
高速公路区域联网不停车收费示范工程暂行技术要求 第 14 部分

联网电子收费 ICC（用户卡） 测试规范

2008 年 8 月

目 录

1	范围.....	1
2	依据/参考的规范和文档	1
3	个人化测试	1
3.1	概述.....	1
3.2	文件测试	1
3.2.1	测试目的:	1
3.2.2	测试步骤:	1
3.3	密钥测试	2
3.3.1	测试目的:	2
3.3.2	测试步骤:	2
4	规范规定的功能测试	3
4.1	基本命令	3
4.1.1	读二进制.....	3
4.1.2	写二进制.....	4
4.1.3	校验 PIN.....	5
4.1.4	修改 PIN.....	6
4.1.5	重装 PIN.....	7
4.1.6	PIN 解锁.....	8
4.1.7	取随机数.....	9
4.1.8	应用锁定.....	10
4.1.9	应用解锁.....	11
4.1.10	卡片锁定.....	11
4.1.11	取响应命令.....	12
4.1.12	选择.....	12
4.2	金融交易命令.....	13
4.2.1	圈存.....	13
4.2.2	圈提.....	14
4.2.3	取现.....	15
4.2.4	消费.....	16
4.2.5	修改透支限额.....	17
4.2.6	读余额.....	17
4.2.7	取交易认证.....	18
4.3	复合消费命令.....	18
4.3.1	复合应用消费.....	19
4.3.2	更新复合应用数据缓存.....	19
5	交易状态机测试.....	20
5.1	测试目的:	20

5.2	测试步骤:	20
6	随机交易测试.....	21
6.1	测试目的:	21
6.2	测试步骤:	21
7	参数测试.....	22
7.1	基本命令	22
7.1.1	读二进制.....	22
7.1.2	写二进制.....	23
7.1.3	校验 PIN.....	23
7.1.4	修改 PIN.....	23
7.1.5	重装 PIN.....	24
7.1.6	PIN 解锁.....	24
7.1.7	取随机数.....	24
7.1.8	应用锁定.....	25
7.1.9	应用解锁.....	25
7.1.10	卡片锁定.....	25
7.1.11	取响应.....	26
7.1.12	选择.....	26
8	防拔插测试.....	26
8.1	概述.....	26
8.2	防拔流程	27
8.2.1	写二进制防拔.....	27
8.2.2	校验 PIN 防拔流程.....	28
8.2.3	修改 PIN/重装 PIN 防拔流程.....	29
8.2.4	解锁 PIN 防拔流程.....	30
8.2.5	应用临时锁定防拔流程.....	31
8.2.6	应用解锁防拔流程.....	32
8.2.7	卡片锁定/应用永久锁定防拔流程.....	33

1 范围

本文档是根据中国金融集成电路 IC 卡规范的电子钱包/存折和扩展应用规范，对规定的卡片基本功能严格按照银行检测中心的检测要求进行测试。

2 依据/参考的规范和文档

- 1) JR/T 0025.4 中国金融集成电路（IC）卡规范 第 1 部分 电子钱包/存折卡片规范
- 2) JR/T 0025.4 中国金融集成电路（IC）卡规范 第 2 部分 电子钱包/存折应用规范
- 3) JR/T 0025.4 中国金融集成电路（IC）卡规范 第 9 部分 电子钱包扩展应用指南
- 4) 银行检测中心 -- 《金融卡测试报告》

3 个人化测试

3.1 概述

该部分重点描述银行卡检测中心要求的个人化文件结构测试。从建立文件的大小、权限，密钥版本、标识及文件的选择响应等方面进行限定。个人化的建立参考附录文档《PBOC2.0 检测指南.doc》。

3.2 文件测试

3.2.1 测试目的：

测试写入文件内容的正确性

3.2.2 测试步骤：

- 1) 选择 MF，读 DIR 文件，应该有两条记录，其值分别为：

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) 读 0015 文件，比较返回的信息与写入的一致。
- 3) 读 0016 文件，比较返回的信息与写入的一致。
- 4) 选择 MF，ADF1，ADF2 后，比较响应 FCI 数据的正确性。
- 5) 使用文件标识符选择 MF、ADF 和 EF，应该返回 6A86
 - I 使用文件标识符选择 MF，应该返回 6A86
 - I 使用文件标识符方式选择 ADF1 和 ADF2，应该返回 6A86
 - I 使用文件标识符方式选择 EF 文件，应该返回 6A86

3.3 密钥测试

3.3.1 测试目的：

测试写入的密钥：PIN，PIN 解锁密钥，PIN 重装密钥，应用维护密钥，圈存，圈提，消费，修改透支限额密钥的版本，标识和值的正确性。

3.3.2 测试步骤：

- 1) 校验 PIN（PIN 值为 1234），应该能够成功
- 2) 将 PIN 锁定，使用 PIN 解锁密钥解锁，并校验原始 PIN，应该能够成功
- 3) 执行 PIN 重装命令装入新的 PIN，PIN 值为 1233；应该能够成功，并校验新装入的 PIN
- 4) 使用维护密钥修改 0015 和 0016 文件，应该能够成功
- 5) 使用密钥索引为 01 和 02 的圈存密钥进行圈存初始化，返回数据中密钥版本号应该为 02，算法标识应该为 00；进行圈存，应该能够成功
- 6) 使用密钥索引为 01 和 02 的圈提密钥进行圈提初始化，返回数据中密钥版本号应该为 05，算法标识应该为 00；进行圈提，应该能够成功
- 7) 使用密钥索引为 01 和 02 的消费密钥进行消费初始化，返回数据中密钥版本号应该为 01，算法标识应该为 00；进行消费，应该能够成功
- 8) 使用密钥索引为 01 和 02 的修改透支限额密钥进行修改透支限额初始化，返回数据中密钥版本号应该为 04，算法标识应该为 00；进行修改透支限额，应该能够成功

4 规范规定的功能测试

该部分根据《中国金融集成电路 IC 卡规范》的要求，对规范中出现的基本功能进行详细测试，按照银行检测中心的检测要求严格限定。

4.1 基本命令

根据规范要求，必须检测的 APDU 命令有：

- 1) READ BINARY
- 2) UPDATE BINARY
- 3) VERIFY
- 4) PIN CHANGE/UNBLOCK
- 5) RELOAD PIN
- 6) GET CHALLENGE
- 7) APPLICATION BLOCK
- 8) APPLICATION UNBLOCK
- 9) CARD BLOCK
- 10) GET RESPONSE
- 11) SELECT

4.1.1 读二进制

4.1.1.1 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）。

4.1.1.2 测试步骤：

- 1) 正确性测试：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
- 2) 如果 P1P2 或 P2 指定的偏移量超过实际文件地址空间，应该返回 6B00

- 3) 执行读二进制命令 LE=00, 应该返回 6CXX (XX 是文件实际长度)
- 4) 读不是二进制文件类型的文件时应该返回 6981
- 5) 读 ID 不存在的文件应该返回 6A82
- 6) 没有当前文件时, 指定读当前文件应该返回 6A82

4.1.2 写二进制

4.1.2.1 测试目的:

UPDATE BINARY 命令用于更新二进制文件中的数据.根据检测要求只能使用 04 方式更新二进制文件。

4.1.2.2 测试步骤:

- 1) 正确性测试: 使用明文+MAC 方式写二进制文件应该返回 9000
- 2) 执行 UPDATE BINARY 使用偏移量方式写文件, 应该返回 9000
- 3) 如果 P1P2 或 P2 指定的偏移量超过文件空间, 应该返回 6B00
- 4) 如果 P1P2 或 P2 指定的偏移量加上要写的长度超过文件空间, 应该返回 6700
- 5) 使用写二进制文件方式写记录文件, 应该返回 6981
- 6) 没有取随机数, 使用明文+MAC 方式写文件, 应该返回 6984
- 7) 明文+MAC 方式写文件时, 如果命令报文中的 MAC 连续三次不对, 应用会被永久锁定
 - 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
- 8) 明文+MAC 方式写文件时, 命令正确运行后, 应该清 MAC 出错的错误计数器:
 - I 第一次执行该命令的 MAC 不对, 应该返回 6988
 - I 第二次正确执行该命令
 - I 再次执行该命令的 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

4.1.3 校验 PIN

4.1.3.1 测试目的:

