

高速公路区域联网不停车收费示范工程暂行技术要求 第 15 部分

联网电子收费

OBE_SAM 安全模块测试规范

2008 年 8 月

目 录

1.概述	1
2.依据/参考的规范和文档	1
3.范围	1
4.卡片物理特性测试	1
4.1 复位信息	1
4.1.1 复位应答的数据位宽度	1
4.1.2 复位应答字符长度	1
4.1.3 复位应答字符帧长度	1
4.1.4 复位完成时间	1
4.1.5 $T_b=400/f$ 时卡片冷复位	1
4.1.6 $T_e=400/f$ 时卡片热复位	1
4.1.7 卡片响应 R_{st} 时间(冷复位)	1
4.1.8 卡片响应 R_{st} 时间(热复位)	2
4.2 PPS 相关	2
4.2.1 PPS 错误格式测试	2
4.2.2 PPS 格式测试	2
4.2.3 PPS 响应反向间隔	2
4.2.4 PPS 响应同向间隔	2
4.3 时钟停止相关（该项测试为可选的）	2
4.3.1 ATR 后时钟停止	2
4.3.2 指令后时钟停止	2
4.3.3 命令头之间时钟停止	3
4.3.4 INS 时钟停止	3
4.3.5 数据之间时钟停止	3
4.3.6 数据之间时钟停止	3
4.4 卡片自身发送性能	3
4.4.1 指令应答的数据位宽度	3
4.4.2 指令应答的字符长度	3
4.4.3 指令应答的字符帧长度	3
4.4.4 指令应答的反向间隔	4
4.4.5 数据重发	4
4.4.6 纠错信号出现的时间	4
4.4.7 纠错信号持续的时间	4
4.4.8 60 间隔时间（该项测试为条件的）	4
4.5 卡片自身接收性能	4
4.5.1 最小位宽接收	4
4.5.2 最大位宽接收	4
4.5.3 最小字符帧接收	5
4.5.4 最大字符帧接收	5
4.5.5 最小字符反向间隔接收	5

4.5.6	最大字符反向间隔接收.....	5
4.5.7	指令重收.....	5
4.5.8	最小纠错信号接收.....	5
4.5.9	最大纠错信号接收.....	5
4.5.10	复位后最快接受 PPS.....	5
4.5.11	复位后最快接受指令.....	6
4.5.12	指令响应发送后最快接受指令.....	6
4.5.13	PPS 响应发送后最快接受指令.....	6
4.6	电器特性相关.....	6
4.6.1	上拉电阻测试.....	6
4.6.2	频率电压组合测试.....	6
4.6.3	电压占空比组合测试.....	6
4.7	卡片工作速度.....	6
5.	OBE_SAM 文件结构	7
5.1	文件结构图.....	7
5.2	文件结构测试.....	8
5.2.1	系统信息文件.....	8
5.2.2	车辆信息文件.....	8
5.2.3	应用交易记录文件.....	9
6.	基本指令功能	11
6.1	概述.....	11
6.2	ESAM 专有命令.....	11
6.2.1	DECREASE COUNTER.....	11
6.2.2	READ DATA.....	12
6.2.3	UPDATE KEY.....	13
6.3	文件读写命令.....	14
6.3.1	READ BINARY.....	14
6.3.2	UPDATE BINARY.....	15
6.3.3	READ RECORD.....	16
6.3.4	UPDATE RECORD.....	17
6.4	文件选择相关命令.....	18
6.4.1	SELECT FILE.....	18
6.4.2	GET RESPONSE.....	19
6.5	随机数测试.....	19
6.5.1	GET CHALLENGE.....	19
7.	ESAM 应用流程测试.....	21
7.1	概述.....	21
7.2	双向认证流程.....	22
7.2.1	测试目的.....	22
7.2.2	测试方法.....	22
7.3	数据更新流程.....	22
7.3.1	测试目的.....	22

7.3.2 测试方法	23
7.4 密钥更新流程	23
7.4.1 测试目的	23
7.4.2 测试方法	23
8.卡片兼容性	24
8.1.1 测试目的	24
8.1.2 测试方法	24
9.EEPROM 的速度和性能	24
9.1 概述	24
9.2EEPROM 的读写速度	24
9.3 EEPROM 的稳定性	25
9.4 卡片性能	25
9.4.1 关键指令执行时间	25

1.概述

本文档基于规范《电子收费 OBE-SAM 安全模块技术要求》，对于 OBE_SAM 安全模块所必需遵守的数据安全存储功能，数据安全读取功能，算法和电气性能进行全方面的测试。

2.依据/参考的规范和文档

- 1) 《电子收费 IC 卡技术要求和数据格式》
- 2) 《电子收费 OBE-SAM 安全模块技术要求》
- 3) 《ETC 应用安全》
- 4) 《电子收费系统 OBE—RSE 交易流程规范》

3.范围

本文档规定了基于电子收费 OBE-SAM 安全模块技术所必需遵守的卡片功能方面的要求，主要包括以下几个方面：

- 1) 卡片的物理特性
- 2) 卡片的文件结构
- 3) 规范规定的基本指令功能
- 4) 规范规定的应用流程功能
- 5) 卡片兼容性
- 6) EEPROM 的速度和性能

