附录 3：

全国高速公路电子不停车收费联网

用户卡、ESAM 文件结构和数据定义

交通运输部路网监测与应急处置中心

交通运输部公路科学研究院

北京市首都公路发展集团有限公司

2014 年 9 月

目 录

第一章 用户卡文件结构和数据定义

1.1 用户卡文件结构

（1） 文件结构图

所有用户卡必须建立以下文件，结构见图 1.1-1。

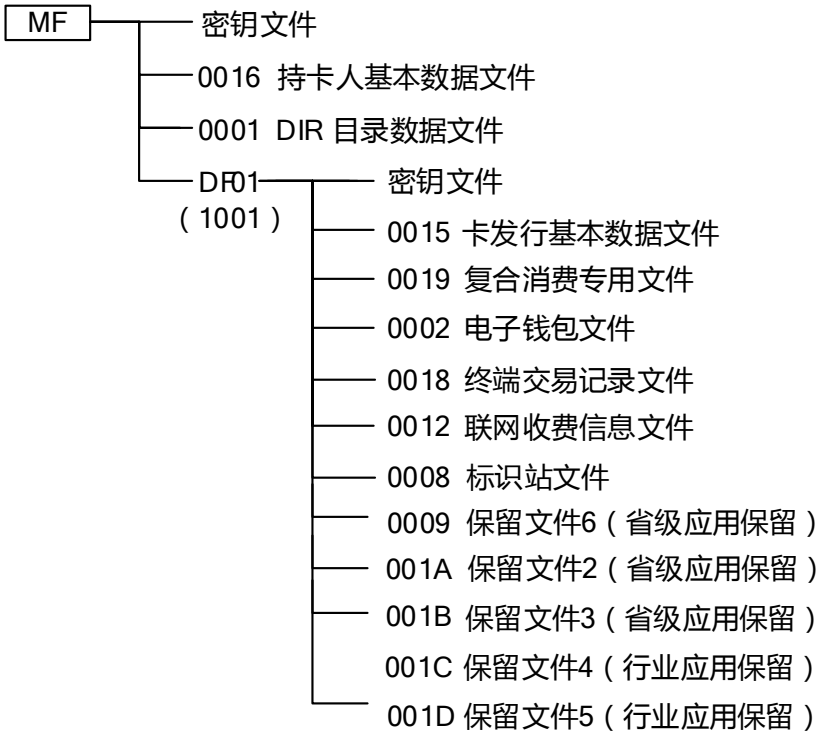

图 1.1-1 用户卡文件结构图

（2） 文件结构说明

用户卡详细文件说明见表 1.1-1。

表1.1-1 用户卡详细文件结构

文件名称	文件类型	文件标识符	读权	写权	备注
MF	主文件	3F00	建立权：$MK_{\_MF}$		厂商交货时已经建立

密钥文件	密钥文件	--	禁止	增加密钥权：$MK_{\_MF}$	禁止读，通过卡片主控密钥 $MK_{\_MF}$ 采用密文+MAC 方式写入密钥
持卡人基本数据文件	二进制文件	0016	自由	$DAMK_{\_MF}$	自由读，写时使用卡片维护密钥 $DAMK_{\_MF}$ 进行线路保护（明文+ MAC）
DIR 目录数据文件	变长记录	0001	自由	$DAMK_{\_MF}$	自由读，写时使用卡片维护密钥 $DAMK_{\_MF}$ 进行线路保护（明文+ MAC）
DF01 联网收费应用目录	目录文件	1001	建立权 $MK_{\_MF}$	擦除权 $MK_{\_MF}$	卡片主控密钥 $MK_{\_MF}$ 认证通过后可以建立和擦除文件
密钥文件	密钥文件	--	禁止	增加密钥权 $MK_{\_DF01}$	禁止读，通过应用主控密钥 $MK_{\_DF01}$ 采用密文+MAC 方式写入密钥
卡片发行基本数据文件	二进制文件	0015	自由	$DAMK_{\_DF01}$	自由读，写时使用应用维护密钥 $DAMK_{\_DF01}$ 进行线路保护（明文+ MAC）
联网收费复合消费过程文件	变长记录文件	0019	自由	$DAMK_{\_DF01}$	自由读，写时使用应用维护子密钥 $DAMK_{\_DF01}$ 线路保护（明文+ MAC）或 UPDATE CAPP DATA CACHE 方式写
电子钱包文件	专用钱包	0002	自由	COS 维护	读写权限与状态寄存器无关；自由读；消费子密钥 DPK 认证后可进行扣款；圈存子密钥 DLK 认证后可充值。

终端交易记录文件	循环文件	0018	PIN	不可写 COS 维护	PIN 验证通过后可读
联网收费信息文件	二进制文件	0012	自由	$UK_{\_DF01}$	自由读，外部认证 $UK_{\_DF01}$ 通过后可以写，无线路保护
标识站文件	二进制文件	0008	自由	$UK_{\_DF01}$	外部认证 $UK_{\_DF01}$ 通过后可以写，无线路保护
保留文件 6	二进制文件	0009	自由	自由	自由读，自由写
保留文件 2	变长记录文件	001A	自由	$DAMK_{\_DF01}$	自由读，写时使用应用维护子密钥 $DAMK_{\_DF01}$ 线路保护（明文+ MAC）或 UPDATE CAPP DATA CACHE 方式写
保留文件 3	变长记录文件	001B	自由	$UK_{\_DF01}$	外部认证 $UK_{\_DF01}$ 通过后可以写，无线路保护
保留文件 4	二进制文件	001C	自由	$UK_{\_DF01}$	外部认证 $UK_{\_DF01}$ 通过后可以写，无线路保护
保留文件 5	二进制文件	001D	自由	$UK_{\_DF01}$	外部认证 $UK_{\_DF01}$ 通过后可以写，无线路保护

