

ICS 35.240.40

A 11

备案号:

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0045.1—2014

代替JR/T 0045.1—2008

中国金融集成电路（IC）卡检测规范 第 1 部分：借记/贷记应用卡片检测规范

China financial integrated circuit card test specifications—
Part 1: Debit/Credit card test specification

2014-07-30 发布

2014-07-30 实施

中国人民银行 发布

目 次

前言	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	4
5 总体要求	8
6 电特性和通讯协议的测试案例	8
6.1 一般要求	8
6.2 电特性测试 (TPSB)	9
6.3 卡片会话测试 (TPSC)	20
6.4 ATR 和字符间时间间隔测试 (TPSE)	23
6.5 T=0 协议测试 (TPSF)	24
6.6 T=1 协议测试 (TPSG)	29
7 借记贷记应用测试的测试案例	46
7.1 标准联机交易	46
7.2 应用锁定命令 (SDML)	46
7.3 应用锁定 (YYSD)	47
7.4 读应用数据 (DQSJ)	59
7.5 获取应用数据 (HQSJ)	64
7.6 PBOC 借记/贷记应用选择 (YYXZ)	65
7.7 应用解锁命令 (JSML)	69
7.8 应用解锁 (YYJS)	70
7.9 卡片锁定命令 (KSML)	77
7.10 卡片锁定 (KPSD)	78
7.11 联机批准交易 (LJPZ)	84
7.12 复合动态数据认证 (FHDT)	85
7.13 上次交易发卡行脚本失败 (JBSB)	96
7.14 卡片风险管理 (FXGL)	100
7.15 双货币超累计交易金额上限检查 (SHJC)	115
7.16 累计脱机交易金额限制数检查 9F5C (LJTJ)	118
7.17 支付系统环境目录 (ZFML)	120
7.18 DDA 测试 (DDCS)	121
7.19 更新卡片数据 (GXSJ)	140
7.20 EXTERNAL AUTHENTICATE 命令 (WBRZ)	147
7.21 上次联机交易发卡行认证失败 (RZSB)	148
7.22 联机交易失败 (LJSB)	156

7.23 GET DATA (GEDA)	172
7.24 GET PROCESSING OPTIONS 命令 (GPML)	172
7.25 发卡行认证 (FKRZ)	173
7.26 应用初始化 (YYCS)	177
7.27 发卡行脚本处理 (JBCL)	178
7.28 日志文件 (RZWJ)	213
7.29 新卡 (XINK)	219
7.30 脱机交易 (LXJY)	237
7.31 联机完成 (LJWC)	239
7.32 联机授权未完成 (LJWW)	250
7.33 PIN CHANGE/UNBLOCK 命令 (PCUC)	258
7.34 持卡人认证 (CKRZ)	262
7.35 PUT DATA 连续交易限制 (国际) (LXXZ)	265
7.36 支付系统环境 (ZFXT) (接触条件下适用)	267
7.37 近距离支付系统环境 (JZFX) (非接适用)	269
7.38 PUT DATA 命令 (PDML)	271
7.39 READ RECORD 命令 (REML)	272
7.40 静态应用数据认证 (JTRZ)	272
7.41 选择 PBOC 借记/贷记应用命令 (XZYY)	278
7.42 前次交易 SDA 失败 (SDSB)	279
7.43 UPDATE RECORD 命令 (URML)	299
7.44 执行交易金额 (双货币) 频度检查 (JEPJ)	301
7.45 执行国际国家频度检查 (GGPJ)	307
7.46 执行指定货币交易金额检查 (JEJC)	309
7.47 执行国际-货币频度检查 9F53=05 (GHJC)	311
7.48 连续脱机交易检查 (LTJC)	315
7.49 VERIFY 命令 (VFML)	324
7.50 防拔测试 (FBCS)	324
7.51 参数测试 (CSCS)	329
7.52 稳定性测试 (WDCS)	334
7.53 卡片在 ATM 上被受理的测试 (ATMT)	335
8 基于借记贷记的小额支付应用的测试案例	335
8.1 电子现金数据的读取 (EFR)	335
8.2 电子现金数据的更新 (EDU)	336
8.3 应用初始化 (EEC)	341
8.4 电子现金余额的更新 (EFS)	345
8.5 电子现金脱机接收后, 拒绝发卡行脚本 (EIS)	346
8.6 脱机数据认证 (EOD)	348
8.7 持卡人认证 (ECV)	350
8.8 卡片行为分析 (ECA)	354
8.9 防插拔 (EFB)	364
8.10 特殊流程 (ATM)	364
8.11 电子现金圈存日志	365

9 个人化要求	370
9.1 概述	370
9.2 基本特征	372
9.3 密钥信息	376
9.4 卡片特征与密钥信息的对应关系	389
9.5 卡片特征	391

前 言

JR/T 0045《中国金融集成电路（IC）卡检测规范》分为5个部分：

- 第1部分：借记/贷记应用卡片检测规范；
- 第2部分：借记/贷记应用终端检测规范；
- 第3部分：借记/贷记应用个人化检测规范；
- 第4部分：非接触卡片检测规范；
- 第5部分：非接触终端检测规范。

本部分为JR/T 0045的第1部分。

本部分依据GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0045.1—2008《中国金融集成电路（IC）卡检测规范 第1部分：借记/贷记应用卡片检测规范》。

本部分与JR/T 0045.1—2008相比主要变化如下：

- 修改了标准的前言；
- 删除 T=1 协议重发的部分案例；
- 删除要求执行发卡行脚本与外部认证关联的案例；
- 修改了部分发卡行脚本执行案例；
- 增加了在长度大于 1024 位的 CA、发卡行和 IC 卡密钥长度时的静态和动态数据认证案例；
- 增加了卡片在 ATM 上被受理的测试；
- 增加了 PPSE 相关案例；
- 增加了基于借记贷记的小额支付检测案例；
- 增加了多应用选择的检测案例；
- 对第 9 章中的个人化要求数据做了少量修改；
- 对原标准在文字描述上的勘误做出修正。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分主要起草单位：中国人民银行、中国银联股份有限公司、银行卡检测中心、中钞信用卡产业发展有限公司、百富计算机技术（深圳）有限公司、深圳市新国都技术股份有限公司、惠尔丰（中国）信息系统有限公司、福建新大陆电脑股份有限公司、上海杉德金卡信息系统科技有限公司、深圳视融达科技有限公司、北京握奇数据系统有限公司、中国金融电子化公司。

本部分主要起草人：王永红、李晓枫、陆书春、潘润红、杜宁、李兴锋、陈则栋、李新、汤沁莹、齐大鹏、刘志刚、张永峰、余沁、郑超、张策、李乃珊、张庆、李春欢、张栋、李一凡、李小平、宁婷婷、何海玲、赵亚平、李伟海、翁锋华、李传婕、隋欣桐、肖含、顾伯华、尤萌、马洁荣、张艳。

本部分于 2008 年首次发布，本次为第一次修订。

引 言

本部分的主要依据是 JR/T 0025.3、JR/T 0025.4 和 JR/T 0025.5，在此基础上制定了中国金融集成电路（IC）卡借记/贷记应用卡片的相关检测案例。

中国金融集成电路（IC）卡检测规范

第1部分：借记/贷记应用卡片检测规范

1 范围

本部分从卡片检测的角度描述了对借记/贷记交易流程的要求，包括卡片内部处理细节、卡片使用数据元、卡片支持指令集等。

本部分适用于由银行发行或受理的金融借记/贷记应用的 IC 卡。其使用对象主要是与金融借记/贷记 IC 卡应用相关的卡片制造、检测、发行、受理，以及应用系统的研制、开发、集成和维护等部门（单位）。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0025—2013 中国金融集成电路（IC）卡规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

半字节 nibble

一个字节的高四位或低四位。

3.2

保护时间 guardtime

同一方向发送的前一个字符奇偶位下降沿和后一个字符起始位下降沿之间的最小时间。

3.3

报文 message

由终端发送给卡片（或反之）的一串字节，不包括传输控制字符。

3.4

报文认证码 message authentication code

对数据的一种对称加密变换，为保护数据发送方发出和接收方收到的数据不被第三方伪造。

3.5

磁条 magstripe

包括磁编码信息的条状物。

3.6

触点 contact

在集成电路卡和外部接口设备之间保持电流连续性的导电元件。

3.7

发卡行行为代码 `issuer action code`

发卡行根据TVR的内容选择的动作。

3.9

公钥 `public key`

在一个实体使用的非对称密钥对中可以被公众使用的密钥。在数字签名方案中，公钥定义了验证函数。

3.10

公钥证书 `public key certificate`

由认证中心签名的不可伪造的某个实体的公钥信息。

3.11

哈希函数 `hash function`

将一个位串映射成固定长度的位串的函数，它满足以下两个特性：

——给定一个输出，不可能通过计算得到与该输出对应的输入；

——给定一个输入，不可能通过计算得到具有相同的输出的另一个输入。

如果哈希函数要求防冲突，它还应满足以下特性：

不可能通过计算找到两个不同的输入具有相同的输出。

3.12

哈希结果 `hash result`

哈希函数输出的位串。

3.13

集成电路 `integrated circuit(s)`

被设计用来完成处理和/或存储功能的电子器件。

3.14

集成电路卡 `integrated circuit(s) card`

内部封装一个或多个集成电路，来完成处理和存储功能的卡片。

3.15

加密 `encipherment`

基于某种加密算法对数据作可逆的变换从而生成密文的过程。

3.16

加密算法 `cryptographic algorithm`

隐藏或显现数据信息内容的变换算法。

3.17

脚本 `script`

发卡行向终端发送的命令或命令序列，目的是向 IC 卡连续输入命令。

3.18

接口设备 `interface device`

终端上插入 IC 卡的部分，包括其中的机械和电气部分。

3.19

金融交易 `financial transaction`

在持卡人和商户或收单行之间发生的通过支付来换取货物或服务的行为。

3.20

静止状态 inactive

当 IC 卡上的电源电压 (VCC) 和其它信号相对于地的电压值小于或等于 0.4 伏时, 则称电源电压和这些信号处于静止状态。

3.21**卡片 card**

支付系统定义的支付卡片。

3.22**块 block**

包含两个或三个域(头域、信息域、尾域)的字符组。

3.23**冷复位 cold reset**

当 IC 卡的电源电压 (VCC) 和其它信号从静止状态中复苏且申请复位信号时, IC 卡产生的复位。

3.24**路径 path**

没有分隔的文件标识符的连接。

3.25**密钥 key**

加密转换中控制操作的一组符号。

3.26**密文 cryptogram**

加密运算的结果。

3.27**密码 ciphertext**

加密的信息。

3.28**命令 command**

终端向 IC 卡发出的一条信息, 该信息启动一个操作或请求一个应答。

3.29**热复位 warm reset**

在时钟 (CLK) 和电源电压 (VCC) 处于激活状态的前提下, IC 卡收到复位信号时产生的复位。

3.30**认证 authentication**

确认一个实体所宣称的身份的措施。

3.31**认证中心 certification authority**

证明公钥和其它相关信息同其拥有者相关联的可信的第三方机构。

3.32**数字签名 digital signature**

对数据的一种非对称加密变换。该变换可以使数据接收方确认数据的来源和完整性, 保护数据发送方发出和接收方收到的数据不被第三方篡改, 也保护数据发送方发出的数据不被接收方篡改。

3.33**T=0**

面向字符的异步半双工传输协议。

3.34

T=1

面向块的异步半双工传输协议。

3.35

响应 response

IC 卡接收到命令报文经过处理后返回给终端的报文。

3.36

应用 application

卡片和终端之间的应用协议和相关的数据集。

3.37

支付系统环境 payment system environment

当符合本规范的支付系统应用被选择，IC 卡中所确立的逻辑条件。

3.38

证书 certificate

由发行证书的认证中心使用其私钥对实体的公钥，身份信息以及其它相关信息进行签名，形成的不可伪造的数据。

3.39

字节 byte

8 个二进制位(位)。

3.40

终端 terminal

为完成金融交易而在交易点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其它部件和接口，例如与主机通讯的接口。

3.41

终端行为代码 terminal action code

终端行为代码（缺省、拒绝、联机）反映了收单行根据 TVR 的内容选择的动作。

3.42

状态 H state H

高电平状态。根据 IC 卡中的逻辑约定，可以是逻辑 1 或逻辑 0。

3.43

状态 L state L

低电平状态。根据 IC 卡中的逻辑约定，可以是逻辑 1 或逻辑 0。

4 符号和缩略语

下列符号和缩略语适用于本文件。

AAC	应用认证密文(Application Authentication Cryptogram)
AAR	应用授权参考(Application Authorization Referral)
AC	应用密文(Application Cryptogram)
ACK	确认(Acknowledgment)
ADA	应用缺省行为(Application Default Action)
ADF	应用数据文件(Application Definition File)
AEF	应用基本文件(Application Elementary File)

AFL	应用文件定位器(Application File Locator)
AID	应用标识符(Application Identifier)
AIP	应用交互特征(Application Interchange Profile)
APDU	应用协议数据单元(Application Protocol Data Unit)
ARPC	授权响应密文(Authorization Response Cryptogram)
ARQC	授权请求密文(Authorization Request Cryptogram)
ATC	应用交易序号(Application Transaction Counter)
ATM	自动柜员机(Automated Teller Machine)
ATR	复位应答(Answer to Reset)
AUC	应用用途控制(Application Usage Control)
BER	基本编码规则(Basic Encoding Rules)
BGT	块保护时间(Block Guard Time)
BWI	块等待时间整数(Block Waiting Time Integer)
BWT	块等待时间(Block Waiting Time)
CA	认证中心(Certificate Authority)
CAM	联机卡片认证(Card Authentication Method)
CDA	复合动态数据认证/应用密文生成
CDOL	卡片风险管理数据对象列表(Card Risk Management Data Object List)
CID	密文信息数据(Cryptogram Information Data)
CLA	命令报文的类别字节(Class Byte of the Command Message)
CLK	时钟(CLK)
Cn	压缩数字格式(Compress Numeric)
C-TPDU	命令 TPDU(Command TPDU)
CVM	持卡人验证方法(Cardholder Verification Method)
CVR	卡片验证结果(Card Verification Results)
CWI	字符等待时间整数(Character Waiting Time Integer)
CWT	字符等待时间(Character Waiting Time)
DAD	目标节点地址(Destination Node Address)
DC	直流(Direct Current)
DDA	动态数据认证(Dynamic Data Authentication)
DDOL	动态数据认证数据对象列表(Dynamic Data Authentication Data Object List)
DF	专用文件(Dedicated File)
DIR	目录(Directory)
DOL	数据对象列表(Data Object List)
EDC	错误检测代码(Error Detection Code)
EF	基本文件(Elementary File)
EMV	Europay MasterCard VISA
etu	基本时间单元(Elementary Time Unit)
FCI	文件控制信息(File Control Information)
GND	地(Ground)
GPO	获取处理选项(GET PROCESSING OPTIONS)
IAC	发卡行行为代码(Issuer Action Code)

IC	集成电路(Integrated Circuit)
ICC	集成电路卡(Integrated Circuit Card)
ICS	功能一致性声明(Implementation Conformance Statement)
IEC	国际电工委员会(International Electrotechnical Commission)
IFD	接口设备(Interface Device)
IFM	接口模块(Interface Module)
IFS	信息域大小(Information Field Size)
IFSC	IC 卡信息域大小(Information Field Size for the ICC)
IFSD	终端信息域大小(Information Field Size for the Terminal)
IFSI	信息域大小整数(Information Field Size Integer)
IIH	高电平输入电流(High Level Input Current)
IIL	低电平输入电流(Low Level Input Current)
INF	信息域(Information Field)
INS	命令报文的指令字节(Instruction Byte of Command Message)
I/O	输入/输出(Input/Output)
IOH	高电平输出电流(High Level Output Current)
IOL	低电平输出电流(Low Level Output Current)
ISO	国际标准化组织(International Organization for Standardization)
k Ω	千欧
Lc	终端应用层(TAL)在情况3或情况4命令中发出数据的实际长度(Exact Length of Data Sent by the TAL in a Case 3 or 4 Command)
LCOL	连续脱机交易下限
Le	在情况2或情况4命令中返回给终端应用层(TAL)的数据最大期望长度(Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command)
LEN	长度(Length)
Licc	IC卡在响应接收到的情况2或情况4命令时卡内有效或剩余的数据(由IC卡决定)的实际长度(Exact Length of Data Available in the ICC to be Returned in Response to the Case 2 or 4 Command Received by the ICC)
LOATC	上次联机交易计数器
Lr	响应数据域的长度(Length of Response Data Field)
LRC	冗余校验(Longitudinal Redundancy Check)
l. s.	最低位
M	必备(Mandatory)
mA	毫安
MAC	报文认证码(Message Authentication Code)
MDK	主密钥(Master DEA Key)
MF	主文件(Master File)
MHz	兆赫
m. s.	最高位
m Ω	毫欧

MΩ	兆欧
N	数字型(Numeric)
NAD	节点地址(Node Address)
NAK	否定的确认(Negative Acknowledgment)
nAs	纳安秒
ns	纳秒
O	可选(Optional)
P1	参数 1(Parameter 1)
P2	参数 2(Parameter 2)
P3	参数 3(Parameter 3)
PAN	主账号(Primary Account Number)
PBOC	中国人民银行(People's Bank of China)
PCB	协议控制字节(Protocol Control Byte)
pF	皮法
PKI	公钥基础设施(Public Key Infrastructure)
PIN	个人密码(Personal Identification Number)
PIX	专用应用标识符扩展(Proprietary Application Identifier Extension)
PTS	协议类型选择(Protocol Type Selection)
R-block	接收就绪块(Receive Ready Block)
RFU	保留(Reserved for Future Use)
RID	注册应用提供商标签(Registered Application Provider Identifier)
RST	复位(Reset)
R-TPDU	响应 TPDU(Response TPDU)
SAD	签名的静态应用数据(Signed Static Application Data)
SDA	静态数据认证(Static Data Authentication)
SFI	短文件标签符(Short File Identifier)
SW1	状态字 1(Status Word One)
SW2	状态字 2(Status Word Two)
TAC	终端行为代码(Terminal Action Code)
TAL	终端应用层(Terminal Application Layer)
TC	交易证书(Transaction Certificate)
TCK	校验字符(Check Character)
TDOL	交易证书数据对象列表(Transaction Certificate Data Object List)
tF	信号幅度从 90%下降到 10%的时间(Fall Time Between 90% and 10% of Signal Amplitude)
TLV	标签、长度、值(Tag Length Value)
TPDU	传输协议数据单元(Transport Protocol Data Unit)
tPX	电压(Vcc 或者信号)测量的 x 时间段(Time period x over which a voltage(Vcc or signal)is monitored)
tR	信号幅度从 10%上升到 90%的时间(Rise Time Between 10% and 90% of Signal Amplitude)
TSI	交易状态信息(Transaction Status Information)
TTL	终端传输层(Terminal Transport Layer)

TVR	终端验证结果(Terminal Verification Results)
UDK	子密钥(Unique DEA Key)
UCOL	连续脱机交易上限
V	伏特(Volt)
V _{CC}	VCC 触点上的测得电压(Voltage Measured on VCC Contact)
VCC	电源电压(Supply Voltage)
V _{IH}	高电平输入电压(High Level Input Voltage)
V _{IL}	低电平输入电压(Low Level Input Voltage)
V _{I/O}	I/O 触点上的测得电压(Voltage Measured on I/O Contact)
V _{OH}	高电平输出电压(High Level Output Voltage)
V _{OL}	低电平输出电压(Low Level Output Voltage)
V _{PP}	VCC 触点上的测得电压(Voltage measured on VPP contact)
VPP	编程电压(Programming Voltage)
V _{RST}	RST 触点上的测得电压(Voltage measured on RST contact)
WI	等待时间整数(Waiting Time Integer)
WTX	等待时间扩展(Waiting Time Extension)
专用的	本规范内未定义或/和超出本规范范围的

5 总体要求

电特性和通讯协议是卡片与受理设备交互的基础，只有电特性和通讯协议正确，卡片才可以正常与受理设备交互。本部分第6章为对电特性和通讯协议的测试案例，不论是支持借记贷记应用的卡片，还是支持基于借记贷记应用的小额支付的卡片，都应通过第6章的测试案例的检测。

第7章是针对卡片中借记贷记应用的测试案例，支持借记贷记应用的卡片应通过这些案例的检测。

第8章是针对卡片中基于借记贷记的小额支付应用的测试案例，支持基于借记贷记的小额支付应用的卡片应通过这些案例的检测。

在进行第6章、第7章和第8章的案例测试时，需要将不同的数据个人化至卡片以实现不同的测试点，第9章规定了这些个人化数据。

6 电特性和通讯协议的测试案例

6.1 一般要求

默认环境条件（温度，湿度等）是指常温 $20\pm 3^{\circ}\text{C}$ ，湿度20%-80%之间。如无特殊说明，后续案例均采用此环境条件。

表1中的这些条件是依照功能一致性声明中的信息设置的，或是在某些特定测试中执行的，这些条件决定了其余测试案例是否适用。如果IC卡期望的条件不是功能一致性声明中指明的，那么测试工具会在整个测试过程中发出一个警告（例如：如果测试工具必须要使用链接，而条件12=“终端不会发起链接”）。

表1 测试案例条件

条件号	条件内容	相反条件内容	在案例中分布
条件1	“接受冷复位ATR”	“没有有效的冷复位ATR”	

条件2	“接受热复位ATR”	“没有有效的热复位ATR”	
条件3	“冷复位ATR为基本ATR”	“冷复位ATR为符合EMV规范的ATR”； “冷复位ATR既不是基本ATR也不是符合EMV规范的ATR”	
条件4	“T=0协议”	“T=1协议”； “其他未知协议”	
条件5	“T=0协议”	“T=1协议”； “其他未知协议”	
条件6	“支持类型C”	“不支持类型C”	参见功能一致性声明
条件7	“没有S（WTX）块”	“可能有S（WTX）块”	参见功能一致性声明
条件8	“IFSC=254”	“IFSC<254”	参见功能一致性声明
条件9	“支持DDA”	“不支持DDA”	参见功能一致性声明
条件10	“支持密文PIN”	“不支持密文PIN”	参见功能一致性声明
条件11	“有卡片发起的链接”	“没有卡片发起的链接”	参见功能一致性声明
条件12	“有终端发起的链接”	“没有终端发起的链接”	参见功能一致性声明
条件13	“使用过程字节‘60’”	“不使用过程字节‘60’”	参见功能一致性声明

6.2 电特性测试（TPSB）

6.2.1 TPSB001-00

测试目的：当供给电压和输入信号在允许的范围内变化时，确保 IC 卡能够正确操作。

测试条件：——表 2 描述了测试组合条件；

——表 3 描述了类型 A 的电特性测试参数。

测试流程：a) 发起冷复位并接收冷复位 ATR；

b) 如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR；

c) 执行一个完整的流程；

d) 在高温和低温下重复该测试所有子案例。

通过标准：ATR 和响应值符合功能一致性声明，Vcc 供给电流 $\leq 50\text{mA}$ （ $\pm 1\text{mA}$ ）。

表2 组合条件

序号	条件
1	典型的常规平均条件
2	最小时钟频率
3	最大时钟频率
4	最小占空比
5	最大占空比
6	最低供电电压加最小信号幅度
7	最高供电电压加最大信号幅度
8	在最大时钟频率下减缓上升和下降时间
9	在最大时钟频率，最小信号幅度下减缓上升和下降时间
10	在最小时钟频率，最小信号幅度下减缓上升和下降时间
11	最高供电电压加最小信号幅度

表3 电特性测试参数（类型 A）

触点	属性	数值	测试序号										
			1	2	3	4	5	6	7	8	9	10	11
VCC	电压	5V(±25mV)	✓	✓	✓	✓	✓			✓			
		4.5V(±25mV)						✓			✓	✓	
		5.5V(±25mV)							✓				✓
CLK	频率	2.5MHZ(±0.1%)	✓			✓	✓	✓	✓				✓
		1MHZ(±0.1%)		✓								✓	
		5MHZ(±0.1%)			✓					✓	✓		
	占空比	50%(±0.5%)	✓	✓	✓			✓	✓				✓
		44%(±0.5%)				✓				✓	✓	✓	
		56%(±0.5%)					✓						
	VIH	4.5V(±25mV)	✓	✓	✓	✓	✓			✓			
		3.15V(±25mV)						✓			✓	✓	
		5.5V(±25mV)							✓				
		3.85V(±25mV)											✓
CLK	VIL	0.5V(±25mV)	✓	✓	✓	✓	✓			✓			
		0V(±25mV)							✓				
		0.9V(±25mV)						✓			✓	✓	
		1.1V(±25mV)											✓
	tR & tF	<18ns	✓	✓	✓	✓	✓	✓	✓				✓
		18ns(±1ns)								✓	✓		
		90ns(±1ns)										✓	
RST	VIH	4.5V(±25mV)	✓	✓	✓	✓	✓			✓			
		3.15V(±25mV)						✓			✓	✓	
		5.5V(±25mV)							✓				
		3.85V(±25mV)											✓
	VIL	0.5V(±25mV)	✓	✓	✓	✓	✓			✓			
		0V(±25mV)							✓				
		0.9V(±25mV)						✓			✓	✓	
		1.1V(±25mV)											✓
	tR & tF	<50ns	✓	✓	✓	✓	✓	✓	✓				✓
		1μs(±10ns)								✓	✓	✓	

表 3 (续)

触点	属性	数值	测试序号										
			1	2	3	4	5	6	7	8	9	10	11
I/O	VIH	4.5V(±25mV)	✓	✓	✓	✓	✓			✓			
		3.15V(±25mV)						✓			✓	✓	
		5.5V(±25mV)							✓				
		3.85V(±25mV)											✓
	VIL	0.5V(±25mV)	✓	✓	✓	✓	✓			✓			
		0V(±25mV)							✓				
		0.9V(±25mV)						✓			✓	✓	
		1.1V(±25mV)											✓
	tR & tF	<50ns	✓	✓	✓	✓	✓	✓	✓				✓
		1μs(±10ns)								✓	✓	✓	

6.2.2 TPSB002-00

测试目的：当供给电压和输入信号在允许的范围内变化时，确保 IC 卡能够正确操作。

测试条件：——表 2 描述了测试组合条件；

——表 4 描述了类型 B 的电特性测试参数。

测试流程：a) 发起冷复位并接收冷复位 ATR；

b) 如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR；

c) 执行一个完整的流程；

d) 在高温和低温下重复该测试所有子案例。

通过标准：ATR 和响应值符合功能一致性声明，Vcc 供给电流≤50mA（±1mA）。

表4 电特性测试参数（类型 B）

触点	属性	数值	测试序号										
			1	2	3	4	5	6	7	8	9	10	11
VCC	电压	3V(±15mV)	✓	✓	✓	✓	✓			✓			
		2.7V(±15mV)						✓			✓	✓	
		3.3V(±15mV)							✓				✓
CLK	频率	2.5MHZ(±0.1%)	✓			✓	✓	✓	✓				✓
		1MHZ(±0.1%)		✓								✓	
		5MHZ(±0.1%)			✓					✓	✓		
	占空比	50%(±0.5%)	✓	✓	✓			✓	✓				✓
		44%(±0.5%)				✓				✓	✓	✓	
		56%(±0.5%)					✓						

表 4 (续)

触点	属性	数值	测试序号										
			1	2	3	4	5	6	7	8	9	10	11
CLK	VIH	2.7V(±15mV)	✓	✓	✓	✓	✓			✓			
		1.9V(±15mV)						✓			✓	✓	
		3.3V(±15mV)							✓				
		2.31 V(±15mV)											✓
	VIL	0.3V(±15mV)	✓	✓	✓	✓	✓			✓			
		0V(±15mV)							✓				
		0.54V(±15mV)						✓			✓	✓	
		0.6V(±15mV)											✓
	tR & tF	<50ns	✓	✓	✓	✓	✓	✓	✓				✓
		1 μ s(±10ns)								✓	✓		
RST	VIH	2.7V(±15mV)										✓	
		1.9V(±15mV)	✓	✓	✓	✓	✓			✓			
		3.3V(±15mV)						✓			✓	✓	
		2.31 V(±15mV)							✓				
	VIL	0.3V(±15mV)											✓
		0V(±15mV)	✓	✓	✓	✓	✓			✓			
		0.54V(±15mV)							✓				
		0.6V(±15mV)						✓			✓	✓	
	tR & tF	<50ns											✓
		1μs(±10ns)	✓	✓	✓	✓	✓	✓	✓				✓
I/O	VIH	2.7V(±15mV)								✓	✓	✓	
		1.9V(±15mV)	✓	✓	✓	✓	✓			✓			
		3.3V(±15mV)						✓			✓	✓	
		2.31 V(±15mV)							✓				
	VIL	0.3V(±15mV)											✓
		0V(±15mV)	✓	✓	✓	✓	✓			✓			
		0.54V(±15mV)							✓				
		0.6V(±15mV)						✓			✓	✓	
	tR & tF	<50ns											✓
		1μs(±10ns)	✓	✓	✓	✓	✓	✓	✓				✓

6.2.3 TPSB003-00

测试目的：当供给电压和输入信号在允许的范围内变化时，确保 IC 卡能够正确操作。

测试条件：——表 2 描述了测试组合条件；

——表 5 描述了类型 C 的电特性测试参数；

条件 6 为“支持类型 C”。

测试流程：a) 发起冷复位并接收冷复位 ATR；

b) 如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR；

c) 执行一个完整的流程；

d) 在高温和低温下重复该测试所有子案例。

通过标准：ATR 和响应值符合功能一致性声明，Vcc 供给电流 $\leq 30\text{mA}$ （精确度 $\pm 50\mu\text{A}$ ）。

表5 电特性测试参数（类型 C）

触点	属性	数值	测试序号										
			1	2	3	4	5	6	7	8	9	10	11
VCC	电压	1.80V($\pm 9\text{mV}$)	✓	✓	✓	✓	✓			✓			
		1.62V($\pm 9\text{mV}$)						✓			✓	✓	
		1.98V($\pm 9\text{mV}$)							✓				✓
CLK	频率	2.5MHZ($\pm 0.1\%$)	✓			✓	✓	✓	✓				✓
		1MHZ($\pm 0.1\%$)		✓								✓	
		5MHZ($\pm 0.1\%$)			✓					✓	✓		
	占空比	50%($\pm 0.5\%$)	✓	✓	✓			✓	✓				✓
		44%($\pm 0.5\%$)				✓				✓	✓	✓	
		56%($\pm 0.5\%$)					✓						
	VIH	1.62V($\pm 9\text{mV}$)	✓	✓	✓	✓	✓			✓			
		1.14V($\pm 9\text{mV}$)						✓			✓	✓	
		1.98V($\pm 9\text{mV}$)							✓				
		1.39V($\pm 9\text{mV}$)											✓
	VIL	0.16V($\pm 9\text{mV}$)	✓	✓	✓	✓	✓			✓			
		0.00V($\pm 9\text{mV}$)							✓				
		0.32V($\pm 9\text{mV}$)						✓			✓	✓	
		0.40V($\pm 9\text{mV}$)											✓
	tR & tF	<18ns	✓	✓	✓	✓	✓	✓	✓				✓
		18ns($\pm 1\text{ns}$)								✓	✓		
		90ns($\pm 1\text{ns}$)										✓	

表 5 (续)

触点	属性	数值	测试序号										
			1	2	3	4	5	6	7	8	9	10	11
RST	VIH	1.62V(±9mV)	✓	✓	✓	✓	✓			✓			
		1.14V(±9mV)						✓			✓	✓	
		1.98V(±9mV)							✓				
		1.39V(±9mV)											✓
	VIL	0.16V(±9mV)	✓	✓	✓	✓	✓			✓			
		0.00V(±9mV)							✓				
		0.32V(±9mV)						✓			✓	✓	
		0.40V(±9mV)											✓
	tR & tF	<50ns	✓	✓	✓	✓	✓	✓	✓				✓
		1μs(±10ns)								✓	✓	✓	
I/O	VIH	1.62V(±9mV)	✓	✓	✓	✓	✓			✓			
		1.14V(±9mV)						✓			✓	✓	
		1.98V(±9mV)							✓				
		1.39V(±9mV)											✓
	VIL	0.16V(±9mV)	✓	✓	✓	✓	✓			✓			
		0.00V(±9mV)							✓				
		0.32V(±9mV)						✓			✓	✓	
		0.40V(±9mV)											✓
	tR & tF	<50ns	✓	✓	✓	✓	✓	✓	✓				✓
		1μs(±10ns)								✓	✓	✓	

6.2.4 TPSB004-00

测试目的：确保在不支持的类型下操作，IC 卡不会损坏。

测试条件：条件 6 为“不支持类型 C”。

测试流程：a) 在类型 B 的设置下，发起冷复位，期待收到冷复位 ATR，执行一个完整的流程，假设 IC 卡没有返回或返回错误的 ATR，也要发送所有命令头来继续交易，释放所有触点，在高温和低温下重复该测试；
 b) 在类型 B 的设置下，发起冷复位，期待收到冷复位 ATR，执行一个完整的流程，假设 IC 卡没有返回或返回错误的 ATR，也要发送所有命令头来继续交易，释放所有触点，在高温和低温下重复该测试；
 c) 在类型 A 的设置下，发起冷复位，期待收到冷复位 ATR，执行一个完整的流程，假设 IC 卡没有返回或返回错误的 ATR，也要发送所有命令头来继续交易，释放所有触点，在高温和低温下重复该测试。

通过标准：IC 卡在类型 B 设置下的流程中能处理所有命令，并能按照功能一致性声明的指定内

容返回响应；IC卡在类型A设置下的流程中能处理所有命令，并能按照功能一致性声明的指定内容返回响应。

6.2.5 TPSB005-00

测试目的：确保当IC卡和终端同时处于发送模式时，IC卡不会损坏。

测试条件：无。

测试流程：a)发起冷复位并接收冷复位ATR，如果条件1为“没有有效的冷复位ATR”，那么发起热复位并接收热复位ATR，初始流程，当IC卡返回至少10字节的响应时，将I/O电平拉低（0V）并持续相当于这10字节传输的时间，然后终止流程，在高温和低温下重复该测试；
b)发起冷复位并接收冷复位ATR，如果条件1为“没有有效的冷复位ATR”，那么发起热复位并接收热复位ATR，初始流程，当IC卡返回至少10字节的响应时，将I/O电平拉高（VCC）并持续相当于这10字节传输的时间，然后终止流程，在高温和低温下重复该测试；
c)发起冷复位并接收冷复位ATR，如果条件1为“没有有效的冷复位ATR”，那么发起热复位并接收热复位ATR，初始流程，执行一个完整且正常的流程，在高温和低温下重复该测试。

通过标准：在第三个正常的流程中，所有ATR和响应都应与功能一致性声明对应。

6.2.6 TPSB006-00

测试目的：确保I/O信号的高低电平在允许的范围内。

测试条件：无。

测试流程：a)设置VCC=4.5V±25mV，发起冷复位并接收冷复位ATR，如果条件1为“没有有效的冷复位ATR”，那么发起热复位并接收热复位ATR，执行一个完整的流程，流程期间，对IC卡响应返回数据位的I/O高电平和低电平进行监控（包括停止位），至少要监控一个命令情况2、一个命令情况3和一个命令情况4，在高温和低温下重复该测试所有子案例；
b)设置VCC=5.0V±25mV，发起冷复位并接收冷复位ATR，如果条件1为“没有有效的冷复位ATR”，那么发起热复位并接收热复位ATR，执行一个完整的流程，流程期间，对IC卡响应返回数据位的I/O高电平和低电平进行监控（包括停止位），至少要监控一个命令情况2、一个命令情况3和一个命令情况4，在高温和低温下重复该测试所有子案例；
c)设置VCC=5.5V±25mV，发起冷复位并接收冷复位ATR，如果条件1为“没有有效的冷复位ATR”，那么发起热复位并接收热复位ATR，执行一个完整的流程，流程期间，对IC卡响应返回数据位的I/O高电平和低电平进行监控（包括停止位），至少要监控一个命令情况2、一个命令情况3和一个命令情况4，在高温和低温下重复该测试所有子案例。

通过标准：IC卡在发送模式下，I/O高电平信号应满足： $(0.7 * VCC) - 25mV \leq VOH \leq VCC + 25mV$ ；IC卡在发送模式下，I/O低电平信号应满足： $0V - 25mV \leq VOL \leq (0.08 * VCC) + 25mV$ 。

6.2.7 TPSB007-00

测试目的：确保I/O信号的高低电平在允许的范围内。

测试条件：无。

测试流程：a) 设置 $VCC=2.7V \pm 15mV$ ，发起冷复位并接收冷复位 ATR，如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，流程期间，对 IC 卡响应返回数据位的 I/O 高电平和低电平进行监控（包括停止位），至少要监控一个命令情况 2、一个命令情况 3 和一个命令情况 4，在高温和低温下重复该测试所有子案例；

b) 设置 $VCC=3.0V \pm 15mV$ ，发起冷复位并接收冷复位 ATR，如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，流程期间，对 IC 卡响应返回数据位的 I/O 高电平和低电平进行监控（包括停止位），至少要监控一个命令情况 2、一个命令情况 3 和一个命令情况 4，在高温和低温下重复该测试所有子案例；

c) 设置 $VCC=3.3V \pm 15mV$ ，发起冷复位并接收冷复位 ATR，如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，流程期间，对 IC 卡响应返回数据位的 I/O 高电平和低电平进行监控（包括停止位），至少要监控一个命令情况 2、一个命令情况 3 和一个命令情况 4，在高温和低温下重复该测试所有子案例。

通过标准：IC 卡在发送模式下，I/O 高电平信号应满足： $(0.7 * VCC) - 15mV \leq VOH \leq VCC + 15mV$ ；IC 卡在发送模式下，I/O 低电平信号应满足： $0V - 15mV \leq VOL \leq (0.15 * VCC) + 15mV$ 。

6.2.8 TPSB008-00

测试目的：确保 I/O 信号的高低电平在允许的范围内。

测试条件：条件 6 为“支持类型 C”。

测试流程：a) 设置 $VCC=1.62V \pm 9mV$ ，发起冷复位并接收冷复位 ATR，如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，流程期间，对 IC 卡响应返回数据位的 I/O 高电平和低电平进行监控（包括停止位），至少要监控一个命令情况 2、一个命令情况 3 和一个命令情况 4，在高温和低温下重复该测试所有子案例；

b) 设置 $VCC=1.80V \pm 9mV$ ，发起冷复位并接收冷复位 ATR，如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，流程期间，对 IC 卡响应返回数据位的 I/O 高电平和低电平进行监控（包括停止位），至少要监控一个命令情况 2、一个命令情况 3 和一个命令情况 4，在高温和低温下重复该测试所有子案例；

c) 设置 $VCC=1.98V \pm 9mV$ ，发起冷复位并接收冷复位 ATR，如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，流程期间，对 IC 卡响应返回数据位的 I/O 高电平和低电平进行监控（包括停止位），至少要监控一个命令情况 2、一个命令情况 3 和一个命令情况 4，在高温和低温下重复该测试所有子案例。

通过标准：IC 卡在发送模式下，I/O 高电平信号应满足： $(0.7 * VCC) - 9mV \leq VOH \leq VCC + 9mV$ ；IC 卡在发送模式下，I/O 低电平信号应满足如下特征： $0V - 9mV \leq VOL \leq (0.15 * VCC) + 9mV$ 。

6.2.9 TPSB009-00

测试目的：确保 I/O 信号的上升时间和下降时间在允许的范围。

测试条件：无。

测试流程：a) 设置 $VCC=4.5V \pm 25mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例；
b) 设置 $VCC=5.0V \pm 25mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例；
c) 设置 $VCC=5.5V \pm 25mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例。

通过标准： $t_R \leq 1.0\mu s + 20ns$ ， $t_F \leq 1.0\mu s + 20ns$ 。

6.2.10 TPSB010-00

测试目的：确保 I/O 信号的上升时间和下降时间在允许的范围。

测试条件：无。

测试流程：a) 设置 $VCC=2.7V \pm 15mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例；
b) 设置 $VCC=3.0V \pm 15mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例；
c) 设置 $VCC=3.3V \pm 15mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例。

通过标准： $t_R \leq 1.0\mu s + 20ns$ ， $t_F \leq 1.0\mu s + 20ns$ 。

6.2.11 TPSB011-00

测试目的：确保 I/O 信号的上升时间和下降时间在允许的范围。

测试条件：条件 6 为“支持类型 C”。

测试流程：a) 设置 $VCC=1.62V \pm 9mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输

期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例；

- b) 设置 $VCC=1.80V \pm 9mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例；
- c) 设置 $VCC=1.98V \pm 9mV$ ，发起冷复位并接收冷复位 ATR，在冷复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，如果条件 2 为“接受热复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，在热复位 ATR 的字符帧传输期间，测量 I/O 信号上升沿 10%到 90%的时间 t_R 和下降沿 90%到 10%的时间 t_F ，在高温和低温下重复该测试所有子案例。

通过标准： $t_R \leq 1.0\mu s + 20ns$ ， $t_F \leq 1.0\mu s + 20ns$ 。

6.2.12 TPSB012-00

测试目的：确保 I/O 电平在 $-0.3V$ 到 $VCC + 0.3V$ 的范围内抖动，IC 卡不会损坏。

测试条件：无。

测试流程：a) 发起冷复位并接收冷复位 ATR；

- b) 如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR；
- c) 按照测试工具对本案例在 I/O 信号电平上的设置执行一个完整的流程；
- d) 无论 IC 卡没有返回或返回错误的 ATR，也要发送所有命令头来继续交易；
- e) 释放触点，测试工具对 I/O 信号电平的设置返回正常状态；
- f) 再次发起冷复位并接收冷复位 ATR；
- g) 如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR；
- h) 执行一个完整的流程；
- i) 在高温和低温下重复该测试。

通过标准：在正常 I/O 设置的第二个流程中，IC 卡正确处理所有命令并按照功能一致性声明的指定内容返回响应。

6.2.13 TPSB013-00

测试目的：确保 CLK 电平在 $-0.3V$ 到 $VCC + 0.3V$ 的范围内抖动，IC 卡不会损坏。

测试条件：无。

测试流程：a) 发起冷复位并接收冷复位 ATR；

- b) 如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR；
- c) 按照测试工具对本案例在 CLK 信号电平上的设置执行一个完整的流程；
- d) 无论 IC 卡没有返回或返回错误的 ATR，也要发送所有命令头来继续交易或是在释放触点之前等待一个相同的时间；
- e) 释放触点，测试工具对 CLK 信号电平的设置返回正常状态；
- f) 再次发起冷复位并接收冷复位 ATR；
- g) 如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR；
- h) 执行一个完整的流程；

i) 在高温和低温下重复该测试。

通过标准：在正常 CLK 设置的第二个流程中，IC 卡正确处理所有命令并按照功能一致性声明的指定内容返回响应。

6.2.14 TPSB014-00

测试目的：确保 RST 电平在 $-0.3V$ 到 $VCC + 0.3V$ 的范围内抖动，IC 卡不会损坏。

测试条件：无。

测试流程：a) 设置测试工具对本案例在 RST 信号电平上的参数；

b) 发起冷复位；

c) 期望接收到冷复位 ATR，如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR，执行一个完整的流程，实际上无论 IC 卡没有返回或返回错误的 ATR，也要发送所有命令头来继续交易或是在释放触点之前等待一个相同的时间；

d) 释放触点，测试工具对 RST 信号电平的设置返回正常状态；

e) 再次发起冷复位并接收冷复位 ATR；

f) 如果条件 1 为“没有有效的冷复位 ATR”，那么发起热复位并接收热复位 ATR；

g) 执行一个完整的流程；

h) 在高温和低温下重复该测试。

通过标准：在正常 RST 设置的第二个流程中，IC 卡正确处理所有命令并按照功能一致性声明的指定内容返回响应。

6.2.15 TPSB015-00

测试目的：确保当终端处于高电平传输过程和低电平传输过程时，IC 卡不会导致流入 IC 卡 I/O 管道的电流超过限定的范围。

测试条件：无。

测试流程：a) $VCC=5.0V \pm 25mV$ ，卡片支持 T=0 协议，使用字节‘00’时，发起冷复位并接收冷复位 ATR，设置测试工具发送一个命令数据域为 16 个连续同样‘00’或‘FF’字节的“选择”命令，同时测量流入 IC 卡 I/O 管道的电流 $I_{I/O}$ ，在高温和低温下重复该测试；

b) $VCC=5.0V \pm 25mV$ ，卡片支持 T=0 协议，使用字节‘FF’时，发起冷复位并接收冷复位 ATR，设置测试工具发送一个命令数据域为 16 个连续同样‘00’或‘FF’字节的“选择”命令，同时测量流入 IC 卡 I/O 管道的电流 $I_{I/O}$ ，在高温和低温下重复该测试；

c) $VCC=5.0V \pm 25mV$ ，卡片支持 T=1 协议，使用字节‘00’，设置测试工具发送一个命令数据域长度等于 (IFSC-6) 且数据是连续同样‘00’或‘FF’字节的“选择”命令，同时测量流入 IC 卡 I/O 管道的电流 $I_{I/O}$ ，在高温和低温下重复该测试；

d) $VCC=5.0V \pm 25mV$ ，卡片支持 T=1 协议，使用字节‘FF’，设置测试工具发送一个命令数据域长度等于 (IFSC-6) 且数据是连续同样‘00’或‘FF’字节的“选择”命令，同时测量流入 IC 卡 I/O 管道的电流 $I_{I/O}$ ，在高温和低温下重复该测试。

通过标准：处于高电平 V_{OH} 时： $I_{I/O} \leq 20\mu A + 2\mu A$ ；处于低电平 V_{OL} 时： $I_{I/O} \leq 500\mu A + 50\mu A$ 。

6.2.16 TPSB016-00

测试目的：确保 IC 卡不会导致 CLK 管道上任何流向的电流超过限定的范围。

测试条件：无。

测试流程：a) 在 $VCC=5.0V \pm 25mV$ ；
 b) 发起冷复位并接收冷复位 ATR；
 c) 设置测试工具保持CLK处在高电平 $VOH=VCC$ ，同时测量流入IC卡CLK管道的电流 I_{CLK} ；
 d) 设置测试工具保持CLK处在低电平 $VOL=0V$ ，同时测量流出IC卡CLK管道的电流 I_{CLK} ；
 e) 在高温和低温下重复该测试。

通过标准：处于高电平 VOH 时： $I_{CLK} \leq 50\mu A + 5\mu A$ ；处于低电平 VOL 时： $I_{CLK} \leq 50\mu A + 5\mu A$ 。

6.2.17 TPSB017-00

测试目的：确保 IC 卡不会导致 RST 管道上任何流向的电流超过限定的范围。

测试条件：无。

测试流程：a) 在 $VCC=5.0V \pm 25mV$ ；
 b) 发起冷复位并接收冷复位 ATR；
 c) 设置测试工具保持RST处在高电平 $VOH=VCC$ ，同时测量流入IC卡RST管道的电流 I_{RST} ；
 d) 设置测试工具保持RST处在低电平 $VOL=0V$ ，同时测量流出IC卡RST管道的电流 I_{RST} ；
 e) 在高温和低温下重复该测试。

通过标准：处于高电平 VOH 时： $I_{RST} \leq 50\mu A + 5\mu A$ ；处于低电平 VOL 时： $I_{RST} \leq 50\mu A + 5\mu A$ 。

6.3 卡片会话测试 (TPSC)

6.3.1 TPSC001-00

测试目的：确保 IC 卡在触点激活时序过程中正确控制 I/O 信号电平。

测试条件：无。

测试流程：a) 按照表 6 设置测试工具的 CLK 频率、VCC 和 RST 时间；
 b) 发起冷复位；
 c) 监测从 CLK 开始到 RST 置为高电平 (t_{p1}) 后的 200 CLK 周期起的 $V_{I/O}$ ；
 d) 接收冷复位 ATR；
 e) 如果条件 2 为“接收热复位 ATR”，那么发起热复位，监测 RST 置为低电平又再次置为高电平 (t_{p2}) 后的 200 CLK 周期起的 $V_{I/O}$ ，接收热复位 ATR；
 f) 在高温和低温下重复该测试所有子案例。

通过标准： t_{p1} 期间的I/O电平应满足： $(0.8 * VCC) - 25mV \leq V_{I/O} \leq VCC + 25mV$ ，冷复位 ATR的内容与功能一致性声明相对应；如果条件2为“接受热复位ATR”，那么 t_{p2} 期间的I/O电平应满足： $(0.8 * VCC) - 25mV \leq V_{I/O} \leq VCC + 25mV$ ，热复位ATR的内容与功能一致性声明相对应。

表6 CLK 频率、VCC 电压和对 RST 时间的控制

子案例			VCC电压	冷热复位后RST 拉高时间
CLK频率3.5MHz	CLK频率1MHz	CLK频率5MHz		
01	07	13	5.0V ± 25mV	40000 CLK周期
02	08	14		45000 CLK周期
03	09	15	4.5V ± 25mV	40000 CLK周期
04	10	16		45000 CLK周期
05	11	17	5.5V ± 25mV	40000 CLK周期
06	12	18		45000 CLK周期

6.3.2 TPSC002-00

测试目的：确保 IC 卡在触点激活时序过程中正确控制 I/O 信号电平。

测试条件：无。

测试流程：a) 按照表 7 设置测试工具的 CLK 频率、VCC 和 RST 时间；
 b) 发起冷复位；
 c) 监测从 CLK 开始到 RST 置为高电平 (t_{p1}) 后的 200 CLK 周期起的 $V_{I/O}$ ；
 d) 接收冷复位 ATR；
 e) 如果条件 2 为“接收热复位 ATR”，那么发起热复位，监测 RST 置为低电平又再次置为高电平 (t_{p2}) 后的 200 CLK 周期起的 $V_{I/O}$ ，接收热复位 ATR；
 f) 在高温和低温下重复该测试所有子案例。

通过标准： t_{p1} 期间的I/O电平应满足： $(0.8 * VCC) - 15mV \leq V_{I/O} \leq VCC + 15mV$ ，冷复位ATR的内容与功能一致性声明相对应；如果条件2为“接受热复位ATR”，那么 t_{p2} 期间的I/O电平应满足： $(0.8 * VCC) - 15mV \leq V_{I/O} \leq VCC + 15mV$ ，热复位ATR的内容与功能一致性声明相对应。

表7 CLK 频率、VCC 电压和对 RST 时间的控制

子案例			VCC电压	冷热复位后RST 拉高时间
CLK频率3.5MHz	CLK频率1MHz	CLK频率5MHz		
01	07	13	3.0V±15mV	40000 CLK周期
02	08	14		45000 CLK周期
03	09	15	2.7V±15mV	40000 CLK周期
04	10	16		45000 CLK周期
05	11	17	3.3V±15mV	40000 CLK周期
06	12	18		45000 CLK周期

6.3.3 TPSC003-00

测试目的：确保 IC 卡在触点激活时序过程中正确控制 I/O 信号电平。

测试条件：条件 6 为“支持类型 C”。

测试流程：a) 按照表 8 设置测试工具的 CLK 频率、VCC 和 RST 时间；
 b) 发起冷复位；
 c) 监测从 CLK 开始到 RST 置为高电平 (t_{p1}) 后的 200 CLK 周期起的 $V_{I/O}$ ；
 d) 接收冷复位 ATR；
 e) 如果条件 2 为“接收热复位 ATR”，那么发起热复位，监测 RST 置为低电平又再次置为高电平 (t_{p2}) 后的 200 CLK 周期起的 $V_{I/O}$ ，接收热复位 ATR；
 f) 在高温和低温下重复该测试所有子案例。

通过标准： t_{p1} 期间的I/O电平应满足： $(0.8 * VCC) - 9mV \leq V_{I/O} \leq VCC + 9mV$ ，冷复位ATR的内容与功能一致性声明相对应；如果条件2为“接受热复位ATR”，那么 t_{p2} 期间的I/O电平应满足： $(0.8 * VCC) - 9mV \leq V_{I/O} \leq VCC + 9mV$ ，热复位ATR的内容与功能一致性声明相对应。

表8 CLK 频率、VCC 电压和对 RST 时间的控制

子案例			VCC电压	冷热复位后RST 拉高时间
CLK频率3.5MHz	CLK频率1MHz	CLK频率5MHz		
01	07	13	1.80V±9mV	40000 CLK周期
02	08	14		45000 CLK周期
03	09	15	1.62V±9mV	40000 CLK周期

04	10	16		45000 CLK周期
05	11	17	1. 98V±9mV	40000 CLK周期
06	12	18		45000 CLK周期

6.3.4 TPSC004-00

测试目的：确保 IC 卡从冷复位和热复位开始到返回 ATR 在指定的时间范围内。

测试条件：无。

测试流程：a) 设置 CLK 频率=3.5MHz，发起冷复位，测量从 RST 上升沿到冷复位 ATR 第一个字节的起始位下降沿的时间 (t_{p1})，如果条件 2 为“接受热复位 ATR”，那么允许冷复位 ATR 从 RST 的上升沿开始等待 22000 个初始 etu ($\pm 100\mu s$) 的时间，之后将 RST 置为低电平持续 42500 CLK 周期 ($\pm 100\mu s$)，然后将 RST 置为高电平来发起热复位，测量从 RST 上升沿到热复位 ATR 第一个字节的起始位下降沿的时间 (t_{p2})，在高温和低温下重复该测试所有子案例；

b) 设置 CLK 频率=1.0MHz，发起冷复位，测量从 RST 上升沿到冷复位 ATR 第一个字节的起始位下降沿的时间 (t_{p1})，如果条件 2 为“接受热复位 ATR”，那么允许冷复位 ATR 从 RST 的上升沿开始等待 22000 个初始 etu ($\pm 100\mu s$) 的时间，之后将 RST 置为低电平持续 42500 CLK 周期 ($\pm 100\mu s$)，然后将 RST 置为高电平来发起热复位，测量从 RST 上升沿到热复位 ATR 第一个字节的起始位下降沿的时间 (t_{p2})，在高温和低温下重复该测试所有子案例；

c) 设置 CLK 频率=5.0MHz，发起冷复位，测量从 RST 上升沿到冷复位 ATR 第一个字节的起始位下降沿的时间 (t_{p1})，如果条件 2 为“接受热复位 ATR”，那么允许冷复位 ATR 从 RST 的上升沿开始等待 22000 个初始 etu ($\pm 100\mu s$) 的时间，之后将 RST 置为低电平持续 42500 CLK 周期 ($\pm 100\mu s$)，然后将 RST 置为高电平来发起热复位，测量从 RST 上升沿到热复位 ATR 第一个字节的起始位下降沿的时间 (t_{p2})，在高温和低温下重复该测试所有子案例。

通过标准：IC 卡返回冷复位 ATR 的时间应满足： $400 \leq t_{p1} \leq 40000$ CLK 周期；如果条件 2 为“接受热复位 ATR”，那么 IC 卡返回热复位 ATR 的时间应满足： $400 \leq t_{p2} \leq 40000$ CLK 周期。

6.3.5 TPSC005-00

测试目的：确保当在一收到冷复位 ATR 中 T0 字符后的字符就拒绝冷复位 ATR 时，IC 卡正确发出热复位 ATR。

测试条件：条件 2 为“接受热复位 ATR”。

测试流程：a) 设置 CLK 频率=3.5MHz，发起冷复位并收到冷复位 ATR 的前两个字节，从冷复位 ATR 中 T0 字符的起始位下降沿起 12 个初始 etu ($0.0/+0.2$ etus)，此时发起热复位，接收热复位 ATR，在高温和低温下重复该测试所有子案例；

b) 设置 CLK 频率=1.0MHz，发起冷复位并收到冷复位 ATR 的前两个字节，从冷复位 ATR 中 T0 字符的起始位下降沿起 12 个初始 etu ($0.0/+0.2$ etus)，此时发起热复位，接收热复位 ATR，在高温和低温下重复该测试所有子案例；

c) 设置 CLK 频率=5.0MHz，发起冷复位并收到冷复位 ATR 的前两个字节，从冷复位 ATR 中 T0 字符的起始位下降沿起 12 个初始 etu ($0.0/+0.2$ etus)，此时发起热复位，接收热复位 ATR，在高温和低温下重复该测试所有子案例。

通过标准：热复位 ATR 的内容与功能一致性声明相对应。

6.4 ATR 和字符间时间间隔测试 (TPSE)

6.4.1 TPSE001-00

测试目的：确保冷复位返回的 ATR 满足 ICS 要求，并保证后续测试顺利进行。

测试条件：无。

测试流程：a) 启动冷复位并接收 ATR；
b) 比较冷复位 ATR 和 ICS 中声明的 ATR。

通过标准：冷复位 ATR 和 ICS 中声明的 ATR 内容一致。

6.4.2 TPSE002-00

测试目的：确保热复位返回的 ATR 满足 ICS 要求，并保证后续测试顺利进行。

测试条件：条件 2 为接受热复位 ATR。

测试流程：a) 启动冷复位并接收 ATR；
b) 启动热复位并接收 ATR；
c) 比较热复位 ATR 和 ICS 中声明的 ATR。

通过标准：热复位 ATR 和 ICS 中声明的 ATR 内容一致。

6.4.3 TPSE003-00

测试目的：确保 IC 卡能够按 ICS 中声明的要求，执行一个完整交易。这是一个测试前的准备，保证后续测试正常进行。

测试条件：无。

测试流程：a) 启动冷复位并接收 ATR；
b) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR；
c) 执行一个完整交易。

通过标准：IC 卡正确执行所有命令，并且和 ICS 中声明的一致。

6.4.4 TPSE004-00

测试目的：确保 IC 卡返回 ATR 的字符间隔时间满足规范要求。

测试条件：无。

测试流程：a) 启动冷复位并接收 ATR；
b) 测量 IC 卡返回的 ATR 所有字符的起始位下降沿之间的时间间隔 t_{P1} ；
c) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡返回 ATR 的字符间隔范围是 $12 \text{ etus} \leq t_{P1} \leq 9600 \text{ etus}$ 。

6.4.5 TPSE005-00

测试目的：确保 IC 卡返回 ATR 的时间在最大要求时间以内。

测试条件：无。

测试流程：a) 启动冷复位并接收 ATR；
b) 测量 IC 卡返回的第一个字符的起始位下降沿到最后一个字符的起始位下降沿的时间间隔 t_{P1} ；
c) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡返回 ATR 的时间 $t_{P1} \leq 19188 \text{ etus}$ (19188 是 19200 减去最少 12 个 etus 的时间)。

6.4.6 TPSE006-00

测试目的：确保 IC 卡返回的字符的位持续时间在许可范围内。

测试条件：无。

测试流程：a) 启动冷复位；
b) 接收冷复位 ATR 及所有字符，测量所有的起始位下降沿到相应位边界的时间 t_{pn} ($n=1$ 到 10)；
c) 继续全部交易；
d) 测量情况 2, 3, 4 下的所有命令字符的 t_{pn} 。

通过标准：IC 卡返回的所有字符的位持续时间 $t_{pn}=(n \pm 0.2) \text{ etus}$ 。

6.4.7 TPSE007-00

测试目的：确保 IC 卡正确解析并接收位持续时间在许可范围内变化的字符。

测试条件：无。

测试流程：a) 启动冷复位并接收 ATR；
b) 发送位持续时间变化的 SELECT 命令，或 S (IFS 请求) 块 (IFSD=254)；
c) 接收过程字或 S (IFS 响应) 块；
d) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡返回正确的状态字，或 S (IFS 响应) 块。

6.5 T=0 协议测试 (TPSF)

6.5.1 TPSF001-00

测试目的：确保 IC 卡发送的字符间的时间间隔满足最小为 12 etus，最大为 $(960 \times D \times WI) \text{ etus}$ (工作等待时间)。

测试条件：条件 4 或条件 5 为 T=0 协议。

测试流程：a) 启动冷复位并接收 ATR；
b) 完成 SELECT 命令处理过程，包括过程字节，GET RESPONSE 命令，FCI 数据和状态字；
c) 测量 IC 卡发送的连续同向字符起始位下降沿间的时间间隔 t_{P1} ；
d) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡发送的字符间的时间间隔范围是 $12 \text{ etus} \leq t_{P1} \leq (960 \times D \times WI) \text{ etus}$ (D 由 TA1 和 TA2 决定， WI 由 TC2 决定。如果 TA1 没有声明，或 TA1 声明了，但是 TA2 没有声明，那么使用默认值 $D=1$ ；如果 TC2 没有声明，那么使用默认值 $WI=10$)。

6.5.2 TPSF002-00

测试目的：确保终端发送上一个字符到 IC 卡发送下一个字符的时间间隔，满足最小为 16 etus 最大为 $(960 \times D \times WI) \text{ etus}$ (工作等待时间)。

测试条件：条件 4 或条件 5 为 T=0 协议。

测试流程：a) 启动冷复位并接收 ATR；
b) 发送命令并接收响应；
c) 交易过程中，测量终端发送最后一个字符的起始位下降沿到卡片发送第一个字符的起始位下降沿时间间隔 t_{P1} ；
d) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡响应时间为 $16 \text{ etus} \leq t_{P1} \leq (960 \times D \times WI) \text{ etus}$ (D 由 TA1 和 TA2 决定， WI 由 TC2 决定。如果 TA1 没有声明，或 TA1 声明了，但是 TA2 没有声明，那么使用默认

值 $D=1$; 如果 TC2 没有声明, 那么使用默认值 $WI=10$)。

6.5.3 TPSF003-00

测试目的: 确保 IC 卡正确接收终端按 TC1 中定义的最小字符间隔的字符。

测试条件: 条件 4 或条件 5 为 T=0 协议。

测试流程: a) 终端用 TC1 中定义的 N 值, 发送字符间隔为 $11.8+N$ 的命令 (如果 TC1 不存在, 就使用 11.8) ($-0.0 \text{ etu} / +0.2 \text{ etu}$);

b) 启动冷复位并接收 ATR;

c) 完成全部交易;

d) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡正确处理所有命令, 并按 ICS 中定义的返回正确响应。

6.5.4 TPSF004-00

测试目的: 确保在 IC 卡发送完最后一个字符后, 能正确接收终端以 15etus 的保护时间下发送的一个字符。

测试条件: 条件 4 或条件 5 为 T=0 协议。

测试流程: a) IC 卡发送最后一个字符起始位下降沿到终端发送第一个字符起始位下降沿的时间间隔为 15 etus ($-0.0 \text{ etu} / +0.2 \text{ etu}$);

b) 启动冷复位并接收 ATR;

c) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡正确完成 SELECT 命令过程并且返回 ICS 指定的 FCI 数据。

6.5.5 TPSF005-00

测试目的: 确保在处理命令情况 4 命令时, IC 卡传送合法过程字节。

测试条件: 条件 4 或条件 5 为 T=0 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 选择应用;

c) 发送 GP0 命令数据头, 并接收过程字;

d) 在状态字的要求下, 发送 GP0 命令数据;

e) 接收 “61xx” 过程字, 请求 GET RESPONSE;

f) 通过 GET RESPONSE 处理接收到的响应数据及状态字;

g) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡用 “A8” 或 “57” 响应 GP0 命令, 用 “61xx” 响应 SELECT 命令。如果后续存在响应数据, IC 卡用 “C0” + “61yy” 的形式响应 GET RESPONSE 命令, 如果后续不存在响应数据, IC 卡用 “C0” + “9000” 的形式响应 GET RESPONSE 命令。

6.5.6 TPSF006-00

测试目的: 确保在处理命令情况 2 命令时, IC 卡传送合法过程字节。

测试条件: 条件 4 或条件 5 为 T=0 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 发送 SELECT 和 GP0 命令过程;

c) 发送 P3= “00” 的 READ RECORD 命令头, 并接收过程字;

d) 重发 P3 等于第二个过程字节的 READ RECORD 命令头;

e) 按如下要求处理接收到的所有过程字节和数据：“B2”为接收所有响应数据，“4D”为接收一个字节响应，并等待下一个字节，“61”为接收第二个状态字节，并通过 GET RESPONSE 命令处理接收到的响应数据；

f) 接收状态字节；

g) 如果需要，就通过 READ RECORD 命令完成其余的情况 2 命令的交易；

h) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：卡片响应第一个 READ RECORD 命令头的过程字节为“6C”+Licc，响应重发的 READ RECORD 命令头的过程字节为“B2”、“4D”或者“61xx”，用“C0”+“61yy”的形式响应 GET RESPONSE 命令。如果后续存在响应数据，IC 卡用“C0”+“61yy”的形式响应 GET RESPONSE 命令，如果后续不存在响应数据，IC 卡返回 9000。

6.5.7 TPSF007-00

测试目的：确保在 $Le > Licc$ 时，IC 卡能够正确处理命令情况 2。

测试条件：条件 4 或条件 5 为 T=0 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送 SELECT 和 GP0 命令过程；

c) 发送 P3=“FF”的 READ RECORD 命令头，并接收过程字；

d) 重发 P3 等于第二个过程字节的 READ RECORD 命令头，并接收下一个过程字；

e) 处理响应数据和状态字节；

f) 如果需要，就通过 READ RECORD 命令完成其余的情况 2 命令的交易；

g) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：卡片响应 READ RECORD 命令头的过程字节为“6C”+Licc，响应重发的 READ RECORD 命令头的过程字节为“B2”、“4D”或者“61xx”，用“C0”+“61yy”的形式响应 GET RESPONSE 命令。如果后续不存在响应数据，IC 卡返回 9000。

6.5.8 TPSF008-00

测试目的：确保在 $Le = Licc$ 时，IC 卡能够正确处理命令情况 2。

测试条件：条件 4 或条件 5 为 T=0 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送 SELECT 和 GP0 命令过程；

c) 发送 P3= Licc 的 READ RECORD 命令头，并接收过程字；

d) 处理响应数据和状态字节；

e) 如果需要，就通过 READ RECORD 命令完成其余的情况 2 命令的交易；

f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：卡片响应 READ RECORD 命令头的过程字节为“6C”+Licc，响应重发的 READ RECORD 命令头的过程字节为“B2”、“4D”或者“61xx”。如果后续不存在响应数据，IC 卡返回 9000。

6.5.9 TPSF009-00

测试目的：确保在 $Le < Licc$ 时，IC 卡能够正确处理命令情况 2。

测试条件：条件 4 或条件 5 为 T=0 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送 SELECT 和 GP0 命令过程；

- c) 发送 P3= “01” 的 READ RECORD 命令头;
- d) 接收卡片返回的第一个过程字节, 如果该字节为 “B2” 或 “4D”, 接收后续数据字节和两个过程字节, 发送 GET RESPONSE 命令, P3 设置为最后一个过程字节, 接收过程字节和数据; 如果该字节为 “6C”, 接收第二个过程字节, 再次发送 READ 命令, P3 设置为第二个过程字节值, 接收过程字节和数据;
- e) 处理响应数据和状态字节;
- f) 如果需要, 就通过 READ RECORD 命令完成其余的情况 2 命令的交易;
- g) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 如果卡片返回的第一个过程字节为 “B2” 或 “4D”, 那么第一个数据字节为 ICS 中指定的数据, 第一个数据字节后的过程字节为 “61xx”, GET RESPONSE 命令头后的过程字节为 “C0” 或者 “3F”, 且后续数据字节同 ICS 指定的数据; 如果卡片返回的第一个过程字节为 “6C”, 那么过程字节等于 ICS 中指定的数据 (Licc) 的长度, READ 命令头后的过程字节为 “B2” 或者 “4D”, 且后续数据字节同 ICS 指定的数据。

6.5.10 TPSF010-00

测试目的: 确保在处理命令情况 3 命令时, IC 卡传送合法过程字节。

测试条件: 条件 4 或条件 5 为 T=0 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 开始交易, 直到出现情况 3 命令 (VERIFY);

c) 发送情况 3 命令头 (VERIFY);

d) 接收过程字节, 并继续交易;

e) 当所有命令发送完成后, 接收状态字节;

f) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 卡片响应 VERIFY 命令头的过程字节为 “20” 或 “DF”。收到正确 PIN, IC 卡返回 9000; 收到错误 PIN, IC 卡返回 “61xx”。

6.5.11 TPSF011-00

测试目的: 确保在终端给出奇偶校验错误的纠错信号后, IC 卡重发一个字符。

测试条件: 条件 4 或条件 5 为 T=0 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 交易开始, 并接收 IC 卡数据;

c) 在收到第二个字符, 将 I/O 信号持续拉低。测量重复字符和前一个字符下降沿的时间间隔 t_{P1} ;

d) 接收重复字符和剩余所有响应的命令;

e) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡重复发送一次字符的时间 $t_{P1} \geq 12.8 \text{ etu}$ (发送方应在字符起始位下降沿 11 ± 0.2 个 etu 后检测 I/O 电平, 所以最早检测到为 10.8 etu , 最早重发为 12.8 etu), 重发字符和错误字符相同, 除错误字符外, 响应数据均和 ICS 中指定的数据相同。

6.5.12 TPSF012-00

测试目的: 确保在终端给出奇偶校验错误的纠错信号后, IC 卡连续四次重发该字符。

测试条件: 条件 4 或条件 5 为 T=0 协议。

测试流程: a) 启动冷复位并接收 ATR;

- b) 交易开始，并接收 IC 卡数据；
- c) 在收到第二个字符，将 I/O 信号持续拉低，测量重复字符和前一个字符下降沿的时间间隔 t_{P1} ；
- d) 接收四次重复字符和剩余所有响应的命令；
- e) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡重复发送四次字符，且每次时间 $t_{P1} \geq 12.8 \text{ etu}$ 注：（发送方应在字符起始位下降沿 11 ± 0.2 个 etu 后检测 I/O 电平，。所以，最早侦测到为 10.8 etu ，最早重发为 12.8 etu ；），重发字符和错误字符相同，除错误字符外，响应数据均和 ICS 中指定的数据相同。

6.5.13 TPSF013-00

测试目的：确保 IC 卡在接收到终端一个奇偶校验错误的字符后，能正确发送奇偶校验错误的纠错信号。

测试条件：条件 4 或条件 5 为 T=0 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 交易开始；
- c) 在接收到来自 IC 卡的过程字节后，发送错误的命令数据，测量在错误字符起始位下降沿至 IC 卡将 I/O 电平置低的时间间隔 t_{P1} ，和 I/O 已经被拉低的时间段 t_{P2} ；
- d) 重发奇偶校验设置正确的字符并且完成交易；
- e) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡在收到错误后， $10.3 \leq t_{P1} \leq 10.7 \text{ etu}$ 将 I/O 信号拉低，I/O 低电平持续时间为 $1 \leq t_{P2} \leq 2 \text{ etu}$ 。在接收正确的字符后，IC 卡继续接收剩余数据并且正常完成交易。

6.5.14 TPSF014-00

测试目的：确保 IC 卡在接收到终端一个奇偶校验错误的字符后，连续四次发送奇偶校验错误的纠错信号。

测试条件：条件 4 或条件 5 为 T=0 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 交易开始；
- c) 在接收到来自 IC 卡的过程字节后，发送错误的命令数据，测量在错误字符起始位下降沿至 IC 卡将 I/O 电平置低的时间间隔 t_{P1} ，和 I/O 已经被拉低的时间段 t_{P2} ；
- d) 多次重发奇偶校验设置错误的字符；
- e) 重发奇偶校验设置正确的字符并且完成交易；
- f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡在每次收到错误后， $10.3 \leq t_{P1} \leq 10.7 \text{ etu}$ 将 I/O 信号拉低，每次 I/O 低电平持续时间为 $1 \leq t_{P2} \leq 2 \text{ etu}$ 。在接收正确的字符后，IC 卡继续接收剩余数据并且正常完成交易。

6.5.15 TPSF015-00

测试目的：确保 IC 卡在接收到终端一个奇偶校验错误的字符后，连续五次发送奇偶校验错误的纠错信号。

测试条件：条件 4 或条件 5 为 T=0 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 交易开始;
- c) 在接收到来自 IC 卡的过程字节后, 发送错误的命令数据, 测量在错误字符起始位下降沿至 IC 卡将 I/O 电平置低的时间间隔 t_{P1} , 和 I/O 已经被拉低的时间段 t_{P2} ;
- d) 重发超过四次的奇偶校验设置错误的字符;
- e) 启动下电时序;
- f) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡在每次收到错误后, $10.3 \leq t_{P1} \leq 10.7$ etu 将 I/O 信号拉低, 每次 I/O 低电平持续时间为 $1 \leq t_{P2} \leq 2$ etu。

6.5.16 TPSF016-00

测试目的: 确保 IC 卡在超出工作等待时间状态时, 启动“60”过程字节, 请求额外工作等待时间。

测试条件: ——条件 4 或条件 5 为 T=0 协议;
——条件 13 为使用过程字节“60”。

测试流程: a) 启动冷复位并接收 ATR;
b) 开始交易并完成交易, 强制 IC 卡请求“60”过程字节;
c) 测量“60”过程字节起始位下降沿到过程字节结束的时间 t_{P1} ;
d) 测量“60”过程字节起始位下降沿到 IC 卡收到下一个过程字节开始的时间 t_{P2} ;
e) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: $12 \text{ etu} \leq t_{P1} \leq \text{WWT}$, $12 \text{ etu} \leq t_{P2} \leq \text{WWT}$ 。如果命令数据头 $Le = "00"$, 那么 IC 卡不返回“60”作为第一个过程字节 ($\text{WWT} = 960 \times D \times WI$ etus, D 由 TA1 和 TA2 决定, WI 由 TC2 决定。如果 TA1 没有声明, 或 TA1 声明了, 但是 TA2 没有声明, 那么使用默认值 $D=1$; 如果 TC2 没有声明, 那么使用默认值 $WI=10$)。

6.5.17 TPSF017-00

测试目的: 确保 IC 卡在收到超出额外保护时间的命令和数据时, 不发送任何数据。

测试条件: 条件 4 或条件 5 为 T=0 协议。

测试流程: a) 启动冷复位并接收 ATR;
b) 在 IC 卡发送最后一个字符起始位下降沿开始, 到终端发送第一个数据开始的时间至少为 10000 etus ($-0.0 \text{ etu} / +2 \text{ etu}$) 后, 发送命令和数据;
c) 启动冷复位并接收 ATR;
d) 完成交易;
e) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 如果命令、命令的数据头或命令数据超出额外保护时间, 那么 IC 卡保持接收模式, 并且不发送任何数据 (或状态字)。IC 卡按 ICS 中定义的数据, 继续接收剩余的数据, 并完成交易。

6.6 T=1 协议测试 (TPSG)

6.6.1 TPSG001-00

测试目的: 确保 IC 卡两个连续字符之间的最小时间间隔是 11 个 etu, 最大间隔是 $(2^{CWT} + 11)$ 个 etu (CWT 是字符等待时间)。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

- b) 发送 S (IFS 请求) 块 (IFSD=254), 测量 IC 卡返回的 S (IFS 响应) 块中的所有字符的起始位的下降沿之间的时间间隔 t_{p1} ;
- c) 发送 SELECT 命令, 测量 IC 卡返回的 I 块中的所有字符的起始位的下降沿之间的时间间隔 t_{p1} ;
- d) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡返回的两个连续字符之间的时间间隔满足 $11 \text{ etus} \leq t_{p1} \leq (2^{\text{CWT}}+11) \text{ etus}$ 。

6.6.2 TPSG002-00

测试目的: 确保 IC 卡从终端接收最后一个字符至返回第一个字符之间的最小时间间隔是块保护时间 (BGT), 最大时间间隔是块等待时间。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

- b) 发送 S (IFS 请求) 块 (IFSD=254), 测量终端发送最后一个 S (IFS 请求) 块起始位的下降沿到 IC 卡返回第一个的 S (IFS 响应) 块的起始位的下降沿之间的时间间隔 t_{p1} ;
- c) 发送 SELECT 命令, 测量终端发送 SELECT 命令的最后一个字节的下降沿到 IC 卡返回的 I 块第一个字节的下降沿之间的时间间隔 t_{p1} ;
- d) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 终端发送最后一个字符到 IC 卡返回第一个字符的时间间隔满足 $22 \text{ etus} \leq t_{p1} \leq (2^{\text{BWT}} \times 960 \times 372D/F + 11) \text{ etus}$ 。

6.6.3 TPSG003-00

测试目的: 确保 IC 卡能正确接收终端按 ATR 的 TC1 中指出的最小字符间隔发送的字符。

测试条件: 条件 4 或条件 5 为 T=1 协议。

- 测试流程: a) 设定终端发送的数据连续字符的起始位的下降沿之间的时间间隔, 采用 TC1 中指定的值 $11.8 + N \text{ etus}$ (如果 TC1 = 'FF' 使用 10.8 etu , 如果 TC1 不存在使用 11.8 etu) $(-0.0 \text{ etu} / +0.2 \text{ etu})$;
- b) 启动冷复位并接收 ATR;
 - c) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;
 - d) 完成全部交易;
 - e) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡正确处理所有命令, 并且返回的响应符合 ICS 规定。

6.6.4 TPSG004-00

测试目的: 确保 IC 卡能正确接收终端按连续字符间的最大字符间隔发送的字符, $\text{CWT} + 4 \text{ etus} = (2^{\text{CWT}} + 11) + 4 \text{ etus}$ 。

测试条件: 条件 4 或条件 5 为 T=1 协议。

- 测试流程: a) 设定终端发送的数据连续两个字符起始位下降沿之间的最大时间间隔采用 TB3 中指定的值 $2^{\text{CWT}} + 15 \text{ etu} (-0.2 \text{ etu} / +0.0 \text{ etu})$;
- b) 启动冷复位并接收 ATR;
 - c) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;
 - d) 完成全部交易;
 - e) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准：IC 卡正确处理所有命令，并且返回的响应符合 ICS 规定。

6.6.5 TPSG005-00

测试目的：确保 IC 卡能正确接收终端在接收到 IC 卡最后一个字符后正好经过块保护时间后发送的字符。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 设定 IC 卡发送块的最后一个字符的起始位的下降沿到终端发送块的第一个字符的起始位的下降沿的时间间隔是 $21et_u (-0.0et_u/+0.2et_u)$ ；
b) 启动冷复位并接收 ATR；
c) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254)；
d) 完成全部交易；
e) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡正确处理所有命令，并且返回的响应符合 ICS 规定。

6.6.6 TPSG006-00

测试目的：确保 IC 卡发送的所有块的 NAD=“00”。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；
b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254)；
c) 完成全部交易并检查所有接收到的数据包中的节点地址（注：终端发送的所有数据包应设为 NAD=“00”）；
d) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡发送的所有块的 NAD=“00”。

6.6.7 TPSG007-00

测试目的：确保 IC 卡发送的第一个 I 块的序列号为 0，以后的 I 块序列号为按次序递增的二进制数。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；
b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254)；
c) 完成全部交易并检查所有接收到的 I 块序列号；
d) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡返回的第一个 I 块的序列号为 0 (PCB 的 b7=0)，随后响应的 I 块中，序列号按二进制每次增加 1。

6.6.8 TPSG008-00

测试目的：确保 IC 卡在终端发送错误的 EDC 命令时能正确响应一个数据块。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；
b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254)；
c) 开始整个交易，直到出现 C-APDU；
d) 发送带有 EDC 错误的第一个 I 块（保证 EDC 字节的奇偶校验位是正确的），并检查 IC 卡响应；

- e) 重发一次正确的 I 块，并完成交易；
- f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：IC 卡收到带有 EDC 错误的 I 块返回一个 R 块，并且它的序列号和带有 EDC 错误的 I 块相同；IC 卡正确的处理重发的 I 块（没有 EDC 错误），并且后续发送的块和返回的响应符合 ICS 规定。

6.6.9 TPSG009-00

测试目的：确保 IC 卡在收到终端发送的含奇偶校验错误的块时，不会将 I/O 电平置为低电平指示奇偶校验错误。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送带有奇偶校验错误的 I 块（保证 EDC 字节的奇偶校验位是正确的），并检查 I/O 电平；

d) 接收 IC 卡响应；

e) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：I/O 在含有奇偶校验错误的字符和下一个字符的保护时间内始终保持高电平，IC 卡响应的 R 块的序列号为 0。

6.6.10 TPSG010-00

测试目的：确保 IC 卡在收到终端（请求重发）的 R 块后，能重发 I 块并忽略 R 块的 b4 到 b1 位。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送第一个 I 块（一个 SELECT 命令），并接收 IC 卡响应；

d) 发送第一个 R 块（PCB 的 b4 到 b1 有误，b5=0），并接收 IC 卡重发块；

e) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：重发的 I 块和之前发送的 I 块相同。

6.6.11 TPSG011-00

测试目的：确保 IC 卡在 ATR 后收到单次错误时响应正确。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送一个错误的 S（IFS 请求）块（IFSD=254），并接收 IC 卡响应；

c) 发送一个正确的 S（IFS 请求）块（IFSD=254），并接收 IC 卡响应；

d) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到一个错误的 S 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到一个正确的 S（IFS 请求）块后，IC 卡返回一个 S（IFS 响应）块。

6.6.12 TPSG012-00

测试目的：确保 IC 卡在 ATR 后收到两次错误时响应正确。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 发送一个带有 EDC 错误的 S (IFS 请求) 块 (IFSD=254)，并接收 IC 卡响应；
- c) 重发这个带有 EDC 错误的 S (IFS 请求) 块 (IFSD=254)，并接收 IC 卡响应；
- d) 发送一个正确的 S (IFS 请求) 块 (IFSD=254)，并接收 IC 卡响应；
- e) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带有 EDC 错误的 S 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到第二个带有 EDC 错误的 S 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到一个正确的 S (IFS 请求) 块后，IC 卡返回一个 S (IFS 响应) 块。

6.6.13 TPSG013-00

测试目的：确保 IC 卡在 ATR 后收到超过两次错误时没有响应。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 发送一个带有 EDC 错误的 S (IFS 请求) 块 (IFSD=254)，并接收 IC 卡响应；
- c) 重发这个带有 EDC 错误的 S (IFS 请求) 块 (IFSD=254)，并接收 IC 卡响应；
- d) 再次重发这个带有 EDC 错误的 S (IFS 请求) 块 (IFSD=254)，并确保 IC 卡无响应；
- e) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带有 EDC 错误的 S 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到第二个带有 EDC 错误的 S 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到第三个带有 EDC 错误的 S 块后，IC 卡无响应（在 BWT+100%以内）。

6.6.14 TPSG014-00

测试目的：确保 IC 卡在 S (IFS 请求) 块后收到单次错误时响应正确。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254)；
- c) 发送一个错误的块，并接收 IC 卡响应；
- d) 发送一个正确的 I 块（一个无误的 SELECT 命令），并接收 IC 卡响应；
- e) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到一个错误的块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到一个正确的 I 块后，IC 卡返回一个 I 块。

6.6.15 TPSG015-00

测试目的：确保 IC 卡在 S (IFS 请求) 块后收到两次错误时响应正确。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254)；
- c) 发送一个带有 EDC 错误的 I 块（一个 SELECT 命令），并接收 IC 卡响应；
- d) 重发这个带有 EDC 错误的 I 块，并接收 IC 卡响应；
- e) 发送一个正确的 I 块，并接收 IC 卡响应；
- f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带有 EDC 错误的 I 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到第二个带有 EDC 错误的 I 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到一个正确的 I 块后，IC 卡返回一个 I 块。

6.6.16 TP SG016-00

测试目的：确保 IC 卡在 S（IFS 请求）块后收到超过两次错误时没有响应。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送一个带有 EDC 错误的 I 块（一个 SELECT 命令），并接收 IC 卡响应；

d) 重发这个带有 EDC 错误的 I 块，并接收 IC 卡响应；

e) 再次重发这个带有 EDC 错误的 I 块，并确保 IC 卡无响应；

f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带有 EDC 错误的 I 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到第二个带有 EDC 错误的 I 块后，IC 卡返回一个 R 块，其中 PCB 的 b5=0；在接收到第三个带有 EDC 错误的 I 块后，IC 卡无响应（在 BWT+100%以内）。

6.6.17 TP SG017-00

测试目的：确保 IC 卡正确重发 S（IFS 响应）块。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 重发这个 S（IFS 请求）块，并接收 IC 卡响应；

d) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：重发的 S（IFS 响应）块和第一次应答 S（IFS 请求）块的 S（IFS 响应）块相同。

6.6.18 TP SG019-00

测试目的：确保 IC 卡在发送完非链接的 I 块（序列号为 0）之后出现单次传输错误时响应正确。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到 IC 卡发送一个非链接的序列号为 0 的 I 块（PCB 的 b6=0，PCB 的 b7=0）；

d) 发送一个错误的块，并接收 IC 卡响应；

e) 发送一个正确的非链接的 I 的块，并接收 IC 卡响应；

f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到一个错误的块后，IC 卡返回一个序列号为 1 的 R 块（PCB 的 b5=1）；在接收到下一个 I 块后，IC 卡返回一个 I 块。

6.6.19 TP SG020-00

测试目的：确保 IC 卡在发送完非链接的 I 块（序列号为 0）之后出现两次传输错误时响应正确。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到 IC 卡发送一个非链接的序列号为 0 的 I 块（PCB 的 b6=0，PCB 的 b7=0）；

d) 发送一个非链接的序列号为 1 的 I 块（PCB 的 b7=1），并且带有 EDC 错误，接收

IC 卡响应;

e) 重发这个带有 EDC 错误的 I 块, 并接收 IC 卡响应;

f) 发送一个非连接的正确的 I 块, 并接收 IC 卡响应;

g) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 在接收到第一个带有 EDC 错误的 I 块后, IC 卡返回一个序列号为 1 的 R 块 (PCB 的 b5=1); 在接收到第二个带有 EDC 错误的 I 块后, IC 卡返回一个序列号为 1 的 R 块 (PCB 的 b5=1); 在接收到下一个 I 块后, IC 卡返回一个 I 块。

6.6.20 TPSG021-00

测试目的: 确保 IC 卡在发送完非链接的 I 块 (序列号为 0) 之后出现超过两次传输错误时没有响应。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254);

c) 发送并处理一个交易中的命令, 直到 IC 卡发送一个非链接的序列号为 0 的 I 块 (PCB 的 b6=0, PCB 的 b7=0);

d) 发送一个非链接的序列号为 1 的 I 块 (PCB 的 b7=1), 并且带有 EDC 错误, 接收 IC 卡响应;

e) 重发这个带有 EDC 错误的 I 块, 并接收 IC 卡响应;

f) 再次重发这个带有 EDC 错误的 I 块, 并确保 IC 卡无响应;

g) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 在接收到第一个带有 EDC 错误的 I 块后, IC 卡返回一个序列号为 1 的 R 块 (PCB 的 b5=1); 在接收到第二个带有 EDC 错误的 I 块后, IC 卡返回一个序列号为 1 的 R 块 (PCB 的 b5=1); 在接收到第三个带有 EDC 错误的 I 块后, IC 卡无响应 (在 BWT+100% 以内)。

6.6.21 TPSG022-00

测试目的: 确保 IC 卡正确重发非链接的 I 块 (序列号为 0)。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254);

c) 发送并处理一个交易中的命令, 直到 IC 卡发送一个非链接的序列号为 0 的 I 块 (PCB 的 b6=0, PCB 的 b7=0);

d) 发送一个序列号为 0 的 R 块 (PCB 的 b5=0), 并接收 IC 卡重发块;

e) 发送一个非链接的 I 块, 并接收 IC 卡响应;

f) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 重发的 I 块和第一次响应 I 块的块相同; 在接收到下一个 I 块后, IC 卡返回一个 I 块。

6.6.22 TPSG023-00

测试目的: 确保 IC 卡在收到重发请求命令出现错误之后的正确重发请求命令时, 重发非链接的 I 块 (序列号为 0)。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254);

c) 发送并处理一个交易中的命令,直到 IC 卡发送一个非链接的序列号为 0 的 I 块(PCB 的 b6=0, PCB 的 b7=0);

d) 发送一个带有 EDC 错误的序列号为 0 的 R 块 (PCB 的 b5=0), 并接收 IC 卡响应;

e) 发送一个正确的序列号为 0 的 R 块 (PCB 的 b5=0), 并接收 IC 卡响应;

f) 发送一个非链接的 I 块, 并接收 IC 卡响应;

g) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 在接收到带有 EDC 错误的 R 块后, IC 卡发送一个序列号为 1 的 R 块 (PCB 的 b5=1); 在接收到正确的 R 块后, IC 卡返回一个序列号为 0 的 I 块 (PCB 的 b7=0), 并且这个 I 块和带有 EDC 错误的 R 块之前 IC 卡发送的 I 块相同; 在接收到下一个 I 块后, IC 卡返回一个 I 块。

6.6.23 TPSEG025-00

测试目的: 确保 IC 卡在发送完非链接的 I 块 (序列号为 1) 之后, 收到单次传输错误时响应正确。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254);

c) 发送并处理一个交易中的命令,直到 IC 卡发送一个非链接的序列号为 1 的 I 块(PCB 的 b6=0, PCB 的 b7=1);

d) 发送一个错误的块, 并接收 IC 卡响应;

e) 发送一个正确的非链接的 I 的块, 并接收 IC 卡响应;

f) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 在接收到一个错误的块后, IC 卡返回一个序列号为 0 的 R 块 (PCB 的 b5=0); 在接收到下一个 I 块后, IC 卡返回一个 I 块。

6.6.24 TPSEG026-00

测试目的: 确保 IC 卡在发送完非链接的 I 块 (序列号为 1) 之后, 收到连续两次传输错误时响应正确。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254);

c) 发送并处理一个交易中的命令,直到 IC 卡发送一个非链接的序列号为 1 的 I 块(PCB 的 b6=0, PCB 的 b7=1);

d) 发送一个非链接的序列号为 0 的 I 块 (PCB 的 b7=0), 并且带有 EDC 错误, 接收 IC 卡响应;

e) 重发这个带有 EDC 错误的 I 块, 并接收 IC 卡响应;

f) 发送一个非连接的正确的 I 块, 并接收 IC 卡响应;

g) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 在接收到第一个带有 EDC 错误的 I 块后, IC 卡返回一个序列号为 0 的 R 块 (PCB 的 b5=0); 在接收到第二个带有 EDC 错误的 I 块后, IC 卡返回一个序列号为 0 的 R 块 (PCB 的 b5=0); 在接收到下一个 I 块后, IC 卡返回一个 I 块。

6.6.25 TPSG027-00

测试目的：确保 IC 卡在发送完非链接的 I 块（序列号为 1）之后，收到超过两次传输错误时没有响应。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；
 b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；
 c) 发送并处理一个交易中的命令，直到 IC 卡发送一个非链接的序列号为 1 的 I 块（PCB 的 b6=0，PCB 的 b7=1）；
 d) 发送一个非链接的序列号为 0 的 I 块（PCB 的 b7=0），并且带有 EDC 错误，接收 IC 卡响应；
 e) 重发这个带有 EDC 错误的 I 块，并接收 IC 卡响应；
 f) 再次重发这个带有 EDC 错误的 I 块，并确保 IC 卡无响应；
 g) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带有 EDC 错误的 I 块后，IC 卡返回一个序列号为 0 的 R 块（PCB 的 b5=0）；在接收到第二个带有 EDC 错误的 I 块后，IC 卡返回一个序列号为 0 的 R 块（PCB 的 b5=0）；在接收到第三个带有 EDC 错误的 I 块后，IC 卡无响应（在 BWT+100% 以内）。

6.6.26 TPSG028-00

测试目的：确保 IC 卡正确重发非链接的 I 块（序列号为 1）。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；
 b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；
 c) 发送并处理一个交易中的命令，直到 IC 卡发送一个非链接的序列号为 1 的 I 块（PCB 的 b6=0，PCB 的 b7=1）；
 d) 发送一个序列号为 1 的 R 块（PCB 的 b5=1），并接收 IC 卡重发块；
 e) 发送一个非链接的 I 块，并接收 IC 卡响应；
 f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：重发的 I 块和第二次响应 I 块的块相同；在接收到下一个 I 块后，IC 卡返回一个 I 块。

6.6.27 TPSG029-00

测试目的：确保 IC 卡在收到重发请求命令出现错误之后的正确重发请求命令时，重发非链接的 I 块（序列号为 1）。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；
 b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；
 c) 发送并处理一个交易中的命令，直到 IC 卡发送一个非链接的序列号为 1 的 I 块（PCB 的 b6=0，PCB 的 b7=1）；
 d) 发送一个带有 EDC 错误的序列号为 1 的 R 块（PCB 的 b5=1），并接收 IC 卡响应；
 e) 发送一个正确的序列号为 1 的 R 块（PCB 的 b5=1），并接收 IC 卡响应；
 f) 发送一个非链接的 I 块，并接收 IC 卡响应；
 g) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到带有 EDC 错误的 R 块后，IC 卡发送一个序列号为 0 的 R 块（PCB 的 b5=0）；在接收到正确的 R 块后，IC 卡返回一个序列号为 1 的 I 块（PCB 的 b7=1），并且这个 I 块和带有 EDC 错误的 R 块之前 IC 卡发送的 I 块相同；在接收到下一个 I 块后，IC 卡返回一个 I 块。

6.6.28 TP SG031-00

测试目的：确保 IC 卡在收到终端发起的一个带链接的 I 块（序列号为 0）后发送一个带链接的块。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到终端强制发送一个带链接的序列号为 0 的 I 块（PCB 的 b7=0，PCB 的 b6=1）；

d) 发送带链接的 I 块（PCB 的 b6=1，LEN=IFSC），并接收 IC 卡响应；

e) 发送链接中的最后一个 I 块（PCB 的 b6=0，LEN≤IFSC），并接收 IC 卡响应；

f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到一个带链接的序列号为 n 的 I 块（PCB 的 b6=1，b7=n）后，IC 卡发送一个序列号为 n+1 的 R 块（PCB 的 b5=n+1）；在接收到链接中的最后一个 I 块后，IC 卡返回一个 I 块。

6.6.29 TP SG032-00

测试目的：在终端发起的一个链接中，确保 IC 卡在收到错误通知时，正确地重发一个 R(ACK) 块（序列号为 1）。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到终端发送第一个带链接的序列号为 0 的 I 块（PCB 的 b7=0，PCB 的 b6=1，LEN=IFSC），并接收 IC 卡响应；

d) 如果 IC 卡发送最后一个 I 块的序列号为 n（PCB 的 b7=n），就发送一个序列号为 n+1 的 R 块（PCB 的 b5=n+1）请求重发，并接收 IC 卡重发响应；

e) 发送第二个带链接的 I 块（指明链接或者发送链接中的最后一个块），并接收 IC 卡响应；

f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带链接的 I 块（PCB 的 b6=1）后，IC 卡发送一个序列号为 1 的 R 块（PCB 的 b5=1）；在接收到请求重发的 R 块后，IC 卡重新发送这个 R 块（PCB 的 b5=1）；在收到第二个带链接的 I 块后，IC 卡返回一个序列号为 0 的 R 块（PCB 的 b5=0）或一个 I 块。

6.6.30 TP SG034-00

测试目的：确保 IC 卡在收到 I 块之后，如果需要请求超过 BWT 的等待时间，能正确地发送一个 S（WTX 请求）块。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;
- c) 开始并完成交易, 强制 IC 卡请求 S (WTX 请求) 块;
- d) 当 IC 卡请求 S (WTX 请求) 块时, 终端用相同的 INF 值返回 S (WTX 响应) 块, 并且等待请求的时间 (+100%), 直到 IC 发送下一个块;
- e) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 每次请求的额外等待时间都需执行 (注: 虽然 ICS 中指明 IC 卡可以请求 S (WTX 请求) 块, 但因交易中不需要, 可能不被执行, 这种情况下该案例可以不测试)。

6.6.31 TPSG035-00

测试目的: 确保 IC 卡在收到正确的 R 块之后, 正确地重发一个 S (WTX 请求) 块。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

- b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;
- c) 开始交易, 强制 IC 卡请求 S (WTX 请求) 块;
- d) 接收 IC 卡请求的 S (WTX 请求) 块;
- e) 发送一个正确的 R 块;
- f) 接收重发的 S (WTX 请求) 块;
- g) 发送 S (WTX 响应) 块;
- h) 接收响应数据并完成交易;
- i) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡重发 S (WTX 请求) 块, 在 S (WTX) 块之后, IC 卡发送的 I 块中的数据符合 ICS 中声明的要求 (注: 虽然 ICS 中指明 IC 卡可以请求 S (WTX 请求) 块, 但因交易中不需要, 可能不被执行, 这种情况下该案例可以不测试)。

6.6.32 TPSG036-00

测试目的: 确保 IC 卡在收到错误的 R 块之后, 正确地重发一个 S (WTX 请求) 块。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

- b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;
- c) 开始交易, 强制 IC 卡请求 S (WTX 请求) 块;
- d) 接收 IC 卡请求的 S (WTX 请求) 块;
- e) 发送一个带有 EDC 错误的 R 块;
- f) 接收重发的 S (WTX 请求) 块;
- g) 发送 S (WTX 响应) 块;
- h) 接收响应数据并完成交易;
- i) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: IC 卡重发 S (WTX 请求) 块, 在 S (WTX) 块之后, IC 卡发送的 I 块中的数据符合 ICS 中声明的要求 (注: 虽然 ICS 中指明 IC 卡可以请求 S (WTX 请求) 块, 但因交易中不需要, 可能不被执行, 这种情况下该案例可以不测试)。

6.6.33 TPSGX19-00

测试目的: 确保 IC 卡在收到终端发起的一个带链接的 I 块 (序列号为 1) 后发送一个带链接的块。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到终端强制发送一个带链接的序列号为 1 的 I 块（PCB 的 b7=1，PCB 的 b6=1）；

d) 发送带链接的 I 块（PCB 的 b6=1，LEN=IFSC），并接收 IC 卡响应；

e) 发送链接中的最后一个 I 块（PCB 的 b6=0，LEN≤IFSC），并接收 IC 卡响应；

f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到一个带链接的序列号为 n 的 I 块（PCB 的 b6=1，b7=n）后，IC 卡发送一个序列号为 n+1 的 R 块（PCB 的 b5=n+1）；在接收到链接中的最后一个 I 块后，IC 卡返回一个 I 块。

6.6.34 TPSGX01-00

测试目的：在终端发起的一个链接中，确保 IC 卡在发送完 R(ACK) 块（序列号为 1）后，终端出现单次错误时，IC 卡响应正确。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到终端发送第一个带链接的序列号为 0 的 I 块（PCB 的 b7=0，PCB 的 b6=1，LEN=IFSC），并接收 IC 卡响应；

d) 发送第二个含有 EDC 错误的带链接的 I 块（指明链接或者发送链接中的最后一个块），并接收 IC 卡响应；

e) 发送第二个正确的带链接的 I 块，并接收 IC 卡响应；

f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带链接的 I 块（PCB 的 b6=1）后，IC 卡发送一个序列号为 1 的 R 块（PCB 的 b5=1）；在收到第二个错误的带链接的 I 块后，IC 卡返回一个序列号为 1 的 R 块（PCB 的 b5=1）；在收到第二个正确的带链接的 I 块后，IC 卡返回一个序列号为 0 的 R 块（PCB 的 b5=0）或一个 I 块。

6.6.35 TPSGX02-00

测试目的：在终端发起的一个链接中，确保 IC 卡在发送完 R(ACK) 块（序列号为 1）后，终端出现多次连续错误时，IC 卡没有响应。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到终端发送第一个带链接的序列号为 0 的 I 块（PCB 的 b7=0，PCB 的 b6=1，LEN=IFSC），并接收 IC 卡响应；

d) 发送第二个含有 EDC 错误的带链接的 I 块（指明链接或者发送链接中的最后一个块），并接收 IC 卡响应；

e) 重发这个含有 EDC 错误的带链接的 I 块，并确保 IC 卡无响应；

f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带链接的 I 块（PCB 的 b6=1）后，IC 卡发送一个序列号为 1 的 R 块（PCB 的 b5=1）；在收到第一个错误的带链接的 I 块后，IC 卡重发这个序列号为 1

的 R 块(PCB 的 b5=1);在收到第二个错误的带链接的 I 块后,IC 卡无响应(在 BWT+100% 以内)。

6.6.36 TPSGX20-00

测试目的:在终端发起的一个链接中,确保 IC 卡在发送完 R(ACK)块(序列号为 0)后,终端出现单次错误时,IC 卡响应正确。

测试条件:条件 4 或条件 5 为 T=1 协议。

测试流程:a)启动冷复位并接收 ATR;

b)发送和处理 S (IFS 请求/响应)块 (IFSD=254);

c)发送并处理一个交易中的命令,直到终端发送第一个带链接的序列号为 1 的 I 块 (PCB 的 b7=1, PCB 的 b6=1, LEN=IFSC),并接收 IC 卡响应;

d)发送第二个含有 EDC 错误的带链接的 I 块(指明链接或者发送链接中的最后一个块),并接收 IC 卡响应;

e)发送第二个正确的带链接的 I 块,并接收 IC 卡响应;

f)如果接受热复位 ATR,就在收到冷复位 ATR 后,启动热复位,并接收热复位 ATR。

通过标准:在接收到第一个带链接的 I 块(PCB 的 b6=1)后,IC 卡发送一个序列号为 0 的 R 块 (PCB 的 b5=1);在收到第二个错误的带链接的 I 块后,IC 卡返回一个序列号为 0 的 R 块(PCB 的 b5=0);在收到第二个正确的带链接的 I 块后,IC 卡返回一个序列号为 1 的 R 块(PCB 的 b5=1)或一个 I 块。

6.6.37 TPSGX21-00

测试目的:在终端发起的一个链接中,确保 IC 卡在发送完 R(ACK)块(序列号为 0)后,终端出现多次连续错误时,IC 卡没有响应。

测试条件:条件 4 或条件 5 为 T=1 协议。

测试流程:a)启动冷复位并接收 ATR;

b)发送和处理 S (IFS 请求/响应)块 (IFSD=254);

c)发送并处理一个交易中的命令,直到终端发送第一个带链接的序列号为 1 的 I 块 (PCB 的 b7=1, PCB 的 b6=1, LEN=IFSC),并接收 IC 卡响应;

d)发送第二个含有 EDC 错误的带链接的 I 块(指明链接或者发送链接中的最后一个块),并接收 IC 卡响应;

e)重发这个含有 EDC 错误的带链接的 I 块,并确保 IC 卡无响应;

f)如果接受热复位 ATR,就在收到冷复位 ATR 后,启动热复位,并接收热复位 ATR。

通过标准:在接收到第一个带链接的 I 块(PCB 的 b6=1)后,IC 卡发送一个序列号为 0 的 R 块 (PCB 的 b5=0);在收到第一个错误的带链接的 I 块后,IC 卡重发这个序列号为 0 的 R 块(PCB 的 b5=0);在收到第二个错误的带链接的 I 块后,IC 卡无响应(在 BWT+100% 以内)。

6.6.38 TPSGX22-00

测试目的:在终端发起的一个链接中,确保 IC 卡在收到错误通知时,正确地重发一个 R(ACK)的块(序列号为 0)。

测试条件:条件 4 或条件 5 为 T=1 协议。

测试流程:a)启动冷复位并接收 ATR;

b)发送和处理 S (IFS 请求/响应)块 (IFSD=254);

- c) 发送并处理一个交易中的命令，直到终端发送第一个带链接的序列号为 1 的 I 块（PCB 的 b7=1，PCB 的 b6=1，LEN=IFSC），并接收 IC 卡响应；
- d) 如果 IC 卡发送最后一个 I 块的序列号为 n（PCB 的 b7=n），就发送一个序列号为 n+1 的 R 块（PCB 的 b5=n+1）请求重发，并接收 IC 卡重发响应；
- e) 发送第二个带链接的 I 块（指明链接或者发送链接中的最后一个块），并接收 IC 卡响应；
- f) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：在接收到第一个带链接的 I 块（PCB 的 b6=1）后，IC 卡发送一个序列号为 0 的 R 块（PCB 的 b5=0）；在接收到请求重发的 R 块后，IC 卡重新发送这个 R 块（PCB 的 b5=0）；在收到第二个带链接的 I 块后，IC 卡返回一个序列号为 1 的 R 块（PCB 的 b5=1）或一个 I 块。

6.6.39 TP SGX03-00

测试目的：确保 IC 卡在收到 R(ACK) 块后，能正确地发送的一个带链接的 I 块（序列号为 0），并忽略 R(ACK) 块 PCB 的 b4 至 b1 位。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到 IC 卡发送一个带链接的序列号为 0 的 I 块（PCB 的 b7=0，PCB 的 b6=1）；

d) 发送一个序列号为 1 的 R 块（PCB 的 b5=1），并接收 IC 卡响应；

e) 如果需要，就继续处理接收到的所有带链接的 I 块（收到 PCB 的 b6=1，b7=n 的 I 块后，终端发送一个 PCB 的 b5=n+1 的 R 块）；

f) 在 IC 卡发送完最后一个链接块后（PCB 的 b6=0），终端发送一个正确的非链接的 I 块，并接收 IC 卡响应；

g) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：除最后一个链接块外，IC 卡发送的所有 I 块的 PCB 的 b6=1；IC 卡发送的最后一个链接 I 块的 PCB 的 b6=0；收到序列号为 n 的 R 块后（PCB 的 b5=n），IC 卡发送一个序列号为 n 的 I 块（PCB 的 b7=n）；在接收到下一个 I 块后，IC 卡返回一个 I 块。

6.6.40 TP SGX18-00

测试目的：确保 IC 卡在收到 R(ACK) 块后，能正确地发送的一个带链接的 I 块（序列号为 1），并忽略 R(ACK) 块 PCB 的 b4 至 b1 位。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到 IC 卡发送一个带链接的序列号为 1 的 I 块（PCB 的 b7=1，PCB 的 b6=1）；

d) 发送一个序列号为 0 的 R 块（PCB 的 b5=0），并接收 IC 卡响应；

e) 如果需要，就继续处理接收到的所有带链接的 I 块（收到 PCB 的 b6=1，b7=n 的 I 块后，终端发送一个 PCB 的 b5=n+1 的 R 块）；

f) 在 IC 卡发送完最后一个链接块后（PCB 的 b6=0），终端发送一个正确的非链接的 I 块，并接收 IC 卡响应；

g)如果接受热复位 ATR,就在收到冷复位 ATR 后,启动热复位,并接收热复位 ATR。

通过标准:除最后一个链接块外,IC 卡发送的所有 I 块的 PCB 的 b6=1;IC 卡发送的最后一个链接 I 块的 PCB 的 b6=0;收到序列号为 n 的 R 块后(PCB 的 b5=n),IC 卡发送一个序列号为 n 的 I 块(PCB 的 b7=n);在接收到下一个 I 块后,IC 卡返回一个 I 块。