VERIFY 命令引发 IC 卡将命令报文数据域内的交易 PIN 数据和与该应用相关的参考 PIN 数据进行比较验证

4.1.3.2 测试步骤:

- 1) 正确性测试: 使用写入的 PIN 值 1234 进行校验, 应该返回 9000
- 2) 选择 MF, 使用 1234 值进行校验, 应该返回 9403
- 3) 如果输入的 PIN 值为 0~9 之间的值不正确, 执行该命令应该返回 63CX
- 4) 如果输入的 PIN 值为 A-F 间的值时, 应该返回 63CX
- 5) 如果校验不正确, 返回码的变化及口令锁定:
 - I 第一次校验不正确, 应该返回 63C2
 - I 第二次校验不正确, 应该返回 63C1
 - I 第三次校验不正确, 应该返回 63C0
 - I 此时, 再次执行该命令, 无论 PIN 是否正确, 都应该返回 6983
- 6) 如果校验正确, 应该清 PIN 的错误计数器:
 - I 先错误校验一次, 返回 63C2
 - I 再正确校验一次, 返回 9000
 - I 再错误校验一次, 应该返回 63C2
 - I 再错误校验一次, 应该返回 63C1
 - I 再正确校验一次, 返回 9000
 - I 再错误校验一次, 应该返回 63C2
- 7) 校验正确后, 验证 PIN 标志位已经设置: 复位后选择应用 ADF1, 执行圈存交易返回 6982, 校验正确后, 圈存交易可以执行
- 8) 校验正确后, 验证卡片的状态机为校验 PIN 的后续状态:
- 9) 复位后选择 ADF1, 读钱包余额应该返回 6982, 校验正确后, 再次读钱包余额, 应该能够成功
- 10) 校验不正确后, 验证 PIN 标志位已经被清:
- 11) 复位后选择应用 ADF1, 执行圈存交易返回 6982, 校验正确后, 圈存交易可以执行, 校验不正确后, 执行圈存交易返回 6982

- 12) 校验不正确，验证卡片的状态机清 0:
- 13) 复位后选择 ADF1，校验正确后，再次读钱包余额，应该能够成功，校验不正确后，读钱包余额应该返回 6982

4.1.4 修改 PIN

4.1.4.1 测试目的:

PIN CHANGE/UNBLOCK 命令用于修改 PIN 为新值，且同时改变 PIN 错误计数器的值。

4.1.4.2 测试步骤:

- 1) 正确性测试:
 - I 测试把口令从 1234 变为 123456123456 并校验
 - I 测试把口令从 123456123456 变为 12345612345F 并校验
 - I 测试把口令从 12345612345F 变为 123F 并校验
 - I 测试把口令从 123F 变为 1234 并校验
- 2) 新老口令的数据长度（数据报文域中 FF 字节前后的长度）都应该在 2 到 6 间，否则返回 6A80，有以下几种组合情况:
 - I 老口令长度为 1，新口令长度为 3
 - I 老口令长度为 7，新口令长度为 3
 - I 老口令长度为 3，新口令长度为 1
 - I 老口令长度为 3，新口令长度为 7
 - I 老口令长度为 1，新口令长度为 7
 - I 老口令长度为 7，新口令长度为 1
- 3) 新、老口令必须符合规范，否则返回 6A80，有以下几种组合情况:
 - I 老口令规范，新口令不规范
 - I 老口令不规范，新口令规范
 - I 老口令不规范，新口令不规范
- 4) 老口令和新口令之间应该用 FF 连接，如果没有 FF，返回 6A80
- 5) 如果修改正确，应该清 PIN 的错误次数：先用错误的老口令修改错误一次，再修改成功，下一次再次用不正确的老口令修改时，应该返回 63CX，其中 X 为最大错

误次数减 1

6) 测试修改时老口令不正确的返回码变化，及口令的锁定：

- l 如果是第一次修改但老口令不正确，应该返回 63C2
- l 如果是第二次修改但老口令不正确，应该返回 63C1
- l 如果是第三次修改但老口令不正确，应该返回 63C0
- l 如果不正确次数已达到三次，不管再次修改的老口令是否正确以及修改命令执行多少次，都应该返回 6983

7) 修改正确后，验证 PIN 标志位应该不变：

- l 原来已验证 PIN 的标志位仍为已验证：复位后选择应用，校验口令正确后，圈存交易可以执行，修改口令成功后，圈存交易仍可以执行
- l 没有验证 PIN 的标志位仍为未验证：复位后选择应用，执行圈存交易返回 6982，修改口令成功后，执行圈存交易仍返回 6982。使用新 PIN 校验成功后，再执行圈存交易应该返回 9000

8) 老口令不正确，执行修改指令后，验证 PIN 标志位应该已经被清：

- l 复位后选择应用，校验口令正确后，圈存交易可以执行，使用错误的老口令执行修改口令后，再次执行圈存交易应该返回 6982

4.1.5 重装 PIN

4.1.5.1 测试目的：

RELOAD PIN 命令用于修改 PIN 为新值，且同时改变 PIN 错误计数器的值。

4.1.5.2 测试步骤：

1) 正确性测试：

- l 分别选择应用 ADF1 和应用 ADF2，正确执行 PIN 重装，应该能够成功
- l 在 PIN 没有被锁的情况通过该指令修改 PIN：
 - ü 从 1234 修改为 123456123456，并校验成功
 - ü 再修改为 1234，并校验成功
 - ü 再修改为 12345612345F，并校验成功
 - ü 再修改为 123F，并校验成功
 - ü 再修改为 1234，并校验成功
- l 在 PIN 被锁的情况通过该指令修改 PIN（原口令为 1234）：
 - ü 锁定口令，修改为 123456123456，并校验成功
 - ü 锁定口令，再修改为 1234，并校验成功

- ü 锁定口令，再修改为 12345612345F，并校验成功
 - ü 锁定口令，再修改为 123F，并校验成功
 - ü 锁定口令，再修改为 1234，并校验成功
- 2) 数据报文中的新口令必须符合规范，否则返回 6A80
 - 3) 测试命令报文中的 MAC 不对，将应用永久锁定的情况：
 - 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
 - 4) 此命令正确运行后，应该清重装 PIN 的错误计数器和 PIN 自身的错误计数器：
 - l 复位选择应用，错误的校验 PIN，应该返回 63C2
 - 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 第三次执行正确执行该命令，再次错误的校验 PIN，应该返回 63C2
 - 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

4.1.6 PIN 解锁

4.1.6.1 测试目的：

PIN CHANGE/UNBLOCK 命令用于将锁定的 PIN 进行解锁，同时恢复 PIN 错误计数器。

4.1.6.2 测试步骤：

- 1) 正确性测试：PIN 锁定后，执行 PIN 解锁，应该返回 9000
- 2) PIN 未被锁死的情况下，执行此命令应该返回 6985
- 3) 在没有取随机数的情况下，执行此命令应该返回 6984
- 4) 使用 UNBLOCKPIN 命令，数据长度为 0（DES 计算前第一个为 00），应该返回 6700
- 5) 测试命令报文中的 MAC 不对，将应用永久锁定的情况：
 - 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
- 6) 测试命令报文中的 PIN 明文不对，将应用永久锁定的情况：
 - l 第一次执行该命令的 PIN 明文不对，应该返回 6988
 - l 第二次执行该命令的 PIN 明文不对，应该返回 6988
 - l 第三次执行该命令的 PIN 明文不对，应该返回 9303，且该应用被永久锁定
- 7) 此命令正确运行后，应该清解锁 PIN 的错误计数器和 PIN 自身的错误计数器：
 - l PIN 锁定后，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 PIN 明文不对，应该返回 6988
 - l 第三次执行正确执行该命令
 - l 再次错误的校验 PIN，应该返回 63C2，直至锁死，再次执行解锁命令
 - l 第一次执行该命令的 PIN 明文不对，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 PIN 明文不对，应该返回 9303，且该应用被永久锁定