（3） 应用要求：

a) 所有保留文件分为行业应用保留文件和省级应用保留文件，行业应用保留文件作为将来行业统一定义使用，各省（区、市）不得自行应用；省级应用保留文件各省（区、市）应严格按照要求建立，并可根据需要自行选择使用，为避免省域间发生冲突，使用前应向交通运输部路网监测与应急处置中心（以下简称“部路网中心”）报备。

b) DF01 应用目录下尚未定义的文件标识符，000A～000F（对应短文件标识符为 0A～0F）作为省级自定义应用保留，各省（区、市）可根

据需要自行定义文件类型、空间长度和操作权限等并使用，并应提前向部路网中心报备；其他短文件标识符作为行业应用保留，各省（区、市）不得应用。

c) 各省（区、市）不得自行更改统一定义的文件类型、空间长度和操作权限等，同时不得自行定义和使用文件中的行业预留字节，所有预留字节初始化时应写为 0xFF。

d) MF 文件下的应用目录文件标识符，1002～100F（DF02～DF0F）作为省级应用保留，各省（区、市）可根据需要建立和使用；其他应用目录文件标识符作为行业应用保留，各省（区、市）不得自行使用；对于有需要拓展使用应用目录文件的省（区、市），应提前向部路网中心报备。

e) 考虑到各省（区、市）不同的应用扩展，将保留文件 2（001A）作为省级应用保留文件。用于实现各省（区、市）对所有的卡片（包含外省（区、市））进行读写操作，通过复合消费指令完成，以变长记录的形式保存；其中复合应用类型标识符指定为各省（区、市）行政区划代码，以区分各省（区、市）的不同应用；各省（区、市）在卡片初始化时应提前为全国 34 个省（区、市）建立标识记录。

f) 考虑到各省（区、市）不同的应用扩展，将保留文件 3（001B）作为省级保留文件。用于实现各省（区、市）对所有的卡片（包含外省（区、市））进行读写操作，通过外部认证完成，以变长记录的形式保存；其中应用类型标识符指定为各省（区、市）行政区划代码，以区分各省（区、市）的不同应用；各省（区、市）在卡片初始化时应提前为全国 34 个省（区、市）建立标识记录。

g) 考虑到部分省（区、市）对路径精确标识的需求，启用全国统一预留文件中的 0008 文件作为标识站应用文件，供实施路径精确标识的省（区、市）使用。

h) 保留文件 4（001C）、保留文件 5（001D）为行业应用保留文件，可通过外部认证完成写入，各省（区、市）不得自行使用。

i) 针对本次全国联网，增加保留文件 6（0009），作为省级应用保留文件。

j) 用户卡文件结构的技术解释由交通运输部公路科学研究院负责。

1.2 数据文件说明

（1） MF 文件下密钥文件

MF 下密钥文件结构见表 1.2-1。

表1.2-1 MF下密钥文件结构

密钥名称	密钥标识	密钥大小	错误计数器
卡片主控密钥 $MK_{\_MF}$	00	10H	3
卡片维护密钥 $DAMK_{\_MF}$	01	10H	3

密钥用途与用法：

a) 制造主密钥外部认证通过后，使用密钥更新命令将其替换成卡片主控密钥；

b) 卡片主控密钥在自身的控制下更新（密文+MAC）；

c) 卡片主控密钥外部认证通过后，可在卡片 MF 下进行文件创建（创建持卡人基本数据文件、DIR 目录数据文件等），并可以对 MF 下密钥文件进行更新；

d) 卡片维护子密钥在卡片主控密钥线路保护控制下装载、更新；

e) 卡片维护子密钥用于 MF 区域的应用数据（持卡人数据文件）维护，持卡人数据文件在卡片维护密钥的安全报文方式下（线路保护）写；

f) 卡片 DF01 下密钥文件的应用主控密钥在卡片主控密钥的线路保护控制下装载（密文+MAC）。

（2） DF01 联网收费应用目录下密钥文件

表1.2-2 DF01联网收费应用目录下密钥文件

密钥名称	密钥标识	密钥大小	算法标识	错误计数器
应用主控密钥 $MK_{\_DF01}$	00	10H	00	3
应用维护子密钥 $AMK_{\_DF01}$	01	10H	00	3
内部认证子密钥 $IK_{\_DF01}$	00	10H	00	--

外部认证子密钥 UK_{DF01}	01	10H	00	3
消费子密钥 1 DPK1	01	10H	00	--
消费子密钥 2 DPK2	02	10H	00	--
圈存子密钥 1 DLK1	01	10H	00	--
圈存子密钥 2 DLK2	02	10H	00	--
TAC 子密钥 DTK	00	10H	00	--
应用 PIN PIN	00	06H	--	3
应用 PIN 解锁子密钥 $DPUK_{DF01}$	00	10H	00	3
应用 PIN 重装子密钥 $DRPK_{DF01}$	01	10H	00	3

