高速公路电子不停车收费（ETC）系统国产密码算法迁移试点工程暂行技术要求

交通运输部公路科学研究院

2018 年 3 月

目　　录

前　　言

为规范和指导高速公路电子不停车收费系统国产密码算法迁移试点工程的建设实施，交通运输部公路局组织交通运输部公路科学研究院编制了《高速公路电子不停车收费（ETC）系统国产密码算法迁移试点工程暂行技术要求》，请试点省份参照执行。后续编制单位要在总结试点工程成功经验的基础上，再进行修订完善，以指导全国范围高速公路 ETC 系统国产密码算法迁移工程的建设实施。

该技术要求的管理权和解释权归交通运输部，日常解释和管理工作由主编单位交通运输部公路科学研究院负责。请各有关单位在实践中注意总结经验，及时将发现的问题和修改意见函告交通运输部公路科学研究院（地址：北京市海淀区西土城路 8 号，邮政编码 100088），以便修订时参考。

1 总体要求

高速公路电子不停车收费（ETC）系统国产密码算法迁移试点工程应符合以下要求：

（1）全国高速公路联网 ETC 系统应通过国产密码算法迁移实现从原来的 3DES 国际算法向 SM4 国产密码算法的转换。

（2）为确保系统稳定运行、平滑过渡，ETC 系统国产密码算法迁移采用路侧和车载“双兼容”方案，即过渡期内路侧系统和车载设备（含车载单元 OBU 和 CPU 用户卡）应同时支持 3DES 和 SM4 两种算法。

（3）在原部省两级密钥体系的基础上，新建部级在线密钥管理和服务平台，统一提供在线密钥管理服务。

（4） ETC 系统中涉及密码算法的关键设备和产品，包括 PSAM 卡、OBE-SAM 和 CPU 用户卡等，应符合 ETC 系统国产密码算法迁移相关技术标准。

（5）ETC 系统国产密码算法迁移流程按以下步骤进行：

第一步：先期改造密钥管理系统、发行系统、客服系统和清分结算系统，使其支持 SM4 国产密码算法。

第二步：面向社会发行同时支持 3DES 算法和 SM4 算法的车载设备；逐步实施收费车道交易系统改造，收费车道应实现对既有车载设备（3DES 算法）和过渡期内车载设备（3DES 和 SM4 算法）的支持。

第三步：待全国收费车道改造完成后，全国的发行系统不再发行同时支持 3DES/SM4 双算法的车载设备，只发行支持 SM4 算法的车载设备。

第四步：随着仅支持 3DES 算法的车载设备自然淘汰，收费车道系统可不再支持 3DES 国际算法的车载设备，进而实现全国高速公路联网 ETC 系统的密码国产化应用。

2 系统要求

2.1 一般规定

全国高速公路联网 ETC 系统国产密码算法迁移工程，应对以下系统进行升级和改造：

（1）部级密钥管理系统、部级在线密钥管理和服务平台。

（2）全国已联网 29 个省（区、市）的省级在线密钥管理系统、车道系统、发行系统、客服系统、清分结算系统。

2.2 部级密钥管理系统

部级密钥管理系统产生 SM4 算法的部级业务主密钥，生成对应的省级业务主密钥，制作 PSAM。

2.3 部级在线密钥管理和服务平台

新建部级在线密钥管理和服务平台，在线管理和分配省级在线密钥管理系统及密码服务资源，将部级统一生成的 SM4 算法省级业务主密钥导入省级在线密钥管理系统，同时为省级业务系统提供在线发行、充值、TAC 校验、PSAM 授权等服务，实现各类业务功能。

2.4 省级在线密钥管理系统

省级在线密钥管理系统作为部级在线密钥管理和服务平台的一部分，实现省级密钥管理，包括：原 3DES 算法密钥的导入，本省 SM4 算法根密钥、业务主密钥的生成/销毁等。

2.5 发行系统

发行系统包括电子标签发行系统和 CPU 用户卡发行系统，应实现 3DES 和 SM4 两套密钥的装载功能，并能够通过 SM4 算法对相关文件进行更新。发行系统应接入省级在线密钥管理系统。

2.6 客服系统

客服系统应能根据卡片版本号来判断 CPU 用户卡支持的算法，既能实现对原有 CPU 用户卡的充值，又能实现对双算法 CPU 用户卡的充值，若 CPU 用户卡支持 SM4 算法，则充值系统应优先选择 SM4 算法进行充值交易。

客服系统应接入省级在线密钥管理系统。客服系统的改造，包括自营网点系统、银行代理系统、银行 ATM 机、其它代理系统及充值终端软件的升级改造。

2.7 车道系统

车道系统在进行交易时，应能根据电子标签的合同版本及 CPU 用户卡的卡片版本号来判断其支持的算法，若电子标签或 CPU 用户卡支持 SM4 算法，则车道系统应优先选择 SM4 算法进行相关的安全认证和交易。交易记录应增加算法标识，用于清分结算系统区分交易记录所对应的算法。

增加 PSAM 在线授权功能，车道系统每次重新上电后，须连接到部级在线密钥管理和服务平台，获得 PSAM 使用权限，否则 PSAM 将无法使用。车道系统应每天定时向部级在线密钥管理和服务平台上报 PSAM 工作状态，部级在线密钥管理和服务平台定期自动生成 PSAM 工作状态报表。必要时，部级在线密钥管理和服务平台可主动查询指定 PSAM 的工作状态。

2.8 清分结算系统

清分结算系统应接入省级在线密钥管理系统，清算软件应能根据交易记录中的算法标识区分 3DES 算法和 SM4 算法产生的交易记录，并对其进行合法性验

证，产生正确的清分结算结果。

3 PSAM 卡数据格式和技术要求

3.1 一般规定

3.1.1 PSAM 卡基本功能应符合下列规定：

1. PSAM 卡应为具有 COS 的接触式 CPU 卡；
2. 应支持一卡多应用，且各应用之间相互独立；
3. 应支持多种文件类型，包括二进制文件、定长记录文件、变长记录文件、循环文件；
4. 在通讯过程中应支持多种安全保护机制（信息的机密性和完整性保护）；
5. 应支持多种安全访问方式和权限（认证功能和口令保护）；
6. 应支持 DES、3DES 和 SM4 算法；
7. 应支持多级密钥分散机制；
8. 应支持密钥使用权限设置；
9. PSAM 卡的应用安全机制应符合本标准附录 A 的有关规定；
10. PSAM 卡数据格式与应用命令应符合本标准附录 B 的有关规定。

3.1.2 PSAM 卡基本参数应符合下列规定：

1. 非易失性存储器容量应不低于 16Kbytes；
2. 卡片应支持 T=0 通信协议；
3. 卡片应支持多种速率选择，握手通信速率从 9600bit/s 开始，符合 PPS 协议，并应支持 57600bit/s 及以上的通信速率；
4. 卡片外部时钟频率应不低于 7.5MHz；
5. 卡片至少应支持工作电压：2.7V～3.3V，对应的工作电流应不超过 6mA；
6. 卡片工作温度：一般要求-25℃～+70℃（寒区-40℃～+70℃），存储温度：-40℃～+85℃，相对工作湿度：10%～95%；

7. 其他物理特性、电气特性应符合 GB/T 16649《识别卡 带触点的集成电路卡》的规定；

8. PSAM 卡安全等级应达到 GM/T 0008《安全芯片密码检测准则》规定的 2 级或以上级别。

3.2 PSAM 卡密钥规定

3.2.1 PSAM 卡中所有密钥都应以记录的形式存储在密钥文件中。

3.2.2 每一条密钥应具有用途、版本、算法标识、错误计数器、使用权限等属性。

3.2.3 密钥用途属性应符合表 4.2.3 的定义：

表 4.2.3 密钥用途定义

序号	密钥用途编码（二进制）	定义
1	xxx0 0000	主控密钥
2	xxx0 0001	维护密钥
3	xxx0 0010	消费密钥
4	xxx0 0110	MAC 密钥
5	xxx0 1000	MAC、加密密钥
6	xxx1 1001	MAC、解密密钥

注：

1. xxx 表示密钥分散级数，000 为不分散，001 为一级分散，010 为二级分散。

3.2.4 MF 下的密钥结构应符合表 4.2.4 的规定。

表 4.2.4 MF 下的密钥结构

密钥名称	密钥用途	密钥版本	密钥长度	算法标识	错误计数器	使用权限
PSAM 卡片主控密钥 $MK_{\_MF}$	00H	40H	10H	04H	3-15	自由
PSAM 卡片维护密钥 $AMK_{\_MF}$	01H	41H	10H	04H	3-15	自由
PSAM 卡片外部认证密钥 $UK_{\_MF}$	00H	41H	10H	04H	3-15	自由

注：

1. 卡片主控密钥在自身的控制下更新（密文+MAC）；
2. 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；
3. 卡片维护密钥在卡片主控密钥线路保护控制下装载、更新；

4. 卡片维护密钥用于 MF 区域的应用数据维护；

5. 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）。

3.2.5 DF01 下的密钥文件结构应符合表 4.2.5 的规定。

表 4.2.5 DF01 下的密钥结构

密钥名称	密钥用途	密钥版本	密钥长度	算法标识	错误计数器	使用权限
PSAM 卡应用 1 主控密钥 MK_{DF01}	00H	40H	10H	04H	3-15	自由
PSAM 卡应用 1 维护密钥 $AMK1_{DF01}$	01H	41H	10H	04H	3-15	自由
CPU 用户卡和 OBU 外部认证密钥 1 UK1	48H	01H	10H	00H	--	UK_{MF}
CPU 用户卡消费密钥 1 PK1	42H	01H	10H	00H	--	UK_{MF}
CPU 用户卡内部认证密钥 1 IK1	48H	03H	10H	00H	--	UK_{MF}
OBU 认证主密钥 1 RK1	48H	02H	10H	00H	--	UK_{MF}
OBU 加密主密钥 1 RK2	59H	03H	10H	00H	--	UK_{MF}
CPU 用户卡和 OBU 外部认证密钥 2 UK2	48H	41H	10H	04H	--	UK_{MF}
CPU 用户卡消费密钥 3 PK3	42H	41H	10H	04H	--	UK_{MF}
CPU 用户卡内部认证密钥 2 IK2	48H	43H	10H	04H	--	UK_{MF}
OBU 认证主密钥 2 RK3	48H	42H	10H	04H	--	UK_{MF}
OBU 加密主密钥 2 RK4	59H	43H	10H	04H	--	UK_{MF}

注：

1. 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. 应用主控密钥在自身的控制下更新（密文+MAC）；

3. 本应用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）；

4. 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；

5. 应用维护子密钥用于 DF01 应用下的应用数据维护。

4 OBE-SAM 数据格式和技术要求

4.1 一般规定

4.1.1 OBE-SAM 的基本功能应符合下列规定：

1. 应为具有 COS 的 CPU 芯片模块；
2. 支持一卡多应用，各应用之间相互独立；
3. 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；
4. 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）；
5. 支持多种安全访问方式和权限（认证功能和口令保护）；
6. 支持 DES、3DES 和 SM4 算法；
7. 支持拆卸状态设定功能；
8. OBE-SAM 的应用安全机制应符合本标准附录 A 的有关规定；
9. OBE-SAM 数据格式与应用命令应符合本标准附录 C 的有关规定。

4.1.2 OBE-SAM 的基本参数应符合下列规定：

1. 非易失性存储器容量应不低于 16Kbytes；
2. 卡片应支持 T=0 通信协议；
3. 通讯速率：最低 57600 bit/s。
4. 电源电压：支持 1.8V 和 3V 两类工作电压；
5. 卡片工作温度：一般要求-25℃～+70℃（寒区-40℃～+70℃），存储温度：-40℃～+85℃，相对工作湿度：10%～95%；
6. 外部工作时钟频率应不低于 7.5MHz；
7. 其他物理特性、电气特性应符合 GB/T 16649《识别卡 带触点的集成电路卡》的规定。
8. OBE-SAM 安全等级应达到 GM/T 0008《安全芯片密码检测准则》规定

的 2 级或以上级别。

4.2 OBE-SAM 密钥规定

4.2.1 OBE-SAM 内密钥结构应符合表 5.2.1 的规定

表 5.2.1 OBE-SAM 内密钥结构

密钥	说明	密钥用途	密钥标识	密钥版本	密钥长度
MF 下密钥文件					
MK_{MF}	MF 系统主控密钥	00H	40H	00H	10H
$DAMK_{MF}$	MF 系统维护密钥	01H	41H	00H	10H
DF01 下密钥文件					
MK_{DF01}	DF01 应用主控密钥	00H	40H	00H	10H
$DAMK_{DF01}$	DF01 应用维护密钥	01H	41H	00H	10H
$UK1_{DF01}$	DF01 外部认证密钥 1	00H	01H	00H	10H
$RK21_{DF01}$	DF01 应用加密密钥 1	01H	03H	00H	10H
$RK22_{DF01}$	DF01 应用加密密钥 2	01H	03H	01H	10H
$RK23_{DF01}$	DF01 应用加密密钥 3	01H	03H	02H	10H
$UK2_{DF01}$	DF01 外部认证密钥 2	00H	41H	00H	10H
$RK3_{DF01}$	DF01 应用认证密钥	01H	42H	00H	10H
$RK41_{DF01}$	DF01 应用加密密钥 4	01H	43H	40H	10H
$RK42_{DF01}$	DF01 应用加密密钥 5	01H	43H	41H	10H
$RK43_{DF01}$	DF01 应用加密密钥 6	01H	43H	42H	10H

注：

1. 密钥标识的高四位为算法标识：‘0’- 3DES，‘4’- SM4。
2. 系统主控密钥在自身的控制下更新（密文+MAC）；
3. 系统主控密钥外部认证通过后，可在卡片 MF 下进行文件创建；
4. 系统维护密钥在卡片主控密钥线路保护控制下装载、更新；
5. 系统维护密钥用于 MF 区域的应用数据维护；
6. 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）；
7. 应用主控密钥在自身的控制下更新（密文+MAC）；
8. 应用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）；
9. 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；
10. 应用维护子密钥用于 DF01 应用下的应用数据维护；
11. 所有密钥的装载和修改应使用密文+MAC 的方式。

4.2.2 OBE-SAM 的密钥用途应符合表 5.2.2 的规定

表 5.2.2 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	用于获得相应文件的更新权限
	UK2_DF01	
计算密钥	RK3_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。
	RK4_DF01	

4.3 OBE-SAM 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）应符合表 5.3.1 的规定。

表 5.3.1 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）

5 CPU 用户卡数据格式和技术要求

5.1 一般规定

5.1.1 基本功能

CPU 用户卡应满足下列规定：

1. 具有操作系统的 CPU 卡，同时具有符合 GB/T 16649.1～16649.3 的接触式接口和符合 ISO/IEC 14443.1～14443.4 非接触式接口的双界面 CPU 卡，或具有符合 ISO/IEC 14443.1～14443.4 非接触式接口的 CPU 卡；
2. 支持一卡多应用，各应用之间相互独立；
3. 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；
4. 应采用硬件真随机数发生器；
5. 在通信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）；
6. 支持多种安全访问方式和权限（认证功能和口令保护）；
7. 支持 JR/T 0025-2013 所规定的 DES、3DES、SM4 算法；
8. 应支持 JR/T 0025-2010 中规定的电子钱包和电子存折功能；
9. 应支持 JR/T 0025-2010 中规定的复合消费功能；
10. CPU 用户卡的应用安全机制应符合本标准附录 A 的有关规定；
11. CPU 用户卡数据格式与应用命令应符合本标准附录 D 的有关规定。
12. 在一次复合应用消费交易中，CPU 用户卡应支持至少 2 条更新复合应用数据缓存命令，且更新的数据长度之和上限应至少为 255 字节。

