全国高等学校物联网技术应用系列教材

电子证件物联网

赵林度　陈宇　任宗伟 ◎ 主编
王旭 ◎ 副主编

中国物资出版社

全国高等学校物联网技术应用系列教材

电子证件物联网

主　编　赵林度　陈　宇　任宗伟
副主编　王　旭

中国物资出版社

图书在版编目（CIP）数据

电子证件物联网/赵林度，陈宇，任宗伟主编．—北京：中国物资出版社，2011.8
（全国高等学校物联网技术应用系列教材）
ISBN 978-7-5047-3906-3

Ⅰ.①电… Ⅱ.①赵…②陈…③任… Ⅲ.①互联网络—应用—高等学校—教材②智能技术—应用—高等学校—教材 Ⅳ.①TP393.4②TP18

中国版本图书馆 CIP 数据核字（2011）第 150894 号

策划编辑	王玉霞	**责任印制**	何崇杭
责任编辑	王玉霞	**责任校对**	孙会香　杨小静

出版发行	中国物资出版社		
社　　址	北京市丰台区南四环西路 188 号 5 区 20 楼	**邮政编码**	100070
电　　话	010-52227568（发行部）	010-52227588 转 307（总编室）	
	010-68589540（读者服务部）	010-52227588 转 305（质检部）	
网　　址	http://www.clph.cn		
经　　销	新华书店		
印　　刷	中国农业出版社印刷厂		
书　　号	ISBN 978-7-5047-3906-3/TP·0072		
开　　本	787mm×1092mm　1/16		
印　　张	18.5	**版　　次**	2011 年 8 月第 1 版
字　　数	462 千字	**印　　次**	2011 年 8 月第 1 次印刷
印　　数	0001—3000 册	**定　　价**	35.00 元

版权所有·侵权必究·印装差错·负责调换

本系列教材编委会

何明珂　北京工商大学

赵林度　东南大学

施先亮　北京交通大学

王旭坪　大连理工大学

计国君　厦门大学

李文锋　武汉理工大学

张亚平　哈尔滨工业大学

王立海　东北林业大学

白世贞　哈尔滨商业大学

李向文　大连海事大学

前　言

随着经济国际化进程的不断深入，国家加大了对物联网技术应用的支持力度，物联网技术已渗透到了我们生活的各个领域中。当前发达国家正在积极筹建物联网标准，并试图垄断物联网建设的关键技术，因此我国只有迅速掌握和建立具有自主知识产权的物联网标准和关键技术，才能在这场竞争中获胜。

本书从物联网技术的基础出发，吸收了国外先进的理念、技术和思想，结合近年来物联网在电子证件方面应用的前沿课题而编写的。本书共分十一章，前四章阐述了电子证件物联网概述、射频识别（RFID）技术、电子证件物联网网络安全技术、电子证件物联网网络管理信息系统与管理信息库；后七章主要阐述了物联网技术在校园卡与校园一卡通、路桥隧自动收费、城市公交自动收费系统、大型体育赛事的安全管理系统、电子证照安全管理系统、银行金融信息卡系统及大型会展门禁管理系统等方面的应用。本书内容丰富、翔实，对从事电子证件物联网安全研究、开发及工程实施的人员具有很好的参考价值。

本书由赵林度、陈宇、任宗伟担任主编，王旭担任副主编。其中第一章至第五章由任宗伟编写，第六章至第十章由陈宇编写，第十一章由李楠、杨少东、马丽、陈化飞、王旭编写，全书由赵林度统审。

本书在编写过程中，参考了许多国内外的相关资料，引用了物联网安全领域已有的一些研究成果和文献资料，在此向原作者表示由衷的谢意。

由于物联网安全技术属于新兴领域，物联网又处于多学科交叉并迅速发展之中，加之编者水平有限，书中表述难免出现疏忽之处，敬请各位专家、读者提出批评意见。

编　者

2011 年 2 月

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

上篇　理论篇

下篇　实践篇

上篇

理论篇

第一章　电子证件物联网概述

第一节　物联网简介

一、物联网概念

1. 物联网的概念

物联网是 EPC（Electronic Product Code）技术和互联网结合的产物，是物流企业在进行供应链管理过程中实现信息交流和管理的先进技术。1999 年美国麻省理工大学 Auto-ID实验室首次提出了 EPC 系统及物联网的概念。物联网是在计算机互联网的基础上，利用 RFID（Radio Frequency Identification）、EPC 编码、无线数据通信等技术，构造一个实现全球物品信息实时共享的物的国际互联网络（Internet Of Things，IOT）。

