

目 录

1. 适用范围.....	3
2. IC 卡概述	4
2.1 卡片分类.....	4
3. Mifare 卡	6
3.1 Mifare 卡概述.....	6
3.2 Mifare 卡工作原理.....	6
3.2.1 Mifare 1 卡应用框图.....	6
3.2.2 Mifare 1 卡功能框图.....	7
3.3 Mifare 卡应用指南.....	9
3.3.1 一卡通与一卡多用.....	9
3.3.2 Mifare 1 卡应用实例.....	10
4. Mifare 1 卡 FAQ.....	13
4.1.1 Mifare 卡的读取距离通常是多少?	13
4.1.2 一张 Mifare 1 卡有多少个扇区?	13
5. 免责声明.....	14
6. 修订历史.....	15
7. 销售信息.....	16

1. 适用范围

本文对常用的射频 IC 卡做了简单的介绍，重点介绍了 NXP Mifare 卡的结构、工作原理和应用指南。本文可以对卡片的应用起到一定的指引作用，供使用 TX500 系列 MIFARE 卡读写模块的用户作为设计参考。

2. IC 卡概述

IC 卡（Intergrated Circuit Card，集成电路卡），又称为智能卡（Smart Card）。它将一个集成电路芯片镶嵌于塑料基片中，封装成卡片的形式，其外形与名片相似，如图 2-1 所示。



图 2-1 常见的卡片

实际上，根据实际需要，卡片可以封装成各种各样的形状，我们称之为异型卡，如图 2-2 所示，其中最后一种为透明封装的异型卡，可以清楚地看到卡片中封装了一个芯片和一个天线线圈。



图 2-2 异形卡

2.1 卡片分类

IC 卡根据其接口方式，分为接触式 IC 卡、非接触式 IC 卡和双介面 IC 卡，如表 2-1 所示。

表 2-1 IC 卡种类——根据接口方式

种类	示 例	说 明	优 点	缺 点
接触式		通过接触式的触点与读写器连接，进行取电和通信。	成本低，读写电路非常简单。	因为触点外露，容易被静电损坏，触点容易锈蚀。
非接触式		与读写器不接触，利用电磁场传递卡片工作所需能量和数据。	无外露触点，不易损坏。 非接触式刷卡，操作舒适。	需要专门的读写电路（芯片），成本较高。
双界面卡		既有接触式的接口，也有非接触式的接口。	结合了接触式和非接触式卡片的优点。 适用于各种场合。	芯片成本较高。

而根据卡中所嵌芯片的不同，又可以分为表 2-2 所示的三类。

表 2-2 IC 卡种类—— 根据内嵌 IC

种 类	特 点	常见卡片型号	应用场合
存储器卡	卡中 IC 为 EEPROM，可读写，没有任何加密特性。安全措施完全由用户处理。	AT24C02、AT24C04、AT24C08、AT24C16、AT24C32、AT24C64	安全性低的场合，例如考勤机里面事件记录的导出等。
逻辑加密卡	卡中的 IC 具有加密逻辑和 EEPROM。	Mifare 1 S50/S70、T5557、SLE4442	安全性中等的场合，例如智能卡水表、门禁、门锁等。
CPU 卡	卡中 IC 具有中央处理器 CPU、EEPROM、RAM 以及卡内操作系统 COS。是真正的“智能卡”。	Mifare PLUS、Mifare Pro、AT90SC3232CRF、AT05SC	安全性要求高的场合，例如金融、保险、交警、政府。

NXP 的 Mifare 1 卡是一种非接触式逻辑加密卡，其 RF 接口符合 ISO/IEC14443 Type A 标准，广泛应用于我们生活的各个方面。Mifare 卡正是本文介绍的重点。

3. Mifare 卡

3.1 Mifare 卡概述

NXP 半导体（由 PHILIPS 创建）是世界上最早研制非接触式 IC 卡芯片的公司之一，曾拥有国际市场上同类产品的六成以上的份额，对非接触式 IC 卡在全世界的推广使用起着不可替代的引导和推动作用。其代表性产品有：内含 1K/4K 字节 EEPROM 的逻辑加密卡芯片 Mifare Standard、384 位/64 字节 EEPROM 的缩减型逻辑加密卡芯片 Mifare Light 和 Mifare UltraLight、4K 字节 EEPROM 的 CPU 卡 Mifare DESFire，以及双界面卡芯片 Mifare PLUS、Mifare PRO 系列、Mifare Prox 系列和 Smart MX 系列。