4. 卡片物理特性测试

4.1 复位信息

4.1.1 复位应答的数据位宽度

- 1) 测试目的：校验卡片复位信息“0”，“1”的位宽在规范范围内。
- 2) 测试要求：0.85etu – 1.15etu

4.1.2 复位应答字符长度

- 1) 测试目的：校验卡片复位信息字符长度在规范范围内。
- 2) 测试要求：9.85etu – 10.15etu

4.1.3 复位应答字符帧长度

- 1) 测试目的：校验卡片复位信息字符帧长度在规范范围内。
- 2) 测试要求：12.5etu-6500etu

4.1.4 复位完成时间

- 1) 测试目的：校验卡片复位完成时间规范范围内。
- 2) 测试要求：<16000etu

4.1.5 $T_b=400/f$ 时卡片冷复位

- 1) 测试目的：校验时钟加于 CLK 后，保持 RST 信号 L 状态 400 周期(tb)内，卡片能够冷复位成功。
- 2) 测试要求：复位成功。

4.1.6 $T_e=400/f$ 时卡片热复位

- 1) 测试目的：校验终端设置 RST 为状态 L400 时钟周期，卡片能够热复位成功。
- 2) 测试要求：复位成功。

4.1.7 卡片响应 Rst 时间(冷复位)

- 1) 测试目的：校验卡片冷复位时“3B”到复位线复位信号上升沿的时间间隔在规范范围内。
- 2) 测试要求：2000/f – 30000/f.

4.1.8 卡片响应 Rst 时间(热复位)

- 1) 测试目的：校验卡片热复位时“3B”到复位线复位信号上升沿的时间间隔在规范范围内。
- 2) 测试要求：2000/f – 30000/f.

4.2 PPS相关

4.2.1 PPS 错误格式测试

- 1) 测试目的：卡片在接收到校验字符错误的 PPS 请求能够正确处理。
- 2) 测试要求：卡片返回校验字符正确的 PPS 响应或长时间没有返回。

4.2.2 PPS 格式测试

- 1) 测试目的：卡片在接收到含有 PPS2, PPS3 的 PPS 请求能够正确处理。
- 2) 测试要求：卡片返回正确的 PPS 响应（与请求保持一致）。

4.2.3 PPS 响应反向间隔

- 1) 测试目的：验证卡片返回 PPS 响应第一个字节（FF）的起始位下降沿与终端发送的最后一个字符起始位下降沿的间隔在规范范围之内。
- 2) 测试要求：18etu – 6500etu.

4.2.4 PPS 响应同向间隔

- 1) 测试目的：验证卡片返回 PPS 响应第一个字节（FF）的起始位下降沿与第二个字符起始位下降沿的间隔在规范范围之内。（连续两个字符间隔）
- 2) 测试要求：12.5etu – 15etu.

4.3 时钟停止相关（该项测试为可选的）

4.3.1 ATR 后时钟停止

- 1) 测试目的：终端在收完复位信息后启动时钟停止，卡片能够正确处理终端启动时钟后发送的指令。
- 2) 测试要求：卡片正确响应终端唤醒时钟后发送指令，并保证时钟停止前后状态一致。

4.3.2 指令后时钟停止

- 1) 测试目的：终端在收完卡片返回第一条指令响应后启动时钟停止，卡片能够正确处理终端启动时钟后发送的指令。

- 2) 测试要求：卡片正确响应终端唤醒时钟后发送指令，并保证时钟停止前后状态一致。

4.3.3 命令头之间时钟停止

- 1) 测试目的：终端在发送命令头部分字节后启动时钟停止，然后启动时钟并发送剩余命令头部分。卡片应该能够正确处理该命令。
- 2) 测试要求：卡片完整接受整个命令头，并正确响应命令。

4.3.4 INS 时钟停止

- 1) 测试目的：终端在收完卡片返回 ins 响应后启动时钟停止，然后启动时钟并发送数据域部分。卡片应该能够正确处理该命令。
- 2) 测试要求：卡片完整接受数据域，并正确响应命令。

4.3.5 数据之间时钟停止

- 1) 测试目的：终端在发送数据部分字节后启动时钟停止，然后启动时钟并发送剩余数据部分。卡片应该能够正确处理该命令。
- 2) 测试要求：卡片完整接受数据域，并正确响应命令。

4.3.6 数据之间时钟停止

- 1) 测试目的：终端在发送数据部分字节后启动时钟停止，然后启动时钟并发送剩余数据部分。卡片应该能够正确处理该命令。
- 2) 测试要求：卡片完整接受数据域，并正确响应命令。