4.1.7 取随机数

4.1.7.1 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

4.1.7.2 测试步骤：

- 1) 正确性测试：
 - l 选择 MF，执行取 4 字节随机数，应该能够成功
 - l 分别选择 ADF1 和 ADF2，执行取 4 字节随机数，应该能够成功
 - l 随机数在各项性能符合要求（按照 FIPS1402）：
 - ü 位 1 的个数在 9725-10275 之间
 - ü 半字节的值出现 0-F 的随机性在 2.16-46.17 之间
 - ü 1 个数据位 1/0 连续出现的间隔数在 2315-2685 之间
 - ü 2 个数据位 1/0 连续出现的间隔数在 1114-1386 之间
 - ü 3 个数据位 1/0 连续出现的间隔数在 527-723 之间
 - ü 4 个数据位 1/0 连续出现的间隔数在 240-384 之间
 - ü 5 个数据位 1/0 连续出现的间隔数在 103-209 之间
 - ü 26 个数据位 1/0 连续出现的次数为 0
- 测试方法：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。

l 对交易初始化命令返回的随机数进行性能测试

2) 随机数的使用特性测试:

l 一次随机数只能提供给紧接着的下一条命令使用,取了随机数后,后面没有接着执行取执行的指令,执行了其他指令后再去执行欲执行的指令,应该返回 6984:

- ü 取随机数,校验口令,使用该随机数执行明文+MAC 写二进制 0015 文件,应该返回 6984
- ü 选择应用,取随机数,校验口令,使用该随机数执行应用临时锁定,应该返回 6984
- ü 选择应用,取随机数,校验口令,使用该随机数执行应用永久锁定,应该返回 6984
- ü 选择应用,将应用临时锁定,取随机数,校验口令,使用该随机数执行应用解锁,应该返回 6984
- ü 选择应用,取随机数,校验口令,使用该随机数执行卡片锁定,应该返回 6984

l 一次随机数只能使用一次

- ü 取随机数,正确执行明文+MAC 写二进制 0016 文件,再次使用该随机数执行该命令,应该返回 6984
- ü 选择应用,取随机数,正确执行应用临时锁定,再次使用该随机数执行应用解锁,应该返回 6984
- ü 选择应用,取随机数,正确执行应用永久锁定,再次使用该随机数执行卡片锁定,应该返回 6984

4.1.8 应用锁定

4.1.8.1 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。

4.1.8.2 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:
 - 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

- | 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

4.1.9 应用解锁

4.1.9.1 测试目的：

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

4.1.9.2 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：
 - | 应用临时锁定后，第一次执行该命令的 MAC 不对，应该返回 6988
 - | 第二次执行该命令的 MAC 不对，应该返回 6988
 - | 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
 - | 第一次执行该命令的 MAC 不对，应该返回 6988
 - | 第二次执行该命令的 MAC 不对，应该返回 6988
 - | 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

4.1.10 卡片锁定

4.1.10.1 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

4.1.10.2 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

4.1.11 取响应命令

4.1.11.1 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。

4.1.11.2 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) 交易指令: 如圈存初始化、圈存、修改透支初始化、修改透支、圈提初始化、圈提、消费初始化、消费、取现初始化、取现、灰锁初始化、灰锁、联机解扣初始化、联机解扣、解扣、取交易认证, 返回 61XX 后执行取响应应该返回 9000
- 4) 执行部分取响应应该返回数据+61XX (XX 是剩余长度)
- 5) 没有响应, 执行取响应命令应该返回 6F00
- 6) 应用锁定后, 选择应用返回 6A81, 执行 GET RESPONSE 命令应该取出 FCI

4.1.12 选择

4.1.12.1 测试目的:

选择命令通过文件名或 AID 来选择 IC 卡中的 PSE、DDF 或 ADF, 成功执行该命令设定 PSE、DDF 或 ADF 的路径。后续命令作用于与用 SFI 选定的 PSE、DDF 或 ADF 相联系的 AEF。从 IC 卡返回的应答报文包含回送 FCI。

4.1.12.2 测试步骤:

- 1) 正确性测试:

I 使用 DF 文件名称选择应用:

- ü 选择 MF, 应该返回的信息格式为: 6F 15 84 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 03 88 01 01
- ü 选择 ADF1, 应该返回的信息格式为: 6F 32 84 09 A0 00 00 00 03 86 98 07 01 A5 25 9F

08 01 02 9F 0C 1E +DATA, 其中 DATA 为写入的 0015 文件信息

- ü 选择 ADF2, 应该返回的信息格式为: 6F 32 84 09 A0 00 00 00 03 86 98 07 02 A5 25 9F 08 01 02 9F 0C 1E +DATA, 其中 DATA 为写入的 0015 文件信息

I 使用 P2=02 方式选择 ADF 应用:

- ü 执行该命令 00 a4 04 00 06 A0 00 00 00 03 86, 应该返回 ADF1 的 FCI 信息
- ü 再执行 00 a4 04 02 06 A0 00 00 00 03 86, 应该返回 ADF2 的 FCI 信息
- ü 再执行 00 a4 04 02 06 A0 00 00 00 03 86, 应该返回 6A82

- 2) 选择密钥文件、钱包文件、存折文件应该返回 6A82
- 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) 执行该命令, P1 为 04 以外的值都返回 6A86

4.2 金融交易命令

根据规范要求, 需要测试的金融交易命令有:

- 1) 圈存
- 2) 圈提
- 3) 取现
- 4) 消费
- 5) 修改透支
- 6) 取余额
- 7) 取交易认证

4.2.1 圈存

4.2.1.1 测试目的:

用于电子钱包/存折圈存功能

4.2.1.2 测试步骤:

- 1) 正确性测试:
 - I 金融应用下可以进行钱包和存折的圈存
 - ü 复位, 选择金融应用
 - ü 校验 PIN
 - ü 钱包圈存

- ü 取交易认证, 取余额, 取标准明细, 并比较结果
- ü 存折圈存
- ü 取交易认证, 取余额, 取标准明细, 并比较结果
- l 测试圈存初始化/圈存返回的响应报文:
 - ü 测试返回的密钥版本应该是对应索引圈存密钥的版本, 返回的算法标识应该是对应索引圈存密钥的算法标识。
 - ü 比较返回的余额、联机交易序号、MAC1
 - ü 测试圈存返回的 TAC
- 2) 圈存初始化返回 6110 时, 取响应指令为 00 C0 00 00 00, 卡片应该返回 6C10, 仍可以通过取响应取出圈存初始化的响应报文并继续正确执行圈存
- 3) 未验证 PIN, 圈存初始化应该返回 69 82
- 4) 验证 PIN, 未进行圈存初始化, 直接进行圈存交易应该返回 69 01
- 5) 验证 PIN, 密钥标识符不正确, 圈存初始化应该返回 94 03
- 6) 圈存初始化成功后, 进行圈存时报文中的 MAC 不对, 应该返回 93 02
- 7) 电子钱包最大余额为 FFFFFFFF, 交易金额+当前余额超过 FFFFFFFF, 圈存初始化应该返回 6985 (交易金额和目标余额都不能超过 FFFFFFFF)
- 8) 电子存折最大余额为 FFFFFFFF, 交易金额+当前余额超过 FFFFFFFF, 圈存初始化应该返回 6985 (交易金额和目标余额都不能超过 FFFFFFFF)
- 9) 遍历测试圈存金额从 00000000 到 FFFFFFFF 的所有情况
- 10) 电子钱包/存折的交易计数器达到 FFFF, 再执行交易命令应该返回 9402

4.2.2 圈提

4.2.2.1 测试目的:

电子存折圈提功能

4.2.2.2 测试步骤:

- 1) 正确性测试:
 - l 分别选择 ADF1 和 ADF2 应用, 都可以进行存折的圈提
 - ü 复位, 选择金融应用
 - ü 校验 PIN
 - ü 存折圈提
 - ü 取交易认证, 取余额, 取标准明细, 并比较结果
 - l 测试圈提初始化/圈提的响应报文
 - ü 测试返回的密钥版本应该是对应索引圈提密钥的版本, 返回的算法标识应该是对应索引圈提密钥的算法标识。

- ü 比较返回的余额、联机交易序号、MAC1
 - ü 测试圈提返回的 MAC3
- 2) 圈提初始化返回 6110 时，取响应指令为 00 C0 00 00 00，卡片应该返回 6C10，仍可以通过取响应取出圈提初始化的响应报文并继续正确执行圈提
 - 3) 未验证 PIN，圈提初始化返回 69 82
 - 4) 验证 PIN，未进行圈提初始化，直接进行圈提交易返回 69 01
 - 5) 验证 PIN，密钥标识符不正确，圈提初始化返回 94 03
 - 6) 圈提初始化成功，进行圈提时报文中的 MAC 不对，返回 93 02
 - 7) 交易金额>应用下的余额，初始化应该返回 94 01
 - 8) 遍历测试圈提金额从 FFFFFFFF 到 00000000 的所有情况
 - 9) 电子存折的交易计数器达到 FFFF，再执行交易命令应该返回 9402

