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 0045.2—2014
代替JR/T 0045.2—2008

中国金融集成电路（IC）卡检测规范 第2部分：借记/贷记应用终端检测规范

China financial integrated circuit card test specifications—
Part 2: Debit/Credit terminal test specification

2014-07-30 发布　　2014-07-30 实施

中国人民银行　发布

目　次

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2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0045.2—2008《中国金融集成电路（IC）卡检测规范　第2部分：借记/贷记应用终端检测规范》。

本部分与JR/T 0045.2—2008相比主要变化如下：

——修改了标准的前言；

——修改了测试案例的案例编号；

——删除了对DDF的描述和与DDF相关的测试案例、金额与PIN的输入过程相关的测试案例和旧的终端随机数测试案例；

——修改了PPS案例测试案例和SDA相关测试案例；

——增加了支持再同步终端测试案例、异常情况测试案例、兼容性测试案例、应用选择测试案例、4种CDA模式测试案例、国密算法测试案例、电子现金终端测试案例、新的终端随机数测试案例、圈存日志测试案例和不支持脱机密文PIN情况的测试案例；

——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、捷德（中国）信息科技有限公司、金雅拓科技（北京）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、李春欢、刘志刚、张永峰、余沁、李乃珊、胡盖、于虹、陆洋、王二军、张跃、金自荣、黄海龙、高大伟、程晋疆、周权、陈莹、冯欢、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 0025.6，在此基础上制定了中国金融集成电路（IC）卡借记/贷记应用终端的相关检测案例。

中国金融集成电路（IC）卡检测规范
第2部分：借记/贷记应用终端检测规范

1 范围

本部分从终端检测角度描述了借记/贷记交易流程的要求，包括终端硬件需求、终端内部处理细节、终端使用数据元、终端支持指令集等。

本部分适用于支持JR/T 0025.6—2013所规定的借记/贷记应用的销售点终端以及其他类似的终端设备。使用对象主要是与金融IC卡应用相关的终端设计、制造、检测，以及应用系统研制、开发、集成和维护的部门（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

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。

3.2

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。

3.3

磁条 magstripe

包括磁编码信息的条状物。

3.4

串联 concatenation

通过把第二个元素的字节添加到第一个元素的结尾将两个元素连接起来。每个元素中的字节在结果串中的顺序和原来从IC卡发到终端时的顺序相同，高位字节在前。在每个字节中比特按由高到低的顺序排列。一组元素或对象可以按下面的方式连接：将第一对元素连接成新的元素，把它作为第一个元素再连接下一个元素，以此类推。

3.5

发卡行行为代码 issuer action code

发卡行根据TVR的内容选择的动作。

3.6
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。

3.7
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。

3.8
哈希函数 hash function

将一个位串映射成固定长度的位串的函数。

3.9
哈希结果 hash result

哈希函数输出的位串。

3.10
集成电路 integrated circuit

被设计用来完成处理和/或存储功能的电子器件。

3.11
集成电路卡 integrated circuit 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。

3.12
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。

3.13
加密算法 cryptographic algorithm

隐藏或显现数据信息内容的变换算法。

3.14
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。

3.15
解密 decipherment

对应加密过程的逆操作。

3.16
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。

3.17
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。

3.18
卡片 card

支付系统定义的支付卡片。

3.19

路径 path

没有分隔的文件标识符的连接。

3.20

密钥 key

加密转换中控制操作的一组符号。

3.21

密钥回收 key revocation

回收使用中的密钥以及处理其使用后的遗留问题的密钥管理过程。密钥回收可以按计划回收或提前回收。

3.22

密文 cryptogram

加密运算的结果。

3.23

密码 ciphertext

加密的信息。

3.24

明文 plaintext

未加密的信息。

3.25

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。

3.26

认证 authentication

确认一个实体所宣称的身份的措施。

3.27

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。

3.28

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。

3.29

填充 padding

向数据串某一边添加附加位。

3.30

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。

3.31

应用 application

卡片和终端之间的应用协议和相关的数据集。

3.32

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。

3.33

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。

3.34

证书回收 certificate revocation

由发行证书的实体废除一个有效证书的过程。

3.35

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。

3.36

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。

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）
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）
ARC 授权响应码（Authorization Response Code）
ARPC 授权响应密文（Authorization Response Cryptogram）
ARQC 授权请求密文（Authorization Request Cryptogram）
ASI 应用选择标识（Application Selection Indicator）
ATC 应用交易序号（Application Transaction Counter）
ATM 自动柜员机（Automated Teller Machine）
AUC 应用用途控制（Application Usage Control）
BER 基本编码规则（Basic Encoding Rules）
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 Rish 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 字节 of the Command Message）
cn	压缩数字格式（compress numeric）
CTPDU	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）
DDA	动态数据认证（Dynamic Data Authentication）
DF	专用文件（Dedicated File）
DIR	目录（Directory）
DOL	数据对象列表（Data Object List）
EF	基本文件（Elementary File）
EMV	Europay MasterCard VISA
FCI	文件控制信息（File Control Information）
GPO	获取处理选项（GET PROCESSING OPTIONS）
IAC	发卡行行为代码（Issuer Action Code）
IAD	发卡行应用数据（Issuer Application Data）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
Lr	响应数据域的长度（Length of Response Data Field）
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 案例 3 or 4 Command）
LCOL	连续脱机交易下限
LDD	IC 卡动态数据的长度（Length of the ICC Dynamic Data）
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（Last Online ATC）
Lr	响应数据域的长度（Length of Response Data Field）
LRC	冗余校验（Longitudinal Redundancy Check）
LT	底层测试工具（Lower Tester）
M	必备（Mandatory）
MA	毫安
MAC	报文认证码（Message Authentication Code）
max-	最大值
MDK	主密钥（Master DEA Key）
MF	主文件（Mater File）
mΩ	兆欧
m/s	米/秒
N	数字型（Numeric）
N/A	不适用
NAD	节点地址（Node Address）

NAK	否定的确认（Negative Acknowledgment）
nAs	纳安秒
N_{CA}	认证中心公钥模数的长度（Length of the Certification Authority Public Key Modulus）
N_I	发卡行公钥模数的长度（Length of the Issuer Public Key Modulus）
N_{IC}	IC卡公钥模数的长度（Length of the ICC Public Key Modulus）
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 字节）
PCO	控制和观测点（Point of Control & Observation）
pF	皮法
P_I	发卡行公钥（Issuer Public Key）
P_{IC}	IC卡公钥（ICC Public Key）
PIN	个人密码（Personal Identification Number）
PIX	专用应用标识符扩展(Proprietary Application Identifier Extension)
PKI	公钥基础设施（Public Key Infrastructure）
PTC	PIN重试次数（PIN Try Counter）
PTS	协议类型选择（Protocol Type Selection）
RFU	保留（Reserved for Future Use）
RID	注册应用提供商标识（Registered Application Provider Identifier）
RTPDU	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	短文件标识符（Short File Identifier）
SW1	状态码1（Status Word One）
SW2	状态码2（Status Word Two）
TAC	终端行为代码（Terminal Action Code）
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）
TLV	标签、长度、值（Tag Length Value）
TRM	终端风险管理（Terminal Risk Management）
TSI	交易状态信息（Transaction Status Information）
TVR	终端验证结果（Terminal Verification Results）
t_F	信号幅度从90%下降到10%的时间（Fall Time Between 90% 和 10% of Signal Amplitude）
t_{Px}	超出监控电压的时间周期x（Time period x over which a Voltage is monitored）
UCOL	连续脱机交易上限（Upper Consecutive Offline Limit）
UDK	子密钥（Unique DEA Key）
UT	上层测试工具（Upper Tester）
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_{OL}	低电平输出电压（Low Level Output Voltage）

V_{OLinst}	发送模式下，I/O 上瞬间低电压
V_{OH}	高电平输出电压（High Level Output Voltage）
V_{OHinst}	发送模式下，I/O 上瞬间高电压
Vpp	编程电压（Programming Voltage）
WI	等待时间整数（Waiting Time Integer）
WTX	等待时间扩展（Waiting Time Extension）
εV	测试工具设备的电压测量精度（Voltage measurement accuracy of the Test Tool equipment）
εs	测试工具设备的时间测量精度（Time measurement accuracy of the Test Tool equipment）
εΩ	测试工具设备的电阻测量精度（Resistance measurement accuracy of the Test Tool equipment）
εN	测试工具设备的压力测量精度(Force measurement accuracy of the Test Tool equipment）
εA	测试工具设备的电流测量精度（Current measurement accuracy of the Test Tool equipment）
ε%	测试工具设备的占空比测量精度（Duty Cycle measurement accuracy of the Test Tool equipment）
εHz	测试工具设备的频率测量精度(Frequency measurement accuracy of the Test Tool equipment）
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，终端才可以正常与卡片交互。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终端，还是支持基于借记贷记应用的小额支付的终端，还是未加载任何应用的读卡模块，都应通过第 6 章的测试案例的检测。

第 7 章是针对终端中借记贷记应用的测试案例，支持借记贷记应用的终端应通过这些案例的检测。

第 8 章是针对终端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终端应通过这些案例的检测。

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±3℃，湿度20%至80%之间。如无特殊说明，后续案例均采用此环境条件。

最低温度默认情况下采用0℃。如果终端支持的最低环境温度高于0℃，则采用终端所支持的最低温度进行测试。

最高温度默认情况下采用50℃。如果终端支持的最高环境温度达不到50℃，则采用终端所支持的最高温度进行测试。

如无特殊说明，测试环境的相对湿度为20%到80%之间。

6.2 机械性测试（JXCS）

6.2.1 JXCS001-00 物理兼容性和触点定位

测试目的：确保终端的物理特性能够接受所有尺寸在最大和最小标准范围之间的 IC 卡，并且，终端和拥有最小面积的触点间可以建立电流连接。

测试条件：默认环境条件；待测产品用标准电源供电；插入相关转接卡：
——x=1：最小尺寸转接卡；
——x=2：最大尺寸转接卡。
测试流程：对两个测试条件分别执行：机械插入带有最小触点面积，尺寸分别为最大和最小的转接卡，通过信号的激活确认电气的连接。从终端中拔出转接卡。
通过标准：相关的测试卡可以无阻碍地插入到待测终端中。正确执行触点激活时序。相关的测试卡可以无阻碍地从待测终端中拔出。

6.2.2 JXCS002-00 接口设备触点压力

测试目的：确保终端施加到卡片每一个触点上的压力在规范规定的范围内。

测试条件：默认环境条件；在开始这个测试案例之前，应先执行案例 JXCS00100；待测产品不接电源。
测试流程：将触点压力测试卡插入终端，对每个存在的触点至少测量 3 次，测量间隔至少为 1 秒钟。
通过标准：每个触点的每次测量都应满足：0.2N - N 触点压力 0.6N + N。

6.3 电特性测试（DXCS）

6.3.1 DXCS001-00 短路保护

测试目的：确保终端内部触点短路或者终端触点与 GND 短路情况下，不会对待测终端造成损坏。
测试条件：正常温度、最低温度、最高温度。
测试流程：按下列流程执行：
a)个短路板开始触点激活，短路板的要求：I/O与GND、CLK与GND和RST与GND触点间的电阻都≤2Ω；
b)将短路板插入 10 秒钟；
c)执行测试案例 DXCS01700；
d)用另外一个短路板重复上述测试，短路板的要求：I/O 与 Vcc、CLK 与 Vcc 和 RST 与 V_{CC} 触点间的电阻都≤ 2Ω；
e)再用一个 V_{CC} 和 GND 之间电阻≤ 2Ω的短路板重复上述测试；
f)每一个温度和短路板的组合都重复 1 次测试。
通过标准：执行完这个测试案例后，任何一个其它的测试案例都能够成功地执行。

6.3.2 DXCS002-00 Vpp 隔离（可选）

测试目的：确保终端的该触点是隔离的。
测试条件：默认环境条件；VPP 是电隔离。
测试流程：在终端上电的情况下，测量 C6 和 GND 之间的直流电阻值。
通过标准：电阻≥10MΩ -εΩ。

6.3.3 DXCS003-00 VPP 电压

测试目的：确保在终端与卡片交易过程中，Vpp 电压不超出规范的极限值。
测试条件：正常温度、最低温度、最高温度；负载电流I_{CC}=2mA和54mA（±1mA）。
测试流程：按下列流程执行：
a)发起一个冷复位，返回一个缺省的T=0的ATR，在最小5秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在整个激活时序中，监控 VPP、ATR 和命令序列的处理；
c)对于所有的温度和负载电流重复上述操作。
通过标准：$0 - \varepsilon V \leq V_{PP} \leq (1.05 \times V_{CC}) + \varepsilon V$。

6.3.4 DXCS004-00 I/O 电流

测试目的：确保终端流入或流出 I/O 触点的电流满足规范要求。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个冷复位，返回一个缺省的 T =0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在命令序列的处理过程中，在 I/O 和 V_{CC} 之间加载一个 33Ω的低值负载，计算 I/O 的电流，直到短路引起下电；
c)在 I/O 和 GND 之间加载负载重复上述操作；
d)对于所有的温度和负载电流都重复上述测试。

通过标准：$-15mA - \varepsilon A \leq I_{I/O} \leq 15mA + \varepsilon A$，且该案例执行后的任何一个测试案例都能够正确执行。

6.3.5 DXCS005-00 I/O 传输电压

测试目的：确保信号的高低电压都满足规范要求。
测试条件：正常温度、最低温度、最高温；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个冷复位，返回一个缺省的 T=0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)监控 V_{OH} 和 V_{OL}；
c)对于所有的温度和负载电流都重复上述测试。

通过标准：$(0.8 \times V_{CC}) - \varepsilon V \leq V_{OH} \leq V_{CC} + \varepsilon V$。$0V - \varepsilon V \leq V_{OL} \leq 0.4V + \varepsilon V$。

6.3.6 DXCS006-00 I/O 传输模式下的上升和下降时间

测试目的：确保信号的上升和下降时间满足规范要求。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个冷复位，返回一个缺省的 T=0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在命令序列的处理过程中：

——测量t_R在10%到90%点信号的上升沿；
——测量t_F在90%到10%点信号的下降沿；

c)对于所有的温度和负载电流都重复上述测试。

通过标准：$t_R \leq 0.8\mu s + \varepsilon s$；$t_F \leq 0.8\mu s + \varepsilon s$。

6.3.7 DXCS007-00 I/O 传输模式下的信号抖动

测试目的：确保信号的抖动满足规范要求。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个冷复位，返回一个缺省的T =0的ATR，在最小5秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在命令序列的处理过程中，监控 V_{OHinst} 和 V_{OLinst}；
c)对于所有的温度和负载电流都重复上述测试。

通过标准：$(0.8 \times V_{CC}) - \varepsilon V \leq V_{OHinst} \leq (V_{CC} + 0.25V) + \varepsilon V$；$-0.25V - \varepsilon V \leq V_{OLinst} \leq 0.4V + \varepsilon V$。

6.3.8 DXCS008-00 I/O 接收模式电压

测试目的：确保终端能够正确解释卡片发送在 I/O 上的信号。

测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）；
测试工具的 I/O 电压：
——V_{IH} =（0.9 x V_{cc}）和V_{IL} =0.1V（t_R & t_F <0.1μs）；
——V_{IH} =V_{cc}和V_{IL} =0V（t_R & t_F <0.1μs）；
——V_{IH} =（0.6 x V_{cc}）和V_{IL} =0.5V（t_R & t_F <0.1μs）。
测试流程：按下列流程执行：
a)发起一个冷复位，返回一个缺省的T =0的ATR，在最小5秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在I/O和GND之间加载负载重复上述操作；
c)对于所有的温度、负载电流和I/O电压下都重复上述测试。
通过标准：每一次的命令序列都能正确执行。

6.3.9 DXCS009-00 I/O 接收的上升和下降时间

测试目的：确保终端能够正确解释卡片发送在 I/O 上的上升和下降时间满足规范的信号（逻辑高和低）。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）；
t_R和t_F值：
——t_R & t_F ≤0.1s（±0.01μs），V_{IH} =（0.9 x V_{cc}）和V_{IL} =0.1V；
——t_R & t_F =1.2s（±0.01μs），V_{IH} =（0.9 x V_{cc}）和V_{IL}=0.1V。
测试流程：按下列流程执行：
a)发起一个冷复位，返回一个缺省的T =0的ATR，在最小5秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在 I/O 和 GND 之间加载负载重复上述操作；
c)对于所有的温度、负载电流和 I/O t_R & t_F下都重复上述测试。
通过标准：每一次的命令序列都能正确执行。

6.3.10 DXCS010-00 CLK 电压

测试目的：确保终端产生的高低电压信号能够在规范规定的范围内。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：
a)发起一个冷复位，返回一个缺省的 T =0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)监控 V_{OH}（t_{P1}）和 V_{OL}（t_{P2}）；
c)对于所有的温度和负载电流都重复上述测试。
通过标准：对于t_{P1}：(V_{CC} - 0.5V) - εV ≤ V_{OH} ≤ V_{CC} + εV；对于 t_{P2}：0V - εV ≤ V_{OL} ≤ 0.4V + εV。

6.3.11 DXCS011-00 CLK 上升和下降时间

测试目的：确保信号的上升和下降时间都在规范规定范围内。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：
a)发起一个冷复位，返回一个缺省的 T =0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)测量上升沿从 10%到 90%点的时间 t_R；
c)测量下降沿从 90%到 10%点的时间 t_F；
d)对于所有的温度和负载电流都重复上述测试。
通过标准：t_R ≤时钟周期的8% + ε秒。t_F ≤时钟周期的8% + ε秒。

6.3.12 DXCS012-00 CLK 信号抖动

测试目的：确保信号的抖动在规范的范围内。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个冷复位，返回一个缺省的 T =0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在命令序列执行的过程中监控 VOHinst 和 VOLinst；
c)对于所有的温度和负载电流都重复上述测试。

通过标准：$(V_{CC} - 0.5V) - \varepsilon V \leq V_{OHinst} \leq (V_{CC} + 0.25V) + \varepsilon V$。$-0.25V - \varepsilon V \leq V_{OLinst} \leq 0.4V+\varepsilon V$。

6.3.13 DXCS013-00 CLK 频率和占空比

测试目的：确保CLK的频率、稳定性和占空比在规范的范围内。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个冷复位，返回一个缺省的 T =0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在命令序列执行的过程中，从 CLK 开始以 50ms 为间隔测量 10 次频率和占空比；
c)对于所有的温度和负载电流都重复上述测试。

通过标准：1MHz - εHz ≤平均频率 ≤5MHz+ εHz。频率的变化 ≤平均频率1%。信号周期的45% - ε% ≤占空比 ≤信号周期的55% + ε%。

6.3.14 DXCS014-00 RST 电压

测试目的：确保终端产生的稳态信号的高低电压都在规范的范围内。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个冷复位，返回一个缺省的 T =0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
b)在命令序列执行的过程中，在 RST 由低变高之前监控 V_{OL}（t_{P1}），然后监控 V_{OH}（t_{P2}）；
c)对于所有的温度和负载电流都重复上述测试。

通过标准：$0V - \varepsilon V \leq V_{OL} \leq 0.4V + \varepsilon V$（$t_{P1}$）。$(V_{CC} - 0.5V) - \varepsilon V \leq V_{OH} \leq V_{CC} + \varepsilon V$（$t_{P2}$）。

6.3.15 DXCS015-00 RST 上升和下降时间

测试目的：确保信号的上升和下降时间在规范的范围内。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个序列使得 RST 由低变高；
b)测量上升沿从 10%到 90%点的时间 t_R；
c)发起一个序列使得 RST 由高变低；
d)测量上升沿从 90%到 10%点的时间 t_F；
e)对于所有的温度和负载电流都重复 10 次上述测试。

通过标准：$t_R \leq 0.8\mu s + \varepsilon$ 秒。$t_F \leq 0.8\mu s + \varepsilon$ 秒。

6.3.16 DXCS016-00 RST 信号抖动

测试目的：确保信号的抖动在规范的范围内。
测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=2mA 和 54mA（±1mA）。
测试流程：按下列流程执行：

a)发起一个序列使得 RST 由低变高；
b)从上升沿 90%（t_{P1}）的点开始监控 V_{OHinst} 5 s（+5%）；

c)发起一个序列使得 RST 由高变低；
d)从下降沿 10%（t_{P2}）的点开始监控 V_{OLinst} 5 s（+5%）；
e)发送一个缺省的 T=0 的 ATR，在卡片和终端之间完成一个完整的命令处理过程；
f)在接收 ATR 的前两个字节期间（t_{P3}）监控 V_{OHinst}；
g)在发送命令头的前两个字节期间（t_{P4}）监控 V_{OHinst}；
h)对于所有的温度和负载电流都重复 10 次上述测试。

通过标准：对于 t_{P1} (V_{CC} - 0.5V) - εV ≤ V_{OHinst} ≤ (V_{CC} + 0.25V) + εV。对于 t_{P2} 0.25V - εV ≤ V_{OLinst} ≤ 0.4V + εV。对于 t_{P3} (V_{CC} - 0.5V) - εV ≤ V_{OHinst} ≤ (V_{CC} + 0.25V) + εV。对于 t_{P4} (V_{CC} - 0.5V) - εV ≤ V_{OHinst} ≤ (V_{CC} + 0.25V) + εV。

6.3.17 DXCS017-00 Vcc 触点电压

测试目的：确保终端产生的电源电压在负载状态下满足规范要求的范围。

测试条件：正常温度、最低温度、最高温度；负载电流 I_{CC}=1mA（±0.1mA）、25mA 和 54mA（±1mA）；终端输入电压分别为正常、最大和最小值。

测试流程：按下列流程执行：
a)发起一个冷复位激活V_{CC}；
b)发送一个缺省的 T =0 的 ATR，在最小 5 秒钟的时间内成功处理卡片和终端之间的一个命令序列；
c)在整个命令过程中监控 V_{CC}；
d)对于所有的温度、负载电流和电源电压下都重复上述测试。

通过标准：V_{cc}应该在下列范围内：0V - εV ≤ V_{CC} ≤ 0.4V + εV。4.6V - εV ≤ V_{CC} ≤ 5.4V + εV。

6.3.18 DXCS018-00 VCC 上的瞬间补偿

测试目的：确保终端产生的电源电压在动态负载状态下满足规范要求的范围。

测试条件：正常温度、最低温度、最高温度；负载电流 ICC=1mA（±0.1mA）、25mA 和 54mA（±1mA）；瞬间负载：频率为 5 MHz ±1.00 kHz，占空比为 50 % ±10%，在没有恒定电流的情况下方波消耗电流脉冲为 20 mA ± 0.5mA；注意：其它的波形和幅度值也可以用来做为执行的选择，但是瞬间残留应在规范的边界之内：<100nA、<400ns、<400nA/s、总的电流不超过 55mA；在 4.00 ns ± 10 ns 的时间内电流尖峰为 95 mA ± 5 mA，频率随着一个 2 KHz 的异步序列而变化；终端输入电流分别为正常、最大和最小值。

测试流程：按下列流程执行：
a)发起一个冷复位激活V_{CC}。发送一个缺省的T =0的ATR，在最小5秒钟的时间内成功处理卡片和终端之间的一个命令序列。在整个命令过程中监控V_{cc}；
b)对于所有的温度、负载电流和电源电压下都重复上述测试。

通过标准：V_{cc}的范围应该为4.6V - εV ≤ V_{CC} ≤ 5.4V + εV（抖动为2.5ns）。

6.4 卡片操作过程测试（CZGC）

6.4.1 CZGC001-00 触点激活时序

测试目的：确保当卡片插入终端时，终端的触点根据预定的时序进行激活。

测试条件：正常温度、最低温度、最高温度；测试开始前卡片应拔出终端；负载电流：I_{CC}=2mA 和 54mA（±1mA）。

测试流程：按下列流程执行：
a)发起一个冷复位启动触点激活时序；
b)在V_{CC}≥0.4V（t_{P1}）之前监控V_{RST}，V_{CLK}和$V_{I/O}$至少1ms；
c)监控V_{RST}，V_{CLK}和$V_{I/O}$从V_{c}c≥0.4V直到V_{cc}≥4.6V（t_{P2}）；
d)监控V_{CC}，V_{RST}和$V_{I/O}$从V_{CC}≥4.6V直到V_{CLK} ≥0.4V（tP3）（对于第一个跳变）；

e)从V_{CLK} ≥4.6V（t_{P4}）（对于第一个跳变）开始监控VCC ，VRST 和 $V_{I/O}$ 200个CLK时间长度（+1%）（在 t_{S1}结束）；

f)从 t_{S1} 到 V_{RST} 0.4V（t_{P5}）监控V_{CC}和 $V_{I/O}$；

g)对于所有负载电流都重复上述测试 10 次。

通过标准：对于 t_{P1} 0V − εV ≤V_{RST} ≤0.4V + εV，0V − εV ≤V_{CLK} ≤0.4V + εV，0V − εV ≤$V_{I/O}$ ≤0.4V + εV。对于 t_{P2} 0V − εV ≤V_{RST} ≤0.4V + εV，0V − εV ≤V_{CLK} ≤0.4V + εV，0V − εV ≤ $V_{I/O}$ ≤V_{CC} + εV 。对于 t_{P3} 4.6V − εV ≤V_{CC} ≤5.4V + εV，0V − εV ≤ V_{RST} ≤0.4V + εV，0V − εV ≤$V_{I/O}$ ≤V_{CC} + εV。对于 t_{P4} 4.6V − εV ≤V_{CC} ≤5.4V + εV，0V − εV ≤ V_{RST} ≤ 0.4V + εV，0V − εV ≤$V_{I/O}$ ≤V_{CC} + εV，4.6V + εV ≤V_{CLK} ≤0.4V − εV 。对于 t_{P5} 4.6V − εV ≤V_{CC} ≤5.4V + εV（0.8 x V_{CC}）− εV ≤$V_{I/O}$ ≤V_{CC} + εV，4.6V + εV ≤V_{CLK} ≤0.4V − εV。

6.4.2 CZGC002-00 触点释放时序

测试目的：确保终端触点的释放时序符合规范要求。

测试条件：正常温度、最低温度、最高温度；负载电流：I_{CC}=2mA 和 54mA（±1mA）。

测试流程：按下列流程执行：

a)发起一个冷复位，不返回ATR发起触点释放时序；

b)测量从V_{RST} ≤ 0.4V 到 V_{CC}≤0.4V （t_{P1}）的时间段；

c)监控 V_{RST} 从 V_{RST}≤ 0.4V 到 V_{CC}≤4.6V（t_{P2}）；

d)监控V_{CLK}， V_{RST} 和 $V_{I/O}$ 从V_{CC} ≤4.6V 到 V_{CC}≤0.4V（t_{P3}）；

e)监控V_{CC}， V_{CLK}， V_{RST} 和 $V_{I/O}$ 从 V_{CC}≤ 0.4V 持续100ms（t_{P4}）；

f)对于所有的温度和负载电流下都重复上述测试。

通过标准：t_{P1} ≤ 100ms + εs。对于 t_{P2} 0V − εV ≤V_{RST} ≤0.4V + εV。对于 t_{P3} 0V − εV ≤V_{CLK} ≤0.4V + εV，0V − εV ≤ V_{RST} ≤0.4V + εV 和 0V − εV ≤$V_{I/O}$ ≤ (V_{CC} + 0.25V) + εV。对于 t_{P4} 0 V − εV ≤V_{CC} ≤0.4V + εV，0V − εV ≤V_{CLK} ≤0.4V + εV，0V − εV ≤V_{RST} ≤ 0.4V + εV ；0V − εV ≤$V_{I/O}$ ≤0.4V + εV。

6.4.3 CZGC003-00 冷复位

测试目的：确保在卡片冷复位的时间内，终端能够按照规范要求正确驱动 RST 线。确保如果终端收到 ATR 能够正确响应。

测试条件：正常温度、最高温度。

测试流程：按下列流程执行：

a)发起一个冷复位，启动触点激活时序；

b)测量从CLK上升沿到RST上升沿之间的时间间隔t_{P1}；

c)在RST上升沿400CLK（±10s）之后返回一个T=0的ATR，并在卡片和终端之间完成一个命令序列；

d)在 RST 上升沿 40，000CLK（±10s）之后返回一个 T=0 的 ATR，重复上述测试；

e)重复 10 次上述测试。

通过标准：40,000 ≤t_{P1} ≤ 45,000时钟周期。在默认的ATR之后，终端应能够正确处理命令序列。

6.4.4 CZGC004-00 热复位

测试目的：确保在卡片热复位的时间内，终端能够按照规范要求正确驱动 RST 线。确保如果终端收到 ATR 能够正确响应。

测试条件：正常温度、最高温度。

测试流程：按下列流程执行：

a)发起一个热复位；

b)测量从RST下降沿到RST上升沿之间的时间间隔t_{P1}；

c)在t_{P1}时间段内监控V_{CC}和CLK；
d)在t_{P1}期间小于200个时钟周期（±10s）（t_{P2}）监控I/O；
e)在RST上升沿400CLK（±10 s）之后返回一个T=0的ATR，并在卡片和终端之间完成一个命令序列；
f)在RST上升沿40，000CLK（±10 s）之后返回一个T=0的ATR，重复上述测试；
g)重复10次上述测试。

通过标准：40,000 ≤ t_{P1} ≤45,000 CLK周期。对于t_{P1} 4.6V - εV ≤V_{CC} ≤5.4V + εV，并且CLK处在激活状态（±εV）。对于t_{P2} (0.8 x V_{CC}) - εV ≤ $V_{I/0}$ ≤ V_{CC} + εV。在缺省的ATR之后，终端应能够正确处理命令序列。

6.5 复位应答（FWYD）

6.5.1 FWYD001-00 在 ATR 中返回最小的有效字符间隔

测试目的：确保卡片返回的 ATR 字符间隔为 11.8 个初始 etu 时，终端应能够正确接收和解释。

测试条件：正常温度、最高温度；卡片返回 ATR 的字符间隔恰好或者稍大于 11.8 个初始 etu。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 FE — — — — — — — — — — — —。

通过标准：终端能够接受 ATR 并且能够继续交易。

6.5.2 FWYD002-00 在 ATR 中返回最大的有效字符间隔

测试目的：确保卡片返回的 ATR 字符间隔为 10，080 个初始 etu 时，终端应能够正确接收和解释。

测试条件：正常温度、最高温度；卡片返回 ATR 的字符间隔为：
——T0 和 TB1 之间的字符间隔恰好或者略小于 10，080 个初始 etu；
——TB1 和 TC1 之间的字符间隔恰好或者略小于 9，108 个初始 etu；
其它字符间隔都是 12 个初始 etu。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 FE — — — — — — — — — — — —。

通过标准：终端能够接受 ATR 并且能够继续交易。

6.5.3 FWYD003-00 ATR 全局期望时间 — 冷复位

测试目的：确保当卡片在冷复位中 20，160 个初始 etu 内返回 ATR，终端应能够正确接收和解释。

测试条件：正常温度、最高温度；卡片返回 ATR 中 TS 后的所有字符总的时间长度等于或稍小于 20，160 个初始 etu。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 80 — — — — — — — — — — — —。

通过标准：终端能够接受 ATR 并且能够继续交易。

6.5.4 FWYD004-00 ATR 全局期望时间 — 热复位

测试目的：确保当卡片在热复位中 20，160 个初始 etu 内返回 ATR，终端应能够正确接收和解释。

测试条件：正常温度、最高温度；一个适当的 ATR 导致终端发出一个热复位，卡片返回热复位 ATR 中 TS 后的所有字符总的时间长度等于或稍小于 20，160 个初始 etu。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 80 — — — — — — — — — — — —。

通过标准：终端能够接受 ATR 并且能够继续交易。

6.5.5 FWYD005-xy 在特殊模式下，当 TA1 = ‘11’，TA1 = ‘12’和 TA1 = ‘13’时的 etu 的测量 — 冷复位

测试目的：确保当卡片在特殊模式下冷复位中返回 ATR 中 TA1 = ‘11’，TA1 = ‘12’ 和 TA1 = ‘13’（并且 TA2 的位 8= ‘0’或 ‘1’）时，终端应能够正确接收和解释。

测试条件：正常温度、最高温度；卡片返回 ATR 中 T0 的位 5 = ‘1’，并且 TA1 为特定值；对所有的模式和协议的冷复位进行测试：

——y=0：T=0；正向约定；

——y=1：T=0；反向约定；

——y=2：T=1；正向约定；

——y=3：T=1；反向约定；

对于 3 种 TA1 的值进行测试：

——x=0：TA1 = ‘11’（D=1）且 TA2 位 8= ‘1’当前 etu =372/f 秒；

——x=1：TA1 = ‘12’（D=2）且 TA2 位 8= ‘1’当前 etu =186/f 秒；

——x=2：TA1 = ‘13’（D=4）且 TA2 位 8= ‘1’当前 etu =93/f 秒；

——x=3：TA1 = ‘11’（D=1）且 TA2 位 8= ‘0’当前 etu =372/f 秒；

——x=4：TA1 = ‘12’（D=2）且 TA2 位 8= ‘0’当前 etu =186/f 秒；

——x=5：TA1 = ‘13’（D=4）且 TA2 位 8= ‘0’当前 etu =93/f 秒。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B F0 11 00 00 10 80 — — — — — — — — — — —；

——xy=01 3F F0 11 00 00 10 80 — — — — — — — — — — —；

——xy=02 3B F0 11 00 00 91 81 — — 61 — 01 00 — — — — 91；

——xy=03 3F F0 11 00 00 91 81 — — 61 — 01 00 — — — — 91；

——xy=10 3B F0 12 00 00 10 80 — — — — — — — — — — —；

——xy=11 3F F0 12 00 00 10 80 — — — — — — — — — — —；

——xy=12 3B F0 12 00 00 91 81 — — 61 — 01 00 — — — — 92；

——xy=13 3F F0 12 00 00 91 81 — — 61 — 01 00 — — — — 92；

——xy=20 3B F0 13 00 00 10 80 — — — — — — — — — — —；

——xy=21 3F F0 13 00 00 10 80 — — — — — — — — — — —；

——xy=22 3B F0 13 00 00 91 81 — — 61 — 01 00 — — — — 93；

——xy=23 3F F0 13 00 00 91 81 — — 61 — 01 00 — — — — 93；

——xy=30 3B F0 11 00 00 10 00 — — — — — — — — — — —；

——xy=31 3F F0 11 00 00 10 00 — — — — — — — — — — —；

——xy=32 3B F0 11 00 00 91 01 — — 61 — 01 00 — — — — 91；

——xy=33 3F F0 11 00 00 91 01 — — 61 — 01 00 — — — — 91；

——xy=40 3B F0 12 00 00 10 00 — — — — — — — — — — —；

——xy=41 3F F0 12 00 00 10 00 — — — — — — — — — — —；

——xy=42 3B F0 12 00 00 91 01 — — 61 — 01 00 — — — — 92；

——xy=43 3F F0 12 00 00 91 01 — — 61 — 01 00 — — — — 92；

——xy=50 3B F0 13 00 00 10 00 — — — — — — — — — — —；

——xy=51 3F F0 13 00 00 10 00 — — — — — — — — — — —；

——xy=52 3B F0 13 00 00 91 01 — — 61 — 01 00 — — — — 93；

——xy=53 3F F0 13 00 00 91 01 — — 61 — 01 00 — — — — 93。

通过标准：终端能够接受冷复位的 ATR 并且能够使用正确的当前 etu 值（F/Df）-继续交易。

6.5.6 FWYD006-xy 在特殊模式下，当 TA1 = ‘11’，TA1 = ‘12’ 和 TA1 = ‘13’ 时 etu 的测量 — 热复位

测试目的：确保当卡片在特殊模式下热复位中返回 ATR 中 TA1 = ‘11’，TA1 = ‘12’ 和 TA1 = ‘13’ 时，终端应能够正确接收和解释。

测试条件：正常温度、最高温度；卡片返回 ATR 中 T0 中位 5 = ‘1’，并且 TA1 为特定值；对所有的模式和协议的冷复位进行测试：

——y=0：T=0；正向约定；

——y=1：T=0；反向约定；

——y=2：T=1；正向约定；

——y=3：T=1；反向约定；

对于 3 种 TA1 的值进行测试：

——x=0：TA1 = ‘11’（D=1）；当前 etu =372/f 秒；

——x=1：TA1 = ‘12’（D=2）；当前 etu =186/f 秒；

——x=2：TA1 = ‘13’（D=4）；当前 etu =93/f 秒。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B F0 11 00 00 10 80 — — — — — — — — — — —；

——xy=01 3F F0 11 00 00 10 80 — — — — — — — — — — —；

——xy=02 3B F0 11 00 00 91 81 — — 61 — 01 00 — — — — 91；

——xy=03 3F F0 11 00 00 91 81 — — 61 — 01 00 — — — — 91；

——xy=10 3B F0 12 00 00 10 80 — — — — — — — — — — —；

——xy=11 3F F0 12 00 00 10 80 — — — — — — — — — — —；

——xy=12 3B F0 12 00 00 91 81 — — 61 — 01 00 — — — — 92；

——xy=13 3F F0 12 00 00 91 81 — — 61 — 01 00 — — — — 92；

——xy=20 3B F0 13 00 00 10 80 — — — — — — — — — — —；

——xy=21 3F F0 13 00 00 10 80 — — — — — — — — — — —；

——xy=22 3B F0 13 00 00 91 81 — — 61 — 01 00 — — — — 93；

——xy=23 3F F0 13 00 00 91 81 — — 61 — 01 00 — — — — 93。

通过标准：终端能够接受热复位的 ATR 并且能够使用正确的当前 etu 值（F/Df）继续交易。

6.5.7 FWYD007-xy 在协商模式下，当 TA1 = ‘11’，TA1 = ‘12’和 TA1 = ‘13’ 时 etu 的测量 — 冷复位

测试目的：确保当卡片在协商模式下冷复位中返回 ATR 中 TA1 = ‘11’，TA1 = ‘12’ 和 TA1 = ‘13’ 时，终端应能够正确接收和解释。

测试条件：正常温度、最高温度；卡片返回 ATR 中 T0 中位 5 = ‘1’，并且 TA1 为特定值；对所有的协议的冷复位进行测试：

——y=0：T=0；

——y=1：T=1；

对于 3 种 TA1 的值进行测试：

——x=0：TA1 = ‘11’ （D=1）；当前 etu =初始 etu；

——x=1：TA1 = ‘12’ （D=2）；当前 etu =初始 etu；

——x=2：TA1 = ‘13’ （D=4）；当前 etu =初始 etu。

对于每个 ATR 都不返回 TA2。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B 70 11 00 00 — — — — — — — — — — — —；

——xy=01 3B F0 11 00 00 81 — — — 31 20 01 — — — — — 70；

——xy=10 3B 70 12 00 00 — — — — — — — — — — — —；

——xy=11 3B F0 12 00 00 81 — — — 31 20 01 — — — — — 73；

——xy=20 3B 70 13 00 00 — — — — — — — — — — — —；

——xy=21 3B F0 13 00 00 81 — — — 31 20 01 — — — — — 72。

通过标准：终端应接受这个冷复位的 ATR，并且使用与初始 etu 相同的当前 etu 完成卡

片交易。对于 x=1 和 x=2 的子案例，如果终端支持参数协商的私有技术，允许其在接收到 ATR 后，发送一个 PPS 请求块（以‘FF’开始，长度为 3 到 6 个字节）。

6.5.8 FWYD008-xy 在协商模式下，当 TA1 =‘11’，TA1 =‘12’和 TA1 =‘13’ 时 etu 的测量 — 热复位

测试目的：确保当卡片在协商模式下热复位中返回 ATR 中 TA1 =‘11’，TA1 =‘12’和 TA1 =‘13’时，终端应能够正确接收和解释。

测试条件：正常温度、最高温度；一个适当的 ATR 导致终端执行一个热复位；对所有的协议的热复位进行测试：

——y=0：T=0；

——y=1：T=1；

对于 3 种 TA1 的值进行测试：

——x=0：TA1 =‘11’（D=1）；当前 etu =初始 etu；

——x=1：TA1 =‘12’（D=2）；当前 etu =初始 etu；

——x=2：TA1 =‘13’（D=4）；当前 etu =初始 etu；

对于每个 ATR 都不返回 TA2。

ATR：	TS	T0	TA1	TB1	TC1	TD1	TA2	TB2	TC2	TD2	TA3	TB3	TC3	TD3	TA4	TB4	TC4	TCK。
——xy=00	3B	70	11	00	00	—	—	—	—	—	—	—	—	—	—	—	—	—；
——xy=01	3B	F0	11	00	00	81	—	—	—	31	20	01	—	—	—	—	—	70；
——xy=10	3B	70	12	00	00	—	—	—	—	—	—	—	—	—	—	—	—	—；
——xy=11	3B	F0	12	00	00	81	—	—	—	31	20	01	—	—	—	—	—	73；
——xy=20	3B	70	13	00	00	—	—	—	—	—	—	—	—	—	—	—	—	—；
——xy=21	3B	F0	13	00	00	81	—	—	—	31	20	01	—	—	—	—	—	72。

通过标准：终端应接受这个热复位的 ATR，并且使用与初始 etu 相同的当前 etu 完成卡片交易。注意：x=1 和 x=2 的子案例，如果终端支持参数协商的私有技术，允许其在接收到 ATR 后，发送一个 PPS 请求块（以‘FF’开始，长度为 3 到 6 个字节）。

6.5.9 FWYD009-0y 字符间隔的测量 — 支持的 TC1 值 — 冷复位 — T=0

测试目的：确保当 T=0 的冷复位中包含取值从‘00’到‘FF’的 TC1 时，终端应能够正确接收并解释。

测试条件：正常温度、最高温度；5 个冷复位测试案例：

——y=0：TC1 =‘00’：最小时间 =12 etus；

——y=1：TC1 =‘80’：最小时间 =140 etus；

——y=2：TC1 =‘F0’：最小时间 =252 etus；

——y=3：TC1 =‘FF’：最小时间 =12 etus；

——y=4：TC1 =‘FE’：最小时间 =266 etus；

注意：y=1 和 y=2，TC1 的值只是一个代表，‘00’< TC1 <‘FF’范围内的其它值都有可能。

ATR：	TS	T0	TA1	TB1	TC1	TD1	TA2	TB2	TC2	TD2	TA3	TB3	TC3	TD3	TA4	TB4	TC4	TCK。
——y =0	3B	60	—	00	00	—	—	—	—	—	—	—	—	—	—	—	—	—；
——y =1	3F	60	—	00	80	—	—	—	—	—	—	—	—	—	—	—	—	—；
——y =2	3B	60	—	00	F0	—	—	—	—	—	—	—	—	—	—	—	—	—；
——y =3	3F	60	—	00	FF	—	—	—	—	—	—	—	—	—	—	—	—	—；
——y =4	3B	60	—	00	FE	—	—	—	—	—	—	—	—	—	—	—	—	—。

通过标准：根据 TC1，终端应以大于或等于最小时间 12 到 266etu 的字符间隔完成交易。

6.5.10 FWYD010-0y 字符间隔的测量 — 支持的 TC1 值 — 冷复位 — T=1

测试目的：确保当 T=1 的冷复位中包含取值从‘1E’到‘FF’的 TC1 时，终端应能够正

确接收并解释 。

测试条件：正常温度、最高温度；3 个 T＝1 冷复位测试案例：

——y=0：TC1 = ‘00’：最小时间 =12 etus；

——y=1：TC1 = ‘1E’：最小时间 =42 etus；

——y=2：TC1 = ‘FF’：最小时间 =11 etus。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y =0 3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71；

——y =1 3B E0 — 00 1E 81 — — — 31 20 05 — — — — — 6B；

——y =2 3B E0 — 00 FF 81 — — — 31 20 01 — — — — — 8E。

通过标准：根据 TC1 对于 T＝1 协议，终端应以大于或等于最小时间 11 到 42etu 的字符间隔完成交易。

6.5.11 FWYD011-Oy 字符间隔测量 — 支持的 TC1 值 — 热复位 — T=0

测试目的：确保当 T=0 的热复位中包含取值从‘00’到‘FF’的 TC1 时，终端应能够正确接收并解释。

测试条件：正常温度、最高温度；热复位时返回一个适当的 ATR；5 个热复位测试案例：

——y=0：TC1 = ‘00’：最小时间 =12 etus；

——y=1：TC1 = ‘80’：最小时间 =140 etus；

——y=2：TC1 = ‘F0’：最小时间 =252 etus；

——y=3：TC1 = ‘FF’：最小时间 =12 etus；

——y=4：TC1 = ‘FE’：最小时间 =266 etus；

注意：y=1 和 y=2，TC1 的值只是一个代表，’00’ < TC1 < ’FF’范围内的其它值都有可能。

ATR： TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B 60 — 00 00 — — — — — — — — — — — — —；

——y=1 3B 60 — 00 80 — — — — — — — — — — — — —；

——y=2 3B 60 — 00 F0 — — — — — — — — — — — — —；

——y=3 3B 60 — 00 FF — — — — — — — — — — — — —；

——y=4 3B 60 — 00 FE — — — — — — — — — — — — —。

通过标准：根据 TC1，终端应以大于或等于最小时间 12 到 266etu 的字符间隔完成交易。

6.5.12 FWYD012-Oy 字符间隔测量 — 支持的 TC1 值 — 热复位 — T=1

测试目的：确保当 T=1 的热复位中包含取值从‘00’到‘FF’的 TC1 时，终端应能够正确接收并解释。

测试条件：正常温度、最高温度；热复位时返回一个适当的 ATR；3 个 T＝1 热复位测试案例：

——y=0：TC1 = ‘00’：最小时间=12 etus；

——y=1：TC1 = ‘1E’：最小时间=42 etus；

——y=2：TC1 = ‘FF’：最小时间=11 etus。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y =0 3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71；

——y =1 3B E0 — 00 1E 81 — — — 31 20 05 — — — — — 6B；

——y =2 3B E0 — 00 FF 81 — — — 31 20 01 — — — — — 8E。

通过标准：根据 TC1，对于 T＝1 协议，终端应以大于或等于最小时间 11 到 266etu 的字符间隔完成交易。

6.5.13 FWYD013-OO 字符间隔测量 — 缺省 TC1 值 — 冷复位 — T=0

测试目的：确保当 T=0 的冷复位中不包含 TC1 时，终端应能够正确接收并解释。

测试条件：正常温度、最高温度；卡片返回的冷复位中没有 TC1，T0 也指明 TC1 不存在。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 20 — 00 — — — — — — — — — — — — —。

通过标准：终端应继续卡片操作过程，其字符间隔大于或等于最小间隔 12etu。

6.5.14 FWYD014-00 字符间隔测量 — 缺省 TC1 —冷复位 — T=1

测试目的：确保当 T=1 的冷复位中不包含 TC1 时，终端应能够正确接收并解释。

测试条件：正常温度、最高温度；卡片返回的冷复位中没有 TC1，T0 也指明 TC1 不存在。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B A0 — 00 — 81 — — — 31 20 11 — — — — — 21。

通过标准：终端应继续卡片操作过程，其字符间隔大于或等于最小间隔 12etu。

6.5.15 FWYD015-00 字符间隔测量 — 缺省 TC1 — 热复位 — T=0

测试目的：确保当 T=0 的热复位中不包含 TC1 时，终端应能够正确接收并解释。

测试条件：正常温度、最高温度；卡片返回的冷复位中没有 TC1，T0 也指明 TC1 不存在。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 20 — 00 — — — — — — — — — — — — —。

通过标准：终端应继续卡片操作过程，其字符间隔大于或等于最小间隔 12etu。

6.5.16 FWYD016-00 字符间隔测量 —缺省 TC1 — 热复位 — T=1

测试目的：确保当 T=1 的热复位中不包含 TC1 时，终端应能够正确接收并解释。

测试条件：正常温度、最高温度；卡片返回的热复位中没有 TC1，T0 也指明 TC1 不存在。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B A0 — 00 — 81 — — — 31 20 11 — — — — — 21。

通过标准：终端应继续卡片操作过程，其字符间隔大于或等于最小间隔 12etu。

6.5.17 FWYD017-0y 冷复位后的一致性 — 基本 ATR

测试目的：确保终端能够正确接收和解释正向、反向约定和各种协议的基本 ATR。

测试条件：正常温度、最高温度；卡片返回指定的冷复位 ATR；5 个冷复位测试案例，见表 1 冷复位测试案例。

表1 冷复位测试案例

Y	协议	约定
0	T＝0	正向约定
1	T＝0	反向约定
2	T＝0	反向约定
3	T＝1	反向约定
4	T＝1	反向约定

注：ATR ’3B E0 00 00 81 31 20 01 71’ 在 FWYD010-00 （正向约定 - T=1）时测试。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y =0 3B 60 — 00 00 — — — — — — — — — — — —；

