

高速公路区域联网不停车收费示范工程暂行技术要求 第 5 部分

电子收费 关键信息编码规则

2008 年 8 月

目 录

目录.....	I
1 OBU 的 MAC 地址编码规则	1
2 RSU 的 BeaconID 编码规则	1
3 合约 (Contract) 相关信息编码规则	1
3.1 ContractSerialNumber 编码规则	1
3.1.1 ESAMProviderID 编码规则	1
3.1.2 OBEProviderID 编码规则	1
3.1.3 ESAMIndividulID 编码规则	1
4 服务提供商编码规则	2
5 用户卡卡号编码规则	2
6 发卡方标识的编码规则	3
7 PSAM 序列号及终端机编号编码规则.....	4
8 分散代码规则	4

1 OBU 的 MAC 地址编码规则

《数据链路层》规定OBU采用4字节固定MAC地址，《应用层》标准附录A中在其ObuConfiguration定义了MAC地址的ASN.1数据类型macID为INTEGER(0..4294967295)。

由此，OBE的专用MAC地址可以使用4字节的二进制数进行编码。

OBE的专用MAC地址可划分为两个部分，如下图所示：

制造商代码	OBU 制造商内部编码
1B	3B

其中：

I 制造商代码

由“公路电子收费密钥管理及安全认证系统”建设单位统一管理，OBU制造商要提交书面申请，经核准后获取其唯一代码。

其取值范围为：0~255，其中：0~254分配给厂商，255保留做测试等用途。

I OBU制造商内部编码

由OBU制造商根据其生产、管理等方面的需要自行定义。其取值范围为：0~16777215 ($2^{24}-1$)。

2 RSU 的 BeaconID 编码规则

《应用层》标准附录A中定义了BeaconID的ASN.1数据类型为：

```
BeaconID ::= SEQUENCE{  
    manufacturerID      INTEGER(0..255),  
    individualID        INTEGER(0..16777215)  
}
```

建议其编码规则同OBU的MAC地址编码规则，即：

I manufacturerID采用“制造商代码”；

I individualID由RSU制造商根据其生产、管理等方面的需要自行定义。其取值范围为：0~16777215 ($2^{24}-1$)。

3 合约（Contract）相关信息编码规则

3.1 ContractSerialNumber 编码规则

《设备应用》标准中，定义ContractSerialNumber的ASN.1数据类型为：

```
ContractSerialNumber ::= SEQUENCE{  
    ESAMProviderID      HEX STRING SIZE (2)  
    OBESProviderID      HEX STRING SIZE (1)  
    ESAMIndividulID     HEX STRING SIZE (5)  
}
```

3.1.1 ESAMProviderID 编码规则

由“公路电子收费密钥管理及安全认证系统”建设单位统一管理ESAMProviderID的分配。

3.1.2 OBESProviderID 编码规则

由“公路电子收费密钥管理及安全认证系统”建设单位统一管理OBESProviderID的分配。

3.1.3 ESAMIndividulID 编码规则

该编码由ESAM厂商提供，要求同一厂商产品的编码不能相同。

4 服务提供商编码规则

“服务提供商标识”是指OBE-SAM中“系统信息文件”（EF01）中的第1~8字节，服务提供商标识由“公路电子收费密钥管理及安全认证系统”建设单位统一分配并登记备案。如服务提供商同时也是用户卡的发卡方，则OBU的“服务提供商”编码与“发卡方标识”的代码相同。

XX	XX	XX	XX	XX	XX	XX	XX
区域代码				服务提供商标识		保留	密钥分散标识

区域代码为各省、直辖市、自治区的唯一标识，用汉字表示。

服务提供商标识为省内服务提供商的唯一标识，由“公路电子收费密钥管理及安全认证系统”建设单位分配并登记。

密钥分散标识定义如下：

- 01- 通过两级分散得到卡片密钥，第一级采用区域代码（复制一次变为8个字节）作为分散因子，第二级采用CPU卡内部编号作为分散因子。
- 02- 通过三级分散得到卡片密钥，第一级采用区域代码（复制一次变为8个字节）作为分散因子，第二级采用运营商标识（补“F”变为8个字节）作为分散因子，第三级采用CPU卡内部编号作为分散因子。
- 03- 通过三级分散得到卡片密钥，第一级采用运营商标识（补“F”变为8个字节）作为分散因子，第二级采用区域代码（复制一次变为8个字节）作为分散因子，第三级采用CPU卡内部编号作为分散因子。