6.6.41 TPSGX06-00

测试目的:确保 IC 卡在发送完带链接的 I 块(序列号为 0)之后,收到单次传输错误时响应正确。

测试条件:条件 4 或条件 5 为 T=1 协议。

测试流程:a)启动冷复位并接收 ATR;

b)发送和处理 S(IFS 请求/响应)块(IFSD=254);

c)发送并处理一个交易中的命令,直到 IC 卡发送一个带链接的序列号为 0 的 I 块(PCB 的 b6=1,PCB 的 b7=0);

d)发送一个错误的 R 块,并接收 IC 卡响应;

e)发送一个正确的序列号为 1 的 R(ACK)块(PCB 的 b5=1),并接收 IC 卡响应;

f)如果需要,就继续处理接收到的所有带链接的 I 块(收到 PCB 的 b6=1, b7=n 的 I 块后,终端发送一个 PCB 的 b5=n+1 的 R 块);

g)在 IC 卡发送完最后一个链接块后(PCB 的 b6=0),终端发送一个正确的非链接的 I 块,并接收 IC 卡响应;

h)如果接受热复位 ATR,就在收到冷复位 ATR 后,启动热复位,并接收热复位 ATR。

通过标准:如果终端发送的上一个 I 块的序列号为 n(PCB 的 b7=n),那么 IC 卡在收到错误的块之后,应当返回一个序列号为 n+1 的 R 块(PCB 的 b5=n+1);收到正确的 R(ACK)块后,IC 卡继续发送其余的链接块;在接收到下一个 I 块后,IC 卡返回一个 I 块。

6.6.42 TPSGX07-00

测试目的:确保 IC 卡在发送完带链接的 I 块(序列号为 0)之后,收到连续两次传输错误时响应正确。

测试条件:条件 4 或条件 5 为 T=1 协议。

测试流程:a)启动冷复位并接收 ATR;

b)发送和处理 S(IFS 请求/响应)块(IFSD=254);

c)发送并处理一个交易中的命令,直到 IC 卡发送一个带链接的序列号为 0 的 I 块(PCB 的 b6=1,PCB 的 b7=0);

d)发送一个带有 EDC 错误的 R 块(序列号为 1),并接收 IC 卡响应;

e)重发这个带有 EDC 错误的 R 块(序列号为 1),并接收 IC 卡响应;

f)发送正确的 R 块(序列号为 1),并接收 IC 卡响应;

g)如果需要,就继续处理接收到的所有带链接的 I 块(收到 PCB 的 b6=1, b7=n 的 I 块后,终端发送一个 PCB 的 b5=n+1 的 R 块);

h)在 IC 卡发送完最后一个链接块后(PCB 的 b6=0),终端发送一个正确的非链接的 I 块,并接收 IC 卡响应;

i)如果接受热复位 ATR,就在收到冷复位 ATR 后,启动热复位,并接收热复位 ATR。

通过标准:如果终端发送的上一个 I 块的序列号为 n(PCB 的 b7=n),那么 IC 卡在收到第一次带有 EDC 错误的 R 块后,应当返回一个序列号为 n+1 的 R 块(PCB 的 b5=n+1);IC 卡收到第二次带有 EDC 错误的 R 块之后,应当返回一个序列号为 n+1 的 R 块(PCB 的

b5=n+1)；收到正确的 R 块后，IC 卡继续发送其余的链接块；在接收到下一个 I 块后，IC 卡返回一个 I 块。

6.6.43 TPSGX08-00

测试目的：确保 IC 卡在发送完带链接的 I 块（序列号为 0）之后，收到超过两次传输错误时没有响应。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到 IC 卡发送一个带链接的序列号为 0 的 I 块（PCB 的 b6=1，PCB 的 b7=0）；

d) 发送一个带有 EDC 错误的 R 块（序列号为 1），并接收 IC 卡响应；

e) 重发这个带有 EDC 错误的 R 块（序列号为 1），并接收 IC 卡响应；

f) 再次重发这个带有 EDC 错误的 R 块（序列号为 1），并确保 IC 卡无响应；

g) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：如果终端发送的上一个 I 块的序列号为 n（PCB 的 b7=n），那么 IC 卡在收到第一次带有 EDC 错误的 R 块后，应当返回一个序列号为 n+1 的 R 块（PCB 的 b5=n+1）；IC 卡收到第二次带有 EDC 错误的 R 块之后，应当返回一个序列号为 n+1 的 R 块（PCB 的 b5=n+1）；在收到第三次带有 EDC 错误的 R 块之后，IC 卡无响应（在 BWT+100%以内）。

6.6.44 TPSGX09-00

测试目的：确保 IC 卡正确重发带链接的 I 块（序列号为 0）。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

b) 发送和处理 S（IFS 请求/响应）块（IFSD=254）；

c) 发送并处理一个交易中的命令，直到 IC 卡发送一个带链接的序列号为 0 的 I 块（PCB 的 b6=1，PCB 的 b7=0）；

d) 发送一个 R 块（序列号为 0），并接收 IC 卡重发块；

e) 发送一个确认的 R 块（序列号为 1），并接收 IC 卡响应；

f) 如果需要，就继续处理接收到的所有带链接的 I 块（收到 PCB 的 b6=1，b7=n 的 I 块后，终端发送一个 PCB 的 b5=n+1 的 R 块）；

g) 在 IC 卡发送完最后一个链接块后（PCB 的 b6=0），终端发送一个正确的非链接的 I 块，并接收 IC 卡响应；

h) 如果接受热复位 ATR，就在收到冷复位 ATR 后，启动热复位，并接收热复位 ATR。

通过标准：收到终端发送的上一个序列号为 0 的 R 块后（PCB 的 b5=0），IC 卡重发上一个 I 块；收到确认的 R 块后（序列号为 1），IC 卡继续发送其余的链接块；在接收到下一个 I 块后，IC 卡返回一个 I 块。

6.6.45 TPSGX12-00

测试目的：确保 IC 卡在发送完带链接的 I 块（序列号为 1）之后，收到单次传输错误时响应正确。

测试条件：条件 4 或条件 5 为 T=1 协议。

测试流程：a) 启动冷复位并接收 ATR；

- b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;
- c) 发送并处理一个交易中的命令,直到 IC 卡发送一个带链接的序列号为 1 的 I 块(PCB 的 b6=1, PCB 的 b7=1) ;
- d) 发送一个错误的 R 块, 并接收 IC 卡响应;
- e) 发送一个正确的序列号为 0 的 R (ACK) 块 (PCB 的 b5=0) , 并接收 IC 卡响应;
- f) 如果需要, 就继续处理接收到的所有带链接的 I 块 (收到 PCB 的 b6=1, b7=n 的 I 块后, 终端发送一个 PCB 的 b5=n+1 的 R 块) ;
- g) 在 IC 卡发送完最后一个链接块后 (PCB 的 b6=0) , 终端发送一个正确的非链接的 I 块, 并接收 IC 卡响应;
- h) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 如果终端发送的上一个 I 块的序列号为 n (PCB 的 b7=n) , 那么 IC 卡在收到错误的块之后, 应当返回一个序列号为 n+1 的 R 块 (PCB 的 b5=n+1) ; 收到正确的 R (ACK) 块后, IC 卡继续发送其余的链接块; 在接收到下一个 I 块后, IC 卡返回一个 I 块。

6.6.46 TPSGX13-00

测试目的: 确保 IC 卡在发送完带链接的 I 块 (序列号为 1) 之后, 收到连续两次传输错误时响应正确。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

- b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;
- c) 发送并处理一个交易中的命令,直到 IC 卡发送一个带链接的序列号为 1 的 I 块(PCB 的 b6=1, PCB 的 b7=1) ;
- d) 发送一个带有 EDC 错误的 R 块 (序列号为 0) , 并接收 IC 卡响应;
- e) 重发这个带有 EDC 错误的 R 块 (序列号为 0) , 并接收 IC 卡响应;
- f) 发送正确的 R 块 (序列号为 0) , 并接收 IC 卡响应;
- g) 如果需要, 就继续处理接收到的所有带链接的 I 块 (收到 PCB 的 b6=1, b7=n 的 I 块后, 终端发送一个 PCB 的 b5=n+1 的 R 块) ;
- h) 在 IC 卡发送完最后一个链接块后 (PCB 的 b6=0) , 终端发送一个正确的非链接的 I 块, 并接收 IC 卡响应;
- i) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 如果终端发送的上一个 I 块的序列号为 n (PCB 的 b7=n) , 那么 IC 卡在收到第一次带有 EDC 错误的 R 块后, 应当返回一个序列号为 n+1 的 R 块 (PCB 的 b5=n+1) ; IC 卡收到第二次带有 EDC 错误的 R 块之后, 应当返回一个序列号为 n+1 的 R 块 (PCB 的 b5=n+1) ; 收到正确的 R 块后, IC 卡继续发送其余的链接块; 在接收到下一个 I 块后, IC 卡返回一个 I 块。

6.6.47 TPSGX14-00

测试目的: 确保 IC 卡在发送完带链接的 I 块 (序列号为 1) 之后, 收到超过两次传输错误时没有响应。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

- b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;
- c) 发送并处理一个交易中的命令,直到 IC 卡发送一个带链接的序列号为 1 的 I 块(PCB

的 b6=1, PCB 的 b7=1) ;

d) 发送一个带有 EDC 错误的 R 块 (序列号为 0) , 并接收 IC 卡响应;

e) 重发这个带有 EDC 错误的 R 块 (序列号为 0) , 并接收 IC 卡响应;

f) 再次重发这个带有 EDC 错误的 R 块 (序列号为 0) , 并确保 IC 卡无响应;

g) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 如果终端发送的上一个 I 块的序列号为 n (PCB 的 b7=n) , 那么 IC 卡在收到第一次带有 EDC 错误的 R 块后, 应当返回一个序列号为 n+1 的 R 块 (PCB 的 b5=n+1) ; IC 卡收到第二次带有 EDC 错误的 R 块之后, 应当返回一个序列号为 n+1 的 R 块 (PCB 的 b5=n+1) ; 在收到第三次带有 EDC 错误的 R 块之后, IC 卡无响应 (在 BWT+100%以内)。

6.6.48 TPSGX15-00

测试目的: 确保 IC 卡正确重发带链接的 I 块 (序列号为 1) 。

测试条件: 条件 4 或条件 5 为 T=1 协议。

测试流程: a) 启动冷复位并接收 ATR;

b) 发送和处理 S (IFS 请求/响应) 块 (IFSD=254) ;

c) 发送并处理一个交易中的命令, 直到 IC 卡发送一个带链接的序列号为 1 的 I 块 (PCB 的 b6=1, PCB 的 b7=1) ;

d) 发送一个 R 块 (序列号为 1) , 并接收 IC 卡重发块;

e) 发送一个确认的 R 块 (序列号为 0) , 并接收 IC 卡响应;

f) 如果需要, 就继续处理接收到的所有带链接的 I 块 (收到 PCB 的 b6=1, b7=n 的 I 块后, 终端发送一个 PCB 的 b5=n+1 的 R 块) ;

g) 在 IC 卡发送完最后一个链接块后 (PCB 的 b6=0) , 终端发送一个正确的非链接的 I 块, 并接收 IC 卡响应;

h) 如果接受热复位 ATR, 就在收到冷复位 ATR 后, 启动热复位, 并接收热复位 ATR。

通过标准: 收到终端发送的上一个序列号为 1 的 R 块后 (PCB 的 b5=1) , IC 卡重发上一个 I 块; 收到确认的 R 块后 (序列号为 0) , IC 卡继续发送其余的链接块; 在接收到下一个 I 块后, IC 卡返回一个 I 块。

7 借记贷记应用测试的测试案例

7.1 标准联机交易

标准联机交易用于复位卡片中的各个计数器, 其流程如下:

——卡片上电 (ATR) ;

——选择 PBOC 借记/贷记应用;

——GET PROCESSING OPTIONS 命令;

——VERIFY 命令;

——第一个 GENERATE AC 命令请求 ARQC;

——EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;

——第二个 GENERATE AC 命令请求 TC。

7.2 应用锁定命令 (SDML)

7.2.1 SDML001-00

测试目的: 验证当 APPLICATION BLOCK 命令中 MAC 数据域的长度小于指定最小长度时, 该命令执

行失败。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；随后执行 APPLICATION BLOCK 命令，命令格式见表 9，该命令 MAC 数据域长度小于 MAC 的指定最小长度（Lc 的值为不正确的 MAC 长度）。

表9 APPLICATION BLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	1E	00	00	03	11 22 33	N/A

通过标准：卡片收到 APPLICATION BLOCK 命令后不应返回状态字‘9000’，推荐返回‘6700’。

7.2.2 SDML002-00

测试目的：验证当 APPLICATION BLOCK 命令中 MAC 数据域的长度大于指定最大长度时，该命令执行失败。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；随后执行 APPLICATION BLOCK 命令，命令格式见表 10，该命令数据域长度大于 MAC 的指定最大长度（Lc 的值为不正确的 MAC 长度）。

表10 APPLICATION BLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	1E	00	00	09	11 22 33 44 55 66 77 88 99	N/A

通过标准：卡片收到 APPLICATION BLOCK 命令后不应返回状态字‘9000’，推荐返回‘6700’。

7.2.3 SDML003-00

测试目的：验证当 APPLICATION BLOCK 命令中 MAC 数据错误时，该命令执行失败。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；随后执行 APPLICATION BLOCK 命令，命令格式见表 11，该命令数据域为错误的 MAC。

表11 APPLICATION BLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	1E	00	00	04	11 22 33 44	N/A

通过标准：卡片收到 APPLICATION BLOCK 命令后不应返回状态字‘9000’，推荐返回‘6988’。

7.2.4 SDML004-00

测试目的：验证当收到成功的 APPLICATION BLOCK 命令时，卡片返回状态字‘9000’。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；随后执行 APPLICATION BLOCK 命令，命令格式见表 12，该命令数据域为正确的 MAC。

表12 APPLICATION BLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	1E	00	00	04	正确的 mac	N/A

通过标准：卡片收到 APPLICATION BLOCK 命令后返回状态字‘9000’。

7.3 应用锁定（YYSD）

7.3.1 YYSD001-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片接受 APPLICATION BLOCK 命令。
验证在成功的执行 APPLICATION BLOCK 命令后，应用被锁定。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准，发卡行认证成功，APPLICATION BLOCK 命令成功；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；
j) APPLICATION BLOCK 命令，正确的 MAC；
k) 交易 3：选择锁定的 PBOC 借记/贷记应用；
l) 卡片上电（ATR）；
m) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到 APPLICATION BLOCK 命令后应返回状态字‘9000’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘6283’。

7.3.2 YYSD002-00

测试目的：验证当交易被联机拒绝，并且发卡行认证成功时，卡片接受 APPLICATION BLOCK 命令。
验证在成功的执行 APPLICATION BLOCK 命令后，应用被锁定。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机拒绝，发卡行认证成功，APPLICATION BLOCK 命令成功；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
i) 第二个 GENERATE AC 命令请求 AAC；
j) APPLICATION BLOCK 命令，正确的 MAC；
k) 交易 3：选择锁定的 PBOC 借记/贷记应用；
l) 卡片上电（ATR）；
m) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到 APPLICATION BLOCK 命令后应返回状态字‘9000’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘6283’。

7.3.3 YYSD003-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片拒绝 MAC 错误的 APPLICATION BLOCK 命令。

验证卡片不锁定应用。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，发卡行认证成功，APPLICATION BLOCK 命令失败；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

j) APPLICATION BLOCK 命令，错误的 MAC；

k) 交易 3：选择锁定的 PBOC 借记/贷记应用；

l) 卡片上电（ATR）。

m) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到 APPLICATION BLOCK 命令后不应返回状态字‘9000’，推荐返回‘6988’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘9000’。

7.3.4 YYS004-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片拒绝 MAC 缺失的 APPLICATION BLOCK 命令。

验证卡片不锁定应用。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，发卡行认证成功，APPLICATION BLOCK 命令失败；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

j) APPLICATION BLOCK 命令，MAC 缺失；

k) 交易 3：选择锁定的 PBOC 借记/贷记应用；

l) 卡片上电（ATR）；

m) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到 APPLICATION BLOCK 命令后不应返回状态字‘9000’，推荐返回‘6988’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘9000’。

7.3.5 YYS005-00

测试目的：验证当交易被联机批准，并且发卡行认证失败时，卡片拒绝 MAC 正确的 APPLICATION BLOCK 命令。验证卡片不锁定应用。

测试条件：卡片类型 1 支持 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准，发卡行认证失败，执行 APPLICATION BLOCK 命令；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，包括错误的 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；
j) APPLICATION BLOCK 命令，正确的 MAC；
k) 交易 3：联机批准，发卡行认证失败，执行 APPLICATION BLOCK 命令；
l) 卡片上电（ATR）；
m) 选择 PBOC 借记/贷记应用；
n) GET PROCESSING OPTIONS 命令；
o) VERIFY 命令；
p) 第一个 GENERATE AC 命令请求 ARQC；
q) EXTERNAL AUTHENTICATE 命令，包括错误的 ARPC；
r) 第二个 GENERATE AC 命令请求 TC；
s) APPLICATION BLOCK 命令，正确的 MAC；
t) 交易 4：选择锁定的 PBOC 借记/贷记应用；
u) 卡片上电（ATR）；
v) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 和 3 中卡片返回的状态字：卡片收到 APPLICATION BLOCK 命令后不应返回状态字‘9000’，推荐返回‘6985’。验证交易 4 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘9000’。

7.3.6 YYS006-00

测试目的：验证当交易被联机批准，并且未执行发卡行认证或者执行成功时，卡片接收 MAC 正确的 APPLICATION BLOCK 命令，并锁定应用。

测试条件：卡片类型 1，支持 APPLICATION BLOCK 命令

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准，发卡行认证未执行，执行 APPLICATION BLOCK 命令；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) 第二个 GENERATE AC 命令请求 TC；
i) APPLICATION BLOCK 命令，MAC 正确；
j) 交易 3：选择锁定的 PBOC 借记/贷记应用；

- k) 卡片上电 (ATR) ;
- l) 选择 PBOC 借记/贷记应用;
- m) 解锁应用;
- n) 交易 4: 联机批准, 发卡行认证失败, 执行 APPLICATION BLOCK 命令;
- o) 卡片上电 (ATR) ;
- p) 选择 PBOC 借记/贷记应用;
- q) GET PROCESSING OPTIONS 命令;
- r) VERIFY 命令;
- s) 第一个 GENERATE AC 命令请求 ARQC;
- t) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- u) 第二个 GENERATE AC 命令请求 TC;
- v) APPLICATION BLOCK 命令, 正确的 MAC;
- w) 交易 5: 选择锁定的 PBOC 借记/贷记应用;
- x) 卡片上电 (ATR) ;
- y) 选择 PBOC 借记/贷记应用;
- z) 解锁应用。

通过标准: 验证交易 2 和 4 中卡片返回的状态字: 卡片收到 APPLICATION BLOCK 命令后应返回状态字 '9000'。验证交易 3 和 5 中卡片返回的状态字: 卡片收到 SELECT 命令后应返回状态字 '6283'。

7.3.7 YYS007-00

测试目的: 验证当交易被联机批准, 并且发卡行认证成功时, 卡片接受第二个 GENERATE AC 命令前的 MAC 正确的 APPLICATION BLOCK 命令。

验证在成功的执行 APPLICATION BLOCK 命令后, 应用被锁定。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION BLOCK 命令。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 联机批准, 发卡行认证成功, 第二个 GENERATE AC 命令前执行 APPLICATION BLOCK 命令;
 - c) 卡片上电 (ATR) ;
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 命令请求 ARQC;
 - h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
 - i) APPLICATION BLOCK 命令, 正确的 MAC;
 - j) 第二个 GENERATE AC 命令请求 TC;
 - k) 交易 3: 选择锁定的 PBOC 借记/贷记应用;
 - l) 卡片上电 (ATR) ;
 - m) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片返回的状态字: 卡片收到 APPLICATION BLOCK 命令后应返回状态字 '9000'。验证交易 3 中卡片返回的状态字: 卡片收到 SELECT 命令后应返回状态字 '6283'。

7.3.8 YYS008-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片接受两个 MAC 正确的 APPLICATION BLOCK 命令。

验证在成功的执行 APPLICATION BLOCK 命令后，应用被锁定。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准，发卡行认证成功，执行两个成功的 APPLICATION BLOCK 命令；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；
j) APPLICATION BLOCK 命令，正确的 MAC；
k) APPLICATION BLOCK 命令，正确的 MAC；
l) 交易 3：选择锁定的 PBOC 借记/贷记应用；
m) 卡片上电（ATR）；
n) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到两个 APPLICATION BLOCK 命令后应返回状态字‘9000’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘6283’。

7.3.9 YYSD009-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片接受第一个 MAC 正确的 APPLICATION BLOCK 命令，拒绝第二个 MAC 错误的 APPLICATION BLOCK 命令。

验证在成功的执行 APPLICATION BLOCK 命令后，应用被锁定。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准，发卡行认证成功，执行一个成功的 APPLICATION BLOCK 命令和一个失败的 APPLICATION BLOCK 命令；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；
j) APPLICATION BLOCK 命令，正确的 MAC；
k) APPLICATION BLOCK 命令，错误的 MAC；
l) 交易 3：选择锁定的 PBOC 借记/贷记应用；
m) 卡片上电（ATR）；
n) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到第一个 APPLICATION BLOCK 命令后应返回

状态字‘9000’。卡片收到第二个 APPLICATION BLOCK 命令后不应返回状态字‘9000’，推荐返回‘6988’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘6283’。

7.3.10 YYS010-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片接受一个 MAC 正确的 APPLICATION UNBLOCK 命令和一个 MAC 正确的 APPLICATION BLOCK 命令。

验证在成功的执行 APPLICATION BLOCK 命令后，应用被锁定。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准，发卡行认证成功，执行一个成功的 APPLICATION UNBLOCK 命令和一个成功的 APPLICATION BLOCK 命令；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；
j) APPLICATION UNBLOCK 命令，正确的 MAC；
k) APPLICATION BLOCK 命令，正确的 MAC；
l) 交易 3：选择锁定的 PBOC 借记/贷记应用；
m) 卡片上电（ATR）；
n) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到 APPLICATION UNBLOCK 命令后应返回状态字‘9000’。卡片收到 APPLICATION BLOCK 命令后应返回状态字‘9000’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘6283’。

7.3.11 YYS011-00

测试目的：验证当 PBOC 借记/贷记应用锁定时，卡片接受发卡行认证成功后执行的 MAC 正确的 APPLICATION BLOCK 命令。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：锁定 PBOC 借记/贷记应用；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；
j) APPLICATION BLOCK 命令，正确的 MAC；
k) 交易 3：卡片强制交易拒绝；

- l) 卡片上电 (ATR) ;
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 ARQC, 卡片应返回 AAC;
- q) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- r) APPLICATION BLOCK 命令, 正确的 MAC。

通过标准: 验证交易 3 卡片返回的状态字: 卡片收到 APPLICATION BLOCK 命令后应返回状态字 ‘9000’。

7.3.12 YYS012-00

测试目的: 如果设置 ADA 中的 “如果 PIN 在本次交易中锁定, 应用锁定” 位, 验证在联机拒绝交易中当 PIN 尝试次数超限时, 卡片应锁定借记/贷记应用。

测试条件: 第 9 章中的卡片特征 19, 支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 当 PIN 尝试次数超限时拒绝脱机交易;
- c) 卡片上电 (ATR) ;
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令, 错误的 PIN;
- g) VERIFY 命令, 错误的 PIN;
- h) VERIFY 命令, 错误的 PIN;
- i) 第一个 GENERATE AC 命令请求 ARQC, 卡片返回 AAC;
- j) 交易 3: 脱机拒绝, 解锁应用解锁 PIN;
- k) 卡片上电 (ATR) ;
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) 第一个 GENERATE AC 命令请求 AAC;
- o) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- p) APPLICATION UNBLOCK 命令, 正确的 MAC;
- q) PIN CHANGE/UNBLOCK 命令, 正确的 MAC。

通过标准: 交易 2: 验证第一个 GENERATE AC 命令: SW1 SW2= ‘9000’ ; CID= ‘00’ ; CVR= ‘03 86 42 00’。交易 3: 卡片收到 SELECT 命令后应返回状态字 ‘6283’ ; 卡片收到 APPLICATION UNBLOCK 命令后应返回状态字 ‘9000’ ; 卡片收到 PIN CHANGE/UNBLOCK 命令后应返回状态字 ‘9000’ ; CID= ‘00’ ; CVR= ‘03 80 40 00’。

7.3.13 YYS013-00

测试目的: 如果设置 ADA 中的 “如果 PIN 在本次交易中锁定, 应用锁定” 位, 验证在联机批准交易中当 PIN 尝试次数减少时, 卡片不锁定借记/贷记应用。

测试条件: 第 9 章中的卡片特征 19, 支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准联机交易, 错误的 PIN 输入;
- c) 卡片上电 (ATR) ;

- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令, 错误的 PIN;
- g) VERIFY 命令, 错误的 PIN;
- h) VERIFY 命令, 正确的 PIN;
- i) 第一个 GENERATE AC 命令请求 ARQC;
- j) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- k) 第二个 GENERATE AC 命令请求 TC ;
- l) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器。

通过标准: 交易 2 验证第二个 GENERATE AC 命令: SW1 SW2= '9000' ; CID= '40' ; CVR= '03 64 00 00' ; 交易 3: 卡片收到 SELECT 命令后返回状态字不应为 '6283' ; 卡片收到 VERIFY 命令后应返回状态字 '9000' ; CVR= '03 64 00 00' 。

7.3.14 YYS014-00

测试目的: 验证当应用交易计数器超出最大值时, 应用锁定且不能解锁。

测试条件: 第 9 章中的卡片特征 24, 该配置的 ATC 从 'FFFD' 开始。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 请求脱机批准;
- c) 卡片上电 (ATR) ;
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) GENERATE AC 命令请求 TC;
- h) EXTERNAL AUTHENTICATE 命令;
- i) APPLICATION UNBLOCK 命令, 正确的 MAC;
- j) 交易 3: 请求脱机批准;
- k) 卡片上电 (ATR) ;
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) GENERATE AC 命令请求 TC。

通过标准: 交易 2: 片收到 GET PROCESSING OPTIONS 命令后不应返回状态字 '9000' , 推荐返回 '6985' ; GENERATE AC SW1 SW2= '6985' , 无密文返回; 卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字 '9000' , 推荐返回 '6985' 。交易 3: 卡片收到 SELECT 命令后应返回状态字 '6283' ; 卡片收到 VERIFY 命令后应返回状态字 '9000' ; GENERATE AC SW1 SW2= '6985' , 无密文返回。

7.3.15 YYS015-00

测试目的: 验证当第一个应用锁定时, 不影响第二个应用的正常使用。

测试条件: 第 9 章中的卡片特征 27, 该配置包括 AID 相同的两个应用。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 成功执行发卡行认证, 并执行应用锁定脚本;
- c) 卡片上电 (ATR) ;

- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) GENERATE AC 命令请求 TC;
- h) EXTERNAL AUTHENTICATE 命令;
- i) APPLICATION BLOCK 命令, 正确的 MAC;
- j) 交易 3: 请求脱机批准;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) GENERATE AC 命令请求 TC;
- p) 交易 4: 选择第二个应用 (A0000003330101) 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- q) 交易 5: 请求脱机批准;
- r) 卡片上电 (ATR);
- s) 选择 PBOC 借记/贷记应用;
- t) GET PROCESSING OPTIONS 命令;
- u) VERIFY 命令;
- v) GENERATE AC 命令请求 TC;
- w) EXTERNAL AUTHENTICATE 命令;
- x) APPLICATION UNBLOCK 命令, 正确的 MAC;
- y) 交易 6: 请求脱机批准;
- z) 卡片上电 (ATR);
- aa) 选择 PBOC 借记/贷记应用;
- ab) GET PROCESSING OPTIONS 命令;
- ac) VERIFY 命令;
- ad) GENERATE AC 命令请求 TC。

通过标准: 交易 1: 执行成功。交易 2: 卡片执行发卡行认证成功; 卡片执行应用锁定成功。交易 3: 卡片收到 SELECT 命令后应返回状态字 '6283'; 卡片收到 VERIFY 命令后应返回状态字 '9000'; GENERATE AC SW1 SW2= '6985', 无密文返回。交易 4: 执行成功。交易 5: 卡片收到 GET PROCESSING OPTIONS 命令后不应返回状态字 '9000', 推荐返回 '6985'; GENERATE AC SW1 SW2= '6985', 无密文返回; 卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字 '9000', 推荐返回 '6985'。交易 6: 卡片收到 SELECT 命令后应返回状态字 '6283'; 卡片收到 VERIFY 命令后应返回状态字 '9000'; GENERATE AC SW1 SW2= '6985', 无密文返回。

7.3.16 YYS016-00

测试目的: 验证当第一个应用锁定时, 不影响第二个应用的正常使用。

测试条件: 第 9 章中的卡片特征 27, 该配置包括 AID 相同的两个应用

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 成功执行发卡行认证, 并执行应用锁定脚本;

c) 卡片上电 (ATR);

- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) GENERATE AC 命令请求 TC;
- h) EXTERNAL AUTHENTICATE 命令;
- i) APPLICATION BLOCK 命令, 正确的 MAC;
- j) 交易 3: 请求脱机批准;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) GENERATE AC 命令请求 TC;
- p) 交易 4: 选择第二个应用 (A0000003330101) 执行发卡行认证成功的联机批准交易;
- q) 选择 PBOC 借记/贷记应用;
- r) GET PROCESSING OPTIONS 命令;
- s) VERIFY 命令;
- t) GENERATE AC 命令请求 ARPC;
- u) 外部认证命令;
- v) GENERATE AC 命令请求 TC;
- w) 执行应用解锁命令;
- x) 交易 5: 选择第一个应用请求脱机批准;
- y) 卡片上电 (ATR);
- z) 选择 PBOC 借记/贷记应用;
- aa) GET PROCESSING OPTIONS 命令;
- ab) VERIFY 命令;
- ac) GENERATE AC 命令请求 TC;
- ad) 交易 6: 选择第二个应用 (A0000003330101) 执行发卡行认证成功的联机批准交易;
- ae) 选择 PBOC 借记/贷记应用;
- af) GET PROCESSING OPTIONS 命令;
- ag) VERIFY 命令;
- ah) GENERATE AC 命令请求 ARPC;
- ai) 外部认证命令;
- aj) GENERATE AC 命令请求 TC;
- ak) 执行应用解锁命令;
- al) 交易 7: 请求脱机批准;
- am) 卡片上电 (ATR);
- an) 选择 PBOC 借记/贷记应用;
- ao) GET PROCESSING OPTIONS 命令;
- ap) VERIFY 命令;
- aq) GENERATE AC 命令请求 TC。

通过标准: 交易 1: 执行成功。交易 2: 卡片执行发卡行认证成功。卡片执行应用锁定成功。交

易 3: 卡片收到 SELECT 命令后应返回状态字 ‘6283’ ; 卡片收到 VERIFY 命令后应返回状态字 ‘9000’ ; GENERATE AC SW1 SW2= ‘6985’ , 无密文返回。交易 4: 执行成功,应用解锁脚本返回‘9000’。交易 5: 卡片收到 SELECT 命令后应返回状态字 ‘6283’ ; 卡片收到 VERIFY 命令后应返回状态字 ‘9000’ ; GENERATE AC SW1 SW2= ‘6985’ , 无密文返回。交易 6: 应用解锁命令执行成功。交易 7: 卡片收到 SELECT 命令后应返回状态字 ‘6283’ 。卡片收到 VERIFY 命令后应返回状态字 ‘9000’ 。GENERATE AC SW1 SW2= ‘6985’ , 无密文返回。

7.3.17 YYS017-00

测试目的: 验证当第一个应用锁定时, 不影响第二个应用的正常使用。

测试条件: 第 9 章中的卡片特征 27, 该配置包括 AID 相同的两个应用

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 成功执行发卡行认证, 并执行应用锁定脚本;

c) 卡片上电 (ATR) ;

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) GENERATE AC 命令请求 TC;

h) EXTERNAL AUTHENTICATE 命令;

i) APPLICATION BLOCK 命令, 正确的 MAC;

j) 交易 3: 请求脱机批准;

k) 卡片上电 (ATR) ;

l) 选择 PBOC 借记/贷记应用;

m) GET PROCESSING OPTIONS 命令;

n) VERIFY 命令;

o) GENERATE AC 命令请求 TC;

p) 交易 4: 选择第二个应用 (A0000003330101) 执行发卡行认证成功的联机批准交易;

q) 选择 PBOC 借记/贷记应用;

r) GET PROCESSING OPTIONS 命令;

s) VERIFY 命令;

t) GENERATE AC 命令请求 ARPC;

u) 外部认证命令;

v) GENERATE AC 命令请求 TC;

w) 执行应用锁定命令;

x) 交易 5: 选择第一个应用请求脱机批准;

y) 卡片上电 (ATR) ;

z) 选择 PBOC 借记/贷记应用;

aa) GET PROCESSING OPTIONS 命令;

ab) VERIFY 命令;

ac) GENERATE AC 命令请求 TC;

ad) 选择第二个应用请求脱机批准;

ae) 卡片上电 (ATR) ;

- af) 选择 PBOC 借记/贷记应用;
- ag) GET PROCESSING OPTIONS 命令;
- ah) VERIFY 命令;
- ai) GENERATE AC 命令请求 TC;
- aj) 交易 6: 选择第一个应用 (A0000003330101) 执行发卡行认证成功的联机批准交易;
- ak) 并执行应用解锁;
- al) 交易 7: 选择第一个应用 (A0000003330101) 执行发卡行认证成功的联机批准交易;
- am) 选择 PBOC 借记/贷记应用;
- an) GET PROCESSING OPTIONS 命令;
- ao) VERIFY 命令;
- ap) GENERATE AC 命令请求 ARPC;
- aq) 外部认证命令;
- ar) GENERATE AC 命令请求 TC;
- as) 交易 8: 选择第二个应用 (A0000003330101) 请求脱机批准;
- at) 卡片上电 (ATR) ;
- au) 选择 PBOC 借记/贷记应用;
- av) GET PROCESSING OPTIONS 命令;
- aw) VERIFY 命令;
- ax) GENERATE AC 命令请求 TC。

通过标准: 交易 1: 执行成功。交易 2: 卡片执行发卡行认证成功; 卡片执行应用锁定成功。交易 3: 卡片收到 SELECT 命令后应返回状态字 '6283'。卡片收到 VERIFY 命令后应返回状态字 '9000'。GENERATE AC SW1 SW2= '6985', 无密文返回。交易 4: 执行成功, 应用锁定命令执行成功。交易 5: 卡片收到 SELECT 命令后应返回状态字 '6283'。卡片收到 VERIFY 命令后应返回状态字 '9000'。GENERATE AC SW1 SW2= '6985', 无密文返回。卡片收到 SELECT 命令后应返回状态字 '6283'。卡片收到 VERIFY 命令后应返回状态字 '9000'。GENERATE AC SW1 SW2= '6985', 无密文返回。交易 6: 应用解锁命令执行成功。交易 7: GAC、外部认证命令执行成功。交易 8: 卡片收到 SELECT 命令后应返回状态字 '6283'。卡片收到 VERIFY 命令后应返回状态字 '9000'。GENERATE AC SW1 SW2= '6985', 无密文返回。

7.4 读应用数据 (DQSJ)

7.4.1 DQSJ001-00

测试目的: 验证 GET PROCESSING OPTIONS 命令后卡片响应所有 READ RECORD 命令的状态字。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR) ;

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) READ RECORD 命令。

通过标准: 所有 SW1 SW2= '9000'。

7.4.2 DQSJ002-00

测试目的：验证 GET PROCESSING OPTIONS 命令后卡片响应所有 READ RECORD 命令的记录模板。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：每个记录模板的标签标签=‘70’；每个记录模板的长度小于等于 252。

7.4.3 DQSJ003-00

测试目的：验证卡片响应 READ RECORD 命令的应用自定义数据。

测试条件：第 9 章中的卡片特征 1，存在应用自定义数据。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：应用自定义数据的长度范围为‘01’至‘20’（标签为‘9F05’）。

7.4.4 DQSJ004-00

测试目的：验证卡片响应 READ RECORD 命令的应用生效日期。

测试条件：第 9 章中的卡片特征 1，存在应用生效日期。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：应用生效日期的长度=‘03’（标签为‘5F25’）；应用生效日期的值=‘95 07 01’。

7.4.5 DQSJ005-00

测试目的：验证卡片响应 READ RECORD 命令的应用失效日期。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：应用失效日期的长度=‘03’（标签为‘5F24’）；应用失效日期的值=‘30 12 31’；在磁条 2 等效数据（标签为‘57’）中的应用失效日期值=‘XX XX XX XX XX XX XX XX D3 01 2X XX…’。

7.4.6 DQSJ006-00

测试目的：验证卡片响应 READ RECORD 命令的应用主账号。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；

d) READ RECORD 命令。

通过标准：应用主账号的长度=‘08’（标签为‘5A’）；应用主账号的值=‘62 28 00 01 00 00 11 17’；在磁条 2 等效数据（标签为‘57’）中的应用主账号值=‘62 28 00 01 00 00 11 17 DX XX XX XX…’。

7.4.7 DQSJ007-00

测试目的：验证卡片响应 READ RECORD 命令的应用主账号序列号。

测试条件：第 9 章中的卡片特征 1，如果应用主账号序列号存在。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：应用主账号序列号的长度=‘01’（标签为‘5F34’）；应用主账号序列号的值=‘01’。

7.4.8 DQSJ008-00

测试目的：验证卡片响应 READ RECORD 命令的应用用途控制。

测试条件：第 9 章中的卡片特征 1，应用用途控制存在。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：应用用途控制的长度=‘02’（标签为‘9F07’）；应用用途控制的值=‘FF C0’。

7.4.9 DQSJ009-00

测试目的：验证卡片响应 READ RECORD 命令的应用版本号。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：应用版本号的长度=‘02’（标签为‘9F08’）；应用版本号的值=‘00 8C’。

7.4.10 DQSJ010-00

测试目的：验证卡片响应 READ RECORD 命令的持卡人姓名扩展。

测试条件：第 9 章中的卡片特征 1，持卡人姓名扩展存在。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：持卡人姓名扩展的长度范围为‘1B’至‘2D’（标签为‘9F0B’）；持卡人姓名扩展的值为字母数字的特殊格式。

7.4.11 DQSJ011-00

测试目的：验证卡片响应 READ RECORD 命令的 CVM 列表。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：CVM 列表的长度=‘12’（标签为‘8E’）；CVM 列表的值=‘00 00 00 00 00 00 00 00 41 03 42 03 5E 03 43 03 1F 00’。

7.4.12 DQSJ012-00

测试目的：验证卡片响应 READ RECORD 命令的 CDOL1。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：CDOL1 的长度=‘15’（标签为‘8C’）；CDOL1 的值=‘9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04’。

7.4.13 DQSJ013-00

测试目的：验证卡片响应 READ RECORD 命令的 CDOL2。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：CDOL1 的长度=‘17’（标签为‘8D’）；CDOL1 的值=‘8A 02 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04’。

7.4.14 DQSJ014-00

测试目的：验证卡片响应 READ RECORD 命令的发卡行行为代码-缺省。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：发卡行行为代码-缺省的长度=‘05’（标签为‘9F0D’）；发卡行行为代码-缺省的值=‘F0 20 04 00 00’。

7.4.15 DQSJ015-00

测试目的：验证卡片响应 READ RECORD 命令的发卡行行为代码-拒绝。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；

- b) 选择 PBOC 借记/贷记应用;
- c) GET PROCESSING OPTIONS 命令;
- d) READ RECORD 命令。

通过标准: 发卡行行为代码-拒绝的长度= '05' (标签为 '9F0E'); 发卡行行为代码-拒绝的值= '00 05 88 00 00'。

7.4.16 DQSJ016-00

测试目的: 验证卡片响应 READ RECORD 命令的发卡行行为代码-联机。

测试条件: 第9章中的卡片特征1。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) READ RECORD 命令。

通过标准: 发卡行行为代码-联机的长度= '05' (标签为 '9F0F'); 发卡行行为代码-联机的值= 'F0 20 04 98 00'。

7.4.17 DQSJ017-00

测试目的: 验证卡片响应 READ RECORD 命令的发卡行国家代码。

测试条件: 第9章中的卡片特征1, AUC 存在。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) READ RECORD 命令。

通过标准: 发卡行国家代码的长度= '02' (标签为 '5F28'); 发卡行国家代码的值= '01 56'。

7.4.18 DQSJ018-00

测试目的: 验证卡片响应 READ RECORD 命令的服务码。

测试条件: 第9章中的卡片特征1, 服务码存在。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) READ RECORD 命令。

通过标准: 服务码的长度= '02' (标签为 '5F30'); 服务码的值= '02 01'。

7.4.19 DQSJ019-00

测试目的: 验证卡片响应 READ RECORD 命令的 LCOL。

测试条件: 第9章中的卡片特征1, 卡片支持终端频度检查。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) READ RECORD 命令。

通过标准: LCOL= '03' (标签为 '9F14')。

7.4.20 DQSJ020-00

测试目的：验证卡片响应 READ RECORD 命令的 UCOL。

测试条件：第 9 章中的卡片特征 1，卡片支持终端频度检查。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：UCOL= '07' (标签为 '9F23')。

7.4.21 DQSJ021-00

测试目的：验证当 PBOC 借记/贷记应用锁定时，在 GET PROCESSING OPTIONS 命令后卡片接受 READ RECORD 命令。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 APPLICATION BLOCK 命令，应用锁定。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：卡片收到 SELECT 命令后应返回状态字 '6283'；卡片收到 READ RECORD 命令后应返回状态字 '9000'。

7.4.22 DQSJ022-00

测试目的：验证当卡锁定时，卡片拒绝 READ RECORD 命令。

测试条件：第 9 章中的卡片特征 1，支持 CARD BLOCK 命令，卡锁定。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PSE；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) READ RECORD 命令。

通过标准：卡片收到 SELECT PSE 命令后应返回状态字 '6A81'；卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 '6A81'；卡片收到 READ RECORD 命令后不应返回状态字 '9000'，推荐返回 '6985' 或 '6A81'。

7.5 获取应用数据 (HQSJ)

7.5.1 HQSJ001-00

测试目的：验证卡片接受获取 ATC 的 GET DATA 命令。

测试条件：第 9 章中的卡片特征 1，卡片支持终端频度检查。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) GET DATA 命令获取 '9F36'。

通过标准：SW1 SW2= '9000'。

7.5.2 HQSJ002-00

测试目的：验证卡片接受获取 LOATC 的 GET DATA 命令。

测试条件：第 9 章中的卡片特征 1，卡片支持终端频度检查。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) GET DATA 命令获取 ‘9F13’。

通过标准：SW1 SW2= ‘9000’。

7.5.3 HQSJ003-00

测试目的：验证卡片接受获取 PIN 尝试计数器的 GET DATA 命令。

测试条件：第 9 章中的卡片特征 1，卡片脱机 PIN。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) GET DATA 命令获取 ‘9F17’。

通过标准：响应= ‘9F 17 01 03 90 00’。

7.6 PBOC 借记/贷记应用选择 (YYXZ)

7.6.1 YYXZ001-00

测试目的：验证 PBOC 借记/贷记应用选择成功后，卡片返回 FCI 模板。

测试条件：第 9 章中的卡片特征 1。

测试流程：发送选择 PBOC 借记/贷记应用的 SELECT 命令。

通过标准：FCI 模板的标签= ‘6F’；FCI 模板的长度最大为 252。

7.6.2 YYXZ002-00

测试目的：验证 PBOC 借记/贷记应用选择成功后，卡片返回 DF 名。

测试条件：第 9 章中的卡片特征 1。

测试流程：发送选择 PBOC 借记/贷记应用的 SELECT 命令。

通过标准：DF 名的标签= ‘84’；DF 名的长度= ‘07’；DF 名的值= ‘A0 00 00 03 33 01 01’。

7.6.3 YYXZ003-00

测试目的：验证 PBOC 借记/贷记应用选择成功后，卡片返回 FCI 专用模板。

测试条件：第 9 章中的卡片特征 1。

测试流程：发送选择 PBOC 借记/贷记应用的 SELECT 命令。

通过标准：FCI 专用模板的标签= ‘A5’。

7.6.4 YYXZ004-00

测试目的：验证 PBOC 借记/贷记应用选择成功后，卡片返回应用优先指示器。

测试条件：第 9 章中的卡片特征 1。

测试流程：发送选择 PBOC 借记/贷记应用的 SELECT 命令。

通过标准：应用优先指示器的标签= ‘87’；应用优先指示器的长度= ‘01’；应用优先指示器的值= ‘01’。

7.6.5 YYXZ005-00

测试目的：验证 PBOC 借记/贷记应用选择成功后，卡片返回 PDOL。

测试条件：第 9 章中的卡片特征 1。

测试流程：发送选择 PBOC 借记/贷记应用的 SELECT 命令。

通过标准：PDOL 的标签=‘9F38’；PDOL 的值=‘9F 1A 02’。

7.6.6 YYXZ006-00

测试目的：验证 PBOC 借记/贷记应用选择成功后，卡片返回 FCI 发卡行自定义数据。

测试条件：第 9 章中的卡片特征 1，FCI 发卡行自定义数据存在。

测试流程：发送选择 PBOC 借记/贷记应用的 SELECT 命令。

通过标准：FCI 发卡行自定义数据的标签=‘BF0C’；FCI 发卡行自定义数据的长度最大为 222 字节。

7.6.7 YYXZ007-00

测试目的：验证当终端在一个有效的 PSE 选择后选择一个无效的 PBOC 借记/贷记应用，卡片返回警告状态字。

测试条件：第 9 章中的卡片特征 1，卡片支持 APPLICATION UNBLOCK 和 APPLICATION BLOCK 命令，支持 PSE，卡片 PBOC 借记/贷记应用锁定。

测试流程：a) 卡片上电 (ATR)；

b) 选择 PSE；

c) 选择无效的 PBOC 借记/贷记应用。

通过标准：卡片收到 SELECT PSE 命令后应返回状态字‘9000’；卡片收到 PBOC 借记/贷记应用选择命令后应返回状态字‘6283’。

7.6.8 YYXZ008-00

测试目的：验证当卡锁定时，终端选择无效的 PSE 后，PBOC 借记/贷记应用无效。

测试条件：第 9 章中的卡片特征 1，卡片支持 CARD BLOCK 和 PSE，卡锁定。

测试流程：a) 卡片上电 (ATR)；

b) 选择无效的 PSE；

c) 选择无效的 PBOC 借记/贷记应用。

通过标准：卡片收到 SELECT PSE 命令后应返回状态字‘6A81’；卡片收到 PBOC 借记/贷记应用选择命令后应返回状态字‘6A81’。

7.6.9 YYXZ009-00

测试目的：验证当卡锁定时，PBOC 借记/贷记应用无效。

测试条件：第 9 章中的卡片特征 1，卡片支持 CARD BLOCK，卡锁定。

测试流程：a) 卡片上电 (ATR)；

b) 选择 PBOC 借记/贷记应用。

通过标准：卡片收到 PBOC 借记/贷记应用选择命令后应返回状态字‘6A81’。

7.6.10 YYXZ010-00

测试目的：卡片锁定状态不变，验证当执行锁应用交易后，PBOC 借记/贷记应用无效。

测试条件：第 9 章中的卡片特征 1，卡片支持 CARD BLOCK，PBOC 借记/贷记应用已锁定。

测试流程：选择无效 PBOC 借记/贷记应用的 SELECT 命令。

通过标准：卡片收到 PBOC 借记/贷记应用选择命令后应返回状态字 ‘6283’。

7.6.11 YYXZ011-00

测试目的：卡片锁定状态不变，验证当执行卡锁定交易后，PBOC 借记/贷记应用无效。

测试条件：第 9 章中的卡片特征 1，卡片支持 CARD BLOCK。

测试流程：a) 选择 PBOC 借记/贷记应用；
b) GET PROCESSING OPTIONS 命令；
c) VERIFY 命令（若支持）；
d) 第一个 GENERATE AC 命令请求 ARQC；
e) EXTERNAL AUTHENTICATE 命令；
f) 第二个 GENERATE AC 命令请求 TC 或 AAC；
g) CARD BLOCK 命令；
h) 选择无效的 PBOC 借记/贷记应用。

通过标准：卡片收到第二个 PBOC 借记/贷记应用选择命令后应返回状态字 ‘6A81’。

7.6.12 YYXZ012-00

测试目的：具有相同 AID 的应用（部分匹配）。

测试条件：第 9 章中的卡片特征 27。

测试流程：a) 交易 1：联机批准交易，但发卡行认证不成功；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 执行 EXTERNAL AUTHENTICATE 命令，ARPC 错误；
h) 第一个 GENERATE AC 命令请求 TC；
i) 交易 2：终端请求联机交易但不能执行联机，且拒绝脱机交易；
j) 卡片上电 (ATR)；
k) 选择 PBOC 借记/贷记应用；
l) GET PROCESSING OPTIONS 命令；
m) VERIFY 命令；
n) 第一个 GENERATE AC 命令请求 ARQC；
o) 第二个 GENERATE AC 命令请求 AAC，ARC=Z3；
p) 交易 3：P2=02 选择应用 2，执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
q) 交易 4：P2=02 选择应用 2，请求脱机批准；
r) 卡片上电 (ATR)；
s) 选择 PBOC 借记/贷记应用；
t) GET PROCESSING OPTIONS 命令；
u) VERIFY 命令；
v) GENERATE AC 命令请求 TC；
w) EXTERNAL AUTHENTICATE 命令；

- x) APPLICATION UNBLOCK 命令, 正确的 MAC;
- y) 交易 5: P2=02 选择应用 2, 请求脱机批准;
- z) 卡片上电 (ATR);
- aa) 选择 PBOC 借记/贷记应用;
- ab) GET PROCESSING OPTIONS 命令;
- ac) VERIFY 命令;
- ad) GENERATE AC 命令请求 TC;
- ae) 交易 6: 选择应用 1 进行正常交易。

通过标准: 交易 1、交易 2: SW1 SW2= '9000'; CID 位 8-7= '00'; CVR 字节 2 高半字节= '2'; CVR 字节 2 位 1= '1'; CVR 字节 3 位 6= '1'; CVR= '03 25 20 00' 或 '03 21 20 00' (用于未校验 PIN); 交易 3: 应用选择和 GAC, SW1 SW2= '9000'。交易 4: 卡片收到 GET PROCESSING OPTIONS 命令后不应返回状态字 '9000', 推荐返回 '6985'; GENERATE AC SW1 SW2= '6985', 无密文返回; 卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字 '9000', 推荐返回 '6985'。交易 5: 卡片收到 SELECT 命令后应返回状态字 '6283'; 卡片收到 VERIFY 命令后应返回状态字 '9000'; GENERATE AC SW1 SW2= '6985', 无密文返回。交易 6: 应用选择和 GAC, SW1 SW2= '9000'。

7.6.13 YYXZ013-00

测试目的: 具有相同 AID 的应用 (完全匹配)。

测试条件: 第 9 章中的卡片特征 27。

测试流程: a) 交易 1: 联机批准交易, 但发卡行认证不成功;

- b) 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 错误;
- h) 第一个 GENERATE AC 命令请求 TC;
- i) 交易 2: 终端请求联机交易但不能执行联机, 且拒绝脱机交易;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 命令请求 ARQC;
- o) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- p) 交易 3: P2=02 选择应用 2, 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- q) 交易 4: P2=02 选择应用 2, 请求脱机批准;
- r) 卡片上电 (ATR);
- s) 选择 PBOC 借记/贷记应用;
- t) GET PROCESSING OPTIONS 命令;
- u) VERIFY 命令;
- v) GENERATE AC 命令请求 TC;

- w) EXTERNAL AUTHENTICATE 命令;
- x) APPLICATION UNBLOCK 命令, 正确的 MAC;
- y) 交易 5: P2=02 选择应用 2, 请求脱机批准;
- z) 卡片上电 (ATR);
- aa) 选择 PBOC 借记/贷记应用;
- ab) GET PROCESSING OPTIONS 命令;
- ac) VERIFY 命令;
- ad) GENERATE AC 命令请求 TC;
- ae) 交易 6: 选择应用 1 进行正常交易。

通过标准: 交易 1、交易 2: SW1 SW2= ‘9000’。CID 位 8-7= ‘00’; CVR 字节 2 高半字节= ‘2’; CVR 字节 2 位 1= ‘1’; CVR 字节 3 位 6= ‘1’; CVR= ‘03 25 20 00’ 或 ‘03 21 20 00’ (用于未校验 PIN)。交易 3: 应用选择和 GAC, SW1 SW2= ‘9000’。交易 4: 卡片收到 GET PROCESSING OPTIONS 命令后不应返回状态字 ‘9000’, 推荐返回 ‘6985’; GENERATE AC SW1 SW2= ‘6985’, 无密文返回; 卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字 ‘9000’, 推荐返回 ‘6985’。交易 5: 卡片收到 SELECT 命令后应返回状态字 ‘6283’; 卡片收到 VERIFY 命令后应返回状态字 ‘9000’; GENERATE AC SW1 SW2= ‘6985’, 无密文返回。交易 6: 应用选择和 GAC, SW1 SW2= ‘9000’。

7.7 应用解锁命令(JSML)

7.7.1 JSML001-00

测试目的: 验证当 APPLICATION UNBLOCK 命令中 MAC 数据域的长度小于指定最小长度时, 该命令执行失败。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

测试流程: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器; 随后执行 APPLICATION UNBLOCK 命令, 命令格式见表 13, 该命令数据域长度小于 MAC 的指定最小长度 (Lc 的值为不正确的 MAC 长度)。

表13 APPLICATION UNBLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	18	00	00	03	11 22 33	N/A

通过标准: 卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字 ‘9000’, 推荐返回 ‘6700’。

7.7.2 JSML002-00

测试目的: 验证当 APPLICATION UNBLOCK 命令中 MAC 数据域的长度大于指定最大长度时, 该命令执行失败。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

测试流程: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器; 随后执行 APPLICATION UNBLOCK 命令, 命令格式见表 14, 该命令数据域长度大于 MAC 的指定最大长度 (Lc 的值为不正确的 MAC 长度)。

表14 APPLICATION UNBLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	18	00	00	09	11 22 33 44 55 66 77 88 99	N/A

通过标准: 卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字 ‘9000’, 推荐返回 ‘6700’。

7.7.3 JSML003-00

测试目的：验证当 APPLICATION UNBLOCK 命令中 MAC 数据错误时，该命令执行失败。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令。

测试流程：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；随后执行 APPLICATION UNBLOCK 命令，命令格式见表 15，该命令数据域为错误的 MAC。

表15 APPLICATION UNBLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	18	00	00	04	11 22 33 44	N/A

通过标准：卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字‘9000’，推荐返回‘6988’。

7.7.4 JSML004-00

测试目的：验证当收到成功的 APPLICATION UNBLOCK 命令时，卡片返回状态字‘9000’。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令。

测试流程：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；随后执行 APPLICATION UNBLOCK 命令，命令格式见表 16，该命令数据域为正确的 MAC。

表16 APPLICATION UNBLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	18	00	00	04	正确的 MAC	N/A

通过标准：卡片收到 APPLICATION UNBLOCK 命令后返回状态字‘9000’。

7.8 应用解锁 (YYJS)

7.8.1 YYJS001-00

测试目的：应用已锁定。终端在第一个 GENERATE AC 命令中请求联机，卡片拒绝交易。验证在成功的发卡行认证后，卡片接受 MAC 正确的 APPLICATION UNBLOCK 命令。

验证应用解锁成功。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令。

测试流程：a) 交易 1：锁定 PBOC 借记/贷记应用；

b) 卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

h) 第二个 GENERATE AC 命令请求 TC；

i) APPLICATION BLOCK 命令，正确的 MAC；

j) 交易 2：脱机拒绝，APPLICATION UNBLOCK 命令成功；

k) 卡片上电 (ATR)；

l) 选择 PBOC 借记/贷记应用；

m) GET PROCESSING OPTIONS 命令；

n) VERIFY 命令；

o) 第一个 GENERATE AC 命令请求 ARQC，卡片返回 AAC；

p) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

- q) APPLICATION UNBLOCK 命令, 正确的 MAC;
- r) 交易 3: 选择 PBOC 借记/贷记应用;
- s) 卡片上电 (ATR);
- t) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片返回的状态字: 卡片收到 APPLICATION UNBLOCK 命令后应返回状态字 '9000'。验证交易 3 中卡片返回的状态字: 卡片收到 SELECT 命令后应返回状态字 '9000'。

7.8.2 YYJS002-00

测试目的: 应用已锁定。终端在第一个 GENERATE AC 命令中请求联机, 卡片拒绝交易。验证在成功的发卡行认证后, 卡片拒绝 MAC 错误的 APPLICATION UNBLOCK 命令。
验证应用解锁失败。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

- 测试流程:
- a) 交易 1: 锁定 PBOC 借记/贷记应用;
 - b) 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 命令请求 ARQC;
 - g) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
 - h) 第二个 GENERATE AC 命令请求 TC;
 - i) APPLICATION BLOCK 命令, 正确的 MAC;
 - j) 交易 2: 卡片拒绝交易, MAC 错误的 APPLICATION UNBLOCK 命令失败;
 - k) 卡片上电 (ATR);
 - l) 选择 PBOC 借记/贷记应用;
 - m) GET PROCESSING OPTIONS 命令;
 - n) VERIFY 命令;
 - o) 第一个 GENERATE AC 命令请求 ARQC, 卡片返回 AAC;
 - p) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
 - q) APPLICATION UNBLOCK 命令, 错误的 MAC;
 - r) 交易 3: 选择无效的 PBOC 借记/贷记应用;
 - s) 卡片上电 (ATR);
 - t) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片返回的状态字: 卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字 '9000', 推荐返回 '6988'。验证交易 3 中卡片返回的状态字: 卡片收到 SELECT 命令后应返回状态字 '6283'。

7.8.3 YYJS003-00

测试目的: 应用已锁定。终端在第一个 GENERATE AC 命令中请求联机, 卡片拒绝交易。验证在成功的发卡行认证后, 卡片拒绝 MAC 缺失的 APPLICATION UNBLOCK 命令。
验证应用解锁失败。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

- 测试流程: a) 交易 1: 锁定 PBOC 借记/贷记应用;

- b) 卡片上电 (ATR) ;
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) APPLICATION BLOCK 命令, 正确的 MAC;
- j) 交易 2: 卡片拒绝交易, MAC 缺失的 APPLICATION UNBLOCK 命令执行失败;
- k) 卡片上电 (ATR) ;
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC, 卡片返回 AAC;
- p) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- q) APPLICATION UNBLOCK 命令, MAC 缺失;
- r) 交易 3: 选择无效的 PBOC 借记/贷记应用;
- s) 卡片上电 (ATR) ;
- t) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片返回的状态字: 卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字 '9000', 推荐返回 '6700', '6987' 或 '6988'。验证交易 3 中卡片返回的状态字: 卡片收到 SELECT 命令后应返回状态字 '6283'。

7.8.4 YYJS004-00

测试目的: 应用已锁定。终端在第一个 GENERATE AC 命令中请求联机, 卡片拒绝交易。验证在失败的发卡行认证后, 卡片拒绝 MAC 正确的 APPLICATION UNBLOCK 命令。
验证应用解锁失败。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

测试流程: a) 交易 1: 锁定 PBOC 借记/贷记应用;

- b) 卡片上电 (ATR) ;
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) APPLICATION BLOCK 命令, 正确的 MAC;
- j) 交易 2: 卡片拒绝交易。失败的发卡行认证后, 执行 APPLICATION UNBLOCK 命令;
- k) 卡片上电 (ATR) ;
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC, 卡片返回 AAC;

- p) EXTERNAL AUTHENTICATE 命令，包括错误的 ARPC；
- q) APPLICATION UNBLOCK 命令，正确的 MAC；
- r) 交易 3：选择无效的 PBOC 借记/贷记应用；
- s) 卡片上电（ATR）；
- t) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到 APPLICATION UNBLOCK 命令后不应返回状态字‘9000’，推荐返回‘6982’或‘6985’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘6283’。

7.8.5 YYJS005-00

测试目的：应用已锁定。终端在第一个 GENERATE AC 命令中请求联机，卡片拒绝交易。验证不执行发卡行认证时，卡片接受 MAC 正确的 APPLICATION UNBLOCK 命令。

验证应用解锁成功。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令。

测试流程：a) 交易 1：锁定 PBOC 借记/贷记应用；

- b) 卡片上电（ATR）；
- c) 选择 PBOC 借记/贷记应用；
- d) GET PROCESSING OPTIONS 命令；
- e) VERIFY 命令；
- f) 第一个 GENERATE AC 命令请求 ARQC；
- g) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
- h) 第二个 GENERATE AC 命令请求 TC；
- i) APPLICATION BLOCK 命令，正确的 MAC；
- j) 交易 2：卡片拒绝交易。不执行发卡行认证，执行 APPLICATION UNBLOCK 命令；
- k) 卡片上电（ATR）；
- l) 选择 PBOC 借记/贷记应用；
- m) GET PROCESSING OPTIONS 命令；
- n) VERIFY 命令；
- o) 第一个 GENERATE AC 命令请求 ARQC，卡片返回 AAC；
- p) APPLICATION UNBLOCK 命令，正确的 MAC；
- q) 交易 3：选择 PBOC 借记/贷记应用；
- r) 卡片上电（ATR）；
- s) 选择 PBOC 借记/贷记应用；
- t) 交易 4：锁定 PBOC 借记/贷记应用；
- u) 卡片上电（ATR）；
- v) 选择 PBOC 借记/贷记应用；
- w) GET PROCESSING OPTIONS 命令；
- x) VERIFY 命令；
- y) 第一个 GENERATE AC 命令请求 ARQC；
- z) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
- aa) 第二个 GENERATE AC 命令请求 TC；
- ab) APPLICATION BLOCK 命令，正确的 MAC；
- ac) 交易 5：执行正确的发卡行认证，执行 APPLICATION UNBLOCK 命令；

- ad) 卡片上电 (ATR) ;
- ae) 选择 PBOC 借记/贷记应用;
- af) GET PROCESSING OPTIONS 命令;
- ag) VERIFY 命令;
- ah) 第一个 GENERATE AC 命令请求 ARQC;
- ai) APPLICATION UNBLOCK 命令, 正确的 MAC;
- aj) 交易 6: 选择 PBOC 借记/贷记应用;
- ak) 卡片上电 (ATR) ;
- al) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 和 5 中的卡片返回的状态字: 卡片收到 APPLICATION UNBLOCK 命令后应返回状态字 '9000'。验证交易 3 和 6 中卡片返回的状态字: 卡片收到 SELECT 命令后应返回状态字 '9000'。

7.8.6 YYJS006-00

测试目的: 应用已锁定。终端在第一个 GENERATE AC 命令中请求联机, 卡片拒绝交易。验证在成功的发卡行认证后, 卡片接受两个 MAC 正确的 APPLICATION UNBLOCK 命令。
验证应用解锁成功。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

测试流程: a) 交易 1: 锁定 PBOC 借记/贷记应用;

- b) 卡片上电 (ATR) ;
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) APPLICATION BLOCK 命令, 正确的 MAC;
- j) 交易 2: 卡片拒绝交易。成功的发卡行认证后, 执行两个 APPLICATION UNBLOCK 命令;
- k) 卡片上电 (ATR) ;
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC, 卡片返回 AAC;
- p) EXTERNAL AUTHENTICATE 命令, 包括错误的 ARPC;
- q) APPLICATION UNBLOCK 命令, 正确的 MAC;
- r) APPLICATION UNBLOCK 命令, 正确的 MAC;
- s) 交易 3: 选择 PBOC 借记/贷记应用;
- t) 卡片上电 (ATR) ;
- u) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片返回的状态字: 卡片收到第一个 APPLICATION UNBLOCK 命令后应返回状态字 '9000'。卡片收到第二个 APPLICATION UNBLOCK 命令后应返回状态字 '9000'。
验证交易 3 中卡片返回的状态字: 卡片收到 SELECT 命令后应返回状态字 '9000'。

7.8.7 YYJS007-00

测试目的：应用已锁定。终端在第一个 GENERATE AC 命令中请求联机，卡片拒绝交易。验证在成功的发卡行认证后，卡片接受第一个 MAC 正确的 APPLICATION UNBLOCK 命令，拒绝第二个 MAC 错误的 APPLICATION UNBLOCK 命令。

验证应用解锁成功。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令。

测试流程：a) 交易 1：锁定 PBOC 借记/贷记应用；
 b) 卡片上电（ATR）；
 c) 选择 PBOC 借记/贷记应用；
 d) GET PROCESSING OPTIONS 命令；
 e) VERIFY 命令；
 f) 第一个 GENERATE AC 命令请求 ARQC；
 g) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
 h) 第二个 GENERATE AC 命令请求 TC；
 i) APPLICATION BLOCK 命令，正确的 MAC；
 j) 交易 2：卡片拒绝交易，成功的发卡行认证后，执行第一个 MAC 正确的 APPLICATION UNBLOCK 命令和第二个 MAC 错误的 APPLICATION UNBLOCK 命令；
 k) 卡片上电（ATR）；
 l) 选择 PBOC 借记/贷记应用；
 m) GET PROCESSING OPTIONS 命令；
 n) VERIFY 命令；
 o) 第一个 GENERATE AC 命令请求 ARQC，卡片返回 AAC；
 p) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
 q) APPLICATION UNBLOCK 命令，正确的 MAC；
 r) APPLICATION UNBLOCK 命令，错误的 MAC；
 s) 交易 3：选择 PBOC 借记/贷记应用；
 t) 卡片上电（ATR）；
 u) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片返回的状态字：卡片收到第一个 APPLICATION UNBLOCK 命令后应返回状态字‘9000’；卡片收到第二个 APPLICATION UNBLOCK 命令后不应返回状态字‘9000’，推荐返回‘6988’。验证交易 3 中卡片返回的状态字：卡片收到 SELECT 命令后应返回状态字‘9000’。

7.8.8 YYJS008-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片接受一个 MAC 正确的 APPLICATION BLOCK 命令和一个 MAC 正确的 APPLICATION UNBLOCK 命令。

验证应用解锁成功。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
 b) 交易 2：联机批准，发卡行认证成功，执行一个成功的 APPLICATION BLOCK 命令和一个成功的 APPLICATION UNBLOCK 命令；
 c) 卡片上电（ATR）；
 d) 选择 PBOC 借记/贷记应用；

- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- i) 第二个 GENERATE AC 命令请求 TC ;
- j) APPLICATION BLOCK 命令, 正确的 MAC;
- k) APPLICATION UNBLOCK 命令, 正确的 MAC;
- l) 交易 3: 选择锁定的 PBOC 借记/贷记应用;
- m) 卡片上电 (ATR) ;
- n) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片返回的状态字: 卡片收到 APPLICATION BLOCK 命令后应返回状态字 ‘9000’ ; 卡片收到 APPLICATION UNBLOCK 命令后应返回状态字 ‘9000’ 。验证交易 3 中卡片返回的状态字: 卡片收到 SELECT 命令后应返回状态字 ‘9000’ 。

7.8.9 YYJS009-00

测试目的: 验证当交易被联机批准, 并且发卡行认证成功时, 卡片接受 MAC 正确的 APPLICATION UNBLOCK 命令。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 联机批准, 发卡行认证成功, APPLICATION UNBLOCK 命令成功;
c) 卡片上电 (ATR) ;
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) VERIFY 命令;
g) 第一个 GENERATE AC 命令请求 ARQC;
h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
i) 第二个 GENERATE AC 命令请求 TC;
j) APPLICATION UNBLOCK 命令, 正确的 MAC。

通过标准: 验证交易 2 卡片返回的状态字: 卡片收到 APPLICATION UNBLOCK 命令后应返回状态字 ‘9000’ 。

7.8.10 YYJS010-00

测试目的: 验证当交易被联机拒绝, 并且发卡行认证成功时, 卡片接受 MAC 正确的 APPLICATION UNBLOCK 命令。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 联机拒绝, 发卡行认证成功, APPLICATION UNBLOCK 命令成功;
c) 卡片上电 (ATR) ;
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) VERIFY 命令;
g) 第一个 GENERATE AC 命令请求 ARQC;
h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;

- i) 第二个 GENERATE AC 命令请求 AAC;
- j) APPLICATION UNBLOCK 命令, 正确的 MAC。

通过标准: 验证交易 2 卡片返回的状态字: 卡片收到 APPLICATION UNBLOCK 命令后应返回状态字 ‘9000’。

7.9 卡片锁定命令 (KSML)

7.9.1 KSML001-00

测试目的: 验证当 CARD BLOCK 命令中 MAC 数据域的长度小于指定最小长度时, 该命令执行失败。
测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK 命令。
测试流程: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器; 随后执行 CARD BLOCK 命令, 命令格式见表 17, 该命令数据域长度小于 MAC 的指定最小长度 (Lc 的值为不正确的 MAC 长度)。

表17 CARD BLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	16	00	00	03	11 22 33	N/A

通过标准: 卡片收到 CARD BLOCK 命令后不应返回状态字 ‘9000’, 推荐返回 ‘6700’。

7.9.2 KSML002-00

测试目的: 验证当 CARD BLOCK 命令中 MAC 数据域的长度大于指定最大长度时, 该命令执行失败。
测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK 命令。
测试流程: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器; 随后执行 CARD BLOCK 命令, 命令格式见表 18, 该命令数据域长度大于 MAC 的指定最大长度 (Lc 的值为不正确的 MAC 长度)。

表18 CARD BLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	16	00	00	09	11 22 33 44 55 66 77 88 99	N/A

通过标准: 卡片收到 CARD BLOCK 命令后不应返回状态字 ‘9000’, 推荐返回 ‘6700’。

7.9.3 KSML003-00

测试目的: 验证当 CARD BLOCK 命令中 MAC 数据错误时, 该命令执行失败。
测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK 命令。
测试流程: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器; 随后执行 CARD BLOCK 命令, 命令格式见表 19, 该命令数据域为错误的 MAC。

表19 CARD BLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	16	00	00	04	11 22 33 44	N/A

通过标准: 卡片收到 CARD BLOCK 命令后不应返回状态字 ‘9000’, 推荐返回 ‘6988’。

7.9.4 KSML004-00

测试目的: 验证当收到成功的 CARD BLOCK 命令时, 卡片返回状态字 ‘9000’。
测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK 命令。
测试流程: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器; 随后执行 CARD BLOCK

命令，命令格式见表 20，该命令数据域为正确的 MAC。

表20 CARD BLOCK 命令报文

CLA	INS	P1	P2	Lc	Data	Le
84	16	00	00	04	正确的 MAC	N/A

通过标准：卡片收到 CARD BLOCK 命令后返回状态字 ‘9000’。

7.10 卡片锁定 (KPSD)

7.10.1 KPSD001-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片接受在第二个 GENERATE AC 命令后执行的 MAC 正确的 CARD BLOCK 命令。

验证卡片锁定 PSE 应用。

验证卡片锁定 PBOC 借记/贷记应用。

测试条件：第 9 章中的卡片特征 1，支持 CARD BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，发卡行认证成功，CARD BLOCK 命令成功；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

j) CARD BLOCK 命令，正确的 MAC；

k) 交易 3：选择无效的 PSE 应用和无效的 PBOC 借记/贷记应用；

l) 卡片上电 (ATR)；

m) 选择 PSE 应用；

n) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字：卡片收到 CARD BLOCK 命令后应返回状态字 ‘9000’。验证交易 3 中卡片返回的状态字：如果支持 PSE 选择，卡片收到 SELECT PSE 命令后应返回状态字 ‘6A81’；卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 ‘6A81’。

7.10.2 KPSD002-00

测试目的：验证当交易被联机拒绝，并且发卡行认证成功时，卡片接受 CARD BLOCK 命令。

验证卡片锁定 PSE 应用。

验证卡片锁定 PBOC 借记/贷记应用。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证和 CARD BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机拒绝，发卡行认证成功，CARD BLOCK 命令成功；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- i) 第二个 GENERATE AC 命令请求 AAC;
- j) CARD BLOCK 命令, 正确的 MAC;
- k) 交易 3: 选择无效的 PSE 应用和无效的 PBOC 借记/贷记应用;
- l) 卡片上电 (ATR);
- m) 选择 PSE 应用;
- n) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字: 卡片收到 CARD BLOCK 命令后应返回状态字 '9000'。验证交易 3 中卡片返回的状态字: 如果支持 PSE 选择, 卡片收到 SELECT PSE 命令后应返回状态字 '6A81'; 卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 '6A81'。

7.10.3 KPSD003-00

测试目的: 验证当交易被联机批准, 并且发卡行认证成功时, 卡片拒绝 MAC 错误的 CARD BLOCK 命令。

验证卡片不锁定 PSE 应用。

验证卡片不锁定 PBOC 借记/贷记应用。

测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 发卡行认证成功, CARD BLOCK 命令成功;

c) 卡片上电 (ATR)。选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 ARQC;

g) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;

h) 第二个 GENERATE AC 命令请求 TC;

i) CARD BLOCK 命令, 错误的 MAC;

j) 交易 3: 选择 PSE 应用和 PBOC 借记/贷记应用;

k) 卡片上电 (ATR);

l) 选择 PSE 应用;

m) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字: 卡片收到 CARD BLOCK 命令后不应返回状态字 '9000', 推荐返回 '6988'。验证交易 3 中卡片返回的状态字: 如果支持 PSE 选择, 卡片收到 SELECT PSE 命令后应返回状态字 '9000'; 卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 '9000'。

7.10.4 KPSD004-00

测试目的: 验证当交易被联机批准, 并且发卡行认证成功时, 卡片拒绝 MAC 缺失的 CARD BLOCK 命令。

验证卡片不锁定 PSE 应用。

验证卡片不锁定 PBOC 借记/贷记应用。

测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 联机批准, 发卡行认证成功, CARD BLOCK 命令失败;
c) 卡片上电 (ATR);
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) VERIFY 命令;
g) 第一个 GENERATE AC 命令请求 ARQC;
h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
i) 第二个 GENERATE AC 命令请求 TC;
j) CARD BLOCK 命令, MAC 缺失;
k) 交易 3: 选择 PSE 应用和 PBOC 借记/贷记应用;
l) 卡片上电 (ATR);
m) 选择 PSE 应用;
n) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字: 卡片收到 CARD BLOCK 命令后不应返回状态字 '9000', 推荐返回 '6987' 或 '6988'。验证交易 3 中卡片返回的状态字: 如果支持 PSE 选择, 卡片收到 SELECT PSE 命令后应返回状态字 '9000'; 卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 '9000'。

7.10.5 KPSD006-00

测试目的: 验证当交易被联机批准时, 未执行发卡行认证或发卡行认证成功, 卡片接收 MAC 正确的 CARD BLOCK 命令。验证卡片锁定 PSE 应用。验证卡片锁定 PBOC 借记/贷记应用。

测试条件: 卡片类型 1, 支持 CARD BLOCK 命令

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 联机批准, 未执行发卡行认证, 执行 CARD BLOCK 命令;
c) 卡片上电 (ATR);
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) VERIFY 命令;
g) 第一个 GENERATE AC 命令请求 ARQC;
h) 第二个 GENERATE AC 命令请求 TC;
i) CARD BLOCK 命令, 正确的 MAC;
j) 交易 3: 选择 PSE 应用和 PBOC 借记/贷记应用;
k) 卡片上电 (ATR);
l) 选择 PSE 应用;
m) 选择 PBOC 借记/贷记应用;
n) 交易 4: 联机批准, 发卡行认证成功, 执行 CARD BLOCK 命令;
o) 卡片上电 (ATR);
p) 选择 PBOC 借记/贷记应用;
q) GET PROCESSING OPTIONS 命令;
r) VERIFY 命令;
s) 第一个 GENERATE AC 命令请求 ARQC;
t) 第二个 GENERATE AC 命令请求 TC;

- u) CARD BLOCK 命令, 正确的 MAC;
- v) 交易 5: 选择 PSE 应用和 PBOC 借记/贷记应用;
- w) 卡片上电 (ATR);
- x) 选择 PSE 应用;
- y) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 和 3 中卡片响应 CARD BLOCK 命令返回的状态字: 卡片收到 CARD BLOCK 命令后应返回状态字 '9000'。验证交易 3 和 5 中卡片返回的状态字: 如果支持 PSE 选择, 卡片收到 SELECT PSE 命令后应返回状态字 '6A81'; 卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 '6A81'。

7.10.6 KPSD005-00

测试目的: 验证当交易被联机批准, 并且发卡行认证失败时, 卡片拒绝 MAC 正确的 CARD BLOCK 命令。

验证卡片不锁定 PSE 应用。

验证卡片不锁定 PBOC 借记/贷记应用。

测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 发卡行认证失败, 执行 CARD BLOCK 命令;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 命令请求 ARQC;

h) EXTERNAL AUTHENTICATE 命令, 包括错误的 ARPC;

i) 第二个 GENERATE AC 命令请求 TC;

j) CARD BLOCK 命令, 正确的 MAC ;

k) 交易 3: 选择 PSE 应用和 PBOC 借记/贷记应用;

l) 卡片上电 (ATR);

m) 选择 PSE 应用;

n) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字: 卡片收到 CARD BLOCK 命令后不应返回状态字 '9000', 推荐返回 '6985'。验证交易 3 中卡片返回的状态字: 如果支持 PSE 选择, 卡片收到 SELECT PSE 命令后应返回状态字 '9000'; 卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 '9000'。

7.10.7 KPSD007-00

测试目的: 验证当交易被联机批准, 并且发卡行认证成功时, 卡片接受第二个 GENERATE AC 命令之前发送的 MAC 正确的 CARD BLOCK 命令。

验证卡片锁定 PSE 应用。

验证卡片锁定 PBOC 借记/贷记应用。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证和 CARD BLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 发卡行认证成功, 在第二个 GENERATE AC 命令之前执行 CARD BLOCK

命令;

- c) 卡片上电 (ATR) ;
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- i) CARD BLOCK 命令, 正确的 MAC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) 交易 3: 选择无效的 PSE 应用和无效的 PBOC 借记/贷记应用;
- l) 卡片上电 (ATR) ;
- m) 选择 PSE 应用;
- n) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字: 卡片收到 CARD BLOCK 命令后应返回状态字 ‘9000’。验证交易 3 中卡片返回的状态字: 如果支持 PSE 选择, 卡片收到 SELECT PSE 命令后应返回状态字 ‘6A81’; 卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 ‘6A81’。

7.10.8 KPSD008-00

测试目的: 验证当交易被联机批准, 并且发卡行认证成功时, 卡片接受两个 MAC 正确的 CARD BLOCK 命令。

验证卡片锁定 PSE 应用。

验证卡片锁定 PBOC 借记/贷记应用。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证和 CARD BLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 发卡行认证成功, 在第二个 GENERATE AC 命令之前执行 CARD BLOCK 命令;

- c) 卡片上电 (ATR) ;
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- i) 第二个 GENERATE AC 命令请求 TC;
- j) CARD BLOCK 命令, 正确的 MAC;
- k) CARD BLOCK 命令, 正确的 MAC;
- l) 交易 3: 选择无效的 PSE 应用和无效的 PBOC 借记/贷记应用;
- m) 卡片上电 (ATR) ;
- n) 选择 PSE 应用;
- o) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字: 卡片收到第一个 CARD BLOCK 命令后应返回状态字 ‘9000’; 卡片收到第二个 CARD BLOCK 命令后应返回状态字 ‘9000’。验证交易 3 中卡片返回的状态字: 如果支持 PSE 选择, 卡片收到 SELECT PSE

命令后应返回状态字‘6A81’；卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字‘6A81’。

7.10.9 KPSD009-00

测试目的：验证当交易被联机批准，并且发卡行认证成功时，卡片接受第一个 MAC 正确的 CARD BLOCK 命令，拒绝第二个 MAC 错误的 CARD BLOCK 命令。

验证卡片锁定 PSE 应用。

验证卡片锁定 PBOC 借记/贷记应用。

测试条件：第 9 章中的卡片特征 1，支持 CARD BLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准，发卡行认证成功，执行一个成功的 CARD BLOCK 命令和一个失败的 CARD BLOCK 命令；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；
j) CARD BLOCK 命令，正确的 MAC；
k) CARD BLOCK 命令，错误的 MAC；
l) 交易 3：选择无效的 PSE 应用和无效的 PBOC 借记/贷记应用；
m) 卡片上电（ATR）；
n) 选择 PSE 应用；
o) 选择 PBOC 借记/贷记应用。

通过标准：验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字：卡片收到第一个 CARD BLOCK 命令后应返回状态字‘9000’；卡片收到第二个 CARD BLOCK 命令后不应返回状态字‘9000’，推荐返回‘6988’。验证交易 3 中卡片返回的状态字：如果支持 PSE 选择，卡片收到 SELECT PSE 命令后应返回状态字‘6A81’；卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字‘6A81’。

7.10.10 KPSD010-00

测试目的：验证当 PBOC 借记/贷记应用锁定时，发卡行认证成功，卡片接受 MAC 正确的 CARD BLOCK 命令。

验证卡片锁定 PSE 应用。

验证卡片锁定 PBOC 借记/贷记应用。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证和 CARD BLOCK 命令。

测试流程：a) 交易 1：锁定 PBOC 借记/贷记应用；
b) 卡片上电（ATR）；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；

- g) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) APPLICATION BLOCK 命令, 正确的 MAC;
- j) 交易 2: 卡片强制拒绝交易, 执行一个成功的 CARD BLOCK 命令;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC, 卡片应返回 AAC;
- p) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- q) CARD BLOCK 命令, 正确的 MAC;
- r) 交易 3: 选择无效的 PSE 应用和无效的 PBOC 借记/贷记应用;
- s) 卡片上电 (ATR);
- t) 选择 PSE 应用;
- u) 选择 PBOC 借记/贷记应用。

通过标准: 验证交易 2 中卡片响应 CARD BLOCK 命令返回的状态字: 卡片收到 CARD BLOCK 命令后应返回状态字 '9000'。验证交易 3 中卡片返回的状态字: 如果支持 PSE 选择, 卡片收到 SELECT PSE 命令后应返回状态字 '6A81'; 卡片收到 SELECT PBOC 借记/贷记应用命令后应返回状态字 '6A81'。

7.11 联机批准交易 (LJPZ)

7.11.1 LJPZ001-00

测试目的: 验证卡片对联机批准交易中命令的正确响应。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC。

通过标准: 验证对所有命令卡片返回的状态字均为 '9000': 选择 PBOC 借记/贷记应用命令。GET PROCESSING OPTIONS 命令; 所有 READ RECORD 命令; VERIFY 命令 (如果支持脱机 PIN); 第一个 GENERATE AC 命令; EXTERNAL AUTHENTICATE 命令; 第二个 GENERATE AC 命令。

7.11.2 LJPZ002-00

测试目的: 验证当不支持发卡行认证时, 卡片对联机批准交易中所有命令的正确响应。

测试条件: 第 9 章中的卡片特征 2。

测试流程: a) 不执行发卡行认证, 复位卡片中的计数器;

- b) 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;

- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 第二个 GENERATE AC 命令请求 TC。

通过标准: 验证对所有命令卡片返回的状态字均为‘9000’: 选择 PBOC 借记/贷记应用命令; GET PROCESSING OPTIONS 命令; 所有 READ RECORD 命令; VERIFY 命令(如果支持脱机 PIN); 第一个 GENERATE AC 命令; 第二个 GENERATE AC 命令。

7.12 复合动态数据认证(FHDT)

7.12.1 FHDT001-00

测试目的: 验证卡片接受 GENERATE AC 命令, 该命令指示此交易符合 CDA 执行条件。交易被联机批准。

测试条件: 第 9 章中的卡片特征 23, 支持 CDA 处理。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 联机批准;
- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理;
- h) EXTERNAL AUTHENTICATE 命令;
- i) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准: 验证交易 2 中第一个 GENERATE AC 命令的响应: SW1 SW2=‘9000’; CID 位 8-7=‘10’; CVR 字节 2 高半字节=‘A’; CVR=‘03 A4 00 02’或‘03 A0 00 02’(用于未校验 PIN)。

7.12.2 FHDT002-00

测试目的: 验证卡片接受 GENERATE AC 命令, 该命令指示此交易符合 CDA 执行条件。交易被脱机批准。

测试条件: 第 9 章中的卡片特征 23, 支持 CDA 处理。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准: 验证交易 2 中第一个 GENERATE AC 命令的响应: SW1 SW2=‘9000’; CID 位 8-7=‘01’; CVR 字节 2 高半字节=‘9’; CVR=‘03 94 00 02’或‘03 90 00 02’(用于未校验 PIN)。

7.12.3 FHDT003-00

测试目的: 验证卡片执行 CDA 时, 卡片对 GENERATE AC 命令的响应数据域中的数据对象应按格式 2 编码(即带有标签‘77’的结构数据对象), 交易被联机批准。

测试条件：第9章中的卡片特征1。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易2：联机批准；
- c) 卡片上电（ATR）；
- d) 选择PBOC借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；
- f) VERIFY 命令；
- g) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理；
- h) EXTERNAL AUTHENTICATE 命令；
- i) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准：验证交易2中第一个 GENERATE AC 命令的响应：响应数据的第一个字节应为标签‘77’；第二个字节应为‘57’；标签‘9F27’长度为‘01’，值为‘80’；标签‘9F36’长度为‘02’，值为交易1的ATC值加1；标签‘9F4B’长度为‘40’；标签‘9F10’长度为‘08’，值为‘07 01 01 03 00 00 00 01’；SW1 SW2=‘9000’。验证交易2中第二个 GENERATE AC 命令的响应：响应数据的第一个字节应为标签‘77’；第二个字节应为‘57’；标签‘9F27’长度为‘01’，值为‘40’；标签‘9F36’长度为‘02’，值为交易1的ATC值加1；标签‘9F4B’长度为‘40’；标签‘9F10’长度为‘08’，值为‘07 01 01 03 00 00 00 01’；SW1 SW2=‘9000’。

7.12.4 FHDT004-00

测试目的：验证卡片执行CDA时，卡片对 GENERATE AC 命令的响应数据域中的数据对象应按格式2进行编码（即带有标签‘77’的结构数据对象），交易被脱机批准。

测试条件：第9章中的卡片特征23。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易2：联机批准；
- c) 卡片上电（ATR）；
- d) 选择PBOC借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；
- f) VERIFY 命令；
- g) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准：验证交易2中第一个 GENERATE AC 命令的响应：响应数据的第一个字节应为标签‘77’；第二个字节应为‘57’；标签‘9F27’长度为‘01’，值为‘40’；标签‘9F36’长度为‘02’，值为交易1的ATC值加1；标签‘9F4B’长度为‘40’；标签‘9F10’长度为‘08’，值为‘07 01 01 03 00 00 00 01’；SW1 SW2=‘9000’。

7.12.5 FHDT005-00

测试目的：验证当交易请求脱机拒绝时，卡片对 GENERATE AC 命令的响应结构正确，该命令请求CDA处理但未执行。

测试条件：第9章中的卡片特征23，支持CDA处理。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易2：脱机拒绝；
- c) 卡片上电（ATR）；
- d) 选择PBOC借记/贷记应用；

- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 AAC 和 CDA 处理, 但不执行 CDA。

通过标准: 验证交易 2 中第一个 GENERATE AC 命令的响应, 该响应无论是格式 1 还是格式 2 编码, 都应包括以下值: CID= '00'; ATC 值为交易 1 的值加 1; 一个八字节的应用密文; 专用发卡行应用数据(分散密钥索引, 密文版本号, CVR, 算法标识); SW1 SW2= '9000'; CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.12.6 FHDT006-00

测试目的: 验证当终端请求交易联机, 卡片强制拒绝时, 卡片对 GENERATE AC 命令的响应结构正确, 该命令请求 CDA 处理但未执行。

测试条件: 第 9 章中的卡片特征 23, 支持 CDA 处理。

测试流程: a) 交易 1: 锁定应用;

b) 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 ARQC;

g) EXTERNAL AUTHENTICATE 命令;

h) 第二个 GENERATE AC 命令请求 TC;

i) APPLICATION BLOCK 命令;

j) 交易 2: 脱机被拒绝, 请求 CDA;

k) 卡片上电 (ATR);

l) 选择 PBOC 借记/贷记应用;

m) GET PROCESSING OPTIONS 命令;

n) VERIFY 命令;

o) 第一个 GENERATE AC 命令请求 ARQC, 该命令 P1 位 5= '1', 卡片返回 AAC 无 CDA 数据;

p) 交易 3: 解锁应用;

q) 卡片上电 (ATR);

r) 选择 PBOC 借记/贷记应用;

s) GET PROCESSING OPTIONS 命令;

t) VERIFY 命令;

u) 第一个 GENERATE AC 命令请求 ARQC, 卡片返回 AAC;

v) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;

w) APPLICATION UNBLOCK 命令。

通过标准: 交易 1: APPLICATION BLOCK 命令响应= '9000'。验证交易 2 中第一个 GENERATE AC 命令的响应, 该响应可以是格式 1 或格式 2 编码: CID= '00'; ATC 值为交易 1 的值加 1; 一个八字节的应用密文; 专用发卡行应用数据(分散密钥索引, 密文版本号, CVR, 算法标识); CVR= '03 84 00 10' 或 '03 80 00 10' (用于未校验 PIN); SW1 SW2= '9000'。交易 3: 第一个 GENERATE AC, CID= '00'; 第一个 GENERATE AC, CVR= '03 84 00 10' 或 '03 80 00 10' (用于未校验 PIN); APPLICATION UNBLOCK 命令 SW1 SW2= '9000'。

7.12.7 FHDT007-00

测试目的：验证当应用已锁定时，卡片对 GENERATE AC 命令的响应结构正确，该命令请求 CDA 处理但未执行。

测试条件：第 9 章中的卡片特征 23，支持 CDA 处理。

测试流程：a) 交易 1：锁定应用；
b) 卡片上电（ATR）；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC，P1 位 5= ‘0’ ；
g) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
h) 第二个 GENERATE AC 命令请求 TC；
i) APPLICATION BLOCK 命令；
j) 交易 2：脱机被拒绝，请求 CDA；
k) 卡片上电（ATR）；
l) 选择 PBOC 借记/贷记应用；
m) GET PROCESSING OPTIONS 命令；
n) VERIFY 命令；
o) 第一个 GENERATE AC 命令请求 ARQC，该命令 P1 第 5 位= ‘1’ ，卡片返回 AAC 无 CDA 数据；
p) 交易 3：解锁应用；
q) 卡片上电（ATR）；
r) 选择 PBOC 借记/贷记应用；
s) GET PROCESSING OPTIONS 命令；
t) VERIFY 命令；
u) 第一个 GENERATE AC 命令请求 ARQC，该命令 P1 第 5 位= ‘0’ ，卡片返回 AAC；
v) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
w) APPLICATION UNBLOCK 命令。

通过标准：交易 1：APPLICATION BLOCK 命令响应= ‘9000’ 。验证交易 2 中第一个 GENERATE AC 命令的响应，该响应可以是格式 1 或格式 2 编码：CID= ‘00’ ；ATC 值为交易 1 的值加 1；一个八字节的应用密文；专用发卡行应用数据（分散密钥索引，密文版本号，CVR，算法标识）；CVR= ‘03 84 00 10’ 或 ‘03 80 00 10’ （用于未校验 PIN）；SW1 SW2= ‘9000’ 。交易 3：第一个 GENERATE AC，CID= ‘00’ ；第一个 GENERATE AC，CVR= ‘03 84 00 10’ 或 ‘03 80 00 10’ （用于未校验 PIN）；APPLICATION UNBLOCK 命令 SW1 SW2= ‘9000’ 。

7.12.8 FHDT008-00

测试目的：交易请求联机，动态签名验证失败，该交易脱机被拒绝 ARC 为 Z3。设置 CVR 中的“上次交易 DDA 失败交易拒绝”位为 ‘1’ 。

测试条件：第 9 章中的卡片特征 23，支持 CDA 处理。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：CDA 失败时交易被终端拒绝；
c) 卡片上电（ATR）；

- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理;
- h) 第二个 GENERATE AC 命令请求 AAC, ARC 为 Z3;
- i) 交易 3: 联机批准, 成功的 CDA;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理, 卡片返回 ARQC;
- o) EXTERNAL AUTHENTICATE 命令;
- p) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准: 验证交易 2 中第二个 GENERATE AC 命令的响应: SW1 SW2= '9000'; CID= '00'; CVR= '03 25 00 02' 或 '03 21 00 02' (用于未校验 PIN)。验证交易 3 中第二个 GENERATE AC 命令的响应: SW1 SW2= '9000'; CID= '40'; CVR= '03 64 80 06' 或 '03 60 80 06' (用于未校验 PIN)。

7.12.9 FHDT009-00

测试目的: 动态签名能在脱机批准时被恢复, 发卡行公钥和 IC 卡公钥分别在发卡行公钥证书和 IC 卡公钥证书解密中被恢复。终端也解密动态签名 (被签名的动态应用数据)。

测试条件: 第 9 章中的卡片特征 23。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准, CDA 成功;
c) 卡片上电 (ATR);
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) VERIFY 命令;
g) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准: 验证恢复数据: 被签名的动态应用数据的长度等于 IC 卡公钥模长度; 数据头应为 '6A' - 字节 1; 恢复数据的结尾应为 'BC' - 最后一个字节; 签名数据格式应为 '05' - 字节 2; IC 卡动态数字长度 (1 字节); IC 卡动态数字 (2-8 字节); CID (1 字节) = '40', 与第一个 GENERATE AC 命令数据中获得的应用密文相同; TC (8 字节), 与卡片生成的相同; 交易数据哈希码 (20 字节) 在 IC 卡动态数据中获得; 恢复的被签名的哈希结果与计算的被签名的哈希结果相同。

7.12.10 FHDT010-00

测试目的: 动态签名能在联机批准时被恢复, 发卡行公钥和 IC 卡公钥分别在发卡行公钥证书和 IC 卡公钥证书解密中被恢复。终端也解密动态签名 (被签名的动态应用数据)。

测试条件: 第 9 章中的卡片特征 23。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 联机批准;
c) 卡片上电 (ATR);

- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理;
- h) EXTERNAL AUTHENTICATE 命令;
- i) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准: 验证第一个 GENERATE AC 命令中的恢复数据: 被签名的动态应用数据的长度等于 IC 卡公钥模长度; 数据头应为 ‘6A’ - 字节 1; 恢复数据的结尾应为 ‘BC’ - 最后一个字节; 签名数据格式应为 ‘05’ - 字节 2; IC 卡动态数字长度 (1 字节); IC 卡动态数字 (2-8 字节); CID (1 字节) = ‘80’, 与 GENERATE AC 命令数据中获得的应用密文相同; ARQC (8 字节), 与卡片生成的相同; 交易数据哈希码 (20 字节) 在 IC 卡动态数据中获得; 恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同; 验证第二个 GENERATE AC 命令中的恢复数据: 被签名的动态应用数据的长度等于 IC 卡公钥模长度; 数据头应为 ‘6A’ - 字节 1; 恢复数据的结尾应为 ‘BC’ - 最后一个字节; 签名数据格式应为 ‘05’ - 字节 2; IC 卡动态数字长度 (1 字节); IC 卡动态数字 (2-8 字节); CID (1 字节) = ‘40’, 与 GENERATE AC 命令数据中获得的应用密文相同; TC (8 字节), 与卡片生成的相同; 交易数据哈希码 (20 字节) 在 IC 卡动态数据中获得; 恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同。

7.12.11 FHDT011-00

测试目的: 验证当上次脱机拒绝交易 CDA 失败时, 卡片设置 CVR 中的 “上次交易 DDA 失败交易拒绝” 位为 ‘1’。

测试条件: 第 9 章中的卡片特征 23, 支持 CDA 处理。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 当 CDA 失败时脱机交易被拒绝;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 AAC 和 CDA 处理;
- h) 交易 3: 脱机批准;
- i) 卡片上电 (ATR);
- j) 选择 PBOC 借记/贷记应用;
- k) GET PROCESSING OPTIONS 命令;
- l) VERIFY 命令;
- m) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准: 验证交易 3 第一个 GENERATE AC 命令的卡片响应: SW1 SW2= ‘9000’; CID 位 8-7= ‘01’; CVR 字节 2 高半字节= ‘9’; CVR 字节 4 位 3= ‘1’; CVR= ‘03 94 00 06’ 或 ‘03 90 00 06’ (用于未校验 PIN)。

7.12.12 FHDT012-00

测试目的: 验证当上次联机批准交易发卡行认证失败时, 卡片不重置 “DDA 失败指示” 位。

测试条件：第9章中的卡片特征23，支持CDA处理。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易2：当CDA失败时脱机交易被拒绝；
- c) 卡片上电（ATR）；
- d) 选择PBOC借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；
- f) VERIFY 命令；
- g) 第一个 GENERATE AC 命令请求 AAC 和 CDA 处理；
- h) 交易3：当发卡行认证失败时联机拒绝；
- i) 卡片上电（ATR）；
- j) 选择PBOC借记/贷记应用；
- k) GET PROCESSING OPTIONS 命令；
- l) VERIFY 命令；
- m) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理；
- n) EXTERNAL AUTHENTICATE 命令，包括错误的 ARPC；
- o) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理，卡片返回 AAC；
- p) 交易4：联机卡片响应；
- q) 卡片上电（ATR）；
- r) 选择PBOC借记/贷记应用；
- s) GET PROCESSING OPTIONS 命令；
- t) VERIFY 命令；
- u) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理，响应 ARQC。

通过标准：交易4验证第一个 GENERATE AC 命令的卡片响应：SW1 SW2= ‘9000’；CID= ‘80’；CVR= ‘03 A4 88 06’ 或 ‘03 A0 88 06’（用于未校验 PIN）。

7.12.13 FHDT013-00

测试目的：动态签名能在脱机批准时被恢复，发卡行公钥和 IC 卡公钥分别在发卡行公钥证书和 IC 卡公钥证书解密中被恢复（1152 位密钥长度）。终端也解密动态签名（被签名的动态应用数据）。

测试条件：第9章中的卡片特征7。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易2：脱机批准，CDA 成功；
- c) 卡片上电（ATR）；
- d) 选择PBOC借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；
- f) VERIFY 命令；
- g) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准：验证恢复数据：被签名的动态应用数据的长度等于 IC 卡公钥模长度（1152 位）。数据头应为 ‘6A’ - 字节1。恢复数据的结尾应为 ‘BC’ - 最后一个字节。签名数据格式应为 ‘05’ - 字节2。IC 卡动态数字长度（1 字节）。IC 卡动态数字（2-8 字节）。CID（1 字节）= ‘40’，与第一个 GENERATE AC 命令数据中获得的应用密文相同。TC（8 字节），与卡片生成的相同。交易数据哈希码（20 字节）在 IC 卡动态数据中获得。验证交易数据哈希码（20 字节）是否计算准确。恢复的被签名的哈希结果与计

算的被签名的哈希结果相同。

7.12.14 FHDT014-00

测试目的：动态签名能在联机批准时被恢复，发卡行公钥和 IC 卡公钥分别在发卡行公钥证书和 IC 卡公钥证书解密中被恢复（1152 位密钥长度）。终端也解密动态签名（被签名的动态应用数据）。

测试条件：第 9 章中的卡片特征 7。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理；

h) EXTERNAL AUTHENTICATE 命令；

i) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准：验证第一个 GENERATE AC 命令中的恢复数据：被签名的动态应用数据的长度等于 IC 卡公钥模长度（1152 位）；数据头应为 ‘6A’ - 字节 1；恢复数据的结尾应为 ‘BC’ - 最后一个字节；签名数据格式应为 ‘05’ - 字节 2；IC 卡动态数字长度（1 字节）。IC 卡动态数字（2-8 字节）；CID（1 字节）= ‘80’，与 GENERATE AC 命令数据中获得的应用密文相同；ARQC（8 字节），与卡片生成的相同；交易数据哈希码（20 字节）在 IC 卡动态数据中获得；恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同。验证第二个 GENERATE AC 命令中的恢复数据：被签名的动态应用数据的长度等于 IC 卡公钥模长度（1152 位）；数据头应为 ‘6A’ - 字节 1；恢复数据的结尾应为 ‘BC’ - 最后一个字节；签名数据格式应为 ‘05’ - 字节 2；IC 卡动态数字长度（1 字节）；IC 卡动态数字（2-8 字节）；CID（1 字节）= ‘40’，与 GENERATE AC 命令数据中获得的应用密文相同；TC（8 字节），与卡片生成的相同；交易数据哈希码（20 字节）在 IC 卡动态数据中获得；验证交易数据哈希码（20 字节）是否计算准确；恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同。

7.12.15 FHDT015-00

测试目的：动态签名能在脱机批准时被恢复，发卡行公钥和 IC 卡公钥分别在发卡行公钥证书和 IC 卡公钥证书解密中被恢复（1408 位密钥长度）。终端也解密动态签名（被签名的动态应用数据）。

测试条件：第 9 章中的卡片特征 8。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：脱机批准，CDA 成功；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准：验证恢复数据：被签名的动态应用数据的长度等于 IC 卡公钥模长度（1408 位）；数

据头应为‘6A’-字节1；恢复数据的结尾应为‘BC’-最后一个字节；签名数据格式应为‘05’-字节2；IC卡动态数字长度（1字节）；IC卡动态数字（2-8字节）；CID（1字节）=‘40’，与第一个GENERATE AC命令数据中获得的应用密文相同；TC（8字节），与卡片生成的相同；交易数据哈希码（20字节）在IC卡动态数据中获得；验证交易数据哈希码（20字节）是否计算准确；恢复的被签名的哈希结果与计算的被签名的哈希结果相同。

7.12.16 FHDT016-00

测试目的：动态签名能在联机批准时被恢复，发卡行公钥和IC卡公钥分别在发卡行公钥证书和IC卡公钥证书解密中被恢复（1408位密钥长度）。终端也解密动态签名（被签名的动态应用数据）。

测试条件：第9章中的卡片特征8。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：联机批准；

c) 卡片上电（ATR）；

d) 选择PBOC借记/贷记应用；

e) GET PROCESSING OPTIONS命令；

f) VERIFY命令；

g) 第一个GENERATE AC命令请求ARQC和CDA处理；

h) EXTERNAL AUTHENTICATE命令；

i) 第二个GENERATE AC命令请求TC和CDA处理。

通过标准：验证第一个GENERATE AC命令中的恢复数据。

被签名的动态应用数据的长度等于IC卡公钥模长度（1408位）；数据头应为‘6A’-字节1；恢复数据的结尾应为‘BC’-最后一个字节；签名数据格式应为‘05’-字节2；IC卡动态数字长度（1字节）；IC卡动态数字（2-8字节）；CID（1字节）=‘80’，与GENERATE AC命令数据中获得的应用密文相同；ARQC（8字节），与卡片生成的相同；交易数据哈希码（20字节）在IC卡动态数据中获得；恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同。验证第二个GENERATE AC命令中的恢复数据：被签名的动态应用数据的长度等于IC卡公钥模长度（1408位）；数据头应为‘6A’-字节1；恢复数据的结尾应为‘BC’-最后一个字节；签名数据格式应为‘05’-字节2；IC卡动态数字长度（1字节）；IC卡动态数字（2-8字节）；CID（1字节）=‘40’，与GENERATE AC命令数据中获得的应用密文相同；TC（8字节），与卡片生成的相同；交易数据哈希码（20字节）在IC卡动态数据中获得；验证交易数据哈希码（20字节）是否计算准确；恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同。

7.12.17 FHDT017-00

测试目的：双算法卡，非对称算法随着算法选择进行改变，对称算法固定使用SM4，动态签名能在脱机批准时被恢复，发卡行公钥和IC卡公钥分别在发卡行公钥证书和IC卡公钥证书解密中被恢复。终端也解密动态签名（被签名的动态应用数据）。

测试条件：第9章中的卡片特征27。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：脱机批准，CDA成功；

- c) 卡片上电 (ATR) ;
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理 ;
- h) 交易 3: 脱机批准, CDA 成功, DF69=00;
- i) 卡片上电 (ATR) ;
- j) 选择 PBOC 借记/贷记应用;
- k) GET PROCESSING OPTIONS 命令;
- l) VERIFY 命令;
- m) 第一个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准: 验证恢复数据: 被签名的动态应用数据的长度等于 IC 卡公钥模长度; 数据头应为 '6A' - 字节 1; 恢复数据的结尾应为 'BC' - 最后一个字节; 签名数据格式应为 '05' - 字节 2; IC 卡动态数字长度 (1 字节); IC 卡动态数字 (2-8 字节); CID (1 字节) = '40', 与第一个 GENERATE AC 命令数据中获得的应用密文相同; TC (8 字节), 与卡片生成的相同; 交易数据哈希码 (20 字节) 在 IC 卡动态数据中获得; 验证交易数据哈希码 (20 字节) 是否计算准确; 恢复的被签名的哈希结果与计算的被签名的哈希结果相同; 交易 3 中, 对称密钥选择仍为 SM4, 相关数据应对应无误。

7.12.18 FHDT018-00

测试目的: 双算法卡, 非对称算法随着算法选择进行改变, 对称算法固定使用 SM4 动态签名能在联机批准时被恢复, 发卡行公钥和 IC 卡公钥分别在发卡行公钥证书和 IC 卡公钥证书解密中被恢复。终端也解密动态签名 (被签名的动态应用数据)。