从网络结构看，物联网就是通过 Internet 将众多 RFID 应用系统链接起来并在广域网范围内对物品身份进行识别的分布式系统。将读写器安装到任何需要采集信息的地方，通过 Internet 进行全程跟踪，实现对物品的识别，这样所有的物品和 Internet 就组成了“物联网”网络，其实质就是利用 RFID 技术，通过计算机互联网以实现全球物品的自动识别，达到信息的互联与实时共享。物联网中 RFID 应用系统可以表示如图 1－1 所示的拓扑结构。

2. 物联网的功能

有了各种 RFID 应用系统和已经覆盖全球的 Internet 网络，那么物联网的网络硬件系统就具备了。Internet 上的计算机终端就是 RFID 应用系统中的计算机，通过 Internet，RFID 应用系统的后台信息系统更加丰富和容易理解。但仅具有物联网硬件系统远不能完成物联网的功能，还需要考虑以下功能：

（1）物联网信息服务（IOT-Information Service，IOT-IS）

物联网的目的是实现贴有 RFID 标签的物品在全球广域网范围内进行识别、跟踪和查询，也就是要求在任何一个地方都能找到与物品 ID 号对应的信息资源库。RFID 标签内存储的信息有限，主要是用来存储标识物品身份的 ID 号。虽然 ID 号中的部分字段可以通过事先约定用来表示物品的某些属性，但仅靠 ID 号所能表达的商品属性信息依然十分有限，远不能涵盖物品生产、加工、原材料、产地、运输、仓储等大量的信息。这些物品信息应该存放于 Internet 上，并且与物品的 ID 号一一对应起来，存放物品信息的计算机称之为物联网信息服务器，通过 Internet 可以访问物联网信息服务器，这台服务器提供的服务称之为“物联网信息服务”。