说明：

a) 应用主控密钥在卡片主控密钥的线路保护控制下装载（密文+MAC）；

b) 应用主控密钥在自身的控制下更新（密文+MAC）；

c) 本密钥文件下其它密钥在应用主控密钥的线路保护控制下装载、更新（密文+MAC）；

d) 应用主控密钥外部认证通过后，可以在 DF01 目录下进行文件创建（密钥文件、卡片发行基本数据文件、联网收费信息文件、钱包文件、终端交易记录文件、保留文件等）；

e) 应用维护子密钥用于 DF01 区域的应用数据维护；

f) 内部认证子密钥用于终端设备验证卡片的合法性；

g) 外部认证子密钥认证通过后可对 DF01 下的联网收费信息文件、保留文件等进行更新；

h) 消费子密钥用于扣款认证操作，圈存子密钥用于充值认证操作，TAC 子密钥用于交易成功后产生 TAC 交易认证码；

i) 应用 PIN 为个人口令密钥，用于钱包充值及读取终端交易记录，PIN 码统一设为 ASCII 码“123456”。

（3） 持卡人基本数据文件

持卡人基本数据文件结构见表 1.2-3。

表1.2-3持卡人基本数据文件结构

文件标识符	0016		
文件类型	二进制文件		
文件主体空间	55 字节		
操作权限	自由读，$DAMK_{\_MF}$ 线路保护写（明文+MAC）		
字节	数据元	长度（字节）	说明
1	持卡人身份标识	1	自定义
2	本系统职工标识	1	自定义
3～22	持卡人姓名	20	持卡人姓名，编码见 GB 2312
23～54	持卡人证件号码	32	持卡人证件号码
55	持卡人证件类型	1	见《收费公路联网收费技术要求》

（4） 卡片发行基本数据文件

卡片发行基本数据文件结构见表 1.2-4。

表1.2-4卡片发行基本数据文件结构

文件标识符	0015		
文件类型	二进制文件		
文件主体空间	50 字节		
操作权限	自由读，$DAMK_{\_DF01}$ 线路保护写（明文+MAC）		
字节	数据元	长度（字节）	说明
1～8	发卡方标识	8	发卡方惟一标识，编码方式见《收费公路联网电子不停车收费技术要求》第二部分 1 关键信息编码
9	卡片类型	1	编码方式见《收费公路联网收费技术要求》表 4.3
10	卡片版本号	1	高 4 位：行业统一定义； 低 4 位：由各省根据需要自定义
11～12	卡片网络编号	2	编码方式见《收费公路联网电子不停车收费技术要求》第二部分 1 关键信息编码，如上海：3101

13～20	用户卡内部编号	8	编码方式见《收费公路联网电子不停车收费技术要求》第二部分 1 关键信息编码
21～24	启用时间	4	格式：CCYYMMDD
25～28	到期时间	4	格式：CCYYMMDD
29～40	车牌号码	12	全牌照 (汉字+字母+数字)信息，采用字符型存储，汉字采用 GB2312 码，如：“京”编码为“BEA9”； 牌照信息不足 12 字节，后补 0x00
41	用户类型	1	见 GB/T 20851.4 P20
42	车牌颜色	1	0x00 –蓝色；0x01–黄色；0x02 –黑色；0x03 –白色；0x04～0xFF 保留
43	车型	1	车型，编码方式见《收费公路联网收费技术要求》表 4.3
44～46	预留	3	行业应用保留
47～50	预留	4	省内自定义应用
说明： （1）依照本文件发行的卡片，版本高 4 位统一定义为“4”； （2）省内不得自行扩展该文件长度。			

（5） 联网收费复合消费过程文件

联网收费复合消费过程文件结构见表 1.2-5。

表1.2-5联网收费复合消费过程文件结构

文件标识符	0019
文件类型	变长记录文件
文件大小	576 字节

操作权限	自由读，写时使用应用维护子密钥 $DAMK_{\_DF01}$ 线路保护（明文+ MAC）或 UPDATE CAPP DATA CACHE 方式写		
字节	数据元	长度（字节）	说明
记录一：收费公路 ETC 专用记录（43 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xAA
2	记录长度	1	0x29
3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4～5	入/出口收费路网号	2	见《收费公路联网收费技术要求》表 4.3
6～7	入/出口收费站号	2	见《收费公路联网收费技术要求》表 4.3
8	入/出口收费车道号	1	见《收费公路联网收费技术要求》表 4.3
9～12	入/出口时间	4	UNIX 时间（注）
13	车型	1	见《收费公路联网收费技术要求》表 4.3
14	入出口状态	1	见《收费公路联网收费技术要求》表 4.3
15～23	预留	9	由省内自定义应用
24～26	收费员工号	3	二进制方式存放入口员工号后六位
27	入/出口班次	1	MTC 车道收费班次
28～39	车牌号码	12	见《收费公路联网收费技术要求》
40～43	预留	4	收费公路 ETC 预留
预留字节			
预留应用记录 1（43 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xB1