测试条件: 第 9 章中的卡片特征 27。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 联机批准;
- c) 卡片上电 (ATR) ;
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理;
- h) EXTERNAL AUTHENTICATE 命令;
- i) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理;
- j) 交易 3: 联机批准, DF69=00;
- k) 卡片上电 (ATR) ;
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理;
- p) EXTERNAL AUTHENTICATE 命令;
- q) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准: 验证第一个 GENERATE AC 命令中的恢复数据: 被签名的动态应用数据的长度等于 IC 卡公钥模长度; 数据头应为 '6A' - 字节 1; 恢复数据的结尾应为 'BC' - 最后一个

字节；签名数据格式应为‘05’-字节2；IC卡动态数字长度（1字节）；IC卡动态数字（2-8字节）；CID（1字节）=‘80’，与GENERATE AC命令数据中获得的应用密文相同；ARQC（8字节），与卡片生成的相同；交易数据哈希码（20字节）在IC卡动态数据中获得；恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同。验证第二个GENERATE AC命令中的恢复数据：被签名的动态应用数据的长度等于IC卡公钥模长度；数据头应为‘6A’-字节1；恢复数据的结尾应为‘BC’-最后一个字节；签名数据格式应为‘05’-字节2；IC卡动态数字长度（1字节）；IC卡动态数字（2-8字节）；CID（1字节）=‘40’，与GENERATE AC命令数据中获得的应用密文相同；TC（8字节），与卡片生成的相同；交易数据哈希码（20字节）在IC卡动态数据中获得；验证交易数据哈希码（20字节）是否计算准确；恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同；交易3中，对称密钥选择仍为SM4，相关数据应对应无误。

7.12.19 FHDT019-00

测试目的：双算法卡，非对称算法随着算法选择进行改变，对称算法固定使用DES，动态签名能在脱机批准时被恢复，发卡行公钥和IC卡公钥分别在发卡行公钥证书和IC卡公钥证书解密中被恢复。终端也解密动态签名（被签名的动态应用数据）。

测试条件：第9章中的卡片特征28

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易2：脱机批准，CDA成功；
- c) 卡片上电（ATR）；
- d) 选择PBOC借记/贷记应用；
- e) GET PROCESSING OPTIONS命令；
- f) VERIFY命令；
- g) 第一个GENERATE AC命令请求TC和CDA处理；
- h) 交易3：脱机批准，CDA成功，DF69=00；
- i) 卡片上电（ATR）；
- j) 选择PBOC借记/贷记应用；
- k) GET PROCESSING OPTIONS命令；
- l) VERIFY命令；
- m) 第一个GENERATE AC命令请求TC和CDA处理。

通过标准：验证恢复数据：被签名的动态应用数据的长度等于IC卡公钥模长度；数据头应为‘6A’-字节1；恢复数据的结尾应为‘BC’-最后一个字节；签名数据格式应为‘05’-字节2；IC卡动态数字长度（1字节）；IC卡动态数字（2-8字节）；CID（1字节）=‘40’，与第一个GENERATE AC命令数据中获得的应用密文相同；TC（8字节），与卡片生成的相同；交易数据哈希码（20字节）在IC卡动态数据中获得；验证交易数据哈希码（20字节）是否计算准确；恢复的被签名的哈希结果与计算的被签名的哈希结果相同。交易2中，对称密钥选择为DES，相关数据应对应无误。

7.12.20 FHDT020-00

测试目的：双算法卡，非对称算法随着算法选择进行改变，对称算法固定使用DES，动态签名能在联机批准时被恢复，发卡行公钥和IC卡公钥分别在发卡行公钥证书和IC卡公钥证书解密中被恢复。终端也解密动态签名（被签名的动态应用数据）。

测试条件：第9章中的卡片特征 28

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2：联机批准；
- c) 卡片上电（ATR）；
- d) 选择 PBOC 借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；
- f) VERIFY 命令；
- g) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理；
- h) EXTERNAL AUTHENTICATE 命令；
- i) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理；
- j) 交易 3：联机批准，DF69=00；
- k) 卡片上电（ATR）；
- l) 选择 PBOC 借记/贷记应用；
- m) GET PROCESSING OPTIONS 命令；
- n) VERIFY 命令；
- o) 第一个 GENERATE AC 命令请求 ARQC 和 CDA 处理；
- p) EXTERNAL AUTHENTICATE 命令；
- q) 第二个 GENERATE AC 命令请求 TC 和 CDA 处理。

通过标准：验证第一个 GENERATE AC 命令中的恢复数据：被签名的动态应用数据的长度等于 IC 卡公钥模长度；数据头应为‘6A’- 字节 1；恢复数据的结尾应为‘BC’- 最后一个字节；签名数据格式应为‘05’- 字节 2；IC 卡动态数字长度（1 字节）；IC 卡动态数字（2-8 字节）；CID（1 字节）=‘80’，与 GENERATE AC 命令数据中获得的应用密文相同；ARQC（8 字节），与卡片生成的相同；交易数据哈希码（20 字节）在 IC 卡动态数据中获得；恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同。验证第二个 GENERATE AC 命令中的恢复数据：被签名的动态应用数据的长度等于 IC 卡公钥模长度；数据头应为‘6A’- 字节 1；恢复数据的结尾应为‘BC’- 最后一个字节；签名数据格式应为‘05’- 字节 2；IC 卡动态数字长度（1 字节）；IC 卡动态数字（2-8 字节）；CID（1 字节）=‘40’，与 GENERATE AC 命令数据中获得的应用密文相同；TC（8 字节），与卡片生成的相同；交易数据哈希码（20 字节）在 IC 卡动态数据中获得；验证交易数据哈希码（20 字节）是否计算准确；恢复的被签名的应用哈希结果与计算的被签名的应用哈希结果相同。交易 3 中，对称密钥选择仍问 DES，相关数据应对应无误。

7.13 上次交易发卡行脚本失败(JBSB)

7.13.1 JBSB001-00

测试目的：验证在联机批准交易中发卡行脚本执行成功，设置 ADA 中的“如果发卡行脚本命令在前次交易中失败，联机交易”位，不设置“联机授权指示”位，之后请求脱机批准。

测试条件：第9章中的卡片特征 20。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2：联机批准，执行发卡行脚本；
- c) 卡片上电（ATR）；
- d) 选择 PBOC 借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；

- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令;
- i) 第二个 GENERATE AC 命令请求 TC;
- j) APPLICATION UNBLOCK 命令, 正确的 MAC;
- k) 交易 3: 脱机批准。

通过标准: 交易 2: 第二个 GENERATE AC 命令, CID= '40'; 第二个 GENERATE AC 命令, CVR = '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN); APPLICATION UNBLOCK 命令, SW1 SW2= '9000'。交易 3 验证第一个 GENERATE AC 命令的卡片响应: SW1 SW2= '9000'; CID= '40'; CVR= '03 94 00 10' 或 '03 90 00 10' (用于未校验 PIN)。

7.13.2 JBSB002-00

测试目的: 在联机批准交易中发卡行脚本执行失败, 设置 ADA 中的“如果发卡行脚本命令在前次交易中失败, 联机交易”位, 设置“联机授权指示”位, 之后请求脱机批准, 卡片强制交易联机。

测试条件: 第 9 章中的卡片特征 20。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 联机批准, 执行错误的发卡行脚本命令;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令;
- i) 第二个 GENERATE AC 命令请求 TC;
- j) APPLICATION UNBLOCK 命令, 错误的 MAC;
- k) 交易 3: 请求脱机批准, 卡片强制交易联机;
- l) 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 TC, 卡片响应 ARQC;
- q) EXTERNAL AUTHENTICATE 命令;
- r) 第二个 GENERATE AC 命令请求 TC。

通过标准: 交易 2: 第二个 GENERATE AC 命令, CID= '40'; 第二个 GENERATE AC 命令, CVR = '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN); APPLICATION UNBLOCK 命令, SW1 SW2≠ '9000', 推荐返回 '6300' 或 '6988'。交易 3: 第一个 GENERATE AC 命令, CID= '80'; 第一个 GENERATE AC 命令, CVR = '03 A4 00 18' 或 '03 A0 00 18' (用于未校验 PIN); 第二个 GENERATE AC 命令, CID= '40'; 第二个 GENERATE AC 命令, CVR = '03 64 00 18' 或 '03 60 00 18' (用于未校验 PIN)。

7.13.3 JBSB003-00

测试目的: 在联机拒绝交易中发卡行脚本执行失败, 设置 ADA 中的“如果发卡行脚本命令在前次

交易中失败，联机交易”位，设置“联机授权指示”位，之后请求脱机批准，卡片强制交易联机。

测试条件：第9章中的卡片特征20。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：联机拒绝，执行错误的发卡行脚本命令；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令；

i) 第二个 GENERATE AC 命令请求 AAC；

j) APPLICATION BLOCK 命令，错误的 MAC；

k) 交易3：请求脱机批准，卡片强制交易联机；

l) 卡片上电（ATR）；

m) 选择 PBOC 借记/贷记应用；

n) GET PROCESSING OPTIONS 命令；

o) VERIFY 命令；

p) 第一个 GENERATE AC 命令请求 TC，卡片响应 ARQC；

q) EXTERNAL AUTHENTICATE 命令；

r) 第二个 GENERATE AC 命令请求 TC。

通过标准：交易2：第二个 GENERATE AC 命令，CID= ‘00’；第二个 GENERATE AC 命令，CVR = ‘03 24 00 00’ 或 ‘03 20 00 00’（用于未校验 PIN）；APPLICATION BLOCK 命令，SW1 SW2≠ ‘9000’，推荐返回 ‘6300’ 或 ‘6988’。交易3：第一个 GENERATE AC 命令，CID= ‘80’；第一个 GENERATE AC 命令，CVR = ‘03 A4 00 18’ 或 ‘03 A0 00 18’（用于未校验 PIN）；第二个 GENERATE AC 命令，CID= ‘40’；第二个 GENERATE AC 命令，CVR = ‘03 64 00 18’ 或 ‘03 60 00 18’（用于未校验 PIN）。

7.13.4 JBSB004-00

测试目的：在联机批准交易中执行 MAC 缺失的发卡行脚本命令，设置 ADA 中的“如果发卡行脚本命令在前次交易中失败，联机交易”位，设置“联机授权指示”位，之后请求脱机批准，卡片强制交易联机。

测试条件：第9章中的卡片特征20。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器。

b) 交易2：联机批准，执行无效的发卡行脚本命令（MAC 缺失）。

c) 卡片上电（ATR）。

d) 选择 PBOC 借记/贷记应用。

e) GET PROCESSING OPTIONS 命令。

f) VERIFY 命令。

g) 第一个 GENERATE AC 命令请求 ARQC。

h) EXTERNAL AUTHENTICATE 命令。

i) 第二个 GENERATE AC 命令请求 TC。

j) APPLICATION UNBLOCK 命令，MAC 缺失。

- k) 交易 3: 请求脱机批准, 卡片强制交易联机。
- l) 卡片上电 (ATR)。
- m) 选择 PBOC 借记/贷记应用。
- n) GET PROCESSING OPTIONS 命令。
- o) VERIFY 命令。
- p) 第一个 GENERATE AC 命令请求 TC, 卡片响应 ARQC。
- q) EXTERNAL AUTHENTICATE 命令。
- r) 第二个 GENERATE AC 命令请求 TC。

通过标准: 交易 2 第二个 GENERATE AC 命令: 第二个 GENERATE AC 命令, CID= '40'; 第二个 GENERATE AC 命令, CVR = '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN); APPLICATION UNBLOCK 命令, SW1 SW2≠ '9000', 推荐返回 '6300' 或 '6985'。

交易 3: 第一个 GENERATE AC 命令, CID= '80'; 第一个 GENERATE AC 命令, CVR = '03 A4 00 08' 或 '03 A0 00 08' (用于未校验 PIN); 第二个 GENERATE AC 命令, CID= '40'; 第二个 GENERATE AC 命令, CVR = '03 64 00 08' 或 '03 60 00 08' (用于未校验 PIN)。

7.13.5 JBSB005-00

测试目的: 在联机拒绝交易中执行 MAC 缺失的发卡行脚本命令, 设置 ADA 中“如果发卡行脚本命令在前次交易中失败, 联机交易”位, 设置“联机授权指示”位, 之后请求脱机批准, 卡片强制交易联机。

测试条件: 第 9 章中的卡片特征 20。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 联机拒绝, 执行无效的发卡行脚本命令 (MAC 缺失);
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令;
- i) 第二个 GENERATE AC 命令请求 AAC;
- j) APPLICATION UNBLOCK 命令, MAC 缺失;
- k) 交易 3: 请求脱机批准, 卡片强制交易联机;
- l) 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 TC, 卡片响应 ARQC;
- q) EXTERNAL AUTHENTICATE 命令;
- r) 第二个 GENERATE AC 命令请求 TC。

通过标准: 交易 2: 第二个 GENERATE AC 命令, CID= '00'; 第二个 GENERATE AC 命令, CVR = '03 24 00 00' 或 '03 20 00 00' (用于未校验 PIN); APPLICATION UNBLOCK 命令, SW1 SW2≠ '9000', 推荐返回 '6300' 或 '6987'。交易 3: 第一个 GENERATE AC 命令, CID= '80'; 第一个 GENERATE AC 命令, CVR = '03 A4 00 08' 或 '03 A0 00

08'（用于未校验 PIN）；第二个 GENERATE AC 命令，CID= '40'；第二个 GENERATE AC 命令，CVR = '03 64 00 08' 或 '03 60 00 08'（用于未校验 PIN）。

7.13.6 JBSB006-00

测试目的：在联机拒绝交易中未执行发卡行认证但执行了一个正确的脚本命令，设置 ADA 中的“如果发卡行脚本命令在前次交易中失败，联机交易”位，设置“联机授权指示”位，之后请求脱机批准，卡片强制交易联机。

测试条件：卡片类型 20，发卡行认证强制，在执行任何发卡行脚本命令前要求执行外部认证成功

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机拒绝，执行正确的发卡行脚本命令，但不执行发卡行认证；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) 执行错误的发卡行认证；

i) 第二个 GENERATE AC 命令请求 AAC；

j) APPLICATION UNBLOCK 命令，MAC 正确；

k) 交易 3：请求脱机批准，卡片强制交易联机；

l) 卡片上电（ATR）；

m) 选择 PBOC 借记/贷记应用；

n) GET PROCESSING OPTIONS 命令；

o) VERIFY 命令；

p) 第一个 GENERATE AC 命令请求 TC，卡片响应 ARQC；

q) EXTERNAL AUTHENTICATE 命令；

r) 第二个 GENERATE AC 命令请求 TC。

通过标准：交易 2：第二个 GENERATE AC 命令，CID= '00'；第二个 GENERATE AC 命令，CVR = '03 24 04 00' 或 '03 20 04 00'（用于未校验 PIN）；APPLICATION UNBLOCK 命令，SW1 SW2= '69 85'。交易 3：第一个 GENERATE AC 命令，CID= '80'；第一个 GENERATE AC 命令，CVR = '03 A4 88 18' 或 '03 A0 88 18'（用于未校验 PIN）。第二个 GENERATE AC 命令，CID= '40'；第二个 GENERATE AC 命令，CVR = '03 64 88 18' 或 '03 60 88 18'（用于未校验 PIN）。

7.14 卡片风险管理 (FXGL)

7.14.1 FXGL001-00

测试目的：第一个 GENERATE AC 请求脱机拒绝，验证卡片接受。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；

b) 选择 PBOC 借记/贷记应用；

c) GET PROCESSING OPTIONS 命令；

d) VERIFY 命令；

e) 第一个 GENERATE AC 命令请求 AAC。

通过标准：SW1 SW2= ‘9000’。

7.14.2 FXGL002-00

测试目的：第一个 GENERATE AC 请求脱机拒绝，验证卡片响应的模板。

测试条件：FXGL001-00 执行成功。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 命令请求 AAC。

通过标准：GENERATE AC 响应格式 1：响应模板标签= ‘80’，长度= ‘12’ — ‘22’。GENERATE AC 响应格式 2：响应模板标签= ‘77’，长度= ‘1D’ — ‘28’。

7.14.3 FXGL003-00

测试目的：第一个 GENERATE AC 请求脱机拒绝，验证卡片响应的 CID。

测试条件：FXGL001-00 执行成功。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 命令请求 AAC。

通过标准：GENERATE AC 响应格式 1：响应的字节 3 为 CID= ‘00’。GENERATE AC 响应格式 2：CID 标签= ‘9F27’，长度= ‘01’，值= ‘00’。

7.14.4 FXGL004-00

测试目的：第一个 GENERATE AC 请求脱机拒绝，验证卡片响应的 ATC。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：脱机拒绝交易；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 请求 AAC。

通过标准：GENERATE AC 响应格式 1：响应的字节 4、字节 5 为 ATC，其值在前次交易基础上加 1。
GENERATE AC 响应格式 2：ATC 标签= ‘9F36’，长度= ‘02’，其值在前次交易基础上加 1。

7.14.5 FXGL005-00

测试目的：第一个 GENERATE AC 请求脱机拒绝，验证卡片响应的 3DES 应用密文 AC。

测试条件：FXGL001-00 执行成功。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；

- c) GET PROCESSING OPTIONS 命令;
- d) VERIFY 命令;
- e) 第一个 GENERATE AC 请求 AAC。

通过标准: GENERATE AC 响应格式 1: 响应的字节 6 至字节 13 为 AC(8 字节), 与重新计算的密文匹配。GENERATE AC 响应格式 2: AC 标签= '9F26', 长度= '08', 与重新计算的密文匹配。

7.14.6 FXGL006-00

测试目的: 第一个 GENERATE AC 请求脱机拒绝, 验证卡片响应发卡行应用数据长度。

测试条件: FXGL001-00 执行成功。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 AAC。

通过标准: GENERATE AC 响应格式 1: 响应的字节 14 为发卡行应用数据的长度指示器, 值= '07'。
GENERATE AC 响应格式 2: 发卡行应用数据 (标签= '9F10') 返回一个长度指示器 (值= '07')。

7.14.7 FXGL007-00

测试目的: 第一个 GENERATE AC 请求脱机拒绝, 验证卡片响应的密钥索引。

测试条件: FXGL001-00 执行成功。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 AAC。

通过标准: GENERATE AC 响应格式 1: 响应的字节 15 为分散密钥索引, 值= '00' 或 '01'。GENERATE AC 响应格式 2: 发卡行应用数据 (标签= '9F10') 返回一个分散密钥索引 (值= '01')。

7.14.8 FXGL008-00

测试目的: 第一个 GENERATE AC 请求脱机拒绝, 验证卡片响应的密文版本号。

测试条件: FXGL001-00 执行成功。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 AAC。

通过标准: GENERATE AC 响应格式 1: 响应的字节 16 为密文版本号, 与卡片支持的密码一致 (01)。
GENERATE AC 响应格式 2: 发卡行应用数据 (标签= '9F10') 返回与卡片支持相一致的密文版本号 (例如: '9F 10 08 07 01 01 03 00 00 00 01')。

7.14.9 FXGL009-00

测试目的：第一个 GENERATE AC 请求脱机拒绝，验证卡片响应的卡片认证结果 CVR。

测试条件：FXGL001-00 执行成功。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 AAC。

通过标准：GENERATE AC 响应格式 1：字节 17 为 CVR 长度指示器，值=‘03’；字节 18 (CVR 字节 2)，高半字节=‘8’。GENERATE AC 响应格式 2：发卡行应用数据 (标签=‘9F10’) 返回 CVR=‘038XXXXX’。

7.14.10 FXGL010-00

测试目的：第一个 GENERATE AC 请求脱机批准，验证卡片响应接受。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 TC。

通过标准：SW1 SW2=‘9000’。

7.14.11 FXGL011-00

测试目的：第一个 GENERATE AC 请求脱机批准，验证卡片响应模板。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 TC。

通过标准：GENERATE AC 响应格式 1：响应模板标签=‘80’；响应模板长度=‘12’—‘22’。
GENERATE AC 响应格式 2：响应模板标签=‘77’；响应模板长度=‘1D’—‘28’。

7.14.12 FXGL012-00

测试目的：第一个 GENERATE AC 请求脱机批准，验证卡片响应的密文信息数据 CID。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 TC。

通过标准：GENERATE AC 响应格式 1：响应的字节 3 为 CID，值=‘40’。GENERATE AC 响应格式 2：卡响应 CID 标签=‘9F27’，长度=‘01’，值=‘40’。

7.14.13 FXGL013-00

测试目的：第一个 GENERATE AC 请求脱机批准，验证卡片响应的应用交易计数器 ATC。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：脱机接受；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 TC。

通过标准：GENERATE AC 响应格式 1：响应的字节 4、字节 5 为 ATC，其值在前次交易基础上加 1。

GENERATE AC 响应格式 2：ATC 标签=‘9F36’，长度=‘02’，其值在前次交易基础上加 1。

7.14.14 FXGL014-00

测试目的：第一个 GENERATE AC 请求脱机批准，验证卡片响应的 3DES 加密的应用密文 AC。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；

b) 选择 PBOC 借记/贷记应用；

c) GET PROCESSING OPTIONS 命令；

d) VERIFY 命令；

e) 第一个 GENERATE AC 请求 TC。

通过标准：GENERATE AC 响应格式 1：响应的字节 6 至字节 13 为 AC(8 字节)，与重新计算的密文匹配。GENERATE AC 响应格式 2：AC 标签=‘9F26’，长度=‘08’，与重新计算的密文匹配。

7.14.15 FXGL015-00

测试目的：第一个 GENERATE AC 请求脱机批准，验证卡片响应发卡行应用数据长度。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；

b) 选择 PBOC 借记/贷记应用；

c) GET PROCESSING OPTIONS 命令；

d) VERIFY 命令；

e) 第一个 GENERATE AC 请求 TC。

通过标准：GENERATE AC 响应格式 1：响应数据中的第 14 字节为发卡行应用数据中的长度，其值应为‘08’。GENERATE AC 响应格式 2：发卡行应用数据（标签=‘9F10’）中的长度为‘08’。

7.14.16 FXGL016-00

测试目的：第一个 GENERATE AC 请求脱机批准，验证卡片响应分散密钥索引。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；

b) 选择 PBOC 借记/贷记应用；

c) GET PROCESSING OPTIONS 命令；

- d) VERIFY 命令;
- e) 第一个 GENERATE AC 请求 TC。

通过标准: GENERATE AC 响应格式 1: 响应数据中的第 15 字节为分散密钥索引, 值=‘00’或‘01’。
GENERATE AC 响应格式 2: 发卡行应用数据 (标签=‘9F10’) 返回一个分散密钥索引 (值=‘01’)。

7.14.17 FXGL017-00

测试目的: 第一个 GENERATE AC 请求脱机批准, 验证卡片响应密文版本号。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 TC。

通过标准: GENERATE AC 响应格式 1: 响应的字节 16 为密文版本号, 与卡片支持的密码一致 (01)。
GENERATE AC 响应格式 2: 发卡行应用数据 (标签=‘9F10’) 返回与卡片支持相一致的密文版本号 (例如: ‘9F 10 08 07 01 01 03 00 00 00 01’)。

7.14.18 FXGL018-00

测试目的: 第一个 GENERATE AC 请求脱机批准, 验证卡片响应 CVR。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 TC。

通过标准: GENERATE AC 响应格式 1: 字节 17 为 CVR 长度指示器, 值=‘03’。字节 18 (CVR 字节 2), 高半字节=‘9’。GENERATE AC 响应格式 2: 发卡行应用数据 (标签=‘9F10’) 返回 CVR=‘039XXXXX’。

7.14.19 FXGL019-00

测试目的: 第一个 GENERATE AC 请求联机, 验证卡片响应模板。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 ARQC。

通过标准: GENERATE AC 响应格式 1: 响应模板标签=‘80’; 响应模板长度=‘12’—‘22’。
GENERATE AC 响应格式 2: 响应模板标签=‘77’; 响应模板长度=‘1D’—‘28’。

7.14.20 FXGL020-00

测试目的: 第一个 GENERATE AC 请求联机, 验证卡片响应 CID。

测试条件：第9章中的卡片特征1。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC。

通过标准：GENERATE AC 响应格式 1：响应的字节 3 为 CID，值=‘80’。GENERATE AC 响应格式 2：卡响应 CID 标签=‘9F27’，长度=‘01’，值=‘80’。

7.14.21 FXGL021-00

测试目的：第一个 GENERATE AC 请求联机，验证卡片响应 ATC。

测试条件：第9章中的卡片特征1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：终端请求联机；
c) 卡片上电（ATR）；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 请求 ARQC。

通过标准：GENERATE AC 响应格式 1：响应的字节 4、字节 5 为 ATC，其值在前次交易基础上加 1。
GENERATE AC 响应格式 2：ATC 标签=‘9F36’，长度=‘02’，其值在前次交易基础上加 1。

7.14.22 FXGL022-00

测试目的：第一个 GENERATE AC 请求联机，验证卡片响应 AC。

测试条件：第9章中的卡片特征1。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC。

通过标准：GENERATE AC 响应格式 1：响应的字节 6 至字节 13 为 AC(8 字节)，与重新计算的密文匹配。GENERATE AC 响应格式 2：AC 标签=‘9F26’，长度=‘08’，与重新计算的密文匹配。

7.14.23 FXGL023-00

测试目的：第一个 GENERATE AC 请求联机，验证卡片响应发卡行应用数据长度指示器。

测试条件：第9章中的卡片特征1。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC。

通过标准: GENERATE AC 响应格式 1: 响应的字节 14 为发卡行应用数据的长度指示器(值=‘07’)。
GENERATE AC 响应格式 2: 发卡行应用数据(标签=‘9F10’)返回一个长度指示器(值=‘07’)。

7.14.24 FXGL024-00

测试目的: 第一个 GENERATE AC 请求联机, 验证卡片响应分散密钥索引。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电(ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC。

通过标准: GENERATE AC 响应格式 1: 响应的字节 15 为分散密钥索引, 值=‘00’或‘01’。GENERATE AC 响应格式 2: 发卡行应用数据(标签=‘9F10’)返回一个分散密钥索引(值=‘01’)。

7.14.25 FXGL025-00

测试目的: 第一个 GENERATE AC 请求联机, 验证卡片响应密文版本号。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电(ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC。

通过标准: GENERATE AC 响应格式 1: 响应的字节 16 为密文版本号, 与卡片支持的密码一致(01)。
GENERATE AC 响应格式 2: 发卡行应用数据(标签=‘9F10’)返回与卡片支持相一致的密文版本号(例如: ‘9F 10 08 07 01 01 03 00 00 00 01’)。

7.14.26 FXGL026-00

测试目的: 第一个 GENERATE AC 请求联机, 验证卡片响应 CVR。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电(ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC。

通过标准: GENERATE AC 响应格式 1: 字节 17 为 CVR 长度指示器, 值=‘03’; 字节 18 (CVR 字节 2), 高半字节=‘A’。GENERATE AC 响应格式 2: 发卡行应用数据(标签=‘9F10’)返回 CVR=‘03AXXXXX’。

7.14.27 FXGL027-00

测试目的: 第二次 GENERATE AC 请求联机拒绝, 验证卡片响应接受。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电(ATR);

- b) 选择 PBOC 借记/贷记应用;
- c) GET PROCESSING OPTIONS 命令;
- d) VERIFY 命令;
- e) 第一个 GENERATE AC 请求 ARQC;
- f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- g) 第二次 GENERATE AC 请求 AAC。

通过标准: SW1 SW2= '9000' 。

7.14.28 FXGL028-00

测试目的: 第二次 GENERATE AC 请求联机拒绝, 验证卡片响应格式。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 卡片上电 (ATR) ;
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 ARQC;
 - f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 - g) 第二次 GENERATE AC 请求 AAC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应模板标签= '80' ; 响应模板长度= '12' — '22' 。

第二次 GENERATE AC 响应格式 2: 响应模板标签= '77' ; 响应模板长度= '1D' — '28' 。

7.14.29 FXGL029-00

测试目的: 第二次 GENERATE AC 请求联机拒绝, 验证卡片响应 CID。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 卡片上电 (ATR) ;
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 ARQC;
 - f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 - g) 第二次 GENERATE AC 请求 AAC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应的字节 3 为 CID, 值= '00' 。第二次 GENERATE AC 响应格式 2: 卡响应 CID 标签= '9F27' , 长度= '01' , 值= '00' 。

7.14.30 FXGL030-00

测试目的: 第二次 GENERATE AC 联机拒绝交易, 验证卡片响应 ATC。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 卡片上电 (ATR) ;
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 ARQC;
 - f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;

g) 第二次 GENERATE AC 请求 AAC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应的字节 4、字节 5 为 ATC, 其值与第一次 GENERATE AC 返回的 ATC 一致。第二次 GENERATE AC 响应格式 2: ATC 标签= '9F36', 长度= '02', 其值与第一次 GENERATE AC 返回的 ATC 一致。

7.14.31 FXGL031-00

测试目的: 第二次 GENERATE AC 请求联机拒绝, 验证卡片响应 AC。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC;
f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
g) 第二次 GENERATE AC 请求 AAC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应的字节 6 至字节 13 为 AC (8 字节), 与重新计算的密文匹配。第二次 GENERATE AC 响应格式 2: AC 标签= '9F26', 长度= '08', 与重新计算的密文匹配。

7.14.32 FXGL032-00

测试目的: 第二次 GENERATE AC 请求联机拒绝, 验证卡片响应发卡行应用数据长度指示器。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC;
f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
g) 第二次 GENERATE AC 请求 AAC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应的字节 14 为发卡行应用数据的长度指示器 (值= '07')。第二次 GENERATE AC 响应格式 2: 发卡行应用数据 (标签= '9F10') 返回一个长度指示器 (值= '07')。

7.14.33 FXGL033-00

测试目的: 第二次 GENERATE AC 请求联机拒绝, 验证卡片响应分散密钥索引。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC;
f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
g) 第二次 GENERATE AC 请求 AAC。

通过标准：第二次 GENERATE AC 响应格式 1：响应的字节 15 为分散密钥索引，值=‘00’或‘01’。
第二次 GENERATE AC 响应格式 2：发卡行应用数据（标签=‘9F10’）返回一个分散密钥索引（值=‘01’）。

7.14.34 FXGL034-00

测试目的：第二次 GENERATE AC 请求联机拒绝，验证卡片响应密文版本号。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
g) 第二次 GENERATE AC 请求 AAC。

通过标准：第二次 GENERATE AC 响应格式 1：响应的字节 16 为密文版本号，与卡片支持的密码一致（01）。第二次 GENERATE AC 响应格式 2：发卡行应用数据（标签=‘9F10’）返回与卡片支持相一致的密文版本号（例如：‘9F 10 08 07 01 01 03 00 00 00 01’）。

7.14.35 FXGL035-00

测试目的：第二次 GENERATE AC 请求联机拒绝，验证卡片响应 CVR。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
g) 第二次 GENERATE AC 请求 AAC。

通过标准：第二次 GENERATE AC 响应格式 1：字节 17 为 CVR 长度指示器，值=‘03’；字节 18（CVR 字节 2），高半字节=‘2’；字节 19（CVR 字节 3）与第一次 GENERATE AC 返回一致。第二次 GENERATE AC 响应格式 2：发卡行应用数据（标签=‘9F10’）返回 CVR=‘032XXXXX’；字节 19（CVR 字节 3）与第一次 GENERATE AC 返回一致。

7.14.36 FXGL036-00

测试目的：第二次 GENERATE AC 请求联机批准，验证卡片响应模板数据格式。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
g) 第二次 GENERATE AC 请求 TC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应模板标签=‘80’; 响应模板长度=‘12’—‘22’。
第二次 GENERATE AC 响应格式 2: 响应模板标签=‘77’; 响应模板长度=‘1D’—‘28’。

7.14.37 FXGL037-00

测试目的: 第二次 GENERATE AC 请求联机批准, 验证卡片响应 CID。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC;
f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
g) 第二次 GENERATE AC 请求 TC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应的字节 3 为 CID, 值=‘40’。第二次 GENERATE AC 响应格式 2: 卡响应 CID 标签=‘9F27’, 长度=‘01’, 值=‘40’。

7.14.38 FXGL038-00

测试目的: 第二次 GENERATE AC 请求联机批准, 验证卡片响应 ATC。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC;
f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
g) 第二次 GENERATE AC 请求 TC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应的字节 4、字节 5 为 ATC, 其值与第一次 GENERATE AC 返回的 ATC 一致。第二次 GENERATE AC 响应格式 2: ATC 标签=‘9F36’, 长度=‘02’, 其值与第一次 GENERATE AC 返回的 ATC 一致。

7.14.39 FXGL039-00

测试目的: 第二次 GENERATE AC 请求联机批准, 验证卡片响应 AC。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 请求 ARQC;
f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
g) 第二次 GENERATE AC 请求 TC。

通过标准: 第二次 GENERATE AC 响应格式 1: 响应的字节 6 至字节 13 为 AC (8 字节), 与重新计算的密文匹配。第二次 GENERATE AC 响应格式 2: AC 标签=‘9F26’, 长度=‘08’, 与重新计算的密文匹配。

7.14.40 FXGL040-00

测试目的：第二次 GENERATE AC 请求联机批准，验证卡片响应发卡行认证数据的长度。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
g) 第二次 GENERATE AC 请求 TC。

通过标准：第二次 GENERATE AC 响应格式 1：响应的字节 14 为发卡行应用数据的长度指示器（值 = ‘07’）。第二次 GENERATE AC 响应格式 2：发卡行应用数据（标签 = ‘9F10’）返回一个长度指示器（值 = ‘07’）。

7.14.41 FXGL041-00

测试目的：第二次 GENERATE AC 请求联机批准，验证卡片响应分散密钥索引。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
g) 第二次 GENERATE AC 请求 TC。

通过标准：第二次 GENERATE AC 响应格式 1：响应的字节 15 为分散密钥索引，值 = ‘00’ 或 ‘01’。
第二次 GENERATE AC 响应格式 2：发卡行应用数据（标签 = ‘9F10’）返回一个分散密钥索引（值 = ‘01’）。

7.14.42 FXGL042-00

测试目的：第二次 GENERATE AC 请求联机批准，验证卡片响应密文版本号。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
g) 第二次 GENERATE AC 请求 TC。

通过标准：第二次 GENERATE AC 响应格式 1：响应的字节 16 为密文版本号，与卡片支持的密文一致 (01)。第二次 GENERATE AC 响应格式 2：发卡行应用数据（标签 = ‘9F10’）返回与卡片支持相一致的密文版本号（例如：‘9F 10 08 07 01 01 03 00 00 00 01’）。

7.14.43 FXGL043-00

测试目的：第二次 GENERATE AC 请求联机批准，验证卡片响应 CVR。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
g) 第二次 GENERATE AC 请求 TC。

通过标准：第二次 GENERATE AC 响应格式 1：字节 17 为 CVR 长度指示器，值=‘03’；字节 18 (CVR 字节 2)，高半字节=‘6’；字节 19 (CVR 字节 3) 与第一次 GENERATE AC 返回一致。第二次 GENERATE AC 响应格式 2：发卡行应用数据 (标签=‘9F10’) 返回 CVR=‘036XXXXX’。字节 19 (CVR 字节 3) 与第一次 GENERATE AC 返回一致。

7.14.44 FXGL044-00

测试目的：验证卡片拒绝第二次 GENERATE AC 请求的联机交易。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
g) 第二次 GENERATE AC 请求 ARQC。

通过标准：第二次 GENERATE AC 卡响应 SW1 SW2≠‘9000’，建议 SW1 SW2=‘6985’。

7.14.45 FXGL045-00

测试目的：验证卡片拒绝第二次 GENERATE AC 请求的脱机交易。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 AAC；
f) 第二次 GENERATE AC 请求 TC 或 AAC。

通过标准：第二次 GENERATE AC 卡响应 SW1 SW2≠‘9000’，建议 SW1 SW2=‘6985’或‘6A86’。

7.14.46 FXGL046-00

测试目的：联机过程中，验证卡片拒绝第三个 GENERATE AC 命令。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；

- d) VERIFY 命令;
- e) 第一个 GENERATE AC 请求 ARQC;
- f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- g) 第二个 GENERATE AC 请求 TC 或 AAC;
- h) 第三个 GENERATE AC 请求 TC 或 AAC。

通过标准: 第三个 GENERATE AC 建议卡响应 SW1 SW2= '6985', 无密文返回。

7.14.47 FXGL047-00

测试目的: 当应用锁定时, 验证第一个 GENERATE AC 卡片响应 AAC。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 锁定应用;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- i) 第二次 GENERATE AC 请求 AAC;
- j) APPLICATION BLOCK 命令, MAC 正确;
- k) 交易 3: 脱机拒绝交易;
- l) 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 请求 TC 或 ARQC, 卡响应 AAC;
- q) 交易 4: 解锁应用;
- r) 卡片上电 (ATR);
- s) 选择 PBOC 借记/贷记应用;
- t) GET PROCESSING OPTIONS 命令;
- u) VERIFY 命令;
- v) 第一个 GENERATE AC 请求 AAC;
- w) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- x) APPLICATION UNBLOCK 命令, MAC 正确。

通过标准: 交易 2: APPLICATION BLOCK SW1 SW2= '9000'。交易 3: SELECT SW1 SW2= '6283'; 第一次 GENERATE AC SW1 SW2= '9000'; CID= '00'。第一次 GENERATE AC 的 CVR= '03 84 00 10' 或 '03 80 00 10' (用于未校验 PIN)。交易 4: SELECT 命令 SW1 SW2= '6283'; 第一个 GENERATE AC SW1 SW2= '9000'; APPLICATION UNBLOCK 命令 SW1 SW2= '9000'。

7.14.48 FXGL048-00

测试目的: 当卡锁定时, 验证卡片拒绝 GENERATE AC 命令。

测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK, 卡片已锁定。

测试流程: a) 卡片上电 (ATR);
 b) 选择无效的 PSE;
 c) 选择 PBOC 借记/贷记应用;
 d) GET PROCESSING OPTIONS 命令;
 e) READ RECORD 命令;
 f) GENERATE AC 命令。

通过标准: SELECT PSE 命令 SW1 SW2= '6A81'; 选择借贷记应用 SW1 SW2= '6A81'; READ RECORD SW1 SW2≠ '9000', 建议返回 '6985' 或 '6A81'; GENERATE AC SW1 SW2≠ '9000', 建议返回 '6985' 或 '6A81'。

7.15 双货币超累计交易金额上限检查 (SHJC)

7.15.1 SHJC001-00

测试目的: 脱机批准交易过程中, 累计交易总金额增加。当交易不能联机时, 验证卡片执行交易金额 (双货币) 的频度检查; 卡片包含 “累计交易总金额 (双货币)” 和 “累计交易总金额上限”; 卡片执行两次脱机交易金额为£14, 第三次交易是国内交易, 交易试图联机但不能联机, 终端接受脱机 (ARC=Y3); 当累计交易总金额超过上限 (¥50), 通过设置 “卡片请求脱机拒绝” 位, 卡片应拒绝交易, 设置 “超过频率检查” 位; 货币转换因子=20000175, 第二应用货币代码= '0826'。

测试条件: 第 9 章中的卡片特征 20。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 授权金额为£14, 交易货币代码为 '0826', 脱机批准交易;
- c) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 TC (授权金额=£14, 交易货币代码= '0826');
- i) 交易 3: 授权金额为£14, 交易货币代码为 '0826', 脱机批准交易;
- j) 第一个 GENERATE AC 请求 TC;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 TC (金额=£14, 交易货币代码= '0826');
- p) 交易 4: 批准国内交易 (金额为¥25, 不能执行联机);
- q) 卡片上电 (ATR);
- r) 选择 PBOC 借记/贷记应用;
- s) GET PROCESSING OPTIONS 命令;
- t) VERIFY 命令;
- u) 第一个 GENERATE AC 请求 ARQC (金额=¥25);
- v) 第二次 GENERATE AC 请求 TC, ARC=Y3, 卡应响应 AAC。

通过标准: 验证交易 4 第二次 GENERATE AC 的响应返回: SW1 SW2= '9000'; CID 位 8-7= '00'; CVR 字节 2 高半字节= '2'; CVR 字节 3 位 6= '1'; CVR= '03 25 20 00' 或 '03 21 20 00' (用于未校验 PIN)。

7.15.2 SHJC002-00

测试目的：脱机批准交易过程中，累计交易总金额增加。当交易不能联机时，验证卡片执行交易金额（双货币）的频度检查；卡片包含“累计交易总金额（双货币）”和“累计交易总金额上限”；卡片执行两次脱机交易金额为£14，第三次交易是国内交易，交易试图联机但不能联机，终端拒绝脱机（ARC=Z3）；当累计交易总金额超过上限（¥50），通过设置“卡片请求脱机拒绝”位卡片应拒绝交易，设置“超过频率检查”位；货币转换因子=20000175，第二应用货币代码=‘0826’。

测试条件：第9章中的卡片特征20。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：授权金额为£14，交易货币代码为‘0826’，脱机批准交易；

c) 卡片上电（ATR）；

d) 选择PBOC借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 TC（金额=£14，交易货币代码=‘0826’）；

h) 交易3：授权金额为£14，交易货币代码为‘0826’，脱机批准交易；

i) 卡片上电（ATR）；

j) 选择PBOC借记/贷记应用；

k) GET PROCESSING OPTIONS 命令；

l) VERIFY 命令；

m) 第一个 GENERATE AC 请求 TC（金额=£14，交易货币代码=‘0826’）；

n) 交易4：拒绝国内交易（金额为¥25，不能执行联机）；

o) 卡片上电（ATR）；

p) 选择PBOC借记/贷记应用；

q) GET PROCESSING OPTIONS 命令；

r) VERIFY 命令；

s) 第一个 GENERATE AC 请求 ARQC（金额=¥25）；

t) 第二次 GENERATE AC 请求 AAC，ARC=Z3，卡应响应 AAC。

通过标准：验证交易4第二次 GENERATE AC 的响应返回：SW1 SW2=‘9000’；CID 位 8-7=‘00’；CVR 字节 2 高半字节=‘2’；CVR 字节 3 位 6=‘1’；CVR=‘03 25 20 00’或‘03 21 20 00’（用于未校验 PIN）。

7.15.3 SHJC003-00

测试目的：脱机批准交易过程中，累计交易总金额增加。当交易不能联机时，验证卡片执行交易金额（双货币）的频度检查；卡片包含“累计交易总金额（双货币）”和“累计交易总金额上限”；卡片执行两次脱机拒绝交易金额为£14，第三次交易是国内交易，交易试图联机但不能联机，终端批准脱机（ARC=Y3）；不设置“超过频率检查”位；货币转换因子=20000175，第二应用货币代码=‘0826’。

测试条件：第9章中的卡片特征20。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：授权金额为£14，交易货币代码为‘0826’，脱机批准交易，脱机拒绝；

c) 卡片上电（ATR）；

d) 选择PBOC借记/贷记应用；

- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 AAC (金额=£14, 交易货币金额=0826);
- h) 交易 3: 授权金额为£14, 交易货币代码为 '0826', 脱机批准交易, 脱机拒绝;
- i) 卡片上电 (ATR);
- j) 选择 PBOC 借记/贷记应用;
- k) GET PROCESSING OPTIONS 命令;
- l) VERIFY 命令;
- m) 第一个 GENERATE AC 请求 AAC (金额=£14, 交易货币金额=0826);
- n) 交易 4: 批准国内交易 (金额为¥25, 不能执行联机);
- o) 卡片上电 (ATR);
- p) 选择 PBOC 借记/贷记应用;
- q) GET PROCESSING OPTIONS 命令;
- r) VERIFY 命令;
- s) 第一个 GENERATE AC 请求 ARQC;
- t) 第二次 GENERATE AC 请求 TC, ARC=Y3。

通过标准: 验证交易 4 第二次 GENERATE AC 的响应返回: SW1 SW2= '9000'; CID 位 8-7= '40'; CVR 字节 2 高半字节= '6'; CVR 字节 3 位 6= '0'; CVR= '03 65 00 00' 或 '03 61 00 00' (用于未校验 PIN)。

7.15.4 SHJC004-00

测试目的: 脱机批准交易过程中, 累计交易总金额增加。当交易不能联机时, 验证卡片执行交易金额 (双货币) 的频度检查; 卡片包含 “累计交易总金额 (双货币)” 和 “累计交易总金额上限”; 卡片执行两次脱机交易金额为£14, 第三次交易是国内交易, 执行联机; 不设置 “超过频率检查” 位。货币转换因子=20000175, 第二应用货币代码= '0826'。

测试条件: 第 9 章中的卡片特征 20。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 授权金额为£14, 交易货币代码为 '0826', 脱机批准交易, 脱机批准;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 请求 TC (金额=£14, 交易货币代码= '0826');
 - h) 交易 3: 授权金额为£14, 交易货币代码为 '0826', 脱机批准交易, 脱机批准;
 - i) 卡片上电 (ATR);
 - j) 选择 PBOC 借记/贷记应用;
 - k) GET PROCESSING OPTIONS 命令;
 - l) VERIFY 命令;
 - m) 第一个 GENERATE AC 请求 TC (金额=£14, 交易货币代码= '0826');
 - n) 交易 4: 批准国内交易 (金额为¥25);
 - o) 卡片上电 (ATR);
 - p) 选择 PBOC 借记/贷记应用;
 - q) GET PROCESSING OPTIONS 命令;

- r) VERIFY 命令;
- s) 第一个 GENERATE AC 请求 ARQC;
- t) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- u) 第二次 GENERATE AC 请求 TC。

通过标准: 验证交易 4 第二次 GENERATE AC 的响应返回: SW1 SW2= '9000'。CID 位 8-7= '40'。CVR 字节 2 高半字节= '6'。CVR 字节 3 位 6= '0'。CVR= '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN)。

7.16 累计脱机交易金额限制数检查 9F5C(LJTJ)

7.16.1 LJTJ001-00

测试目的: 交易不能执行联机时终端请求批准交易, 执行交易金额频度检查, 累计脱机批准交易总金额增加。

测试条件: 第 9 章中的卡片特征 20, 支持交易金额频度检查上限, 所有交易的授权金额为 ¥25。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准脱机;
- c) 交易 3: 批准脱机;
- d) 交易 4: 交易不能联机时请求批准交易;
- e) 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 请求 ARQC;
- j) 第二次 GENERATE AC 请求 TC, ARC=Y3, 卡应响应 AAC。

通过标准: 交易 2 第一个 GENERATE AC 响应: SW1 SW2= '9000'; CID= '40'; CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。交易 3 第一个 GENERATE AC 响应: SW1 SW2= '9000'; CID= '40'; CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。交易 4 第二次 GENERATE AC 响应: SW1 SW2= '9000'; CID= '00'; CVR= '03 25 20 00' 或 '03 21 20 00' (用于未校验 PIN)。

7.16.2 LJTJ002-00

测试目的: 不能执行联机时, 终端请求拒绝交易, 执行交易金额频度检查, 累计脱机批准交易总金额增加。

测试条件: 第 9 章中的卡片特征 20, 支持交易金额频度检查上限, 所有交易的授权金额为 ¥25。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准交易;
- c) 交易 3: 批准交易;
- d) 交易 4: 不能执行联机时, 请求拒绝;
- e) 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 请求 ARQC;
- j) 第二次 GENERATE AC 请求 AAC, ARC=Z3。

通过标准：交易 2 第一个 GENERATE AC 响应：SW1 SW2= ‘9000’。CID= ‘40’；CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。交易 3 第一个 GENERATE AC 响应：SW1 SW2= ‘9000’；CID= ‘40’；CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。交易 4 第二次 GENERATE AC 响应：SW1 SW2= ‘9000’；CID= ‘00’；CVR= ‘03 25 20 00’ 或 ‘03 21 20 00’（用于未校验 PIN）。

7.16.3 LJTJ003-00

测试目的：不能执行联机时，终端请求批准交易，执行交易金额频度检查，累计脱机拒绝交易金额不增加。

测试条件：第 9 章中的卡片特征 20，支持交易金额频度检查上限，所有交易的授权金额为 ¥25，脱机拒绝交易，累计脱机拒绝交易金额不增加。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：拒绝脱机；

c) 交易 3：拒绝脱机；

d) 交易 4：不能执行联机时，请求批准交易；

e) 卡片上电（ATR）；

f) 选择 PBOC 借记/贷记应用；

g) GET PROCESSING OPTIONS 命令；

h) VERIFY 命令；

i) 第一个 GENERATE AC 请求 ARQC；

j) 第二次 GENERATE AC 请求 TC，ARC=Y3。

通过标准：交易 2 第一个 GENERATE AC 响应：SW1 SW2= ‘9000’；CVR= ‘03 84 00 00’ 或 ‘03 80 00 00’（用于未校验 PIN）。交易 3 第一个 GENERATE AC 响应：SW1 SW2= ‘9000’；CID= ‘00’；CVR= ‘03 84 00 00’ 或 ‘03 80 00 00’（用于未校验 PIN）。交易 4 第二次 GENERATE AC 响应：SW1 SW2= ‘9000’；CID= ‘40’；CVR= ‘03 65 00 00’ 或 ‘03 61 00 00’（用于未校验 PIN）。

7.16.4 LJTJ004-00

测试目的：当交易联机成功时，尽管交易金额频度检查未执行，累计脱机批准交易总金额增加。

测试条件：第 9 章中的卡片特征 20，支持交易金额频度检查上限，所有交易的授权金额为 ¥25。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：批准脱机；

c) 交易 3：批准脱机；

d) 交易 4：发卡行认证有效，联机批准交易；

e) 卡片上电（ATR）；

f) 选择 PBOC 借记/贷记应用；

g) GET PROCESSING OPTIONS 命令；

h) VERIFY 命令；

i) 第一个 GENERATE AC 请求 ARQC；

j) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

k) 第二次 GENERATE AC 请求 TC。

通过标准：交易 2 第一个 GENERATE AC 响应：SW1 SW2= ‘9000’；CID= ‘40’；CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。交易 3 第一个 GENERATE AC 响应：SW1

SW2= '9000' ; CID= '40' ; CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。交易 4 第二次 GENERATE AC 响应: SW1 SW2= '9000' ; CID= '40' ; CVR= '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN)。

7.17 支付系统环境目录 (ZFML)

7.17.1 ZFML001-00

测试目的: 验证 PSE 选择后卡片接受 READ RECORD 命令。

测试条件: 第 9 章中的卡片特征 1, 支持 PSE。

测试流程: a) 卡片上电 (ATR);

b) SELECT PSE 命令;

c) READ RECORD 命令读取 PSE 中所有 DIR 文件。

通过标准: 至少第一个 READ RECORD 命令的 SW1 SW2= '9000'。

7.17.2 ZFML002-00

测试目的: 验证 PSE 选择后收到 READ RECORD 命令卡片响应的记录模板。

测试条件: 第 9 章中的卡片特征 1, 支持 PSE。

测试流程: a) 卡片上电 (ATR);

b) SELECT PSE 命令;

c) READ RECORD 命令读取 PSE 中所有 DIR 文件。

通过标准: 所有记录模板标签= '70'。记录模板的长度小于 252 字节。

7.17.3 ZFML003-00

测试目的: 验证 PSE 选择后收到 READ RECORD 命令卡片响应的应用模版。

测试条件: 第 9 章中的卡片特征 1, 支持 PSE。

测试流程: a) 卡片上电 (ATR);

b) SELECT PSE 命令;

c) READ RECORD 命令读取 PSE 中所有 DIR 文件。

通过标准: 应用模板标签= '61'。应用模板的长度小于 252 字节。

7.17.4 ZFML004-00

测试目的: 验证 PSE 选择后收到 READ RECORD 命令响应的 AID 名。

测试条件: 第 9 章中的卡片特征 1, 支持 PSE。

测试流程: a) 卡片上电 (ATR);

b) SELECT PSE 命令;

c) READ RECORD 命令读取 PSE 中所有 DIR 文件。

通过标准: ADF 名标签= '4F'。ADF 名长度范围是 '05' — '10'。

7.17.5 ZFML005-00

测试目的: 验证 PSE 选择后收到 READ RECORD 命令卡片响应的应用标签。

测试条件: 第 9 章中的卡片特征 1, 支持 PSE。

测试流程: a) 卡片上电 (ATR);

b) SELECT PSE 命令;

c) READ RECORD 命令读取 PSE 中所有 DIR 文件。

通过标准：应用标签=‘50’。应用标签的长度最大为‘10’。应用标签的值应为 ans 格式。

7.17.6 ZFML006-00

测试目的：验证 PSE 选择后收到 READ RECORD 命令卡片响应的应用首选名称。

测试条件：第 9 章中的卡片特征 1，支持 PSE 且首选应用名称存在。

测试流程：a) 卡片上电 (ATR)；
b) SELECT PSE 命令；
c) READ RECORD 命令读取 PSE 中所有 DIR 文件。

通过标准：应用首选名标签=‘9F12’。应用首选名长度最大为‘10’。应用首选名的值应为 ans 格式。

7.17.7 ZFML007-00

测试目的：验证 PSE 选择后收到 READ RECORD 命令卡片响应的应用优先指示器。

测试条件：第 9 章中的卡片特征 1，支持 PSE 且存在多个应用。

测试流程：a) 卡片上电 (ATR)；
b) SELECT PSE 命令；
c) READ RECORD 命令读取 PSE 中所有 DIR 文件。

通过标准：应用优先指示器标签=‘87’。应用优先指示器的长度为‘01’。应用优先指示器的值为‘X000XXXX’。

7.17.8 ZFML008-00

测试目的：验证 PSE 选择后收到 READ RECORD 命令卡片响应的目录自定义模板。

测试条件：第 9 章中的卡片特征 1，支持 PSE 且目录自定义模板存在。

测试流程：a) 卡片上电 (ATR)；
b) SELECT PSE 命令；
c) READ RECORD 命令读取 PSE 中所有 DIR 文件。

通过标准：目录自定义模板标签=‘73’。目录自定义模板的长度小于 252 字节。

7.17.9 ZFML009-00

测试目的：验证卡锁定后 PSE 选择收到 READ RECORD 命令，卡片应无响应数据。

测试条件：第 9 章中的卡片特征 1，支持 CARD BLOCK 命令，卡片已锁定。

测试流程：a) 卡片上电 (ATR)；
b) SELECT PSE 命令；
c) READ RECORD 命令。

通过标准：SELECT PSE SW1 SW2=‘6A81’。READ RECORD SW1 SW2≠‘9000’，建议返回‘6985’或‘6A81’。

7.18 DDA 测试 (DDCS)

7.18.1 DDCS001-00

测试目的：验证脱机批准交易中 DDA 执行成功，卡片不设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2: DDA 执行成功, 批准脱机交易;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 TC。

通过标准: 验证交易 2 第一次 GENERATE AC 卡片的响应: SW1 SW2= '9000'; CID 位 8-7= '01'; CVR 字节 2 高半字节= '9'; CVR 字节 4= '02'; CVR= '03 94 00 02' 或 '03 90 00 02' (用于未校验 PIN)。

7.18.2 DDCS002-00

测试目的: 脱机批准交易中 DDA 执行失败, 验证卡片应接受随后的脱机批准交易。

验证卡片不设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 21。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 执行 DDA 失败时, 批准脱机交易;
c) 卡片上电 (ATR);
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) INTERNAL AUTHENTICATE 命令;
g) VERIFY 命令;
h) 第一个 GENERATE AC 请求 TC;
i) 交易 3: DDA 成功, 脱机交易批准。

通过标准: 验证交易 3 第一次 GENERATE AC 卡片的响应: SW1 SW2= '9000'; CID 位 8-7= '01'; CVR 字节 2 高半字节= '9'; CVR 字节 4= '02'; CVR= '03 94 00 02' 或 '03 90 00 02' (用于未校验 PIN)。

7.18.3 DDCS003-00

测试目的: 脱机拒绝交易中 DDA 执行失败, 验证卡片应接受随后的脱机批准交易。

验证卡片设置 CVR “上次交易 DDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 21。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: DDA 执行失败, 脱机拒绝交易;
c) 卡片上电 (ATR);
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) INTERNAL AUTHENTICATE 命令;
g) VERIFY 命令;
h) 第一个 GENERATE AC 请求 AAC;
i) 交易 3: DDA 成功, 脱机交易批准。

通过标准: 验证交易 3 第一次 GENERATE AC 卡片的响应: SW1 SW2= '9000'; CID 位 8-7= '01'; CVR 字节 2 高半字节= '9'; CVR 字节 4= '06'; CVR= '03 94 00 06' 或 '03 90 00

06'（用于未校验 PIN）。

7.18.4 DDCS004-00

测试目的：脱机拒绝交易中 DDA 执行成功，验证卡片应接受随后的脱机批准交易。

验证卡片不设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：DDA 执行成功，脱机拒绝交易；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) INTERNAL AUTHENTICATE 命令；

g) VERIFY 命令；

h) 第一个 GENERATE AC 请求 AAC；

i) 交易 3：DDA 成功脱机交易批准。

通过标准：验证交易 3 第一次 GENERATE AC 卡片的响应：SW1 SW2=‘9000’；CID 位 8-7=‘01’；CVR 字节 2 高半字节=‘9’；CVR 字节 4=‘02’；CVR=‘03 94 00 02’或‘03 90 00 02’（用于未校验 PIN）。

7.18.5 DDCS005-00

测试目的：联机拒绝交易中 DDA 执行失败，验证卡片应接受随后的脱机批准交易。

验证卡片不设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：DDA 执行失败，拒绝联机交易；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) INTERNAL AUTHENTICATE 命令；

g) VERIFY 命令；

h) 第一个 GENERATE AC 请求 ARQC；

i) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

j) 第二次 GENERATE AC 请求 AAC；

k) 交易 3：DDA 成功脱机交易批准。

通过标准：验证交易 3 第一次 GENERATE AC 卡片的响应：SW1 SW2=‘9000’；CID 位 8-7=‘01’；CVR 字节 2 高半字节=‘9’；CVR 字节 4=‘02’；CVR=‘03 94 00 02’或‘03 90 00 02’（用于未校验 PIN）。

7.18.6 DDCS006-00

测试目的：联机拒绝交易中 DDA 执行成功，验证卡片应接受随后的脱机批准交易。

验证卡片不设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2: DDA 执行成功, 拒绝联机交易;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- j) 第二次 GENERATE AC 请求 AAC;
- k) 交易 3: DDA 成功, 脱机交易批准。

通过标准: 验证交易 3 第一次 GENERATE AC 卡片的响应: SW1 SW2= '9000'; CID 位 8-7= '01'; CVR 字节 2 高半字节= '9'; CVR 字节 4= '02'; CVR= '03 94 00 02' 或 '03 90 00 02' (用于未校验 PIN)。

7.18.7 DDCS007-00

测试目的: 当请求联机交易但终端不能执行联机且交易拒绝脱机 DDA 执行失败时, 验证卡片强制随后的交易联机。

卡片设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 21。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 交易请求执行联机但终端不能执行联机, DDA 执行失败, 交易脱机拒绝;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) INTERNAL AUTHENTICATE 命令;
 - g) VERIFY 命令;
 - h) 第一个 GENERATE AC 请求 ARQC;
 - i) 第二次 GENERATE AC 请求 AAC, ARC=Z3;
 - j) 交易 3: 第一次 GENERATE AC 命令, 终端请求 TC 后卡片请求联机;
 - k) 卡片上电 (ATR);
 - l) 选择 PBOC 借记/贷记应用;
 - m) GET PROCESSING OPTIONS 命令;
 - n) INTERNAL AUTHENTICATE 命令;
 - o) VERIFY 命令;
 - p) 第一个 GENERATE AC 请求 TC, 卡应响应 ARQC。

通过标准: 验证交易 3 第一次 GENERATE AC 卡片的响应: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3= '80'; CVR 字节 4= '06'; CVR= '03 A4 80 06' 或 '03 A0 80 06' (用于未校验 PIN)。

7.18.8 DDCS008-00

测试目的: 当请求联机交易但终端不能执行联机且交易拒绝脱机 DDA 执行成功时, 验证卡片强制随后的交易联机。

卡片不设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第9章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
 b) 交易 2：请求交易联机但终端不能执行联机，DDA 执行成功，交易拒绝脱机；
 c) 卡片上电（ATR）；
 d) 选择 PBOC 借记/贷记应用；
 e) GET PROCESSING OPTIONS 命令；
 f) INTERNAL AUTHENTICATE 命令成功；
 g) VERIFY 命令；
 h) 第一个 GENERATE AC 请求 ARQC；
 i) 第二次 GENERATE AC 请求 AAC，ARC=Z3；
 j) 交易 3：第一次 GENERATE AC 命令，终端请求 TC 后卡片请求联机；
 k) 卡片上电（ATR）；
 l) 选择 PBOC 借记/贷记应用；
 m) GET PROCESSING OPTIONS 命令；
 n) INTERNAL AUTHENTICATE 命令成功；
 o) VERIFY 命令；
 p) 第一个 GENERATE AC 请求 TC，卡应响应 ARQC。

通过标准：验证交易 3 第一次 GENERATE AC 卡片的响应：SW1 SW2=‘9000’；CID 位 8-7=‘10’；CVR 字节 2 高半字节=‘A’；CVR 字节 3=‘80’；CVR 字节 4=‘02’；CVR=‘03 A4 80 02’或‘03 A0 80 02’（用于未校验 PIN）。

7.18.9 DDCS009-00

测试目的：脱机拒绝交易（交易 2）中 DDA 执行失败，交易脱机拒绝（交易 3），验证卡片接受随后的联机交易。

卡片设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第9章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
 b) 交易 2：DDA 失败，拒绝脱机交易；
 c) 卡片上电（ATR）；
 d) 选择 PBOC 借记/贷记应用；
 e) GET PROCESSING OPTIONS 命令；
 f) INTERNAL AUTHENTICATE 命令；
 g) VERIFY 命令；
 h) 第一个 GENERATE AC 请求 AAC；
 i) 交易 3：DDA 成功，拒绝脱机交易；
 j) 卡片上电（ATR）；
 k) 选择 PBOC 借记/贷记应用；
 l) GET PROCESSING OPTIONS 命令；
 m) INTERNAL AUTHENTICATE 命令成功；
 n) VERIFY 命令；
 o) 第一个 GENERATE AC 请求 AAC；
 p) 交易 4：DDA 成功，批准联机交易；
 q) 卡片上电（ATR）；

- r) 选择 PBOC 借记/贷记应用;
- s) GET PROCESSING OPTIONS 命令;
- t) INTERNAL AUTHENTICATE 命令成功;
- u) VERIFY 命令;
- v) 第一个 GENERATE AC 请求 ARQC;
- w) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- x) 第二次 GENERATE AC 请求 TC。

通过标准: 交易 2 第一次 GENERATE AC 卡片响应: SW1 SW2= '9000' ; CID= '00' ; CVR= '03 84 00 02' 或 '03 80 00 02' (用于未校验 PIN)。交易 3 第一次 GENERATE AC 卡片响应: SW1 SW2= '9000' ; CID= '00' ; CVR= '03 84 00 06' 或 '03 80 00 06' (用于未校验 PIN)。交易 4 第一次 GENERATE AC 卡片响应: SW1 SW2= '9000' ; CID= '40' ; CVR= '03 64 00 06' 或 '03 60 00 06' (用于未校验 PIN)。

7.18.10 DDCS010-00

测试目的: 脱机拒绝交易 (交易 2) 中 DDA 失败、脱机批准交易 (交易 3) 后, 验证卡片接受随后的脱机批准交易。

测试条件: 第 9 章中的卡片特征 21。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: DDA 执行失败, 拒绝脱机交易;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令失败;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: DDA 成功脱机交易批准;
- j) 交易 4: DDA 成功脱机交易批准。

通过标准: 验证交易 4 第一次 GENERATE AC 卡片的响应: SW1 SW2= '9000' ; CID 位 8-7= '01' ; CVR 字节 2 高半字节= '9' ; CVR 字节 4= '06' ; CVR= '03 94 00 06' 或 '03 90 00 06' (用于未校验 PIN)。

7.18.11 DDCS011-00

测试目的: 脱机拒绝交易 (交易 2) 中 DDA 执行失败、发卡行认证失败联机拒绝交易 (交易 3)、交易强制联机 (交易 4)、交易批准脱机 (交易 5), 验证卡片接受随后的脱机批准交易。

卡片不设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 21。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: DDA 失败拒绝脱机;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令;

- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: DDA 成功, 发卡行认证无效, 拒绝联机交易;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) INTERNAL AUTHENTICATE 命令成功;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- q) 第二次 GENERATE AC 请求 TC, 卡应响应 AAC;
- r) 交易 4: DDA 成功, 批准联机交易;
- s) 卡片上电 (ATR);
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) INTERNAL AUTHENTICATE 命令成功;
- w) VERIFY 命令;
- x) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- y) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- z) 第二次 GENERATE AC 请求 TC;
- aa) 交易 5: DDA 成功, 批准脱机交易;
- ab) 卡片上电 (ATR);
- ac) 选择 PBOC 借记/贷记应用;
- ad) GET PROCESSING OPTIONS 命令;
- ae) INTERNAL AUTHENTICATE 命令成功;
- af) VERIFY 命令;
- ag) 第一个 GENERATE AC 请求 TC。

通过标准: 交易 2 第一次 GENERATE AC 响应: SW1 SW2= '9000' ; CID= '00' ; CVR= '03 84 00 02' 或 '03 80 00 02' (用于未校验 PIN)。交易 3 第二次 GENERATE AC 响应: SW1 SW2= '9000' ; CID= '00' ; CVR= '03 2C 00 06' 或 '03 28 00 06' (用于未校验 PIN)。交易 4 第二次 GENERATE AC 响应: SW1 SW2= '9000' ; CID= '40' ; CVR= '03 64 88 06' 或 '03 60 88 06' (用于未校验 PIN)。交易 5 第一次 GENERATE AC 响应: SW1 SW2= '9000' ; CID= '40' ; CVR= '03 94 00 02' 或 '03 90 00 02' (用于未校验 PIN)。

7.18.12 DDCS012-00

测试目的: DDA 执行失败卡片接受脱机拒绝交易 (交易 2), 发卡行认证失败交易强制联机 (交易 3)、发卡行认证失败交易被拒绝 (交易 4)、卡片强制交易联机 (交易 5)。

验证卡片设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 21。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: DDA 执行失败, 拒绝脱机;

c) 卡片上电 (ATR);

- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令失败;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: DDA 执行成功, 发卡行认证无效, 拒绝联机交易;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) INTERNAL AUTHENTICATE 命令成功;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- q) 第二次 GENERATE AC 请求 TC, 卡应响应 AAC;
- r) 交易 4: DDA 成功, 发卡行认证无效, 拒绝联机交易;
- s) 卡片上电 (ATR);
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) INTERNAL AUTHENTICATE 命令成功;
- w) VERIFY 命令;
- x) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- y) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- z) 第二次 GENERATE AC 请求 TC, 卡应响应 AAC;
- aa) 交易 5: 第一次 GENERATE AC 终端请求 TC 后, 卡片请求执行联机;
- ab) 卡片上电 (ATR);
- ac) 选择 PBOC 借记/贷记应用;
- ad) GET PROCESSING OPTIONS 命令;
- ae) INTERNAL AUTHENTICATE 命令成功;
- af) VERIFY 命令;
- ag) 第一个 GENERATE AC 请求 TC, 卡应响应 ARQC。

通过标准: 交易 2 第一次 GENERATE AC: CID= '00'; CVR= '03 84 00 02' 或 '03 80 00 02' (用于未校验 PIN)。交易 3 第一次 GENERATE AC: CID= '80'; CVR= '03 A4 00 06' 或 '03 A0 00 06' (用于未校验 PIN)。交易 3 第二次 GENERATE AC: CID= '00'; CVR= '03 2C 00 06' 或 '03 28 00 06' (用于未校验 PIN)。交易 4 第一次 GENERATE AC: CID= '80'; CVR= '03 A4 88 06' 或 '03 A0 88 06' (用于未校验 PIN)。交易 4 第二次 GENERATE AC: CID= '00'; CVR= '03 2C 88 06' 或 '03 28 88 06' (用于未校验 PIN)。交易 5 第一次 GENERATE AC: CID= '80'; CVR= '03 A4 A8 06' 或 '03 A0 A8 06' (用于未校验 PIN)。

7.18.13 DDCS013-00

测试目的: 脱机拒绝交易 (交易 2) 中终端不能执行联机且 DDA 执行失败; 终端不能执行联机但强制交易联机, 交易拒绝脱机 (交易 3); 验证卡片接受随后的脱机交易。

卡片设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第9章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2：不能执行联机，DDA 失败，拒绝交易；
- c) 卡片上电（ATR）；
- d) 选择 PBOC 借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；
- f) INTERNAL AUTHENTICATE 命令失败；
- g) VERIFY 命令；
- h) 第一个 GENERATE AC 请求 ARQC；
- i) 第二次 GENERATE AC 请求 AAC，ARC=Z3；
- j) 交易 3：卡片请求执行联机，DDA 成功，拒绝交易不能执行联机；
- k) 卡片上电（ATR）；
- l) 选择 PBOC 借记/贷记应用；
- m) GET PROCESSING OPTIONS 命令；
- n) INTERNAL AUTHENTICATE 命令成功；
- o) VERIFY 命令；
- p) 第一个 GENERATE AC 请求 TC，卡响应 ARQC；
- q) 第二次 GENERATE AC 请求 AAC，ARC=Z3；
- r) 交易 4：请求脱机批准，DDA 成功，卡片强制交易联机；
- s) 卡片上电（ATR）；
- t) 选择 PBOC 借记/贷记应用；
- u) GET PROCESSING OPTIONS 命令；
- v) INTERNAL AUTHENTICATE 命令成功；
- w) VERIFY 命令；
- x) 第一个 GENERATE AC 请求 TC，卡响应 ARQC。

通过标准：交易 2 第一次 GENERATE AC：CID= ‘80’；CVR= ‘03 A4 00 02’ 或 ‘03 A0 00 02’（用于未校验 PIN）。交易 2 第二次 GENERATE AC：CID= ‘00’；CVR= ‘03 25 00 02’ 或 ‘03 21 00 02’（用于未校验 PIN）。交易 3 第一次 GENERATE AC：CID= ‘80’；CVR= ‘03 A4 80 06’ 或 ‘03 A0 80 06’（用于未校验 PIN）。交易 3 第二次 GENERATE AC：CID= ‘00’；CVR= ‘03 25 80 06’ 或 ‘03 21 80 06’（用于未校验 PIN）。交易 4 第一次 GENERATE AC：SW1 SW2= ‘9000’；CID= ‘80’；CVR= ‘03 A4 80 06’ 或 ‘03 A0 80 06’（用于未校验 PIN）。

7.18.14 DDCS014-00

测试目的：脱机拒绝交易中 DDA 执行失败（交易 2），联机批准交易发卡行认证未执行（交易 3），验证卡片强制随后的交易联机。

测试条件：第9章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2：DDA 执行失败，拒绝脱机交易；
- c) 卡片上电（ATR）；
- d) 选择 PBOC 借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；
- f) INTERNAL AUTHENTICATE 命令失败；

- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: 未执行发卡行认证, 拒绝联机;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) INTERNAL AUTHENTICATE 命令成功;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 ARQC;
- p) 第二次 GENERATE AC 请求 AAC;
- q) 交易 4: 第一次 GENERATE AC 终端请求 TC 后, 卡片请求执行联机;
- r) 卡片上电 (ATR);
- s) 选择 PBOC 借记/贷记应用;
- t) GET PROCESSING OPTIONS 命令;
- u) INTERNAL AUTHENTICATE 命令成功;
- v) VERIFY 命令;
- w) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证交易 4 第一次 GENERATE AC 卡片的响应返回: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3= '88'; CVR 字节 4= '06'; CVR= '03 A4 88 06' 或 '03 A0 88 06' (用于未校验 PIN)。

7.18.15 DDCS015-00

测试目的: 请求联机交易但终端不能执行联机, 交易批准脱机 DDA 执行失败, 验证卡片请求随后的交易联机。

卡片不设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 21。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 交易请求执行联机但终端不能执行联机。DDA 执行失败, 交易批准脱机;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) INTERNAL AUTHENTICATE 命令;
 - g) VERIFY 命令;
 - h) 第一个 GENERATE AC 请求 ARQC;
 - i) 第二次 GENERATE AC 请求 TC, ARC=Y3;
 - j) 交易 3: 第一次 GENERATE AC 终端请求 TC 后, 卡片请求执行联机;
 - k) 卡片上电 (ATR);
 - l) 选择 PBOC 借记/贷记应用;
 - m) GET PROCESSING OPTIONS 命令;
 - n) INTERNAL AUTHENTICATE 命令;
 - o) VERIFY 命令;
 - p) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证交易 3 第一次 GENERATE AC 卡片的响应返回: SW1 SW2= '9000'; CID 位 8-7=

‘10’；CVR 字节 2 高半字节= ‘A’；CVR 字节 4= ‘02’；CVR= ‘03 A4 80 02’ 或 ‘03 A0 80 02’（用于未校验 PIN）。

7.18.16 DDCS016-00

测试目的：脱机拒绝交易 DDA 失败（交易 2），发卡行认证不成功卡片强制批准联机交易（交易 3），终端不能执行联机交易批准脱机（交易 4），交易强制联机（交易 5），验证卡片接受。验证卡片设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 21。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2：DDA 失败，拒绝脱机；
- c) 选择 PBOC 借记/贷记应用；
- e) GET PROCESSING OPTIONS 命令；
- f) INTERNAL AUTHENTICATE 命令失败；
- g) VERIFY 命令；
- h) 第一个 GENERATE AC 请求 AAC；
- i) 交易 3：DDA 执行成功，发卡行认证失败，终端请求批准联机交易，卡片拒绝；
- j) 卡片上电（ATR）；
- k) 选择 PBOC 借记/贷记应用；
- l) GET PROCESSING OPTIONS 命令；
- m) INTERNAL AUTHENTICATE 命令；
- n) VERIFY 命令；
- o) 第一个 GENERATE AC 请求 ARQC；
- p) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；
- q) 第二次 GENERATE AC 请求 TC，卡应响应 AAC；
- r) 交易 4：DDA 执行成功，卡片最初强制交易联机但终端不能执行交易联机，批准交易；
- s) 卡片上电（ATR）；
- t) 选择 PBOC 借记/贷记应用；
- u) GET PROCESSING OPTIONS 命令；
- v) INTERNAL AUTHENTICATE 命令成功；
- w) VERIFY 命令；
- x) 第一个 GENERATE AC 请求 TC，卡响应 ARQC；
- y) 第二次 GENERATE AC 请求 TC，ARC=Y3；
- z) 交易 5：DDA 执行成功请求批准脱机，卡片强制交易联机；
- aa) 卡片上电（ATR）；
- ab) 选择 PBOC 借记/贷记应用；
- ac) GET PROCESSING OPTIONS 命令；
- ad) INTERNAL AUTHENTICATE 命令成功；
- ae) VERIFY 命令；
- af) 第一个 GENERATE AC 请求 TC，卡响应 ARQC。

通过标准：交易 2 第一次 GENERATE AC：CID= ‘00’；CVR= ‘03 84 00 02’ 或 ‘03 80 00 02’（用于未校验 PIN）。交易 3 第一次 GENERATE AC：CID= ‘80’；CVR= ‘03 A4 00 06’ 或 ‘03 A0 00 06’（用于未校验 PIN）。交易 3 第二次 GENERATE AC：CID= ‘00’；

CVR= ‘03 2C 00 06’ 或 ‘03 28 00 06’（用于未校验 PIN）。交易 4 第一次 GENERATE AC: CID= ‘80’；CVR= ‘03 A4 88 06’ 或 ‘03 A0 88 06’（用于未校验 PIN）。交易 4 第二次 GENERATE AC: CID= ‘40’；CVR= ‘03 65 88 06’ 或 ‘03 61 88 06’（用于未校验 PIN）。交易 5 第一次 GENERATE AC: SW1 SW2= ‘9000’；CID= ‘80’；CVR= ‘03 A4 A8 06’ 或 ‘03 A0 A8 06’（用于未校验 PIN）。

7.18.17 DDCS017-00

测试目的：脱机拒绝交易中终端不能执行联机且 DDA 失败（交易 2），交易强制联机，但终端不能执行联机，交易批准脱机（交易 3），验证卡片请求执行联机。

验证卡片设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 22。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：交易请求联机但终端不能执行联机，DDA 执行失败，交易拒绝脱机；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) INTERNAL AUTHENTICATE 命令；

g) VERIFY 命令；

h) 第一个 GENERATE AC 请求 ARQC，TVR 字节 1 位 4= ‘1’ 表明 DDA 执行失败；

i) 第二次 GENERATE AC 请求 AAC，TVR 字节 1 位 4= ‘1’ 表明 DDA 执行失败，ARC=Z3；

j) 交易 3：第一次 GENERATE AC 终端请求 TC 后，卡片请求执行联机。终端不能执行联机，交易批准脱机；

k) 卡片上电（ATR）；

l) 选择 PBOC 借记/贷记应用；

m) GET PROCESSING OPTIONS 命令；

n) INTERNAL AUTHENTICATE 命令成功；

o) VERIFY 命令；

p) 第一个 GENERATE AC 请求 TC，卡响应 ARQC；

q) 第二次 GENERATE AC 请求 TC，ARC=Y3；

r) 交易 4：第一次 GENERATE AC 终端请求 TC 后，卡片请求交易联机；

s) 卡片上电（ATR）；

t) 选择 PBOC 借记/贷记应用；

u) GET PROCESSING OPTIONS 命令；

v) INTERNAL AUTHENTICATE 命令成功；

w) VERIFY 命令；

x) 第一个 GENERATE AC 请求 TC，卡响应 ARQC。

通过标准：验证交易 4 第一次 GENERATE AC 卡片的响应：SW1 SW2= ‘9000’；CID 位 8-7= ‘10’；CVR 字节 2 高半字节= ‘A’；CVR 字节 4= ‘06’；CVR= ‘03 A4 80 06’ 或 ‘03 A0 80 06’（用于未校验 PIN）。

7.18.18 DDCS018-00

测试目的：验证卡片接受脱机拒绝交易 DDA 失败（交易 2），发卡行认证失败卡片强制交易联机（交易 3），终端不能执行联机交易批准脱机（交易 4），交易强制联机（交易 5）。

验证卡片设置 CVR 的“上次交易 DDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 22。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：DDA 失败，拒绝脱机交易；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) INTERNAL AUTHENTICATE 命令，哈希结果不匹配；

g) VERIFY 命令；

h) 第一个 GENERATE AC 请求 AAC；

i) 交易 3：批准联机，DDA 执行成功，发卡行认证失败；

j) 卡片上电（ATR）；

k) 选择 PBOC 借记/贷记应用；

l) GET PROCESSING OPTIONS 命令；

m) INTERNAL AUTHENTICATE 命令；

n) VERIFY 命令；

o) 第一个 GENERATE AC 请求 ARQC；

p) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；

q) 第二次 GENERATE AC 请求 TC；

r) 交易 4：DDA 执行成功，最初卡片强制联机，但终端不能执行联机，批准交易；

s) 卡片上电（ATR）；

t) 选择 PBOC 借记/贷记应用；

u) GET PROCESSING OPTIONS 命令；

v) INTERNAL AUTHENTICATE 命令；

w) VERIFY 命令；

x) 第一个 GENERATE AC 请求 TC，卡响应 ARQC；

y) 第二次 GENERATE AC 请求 TC，ARC=Y3；

z) 交易 5：DDA 成功，请求批准脱机，卡片强制交易联机；

aa) 卡片上电（ATR）；

ab) 选择 PBOC 借记/贷记应用；

ac) GET PROCESSING OPTIONS 命令；

ad) INTERNAL AUTHENTICATE 命令成功；

ae) VERIFY 命令；

af) 第一个 GENERATE AC 请求 TC，卡响应 ARQC。

通过标准：交易 2 第一次 GENERATE AC：CID=‘00’；CVR=‘03 84 00 02’或‘03 80 00 02’（用于未校验 PIN）。交易 3 第一次 GENERATE AC：CID=‘80’；CVR=‘03 A4 00 06’或‘03 A0 00 06’（用于未校验 PIN）。交易 3 第二次 GENERATE AC：CID=‘40’；CVR=‘03 6C 00 06’或‘03 68 00 06’（用于未校验 PIN）。交易 4 第一次 GENERATE AC：CID=‘80’；CVR=‘03 A4 88 06’或‘03 A0 88 06’（用于未校验 PIN）。交易 4 第二次 GENERATE AC CID=‘40’；CVR=‘03 65 88 06’或‘03 61 88 06’（用于未校验 PIN）。交易 5 第一次 GENERATE AC：SW1 SW2=‘9000’；CID=‘80’；CVR=‘03 A4 A8 06’或‘03 A0 A8 06’（用于未校验 PIN）。

测试目的：验证卡片动态数据认证响应正确，签名数据正确。

测试条件：第9章中的卡片特征3（1152位密钥 仅支持DDA卡片）

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：DDA失败，拒绝脱机交易；
c) 卡片上电（ATR）；
d) 选择PBOC借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) INTERNAL AUTHENTICATE 命令，哈希结果不匹配；
g) VERIFY 命令；
h) 第一个 GENERATE AC 请求 AAC；
i) 交易3：批准联机，DDA执行成功，发卡行认证失败；
j) 卡片上电（ATR）；
k) 选择PBOC借记/贷记应用；
l) GET PROCESSING OPTIONS 命令；
m) INTERNAL AUTHENTICATE 命令；
n) VERIFY 命令；
o) 第一个 GENERATE AC 请求 ARQC；
p) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；
q) 第二次 GENERATE AC 请求 TC；
r) 交易4：DDA执行成功，最初卡片强制联机，但终端不能执行联机，批准交易；
s) 卡片上电（ATR）；
t) 选择PBOC借记/贷记应用；
u) GET PROCESSING OPTIONS 命令；
v) INTERNAL AUTHENTICATE 命令；
w) VERIFY 命令；
x) 第一个 GENERATE AC 请求 TC，卡响应 ARQC；
y) 第二次 GENERATE AC 请求 TC，ARC=Y3；
z) 交易5：DDA成功，请求批准脱机，卡片强制交易联机；
aa) 卡片上电（ATR）；
ab) 选择PBOC借记/贷记应用；
ac) GET PROCESSING OPTIONS 命令；
ad) INTERNAL AUTHENTICATE 命令成功；
ae) VERIFY 命令；
af) 第一个 GENERATE AC 请求 TC，卡响应 ARQC。

通过标准：验证DDA中的数据是否正确。验证9F10中的对称算法标识是否正确。

7.18.20 DDCS020-00

测试目的：验证卡片动态数据认证响应正确，签名数据正确。

测试条件：第9章中的卡片特征4（1408位密钥 仅支持DDA卡片）

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：DDA失败，拒绝脱机交易；
c) 卡片上电（ATR）；
d) 选择PBOC借记/贷记应用；

- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令, 哈希结果不匹配;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: 批准联机, DDA 执行成功, 发卡行认证失败;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) INTERNAL AUTHENTICATE 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- q) 第二次 GENERATE AC 请求 TC;
- r) 交易 4: DDA 执行成功, 最初卡片强制联机, 但终端不能执行联机, 批准交易;
- s) 卡片上电 (ATR);
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) INTERNAL AUTHENTICATE 命令;
- w) VERIFY 命令;
- x) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- y) 第二次 GENERATE AC 请求 TC, ARC=Y3;
- z) 交易 5: DDA 成功, 请求批准脱机, 卡片强制交易联机;
- aa) 卡片上电 (ATR);
- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) INTERNAL AUTHENTICATE 命令成功;
- ae) VERIFY 命令;
- af) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证 DDA 中的数据是否正确。验证 9F10 中的对称算法标识是否正确。

7.18.21 DDCS021-00

测试目的: 验证卡片动态数据认证响应正确, 签名数据正确。

测试条件: 第 9 章中的卡片特征 5 (1976 位密钥 支持 DDA 卡片)

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: DDA 失败, 拒绝脱机交易;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令, 哈希结果不匹配;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: 批准联机, DDA 执行成功, 发卡行认证失败;
- j) 卡片上电 (ATR);

- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) INTERNAL AUTHENTICATE 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- q) 第二次 GENERATE AC 请求 TC;
- r) 交易 4: DDA 执行成功, 最初卡片强制联机, 但终端不能执行联机, 批准交易;
- s) 卡片上电 (ATR) ;
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) INTERNAL AUTHENTICATE 命令;
- w) VERIFY 命令;
- x) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- y) 第二次 GENERATE AC 请求 TC, ARC=Y3;
- z) 交易 5: DDA 成功, 请求批准脱机, 卡片强制交易联机;
- aa) 卡片上电 (ATR) ;
- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) INTERNAL AUTHENTICATE 命令成功;
- ae) VERIFY 命令;
- af) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证 DDA 中的数据是否正确。验证 9F10 中的对称算法标识是否正确。

7.18.22 DDCS022-00

测试目的: 验证卡片动态数据认证响应正确, 签名数据正确。

测试条件: 第 9 章中的卡片特征 7 (1152 位密钥 支持 DDA CDA 卡片)

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: DDA 失败, 拒绝脱机交易;
- c) 卡片上电 (ATR) ;
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令, 哈希结果不匹配;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: 批准联机, DDA 执行成功, 发卡行认证失败;
- j) 卡片上电 (ATR) ;
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) INTERNAL AUTHENTICATE 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;

- q) 第二次 GENERATE AC 请求 TC;
- r) 交易 4: DDA 执行成功, 最初卡片强制联机, 但终端不能执行联机, 批准交易;
- s) 卡片上电 (ATR);
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) INTERNAL AUTHENTICATE 命令;
- w) VERIFY 命令;
- x) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- y) 第二次 GENERATE AC 请求 TC, ARC=Y3;
- z) 交易 5: DDA 成功, 请求批准脱机, 卡片强制交易联机;
- aa) 卡片上电 (ATR);
- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) INTERNAL AUTHENTICATE 命令成功;
- ae) VERIFY 命令;
- af) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证 DDA 中的数据是否正确。验证 9F10 中的对称算法标识是否正确。

7.18.23 DDCS023-00

测试目的: 验证卡片动态数据认证响应正确, 签名数据正确。

测试条件: 第 9 章中的卡片特征 8 (1408 位密钥 支持 DDA CDA 卡片)

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: DDA 失败, 拒绝脱机交易;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令, 哈希结果不匹配;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: 批准联机, DDA 执行成功, 发卡行认证失败;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) INTERNAL AUTHENTICATE 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- q) 第二次 GENERATE AC 请求 TC;
- r) 交易 4: DDA 执行成功, 最初卡片强制联机, 但终端不能执行联机, 批准交易;
- s) 卡片上电 (ATR);
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) INTERNAL AUTHENTICATE 命令;

- w) VERIFY 命令;
- x) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- y) 第二次 GENERATE AC 请求 TC, ARC=Y3;
- z) 交易 5: DDA 成功, 请求批准脱机, 卡片强制交易联机;
- aa) 卡片上电 (ATR);
- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) INTERNAL AUTHENTICATE 命令成功;
- ae) VERIFY 命令;
- af) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证 DDA 中的数据是否正确。验证 9F10 中的对称算法标识是否正确。

7.18.24 DDCS024-00

测试目的: 验证卡片动态数据认证响应正确, 签名数据正确。

测试条件: 第 9 章中的卡片特征 9 (1976 位密钥 支持 DDA CDA 卡片)

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: DDA 失败, 拒绝脱机交易;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令, 哈希结果不匹配;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 请求 AAC;
- i) 交易 3: 批准联机, DDA 执行成功, 发卡行认证失败;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) INTERNAL AUTHENTICATE 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- q) 第二次 GENERATE AC 请求 TC;
- r) 交易 4: DDA 执行成功, 最初卡片强制联机, 但终端不能执行联机, 批准交易;
- s) 卡片上电 (ATR);
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) INTERNAL AUTHENTICATE 命令;
- w) VERIFY 命令;
- x) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- y) 第二次 GENERATE AC 请求 TC, ARC=Y3;
- z) 交易 5: DDA 成功, 请求批准脱机, 卡片强制交易联机;
- aa) 卡片上电 (ATR);
- ab) 选择 PBOC 借记/贷记应用;

- ac) GET PROCESSING OPTIONS 命令;
- ad) INTERNAL AUTHENTICATE 命令成功;
- ae) VERIFY 命令;
- af) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证 DDA 中的数据是否正确。验证 9F10 中的对称算法标识是否正确。

7.18.25 DDCS025-00

测试目的: 在非对称算法随 DF61 进行切换的同时, 对称算法固定为 SM4, 验证卡片动态数据认证响应正确, 签名数据正确 (双算法 27)。

测试条件: 第 9 章中的卡片特征双算法 27 (双算法中非对称算法为 RSA/SHA1, 对称算法为 SM4)

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: DDA 成功, DF69=01, 采用国密算法;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令, 哈希结果匹配;
- g) 第一个 GENERATE AC 请求 TC;
- h) 交易 3: DDA 成功, DF69=00, 采用国际算法;
- i) 卡片上电 (ATR);
- j) 选择 PBOC 借记/贷记应用;
- k) GET PROCESSING OPTIONS 命令;
- l) INTERNAL AUTHENTICATE 命令, 哈希结果匹配;
- m) 第一个 GENERATE AC 请求 TC。

通过标准: 验证 DDA 中的数据是否正确。验证 9F10 中的对称算法标识是否正确。交易 3 中密文和 mac 计算使用的认为 SM4 算法, 9F10 中的算法指示器同时指示为 SM4。

7.18.26 DDCS026-00

测试目的: 在非对称算法随 DF61 进行切换的同时, 对称算法固定为 DES, 验证卡片动态数据认证响应正确, 签名数据正确 (双算法 27)。

测试条件: 第 9 章中的卡片特征双算法 27 (双算法中非对称算法为 RSA/SHA1, 对称算法为 SM4)

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: DDA 成功, DF69=01, 采用国密算法;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) INTERNAL AUTHENTICATE 命令, 哈希结果匹配;
- g) 第一个 GENERATE AC 请求 TC;
- h) 交易 3: DDA 成功, DF69=00, 采用国际算法;
- i) 卡片上电 (ATR);
- j) 选择 PBOC 借记/贷记应用;
- k) GET PROCESSING OPTIONS 命令;
- l) INTERNAL AUTHENTICATE 命令, 哈希结果匹配;
- m) 第一个 GENERATE AC 请求 TC。

通过标准：验证 DDA 中的数据是否正确。验证 9F10 中的对称算法标识是否正确。交易 2 中密文和 mac 计算使用的认为 DES 算法，9F10 中的算法指示器同时指示为 DES。

7.19 更新卡片数据 (GXSJ)

7.19.1 GXSJ001-00

测试目的：当发卡行认证成功交易联机批准时，第二次 GENERATE AC 命令后执行 PUT DATA 命令修改 LCOL，验证卡片接受 PUT DATA 命令。验证卡片接受新的 LCOL 值。当前的脱机交易下限值是 3，此次交易后该值应为 2。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：发卡行认证成功，批准联机。PUT DATA 命令修改 LCOL 成功；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
i) 第二次 GENERATE AC 请求 TC；
j) PUT DATA 命令修改 LCOL，MAC 正确；
k) 交易 3：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
l) 交易 4：脱机批准；
m) 交易 5：脱机批准；
n) 交易 6：第一次 GENERATE AC 终端请求 TC，卡片请求执行联机；
o) 卡片上电 (ATR)；
p) 选择 PBOC 借记/贷记应用；
q) GET PROCESSING OPTIONS 命令；
r) VERIFY 命令；
s) 第一个 GENERATE AC 请求 TC，卡响应 ARQC。

通过标准：验证交易 2 PUT DATA 命令返回 SW1 SW2= '9000'。验证交易 6 第一次 GENERATE AC 的响应：SW1 SW2= '9000'；CID 位 8-7= '10'；CVR 字节 2 高半字节= 'A'；CVR 字节 3 位 6= '1'；

7.19.2 GXSJ002-00

测试目的：联机拒绝交易过程中（发卡行认证成功），验证卡片接受 PUT DATA 命令修改 LCOL。验证卡片接受脱机交易下限的新值。当前的脱机交易下限值是 3，此次交易后该值应为 2。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：发卡行认证成功拒绝联机交易，PUT DATA 命令修改 LCOL 成功；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；

- g) 第一个 GENERATE AC 请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- i) 第二次 GENERATE AC 请求 AAC;
- j) PUT DATA 命令修改 LCOL, MAC 正确;
- k) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- l) 交易 4: 脱机批准;
- m) 交易 5: 脱机批准;
- n) 交易 6: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;
- o) 卡片上电 (ATR);
- p) 选择 PBOC 借记/贷记应用;
- q) GET PROCESSING OPTIONS 命令;
- r) VERIFY 命令;
- s) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证交易 2 PUT DATA 命令返回 SW1 SW2= '9000'。验证交易 6 第一次 GENERATE AC 的响应: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 6= '1'; CVR= '03 A4 20 00' 或 '03 A0 20 00' (用于未校验 PIN)。

7.19.3 GXSJ003-00

测试目的: 发卡行认证成功联机批准交易时, 验证卡片拒绝 PUT DATA 命令修改 ADA。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 发卡行认证成功, 联机批准交易, PUT DATA 命令修改 ADA;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 请求 ARQC;
 - h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 - i) 第二次 GENERATE AC 请求 TC;
 - j) PUT DATA 命令修改 ADA, MAC 正确。

通过标准: 验证交易 2 返回的 SW1 SW2: PUT DATA 命令返回 SW1 SW2≠ '9000', 推荐返回 SW1 SW2= '6A80'。

7.19.4 GXSJ004-00

测试目的: 发卡行认证成功交易批准联机时, 验证卡片应拒绝 MAC 错误的 PUT DATA 命令修改 LCOL。

验证卡片不接受 LCOL 的新值。当前的 LCOL 值为 3, 交易后验证该值应无变化。

测试条件: 第 9 章中的卡片特征 1, 支持 PUT DATA 命令修改 LCOL (连续脱机机交易下限)。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 发卡行认证成功批准交易联机, PUT DATA 命令修改 LCOL 失败;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;

- g) 第一个 GENERATE AC 请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- i) 第二次 GENERATE AC 请求 TC;
- j) PUT DATA 命令修改 LCOL MAC 错误;
- k) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- l) 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 请求 ARQC;
- q) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- r) 第二次 GENERATE AC 请求 TC;
- s) 交易 4: 脱机批准;
- t) 交易 5: 脱机批准;
- u) 交易 6: 脱机批准;
- v) 交易 7: 第一次 GENERATE AC 终端请求 TC 后, 卡片请求执行联机;
- w) 卡片上电 (ATR);
- x) 选择 PBOC 借记/贷记应用;
- y) GET PROCESSING OPTIONS 命令;
- z) VERIFY 命令;
- aa) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证交易 2 PUT DATA 命令返回的 SW1 SW2≠‘9000’, 推荐返回 SW1 SW2=‘6988’。
验证交易 6 第一次 GENERATE AC 卡片的响应: SW1 SW2=‘9000’; CID 位 8-7=‘01’;
CVR 字节 2 高半字节=‘9’; CVR 字节 3 位 6=‘0’。验证交易 7 第一次 GENERATE AC
卡片的响应: SW1 SW2=‘9000’; CID 位 8-7=‘10’; CVR 字节 2 高半字节=‘A’;
CVR 字节 3 位 6=‘1’; CVR=‘03 A4 20 00’或‘03 A0 20 00’ (用于未校验 PIN)。

7.19.5 GXSJ005-00

测试目的: 发卡行认证成功批准交易联机时, 验证卡片应拒绝无 MAC 的 PUT DATA 命令修改 LCOL。

验证卡片不接受 LCOL 的新值。当前的 LCOL 值为 3, 交易后验证该值应无变化。

测试条件: 第 9 章中的卡片特征 1, 支持 PUT DATA 命令修改 LCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 发卡行认证成功批准交易联机, PUT DATA 命令修改 LCOL 失败;
c) 卡片上电 (ATR);
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) VERIFY 命令;
g) 第一个 GENERATE AC 请求 ARQC。
h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
i) 第二次 GENERATE AC 请求 TC;
j) PUT DATA 命令修改 LCOL, MAC 缺失;
k) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
l) 交易 4: 脱机批准;

- m) 交易 5: 脱机批准;
- n) 交易 6: 脱机批准;
- o) 交易 7: 第一次 GENERATE AC 终端请求 TC 后, 卡片请求执行联机;
- p) 卡片上电 (ATR);
- q) 选择 PBOC 借记/贷记应用;
- r) GET PROCESSING OPTIONS 命令;
- s) VERIFY 命令;
- t) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证交易 2 PUT DATA 命令返回的 SW1 SW2≠‘9000’, 推荐返回 SW1 SW2=‘6987’或‘6988’。验证交易 6 第一次 GENERATE AC 的响应返回: SW1 SW2=‘9000’; CID 位 8-7=‘01’; CVR 字节 2 高半字节=‘9’; CVR 字节 3 位 6=‘0’。验证交易 7 第一次 GENERATE AC 的响应返回: SW1 SW2=‘9000’; CID 位 8-7=‘10’; CVR 字节 2 高半字节=‘A’; CVR 字节 3 位 6=‘1’; CVR=‘03 A4 20 00’或‘03 A0 20 00’ (用于未校验 PIN)。

7.19.6 GXSJ006-00

测试目的: 发卡行认证不成功批准交易联机时, 验证卡片拒绝 MAC 正确的 PUT DATA 命令修改 LCOL。验证卡片不接受 LCOL 的新值。当前的 LCOL 值为 3, 交易后验证该值应无变化。

测试条件: 第 9 章中的卡片特征 1, 支持 PUT DATA 命令修改 LCOL, 执行任何一个发卡行脚本之前, 请求的 EXTERNAL AUTHENTICATE 命令失败。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 发卡行认证失败批准交易联机, PUT DATA 命令修改 LCOL;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- i) 第二次 GENERATE AC 请求 TC;
- j) PUT DATA 命令修改 LCOL, MAC 正确;
- k) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- l) 交易 4: 脱机批准;
- m) 交易 5: 脱机批准;
- n) 交易 6: 脱机批准;
- o) 交易 7: 第一次 GENERATE AC 命令, 终端请求 TC 后, 卡片请求执行联机;
- p) 卡片上电 (ATR);
- q) 选择 PBOC 借记/贷记应用;
- r) GET PROCESSING OPTIONS 命令;
- s) VERIFY 命令。
- t) 第一个 GENERATE AC 请求 TC, 卡片响应 ARQC。

通过标准: 验证交易 2 PUT DATA 命令返回的 SW1 SW2≠‘9000’, 推荐返回‘6985’。验证交易 6 第一次 GENERATE AC 的响应返回: SW1 SW2=‘9000’; CID 位 8-7=‘01’; CVR 字节 2 高半字节=‘9’; CVR 字节 3 位 6=‘0’。验证交易 7 第一次 GENERATE AC 的

响应返回: SW1 SW2= '9000' ; CID 位 8-7= '10' ; CVR 字节 2 高半字节= 'A' ; CVR 字节 3 位 6= '1' 。

7.19.7 GX SJ007-00

测试目的: 未执行发卡行认证或执行发卡行认证成功交易批准联机时, 验证卡片接受 MAC 正确的 PUT DATA 命令修改 LCOL。当前的 LCOL 值为 3, 交易后验证该值应为 2。

测试条件: 第 9 章中的卡片特征 1, 支持 PUT DATA 命令修改 LCOL, 执行任何一个发卡行脚本之前 EXTERNAL AUTHENTICATE 命令无需成功。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 未执行发卡行认证批准联机交易, PUT DATA 命令修改 LCOL;

c) 卡片上电 (ATR) ;

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 请求 ARQC;

h) 第二次 GENERATE AC 请求 TC;

i) PUT DATA 命令修改 LCOL, MAC 正确;

j) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

k) 交易 4: 脱机批准;

l) 交易 5: 脱机批准;

m) 交易 6: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;

n) 卡片上电 (ATR) ;

o) 选择 PBOC 借记/贷记应用;

p) GET PROCESSING OPTIONS 命令;

q) VERIFY 命令;

r) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;

s) 交易 7: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

t) 交易 8: 脱机批准;

u) 交易 9: 脱机批准;

v) 交易 10: 脱机批准;

w) 交易 11: 第一次 GENERATE AC 命令, 终端请求 TC 后, 卡片请求执行联机;

x) 卡片上电 (ATR) ;

y) 选择 PBOC 借记/贷记应用;

z) GET PROCESSING OPTIONS 命令;

aa) VERIFY 命令;

ab) 第一个 GENERATE AC 请求 TC, 卡片响应 ARQC。

通过标准: 交易 2 PUT DATA 命令返回的 SW1 SW2= '9000' 。交易 6 第一次 GENERATE AC 响应: SW1 SW2= '9000' ; CID= '80' ; CVR= '03 A4 20 00' 或 '03 A0 20 00' (用于未校验 PIN) 。

7.19.8 GX SJ008-00

测试目的: 发卡行认证成功批准交易联机时, 验证卡片接受在第二次 GENERATE AC 命令前执行的 MAC 正确的 PUT DATA 命令修改 LCOL。验证卡片接受 LCOL 的新值。当前的 LCOL 值为

3, 交易后验证该值应为 2。

测试条件: 第 9 章中的卡片特征 1, 支持 PUT DATA 命令修改 LCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 发卡行认证成功批准联机交易, PUT DATA 命令修改 LCOL;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 请求 ARQC;

h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;

i) PUT DATA 命令修改 LCOL, MAC 正确;

j) 第二次 GENERATE AC 请求 TC;

k) 交易 3: 脱机批准;

l) 交易 4: 脱机批准;

m) 交易 5: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;

n) 卡片上电 (ATR);

o) 选择 PBOC 借记/贷记应用;

p) GET PROCESSING OPTIONS 命令;

q) VERIFY 命令;

r) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证交易 2 PUT DATA 命令返回的 SW1 SW2= '9000'。验证交易 5 第一次 GENERATE AC 命令卡片的响应: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 6= '1'; CVR= '03 A4 20 00' 或 '03 A0 20 00' (用于未校验 PIN)。

7.19.9 GX SJ009-00

测试目的: 发卡行认证成功批准交易联机时, 验证卡片接受两个 MAC 正确的 PUT DATA 命令修改的 LCOL。验证卡片接受第二个 LCOL 的新值。当前 LCOL 值为 3, 交易后第一个 LCOL 新值为 2, 第二个新值为 1。

测试条件: 第 9 章中的卡片特征 1, 支持 PUT DATA 命令修改 LCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 发卡行认证成功批准交易联机, 两个成功的 PUT DATA 命令修改 LCOL;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 请求 ARQC;

h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;

i) 第二次 GENERATE AC 请求 TC;

j) PUT DATA 命令修改 LCOL, MAC 正确;

k) PUT DATA 命令修改 LCOL, MAC 正确;

l) 交易 3: 脱机批准;

m) 交易 4: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;

n) 卡片上电 (ATR);

- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: 验证交易 2 两个 PUT DATA 命令响应的 SW1 SW2= '9000'。验证交易 4 第一次 GENERATE AC 命令卡片的响应: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 6= '1'; CVR= '03 A4 20 20' 或 '03 A0 20 20' (用于未校验 PIN)。

7.19.10 GXSJ010-00

测试目的: 联机批准交易, 发送两个 PUT DATA 命令的发卡行脚本, 第一个脚本 MAC 正确卡片应接受, 第二个脚本 MAC 错误卡片应拒绝。验证卡片接受第一个发卡行脚本, 拒绝第二个发卡行脚本。

测试条件: 第 9 章中的卡片特征 1, 支持 PUT DATA 命令修改 LCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 发卡行认证成功, 两个发卡行脚本命令, 批准联机交易;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- i) 第二次 GENERATE AC 请求 TC;
- j) PUT DATA 命令修改 LCOL, MAC 正确, LCOL 的新值为 02;
- k) PUT DATA 命令修改 LCOL, MAC 错误, LCOL 的新值为 01;
- l) 交易 3: 脱机批准;
- m) 交易 4: 脱机批准;
- n) 交易 5: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;
- o) 卡片上电 (ATR);
- p) 选择 PBOC 借记/贷记应用;
- q) GET PROCESSING OPTIONS 命令;
- r) VERIFY 命令;
- s) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- t) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- u) 第二次 GENERATE AC 请求 TC;
- v) PUT DATA 命令修改 LCOL, MAC 错误, LCOL 新值为 03。

通过标准: 交易 2 第二次 GENERATE AC 返回的 CVR= '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN)。交易 2 第一次 PUT DATA 命令 SW1 SW2= '9000'。交易 2 第二次 GENERATE AC 命令 SW1 SW2≠ '9000', 推荐返回 SW1 SW2= '6988'。交易 3 第一次 GENERATE AC 响应: SW1 SW2= '9000'; CID= '40'; CVR= '03 94 00 28'。交易 4 第一次 GENERATE AC 响应: SW1 SW2= '9000'; CID= '40'; CVR= '03 94 00 28' 或 '03 90 00 28' (用于未校验 PIN)。交易 5 第二次 GENERATE AC 响应: SW1 SW2= '9000'; CID= '40'; CVR= '03 64 20 28' 或 '03 60 20 28' (用于未校验 PIN)。

