

高速公路区域联网不停车收费示范工程暂行技术要求 第 16 部分

联网电子收费

PSAM 卡测试规范

2008 年 8 月

目 录

1.概述.....	3
2.依据/参考的规范和文档.....	3
3.范围.....	3
4.PSAM 卡片文件结构.....	4
4.1 文件结构.....	4
4.2 文件结构测试.....	4
4.2.1 DIR 文件	4
5.基本指令功能.....	5
5.1 概述.....	5
5.2 文件读写相关命令.....	5
5.2.1 READ BINARY	5
5.2.2 UPDATE BINARY	7
5.3 应用安全相关命令.....	7
5.3.1 APPLICATION BLOCK	7
5.3.2 APPLICATION UNBLOCK	8
5.3.3 CARD LOCK	9
5.4 文件选择相关指令.....	9
5.4.1 SELECT FILE	9
5.4.2 GET REPOSE	10
5.5 密钥管理.....	10
5.5.1 WRITE KEY	10
5.6 PSAM 卡专有命令.....	11
5.6.1 DELIVERY KEY	11
5.6.2 CIPHER DATA	11
5.6.3 INIT SAM FOR PURCHASE (计算 MAC1)	12
5.6.4 CREDIT SAM FOR PURCHASE (校验 MAC2)	12
5.7 随机数测试.....	13
5.7.1 GET CHALLENGE	13
6.防拔功能测试.....	14
6.1 概述.....	14
6.2 写二进制防拔流程.....	15
6.3 应用临时锁定防拔流程.....	16
6.4 应用解锁防拔流程.....	17
6.5 卡片锁定/应用永久锁定防拔流程.....	18
6.6 WRITE KEY 防拔流程.....	19
6.7 PURCHASE (校验 MAC2) 防拔流程.....	20

1.概述

本测试规范基于《示范性工程 PSAM 卡应用命令接口》，对于 PSAM 卡片支持的应用命令进行测试。

2.依据/参考的规范和文档

- 1) 《收费公路联网收费技术要求》
- 2) 《联网电子收费 PSAM 卡应用指南》
- 3) 《JR/T 0025-2005 中国金融集成电路（IC）卡规范》