2	记录长度	1	0x29
3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-43	记录内容	40	
预留应用记录 2（43 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xB2
2	记录长度	1	0x29
3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-43	记录内容	40	
预留应用记录 3（43 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xB3
2	记录长度	1	0x29
3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-43	记录内容	40	
预留应用记录 4（43 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xB4
2	记录长度	1	0x29
3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-43	记录内容	40	
预留应用记录 5（43 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xB5
2	记录长度	1	0x29

3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-43	记录内容	40	
预留应用记录 6（63 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xC1
2	记录长度	1	0x3D
3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-63	记录内容	60	
预留应用记录 7（63 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xC2
2	记录长度	1	0x3D
3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-63	记录内容	60	
预留应用记录 8（96 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0xD1
2	记录长度	1	0x5E
3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-96	记录内容	93	
预留应用记录 9（96 字节）			
1	复合应用类型标识符	1	为了使卡片在全国范围内通用，需要统一该标识，指定为固定值 0XD2
2	记录长度	1	0x5E

3	应用锁定标志	1	0x00: 未锁定；0x01: 已锁定；其他值：保留
4-96	记录内容	93	
说明：UNIX 时间是 UNIX 或类 UNIX 系统使用的时间表示方式，从格林威治标准时间 1970 年 1 月 1 日 0 时 0 分 0 秒起至现在的总秒数，不包括闰秒。			

（6） 电子钱包文件

电子钱包文件结构见表 1.2-6。

表1.2-6 电子钱包文件结构

文件标识符	0002		
文件类型	钱包文件，循环记录		
文件主体空间	COS 自定义		
操作权限	自由读，写权 COS 维护		
字节	数据元	长度（字节）	说明
COS 自定义	金额	COS 自定义	电子钱包当前金额

（7） 终端交易记录文件

终端交易记录文件结构见表 1.2-7。

表1.2-7 终端交易记录文件结构

文件标识符	0018		
文件类型	循环记录文件		
文件主体空间	记录长度为 23 字节，不少于 50 条交易记录		
操作权限	COS 管理，外部不可写，读取需要 PIN 验证		
字节	数据元	长度（字节）	说明
1～2	联机交易序号	2	用户卡内产生的交易流水号
3～5	透支限额	3	透支限额
6～9	交易金额	4	交易金额
10	交易类型标识	1	圈存；消费

11～16	终端机编号	6	通过网络标识的终端机惟一编码
17～20	交易日期	4	格式：CCYYMMDD
21～23	交易时间	3	格式：HHMMSS

（8） 联网收费信息文件

该文件为传统消费模式下的收费信息文件，在复合消费模式下无效，详细文件结构见表 1.2-8。

表1.2-8 联网收费信息文件结构

文件标识符	0012		
文件类型	二进制文件		
文件主体空间	40 字节		
操作权限	自由读，外部认证 UK_DF01 通过后可写		
字节	数据元	长度（字节）	说明
1～2	入口收费路网号	2	
3～4	入口收费站号	2	
5	入口收费车道号	1	
6～9	入口时间	4	UNIX 时间
10	车型	1	
11	入出口状态	1	
12～20	标识站	9	
21～23	收费员工号	3	
24	入口班次	1	
25～36	车牌号码	12	
37～40	预留	4	

（9） 标识站应用文件

标识站文件的文件结构见表 1.2-9。

表1.2-9 标识站应用文件的文件结构

文件标识符	0008

文件类型	二进制文件		
文件主体空间	128 字节		
操作权限	自由读，外部认证通过后明文写		
字节	数据元	长度（字节）	说明
1～128	保留	128	保留的应用扩展数据单元
说明：实施路径精确标识的省（区、市）收费车道入/出口应清除本文件内容			

（10） 保留文件 6

保留文件 6 的文件结构见表 1.2-10。

表1.2-10 保留文件6的文件结构

文件标识符	0009		
文件类型	二进制文件		
文件主体空间	512 字节		
操作权限	自由读，自由写		
字节	数据元	长度（字节）	说明
1～512	保留	512	保留的应用扩展数据单元

（11） 保留文件 2

保留文件 2 的文件结构见表 1.2-11。

表1.2-11 保留文件2的文件结构

文件标识符	001A		
文件类型	变长记录文件		
文件大小	1024 字节		
操作权限	自由读，写时使用应用维护子密钥 $DAMK_{\_DF01}$ 线路保护（明文+ MAC）或 UPDATE CAPP DATA CACHE 方式写		
字节	数据元	长度（字节）	说明

1	复合应用类型标识符	1	为了使卡片在全国范围内进行辨识，该标识指定为各省（区、市）行政区划代码，以区分各省（区、市）自定义应用，按照 GB/T 2260 编码，如北京市，编码为“11”
2	记录长度	1	
3	应用锁定标志	1	
4～30	记录内容	27	
31	复合应用类型标识符	1	天津市，编码为“12”
32	记录长度	1	
33	应用锁定标志	1	
34～60	记录内容	27	
……			依次建立各省（区、市）记录[注]
991	复合应用类型标识符	1	澳门特别行政区，编码为“82”
992	记录长度	1	
993	应用锁定标志	1	
994～1020	记录内容	27	
1021～1024	预留	4	