——y =1 3F 60 — 00 00 — — — — — — — — — — — —；

——y =2 3F 60 — 00 FE — — — — — — — — — — — —；

——y =3 3F E0 — 00 1E 81 — — — 31 10 05 — — — — — 5B；

——y =4 3F E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端应接受 ATR，并且按照正确的协议和约定进行后续交易。

6.5.18 FWYD018-0y 热复位后的一致性 — 基本 ATR

测试目的：确保终端能够正确接收和解释正向、反向约定和各种协议的基本 ATR。

测试条件：正常温度、最高温度；卡片返回指定的热复位 ATR；7 个热复位测试案例，见表 2 热复位测试案例。

表2 热复位测试案例

Y	协议	约定
0	T＝0	正向约定

1	T＝0	反向约定
2	T＝0	正向约定
3	T＝0	反向约定
4	T＝0	反向约定
5	T＝1	反向约定
6	T＝1	反向约定

注： ATR ’3B 00 00 81 31 20 01 71’ 在FWYD01200（正向约定 - T=1）时测试。

ATR： TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y =0 3B 60 — 00 00 — — — — — — — — — — — — —；

——y =1 3F 60 — 00 00 — — — — — — — — — — — — —；

——y =2 3B 60 — 01 00 — — — — — — — — — — — — —；

——y =3 3F 60 — 01 00 — — — — — — — — — — — — —；

——y =4 3F 60 — 00 FE — — — — — — — — — — — — —；

——y =5 3F E0 — 00 1E 81 — — — 31 10 05 — — — — — 5B；

——y =6 3F E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端应接受 ATR，并且按照正确的协议和约定进行后续交易。

6.5.19 FWYD019-0y ATR 比基本 ATR 长 — 冷复位

测试目的：确保终端能够正确接收并解释长度大于基本 ATR 的冷复位应答。

测试条件：正常温度、最高温度；该测试应该在所有协议的冷复位下进行：

——y =0：T=0；

——y =1：T=1；

这个 ATR 包含 PBOC2-0 规范中规定的所有可能的字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B FF 11 00 00 D0 80 — 0A F1 20 01 00 71 00 00 00 7A；

——y=1 3B FF 11 00 00 D1 81 — 0A F1 20 01 00 71 00 00 00 7A。

历史字节：FF，5A，A5，5A，A5，5A，A5，5A，A5，5A，A5，5A，A5，90，00。

通过标准：终端应接受这个 ATR 并且继续卡片交易。

6.5.20 FWYD020-0y ATR 比基本 ATR 长 — 热复位

测试目的：确保终端能够正确接收并解释长度大于基本 ATR 的热复位应答。

测试条件：正常温度、最高温度；该测试应该在所有协议的热复位下进行：

——y =0：T=0；

——y =1：T=1；

这个 ATR 包含 pboc2-0 规范中规定的所有可能的字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B FF 11 00 00 D0 80 — 0A F1 20 01 00 71 00 00 00 7A；

——y=1 3B FF 11 00 00 D1 81 — 0A F1 20 01 00 71 00 00 00 7A。

历史字节：FF，5A，A5，5A，A5，5A，A5，5A，A5，5A，A5，5A，A5，90，00。

通过标准：终端应接受这个 ATR 并且继续卡片交易。

6.5.21 FWYD021-0y 支持的 T0 值 — 冷复位

测试目的：确保终端能够接受冷复位中包含支持的 T0 值（假设返回值与接口字符和历史字节相一致）。

测试条件：正常温度、最高温度；卡片返回如下 T＝0 的冷复位 ATR：

——y =0：发送的 TD1，T0 的位 8 被置成‘1’；

卡片返回如下 T＝1 的冷复位 ATR：

——y =1：T0 位 5 和位 7 被设置成‘1’，TA1 和 TC1 存在；

——y =2：T0 位 7 被设置成‘0’，TC1 不存在。

——ATR ‘3B 60 00 00’在 FWYD009-00 中测试（T0＝‘60’）；

——ATR ‘3B 20 00’在FWYD013-00中测试（T0＝‘20’）；
——ATR ‘3B 70 11 00 00’在FWYD007-00中测试（T0＝‘70’）；
——ATR ‘3B E0 00 00 81 31 20 01 71在FWYD010-00中测试（T0＝‘E0’）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B E0 － 00 00 80 － － － 71 20 01 00 － － － － 30；
——y=1 3B F0 11 00 00 81 － － － 61 － 01 00 － － － － 00；
——y=2 3B A0 － 00 － 81 － － － 71 20 01 00 － － － － 71。

通过标准：终端应接受这个ATR并且继续卡片交易。

6.5.22 FWYD022-0y 支持的T0值 — 热复位

测试目的：确保终端能够接受冷复位中包含支持的T0值（假设返回值与接口字符和历史字节相一致）。

测试条件：正常温度、最高温度；ATR导致终端发起热复位，卡片返回如下T＝0的热复位ATR：
——y =0：发送的TD1 ，T0的位8被置成‘1’；
卡片返回如下T＝1的热复位ATR：
——y =1：T0 位5和位7被设置成‘1’，TA1和TC1存在；
——y =2：T0 位7被设置成‘0’，TC1不存在；
——ATR ‘3B 60 00 00’ 在FWYD011-00中测试（T0＝‘60’）；
——ATR ‘3B 20 00’在FWYD015-00中测试（T0＝‘20’）；
——ATR ‘3B F0 11 00 00 10 80’在FWYD006-00中测试（T0＝‘F0’）；
——ATR ‘3B E0 00 00 81 31 20 01 71在FWYD012-00中测试（T0＝‘E0’）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B E0 － 00 00 80 － － － 71 20 01 00 － － － － 30；
——y=1 3F F0 11 00 00 81 － － － 61 － 01 00 － － － － 00；
——y=2 3B A0－00 － 81 － － － 71 20 01 00 － － － － 71。

通过标准：终端应接受这个ATR并且继续卡片交易。

6.5.23 FWYD023-00 支持的TB1值，Vpp的测量 — 冷复位

测试目的：确保终端能够接受冷复位中包含支持的TB1值，并且不产生Vpp。

测试条件：正常温度、最高温度；卡片返回一个TB1＝‘00’的T＝1 ATR。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 － 00 00 81 － － － 31 20 01 － － － － － 71。

通过标准：终端应接受这个ATR并且继续卡片交易，不产生Vpp。

6.5.24 FWYD024-0y 支持的TB1值，Vpp测量 — 热复位

测试目的：确保终端能够接受热复位中包含支持的TB1值，并且不产生Vpp。

测试条件：正常温度、最高温度；一个适当的ATR导致终端发起热复位；4个热复位ATR测试案例：
——y=0：T=0：TB1为任意值；
——y=1：T=0：未发送TB1 ；
——y=2：T=1：TB1为任意值；
——y=3：T=1：未发送TB1。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y =0 3B 60 － A5 00 － － － － － － － － － － － －；
——y =1 3B 40 － － 00 － － － － － － － － － － － －；
——y =2 3B E0 － A5 00 81 － － － 31 20 01 － － － － － D4；
——y =3 3B C0 － － 00 81 － － － 31 20 01 － － － － － 51。

通过标准：终端应接受这个ATR并且继续卡片交易，不产生Vpp。

6.5.25 FWYD025-0y 支持的 TD1 值 — 冷复位

测试目的：确保终端能够接受冷复位中包含支持的 TD1 值。

测试条件：正常温度、最高温度；两个冷复位 ATR 测试案例：

——y =0：T=1，TD1 =‘81’ ，发送 TD2；

——y =1：T=1，TD1 =‘91’，发送 TA2 和 TD2；

——ATR ’3B E0 00 00 40 0A’ 在 FWYD027-00 中测试（TD1 =’40’）；

——ATR ’3B F0 11 00 00 10 80’ 在 FWYD005-00 中测试 （TD1 =’10’）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y =0 3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF；

——y =1 3B E0 — 00 00 91 81 — — 31 FE 01 — — — — — 3E。

通过标准：终端应接受这个 ATR 并且继续卡片交易。

6.5.26 FWYD026-0y 支持的 TD1 值 — 热复位

测试目的：确保终端能够接受热复位中包含支持的 TD1 值。

测试条件：正常温度、最高温度；一个适当的 ATR 导致终端发起热复位；三个热复位 ATR 测试案例：

——y =0：T=0，TD1 =‘10’，发送 TA2；

——y =1：T=1，TD1 =‘81’，发送 TD2；

——y =2：T=1，TD1 =‘91’，发送 TA2 和 TD2；

ATR ’3B E0 00 00 40 0A’ 在 FWYD028-00 中测试（TD1 =’40’）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y =0 3B E0 — 00 00 10 80 — — — — — — — — — — —；

——y =1 3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF；

——y =2 3B E0 — 00 00 91 81 — — 31 FE 01 — — — — — 3E。

通过标准：终端应接受这个 ATR 并且继续卡片交易。

6.5.27 FWYD027-00 支持的 TC2 值 — 冷复位

测试目的：确保终端能够接受冷复位中包含支持的 TC2 值。

测试条件：正常温度、最高温度；卡片发送 TC2＝‘0A’的 T＝0 ATR；

ATR‘3B 60 00 00 ’在FWYD009-00 中测试（TC2不存在’）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 40 — — 0A — — — — — — — — —。

通过标准：终端应接受这个 ATR 并且继续卡片交易。

6.5.28 FWYD028-00 支持的 TC2 值 — 热复位

测试目的：确保终端能够接受热复位中包含支持的 TC2 值。

测试条件：正常温度、最高温度；一个适当的 ATR 导致终端发起热复位，卡片发送 TC2＝‘0A’的 T＝0 热复位 ATR；

ATR‘3B 60 00 00’在 FWYD011-00 中测试（TC2 不存在）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 40 — — 0A — — — — — — — — — —。

通过标准：终端应接受这个 ATR 并且继续卡片交易。

6.5.29 FWYD029-00 支持的 TD2 值 — 冷复位

测试目的：确保终端能够接受冷复位中包含支持的 TD2 值。

测试条件：正常温度、最高温度；卡片发送的冷复位 ATR 中 TD2 的低半字节为‘E’（暗示 TD1 低半字节为‘0’）；

——ATR‘3B E0 00 00 81 31 20 01 71’在 FWYD010-00 中测试（TD2 =‘31’）；

——ATR‘3F F0 11 00 00 81 61 01 00 00’在 FWYD021-00 中测试 （TD2

='61'）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 80 — — — 0E — — — — — — — 6E。

通过标准：终端应接受这个 ATR 并且继续卡片交易。

6.5.30 FWYD030-00 支持的 TD2 — 热复位

测试目的：确保终端能够接受热复位中包含支持的 TD2 值。

测试条件：正常温度、最高温度；卡片发送的热复位 ATR 中 TD2 的低半字节为'E'（暗示 TD1 低半字节为'0'）；

——ATR'3B E0 00 00 81 31 20 01 71'在 FWYD012-00 中测试（TD2='31'）；

——ATR'3F F0 11 00 00 81 61 01 00 00'在 FWYD022-00 中测试（TD2='61'）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 80 — — — 0E — — — — — — — 6E。

通过标准：终端应接受这个 ATR 并且继续卡片交易。

6.5.31 FWYD031-00 缺省的 TA3 值 — 冷复位

测试目的：确保终端能够接受并解释不包含 TA3 的冷复位应答。

测试条件：正常温度、最高温度；卡片发送 T=1 的冷复位应答，无 TA3，与 TD2 中指示相一致。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 21 — 01 — — — — — 41。

通过标准：终端应在后续的有连接或者无连接的 I 块中使用 IFSI='20'（例如使用缺省的 TA3 值）继续卡片交易。

6.5.32 FWYD032-00 缺省的 TA3 值 — 热复位

测试目的：确保终端能够接受并解释不包含 TA3 的热复位应答。

测试条件：正常温度、最高温度；卡片返回一个适当的 ATR 导致终端发起热复位，卡片发送 T=1 的热复位应答，无 TA3，与 TD2 中指示相一致。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 21 — 01 — — — — — 41。

通过标准：终端应在后续的有连接或者无连接的 I 块中使用 IFSI='20'（例如使用缺省的 TA3 值）继续卡片交易。

6.5.33 FWYD033-0y 支持的 TB3 值 — 冷复位

测试目的：确保终端能够接受并解释包含 TB3 的冷复位应答。

测试条件：正常温度、最高温度；卡片发送 T=1 的冷复位应答；三个冷复位测试案例：

——y =0：2^{CWI} =32 ；N+1 =1；BWI =4；

——y =1：2^{CWI} =2 ；N+1 =1；BWI =4；

——y =2：2^{CWI} =32 ；N+1 =31；BWI =4。

注：上述列出的值只是一个代表，任何正确的TB3/TC1的联合都是有可能的。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 81 — — — 31 20 45 — — — — — 35；

——y=1 3B E0 — 00 00 81 — — — 31 20 41 — — — — — 31；

——y=2 3B E0 — 00 1E 81 — — — 31 20 45 — — — — — 2B。

通过标准：终端应接受 ATR 并继续卡片交易。

6.5.34 FWYD034-0y 支持的 TB3 值 — 热复位

测试目的：确保终端能够接受并解释包含 TB3 的热复位应答。

测试条件：正常温度、最高温度；一个适当的 ATR 导致终端发起热复位，卡片发送 T=

1 的热复位应答；三个热复位测试案例：

——y =0：2^{CWI} =32 ；N+1 =1； BWI =4；

——y =1：2^{CWI} =2 ；N+1 =1； BWI =4；

——y =2：2^{CWI} =32 ；N+1 =31； BWI =4。

注：上述列出的值只是一个代表，任何正确的TB3/TC1的联合都是有可能的。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 81 — — — 31 20 45 — — — — — 35；

——y=1 3B E0 — 00 00 81 — — — 31 20 41 — — — — — 31；

——y=2 3B E0 — 00 1E 81 — — — 31 20 45 — — — — — 2B。

通过标准：终端应接受 ATR 并继续卡片交易。

6.5.35 FWYD035-00 支持的 TC3 — 冷复位

测试目的：确保终端能够接受包含支持的 TC3 值的冷复位应答。

测试条件：正常温度、最高温度；卡片发送 T＝1 的冷复位应答 TC3＝‘00’；

ATR‘3B E0 00 00 81 31 20 01 71’在 FWYD010-00 中测试（不返回 TC3）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 70 20 01 00 — — — — 31。

通过标准：终端应接受 ATR 并继续卡片交易。

6.5.36 FWYD036-00 支持的 TC3 — 热复位

测试目的：确保终端能够接受包含支持的 TC3 值的热复位应答。

测试条件：正常温度、最高温度；卡片返回一个适当的 ATR，引起终端的热复位，然后，卡片发送一个 TC3＝‘00’的 T＝1 热复位 ATR；

ATR‘3B E0 00 00 81 31 20 01 71’在 FWYD012-00 中测试（不返回 TC3）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 70 20 01 00 — — — — 31。

通过标准：终端应接受 ATR 并继续卡片交易。

6.5.37 FWYD037-0y 冷、热复位使用不同的约定

测试目的：确保终端能够接受与冷复位不同的热复位约定。

测试条件：正常温度、最高温度，见表 3 协议约定。

表3 协议约定

Y	错误的冷复位ATR约定	正确的热复位ATR约定	使用协议
0	正向	反向	T=0
1	反向	正向	T=0
2	正向	反向	T=1
3	反向	正向	T=1

冷复位ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B 60 — 05 00 — — — — — — — — — — — —；

——y=1 3F 60 — 05 00 — — — — — — — — — — — —；

——y=2 3B E0 — 05 00 81 — — — 71 20 01 00 — — — — 34；

——y=3 3F E0 — 05 00 81 — — — 71 20 01 00 — — — — 34。

热复位ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B 60 — 05 00 — — — — — — — — — — — —；

——y=1 3F 60 — 05 00 — — — — — — — — — — — —；

——y=2 3F E0 — 00 00 81 — — — 71 20 01 00 — — — — 31；

——y=3 3B E0 — 00 00 81 — — — 71 20 01 00 — — — — 31。

通过标准：终端应接受热复位 ATR 并根据热复位 ATR 中表明的约定方式继续卡片交易。

6.5.38 FWYD038-00 ATR 全局时间超限 — 冷复位 （1）

测试目的：确保如果冷复位 ATR 的所有字符没有在 TS 后的 20160 个初始 etu 内收到，终端应该拒绝 IC 卡。

测试条件：正常温度、最高温度；卡片以接近字符间隔最大为 9600 个初始 etu 发送冷复位 ATR 的前三个字符（TS、T0 和 TB1），但是不发送 TC1。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端应在 TS 起始位开始的 24000（4800＋19200 初始 etu）个初始 etu 内发起下电时序。

6.5.39 FWYD039-00 ATR 全局时间超限 — 冷复位 （2）

测试目的：确保如果冷复位 ATR 的所有字符没有在 TS 后的 20160 个初始 etu 内收到，终端应该拒绝 IC 卡。

测试条件：默认环境条件；卡片在 TS 后的至少 20160＋1 个初始 etu 内发送完所有的冷复位 ATR 字符（卡片发送的字符间隔为最大值 9600 初始 etu）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端应在 TS 起始位开始的 24000（4800＋19200 初始 etu）个初始 etu 内发起下电时序。

6.5.40 FWYD040-00 ATR 全局时间超限 — 热复位 （1）

测试目的：确保如果热复位 ATR 的所有字符没有在 TS 后的 20160 个初始 etu 内收到，终端应该拒绝 IC 卡。

测试条件：正常温度、最高温度；一个适当的 ATR 使终端启动热复位，卡片以接近字符间隔最大为 9600 个初始 etu 发送热复位 ATR 的前三个字符(TS、T0 和 TB1)，但是不发送 TC1。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端应在 TS 起始位开始的 24000（4800＋19200 初始 etu）个初始 etu 内发起下电时序。

6.5.41 FWYD041-00 ATR 全局时间超限 — 热复位 （2）

测试目的：确保如果热复位 ATR 的所有字符没有在 TS 后的 20160 个初始 etu 内收到，终端应该拒绝 IC 卡。

测试条件：正常温度、最高温度；一个适当的 ATR 使终端启动热复位，卡片在发送 TS 后的至少 20160＋1 个初始 etu 内发送完所有的热复位 ATR 字符（卡片发送的字符间隔为最大值 9600 初始 etu）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端应在 TS 起始位开始的 24000（4800＋19200 初始 etu）个初始 etu 内发起下电时序。

6.5.42 FWYD042-00 ATR 超限最大字符间隔—冷复位 （1）

测试目的：确保如果冷复位 ATR 相邻字符间隔超过 10080 个初始 etu，终端应启动下电时序。

测试条件：正常温度、最高温度；卡片发送一个或几个冷复位 ATR 字符，然后不再发送其余的字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端应在冷复位 ATR 的 TS 起始位开始的 14400（4800＋9600）个初始 etu 内发起下电时序。

6.5.43 FWYD043-00 ATR 超限最大字符间隔—冷复位（2）

测试目的：确保如果卡片 ATR 的同向字符间隔超过 10080 个初始 etu，终端应该启动下电时序。

测试条件：正常温度、最高温度；卡片发送一个冷复位 ATR，T0 与 TB1 或者 TB1 与 TC1 之间的字符间隔为 10080＋1＝10081 个初始 etu（但是 ATR 的总时间是 19200 etu）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － － －。

通过标准：终端应在冷复位 ATR 的 TS 起始位开始的 14400（4800＋9600 初始 etu）个初始 etu 内发起下电时序。

6.5.44 FWYD044-00 ATR 超限最大字符间隔—热复位（1）

测试目的：确保如果热复位 ATR 相邻字符间隔超过 10080 个初始 etu，终端应启动下电时序。

测试条件：正常温度、最高温度；卡片发送一个或几个热复位 ATR 字符，然后不再发送其余的字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － － －。

通过标准：终端应在热复位 ATR 的 TS 起始位开始的 14400（4800＋9600）个初始 etu 内发起下电时序。

6.5.45 FWYD045-00 ATR 超限最大字符间隔－热复位（2）

测试目的：确保如果卡片 ATR 的同向字符间隔超过 10080 个初始 etu，终端应该启动下电时序。

测试条件：正常温度、最高温度；卡片发送一个热复位 ATR，T0 与 TB1 或者 TB1 与 TC1 之间的字符间隔为 10080＋1＝10081 个初始 etu(但是 ATR 的总时间是 19200 etu）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － － －。

通过标准：终端应在热复位 ATR 的 TS 起始位开始的 14400（4800＋9600 初始 etu）个初始 etu 内发起下电时序。

6.5.46 FWYD046-00 不正确的冷复位 ATR 发起延迟（1）

测试目的：确保如果卡片冷复位 ATR 发起延迟超过上限（超过 2000 个时钟周期），终端应拒绝 IC 卡。

测试条件：正常温度、最高温度；卡片不发送 ATR 字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － － －。

通过标准：终端应在RST拉高后的42000 clock + 50ms内发起下电时序。

6.5.47 FWYD047-00 不正确的冷复位 ATR 发起延迟 （2）

测试目的：确保如果卡片冷复位 ATR 发起延迟超过上限（超过 2000 个时钟周期），终端应拒绝 IC 卡。

测试条件：正常温度、最高温度；从 RST 拉高开始，卡片至少等待 42001 个时钟周期再发送 ATR 第一个字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端应在RST拉高后的42000 clock + 50ms内发起下电时序。

6.5.48 FWYD048-00 不正确的热复位 ATR 发起延迟 （1）

测试目的：确保如果卡片热复位 ATR 发起延迟超过上限（超过 2000 个时钟周期），终端应拒绝 IC 卡。

测试条件：正常温度、最高温度；卡片令终端发起热复位，但卡片不发送热复位 ATR 字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端应在RST拉高后的42000 clock + 50ms内发起下电时序。

6.5.49 FWYD049-00 不正确的热复位 ATR 发起延迟 （2）

测试目的：确保如果卡片热复位 ATR 发起延迟超过上限（超过 2000 个时钟周期），终端应拒绝 IC 卡。

测试条件：正常温度、最高温度；从 RST 拉高开始，卡片至少等待 42001 个时钟周期再发送 ATR 第一个字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端应在RST拉高后的42000 clock + 50ms内发起下电时序。

6.5.50 FWYD050-0y 无效的 ATR — 校验错误 — 冷复位

测试目的：确保如果卡片冷复位ATR中含有奇偶校验错误，终端应拒绝卡片。

测试条件：正常温度、最高温度；卡片发送如下 ATR，其中有一个字符的奇偶校验错误：

——y=0：T=0；

——y=1：T=1。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B 60 — 00 00 — — — — — — — — — — — —；
——y=1 3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF。

通过标准：终端应在冷复位ATR的TS字符起始位下降沿开始的24000个初始etu之内将RST置为低电平，启动下电时序。

6.5.51 FWYD051-0y 无效的 ATR — 校验错误 — 热复位

测试目的：确保如果卡片热复位ATR中含有奇偶校验错误，终端应拒绝卡片。

测试条件：正常温度、最高温度；卡片发送如下 ATR，其中有一个字符的奇偶校验错误：

——y=0：T=0；

——y=1：T=1。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B 60 — 00 00 — — — — — — — — — — — —；
——y=1 3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF。

通过标准：终端应在热复位ATR的TS字符起始位下降沿开始的24000个初始etu之内将RST置为低电平，启动下电时序。

6.5.52 FWYD052-0y 不正确的 TS — 冷复位

测试目的：确保如果卡片冷复位ATR中的TS不是‘3B’或者‘3F’，终端应拒绝卡片。

测试条件：正常温度、最高温度；根据 TS 的值有 4 个冷复位测试案例：

——y=0：（H）LHLHHHHLLH；

——y=1：（H）LHLHHHHLLL；

——y=2：（H）LHHLLLLHLL；

——y=3：（H）LHHLLLLHLH；

——y＝0 和 y＝1 对应的是正向约定没有/有奇偶校验错误的‘3D’；

——y＝2 和 y＝3 对应的是反向约定没有/有奇偶校验错误的‘3D’；

此外，如果 y＝0 在反向约定中被解释，它会导致一个奇偶校验错误，y＝2 时的正向约定也是如此。这就是为什么每一种约定都有两种校验位的值，用以确保 ATR 不会因为奇偶校验错误而被拒绝。

ATR： TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

y=0～3 3D 60 － 00 00 － － － － － － － － － － － － － －。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.53 FWYD053-0y 不正确的 TS — 热复位

测试目的：确保如果卡片热复位 ATR 中的 TS 不是‘3B’或者‘3F’，终端应拒绝卡片。

测试条件：正常温度、最高温度；根据 TS 的值有 4 个热复位测试案例：

——y=0：（H）LHLHHHHLLH；

——y=1：（H）LHLHHHHLLL；

——y=2：（H）LHHLLLLHLL；

——y=3：（H）LHHLLLLHLH；

——y＝0 和 y＝1 对应的是正向约定没有/有奇偶校验错误的‘3D’；

——y＝2 和 y＝3 对应的是反向约定没有/有奇偶校验错误的‘3D’；

此外，如果 y＝0 在反向约定中被解释，它会导致一个奇偶校验错误，y＝2 时的正向约定也是如此。这就是为什么每一种约定都有两种校验位的值，用以确保 ATR 不会因为奇偶校验错误而被拒绝。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

y=0～3 3D 60 － 00 00 － － － － － － － － － － － － －。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.54 FWYD054-0y ATR 中字符超限 — 冷复位

测试目的：确保如果卡片冷复位 ATR 中返回的数据与接口字符不一致或者不能表明接口字符，终端应拒绝卡片。

测试条件：正常温度、最高温度；卡片发送如下 T＝0 的 ATR：

——y =0：T0 位 6 =0，位 7 =1：发送 TB1 和 TC1；

——y =1：T0 位 6 =1，位 7 =0：发送 TB1 和 TC1；

T0 与同时具备 TB1 和 TC1 有冲突；如果终端一收到 T0 或者 TDi 中所表明的所有字符就终止卡片交易时，测试案例：y＝0 和 y＝1 才能执行。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B 40 － 00 00 － － － － － － － － － － － － －；

——y=1 3B 20 － 00 00 － － － － － － － － － － － － －。

通过标准：终端应在收到 T0 后，TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.55 FWYD055-0y ATR 中字符超限 — 热复位

测试目的：确保如果卡片热复位 ATR 中返回的数据与接口字符不一致或者不能表明接口字符，终端应拒绝卡片。

测试条件：正常温度、最高温度；一个适当的 ATR 导致终端发起热复位；卡片发送如下 T＝0 的热复位 ATR：

——y =0：T0 位 6 =‘0’，位 7 =‘1’：发送 TB1 和 TC1；

——y =1：T0 位 6 =‘1’，位 7 =‘0’：发送 TB1 和 TC1；

T0 与 TB1 和 TC1 的实际存在有冲突；如果终端一收到 T0 或者 TDi 中所表明

的所有字符就终止卡片交易时，测试案例 y＝0 和 y＝1 才能执行。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B 40 － 00 00 － － － － － － － － － － － － －；

——y=1 3B 20 － 00 00 － － － － － － － － － － － － －。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.56 FWYD056-Oy 特定模式下不支持的 TA1 — 冷复位

测试目的：确保终端拒绝 TA1 的值超出‘11’到‘13’的特定模式下的冷复位 ATR。

测试条件：正常温度、最高温度；该案例只在终端不支持超出‘11’到‘13’范围的 TA1 并且支持 TA2 的情况下才被执行；针对两种不同的协议测试冷复位 ATR：

——y =0：T＝0（T0 的位 5＝‘1’，TA1 值超出‘11’到‘13’，返回 TA2）；

——y =1：T＝1（T0 的位 5＝‘1’，TA1 值超出‘11’到‘13’，返回 TA2）；

TS 与同时具备 TB1 和 TC1 有冲突；如果终端一收到 T0 或者 TDi 中所表明的所有字符就终止卡片交易时，测试案例 y＝0 和 y＝1 才能执行。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B F0 D6 00 00 10 00 － － － － － － － － － － －；

——y=1 3B F0 D6 00 00 91 01 － － 31 40 01 － － － － － C6。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.57 FWYD057-Oy 特定模式下不支持的 TA1 — 热复位

测试目的：确保终端拒绝 TA1 的值超出‘11’到‘13’的特定模式下的热复位 ATR。

测试条件：正常温度、最高温度；该案例只在终端不支持超出‘11’到‘13’范围的 TA1 并且支持 TA2 的情况下才被执行；针对两种不同的协议测试冷复位 ATR：

——y =0：T＝0（T0 的位 5＝‘1’，TA1 值超出‘11’到‘13’，返回 TA2）；

——y =1：T＝1（T0 的位 5＝‘1’，TA1 值超出‘11’到‘13’，返回 TA2）；

TS 与同时具备 TB1 和 TC1 有冲突；如果终端一收到 T0 或者 TDi 中所表明的所有字符就终止卡片交易时，测试案例 y＝0 和 y＝1 才能执行。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B F0 D6 00 00 10 00 － － － － － － － － － － －；

——y=1 3B F0 D6 00 00 91 01 － － 31 40 01 － － － － － C6。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.58 FWYD058-Oy 不支持的 TB1 — 冷复位

测试目的：确保终端拒绝包含有不支持的 TB1 的冷复位 ATR。

测试条件：正常温度、最高温度；4 个冷复位测试案例：

——y=0：T=0：TB1≠‘00’；

——y=1：T=0：TB1 不存在；

——y=2：T=1：TB1≠‘00’；

——y=3：T=1：TB1 不存在。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B 60 － 05 00 － － － － － － － － － － － － －；

——y=1 3B 40 － － 00 － － － － － － － － － － － － －；

——y=2 3B E0 － 10 00 81 － － － 31 20 01 － － － － － 61；

——y=3 3B C0 － － 00 81 － － － 31 20 01 － － － － － 51。

通过标准：终端应在收到 T0 后，TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.59 FWYD059-Oy 不支持的 TD1 — 冷复位

测试目的：确保终端拒绝包含有不支持的 TD1 的冷复位 ATR。

测试条件：正常温度、最高温度；2 个冷复位测试案例：

——y=0：T=0：半位为‘E’；

——y=1：T=0：半位不是‘0’、‘1’或者‘E’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 0E — — — — — — — — — — — EE；

——y=1 3F E0 — 00 00 04 — — — — — — — — — — — E4。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.60 FWYD060-Oy 不支持的 TD1 — 热复位

测试目的：确保终端拒绝包含有不支持的 TD1 的热复位 ATR。

测试条件：正常温度、最高温度；一个适当的 ATR 引起终端发起热复位，2 个热复位测试案例：

——y=0：T=0：低半字节为‘E’；

——y=1：T=0：低半字节不是‘0’、‘1’或者‘E’；

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 0E — — — — — — — — — — — EE；

——y=1 3F E0 — 00 00 04 — — — — — — — — — — — E4。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.61 FWYD061-OO 不支持的 TA2 — 冷复位

测试目的：确保终端拒绝包含有不支持的 TA2 的冷复位 ATR。

测试条件：正常温度、最高温度；TD1 表明 TA2 存在，但是 TA2 的位 5 等于‘1’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 10 10 — — — — — — — — — — —。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.62 FWYD062-Oy 特定模式下不支持的 TA1 — 冷复位

测试目的：确保终端拒绝包含 TA1 的值为‘11’、‘12’和‘13’之外的值的 ATR（除非终端支持值为‘11’、‘12’和‘13’之外的 TA1）。

测试条件：正常温度、最高温度；这项测试仅在支持值为‘11’、‘12’和‘13’之外的 TA1 且支持 TA2 的终端上执行；测试在两种协议下进行：

——y=0：T=0（T0 位 5=‘1’，TA1 为‘11’、‘12’和‘13’之外的值且返回的 TA2 位 8=‘0’）；

——y=1：T=1（T0 位 5=‘1’，TA1 为‘11’、‘12’和‘13’之外的值且返回的 TA2 位 8=‘0’）；

——y=2：T=0（T0 位 5=‘1’，TA1 为‘11’、‘12’和‘13’之外的值且返回的 TA2 位 8=‘1’）；

——y=3：T=1（T0 位 5=‘1’，TA1 为‘11’、‘12’和‘13’之外的值且返回的 TA2 位 8=‘1’）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B F0 D6 00 00 10 00 — — — — — — — — — —；

——y=1 3B F0 D6 00 00 91 01 — — 31 40 01 — — — — — C6；

——y=2 3B F0 D6 00 00 10 80 — — — — — — — — — —；

——y=3 3B F0 D6 00 00 91 81 — — 31 40 01 — — — — — 46。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位时序。

6.5.63 FWYD063-00 TB2 不匹配 — 冷复位

测试目的：确保终端拒绝包含 TB2 的冷复位 ATR。

测试条件：正常温度、最高温度；在冷复位 ATR 中 TD1 表明 TB2 存在（位 6＝‘1’），并且返回 TB2。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 A1 — 00 — 31 20 01 — — — — — 51。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.64 FWYD064-00 TB2 不匹配 — 热复位

测试目的：确保终端拒绝包含 TB2 的热复位 ATR。

测试条件：正常温度、最高温度；一个适当的 ATR 使得终端发起热复位；在热复位 ATR 中 TD1 表明 TB2 存在（位 6＝‘1’），并且返回 TB2。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 A1 — 00 — 31 20 01 — — — — — 51。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.65 FWYD065-0y 不支持的 TC2 — 冷复位

测试目的：确保终端拒绝包含不支持的 TC2 值的冷复位 ATR。

测试条件：正常温度、最高温度；4 个冷复位 ATR 测试案例：

——y=0：TC2 =‘00’；

——y=1：TC2 >‘0A’；

测试案例 y=2 和 y=3（取值范围‘01’ 到‘09’），根据 ICS 文档执行。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 — 00 00 40 — — 00 — — — — — — — — —；

——y＝1 3B E0 — 00 00 40 — — 0B — — — — — — — — —；

——y＝2 3B E0 — 00 00 40 — — 01 — — — — — — — — —；

——y＝3 3B E0 — 00 00 40 — — 09 — — — — — — — — —。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.66 FWYD066-0y 不支持的 TC2 — 热复位

测试目的：确保终端拒绝包含不支持的 TC2 值的热复位 ATR。

测试条件：正常温度、最高温度；一个适当的 ATR 使得终端发起热复位；4 个热复位 ATR 测试案例：

——y=0：TC2 =‘00’；

——y=1：TC2 >‘0A’；

测试案例 y=2 和 y=3（取值范围‘01’ 到‘09’） 根据 ICS 文档执行。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 — 00 00 40 — — 00 — — — — — — — — —；

——y＝1 3B E0 — 00 00 40 — — 0B — — — — — — — — —；

——y＝2 3B E0 — 00 00 40 — — 01 — — — — — — — — —；

——y＝3 3B E0 — 00 00 40 — — 09 — — — — — — — — —。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.67 FWYD067-0y 不支持的 TD2 — 冷复位

测试目的：确保终端拒绝包含不支持的 TD2 值（低字节）的冷复位 ATR。

测试条件：正常温度、最高温度；3 个冷复位 ATR 测试案例：

——y=0：低字节＝‘0’；

——y=1：低字节＝‘E’，并且 TD1 的低字节＝‘1’；

——y=2：低字节＝‘F’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 — 00 00 81 — — — 20 — 01 — — — — — 40；

——y＝1 3B E0 — 00 00 81 — — — 2E — 01 — — — — — 4E；

——y＝2 3B E0 — 00 00 81 — — — 2F — 01 — — — — — 4F。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.68 FWYD068-0y 不支持的 TD2 — 热复位

测试目的：确保终端拒绝包含不支持的 TD2 值（低字节）的热复位 ATR。

测试条件：正常温度、最高温度；一个适当的 ATR 使得终端发起热复位；3 个热复位 ATR 测试案例：

——y=0：低字节＝‘0’；

——y=1：低字节＝‘E’，并且 TD1 的低字节＝‘1’；

——y=2：低字节＝‘F’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 — 00 00 81 — — — 20 — 01 — — — — — 40；

——y＝1 3B E0 — 00 00 81 — — — 2E — 01 — — — — — 4E；

——y＝2 3F E0 — 00 00 81 — — — 2F — 01 — — — — — 4F。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.69 FWYD069-0y 不支持的 TA3 — 冷复位

测试目的：确保终端拒绝包含不支持的 TA3 值的冷复位 ATR。

测试条件：正常温度、最高温度；卡片发送一个 TA3 值错误的 ATR（T＝1）； 3 个冷复位 ATR 测试案例：

——y=0：TA3 =‘FF’；

——y=1：TA3 =‘00’；

——y=2：TA3 =‘0F’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK

——y＝0 3B E0 — 00 00 81 — — — 31 FF 01 — — — — — AE；

——y＝1 3B E0 — 00 00 81 — — — 31 00 01 — — — — — 51；

——y＝2 3B E0 — 00 00 81 — — — 31 0F 01 — — — — — 5E。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.70 FWYD070-0y 不支持的 TA3 — 热复位

测试目的：确保终端拒绝包含不支持的 TA3 值的热复位 ATR。

测试条件：正常温度、最高温度；一个适当的冷复位 ATR 使得终端发起热复位；卡片发送一个 TA3 值错误的 ATR （T＝1）；3 个热复位 ATR 测试案例：

——y=0：TA3 =‘FF’；

——y=1：TA3 =‘00’；

——y=2：TA3 =‘0F’；

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 － 00 00 81 － － － 31 FF 01 － － － － － AE；

——y＝1 3B E0 － 00 00 81 － － － 31 00 01 － － － － － 51；

——y＝2 3B E0 － 00 00 81 － － － 31 0F 01 － － － － － 5E。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.71 FWYD071-Oy 不支持的 TB3 — 冷复位

测试目的：确保终端拒绝包含不支持的 TB3 值的冷复位 ATR。

测试条件：正常温度、最高温度；卡片发送一个 T＝1 的冷复位 ATR；4 个冷复位 ATR 测试案例：

——y=0：TB3 不存在；

——y=1：BWI ＞ 4；

——y=2：CWI ＞ 5；

——y=3：CWI 为 2CWI =N+1。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 － 00 00 81 － － － 11 40 － － － － － － 30；

——y＝1 3B E0 － 00 00 81 － － － 31 40 51 － － － － － 41；

——y＝2 3B E0 － 00 00 81 － － － 31 40 06 － － － － － 16；

——y＝3 3B E0 － 00 00 81 － － － 31 40 00 － － － － － 10。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动热复位。

6.5.72 FWYD072-Oy 不支持的 TB3 — 热复位

测试目的：确保终端拒绝包含不支持的 TB3 值的热复位 ATR。

测试条件：正常温度、最高温度；一个适当的 ATR 使得终端发起热复位，之后卡片发送一个 T＝1 的热复位 ATR；4 个热复位 ATR 测试案例：

——y=0：TB3 不存在；

——y=1：BWI ＞ 4；

——y=2：CWI ＞ 5；

——y=3：CWI 为 2^{CWI}=N+1；

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 － 00 00 81 － － － 11 40 － － － － － － 30；

——y＝1 3B E0 － 00 00 81 － － － 31 40 51 － － － － － 41；

——y＝2 3B E0 － 00 00 81 － － － 31 40 06 － － － － － 16；

——y＝3 3B E0 － 00 00 81 － － － 31 40 00 － － － － － 10。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.73 FWYD073-Oy 不支持的 TC3 — 冷复位

测试目的：确保终端拒绝包含不支持的 TC3 值的冷复位 ATR。

测试条件：正常温度、最高温度；2 个冷复位 ATR 测试案例：

——y=0：TC3 =‘FF’；

——y=1：‘00’＜TC3＜‘FF’：TC3 =‘01’；

对于 y＝1，TC3 的值只是一个代表，其它任何范围在‘00’＜TC3＜‘FF’的值都是可能的。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 － 00 00 81 － － － 71 40 01 FF － － － － AE；

——y＝1 3B E0 － 00 00 81 － － － 71 40 01 01 － － － － 50。

通过标准：终端应在冷复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内

将 RST 置为低电平，启动热复位。

6.5.74 FWYD074-Oy 不支持的 TC3 — 热复位

测试目的：确保终端拒绝包含不支持的 TC3 值的热复位 ATR。

测试条件：正常温度、最高温度；一个适当的 ATR 使得终端发起热复位，然后卡片发送一个热复位 ATR；2 个热复位 ATR 测试案例：

——y=0：TC3 =‘FF’；

——y=1：‘00’<TC3 <‘FF’：TC3 =‘01’；

对于 y＝1，TC3 的值只是一个代表，其它任何范围在‘00’<TC3 <‘FF’的值都是可能的。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 — 00 00 81 — — — 71 40 01 FF — — — — AE；

——y＝1 3B E0 — 00 00 81 — — — 71 40 01 01 — — — — 50。

通过标准：终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.75 FWYD075-Oy 当协议不是 T=0 时，TCK 无效 — 冷复位

测试目的：确保终端在使用的不是 T＝0 协议时，拒绝冷复位 ATR 不包含 TCK 或者包含错误的 TCK 的卡片。

测试条件：正常温度、最高温度；2 个冷复位 ATR 测试案例：

——y=0：冷复位 ATR 不返回 TCK（ATR 持续时间小于 9600 初始 etu）；

——y=1：TCK 无效。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 — 00 00 81 — — — 31 40 11 — — — — — —；

——y＝1 3B E0 — 00 00 81 — — — 31 20 01 — — — — — 61。

通过标准：终端对于缺失 TCK 的情况，终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 14400 个初始 etu 之内将 RST 置为低电平，启动下电时序。对于 TCK 不正确的情况，终端应在热复位 ATR 的 TS 字符起始位下降沿开始的 24000 个初始 etu 之内将 RST 置为低电平，启动下电时序。

6.5.76 FWYD076-Oy 当协议不是 T=0 时，无效的 TCK — 热复位

测试目的：确保终端在使用的不是 T＝0 协议时，拒绝热复位 ATR 不包含 TCK 或者包含错误的 TCK 的卡片。

测试条件：正常温度、最高温度；一个适当的 ATR 使得终端发起热复位，卡片发送一个热复位 ATR；2 个热复位 ATR 测试案例：

——y=0：冷复位 ATR 不返回 TCK（ATR 持续时间小于 9600 初始 etu）。

——y=1：TCK 无效。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y＝0 3B E0 — 00 00 81 — — — 31 40 11 — — — — — —；

——y＝1 3B E0 — 00 00 81 — — — 31 20 01 — — — — — 61。

通过标准：对于缺失TCK的情况，终端应在热复位ATR的TS字符起始位下降沿开始的14400个初始etu之内将RST置为低电平，启动下电时序。对于TCK不正确的情况，终端应在热复位ATR的TS字符起始位下降沿开始的24000个初始etu之内将RST置为低电平，启动下电时序。

6.6 协议测试：T=0（XYCS）

6.6.1 XYCS001-00 etu 测量 — 冷复位

测试目的：确保当终端收到一个基本 T＝0 冷复位 ATR，在后续的数据交换中继续使用缺省的 D＝1 和 F＝372。

测试条件：正常温度、最高温度；卡片发送一个冷复位 ATR，不包含 TA1 和 TA2。调用 T＝0 协议。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － －。

通过标准：终端应使用当前的 etu 值 372/f 秒（与初始 etu 相同）继续卡片操作过程。

6.6.2 XYCS002-00 etu 测量 — 热复位

测试目的：确保当终端收到一个基本 T＝0 热复位 ATR，在后续的数据交换中继续使用缺省的 D＝1 和 F＝372。

测试条件：正常温度、最高温度；一个适当的 ATR 使得终端发起热复位；卡片发送一个热复位 ATR，不包含 TA1 和 TA2；调用 T＝0 协议。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － －。

通过标准：终端应使用当前的 etu 值 372/f 秒（与初始 etu 相同）继续卡片操作过程。

6.6.3 XYCS003-00 可接收最小同向字符间隔

测试目的：确保终端能够接收最小同向字符间隔为 11-8etu 的字符。

测试条件：ATR 采用 T＝0 协议；卡片发送的相邻字符间隔为 11-8etu。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 FF － － － － － － － － － － － －。

通过标准：终端应能够接收并正确识别卡片发送的字符，继续卡片操作过程。

6.6.4 XYCS004-00 可接收最小反向字符间隔

测试目的：确保终端能够接收终端发送最后一个字符 15etu 内卡片返回的字符。

测试条件：ATR 采用 T＝0 协议；卡片在终端最后一个字符后 15etu 发送一个字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 FF － － － － － － － － － － － －。

通过标准：终端应能够接收并识别卡片发送的字符，继续卡片操作过程。

6.6.5 XYCS005-0y 可接收最大同向字符间隔 （工作等待时间）

测试目的：确保终端能够接收最大同向字符间隔为工作等待时间＋D×480etu 的字符。

测试条件：正常温度、最高温度；ATR 采用 T＝0 协议；卡片发送的相邻字符间隔等于或稍小于 WWT＋D×480etu，WWT＝960×D×WI（如果不存在 TC2，那么该值为 9599etu）；测试在 3 种 D 值下进行：

——y=0：D=1；

——y=1：D=2；

——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 － 00 00 10 80 － － － － － － － － － － －；

——y=1 3B F0 12 00 00 10 80 － － － － － － － － － －；

——y=2 3B F0 13 00 00 10 80 － － － － － － － － － －。

通过标准：终端应能够接收并正确识别卡片发送的字符，继续卡片操作过程。

6.6.6 XYCS006-0y 可接收最大反向字符间隔 （工作等待时间）

测试目的：确保终端能够接收终端发送完最后一个字符后，卡片返回最大反向字符间隔为工作等待时间＋D×480etu 的字符。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；在终端发送最后一个字符后，卡片等待等于或稍小于 WWT＋D×480etu，WWT＝960×D×WI（如果不存在 TC2，那么该值为 9599etu）随后发送一个字符；测试在 3 种 D 值下进行：

——y=0：D=1；
——y=1：D=2；
——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B E0 — 00 00 — — — — — — — — — — — — —；
——y=1 3B F0 12 00 00 10 80 — — — — — — — — — — —；
——y=2 3B F0 13 00 00 10 80 — — — — — — — — — — —。

通过标准：终端应能够接收并正确识别卡片发送的字符，继续卡片操作过程。

6.6.7 XYCS007-00 终端冷复位后的最小反向字符间隔

测试目的：确保终端在收到卡片返回的最后一个字符后（包括 ATR 的最后一个字符），以最小字符间隔 16etu 发送一个字符。

测试条件：正常温度、最高温度；ATR 采用 T＝0 协议。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：收到冷复位 ATR 后，终端应继续卡片操作过程，终端发送的第一个字符与卡片发送的前一个字符的间隔大于或等于 16etu。

6.6.8 XYCS008-00 终端热复位后的最小反向字符间隔

测试目的：确保终端在收到卡片返回的最后一个字符后（包括 ATR 的最后一个字符），以最小字符间隔 16etu 发送一个字符。

测试条件：正常温度、最高温度；一个适当的 ATR 使终端执行热复位，然后卡片发送一个热复位 ATR；ATR 采用 T＝0 协议。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：收到热复位 ATR 后，终端应继续卡片操作过程，终端发送的第一个字符与卡片发送的前一个字符的间隔大于或等于 16etu。

6.6.9 XYCS009-00 INS 过程字节— 情况 3 和 4

测试目的：确保当过程字节等于 INS 字节时，终端发送所有的剩余字节。

测试条件：正常温度、最高温度；ATR 采用 T＝0 协议；卡片对于情况 3 或 4 的命令头响应一个值为‘INS’的字节。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：收到 INS 过程字节后，终端应发送命令头中 Lc 所指明数量的字符。

6.6.10 XYCS010-00 INS 过程字节— 情况 2

测试目的：确保当过程字节等于 INS 字节时，终端接收卡发来的所有的剩余字节。

测试条件：正常温度、最高温度；ATR 采用 T＝0 协议；一个情况 2 的命令从终端的应用层（UT）传到传输层（TTL）；一接到这个 Le=‘00’的命令，卡片就会发送过程字节‘6C Licc’;终端发送 Le=‘Licc’的命令,卡片返回‘INS’字节后面跟随卡片发来的所有剩余数据。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端接受卡片传送的数据（之后紧跟‘9000’），并且继续卡片交易。