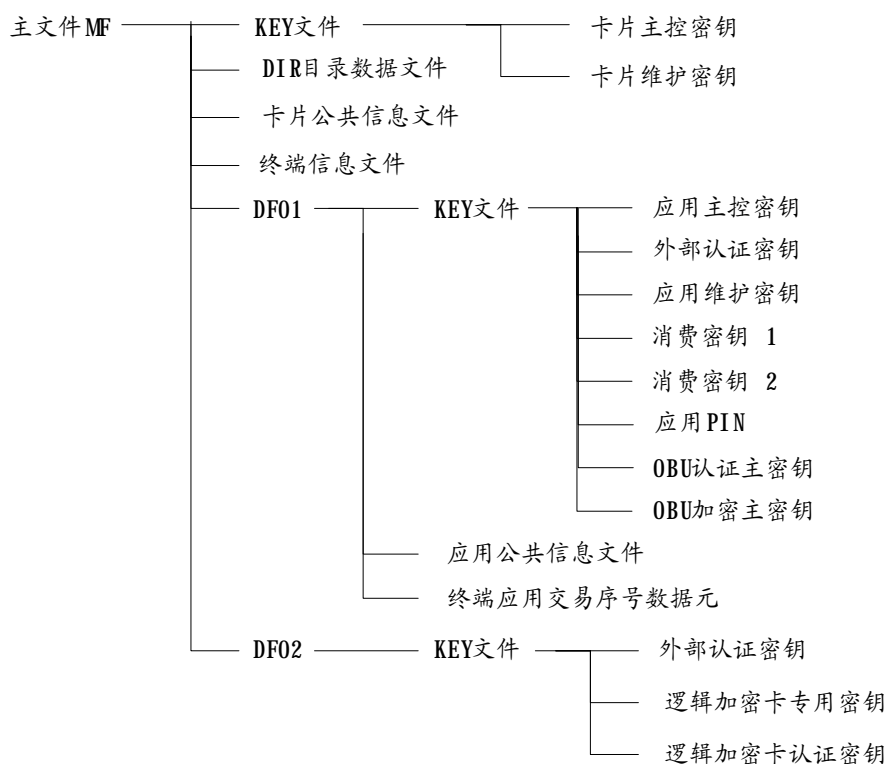
3.范围

本文档规定了基于电子收费 PSAM 卡片支持的应用命令和文件结构进行测试，主要包括以下几个方面：

- 1) 卡片的文件结构；
- 2) 规范规定的基本指令功能；
- 3) 卡片防拔测试。

4.PSAM 卡片文件结构

4.1 文件结构



4.2 文件结构测试

对于检测指南中规定的文件进行测试，检查每个文件内容与写入的一致。

4.2.1 DIR 文件

4.2.1.1 测试目的

DIR 文件是 MF 下的目录文件，读写权限为自由，检查返回数据内容的正确性。

4.2.1.2 测试方法

测试步骤：

1) 选择 MF，读 DIR 文件应该返回

记录一：70 13 61 11 4F 09 A0 00 00 00 03 86 98 07 01 50 04 50 42 4F 43

记录二：70 13 61 11 4F 09 A0 00 00 00 03 86 98 07 02 50 04 50 42 4F 43

读第三条记录，应该返回 6A83

2) LE=00，应该返回 6C15

5.基本指令功能

5.1 概述

本文档规定了基于电子收费 PSAM 卡片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) 文件读写相关的指令：
 - I READ BINARY
 - I UPDATE BINARY
- 2) 应用安全相关指令：
 - I APPLICATION BLOCK
 - I APPLICATION UNBLOCK
 - I CARD LOCK
 - I RELOAD PIN
 - I GET CHALLENGE
- 3) 文件选择相关指令：
 - I SELECT FILE
 - I GET REPOSE
- 4) 密钥管理：
 - I CHANGE KEY
 - I WRITE KEY
- 5) PSAM 卡专有命令：
 - I CIPHER DATA
 - I DELIVERY KEY
 - I INIT SAM FOR PURCHASE
 - I CREDIT SAM FOR PURCHASE

5.2 文件读写相关命令

5.2.1 READ BINARY

5.2.1.1 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）。

5.2.1.2 测试方法

测试步骤:

- 1) 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。
- 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;
 - I 命令返回 61XX, 如果取响应的长度小于 XX, 应该返回 6CXX。
- 5) 读不是二进制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。

5.2.2 UPDATE BINARY

5.2.2.1 测试目的

UPDATE BINARY 命令用于更新二进制文件中的数据。

5.2.2.2 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，MAC 不正确应该返回 6988。

5.3 应用安全相关命令

5.3.1 APPLICATION BLOCK

5.3.1.1 测试目的

应用锁定命令执行成功后，锁定当前有效的应用。应用临时锁定后选择应用应该返回 6A81，可以通过 GET RESPONSE 命令获取 FCI 信息，应用被永久锁定应该返回 9303。

5.3.1.2 测试方法

测试步骤：

- 1) 复位，选择应用，执行应用临时锁定，应该可以执行成功，再次选择该应用应该

返回 6A81。

- 2) 继续执行应用永久锁定，同样应该可以执行成功，再次选择该应用应该返回 9303。
- 3) 应用已被临时锁定时，再次执行应用临时锁定命令应该返回 9000。
- 4) 应用临时锁定后，执行选择该应用的指令，虽然返回 6A81，但仍可以紧接着通过取响应指令得到正常选择该应用的 FCI，取出全部响应的返回码为 9000。
- 5) 测试命令报文中的 MAC 不对，导致应用永久锁定的情况：
 - I 第一次执行该命令的 MAC 不对，应该返回 6988；
 - I 第二次执行该命令的 MAC 不对，应该返回 6988；
 - I 第三次执行该命令的 MAC 不对，应该返回 9303，且该应用被永久锁定。
- 6) 执行此命令前应该先从卡取随机数，否则返回 6984。
- 7) 应用临时锁定后，在该应用下只能执行取随机数、应用解锁、应用临时锁定、应用永久锁定、卡片锁定这四条命令，执行其他命令均返回 6985。
- 8) 应用永久锁定后，执行选择该应用的指令，应该返回 9303 且无法通过取响应指令得到该应用的 FCI，执行取响应返回 9303。
- 9) 应用永久锁定后，在该应用下只能执行取随机数、卡片锁定这两条命令，执行其他命令均返回 9303。
- 10) 被临时锁定的应用，可以通过应用解锁命令将此应用解锁。
- 11) 被永久锁定的应用，无法通过应用解锁命令将此应用解锁。

5.3.2 APPLICATION UNBLOCK

5.3.2.1 测试目的

APPLICATION UNBLOCK 命令执行成功后，解锁当前锁定的应用。

5.3.2.2 测试方法

测试步骤：

- 1) 应用临时锁定后执行应用解锁，应该返回 9000。
- 2) 应用永久锁定后执行应用解锁，应该返回 9303。
- 3) 应用没有被锁定时，执行此命令，应该返回 6985。
- 4) 执行此命令前必须产生随机数，否则返回 6984。
- 5) 执行应用解锁命令正确后，应该清解锁错误计数器：
 - I 应用临时锁定后，第一次执行该命令的 MAC 不对，应该返回 6988；
 - I 第二次执行该命令的 MAC 不对，应该返回 6988；