4.2.3 取现

4.2.3.1 测试目的:

电子存折取现

4.2.3.2 测试步骤:

- 1) 正确性测试:
 - I 金融应用下可以进行存折的取现
 - ü 复位，选择金融应用
 - ü 校验 PIN
 - ü 存折取现
 - ü 取交易认证，取余额，取标准明细，并比较结果
 - I 测试取现初始化/取现的响应报文
 - ü 测试返回的密钥版本应该是对应索引消费密钥的版本，返回的算法标识应该是对应索引消费密钥的算法标识。
 - ü 比较返回的余额、联机交易序号、透支限额
 - ü 测试取现返回的 TAC 和 MAC2
- 2) 取现初始化返回 610F 时，取响应指令为 00 C0 00 00 00，卡片应该返回 6C0F，仍可以通过取响应取出取现初始化的响应报文并继续正确执行取现
- 3) 未验证 PIN，取现初始化返回 69 82
- 4) 验证 PIN，未进行取现初始化，直接进行取现交易返回 69 01
- 5) 验证 PIN，密钥标识符不正确，取现初始化返回 94 03
- 6) 取现初始化成功，进行消费时报文中的 MAC 不对，返回 93 02

- 7) 交易金额大于应用余额，取现初始化应该返回 94 01
- 8) 遍历测试取现金额从 FFFFFFFF 到 00000000 的所有情况
- 9) 电子存折的交易计数器达到 FFFF，再执行交易命令应该返回 9402

4.2.4 消费

4.2.4.1 测试目的：

电子钱包/电子存折消费功能

4.2.4.2 测试步骤：

- 1) 正确性测试：
 - I 选择 ADF1 和 ADF2 应用，都应该可以进行钱包和存折的消费
 - ü 复位，选择金融应用
 - ü 钱包消费
 - ü 校验 PIN
 - ü 取交易认证，取余额，取标准明细（电子钱包消费不取明细，取出的明细应该是上一笔交易的明细），并比较结果
 - ü 存折消费
 - ü 取交易认证，取余额，取标准明细，并比较结果
 - I 测试消费初始化/消费的响应报文
 - ü 测试返回的密钥版本应该是对应索引消费密钥的版本，返回的算法标识应该是对应索引消费密钥的算法标识。
 - ü 比较返回的余额、脱机交易序号、透支限额
 - ü 测试消费返回的 TAC 和 MAC2
- 2) 消费初始化返回 610F 时，取响应指令为 00 C0 00 00 00，卡片应该返回 6C0F，仍可以通过取响应取出消费初始化的响应报文并继续正确执行消费
- 3) 未验证 PIN，消费初始化返回 69 82
- 4) 验证 PIN，未进行消费初始化，直接进行消费交易返回 69 01
- 5) 验证 PIN，密钥标识符不正确，消费初始化返回 94 03
- 6) 消费初始化成功，进行消费时报文中的 MAC 不对，返回 93 02
- 7) 交易金额大于卡中应用余额，消费初始化应该返回 94 01
- 8) 遍历测试消费金额从 FFFFFFFF 到 00000000 的所有情况
- 9) 电子存折或钱包的交易计数器达到 FFFF，再执行交易命令应该返回 9402

4.2.5 修改透支限额

4.2.5.1 测试目的:

测试电子存折修改透支限额功能

4.2.5.2 测试步骤:

1) 正确性测试:

- I 选择 ADF1 和 ADF2 应用, 应用都可以进行存折的修改透支限额
 - ü 复位, 选择金融应用
 - ü 校验 PIN
 - ü 存折修改透支限额
 - ü 取交易认证, 取余额, 取标准明细, 并比较结果
- I 测试修改透支限额初始化/修改透支限额返回的响应报文
 - ü 测试返回的密钥版本应该是对应索引修改透支密钥的版本, 返回的算法标识应该是对应索引修改透支密钥的算法标识。
 - ü 比较返回的余额、联机交易序号、旧透支限额、MAC1
 - ü 测试修改透支限额返回的 TAC

- 2) 修改透支限额初始化返回 6113 时, 取响应指令为 00 C0 00 00 00, 卡片应该返回 6C13, 仍可以通过取响应取出修改透支限额初始化的响应报文并继续正确执行修改透支限额
- 3) 未验证 PIN, 修改透支限额初始化返回 69 82
- 4) 验证 PIN, 未进行修改透支限额初始化, 直接进行修改透支限额交易返回 69 01
- 5) 验证 PIN, 密钥标识符不正确, 修改透支限额初始化返回 94 03
- 6) 修改透支限额初始化成功, 进行修改透支限额时报文中的 MAC 不对, 返回 93 02
- 7) 如果旧余额-旧限额+新限额<0, 修改透支命令应该返回 9401
- 8) 如果旧余额-旧限额+新限额>0xFFFFFFFF, 修改透支命令应该返回 6985
- 9) 电子存折的交易计数器达到 FFFF, 再执行交易命令应该返回 9402

4.2.6 读余额

4.2.6.1 测试目的:

电子钱包/电子存折读余额功能

4.2.6.2 测试步骤:

- 1) 正确性测试: 金融应用 ADF1 和 ADF2 下, 读电子存折、电子钱包余额
 - I 复位, 选择应用

- l 读电子钱包余额，应该能够正确返回电子钱包的余额
 - l 校验 PIN
 - l 读电子存折余额，应该能够正确返回电子存折的余额
 - l 读电子钱包余额，应该能够正确返回电子钱包的余额
- 2) 未验证 PIN，读电子存折余额，应返回 69 82

4.2.7 取交易认证

4.2.7.1 测试目的：

取交易认证功能

4.2.7.2 测试步骤：

- 1) 正确性测试：金融应用 ADF1 和 ADF2 下的各种交易后取交易认证：
- l 圈存：钱包、存折
 - l 圈提：存折
 - l 消费：钱包、存折
 - l 取现：存折
 - l 修改透支：存折
- 2) 执行该命令交易序号不正确应该返回 9406
- l 交易类型在许可范围内，但报文中的交易序号不是最近一笔金融交易的交易序号，应该返回 9406
 - l 交易类型在许可范围内，交易序号是最近一笔金融交易的交易序号，但交易类型不对，也应该返回 9406

4.3 复合消费命令

根据规范要求，需要测试的复合消费命令有：

- 1) 复合应用消费初始化
- 2) 更新复合应用数据缓存
- 3) 复合应用消费

4.3.1 复合应用消费

4.3.1.1 测试目的:

用于复合应用消费交易

4.3.1.2 测试步骤:

- 1) 正确性测试: 执行复合应用消费初始化命令成功后, 检查返回电子钱包余额, 交易序号, 密钥信息的正确性, 再继续执行复合应用消费命令, 验证返回 MAC1 的正确性。
- 2) 没有执行初始化复合应用消费交易命令, 执行复合应用消费交易应该返回 6901
- 3) 金额不足执行该命令应该返回 9401。
- 4) 密钥标识符不正确应该返回 9403
- 5) 应用被临时锁定, 复合应用消费应该返回 6985
- 6) 应用被永久锁定, 复合应用消费应该返回 9303
- 7) 卡片锁定, 复合应用消费应该返回 6A81

4.3.2 更新复合应用数据缓存

4.3.2.1 测试目的:

用于复合应用消费交易中更新复合应用数据缓存, 缓存数据将被复合应用消费命令用于改写复合应用专用文件中的相关记录。

4.3.2.2 测试步骤:

- 1) 正确性测试: 应用类型标识 01, 应用锁定标志 00, 执行更新复合应用数据缓存命令应该返回 9000
- 2) 更新复合应用数据缓存命令长度错误应该返回 6700
- 3) 更新复合应用数据缓存命令与文件结构不相容应该返回 6981
- 4) 更新复合应用数据缓存记录号不存在应该返回 6A83
- 5) 更新复合应用数据缓存, 文件不存在应该返回 6A82
- 6) 更新复合应用数据缓存命令长度大于复合专用文件中相应记录长度返回 6A84
- 7) 如果应用锁定标志设置, 更改复合应用缓存数据应该返回 9407