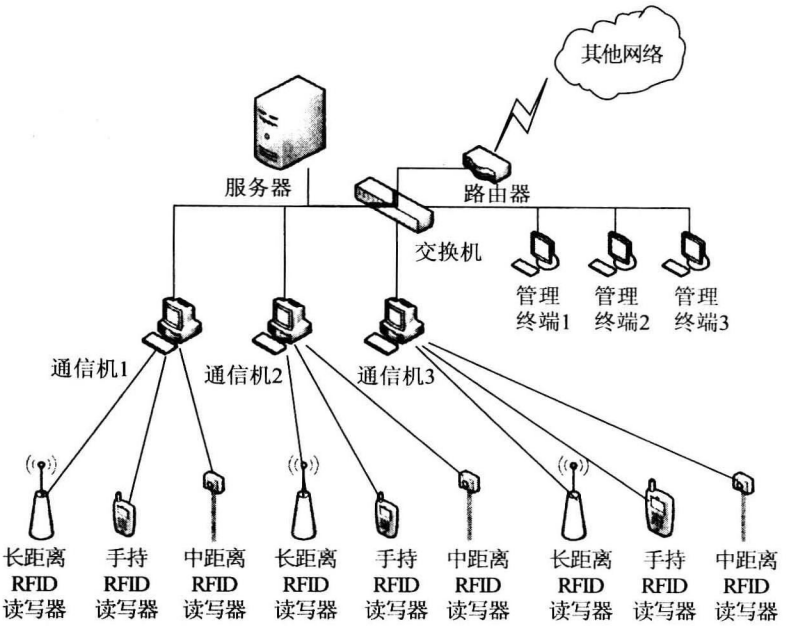

图 1-1　RFID 应用系统拓扑结构

（2）物联网名称解析服务（IOT-Name Service，IOT-NS）

如果 Internet 上某台计算机 A（或直接连到 Internet 上的读写器）当前获得了一个物品标签的 ID 号，那么其通过什么方式获得“物联网信息服务器”上的这个 ID 号对应的物品属性信息呢？这就需要 Internet 上有另外一台服务器 B。服务器 B 能够将标签的 ID 号转换成其对应的资源地址统一资源标识（Universal Resource Identifier，URI），并将地址返回给计算机 A，计算机 A 再根据资源地址（URI）找到对应的“物联网信息服务器”以获得对应于此 ID 号的物品的属性及相关信息，同时“物联网信息服务器”还可以更新数据库，记录下此物品当前的信息（例如解析时间、标签当前位置、当前识别此标签的读写器的 ID 号等）。这里的名称解析服务器是专门用来解析物联网标签的 ID 的，其提供的服务称为“物联网名称解析服务”。此服务类似于 Internet 上的 DNS 服务，只不过后者是将客户端输入的网址转换成其对应的网络资源地址。

（3）物联网中间件服务（IOT-Middle Ware Service，IOT-MWS）

物联网上的 RFID 应用系统种类繁多，各 RFID 应用系统中采用的硬件设备（如读写器）是不同厂家生产的，而物联网本身应该是开放和标准的，以方便各种用户接入。这就好比计算机为方便各种外接设备的接入而采用驱动程序的道理一样。在物联网中这种角色称为中间件（Middle Ware）。物联网中间件负责实现与 RFID 硬件以及配套设备的信息交互和管理，同时作为一个软硬件集成的桥梁，完成与上层复杂应用的信息交换。它是 RFID 应用框架中相当重要的一环，总的来说，物联网中间件起到一个中介的作用，它屏蔽前端硬件的复杂性，并把采集的数据发送到后端的 IT 系统，在此将其称之为“物联网中间件服务”。

此为试读，需要完整PDF请访问：www.ertongbook.com

（4）物联网中的RFID编码及射频识别

RFID工作的频段很多，典型的有125kHz、134kHz、13.56MHz、433MHz、2.45GHz、5.8GHz等。物联网中并不是都会使用这些RFID频段的标签，物联网主要解决的是物流问题，一般选择适合物流的RFID频段标签，同时这个频段要受到所在国的频率资源规定的限制，例如美国主要考虑的是900MHz和13.56MHz的无源标签，而日本采用2.45GHz频段。中国目前物流频段的选择主要向欧美靠近，稍有不同。物联网中的射频识别部分（包括读写器和标签）也需要针对物联网的需求和特点作出一些规范，而不像其他的RFID应用项目，只要能满足RFID应用需求就可以。

除了频段选择之外，还有一个主要问题就是物联网标签ID号的编码了。要想在Internet上获得自己对应的资源信息，这个ID号必须是唯一的，而且其编码规则和解析方式能够通过和物联网解析服务对应起来，这样才能够通过标签ID号访问其对应的物品的属性等信息。

在该系统中，每一个物品都被赋予了一个独一无二的代码，并存储于物品上的电子标签中，同时将这个代码所对应的详细信息和属性（包括名称和类别、生产日期、保质期等）存储在IOT-IS服务器中。当物品从生产到流通的各个环节中被识别并记录时，通过TOT-NS的解析可获得物品所属信息服务系统的URI，进而通过网络IOT-NS服务器获得其代码所对应的信息和属性，以进行物品的识别和达到对物流与供应链自动追踪管理的目的。

物联网的目标是为每一个物品建立全球可交流识别的、开放的统一标准，智能跟踪与管理的体系。其最终目的是构造“泛在网络社会”（Ubiquitous Network Society）。无处不在的各种传感器与物品产生各种实时信息，这些信息通过互联网进行交换，实现物品“运筹帷幄，决胜千里”的物流与供应链控制与过程管理。所以，“泛在”不但指地域的无处不在，也指涉及我们社会的方方面面，如日常消费、生产运输、安全追踪、物流交通、贸易采购、医疗卫生等。因此，物联网的“泛在”概念一经提出，立即受到了各国政府、行业和学术界的广泛重视。