注释：以上各项（1.3.2 – 1.3.6）在不同波特率下都应该测试。

4.4 卡片自身发送性能

4.4.1 指令应答的数据位宽度

- 1) 测试目的：校验卡片指令应答信息“0”，“1”的位宽在规范范围内。
- 2) 测试要求：0.85etu – 1.15etu

4.4.2 指令应答的字符长度

- 1) 测试目的：校验卡片指令应答信息字符长度在规范范围内。
- 2) 测试要求：9.85etu – 10.15etu

4.4.3 指令应答的字符帧长度

- 1) 测试目的：校验卡片指令应答信息字符帧长度在规范范围内。

- 2) 测试要求: $12.5\text{etu}-15*\text{Di etu}$ 。

4.4.4 指令应答的反向间隔

- 1) 测试目的: 校验卡片指令应答第一个字符的起始位与终端发送最后一个字符的起始位间隔在规范范围内 (只包括 3s 指令 INS, 无效指令 SW1, 取随机数指令 INS 的反向间隔)。
- 2) 测试要求: $18\text{etu}-500*\text{Di etu}$ (pps 下: $18\text{etu}-500*\text{Di etu}$)

4.4.5 数据重发

- 1) 测试目的: 校验卡片正确重发 (1-4 次), 并且错误字符和正确字符间隔在规范范围之内 (包括 INS, DATA, SW)。
- 2) 测试要求: 卡片正确重发 (1-4 次), 间隔: $13.00\text{etu} - 16.00\text{etu}$

4.4.6 纠错信号出现的时间

- 1) 测试目的: 校验卡片发送纠错信号出现时间在规范范围之内。
- 2) 测试要求: $10.3\text{etu} - 10.7\text{etu}$

4.4.7 纠错信号持续的时间

- 1) 测试目的: 校验卡片发送纠错信号持续时间在规范范围之内。
- 2) 测试要求: $1.0\text{etu} - 2.0\text{etu}$

4.4.8 60 间隔时间 (该项测试为条件的)

- 1) 测试目的:
如果卡片在命令执行中发送 “60”, 校验卡片发送 “60” 间隔在规范范围之内。
- 2) 测试要求: $(3200\text{etu} - 6500) * \text{Di etu}$

注释: 以上各项 (1.4.1 – 1.4.9) 在不同波特率下都应该测试。

4.5 卡片自身接收性能

4.5.1 最小位宽接收

- 1) 测试目的: 校验卡片正确接受一个字符为 9.8etu 的指令。
- 2) 测试要求: 卡片正确响应指令

4.5.2 最大位宽接收

- 1) 测试目的: 校验卡片正确接受一个字符为 10.2etu 的指令。
- 2) 测试要求: 卡片正确响应指令

4.5.3 最小字符帧接收

- 1) 测试目的：校验卡片正确接受字符帧间隔 11.8etu 的指令。
- 2) 测试要求：卡片正确响应指令

4.5.4 最大字符帧接收

- 1) 测试目的：校验卡片正确接受字符帧间隔 $9600 \cdot \text{Di etu}$ 的指令。
- 2) 测试要求：卡片正确响应指令

4.5.5 最小字符反向间隔接收

- 1) 测试目的：校验卡片正确接受反向间隔为 11.8etu 的指令。
- 2) 测试要求：卡片正确响应指令。

4.5.6 最大字符反向间隔接收

- 1) 测试目的：校验卡片正确接受反向间隔为 $9600 \cdot \text{Di etu}$ 的指令。
- 2) 测试要求：卡片正确响应指令。

4.5.7 指令重收

- 1) 测试目的：校验卡片正确接受终端重发的指令（1-4 次）。
- 2) 测试要求：卡片正确响应指令。

4.5.8 最小纠错信号接收

- 1) 测试目的：校验卡片正确接受终端发送纠错信号（起始时间： 10.3etu ，持续时间 1.0etu ）。
- 2) 测试要求：卡片正确接受纠错信号，并重发数据。

4.5.9 最大纠错信号接收

- 1) 测试目的：校验卡片正确接受终端发送纠错信号（起始时间： 10.7etu ，持续时间 2.0etu ）。
- 2) 测试要求：卡片正确接受纠错信号，并重发数据。

4.5.10 复位后最快接受 PPS

- 1) 测试目的：终端在接收完复位信息最后一个字节起始位下降沿，延迟 11.8etu 发送 PPS 请求，卡片能够正确响应。
- 2) 测试要求：卡片正确接受 PPS 请求，并发送正确 PPS 响应。

4.5.11 复位后最快接受指令

- 1) 测试目的：终端在接收完复位信息最后一个字节起始位下降沿，延迟 11.8 μ s 发送指令，卡片能够正确响应。
- 2) 测试要求：卡片正确接受指令，并发送正确指令响应。

4.5.12 指令响应发送后最快接受指令

- 1) 测试目的：终端在接收完卡片指令响应最后一个字节起始位下降沿，延迟 11.8 μ s 发送指令，卡片能够正确响应。
- 2) 测试要求：卡片正确接受指令，并发送正确指令响应。

4.5.13 PPS 响应发送后最快接受指令

- 1) 测试目的：终端在接收完卡片 PPS 响应最后一个字节起始位下降沿，延迟 11.8 μ s 发送指令，卡片能够正确响应。
- 2) 测试要求：卡片正确接受指令，并发送正确指令响应。