5 交易状态机测试

5.1 测试目的：

在金融交易中卡片总是处于一种状态下，在一种状态下，某些命令应该能执行。在卡片从终端收到一条命令后，它必须检查当前状态是否允许执行。

5.2 测试步骤：

1) 正确性测试：

- I 交易初始化后，卡片金融该交易状态，正确执行相应的交易，应该能够成功
分别测试以下几种情况：
 - ü 圈存状态：钱包、存折
 - ü 圈提状态：存折
 - ü 消费状态：钱包、存折
 - ü 取现状态：存折
 - ü 修改透支状态：存折

2) 交易初始化后，执行相对应的交易应该能够成功；执行其他交易，应该返回 6901

3) 交易初始化后，插入取交易认证命令对当前状态机的影响（金融应用下需测试的状态和步骤 1 相同）：

- I 执行交易初始化命令，进入该交易状态，执行正确的取交易认证命令，卡片的交易状态不变，可以继续执行交易指令
- I 执行交易初始化命令，进入该交易状态，执行错误的取交易认证命令，卡片的交易状态变为空闲状态，继续执行交易指令应该返回 6901

4) 交易初始化后，插入读余额命令对当前状态机的影响（金融应用下需测试的状态和步骤 1 相同）：

- I 执行交易初始化命令，进入该交易状态，执行正确的读余额命令，卡片的交易状态不变，可以继续执行交易指令
- I 执行交易初始化命令，进入该交易状态，执行错误的读余额命令，卡片的交易状态变为空闲状态，继续执行交易指令应该返回 6901

5) 交易初始化后，卡片进入该交易状态，中间插入读余额、取交易认证以外的指令，

卡片的交易状态变为空闲状态，继续执行交易指令将返回 6901（使用一条交易指令和一条非交易指令进行测试）：金融应用和石化应用下需测试的状态和步骤 1 相同

6) 交易初始化后，再执行交易命令对当前状态机的影响：

- l 执行对应的交易命令成功后，再继续执行交易命令，应该返回 6901
- l 执行其他的交易命令，应该返回 6901
- l 执行对应的交易命令，但是执行失败，再正确执行交易命令，应该返回 6901
- l 再执行错误的交易初始化命令，执行对应的交易命令应该返回 6901。

6 随机交易测试

6.1 测试目的：

随机执行金融/石化应用下各种可以执行的交易，每笔交易后要求比较每一个可能产生影响和变化的值：包括交易明细中的每一项、交易认证、余额。

6.2 测试步骤：

- 1) 将每种交易类型顺序编号，编号时规定：加油交易的编号>一般金融交易，具体每种交易类型的编号为：0—电子存折圈存、1—电子钱包圈存、2—电子存折圈提、3—电子存折消费、4—电子钱包消费、5—电子存折取现、6—修改透支限额
- 2) 根据卡片类型确定要建立哪种类型应用，并进行个人化（写入两组交易密钥），预设各种全局变量的值：

```
%wedljyjh=0000          //存折联机交易序号
%wedtjyjh=0000          //存折脱机交易序号
%wepljyjh=0000          //钱包联机交易序号
%weptjyjh=0000          //钱包脱机交易序号
%iedbal=0               //存折上的实际金额，不包括透支限额
%iedlimit=0             //存折上的透支限额 iedbal+iedlimit=读余额返回的余额
%iepbal=0               //钱包余额
%imaxlx                //最大交易类型编号，金融卡时该值为 7，加油卡时该值为 9
%itotal                //进行多少笔交易，最起码执行 1000
```


- 3) 随机生成要测试的交易类型
- 4) 根据交易类型进行交易，并比较交易时，终端机编号，交易时间为随机取得，交易密钥从两组交易密钥中随机选择，交易金额按照以下规律选取：
 - Ⅰ 存钱交易：存入 0~（最大金额-现有余额）间的随机金额
 - Ⅰ 花钱交易：花掉 0~现有余额间的随机金额，
 - Ⅰ 修改透支：当除去原透支后的钱（卡上的实际金额）>0 时，交易金额为 0~卡上的实际金额，当卡上的实际金额<0 时，交易金额 1-卡上的实际金额
- 5) 转第 3 步

7 参数测试

本部分主要对每个规范中规定的命令的参数 CLA,P1,P2,P3 进行详细测试

7.1 基本命令

7.1.1 读二进制

- 1) CLA: 00
 - Ⅰ CLA 取 00 以外的值，应该返回 6E00
- 2) P1P2: P1 高三位为 100 低五位为短的文件标识符，最高位不为 1 所读文件为当前文件
 - Ⅰ P1 值在 0x95-0x9F 之间，如果不为 0x95、0x96 和 0x98，应该返回 6A82
 - Ⅰ P1 取 0x95-0x9F 以外的值，应该返回 6A86
- 3) P2
 - Ⅰ P2 偏移量超过文件空间应该返回 6B00
- 4) P3:
 - Ⅰ P3 长度超过文件实际空间应该返回 6700

7.1.2 写二进制

- 1) CLA: 04
 - I CLA 取 04 以外的值, 应该返回 6E00
- 2) P1P2: P1 高三位为 100 低五位为短的文件标识符, 最高位不为 1 所读文件为当前文件
 - I P1 值在 0x95-0x9F 之间, 如果不为 0x95、0x96 和 0x98, 应该返回 6A82
 - I P1 取 0x95-0x9F 以外的值, 应该返回 6A86
- 3) P2
 - I P2 偏移量超过文件空间应该返回 6B00
- 4) P3:
 - I P3 长度超过文件实际空间应该返回 6700

7.1.3 校验 PIN

- 1) CLA: 00
 - I CLA 取 00 以外的值, 应该返回 6E00
- 2) P1: 00
 - I P1 取 00 以外的任何值, 应该返回 6A 86
- 3) P2: 00
 - I P2 取 00 以外的任何值, 应该返回 6A 86
- 4) P3: 02
 - I P3 取 0x02 以外的任何值应该返回 6700

7.1.4 修改 PIN

- 1) CLA: 80
 - I CLA 取 80 以外的任何值, 应该返回 6E 00
- 2) P1: 01/00
 - I P1 取 00/01 以外的任何值, 应该返回 6A 86
- 3) P2: 00
 - I P2 取 00 以外的任何值, 应该返回 6A 86
- 4) P3: LC (05-0D)

┆ P3 取 05-0D 以外的任何值，应该返回 67 00

7.1.5 重装 PIN

1) CLA: 80

┆ CLA 取以外的任何值，应该返回 6E 00

2) P1: 00/01

┆ P1 取 00/01 以外的任何值，应该返回 6A 86

3) P2: 00

┆ P2 取 00 以外的任何值，应该返回 6A 86

4) P3: LC(06-0A)

┆ P3 取 06-0A 以外的任何值，应该返回 67 00

7.1.6 PIN 解锁

1) CLA: 84

┆ CLA 取 84 以外的任何值，应该返回 6E 00

2) P1: 00

┆ P1 取 00 以外的任何值，应该返回 6A 86

3) P2: 01

┆ P2 取 01 以外的任何值，应该返回 6A 86

4) P3: LC(0C)

┆ P3 取 0C 以外的任何值，应该返回 67 00

7.1.7 取随机数

1) CLA: 00

┆ CLA 取 00 以外的任何值，应该返回 6E 00

2) P1: 00

┆ P1 取 00 以外的任何值，应该返回 6A 86

3) P2: 00

┆ P2 取 00 以外的任何值，应该返回 6A 86

4) P3: LC(04 和 08)

I P3 取 04 和 08 以外的任何值，应该返回 67 00

7.1.8 应用锁定

1) CLA: 84

I CLA 取 84 以外的任何值，应该返回 6E 00

2) P1: 00

I P1 取 00 以外的任何值，应该返回 6A 86

3) P2: 00/01

I P2 取 00/01 以外的任何值，应该返回 6A 86

4) P3: LC(04)

I P3 取 04 以外的任何值，应该返回 67 00

7.1.9 应用解锁

1) CLA: 84

I CLA 取 84 以外的任何值，应该返回 6E 00

2) P1: 00

I P1 取 00 以外的任何值，应该返回 6A 86

3) P2: 00

I P2 取 00 以外的任何值，应该返回 6A 86

4) P3: LC(04)