这里主要介绍在全球影响最大、应用最广泛的 Mifare Standard 中的 Mifare 1 S50 卡芯片。为了便于描述，以下称为 Mifare 1 卡。

Mifare 1 卡主要特性：

- 符号国际标准 ISO/IEC14443 Type A；
- 工作频率 13.56MHz；
- 数据传输率 106kbps；
- 高度安全性：数据流加密传输，3 次相互认证的双向验证机制；
- 世界唯一的 32 位（4 字节）卡号；
- 一次典型完整处理时间 < 0.1S；
- 卡内 1K 字节 EEPROM 划分为 16 个扇区，每区 4 块，每块 16 字节，各个扇区可以独立采取多种形式的密钥保护，实现一卡多用和一卡通。

3.2 Mifare 卡工作原理

3.2.1 Mifare 1 卡应用框图

一个 Mifare 1 卡应用系统，至少包括三个部分：读写器（读写模块）、控制器和 Mifare 1 卡，如图 3-1 所示。

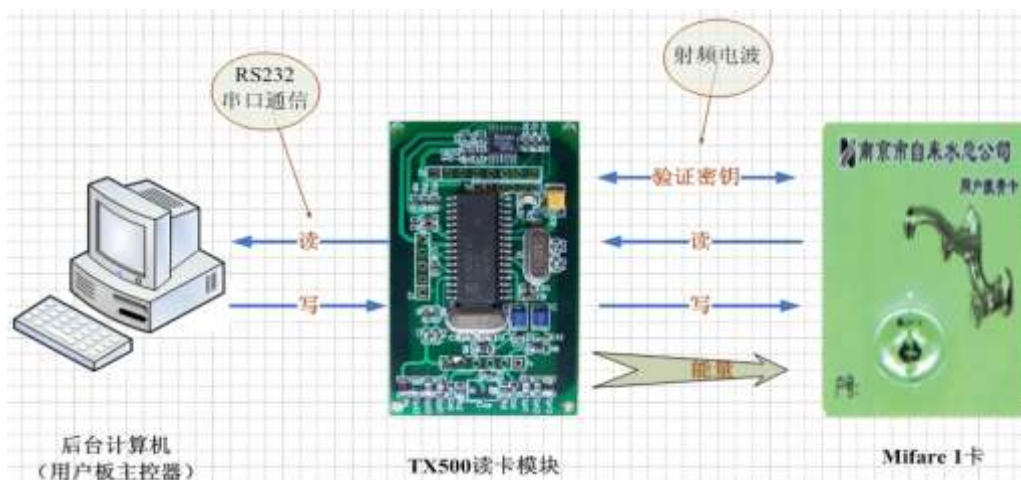


图 3-1 Mifare 卡应用系统框图

上图中，三个部分分工合作，缺一不可，各部分作用分述如下：

- **Mifare 1 卡：**存储数据，例如购水量、购电量等；
- **TX500 系列 MIFARE 卡读写模块：**通过射频电波为卡片提供工作所需能量，并与卡片进行通信，实现密钥验证、读卡、写卡等低级操作；同时，TX500 为后台计算机或者主控器提供读写卡片的高级接口，封装了读写卡片的复杂性；
- **后台计算机(或主控器)：**可以是 PC 或者单片机 80C51 等，通过串口或者 SPI 等与 TX500 系列 MIFARE 卡读写模块通信，控制其对卡片进行读写操作，可以把购水量、购电量等写入卡中，或者从卡中扣除购水量等，并实现整个系统的其他功能。

