

# T/TTS

## 中国智能交通产业联盟标准

T/TTS 0043—2015

---

### 公交管理卡规范

**Bus Management Card Specification**

2015- 11- 23 发布

2016- 01- 01 实施

---

中国智能交通产业联盟 发布



# 目 次

目次 .....	I
前言 .....	II
1 管理卡种类 .....	1
2 管理卡结构图 .....	2
3 管理卡应用信息目录 .....	3
3.1 密钥文件 .....	3
3.2 公共应用基本信息文件 .....	4
4 管理卡数据应用目录 .....	4
4.1 密钥文件 .....	4
4.2 公交管理卡运营信息文件 .....	5
4.3 咪表管理卡运营信息文件 .....	7
5 说明 .....	9
5.1 预留文件 .....	9
5.2 管理卡运营信息文件读写描述 .....	10

## 前 言

本部分按照 GB/T 1.1-2009 给出的规则起草。

本标准由中国智能交通产业联盟提出并归口。

本标准于 2015 年 11 月首次发布，本次为首次发布。

本标准起草单位：广东岭南通股份有限公司、深圳市雄帝科技股份有限公司、大唐微电子技术有限公司、北京聚利科技股份有限公司。

本标准主要起草人：方晓洪、高天雷、程跃、桂杰。

# 公交管理卡规范

## 1 范围

本标准规定了公共交通的相关管理卡规范，如司机卡、线路卡、车辆卡等管理卡的文件结构、文件内容、内部数据格式等。

本标准适用于公共交通相关的管理卡。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0025.1-2005 《中国金融集成电路（IC）卡规范 第1部分 电子钱包/电子存折卡片规范》

JR/T 0025.2-2005 《中国金融集成电路（IC）卡规范 第2部分 电子钱包/电子存折应用规范》

JR/T 0025.8-2005 《中国金融集成电路（IC）卡规范 第8部分 与应用无关的非接触式规范》

JR/T 0025.9-2005 《中国金融集成电路（IC）卡规范 第9部分 电子钱包扩展应用指南》

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**管理卡记录 management card record**

终端产生的各类设置卡、司机卡等管理卡类的刷卡记录。

### 3.2

**终端 terminal**

在交易点安装、用于与IC卡配合共同完成交易的设备。它应包括接口设备，也可包括其它的部件和接口（如与主机的通讯）。

## 4 缩略语

BCD：二进码十进数（Binary-Coded Decimal）

HEX：十六进制（Hexadecimal）

PSAM：销售点终端安全存取模块(Purchase Secure Access Module)

- DES: 数据加密标准 (Data Encryption Standard)
- AID: 应用标识符 (Application IDentification)
- MF: 主文件(Master File)
- DDF: 目录专用文件(Directory Definition File)
- ADF: 应用专用文件(Application Definition File)
- ACK: 应用主控密钥(Application main Control Key)
- DACK: 外部认证密钥(Distribution Authentication Key)
- DAMK: 应用维护密钥(Distribution Application Maintenance Key)

## 5 管理卡种类

目前用到以下种类的管理卡，可扩充：

- a) 公交类管理卡
  - 线路管理卡
  - 车辆管理卡
  - 司机管理卡
  - 数据采集管理卡
- b) 咪表类管理卡
  - 管理员卡
  - 参数费率卡
  - 考勤卡
  - 采集卡

## 6 管理卡结构图

管理卡主要包括线路管理卡、车辆管理卡、司机管理卡、采集管理卡，这些卡均为 CPU 卡。根据树状的卡内文件结构，管理卡内的文件分为 3 类：主文件 MF、目录专用文件 DDF、应用专用文件 ADF，结构图如图 1 所示。