6.6.11 XYCS011-0y INS 补码字节— 情况 3 或 4

测试目的：确保当过程字节等于 INS 字节的补码时，终端发送下一个字节数据。

测试条件：正常温度、最高温度；ATR 采用 T＝0 协议；接下来 2 个测试案例：
——y =0：收到终端发送的每一个字符后，卡片都发送一个 INS 过程字节的

补码；

——y =1：收到终端发送的第一个字符后，卡片发送一对字节 INS 补码、INS 过程字节。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － －。

通过标准：终端应根据过程字节：

——y=0：终端收到每个 INS 过程字节的补码后，发送一个单独的字节，并且继续卡片操作过程；

——y=1：终端在收到全部的 INS 过程字节补码后发送第一个字符（每个字节由 INS 过程字节的补码控制），然后接收 INS 后发送剩余的数据，并且继续卡片后续操作过程。

6.6.12 XYCS012-Oy INS 补码过程字节— 情况 2

测试目的：确保当过程字节等于 INS 字节的补码时，终端发送下一个字节数据。

测试条件：正常温度、最高温度；ATR 调用 T＝0 协议；一个情况 2 的命令从终端的应用层（UT）传到传输层（TTL）；一接到这个 Le=‘00’的命令，卡片就会发送过程字节‘6C Licc’；一收到终端发来的 Le=‘Licc’（命令头的 P3 字节）的情况 2 命令头：

——y=0：卡片在第一个字节响应数据之前，发送 INS 过程字节的补码，然后每发一个字节的响应数据之前都发送一个 INS 过程字节的补码直到所有的响应数据已经全部传送给终端；

——y=1：卡片在第一个字节响应数据之前，发送 INS 过程字节的补码，然后再发一个 INS 过程字节后面紧跟着所有剩余的响应数据。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － －。

通过标准：终端应根据过程字节：

——y=0：终端依次接收卡片发送的数据，并且继续卡片后续操作过程；

——y=1：终端在收到全部的 INS 过程字节的补码后接收第一个数据字符（每个字节由 INS 补控制），然后接收 INS 后发送剩余的数据，并且继续卡片后续操作过程。

6.6.13 XYCS013-Oy 过程字节‘60’

测试目的：确保当终端收到过程字节‘60’时使用额外工作等待时间。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；3 个测试案例：

——y =0：一个过程字节‘60’；

——y =1：10 个连续的过程字节‘60’；

——y =2：50 个连续的过程字节‘60’；

在前一个过程字节‘60’后，恰好在工作等待时间超时前，卡片返回下一个字符。

注：对于 y=1 和 y=2，重复的次数只是一个参考，卡片将发送多个连续过程字节‘60’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 － 00 00 － － － － － － － － － － － －。

通过标准：当终端收到过程字节‘60’后，等待额外工作等待时间，然后继续卡片后续操作过程。

6.6.14 XYCS014-Oy 过程字节‘60’ 在过程字节 INS 中

测试目的：确保当过程字节‘60’包含在发送或接收的数据中，终端应使用额外工作等待时间，并且不能把‘60’当成数据字节。

测试条件：正常温度、最高温度；ATR 采用 T＝0 协议；2 个测试案例：

——y =0：卡片在过程字节 INS 的补码控制下发送数据，包括一个过程字节

‘60’，并使用额外工作等待时间直到发送下一个过程字节；

——y =1：卡片通过发送 INS 的补码从终端接收数据，包括一个过程字节‘60’，并使用额外工作等待时间直到发送下一个过程字节。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端：

——y=0：终端接受卡片以字节形式发送的数据，并且继续卡片后续操作过程；

——y=1：终端以字节形式发送数据，并且继续卡片后续操作过程。

6.6.15 XYCS015-00 过程字节’61’ — 情况 2

测试目的：确保当收到过程字节‘61’时，终端等待下一个过程字节，然后向卡片发送最大长度为 xx 的 GET RESPONSE 命令头，xx 的值是第二个过程字节。

测试条件：正常温度、最高温度；ATR 调用 T＝0 协议；一个情况 2 的命令从终端的应用层（UT）传到传输层（TTL）；一接到这个 Le=‘00’（命令头的 P3 字节）的命令头：

——y=0：卡片发送过程字节‘61’，然后发送过程字节‘xx’（xx 在‘01’到 Licc 之间取值）。对至少一个情况 2 的命令，至少连续发了十次的过程字节‘61’；

——y=1：卡片发送过程字节‘61’，然后发送过程字节‘xx’，

‘xx’=‘INS 补码’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：当收到过程字节‘61xx’，终端应发送GET RESPONSE命令头，其中P3‘xx’。终端应该能够用至少10个的GET RESPONSE命令来正确接收命令情况2的数据。

6.6.16 XYCS016-xy 状态字节‘6x’ 或者 ’9x’

测试目的：确保当收到状态字节‘6x’（除了’60’，’61’，’6C’）或者‘9x’，终端应等待下一个字节 SW2。

测试条件：正常温度、最高温度；ATR 采用 T＝0 协议；表 4 状态字节列出了 29 个子案例，其中子案例 00、01、02、03、04、05、15 和 16 是强制的，均要执行。子案例 06 到 14 和 17 到 28 可以不执行；

表4 状态字节

Xy	00	01	02	03	04	05	06	07	08	09	10
SW1 SW2	62xx	63xx	6700	6Axx	6Fxx	9000	64xx	65xx	66xx	68xx	69xx
Xy	11	12	13	14	15	16	17	18	19	20	21
SW1 SW2	6Bxx	6D00	6E00	91xx	92xx	93xx	94xx	95xx	96xx	97xx	98xx
Xy	22	23	24	25	26	27	28				
SW1 SW2	99xx	9Axx	9Bxx	9Cxx	9Dxx	9Exx	9Fxx				

当 SW2＝‘xx’时，意味着一个‘00’到‘FF’的值。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端应等待下一个状态字节，并继续卡片后续操作过程。

6.6.17 XYCS017-0y 最大可接收同向字符间隔超限（工作等待时间）（1）

测试目的：确保当卡片两个字符之间的工作等待时间超限（超过 D×480etu），终端应发起下电时序。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；当发送了 ATR 并且收到了

终端的响应，卡片将发送一个或几个字节，但不发送其余的字节；测试在3个D值的情况下进行：

——y=0：D=1；

——y=1：D=2；

——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 —00 00 10 80 — — — — — — — — — — —；

——y=1 3B F0 12 00 00 10 80 — — — — — — — — — — —；

——y=1 3B F0 13 00 00 10 80 — — — — — — — — — — —。

通过标准：终端应在发生超时的字符起始位开始{WWT +（D x 9,600）} etu内发起下电时序。

6.6.18 XYCS018-0y 最大可接收同向字符间隔超限（工作等待时间） （2）

测试目的：确保当卡片两个字符之间的工作等待时间超限（超过D×480etu），终端应发起下电时序。

测试条件：正常温度、最高温度；ATR指出使用T＝0协议；当卡片返回了ATR并且收到了终端的命令头，卡片将以字符间隔至少为WWT + D x 480 + 1 etu发送字符；测试在3个D值的情况下进行：

——y=0：D=1；

——y=1：D=2；

——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 10 80 — — — — — — — — — — —；

——y=1 3B F0 12 00 00 10 80 — — — — — — — — — — —；

——y=1 3B F0 13 00 00 10 80 — — — — — — — — — — —。

通过标准：终端应在发生超时的字符起始位开始{WWT + （D x 9，600）} etu内发起下电时序。

6.6.19 XYCS019-0y 最大可接收反向字符间隔超限 （工作等待时间） （1）

测试目的：确保当从终端发送的最后一个字符起超过工作等待时间+D×480 etu后，卡片返回字符，终端应发起下电时序。

测试条件：正常温度、最高温度；ATR指出使用T＝0协议；当发送了ATR并且收到了终端的命令头，卡片不响应；测试在3个D值的情况下进行：

——y=0：D=1；

——y=1：D=2；

——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4TC4 TCK。

——y=0 3B E0 — 00 00 10 80 — — — — — — — — — — —；

——y=1 3B F0 12 00 00 10 80 — — — — — — — — — — —；

——y=1 3B F0 13 00 00 10 80 — — — — — — — — — — —。

通过标准：终端应在发生超时的字符起始位开始{WWT +（D x 9，600）} etu内发起下电时序。

6.6.20 XYCS020-0y 最大可接收反向字符间隔超限 （工作等待时间） （2）

测试目的：确保当从终端发送的最后一个字符起超过工作等待时间+D×480 etu后，卡片返回字符，终端应发起下电时序。

测试条件：正常温度、最高温度；ATR指出使用T＝0协议；当发送了ATR并且收到了终端的响应后，卡片在发送第一个字符前（WWT =960 x D x WI）至少等待WWT +（D x 480）etu；测试在3个D值的情况下进行：

——y=0：D=1；

——y=1：D=2；
——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B E0 — 00 00 10 80 — — — — — — — — — — —；
——y=1 3B F0 12 00 00 10 80 — — — — — — — — — — —；
——y=1 3B F0 13 00 00 10 80 — — — — — — — — — — —。

通过标准：终端应在发生超时的字符起始位开始{WWT +（D x 9，600）} etu 内发起下电时序。

6.6.21 XYCS021-00 不支持的过程字节或状态字节

测试目的：确保当收到不支持的过程字节，终端应下电。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；2 个测试案例：
——y=0：在收到终端发送的命令后，卡片返回‘00’代替过程字节 INS；
——y=1：在收到终端处理的命令头后，卡片返回‘FF xx’代替SW1 SW2‘9000’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端应在无效字节的起始位开始到 RST 变低的 9600etu 内发起下电时序。

6.6.22 XYCS022-0y 错误检测 （奇偶校验）

测试目的：确保当收到的字符奇偶校验错误，终端应发送一个错误信号。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；卡片在协议交换时发送一个奇偶校验错误的字符；2 个测试案例：
——y=0：正向约定（TS＝‘3B’）；
——y=1：反向约定（TS＝‘3F’）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B 60 — 00 00 — — — — — — — — — — — —；
——y=1 3F 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端应在包含奇偶校验错误的字符起始位开始的10.5±0.2etu内将IO置成低电平，这个低电平持续的时间为1（最小）到2个（最大）etu。当收到无奇偶校验错误的重发字符后，终端应继续正常处理。

6.6.23 XYCS023-00 多次错误重发（接收）

测试目的：确保终端能够最多 4 次指明卡片发送字节的奇偶校验错误。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；卡片重复 4 次发送同一个奇偶校验错误的字符，第五次发送奇偶校验正确的字符。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端每次收到奇偶校验错误的字符，终端应在错误字符起始位开始 10.5±0.2etu 内发送一个 1 到 2 个 etu 长度的低电平信号。当收到无奇偶校验错误的重发字符，终端应继续正常处理。

6.6.24 XYCS024-0y 超过错误重发次数（接收）

测试目的：确保终端在接收到 4 次奇偶校验错误的字符时能够正确给出重发信号，再次收到奇偶校验错误的字符时启动下电时序。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；卡片重复 5 次发送同一个奇偶校验错误的字符；测试在 3 个 D 值下进行：
——y=0：D=1；
——y=1：D=2；
——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 10 80 — — — — — — — — — — —；
——y=1 3B F0 12 00 00 10 80 — — — — — — — — — — —；
——y=2 3B F0 13 00 00 10 80 — — — — — — — — — — —。

通过标准：终端前 4 次收到奇偶校验错误的字符，终端应在错误字符起始位开始 10.5±0.2etu 内发送一个 1 到 2 个 etu 长度的低电平信号。当收到第 5 次奇偶校验错误的重发字符时，终端应在奇偶校验错误的字符起始位开始的 D×960etu 内，将 RST 变低发起下电时序。

6.6.25 XYCS025-00 重发字符的解释

测试目的：确保当卡片发送的奇偶校验错误的字符后面跟随着校验正确的字符时，终端应存储并使用正确的重发字符。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端正确解释重发字符并继续卡片操作。

6.6.26 XYCS026-00 错误纠正

测试目的：确保终端收到错误信号能够重发有争议的字符。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；卡片通过将 I/O 线置低来表明错误，低电平状态从假定有错的字符的起始位下降沿开始测量；这个测试案例可能根据表 5 选项执行表中的两个选项来执行。第一个选项利用单独的子案例实现多个开始低电平状态的时间和持续时间。第二个选项多个子案例使用固定的低电平持续时间。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

表5 选项执行表

选项	测试案例	开始（etu）	持续（etu）	结束（etu）
1	y=0	10-5	1-5	12
	y=1	10-3	1	11-3
	y=2	10-3	2	12-3
	y=3	10-7	1	11-7
	y=4	10-7	2	12-7
r2	y=0	10-7	0-6	11-3

通过标准：终端在检测到错误后最少 2 个 etu 后重发字符，也就是从错误字符起始位起延迟至少 12.8etu 后重发字符。

6.6.27 XYCS027-00 多次错误重发 （传输）

测试目的：确保如果卡片在最后一个字符外的每个字符后都表明错误，终端能够最多 5 次重发有争议的字符。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；在终端发送一个字符后，卡片重复 4 次发送信号表明奇偶校验错误。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端应连续 5 次重发有争议的字符，并继续正常处理。

6.6.28 XYCS028-0y 超过错误重发次数 （传输）

测试目的：确保终端在连续 5 次收到表明奇偶校验错误的重发信号时下电。

测试条件：正常温度、最高温度；ATR 指出使用 T＝0 协议；卡片重复 5 次发送表明奇偶校验错误的信号；测试在 3 个 D 值下进行：

——y=0：D=1；

——y=1：D=2；
——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 10 80 — — — — — — — — — — —；
——y=1 3B F0 12 00 00 10 80 — — — — — — — — — — —；
——y=2 3B F0 13 00 00 10 80 — — — — — — — — — — —。

通过标准：终端应在第 5 次包含奇偶校验错误信号的字符起始位开始的 D×960etu 内发起下电时序。

6.7 协议测试：T=1（XYCS）

6.7.1 XYCS101-00 最小字符间隔

测试目的：确保终端能正确接收 IC 卡发送的最小字符间隔时间的字符。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片发送连续字符间隔为 10.8 个 etu 的块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF。

通过标准：终端正确接收卡片发送的块并继续卡片后续操作过程。

6.7.2 XYCS102-0y 字符等待时间（CWT）

测试目的：确保终端能正确接收 IC 卡发送的最大字符间隔为（CWT+4）etu 的字符。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片发送连续字符间隔为 CWT+4 个 etu 的块；此项测试将按照表 6 字符间隔不同的 TB3 的值重复测试。

表6 字符间隔

y	TB3	CWI	CWT（etus）	响应时间（etus）
0	01	1	13	17
1	02	2	15	19
2	03	3	19	23
3	04	4	27	31
4	05	5	43	47

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71；
——y=1 3B E0 — 00 00 81 — — — 31 20 02 — — — — — 72；
——y=2 3B E0 — 00 00 81 — — — 31 20 03 — — — — — 73；
——y=3 3B E0 — 00 00 81 — — — 31 20 04 — — — — — 74；
——y=4 3B E0 — 00 00 81 — — — 31 20 05 — — — — — 75。

通过标准：终端正确接收卡片发送的块并继续卡片后续操作。

6.7.3 XYCS103-xy 块等待时间（BWT）

测试目的：确保终端能正确接收在其发送的最后一个字符之后（BWT+D x 960）etu 内 IC 卡发送的块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片接收到终端发送的最后一个块的最后一个字符后，等待（BWT+D x 960）etu 发送一个块；此项测试将按照表 7 TB3 选项及 D 值的不同重复测试。

表7 TB3选项及D值

X	y	TA1	TB3	BWI	BWT（etus） [（2^{BWI} x 960 x 372D/f） +11]	响应时间（etus） （=BWT+D x 960）
0	0	11或缺省 （D=1）	01	0	971	1931
	1		11	1	1931	2891
	2		21	2	3851	4811

	3		31	3	7691	8651
	4		41	4	15371	16331
1	0	12 （D=2）	01	0	1931	3851
	1		11	1	3851	5771
	2		21	2	7691	9611
	3		31	3	15371	17291
	4		41	4	30731	32651
2	0	13 （D=4）	01	0	3851	7691
	1		11	1	7691	11531
	2		21	2	15371	19211
	3		31	3	30731	34571
	4		41	4	61451	65291

ATR： TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；

——xy=01 3B E0 — 00 00 91 81 — — 31 20 11 — — — — — F0；

——xy=02 3B E0 — 00 00 91 81 — — 31 20 21 — — — — — C0；

——xy=03 3B E0 — 00 00 91 81 — — 31 20 31 — — — — — D0；

——xy=04 3B E0 — 00 00 91 81 — — 31 20 41 — — — — — A0；

——xy=10 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；

——xy=11 3B F0 12 00 00 91 81 — — 31 20 11 — — — — — F2；

——xy=12 3B F0 12 00 00 91 81 — — 31 20 21 — — — — — C2；

——xy=13 3B F0 12 00 00 91 81 — — 31 20 31 — — — — — D2；

——xy=14 3B F0 12 00 00 91 81 — — 31 20 41 — — — — — A2；

——xy=20 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3；

——xy=21 3B F0 13 00 00 91 81 — — 31 20 11 — — — — — F3；

——xy=22 3B F0 13 00 00 91 81 — — 31 20 21 — — — — — C3；

——xy=23 3B F0 13 00 00 91 81 — — 31 20 31 — — — — — D3；

——xy=24 3B F0 13 00 00 91 81 — — 31 20 41 — — — — — A3。

通过标准：终端正确接收卡片发送的块并继续卡片后续操作。

6.7.4 XYCS104-00 块保护时间（BGT）

测试目的：确保终端在其发送的最后一个字符之后，能正确接收不早于（BGT1）etu 时 IC 卡发送的块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片接收到终端发送的最后一个块后，等待至少（BGT1）etu 发送一个块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF。

通过标准：终端正确接收卡片发送的块并继续卡片后续操作。

6.7.5 XYCS105-00 冷复位后块保护时间（BGT）

测试目的：确保终端接收到的最后一个字符（包括 ATR 的最后一个字符）和在相反方向发送的第一个字符之间的最小时间间隔为 22 个 etu。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端在等于或大于 22 个 etu 的时间间隔（接收到的最后一个字符和在相反方向发送的第一个字符之间）继续卡片后续操作。

6.7.6 XYCS106-00 热复位后块保护时间（BGT）

测试目的：确保终端接收到的最后一个字符（包括 ATR 的最后一个字符）和在相反方向发送的第一个字符之间的最小时间间隔为 22 个 etu。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；一个适当的 ATR 导致终端执行热复位。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端在等于或大于 22 个 etu 的时间间隔（接收到的最后一个字符和在相反方向发送的第一个字符之间）继续卡片后续操作。

6.7.7 XYCS107-0y 链接块——WTX 请求

测试目的：确保终端在链接中正确处理一个 WTX 请求并执行。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片发送一个等待时间扩展请求（WTX=BWT x m），在接收到终端发送的最后一个块的最后一个字符后等待等于或稍小于（WTX + mxDx960）个 etu 后，卡片再发送一个块；此项通过三个 D 值测试：

——y=0：D=1；

——y=1：D=2；

——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B A0 — 00 — 91 81 — — 71 20 01 00 — — — — E0；

——y=1 3B B0 12 00 — 91 81 — — 71 20 01 00 — — — — E2；

——y=2 3B B0 13 00 — 91 81 — — 71 20 01 00 — — — — E3。

通过标准：终端正确处理链接，执行 WTX 扩展，接收块并继续卡片后续操作。

6.7.8 XYCS108-00 第一个 I 块的序列号

测试目的：确保终端发送的第一个 I 块的序列号为 0。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF。

通过标准：终端发送得第一个 I 块的序列号为 0（PCB 的第 7 位）。

6.7.9 XYCS109-00 I 块的有效交替

测试目的：确保终端正确地发送和接收无链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；I 块将在终端和卡之间至少交替 5 次。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端以正确的序列号发送 I 块，并正确接收来自卡的数据。

6.7.10 XYCS110-00 链接——终端接收

测试目的：确保终端正确接收带链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡向终端发送带链接的块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端正确接收卡发送的带链接的 I 块，正确管理 R 块的序列号并继续卡片后续操作。

6.7.11 XYCS111-00 链接——R 块的序列号

测试目的：确保终端即使接收错误的块仍能够正确管理 R 块的序列号（按照一位编码的模 2 计数器，以指示终端期望接收的下一个 I 块）。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片正确链接块，随后在响应 R 块时发送错误的块，该 R 块用来确认之前带链接的 I 块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF。

通过标准：终端正确的管理序列号。

6.7.12 XYCS112-00 双向的链接

测试目的：确保终端正确处理双向带链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡正确响应带链接的块，之后发送链接的块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端遵守传输 I 块的先后顺序，正确的执行需要链接数据的截短，从而使得数据链接处理正确；同时终端能接收带链接的 I 块。

6.7.13 XYCS113-0y 终端发送链接块和无链接块——遵守 IFSI 值

测试目的：确保终端遵守 IFSI 值（该值由卡片返回的 ATR 中的 TA3 得到）：终端发出的任何信息块的信息域大小应小于或等于该值。

测试条件：正常温度、最高温度；以下定义九个子案例。y=0 和 y=1 子案例是强制的，均须执行。y=2 至 y=8 子案例可选择执行。指定的 TA3 的值为有意设定的，作为测试潜在值范围的测试用例，测试时可以用其它接近的值代替；ATR 调用 T=1 协议；TA3 的值从 16 变化至 254：

——y=0：TA3 =10；
——y=1：TA3 =20；
——y=2：TA3 =40；
——y=3：TA3 =60；
——y=4：TA3 =80；
——y=5：TA3 =A0；
——y=6：TA3 =C0；
——y=7：TA3 =E0；
——y=8：TA3 =FE。

注：TA3 的值仅仅为列举——16 至 254 中的其它任意 9 个值都允许使用。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 81 — — — 31 10 01 — — — — — 41；
——y=1 3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71；
——y=2 3B E0 — 00 00 81 — — — 31 40 01 — — — — — 11；
——y=3 3B E0 — 00 00 81 — — — 31 60 01 — — — — — 31；
——y=4 3B E0 — 00 00 81 — — — 31 80 01 — — — — — D1；
——y=5 3B E0 — 00 00 81 — — — 31 A0 01 — — — — — F1；
——y=6 3B E0 — 00 00 81 — — — 31 C0 01 — — — — — 91；
——y=7 3B E0 — 00 00 81 — — — 31 E0 01 — — — — — B1；
——y=8 3B E0 — 00 00 81 — — — 31 FE 01 — — — — — AF。

通过标准：终端在发送链接块和无链接 I 块时均遵守 IFSI 值。

6.7.14 XYCS114-0y 带链接和无链接——在两个链中重复请求改变 IFSC

测试目的：确保终端正确的响应连续改变 IFSC 的请求，并且能够调整（使用链接或不使用链接）带链接块的大小以适应新的 IFSC。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；初始 IFSC（值为 16）包含在 TA3 可变的 ATR 中；卡发送若干个不同 INF 域的 S（IFS 请求）块；终端向 TTL 发送不同大小的 CAPDU；以下定义三个子案例。y=0 子案例是强制的，均须执行。y=1 至 y=2 子案例可选择执行：

——y=0：CAPDU 的大小为 16；

——y=1：CAPDU 的大小为 150；
——y=2：CAPDU 的大小为 260；
在上面 y=1 案例中的 CAPDU 值仅为列举。在实际应用中可以为 y=0 和 y=2 中 CAPDU 值之间的其它值。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 10 01 — — — — — 41。

通过标准：终端遵守 ATR 中指定的 IFSI 值，通过发送 S 块响应（IFS 响应）确定 S 块请求（IFS 请求），并调整块的大小以适应新的 IFSC。

6.7.15 XYCS115-xy 字符等待时间（CWT）超限（1）

测试目的：确保如果卡超出 CWT（大于 4 个 etu），终端启动下电时序或发送 R 块或 S 请求块（依据未应答的块的类型）。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡发送一个或多个字符，之后不再发送其余字符：
——x=0：为 I 块、R 块或 S 应答块；
——x=1：为 S 请求块；
此项测试将按照表 8 TB3 值重复执行。

表 8 TB3 值

y	TB3	CWI	CWT（etus）
0	01	1	13
1	02	2	15
2	03	3	19
3	04	4	27
4	05	5	43

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71；
——y=1 3B E0 — 00 00 81 — — — 31 20 02 — — — — — 72；
——y=2 3B E0 — 00 00 81 — — — 31 20 03 — — — — — 73；
——y=3 3B E0 — 00 00 81 — — — 31 20 04 — — — — — 74；
——y=4 3B E0 — 00 00 81 — — — 31 20 05 — — — — — 75。

通过标准：x=0 和 x=1：终端启动下电时序。或 x=0：终端发送 R 块。x=1：终端发送 S 请求块。以上动作应在最后一个接收到的字符的起始位下降沿开始的（CWT+4）个 etu 到（CWT+4800）个 etu 之内完成。

6.7.16 XYCS116-xy 字符等待时间（CWT）超限（2）

测试目的：确保如果卡超出 CWT（大于 4 个 etu），终端启动下电时序或发送 R 块或 S 请求块（依据未应答的块的类型）。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡发送一个块，其字符间隔至少为 CWT+5 个 etu（以后称之为响应时间）：
——x=0：为 I 块、R 块或 S 应答块；
——x=1：为 S 请求块；
此项测试将按照表 9 TB3 值重复执行。

表 9 TB3 值

y	TB3	CWI	CWT（etus）	响应时间（etus）（=CWT+4+1）
0	01	1	13	18
1	02	2	15	20
2	03	3	19	24
3	04	4	27	32
4	05	5	43	48

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71；

——y=1 3B E0 — 00 00 81 — — — 31 20 02 — — — — — 72；

——y=2 3B E0 — 00 00 81 — — — 31 20 03 — — — — — 73；

——y=3 3B E0 — 00 00 81 — — — 31 20 04 — — — — — 74；

——y=4 3B E0 — 00 00 81 — — — 31 20 05 — — — — — 75。

通过标准：x=0 和 x=1：终端启动下电时序。或 x=0：终端发送 R 块。x=1：终端发送 S 请求块。以上动作应在最后一个接收到的字符的起始位下降沿开始的（CWT+4）个 etu 到（CWT+4800）个 etu 之内完成。

6.7.17 XYCS117-xy 响应 S 请求块时块等待时间（BWT）超限（1）

测试目的：确保如果卡超出块等待时间（BWT）D x 960 个 etu，终端启动下电时序或发送 S 请求块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡对终端发送的 S 请求块无响应；此项测试包括三个 D 值：

——x=0：D=1；

——x=1：D=2；

——x=2：D=4；

此项测试将按照表 10 TB3 值重复执行。

表 10 TB3 值

x	y	TA1	TB3	BWI	BWT（etus） [（2^{BWI} x 960 x 372D/f） +11]
0	0	11或缺省（D=1）	01	0	971
	1		11	1	1931
	2		21	2	3851
	3		31	3	7691
	4		41	4	15371
1	0	12 （D=2）	01	0	1931
	1		11	1	3851
	2		21	2	7691
	3		31	3	15371
	4		41	4	30731
2	0	13 （D=4）	01	0	3851
	1		11	1	7691
	2		21	2	15371
	3		31	3	30731
	4		41	4	61451

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；

——xy=01 3B E0 — 00 00 91 81 — — 31 20 11 — — — — — F0；

——xy=02 3B E0 — 00 00 91 81 — — 31 20 21 — — — — — C0；

——xy=03 3B E0 — 00 00 91 81 — — 31 20 31 — — — — — D0；

——xy=04 3B F0 — 00 00 91 81 — — 31 20 41 — — — — — A0；

——xy=10 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；

——xy=11 3B F0 12 00 00 91 81 — — 31 20 11 — — — — — F2；

——xy=12 3B F0 12 00 00 91 81 — — 31 20 21 — — — — — C2；

——xy=13 3B F0 12 00 00 91 81 — — 31 20 31 — — — — — D2；

——xy=14 3B F0 12 00 00 91 81 — — 31 20 41 — — — — — A2；

——xy=20 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3；

——xy=21 3B F0 13 00 00 91 81 — — 31 20 11 — — — — — F3；

——xy=22 3B F0 13 00 00 91 81 — — 31 20 21 — — — — — C3；

——xy=23 3B F0 13 00 00 91 81 — — 31 20 31 — — — — — D3；
——xy=24 3B F0 13 00 00 91 81 — — 31 20 41 — — — — — A3。

通过标准：终端启动下电时序或终端发送 S 请求块。以上动作应在未收到应答的块的最后一个字节的起始位下降沿开始的{BWT+(Dx960)}个 etu 到{BWT+(Dx4800)}个 etu 之内完成。

6.7.18 XYCS118-xy 响应 S 请求块时块等待时间（BWT）超限（2）

测试目的：确保如果卡超出块等待时间（BWT）Dx960 个 etu，终端启动下电时序或发送 S 请求块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；接收到 ATR 后，终端发送 S 请求块请求卡响应；卡在发送回应之前至少等待“响应时间”；此项测试包括三个 D 值：

——x=0：D=1；
——x=1：D=2；
——x=2：D=4；

此项测试将按照表 11 TB3 值重复执行。

表 11 TB3 值

X	y	TA1	TB3	BWI	BWT（etus）[(2^{BWI} x 960 x 372D/f) +11]	响应时间（etus）(=BWT+D x 960+1)
0	0	11或缺省（D=1）	01	0	971	1932
	1		11	1	1931	2892
	2		21	2	3851	4812
	3		31	3	7691	8652
	4		41	4	15371	16332
1	0	12（D=2）	01	0	1931	3852
	1		11	1	3851	5772
	2		21	2	7691	9612
	3		31	3	15371	17292
	4		41	4	30731	32652
2	0	13（D=4）	01	0	3851	7692
	1		11	1	7691	11532
	2		21	2	15371	19212
	3		31	3	30731	34572
	4		41	4	61451	65292

ATR： TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；
——xy=01 3B E0 — 00 00 91 81 — — 31 20 11 — — — — — F0；
——xy=02 3B E0 — 00 00 91 81 — — 31 20 21 — — — — — C0；
——xy=03 3B E0 — 00 00 91 81 — — 31 20 31 — — — — — D0；
——xy=04 3B F0 — 00 00 91 81 — — 31 20 41 — — — — — A0；
——xy=10 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；
——xy=11 3B F0 12 00 00 91 81 — — 31 20 11 — — — — — F2；
——xy=12 3B F0 12 00 00 91 81 — — 31 20 21 — — — — — C2；
——xy=13 3B F0 12 00 00 91 81 — — 31 20 31 — — — — — D2；
——xy=14 3B F0 12 00 00 91 81 — — 31 20 41 — — — — — A2；
——xy=20 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3；
——xy=21 3B F0 13 00 00 91 81 — — 31 20 11 — — — — — F3；
——xy=22 3B F0 13 00 00 91 81 — — 31 20 21 — — — — — C3；
——xy=23 3B F0 13 00 00 91 81 — — 31 20 31 — — — — — D3；
——xy=24 3B F0 13 00 00 91 81 — — 31 20 41 — — — — — A3。

通过标准：终端启动下电时序或终端发送 S 请求块。以上动作应在未收到应答的块的最

后一个字节的起始位下降沿开始的{BWT+(Dx960)}个 etu 到{BWT+(Dx4800)}个 etu 之内完成。

6.7.19 XYCS119-xy 响应 I 块、R 块或 S 响应块时块等待时间（BWT）超限（1）

测试目的：确保如果卡超出块等待时间（BWT）Dx960 个 etu，终端启动下电时序或发送 R 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡对终端发送的 I 块、R 块或 S 响应块无响应；此项测试包括三个 D 值：

——x=0：D=1；

——x=1：D=2；

——x=2：D=4；

此项测试将按照表 12 TB3 值重复执行。

表 12 TB3 值

x	y	TA1	TB3	BWI	BWT（etus） [（2^{BWI} x 960 x 372D/f） +11]
0	0	11或缺省（D=1）	01	0	971
	1		11	1	1931
	2		21	2	3851
	3		31	3	7691
	4		41	4	15371
1	0	12 （D=2）	01	0	1931
	1		11	1	3851
	2		21	2	7691
	3		31	3	15371
	4		41	4	30731
2	0	13 （D=4）	01	0	3851
	1		11	1	7691
	2		21	2	15371
	3		31	3	30731
	4		41	4	61451

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；

——xy=01 3B E0 — 00 00 91 81 — — 31 20 11 — — — — — F0；

——xy=02 3B E0 — 00 00 91 81 — — 31 20 21 — — — — — C0；

——xy=03 3B E0 — 00 00 91 81 — — 31 20 31 — — — — — D0；

——xy=04 3B F0 — 00 00 91 81 — — 31 20 41 — — — — — A0；

——xy=10 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；

——xy=11 3B F0 12 00 00 91 81 — — 31 20 11 — — — — — F2；

——xy=12 3B F0 12 00 00 91 81 — — 31 20 21 — — — — — C2；

——xy=13 3B F0 12 00 00 91 81 — — 31 20 31 — — — — — D2；

——xy=14 3B F0 12 00 00 91 81 — — 31 20 41 — — — — — A2；

——xy=20 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3；

——xy=21 3B F0 13 00 00 91 81 — — 31 20 11 — — — — — F3；

——xy=22 3B F0 13 00 00 91 81 — — 31 20 21 — — — — — C3；

——xy=23 3B F0 13 00 00 91 81 — — 31 20 31 — — — — — D3；

——xy=24 3B F0 13 00 00 91 81 — — 31 20 41 — — — — — A3。

通过标准：终端启动下电时序或终端发送 R 块。以上动作应在未收到应答的块的最后一个字节的起始位下降沿开始的{BWT+（Dx960）}个 etu 到{BWT+（Dx4800）}个 etu 之内完成。

6.7.20 XYCS120-xy 响应 I 块、R 块或 S 响应块时块等待时间（BWT）超限（2）

测试目的：确保如果卡超出块等待时间（BWT）Dx960 个 etu，终端启动下电时序或发送 R 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；接收到 ATR 后，终端发送 I 块、R 块或 S 响应块请求卡响应；卡在发送回应之前至少等待“响应时间”；此项测试包括三个 D 值：

——x=0：D=1；

——x=1：D=2；

——x=2：D=4；

此项测试将按照下表 13 TB3 值重复执行。

表 13 TB3 值

X	y	TA1	TB3	BWI	BWT（etus） [（2^{BWI} x 960 x 372D/f） +11]	响应时间（etus） （=BWT+D x 960+1）
0	0	11或缺省 （D=1）	01	0	971	1932
	1		11	1	1931	2892
	2		21	2	3851	4812
	3		31	3	7691	8652
	4		41	4	15371	16332
1	0	12 （D=2）	01	0	1931	3852
	1		11	1	3851	5772
	2		21	2	7691	9612
	3		31	3	15371	17292
	4		41	4	30731	32652
2	0	13 （D=4）	01	0	3851	7692
	1		11	1	7691	11532
	2		21	2	15371	19212
	3		31	3	30731	34572
	4		41	4	61451	65292

ATR： TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；

——xy=01 3B E0 — 00 00 91 81 — — 31 20 11 — — — — — F0；

——xy=02 3B E0 — 00 00 91 81 — — 31 20 21 — — — — — C0；

——xy=03 3B E0 — 00 00 91 81 — — 31 20 31 — — — — — D0；

——xy=04 3B F0 — 00 00 91 81 — — 31 20 41 — — — — — A0；

——xy=10 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；

——xy=11 3B F0 12 00 00 91 81 — — 31 20 11 — — — — — F2；

——xy=12 3B F0 12 00 00 91 81 — — 31 20 21 — — — — — C2；

——xy=13 3B F0 12 00 00 91 81 — — 31 20 31 — — — — — D2；

——xy=14 3B F0 12 00 00 91 81 — — 31 20 41 — — — — — A2；

——xy=20 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3；

——xy=21 3B F0 13 00 00 91 81 — — 31 20 11 — — — — — F3；

——xy=22 3B F0 13 00 00 91 81 — — 31 20 21 — — — — — C3；

——xy=23 3B F0 13 00 00 91 81 — — 31 20 31 — — — — — D3；

——xy=24 3B F0 13 00 00 91 81 — — 31 20 41 — — — — — A3。

通过标准：终端启动下电时序或终端发送 R 块。以上动作应在未收到应答的块的最后一个字节的起始位下降沿开始的{BWT+（Dx960）}个 etu 到{BWT+（Dx4800）}个 etu 之内完成。

6.7.21 XYCS121-0y 无链接的块——正确、错误的等待时间扩展（WTX）应用

测试目的：确保终端正确的解释 S 块（WTX 响应），响应并执行等待时间扩展。同时确保如果卡没有另发 S 块（WTX 响应）而再一次应用扩展，终端启动下电时序或发送 R 块（仅有一种可能）。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡请求扩展等待时间（BWTxm），在扩展等待时间超限（称为“响应时间”）前发送块；然后，没有再次请求扩展等待时间，卡使用相同的响应时间发送块；

此项测试包括三个 D 值：

——y=0：D=1；

——y=1：D=2；

——y=2：D=4；

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——y=0 3B A0 — 00 — 91 81 — — 71 20 01 00 — — — — E0；

——y=1 3B B0 12 00 — 91 81 — — 71 20 01 00 — — — — E2；

——y=2 3B B0 13 00 — 91 81 — — 71 20 01 00 — — — — E3。

通过标准：终端正确的确认等待时间扩展并接收卡发送的 I 块，然后终端启动下电时序或发送 R 块。以上动作应在卡未请求等待时间扩展而再一次应用 BWT 发送的块的最后一个字节的起始位下降沿开始的{BWT+（Dx960）}个 etu 到{BWT+（Dx4800）}个 etu 之内完成。

6.7.22 XYCS122-00 等待时间扩展（WTX）超限（1）

测试目的：确保如果超出等待时间扩展（WTX）mxDx960 个 etu，终端启动下电时序或发送 R 块（仅有一种可能）。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；交换 S（WTX）块后，卡无响应；

此项测试包括三个 D 值：

——x=0：D=1；

——x=1：D=2；

——x=2：D=4；

此项测试将按照下表 14 TB3 值重复执行。

表 14 TB3 值

X	y	TA1	TB3	BWI	BWT（etus）[（2^{BWI} x 960 x 372D/f） +11]	WTX（etus）（=BWT x m）例如m=3
0	0	11或缺省（D=1）	01	0	971	2913
	1		11	1	1931	5793
	2		21	2	3851	11553
	3		31	3	7691	23073
	4		41	4	15371	46113
1	0	12（D=2）	01	0	1931	5793
	1		11	1	3851	11553
	2		21	2	7691	23073
	3		31	3	15371	46113
	4		41	4	30731	92193
2	0	13（D=4）	01	0	3851	11553
	1		11	1	7691	23073
	2		21	2	15371	46113
	3		31	3	30731	92193
	4		41	4	61451	184353

ATR： TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；

——xy=01 3B E0 — 00 00 91 81 — — 31 20 11 — — — — — F0；

——xy=02 3B E0 — 00 00 91 81 — — 31 20 21 — — — — — C0；

——xy=03 3B E0 — 00 00 91 81 — — 31 20 31 — — — — — D0；

——xy=04 3B F0 — 00 00 91 81 — — 31 20 41 — — — — — A0；

——xy=10 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；

——xy=11 3B F0 12 00 00 91 81 — — 31 20 11 — — — — — F2；

——xy=12 3B F0 12 00 00 91 81 — — 31 20 21 — — — — — C2；
——xy=13 3B F0 12 00 00 91 81 — — 31 20 31 — — — — — D2；
——xy=14 3B F0 12 00 00 91 81 — — 31 20 41 — — — — — A2；
——xy=20 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3；
——xy=21 3B F0 13 00 00 91 81 — — 31 20 11 — — — — — F3；
——xy=22 3B F0 13 00 00 91 81 — — 31 20 21 — — — — — C3；
——xy=23 3B F0 13 00 00 91 81 — — 31 20 31 — — — — — D3；
——xy=24 3B F0 13 00 00 91 81 — — 31 20 41 — — — — — A3。

通过标准：终端启动下电时序或终端发送 R 块。以上动作应在未收到应答的块的最后一个字节的起始位下降沿开始的{WTX+(mxDx960)}个 etu 到{WTX+(mxDx4800)}个 etu 之内完成。

6.7.23 XYCS123-xy 等待时间扩展（WTX）超限（2）

测试目的：确保如果超出等待时间扩展（WTX）960 个 etu，终端启动下电时序。或发送 R 块（仅有一种可能）。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；交换 S（WTX）块后，卡等待“响应时间”后发送回应块；此项测试将按照表 15 TB3 值重复执行。

表 15 TB3 值

X	y	TA1	TB3	BWI	BWT（etus）[（2^{BWI} x 960 x 372D/f） +11]	WTX（etus）（=BWT x m）例如 m=3	响应时间（etus）（=WTX+m x D x 960+1）例如m=3
0	0	11或缺省（D=1）	01	0	971	2913	5794
	1		11	1	1931	5793	8674
	2		21	2	3851	11553	14434
	3		31	3	7691	23073	25954
	4		41	4	15371	46113	48994
1	0	12（D=2）	01	0	1931	5793	11554
	1		11	1	3851	11553	17314
	2		21	2	7691	23073	28834
	3		31	3	15371	46113	51874
	4		41	4	30731	92193	97954
2	0	13（D=4）	01	0	3851	11553	23074
	1		11	1	7691	23073	34594
	2		21	2	15371	46113	57634
	3		31	3	30731	92193	103714
	4		41	4	61451	184353	195874

ATR： TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——xy=00 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；
——xy=01 3B E0 — 00 00 91 81 — — 31 20 11 — — — — — F0；
——xy=02 3B E0 — 00 00 91 81 — — 31 20 21 — — — — — C0；
——xy=03 3B E0 — 00 00 91 81 — — 31 20 31 — — — — — D0；
——xy=04 3B F0 — 00 00 91 81 — — 31 20 41 — — — — — A0；
——xy=10 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；
——xy=11 3B F0 12 00 00 91 81 — — 31 20 11 — — — — — F2；
——xy=12 3B F0 12 00 00 91 81 — — 31 20 21 — — — — — C2；
——xy=13 3B F0 12 00 00 91 81 — — 31 20 31 — — — — — D2；
——xy=14 3B F0 12 00 00 91 81 — — 31 20 41 — — — — — A2；
——xy=20 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3；
——xy=21 3B F0 13 00 00 91 81 — — 31 20 11 — — — — — F3；
——xy=22 3B F0 13 00 00 91 81 — — 31 20 21 — — — — — C3；
——xy=23 3B F0 13 00 00 91 81 — — 31 20 31 — — — — — D3；

——xy=24 3B F0 13 00 00 91 81 — — 31 20 41 — — — — — A3。

通过标准：终端启动下电时序或终端发送 R 块。以上动作应在未收到应答的块的最后一个字节的起始位下降沿开始的{WTX+(mxDx960)}个 etu 到{WTX+(mxDx4800)}个 etu 之内完成。

6.7.24 XYCS124-0y 无链接的块——传输错误，之后错误通知

测试目的：确保终端正确处理一个传输错误的块，这个数据块后面跟随一个关于无链接 I 块的错误通知。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片返回有传输错误的无链接的 I 块，在接收到要求重发的 R 块后发送一错误通知（在第一个 I 块中），随后发送一个无链接的 I 块响应终端重发的 I 块；此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——y=0：奇偶校验错；

——y=1：EDC 错；

——y=2：奇偶校验/EDC 联合错；

——选项 2：

——y=0：奇偶校验/EDC 联合错；

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端发送 R 块指示收到传输错误的块，发送 I 块响应卡发送的 R 块并在收到后续的 I 块后继续卡片后续操作。

6.7.25 XYCS125-xy 无链接的块——响应 I 块时语法/语义错误，之后错误通知，再发 I 块

测试目的：确保终端正确处理语法/语义错误的数据块（无链接 I 块的响应块），这个数据块后面跟随一个关于之前无链接 I 块的错误指示，之后接收一无链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块为 R 块、I 块或 S（请求）块时，卡片返回有语法/语义错误（14 个测试案例）的块，在接收到要求重发的 R 块后发送一错误通知，随后发送一个无链接的 I 块：

——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；

——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；

——xy=02： LEN 等于 FF 的 I 块(数据块的 INF 部分的实际长度小于 255)；

——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=04：INF 小于 10 的 S（IFS 响应）块；

——xy=05：INF 等于 FF 的 S（IFS 响应）块；

——xy=06：第 6 位等于 1 的 R 块；

——xy=07：序列号错误的 R 块；

——xy=08：序列号错误的 I 块；

——xy=09：S（放弃响应）块；

——xy=10：S（WTX 响应）；

——xy=11：S（IFS 响应）；

——xy=12：S（再同步响应）块；

——xy=13：未知的 S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端发送 R 块指示收到错误的块，发送 I 块响应卡发送的各种错误的 R 块，并在收到后续的 I 块后继续卡片后续操作。对于 xy=02，允许终端因为 CWT 超限下电。

6.7.26 XYCS126-0y 无链接的块——响应 I 块时传输错误次数超限

测试目的：确保终端连续三次接收到传输错误的数据块（无链接 I 块的响应块）后行为正确。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接的 I 块时，卡连续三次返回有传输错误数据块；此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——y=0：奇偶校验错；

——y=1：EDC 错；

——y=2：奇偶校验/EDC 联合错；

——选项 2：

——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在接收到前两次错误的数据块时，终端发送两次 R 块，随后在其发送的第二个 R 块的最后一个字节的起始位下降沿开始的{BWT +（Dx14400）}个 etu 之内终端启动下电时序。如果终端支持再同步，终端允许在一接收到第三个错误的块就发送一个有效地 S 块（就是一个 NAD=‘00’,PCB=‘C0’的块）。

6.7.27 XYCS127-xy 无链接的块——响应 I 块时语法/语义错误次数超限

测试目的：确保终端连续三次收到语法/语义错误的数据块（无链接 I 块的响应块）后行为正确。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块为 R 块、I 块或 S（请求）块时，卡连续三次返回有语法/语义错误的块：

——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；

——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；

——xy=02：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；

——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=04：INF 小于 10 的 S（IFS 响应）块；

——xy=05：INF 等于 FF 的 S（IFS 响应）块；

——xy=06：第 6 位等于 1 的 R 块；

——xy=07：序列号错误的 R 块；

——xy=08：序列号错误的 I 块；

——xy=09：S（放弃响应）块；

——xy=10：S（WTX 响应）；

——xy=11：S（IFS 响应）；

——xy=12：S（再同步响应）块；

——xy=13：未知的 S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在接收到前两次错误的数据块时，终端发送两次 R 块，随后在其发送的第二个 R 块的最后一个字节的起始位下降沿开始的{BWT +（Dx14400）}个 etu 之内终端启动下电时序。

注：如果终端支持再同步，终端允许在一接收到第三个错误的块就发送一个有效地 S 块（就是一个 NAD=‘00’,PCB=‘C0’的块）。对于 xy=02，允许终端因为 CWT 超限下电/再同步。

6.7.28 XYCS128-xy 无链接的块——响应 I 块时存在一或两个传输错误，随后发送 I 块

测试目的：确保终端在收到一个或连续两个传输错误的块（无链接 I 块的响应块）后能够正确的给予响应，随后正确接收一个正确的无链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应一个无链接的 I 块时，卡

片返回一个或连续两个（y=0 或 1）有传输错误数据块，随后发送一个正确的无链接的 I 块：

——x=0：奇偶校验错；

——x=1：EDC 错；

——x=2：奇偶校验/EDC 联合错；

——y=0：一次错误；

——y=1：两次连续错误；

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的块后发送 R 块通知错误，并在收到后续的 I 块后继续卡片后续操作。

6.7.29 XYCS129-xy 无链接的块——响应 I 块时语法/语义错误，之后再发 I 块

测试目的：确保终端在收到语法/语义错误的数据块（无链接 I 块的响应块）后能够正确的给予响应，随后正确接收一个正确的无链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块为 R 块、I 块或 S（请求）块时，卡片返回有语法/语义错误的块，随后发送一个正确的无链接的 I 块：

——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；

——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；

——xy=02：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；

——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=04：INF 小于 10 的 S（IFS 响应）块；