3.2.2 Mifare 1 卡功能框图

首先，我们把一张卡片的 PVC 膜剥开，看看其内部是什么样的，如图 3-2 所示。

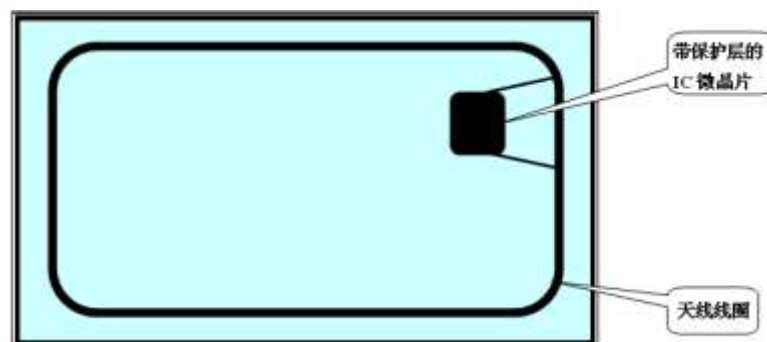


图 3-2 卡片内部结构

从上图可以看到，一张卡片里面实际上封装了一个天线线圈和一个 IC 芯片，这个芯片正是我们下面要详述的 Mifare 1 S50 智能卡芯片。Mifare 1 卡芯片的内部功能如图 3-3 所示。



图 3-3 Mifare 1 卡芯片功能框图

上图中，射频接口通过射频电波取得工作所需能量，并与 TX500 系列 MIFARE 卡读写模块通信；数字控制单元实现加密、认证与存取控制等功能，是整个 IC 的核心；存储器保存着各种应用数据和相应的密钥，这是我们在卡片应用中需要重点了解的部分，其他部分可参考 IC 数据手册。