注释：以上各项（1.5.1 – 1.5.9, 1.5.12）在不同波特率下都应该测试。

4.6 电器特性相关

4.6.1 上拉电阻测试

- 1) 测试目的：终端不提供额外的上拉电阻（I/O 线）。卡片能够正常使用。
- 2) 测试要求：卡片正确复位和响应指令。

4.6.2 频率电压组合测试

- 1) 测试目的：在不同的电压和频率下（VCC: 1.0V – 5.2V, F: 1M-5M）。卡片能够正常使用。
- 2) 测试要求：卡片正确复位和响应指令。

4.6.3 电压占空比组合测试

- 1) 测试目的：在不同的电压和占空比下（VCC: 1.0V – 5.2V, D: 40%-60%）。卡片能够正常使用。
- 2) 测试要求：卡片正确复位和响应指令。

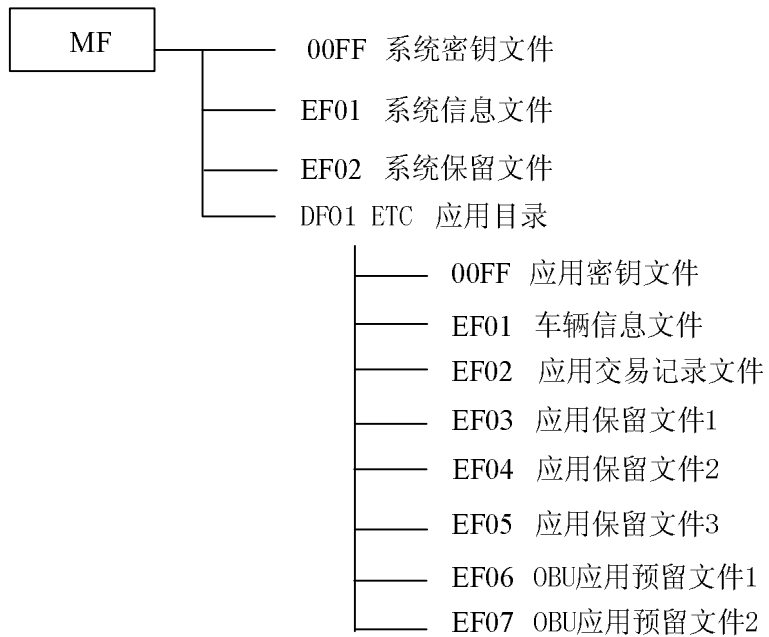
注释：以上各项（1.6.2 – 1.6.3）在不同波特率下都应该测试。

4.7 卡片工作速度

- 1) 测试目的：卡片速度在最低 57600BPS 可以正常工作。
- 2) 测试要求：终端波特率 57600，测试卡片的正确复位和执行所有命令。

5. OBE_SAM 文件结构

5.1 文件结构图



5.2 文件结构测试

对于规范中文件内容为保留的，对此类文件没有进行测试。

5.2.1 系统信息文件

5.2.1.1 测试目的

MF 下的 EF01 文件是系统信息文件，文件权限是读自由，写需要使用明文+MAC 方式.检查文件的读写权限，并检查修改后文件内容的正确性。

5.2.1.2 测试方法

测试初始条件：卡片已经个人化

测试步骤：

- 1) 选择该文件应该返回 9000
- 2) 执行 READ BINARY 命令读该文件应该可以成功，检查返回数据应该与写入的数据一致
- 3) 执行 UPDATE BINARY 命令，使用明文方式修改该文件应该返回 6A80，再次读该文件应该和原始数据一致
- 4) 执行 UPDATE BINARY 命令，使用明文+MAC 方式，密钥是 DAMK_DF01，修改该文件应该可以成功.再次读该文件应该是新写入的数据
- 5) 执行 UPDATE BINARY 命令，使用密文+MAC 方式修改该文件应该返回 6A80
- 6) 执行 UPDATE BINARY 命令，使用明文+MAC 方式修改该文件，密钥不正确，应该返回 6A88

5.2.2 车辆信息文件

5.2.2.1 测试目的

DF01 应用下的 EF01 文件是车辆信息文件，文件权限是读密文，写需要使用明文+MAC 方式.检查文件的读写权限，并检查修改后文件内容的正确性。

5.2.2.2 测试方法

测试初始条件：卡片已经个人化

测试步骤：

- 1) 选择应用后，选择该文件返回 9000。
- 2) 执行 READ BINARY 命令，使用明文方式读该文件应该返回 6982
- 3) 执行 READ BINARY 命令，使用明文+MAC 方式读该文件应该返回 6982
- 4) 执行 READ BINARY 命令，使用密文方式，密钥是 RK2_DF01，读该文件应该可以成功.检查返回文件内容的正确性
- 5) 执行 UPDATE BINARY 命令，使用明文方式修改该文件应该返回 6A80，再次读该文件应该和原始数据一致
- 6) 执行 UPDATE BINARY 命令，使用明文+MAC 方式，密钥是 DAMK_DF01，修改该文件应该可以成功.再次读该文件应该是新写入的数据
- 7) 执行 UPDATE BINARY 命令，使用密文+MAC 方式修改该文件应该返回 6A80
- 8) 执行 UPDATE BINARY 命令，使用明文+MAC 方式修改该文件，密钥不正确，应该返回 6A88