5.1.2 基本参数

CPU 用户卡应符合下列规定：

1. 存储容量应不低于 16Kbytes；
2. 接触界面应支持 T=0 通信协议，非接触界面应支持 ISO/IEC

14443-1~14443-4 Type A 通信协议；

3. 非接触界面通讯速率应不低于 106kbit/s；
4. 接触界面支持多种速率选择，握手通讯速率从 9600bit/s 开始，支持 PPS，并应支持 57600bit/s 及以上通讯速率。
5. 接触界面外部时钟频率应不低于 7.5MHz；
6. 接触界面应能支持 3V 或 1.8V 两类工作电压；
7. 应支持文件标识符选择目录方式；
8. 非接触工作频率应为 13.56MHz±7kHz；
9. 钱包消费交易在接触方式，时钟频率为 3.579MHz 时，钱包消费交易（消费/取现命令）时间应小于 70ms。

5.1.3 物理特性

CPU 用户卡的物理特性应符合下列规定：

1. 环境条件应符合下列规定：

1） 工作温度：一般要求-25℃～+70℃（寒区-40℃～+70℃）；
2） 存储温度：-40℃～+85℃；
3） 相对工作湿度：10%～95%。

2. 没有涉及的其它卡片物理特性和电气特性应符合 GB/T 16649.1 和 ISO/IEC 14443 的规定。

5.1.4 其它要求

CPU 用户卡应满足下列要求：

1. 卡片应通过具有相关检测资质的第三方机构的检测；
2. 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；
3. 未在本标准中明确提出的 CPU 用户卡应用命令和安全机制，应符合 JR/T0025-2010。
4. 安全等级应达到 GM/T 0008《安全芯片密码检测准则》规定的 2 级或以上级别。

5.2 CPU 用户卡密钥规定

5.2.1 MF 下密钥文件结构应符合表 6.2.1 的规定：

表 6.2.1 MF 下密钥文件结构

密钥名称	密钥标识	密钥长度	算法标识	错误计数器
卡片主控密钥 $MK_{\_MF}$	40H	10H	04H	3-15
卡片维护密钥 $DAMK_{\_MF}$	41H	10H	04H	3-15

注：

1. 制造主密钥外部认证通过后，将其替换成卡片主控密钥；
2. 卡片主控密钥在自身的控制下更新（密文+MAC）；
3. 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；
4. 卡片维护密钥在卡片主控密钥线路保护控制下装载、更新；
5. 卡片维护密钥用于 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；
6. 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）。

5.2.2 DF01 联网收费应用目录下密钥文件结构应符合表 6.2.2 的规定：

表 6.2.2 DF01 联网收费应用目录下密钥文件结构

密钥名称	密钥标识	密钥长度	算法标识	错误计数器
应用主控密钥 MK_DF01	40H	10H	04H	3-15
应用维护子密钥 DAMK_DF01	41H	10H	04H	3-15
外部认证子密钥 1 UK1_DF01	01H	10H	00H	3-15
内部认证子密钥 1 $IK1_{\_DF01}$	00H	10H	00H	--
消费子密钥 1 DPK1	01H	10H	00H	--
消费子密钥 2 DPK2	02H	10H	00H	--
TAC 子密钥 1 DTK1	00H	10H	00H	--
应用 PIN PIN	00H	06H	--	3-15
应用 PIN 解锁子密钥 1 DPUK1_DF01	00H	10H	00H	3-15
应用 PIN 重装子密钥 1 DRPK1_DF01	01H	10H	00H	3-15
外部认证子密钥 2 UK2_DF01	41H	10H	04H	3-15
内部认证子密钥 2 $IK2_{\_DF01}$	40H	10H	04H	--
消费子密钥 3 DPK3	41H	10H	04H	--
消费子密钥 4 DPK4	42H	10H	04H	--
圈存子密钥 3 DLK3	41H	10H	04H	--
圈存子密钥 4 DLK4	42H	10H	04H	--
TAC 子密钥 2 DTK2	40H	10H	04H	--
应用 PIN 解锁子密钥 2 DPUK2_DF01	40H	10H	04H	3-15
应用 PIN 重装子密钥 2 DRPK2_DF01	41H	10H	04H	3-15

注：

1. 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. 应用主控密钥在自身的控制下更新（密文+MAC）；
3. 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）；
4. 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）；
5. 应用维护子密钥用于 DF01 区域的应用数据维护；
6. 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；
7. 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；
8. 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”。

6 应用系统兼容性

6.1 关键信息编码定义

6.1.1 版本号

支持国密 SM4 算法的卡片，CPU 用户卡发行基本数据文件（0015）第 10 字节“卡片版本号”的高 4 位统一定义为 5，OBE-SAM 系统信息文件（EF01）第 10 字节“合同版本”的高 4 位统一定义为 5， PSAM 卡 MF 下卡片公共信息文件（0015）第 11 字节 PSAM 版本号定义为 0x05。

6.1.2 CPU 用户卡消费密钥标识

PSAM 卡内 DF01 下的 0017 文件增加第 26 字节，该字节定义为“用户卡消费密钥标识”（假设其值为 Y），即 CPU 用户卡当前使用的消费子密钥标识为 Y。

6.1.3 OBU 应用加密密钥版本

PSAM 卡内 DF01 下的 0017 文件增加第 27 字节，该字节定义为“OBU 应用加密密钥版本”（假设其值为 Z），即，OBE-SAM 当前使用的应用加密密钥版本为 Z。

6.2 OBU 和 CPU 用户卡的发行

ETC 系统国产密码算法迁移过程中，发行的 OBU 和 CPU 用户卡应同时支持 3DES 和 SM4 两种算法。发行版本号应符合 6.1.1。

6.3 车道交易流程

6.3.1 交易流程概述

对于 PSAM 版本号小于 0x05 的，按原有处理流程不变；对于 PSAM 版本号大于或等于 0x05 的，按如下流程处理：

若 CPU 用户卡及 ESAM 版本号等于 FF 或高 4 位小于 5，则按已有交易流程不变；若 CPU 用户卡及 ESAM 版本号不等于 FF 且高 4 位大于等于 5，则：

（1）车道系统在发起复合消费交易前，从 PSAM 卡预读“用户卡消费密钥标识”Y 和“OBU 应用加密密钥版本”Z，指定标识号为 Y 的消费密钥（复合消费初始化命令的命令报文数据域首字节）进行复合消费初始化， PSAM 据此选择密钥版本为 Y 的消费主密钥计算 MAC1 及校验 MAC2。

（2）车道系统在读取车辆信息文件时，指定 OBE-SAM 使用密钥版本为 Z 的 DF01 应用加密密钥（Read Data 命令的数据域末字节），PSAM 选择密钥版本为（Z+3）的 OBU 加密主密钥对读取的车辆信息进行认证。

6.3.2 车道系统处理流程

车道系统按如下规则处理，即可保证在密钥版本更新后交易流程正常进行。

（1）车道终端针对消费密钥的处理流程如下：

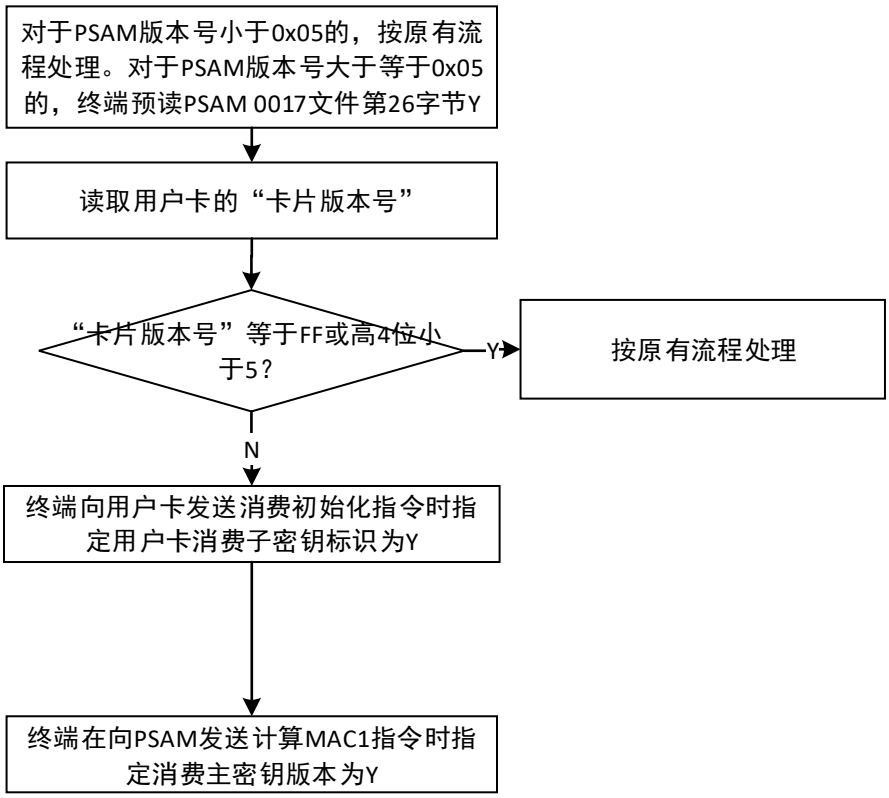

图 7.3.2-1 车道终端选择 CPU 用户卡密钥版本规则

（2）车道终端针对 OBU 加密密钥的处理流程如下：

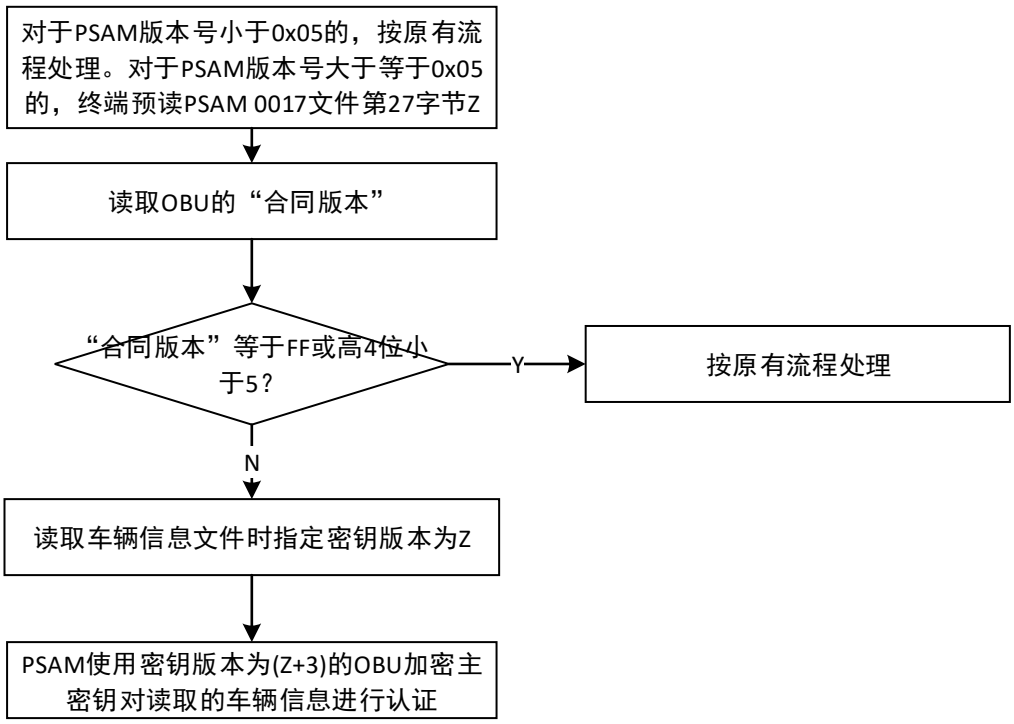

图 7.3.2-2 车道终端选择标签密钥版本规则

6.3.3 车道交易记录

车道交易记录应包含 CPU 用户卡的“卡片版本号”字段和 OBE-SAM 的“合同版本”字段。

6.4 密钥版本替换流程

6.4.1 消费密钥的应用流程

消费交易过程中的消费密钥的应用流程如下：

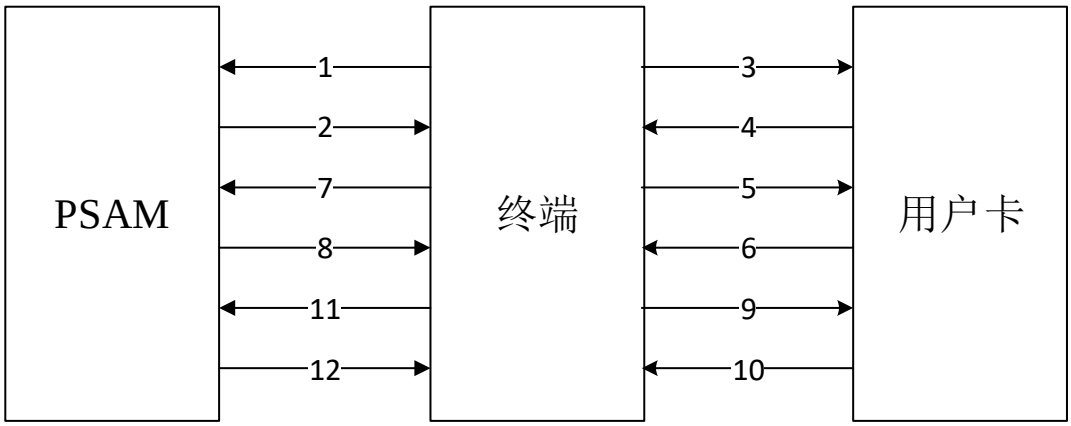

图 7.4.1 消费密钥的应用流程示意图

1. 终端选择 PSAM 卡文件，PSAM 版本号小于 0x05 的，按已有流程处理，PSAM 版本号大于等于 0x05 的，按如下流程处理；
2. PSAM 卡返回终端机编号、“用户卡消费密钥标识”Y 和“OBU 应用加密密钥版本”Z；
3. 终端选择 CPU 用户卡文件；
4. CPU 用户卡返回卡片版本号、发卡方标识、应用序列号等信息；
5. 终端发起消费初始化，指定使用 CPU 用户卡中标识为 Y’（若用户卡版本号高 4 位小于 5 或等于 FF，则 Y’=（Y 的低 4 位），否则 Y’=Y）的消费子密钥；
6. CPU 用户卡返回数据；
7. 终端指定使用 PSAM 中密钥版本为 Y’的消费主密钥计算 MAC1；
8. PSAM 卡返回 MAC1、终端脱机交易序号；
9. 终端对 CPU 用户卡发消费命令；
10. CPU 用户卡返回 MAC2 和 TAC；
11. 终端利用 PSAM 卡校验 MAC2；
12. PSAM 卡返回校验结果。