7.19.11 GXSJ011-00

测试目的：发卡行认证成功联机批准交易时，验证卡片接受 MAC 正确的 PUT DATA 命令修改 LCOL，和 MAC 正确的 APPLICATION UNBLOCK 命令。验证卡片接受 LCOL 的新值。修改前 LCOL 值为 3，修改后第 LCOL 新值为 2。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL 和 APPLICATION UNBLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：发卡行认证成功批准联机交易，执行成功的 PUT DATA 命令修改 LCOL 和 APPLICATION UNBLOCK 命令；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

i) 第二次 GENERATE AC 请求 TC；

j) APPLICATION UNBLOCK，MAC 正确；

k) PUT DATA 命令修改 LCOL，MAC 正确；

l) 交易 3：脱机批准；

m) 交易 4：脱机批准；

n) 交易 5：第一次 GENERATE AC 命令终端请求 TC 后，卡片请求执行联机；

o) 卡片上电 (ATR)；

p) 选择 PBOC 借记/贷记应用；

q) GET PROCESSING OPTIONS 命令；

r) VERIFY 命令；

s) 第一个 GENERATE AC 请求 TC，卡响应 ARQC。

通过标准：验证交易 2 APPLICATION UNBLOCK 命令返回的 SW1 SW2=‘9000’。验证交易 2 PUT DATA 命令响应的 SW1 SW2=‘9000’。验证交易 5 第一次 GENERATE AC 的响应返回：SW1 SW2=‘9000’；CID 位 8-7=‘10’；CVR 字节 2 高半字节=‘A’；CVR 字节 3 位 6=‘1’；CVR=‘03 A4 20 20’或‘03 A0 20 20’（用于未校验 PIN）。

7.20 EXTERNAL AUTHENTICATE 命令 (WBRZ)

7.20.1 准备步骤

7.20 条的准备步骤如下。

a) 卡片上电 (ATR)；

b) 选择 PBOC 借记/贷记应用；

c) GET PROCESSING OPTIONS 命令；

d) VERIFY 命令；

e) 第一次 GENERATE AC 请求 ARQC。

7.20.2 WBRZ001-00

测试目的：执行数据域长度小于 0A 的 EXTERNAL AUTHENTICATE 命令应不成功。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：准备步骤完成后，执行长度小于 Lc 的 EXTERNAL AUTHENTICATE 命令：‘00 82 00 00 08’，ARPC 为 8 字节的密文。

通过标准：卡响应 EXTERNAL AUTHENTICATE 命令 SW1 SW2≠‘9000’，建议‘6700’或‘6A80’。

7.20.3 WBRZ002-00

测试目的：执行数据域长度大于 0A 的 EXTERNAL AUTHENTICATE 命令应不成功。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：准备步骤执行完成后，执行长度大于 Lc 的 EXTERNAL AUTHENTICATE 命令：‘00 82 00 00 0C’，ARPC 为 8 字节的密文。

通过标准：卡片响应 EXTERNAL AUTHENTICATE 命令 SW1 SW2≠‘9000’，建议‘6700’或‘6A80’。

7.21 上次联机交易发卡行认证失败(RZSB)

7.21.1 RZSB001-00

测试目的：脱机批准的交易，卡不支持发卡行认证时，验证卡片重置“发卡行认证失败指示器”位。

测试条件：第 9 章中的卡片特征 2。

测试流程：a) 交易 1：不执行发卡行认证联机批准交易，复位卡片中的计数器；

b) 交易 2：不支持发卡行认证，批准交易联机；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC；

h) 第二次 GENERATE AC 请求 TC；

i) 交易 3：脱机批准。

通过标准：SW1 SW2=‘9000’；CID 位 8-7=‘01’；CVR 字节 2 高半字节=‘9’；CVR 字节 3 位 4=‘0’；CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.21.2 RZSB002-00

测试目的：拒绝的交易，卡片不支持发卡行认证，验证卡片重置“发卡行认证失败指示器”位。

测试条件：第 9 章中的卡片特征 2。

测试流程：a) 交易 1：不执行发卡行认证联机批准交易，以复位卡片中的计数器；

b) 交易 2：不支持发卡行认证，未执行发卡行认证，拒绝交易联机；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC；

h) 第二次 GENERATE AC 请求 AAC；

i) 交易 3：脱机批准。

通过标准：SW1 SW2=‘9000’；CID 位 8-7=‘01’；CVR 字节 2 高半字节=‘9’；CVR 字节 3 位 4=‘0’；CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.21.3 RZSB003-00

测试目的：批准的联机交易发卡行认证执行时，验证卡片重置“发卡行认证失败指示器”位。

测试条件：第9章中的卡片特征1，支持发卡行认证。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：批准交易联机，发卡行认证成功；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一次 GENERATE AC 请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

i) 第二次 GENERATE AC 请求 TC；

j) 交易3：脱机批准。

通过标准：SW1 SW2= ‘9000’；CID 位 8-7= ‘01’；CVR 字节 2 高半字节= ‘9’；CVR 字节 3 位 4= ‘0’；CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。

7.21.4 RZSB004-00

测试目的：拒绝联机交易当发卡行认证执行时，验证卡片重置“发卡行认证失败指示器”位。

测试条件：第9章中的卡片特征1，支持发卡行认证。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：发卡行认证成功，拒绝联机交易；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

i) 第二次 GENERATE AC 请求 AAC；

j) 交易3：脱机批准。

通过标准：SW1 SW2= ‘9000’；CID 位 8-7= ‘01’；CVR 字节 2 高半字节= ‘9’；CVR 字节 3 位 4= ‘0’；CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。

7.21.5 RZSB005-00

测试目的：批准的联机交易执行发卡行认证失败时，验证卡片设置“发卡行认证失败指示器”位。

当未设置 ADA 中的“如何发卡行认证失败，下次联机交易”位，前次交易发卡行认证失败，设置“联机授权指示”位时，验证卡片强制下次交易联机。

测试条件：第9章中的卡片特征4，支持发卡行认证。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：批准联机交易，发卡行认证失败；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

- g) 第一个 GENERATE AC 请求 ARQC;
- h) hEXTERNAL AUTHENTICATE 命令, ARPC 错误;
- i) 第二次 GENERATE AC 请求 TC;
- j) 交易 3: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 4= '1'; CVR= '03 A4 88 00' 或 '03 A0 88 00' (用于未校验 PIN)。

7.21.6 RZSB006-00

测试目的: 批准联机交易, 当发卡行认证执行失败时, 验证卡片设置“发卡行认证失败指示器”位。当设置 ADA 中的“如何发卡行认证失败, 下次联机交易”位, 验证卡片强制下次交易联机。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 发卡行认证失败, 批准交易联机;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, ARPC 错误;
- i) 第二次 GENERATE AC 请求 TC;
- j) 交易 3: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 4= '1'; CVR= '03 A4 88 00' 或 '03 A0 88 00' (用于未校验 PIN)。

7.21.7 RZSB007-00

测试目的: 联机拒绝交易当执行发卡行认证失败时, 验证卡片设置“发卡行认证失败指示器”位。当未设置 ADA 中的“如何发卡行认证失败, 下次联机交易”位, 前次交易发卡行认证失败设置“联机授权指示”位时, 验证卡片强制下次交易联机。

测试条件: 第 9 章中的卡片特征 4, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 拒绝交易联机, 发卡行认证不成功;
- c) 卡片上电 (ATR);

- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, ARPC 错误;
- i) 第二次 GENERATE AC 请求 AAC;
- j) 交易 3: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 4= '1'; CVR= '03 A4 88 00' 或 '03 A0 88 00' (用于未校验 PIN)。

7.21.8 RZSB008-00

测试目的: 拒绝联机交易, 当发卡行认证执行失败时, 验证卡片设置“发卡行认证失败指示器”位。当设置 ADA 中的“如果发卡行认证失败, 下次联机交易”位, 验证卡片强制下次交易联机。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 拒绝联机交易, 发卡行认证失败;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, ARPC 错误;
- i) 第二次 GENERATE AC 请求 AAC;
- j) 交易 3: 第一次 GENERATE AC 命令终端请求 TC 后, 卡片请求执行联机;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 4= '1'; CVR= '03 A4 88 00' 或 '03 A0 88 00' (用于未校验 PIN)。

7.21.9 RZSB009-00

测试目的: 批准交易, 当不支持发卡行认证时, 验证卡片重置“发卡行认证失败指示器”位。

下次交易脱机拒绝, 验证卡片不设置 CVR 的“上次联机交易发卡行认证失败”位。

测试条件: 第 9 章中的卡片特征 2, 不支持发卡行认证。

测试流程: a) 交易 1: 不执行发卡行认证联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 不支持发卡行认证, 批准交易联机;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) 第二次 GENERATE AC 请求 TC;
- i) 交易 3: 脱机拒绝。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '00'; CVR 字节 2 高半字节= '8'; CVR 字节 3 位 4= '0'; CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.21.10 RZSB010-00

测试目的: 联机批准交易, 当发卡行认证执行时, 验证卡片重置“发卡行认证失败指示器”位。下次交易拒绝脱机, 验证卡片不设置 CVR 的“上次联机交易发卡行认证失败”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 发卡行认证成功, 批准交易联机;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 请求 ARQC;
 - h) EXTERNAL AUTHENTICATE 命令, ARPC 正确;
 - i) 第二次 GENERATE AC 请求 TC;
 - j) 交易 3: 脱机拒绝。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '00'; CVR 字节 2 高半字节= '8'; CVR 字节 3 位 4= '0'; CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.21.11 RZSB011-00

测试目的: 批准联机交易, 执行发卡行认证失败时, 验证卡片设置“发卡行认证失败指示器”位。无论如何设置 ADA 中的“如果发卡行认证失败, 下次联机交易”位, 下次交易均被脱机拒绝, 验证卡片设置 CVR 的“上次联机交易发卡行认证失败”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 发卡行认证失败, 批准交易联机;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 请求 ARQC;
 - h) EXTERNAL AUTHENTICATE 命令, ARPC 错误;
 - i) 第二次 GENERATE AC 请求 TC;
 - j) 交易 3: 脱机拒绝。

通过标准：SW1 SW2= ‘9000’；CID 位 8-7= ‘00’；CVR 字节 2 高半字节= ‘8’；CVR 字节 3 位 4= ‘1’；CVR= ‘03 84 88 00’ 或 ‘03 80 88 00’（用于未校验 PIN）。

7.21.12 RZSB012-00

测试目的：批准交易，发卡行认证应执行但未执行时，验证卡片设置“发卡行认证失败指示器”位。设置 ADA 中的“如果发卡行认证失败，下次联机交易”位，验证卡片强制下次交易联机并设置 CVR 的“上次联机交易发卡行认证失败”位。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：未执行发卡行认证（支持且应执行），批准交易联机；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC；

h) 第二次 GENERATE AC 请求 TC；

i) 交易 3：第一次 GENERATE AC 终端请求 TC 后，卡片请求执行联机；

j) 卡片上电（ATR）；

k) 选择 PBOC 借记/贷记应用；

l) GET PROCESSING OPTIONS 命令；

m) VERIFY 命令；

n) 第一个 GENERATE AC 请求 TC，卡响应 ARQC。

通过标准：SW1 SW2= ‘9000’；CID 位 8-7= ‘10’；CVR 字节 2 高半字节= ‘A’；CVR 字节 3 位 4= ‘1’；CVR= ‘03 A4 88 00’ 或 ‘03 A0 88 00’（用于未校验 PIN）。

7.21.13 RZSB013-00

测试目的：批准交易，发卡行认证必需执行但未执行时，验证卡片设置“发卡行认证失败指示器”位。上次交易发卡行认证失败设置“联机授权指示”位，未设置 ADA 中的“如果发卡行认证失败，下次联机交易”位，验证卡片强制下次交易联机。

验证卡片设置 CVR 的“上次联机交易发卡行认证失败”位。

测试条件：第 9 章中的卡片特征 4，强制支持发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：未执行发卡行认证（支持且应执行），批准交易联机；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC；

h) 第二次 GENERATE AC 请求 TC；

i) 交易 3：第一次 GENERATE AC 终端请求 TC 后，卡片请求执行联机；

j) 卡片上电（ATR）；

k) 选择 PBOC 借记/贷记应用；

l) GET PROCESSING OPTIONS 命令；

m) VERIFY 命令;

n) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 4= '1'; CVR= '03 A4 88 00' 或 '03 A0 88 00' (用于未校验 PIN)。

7.21.14 RZSB014-00

测试目的: 拒绝交易, 发卡行认证应执行但未执行时, 验证卡片设置“发卡行认证失败指示器”位。设置 ADA 中的“如果发卡行认证失败, 下次联机交易”位, 验证卡片强制下次交易联机并设置 CVR 的“上次联机交易发卡行认证失败”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 未执行发卡行认证, 拒绝联机;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 请求 ARQC;

h) 第二次 GENERATE AC 请求 AAC;

i) 交易 3: 第一次 GENERATE AC 终端请求 TC 后, 卡片请求执行联机;

j) 卡片上电 (ATR);

k) 选择 PBOC 借记/贷记应用;

l) GET PROCESSING OPTIONS 命令;

m) VERIFY 命令;

n) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 4= '1'; CVR= '03 A4 88 00' 或 '03 A0 88 00' (用于未校验 PIN)。

7.21.15 RZSB015-00

测试目的: 拒绝交易, 发卡行认证应执行但未执行时, 验证卡片设置“发卡行认证失败指示器”位。上次交易发卡行认证失败设置“联机授权指示”位, 未设置 ADA 中的“如果发卡行认证失败, 下次联机交易”位, 验证卡片强制下次交易联机。验证卡片设置 CVR 的“上次联机交易发卡行认证失败”位。

测试条件: 第 9 章中的卡片特征 4, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 未执行发卡行认证 (支持且应执行), 拒绝联机交易;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 请求 ARQC;

h) 第二次 GENERATE AC 请求 AAC;

i) 交易 3: 第一次 GENERATE AC 终端请求 TC 后, 卡片请求执行联机;

j) 卡片上电 (ATR);

- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '10'; CVR 字节 2 高半字节= 'A'; CVR 字节 3 位 4= '1'; CVR= '03 A4 88 00' 或 '03 A0 88 00' (用于未校验 PIN)。

7.21.16 RZSB016-00

测试目的: 当交易不能执行联机发卡行认证未执行且交易拒绝时, 验证卡片不设置“发卡行认证失败指示器”位。

测试条件: 第 9 章中的卡片特征 3, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 不能执行联机时, 交易拒绝;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) 第二次 GENERATE AC 请求 AAC, ARC=Z3;
- i) 交易 3: 请求批准脱机;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 请求 TC, 卡响应 ARQC;
- o) EXTERNAL AUTHENTICATE 命令, ARPC 正确;
- p) 第二次 GENERATE AC 请求 TC。

通过标准: 交易 2 第二次 GENERATE AC 响应: SW1 SW2= '9000'; CID= '00'; CVR= '03 25 00 00' 或 '03 21 00 00' (用于未校验 PIN)。交易 3 第二次 GENERATE AC 响应: SW1 SW2= '9000'; CID= '40'; CVR= '03 64 80 00' 或 '03 60 80 00' (用于未校验 PIN)。

7.21.17 RZSB017-00

测试目的: 批准的联机交易, 发卡行认证应执行但未执行时, 验证卡片设置“发卡行认证失败指示器”位。无论如何设置 ADA 中的“如果发卡行认证失败, 下次联机交易”位, 下次交易均被脱机拒绝, 验证卡片设置 CVR 的“上次联机交易发卡行认证失败”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 未执行发卡行认证 (支持且应执行), 批准联机交易;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;

- g) 第一个 GENERATE AC 请求 ARQC;
- h) 第二次 GENERATE AC 请求 TC;
- i) 交易 3: 脱机拒绝。

通过标准: SW1 SW2= '9000' ; CID 位 8-7= '00' ; CVR 字节 2 高半字节= '8' ; CVR 字节 3 位 4= '1' ; CVR= '03 84 88 00' 或 '03 80 88 00' (用于未校验 PIN)。

7.21.18 RZSB018-00

测试目的: 联机批准交易, 发卡行认证 (可选) 未执行时, 验证卡片重置 “发卡行认证失败指示器” 位。无论如何设置 ADA 中的 “如果发卡行认证失败, 下次联机交易” 位, 下次交易均被脱机拒绝, 验证卡片不设置 CVR 的 “上次联机交易发卡行认证失败” 位。

测试条件: 第 9 章中的卡片特征 3, 支持发卡行认证 (可选)。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 未执行发卡行认证 (支持, 可选), 批准联机;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) 第二次 GENERATE AC 请求 TC;
- i) 交易 3: 脱机拒绝。

通过标准: SW1 SW2= '9000' ; CID 位 8-7= '00' ; CVR 字节 2 高半字节= '8' ; CVR 字节 3 位 4= '0' ; CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.22 联机交易失败 (LJSB)

7.22.1 LJSB001-00

测试目的: 当交易不能执行联机并且被脱机拒绝 ARC=Z3, 不设置 ADA 中的 “如果交易拒绝, 生成通知” 位时, 验证卡片不设置 CID 中的 “需要通知” 位。验证卡片设置 CVR 中的 “不能联机” 位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 终端请求联机但是不能联机且拒绝脱机;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) 第二个 GENERATE AC 命令请求 AAC, ARC =Z3。

通过标准: SW1 SW2= '9000' ; CID 位 8-7= '00' ; CID 位 4= '0' ; CVR 字节 2 高半字节= '2' ; CVR 字节 2 位 1= '1' ; CID= '00' ; CVR= '03 25 00 00' 或 '03 21 00 00' (用于未校验 PIN)。

7.22.2 LJSB002-00

测试目的: 当交易不能执行联机并且被脱机拒绝 ARC=Z3, 设置 ADA 中的 “如果交易拒绝, 生成

通知”位时，验证卡片设置 CID 中的“需要通知”位。

验证卡片设置 CVR 中的“不能联机”位。

测试条件：第 9 章中的卡片特征 14，对于脱机拒绝交易，支持 ADA 需要生成脱机通知。所有交易的终端国家代码≠‘0156’，支持连续国际交易（基于国家）频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：终端请求联机但是不能联机且拒绝脱机；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) 第二个 GENERATE AC 命令请求 AAC，ARC=Z3。

通过标准：第一个 GENERATE AC：CID=‘80’；CVR=‘03 A4 20 00’或‘03 A0 20 00’（用于未校验 PIN）。第二个 GENERATE AC：CID=‘08’；第二个 GENERATE AC，CVR=‘03 25 20 00’或‘03 21 20 00’（用于未校验 PIN）。

7.22.3 LJSB003-00

测试目的：当交易不能执行联机并且被脱机批准 ARC=Y3，验证卡片设置 CVR 的“不能联机”位。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：终端不能执行联机，脱机批准；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) 第二个 GENERATE AC 命令请求 TC，ARC=Y3。

通过标准：SW1 SW2=‘9000’；CID 位 8-7=‘01’；CID 位 4=‘0’；CVR 字节 2 高半字节=‘6’；CVR 字节 2 位 1=‘1’；CVR=‘03 65 00 00’或‘03 61 00 00’（用于未校验 PIN）。

7.22.4 LJSB004-00

测试目的：交易不能联机且拒绝脱机交易，ARC=Z3，验证卡片不设置 CVR 中的“超过频率检查”位，ATC 与 LOATC 之差小于 UCOL。

测试条件：第 9 章中的卡片特征 7，支持连续脱机交易（上限）频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：终端请求联机但是不能联机且拒绝脱机；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) 第二个 GENERATE AC 命令请求 AAC，ARC=Z3。

通过标准：SW1 SW2=‘9000’；CID 位 8-7=‘00’；CVR 字节 2 高半字节=‘2’；CVR 字节 2 位

1= ‘1’ ; CVR 字节 3 位 6= ‘0’ ; CVR= ‘03 25 00 00’ 或 ‘03 21 00 00’ （用于未校验 PIN）。

7.22.5 LJSB005-00

测试目的：交易不能执行联机，允许脱机交易，ARC=Y3，卡片不设置 CVR 中的“超过频率检查”位，ATC 与 LOATC 之差小于 UC0L。

测试条件：第 9 章中的卡片特征 7，支持连续脱机交易频度检查（上限）。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：终端需要执行联机交易但不能联机，允许脱机交易；

c) 卡片上电（ATR）；

d) 选择应用；

e) 执行 GET PROCESSING OPTIONS 命令；

f) 执行 VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC；

h) 第二个 GENERATE AC 请求 TC，ARC=Y3。

通过标准：SW1 SW2= ‘9000’ ; CID 位 8-7= ‘01’ ; CVR 字节 2 高半字节= ‘6’ ; CVR 字节 2 位 1= ‘1’ ; CVR 字节 3 位 6= ‘0’ ; CVR= ‘03 65 00 00’ 或 ‘03 61 00 00’ （用于未校验 PIN）。

7.22.6 LJSB006-00

测试目的：交易不能执行联机且拒绝脱机交易，ARC=Z3，卡片不设置 CVR 中的“超过频率检查”位，ATC 与 LOATC 之差等于 UC0L。

测试条件：第 9 章中的卡片特征 7，支持连续脱机交易频度检查（上限）。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：终端请求联机但是不能联机且拒绝脱机；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) 第二个 GENERATE AC 命令请求 AAC，ARC=Z3；

i) 交易 3：终端请求联机但是不能联机且拒绝脱机；

j) 卡片上电（ATR）；

k) 选择 PBOC 借记/贷记应用；

l) GET PROCESSING OPTIONS 命令；

m) VERIFY 命令；

n) 第一个 GENERATE AC 命令请求 ARQC；

o) 第二个 GENERATE AC 命令请求 AAC，ARC=Z3；

p) 交易 4：终端请求联机但是不能联机且拒绝脱机；

q) 卡片上电（ATR）。

r) 选择 PBOC 借记/贷记应用；

s) GET PROCESSING OPTIONS 命令；

t) VERIFY 命令；

- u) 第一个 GENERATE AC 命令请求 ARQC;
- v) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- w) 交易 5: 终端请求联机但是不能联机且拒绝脱机;
- x) 卡片上电 (ATR);
- y) 选择 PBOC 借记/贷记应用;
- z) GET PROCESSING OPTIONS 命令;
- aa) VERIFY 命令;
- ab) 第一个 GENERATE AC 命令请求 ARQC;
- ac) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- ad) 交易 6: 终端请求联机但是不能联机且拒绝脱机;
- ae) 卡片上电 (ATR);
- af) 选择 PBOC 借记/贷记应用;
- ag) GET PROCESSING OPTIONS 命令;
- ah) VERIFY 命令;
- ai) 第一个 GENERATE AC 命令请求 ARQC;
- aj) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- ak) 交易 7: 终端请求联机但是不能联机且拒绝脱机;
- al) 卡片上电 (ATR);
- am) 选择 PBOC 借记/贷记应用;
- an) GET PROCESSING OPTIONS 命令;
- ao) VERIFY 命令;
- aq) 第一个 GENERATE AC 命令请求 ARQC;
- aq) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- ar) 交易 8: 终端请求联机但是不能联机且拒绝脱机;
- as) 卡片上电 (ATR);
- at) 选择 PBOC 借记/贷记应用;
- au) GET PROCESSING OPTIONS 命令;
- av) VERIFY 命令;
- aw) 第一个 GENERATE AC 命令请求 ARQC;
- ax) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '00'; CVR 字节 2 高半字节= '2'; CVR 字节 2 位 1= '1'; CVR 字节 3 位 6= '0'; CVR= '03 25 80 00' 或 '03 21 80 00' (用于未校验 PIN)。

7.22.7 LJSB007-00

测试目的: 交易不能联机且拒绝脱机交易, ARC=Z3, 卡片设置 CVR 中的“超过频率检查”位, ATC 与 LOATC 之差大于 UCOL。

测试条件: 第 9 章中的卡片特征 7, 支持连续脱机交易频率检查 (上限)。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 终端请求联机但是不能联机且拒绝脱机;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- i) 交易 3: 终端请求联机但是不能联机且拒绝脱机;
- j) 卡片上电(ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 命令请求 ARQC;
- o) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- p) 交易 4: 终端请求联机但是不能联机且拒绝脱机;
- q) 卡片上电(ATR);
- r) 选择 PBOC 借记/贷记应用;
- s) GET PROCESSING OPTIONS 命令;
- t) VERIFY 命令;
- u) 第一个 GENERATE AC 命令请求 ARQC;
- v) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- w) 交易 5: 终端请求联机但是不能联机且拒绝脱机;
- x) 卡片上电(ATR);
- y) 选择 PBOC 借记/贷记应用;
- z) GET PROCESSING OPTIONS 命令;
- aa) VERIFY 命令;
- ab) 第一个 GENERATE AC 命令请求 ARQC;
- ac) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- ad) 交易 6: 终端请求联机但是不能联机且拒绝脱机;
- ae) 卡片上电(ATR);
- af) 选择 PBOC 借记/贷记应用;
- ag) GET PROCESSING OPTIONS 命令;
- ah) VERIFY 命令;
- ai) 第一个 GENERATE AC 命令请求 ARQC;
- aj) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- ak) 交易 7: 终端请求联机但是不能联机且拒绝脱机;
- al) 卡片上电(ATR);
- am) 选择 PBOC 借记/贷记应用;
- an) GET PROCESSING OPTIONS 命令;
- ao) VERIFY 命令;
- ap) 第一个 GENERATE AC 命令请求 ARQC;
- aq) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- ar) 交易 8: 终端请求联机但是不能联机且拒绝脱机;
- as) 卡片上电(ATR);
- at) 选择 PBOC 借记/贷记应用;
- au) GET PROCESSING OPTIONS 命令;
- av) VERIFY 命令;

- aw) 第一个 GENERATE AC 命令请求 ARQC;
- ax) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- ay) 交易 9: 终端请求联机但是不能联机且拒绝脱机;
- az) 卡片上电 (ATR);
- ba) 选择 PBOC 借记/贷记应用;
- bb) GET PROCESSING OPTIONS 命令;
- bc) VERIFY 命令;
- bd) 第一个 GENERATE AC 命令请求 ARQC;
- be) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '00'; CVR 字节 2 高半字节= '2'; CVR 字节 2 位 1= '1'; CVR 字节 3 位 6= '1'; CVR= '03 25 A0 00' 或 '03 21 A0 00' (用于未校验 PIN)。

7.22.8 LJSB008-00

测试目的: 交易不能联机且拒绝脱机交易, ARC=Z3, 验证卡片设置 CVR 中的“超过频率检查”位, ATC 与 LOATC 之差大于 UCOL (UCOL=0)。

测试条件: 第 9 章中的卡片特征 15, 支持连续脱机交易频率检查 (上限)。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 终端请求联机但是不能联机且拒绝脱机;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3。

通过标准: SW1 SW2= '9000'。CID 位 8-7= '00'; CVR 字节 2 高半字节= '2'; CVR 字节 2 位 1= '1'; CVR 字节 3 位 6= '1'; CVR= '03 25 20 00' 或 '03 21 20 00' (用于未校验 PIN)。

7.22.9 LJSB009-00

测试目的: 交易不能联机, 允许脱机交易, ARC=Y3, 验证卡片设置 CVR 中的“超过频率检查”位, ATC 与 LOATC 的差值大于 UCOL, 此时卡片应拒绝脱机交易。

测试条件: 第 9 章中的卡片特征 15, 支持连续脱机交易频度检查 (上限)。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 终端请求联机但是不能联机终端请求脱机批准, 卡片强制交易拒绝脱机;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) 第二个 GENERATE AC 命令请求 TC, ARC=Y3, 卡片返回 AAC。

通过标准: SW1 SW2= '9000'; CID 位 8-7= '00'; CVR 字节 2 高半字节= '2'; CVR 字节 2 位 1= '1'; CVR 字节 3 位 6= '1'; CVR= '03 25 20 00' 或 '03 21 20 00' (用于未

校验 PIN)。

7.22.10 LJSB010-00

测试目的：新卡，第一笔交易批准联机（执行发卡行认证失败），第二笔交易不能联机且拒绝脱机且 ARC=Z3，验证卡片设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 1，新卡，支持发卡行认证。

测试流程：a) 交易 1：联机批准交易，但发卡行认证不成功；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；。
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 执行 EXTERNAL AUTHENTICATE 命令，ARPC 错误；
h) 第一个 GENERATE AC 命令请求 TC；
i) 交易 2：终端请求联机交易但不能执行联机，且拒绝脱机交易；
j) 卡片上电 (ATR)；
k) 选择 PBOC 借记/贷记应用；
l) GET PROCESSING OPTIONS 命令；
m) VERIFY 命令；
n) 第一个 GENERATE AC 命令请求 ARQC；
o) 第二个 GENERATE AC 命令请求 AAC，ARC=Z3。

通过标准：SW1 SW2=‘9000’；CID 位 8-7=‘00’；CVR 字节 2 高半字节=‘2’；CVR 字节 2 位 1=‘1’；CVR 字节 3 位 5=‘1’；CVR=‘03 25 98 00’或‘03 21 98 00’（用于未校验 PIN）。

7.22.11 LJSB011-00

测试目的：新卡，第一笔交易批准联机，执行发卡行认证不成功。第二笔交易不能执行联机但批准脱机，ARC=Y3，不设置 ADA 中的“如果是新卡，当交易无法联机时拒绝交易”位时，验证卡片批准交易脱机且设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 1，新卡，支持发卡行认证。

测试流程：a) 交易 1：联机批准交易，但发卡行认证不成功；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 执行 EXTERNAL AUTHENTICATE 命令，ARPC 错误；
h) 第一个 GENERATE AC 命令请求 TC；
i) 交易 2：终端请求联机交易但不能执行联机，且脱机批准交易；
j) 卡片上电 (ATR)；
k) 选择 PBOC 借记/贷记应用；
l) GET PROCESSING OPTIONS 命令；
m) ERIFY 命令；

- n) 第一个 GENERATE AC 命令请求 ARQC;
- o) 第二个 GENERATE AC 命令请求 TC, ARC=Y3。

通过标准: SW1 SW2= '9000' ; CID 位 8-7= '01' ; CVR 字节 2 高半字节= '6' ; CVR 字节 2 位 1= '1' ; CVR 字节 3 位 5= '1' ; CVR= '03 65 98 00' 或 '03 61 98 00' (用于未校验 PIN) 。

7.22.12 LJSB012-00

测试目的: 新卡, 第一笔交易批准联机, 执行发卡行认证不成功。第二笔交易不能执行联机, ARC=Y3, 设置 ADA 中的“如果是新卡, 当交易无法联机时拒绝交易”位时, 验证卡片拒绝交易脱机并且设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 16, 支持新卡检查和发卡行认证。

测试流程: a) 交易 1: 联机批准交易, 但发卡行认证不成功;

- b) 卡片上电(ATR) ;
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 错误;
- h) 第一个 GENERATE AC 命令请求 TC;
- i) 交易 2: 终端请求联机交易但不能执行联机, 且脱机批准交易;
- j) 卡片上电(ATR) ;
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 命令请求 ARQC;
- o) 第二个 GENERATE AC 命令请求 TC, ARC=Y3, 但卡片返回 AAC。

通过标准: SW1 SW2= '9000' , CID 位 8-7= '00' , CVR 字节 2 高半字节= '2' , CVR 字节 2 位 1= '1' , CVR 字节 3 位 5= '1' , CVR= '03 25 98 00' 或 '03 21 98 00' (用于未校验 PIN) 。

7.22.13 LJSB013-00

测试目的: 终端不执行 VERIFY 命令, 卡片参考 PIN 未锁定, 交易不能联机且拒绝脱机。验证卡片不设置“脱机 PIN 执行”位、“脱机 PIN 认证失败”位、“PIN 锁定”位, 设置 CVR 中的“不能联机”位, 卡片拒绝交易脱机处理。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 卡片上电(ATR) ;
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 错误;
- h) 第二个 GENERATE AC 命令请求 TC;

- i) 交易 2: 终端请求联机但是不能联机且拒绝脱机, 未执行 VERIFY 命令;
- j) 卡片上电(ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) 第一个 GENERATE AC 命令请求 ARQC;
- n) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '2', CVR 字节 2 位 3= '0', CVR 字节 2 位 2= '0', CVR 字节 2 位 1= '1', CVR 字节 3 位 7= '0', CVR= '03 21 00 00' 或 '03 21 00 00' (用于未校验 PIN)。

7.22.14 LJSB014-00

测试目的: 终端不执行 VERIFY 命令, 卡片参考 PIN 未锁定, 终端不能进行联机且希望批准脱机; 验证卡片不设置“脱机 PIN 执行”位、“脱机 PIN 认证失败”位、“PIN 锁定”位, 设置 CVR 中的“不能联机”位, 卡片批准交易脱机。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 卡片上电(ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 命令请求 ARQC;
 - g) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 正确;
 - h) 第二个 GENERATE AC 命令请求 TC;
 - i) 交易 2: 终端请求联机但是不能联机且脱机批准, 未执行 VERIFY 命令;
 - j) 卡片上电(ATR);
 - k) 选择 PBOC 借记/贷记应用;
 - l) GET PROCESSING OPTIONS 命令;
 - m) 第一个 GENERATE AC 命令请求 ARQC;
 - n) 第二个 GENERATE AC 命令请求 TC, ARC=Y3。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '6', CVR 字节 2 位 3= '0', CVR 字节 2 位 2= '0', CVR 字节 2 位 1= '1', CVR 字节 3 位 7= '0', CVR= '03 61 00 00' 或 '03 61 00 00' (用于未校验 PIN)。

7.22.15 LJSB015-00

测试目的: 终端未执行 VERIFY 命令, 卡片参考 PIN 锁定, 终端不能执行联机且拒绝脱机, 不设置 ADA 中的“如果 PIN 在前次交易中锁定, 当交易无法联机时拒绝交易”位; 验证卡片不设置 CVR 中的“脱机 PIN 执行”位、“脱机 PIN 认证失败”位, 但设置“不能联机”位和“PIN 锁定”位, 卡片拒绝交易脱机。

测试条件: 第 9 章中的卡片特征 17, 支持脱机 PIN。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 卡片上电(ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;

- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 正确;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) 交易 2: 锁定 PIN;
- j) 卡片上电(ATR) ;
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令, 错误的 PIN;
- n) VERIFY 命令, 错误的 PIN;
- o) VERIFY 命令, 错误的 PIN;
- p) 第一个 GENERATE AC 命令请求 ARQC;
- q) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- r) 第二个 GENERATE AC 命令请求 TC;
- s) 交易 3: 终端请求联机但是不能联机, 未执行 VERIFY 命令, 拒绝交易脱机;
- t) 卡片上电(ATR) ;
- u) 选择 PBOC 借记/贷记应用;
- v) GET PROCESSING OPTIONS 命令;
- w) 第一个 GENERATE AC 命令请求 ARQC;
- x) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '2',
CVR 字节 2 位 3= '0', CVR 字节 2 位 2= '0', CVR 字节 2 位 1= '1', CVR 字节 3
位 7= '1', CVR= '03 21 40 00' 或 '03 21 00 00' (用于未校验 PIN)。

7.22.16 LJSB016-00

测试目的: 终端未执行 VERIFY 命令, 参考 PIN 锁定。终端不能执行联机、批准脱机。

不设置 ADA 中的“如果 PIN 在前次交易中锁定, 当交易无法联机时拒绝交易”位, 验证卡片不设置“脱机 PIN 执行”位或“脱机 PIN 认证失败”位, 设置 CVR 中的“PIN 锁定”位和“不能联机”位, 卡片批准交易脱机。

测试条件: 第 9 章中的卡片特征 10, 支持连续脱机交易频度检查(上限)。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 卡片上电(ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) EXTERNAL AUTHENTICATE, 正确 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) 交易 2: 锁定 PIN;
- j) 卡片上电(ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令, 错误的 PIN;

- n) VERIFY 命令, 错误的 PIN;
- o) VERIFY 命令, 错误的 PIN;
- p) 第一个 GENERATE AC 命令请求 ARQC;
- q) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- r) 第二个 GENERATE AC 命令请求 TC;
- s) 交易 3: 终端请求联机但是不能联机, 未执行 VERIFY 命令批准交易脱机;
- t) 卡片上电 (ATR);
- u) 选择 PBOC 借记/贷记应用;
- v) GET PROCESSING OPTIONS 命令;
- w) 第一个 GENERATE AC 命令请求 ARQC;
- x) 第二个 GENERATE AC 命令请求 TC, ARC=Y3。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '6', CVR 字节 2 位 3= '0', CVR 字节 2 位 2= '0', CVR 字节 2 位 1= '1', CVR= '03 61 40 00' 或 '03 61 00 00' (用于未校验 PIN)。

7.22.17 LJSB017-00

测试目的: 卡片未执行 VERIFY 命令, PIN 已锁定。交易不能联机且拒绝脱机。设置 ADA 的“如果 PIN 在前次交易中锁定, 当交易无法联机时拒绝交易”位, 验证卡片设置 CVR 的“不能联机”位和“PIN 锁定”位, 交易拒绝脱机。

测试条件: 第 9 章中的卡片特征 17, 支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) EXTERNAL AUTHENTICATE, 正确 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) 交易 2: 锁定 PIN;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令, 错误的 PIN;
- n) VERIFY 命令, 错误的 PIN;
- o) VERIFY 命令, 错误的 PIN;
- p) 第一个 GENERATE AC 命令请求 ARQC;
- q) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- r) 第二个 GENERATE AC 命令请求 TC;
- s) 交易 3: 终端请求联机但是不能联机, 未执行 VERIFY 命令拒绝交易脱机;
- t) 卡片上电 (ATR);
- u) 选择 PBOC 借记/贷记应用;
- v) GET PROCESSING OPTIONS 命令;
- w) 第一个 GENERATE AC 命令请求 ARQC;

x) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '2', CVR 字节 2 位 1= '1', CVR 字节 3 位 7= '1', CVR= '03 21 40 00' 或 '03 21 00 00' (用于未校验 PIN)。

7.22.18 LJSB018-00

测试目的: 未执行 VERIFY 命令, PIN 已锁定。终端不能执行联机请求批准脱机。设置 ADA 中的“如果 PIN 在前次交易中锁定, 当交易无法联机时拒绝交易”位, 卡片设置 CVR 的“不能联机”位和“PIN 锁定”位, 交易拒绝脱机。

测试条件: 第 9 章中的卡片特征 17, 支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 ARQC;

g) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;

h) 第二个 GENERATE AC 命令请求 TC;

i) 交易 2: 锁定 PIN;

j) 卡片上电 (ATR);

k) 选择 PBOC 借记/贷记应用;

l) GET PROCESSING OPTIONS 命令;

m) VERIFY 命令, 错误的 PIN;

n) VERIFY 命令, 错误的 PIN;

o) VERIFY 命令, 错误的 PIN;

p) 第一个 GENERATE AC 命令请求 ARQC;

q) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;

r) 第二个 GENERATE AC 命令请求 TC;

s) 交易 3: 终端请求联机但是不能联机且脱机授受, 但 ARC=Z3, 未执行 VERIFY 命令;

t) 卡片上电 (ATR);

u) 选择 PBOC 借记/贷记应用;

v) GET PROCESSING OPTIONS 命令;

w) 第一个 GENERATE AC 命令请求 ARQC;

x) 第二个 GENERATE AC 命令请求 TC, ARC=Z3, 卡片返回 AAC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '2', CVR 字节 2 位 1= '1', CVR 字节 3 位 7= '1', CVR= '03 21 40 00' 或 '03 21 00 00' (用于未校验 PIN)。

7.22.19 LJSB019-00

测试目的: 新卡, 当交易不能执行联机且请求脱机拒绝时, 不设置 ADA 中的“如果交易拒绝, 生成通知”位, 验证卡片不设置 CID 中的“需要通知”位。

测试条件: 第 9 章中的卡片特征 1, 新卡。

测试流程: a) 交易 1: 终端请求联机但是不能联机且脱机拒绝;

- b) 卡片上电(ATR) ;
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CID 位 4= '0', CVR 字节 2 高半字节= '2', CVR 字节 2 位 1= '1', CVR 字节 3 位 5= '1', CID= '00', CVR= '03 25 10 00' 或 '03 21 10 00' (用于未校验 PIN)。

7.22.20 LJSB020-00

测试目的: 新卡, 交易不能执行联机且拒绝脱机, 设置 ADA 的“如果交易拒绝, 生成通知”位, 验证卡片设置 CID 的“需要通知”位。

测试条件: 第 9 章中的卡片特征 14, 新卡, 交易拒绝脱机时支持 ADA 的脱机需要通知位, 所有交易的终端国家代码≠ '0156', 支持连续国际交易(基于国家)频度检查。

测试流程: a) 交易 1: 终端请求联机但是不能联机, 脱机拒绝;

- b) 卡片上电(ATR) ;
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3。

通过标准: 第一个 GENERATE AC, CID= '80', 第一个 GENERATE AC, CVR= '03 A4 30 00' 或 '03 A0 30 00' (用于未校验 PIN), 第二个 GENERATE AC, CID= '08', 第二个 GENERATE AC, CVR= '03 25 30 00' 或 '03 21 30 00' (用于未校验 PIN)。

7.22.21 LJSB021-00

测试目的: 新卡, 交易不能执行联机且希望交易批准脱机, 不设置 ADA 中的“如果是新卡, 当交易无法联机时拒绝交易”位, 验证卡片批准交易脱机。

测试条件: 第 9 章中的卡片特征 1, 新卡。

测试流程: a) 交易 1: 终端请求联机但是不能联机, 脱机批准;

- b) 卡片上电(ATR) ;
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 第二个 GENERATE AC 命令请求 TC, ARC=Y3。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '6', CVR 字节 2 位 1= '1', CVR 字节 3 位 5= '1', CVR= '03 65 10 00' 或 '03 61 10 00' (用于未校验 PIN)。

7.22.22 LJSB022-00

测试目的: 新卡, 交易不能执行联机且请求批准脱机, 不设置 ADA 中的“如果交易拒绝, 生成通

知”位、设置“如果是新卡，当交易无法联机时拒绝交易”位，验证卡片不设置CID的“需要通知”位，卡片强制交易拒绝脱机。

测试条件：第9章中的卡片特征16，支持新卡检查。

测试流程：a) 交易1：终端请求联机但是不能联机，请求脱机批准，卡片拒绝；

b) 卡片上电(ATR)；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) 第二个 GENERATE AC 命令请求 TC，ARC=Y3，卡片返回 AAC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘00’，CID 位 4=‘0’，CVR 字节 2 高半字节=‘2’，CVR 字节 2 位 1=‘1’，CVR 字节 3 位 5=‘1’，CID=‘00’，CVR=‘03 25 10 00’或‘03 21 10 00’（用于未校验 PIN）。

7.22.23 LJSB023-00

测试目的：新卡，交易不能执行联机且要求批准脱机，设置 ADA 中的“如果交易拒绝，生成通知”位和“如果是新卡，当交易无法联机时拒绝交易”位，验证卡片设置 CID 的“需要通知”位且卡片强制交易拒绝脱机。

测试条件：第9章中的卡片特征18，支持新卡检查和 ADA “如果交易脱机拒绝，需要通知”位。

测试流程：a) 交易1：终端请求联机但是不能联机，脱机批准，卡片拒绝；

b) 卡片上电(ATR)；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) 第二个 GENERATE AC 命令请求 TC，ARC=Y3，卡片返回 AAC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘00’，CID 位 4=‘1’，CVR 字节 2 高半字节=‘2’，CVR 字节 2 位 1=‘1’，CVR 字节 3 位 5=‘1’，CID=‘08’，CVR=‘03 25 10 00’或‘03 21 10 00’（用于未校验 PIN）。

7.22.24 LJSB024-00

测试目的：交易不能执行联机且批准脱机交易，ARC=Y3，验证卡片不设置 CVR 的“超过频率检查”位，ATC 与 LOATC 之差等于 UCOL。

测试条件：第9章中的卡片特征7，支持连续脱机交易频度检查（上限）。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：终端请求联机但是不能联机，脱机批准；

c) 卡片上电(ATR)；

d) 选择PBOC借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) 第二个 GENERATE AC 命令请求 TC，ARC=Y3；

i) 交易3：终端请求联机但是不能联机，脱机批准；

- j) 卡片上电(ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 命令请求 ARQC;
- o) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;
- p) 交易 4: 终端请求联机但是不能联机, 脱机批准;
- q) 卡片上电(ATR);
- r) 选择 PBOC 借记/贷记应用;
- s) GET PROCESSING OPTIONS 命令;
- t) VERIFY 命令;
- u) 第一个 GENERATE AC 命令请求 ARQC;
- v) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;
- w) 交易 5: 终端请求联机但是不能联机, 脱机批准;
- x) 卡片上电(ATR);
- y) 选择 PBOC 借记/贷记应用;
- z) GET PROCESSING OPTIONS 命令;
- aa) VERIFY 命令;
- ab) 第一个 GENERATE AC 命令请求 ARQC;
- ac) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;
- ad) 交易 6: 终端请求联机但是不能联机, 脱机批准;
- ae) 卡片上电(ATR);
- af) 选择 PBOC 借记/贷记应用;
- ag) GET PROCESSING OPTIONS 命令;
- ah) VERIFY 命令;
- ai) 第一个 GENERATE AC 命令请求 ARQC;
- aj) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;
- ak) 交易 7: 终端请求联机但是不能联机, 脱机批准;
- al) 卡片上电(ATR);
- am) 选择 PBOC 借记/贷记应用;
- an) GET PROCESSING OPTIONS 命令;
- ao) VERIFY 命令;
- ap) 第一个 GENERATE AC 命令请求 ARQC;
- aq) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;
- ar) 交易 8: 终端请求联机但是不能联机, 脱机批准;
- as) 卡片上电(ATR);
- at) 选择 PBOC 借记/贷记应用;
- au) GET PROCESSING OPTIONS 命令;
- av) VERIFY 命令;
- aw) 第一个 GENERATE AC 命令请求 ARQC;
- ax) 第二个 GENERATE AC 命令请求 TC, ARC=Y3。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '6', CVR 字节 2 位 1= '1', CVR 字节 3 位 6= '0', CVR= '03 65 80 00' 或 '03 61 80 00' (用于未

校验 PIN)。

7.22.25 LJSB025-00

测试目的：交易不能执行联机且批准脱机，ARC=Y3，验证当 ATC 与 LOATC 之差大于 UCOL 时，卡片设置 CVR 的“超过频率检查”位，卡片拒绝交易脱机。

测试条件：第 9 章中的卡片特征 7，支持连续脱机交易频度检查（上限）。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：终端请求联机但是不能联机，脱机批准；

c) 卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) 第二个 GENERATE AC 命令请求 TC，ARC=Y3；

i) 交易 3：终端请求联机但是不能联机，脱机批准；

j) 卡片上电(ATR)；

k) 选择 PBOC 借记/贷记应用；

l) GET PROCESSING OPTIONS 命令；

m) VERIFY 命令；

n) 第一个 GENERATE AC 命令请求 ARQC；

o) 第二个 GENERATE AC 命令请求 TC，ARC=Y3；

p) 交易 4：终端请求联机但是不能联机，脱机批准；

q) 卡片上电(ATR)；

r) 选择 PBOC 借记/贷记应用；

s) GET PROCESSING OPTIONS 命令；

t) VERIFY 命令；

u) 第一个 GENERATE AC 命令请求 ARQC；

v) 第二个 GENERATE AC 命令请求 TC，ARC=Y3；

w) 交易 5：终端请求联机但是不能联机，脱机批准；

x) 卡片上电(ATR)；

y) 选择 PBOC 借记/贷记应用；

z) GET PROCESSING OPTIONS 命令；

aa) VERIFY 命令；

ab) 第一个 GENERATE AC 命令请求 ARQC；

ac) 第二个 GENERATE AC 命令请求 TC，ARC=Y3；

ad) 交易 6：终端请求联机但是不能联机，脱机批准；

ae) 卡片上电(ATR)；

af) 选择 PBOC 借记/贷记应用；

ag) GET PROCESSING OPTIONS 命令；

ah) VERIFY 命令；

ai) 第一个 GENERATE AC 命令请求 ARQC；

aj) 第二个 GENERATE AC 命令请求 TC，ARC=Y3；

ak) 交易 7：终端请求联机但是不能联机，脱机批准；

- a1) 卡片上电(ATR);
- am) 选择 PBOC 借记/贷记应用;
- an) GET PROCESSING OPTIONS 命令;
- ao) VERIFY 命令;
- ap) 第一个 GENERATE AC 命令请求 ARQC;
- aq) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;
- ar) 交易 8: 终端请求联机但是不能联机, 脱机批准;
- as) 卡片上电(ATR);
- at) 选择 PBOC 借记/贷记应用;
- au) GET PROCESSING OPTIONS 命令;
- av) VERIFY 命令;
- aw) 第一个 GENERATE AC 命令请求 ARQC;
- ax) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;
- ay) 交易 9: 终端请求联机但是不能联机, 脱机批准。卡片强制交易拒绝脱机;
- az) 卡片上电(ATR);
- ba) 选择 PBOC 借记/贷记应用;
- bb) GET PROCESSING OPTIONS 命令;
- bc) VERIFY 命令;
- bd) 第一个 GENERATE AC 命令请求 ARQC;
- be) 第二个 GENERATE AC 命令请求 TC, ARC=Y3, 卡片返回 AAC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '2', CVR 字节 2 位 1= '1', CVR 字节 3 位 6= '1', CVR= '03 25 A0 00' 或 '03 21 A0 00' (用于未校验 PIN)。

7.23 GET DATA (GEDA)

7.23.1 GEDA001-00

测试目的: 对于成功的 GET DATA 命令, 卡片响应返回 '9000'。

测试条件: 第 9 章中的卡片特征 20 或者第 9 章中的卡片特征 1 (如果不支持第 9 章中的卡片特征 20)。

- 测试流程:
- a) 卡片上电(ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) GET DATA 命令, P1P2 = '9F13';
 - e) GET DATA 命令, P1P2 = '9F17';
 - f) GET DATA 命令, P1P2 = '9F36';
 - g) GET DATA 命令, P1P2 = '9F4F'。

通过标准: 所有 GET DATA 命令 SW1 SW2= '9000'。

7.24 GET PROCESSING OPTIONS 命令 (GPML)

7.24.1 GPML001-00

测试目的: 针对成功的 GET PROCESSING OPTIONS 命令 (PDOL 存在), 卡片返回 '9000'。

测试条件: 第 9 章中的卡片特征 1, PDOL 存在。

测试流程：a) 执行正确的 GET PROCESSING OPTIONS 命令，PDOL 正确。
通过标准：SW1 SW2= ‘9000’ 。

7.24.2 GPML002-00

测试目的：无 PDOL 且数据错误，则执行 GET PROCESSING OPTIONS 命令应不成功。
测试条件：第 9 章中的卡片特征 1，PDOL 不存在。
测试流程：a) 执行 GET PROCESSING OPTIONS 命令，命令格式见表 21，其数据不正确。

表21 GET PROCESSING OPTIONS 命令报文

CLA	INS	P1	P2	Lc	Data	Le
80	A8	00	00	02	85 00	N/A

通过标准：SW1 SW2≠ ‘9000’，建议返回 ‘6A80’、‘6984’、‘6985’。

7.24.3 GPML003-00

测试目的：PDOL 存在但数据错误，执行 GET PROCESSING OPTIONS 命令应不成功。
测试条件：第 9 章中的卡片特征 1，PDOL 存在。
测试流程：a) 执行 GET PROCESSING OPTIONS 命令，命令格式见表 22，其数据不正确。

表22 GET PROCESSING OPTIONS 命令报文

CLA	INS	P1	P2	Lc	Data	Le
80	A8	00	00	04	85 02 01 56	N/A

* PDOL 是不同的，这个例子中的 PDOL 数据代表的是终端国家代码。

通过标准：SW1 SW2≠ ‘9000’，建议返回 ‘6984’、‘6985’。

7.25 发卡行认证(FKRZ)

7.25.1 FKRZ001-00

测试目的：计算 ARPC 的密钥不正确，验证卡片拒绝 EXTERNAL AUTHENTICATE 命令。
测试条件：第 9 章中的卡片特征 1，支持发卡行认证与指定货币的交易金额频度检查。
测试流程：a) 卡片上电(ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 命令请求 ARQC；
f) 执行 EXTERNAL AUTHENTICATE 命令，ARPC 错误。
注：用错误的密钥计算出 ARPC。
通过标准：SW1 SW2= ‘6300’ 。

7.25.2 FKRZ002-00

测试目的：计算 ARPC 的 ARC 不正确，验证卡片拒绝 EXTERNAL AUTHENTICATE 命令。
测试条件：第 9 章中的卡片特征 1，支持发卡行认证。
测试流程：a) 卡片上电(ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；

- e) 第一个 GENERATE AC 命令请求 ARQC;
 - f) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 错误 (ARC= '3030')。
- 注: 计算 ARPC (ARC= '3130')。

通过标准: SW1 SW2= '6300' 。

7.25.3 FKRZ003-00

测试目的: 计算 ARPC 的 ARQC 不同于用第一个 GENERATE AC 返回的 ARQC, 验证卡片拒绝 EXTERNAL AUTHENTICATE 命令。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证与指定货币的交易金额频度检查。

- 测试流程:
- a) 卡片上电 (ATR);
 - b) 选择 PBOC 借记/贷记应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 命令请求 ARQC;
 - f) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 错误。
- 注: 计算 ARPC 的 ARQC 不同于用第一个 GENERATE AC 返回的 ARQC。

通过标准: SW1 SW2= '6300' 。

7.25.4 FKRZ004-00

测试目的: 验证卡片拒绝第二个带有正确 ARPC 的 EXTERNAL AUTHENTICATE 命令, 设置发卡行认证失败指示器。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 终端联机拒绝, 多个发卡行认证;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 命令请求 ARQC;
 - h) EXTERNAL AUTHENTICATE 命令, ARPC 正确;
 - i) EXTERNAL AUTHENTICATE 命令, ARPC 正确;
 - j) 第二个 GENERATE AC 命令请求 AAC;
 - k) 交易 3: 终端请求脱机批准, 卡片强制联机批准;
 - l) 卡片上电 (ATR);
 - m) 选择 PBOC 借记/贷记应用;
 - n) GET PROCESSING OPTIONS 命令;
 - o) VERIFY 命令;
 - p) 第一个 GENERATE AC 命令请求 TC, 卡片返回 ARQC;
 - q) EXTERNAL AUTHENTICATE 命令, ARPC 正确;
 - r) 第二个 GENERATE AC 命令请求 TC。

通过标准: 交易 2: 第一个 GENERATE AC, CID= '80', 第一个 GENERATE AC, CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN), 第一次 EXTERNAL AUTHENTICATE 命令, SW1 SW2= '9000', 第二次 EXTERNAL AUTHENTICATE 命令, SW1 SW2= '6985', 第二个

GENERATE AC, CID= '00' , 第二个 GENERATE AC, CVR= '03 2C 00 00' 或 '03 24 00 00' (用于未校验 PIN)。交易 3: 第一个 GENERATE AC, CID= '80' , 第一个 GENERATE AC, CVR= '03 A4 88 00' 或 '03 A0 08 00' (用于未校验 PIN) , 第二个 GENERATE AC, CID= '40' , 第二个 GENERATE AC, CVR= '03 64 88 00' 或 '03 60 08 00' (用于未校验 PIN) ,

7.25.5 FKRZ005-00

测试目的: 验证卡片拒绝带有错误 ARPC 的第二个 EXTERNAL AUTHENTICATE 命令。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 卡片上电 (ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) VERIFY 命令;
e) 第一个 GENERATE AC 命令请求 ARQC;
f) EXTERNAL AUTHENTICATE 命令 (错误的 ARPC);
g) EXTERNAL AUTHENTICATE 命令 (错误的 ARPC)。
注: 用错误的密钥计算 ARPC。

通过标准: SW1 SW2= '6985' 。

7.25.6 FKRZ006-00

测试目的: 借记/贷记应用锁定, ARPC 正确, 验证卡片接收 EXTERNAL AUTHENTICATE 命令, ARPC 由 AAC 计算得出。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证、应用锁定以及应用解锁, 借记/贷记应用锁定。

测试流程: a) 卡片上电 (ATR)。
b) 选择 PBOC 借记/贷记应用。
c) GET PROCESSING OPTIONS 命令。
d) VERIFY 命令。
e) 第一个 GENERATE AC 命令请求 ARQC (卡片返回 AAC)。
f) EXTERNAL AUTHENTICATE 命令。

通过标准: 选择 PBOC 借记/贷记应用, SW1 SW2= '6283' , EXTERNAL AUTHENTICATE 命令, SW1 SW2= '9000' 。

7.25.7 FKRZ007-00

测试目的: 卡锁定, 验证卡片拒绝 EXTERNAL AUTHENTICATE 命令。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证与卡锁定, 卡片已经锁定。

测试流程: a) 卡片上电 (ATR);
b) 选择无效的 PSE;
c) 选择无效的 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) 第一个 GENERATE AC 命令请求 ARQC;
f) EXTERNAL AUTHENTICATE 命令。

通过标准: 选择 PSE, SW1 SW2= '6A81' , 选择借记/贷记命令, SW1 SW2= '6A81' , EXTERNAL

AUTHENTICATE 命令 SW1 SW2≠‘9000’，建议返回 SW1 SW2=‘6985’或‘6A81’。

7.25.8 FKRZ008-00

测试目的：未选择 PBOC 借记/贷记应用，验证卡片拒绝 EXTERNAL AUTHENTICATE 命令。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：a) 卡片上电 (ATR)；
b) GET PROCESSING OPTIONS 命令；
c) 第一个 GENERATE AC 命令请求 ARQC；
d) EXTERNAL AUTHENTICATE 命令。

通过标准：EXTERNAL AUTHENTICATE 命令 SW1 SW2≠‘9000’，建议返回 SW1 SW2=‘6985’。

7.25.9 FKRZ009-00

测试目的：借记/贷记应用未初始化，验证卡片拒绝 EXTERNAL AUTHENTICATE 命令。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) 第一个 GENERATE AC 命令请求 ARQC；
d) EXTERNAL AUTHENTICATE 命令。

通过标准：EXTERNAL AUTHENTICATE 命令返回 SW1 SW2≠‘9000’，建议返回 SW1 SW2=‘6985’。

7.25.10 FKRZ010-00

测试目的：在执行第二个 GENERATE AC 命令请求联机批准交易后，验证卡片拒绝执行第二个 EXTERNAL AUTHENTICATE 命令。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证、指定货币的交易金额频度检查。

测试流程：a) 卡片上电 (ATR)。
b) 选择 PBOC 借记/贷记应用。
c) GET PROCESSING OPTIONS 命令。
d) 第一个 GENERATE AC 命令请求 ARQC。
e) EXTERNAL AUTHENTICATE 命令。
f) 第二个 GENERATE AC 命令请求 TC。
g) EXTERNAL AUTHENTICATE 命令。

通过标准：对于第二个 EXTERNAL AUTHENTICATE 命令卡返回 SW1 SW2=‘6985’。

7.25.11 FKRZ011-00

测试目的：在执行第二个 GENERATE AC 命令请求联机拒绝交易后，验证卡片拒绝执行第二个 EXTERNAL AUTHENTICATE 命令。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证、指定货币的交易金额频度检查。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 第一个 GENERATE AC 命令请求 ARQC；
e) EXTERNAL AUTHENTICATE 命令；
f) 第二个 GENERATE AC 命令请求 AAC；

g) EXTERNAL AUTHENTICATE 命令。

通过标准：对于第二个 EXTERNAL AUTHENTICATE 命令卡返回 SW1 SW2= ‘6985’。

7.26 应用初始化(YYCS)

7.26.1 YYCS001-00

测试目的：验证卡片对 GET PROCESSING OPTIONS 命令的响应。

测试条件：标准联机交易成功。

测试流程：a) 卡片上电(ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令。

通过标准：返回数据模板标签为 ‘80’，返回数据模块的长度=AIP 长度+AFL 的长度，至少为 ‘06’。

7.26.2 YYCS002-00

测试目的：在 GET PROCESSING OPTIONS 响应的数据域中检查 AIP、AFL。

测试条件：标准联机交易成功。

测试流程：a) 卡片上电(ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令。

通过标准：AIP= ‘5C 00’，AFL 至少 4 字节。

7.26.3 YYCS003-00

测试目的：检查 AFL 每个单元的第 1 字节的值。

测试条件：标准联机交易成功。

测试流程：a) 卡片上电(ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令。

通过标准：每个单元第 1 字节= ‘XXXXX000’。

7.26.4 YYCS004-00

测试目的：检查 AFL 每个单元的第 2 字节的值。

测试条件：标准联机交易成功。

测试流程：a) 卡片上电(ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令。

通过标准：每个单元的第 2 个字节≠0。

7.26.5 YYCS005-00

测试目的：检查 AFL 每个单元的第 3 字节的值。

测试条件：标准联机交易成功。

测试流程：a) 卡片上电(ATR)。
b) 选择 PBOC 借记/贷记应用。
c) GET PROCESSING OPTIONS 命令。

通过标准：每个单元的第 3 字节≥每个单元的第 2 字节。

7.26.6 YYCS006-00

测试目的：检查 AFL 每个单元的第 4 字节的值。

测试条件：标准联机交易成功。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令。

通过标准：至少一个单元非零。

7.26.7 YYCS007-00

测试目的：选择应用无效时，验证卡片接受 GET PROCESSING OPTIONS 命令。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK、APPLICATION BLOCK，应用已锁定。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令。

通过标准：选择应用 SW1 SW2= ‘6283’，GET PROCESSING OPTIONS 命令，SW1 SW2= ‘9000’。

7.26.8 YYCS008-00

测试目的：卡已锁定，卡片应拒绝执行 GET PROCESSING OPTIONS 命令。

测试条件：第 9 章中的卡片特征 1，支持 CARD BLOCK，卡已被锁定。

测试流程：a) 卡片上电 (ATR)；
b) 选择无效的 PSE；
c) 选择无效的 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令。

通过标准：选择 PSE，SW1 SW2= ‘6A81’，选择借贷记应用，SW1 SW2= ‘6A81’，执行 GET PROCESSING OPTIONS 命令 SW1 SW2≠ ‘9000’，推荐返回 ‘6985’ 或 ‘6A81’。

7.26.9 YYCS009-00

测试目的：未选择应用，卡片应拒绝执行 GET PROCESSING OPTIONS 命令。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) GET PROCESSING OPTIONS 命令。

通过标准：执行 GET PROCESSING OPTIONS 命令，SW1 SW2≠ ‘9000’，建议返回 SW1 SW2= ‘6985’。

7.27 发卡行脚本处理 (JBCL)

7.27.1 JBCL001-00

测试目的：卡片批准交易脱机，验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易 3 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 置 ‘0000’。验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：批准脱机；

c) 交易 3: 批准脱机。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 4= '00', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.27.2 JBCL002-00

测试目的: 卡片拒绝交易脱机, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易 3 批准脱机, 验证卡片设置 CVR 的第 4 字节位 8-5 置 '0000', 验证卡片不设置 CVR 中的“上次发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 拒绝脱机;

c) 交易 3: 批准脱机。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 4= '00', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.27.3 JBCL003-00

测试目的: 交易请求联机但终端不能执行联机且交易拒绝脱机, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。验证卡片请求交易 3 执行联机 (因为前次交易中已设置“联机授权指示”位), 验证卡片设置 CVR 的第 4 字节位 8-5 置 '0000', 验证卡片不设置 CVR 中的“上次发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 终端请求联机但是不能联机, 拒绝脱机;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 命令请求 ARQC;

h) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;

i) 交易 3: 在第一个 GENERATE AC 中终端请求 TC 后, 卡片请求执行联机;

j) 卡片上电 (ATR);

k) 选择 PBOC 借记/贷记应用;

l) GET PROCESSING OPTIONS 命令;

m) VERIFY 命令;

n) 第一个 GENERATE AC 命令请求 TC, 卡返回 ARQC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '00', CVR= '03 A4 80 00' 或 '03 A0 80 00' (用于未校验 PIN)。

7.27.4 JBCL004-00

测试目的: 联机批准交易中, 当卡片未执行发卡行脚本命令时, 验证卡片不设置“发卡行脚本命

令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易 3 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 置‘0000’，验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：未执行发卡行脚本，批准联机；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

j) 交易 3：批准脱机。

通过标准：验证交易 3 第一个 GENERATE AC 返回响应，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘00’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.27.5 JBCL005-00

测试目的：联机拒绝交易过程中，卡片未执行发卡行脚本命令时，验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易 3 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 置‘0000’，验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：未执行发卡行脚本，联机拒绝；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 AAC；

j) 交易 3：批准脱机。

通过标准：验证交易 3 第一个 GENERATE AC 返回响应，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘00’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.27.6 JBCL006-00

测试目的：联机批准交易过程中，卡片执行成功的发卡行脚本命令（例如：APPLICATION UNBLOCK 命令），验证卡片设置“发卡行脚本命令计数器”位和重置“发卡行脚本失败指示器”位。交易 3 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 为‘0001’，验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第9章中的卡片特征1，支持 APPLICATION BLOCK 命令和 APPLICATION UNBLOCK 命令。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：批准联机（发卡行脚本命令执行成功）；

c) 卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

j) 执行 APPLICATION UNBLOCK 命令（MAC 正确）；

k) 交易3：批准脱机。

通过标准：验证交易3 第一个 GENERATE AC 返回响应，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘10’，CVR=‘03 94 00 10’ 或 ‘03 90 00 10’（用于未校验 PIN）。

7.27.7 JBCL007-00

测试目的：联机拒绝交易过程中，卡片执行成功的发卡行脚本命令（例如：APPLICATION UNBLOCK 命令），验证卡片设置“发卡行脚本命令计数器”位和重置“发卡行脚本失败指示器”位。交易3 批准脱机，验证卡片设置 CVR 的第4字节位 8-5 为‘0001’，验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第9章中的卡片特征1，支持 APPLICATION BLOCK 命令和 APPLICATION UNBLOCK 命令。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：拒绝联机（执行发卡行脚本命令成功）；

c) 卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 AAC；

j) 执行 APPLICATION UNBLOCK 命令，MAC 正确；

k) 交易3：批准脱机。

通过标准：验证交易3 第一个 GENERATE AC 返回响应，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘10’，CVR=‘03 94 00 10’ 或 ‘03 90 00 10’（用于未校验 PIN）。

7.27.8 JBCL008-00

测试目的：联机批准交易过程中，卡片执行失败的发卡行脚本命令（例如：APPLICATION UNBLOCK 命令）。发卡行脚本命令不包含 MAC，验证卡片不设置“发卡行脚本命令计数器”位但设置“上次交易发卡行脚本处理失败指针”位。交易3 批准脱机，验证卡片设置 CVR 的第4字节位 8-5 为‘0000’，验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第9章中的卡片特征1，支持 APPLICATION BLOCK 命令和 APPLICATION UNBLOCK 命令。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：批准联机（执行发卡行脚本命令不成功）；

c) 卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

j) 执行 APPLICATION UNBLOCK 命令，无 MAC；

k) 交易3：批准脱机。

通过标准：验证交易3第一个 GENERATE AC 返回响应，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘08’，CVR=‘03 94 00 08’或‘03 90 00 08’（用于未校验 PIN）。

7.27.9 JBCL009-00

测试目的：联机批准交易过程中，卡片执行失败的发卡行脚本命令（例如：APPLICATION UNBLOCK 命令）。发卡行脚本命令 MAC 错误，验证卡片设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易3批准脱机，验证卡片设置 CVR 的第4字节位 8-5 为‘0001’，验证卡片设置 CVR 中的“上次发卡行脚本处理失败”位。

测试条件：第9章中的卡片特征1，支持 APPLICATION BLOCK 命令和 APPLICATION UNBLOCK 命令。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：批准联机（执行发卡行脚本命令不成功）；

c) 卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

j) APPLICATION UNBLOCK 命令，MAC 错误；

k) 交易3：批准脱机。

通过标准：验证交易3第一个 GENERATE AC 返回响应，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘18’，CVR=‘03 94 00 18’或‘03 90 00 18’（用于未校验 PIN）。

7.27.10 JBCL010-00

测试目的：联机批准交易过程中，卡片执行失败的发卡行脚本命令（例如：PUT DATA 命令修改 UCOL）。发卡行脚本命令不包含 MAC，验证卡片不设置“发卡行脚本命令计数器”位但设置“上次交易发卡行脚本处理失败指针”位。交易3批准脱机，验证卡片设置 CVR 的第4字节位 8-5 为‘0000’，验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第9章中的卡片特征1，支持PUT DATA命令修改UCOL。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：批准联机（执行发卡行脚本命令不成功）；

c) 卡片上电(ATR)；

d) 选择PBOC借记/贷记应用；

e) GET PROCESSING OPTIONS命令；

f) VERIFY命令；

g) 第一个GENERATE AC命令请求ARQC；

h) EXTERNAL AUTHENTICATE命令，正确ARPC；

i) 第二个GENERATE AC命令请求TC；

j) 执行PUT DATA命令修改UCOL，无MAC；

k) 交易3：批准脱机。

通过标准：验证交易3第一个GENERATE AC返回响应，SW1 SW2=‘9000’，CID位8-7=‘01’，CVR字节2高半字节=‘9’，CVR字节4=‘08’，CVR=‘03 94 00 08’或‘03 90 00 08’（用于未校验PIN）。

7.27.11 JBCL011-00

测试目的：联机拒绝交易过程中，卡片执行失败的发卡行脚本命令（例如：PUT DATA命令修改LCOL）。发卡行脚本命令不包含MAC，验证卡片不设置“发卡行脚本命令计数器”位但设置“上次交易发卡行脚本处理失败指针”位。交易3批准脱机，设置CVR的第4字节位8-5为‘0000’，验证卡片设置CVR中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第9章中的卡片特征1，支持PUT DATA命令修改LCOL。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：批准联机（执行发卡行脚本命令不成功）；

c) 卡片上电(ATR)；

d) 选择PBOC借记/贷记应用；

e) GET PROCESSING OPTIONS命令；

f) VERIFY命令；

g) 第一个GENERATE AC命令请求ARQC；

h) EXTERNAL AUTHENTICATE命令，正确ARPC；

i) 第二个GENERATE AC命令请求TC；

j) 执行PUT DATA命令修改LCOL，无MAC；

k) 交易3：批准脱机。

通过标准：验证交易3第一个GENERATE AC返回响应，SW1 SW2=‘9000’，CID位8-7=‘01’，CVR字节2高半字节=‘9’，CVR字节4=‘08’，CVR=‘03 94 00 08’或‘03 90 00 08’（用于未校验PIN）。

7.27.12 JBCL012-00

测试目的：联机拒绝交易过程中，卡片执行失败的发卡行脚本命令（例如：PUT DATA命令修改LCOL）。发卡行脚本命令包含错误MAC，验证卡片设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易3批准脱机，验证卡片设置CVR的第4字节位8-5为‘0001’，验证卡片设置CVR中的“上次交易发卡行脚本处理失败

指针”位。

测试条件：第9章中的卡片特征1，支持PUT DATA命令修改LCOL。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：拒绝联机（执行发卡行脚本命令不成功）；

c) 卡片上电(ATR)；

d) 选择PBOC借记/贷记应用；

e) GET PROCESSING OPTIONS命令；

f) VERIFY命令；

g) 第一个GENERATE AC命令请求ARQC；

h) EXTERNAL AUTHENTICATE命令，正确ARPC；

i) 第二个GENERATE AC命令请求AAC；

j) PUT DATA命令修改LCOL，MAC错误；

k) 交易3：批准脱机。

通过标准：验证交易3第一个GENERATE AC返回响应，SW1 SW2=‘9000’，CID位8-7=‘01’，CVR字节2高半字节=‘9’，CVR字节4=‘18’，CVR=‘03 94 00 18’或‘03 90 00 18’（用于未校验PIN）。

7.27.13 JBCL013-00

测试目的：联机拒绝交易过程中，卡片执行失败的发卡行脚本命令（例如：PUT DATA命令修改UCOL）。发卡行脚本命令不包含MAC，验证卡片不设置“发卡行脚本命令计数器”位但设置“上次交易发卡行脚本处理失败指针”位。交易3批准脱机，验证设置CVR的第4字节位8-5为‘0000’，验证卡片设置CVR中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第9章中的卡片特征1，支持PUT DATA命令修改UCOL。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：拒绝联机（执行发卡行脚本命令不成功）；

c) 卡片上电(ATR)；

d) 选择PBOC借记/贷记应用；

e) GET PROCESSING OPTIONS命令；

f) VERIFY命令；

g) 第一个GENERATE AC命令请求ARQC；

h) EXTERNAL AUTHENTICATE命令，正确ARPC；

i) 第二个GENERATE AC命令请求AAC；

j) PUT DATA命令修改UCOL，无MAC；

k) 交易3：批准脱机。

通过标准：验证交易3第一个GENERATE AC返回响应，SW1 SW2=‘9000’，CID位8-7=‘01’。CVR字节2高半字节=‘9’，CVR字节4=‘08’，CVR=‘03 94 00 08’或‘03 90 00 08’（用于未校验PIN）。

7.27.14 JBCL014-00

测试目的：在联机批准交易过程中，卡片执行两次成功的发卡行脚本命令（APPLICATION UNBLOCK命令和PUT DATA命令修改LCOL）。验证卡片设置“发卡行脚本命令计数器”位为2和重置“发卡行脚本失败指示器”位。交易3批准脱机，验证卡片设置CVR的第4字

字节 8-5 为 ‘0010’，验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：批准联机（执行两个成功的发卡行脚本命令）；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

j) APPLICATION UNBLOCK 命令，MAC 正确；

k) PUT DATA 命令修改 LCOL，MAC 正确；

l) 交易 3：批准脱机。

通过标准：验证交易 3 第一个 GENERATE AC 返回响应，SW1 SW2= ‘9000’，CID 位 8-7= ‘01’，CVR 字节 2 高半字节= ‘9’，CVR 字节 4= ‘20’，CVR= ‘03 94 00 20’ 或 ‘03 90 00 20’（用于未校验 PIN）。

7.27.15 JBCL015-00

测试目的：在联机交易拒绝过程中，卡片执行两次成功的发卡行脚本命令（APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 LCOL）。验证卡片设置“发卡行脚本命令计数器”位为 2 和重置“发卡行脚本失败指示器”位。交易 3 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 为 ‘0010’，验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：拒绝联机（执行发卡行脚本成功）；

c) 卡片上电 (ATR)；

d) 选择应用；

e) 执行 GET PROCESSING OPTIONS 命令；

f) 执行 VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，ARPC 正确；

i) 第二个 GENERATE AC 请求 AAC；

j) APPLICATION UNBLOCK 命令，MAC 正确；

k) PUT DATA 命令修改 LCOL，MAC 正确；

l) 交易 3：批准脱机。

通过标准：验证交易 3 第一个 GENERATE AC 返回响应，SW1 SW2= ‘9000’，CID 位 8-7= ‘01’，CVR 字节 2 高半字节= ‘9’，CVR 字节 4= ‘20’，CVR= ‘03 94 00 20’ 或 ‘03 90 00 20’（用于未校验 PIN）。

7.27.16 JBCL016-00

测试目的：联机批准交易过程中，第二个 GENERATE AC 命令之后卡片收到两个发卡行脚本命令，第一个发卡行脚本（如 APPLICATION UNBLOCK 命令）成功，MAC 正确；第二个发卡行脚本（如 PUT DATA 命令修改 LCOL）不成功，MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。交易 3 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 为‘0010’，验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK、APPLICATION BLOCK 和 PUT DATA 命令修改 LCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：批准联机（两个发卡行脚本），第一个发卡行脚本命令成功（MAC 正确）；
c) 第二个发卡行脚本命令不成功（MAC 错误）；
d) 卡片上电（ATR）；
e) 选择 PBOC 借记/贷记应用；
f) GET PROCESSING OPTIONS 命令；
g) VERIFY 命令；
h) 第一个 GENERATE AC 命令请求 ARQC；
i) EXTERNAL AUTHENTICATE 命令，正确 ARPC；
j) 第二个 GENERATE AC 命令请求 TC；
k) APPLICATION UNBLOCK，MAC 正确；
l) PUT DATA 命令修改 UCOL，MAC 错误；
m) 交易 3：批准脱机。

通过标准：验证交易 3 第一个 GENERATE AC 返回响应，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘28’，CVR=‘03 94 00 28’或‘03 90 00 28’（用于未校验 PIN）。

7.27.17 JBCL017-00

测试目的：联机拒绝交易过程中，第二个 GENERATE AC 命令之后卡片收到两个发卡行脚本命令，第一个发卡行脚本（如 APPLICATION UNBLOCK 命令）成功，MAC 正确；第二个发卡行脚本（如 PUT DATA 命令修改 UCOL）不成功，MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。交易 3 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 为‘0010’，验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK、APPLICATION BLOCK 和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：拒绝联机（两个发卡行脚本），第一个发卡行脚本命令成功（MAC 正确）；
c) 第二个发卡行脚本命令不成功（MAC 错误）；
d) 卡片上电（ATR）；
e) 选择应用；
f) 执行 GET PROCESSING OPTIONS 命令；
g) 执行 VERIFY 命令；
h) 第一个 GENERATE AC 请求 ARQC；
i) EXTERNAL AUTHENTICATE 命令，ARPC 正确；

- j) 第二个 GENERATE AC 请求 AAC;
- k) APPLICATION UNBLOCK 命令, MAC 错误;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 批准脱机。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 4= '28', CVR= '03 94 00 28' 或 '03 90 00 28' (用于未校验 PIN)。

7.27.18 JBCL018-00

测试目的: 卡片批准交易脱机, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易 3 拒绝脱机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0000', 验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 批准脱机;

c) 交易 3: 拒绝脱机。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 4= '00', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.27.19 JBCL019-00

测试目的: 卡片拒绝交易脱机, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易 3 拒绝脱机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0000', 验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 拒绝脱机;

c) 交易 3: 拒绝脱机。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 4= '00', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.27.20 JBCL020-00

测试目的: 联机批准交易过程中, 卡片不执行发卡行脚本命令, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易 3 拒绝脱机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0000', 验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 批准联机 (未执行发卡行脚本命令);

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- i) 第二个 GENERATE AC 命令请求 TC;
- j) 交易 3: 拒绝脱机。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 4= '00', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.27.21 JBCL021-00

测试目的: 联机拒绝交易过程中, 卡片不执行发卡行脚本命令, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。交易 3 拒绝脱机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0000', 验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 拒绝联机 (未执行发卡行脚本命令);
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- i) 第二个 GENERATE AC 命令请求 AAC;
- j) 交易 3: 拒绝脱机。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 4= '00', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.27.22 JBCL022-00

测试目的: 联机批准交易过程中, 卡片执行成功的 APPLICATION BLOCK 命令, 验证卡片设置“发卡行脚本命令计数器”位为 1 和重置“发卡行脚本失败指示器”位。卡片强制交易 3 拒绝脱机, 验证卡片设置 CVR 的第 4 字节位 8-7 为 '0001', 验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 和 APPLICATION BLOCK。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准联机 (执行发卡行脚本命令成功);
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;

- i) 第二个 GENERATE AC 命令请求 TC;
- j) APPLICATION BLOCK 命令, MAC 正确;
- k) 交易 3: 终端请求 ARQC 后卡片返回 AAC;
- l) 卡片上电(ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 ARQC, 卡返 AAC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 4= '10', CVR= '03 84 00 10' 或 '03 80 00 10' (用于未校验 PIN)。

7.27.23 JBCL023-00

测试目的: 联机拒绝交易过程中, 卡片执行成功的 APPLICATION BLOCK 命令, 验证卡片设置“发卡行脚本命令计数器”位为 1 和重置“发卡行脚本失败指示器”位。卡片强制交易 3 拒绝脱机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0001', 验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 和 APPLICATION BLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 拒绝联机(执行成功的发卡行脚本命令);
- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- i) 第二个 GENERATE AC 命令请求 AAC;
- j) 执行 APPLICATION BLOCK 命令, MAC 正确;
- k) 交易 3: 终端请求 ARQC 后, 卡片返回 AAC;
- l) 卡片上电(ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 ARQC, 卡返 AAC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 4= '10', CVR= '03 84 00 10' 或 '03 80 00 10' (用于未校验 PIN)。

7.27.24 JBCL024-00

测试目的: 联机批准交易过程中, 执行第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本(如 APPLICATION BLOCK 命令)成功, MAC 正确; 第二个发卡行脚本(如 PUT DATA 命令修改 LCOL)不成功, MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。

卡片强制交易 3 拒绝脱机，验证卡片设置 CVR 的第 4 字节位 8-5 为 ‘0010’，验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK、APPLICATION UNBLOCK 和 PUT DATA 命令修改 LCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：批准联机（两个发卡行脚本），第一个发卡行脚本命令成功，MAC 正确；
c) 第二个发卡行脚本命令不成功，MAC 错误；
d) 卡片上电 (ATR)；
e) 选择 PBOC 借记/贷记应用；
f) GET PROCESSING OPTIONS 命令；
g) VERIFY 命令；
h) 第一个 GENERATE AC 命令请求 ARQC；
i) EXTERNAL AUTHENTICATE 命令，正确 ARPC；
j) 第二个 GENERATE AC 命令请求 TC；
k) APPLICATION BLOCK 命令，MAC 正确；
l) PUT DATA 命令修改 LCOL，MAC 错误；
m) 交易 3：终端请求 ARQC 后，卡返回 AAC；
n) 卡片上电 (ATR)；
o) 选择 PBOC 借记/贷记应用；
p) GET PROCESSING OPTIONS 命令；
q) VERIFY 命令；
r) 第一个 GENERATE AC 命令请求 ARQC，卡返 AAC。

通过标准：验证交易 3 第一个 GENERATE AC 返回响应，SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 4= ‘28’，CVR= ‘03 84 00 28’ 或 ‘03 80 00 28’（用于未校验 PIN）。

7.27.25 JBCL025-00

测试目的：联机拒绝交易过程中，第二个 GENERATE AC 之后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（如：APPLICATION BLOCK 命令）成功，MAC 正确；第二个发卡行脚本命令（PUT DATA 命令修改 LCOL）不成功，MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。

卡片强制交易 3 拒绝脱机，验证卡片设置 CVR 的第 4 字节位 8-5 为 ‘0010’，验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK、APPLICATION BLOCK 及 PUT DATA 命令修改 LCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：拒绝联机（两个发卡行脚本），第一条发卡行脚本命令成功，MAC 正确；
c) 第二条发卡行脚本命令不成功，MAC 错误；
d) 卡片上电 (ATR)；
e) 选择 PBOC 借记/贷记应用；
f) GET PROCESSING OPTIONS 命令；
g) VERIFY 命令；
h) 第一个 GENERATE AC 命令请求 ARQC；

- i) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- j) 第二个 GENERATE AC 命令请求 AAC;
- k) APPLICATION BLOCK 命令, MAC 正确;
- l) PUT DATA 命令修改 LCOL, MAC 错误;
- m) 交易 3: 终端请求 ARQC 后, 卡片返回 AAC;
- n) 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC, 卡返 AAC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 4= '28', CVR= '03 84 00 28' 或 '03 80 00 28' (用于未校验 PIN)。

7.27.26 JBCL026-00

测试目的: 卡片批准交易脱机, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。

终端请求交易 3 执行联机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0000', 验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准脱机;
- c) 交易 3: 终端请求执行联机;
- d) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '00', CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN)。

7.27.27 JBCL027-00

测试目的: 卡片拒绝交易脱机, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。

终端请求交易 3 执行联机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0000', 验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 拒绝脱机;
- c) 交易 3: 终端请求执行联机;
- d) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;

- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '00', CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN)。

7.27.28 JBCL028-00

测试目的: 联机批准交易过程中, 卡片不执行发卡行脚本命令, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。

终端请求交易 3 执行联机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0000', 验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准联机 (未执行发卡行脚本);
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- i) 第二个 GENERATE AC 命令请求 TC;
- j) 交易 3: 终端请求执行联机;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '00', CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN)。

7.27.29 JBCL029-00

测试目的: 拒绝联机交易过程中, 卡片不执行发卡行脚本命令, 验证卡片不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。

终端请求交易 3 执行联机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0000', 验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 拒绝联机 (未执行发卡行脚本);
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;

- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- i) 第二个 GENERATE AC 命令请求 AAC;
- j) 交易 3: 终端请求执行联机;
- k) 卡片上电(ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '00', CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN)。

7.27.30 JBCL030-00

测试目的: 联机批准交易过程中, 卡片执行一个成功的发卡行脚本命令(如: APPLICATION UNBLOCK 命令), 验证卡片设置“发卡行脚本命令计数器”位为 1 和重置“发卡行脚本失败指示器”位。

终端请求交易 3 执行联机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0001', 验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准联机(成功的发卡行脚本);
- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- i) 第二个 GENERATE AC 命令请求 TC;
- j) APPLICATION UNBLOCK 命令, MAC 正确;
- k) 交易 3: 终端请求执行联机;
- l) 卡片上电(ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '10', CVR= '03 A4 00 10' 或 '03 A0 00 10' (用于未校验 PIN)。

7.27.31 JBCL031-00

测试目的: 交易被联机拒绝过程中, 卡片执行一个成功的发卡行脚本命令(如: APPLICATION

UNBLOCK 命令)，验证卡片设置“发卡行脚本命令计数器”位为 1 和重置“发卡行脚本失败指示器”位。

终端请求交易 3 执行联机，验证卡片设置 CVR 的第 4 字节位 8-5 为‘0001’，验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：拒绝联机（成功的发卡行脚本）；

c) 卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 AAC；

j) APPLICATION UNBLOCK 命令，MAC 正确；

k) 交易 3：终端请求执行联机；

l) 卡片上电(ATR)；

m) 选择 PBOC 借记/贷记应用；

n) GET PROCESSING OPTIONS 命令；

o) VERIFY 命令；

p) 第一个 GENERATE AC 命令请求 ARQC。

通过标准：验证交易 3 第一个 GENERATE AC 返回响应，SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 4=‘10’，CVR=‘03 A4 00 10’或‘03 A0 00 10’（用于未校验 PIN）。

7.27.32 JBCL032-00

测试目的：交易被联机批准过程中，第二个 GENERATE AC 后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（如：APPLICATION UNBLOCK 命令）成功，MAC 正确；第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）不成功，MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。

终端请求交易 3 执行联机，验证卡片设置 CVR 的第 4 字节位 8-5 为‘0010’，验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：批准联机（两个发卡行脚本命令），第一个发卡行脚本命令成功，MAC 正确。第二个发卡行脚本命令不成功，MAC 错误；

c) 卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) 第二个 GENERATE AC 命令请求 TC；

- j) APPLICATION UNBLOCK 命令, MAC 正确;
- k) PUT DATA 命令修改 UCOL, MAC 错误;
- l) 交易 3: 终端请求执行联机;
- m) 卡片上电 (ATR);
- n) 选择 PBOC 借记/贷记应用;
- o) GET PROCESSING OPTIONS 命令;
- p) VERIFY 命令;
- q) 第一个 GENERATE AC 命令请求 ARQC

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '28', CVR= '03 A4 00 28' 或 '03 A0 00 28' (用于未校验 PIN)。

7.27.33 JBCL033-00

测试目的: 交易被联机拒绝过程中, 第二个 GENERATE AC 后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (如: APPLICATION UNBLOCK 命令) 成功, MAC 正确; 第二个发卡行脚本命令 (如: PUT DATA 命令修改 UCOL) 不成功, MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。终端请求交易 3 执行联机, 验证卡片设置 CVR 的第 4 字节位 8-5 为 '0010', 验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 和 PUT DATA 命令修改 UCOL。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 拒绝联机 (两个发卡行脚本), 第一个发卡行脚本成功, MAC 正确。第二个发卡行脚本命令不成功, MAC 错误;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 命令请求 ARQC;
 - h) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
 - i) 第二个 GENERATE AC 命令请求 AAC;
 - j) APPLICATION UNBLOCK 命令, MAC 正确;
 - k) PUT DATA 命令修改 UCOL, MAC 错误;
 - l) 交易 3: 终端请求执行联机;
 - m) 卡片上电 (ATR);
 - n) 选择 PBOC 借记/贷记应用;
 - o) GET PROCESSING OPTIONS 命令;
 - p) VERIFY 命令;
 - q) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: 验证交易 3 第一个 GENERATE AC 返回响应, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '28', CVR= '03 A4 00 28' 或 '03 A0 00 28' (用于未校验 PIN)。

7.27.34 JBCL034-00

测试目的：交易被联机批准过程中，第二个 GENERATE AC 后，终端收到两个发卡行脚本命令。第一个发卡行脚本命令（如：APPLICATION UNBLOCK 命令）成功，MAC 正确；第二个发卡行脚本命令（如：PUT DATA 命令修改 UCOL）不成功，MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。交易 3 批准脱机。交易 4 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 为‘0010’。验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：批准联机（两个发卡行脚本命令），第一个发卡行脚本命令成功，MAC 正确。第二个发卡行脚本命令不成功，MAC 错误；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；
j) APPLICATION UNBLOCK 命令，MAC 正确；
k) PUT DATA 命令修改 UCOL，MAC 错误；
l) 交易 3：批准脱机；
m) 交易 4：批准脱机。

通过标准：验证交易 4 的第一个 GENERATE AC 的响应返回，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘28’，CVR=‘03 94 00 28’ 或 ‘03 90 00 28’（用于未校验 PIN）。

7.27.35 JBCL035-00

测试目的：交易被联机批准过程中，第二个 GENERATE AC 后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（如：APPLICATION UNBLOCK 命令）成功，MAC 正确；第二个发卡行脚本命令（如：PUT DATA 命令修改 UCOL）不成功，MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。交易 3 拒绝脱机。交易 4 批准脱机。验证卡片设置 CVR 的第 4 字节位 8-5 为‘0010’，验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：批准联机（两个发卡行脚本命令）。第一个发卡行脚本命令成功，MAC 正确。第二个发卡行脚本命令不成功，MAC 错误；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；
i) 第二个 GENERATE AC 命令请求 TC；

- i) APPLICATION UNBLOCK 命令, MAC 正确;
- j) PUT DATA 命令修改 UCOL, MAC 错误;
- k) 交易 3: 拒绝脱机;
- l) 交易 4: 批准脱机。

通过标准: 验证交易 4 的第一个 GENERATE AC 的响应返回, SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 4= '28', CVR= '03 94 00 28' 或 '03 90 00 28' (用于未校验 PIN)。

7.27.36 JBCL036-00

测试目的: 交易被联机批准过程中, 第二个 GENERATE AC 后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (如: APPLICATION UNBLOCK 命令) 成功, MAC 正确; 第二个发卡行脚本命令 (如: PUT DATA 命令修改 UCOL) 不成功, MAC 错误。验证卡片设置“发卡行脚本命令计数器”位为 2 和设置“上次交易发卡行脚本处理失败指针”位。交易 3 请求执行联机但终端不能执行联机, 交易 3 拒绝脱机。卡片请求交易 4 执行联机, 因为在先前的交易中已经设置“联机授权指示”位。验证卡片设置 CVR 的第 4 字节位 8-5 为 '0010', 验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准联机 (两个发卡行脚本), 第一个发卡行脚本命令成功, MAC 正确。
- c) 第二个发卡行脚本命令不成功, MAC 错误;
- d) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 正确 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, MAC 正确;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 终端请求执行联机, 但终端不能执行联机。拒绝交易脱机;
- n) 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) 第一个 GENERATE AC 命令请求 AAC, ARC=Z3;
- t) 交易 4: 终端请求 TC 后, 卡片请求交易执行联机;
- u) 卡片上电 (ATR);
- v) 选择 PBOC 借记/贷记应用;
- w) GET PROCESSING OPTIONS 命令;
- x) VERIFY 命令;
- y) 第一个 GENERATE AC 命令请求 TC, 卡片返回 ARQC。

通过标准: 验证交易 4 的第一个 GENERATE AC 的响应返回, SW1 SW2= '9000', CID 位 8-7= '10',

CVR 字节 2 高半字节= ‘A’，CVR 字节 4= ‘28’，CVR= ‘03 A4 80 28’ 或 ‘03 A0 80 28’ （用于未校验 PIN）。

7.27.37 JBCL037-00

测试目的：交易被联机批准过程中，在第二个 GENERATE AC 之前，卡片收到两个发卡行脚本命令。

第一个发卡行脚本命令（如：APPLICATION UNBLOCK 命令）成功，MAC 正确；第二个发卡行脚本命令（如：PUT DATA 命令修改 UCOL）成功，MAC 正确。

交易 3 批准脱机，验证卡片设置 CVR 的第 4 字节位 8-5 为 ‘0000’。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：第二个 GENERATE AC 之前，执行批准联机交易（执行两个发卡行脚本命令）。第一个发卡行脚本命令成功，MAC 正确；第二个发卡行脚本命令成功，MAC 正确；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

i) APPLICATION UNBLOCK 命令，MAC 正确；

j) PUT DATA 命令修改 UCOL，MAC 正确；

k) 第二个 GENERATE AC 命令请求 TC；

l) 交易 3：批准脱机。

通过标准：验证交易 3 的第一个 GENERATE AC 的响应返回，SW1 SW2= ‘9000’，CID 位 8-7= ‘01’，CVR 字节 2 高半字节= ‘9’，CVR 字节 4= ‘00’，CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’ （用于未校验 PIN）。

7.27.38 JBCL038-00

测试目的：交易被联机批准时，在第二个 GENERATE AC 命令后，卡片收到两个发卡行脚本命令。

第一个发卡行脚本命令（APPLICATION UNBLOCK 命令）MAC 正确，执行成功。第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）MAC 错误，执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2，设置“上次交易发卡行脚本处理失败指针”位。

交易 3 是联机批准交易，未执行发卡行认证（发卡行认证是可选的）。交易 4 是脱机批准交易。验证卡片设置 CVR 的第 4 个字节的第 8-5 位为 ‘0000’，验证卡片不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 3，发卡行认证可选，支持 APPLICATION UNBLOCK 和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，执行两个发卡行脚本。第一个发卡行脚本命令成功，MAC 正确。

c) 第二个发卡行脚本命令不成功，MAC 错误；

d) 卡片上电 (ATR)；

e) 选择 PBOC 借记/贷记应用；

f) GET PROCESSING OPTIONS 命令；

- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, 正确的 MAC;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 支持发卡行认证且是可选的, 未执行发卡行认证, 联机批准;
- n) 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) 第二个 GENERATE AC 命令请求 TC;
- t) 交易 4: 脱机批准。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 4= '00', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.27.39 JBCL039-00

测试目的: 交易被联机批准时, 在第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (APPLICATION UNBLOCK 命令) MAC 正确, 执行成功。第二个发卡行脚本命令 (PUT DATA 命令修改 UCOL) MAC 错误, 执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2, 设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机批准交易, 未执行发卡行认证 (发卡行认证是强制执行)。因为前次交易已设置“联机授权指示”位, 卡片请求交易执行联机。验证卡片设置 CVR 的第 4 字节第 8-5 位为 '0010', 验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 联机批准, 执行两个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确;
- c) 第二个发卡行脚本命令不成功, MAC 错误;
- d) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, 正确的 MAC;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 支持发卡行认证且是可选的, 未执行发卡行认证, 联机批准;
- n) 卡片上电 (ATR);

- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) 第二个 GENERATE AC 命令请求 TC;
- t) 交易 4: 终端请求 TC 后, 卡片请求交易执行联机;
- u) 卡片上电 (ATR);
- v) 选择 PBOC 借记/贷记应用;
- w) GET PROCESSING OPTIONS 命令;
- x) VERIFY 命令;
- y) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '28', CVR= '03 A4 88 28' 或 '03 A0 88 28' (用于未校验 PIN)。

7.27.40 JBCL040-00

测试目的: 交易被联机批准时, 在第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (APPLICATION UNBLOCK 命令) MAC 正确, 执行成功。第二个发卡行脚本命令 (PUT DATA 命令修改 UCOL) MAC 错误, 执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2, 设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机批准交易 (发卡行认证执行失败)。由于上次交易设置“联机授权指示”位, 交易 4 中卡片请求执行联机。验证卡片应设置 CVR 的第 4 个字节的第 8-5 位为 '0010', 验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 执行两个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确;

c) 第二个发卡行脚本命令不成功, MAC 错误;

d) 卡片上电 (ATR);

e) 选择 PBOC 借记/贷记应用;

f) GET PROCESSING OPTIONS 命令;

g) VERIFY 命令;

h) 第一个 GENERATE AC 命令请求 ARQC;

i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;

j) 第二个 GENERATE AC 命令请求 TC;

k) APPLICATION UNBLOCK 命令, 正确的 MAC;

l) PUT DATA 命令修改 UCOL, MAC 错误;

m) 交易 3: 发卡行认证执行失败, 联机批准;

n) 卡片上电 (ATR);

o) 选择 PBOC 借记/贷记应用;

p) GET PROCESSING OPTIONS 命令;

q) VERIFY 命令;

r) 第一个 GENERATE AC 命令请求 ARQC;

s) EXTERNAL AUTHENTICATE 命令, 包括错误的 ARPC;

- t) 第二个 GENERATE AC 命令请求 TC;
- u) 交易 4: 终端请求 TC 后, 卡片请求交易执行联机;
- v) 卡片上电 (ATR);
- w) 选择 PBOC 借记/贷记应用;
- x) GET PROCESSING OPTIONS 命令;
- y) VERIFY 命令;
- z) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '28', CVR= '03 A4 88 28' 或 '03 A0 88 28' (用于未校验 PIN)。

7.27.41 JBCL041-00

测试目的: 交易被联机批准时, 在第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (APPLICATION UNBLOCK 命令) MAC 正确, 执行成功。第二个发卡行脚本命令 (PUT DATA 命令修改 UCOL) MAC 错误, 执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2, 设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机批准交易 (发卡行认证执行成功)。交易 4 是脱机批准交易。验证卡片应设置 CVR 的第 4 个字节的第 8-5 位为 '0000', 验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 联机批准, 执行两个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确;
- c) 第二个发卡行脚本命令不成功, MAC 错误;
- d) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, 正确的 MAC;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 发卡行认证执行成功, 联机批准;
- n) 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- t) 第二个 GENERATE AC 命令请求 TC;
- u) 交易 4: 脱机批准。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 4= '00', CVR= '03 94 00 00' 或 '03 90 00

00'（用于未校验 PIN）。

7.27.42 JBCL042-00

测试目的：交易被联机批准时，在第二个 GENERATE AC 命令后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（APPLICATION UNBLOCK 命令）MAC 正确，执行成功。第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）MAC 错误，执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2，设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机拒绝交易，未执行发卡行认证（卡片支持发卡行认证且是可选的）。交易 4 是脱机批准交易。验证卡片应设置 CVR 的第 4 个字节的第 8-5 位为‘0000’，验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 3，发卡行认证可选，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：

- a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
- b) 交易 2：联机批准，执行两个发卡行脚本。第一个发卡行脚本命令成功，MAC 正确；
- c) 第二个发卡行脚本命令不成功，MAC 错误；
- d) 卡片上电（ATR）；
- e) 选择 PBOC 借记/贷记应用；
- f) GET PROCESSING OPTIONS 命令；
- g) VERIFY 命令；
- h) 第一个 GENERATE AC 命令请求 ARQC；
- i) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；
- j) 第二个 GENERATE AC 命令请求 TC；
- k) APPLICATION UNBLOCK 命令，正确的 MAC；
- l) PUT DATA 命令修改 UCOL，MAC 错误；
- m) 交易 3：支持发卡行认证且是可选的，未执行发卡行认证，联机拒绝；
- n) 卡片上电（ATR）；
- o) 选择 PBOC 借记/贷记应用；
- p) GET PROCESSING OPTIONS 命令；
- q) VERIFY 命令；
- r) 第一个 GENERATE AC 命令请求 ARQC；
- s) 第二个 GENERATE AC 命令请求 AAC；
- t) 交易 4：脱机批准。

通过标准：验证交易 4 的第一个 GENERATE AC 返回的数据，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 4=‘00’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.27.43 JBCL043-00

测试目的：交易被联机批准时，在第二个 GENERATE AC 命令后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（APPLICATION UNBLOCK 命令）MAC 正确，执行成功。第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）MAC 错误，执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2，设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机拒绝交易，未执行发卡行认证（卡片支持发卡行认证且是强制执行的）。由于上次交易设置“联机授权指示”位，交易 4 中卡片请求执行联机。验证卡片应设

置 CVR 的第 4 个字节的第 8-5 位为 ‘0010’，验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，执行两个发卡行脚本。第一个发卡行脚本命令成功，MAC 正确；

c) 第二个发卡行脚本命令不成功，MAC 错误；

d) 卡片上电（ATR）；

e) 选择 PBOC 借记/贷记应用；

f) GET PROCESSING OPTIONS 命令；

g) VERIFY 命令；

h) 第一个 GENERATE AC 命令请求 ARQC；

i) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

j) 第二个 GENERATE AC 命令请求 TC；

k) APPLICATION UNBLOCK 命令，正确的 MAC；

l) PUT DATA 命令修改 UCOL，MAC 错误；

m) 交易 3：支持发卡行认证且是强制执行的，未执行发卡行认证，联机拒绝；

n) 卡片上电（ATR）；

o) 选择 PBOC 借记/贷记应用；

p) GET PROCESSING OPTIONS 命令；

q) VERIFY 命令；

r) 第一个 GENERATE AC 命令请求 ARQC；

s) 第二个 GENERATE AC 命令请求 AAC；

t) 交易 4：终端请求 TC 后，卡片请求交易执行联机；

u) 卡片上电（ATR）；

v) 选择 PBOC 借记/贷记应用；

w) GET PROCESSING OPTIONS 命令；

x) VERIFY 命令；

y) 第一个 GENERATE AC 请求 TC，卡片返回 ARQC。

通过标准：验证交易 4 的第一个 GENERATE AC 返回的数据 SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 4= ‘28’，CVR= ‘03 A4 88 28’ 或 ‘03 A0 88 28’（用于未校验 PIN）。

7.27.44 JBCL044-00

测试目的：交易被联机批准时，在第二个 GENERATE AC 命令后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（APPLICATION UNBLOCK 命令）MAC 正确，执行成功。第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）MAC 错误，执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2，设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机拒绝交易（发卡行认证执行未成功）。由于上次交易设置“联机授权指示”位，交易 4 中卡片请求执行联机。验证卡片应设置 CVR 的第 4 个字节的第 8-5 位为 ‘0010’，验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，执行两个发卡行脚本。第一个发卡行脚本命令成功，MAC 正确。

- c) 第二个发卡行脚本命令不成功, MAC 错误;
- d) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, 正确的 MAC;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 支持发卡行认证且是强制执行的, 未执行发卡行认证, 联机拒绝;
- n) 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) EXTERNAL AUTHENTICATE 命令, 包括错误的 ARPC;
- t) 第二个 GENERATE AC 命令请求 AAC;
- u) 交易 4: 终端请求 TC 后, 卡片请求交易执行联机;
- v) 卡片上电 (ATR);
- w) 选择 PBOC 借记/贷记应用;
- x) GET PROCESSING OPTIONS 命令;
- y) VERIFY 命令;
- z) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '28', CVR= '03 A4 88 28' 或 '03 A0 88 28' (用于未校验 PIN)。

7.27.45 JBCL045-00

测试目的: 交易被联机批准时, 在第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (APPLICATION UNBLOCK 命令) MAC 正确, 执行成功。第二个发卡行脚本命令 (PUT DATA 命令修改 UCOL) MAC 错误, 执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2, 设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机拒绝交易 (发卡行认证执行成功)。交易 4 是脱机批准交易。验证卡片应设置 CVR 的第 4 个字节的第 8-5 位为 '0000', 验证卡片不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 联机批准, 执行两个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确。;
c) 第二个发卡行脚本命令不成功, MAC 错误;
d) 卡片上电 (ATR);
e) 选择 PBOC 借记/贷记应用;
f) GET PROCESSING OPTIONS 命令;

- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, 正确的 MAC;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 发卡行认证执行成功, 联机拒绝;
- n) 卡片上电 (ATR);
- i) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- t) 第二个 GENERATE AC 命令请求 AAC;
- u) 交易 4: 脱机批准。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 4= '00', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.27.46 JBCL046-00

测试目的: 交易被联机批准时, 在第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (APPLICATION UNBLOCK 命令) MAC 正确, 执行成功。第二个发卡行脚本命令 (PUT DATA 命令修改 UCOL) MAC 错误, 执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2, 设置“上次交易发卡行脚本处理失败指针”位。交易 3 是脱机批准交易。交易 4 是脱机拒绝交易。验证卡片应设置 CVR 的第 4 个字节的第 8-5 位为 '0010', 验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 联机批准, 执行两个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确;
 - c) 第二个发卡行脚本命令不成功, MAC 错误;
 - d) 卡片上电 (ATR);
 - e) 选择 PBOC 借记/贷记应用;
 - f) GET PROCESSING OPTIONS 命令;
 - g) VERIFY 命令;
 - h) 第一个 GENERATE AC 命令请求 ARQC;
 - i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
 - j) 第二个 GENERATE AC 命令请求 TC;
 - k) APPLICATION UNBLOCK 命令, MAC 正确;
 - l) PUT DATA 命令修改 UCOL, MAC 错误;
 - m) 交易 3: 脱机批准;
 - n) 交易 4: 脱机拒绝。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '00',

CVR 字节 2 高半字节= ‘8’，CVR 字节 4= ‘28’，CVR= ‘03 84 00 28’ 或 ‘03 80 00 28’（用于未校验 PIN）。

7.27.47 JBCL047-00

测试目的：交易被联机批准时，在第二个 GENERATE AC 命令后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（APPLICATION UNBLOCK 命令）MAC 正确，执行成功。第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）MAC 错误，执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2，设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机批准交易（发卡行认证执行未成功）。交易 4 是脱机拒绝交易。验证卡片应设置 CVR 的第 4 个字节的第 8-5 位为 ‘0010’，验证卡片设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，执行两个发卡行脚本。第一个发卡行脚本命令成功，MAC 正确；

c) 第二个发卡行脚本命令不成功，MAC 错误；

d) 卡片上电（ATR）；

e) 选择 PBOC 借记/贷记应用；

f) GET PROCESSING OPTIONS 命令；

g) VERIFY 命令；

h) 第一个 GENERATE AC 命令请求 ARQC；

i) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

j) 第二个 GENERATE AC 命令请求 TC；

k) APPLICATION UNBLOCK 命令，MAC 正确；

l) PUT DATA 命令修改 UCOL，MAC 错误；

m) 交易 3：发卡行认证执行未成功，联机批准；

n) 卡片上电（ATR）；

o) 选择 PBOC 借记/贷记应用；

p) GET PROCESSING OPTIONS 命令；

q) VERIFY 命令；

r) 第一个 GENERATE AC 命令请求 ARQC；

s) EXTERNAL AUTHENTICATE 命令，包括错误的 ARPC；

t) 第二个 GENERATE AC 命令请求 TC；

u) 交易 4：脱机拒绝。

通过标准：验证交易 4 的第一个 GENERATE AC 返回的数据，SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 4= ‘28’，CVR= ‘03 84 88 28’ 或 ‘03 80 88 28’（用于未校验 PIN）。

