

高速公路区域联网不停车收费示范工程暂行技术要求 第 6 部分

## 电子收费 IC 卡技术要求和数据格式

2008 年 8 月

# 目 次

1 范围.....	1
2 规范性引用文件.....	1
3 术语、定义和缩略语.....	1
4 用户卡技术要求.....	1
5 PSAM 卡技术要求 .....	2
6 用户卡数据格式.....	3
7 PSAM 卡格式 .....	3
8 数据编码定义.....	3

## 1 范围

本标准规定了道路电子收费应用中用于非现金支付的IC卡的数据格式及编码。

本标准适用于智能交通之电子收费系统及相关领域，即道路收费系统中的各种非现金收费应用，包括不停车电子收费系统及人工非现金收费系统等。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 16649 识别卡 带触点的集成电路卡

JR/T 0025-2005 中国金融集成电路（IC）卡规范

GB/T 2423 电工电子产品环境试验

ISO/IEC 14443-2000 识别卡 非接触式集成电路卡 近程卡（Identification cards - Contactless integrated circuit cards - Proximity cards）

《收费公路联网收费技术要求》

## 3 术语、定义和缩略语

### 3.1 术语和定义

下列术语和定义适用于本标准。

#### 3.1.1

用户卡 subscriber card

在道路收费系统中具有支付能力的CPU卡。根据应用和发行方法可以分为记账卡、储值卡等类型。

### 3.2 缩略语

下列缩略语适用于本标准。

COS 芯片操作系统（chip operating system）

IC 集成电路（integrated circuit）；

ISAM 充值安全存取模块（increase secure access module）

PBOC 中国人民银行（people bank of china）

PSAM 消费安全存取模块（purchase secure access module）

PPS 协议和参数选择（protocol and parameters selection）

## 4 用户卡技术要求

### 4.1 功能要求

本标准所定义的各种卡片应满足如下功能要求：

- 支持一卡多应用，各应用之间相互独立；
- 支持多种文件类型 包括二进制文件，定长记录文件，变长记录文件，循环文件；
- 在通讯过程中支持多种安全保护机制（信息的机密性和完整性保护）；
- 支持多种安全访问方式和权限（认证功能和口令保护）；
- 支持 JR/T 0025-2005 所规定的 Single DES、Triple DES 算法；
- 用户卡应支持 JR/T 0025-2005 中规定的电子钱包和电子存折功能；
- 用户卡应支持 JR/T 0025-2005 中规定的复合消费功能；
- 支持多级密钥分散机制，用分散后的密钥作为临时密钥对数据进行加密、解密、MAC 等运算，以完成终端与卡片之间的合法性认证等功能。

## 4.2 参数要求

- 非接触界面通讯速率应不低于 106kbps;
- 用户卡应支持 PPS, 握手通讯速率从 9600bps 开始, 可以支持更高通讯速率。
- 接触界面传输协议应支持 T=0 协议;
- 用户卡存储容量应不低于 8Kbytes;
- 接触界面复位信息 (ATR) 应支持 PPS 协议选择, 包括版本信息及历史字节;
- 非接触界面复位信息 (ATS) 应遵循 ISO14443;
- 交易记录符合联网收费技术要求的规定;
- 用户卡应支持短文件标识符选择目录方式;
- 非接触工作频率应为 13.56MHz $\pm$ 7kHz;
- 钱包消费交易在接触方式, 时钟 3.579MHz 时, 钱包消费交易 (消费/取现命令) 时间应小于 100ms;
- 应采用硬件 DES 协处理器和硬件真随机数发生器;

## 4.3 物理特性

本规范没有涉及的其它卡片物理特性应符合 GB/T 16649.1 和 ISO/IEC 10373-1 的规定。

### 4.3.1 环境条件

- a) 工作温度: 一般要求 -25℃ $\sim$ +70℃;
- b) 存储温度: -40℃ $\sim$ +70℃;
- c) 相对工作湿度: 5% $\sim$ 100%。