6.4.2 消费密钥版本替换流程

消费密钥版本替换流程如图 7.4.2 所示。

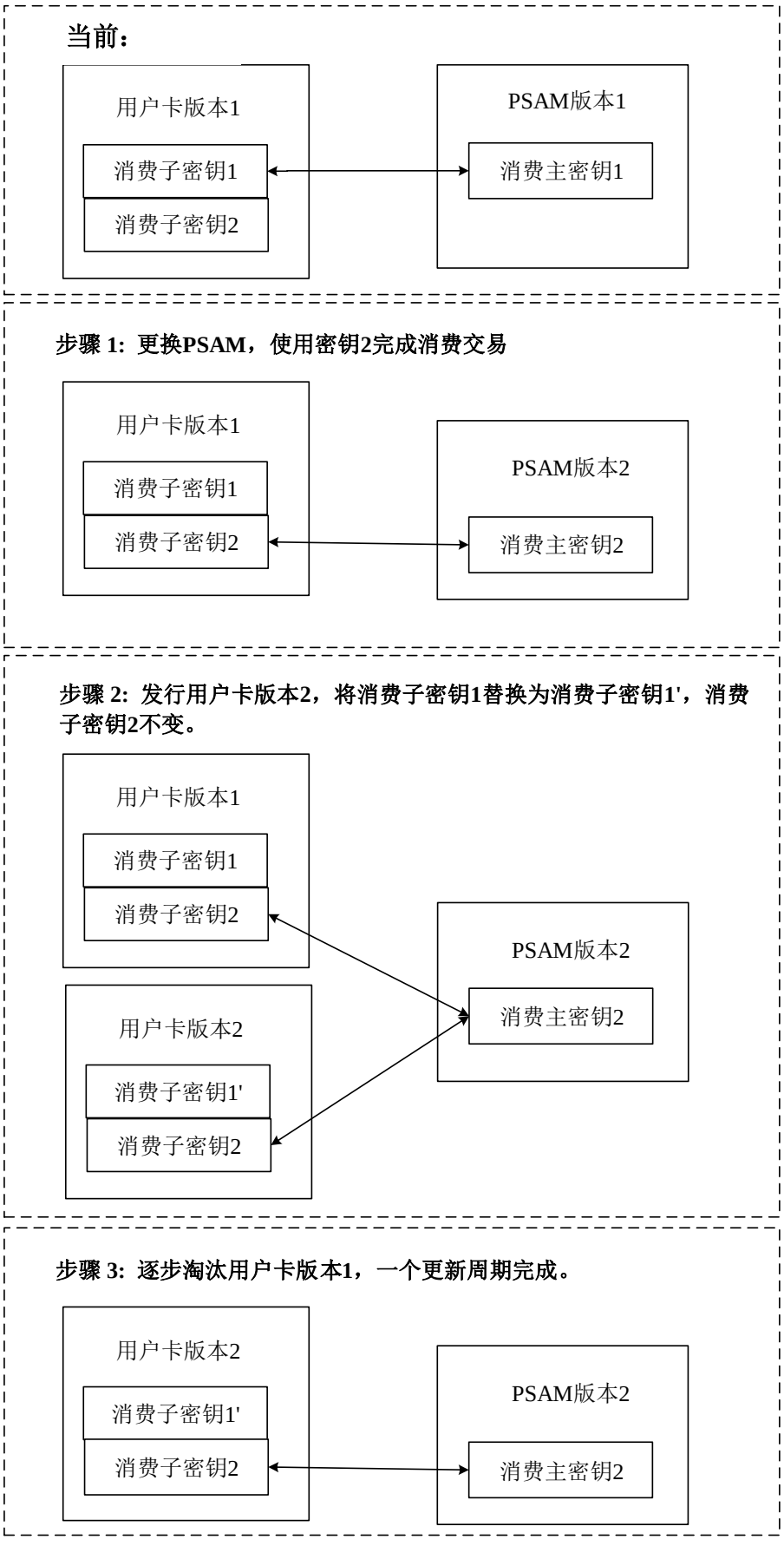

图 7.4.2 消费密钥版本替换流程示意图

当前，CPU 用户卡内装有两条消费子密钥，分别是消费子密钥 1 和消费子密钥 2，该版本 CPU 用户卡称为 CPU 用户卡版本 1。PSAM 内装有一条消费密钥，即消费主密钥 1，与消费子密钥 1 对应，该 PSAM 版本称为 PSAM 版本 1。（当前）

当需要更新密钥 1 时，先将终端上的所有 PSAM 更换为版本 2，版本 2 的 PSAM 内装有消费主密钥 2，与消费子密钥 2 相对应。终端根据 PSAM 内的密钥索引号，确定使用 CPU 用户卡中的相应消费子密钥完成消费交易。（步骤 1)

发行 CPU 用户卡版本 2，装载消费子密钥 1’（索引号与消费子密钥 1 相同）和消费子密钥 2。此时 CPU 用户卡版本 2 和版本 1 同时存在，均使用消费密钥 2 完成消费交易。(步骤 2)

以自然过渡方式或充值时在线更新方式，逐步淘汰装载消费子密钥 1 的 CPU 用户卡即 CPU 用户卡版本 1，CPU 用户卡全部过渡到版本 2。至此，一个完整的密钥更新周期完成。(步骤 3）

6.4.3 应用加密密钥的应用流程

从 OBU 读取车辆信息文件过程中应用加密密钥的应用流程如下：

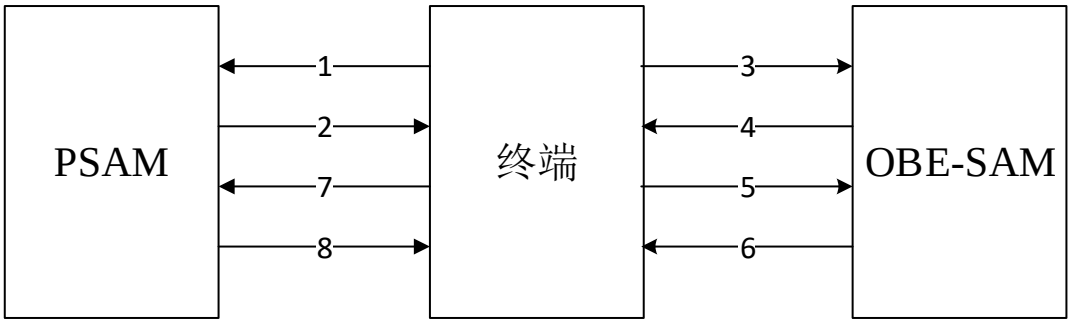

图 7.4.3 应用加密密钥的应用流程示意图

1. 终端选择 PSAM 卡文件，PSAM 版本号小于 0x05 的，按已有流程处理，PSAM 版本号大于等于 0x05 的，按如下流程处理；
2. PSAM 卡返回终端机编号、“用户卡消费密钥标识”Y 和“OBU 应用加密密钥版本”Z；
3. 终端读取 OBU 文件；
4. OBE-SAM 返回合同版本、发卡方标识、合同序列号等信息；
5. 终端发起读车辆信息指令，指定使用 OBE-SAM 中版本号为 Z’（ 若

合同版本高 4 位小于 5 或等于 FF，则 Z’=（Z 的低 4 位），否则 Z’=Z）的应用加密子密钥；

6. OBU 返回车辆信息密文；
7. 终端利用 PSAM 卡解密车辆信息密文，指定使用 PSAM 中密钥版本为（Z’+3）的 OBU 加密主密钥；
8. PSAM 卡返回车辆信息明文。

6.4.4 应用加密密钥版本替换流程

应用加密密钥版本替换流程如下图所示。

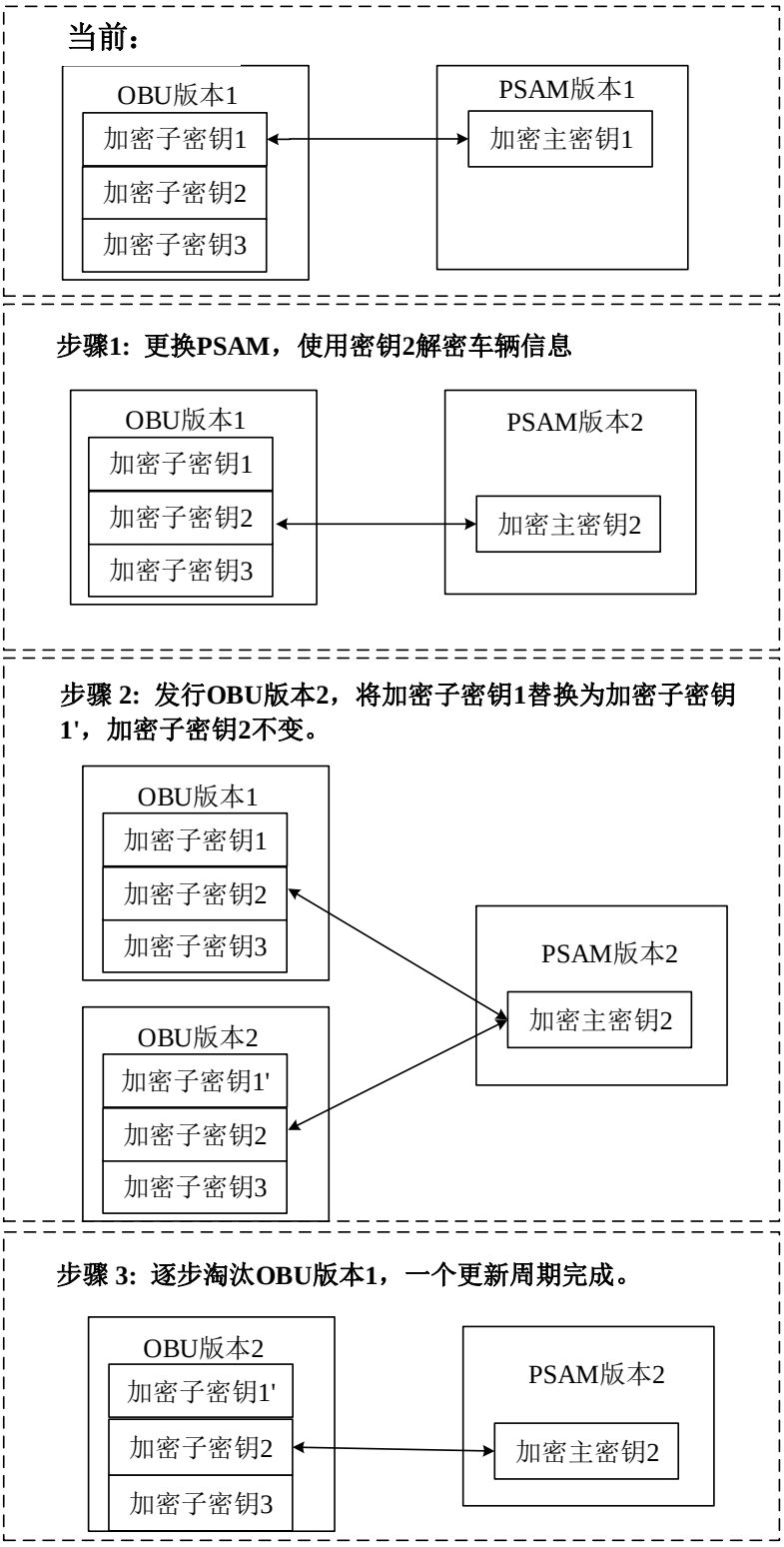

图 7.4.4 应用加密密钥版本替换流程示意图

附录 A 智能卡应用安全机制

A.1 安全计算方法

A.1.1 密钥分散计算方法

由主密钥和 8 字节分散因子推导出子密钥的过程应符合下列规定：

1 对于数据分组长度为 64 位的加密算法，密钥分散方式应符合下列规定：

1) 将一个 16 字节长度的主密钥 MK，对分散因子进行处理，推导出一个 16 字节长度的子密钥 DK，如图 A.1.1-1 和图 A.1.1-2。

2) 推导 DK 左半部分的方法是：

第一步：将分散因子作为输入数据；

第二步：将 MK 作为加密密钥；

第三步：用 MK 对输入数据进行 3DEA 运算。

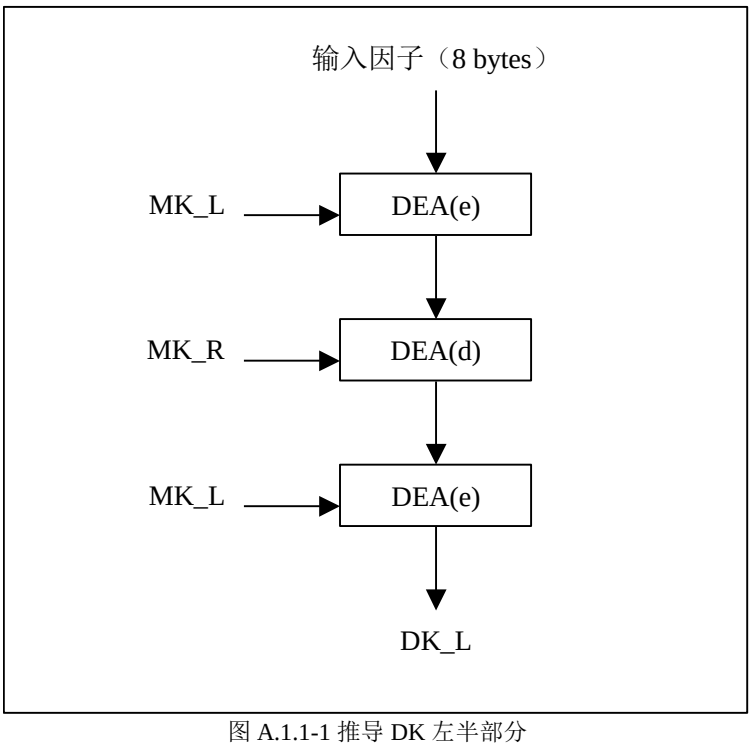

图 A.1.1-1 推导 DK 左半部分

3) 推导 DK 右半部分的方法是：

第一步：将分散因子求反，作为输入数据；

第二步：将 MK 作为加密密钥；

第三步：用 MK 对输入数据进行 3DEA 运算。

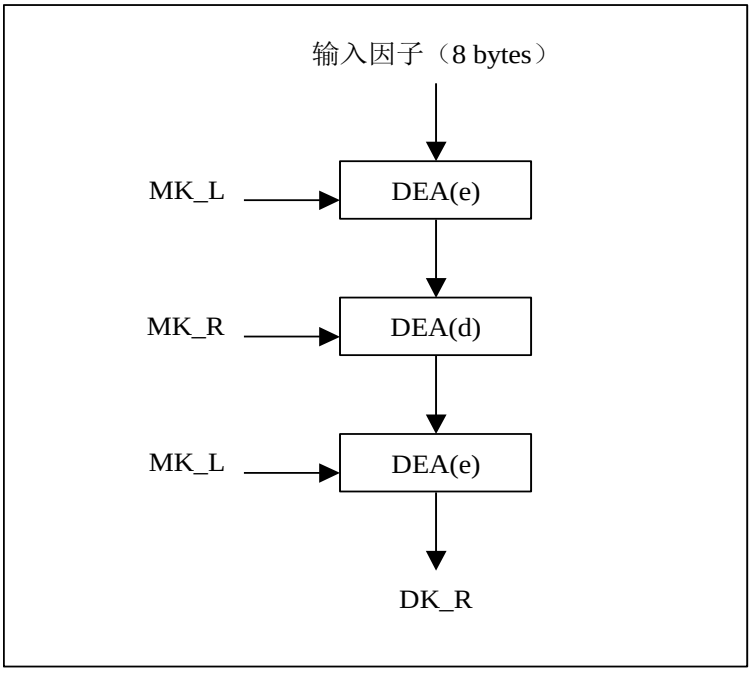

图 A.1.1-2 推导 DK 右半部分

2　对于数据分组长度为 128 位的加密算法，密钥分散方式应符合下列规定：

将16字节主密钥MK对分散因子进行处理，推导出一个16字节长度的子密钥DK，如图A.1.1-3所示。

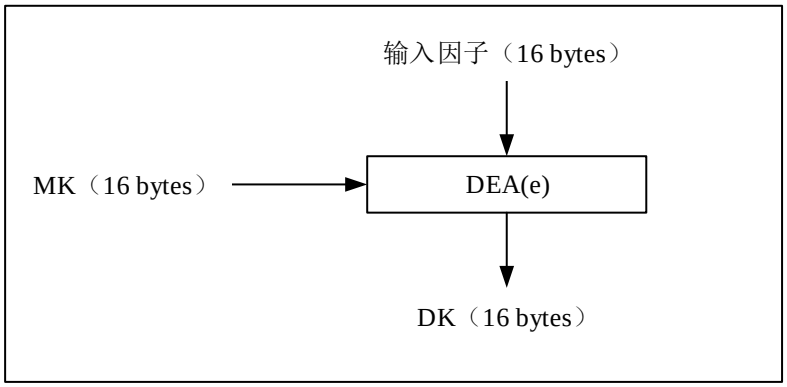

图 A.1.1-3 数据分组长度为 64 位的算法推导 DK

推导DK的方法是：

第一步：将分散因子按位取反，按照“分散因子”||“分散因子的反”的顺序连接在一起，组成16字节输入因子；

第二步：将MK作为加密密钥；

第三步：用MK对输入数据进行DEA加密运算。

A.1.2　数据加密的计算方法

1　对于数据分组长度为 64 位的加密算法，应按照如下方式对数据进行加

密：

第一步：LD（1 字节）表示明文数据的长度，在明文数据前加上 LD 产生新的数据块；

第二步：将该数据块分成 8 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节；

第三步：如果最后（或唯一）的数据块的长度是 8 字节的话，转到第四步；如果不足 8 字节，则在其后加入 0x80，如果达到 8 字节长度，则转到第四步；否则在其后加入 0x00 直到长度达到 8 字节；