- l 第三次执行正确执行该命令，该应用被解锁，再次将应用临时锁定后；
- l 第一次执行该命令的 MAC 不对，应该返回 6988；
- l 第二次执行该命令的 MAC 不对，应该返回 6988；
- l 第三次执行该命令的 MAC 不对，应该返回 9303，且该应用被永久锁定。

5.3.3 CARD LOCK

5.3.3.1 测试目的

CARD BLOCK 命令成功后，应用环境被锁定，执行任何命令都应该返回 6A81。

5.3.3.2 测试方法

测试步骤：

- 1) 卡片锁定后，应该无法执行所有命令，皆返回 6A81。
- 2) 执行此命令前必须先取随机数，否则返回 6984。
- 3) 执行该指令时 MAC 不对，应该返回 6988，错误任意次后仍应该返回 6988。

5.4 文件选择相关指令

5.4.1 SELECT FILE

5.4.1.1 测试目的

SELECT FILE 命令通过文件标识或应用名选择 IC 卡中的 MF、DDF、ADF 或 EF 文件。

5.4.1.2 测试方法

测试步骤：

- 1) 选择 MF/DDF/ADF 通过取响应返回响应报文采用 TLV 格式。

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

- 2) 密钥文件，存折文件应该不能被选择，选择此类文件时应该返回 6A86。
- 3) 应用被临时锁定时，选择应用应该返回 6A81。
- 4) 应用被永久锁定时，选择应用应该返回 9303。

5.4.2 GET RESPONSE

5.4.2.1 测试目的

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

5.4.2.2 测试方法

测试步骤：

- 1) 正确性测试：应用没有锁定，选择 MF 和 ADF，应该返回 61XX，执行 GET RESPONSE 命令取出 FCI 应该可以成功。
- 2) 读二进制时指定 P3=00，返回 6CXX（XX 是实际长度）。
- 3) 执行部分取响应应该返回数据+61XX（XX 是剩余长度）。
- 4) 没有响应，执行取响应命令应该返回 6F00。
- 5) 应用锁定后，选择应用返回 6A81，执行 GET RESPONSE 命令应该取出 FCI。

5.5 密钥管理

5.5.1 WRITE KEY

5.5.1.1 测试目的

WRITE KEY 命令用于向卡片装载或更新密钥。

5.5.1.2 测试方法

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 LC 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。

5.6 PSAM卡专有命令

5.6.1 DELIVERY KEY

5.6.1.1 测试目的

DELIVERY KEY 命令时用于将指定的 KEY 分散至临时密钥寄存器,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。

5.6.1.2 测试方法

测试步骤:

- 1) 该命令在应用没有锁定且已经写入密钥的情况下执行应该返回 9000。
- 2) 主控密钥,维护密钥,消费密钥不支持 DES 初始化,应该返回 6989。
- 3) 执行 DES 初始化时,P1 的高三位与 LC 的长度不匹配时,应该返回 6A80,有以下几种情况:
 - I P1 的高三位为 0,LC 长度为 8;
 - I P1 的高三位为 1,LC 长度为 0 或 10。
- 4) 执行 DELIVERY KEY 如果 LC 不是 8 的倍数,应该返回 6700。
- 5) 执行 DELIVERY KEY 密钥标识符不存在应该返回 9403。
- 6) 应用临时锁定后执行 DELIVERY KEY 应该返回 6985。
- 7) 应用永久锁定后执行 DELIVERY KEY 应该返回 9303。
- 8) 卡片锁定后执行 DELIVERY KEY 应该返回 6A81。

5.6.2 CIPHER DATA

5.6.2.1 测试目的

CIPHER DATA 命令用于对输入数据进行安全计算。

5.6.2.2 测试方法

测试步骤:

- 1) 执行 DELIVERY KEY 命令成功后, 执行该命令应该返回 9000。
 - I P1=05 时计算 MAC 的正确性;
 - I P1=08 时计算 MAC 的正确性。
- 2) P1=08 时执行该命令 LC 的长度大于等于 9 字节都应该返回 9000。
- 3) 执行 CIPHER DATA 前必须成功执行 DELIVERY KEY, 并且两条命令之间不能插入其他命令, 否则返回 6901。
- 4) P1=05 时执行该命令 LC 的长度不是 8 的倍数应该返回 6700。
- 5) P1=05/08 时执行该命令 LC 的长度小于 9 字节应该返回 6700。

5.6.3 INIT SAM FOR PURCHASE (计算 MAC1)

5.6.3.1 测试目的

INIT SAM FOR PURCHASE 命令支持三级消费密钥分散机制, 并产生 MAC1。

5.6.3.2 测试方法

测试步骤:

- 1) 在应用没有锁定的情况下使用密钥版本 01 和 02 的消费密钥进行计算, 应该返回 9000。
- 2) 执行 MAC1 计算命令时, 密钥分散级别与数据不符, 应该返回 6A80。
- 3) 密钥版本不正确应该返回 9403。
- 4) 消费密钥算法标识不正确, 应该返回 6A80。
- 5) 应用被永久锁定后, 执行计算 MAC1 命令, 应该返回 9303。
- 6) 卡片锁定后, 执行计算 MAC1 命令, 应该返回 6A81。

5.6.4 CREDIT SAM FOR PURCHASE (校验 MAC2)

5.6.4.1 测试目的

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。MAC2 校验失败, 计算 MAC2 的 KEY 限制计数器减一, 并回送状态码'63Cx'。当 KEY 限制计数器减为 0 值时, 锁定当前应用, 可通过应用维护密钥解锁锁定应用。CREDIT SAM FOR PURCHASE 命令成功后, SAM 卡将应用中的消费交易序号加 1。

5.6.4.2 测试方法

测试步骤:

- 1) 正确性测试:
 - I 复位, 选择应用;
 - I MAC1 计算;
 - I 校验 MAC2, 同时终端交易序号自动加 1。
- 2) 没有成功执行 INIT SAM FOR PURCHASE, 直接执行 PURCHASE 应该返回 6901。
- 3) 测试校验 MAC2 不正确的返回码变化及密钥的锁定。
 - I 如果是第一次不正确, 应该返回 63C2;
 - I 如果是第二次不正确, 应该返回 63C1;
 - I 如果是第三次不正确, 应该返回 63C0;
 - I 如果不正确的次数达到三次, 不管下一次校验 MAC2 是否成功以及重复多少次, 都应该返回 6985。此时消费密钥所在的应用应该被临时锁定了;
 - I 执行应用解锁命令应该返回 9000。执行校验 MAC2 失败, 应该返回 63c2。
- 4) 如果校验 MAC2 正确, 应该清计数器的错误次数: 先执行校验 MAC2 失败, 在执行校验 MAC2 成功, 下一次再用不正确的 MAC2 进行校验, 应该返回 63CX, 其中 X 为最大错误次数减 1。
- 5) 应用被永久锁定后, 执行计算 MAC2 命令, 应该返回 9303。
- 6) 卡片锁定后, 执行计算 MAC2 命令, 应该返回 6A81。