7.27.48 JBCL048-00

测试目的：交易被联机批准时，在第二个 GENERATE AC 命令后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（APPLICATION UNBLOCK 命令）MAC 正确，执行成功。第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）MAC 错误，执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2，设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机批准交易（发卡行认证执行成功）。交易 4 是脱机拒绝交易。验证卡片

应设置 CVR 的第 4 个字节的第 8-5 位为 ‘0000’，验证卡片不应设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，执行两个发卡行脚本。第一个发卡行脚本命令成功，MAC 正确；

c) 第二个发卡行脚本命令不成功，MAC 错误；

d) 卡片上电（ATR）；

e) 选择 PBOC 借记/贷记应用；

f) GET PROCESSING OPTIONS 命令；

g) VERIFY 命令；

h) 第一个 GENERATE AC 命令请求 ARQC；

i) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

j) 第二个 GENERATE AC 命令请求 TC；

k) APPLICATION UNBLOCK 命令，MAC 正确；

l) PUT DATA 命令修改 UCOL，MAC 错误；

m) 交易 3：发卡行认证执行成功，联机批准；

n) 卡片上电（ATR）；

o) 选择 PBOC 借记/贷记应用；

p) GET PROCESSING OPTIONS 命令；

q) VERIFY 命令；

r) 第一个 GENERATE AC 命令请求 ARQC；

s) EXTERNAL AUTHENTICATE 命令，包括正确的 ARPC；

t) 第二个 GENERATE AC 命令请求 TC；

u) 交易 4：脱机拒绝。

通过标准：验证交易 4 的第一个 GENERATE AC 返回的数据：SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 4= ‘00’，CVR= ‘03 84 00 00’ 或 ‘03 80 00 00’（用于未校验 PIN）。

7.27.49 JBCL049-00

测试目的：交易被联机批准时，在第二个 GENERATE AC 命令后，卡片收到两个发卡行脚本命令。第一个发卡行脚本命令（APPLICATION UNBLOCK 命令）MAC 正确，执行成功。第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）MAC 错误，执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2，设置“上次交易发卡行脚本处理失败指针”位。交易 3 是脱机批准交易。交易 4 终端请求联机。验证卡片应设置 CVR 的第 4 个字节的第 8-5 位为 ‘0010’，验证卡片应设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，执行两个发卡行脚本。第一个发卡行脚本命令成功，MAC 正确；

c) 第二个发卡行脚本命令不成功，MAC 错误；

d) 卡片上电（ATR）；

e) 选择 PBOC 借记/贷记应用；

f) GET PROCESSING OPTIONS 命令；

- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, MAC 正确;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 脱机批准;
- n) 交易 4: 终端请求联机;
- o) 卡片上电 (ATR);
- p) 选择 PBOC 借记/贷记应用;
- q) GET PROCESSING OPTIONS 命令;
- r) VERIFY 命令;
- s) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '28', CVR= '03 A4 00 28' 或 '03 A0 00 28' (用于未校验 PIN)。

7.27.50 JBCL050-00

测试目的: 交易被联机批准时, 在第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (APPLICATION UNBLOCK 命令) MAC 正确, 执行成功。第二个发卡行脚本命令 (PUT DATA 命令修改 UCOL) MAC 错误, 执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2, 设置“上次交易发卡行脚本处理失败指针”位。交易 3 是联机批准交易 (发卡行认证成功)。交易 4 终端请求联机。验证卡片设置 CVR 的第 4 个字节的第 8-5 位为 '0000', 验证卡片应不设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 执行两个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确;

c) 第二个发卡行脚本命令不成功, MAC 错误;

d) 卡片上电 (ATR);

e) 选择 PBOC 借记/贷记应用;

f) GET PROCESSING OPTIONS 命令;

g) VERIFY 命令;

h) 第一个 GENERATE AC 命令请求 ARQC;

i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;

j) 第二个 GENERATE AC 命令请求 TC;

k) APPLICATION UNBLOCK 命令, MAC 正确;

l) PUT DATA 命令修改 UCOL, MAC 错误;

m) 交易 3: 发卡行认证执行成功, 联机批准;

n) 卡片上电 (ATR);

o) 选择 PBOC 借记/贷记应用;

p) GET PROCESSING OPTIONS 命令;

q) VERIFY 命令;

- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- t) 第二个 GENERATE AC 命令请求 TC;
- u) 交易 4: 终端请求联机;
- v) 卡片上电 (ATR);
- w) 选择 PBOC 借记/贷记应用;
- x) GET PROCESSING OPTIONS 命令;
- y) VERIFY 命令;
- z) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: 验证交易 4 的第一个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '00', CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN)。

7.27.51 JBCL051-00

测试目的: 包含安全信息的发卡行脚本命令个数的最大值应反应到“发卡行脚本命令计数器”位, 包括那些安全信息错误的脚本命令。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 执行 15 个发卡行脚本命令, 其中 14 个 MAC 正确, 第 15 个 MAC 错误;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 命令请求 ARQC;

h) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;

i) 第二个 GENERATE AC 命令请求 TC;

j) APPLICATION UNBLOCK 命令, MAC 正确;

k) APPLICATION UNBLOCK 命令, MAC 正确;

l) APPLICATION UNBLOCK 命令, MAC 正确;

m) APPLICATION UNBLOCK 命令, MAC 正确;

n) APPLICATION UNBLOCK 命令, MAC 正确;

o) APPLICATION UNBLOCK 命令, MAC 正确;

p) APPLICATION UNBLOCK 命令, MAC 正确;

q) APPLICATION UNBLOCK 命令, MAC 正确;

r) APPLICATION UNBLOCK 命令, MAC 正确;

s) APPLICATION UNBLOCK 命令, MAC 正确;

t) APPLICATION UNBLOCK 命令, MAC 正确;

u) APPLICATION UNBLOCK 命令, MAC 正确;

v) APPLICATION UNBLOCK 命令, MAC 正确;

w) APPLICATION UNBLOCK 命令, MAC 正确;

x) PUT DATA 命令修改 UCOL, MAC 错误;

y) 交易 3: 脱机批准。

通过标准：交易 2，第一个 GENERATE AC 中 CID= ‘80’，第一个 GENERATE AC 中 CVR= ‘03 A4 00 00’ 或 ‘03 A0 00 00’（用于未校验 PIN），第二个 GENERATE AC 中 CID= ‘40’，第二个 GENERATE AC 中 CVR= ‘03 64 00 00’ 或 ‘03 60 00 00’（用于未校验 PIN），交易 3 的第一个 GENERATE AC，SW1 SW2= ‘9000’，CID= ‘40’，CVR= ‘03 94 00 F8’ 或 ‘03 90 00 F8’（用于未校验 PIN）。

7.27.52 JBCL052-00

测试目的：交易请求执行联机但终端不能执行联机，交易被脱机批准。验证卡片应不设置“发卡行脚本命令计数器”位和“上次交易发卡行脚本处理失败指针”位。

交易 3 是强制联机交易，验证卡片设置 CVR 的第 4 字节第 8-5 位为 ‘0000’，验证卡片应不设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：交易请求执行联机但终端不能执行联机，交易脱机批准；

c) 卡片上电（ATR）；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) 第二个 GENERATE AC 命令请求 TC 且 ARC 为 Y3；

i) 交易 3：终端请求脱机批准，卡片返回 ARQC；

j) 卡片上电（ATR）；

k) 选择 PBOC 借记/贷记应用；

l) GET PROCESSING OPTIONS 命令；

m) VERIFY 命令；

n) 第一个 GENERATE AC 命令请求 TC，卡片返回 ARQC。

通过标准：验证交易 3 的第一个 GENERATE AC 的返回数据，SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 4= ‘00’，CVR= ‘03 A4 80 00’ 或 ‘03 A0 80 00’（用于未校验 PIN）。

7.27.53 JBCL053-00

测试目的：交易被联机批准时，在第二个 GENERATE AC 命令后，卡片收到两个发卡行脚本命令。

第一个发卡行脚本命令（APPLICATION UNBLOCK 命令）MAC 正确，执行成功。第二个发卡行脚本命令（PUT DATA 命令修改 UCOL）MAC 错误，执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2，设置“上次交易发卡行脚本处理失败指针”位。

交易 3 请求联机但终端不能联机，交易 3 是脱机批准交易交易 4 强制联机，验证卡片设置 CVR 的第 4 字节 8-5 位为 ‘0010’，验证卡片设置 CVR 的“上次交易发卡行脚本处理失败指针”位。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准，执行两个发卡行脚本。第一个发卡行脚本命令成功，MAC 正确；

c) 第二个发卡行脚本命令不成功，MAC 错误；

d) 卡片上电（ATR）；

- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, MAC 正确;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 终端请求联机但无法联机, 交易脱机批准;
- n) 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) 第二个 GENERATE AC 命令请求 TC 且 ARC 为 Y3;
- t) 交易 4: 终端请求脱机批准, 卡片返回 ARQC;
- u) 卡片上电 (ATR);
- v) 选择 PBOC 借记/贷记应用;
- w) GET PROCESSING OPTIONS 命令;
- x) VERIFY 命令;
- y) 第一个 GENERATE AC 命令请求 TC, 卡片返回 ARQC。

通过标准: 验证交易 4 的第一个 GENERATE AC 的返回数据, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '28', CVR= '03 A4 80 28' 或 '03 A0 80 28' (用于未校验 PIN)。

7.27.54 JBCL054-00

测试目的: 交易被联机批准时, 在第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (APPLICATION UNBLOCK 命令) MAC 正确, 执行成功。第二个发卡行脚本命令 (PUT DATA 命令修改 UCOL) MAC 错误, 执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2, 设置“上次交易发卡行脚本处理失败指针”位。交易 3 请求联机但终端无法联机, 交易脱机批准。交易 4 是脱机拒绝交易。验证卡片设置 CVR 的第 4 个字节的第 8-5 位为 '0010', 验证卡片应设置 CVR 中的“上次交易发卡行脚本处理失败指针”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 执行两个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确;

c) 第二个发卡行脚本命令不成功, MAC 错误;

d) 卡片上电 (ATR);

e) 选择 PBOC 借记/贷记应用;

f) GET PROCESSING OPTIONS 命令;

g) VERIFY 命令;

h) 第一个 GENERATE AC 命令请求 ARQC;

i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;

- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, 正确的 MAC;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 终端请求联机但无法联机, 交易脱机批准;
- n) 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) 第二个 GENERATE AC 命令请求 TC 且 ARC 为 Y3;
- t) 交易 4: 脱机拒绝。

通过标准: 验证交易 4 的第一个 GENERATE AC 的返回数据, SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 4= '28', CVR= '03 84 80 28' 或 '03 80 80 28' (用于未校验 PIN)。

7.27.55 JBCL055-00

测试目的: 交易被联机批准时, 在第二个 GENERATE AC 命令后, 卡片收到两个发卡行脚本命令。第一个发卡行脚本命令 (APPLICATION UNBLOCK 命令) MAC 正确, 执行成功。第二个发卡行脚本命令 (PUT DATA 命令修改 UCOL) MAC 错误, 执行未成功。验证卡片设置“发卡行脚本命令计数器”位为 2, 设置“上次交易发卡行脚本处理失败指针”位。交易 3 请求联机但终端无法联机, 交易脱机批准。交易 4 终端请求联机。验证卡片设置 CVR 的第 4 个字节的第 8-5 位为 '0010', 验证卡片应设置 CVR 中的“上次交易发卡行脚本处理失败”位。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 联机批准, 执行两个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确;
- c) 第二个发卡行脚本命令不成功, MAC 错误;
- d) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 ARQC;
- i) EXTERNAL AUTHENTICATE 命令, 包括正确的 ARPC;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) APPLICATION UNBLOCK 命令, MAC 正确;
- l) PUT DATA 命令修改 UCOL, MAC 错误;
- m) 交易 3: 终端请求联机但无法联机, 交易脱机批准;
- n) 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 ARQC;
- s) 第二个 GENERATE AC 命令请求 TC 且 ARC 为 Y3;

- t) 交易 4: 终端请求联机;
- u) 卡片上电 (ATR);
- v) 选择 PBOC 借记/贷记应用;
- w) GET PROCESSING OPTIONS 命令;
- x) VERIFY 命令;
- y) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: 验证交易 4 的第一个 GENERATE AC 的返回数据, SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 4= '28', CVR= '03 A4 80 28' 或 '03 A0 80 28' (用于未校验 PIN)。

7.27.56 JBCL056-00

测试目的: 在多个脚本处理过程中, 如果之前的脚本 MAC 错误, 则后续的脚本命令应处理失败, 并推荐返回 6985。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 执行四个发卡行脚本。第一个发卡行脚本命令成功, MAC 正确;

c) 第二个发卡行脚本命令不成功, MAC 错误。

通过标准: 验证交易 2 的第一个脚本的返回数据, SW1 SW2= '9000', 交易 2 的第二个脚本的返回数据, SW1 SW2= '6988', 交易 2 的第三个脚本的返回数据, SW1 SW2= '6985', 交易 2 的第四个脚本的返回数据, SW1 SW2= '6985'。

7.27.57 JBCL057-00

测试目的: 在多个脚本处理过程中, 如果之前的脚本 MAC 错误, 则后续的脚本命令应处理失败, 并推荐返回 6985。

测试条件: 第 9 章中的卡片特征 1, 支持 APPLICATION UNBLOCK 命令和 PUT DATA 命令修改 UCOL。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准, 执行四个发卡行脚本。第一个发卡行脚本命令失败, MAC 不正确; 第二至第四个发卡行脚本命令执行不成功。

通过标准: 验证交易 2 的第一个脚本的返回数据, SW1 SW2= '6988', 交易 2 的第二个脚本的返回数据, SW1 SW2= '6985', 交易 2 的第三个脚本的返回数据, SW1 SW2= '6985', 交易 2 的第四个脚本的返回数据, SW1 SW2= '6985'。

7.28 日志文件(RZWJ)

7.28.1 RZWJ001-00

测试目的: 交易被联机批准应成功记入日志。

测试条件: 第 9 章中的卡片特征 1, 支持交易日志, 新卡。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机批准;

c) 交易 3: 读出所有的日志文件;

d) 卡片上电 (ATR);

e) 选择 PBOC 借记/贷记应用;

f) GET DATA 命令 (日志格式 '9F4F');

g) READ RECORD 根据日志入口读出交易明细文件中所有的记录。

通过标准: 交易 2, AFL 不包含与日志文件入口重合的文件定位, 第一个 GENERATE AC 中 CID='80', 第一个 GENERATE AC 中 CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN), 第二个 GENERATE AC 中 CID= '40', 第二个 GENERATE AC 中 CVR= '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN), 交易 3, 每一个交易明细中仅记录日志格式 (标签 '9F4F') 中指出的数据对象, 内容不包括 AEF 数据模板 (标签 '70'), 记录的个数可能是 2 个, 最近的日志, 记录 1, 含有与交易 2 相关联的数据。

7.28.2 RZWJ002-00

测试目的: 交易被脱机批准应成功记录日志。

测试条件: 第 9 章中的卡片特征 1, 支持交易日志。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 脱机批准;

c) 交易 3: 读出所有的日志文件;

d) 卡片上电 (ATR);

e) 选择 PBOC 借记/贷记应用;

f) GET DATA 命令, 取得日志格式 ('9F4F')。

g) READ RECORD 根据日志入口读出交易明细文件中所有的记录。

通过标准: 交易 2, AFL 不包含与日志文件入口重合的文件定位, 第一个 GENERATE AC 中 CID='40', 第一个 GENERATE AC 中 CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。交易 3, 每一个交易明细中仅记录日志格式 (标签 '9F4F') 中指出的数据对象, 内容不包括 AEF 数据模板 (标签 '70'), 记录的交易个数可能是 4 个, 最近的日志, 记录 1, 含有与交易 2 相关联的数据。

7.28.3 RZWJ003-00

测试目的: 不能执行联机, 脱机批准交易应能成功记录日志。

测试条件: 第 9 章中的卡片特征 1, 支持交易记录日志。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 批准交易不能执行联机;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 请求 ARQC;

h) 第二个 GENERATE AC 请求 TC, ARC=Y3;

i) 交易 3: 读出所有的日志文件;

j) 卡片上电 (ATR);

k) 选择 PBOC 借记/贷记应用;

l) GET DATA 命令, 取得日志格式 ('9F4F');

m) READ RECORD 根据日志入口读出交易明细文件中所有的记录。

通过标准: 交易 2, AFL 不包含与日志文件入口重合的文件定位, 第一个 GENERATE AC, CID='80', 第一个 GENERATE AC, CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN), 第二个 GENERATE AC, CID= '40', 第二个 GENERATE AC, CVR= '03 65 00 00' 或 '03

61 00 00' (用于未校验 PIN), 交易 3, 每一个交易明细中仅记录日志格式 (标签 '9F4F') 中指出的数据对象, 内容不包括 AEF 数据模板 (标签 '70'), 记录的交易个数可能是 6, 最近的日志, 记录 1, 含有与交易 2 相关联的数据。

7.28.4 RZWJ004-00

测试目的: 应用锁定后, 交易日志文件仍然可用。

测试条件: 第 9 章中的卡片特征 1, 支持交易记录日志。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机交易拒绝, 锁定应用;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 请求 ARQC;

h) EXTERNAL AUTHENTICATE 命令;

i) 第二个 GENERATE AC 请求 AAC;

j) APPLICATION BLOCK 命令, MAC 正确;

k) 交易 3: 脱机拒绝, 应用解锁;

l) 卡片上电 (ATR);

m) 选择 PBOC 借记/贷记应用;

n) GET DATA 命令, 取得日志格式 ('9F4F');

o) GET PROCESSING OPTIONS 命令;

p) READ RECORD 命令, 读出所有的日志入口文件, 文件是指 SFI N 的记录 1—X (其中 N 是在入口文件中由 SFI 定义的。X 是指在入口文件中定义的记录的最多数量);

q) 执行 VERIFY 命令, 第一个 GENERATE AC 请求 AAC;

r) EXTERNAL AUTHENTICATE 命令;

s) APPLICATION UNBLOCK 命令, MAC 正确。

通过标准: 交易 2, 第一个 GENERATE AC 中 CID= '80', 第一个 GENERATE AC 中 CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN), 第二个 GENERATE AC 中 CID= '00', 第二个 GENERATE AC 中 CVR= '03 24 00 00' 或 '03 20 00 00' (用于未校验 PIN), APPLICATION BLOCK 命令, SW1 SW2= '9000', 交易 3, SELECT 命令, SW1 SW2= '6283', GET DATA 的响应是一串数据对象的标签和长度, 日志入口文件定义的 SFI 中的所有记录都应成功读出, 最近的日志, RECORD 1, 不包含与交易 2 相关的数据, 第一个 GENERATE AC, CID= '00', 第一个 GENERATE AC, CVR= '03 84 00 10' 或 '03 80 00 10' (用于未校验 PIN), APPLICATION UNBLOCK 命令, SW1 SW2= '9000',

7.28.5 RZWJ005-00

测试目的: 脱机批准交易成功记入日志文件。

测试条件: 第 9 章中的卡片特征 3, 支持交易记录日志, 新卡。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 脱机批准;

c) 交易 3: 读出所有的日志入口文件;

d) 卡片上电 (ATR);

- e) 选择 PBOC 借记/贷记应用;
- f) GET DATA 命令, 取得日志格式 (标签 ‘9F4F’);
- g) READ RECORD 命令, 读出所有的日志入口文件, 文件是指 SFI N 的记录 1—X (其中 N 是在入口文件中由 SFI 定义的; X 是指在入口文件中定义的记录的最多数量)。

通过标准: 交易 2, AFL 不包含一个与入口日志文件相符合的入口, SFI N 记录 1 到 X, 第一个 GENERATE AC 中 CID= ‘40’, 第一个 GENERATE AC 中 CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’ (用于未校验 PIN), 交易 3, 每一个入口日志记录由日志格式 (标签 ‘9F4F’) 决定, 内容只包括数据对象, 不包括 AEF 数据数据模板 (标签 ‘70’), 记录的交易个数可能是 2 个, 最近的日志文件, 记录 1, 包含与交易 2 相关的数据,

7.28.6 RZWJ006-00

测试目的: 不能执行联机, 但批准交易脱机, 应成功记录日志文件。

测试条件: 第 9 章中的卡片特征 3, 支持交易记录日志。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 批准交易不能执行联机;
- c) 卡片上电 (ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) 第二个 GENERATE AC 请求 TC, ARC=Y3;
- i) 交易 3—读出所有的日志入口文件;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET DATA 命令, 取得日志格式 (标签 ‘9F4F’);
- m) READ RECORD 命令, 读出所有的日志入口文件, 文件是指 SFI N 的记录 1—X (其中 N 是在入口文件中由 SFI 定义的; X 是指在入口文件中定义的记录的最多数量)。

通过标准: 交易 2, AFL 不包含一个与入口日志文件相符合的入口, SFI N 记录 X, 第一个 GENERATE AC 中 CID= ‘80’, 第一个 GENERATE A 中 CVR= ‘03 A4 00 00’ 或 ‘03 A0 00 00’ (用于未校验 PIN), 第二个 GENERATE AC 中 CID= ‘40’, 第二个 GENERATE AC, CVR= ‘03 65 00 00’ 或 ‘03 61 00 00’ (用于未校验 PIN), 交易 3, 每一个入口日志记录由日志格式 (标签 ‘9F4F’) 决定, 内容只包括数据对象, 不包括 AEF 数据数据模板 (标签 ‘70’), 记录的交易个数可能是 4 个, 最近的日志文件, 记录 1, 包含与交易 2 相关的数据。

7.28.7 RZWJ007-00

测试目的: 脱机拒绝交易不记入日志文件。

测试条件: 第 9 章中的卡片特征 1, 支持交易记录日志文件。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机拒绝;
- c) 交易 3: 读出所有的日志入口文件;
- d) 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;

f) GET DATA 命令, 取得日志格式 (标签 '9F4F') ;

g) READ RECORD 命令, 读出所有的日志入口文件, 文件是指 SFI N 的记录 1—X (其中 N 是在入口文件中由 SFI 定义的; X 是指在入口文件中定义的记录的最多数量)。

通过标准: 交易 2, AFL 不包含一个与入口日志文件相符合的入口, SFI N 记录 1 到 X, 第一个 GENERATE AC 中 CID= '00', 第一个 GENERATE AC 中 CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN), 交易 3, 每一个入口日志记录由日志格式 (标签 '9F4F') 决定, 内容只包括数据对象, 不包括 AEF 数据数据模板 (标签 '70'), 记录的交易个数可能是 5, 最近的日志文件, 记录 1, 不包含来自交易 2 的数据。

7.28.8 RZWJ008-00

测试目的: 联机交易拒绝不记入日志文件。

测试条件: 第 9 章中的卡片特征 1, 支持交易记录日志。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 联机拒绝;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) 执行 VERIFY 命令;

g) 第一个 GENERATE AC 请求 ARQC;

h) EXTERNAL AUTHENTICATE 命令;

i) 第二个 GENERATE AC 请求 AAC;

j) 交易 3: 读出所有的日志入口文件;

k) 卡片上电 (ATR);

l) 选择 PBOC 借记/贷记应用;

m) GET DATA 命令, 取得日志格式 (标签 '9F4F') ;

n) READ RECORD 命令, 读出所有的日志入口文件, 文件是指 SFI N 的记录 1—X (其中 N 是在入口文件中由 SFI 定义的。X 是指在入口文件中定义的记录的最多数量)。

通过标准: 交易 2, AFL 不包含一个与入口日志文件相符合的入口, SFI N 记录 1 到 X, 第一个 GENERATE AC 中 CID= '80', 第一个 GENERATE AC 中 CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN), 第二个 GENERATE AC 中 CID= '00', 第二个 GENERATE AC 中 CVR= '03 24 00 00' 或 '03 20 00 00' (用于未校验 PIN), 交易 3, 每一个入口日志记录由日志格式 (标签 '9F4F') 决定, 内容只包括数据对象, 不包括 AEF 数据数据模板 (标签 '70'), 记录的交易个数可能是 6, 最近的日志文件, 记录 1, 不包含来自交易 2 的数据。

7.28.9 RZWJ009-00

测试目的: 不能执行联机, 拒绝脱机交易不记入日志文件。

测试条件: 第 9 章中的卡片特征 1, 支持交易记录日志。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 拒绝交易不能执行联机;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

- f) VERIFY 命令;
- g) 第一个 GENERATE AC 请求 ARQC;
- h) 第二个 GENERATE AC 请求 AAC, ARC=Z3;
- i) 交易 3: 读出所有的日志入口文件;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET DATA 命令, 取得日志格式 (标签 '9F4F');
- m) READ RECORD 命令, 读出所有的日志入口文件, 文件是指 SFI N 的记录 1—X (其中 N 是在入口文件中由 SFI 定义的; X 是指在入口文件中定义的记录的最多数量)。

通过标准: 交易 2, AFL 不包含一个与入口日志文件相符合的入口, SFI N 记录 1 到 X, 第一个 GENERATE AC 中 CID= '80', 第一个 GENERATE AC 中 CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN), 第二个 GENERATE AC 中 CID= '00', 第二个 GENERATE AC 中 CVR= '03 25 00 00' 或 '03 21 00 00' (用于未校验 PIN), 交易 3, 每一个入口日志记录由日志格式 (标签 '9F4F') 决定, 内容只包括数据对象, 不包括 AEF 数据数据模板 (标签 '70'), 记录的交易个数可能是 7, 最近的日志文件, 记录 1, 不包含来自交易 2 的数据。

7.28.10 RZWJ010-00

测试目的: 循环文件的结构决定支持交易日志文件的最大数量 (在日志入口中指定)。

测试条件: 第 9 章中的卡片特征 1, 支持交易记录日志, 新卡。

- 测试流程:
- a) 交易 1 至 X: 发卡行认证成功, 联机交易批准后, ATC 增加自 0 至 X;
 - b) 交易 X+1: 读出所有的日志入口文件 (其中 X 是指在日志入口中指定的记录的最大个数);
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET DATA 命令, 取得日志格式 (标签 '9F4F');
 - f) READ RECORD 命令, 读出所有的日志入口文件, 文件是指 SFI N 的记录 1—X (其中 N 是在入口文件中由 SFI 定义的; X 是指在入口文件中定义的记录的最大数量);
 - g) 交易 X+2: 发卡行认证成功, 联机批准交易, ATC 由 X 增加为 X+1;
 - h) 交易 X+3: 读出所有的日志入口文件;
 - i) 卡片上电 (ATR);
 - j) 选择 PBOC 借记/贷记应用;
 - k) GET DATA 命令, 取得日志格式 (标签 '9F4F');
 - l) READ RECORD 命令, 读出所有的日志入口文件, 文件是指 SFI N 的记录 1—X (其中 N 是在入口文件中由 SFI 定义的; X 是指在入口文件中定义的记录的最大数量)。

通过标准: 交易 X+1, 每一个入口日志记录由日志格式 (标签 '9F4F') 决定, 内容只包括数据对象, 不包括 AEF 数据数据模板 (标签 '70'), 记录个数 X, 最近的日志文件, 记录 1, 包含来自交易 X 的数据, 交易 X+3, 每一个入口日志记录由日志格式 (标签 '9F4F') 决定, 内容只包括数据对象, 不包括 AEF 数据数据模板 (标签 '70'), 记录个数为 X, 最近的日志文件, 记录 1, 包含来自交易 X+2 的数据。

7.28.11 RZWJ011-00

测试目的: 联机现金批准交易成功记入日志文件。

测试条件：第9章中的卡片特征1，支持交易记录日志文件，所有交易的交易类型为‘01’。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：联机批准；

c) 交易3：读出所有的日志入口文件；

d) 卡片上电（ATR）；

e) 选择PBOC借记/贷记应用；

f) GET DATA 命令，取得日志格式（标签‘9F4F’）；

g) READ RECORD 命令，读出所有的日志入口文件，文件是指SFI N的记录1—X（其中N是在入口文件中由SFI定义的；X是指在入口文件中定义的记录的最大数量）。

通过标准：交易2，AFL不包含一个与入口日志文件相符合的入口，SFI N记录1到X，第一个GENERATE AC中CID=‘80’，第一个GENERATE AC中CVR=‘03 A4 00 00’或‘03 A0 00 00’（用于未校验PIN），第二个GENERATE AC中CID=‘40’，第二个GENERATE AC中CVR=‘03 64 00 00’或‘03 60 00 00’（用于未校验PIN），交易3，每一个入口日志记录由日志格式（标签‘9F4F’）决定，内容只包括数据对象，不包括AEF数据数据模板（标签‘70’），最近的日志文件，记录1，包含与交易2相关联的数据。

7.29 新卡(XINK)

7.29.1 XINK001-00

测试目的：卡片未设置ADA中的“如果是新卡，联机交易”位，验证新卡批准交易脱机。

LOATC为‘0000’，验证卡片设置CVR中的“新卡”位。

测试条件：第9章中的卡片特征10，卡片行为分析支持新卡检查。

测试流程：a) 交易1：脱机批准。

通过标准：SW1 SW2=‘9000’，CID位8-7=‘01’，CVR字节2高半字节=‘9’，CVR字节3位5=‘1’，CVR=‘03 94 10 00’或‘03 90 10 00’（用于未校验PIN）。

7.29.2 XINK002-00

测试目的：卡片设置ADA中的“如果是新卡，联机交易”位，验证新卡请求交易执行联机。

LOATC为‘0000’，验证卡片设置CVR中的“新卡”位。

测试条件：第9章中的卡片特征1，卡片行为分析支持新卡检查。

测试流程：a) 交易1：终端在第一个GENERATE AC命令中请求脱机批准，卡片返回要求联机；

b) 卡片上电（ATR）；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个GENERATE AC命令请求TC，卡片应返回ARQC。

通过标准：SW1 SW2=‘9000’，CID位8-7=‘10’，CVR字节2高半字节=‘A’，CVR字节3位5=‘1’，CVR=‘03 A4 10 00’或‘03 A0 10 00’（用于未校验PIN）。

7.29.3 XINK003-00

测试目的：卡片设置ADA中的“如果是新卡，联机交易”位，由于卡片不支持发卡行认证而未执行发卡行认证，交易批准联机成功后，验证新卡更新LOATC。

验证卡片批准下次交易脱机（不设置CVR的“新卡”位）。

测试条件：第9章中的卡片特征2，卡片行为分析支持新卡检查。

测试流程：a) 交易1：终端在第一个 GENERATE AC 命令中请求 TC 后，卡片返回请求联机。批准联机交易，由于卡片不支持发卡行认证，未执行发卡行认证；

b) 卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；

g) 第二个 GENERATE AC 命令请求 TC；

h) 交易2：脱机批准。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '01'，CVR 字节 2 高半字节= '9'，CVR 字节 3 位 5= '0'，CVR= '03 94 00 00' 或 '03 90 00 00'（用于未校验 PIN）。

7.29.4 XINK004-00

测试目的：卡片未设置 ADA 中的“如果是新卡，联机交易”位，由于卡片不支持发卡行认证而未执行发卡行认证，交易批准联机成功后，验证新卡更新 LOATC。

验证卡片批准下次交易脱机（不设置 CVR 的“新卡”位）。

测试条件：第9章中的卡片特征9，卡片行为分析支持新卡检查。

测试流程：a) 交易1：终端在第一个 GENERATE AC 命令中请求联机。由于卡片不支持发卡行认证，联机交易未执行发卡行认证；

b) 卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) 第二个 GENERATE AC 命令请求 TC；

h) 交易2：脱机批准。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '01'，CVR 字节 2 高半字节= '9'，CVR 字节 3 位 5= '0'，CVR= '03 94 00 00' 或 '03 90 00 00'（用于未校验 PIN）。

7.29.5 XINK005-00

测试目的：卡片设置 ADA 中的“如果是新卡，联机交易”位，卡片不支持发卡行认证，未执行发卡行认证，交易联机拒绝，验证卡片应不更新 LOATC。

验证卡片请求下次交易联机，设置 CVR 中的“新卡”位。

测试条件：第9章中的卡片特征2，卡片行为分析支持新卡检查。

测试流程：a) 交易1：终端在第一个 GENERATE AC 命令中请求 TC 后，卡片返回请求联机。由于卡片不支持发卡行认证，未执行发卡行认证。交易被联机拒绝；

b) 卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) 第二个 GENERATE AC 命令请求 AAC；

- h) 交易 2: 终端在第一个 GENERATE AC 命令请求 TC 后, 卡片要求联机;
- i) 卡片上电 (ATR);
- j) 选择 PBOC 借记/贷记应用;
- k) GET PROCESSING OPTIONS 命令;
- l) VERIFY 命令;
- m) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 5= '1', CVR= '03 A4 10 00' 或 '03 A0 10 00' (用于未校验 PIN)。

7.29.6 XINK006-00

测试目的: 卡片未设置 ADA 中的“如果是新卡, 联机交易”位, 由于卡片不支持发卡行认证, 未执行发卡行认证, 交易联机拒绝, 验证卡片应更新 LOATC。

验证卡片批准交易脱机时, 设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 9, 卡片行为分析支持新卡检查。

- 测试流程: a) 交易 1: 终端在第一个 GENERATE AC 命令中请求联机 (ARQC)。卡片不支持发卡行认证, 未执行发卡行认证, 交易联机拒绝;
- b) 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 命令请求 TC. 卡片应返回 ARQC;
 - g) 第二个 GENERATE AC 命令请求 AAC;
 - h) 交易 2: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 5= '1', CVR= '03 94 10 00' 或 '03 90 10 00' (用于未校验 PIN)。

7.29.7 XINK007-00

测试目的: 卡片设置 ADA 中的“如果是新卡, 联机交易”位, 发卡行认证执行成功, 交易批准联机, 验证卡片应更新 LOATC。

验证卡片批准随后的两笔脱机交易, 卡片未设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查且卡片支持发卡行认证。

- 测试流程: a) 交易 1: 终端在第一个 GENERATE AC 命令中请求 TC, 卡片返回联机请求;
- b) 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSINGF OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 终端在第一个 GENERATE AC 命令中请求 TC, 卡片应返回 ARQC;
 - g) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 正确;
 - h) 第二个 GENERATE AC 命令请求 TC;
 - i) 交易 2: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 5= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.29.8 XINK008-00

测试目的：卡片不设置 ADA 中的“如果是新卡，联机交易”位，发卡行认证执行成功，交易联机批准。验证卡片应更新 LOATC。

验证卡片批准下次交易脱机，卡片未设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 10，卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程：a) 交易 1：发卡行认证成功，交易联机批准；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 执行 EXTERNAL AUTHENTICATE 命令，ARPC 正确；
h) 第二个 GENERATE AC 命令请求 TC；
i) 交易 2：脱机批准。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 5=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.29.9 XINK009-00

测试目的：卡片设置 ADA 中的“如果是新卡，联机交易”位，发卡行认证成功后，交易联机拒绝，验证卡片应不更新 LOATC。

验证卡片请求下笔交易联机且应设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 1，卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程：a) 交易 1：终端在第一个 GENERATE AC 命令中请求 TC 后，卡片返回请求联机。交易联机拒绝；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；
g) 第二个 GENERATE AC 命令请求 AAC；
h) 交易 2：终端在第一个 GENERATE AC 命令中请求 TC 后，卡片返回请求联机；
i) 卡片上电 (ATR)；
j) 选择 PBOC 借记/贷记应用；
k) GET PROCESSING OPTIONS 命令；
l) VERIFY 命令；
m) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 5=‘1’，CVR=‘03 A4 10 00’或‘03 A0 10 00’（用于未校验 PIN）。

7.29.10 XINK010-00

测试目的：卡片未设置 ADA 中的“如果是新卡，联机交易”位，发卡行认证成功后，交易联机拒绝，验证卡片应不更新 LOATC。

验证卡片批准下次交易脱机，应设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 10，卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程: a) 交易 1: 发卡行认证成功, 交易联机拒绝;

- b) 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 正确;
- h) 第二个 GENERATE AC 命令请求 AAC;
- i) 交易 2: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 5= '1', CVR= '03 94 10 00' 或 '03 90 10 00' (用于未校验 PIN)。

7.29.11 XINK011-00

测试目的: 卡片设置 ADA 中的“如果是新卡, 联机交易”位, 发卡行认证未执行成功, 联机交易执行成功, 验证卡片应不更新 LOATC。

验证卡片请求下次交易联机且应设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程: a) 交易 1: 终端在第一个 GENERATE AC 命令中请求 TC 后, 卡片返回请求联机。发卡行认证执行未成功, 交易联机批准;

- b) 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) 执行校验 VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC;
- g) 执行 EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) 交易 2: 终端在第一个 GENERATE AC 命令请求 TC 后, 卡片要求联机;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 5= '1', CVR= '03 A4 98 00' 或 '03 A0 98 00' (用于未校验 PIN)。

7.29.12 XINK012-00

测试目的: 卡片未设置 ADA 中的“如果是新卡, 联机交易”位, 发卡行认证未执行成功, 联机交易执行成功, 验证卡片应不更新 LOATC。

前次交易发卡行认证失败, 验证卡片请求下次交易联机且应设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 10, 卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程: a) 交易 1: 发卡行认证未成功, 交易联机批准;

- b) 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;

- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 执行 EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- h) 第二个 GENERATE AC 命令请求 TC;
- i) 交易 2: 终端在第一个 GENERATE AC 命令中请求 TC 后, 卡片要求联机;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 5= '1', CVR= '03 A4 98 00' 或 '03 A0 98 00' (用于未校验 PIN)。

7.29.13 XINK013-00

测试目的: 卡片设置 ADA 中的“如果是新卡, 联机交易”位, 发卡行认证未执行成功, 交易联机拒绝, 验证卡片应不更新 LOATC。验证卡片请求下次交易联机且应设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程: a) 交易 1: 终端在第一个 GENERATE AC 请求 TC 后, 卡片要求联机。发卡行认证未成功, 交易联机拒绝;

- b) 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 TC, 卡片返回 ARQC;
- g) 执行 EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- h) 第二个 GENERATE AC 命令请求 AAC;
- i) 交易 2: 终端在第一个 GENERATE AC 命令中请求 TC 后, 卡片要求联机;
- j) 卡片上电 (ATR);
- k) 选择 PBOC 借记/贷记应用;
- l) GET PROCESSING OPTIONS 命令;
- m) VERIFY 命令;
- n) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 5= '1', CVR= '03 A4 98 00' 或 '03 A0 98 00' (用于未校验 PIN)。

7.29.14 XINK014-00

测试目的: 卡片未设置 ADA 中的“如果是新卡, 联机交易”位, 发卡行认证未成功, 交易联机拒绝, 验证卡片应不更新 LOATC。上次交易发卡行认证失败, 验证卡片请求下次交易联机且应设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 10, 卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程: a) 交易 1: 发卡行认证未成功, 交易联机拒绝;

- b) 卡片上电(ATR);
- c) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) 执行 EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- i) 第二个 GENERATE AC 请求 AAC;
- j) 交易 2: 终端在第一个 GENERATE AC 命令请求 TC 后, 卡片要求联机;
- k) 卡片上电(ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 5 = '1', CVR= '03 A4 98 00' 或 '03 A0 98 00' (用于未校验 PIN)。

7.29.15 XINK015-00

测试目的: 卡片设置 ADA 中的“如果是新卡, 联机交易”位, 卡片支持发卡行认证且是强制性执行的, 未执行发卡行认证, 交易联机拒绝, 验证新卡应不更新 LOATC。验证卡片请求下次交易应联机且应设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查, 卡片支持发卡行认证且是强制性执行的。

测试流程: a) 交易 1: 终端在第一个 GENERATE AC 命令中请求 TC 后, 卡片返回请求联机。由于卡片支持发卡行认证且是强制性执行的, 未执行发卡行认证, 交易联机拒绝;

- b) 卡片上电(ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC;
- g) 第二个 GENERATE AC 命令请求 AAC;
- h) 交易 2: 终端在第一个 GENERATE AC 命令中请求 TC, 卡片要求联机;
- i) 卡片上电(ATR);
- j) 选择 PBOC 借记/贷记应用;
- k) GET PROCESSING OPTIONS 命令;
- l) VERIFY 命令;
- m) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 5= '1', CVR= '03 A4 98 00' 或 '03 A0 98 00' (用于未校验 PIN)。

7.29.16 XINK016-00

测试目的: 卡片未设置 ADA 中的“如果是新卡, 联机交易”位, 卡片支持发卡行认证且是强制性执行的, 未执行发卡行认证, 交易联机拒绝, 验证新卡应不更新 LOATC。上次交易中发卡行认证未执行, 验证卡片请求下次交易联机且应设置 CVR 中的“新卡”位。

测试条件：第9章中的卡片特征10，卡片行为分析支持新卡检查，卡片支持发卡行认证且是强制性执行的。

测试流程：a) 交易1：由于卡片支持发卡行认证且是强制性执行的，未执行发卡行认证，交易联机拒绝；

b) 卡片上电(ATR)；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) 第二个 GENERATE AC 命令请求 AAC；

h) 交易2：终端在第一个 GENERATE AC 命令中请求 TC，卡片要求联机；

i) 卡片上电(ATR)；

j) 选择PBOC借记/贷记应用；

k) GET PROCESSING OPTIONS 命令；

l) VERIFY 命令；

m) 第一个 GENERATE AC 请求 TC，卡片返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 5=‘1’，CVR=‘03 A4 98 00’或‘03 A0 98 00’（用于未校验 PIN）。

7.29.17 XINK017-00

测试目的：卡片设置 ADA 中的“如果是新卡，联机交易”位，卡片支持发卡行认证且是强制性执行的，但未执行发卡行认证，交易联机批准，验证卡片应不更新 LOATC。验证请求卡片下次交易联机且应设置 CVR 中的“新卡”位。

测试条件：第9章中的卡片特征1，卡片行为分析支持新卡检查，卡片支持发卡行认证且是强制性执行的。

测试流程：a) 交易1：终端在第一个 GENERATE AC 命令中请求 TC 后，卡片返回请求联机。卡片支持发卡行认证且是强制性执行的，未执行发卡行认证，交易联机批准；

b) 卡片上电(ATR)；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；

g) 第二个 GENERATE AC 命令请求 TC；

h) 交易2：终端在第一个 GENERATE AC 命令请求 TC 后，卡片要求联机；

i) 卡片上电(ATR)；

j) 选择PBOC借记/贷记应用；

k) GET PROCESSING OPTIONS 命令；

l) VERIFY 命令；

m) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 5=‘1’。CVR=‘03 A4 98 00’或‘03 A0 98 00’（用于未校验 PIN）。

7.29.18 XINK018-00

测试目的：卡片设置 ADA 中的“如果是新卡，联机交易”位，卡片支持发卡行认证且是强制性执行的，但未执行发卡行认证，交易联机批准，验证卡片应不更新 LOATC。上次交易未执行发卡行认证，验证卡片请求下次交易联机且应设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 10，卡片行为分析支持新卡检查，支持发卡行认证且是强制执行的。

测试流程：a) 交易 1：卡片支持发卡行认证且是强制性的，未执行发卡行认证，交易联批准；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 第二个 GENERATE AC 命令请求 TC；
h) 交易 2：第一个 GENERATE AC 终端请求 TC，卡片返回请求联机；
i) 卡片上电 (ATR)；
j) 选择 PBOC 借记/贷记应用；
k) GET PROCESSING OPTIONS 命令；
l) VERIFY 命令；
m) 第一个 GENERATE AC 命令请求 TC，卡片返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 5=‘1’，CVR=‘03 A4 98 00’ 或 ‘03 A0 98 00’（用于未校验 PIN）。

7.29.19 XINK019-00

测试目的：卡片设置 ADA 中的“如果是新卡，联机交易”位，卡片支持发卡行认证且是可选的，未执行发卡行认证，交易联机拒绝，验证卡片应不更新 LOATC。验证卡片请求下次交易联机，设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 3，卡片行为分析支持新卡检查，卡片支持发卡行认证且是可选的。

测试流程：a) 交易 1：终端在第一个 GENERATE AC 命令中请求 TC，卡片返回联机请求，卡片支持发卡行认证且是可选的，未执行发卡行认证，联机交易失败；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSINGF OPTIONS 命令；
e) VERIFY 命令；
f) 终端在第一个 GENERATE AC 命令中请求 TC，卡片应返回 ARQC；
g) 第二个 GENERATE AC 命令请求 AAC；
h) 交易 2：终端在第一个 GENERATE AC 命令中请求 TC，卡片返回联机请求；
i) 卡片上电 (ATR)；
j) 选择 PBOC 借记/贷记应用；
k) GET PROCESSINGF OPTIONS 命令；
l) VERIFY 命令；
m) 终端在第一个 GENERATE AC 命令中请求 TC，卡片应返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 5=‘1’，CVR=‘03 A4 10 00’ 或 ‘03 A0 10 00’（用于未校验 PIN）。

7.29.20 XINK020-00

测试目的：卡片未设置 ADA 中的“如果是新卡，联机交易”位，卡片支持发卡行认证且是可选的，未执行发卡行认证，交易联机拒绝，验证卡片应不更新 LOATC。验证卡片批准下笔交易脱机，设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 8，卡片行为分析支持新卡检查，卡片支持发卡行认证且是可选的。

测试流程：a) 交易 1：卡片支持发卡行认证且是可选的，未执行发卡行认证，联机交易失败；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 第二个 GENERATE AC 命令请求 AAC；
h) 交易 2：脱机批准。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 5=‘1’，CVR=‘03 94 10 00’或‘03 90 10 00’（用于未校验 PIN）。

7.29.21 XINK021-00

测试目的：卡片设置 ADA 中的“如果是新卡，联机交易”位，卡片支持发卡行认证且是可选的，未执行发卡行认证，交易联机批准，验证卡片应更新 LOATC。验证卡片批准下笔交易脱机，不设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 3，卡片行为分析支持新卡检查，卡片支持发卡行认证且是可选的。

测试流程：a) 交易 1：终端在第一个 GENERATE AC 命令中请求 TC 后，卡片返回请求联机。卡片支持发卡行认证且是可选的，未执行发卡行认证，联机交易成功；
b) 卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；
g) 第二个 GENERATE AC 命令请求 TC；
h) 交易 2：脱机批准。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 5=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.29.22 XINK022-00

测试目的：卡片未设置 ADA 中的“如果是新卡，联机交易”位，卡片支持发卡行认证且是可选的，未执行发卡行认证，交易联机批准，验证卡片应更新 LOATC。
验证卡片批准下笔交易脱机，不设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 8，卡片行为分析支持新卡检查，卡片支持发卡行认证且是可选的。

测试流程：a) 交易 1：卡片支持发卡行认证且是可选的，未执行发卡行认证，交易联机成功，卡片上电 (ATR)；

- b) 选择 PBOC 借记/贷记应用;
- c) GET PROCESSING OPTIONS 命令;
- d) VERIFY 命令;
- e) 第一个 GENERATE AC 命令请求 ARQC;
- f) 第二个 GENERATE AC 命令请求 TC;
- g) 交易 2: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 5= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.29.23 XINK023-00

测试目的: 卡片未设置 ADA 中的“如果是新卡, 联机交易”位, 交易脱机拒绝, 验证卡片应设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 10, 卡片行为分析支持新卡检查。

测试流程: a) 交易 1: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '1', CVR= '03 84 10 00' 或 '03 80 10 00' (用于未校验 PIN)。

7.29.24 XINK024-00

测试目的: 卡片设置 ADA 中的“如果是新卡, 联机交易”位, 交易脱机拒绝, 验证卡片应设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查。

测试流程: a) 交易 1: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '1', CVR= '03 84 10 00' 或 '03 80 10 00' (用于未校验 PIN)。

7.29.25 XINK025-00

测试目的: 无论新卡是否设置 ADA 中的“如果是新卡, 联机交易”位, 卡片由于不支持发卡行认证而未执行发卡行认证, 交易联机批准, 验证卡片应更新 LOATC。交易脱机拒绝, 验证卡片应不设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 9, 卡片行为分析支持新卡检查。

测试流程: a) 交易 1: 终端在第一个 GENERATE AC 命令中请求 ARQC。由于卡片不支持发卡行认证而未执行发卡行认证, 交易联机批准;

- b) 卡片上电(ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 ARQC;
- g) 第二个 GENERATE AC 命令请求 TC;
- h) 交易 2: 脱机拒绝;
- i) 卡片上电(ATR);
- j) 选择 PBOC 借记/贷记应用;
- k) GET PROCESSING OPTIONS 命令;
- l) VERIFY 命令;

m) 第一个 GENERATE AC 命令请求 AAC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.29.26 XINK026-00

测试目的: 无论新卡是否设置 ADA 中的“如果是新卡, 联机交易”位, 卡片由于不支持发卡行认证而未执行发卡行认证, 交易联机拒绝, 验证卡片应更新 LOATC。交易脱机拒绝, 验证卡片应设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 9, 卡片行为分析支持新卡检查。

测试流程: a) 交易 1: 终端在第一个 GENERATE AC 命令中请求 ARQC, 由于卡片不支持发卡行认证而未执行发卡行认证, 交易联机拒绝;

b) 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 ARQC;

g) 第二个 GENERATE AC 命令请求 AAC;

h) 交易 2: 脱机拒绝;

i) 卡片上电 (ATR);

j) 选择 PBOC 借记/贷记应用;

k) GET PROCESSING OPTIONS 命令;

l) VERIFY 命令;

m) 第一个 GENERATE AC 命令请求 AAC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '1', CVR= '03 84 10 00' 或 '03 80 10 00' (用于未校验 PIN)。

7.29.27 XINK027-00

测试目的: 无论新卡是否设置 ADA 中的“如果是新卡, 联机交易”位, 发卡行认证执行成功, 联机交易执行成功, 验证卡片应更新 LOATC。下笔交易脱机拒绝, 验证卡片应不设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功, 交易联机批准;

b) 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 ARQC;

g) 执行 EXTERNAL AUTHENTICATE 命令, ARPC 正确;

h) 第二个 GENERATE AC 命令请求 TC;

i) 交易 2: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.29.28 XINK028-00

测试目的：无论新卡是否设置 ADA 中的“如果是新卡，联机交易”位，发卡行认证执行成功，联机交易执行失败，验证卡片不应更新 LOATC。下次交易脱机拒绝，验证卡片设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 1，卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程：a) 交易 1：发卡行认证成功，联机拒绝；

b) 卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，正确 ARPC；

h) 第二个 GENERATE AC 命令请求 AAC；

i) 交易 2：脱机拒绝；

j) 卡片上电(ATR)；

k) 选择 PBOC 借记/贷记应用；

l) GET PROCESSING OPTIONS 命令；

m) VERIFY 命令；

n) 第一个 GENERATE AC 命令请求 ARQC。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 3 位 5= ‘1’，CVR= ‘03 84 10 00’ 或 ‘03 80 10 00’（用于未校验 PIN）。

7.29.29 XINK029-00

测试目的：无论新卡是否设置 ADA 中的“如果是新卡，联机交易”位，发卡行认证未执行成功，联机交易执行成功，验证卡片不应更新 LOATC。下次交易脱机拒绝，验证卡片设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 1，卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程：a) 交易 1：联机批准，发卡行认证失败；

b) 卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；

h) 第二个 GENERATE AC 命令请求 TC；

i) 交易 2：脱机拒绝。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 3 位 5= ‘1’，CVR= ‘03 84 98 00’ 或 ‘03 80 98 00’（用于未校验 PIN）。

7.29.30 XINK030-00

测试目的：无论新卡是否设置 ADA 中的“如果是新卡，联机交易”位，发卡行认证未执行成功，联机交易执行失败，验证卡片不应更新 LOATC。下次交易脱机拒绝，验证卡片设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 1，卡片行为分析支持新卡检查且卡片支持发卡行认证。

测试流程: a) 交易 1: 发卡行认证失败, 联机拒绝;
b) 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第一个 GENERATE AC 命令请求 ARQC;
g) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
h) 第二个 GENERATE AC 命令请求 AAC;
i) 交易 2: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '1', CVR= '03 84 98 00' 或 '03 80 98 00' (用于未校验 PIN)。

7.29.31 XINK031-00

测试目的: 无论新卡是否设置 ADA 中的“如果是新卡, 联机交易”位, 卡片支持发卡行认证且是强制性执行的, 但未执行发卡行认证, 联机交易执行成功, 验证卡片不应更新 LOATC。下次交易脱机拒绝, 验证卡片设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查且卡片支持发卡行认证且是强制性执行的。

测试流程: a) 交易 1: 卡片支持发卡行认证且是强制性执行的, 未执行发卡行认证, 联机完成;
b) 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第一个 GENERATE AC 命令请求 ARQC;
g) 第二个 GENERATE AC 命令请求 TC;
h) 交易 2: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '1', CVR= '03 84 98 00' 或 '03 80 98 00' (用于未校验 PIN)。

7.29.32 XINK032-00

测试目的: 无论新卡是否设置 ADA 中的“如果是新卡, 联机交易”位, 卡片支持发卡行认证且是强制性执行的, 未执行发卡行认证, 联机交易执行失败, 验证卡片不应更新 LOATC。下次交易脱机拒绝, 验证卡片设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查且卡片支持发卡行认证且是强制性执行的。

测试流程: a) 交易 1: 卡片支持发卡行认证且是强制性执行的, 未执行发卡行认证, 联机拒绝;
b) 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第一个 GENERATE AC 命令请求 ARQC;
g) 第二个 GENERATE AC 命令请求 AAC;
h) 交易 2: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '1', CVR= '03 84 98 00' 或 '03 80 98 00' (用于未校验 PIN)。

7.29.33 XINK033-00

测试目的: 无论新卡是否设置 ADA 中的“如果是新卡, 联机交易”位, 卡片支持发卡行认证且是可选的, 未执行发卡行认证, 联机交易执行成功, 验证卡片应更新 LOATC。下次交易脱机拒绝, 验证卡片设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 3, 卡片行为分析支持新卡检查且卡片支持发卡行认证且是可选的。

测试流程: a) 交易 1: 卡片支持发卡行认证且是可选的, 未执行发卡行认证, 联机批准;
b) 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第一个 GENERATE AC 命令请求 ARQC;
g) 第二个 GENERATE AC 命令请求 TC;
h) 交易 2: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.29.34 XINK034-00

测试目的: 无论新卡是否设置 ADA 中的“如果是新卡, 联机交易”位, 卡片支持发卡行认证且是可选的, 未执行发卡行认证, 联机交易执行失败, 验证卡片应不更新 LOATC。下次交易脱机拒绝, 验证卡片设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 3, 卡片行为分析支持新卡检查且卡片支持发卡行认证且是可选的。

测试流程: a) 交易 1: 卡片支持发卡行认证且是可选的, 未执行发卡行认证, 联机拒绝;
b) 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第一个 GENERATE AC 命令请求 ARQC;
g) 第二个 GENERATE AC 命令请求 AAC;
h) 交易 2: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 5= '1', CVR= '03 84 10 00' 或 '03 80 10 00' (用于未校验 PIN)。

7.29.35 XINK035-00

测试目的: 卡片未设置 ADA 中的“如果是新卡, 联机交易”位, 验证新卡批准第一笔交易脱机。下笔交易中验证 LOATC 应为 '0000', 验证卡片应设置 CVR 中的“新卡”位 (LCOL=03)。

测试条件: 第 9 章中的卡片特征 10, 卡片行为分析支持新卡检查。

测试流程: a) 交易 1: 脱机批准;
b) 交易 2: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 5= '1', CVR= '03 94 10 00' 或 '03 90 10 00' (用于未校验 PIN)。

7.29.36 XINK036-00

测试目的: 卡片未设置 ADA 中的“如果是新卡, 联机交易”位, 验证新卡批准第一笔交易脱机。验证后续两笔脱机批准交易的 LOATC 为 '0000', 验证卡片设置 CVR 中的“新卡”位。LOATC 未更新, 第四笔交易时验证卡片应设置 CVR 中的“新卡”位。由于频度检查超限, 卡片请求第 4 笔交易联机 (LCOL 设为 3)。

测试条件: 第 9 章中的卡片特征 10, 卡片行为分析支持新卡检查且频度检查支持检查连续脱机交易次数下限。

测试流程: a) 交易 1: 脱机批准;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 终端在第一个 GENERATE AC 命令中请求 TC, 卡片返 ARQC;
e) 卡片上电 (ATR);
f) 选择 PBOC 借记/贷记应用;
g) GET PROCESSING OPTIONS 命令;
h) VERIFY 命令;
i) 第一个 GENERATE AC 命令请求 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 5= '1', CVR= '03 A4 30 00' 或 '03 A0 30 00' (用于未校验 PIN)。

7.29.37 XINK037-00

测试目的: 卡片设置 ADA 中的“如果是新卡, 联机交易”位, 交易脱机拒绝, 验证卡片不应更新 LOATC。验证卡片请求下次交易联机且设置 CVR 中的“新卡”位。

测试条件: 第 9 章中的卡片特征 1, 卡片行为分析支持新卡检查。

测试流程: a) 交易 1: 终端在第一个 GENERATE AC 中请求 TC, 卡片返 ARQC。终端无法联机, 交易脱机拒绝;

b) 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC;
g) 第二个 GENERATE AC 命令请求 AAC 且 ARC 为 Z3;
h) 交易 2: 终端在第一个 GENERATE AC 命令中请求 TC, 卡片返回 ARQC;
i) 卡片上电 (ATR);
j) 选择 PBOC 借记/贷记应用;
k) GET PROCESSING OPTIONS 命令;
l) VERIFY 命令;
m) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 5= '1', CVR= '03 A4 90 00' 或 '03 A0 90 00' (用于未校验 PIN)。

7.29.38 XINK038-00

测试目的：卡片设置 ADA 中的“如果是新卡，联机交易”位，卡片请求交易联机后，将卡片从终端中拔出，验证卡片不应更新 LOATC。验证卡片请求下次交易联机且设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 1，卡片行为分析支持新卡检查。

测试流程：a) 交易 1：终端在第一个 GENERATE AC 中请求 TC，卡片返 ARQC。在第一个 GENERATE AC 命令中返回联机后，将卡片从终端拔出；

b) 卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；

g) 交易 2：终端在第一个 GENERATE AC 命令中请求 TC，卡片返回要求联机；

h) 卡片上电 (ATR)；

i) 选择 PBOC 借记/贷记应用；

j) GET PROCESSING OPTIONS 命令；

k) VERIFY 命令；

l) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '10'，CVR 字节 2 高半字节= 'A'，CVR 字节 3 位 5= '1'，CVR= '03 A4 90 00' 或 '03 A0 90 00'（用于未校验 PIN）。

7.29.39 XINK039-00

测试目的：卡片未设置 ADA 中的“如果是新卡，联机交易”位，交易脱机拒绝，验证新卡不应更新 LOATC。由于上笔交易联机授权位置位，验证卡片请求下次交易联机且设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 10，卡片行为分析支持新卡检查，卡片支持发卡行认证且是强制性执行的。

测试流程：a) 交易 1：终端请求联机，而无法联机，脱机拒绝；

b) 卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；

g) 第二个 GENERATE AC 命令请求 AAC 且 ARC 为 Z3；

h) 交易 2：终端在第一个 GENERATE AC 命令中请求 TC，卡片要求联机；

i) 卡片上电 (ATR)；

j) 选择 PBOC 借记/贷记应用；

k) GET PROCESSING OPTIONS 命令；

l) VERIFY 命令；

m) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '10'，CVR 字节 2 高半字节= 'A'，CVR 字节 3 位 5= '1'，CVR= '03 A4 90 00' 或 '03 A0 90 00'（用于未校验 PIN）。

7.29.40 XINK040-00

测试目的：卡片未设置 ADA 中的“如果是新卡，联机交易”位，当终端请求交易联机后，将卡片从终端拔出，验证卡片不应更新 LOATC。由于上笔交易联机授权位置位，验证卡片请求下次交易联机且设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 10，卡片行为分析支持新卡检查。

测试流程：a) 交易 1：终端请求联机，在第一个 GENERATE AC 命令中返回联机后，将卡片拔出；

b) 卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；

g) 交易 2：终端在第一个 GENERATE AC 命令中请求 TC，卡片返回 ARQC；

h) 卡片上电(ATR)；

i) 选择 PBOC 借记/贷记应用；

j) GET PROCESSING OPTIONS 命令；

k) VERIFY 命令；

l) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 5=‘1’，CVR=‘03 A4 90 00’或‘03 A0 90 00’（用于未校验 PIN）。

7.29.41 XINK041-00

测试目的：卡片设置 ADA 中的“如果是新卡，联机交易”位，终端脱机交易执行成功，验证卡片不应更新 LOATC。验证卡片请求下笔交易联机且设置 CVR 中的“新卡”位。

测试条件：第 9 章中的卡片特征 1，卡片行为分析支持新卡检查。

测试流程：a) 交易 1：终端第一个 GENERATE AC 请求 TC，卡片返 ARQC。终端无法联机，脱机批准；

b) 卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；

g) 第二个 GENERATE AC 命令请求 TC 且 ARC 为 Y3；

h) 交易 2：终端在第一个 GENERATE AC 命令中请求 TC，卡片返回要求联机；

i) 卡片上电(ATR)；

j) 选择 PBOC 借记/贷记应用；

k) GET PROCESSING OPTIONS 命令；

l) VERIFY 命令；

m) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID=‘80’，CVR=‘03 A4 90 00’或‘03 A0 90 00’（用于未校验 PIN）。

7.29.42 XINK042-00

测试目的：卡片未设置 ADA 中的“如果是新卡，联机交易”位，交易脱机批准，验证新卡不更新 LOATC。验证卡片强制下笔交易联机且设置 CVR 中的“新卡”位。

测试条件：第9章中的卡片特征10，卡片行为分析支持新卡检查。

测试流程：a) 交易1：终端在请求联机，而终端无法联机，脱机批准；

- b) 卡片上电(ATR)；
- c) 选择PBOC借记/贷记应用；
- d) GET PROCESSING OPTIONS 命令；
- e) VERIFY 命令；
- f) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC；
- g) 第二个 GENERATE AC 命令请求 TC 且 ARC 为 Y3；
- h) 交易2：终端请求脱机批准，卡片返回 ARQC；
- i) 卡片上电(ATR)；
- j) 选择PBOC借记/贷记应用；
- k) GET PROCESSING OPTIONS 命令；
- l) VERIFY 命令；
- m) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '10'，CVR 字节 2 高半字节= 'A'，CVR 字节 3 位 5= '1'，CVR= '03 A4 90 00' 或 '03 A0 90 00'（用于未校验 PIN）。

7.30 脱机交易 (LXJY)

7.30.1 LXJY001-00

测试目的：卡片未设置 ADA 中的“如果交易拒绝，生成通知”位，脱机交易拒绝，验证卡片应不设置 CID 中的“需要通知”位。

测试条件：第9章中的卡片特征1。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：脱机拒绝。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '00'，CID 位 4= '0'，CVR 字节 2 高半字节= '8'，CID= '00'，CVR= '03 84 00 00' 或 '03 80 00 00'（用于未校验 PIN）。

7.30.2 LXJY002-00

测试目的：卡片设置 ADA 中的“如果交易拒绝，生成通知”位，脱机交易拒绝，验证卡片应设置 CID 中的“需要通知”位。

测试条件：第9章中的卡片特征4，支持卡片设置 ADA 中的“如果交易拒绝，生成通知”位。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：脱机拒绝。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '00'，CID 位 4= '1'，CVR 字节 2 高半字节= '8'，CID= '08'，CVR= '03 84 00 00' 或 '03 80 00 00'（用于未校验 PIN）。

7.30.3 LXJY003-00

测试目的：当 PIN 尝试次数超限且卡片设置 ADA 中的“如果 PIN 在本次交易中已锁而且交易拒绝，生成通知”位时，脱机拒绝交易，验证卡片设置“需要通知”位且设置 CID 的位 3-位 1 为 '010'。

测试条件：第9章中的卡片特征4，PIN 尝试次数超限，交易失败且生成脱机通知位。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：PIN 尝试次数超限，脱机拒绝；

- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令, 错误的 PIN;
- g) VERIFY 命令, 错误的 PIN;
- h) VERIFY 命令, 错误的 PIN;
- i) 终端在第一个 GENERATE AC 命令中请求 AAC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CID 位 4= '1', CID 位 3-1= '010', CVR 字节 2 高半字节= '8', CID= '0A', CVR= '03 86 40 00' 或 '03 80 40 00' (用于未校验 PIN)。

7.30.4 LXJY004-00

测试目的: 当 PIN 尝试次数超限且卡片未设置 ADA 中的“如果 PIN 在本次交易中已锁而且交易拒绝, 生成通知”位时, 脱机拒绝交易, 验证卡片不设置“需要通知”位, 设置 CID 的位 3-位 1 为 '010'。

测试条件: 第 9 章中的卡片特征 1, 卡片支持脱机 PIN 和 PIN UNBLOCK 命令。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: PIN 尝试次数超限, 脱机拒绝;
- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令, 错误的 PIN;
- g) VERIFY 命令, 错误的 PIN;
- h) VERIFY 命令, 错误的 PIN;
- i) 终端在第一个 GENERATE AC 命令中请求 AAC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CID 位 4= '0', CID 位 3-1= '000', CVR 字节 2 高半字节= '8', CID= '00'。CVR= '03 86 40 00' 或 '03 80 40 00' (用于未校验 PIN)。

7.30.5 LXJY005-00

测试目的: 前次交易 PIN 尝试次数超限, 卡片强制拒绝交易, 验证使用 PIN CHANGE/UNBLOCK 命令可将 PIN 成功解锁。

测试条件: 第 9 章中的卡片特征 1, 卡片支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: PIN 尝试次数超限, 脱机拒绝;
- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令, 错误的 PIN;
- g) VERIFY 命令, 错误的 PIN;
- h) VERIFY 命令, 错误的 PIN;
- i) 终端在第一个 GENERATE AC 命令中请求 AAC;
- j) 交易 3: 脱机拒绝后, 使用 PIN UNBLOCK 命令解锁成功;

- k) 卡片上电(ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) 终端在第一个 GENERATE AC 命令中请求 ARQC, 卡片返回 AAC;
- o) EXTERNAL AUTHENTICATE 命令;
- p) 使用正确的 MAC 执行 PIN CHANGE/UNBLOCK 命令。

通过标准: 交易 2, 第一个 VERIFY SW1 SW2= '63C2', 第二个 VERIFY SW1 SW2= '63C1', 第三个 VERIFY SW1 SW2= '63C0', CID= '00', CVR= '03 86 40 00', 交易 3, CID= '00', CVR= '03 80 40 00', PIN CHANGE/UNBLOCK SW1 SW2 = '9000'。

7.30.6 LXJY006-00

测试目的: 前次交易 PIN 尝试次数超限, 卡片强制拒绝交易, 在不进行外部认证的情况下, 使用 PIN CHANGE/UNBLOCK 命令可将 PIN 成功解锁。

测试条件: 第 9 章中的卡片特征 1, 卡片支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: PIN 尝试次数超限, 脱机拒绝;
- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令, 错误的 PIN;
- g) VERIFY 命令, 错误的 PIN;
- h) VERIFY 命令, 错误的 PIN;
- i) 终端在第一个 GENERATE AC 命令中请求 AAC;
- j) 交易 3: 脱机拒绝后, 使用 PIN UNBLOCK 命令解锁成功;
- k) 卡片上电(ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) 终端在第一个 GENERATE AC 命令中请求 ARQC, 卡片返回 AAC;
- o) EXTERNAL AUTHENTICATE 命令;
- p) 使用正确的 MAC 执行 PIN CHANGE/UNBLOCK 命令;
- q) 交易 4: 脱机拒绝后, 使用 PIN UNBLOCK 命令解锁成功;
- r) 卡片上电(ATR);
- s) 选择 PBOC 借记/贷记应用;
- t) GET PROCESSING OPTIONS 命令;
- u) 终端在第一个 GENERATE AC 命令中请求 ARQC, 卡片返回 AAC;
- v) 使用正确的 MAC 执行 PIN CHANGE/UNBLOCK 命令。

通过标准: 交易 2, 第一个 VERIFY SW1 SW2= '63C2', 第二个 VERIFY SW1 SW2= '63C1', 第三个 VERIFY SW1 SW2= '63C0', CID= '00', CVR= '03 86 40 00', 交易 3, CID= '00', CVR= '03 80 40 00', 外部认证命令响应为非 9000, PIN CHANGE/UNBLOCK SW1 SW2 = '6985', 交易 4, CID= '00', CVR= '03 80 40 00', PIN CHANGE/UNBLOCK SW1 SW2 = '9000'。

7.31 联机完成(LJWC)

7.31.1 LJWC001-00

测试目的：发卡行认证不支持，未执行发卡行认证的情况下，卡片联机拒绝交易，验证卡片应不设置 CVR 的“联机授权后，发卡行认证没有执行”位。

测试条件：第 9 章中的卡片特征 2。

测试流程：a) 交易 1：不执行发卡行认证的联机批准交易，以复位卡片中的计数器；
b) 交易 2：未执行发卡行认证，联机交易拒绝；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) 第二个 GENERATE AC 命令请求 AAC。

通过标准：验证交易 2 中卡片返回的数据，SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘2’，CVR 字节 3 位 3= ‘0’，CVR= ‘03 24 00 00’ 或 ‘03 20 00 00’（用于未校验 PIN）。

7.31.2 LJWC002-00

测试目的：发卡行认证支持，无论是强制执行还是可选，均未执行发卡行认证，卡片拒绝联机交易，验证卡片应设置 CVR 中的“联机授权后，发卡行认证没有执行”位。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：a) 交易 1：执行发卡行认证的联机批准交易，以复位卡片中的计数器；
b) 交易 2：未执行发卡行认证，联机交易拒绝；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) 第二个 GENERATE AC 命令请求 AAC。

通过标准：验证交易 2 中卡片返回的数据，SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘2’，CVR 字节 3 位 3= ‘1’，CVR= ‘03 24 04 00’ 或 ‘03 20 04 00’（用于未校验 PIN）。

7.31.3 LJWC003-00

测试目的：发卡行认证成功，但发卡行认证数据中的 ARC 不是 00、10 或 11，终端请求拒绝交易联机，验证卡片不设置 CVR 中的“发卡行认证执行但失败”位和“联机授权后，发卡行认证没有执行”位。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：发卡行认证成功，ARC 不是 00、10 或 11，联机交易拒绝；
c) 卡片上电 (ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；

- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3035' ;
- i) 第二个 GENERATE AC 命令请求 AAC。

通过标准: 验证交易 2 中卡片返回的数据, SW1 SW2= '9000' , CID 位 8-7= '00' , CVR 字节 2 高半字节= '2' , CVR 字节 2 位 4= '0' , CVR 字节 3 位 3= '0' , CVR= '03 24 00 00' 或 '03 20 00 00' (用于未校验 PIN)。

7.31.4 LJWC004-00

测试目的: 发卡行认证失败, 但发卡行认证数据中的 ARC 不是 00、10 或 11, 终端请求拒绝交易联机, 验证卡片设置 CVR 中的“发卡行认证执行但失败”位, 不设置“联机授权后, 发卡行认证没有执行”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 发卡行认证成功, ARC 不是 00、10 或 11, 联机交易拒绝;

c) 卡片上电(ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 命令请求 ARQC;

h) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3038' ;

i) 第二个 GENERATE AC 命令请求 AAC。

通过标准: 验证交易 2 中卡片返回的数据, 第一个 GENERATE AC, CID= '80' , 第一个 GENERATE AC, CVR= '03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN), 第二个 GENERATE AC, CID= '00' , 第二个 GENERATE AC, CVR= '03 2C 00 00' 或 '03 28 00 00' (用于未校验 PIN)。

7.31.5 LJWC005-00

测试目的: 卡片不支持发卡行认证, 未执行发卡行认证, 卡片批准联机交易, 验证卡片应不设置 CVR 中的“联机授权后, 发卡行认证没有执行”位。

测试条件: 第 9 章中的卡片特征 2。

测试流程: a) 交易 1: 不执行发卡行认证的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 未执行发卡行认证批准交易联机;

c) 卡片上电(ATR);

d) 选择 PBOC 借记/贷记应用;

e) GET PROCESSING OPTIONS 命令;

f) VERIFY 命令;

g) 第一个 GENERATE AC 命令请求 ARQC;

h) 第二个 GENERATE AC 命令请求 TC。

通过标准: 验证交易 2 中卡片返回的数据, SW1 SW2= '9000' , CID 位 8-7= '01' , CVR 字节 2 高半字节= '6' , CVR 字节 3 位 3= '0' , CVR= '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN)。

7.31.6 LJWC006-00

测试目的：卡片支持发卡行认证且是可选的，未执行发卡行认证，卡片批准交易联机，验证卡片应设置 CVR 中的“联机授权后，发卡行认证没有执行”位。

测试条件：第 9 章中的卡片特征 3，支持发卡行认证且是可选的。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：未执行发卡行认证，批准联机交易；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) 第二个 GENERATE AC 命令请求 TC。

通过标准：验证交易 2 中卡片返回的数据，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘6’，CVR 字节 3 位 3=‘1’，CVR=‘03 64 04 00’或‘03 60 00 00’（用于未校验 PIN）。

7.31.7 LJWC007-00

测试目的：卡片支持发卡行认证且强制执行，未执行发卡行认证，终端请求批准交易联机。

当未设置 ADA 中的“如果发卡行认证必备但没有收到 APRC，拒绝交易”位，验证卡片批准交易。

验证卡片应不设置“需要通知”位，CID 的位 3-1 应不设置为‘011’。

验证卡片设置 CVR 中的“联机授权后，发卡行认证没有执行”位。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证且强制执行。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：未执行发卡行认证，批准联机交易；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) 第二个 GENERATE AC 命令请求 TC。

通过标准：验证交易 2 中卡片返回的数据，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CID 位 4=‘0’，CID 位 3-1=‘000’，CVR 字节 2 高半字节=‘6’，CVR 字节 3 位 3=‘1’，CVR=‘03 64 04 00’或‘03 60 04 00’（用于未校验 PIN）。

7.31.8 LJWC008-00

测试目的：发卡行认证成功，终端请求批准联机交易。发卡行认证数据中的 ARC 为 00、01、02、10 和 11。卡片批准交易联机。验证卡片应不设置 CVR 中的“联机授权后，发卡行认证没有执行”位。验证卡片应不设置 CVR 中的“发卡行认证执行但失败”位。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：发卡行认证成功，联机批准，ARC 为 00；

c) 卡片上电 (ATR)；

d) 选择 PBOC 借记/贷记应用；

- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3030' ;
- i) 第二个 GENERATE AC 命令请求 TC;
- j) 交易 3: 发卡行认证成功, 联机批准, ARC 为 01;
- k) 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3031' ;
- q) 第二个 GENERATE AC 命令请求 TC;
- r) 交易 4: 发卡行认证成功, 联机批准, ARC 为 02;
- s) 卡片上电 (ATR);
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) VERIFY 命令;
- w) 第一个 GENERATE AC 命令请求 ARQC;
- x) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3032' ;
- y) 第二个 GENERATE AC 命令请求 TC;
- z) 交易 5: 发卡行认证成功, 联机交易批准, ARC 为 10;
- aa) 卡片上电 (ATR);
- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) VERIFY 命令;
- ae) 第一个 GENERATE AC 命令请求 ARQC;
- af) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3130' ;
- ag) 第二个 GENERATE AC 命令请求 TC;
- ah) 交易 6: 发卡行认证成功, 联机批准, ARC 为 11;
- ai) 卡片上电 (ATR);
- aj) 选择 PBOC 借记/贷记应用;
- ak) GET PROCESSING OPTIONS 命令;
- al) VERIFY 命令;
- am) 第一个 GENERATE AC 命令请求 ARQC;
- an) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3131' ;
- ao) 第二个 GENERATE AC 命令请求 TC。

通过标准: 验证交易 2 到交易 6 第二个 GENERATE AC 中的返回数据, SW1 SW2= '9000' , CID 位 8-7= '01' , CVR 字节 2 高半字节= '6' , CVR 字节 3 位 3= '0' , CVR= '03 64 00 00' 或 '03 60 00 00' (用于未校验 PIN)。

7.31.9 LJWC009-00

测试目的: 发卡行认证执行成功后, 终端请求批准交易联机。发卡行认证数据中的 ARC 不是 00、

01、02、10 和 11。卡片强制拒绝交易联机。验证卡片应不设置 CVR 中的“联机授权后，发卡行认证没有执行”位。验证卡片应不设置 CVR 中的“发卡行认证执行但失败”位。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：发卡行认证执行成功，ARC 为‘0544’，卡片拒绝交易联机；
c) 卡片上电(ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，正确的 ARPC，ARC 为‘0544’；
i) 第二个 GENERATE AC 命令请求 TC，卡片应返回 AAC。

通过标准：验证交易 2 中卡片返回的数据，第一个 GENERATE AC，CID=‘80’，第一个 GENERATE AC，CVR=‘03 A4 00 00’或‘03 A0 00 00’（用于未校验 PIN），第二个 GENERATE AC，CID=‘00’，第二个 GENERATE AC，CVR=‘03 24 00 00’或‘03 20 00 00’（用于未校验 PIN）。

7.31.10 LJWC010-00

测试目的：发卡行认证执行失败，终端请求批准交易联机。发卡行认证数据中的 ARC 为 00、01、02、10 和 11。当设置 ADA 中的“如果发卡行认证执行但失败，拒绝交易”位，未设置“如果因为发卡行认证失败或没有执行导致交易拒绝，生成通知”位时，验证卡片强制交易拒绝联机。验证卡片设置 CVR 中的“发卡行认证执行但失败”位。验证卡片不设置“需要通知”位，不设置 CID 位 3-1 为‘011’。

测试条件：第 9 章中的卡片特征 12，支持发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：发卡行认证执行未成功，ARC 为 00，卡片强制拒绝交易；
c) 卡片上电(ATR)；
d) 选择 PBOC 借记/贷记应用；
e) GET PROCESSING OPTIONS 命令；
f) VERIFY 命令；
g) 第一个 GENERATE AC 命令请求 ARQC；
h) EXTERNAL AUTHENTICATE 命令，错误的 ARPC，ARC 为‘3030’；
i) 第二个 GENERATE AC 命令请求 TC，卡片应返回 AAC；
j) 交易 3：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
k) 交易 4：发卡行认证执行未成功，ARC 为 01，卡片强制拒绝交易；
l) 卡片上电(ATR)；
m) 选择 PBOC 借记/贷记应用；
n) GET PROCESSING OPTIONS 命令；
o) VERIFY 命令；
p) 第一个 GENERATE AC 命令请求 ARQC；
q) EXTERNAL AUTHENTICATE 命令，错误的 ARPC，ARC 为‘3031’；
r) 第二个 GENERATE AC 命令请求 TC，卡片应返回 AAC；

- s) 交易 5: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- t) 交易 6: 发卡行认证执行未成功, ARC 为 02, 卡片强制拒绝交易;
- u) 卡片上电 (ATR);
- v) 选择 PBOC 借记/贷记应用;
- w) GET PROCESSING OPTIONS 命令;
- x) VERIFY 命令;
- y) 第一个 GENERATE AC 命令请求 ARQC;
- z) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 ‘3032’;
- aa) 第二个 GENERATE AC 命令请求 TC, 卡片应返回 AAC;
- ab) 交易 7: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- ac) 交易 8: 发卡行认证执行未成功, ARC 为 10, 卡片强制拒绝交易;
- ad) 卡片上电 (ATR);
- ae) 选择 PBOC 借记/贷记应用;
- af) GET PROCESSING OPTIONS 命令;
- ag) VERIFY 命令;
- ah) 第一个 GENERATE AC 命令请求 ARQC;
- ai) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 ‘3130’;
- aj) 第二个 GENERATE AC 命令请求 TC, 卡片应返回 AAC;
- ak) 交易 9: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- al) 交易 10: 发卡行认证执行未成功, ARC 为 11, 卡片强制拒绝交易;
- am) 卡片上电 (ATR);
- an) 选择 PBOC 借记/贷记应用;
- ao) GET PROCESSING OPTIONS 命令;
- ap) VERIFY 命令;
- aq) 第一个 GENERATE AC 命令请求 ARQC;
- ar) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 ‘3131’;
- as) 第二个 GENERATE AC 命令请求 TC, 卡片应返回 AAC。

通过标准: 验证交易 2、交易 4、交易 6、交易 8 和交易 10 的第二个 GENERATE AC 返回的数据。SW1 SW2= ‘9000’, CID 位 8-7= ‘00’。CID 位 4= ‘0’, CID 位 3-1= ‘000’, CVR 字节 2 高半字节= ‘2’, CVR 字节 2 位 4= ‘1’, CID= ‘00’, CVR= ‘03 2C 00 00’ 或 ‘03 28 00 00’ (用于未校验 PIN)。

7.31.11 LJWC011-00

测试目的: 发卡行认证执行未成功, 终端请求批准交易联机。发卡行认证数据中的 ARC 为 00、01、02、10 和 11。当设置 ADA 中的“如果发卡行认证执行但失败, 拒绝交易”位, 设置“如果因为发卡行认证失败或没有执行导致交易拒绝, 生成通知”位时, 验证卡片强制联机拒绝交易。验证卡片设置 CVR 中的“发卡行认证执行但失败”位。验证卡片设置 CID 的“需要通知”位。

测试条件: 第 9 章中的卡片特征 13, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 发卡行认证执行未成功, ARC 为 00, 卡片强制拒绝交易;

c) 卡片上电 (ATR);

d) 选择 PBOC 借记/贷记应用;

- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3030' ;
- i) 第二个 GENERATE AC 命令请求 TC, 卡片应返回 AAC;
- j) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- k) 交易 4: 发卡行认证执行未成功, ARC 为 01, 卡片强制拒绝交易;
- l) 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 ARQC;
- q) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3031' ;
- r) 第二个 GENERATE AC 命令请求 TC, 卡片应返回 AAC;
- s) 交易 5: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- t) 交易 6: 发卡行认证执行未成功, ARC 为 02, 卡片强制拒绝交易;
- u) 卡片上电 (ATR);
- v) 选择 PBOC 借记/贷记应用;
- w) GET PROCESSING OPTIONS 命令;
- x) VERIFY 命令;
- y) 第一个 GENERATE AC 命令请求 ARQC;
- z) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3032' ;
- aa) 第二个 GENERATE AC 命令请求 TC, 卡片应返回 AAC;
- ab) 交易 7: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- ac) 交易 8: 发卡行认证执行未成功, ARC 为 10, 卡片强制拒绝交易;
- ad) 卡片上电 (ATR);
- ae) 选择 PBOC 借记/贷记应用;
- af) GET PROCESSING OPTIONS 命令;
- ag) VERIFY 命令;
- ah) 第一个 GENERATE AC 命令请求 ARQC;
- ai) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3130' ;
- aj) 第二个 GENERATE AC 命令请求 TC, 卡片应返回 AAC;
- ak) 交易 9: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- al) 交易 10: 发卡行认证执行未成功, ARC 为 11, 卡片强制拒绝交易;
- am) 卡片上电 (ATR);
- an) 选择 PBOC 借记/贷记应用;
- ao) GET PROCESSING OPTIONS 命令;
- ap) VERIFY 命令;
- aq) 第一个 GENERATE AC 命令请求 ARQC;
- ar) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3131' ;
- as) 第二个 GENERATE AC 命令请求 TC, 卡片应返回 AAC。

通过标准: 沿海交易 2、交易 4、交易 6、交易 8 和交易 10 的第二个 GENERATE AC 返回的数据, SW1 SW2= '9000', CID 位 8-7= '00', CID 位 4= '1', CVR 字节 2 高半字节= '2',

CVR 字节 2 位 4= ‘1’，CID= ‘08’，CVR= ‘03 2C 00 00’ 或 ‘03 28 00 00’（用于未校验 PIN）。

7.31.12 LJWC012-00

测试目的：发卡行认证执行未成功，终端请求批准交易联机。发卡行认证数据中的 ARC 为 00、01、02、10 和 11。当未设置 ADA 中的“如果发卡行认证执行但失败，拒绝交易”位，不论卡片是否设置 ADA 中的“如果因为发卡行认证失败或没有执行导致交易拒绝，生成通知”位，验证卡片批准交易联机。验证卡片设置 CVR 中的“发卡行认证执行但失败”位。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：发卡行认证执行未成功，ARC 为 00，卡片批准联机交易；

c) 卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 命令请求 ARQC；

h) EXTERNAL AUTHENTICATE 命令，错误的 ARPC，ARC 为 ‘3030’；

i) 第二个 GENERATE AC 命令请求 TC；

j) 交易 3：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

k) 交易 4：发卡行认证执行未成功，ARC 为 01，卡片批准联机交易；

l) 卡片上电(ATR)；

m) 选择 PBOC 借记/贷记应用；

n) GET PROCESSING OPTIONS 命令；

o) VERIFY 命令；

p) 第一个 GENERATE AC 命令请求 ARQC；

q) EXTERNAL AUTHENTICATE 命令，错误的 ARPC，ARC 为 ‘3031’；

r) 第二个 GENERATE AC 命令请求 TC；

s) 交易 5：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

t) 交易 6：发卡行认证执行未成功，ARC 为 02，卡片批准联机交易；

u) 卡片上电(ATR)；

v) 选择 PBOC 借记/贷记应用；

w) GET PROCESSING OPTIONS 命令；

x) VERIFY 命令；

y) 第一个 GENERATE AC 命令请求 ARQC；

z) EXTERNAL AUTHENTICATE 命令，错误的 ARPC，ARC 为 ‘3032’；

aa) 第二个 GENERATE AC 命令请求 TC；

ab) 交易 7：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

ac) 交易 8：发卡行认证执行未成功，ARC 为 10，卡片批准联机交易；

ad) 卡片上电(ATR)；

ae) 选择 PBOC 借记/贷记应用；

af) GET PROCESSING OPTIONS 命令；

ag) VERIFY 命令；

- ah) 第一个 GENERATE AC 命令请求 ARQC;
- ai) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3130' ;
- aj) 第二个 GENERATE AC 命令请求 TC;
- ak) 交易 9: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- al) 交易 10: 发卡行认证执行未成功, ARC 为 11, 卡片批准联机交易;
- am) 卡片上电 (ATR);
- an) 选择 PBOC 借记/贷记应用;
- ao) GET PROCESSING OPTIONS 命令;
- ap) VERIFY 命令;
- aq) 第一个 GENERATE AC 命令请求 ARQC;
- ar) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3131' ;
- as) 第二个 GENERATE AC 命令请求 TC。

通过标准: 验证交易 2、交易 4、交易 6、交易 8 和交易 10 的第二个 GENERATE AC 的返回, SW1 SW2='9000', CID 位 8-7='01', CVR 字节 2 高半字节='6', CVR 字节 2 位 4='1', CVR='03 6C 00 00' 或 '03 68 00 00' (用于未校验 PIN)。

7.31.13 LJWC013-00

测试目的: 发卡行认证执行未成功, 终端请求批准交易联机。发卡行认证数据中的 ARC 不是 00、01、02、10 和 11。不论卡片是否设置 ADA 中的“如果发卡行认证执行但失败, 拒绝交易”位, 也不论卡片是否设置 ADA 中的“如果因为发卡行认证失败或没有执行导致交易拒绝, 生成通知”位, 验证卡片强制交易拒绝联机。验证卡片设置 CVR 中的“发卡行认证执行但失败”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 发卡行认证执行未成功, ARC 为 15, 卡片强制拒绝交易;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 命令请求 ARQC;
 - h) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3135' 。
 - i) 第二个 GENERATE AC 命令请求 TC, 卡返回 AAC。

通过标准: 验证交易中卡片返回的数据, 第一个 GENERATE AC, CID='80', 第一个 GENERATE AC, CVR='03 A4 00 00' 或 '03 A0 00 00' (用于未校验 PIN), 第二个 GENERATE AC, CID='00', 第二个 GENERATE AC, CVR='03 2C 00 00' 或 '03 28 00 00' (用于未校验 PIN)。

7.31.14 LJWC014-00

测试目的: 发卡行认证成功, 发卡行认证数据中的 ARC 为 00、10 或 11, 终端请求拒绝交易联机, 验证卡片不设置 CVR 中的“发卡行认证执行但失败”位和“联机授权后, 发卡行认证没有执行”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 发卡行认证执行成功, ARC 为 00, 联机拒绝;
- c) 卡片上电(ATR);
- d) 选择 PBOC 借记/贷记应用;
- e) GET PROCESSING OPTIONS 命令;
- f) VERIFY 命令;
- g) 第一个 GENERATE AC 命令请求 ARQC;
- h) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3030' ;
- i) 第二个 GENERATE AC 命令请求 AAC;
- j) 交易 3: 发卡行认证执行成功, ARC 为 10, 联机拒绝;
- k) 卡片上电(ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 ARQC;
- p) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3130' ;
- q) 第二个 GENERATE AC 命令请求 AAC;
- r) 交易 4: 发卡行认证执行成功, ARC 为 11, 联机拒绝;
- s) 卡片上电(ATR);
- t) 选择 PBOC 借记/贷记应用;
- u) GET PROCESSING OPTIONS 命令;
- v) VERIFY 命令;
- w) 第一个 GENERATE AC 命令请求 ARQC;
- x) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC, ARC 为 '3131' ;
- y) 第二个 GENERATE AC 命令请求 AAC。

通过标准: 验证交易 2—4 的第二个 GENERATE AC 命令的返回数据, SW1 SW2= '9000' ,
CID 位 8-7= '00' , CVR 字节 2 高半字节= '2' , CVR 字节 2 位 4= '0' , CVR 字节
3 位 3= '0' , CVR= '03 24 00 00' 或 '03 20 00 00' (用于未校验 PIN)。

7.31.15 LJWC015-00

测试目的: 发卡行认证未成功, 发卡行认证数据中的 ARC 为 00、10 或 11, 终端请求拒绝交易联机, 验证卡片设置 CVR 中的“发卡行认证执行但失败”位, 不设置“联机授权后, 发卡行认证没有执行”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 发卡行认证执行未成功, ARC 为 00, 联机拒绝;
c) 卡片上电(ATR);
d) 选择 PBOC 借记/贷记应用;
e) GET PROCESSING OPTIONS 命令;
f) VERIFY 命令;
g) 第一个 GENERATE AC 命令请求 ARQC;
h) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3030' ;
i) 第二个 GENERATE AC 命令请求 AAC;
j) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- k) 交易 4: 发卡行认证执行未成功, ARC 为 10, 联机拒绝;
- l) 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 ARQC;
- q) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3130' ;
- r) 第二个 GENERATE AC 命令请求 AAC;
- s) 交易 5: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- t) 交易 6: 发卡行认证执行未成功, ARC 为 11, 联机拒绝;
- u) 卡片上电 (ATR);
- v) 选择 PBOC 借记/贷记应用;
- w) GET PROCESSING OPTIONS 命令;
- x) VERIFY 命令;
- y) 第一个 GENERATE AC 命令请求 ARQC;
- z) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC, ARC 为 '3131' ;
- aa) 第二个 GENERATE AC 命令请求 AAC。

通过标准: 验证交易 2、4 和 6 的第二个 GENERATE AC 命令的返回数据, SW1 SW2= '9000' , CID 位 8-7= '00' , CVR 字节 2 高半字节= '2' , CVR 字节 2 位 4= '1' , CVR 字节 3 位 3= '0' , CVR= '03 2C 00 00' 或 '03 28 00 00' (用于未校验 PIN)。

7.32 联机授权未完成 (LJWW)

7.32.1 LJWW001-00

测试目的: 联机批准交易, 卡片不支持发卡行认证, 未执行发卡行认证, 验证卡片重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 2

- 测试流程:
- a) 交易 1: 不执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 由于卡片不支持发卡行认证, 未执行发卡行认证, 批准联机交易;
 - c) 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 命令请求 ARQC;
 - h) 第二个 GENERATE AC 命令请求 TC;
 - i) 交易 3: 脱机批准。

通过标准: 验证交易 3 的第一个 GENERATE AC 的返回数据, SW1 SW2= '9000' , CID 位 8-7= '01' , CVR 字节 2 高半字节= '9' , CVR 字节 3 位 8= '0' , CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.32.2 LJWW002-00

测试目的: 联机拒绝交易, 卡片不支持发卡行认证, 未执行发卡行认证, 验证卡片重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 2

测试流程: a) 交易 1: 不执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 b) 交易 2: 由于卡片不支持发卡行认证, 未执行发卡行认证, 联机交易拒绝;
 c) 卡片上电(ATR);
 d) 选择 PBOC 借记/贷记应用;
 e) GET PROCESSING OPTIONS 命令;
 f) VERIFY 命令;
 g) 第一个 GENERATE AC 命令请求 ARQC;
 h) 第二个 GENERATE AC 命令请求 AAC;
 i) 交易 3: 脱机批准。

通过标准: 验证交易 3 的第一个 GENERATE AC 的返回数据, SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 8= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.32.3 LJWW003-00

测试目的: 发卡行认证执行成功, 联机交易成功, 验证卡片重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 b) 交易 2: 发卡行认证成功, 联机交易批准, 卡片上电(ATR);
 c) 选择 PBOC 借记/贷记应用;
 d) GET PROCESSING OPTIONS 命令;
 e) OVERIFY 命令;
 f) 第一个 GENERATE AC 命令请求 ARQC;
 g) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 h) 第二个 GENERATE AC 命令请求 AAC;
 i) 交易 3: 脱机批准。

通过标准: 验证交易 3 的第一个 GENERATE AC 的返回数据: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 8= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.32.4 LJWW004-00

测试目的: 发卡行认证执行成功, 联机交易拒绝, 验证卡片重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 b) 交易 2: 发卡行认证成功, 联机交易拒绝, 卡片上电(ATR);
 c) 选择 PBOC 借记/贷记应用;
 d) GET PROCESSING OPTIONS 命令;
 e) VERIFY 命令;
 f) 第一个 GENERATE AC 命令请求 ARQC;
 g) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 h) 第二个 GENERATE AC 命令请求 AAC;
 i) 交易 3: 脱机批准。

通过标准: 验证交易 3 的第一个 GENERATE AC 命令中的返回数据: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 8= '0', CVR= '03 94 00 00'

或 ‘03 90 00 00’（用于未校验 PIN）。

7.32.5 LJWW005-00

测试目的：联机批准交易，发卡行认证执行失败，验证卡片不重置“联机授权指示”位。

测试条件：第9章中的卡片特征1，支持发卡行认证。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：发卡行认证未成功，联机交易批准，卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；

h) 第二个 GENERATE AC 命令请求 TC；

i) 交易3：终端在第一个 GENERATE AC 命令中请求 TC，卡片返回要求联机，卡片上电(ATR)；

j) 选择 PBOC 借记/贷记应用；

k) GET PROCESSING OPTIONS 命令；

l) VERIFY 命令；

m) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：验证交易3的第一个 GENERATE AC 命令中的返回数据：SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 3 位 8= ‘1’，CVR= ‘03 A4 88 00’ 或 ‘03 A0 88 00’（用于未校验 PIN）。

7.32.6 LJWW006-00

测试目的：发卡行认证执行，但执行失败，联机拒绝交易，验证卡片不重置“联机授权指示”位。

测试条件：第9章中的卡片特征1，支持发卡行认证。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：发卡行认证未成功，联机交易拒绝，卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；

h) 第二个 GENERATE AC 命令请求 AAC；

i) 交易3：终端在第一个 GENERATE AC 命令中请求 TC，卡片返回要求联机，卡片上电(ATR)；

j) 选择 PBOC 借记/贷记应用；

k) GET PROCESSING OPTIONS 命令；

l) VERIFY 命令；

m) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：验证交易3的第一个 GENERATE AC 的返回数据：SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 3 位 8= ‘1’，CVR= ‘03 A4 88 00’ 或 ‘03 A0 88 00’（用于未校验 PIN）。

7.32.7 LJWW007-00

测试目的：发卡行认证是强制性执行的，但未执行，联机交易拒绝，验证卡片不重置“联机授权指示”位。

测试条件：第9章中的卡片特征1，支持发卡行认证且强制执行

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：未执行发卡行认证，联机交易拒绝：卡片上电(ATR)；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) 第二个 GENERATE AC 命令请求 AAC；

h) 交易3：终端在第一个 GENERATE AC 命令中请求 TC，卡片返回要求联机：卡片上电(ATR)；

i) 选择PBOC借记/贷记应用；

j) GET PROCESSING OPTIONS 命令；

k) VERIFY 命令；

l) 第一个 GENERATE AC 命令请求 TC，卡片返回 ARQC。

通过标准：验证交易3的第一个 GENERATE AC 的返回数据：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 8=‘1’，CVR=‘03 A4 88 00’或‘03 A0 80 00’（用于未校验 PIN）。

7.32.8 LJWW008-00

测试目的：发卡行认证是强制性执行的，但未执行，联机交易批准，验证卡片不重置“联机授权指示”位。

测试条件：第9章中的卡片特征1，支持发卡行认证且强制执行。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：未执行发卡行认证，联机交易批准：卡片上电(ATR)；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) 第二个 GENERATE AC 命令请求 TC；

h) 交易3：终端在第一个 GENERATE AC 命令中请求 TC 卡片返回要求联机：卡片上电(ATR)；

i) 选择PBOC借记/贷记应用；

j) GET PROCESSING OPTIONS 命令；

k) VERIFY 命令；

l) 第一个 GENERATE AC 命令请求 TC，卡片应返回 ARQC。

通过标准：验证交易3的第一个 GENERATE AC 的返回数据：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 8=‘1’，CVR=‘03 A4 88 00’或‘03 A0 88 00’（用于未校验 PIN）。

7.32.9 LJWW009-00

测试目的：发卡行认证可选，未执行发卡行认证，联机交易拒绝，验证卡片重置“联机授权指示”位。

测试条件：第9章中的卡片特征3，支持发卡行认证且是可选的。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：未执行发卡行认证，支持发卡行认证且是可选的，联机交易拒绝，卡片上电(ATR)；
c) 选择PBOC借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 第二个 GENERATE AC 命令请求 AAC；
h) 交易3：脱机批准。

通过标准：验证交易3的第一个 GENERATE AC 的返回数据：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 8=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.32.10 LJWW010-00

测试目的：发卡行认证可选，未执行发卡行认证，联机交易批准，验证卡片重置“联机授权指示”位。

测试条件：第9章中的卡片特征3，支持发卡行认证且是可选的。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：未执行发卡行认证，支持发卡行认证且是可选的，联机交易批准，卡片上电(ATR)；
c) 选择PBOC借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 第二个 GENERATE AC 命令请求 TC；
h) 交易3：脱机批准。

通过标准：验证交易3的第一个 GENERATE AC 的返回数据：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 8=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.32.11 LJWW011-00

测试目的：将卡片从终端中拔出，验证卡片不重置“联机授权指示”位。

测试条件：第9章中的卡片特征1

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：在第一个 GENERATE AC 命令请求联机后，将卡片从终端中拔出，卡片上电(ATR)；
c) 选择PBOC借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；

- g) 交易 3: 终端在第一个 GENERATE AC 命令请求 TC, 卡片返回要求联机, 卡片上电 (ATR);
- h) 选择 PBOC 借记/贷记应用;
- i) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- k) 第一个 GENERATE AC 命令请求 TC, 卡片返回 ARQC。

通过标准: 验证交易 3 的第一个 GENERATE AC 命令的返回数据: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 8= '1', CVR= '03 A4 80 00' 或 '03 A0 80 00' (用于未校验 PIN)。

7.32.12 LJWW012-00

测试目的: 终端请求联机交易但无法联机, 终端拒绝交易脱机, 验证卡片不重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 终端请求联机, 但不能联机, 终端应拒绝脱机交易, 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 命令请求 ARQC;
 - g) 第二个 GENERATE AC 命令请求 AAC 且 ARC 为 Z3;
 - h) 交易 3: 终端在第一个 GENERATE AC 命令中请求 TC, 卡片返回要求联机: 卡片上电 (ATR);
 - i) 选择 PBOC 借记/贷记应用;
 - j) GET PROCESSING OPTIONS 命令;
 - k) VERIFY 命令;
 - l) 第一个 GENERATE AC 命令请求 TC, 卡片应返回 ARQC。

通过标准: 验证交易 3 的第一个 GENERATE AC 命令的返回数据: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 8= '1', CVR= '03 A4 80 00' 或 '03 A0 80 00' (用于未校验 PIN)。

7.32.13 LJWW013-00

测试目的: 联机批准交易, 卡片不支持发卡行认证, 未执行发卡行认证, 验证卡片重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 2。

- 测试流程:
- a) 交易 1: 不执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 卡片不支持发卡行认证, 未执行发卡行认证, 联机交易批准: 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 命令请求 ARQC ;
 - g) 第二个 GENERATE AC 命令请求 TC;

h) 交易 3: 脱机拒绝。

通过标准: 验证交易 3 的第一个 GENERATE AC 命令的返回数据: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 8= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.32.14 LJWW014-00

测试目的: 发卡行认证执行, 联机交易批准, 验证卡片重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 1, 卡片支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 发卡行认证成功, 联机交易批准, 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 ARQC;

g) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;

h) 第二个 GENERATE AC 命令请求 TC;

i) 交易 3: 脱机拒绝。

通过标准: 验证交易 3 的第一个 GENERATE AC 命令的返回数据: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 8= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.32.15 LJWW015-00

测试目的: 发卡行认证执行失败, 联机交易批准, 验证卡片重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 发卡行认证未成功, 联机交易批准: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 ARQC;

g) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;

h) 第二个 GENERATE AC 命令请求 TC;

i) 交易 3: 脱机拒绝。

通过标准: 验证交易 3 的第一个 GENERATE AC 命令的返回数据: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 8= '1', CVR= '03 84 88 00' 或 '03 80 88 00' (用于未校验 PIN)。

7.32.16 LJWW016-00

测试目的: 发卡行认证是强制执行的, 未执行发卡行认证, 联机交易批准, 验证卡片不重置“联机授权指示”位。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 卡片支持发卡行认证且是强制执行的, 未执行发卡行认证, 联机交易批

- 准：卡片上电(ATR)；
- c) 选择 PBOC 借记/贷记应用；
 - d) GET PROCESSING OPTIONS 命令；
 - e) VERIFY 命令；
 - f) 第一个 GENERATE AC 命令请求 ARQC；
 - g) 第二个 GENERATE AC 命令请求 TC；
 - h) 交易 3：脱机拒绝。

通过标准：验证交易 3 的第一个 GENERATE AC 命令的返回数据：SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 3 位 8= ‘1’，CVR= ‘03 84 88 00’ 或 ‘03 80 88 00’（用于未校验 PIN）。

7.32.17 LJWW017-00

测试目的：发卡行认证可选，未执行发卡行认证，联机交易批准，验证卡片重置“联机授权指示”位。

测试条件：第 9 章中的卡片特征 3，支持发卡行认证且是可选的。

- 测试流程：
- a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
 - b) 交易 2：卡片支持发卡行认证且是可选的，未执行发卡行认证，联机交易批准，卡片上电(ATR)；
 - c) 选择 PBOC 借记/贷记应用；
 - d) GET PROCESSING OPTIONS 命令；
 - e) VERIFY 命令；
 - f) 第一个 GENERATE AC 命令请求 ARQC；
 - g) 第二个 GENERATE AC 命令请求 TC；
 - h) 交易 3：脱机拒绝。

通过标准：验证交易 3 的第一个 GENERATE AC 命令的返回数据：SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 3 位 8= ‘0’，CVR= ‘03 84 00 00’ 或 ‘03 80 00 00’（用于未校验 PIN）。

7.32.18 LJWW018-00

测试目的：将卡片从终端拔出，验证卡片不重置“联机授权指示”位。

测试条件：第 9 章中的卡片特征 1。

- 测试流程：
- a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
 - b) 交易 2：在第一个 GENERATE AC 命令请求联机后将卡片从终端拔出：卡片上电(ATR)；
 - c) 选择 PBOC 借记/贷记应用；
 - d) GET PROCESSING OPTIONS 命令；
 - e) VERIFY 命令；
 - f) 第一个 GENERATE AC 命令请求 ARQC；
 - g) 交易 3：脱机拒绝。

通过标准：验证交易 3 的第一个 GENERATE AC 命令的返回数据：SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 3 位 8= ‘1’，CVR= ‘03 84 80 00’ 或 ‘03 80 80 00’（用于未校验 PIN）。

7.32.19 LJWW019-00

测试目的：请求联机而终端无法联机，终端批准脱机交易，验证卡片不重置“联机授权指示”位。

测试条件：第9章中的卡片特征1。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：请求联机而终端无法联机，终端执行脱机批准，卡片上电(ATR)；
c) 选择PBOC借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 第二个 GENERATE AC 命令请求 TC 且 ARC 为 Y3；
h) 交易3：终端请求脱机批准，卡片返回 ARQC，卡片上电(ATR)；
i) 选择PBOC借记/贷记应用；
j) GET PROCESSING OPTIONS 命令；
k) VERIFY 命令；
l) 第一个 GENERATE AC 命令请求 TC，卡片返回 ARQC。

通过标准：验证交易3的第一个 GENERATE AC 命令的返回数据：SW1 SW2= ‘9000’，CID= ‘80’，CVR= ‘03 A4 80 00’ 或 ‘03 A0 80 00’（用于未校验 PIN）。

7.32.20 LJWW020-00

测试目的：请求联机而终端无法联机，终端批准脱机交易，验证卡片不重置“联机授权指示”位。

测试条件：第9章中的卡片特征1。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器。
b) 交易2：请求联机而终端无法联机，终端执行脱机批准，卡片上电(ATR)。
c) 选择PBOC借记/贷记应用。
d) GET PROCESSING OPTIONS 命令。
e) VERIFY 命令。
f) 第一个 GENERATE AC 命令请求 ARQC。
g) 第二个 GENERATE AC 命令请求 TC 且 ARC 为 Y3。
h) 交易3：脱机拒绝。