第四步：按照图 A.1.2-1 所示的算法使用指定密钥对每一个数据块进行加密；

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起。

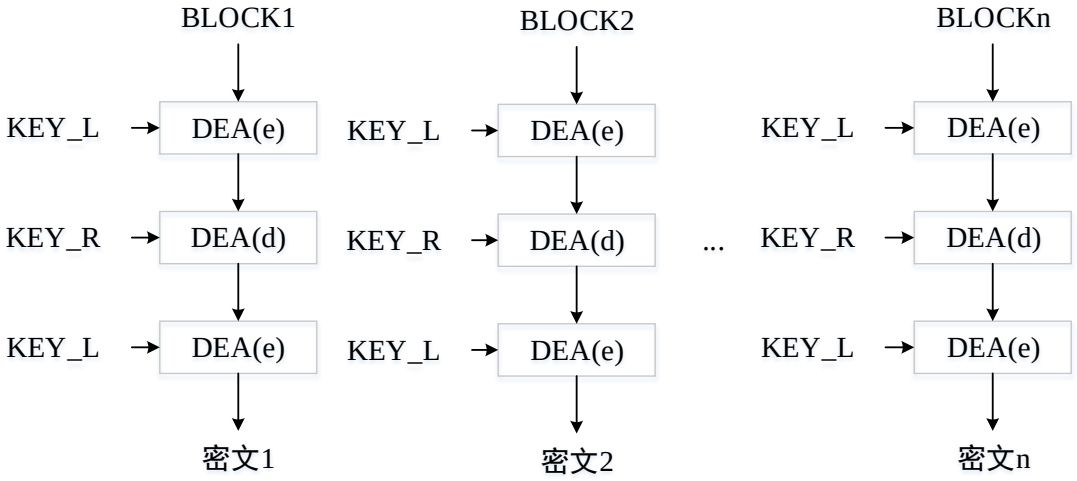

图 A.1.2-1 数据分组长度为 64 位的 DEA 数据加密算法

2　对于数据分组长度为 128 位的加密算法，按照如下方式对数据进行加密：

第一步：LD（1 字节）表示明文数据的长度，在明文数据前加上 LD 产生新的数据块；

第二步：将该数据块分成 16 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 个字节；

第三步：如果最后（或唯一）的数据块的长度是 16 字节的话，转到第四步；如果不足 16 字节，则在其后加入 0x80，如果达到 16 字节长度，则转到第四步；否则在其后加入 0x00 直到长度达到 16 字节；

第四步：按照图 A.1.2-2 所示的算法使用指定密钥对每一个数据块进行加密。

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起。

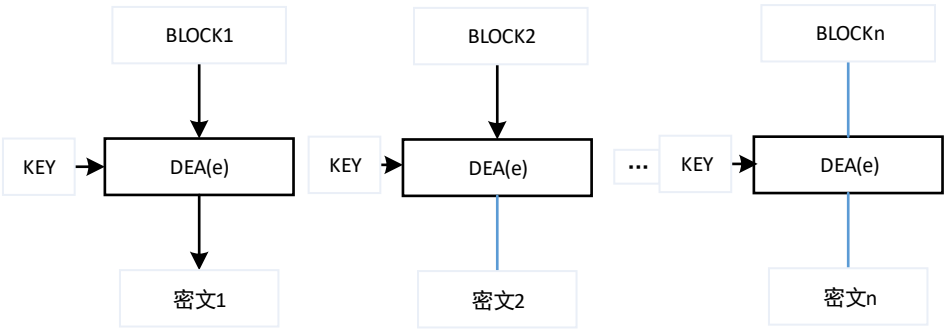

图 A.1.2-2 数据分组长度为 128 位的 DEA 数据加密算法

A.1.3 过程密钥的计算方法

1 对于数据分组长度为 64 位的加密算法，应按照图 A.1.3-1 方式产生过程密钥：

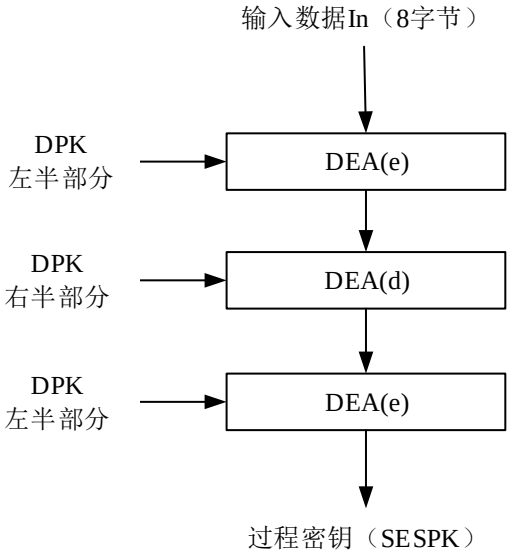

图 A.1.3-1 数据分组长度为 64 位的算法的过程密钥产生

2 对于数据分组长度为 128 位的加密算法，应按照图 A.1.3-2 方式产生过程密钥：

第一步：将输入数据In按位取反得到（~In），即（~In）= In ⊕ (0xFF||0xFF||0xFF||0xFF||0xFF||0xFF||0xFF||0xFF)，按照In||(~In)的顺序连接在一起，组成16字节输入数据；

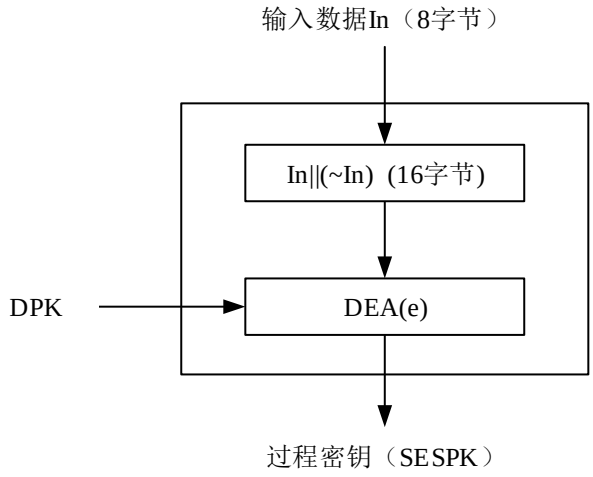

图 A.1.3-2 数据分组长度为 128 位的算法的过程密钥产生

第二步：将DPK作为加密密钥；

第三步：用DPK对In||(~In)进行DEA加密运算得到过程密钥。

A.1.4 安全报文的计算方法

1 命令安全报文中的 MAC 应符合下列规定：

1) 对于数据分组长度为 64 位的加密算法，应按照如下方式使用DEA 加密方式产生MAC：

第一步：终端通过向IC卡发GET CHALLENGE命令获得一个4字节随机数，后补 4 字节 0x00 作为初始值；

第二步：将 5 字节命令头（CLA，INS，P1，P2，Lc）和命令数据域中的明文或密文数据连接在一起形成数据块。这里的 Lc 应是数据长度加上将计算出的 MAC 的长度（4 字节）后得到的实际长度；

第三步：将该数据块分成 8 字节为单位的数据块，表示为 BLOCK1、BLOCK2、 BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节；

第四步：如果最后的数据块的长度是 8 字节的话，则在该数据块之后再加一个完整的 8 字节数据块 0x8000000000000000，转到第五步；如果最后的数据块的长度不足 8 字节，则在其后加入 0x80， 如果达到 8 字节长度，则转到第五步；否则接着在其后加入 0x00 直到长度达到 8 字节。

第五步：按图 A.1.4-1 所示的算法对这些数据块使用指定密钥进行加密来产生 MAC。

第六步：最终取计算结果高 4 字节作为 MAC。

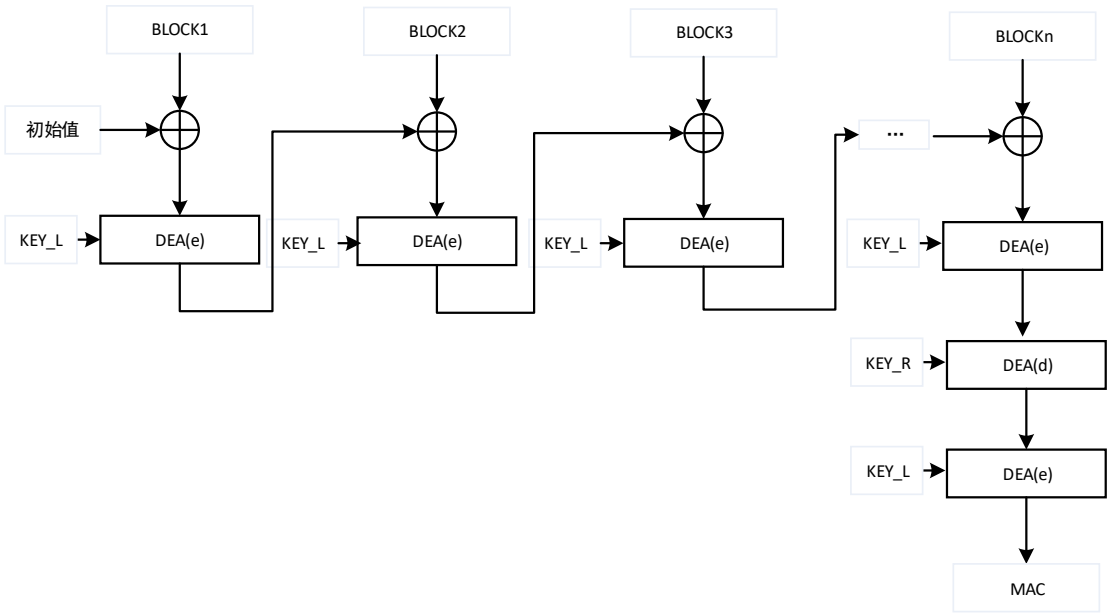

图 A.1.4-1 安全报文中数据分组长度为 64 位的 MAC 算法

2) 对于数据分组长度为 128 位的加密算法，应按照如下方式使用 DEA 加密方式产生 MAC：

第一步：终端通过向 IC 卡发 GET CHALLENGE 命令获得一个 4 字节随机数，后补 12 字节 0x00 作为初始值；

第二步：将 5 字节命令头（CLA，INS，P1，P2，Lc）和命令数据域中的明文或密文数据连接在一起形成数据块。 注意，这里的 Lc 应是数据长度加上将计算出的 MAC 的长度（4 字节）后得到的实际长度；

第三步：将该数据块分成 16 字节为单位的数据块， 表示为 BLOCK1、BLOCK2、 BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 个字节；

第四步：如果最后的数据块的长度是 16 字节的话，则在该数据块之后再加一个完整的 16 字节数据块 0x80000000000000000000000000000000’，转到第五步；如果最后的数据块的长度不足 16 字节，则在其后加入 0x80，如果达到 16 字节长度，则转到第五步；否则接着在其后加入 0x00 直到长度达到 16 字节。

第五步：按图 A.1.4-2 所示的算法对这些数据块使用指定密钥进行加密来产生 MAC。

第六步：最终取计算结果高 4 字节作为 MAC。

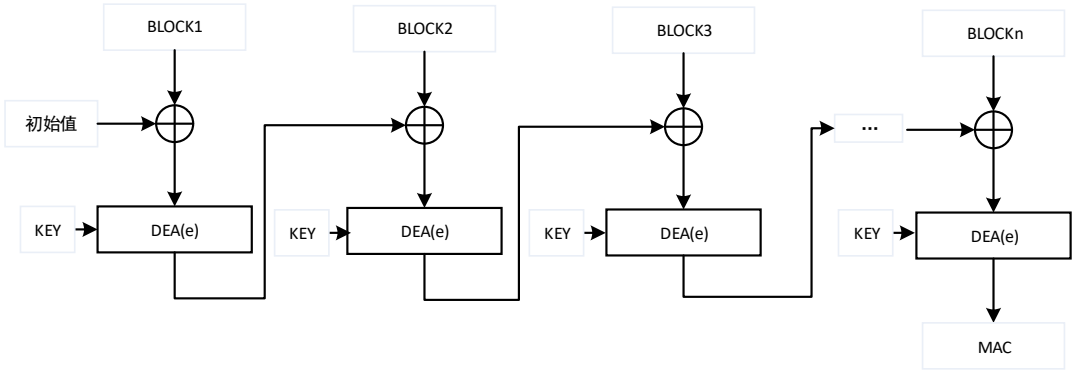

图 A.1.4-2 安全报文中数据分组长度为 128 位的 MAC 算法

2　交易中的 MAC 应符合下列规定：

1) 交易过程中，先用指定密钥产生过程密钥，再用过程密钥计算 MAC。

2) 对于数据分组长度为 64 位的加密算法，应按照如下方式使用 DEA 加密方式产生 MAC：

第一步：将 8 字节 0x00 设定为初始值；

第二步：将所有输入数据按指定顺序连接成一个数据块；

第三步：将该数据块分成 8 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节；

第四步：如果最后的数据块的长度是 8 字节的话，则在该数据块之后再加一个完整的 8 字节数据块 0x8000000000000000，转到第五步；如果最后的数据块的长度不足 8 字节，则在其后加入 0x80，如果达到 8 字节长度，则转到第五步；否则在其后加入 0x00 直到长度达到 8 字节；

第五步：按照图 A.1.4-3 所示的算法对这些数据块使用过程密钥（单倍长度）进行加密来产生 MAC；

第六步：最终取计算结果高 4 字节作为 MAC。

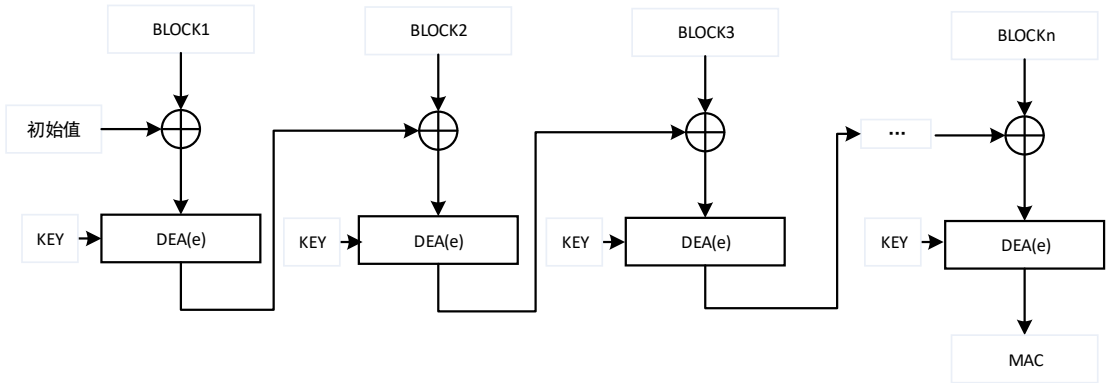

图 A.1.4-3 交易中的 MAC 算法

3) 对于数据分组长度为 128 位的加密算法，应按照如下方式使用 DEA 加密方式产生 MAC：

第一步：将 16 字节 0x00 设定为初始值；

第二步：将所有输入数据按指定顺序连接成一个数据块；

第三步：将该数据块分成 16 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~16 个字节；

第四步：如果最后的数据块的长度是 16 字节的话，则在该数据块之后再加一个完整的 16 字节数据块 0x80000000000000000000000000000000，转到第五步；如果最后的数据块的长度不足 16 字节，则在其后加入 0x80， 如果达到 16 字节长度，则转到第五步；否则在其后加入 0x00 直到长度达到 16 字节；