Mifare 1 S50 卡的存储器空间分配如图 3-4 所示。

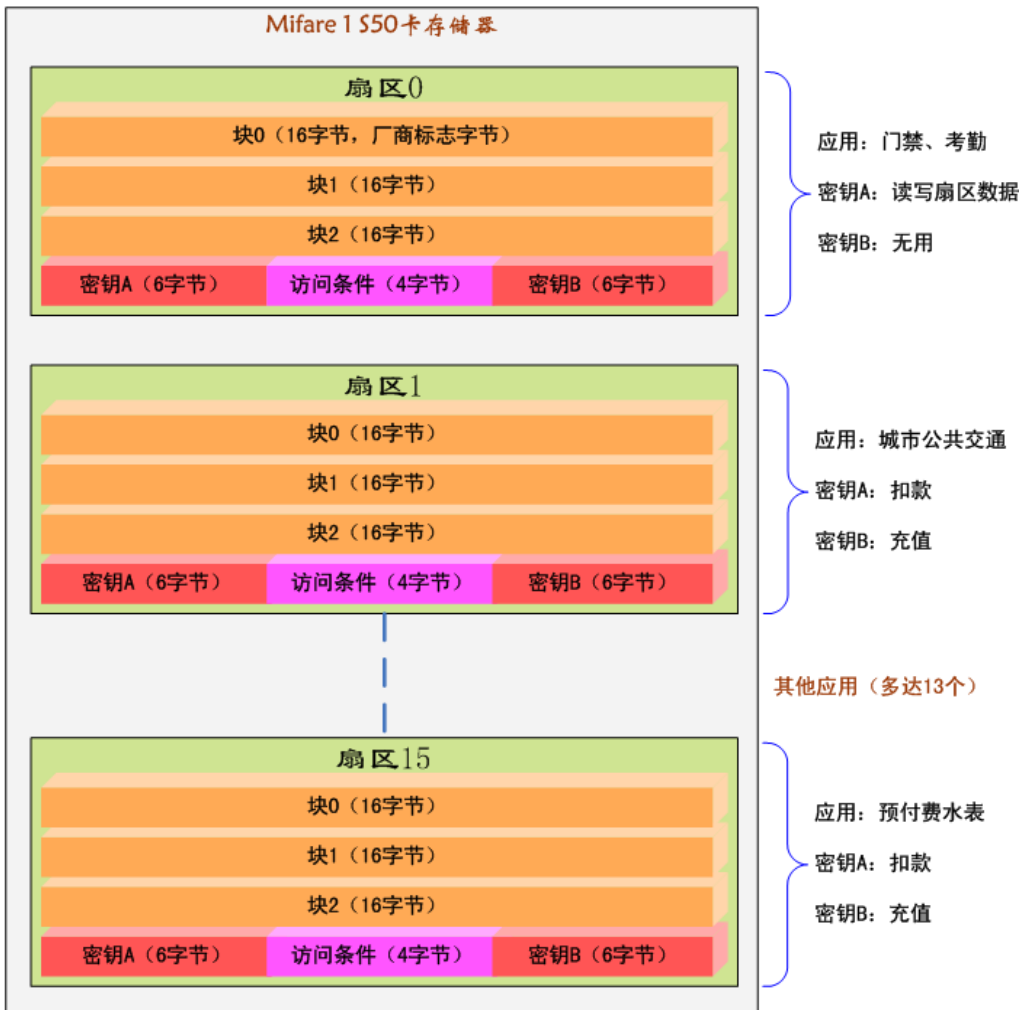


图 3-4 Mifare 1 S50 卡存储器结构

从图 3-4 可以看到，S50 卡的存储空间分为 16 个扇区（Sector），每区 4 块（Block），每块 16 字节。

各区的块 3 包含本扇区的密钥 A、密钥 B 以及本扇区各块的访问条件。除 0 区块 0 外的其余 3 块均用于数据存储。

0 区的块 0 存放着不可改变的厂商代码，其中前面 4 个字节为卡号（序列号 SN）。

从图 3-4 还可以看到，一张 Mifare 1 S50 卡可以同时用于 16 种不同的应用，例如门禁考勤、公交、预付费水表等。每个应用都是完全独立的，拥有独立的两套密码：密钥 A 和密钥 B。所有的应用只是共用“射频接口”和“数字控制单元”。实际上，每个应用可以把这张卡片看成完全属于本应用系统的，与其它的 application 没有任何关系。这就是我们所说的“一卡多用”。

3.3 Mifare 卡应用指南

Mifare 1 卡的高安全性、高速数据传输的特性，特别是其可以同时用于多达 16 个不同应用系统的特性，使其在国内的应用迅速普及。目前，Mifare 1 卡广泛应用于以下领域：

- 公共交通系统：如公共汽车、地铁、出租车、轮渡等；
- 城市生活公用收费：如电话、电表、煤气表、水表等；
- 公用收费系统：如高速公路、路桥收费、码头、港口停泊、停车收费、娱乐场所等的刷卡系统，实现不停车收费等更便捷的收费方式；
- 金融、证券领域：如银行、邮政、电信、证券交易、商场消费等；
- 出入口管理系统：如上岗管理、考勤管理、门禁管理等。

3.3.1 一卡通与一卡多用

随着 IC 卡的普及应用，人们对“一卡通”和“一卡多用”这两个词已经不再陌生，且往往不加区分地混为一谈。实际上，它们是在概念和作用形式上既有共性，又存差异的两种应用思路。它们的差异首先表现于：卡数据的共享。如图 3-5 和所示。

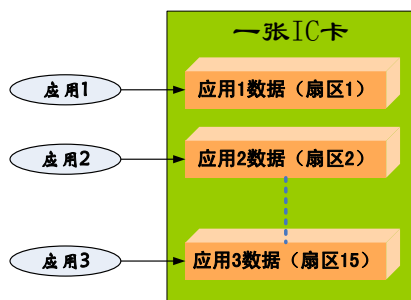


图 3-5 一卡多用

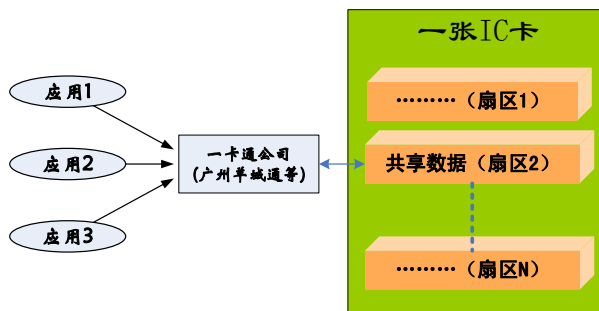


图 3-6 一卡通

“一卡多用”是把不同应用目的的数据分别放在一张卡片的各个扇区，每项应用只能通过自己的密钥独立访问指定扇区。各应用相互独立，互不影响。如图 3-5 所示。

“一卡通”也将不同应用的数据存放在一张卡上，但某些数据可以被不同类型的应用共享。如公交一卡通上的“电子钱包”中的储值就可以用于公交汽车、地铁和出租车等公共交通工具的付费。当然，这些应用的结算管理必须由一个中间管理机构（例如一卡通公司）统一进行，如图 3-6 所示。

表 3-1 为“一卡通”与“一卡多用”两种应用模式的进一步对比。

表 3-1 “一卡通”与“一卡多用”的对比

	一卡多用	一卡通
数据在同一卡否	是	是
应用数据共享否	否	是
卡管理统一否	否	是
个人化信息统一否	否	是
统一充值否	否	是
各类应用的消费/使用	分开	分开
卡的挂失/解挂	简单	麻烦
各类应用间的关系	无	有
各类应用的安全入口（密钥）统一否	否	是