注：本文件应按以下顺序建立记录（省区市名称，代码）：

（1）北京市，“11”；（2）天津市，“12”；（3）河北省，“13”；（4）山西省，“14”；（5）内蒙古自治区，“15”；（6）辽宁省，“21”；（7）吉林省，“22”；（8）黑龙江省，“23”；（9）上海市，“31”；（10）江苏省，“32”；（11）浙江省，“33”；（12）安徽省，“34”；（13）福建省，“35”；（14）江西省，“36”；（15）山东省，“37”；（16）河南省，“41”；（17）湖北省，“42”；（18）湖南省，“43”；（19）广东省，“44”；（20）广西壮族自治区，“45”；（21）海南省，“46”；（22）重庆市，“50”；（23）四川省，“51”；（24）贵州省，“52”；（25）云南省，“53”；（26）西藏自治区，“54”；（27）陕西省，“61”；（28）甘肃省，“62”；（29）青海省，“63”；（30）宁夏回族自治区，“64”；（31）新疆维吾尔自治区，“65”；（32）台湾省，“71”；（33）香港特别行政区，“81”；（34）澳门特别行政区，“82”。

（12） 保留文件 3

保留文件 3 的文件结构见表 1.2-12。

表1.2-12 保留文件3的文件结构

文件标识符	001B		
文件类型	变长记录文件		
文件大小	1024 字节		
操作权限	自由读，外部认证 UK_DF01 通过后可以写，无线路保护		
字节	数据元	长度（字节）	说明
1	应用类型标识符	1	为了使卡片在全国范围内进行辨识，该标识指定为各省（区、市）行政区划代码，以区分各省（区、市）自定义应用，按照 GB/T 2260 编码，如北京市，编码为“11”
2	记录长度	1	
3	应用锁定标志	1	
4～30	记录内容	27	
31	复合应用类型标识符	1	天津市，编码为“12”
32	记录长度	1	
33	应用锁定标志	1	
34～60	记录内容	27	
……			依次建立各省（区、市）记录[注]
991	复合应用类型标识符	1	澳门特别行政区，编码为“82”
992	记录长度	1	
993	应用锁定标志	1	
994～1020	记录内容	27	
1021～1024	预留	4	

注：本文件应按以下顺序建立记录（省区市名称，代码）： （1）北京市，“11”；（2）天津市，“12”；（3）河北省，“13”；（4）山西省，“14”；（5）内蒙古自治区，“15”；（6）辽宁省，“21”；（7）吉林省，“22”；（8）黑龙江省，“23”；（9）上海市，“31”；（10）江苏省，“32”；（11）浙江省，“33”；（12）安徽省，“34”；（13）福建省，“35”；（14）江西省，“36”；（15）山东省，“37”；（16）河南省，“41”；（17）湖北省，“42”；（18）湖南省，“43”；（19）广东省，“44”；（20）广西壮族自治区，“45”；（21）海南省，“46”；（22）重庆市，“50”；（23）四川省，“51”；（24）贵州省，“52”；（25）云南省，“53”；（26）西藏自治区，“54”；（27）陕西省，“61”；（28）甘肃省，“62”；（29）青海省，“63”；（30）宁夏回族自治区，“64”；（31）新疆维吾尔自治区，“65”；（32）台湾省，“71”；（33）香港特别行政区，“81”；（34）澳门特别行政区，“82”。

（13） 保留文件 4

保留文件 4 的文件结构见表 1.2-13。

表1.2-13 保留文件4的文件结构

文件标识符	001C		
文件类型	二进制文件		
文件主体空间	255 字节		
操作权限	读写（自由读，外部认证密钥认证通过后可写）		
字节	数据元	长度（字节）	说明
1～255	保留	255	保留的应用扩展数据单元