第五步：按照0所示的算法对这些数据块使用过程密钥进行加密来产生 MAC；

第六步：最终取计算结果（高 4 字节）作为 MAC。

3 TAC 计算方法应符合下列规定：

1) TAC 的计算不采用过程密钥方式。

2) 对于数据分组长度为 64 位的加密算法，先用 TAC 密钥左右 8 字节异或运算后的结果作为密钥，再按照交易中的 MAC 描述的机制计算 TAC。

3) 对于数据分组长度为 128 位的加密算法，直接使用 TAC 密钥按照交易中的 MAC 描述的机制计算 TAC。

4 双向认证中的鉴别码应符合下列规定：

1) 将文件数据进行 CRC 计算（多项式 X16+X12+X5+1，起始 0xFFFF），产生两字节 CRC0 和 CRC1；

2) 将送入的随机数(8bytes)最低两字节分别更换为 CRC1、CRC0，形成 8 字节临时数据；

3) 对于 3DES 算法，使用计算密钥对 8 字节数据进行加密计算：MAC = TDES(KEY_MAC，CRC0||CRC1||Rand(高 6 字节))

4) 对于 SM4 算法，使用计算密钥对（8 字节数据后补 8 字节 0x00 后组成的 16 字节数据）进行加密计算：MAC = SM4(KEY_MAC，CRC0||CRC1||Rand(高

6 字节)||0x0000000000000000)。

A.3 认可的加密算法

A.3.1 DES/3DES 算法应遵从《中国金融集成电路（IC）卡规范》JR/T 0025 第 7 部分 12.1.1 条的规定。

A.3.2 SM4 算法应遵从《SM4 分组密码算法》GM/T 0002 的规定。

A.4 算法选择

A.4.1 卡片在处理命令时，应根据卡内所用密钥的算法标识属性来决定采用的算法。

A.4.2 算法标识定义应符合下列规定：

1 ‘00’：3DES

2 ‘04’：SM4

3 其它值：保留

附录 B PSAM 卡数据格式与应用命令集

B.1 PSAM 卡数据格式

B.1.1 PSAM 卡的文件结构应符合图 B.1.1 的规定：

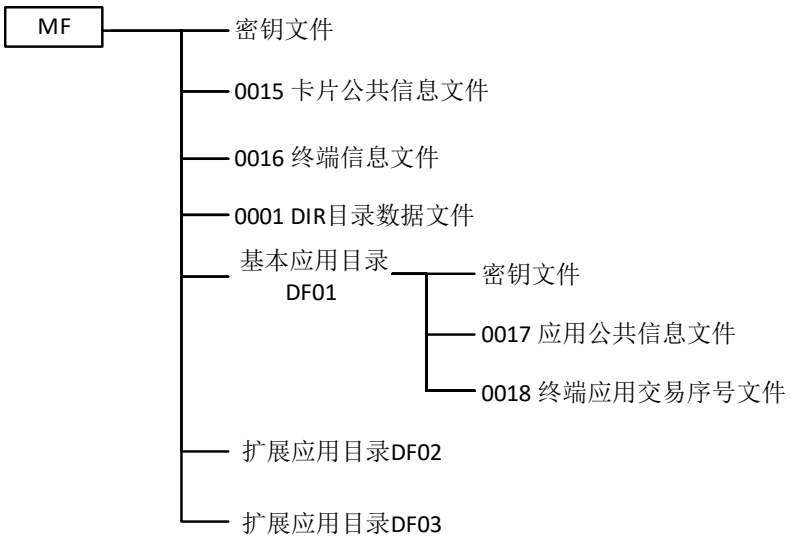

图 B.1.1 PSAM 卡文件结构

B.1.2 PSAM 卡的详细文件结构应符合表 B.1.2 的规定：

表 B.1.2 PSAM 卡文件结构

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/擦除权：MK_{MF}		厂商交货时已经建立
1	密钥文件	密钥文件	--	禁止	增加密钥权：MK_{MF}	通过卡片主控密钥 MK_{MF} 采用密文+MAC 方式写入密钥
2	DIR 目录数据文件	变长记录	0001	自由	AMK_{MF}	自由读，写时使用卡片维护密钥进行线路保护（明文+MAC）
3	卡片公共信息文件	二进制文件	0015	自由	AMK_{MF}	自由读，写时使用卡片维护密钥进行线路保护（明文+MAC）
4	终端信息文件	二进制文件	0016	自由	AMK_{MF}	自由读，写时使用卡片维护密钥进行线路保护（明文+MAC）
DF01 联网电子收费应用		目录文件	DF01	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
1	密钥文件	密钥文件	--	禁止	增加密钥权：MK_{DF01}	DF01 应用密钥采用密文+MAC 方式写入
2	应用公共信息文件	二进制文件	0017	自由	AMK_{DF01}	自由读，写时使用应用维护密钥 AMK_{DF01} 进行线路保护（明文+MAC）
3	终端应用交易序号文件	二进制文件	0018	自由	不可写，COS 维护	用于存储终端交易序号，由 COS 维护
扩展应用目录 DF02		目录文件	DF02	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
扩展应用目录 DF03		目录文件	DF03	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

B.1.3 MF 下的卡片公共信息文件（0015）结构应符合表 B.1.3 的规定：

表 B.1.3 MF 下卡片公共信息文件结构

字节	数据元	长度（字节）
1-10	PSAM 序列号	10
11	PSAM 版本号	1
12	密钥卡类型	1
13-14	发卡方自定义 FCI 数据	2

B.1.4 MF 下的终端信息文件（0016）结构应符合表 B.1.4 的规定：

表 B.1.4 MF 下的终端信息文件

字节	数据元	长度（字节）
1-6	终端机编号	1-6

B.1.5 DF01 下的应用公共信息文件（0017）结构应符合表 B.1.5 的规定：

表 B.1.5DF01 下的应用公共信息文件

字节	数据元	长度（字节）
1	密钥索引号	1
2-9	发行方标识	8
10-17	应用区域标识	8
18-21	应用启用日期	4
22-25	应用有效日期	4
26	用户卡消费密钥标识	1
27	OBU 应用加密密钥版本	1

B.2 PSAM 卡应用命令集

B.2.1 EXTERNAL AUTHENTICATE 命令应符合下列规定：

1 EXTERNAL AUTHENTICATE 命令执行成功后，应使外部接口设备对 PSAM 卡获得某种操作授权。

2 接口设备提供的认证数据应按以下规则产生：

1) 用 GET CHALLENGE 命令向 IC 卡申请一组随机数；

2) 用指定密钥对随机数（后面填充 0x00 至 8 字节（3DES）或 16 字节（SM4）后）做加密运算产生。

3) 对于 SM4 算法，认证数据为 16 字节密文前后 8 字节进行异或的结果，长度仍为 8 字节。

3 EXTERNAL AUTHENTICATE 命令执行时应满足 P2 参数所指定密钥的使用权限。

4 密钥验证失败时相应外部认证密钥的错误计数器应减 1，当计数器减为‘0’值时，密钥被锁定。

5 EXTERNAL AUTHENTICATE 命令报文格式应符合表 B.2.1-1 的规定：

表 B.2.1-1 EXTERNAL AUTHENTICATE 命令报文格式

代码	数　值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	密钥版本
Lc	‘08’
DATA	认证数据（8 字节）
Le	不存在

6 EXTERNAL AUTHENTICATE 命令响应状态应符合表 B.2.1-2 的规定：

表 B.2.1-2 响应信息中的状态码

SW1	SW2	说　明
90	00	命令执行成功
63	Cx	认证失败，还可认证 x 次
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.2　SELECT FILE 命令应符合下列规定：

1　SELECT FILE 命令应通过文件标识或应用名选择 PSAM 卡中的 MF、ADF 或 EF 文件。

2　SELECT FILE 命令的响应报文应包含回送 FCI，FCI 数据从数据分组中获得。

3　SELECT FILE 命令无使用条件限制。

4　SELECT FILE 命令不能用于选择安全文件（SF）。

5　SELECT FILE 命令的报文格式应符合表 B.2.2-1 的要求：

表 B.2.2-1 SELECT FILE 命令报文格式

代码	数　值
CLA	‘00’
INS	‘A4’
P1	‘00’通过 FID 选择 DF、EF，当 Lc=‘00’时，选 MF ‘04’通过 DF 名选择应用
P2	‘00’ ‘02’选择下一个文件（P1=04h 时）
Lc	P1=‘00’时，Lc=‘00’或‘02’ P1=‘04’时，Lc=‘05’~‘10’
DATA	文件标识符（FID—2 字节） 应用名（App-Name，P1=‘04’）
Le	FCI 文件的信息长度（选择 DF 时）

6　SELECT FILE 命令的响应报文数据应符合表 B.2.2-2 的要求：

表 B.2.2-2 成功选择 ADF 后回送的 FCI

标签	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名	M

7　SELECT FILE 命令的响应状态码应符合表 B.2.2-3 的要求：

表 B.2.2-3 响应信息中的状态码

SW1	SW2	说　明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
62	83	选择文件无效
62	84	FCI 格式与 P2 指定的不符
64	00	标志状态位没变
67	00	Lc 长度错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	87	Lc 与 P1-P2 不匹配
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.3 READ RECORD 命令应符合下列规定：

1 READ RECORD 命令读取记录文件中指定的记录。

2 READ RECORD 命令执行时应满足相应文件的读权限和控制属性。

3 READ RECORD 命令报文格式应符合表 B.2.3-1 的规定。

表 B.2.3-1 READ RECORD 命令报文格式

代码	值
CLA	‘00’
INS	‘B2’
P1	记录的序号
P2	引用控制参数（见下表）
Lc	不存在
Data	不存在
Le	‘00’

4 READ RECORD 命令引用控制参数应符合见表 B.2.3-2 的规定。

表 B.2.3-2 READ RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X				SFI
					1	0	0	P1 为记录的序号

5 执行成功的 READ RECORD 命令响应报文数据域应由读取的记录组成。

6 READ RECORD 命令响应状态码应符合表 B.2.3-3 的规定。

表 B.2.3-3 响应信息中可能返回的状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效(未申请随机数)
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6C	xx	Le 错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.4 UPDATE RECORD 命令应符合下列规定：

1 UPDATE RECORD 命令用给定的数据代替记录文件中指定的记录。

2 对线性记录文件，可按记录号顺序添加记录。

3 UPDATE RECORD 命令的执行应满足相应文件的写权限和控制属性。

4 UPDATE RECORD 命令报文格式应符合表 B.2.4-1 的规定。

表 B.2.4-1 UPDATE RECORD 命令报文格式

代码	值
CLA	‘00’或‘04’
INS	‘DC’
P1	P1=‘00’：表示当前记录，P1≠‘00’：指定的记录号或记录标识
P2	见下表
Lc	后续数据域长度
Data	输入数据
Le	不存在

5 UPDATE RECORD 命令引用控制参数应符合表 B.2.4-2 的规定。

表 B.2.4-2 UPDATE RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X				SFI
					0	0	0	第一个记录
					0	0	1	最后一个记录
					0	1	0	下一个记录
					0	1	1	上一个记录
					1	0	0	记录号在 P1 中给出
其余值								RFU

6 UPDATE RECORD 命令报文数据域由更新原有记录的新记录组成。

7 使用安全报文时，命令报文的数据域中应包括 MAC。MAC 是由卡片维护密钥或应用维护密钥对更新原有记录的新记录计算而得到的。

8 UPDATE RECORD 命令响应状态码应符合表 B.2.4-3 的规定。

表 B.2.4-3 响应信息中的状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.5 READ BINARY 命令应符合下列规定：

1 READ BINARY 命令用于读出透明文件的内容。

2 READ BINARY 命令的执行应满足访问文件的读权限和控制属性。

3 READ BINARY 命令报文格式应符合表 B.2.5-1 的规定。

表 B.2.5-1 READ BINARY 命令报文格式

代码	数　值								
CLA	‘00’或‘04’								
INS	‘B0’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	1）不存在——明文方式 2）‘04’——校验方式								
DATA	1）不存在 2）MAC								
Le	期望返回的数据长度								

4　READ BINARY 命令响应信息中的数据为明文或密文数据，当 Le 的值为零时，当从指定的偏移量至文件结束，长度小于 256 字节、等于 256 字节、大于 256 字节时，返回数据长度应符合表 B.2.5-2 的规定

表 B.2.5-2 Le=0 时的命令响应信息

实际长度	小于 256 字节	等于 256 字节	大于 256 字节
返回数据	6CXX，其中 XX 为实际长度	返回 256 字节	返回 256 字节

5　READ BINARY 命令的响应状态码应符合表 B.2.5-3 的规定。

表 B.2.5-3 响应信息中的状态码

SW1	SW2	说　明
90	00	命令执行成功
61	xx	还有 xx 字节要返回
62	81	部分回送的数据可能有错
62	82	文件长度<Le
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6C	xx	Le 长度错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.6　UPDATE BINARY 命令应符合下列规定：

1　UPDATE BINARY 命令用于更新透明文件中的数据。

2　UPDATE BINARY 命令的执行应满足文件的写权限和控制属性。

3　UPDATE BINARY 命令报文格式应符合表 B.2.6-1 的规定。

表 B.2.6-1 UPDATE BINARY 命令报文格式

代码	数　值								
CLA	‘00’或‘04’								
INS	‘D6’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	DATA 域的长度： 明文方式：　‘00’< Lc ≤‘FF’ 加密方式：　‘08’≤ Lc ≤‘48’（模 8） 校验方式：　‘04’< Lc ≤‘44’ 校验加密方式：‘0C’≤ Lc ≤‘4C’（模 8+4）								
DATA	明文方式：　明文数据 加密方式：　密文数据 校验方式：　明文数据||校验码 校验加密方式：密文数据||校验码								
Le	不存在								

4　UPDATE BINARY 命令响应状态码应符合表 B.2.6-2 的规定。

表 B.2.6-2　响应信息中的状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.7　GET CHALLENGE 命令应符合下列规定：

1　GET CHALLENGE 命令从 PSAM 卡中获取一组随机数，用于相关命令的安全认证。

2　GET CHALLENGE 命令无使用条件限制。

3　GET CHALLENGE 命令报文格式见表 B.2.7-1。

表 B.2.7-1 GET CHALLENGE 命令报文格式

代码	数　值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘04’,‘08’或‘10’随机数长度

4　GET CHALLENGE 命令响应状态码应符合表 B.2.7-2 的规定。

表 B.2.7-2 响应信息中的状态码

SW1	SW2	说　明
90	00	命令执行成功
67	00	Le 长度错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

B.2.8　GET RESPONSE 命令应符合下列规定：

1　GET RESPONSE 命令从 PSAM 卡中向接口设备传送 APDU 的数据。

2　GET RESPONSE 命令无使用条件限制。

3　GET RESPONSE 命令报文格式应符合表 B.2.8-1 的规定。

表 B.2.8-1 GET RESPONSE 命令报文格式

代码	数　值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	响应的最大数据长度

4　GET RESPONSE 命令响应状态码应符合表 B.2.8-2 的规定。

表 B.2.8-2 响应信息中可能返回的状态码

SW1	SW2	说　明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
62	81	回送数据可能有错
67	00	Lc 或 Le 长度错误
6A	86	P1、P2 参数错
6C	xx	长度错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
6F	00	数据无效

B.2.9　APPLICATION UNBLOCK 命令应符合下列规定：

1　APPLICATION UNBLOCK 命令用于恢复当前应用。当命令成功完成后，对应用访问的限制将被取消，利用消费密钥校验 MAC2 的错误计数器将被重置。

2　APPLICATION UNBLOCK 命令执行前应执行 GET CHANLLENGE 命令取得 4 字节的随机数。

3　APPLICATION UNBLOCK 命令的执行采用校验模式。计算校验码使用的 KEY 为 ADF 文件中的应用维护密钥。

4　如果应用解锁连续失败三次，卡将永久锁定此应用。

5　APPLICATION UNBLOCK 命令报文格式应符合表 B.2.9-1 的规定。

表 B.2.9-1 APPLICATION UNBLOCK **命令报文格式**

代码	数　值
CLA	‘84’
INS	‘18’
P1	‘00’
P2	‘00’
Lc	‘04’
DATA	信息认证码（MAC）
Le	不存在

6　APPLICATION UNBLOCK 命令的响应状态码应符合表 B.2.9-2 的规定。

表B.2.9-2 响应信息中的状态码

SW1	SW2	说　明
90	00	命令执行成功
62	81	回送数据出错
62	83	选择文件无效
64	00	状态标志位未变
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	00	无信息提供
69	82	不满足安全状态
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	88	安全信息（MAC）数据错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.10　CIPHER DATA 命令应符合下列规定：

