

# 智能卡

## 概念介绍

智能卡是一种可以存储数据用以和管理系统交互的卡片,管理系统通过对智能卡的写入、修改、读取和加解密来实现各种管理功能。通常智能卡用以绑定代表某一类事物并对其进行描述授权,比如:人员和物品。

智能卡可完成通行的钥匙、资金结算、考勤和某些控制操作,如可开启门禁、就餐、购物、停车、巡更、办公等各项活动。使用越来越普及,它不仅有着不可替代的地位,而且也为了提高信息处理效率和系统安全性等方面做出了重要贡献。

在实际应用中根据用户需求可以选择只读式 ID 卡①、读写式 IC 卡②和加密管理 CPU 卡。

- 中文名: 智能卡 刷卡方式: 接触式卡、非接触式卡、双界面卡
- 英文名: Smart Card 主流芯片: M1 芯片、CPU 芯片、ICode2 芯片、Ti 芯片
- 应用领域: 物联网、门禁控制、考勤等领域

## 智能卡的由来

智能卡的名称来源于英文名词 Smart Card, 又称为集成电路卡。即 IC 卡 (Integrated Circuit card)。IC 卡的概念是 70 年代初提出来的, 1974 年法国人罗兰德·莫瑞诺 (Roland Moreno) 第一次将可进行变成设置的 IC 芯片放于卡片中, 使卡片具有更多的功能。当时他在专利申请书中, 对于这项发明做了如下阐述: 卡片上具有可进行自我保护的存储器。这样就诞生了世界上第一张 IC 卡。法国布尔 (Boole) 公司于 1976 年首先创造出 IC 卡产物。1984 年, 法国的 PTT (Posts,Telegraphs andTelephones) 将 IC 卡用于电话卡, 由于 IC 卡良好的安全性和可靠性, 获得了意想不到的成功。随后, 国际标准化组织 (ISO, International Standardization Organization) 与国际电工委员会 (IEC, International Electrotechnical Commission) 的联合技术委员会为之制订了一系列的国际标准、规范, 极大地推动了 IC 卡的研究和发展。

## 智能卡分类

## 1. 根据安全程度划分


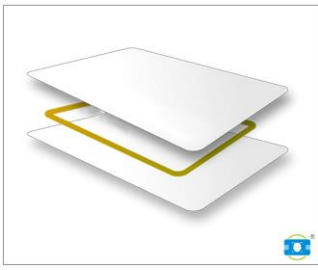
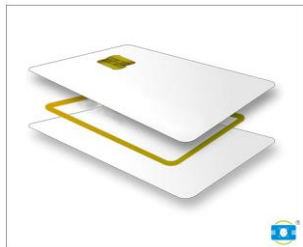
根据安全程度分类: 强加密、简单加密、无加密

	强加密: CPU 卡	简单加密: IC 卡	无加密: ID 卡
操作系统	带有 COS 系统	无 COS 系统	无 COS 系统
硬件加密模块	硬件 DES 运算模块	无	无
算法支持	标准 DES 算法	厂家专用不公开算法	无
密钥长度	16 字节 DES	12 字节口令	无
交易安全性	不可被非法访问; 与 PSAM 之间严格双向认证流程; 交易自动形成不可抵赖的 TAC 码	口令保护钱包, 不效验口令错误次数; 口令更换是明文可被截获, 卡片不能验证设备合法性	卡号在封卡前写入后不可再更改, 绝对确保卡号的唯一性和安全性
终端安全性	采用动态密钥, 密钥存储、交易验证与加密计算都由 SAM 卡独立完成, 安全有保障	采用固定密钥, 不支持 SAM 卡双向认证	数据存储采用 EEPROM, 数据保存时间超过 10 年;
多应用	支持多应用, 应用之间独立; 每个应用的 COS、容量、功能可自行定义, 可完全不同, 支持多种认证方式	简单支持多应用, 应用数量与每个应用容量有限	常用于门禁控制
容量	4Kbyte-80Kbyte	8Kbyte	数据存储容量共 64 位, 包括制造商、发行商和用户

			代码
空间分配	文件方式，任意大小自由分配，并可灵活设置访问条件	扇区方式，每区域64Kbyte，会造成空间浪费	无
数据完整性	支持断电保护和防插拔处理，由COS保证数据完整性	不支持断电保护，需要人为备份和恢复机制	无
通信速率	106Kbps，最高可达847Kbps	106Kbps	106Kbps

