

高速公路区域联网不停车收费示范工程暂行技术要求 第 7 部分

电子收费 OBE_SAM 安全模块技术要求

2008 年 8 月

目 次

1.	范围	2
2.	缩略语	2
3.	OBE-SAM 的主要功能	2
4.	OBE-SAM 文件结构	2
5.	文件详细说明	4
6.	OBE_SAM 内密钥说明	7
7.	OBE_SAM 密钥管理	7
8.	ESAM 复位信息的约定	7
9.	OBE_SAM 应用命令集	8

电子收费 OBE_SAM 安全模块技术要求

1. 范围

本标准规定了 OBE-SAM 的主要功能、OBE-SAM 文件结构、文件详细说明、OBE_SAM 内密钥说明、OBE_SAM 密钥管理、ESAM 复位信息的约定、OBE_SAM 应用命令集。

2. 缩略语

an: 字母数字型 (Alphanumeric)

b: 二进制 (Binary)

cn: 压缩数字 (Compressed Numeric)

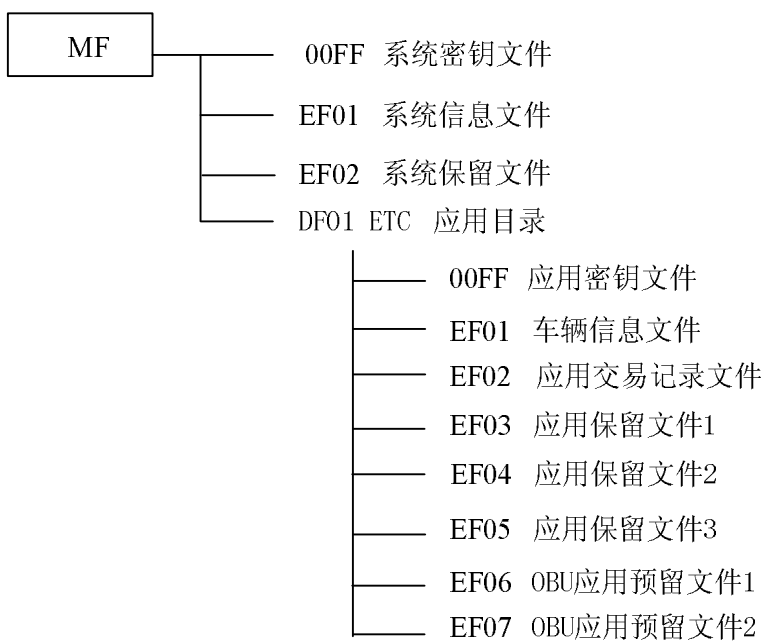
3. OBE-SAM 的主要功能

OBE-SAM 的主要功能如下:

- | 数据安全存储功能;
- | 数据安全读取功能;
- | 硬件 DES 协处理器;
- | TDES 加解密计算功能;
- | TDES MAC 计算功能;
- | 文件访问控制功能;
- | 拆卸判定标志位安全设定功能;
- | 电源电压: 1.8V—3.6V 能正常工作;
- | 外部工作时钟频率不低于 5MHz
- | 操作速度: 最低 57600bps, 各家厂商根据自身情况自由选购。

4. OBE-SAM 文件结构

4.1. 文件结构图



5. 文件详细说明

5.1. 系统信息文件

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	服务提供商编码
9	cn	1	协约类型
10	cn	1	合同版本
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

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		

5.2. MF 下保留文件

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

5.3. ETC 应用车辆信息文件

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
13 – 14	an	2	车牌颜色
15	cn	1	车型
16	cn	1	车辆用户类型
17– 20	cn	4	车辆尺寸 (长[2 字节] X 宽[1 字节] X 高[1 字节])
21	cn	1	车轮数
22	cn	1	车轴数
23 – 24	cn	2	轴距
25 – 27	cn	3	车辆载重/座位数
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