5.2.3 应用交易记录文件

5.2.3.1 测试目的

DF01 应用下的 EF02 文件是应用交易记录文件，文件类型是：循环定长记录文件。文件权限是读写自由。当车辆进入收费站缴费后，卡片就会记录这次交易的内容。一次写一条记录，最多可以记录 50 条记录，当记录超过 50 条，则会自动覆盖最早写入的那条记录。该文件应该是卡片自动填写，外部不可以修改该文件。

5.2.3.2 测试方法

测试初始条件：卡片个人化

测试步骤：

- 9) 选择应用后，选择该文件应该返回 9000
- 10) 卡片没有缴费记录，读该文件应该返回 6A83
- 11) 卡片没有记录，写该文件应该返回 6A83
- 12) 卡片交易应用记录的正确性

I 交易日志记录是循环记录文件，最近的交易包含于记录 1，次近的包

含于记录 2，依次类推，多次交易后检查交易日志文件的正确性

I 卡片交易日志有 N 条记录，读出 N+1 条记录应该返回 6A83

13) 执行 UPDATE RECORD 命令修改任一记录都应该返回 6982

6.基本指令功能

6.1 概述

本文档规定了基于电子收费 OBE-SAM 安全模块中规定了一些智能卡必须遵守的基本功能要求，本章主要就是逐个指令描述应该实现的功能和要求。本章描述的指令包括：

- 1) ESAM 专有命令
 - I DECREASE COUNTER
 - I READ DATA
 - I UPDATE KEY
- 2) 文件读写命令
 - I READ BINARY
 - I UPDATE BINARY
 - I READ RECORD
 - I UPDATE RECORD
- 3) 文件选择相关指令
 - I SELECT FILE
 - I GET RESPONSE
- 4) 认证相关命令
 - I GET CHALLENGE

6.2 ESAM专有命令

6.2.1 DECREASE COUNTER

6.2.1.1 测试目的

DECREASE COUNTER 命令用于记录拆卸次数，该命令执行成功后则拆卸次数每次固定减 1。

6.2.1.2 测试方法

测试步骤：

- 1) 复位后，执行该命令应该可以返回 6A82

- 2) 复位后，选择应用，执行该命令应该可以成功，检查返回的剩余次数的正确性，此时应该等于 $X-2$ (X 是拆卸的最大次数，在 EF01 系统信息文件中第 27 字节定义该拆卸次数)
- 3) 连续多次执行该命令应该可以成功，检查返回的剩余次数的正确
- 4) 执行其他命令后再执行该命令应该可以成功，检查返回的剩余次数的正确性
- 5) 拆卸次数等于 00 后，再执行该命令应该返回 6985
- 6) 修改 EF01 系统信息文件的拆卸次数为 FF (0F 为最大拆卸次数，低 4 字节有效)，执行一次该命令应该返回 0E

6.2.2 READ DATA

6.2.2.1 测试目的

READ DATA 命令用于读出应用车辆信息文件中的数据，读写的数据为密文。并计算返回数据密文的正确性。

6.2.2.2 测试方法

测试初始条件：卡片已经写入车辆信息文件的内容

测试步骤：

- 1) 执行该命令 P1P2=000 的正确性测试响应报文应该是鉴别码+读取数据密文，计算返回数据的正确性。

鉴别码的计算方法：

- a) 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。
- b) 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。
- c) 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：

- a) 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。
- 2) 执行该命令命令域中的期望读取的信息数据明文长度小于车辆信息文件的大小，应该可以读出文件内容
- 3) 执行该命令命令域中的期望读取的信息数据明文长度大于车辆信息文件的大小，应该返回 6CXX（XX 是文件的最大长度）
- 4) 分别使用密钥版本是 01， 02 的执行 READ DATA 命令，验证返回数据密文的正确性
- 5) 执行该命令密钥版本不正确，应该返回 9403
- 6) 执行该命令 P1P2 按照偏移量读车辆信息文件应该可以成功
- 7) 如果 P1P2 或 P2 指定的偏移量超出文件范围，应该返回 6B00

6.2.3 UPDATE KEY

6.2.3.1 测试目的

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。

6.2.3.2 测试方法

测试初始条件：卡片个人化中已经存在密钥

测试步骤：

- 1) UPTDATE KEY 命令的正确性
 - I 执行该命令 P2=00 更新主控密钥，密钥长度是 8 字节或者 16 字节都应该可以成功
 - I 执行该命令 P2=FF 更新其他密钥，密钥长度是 8 字节或者 16 字节都应该可以成功
- 2) 执行该命令密钥信息是明文应该返回 6A80
- 3) 执行该命令 MAC 不正确，应该返回 6988
- 4) 执行该命令密钥长度不正确，应该返回 6700
- 5) 执行该命令更新不存在的密钥，应该返回 6A88
- 6) 没有执行取随机数应该返回 6984

6.3 文件读写命令

6.3.1 READ BINARY

6.3.1.1 测试目的

READ BINARY 命令用于读出二进制文件的内容（或部分内容）。

6.3.1.2 测试方法

测试步骤：

7) 正确性测试：

- I 明文方式读的二进制文件，可以使用明文方式读出，也可以使用明文+MAC 方式读出，此方式读出时，通过取响应返回的报文中不包含 MAC
- I 明文+MAC 方式读的二进制文件，使用明文+MAC 方式读出时，通过取响应返回的报文中最后四个字节为 MAC