3. 物联网的特点

物联网是一种在全球范围内对每个物品进行跟踪、监控的全新理念，它将在全球范围内从根本上提高对物品产生、配送、仓储、销售等环节的监控水平，将成为继条码技术之后，再次变革商品零售、物流配送及物品跟踪管理模式的一项新技术，将在根本上改变供应链流程和管理手段。概括来说，物联网具有以下几个特点：

（1）对物品实现唯一的标识

传统的条码（Bar-code）编码体系，是对每一种商品项目进行编码，对传统的商品包装和物流管理产生了巨大的作用，但由于条码的非唯一标识的属性，使对物品的自动化管理只能够停留在类级别的层面上。而物联网的EPC技术，则是能够对单个而不是对一类物品进行编码，它通过对物品的唯一标识，并借助计算机网络系统，完成对单个物体的访问，突破了传统条码所不能完成的对单品的跟踪和管理任务。

（2）对物品快速分级进行处理

EPC结构中，沿袭了原有的按不同类型的容器进行编码特点，将物流过程中不同的货

品、集装箱、托盘和仓库等进行分层级编码，解决在同一时间进行多种标签识别的问题。如一辆满载贴有 EPC 标签物品的集装箱通过读写器的扫描区时，读写器将会得到大量的不同层级的 EPC 标签信息，此时，EPC 系统可以明确地辨认出货物、包装箱和集装箱的信息，并根据需要对有关信息进行处理，达到快速分级处理的效果，大大提高了工作效率。

（3）对物品物流信息的实时监控

物联网是在互联网的基础上对物流信息进行跟踪、监控的实时网络，任何一个安装有读写器的终端，都可以通过射频扫描技术读取物品的相关信息，并通过互联网的信息传输作用，实现对物品物流信息的实时监控。

（4）对信息实现自动非接触式处理

EPC 系统的一个核心元素就是 RFID 技术，它是利用射频信号及其空间耦合和传输特性进行非接触双向通信，实现对静止或移动物品的自动识别，并进行数据交换的一项自动识别技术。这种自动非接触式处理的特点，可以实现对动态物流与供应链信息进行高效管理，有效地降低物流成本。

（5）可以实现供应链各个环节信息共享

在供应链中的任何一个物品都被贴上唯一标识自己的电子标签，通过互联网和射频技术，可以在供应链中任何一个环节将该物品的信息自动记录下来并实现共享。

二、物联网实现原理

物联网是在计算机互联网的基础上，利用 RFID、无线数据通信等技术，构造一个覆盖世界上万事万物的“Internet of Things”。在这个网络中，物品（商品）能够彼此进行“交流”，而无须人的干预。其实质是利用射频自动识别（RFID）技术，通过计算机互联网实现物品（商品）的自动识别和信息的互联与共享。

而 RFID，正是能够让物品“开口说话”的一种技术。在物联网的构想中，RFID 标签中存储着规范而具有互用性的信息，通过无线数据通信网络把它们自动采集到中央信息系统，实现物品（商品）的识别，进而通过开放性的计算机网络实现信息交换和共享，实现对物品的“透明”管理。

“物联网”概念的问世，打破了之前的传统思维。过去的思路一直是将物理基础设施和 IT 基础设施分开：一方面是机场、公路、建筑物，而另一方面是数据中心、个人电脑、宽带等。而在“物联网”时代，钢筋混凝土、电缆将与芯片、宽带整合为统一的基础设施，在此意义上，基础设施更像是一块新的地球工地，世界的运转就在它上面进行，其中包括经济管理、生产运行、社会管理乃至个人生活。