## 2. 根据刷卡方式划分

可以分为接触式和非接触式、双界面卡

	接触式	非接触式	双界面卡
外观样式			
介绍	芯片封装在PVC材料里层，但触点外露。需要与卡槽产生物理接触才能读取数据；	芯片依然封装在PVC材料里层，但是通过内置的线圈感应读写卡设备上的电波，从而实现非接触式的读写数据	集合接触式和非接触式接口融为一体，两种接口共享着相同的微控制器、操作系统、EEPROM。包含一个微控制器芯片和一个连接到微控制器的天线线圈。读写器产生的磁场提供能量，通过射频实现能量供应和数据传输。

			两个界面遵循两个不同的规范，接触界面符合两个不同的规范 ISO/IEC7816；非接触符合 ISO/IEC14443。使之成为一卡多用的载体。
符合标准	ISO/IEC7816 标准	ISO/IEC14443 标准	接触界面符合 ISO/IEC7816； 非接触符合 ISO/IEC14443。

### 3. 根据刷卡距离划分

根据刷卡距离划分可以分为:0cm、0-8cm、10cm-1M、10M、超远距离（读卡距离和读卡设备相关）。

	0cm	0-8cm	10cm-1M	10M	超远距离
常见类型	异形智能卡 (钥匙扣/ 滴胶卡)	ID/IC 芯片 (卡片式)	ICODE2、 Ti	915M	2.4G 有源 卡
工作频率	125KHZ	125KHZ、 13.56MHZ	13.56MHz	860 ~ 960MHz	2.4GHZ 和 5.8GHZ
传输速度	传输速度较低，感应距离较短，无法主动发送信号，需要读卡器供能。	感应距离远，传输速度较高，无法主动发送信号，需读卡器供能	传输速度较高，感应距离较远，一般不需要外接电源，由读卡器供能，	传输速度最快，感应距离最远	传输速度最快，感应距离最远， 自带电源功能，可主动发送信号
应用场景	门禁控制	校园卡、城市一卡通、 银行卡	物流仓储	无障碍会议 签到	高速 ETC 收费系统

--	--	--	--	--	--

## 异形智能卡

通常智能卡是国际标准尺寸（85.6mm\*54mm），随着市场上的不同需求，并可定制个性化可做任意形状，主要包括：滴胶卡、钥匙扣、腕带等。可封装各类智能芯片。

	滴胶卡	钥匙扣	腕带
外观			

## 智能卡主流品牌



## 智能卡应用

### 1. 智能卡在金融领域应用

《中国人民银行关于推进金融 IC 卡应用工作的意见》Q1 中，意味着我国银行卡将顺应国际潮流，加速从磁条卡时代向智能卡时代转换。

与使用磁条的传统银行卡相比较，选用智能卡安全性更高。与磁条卡不同，智能卡记录的信息是动态的，芯片是一台小型计算机，每次交易的效验值不同，所以被复制的可能性就很小。另外，磁条卡比较容易受到外界的干扰，比如手机、电视等放在一起太近会产生微波干扰，将会影响芯片的读取。

	磁条银行卡	芯片银行卡
存储容量	利用磁性载体记录字母与数字信息，	以芯片作为载体，根据芯片的型号不同容量也有差异。

	存储容量大约在 200 个字符;	小的容量几百个字符, 大的上百万个字符。
数据处理	只能存储信息用于读取, 无运算能力	具备处理器, 有运算能力可与终端交互
使用时寿命	易磨损容易被其他磁场干扰	具有防磁、防静电、防机械损坏和防化学破坏, 使用寿命长, 信息保存年限久
便利性	只能通过刷卡的方式并需要连接银行系统读取	有接触式、非接触式两种读取方式, 可快速支付。 而且可以不连接后台系统使用
造价	价格低廉	与磁条卡相对来说价格略高



## 2. 智能卡在社会保障卡领域应用

一代社保卡、二代社保卡、三代社保卡有什么差别?