8) 明文方式读的文件，采用明文方式读出，最多将读出偏移量后的所有字节或偏移量后的 255 个字节：

- I 如果偏移量后的字节超过 255 个，最多返回 255 个字节
- I 如果偏移量后的字节小于 255 个，最多返回偏移量后的所有字节

9) 明文方式读的文件，采用明文+MAC 方式读出，最多将读出偏移量后的所有字节或偏移量后的 255 个字节：

- I 如果偏移量后的字节超过 255 个，最多返回 255 个字节
- I 如果偏移量后的字节小于 255 个，最多返回偏移量后的所有字节

10) 明文+MAC 方式读的文件，采用明文+MAC 方式读出，最多将读出偏移量后的所有字节或偏移量后的读通信区长度(RLEN)-4 个字节

- I 如果偏移量后的字节超过 RLEN-4 个，最多返回 RLEN-4 个字节
- I 如果偏移量后的字节小于 RLEN-4 个，最多返回偏移量后的所有字节

- I 命令返回 61XX，如果取响应的长度小于 XX，应该返回 6CXX

11) 读不是二进制文件类型的文件时应该返回 6981

12) 读 ID 不存在的文件应该返回 6A82

13) 没有当前文件时，指定读当前文件应该返回 6A82

- 14) 如果 P1P2 或 P2 指定的偏移量超出文件范围，应该返回 6B00
- 15) 如果 P1P2 或 P2 指定的偏移量加上要读的长度超过实际文件地址空间，应该返回 6CXX
- 16) 在没有取随机数的情况下，使用带 MAC 方式执行此命令时（CLA=04）时，应该返回 6984
- 17) 使用校验方式读文件时，如果命令报文中的 MAC 不正确应该返回 6988

6.3.2 UPDATE BINARY

6.3.1.1 测试目的

UPDATE BINARY 命令用于更新二进制文件中的数据.

6.3.1.2 测试方法

测试步骤:

- 1) 正确性测试：分别使用明文方式，密文方式，校验方式，校验加密方式写文件，应该可以成功
- 2) 测试文件更新的影响，执行该命令后，文件内容应该只改变了从偏移量开始的数据明文长度的内容：
 - I 明文方式写的二进制文件
 - I 密文方式写的二进制文件
 - I 校验方式写的二进制文件
 - I 校验加密方式写的二进制文件
- 3) 写不是二进制文件类型的文件时应该返回 6981
- 4) 写 ID 不存在的文件应该返回 6A82
- 5) 没有当前文件时，指定写当前文件应该返回 6A82
- 6) 如果 P1P2 或 P2 指定的偏移量超出文件范围，应该返回 6B00
- 7) 如果 P1P2 或 P2 指定的偏移量加上要写的长度超过实际文件地址空间，应该返回 6700
- 8) 在没有取随机数的情况下，使用带 MAC 方式执行此命令时（CLA=04），应该返回 6984
- 9) 使用加密方式执行修改二进制，密文信息不正确应该返回 6988

- 10) 使用校验方式执行修改二进制，校验码不正确应该返回 6982
- 11) 使用校验加密方式执行修改二进制，密文信息不正确应该返回 6988

6.3.3 READ RECORD

6.3.3.1 测试目的

READ RECORD 命令读记录文件中的内容

6.3.3.2 测试方法

测试步骤:

- 1) 正确性测试:
 - I 明文方式读的记录文件，可以使用明文方式读出，也可以使用明文+MAC 方式读出，此方式读出时，通过取响应返回的报文中不包含 MAC
 - I 明文+MAC 方式读的记录文件，使用明文+MAC 方式读出时，通过取响应返回的报文中最后四个字节为 MAC
- 2) 明文方式读的文件，采用明文方式读出，最多将读出偏移量后的所有字节或偏移量后的 255 个字节:
 - I 如果偏移量后的字节超过 255 个，最多返回 255 个字节
 - I 如果偏移量后的字节小于 255 个，最多返回偏移量后的所有字节
- 3) 明文方式读的文件，采用明文+MAC 方式读出，最多将读出偏移量后的所有字节或偏移量后的 255 个字节:
 - I 如果偏移量后的字节超过 255 个，最多返回 255 个字节
 - I 如果偏移量后的字节小于 255 个，最多返回偏移量后的所有字节
- 4) 明文+MAC 方式读的文件，采用明文+MAC 方式读出，最多将读出偏移量后的所有字节或偏移量后的读通信区长度(RLEN)-4 个字节
 - I 如果偏移量后的字节超过 RLEN-4 个，最多返回 RLEN-4 个字节
 - I 如果偏移量后的字节小于 RLEN-4 个，最多返回偏移量后的所有字节
- 5) 读不是记录文件类型的文件时应该返回 6981