——xy=05：INF 等于 FF 的 S（IFS 响应）块；

——xy=06：第 6 位等于 1 的 R 块；

——xy=07：序列号错误的 R 块；

——xy=08：序列号错误的 I 块；

——xy=09：S（放弃响应）块；

——xy=10：S（WTX 响应）；

——xy=11：S（IFS 响应）；

——xy=12：S（再同步响应）块；

——xy=13：未知的 S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的块后发送 R 块通知错误，并在收到后续的 I 块后继续卡片后续操作。

注：对于 xy=02，允许终端因为 CWT 超限下电。

6.7.30 XYCS130-xy 无链接的块——响应 I 块时连续两次语法/语义错误，之后再发 I 块

测试目的：确保终端连续两次接收到语法/语义错误的数据块（无链接 I 块的响应块）后能够正确的给予响应。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块为 R 块、I 块或 S（请求）块时，卡连续两次返回有语法/语义错误的块，随后再发出一正确的无链接的 I 块：

——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；

——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；

——xy=02：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；

——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=04：INF 小于 10 的 S（IFS 响应）块；

——xy=05：INF 等于 FF 的 S（IFS 响应）块；

——xy=06：第 6 位等于 1 的 R 块；
——xy=07：序列号错误的 R 块；
——xy=08：序列号错误的 I 块；
——xy=09：S（放弃响应）块；
——xy=10：S（WTX 响应）；
——xy=11：S（IFS 响应）；
——xy=12：S（再同步响应）块；
——xy=13：未知的 S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的块后发送 R 块通知错误，并在收到后续的 I 块后继续卡片后续操作。

注：对于 xy=02，允许终端因为 CWT 超限下电。

6.7.31 XYCS1310y 无链接的块——响应 I 块时传输错误，随后发送错误通知的 R 块，再发送正确的 I 块

测试目的：确保终端能正确处理接收到的传输错误的数据块（无链接 I 块的响应块），随后接收关于之前 R 块的错误通知，再接收一个 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接的 I 块时，卡片返回有传输错误的数据块，随后在响应后续的 R 块时发出错误通知，再发送一个正确的无链接的 I 块。此项测试可使用以下的 1 或 2 选项执行：

——选项 1：
——y=0：奇偶校验错；
——y=1：EDC 错；
——y=2：奇偶校验/EDC 联合错；
——选项 2：
——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的块后发送 R 块通知错误，之后收到卡片发送的 R 块后再次重复通知错误的 R 块，并在收到后续的 I 块后继续卡片后续操作。

6.7.32 XYCS132-xy 无链接的块——响应 I 块时语法/语义错误，随后发送错误通知的 R 块，再发送正确的 I 块

测试目的：确保终端能正确处理接收到的语法/语义错误的数据块（无链接 I 块的响应块），随后接收关于前一个 R 块的错误通知，再接收一个 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块为 R 块、I 块或 S（请求）块时，卡片返回有语法/语义错误（14 个测试案例）的块，随后返回一个 R 块指示终端发送的 R 块不正确：

——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；
——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；
——xy=02：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；
——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；
——xy=04：INF 小于 10 的 S（IFS 响应）块；
——xy=05：INF 等于 FF 的 S（IFS 响应）块；
——xy=06：第 6 位等于 1 的 R 块；
——xy=07：序列号错误的 R 块；
——xy=08：序列号错误的 I 块；
——xy=09：S（放弃响应）块；
——xy=10：S（WTX 响应）；

——xy=11：S（IFS 响应）；
——xy=12：S（再同步响应）块；
——xy=13：未知的 S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的块后发送 R 块，之后收到卡片发送的 R 块后再次重复通知错误的 R 块，并在收到后续的 I 块后继续卡片后续操作。

注：对于xy=02，允许终端因为CWT超限下电。

6.7.33 XYCS133-0y 无链接的块——响应 I 块时连续两次传输错误，随后发送错误通知

测试目的：确保终端连续两次接收到传输错误的数据块（无链接 I 块的响应块）后能够给予正确的处理，随后接收错误通知。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接的 I 块时，卡连续两次返回有传输错误的数据块，随后发送错误通知：

此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

以下的所有错误都会生成，并且两个错误的块不包括相同的两个错，因此，将执行两次以生成以下错误（第一个块奇偶校验错，第二个块 EDC 错；随后循环第一个块 EDC 错，第二个块奇偶校验错）。

——y=0：奇偶校验错；
——y=1：EDC 错；
——y=2：奇偶校验/EDC 联合错；
——选项 2：
——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的块后发送 R 块通知错误，之后收到卡片发送的 R 块后再次重复通知错误的 R 块，并在收到后续的 I 块后继续卡片后续操作。

6.7.34 XYCS134-00 无链接的块——响应 I 块时连续两次语法/语义错误，随后发送错误通知

测试目的：确保终端连续两次接收到语法/语义错误的数据块（无链接 I 块的响应块）后能够给予正确的处理，随后接收关于前一个 R 块的错误通知，再接收一个正确的无链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块为 R 块、I 块或 S（请求）块时，卡片连续两次返回有语法/语义错误的块，随后发送一个错误通知，再发送一个无链接的 I 块：

——NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；
——LEN 不等于 0 的 R 块（INF 大小等于 LEN）；
——LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；
——INF 小于 10 的 S（IFS 响应）块；
——INF 等于 FF 的 S（IFS 响应）块；
——第 6 位等于 1 的 R 块；
——序列号错误的 R 块；
——序列号错误的 I 块；
——S（WTX 响应）；
——S（IFS 响应）；
——S（再同步响应）块；
——S（放弃响应）块；
——未知的 S（请求）；

——LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的块后发送 R 块，之后收到卡片发送的 R 块后再次重复通知错误的 R 块，并在收到后续的 I 块后继续卡片后续操作。当接收到 LEN 等于 FF 的 I 块时，允许终端因为 CWT 超限下电。

6.7.35 XYCS135-0y 无链接的块——响应 S（IFS 响应）块时传输错误，随后发送 I 块

测试目的：确保终端接收到传输错误的数据块（S（IFS 响应）块的后续块）后能够给予正确的处理，随后接收一个无链接的块，并正确响应。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接的 I 块时，卡片发送一个 S（IFS 请求）块，随后在响应 S（IFS 响应）块时发送一传输错误的数据块，再发送一无链接的 I 块：此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——y=0：奇偶校验错；

——y=1：EDC 错；

——y=2：奇偶校验/EDC 联合错；

——选项 2：

——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在实现 IFSC 改变后，终端接收到错误的块，随后发送 R 块通知错误，并在收到有效 I 块时继续卡片后续操作。

6.7.36 XYCS136-xy 无链接的块——响应 S（IFS 响应）块时语法/语义错误，随后发送 I 块

测试目的：确保终端接收到语法/语义错误的数据块（S（IFS 响应）块的响应块）后能够给予正确的处理，随后接收一个无链接的块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接的 I 块时，卡片发送一个 S（IFS 请求）块；当期望响应 S（IFS 响应）块的数据块为 I 块或 S（请求）块时，卡片返回有语法/语义错误（12 个测试案例）的块，随后发送一个无链接的 I 块：

——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；

——xy=01：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；

——xy=02：序列号错误的 I 块；

——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=04：INF 小于 10 的 S（IFS 响应）块；

——xy=05：INF 等于 FF 的 S（IFS 响应）块；

——xy=06：任意 R 块；

——xy=07：S（WTX 响应）；

——xy=08：S（IFS 响应）；

——xy=09：S（再同步响应）块；

——xy=10：S（Abort 响应）；

——xy=11：未知的 S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在实现 IFSC 改变后，终端接收到错误的块，随后发送 R 块通知错误，并在收到有效 I 块时继续卡片后续操作。

注：当 xy=01 时，允许终端因为 CWT 超限下电。

6.7.37 XYCS137-0y 无链接的块—响应 S（IFS 响应）块时传输错误，随后发送错误通知，之后 I 块

测试目的：确保终端正确处理接收到的传输错误的数据块，随后依次接收关于之前 R 块的错误通知和一个无链接的块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接 I 块时，卡片发送一个 S（IFS 请求）块，之后在响应 S（IFS 响应）块时发送一传输错误（两个选项）的数据块，再依次发送一通知错误的 R 块和一无链接的数据块：

此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——y=0：奇偶校验错；

——y=1：EDC 错；

——y=2：奇偶校验/EDC 联合错；

——选项 2：

——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在实现 IFSC 改变后，终端接收到错误的块时发送 R 块通知错误，随后接收到卡片发送的 R 块终端重复发送原 R 块，并在收到有效 I 块后继续卡片后续操作。

6.7.38 XYCS138-xy 无链接的块——响应 S（IFS 响应）块时语法/语义错误，随后发送错误通知，之后 I 块

测试目的：确保终端依次正确处理接收到的语法/语义错误的数据块，对先前 R 块的错误通知和一个无链接的块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接的 I 块时，卡片发送一个 S（IFS 请求）块；当期望响应 S（IFS 响应）块的数据块为 I 块或 S（请求）块时，卡片返回有语法/语义错误（12 个测试案例）的块，再依次发送一通知错误的 R 块和一无链接的 I 块：

——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；

——xy=01：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；

——xy=02：序列号错误的 I 块；

——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=04：INF 小于 10 的 S（IFS 响应）块；

——xy=05：INF 等于 FF 的 S（IFS 响应）块；

——xy=06：任意 R 块；

——xy=07：S（WTX 响应）；

——xy=08：S（IFS 响应）；

——xy=09：S（再同步响应）块；

——xy=10：S（Abort 响应）；

——xy=11：未知的 S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在实现 IFSC 改变后，终端接收到错误的块时发送 R 块通知错误，随后接收到卡片发送的 R 块后终端重复发送原 R 块，并在收到有效 I 块后继续卡片后续操作。

注：当xy=01时，允许终端因为CWT超限下电。

6.7.39 XYCS139-00 无链接的块——关于 I 块的错误通知，之后发送 I 块

测试目的：确保终端正确处理指示 I 块错误的通知，随后接收一个无链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片通知之前收到的无链接 I 块不正确，随后发送一个无链接的 I 块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端在接收到通知错误的 R 块后重发 I 块，并在收到后续有效 I 块后继续卡片后续操作。

6.7.40 XYCS140-00 无链接的块——连续两次关于 I 块的错误通知，之后发送 I 块

测试目的：确保终端正确处理连续两次指示 I 块错误的通知，随后接收一个无链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片连续两次指示收到的无链接 I 块不正确（在第一次错误通知后卡片应该保持接收模式），随后发送一个无链接的 I 块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端在连续两次接收到通知错误的 R 块后均重发 I 块，并在收到后续有效 I 块后继续卡片后续操作。

6.7.41 XYCS141-00 无链接的块——关于 I 块的错误通知次数超限

测试目的：确保终端在连续三次发送相同的 I 块但没有得到有效的响应后，能够行为正确。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片连续三次指示收到的无链接 I 块不正确（在第一次错误通知后卡片应该保持接收模式）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到 R 块后两次重发 I 块，并在终端发送的最后一个块的最后一个字节起始位下降沿开始的{BWT+（Dx14400）}个 etu 内启动下电时序。

注：如果终端支持再同步，终端允许在一接收到第三个错误的块就发送一个有效地 S 块（就是一个 NAD=‘00’，PCB=‘C0’的块）。接收到三次连续的 R 块后终端应下电/再同步。

6.7.42 XYCS142-0y 无链接的块——响应 I 块时传输错误，随后发送 S（IFS 请求）

测试目的：确保终端正确处理传输错误的数据块，之后接收 S（IFS 请求）块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接数据块时，卡片发送一个传输错误的数据块，随后发送一个 S（IFS 请求）块；此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——y=0：奇偶校验错；

——y=1：EDC 错；

——y=2：奇偶校验/EDC 联合错；

——选项 2：

——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端发送一个指示错误数据块的 R 块，随后接收到正确的 S（IFS 请求）块后发送 S（IFS 响应）块。

6.7.43 XYCS143-xy 无链接的块——响应 I 块时语法/语义错误，随后发送 S（IFS 请求）

测试目的：确保终端正确处理卡片响应无链接 I 块时发送的语法/语义错误的块，之后接收 S（IFS 请求）块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块

为R块、I块或S（请求）块时，卡片返回有语法/语义错误（14个测试案例）的块，再发送一正确的S（IFS请求）块：

——xy=00：NAD错的R块、I块或S（请求）块（除非ICS文档支持）；

——xy=01：LEN等于FF的I块（数据块的INF部分的实际长度小于255）；

——xy=02：LEN不等于0的R块（INF大小等于LEN）；

——xy=03：LEN不等于01的S（请求）块（INF大小等于LEN）；

——xy=04：INF小于10的S（IFS响应）块；

——xy=05：INF等于FF的S（IFS响应）块；

——xy=06：序列号错误的I块；

——xy=07：序列号错误的R块；

——xy=08：第6位等于1的R块；

——xy=09：未知的S（请求）；

——xy=10：S（WTX响应）；

——xy=11：S（IFS响应）；

——xy=12：S（放弃响应）块；

——xy=13：S（再同步响应）块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端发送一个指示错误数据块的R块，随后接收到正确的S（IFS请求）块后发送S（IFS响应）块。

注：对于xy=01，允许终端因为CWT超限下电。

6.7.44 XYCS144-00 无链接的块——关于S（IFS请求）块的错误通知，之后发送S（IFS响应）块

测试目的：确保终端正确处理指示S（IFS请求）块错误的通知，随后接收一个S（IFS响应）块。

测试条件：正常温度、最高温度；ATR调用T=1协议；卡片通知之前收到的S（IFS请求）块不正确，随后发送一个S（IFS响应）块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端在接收到通知错误的R块后重发S（IFS请求）块，并在收到S（IFS响应）块后继续卡片后续操作。

6.7.45 XYCS145-0y 无链接的块——响应S（IFS请求）块时传输错误，随后发送S（IFS响应）

测试目的：确保终端正确处理卡片响应S（IFS请求）块时发送的传输错误的数据块，紧接着接收S（IFS响应）块。

测试条件：正常温度、最高温度；ATR调用T=1协议；在响应S（IFS请求）块时，卡片发送一个传输错误的数据块，随后返回一个S（IFS响应）块。此项测试可使用以下的1或2选项执行：

——选项1：

——y=0：奇偶校验错；

——y=1：EDC错；

——y=2：奇偶校验/EDC联合错；

——选项2：

——y=0：奇偶校验/EDC联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端重发S（IFS请求）块并在接收到后续的S（IFS响应）块后继续卡片后

续操作。

6.7.46 XYCS146-xy 无链接的块——响应 S（IFS 请求）块时语法/语义错误，随后发送 S（IFS 响应）

测试目的：确保终端正确处理卡片响应 S（IFS 请求）块时发送的语法/语义错误的块，之后接收 S（IFS 响应）块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应 S（请求）块的数据块为 R 块、S（响应）块时，卡片返回有语法/语义错误的块，之后再返回一 S（IFS 响应）块：

——xy=00：NAD 错的 S（响应）块或 R 块（除非 ICS 文档支持）；

——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；

——xy=02：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=03：INF 不等于 FE 的 S（IFS 响应）块；

——xy=04：序列号错误的 R 块；

——xy=05：第 6 位等于 1 的 R 块；

——xy=06：任意 I 块；

——xy=07：未知的 S（响应）；

——xy=08：S（WTX 响应）；

——xy=09：S（IFS 响应）；

——xy=10：S（放弃响应）块；

——xy=11：S（再同步响应）块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 80 01 — — — — — D1。

通过标准：终端重发 S（IFS 请求）块并在接收到后续的 S（IFS 响应）块后继续卡片后续操作。

6.7.47 XYCS147-00 无链接的块——关于 S（IFS 响应）块的错误通知，之后发送 I 块

测试目的：确保终端正确处理指示 S（IFS 响应）块错误的通知，随后接收一个无链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；响应终端的无链接 I 块，卡片发送一个 S（IFS 请求）块，在终端返回 S（IFS 响应）块后卡片通知错误（通过重复发送 S（IFS 请求）块的方式），随后响应终端重复发送的 S（IFS 响应）块，卡片再发送一个无链接的 I 块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到重发 S（IFS 请求）块后再次发送 S（IFS 响应）块，并在收到后续 I 块后继续卡片后续操作。

6.7.48 XYCS148-xy 无链接的块——响应 I 块时一个或连续两个传输错误，随后发送 S（WTX 请求）块

测试目的：确保终端接收到一个或连续两个传输错误的数据块（无链接 I 块的响应块）后能够给予正确的处理，随后接收一个 S（WTX 请求）块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接的 I 块时，卡片返回一个或两个（y=0 或 y=1）传输错误的数据块，再发送一正确的 S（WTX 请求）块：

此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——x=0：奇偶校验错；

——x=1：EDC 错；

——x=2：奇偶校验/EDC 联合错；

——选项 2：
——x=0：奇偶校验/EDC 联合错；
此项测试将按照错误数据块的不同个数重复执行：
——y=0：生成一个错误；
——y=1：生成两个错误；
接收到 S（WTX 响应）块后，卡片等待大于 BWT 小于 BWT 扩展的时间，随后发送下一个 I 块（扩展等待时间=BWTxm）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B A0 — 00 — 81 — — — 31 20 21 — — — — — 11。

通过标准：对每一个错误的数据块终端发送 R 块通知错误，随后接收到 S（WTX 请求）块后发送 S（WTX 响应）块，并接受卡片使用 WTX 扩展。

6.7.49 XYCS149-xy 无链接的块——响应 I 块时语法/语义错误，随后发送 S（WTX 请求）块

测试目的：确保终端接收到语法/语义错误的数据块（无链接 I 块的响应块）后能够给予正确的处理，随后接收一个 S（WTX 请求）块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块为 R 块、I 块或 S（请求）块时，卡片返回有语法/语义错误的块，再发送一正确的 S（WTX 请求）块：
——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；
——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；
——xy=02：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；
——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；
——xy=04：INF 小于 10 的 S（IFS 响应）块；
——xy=05：INF 等于 FF 的 S（IFS 响应）块；
——xy=06：第 6 位等于 1 的 R 块；
——xy=07：序列号错误的 R 块；
——xy=08：序列号错误的 I 块；
——xy=09：S（WTX 响应）；
——xy=10：S（IFS 响应）；
——xy=11：S（放弃响应）块；
——xy=12：S（再同步响应）块；
——xy=13：未知的 S（请求）；
接收到 S（WTX 响应）块后，卡片等待大于 BWT 小于 BWT 扩展的时间，随后发送下一个 I 块（扩展等待时间=BWTxm）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B A0 — 00 — 81 — — — 31 20 21 — — — — — 11。

通过标准：对每一个错误的数据块终端发送 R 块通知错误，随后接收到 S（WTX 请求）块后发送 S（WTX 响应）块，并接受卡片使用 WTX 扩展。
注：对于 xy=02，允许终端因为 CWT 超限下电。

6.7.50 XYCS150-xy 无链接的块——响应 I 块时连续两次语法/语义错误，随后发送 S（WTX 请求）块

测试目的：确保终端连续两次接收到语法/语义错误的数据块（无链接 I 块的响应块）后能够给予正确的处理，随后接收一个 S（WTX 请求）块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应无链接 I 块的数据块为 R 块、I 块或 S（请求）块时，卡两次返回有语法/语义错误的块，再发送一正确的 S（WTX 请求）块：
——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；
——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；

——xy=02：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；
——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；
——xy=04：INF 小于 10 的 S（IFS 响应）块；
——xy=05：INF 等于 FF 的 S（IFS 响应）块；
——xy=06：第 6 位等于 1 的 R 块；
——xy=07：序列号错误的 R 块；
——xy=08：序列号错误的 I 块；
——xy=09：S（WTX 响应）；
——xy=10：S（IFS 响应）；
——xy=11：S（放弃响应）块；
——xy=12：S（再同步响应）块；
——xy=13：未知的 S（请求）；
接收到 S（WTX 响应）块后，卡片等待大于 BWT 小于 BWT 扩展的时间，随后发送下一个 I 块（扩展等待时间=BWTxm）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B A0 — 00 — 81 — — — 31 20 21 — — — — — 11。

通过标准：对每一个错误的数据块终端发送 R 块通知错误，随后接收到 S（WTX 请求）块后发送 S（WTX 响应）块，并接受卡片使用 WTX 扩展。
注：对于 xy=02，允许终端因为 CWT 超限下电。

6.7.51 XYCS151-00 无链接的块——关于 S（WTX 响应）块的错误通知

测试目的：确保终端正确处理指示 S（WTX 响应）块错误的通知，并在接收后续的无链接 I 块时执行等待时间扩展。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；响应终端的无链接 I 块，卡片发送一个 S（WTX 请求）块，然后再重复发送这个 S（WTX 请求）块以通知终端发出的 S（WTX 响应）块不正确。接收到终端第二次发送的 S（WTX 响应）块后，卡片等待大于 BWT 小于 BWT 扩展的时间，随后发送下一个 I 块（扩展等待时间=BWTxm）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B A0 — 00 — 81 — — — 31 20 31 — — — — — 01。

通过标准：终端接收到重发的 S（WTX 请求）块后再次发送 S（WTX 响应）块，并在收到后续 I 块后执行等待时间扩展、继续卡片后续操作。

6.7.52 XYCS152-0y 终端带链接——响应 I 块时传输错误

测试目的：确保终端正确处理传输错误的块（带链接 I 块的响应块），之后接收一个 R 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应带链接的 I 块时，卡片返回有传输错误的数据块，随后在终端发送指示错误的 R 块后卡片返回一个 R 块确认以前的 I 块：
此项测试可使用以下的 1 或 2 选项执行：
——选项 1：
——y=0：奇偶校验错；
——y=1：EDC 错；
——y=2：奇偶校验/EDC 联合错；
——选项 2：
——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端发送 R 块指示收到传输错误的块，并在收到后续的 R 块后继续卡片后续操作。

6.7.53 XYCS153-xy 终端带链接——响应 I 块时语法/语义错误

测试目的：确保终端正确处理语法/语义错误的 R 块（带链接 I 块的响应块），之后接收一个 R 块以确认之前收到的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应带链接的 I 块的数据块为 R 块、S（请求）块时，卡片返回有语法/语义错误的块，之后再发送一个 R 块以响应终端指示错误的 R 块：

——xy=00：NAD 错的 S（请求）块或 R 块（除非 ICS 文档支持）；

——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；

——xy=02：第 6 位等于 1 的 R 块；

——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=04：INF 小于 10 的 S（IFS 响应）块；

——xy=05：INF 等于 FF 的 S（IFS 响应）块；

——xy=06：S（放弃响应）块；

——xy=07：S（WTX 响应）；

——xy=08：S（IFS 响应）；

——xy=09：S（再同步响应）块；

——xy=10：未知的 S（响应）；

——xy=11：I 块（序列号等于期望终端返回的下一个带链接的 I 块的序列号）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端发送 R 块指示收到传输错误的块，并在收到后续的 R 块后继续卡片后续操作。

6.7.54 XYCS154-0y 终端带链接——响应 I 块时传输错误次数超限

测试目的：确保终端连续三次接收到传输错误的数据块（带链接 I 块的响应块）后行为正确。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应带链接的 I 块时，卡连续三次返回有传输错误数据块。

此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——y=0：奇偶校验错；

——y=1：EDC 错；

——y=2：奇偶校验/EDC 联合错；

——选项 2：

——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在接收到前两次错误的数据块时，终端发送两次 R 块，并随后在其发送的第二个 R 块的最后一个字节的起始位下降沿开始的{BWT +（Dx14400）}个 etu 之内终端启动下电时序。如果终端支持再同步，终端允许在一接收到第三个错误的块就发送一个有效地 S 块（就是一个 NAD=‘00’,PCB=‘C0’的块）。

6.7.55 XYCS155-xy 终端带链接——响应 I 块时语法/语义错误次数超限

测试目的：确保终端连续三次收到语法/语义错误的数据块（带链接 I 块的响应块）后行为正确。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应带链接的 I 块的数据块为 R 块、S（请求）块时，卡片连续三次返回有语法/语义错误的数据块：

——xy=00：NAD 错的 S（请求）块或 R 块（除非 ICS 文档支持）；

——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；
——xy=02：第 6 位等于 1 的 R 块；
——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；
——xy=04：INF 小于 10 的 S（IFS 响应）块；
——xy=05：INF 等于 FF 的 S（IFS 响应）块；
——xy=06：S（放弃响应）块；
——xy=07：S（WTX 响应）；
——xy=08：S（IFS 响应）；
——xy=09：S（再同步响应）块；
——xy=10：未知的 S（响应）；
——xy=11：I 块（序列号等于期望终端返回的下一个带链接的 I 块的序列号）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在接收到前两次错误的数据块时，终端发送两次 R 块，并随后在其发送的第二个 R 块的最后一个字节的起始位下降沿开始的{BWT +（Dx14400）}个 etu 之内终端启动下电时序。

注：如果终端支持再同步，终端允许在一接收到第三个错误的块就发送一个有效地S块（就是一个NAD='00',PCB='C0'的块）。

6.7.56 XYCS156-00 终端带链接——关于 I 块的错误通知次数超限

测试目的：确保终端连续三次发送数据块但没有得到有效的响应后，能够行为正确。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在接收到终端带链接的 I 块后，卡片连续四次返回 R 块以指示错误。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到 R 块后两次重发 I 块，并在终端请求的最后一个块的最后一个字节起始位下降沿开始的{BWT+（Dx14400）}个 etu 内启动下电时序。

注：如果终端支持再同步，终端允许在一接收到第三个错误的块就发送一个有效地 S 块（就是一个 NAD=‘00’,PCB=‘C0’的块）。接收到三次连续的 R 块后终端应下电/再同步。

6.7.57 XYCS157-0y 终端带链接——接收到 S（放弃请求）块

测试目的：确保终端接收到 S（放弃请求）块后启动下电时序。

测试条件：如果 ICS 文档没有指明终端支持放弃请求，此项测试执行；正常温度、最高温度；ATR 调用 T=1 协议；响应终端发送的带链接的数据块，卡片发送一个 S（放弃请求）块。

此项测试考虑三个 D 值：
——y=0：D=1；
——y=1：D=2；
——y=2：D=4。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。
——y=0 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；
——y=1 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；
——y=2 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3。

通过标准：终端在接收到 S（放弃请求）块的最后一个字节起始位下降沿开始的（Dx9600）个 etu 内启动下电时序。

6.7.58 XYCS158-00 链接——关于 R 块的错误通知

测试目的：确保终端在链接中正确响应关于 R 块的错误通知。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片向终端发送带链接的数据块，之后返回一个 R 块指明终端确认前一个带链接 I 块的 R 块不正确，接着发送下一个带链接的 I 块。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到 R 块后重发 R 块，并在收到后续带链接的 I 块后继续卡片后续操作。

6.7.59 XYCS159-00 链接——响应 R 块时传输错误，随后发送 I 块

测试目的：确保终端在链接中正确响应传输错误的数据块（R 块的响应块），随后接收一个带链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；卡片在接收到确认前一个带链接 I 块的 R 块后返回一传输错误的数据块，接着发送下一个带链接的 I 块；

此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——y=0：奇偶校验错；

——y=1：EDC 错；

——y=2：奇偶校验/EDC 联合错；

——选项 2：

——y=0：奇偶校验/EDC 联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的数据块后重发 R 块，并在收到后续带链接的 I 块后继续卡片后续操作。

6.7.60 XYCS160-xy 无链接的块——响应 R 块时语法/语义错误，随后发送 I 块

测试目的：确保终端在链接中正确响应语法/语义错误的数据块（R 块的响应块），随后接收一个带链接的 I 块。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应 R 块（用于确认前一个带链接的 I 块）的数据块为 R 块、I 块或 S（请求）块时，卡片返回有语法/语义错误的数据块，随后发送一个带链接的 I 块：

——xy=00：NAD 错的 R 块、I 块或 S（请求）块（除非 ICS 文档支持）；

——xy=01：LEN 不等于 0 的 R 块（INF 大小等于 LEN）；

——xy=02：LEN 等于 FF 的 I 块（数据块的 INF 部分的实际长度小于 255）；

——xy=03：LEN 不等于 01 的 S（请求）块（INF 大小等于 LEN）；

——xy=04：INF 小于 10 的 S（IFS 响应）块；

——xy=05：INF 等于 FF 的 S（IFS 响应）块；

——xy=06：第 6 位等于 1 的 R 块；

——xy=07：序列号错误的 R 块；

——xy=08：序列号错误的 I 块；

——xy=09：S（放弃响应）块；

——xy=10：S（WTX 响应）；

——xy=11：S（IFS 响应）；

——xy=12：S（再同步响应）块；

——xy=13：未知的 S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误的数据块后重发 R 块，并在收到后续带链接的 I 块后继续卡片后续操作。

注：对于xy=02，允许终端因为CWT超限下电。

6.7.61 XYCS161-0y 双向链接——关于链的最后一块的错误通知，随后在卡片链接中两个传输错误

测试目的：确保终端正确处理链的最后一块的错误通知，之后在卡片链接中依次接收一个传输错误的数据块，响应R块时另一个传输错误的数据块。

测试条件：正常温度、最高温度；ATR调用T=1协议；卡片通知链的最后一块不正确，并在响应重发的I块时返回传输错误的数据块；终端请求重发，卡片依次发送一个正确的带链接I块的第一块、有传输错误的数据块；最后卡片发送正确的链的最后一块：

此项测试可使用以下的1或2选项执行：

——选项1：

——y=0：奇偶校验错；

——y=1：EDC错；

——y=2：奇偶校验/EDC联合错；

——选项2：

——y=0：奇偶校验/EDC联合错。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误通知后重发链的最后一块，之后接收到每个错误的数据块均返回R块，并在收到带链接I块的最后一块后继续卡片后续操作。

6.7.62 XYCS162-xy 双向链接——关于链的最后一块的错误通知，随后在卡片链接中两个语法/语义错误

测试目的：确保终端正确处理链的最后一块的错误通知，之后接收语法/语义错误的带链接的数据块。

测试条件：正常温度、最高温度；ATR调用T=1协议；卡片通知链的最后一块不正确。当期望响应重发的I块的数据块为R块、I块或S（请求）块时，卡片返回语法/语义错误的数据块（14个测试案例）；终端请求重发，卡片依次发送一个正确的带链接I块的第一块、有语法/语义错误的数据块（14个测试案例）；最后卡片发送正确的链的最后一块：

——xy=00：NAD错的R块、I块或S（请求）块（除非ICS文档支持）；

——xy=01：LEN不等于0的R块（INF大小等于LEN）；

——xy=02：LEN等于FF的I块（数据块的INF部分的实际长度小于255）；

——xy=03：LEN不等于01的S（请求）块（INF大小等于LEN）；

——xy=04：INF小于10的S（IFS响应）块；

——xy=05：INF等于FF的S（IFS响应）块；

——xy=06：第6位等于1的R块；

——xy=07：序列号错误的R块；

——xy=08：序列号错误的I块；

——xy=09：S（放弃响应）块；

——xy=10：S（WTX响应）；

——xy=11：S（IFS响应）；

——xy=12：S（再同步响应）块；

——xy=13：未知的S（请求）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：终端接收到错误通知后重发链的最后一块，之后接收到每个错误的数据块均返回R块，并在收到带链接I块的最后一块后继续卡片后续操作。

注：对xy=02，允许终端因为CWT超限下电。

6.7.63 XYCS163-00 响应 I 块时错误次数超限，尝试再次同步

该案例已经从本文档彻底删除。

6.7.64 XYCS164-xy 终端带链接——允许下电延迟时间变化，响应 I 块时错误次数超限

测试目的：确保终端连续三次接收到无效的数据块（I 块的响应块）后能够应用正确的时间（D 和 BWT）下电（或者发送一个再同步请求）。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；当期望响应带链接 I 块的数据块为 I 块、R 块或 S（请求）块时，卡片连续三次返回错误的数据块。

此项测试包括三个 D 值：

——x=0：D=1；

——x=1：D=2；

——x=2：D=3；

此项测试包括若干个 BWT（TB3）值，见表 16 BWT 值。

表 16 BWT 值

X	y	TA1	TB3	BWI	BWT（etus）[（2^{BWI} x 960 x 372D/f） +11]	下电延迟（etus）（=BWT+ D x 14400）
0	0	11或缺省（D=1）	01	0	971	15371
	1		11	1	1931	16331
	2		21	2	3851	18251
	3		31	3	7691	22091
	4		41	4	15371	29771
1	0	12（D=2）	01	0	971	29771
	1		11	1	1931	30731
	2		21	2	3851	32651
	3		31	3	7691	39491
	4		41	4	15371	44171
2	0	13（D=4）	01	0	971	58571
	1		11	1	1931	59531
	2		21	2	3851	61451
	3		31	3	7691	65291
	4		41	4	15371	72971

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

——xy=00 3B E0 — 00 00 91 81 — — 31 20 01 — — — — — E0；

——xy=01 3B E0 — 00 00 91 81 — — 31 20 11 — — — — — F0；

——xy=02 3B E0 — 00 00 91 81 — — 31 20 21 — — — — — C0；

——xy=03 3B E0 — 00 00 91 81 — — 31 20 31 — — — — — D0；

——xy=04 3B F0 — 00 00 91 81 — — 31 20 41 — — — — — A0；

——xy=10 3B F0 12 00 00 91 81 — — 31 20 01 — — — — — E2；

——xy=11 3B F0 12 00 00 91 81 — — 31 20 11 — — — — — F2；

——xy=12 3B F0 12 00 00 91 81 — — 31 20 21 — — — — — C2；

——xy=13 3B F0 12 00 00 91 81 — — 31 20 31 — — — — — D2；

——xy=14 3B F0 12 00 00 91 81 — — 31 20 41 — — — — — A2；

——xy=20 3B F0 13 00 00 91 81 — — 31 20 01 — — — — — E3；

——xy=21 3B F0 13 00 00 91 81 — — 31 20 11 — — — — — F3；

——xy=22 3B F0 13 00 00 91 81 — — 31 20 21 — — — — — C3；

——xy=23 3B F0 13 00 00 91 81 — — 31 20 31 — — — — — D3；

——xy=24 3B F0 13 00 00 91 81 — — 31 20 41 — — — — — A3。

通过标准：终端发送两个 R 块通知前两个错误的数据块，并在其发送的第二个 R 块的最后一个字节起始位下降沿开始的{BWT+（Dx14400）}个 etu 内启动下电时序。

注：如果终端支持再同步，终端允许在一接收到第三个错误的块就发送一个有效地S块（就是一个NAD=‘00’，PCB=‘C0’的块）。

6.7.65 XYCS165-0y 无链接的块——响应 S 块（IFS 请求）时传输错误次数超限

测试目的：确保终端连续三次接收到传输错误的数据块（无链接 S 块（IFS 请求）的响应块）后行为正确。

测试条件：正常温度、最高温度；ATR 调用 T=1 协议；在响应无链接的 S 块时，卡连续三次返回有传输错误数据块；此项测试可使用以下的 1 或 2 选项执行：

——选项 1：

——y=0：奇偶校验错；

——y=1：EDC 错；

——y=2：奇偶校验/EDC 联合错；

——选项 2：

——y=0：奇偶校验/EDC 联合错；

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B E0 — 00 00 81 — — — 31 20 01 — — — — — 71。

通过标准：在接收到前两次错误的数据块时，终端重新发送 S 块，并随后在其发送的第三个 S 块的最后一个字节的起始位下降沿开始的{BWT +（Dx14400）}个 etu 之内终端启动下电时序。

注：如果终端支持再同步，终端允许在一接收到第三个错误的块就发送一个有效地S块(就是一个NAD='00',PCB='C0'的块）。

6.8 终端传输层（ZDCS）

6.8.1 ZDCS001-00 情况 1

测试目的：确保当一个情况 1 命令发出时，终端能处理命令后返回的状态码。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 1 命令从 UT 传送至 TTL。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：传输层向应用层传递正确的 RAPDU（‘9000’）。

6.8.2 ZDCS002-00 情况 2——’6C’

测试目的：确保终端正确处理响应情况 2 命令头的过程字节’6C’。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 1 命令从 UT 传送至 TTL；接收到命令头，卡片发送过程字节’6C’，随后发送第二个过程字节’Licc’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：传输层接收到‘6Cxx’后再次发送情况 2 命令头，其中 P3 设为‘xx’；向应用层传递 RAPDU。继续后续操作。

6.8.3 ZDCS003-00 情况 2——响应命令头时接收到错误状态

测试目的：确保终端接收到响应情况 2 命令头的错误状态时能够停止处理命令。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 2 命令从 UT 传送至 TTL；接收到命令头，卡片返回错误的过程字节。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：接收错误的状态字节后传输层停止处理情况 2 命令，并向应用层传递错误。

6.8.4 ZDCS004-00 情况 2——‘6C’和‘61’

测试目的：确保终端正确处理过程字节为‘61’和‘6C’的情况 2 命令。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 2 命令从 UT 传送至 TTL；接收到命令头，卡片发送过程字节‘6C Licc’；随后接收到第二个命令头

后卡片发送过程字节‘61yy’（‘yy’ 指‘01’至‘ Licc’范围中的任意值);对于至少一个命令情况 2 的命令,终端应发送至少 10 个 GET RESPONSE 命令（也就是说卡片要至少发 10 个过程字节‘61 yy’给终端）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 FF — — — — — — — — — — — — —。

通过标准:终端接收到过程字节‘6Cxx’后再次发送情况 2 命令头,其中 P3 设为‘xx’。

接收到过程字节‘61yy’后发送 GET RESPONSE 命令（其中 P3 设为小于‘yy’）,

向应用层传递 RAPDU。继续后续操作。能够通过至少 10 个 GET RESPONSE 命令来正确接收情况 2 命令的数据。

6.8.5 ZDCS005-00 情况 3——常规处理

测试目的：确保终端正确处理情况 3 命令。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 3 命令从应用层传送至终端传输层；接收到命令头，卡片发送过程字节（INS 或$\overline{\text{INS}}$）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端传输层接收到过程字节后发送数据，正确处理情况 3 命令。接收到状态字节‘9000’后继续后续操作。

6.8.6 ZDCS006-00 情况 4——正常处理

测试目的：确保终端正确处理情况 4 命令。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 4 命令从应用层传送至传输层；接收到命令头，卡片发送过程字节（INS 或$\overline{\text{INS}}$），然后一接收到数据，卡片就发送过程字节‘61yy’（‘yy’指‘01’至‘Licc’范围中的任意值）；对于至少一个命令情况 4 的命令，终端应发送至少 10 个 GET RESPONSE 命令（也就是说卡片要至少发 10 个过程字节‘61yy’给终端）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端传输层接收到过程字节后发送数据，正确处理情况 4 命令。接收到过程字节‘61 Licc’后发送 GET RESPONSE 命令（其中 P3 设为‘Licc’）。

向应用层传递 RAPDU。继续后续操作。能够通过至少 10 个 GET RESPONSE 命令来正确接收情况 4 命令的数据。

6.8.7 ZDCS007-00 情况 4——过程字节’61’

测试目的：确保终端正确处理过程字节为‘61’的情况 4 命令。

测试条件：正常温度、最高温度;ATR 调用 T=0 协议;一个情况 4 命令从 UT 传送至 TTL;接收到命令头，卡片发送过程字节（INS 或$\overline{\text{INS}}$）；随后接收到数据后卡片发送过程字节‘61yy’（‘yy’ 指‘01’至‘Licc’范围中的任意值）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端传输层接收到过程字节后发送数据，正确处理情况4命令。接收到过程字节‘61xx’后发送GET RESPONSE命令。向应用层传递RAPDU。继续后续操作。

6.8.8 ZDCS008-0y 情况 4——紧跟过程字节‘61’后的响应数据返回警告状态

测试目的：确保终端接收到警告状态（紧跟过程字节‘61’后的响应数据）时能够正确处理。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 4 命令从 UT 传送至 TTL；接收到命令头，卡片发送一过程字节（INS 或$\overline{\text{INS}}$）；随后接收到数据后卡

片发送’61 Licc’；接收到 GET RESPONSE 命令后，卡片紧跟响应数据返回警告状态：

——y=0 状态为’62xx’；

——y=1 状态为’63xx’。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

y=0&1 3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端传输层接收到过程字节后发送数据，正确处理命令。接收到过程字节‘61 Licc’后发送 GET RESPONSE 命令（其中 P3 设为‘Licc’）。向应用层传递 RAPDU。继续卡片后续操作。

6.8.9 ZDCS009-0y 情况 4——发送命令数据后接收状态码

测试目的：确保当发送命令数据后接收到状态码时，终端能正确处理情况 4 命令。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 4 命令从 UT 传送至 TTL；接收到命令头，卡片发送一过程字节（INS 或$\overline{\text{INS}}$）；随后接收到数据后卡片发送：

——y=0：正确的警告状态（‘62xx’或‘63xx’或‘9xxx’但不包括’9000’）；

——y=1：错误的警告状态（y=0 之外的其它状态码）。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：——y=0：终端传输层接收到过程字节后发送数据，正确处理情况 4 命令。

接收到状态码后发送 GET RESPONSE 命令（其中 P3 设为‘0’）。

接收到过程字节‘61 Licc’后发送 GET RESPONSE 命令（其中 P3 设为‘Licc’）。

向应用层传递 RAPDU。继续后续操作。

——y=1：终端传输层；接收到过程字节后发送数据。接收到卡片返回的状态码后停止处理命令。在以上两个案例中，接收到的状态码将无变化的映射到 RAPDU 的强制后缀上。

6.8.10 ZDCS010-0y 情况 4——紧跟过程字节‘61’后的响应数据返回错误提示

测试目的：确保终端应用层接收到错误提示状态（紧跟过程字节‘61’后的响应数据）时能够正确处理。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 4 命令从 UT 传送至 TTL；接收到命令头，卡片发送一过程字节（INS 或$\overline{\text{INS}}$）；随后接收到数据后卡片发送过程字节‘61’；接收到 GET RESPONSE 命令后，卡片返回错误状态，状态码 SW1SW2 是可变的：

——y=0 状态为‘6281’；

——y=1 状态为‘6700’；

——y=2 状态为‘6F00’；

——y=3 状态为‘6A86’；

LT/UT 层能够比较输入和输出值。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — — —。

通过标准：终端传输层接收到过程字节后发送数据，发送数据。接收到过程字节‘61xx’后发送 GET RESPONSE 命令（其中 P3 设为‘Licc’）。接收到错误状态后停止命令处理。另外，接收到的状态码将无变化的映射到 RAPDU 的强制后缀上。

6.8.11 ZDCS011-0y 情况 4——接收到数据后警告状态，GET RESPONSE 命令后错误状态

测试目的：确保终端能够正确处理以下情况：发送命令数据后接收到警告状态，之后发

送 GET RESPONSE 命令后接收到错误状态。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 4 命令从 UT 传送至 TTL；接收到命令头，卡片发送一过程字节（INS 或$\overline{\text{INS}}$）；随后接收到数据后卡片发送警告状态‘62xx’或‘63xx’；随后，接收到 GET RESPONSE 命令后，卡片发送错误状态（四种不同的错误状态）：

——y=0：‘6281’；

——y=1：‘6700’；

——y=2：‘6F00’；

——y=3：‘6A86’；

LT/UT 层能够比较输入输出值。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端传输层接收到过程字节后发送数据。接收到警告状态后发送 GET RESPONSE 命令（其中 P3 设为‘0’）。接收到卡片返回的错误状态后停止处理命令。此外，状态码 SW1SW2 将作为 RAPDU 的强制后缀传递给应用层。

6.8.12 ZDCS012-0y 情况 2、3 或 4——命令头后返回的状态

测试目的：确保接收到响应命令头的错误状态或警告状态时，终端能够停止处理情况 2、3 或 4 命令。

测试条件：正常温度、最高温度；ATR 调用 T=0 协议；一个情况 4 命令从 UT 传送至 TTL；接收到命令头，卡片返回错误或警告状态；三个测试案例：

——y=0：情况 2 命令；

——y=1：情况 3 命令；

——y=2：情况 4 命令。

ATR：TS T0 TA1 TB1 TC1 TD1 TA2 TB2 TC2 TD2 TA3 TB3 TC3 TD3 TA4 TB4 TC4 TCK。

3B 60 — 00 00 — — — — — — — — — — — —。

通过标准：终端传输层接收到卡片返回的状态后停止处理命令，并将其传递给应用层。

7 借记贷记应用的测试案例

7.1 数据元和命令（YSML）

7.1.1 YSML001-01 数据元存储（1）

测试目的：确保取得的数据元的值存储在终端的缓冲器中，以便在稍后的应用中使用。

终端配置：N/A。

测试条件：终端接收和存储卡发送的数据元。

卡片配置：——在第一个 GENERATE AC 中，卡片响应 ARQC；

——CDOL2请求所有在AFL指定的文件中读取的数据元，不包括CDOL1、CDOL2（期望返回数据的总长度不超过256个字节）；

——CDOL请求标签为‘93’的签名的静态应用数据。

测试流程：选择卡片应用，执行交易。

通过标准：终端应批准并完成交易。卡在第二个 GENERATE AC 中接收到的数据域，应该同在读应用数据阶段存储下的值一致。Tag 标签‘93’或其他的加密数据元不应以明文的形式出现。

7.1.2 YSML001-02 数据元存储（2）

测试目的：确保取得的数据元的值存储在终端的缓冲器中，以便在稍后的应用中使用。

终端配置：N/A。

测试条件：终端接收和存储卡发送的数据元。

卡片配置：——CDOL1请求所有在AFL指定的文件中读取的数据元，不包括CDOL1、CDOL2（期望返回数据的总长度不超过256个字节）；
——CDOL1请求标签为‘93’的签名的静态应用数据；
——卡中的参数应设置以确保交易是脱机批准的。
测试流程：选择卡片应用，执行交易。
通过标准：卡在第一个GENERATE AC中接收到的数据域，应该同在读取应用数据阶段存储下的值一致。

7.1.3 YSML001-03 数据元存储

测试目的：确保取得的数据元的值存储在终端的缓冲器中，以便在稍后的应用中使用。
终端配置：支持批数据捕获、支持仅脱机或者支持脱机/联机。
测试条件：终端接收和存储卡发送的数据元。
卡片配置：设置卡片发送的数据，确保交易被批准。
测试流程：选择卡片应用，执行交易。
通过标准：终端应批准并完成交易。当批数据捕获或联机数据捕获时，储存在终端缓冲器中的数据应该与卡发送的数据一致。

7.1.4 YSML001-04 TLV中长度的编码

测试目的：确保终端能够正确的识别TLV数据对象中以‘00’为编码的长度域（在ISO/IEC 7816中定义）。以‘00’为长度的数据元应被认为不存在。
终端配置：N/A。
卡片配置：卡文件记录中包含一个长度域编码为‘00’的数据对象。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该认为该数据不存在，并通过请求一个TC或AAC来完成交易。

7.1.5 YSML002-00 数据对象到记录的映射

测试目的：确保终端能够接受任何从数据对象到记录的映射。
终端配置：N/A。
卡片配置：——卡中的数据对象被映射到不同的记录中（与AFL保持一致性）（例如：二磁道等价数据能够被存放在任意SFI的文件中）；
——卡中的数据对象在记录中排列顺序是不同的（例如：失效日期、PAN、CDOL1、CDOL2等必备数据对象能够以不同的顺序排列）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该正确完成读取应用数据阶段，通过请求一个TC或AAC来完成交易。数据对象应该以正确的值存储在终端里（随时可能使用这些值）。

7.1.6 YSML004-00 支付系统目录的编码：SFI范围（1）

测试目的：——确保如果终端支持PSE选择，它应该接受目录文件的SFI在1到10的任何值；
——确保如果终端支持PSE选择，它应该能够正确获取目录文件。
终端配置：支持支持PSE。
卡片配置：卡包含一个PSE。
子类案例：——案例01：选择PSE后，卡返回的FCI中的SFI是1；
——案例02：选择PSE后，卡返回的FCI中的SFI是2；
——案例03：选择PSE后，卡返回的FCI中的SFI是3；
——案例04：选择PSE后，卡返回的FCI中的SFI是4；
——案例05：选择PSE后，卡返回的FCI中的SFI是5；
——案例06：选择PSE后，卡返回的FCI中的SFI是6；
——案例07：选择PSE后，卡返回的FCI中的SFI是7；
——案例08：选择PSE后，卡返回的FCI中的SFI是8；

——案例 09：选择 PSE 后，卡返回的 FCI 中的 SFI 是 9；
——案例 10：选择 PSE 后，卡返回的 FCI 中的 SFI 是 10。
测试流程：对所有的情况来说，使用PSE选择卡片应用，执行交易。
通过标准：对所测试的每一个 SFI，卡都应收到一个读记录命令，读相应的目录文件。