其它保留。

5 用户卡卡号编码规则

用户卡（包括储值卡和记账卡）的卡号对应JR/T 0025.2-2005（PBOC 2.0）附录C ED/EP应用的基本数据文件（EF）的表C.1 ED和EP应用的公共应用基本数据文件中11~20字节“应用序列号”。在公路电子收费应用中为“卡片发行基本数据文件（0015文件）”中的“卡片网络编号”（2B）+“CPU卡内部编号”（8B）。

其中，“卡片网络编号”由“公路电子收费密钥管理及安全认证系统”建设方统一编号；“CPU卡内部编号”由卡片发行商自行定义。

建议用户卡卡号整体采用压缩BCD码的编码方式，每字节表示两个数字，共20位（4+16）数字，并用于卡片的表面光刻打印。在卡片上光刻打印时，采用4个数字为一组的方式，组与组之间用一个空格隔开。

I “卡片网络编号”的编码规则

省级行政区划代码	运营商序号
1B	1B

“卡片网络编号”的第1个字节为“省级行政区划代码”（GB/T 2260-2002 中华人民共和国行政区划代码），如表1所示。

“卡片网络编号”的第2个字节为行政区域内“运营商序号”，北京ETC专营公司的序号为“01”。

北京国标IC卡的“卡片网络编号”为：“1101”。

I “CPU卡内部编号”的编码规则

“CPU卡内部编号”可表示16个数字（0~9），可划分为四个部分

表1 CPU卡内部编号的组成

初始化年份	初始化星期	卡片类型	卡片序列号
YY（1B）	WW（1B）	XX（1B）	XX（5B）

其中：

“初始化年份”和“初始化星期”用于表示卡片的批次。

“卡片类型编码”参照《公路联网收费技术要求》及IC卡格式国标中的有关规定：

表2 卡片类型编码

代码	含义
21	年 / 月票卡
22	储值卡
23	记帐卡
.....	保留
51	测试用年 / 月票卡
52	测试用储值卡
53	测试用记账卡

“卡片序列号”采用顺序编号的方式，可容纳9,999,999,999张卡片。

6 发卡方标识的编码规则

“发卡方标识”是指用户IC卡中“卡片发行基本数据文件”（0015文件）中的第1~8字节，发卡方标识由“公路电子收费密钥管理及安全认证系统”建设单位统一分配并登记备案。如发卡单位同时也是ETC系统运营商（发行OBU），则“发卡方标识”的代码与OBU的“服务提供商”编码相同。

XX	XX	XX	XX	XX	XX	XX	XX
区域代码				运营商标识		保留	密钥分散标识

区域代码为各省、直辖市、自治区的唯一标识，用汉字表示。

运营商标识为省内运营商的唯一标识，由“公路电子收费密钥管理及安全认证系统”建设单位分配并登记。

密钥分散标识定义如下：

- 01- 通过两级分散得到卡片密钥，第一级采用区域代码（复制一次变为8个字节）作为分散因子，第二级采用CPU卡内部编号作为分散因子。
- 02- 通过三级分散得到卡片密钥，第一级采用区域代码（复制一次变为8个字节）作为分散因子，第二级采用运营商标识（补“F”变为8个字节）作为分散因子，第三级采用CPU卡内部编号作为分散因子。
- 03- 通过三级分散得到卡片密钥，第一级采用运营商标识（补“F”变为8个字节）作为分散因子，第二级采用区域代码（复制一次变为8个字节）作为分散因子，第三级采用CPU卡内部编号作为分散因子。

其它保留。

7 PSAM 序列号及终端机编号编码规则

由“公路电子收费密钥管理及安全认证系统”建设单位统一编码。

8 分散代码规则

一级分散代码由“公路电子收费密钥管理及安全认证系统”建设方规定。二级分散代码由各省（直辖市）自行定义，该级分散可选。用户卡分散采用CPU卡内部编号；ESAM（OBU）分散采用合同序列号。