通过标准：验证交易3的第一个 GENERATE AC 命令的返回数据：第一个 GENERATE AC，CID= ‘00’，第一个 GENERATE AC，CVR= ‘03 84 80 00’ 或 ‘03 80 80 00’（用于未校验 PIN）。

7.33 PIN CHANGE/UNBLOCK 命令(PCUC)

7.33.1 PCUC001-00

测试目的：使用少于4位的MAC执行PIN UNBLOCK命令未成功。

测试条件：第9章中的卡片特征1，支持脱机PIN和PIN UNBLOCK命令(P2= ‘00’)。

测试流程：准备后，执行一个PIN UNBLOCK命令，命令格式见表23，其MAC长度小于4位，Lc应为错误的MAC长度。

表23 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	00	03	11 22 33	N/A

通过标准：PIN UNBLOCK 命令的返回码 SW1 SW2 不应为 ‘9000’，推荐的返回码为 ‘6700’。

7.33.2 PCUC002-00

测试目的：使用大于 8 位的 MAC 执行 PIN UNBLOCK 命令未成功。
测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN UNBLOCK 命令(P2= ‘00’)。
测试流程：准备后， 执行一个 PIN UNBLOCK 命令， 命令格式见表 24， 其 MAC 长度大于 8 位， Lc 应为错误的 MAC 长度。

表24 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	00	09	11 22 33 44 55 66 77 88 99	N/A

通过标准：PIN UNBLOCK 命令的返回码 SW1 SW2 不应为 ‘9000’， 推荐的返回码为 ‘6700’。

7.33.3 PCUC003-00

测试目的：使用小于 4 位的 MAC 执行 PIN CHANGE(当前 PIN)命令未成功。
测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN CHANGE 命令(P2= ‘01’)。
测试流程：执行一个 PIN CHANGE(当前 PIN)命令， 命令格式见表 25， 其 MAC 长度小于 4 位， Lc 应为错误的 MAC 长度。

表25 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	01	13	78 96 32 14 75 36 98 74 12 25 58 87 15 59 95 51 24 11 22	N/A

通过标准：PIN UNBLOCK（当前 PIN）命令的返回码 SW1 SW2 不应为 ‘9000’， 推荐的返回码为 ‘6700’。

7.33.4 PCUC004-00

测试目的：使用大于 8 位的 MAC 执行 PIN CHANGE(当前 PIN)命令未成功。
测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN CHANGE(P2= ‘01’)。
测试流程：执行一个 PIN CHANGE(当前 PIN)命令， 命令格式见表 26， 其 MAC 长度大于 8 位， Lc 应为错误的 MAC 长度。

表26 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	01	13	78 96 32 14 75 36 98 74 12 25 58 87 15 59 95 51 24 11 22 33 44 55 66 77 88 99	N/A

通过标准：PIN UNBLOCK（当前 PIN）命令的返回码 SW1 SW2 不应为 ‘9000’， 推荐的返回码为 ‘6700’。

7.33.5 PCUC005-00

测试目的：使用小于 4 位的 MAC 执行 PIN CHANGE(新 PIN)命令未成功。
测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN CHANGE 命令(P2= ‘02’)。
测试流程：准备后， 执行一个 PIN CHANGE(新 PIN)命令， 命令格式见表 27， 其 MAC 长度小于 4 位， Lc 应为错误的 MAC 长度。

表27 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	02	13	78 96 32 14 75 36 98 74 12 25 58 87 15 59 95 51 24 11 22	N/A

通过标准：PIN UNBLOCK（当前 PIN）命令的返回码 SW1 SW2 不应为‘9000’，推荐的返回码为‘6700’。

7.33.6 PCUC006-00

测试目的：使用大于 8 位的 MAC 执行 PIN CHANGE(新 PIN)命令未成功。
测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN CHANGE 命令(P2=‘02’)。
测试流程：准备后，执行一个 PIN CHANGE(新 PIN)命令，命令格式见表 28，其 MAC 长度大于 8 位，Lc 应为错误的 MAC 长度。

表28 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	02	13	78 96 32 14 75 36 98 74 12 25 58 87 15 59 95 51 24 11 22 33 44 55 66 77 88 99	N/A

通过标准：PIN UNBLOCK（当前 PIN）命令的返回码 SW1 SW2 不应为‘9000’，推荐的返回码为‘6700’。

7.33.7 PCUC007-00

测试目的：使用错误的 MAC 执行 PIN UNBLOCK 命令未成功。
测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN UNBLOCK 命令(P2=‘00’)。
测试流程：准备后，执行一个 PIN UNBLOCK 命令，命令格式见表 29，使用错误的 MAC。

表29 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	00	04	11 22 33 44	N/A

通过标准：PIN UNBLOCK（当前 PIN）命令的返回码 SW1 SW2 不应为‘9000’，推荐的返回码为‘6988’。

7.33.8 PCUC008-00

测试目的：执行正确的 PIN UNBLOCK 命令，卡片应返回 9000。
测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN UNBLOCK 命令(P2=‘00’)。
测试流程：准备后，执行一个 PIN UNBLOCK 命令，命令格式见表 30，使用正确的 MAC。

表30 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	00	04	11 22 33 44	N/A

通过标准：SW1 SW2 = ‘9000’。

7.33.9 PCUC009-00

测试目的：使用错误的 MAC 执行 PIN CHANGE(当前 PIN)命令未成功。
测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN UNBLOCK 命令(P2=‘01’)。
测试流程：准备后，执行一个 PIN CHANGE(当前 PIN)命令，命令格式见表 31，使用错误的 MAC。

表31 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	01	14	78 96 32 14 75 36 98 74 12 25 58 87 15 59 95 51 24 11 22 33 44	N/A

通过标准：PIN UNBLOCK（当前 PIN）命令的返回码 SW1 SW2 不应为 ‘9000’，推荐的返回码为 ‘6988’。

7.33.10 PCUC010-00

测试目的：执行正确的 PIN CHANGE 命令（当前 PIN），卡片应返回 ‘9000’。

测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN CHANGE 命令(P2= ‘01’)。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机请求，执行正确的 PIN CHANGE 命令，使用新参考 PIN 为 12345：卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令(参考 PIN=1234)；

f) 第一个 GENERATE AC 命令请求 ARQC；

g) 执行 EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

h) 第二个 GENERATE AC 命令请求 TC；

i) 使用正确的 MAC 执行 PIN CHANGE/UNBLOCK 命令；

j) 交易 3：联机请求，执行正确的 PIN CHANGE 命令，保存参考 PIN 为 1234：卡片上电(ATR)；

k) 选择 PBOC 借记/贷记应用；

l) GET PROCESSING OPTIONS 命令；

m) VERIFY 命令(参考 PIN=12345)；

n) 第一个 GENERATE AC 命令请求 ARQC；

o) 执行 EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

p) 第二个 GENERATE AC 命令请求 TC；

q) 使用正确的 MAC 执行 PIN CHANGE/UNBLOCK 命令；

r) 交易 4：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器，参考 PIN 为 1234。

通过标准：验证交易 2：PIN CHANGE/UNBLOCK SW1 SW2= ‘9000’ ,CVR= ‘03 64 00 00’。验证交易 3：VERIFY 命令（PIN=12345）SW1 SW2= ‘9000’ ,PIN CHANGE/UNBLOCK SW1 SW2= ‘9000’ ,CVR= ‘03 64 00 10’。验证交易 4：VERIFY 命令（PIN=1234）SW1 SW2 = ‘9000’。

7.33.11 PCUC011-00

测试目的：使用错误的 MAC 执行 PIN CHANGE(新 PIN)命令未成功。

测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN CHANGE 命令(P2= ‘02’)。

测试流程：准备后，执行一个 PIN CHANGE(新 PIN)命令，命令格式见表 32，使用错误的 MAC。

表32 PIN UNBLOCK 命令

CLA	INS	P1	P2	Lc	Data	Le
84	24	00	02	15	78 96 32 14 75 36 98 74 12 25 58 87 15 59 95 51 24 11 22 33 44	N/A

通过标准：PIN UNBLOCK(新 PIN)命令的返回码 SW1 SW2 不应为 ‘9000’，推荐的返回码为 ‘6988’。

7.33.12 PCUC012-00

测试目的：对未知 PIN 执行 PIN CHANGE 命令成功。

测试条件：第 9 章中的卡片特征 1，支持脱机 PIN 和 PIN CHANGE 命令(P2= ‘02’)。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机请求，执行正确的 PIN CHANGE 命令对未知 PIN 的卡，使用新参考 PIN 为 12345：卡片上电(ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令(参考 PIN=1234)；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) 执行 EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
h) 第二个 GENERATE AC 命令请求 TC；
i) 使用正确的 MAC 执行 PIN CHANGE/UNBLOCK 命令；
j) 交易 3：联机请求，执行正确的 PIN CHANGE 命令对未知 PIN 的卡，保存参考 PIN 为 1234：卡片上电(ATR)；
k) 选择 PBOC 借记/贷记应用；
l) GET PROCESSING OPTIONS 命令；
m) VERIFY 命令(参考 PIN=12345)；
n) 第一个 GENERATE AC 命令请求 ARQC；
o) 执行 EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
p) 第二个 GENERATE AC 命令请求 TC；
q) 使用正确的 MAC 执行 PIN CHANGE/UNBLOCK 命令；
r) 交易 4：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器，确保参考 PIN 为 1234。

通过标准：验证交易 2：PIN CHANGE/UNBLOCK SW1 SW2= ‘9000’，CVR= ‘03 64 00 00’。验证交易 3：VERIFY 命令(参考 PIN=12345) SW1 SW2= ‘9000’，PIN CHANGE/UNBLOCK 命令, SW1 SW2= ‘9000’，CVR= ‘03 64 00 10’。验证交易 4：VERIFY 命令(PIN=1234) SW1 SW2= ‘9000’。

7.34 持卡人认证(CKRZ)

7.34.1 CKRZ001-00

测试目的：批准脱机交易，不执行脱机 PIN 时，验证卡片不设置 CVR 的“脱机 PIN 执行”位。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：脱机批准：卡片上电(ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) 第一个 GENERATE AC 请求 TC。

通过标准：验证交易 2：SW1 SW2= ‘9000’，CID= ‘40’，CVR 字节 2 位 3= ‘0’，CVR 字节 2 位 2= ‘0’，CVR 字节 3 位 7= ‘0’。

7.34.2 CKRZ002-00

测试目的：脱机交易拒绝，不执行脱机 PIN 时，验证卡片不设置 CVR 的“脱机 PIN 执行”位。

测试条件：第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 b) 交易 2: 脱机拒绝: 卡片上电 (ATR);
 c) 选择 PBOC 借记/贷记应用;
 d) GET PROCESSING OPTIONS 命令;
 e) 第一个 GENERATE AC 请求 AAC。

通过标准: 验证交易第一个 GENERATE AC 命令中的返回数据: SW1 SW2= '9000', CID= '00',
 CVR 字节 2 位 3= '0', CVR 字节 2 位 2= '0', CVR 字节 3 位 7= '0'。

7.34.3 CKRZ003-00

测试目的: 联机交易, 不执行脱机 PIN 时, 验证第一个 GENERATE AC 返回 CVR 不设置“脱机 PIN 认证执行”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 b) 交易 2: 请求执行联机: 卡片上电 (ATR);
 c) 选择 PBOC 借记/贷记应用;
 d) GET PROCESSING OPTIONS 命令;
 e) 第一个 GENERATE AC 请求 ARQC。

通过标准: 验证交易第一个 GENERATE AC 命令中的返回数据: SW1 SW2= '9000', CID= '80',
 CVR 字节 2 位 3= '0', CVR 字节 2 位 2= '0', CVR 字节 3 位 7= '0'。

7.34.4 CKRZ004-00

测试目的: 联机批准交易, 不执行脱机 PIN 时, 验证第二个 GENERATE AC 返回, 不设置 CVR 中的“脱机 PIN 执行”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 b) 交易 2: 联机批准: 卡片上电 (ATR);
 c) 选择 PBOC 借记/贷记应用;
 d) GET PROCESSING OPTIONS 命令;
 e) 第一个 GENERATE AC 请求 ARQC;
 f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 g) 第二个 GENERATE AC 请求 TC。

通过标准: 验证交易第二个 GENERATE AC 命令中的返回数据: SW1 SW2= '9000', CID= '40',
 CVR 字节 2 位 3= '0', CVR 字节 2 位 2= '0', CVR 字节 3 位 7= '0'。

7.34.5 CKRZ005-00

测试目的: 拒绝联机交易, 不执行脱机 PIN 时, 验证卡片第二个 GENERATE AC 返回, 不设置 CVR 中的“脱机 PIN 执行”位。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 b) 交易 2: 联机拒绝: 卡片上电 (ATR);
 c) 选择 PBOC 借记/贷记应用;
 d) GET PROCESSING OPTIONS 命令;
 e) 第一个 GENERATE AC 请求 ARQC;

f) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;

g) 第二个 GENERATE AC 请求 AAC。

通过标准: 验证交易第二个 GENERATE AC 命令中的返回数据: SW1 SW2= '9000', CID= '00', CVR 字节 2 位 3= '0', CVR 字节 2 位 2= '0', CVR 字节 3 位 7= '0'。

7.34.6 CKRZ006-00

测试目的: 批准脱机交易, 执行脱机 PIN, 验证卡片设置 CVR 的“脱机 PIN 执行”位。

测试条件: 第 9 章中的卡片特征 1, 支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 请求脱机批准: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 TC。

通过标准: 验证交易第一个 GENERATE AC 命令中的返回数据: SW1 SW2= '9000', CID= '40', CVR 字节 2 位 3= '1', CVR 字节 2 位 2= '0', CVR 字节 3 位 7= '0'。

7.34.7 CKRZ007-00

测试目的: 脱机交易拒绝, 执行脱机 PIN, 验证卡片设置 CVR 的“脱机 PIN 执行”位。

测试条件: 第 9 章中的卡片特征 1, 支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 请求脱机拒绝: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 AAC。

通过标准: 验证交易第一个 GENERATE AC 命令中的返回数据: SW1 SW2= '9000', CID= '00', CVR 字节 2 位 3= '1', CVR 字节 2 位 2= '0', CVR 字节 3 位 7= '0'。

7.34.8 CKRZ008-00

测试目的: 联机交易, 执行脱机 PIN 时, 验证卡片第一个 GENERATE AC 返回, 设置 CVR 的“脱机 PIN 执行”位。

测试条件: 第 9 章中的卡片特征 1, 支持脱机 PIN。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 请求执行联机: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 ARQC。

通过标准: 验证交易第一个 GENERATE AC 命令中的返回数据: SW1 SW2= '9000', CID= '80', CVR 字节 2 位 3= '1', CVR 字节 2 位 2= '0', CVR 字节 3 位 7= '0'。

7.34.9 CKRZ009-00

测试目的：批准联机交易，脱机 PIN 执行时，验证卡片第二个 GENERATE AC 返回，设置 CVR 的“脱机 PIN 执行”位。

测试条件：第 9 章中的卡片特征 1，支持脱机 PIN。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机批准：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

h) 第二个 GENERATE AC 请求 TC。

通过标准：验证交易第二个 GENERATE AC 命令中的返回数据：SW1 SW2=‘9000’，CID=‘40’，CVR 字节 2 位 3=‘1’，CVR 字节 2 位 2=‘0’，CVR 字节 3 位 7=‘0’。

7.34.10 CKRZ010-00

测试目的：联机拒绝交易，脱机 PIN 执行时，验证卡片第二个 GENERATE AC 返回，设置 CVR 的“脱机 PIN 执行”位。

测试条件：第 9 章中的卡片特征 1，支持脱机 PIN。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：联机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

h) 第二个 GENERATE AC 请求 AAC。

通过标准：验证交易第二个 GENERATE AC 命令中的返回数据：SW1 SW2=‘9000’，CID=‘00’，CVR 字节 2 位 3=‘1’，CVR 字节 2 位 2=‘0’，CVR 字节 3 位 7=‘0’。

7.35 PUT DATA 连续交易限制（国际）(LXXZ)

7.35.1 LXXZ001-00

测试目的：联机批准后，PUT DATA 命令修改连续交易限制（国际）成功，MAC 正确。

测试条件：第 9 章中的卡片特征 7，支持 PUT DATA 修改连续交易限制（国际），所有交易货币代码≠‘0156’。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：PUT DATA 命令修改连续交易限制（国际），联机批准：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC 命令；

h) 第二个 GENERATE AC 请求 TC；

i) PUT DATA 命令修改连续交易限制（国际），MAC 正确，新值为 03；

- j) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- k) 交易 4: 脱机批准;
- l) 交易 5: 脱机批准;
- m) 交易 6: 脱机批准;
- n) 交易 7: PUT DATA 命令修改连续交易限制 (国际) MAC 正确, 联机批准: 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;
- s) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- t) 第二个 GENERATE AC 请求 TC;
- u) PUT DATA 命令修改连续交易限制 (国际), MAC 正确, 新值 05。

通过标准: 验证交易 2 第二个 GENERATE AC 的响应: SW1 SW2= '9000', CID= '40', CVR= '03 64 00 00' 或 '03 60 00 00'。验证交易 4、5、6 第一个 GENERATE AC 的响应: SW1 SW2= '9000', CID= '40', CVR= '03 94 00 00' 或 '03 90 00 00'。验证交易 7: 第一个 GENERATE AC, CID= '80', 第一个 GENERATE AC, CVR= '03 A4 20 00' 或 '03 A0 20 00', 第二个 GENERATE AC, CID= '40', 第二个 GENERATE AC, CVR= '03 64 20 00' 或 '03 60 20 00', PUT DATA 命令, SW1 SW2= '9000'。

7.35.2 LXXZ002-00

测试目的: 联机批准后, 执行 PUT DATA 命令修改连续交易限制 (国际), MAC 错误; 发卡行认证成功执行。连续交易限制数 (国际) 为 5。

测试条件: 第 9 章中的卡片特征 7, 支持 PUT DATA 命令修改连续交易限制 (国际), 所有交易的交易货币代码≠ '0156'。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: PUT DATA 命令修改连续交易限制 (国际), MAC 错误, 联机批准交易: 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 请求 ARQC;
 - g) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 - h) 第二个 GENERATE AC 请求 TC;
 - i) PUT DATA 命令修改连续交易限制 (国际), MAC 错误;
 - j) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - k) 交易 4: 脱机批准交易;
 - l) 交易 5: 脱机批准交易;
 - m) 交易 6: 脱机批准交易;
 - n) 交易 7: 脱机批准交易。

通过标准: 验证交易 7 第一个 GENERATE AC 返回 TC, CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.35.3 LXXZ003-00

测试目的：联机批准后，执行 PUT DATA 命令修改连续交易限制（国际），无 MAC。成功执行发卡行认证。连续交易限制（国际）数为 5。

测试条件：第 9 章中的卡片特征 7，支持 PUT DATA 命令修改连续交易限制（国际），所有交易的交易货币代码≠‘0156’。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：PUT DATA 命令修改连续交易限制（国际），无 MAC，联机批准交易：卡片上电(ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 请求 ARQC；
g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
h) 第二个 GENERATE AC 请求 TC；
i) PUT DATA 命令连续交易限制（国际），无 MAC；
j) 交易 3：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
k) 交易 4：脱机批准交易；
l) 交易 5：脱机批准交易；
m) 交易 6：脱机批准交易；
n) 交易 7：脱机批准交易。

通过标准：交易 7 第一个 GENERATE AC 卡返回 TC，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.36 支付系统环境(ZFXT)（接触条件下适用）

7.36.1 ZFXT001-00

测试目的：验证卡片接受 SELECT PSE 命令。

测试条件：第 9 章中的卡片特征 1，支持 PSE。

测试流程：执行 SELECT PSE 命令。

通过标准：SW1 SW2=‘9000’。

7.36.2 ZFXT002-00

测试目的：卡片不支持 PSE，执行 SELECT 命令，验证响应状态字为‘6A82’。

测试条件：第 9 章中的卡片特征 1，不支持 PSE。

测试流程：执行 SELECT PSE 命令。

通过标准：SW1 SW2=‘6A82’。

7.36.3 ZFXT003-00

测试目的：选择 PSE 成功，验证返回的 FCI 模板标签。

测试条件：见 ZFXT001，支持 PSE。

测试流程：执行 SELECT PSE 命令。

通过标准：FCI 模板标签=‘6F’，FCI 模板长度最大为 252 字节。

7.36.4 ZFXT004-00

测试目的：选择 PSE 成功，验证返回的 DF 名。

测试条件：见 ZFXT001，支持 PSE。

测试流程：执行 SELEC PSE 命令。

通过标准：DF 名标签= ‘84’，DF 名长度= ‘0E’，DF 名为 1PAY.SYS.DDF01。

7.36.5 ZFXT005-00

测试目的：选择 PSE 成功，验证返回的 FCI 专有模板。

测试条件：见 ZFXT001，支持 PSE。

测试流程：执行 SELECT PSE 命令。

通过标准：FCI 专有模板标签= ‘A5’。

7.36.6 ZFXT006-00

测试目的：选择 PSE 成功，验证返回的 SFI 目录。

测试条件：见 ZFXT001，支持 PSE。

测试流程：执行 SELECT PSE 命令。

通过标准：SFI 目录的标签= ‘88’，SFI 目录的长度= ‘01’，SFI 目录的值在 ‘01’ — ‘0A’ 范围内。

7.36.7 ZFXT007-00

测试目的：选择 PSE 成功，验证返回的首选语言。

测试条件：见 ZFXT001，支持 PSE，首选语言存在。

测试流程：执行 SELECT PSE 命令。

通过标准：首选语言的标签= ‘5F2D’，首选语言的长度 ‘02’ — ‘08’，首选语言的内容是字母数字格式。

7.36.8 ZFXT008-00

测试目的：选择 PSE 成功，验证返回的发卡行代码表索引。

测试条件：见 ZFXT001，支持 PSE，发卡行代码表索引存在。

测试流程：执行 SELECT PSE 命令。

通过标准：发卡行代码表索引的标签= ‘9F11’，发卡行代码表索引的长度= ‘01’，发卡行代码表索引的值为 ‘01’ — ‘0A’。

7.36.9 ZFXT009-00

测试目的：选择 PSE 成功，验证返回的发卡行自定义数据。

测试条件：见 ZFXT001，支持 PSE，发卡行自定义数据存在。

测试流程：执行 SELECT PSE 命令。

通过标准：FCI 发卡行数据标签= ‘BF0C’，FCI 发卡行数据的长度最大为 222。

7.36.10 ZFXT010-00

测试目的：交易后，未重置卡片，验证是否可以重新选择 PSE。

测试条件：第 9 章中的卡片特征 1，支持 PSE。

测试流程：a) SELECT 命令；

b) GET PROCESSING OPTIONS 命令；

c) VERIFY 命令（如果支持）；

- d) 第一个 GENERATE AC 命令请求 TC 或 AAC;
- e) SELECT PSE 命令。

通过标准: SW1 SW2= '9000' 。

7.36.11 ZFXT011-00

测试目的: 卡片锁定后, 未重置卡片, 验证 PSE 无效。

测试条件: 第 9 章中的卡片特征 1, 支持 PSE 和 CARD BLOCK 命令。

测试流程: a) SELECT 命令;

b) GET PROCESSING OPTIONS 命令;

c) VERIFY 命令 (如支持);

d) 第一个 GENERATE AC 请求 ARQC;

e) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;

f) 第二个 GENERATE AC 请求 TC 或 AAC;

g) CARD BLOCK 命令;

h) SELECT PSE 命令。

通过标准: SELECT PSE 命令的 SW1 SW2= '6A81' 。

7.36.12 ZFXT012-00

测试目的: 卡片锁定后, 重置卡片, 验证 PSE 无效。

测试条件: 第 9 章中的卡片特征 1, 支持 CARD BLOCK, 卡片已锁定。

测试流程: a) 卡片复位;

b) SELECT PSE 命令。

通过标准: SELECT PSE 命令的 SW1 SW2= '6A81' 。

7.37 近距离支付系统环境 (JZFX) (非接适用)

7.37.1 PPSE001-00

测试目的: PPSE 选择卡片中的非接触金融应用的 AID, 应在 SELECT PPSE 命令响应的 FCI 中返回。

测试条件: 1 号特征。

测试流程: a) 上电;

b) 选择应用 (PPSE) 。

通过标准: 验证卡响应 FCI 数据应符合 FCI 模板要求。

7.37.2 PPSE002-00

测试目的: 卡片中的非接触入口 PPSE 在接触下选择应不能批准。

测试条件: 1 号特征。

测试流程: a) 接触下上电;

b) 选择应用 (PPSE) 。

通过标准: 验证卡响应 SELECT PPSE 为 6A82。

7.37.3 PPSE003-00

测试目的: 卡片在非接触下直接选择 AID, 应能进行非接 PBOC 交易。

测试条件: 1 号特征。

测试流程: a) 接触下上电;

- b) 选择 AID 应用;
- c) GP0;
- d) READ RECORD;
- e) GAC ARQC;
- f) GAC TC。

通过标准: 验证 SELECT 返回的 FCI 不是 qPBOC 交易 FCI 模板, 验证 GP0 卡返回数据格式应为 PBOC GP0 响应模板。

7.37.4 PPSE004-00

测试目的: 卡片在非接触下应能通过 PPSE 选择方式进行正确的借贷记交易。

测试条件: 1 号特征。

- 测试流程:
- a) 非接触下上电;
 - b) 选择 PPSE;
 - c) GP0;
 - d) READ RECORD;
 - e) GAC ARQC;
 - f) GAC TC。

通过标准: 验证 SELECT 返回的 FCI 不是借记贷记 FCI 模板, 验证选中的交易是否能执行正常交易流程。

7.37.5 PPSE005-00

测试目的: 未重置卡片, 验证是否可以重新选择 PPSE。

测试条件: 1 号特征。

- 测试流程:
- a) 非接触下上电;
 - b) 选择 PPSE;
 - c) GP0;
 - d) READ RECORD;
 - e) GAC ARQC;
 - f) GAC TC;
 - g) SELECT PPSE 命令。

通过标准: 第 7 步 SW1 SW2= '9000' 。

7.37.6 PPSE006-00

测试目的: 卡片锁定后, 未重置卡片, 验证 PPSE 无效。

测试条件: 1 号特征。

- 测试流程:
- a) SELECT 命令;
 - b) GET PROCESSING OPTIONS 命令;
 - c) VERIFY 命令 (如支持);
 - d) 第一个 GENERATE AC 请求 ARQC;
 - e) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 - f) 第二个 GENERATE AC 请求 TC 或 AAC;
 - g) CARD BLOCK 命令;
 - h) SELECT PPSE 命令。

通过标准：SELECT PSE 命令的 SW1 SW2= ‘6A81’ 。

7.37.7 PPSE007-00

测试目的：卡片锁定后，重置卡片，验证 PPSE 无效。

测试条件：1 号特征。

测试流程：a) 卡片复位；
b) SELECT PPSE 命令。

通过标准：SELECT PSE 命令的 SW1 SW2= ‘6A81’ 。

7.38 PUT DATA 命令(PDML)

7.38.1 PDML001-00

测试目的：MAC 少于 4 个字节，PUT DATA 命令不成功。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL 或 UCOL。

测试流程：准备测试条件完成后，执行 PUT DATA 命令（MAC 少于 4 个字节，命令格式见表 33），
Lc 符合实际数据域长度。

表33 PUT DATA 命令格式

CLA	INS	P1	P2	Lc	DATA	Le
04	DA	9F	58 或 59	04	03 11 22 33	N/A

通过标准：PUT DATA 命令的 SW1 SW2≠ ‘9000’，推荐返回 ‘6700’ 。

7.38.2 PDML002-00

测试目的：MAC 大于 8 个字节，PUT DATA 命令不成功。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL 或 UCOL。

测试流程：准备测试条件完成后，执行 PUT DATA 命令（MAC>8 字节，命令格式见表 34），Lc
符合实际数据域长度。

表34 PUT DATA 命令格式

CLA	INS	P1	P2	Lc	DATA	Le
04	DA	9F	58 或 59	0A	03 11 22 33 44 55 66 77 88 99	N/A

通过标准：PUT DATA 命令的 SW1 SW2≠ ‘9000’，推荐返回 ‘6700’ 。

7.38.3 PDML003-00

测试目的：PUT DATA 命令不成功，MAC 错误。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL 或 UCOL。

测试流程：准备测试条件完成后，执行 PUT DATA 命令（MAC 不正确，命令格式见表 35）。

表35 PUT DATA 命令格式

CLA	INS	P1	P2	Lc	DATA	Le
04	DA	9F	58 或 59	05	03 11 22 33 44	N/A

通过标准：PUT DATA 命令的 SW1 SW2≠ ‘9000’，建议返回 ‘6988’ 。

7.38.4 PDML004-00

测试目的：PUT DATA 命令成功，验证卡片响应状态字为 ‘9000’ 。

测试条件：第 9 章中的卡片特征 1，支持 PUT DATA 命令修改 LCOL 或 UCOL。

测试流程：准备测试条件完成后，执行 PUT DATA 命令（数据域中 MAC 正确，命令格式见表 36）。

表36 PUT DATA 命令格式

CLA	INS	P1	P2	Lc	DATA	Le
04	DA	9F	58 或 59	05	03 11 22 33 44	N/A

通过标准：PUT DATA 命令的 SW1 SW2= ‘9000’ 。

7.39 READ RECORD 命令（REML）

7.39.1 REML001-00

测试目的：成功的 READ RECORD 命令，验证卡片返回 ‘9000’ 。

测试条件：标准联机交易成功。

测试流程：准备测试条件后，执行正确的 REAR RECORD 命令，命令格式见表 37。

表37 PUT DATA 命令格式

CLA	INS	P1	P2	Lc	DATA	Le
00	位 2	01	0C	N/A	N/A	00

通过标准：SW1 SW2= ‘9000’ 。

7.40 静态应用数据认证（JTRZ）

7.40.1 JTRZ001-00

测试目的：对不用于数据签名的记录，验证 AFL 中对应的每个元素的第 4 字节不等于 0。

个人化过程中要求签名的数据所在的记录，验证 AFL 中对应元素的第 4 字节不等于 0。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：验证签名数据，数据应包含标签、长度、值，验证在已签名的记录中不应存在未签名的数据。

7.40.2 JTRZ002-00

测试目的：验证卡片接受 READ RECORD 命令，该命令包含 SDA 所需的数据对象。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：SW1 SW2= ‘9000’ 。

7.40.3 JTRZ003-00

测试目的：验证 READ RECORD 命令的响应数据模板，该命令包含 SDA 所需的数据对象。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准: 响应数据模板的标签= '70', 响应数据模板的长度 \leq 252。

7.40.4 JTRZ004-00

测试目的: 验证 READ RECORD 命令响应的 CA 公钥, 该命令包含 SDA 所需的数据对象。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电 (ATR);

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准: CA 公钥标签= '8F', CA 公钥的长度= '01', CA 公钥的值= '99'。

7.40.5 JTRZ005-00

测试目的: 验证 READ RECORD 命令响应的发卡行公钥指数, 该命令包含 SDA 所需的数据对象。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电 (ATR);

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准: 发卡行公钥指数的标签= '9F32', 发卡行公钥指数的长度= '01', 发卡行公钥指数的值= '03'。

7.40.6 JTRZ006-00

测试目的: 验证 READ RECORD 命令响应的发卡行公钥证书, 该命令包含 SDA 所需的数据对象。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电 (ATR);

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准: 发卡行公钥证书的标签= '90', 发卡行公钥证书的长度= '80'。

7.40.7 JTRZ007-00

测试目的: 验证 READ RECORD 命令响应的已签名的应用数据, 该命令包含 SDA 所需的数据对象。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电 (ATR);

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准: 签名应用数据的标签= '93', 签名应用数据的长度等于发卡行公钥模。

7.40.8 JTRZ008-00

测试目的：对不用于数据签名的记录，验证 AFL 中对应的每个元素的第 4 字节等于 0（1152 位密钥）。

个人化过程中要求签名的数据所在的记录，验证 AFL 中对应元素的第 4 字节不等于 0。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：验证签名数据，数据应包含标签、长度、值，验证在已签名的记录中不应存在未签名的数据。

7.40.9 JTRZ009-00

测试目的：验证卡片接受 READ RECORD 命令，该命令包含 SDA 所需的数据对象（1152 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) READ RECORD 命令。

通过标准：SW1 SW2=‘9000’。

7.40.10 JTRZ010-00

测试目的：验证 READ RECORD 命令的响应数据模板，该命令包含 SDA 所需的数据对象（1152 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：响应数据模板的标签=‘70’，响应数据模板的长度≤252。

7.40.11 JTRZ011-00

测试目的：验证 READ RECORD 命令响应的 CA 公钥，该命令包含 SDA 所需的数据对象（1152 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：CA 公钥标签=‘8F’，CA 公钥的长度=‘01’，CA 公钥的值=‘90’。

7.40.12 JTRZ012-00

测试目的：验证 READ RECORD 命令响应的发卡行公钥指数，该命令包含 SDA 所需的数据对象（1152 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：发卡行公钥指数的标签=‘9F32’，发卡行公钥指数的长度=‘01’，发卡行公钥指数的值=‘03’。

7.40.13 JTRZ013-00

测试目的：验证 READ RECORD 命令响应的发卡行公钥证书，该命令包含 SDA 所需的数据对象（1152 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：发卡行公钥证书的标签=‘90’，发卡行公钥证书的长度=‘90’。

7.40.14 JTRZ014-00

测试目的：验证 READ RECORD 命令响应的已签名的应用数据，该命令包含 SDA 所需的数据对象（1152 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：签名应用数据的标签=‘93’，签名应用数据的长度等于发卡行公钥模。

7.40.15 JTRZ015-00

测试目的：对不用于数据签名的记录，验证 AFL 中对应的每个元素的第 4 字节等于 0（1408 位密钥）。

个人化过程中要求签名的数据所在的记录，验证 AFL 中对应元素的第 4 字节不等于 0。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：验证签名数据，数据应包含标签、长度、值，验证在已签名的记录中不应存在未签名的数据。

7.40.16 JTRZ016-00

测试目的：验证卡片接受 READ RECORD 命令，该命令包含 SDA 所需的数据对象（1408 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程: a) 卡片上电(ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) READ RECORD 命令。

通过标准: SW1 SW2= '9000'。

7.40.17 JTRZ017-00

测试目的: 验证 READ RECORD 命令的响应数据模板, 该命令包含 SDA 所需的数据对象(1408 位密钥)。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电(ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) 执行 READ RECORD 命令。

通过标准: 响应数据模板的标签= '70', 响应数据模板的长度≤252。

7.40.18 JTRZ018-00

测试目的: 验证 READ RECORD 命令响应的 CA 公钥, 该命令包含 SDA 所需的数据对象(1408 位密钥)。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电(ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) 执行 READ RECORD 命令。

通过标准: CA 公钥标签= '8F', CA 公钥的长度= '01', CA 公钥的值= 'B0'。

7.40.19 JTRZ019-00

测试目的: 验证 READ RECORD 命令响应的发卡行公钥指数, 该命令包含 SDA 所需的数据对象(1408 位密钥)。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电(ATR);
b) 选择 PBOC 借记/贷记应用;
c) GET PROCESSING OPTIONS 命令;
d) 执行 READ RECORD 命令。

通过标准: 发卡行公钥指数的标签= '9F32', 发卡行公钥指数的长度= '01', 发卡行公钥指数的值= '03'。

7.40.20 JTRZ020-00

测试目的: 验证 READ RECORD 命令响应的发卡行公钥证书, 该命令包含 SDA 所需的数据对象(1408 位密钥)。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电(ATR);
b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准: 发卡行公钥证书的标签= '90', 发卡行公钥证书的长度= 'B0'。

7.40.21 JTRZ021-00

测试目的: 验证 READ RECORD 命令响应的已签名的应用数据, 该命令包含 SDA 所需的数据对象 (1408 位密钥)。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电 (ATR);

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准: 签名应用数据的标签= '93', 签名应用数据的长度等于发卡行公钥模。

7.40.22 JTRZ022-00

测试目的: 对不用于数据签名的记录, 验证 AFL 中对应的每个元素的第 4 字节等于 0 (1976 位密钥)。

个人化过程中要求签名的数据所在的记录, 验证 AFL 中对应元素的第 4 字节不等于 0。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电 (ATR);

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准: 验证签名数据, 数据应包含标签、长度、值, 验证在已签名的记录中不应存在未签名的数据。

7.40.23 JTRZ023-00

测试目的: 验证卡片接受 READ RECORD 命令, 该命令包含 SDA 所需的数据对象 (1976 位密钥)。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电 (ATR);

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) READ RECORD 命令。

通过标准: SW1 SW2= '9000'。

7.40.24 JTRZ024-00

测试目的: 验证 READ RECORD 命令的响应数据模板, 该命令包含 SDA 所需的数据对象 (1976 位密钥)。

测试条件: 标准联机交易成功, 支持 SDA。

测试流程: a) 卡片上电 (ATR);

b) 选择 PBOC 借记/贷记应用;

c) GET PROCESSING OPTIONS 命令;

d) 执行 READ RECORD 命令。

通过标准：响应数据模板的标签=‘70’，响应数据模板的长度≤252。

7.40.25 JTRZ025-00

测试目的：验证 READ RECORD 命令响应的 CA 公钥，该命令包含 SDA 所需的数据对象（1976 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：CA 公钥标签=‘8F’，CA 公钥的长度=‘01’，CA 公钥的值=‘F8’。

7.40.26 JTRZ026-00

测试目的：验证 READ RECORD 命令响应的发卡行公钥指数，该命令包含 SDA 所需的数据对象（1976 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)。
b) 选择 PBOC 借记/贷记应用。
c) GET PROCESSING OPTIONS 命令。
d) 执行 READ RECORD 命令。

通过标准：发卡行公钥指数的标签=‘9F32’，发卡行公钥指数的长度=‘01’，发卡行公钥指数的值=‘03’。

7.40.27 JTRZ027-00

测试目的：验证 READ RECORD 命令响应的发卡行公钥证书，该命令包含 SDA 所需的数据对象（1976 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：发卡行公钥证书的标签=‘90’，发卡行公钥证书的长度=‘F7’。

7.40.28 JTRZ028-00

测试目的：验证 READ RECORD 命令响应的已签名的应用数据，该命令包含 SDA 所需的数据对象（1976 位密钥）。

测试条件：标准联机交易成功，支持 SDA。

测试流程：a) 卡片上电 (ATR)；
b) 选择 PBOC 借记/贷记应用；
c) GET PROCESSING OPTIONS 命令；
d) 执行 READ RECORD 命令。

通过标准：签名应用数据的标签=‘93’，签名应用数据的长度等于发卡行公钥模。

7.41 选择 PBOC 借记/贷记应用命令 (XZYY)

7.41.1 XZYY001-00

测试目的：执行成功的 SELECT 命令，验证卡片返回 ‘9000’。

测试条件：标准联机交易成功。

测试流程：成功的 ATR 之后，执行 SELECT 命令。

通过标准：SW1 SW2= ‘9000’。

7.41.2 XZYY002-00

测试目的：执行 SELECT 命令选择一个不存在的应用，此命令应不成功。

测试条件：第 9 章中的卡片特征 1。

测试流程：成功的 ATR 后，执行 SELECT 命令（语法正确，应用无效）。

通过标准：SELECT 命令的 SW1 SW2≠ ‘9000’，建议返回 ‘6A82’。

7.41.3 XZYY003-00

测试目的：执行 SELECT 命令（所选应用已锁定）不成功。

测试条件：第 9 章中的卡片特征 1，支持 APPLICATION BLOCK 和 APPLICATION UNBLOCK 应用，所选应用已锁定。

测试流程：成功的 ATR 后，执行 SELECT 命令（语法正确，应用无效）。

通过标准：SELECT PBOC 命令的 SW1 SW2= ‘6283’。

7.41.4 XZYY004-00

测试目的：建立候选列表，卡片应正确的响应 SELECT 和 SELECT NEXT 命令。终端支持的 AID= ‘A0 00 00 03 33 01 01’，卡片个人化后支持应用 ‘A0 00 00 03 33 01 01 01’ 和 ‘A0 00 00 03 33 01 01 02’。

测试条件：第 9 章中的卡片特征 27，一个终端的 AID 支持多个 ADF。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：脱机批准：卡片上电 (ATR)；

c) 建立候选列表，选择 A0 00 00 03 33 01 01；

d) 选择下一个，基于更长的匹配的卡响应；

e) 选择下一个，基于更长的匹配的卡响应；

f) 最终选择 A0 00 00 03 33 01 01 01；

g) GET PROCESSING OPTIONS 命令；

h) VERIFY 命令；

i) 第一个 GENERATE AC 请求 ARQC；

j) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

k) 第二个 GENERATE AC 请求 TC。

通过标准：验证交易 2：SELECT 命令响应的 DF 名为 ‘A0 00 00 03 33 01 01 01’ 或 ‘A0 00 00 03 33 01 01 02’，第一个 SELECT NEXT 命令响应的 DF 名为 ‘A0 00 00 03 33 01 01 01’ 或 ‘A0 00 00 03 33 01 01 02’，与前一次 SELECT 命令响应的不同，第二次 SELECT NEXT 命令响应的 SW1 SW2= ‘6A82’，CID= ‘40’，CVR= ‘03 64 00 00’ 或 ‘03 60 00 00’（用于未校验 PIN）。

7.42 前次交易 SDA 失败 (SDSB)

7.42.1 SDSB001-00

测试目的：验证对于一个脱机批准交易，当脱机 SDA 通过时，卡片重置“SDA 失败指针”位。

验证当交易脱机批准，卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：脱机批准；

c) 交易 3：脱机批准。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 1=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.42.2 SDSB002-00

测试目的：验证对于一个联机批准交易，当脱机 SDA 通过时，卡片重置“SDA 失败指针”位。

验证当交易脱机批准，卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 成功，联机批准：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

h) 第二个 GENERATE AC 请求 TC；

i) 交易 3：脱机批准。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 1=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.42.3 SDSB003-00

测试目的：验证对于一个脱机拒绝交易，当不支持脱机 SDA 时，卡片不设置“SDA 失败指针”位。

验证当交易脱机批准，卡片不设置 CVR 中“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 11。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：未执行 SDA，脱机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 AAC；

g) 交易 3：脱机批准。

通过标准：第一个 GENERATE AC 命令，SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 1=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.42.4 SDSB004-00

测试目的：验证对于一个脱机拒绝交易，当支持脱机 SDA（AIP 字节 1 位 7=‘1’）且认证通过时，卡片不设置“SDA 失败指针”位。验证当交易脱机批准，卡片设置 CVR 中的“上

次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 成功，脱机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 AAC；

g) 交易 3：脱机批准。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘01’，CVR 字节 2 高半字节= ‘9’，CVR 字节 3 位 1= ‘0’，CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。

7.42.5 SDSB005-00

测试目的：验证对于一个脱机拒绝交易，当支持脱机 SDA（AIP 字节 1 位 7= ‘1’）且认证失败时，卡片设置“SDA 失败指针”位。验证当交易脱机批准，卡片设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 失败，脱机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7= ‘1’；

g) 交易 3：脱机批准。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘01’，CVR 字节 2 高半字节= ‘9’，CVR 字节 3 位 1= ‘0’，CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。

7.42.6 SDSB006-00

测试目的：验证对于一个联机拒绝交易，当不支持脱机 SDA 时，卡片不设置“SDA 失败指针”位。

验证当交易脱机批准，卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 11。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：未执行 SDA，联机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

h) 第二个 GENERATE AC 请求 AAC；

i) 交易 3：脱机批准。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘01’，CVR 字节 2 高半字节= ‘9’，CVR 字节 3 位 1= ‘0’，CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。

7.42.7 SDSB007-00

测试目的：验证对于一个联机拒绝交易，当支持脱机 SDA（AIP 字节 1 位 7=‘1’）且认证通过时，卡片不设置“SDA 失败指针”位。验证当交易脱机批准，卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 成功，联机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 ARQC；

g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

h) 第二个 GENERATE AC 请求 AAC；

i) 交易 3：脱机批准。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 1=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.42.8 SDSB008-00

测试目的：验证对于一个联机拒绝交易，当支持脱机 SDA（AIP 字节 1 位 7=‘1’）且认证失败时，卡片不设置“SDA 失败指针”位。验证当交易脱机批准，卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 失败，联机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 ARQC，TVR 字节 1 位 7=‘1’；

g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

h) 第二个 GENERATE AC 请求 AAC，TVR 字节 1 位 7=‘1’；

i) 交易 3：脱机批准。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘01’，CVR 字节 2 高半字节=‘9’，CVR 字节 3 位 1=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验 PIN）。

7.42.9 SDSB009-00

测试目的：验证对于一个脱机拒绝交易，当交易不能执行联机且不支持 SDA 时，卡片不设置“SDA 失败指针”位。验证当设置“卡片请求联机指示”位时，卡片请求交易联机。验证卡片不设置 CVR 中的“上次交易脱机 SDA 失败，交易脱机拒绝”位。

测试条件：第 9 章中的卡片特征 11。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：请求交易执行联机，但终端不能执行联机。未执行 SDA，交易脱机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

- e) VERIFY 命令;
- f) 第一个 GENERATE AC 请求 ARQC;
- g) 第二个 GENERATE AC 请求 AAC, ARC=Z3;
- h) 交易 3: 第一个 GENERATE AC 终端请求 TC 后, 卡片请求执行联机: 卡片上电 (ATR);
- i) 选择 PBOC 借记/贷记应用;
- j) GET PROCESSING OPTIONS 命令;
- k) VERIFY 命令;
- l) 第一个 GENERATE AC 请求 TC, 卡返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 1= '0', CVR= '03 A4 80 00' 或 '03 A0 80 00' (用于未校验 PIN)。

7.42.10 SDSB010-00

测试目的: 验证对于一个脱机批准交易, 当脱机 SDA 认证通过时, 卡片不设置“SDA 失败指针”位。验证当交易脱机拒绝, 卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器。
b) 交易 2: 脱机批准。
c) 交易 3: 拒绝脱机。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 1= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.42.11 SDSB011-00

测试目的: 验证对于一个脱机拒绝交易, 当支持脱机 SDA (AIP 字节 1 位 7= '1') 且认证通过时, 卡片不设置“SDA 失败指针”位。验证当交易脱机拒绝, 卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: SDA 成功, 脱机拒绝: 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第二个 GENERATE AC 请求 AAC;
g) 交易 3: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节 = '8', CVR 字节 3 位 1= '0'。CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.42.12 SDSB012-00

测试目的: 验证对于一个脱机拒绝交易, 当支持脱机 SDA (AIP 字节 1 位 7= '1') 且认证失败时, 卡片设置“SDA 失败指针”位。验证当交易脱机拒绝, 卡片设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);

- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;
- g) 交易 3: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 1= '1', CVR= '03 84 10 00' 或 '03 80 10 00' (用于未校验 PIN)。

7.42.13 SDSB013-00

测试目的: 验证对于一个脱机拒绝交易, 当交易不能执行联机, 支持脱机 SDA (AIP 字节 1 位 7= '1') 且认证通过时, 卡片不设置“SDA 失败指针”位。验证当交易脱机拒绝, 卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 请求交易执行联机, 但终端不能执行联机。SDA 成功, 交易脱机拒绝: 卡片上电 (ATR);
 - d) 选择 PBOC 借记/贷记应用;
 - e) GET PROCESSING OPTIONS 命令;
 - f) VERIFY 命令;
 - g) 第一个 GENERATE AC 请求 ARQC;
 - h) 第二个 GENERATE AC 请求 AAC, ARC=Z3;
 - i) 交易 3: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 1= '0', CVR= '03 84 80 00' 或 '03 80 80 00' (用于未校验 PIN)。

7.42.14 SDSB014-00

测试目的: 验证对于一个脱机拒绝交易, 当支持脱机 SDA (AIP 字节 1 位 7= '1') 且认证失败时, 卡片设置“SDA 失败指针”位。验证当交易脱机拒绝, 卡片设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 请求交易执行联机, 但终端不能执行联机。SDA 失败, 交易脱机拒绝: 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 请求 ARQC, TVR 字节 1 位 7= '1' ;
 - g) 第二个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;
 - h) 交易 3: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 1= '1', CVR= '03 84 81 00' 或 '03 80 81 00' (用于未校验 PIN)。

7.42.15 SDSB015-00

测试目的：验证对于一个脱机批准交易，当脱机 SDA 认证通过时，卡片重置“SDA 失败指针”位。

验证当交易执行联机，卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：脱机批准；

c) 交易 3：终端请求交易执行联机：卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 1=‘1’，CVR=‘03 A4 00 00’或‘03 A0 00 00’（用于未校验 PIN）。

7.42.16 SDSB016-00

测试目的：验证对于一个脱机批准交易，当脱机 SDA 认证通过时，卡片重置“SDA 失败指针”位。

验证当交易执行联机，卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：脱机批准；

c) 交易 3：终端请求交易执行联机：卡片上电(ATR)；

d) 选择 PBOC 借记/贷记应用；

e) GET PROCESSING OPTIONS 命令；

f) VERIFY 命令；

g) 第一个 GENERATE AC 请求 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 1=‘0’，CVR=‘03 A4 00 00’或‘03 A0 00 00’（用于未校验 PIN）。

7.42.17 SDSB017-00

测试目的：验证对于一个脱机拒绝交易，当支持脱机 SDA（AIP 字节 1 位 7=‘1’）且认证失败时，卡片设置“SDA 失败指针”位。验证当交易执行联机，卡片设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 失败，脱机拒绝：卡片上电(ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7=‘1’；

g) 交易 3：终端请求交易执行联机：卡片上电(ATR)；

h) 选择 PBOC 借记/贷记应用；

i) GET PROCESSING OPTIONS 命令；

j) VERIFY 命令；

k) 第一个 GENERATE AC 请求 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 1= '1', CVR= '03 A4 01 00' 或 '03 A0 01 00' (用于未校验 PIN)。

7.42.18 SDSB018-00

测试目的: 验证对于一个脱机交易拒绝, 当交易不能执行联机, 支持脱机 SDA (AIP 字节 1 位 7= '1') 且认证通过时, 卡片不设置“SDA 失败指针”位。验证当设置“卡片请求联机指示”位时, 卡片请求交易执行联机。验证卡片不设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 请求交易执行联机, 但终端不能执行联机。SDA 成功, 交易脱机拒绝: 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第一个 GENERATE AC 请求 ARQC;
g) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
h) 第二个 GENERATE AC 请求 AAC, ARC=Z3;
i) 交易 3: 第一个 GENERATE AC 终端请求 TC 后, 卡片请求执行联机: 卡片上电 (ATR)。
j) 选择 PBOC 借记/贷记应用;
k) GET PROCESSING OPTIONS 命令;
l) VERIFY 命令;
m) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 1= '0', CVR= '03 A4 80 00' 或 '03 A0 80 00' (用于未校验 PIN)。

7.42.19 SDSB019-00

测试目的: 验证对于一个脱机拒绝交易, 当交易不能执行联机, 支持脱机 SDA (AIP 字节 1 位 7= '1') 且认证失败时, 卡片设置“SDA 失败指针”位。验证当设置“卡片请求联机指示”位时, 卡片请求交易执行联机。验证卡片设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 请求交易执行联机, 但终端不能执行联机。SDA 失败, 交易脱机拒绝: 卡片上电 (ATR);
c) 选择 PBOC 借记/贷记应用;
d) GET PROCESSING OPTIONS 命令;
e) VERIFY 命令;
f) 第一个 GENERATE AC 请求 ARQC, TVR 字节 1 位 7= '1';
g) 第二个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1';
h) 交易 3: 第一个 GENERATE AC 终端请求 TC 后, 卡片请求执行联机: 卡片上电 (ATR)。
i) 选择 PBOC 借记/贷记应用;
k) GET PROCESSING OPTIONS 命令;

1) VERIFY 命令;

m) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 1= '1', CVR= '03 A4 81 00' 或 '03 A0 81 00' (用于未校验 PIN)。

7.42.20 SDSB020-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。脱机交易批准, 验证卡片设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。交易 4 批准脱机, 验证卡片不重置 CVR 中的“SDA 失败指针”位, 设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;

g) 交易 3: 脱机批准;

h) 交易 4: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 1= '1', CVR= '03 94 01 00' 或 '03 90 01 00' (用于未校验 PIN)。

7.42.21 SDSB021-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。脱机交易拒绝, 验证卡片设置 CVR 中的“上次交易 SDA 失败交易拒绝”位。脱机交易批准, 验证卡片不设置 CVR 的“SDA 失败指针”位, 设置“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;

g) 交易 3: 脱机拒绝;

h) 交易 4: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 1= '1', CVR= '03 94 01 00' 或 '03 90 01 00' (用于未校验 PIN)。

7.42.22 SDSB022-00

测试目的: 验证对于一个脱机拒绝交易, 交易不能执行联机、支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。当设置“卡片请求联机指示”位时, 请求执行联机, 但终端不能执行联机, 验证交易脱机拒绝。当设置“卡片请求联机指示”

位时，验证交易执行联机。验证卡片不设置 CVR 的“SDA 失败指针”位，设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：请求交易执行联机但终端不能执行联机，SDA 失败，脱机交易拒绝：卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 请求 ARQC，TVR 字节 1 位 7=‘1’；
g) 第二个 GENERATE AC 请求 AAC，ARC=Z3，TVR 字节 1 位 7=‘1’；
h) 交易 3：第一个 GENERATE AC 终端请求 TC 后，卡片请求执行联机。终端不能执行联机。脱机交易拒绝：卡片上电 (ATR)；
i) 选择 PBOC 借记/贷记应用；
j) GET PROCESSING OPTIONS 命令；
k) VERIFY 命令；
l) 第一个 GENERATE AC 请求 TC，卡片返回 ARQC；
m) 第二个 GENERATE AC 请求 AAC，ARC=Z3；
n) 交易 4：终端请求 TC 后，卡片请求执行联机：卡片上电 (ATR)；
o) 选择 PBOC 借记/贷记应用；
p) GET PROCESSING OPTIONS 命令；
q) VERIFY 命令；
r) 第一个 GENERATE AC 请求 TC，卡片返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 1=‘1’，CVR=‘03 A4 81 00’或‘03 A0 81 00’（用于未校验 PIN）。

7.42.23 SDSB023-00

测试目的：验证对于一个脱机拒绝交易，支持 SDA（AIP 字节 1 位 7=‘1’）但认证失败，卡片设置“SDA 失败指针”位。未执行发卡行认证（不支持），验证交易联机批准。脱机交易批准，验证卡片重置“SDA 失败指针”位，不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 2，支持 SDA。

测试流程：a) 交易 1：不执行发卡行认证联机批准交易，以复位卡片中的计数器；
b) 交易 2：SDA 失败，脱机拒绝：卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7=‘1’；
g) 交易 3：未执行发卡行认证（不支持），联机批准：卡片上电 (ATR)；
h) 选择 PBOC 借记/贷记应用；
i) GET PROCESSING OPTIONS 命令；
j) VERIFY 命令；
k) 第一个 GENERATE AC 请求 ARQC；

l) 第二个 GENERATE AC 请求 TC;

m) 交易 4: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 1= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.42.24 SDSB024-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。未执行发卡行认证 (支持、可选), 验证批准交易联机。脱机交易批准, 验证卡片重置“SDA 失败指针”位, 不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 3, 支持 SDA 和发卡行认证 (可选)。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;

g) 交易 3: 未执行发卡行认证 (支持、可选), 联机批准: 卡片上电 (ATR);

h) 选择 PBOC 借记/贷记应用;

i) GET PROCESSING OPTIONS 命令;

j) VERIFY 命令;

k) 第一个 GENERATE AC 请求 ARQC;

l) 第二个 GENERATE AC 请求 TC;

m) 交易 4: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 1= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.42.25 SDSB025-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。未执行发卡行认证 (支持、必选), 验证交易联机批准。当设置“卡片请求联机指示”位时, 验证交易执行联机。验证卡片不重置“SDA 失败指针”位, 设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA、发卡行认证 (必选)。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;

g) 交易 3: 未执行发卡行认证, 联机批准: 卡片上电 (ATR);

h) 选择 PBOC 借记/贷记应用;

i) GET PROCESSING OPTIONS 命令;

j) VERIFY 命令;

- k) 第一个 GENERATE AC 请求 ARQC;
- l) 第二个 GENERATE AC 请求 TC;
- m) 交易 4: 终端请求 TC 后, 卡片请求交易执行联机: 卡片上电(ATR);
- n) 选择 PBOC 借记/贷记应用;
- o) GET PROCESSING OPTIONS 命令;
- p) VERIFY 命令;
- q) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 1= '1', CVR= '03 A4 89 00' 或 '03 A0 89 00' (用于未校验 PIN)。

7.42.26 SDSB026-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 验证卡片设置“SDA 失败指针”位。发卡行认证失败, 验证交易联机批准。当设置“卡片请求联机指示”位时, 验证交易执行联机。验证卡片不重置“SDA 失败指针”位, 设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA 和发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电(ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;
- g) 交易 3: 发卡行认证失败, 联机批准: 卡片上电(ATR);
- h) 选择 PBOC 借记/贷记应用;
- i) GET PROCESSING OPTIONS 命令;
- k) VERIFY 命令;
- l) 第一个 GENERATE AC 请求 ARQC;
- m) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- n) 第二个 GENERATE AC 请求 TC;
- o) 交易 4: 终端请求 TC 后, 卡片请求交易执行联机: 卡片上电(ATR);
- p) 选择 PBOC 借记/贷记应用;
- q) GET PROCESSING OPTIONS 命令;
- r) VERIFY 命令;
- s) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 1= '1', CVR= '03 A4 89 00' 或 '03 A0 89 00' (用于未校验 PIN)。

7.42.27 SDSB027-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。发卡行认证成功, 验证交易联机批准。验证卡片重置“SDA 失败指针”位, 不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA 和发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;
- g) 交易 3: 发卡行认证成功, 联机批准: 卡片上电 (ATR);
- h) 选择 PBOC 借记/贷记应用;
- i) GET PROCESSING OPTIONS 命令;
- j) VERIFY 命令;
- k) 第一个 GENERATE AC 请求 ARQC;
- l) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- m) 第二个 GENERATE AC 请求 TC;
- n) 交易 4: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 1= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.42.28 SDSB028-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。未执行发卡行认证 (不支持), 验证交易联机拒绝。验证交易脱机批准, 卡片重置“SDA 失败指针”位, 不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 2。

测试流程: a) 交易 1: 不执行发卡行认证联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;
- g) 交易 3: 未执行发卡行认证 (不支持), 联机拒绝: 卡片上电 (ATR);
- h) 选择 PBOC 借记/贷记应用;
- i) GET PROCESSING OPTIONS 命令;
- j) VERIFY 命令;
- k) 第一个 GENERATE AC 请求 ARQC;
- l) 第二个 GENERATE AC 请求 AAC;
- m) 交易 4: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 1= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.42.29 SDSB029-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。未执行发卡行认证 (支持、可选), 验证交易联机拒绝。验证交易脱机批准, 卡片重置“SDA 失败指针”位, 不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第9章中的卡片特征3，支持SDA和发卡行认证（可选）。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：SDA失败，脱机拒绝：卡片上电(ATR)；
c) 选择PBOC借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个GENERATE AC 请求AAC，TVR字节1位7=‘1’；
g) 交易3：未执行发卡行认证（支持且可选），联机拒绝：卡片上电(ATR)；
h) 选择PBOC借记/贷记应用；
i) GET PROCESSING OPTIONS 命令；
j) VERIFY 命令；
k) 第一个GENERATE AC 请求ARQC；
l) 第二个GENERATE AC 请求AAC；
m) 交易4：脱机批准。

通过标准：SW1 SW2=‘9000’，CID位8-7=‘01’，CVR字节2高半字节=‘9’，CVR字节3位1=‘0’，CVR=‘03 94 00 00’或‘03 90 00 00’（用于未校验PIN）。

7.42.30 SDSB030-00

测试目的：验证对于一个脱机拒绝交易，支持SDA（AIP字节1位7=‘1’）但认证失败，卡片设置“SDA失败指针”位。未执行发卡行认证（支持、必选），验证交易联机拒绝。当设置“卡片请求联机指示”位时，验证交易执行联机。验证卡片不重置“SDA失败指针”位，设置CVR的“上次交易SDA失败交易拒绝”位。

测试条件：第9章中的卡片特征1，支持SDA、发卡行认证（必选）。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：SDA失败，脱机拒绝：卡片上电(ATR)；
c) 选择PBOC借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个GENERATE AC 请求AAC，TVR字节1位7=‘1’；
g) 交易3：未执行发卡行认证，联机拒绝：卡片上电(ATR)；
h) 选择PBOC借记/贷记应用；
i) GET PROCESSING OPTIONS 命令；
j) VERIFY 命令；
k) 第一个GENERATE AC 请求ARQC；
l) 第二个GENERATE AC 请求AAC；
m) 交易4：终端请求TC后，卡片请求交易执行联机：卡片上电(ATR)；
n) 选择PBOC借记/贷记应用；
o) GET PROCESSING OPTIONS 命令；
p) VERIFY 命令；
q) 第一个GENERATE AC 请求TC，卡片返回ARQC。

通过标准：SW1 SW2=‘9000’，CID位8-7=‘10’，CVR字节2高半字节=‘A’，CVR字节3位1=‘1’，CVR=‘03 A4 89 00’或‘03 A0 89 00’（用于未校验PIN）。

7.42.31 SDSB031-00

测试目的：验证对于一个脱机拒绝交易，支持 SDA（AIP 字节 1 位 7=‘1’）但认证失败，卡片设置“SDA 失败指针”位。发卡行认证失败，验证交易联机拒绝。当设置“卡片请求联机指示”位时，验证交易执行联机。验证卡片不设置“SDA 失败指针”位，设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA 和发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 失败，脱机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7=‘1’；

g) 交易 3：发卡行认证失败，联机拒绝：卡片上电 (ATR)；

h) 选择 PBOC 借记/贷记应用；

i) GET PROCESSING OPTIONS 命令；

j) VERIFY 命令；

k) 第一个 GENERATE AC 请求 ARQC；

l) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；

m) 第二个 GENERATE AC 请求 AAC；

n) 交易 4：终端请求 TC 后，卡片请求交易执行联机：卡片上电 (ATR)；

o) 选择 PBOC 借记/贷记应用；

p) GET PROCESSING OPTIONS 命令；

q) VERIFY 命令；

r) 第一个 GENERATE AC 请求 TC，卡片返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 1=‘1’，CVR=‘03 A4 89 00’或‘03 A0 89 00’（用于未校验 PIN）。

7.42.32 SDSB032-00

测试目的：验证对于一个脱机拒绝交易，支持 SDA（AIP 字节 1 位 7=‘1’）但认证失败，卡片设置“SDA 失败指针”位。发卡行认证成功，验证交易联机拒绝。验证卡片重置“SDA 失败指针”位，不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA 和发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 失败，脱机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7=‘1’；

g) 交易 3：发卡行认证成功，联机拒绝：卡片上电 (ATR)；

h) 选择 PBOC 借记/贷记应用；

i) GET PROCESSING OPTIONS 命令；

j) VERIFY 命令；

k) 第一个 GENERATE AC 请求 ARQC；

l) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

m) 第二个 GENERATE AC 请求 AAC;

n) 交易 4: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 1= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.42.33 SDSB033-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。验证交易脱机批准, 卡片设置 CVR 的“上次交易 SDA 失败交易拒绝”位。交易脱机拒绝, 验证卡片不重置“SDA 失败指针”位, 设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;

g) 交易 3: 脱机批准;

h) 交易 4: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 1= '1', CVR= '03 84 01 00' 或 '03 80 01 00' (用于未校验 PIN)。

7.42.34 SDSB034-00

测试目的: 验证对于一个脱机拒绝交易, 支持 SDA (AIP 字节 1 位 7= '1') 但认证失败, 卡片设置“SDA 失败指针”位。发卡行认证失败, 验证交易联机批准。交易脱机拒绝, 验证卡片不重置“SDA 失败指针”位, 设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件: 第 9 章中的卡片特征 1, 支持 SDA 和发卡行认证。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: SDA 失败, 脱机拒绝: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 AAC, TVR 字节 1 位 7= '1' ;

g) 交易 3: 发卡行认证失败, 联机批准: 卡片上电 (ATR);

h) 选择 PBOC 借记/贷记应用;

i) GET PROCESSING OPTIONS 命令;

j) VERIFY 命令;

k) 第一个 GENERATE AC 请求 ARQC;

l) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;

m) 第二个 GENERATE AC 请求 TC;

n) 交易 4: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 1= '1', CVR= '03 84 89 00' 或 '03 80 89 00' (用于未校验 PIN)。

7.42.35 SDSB035-00

测试目的：验证对于一个脱机拒绝交易，支持 SDA（AIP 字节 1 位 7=‘1’）但认证失败，卡片设置“SDA 失败指针”位。发卡行认证成功，验证交易联机批准。交易脱机拒绝，验证卡片重置“SDA 失败指针”位，不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA 和发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 失败，脱机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7=‘1’；

g) 交易 3：发卡行认证成功，联机批准：卡片上电 (ATR)；

h) 选择 PBOC 借记/贷记应用；

i) GET PROCESSING OPTIONS 命令；

j) VERIFY 命令；

k) 第一个 GENERATE AC 请求 ARQC；

l) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；

m) 第二个 GENERATE AC 请求 TC；

n) 交易 4：脱机拒绝。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘00’，CVR 字节 2 高半字节=‘8’，CVR 字节 3 位 1=‘0’，CVR=‘03 84 00 00’或‘03 80 00 00’（用于未校验 PIN）。

7.42.36 SDSB036-00

测试目的：验证对于一个脱机拒绝交易，支持 SDA（AIP 字节 1 位 7=‘1’）但认证失败，卡片设置“SDA 失败指针”位。脱机交易拒绝，验证卡片设置 CVR 的“上次交易 SDA 失败交易拒绝”位。交易执行联机，验证卡片不重置“SDA 失败指针”位，设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易 2：SDA 失败，脱机拒绝：卡片上电 (ATR)；

c) 选择 PBOC 借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7=‘1’；

g) 交易 3：脱机拒绝；

h) 交易 4：终端请求执行联机：卡片上电 (ATR)；

i) 选择 PBOC 借记/贷记应用；

j) GET PROCESSING OPTIONS 命令；

k) VERIFY 命令；

l) 第一个 GENERATE AC 请求 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 1=‘1’，CVR=‘03 A4 01 00’或‘03 A0 01 00’（用于未校验 PIN）。

7.42.37 SDSB037-00

测试目的：验证对于一个脱机拒绝交易，支持 SDA（AIP 字节 1 位 7=‘1’）但认证失败，卡片设置“SDA 失败指针”位。发卡行认证成功，验证交易联机批准。交易执行联机，验证卡片重置“SDA 失败指针”位，不设置 CVR 的“上次交易 SDA 交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA 和发卡行认证。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2：SDA 失败，脱机拒绝：卡片上电 (ATR)；
- c) 选择 PBOC 借记/贷记应用；
- d) GET PROCESSING OPTIONS 命令；
- e) VERIFY 命令；
- f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7=‘1’；
- g) 交易 3：发卡行认证成功，联机批准：卡片上电 (ATR)；
- h) 选择 PBOC 借记/贷记应用；
- i) GET PROCESSING OPTIONS 命令；
- j) VERIFY 命令；
- k) 第一个 GENERATE AC 请求 ARQC；
- l) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
- m) 第二个 GENERATE AC 请求 TC；
- n) 交易 4：终端请求交易执行联机：卡片上电 (ATR)；
- o) 选择 PBOC 借记/贷记应用；
- p) GET PROCESSING OPTIONS 命令；
- q) VERIFY 命令；
- r) 第一个 GENERATE AC 请求 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 1=‘0’，CVR=‘03 A4 00 00’或‘03 A0 00 00’（用于未校验 PIN）。

7.42.38 SDSB038-00

测试目的：交易不能执行联机且 SDA 成功脱机批准，验证卡片不设置“SDA 失败指针”位。卡片强制最终的交易联机，卡片不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA，脱机批准后不重置“联机授权指示”位。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2：请求交易执行联机，但终端不能执行联机。SDA 成功，交易脱机批准：卡片上电 (ATR)；
- c) 选择 PBOC 借记/贷记应用；
- d) GET PROCESSING OPTIONS 命令；
- e) VERIFY 命令；
- f) 第一个 GENERATE AC 请求 ARQC；
- g) 第二次 GENERATE AC 请求 TC，ARC=Y3；
- h) 交易 3：终端请求脱机批准，返回 ARQC：卡片上电 (ATR)；
- i) 选择 PBOC 借记/贷记应用；
- j) GET PROCESSING OPTIONS 命令；
- k) VERIFY 命令；
- l) 第一个 GENERATE AC 请求脱机批准，返回 ARQC。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 3 位 1= ‘0’，CVR= ‘03 A4 80 00’ 或 ‘03 A0 80 00’（用于未校验 PIN）。

7.42.39 SDSB039-00

测试目的：脱机批准交易，终端不能执行联机且 SDA 成功，验证卡片不设置“SDA 失败指针”位。交易脱机拒绝，验证卡片不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA，脱机批准后不重置“联机授权指示”位。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：请求交易执行联机但终端不能执行联机，SDA 成功，交易脱机批准：卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 请求 ARQC；
g) 第二个 GENERATE AC 请求 TC，ARC=Y3；
h) 交易 3：脱机拒绝。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘00’，CVR 字节 2 高半字节= ‘8’，CVR 字节 3 位 1= ‘0’，CVR= ‘03 84 80 00’ 或 ‘03 80 00 00’（用于未校验 PIN）。

7.42.40 SDSB040-00

测试目的：脱机批准交易，交易不能执行联机且执行脱机 SDA 成功，验证卡片不设置“SDA 失败指针”位。交易执行联机，验证卡片不设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA，脱机批准后不重置“联机授权指示”位。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：请求交易执行联机，但终端不能执行联机，SDA 成功，交易脱机批准：卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 请求 ARQC；
g) 第二个 GENERATE AC 请求 TC，ARC=Y3；
h) 交易 3：终端请求交易执行联机：卡片上电 (ATR)；
i) 选择 PBOC 借记/贷记应用；
j) GET PROCESSING OPTIONS 命令；
k) VERIFY 命令；
l) 第一个 GENERATE AC 请求 ARQC。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 3 位 1= ‘0’，CVR= ‘03 A4 80 00’ 或 ‘03 A0 80 00’（用于未校验 PIN）。

7.42.41 SDSB041-00

测试目的：SDA 失败，脱机拒绝，验证卡片设置“SDA 失败指针”位。脱机批准（不能执行联机）后，指示器仍设置，而后脱机拒绝。基于设置 CVR 的“上次交易 SDA 失败交易拒绝”位来设置“SDA 失败指针”位。

测试条件：第9章中的卡片特征1，支持SDA，脱机批准后不重置“联机授权指示”位。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：SDA失败，交易脱机拒绝：卡片上电(ATR)；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个GENERATE AC 请求AAC，TVR字节1位7=‘1’；

g) 交易3：脱机批准（不能执行联机）：卡片上电(ATR)；

h) 选择PBOC借记/贷记应用；

i) GET PROCESSING OPTIONS 命令；

j) VERIFY 命令；

k) 第一个GENERATE AC 请求ARQC；

l) 第二个GENERATE AC 请求TC，ARC=Y3；

m) 交易4：脱机拒绝。

通过标准：SW1 SW2=‘9000’，CID=‘00’，CVR字节3位1=‘0’，CVR=‘03 84 81 00’或‘03 80 81 00’（用于未校验PIN）。

7.42.42 SDSB042-00

测试目的：验证对于一个脱机拒绝交易，交易不能执行联机，支持SDA（AIP字节1位7=‘1’）但认证失败，卡片设置“SDA失败指针”位。当设置“卡片请求联机指示”位时，请求交易执行联机，但终端不能执行联机，验证交易脱机批准。强制交易联机，验证卡片不重置“SDA失败指针”位，设置CVR的“上次交易SDA失败交易拒绝”位。

测试条件：第9章中的卡片特征1，支持SDA，脱机批准后重置“联机授权指示”位。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

b) 交易2：请求交易执行联机但终端不能执行联机，SDA失败，交易脱机拒绝：卡片上电(ATR)；

c) 选择PBOC借记/贷记应用；

d) GET PROCESSING OPTIONS 命令；

e) VERIFY 命令；

f) 第一个GENERATE AC 请求ARQC，TVR字节1位7=‘1’；

g) 第二个GENERATE AC 请求AAC，ARC=Z3，TVR字节1位7=‘1’；

h) 交易3：第一个GENERATE AC 终端请求TC后，卡片请求执行联机。终端不能执行联机，脱机交易批准：卡片上电(ATR)；

i) 选择PBOC借记/贷记应用；

j) GET PROCESSING OPTIONS 命令；

k) VERIFY 命令；

l) 第一个GENERATE AC 请求TC，卡片返回ARQC；

m) 第二个GENERATE AC 请求TC，ARC=Y3；

n) 交易4：终端请求脱机批准，返回ARQC：卡片上电(ATR)；

o) 选择PBOC借记/贷记应用；

p) GET PROCESSING OPTIONS 命令；

q) VERIFY 命令；

r) 第一个GENERATE AC 请求TC，卡片返回ARQC。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 3 位 1= ‘1’，CVR= ‘03 A4 81 00’ 或 ‘03 A0 81 00’（用于未校验 PIN）。

7.42.43 SDSB043-00

测试目的：验证对于一个脱机拒绝交易，支持 SDA（AIP 字节 1 位 7= ‘1’）但认证失败，卡片设置“SDA 失败指针”位。请求交易执行联机但终端不能执行联机，验证交易脱机批准。交易执行联机，验证卡片不重置“SDA 失败指针”位，设置 CVR 的“上次交易 SDA 失败交易拒绝”位。

测试条件：第 9 章中的卡片特征 1，支持 SDA，脱机批准后不重置“联机授权指示”位。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：SDA 失败，脱机交易拒绝：卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 请求 AAC，TVR 字节 1 位 7= ‘1’；
g) 交易 3：第一个 GENERATE AC，终端请求执行联机。终端不能执行联机，脱机交易批准：卡片上电 (ATR)；
h) 选择 PBOC 借记/贷记应用；
i) GET PROCESSING OPTIONS 命令；
j) VERIFY 命令；
k) 第一个 GENERATE AC 请求 ARQC；
l) 第二个 GENERATE AC 请求 TC，ARC=Y3；
m) 交易 4：终端请求交易执行联机：卡片上电 (ATR)；
n) 选择 PBOC 借记/贷记应用；
o) GET PROCESSING OPTIONS 命令；
p) VERIFY 命令；
q) 第一个 GENERATE AC 请求 ARQC。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 3 位 1= ‘1’，CVR= ‘03 A4 81 00’ 或 ‘03 A0 81 00’（用于未校验 PIN）。

7.43 UPDATE RECORD 命令 (URML)

7.43.1 URML001-00

测试目的：成功的联机批准，执行 MAC 正确的 UPDATE RECORD 命令成功。

测试条件：第 9 章中的卡片特征 1，支持 UPDATE RECORD 修改 LCOL 和 UCOL。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准，UPDATE RECORD 修改 LCOL（‘9F14’），新值=2：卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令；
g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
h) 第二个 GENERATE AC 命令；

- i) UPDATE RECORD 命令修改 LCOL, MAC 正确;
- j) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
- k) 交易 4: 联机批准, UPDATE RECORD 修改 LCOL (‘9F14’), 新值=3: 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令;
- p) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- q) 第二个 GENERATE AC 命令;
- r) UPDATE RECORD 命令修改 LCOL, MAC 正确。

通过标准: 验证交易 3 中 SFI 4, 记录 1 READ RECORD 响应: LCOL 的值 = ‘02’ (标签 ‘9F14’)。

7.43.2 URML002-00

测试目的: 成功的联机批准, 执行 MAC 错误的 UPDATE RECORD 命令。发卡行认证执行成功。修改前=03。修改后=03。

测试条件: 第 9 章中的卡片特征 1, 支持 UPDATE RECORD 修改 LCOL 和 UCOL。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 联机批准, UPDATE RECORD 修改 LCOL (‘9F14’) MAC 错误: 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 命令 ;
 - g) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 - h) 第二个 GENERATE AC 命令;
 - i) UPDATE RECORD 命令修改 LCOL, MAC 错误;
 - j) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器。

通过标准: 验证交易 3 中 SFI 4, 记录 1 的 READ RECORD 返回响应: LCOL 的值 = ‘03’ (标签 ‘9F14’)。

7.43.3 URML003-00

测试目的: 成功的联机批准, 执行无 MAC 的 UPDATE RECORD 命令。发卡行认证执行成功。修改前=03。修改后=03。

测试条件: 第 9 章中的卡片特征 1, 支持 UPDATE RECORD 修改 LCOL 和 UCOL。

- 测试流程:
- a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
 - b) 交易 2: 批准联机交易, 执行 UPDATE RECORD 命令修改 LCOL, 无 MAC: 卡片上电 (ATR);
 - c) 选择 PBOC 借记/贷记应用;
 - d) GET PROCESSING OPTIONS 命令;
 - e) VERIFY 命令;
 - f) 第一个 GENERATE AC 命令;
 - g) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
 - h) 第二个 GENERATE AC 命令;

i) UPDATE RECORD 命令修改 LCOL, 无 MAC;

g) 交易 3: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器。

通过标准: 验证交易 3 中 SFI 4, 记录 1 的 READ RECORD 返回响应: LCOL 的值 = '03' (标签 '9F14')。

7.44 执行交易金额(双货币)频度检查 (JEPJ)

7.44.1 JEPJ001-00

测试目的: 累计脱机交易金额(双货币)加本次授权金额等于累计脱机交易总金额限制(双货币)。

授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额(双货币)的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 脱机批准;

c) 交易 3: 脱机批准;

d) 交易 4: 脱机批准。

通过标准: 验证交易 4 第一个 GENERATE AC 命令返回的响应: 返回 TC, CVR = '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.44.2 JEPJ002-00

测试目的: 累计脱机交易总金额(双货币)加本次授权金额大于累计脱机交易总金额限制(双货币)。

授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额(双货币)的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 脱机批准;

c) 交易 3: 脱机批准;

d) 交易 4: 脱机批准;

e) 交易 5: 第一个 GENERATE AC 命令终端请求 TC, 卡响应联机: 卡片上电(ATR)。

f) 选择 PBOC 借记/贷记应用;

g) GET PROCESSING OPTIONS 命令;

h) VERIFY 命令;

i) 第一个 GENERATE AC 命令 请求 TC, 卡返回 ARQC。

通过标准: 验证交易 5 第一个 GENERATE AC 命令返回的响应: 返回 ARQC。CVR = '03 A4 20 00' 或 '03 A0 20 00'。

7.44.3 JEPJ003-00

测试目的: 发卡行认证成功, 联机批准交易后, 验证卡片重置累计脱机交易总金额(双货币)。

授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额(双货币)的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 脱机批准;

c) 交易 3: 脱机批准;

d) 交易 4: 脱机批准;

e) 交易 5: 联机批准: 卡片上电(ATR);

- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令 请求 TC, 卡应该返回 ARQC;
- j) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- k) 第二个 GENERATE AC 命令请求 TC;
- l) 交易 6: 脱机批准。

通过标准: 验证交易 6 第一个 GENERATE AC 命令返回的响应: 返回 TC, CVR= '03 94 00 00' 或 '03 90 00 00'。

7.44.4 JEPJ004-00

测试目的: 发卡行认证未执行(支持且要求应执行), 验证不重置累计脱机交易总金额(双货币)。
授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额(双货币)的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准;
- d) 交易 4: 脱机批准;
- e) 交易 5: 联机拒绝: 卡片上电(ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令请求 TC, 卡返回 ARQC;
- j) 第二个 GENERATE AC 命令请求 AAC;
- k) 交易 6: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电(ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC。

通过标准: 验证交易 6 第一个 GENERATE AC 命令返回的响应: 返回 ARQC, CVR= '03 A4 A8 00' 或 '03 A0 A8 00'。

7.44.5 JEPJ005-00

测试目的: 联机批准交易中, 支持发卡行认证且要求强制执行, 但未执行发卡行认证, 验证不重置累计脱机交易总金额(双货币)。授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额(双货币)的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准;
- d) 交易 4: 脱机批准;
- e) 交易 5: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电(ATR);

- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令 请求 TC, 卡返回 ARQC;
- j) 第二个 GENERATE AC 命令 请求 TC;
- k) 交易 6: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- o) 第一个 GENERATE AC 命令请求 TC。

通过标准: 验证交易 6 第一个 GENERATE AC 返回的响应: 返回 ARQC, CVR= '03 A4 A8 00' 或 '03 A0 A8 00'。

7.44.6 JEPJ006-00

测试目的: 联机拒绝交易中, 发卡行认证执行失败, 验证不重置累计脱机交易总金额 (双货币)。
授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额 (双货币) 的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准;
- d) 交易 4: 脱机批准;
- e) 交易 5: 联机拒绝: 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC;
- j) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- k) 第二个 GENERATE AC 命令请求 AAC;
- l) 交易 6: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC。

通过标准: 验证交易 6 第一个 GENERATE AC 命令返回的响应: 返回 ARQC, CVR= '03 A4 A8 00' 或 '03 A0 A8 00'。

7.44.7 JEPJ007-00

测试目的: 联机批准交易中, 发卡行认证执行失败, 验证不重置累计脱机交易总金额 (双货币)。
授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额 (双货币) 的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准;
- d) 交易 4: 脱机批准;
- e) 交易 5: 联机批准: 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC;
- j) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC 命令;
- k) 第二个 GENERATE AC 命令请求 TC;
- l) 交易 6: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令。

通过标准: 验证交易 6 第一个 GENERATE AC 命令返回的响应: 返回 ARQC, CVR= '03 A4 A8 00' 或 '03 A0 A8 00'。

7.44.8 JEPJ008-00

测试目的: 如果交易货币代码等于第二应用货币代码, 验证累计脱机交易总金额 (双重货币) 加上转换金额没有超过累计脱机交易总金额限制 (双货币)。转换金额=52.50。授权金额=¥30.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额 (双货币) 的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准。

通过标准: 验证交易 3 第一个 GENERATE AC 命令返回的响应: 返回 TC, CVR= '03 94 00 00' 或 '03 90 00 00'。

7.44.9 JEPJ009-00

测试目的: 如果交易货币代码等于第二应用货币代码, 验证累计脱机交易总金额 (双货币) 加上转换金额大于累计脱机交易总金额限制 (双货币)。转换金额=52.50。授权金额=¥30.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额 (双货币) 的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准;
- d) 交易 4: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡响应联机: 卡片上电 (ATR);
- e) 选择 PBOC 借记/贷记应用;
- f) GET PROCESSING OPTIONS 命令;
- g) VERIFY 命令;
- h) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC。

通过标准：验证交易 4 第一个 GENERATE AC 命令返回的响应：返回 ARQC, CVR= ‘03 A4 20 00’ 或 ‘03 A0 20 00’。

7.44.10 JEPJ010-00

测试目的：如果交易货币代码等于第二应用货币代码，对于脱机交易拒绝，验证累计脱机交易总金额（双货币）加上转换金额等于累计脱机交易总金额限制（双货币）。转换金额=52.50。授权金额=¥30.00。

测试条件：第 9 章中的卡片特征 5，交易金额（双货币）的频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：脱机拒绝；
c) 交易 3：脱机拒绝。

通过标准：验证交易 3 第一个 GENERATE AC 命令返回的响应：返回 AAC, CVR= ‘03 84 00 00’ 或 ‘03 80 00 00’（用于未校验 PIN）。

7.44.11 JEPJ011-00

测试目的：验证累计脱机交易总金额（双货币）加上转换金额没有超过累计脱机交易总金额限制（双货币）。转换金额=52.50。授权金额=¥30.00。

测试条件：第 9 章中的卡片特征 5，交易金额（双货币）的频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：联机批准：卡片上电 (ATR)；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 命令请求 ARQC；
g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC 命令；
h) 第二个 GENERATE AC 命令请求 TC；
i) 交易 3：联机批准：卡片上电 (ATR)；
j) 选择 PBOC 借记/贷记应用；
k) GET PROCESSING OPTIONS 命令；
l) VERIFY 命令；
m) 第一个 GENERATE AC 命令请求 ARQC；
n) EXTERNAL AUTHENTICATE 命令，正确的 ARPC 命令；
o) 第二个 GENERATE AC 命令请求 TC；
p) 交易 4：脱机批准。

通过标准：验证交易 4 第一个 GENERATE AC 命令返回的响应：返回 TC, CVR= ‘03 94 00 00’ 或 ‘03 90 00 00’（用于未校验 PIN）。

7.44.12 JEPJ012-00

测试目的：脱机拒绝交易（国际），验证累计脱机交易总金额（双货币）没有加上授权金额。授权金额=¥50.00。

测试条件：第 9 章中的卡片特征 5，交易金额（双货币）的频度检查，在脱机拒绝后累计金额没有增加。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；

- b) 交易 2: 脱机拒绝;
- c) 交易 3: 脱机拒绝;
- d) 交易 4: 脱机拒绝;
- e) 交易 5: 在第一个 GENERATE AC 命令中, 卡接受 TC: 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 TC。

通过标准: 验证交易 5 第一个 GENERATE AC 命令返回的响应: 返回 TC, CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.44.13 JEPJ013-00

测试目的: 交易不能联机且脱机拒绝时, 验证累计脱机交易总金额 (双货币) 应不增加。
授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额 (双货币) 的频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 无法联机执行交易: 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC;
- g) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- h) 交易 3: 无法联机执行交易: 卡片上电 (ATR);
- i) 选择 PBOC 借记/贷记应用;
- j) GET PROCESSING OPTIONS 命令;
- k) VERIFY 命令;
- l) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC;
- m) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- n) 交易 4: 无法联机执行交易: 卡片上电 (ATR);
- o) 选择 PBOC 借记/贷记应用;
- p) GET PROCESSING OPTIONS 命令;
- q) VERIFY 命令;
- r) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC;
- s) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- t) 交易 5: 无法联机执行交易: 卡片上电 (ATR);
- u) 选择 PBOC 借记/贷记应用;
- v) GET PROCESSING OPTIONS 命令;
- w) VERIFY 命令;
- x) 第一个 GENERATE AC 命令请求 AAC, 卡应该返回 ARQC;
- y) 第二个 GENERATE AC 命令请求 AAC, ARC=Z3;
- z) 交易 6: 第一次 GENERATE AC 终端请求 TC, 卡片请求执行联机: 卡片上电 (ATR);
- aa) 选择 PBOC 借记/贷记应用;
- ab) GET PROCESSING OPTIONS 命令;

ac) VERIFY 命令;

ad) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC。

通过标准: 验证交易 6 第一个 GENERATE AC 返回的响应: 返回 ARQC, CVR= '03 A4 80 00' 或 '03 A0 80 00' (用于未校验 PIN)。

7.44.14 JEPJ014-00

测试目的: 交易不能联机且脱机批准时, 验证累计脱机交易总金额(双货币)增加。

授权金额=¥50.00。

测试条件: 第 9 章中的卡片特征 5, 交易金额(双货币)的频度检查, 脱机批准后不重置“联机授权指示”位。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 无法联机执行交易: 卡片上电(ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 ARQC;

g) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;

h) 交易 3: 无法联机执行交易: 卡片上电(ATR);

i) 选择 PBOC 借记/贷记应用;

j) GET PROCESSING OPTIONS 命令;

k) VERIFY 命令;

l) 第一个 GENERATE AC 命令请求 ARQC;

m) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;

n) 交易 4: 无法联机执行交易: 卡片上电(ATR);

o) 选择 PBOC 借记/贷记应用;

p) GET PROCESSING OPTIONS 命令;

q) VERIFY 命令;

r) 第一个 GENERATE AC 命令请求 ARQC;

s) 第二个 GENERATE AC 命令请求 TC, ARC=Y3;

t) 交易 5: 第一次 GENERATE AC 终端请求 TC, 卡片请求执行联机: 卡片上电(ATR);

u) 选择 PBOC 借记/贷记应用;

v) GET PROCESSING OPTIONS 命令;

w) VERIFY 命令;

x) 第一个 GENERATE AC 命令请求 TC, 卡返回 ARQC。

通过标准: 验证交易 5 第一个 GENERATE AC 命令返回的响应: 返回 ARQC, CVR= '03 A4 A0 00' 或 '03 A0 A0 00' (用于未校验 PIN)。

7.45 执行国际国家频度检查 (GGPJ)

7.45.1 GGPJ001-00

测试目的: 验证当连续交易限制(国际—国家)超出时, 卡请求联机批准。并验证 CVR 相应位被设置表明频度检查超出。

测试条件: 第 9 章中的卡片特征 25, 支持连续脱机国际交易金额总计(基于国家)频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准;
- d) 交易 4: 脱机批准;
- e) 交易 5: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC。

通过标准: 验证交易 5 第一个 GENERATE AC 命令返回的响应: 返回 TC, CVR= '03 A4 20 00' 或 '03 A0 20 00' (用于未校验 PIN)。

7.45.2 GGPJ002-00

测试目的: 验证如果发卡行认证成功执行且交易拒绝, 不重置连续交易计数器 (国际—国家)。

测试条件: 第 9 章中的卡片特征 25, 支持连续脱机国际交易金额总计 (基于国家) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准;
- d) 交易 4: 脱机批准;
- e) 交易 5: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC;
- j) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- k) 第二个 GENERATE AC 命令请求 AAC ;
- l) 交易 6: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC。

通过标准: 验证交易 5 第一个 GENERATE AC 命令返回的响应: 返回 ARQC。验证交易 6 第一个 GENERATE AC 命令返回的响应: 返回 ARQC, CVR= '03 A4 20 00' 或 '03 A0 20 00' (用于未校验 PIN)。

7.45.3 GGPJ003-00

测试目的: 验证如果发卡行认证 (可选) 没有执行且交易批准, 重置连续交易计数器 (国际—国家)。

测试条件: 第 9 章中的卡片特征 26, 支持连续脱机国际交易金额总计 (基于国家) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;

- c) 交易 3: 脱机批准;
- d) 交易 4: 脱机批准;
- e) 交易 5: 在第一个 GENERATE AC 命令终端请求 TC 时, 卡请求联机执行: 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 命令请求 TC, 卡应该返回 ARQC ;
- j) 第二个 GENERATE AC 命令请求 TC;
- k) 交易 6: 脱机批准。

通过标准: 验证交易 5 第一个 GENERATE AC 命令返回的响应: 返回 ARQC。验证交易 6 第一个 GENERATE AC 命令返回的响应: 返回 TC, CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.46 执行指定货币交易金额检查 (JEJC)

7.46.1 JEJC001-00

测试目的: 在联机批准交易后, 对于第二个脱机国内交易, 验证累计交易总计金额加上授权金额没有超过累计交易金额限制。第三个脱机交易 (交易 4) 是一个批准的脱机国际交易。如果交易货币代码与应用货币代码不同, 验证卡应该不检查累计交易总计金额加上授权金额超过累计交易总计金额限制。卡片应该不设置 CVR 中的“超过频率检查”位。累计交易总计金额限制是¥100.00。

测试条件: 第 9 章中的卡片特征 7, 支持指定货币的交易金额频度检查

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 带有交易金额为¥50.00 的脱机批准 (国内): 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码相同), 授权金额为¥50.00;

g) 交易 3: 带有交易金额为¥50.00 的脱机批准 (国内): 卡片上电 (ATR);

h) 选择 PBOC 借记/贷记应用;

i) GET PROCESSING OPTIONS 命令;

j) VERIFY 命令 命令;

k) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码相同), 授权金额为¥50.00;

l) 交易 4: 带有交易金额为 £ 50.00 的脱机批准 (国际): 卡片上电 (ATR);

m) 选择 PBOC 借记/贷记应用;

n) GET PROCESSING OPTIONS 命令;

o) VERIFY 命令;

p) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码相同), 授权金额为¥50.00。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 6= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.46.2 JEJC002-00

测试目的：在联机批准交易后，对于第三个脱机国内交易，验证累积交易总计金额加上授权金额超过累计交易总金额限制。验证卡片请求第三笔脱机国内交易（交易4）执行联机。如果累积交易总计金额加上授权金额超过累计交易总计界限，验证卡片应该设置CVR中的“超过频率检查”位。累积交易总计金额限制是¥100.00。

测试条件：第9章中的卡片特征7，支持指定货币的交易金额频度检查。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：带有交易金额为¥50.00的脱机批准（国内）：卡片上电(ATR)；
c) 选择PBOC借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个GENERATE AC 命令请求TC（交易货币代码与应用货币代码相同），授权金额为¥50.00；
g) 交易3：带有交易金额为¥50.00的脱机批准（国内）：卡片上电(ATR)；
h) 选择PBOC借记/贷记应用；
i) GET PROCESSING OPTIONS 命令；
j) VERIFY 命令；
k) 第一个GENERATE AC 命令请求TC（交易货币代码与应用货币代码相同），授权金额为¥50.00；
l) 交易4：终端在第一个GENERATE AC 请求TC（交易货币代码与应用货币代码相同），卡片请求联机，交易金额为¥50.00：卡片上电(ATR)；
m) 选择PBOC借记/贷记应用；
n) GET PROCESSING OPTIONS 命令；
o) VERIFY 命令；
p) 终端在第一个GENERATE AC 请求TC（交易货币代码与应用货币代码相同），授权金额为¥50.00，卡应该返回ARQC。

通过标准：SW1 SW2=‘9000’，CID位8-7=‘10’，CVR字节2高半字节=‘A’，CVR字节3位6=‘1’，CVR=‘03 A4 20 00’或‘03 A0 20 00’（用于未校验PIN）。

7.46.3 JEJC003-00

测试目的：对于脱机拒绝国内交易，验证累计交易总金额没有增加。累计交易总金额界限是¥100.00。

测试条件：第9章中的卡片特征7，支持指定货币的交易金额频度检查，对于脱机拒绝累计金额不增加。

测试流程：a) 交易1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易2：带有交易金额为¥50.00的脱机拒绝（国内）：卡片上电(ATR)；
c) 选择PBOC借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个GENERATE AC 命令请求AAC（交易货币代码与应用货币代码相同），授权金额为¥50.00；
g) 交易3：带有交易金额为¥50.00的脱机批准（国内）：卡片上电(ATR)；
h) 选择PBOC借记/贷记应用；

- i) GET PROCESSING OPTIONS 命令;
- j) VERIFY 命令 ;
- k) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码相同), 授权金额为¥50.00;
- l) 交易 4: 带有交易金额为¥50.00 的脱机拒绝 (国内): 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令 ;
- p) 第一个 GENERATE AC 命令请求 AAC (交易货币代码与应用货币代码相同), 授权金额为¥50.00。

通过标准: SW1 SW2= '9000', CID= '00', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.47 执行国际-货币频度检查 9F53=05 (GHJC)

7.47.1 GHJC001-00

测试目的: 验证在联机批准交易后, 对于第五个脱机国际交易, 连续交易计数器加上 1 没有超过连续脱机交易限制 (国际)。第六个脱机交易 (交易 7) 是一个批准的脱机国内交易。验证如果交易货币代码与应用货币代码相同, 卡片应该不设置 CVR 中的“超过频率检查”位。连续脱机交易限制 (国际) 是 5。

测试条件: 第 9 章中的卡片特征 7, 支持累计连续国际交易 (基于货币) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准 (国际): 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- g) 交易 3: 脱机批准 (国际): 卡片上电 (ATR);
- h) 选择 PBOC 借记/贷记应用;
- i) GET PROCESSING OPTIONS 命令;
- j) VERIFY 命令;
- k) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- l) 交易 4: 脱机批准 (国际): 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- q) 交易 5: 脱机批准 (国际): 卡片上电 (ATR);
- r) 选择 PBOC 借记/贷记应用;
- s) GET PROCESSING OPTIONS 命令;
- t) VERIFY 命令;
- u) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- v) 交易 6: 脱机批准 (国际): 卡片上电 (ATR);
- w) 选择 PBOC 借记/贷记应用;

- x) GET PROCESSING OPTIONS 命令;
- y) VERIFY 命令;
- z) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- aa) 交易 7: 脱机批准 (国内): 卡片上电 (ATR);
- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) VERIFY 命令;
- ae) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码相同)。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 6= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.47.2 GHJC002-00

测试目的: 验证在联机批准交易后, 对于第六个脱机国际交易, 连续交易计数器加上 1 超过连续脱机交易限制 (国际)。验证卡片请求第六个脱机国际交易 (交易 7) 执行联机。验证如果交易货币代码与应用货币代码不同, 卡应该设置 CVR 中的“超过频率检查”位。连续脱机交易限制 (国际) 是 5。

测试条件: 第 9 章中的卡片特征 7, 支持累计连续国际交易 (基于货币) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准 (国际): 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- g) 交易 3: 脱机批准 (国际): 卡片上电 (ATR);
- h) 选择 PBOC 借记/贷记应用;
- i) GET PROCESSING OPTIONS 命令;
- j) VERIFY 命令;
- k) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- l) 交易 4: 脱机批准 (国际): 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- q) 交易 5: 脱机批准 (国际): 卡片上电 (ATR);
- r) 选择 PBOC 借记/贷记应用;
- s) GET PROCESSING OPTIONS 命令;
- t) VERIFY 命令;
- u) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- v) 交易 6: 脱机批准 (国际): 卡片上电 (ATR);
- w) 选择 PBOC 借记/贷记应用;
- x) GET PROCESSING OPTIONS 命令;
- y) VERIFY 命令;
- z) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);

- aa) 交易 7: 终端在第一个 GENERATE AC 请求 TC (交易货币代码与应用货币代码不同), 卡请求联机: 卡片上电 (ATR);
- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) VERIFY 命令;
- ae) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同), 卡应该返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 6= '1', CVR= '03 A4 20 00' 或 '03 A0 20 00' (用于未校验 PIN)。

7.47.3 GHJC003-00

测试目的: 验证在联机批准交易后, 对于第五个脱机国际交易, 连续交易计数器加上 1 没有超过连续脱机交易限制 (国际)。第六个脱机交易 (交易 7) 是脱机拒绝国内交易。验证如果交易货币代码与应用货币代码相同, 卡不应该设置 CVR 中的“超过频率检查”位。连续脱机交易限制 (国际) 是 5。

测试条件: 第 9 章中的卡片特征 7, 支持累计连续国际交易 (基于货币) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准 (国际): 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- g) 交易 3: 脱机批准 (国际): 卡片上电 (ATR);
- h) 选择 PBOC 借记/贷记应用;
- i) GET PROCESSING OPTIONS 命令;
- j) VERIFY 命令;
- k) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- l) 交易 4: 脱机批准 (国际): 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- q) 交易 5: 脱机批准 (国际): 卡片上电 (ATR);
- r) 选择 PBOC 借记/贷记应用;
- s) GET PROCESSING OPTIONS 命令;
- t) VERIFY 命令;
- u) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- v) 交易 6: 脱机批准 (国际): 卡片上电 (ATR);
- w) 选择 PBOC 借记/贷记应用;
- x) GET PROCESSING OPTIONS 命令;
- y) VERIFY 命令;
- z) 第一个 AC 请求 TC (交易货币代码与应用货币代码不同);
- aa) 交易 7: 脱机拒绝 (国内): 卡片上电 (ATR);

- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) VERIFY 命令;
- ae) 第一个 GENERATE AC 命令请求 AAC (交易货币代码与应用货币代码相同)。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 6= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.47.4 GHJC004-00

测试目的: 验证在联机批准交易后, 对于第六个脱机国际交易, 连续交易计数器加上 1 超过连续脱机交易限制 (国际)。验证如果第六个脱机国际交易 (交易 7) 是脱机拒绝的, 且交易货币代码与应用货币代码不同, 卡应该设置 CVR 中的“超过频率检查”位。连续脱机交易限制 (国际) 是 5。

测试条件: 第 9 章中的卡片特征 7, 支持累计连续国际交易 (基于货币) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准 (国际): 卡片上电 (ATR);
- c) 选择 PBOC 借记/贷记应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令;
- f) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- g) 交易 3: 脱机批准 (国际): 卡片上电 (ATR);
- h) 选择 PBOC 借记/贷记应用;
- i) GET PROCESSING OPTIONS 命令;
- j) VERIFY 命令;
- k) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- l) 交易 4: 脱机批准 (国际): 卡片上电 (ATR);
- m) 选择 PBOC 借记/贷记应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- q) 交易 5: 脱机批准 (国际): 卡片上电 (ATR);
- l) 选择 PBOC 借记/贷记应用;
- m) GET PROCESSING OPTIONS 命令;
- n) VERIFY 命令;
- u) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- v) 交易 6: 脱机批准 (国际): 卡片上电 (ATR);
- w) 选择 PBOC 借记/贷记应用;
- x) GET PROCESSING OPTIONS 命令;
- y) VERIFY 命令;
- z) 第一个 GENERATE AC 命令请求 TC (交易货币代码与应用货币代码不同);
- aa) 交易 7: 交易货币代码与应用货币代码不同的脱机拒绝: 卡片上电 (ATR);
- ab) 选择 PBOC 借记/贷记应用;
- ac) GET PROCESSING OPTIONS 命令;
- ad) VERIFY 命令;

ae) 第一个 GENERATE AC 命令请求 AAC (交易货币代码与应用货币代码不同)。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 6= '1', CVR= '03 84 20 00' 或 '03 80 20 00' (用于未校验 PIN)。

7.48 连续脱机交易检查 (LTJC)

7.48.1 LTJC001-00

测试目的: 联机批准后, 验证对于一个脱机交易, ATC 和 LOATC 之间的差比 LCOL 小。当 ATC 与 LOATC 之间的差比 LCOL 小时, 验证卡不设置 CVR 中的“超过频率检查”位。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 6= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.48.2 LTJC002-00

测试目的: 联机批准后, 验证对于三个脱机交易, ATC 和 LOATC 之间的差比 LCOL 小。

当 ATC 与 LOATC 之间的差比 LCOL 小或相等时, 验证卡不设置 CVR 中的“超过频率检查”位。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 6= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.48.3 LTJC003-00

测试目的: 联机批准后, 验证对于第四个脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。

当 ATC 与 LOATC 之间的差比 LCOL 大于时, 验证卡不设置 CVR 中的“超过频率检查”位, 并请求联机。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 脱机批准;
e) 交易 5: 在终端第一次 GENERATE AC 请求 TC 后, 卡请求联机: 卡片上电 (ATR);
f) 选择 PBOC 借记/贷记应用;
g) GET PROCESSING OPTIONS 命令;
h) VERIFY 命令;
i) 第一次 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 6= '1', CVR= '03 A4 20 00' 或 '03 A0 20 00' (用于未校验 PIN)。

7.48.4 LTJC004-00

测试目的：联机批准后，验证对于一个连续的脱机交易，ATC 和 LOATC 之间的差大于 LCOL。

当 ATC 与 LOATC 之间的差比 LCOL 要大时，验证卡设置 CVR 中的“超过频率检查”位，并请求联机。LCOL 值为 0。

测试条件：第 9 章中的卡片特征 6，支持累计连续脱机交易（下限）频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：在终端第一次 GENERATE AC 请求 TC 后，卡请求联机：卡片上电（ATR）；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一次 GENERATE AC 请求 TC，卡片返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 6=‘1’，CVR=‘03 A4 20 00’或‘03 A0 20 00’（用于未校验 PIN）。

7.48.5 LTJC005-00

测试目的：联机批准后，验证对于第四个连续的脱机交易，ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时，验证卡设置 CVR 中的“超过频率检查”位，并请求联机。卡请求第四个脱机交易（交易 5）联机执行，交易 5 发卡行认证成功，但联机拒绝。验证卡不更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件：第 9 章中的卡片特征 1，支持累计连续脱机交易（下限）频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：脱机批准；
c) 交易 3：脱机批准；
d) 交易 4：脱机批准；
e) 交易 5：在终端第一次 GENERATE AC 请求 TC 后，卡请求联机。交易的发卡行认证成功，但联机拒绝：卡片上电（ATR）；
f) 选择 PBOC 借记/贷记应用；
g) GET PROCESSING OPTIONS 命令；
h) VERIFY 命令；
i) 第一次 GENERATE AC 请求 TC，卡片返回 ARQC；
j) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
k) 第二次 GENERATE AC 请求 AAC；
l) 交易 6：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机：卡片上电（ATR）；
m) 选择应用；
n) GET PROCESSING OPTIONS 命令；
o) VERIFY 命令；
p) 第一次 GENERATE AC 请求 TC，卡片返回 ARQC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘10’，CVR 字节 2 高半字节=‘A’，CVR 字节 3 位 6=‘1’，CVR=‘03 A4 20 00’或‘03 A0 20 00’（用于未校验 PIN）。

7.48.6 LTJC006-00

测试目的：联机批准后，验证对于一个连续的脱机交易，ATC 和 LOATC 之间的差比 LCOL 要大。

当 ATC 与 LOATC 之间的差比 LCOL 要大时，验证卡设置 CVR 中的“超过频率检查”位，

并请求联机。卡请求脱机交易（交易 2）联机执行，交易 2 发卡行认证成功，但联机拒绝。验证卡不更新 LOATC 为当前 ATC 的值。LCOL 值为 0。

测试条件：第 9 章中的卡片特征 6，支持发卡行认证，支持累计连续脱机交易（下限）频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机。交易的发卡行认证成功，但联机拒绝：卡片上电（ATR）；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一次 GENERATE AC 请求 TC，卡片返回 ARQC；
g) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
h) 第二次 GENERATE AC 请求 AAC；
i) 交易 3：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机：卡片上电（ATR）。
j) 选择应用；
k) GET PROCESSING OPTIONS 命令；
l) VERIFY 命令；
m) 第一次 GENERATE AC 请求 TC，卡片返回 ARQC。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '10'，CVR 字节 2 高半字节= 'A'，CVR 字节 3 位 6= '1'，CVR= '03 A4 20 00' 或 '03 A0 20 00'（用于未校验 PIN）。