- 6) 读 ID 不存在的文件应该返回 6A82
- 7) 没有当前文件时，指定读当前文件应该返回 6A82
- 8) 如果 P1P2 或 P2 指定的偏移量超出文件范围，应该返回 6B00
- 9) 如果 P1P2 或 P2 指定的偏移量加上要读的长度超过实际文件地址空间，应该返回 6CXX
- 10) 在没有取随机数的情况下，使用带 MAC 方式执行此命令时（CLA=04）时，应该返回 6984
- 11) 使用校验方式读文件时，如果命令报文中的 MAC 不正确应该返回 6988

6.3.4 UPDATE RECORD

6.3.4.1 测试目的

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。

6.3.4.2 测试方法

测试步骤：

- 1) 正确性测试，执行该命令更新定长记录文件和循环记录文件，使用：分别使用明文方式，密文方式，校验方式，校验加密方式写文件，应该可以成功
- 2) 对于 P2 的测试
 - l p2=xxxxx000b (P1 指定的记录标识符的第一个记录)
 - l p2=xxxxx001b (P1 指定的记录标识符的最后一个记录)
 - l p2=xxxxx010b (P1 指定的记录标识符的下一个记录)
 - l p2=xxxxx011b (P1 指定的记录标识符的上一个记录)
 - l p2=xxxxx100b (P1 指定的记录)
- 3) 记录空间已满，写定长记录文件，应该返回 6A83
- 4) 文件 ID 不存在时，写记录应该返回 6A82
- 5) 没有当前文件时，指定写当前文件应该返回 6A82
- 6) 文件类型不匹配时写记录文件，应该返回 6981
- 7) 定长记录文件写入的记录长度不等于文件的记录长度时，应该返回 6700

- 8) 变长记录文件要写入的记录长度>现有的记录长度时，应该返回 6700
- 9) 变长记录文件要写入的记录长度<现有的记录长度时，应该返回 9000
- 10) 在没有取随机数的情况下，使用带 MAC 方式执行此命令时（CLA=04），应该返回 6984

6.4 文件选择相关命令

6.4.1 SELECT FILE

6.4.1.1 测试目的

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。

6.4.1.2 测试方法

测试步骤：

- 1) 选择 MF/DDF/ADF/AEF 通过取响应返回响应报文采用 TLV 格式，对于 MF/DDF/ADF 通过文件名和标识得到的响应报文相同：

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
	'9F0C' FCI 文件内容	O

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
	'9F0C' FCI 文件内容	O

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
	'9F0C'	FCI 文件内容	O

6.4.2 GET RESPONSE

6.4.2.1 测试目的

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。

6.4.2.2 测试方法

测试步骤：

- 1) 可以执行取响应的几种情况：
 - I 选择文件(应用没有锁定时返回 61XX, 应用临时锁定时返回 6A81), 取出文件的 FCI
 - I 读二进制文件时指定 P3=00, 返回 6CXX, 告知可以继续取出 XX 长度的文件内容
 - I 执行部分取响应后, 仍有响应未取的情况下
- 2) 其它情况下, 执行取响应指令都应该返回 6F00
- 3) 返回 61XX 后, 如果取响应的长度超出 XX 或=00, 卡片返回 6CXX, 仍可以继续取响应

6.5 随机数测试

6.5.1 GET CHALLENGE

6.5.1.1 测试目的

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。

6.5.1.2 测试方法

测试步骤：

- 1) 正确性测试：可以取 4 个字节或 8 个字节的随机数
- 2) 执行随机数长度不是 4 或 8 字节应该返回 6700

- 3) 分析随机数的使用特性：取随机数后，选择其他应用后，执行了其他指令后再去执行欲执行的指令，应该返回 6984：
- I 取随机数，执行选择应用后，使用该随机数执行明文+MAC 写二进制文件，应该返回 6984
 - I 取随机数，执行选择应用后，使用该随机数执行明文+MAC 写记录文件，应该返回 6984
 - I 取随机数，执行选择应用后，使用该随机数执行明文+MAC 读二进制文件，应该返回 6984
 - I 取随机数，执行选择应用后，使用该随机数执行明文+MAC 读记录文件，应该返回 6984
 - I 选择应用，取随机数，执行选择应用后，使用该随机数执行 UPDATE KEY 命令，应该返回 6984
- 4) 随机数在各项性能符合要求（按照 FIPS1402）：
- I 取 2500 个随机数到文件中，用测试程序中提供的工具进行分析

7.ESAM 应用流程测试

7.1 概述

本章主要是对 ETC 的应用安全，与 PSAM 交互的应用流程进行测试：

- 1) 双向认证流程
- 2) 数据更新流程
- 3) 密钥更新流程

7.2 双向认证流程

7.2.1 测试目的

ESAM 与 PSAM 卡双向认证获得访问数据的许可

7.2.2 测试方法

OBU	RSU
ESAM 复位	PSAM 复位
	发送 8 字节随机数给 OBU
ESAM 选择文件 DF01 '00A4000002DF01'	
ESAM 加密读取车辆信息文件，获取鉴别码+车牌号+车型密文 '00B400000A' + Random_RSU + '0D0000' 返回密文信息 EncryData 给 RSU。	
ESAM 读取系统信息文件中的区域分散代码（分散因子）+合同号（分散因子）共 16 字节 '00B0820A10' 并将分散因子 FensanYinzi 发送给 RSU	
	RSU 获得 1、鉴别码 + 车牌号 + 车型密文 EncryData 2、分散因子 FensanYinzi
	PSAM 选择文件 DF01 00A4000002DF01
	RSU 分散密钥 801A590310+FensanYinzi RSU 解密数据 '80FA800018'+ EncryData +'18'
	RSU 获得鉴别码+车牌号+车型明文 RSU 用 Random_RSU+车牌号+车型， 计算鉴别码。 '80FA080015'+ Random_RSU +CarNo+CarStyle+'08' 返回 MACRSU RSU 比对计算的结果和解密的结果。如果一致则验证通过。