## 4.4 电气特性

- 用户卡在 1.8V $\sim$ 5.5V 之间应能正常工作;
- 卡片接触界面时钟最高应能够支持 10MHz 或更高;

## 4.5 其它要求

- 卡片应通过银行卡检测中心的检测;
- 双界面卡为单一芯片, 支持双接口, 保证接触方式和非接触方式访问的资源是一致的, 对与芯片的操作与操作方式无关。接触和非接触都可以对相同数据区读写, 可以对同一个电子钱包/电子存折操作;
- 卡片严格按照金融规范 (PBOC2.0) 中的指令和安全机制, 实现读写设备对多个厂商卡片的兼容

## 5 PSAM 卡技术要求

### 5.1 功能要求

- PSAM 卡应支持 JR/T 0025-2005 所规定的 PSAM 卡消费交易流程;

### 5.2 参数要求

- 接触界面传输协议应支持 ISO7816 T=0 协议;
- 接触界面复位信息 (ATR) 应支持 PPS 选择, 可以支持更高通讯速率;
- 应采用硬件 DES 协处理器和硬件真随机数发生器;

### 5.3 物理特性

- a) 工作温度: 一般要求 -25℃ $\sim$ +70℃;
- b) 存储温度: -40℃ $\sim$ +70℃;
- c) 相对工作湿度: 5% $\sim$ 100%;

### 5.4 电气特性

- PSAM 卡在 1.8V $\sim$ 5.5V 之间应能正常工作;

——卡片接触界面时钟最高应能够支持7.0MHz或更高；

5.5 其它要求

——卡片严格按照中国金融IC卡PSAM卡应用规范中的指令和安全机制,实现读写设备对多个厂商卡片的兼容；

6 用户卡数据格式

参照《公路联网收费技术要求》4.2.4。其中联网收费信息文件结构

补充说明：0019文件中第一个字节的值为AA，它的含义为“复合应用类型标识符”，为了使卡片在全国范围内通用，需要统一该标识，所以指定为一个固定的值‘AA’。

1	复合应用类型标识符	1	AA
---	-----------	---	----

7 PSAM 卡格式

参照《公路联网收费技术要求》4.2.5。

8 数据编码定义

参照《公路联网收费技术要求》4.3。

9 用户卡应用指令

用户卡指令应符合JR/T 0025-2005的规定，其中内部认证指令补充定义如下：

9.1 Internal Authentication（内部认证）

9.1.1 定义与范围

Internal Authentication命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

9.1.2 注意事项

在满足该密钥的使用条件时才能执行此命令。

9.1.3 命令报文

表1 Internal Authentication命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	88	-
P1	1	00	加密
		01	解密
		02	计算MAC
P2	1	XX	DES密钥标识号
Lc	1	XX	-
DATA	XX	XX...XX	认证数据
Le	1	00	-

说明：

- l P1=00，表示进行加密运算，密钥类型是DES加密密钥
- l P1=01，表示进行解密运算，密钥类型是DES解密密钥
- l P1=02，表示进行MAC运算，密钥类型是DES&MAC密钥

9.1.4 命令报文数据域

命令报文数据域的内容是应用专用的认证数据。

### 9.1.5 响应报文数据域

响应报文数据域的内容是相关认证数据，即DES运算的结果。

### 9.1.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表2 Internal Authentication命令响应状态码

SW1	SW2	意义
90	00	正确执行
61	XX	正确执行 XX表示响应数据长度。可用Get Response 命令取回响应数据。（仅用于T=0）
62	81	回送的数据可能有错
64	00	标志状态位未变
67	00	错误的长度
69	81	密钥与运算方法不匹配
69	82	不满足安全状态
69	85	不满足使用条件
6A	80	数据域参数不正确
6A	82	KEY文件不存在
6A	86	参数P1 P2不正确
94	03	密钥未找到