7.48.7 LTJC007-00

测试目的：联机批准后，验证对于第四个连续的脱机交易，ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时，验证卡设置 CVR 中的“超过频率检查”位，并请求联机。卡请求第四个脱机交易（交易 5）联机执行，交易 5 发卡行认证成功，联机批准。验证卡更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证，支持累计连续脱机交易（下限）频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：脱机批准；
c) 交易 3：脱机批准；
d) 交易 4：脱机批准；
e) 交易 5：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机。交易的发卡行认证成功，联机批准：卡片上电（ATR）；
f) 选择 PBOC 借记/贷记应用；
h) GET PROCESSING OPTIONS 命令；
i) VERIFY 命令；
j) 第一次 GENERATE AC 请求 TC，卡片返回 ARQC；
k) EXTERNAL AUTHENTICATE 命令，正确的 ARPC；
l) 第二次 GENERATE AC 请求 TC；
m) 交易 6：脱机批准。

通过标准：SW1 SW2= '9000'，CID 位 8-7= '01'，CVR 字节 2 高半字节= '9'，CVR 字节 3 位 6= '0'，CVR= '03 94 00 00' 或 '03 90 00 00'（用于未校验 PIN）。

7.48.8 LTJC008-00

测试目的：联机批准后，验证对于第四个连续的脱机交易，ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时，验证卡设置 CVR 中的“超过频率检查”位，并请求联机。卡请求第四个脱机交易（交易 5）联机执行，交易 5 发卡行认证失败，联机批准。验证卡不更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件：第 9 章中的卡片特征 1，支持发卡行认证，支持累计连续脱机交易（下限）频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：脱机批准；
c) 交易 3：脱机批准；
d) 交易 4：脱机批准；
e) 交易 5：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机。交易的发卡行认证不成功，联机批准：卡片上电（ATR）；
f) 选择 PBOC 借记/贷记应用；
g) GET PROCESSING OPTIONS 命令；
h) VERIFY 命令；
i) 第一个 GENERATE AC 请求 TC，卡片返回 ARQC；
j) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；
k) 第二次 GENERATE AC 请求 TC；
l) 交易 6：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机：卡片上电（ATR）；
m) 选择 PBOC 借记/贷记应用；
n) GET PROCESSING OPTIONS 命令；
o) VERIFY 命令；
p) 第一次 GENERATE AC 请求 TC，卡片返回 ARQC。

通过标准：SW1 SW2= ‘9000’，CID 位 8-7= ‘10’，CVR 字节 2 高半字节= ‘A’，CVR 字节 3 位 6= ‘1’，CVR= ‘03 A4 A8 00’ 或 ‘03 A0 A8 00’（用于未校验 PIN）。

7.48.9 LTJC009-00

测试目的：联机批准后，验证对于一个连续的脱机交易，ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时，验证卡设置 CVR 中的“超过频率检查”位，并请求联机。卡请求连续脱机交易（交易 2）联机执行，交易 2 发卡行认证失败，联机批准。验证卡不更新 LOATC 为当前 ATC 的值。LCOL 值为 0。

测试条件：第 9 章中的卡片特征 6，支持发卡行认证，支持累计连续脱机交易（下限）频度检查。

测试流程：a) 交易 1：执行发卡行认证成功的联机批准交易，以复位卡片中的计数器；
b) 交易 2：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机。交易的发卡行认证不成功，联机批准：卡片上电（ATR）；
c) 选择 PBOC 借记/贷记应用；
d) GET PROCESSING OPTIONS 命令；
e) VERIFY 命令；
f) 第一个 GENERATE AC 请求 TC，卡片返回 ARQC；
g) EXTERNAL AUTHENTICATE 命令，错误的 ARPC；
h) 第二个 GENERATE AC 请求 TC；
i) 交易 3：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机：卡片上电（ATR）；
j) 选择 PBOC 借记/贷记应用；
k) GET PROCESSING OPTIONS 命令；

l) VERIFY 命令;

m) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 6= '1', CVR= '03 A4 A8 00' 或 '03 A0 A8 00' (用于未校验 PIN)。

7.48.10 LTJC010-00

测试目的: 联机批准后, 验证对于第四个连续的脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求第四个脱机交易 (交易 5) 联机执行, 交易 5 没有执行发卡行认证 (支持并强制), 联机批准。验证卡不更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 发卡行认证强制, 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 脱机批准;

c) 交易 3: 脱机批准;

d) 交易 4: 脱机批准;

e) 交易 5: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机。交易没有执行发卡行认证 (支持并强制), 联机批准: 卡片上电 (ATR);

f) 选择 PBOC 借记/贷记应用;

g) GET PROCESSING OPTIONS 命令;

h) VERIFY 命令;

i) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;

j) 第二个 GENERATE AC 请求 TC;

k) 交易 6: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机: 卡片上电 (ATR);

l) 选择 PBOC 借记/贷记应用;

m) GET PROCESSING OPTIONS 命令;

n) VERIFY 命令;

o) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 6= '1', CVR= '03 A4 A8 00' 或 '03 A0 A8 00' (用于未校验 PIN)。

7.48.11 LTJC011-00

测试目的: 联机批准后, 验证对于一个连续脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。

当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求连续脱机交易 (交易 2) 联机执行, 交易 2 没有执行发卡行认证 (支持并强制), 联机批准。验证卡不更新 LOATC 为当前 ATC 的值。LCOL 值为 0。

测试条件: 第 9 章中的卡片特征 6, 支持发卡行认证, 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

b) 交易 2: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机。交易没有执行发卡行认证 (支持并强制), 联机批准: 卡片上电 (ATR);

c) 选择 PBOC 借记/贷记应用;

d) GET PROCESSING OPTIONS 命令;

e) VERIFY 命令;

f) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;

- g) 第二个 GENERATE AC 请求 TC;
- h) 交易 3: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机: 卡片上电 (ATR);
- i) 选择 PBOC 借记/贷记应用;
- j) GET PROCESSING OPTIONS 命令;
- k) VERIFY 命令;
- l) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC。

通过标准: SW1 SW2= '9000', CID 位 8-7= '10', CVR 字节 2 高半字节= 'A', CVR 字节 3 位 6= '1', CVR= '03 A4 A8 00' 或 '03 A0 A8 00' (用于未校验 PIN)。

7.48.12 LTJC012-00

测试目的: 联机批准后, 验证对于第四个连续脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求第四个脱机交易 (交易 5) 联机执行, 交易 5 没有执行发卡行认证 (支持或可选), 联机批准。验证卡更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 发卡行认证可选, 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 脱机批准;
e) 交易 5: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机。交易没有执行发卡行认证 (支持且可选), 联机批准: 卡片上电 (ATR);
f) 选择 PBOC 借记/贷记应用;
g) GET PROCESSING OPTIONS 命令;
h) VERIFY 命令;
i) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;
j) 第二个 GENERATE AC 请求 TC;
k) 交易 6: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 6= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.48.13 LTJC013-00

测试目的: 一个批准联机交易后, 验证对于第四个连续脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求第四个脱机交易 (交易 5) 联机执行, 交易 5 没有执行发卡行认证 (不支持), 联机批准。验证卡更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 2, 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 脱机批准;
e) 交易 5: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机。交易没有执行发卡行认证 (不支持), 联机批准: 卡片上电 (ATR);
f) 选择 PBOC 借记/贷记应用;

- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;
- j) 第二个 GENERATE AC 请求 TC;
- k) 交易 6: 脱机批准。

通过标准: SW1 SW2= '9000', CID 位 8-7= '01', CVR 字节 2 高半字节= '9', CVR 字节 3 位 6= '0', CVR= '03 94 00 00' 或 '03 90 00 00' (用于未校验 PIN)。

7.48.14 LTJC014-00

测试目的: 一个批准联机交易后, 验证对于三个连续的脱机交易, ATC 和 LOATC 之间的差比 LCOL 小。当 ATC 与 LOATC 之间的差比 LCOL 小或相等时, 验证卡不设置 CVR 中的“超过频率检查”位, 并请求联机。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 支持累计连续脱机交易(下限)频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 6= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.48.15 LTJC015-00

测试目的: 联机批准后, 验证对于第四个连续的脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。第四个连续的脱机交易脱机拒绝。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 支持累计连续脱机交易(下限)频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 脱机批准;
e) 交易 5: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 6= '1', CVR= '03 84 20 00' 或 '03 80 20 00' (用于未校验 PIN)。

7.48.16 LTJC016-00

测试目的: 一个批准联机交易后, 验证对于第四个连续的脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求第四个脱机交易(交易 5)联机执行, 交易 5 发卡行认证成功, 联机批准。交易 6 脱机拒绝。验证卡更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证, 支持累计连续脱机交易(下限)频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;

- d) 交易 4: 脱机批准;
- e) 交易 5: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机。交易发卡行认证成功, 联机批准: 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;
- j) EXTERNAL AUTHENTICATE 命令, 正确的 ARPC;
- k) 第二个 GENERATE AC 请求 TC;
- l) 交易 6: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 6= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.48.17 LTJC017-00

测试目的: 一个批准联机交易后, 验证对于第四个连续的脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求第四个脱机交易 (交易 5) 联机执行, 交易 5 发卡行认证不成功, 联机批准。交易 6 脱机拒绝。验证卡不更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证, 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;

- b) 交易 2: 脱机批准;
- c) 交易 3: 脱机批准;
- d) 交易 4: 脱机批准;
- e) 交易 5: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机。交易发卡行认证不成功, 联机批准: 卡片上电 (ATR);
- f) 选择 PBOC 借记/贷记应用;
- g) GET PROCESSING OPTIONS 命令;
- h) VERIFY 命令;
- i) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;
- j) EXTERNAL AUTHENTICATE 命令, 错误的 ARPC;
- k) 第二个 GENERATE AC 请求 TC;
- l) 交易 6: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 6= '1', CVR= '03 84 A8 00' 或 '03 80 A8 00' (用于未校验 PIN)。

7.48.18 LTJC018-00

测试目的: 一个批准联机交易后, 验证对于第四个连续的脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求第四个脱机交易 (交易 5) 联机执行, 交易 5 没有执行发卡行认证 (支持并强制), 联机批准。交易 6 脱机拒绝。验证卡不更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 1, 支持发卡行认证 (强制), 支持累计连续脱机交易 (下限)

频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 脱机批准;
e) 交易 5: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机。交易没有执行发卡行认证 (支持并强制执行), 联机批准: 卡片上电 (ATR);
f) 选择 PBOC 借记/贷记应用;
g) GET PROCESSING OPTIONS 命令;
h) VERIFY 命令;
i) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;
j) 第二个 GENERATE AC 请求 TC;
k) 交易 6: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 6= '1', CVR= '03 84 A8 00' 或 '03 80 A8 00' (用于未校验 PIN)。

7.48.19 LTJC019-00

测试目的: 一个批准联机交易后, 验证对于第四个连续的脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求第四个脱机交易 (交易 5) 联机执行, 交易 5 没有执行发卡行认证 (可选), 联机批准。交易 6 脱机拒绝。验证卡更新 LOATC 为当前 ATC 的值。LCOL 值为 3。

测试条件: 第 9 章中的卡片特征 3, 支持发卡行认证 (可选), 支持累计连续脱机交易 (下限) 频度检查。

测试流程: a) 交易 1: 执行发卡行认证成功的联机批准交易, 以复位卡片中的计数器;
b) 交易 2: 脱机批准;
c) 交易 3: 脱机批准;
d) 交易 4: 脱机批准;
e) 交易 5: 在终端第一个 GENERATE AC 请求 TC 后, 卡请求联机。交易没有执行发卡行认证 (可选), 联机批准: 卡片上电 (ATR);
f) 选择 PBOC 借记/贷记应用;
g) GET PROCESSING OPTIONS 命令;
h) VERIFY 命令;
i) 第一个 GENERATE AC 请求 TC, 卡片返回 ARQC;
j) 第二个 GENERATE AC 请求 TC;
k) 交易 6: 脱机拒绝。

通过标准: SW1 SW2= '9000', CID 位 8-7= '00', CVR 字节 2 高半字节= '8', CVR 字节 3 位 6= '0', CVR= '03 84 00 00' 或 '03 80 00 00' (用于未校验 PIN)。

7.48.20 LTJC020-00

测试目的: 一个批准联机交易后, 验证对于第四个连续的脱机交易, ATC 和 LOATC 之间的差比 LCOL 要大。当 ATC 与 LOATC 之间的差比 LCOL 要大时, 验证卡设置 CVR 中的“超过频率检查”位, 并请求联机。卡请求第四个脱机交易 (交易 5) 联机执行, 交易 5 没有执行

发卡行认证（不支持），联机批准。交易 6 脱机拒绝。验证卡更新 LOATC 为当前 ATC 的值。

LCOL 值为 3。

测试条件：第 9 章中的卡片特征 2，支持累计连续脱机交易（下限）频度检查。

测试流程：a) 交易 1：不执行发卡行认证联机批准交易，以复位卡片中的计数器；

b) 交易 2：脱机批准；

c) 交易 3：脱机批准；

d) 交易 4：脱机批准；

e) 交易 5：在终端第一个 GENERATE AC 请求 TC 后，卡请求联机。交易没有执行发卡行认证（不支持），联机批准：卡片上电（ATR）；

f) 选择 PBOC 借记/贷记应用；

g) GET PROCESSING OPTIONS 命令；

h) VERIFY 命令；

i) 第一个 GENERATE AC 请求 TC，卡片返回 ARQC；

j) 第二个 GENERATE AC 请求 TC；

k) 交易 6：脱机拒绝：卡片上电（ATR）；

l) 选择 PBOC 借记/贷记应用；

m) GET PROCESSING OPTIONS 命令；

n) VERIFY 命令；

第一个 GENERATE AC 请求 AAC。

通过标准：SW1 SW2=‘9000’，CID 位 8-7=‘00’，CVR 字节 2 高半字节=‘8’，CVR 字节 3 位 6=‘0’，CVR=‘03 84 00 00’或‘03 80 00 00’（用于未校验 PIN）。

7.49 VERIFY 命令 (VFML)

7.49.1 VFML001-00

测试目的：验证卡在成功的 VERIFY 命令后响应返回‘9000’。

测试条件：N/A。

测试流程：发送一个正确的 VERIFY 命令。

通过标准：SW1 SW2=‘9000’。

7.49.2 VFML002-00

测试目的：验证卡在带有无效数据域的 VERIFY 命令后响应返回‘63C2’。

测试条件：第 9 章中的卡片特征 1，支持脱机 PIN。

测试流程：准备后，发送一个带有不正确数据域的 VERIFY 命令。

注：数据域是一个不正确的 PIN。

通过标准：SW1 SW2=‘63C2’。

7.50 防拔测试 (FBCS)

7.50.1 FBCE001-00

测试目的：确保在执行 VERIFY 命令时断电，卡片 EEPROM 内计数器 PTC 不会发生错误。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 循环执行如下测试流程，直到断电时间使得 VERIFY 命令成功；

- b) 交易 1: 卡片上电 (ATR) ;
- c) 选择应用;
- d) GET PROCESSING OPTIONS 命令;
- e) VERIFY 命令 (错误的 PIN) ;
- f) GET DATA 命令取 PIN 尝试次数计数器 9F17;
- g) 交易 2: 卡片上电 (ATR) ;
- h) 选择应用;
- i) GET PROCESSING OPTIONS 命令;
- j) VERIFY 命令 (错误的 PIN) , 发出命令后, 读卡器断电;
- k) 交易 3: 卡片上电 (ATR) ;
- l) 选择应用;
- m) GET PROCESSING OPTIONS 命令;
- n) GET DATA 命令取 PIN 尝试次数计数器 9F17;
- o) 交易 4: 卡片上电 (ATR) ;
- p) 选择应用;
- q) GET PROCESSING OPTIONS 命令;
- r) VERIFY 命令 (正确的 PIN) ;
- s) GET DATA 命令取 PIN 尝试次数计数器 9F17。

通过标准: 交易 1 中 GET DATA 命令响应数据 PIN 尝试次数应为 02。交易 3 中 GET DATA 命令响应数据 PIN 尝试次数应为 02 或 01。如果交易 2 中 VERIFY 执行成功 (返回状态字 '9000') , 则 PIN 尝试次数计数器应为 01。交易 4 中 GET DATA 命令响应数据 PIN 尝试次数应为 03。

7.50.2 FBCE002-00

测试目的: 确保在执行 GET PROCESSING OPTIONS 命令时断电, 卡片 EEPROM 内计数器 ATC 不会发生错误。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 循环执行如下测试流程, 直到断电时间使得 GET PROCESSING OPTIONS 命令成功;

- b) 交易 1: 卡片上电 (ATR) ;
- c) 选择应用;
- d) GET PROCESSING OPTIONS 命令;
- e) GET DATA 命令 (9F36) ;
- f) 交易 2: 卡片上电 (ATR) ;
- g) 选择应用;
- h) GET DATA 命令 (9F36) ;
- i) GET PROCESSING OPTIONS 命令, 发出命令后, 读卡器断电;
- j) 交易 3: 卡片上电 (ATR) ;
- k) 选择应用;
- l) GET DATA 命令 (9F36)。

通过标准: 交易 3 中 GET DATA 命令取回的 ATC 应等于交易 1 的 ATC 或等于交易 1 的 ATC+1。

如果交易 2 的 GET PROCESSING OPTIONS 命令执行成功 (返回状态字 '9000') , 则取回的 ATC 应等于交易 1 的 ATC+1。

7.50.3 FBCE003-00

测试目的：确保在执行 GENERATE AC 命令时断电，卡片 EEPROM 内计数器 LOATC 不会发生错误。

测试条件：第 9 章中的卡片特征 1

测试流程：a) 交易 1：成功的联机交易：卡片上电（ATR）；
b) 选择应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令；
g) 第二个 GENERATE AC 请求 TC；
h) 交易 2：卡片上电（ATR）；
i) 选择应用；
j) GET DATA 命令(9F36)；
k) GET DATA 命令(9F13)；
l) 循环执行以下两笔交易，直到断电的命令执行成功：交易 3：卡片上电（ATR）；
m) 选择应用；
n) GET PROCESSING OPTIONS 命令；
o) VERIFY 命令；
p) 第一个 GENERATE AC 请求 ARQC；
q) EXTERNAL AUTHENTICATE 命令；
r) 第二个 GENERATE AC 请求 TC，发出命令后，读卡器断电；
s) 交易 4：卡片上电（ATR）；
t) 选择应用；
u) GET DATA 命令(9F36)；
v) GET DATA 命令(9F13)。

通过标准：交易 2 中 GET DATA 命令取回的 ATC 和 LOATC 应相等。交易 4 中 GET DATA 命令取回的 LOATC 应等于 ATC 或最初的 LOATC。如果交易 3 的第 2 个 GENERATE AC 命令执行成功（返回状态字‘9000’），则 LOATC 应等于 ATC。

7.50.4 FBCE004-00

测试目的：确保在执行 PIN CHANGE/UNBLOCK 命令时断电，卡片 EEPROM 内计数器 PTC 不会发生错误。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：成功的联机交易：卡片上电（ATR）；
b) 选择应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令；
e) 第一个 GENERATE AC 请求 ARQC；
f) EXTERNAL AUTHENTICATE 命令；
g) 第二个 GENERATE AC 请求 TC；
h) PIN CHANGE/UNBLOCK (P2= ‘02’，由原 PIN 修改为新 PIN2)；
i) 交易 2：卡片上电（ATR）；
j) 选择应用；
k) GET DATA 命令(9F17)；

- l) VERIFY 命令 (新 PIN) ;
- m) 循环执行以下交易, 直到断电的命令执行成功: 交易 3: 卡片上电 (ATR) ;
- n) 选择应用;
- o) GET PROCESSING OPTIONS 命令;
- p) VERIFY 命令 (错误的 PIN) ;
- q) 交易 4: 卡片上电 (ATR) ;
- r) 选择应用;
- s) GET PROCESSING OPTIONS 命令;
- t) 第一个 GENERATE AC 请求 ARQC;
- u) EXTERNAL AUTHENTICATE 命令;
- v) 第二个 GENERATE AC 请求 TC;
- w) PIN CHANGE/UNBLOCK (P2= '02' , 新 PIN 修改为原 PIN), 断电;
- x) 交易 5: 卡片上电 (ATR) ;
- y) 选择应用;
- z) GET PROCESSING OPTIONS 命令;
- aa) GET DATA 命令 (9F17) , 如返回 PTC=02, 则: VERIFY 命令 (原 PIN 值) ;
- ab) VERIFY 命令 (新 PIN 值) ;
- ac) 否则: VERIFY 命令 (新 PIN 值) ;
- ad) VERIFY 命令 (原 PIN 值) 。

通过标准: 交易 1: PIN CHANGE/UNBLOCK 应执行成功。交易 2: GET DATA 命令取回的 PTC 应为 03。VERIFY (新 PIN 值) 命令成功。交易 3: VERIFY 命令 (旧 PIN) 卡应返回状态字 '63C2'。交易 5: GET DATA 命令取回的 PTC 为 02, 卡返回 VERIFY 命令 (原 PIN 值) 状态字为 '63C1', VERIFY 命令 (新 PIN 值) 状态字为 '9000'。或 GET DATA 命令取回的 PTC 为 03, 卡返回 VERIFY 命令 (原 PIN 值) 状态字为 '9000', VERIFY 命令 (新 PIN 值) 状态字为 '63C2'。如果交易 4, PIN CHANGE/UNBLOCK 执行成功 (返回状态字 9000), 则 GET DATA 命令取回的 PTC 为 03, 卡返回 VERIFY 命令 (原 PIN 值) 状态字为 '9000', VERIFY 命令 (新 PIN 值) 状态字为 '63C2'。

7.50.5 FBCE005-00

测试目的: 确保在执行 PUT DATA 命令时断电, 卡片 EEPROM 内计数器连续脱机交易限制数不会发生错误。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 交易 1: 成功的联机交易: 卡片上电 (ATR) ;

- b) 选择应用;
- c) GET PROCESSING OPTIONS 命令;
- d) VERIFY 命令;
- e) 第一个 GENERATE AC 请求 ARQC;
- f) EXTERNAL AUTHENTICATE 命令;
- g) 第二个 GENERATE AC 请求 TC;
- h) PUT DATA 命令 (9F53);
- i) 交易 2: 卡片上电 (ATR) ;
- j) 选择应用;
- k) GET DATA 命令 (9F53);

- l) 循环进行以下交易,直到断电的命令执行成功:交易 3:断电交易:卡片上电(ATR);
- m) 选择应用;
- n) GET PROCESSING OPTIONS 命令;
- o) VERIFY 命令;
- p) 第一个 GENERATE AC 请求 ARQC;
- q) EXTERNAL AUTHENTICATE 命令;
- r) 第二个 GENERATE AC 请求 TC;
- s) PUT DATA 命令(9F53)断电;
- t) 交易 4:卡片上电(ATR);
- u) 选择应用;
- v) GET DATA 命令(9F53)。

通过标准:交易 2:GET DATA 取得的 9F53 为修改后的新值。交易 4:GET DATA 取得的 9F53 应为修改后的新值或等于原值。如交易 3 的 PUT DATA 命令执行成功,则 GET DATA 取得的 9F53 应为修改后的新值。

7.50.6 FBCE006-00

测试目的:确保在执行 PUT DATA 命令时断电,卡片 EEPROM 内计数器 UCOL 不会发生错误。

测试条件:第 9 章中的卡片特征 1。

测试流程:a) 交易 1:成功的联机交易:卡片上电(ATR);

- b) 选择应用;
- c) GET PROCESSING OPTIONS 命令;
- d) VERIFY 命令;
- e) 第一个 GENERATE AC 请求 ARQC;
- f) EXTERNAL AUTHENTICATE 命令;
- g) 第二个 GENERATE AC 请求 TC;
- h) PUT DATA (9F59);
- i) 交易 2:卡片上电(ATR);
- j) 选择应用;
- k) GET DATA 命令(9F59);
- l) 循环进行以下交易,直到断电的命令执行成功:交易 3:断电交易;
- m) 卡片上电(ATR);
- n) 选择应用;
- o) GET PROCESSING OPTIONS 命令;
- p) VERIFY 命令;
- q) 第一个 GENERATE AC 请求 ARQC;
- r) EXTERNAL AUTHENTICATE 命令;
- s) 第二个 GENERATE AC 请求 TC;
- t) PUT DATA (9F59)断电;
- u) 交易 4:卡片上电(ATR);
- v) 选择应用;
- w) GET DATA 命令(9F59)。

通过标准:交易 2:GET DATA 取得的 9F59 为修改后的新值。交易 4:GET DATA 取得的 9F59 应为修改后的新值或等于原值。如交易 3 的 PUT DATA 命令执行成功,则 GET DATA 取得的

9F59 应为修改后的新值。

7.50.7 FBCE007-00

测试目的：确保在执行 PUT DATA 命令时断电，卡片 EEPROM 内计数器 LCOL 不会发生错误。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 交易 1：成功的联机交易：卡片上电（ATR）；
 b) 选择应用；
 c) GET PROCESSING OPTIONS 命令；
 d) VERIFY 命令；
 e) 第一个 GENERATE AC 请求 ARQC；
 f) EXTERNAL AUTHENTICATE 命令；
 g) 第二个 GENERATE AC 请求 TC；
 h) PUT DATA (9F58)；
 i) 交易 2：卡片上电（ATR）；
 j) 选择应用；
 k) GET DATA 命令 (9F58)；
 l) 循环进行以下交易，直到断电的命令执行成功：交易 3：断电交易：卡片上电（ATR）；
 m) 选择应用；
 n) GET PROCESSING OPTIONS 命令；
 o) VERIFY 命令；
 p) 第一个 GENERATE AC 请求 ARQC；
 q) EXTERNAL AUTHENTICATE 命令；
 r) 第二个 GENERATE AC 请求 TC；
 s) PUT DATA (9F58) 断电；
 t) 交易 4：卡片上电（ATR）；
 u) 选择应用；
 v) GET DATA 命令 (9F58)。

通过标准：交易 2:GET DATA 取得的 9F58 为修改后的新值。交易 4：GET DATA 取得的 9F58 应为修改后的新值或等于原值。如交易 3 的 PUT DATA 命令执行成功，则 GET DATA 取得的 9F58 应为修改后的新值。

7.51 参数测试 (CSCS)

7.51.1 CSCS001-00

测试目的：确保发送格式错误的 APPLICATION BLOCK 命令时，命令不能成功执行。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；
 b) 选择应用；
 c) GET PROCESSING OPTIONS 命令；
 d) VERIFY 命令；
 e) 第一个 GENERATE AC 请求 ARQC；
 f) EXTERNAL AUTHENTICATE 命令；
 g) 第二个 GENERATE AC 请求 TC；
 h) APPLICATION BLOCK 命令（CLA 错误）；

- i) APPLICATION BLOCK 命令 (P1 错误) ;
- j) APPLICATION BLOCK 命令 (P2 错误) ;
- k) APPLICATION BLOCK 命令 (LC 错误) 。

通过标准: 卡片返回 APPLICATION BLOCK 命令的状态字不是 ‘9000’ , 推荐 CLA 错返回状态字 6E00; P1、P2 错返回状态字 ‘6A86’ ; LC 错返回状态字 ‘6700’ 。

7.51.2 CSCS002-00

测试目的: 确保发送格式错误的 APPLICATION UNBLOCK 命令时, 命令不能成功执行。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 卡片上电 (ATR) ;
 - b) 选择应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 ARQC;
 - f) EXTERNAL AUTHENTICATE 命令;
 - g) 第二个 GENERATE AC 请求 TC;
 - h) APPLICATION UNBLOCK 命令 (CLA 错误) ;
 - i) APPLICATION UNBLOCK 命令 (P1 错误) ;
 - j) APPLICATION UNBLOCK 命令 (P2 错误) ;
 - k) APPLICATION UNBLOCK 命令 (LC 错误) 。

通过标准: 卡片返回 APPLICATION UNBLOCK 命令的状态字不是 ‘9000’ , 推荐 CLA 错返回状态字 6E00; P1、P2 错返回状态字 ‘6A86’ ; LC 错返回状态字 ‘6700’ 。

7.51.3 CSCS003-00

测试目的: 确保发送格式错误的 CARD BLOCK 命令时, 命令不能成功执行。

测试条件: 第 9 章中的卡片特征 1。

- 测试流程:
- a) 卡片上电 (ATR) ;
 - b) 选择应用;
 - c) GET PROCESSING OPTIONS 命令;
 - d) VERIFY 命令;
 - e) 第一个 GENERATE AC 请求 ARQC;
 - f) EXTERNAL AUTHENTICATE 命令;
 - g) 第二个 GENERATE AC 请求 TC;
 - h) CARD BLOCK 命令 (CLA 错误) ;
 - i) CARD BLOCK 命令 (P1 错误) ;
 - j) CARD BLOCK 命令 (P2 错误) ;
 - k) CARD BLOCK 命令 (LC 错误) 。

通过标准: 卡片返回 CARD BLOCK 命令的状态字不是 ‘9000’ , 推荐 CLA 错返回状态字 ‘6E00’ ; P1、P2 错返回状态字 ‘6A86’ ; LC 错返回状态字 ‘6700’ 。

7.51.4 CSCS004-00

测试目的: 确保发送格式错误的 EXTERNAL AUTHENTICATE 命令时, 命令不能成功执行。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
 b) 选择应用;
 c) GET PROCESSING OPTIONS 命令;
 d) VERIFY 命令;
 e) 第一个 GENERATE AC 请求 ARQC;
 f) EXTERNAL AUTHENTICATE 命令 (CLA 错误);
 g) EXTERNAL AUTHENTICATE 命令 (P1 错误);
 h) EXTERNAL AUTHENTICATE 命令 (P2 错误);
 i) EXTERNAL AUTHENTICATE 命令 (LC 错误)。

通过标准: 卡片返回 EXTERNAL AUTHENTICATE 命令的状态字不是 '9000', 推荐 CLA 错返回状态字 '6E00'; P1、P2 错返回状态字 '6A86'; LC 错返回状态字 '6700'。

7.51.5 CSCS005-00

测试目的: 确保发送格式错误的 GENERATE AC 命令时, 命令不能成功执行。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
 b) 选择应用;
 c) GET PROCESSING OPTIONS 命令;
 d) VERIFY 命令;
 e) 第一个 GENERATE AC 命令 (CLA 错误);
 f) 第一个 GENERATE AC 命令 (P1 错误);
 g) 第一个 GENERATE AC 命令 (P2 错误);
 h) 第一个 GENERATE AC 命令 (LC 错误)。

通过标准: 卡片返回 GENERATE AC 命令的状态字不是 '9000', 推荐 CLA 错返回状态字 '6E00'; P1、P2 错返回状态字 '6A86'; LC 错返回状态字 '6700'。

7.51.6 CSCS006-00

测试目的: 确保发送格式错误的 GET DATA 命令时, 命令不能成功执行。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);
 b) 选择应用;
 c) GET PROCESSING OPTIONS 命令;
 d) GET DATA 命令 (CLA 错误);
 e) GET DATA 命令 (P1 错误);
 f) GET DATA 命令 (P2 错误);
 g) GET DATA 命令 (LC 错误)。

通过标准: 卡片返回 GET DATA 命令的状态字不是 '9000', 推荐 CLA 错返回状态字 '6E00'; P1、P2 错返回状态字 '6A86'; LC 错返回状态字 '6700'。

7.51.7 CSCS007-00

测试目的: 确保发送格式错误的 GET PROCESSING OPTIONS 命令时, 命令不能成功执行。

测试条件: 第 9 章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);

- b) 选择应用;
- c) GET PROCESSING OPTIONS 命令 (CLA 错误);
- d) GET PROCESSING OPTIONS 命令 (P1 错误);
- e) GET PROCESSING OPTIONS 命令 (P2 错误);
- f) GET PROCESSING OPTIONS 命令 (LC 错误)。

通过标准: 卡片返回 GET PROCESSING OPTIONS 命令的状态字不是 ‘9000’, 推荐 CLA 错返回状态字 ‘6E00’; P1、P2 错返回状态字 ‘6A86’; LC 错返回状态字 ‘6700’。

7.51.8 CSCS008-00

测试目的: 确保发送格式错误的 INTERNAL AUTHENTICATE 命令时, 命令不能成功执行。

测试条件: 第9章中的卡片特征 21。

测试流程: a) 卡片上电 (ATR);

- b) 选择应用;
- c) GET PROCESSING OPTIONS 命令;
- d) INTERNAL AUTHENTICATE 命令 (CLA 错误);
- e) INTERNAL AUTHENTICATE 命令 (P1 错误);
- f) INTERNAL AUTHENTICATE 命令 (P2 错误);
- g) INTERNAL AUTHENTICATE 命令 (LC 错误)。

通过标准: 卡片返回 INTERNAL AUTHENTICATE 命令的状态字不是 ‘9000’, 推荐 CLA 错返回状态字 ‘6E00’; P1、P2 错返回状态字 ‘6A86’; LC 错返回状态字 ‘6700’。

7.51.9 CSCS009-00

测试目的: 确保发送格式错误的 PIN CHANGE 命令时, 命令不能成功执行。

测试条件: 第9章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);

- b) 选择应用;
- c) GET PROCESSING OPTIONS 命令;
- d) VERIFY 命令;
- e) 第一个 GENERATE AC 请求 ARQC;
- f) EXTERNAL AUTHENTICATE 命令;
- g) 第二个 GENERATE AC 请求 TC;
- h) PIN CHANGE 命令 (CLA 错误);
- i) PIN CHANGE 命令 (P1 错误);
- j) PIN CHANGE 命令 (P2 错误);
- k) PIN CHANGE 命令 (LC 错误)。

通过标准: 卡片返回 PIN CHANGE 命令的状态字不是 ‘9000’, 推荐 CLA 错返回状态字 ‘6E00’; P1、P2 错返回状态字 ‘6A86’; LC 错返回状态字 ‘6700’。

7.51.10 CSCS010-00

测试目的: 确保发送格式错误的 PIN UNBLOCK 命令时, 命令不能成功执行。

测试条件: 第9章中的卡片特征 1。

测试流程: a) 卡片上电 (ATR);

- b) 选择应用;

- c) GET PROCESSING OPTIONS 命令；
- d) VERIFY 命令；
- e) 第一个 GENERATE AC 请求 ARQC；
- f) EXTERNAL AUTHENTICATE 命令；
- g) 第二个 GENERATE AC 请求 TC；
- h) PIN UNBLOCK 命令 (CLA 错误)；
- i) PIN UNBLOCK 命令 (P1 错误)；
- j) PIN UNBLOCK 命令 (P2 错误)；
- k) PIN UNBLOCK 命令 (LC 错误)。

通过标准：卡片返回 PIN UNBLOCK 命令的状态字不是‘9000’，推荐 CLA 错返回状态字‘6E00’；P1、P2 错返回状态字‘6A86’；LC 错返回状态字‘6700’。

7.51.11 CSCS011-00

测试目的：确保发送格式错误的 PUT DATA 命令时，命令不能成功执行。

测试条件：第 9 章中的卡片特征 1。

- 测试流程：
- a) 卡片上电 (ATR)；
 - b) 选择应用；
 - c) GET PROCESSING OPTIONS 命令；
 - d) VERIFY 命令；
 - e) 第一个 GENERATE AC 请求 ARQC；
 - f) EXTERNAL AUTHENTICATE 命令；
 - g) 第二个 GENERATE AC 请求 TC；
 - h) PUT DATA 命令 (CLA 错误)；
 - i) PUT DATA 命令 (P1 错误)；
 - j) PUT DATA 命令 (P2 错误)；
 - k) PUT DATA 命令 (LC 错误)。

通过标准：卡片返回 PUT DATA 命令的状态字不是‘9000’，推荐 CLA 错返回状态字‘6E00’；P1、P2 错返回状态字‘6A86’；LC 错返回状态字‘6700’。

7.51.12 CSCS012-00

测试目的：确保发送格式错误的 READ RECORD 命令时，命令不能成功执行。

测试条件：第 9 章中的卡片特征 1。

- 测试流程：
- a) 卡片上电 (ATR)；
 - b) 选择应用；
 - c) GET PROCESSING OPTIONS 命令；
 - d) READ RECORD 命令 (CLA 错误)；
 - e) READ RECORD 命令 (P1 错误)；
 - f) READ RECORD 命令 (P2 错误)；
 - g) READ RECORD 命令 (LC 错误)。

通过标准：卡片返回 READ RECORD 命令的状态字不是‘9000’，推荐 CLA 错返回状态字‘6E00’；P1、P2 错返回状态字‘6A86’；LC 错返回状态字‘6700’。

7.51.13 CSCS013-00

测试目的：确保发送格式错误的 SELECT 命令时，命令不能成功执行。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；
b) SELECT 命令（CLA 错误）；
c) SELECT 命令（P1 错误）；
d) SELECT 命令（P2 错误）；
e) SELECT 命令（LC 错误）。

通过标准：卡片返回 SELECT 命令的状态字不是‘9000’，推荐 CLA 错返回状态字‘6E00’；P1、P2 错返回状态字‘6A86’；LC 错返回状态字‘6700’。

7.51.14 CSCS014-00

测试目的：确保发送格式错误的 UPDATE RECORD 命令时，命令不能成功执行。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；
b) 选择应用；
c) GET PROCESSING OPTIONS 命令；
d) UPDATE RECORD 命令（CLA 错误）；
e) UPDATE RECORD 命令（P1 错误）；
f) UPDATE RECORD 命令（P2 错误）；
g) UPDATE RECORD 命令（LC 错误）。

通过标准：卡片返回 UPDATE RECORD 命令的状态字不是‘9000’，推荐 CLA 错返回状态字‘6E00’；P1、P2 错返回状态字‘6A86’；LC 错返回状态字‘6700’。

7.51.15 CSCS015-00

测试目的：确保发送格式错误的 VERIFY 命令时，命令不能成功执行。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电（ATR）；
b) 选择应用；
c) GET PROCESSING OPTIONS 命令；
d) VERIFY 命令（CLA 错误）；
e) VERIFY 命令（P1 错误）；
f) VERIFY 命令（P2 错误）；
g) VERIFY 命令（LC 错误）。

通过标准：卡片返回 VERIFY 命令的状态字不是‘9000’，推荐 CLA 错返回状态字‘6E00’；P1、P2 错返回状态字‘6A86’；LC 错返回状态字‘6700’。

7.52 稳定性测试(WDCS)

7.52.1 WDCS001-00

测试目的：确保卡片能够连续进行上万次的随机读写。

测试条件：第 9 章中的卡片特征 1。

测试流程：连续 1 万次上电，执行正常交易（包括脱机、联机）。

通过标准：全部交易正确执行，卡片状态正常。

7.53 卡片在 ATM 上被受理的测试 (ATMT)

7.53.1 ATMT001-00

测试目的：当 GPO 和 GAC 发送的货币代码不同时，卡片应正常完成交易。

测试条件：第 9 章中的卡片特征 1

测试流程：a) 卡片上电 (ATR)；
b) 选择应用；
c) GET PROCESSING OPTIONS 命令，金额 20 元，交易货币码 0000，9F7A=00；
d) VERIFY 命令 (可选)；
e) 第一次 GENERATE AC 命令，终端请求联机，金额 20 元，交易货币码 0156；
f) 第二次 GENERATE AC 命令，终端请求批准，金额 20 元，交易货币码 0156。

通过标准：第一次 GENERATE AC 命令时，卡片应请求联机，第二次 GENERATE AC 命令时，卡片应请求批准，第一次和第二次 GENERATE AC 命令时，卡片应使用本次 GENERATE AC 命令时终端发来的交易货币码和授权金额计算应用密文。

7.53.2 ATMT002-00

测试目的：当 GPO 和 GAC 发送的授权金额不同时，卡片应正常完成交易。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择应用；
c) GET PROCESSING OPTIONS 命令，金额 0 元，交易货币码 0156，9F7A=00；
d) VERIFY 命令 (可选)；
e) 第一次 GENERATE AC 命令，终端请求联机，金额 20 元，交易货币码 0156；
f) 第二次 GENERATE AC 命令，终端请求批准，金额 20 元，交易货币码 0156。

通过标准：第一次 GENERATE AC 命令时，卡片应请求联机，第二次 GENERATE AC 命令时，卡片应请求批准，第一次和第二次 GENERATE AC 命令时，卡片应使用本次 GENERATE AC 命令时终端发来的交易货币码和授权金额计算应用密文。

7.53.3 ATMT003-00

测试目的：当 GPO 和 GAC 发送的货币代码和授权金额都不同时，卡片应正常完成交易。

测试条件：第 9 章中的卡片特征 1。

测试流程：a) 卡片上电 (ATR)；
b) 选择应用；
c) GET PROCESSING OPTIONS 命令，金额 0 元，交易货币码 0000，9F7A=00；
d) VERIFY 命令 (可选)；
e) 第一次 GENERATE AC 命令，终端请求联机，金额 20 元，交易货币码 0156；
f) 第二次 GENERATE AC 命令，终端请求批准，金额 20 元，交易货币码 0156。

通过标准：第一次 GENERATE AC 命令时，卡片应请求联机，第二次 GENERATE AC 命令时，卡片应请求批准，第一次和第二次 GENERATE AC 命令时，卡片应使用本次 GENERATE AC 命令时终端发来的交易货币码和授权金额计算应用密文。

8 基于借记贷记的小额支付应用的测试案例

8.1 电子现金数据的读取 (EFR)

8.1.1 EFR001

测试目的：余额能够正常获取。

测试条件：卡特征 29，支持电子现金，新卡。

测试流程：a) 上电。

b) 选择应用。

c) GET DATA 9F79。

通过标准：GET DATA返回余额为“00 00 00 00 20 00”。

8.1.2 EFR002

测试目的：电子现金重置阈值能够正常获取。

测试条件：卡特征29，支持电子现金。

测试流程：a) 上电；

b) 选择应用；

c) GET DATA 9F6D。

通过标准：GET DATA返回余额为“00 00 00 00 15 00”。

8.1.3 EFR003

测试目的：电子现金余额上限能够正常获取。

测试条件：卡特征29，支持电子现金。

测试流程：a) 上电；

b) 选择应用；

c) GET DATA 9F77。

通过标准：GET DATA返回余额为“00 00 00 01 00 00”。

8.1.4 EFR004

测试目的：电子现金单笔交易限额能够正常获取。

测试条件：卡特征29，支持电子现金。

测试流程：a) 上电；

b) 选择应用；

c) GET DATA 9F78。

通过标准：GET DATA返回余额为“00 00 00 00 10 00”。

8.2 电子现金数据的更新（EDU）

8.2.1 EDU001

测试目的：电子现金余额能够正常更新。

测试条件：卡特征29，支持电子现金。

测试流程：a) 发卡行认证成功的联机交易，交易金额10.0，终端电子现金支持指示器=00；

b) 交易1：上电；

c) 选择应用；

d) GET DATA 9F79；

e) 交易2：选择应用；

f) GP0 电子现金终端指示器=01，授权金额为 2.00；

- g) 第一个 GAC 请求 ARQC;
- h) 第二个 GAC 请求 TC;
- i) PUT Data 9F79 为 0000 00 00 99 00。

通过标准: 交易2中put data应返回9000。

8.2.2 EDU002

测试目的: 电子现金余额能够正常更新。

测试条件: 卡特征29, 支持电子现金。

- 测试流程:
- a) 发卡行认证成功的联机交易, 交易金额10.0, 终端电子现金支持指示器=00;
 - b) 交易1: 上电;
 - c) 选择应用;
 - d) GET DATA 9F79;
 - e) 交易2: 选择应用;
 - f) GP0 电子现金终端指示器=00, 授权金额为 2.00;
 - g) Verify;
 - h) 第一个 GAC 请求 ARQC;
 - i) 外部认证命令, 正确的 MAC;
 - j) 第二个 GAC 请求 TC;
 - k) PUT Data 9F79 为 00 00 00 00 30 00。

通过标准: 交易2: put data应返回9000。

8.2.3 EDU003

测试目的: 电子现金余额超出电子现金余额上限的更新应不成功。

测试条件: 卡特征29, 支持电子现金。

- 测试流程:
- a) 发卡行认证成功的联机交易, 交易金额10.0, 终端电子现金支持指示器=00;
 - b) 交易1: 上电;
 - c) 选择应用;
 - d) GET DATA 9F79;
 - e) 交易2: 选择应用;
 - f) GP0 电子现金终端指示器=00, 授权金额为 2.00;
 - g) Verify;
 - h) 联机批准;
 - i) PUT Data 9F79 为 00 00 00 01 01 00。

通过标准: 交易2: put data应返回不成功。

8.2.4 EDU004

测试目的: 无效的PUT DATA命令不能够更新电子现金余额。

测试条件: 卡特征29, 支持电子现金, 授权金额为2.00。

- 测试流程:
- a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00, 第2个GAC后修改电子现金余额为00 00 00 00 10 00;
 - b) 交易2: 借记贷记交易, 联机接受, 无效的PUT DATA设置电子现金余额;
 - c) 交易3: 电子现金交易, 脱机接受。

通过标准：在交易2中，GPO的响应包含借记贷记 AIP='7C 00'，且第一个GAC响应正确，PUT DATA命令SW1SW2不是9000，建议返回6988。在交易3中，GET DATA获取的电子现金余额为10.0，GAC响应正确。

8.2.5 EDU005

测试目的：结合电子现金余额与主账户余额时，电子现金余额更新为零。

测试条件：卡特征29，支持电子现金。

测试流程：a) 发卡行认证成功的联机交易，交易金额10.0，终端电子现金支持指示器=00；
b) 交易1：上电；
c) 选择应用；
d) GET DATA 9F79；
e) 交易2：选择应用；
f) GPO 电子现金终端指示器=00，授权金额为 200.00；
g) Verify；
h) 联机批准；
i) PUT Data 9F79 为 00 00 00 00 00 00；
j) 交易3：上电；
k) 选择应用；
l) GET DATA 9F79；
m) 交易4：选择应用；
n) GPO 电子现金终端指示器=00，授权金额为 200.00；
o) Verify；
p) PUT Data 9F79 为 00 00 00 00 20 00。

通过标准：在交易2中，put data应返回9000。交易3中，GET DATA返回余额应等于00 00 00 00 00 00。交易4中put data应返回9000。

8.2.6 EDU006

测试目的：电子现金重值阈置能够正常更新。

测试条件：卡特征29，支持电子现金。

测试流程：a) 发卡行认证成功的联机交易，交易金额10.0，终端电子现金支持指示器=00；
b) 交易1：上电；
c) 选择应用；
d) GET DATA 9F6D；
e) 交易2：选择应用；
f) GPO 电子现金终端指示器=00，授权金额为 2.00；
g) Verify；
h) 联机批准；
i) PUT Data 9F6D 为 00 00 00 00 20 00；
j) 交易3：上电；
k) 选择应用；
l) GET DATA 9F6D；
m) 交易4：选择应用；
n) GPO电子现金终端指示器=00，授权金额为2.00；

- o) Verify;
- p) 联机批准;
- q) PUT Data 9F6D 为 00 00 00 00 15 00;
- r) 交易5: 上电;
- s) 选择应用;
- t) GET DATA 9F6D。

通过标准: 在交易1中, GET DATA返回9F6D应等于00 00 00 00 15 00。交易2中, put data应返回9000。交易3中, GET DATA返回9F6D应等于00 00 00 00 20 00。交易4中, put data应返回9000。交易5中, GET DATA返回9F6D应等于00 00 00 00 15 00。

8.2.7 EDU007

测试目的: 无效的PUT DATA命令不能够更新电子现金重置阈值。

测试条件: 卡特征29, 支持电子现金, 授权金额为2.00。

- 测试流程:
- a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;
 - b) 交易2: 上电;
 - c) 选择应用;
 - d) GET DATA 9F6D;
 - e) 交易3: 借记贷记交易, 联机接受, 无效的PUT DATA设置电子现金重置阈值;
 - f) 交易4: 电子现金交易。

通过标准: 在交易2中, GET DATA返回等于00 00 00 00 15 00。交易3中, GP0的响应包含借记贷记 AIP='7C 00', PUT DATA命令SW1SW2不是9000, 建议返回6988。交易4中, GET DATA返回等于00 00 00 00 15 00, GAC响应正确。

8.2.8 EDU008

测试目的: 电子现金单笔交易限额能够正常更新。

测试条件: 卡特征29, 支持电子现金。

- 测试流程:
- a) 交易1: 上电;
 - b) 选择应用;
 - c) GET DATA 9F78;
 - d) 交易2: 选择应用;
 - e) GP0电子现金终端指示器=00, 授权金额为2.00;
 - f) Verify;
 - g) 第一个GAC请求ARQC;
 - h) 外部认证命令, 正确的MAC;
 - i) 第二个GAC请求TC;
 - j) PUT Data 9F78 为00 00 00 00 18 00;
 - k) 交易3: 上电;
 - l) 选择应用;
 - m) GET DATA 9F78;
 - n) 交易4: 选择应用;
 - o) GP0电子现金终端指示器=00, 授权金额为2.00;
 - p) Verify;
 - q) 联机批准;

- r) PUT Data 9F78 为00 00 00 00 10 00;
- s) 交易 5: 上电;
- t) 选择应用;
- u) GET DATA 9F78。

通过标准: 在交易1中, GET DATA返回9F78应等于00 00 00 00 10 00。交易2中, put data应返回9000。交易3中, GET DATA返回9F78应等于00 00 00 00 18 00。交易4中, put data应返回9000。交易5中, GET DATA返回9F78应等于00 00 00 00 10 00。

8.2.9 EDU009

测试目的: 无效的PUT DATA命令不能够更新电子现金单笔交易限额。

测试条件: 卡特征29, 支持电子现金, 授权金额为2.00。

测试流程: a) 交易1, 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;

- b) 交易 2: 上电;
- c) 选择应用;
- d) GET DATA 9F78;
- e) 交易 3: 借记贷记交易, 联机接受, 无效的 PUT DATA 设置电子现金单笔交易限额;
- f) 交易 4: 电子现金交易;
- g) 上电;
- h) 选择应用;
- i) GET DATA 9F78。

通过标准: 在交易2中, GET DATA返回等于00 00 00 00 10 00。交易3中, GP0的响应包含借记贷记 AIP= '7C 00', 且PUT DATA命令SW1SW2不是9000, 建议返回6988。交易4中, GET DATA返回等于00 00 00 00 10 00。

8.2.10 EDU010

测试目的: 电子现金余额上限能够正常更新。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 交易金额10.0, 终端电子现金支持指示器=00;

- b) 交易 2: 上电;
- c) 选择应用;
- d) GET DATA 9F77;
- e) 交易 3: 选择应用;
- f) GP0 电子现金终端指示器=00, 授权金额为 2.00;
- g) Verify;
- h) 联机批准;
- i) PUT Data 9F77 为 00 00 00 00 55 00;
- j) 交易 4: 上电;
- k) 选择应用;
- l) GET DATA 9F77;
- m) 交易 5: 选择应用;
- n) GP0 电子现金终端指示器=00, 授权金额为 2.00;
- o) Verify;
- p) 联机批准;

- q) PUT Data 9F77 为 00 00 00 01 00 00;
- r) 交易 6: 上电;
- s) 选择应用;
- t) GET DATA 9F77。

通过标准: 在交易2中, GET DATA返回余额上限正确。交易3中, put data应返回9000。交易4中, GET DATA返回余额上限正确。交易5中, put data应返回9000。交易6中, GET DATA返回余额上限正确。

8.2.11 EDU011

测试目的: 无效的PUT DATA命令不能够更新电子现金余额上限。

测试条件: 卡特征29, 支持电子现金, 授权金额为2.00。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;

- b) 交易 2: 上电;
- c) 选择应用;
- d) GET DATA 9F77;
- e) 交易 3: 借记贷记交易, 联机接受, 无效的 PUT DATA 设置电子现金余额上限;
- f) 选择应用;
- g) GP0电子现金终端指示器=00;
- h) Verify;
- i) 第一个GAC请求ARQC;
- j) EXTERNAL AUTHENTICATE;
- k) 第二个GAC请求TC;
- l) 带无效MAC的PUT DATA命令设置9F77, 新值为00 00 00 00 57 00;
- m) 交易 4: 电子现金交易;
- n) 上电;
- o) 选择应用;
- p) GET DATA 9F77。

通过标准: 在交易2中, GET DATA返回等于00 00 00 01 00 00。交易3中, GP0的响应包含借记贷记 AIP='7C 00', PUT DATA命令SW1SW2不是9000, 建议返回6988。交易4中, GET DATA返回等于00 00 00 01 00 00。

8.3 应用初始化 (EEC)

8.3.1 EEC001

测试目的: 当电子现金终端支持指示器为01, 卡应成功的处理一个电子现金交易。

测试条件: 卡特征29, 支持电子现金, 新卡。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 交易金额10.0, 终端电子现金支持指示器=00;
b) 交易 2: 电子现金交易脱机接受。

通过标准: 验证对于交易1第二个GAC的响应, 卡响应SW1SW2是9000, CVR第二字节高半字节='6', 余额和CVR正确。

8.3.2 EEC002

测试目的: 当终端不支持电子现金, 卡应按借记贷记处理交易。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;
b) 交易 2: 选择应用;
c) GP0电子现金终端指示器=01 , 授权金额为2.00;
d) Verify;
e) 第一个GAC请求AAC;
F) 交易 3: 选择应用;
g) GP0电子现金终端指示器=00 , 授权金额为2.00;
h) Verify;
i) 第一个GAC请求TC;
j) 交易 4: 选择应用;
k) GP0电子现金终端指示器=01 , 授权金额为2.00;
l) Verify;
m) 第一个GAC请求TC。

通过标准: 交易2中, GP0响应的AFL中指定的记录中应包含电子现金发卡行授权码, GP0响应的AIP=58 00, GET DATA获取的电子现金余额应该等于GAC 9F10中返回的余额。交易3中, GP0响应的AFL中指定的记录中应不包含电子现金发卡行授权码, GP0响应的AIP=7C 00。交易4中余额和CVR正确。

8.3.3 EEC003

测试目的: 交易货币代码与应用货币代码不匹配时, 卡应按借记贷记处理交易。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;
b) 交易 2: 取余额;
c) 选择应用;
d) GET DATA 9F79;
e) 交易 3: 选择应用;
f) GP0电子现金终端指示器=01 , 货币代码为0840, 授权金额为2.00;
g) Verify;
h) 第一个GAC请求TC;
i) 交易 4: 选择应用;
j) GET DATA 9F79;
k) 交易 5: 选择应用;
l) GP0电子现金终端指示器=01 , 货币代码为0840, 授权金额为2.00;
m) Verify;
n) 第一个GAC请求TC;
o) 交易 6: 选择应用;
p) GET DATA 9F79。

通过标准: 交易3、交易5中, GP0响应的AFL中指定的记录中应不包含电子现金发卡行授权码。GP0响应的AIP=7C 00。交易 2、交易 4、交易 6 三个交易中获得的余额应相等。

8.3.4 EEC004

测试目的: 对于授权金额大于电子现金余额的交易, 支持电子现金的卡将其作为借记贷记交易处理。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00。发脚本Put DATA 修改余额为16元；

b) 交易 2：电子现金脱机接受；

c) 选择应用；

d) GP0电子现金终端指示器=01，授权金额为9.00；

e) GET DATA 9F79；

f) GET DATA 9F6D；

g) Verify；

h) 第一个GAC请求TC；

i) 交易 3：电子现金脱机接受，授权金额为 5.00；

j) 交易 4：电子现金余额不足，交易被作为借记贷记标准交易处理，联机接受；

k) 交易 5：电子现金余额不足，交易作为借记贷记标准交易（1）处理，授权金额为 2.01。

通过标准：交易1中，PUT DATA修改电子现金余额应成功。交易2中，GP0的响应包含电子现金 AIP= '58 00'，GP0的响应AFL的记录中应包含电子现金发卡行授权码，第一个GAC SW1SW2是9000，余额和CVR正确。交易3中，GP0的响应包含电子现金 AIP= '58 00'，GP0的响应AFL的记录中应包含电子现金发卡行授权码，第一个GAC SW1SW2是9000，余额和CVR正确。交易4中，GP0的响应包含借记贷记 AIP= '7C 00'，第二个GAC SW1SW2是9000，余额和CVR正确。交易5中，GP0的响应包含借记贷记 AIP= '7C 00'，第一个GAC SW1SW2是9000 卡片返回TC，余额和CVR正确。

8.3.5 EEC005

测试目的：对于授权金额大于电子现金单笔交易限额的交易，支持电子现金的卡将其作为借记贷记交易处理。

测试条件：卡特征29，支持电子现金、电子现金单笔交易限额。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00。第二个GAC后PUT DATA 电子现金单笔交易限额设置为新值'00 00 00 00 05 00'，第二个GAC后PUT DATA电子现金余额为“00 00 00 00 20 00”；

b) 交易 2：将授权金额超出电子现金单笔交易限额的交易作为借记贷记交易处理（1）；

c) 交易 3：将授权金额等于电子现金单笔交易限额的交易作为小额交易处理；

d) 交易 4：将授权金额大于电子现金单笔交易限额的交易作为标准借记贷记交易（2）；

e) 交易 5：将授权金额等于电子现金单笔交易限额的交易作为小额交易处理；

f) 交易 6：将授权金额大于电子现金单笔交易限额的交易作为标准借记贷记交易（2）。

通过标准：交易2中，GP0的响应包含借记贷记 AIP= '7C 00'，GP0的响应的AFL指定的记录中不含有电子现金发卡行授权码，余额和CVR正确。交易3中，GP0的响应包含借记贷记 AIP= '58 00'，GP0的响应的AFL指定的记录中含有电子现金发卡行授权码，余额和CVR正确。交易4中，GP0的响应包含借记贷记 AIP= '7C 00'，GP0的响应的AFL指定的记录中不含有电子现金发卡行授权码，余额和CVR正确。交易5中，GP0的响应包含借记贷记 AIP= '58 00'，GP0的响应的AFL指定的记录中含有电子现金发卡行授权码，余额和CVR正确。交易6中，GP0的响应包含借记贷记 AIP= '7C 00'，GP0的响应的AFL指定的记录中不含有电子现金发卡行授权码，余额和CVR正确。

8.3.6 EEC006

测试目的：当上一笔交易发卡行认证失败，卡应将交易作为借记贷记交易处理。

测试条件：卡特征29，支持电子现金，授权金额为2.00。

测试流程：a) 交易1:发卡行认证成功的联机交易，终端电子现金支持指示器=00；

b) 交易2:借记贷记交易发卡行认证失败，联机拒绝；

c) 交易3:以电子现金交易开始，但卡按借记贷记交易处理，联机接受。

通过标准：交易2中，GP0的响应包含借记贷记 AIP= '7C 00'。交易3中，GP0的响应包含借记贷记 AIP= '7C 00'，GAC响应正确。

8.3.7 EEC007

测试目的：当上一笔交易PIN锁定，卡应将交易作为借记贷记交易处理。

测试条件：卡特征30，支持电子现金。

测试流程：a) 交易1:发卡行认证成功的联机交易，终端电子现金支持指示器=00；

b) 交易2:借记贷记交易 PIN 锁定，联机拒绝；

c) 交易3:以电子现金交易开始，但卡按借记贷记交易处理，联机拒绝；

d) 交易4:借记贷记联机接受，PIN 解锁。

通过标准：交易2中，GP0的响应包含借记贷记 AIP= '7D 00'。交易3中，GP0的响应包含借记贷记 AIP= '7D 00'，第二个GAC SW1SW2是9000，余额和CVR正确。交易4中，GP0的响应包含借记贷记 AIP= '7D 00'，PIN CHANGE/UNBLOCK SW1SW2是9000。

8.3.8 EEC008

测试目的：当上一笔交易PIN锁定，卡应将交易作为借记贷记交易处理。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1:发卡行认证成功的联机交易，终端电子现金支持指示器=00, 修改电子现金余额=20.00；

b) 交易2:借记贷记交易 PIN 锁定，联机拒绝；

c) 交易3:以电子现金交易开始，但卡按借记贷记交易处理，联机拒绝,应用解锁；

d) 交易4:以电子现金交易开始，但卡按借记贷记交易处理,交易拒绝；

e) 交易5:以电子现金交易开始，但卡按借记贷记交易处理,PIN 解锁；

f) 交易6:以电子现金交易开始，电子现金交易；

g) 交易7:以电子现金交易开始，电子现金交易。

通过标准：交易2中，GP0的响应包含借记贷记 AIP= '7C 00'。交易3中，select返回SW=6283，GP0的响应包含借记贷记 AIP= '7C 00'，Verify pin 返回 SW=6984，第一个GAC返回的CID=00，第一个GAC CVR= '03 86 40 00'，应用解锁脚本命令应该执行成功。交易4中，select 返回 SW=9000，GP0的响应包含借记贷记 AIP= '7C 00'，GP0响应的AFL中指定的记录中应不包含电子现金发卡行授权码 9F74，Verify pin 返回 SW=6984，第一个GAC返回的CID=00，第一个GAC CVR= '03 86 40 00'。交易5中，select 返回 SW=9000，GP0的响应包含借记贷记 AIP= '7C 00'，GP0响应的AFL中指定的记录中应不包含电子现金发卡行授权码 9F74，Verify pin 返回 SW=6984，第一个GAC返回的CID=00，第一个GAC CVR= '03 86 40 00'，PIN 解锁脚本命令应该执行成功。交易6中，GP0的响应包含电子现金 AIP= '58 00'，GP0响应的AFL中指定的记录中应包含电子现金发卡行授权码 9F74，第一个GAC卡片返回 CVR= "03 94 00 00"，GAC中返回的余额=19.00。交易7中，GP0的响应包含电子现金 AIP= '58 00'，GP0响应的AFL中指定的记录中应包含电子现金发卡行授权码 9F74，第一个GAC卡片

返回 CVR=" 03 94 00 00"，GAC 中返回的余额=18.00。

8.3.9 EEC009

测试目的：当上一笔交易发卡行脚本执行失败，卡应将交易作为借记贷记交易处理。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1: 发卡行认证成功的联机交易，终端电子现金支持指示器=00，发put data 脚本修改卡片电子现金余额为20.00；

b) 交易2: 借记贷记交易，脚本执行失败；

c) 交易3: 以电子现金交易开始，但卡按借记贷记交易处理，联机交易；

d) 交易4: 以电子现金交易开始，执行电子现金交易。

通过标准：交易1中，修改余额的脚本应执行成功。交易2中，GP0的响应包含借记贷记 AIP=' 7C 00'，修改余额的脚本命令应返回 SW 不等于 9000。交易3中，GP0 的响应包含借记贷记 AIP=' 7C 00'。GP0 响应的 AFL 中指定的记录中应不包含电子现金发卡行授权码 9F74，第一个 GAC 卡片返回密文类型为 ARQC，第一个 GAC 卡片返回 CVR=" 03 A4 00 18"，第二个 GAC SW1SW2 是 9000，第二个 GAC CVR=' 03 34 00 00'。交易4中，GP0 的响应包含电子现金 AIP=' 58 00'，GP0 响应的 AFL 中指定的记录中应包含电子现金发卡行授权码 9F74，第一个 GAC 卡片返回 CVR=" 03 94 00 00"，GAC 中返回的余额=19.00。

8.3.10 EEC010

测试目的：当上一笔交易发卡行脚本执行失败，卡应将交易作为借记贷记交易处理。

测试条件：卡特征30，支持电子现金。

测试流程：a) 交易1: 发卡行认证成功的联机交易，终端电子现金支持指示器=00，发put data 脚本修改卡片电子现金余额为20.00；

b) 交易2: 借记贷记交易，脚本执行失败；

c) 交易3: 以电子现金交易开始，但卡按借记贷记交易处理，脱机交易；

d) 交易4: 以电子现金交易开始，但卡按借记贷记交易处理，脱机交易；

e) 交易5: 借记贷记交易，发卡行认证成功；

f) 交易6: 以电子现金交易开始，执行电子现金。

通过标准：交易1中，修改余额的脚本应执行成功。交易2中，GP0的响应包含借记贷记 AIP=' 7D 00'，修改余额的脚本命令应返回 SW<>9000。交易3中，GP0 的响应包含借记贷记 AIP=' 7D 00'，GP0 响应的 AFL 中指定的记录中应不包含电子现金发卡行授权码 9F74，第一个 GAC 卡片返回密文类型为 TC，第一个 GAC 卡片返回 CVR=" 03 94 00 18"。交易4中，GP0 的响应包含借记贷记 AIP=' 7D 00'，GP0 响应的 AFL 中指定的记录中应不包含电子现金发卡行授权码 9F74，第一个 GAC 卡片返回密文类型为 TC，第一个 GAC 卡片返回 CVR=" 03 94 00 18"。交易5中，GP0 的响应包含借记贷记 AIP=' 7D 00'，GP0 响应的 AFL 中指定的记录中应不包含电子现金发卡行授权码 9F74，第二个 GAC 卡片返回 CVR=" 03 34 00 00"。交易6中，GP0 的响应包含电子现金 AIP=' 7C 00'，GP0 响应的 AFL 中指定的记录中应包含电子现金发卡行授权码 9F74，第一个 GAC 卡片返回 CVR=" 03 94 00 00"，GAC 中返回的余额=19.00。

8.4 电子现金余额的更新（EFS）

8.4.1 EFS001

测试目的：在GAC返回TC后，电子现金卡应减少电子现金余额

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put DATA 9F79 10.00;

b) 交易2：电子现金交易，第一个GAC请求TC。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC中9F10正确，Mac应计算正确。

8.4.2 EFS002

测试目的：当电子现金交易失败后，电子现金余额应不发生变化。

测试条件：卡特征29，支持电子现金，授权金额为2.00。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put DATA 9F79 10.00;

b) 交易2：电子现金交易，脱机拒绝。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC中9F10正确，Mac应计算正确。

8.4.3 EFS003

测试目的：当终端请求电子现金交易联机时，电子现金余额应不发生变化。

测试条件：卡特征29，支持电子现金，授权金额为2.00。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put DATA 9F79 10.00;

b) 交易2：电子现金交易，请求联机，授权响应码 3030。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC响应正确，验证MAC正确。

8.4.4 EFS004

测试目的：当终端请求电子现金交易联机时，拒绝时，电子现金余额应不发生变化。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put DATA 9F79 10.00;

b) 交易2：电子现金交易，请求联机，授权金额为2.00，授权响应码 3035。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC响应正确，验证MAC正确。

8.4.5 EFS005

测试目的：当借记贷记交易联机且不能联机，脱机接受时，电子现金余额不会被重置。

测试条件：卡特征29，支持电子现金，联机授权指示符在脱机接受后不被重置。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put DATA 9F79 10.00;

b) 交易2：借记贷记交易，联机且不能联机，授权金额为2.0，ARC为5933;

c) 交易3：电子现金交易，脱机接受，授权金额为2.0;

d) 交易5：但卡按借记贷记交易处理，联机接受。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC响应正确，验证MAC正确。

交易3中，GP0的响应包含借记贷记 AIP= '58 00'，GAC、MAC正确。交易4中，GAC响应正确。

8.5 电子现金脱机接收后，拒绝发卡行脚本（EIS）

8.5.1 EIS001

测试目的：电子现金交易脱机接受后，卡应该拒绝发卡行脚本。

测试条件：卡特征29，支持电子现金，授权金额为2.00。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00，put data 电子现金余额为20.00；

b) 交易2：电子现金交易，脱机接受，应用锁定；

c) 交易3：验证应用未被锁定。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC响应正确，应用锁定SW1SW2不是9000，建议返回6985或6982。交易3，选择应用返回9000。

8.5.2 EIS002

测试目的：电子现金交易脱机接受后，卡应该拒绝发卡行脚本。

测试条件：卡特征29，支持电子现金，授权金额为2.00。

测试流程：a) 交易1：读取电子现金余额；

b) 交易2：电子现金交易，脱机接受；

c) 交易3：验证电子现金余额未被更改。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC响应正确，PUT DATA SW1SW2不是9000，建议返回6985或6982。交易3，返回的余额与交易1相等。

8.5.3 EIS003

测试目的：电子现金交易脱机接受后，卡应该拒绝发卡行脚本。

测试条件：卡特征29，支持电子现金，授权金额为2.00。

测试流程：a) 交易1：读取电子现金余额上限。

b) 交易2：电子现金交易，脱机接受。

c) 交易3：验证电子现金余额上限未被更改。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC响应正确，PUT DATA SW1SW2不是9000，建议返回6985或6982。交易3中，返回的电子现金余额上限与交易1返回相等。

8.5.4 EIS004

测试目的：电子现金交易脱机接受后，卡应该拒绝发卡行脚本。

测试条件：卡特征29，支持电子现金，授权金额为2.00。

测试流程：a) 交易1：读取电子现金重置阈值；

b) 交易2：电子现金交易，脱机接受；

c) 交易3：验证电子现金重置阈值未被更改。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，GAC响应正确，PUT DATA SW1SW2不是9000，建议返回6985或6982。交易3，返回的电子现金重置阈值与交易1返回相等。

8.5.5 EIS005

测试目的：电子现金交易脱机接受后，卡应该拒绝发卡行脚本。

测试条件：卡特征29，支持电子现金，授权金额为2.00。

测试流程：a) 交易1：读取电子现金单笔交易限额；

b) 交易2：电子现金交易，脱机接受；

c) 交易 3: 验证电子现金单笔交易限额未被更改。

通过标准: 交易2中, GP0的响应包含电子现金 AIP= '58 00', GAC响应正确, PUT DATA SW1SW2不是9000, 建议返回6985或6982。交易3, 返回的电子现金单笔交易限额与交易1返回相等。

8.5.6 EIS006

测试目的: 电子现金交易脱机接受后, 卡应该拒绝发卡行脚本。

测试条件: 卡特征29, 支持电子现金, 授权金额为2.00。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;

b) 交易 2: 电子现金交易, 脱机接受。

通过标准: 交易2, GP0的响应包含电子现金 AIP= '58 00', GAC响应正确, PIN Unblock SW1SW2不是9000, 建议返回6985或6982。

8.6 脱机数据认证 (EOD)

8.6.1 EOD001

测试目的: 电子现金交易的动态数据认证。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00, put data 9F79=000000001000;

b) 交易 2: 电子现金交易。

通过标准: 交易2中, GP0的响应包含电子现金 AIP= '7C 00', 内部认证命令返回9000, 返回的DDA签名正确, GAC响应正确, Mac应计算正确。

8.6.2 EOD002

测试目的: 电子现金交易的动态数据认证。

测试条件: 卡特征30, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00, put data 9F79=000000001000;

b) 交易 2: 电子现金交易。

通过标准: 交易2, GP0的响应包含电子现金 AIP= '7D 00', 内部认证命令返回9000, 返回的DDA签名正确, GAC中9F10中的余额应正确, Mac应计算正确。

8.6.3 EOD003

测试目的: 电子现金交易的复合动态数据认证。

测试条件: 卡特征30, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00, put data 9F79=000000001000;

b) 交易 2: 电子现金交易。

通过标准: 交易2中, GP0的响应包含电子现金 AIP= '7D 00', 返回的CDA签名正确, GAC中9F10中的余额应正确, Mac应计算正确。

8.6.4 EOD004

测试目的: 电子现金交易的动态数据认证-1408位密钥。

测试条件：卡特征51，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put data 9F79=000000001000;

b) 交易2：电子现金交易，内部认证命令+4个字节随机数，第一个GAC请求TC。

通过标准：交易2, GP0的响应包含电子现金 AIP= '7D 00', 内部认证命令返回9000, 返回的DDA签名正确, GAC中9F10中的余额应正确, Mac应计算正确。

8.6.5 E0D005

测试目的：电子现金交易的复合动态数据认证-1408位密钥。

测试条件：卡特征51，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put data 9F79=000000001000;

b) 交易2：电子现金交易；

c) 选择应用；

d) 第一个GAC请求ARQC；

e) 第二个GAC请求TC。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '7D 00', 返回的CDA签名正确，GAC中9F10中的余额应正确，Mac应计算正确。

8.6.6 E0D006

测试目的：电子现金交易的动态数据认证-1408位密钥。

测试条件：卡特征51，支持电子现金（特殊个人化，对称算法固定为对称算法为SM4）。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put data 9F79=000000001000;

b) 交易2：电子现金交易；

c) 内部认证命令+4个字节随机数；

d) 第一个GAC请求TC。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '7D 00', 内部认证命令返回9000, 返回的DDA签名正确，GAC中9F10中的余额应正确，Mac应计算正确。

8.6.7 E0D007

测试目的：电子现金交易的复合动态数据认证-1408位密钥。

测试条件：卡特征51，支持电子现金（特殊个人化，对称算法固定为对称算法为SM4）。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put data 9F79=000000001000;

b) 交易2：电子现金交易；

c) 选择应用；

d) 第一个GAC请求ARQC；

e) 第二个GAC请求TC。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '7D 00', 返回的CDA签名正确，GAC中9F10中的余额应正确，Mac应计算正确。

8.6.8 E0D008

测试目的：电子现金交易的动态数据认证-1408位密钥。

测试条件：卡特征52，支持电子现金（特殊个人化，对称算法固定为对称算法为3DES）。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put data 9F79=000000001000;
b) 交易2：电子现金交易;
c) 内部认证命令+4个字节随机数;
d) 第一个GAC请求TC。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '7D 00'，内部认证命令返回9000，返回的DDA签名正确，GAC中9F10中的余额应正确，Mac应计算正确。

8.6.9 E0D009

测试目的：电子现金交易的复合动态数据认证-1408位密钥。

测试条件：卡特征52，支持电子现金（特殊个人化，对称算法固定为对称算法为3DES）。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put data 9F79=000000001000;
b) 交易2：电子现金交易;
c) 选择应用;
d) 第一个GAC请求ARQC;
e) 第二个GAC请求TC。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '7D 00'，返回的CDA签名正确，GAC中9F10中的余额应正确，Mac应计算正确。

8.7 持卡人认证（ECV）

8.7.1 ECV001

测试目的：明文PIN验证失败的处理。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put data 9F79=000000001000;
b) 交易2：电子现金交易;
c) 选择应用 ;
d) GP0 电子现金终端指示器=01，授权金额为2.00;
e) GET DATA 9F79;
f) GET DATA 9F6D;
g) Verify 错误的PIN=12345;
h) Verify 正确的PIN=1234;
i) 第一个GAC请求TC;
j) 交易3：选择应用 ;
k) GP0 电子现金终端指示器=01，授权金额为2.00;
l) GET DATA 9F79;
m) GET DATA 9F6D;
n) Verify 错误的PIN=12345;
o) Verify 错误的PIN=123456;
p) Verify 正确的PIN=1234;

q) 第一个 GAC 请求 TC。

通过标准：交易2中，GP0的响应包含电子现金 AIP= '58 00'，第一个Verify卡片返回63C2，第二个Verify卡片返回9000，GAC中9F10应正确，Mac应计算正确。交易3中，GP0的响应包含电子现金 AIP= '58 00'，第一个Verify卡片返回63C2，第二个Verify卡片返回63C1，第三个Verify卡片返回9000，GAC中9F10应正确，Mac应计算正确。

8.7.2 ECV002

测试目的：明文PIN验证失败的处理。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00, put data 9F79=000000001000;
b) 交易 2：选择应用；
c) GP0 电子现金终端指示器=01，授权金额为 2.00；
d) GET DATA 9F79；
e) GET DATA 9F6D；
f) Verify 错误的 PIN=12345；
g) 第一个 GAC 请求 TC。

通过标准：交易2, GP0的响应包含电子现金 AIP= '58 00', Verify卡片返回63C2, GAC中9F10应正确, Mac应计算正确。

8.7.3 ECV003

测试目的：明文PIN锁定的处理。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00；
b) Verify 正确的 PIN；
c) put data 9F79；
d) 交易 2：电子现金交易；
e) 选择应用；
f) GP0 电子现金终端指示器=01，授权金额为 2.00；
g) GET DATA 9F79、9F6D；
h) Verify 错误的 PIN=12345；
i) Verify 错误的 PIN=12345；
j) Verify 错误的 PIN=12345；
k) 第一个 GAC 请求 AAC；
l) 交易 3：选择应用；
m) GP0 电子现金终端指示器=01，授权金额为 2.00；
n) GET DATA 9F79；
o) GET DATA 9F6D；
p) Verify 正确的 PIN=1234；
q) 第一个 GAC 请求 TC；
r) 发卡行认证, 正确 mac；
s) 应用解锁命令，正确 mac；
t) PIN 解锁命令，正确 mac；

- u) 交易 4: 选择应用;
- v) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- w) Verify 正确的 PIN=1234;
- x) 第一个 GAC 请求 ARQC;
- y) 发卡行认证, 正确 mac;
- z) 第二个 GAC 请求 TC。

通过标准: 交易2中, GP0的响应包含电子现金 AIP= '58 00', 第一个Verify卡片返回63C2, 第三个Verify卡片返回63C0, GAC中9F10应正确, Mac应计算正确。交易3中, Select命令返回6283, Verify命令返回6984, GAC命令返回AAC, GAC中9F10应正确, Mac应计算正确, 应用解锁命令返回9000, PINUnblock命令返回9000。交易4中, Select命令返回9000, Verify卡片返回9000, GAC1卡片返回9000, 返回CID=80, 发卡行认证卡片返回9000, GAC2卡片返回9000, 返回CID=40。

8.7.4 ECV004

测试目的: 明文PIN锁定的处理。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;

- b) Verify 正确的 PIN;
- c) put data 9F79;
- d) 交易 2: 电子现金交易;
- e) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- f) GET DATA 9F79;
- g) GET DATA 9F6D;
- h) Verify 连续 3 次错误的 PIN=12345;
- i) 第一个 GAC 请求 AAC;
- j) 交易 3: GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- k) Verify 正确的 PIN=1234;
- l) 第一个 GAC 请求 TC;
- m) 发卡行认证, 正确 ARPC;
- n) 应用解锁命令, 正确 mac;
- o) 交易 4: GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- p) 第一个 GAC 请求 TC;
- q) 交易 5: GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- r) 第一个 GAC 请求 ARQC;
- s) 发卡行认证, 正确 mac;
- t) PIN 解锁命令;
- u) 交易 6: GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- v) Verify 正确 pin;
- w) get data 9F6D;
- x) GET DATA 9F79;
- y) 第一个 GAC 请求 TC;
- z) 第二个 GAC 请求 TC。

通过标准: 交易2中, GP0的响应包含电子现金 AIP= '58 00', 第一个Verify卡片返回63C2,

第二个 Verify 卡片返回 63C1, 第三个 Verify 卡片返回 63C0, GAC 中 9F10 应正确, Mac 应计算正确。交易 3 中, Select 命令返回 6283, Verify 命令返回 6984, GAC 命令返回 AAC, GAC 中 9F10 应正确, Mac 应计算正确, 应用解锁命令返回 9000。交易 4 中, Select 命令返回 9000, 卡片返回的 AIP=7C00, GAC1 卡片返回 9000, 返回 CID=00, CVR=03804010。交易 5 中, GAC1 卡片返回 9000, 返回 CID=00, 发卡行认证卡片返回 9000, PIN 解锁命令返回 9000。交易 6 中, Verify 卡返回 9000, 第一个 GAC, 卡返回 TC, GAC 中 9F10 应正确, Mac 应计算正确。

8.7.5 ECV005

测试目的: 明文PIN锁定的处理。

测试条件: 卡特征30, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;

b) Verify 正确的 PIN;

c) put data 9F79=000000001000;

d) 交易 2: 电子现金交易;

e) 选择应用;

f) GP0 电子现金终端指示器=01 , 授权金额为 2.00;

g) GET DATA 9F79;

h) GET DATA 9F6D;

i) Verify 错误的 PIN=12345;

j) Verify 错误的 PIN=12345;

k) Verify 错误的 PIN=12345;

l) 第一个 GAC 请求 TC;

m) 交易 3: 选择应用 ;

n) GP0 电子现金终端指示器=01 , 授权金额为 2.00;

o) GET DATA 9F17;

p) 第一个 GAC 请求 TC;

q) 发卡行认证, 正确 mac;

r) 第二个 GAC 请求 TC, 授权响应码 3030;

s) PIN 解锁, mac 正确;

t) 交易 4: 电子现金交易;

u) 选择应用;

v) GP0 电子现金终端指示器=01 , 授权金额为 5.00;

w) GET DATA 9F79;

x) GET DATA 9F6D;

y) Verify PIN=1234;

z) 第一个 GAC 请求 TC。

通过标准: 交易1中, GP0响应的AIP=7D 00。交易2中, GP0的响应包含电子现金 AIP= '7C 00', GET DATA 9F79=000000001000, 第一个 Verify 卡片返回 63C2, 第二个 Verify 卡片返回 63C1, 第三个 Verify 卡片返回 63C0, GAC 返回 9000, 响应的 CID=40, GAC 中 9F10 应正确, Mac 应计算正确。交易 3 中, 第一个 GAC 命令卡返回 CID=80, GAC 中 9F10 应正确, Mac 应计算正确, 第二个 GAC 命令卡返回 CID=40, PIN 解锁命令返回 9000, GAC 中 9F10 应正确, Mac 应计算正确。交易 4 中, verify 返回 9000, GAC 命

令卡返回 CID=40, GAC 中 9F10 应正确, Mac 应计算正确。

8.7.6 ECV006

测试目的: 明文PIN锁定的处理。

测试条件: 卡特征30, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00, put data 9F79=000000001000;

b) 交易 2: 电子现金交易;

c) GP0 电子现金终端指示器=01 , 授权金额为 2.00;

d) GET DATA 9F79;

e) GET DATA 9F6D;

f) Verify 连续 3 次错误的 PIN=12345;

g) 第一个 GAC 请求 TC;

h) 交易 3: GP0 电子现金终端指示器=01 , 授权金额为 2.00;

i) 第一个 GAC 请求 TC;

j) 第二个 GAC 请求 TC, 授权响应码 5933;

k) 交易 4: 电子现金交易;

l) GP0 电子现金终端指示器=01 , 授权金额为 5.00;

m) GET DATA 9F79;

n) GET DATA 9F6D;

o) Verify PIN=1234;

p) 第一个 GAC 请求 TC;

q) 发卡行认证, 正确 mac;

r) 第二个 GAC 请求 TC, 授权响应码 3030;

s) PIN 解锁, mac 正确;

t) 交易 5: 电子现金交易;

u) GP0 电子现金终端指示器=01 , 授权金额为 5.00;

v) GET DATA 9F79;

w) GET DATA 9F6D;

x) Verify PIN=1234;

y) 第一个 GAC 请求 TC。

通过标准: 交易1中, GP0响应的AIP=7D 00。交易2中, GP0的响应包含电子现金 AIP= '7C 00', GET DATA 9F79=000000001000, 第一个 Verify 卡片返回 63C2, 第二个 Verify 卡片返回 63C1, 第三个 Verify 卡片返回 63C0, GAC 返回 9000, 响应的 CID=40, GAC 中 9F10 应正确, Mac 应计算正确。交易 3 中, Select 命令返回 9000, 第一个 GAC 命令卡返回 CID=80, GAC 中 9F10 应正确, Mac 应计算正确, 第二个 GAC 命令卡应返回 CID=00, GAC 中 9F10 应正确, Mac 应计算正确。交易 4 中, verify 卡返回 6984, 第一个 GAC 命令卡返回 CID=80, GAC 中 9F10 应正确, Mac 应计算正确, 第二个 GAC 命令卡返回 CID=40, PIN 解锁命令返回 9000。交易 5 中, Verify 返回 9000, GAC 返回 9000, CID=40, GAC 中 9F10 应正确, Mac 应计算正确。

8.8 卡片行为分析 (ECA)

8.8.1 ECA001

测试目的：确保电子现金卡跳过上次联机授权未完成检查。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00；
 b) Verify 正确的 PIN；
 c) put data 9F79=000000001000；
 d) 交易 2：联机授权未完成；
 e) 选择应用；
 f) GP0 电子现金终端指示器=00，授权金额为 2.00；
 g) Verify PIN；
 h) 第一个 GAC 请求 ARQC（发完此命令后，开始一笔交易）；
 i) 交易 3：电子现金交易；
 j) 选择应用；
 k) GP0 电子现金终端指示器=01，授权金额为 2.00；
 l) Verify PIN；
 m) 第一个 GAC 请求 TC。

通过标准：交易1中，修改余额成功。交易2中，GP0返回的AIP为7C00。交易3中，GP0返回的AIP为5800，GP0返回的AFL指定的记录中包含9F74，GAC中9F10应正确。

8.8.2 ECA002

测试目的：确保电子现金卡跳过上次联机授权未完成检查。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00；
 b) Verify 正确的 PIN；
 c) put data 9F79=000000001000；
 d) 交易 2：联机授权未完成；
 e) 选择应用；
 f) GP0 电子现金终端指示器=00，授权金额为 2.00；
 g) Verify PIN；
 h) 第一个 GAC 请求 ARQC；
 i) 第二个 GAC 请求 TC，ARC=5933；
 j) 交易 3：电子现金交易；
 k) 选择应用；
 l) GP0 电子现金终端指示器=01，授权金额为 2.00；
 m) Verify PIN；
 n) 第一个 GAC 请求 TC。

通过标准：交易1中，修改余额成功。交易2中，GP0返回的AIP为7C00。交易3中，GP0返回的AIP为5800，GP0返回的AFL指定的记录中包含9F74，GAC中9F10应正确。

8.8.3 ECA003

测试目的：电子现金交易跳过新卡的处理。

测试条件：卡特征29，新卡，支持电子现金。

测试流程：a) 交易1：电子现金交易。
 b) GP0 电子现金终端指示器=01，授权金额为 2.00；

- c) GET DATA 9F13;
- d) GET DATA 9F36;
- e) GET DATA 9F79;
- f) GET DATA 9F6D;
- g) Verify PIN=1234;
- h) 第一个 GAC 请求 TC;
- i) 交易 2: 电子现金交易;
- j) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- k) GET DATA 9F13;
- l) GET DATA 9F36;
- m) GET DATA 9F79;
- n) GET DATA 9F6D;
- o) Verify PIN=1234;
- p) 第一个 GAC 请求 TC;
- q) 交易 3: GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- r) Verify PIN=1234;
- s) 第一个 GAC 请求 TC;
- t) 发卡行认证, 正确 mac;
- u) 第二个 GAC 请求 TC, 授权响应码 3030;
- v) 交易 4: 电子现金交易;
- w) GP0 电子现金终端指示器=01 , 授权金额为 5.00;
- x) GET DATA 9F13, GET DATA 9F36;
- y) Verify PIN;
- z) 第一个 GAC 请求 TC。

通过标准: 交易1中, GP0响应的AIP=58 00, GET DATA 9F36返回0001, GET DATA 9F13返回0000, GET DATA 9F79 返回 00 00 00 00 20 00, Verify 返回 9000, 第一个 GAC 返回 9000, CID=40, GAC 中 9F10 应正确, Mac 应计算正确。交易 2 中, GP0 响应的 AIP=58 00, GET DATA 9F13 返回 0000, GET DATA 9F79 返回 00 00 00 00 18 00, GET DATA 9F36 返回值=交易 1 中 GET DATA 9F36 返回值+1, 第一个 GAC 返回 9000, CID=40, GAC 中 9F10 应正确, Mac 应计算正确。交易 3 中, 第一个 GAC 命令卡返回 CID=80, GAC 中 9F10 应正确, Mac 应计算正确, 第二个 GAC 命令卡返回 CID=40, GAC 中 9F10 应正确, Mac 应计算正确。交易 4 中, GET DATA 9F13 返回值应= GET DATA 9F36 返回值-1, 第一个 GAC 命令卡返回 CID=40, GAC 中 9F10 应正确。

8.8.4 ECA004

测试目的: 电子现金交易跳过新卡的处理。

测试条件: 卡特征30, 新卡, 支持电子现金。

测试流程: a) 交易1: 电子现金交易。

- b) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- c) GET DATA 9F13;
- d) GET DATA 9F36;
- e) GET DATA 9F79;
- f) GET DATA 9F6D;

- g) Verify PIN=1234;
- h) 第一个 GAC 请求 TC;
- i) 交易 2: 电子现金交易;
- j) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- k) GET DATA 9F13;
- l) GET DATA 9F36;
- m) GET DATA 9F79;
- n) GET DATA 9F6D;
- o) Verify PIN=1234;
- p) 第一个 GAC 请求 ARQC;
- q) 第二个 GAC 请求 TC. 授权响应码为 5933 (Y3) ;
- r) 交易 3: GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- s) 第一个 GAC 请求 ARQC;
- t) 第二个 GAC 请求 TC, 授权响应码为 5933 (Y3) ;
- u) 交易 4 : GP0 电子现金终端指示器=00 , 授权金额为 5.00;
- v) GET DATA 9F13;
- w) GET DATA 9F36;
- x) 第一个 GAC 请求 TC;
- y) 发卡行认证;
- z) 第二个 GAC 请求 TC, 授权响应码 3030。

通过标准: 交易1中, GP0响应的AIP=7C 00, GET DATA 9F36返回0001, GET DATA 9F79返回00 00 00 20 00, Verify 返回9000, 第一个GAC返回9000, CID=40, GAC中9F10应正确, Mac 应计算正确。交易 2 中, GP0 响应的 AIP=7C 00, GET DATA 9F13 返回 0000, GET DATA 9F79 返回 00 00 00 00 18 00, GET DATA9F36 返回值=交易 1 中 GET DATA9F36 返回值+1, 第一个 GAC 返回 9000, CID=80, GAC 中 9F10 应正确, Mac 应计算正确, 第二个 GAC 返回 9000, CID=00, GAC 中 9F10 应正确, Mac 应计算正确。交易 3 中, 第一个 GAC 命令卡返回 CID=80, GAC 中 9F10 应正确, Mac 应计算正确, 第二个 GAC 命令卡返回 CID=00, GAC 中 9F10 应正确, Mac 应计算正确。交易 4 中, GET DATA 9F13 返回值应=0000, 第一个 GAC 命令卡返回 CID=80。

8.8.5 ECA005

测试目的: 确保电子现金卡执行上次交易SDA失败检查。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;

- b) Verify 正确的 PIN;
- c) put data 9F79=000000001000;
- d) 交易 2: SDA 失败的脱机拒绝交易;
- e) 选择应用 ;
- f) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- g) Verify PIN;
- h) 第一个 GAC 请求 AAC (TVR=4000000000) ;
- i) 交易 3: 电子现金交易;
- j) 选择应用 ;

- k) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- l) Verify PIN;
- m) 第一个 GAC 请求 TC;
- n) 交易 4: 电子现金交易;
- o) 选择应用;
- p) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- q) Verify PIN;
- r) 第一个 GAC 请求 TC。

通过标准: 交易1中, 修改余额成功。交易2中, GP0返回的AIP为7C00。交易3中, GP0返回的AIP为5800, GP0返回的AFL指定的记录中包含9F74, GAC响应正确。交易4中, GP0返回的AIP为5800, GP0返回的AFL指定的记录中包含9F74, GAC响应正确。

8.8.6 ECA006

测试目的: 确保电子现金卡执行上次交易SDA失败检查。

测试条件: 卡特征29, 支持电子现金。

- 测试流程:
- a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;
 - b) Verify 正确的 PIN;
 - c) put data 9F79=000000001000;
 - d) 交易 2: SDA 失败的脱机拒绝交易;
 - e) 交易 3: 电子现金交易;
 - f) 选择应用;
 - g) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
 - h) Verify PIN;
 - i) 第一个 GAC 请求 TC;
 - j) 交易 4: 电子现金交易;
 - k) 选择应用;
 - l) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
 - m) Verify PIN;
 - n) 第一个 GAC 请求 TC。

通过标准: 交易1中, 修改余额成功。交易2中, GP0返回的AIP为7C00。交易3中, GP0返回的AIP为5800, GP0返回的AFL指定的记录中包含9F74, GAC响应正确。交易4中, GP0返回的AIP为5800, GP0返回的AFL指定的记录中包含9F74, GAC响应正确。

8.8.7 ECA007

测试目的: 确保电子现金卡执行上次交易DDA失败检查。

测试条件: 卡特征30, 支持电子现金。

- 测试流程:
- a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;
 - b) Verify 正确的 PIN;
 - c) put data 9F79=000000001000;
 - d) 交易 2: DDA 失败的脱机拒绝交易;
 - e) 交易 3: 电子现金交易;
 - f) 选择应用 ;
 - g) GP0 电子现金终端指示器=01 , 授权金额为 2.00;

- h) Verify PIN;
- i) 第一个 GAC 请求 TC;
- j) 交易 4: 电子现金交易;
- k) 选择应用 ;
- l) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- m) Verify PIN;
- n) 第一个 GAC 请求 TC。

通过标准: 交易1中, 修改余额成功。交易2中, GP0返回的AIP为7D00。交易3中, GP0返回的AIP为7C00, GP0返回的AFL指定的记录中包含9F74, GAC响应正确。交易4中, GP0返回的AIP为7C00, GP0返回的AFL指定的记录中包含9F74, GAC响应正确。

8.8.8 ECA008

测试目的: 确保电子现金卡执行上次交易DDA失败检查。

测试条件: 卡特征30, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;

- b) Verify 正确的 PIN;
- c) put data 9F79=000000001000;
- d) 交易 2: SDA 失败的脱机拒绝交易;
- e) 交易 3: 电子现金交易;
- f) 选择应用 ;
- g) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- h) Verify PIN;
- i) 第一个 GAC 请求 TC;
- j) 交易 4: 电子现金交易;
- k) 选择应用 ;
- l) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- m) Verify PIN;
- n) 第一个 GAC 请求 TC;
- o) 交易 5: 借记贷记交易;
- p) 选择应用 ;
- q) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- r) Verify PIN;
- s) 第一个 GAC 请求 TC;
- t) External Authentication;
- u) 第二个 GAC 请求 TC;
- v) 交易 6: 电子现金交易;
- w) 选择应用 ;
- x) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- y) Verify PIN;
- z) 第一个 GAC 请求 TC。

通过标准: 交易1中, 修改余额成功。交易2中, GP0返回的AIP为7D00。交易3中, GP0返回的AIP为7C00, GP0返回的AFL指定的记录中包含9F74, GAC响应正确。交易4中, GP0返回的AIP为7C00, GP0返回的AFL指定的记录中包含9F74, GAC响应正确。交易5中, GP0返回

的AIP为7D00，GAC响应正确。交易6中，GP0返回的AIP为7C 00，GP0返回的AFL指定的记录中包含9F74，GAC响应正确。

8.8.9 ECA009

测试目的：确保电子现金卡不执行连续脱机交易下限的处理。

测试条件：卡特征29，支持电子现金。

测试流程：a) 交易1：发卡行认证成功的联机交易，终端电子现金支持指示器=00；

b) Verify 正确的PIN；

c) put data 9F79=000000002000；

d) 交易2：电子现金交易；

e) 选择应用；

f) GP0 电子现金终端指示器=01，授权金额为2.00；

g) GET DATA 9F79；

h) GET DATA 9F6D；

i) Verify PIN=1234；

j) 第一个GAC请求TC；

k) 交易3：电子现金交易；

l) 选择应用；

m) GP0 电子现金终端指示器=01，授权金额为2.00；

n) GET DATA 9F79；

o) GET DATA 9F6D；

p) Verify PIN=1234；

q) 第一个GAC请求TC；

r) 交易4：电子现金交易；

s) 选择应用；

t) GP0 电子现金终端指示器=01，授权金额为2.00；

u) GET DATA 9F79；

v) GET DATA 9F6D；

w) Verify PIN=1234；

x) 第一个GAC请求TC；

y) 交易5：电子现金交易；

z) 选择应用；

aa) GP0 电子现金终端指示器=01，授权金额为2.00；

ab) GET DATA 9F79；

ac) GET DATA 9F6D；

ad) Verify PIN=1234；

ae) 第一个GAC请求TC；

af) 交易6：借记贷记交易；

ag) 选择应用；

ah) GP0 电子现金终端指示器=00，授权金额为2.00；

ai) Verify PIN=1234；

aj) 第一个GAC请求TC(不发第二个GAC)。

通过标准：交易1中，GP0响应的AIP=7C 00。交易2中，GP0的响应包含电子现金 AIP= '58 00'，

GET DATA 9F79=000000002000, 第一个 GAC 返回 9000, 响应的 CID=40, GAC 响应正确, Mac 应计算正确。交易 3 中, GP0 的响应包含电子现金 AIP= '58 00', GET DATA 9F79=000000001800, 第一个 GAC 返回 9000, 响应的 CID=40, GAC 响应正确, Mac 应计算正确。交易 4 中, GP0 的响应包含电子现金 AIP= '58 00', GET DATA 9F79=000000001600, 第一个 GAC 返回 9000, 响应的 CID=40, GAC 响应正确, Mac 应计算正确。交易 5 中, GP0 的响应包含电子现金 AIP= '58 00', GET DATA 9F79=000000001400, 第一个 GAC 返回 9000, 响应的 CID=40, GAC 响应正确, Mac 应计算正确。交易 6 中, GP0 的响应包含电子现金 AIP= '7C 00', 第一个 GAC 返回 9000, 响应的 CID=80, GAC 响应正确, Mac 应计算正确。

8.8.10 ECA010

测试目的: 确保电子现金卡不执行连续脱机交易下限的处理。

测试条件: 卡特征30, 支持电子现金。

测试流程: a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;

b) Verify 正确的 PIN;

c) put data 9F79=000000002000;

d) 交易 2: 电子现金交易;

e) 选择应用 ;

f) GP0 电子现金终端指示器=01 , 授权金额为 2.00;

g) ET DATA 9F79;

h) GET DATA 9F6D;

i) Verify PIN=1234;

j) 第一个 GAC 请求 TC;

k) 交易 3: 电子现金交易;

l) 选择应用 ;

m) GP0 电子现金终端指示器=01 , 授权金额为 2.00;

n) GET DATA 9F79;

o) GET DATA 9F6D;

p) Verify PIN=1234;

q) 第一个 GAC 请求 TC;

r) 交易 4: 电子现金交易;

s) 选择应用 ;

t) GP0 电子现金终端指示器=01 , 授权金额为 2.00;

u) GET DATA 9F79;

v) GET DATA 9F6D;

w) Verify PIN=1234;

x) 第一个 GAC 请求 TC;

y) 交易 5: 电子现金交易;

z) 选择应用 ;

aa) GP0 电子现金终端指示器=01 , 授权金额为 2.00;

ab) GET DATA 9F79;

ac) GET DATA 9F6D;

ad) Verify PIN=1234;

- ae) 第一个 GAC 请求 TC;
- af) 交易 6: 借记贷记交易;
- ag) 选择应用 ;
- ah) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- ai) Verify PIN=1234;
- aj) 第一个 GAC 请求 TC(不发第二个 GAC)。

通过标准: 交易1中, GP0响应的AIP=7C 00。交易2中, GP0的响应包含电子现金 AIP= '58 00', GET DATA 9F79=000000002000, 第一个 GAC 返回 9000, 响应的 CID=40, GAC 响应正确, Mac 应计算正确。交易 3 中, GP0 的响应包含电子现金 AIP= '58 00', GET DATA 9F79=000000001800, 第一个 GAC 返回 9000, 响应的 CID=40, GAC 响应正确, Mac 应计算正确。交易 4 中, GP0 的响应包含电子现金 AIP= '58 00', GET DATA 9F79=000000001600, 第一个 GAC 返回 9000, 响应的 CID=40, GAC 响应正确, Mac 应计算正确。交易 5 中, GP0 的响应包含电子现金 AIP= '58 00', GET DATA 9F79=000000001400, 第一个 GAC 返回 9000, 响应的 CID=40, GAC 响应正确, Mac 应计算正确。交易 6 中, GP0 的响应包含电子现金 AIP= '7C 00', 第一个 GAC 返回 9000, 响应的 CID=80, GAC 响应正确, Mac 应计算正确。

8.8.11 ECA011

测试目的: 发卡行认证失败的处理。

测试条件: 卡特征30, 支持电子现金。

- 测试流程:
- a) 交易1: 发卡行认证成功的联机交易, 终端电子现金支持指示器=00;
 - b) Verify 正确的 PIN;
 - c) put data 9F79=000000001000;
 - d) 交易 2: 电子现金交易;
 - e) 选择应用 ;
 - f) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
 - g) Verify PIN=1234;
 - h) 第一个 GAC 请求 ARQC;
 - i) 发卡行认证, 错误的 mac;
 - j) 第二个 GAC 请求 TC, 授权响应码 3030。

通过标准: 交易1中, GP0响应的AIP=7D 00。交易2中, GP0的响应包含电子现金 AIP= '7D 00', GET DATA 9F79=000000001000, 发卡行认证卡返回 6300, 第二个 GAC 返回 9000, 响应的 CID=00, 第二个 GAC 响应正确, Mac 应计算正确。

8.8.12 ECA012

测试目的: 电子现金交易无法正常联机时, 执行新卡检查。

测试条件: 卡特征29, 新卡, 支持电子现金。

- 测试流程:
- a) 交易1: 电子现金交易;
 - b) 选择应用 ;
 - c) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
 - d) GET DATA 9F13;
 - e) GET DATA 9F36;
 - f) GET DATA 9F79;

- g) GET DATA 9F6D;
- h) Verify PIN=1234;
- i) 第一个 GAC 请求 TC;
- j) 交易 2: 电子现金交易;
- k) 选择应用 ;
- l) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- m) GET DATA 9F13;
- n) GET DATA 9F36;
- o) GET DATA 9F79;
- p) GET DATA 9F6D;
- q) Verify PIN=1234;
- r) 一个 GAC 请求 ARQC;
- s) 二个 GAC 请求 TC (ARC=5933) 。

通过标准: 交易1中, GP0响应的AIP=58 00, GET DATA 9F13返回0000, GET DATA 9F79返回00 00 00 00 20 00, 第一个GAC返回9000, CID=40, GAC响应正确, Mac应计算正确。交易2中, GP0响应的AIP=58 00, GET DATA 9F13返回0000, 第一个GAC返回9000, CID=80, GAC响应正确, Mac应计算正确, 第二个GAC返回9000, CID=40, GAC响应正确, Mac应计算正确。

8.8.13 ECA013

测试目的: 电子现金交易无法正常联机时, 执行新卡检查。

测试条件: 卡特征30, 新卡, 支持电子现金。

- 测试流程:
- a) 交易1: 电子现金交易;
 - b) 选择应用 ;
 - c) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
 - d) GET DATA 9F13;
 - e) GET DATA 9F36;
 - f) GET DATA 9F79;
 - g) GET DATA 9F6D;
 - h) Verify PIN=1234;
 - i) 第一个 GAC 请求 TC;
 - j) 交易 2: 电子现金交易;
 - k) 选择应用 ;
 - l) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
 - m) GET DATA 9F13;
 - n) GET DATA 9F36;
 - o) GET DATA 9F79;
 - p) GET DATA 9F6D;
 - q) Verify PIN=1234;
 - r) 第一个 GAC 请求 ARQC;
 - s) 第二个 GAC 请求 TC (ARC=5933) 。

通过标准: 交易1中, GP0响应的AIP=7C 00, GET DATA 9F13返回0000, GET DATA 9F79返回00 00 00 00 20 00, 第一个GAC返回9000, CID=40, GAC中9F10应正确, Mac应计算正确。

交易 2 中, GPO 响应的 AIP=7C 00, GET DATA 9F13 返回 0000, 第一个 GAC 返回 9000, CID=80, GAC 响应正确, Mac 应计算正确, 第二个 GAC 返回 9000, CID=00, GAC 响应正确, Mac 应计算正确。

8.9 防插拔 (EFB)

8.9.1 EFB001

测试目的: 在执行GAC作时模拟断电操作, 然后判断余额正确。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 进行电子现金交易。

通过标准: 如GAC响应9000, 余额应正常扣取, 否则应保持不变。

8.9.2 EFB002

测试目的: 在执行圈存操作时模拟断电操作, 然后判断圈存日志记录和圈存操作保持一致。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 进行电子现金圈存交易。

通过标准: 如脚本响应9000, 余额应正常增加, 圈存日志应正常保存, 否则应保持不变。

8.10 特殊流程 (ATM)

8.10.1 ATM001

测试目的: 标准借贷记交易时, 若终端在GAC命令中给出的授权金额与GPO命令中给出的授权金额不一致, 或终端在GAC命令中给出的交易货币码与GPO命令中给出的交易货币代码不一致, 或上述两种数据均不一致时, 卡片应以GAC时的数据为准正常完成交易。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 交易 1: 授权金额不一致;

b) 交易 2: 交易货币代码不一致;

c) 交易 3: 授权金额与应用货币代码均不一致。

通过标准: 在交易1、交易2、交易3中, 第一次GAC卡片均返回ARQC, 状态字为9000, 第二次GAC卡片均返回TC, 状态字为9000。

8.10.2 ATM002

测试目的: 若卡片在GPO命令时判定为电子现金交易, 若终端在GAC命令中给出的授权金额与GPO命令中给出的授权金额不一致, 或终端在GAC命令中给出的交易货币码与GPO命令中给出的交易货币代码不一致, 或上述两种数据均不一致时, 当终端请求脱机批准时, 卡片以GPO时的数据为准拒绝交易; 当终端请求联机时, 卡片应以GAC时的数据为准正常完成交易。

测试条件: 卡特征29, 支持电子现金。

测试流程: a) 交易 1: 授权金额不一致, 终端请求联机;

b) 交易 2: 授权金额不一致 (1), 终端请求脱机批准;

c) 交易 3: 授权金额不一致 (2), 终端请求脱机批准;

d) 交易 4: 交易货币代码不一致, 终端请求联机;

e) 交易 5: 交易货币代码不一致, 终端请求脱机批准;

f) 上电;

g) 选择应用 ;