5.7 随机数测试

5.7.1 GET CHALLENGE

5.7.1.1 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。

5.7.1.2 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。

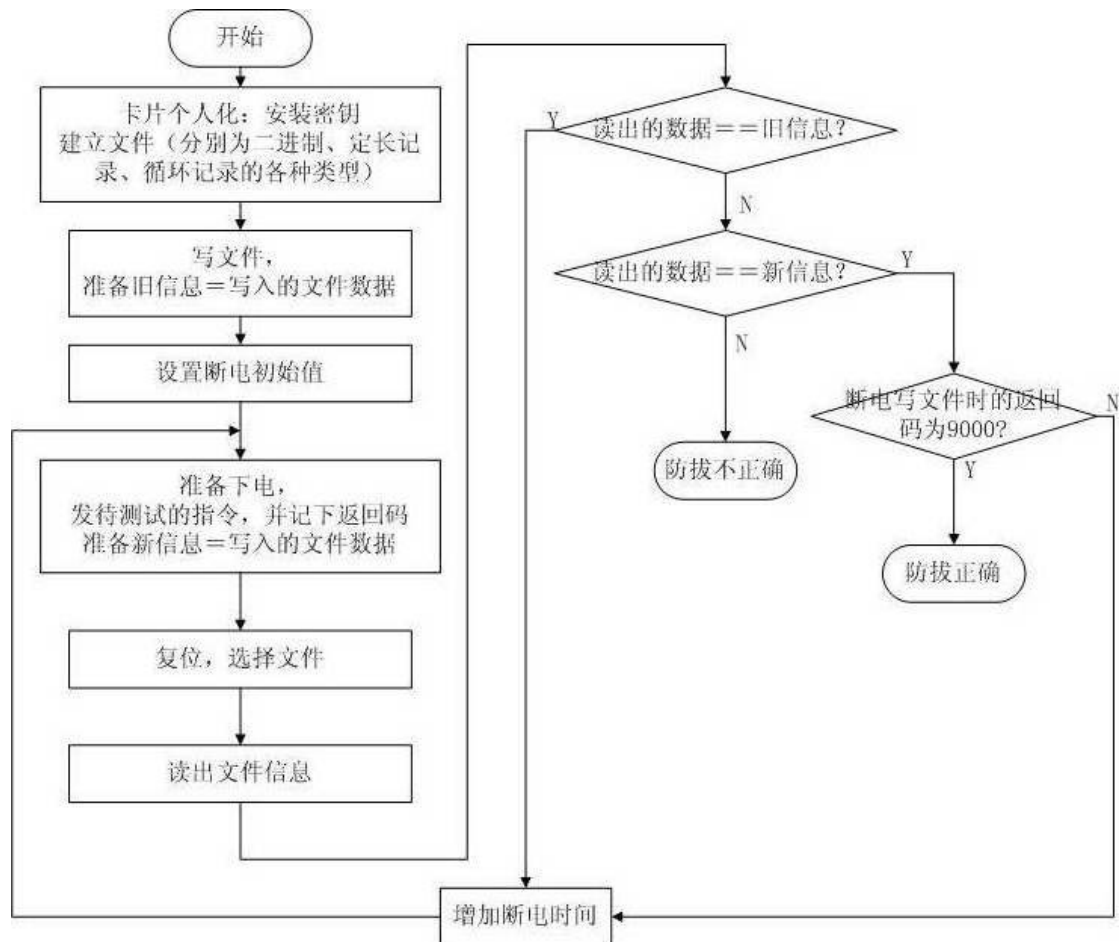
6.防拔功能测试

6.1 概述

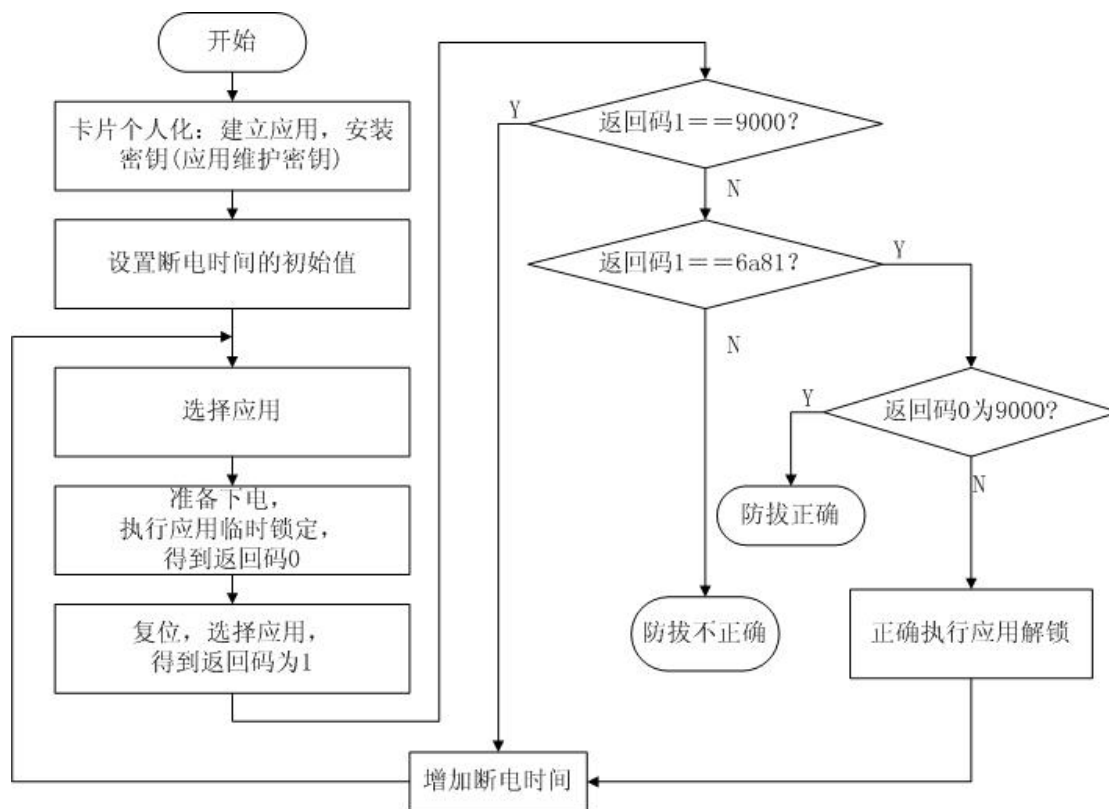
卡片必须在命令处理过程中的任何情况下，甚至在更新 EEPROM 过程中掉电的情况下，保持数据的完整性。因此需要在每次更新数据前对数据进行备份，并且在重新加电后自动地触发恢复机制。一旦卡片确认更新数据完成，备份数据被丢弃。