物联网可分为五层：末梢节点（采集控制）层、接入层、承载网络层、应用控制层和用户层。如图 1－2 所示。

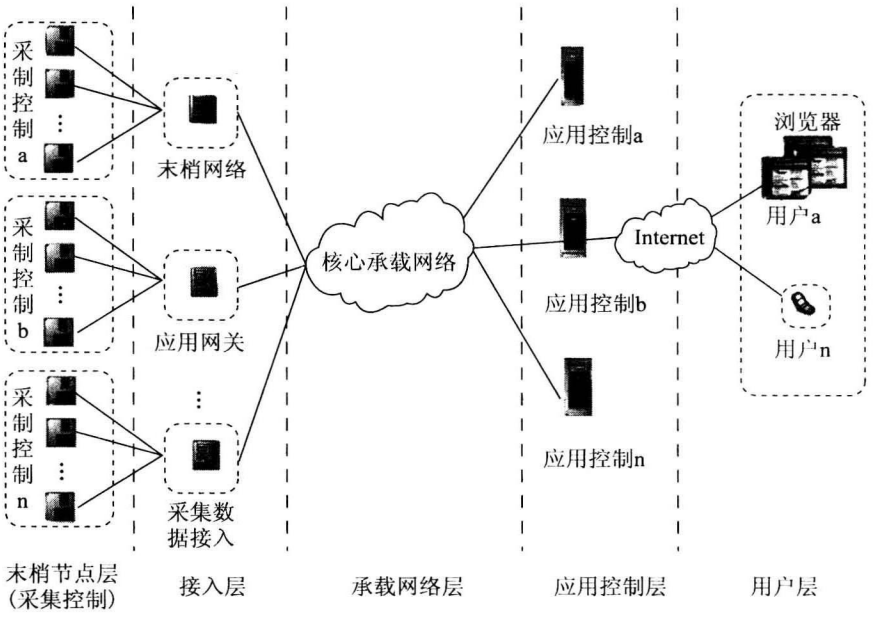

图 1-2　物联网组成示意

末梢节点层是物联网的皮肤和五官识别物体，负责采集信息。末梢节点层包括二维码标签和识读器、RFID 标签和读写器、摄像头、GPS、传感器、终端、传感器网络等，主要是识别物体、采集信息，与人体结构中皮肤和五官的功能相似。

对于目前关注和应用较多的 RFID 网络来说，张贴安装在设备上的 RFID 标签和用来识别 RFID 信息的扫描仪、感应器均属于物联网的末梢节点层。在这一类物联网中被检测的信息是 RFID 标签内容，高速公路不停车收费系统、超市仓库管理系统等都是基于这一类结构的物联网。如图 1-3 所示。

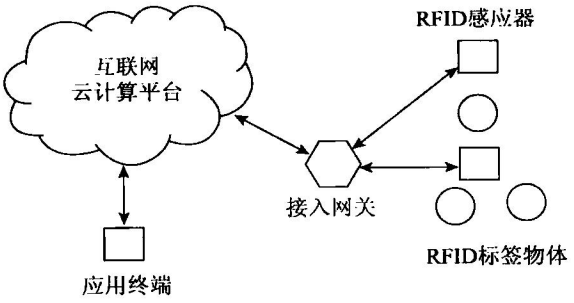

图 1-3　物联网末梢节点层结构—RFID 感应方式

用于战场环境信息收集的智能微尘网络，末梢节点层由智能传感器节点和接入网关组成，智能节点感知信息（温度、湿度、图像等），并自行组网传递到上层网关接入点，由网关将收集到的感应信息通过网络层提交到后台处理。环境监控、污染监控等应用都是基

于这一类结构的物联网。如图 1-4 所示。

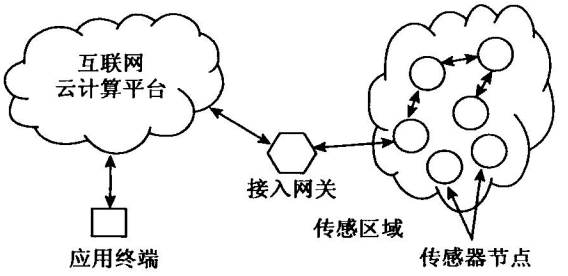

图 1-4　物联网末梢节点层结构—自组网多跳方式

接入层由基站（sink）节点和接入网关（Access Gateway）组成，完成应用末梢各节点信息的组网控制和信息汇集，或完成向末梢节点下发信息的转发等功能。也就是末梢节点之间完成组网后，如果末梢节点需要上传数据，则将数据发送给基站节点，基站节点收到数据后，通过接入网关完成和承载网络的链接；而应用控制层需要下发控制数据时，接入网关接收到承载网络的数据后，由基站节点将数据发送给末梢节点，从而完成末梢节点与承载网络之间的信息转发和交互的功能。