7.1.7 YSML013-00 DOL 的处理：未知标签（1）

测试目的：验证当DOL中指定出的数据对象的标签无法被终端识别时，终端应提供一个长度为DOL指定长度的数据单元，并应把该数据单元所有的数值部分设置为16进制的0。
终端配置：N/A。
子类案例：——案例 01：卡的PDOL中包含一个数据对象，该对象的标签终端无法识别；
——案例 02：卡的 CDOL1 中包含一个数据对象，该对象的标签终端无法识别；
——案例 03：卡的 CDOL2 中包含一个数据对象，该对象的标签终端无法识别，并且在第一次 GENERATE AC 时卡请求返回 ARQC；
——案例 04：卡的 TDOL 中包含一个数据对象，该对象的标签终端无法识别。
测试流程：选择卡片应用，执行交易（特别是DOL的处理）。
通过标准：卡接收到的数据，代表着未知数据对象的部分用十六进制的0补齐（填充的部分与DOL中数据对象的长度相同）。

7.1.8 YSML013-01 DOL 的处理：未知标签（2）

测试目的：验证当DOL中指出指定的数据对象的标签无法被终端识别时，终端应提供一个长度为DOL指定长度的数据单元，并应把该数据单元所有的数值部分设置为16进制的0。（针对动态数据认证）。
终端配置：支持支持DDA。
卡片配置：卡的DDOL中包含一个数据对象，该对象的标签对于终端是未知的。
测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。
通过标准：终端应该发送INTERNAL AUTHENTICATE命令给卡，其中无法识别的数据对象用十六进制的0补齐（填充的部分与DOL中数据对象的长度相同）。

7.1.9 YSML014-00 DOL 的处理：结构数据对象的标签

测试目的：验证当DOL中指定的数据对象的标签表示一个结构数据对象时，终端应该根据指定的长度用十六进制全0填充。
终端配置：N/A。
子类案例：——案例 01：卡的PDOL中包含一个结构数据对象；
——案例 02：卡的 CDOL1 中包含一个结构数据对象；
——案例 03：卡的 CDOL2 中包含一个结构数据对象，并且卡在第一次 GENERATE AC 时请求返回 ARQC；
——案例 04：卡的 TDOL 中包含一个数据对象，该对象的标签对于终端是未知的。
测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。
通过标准：卡接收到的数据，代表着结构数据对象的部分 DOL 域用十六进制的 0 补齐（填充的部分与 DOL 中数据对象的长度相同）。

7.1.10 YSML014-01 DOL 的处理：结构数据对象的标签（2）

测试目的：验证当DOL中指定的数据对象的标签表示一个结构数据对象时，终端在使用动态数据验证时，应该根据指定的长度用十六进制全0填充。
终端配置：支持支持 DDA。
卡片配置：卡的DDOL中包含一个结构数据对象。
测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：终端应该发送 INTERNAL AUTHENTICATE 命令给卡，命令域中代表着结构数据对象的部分其中结构数据对象的部分 DOL 域用十六进制的 0 补齐（填充的部分与 DOL 中数据对象的长度相同）。

7.1.11 YSML015-00 DOL 的处理：IC 卡中数据的缺失（1）

测试目的：验证当DOL中指定一个可选静态数据对象，该数据对象终端可以识别，但是它在IC卡记录中未出现，命令域中应该在相应的位置填充十六进制的0。

终端配置：N/A。

子类案例：——案例01：卡在CDOL1中请求一个卡中缺失的IC卡静态数据（例如：发卡行行为代码——缺省，标签‘9F0D’）；

——案例02：卡在的CDOL2中请求一个卡中缺失的IC卡静态数据，并且卡在第一次GENERATE AC时请求返回ARQC（例如：发卡行行为代码——缺省，标签‘9F0D’）；

——案例03：卡在的TDOL中请求一个卡中缺失的IC卡静态数据（例如：发卡行行为代码——缺省，标签‘9F0D’）。

测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：卡接收到的数据，代表着缺失的可选静态数据对象的部分域用十六进制的 0 补齐（填充的部分与 DOL 中数据对象的长度相同）。

7.1.12 YSML015-01 DOL 的处理：IC 卡中数据的缺失（2）

测试目的：验证当DOL中指定一个可选静态数据对象，该数据对象终端可以识别，但是它在IC卡记录中未出现，命令域中应该在相应的位置填充十六进制的0。（使用动态数据验证）。

终端配置：支持支持DDA。

卡片配置：卡在的DDOL中请求一个卡中缺失的IC卡静态数据（例如：发卡行行为代码——缺省，标签‘9F0D’）。

测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：终端应该发送 INTERNAL AUTHENTICATE 命令给卡，命令域中代表着缺失的可选静态数据对象的部分其中代表着缺失可选静态数据对象的部分域用十六进制的 0 补齐（填充的部分与 DOL 中数据对象的长度相同）。

7.1.13 YSML016-00 DOL 的处理：长度不足的数据对象，数字的格式（1）

测试目的：验证当DOL中指出指定的长度小于数据对象的实际长度时，若该数据对象是数字（n）格式，则数据元最左端的字节将被截删去。

终端配置：N/A。

子类案例：——案例01：卡的PDOL中包含一个数据对象，该数据对象为数字格式，且其长度小于数据对象的实际长度；

——案例02：卡的CDOL1中包含一个数据对象，该数据对象为数字格式，且其长度小于数据对象的实际长度；

——案例03：卡的CDOL2中包含一个数据对象，该数据对象为数字格式，且其长度小于数据对象的实际长度。在第一次GENERATE AC时卡请求返回ARQC；

——案例04：卡的TDOL中包含一个数据对象，该数据对象为数字格式，且其长度小于数据对象的实际长度。

测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：卡接收到的数据，代表着该数据对象的数据部分，其部分长度被正确地截取（该部分的数据长度与 DOL 中规定的长度相同）。

7.1.14 YSML016-01 DOL 的处理：长度不足的数据对象，数字的格式（2）

测试目的：验证当DOL中指出的长度小于数据对象的实际长度时，若该数据对象是数字

（n）格式，则数据元最左端的字节将被截删去。

终端配置：支持支持 DDA。

卡片配置：卡的DDOL中包含一个数据对象，应用失效日期（标签为“‘5F24’”），且其长度小于数据对象的实际长度。

测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：终端应该发送一个 INTERNAL AUTHENTICATE 命令给卡，命令域中代表着该数据对象的部分，其长度被正确地截取其中代表着该数据对象的数据部分，长度被正确截取（该部分的数据长度与 DOL 中规定的长度相同）。

7.1.15 YSML017-00 DOL 的处理：长度不足的数据对象，其他的格式（1）

测试目的：验证当DOL中指出的长度小于数据对象的实际长度时，若数据对象是除数字以外的其他格式（包括压缩数字格式），则数据元最右端的字节将被截删去。

终端配置：N/A。

子类案例：——案例01：卡的PDOL中包含一些数据对象，这些该数据对象为字母数字型或字母数字及特殊字符型或压缩数字型或二进制型的格式，且其长度比数据对象的实际长度要短；

——案例02：卡的CDOL1中包含一些数据对象，该这些数据对象为字母数字型或字母数字及特殊字符型或压缩数字型或二进制型的格式，且其长度比数据对象的实际长度要短；

——案例03：卡的CDOL2中包含一些数据对象，这些该数据对象为字母数字型或字母数字及特殊字符型或压缩数字型或二进制型的格式，且其长度比数据对象的实际长度要短，并且。在第一次GENERATE AC时卡请求返回ARQC；

——案例04：卡的TDOL中包含一些数据对象，这些该数据对象为字母数字型或字母数字及特殊字符型或压缩数字型或二进制型的格式，且其长度比数据对象的实际长度要短。

测试流程：选择卡片应用，执行交易（特别是DOL的处理）。

通过标准：卡接收到的数据，代表着该数据对象的部分，其长度被正确地截取代表着该数据对象的数据部分，长度被正确地截取（该部分的数据长度与 DOL 中规定的长度相同）。

7.1.16 YSML017-01 DOL 的处理：长度不足的数据对象，其他的格式（2）

测试目的：验证当DOL中指出的长度小于数据对象的实际长度时，若数据对象是除数字以外的其他格式（包括压缩数字格式），则数据元最右端的字节将被截删去（针对动态数据认证）。

终端配置：支持支持 DDA。

卡片配置：卡的DDOL中包含一些个数据对象，该这些数据对象为字母数字型或字母数字及特殊字符型或压缩数字型或二进制型的格式，且其长度比数据对象的实际长度要短。

测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：终端应该发送一个 INTERNAL AUTHENTICATE 命令给卡，命令域中代表着该数据对象的部分，其长度被正确地截取其中代表着该数据对象的数据部分，长度被正确截取（该部分的数据长度与 DOL 中规定的长度相同）。

7.1.17 YSML018-00 DOL 的处理：长度超出的数据对象，数字的格式（1）

测试目的：验证当 DOL 中指定的长度大于数据对象的实际长度，若数据对象是数字格式，则终端应在实际数据元的最左端用十六进制的‘0’填补填充。

终端配置：N/A。

子类案例：——案例01：卡的PDOL中包含一个数据对象，该数据对象为数字格式，且其长度比数据对象的实际长度要长；

——案例02：卡的CDOL1中包含一个数据对象，该数据对象为数字格式，且其长度比数据对象的实际长度要长；
——案例03：卡的CDOL2中包含一个数据对象，该数据对象为数字格式，且其长度比数据对象的实际长度要长，并且。在第一次GENERATE AC时卡请求返回ARQC；
——案例04：卡的TDOL中包含一个数据对象，该数据对象为数字格式，且其长度比数据对象的实际长度要长。

测试流程：选择卡片应用，执行交易（特别是DOL的处理）。

通过标准：卡接收到的数据，代表着该数据对象的部分，代表着该数据对象的域应在最左端前面正确地用十六进制的‘0’填充补（该部分的数据长度该域长度与 DOL 中数据对象的长度相同）。

7.1.18 YSML018-01 DOL 的处理：长度超出的数据对象，数字的格式（2）

测试目的：验证当DOL中指定的长度大于数据对象的实际长度，若数据对象是数字格式，则终端应在实际数据元的最左端用十六进制的‘0’填补填充（针对动态数据认证）。通过使用动态数据认证验证。

终端配置：支持 DDA。

卡片配置：卡的DDOL中包含一个数据对象，应用失效日期（标签为“5F 24”），且其长度比数据对象的实际长度要长。

测试流程：选择卡片应用，执行交易（特别是DOL的处理）。

通过标准：终端应该发送 INTERNAL AUTHENTICATE 命令给卡，命令域中代表着该数据对象的部分，其中代表着该数据对象的域应在最左端正确地左侧用十六进制的‘0’填充（该部分的数据长度该域长度与 DOL 中数据对象的长度相同）。

7.1.19 YSML019-00 DOL 的处理：长度超出的数据对象，压缩数字格式（1）

测试目的：验证当DOL中指定的长度大于数据对象的实际长度，若数据对象是压缩数字格式，则终端应在数据元最右末端用十六进制的‘FF’填充填充十六进制的‘FF’。

终端配置：N/A。

子类案例：——案例01：卡的CDOL1中包含一个数据对象，该数据对象为压缩数字格式，且其长度比数据对象的实际长度要长；
——案例02：卡的CDOL2中包含一个数据对象，该数据对象为压缩数字格式，且其长度比数据对象的实际长度要长，并且。卡在第一次GENERATE AC时请求返回ARQC。

测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：卡接收到的数据，代表着该数据对象的部分，代表着该数据对象的域应在最右端正确地用十六进制的‘FF’填充正确地在末尾填充‘FF’（该部分的数据长度该域的数据长度与 DOL 中数据对象的长度相同）。

7.1.20 YSML019-01 DOL 的处理：长度超出的数据对象，压缩数字格式（2）

测试目的：验证当DOL中指定的长度大于数据对象的实际长度，若数据对象是压缩数字格式，则终端应在数据元最右末端用十六进制的‘FF’填充填充十六进制的‘FF’（针对动态数据认证）。通过动态数据认证验证。

终端配置：支持 DDA。

卡片配置：卡的DDOL中包含一个数据对象，该数据对象为压缩数字格式，且其长度比数据对象的实际长度要长。

测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：终端应该发送 INTERNAL AUTHENTICATE 命令给卡，命令域中代表该数据对象的部分，应在最右端正确地用十六进制的‘FF’填充（该部分的数据长度与 DOL 中数据对象的长度相同）其中代表着该数据对象的域在末尾用十六进制的

‘FF’填充（该域长度与 DOL 中数据对象的长度相同）。

7.1.21 YSML020-00 DOL 的处理：长度超出的数据对象，其他格式（1）

测试目的：验证当DOL中指定的长度大于数据对象的实际长度，若数据对象是除数字或压缩数字格式以外的其他格式，则终端应在数据元最右端用十六进制的‘0’填充最末端填充十六进制的‘0’。

终端配置：N/A。

子类案例：——案例 01：卡的 PDOL 中包含一些数据对象，这些数据对象分别为字母数字型（接口设备序列号 9F 1E）、字母数字及特殊字符型特殊字符型（商户标识‘9F 16’）及二进制型（附加终端性能‘9F 40’）的格式（附加终端性能‘9F 40’），且其长度比数据对象的实际长度要长；

——案例 02：卡的 CDOL1 中包含一些数据对象，这些数据对象分别为字母数字型（接口设备序列号‘9F 1E’）、或字母数字及特殊字符型特殊字符型（商户标识‘9F 16’）及二进制型（交易状态信息‘9B’）的格式（交易状态信息‘9B’），且其长度比数据对象的实际长度要长；

——案例 03：卡的 CDOL2 中包含一些数据对象，这些数据对象分别为字母数字型（接口设备序列号‘9F1E’）、字母数字及特殊字符型（商户标识‘9F 16’）及二进制型（交易状态信息‘9B’）的格式，且其长度比数据对象的实际长度要长。为字母数字型（接口设备序列号‘9F1E’）、或特殊字符型（商户标识‘9F 16’）及二进制型的格式（交易状态信息‘9B’），且其长度比数据对象的实际长度要长，并且卡在第一次 GENERATE AC 时请求返回 ARQC；

——案例 04：卡的 TCDOL 中包含一些数据对象，这些数据对象分别为字母数字型（接口设备序列号‘9F1E’）、字母数字及特殊字符型（商户标识‘9F 16’）及二进制型（交易状态信息‘9B’）的格式，为字母数字型（接口设备序列号‘9F 1E’）、或特殊字符型（商户标识‘9F16’）及二进制型的格式（交易状态信息‘9B’），且其长度比数据对象的实际长度要长；

——案例 05：卡的 CDOL2 中包含一个数据对象（发卡行认证数据），其长度比数据对象的实际长度要长（发卡行认证数据的实际长度为 12 字节，CDOL2 请求的长度为 14 字节）。

测试流程：选择卡片应用，执行交易 （特别是DOL的处理）。

通过标准：卡接收到的数据，代表着该数据对象的部分，应在最右端正确地用十六进制的‘0’填充（该部分的数据长度与 DOL 中数据对象的长度相同）。代表着该数据对象的域正确地在末尾填充十六进制的‘0’（该域长度与 DOL 中数据对象的长度相同）。

7.1.22 YSML020-01 DOL 的处理：长度超出的数据对象，其他格式（2）

测试目的：验证当DOL中指定的长度大于数据对象的实际长度，若数据对象是除数字或压缩数字格式以外的其他格式，则终端应在数据元最右端用十六进制的‘0’填充最末端填充十六进制的‘0’（针对动态数据认证）。通过动态数据认证验证。

终端配置：支持 DDA。

卡片配置：卡的DDOL中包含一些个数据对象，这些该数据对象为字母数字型或字母数字及特殊字符型或二进制型的格式，且其长度比数据对象的实际长度要长。

测试流程：选择卡片应用，执行交易（特别是DOL的处理）。

通过标准：终端应该返回发送 INTERNAL AUTHENTICATE 命令给卡，命令域中代表着该数

据对象的部分，应在最右端正确地用十六进制的‘0’填充（该部分的数据长度与 DOL 中数据对象的长度相同）。其中代表着该数据对象的域正确地在末尾填充十六进制的‘0’（该域长度与 DOL 中数据对象的长度相同）。

7.1.23 YSML021-00 DOL 的处理：不适用的数据（1）

测试目的：验证当DOL中的数据对象在终端可以识别，但这些数据对象不适用于当前交易，那么代表该数据对象的命令域部分将用十六进制的‘0’填充填充16进制的‘0’。

终端配置：N/A。

卡片配置：——卡中不存在LCOL和UCOL。

子类案例：——案例01：卡在PDOL中请求LOATC；
——案例02：卡在CDOL1中请求LOATC；
——案例03：卡在CDOL2中请求LOATC；
——案例04：卡在TDOL中请求LOATC。

测试流程：选择卡片应用，执行交易（特别是DOL的处理）。

通过标准：卡接收到的数据，代表着该数据对象的部分代表着该数据对象的命令域部分用十六进制的‘0’填充（该部分的数据长度该域长度与 DOL 中数据对象的长度相同）。

7.1.24 YSML021-01 DOL 的处理：不适用的数据（2）

测试目的：验证当DOL中的数据对象在终端可以识别，但这些数据对象不适用于当前交易，那么命令域中代表该数据对象的命令域部分将用十六进制的‘0’填充（针对动态数据认证）。填充16进制的‘0’。通过动态数据认证验证。

终端配置：支持 DDA。

卡片配置：——卡中不存在LCOL和UCOL；
——卡在DDOL中请求LOATC。

测试流程：选择卡片应用，执行交易（特别是DOL的处理）。

通过标准：终端应该返回发送 INTERNAL AUTHENTICATE 命令给卡，命令域中代表着该数据对象的命令域部分用十六进制的‘0’填充（该部分的数据长度该域长度与 DOL 中数据对象的长度相同）。

7.1.25 YSML022-00 数据对象列表一致性（1）

测试目的：PDOL中请求的数据对象在应用初始化过程中是有效的，并且在整个交易过程中要保持一致。

终端配置：N/A。

卡片配置：——卡片PDOL中包含如下数据对象：终端国家代码；交易日期。
——除了缺省的值外，卡片的 CDOL1 和 CDOL2 还包括如下数据对象：终端国家代码；交易日期。
——终端行为分析的结果使终端在第一个 GENERATE AC 请求 TC 或 ARQC；
——卡片在第一个 GENERATE AC 响应返回 ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。GET PROCESSING OPTIONS 命令应该发送如下值：终端国家代码和交易日期。第一个 GENERATE AC 命令应该发送同 GET PROCESSING OPTIONS 命令一样的值：终端国家代码交易日期。第二个 GENERATE AC 命令应该发送同 GET PROCESSING OPTIONS 和第一个 GENERATE AC 命令一样的值：终端国家代码和交易日期。

7.1.26 YSML023-00 数据对象列表一致性（2）

测试目的：PDOL中请求的数据对象在应用初始化过程中是有效的，并且在整个交易过程中要保持一致。

终端配置：N/A。

卡片配置：——卡片PDOL中包含如下数据对象：附加终端性能；终端应用标识（AID）；接口设备（IFD）序列号；终端性能；终端国家代码；终端类型；交易序号；交易时间；交易日期；

——除了缺省的值外，卡片CDOL1和CDOL2还包括如下数据对象：终端附加性能；接口设备（IFD）序列号；终端性能；终端国家代码；终端类型；交易序号；交易时间；交易日期；终端应用标识（AID）— 收单行标识；

——终端行为分析结果使终端在第一个GENERATE AC请求TC或ARQC。

——卡片在第一个GENERATE AC响应返回ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：——终端应该通过请求一个 TC 或 AAC 来完成交易；

——GET PROCESSING OPTIONS 命令应该发送如下值：终端附加性能；接口设备（IFD）序列号；终端性能；终端国家代码；终端类型；交易序号；交易时间；交易日期；终端应用标识（AID—收单行标识；

——第一个 GENERATE AC 命令应该发送同 GET PROCESSING OPTIONS 命令一样的值：终端附加性能；接口设备（IFD）序列号；终端性能；终端国家代码；终端类型；交易序号；交易时间（与 GET PROCESSING OPTIONS 中发送的交易时间相同）；交易日期；终端应用标识；

——第二个 GENERATE AC 命令应该发送同 GET PROCESSING OPTIONS 和第一个 GENERATE AC 命令一样的值：终端附加性能；接口设备（IFD）序列号；终端性能；终端国家代码；终端类型；交易序号；交易时间（与 GET PROCESSING OPTIONS 中发送的交易时间相同）；交易日期；终端应用标识。

7.1.27 YSML025-00 在 AIP 中指定的 EXTERNAL AUTHENTICATE 功能的正常处理

测试目的：——确保终端接受对于EXTERNAL AUTHENTICATE命令响应正确的状态‘9000’，且终端认为它是成功的处理；

——确保终端认为卡片对外部认证命令的响应无数据域；

——确保若EXTERNAL AUTHENTICATE命令已经发给了卡，终端置TSI中的‘发卡行认证已经执行’位为‘1’；

——如果AIP中指明支持发卡行认证，确保终端执行发卡行认证。

终端配置：仅联机终端或有联机能力的脱机终端支持脱机/联机。

卡片配置：——卡的参数已经设置，确保交易是联机完成的；

——卡的AIP指明支持发卡行认证（AIP的字节1，位3为‘1’）；

——在模拟发卡行的响应中，发卡行认证数据传回给终端；

——卡应该返回状态‘9000’作为对 EXTERNAL AUTHENTICATE 命令的响应，且不返回数据域。

测试流程：选择卡片应用，执行交易（特别是联机处理和发卡行认证处理）。

通过标准：终端应该处理交易直到完成。卡应该在接收到第一个 GENERATE AC 命令后接收到 EXTERNAL AUTHENTICATE 命令。在接收到第二个 GENERATE AC 命令时，TVR 的字节 5，位 7 =‘0’（发卡行认证成功）。在接收到第二个 GENERATE AC 命令时，TSI 的字节 1，位 5 =‘1’（即发卡行认证已执行）。

7.1.28 YSML025-01 拒绝的 ARC，发卡行认证数据为批准的 ARC

测试目的：确保终端的密文请求是建立在授权或金融交易响应中的授权响应码的基础之上，而不是可能出现在发卡行认证数据中的其他数据。

终端配置：仅联机终端或有联机能力的脱机终端。

卡片配置：——卡的参数已经设置，确保交易是联机完成的；

——卡的AIP指明支持发卡行认证（AIP的字节1 ，第3位为‘1’）；

——授权或金融响应中返回拒绝的授权响应码；

——模拟的发卡行认证数据以如下格式发送给终端：一个有效的8个字节的授权响应密文和2个字节表明批准的授权响应码；
——EXTERNAL AUTHENTICATE命令将上述的发卡行认证数据发送给终端卡片；
——卡应向EXTERNAL AUTHENTICATE命令返回响应状态码‘9000’；
——CDOL2请求授权响应码（标签‘8A’）。

测试流程：选择卡片应用，执行交易（特别是联机处理和发卡行认证处理）。

通过标准：终端应该处理交易直到完成。在接收到第二个 GENERATE AC 命令时，TVR 的字节 5 位 7 =‘0’（发卡行认证成功）。在接收到第二个 GENERATE AC 命令时，TSI 的字节 1 位 5 =‘1’（发卡行认证已执行）。终端发第二个 GENERATE AC 命令请求 AAC。授权响应码应该与后台传输的一致。

7.1.29 YSML025-02 批准的 ARC，发卡行认证数据为拒绝的 ARC

测试目的：确保终端的密文请求是建立在授权或金融交易响应中的授权响应码的基础之上，而不是可能出现在发卡行认证数据中的其他数据。

终端配置：仅联机终端或有联机能力的脱机终端仅联机或支持脱机/联机。

卡片配置：——卡的参数已经设置，确保交易是联机完成的；
——卡的AIP指明支持发卡行认证；
——后台应该在授权或金融响应中返回批准；
——模拟的发卡行认证数据以如下格式发送给终端：一个有效的8字节的授权响应密文和2字节表明拒绝的授权响应码；
——EXTERNAL AUTHENTICATE命令将上述的发卡行认证数据发送给终端卡片；
——卡对EXTERNAL AUTHENTICATE命令返回响应状态码‘9000’；
——CDOL2请求授权响应码（标签‘8A’）。

测试流程：选择卡片应用，执行交易（特别是联机处理和发卡行认证处理）。

通过标准：终端应该处理交易直到完成。在接收到第二个 GENERATE AC 命令时，TVR 的字节 5，位 7 =‘0’（发卡行认证成功）。在接收到第二个 GENERATE AC 命令时，TSI 的字节 1，位 5 =‘1’（发卡行认证已执行）。终端发第二个 GENERATE AC 命令请求 TC。授权响应码应该与后台传输的一致。

7.1.30 YSML025-03 电话授权的 ARC，发卡行认证数据的 ARC 表示批准

测试目的：确保终端的密文请求是建立在授权或金融交易响应中的授权响应码的基础之上，而不是可能出现在发卡行认证数据中的其他数据。

终端配置：仅联机终端或有联机能力的脱机终端仅联机或支持脱机/联机、发卡行发起的授权参考支持发卡行发起的语音授权。

卡片配置：——卡的参数已经设置，确保交易是联机完成的；
——卡的AIP指明支持发卡行认证；
——后台应该在授权或金融响应中返回电话授权；
——模拟的发卡行认证数据以如下格式发送给终端：一个有效的8字节的授权响应密文和2字节表明批准的授权响应码；
——EXTERNAL AUTHENTICATE命令将上述的发卡行认证数据发送给终端卡片；
——卡对EXTERNAL AUTHENTICATE命令返回响应状态码‘9000’；
——CDOL2请求授权响应码（标签‘8A’）。

测试流程：选择卡片应用，执行交易 （特别是联机处理和发卡行认证处理）。

通过标准：终端应该处理交易直到完成。在接收到第二个 GENERATE AC 命令时，TVR 的字节 5，位 7 =‘0’（发卡行认证成功）。在接收到第二个 GENERATE AC 命令时，TSI 的字节 1，位 5 =‘1’（发卡行认证已执行）。终端应该显示‘联系发卡行’信息并完成授权。授权响应码应该与后台传输的一致。

7.1.31 YSML025-04 EXTERNAL AUTHENTICATE 状态码的处理（1）

测试目的：确保当发卡行认证数据不存在，且交易已批准时，终端不会拒绝交易。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：——卡的参数已经设置，确保交易是联机完成的；
——联机处理过程中，发卡行应批准交易（授权响应码为批准）；
——发卡行响应报文中发卡行认证数据不存在；
——TAC和IAC所有位均置零；
——卡的AIP指明支持发卡行认证（AIP的字节1，位3为‘1’）。
测试流程：选择卡片应用，执行交易（特别是联机处理和发卡行认证处理）。
通过标准：终端应该处理交易直到完成且交易批准。接收到第二个 GENERATE AC 命令时，TVR 的字节 5，位 7 =‘0’（发卡行认证未执行）。接收到第二个 GENERATE AC 命令时，TSI 的字节 1，位 5 =‘0’（发卡行认证未执行）。

7.1.32 YSML026-00 EXTERNAL AUTHENTICATE 状态码的处理（2）

测试目的：确保终端接受 EXTERNAL AUTHENTICATE 命令的响应的不同于‘9000’或‘6985’等的失败的状态码，并作为失败处理认为外部认证失败，设置TVR中‘发卡行认证失败’位为‘1’。
终端配置：仅联机终端或有联机能力的脱机终端仅联机或支持脱机/联机。
卡片配置：——卡的参数已经设置，确保交易是联机完成的；
——卡的AIP指明支持发卡行认证（AIP的字节1，位3为‘1’）；
——卡的参数已经设置，确保卡片在第二次GENERATE AC时返回TC；
——在模拟的发卡行响应中将发卡行认证数据传回给终端。
子类案例：——案例01：卡片返回状态码‘6283’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例02：卡片返回状态码‘6300’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例03：卡片返回状态码‘63Cx’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例04：卡片返回状态码‘6983’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例05：卡片返回状态码‘6984’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例06：卡片返回状态码‘6A81’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例07：卡片返回状态码‘6A82’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例08：卡片返回状态码‘6A83’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例09：卡片返回状态码‘6A88’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例10：卡片返回状态码‘9001’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例11：卡片返回状态码‘6400’，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例12：卡片返回状态码‘6500’，作为 EXTERNAL AUTHENTICATE 命令的响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该处理交易直到完成且交易批准。接收到第二个 GENERATE AC 命令时，TVR 的字节 5，位 7 =‘1’（发卡行认证失败）。接收到第二个 GENERATE AC

命令时，TSI 的字节 1，位 5 ='1'（发卡行认证已进行执行）。

7.1.33 YSML026-01 EXTERNAL AUTHENTICATE 状态码的处理（3）

测试目的：确保终端接受 EXTERNAL AUTHENTICATE 命令的响应不同于'9000'或'6985'等失败的状态码，并认为外部认证失败，设置TVR中'发卡行认证失败'位为'1'。

终端配置：仅联机终端或有联机能力的脱机终端。

卡片配置：——卡的参数已经设置，确保交易是联机完成的；
——卡的AIP指明支持发卡行认证（AIP的字节1，位3为'1'）；
——在模拟的发卡行响应中将发卡行认证数据传回给终端；
——卡片在第二次GENERATE AC时返回AAC。

子类案例：——案例01：卡片返回状态码'6283'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例02：卡片返回状态码'6300'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例03：卡片返回状态码'63Cx'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例04：卡片返回状态码'6983'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例05：卡片返回状态码'6984'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例06：卡片返回状态码'6A81'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例07：卡片返回状态码'6A82'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例08：卡片返回状态码'6A83'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例09：卡片返回状态码'6A88'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例10：卡片返回状态码'9001'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例11：卡片返回状态码'6400'，作为 EXTERNAL AUTHENTICATE 命令的响应；
——案例12：卡片返回状态码'6500'，作为 EXTERNAL AUTHENTICATE 命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该处理交易直到完成且交易拒绝。接收到第二个 GENERATE AC 命令时，TVR 的字节 5，位 7 ='1'（发卡行认证失败）。接收到第二个 GENERATE AC 命令时，TSI 的字节 1，位 5 ='1'（发卡行认证已执行）。

7.1.34 YSML027-00 GENERATE AC 的正常处理

测试目的：确保终端接受一个正确的状态码'9000'作为GENERATE AC命令的响应，并作为正常的处理。

终端配置：N/A。

卡片配置：卡返回'9000'作为对GENERATE AC的有效响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。

7.1.35 YSML029-04 GET DATA 的失败处理（1）

测试目的：确保当执行频度检查时，终端应该接受一个失败的状态码'6A81'或是'6A88'

作为GET DATA命令的响应，并认为GET DATA作为失败处理。

终端配置：支持频度检查。

卡片配置：——卡的AIP指明需要执行TRM（字节1，位4为‘1’）；
——卡在读取应用数据期间返回标签‘9F14’、‘9F23’的数值。

子类案例：——案例01：卡片返回状态码‘6A81’作为GET DATA命令的响应；
——案例02：卡片返回状态码‘6A88’作为GET DATA命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 命令中 TVR 的字节 4，位 7 =‘1’（超过连续脱机交易下限）。第一个 GENERATE AC 命令中的 TVR 字节 4 位 6 =‘1’（超过连续脱机交易限）。

7.1.36 YSML029-05 GET DATA 的失败处理（2）

测试目的：确保当执行频度检查时，终端应该接受一个失败的状态码‘6A81’或‘6A88’作为GET DATA命令的响应接受对GET DATA命令失败的状态码‘6A81’或是‘6A88’，并认为GET DATA处理失败，并作为失败处理。

终端配置：支持频度检查。

卡片配置：——卡的AIP指明支持TRM（字节1，位4为‘1’）；
——卡在读取应用数据期间返回标签为‘9F14’、‘9F23’的数值。

子类案例：——案例01：卡片返回状态‘6A81’作为GET DATA命令的响应；
——案例02：卡片返回状态‘6A88’作为GET DATA命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 命令中 TVR 的字节 4，位 7 =‘1’（超过连续脱机交易下限）。第一个 GENERATE AC 命令中 TVR 的字节 4，位 6 =‘1’（超过连续脱机交易上限）。

7.1.37 YSML029-06 GET DATA 的失败处理（3）

测试目的：确保终端接受一个失败的状态码‘6A81’或‘6A88’作为GET DATA命令的响应接受对GET DATA命令失败的状态码‘6A81’或是‘6A88’，并认为GET DATA处理失败，且继续进行PIN验证的处理。

终端配置：支持脱机明文 PIN、支持 Get Data 取 PIN 重试次数。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1 位5为‘1’）；
——CVM列表请求‘脱机明文PIN，若终端支持’。

子类案例：——案例01：卡片返回状态‘6A81’作为GET DATA命令的响应；
——案例02：卡片返回状态‘6A88’作为GET DATA命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。终端执行 PIN 的处理。

7.1.38 YSML029-08 GET DATA 的状态码处理（1）

测试目的：确保当频度检查时，若 GET DATA 命令的响应不是‘9000’、‘6A81’或‘6A88’，终端应该继续处理交易。

终端配置：支持频度检查。

卡片配置：——卡的AIP指明支持TRM（字节1，位4为‘1’）；
——卡在读取应用数据期间返回标签为‘9F14’、‘9F23’的数值。

子类案例：——案例01：卡片返回状态‘6283’作为GET DATA命令的响应；
——案例02：卡片返回状态‘6300’作为GET DATA命令的响应；
——案例03：卡片返回状态‘63Cx’作为GET DATA命令的响应；
——案例04：卡片返回状态‘6983’作为GET DATA命令的响应；
——案例05：卡片返回状态‘6984’作为GET DATA命令的响应；

——案例06：卡片返回状态‘6985’作为GET DATA命令的响应；
——案例07：卡片返回状态‘6A82’作为GET DATA命令的响应；
——案例08：卡片返回状态‘6A83’作为GET DATA命令的响应；
——案例09：卡片返回状态‘6400’作为GET DATA命令的响应；
——案例10：卡片返回状态‘6500’作为GET DATA命令的响应；
——案例11：卡片返回状态‘9001’作为GET DATA命令的响应；
——案例12：卡片返回状态‘6D00’作为GET DATA命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该继续处理交易直到完成。

7.1.39 YSML029-09 GET DATA 的状态码处理（2）

测试目的：确保当频度检查时，若 对于GET DATA 命令的响应不是‘9000’、‘6A81’或是‘6A88’，终端应该继续处理交易。

终端配置：支持支持频度检查。

卡片配置：——卡的AIP指明支持TRM（字节1，位4为‘1’）；
——卡在读取应用数据期间返回标签为‘9F14’、‘9F23’的数值；
——读取应用数据期间，卡片返回标签‘9F14’和‘9F23’。

子类案例：——案例01：卡片返回状态‘6283’作为GET DATA命令的响应；
——案例02：卡片返回状态‘6300’作为GET DATA命令的响应；
——案例03：卡片返回状态‘63Cx’作为GET DATA命令的响应；
——案例04：卡片返回状态‘6983’作为GET DATA命令的响应；
——案例05：卡片返回状态‘6984’作为GET DATA命令的响应；
——案例06：卡片返回状态‘6985’作为GET DATA命令的响应；
——案例07：卡片返回状态‘6A82’作为GET DATA命令的响应；
——案例08：卡片返回状态‘6A83’作为GET DATA命令的响应；
——案例09：卡片返回状态‘6400’作为GET DATA命令的响应；
——案例10：卡片返回状态‘6500’作为GET DATA命令的响应；
——案例11：卡片返回状态‘9001’作为GET DATA命令的响应；
——案例12：卡片返回状态‘6D00’作为GET DATA命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该继续处理交易直到完成。

7.1.40 YSML029-10 GET DATA 的状态码处理（3）

测试目的：确保当PIN验证处理时，若 对于GET DATA 命令的响应不是‘9000’、‘6A81’或是‘6A88’时，终端应该继续处理交易。

终端配置：——支持脱机明文 PIN；
——支持 Get Data 取 PIN 重试次数。

卡片配置：——卡的AIP指明终端支持持卡人确认（AIP字节1，位5为‘1’）；
——CVM列表请求‘脱机明文PIN，若终端支持’。

子类案例：——案例01：卡片返回状态‘6283’作为GET DATA命令的响应；
——案例02：卡片返回状态‘6300’作为GET DATA命令的响应；
——案例03：卡片返回状态‘63Cx’作为GET DATA命令的响应；
——案例04：卡片返回状态‘6983’作为GET DATA命令的响应；
——案例05：卡片返回状态‘6984’作为GET DATA命令的响应；
——案例06：卡片返回状态‘6985’作为GET DATA命令的响应；
——案例07：卡片返回状态‘6A82’作为GET DATA命令的响应；
——案例08：卡片返回状态‘6A83’作为GET DATA命令的响应；
——案例09：卡片返回状态‘6400’作为GET DATA命令的响应；
——案例10：卡片返回状态‘6500’作为GET DATA命令的响应；
——案例11：卡片返回状态‘9001’作为GET DATA命令的响应；

——案例12：卡片返回状态‘6D00’作为GET DATA命令的响应；
——案例13：卡片返回状态‘6E00’作为GET DATA命令的响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该继续处理交易直到完成。

7.1.41 YSML030-00 GET PROCESSING OPTIONS的正常处理

测试目的：——确保终端应该接受GET PROCESSING OPTIONS命令正确的响应状态码‘9000’，并认为成功处理；
——确保在应用最终选择应用功能后，终端立即发送GET PROCESSING OPTIONS命令。
终端配置：N/A。
卡片配置：卡片返回状态‘9000’作为GET PROCESSING OPTIONS命令的正确响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。在最终选择处理之后，卡应该接收到一个GET PROCESSING OPTIONS命令。

7.1.42 YSML030-05 GET PROCESSING OPTIONS的失败处理（1）

测试目的：确保终端应该接受对GET PROCESSING OPTIONS命令的失败响应状态码‘6985’，并作为失败处理认为GPO处理失败，，并且终端返回应用选择阶段。
终端配置：——支持持卡人确认；
——终端支持三个AIDs（卡片也需支持）。
卡片配置：——卡片和终端有三个共同支持的应用；
——卡片AID满足：应用1的应用优先指示器位8设置成‘1’；应用2的应用优先指示器位8设置成‘1’；应用3的应用优先指示器位8设置成‘0’；
——卡片返回状态‘6985’作为选择第一个选择应用的时GET PROCESSING OPTIONS命令的响应（应用1）。
测试流程：第一个在候选列表中的应用已经选择，接着被删除，终端开始第二个匹配应用的选择。
通过标准：在 GET PROCESSING OPTIONS 响应‘6985’时，终端应该返回到最终选择处理。只有应用2和应用3保存在应用候选列表中，终端将这两个应用提供给持卡人进行确认。终端通过请求TC或者AAC完成对应用2或者应用3的交易处理。

7.1.43 YSML030-06 GET PROCESSING OPTIONS的失败处理（2）

测试目的：确保终端应该接受对GET PROCESSING OPTIONS命令的失败的响应状态码‘6985’，并认为GPO处理失败，作为失败处理，返回应用选择阶段。
终端配置：——不支持持卡人确认；
——终端支持三个AIDs（卡也同时支持）。
卡片配置：——卡片和终端有三个共同支持的应用；
——卡片AID满足：应用1的应用优先指示器位8设置成‘1’；应用2的应用优先指示器位8设置成‘0’；应用3的应用优先指示器位8设置成‘0’；
——卡片中应用2比应用3的优先级高；
——卡片返回状态‘6985’作为选择应用2的GET PROCESSING OPTIONS命令的响应。
测试流程：选择卡片应用，执行交易。
通过标准：在 GET PROCESSING OPTIONS 响应‘6985’时，终端应该返回到最终选择处理。终端应该通过请求一个TC或AAC完成对应用3的交易处理。

7.1.44 YSML031-00 INTERNAL AUTHENTICATE的正常处理

测试目的：确保终端应该接受INTERNAL AUTHENTICATE命令正确的响应状态码‘9000’，作为并认为INTERNAL AUTHENTICATE成功处理成功。

终端配置：支持 DDA。
卡片配置：——卡的AIP指明支持DDA（AIP的字节1，位6为‘1’）；
——卡片返回状态‘9000’作为 INTERNAL AUTHENTICATE 命令的正确响应。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易；第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 =‘0’（DDA 成功）；在接收到第一个 GENERATE AC 命令时，TSI 的字节 1，位 8 =‘1’（脱机数据认证已进行执行）；第一个 GENERATE AC 命令中的 TVR 字节 1，位 3 =‘0’（未使用 CDA）；第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。

7.1.45 YSML031-01 INTERNAL AUTHENTICATE 的状态码处理

测试目的：确保若对于INTERNAL AUTHENTICATEGET PROCESSING OPTIONS命令的响应不是‘9000’、‘6A81’或是‘6A88’时，终端应该终止交易。
终端配置：支持 DDA。
卡片配置：——卡的AIP指明终端支持动态数据认证（AIP的字节1，位6为‘1’）。
子类案例：——案例01：卡片返回状态‘6283’作为INTERNAL AUTHENTICATE命令的响应；
——案例02：卡片返回状态‘6300’作为INTERNAL AUTHENTICATE命令的响应；
——案例03：卡片返回状态‘63Cx’作为INTERNAL AUTHENTICATE命令的响应；
——案例04：卡片返回状态‘6983’作为INTERNAL AUTHENTICATE命令的响应；
——案例05：卡片返回状态‘6984’作为INTERNAL AUTHENTICATE命令的响应；
——案例06：卡片返回状态‘6985’作为INTERNAL AUTHENTICATE命令的响应；
——案例07：卡片返回状态‘6A81’作为INTERNAL AUTHENTICATE命令的响应；
——案例08：卡片返回状态‘6A82’作为INTERNAL AUTHENTICATE命令的响应；
——案例09：卡片返回状态‘6A83’作为INTERNAL AUTHENTICATE命令的响应；
——案例10：卡片返回状态‘6A88’作为INTERNAL AUTHENTICATE命令的响应；
——案例11：卡片返回状态‘6400’作为INTERNAL AUTHENTICATE命令的响应；
——案例12：卡片返回状态‘6500’作为INTERNAL AUTHENTICATE命令的响应；
——案例13：卡片返回状态‘9001’作为INTERNAL AUTHENTICATE命令的响应；
——案例14：卡片返回状态‘6D00’作为INTERNAL AUTHENTICATE命令的响应；
——案例15：卡片返回状态‘6E00’作为INTERNAL AUTHENTICATE命令的响应；
——案例16：卡片返回状态‘6A86’作为INTERNAL AUTHENTICATE命令的响应；
——案例17：卡片返回状态‘6700’作为INTERNAL AUTHENTICATE命令的响应。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该终止交易。

7.1.46 YSML032-00 READ RECORD 的正常处理

测试目的：确保终端应该接受对READ RECORD命令正确的响应状态码‘9000’‘9000’的响应，并认为READ RECORD成功处理。
终端配置：N/A。
卡片配置：卡片返回状态‘9000’作为READ RECORD命令的正确响应。
测试流程：选择卡片应用，执行交易（特别是读取应用数据阶段）。
通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。

7.1.47 YSML033-00 SELECT 的正常处理

测试目的：确保终端应该接受对SELECT命令正确的响应状态码‘9000’‘9000’的响应，并认为SELECT成功处理。
终端配置：N/A。
卡片配置：卡片返回状态‘9000’作为 SELECT 命令的正确响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.1.48 YSML033-01 SELECT ADF 的失败处理

测试目的：确保终端在使用AID列表选择时，应该接受SELECT ADF 命令的响应状态码‘6283’，并认为SELECT ADF处理失败。
终端配置：终端支持卡的应用。
卡片配置：——卡不支持PSE；
——卡支持三个应用；
——选择卡支持的第一个应用时，卡片返回状态码‘6283’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该选择其他两个应用中的一个。

7.1.49 YSML033-02 SELECT PSE 的状态码处理

测试目的：确保确保若对于响应 SELECT PSE 命令的响应状态码不是‘9000’或是‘6A81’时，终端使用 AID 列表选择方法。
终端配置：支持 PSE。
子类案例：——案例 01：卡片返回状态‘6300’作为 SELECT PSE 的响应；
——案例 02：卡片返回状态‘63Cx’作为 SELECT PSE 的响应；
——案例 03：卡片返回状态‘6983’作为 SELECT PSE 的响应；
——案例 04：卡片返回状态‘6984’作为 SELECT PSE 的响应；
——案例 05：卡片返回状态‘6985’作为 SELECT PSE 的响应；
——案例 06：卡片返回状态‘6A83’作为 SELECT PSE 的响应；
——案例 07：卡片返回状态‘6A88’作为 SELECT PSE 的响应；
——案例 08：卡片返回状态‘6283’作为 SELECT PSE 的响应；
——案例 09：卡片返回状态‘6400’作为 SELECT PSE 的响应；
——案例 10：卡片返回状态‘6500’作为 SELECT PSE 的响应；
——案例 11：卡片返回状态‘9001’作为 SELECT PSE 的响应；
——案例 12：卡片返回状态‘6A82’作为 SELECT PSE 的响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该首先通过 PSE 方式进行选择。终端应该转换到 AID 列表选择方式。终端应该通过请求一个 TC 或 AAC 来完成交易。

7.1.50 YSML033-04 SELECT ADF 的失败处理（2）

测试目的：确保在采用AID列表选择方式时期间，终端接受状态‘6A81’作为对SELECT ADF命令的响应，并认为SELECT ADF处理失败。
终端配置：N/A。
卡片配置：——卡片不支持PSE；
——卡片对第一个 SELECT ADF 的响应返回状态码‘6A81’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该选择终止交易。

7.1.51 YSML034-02 VERIFY 的失败处理（1）

测试目的：——确保终端接受状态码‘63Cx’作为对VERIFY命令的响应，并能理解‘x’为所提供的PIN尝试计数值的值；
——确保若 VERIFY 命令返回‘63Cx’且‘x’大于 0 时，终端应该显示特定的信息并提示另外输入一次 PIN 的输入。
终端配置：支持脱机明文 PIN。
卡片配置：——卡片的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——CVM 列表是请求‘卡片明文 PIN 验证’‘脱机明文 PIN 验证，总是’（0100）；
——卡片返回‘63C2’作为对第一个 VERIFY 命令的响应；

——卡片返回‘63C1’作为对第二个 VERIFY 命令的响应；
——卡片返回‘63C0’作为对第三个 VERIFY 命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。在第二次或第三次尝试时，终端应该显示一个特定的信息，并提示输入 PIN 输入。在第三次尝试后，因 PIN 重试次数已经为零，终端停止发送 VERIFY 命令。第一个 GENERATE AC 命令中的 TVR 字节 3，位 6 = ‘1’（PIN 重试次数超限）。在接收到第一个 GENERATE AC 命令时，TSI 的字节 1，位 7 = ‘1’（持卡人认证已进行验证已执行）。

7.1.52 YSML034-07 VERIFY 的失败处理（2）

测试目的：——确保终端接受一个失败状态码‘6983’和‘6984’作为对VERIFY命令的响应，并并认为VERIFY处理失败；
——确保如果CVM列表请求一个脱机明文PIN验证N是被选择的CVM且PIN在第一次发送最初使用VERIFY命令前已时被锁定，确保终端设置TVR中‘PIN 重试次数超限’位为‘1’。

终端配置：支持脱机明文 PIN。

卡片配置：——卡片的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——CVM列表是请求‘脱机明文PIN验证，总是’（01 00）。

子类案例：——案例01：卡片返回‘6983’作为对VERIFY命令的响应；
——案例02：卡片返回‘6984’作为对VERIFY命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节3，位6 =‘1’（PIN重试次数超限）。第一个GENERATE AC命令中的TVR字节3，位8=‘1’（持卡人验证不成功）。在接收到第一个GENERATE AC命令时，TSI的字节1，位7 =‘1’（持卡人认证已执行）。