6.2 写二进制防拔流程

测试步骤：使用明文+MAC 写二进制，每次写入的明文数据长度为 19H。

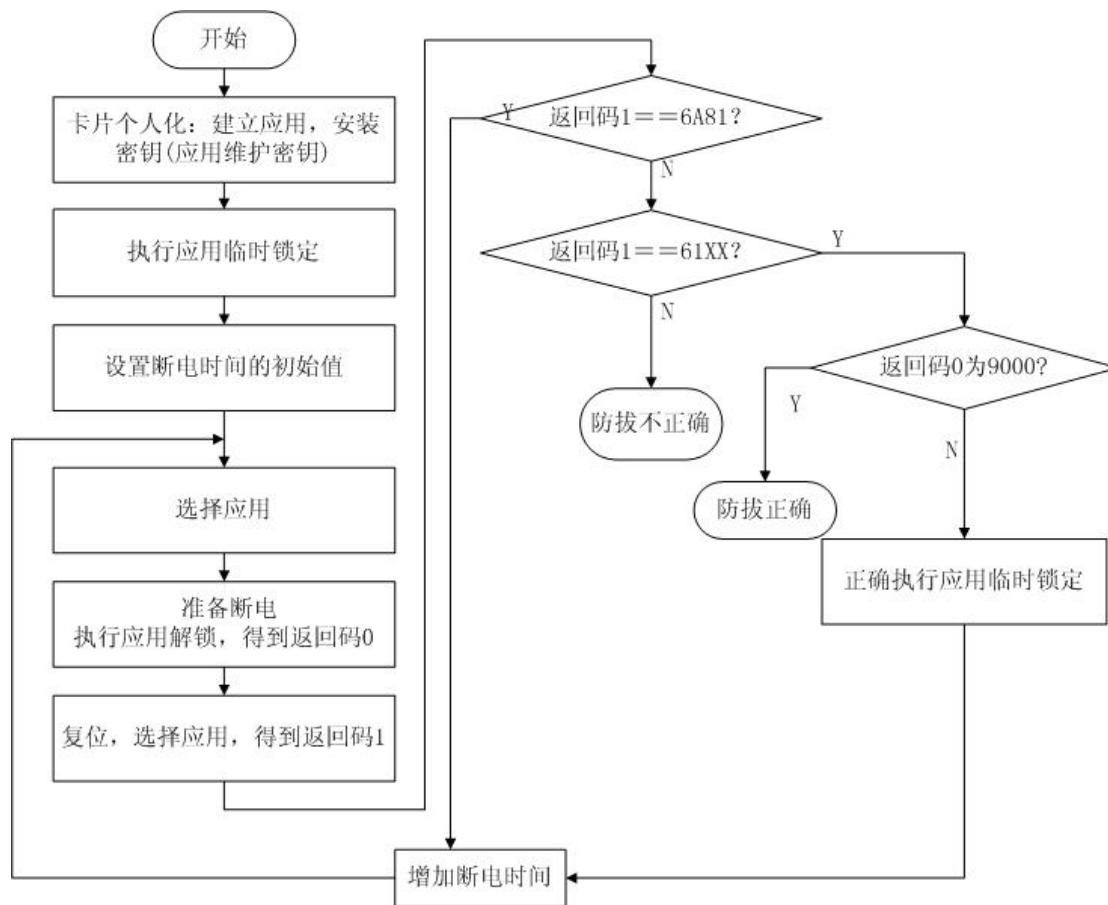


6.3 应用临时锁定防拔流程



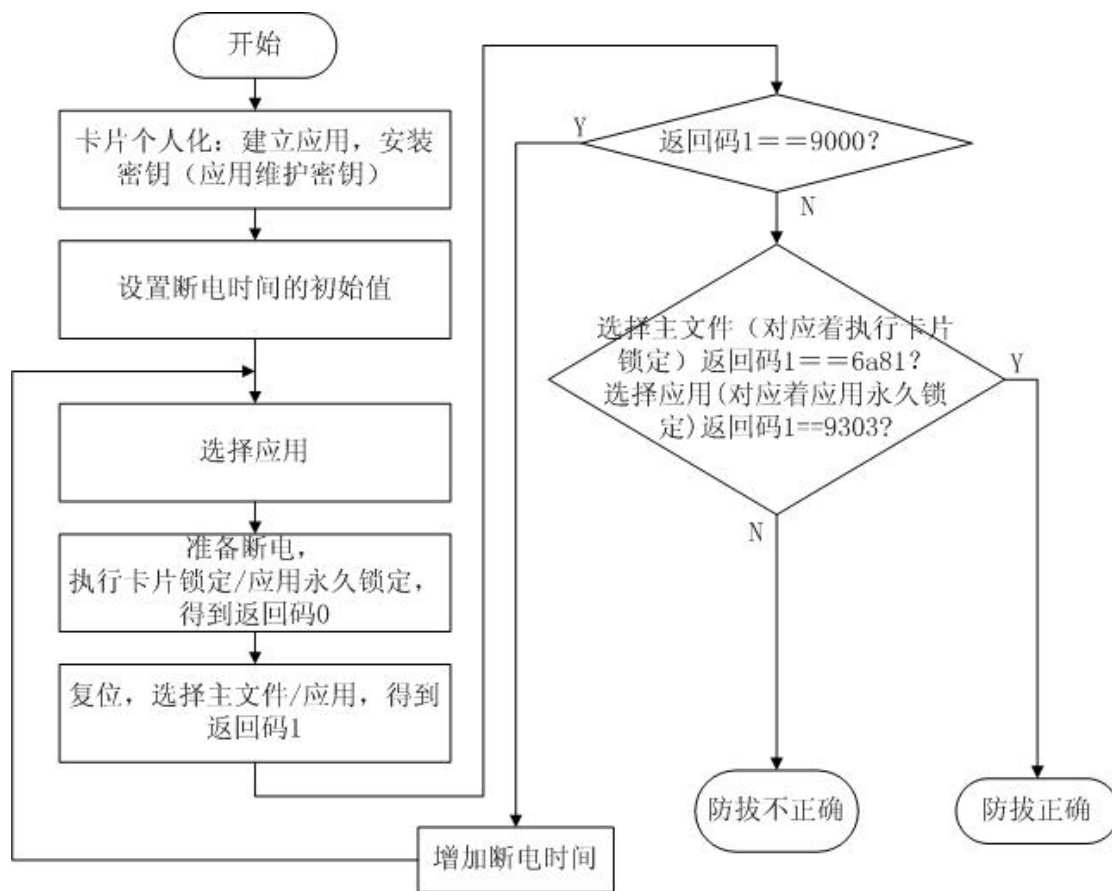