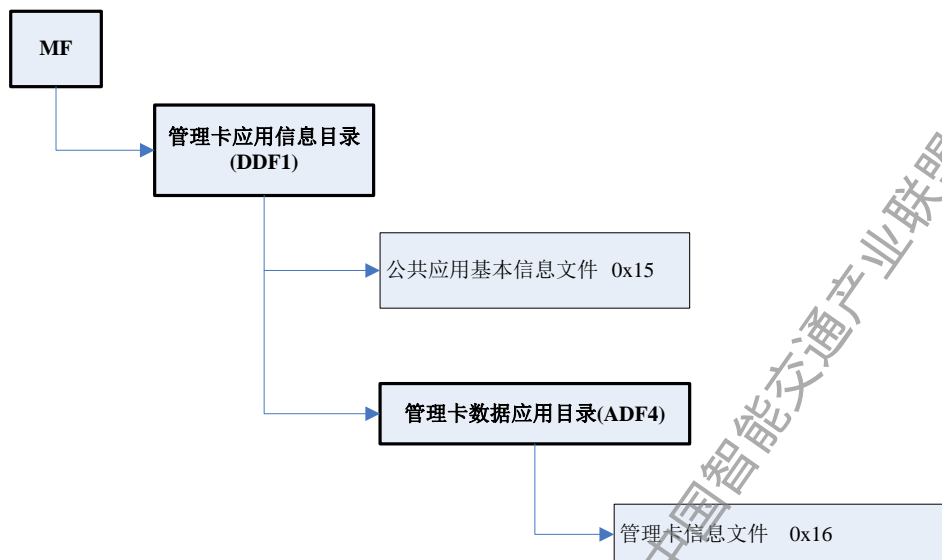


图 1 管理卡结构图

## a) 主文件 MF

在每一张卡片文件系统的文件树中都只存在着一个根文件，其他所有文件都是该文件的子文件。这个文件也是整个卡片的入口，称为 MF。每张卡片有且只有一个 MF。

## b) 专用文件 DF

DF 类似与 PC 文件系统中的目录文件，一般情况下，可以将 MF 看作是特殊的 DF。

为了标识不同的 DF，每一个 DF 具有一个同级 DF 下唯一的文件标识符和一个卡内全局唯一的应用标识符 AID。在实现上，文件标识符使用一个 WORD 类型的整数来标识，应用标识符 AID 使用一个有限长的二进制串作为该 DF 对应的应用的简单描述。

可以将 DF 分为 DDF 和 ADF 两类。

## 7 管理卡应用信息目录

应用标识符 AID: PAY.APPY (50 41 59 2E 41 50 50 59)

目录标识符: DDF1

## 7.1 密钥文件

DDF1 密钥文件表如表 1 所示。

表 1 DDF1 密钥文件表

文件存取控制	改写 = 安全报文，读取 = 禁止						
文件类型	线性定长文件			短文件标识		0x19	
文件内容	数据长度	密钥标识	后续状态	数据类型	尝试次数	备注	密钥权限
ACK	16	00	FF	HEX	3	应用主控密钥	
DAMK3	16	00	--	HEX	A	应用维护密钥 3	联机后台

## 7.2 公共应用基本信息文件

公共应用基本信息文件见表 2。

表 2 公共应用基本信息文件表

文件存取控制	改写 = 安全报文，读取 = 自由		
文件长度	88		
文件类型	二进制文件	短文件标识	0x15
文件内容	数据长度	数据类型	备注
发卡方标识	8	HEX	
城市代码	2	BCD	
行业代码	1	BCD	
逻辑卡号序列号	5	BCD	
卡类型	2	BCD	9500 城市运营中心管理卡
钱包标识	0.5	HEX	
版本	0.5	HEX	
卡认证码	4	HEX	
应用启用日期	4	BCD	YYYYMMDD
应用有效日期	4	BCD	
发行日期	4	BCD	
供货商代码	2	HEX	
芯片版本	2	HEX	
初始押金	4	HEX	
发行批号	2	HEX	
服务商代码	2	HEX	
发卡商	1	HEX	
区域代码	1	HEX	
区域卡序号	8	HEX	
区域卡类型	4	HEX	
区域备用	6	HEX	
扩展应用类型	2	HEX	
预留	21	HEX	

## 8 管理卡数据应用目录

应用标识符 AID: PAY.EXT1 (50 41 59 2E 45 58 54 31)

目录标识符: ADF4

## 8.1 密钥文件

ADF4 密钥文件表如表 3 所示。

表 3 ADF4 密钥文件表

文件存取控制	改写 = 安全报文, 读取 = 禁止						
文件类型	线性定长文件			短文件标识		0x19	
文件内容	数据长度	密钥标识	后续状态	数据类型	尝试次数	备注	密钥权限
ACK	16	00	FF	HEX	3	应用主控密钥	-
DACK4	16	01	44	HEX	A	外部认证密钥	读 (PSAM) 管理卡
DACK5	16	02	55	HEX	A	外部认证密钥	写 (PSAM) 管理卡
DAMK1	16	00	--	HEX	A	应用维护密钥 1	-
DACK1	16	03	EE	HEX	A	外部认证密钥	联机写
DACK2	16	04	22	HEX	A	外部认证密钥	联机写