- h) GP0 9F02=00 00 00 00 02 00, 5F2A=0156, 9F7A=01;
- i) 第一次 GAC 请求 TC, 9F02=00 00 00 00 02 00, 5F2A=0344;
- j) 交易 6: 授权金额与应用货币代码均不一致, 终端请求联机;
- k) 上电;
- l) 选择应用 ;
- m) GP0 9F02=00 00 00 00 00 00, 5F2A=0000, 9F7A=01;
- n) 第一次 GAC 请求 ARQC, 9F02=00 00 00 00 02 00, 5F2A=0156;
- o) 第二次 GAC 请求 TC;
- p) 交易 7: 授权金额与应用货币代码均不一致, 终端请求脱机批准 (1);
- q) 上电;
- r) 选择应用 ;
- s) GP0 9F02=00 00 00 00 00 00, 5F2A=0156, 9F7A=01;
- t) 第一次 GAC 请求 TC, 9F02=00 00 00 00 02 00, 5F2A=0344;
- u) 交易 8: 授权金额与应用货币代码均不一致, 终端请求脱机批准 (2);
- v) 上电;
- w) 选择应用 ;
- x) GP0 9F02=00 00 00 00 01 00, 5F2A=0156, 9F7A=01;
- y) 第一次 GAC 请求 TC, 9F02=00 00 00 00 02 00, 5F2A=0344。

通过标准: 在交易1、交易4、交易6中, 第一次GAC卡片返回ARQC, 状态字为9000, 第二次GAC卡片返回TC, 状态字为9000。在交易2、交易3、交易5、交易7、交易8中, 第一次GAC卡片返回ARQC, 状态字为9000, 第二次GAC卡片返回TC, 状态字为9000。

8.11 电子现金圈存日志

8.11.1 ELD001

测试目的: 电子现金交易执行 现金充值交易, 卡片应能正确记录日志信息并能正确读取。

测试条件: 卡特征29。

测试流程: a) 交易1: 标准借贷记交易;

- b) 选择应用 ;
- c) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- d) Verify PIN=1234;
- e) 第一个 GAC 请求 ARQC;
- f) 第二个 GAC 请求 TC;
- g) 交易 2: 选择应用 ;
- h) GET DATA 9F79;
- i) 交易 3: 电子现金交易;
- j) 选择应用 ;
- k) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- l) 第一个 GAC 请求 ARQC (电子现金 现金圈存);
- m) 二个 GAC 请求 TC (ARC=3030);
- n) PUT DATA 9F79 99.00;
- o) 交易 4: 选择应用;
- p) GET DATA 9F79;
- q) 交易 5: 读记录方式读取第一条日志记录;

r) 批读取方式读取记录。

通过标准：交易5中，日志记录中的 P1 P2 9F79前值和终值 应该与实际相符（包括单条读取模式和批读取模式）。

8.11.2 ELD002

测试目的：电子现金交易执行 查正常的交易日志，应有该笔交易记录。

测试条件：卡特征29。

测试流程：a) 交易1：标准借贷记交易；

b) 选择应用；

c) GP0 电子现金终端指示器=00，授权金额为 2.00；

d) Verify PIN=1234；

e) 一个 GAC 请求 ARQC；

f) 第二个 GAC 请求 TC；

g) 交易 2：选择应用；

h) GET DATA 9F79；

i) 交易 3：电子现金交易；

j) 选择应用；

k) GP0 电子现金终端指示器=01，授权金额为 2.00；

l) 第一个 GAC 请求 ARQC（电子现金非指定账户圈存交易）；

m) 第二个 GAC 请求 TC（ARC=3030）；

n) PUT DATA 9F79 99.00；

o) 交易 4：选择应用；

p) GET DATA 9F79；

q) 交易 5：读记录方式读取第一条日志记录；

r) 批读取方式读取记录；

s) 交易 6：选择应用；

t) 读交易日志，入口 9F4D。

通过标准：交易5中，日志记录中的 P1 P2 9F79前值和终值 应该与实际相符（包括单条读取模式和批读取模式）。交易6中，日志中有交易3的记录。

8.11.3 ELD003

测试目的：电子现金交易执行，圈存交易日志不能被更新。

测试条件：卡特征29。

测试流程：a) 交易1：标准借贷记交易；

b) 选择应用；

c) GP0 电子现金终端指示器=00，授权金额为 2.00；

d) Verify PIN=1234；

e) 第一个 GAC 请求 ARQC；

f) 第二个 GAC 请求 TC；

g) 交易 2：选择应用；

h) GET DATA 9F79；

i) 交易 3：电子现金交易；

j) 选择应用；

- k) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- l) 第一个 GAC 请求 ARQC (电子现金指定账户圈存交易);
- m) 第二个 GAC 请求 TC (ARC=3030);
- n) PUT DATA 9F79 99.00;
- o) 交易 4: 选择应用 ;
- p) GET DATA 9F79;
- q) 交易 5: 读记录方式读取第一条日志记录;
- r) 批读取方式读取记录;
- s) 交易 6: 选择应用;
- t) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- u) 第一个 GAC 请求 ARQC (电子现金指定账户圈存交易);
- v) 第二个 GAC 请求 TC (ARC=3030);
- w) 脚本命令, 更新交易日志记录。

通过标准: 交易5中, 日志记录中的 P1 P2 9F79前值和终值 应该与实际相符 (包括单条读取模式和批读取模式)。交易6中, 更新交易日志记录不成功。

8.11.4 ELD004

测试目的: 电子现金交易执行 消费交易, 并更改9F79, 卡片应能正确记录日志信息并能正确读取, 同时电子现金圈存日志文件应不能通过update record进行更新。

测试条件: 卡特征29。

测试流程: a) 交易1: 标准借贷记交易;

- b) 选择应用 ;
- c) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- d) Verify PIN=1234;
- e) 第一个 GAC 请求 ARQC;
- f) 第二个 GAC 请求 TC;
- g) 交易 2: 选择应用 ;
- h) GET DATA 9F79;
- i) 交易 3: 电子现金交易;
- j) 选择应用 ;
- k) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- l) 第一个 GAC 请求 ARQC (00 消费交易);
- m) 第二个 GAC 请求 TC (ARC=3030);
- n) PUT DATA 9F79 99.00;
- o) 交易 4: 选择应用 ;
- p) GET DATA 9F79;
- q) 交易 5: 读记录方式读取第一条日志记录;
- r) 批读取方式读取记录。

通过标准: 交易5中, 日志记录中的 P1 P2 9F79前值和终值 应该与实际相符 (包括单条读取模式和批读取模式)。

8.11.5 ELD005

测试目的：电子现金交易执行圈存日志入口指定的上限的圈存交易，并更改9F79，卡片应能正确记录日志信息并能正确读取。

测试条件：卡特征29。

测试流程：a) 交易1：标准借贷记交易；
b) 选择应用；
c) GP0 电子现金终端指示器=00，授权金额为 2.00；
d) Verify PIN=1234；
e) 第一个 GAC 请求 ARQC；
f) 第二个 GAC 请求 TC；
g) 交易 2：选择应用；
h) GET DATA 9F79；
i) 交易 3：电子现金交易；
g) 选择应用；
k) GP0 电子现金终端指示器=01，授权金额为 2.00；
l) 第一个 GAC 请求 ARQC（63 圈存交易）；
m) 第二个 GAC 请求 TC（ARC=3030）；
n) PUT DATA 9F79 99.00；
o) 重复交易 3 至上限次数；
p) 交易 4：选择应用；
q) 读记录方式读取第一条日志记录；
r) 批读取方式读取记录；
s) 交易 5：选择应用；
t) GP0 电子现金终端指示器=01，授权金额为 2.00；
u) 第一个 GAC 请求 ARQC（63 圈存交易）；
v) 第二个 GAC 请求 TC（ARC=3030）；
w) 交易 6：选择应用；
x) 读记录方式读取第一条日志记录；
y) 批读取方式读取记录。

通过标准：交易4中，日志记录中的 P1 P2 9F79前值和终值 应该与实际相符（包括单条读取模式和批读取模式）。交易6中，日志更新正确，即仍然包括上限条圈存日志，最新一条记录信息为交易5的具体信息。

8.11.6 ELD006

测试目的：应用锁定后日志信息仍能读取，并且信息准确（请使用ELD005通过的卡片继续进行此案例）。

测试条件：卡特征29。

测试流程：a) 交易1：标准借贷记交易；
b) 选择应用；
c) GP0 电子现金终端指示器=00，授权金额为 2.00；
d) Verify PIN=1234；
e) 第一个 GAC 请求 ARQC；
f) 第二个 GAC 请求 TC；
g) 交易 2；选择应用；

- h) Verify PIN=1234;
- i) 第一个 GAC 请求 ARQC;
- j) 第二个 GAC 请求 TC;
- k) 执行 ApplicationBlock 命令;
- l) 交易 3; 选择应用 ;
- m) 读记录方式读取第一条日志记录;
- n) 批读取方式读取记录。

通过标准: 交易3中, 日志记录中的 P1 P2 9F79前值和终值 应该与实际相符 (包括单条读取模式和批读取模式)。

8.11.7 ELD007

测试目的: 异常情况 (put data 超过上限额) putdata 不成功应无日志保存。

测试条件: 卡特征29。

- 测试流程:
- a) 交易1: 标准借贷记交易;
 - b) 选择应用 ;
 - c) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
 - d) Verify PIN=1234;
 - e) 第一个 GAC 请求 ARQC;
 - f) 第二个 GAC 请求 TC;
 - g) 交易 2: 选择应用 ;
 - h) GET DATA 9F79;
 - i) 交易 3: 电子现金交易;
 - j) 选择应用 ;
 - k) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
 - l) 第一个 GAC 请求 ARQC (电子现金指定账户圈存交易);
 - m) 第二个 GAC 请求 TC (ARC=3030);
 - n) PUT DATA 9F79 101.00 put data 超过上限额;
 - o) 交易 4: 选择应用 ;
 - p) GET DATA 9F79;
 - q) 交易 5: 读记录方式读取第一条日志记录;
 - r) 批读取方式读取记录。

通过标准: 交易 5 中, 日志记录中应不包含上笔较易的相关数值。

8.11.8 ELD008

测试目的: 异常情况 (MAC错误) putdata 不成功应无日志保存。

测试条件: 卡特征29。

- 测试流程:
- a) 交易1: 标准借贷记交易;
 - b) 选择应用 ;
 - c) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
 - d) Verify PIN=1234;
 - e) 第一个 GAC 请求 ARQC;
 - f) 第二个 GAC 请求 TC;
 - g) 交易 2: 选择应用 ;

- h) GET DATA 9F79;
- i) 交易 3: 电子现金交易;
- j) 选择应用 ;
- k) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- l) 第一个 GAC 请求 ARQC (电子现金指定账户圈存交易);
- m) 第二个 GAC 请求 TC (ARC=3030);
- n) PUT DATA 9F79 99.00 (MAC 错误);
- o) 交易 4: 选择应用 ;
- p) GET DATA 9F79;
- q) 交易 5: 读记录方式读取第一条日志记录;
- r) 批读取方式读取记录。

通过标准: 交易 5 中, 日志记录中应不包含上笔较易的相关数值。

8.11.9 ELD009

测试目的: 异常情况 (put data 00) putdata 不成功应无日志保存。

测试条件: 卡特征 29。

测试流程: a) 交易 1: 标准借贷记交易;

- b) 选择应用;
- c) GP0 电子现金终端指示器=00 , 授权金额为 2.00;
- d) Verify PIN=1234;
- e) 第一个 GAC 请求 ARQC;
- f) 第二个 GAC 请求 TC;
- g) 交易 2: 选择应用;
- h) GET DATA 9F79;
- i) 交易 3: 选择应用;
- j) GP0 电子现金终端指示器=01 , 授权金额为 2.00;
- k) 第一个 GAC 请求 ARQC (电子现金指定账户圈存交易);
- l) 第二个 GAC 请求 TC (ARC=3030);
- m) PUT DATA 9F79 00.00;
- n) 交易 4: 选择应用 ;
- o) GET DATA 9F79;
- p) 交易 5: 读记录方式读取第一条日志记录;
- q) 批读取方式读取记录。

通过标准: 交易 5 中日志记录中的 P1 P2 9F79 前值和终值 应该与实际相符 (包括单条读取模式和批读取模式)。

9 个人化要求

9.1 概述

本部分第 9.2 条列出了个人化数据的公共部分, 称为基本特征, 第 9.5 条列出的每个个人化特征都继承于基本特征。可理解为 C++ 语言中的父类/基类。

本部分第 9.3 条列出了所有可能被用到的公钥证书、非对称公私钥对、对称密钥等信息。

本部分第 9.5 条列出了针对不同测试点所涉及的各种个人化数据, 称为卡片特征。卡片特征继承

自基本特征，可理解为 C++语言中的子类。

本部分第 9.4 条列出了卡片特征与选用的密钥之间的关系。

基本特征和卡片特征为测试时所必需的数据对象，可能并不能涵盖 JR/T 0025 规范中规定的所有数据对象，对于没有在此定义的数据对象，可自行为其赋值。

根据卡片功能的不同，可能不需要支持本部分中列出的全部卡片特征。表 38 列出了支持不同功能的卡片所应支持的卡片特征。

若送检的卡片仅支持双算法，则应为每种卡片特征准备两套个人化数据，这两套个人化数据的区别在于 PDOL，一个带有 DF69，另一个不带有 DF69。若送检的卡片仅支持一种算法（不论是国际还是国密），则只需为每种卡片特征准备一套个人化数据。

若送检的卡片支持双币，则应为每种卡片特征准备两套个人化数据，一套数据用于测试单币，另一套数据用于测试双币，两套个人化数据的主要区别在于 9F68 字节 1 指明的支持的脱机金额检查的类型不同。

若送检的卡片支持扩展，则应在保留前面已建立的个人化数据的基础上，再准备一套用于测试扩展应用的个人化数据。

表38 卡片支持的功能与卡片特征的对应关系

卡片支持的应用	送检时应准备的卡片特征
仅支持国际算法的卡片	
接触式借记/贷记	卡片特征 1 至卡片特征 27
接触式基于借记贷记应用的小额支付	卡片特征 29、30、51
快速借记/贷记	卡片特征 31 至卡片特征 45，卡片特征 48 和卡片特征 49，卡片特征 53 至卡片特征 55
非接触式小额支付扩展	卡片特征 31 至卡片特征 49，卡片特征 53 至卡片特征 55
非接触式借记/贷记	卡片特征 1 至卡片特征 27（加入 PPSE 并采用非接界面下的 PDOL 个人化数据）
非接触式基于借记贷记应用的小额支付	卡片特征 29、30、51（加入 PPSE 并采用非接界面下的 PDOL 个人化数据）
仅支持国密算法的卡片	
接触式借记/贷记	卡片特征 1 至卡片特征 27（采用非接界面下支持国密算法的 PDOL 个人化数据）
接触式基于借记贷记应用的小额支付	卡片特征 29 至卡片特征 30（加入 PPSE 并采用非接界面下的 PDOL 个人化数据）
快速借记/贷记	卡片特征 31 至卡片特征 45，卡片特征 48 和卡片特征 49
非接触式小额支付扩展	卡片特征 31 至卡片特征 47
非接触式借记/贷记	卡片特征 1 至卡片特征 27（加入 PPSE 并采用非接界面下支持国密算法的 PDOL 个人化数据）
非接触式基于借记贷记应用的小额支付	卡片特征 29 至卡片特征 30（加入 PPSE 并采用非接界面下支持国密算法的 PDOL 个人化数据）
支持国际算法和国密算法的卡片	
接触式借记/贷记	卡片特征 1 至卡片特征 28（与仅支持国密算法的卡片特征相比加入了国际对称与非对称算法相关的必备数据）
接触式基于借记贷记应用的小额支付	卡片特征 29 至卡片特征 30（与仅支持国密算法的卡片特征相比加入了国际对称与非对称算法相关的必备数据）

	卡片特征 51 和卡片特征 52
快速借记/贷记	卡片特征 31 至卡片特征 45, 卡片特征 48 和卡片特征 49, 卡片特征 53 至卡片特征 55
非接触式小额支付扩展	卡片特征 31 至卡片特征 49, 卡片特征 53 至卡片特征 55
非接触式借记/贷记	卡片特征 1 至卡片特征 28 (与仅支持国密算法的卡片特征相比加入了国际对称与非对称算法相关的必备数据)
非接触式基于借记贷记应用的小额支付	卡片特征 29 至卡片特征 30 (与仅支持国密算法的卡片特征相比加入了国际对称与非对称算法相关的必备数据) 卡片特征 51 和卡片特征 52

9.2 基本特征

9.2.1 借记/贷记基本特征

表 39 列出了支持借记/贷记功能的卡片的基本特征, 数据分组可由自行设计。但 SFI=1 的文件的 1 号记录除外, SFI 1 的 1 号记录应存储以下数据: 70 2C 57 11 62 28 00 01 00 00 11 17 D3 01 22 01 01 23 45 67 89 9F 1F 16 30 31 30 32 30 33 30 34 30 35 30 36 30 37 30 38 30 39 30 41 30 42。

表39 借记/贷记基本特征

数据元素	标签	数值
应用货币代码	9F51	01 56
应用货币代码	9F42	01 56
应用生效日期	5F25	95 07 01
应用失效日期	5F24	30 12 31
应用标识符	4F	A0 00 00 03 33 01 01
应用交互特征	82	5C 00
应用标签	50	50 42 4F 43 20 43 72 65 64 69 74
应用主帐号	5A	62 28 00 01 00 00 11 17
应用主帐号序列号	5F34	01
应用首选名称	9F12	43 41 52 44 20 49 4D 41 47 45 20 30 30 30 31
应用优先指示器	87	01
应用用途控制	9F07	FF C0
应用版本号	9F08	00 30
CDOL1	8C	9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9F 21 03 9C 01 9F 37 04
CDOL2	8D	8A 02 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9F 21 03 9C 01 9F 37 04
持卡人姓名	5F20	46 55 4C 4C 20 46 55 4E 43 54 49 4F 4E 41 4C
CVM 列表	8E	00 00 00 00 00 00 00 00 41 03 42 03 5E 03 43 03 1F 00
CA 公钥索引	8F	80
连续交易计数器 (国际)	--	00
连续交易限制数 (国际)	9F53	05
连续交易计数器 (国际-国家)	--	00
连续交易限制数 (国际-国家)	9F72	00

表 39 (续)

数据元素	标签	数值
密文版本号	--	01
累计交易金额		00 00 00 00 00 00
累计交易金额限制数	9F54	00 00 00 01 00 00
数据认证代码		DA C5
分散密钥索引	--	01
发卡行行为代码-缺省	9F0D	F0 20 04 00 00
发卡行行为代码-拒绝	9F0E	00 50 88 00 00
发卡行行为代码-联机	9F0F	F0 20 04 98 00
发卡行应用数据	9F10	07 01 01 03 00 00 00 xx
发卡行认证指示位	9F56	80
发卡行代码表索引	9F11	01
发卡行国家代码	5F28	01 56
发卡行国家代码	9F57	01 56
首选语言	5F2D	7A 68 65 6E 66 72 64 65
日志入口	9F4D	0B 0A
日志格式	9F4F	9A 03 9F 21 03 9F 02 06 9F 03 06 9F 1A 02 5F 2A 02 9F 4E 14 9C 01 9F 36 02
联机授权指示位	--	00
PDOL 接触界面 (若卡片不支持国密)	9F 38	9F 33 03 9F 4E 14
PDOL 非接触界面 (若卡片不支持国密)	9F 38	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 33 03 9F 4E 14 9F 7A 01
PDOL 接触界面 (若卡片支持国密)	9F 38	9F 33 03 9F 4E 14 DF 69 01
PDOL 非接触界面 (若卡片支持国密)	9F 38	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 33 03 9F 4E 14 9F 7A 01 DF 69 01
PIN尝试计数器	9F17	03
PIN尝试限制数	--	03
参考 PIN 数据	--	12 34
第二应用货币代码	9F76	00 00
服务码	5F30	02 01
磁道 1 自定义数据	9F1F	30 31 30 32 30 33 30 34 30 35 30 36 30 37 30 38 30 39 30 41 30 42
磁道 2 等效数据	57	62 28 00 01 00 00 11 17 D3 01 22 01 01 23 45 67 89
产品标识信息	9F63	11 22 33 44 55 66 77 88 00 00 00 00 00 00 00 00

如送检双算法借贷记片则除文中规定的双算法的个人化特征外应另附使用不支持国密的 PDOL 进行个人化(即 PDOL 中不带 DF6901)的 1-10 号卡特征文件。

9.2.2 基于借记贷记应用的小额支付基本特征

基于借记贷记应用的小额支付基本特征见表 40, 双币电子现金基本特征见表 41, 表 40 和表 41

中未定义的数据在表 39 中规定。9F10 中 IDD 的值选择长度 10 字节，ID 选择 0X01 类型。

表40 基于借记贷记应用的小额支付基本特征

数据	标签 — T	长度 — L	数值 — V
PDOL 接触界面 (若卡片不支持国密)	9F 38	0C	9F 1A 02 9F 7A 01 9F 02 06 5F 2A 02 9F 4E 14
PDOL 非接触界面 (若卡片不支持国密)	9F 38		9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 33 03 9F 4E 14 9F 7A 01
PDOL 接触界面 (若卡片支持国密)	9F 38	0C	9F 1A 02 9F 7A 01 9F 02 06 5F 2A 02 9F 4E 14 DF 69 01
PDOL 非接触界面 (若卡片支持国密)	9F 38		9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 33 03 9F 4E 14 9F 7A 01 DF 69 01
CVM 列表	8E	0A	00 00 00 00 00 00 00 00 01 00
电子现金余额	9F79	06	00 00 00 00 20 00
电子现金余额上限	9F77	06	00 00 00 01 00 00
电子现金发卡行授权码	9F74	06	45 43 43 31 31 31
电子现金单笔交易限额	9F78	06	00 00 00 00 10 00
电子现金重置阈值	9F6D	06	00 00 00 00 15 00
IAC-default	9F0D	05	7C 70 B8 08 00
IAC-denial	9F0E	05	7C 70 B8 08 00
IAC-online	9F0F	05	00 00 00 00 00
圈存日志入口	DF4D	2	0C 0A
圈存日志格式	DF4F	10	9A 03 9F 21 03 9F 1A 02 9F 4E 14 9C 01 9F 36 02
产品标识信息	9F63	10	11 22 33 44 55 66 77 88 00 00 00 00 00 00 00 00
发卡行应用数据	9F10	0x13	07 01 01 03 00 00 00 xx 0A 01 xx xx xx xx yy yy yy yy

表41 双币电子现金基本特征

数据	标签 — T	长度 — L	数值 — V
第二币种电子现金应用货币代码	DF71	02	03 44
第二币种电子现金余额 (EC Balance)	DF79	06	00 00 00 10 00 00
第二币种电子现金余额上限 (EC Balance Limit)	DF77	06	00 00 00 20 00 00
第二币种电子现金单笔交易限额 (EC Single Transaction Limit)	DF78	06	00 00 00 05 00 00
第二币种电子现金重置阈值 (EC Reset Threshold)	DF76	06	00 00 00 00 50 00
连续交易限制数 (国际-货币)	9F53	01	02
连续交易限制数 (国际-国家)	9F72	01	00

9.2.3 快速借记/贷记（又名 qPBOC）基本特征

读记录时卡片至少应返回以下数据，以下数据至少分四条记录存储：

- 93：签名的静态应用数据；
- 8F：CA 公钥索引；
- 90：发卡行公钥证书；
- 92：发卡行公钥余数；
- 9F32：发卡行公钥指数；
- 9F46：IC 卡公钥证书；
- 9F47：IC 卡公钥指数；
- 9F48：IC 卡公钥余数；
- 5F24：应用失效期；
- 5F25：应用生效期；
- 5A：应用主帐号；
- 9F74：电子现金发卡行授权码；
- 9F08：应用版本号。

表 42 定义了快速借记/贷记的基本特征，表 43 定义了双币快速借记/贷记的基本特征。

表42 快速借记/贷记基本特征

数据	标签 — T	长度 — L	数值 — V
电子现金余额	9F79	06	00 00 00 01 00 00
电子现金余额上限	9F77	06	00 00 00 01 50 00
电子现金发卡行授权码	9F74	06	45 43 43 31 31 31
电子现金单笔交易限额	9F78	06	00 00 00 00 10 00
电子现金重置阈值	9F6D	06	00 00 00 00 15 00
卡片交易属性	9F6C	02	30 00
卡片 CVM 限额	9F6B	06	00 00 00 00 05 00
PDOL 非接触式 (若卡片不支持国密)	9F38		9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04
PDOL 非接触式 (若卡片支持国密)	9F38		9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 DF 69 01
产品标识信息	9F63	10	11 22 33 44 55 66 77 88 00 00 00 00 00 00 00 00
连续交易限制数（国际-货币）	9F53	01	03
密文版本		01	0X01, 0X17
发卡行应用数据	9F10	0x13	07 01 01 03 00 00 00 xx 0A 01 xx xx xx xx yy yy yy yy
脱机可用余额	9F5D	06	00 00 00 00 00 01
应用交互特征（AIP）-快速借记 贷记路径	82	02	70 00
应用交互特征（AIP）-借记/贷记 路径	82	02	7C 00

表43 双币快速借记/贷记基本特征

数据	标签 — T	长度 — L	数值 — V
第二币种电子现金应用货币代码	DF71	02	03 44
第二币种卡片 CVM 限额	DF72	06	00 00 00 00 05 00
第二币种电子现金余额	DF79	06	00 00 00 02 00 00
第二币种电子现金余额上限	DF77	06	00 00 00 03 00 00
第二币种电子现金单笔交易限额	DF78	06	00 00 00 00 20 00
第二币种电子现金重置阈值	DF76	06	00 00 00 00 30 00
卡片附加处理	9F68	04	Byte1 bit 8 = 1 支持小额检查

9.2.4 非接触式小额支付扩展基本特征

表 44 定义了非接触式小额支付扩展的基本特征，表 44 中未定义的数据在表 43 中定义。

表44 非接触式小额支付扩展基本特征

数据对象	说明	数值
PDOL	密文版本01	DF 60 01 9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04
	密文版本17	DF 60 01 9F 66 04 9F 02 06 9F 37 04 5F 2A 02
分段扣费应用标识 DF61	BF0C 模板	0x02
卡片附加处理 9F68	所有的卡片特征	Byte1 bit 8 = 1 支持小额检查 Byte1 bit 7 = 0 不支持“小额和 CTTA 检查” Byte1 bit 6 = 0 不支持“小额或 CTTA 检查”

除此之外，支持非接触式小额支付扩展应用的卡片还应初始化 2 个扩展应用专用文件：一个变长文件和一个循环文件。如下：

- 变长文件，其 SFI=0x19。该文件至少可开通 7 个行业应用，即至少可 Append 7 条记录。每个记录不超过 128 字节。开通密钥：191A5F026001DF259A03019C37049F11。
- 循环文件，其 SFI=0x1E。该文件包含 10 条循环记录，每个记录不超过 128 字节。开通密钥：191A5F026001DF259A03019C37049F11。

9.3 密钥信息

9.3.1 对称密钥-3DES

表 45 定义了 DES 算法适用的对称密钥，在使用此类密钥时无需使用 PAN 和 PANSN 分散这些密钥。

表45 对称密钥-3DES

密钥名称	密钥值
应用密文密钥	11 22 33 44 00 66 77 88 11 22 33 44 55 00 77 88
安全报文认证（MAC）密钥	8B 4F 85 4F 08 31 FB F2 63 5A 21 2E 4D DD B9 2A
安全报文加密密钥	11 22 00 44 55 66 77 88 11 22 33 00 55 66 77 88

9.3.2 对称密钥-SM4

表 46 定义了 SM4 算法适用的对称密钥，在使用此类密钥时无需使用 PAN 和 PANSN 分散这些密钥。

表46 对称密钥-SM4

密钥名称	密钥值
应用密文密钥	11 22 33 44 00 66 77 88 11 22 33 44 55 00 77 88
安全报文认证 (MAC) 密钥	8B 4F 85 4F 08 31 FB F2 63 5A 21 2E 4D DD B9 2A
安全报文加密密钥	11 22 00 44 55 66 77 88 11 22 33 00 55 66 77 88

9.3.3 发卡行公私钥对及证书 RSA-1024 位

CA 公钥索引:

- 标签 = 8F;
- 长度 = 01;
- 值 = 80。

发卡行公钥证书 = (1024 位 s, 128 字节 s, 0x80):

- 标签= 90;
- 长度= 80;

——值=22 91 03 A5 E3 12 0F 2D 28 62 09 11 76 AA 2B D4 E2 4D 69 E7 EE F7 B9 19 5C 91
EA 00 88 AE CF F4 7E DF A0 BE EF 7C 39 1D F3 B0 5F 71 7D CC 06 FF C8 EE FF 90 BA 14 21 2B
8A 52 AD 48 B3 32 77 B2 E2 30 D4 0B 3E 76 DC 59 77 89 26 F1 D8 73 9E 10 6C D7 41 DE 06 A7
42 3D FB A2 5E 02 F1 2E 54 3D 13 D1 B4 71 80 65 26 02 49 81 B7 D2 6B 4B F6 E5 55 86 04 CC
C2 89 F5 9E 8A 80 2F 45 FB 3D 9E 67。

发卡行公钥余数:

- 标签= 92;
- 长度= 24;

——数值= 8B 64 3D 1E AF 2E A7 84 AC 20 53 03 C9 0E 74 5E A2 EF A5 CB F0 2C C4 7D 47
83 3B B7 B2 7E CC 69 62 38 5A 4B。

发卡行公钥指数:

- 标签= 9F32;
- 长度= 01;
- 值= 03。

发卡行公钥(1024 位 s, 128 字节 s, 0x80):

BEED0D6A8DAC95071540856B8F130385BFFFA8451F15E1676EDEDDF1ABBFDE4B96E6EBD5145F314DB606F4
4BD848CB38DC500431C6A82B0A70DCCD5BCB6E6A9149CFB8EB53F52AAD47D12A800C55D79FCEFF7485699AB
612FF334158B643D1EAF2EA784AC205303C90E745EA2EFA5CBF02CC47D47833BB7B27ECC6962385A4B。

发卡行私钥(1024 位 s, 128 字节 s, 0x80):

7F 48 B3 9C 5E 73 0E 04 B8 D5 AE 47 B4 B7 57 AE 7F FF C5 83 6A 0E 96 44 F4 94 93 F6 72
7F FE 98 7B 9E F4 7E 36 2E A2 0D E7 95 9F 83 29 03 08 77 B3 D8 AA D7 68 47 01 CB 1A 09 33
39 28 79 EF 1A 3A 8F 57 A9 DB 89 2F 4C E7 80 FD 0E 31 85 7C E7 8D E1 C5 45 D6 07 F7 29 87
55 AE 0A 66 36 91 5D F0 02 C0 5B 21 0E 9D 37 2A BD F2 1C 24 E8 CB D4 9D 0D C9 BA 32 DC C5
5B 6B 02 1A 85 9A F3 2F 1B。

认证中心签名的发卡行公钥数据:

02 62 28 00 FF 12 30 00 00 01 01 01 80 01 BE ED 0D 6A 8D AC 95 07 15 40 85 6B 8F 13 03
85 BF FF A8 45 1F 15 E1 67 6E DE DD F1 AB BF FD E4 B9 6E 6E BD 51 45 F3 14 DB 60 6F 44 BD

3C6D6E588D8B2235B0C79B14AE992118DCD568869859CD7F970B1A82597F67A4E5FB9B1BF6E1096942D3ECD
2258A0D1CDD48BBB60E799B09BB0FA9A5A1A2E9B39BD379792AA0135C9E4C9D6D642366EDB452A5A4E8D318
6F60747EB2B9C10A579B490C5985873。

发卡行公钥证书 = (1152 位 s, 144 字节 s, 0x90):

——标签= 90;

——长度= 90;

——值=

7958064ECCBBF90B89D4D9FE6FA8286654A697EAD27575D20C0D39D4AFA0C4AA2AD7B6CC7413F69B9D3
EA835701C0AA93228495F1F08703AF46BFB0191FB7F03DF4296C797B874A1F9C40EA7B0290268FB041CC83E
E2E86415C6E307B391DE90CED3BBFD7856218D274CF82B16614C9570F326680A71649F1C618C0DB351D8406
F94192F53D2DBF1A3DD1DD0EEFA116A。

发卡行公钥余数:

——标签= 92;

——长度= 24;

——数值=DA7D9ED0CB4FB9A1182967B17314701AC51969D44B85798C8ECE039CD0C11714E9CC19EB。

发卡行公钥指数:

——标签= 9F32;

——长度= 01;

——值= 03。

哈希输入数据:

02622800FF123000000101019001C035D8F6D8E3E2EBAE78AD5BE456A7C06C2051B6E8271C8AF661113
203893B42F0AB631CB5BFEB0894CDE3A1FC9BACFF6BF8D5E28CD918BAF22C73DFC31352ABC3F9F1BF5EDCF7
9A3B1727F8E958AABC098AC6B1FD5A98095715DBA46F2510249B8EEE8FF7EA33C03A6F7943DA7D9ED0CB4FB
9A1182967B17314701AC51969D44B85798C8ECE039CD0C11714E9CC19EB03。

参与脱机数据认证的静态数据为:

5A0862280001000011175F24033012315F25039507019F08020030。

认证中心签名的发卡行公钥数据:

6A02622800FF123000000101019001C035D8F6D8E3E2EBAE78AD5BE456A7C06C2051B6E8271C8AF6611
13203893B42F0AB631CB5BFEB0894CDE3A1FC9BACFF6BF8D5E28CD918BAF22C73DFC31352ABC3F9F1BF5EDC
F79A3B1727F8E958AABC098AC6B1FD5A98095715DBA46F2510249B8EEE8FF7EA33C03A6F79433542641AD3E
4BE7936B79A138346464F72C041E1BC。

9.3.5 发卡行公私钥对及证书 RSA-1280 位

暂无, 此条保留给将来使用。

9.3.6 发卡行公私钥对及证书 RSA-1408 位

CA 公钥索引:

——标签 = 8F;

——长度 = 01;

——值 = 84。

CA 公钥:

F9EA5503CFE43038596C720645A94E0154793DE73AE5A935D1FB9D0FE77286B61261E3BB1D3DFEC5474
49992E2037C01FF4EFB88DA8A82F30FEA3198D5D16754247A1626E9CFFB4CD9E31399990E43FCA77C744A93

685A260A20E6A607F3EE3FAE2ABBE99678C9F19DFD2D8EA76789239D13369D7D2D56AF3F2793068950B5BD808C462571662D4364B30A2582959DB238333BADACB442F9516B5C336C8A613FE014B7D773581AE10FDF7BDB2669012D。

发卡行公钥：

CE69697219A3AB2438210B449809119F52E12291F7D642B6C8D72828482FE4B6AB1FB7D3B4A685DF971F8EFD898E82BB8F31D9A639B7F76215CDA8FF9A6387E2375D619DB4E0440BBAEB4232BF620EA73BAAF60F4195D4571F82C2BAC6B17196CEFA5D3A3C59EDA526BE69705DB89058D72903F2A6AFF949FF8BF6D2FF44968D24D8F8DB2437C0ECAA63B57BAFC9AAD1082B549F009EAD566BE0EB610EB8897033EF2296330DD3C3B04BB7C1D7E3C481。

发卡行私钥：

899B9BA1666D1CC2D016078310060BBF8C96170BFA8ED72485E4C570301FEDCF1CBFCFE2786F03EA64BFB4A9065F01D25F7691197BCFFA4163DE70AA66ED05417A3E4113CDEAD807D1F22C21D4EC09C4D271F95F810E8D8E3786DE863D69AD7D2FFDBEBF85D2CED352245504F751FB439F7D82F8BFA759C5D66AD8D67CEE9E562109F6D24F154163A69C0FD8D5A592DA761BDDCF5E177FE3AF023AE50A5FE146F34B648CC12FA2D08217B7C27B20A12B。

发卡行公钥证书 = (1408 位, 176 字节 s, 0xB0)：

——标签= 90；

——长度= B0；

——值=

E5A476B7802A368CB511989629787CFE7DBDB57D37F94F258F97B355D14F2A9F3184C41A2F99711C23D689CD49B8C178DD64092F52BA3B54A4B0246C11FA3224D6A4A7DC68DF3DFF1CE4787331FBD5416103BF62B7F98998048AE40B13988AD07DA6DC55E42F897326AFF443EAB4710F7139DA3656F479CB550C6E2B8DFC9D809E0B419BD8D22CFA5463570D133C1FAFAFA728107AC335B27B2CA076C5FA13C24F494D04EABD56FCFF42162E5117A8F0。

发卡行公钥余数：

——标签= 92；

——长度= 24；

——数值=AFC9AAD1082B549F009EAD566BE0EB610EB8897033EF2296330DD3C3B04BB7C1D7E3C481。

发卡行公钥指数：

——标签= 9F32；

——长度= 01；

——值= 03。

认证中心签名的发卡行公钥数据：

6A02622800FF12300000010101b001CE69697219A3AB2438210B449809119F52E12291F7D642B6C8D72828482FE4B6AB1FB7D3B4A685DF971F8EFD898E82BB8F31D9A639B7F76215CDA8FF9A6387E2375D619DB4E0440BBAEB4232BF620EA73BAAF60F4195D4571F82C2BAC6B17196CEFA5D3A3C59EDA526BE69705DB89058D72903F2A6AFF949FF8BF6D2FF44968D24D8F8DB2437C0ECAA63B57B8E9CABAF2F917B4D130A51E7A1BEE14B41B55104BC。

哈希输入数据：

02622800FF12300000010101b001CE69697219A3AB2438210B449809119F52E12291F7D642B6C8D72828482FE4B6AB1FB7D3B4A685DF971F8EFD898E82BB8F31D9A639B7F76215CDA8FF9A6387E2375D619DB4E0440BBAEB4232BF620EA73BAAF60F4195D4571F82C2BAC6B17196CEFA5D3A3C59EDA526BE69705DB89058D72903F2A6AFF949FF8BF6D2FF44968D24D8F8DB2437C0ECAA63B57BAFC9AAD1082B549F009EAD566BE0EB610EB8

897033EF2296330DD3C3B04BB7C1D7E3C48103。

发卡行认证哈希结果：

8E9CABAF2F917B4D130A51E7A1BEE14B41B55104。

数据验证代码：

DA C1。

参与签名的记录数据为：

5A0862280001000011175F24033012315F25039507019F08020030。

发卡行公私钥对及证书 RSA-1984 位：

CA 公钥索引：

——标签 = 8F；

——长度 = 01；

——值 = 85。

CA 公钥：

C9242EC6030F10E5225E722AA17D9DC894299233AEC3219B950D4F243AF530FA13E3A31AFAA0D4BF4DE
562B6B4C3108AEBBC6CB080F90770D532F241BC1536401E1BF72F9DC1B08933B9BF77403F6A0FB5777BAA4C
9BE91574BBFB521342A20386790512221F477FBC53FF1B6533A015815435410EC272F0A34EA0735C439677
D7E46FBA766EC00CED59B6715E3412D6FB8A934BF9D1497A24A6252C52D7586FD66A450FB5D2B4484EC9230
61439622BC0535316CD4231C13C627BF4D2EDE1C02C802464658F1B9D7FF23A3698510FA90D0C3164942FB3
59255CD823CB2635B3F167FBDFC900641B970D602A2771A7F4F94DF6D34BE8BBB。

发卡行公钥证书 = (1984 位 s, 248 字节 s, 0x7C0)：

——标签= 90；

——长度= F8；

——值=

2780A14C013F969B8E2F54FFBA93E55D881B43951BC6740A6B96D352736ABB1B943F70EF02A8256F0EB
0605B1902861C64BEBED009BFB3D1F186D2915EA63D5D48B002EA0318835AF5FB0D6F9F0262F183F9EE6D8F
97FF465A8D87207FEF044F3A7BFFE2BFBF2E96FAB3DB26A449952FFFE6C17845E14A3B40F72F5DE22281DF
572D0215B77217AFA7D2107EDDCDB428BCA66BB949BE67B78734D5482260370C7E215BA77D1DB6E16CDB705
37C3C749E0C2E7FCE3166483526C5A3629AB3DC372EF5E211090F62CCD0089B1A0B0603A12FE25E426A8F66
9014447F8A6837EDF887713FD00053F46BE29A8E2996B6ED1A52EA373ECB51D86。

发卡行公钥余数：

——标签= 92；

——长度= 24；

——数值=B1F73EAC3DAAFF10F54AFE269D55BCCA7AC1AB3E69776204043062520578309C2E98184D。

发卡行公钥指数：

——标签= 9F32；

——长度= 01；

——值= 03。

发卡行公钥：

BE41AACA0C6A8B8938FE69E1564640985B0CCA43B034CE1D62C8E3E777912047F1523AA797612175207
CDA361152EC984BDFB3C3B57476014D84F3949A151CCC71B20F8682B68331D55AA702082B5815BF9EFC278
B95A970C1486DDE544B197E4329A9894376684B708185DBE91D343AC6D35CFD4BDB46A0984020011085272F
2F4286294A130723600253270FF4A59BADBB0956ED5D28AF817F1E7D103253EEF2548F36689A7A25A60D2BD
E2CAF5C9F1B3F583FD15344750A97E08713A31E54EFEE41B025F9C5AD64A313793C66C00D7867FEAB1F73EA

C3DAAFF10F54AFE269D55BCCA7AC1AB3E69776204043062520578309C2E98184D。

发卡行私钥:

7ED671DC084707B0D0A99BEB8ED98065920886D7CACDDEBE41DB429A4FB615854B8C271A64EB6BA36AF
DE6CEB637486587EA7CD2D23A2F95633ADF7B866B8BDDDA1215FAF01CF022138E71A015AC7900E7FBBF52C50
7B91BA080DAF3E98D8766542CC671062CF99ADCF5ABAE929B68CD7C848CE8A8DD3CD9C0658015439986990A
2421D4443678B12BABAE019B2779D6C535BA1DC856914576EE91BCEB4A71EE302D919C252B3BC3F4EC7722E
E15408945D293A5890E79B3F084FCFA71C6FCB9BCEB31D32E695193AC7B9BD0EE03A8FBEB8236C7DF505E3B
0D64C9A1C23B4BBEFD6EA9432BA6A0A0C2EA5C4541F71980E511FB2A513C89313。

认证中心签名的发卡行公钥数据:

6A02622800FF12300000010101f801BE41AACA0C6A8B8938FE69E1564640985B0CCA43B034CE1D62C8E
3E777912047F1523AA797612175207CDA361152EC984BDFBB3C3B57476014D84F3949A151CCC71B20F8682B
68331D55AA702082B5815BF9EFC278B95A970C1486DDE544B197E4329A9894376684B708185DBE91D343AC6
D35CFD4BDB46A0984020011085272F2F4286294A130723600253270FF4A59BADBB0956ED5D28AF817F1E7D1
03253EEF2548F36689A7A25A60D2BDE2CAF5C9F1B3F583FD15344750A97E08713A31E54EFEE41B025F9C5AD
64A313793C66C00D7867FEAA85A35A8179423F1B3B6EFC1DA1B944C34FB92F6BC。

哈希输入数据:

02622800FF12300000010101f801BE41AACA0C6A8B8938FE69E1564640985B0CCA43B034CE1D62C8E3E
777912047F1523AA797612175207CDA361152EC984BDFBB3C3B57476014D84F3949A151CCC71B20F8682B68
331D55AA702082B5815BF9EFC278B95A970C1486DDE544B197E4329A9894376684B708185DBE91D343AC6D3
5CFD4BDB46A0984020011085272F2F4286294A130723600253270FF4A59BADBB0956ED5D28AF817F1E7D103
253EEF2548F36689A7A25A60D2BDE2CAF5C9F1B3F583FD15344750A97E08713A31E54EFEE41B025F9C5AD64
A313793C66C00D7867FEAB1F73EAC3DAAFF10F54AFE269D55BCCA7AC1AB3E69776204043062520578309C2E
98184D03。

发卡行认证哈希结果:

A85A35A8179423F1B3B6EFC1DA1B944C34FB92F6。

数据验证代码:

DA C1。

参与签名的记录数据为:

5A0862280001000011175F24033012315F25039507019F08020030。

9.3.7 发卡行公私钥对及证书-SM2-推荐曲线-索引 57

CA 公钥索引:

——标签= 8F;

——长度= 01;

——值= 57。

CA 公钥:

E8105E77861FD2EB727C84E36D3D4A5666BD0ADCE8781F0145D3D82D72B92748E22D5404C6C41F3EC8B
790DE2F61CF29FAECB168C79F5C8666762D53CC26A460。

发卡行公钥:

9F483BF2CC71C5093728318061E3F768EA7C170F82DD8C4B979FBD8C76A129F93FB5746E96F5E49B987
FFB521E473B25E1B017C30BE3FC638BA14D5FA4AADC16。

发卡行私钥:

1F34E60E7FAC21CC2B26DD34462B64A6FAE2495ED1DD383B8138BEA100FF9B7A。

参与脱机数据认证的静态数据:

5A0862280001000011175F24033012315F25039507019F08020030。

9F4A 数据 : 82。

证书格式 : 12。

发卡行标识 : 62280001。

证书失效日期 : 1220。

证书序列号 : 000001。

发卡行公钥签名算法标识 : 04。

发卡行公钥加密算法标识 : 00。

发卡行公钥参数标识 : 11。

发卡行公钥长度 : 40。

CA 哈希值:

73DF81BF5CC82AABB7CF3C9165EDEEA2EC0CCC56AB19F1661E012CD33D4BFBEC55A88990EB25B4A4058
C8E4B11C1F9EA2055E403CA76AC8A991DE80A35BED348。

发卡行公钥证书 Tag_90 :

12622800011220000001040011409F483BF2CC71C5093728318061E3F768EA7C170F82DD8C4B979FBD8
C76A129F93FB5746E96F5E49B987FFB521E473B25E1B017C30BE3FC638BA14D5FA4AADC1673DF81BF5CC82A
ABB7CF3C9165EDEEA2EC0CCC56AB19F1661E012CD33D4BFBEC55A88990EB25B4A4058C8E4B11C1F9EA2055E
403CA76AC8A991DE80A35BED348。

签名的静态应用数据:

签名数据格式: 13。

数据验证代码: DAC1。

9.3.8 发卡行公私钥对及证书-SM2-推荐曲线-索引 58

CA 公钥索引:

——标签= 8F;

——长度= 01;

——值= 58。

CA 公钥:

FFC2B1513320C275411DBADD2188203F7B62519F8C7BA98EF8AA9FD6D2E475984E383C3E12784B42B06
6960EEA0C8FC8099E14128055D67A666CCA5A058C26A4。

发卡行私钥:

AAF8CE02045DD01619D689EE731C551159BE7EB2D51A372FF56B556E5CB2FDE3。

发卡行公钥:

173A31DD681C6F8FE3BA6C354AD3924A4ADFD15EB0581BC1B37A1EB1C88DA29B47155F62FCF4CCCD201
B134351A049D77E81F6A6C66E9CB32664F41348DA11F6。

参与脱机数据认证的静态数据 :

5A0862280001000011175F24033012315F25039507019F08020030。

9F4A 数据: 82。

证书格式: 12。

发卡行标识: 62280001。

证书失效日期: 1220。

证书序列号: 000002。

发卡行公钥签名算法标识: 04。

发卡行公钥加密算法标识: 00。

发卡行公钥参数标识: 11。

发卡行公钥长度: 40。

CA 哈希值:

3499A2A0A7FED8F74F119B416FF728BA98EF0A32A36BCCB8D0110623D466425CA44C68F8E49121D9BFA
9484CAEF9B476C5EB576D1A8DD6BC4A0986AF4134ABAF。

Tag_90:

1262280001122000000204001140173A31DD681C6F8FE3BA6C354AD3924A4ADFD15EB0581BC1B37A1EB
1C88DA29B47155F62FCF4CCCD201B134351A049D77E81F6A6C66E9CB32664F41348DA11F63499A2A0A7FED8
F74F119B416FF728BA98EF0A32A36BCCB8D0110623D466425CA44C68F8E49121D9BFA9484CAEF9B476C5EB5
76D1A8DD6BC4A0986AF4134ABAF。

签名数据格式: 13。

数据验证代码: DAC1。

9.3.9 IC 卡公私钥对-768 位

E=01 00 01。

N=C5BD39EFF93AC495A771653D66341F660E8DF31237C0A28729661C45C9F4384CF26F687B69FB717C7
595B4D26B533459BC1FC4367623654C29BAEF473FD085C191EC9626E579E233322944AC7C31E850928FD8B
098289DD917D3A288B7BDD55。

D=1E FD 63 FA 1F 06 3D CE F2 7A 0C 12 CE 54 B6 E3 08 BE E8 6C 5F 7E 7A 3A 52 9B A5 2C
AE D4 EE 89 E8 A8 DB 28 14 59 0A D5 25 9C 7B C5 4A 7A B4 C6 60 82 4E 43 72 EF 22 AE 81 3F
2E 0F 0F 5B 4F E5 D1 CC 52 30 7F 7D D9 7D F6 88 59 19 F5 FA C9 3D 91 D6 52 2F DC A6 4B 3A
49 1B BF DD 26 62 C2 55。

P=FC 03 51 2F ED 42 39 4B 44 26 11 AA C0 61 B6 65 23 EC 90 FB 67 45 D3 12 97 CA 31 0E
1F 68 33 FF FF CC 5E D3 4B F8 AC 3B 52 C7 AA 75 4F CF 29 8B。

Q=C8 DE 18 01 D8 0C DF CB 0F C2 FE 4E 6C 7B 1D CB 99 C9 FB ED 69 F4 B9 EA 3E EA D4 16
6B DE 9C A5 82 E5 87 A8 70 D7 82 3E F6 4D 73 C3 20 F5 30 9F。

$d \bmod (p-1)=24$ E2 77 67 84 5A 44 F8 77 28 FB 3C FA 9B 52 8E CB 0B 3C CD 0E F8 71 44 2F
63 30 7A D8 AD EF AE 70 4A 01 36 FB CF 91 A5 BD 1F EC 1A EF 6B 6A B1。

$d \bmod (q-1)=BB$ 1B 1E 73 C1 43 A4 C7 2B 44 70 CC AE 82 34 6B EE 32 56 E8 7C F5 48 A4 E9
BC A6 98 C8 1C 52 00 5E A0 DE 2F CA 05 05 3F 0F 01 70 9E C7 B9 7D 73。

$1/p \bmod q=44$ 26 93 8C 18 98 D9 32 86 8B AB 3A F8 E9 7C 36 9A AF 24 1A 12 35 FE A9 69
76 1C 89 06 A5 2B B0 17 AC 3D F6 CD 9C 95 F1 EB FD 8F A4 D9 E1 0B 7C。

$1/q \bmod p=A6$ 82 73 0F 92 13 80 57 49 E4 74 FB 08 D6 C0 08 88 59 2B 18 8C 7B D6 D1 5C
C8 64 38 54 75 4E D4 C8 C3 23 00 D1 63 1F F5 99 F7 44 C0 7C 90 F1 BE。

9.3.10 IC 卡公私钥对-1024 位

E=01 00 01。

N=9D D7 30 66 9F 27 89 29 44 A6 8C 0C 62 34 4C 0E 8E C5 7C 2A A7 80 04 B0 14 C2 6A 0B
0F 3B 51 7A 0B 60 D3 55 DF BC 89 29 BB C5 9C EB CD 0C CA 13 CD AA 0C 94 E9 1C 84 A2 6E 7D
BE 6B 58 59 5C 4E FF 2D 71 7C B9 EB 96 5C 15 D2 87 AF 60 AC 28 D0 6B C5 12 82 BC 4A 51 8B
0E A3 AB A9 34 3F 17 7854 5F FB 49 EE 84 0B BC EA 45 7D BA AB BF D7 55 BA 0F 94 3A 08 A5

9C FF B6 06 6B 40 84 76 75 99。

D=0B CB 45 89 95 80 DD C5 E0 A4 55 38 A3 A9 E6 B8 FB C0 13 EC 18 01 FF D7 AC 65 6E 89
0F 05 4E AC 40 E7 66 43 37 69 9E 12 29 3E B5 E0 04 BD 5C E8 27 E8 F9 F1 B2 8D 77 F7 AF 2B
E4 2B 9F 39 66 25 3E EA 28 62 E0 54 7B A7 8D C0 DC 9C 5C 87 5E 82 02 03 82 B9 31 49 90 7A
52 4B 5E 42 07 86 F6 63 77 B5 0B BD 17 D5 AD 8B 56 BB 1D 97 2D FE 45 5F E1 68 75 AC 90 36
FD F3 BB FC 14 4C B5 E2 52 01。

P=D0 BA D2 86 ED 4E 1C BE 6C ED 53 91 A9 69 6E D5 8F 31 7E 4A 52 D0 E3 7C 75 5C 01 22
5F 67 6A B7 12 A1 5D 1B 95 3B D6 7F B8 DF B6 10 65 59 65 35 25 83 B4 6B 26 0E 48 16 61 DF
74 FE 85 C2 0A C1。

Q=C1 96 0C 87 E0 33 3F CB B1 C2 BB EB 78 70 19 D6 08 0B 33 C8 F5 03 9C 2B D5 5C C1 D2
47 39 8A A5 DB D4 7F A4 E1 FF 85 F4 25 D2 14 B4 B3 2A 34 1E 72 C1 F9 FF 67 65 D1 15 59 63
BE C0 2E 89 58 D9。

$d \bmod p-1=3D\ 25\ AD\ CD\ 07\ 31\ ED\ EB\ BF\ 3F\ 5B\ 4E\ FD\ C1\ 3C\ 4D\ E5\ D0\ 0A\ FE\ 3C\ FA\ A2\ D9\ F0$
 $0B\ 8E\ ED\ 81\ E3\ 6A\ F8\ CC\ C5\ 66\ E0\ 50\ BC\ A1\ DE\ F2\ CA\ DE\ AC\ 38\ F4\ 92\ 58\ 9A\ 6F\ D5\ E7\ D9\ D3\ 2F$
 $3D\ 17\ 58\ FE\ 0E\ 1E\ 23\ 35\ 41。$

$d \bmod q-1=5A\ 24\ 79\ BF\ 47\ 99\ F5\ A9\ EF\ 23\ 63\ 87\ F9\ 34\ 12\ 03\ C5\ 09\ 1A\ 5B\ 08\ 24\ 5F\ 33\ 56$
 $0D\ F4\ 3E\ EB\ 65\ 92\ F7\ 3A\ 8F\ 0F\ C5\ 02\ 6B\ 8E\ BF\ AA\ 60\ D1\ BD\ 76\ F4\ 3F\ 02\ B2\ A3\ 3A\ BB\ 40\ 35\ 7C$
 $0F\ B9\ E9\ 25\ 68\ AE\ 02\ CC\ B9。$

$1/q \bmod p=0E\ B4\ 1A\ 42\ 80\ 1F\ 08\ D5\ C1\ 6E\ E5\ 93\ 80\ 0E\ 16\ C4\ 28\ 9A\ 63\ 9D\ 1D\ 16\ FC\ D3\ 66$
 $FE\ 4D\ 80\ A4\ 15\ 4B\ 15\ FB\ 25\ AC\ 5C\ 24\ D7\ 60\ 78\ 48\ B5\ 5F\ 02\ 22\ 30\ FE\ 4F\ AD\ 49\ 13\ AD\ 52\ 6C\ B9$
 $28\ A7\ 62\ F1\ 83\ 62\ 5D\ 77\ 5B。$

9.3.11 IC卡公私钥对-1152位

E=03。

N=C345B4CD6FFC58E5C7ACFD6D0EA4EA9CEB288F30E5CAE9499D38A6FD0E378194A45A79E25E6DDE3
DE5AA42584D450B350892B689F05E5B1A54B401CC9E486B43F6290A7C3863F3790EC4BBB34E078D7D98E247
E89EFAB315C8F0A6E9B2A4802473C24800F16CF499D63F940099FA6B759F06226DE4A07C2E47A387D3A72A2
FEB78028C04E5E903AC0BE73A7AF73FE5。

D=822E7888F552E5EE851DFA8F35F189C689CC5B4CB43DC9B8668D06F535ECFABB86D91A696E99E942
943C6D6E588D8B2235B0C79B14AE992118DCD568869859CD7F970B1A82597F67A4E5FB9B1BF6E1096942D3E
CD2258A0D1CDD48BBB60E799B09BB0FA9A5A1A2E9B39BD379792AA0135C9E4C9D6D642366EDB452A5A4E8D3
186F60747EB2B9C10A579B490C5985873。

P=F824ECAF6B399C804E97C3F0577360F4DB2B35FD686AF75DA8F7356E446797322845249C02223984
7497AF19CFCODE4CE7D15B9FCA96566383EEF7CF39019797C5340FA7BFA9027。

Q=C974487571EB48AC96D1222AAF743FB28D617E757A1A99A3C0FAC5793523CC3B8E7B5176DD1BD7D15
DA6B4020EA72F45B981A60E4F87F0FF68C808233094657137821766D6982B13。

$d \bmod (p-1)=$

A56DF31FCF2D1130034652D4AE4F795F8921CCEA8F0474F93C5FA239ED8450F76C5836DBD56C17BADA3
0FCA11352B3EDDEF0E7BFDC643997AD49FA8A26010FBA83780A6FD51B56F。

$d \bmod q-1=$

864D85A3A14785C8648B6C1C74F82A7708EBA9A3A6BC666D2B51D8FB78C28827B452364F3E128FE0E91
9CD56B46F74D926566EB435054B54F0855AC22062EE4B7A56BA448F101CB7。

$1/q \bmod p=$

55FC824EF4466D5C0FAE99FE250633410E762A8402F6CF6F0C71CACCC9D16A9652E2CC74F546445C6B9
 FDF33F5D699799F8CD7908CBC03E9DE6A350B75A2165FD73782B8B0309009。

9.3.12 IC卡公私钥对-1280位

E=01 00 01。

N=D0 1B E7 8B 92 64 3C 6C 35 20 AA 59 FD 28 08 48 69 F8 05 E7 FC 94 F4 28 98 69 9C A8
 97 0E 50 92 3C 90 96 25 F4 5B 40 47 2B 42 95 D6 DA 94 23 DB 16 1B F5 CE AB 58 06 C0 2F 7E
 C0 25 B5 12 AA 32 1F 6D 68 71 5A 5F EE E6 92 3F 95 14 34 82 1D 9B 92 31 31 0C 47 31 94 69
 F0 D8 01 46 3A 00 EA 8B 22 22 5E 3D 33 3A B1 71 86 59 F8 9D E4 29 3F 58 D5 CB 54 1F E1 40
 CF D3 E5 9E 11 E3 8C 4B DC A2 83 2F 61 99 51 CA D7 77 23 6D 7C B7 75 76 C8 E4 C5 F9 02 F9
 0F 38 49 94 3D 4C 7D 0F 04 94 79 B9。

D=01 BC 64 84 B8 31 38 85 23 E1 A4 8A 20 F5 21 DC 8E 1B 10 DC 36 87 27 8C E4 78 92 63
 4A F4 9B 9C C7 54 8D 6C 13 A0 64 90 DE 13 82 C7 20 06 4C 50 EF 86 46 D9 4A 79 EE D4 7B 90
 F0 6E B5 6B F5 1A 25 EE 4B B3 66 5A EB D5 E5 DD 11 E9 46 91 84 9D B1 10 9C A3 9D 68 24 21
 8F 08 D7 FD 99 7E 5E E2 82 D3 75 29 F8 B0 D5 0D 00 3D A6 DE 27 14 5E 12 AD 7F 33 B3 77 5C
 BB 1C 05 A0 E3 5F E2 3E C0 F5 B5 52 3C F8 FB 54 92 B9 E7 4B 8F F9 CB F8 E7 DF D2 3A D6 97
 BD 78 5B 7F 54 96 74 CC 6B C8 96 61。

P=D6 27 02 8E 7F 01 5F 22 22 56 AB 78 7E E1 F3 28 2F 37 2C 1F EA 6B 7D E7 49 B4 BA 6F
 B1 12 56 D5 92 4F F3 45 EE F2 17 A4 D0 FB D5 0C 99 72 3D C5 B6 88 66 6E C4 0F AB 01 CA CC
 9D 70 15 23 13 A1 4E 12 6A A0 70 CB 46 90 DF 0A B9 33 99 D6 44 CF。

Q=F8 C6 92 E9 77 C1 98 63 0B D1 B6 B0 50 5D 3A 68 64 42 9D 76 F3 D4 01 5A CD 82 B1 C8
 C2 C4 92 CB 45 19 69 97 93 4E CF 8E E4 21 24 C0 56 24 4B 9A 2B 95 AC 3B E5 0A C1 C6 D1 B2
 B2 4F 84 86 5B 02 CB 92 8A A6 A3 60 12 25 0B A0 05 F1 9F 58 0A F7。

$d \bmod (p-1)=$

82 1F 0F E9 9F 78 28 E2 E7 B4 7B D9 EA 56 C6 55 7B 62 ED B7 B2 CB 7F A3 E2 60 23 0C 2C
 AE 74 FE AE 39 50 1B 05 16 2A 91 A5 BD EE F5 09 E3 A5 6F 15 FB 09 2A 72 8D 06 9E 3F 28 56
 DD 3C AA A4 89 D5 93 51 20 8D 88 A6 26 EE AF 68 5A D7 35 9F 77。

$d \bmod (q-1)=$

94 E3 8B 93 8D 27 E1 83 0D D4 D2 68 CD 80 2E 6F C1 E9 98 82 53 C5 C3 95 CB BF 77 95 B6
 F3 9D 03 68 F4 9F 9C A6 FE 18 FC E5 0D ED 07 EB C6 47 35 1A F6 B6 21 16 A0 8C 7E E8 8B F1
 69 E3 DF E1 62 57 E1 F9 77 67 FA 1C 81 ED 66 35 88 79 9C 60 DB。

$1/p \bmod q=$

77 55 9B F3 47 48 68 88 2A 20 EF 90 7F E7 1E 7B 99 65 87 1B 66 B4 70 EF 28 0F 1F E0 EF
 01 0C E7 39 F6 C0 5B 66 D3 2A 5E 1E 30 FD F1 9E DA 68 B5 4B 86 62 DD 20 18 70 5D 15 B6 DA
 2B 42 D6 43 6D F7 39 95 B1 78 30 8C AF 5F 3C 8A 52 2F 16 FC 85。

$1/q \bmod p=$

6F 6D 22 AD 15 66 B9 57 2D 08 B5 78 95 44 A6 73 3A C1 A6 03 74 50 C8 58 4D BA 3E 8A 64
 AD F2 FE 56 2B BE 84 90 31 03 AD A5 F6 CD F8 A4 73 00 34 C7 A4 04 CD B1 B6 F1 B1 E8 3B 95
 14 B9 59 7A 21 A7 FB 9A 9B 2E 83 89 52 16 92 DB 23 DE BB A8 89。

9.3.13 IC卡公私钥对-1408位

E=03。

N=B231678044B98D5CF9DF30B9541E94C2BECD7352FC9D96F86D197518333E2D1D1AA584E12A1DEC60F

11B3CD2AEB3630184FFFD3998E5C149862C5063149404E5C4FDB9FF30416B846BEF1F656BB40CF9092888AB904A2C7659A3F14CFC3F930532D869D014E669C533B763A88114156DC2061A5316780B173BD04BE8471E975EE318CA9D327BF28AEE954ECDC5B4C0FAD9EFCB659FE3C01E431F3440B3E0167DD5DCDE431E1378745DAE9D4C50432D7D。

D=76CB9A5583265E3DFBEA207B8D69B881D488F78CA8690F5048BBA365777EC8BE11C3ADEB71694840A0BCD3371F2242010355537BBB43D631041D8AECB862ADEE8353D154CAD647AD9D4A14EE47CD5DFB5B705B1D0ADC1DA31ECF91F87CAD95B0D5272581329781A0EECD9C1981354F71ACF7E1D8A4B338CEF08EB808835E9C5F71E32E1932024DB204A87A2E134650170848934899F163045B3FCC588E2C561F3260FF6033B33AEFA641B0AA9A52A693。

P=DD289AD283534834B4BEC487401CE9E755ACBA1C4B6816C36BC38E3E59C5BED25167C20CF8F877D3EBDB1208F48A9309E1E438813AC31CDF170B81508E38360788F69AF6E673668ACD3C9F279A539FFF88EDB9E3E298B48B。

Q=CE43FB85BDE7EA473E5EED0708E63D6C77D63F65F3DC077FD2CEB94FC5A5770E819275CE891834FBCA86F36E72EDEAF605B45F076E082BF936776D282AC175903148E6C4F82A2EC43D0EC00B3633000D5B5E5A68862E7F17。

$d \bmod (p-1) =$

9370673702378578787F2DAF8013469A391DD1683245648247D7B429912E7F36E0EFD6B350A5A537F3D3615B4DB1B75BEBED7B00D1D76894BA07AB8B097ACEAFB0A4674F444CEF07337DBF6FBC37BFFFB09E7BED41BB2307。

$d \bmod (q-1) =$

8982A7AE7E9A9C2F7EE9F35A05EED39DA5397F994D3D5A5537347B8A83C3A4B45661A3DF061023528704A249A1F3F1F95922EA04F40572A6244F9E1AC72BA3B5763099D8A5717482D35F2AB224220008E7943C45AEC9AA0F。

$1/q \bmod p =$

CAACCAB9F685356F8E0F3A72733BE0ED370D0F4B276F19EB009D7317A010E69AA26988ECE98306FEBDE63A29F92B9F151AE46C979D096807484A5FFA126D7C0B1E0FC0FBC2783BCAC9140C0A138036DD205262A05995FACA。

9.3.14 IC卡公私钥对-1976 位

此种长度的密钥，卡片可选支持，如不支持应按照不支持 DDA，支持 SDA 处理，AIP 设为‘50 00’，SDA 需要的数据与卡片特征 33 中相同。

E=03。

N=C069B5366269430B73FD1876A2CA3B87B63DED06BC35495834893070E6281237E061AB46902A6D8CC6605A6C42D2A325486DD3A5AB20C061A6512B7E91BB123ECC7E05FECD181F4D819FC2D49CD57D266DA3A511F625DA39BCEF0FC18583281708FF01D11146DAF6DA23355EA981F85F6576FE18E3F02BE68BD759EC4777421991AB5D512985FA3D05A77B45B76C59531977FC67394DB78B25E9F8D592720B726CB4FE3E8B5E8F74558ADE0C32AF8E382AF9A2FEB3D45250CF3D36B0E76C37029B216D06F5E3B64C1DCAF2860956C2D44F0A4A02541D71685611F99899F33EE187CBE9A003733D8D9EB43EEDF1CE0837A8F12A0E0DB19。

D=804678CEEC462CB24D5365A46C86D25A797E9E047D78DB902306204B441AB6CFEAEBC784601C4908884403C482C8C6CC3859E8D191CC08041198B72546127617F32FEAEA9DE1014DE566A81E31338FE199E6D18B6A4193C267DF4B52BAE57700F5B54ABE0B62F3CA4916CCE3F1BABFAEA43A4A965ED4AC7EF07E4E575986054B2005068D08424536C6657C94859842804CD533A22260404401A5B26BF70788AE48AB79FB980E759C23854E84B0BFF731A2D17D4A4AB5E0EF9ED2F8970D2F627C1DED92345D933935655612F76064D94356F6B979AD4BE

23FFF992C90A58921836390B50465ABD5F4D87CC415859A17989A580465FF5EC3。

$P=0DEF93298FEE3B0CE64863BA0621203309DEA4C84214CD9A1A26C0C277A974A67FA866735A40A5E1F95BFD17972CF11B088D20A339B79C721FB02F239C2E5C8A2E104EBEE9E138180DF6B9AF508A595694B68262319E997BF6D7915A71D34B32661C255A44D5322F56E45B5C3ECC12DBB43022A8BD2AB04E56F7E5DB。$

$Q=0DCE9B42A0FAD81F1B3DD13DCB85A209CBB46D9992A98A18391943B89B06716D6BBE356057792436F128A320F5E31F9D112CEA62DF56D8EC20CAFD5021705AD45A6A60F0CC1B95A373EC47B6441F823C20997BC416A3E51272C9BEA944B2B02A5A752C27642DF17FBC835A16AAC91D421A66931461685ABDB0E9E71B。$

$d \bmod (q-1)=$

094A621BB5497CB34430427C041615775BE9C3302C0DDE66BC19D5D6FA70F86EFFF599A23C2B194150E7FE0FBA1DF61205B36B177BCFBDA16A7574C2681EE85C1EB589D49BEB7ABAB3F9D11F8B06E639B879AC417669BBA7F9E50B91A1378776EEBD6E3C2DE376CA39ED923D7F32B73D22CAC1C5D371CADEE4A543E7。

$d \bmod (q-1)=$

09346781C0A73ABF677E8B7E87AE6C0687CD9E6661C65C102610D7D06759A0F39D2978EAE4FB6D79F61B176B4E976A68B61DF1973F8F3B4815DCA8E0164AE7383C46EB4B32BD0E6CF7F2DA7982BFAC2815BBA7D80F17EE0C4C867F1B8321CAC6E6F8C81A42C94BAA7DACE6B9C730BE2C1199B762EB9AE729209BEF67。

$1/q \bmod p=$

04D6F6AF71A11ACD2E14C2BA7620A614295638A3DA278E38875249F222E16ED2CABD32F40FDB7BCC88B6C53CBA362021BF877CB4AAB81E45BF800FB109ED01F13A1337F70F626E01F995390BF11D57924EF55FDBF40B3DCBAABB9ECBC843F90F890C45922C9F8876C93ACF37F5EAEA6BFF1FE14CF4D07D0BCCEC6BA1。

9.3.15 IC卡公私钥对-1984位

$E=03。$

$N=97CF8BAD30CAE0F9A89285454DDDE967AAFBCD4BC0B78F29ECB1005286F15F6D7532A9C476607C73FF7424316DFC741894AA52EDBAF909719C7B53448343B45CF2F00A8ABFB78CEE8E848933AAED97DBE84F0730F34FB1AA1528D3D6EC75B73252A30D0C717518BE36458ADD0FBFB854C65497F3F54084154B60F51561361EE8E85F742A54005524CB00FEB334276E0E63DAD86C079A9A3DF5DD32BECAD1AB2B71F5F0A0E95A4000D01F1044A578AAD92E9FDE92E3C6AA3DCD4913DFA5552537E7DE75E241FAED455D76CB8FCAFEED3FD6DAB24D7A9C32852F866C751D7710F494A0DF11B67FAECDD87A9A4E2CC44F6F27E46E3C0CCCD0F。$

$D=194D41F232CC7AD446C3163637A4FC3BF1D4A2374AC94286FCC82AB86BD2E53CE8DDC6F613BABF68AA935B5D9254BE0418C70DD249D42C3D9A148DE0C08B48BA287D57171FF3ECD2751616DDF1D243F9FC0D2BDD7DE29D9C58DC234E7CBE49330DC5D78212E8D975090B9724D7F540E210E1953538AC0AE373AD3838C182F8DACD16829DD30E9698B309007E068BC76C44A7CE2113D6C7CEC6AC1B6FD27E53BF0082EB33AEBE02DC15B7942018420E0584224EBC6C49BDC0A9EF42210E363751AAC6F01165A57ED7DA3F9DFC1BEABBE6CBEE4F7253C7D3137996368D10E99D1FC187F6270856194E53E38E0CAD1439B9EA2CBEA4EE9077B3。$

$P=C27D0FDC2204F4BF077CE1AD370EE401D1848B2D164FC46B3F3AB9B23506FDABFF38EFC558C39EBD893B9024A0194DCA34214ECA18B26B8D4336B9A8B55C0F21C9DDF5DA0C120F64F0E46A505C74D261F2FD5B666F9E8DC44AF10BDC0269AE8B9482949B7E906B901247F7EA55D23A1F4425CD33E4A8891DC027D649。$

$Q=C7D30991956B3E334630E90B46CB04CD3B5C3657B19C3F3A515731B318CD9073DCAF34735B4A3D166CE602B2EA9B2A7984A9E7C26169B9F1614B3E772BDCF555DB32108F71C23790D15A4B74DBE4E66E62322C04C63940B29609C4D7770970ED57DB2DB54189DD76D71B6B2C90601B39902D1D6790C945E869422897。$

$d \bmod (p-1)=$

81A8B53D6C034DD4AFA896737A09ED568BADB21E0EDFD8477F7C7BCC2359FE72AA25F52E3B2D147E5B7D0AC3156633DC22C0DF3165CC47B382247BC5CE3D5F6BDBE94E915D615F98A09846E03DA336EBF75392444A

69B3D831F607E8019BC9B26301B867A9B59D0AB6DAA546E3E17C14D8193377EDC5B0BE801A8EDB。

$d \bmod (q-1) =$

85375BB6639CD4222ECB460784875888D23D798FCBBD7F7C363A212210890AF7E874CDA23CDC28B99DE
EAC7747121C51031BEFD6EB9BD14B963229A4C7E8A38E9221605FA12C250B363C324DE7EDEEF44176C8032E
D0D5CC6406833A4F5BA09E3A921E78D65BE8F9E4BCF21DB595677BB57368EFB5DB83F0462C1B0F。

$1/q \bmod p =$

474B5A7EFC099D5B9E6D80AFDD7C04814A6A804414338B966AF7D0C4B92049552085A96B74CC61D06E7
7618540C240A7E5593AFBD00148F6939D1CA5451511D31CB09128247E3D3ECA9E49871CFB6C6614B070C7AD
EE4AFFD2E62A3746D71132B6B6FE1CCC32BFAF836D87A01743E6BCB4E2C9F1FE67696EB226BB0E。

9.3.16 IC 卡公私钥对及证书-SM2-推荐曲线-索引 57

IC 卡私钥:

4EFF3E9B796688F38E006DEB21E101C01028903A06023AC5AAB8635F8E307A53。

IC 卡公钥:

C3AC12B81B9D175936B5BF72BB8FE3A2266BC013B2E94F5837F16AA1C01AA7323B75626AB64D02AED20
CC6F440841F10EE6873BCBEA3F41D6869D0FEADD71154。

9.3.17 IC 卡公私钥对及证书-SM2-推荐曲线-索引 58

IC 卡私钥:

E23073A44CA215D6C26CA68847B388E39520E0026E62294B557D6470440CA0AE。

IC 卡公钥:

3AFD58A8749CBDB6F59956BE0286CAFF3123976DC4C67DD5AAA2ADCA6909B8C3EC83B847D33AA8BDD9C
AFE9BBAC519524AA7DF47EA7EDD12297CF1A9BB3DA07E。

9.4 卡片特征与密钥信息的对应关系

卡片特征中是否个人化动态数据认证相关数据应根据 9.5 条中卡片 AIP 的具体设置进行处理。表 47 体现了卡片特征与密钥信息的对应关系。

表47 卡片特征与密钥的对应关系

卡片特征	采用算法	发卡行公私钥对	IC 卡公私钥对	对称密钥
1	仅国际	RSA 1024 位, 见 9.3.3	RSA 1024 位, 见 9.3.11	3DES, 见 9.3.1
2		RSA 1024 位, 见 9.3.3	RSA 1024 位, 见 9.3.11	3DES, 见 9.3.1
3		RSA 1152 位, 见 9.3.3	RSA 1152 位, 见 9.3.12	3DES, 见 9.3.1
4		RSA 1408 位, 见 9.3.6	RSA 1408 位, 见 9.3.14	3DES, 见 9.3.1
5		RSA 1984 位, 见 9.3.7	RSA 1976 位, 见 9.3.15	3DES, 见 9.3.1
6		RSA 1024 位, 见 9.3.3	RSA 1024 位, 见 9.3.11	3DES, 见 9.3.1
7		RSA 1152 位, 见 9.3.4	RSA 1152 位, 见 9.3.12	3DES, 见 9.3.1
8		RSA 1408 位, 见 9.3.6	RSA 1408 位, 见 9.3.14	3DES, 见 9.3.1
9		RSA 1984 位, 见 9.3.7	RSA 1976 位, 见 9.3.15	3DES, 见 9.3.1
10 至 27		RSA 1024 位, 见 9.3.3	RSA 1024 位, 见 9.3.11	3DES, 见 9.3.1
29	仅国际	RSA 1024 位, 见 9.3.3	RSA 1024 位, 见 9.3.11	3DES, 见 9.3.1
30		RSA 1152 位, 见 9.3.4	RSA 1152 位, 见 9.3.12	3DES, 见 9.3.1

表 47 (续)

卡片特征	采用算法	发卡行公私钥对	IC 卡公私钥对	对称密钥
51		RSA 1408 位, 见 9.3.6	RSA 1408 位, 见 9.3.14	3DES, 见 9.3.1
1 至 30	仅国密	SM2-推荐曲线-索引 57, 见 9.3.8	SM2-推荐曲线-索引 57, 见 9.3.8	SM4, 见 9.3.2
1	双算法	RSA 1024 位, 见 9.3.3 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1024 位, 见 9.3.11 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
2		RSA 1024 位, 见 9.3.3 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1024 位, 见 9.3.11 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
3		RSA 1152 位, 见 9.3.4 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1152 位, 见 9.3.12 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
4		RSA 1408 位, 见 9.3.6 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1408 位, 见 9.3.14 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
5		RSA 1984 位, 见 9.3.7 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1976 位, 见 9.3.15 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
6		RSA 1024 位, 见 9.3.3 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1024 位, 见 9.3.11 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
7		RSA 1152 位, 见 9.3.4 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1152 位, 见 9.3.12 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
8		RSA 1408 位, 见 9.3.6 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1408 位, 见 9.3.14 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
9		RSA 1984 位, 见 9.3.7 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1976 位, 见 9.3.15 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
10 至 26		RSA 1024 位, 见 9.3.3 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1024 位, 见 9.3.11 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1 SM4, 见 9.3.2
27		RSA 1024 位, 见 9.3.3 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1024 位, 见 9.3.11 SM2-推荐曲线-索引 57, 见 9.3.8	SM4, 见 9.3.2
28		RSA 1024 位, 见 9.3.3 SM2-推荐曲线-索引 57, 见 9.3.8	RSA 1024 位, 见 9.3.11 SM2-推荐曲线-索引 57, 见 9.3.8	3DES, 见 9.3.1

表 47 (续)

卡片特征	采用算法	发卡行公私钥对	IC 卡公私钥对	对称密钥
29	双算法	RSA 1024 位，见 9.3.3 SM2-推荐曲线-索引 57，见 9.3.8	RSA 1024 位，见 9.3.11 SM2-推荐曲线-索引 57，见 9.3.8	3DES，见 9.3.1 SM4，见 9.3.2
30	双算法	RSA 1152 位，见 9.3.6 SM2-推荐曲线-索引 57，见 9.3.8	RSA 1152 位，见 9.3.12 SM2-推荐曲线-索引 57，见 9.3.8	3DES，见 9.3.1 SM4，见 9.3.2
51		RSA 1408 位，见 9.3.6 SM2-推荐曲线-索引 57，见 9.3.8	RSA 1408 位，见 9.3.14 SM2-推荐曲线-索引 57，见 9.3.8	SM4，见 9.3.2
52		RSA 1408 位，见 9.3.6 SM2-推荐曲线-索引 57，见 9.3.8	RSA 1408 位，见 9.3.14 SM2-推荐曲线-索引 57，见 9.3.8	3DES，见 9.3.1
31	仅国际	1024 位，见 9.3.3	768 位，见 9.3.10	3DES，见 9.3.1
32			1024 位，见 9.3.11	
33				
34				
35				
36		1152 位，见 9.3.4	1152 位，见 9.3.12	
37				
38		1408 位，见 9.3.6	1280 位，见 9.3.13	
39				
40		1984 位，见 9.3.7	1976 位，见 9.3.15	
41 和 53		1024 位，见 9.3.3	1024 位，见 9.3.11	
42				
43				
44				
45				
46		1408 位，见 9.3.6	1408 位，见 9.3.14	3DES，见 9.3.1
47				3DES，见 9.3.1
48 和 54	1984 位，见 9.3.7	1984 位，见 9.3.16	3DES，见 9.3.1	
49 和 55	仅国密	SM2-推荐曲线-索引 57，见 9.3.8	SM2-推荐曲线-索引 57，见 9.3.8	SM4，见 9.3.2
31 至 49				
53 至 55				
31 至 43	双算法	同时具备上述“仅国际”的密钥和“仅国密”的密钥。		
44		同时具备上述“仅国际”的密钥和“仅国密”的密钥。		SM4，见 9.3.2
45				3DES，见 9.3.1
46 至 49 53 至 55		同时具备上述“仅国际”的密钥和“仅国密”的密钥。		

9.5 卡片特征

9.5.1 卡片特征 1 至卡片特征 19

表 48 基于本部分第 9.2.1 条规定的借记/贷记基本特征。对卡片个性化特征 1，SFI 4 的 1 号记录应存储以下数据：70 08 9F 14 01 03 9F 23 01 07。

表48 卡片特征 1 至卡片特征 19

应用首选名称 [9F 12]	AIP [82]	ADA [9F 52]	发卡行 认证指 示位 [9F 56]	LCOL [9F 58]	UCOL [9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 31 卡片特征 1	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	82 40 -如果发卡行认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限， 拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 32 卡片特征 2	58 00 -支持 SDA -支持持卡人认证 -执行终端风险管理	82 40 -如果发卡行认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限， 拒绝交易	N/A	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 33 卡片特征 3	7C 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	82 40 -如果发卡行认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限， 拒绝交易	00 -可选	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 34 卡片特征 4	7C 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	1E 40 -如果交易拒绝脱机执行，生成通知 -如果在本次交易中 PIN 尝试次数超出而 且交易拒绝，生成通知 -如果因为发卡行认证失败或没有执行导 致交易拒绝，生成通知 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限， 拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 36 卡片特征 6	7C 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	82 40 -如果发卡行认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限， 拒绝交易	80 -强制	00	07

表 48 (续)

应用首选名称 [9F 12]	AIP [82]	ADA [9F 52]	发卡行 认证指 示位 [9F 56]	LCOL [9F 58]	UCOL [9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 37 卡片特征 7	7D 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证 -支持复合 CDA- GENERATE AC	82 40 -如果发卡行认证失败, 下次联机交易 -如果是新卡, 联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	09	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 38 卡片特征 8	7D 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证 -支持复合 CDA- GENERATE AC	80 40 -如果发卡行认证失败, 下次联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	00 -可选	03	09
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 39 卡片特征 9	79 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持复合 CDA- GENERATE AC	80 40 -如果发卡行认证失败, 下次联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	N/A	09	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 30 卡片特征 10	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	80 00 -如果发卡行认证失败, 下次联机交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 31 卡片特征 11	1C 00 -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	82 40 -如果发卡行认证失败, 下次联机交易 -如果是新卡, 联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	03	07

表 48 (续)

应用首选名称 [9F 12]	AIP [82]	ADA [9F 52]	发卡行 认证指 示位 [9F 56]	LCOL [9F 58]	UCOL [9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 32 卡片特征 12	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	C2 40 -如果发卡行认证失败, 下次联机交易 -如果发卡行认证执行但失败, 拒绝交易 -如果是新卡, 联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	09	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 33 卡片特征 13	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	C6 40 -如果发卡行认证失败, 下次联机交易 -如果发卡行认证执行但失败, 拒绝交易 -如果因为发卡行认证失败或没有执行导 致交易拒绝, 生成通知 -如果是新卡, 联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 34 卡片特征 14	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	92 40 -如果发卡行认证失败, 下次联机交易 -如果交易拒绝脱机执行, 生成通知 -如果是新卡, 联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 35 卡片特征 15	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	82 40 -如果发卡行认证失败, 下次联机交易 -如果是新卡, 联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	03	00
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 36 卡片特征 16	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	83 40 -如果发卡行认证失败, 下次联机交易 -如果是新卡, 联机交易 -如果是新卡, 当交易无法联机时拒绝交 易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	03	07

表 48 (续)

应用首选名称 [9F 12]	AIP [82]	ADA [9F 52]	发卡行 认证指 示位 [9F 56]	LCOL [9F 58]	UCOL [9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 37 卡片特征 17	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	82 30 -如果发卡行认证失败, 下次联机交易 -如果是新卡, 联机交易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易 -如果在前次交易中 PIN 尝试次数超限, 当交易无法联机时拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 38 卡片特征 18	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	93 40 -如果发卡行认证失败, 下次联机交易 -如果交易拒绝脱机执行, 生成通知 -如果是新卡, 联机交易 -如果是新卡, 当交易无法联机时拒绝交 易 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 39 卡片特征 19	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	82 C0 -如果发卡行认证失败, 下次联机交易 -如果是新卡, 联机交易 -如果在本次交易中 PIN 尝试次数超限, 应用锁定 -如果在前次交易中 PIN 尝试次数超限, 拒绝交易	80 -强制	03	07

9.5.2 卡片特征 20

表 49 基于本部分第 9.2.1 条规定的借记/贷记基本特征。此特征用于测试执行频度检查和发卡行脚本处理失败。使用最大值个人化此类数据元素, 以保证不引起包括此类元素的频度检查超限条件。

表49 卡片特征 20

数据元素	值
LCOL [9F 58]	0F
UCOL [9F 59]	0F
连续交易限制数 (国际) [9F 53]	0F
累计交易金额限制数 [9F 54]	000099999999
累计交易金额限制数 (双货币) [9F 75]	000000030000

表 49 (续)

应用首选名称 [9F 12]	AIP [82]	发 卡 行 认 证 指 示 位 [9F 56]	ADA [9F 52]	连 续 交 易 限 制 数 [9F 72]	累 计 交 易 金 额 上 限[9F 5C]	第 二 应 用 货 币 代 码 [9F 76]	货 币 转 换 因 子 [9F 73]
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 30 卡片特征 20	5C 00 -支持SDA -支持持卡人 认证 -执行终端风 险管理 -支持发卡行 认证	80 -强制	C2 48 -如果发卡行认证失 败, 下次联机交易 -如果发卡行认证执 行但失败, 拒绝交易 -如果是新卡, 联机交 易 -如果在前次交易中 PIN尝试次数超限, 拒 绝交易 -如果发卡行脚本命 令在前次交易中失 败, 联机交易	05	000000005000	0826	20000175

9.5.3 卡片特征 21 至卡片特征 23

表 50 基于本部分第 9.2.1 条规定的借记/贷记基本特征。卡片特征 21 和 22 针对支持 DDA 的卡片。
卡片特征 23 针对支持支持 CDA 的卡片。

表50 卡片特征 21 至卡片特征 23

应用首选名称 [9F 12]	AIP [82]	ADA [9F 52]	发 卡 行 认 证 指 示 位 [9F 56]	LCOL [9F 58]	UCOL [9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 31 卡片特征 21	7C 00 -支持SDA -支持DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	C0 00 -如果发卡行认证失败, 下次联机交易 -如果发卡行认证执行但失败, 拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 32 卡片特征 22	7C 00 -支持SDA -支持DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证	A2 00 -如果发卡行认证失败, 下次联机交易 -如果发卡行认证必备但没有收到 ARPC, 拒绝交易 -如果是新卡, 联机交易	80 -强制	03	07

表 50（续）

应用首选名称 [9F 12]	AIP [82]	ADA [9F 52]	发卡行 认证指 示位 [9F 56]	LCOL [9F 58]	UCOL [9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 33 卡片特征 23	7D 00 -支持SDA -支持DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证 -支持复合 CDA- GENERATE AC	C0 00 -如果发卡行认证失败，下次联机交易 -如果发卡行认证执行但失败，拒绝交易	80 -强制		

9.5.4 卡片特征 24

表 51 用于测试加强 ATC 处理（Enhanced ATC Processing）。此特征除了以下标明的数据其余均按卡片特征 1 个人化。

表51 卡片特征 24

应用首选名称 [9F 12]	应用交易计数器 [9F 36]
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 34 卡片特征 24	FF FD

9.5.5 卡片特征 5，25，26

表 52 基于本部分第 9.2.1 条规定的借记/贷记基本特征。此类特征用于测试附加频度和更新功能。此类特征对于支持累计连续国际交易（货币）、交易金额（双货币）、更新记录和写数据的频度检查的卡片是必需的。使用最大值个人化此类数据元素，以保证不引起包括这些元素的频度检查超限条件。

表52 卡片特征 5，25，26

数据元素	值
LCOL[9F 58]	0F
UCOL[9F 59]	0F
连续交易限制数（国际）[9F 53]	0F
累计交易金额限制数[9F 54]	000099999999

表 52 (续)

应用首选名称 [9F 12]	AIP [82]	AIA [9F 56]	ADA [9F 52]	连 续 交 易 限 制 数 [9F 72]	累 计 交 易 金 额 限 制 数 (双 货 币) [9F 75]	第 二 应 用 货 币 代 码 [9F 76]	货 币 转 换 因 子 [9F 73]
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 35 卡片特征 5	7C 00 -支持SDA -支持DDA -支持持卡人 认证 -执行终端风 险管理 -支持发卡行 认证	80 -强制	82 40 -如果发卡行认证失 败, 下次联机交易 -如果是新卡, 联机交 易 -如果在前次交易中 PIN尝试次数超限, 拒 绝交易	0F	000000015000	0826	20000175
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 35 卡片特征 25	5C 00 -支持SDA -支持持卡人 认证 -执行终端风 险管理 -支持发卡行 认证	80 -强制	82 40 -如果发卡行认证失 败, 下次联机交易 -如果是新卡, 联机交 易 -如果在前次交易中 PIN尝试次数超限, 拒 绝交易	03	000000015000	0826	20000175
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 36 卡片特征 26	5C 00 -支持SDA -支持持卡人 认证 -执行终端风 险管理 -支持发卡行 认证	00 -可选	82 40 -如果发卡行认证失 败, 下次联机交易 -如果是新卡, 联机交 易 -如果在前次交易中 PIN尝试次数超限, 拒 绝交易	03	000000015000	0826	20000175

9.5.6 卡片特征 27

表 53 和表 54 基于本部分第 9.2.1 条规定的借记/贷记基本特征。本特征用于测试多应用选择 (Multi Application Select)。应用 1 此特征除了以下标明的数据其余均按卡片特征 1 个人化, 应用选择时应首选项选中此应用。

表53 卡片特征 27 (1)

应用首选名称 [9F 12]	应用标识符 [84]	应用交互特征 [82]
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 37	A0 00 00 03 33 01 01 01	7D 00

应用 2 此征除了以下标明的数据其余均按卡片特征 1 个人化。

表54 卡片特征 27（2）

应用首选名称	应用标识符	应用交易	应用交互特征
[9F 12]	[84]	计数器 [9F 36]	[82]
43 41 52 44 20 49 4D 41 47 45 20 30 40 32 37	A0 00 00 03 33 01 01 02	FF FD	7D 00

9.5.7 卡片特征 28

本特征基于卡片特征 23，卡片支持的算法类型和密钥长度见本文档 9.4 条。

9.5.8 卡片特征 29，30

表 55 用于仅支持传统加密算法的基于借记贷记应用的小额支付（即电子现金）功能，对于支持基于借记贷记应用的小额支付的卡必须能够支持多个 AIP、AFL、CVM 列表。除下表定义的数据外，其余数据按卡片特征 1 个人化。对于卡片特征 29 应使用特征 21 中的 DDA 相关数据（IC 卡密钥、发卡行公钥证书、CA 公钥等）。

表55 卡片特征 29，30

应用首选名称	AIP	ADA	发卡行	LCOL	UCOL
[9F 12]	[82]	[9F 52]	认证指 示位 [9F 56]	[9F 58]	[9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 39 卡片特征 29	7C 00 — 借记/贷记 -支持 SDA、DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证 78 00 — 基于借记贷 记应用的小额支付 -支持 SDA、DDA -支持持卡人认证 -执行终端风险管理	82 C8 -如果发卡行认证失败，下次联机交易 -如果是新卡，联机交易 -如果 PIN 在本次交易中锁定，应用锁定。 -如果 PIN 在前次交易中锁定，拒绝交易 -如果发卡行脚本命令在前次交易中失 败，联机交易	80 -强制	03	07

表 55（续）

应用首选名称 [9F 12]	AIP [82]	ADA [9F 52]	发卡行 认证指 示位 [9F 56]	LCOL [9F 58]	UCOL [9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 33 30 卡片特征 30	7D 00 — 借记/贷记 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证 -支持 CDA 7D 00 — 基于借记贷 记应用的小额支付 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡行认证 -支持 CDA	41 30 -如果发卡行认证执行但失败，拒绝交易 -如果是新卡，当交易无法联机时拒绝交 易 -如果 PIN 在前次交易中锁定，联机交易 -如果 PIN 在前次交易中锁定，当交易无 法联机时拒绝交易	80 -强制	03	07

9.5.9 卡片特征 31

表 56 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表56 卡片特征 31

	卡片附加处理	卡片交易属性	LOATC
卡片特征 31	PBOC 3.0 及 UICS: 92 70 10 00 - 支持小额检查 - 支持新卡检查 - 卡优先选择接触式借记/贷记联机 - 不允许不匹配货币的交易 - 如果是新卡且读卡器仅支持脱机则拒绝 交易 - 支持签名 - 快速借记贷记脱机批准的交易，卡片记 录交易日志	30 00	1

9.5.10 卡片特征 32

表 57 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表57 卡片特征 32

	卡片附加处理	卡片交易属性	CTTAUL
卡片特征 32	44 00 50 00 — 支持小额和 CTTA 检查 — 允许货币不匹配的脱机交易 — 不匹配货币的交易支持联机 PIN — 支持签名	30 00	102.00

9.5.11 卡片特征 33

表 58 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表58 卡片特征 33

	卡片附加处理	密文版本	卡片 CVM 限额	CTTAUL
卡 片 特 征 33	41 20 80 00 — 支持小额和 CTTA 检查 — 返回脱机消费可用余额 — 如果是新卡且读卡器仅支持脱机则 拒绝交易 — 匹配货币的交易支持联机 PIN	01	00 00 00 00 11 00	110

9.5.12 卡片特征 34

表 59 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表59 卡片特征 34

	卡片附加处理	密文版本	CTTAL	CTTAUL
卡片特征 34	21 00 F0 00 — 支持小额或CTTA检查 — 返回脱机消费可用余额 — 匹配货币的交易支持联机PIN — 不匹配货币的交易支持联机PIN — 对于不匹配货币交易，卡要求CVM — 支持签名	01	50.00	102.00

9.5.13 卡片特征 35

表 60 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表60 卡片特征 35

	卡片附加处理	卡片 CVM 限额	CTTAL	CTTAUL	交易日志入口
卡片特征 35	41 10 20 00 — 支持小额和 CTTA 检查 — 返回脱机消费可用余额 — 对于不匹配货币交易，卡要求 CVM — 快速借记/贷记脱机批准的交易，卡片 记录交易日志	00 00 00 00 11 00	70.00	不存在	0B14

9.5.14 卡片特征 36

表 61 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表61 卡片特征 36

	卡片附加处理	CTTAL	CTTAUL
卡片特征 36	01 00 10 00 — 返回脱机消费可用余额 — 支持签名	不存在	不存在

9.5.15 卡片特征 37

表 62 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表62 卡片特征 37

	卡片附加处理	PDOL	密文版本	LOATC	卡片 CVM 限额 和第二币种卡 片 CVM 限额
卡片特征 37	83 10 40 00 —支持小额检查 — 卡优先选择接触式借记/ 贷记联机 — 返回脱机消费可用余额 — 不匹配货币的交易支持联 机 PIN —快速借记/贷记脱机批准的 交易, 卡片记录交易日志	支持国密: 9F 66 04 9F 02 06 9F 37 04 5F 2A 02 DF 69 01 不支持国密: 9F 66 04 9F 02 06 9F 37 04 5F 2A 02	17	0	00 00 00 00 11 00

9.5.16 卡片特征 38

表 63 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表63 卡片特征 38

	卡片附加处理	PDOL	密文版本	9F17
卡片特征 68	81 00 30 00 — 支持小额检查 卡片不选择接触式借记贷记联机 — 返回脱机消费可用余额 — 对于不匹配货币交易, 卡要求 CVM — 支持签名	支持国密: 9F 66 04 9F 02 06 9F 37 04 5F 2A 02 DF 69 01 不支持国密: 9F 66 04 9F 02 06 9F 37 04 5F 2A 02	17	0

9.5.17 卡片特征 39

表 64 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表64 卡片特征 39

	卡片附加处理	应用交易计数器 [9F 36]	9F17	CTTAL
卡片特征 39	2C 00 F0 00 – 支持小额或 CTTA 检查 – 支持 PIN 重试次数超过检查 – 允许货币不匹配的脱机交易 – 匹配货币的交易支持联机 PIN – 对于不匹配货币交易，卡要求 CVM – 支持签名	FF E0	0	50.00

9.5.18 卡片特征 40

表 65 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表65 卡片特征 40

	卡片附加处理	9F17	CTTAL	CTTAUL
卡片特征 40	24 10 B0 00 – 支持小额或 CTTA 检查 – 允许货币不匹配的脱机交易 – 匹配货币的交易支持联机 PIN – 对于不匹配货币交易，卡要求 CVM – 支持签名 – 快速借记/贷记脱机批准的交易，卡片记录交易日志	3	50.00	102.00

9.5.19 卡片特征 41

表 66 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。如不支持 1976 位的 IC 卡密钥，则将 AIP 改为仅支持 SDA。

表66 卡片特征 41

	卡片附加处理	9F17	CTTAL	CTTAUL
卡片特征 41	45 90 F0 00 – 支持小额和 CTTA 检查 – 允许货币不匹配的脱机交易 – 返回脱机消费可用余额 – 支持预付 – 匹配货币的交易支持联机 PIN – 对于不匹配货币的交易支持联机 PIN – 对于不匹配货币交易，卡要求 CVM – 支持签名 – 快速借记/贷记脱机批准的交易，卡片记录交易日志	3	50.00	102.00

9.5.20 卡片特征 42

表 67 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表67 卡片特征 42

	卡片附加处理	PDOL	9F17
卡片特征 42	85 80 F0 00 – 支持小额检查 – 允许货币不匹配的脱机交易 – 返回脱机消费可用余额 – 支持预付 匹配货币的交易支持联机 PIN – 对于不匹配货币的交易支持联机 PIN – 对于不匹配货币交易，卡要求 CVM – 支持签名	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04	3

9.5.21 卡片特征 43

表 68 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

此特征的非接触界面下的 PDOL 9F38 应设置为 9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04（即不含有 SM 算法支持指示器）。

表68 卡片特征 43

	卡片附加处理	PDOL	CTTAL	CTTAUL
卡片特征 43	PBOC 3.0及UICS: 8D 00 30 00 – 支持小额检查 – 支持 PIN 重试次数超过检查 – 允许货币不匹配的脱机交易 – 返回脱机消费可用余额 – 对于不匹配货币交易，卡要求 CVM – 支持签名	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04	不存在	不存在

9.5.22 卡片特征 44

表 69 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表69 卡片特征 44

	卡片附加处理	密文版本	CTTAUL
卡片特征44	41 20 80 00 – 支持小额和CTTA检查 –返回脱机消费可用余额 –如果是新卡且读卡器仅支持脱机则拒绝交易 –匹配货币的交易支持联机PIN	01	110

9.5.23 卡片特征 45

表 70 基于本部分第 9.2.3 条规定的快速借记/贷记基本特征。

表70 卡片特征 45

	卡片附加处理	密文版本	卡片 CVM 限额	CTTAUL
卡片特征 45	51 20 80 00 — 支持小额和 CTTA 检查 — 支持新卡检查 — 返回脱机消费可用余额 — 如果是新卡且读卡器仅支持脱机则拒绝交易 — 匹配货币的交易支持联机 PIN	01	00 00 00 00 11 00	110

9.5.24 卡片特征 46

表 71 基于本部分第 9.2.4 条规定的非接触式小额支付扩展基本特征。

表71 卡片特征 46

数据对象	Tag	Length	Value
AIP	82	02	70 00 — 快速借记/贷记 AIP —支持 SDA —支持持卡人认证 —支持 DDA
卡片附加处理	9F68	04	81 10 00 00 —支持小额检查 —返回脱机消费可用余额 —快速借记/贷记脱机批准的交易，记录交易日志
电子现金余额	9F79	06	00 00 00 10 00 00
电子现金余额上限	9F77	06	00 00 00 50 00 00
电子现金单笔交易限额	9F78	06	00 00 00 10 00 00
电子现金重置阈值	9F6D	06	00 00 00 00 00 00
卡片交易属性	9F6C	02	00 00
卡片 CVM 限额	9F6B	06	00 00 00 10 00 00
连续交易限制数（国际-货币）	9F53	01	00

对于卡片特征 46，除 SFI=0x19 和 SFI=0x1E 的扩展应用专用文件外，再新增三个变长文件，总共四个变长文件和一个循环文件：

- 变长文件，其 SFI=0x1。该文件至少可开通 4 个行业应用，即至少可 Append 4 条记录。每个记录不超过 128 字节。开通密钥：15A912A5F029C6001DF2539A00137049。
- 变长文件，其 SFI=0x16。该文件可开通 2 个行业应用，即可 Append 2 条记录。每个记录不超过 128 字节。开通密钥：167312850029B6001DC2539A0013E049。
- 变长文件，其 SFI=0x17。该文件可开通 7 个行业应用，即至少可 Append 7 条记录。每个记录不超过 128 字节。开通密钥：191A5F026001DF259A03019C37049F11。

9.5.25 卡片特征 47

表 72 基于卡片特征 46，除下表规定的的数据外，其余数据均按照卡片特征 46 来设置。

表72 卡片特征 47

数据对象	Tag	Length	Value
可用脱机消费金额	9F5D	06	00 00 00 00 00 01
电子现金分段扣费透支限额	DF62	06	00 00 00 10 00 00
电子现金分段扣费已透支额	DF63	06	00 00 00 00 00 00

9.5.26 卡片特征 48

数据同卡片特征 31，区别在于以下两点：

——选用的密钥长度，具体见本部分第 9.4 条；

——9F46、9F48 和 93，具体见下文定义。

IC 卡公钥证书（9F46）=

8BD42B1C967A3C4CC383CF4B4B8EEFBB21A6945BF15F22072E6BE2E9FF0786DC489A04649F16A61E40CCAD3
C9B6D6D2DBCC12C71A0D80C07278A476C00C7A23F24EC33B96AC6B93653A85E69357A42F7325B5668268C6E
0C07204F3F7DAB061CDA383BD38FDFD3DAC4695E1ABF55C0F0E4440B12632E3F49BA145CCB4C7C7C6FB69DB
A70C8C5D7360CEB96D2B51B1C21BEEDC76F006C1C59F6460A4E426539C5D0E11E706A9ADC8C9A7BD197486A
104F

IC 卡公钥余项（9F48）=

F28AEE954ECDC5B4C0FAD9EFCB659FE3C01E431F3440B3E0167DD5DCDE431E1378745DAE9D4C50432D7D

签名的静态数据（93）=

4CDC5B13C43682BBAC78EC274CEC76ACE557B7C9984BABAC9272926ABAECEAE2808865F05ACAF4E28A261E8
870BF659156E85EE800B841C693E4AC7612E774B6EECF234522339C3F31CD33183A0A6FD6203659393A0F54
BDC30208305821D7EACD5101DAFD25BAFBCFCEFB9B8433610A29E7E045968E89A40D86CF18A3C94ED88072
91EF37AC02BA666D113E961B8F82A19F68BD38A8A0387EAE23199106FC7F3B8413EE1B3E04BB3CA14179BB5
51E5

9.5.27 卡片特征 49

数据同卡片特征 31，区别在于以下两点：

——选用的密钥长度，具体见本部分第 9.4 条；

——9F46、9F48 和 93，具体见下文定义。

IC 卡公钥证书（9F46）=

007F462A2A922F806A4CEF5A74352E0F5BB0A453CB9F3DD8933C173B93751EC15BB96BDB1425201C99A6028
16CC4C84584B2CEC03F3E82759A7B1EC03CA9A37AFB55700D194CF3B851B6FD9EB69C3913E024872D3DF424
4D0CE1C68C50AE4AF5AA73B3FDEADA64CAD6CE8F45A4B6378D305925C0B7E1F3C88BB4104E56150357BA64C
B16C97405EFFC0ACE23BD94920B18813D1BA8E2D1ED1083416E5DD0B2E77E160B69A7427A118317C9C920E
A9E4ED7448B26FF5EC8A6416E996DBB0A6B069F745C0B396EFF77F2309BA64F471F7267C9B9BDAA1BB1C4BE
B3D727916291C808CEC1BBD526C9DC9C7398234EFB64F52A94622AB90EFBE87

IC 卡公钥余项（9F48）=

EED3FD6DAB24D7A9C32852F866C751D7710F494A0DF11B67FAECDD87A9A4E2CC44F6F27E46E3C0CCCD0F

签名的静态数据（93）=

0011073D70FB2BAE07B5C32212AEEE4E6348F0640449A4F3BCDFFC51C7728D5BE0786B1BC2F9101DF59E3C5
322F4E2FA5892DF5812DE602F36DA2A3199B443C7034534C783DFF3871A694C58D28EA410A0B4828D7E9385

AA3C36DA4052BF14AF632CEC093E24A6799BEE4ED146D02CCF493B4A612570E12C7D87DC758C51BFFFCFC46
7F241F678683B4A3B95AE0FC165BEB27B5DC955960799DAC455A44767804FE773A09F103BCC9B0FE8EA73F8
EA41AB25B28F8051BEAA21DDCE6B24C62EA061360B38FD5D7BBBCB4558C5CC175FC31D1E05CD41D63F1C86B
F7EFC9114B37BDF86036342E66932DD103F95E967A4EB0D52CC5FFC101BBA

9.5.28 卡片特征 51, 52

数据同卡片特征 30, 区别在于选用的密钥长度, 具体见本部分第 9.4 条。

9.5.29 卡片特征 53

数据同卡片特征 41, 区别在于卡片附加处理 (9F68)。

卡片特征 53 的 9F68 的值为 85 80 F0 00。

9.5.30 卡片特征 54

数据同卡片特征 48, 区别在于卡片附加处理 (9F68)。

卡片特征 54 的 9F68 的值为 92 60 10 00。

9.5.31 卡片特征 55

数据同卡片特征 49, 区别在于卡片附加处理 (9F68)。

卡片特征 55 的 9F68 的值为 92 60 10 00。