1999 年 12 月全国首张社会保障卡在上海发行, 此阶段为第一代社会保障卡, 采用接触式 CPU 卡芯片, 功能从最初支持就医结算, 逐步形成“一卡多用、全国通用”的发展格局。2011 年, 人力资源社会保障部和中国人民银行联合推进社会保障卡加载金融功能, 此阶段为第二代社会保障卡, 在一个芯片中实现社会保障和金融双功能。第三代社保卡在 2017 年启动发行, 采用双界面、大容量 CPU 卡芯片, 增加数字证书, 进一步实现非接触读卡和安全规范用卡。

	第一代社保卡	第二代社保卡	第三代社保卡
芯片技术	接触式 CPU 卡	接触式 CPU 卡 32K 数据容量	双界面 CPU 卡 48K\80K+数据容量

	8k/16k 数据容量 符合社保卡 1.0 规范	符合社保卡 2.0 规范、金融 IC 卡 PBOC2.0 规范	符合社保卡 3.0 规范、金融 IC 卡 PBOC3.0 规范
安全技术	DES/SSF33 算法	DES/SSF33/RSA 算法	DES\SSF33\RSA\SM2\SM3\SM4 算法
主要应用	社会保障应用	社会保障应用、金融应用	社会保障应用、金融应用
终端设备	脱机、联机用卡 接触式读写卡	脱机、联机用卡 接触式读写卡	脱机、联机用卡 接触式、非接触式读写卡 互联网用卡

其他应用领域

政企单位

公司团体

公共安全类：临时身份证、居住证等

教育类：学生卡、图书借阅卡等

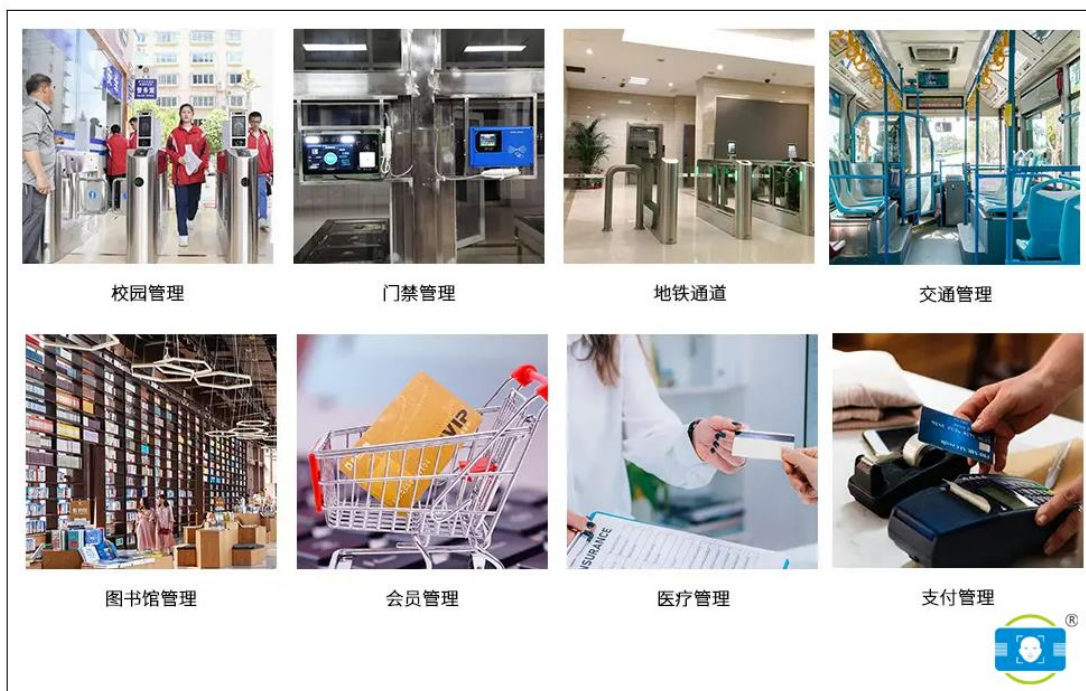
金融类：银行卡、医保卡、金融社保卡等

安防类：单位门禁卡、会议通行证等

交通类：交通卡

服务类：会员卡、积分卡等

社会服务类：健康证 Q2



注解:

只读式 ID 卡①:卡片在出厂时由厂家植入了一串全球唯一编码,此编码可以用以绑定某个人或者事物用以管理。通常可以用于小区楼宇门禁或者超市物品识别等。

读写式 IC 卡②: IC 卡芯片具有一定的容量, 可进行写入数据和存储数据的能力。

引用:

Q1 引用自[搜狐万柏林区食品药品监督管理局新闻 2019-02-22](#)

Q2 引用自《[中国人民银行关于推进金融 IC 卡应用工作的意见](#)》

免责声明:以上内容来源于网络公开信息和自撰, 如侵犯您的权利或是有不准确的描述请通知我们。我们将及时删除有关您的内容且我们不对内容的权威性负责。

声明:谢绝同业公司复制或转载, 非同业公司可下载使用, 请注明出处。