DACK1: 预留文件 1 写用; DACK2: 预留文件 2 写用

## 8.2 公交管理卡运营信息文件

——注: 一阶段可以在“兼容备用”存储自定义信息。

### 8.2.1 车辆管理卡

车辆管理卡信息文件表如表 4 所示。

表 4 车辆管理卡信息文件表

文件存取控制	改写 = 外部认证, 读取 = 外部认证		
文件长度	1024		
文件类型	二进制文件	短文件标识	0x16
文件内容	数据长度	数据类型	备注
管理卡类型	1	BCD	01 车辆管理卡
车辆自编码	3	BCD	
启用日期	4	BCD	YYYYMMDD
运营公司代码	2	BCD	
信息认证码	4	BCD	
预留	242		
兼容备用	768		

车辆管理卡主要是对公交车辆进行管理, 车辆管理卡是一车一卡, 对应一个车牌号, 作为车辆在本系统内的唯一标识。

### 8.2.2 线路管理卡

线路管理卡的管理对象是公交线路。线路管理卡是一线多卡, 各卡内容一样, 作为冗余或同时使用。

线路管理卡作为线路在本系统内的唯一标识。AB 线、日夜班需等需以不同的编码体现。折扣率取值：0x00-0x64（0x00 为免费，0x64 为全价）

线路管理卡信息表如表 5 所示。

表 5 线路管理卡信息表

文件存取控制	改写 = 外部认证, 读取 = 外部认证		
文件长度	1024		
文件类型	二进制文件	短文件标识	0x16
文件内容	数据长度	数据类型	备注
管理卡类型	1	BCD	02 线路管理卡
线路自编码	3	BCD	
启用日期	4	BCD	YYYYMMDD
运营公司代码	2	BCD	
分公司代码	3	BCD	
信息认证码	4	BCD	
GPK_类型	1	HEX	0x02: PKI, 0x19:PSAM, 0x12: PKI+PSAM
消费参数	1	HEX	0x80: 正常消费
卡离线有效期启用	1	BCD	00 (不判断离线时间) 或 01 (需要判断离线时间)
卡离线有效期	1	BCD	以月为单位, 如: 学生卡离线时间 4 个月则填 0x04
服务商代码	2	HEX	
票价	2	HEX	低位在前, 高位在后
附加费	2	HEX	低位在前, 高位在后
区域代码+区域卡类	4*64=256	HEX (1)+HEX (2)	共 64 组区域卡类型 (低位在前)+折扣率, 每组
预留	229		
兼容备用	512		

### 8.2.3 司机管理卡 (操作员卡)

司机管理卡用于开关收费机、司机考勤。司机管理卡信息表如表 6 所示。

表 6 司机管理卡信息表

文件存取控制	改写 = 外部认证, 读取 = 外部认证		
文件长度	1024		
文件类型	二进制文件	短文件标识	0x16
文件内容	数据长度	数据类型	备注
管理卡类型	1	BCD	03 司机管理卡

表 6 司机管理卡信息表(续)

文件内容	数据长度	数据类型	备注
司机自编码	4	BCD	
启用日期	4	BCD	YYYYMMDD
运营公司代码	2	BCD	
信息认证码	4	BCD	
预留	241		
兼容备用	768		

#### 8.2.4 数据采集管理卡

数据采集管理卡的管理对象是收费机。是授权收费机可以进行数据采集的管理卡。数据采集管理卡信息表如表 7 所示。

表 7 数据采集管理卡信息表

文件存取控制	改写 = 外部认证, 读取 = 外部认证		
文件长度	1024		
文件类型	二进制文件	短文件标识	0x16
文件内容	数据长度	数据类型	备注
管理卡类型	1	BCD	04 采集管理卡
采集卡自编码	3	BCD	
启用日期	4	BCD	YYYYMMDD
运营公司代码	2	BCD	
信息认证码	4	BCD	
预留	242		
兼容备用	768		

#### 8.3 咪表管理卡运营信息文件

——注：一阶段可以在“兼容备用”存储自定义信息。

##### 8.3.1 管理员卡

管理员卡主要用于对咪表的复位，咪表管理卡信息表如表 8 所示。

表 8 咪表管理卡文件

文件存取控制	改写 = 外部认证, 读取 = 外部认证		
文件长度	1024		
文件类型	二进制文件	短文件标识	0x16
文件内容	数据长度	数据类型	备注

表 8 咪表管理卡文件(续)

文件内容	数据长度	数据类型	备注
管理卡类型	1	BCD	05 管理员卡
自编码	3	BCD	
启用日期	4	BCD	YYYYMMDD
运营公司代码	2	BCD	
信息认证码	4	BCD	
咪表商户编号	2	HEX	
预留	240		
兼容备用	768		