应用临时锁定防拔测试流程图

6.4 应用解锁防拔流程



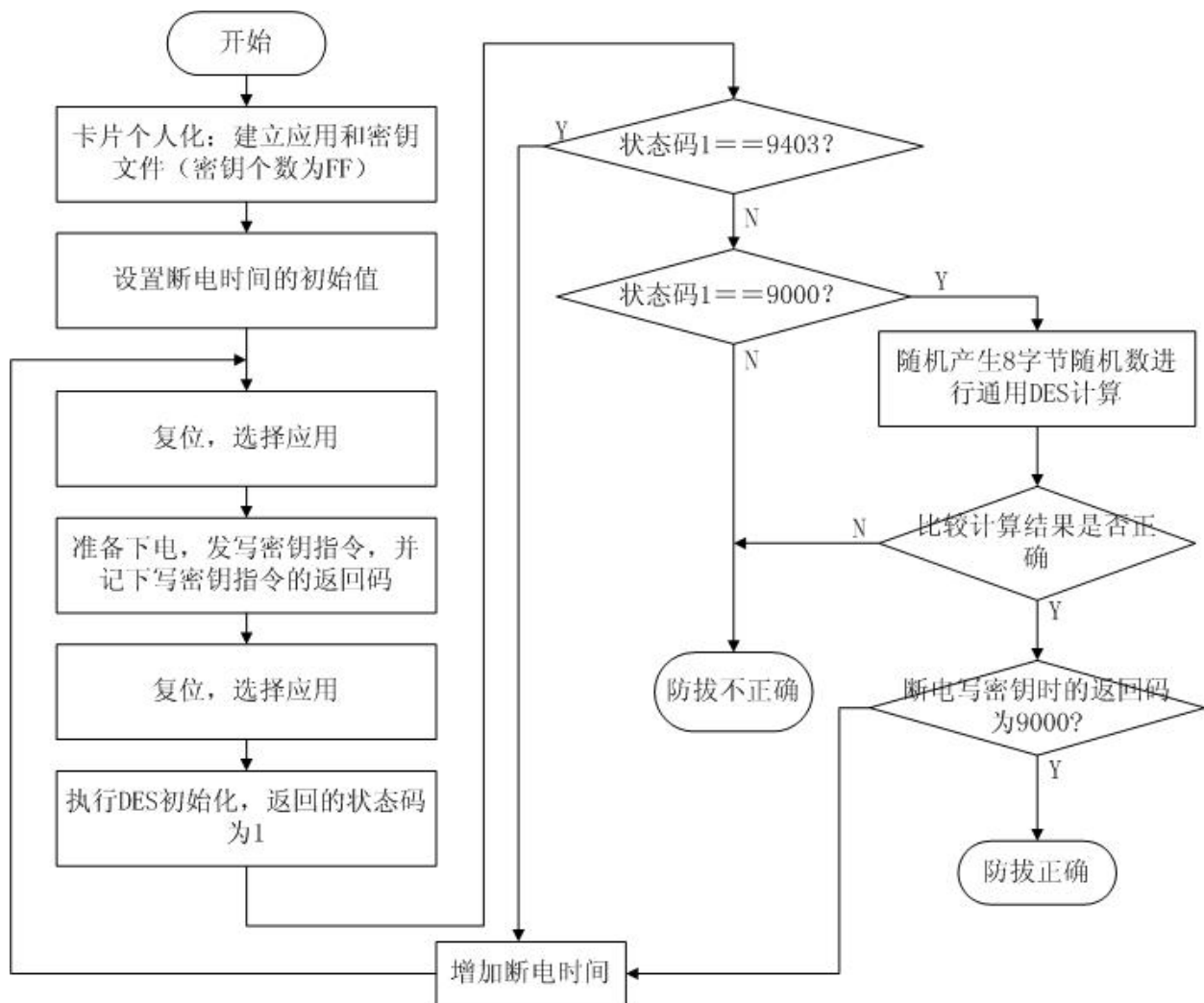
应用解锁交易防拔测试流程图

6.5 卡片锁定/应用永久锁定防拔流程