7.3 数据更新流程

7.3.1 测试目的

更新卡片中的关键数据一起传送一组鉴别码，RSE 验证数据的合法性后将数

据更新。

7.3.2 测试方法

OBU	RSU
ESAM 复位	
ESAM 选择文件 DF01 '00A4000002DF01'	
ESAM 读取系统信息文件中的区域分散代码（分散因子）+合同号（分散因子）共 16 字节 '00B0820A10' 并将分散因子 FensanYinzi 发送给 RSU	
ESAM 取 4 字节随机数 '0084000004' 返回 Random，并发送给 RSU	
	RSU 获得分散因子 FensanYinzi
	PSAM 选择文件 DF01 00A4000002DF01
	RSU 分散密钥 '801A460210'+FensanYinZi RSU 计算 MAC '80FA050038'+Random+'00000000'+ 04D6820027'+AABBCCDDEEFF668 801021122334455667788112233445 5667788032007080820080808'+800 00000000000000'+08' 返回 Dataout MAC=left（Dataout，8）取左 4 字节， 并将 MAC 发送给 OBU
OBU 明文+MAC 更新数据 '04D6820027'+AABBCCDDEEFF668801021122 334455667788112233445566778803200708082 0080808'+MAC	

7.4 密钥更新流程

7.4.1 测试目的

为保证数据传输的安全性，将卡片中的数据采用密文方式进行更新

7.4.2 测试方法

OBU	母卡
ESAM 复位	
ESAM 选择文件 DF01	

'00A4000002DF01'	
ESAM 读取系统信息文件中的区域分散代码（分散因子）+合同号（分散因子）共 16 字节 '00B0820A10' 并将分散因子 FensanYinzi 发送给 RSU	
ESAM 取 4 字节随机数 '0084000004' 返回 Random，并发送给 RSU	
	母卡获得分散因子 FensanYinzi
	母卡分散密钥 '801A1E0110'+FenSanYinZi
	母卡导出密钥 'BFE6800310'+Random+'00000000'+ '84D401FF1C'+ '010300' 返回密钥密文+MAC 值 KeyData
ESAM 更新密钥 '84D401FF1C'+KeyData	

8. 卡片兼容性

8.1.1 测试目的

在不同的终端/读卡器上，各种规范规定和自定义的指令都可以正常执行。

8.1.2 测试方法

使用卡片在不同的终端上执行建立文件系统、个人化、测试卡片基本指令和交易流程等内容。

9. EEPROM 的速度和性能

9.1 概述

EEPROM 的性能是影响卡片性能的关键因素，EEPROM 的读写速度影响卡片的工作效率，EEPROM 的稳定性影响卡片的使用寿命。

9.2 EEPROM 的读写速度

测试方法：

- 1) 建立文件系统（建立一个大小为 4K 的二进制文件、读写权限为自由，

方式为明文)

- 2) 将文件内容填充为 55
- 3) 记录将文件内容全部填为 AA 的时间 (一次写入 60H 个字节)
- 4) 记录将文件内容全部读出的时间 (一次读出 60H 个字节)

9.3 EEPROM的稳定性

测试方法:

- 1) 建立文件系统 (建立一个大小为所有 EE 空间的二进制文件、读写权限为自由, 方式为明文)
 - I 测试随机读写
 - I 设置 EE 的内容为文件偏移量的低位字节
 - I 从文件空间范围内随机选择一个地址, 在 60H 长度范围内随机选择一个长度, 写入内容仍为偏移量的低位字节 (如果偏移地址+长度大于文件空间, 则改变长度)
 - I 读出写入内容以及偏移量前 255 个字节的内容以及偏移量+写长度后的 255 个字节的内容 (如果前后不足 255 个字节, 则取全部)
 - I 重复上述两步 100,000 次, 应该不会出错
- 2) 测试固定位置的读写
 - I 选择一个地址: 如文件偏移量开始初
 - I 第一次全部写入 30H 个 55aa, 读出比较
 - I 第一次全部写入 30H 个 aa55, 读出比较
 - I 重复上述两步 100,000 次, 应该不会出错

重新选择一个地址: 如文件偏移量为文件长度的 1/3 处、文件偏移量为文件长度的 2/3 处, 重复上述四步

9.4 卡片性能

9.4.1 关键指令执行时间

- 1) 测试目的: 校验卡片关键指令处理时间在需求范围之内。
- 2) 测试要求: 满足需求规定