（14） 保留文件 5

保留文件 5 的文件结构见表表 1.2-14。

表1.2-14 保留文件5的文件结构

文件标识符	001D
文件类型	二进制文件
文件主体空间	255 字节
操作权限	读写（自由读，外部认证密钥认证通过后可写）

字节	数据元	长度（字节）	说明
1～255	保留	255	保留的应用扩展数据单元

第二章 OBE-SAM 卡文件结构和数据定义

2.1 OBE-SAM 卡文件结构

（1）文件结构图

所有 OBE-SAM 必须建立以下文件，结构见图 2.1-1。

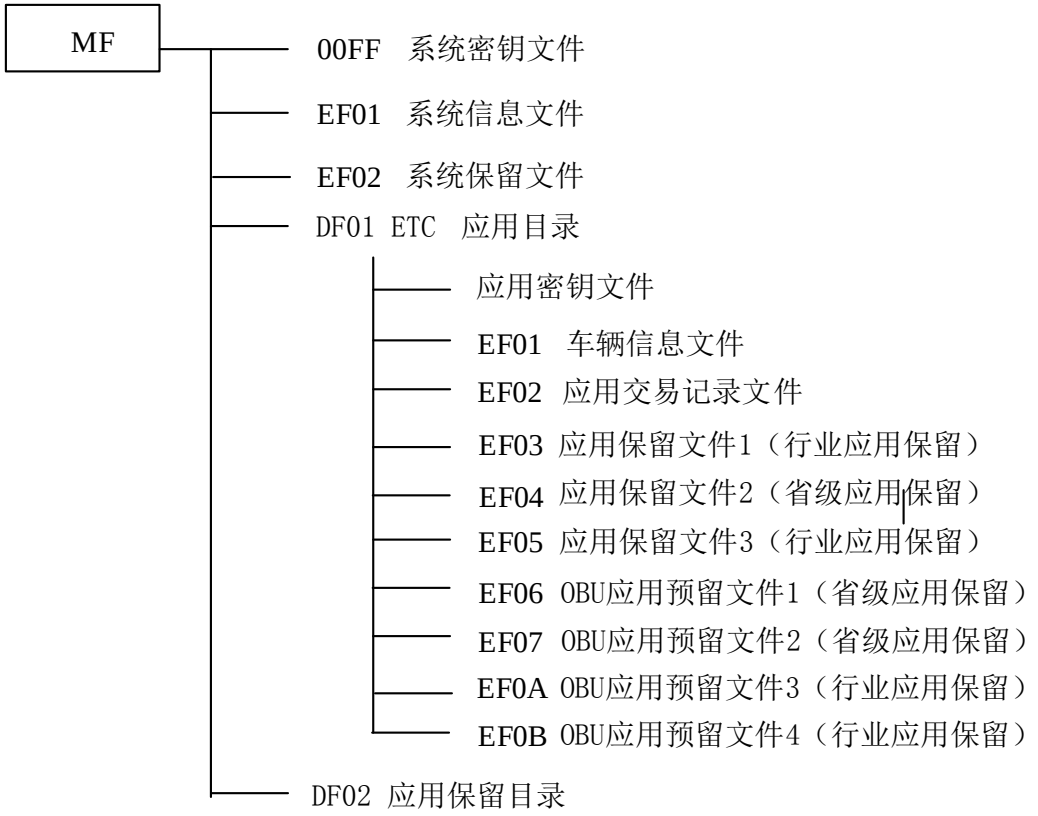

图 2.1-1 OBE-SAM 文件结构

（2）文件结构说明

OBE-SAM 详细文件说明见表 2.1-1。

表2.1-1 OBE-SAM详细文件结构

文件名称	文件类型	文件标识符	读权	写权	备注
MF	主文件	3F00	建立权：$MK_{\_MF}$		厂商交货时已经建立
密钥文件	密钥文件	--	禁止	增加密钥权：$MK_{\_MF}$	禁止读，通过卡片主控密钥 $MK_{\_MF}$ 采用密文+MAC 方式写入密钥
系统信息文件	二进制文件	EF01	自由	$DAMK_{\_MF}$	自由读，写时使用卡片维护密钥 $DAMK_{\_MF}$ 进行线路保护（明文+ MAC）
系统保留文件	二进制文件	EF02	自由	$DAMK_{\_MF}$	自由读，写时使用卡片维护密钥 $DAMK_{\_MF}$ 进行线路保护（明文+ MAC）
DF01 ETC 应用目录	目录文件	DF01	建立权 $MK_{\_MF}$	擦除权 $MK_{\_MF}$	卡主控密钥 $MK_{\_MF}$ 认证通过后可以建立和擦除文件
应用密钥文件	密钥文件	--	禁止	增加密钥权 $MK_{\_DF01}$	禁止读，通过应用主控密钥 $MK_{\_DF01}$ 采用密文+MAC 方式写入密钥
车辆信息文件	二进制文件	EF01	$RK2_{\_DF01}$ 线路保护	$DAMK_{\_DF01}$	$RK2_{\_DF01}$ 线路保护读，写时使用应用维护密钥 $DAMK_{\_DF01}$ 进行线路保护（明文+ MAC）
应用交易记录文件	循环定长记录文件	EF02	自由	自由	自由读，自由写

应用保留文件 1	二进制文件	EF03	自由	$DAMK_{\_DF01}$	自由读，写时使用应用维护密钥 $DAMK_{\_DF01}$ 进行线路保护（明文+ MAC）
应用保留文件 2	二进制文件	EF04	自由	自由	自由读，自由写
应用保留文件 3	二进制文件	EF05	认证读	$DAMK_{\_DF01}$	认证读，写时使用应用维护密钥 $DAMK_{\_DF01}$ 进行线路保护（明文+ MAC）
OBU 应用预留文件 1	二进制文件	EF06	自由	$DAMK_{\_DF01}$	自由读，写时使用应用维护密钥 $DAMK_{\_DF01}$ 进行线路保护（明文+ MAC）
OBU 应用预留文件 2	二进制文件	EF07	自由	自由	自由读，自由写
OBU 应用预留文件 3	二进制文件	EF0A	自由	认证写	自由读，外部认证 $UK_{\_DF01}$ 通过后可以写，无线路保护
OBU 应用预留文件 4	二进制文件	EF0B	自由	认证写	自由读，外部认证 $UK_{\_DF01}$ 通过后可以写，无线路保护