7.1.53 YSML035-00 GENERATE AC 的状态码处理

测试目的：确保当对于GENERATE AC命令的响应不是‘9000’时，终端应该终止交易。

终端配置：N/A。

子类案例：——案例01：卡片返回状态‘6283’作为GENERATE AC命令的响应；
——案例02：卡片返回状态‘6300’作为GENERATE AC命令的响应；
——案例03：卡片返回状态‘63Cx’作为GENERATE AC命令的响应；
——案例04：卡片返回状态‘6983’作为GENERATE AC命令的响应；
——案例05：卡片返回状态‘6984’作为GENERATE AC命令的响应；
——案例06：卡片返回状态‘6985’作为GENERATE AC命令的响应；
——案例07：卡片返回状态‘6A81’作为GENERATE AC命令的响应；
——案例08：卡片返回状态‘6A82’作为GENERATE AC命令的响应；
——案例09：卡片返回状态‘6A83’作为GENERATE AC命令的响应；
——案例10：卡片返回状态‘6A88’作为GENERATE AC命令的响应；
——案例11：卡片返回状态‘9001’作为GENERATE AC命令的响应；
——案例12：卡片返回状态‘6400’作为GENERATE AC命令的响应；
——案例13：卡片返回状态‘6500’作为GENERATE AC命令的响应；
——案例14：卡片返回状态‘6D00’作为GENERATE AC命令的响应；
——案例15：卡片返回状态‘6E00’作为GENERATE AC命令的响应；
——案例16：卡片返回状态‘6A86’作为GENERATE AC命令的响应；
——案例17：卡片返回状态‘6700’作为GENERATE AC命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该终止交易。

7.1.54 YSML037-00 GET PROCESSING OPTIONS 的状态码处理

测试目的：确保当对于GET PROCESSING OPTIONS命令的响应不是‘9000’或‘6985’时，终端应该终止交易。

终端配置：N/A。

子类案例：
——案例01：卡片返回状态‘6283’作为GET PROCESSING OPTIONS命令的响应；
——案例02：卡片返回状态‘6300’作为GET PROCESSING OPTIONS命令的响应；
——案例03：卡片返回状态‘63Cx’作为GET PROCESSING OPTIONS命令的响应；
——案例04：卡片返回状态‘6983’作为GET PROCESSING OPTIONS命令的响应；
——案例05：卡片返回状态‘6984’作为GET PROCESSING OPTIONS命令的响应；
——案例06：卡片返回状态‘9001’作为GET PROCESSING OPTIONS命令的响应；
——案例07：卡片返回状态‘6A81’作为GET PROCESSING OPTIONS命令的响应；
——案例08：卡片返回状态‘6A82’作为GET PROCESSING OPTIONS命令的响应；
——案例09：卡片返回状态‘6A83’作为GET PROCESSING OPTIONS命令的响应；
——案例10：卡片返回状态‘6A88’作为GET PROCESSING OPTIONS命令的响应；
——案例11：卡片返回状态‘6500’作为GET PROCESSING OPTIONS命令的响应；
——案例12：卡片返回状态‘6400’作为GET PROCESSING OPTIONS命令的响应；
——案例14：卡片返回状态‘6D00’作为GET PROCESSING OPTIONS命令的响应；
——案例15：卡片返回状态‘6E00’作为GET PROCESSING OPTIONS命令的响应；
——案例16：卡片返回状态‘6700’作为GET PROCESSING OPTIONS命令的响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该终止交易。

7.1.55 YSML039-00 READ RECORD 的状态码处理

测试目的：确保当对于应用选择以外的READ RECORD命令的响应不是‘9000’时，终端应该终止交易。

终端配置：N/A。

子类案例：在读取应用数据阶段，卡片返回如下的状态码作为READ RECORD命令的响应：
——案例01：卡片返回状态‘6283’作为READ RECORD命令的响应；
——案例02：卡片返回状态‘6300’作为READ RECORD命令的响应；
——案例03：卡片返回状态‘63Cx’作为READ RECORD命令的响应；
——案例04：卡片返回状态‘6983’作为READ RECORD命令的响应；
——案例05：卡片返回状态‘6984’作为READ RECORD命令的响应；
——案例06：卡片返回状态‘6985’作为READ RECORD命令的响应；
——案例07：卡片返回状态‘6A81’作为READ RECORD命令的响应；
——案例08：卡片返回状态‘6A82’作为READ RECORD命令的响应；
——案例09：卡片返回状态‘6A88’作为READ RECORD命令的响应；
——案例10：卡片返回状态‘6A83’作为READ RECORD命令的响应；
——案例11：卡片返回状态‘6500’作为READ RECORD命令的响应；
——案例12：卡片返回状态‘6400’作为READ RECORD命令的响应；
——案例13：卡片返回状态‘9001’作为READ RECORD命令的响应；
——案例14：卡片返回状态‘6D00’作为READ RECORD命令的响应；
——案例15：卡片返回状态‘6E00’作为READ RECORD命令的响应；
——案例16：卡片返回状态‘6A86’作为READ RECORD命令的响应。

测试流程：选择卡片应用，执行交易直到读取应用数据阶段。

通过标准：终端应该终止交易。

7.1.56 YSML040-00 VERIFY 的状态码处理

测试目的：确保当VERIFY命令的响应不是‘9000’、‘63Cx’、‘6983’和‘6984’时，终端应该终止交易。

终端配置：支持脱机明文 PIN。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡支持脱机明文PIN验证。
子类案例：——案例01：卡片返回状态‘6283’作为VERIFY命令的响应；
——案例02：卡片返回状态‘6300’作为VERIFY命令的响应；
——案例03：卡片返回状态‘6985’作为VERIFY命令的响应；
——案例04：卡片返回状态‘6A81’作为VERIFY命令的响应；
——案例05：卡片返回状态‘6A82’作为VERIFY命令的响应；
——案例06：卡片返回状态‘6A83’作为VERIFY命令的响应；
——案例07：卡片返回状态‘6A88’作为VERIFY命令的响应；
——案例08：卡片返回状态‘9001’作为VERIFY命令的响应；
——案例09：卡片返回状态‘6400’作为VERIFY命令的响应；
——案例10：卡片返回状态‘6500’作为VERIFY命令的响应；
——案例09：卡片返回状态‘6D00’作为VERIFY命令的响应；
——案例10：卡片返回状态‘6E00’作为VERIFY命令的响应。
测试流程：选择卡片应用，执行交易（特别是持卡人认证）。
通过标准：终端应该终止交易。

7.1.57 YSML041-00 RFU 字节和位的编码（1）

测试目的：确保除非另有规定，确保终端应将表明 RFU 的数据（字节和位）设置成零。特别是对于 TVR、TSI、终端性能、附加终端性能和 GENERATE AC 相关控制参数等。
终端配置：N/A。
卡片配置：N/A。
测试流程：选择卡片应用，执行交易。
通过标准：接收到第一个 GENERATE AC 命令时，TVR：字节 1，位 2 1；字节 2，位 3 1；字节 3，位 2 1；字节 4，位 3 1；字节 5，位 4 1 都设成‘0’。接收到第一个 GENERATE AC 命令时，TSI ：字节 1，位 2 1；字节 2，位 8 1 都设成‘0’。接收到第一个 GENERATE AC 命令时，终端性能：字节 1，位 5 1；字节 2，位 3 2；字节 3，位 3 1 以及位 5 都设成‘0’。接收到第一个 GENERATE AC 命令时，附加终端性能：字节 2，位 7 1； 字节 3，位 4 1；字节 4，位 4 3 都设成‘0’。卡收到的 GENERATE AC 命令的相关控制参数应该有位 1 4 和 6 都设成‘0’。

7.1.58 YSML041-01 RFU 字节和位的编码（2）

测试目的：确保除非另有规定，终端应将表明 RFU 的数据（字节和位）设置成零。这应用于 VERIFY 命令参考数据（P2）的限定值。
终端配置：支持脱机明文 PIN。
卡片配置：——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——CVM‘脱机明文 PIN，总是’（0100）。
测试流程：选择卡片应用，执行交易（特别是持卡人认证）。
通过标准：卡接收到的 VERIFY 命令参考数据（P2）的限定值位 4 1 应该都设成‘0’。

7.1.59 YSML041-03 RFU 字节和位的编码（3）

测试目的：确保终端能够设置零数据（位和字节）为零表明 RFU，并能够识别卡中 RFU 位设置成‘0’的数据。对 IAC 和 TAC 都适用。
终端配置：N/A。
卡片配置：IACs 和 TACs 的 RFU 位设置为‘0’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该使用并且能够识别不应终止交易，应根据 TAC 和 IAC 的设置，通过

请求一个 TC 或 AAC 来完成交易。

7.1.60 YSML041-04 RFU 字节和位的编码（4）（隐含的）

测试目的：确保终端不用 RFU 的位，即使 RFU 的位被设置为‘1’。适用于 IAC
终端配置：N/A。
卡片配置：IAC 的 RFU 位设置为‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该忽略 RFU 中设置成‘1’的位，并继续正常的交易处理。

7.1.61 YSML054-00 GENERATE AC 返回的数据域的格式（格式一）（1）

测试目的：确保终端能够识别根据格式一编码的 GENERATE AC 命令返回的数据域，特别是返回数据中数据对象值的顺序。
终端配置：N/A。
子类案例：——案例 01：GENERATE AC 命令的响应只包含强制的数据对象，并且按照格式一编码（模板 80）；
——案例 02：GENERATE AC 命令的响应包含强制的数据对象和发卡行应用数据，并且按照格式一编码（模板 80）；
——案例 03：GENERATE AC 命令的响应包含强制的数据对象和发卡行应用数据，并且按照格式一编码（模板 80）。标签‘80’的长度以两个字节编码（81 xx）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该接受卡并正确解释格式一的数据域。终端应该通过请求一个 TC 或 AAC 来完成交易。终端中的和包含在批上送或者金融/授权请求中的 CID、ATC、应用密文、发卡行应用数据应该与卡片返回的值一致。

7.1.62 YSML054-01 GENERATE AC 返回的数据域的格式（格式一） （2）

测试目的：若根据格式一编码的 GENERATE AC 命令返回的数据域长度超过允许的最大值，确保终端应该终止交易。
终端配置：N/A。
卡片配置：GENERATE AC 命令的响应按照格式一编码（模板 80），包含强制的数据对象和发卡行应用数据（长度为 32 个字节），并且在强制的数据对象前填充了 5 个字节的‘00’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该接受卡并正确解释格式一的数据域。终止交易。

7.1.63 YSML055-00 GENERATE AC 返回的数据域的格式（格式二）（1）

测试目的：确保终端能够识别根据格式二编码的GENERATE AC命令的返回数据域。
终端配置：N/A。
子类案例：——案例01：GENERATE AC命令的响应只包含强制的数据对象，并且按照格式二编码（模板 77）；
——案例 02：GENERATE AC 命令的响应只包含强制的数据对象和发卡行应用数据，并且按照格式二编码（模板 77）；
——案例 03：GENERATE AC 命令的响应包含强制的数据对象和发卡行应用数据，并且按照格式二编码（模板 77）。标签‘77’的长度以两个字节编码（81 xx）；
——案例 04：GENERATE AC 命令的响应包含强制的数据对象、发卡行应用数据和自定义数据，使 GENERATE AC 命令响应的总长度超过 150 字节，并且按照格式二编码（模板 77）。标签‘77’的长度以两个字节编码（81 xx）。
测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡并正确解释格式二的数据域。终端应该继续交易，并根据卡对GENERATE AC命令的响应来结束交易。

7.1.64 YSML055-01 GENERATE AC返回的数据域的格式（格式二）（2）

测试目的：确保终端能够识别根据格式二编码的GENERATE AC命令的返回数据域，且数据元之间用十六进制的‘00’填充。

终端配置：N/A。

子类案例：——案例01：GENERATE AC命令的响应只包含强制的数据对象，按照格式二编码（模板 77），两个数据元之间填充了50个字节的‘00’；

——案例 02：GENERATE AC 命令的响应包含强制的数据对象和发卡行应用数据，按照格式二编码（模板 77），最后一个数据元之后填充了 50 个字节的‘00’；

——案例 03：GENERATE AC 命令的响应包含强制的数据对象和发卡行应用数据，并且按照格式二编码（模板 77）。标签‘77’的长度以两个字节编码（81 xx），两个数据元之间填充了 50 个字节的‘00’；

——案例 04：GENERATE AC 命令的响应包含强制的数据对象、发卡行应用数据和自定义数据，使 GENERATE AC 命令响应的总长度超过 150 字节，并且按照格式二编码（模板 77）。标签‘77’的长度以两个字节编码（81 xx），最后一个数据元之后填充了 50 个字节的‘00’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡并正确解释格式二的数据域。终端应该继续交易，并根据卡对GENERATE AC命令的响应来结束交易。

7.1.65 YSML056-00 GENERATE AC命令响应中自定义数据对象的传输：格式二

测试目的：确保当GENERATE AC命令使用格式二返回响应时，终端能够忽略包含在GENERATE AC命令响应中的自定义数据对象。

终端配置：N/A。

卡片配置：GENERATE AC命令的响应用格式二编码，包含自定义数据对象（模板 77）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，并忽略采用格式二编码的GENERATE AC命令用格式二编码的响应中的自定义数据对象。终端应该通过请求一个TC或AAC来完成交易。

7.1.66 YSML058-00 应用交易计数器

测试目的：确保终端接受在GENERATE AC命令的响应中包含的有效格式的应用交易计数器。

终端配置：N/A。

卡片配置：——CDOL2请求应用交易计数器；

——第一次 GENERATE AC 命令，卡片响应 ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该处理交易直到结束。终端在第二次GENERATE AC命令数据域中提供的ATC，应该与卡片在第一次GENERATE AC期间返回的值相同。

7.1.67 YSML059-00 应用密文

测试目的：确保终端接受在GENERATE AC命令的响应中包含的有效格式的应用密文。

终端配置：N/A。

卡片配置：——应用密文可以是实际数据也可以是测试值数据；

——CDOL2 请求应用密文；

——卡片在第一次 GENERATE AC 命令响应时返回 ARQC。

测试流程：选择卡片应用，执行交易。
通过标准：终端应该接受卡片，并且处理交易直到结束。终端在第二次GENERATE AC命令数据域中提供的应用密文，应该与卡片在第一次GENERATE AC期间返回的值相同。

7.1.68 YSML060-00 发卡行应用数据

测试目的：确保终端接受在GENERATE AC命令的响应中包含的有效格式的发卡行应用数据。
终端配置：N/A。
卡片配置：——GENERATE AC的响应包含发卡行应用数据；
——CDOL2 请求发卡行应用数据；
——卡片在第一次 GENERATE AC 时返回响应 ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该接受卡片，并且处理交易直到结束。终端在第二次GENERATE AC命令数据域中提供的发卡行应用数据，应该与卡片在第一次GENERATE AC期间返回的值相同。

7.1.69 YSML061-00 密文信息数据：AAC

测试目的：验证终端能够正确解释GENERATE AC命令的响应中卡片返回请求AAC。确保终端接受在GENERATE AC命令中响应的有效密文信息数据。
终端配置：N/A。
子类案例：卡响应第一个GENERATE AC命令：
——案例 01：卡响应一个 AAC，没有通知（00）；
——案例 02：卡响应一个 AAC，带有通知且无原因（08）；
——案例 03：卡响应一个 AAC，带有通知且原因是超出 PIN 重试次数（0A）；
——案例 04：卡响应一个 AAC，带有通知且原因是发卡行认证失败（0B）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该拒绝交易。

7.1.70 YSML062-00 密文信息数据：TC（1）

测试目的：验证终端能够正确解释GENERATE AC命令的响应中卡片返回请求TC。确保终端接受在GENERATE AC命令中响应的有效密文信息数据。
终端配置：仅脱机终端或有联机能力的脱机终端支持脱机或支持脱机/联机。
子类案例：卡响应第一个GENERATE AC命令：
——案例01：卡响应一个TC，没有通知（40）；
——案例02：卡响应一个TC，带有通知且无原因（48）；
——案例03：卡响应一个TC，带有通知且原因是超出PIN重试次数（4A）；
——案例04：卡响应一个TC，带有通知且原因是发卡行认证失败（4B）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该脱机批准脱机交易。

7.1.71 YSML062-01 密文信息数据：TC（2）

测试目的：验证终端能够正确解释GENERATE AC命令的响应中卡片返回TC请求TC。确保终端接受在GENERATE AC命令中响应的有效密文信息数据。
终端配置：仅联机终端或有联机能力的脱机终端支持联机或支持脱机/联机。
子类案例：卡响应第二个GENERATE AC命令：
——案例01：卡响应一个TC，没有通知（40）；
——案例02：卡响应一个TC，带有通知且无原因（48）；
——案例03：卡响应一个TC，带有通知且原因是超出PIN重试次数（4A）；
——案例04：卡响应一个TC，带有通知且原因是发卡行认证失败（4B）。

测试流程：选择卡片应用，执行交易。
通过标准：终端应该联机批准联机交易。

7.1.72 YSML063-00 密文信息数据：ARQC

测试目的：验证终端能够正确解释GENERATE AC命令的响应中正确解释请求ARQC的GENERATE AC命令的响应卡片返回ARQC。
终端配置：仅联机终端或有联机能力的脱机终端支持联机或支持脱机/联机。
子类案例：卡响应第一个GENERATE AC命令：
——案例01：卡响应一个ARQC，没有通知（80）；
——案例02：卡响应一个ARQC，带有通知且无原因（88）；
——案例03：卡响应一个ARQC，带有通知且原因是超出PIN重试次数（8A）；
——案例04：卡响应一个ARQC，带有通知且原因是发卡行认证失败（8B）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该完成联机交易。

7.1.73 YSML064-00 密文信息数据：AAR

测试目的：验证终端能够正确解释GENERATE AC命令的响应中卡片返回AAR，并认为有逻辑错误，终止交易正确解释请求AAR的GENERATE AC命令的响应。
终端配置：N/A。
子类案例：卡响应第一个GENERATE AC命令：
——案例01：卡响应一个AAR，没有通知（C0）；
——案例02：卡响应一个AAR，带有通知且无原因（C8）；
——案例03：卡响应一个AAR，带有通知且原因是超出PIN重试次数（CA）；
——案例04：卡响应一个AAR，带有通知且原因是发卡行认证失败（CB）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该终止交易。

7.1.74 YSML067-00 密文信息数据：PIN 重试次数超限

测试目的：验证终端能够正确解释请求通知的GENERATE AC命令的响应中密文信息数据要求通知，并表明通知原因是PIN重试次数超限。
终端配置：支持通知。
卡片配置：——在第一个GENERATE AC命令响应时，卡请求返回AAC并要求通知；
——卡指明的通知原因是PIN重试次数超限。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该发送一个联机通知或是创建一个脱机通知。在通知中包含的交易拒绝原因应该是PIN重试次数超限。

7.1.75 YSML068-00 密文信息数据中要求通知，交易无法联机

测试目的：当卡片在密文信息数据中要求通知，交易无法联机，不能被后台捕获时，终端应终止交易。
终端配置：——支持通知；
——支持联机数据捕获；
——不支持批数据捕获。
卡片配置：——终端在第一个GENERATE AC时请求TC或ARQC。
子类案例：——案例01：卡响应一个ARQC，带有通知且无原因（88）；
——案例02：卡响应一个ARQC，带有通知且原因是超出PIN重试次数（8A）；
——交易无法联机。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该终止交易。

7.1.76 YSML069-00 密文信息数据中要求通知，终端不支持通知

测试目的：当卡片在密文信息数据中要求通知，但终端不支持通知，交易无法联机时，终端应忽略这个通知的请求。

终端配置：不支持通知。

卡片配置：——终端在第一个GENERATE AC时请求TC或ARQC。

子类案例：——案例01：卡响应一个ARQC，带有通知且无原因（CID=88）；
——案例02：卡响应一个ARQC，带有通知且原因是超出PIN重试次数（CID=8A）；
——交易无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该忽略该通知的请求并完成交易。

7.1.77 YSML070-00 GET DATA 返回的数据域的格式（ATC）2CA-070-00

测试目的：确保当终端在风险管理期间请求ATC时，终端能够识别GET DATA命令返回的数据域。确保当卡中存在脱机限额上下限时，终端可以通过使用GET DATA命令取得ATC。

终端配置：支持频度检查。

卡片配置：——卡的AIP指明支持TRM（AIP的字节1，位4为‘1’）；
——卡中包含UCOL和LCOL（用于获取ATC）；
——卡片返回状态‘9000’作为GET DATA命令的有效响应（ATC）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡片并完成交易。卡片应该接收到GET DATA命令（80 CA 9F 36）。第一个GENERATE AC命令中的TVR字节1，位6 =‘0’（IC卡数据未缺失）。在接收到第一个GENERATE AC命令时，TSI的字节1，位4 =‘1’（终端风险管理已进行执行）。

7.1.78 YSML071-00 GET DATA 返回的数据域的格式（LOATC）

测试目的：——确保当终端在风险管理期间请求LOATC时，终端能够识别GET DATA命令返回的数据域；
——确保终端通过GET DATA命令得到LOATC。

终端配置：支持频度检查。

卡片配置：——卡的AIP指明支持TRM（AIP的字节1，位4为‘1’）；
——卡中包含UCOL和LCOL（用于获取LOATC）；
——卡片返回状态‘9000’作为GET DATA命令的有效响应（LOATC）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡并完成交易。卡片应该接收到GET DATA命令（80 CA 9F 13）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 6 =‘0’（IC 卡数据未缺失）。在接收到第一个 GENERATE AC 命令时，TSI 的字节 1，位 4 =‘1’（终端风险管理已进行执行）。

7.1.79 YSML072-00 GET DATA 返回的数据域的格式（PIN 尝试限制）——PIN 重试次数等于 0 时的终端行为

测试目的：——确保在脱机明文PIN验证期间请求PIN重试次数时，终端能够识别通过GET DATA返回的数据域；
——确保若通过GET DATA返回的PIN重试次数为0，终端设置TVR中的‘PIN重试次数超限’为‘1’，并继续对CVM的处理。

终端配置：支持 Get Data 取 PIN 重试次数、支持脱机明文 PIN。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——CVM 列表为‘脱机明文 PIN 的验证，总是’（41 00）并跟随‘CVM 失败，

总是’（0000）；
——PIN 重试次数为 0；
——卡片返回状态‘9000’作为 GET DATA 命令的有效响应(PIN 重试次数)。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，通过请求一个TC或AAC来完成交易。终端应该不显示有关PIN重试次数的任何特殊信息。第一个GENERATE AC命令中的TVR字节3，位6 =‘1’（PIN重试次数超限）。在接收到第一个GENERATE AC命令时，TSI的字节1，位7 =‘1’（持卡人认证已进行执行）。在接收到第一个GENERATE AC命令时，CVM结果显示‘CVM失败，总是，处理失败’作为最后CVM的处理结果（‘-00 00 01’）。

7.1.80 YSML074-00 GET PROCESSING OPTIONS 数据域的格式（PDOL）

测试目的：——确保若在卡最终选择ADF时卡返回的FCI中存在PDOL，终端发送一个GET PROCESSING OPTIONS命令，该命令数据域中是一个标签为‘83’的结构数据对象，其长度域是后续数据的长度、值域是根据PDOL编码连接的数据元；
——确保终端支持有效的PDOL。

终端配置：N/A。

子类案例：——案例 01：PDOL 包含 TVR 和 TSI；
——案例 02：由卡片返回的 PDOL 包含 TVR、TSI 以及终端性能；
——案例 03：由卡片返回的 PDOL 包含 TVR 和终端编号。

测试流程：选择卡片应用，执行交易。

通过标准：卡片接收到格式正确的GET PROCESSING OPTIONS数据域：由标签‘83’数据对象的值域、长度域以及PDOL请求的数据组成为标签‘83’的结构数据对象。

7.1.81 YSML075-00 GET PROCESSING OPTIONS 数据域的格式（没有 PDOL）

测试目的：确保若在最终选择ADF时卡返回的FCI中若在选择的ADF的FCI中不存在PDOL，终端发送一个GET PROCESSING OPTIONS命令，该命令数据域中是一个为标签为‘83’，长度为0的结构数据对象。

终端配置：N/A。

卡片配置：最终选择的ADF的FCI中不返回PDOL。

测试流程：选择卡片应用，执行交易。

通过标准：卡应该接收到正确格式的GET PROCESSING OPTIONS数据域：‘83 00’。

7.1.82 YSML076-00 GET PROCESSING OPTIONS 数据域的格式：PDOL 为空（隐含的）

测试目的：确保若在最终选择ADF时PDOL为空，终端发送一个GET PROCESSING OPTIONS命令，该命令数据域是一个标签为‘83’，长度为0的结构数据对象。

终端配置：N/A。

卡片配置：最终选择ADF的FCI中返回PDOL，且该PDOL为空。

测试流程：选择卡片应用，执行交易。

通过标准：卡应该接收到正确格式的GET PROCESSING OPTIONS数据域：‘8300’。

7.1.83 YSML077-00 GET PROCESSING OPTIONS 返回数据域的格式：格式一（1）

测试目的：确保终端识别GET PROCESSING OPTIONS命令返回的数据域，且该数据域根据格式一编码。

终端配置：N/A。

卡片配置：——CDOL1 请求 AIP。

子类案例：——案例 01：GET PROCESSING OPTIONS 的响应包含格式一编码的 AIP 和 AFL（模板 80）；
——案例 02：GET PROCESSING OPTIONS 的响应包含格式一编码的 AIP 和 AFL

（模板 80）。标签‘80’的长度域以两字节编码（81 xx）；

——案例 03：GET PROCESSING OPTIONS 的响应包含格式一编码的 AIP 和 AFL（模板 80）。标签‘80’的长度域以两字节编码（81 xx），由于存在多个 AFL 分支，GPO 响应的总长度超过 150 字节。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，通过请求一个TC或AAC来来完成交易。GENERATE AC命令中AIP的值应该与卡片返回的值一致。卡接收到的READ RECORD命令参数（P1、P2）与AFL一致。

7.1.84 YSMLO77-01 GET PROCESSING OPTIONS 返回数据域的格式：格式一（2）

测试目的：——确保终端识别GET PROCESSING OPTIONS命令返回的数据域，且该数据域根据格式一编码；

——确保若返回的模板的两个数据元之间存在十六进制的‘00’填充字节，终端应该终止交易。

终端配置：N/A。

子类案例：——案例 01：GET PROCESSING OPTIONS 的响应包含格式一编码的 AIP 和 AFL（模板 80）。AFL 后填充了 5 字节的‘00’（在模板‘80’内）；

——案例 02：GET PROCESSING OPTIONS 的响应包含格式一编码的 AIP 和 AFL（模板 80）。AIP 和 AFL 之间填充了 5 个字节的‘00’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该终止交易。

7.1.85 YSMLO78-OO GET PROCESSING OPTIONS 返回数据域的格式：格式二（1）

测试目的：确保终端识别由GET PROCESSING OPTIONS命令返回的数据域，且该数据域根据格式二编码。

终端配置：N/A。

卡片配置：——CDOL1 请求 AIP。

子类案例：——案例 01：GET PROCESSING OPTIONS 的响应包含格式二编码的 AIP 和 AFL（模板 77）；

——案例 02：GET PROCESSING OPTIONS 的响应包含格式二编码的 AIP 和 AFL（模板 77）。标签‘77’的长度域以两字节编码（81 xx）；

——案例 03：GET PROCESSING OPTIONS 的响应包含格式二编码的 AIP 和 AFL（模板 77）。标签‘77’的长度域以两字节编码（81 xx），由于存在多个 AFL 分支，GPO 响应的总长度超过 150 字节；

——案例 04：GET PROCESSING OPTIONS 的响应包含格式二编码的 AIP、AFL 和预留的数据元（标签‘9F30’，长度 10 字节）（模板 77）；

——案例 05：GET PROCESSING OPTIONS 的响应包含格式二编码的 AIP、AFL 和预留的数据元（标签‘9F24’，长度 50 字节）（模板 77），标签‘77’的长度域以两字节编码（81 xx）；

——案例 06：GET PROCESSING OPTIONS 的响应包含格式二编码的 AIP、AFL 和预留的数据元（标签‘9F28’，长度 150 字节）（模板 77），标签‘77’的长度域以两字节编码（81 xx）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，请求一个TC或AAC来完成交易。GENERATE AC命令中AIP的值应该与卡片返回的值一致。卡接收到的READ RECORD命令参数（P1、P2）与AFL一致。

7.1.86 YSMLO78-01 GET PROCESSING OPTIONS 返回数据域的格式：格式二（2）

测试目的：——确保终端识别由GET PROCESSING OPTIONS命令返回的数据域，且该数据

域根据格式二编码；

——确保若返回的两个数据元之间存在十六进制的‘00’填充字节，终端应该忽略此填充。

终端配置：N/A。

子类案例：——案例 01：GET PROCESSING OPTIONS 的响应包含格式二编码的 AIP 和 AFL（模板 77）。AFL 后填充了 10 字节的‘00’（在模板‘77’内）；

——案例 02：GET PROCESSING OPTIONS 的响应包含格式二编码的 AIP 和 AFL（模板 77）。AIP 和 AFL 之间填充了 50 个字节的‘00’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，请求一个TC或AAC来完成交易。GENERATE AC命令中AIP的值应该与卡片返回的值一致。卡接收到的READ RECORD命令参数（P1、P2）与AFL一致。

7.1.87 YSML082-00 INTERNAL AUTHENTICATE 数据域的格式

测试目的：确保终端发送INTERNAL AUTHENTICATE命令，数据域包含DDOL中请求的数据对象。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持DDA（AIP的字节1，位6为‘1’）；

——卡包含 DDOL 以及动态数据认证所需的所有数据。

测试流程：选择卡片应用，执行交易。

通过标准：卡应该接收到格式正确的 INTERNAL AUTHENTICATE 数据域：包含 DDOL 中请求的数据对象的值域。

7.1.88 YSML083-00 INTERNAL AUTHENTICATE 返回数据域的格式：格式一

测试目的：确保终端能够识别由INTERNAL AUTHENTICATE返回的数据域，该数据域用格式一编码。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；

——卡包含 DDOL 以及动态数据认证所需的所有数据。

子类案例：——案例 01：卡响应 INTERNAL AUTHENTICATE 应该是用格式一编码的正确密文（模板 80）；

——案例 02：卡响应 INTERNAL AUTHENTICATE 应该是用格式一编码的正确密文（模板 80）。标签‘80’的长度域以两字节编码（81 xx）；

——案例 03：卡响应 INTERNAL AUTHENTICATE 应该是用格式一编码的正确密文（模板 80）。标签‘80’的长度域以两字节编码（81 xx），且 IC 卡公钥长度大于 150 字节。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，来完成交易通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行执行）。

7.1.89 YSML084-00 INTERNAL AUTHENTICATE 返回数据域的格式：格式二（1）

测试目的：确保终端能够识别由INTERNAL AUTHENTICATE返回的数据域，且该数据域用格式二编码。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；

——卡包含 DDOL 以及动态数据认证所需的所有数据。

子类案例：——案例 01：卡响应 INTERNAL AUTHENTICATE 应该是用格式二编码的正确密文（模板 77）；
——案例 02：卡响应 INTERNAL AUTHENTICATE 应该是用格式二编码的正确密文（模板 77）。标签‘77’的长度域以两字节编码（81 xx）；
——案例 03：卡响应 INTERNAL AUTHENTICATE 应该是用格式二编码的正确密文（模板 77）。标签‘77’的长度域以两字节编码（81 xx），且 IC 卡公钥长度大于 150 字节；
——案例 04：卡响应 INTERNAL AUTHENTICATE 应该是用格式二编码的正确密文和预留数据（标签‘9F30’，长度 10 字节）（模板 77）；
——案例 05：卡响应 INTERNAL AUTHENTICATE 应该是用格式二编码的正确密文和预留数据（标签‘9F24’，长度 50 字节）（模板 77）。标签‘77’的长度域以两字节编码（81 xx）；
——案例 06：卡响应 INTERNAL AUTHENTICATE 应该是用格式二编码的正确密文和预留数据（标签‘9F28’，长度 50 字节）（模板 77）。标签‘77’的长度域以两字节编码（81 xx），且 IC 卡公钥长度大于 150 字节。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，来完成交易通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行执行）。

7.1.90 YSML084-01 INTERNAL AUTHENTICATE 返回数据域的格式：格式二（2）

测试目的：——确保终端能够识别由INTERNAL AUTHENTICATE返回的数据域，且该数据域用格式二编码；
——确保若返回的两个数据元之间存在十六进制的‘00’填充字节，终端应该忽略此填充。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡包含 DDOL 以及动态数据认证所需的所有数据。

子类案例：——案例 01：卡响应 INTERNAL AUTHENTICATE 应该是用格式二编码的正确密文（模板 77）。密文后填充了 10 字节的‘00’（在模板‘77’内）；
——案例 02：卡响应 INTERNAL AUTHENTICATE 应该是用格式二编码的正确密文（模板 77）。密文后填充了 50 字节的‘00’（在模板‘77’内），填充字节后紧随一个自定义数据元。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，来完成交易通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已执行）。

7.1.91 YSML089-00 READ RECORD 返回数据域的格式

测试目的：确保终端能够识别READ RECORD返回的数据域。

终端配置：N/A。

卡片配置：——AFL不为空；
——CDOL1 请求 PAN 和应用失效日期；
——卡中所有强制数据都存在。

测试流程：选择卡片应用，执行交易。
通过标准：终端应该接受卡，通过请求一个TC或AAC来完成交易。PAN和应用失效终止日期的值应该与卡片返回的值一致。

7.1.92 YSML092-00 SELECT 数据域的格式

测试目的：验证终端能够发传送正确编码SELECT命令数据域。
终端配置：N/A。
卡片配置：无特殊卡片配置。
测试流程：选择卡片应用，执行交易。
通过标准：卡接收到的SELECT命令数据域包含所选择应用的AID。

7.1.93 YSML093-00 SELECT PSE 返回数据域的格式

测试目的：确保终端若支持用PSE选择，它应该能够识别由SELECT PSE命令数据域返回的FCI。
终端配置：支持PSE。
卡片配置：——卡片包含一个PSE；
——PSE 的 FCI 包含所有强制的数据域：FCI 模板（‘6F’）、DF 名（‘84’）、FCI 私有模板（‘A5’）和目录文件 SFI（‘88’）；
——PSE 的 FCI 包含所有可选的数据对象：首选语言（‘5F2D’）、发卡行代码表索引（‘9F11’），PSE 的 FCI 发卡行自定义数据（‘BF0C’）包含数据域：‘5F54’银行标识码（BIC）、‘5F53’国际银行帐目号（IBAN）、‘5F55’发卡行国家代码（alpha 2）、‘5F56’发卡行国家代码（alpha 3）和‘42’发卡行标识码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该接受卡，通过请求一个TC或AAC来完成交易。卡应该收到一个READ RECORD命令，其SFI根据FCI数据编码返回。

7.1.94 YSML094-00 SELECT PSE 返回数据域的格式：无可选数据

测试目的：确保终端若支持用PSE选择，它应该接受SELECT PSE命令返回的数据域中不带有缺少可选数据对象的PSE。
终端配置：支持PSE。
卡片配置：——卡片包含一个PSE。
——PSE 的 FCI 包含所有强制的数据域，但无可选数据域：FCI 模板（‘6F’）、DF 名（‘84’）、FCI 私有模板（‘A5’）和目录文件 SFI（‘88’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该接受卡，来完成交易通过请求一个TC或AAC来完成交易。终端应该提示选择语言或是使用缺省语言（若仅支持一种）。卡应该收到一个READ RECORD命令，其SFI根据FCI数据编码返回。

7.1.95 YSML097-00 SELECT ADF 返回数据域的格式

测试目的：确保终端能够识别SELECT ADF命令返回的数据域。
终端配置：N/A。
卡片配置：——卡包含一个ADF；
——ADF 的 FCI 包含所有强制的数据域：FCI 模板（‘6F’）、DF 名（‘84’）、FCI 私有模板（‘A5’）、应用标签（‘50’）；
——ADF 的 FCI 包含可选的数据对象：应用优先指示符（‘87’）、PDOL（‘9F38’）、语言优先选择（‘5F2D’）、发卡行编码列表索引（‘9F11’）、应用首选名称（‘9F12’）、应用标签（‘50’）和 FCI 发卡行自定义数据（‘BF0C’）包含数据域：‘9F4D’日志入口、‘5F54’银行标识码(BIC)、‘5F53’国际银行帐目号(IBAN)、‘5F55’

发卡行国家代码（alpha 2）、‘5F56’发卡行国家代码（alpha 3）和‘42’发卡行标识码。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，来完成交易通过请求一个TC或AAC来完成交易。

7.1.96 YSML098-00 SELECT ADF 返回数据域的格式：可选数据

测试目的：确保终端若支持PSE选择，它应该接受在SELECT ADF命令返回的数据域中缺少可选数据。

终端配置：N/A。

卡片配置：——卡包含一个ADF；

——ADF 的FCI 包含所有强制的数据域，但无可选数据域：FCI 模板（‘6F’）、DF 名（‘84’）、FCI 私有模板（‘A5’，长度为 00）、应用标签（‘50’）（应用标签为可选数据）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，来完成交易通过请求一个TC或AAC来完成交易。

7.1.97 YSML099-00 来自 SELECT ADF 的 FCI 中的自定义数据的响应

测试目的：确保终端忽略SELECT ADF命令返回的数据域中的自定义数据。

终端配置：N/A。

卡片配置：——卡包含一个ADF。

子类案例：——案例01：在ADF的FCI中，FCIFCI模板内，ADF的FCI（标签‘6F’）包含附加的自定义数据域；

——案例 02：ADF 的 FCI 中，发卡行任意自定数据（标签‘BF0C’）包含自定义数据域：标签 ‘9F7E’带有最大的长度和任意值；

——案例 03：ADF 的 FCI 中，FCI 模板 ADF 的 FCI（标签‘6F’）包含发卡行国家代码数据对象；

——案例 04：ADF 的 FCI 中，发卡行自定数据发卡行任意数据（标签‘BF0C’）包含发卡行国家代码数据对象（标签‘5F55’）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该忽略不可识别的或附加的借记/贷记应用数据对象。终端应该接受卡，来完成交易通过请求一个TC或AAC来完成交易。

7.1.98 YSML099-01 来自 SELECT PSE 的 FCI 中的自定义数据的响应

测试目的：确保终端若支持PSE选择，它应该忽略SELECT PSE命令返回的数据域中的自定义数据。

终端配置：支持PSE。

卡片配置：——卡包含一个PSE。

子类案例：——案例01：PSE的FCI中，FCI模板（标签‘6F’）包含附加的自定义数据域；

——案例02：PSE的FCI中，发卡行任意数据（标签‘BF0C’）包含自定义数据域：标签‘5F50’带有任意的长度和任意值；

——案例03：PSE的FCI中，FCI模板（标签‘6F’）包含发卡行国家代码数据对象；

——案例04：PSE的FCI中，发卡行任意数据（标签‘BF0C’）包含发卡行国家代码数据对象；

——案例05：PSE的FCI中，发卡行任意数据（标签‘BF0C’）包含数据域：标签‘5F54’银行标识符编码（BIC）、标签‘5F53’国际银行账户编号（IBAN）、标签‘5F55’发卡行国家代码’、标签‘5F56’ 发卡行国家代码、标签‘42’发卡行标识号。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该忽略不能识别的或附加的借记/贷记应用数据对象。终端在应用选

择阶段应该采用PSE选择，并通过请求一个TC或AAC来完成交易。

7.1.99 YSML100-01 PSE 选择中用于内部处理的附加数据对象

测试目的：确保终端若支持PSE选择，它应该忽略或使用PSE选择中用于内部处理的附加数据对象。

终端配置：支持PSE。

卡片配置：——卡包含一个PSE；

——ADF 入口的目录任意自定义模板（模板‘73’）包含数据域：标签‘5F54’银行标识符编码（BIC）、标签‘5F53’国际银行账户编号（IBAN）、标签‘5F55’发卡行国家代码’、标签‘5F56’ 发卡行国家代码、标签‘42’发卡行标识号。

测试流程：选择卡片应用，执行交易。

通过标准：终端在应用选择阶段应该采用PSE选择，并通过请求一个TC或AAC来完成交易。用于内部处理的附加数据对象或者被忽略或者被终端使用。

7.1.100 YSML103-00 可选脱机明文 PIN 的 VERIFY 数据域的格式

测试目的：——确保当CVM请求脱机明文PIN时，终端发送一个VERIFY命令，该命令数据域带有脱机明文PIN块；

——确保终端发送一个VERIFY命令，该命令数据域带有标签为‘99’的值域。

终端配置：支持脱机明文PIN。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；

——卡支持脱机明文PIN验证；

——卡中的CVM是‘脱机明文PIN，总是’（01 00）。

子类案例：——案例01：PIN长度是4；

——案例02：PIN长度是5；

——案例03：PIN长度是6；

——案例04：PIN长度是7；

——案例05：PIN长度是8；

——案例06：PIN长度是9；

——案例07：PIN长度是10；

——案例08：PIN长度是11；

——案例09：PIN长度是12。

测试流程：选择卡片应用，且对于所有长度的PIN进行测试，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该接收到一个有正确格式的VERIFY数据域，其中带有标签为‘99’的值域（没有标签和长度）。

7.1.101 YSML109-00 可选脱机明文 PIN 的 VERIFY 数据域的格式最大数据长度

测试目的：——确保当CVM选项为明文PIN时，终端发送一个VERIFY命令，该命令数据域带有明文脱机PIN的块。终端能够支持数据元具有最大数据长度；

——确保终端发送一个VERIFY命令，该命令数据域带有标签为‘99’的值域。

终端配置：支持明文PIN终端的所有数据元具有最大长度。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）。FCI模板具有最大长度（252字节），包含所有强制数据和可选数据（发卡行自定义数据除外）；

——卡支持脱机PIN验证；

——AID为16字节；

——应用首选名为16字节；

——应用标签为16字节；

——卡片支持4中首选语言（标签‘5F2D’）；

——在GPO命令中PDOL请求的数据长度超过128字节，PDOL的长度使FCI模板

达到最大长度；

——卡中的CVM是‘明文PIN验证，总是’（0100）。CDOL1请求终端所有的数据和其他数据（如果需要），使第一个GENERATE AC命令的数据域达到最大长度（255字节）。

子类案例：——案例01：PIN长度是4。每个记录只包含一个数据元（一个记录一个数据元）且所有的可选数据元都应存在；卡片中所有可变长度的数据元（一个记录一个数据元）应为最大长度，且每条记录应填充‘00’至254字节；

——案例02：PIN长度是5；

——案例03：PIN长度是6；

——案例04：PIN长度是7；

——案例05：PIN长度是8；

——案例06：PIN长度是9；

——案例07：PIN长度是10；

——案例08：PIN长度是11；

——案例09：PIN长度是12。

测试流程：卡中的应用被选择选择卡片应用，且对于所有长度的PIN进行测试，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.1.102 YSML110-00 最大数据长度：CVM 列表

测试目的：确保终端能够支持数据元具有最大数据长度。

终端配置：终端的所有数据元具有最大长度。

卡片配置：——FCI模板具有最大长度（252字节），包含所有强制数据和可选数据（发卡行自定义数据除外）；

——AID为16字节；

——应用首选名为16字节；

——应用标签为16字节；

——卡片支持4中首选语言（标签‘5F2D’）；

——在GPO命令中PDOL请求的数据长度超过128字节，PDOL的长度使FCI模板达到最大长度；

——CDOL1请求终端所有的数据和其他数据（如果需要），使第一个GENERATE AC命令的数据域达到最大长度（255字节）；

——每个记录只包含一个数据元（一个记录一个数据元）且所有的可选数据元都应存在；

——CVM列表长度为248字节（120个CVM入口），终端执行最后一个CVM入口；

——卡片中所有可变长度的数据元（一个记录一个数据元）应为最大长度，且每条记录应填充‘00’至254字节。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.1.103 YSML111-00 最大数据长度：发卡行脚本命令（1）

测试目的：确保终端能够支持数据元具有最大数据长度，特别是发卡行脚本命令。

终端配置：仅联机终端或有联机能力的脱机终端。

卡片配置：——FCI模板具有最大长度（252字节），包含所有强制数据和可选数据（发卡行自定义数据除外）；

——AID为16字节；

——应用首选名为16字节；

——应用标签为16字节；

——卡片支持4中首选语言（标签‘5F2D’）；

——在GPO命令中PDOL请求的数据长度超过128字节，PDOL的长度使FCI模板达到最大长度；
——CDOL1请求终端所有的数据和其他数据（如果需要），使第一个GENERATE AC命令的数据域达到最大长度（255字节）；
——每个记录只包含一个数据元（一个记录一个数据元）且所有的可选数据元都应存在；
——卡片中所有可变长度的数据元（一个记录一个数据元）应为最大长度，且每条记录应填充‘00’至254字节；
——卡片在第一个GENERATE AC命令返回ARQC；
——授权响应报文包含一个‘71’脚本，此脚本只包含一个命令，脚本的长度为终端所支持的最大长度（最短128字节，包括脚本头（标签和长度））；
——卡片对脚本命令返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡片应该在第二个GENERATE AC之前接收到脚本中所有的命令。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已执行）。在金融确认报文或批数据采集报文中，标签‘71’的发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。

7.1.104 YSML112-00 最大数据长度：发卡行脚本命令（2）

测试目的：确保如果授权或金融响应报文中包含一个或多个脚本，且脚本的总长度小于或等于128字节时，终端能够正确管理和执行脚本。

终端配置：仅联机终端或有联机能力的脱机终端。

卡片配置：——FCI模板具有最大长度（252字节），包含所有强制数据和可选数据（发卡行自定义数据除外）；
——AID为16字节；
——应用首选名为16字节；
——应用标签为16字节；
——卡片支持4中首选语言（标签‘5F2D’）；
——在GPO命令中PDOL请求的数据长度超过128字节，PDOL的长度使FCI模板达到最大长度；
——CDOL1请求终端所有的数据和其他数据（如果需要），使第一个GENERATE AC命令的数据域达到最大长度（255字节）；
——每个记录只包含一个数据元（一个记录一个数据元）且所有的可选数据元都应存在；
——卡片中所有可变长度的数据元（一个记录一个数据元）应为最大长度，且每条记录应填充‘00’至254字节；
——卡片的参数已设置，使交易能够联机完成；
——授权响应报文包含三个‘71’脚本，脚本的长度为终端所支持的在ICS中指明的最大值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡片应该接收到脚本中所有的命令。

7.1.105 YSML113-00 最大数据长度：发卡行脚本命令（3）

测试目的：确保如果授权或金融响应报文中包含一个或多个脚本，且脚本的总长度小于或等于128字节时，终端能够正确管理和执行脚本。

终端配置：仅联机终端或有联机能力的脱机终端。

卡片配置：——FCI模板具有最大长度（252字节），包含所有强制数据和可选数据（发卡行自定义数据除外）；
——AID为16字节；
——应用首选名为16字节；
——应用标签为16字节；
——卡片支持4中首选语言（标签‘5F2D’）；
——在GPO命令中PDOL请求的数据长度超过128字节，PDOL的长度使FCI模板达到最大长度；
——CDOL1请求终端所有的数据和其他数据（如果需要），使第一个GENERATE AC命令的数据域达到最大长度（255字节）；
——每个记录只包含一个数据元（一个记录一个数据元）且所有的可选数据元都应存在；
——卡片中所有可变长度的数据元（一个记录一个数据元）应为最大长度，且每条记录应填充‘00’至254字节；
——卡片的参数已设置，使交易能够联机完成；
——授权响应报文包含三个‘72’脚本，脚本的长度为终端所支持的在ICS中指明的最大值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡片应该接收到脚本中所有的命令。

7.1.106 YSML114-00 最大数据长度：发卡行脚本命令（4）

测试目的：确保终端能够支持数据元具有最大数据长度，特别是发卡行脚本命令。

终端配置：仅联机终端或有联机能力的脱机终端。

卡片配置：——FCI模板具有最大长度（252字节），包含所有强制数据和可选数据（发卡行自定义数据除外）；
——AID为16字节；
——应用首选名为16字节；
——应用标签为16字节；
——卡片支持4种首选语言（标签‘5F2D’）；
——在GPO命令中PDOL请求的数据长度超过128字节，PDOL的长度使FCI模板达到最大长度；
——CDOL1请求终端所有的数据和其他数据（如果需要），使第一个GENERATE AC命令的数据域达到最大长度（255字节）；
——每个记录只包含一个数据元（一个记录一个数据元）且所有的可选数据元都应存在；
——卡片中所有可变长度的数据元（一个记录一个数据元）应为最大长度，且每条记录应填充‘00’至254字节；
——卡片在第一个GENERATE AC命令返回ARQC；
——授权响应报文包含一个‘72’脚本，此脚本只包含一个命令，脚本的长度为终端所支持的最大长度（最短128字节，包括脚本头（标签和长度））；
——卡片对脚本命令返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡片应该在第二个GENERATE AC之前接收到脚本中所有的命令。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。在金融确认报文或批数据采集报文中TSI字节1，位3 =‘1’（脚本处理已执行）。在金融确认报文或批数据采集报文中，标签‘72’的发卡行脚本结果字节1应被

