ROM、EEPROM 等存储器，存储容量可以从几个字节到几兆字节。卡上可以存储文字、声音、图形、图像等各种信息。在磁卡系统中，持卡人的信息存放在中心数据库系统，每次使用都必须通过终端，以网络形式从数据库中提取持卡人的信息，现在智能卡本身就可以存储这些信息，终端设备不再需要联网，使用的灵活性大大增强，交易的实时性也明显改善。

4. 智能卡生命周期

智能卡从设计到发行，一般可归纳成 9 个步骤。

（1）智能卡软、硬件设计

系统设计：根据应用系统对卡的功能和安全的要求设计卡内芯片（或考虑设计通用芯片），并根据工艺水平和成本对智能卡的 CPU、存储器容量和通信接口等提出具体要求，或对逻辑加密卡的逻辑功能和存储区的分配提出具体要求。

软件设计：包括卡片操作系统 COS（Chip Operating System）和应用软件的设计。

该过程由设计者完成。

（2）芯片制造

设计者将设计好的版图提交给芯片制造厂。制造厂根据设计与工艺过程的要求，产生多层掩膜版。在一个圆片（Wafer）上可制作几百～几千个相互独立的电路，每个电路即为一个小芯片（die）。小片上除有按 IC 卡标准（8 个触点）设计的压焊块外，还应有专供测试用的探针压块。圆片厚度要符合 IC 卡的规定，研磨后将圆片切割成众多小芯片。该过程由半导体厂家完成。

（3）掩膜

在芯片制造过程中将 COS 掩膜固化到芯片的 ROM 中，通常称硬掩膜（Mask）。传输密钥也可在此时写入。传输密钥是为了防止卡片在从制造厂运输到发行商的途中被窃而采取的防卫措施，是仅为制造厂和发行商知道的密码。发行商接收到卡片后要首先核对传输密钥，如核对不正确，卡将自锁。该过程由半导体厂家完成。

（4）模块封装

对小硅片进行光刻以产生必要的电路，并将它封装在黑色的集成电路模块中。将集成电路的输入/输出端连接到大的接触面上，便于今后读/写器的操作。将芯片安装在有 8 个触点的智能卡专用载带上，制成模块。该过程由模块封装厂家完成。

（5）卡片制造

按客户要求印制塑料基片，即卡基，将模块镶嵌到卡基上，制成智能卡，并完成卡片表面的印刷工作。该过程由制卡厂家完成。

（6）卡片初始化

设置卡片的基本参数及安装卡片初始密钥。该过程在卡片出厂后实施，通常由制卡厂家完成。