1　CIPHER DATA 命令用于对输入数据进行安全计算，支持的安全计算包括：DES 加密解密，DES 计算 MAC，3DES 加密解密，3DES 计算 MAC、SM4 加解密、SM4 计算 MAC。

2　CIPHER DATA 命令的执行应以 DELIVERY KEY 命令为前提条件，即该命令的上一条命令应是 DELIVERY KEY。该命令所使用的 KEY，固定为临时密钥寄存器中的 KEY。

3　本命令成功执行后，临时密钥寄存器中的 KEY 即刻失效。

4　CIPHER DATA 命令报文格式应符合表 B.2.10-1 的规定。

表 B.2.10-1 CIPHER DATA 命令

代码	数　值
CLA	‘80’
INS	‘FA’
P1	‘00’ 无后续块加密计算 ‘05’惟一一块 MAC 计算 ‘08’交通运输部 MAC 计算 ‘80’无后续块解密
P2	‘00’
Lc	P1 = ‘08’时：Lc >= 9 （DES） P1 = ‘08’时：Lc >= 17 （SM4）
	P1 = 其他值： DES 算法：Lc 应是 8 的整数倍；SM4 算法：Lc 应是 16 的整数倍
DATA	安全计算数据。 P1=‘05’，则第一个数据块为 MAC 计算初始值（DES 算法为 8 字节，SM4 算法为 16 字节）； P1 = ‘08’时，随机数（8 字节）+文件数据（DES）；16 字节的初始值（8 字节随机数||8 字节 00）+文件数据（SM4）； P1 = ‘80’ 无后续块解密。
Le	不存在

5　CIPHER DATA 命令的响应状态码应符合表 B.2.10-2 的规定。

表 B.2.10-2 响应信息中可能的状态码

SW1	SW2	说　明
90	00	命令执行成功
61	xx	有 xx 字节要返回
67	00	Lc 长度错误
69	01	Delivery Key 命令没有执行或无效
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.11　CREDIT SAM FOR PURCHASE 命令应符合下列规定：

1　CREDIT SAM FOR PURCHASE 命令利用 INIT SAM FOR PURCHASE 命令产生的过程密钥 SESPK 校验 MAC2。

2　MAC2 校验失败时，计算 MAC2 的 KEY 错误计数器减一，并回送状态码‘63Cx’。当 KEY 错误计数器减为 0 值时，锁定当前应用，可通过应用维护密钥解锁锁定应用。

3　CREDIT SAM FOR PURCHASE 命令成功后，SAM 卡将应用中的消费交易序号加 1。

4　卡片的状态在命令执行后将复原为 MAC1 校验前的状态。

5　用于 MAC2 计算的数据，应符合 JR/T0025-2010《中国金融集成电路（IC）卡规范》。

6　CREDIT SAM FOR PURCHASE 命令应在 INIT SAM FOR PURCHASE 命令成功执行后才能进行。

7　CREDIT SAM FOR PURCHASE 命令报文格式应符合表 B.2.11-1 的规定。

表 B.2.11-1 CREDIT SAM FOR PURCHASE 命令报文格式

代码	值
CLA	‘80’
INS	‘72’
P1	‘00’
P2	‘00’
Lc	‘04’
Data	MAC2
Le	不存在

8 CREDIT SAM FOR PURCHASE 命令响应状态码应符合表 B.2.11-2 的规定。

表 B.2.11-2 响应信息中的状态码

SW1	SW2	含义
90	00	命令成功执行
67	00	Lc 长度错
69	01	命令不接受（无效状态）
69	85	使用条件不满足（应用非永久锁定）
6A	81	功能不支持（卡锁定）
6A	86	参数 P1，P2 不正确
6D	00	命令不存在
6E	00	CLA 错
93	02	MAC 无效
93	03	应用永久锁定

B.2.12 DELIVERY KEY 命令应符合下列规定：

1 DELIVERY KEY 命令将指定的 KEY 分散至临时密钥寄存器中。

2 该命令只支持分散 KEY，不产生过程 KEY。分散后的子 KEY 继承原始 KEY 的属性。

3 DELIVERY KEY 命令的执行应满足 KEY 的使用权。

4 DELIVERY KEY 命令报文格式应符合表 B.2.12-1 的规定。

表 B.2.12-1 DELIVERY KEY 命令报文格式

代码	数　值
CLA	‘80’
INS	‘1A’
P1	密钥用途
P2	密钥标识
Lc	分散数据长度 ‘00’，分散级数为 0 时 ‘08’，分散级数为 1 时 ‘10’，分散级数为 2 时 ‘18’，分散级数为 3 时 其它值保留
DATA	Lc=‘00’不存在 分散因子
Le	不存在

5 DELIVERY KEY 命令响应状态码应符合表 B.2.12-2 的规定。

表 B.2.12-2 响应信息中的状态码

SW1	SW2	说　明
90	00	命令执行成功
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.13 INIT SAM FOR PURCHASE 命令应符合下列规定：

1　INIT SAM FOR PURCHASE 命令支持最多三级消费密钥分散机制，并产生 MAC1。

2　PSAM 卡产生脱机交易流程中 MAC1 的过程如下所示：

1） PSAM 在其内部用 GMPK（全国消费主密钥）对地区分散因子分散，得到二级消费主密钥 BMPK；

2） PSAM 在其内部用 BMPK 对卡片应用序列号分散，得到卡片消费子密钥 DPK；

3） PSAM 在其内部用 DPK 对卡片传来的伪随机数、脱机交易序号、终端交易序号加密，得到过程密钥 SESPK，作为临时密钥存放在卡中；

4） PSAM 在其内部用 SESPK 对交易金额、交易类型标识、终端机编号、交易日期（终端）和交易时间（终端）加密得到 MAC1，将 MAC1 传送出去。

3　INIT SAM FOR PURCHASE 命令中消费密钥的分散过程由 Lc 和消费密钥的属性共同确定，如果二者不一致，则返回错误信息。

4　只有执行 INIT SAM FOR PURCHASE 命令后，才可执行 MAC2 校验命令。

5　INIT SAM FOR PURCHASE 命令报文格式应符合表 B.2.13-1 的规定。

表 B.2.13-1 INIT SAM FOR PURCHASE 命令报文格式

代码	值
CLA	‘80’
INS	‘70’
P1	‘00’
P2	‘00’
Lc	14h＋8×N（N＝1，2，3）
Data	用户卡随机数，4 字节 用户卡交易序号，2 字节 交易金额，4 字节 交易类型标识，1 字节 交易日期（终端），4 字节 交易时间（终端），3 字节 消费密钥版本号，1 字节 消费密钥算法标识，1 字节 用户卡应用序列号，8 字节 分散因子的选取规则按《收费公路联网电子不停车收费技术要求》（交通运输部 2011 年第 13 号公告）第二部分“1 关键信息编码”执行
Le	‘08’（终端交易序号，4 字节；MAC1， 4 字节）

6　INIT SAM FOR PURCHASE 命令响应状态码应符合表 B.2.13-2 的规定。

表 B.2.13-2 响应信息中的状态码

SW1	SW2	含义
90	00	命令执行成功
67	00	Lc 长度错
69	85	使用条件不满足（应用非永久锁定）
6A	81	功能不支持（卡锁定）
6A	86	参数 P1，P2 不正确
6A	88	未找到密钥参数
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.14 WRITE KEY 命令应符合下列规定：

1　WRITE KEY 命令装载或更新 PSAM 卡中的计算密钥，主控密钥采用 SM4 算法。

2　执行 WRITE KEY 命令前，先要执行 GET CHANLLEGE 命令。

3　WRITE KEY 命令数据域中的密钥信息内容：

1） 密钥用途　　1 字节

2） 密钥版本　　1 字节

3） 密钥算法标识　1 字节

4） 密钥使用权限　1 字节

5） 错误计数器　　1 字节

6） 密钥值　　8 字节或 16 字节

4　WRITE KEY 命令报文格式应符合表 B.2.14-1 的规定。

表 B.2.14-1 WRITE KEY 命令报文格式

代码	值
CLA	‘84’
INS	‘D4’
P1	‘00’
P2	‘00’
Lc	‘14’或‘24’
Data	密文密钥信息 ‖ MAC
Le	不存在

5　WRITE KEY 命令响应状态码应符合表 B.2.14-2 的规定。

表 B.2.14-2 响应信息中的状态码

SW1	SW2	含义
90	00	命令执行成功
65	81	内存失败
67	00	Lc 长度错
69	83	认证密钥锁定
69	84	引用数据无效（未取随机数）
69	85	使用条件不满足（应用非永久锁定）
69	88	安全报文数据项不正确
6A	80	数据域参数不正确
6A	81	功能不支持（卡锁定）
6A	86	参数 P1，P2 不正确
6A	88	未找到密钥参数
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.2.15 SET ALGORITHM 命令应符合下列规定：

1 SET ALGORITHM 命令实现永久关闭 3DES 算法的功能。执行该命令成功后，所有指定使用 3DES 密钥进行运算的命令都应返回错误状态 SW=6600。

2 执行 SET ALGORITHM 命令前，需要先认证 PSAM 卡外部认证密钥 UK_MF 成功后才能取得执行权限。

3 SET ALGORITHM 命令报文格式应符合表 B.2.15-1 的规定。

表 B.2.15-1 SET ALGORITHM 命令报文格式

代码	值
CLA	‘80’
INS	‘FE’
P1	‘03’
P2	‘00’
Lc	‘00’
Data	不存在
Le	不存在

4 SET ALGORITHM 命令的响应状态码应符合表 B.2.15-2 的规定。

表 B.2.15-2 响应信息中的状态码

SW1	SW2	含义
90	00	命令执行成功
65	81	内存失败
69	82	不满足安全状态
6A	86	参数 P1，P2 不正确
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

附录 C OBE-SAM 数据格式与应用命令集

C.1 OBE-SAM 数据格式

C.1.1 OBE-SAM 的文件结构应符合图 C.1.1 的规定：

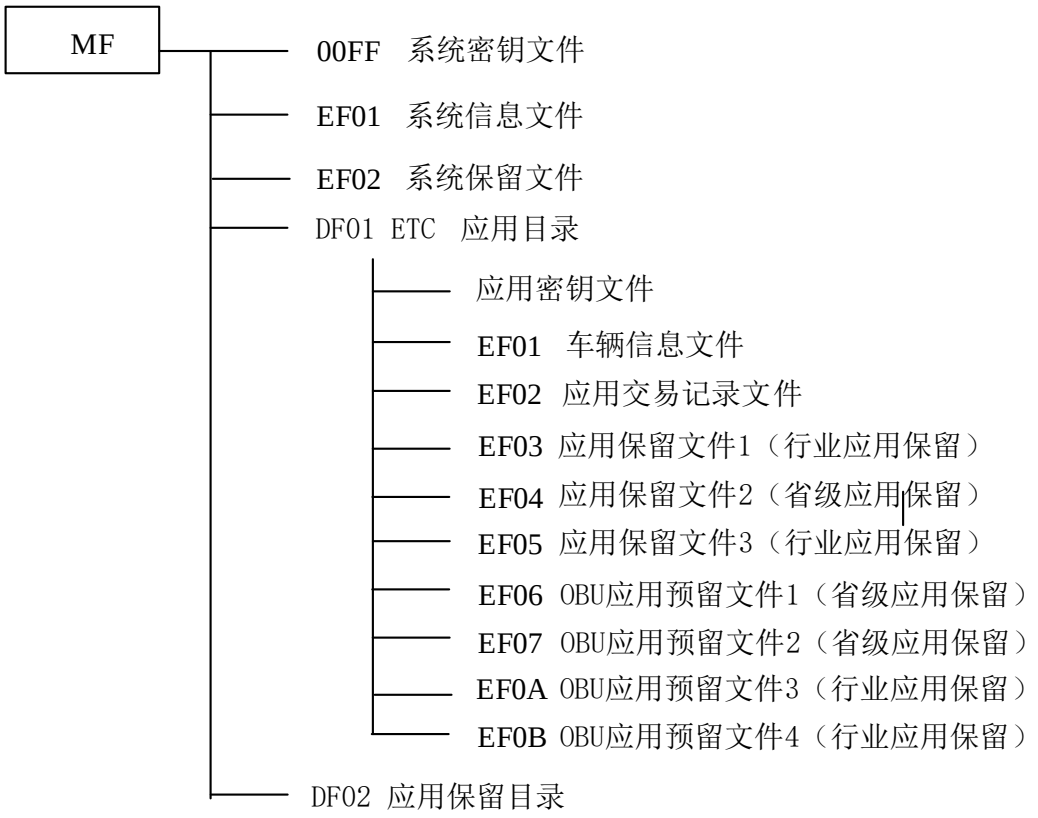

图 C.1.1 OBE-SAM 文件结构

C.1.2 OBE-SAM 详细文件结构应符合表 C.1.2 的规定：

表 C.1.2 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	DF01 应用加密密钥线路保护	$DAMK_{DF01}$	DF01 应用加密密钥线路保护读，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，57 字 x50 条记录
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

注：

1. 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。
2. 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。

3. 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；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。
4. 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。
5. 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。
6. 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。

C.1.3 系统信息文件（EF01）结构应符合表 C.1.3-1 的规定：

表 C.1.3-1 系统信息文件

字节	类型	长度（字节）	内容
1 – 8	cn	8	发行方标识，
9	cn	1	协约类型
10	cn	1	合同版本 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，格式应符合C.1.3-2 的规定。
28 – 99	an	72	预留
说明： （1）依照本标准发行的 OBE-SAM，版本高 4 位统一定义为“5”，以后升级时可修改为更大值； （2）省内不得自行扩展该文件长度。			

C.1.3-2 拆卸状态定义

	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		

C.1.4 系统保留文件应符合表 C.1.4 的规定：

表 C.1.4 系统保留文件

字节	类型	长度（字节）	内容
1 – 512	an	512	预留

C.1.5 车辆信息文件结构应符合表 C.1.5 的规定：

表C.1.5车辆信息文件

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；0x04-小型新能源汽车号牌颜色；0x05-大型新能源汽车号牌颜色； 0x06～0xFF 保留
15	cn	1	车型，编码方式见 GB/T 31442-2015 附表 A.1
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

C.1.6 应用交易记录文件结构应符合表 C.1.6 的规定：

表 C.1.4 应用交易记录文件

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，编码方式见 GB/T 31442-2015 附表 A.1
7– 8	b	2	收费站编码，编码方式见 GB/T 31442-2015 附表 A.1
9	b	1	收费车道编码，编码方式见 GB/T 31442-2015 附表 A.1
10	b	1	卡类型，编码方式见 GB/T 31442-2015 附表 A.1
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。