设置成‘20’，脚本执行成功。

7.1.107 YSML115-00 来自终端或者发卡行的数据（1）

测试目的：确保终端中的数据不会被卡片中的数据所代替。
终端配置：N/A。
子类案例：CDOL1请求以下子案例中的所有数据。在以下子案例中，从卡片记录中读出的终端或发卡行数据与终端或发卡行提供的数据不一致：
——案例 01：卡片的一个记录中包含标签‘授权金额’（数字型）；
——案例 02：卡片的一个记录中包含标签‘授权金额’（二进制型）；
——案例 03：卡片的一个记录中包含标签‘终端AID’；
——案例 04：卡片的一个记录中包含标签‘CVM结果’；
——案例 05：卡片的一个记录中包含标签‘商户分类码’；
——案例 06：卡片的一个记录中包含标签‘商户标识’；
——案例 07：卡片的一个记录中包含标签‘商户名称和地点’；
——案例 08：卡片的一个记录中包含标签‘POS输入方式’；
——案例 09：卡片的一个记录中包含标签‘终端标识’；
——案例 10：卡片的一个记录中包含标签‘终端性能’；
——案例 11：卡片的一个记录中包含标签‘终端验证结果’；
——案例 12：卡片的一个记录中包含标签‘交易日期’；
——案例 13：卡片的一个记录中包含标签‘交易类型’；
——案例 14：卡片的一个记录中包含标签‘交易状态信息’；
——案例 15：卡片的一个记录中包含标签‘不可预知数’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个 GENERATE AC命令域里的数据由终端提供，而不是被卡片中的具有相同标签的数据所替代。

7.1.108 YSML115-01 来自终端或者发卡行的数据（2）

测试目的：确保终端或发卡行的数据不会被卡片中的数据所代替。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：卡片的参数已设置，使交易能够联机完成。
子类案例：CDOL2请求以下子案例中的所有数据。在以下子案例中，从卡片记录中读出的终端或发卡行数据与终端或发卡行提供的数据不一致；
——案例 01：卡片的一个记录中包含标签‘发卡行认证数据’；
——案例 02：卡片的一个记录中包含标签‘授权响应码’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第二个 GENERATE AC命令域里的数据由发卡行提供，而不是被卡片中的具有相同标签的数据所替代。

7.1.109 YSML116-00 发卡行批准的交易（1）

测试目的：验证当发卡行认证失败，卡片在第二个GENERATE AC命令返回TC时，终端接收发卡行批准的交易。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：——卡片的参数已设置，使交易能够联机完成；
——卡的AIP指明支持发卡行认证认证（AIP的字节1，位3为‘1’）；
——后台应该在授权或金融响应中返回批准；
——模拟的发卡行认证数据以如下格式发送给终端：一个有效的8字节的授权响应密文和2字节表明批准的授权响应码；
——卡片返回‘6300’作为对外部认证命令的响应。
子类案例：卡响应第二个GENERATE AC命令：
——案例01：卡响应一个TC，没有通知（40）；

——案例02：卡响应一个TC，带有通知且无原因（48）；
——案例03：卡响应一个TC，带有通知且原因是发卡行认证失败（4B）。
测试流程：选择卡片应用，执行交易直到完成。
通过标准：终端应该处理交易直到完成，并批准交易。

7.1.110 YSML117-00 发卡行批准的交易（2）

测试目的：验证当发卡行认证失败，卡片在第二个GENERATE AC命令返回AAC时，终端拒绝发卡行批准的交易。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：——卡片的参数已设置，使交易能够联机完成；
——卡的AIP指明支持发卡行认证认证（AIP的字节1，位3为‘1’）；
——后台应该在授权或金融响应中返回批准；
——模拟的发卡行认证数据以如下格式发送给终端：一个有效的8字节的授权响应密文和2字节表明批准的授权响应码；
——卡片返回‘6300’作为对外部认证命令的响应。
子类案例：卡响应第二个GENERATE AC命令：
——案例01：卡响应一个AAC，没有通知（00）；
——案例02：卡响应一个AAC，带有通知且无原因（08）；
——案例03：卡响应一个AAC，带有通知且原因是发卡行认证失败（0B）。
测试流程：选择卡片应用，执行交易直到完成。
通过标准：终端应该处理交易直到完成，并拒绝交易。

7.1.111 YSML118-00 SELECT PSE 返回的数据顺序不同于规范规定

测试目的：确保终端如果支持 PSE 选择，它能够识别 SELECT PSE 命令返回的 FCI 数据，即使数据的顺序不同于规范规定。
终端配置：支持 PSE。
卡片配置：——卡含有 PSE；
——PSE 的 FCI 包含所有强制数据：FCI 模板（‘6F’），FCI 专用模板（‘A5’），目录文件的 SFI（‘88’），DF 名（‘84’）；
——PSE 的 FCI 包含所有可选数据，顺序如下：发卡行代码索引表（‘9F11’），首选语言（‘5F2D’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。卡应该接收到一个带有 SFI 的 READ RECORD 命令，其中的 SFI 根据 Select PSE 命令返回的 FCI 中的 SFI 进行编码。

7.1.112 YSML118-01 SELECT PSE 返回的数据中模板‘6F’或‘A5’中存在未期望的数据

测试目的：确保终端如果支持 PSE 选择，它能够识别 SELECT PSE 命令返回的 FCI 数据且忽略模板‘6F’或‘A5’中存在的未期望数据。
终端配置：支持 PSE。
卡片配置：卡含有 PSE。
子类案例：——案例 01：PSE 的 FCI 包含所有强制数据：FCI 模板（‘6F’），DF 名（‘84’），应用标签（‘50’），FCI 专用模板（‘A5’），目录文件的 SFI（‘88’）；
——案例 02：PSE 的 FCI 包含所有强制数据：FCI 模板（‘6F’），DF 名（‘84’），FCI 专用模板（‘A5’），目录文件的 SFI（‘88’），应用标签（‘50’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。卡应该接收到一个带有 SFI 的 READ RECORD 命令，其中的 SFI 根据 Select PSE 命令返回的 FCI 中的 SFI 进行编码。

7.1.113 YSML119-00 SELECT ADF 返回的在模板中的数据顺序

测试目的：确保终端接受 SELECT ADF 命令返回的数据的顺序不同于规范规定。
终端配置：终端支持卡片的一个应用。
卡片配置：——卡不支持 PSE；
——对于 SELECT ADF 命令，卡片返回的数据顺序如下：FCI 模板（‘6F’），FCI 专用模板（‘A5’），应用优先指示器（‘87’），应用标签（‘50’），应用首选名（‘9F12’），DF 名（‘84’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应选择应用并继续交易。

7.1.114 YSML119-01 SELECT PSE 返回的在模板中的数据顺序

测试目的：确保终端接受 SELECT PSE 命令返回的数据的顺序不同于规范规定。
终端配置：终端支持卡片的一个应用。
卡片配置：——卡支持 PSE；
——对于 SELECT PSE 命令，卡片返回的数据顺序如下：FCI 模板（‘6F’），FCI 专用模板（‘A5’），首选语言（‘5F2D’），发卡行索引代码表（‘9F11’），目录文件的 SFI（‘88’），DF 名（‘84’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端用 PSE 方式选择应用并继续交易。

7.1.115 YSML119-02 GET PROCESSING OPTIONS 返回的在模板中的数据顺序（格式二）

测试目的：确保终端接受 GET PROCESSING OPTIONS 命令返回的数据（格式二）的顺序不同于规范规定。
终端配置：N/A。
卡片配置：——卡支持 PSE；
——对于 GET PROCESSING OPTIONS 命令，卡片返回的数据（格式二）顺序如下：AFL（‘94’）,AIP（‘82’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应执行交易直到完成。

7.1.116 YSML119-03 第一次 GENERATE AC 返回的在模板中的数据顺序（格式二），未请求 CDA

测试目的：确保终端接受 GENERATE AC 命令返回的数据的顺序不同于规范规定。
终端配置：N/A。
卡片配置：对于第一次 GENERATE AC 命令，卡片返回的数据顺序如下：应用密文（‘9F26’），密文信息数据（‘9F27’），发卡行应用数据（‘9F10’），应用交易计数器（‘9F36’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应选择应用，继续交易直到完成。

7.1.117 YSML119-04 第二次 GENERATE AC 返回的在模板中的数据顺序（格式二），未请求 CDA

测试目的：确保终端接受 GENERATE AC 命令返回的数据的顺序不同于规范规定。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：——卡片的参数已设置，使交易能够联机完成；
——对于第二次 GENERATE AC 命令，卡片返回的数据顺序如下：应用交易计数器（‘9F36’），应用密文（‘9F26’），密文信息数据（‘9F27’），发卡行应用数据（‘9F10’）。
测试流程：选择卡片应用，交易进行联机处理。
通过标准：终端应选择应用，继续交易直到完成。

7.1.118 YSML119-05 第一次 GENERATE AC 返回的在模板中的数据顺序（格式二），请求 CDA

测试目的：确保终端接受 GENERATE AC 命令返回的数据的顺序不同于规范规定。
终端配置：支持 CDA。
卡片配置：——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——IAC 和 TAC 的设置使终端在第一次 GENERATE AC 请求 TC；
——对于第一次 GENERATE AC 命令，卡片返回的数据（格式二）顺序如下：发卡行应用数据（‘9F10’），签名的动态应用数据（‘9F4B’），密文信息数据（‘9F27’），应用交易计数器（‘9F36’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应选择应用，继续交易直到完成。

7.1.119 YSML119-06 第二次 GENERATE AC 返回的在模板中的数据顺序（格式二），请求 CDA

测试目的：确保终端接受 GENERATE AC 命令返回的数据的顺序不同于规范规定。
终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
卡片配置：——卡的AIP指明支持CDA（AIP的字节1，位1=‘1’）；
——IAC 和 TAC 的设置使终端在第一次 GENERATE AC 请求 ARQC；
——在联机处理中，发卡行应批准交易；
——对于第二次 GENERATE AC 命令，卡片返回的数据（格式二）顺序如下：签名的动态应用数据（‘9F4B’），应用交易计数器（‘9F36’），密文信息数据（‘9F27’），发卡行应用数据（‘9F10’）。
测试流程：选择卡片应用，交易联机处理。
通过标准：终端应选择应用，继续交易直到完成。

7.1.120 YSML119-07 读取目录文件 READ RECORD 返回的在模板中的数据的顺序

测试目的：确保终端接受读取目录文件 READ RECORD 命令返回的数据的顺序不同于规范规定。
终端配置：——支持 PSE；
——终端支持卡片中的一个应用。
卡片配置：——卡支持PSE；
——IAC 和 TAC 的设置使终端在第一次 GENERATE AC 请求 ARQC 和 CDA；
——在联机处理中，发卡行应批准交易；
——对于读取支付系统目录文件的 READ Record 命令，卡片返回的 ADF 入口数据的顺序如下：应用标签（‘50’），应用首选名（‘9F12’），DF 名（‘4F’），应用优先指示器（‘87’）。
测试流程：用 PSE 方式进行应用选择，执行交易直到完成，并批准交易。
通过标准：终端应使用PSE方式进行应用选择，不转换到AID列表方式。执行交易直到完成，并批准交易。

7.1.121 YSML120-00 SELECT PSE 的响应存在填充数据

测试目的：确保当 SELECT PSE 的响应存在填充数据时，终端能够继续进行应用选择。
终端配置：支持 PSE。
子类案例：——案例01（模板‘BF0C’中存在填充数据，在原有的数据之前）；
——案例02（模板‘BF0C’中存在填充数据，在原有的数据之后）；
——案例03（模板‘BF0C’中存在填充数据，在原有的数据之间）。
测试流程：选择卡片应用，执行交易直到完成，并批准交易。
通过标准：终端应使用PSE方式进行应用选择，不转换到AID列表方式。执行交易直到完

成，并批准交易。

7.1.122 YSML120-01 读取 PSE 支付系统目录文件的响应存在填充数据

测试目的：确保当读取 PSE 目录文件的响应存在填充数据时，终端能够继续进行应用选择。
终端配置：支持 PSE。
子类案例：——案例01（填充数据在第一个模板‘61’之前）；
——案例02（填充数据在两个模板‘61’之间）；
——案例03（填充数据在最后一个模板‘61’之后）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应使用PSE方式进行应用选择，不转换到AID列表方式。执行交易直到完成，并批准交易。

7.1.123 YSML121-00 最小数据长度（1）

测试目的：确保终端能够支持数据元长度为最小。
终端配置：——仅脱机终端；
——终端的所有数据元长度都为最小。
卡片配置：——IAC和TAC的设置使交易批准。
——FCI模板包含：AID长度为5字节，应用首选名长度为1字节，应用标签长度为1字节，卡片支持1种首选语言（标签‘5F2D’），PDOL为空。
——CVM列表为最小长度（一条持卡人验证方法）。
——卡片中所有可变长度的数据元应为最小长度。
测试流程：选择卡片应用，执行交易直到完成，并批准交易。
通过标准：终端应通过请求一个TC来完成交易。

7.1.124 YSML121-01 最小数据长度（2）

测试目的：确保终端能够支持数据元长度为最小。
终端配置：——仅联机终端或有联机能力的脱机终端；
——终端的所有数据元长度都为最小。
卡片配置：——IAC和TAC的设置使交易联机并批准。
——FCI模板包含：AID长度为5字节，应用首选名长度为1字节，应用标签长度为1字节，卡片支持1种首选语言（标签‘5F2D’），PDOL为空。
——CVM列表为最小长度（一条持卡人验证方法）。
——卡片中所有可变长度的数据元应为最小长度。
测试流程：选择卡片应用，交易联机并批准。
通过标准：终端应通过请求一个TC来完成交易。

7.2 应用选择（YYXZ）

7.2.1 YYXZ002-00 PSE 的定义

测试目的：确保终端若支持PSE选择，它应该识别PSE格式，特别是且PSE的FCI以及可选数据对象。
终端配置：支持PSE。
卡片配置：N/A。
测试流程：用PSE方式进行应用选择。用PSE的应用选择处理被执行。
通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该接收到一个带有SFI的READ RECORD命令，其中的SFI根据Select PSE命令返回的FCI中的SFI进行编码。

7.2.2 YYXZ004-00 支付系统目录中记录的定义

测试目的：确保终端若支持PSE选择，它应该识别包含在PSE目录文件中记录的格式，特别是带有多个入口的记录。
终端配置：支持PSE。
卡片配置：——PSE包含一个带有多个ADF入口的目录文件；
——目录的第一个记录包含3个ADF入口。
测试流程：对于所有支持的具有优先级的应用优先级，都能用PSE方式进行应用选择执行PSE的应用选择方式。
通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该接收到一个带有SFI的READ RECORD命令，其中的SFI根据SELECT PSE命令的返回的FCI中的SFI进行编码。

7.2.3 YYXZ005-00 目录入口格式的定义

测试目的：确保终端若支持PSE选择，它应该忽略可能出现在目录入口中的非期望标签和出现在目录记录中但未包含在应用模板中的其他数据对象。
终端配置：支持PSE。
卡片配置：PSE包含一个带有多个ADF入口的目录文件。
子类案例：目录文件的第一个记录包含：
——案例 01：模板‘70’包含：应用首选名称，发卡行标识符；
——案例 02：模板‘70’包含：带有最大长度和任意值的私有标签‘5F05’；
——案例 03：模板‘73’包含：带有最大长度和任意值的私有标签‘5F05’。
测试流程：用PSE方式进行应用选择。执行PSE应用选择。
通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该接收到一个带有SFI的READ RECORD命令，其中的SFI根据SELECT PSE命令的返回的FCI中的SFI进行编码。

7.2.4 YYXZ007-00 终端支持的应用列表

测试目的：验证终端能够维护带有AID的应用列表。
终端配置：N/A。
卡片配置：卡片不支持PSE选择，强制让终端使用应用其他的选择技术应用选择方式（通过使用它的AID列表方式）。
测试流程：用AID列表方式进行应用选择。执行AID列表的应用选择，进行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端用存储在终端内的每一个AID发送SELECT命令。

7.2.5 YYXZ010-00 AID 的匹配（1）

测试目的：确保终端对于每个应用保存存一个指示，用以指明使用哪一种个匹配标准。
终端配置：支持持卡人确认。
卡片配置：——卡包含中的一个应用的AID与保存在终端中一个应用的AID匹配的应用；
——显示给持卡人显示一个应用列表。
子类案例：——案例01：卡片不包含其他应用；
——案例02：卡片包含终端支持的其他应用。
测试流程：用AID列表方式进行应用选择。执行AID列表的应用选择，进行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该提示持卡人哪些应用可以选择。

7.2.6 YYXZ010-01 AID 的匹配（2）

测试目的：确保终端对于每个应用保存一个指示，用以指明使用哪一种个匹配标准。
终端配置：不支持持卡人确认。

卡片配置：——卡中一个应用的AID与保存在终端中的优先级最高的应用的AID相匹配；
——显示给持卡人一个列表。
子类案例：——案例01：卡片不包含其他应用；
——案例02：卡片包含终端支持的其他应用。
测试流程：用AID列表方式进行应用选择。执行AID列表的应用选择，进行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该选择优先级最高的应用。

7.2.7 YYXZ011-00 AID的匹配：以终端AID开始的AID（1）

测试目的：确保终端对于每个应用保存一个指示，用以指明使用哪一个匹配标准。
终端配置：——支持持卡人确认；
——终端支持3个AID，但其中一个支持的AID值与卡中所有AID的开端相匹配。所有的AID都具有ASI表明接受部分匹配。
卡片配置：——卡包含3个应用，这些应用的AID与保存在终端里的一个AID部分匹配；
——卡中的应用有不同的优先级；
——给持卡人显示一个应用列表，显示给持卡人一个列表。
测试流程：用AID列表方式进行应用选择。执行AID列表的应用选择，进行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该向持卡人表明哪些应用可以选择。

7.2.8 YYXZ011-01 AID的匹配：以终端AID开始的AID（2）

测试目的：确保终端对于每个应用保存一个指示，用以指明使用哪一个匹配标准。
终端配置：——不支持持卡人确认；
——终端支持3个AID，但其中一个支持的AID值与卡中所有AID部分匹配。所有的AID都具有ASI表明接受部分匹配。
卡片配置：——卡应包含3个应用。这些应用的AID与保存在终端里的一个AID部分匹配；
——卡中的应用有不同的优先级。
测试流程：a）用AID列表方式进行应用选择；
b）执行AID列表的应用选择，进行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该选择优先级最高的应用。

7.2.9 YYXZ012-00 使用支付系统目录的选择：SELECT PSE

测试目的：确保终端若支持PSE选择，它应发出一个SELECT‘1PAY-SYS-DDF01’命令。
终端配置：支持PSE。
卡片配置：卡片对SELECT PSE命令返回给选择PSE的响应为‘9000’，并返回响应数据。
测试流程：用PSE方式进行应用选择。执行PSE应用选择。
通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应收到一个SELECT‘1PAY-SYS-DDF01’命令。

7.2.10 YYXZ013-00 使用支付系统目录的选择：卡片锁定或命令不支持

测试目的：确保终端若支持PSE选择，且卡片返回‘6A81’作为对SELECT PSE命令的响应，终端应终止交易。
终端配置：支持PSE。
卡片配置：卡对SELECT PSE命令返回‘6A81’。
测试流程：用PSE方式进行应用选择。执行PSE应用选择。
通过标准：终端应该终止交易。

7.2.11 YYXZ016-00 表明记录结束

测试目的：确保终端若支持PSE选择，终端选择PSE并发送READ RECORD命令，直到卡响

应‘6A83’。

终端配置：支持PSE。

卡片配置：卡的PSE目录文件包含一个在两个记录，两个记录中有三个入口的PSE目录文件。

测试流程：用PSE方式进行应用选择。执行PSE应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该发送一系列READ RECORD命令，直到卡响应‘6A83’。

7.2.12 YYXZ017-00 目录入口不存在

测试目的：确保终端若支持PSE选择，且卡对READ RECORD记录1的响应是‘6A83’，则终端应该转换到应用AID列表选择方式。

终端配置：支持PSE。

卡片配置：卡对PSE目录文件的记录1的READ RECORD命令的响应是‘6A83’。

测试流程：用PSE方式进行应用选择。执行PSE应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在卡对PSE目录文件的记录1的READ RECORD命令的响应‘6A83’后，终端应该发送一系列SELECT AID命令。

7.2.13 YYXZ018-00 目录入口的处理（1）

测试目的：确保终端如果支持PSE选择，终端应该从目录文件的第一个记录的第一个入口开始，依次处理每个入口。

终端配置：——支持PSE；
——支持持卡人确认；
——不支持优先选择顺序。
——终端支持卡目录文件目录中列出的所有的ADF（仅在应用选择处理中）。

卡片配置：——卡的目录文件包含一个在一个记录，这个记录中有三个入口的目录文件；
——卡中所有的应用都没有优先级。

测试流程：用PSE方式进行应用选择。执行PSE应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。所有终端和卡共同支持的应用都应该显示给持卡人。

7.2.14 YYXZ019-01 完全匹配的候选列表（1）

测试目的：确保终端如果支持PSE选择，只要目录文件的入口与终端支持的其中一个应用名完全匹配，则终端将应用加入到候选列表。

终端配置：——支持PSE；
——支持卡片确认；
——终端支持卡目录文件中所列出的所有ADF（仅在应用选择处理中）。

卡片配置：——卡包含一个PSE目录文件带有应用1、应用2和应用3的入口；
——卡包含3个应用（ADF）（所有的都在PSE目录文件中列出）；
——卡中所有应用的AID与终端支持的应用部分匹配。

子类案例：——案例01：目录文件中的所有入口都有优先权，有最高优先权的是第一个入口；
——案例02：目录文件中的所有入口都有优先权，有最高优先权的是第二个入口；
——案例03：目录文件中的所有入口都有优先权，有最高优先权的是第三个入口；

测试流程：用PSE方式进行应用选择。执行PSE应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。所有在候选列表里的应用都应该显示给持卡人。

7.2.15 YYXZ019-02 完全匹配的候选列表（2）

测试目的：确保终端如果支持PSE选择，只要目录文件的入口与终端支持的其中一个应用名完全匹配，则终端将应用加入到候选列表。
终端配置：——支持PSE；
——不支持卡片确认；
——终端支持卡目录文件中所列出的所有ADF（仅在应用选择处理中）。
卡片配置：——卡包含一个PSE目录文件带有应用1、应用2和应用3的入口；
——卡包含3个应用（ADF）（所有的都在PSE目录文件中列出）；
——应用3有最高的优先级；
——卡中所有应用的AID与终端支持的应用部分匹配。
测试流程：用PSE方式进行应用选择。执行PSE应用选择。
通过标准：终端应该通过请求一个TC或AAC来完成交易。
终端选择有最高优先级的应用。

7.2.16 YYXZ019-04 部分匹配的候选列表（1）

测试目的：确保终端如果支持PSE选择，只要目录文件的入口与终端支持的其中一个应用名部分匹配，且ASI支持部分匹配，则终端将应用加入到候选列表。
终端配置：——终端支持卡目录文件中所列出的所有ADF（仅在应用选择处理中）；
——ASI支持部分匹配。
卡片配置：——卡包含一个PSE目录文件带有应用1、应用2和应用3的入口；
——卡包含3个应用（ADF）（所有的都在PSE目录文件中列出）；
——卡中所有应用的AID与终端支持的应用部分匹配。
测试流程：用PSE方式进行应用选择。执行PSE应用选择。
通过标准：终端应该通过请求一个TC或AAC来完成交易。所有在候选列表里的应用都应该显示给持卡人。

7.2.17 YYXZ019-05 部分匹配的候选列表（2）

测试目的：确保终端如果支持PSE选择，只要目录文件的入口与终端支持的其中一个应用名部分匹配，且ASI支持部分匹配，则终端将应用加入到候选列表。
终端配置：——支持PSE；
——不支持卡片确认；
——终端支持卡目录文件中列出的所有的ADF（仅在应用选择处理中）；
——ASI支持部分匹配。
卡片配置：——卡包含一个PSE目录文件带有应用1、应用2和应用3的入口；
——卡包含3个应用（ADF）（所有的都在PSE目录文件中列出）；
——应用3有最高的优先级；
——卡中所有应用的AID与终端支持的应用部分匹配。
测试流程：用PSE方式进行应用选择。执行PSE应用选择。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端选择有最高优先级的应用。

7.2.18 YYXZ023-00 PSE 选择后候选列表为空

测试目的：确保终端如果支持PSE选择，且目录文件中没有与终端支持应用相匹配的入口，则终端转换到AID列表选择方式。
终端配置：支持PSE。
卡片配置：在选择PSE处理期间，不存在与终端支持的应用相匹配的目录文件入口。
测试流程：用PSE方式进行应用选择。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该转换到AID列表选择方式。

7.2.19 YYXZ023-01 PSE 选择 READ RECORD 的失败处理（1）

测试目的：确保如果在PSE应用选择中执行READ RECORD 时发生返回的状态码错误（不

是‘9000’或‘6A83’），终端应该清除候选列表并转为AID列表选择方式。

终端配置：支持PSE。

卡片配置：——卡包含一个PSE；

——卡片和终端有3个共同支持的应用。

子类案例：在PSE选择的第二个READ RECORD命令，卡片响应如下状态码：

——案例01：卡对READ RECORD响应状态码‘6300’；

——案例02：卡对READ RECORD响应状态码‘6283’；

——案例03：卡对READ RECORD响应状态码‘6300’；

——案例04：卡对READ RECORD响应状态码‘63Cx’；

——案例05：卡对READ RECORD响应状态码‘6983’；

——案例06：卡对READ RECORD响应状态码‘6984’；

——案例07：卡对READ RECORD响应状态码‘6985’；

——案例08：卡对READ RECORD响应状态码‘6A81’；

——案例09：卡对READ RECORD响应状态码‘6A82’；

——案例10：卡对READ RECORD响应状态码‘6A88’；

——案例11：卡对READ RECORD响应状态码‘6400’；

——案例12：卡对READ RECORD响应状态码‘6500’；

——案例13：卡对READ RECORD响应状态码‘9001’。

测试流程：首先用PSE方式进行应用选择，然后转为AID列表选择方式候选列表中的第一个应用被选择，然后被从候选列表中删除，终端发起对第二个共同支持应用的选择。

通过标准：当收到响应的错误的状态码，终端应该终止PSE处理，回到应用选择功能阶段，使用AID列表进行选择。

7.2.20 YYXZ024-00 AID 列表选择

测试目的：——确保终端能够正确使用AID列表进行选择；

——确保终端如果使用AID列表的选择方式，它应该从终端支持的应用用列表中的第一个AID发送第一个SELECT命令。

终端配置：支持多个应用。

卡片配置：N/A。

测试流程：用AID列表方式进行应用选择。使用AID列表方式选择应用。

通过标准：终端应该通过请求一个TC或AAC来完成交易；卡接收到第一个SELECT ‘AID’命令，该命令应该带有终端支持的AID列表中第一个AID；对于终端支持的每个应用，卡都应该接收到一个SELECT ‘AID’命令。

7.2.21 YYXZ025-06 DF 名称和 AID 相同并且 SELECT 命令成功

测试目的：确保如果卡片中应用的DF名称和终端的AID相同，且SELECT命令成功（SW1 SW2为‘9000’），终端应将所选择文件卡片该应用的的FCI信息添加到候选列表，并继续用终端列表中下一个AID发送另一个SELECT命令。

终端配置：——终端支持用AID选择；

——终端至少支持2个应用。

卡片配置：——卡至少支持在第一个SELECT命令中指明的应用（AID名和DF名相同）；

——卡对第一个SELECT命令响应‘9000’。

测试流程：用AID列表方式进行应用选择。使用AID列表方式选择应用。

通过标准：终端应该通过请求一个TC或AAC来完成交易；包括最终SELECT命令在内，终端应该发送至少三个SELECT命令。

7.2.22 YYXZ026-05 DF 名称和 AID 相同并且应用锁定

测试目的：确保如果卡片中应用的DF名称和终端的AID相同，且卡片中该应用已经锁定（SW1 SW2为‘6283’），终端将用列表中下一个AID发送另一个SELECT命令，

并且不将该应用DF名称加到候选列表中。

终端配置：——终端支持用AID选择；
——终端至少支持2个应用。

卡片配置：卡对第一个SELECT命令响应‘6283’。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易；终端应该发送至少两个SELECT命令；在应用选择期间，对于终端第一个Select命令的响应为‘6283’的第一个AID应用不应在用于最终选择的候选列表中。

7.2.23 YYXZ028-00 AID 列表选择

测试目的：确保当终端选择列表中的下一个应用时，如果卡响应的状态码不是‘9000’、‘6A81’或‘6283’，终端不将这个AID加入候选列表。

终端配置：终端至少支持3种与卡至少共同支持的3个AID。

子类案例：对于其中一个种共同支持的AID进行发送SELECT命令时，卡响应如下状态码：
——案例01：卡片返回状态‘6300’作为SELECT 应用命令的响应；
——案例02：卡片返回状态‘63Cx’作为SELECT 应用命令的响应；
——案例03：卡片返回状态‘6983’作为SELECT 应用命令的响应；
——案例04：卡片返回状态‘6984’作为SELECT 应用命令的响应；
——案例05：卡片返回状态‘6985’作为SELECT 应用命令的响应；
——案例06：卡片返回状态‘6A82’作为SELECT 应用命令的响应；
——案例07：卡片返回状态‘6A83’作为SELECT 应用命令的响应；
——案例08：卡片返回状态‘6A88’作为SELECT 应用命令的响应；
——案例09：卡片返回状态‘9001’作为SELECT 应用命令的响应；
——案例10：卡片返回状态‘6400’作为SELECT 应用命令的响应；
——案例11：卡片返回状态‘6500’作为SELECT 应用命令的响应。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡在对于终端SELECT以上指定的AID，卡片响应状态码非‘9000’、‘6A81’或‘6283’时，它卡片应该继续接收到一个SELECT ‘AID’命令，该命令带有终端AID列表中的下一个AID。终端应该指示给持卡人哪些应用可以被选择或者选择剩余两个共同支持的应用中的一个。

7.2.24 YYXZ029-00 AID 列表选择：候选列表完成

测试目的：确保在终端列表中已经没有AID可以选择时，终端能够完成候选列表。

终端配置：支持持卡人确认。

卡片配置：——终端与卡至少共同支持2个AID。终端和卡片至少有2种共同支持的AID；
——卡中包含一种终端不支持的AID；
——给持卡人显示一个应用列表。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该接收到对于终端列表中所有AID的SELECT AID命令。终端应该显示给持卡人哪些应用可以被选择。

7.2.25 YYXZ031-00 ASI 应用选择指示符：完全匹配

测试目的：——确保如果IC卡中的DF名比终端中AID的要长，但是它们直到终端AID的最后一个字符都是相同的，则终端应该检查应用选择指示符；
——如果应用选择指示符指明部分匹配是不允许的，则终端应不将该AID加入到候选列表，并且用下一个AID来重发SELECT命令。

终端配置：N/A。

卡片配置：——对于第一个AID选择，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID的最后一个字符都是相同的；

——终端应用选择指示符只允许被选择的AID出现一次（完全匹配）；
——卡片包含另一个应用的DF名与终端AID完全匹配。

测试流程：用AID列表方式进行应用选择。使用AID列表方式选择应用。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在SELECT AID命令后，卡应该：或者接收P2选项设置为‘下一个’的SELECT ‘AID’命令，直到卡响应‘6A82’；或者是接收一个带有下一个AID名的SELECT ‘AID’命令。终端应该不将第一个AID添加到候选列表中。

7.2.26 YYXZ031-06 DF 名称比 AID 长、部分匹配并且应用未锁定

测试目的：——确保如果 IC 卡中的 DF 名比终端中 AID 的要长，但是它们直到终端 AID 的最后一个字符都是相同的，则终端应该检查应用选择指示符；
——如果指示符表明部分匹配是允许的，应用没有锁定，则终端将 AID 加入到候选列表，并重发 SELECT 命令，该命令使用于以前相同的命令数据，但将 P2 设置为 ‘02’ 。

终端配置：——终端与卡至少共同支持3个AID；
——终端应用选择指示符允许被选择的AID多次出现（部分匹配）。

卡片配置：——卡片包含3个应用；
——对于第一个卡片和终端共同支持的AID，卡片AID选择，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID的最后一个字符都是相同的；
——卡片中每个应用的应用优先指示器指明的应用优先级是不同的，应用优先级最高的AID在最后一个SELECT NEXT命令返回；
——卡对第一次SELECT NEXT命令响应状态码‘9000’。

子类案例：——案例01：卡对第二次SELECT NEXT命令响应状态码‘6A82’；
——案例02：卡对第二次SELECT NEXT命令响应状态码‘9000’，卡对第三次SELECT NEXT命令响应状态码‘6A82’；
——案例03：卡对第二次和第三次SELECT NEXT命令响应状态码‘9000’，卡对第四次SELECT NEXT命令响应状态码‘6A82’。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个SELECT AID命令后，卡应该接收到若干个P2选项设置为‘下一个’的SELECT AID命令。最终选择终端应该以完整的AID发送Select命令，并继续用这个AID完成交易将SELECT NEXT命令响应‘9000’的AID添加到候选列表中。

7.2.27 YYXZ031-07 DF 名称比 AID 的长、部分匹配并且应用锁定

测试目的：——确保如果 IC 卡中的 DF 名比终端中 AID 的要长，但是它们直到终端 AID 的最后一个字符都是相同的，则终端应该检查应用选择指示符；
——如果应用选择指示符表明部分匹配是允许的，应用被锁定，则终端将 AID 加入到候选列表，并重发 SELECT 命令，该命令使用于以前相同的命令数据，但是 P2 设置为 ‘02’ 。

终端配置：——终端至少支持1个AID；
——终端应用选择指示符允许被选择的AID多次出现（部分匹配）。

卡片配置：——对于第一个终端第一个Select AID命令选择，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID的最后一个字符都是相同的；
——卡片对第一次SELECT命令响应状态码‘6283’。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该请求一个TC或AAC来完成交易。第一个SELECT AID命令后，卡应该接收到P2选项设置为‘下一个’的SELECT AID命令，直到卡片返回‘6A82’。终端不应该将第一个AID添加到候选列表中。

7.2.28 YYXZ031-08 DF 名称比 AID 的长、部分匹配

测试目的：确保若终端和卡片共同支持若干个应用，终端应该给持卡人提供一个应用列表进行确认，终端应该选择持卡人确认的那个应用。

终端配置：——支持持卡人确认；
——终端和卡片有3个AID匹配（终端里的AID为5字节）；
——终端应用选择指示符允许被选择的AID多次出现（部分匹配）。

卡片配置：——卡片包含3个应用；
——对于卡片和终端共同支持的AID，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID的最后一个字符都是相同的；
——卡片中DF名长于终端AID的部分AID1：10 10 01，AID2：10 10 00，AID3：10 10 03；
——卡片对第一、二、三次SELECT NEXT命令响应状态码‘9000’，对第四次SELECT NEXT命令响应状态码‘6A82’。

子类案例：——案例01：持卡人选择应用1；
——案例02：持卡人选择应用2；
——案例03：持卡人选择应用3。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC来完成交易。第一个SELECT AID命令后，卡应该接收到若干个P2选项设置为‘下一个’的SELECT AID命令。终端应提供一个应用列表给持卡人进行确认，并在最终选择以持卡人确认的那个AID发用Select命令（案例01对应AID1，案例02对应AID2，案例03对应AID3）。最终选择的AID与建立候选列表时卡返回的由持卡人确认的ADF应该一致。

7.2.29 YYXZ032-00 DF 名与 AID 不同

测试目的：确保如果卡片返回的 FCI 中的 DF 名称与终端用于选择 AID 的不同或是比其短，则终端不应该重发使用部分名称选项的 SELECT 命令，而是继续处理终端列表中下一个 AID。

终端配置：终端至少支持2个AID。

子类案例：——案例01：对于第一个AID选择，卡片返回FCI中的DF名比终端用于选择的AID短；
——案例02：对于第一个AID选择，卡片返回FCI中的DF名称与终端用于选择的AID不同。

测试流程：用AID列表方式进行应用选择。使用AID列表方式选择应用。

通过标准：终端应该通过请求一个TC或AAC来完成交易。对于在第一个SELECT AID 的FCI中命令，卡片返回错误的AID名并响应‘9000’后，卡片应该接收到带有终端列表中下一个应用AID的SELECT AID命令。

7.2.30 YYXZ034-00 应用部分匹配：支持下一个选项：90-00

测试目的：确保如果卡对于带有‘下一个’选项的SELECT命令返回‘9000’，则终端将选择文件FCI中的DF名称加入到候选列表并继续应用选择处理。

终端配置：——终端的应用选择指示符允许AID部分匹配；
——终端至少支持2个AID。

卡片配置：——对于终端第一个Select AID命令，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID的最后一个字符都是相同的。对于第一个AID选择，卡片返回FCI中的DF名称比终端用于选择的AID的要长，——但是它们直到终端AID中的最后一个字符都是相同的；
——卡对带有‘下一个’选项的SELECT命令返回‘9000’（卡中3个种应用带有相同的AID的开头）。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该接收到一系列的的SELECT AID命令（ P2选项设置为‘下一个’），直到卡响应‘6A82’。在接收这一系列命令后，卡应该接收到带有终端列表中下一个应用AID的SELECT AID命令。

7.2.31 YYXZ035-00 应用部分匹配：下一个选项失败：6283

测试目的：确保如果卡对于带有‘下一个’选项的SELECT命令返回‘6283’，则终端不会将该AID加入到候选列表；在选择终端列表中下一个AID前，终端应继续发送带有‘下一个’选项的SELECT命令。

终端配置：终端至少支持2个AID。

卡片配置：——对于终端第一个Select AID命令，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID的最后一个字符都是相同的。对于第一个AID选择，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID中的最后一个字符是相同的；

——卡对带有‘下一个’选项的第一个SELECT命令返回‘6283’；

——卡对带有‘下一个’选项的接下来的SELECT命令返回‘6A82’。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端以发送状态为‘6283’响应上述指定AID发送SELECT AID命令，卡片响应状态‘6283’时的SELECT后，卡应该继续接收到SELECT AID命令，且该命令 P2选项设置为‘下一个’，并且命令域中AID的值也与前一个相同。候选列表应该不包含SELECT命令返回‘6283’的AID。

7.2.32 YYXZ036-00 应用部分匹配：下一个选项失败：其他

测试目的：确保如果卡对带有‘下一个’选项的SELECT命令返回的状态码不是‘9000’或‘6283’，终端继续对AID列表中下一个应用发送SELECT命令。

终端配置：终端至少支持2个AID。

卡片配置：对于终端第一个Select AID命令，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID的最后一个字符都是相同的。对于第一个AID选择，卡片返回FCI中的DF名称比终端用于选择的AID的要长，但是它们直到终端AID中的最后一个字符都是相同的。

子类案例：——案例01：卡片返回状态‘6300’作为对带有‘下一个’选项的SELECT命令的响应；

——案例 02：卡片返回状态‘63Cx’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 03：卡片返回状态‘6983’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 04：卡片返回状态‘6984’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 05：卡片返回状态‘6985’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 06：卡片返回状态‘6A81’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 07：卡片返回状态‘6A82’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 08：卡片返回状态‘6A83’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 09：卡片返回状态‘6A88’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 10：卡片返回状态‘6400’作为对带有‘下一个’选项的 SELECT 命令的响应；

——案例 11：卡片返回状态‘6500’作为对带有‘下一个’选项的 SELECT 命令的响应；
——案例 12：卡片返回状态‘9001’作为对带有‘下一个’选项的 SELECT 命令的响应。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端以上述指定AID发送SELECT AID命令，卡片在发送SELECT选择上述指定的AID卡片响应状态码非‘9000’或‘6283’时，卡应该接收到SELECT AID命令，该命令带有终端AID列表中下一个应用的AID。

7.2.33 YYXZ037-00 最终选择：无共同支持的应用

测试目的：确保如果终端和卡片没有共同支持的应用（候选列表为空），则终端终止交易。

终端配置：N/A。

卡片配置：卡片和终端没有相互匹配的AID。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该终止交易。

7.2.34 YYXZ038-00 最终选择：一个共同支持的应用

测试目的：确保如果只有一个AID是终端和卡片共同支持的且应用优先指示符的位8为‘0’，则终端自动选择这个AID。

终端配置：N/A。

卡片配置：——卡片和终端只有一个相互匹配的AID；
——卡片返回的应用优先指示符的位8为‘0’。

测试流程：a）用AID列表方式进行应用选择；
b）使用AID列表方式选择应用。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该自动选择这个共同支持的AID。

7.2.35 YYXZ038-01 最终选择：终端 AID 匹配 DF 名和卡 AID

测试目的：确保若终端在最终选择时所用的AID和卡片FCI返回的DF名相同，终端设置其数据元“应用标识符（AID）—终端”（标签‘9F06’）的值与卡片FCI返回的DF名相同。

终端配置：N/A。

卡片配置：——卡片和终端有一个相互匹配的AID；
——卡片返回的FCI中的DF名和卡片AID的值相同；
——卡片返回的应用优先指示符的位8为‘0’。

子类案例：卡片的PDOL请求终端AID：
——案例 01：AID为5字节；
——案例 02：AID为7字节；
——案例 03：AID为8字节；
——案例 04：AID为16字节。

测试流程：用AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC来完成交易。终端应该选择这个共同支持的AID。GPO 命令域里终端 AID（‘9F06’）的值应该与卡片 FCI 返回的 DF 名（‘84’）相同。

7.2.36 YYXZ039-00 最终选择：持卡人确认 （1）

测试目的：确保如果只有一个AID是终端和卡片共同支持的，应用优先指示符的位8为‘1’且终端支持持卡人确认，终端应请求持卡人确认，如果持卡人批准则选择这

个应用。
终端配置：支持持卡人确认。
卡片配置：——卡片和终端有一个相互匹配的AID；
——卡片返回的应用指示符的位8为‘1’。
测试流程：用AID列表方式进行应用选择。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该请求持卡人的确认，并产生发送一个SELECT命令作为对该确认的响应。

7.2.37 YYXZ039-01 最终选择：持卡人确认 （2）

测试目的：确保如果有若干个AID是终端和卡片共同支持的，终端应请求持卡人确认，终端根据持卡人确认的应用发送最终选择命令。
终端配置：支持持卡人确认。
卡片配置：——卡片和终端有3个相互匹配的AID：AID1=xx xx xx xx xx 10 10 01，AID2=xx xx xx xx xx 10 10 02，AID3=xx xx xx xx xx 10 10 03，其中xx xx xx xx xx对于3个AID是相同的。
子类案例：——案例 01：持卡人选择AID1；
——案例 02：持卡人选择AID2；
——案例 03：持卡人选择AID3。
测试流程：用AID列表方式进行应用选择。
通过标准：终端应该通过请求一个TC来完成交易。终端应该请求持卡人确认，并根据持卡人确认的应用发送最终SELECT AID命令（案例01选择AID1，案例02选择AID2，案例03选择AID3）。最终选择命令里的AID与卡片返回的DF名相同。

7.2.38 YYXZ040-00 最终选择：不支持持卡人确认

测试目的：确保如果只有一个AID是终端和卡片共同支持的，应用优先指示符的位8为‘1’且终端不支持持卡人确认，则终端终止交易。
终端配置：不支持持卡人确认。
卡片配置：——卡片和终端有一个相互匹配的AID；
——卡片返回的应用指示符的位8为‘1’。
测试流程：使用AID或PSE方式进行应用选择。
通过标准：终端应该终止交易。

7.2.39 YYXZ041-00 最终选择：持卡人不批准

测试目的：确保如果只有一个AID是终端和卡片共同支持的，应用优先指示符的位8为‘1’且终端支持持卡人确认但持卡人不批准，则终端终止交易。
终端配置：支持持卡人确认。
卡片配置：——卡片和终端有一个相互匹配的AID；
——卡片返回的应用指示符的位8为‘1’；
——持卡人不批准这个选择。
测试流程：用PSE或AID列表方式进行应用选择。
通过标准：终端应该终止交易。

7.2.40 YYXZ042-00 显示应用给持卡人：优先顺序

测试目的：确保如果多个种应用是终端和卡片共同支持的，并且终端支持列表显示，则终端按照优先级的顺序显示列表。
终端配置：支持持卡人确认。
卡片配置：——卡片和终端有三个相互匹配的AID；
——应用有不同的优先级。
测试流程：用AID列表方式进行应用选择。使用AID列表方式选择应用。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该显示一个应用列表，

该列表按照应用的其优先级排序（最高优先级在第一个）。

7.2.41 YYXZ042-01 显示应用给持卡人：支持持卡人确认

测试目的：确保如果多个种应用是终端和持卡人共同支持的，并支持持卡人确认，则终端应该将所有的共同支持的应用提示给持卡人。
终端配置：支持持卡人确认。
卡片配置：卡片和终端有三个相互匹配的AID。
测试流程：用AID列表方式进行应用选择。使用AID列表方式选择应用。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该显示一个完整的卡和终端共同支持的应用列表。

7.2.42 YYXZ049-00 不支持持卡人确认的终端应用选择

测试目的：确保如果多个应用是终端和持卡人共同支持的确保如果多种应用是共同支持的，优先级存在并不需要确认，则终端应该选择优先级最高的应用。
终端配置：不支持持卡人确认。
卡片配置：——卡片和终端有三个相互匹配的AID；
——应用有不同的优先级；
——应用优先级指示符中不要求确认；
——终端不将列表显示给持卡人。
测试流程：用AID列表方式进行应用选择。使用AID列表方式选择应用。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该选择有最高优先级的应用，并发送最终SELECT AID命令（其AID为带有最高优先级的应用）。

7.2.43 YYXZ050-00 不支持持卡人确认的终端应用选择：需要确认

测试目的：确保如果多个应用是终端和卡片共同支持的，终端不支持列表显示，卡片中应用有优先级顺序且一些应用需要确认，则终端应该选择带有最高优先级的应用（且不需要确认的应用）。
终端配置：不支持持卡人确认。
卡片配置：——卡片和终端有三个相互匹配的AID；
——应用有不同的优先级；
——有最高优先级的应用需要持卡人确认；
——终端不将应用列表显示给持卡人。
测试流程：a）用AID列表方式进行应用选择；
b）使用AID列表方式选择应用。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该选择有最高优先级的应用（且不需要确认的应用），并发送最终SELECT AID命令（其AID为具有最高优先级且不需要确认的应用）。

7.2.44 YYXZ053-00 来自候选列表的最终应用选择：AID 列表（1）

测试目的：确保一旦一个应用被选择，则终端应该发送一个使用，以之前从这个应用FCI中读取的DF名称发送SELECT命令（如果采用AID列表方式进行应用选择使用AID列表方式选择应用）。
终端配置：不支持持卡人确认。
卡片配置：——卡片和终端有三个相互匹配的AID；
——应用有不同的优先级；
——终端采用AID列表方式进行应用选择使用AID列表的选择方式进行处理。
测试流程：用AID列表方式进行应用选择使用AID列表方式选择应用。
通过标准：终端应该通过请求一个TC或AAC来完成交易。卡在接收到一系列以个对于终端列表中所有AID发送的SELECT命令后，它应该接收到一个最终SELECT命令，该命令带有优先级最高的应用的DF名称。

7.2.45 YYXZ053-01 来自候选列表的最终应用选择：AID 列表（2）

测试目的：确保一旦一个应用被选择，则终端应该使用之前从FCI中读取的DF名称发送SELECT命令（如果采用AID列表方式进行应用选择，使用AID列表方式选择应用）。

终端配置：支持持卡人确认。

卡片配置：——卡片和终端有三个相互匹配的AID；
——应用有不同的优先级；
——终端采用AID列表方式进行应用选择使用AID列表的选择方式进行处理。

测试流程：用AID列表方式进行应用选择使用AID列表方式选择应用。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡在接收到一系列以终端列表中所有AID发送的SELECT命令后，卡在接收到一个对于终端列表中所有AID的SELECT命令后，它应该接收到一个最终SELECT命令，该命令带有持卡人所选应用的DF名称。