末梢节点与接入层构成了物联网的信息采集和控制，其按照接入网络的复杂性不同可分为简单接入方式和多跳接入方式。简单接入就是在采集设备获取信息后直接通过有线或无线方式将信息直接发送至承载网络，如目前 RFID 读写设备主要采用简单接入方式。简单接入方式可用于终端设备分散数据量的业务应用。而多跳接入是利用无线传感器（WSN）技术，将具有无线通信与计算能力的微小传感器节点通过自组方式，各节点能根据环境的变化，自主地完成网络自适应组织和信息的传递。由于节点间距离较短，一般采用多跳方式进行通信。而后传感器网络最终将信息通过接入网关传递到承载网络。典型的无线传感器设备有 ZigBee、UWB 等。多跳接入方式适用于终端设备分别集中、终端与网络间传递数据量较小的应用。通过采用多跳接入方式可以降低末梢节点、接入层和承载网络的建设投资和应用成本，以及方便建设实施工作和提升接入网络的健壮性。

网络层是物联网的神经中枢和大脑，负责信息的传递和处理。网络层包括通信与互联网的融合网络、网络管理中心、信息中心和智能处理中心等。

应用控制层是物联网的“社会分工”与行业需求结合，实现广泛智能化。应用控制层是物联网与行业专业技术的深度融合，与行业需求结合，实现行业智能化，这类似于人的社会分工，最终构成人类社会。

用户层为用户提供物联网应用 UI 接口，包括用户设备（如 PC、手机）、客户端等。

三、物联网实施步骤

物联网的实施实质是利用 RFID 技术。RFID 是 20 世纪 90 年代开始兴起的一种自动识别技术，也是目前比较先进的一种非接触识别技术。以简单 RFID 系统为基础，结合已有的网络技术、数据库技术、中间件技术等，构筑一个由大量联网的阅读器和无数移动的

标签组成的，比 Internet 更为庞大的物联网成为 RFID 技术发展的趋势。

一般来讲，物联网的开展步骤主要有如下几点：

（1）对物体属性进行标识，属性包括静态的和动态的，静态属性可以直接存储在标签中，动态属性需要先由传感器实时探测；

（2）需要识别设备完成对物体属性的读取，并将信息转换为适合网络传输的数据格式；

（3）将物体的信息通过网络传输到信息处理中心（处理中心可能是分布式的，如家里的电脑或者手机，也可能是集中式的，如中国移动的 IDC），由处理中心完成物体通信的相关计算。

第二节　电子证件概述

一、电子证件的定义

证件，顾名思义是一种证明身份或资料的文件（凭证）。证件存在的形式千变万化，从一张纸到一个本子，从一块牌子到一张卡片，但它们的功能不变，即证明持有人的身份或资格。

随着我国经济的高速发展，各行各业对“身份识别类证件”的要求也越来越高，主要体现在证件信息内容的管理，证件安全性、防伪、数字化和信息化等方面。电子证件随之产生，它是指在制作证件的时候加入射频标签，从而使其具有存储容量大、安全性高、无外露触点以及防污、防磁、抗静电、抗射线等技术特点。

二、电子证件的发展

自从 20 世纪磁卡出现以来，电子证件开始稳步发展，大致经历了以下三个阶段：

第一阶段：带有记忆功能的磁性电子证件的出现与发展。从磁卡发明到 20 世纪 80 年代，信用卡、出入证、借书证等使用磁性技术的证件大量出现，用以进行身份识别与信息记录。