I P3 取 04 以外的任何值，应该返回 67 00

7.1.10 卡片锁定

1) CLA: 84

I CLA 取 84 以外的任何值，应该返回 6E 00

2) P1: 00

I P1 取 00 以外的任何值，应该返回 6A 86

3) P2: 00

I P2 取 00 以外的任何值，应该返回 6A 86

4) P3: LC(04)

┆ P3 取 04 以外的任何值, 应该返回 67 00

7.1.11 取响应

1) CLA: 00

┆ CLA 取 00 以外的任何值, 应该返回 6E 00

2) P1: 00

┆ P1 取 00 以外的任何值, 应该返回 6A 86

3) P2: 00

┆ P2 取 00 以外的任何值, 应该返回 6A 86

4) P3: (LE 为响应的期望数据长度)

┆ P3 的值为选择文件后响应的长度, 不需要测试

7.1.12 选择

1) CLA: 00

┆ CLA 取 00 以外的任何值, 应该返回 6E 00

2) P1: 04

┆ P1 取 04 以外的任何值, 应该返回 6A 86

3) P2: 00/02

┆ P2 取 00/02 以外的任何值, 应该返回 6A 86

4) P3: LC(05-10)

┆ P3 取 05-10 以外的任何值, 应该返回 67 00

8 防拔插测试

8.1 概述

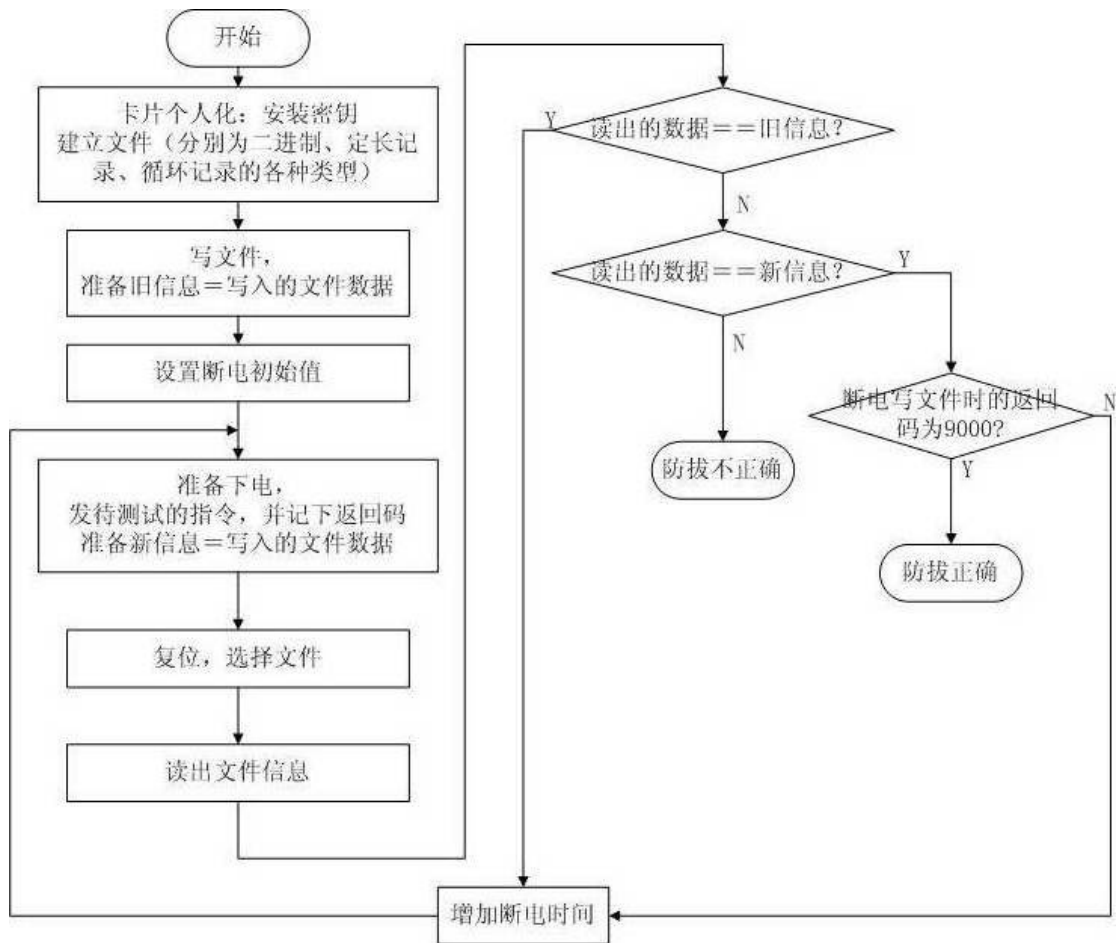
卡片必须在命令处理过程中的任何情况下, 甚至在更新 EEPROM 过程中掉电的情况下, 保持数据的完整性。因此需要在每次更新数据前对数据进行备份, 并且在重新加电后