（3）应用要求：

a) 图 2.1-1 定义的所有保留文件分为行业应用保留文件和省级应用保留文件，行业应用保留文件作为将来行业统一定义使用，各省（区、市）不得自行应用；省级应用保留文件各省（区、市）应严格按照要求建立，并可根据需要使用，同时应向部路网中心报备。

b) 各省（区、市）不得自行更改统一定义的文件类型、空间长度和操作权限等，同时不得自行定义和使用文件中的行业预留字节，所有预留字节初始化时应写为 0xFF。

c) MF 文件下的应用目录文件标识符，DF02～DF0F 作为省级应用保留，

各省（区、市）可根据需要建立和使用，并应提前向部路网中心报备；其他应用目录文件标识符作为行业应用保留，各省（区、市）不得自行使用。

d) 应用保留文件 1（EF03）和应用保留文件 3（EF05），作为行业应用保留文件，各省（区、市）自定义应用不得自行使用；应用保留文件 2（EF04）作为省级应用保留文件。

e) OBU 应用预留文件 1（EF06）和 OBU 应用预留文件 2（EF07），作为省级应用保留文件。

f) 考虑到未来拓展应用，增加 OBU 应用预留文件 3（000A）和 OBU 应用预留文件 4（000B），作为行业应用保留文件，各省（区、市）自定义应用不得自行使用。

g) OBE-SAM 文件结构的技术解释由交通运输部公路科学研究院负责。

2.2 数据文件说明

（1）系统信息文件

系统信息文件详细说明见 02。

表2.2-2 系统信息文件说明

文件标识（FID）			‘EF01’
文件类型			二进制文件
文件大小			99 字节
读取：自由			写入：$DAMK_{\_MF}$ 线路保护（明文 + MAC）
字节	类型	长度（字节）	内容
1 – 8	cn	8	发行方标识，见《收费公路联网电子不停车收费技术要求》 第二部分 1 关键信息编码
9	cn	1	协约类型
10	cn	1	高 4 位：行业统一定义； 低 4 位：由各省根据需要自定义
11 – 18	cn	8	合同序列号

19– 22	cn	4	合同签署日期 格式：CCYYMMDD
23 – 26	cn	4	合同过期日期 格式：CCYYMMDD
27	B	1	拆卸状态
28 – 99	an	72	预留
说明： （1）依照本文件发行的 OBE-SAM，版本高 4 位统一定义为“4”； （2）省内不得自行扩展该文件长度。			

拆卸状态说明见03。

表2.2-3 拆卸状态说明

	值	状态	描述
高 4 位	0000	RS	由路侧根据防拆信息控制 OBU 的通行
	0001	OB	由 OBU 根据防拆信息设置自身工作状态
	1111	NU	防拆信息未启用
	注：其它值被保留		
低 4 位	0000	PF	标签已被非法拆卸
	0001	OK	正常工作状态
	注：其它值被保留		

（2）MF 下保留文件

MF 下保留文件详细说明见 04。

表2.2-4 MF下保留文件说明

文件标识（FID）			‘EF02’
文件类型			二进制文件
文件大小			512 字节
读取：自由			写入：DAMK $_{MF}$ 线路保护（明文 + MAC）
字节	类型	长度（字节）	内容
1 – 512	an	512	预留

（3）ETC 应用车辆信息文件

ETC 应用车辆信息文件详细说明见 05。

表2.2-5 ETC应用车辆信息文件说明

文件标识（FID）			‘EF01’
文件类型			二进制文件
文件大小			79 字节
读取：RK2_DF01 线路保护（密文）			写入：DAMK _DF01 线路保护（明文 + MAC）
字节	类型	长度（字节）	内容
1 – 12	an	12	车牌号，全牌照 (汉字+字母+数字）信息，采用字符型存储，汉字采用 GB2312 码，如：“京”编码为“BEA9”；牌照信息不足 12 字节，后补 0x00
13 – 14	an	2	车牌颜色 高字节： 00H 低字节：00H – 蓝色；01H – 黄色；02H – 黑色；03H – 白色
15	cn	1	车型，编码方式见《收费公路联网收费技术要求》表 4.3
16	cn	1	车辆用户类型，编码方式见 GB/T 20851.4 – 2007，P20
17– 20	cn	4	车辆尺寸（长[2 字节] X 宽[1 字节] X 高[1 字节]），单位：dm。
21	cn	1	车轮数
22	cn	1	车轴数
23 – 24	cn	2	轴距，单位：dm
25 – 27	cn	3	车辆载重/座位数，其中，载重的单位为：kg
28 – 43	an	16	车辆特征描述
44–59	an	16	车辆发动机号
60 – 79	b	20	保留字段

（4）ETC 应用交易记录文件

ETC 应用交易记录文件详细说明见 06。

表2.2-6 ETC应用交易记录文件说明

文件标识（FID）			‘EF02’
文件类型			循环定长记录文件
文件大小			57 字节×50 条记录
读取：自由			写入：自由
字节	类型	长度（字节）	内容
1 – 4	Datetime	4	出入口时间（UNIX 时间）
5—6	b	2	路网编码，见《收费公路联网收费技术要求》表 4.3
7– 8	b	2	收费站编码，见《收费公路联网收费技术要求》表 4.3
9	b	1	收费车道编码，见《收费公路联网收费技术要求》表 4.3
10	b	1	卡类型，见《收费公路联网收费技术要求》表 4.3
11-18	b	8	卡号
19	b	1	车型
20-31	b	12	车牌号
32-33	SmallInt	2	收费额
34-37	b	4	OBU 的 MAC 地址
38-57	b	20	保留字段

注：UNIX 时间是 UNIX 或类 UNIX 系统使用的时间表示方式，从格林威治标准时间 1970 年 1 月 1 日 0 时 0 分 0 秒起至现在的总秒数，不包括闰秒。

（5）应用保留文件 1

应用保留文件 1 详细说明见 07。

表2.2-7 应用保留文件1说明

文件标识（FID）			‘EF03’
文件类型			二进制文件
文件大小			512 字节
读取：自由			写入：$DAMK_{DF01}$ 线路保护（明文 + MAC）
字节	类型	长度（字节）	内容