5.4. ETC 应用交易记录文件

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 X 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 (参见公路联网收费技术要求)
7–8	b	2	收费站编码 (参见公路联网收费技术要求)
9	b	1	收费车道编码 (参见公路联网收费技术要求)
10	b	1	卡类型标志 (1 储值卡 2 记帐卡 3 公务卡 4 ...) (参见公路联网收费技术要求)
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

5.5. 应用保留文件 1

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

5.6. 应用保留文件 2

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 – 512	an	512	预留

5.7. 应用保留文件 3

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			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

5.8. OBU 应用预留文件 1

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

5.9. OBU 应用预留文件 2

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

6. 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	10	00	16	0
DAMK_DF01	DF01 应用维护密钥	01	11	00	16	0
RK1_DF01	DF01 应用认证密钥	01	12	00	16	0
RK2_DF01	DF01 应用加密密钥	01	13	00	16	0
RK2_DF01	DF01 应用加密密钥	01	13	01	16	0
RK2_DF01	DF01 应用加密密钥	01	13	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。

7. 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
应用维护密钥	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	
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 1：所有密钥的装载和修改必须使用密文+MAC 的方式。

8. ESAM 复位信息的约定

ESAM 复位信息中历史字节的约定如下（共 15 字节）：

名称	类型	长度（字节）	说明
交通部标识	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 ITS 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	唯一性（在卡商内部）

9. OBE_SAM 应用命令集

9.1. DECREASE COUNTER 命令

9.1.1. 定义和范围

将拆卸次数减 1

9.1.2. 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'

9.1.3. 命令报文数据域

每次固定减 1，命令报文数据域不存在。

9.1.4. 相应报文数据域

返回剩余次数。

9.1.5. 相应报文状态码

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

9.2. GET CHALLENGE 命令

9.2.1. 定义和范围

GET CHALLENGE 命令请求一个永远全过程的随机数。

除非掉电、选择了其他应用后又发出了一个 GET CHALLENGE 命令，该随机数将一直有效。

9.2.2. 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'

9.2.3. 命令报文数据域

命令报文数据域不存在。

9.2.4. 响应报文数据域

响应报文数据域包括随机数，长度为 4 字节或 8 字节。

9.2.5. 响应报文状态码

ESAM 回送的响应信息中可能出现的状态码有：

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

9.3. GET RESPONSE 命令

9.3.1. 定义和范围

当 APDU 不能用现有协议传输时，GET RESPONSE 命令提供了一种从 ESAM 向接口设备传送 APDU（或 APDU 的一部分）的传输方法。

9.3.2. 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

9.3.3. 命令报文数据域

命令报文数据域不存在。

9.3.4. 响应报文数据域

响应报文数据域的长度由 Le 的值决定。

如果 Le 的值为零，在附加数据有效时，ESAM 必须回送状态码‘6CXX’，否则回送状态码‘6F00’。

9.3.5. 响应报文状态码

ESAM 回送的响应信息中可能出现的状态码有：

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

9.4. READ DATA 命令

9.4.1. 定义和范围

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。

9.4.2. 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

9.4.3. 命令报文数据域

命令报文长度为‘09’，读取车辆信息文件时，ESAM 将先通过随机数和期望读取的明文数据计算鉴别码。然后以下面格式组织数据并加密：

鉴别码 + 期望读取的数据明文

9.4.4. 响应报文数据域

命令执行后，ESAM 会先计算鉴别码，然后将鉴别码+读取数据，并以密文形式返回加密读取结果。

鉴别码的计算方法：

- 将文件数据进行 CRC 计算（多项式 $X^{16}+X^{12}+X^5+1$ ，起始 FFFFH），产生两字节 CRC0 和 CRC1。
- 将送入的随机数(8 bytes) 最低两字节分别更换为 CRC1, CRC0，形成 8 字节临时数据。
- 使用计算密钥对 8 字节数据进行加密计算：

$$\text{mac} = \text{TDES}(\text{KEYmac}, \text{CRC0} || \text{CRC1} || \text{rand (高 6 字节)})$$