第二阶段：带有集成电路芯片的智能电子证件的出现和发展。早在 1968 年德国发明家 Jurger Dethloff 和 Helmut Grotrupp 就提出了将集成电路加入身份识别卡中的设想，并于同年获得了专利权。1970 年，日本人 Kunitaka Arimura 也提出了类似的应用。1978 年，第一张采用 Siemens SIKART 晶片的身份识别及交易卡（Identification and Transaction Cards）诞生了。智能卡（IC 卡）将一个专用的集成电路芯片镶嵌于符合 ISO 7816 标准的 PVC（或 ABS 等）塑料基片中，封装成外形与磁卡类似的卡片形式即制成一张 IC 卡。当然也可以封装成纽扣、钥匙、饰物等特殊形状。

第三阶段：电子证件的无线化、网络化发展。从 20 世纪 80 年代至今，非接触 IC 卡（RFID）的出现是智能卡发展中的重要里程碑：它通过磁耦合或微波的方式来实现能量与信号的非接触传输，从而有效地解决了接触式智能卡使用机械电气触点产生的静电击穿、机械磨损、易受污染或潮湿环境影响等问题。被认为是身份识别、票据物流等方面的重要

替代技术。在计算机身份认证、互联网身份验证、电子商务及手机购物的身份认证等方面的需求推动下，含有电子证书及生物特征的电子证件得到快速发展，顺应了网络化发展的趋势。

三、电子证件的分类

目前的证卡主要分为：条码卡（包括一维条码和二维条码）、磁卡、IC 卡和 RFID 卡。表 1－1 给出了几种卡的性能对比。

表 1－1　　RFID 卡与条码、磁卡、IC 卡的性能对比

	信息载体	信息量	读写性	读取方式	保密性	智能性	抗干扰	寿命	成本
条码	纸、塑料薄膜等	小	只读	CCD 或激光束扫描	差	无	差	较短	最低
磁卡	磁性物质	一般	读/写	电磁转换	一般	无	较差	短	低
IC 卡	EEPROM	大	读/写	电擦除、写入	最好	无	较好	长	较高
RFID 卡	EEPROM	大	读/写	无线通信	最好	有	很好	最长	较低

非接触式 IC 卡又可分为逻辑加密 IC 卡和 CPU 卡。逻辑加密 IC 卡，即在非加密存储卡的基础上增加了加密逻辑电路，加密逻辑电路通过校验密码方式来保护卡内的数据对于外部访问是否开放，但只是低层次的安全保护，无法防范恶意性的供给。非接触式 CPU 卡，也称智能卡，卡内的集成电路中带有微处理器 CPU、存储单元（包括随机存储器 RAM、程序存储器 ROM、用户数据存储器 EEPROM）以及芯片操作系统 COS。装有 COS 的 CPU 卡相当于一台微型计算机，不仅具有数据存储功能，同时具有命令处理和数据安全保护等功能。几种 CPU 卡的对比如表 1－2 所示。

表 1－2　　几种 CPU 卡的对比

	加密技术	传输速率	卡容量（kB）	应　用
PIV	PIV-C. 1-C. 69 Cosmo 64 RSA Dual	106kbps	≥32	个人身份证卡等
CAC	RSA. DES	106kbps	≥32	军人身份卡、电子护照等
Inside Contactless	AES	106kbps	≥32	智能卡、身份卡、多用卡
Gemalto	RSA-2k、3-DES、AES、MD5 等	223kbps	80	智能卡、SIM、电子护照等
RFID	AES 和 SHA	650kbps	32～80	护照卡、EDL/EIC

基于 Java 的智能卡（又称为通用接入卡或 CAC 卡）被提供给现役、预备役、国民卫队军人和国防部文职人员，对经授权的用户提供全世界军事网站的物理接入，并允许其按一定模式进入国防部网络和计算机系统。当前，CAC 卡已经成为美国现役人员的标准身份证明，这种安全可靠、多功能的智能卡主要应用于体征鉴定以及军用设施和网络的通行证。

此为试读，需要完整PDF请访问：www.ertongbook.com