C.1.7 应用保留文件 1（EF03）结构应符合表 C.1.7 的规定：

表 C.1.7 应用保留文件 1

字节	类型	长度（字节）	内容
1 – 512	an	512	预留

C.1.8 应用保留文件 2（EF04）结构应符合表 C.1.8 的规定：

表 C.1.8 应用保留文件 2

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

C.1.9 应用保留文件 3（EF05）结构应符合表 C.1.9 的规定：

表 C.1.9 应用保留文件 3

字节	类型	长度（字节）	内容
1 – 512	an	512	预留

C.1.10 OBU 应用预留文件 1（EF06）结构应符合表 C.1.10 的规定：

表 C.1.10 OBU 应用预留文件 1

字节	类型	长度（字节）	内容
1 – 512	an	512	预留

C.1.11 OBU 应用预留文件 2（EF07）应符合表 C.1.11 的规定

表 C.1.11 OBU 应用预留文件 2

字节	类型	长度（字节）	内容
1 – 512	an	512	预留

C.1.12 OBU 应用预留文件 3（EF0A）结构应符合表 C.1.12 的规定：

表 C.1.12 OBU 应用预留文件 3

字节	类型	长度（字节）	内容
1 – 128	an	128	预留

C.1.13 OBU 应用预留文件 4（EF0B）结构应符合表 C.1.13 的规定：

表 C.1.13 OBU 应用预留文件 4

字节	类型	长度（字节）	内容
1 – 512	an	512	预留

C.2 OBE-SAM 应用命令集

C.2.1 DECREASE COUNTER 命令应符合下列规定：

1 DECREASE COUNTER 命令每成功执行一次，拆卸次数（即拆卸状态的低 4 位）应减 1.

2 DECREASE COUNTER 命令报文应符合表 C.2.1-1 的规定：

表 C.2.1-1 DECREASE COUNTER 命令报文

代码	数　值
CLA	‘00’
INS	‘59’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘01’

3 DECREASE COUNTER 命令报文数据域不存在。

4 DECREASE COUNTER 命令响应报文数据域应为剩余次数。

5 DECREASE COUNTER 命令响应报文状态码应符合表 C.2.1-2 的规定：

表 C.2.1-2 DECREASE COUNTER 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	85	使用条件不满足，拆卸次数已经为 0
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

C.2.2　EXTERNAL AUTHENTICATE 命令应符合下列规定：

1　EXTERNAL AUTHENTICATE 命令执行成功后，应使外部接口设备对 PSAM 卡获得某种操作授权。

2　接口设备提供的认证数据应按以下规则产生：

1) 用 GET CHALLENGE 命令向 IC 卡申请一组随机数；

2) 用指定密钥对随机数（后面填充 0x00 至 8 字节（3DES）或 16 字节（SM4）后）做加密运算产生。

3) 对于 SM4 算法，认证数据为 16 字节密文前后 8 字节进行异或的结果，长度仍为 8 字节。

3　EXTERNAL AUTHENTICATE 命令执行时应满足 P2 参数所指定密钥的使用权限。

4　密钥验证失败时相应外部认证密钥的错误计数器应减 1，当计数器减为‘0’值时，密钥被锁定。

5　EXTERNAL AUTHENTICATE 命令报文格式应符合表 C.2.2-1 的规定：

C.2.2-1 EXTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	外部认证密钥标识
Lc	‘08’
Data	认证数据
Le	不存在

6　命令响应报文状态码应符合表 C.2.2-2 的规定：

C.2.2-2 EXTERNAL AUTHENTICATION 响应报文状态码

SW1	SW2	含　义
90	00	命令执行成功
63	‘CX’	认证失败，‘X’为剩余的可尝试次数
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘6A’	‘86’	参数 P1 P2 不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

C.2.3　GET CHALLENGE 命令应符合下列规定：

1　GET CHALLENGE 命令请求一个用于安全相关过程(例如安全报文)的随机数，该随机数只能用于下一条指令，无论下一条指令是否使用了该随机数，该随机数都将立即失效。

2　GET CHALLENGE 命令报文应符合表 C.2.3-1 的规定。

表 C.2.3-1 GET CHALLENGE 命令报文

代码	数　值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘04’,‘08’ ,‘10’

3　GET CHALLENGE 命令响应报文数据域为随机数，长度为 4 字节或 8 字节或 16 字节。

4　GET CHALLENGE 命令响应报文状态码应符合表 C.2.3-2 的规定：

表 C.2.3 -2 GET CHALLENGE 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
67	00	Le 长度错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

C.2.4　GET RESPONSE 命令应符合下列规定：

1　当 APDU 不能用现有协议传输时，GET RESPONSE 命令提供了一种从 OBE-SAM

向接口设备传送 APDU（或 APDU 的一部分）的传输方法。

2　GET RESPONSE 命令报文应符合表 C.2.4-1 的规定。

表 C.2.4-1 GET RESPONSE 命令报文

代码	数　值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	响应的最大数据长度

3　GET RESPONSE 命令响应报文数据域长度由 Le 的值决定。如果 Le 的值为零，在附加数据有效时，OBE-SAM 应回送状态码‘6CXX’，否则回送状态码‘6F00’。

4　OBE-SAM 回送的响应信息中出现的状态码应符合表 C.2.4-2 的规定。

表 C.2.4-2 GET RESPONSE 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
62	81	回送数据有错
67	00	Lc 或 Le 长度错误
6A	86	P1、P2 参数错
6C	xx	长度错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
6F	00	数据无效

C.2.5　Get SN 命令应符合下列规定：

1　Get SN 命令用于读取 OBE-SAM 安全模块中卡商惟一的芯片序列号。

2　Get SN 命令执行无权限限制。

3　Get SN 命令报文应符合表 C.2.5-1 的规定。

表 C.2.5-1 Get SN 命令报文

代码	数　值
CLA	‘80’
INS	‘F6’
P1	‘00’
P2	‘03’
Lc	不存在
DATA	不存在
Le	‘04’

4　Get SN 命令响应报文数据域包括 4 字节芯片序列号。

5　OBE-SAM 回送的响应信息中出现的状态码应符合表 C.2.5-2 的规定：

表 C.2.5-2 Get SN 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
6A	86	P1、P2 参数错
6C	xx	Le 错误
6D	00	命令不存在
6E	00	CLA 错

C.2.6　READ DATA 命令应符合下列规定：

1　READ DATA 命令用于读出应用车辆信息文件中的数据，读出的数据为密文。

2　READ DATA 命令报文格式应符合表 C.2.6-1 的规定。

表 C.2.6-1 READ DATA 命令报文

代码	数　值
CLA	‘00’
INS	‘B4’
P1	偏移地址高字节
P2	偏移地址低字节
Lc	‘0A’
DATA	随机数(8B)+期望读取的信息数据明文长度(1B)+密钥版本（1B）
Le	00

3　READ DATA 命令响应报文数据域应为“鉴别码+读取数据”的密文形式，鉴别码和密文的计算方法应符合附录 A 的规定。

4　OBE-SAM 回送的响应信息中的状态码应符合表 C.2.6-2 的规定。

表 C.2.6-2 READ DATA 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
61	xx	还有 xx 字节要返回
62	81	部分回送的数据有错
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是二进制文件
69	85	使用条件不满足
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6C	xx	Le 长度错误。‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

C.2.7　READ BINARY 命令

1　READ BINARY 命令用于读出二进制文件的内容（或部分内容）。

2　READ BINARY 命令报文应符合表 C.2.7-1 的规定。

表 C.2.7-1 READ BINARY 命令报文

代码	数　值								
CLA	‘00’或‘04’								
INS	‘B0’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	1）不存在——明文方式 2）‘04’——校验方式								
DATA	1）不存在 2）MAC								
Le	期望返回的数据长度								

3　READ BINARY 命令报文数据域一般情况下不存在。当使用安全报文时，命令报

文数据域中应包含 MAC。MAC 的计算方法和长度应符合附录 A 的规定。

6　READ BINARY 命令响应报文数据域，当 Le 的值为零时，当从指定的偏移量至文件结束，长度小于 256 字节、等于 256 字节、大于 256 字节时，返回数据长度应符合表 C.2.7-2 的规定

表 C.2.7-2 Le=0 时的命令响应信息

实际长度	小于 256 字节	等于 256 字节	大于 256 字节
返回数据	6CXX，其中 XX 为实际长度	返回 256 字节	返回 256 字节

4　OBE-SAM 回送的响应信息中的状态码应符合表 C.2.7-3 的规定。

表 C.2.7-3 READ BINARY 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
61	Xx	还有 xx 字节要返回
62	81	部分回送的数据有错
62	82	文件长度<Le
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是二进制文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6C	Xx	Le 长度错误。‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

C.2.8　READ RECORD 命令应符合下列规定：

1　READ RECORD 命令读记录文件中的内容。

2　READ RECORD 命令报文应符合表 C.2.8-1 的规定。

表 C.2.8-1 READ RECORD 命令报文

代码	数　值								
CLA	‘00’或‘04’								
INS	‘B2’								
P1	记录号								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	0	0	0	0	-	-	-	当前文件
	x	x	x	x	x	-	-	-	通过 SFI 方式访问
	-	-	-	-	-	1	0	0	P1 指定的记录号
	其他值								保留
Lc	1) 不存在——明文方式 2)‘04’—— 命令报文校验方式								
DATA	1）不存在——明文方式 2）MAC——校验方式								
Le	期望返回的记录数据								

3　一般情况下命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含 MAC。MAC 的计算方法和长度由应用决定。

4　所有执行成功的 READ RECORD 命令的响应报文数据域由读取的记录组成。

5　OBE-SAM 回送的响应信息中的状态码应符合表 C.2.8-2 的规定。

表 C.2.8-2 READ RECORD 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
62	81	回送的数据有错
64	00	标志状态位没变
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效(未申请随机数)
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6C	xx	Le 错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

C.2.9　SELECT FILE 命令应符合下列规定

1　SELECT FILE 命令通过文件标识或应用名选择 OBE-SAM 中的 MF、DDF、ADF 或 EF 文件。

2　成功执行该命令设定 MF、DDF 或 ADF 的路径。

3　应用到 EF 的后续命令将采用 SFI 方式联系到所选定的 MF、DDF 或 ADF。

4　从 OBE-SAM 返回的应答报文包含回送 FCI。

5　FCI 数据从数据分组中获得。

6　SELECT FILE 命令报文应符合表 C.2.9-1 的规定。

表 C.2.9-1 SELECT FILE **命令报文**

代码	数　值
CLA	‘00’
INS	‘A4’
P1	‘00’通过 FID 选择 DF、EF，当 Lc=‘00’时，选 MF ‘04’通过 DF 名选择应用
P2	‘00’ ‘02’选择下一个文件（P1=04h 时）
Lc	P1=‘00’时，Lc=‘00’或‘02’ P1=‘04’时，Lc=‘05’~‘10’
DATA	文件标识符（FID—2 字节） 应用名（App-Name，P1=‘04’）
Le	FCI 文件的信息长度（选择 DF 时）

7　命令报文数据域应包括所选择的 DDF 名、DF 名或 FID，以及 EF 的 FID。

8　响应报文数据域中的数据应包括所选择的 MF、DDF、ADF 的 FCI。

9　成功选择 MF 后回送的 FCI 应符合表 C.2.9-2 的规定。

表 C.2.9-2 **成功选择** MF **响应报文** FCI

标识	值			存在性
‘6F’	FCI 模板			M
	‘84’	DF		M
	‘A5’	FCI 数据专用模板		M
		‘88’	目录基本文件的 SFI	M
		‘9F0C’	FCI 文件内容	O

10　成功选择 DDF 后回送的 FCI 应符合表 C.2.9-3 的规定。

表 C.2.9-3 **成功选择** DDF **响应报文** FCI

标签	值			存在性
‘6F’	FCI 模板			M
	‘84’	DF 名		M
	‘A5’	FCI 数据专用模板		M
		‘88’	目录基本文件的 SFI	M
		‘9F0C’	FCI 文件内容	O

11　成功选择 ADF 后回送的 FCI 应符合表 C.2.9-4 的规定。

表 C.2.9-4 成功选择 ADF 响应报文 FCI

标签	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名	M
	‘A5’	FCI 数据专用模板	M
	‘9F0C’	FCI 文件内容	O

12 OBE-SAM 回送的响应信息中的状态码应符合表 C.2.9-5 的规定。

表 C.2.9-5 SELECT FILE 响应报文状态码

SW1	SW2	说 明
90	00	命令执行成功
62	83	选择文件无效
62	84	FCI 格式与 P2 指定的不符
64	00	标志状态位没变
67	00	Lc 长度错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	87	Lc 与 P1-P2 不匹配
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

C.2.10 UPDATE BINARY 命令

1 UPDATE BINARY 命令用于更新二进制文件中的数据。

2 UPDATE BINARY 命令报文应符合表 C.2.10-1 的规定。

表 C.2.10-1 UPDATE BINARY 命令报文

代码	数 值								
CLA	‘00’或‘04’								
INS	‘D6’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	DATA 域数据长度								
DATA	明文方式： 明文数据 加密方式： 密文数据 校验方式： 明文数据||校验码 校验加密方式：密文数据||校验码								
Le	不存在								

3 命令报文数据域包括更新原有数据的数据域。

4 OBE-SAM 回送的响应信息中的状态码应符合表 C.2.10-2 的规定。

表 C.2.10-2 UPDATE BINARY 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是二进制文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

C.2.11 UPDATE RECORD 命令应符合下列规定：

1　UPDATE RECORD 命令用于更新记录文件中的数据。

2　在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

3　UPDATE RECORD 命令报文应符合表 C.2.11-1 的规定。

表 C.2.11-1 UPDATE RECORD 命令报文

代码	数　值								
CLA	‘00’或‘04’								
INS	‘DC’								
P1	P1= ’00’ 表示当前记录 P1≠ ‘00’ 表示指定的记录号或记录标识								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	0	0	0	0	-	-	-	当前文件
	x	x	x	x	x	-	-	-	通过 SFI 方式访问
	-	-	-	-	-	1	0	0	P1 指定的记录号
	-	-	-	-	-	0	0	0	第一条记录
	-	-	-	-	-	0	0	1	最后一条记录
	-	-	-	-	-	0	1	0	下一条记录
	-	-	-	-	-	0	1	1	前一条记录
	任何其他值								保留
Lc	DATA 域数据长度								
DATA	明文方式：　　明文记录数据 加密方式：　　密文记录数据 校验方式：　　明文记录数据||校验码 校验加密方式：密文记录数据|校验码								
Le	不存在								

4　命令报文数据域由更新原有记录的新记录组成。

5　OBE-SAM 回送的响应信息中的状态码应符合表 C.2.11-2 的规定。

表 C.2.11-2 UPDATE RECORD 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	84	存储空间不够
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

C.2.12 UPDATE KEY 命令应符合下列规定：

1　UPDATE KEY 命令用于更新一个已经存在的密钥。

2　本命令可支持 8 字节或 16 字节的密钥，密钥写入应采用密文+MAC 的方式，在主控密钥的控制下进行。

3　在密钥装载前应用 GET CHANLLEGE 命令从 OBE-SAM 取一个 4 字节的随机数。

4　UPDATE KEY 命令报文应符合表 C.2.12-1 的规定。

表 C.2.12-1 UPDATE KEY 命令报文

代 码	值
CLA	‘84’
INS	‘D4’
P1	‘01’
P2	‘00’--更新主控密钥 ‘FF’--更新其他密钥
Lc	‘14’或‘24’
DATA	密文密钥信息‖MAC
Le	不存在

5　命令报文数据域包括要装载的密钥密文信息和 MAC。密钥密文信息是用主控密钥对以下数据加密（按所列顺序）产生的：

——密钥用途

——密钥标识

——版本

——密钥值

MAC 是用主控密钥对以下数据进行 MAC 计算（按所列顺序）产生的：

——CLA

——INS

——P1

——P2

——Lc

——密钥密文信息

装载 8 字节的单长度密钥时，数据长度为 0x14；装载 16 字节的双长度密钥时，数据长度为 0x24。

6　响应信息中的状态码应符合表 C.2.12-2 的规定。

表 C.2.12-2 UPDATE KEY 响应报文状态码

SW1	SW2	含　义
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	88	安全信息（MAC 和密文）数据错误
6A	80	数据域参数错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到密钥数据
6A	84	文件空间已满
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