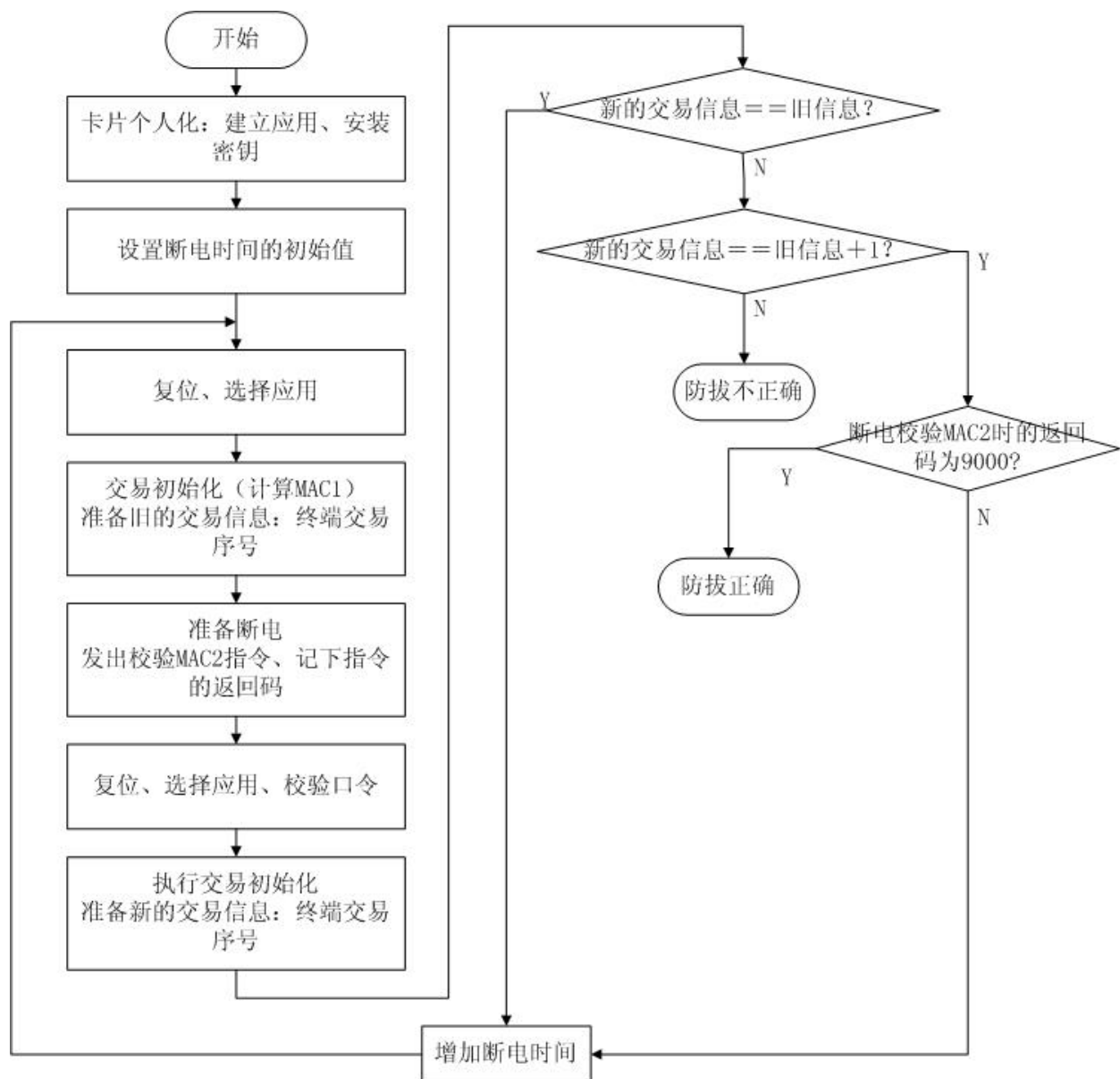
卡锁定、应用永久锁定防拔测试流程图

6.6 WRITE KEY防拔流程



写密钥防拔测试流程图

6.7 PURCHASE（校验MAC2）防拔流程



普通消费校验MAC2防拔测试流程图