显然，由于一卡通模式下的数据共享（互通），导致不同应用间的相互关联和影响，以致“一卡通”的实施难度远较“一卡多用”大。此外，有些应用希望通过数据共“通”，为用户提供最便利的服务；但另有些却要求数据的独享性和独立的密钥，以保护用户和业主的利益。因此，实际应用中对二者的取舍，应根据实际需要确定，并可采取先“一卡多用”，条件成熟再过渡的渐进办法。在同一卡上，也可采取部分应用“一卡通”，另一些应用“一卡多用”的两类模式并存方式。

3.3.2 Mifare 1 卡应用实例

国内最大的一卡通应用，就是城市公交一卡通系统。我们就以此为例来说明 Mifare1 卡的应用。先来看一下公交一卡通的体系结构，如图 3-7 所示。

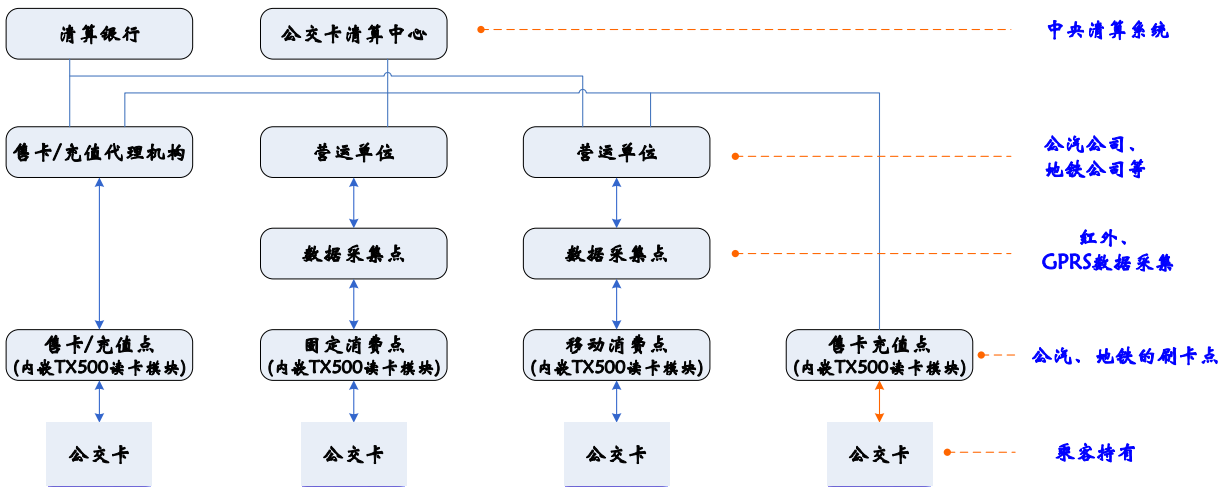


图 3-7 公交一卡通体系结构

- 从图 3-7 可以看到，整个体系结构由上到下分为五层：
- **中央清算系统：**系统的第一层。由清算中心和清算银行组成。前者负责卡片发行、运营管理、业务清算和密钥的生成/发行/管理等；后者根据前者提供的清算结果，对各营运单位和售卡充值结果的应收/应付款进行划拨等。
 - **营运层：**由营运单位和售卡充值代理机构组成。前者指公共汽车、地铁、轻轨、出

租车和轮渡等公共交通公司的控制结算中心；后者为提供售卡充值点的经营单位，可以是银行、超市或各营运单位，负责各售卡充值点营业资金的汇总和上缴清算银行，并将各售卡充值点的售卡和充值交易数据上报清算中心。

- **数据采集层：**由位于各营运公司基层的各个数据采集点组成。由于各行业营运方式的不同，所采取数据采集的形式亦多种多样。公共汽车通常是在每天收车回车库时用红外采集器或者微波采集器或大容量 IC 卡采集；地铁/轻轨则由各车站的车站计算机采集所辖车站设备的所有交易数据，并通过其专用通信线路，定时传送到地铁/轻轨结算中心；流动性大且无固定行车路线和规律的出租车，则应在取得一定交易数额后，去附近数据采集点由相应采集介质（IC 卡、便携式有线或无线采集器）进行数据采集及系统参数和黑名单等信息的装载。
- **充值/销售点：**售卡充值点可位于银行、超市或营运公司的营业场所，也可由清算中心在人流密集的地方自行设置。消费点有移动式与固定式之分，公共汽车和出租车为移动式；地铁、轻轨和轮渡为固定式。
- **交通卡：**为持卡人（乘客）持有的交通卡。