示例: 05 000006 20130619 0000 00000000 3501 +后续为 0。

### 8.3.2 参数费率卡

参数费率卡用于设置咪表的收费标准, 咪表参数费率卡文件如表 9 所示。

表 9 咪表参数费率卡文件

文件存取控制	改写 = 外部认证, 读取 = 外部认证		
文件长度	1024		
文件类型	二进制文件	短文件标识	0x16
文件内容	数据长度	数据类型	备注
管理卡类型	1	BCD	06 参数费率管理卡
自编码	3	BCD	
启用日期	4	BCD	YYYYMMDD
运营公司代码	2	BCD	
分公司代码	3	BCD	
信息认证码	4	BCD	
收费开始时间	2	BCD	HHMM
收费结束时间	2	BCD	HHMM
折扣率	1	HEX	0x00-0x64
单次最大停车费	2	HEX	单位: 分(低位在前, 高位在后)
最小收费时间	1	HEX	单位: 分钟
最小收费金额	2	HEX	单位分(低位在前, 高位在后)
起步免费泊车时间	1	HEX	单位: 分钟
夜间收费	2	HEX	单位分(低位在前, 高位在后)
单次最大泊车时间	1	HEX	单位: 小时
预留	479		
兼容备用	512		

示例: 06 000001 20130619 0000 000000 00000000 3501 0800 1600 50 8813 1E 6400 15 F401 E001+后续为 0。

### 8.3.3 考勤卡

考勤卡相当于公交司机卡, 用于考勤。考勤卡文件如表 10 所示。

表 10 考勤卡文件

文件存取控制	改写 = 外部认证, 读取 = 外部认证		
文件长度	1024		
文件类型	二进制文件	短文件标识	0x16
文件内容	数据长度	数据类型	备注
管理卡类型	1	BCD	07 考勤卡
自编码	4	BCD	
启用日期	4	BCD	YYYYMMDD
运营公司代码	2	BCD	
信息认证码	4	BCD	
咪表商户编号	2	HEX	
预留	239		
兼容备用	768		

示例: 07 000006 20130619 0000 00000000 3501 +后续为 0。

### 8.3.4 采集卡

采集卡文件如表 11 所示。

表 11 采集卡文件

文件存取控制	改写 = 外部认证, 读取 = 外部认证		
文件长度	1024		
文件类型	二进制文件	短文件标识	0x16
文件内容	数据长度	数据类型	备注
管理卡类型	1	BCD	08 采集管理卡
自编码	3	BCD	
启用日期	4	BCD	YYYYMMDD
运营公司代码	2	BCD	
信息认证码	4	BCD	
咪表商户编号	2	HEX	
预留	240		
兼容备用	768		

示例: 08 000006 20130619 0000 00000000 3501 +后续为 0

## 9 说明

### 9.1 预留文件

#### 9.1.1 预留文件 1

预留文件 1 信息见表 12。

表 12 预留文件 1 信息表

文件存取控制	改写 = 外部认证, 读取 = 自由		
文件长度	100		
文件类型	二进制文件	短文件标识	0x11
文件内容	数据长度	数据类型	备注

### 9.1.2 预留文件 2

预留文件 2 信息见表 13。

表 13 预留文件 2 信息表

文件存取控制	改写 = 外部认证, 读取 = 自由		
文件长度	100		
文件类型	二进制文件	短文件标识	0x12
文件内容	数据长度	数据类型	备注

## 9.2 管理卡运营信息文件读写描述

a) 两密钥均是二级分散, 分散因子如下:

第一级分散因子: 扩展应用类型 (2 字节) +6 字节固定值 (112233445566H)。

第二级分散因子: 物理卡号 (前 5 字节) + 厂商代码 (1 字节) + 逻辑号后 2 字节。

用专用指令 C4FE000000 获取卡片信息, 前 5 字节为物理卡号, 第 8 字节为厂商代码, 逻辑卡号  
请见本文档的 3 管理卡应用信息目录的 3.2 公共应用基本信息文件。

b) PSAM 中对应的密钥见表 14。

表 14 PSAM 中对应的密钥文件表

密钥应用范围	密钥	PSAM 应用目录	在 PSAM 卡中的密钥索引
读卡时所使用的密钥	28	1002	18
写卡时所使用的密钥	28	1002	19

c) PSAM 卡只进行一级分散处理, 二级分散时只做加密处理, 则需要对二级分散因子进行取反后, 同时将二级分散因子和二级分散因子的取反送入 PSAM 卡(80 FA 00 00 10 +因子 2+因子 2 的取反), PSAM 得到分散后的子密钥, 这时用该子密钥在终端内做 3DES 加密后, 再做外部认证。

中国智能交通产业联盟标准

**公交管理卡规范**

T/ITS 0043-2015

北京市海淀区西土城路 8 号（100088）

中国智能交通产业联盟印刷

网址：<http://www.c-its.org>

2015 年 11 月第一版 2015 年 11 月第一次印刷