加密计算方法：

- 用 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。

- b) 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。
- c) 如果最后（或唯一）的数据块的长度是 8 字节的话，转到 d)；如果不足 8 字节，则在其后加入 16 进制数 ‘80’，如果达到 8 字节长度，则转到 d)；否则在其后加入 16 进制数 ‘00’ 直到长度达到 8 字节。
- d) 使用计算密钥对每一个数据块进行 3des 加密。
- e) 计算结束后，所有加密后的数据块依照原顺序连接在一起。

9.4.5. 响应报文状态码

ESAM 回送的响应信息中可能出现的状态码有：

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
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

9.5. READ BINARY 命令

9.5.1. 定义和范围

READ BINARY 命令用于读出二进制文件的内容（或部分内容）。

9.5.2. 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								

9.5.3. 命令报文数据域

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。

9.5.4. 响应报文数据域

当 Le 的值为零时，只要文件的最大长度在 256（短长度）或 65536（扩展长度）之内，则其全部字节将被读出。

9.5.5. 响应报文状态码

ESAM 回送的响应信息中可能出现的状态码有：

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

9.6. READ RECORD 命令

9.6.1. 定义和范围

READ RECORD 命令读记录文件中的内容。

9.6.2. 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								

9.6.3. 命令报文数据域

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。

9.6.4. 响应报文数据域

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。

9.6.5. 响应报文状态码

ESAM 回送的响应信息中可能出现的状态码有：

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	回送的数据可能有错
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

9.7. SELECT FILE 命令

9.7.1. 定义和范围

SELECT FILE 命令通过文件标识或应用名选择 ESAM 中的 MF、DDF、ADF 或 EF 文件。成功执行该命令设定 MF、DDF 或 ADF 的路径。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。从 ESAM 返回的应答报文包含回送 FCI。FCI 数据从数据分组中获得。

9.7.2. 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= ‘01’ ~ ‘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）

9.7.3. 命令报文数据域

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。

9.7.4. 响应报文数据域

响应报文数据域中的数据应包括所选择的 MF、DDF、ADF 的 FCI。

下表定义了成功选择 MF 后回送的 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
	‘9FOC’	FCI 文件内容	0

下表定义了成功选择 DDF 后回送的 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
	‘9FOC’	FCI 文件内容	0

下表定义了成功选择 ADF 后回送的 FCI：

标签	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名	M
	‘A5’	FCI 数据专用模板	M
	‘9FOC’	FCI 文件内容	0

9.7.5. 响应报文状态码

ESAM 回送的响应信息中可能出现的状态码有：

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

9.8. UPDATE BINARY 命令

9.8.1. 定义和范围

UPDATE BINARY 命令用于更新二进制文件中的数据。

9.8.2. 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								

9.8.3. 命令报文数据域

命令报文数据域包括更新原有数据的数据域。

9.8.4. 响应报文数据域

响应报文数据域不存在。

9.8.5. 响应报文状态码

ESAM 回送的响应信息中可能出现的状态码有：

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

9.9. UPDATE RECORD 命令

9.9.1. 定义和范围

UPDATE RECORD 命令用于更新记录文件中的数据。

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。

9.9.2. 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								
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								

9.9.3. 命令报文数据域

命令报文数据域由更新原有记录的新记录组成。

9.9.4. 响应报文数据域

响应报文数据域不存在。

9.9.5. 响应报文状态码

ESAM 回送的响应信息中可能出现的状态码有：

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

9.10. UPDATE KEY 命令

9.10.1. 定义和范围

UPDATE KEY 命令用于更新一个已经存在的密钥。（用于装载正式密钥）

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

在密钥装载前必须用 GET CHANLLEGE 命令从 ESAM 取一个 4 字节的随机数。

9.10.2. 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 ‘1C’
DATA	密文密钥信息 MAC
Le	不存在

9.10.3. 命令报文数据域

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 14h；装载 16 字节的双长度密钥时，数据长度为 1Ch。

9.10.4. 响应报文数据域

响应报数据域不存在。

9.10.5. 响应报文状态码

响应信息中可能返回的状态码有：

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