公交一卡通的最突出的例子就是香港八达通系统，虽然其主要采用 FeliCa 系列非接触式卡，但对于 Mifare 1 卡的应用具有同样的借鉴意义。该系统于 1997 年 9 月问世，当时仅可用于地铁、九广东铁、九广轻铁、九巴、城巴和香港小轮 6 种交通工具的乘坐。此后，八达通迅速向其它交通设施延伸，如图 3-8 所示。

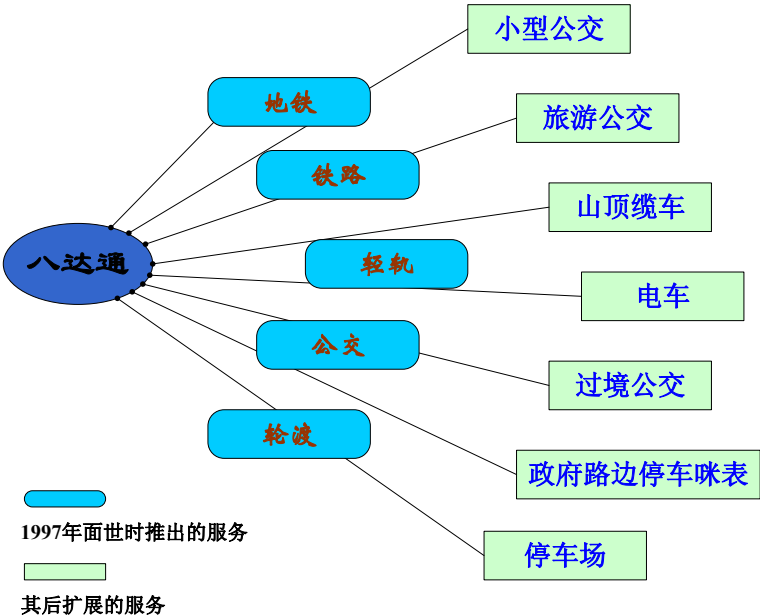


图 3-8 八达通 交通领域应用示意图

在逐步完善交通领域应用的同时，八达通又不断更新其应用层面，形成庞大的跨行业应用平台，如图 3-9 所示。

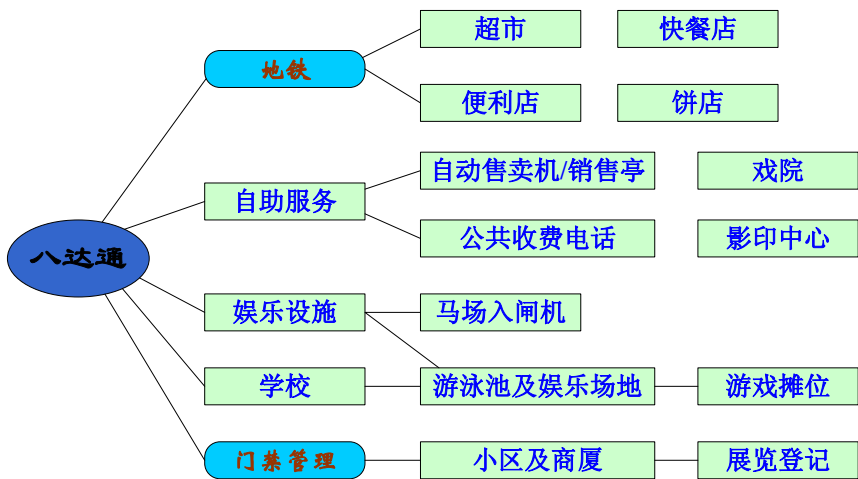


图 3-9 八达通 非公交领域应用示意图

现今八达通卡的发行量已经超过 1000 万枚，日交易量 800 万宗，涉及金额 5600 万港币。接受八达通卡的交通机构和商户已超过 253 家，且建立了近 2000 个分布广泛的充值点，安装有 3000 多台充值机，并与 19 家银行提供八达通自动充值服务，形成一个庞大高效的消费服务管理体系。