C.2.13　SET ALGORITHM 命令应符合下列规定

1　该命令实现永久关闭应用下 3DES 算法的功能。

2　执行该命令成功后，在相应应用下所有指定使用 3DES 密钥进行运算的命令都应返回错误状态 SW=6600。

3　执行 SET ALGORITHM 命令前，需要先选择应用，然后认证应用外部认证密钥成功后才能取得执行权限。

4　SET ALGORITHM 命令报文格式应符合表 C.2.13-1 的规定。

表 C.2.13-1 SET ALGORITHM 命令报文格式

代码	值
CLA	‘80’
INS	‘FE’
P1	‘03’
P2	‘00’
Lc	‘00’
Data	不存在
Le	不存在

5　响应信息中的状态码应符合表 C.2.13-2 的规定。

表 C.2.13-2 响应信息中的状态码

SW1	SW2	含义
90	00	命令执行成功
65	81	内存失败
69	82	不满足安全状态
6A	86	参数 P1，P2 不正确
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

附录 D CPU 用户卡数据格式与应用命令集

D.1 CPU 用户卡数据格式

D.1.1 CPU 用户卡的文件结构应符合图 D.1.1 的规定。

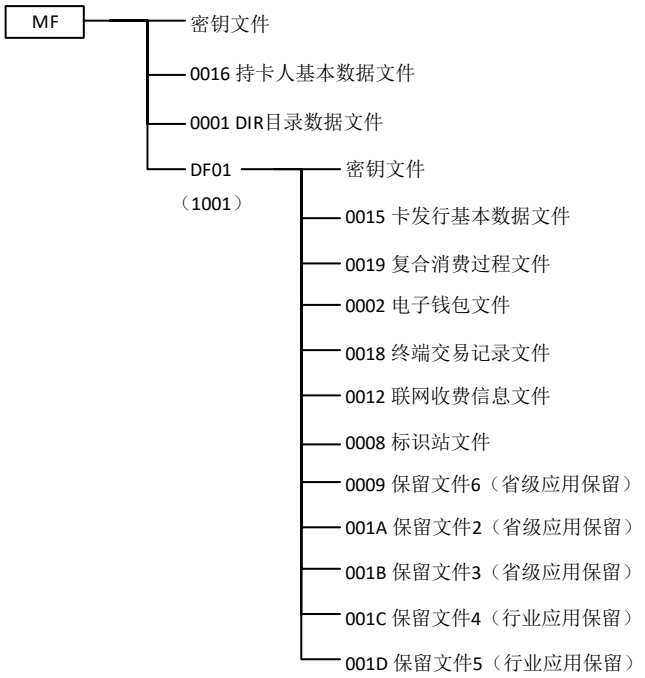

图 D.1.1 CPU 用户卡文件结构图

D.1.2 CPU 用户卡详细文件结构应符合表 D.1.2 的规定：

表 D.1.2 CPU 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/擦除权：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，记录长度为 23 字节，不少于 50 条交易记录
联网收费信息文件	二进制文件	0012	自由	$UK1_{DF01}$ 或 $UK2_{DF02}$	自由读，外部认证 $UK1_{DF01}$ 或 $UK2_{DF02}$ 通过后可以写，无线路保护
标识站文件	二进制文件	0008	自由	$UK1_{DF01}$ 或 $UK2_{DF02}$	外部认证 $UK1_{DF01}$ 或 $UK2_{DF02}$ 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	$UK1_{DF01}$ 或 $UK2_{DF02}$	外部认证 $UK1_{DF01}$ 或 $UK2_{DF02}$ 通过后可以写，无线路保护
保留文件 4	二进制文件	001C	自由	$UK1_{DF01}$ 或 $UK2_{DF02}$	外部认证 $UK1_{DF01}$ 或 $UK2_{DF02}$ 通过后可以写，无线路保护
保留文件 5	二进制文件	001D	自由	$UK1_{DF01}$ 或 $UK2_{DF02}$	外部认证 $UK1_{DF01}$ 或 $UK2_{DF02}$ 通过后可以写，无线路保护

注：

1. 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。
2. 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；其他短文件标识符作为行业应用保留，各省（区、市）不得应用。
3. 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。
4. 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。
5. 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。
6. 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，通过外部认证达到写入权限，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。
7. 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。
8. 保留文件 4（001C）、保留文件 5（001D）为行业应用保留文件，可通过外部认证达到写入权限，各省（区、市）不得自行使用。
9. 保留文件 6（0009），作为省级应用保留文件。

D.1.3 持卡人基本数据文件（0016）结构应符合表 D.1.3 的规定。

表 D.1.3 持卡人基本数据文件结构

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	编码方式见 GB/T 31442-2015 附表 A.1

D.1.4 卡片发行基本数据文件（0015）结构应符合表 D.1.4 的规定。

D.1.4 卡片发行基本数据文件结构

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》（交通运输部 2011 年第 13 号公告）第二部分“1 关键信息编码”
9	卡片类型	1	编码方式见 GB/T 31442-2015 附表 A.1
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	编码方式为：省级行政区划代码+运营商序号，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》（交通运输部 2011 年第 13 号公告）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-小型新能源汽车号牌颜色；0x05-大型新能源汽车号牌颜色； 0x06～0xFF 保留
43	车型	1	车型，编码方式见 GB/T 31442-2015 附表 A.1
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）依照本标准发行的卡片，版本高 4 位统一定义为“5”，以后升级时可修改为更大值；

（2）省内不得自行扩展该文件长度。

D.1.5 联网收费复合消费过程文件（0019）结构应符合表 D.1.5 的规定。

表 D.1.5 联网收费复合消费过程文件结构

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	编码方式见 GB/T 31442-2015 附表 A.1
6～7	入/出口收费站号	2	编码方式见 GB/T 31442-2015 附表 A.1
8	入/出口收费车道号	1	编码方式见 GB/T 31442-2015 附表 A.1
9～12	入/出口时间	4	UNIX 时间（注）
13	车型	1	编码方式见 GB/T 31442-2015 附表 A.1
14	入出口状态	1	编码方式见 GB/T 31442-2015 附表 A.1
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	编码方式见 GB/T 31442-2015 附表 A.1
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

字节	数据元	长度（字节）	说明
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。			

D.1.6 电子钱包文件（0002）结构应符合表 D.1.6 的规定。

表 D.1.6 电子钱包文件结构

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

D.1.7 终端交易记录文件（0018）结构应符合表 D.1.7 的规定。

表 D.1.7 终端交易记录文件结构

字节	数据元	长度（字节）	说明
1～2	联机或脱机交易序号	2	CPU 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、复合消费等
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

D.1.8 联网收费信息文件（0012）结构应符合表 D.1.8 的规定

表 D.1.8 联网收费信息文件结构

字节	数据元	长度（字节）	说明
1～2	入口收费路网号	2	编码方式见 GB/T 31442-2015 附表 A.1
3～4	入口收费站号	2	编码方式见 GB/T 31442-2015 附表 A.1
5	入口收费车道号	1	编码方式见 GB/T 31442-2015 附表 A.1
6～9	入口时间	4	UNIX 时间
10	车型	1	编码方式见 GB/T 31442-2015 附表 A.1
11	入出口状态	1	编码方式见 GB/T 31442-2015 附表 A.1
12～20	标识站	9	编码方式见 GB/T 31442-2015 附表 A.1
21～23	收费员工号	3	二进制方式存放入口员工号后六位
24	入口班次	1	MTC 车道收费班次
25～36	车牌号码	12	编码方式见 GB/T 31442-2015 附表 A.1
37～40	预留	4	

D.1.9 标识站应用文件（0008）结构见表 D.1.9。

表 D.1.9 标识站应用文件的文件结构

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			

D.1.10 保留文件 6（0009）结构应符合表 D.1.10 的规定。

表 D.1.10 保留文件 6 的文件结构

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

D.1.11 保留文件 2（001A）结构应符合表 D.1.11 的规定。

表 D.1.11 保留文件 2 的文件结构

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”。

D.1.12 保留文件 3（001B）结构应符合表 D.1.12 的规定。

表 D.1.12 保留文件 3 的文件结构

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”。

D.1.13 保留文件 4（001C）结构应符合表 D.1.13 的规定。

表 D.1.13 保留文件 4 的文件结构

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

D.1.14 保留文件 5（001D）结构应符合表 D.1.14 的规定。

表 D.1.14 保留文件 5 的文件结构

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

D.2 CPU 用户卡应用命令集

D.2.1 未在本标准列出的 CPU 用户卡应用命令应符合 JR/T 0025.1-2010，JR/T 0025.2-2010，JR/T 0025.9-2010。

D.2.2 EXTERNAL AUTHENTICATION 命令符合下列规定：

1 EXTERNAL AUTHENTICATE 命令执行成功后，应使外部接口设备对 PSAM 卡获得某种操作授权。

2 接口设备提供的认证数据应按以下规则产生：

1) 用 GET CHALLENGE 命令向 IC 卡申请一组随机数；

2) 用指定密钥对随机数（后面填充 0x00 至 8 字节（3DES）或 16 字节（SM4）后）做加密运算产生。

3) 对于 SM4 算法，认证数据为 16 字节密文前后 8 字节进行异或的结果，长度仍为 8 字节。

3 EXTERNAL AUTHENTICATE 命令执行时应满足 P2 参数所指定密钥的使用权限。

4 密钥验证失败时相应外部认证密钥的错误计数器应减 1，当计数器减为‘0’值时，密钥被锁定。

5 EXTERNAL AUTHENTICATE 命令报文格式应符合表 D.2.2-1 的规定：

表 D.2.2-1 EXTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	外部认证密钥标识
Lc	‘08’
Data	认证数据
Le	不存在

6 EXTERNAL AUTHENTICATE 命令响应报文状态码应符合表 D.2.2-2 的规定

表 D.2.2-2 EXTERNAL AUTHENTICATION 响应状态码

SW1	SW2	含　义
‘90’	‘00’	认证成功
‘63’	‘CX’	认证失败，‘X’为剩余的可尝试次数
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘6A’	‘86’	参数 P1 P2 不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

D.2.3　GET CHALLENGE 命令应符合下列规定

1　GET CHALLENGE 命令请求一个用于安全相关过程(例如安全报文)的随机数。

2　该随机数只能用于下一条指令，无论下一条指令是否使用了该随机数，该随机数都将立即失效。

3　GET CHALLENGE 命令报文应符合表 D.2.3-1 的规定。

表 D.2.3-1 GET CHALLENGE 命令报文

代码	数　值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘04’,‘08’, ‘10’

4　响应报文数据域包括随机数，长度为 4 字节或 8 字节或 16 字节。

5　OBE-SAM 回送的响应信息中出现的状态码应符合表 D.2.3-2 的规定。

表 D.2.3-2 GET CHALLENGE 响应报文状态码

SW1	SW2	说　明
90	00	命令执行成功
67	00	Le 长度错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

D.2.4 INTERNAL AUTHENTICATION 命令应符合下列规定

1 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。

2 INTERNAL AUTHENTICATION 命令报文编码应符合表 D.2.4-1 的规定。

表 D.2.4-1 INTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘88’
P1	‘00’
P2	内部认证密钥标识
Lc	认证数据的长度
Data	认证数据
Le	‘00’

3 命令报文数据域的内容是应用专用的认证数据。

4 响应报文数据域内容是相关认证数据。

5 响应报文状态字应符合表 D.2.4-2 的规定

表 D.2.4-2 INTERNAL AUTHENTICATION 响应状态码

SW1	SW2	含 义
90	00	命令执行成功
‘62’	‘81’	回送的数据可能有错
‘64’	‘00’	标志状态位未变
‘67’	‘00’	Lc 域不存在
‘68’	‘82’	不支持安全报文
‘69’	‘85’	不满足使用条件
‘6A’	‘80’	数据域参数不正确
‘6A’	‘86’	P1 和 P2 错误
‘6D’	‘00’	INS 不支持或错误

D.2.5 PIN UNBLOCK 命令

1 PIN UNBLOCK 命令为发卡方提供了解锁个人识别码的功能。 当 PIN UNBLOCK 命令成功完成后，卡将执行以下功能：

——重置个人识别码尝试计数器的值。 命令中个人识别码的传递采用加密方式。

2 PIN UNBLOCK 命令报文编码应符合表 D.2.5-1 的规定。

表D.2.5-1 PIN UNBLOCK 命令报文

代码	值
CLA	‘84’
INS	‘24’
P1	‘00’
P2	应用 PIN 解锁子密钥的标识
Lc	数据字节数
Data	加密的个人识别码数据元和报文鉴别码（MAC）数据元
Le	不存在

3　命令报文数据域由加密的个人识别码数据元和其后的 MAC 数据元组成。加密和 MAC 计算方法应符合附录 A 的规定。

4　　响应报文状态码应符合表 D.2.5-2 的规定

表 D.2.5-2 PIN UNBLOCK **警告状态**

SW1	SW2	含　义
90	00	命令执行成功
‘62’	‘00’	无信息提供
‘62’	‘81’	数据或能出错
‘64’	‘00’	标志状态位没变
‘65’	‘81’	内存失败
‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘85’	使用条件不满足（PIN 未锁定）
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	P1 和 P2 错误
‘6A’	‘88’	未找到引用数据
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用被永久锁定

D.2.6　重装个人识别码（RELOAD PIN）命令

1　重装个人识别码（RELOAD PIN）命令用于发卡方重新给持卡人产生一个新的 PIN（可以与原 PIN 相同）。 重装个人识别码（RELOAD　PIN）只能在拥有或能访问到重装 PIN 子密钥（DRPK）的发卡方终端上执行。在成功执行重装个人识别码（RELOAD　PIN）命令后，IC 卡必须完成以下操作：

——PIN 尝试计数器复位。

——IC 卡的原 PIN 必须设置为新的 PIN 值。命令中的 PIN 数据以明文传送。

2 RELOAD PIN 命令连续执行三次失败后，应用将永久锁定。

3 重装个人识别码（RELOAD PIN）命令报应符合表 D.2.6-1 的规定。

表 D.2.6-1 重装个人识别码（RELOAD PIN）命令报文

代码	值
CLA	‘80’
INS	‘5E’
P1	‘00’
P2	应用 PIN 重装子密钥的标识
Lc	‘06’～‘0A’
Data	见表 D.2.6-2
Le	不存在

4 命令报文数据域应符合表 D.2.6-2 的规定

表 D.2.6-2 重装个人识别码（RELOAD PIN）命令报文数据域

说明	长度（字节）
重装的 PIN 值	2-6
MAC	4

5 对于 3DES 算法，用 DRPK 左右 8 字节进行异或运算后的结果按照附录 A 中描述的机制对新 PIN 值计算 MAC。

6 对于 SM4 算法，用 DRPK 密钥按照附录 A 中描述的机制对新 PIN 值计算 MAC。

7 响应报文的状态字应符合表 D.2.6-3 的规定

表 D.2.6-3 重装个人识别码（RELOAD PIN）响应状态码

SW1	SW2	含义
‘90’	‘00’	命令执行成功
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘69’	‘88’	安全信息数据对象不正确
‘6A’	‘80’	PIN 格式不规范
‘6A’	‘86’	P1 和 P2 参数不正确
‘6A’	‘88’	引用数据找不到
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用永久锁住

D.2.7 SET ALGORITHM 命令

1 该命令实现永久关闭应用下 3DES 算法的功能。执行该命令成功后，相应应用下所有指定使用 3DES 密钥进行运算的命令都应返回错误状态 SW=6600。

2 执行 SET ALGORITHM 命令前，需要先选择应用目录，然后认证外部认证子密钥成功后才能取得执行权限。

3 SET ALGORITHM 命令报文格式应符合表 D.2.7-1 的规定。

表 D.2.7-1 SET ALGORITHM 命令报文格式

代码	值
CLA	‘80’
INS	‘FE’
P1	‘03’
P2	‘00’
Lc	‘00’
Data	不存在
Le	不存在

4 响应信息中的状态码应符合表 D.2.7-2 的规定。

表 D.2.7-2 响应信息中的状态码

SW1	SW2	含义
90	00	命令执行成功
65	81	内存失败
69	82	不满足安全状态
6A	86	参数 P1，P2 不正确
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定