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。

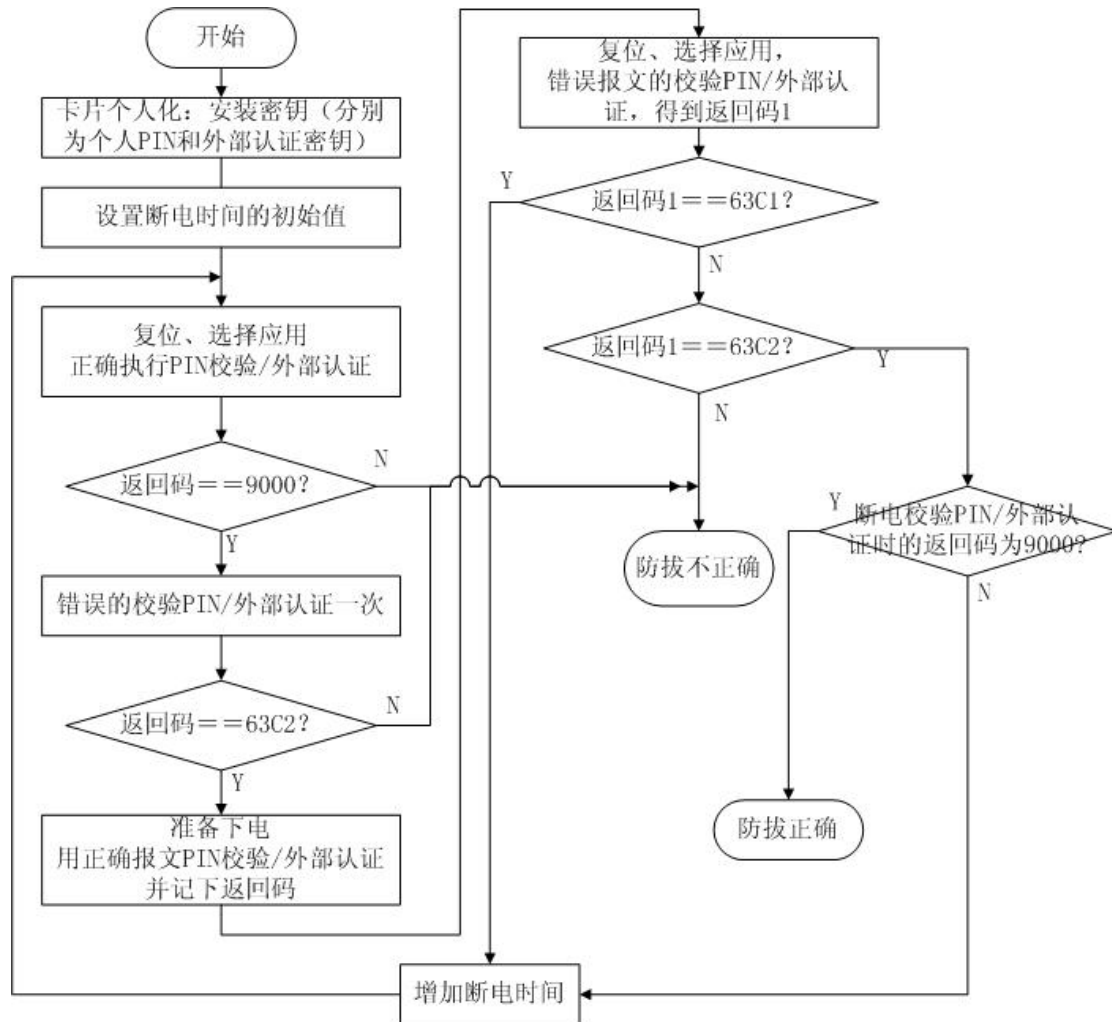
8.2 防拔流程

8.2.1 写二进制防拔

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 37H。

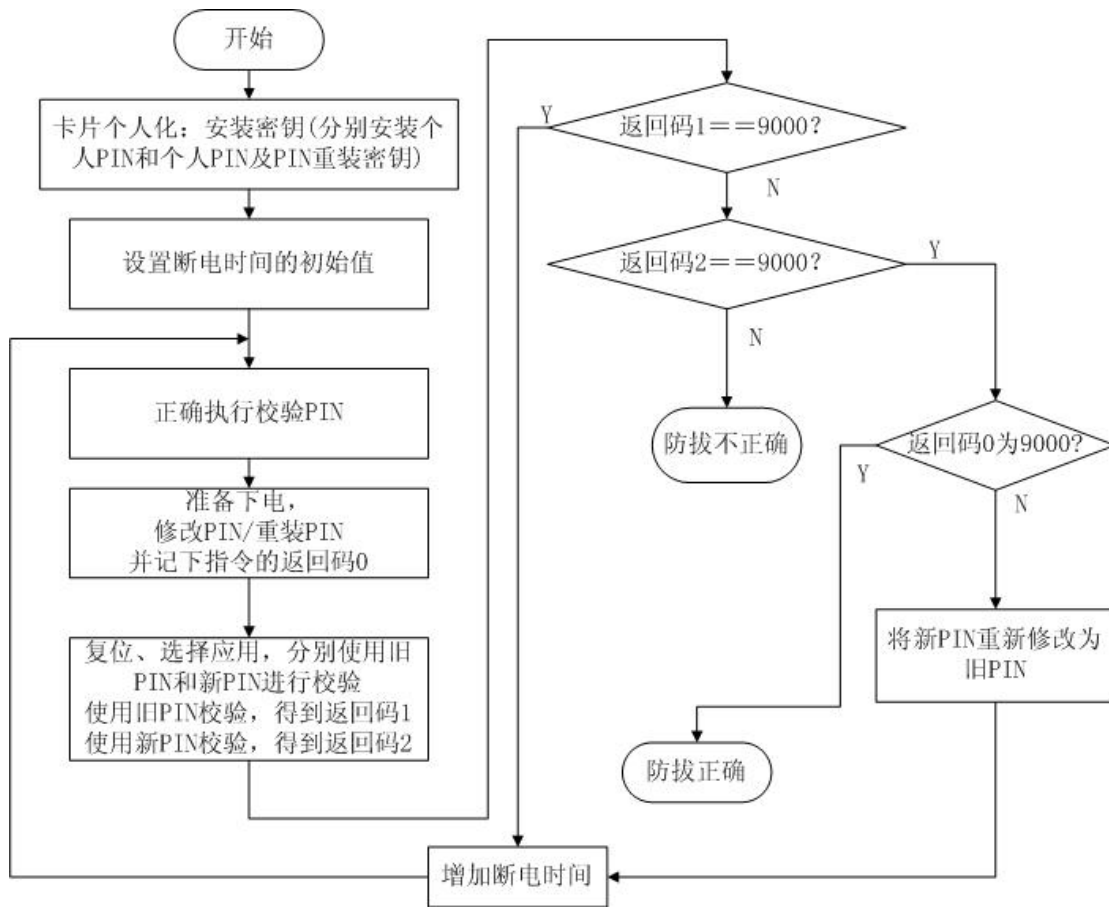


8.2.2 校验 PIN 防拔流程



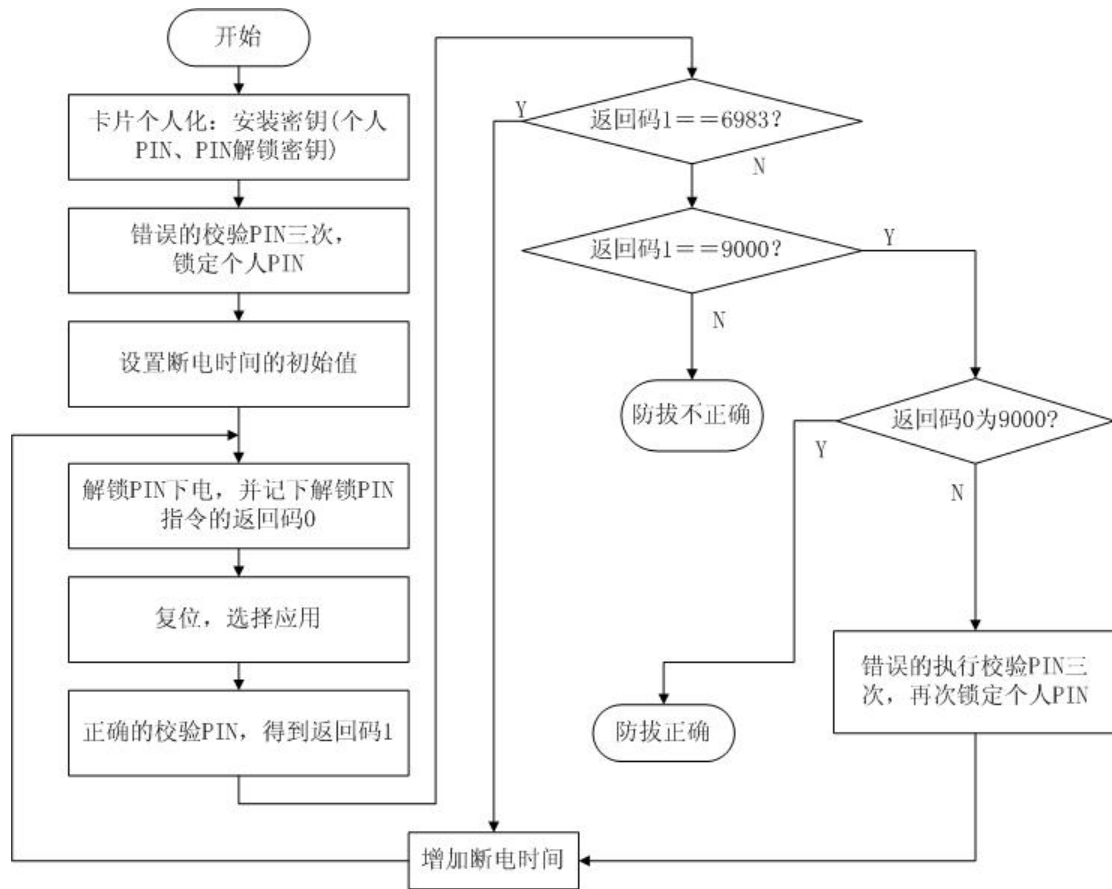
校验PIN、外部认证防拔测试流程图