1 – 512	an	512	预留

（6）应用保留文件 2

应用保留文件 2 详细说明见 08。

表2.2-8 应用保留文件说明

文件标识（FID）			‘EF04’
文件类型			二进制文件
文件大小			512 字节
读取：自由			写入：自由
字节	类型	长度（字节）	内容
1	an	1	路方所在省级行政区划代码，符合 GB/T 2260，采用压缩 BCD 编码
2-512	an	511	保留

（7）应用保留文件 3

应用保留文件 3 详细说明见 09。

表2.2-9 应用保留文件3说明

文件标识（FID）			‘EF05’
文件类型			二进制文件
文件大小			512 字节
读取：认证读（安全报文）			写入：$DAMK_{DF01}$ 线路保护（明文 + MAC）
字节	类型	长度（字节）	内容
1 – 512	an	512	预留

（8）OBU 应用预留文件 1

OBU 应用预留文件 1 详细说明见 0。

表2.2-10 OBU应用预留文件1说明

文件标识（FID）	‘EF06’
文件类型	二进制文件
文件大小	512 字节

读取：自由			写入：DAMK $_{DF01}$ 线路保护（明文 + MAC）
字节	类型	长度（字节）	内容
1 – 512	an	512	预留

（9）OBU 应用预留文件 2

OBU 应用预留文件 2 详细说明见 0。

表2.2-11 OBU应用预留文件2说明

文件标识（FID）			‘EF07’
文件类型			二进制文件
文件大小			512 字节
读取：自由			写入：自由
字节	类型	长度（字节）	内容
1 – 512	an	512	预留

（10）OBU 应用预留文件 3

OBU 应用预留文件 3 详细说明见 02。

表2.2-12 OBU应用预留文件3说明

文件标识（FID）			‘EF0A’
文件类型			二进制文件
文件大小			128 字节
读取：自由			写入：外部认证密钥认证通过后可写
字节	类型	长度（字节）	内容
1 – 128	an	128	预留

（11）OBU 应用预留文件 4

OBU 应用预留文件 4 详细说明见 03。

表2.2-13 OBU应用预留文件4说明

文件标识（FID）	‘EF0B’
文件类型	二进制文件
文件大小	512 字节

读取：自由			写入：外部认证密钥认证通过后可写
字节	类型	长度（字节）	内容
1 – 512	an	512	预留

2.3 OBE-SAM 内密钥说明

OBE-SAM 内密钥说明见 0。

表2.3-1 OBE-SAM内密钥说明

密钥	说明	用途	标识	版本	长度	分散级数
MF 下安全文件						
$MK_{\_MF}$	MF 主控密钥	00	00	00	16	0
$DAMK_{\_MF}$	MF 系统维护密钥	01	01	00	16	0
DF01 下安全文件						
$MK_{\_DF01}$	DF01 主控密钥	00	00	00	16	0
$DAMK_{\_DF01}$	DF01 应用维护密钥	01	01	00	16	0
$UK_{\_DF01}$	DF01 外部认证密钥	00	01	00	16	0
$RK1_{\_DF01}$	DF01 应用认证密钥	01	02	00	16	0
$RK2_{\_DF01}$	DF01 应用加密密钥	01	03	00	16	0
$RK2_{\_DF01}$	DF01 应用加密密钥	01	03	01	16	0
$RK2_{\_DF01}$	DF01 应用加密密钥	01	03	02	16	0

注：密钥用途说明。‘00’ 外部认证密钥，用于外部认证命令；‘01’ 传输密钥，用于数据传输时加密或计算 MAC。

2.4 OBE-SAM 内密钥管理

OBE-SAM 密钥管理见 0。

表2.4 -1 OBE-SAM密钥管理

分类	密钥	用途

主控密钥	$MK_{\_MF}$	控制 MF 下文件的建立和密钥的写入
	$MK_{\_DF01}$	控制 DF01 下文件的建立和密钥的写入
维护密钥	$DAMK_{\_MF}$	发卡方或应用提供方用于产生更新二进制文件或记录命令的 MAC
	$DAMK_{\_DF01}$	
外部认证密钥	$UK_{\_DF01}$	用于验证路侧设备的合法性
计算密钥	$RK1_{\_DF01}$	用于产生读二进制文件或记录命令的 MAC
计算密钥	$RK2_{\_DF01}$	用于加密读取车辆信息文件信息。

注：所有密钥的装载和修改应使用密文+MAC 的方式。

2.5 OBE-SAM 卡复位信息的约定

OBE-SAM 复位信息中历史字节的约定（共 15 字节）见 0。

表2.5-1 OBE-SAM复位信息的约定

名称	类型	长度（字节）	说明
交通运输部标识	an	1	固定为’4A’
芯片商注册标识号	an	2	芯片厂商注册标识
OBE 厂商标识	an	2	由收费公路电子收费密钥管理单位分配
COS 版本号	cn	1	主版本号+次版本号，范围 1.0~9.9
COS 修订版本号	cn	1	范围 0~99
YEAR	cn	1	生产年份
MON	cn	1	生产月份
DAY	cn	1	生产日
ESAM 结构版本	cn	1	ESAM 结构版本号
流水号	an	4	惟一性（在卡商内部）