8.2.3 修改 PIN/重装 PIN 防拔流程



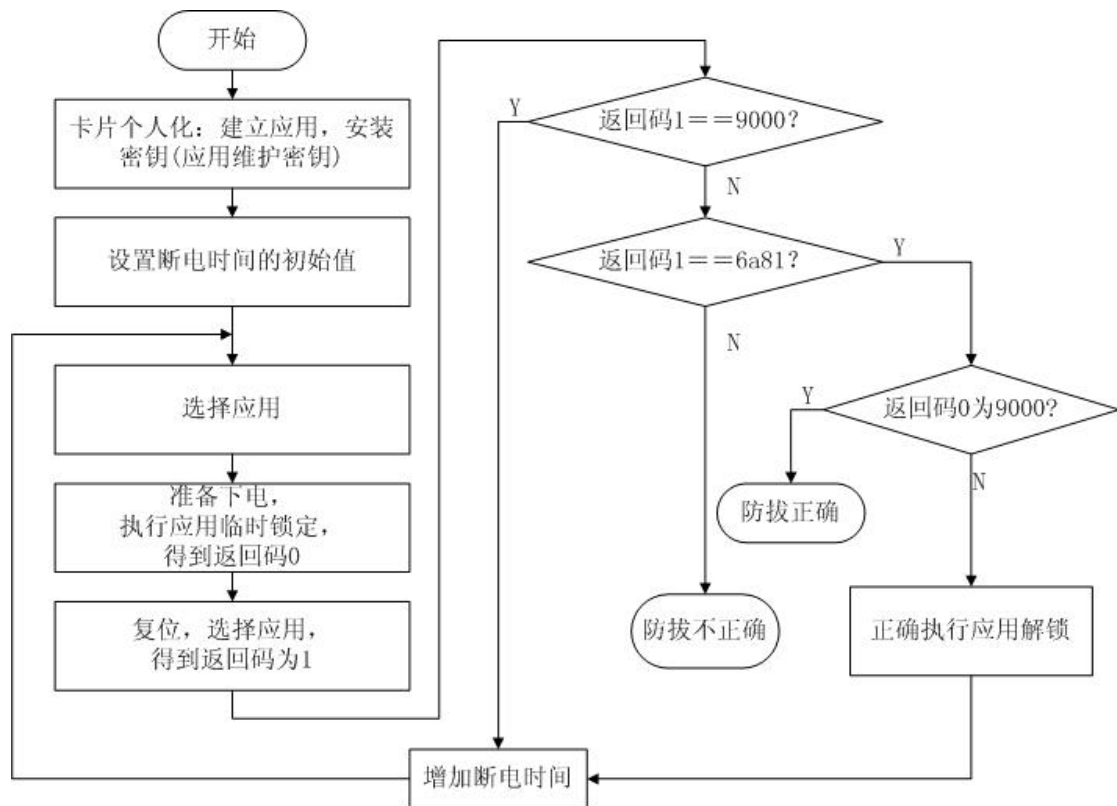
修改PIN、重装PIN防拔测试流程图

8.2.4 解锁 PIN 防拔流程



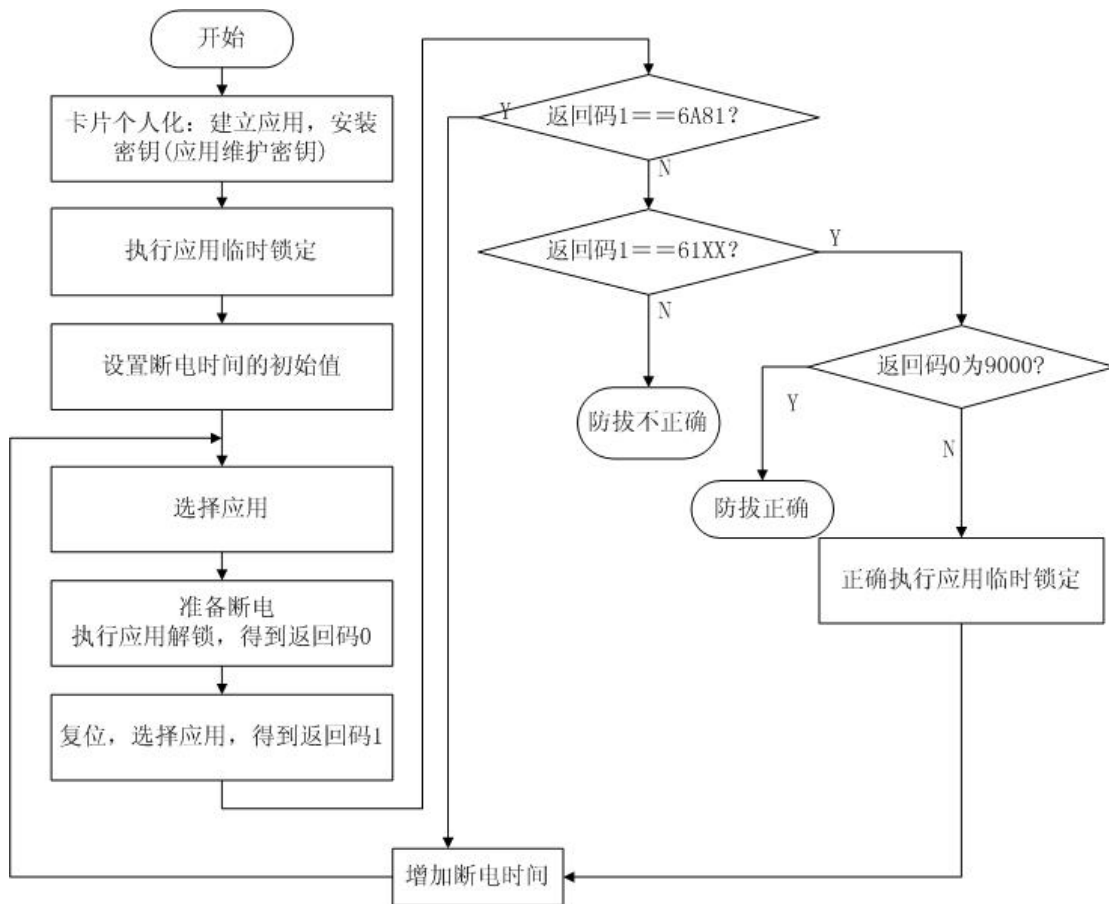
PIN解锁防拔测试流程图

8.2.5 应用临时锁定防拔流程



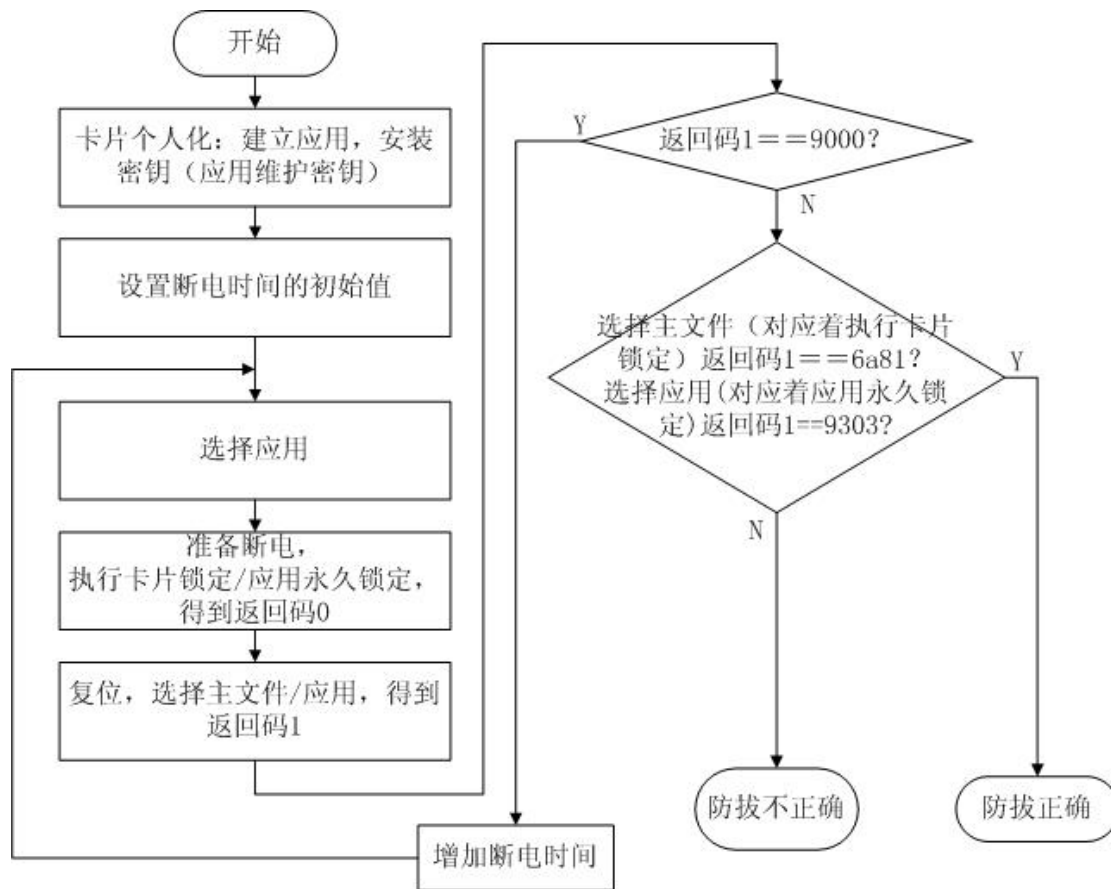
应用临时锁定防拔测试流程图

8.2.6 应用解锁防拔流程



应用解锁交易防拔测试流程图

8.2.7 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