7.2.46 YYXZ054-00 来自候选列表的最终应用选择：PSE

测试目的：确保如果终端支持并采用PSE方式进行应用选择执行PSE方式的应用选择，一旦最终被选择的应用确定，则终端将以从发送一个PSE使用目录中读取的ADF名称发送一个SELECT命令。

终端配置：支持PSE。

卡片配置：——终端支持PSE；
——卡片和终端有三个相互匹配的AID；
——应用有不同的优先级；
——终端采用PSE方式进行应用选择，使用PSE方式的应用选择。

测试流程：用PSE方式进行应用选择。使用PSE方式选择应用。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡在接收到对于卡目录中所有记录的READ RECORD命令后，它应该接收到一个最终SELECT命令，该命令带有具有最高优先级应用的ADF名称。终端应该选择这个应用。

7.2.47 YYXZ055-00 来自候选列表的应用最终选择：SELECT 状态码不同于 90-00

测试目的：确保如果卡对最终选择应用的SELECT命令返回的状态码不是‘9000’，则终端将该应用从共同支持的应用的列表中删除，并返回最终应用选择应用处理阶段。

终端配置：N/A。

卡片配置：——卡片和终端有三个相互匹配的AID；
——应用有不同的优先级。

子类案例：卡在收到应用最终选择命令后返回的状态码不是‘9000’：
——案例01：卡片返回状态‘6283’作为基于最终选择的SELECT命令的响应；
——案例02：卡片返回状态‘6300’作为基于最终选择的SELECT命令的响应；
——案例03：卡片返回状态‘63Cx’作为基于最终选择的SELECT命令的响应；
——案例04：卡片返回状态‘6983’作为基于最终选择的SELECT命令的响应；
——案例05：卡片返回状态‘6984’作为基于最终选择的SELECT命令的响应；
——案例06：卡片返回状态‘6985’作为基于最终选择的SELECT命令的响应；
——案例07：卡片返回状态‘6A81’作为基于最终选择的SELECT命令的响应；
——案例08：卡片返回状态‘6A82’作为基于最终选择的SELECT命令的响应；
——案例09：卡片返回状态‘6A83’作为基于最终选择的SELECT命令的响应；
——案例10：卡片返回状态‘6A88’作为基于最终选择的SELECT命令的响应；
——案例11：卡片返回状态‘9001’作为基于最终选择的SELECT命令的响应；
——案例12：卡片返回状态‘6400’作为基于最终选择的SELECT命令的响应；
——案例13：卡片返回状态‘6500’作为基于最终选择的SELECT命令的响应。

测试流程：使用AID列表或PSE方式选择应用或AID列表方式进行应用选择。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在卡响应给最终选择的状态码不是‘9000’时，终端应该将该应用从候选列表中删除并应该返回最终选择处理阶段。第二次个选择处理应用选择期间产生的候选列表不再包含上述最终选择期间所选的应用。

7.3 安全方面（AQFM）

7.3.1 AQFM003-00 对于每个 RID 终端应该能够存储 6 个 CA 索引

测试目的：确保如果终端支持SDA，它应该能够存储6个CA公钥以及与密钥同时用到的相关信息，并能够在给定RID和CA公钥索引后定位相应密钥。

终端配置：支持SDA。

卡片配置：——终端支持3个RID（RID1、RID2和RID3）；
——对于每个RID，终端都载入6个CA公钥（密钥索引从00到05）；
——卡的AIP指明支持SDA（AIP的字节1，位7为‘1’）。

子类案例：——案例01：卡包含基于RID1、密钥索引为00的静态签名和相关数据；
——案例02：卡包含基于RID1、密钥索引为01的静态签名和相关数据；
——案例03：卡包含基于RID1、密钥索引为02的静态签名和相关数据；
——案例04：卡包含基于RID1、密钥索引为03的静态签名和相关数据；
——案例05：卡包含基于RID1、密钥索引为04的静态签名和相关数据；
——案例06：卡包含基于RID1、密钥索引为05的静态签名和相关数据；
——案例07：卡包含基于RID2、密钥索引为00的静态签名和相关数据；
——案例08：卡包含基于RID2、密钥索引为01的静态签名和相关数据；
——案例09：卡包含基于RID2、密钥索引为02的静态签名和相关数据；
——案例10：卡包含基于RID2、密钥索引为03的静态签名和相关数据；
——案例11：卡包含基于RID2、密钥索引为04的静态签名和相关数据；
——案例12：卡包含基于RID2、密钥索引为05的静态签名和相关数据；
——案例13：卡包含基于RID3、密钥索引为00的静态签名和相关数据；
——案例14：卡包含基于RID3、密钥索引为01的静态签名和相关数据；
——案例15：卡包含基于RID3、密钥索引为02的静态签名和相关数据；
——案例16：卡包含基于RID3、密钥索引为03的静态签名和相关数据；
——案例17：卡包含基于RID3、密钥索引为04的静态签名和相关数据；
——案例18：卡包含基于RID3、密钥索引为05的静态签名和相关数据。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 = ‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.2 AQFM004-00 SDA 的算法

测试目的：——确保对于静态数据认证，终端支持特定的可逆算法；
——确保终端在静态数据认证中支持发卡行公钥算法标识为‘01’；
——确保终端在静态数据认证中支持哈希算法标识为‘01’。

终端配置：支持SDA。

卡片配置：——卡中的静态签名是正确的（它是通过使用可逆算法计算出）；
——卡中发卡行公钥证书是使用发卡行公钥算法标识为‘01’计算的；
——卡中发卡行公钥证书是使用哈希算法标识为‘01’计算的；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 = ‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.3 AQFM006-00 所有模的位长度

测试目的：确保对于静态数据认证，终端支持的模数的位长度是8的倍数。
终端配置：支持SDA。
卡片配置：——卡中的静态签名是有效的；
——使用的模的长度是8的倍数；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）；
——案例01：测试针对CA公钥；
——案例02：测试针对发卡行公钥。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 = ‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.4 AQFM007-00 CA 公钥指数的值

测试目的：确保终端支持静态数据认证中CA公钥的指数为3和$2^{16}+1$。
终端配置：支持SDA。
卡片配置：——卡中的静态签名是有效的；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
子类案例：——案例01：CA公钥指数为3；
——案例02：CA公钥指数为 $2^{16}+1$。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.5 AQFM008-00 发卡行公钥指数的值

测试目的：确保终端支持静态数据认证中发卡行公钥的指数为3和 $2^{16}+1$。
终端配置：支持SDA。
卡片配置：——卡中的静态签名是有效的；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
子类案例：——案例01：发卡行公钥指数为3；
——案例02：发卡行公钥指数为 $2^{16}+1$。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 = ‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.6 AQFM009-00 数据缺失：CA 公钥索引

测试目的：——确保如果IC卡中缺少CA公钥索引，终端的静态数据认证失败；
——确保如果在AIP中脱机静态数据认证是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。
终端配置：支持SDA。
卡片配置：——卡中缺少CA公钥索引；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.7 AQFM010-00 数据缺失：发卡行公钥证书

测试目的：确保如果IC卡中缺少发卡行公钥证书，终端的静态数据认证失败。
终端配置：支持SDA。
卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.8 AQFM011-00 数据缺失：发卡行公钥指数

测试目的：确保如果IC卡中缺少发卡行公钥指数，终端的静态数据认证失败。
终端配置：支持SDA。
卡片配置：——卡中缺少发卡行公钥指数；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.9 AQFM012-00 数据缺失：签名静态应用数据

测试目的：——确保如果IC卡中缺少签名的静态应用数据，终端的静态数据认证失败；
——确保如果在AIP中SDA是支持的，且卡中缺少静态应用数据，则终端设置TVR中‘IC卡数据缺失’位为‘1’。
终端配置：支持SDA。
卡片配置：——卡中缺少静态应用数据；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，

位6 = ‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 = ‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.10 AQFM014-00 CA 公钥恢复用于执行 SDA：密钥不存在

测试目的：确保如果终端支持静态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的静态数据认证失败。

终端配置：——支持SDA；
——终端不包含卡中引用的CA公钥。

卡片配置：卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 = ‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 = ‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.11 AQFM014-01 CA 公钥恢复用于执行 DDA：密钥不存在

测试目的：确保如果终端支持动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的动态数据认证处理失败。

终端配置：——支持DDA；
——终端不包含卡中引用的CA公钥。

卡片配置：卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 = ‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 = ‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.12 AQFM014-02 CA 公钥恢复用于执行 CDA：密钥不存在

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使第一个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个GENERATE AC应不请求CDA。终端应该依据TAC和IAC设置请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 = ‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.13 AQFM014-04 CA 公钥恢复用于执行 CDA：密钥不存在（2）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败；
——终端不包含卡中引用的CA公钥。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使第一个GENERATE AC请求TC。
测试流程：选择卡片应用，执行交易。
通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.14 AQFM014-05 CA公钥恢复用于执行CDA：密钥不存在（3）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败；
——终端不包含卡中引用的CA公钥。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC时卡返回ARQC；
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC，第二个GENERATE AC请求TC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.15 AQFM014-06 CA公钥恢复用于执行CDA：密钥不存在（4）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败；
——终端不包含卡中引用的CA公钥。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC时卡返回ARQC；

——设置IAC和TAC使终端第一个GENERATE AC请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 = ‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 = ‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1,位7 = ‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 = ‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时（万一终端请求AAC而缺少第二个GENERATE AC，此通过标准仅在终端有能力存储失败交易时生效），其字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.16 AQFM014-07 CA 公钥恢复用于执行 CDA：密钥不存在（5）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——终端无法联机；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码 ；
——终端行为分析前不能探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC时卡返回ARQC；
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.17 AQFM014-08 CA 公钥恢复用于执行 CDA：密钥不存在（6）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC。
——交易联机批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端在第一个和第二个GENERATE AC应不请求CDA。终端应该通过请求一个TC

来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.18 AQFM014-09 CA 公钥恢复用于执行 CDA：密钥不存在（7）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC；
——交易联机拒绝。

测试流程：选择卡片应用，执行交易。

通过标准：终端在第一个和第二个GENERATE AC应不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.19 AQFM015-00 发卡行公钥证书的长度

测试目的：确保如果终端支持静态数据认证，且发卡行公钥证书的长度与CA公钥模数的值不同，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

子类案例：——案例01：卡中发卡行公钥证书的长度大于终端中CA公钥模数的值；
——案例02：卡中发卡行公钥证书的长度小于终端中CA公钥模数的值。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.20 AQFM017-00 恢复数据的结尾不是‘BC’

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中发卡行公钥证书被恢复，但其数据结尾不是‘BC’；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.21 AQFM018-00 恢复数据头不是‘6A’

测试目的：确保如果从发卡行公钥证书中恢复的数据头不是‘6A’，则终端的静态数据认证处理失败。
终端配置：支持SDA。
卡片配置：——卡中发卡行公钥证书被恢复，但其数据头不是‘6A’；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.22 AQFM019-00 证书格式不等于 ‘02’

测试目的：确保如果从发卡行公钥证书中恢复的证书格式不是‘02’，则终端的静态数据认证处理失败。
终端配置：支持SDA。
卡片配置：——卡中发卡行公钥证书被恢复，但其证书格式不是‘02’；
——卡的AIP指明支持SDA（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.23 AQFM020-00 计算出的哈希结果与恢复的哈希结果不同

测试目的：确保如果从发卡行公钥证书中计算出的哈希结果与恢复的哈希结果不同，则终端的静态数据认证处理失败。
终端配置：支持SDA。
卡片配置：——卡中发卡行公钥证书使用带有不正确的哈希值的数据计算得到；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
子类案例：——案例01：哈希值的第一字节有错误；
——案例02：哈希值的最后一个字节有错误。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.24 AQFM021-00 发卡行标识符与 PAN 最左端 3 到 8 位数字不匹配

测试目的：确保如果恢复的发卡行标识符与PAN最左端3到8位数字不匹配，则终端的静态数据认证处理失败。
终端配置：支持SDA。
卡片配置：卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
子类案例：——案例01：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不

同的发卡行标识符：所有3到8位数字不同。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.25 AQFM022-00 证书失效日期早于今天日期

测试目的：确保如果证书失效日期早于今天日期，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中发卡行公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.26 AQFM023-00 无效的 RID、CA 公钥索引以及证书序列号，SDA

测试目的：确保如果RID、CA公钥索引及证书序列号连接起来的结果表明是已回收的证书，则终端的静态数据认证处理失败。

终端配置：——支持SDA；
——支持发卡行公钥证书的回收；
——终端支持3个RID；
——终端内每个RID装载30个CRL入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡中发卡行公钥证书包含RID、CA公钥索引及证书序列号，该证书存在于终端的回收列表中；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

子类案例：——案例01：终端装载30条CRL入口，指定RID 1在回收列表中；
——案例02：终端装载30条CRL入口，指定RID 2在回收列表中；
——案例03：终端装载30条CRL入口，指定RID 3在回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.27 AQFM023-01 证书回收列表的更新，移除

测试目的：确保终端能够通过删除入口更新证书回收列表。

终端配置：——支持SDA；
——支持发卡行公钥证书的回收。

卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位6为‘0’；字节1，位5为‘0’；字节1，位1为‘0’）；
——执行PBOC交易前，证书回收列表更新已完成；

——卡中发卡行公钥证书包含RID、CA公钥索引及证书序列号，该证书已从终端证书回收列表中移除。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。

7.3.28 AQFM023-02 证书回收列表的更新，增加

测试目的：确保终端能够通过增加入口更新证书回收列表。

终端配置：——支持SDA；
——支持发卡行公钥证书的回收；
——终端已装载29个证书回收列表入口，案例AQFM02700已先于此案例执行。

卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位6为‘0’；字节1，位5为‘0’；字节1，位1为‘0’）；
——执行PBOC交易前，证书回收列表更新已完成；
——卡中发卡行公钥证书包含RID、CA公钥索引及证书序列号，该证书已装载在终端证书回收列表中。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是静态数据认证）；
c）请注意：案例AQFM02700应先于此案例执行。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.29 AQFM024-00 不识别的发卡行公钥算法

测试目的：确保如果发卡行公钥算法不支持（不是‘01’），则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中发卡行公钥证书不是使用公钥算法标识为‘01’的算法计算的；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.30 AQFM026-00 签名静态应用数据长度不正确

测试目的：确保如果终端支持静态数据认证，且签名静态应用数据的长度与发卡行公钥模数的值不同，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：卡的AIP指明支持SDA（AIP的字节1，位7为‘1’）。

子类案例：——案例01：签名静态应用数据的长度大于卡中发卡行公钥模的长度；
——案例02：签名静态应用数据的长度小于卡中发卡行公钥模的长度。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3

='0'（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.3.31 AQFM028-00 恢复数据的结尾不是‘BC’

测试目的：确保如果从签名的静态应用数据中恢复的数据结尾不是'BC'，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中签名的静态应用数据被恢复，但其数据结尾不是'BC'；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为'1'）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 ='1'（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 ='0'（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.3.32 AQFM029-00 恢复数据头不是‘6A’

测试目的：确保如果从签名的静态应用数据中恢复的数据头不是'6A'，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中发卡行公钥证书被恢复，但其数据头不是'6A'；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为'1'）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 ='1'（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 ='0'（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.3.33 AQFM030-00 证书格式不为‘03’

测试目的：确保如果从签名静态应用数据中恢复的证书格式不是'03'，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中签名静态应用数据不是使用证书格式为'03'的数据计算得到；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为'1'）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 ='1'（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 ='0'（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.3.34 AQFM031-00 计算出的哈希结果与恢复的哈希结果不同

测试目的：确保如果从签名静态应用数据中计算出的哈希结果与恢复的哈希结果不同，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中签名静态应用数据使用带有不正确的哈希值的数据计算得到；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为'1'）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.35 AQFM032-00 静态数据认证中的SDA标签列表（1）

测试目的：确保终端在执行SDA时检查SDA标签列表只包含AIP。
终端配置：支持SDA。
卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
子类案例：——案例01：SDA标签列表包含AFL；
——案例02：SDA标签列表包含AFL和AIP。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.36 AQFM032-01 静态数据认证中的SDA标签列表（2）

测试目的：确保终端在执行SDA时检查SDA标签列表只包含AIP。
终端配置：支持SDA。
卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）；
——SDA标签列表包含标签‘82’（AIP）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.37 AQFM033-00 数据认证码的存储

测试目的：确保在执行SDA时，终端将数据认证码存储在标签‘9F45’中。
终端配置：支持SDA。
卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）；
——CDOL1请求标签‘9F45’；
——数据认证码为‘DAC0’。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。在接收到第一个GENERATE AC命令时，标签‘9F45’中的值为‘DAC0’。

7.3.38 AQFM036-00 对于每个RID终端应该能存储6个CA索引（1）

测试目的：确保如果终端支持动态数据认证，且它能够存储6个CA公钥及与密钥一起使用的相关信息，则在给定RID和CA公钥索引时，终端能够定位到相应密钥。
终端配置：支持DDA。
卡片配置：——终端支持2个RID（RID1和RID2）；
——对于每个RID，终端都载入6个CA公钥（从公钥索引00至05）；

——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

子类案例：——案例01：卡包含基于RID1、密钥索引01产生正确的动态签名和相关数据；
——案例02：卡包含基于RID1、密钥索引03产生正确的动态签名和相关数据；
——案例03：卡包含基于RID1、密钥索引04产生正确的动态签名和相关数据；
——案例04：卡包含基于RID2、密钥索引01产生正确的动态签名和相关数据；
——案例05：卡包含基于RID2、密钥索引03产生正确的动态签名和相关数据；
——案例06：卡包含基于RID2、密钥索引04产生正确的动态签名和相关数据。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.39 AQFM036-01 对于每个RID，终端应该能存储6个CA索引（2）

测试目的：确保如果终端支持复合动态数据认证，且它能够存储6个CA公钥及与密钥一起使用的相关信息，则在给定RID和CA公钥索引时，终端能够定位到相应密钥。

终端配置：支持CDA。

卡片配置：——终端支持2个RID；
——对于每个RID，终端都载入6个CA公钥（公钥索引从00至05），如测试案例AQFM03800；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

子类案例：——案例01：卡包含基于RID1、密钥索引00产生正确的动态签名和相关数据；
——案例02：卡包含基于RID1、密钥索引02产生正确的动态签名和相关数据；
——案例03：卡包含基于RID1、密钥索引05产生正确的动态签名和相关数据；
——案例04：卡包含基于RID2、密钥索引01产生正确的动态签名和相关数据；
——案例05：卡包含基于RID2、密钥索引02产生正确的动态签名和相关数据；
——案例06：卡包含基于RID2、密钥索引05产生正确的动态签名和相关数据。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息中的TSI 的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.40 AQFM037-00 DDA的算法（1）

测试目的：——确保对于动态数据认证，终端支持特定的可逆算法；
——确保对于动态数据认证，终端支持发卡行公钥算法标识为‘01’；
——确保对于动态数据认证，终端支持IC卡公钥算法标识为‘01’；
——确保对于动态数据认证，终端支持哈希算法标识为‘01’。

终端配置：支持DDA。

卡片配置：——卡计算出的动态签名是有效的（它是通过使用可逆算法计算出）；
——卡中发卡行公钥证书用算法标识为‘01’的公钥算法计算得到；
——卡中IC卡公钥证书用算法标识为‘01’的公钥算法计算得到；
——卡中发卡行公钥证书用算法标识为‘01’的哈希算法计算得到；
——卡中IC卡公钥证书用算法标识为‘01’的哈希算法计算得到；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR

字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.41 AQFM037-01 DDA 的算法（2）

测试目的：——确保对于CDA，终端支持特定的可逆算法；
——确保在复合动态数据认证中，终端支持发卡行公钥算法标识为‘01’；
——确保在复合动态数据认证中，终端支持IC卡公钥算法标识为‘01’；
——确保在复合动态数据认证中，终端支持哈希算法标识为‘01’。
终端配置：支持CDA。
卡片配置：——卡计算出的动态签名是有效的（它是通过使用可逆算法计算出）；
——卡中发卡行公钥证书用算法标识为‘01’的公钥算法计算得到；
——卡中IC卡公钥证书用算法标识为‘01’的公钥算法计算得到；
——卡中发卡行公钥证书用算法标识为‘01’的哈希算法计算得到；
——卡中IC卡公钥证书用算法标识为‘01’的哈希算法计算得到；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息中的TSI 的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.42 AQFM039-00 所有模的位长度

测试目的：确保对于动态数据认证，终端支持的模数的位长度是8的倍数。
终端配置：支持DDA。
卡片配置：——卡计算的动态签名是有效的；
——对于CA密钥、发卡行密钥和IC卡密钥，使用的模的长度是8的倍数；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.43 AQFM039-01 所有模的位长（2）

测试目的：确保对于复合动态数据认证，终端支持的模数的位长度是8的倍数。
终端配置：支持CDA。
卡片配置：——卡计算的动态签名是有效的；
——对于CA密钥、发卡行密钥和IC卡密钥，使用的模的长度是8的倍数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息中的TSI 的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.44 AQFM040-00 CA公钥指数的值（1）

测试目的：确保终端支持动态数据认证中CA公钥的指数为3和 $2^{16}+1$。
终端配置：支持DDA。
卡片配置：——卡计算的动态签名是有效的；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
子类案例：——案例01：CA公钥指数为3；
——案例02：CA公钥指数为 $2^{16}+1$。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.45 AQFM040-01 CA公钥指数的值（2）

测试目的：确保终端支持复合动态数据认证中CA公钥的指数为3和 $2^{16}+1$。
终端配置：支持CDA。
卡片配置：——卡计算的动态签名是有效的；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。
子类案例：——案例01：CA公钥指数为3；
——案例02：CA公钥指数为 $2^{16}+1$。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息中的TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.46 AQFM041-00 发卡行公钥指数的值（1）

测试目的：确保终端支持动态数据认证中发卡行公钥的指数为3和 $2^{16}+1$。
终端配置：支持DDA。
卡片配置：——卡计算的动态签名是有效的；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
子类案例：——案例01：发卡行公钥指数为3；
——案例02：发卡行公钥指数为 $2^{16}+1$。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.47 AQFM041-01 发卡行公钥指数的值（2）

测试目的：确保终端支持复合动态数据认证中发卡行公钥的指数为3和 $2^{16}+1$。
终端配置：支持CDA。
卡片配置：——卡计算的动态签名是有效的；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。
子类案例：——案例01：发卡行公钥指数为3；
——案例02：发卡行公钥指数为 $2^{16}+1$。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息中的TSI 的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.48 AQFM042-00 IC卡公钥指数的值（1）

测试目的：确保终端支持动态数据认证中IC卡公钥的指数为3和 $2^{16}+1$。

终端配置：支持DDA。

卡片配置：——卡计算的动态签名是有效的；

——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

子类案例：——案例01：IC卡公钥指数为3；

——案例02：IC卡公钥指数为 $2^{16}+1$。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.49 AQFM042-01 IC卡公钥指数的值（2）

测试目的：确保终端支持复合动态数据认证中IC卡公钥的指数为3和 $2^{16}+1$。

终端配置：支持CDA。

卡片配置：——卡计算的动态签名是有效的；

——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

子类案例：——案例01：发卡行公钥指数为3；

——案例02：发卡行公钥指数为 $2^{16}+1$。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息中的TSI 的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.50 AQFM043-00 数据缺失：CA公钥索引（1）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端动态数据认证处理失败；

——确保如果在AIP中DDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：支持DDA。

卡片配置：——卡中缺少CA公钥索引；

——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.51 AQFM043-01 数据缺失：CA 公钥索引（2）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.52 AQFM043-02 数据缺失：CA 公钥索引（3）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.53 AQFM043-03 数据缺失：CA 公钥索引（4）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；

——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡在第一个GENERATE AC命令时返回ARQC；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.54 AQFM043-04 数据缺失：CA 公钥索引（5）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡在第一个GENERATE AC命令时返回ARQC；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.55 AQFM043-05 数据缺失：CA 公钥索引（6）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；

——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡在第一个GENERATE AC命令时返回ARQC；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.56 AQFM044-00 数据缺失：发卡行公钥证书（1）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端动态数据认证处理失败；
——确保如果在AIP中指明支持脱机动态数据认证，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：支持DDA。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.57 AQFM044-01 数据缺失：发卡行公钥证书（2）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.58 AQFM044-02 数据缺失：发卡行公钥证书（3）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.59 AQFM044-03 数据缺失：发卡行公钥证书（4）

测试目的：——确保如果 IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前没有探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.60 AQFM044-04 数据缺失：发卡行公钥证书（5）

测试目的：——确保如果IC卡中缺少发卡行公钥证书， 终端复合动态数据认证处理失败；

——确保如果在AIP中支持CDA，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；

——仅联机终端；

——CDA从不请求，第一个GAC请求ARQC时；

——CDA总是请求，在第二个GAC请求TC时；

——终端行为分析前没有探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；

——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——卡在第一个GENERATE AC命令返回ARQC；

——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；

——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.61 AQFM044-05 数据缺失：发卡行公钥证书（6）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；

——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；

——仅联机终端；

——CDA从不请求，第一个GAC请求ARQC时；

——当不能联机时，正常处理缺省行为码；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；

——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.62 AQFM044-06 数据缺失：发卡行公钥证书（7）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.63 AQFM044-07 数据缺失：发卡行公钥证书（8）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机拒绝。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC

来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.64 AQFM045-00 数据缺失：发卡行公钥指数（1）

测试目的：——确保如果IC卡中缺少发卡行公钥指数，终端对DDA处理失败；
——确保如果在AIP中指明支持脱机动态数据认证，且卡中缺少发卡行公钥指数，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：支持DDA。

卡片配置：——卡中缺少发卡行公钥指数；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.65 AQFM045-01 数据缺失：发卡行公钥指数（2）

测试目的：——确保如果IC卡中缺少发卡行公钥指数，终端复合动态数据认证处理失败；
——确保如果在AIP中支持复合动态数据认证，且卡中缺少发卡行公钥指数，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥指数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应在GENERATE AC命令中不请求CDA。终端应该依据TAC和IAC设置请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.66 AQFM045-02 数据缺失：发卡行公钥指数（3）

测试目的：——确保如果IC卡中缺少发卡行公钥指数，终端复合动态数据认证处理失败；
——确保如果在AIP中支持复合动态数据认证，且卡中缺少发卡行公钥指数，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥指数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第

二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.67 AQFM045-03 数据缺失：发卡行公钥指数（4）

测试目的：——确保如果IC卡中缺少发卡行公钥指数，终端复合动态数据认证处理失败；
——确保如果在AIP中支持复合动态数据认证，且卡中缺少发卡行公钥指数，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——第一个GENAC请求ARQC时，CDA总是请求；
——终端行为分析前没有探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥指数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.68 AQFM045-04 数据缺失：发卡行公钥指数（5）

测试目的：——确保如果IC卡中缺少发卡行公钥指数，终端复合动态数据认证处理失败；
——确保如果在AIP中支持复合动态数据认证，且卡中缺少发卡行公钥指数，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前没有探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥指数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；

——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.69 AQFM045-05 数据缺失：发卡行公钥指数（6）

测试目的：——确保如果IC卡中缺少发卡行公钥指数，终端复合动态数据认证处理失败；

——确保如果在AIP中复合动态数据认证是支持的，且卡中缺少发卡行公钥指数，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；

——仅联机终端；

——CDA从不请求，第一个GAC请求ARQC时；

——当不能联机时，正常处理缺省行为码；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥指数；

——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——卡在第一个GENERATE AC命令返回ARQC；

——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；

——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.70 AQFM046-00 数据缺失：IC卡公钥证书（1）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端动态数据认证处理失败；

——确保如果在AIP中指明动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：支持DDA。

卡片配置：——卡中缺少IC卡公钥证书；

——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 ='1'（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 ='1'（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 ='0'（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 ='0'（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.3.71 AQFM046-01 数据缺失：IC卡公钥证书（2）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；
——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中'IC卡数据缺失'位为'1'。

终端配置：——支持CDA；
——在终端行为分析之前检测到CDA失败。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为'1'）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 ='1'（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 ='1'（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 ='0'（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.3.72 AQFM046-04 数据缺失：IC卡公钥证书（3）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；
——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中'IC卡数据缺失'位为'1'。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为'1'）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中或金融确认信息或批上送信息中的TVR字节1，位3 ='1'（CDA失败）。
第二个GENERATE AC命令中的TVR字节1，位6 ='1'（IC卡数据缺失），或包含在金融确认信息或批上送信息中（当终端有存储失败或终止交易能力时此通过标准适用）；或终端有类似打印凭证功能来显示TVR。第一个GENERATE AC命令中的TVR字节1，位7 ='0'（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 ='1'（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 ='1'（脱机数据认证已进行）。

7.3.73 AQFM046-05 数据缺失：IC卡公钥证书（4）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；

——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时或当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.74 AQFM046-06 数据缺失：IC卡公钥证书（5）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；
——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.75 AQFM046-07 数据缺失：IC卡公钥证书（6）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；

——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.76 AQFM047-00 数据缺失：IC卡公钥指数（1）

测试目的：——确保如果IC卡中IC卡公钥指数缺失，终端动态数据认证失败；
——确保如果在AIP中指明支持脱机动态数据认证并且卡中IC卡公钥指数缺失，终端在TVR中设置‘IC卡数据缺失’位为‘1’。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——IC卡中不存在IC卡公钥指数。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.77 AQFM047-01 数据缺失：IC卡公钥指数（2）

测试目的：——确保如果IC卡中IC卡公钥指数缺失，终端复合动态数据认证过程失败；
——确保如果在AIP中指明支持复合动态数据认证并且卡中IC卡公钥指数缺失，终端在TVR中设置“IC卡数据缺失”位为‘1’。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——IC卡中不存在IC卡公钥指数。

测试流程：选择卡片应用，执行交易。

通过标准：终端应在GENERATE AC命令中不请求CDA。终端应该依据TAC和IAC设置请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.78 AQFM047-04 数据缺失：IC卡公钥指数（3）

测试目的：——确保如果IC卡中IC卡公钥指数缺失，终端复合动态数据认证过程失败；
——确保如果在AIP中指明支持复合动态数据认证并且卡中IC卡公钥指数缺失，终端在TVR中设置“IC卡数据缺失”位为‘1’。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥指数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中或金融确认信息或批上送信息中的TVR字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.79 AQFM047-05 数据缺失：IC卡公钥指数（4）

测试目的：——确保如果IC卡中IC卡公钥指数缺失，终端复合动态数据认证过程失败；
——确保如果在AIP中指明支持复合动态数据认证并且卡中IC卡公钥指数缺失，终端在TVR中设置“IC卡数据缺失”位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥指数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令

中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.80 AQFM047-06 数据缺失：IC卡公钥指数（5）

测试目的：——确保如果IC卡中IC卡公钥指数缺失，终端复合动态数据认证过程失败；
——确保如果在AIP中指明支持复合动态数据认证并且卡中IC卡公钥指数缺失，终端在TVR中设置“IC卡数据缺失”位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，第二个GAC请求TC时；
——终端行为分析前没有探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥指数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.81 AQFM047-07 数据缺失：IC卡公钥指数（6）

测试目的：——确保如果IC卡中IC卡公钥指数缺失，终端复合动态数据认证过程失败；
——确保如果在AIP中指明支持复合动态数据认证并且卡中IC卡公钥指数缺失，终端在TVR中设置“IC卡数据缺失”位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前没有探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥指数；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类

似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.82 AQFM050-00 发卡行公钥证书长度（1）

测试目的：确保如果终端支持动态数据认证，发卡行公钥证书的长度与CA公钥模长度不一致，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）。

子类案例：——案例01：发卡行公钥证书的长度大于CA公钥模长度；
——案例02：发卡行公钥证书的长度小于CA公钥模长度。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.83 AQFM050-01 发卡行公钥证书长度（2）

测试目的：确保如果终端支持复合动态数据认证，发卡行公钥证书的长度与CA公钥模长度不一致，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 = ‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

子类案例：——案例01：发卡行公钥证书的长度大于CA公钥模长度；
——案例02：发卡行公钥证书的长度小于CA公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端应在GENERATE AC命令中不请求CDA。终端应该依据TAC和IAC设置请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.84 AQFM050-03 发卡行公钥证书长度（3）

测试目的：确保如果终端支持复合动态数据认证，发卡行公钥证书的长度与CA公钥模长度不一致，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 = ‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

子类案例：——案例01：发卡行公钥证书的长度大于CA公钥模长度；
——案例02：发卡行公钥证书的长度小于CA公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 ='1'（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 ='1'（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 ='1'（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 ='0'（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TSI字节1，位8 ='1'（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 ='1'（脱机数据认证已进行）。

7.3.85 AQFM050-04 发卡行公钥证书长度（4）

测试目的：确保如果终端支持复合动态数据认证，发卡行公钥证书的长度与CA公钥模长度不一致，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时或当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 = '1'）；
——卡在第一个GENERATE AC命令返回ARQC。

子类案例：——案例01：发卡行公钥证书的长度大于CA公钥模长度；
——案例02：发卡行公钥证书的长度小于CA公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 ='1'（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 ='0'（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.3.86 AQFM050-05 发卡行公钥证书长度（5）

测试目的：确保如果终端支持复合动态数据认证，发卡行公钥证书的长度与CA公钥模长度不一致，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 = '1'）；
——卡在第一个GENERATE AC命令返回ARQC。

子类案例：——案例01：发卡行公钥证书的长度大于CA公钥模长度；
——案例02：发卡行公钥证书的长度小于CA公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交

易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.87 AQFM050-06 发卡行公钥证书长度（6）

测试目的：确保如果终端支持复合动态数据认证，发卡行公钥证书的长度与CA公钥模长度不一致，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 = ‘1’）；
——卡在第一个GENERATE AC命令返回ARQC。

测试条件：终端无法联机。

子类案例：——案例01：发卡行公钥证书的长度大于CA公钥模长度；
——案例02：发卡行公钥证书的长度小于CA公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 = ‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 = ‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 = ‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.88 AQFM050-07 发卡行公钥证书长度（7）

测试目的：确保如果终端支持复合动态数据认证，发卡行公钥证书的长度与CA公钥模长度不一致，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机批准。

子类案例：——案例01：发卡行公钥证书的长度大于CA公钥模长度；
——案例02：发卡行公钥证书的长度小于CA公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 = ‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.89 AQFM050-08 发卡行公钥证书长度（8）

测试目的：确保如果终端支持复合动态数据认证，发卡行公钥证书的长度与CA公钥模长度不一致，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机拒绝。

子类案例：——案例01：发卡行公钥证书的长度大于CA公钥模长度；
——案例02：发卡行公钥证书的长度小于CA公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 = ‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.90 AQFM052-00 恢复数据结尾不是‘BC’（1）

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 = ‘1’）；
——卡中的发卡行公钥证书用结尾不是‘BC’的数据计算得到。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 = ‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 = ‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.91 AQFM052-01 恢复数据结尾不是‘BC’（2）

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =1）；
——卡中发卡行公钥证书被恢复，但其数据结尾不是‘BC’；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端在GENERATE AC命令中应不请求CDA。第一个GENERATE AC命令中的TVR字节1，位3 = ‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 = ‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.92 AQFM052-03 恢复数据结尾不是‘BC’（3）

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =1）；
——卡中发卡行公钥证书被恢复，但其数据结尾不是‘BC’；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.93 AQFM052-04 恢复数据结尾不是‘BC’（4）

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——卡中发卡行公钥证书被恢复，但其数据结尾不是‘BC’；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.94 AQFM052-05 恢复数据结尾不是‘BC’（5）

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——CDA总是请求，在第二个GAC请求TC；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；

——卡中发卡行公钥证书被恢复，但其数据结尾不是‘BC’；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个 GENERATE AC 命令返回 ARQC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.95 AQFM052-06 恢复数据结尾不是‘BC’（6）

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败；

卡片配置：——卡的 AIP 指明支持复合动态数据认证 （AIP 字节 1，位 1 =1）；
——卡中发卡行公钥证书被恢复，但其数据结尾不是‘BC’；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个 GENERATE AC 命令返回 ARQC；

测试条件：——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.96 AQFM052-07 恢复数据结尾不是‘BC’（7）

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证 （AIP 字节 1，位 1 =1）；
——卡中发卡行公钥证书被恢复，但其数据结尾不是‘BC’；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——交易联机批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.97 AQFM052-08 恢复数据结尾不是‘BC’（8）

测试目的：确保如果从发卡行公钥证书中恢复的数据结尾不是‘BC’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP字节1，位1 =1）；
——卡中发卡行公钥证书被恢复，但其数据结尾不是‘BC’；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——交易联机拒绝。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.98 AQFM053-00 恢复数据头不是‘6A’（1）

测试目的：确保如果从发卡行公钥证书中恢复的数据头不是‘6A’，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP字节1，位6 =‘1’）；
——卡中的发卡行公钥证书用开头不是‘6A’的数据计算得到。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.99 AQFM053-01 恢复数据头不是‘6A’（2）

测试目的：确保如果从发卡行公钥证书中恢复的数据头不是‘6A’，终端动态数据认证处理失败。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP字节1，位6 =‘1’）；
——卡中的发卡行公钥证书用开头不是‘6A’的数据计算得到。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该依据TAC和IAC设置请求一个TC或AAC来完成交易。终端在GENERATE AC命令中应不请求CDA。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位

4 = ‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 = ‘1’（脱机数据认证已进行）。

7.3.100 AQFM053-03 恢复数据头不是‘6A’（3）

测试目的：确保如果从发卡行公钥证书中恢复的数据头不是‘6A’，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =1）；
——卡中的发卡行公钥证书用开头不是‘6A’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.101 AQFM053-04 恢复数据头不是‘6A’（4）

测试目的：确保如果从发卡行公钥证书中恢复的数据头不是‘6A’，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——卡中的发卡行公钥证书用开头不是‘6A’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.102 AQFM053-05 恢复数据头不是‘6A’（5）

测试目的：确保如果从发卡行公钥证书中恢复的数据头不是‘6A’，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；

——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——卡中的发卡行公钥证书用开头不是‘6A’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.103 AQFM053-06 恢复数据头不是‘6A’（6）

测试目的：确保如果从发卡行公钥证书中恢复的数据头不是‘6A’，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =1）；
——卡中的发卡行公钥证书用开头不是‘6A’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.104 AQFM054-00 证书格式不等于‘02’（1）

测试目的：确保如果从发卡行公钥证书中恢复的证书格式不等于‘02’，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.105 AQFM054-01 证书格式不等于‘02’（2）

测试目的：确保如果从发卡行公钥证书中恢复的证书格式不等于‘02’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——终端行为分析前有能力探测到 CDA 失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该依据 TAC 和 IAC 设置请求一个 TC 或 AAC 来完成交易。终端在 GENERATE AC 命令中应不请求 CDA。第一个 GENERATE AC 命令中的 TVR 字节 1，位 3 = ‘1’（CDA 失败）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 = ‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 = ‘0’（未使用 DDA）。第一个 GENERATE AC 命令中的 TSI 字节 1，位 8 = ‘1’（脱机数据认证已进行）。

7.3.106 AQFM054-03 证书格式不等于‘02’（3）

测试目的：确保如果从发卡行公钥证书中恢复的证书格式不等于‘02’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证 （AIP 字节 1，位 1 =1）；
——卡中发卡行公钥证书不是使用证书格式为 ‘02’ 的数据计算得到。
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.107 AQFM054-04 证书格式不等于‘02’（4）

测试目的：确保如果从发卡行公钥证书中恢复的证书格式不等于‘02’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.108 AQFM054-05 证书格式不等于‘02’（5）

测试目的：确保如果从发卡行公钥证书中恢复的证书格式不等于‘02’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.109 AQFM054-05 证书格式不等于‘02’（6）

测试目的：确保如果从发卡行公钥证书中恢复的证书格式不等于‘02’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC。

测试条件：终端无法联机。
测试流程：选择卡片应用，执行交易。
通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 ='1'（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 ='1'（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 ='0'（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 ='1'（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 ='1'（脱机数据认证已进行）。

7.3.110 AQFM055-00 计算的哈希结果与恢复的哈希结果不同（1）

测试目的：确保如果计算的哈希结果与从发卡行公钥证书中恢复的哈希结果不相等，动态数据认证处理失败。
终端配置：支持DDA。
卡片配置：——卡的AIP指明支持脱机动态数据认证（AIP 字节1，位6 ='1'）；
——卡中的发卡行公钥证书用错误的哈希值计算得到。
子类案例：——案例01：哈希结果的第一个字节出错；
——案例02：哈希结果的最后一个字节出错。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 ='1'（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 ='0'（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 ='0'（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.3.111 AQFM055-01 计算的哈希结果与恢复的哈希结果不同（2）

测试目的：确保如果计算的哈希结果与从发卡行公钥证书中恢复的哈希结果不相等，动态数据认证处理失败。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证 （AIP 字节 1，位 1 =1）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中的发卡行公钥证书用错误的哈希值计算得到。
子类案例：——案例01：哈希结果的第一个字节出错；
——案例02：哈希结果的最后一个字节出错。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。终端在 GENERATE AC 命令中应不请求 CDA。第一个 GENERATE AC 命令中的 TVR 字节 1，位 3 = '1'（CDA 失败）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 = '0'（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 = '0'（未使用 DDA）。第一个 GENERATE AC 命令中的 TSI 字节 1，位 8 = '1'（脱机数据认证已进行）。

7.3.112 AQFM055-03 计算的哈希结果与恢复的哈希结果不同（3）

测试目的：确保如果计算的哈希结果与从发卡行公钥证书中恢复的哈希结果不相等，动态数据认证处理失败。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =1）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中的发卡行公钥证书用错误的哈希值计算得到。

子类案例：——案例01：哈希结果的第一个字节出错；
——案例02：哈希结果的最后一个字节出错。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.113 AQFM055-04 计算的哈希结果与恢复的哈希结果不同（4）

测试目的：确保如果计算的哈希结果与从发卡行公钥证书中恢复的哈希结果不相等，动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——卡中的发卡行公钥证书用错误的哈希值计算得到。

子类案例：——案例01：哈希结果的第一个字节出错；
——案例02：哈希结果的最后一个字节出错。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.114 AQFM055-05 计算的哈希结果与恢复的哈希结果不同（5）

测试目的：确保如果计算的哈希结果与从发卡行公钥证书中恢复的哈希结果不相等，动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——CDA总是请求，在第二个GAC请求TC；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE

AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——卡中的发卡行公钥证书用错误的哈希值计算得到；
——发卡行响应批准。

子类案例：——案例01：哈希结果的第一个字节出错。
——案例02：哈希结果的最后一个字节出错。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.115 AQFM055-06 计算的哈希结果与恢复的哈希结果不同（6）

测试目的：确保如果计算的哈希结果与从发卡行公钥证书中恢复的哈希结果不相等，动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——终端无法联机；
——卡中的发卡行公钥证书用错误的哈希值计算得到。

子类案例：——案例01：哈希结果的第一个字节出错；
——案例02：哈希结果的最后一个字节出错。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.116 AQFM055-07 计算的哈希结果与恢复的哈希结果不同（7）

测试目的：确保如果计算的哈希结果与从发卡行公钥证书中恢复的哈希结果不相等，动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；

——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——交易联机批准；
——卡中的发卡行公钥证书用错误的哈希值计算得到。

子类案例：——案例01：哈希结果的第一个字节出错；
——案例02：哈希结果的最后一个字节出错。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.117 AQFM055-08 计算的哈希结果与恢复的哈希结果不同（8）

测试目的：确保如果计算的哈希结果与从发卡行公钥证书中恢复的哈希结果不相等，动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——交易联机拒绝；
——卡中的发卡行公钥证书用错误的哈希值计算得到。

子类案例：——案例01：哈希结果的第一个字节出错；
——案例02：哈希结果的最后一个字节出错。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.118 AQFM056-00 发卡行标识与 PAN 最左边的 3 到 8 位不匹配（1）

测试目的：确保如果恢复的发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）。

子类案例：——案例01：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.119 AQFM056-01 发卡行标识与 PAN 最左边的 3 到 8 位不匹配（2）

测试目的：确保如果恢复的发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：——支持CDA；

——终端行为分析前探测到CDA失败。

卡片配置：卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

子类案例：——案例01：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；

——案例02：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；

——案例03：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端在GENERATE AC命令时不应请求CDA。终端应该依据TAC和IAC设置请求TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.120 AQFM056-03 发卡行标识与PAN最左边的3到8位不匹配（3）

测试目的：确保如果恢复的发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：——支持CDA；

——仅脱机终端或可联机的脱机终端；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

子类案例：——案例01：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；

——案例02：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；

——案例03：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.121 AQFM056-04 发卡行标识与PAN最左边的3到8位不匹配（4）

测试目的：确保如果恢复的发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：——支持CDA；

——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC。

子类案例：——案例01：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.122 AQFM056-05 发卡行标识与PAN最左边的3到8位不匹配（5）

测试目的：确保如果恢复的发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——发卡行响应批准。

子类案例：——案例01：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.123 AQFM056-06 发卡行标识与PAN最左边的3到8位不匹配（6）

测试目的：确保如果恢复的发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认

证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——终端无法联机。

子类案例：——案例01：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书被恢复，带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.124 AQFM057-00 证书失效日期早于今天日期（1）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.125 AQFM057-01 证书失效日期早于今天日期（2）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个

GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.126 AQFM057-03 证书失效日期早于今天日期（3）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.127 AQFM057-04 证书失效日期早于今天日期（4）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.128 AQFM057-05 证书失效日期早于今天日期（5）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——CDA总是请求，在第二个GAC请求TC；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.129 AQFM057-06 证书失效日期早于今天日期（6）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.130 AQFM057-07 证书失效日期早于今天日期（7）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。
终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机批准；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC

来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.131 AQFM057-08 证书失效日期早于今天日期（8）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机拒绝；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.132 AQFM058-00 RID、CA 公钥索引和证书序列号无效，DDA（1）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个 RID 对应三十个公钥入口，如果 RID、CA 公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端动态数据认证失败。

终端配置：——支持 DDA；
——支持发卡行公钥证书的回收；
——终端支持三个 RID；
——终端内每个 RID 装载 30 个 CRL 入口，其中 29 个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）。

子类案例：——案例 01：终端装载 30 条 CRL 入口，指定 RID 1 在回收列表中；
——案例02：终端装载30条CRL入口，指定RID 2在回收列表中；
——案例03：终端装载30条CRL入口，指定RID 3在回收列表中；
——卡中的发卡行公钥证书恢复后，RID、CA 公钥索引和证书序列号表明证书在终端证书回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 =‘1’（脱机数据认证已进行）。

7.3.133 AQFM058-01 RID、CA 公钥索引和证书序列号无效，CDA（2）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个 RID 对应三十条公钥入口，如果 RID、CA 公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——支持发卡行公钥证书的回收；

——终端行为分析前有能力探测到CDA失败；
——终端支持三个RID；
——终端内每个RID装载30个CRL入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

子类案例：——案例01：终端装载30条CRL入口，指定RID 1在回收列表中；
——案例02：终端装载30条CRL入口，指定RID 2在回收列表中；
——案例03：终端装载30条CRL入口，指定RID 3在回收列表中；
——卡中的发卡行公钥证书恢复后，RID、CA公钥索引和证书序列号表明证书在终端证书回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.134 AQFM058-03 RID、CA公钥索引和证书序列号无效（3）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个RID对应三十个公钥入口，如果RID、CA公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败；
——支持发卡行公钥证书的回收；
——终端支持三个RID；
——终端内每个RID装载30个CRL入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

子类案例：——案例01：终端装载30条CRL入口，指定RID 1在回收列表中；
——案例02：终端装载30条CRL入口，指定RID 2在回收列表中；
——案例03：终端装载30条CRL入口，指定RID 3在回收列表中；
——卡中的发卡行公钥证书恢复后，RID、CA公钥索引和证书序列号表明证书在终端证书回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显

示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.135 AQFM058-04 证书回收列表的更新，移除（1）

测试目的：确保终端能够通过删除入口更新证书回收列表。

终端配置：——支持DDA；
——支持发卡行公钥证书的回收；
——终端已装载案例AQFM13200中描述的30个证书回收列表入口。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位7为‘0’；字节1，位5为‘0’；字节1，位1为‘0’）；
——执行交易前，证书回收列表更新已完成；
——一个有效的证书回收列表从终端移除，而卡片中的发卡行公钥证书是根据与该有效入口香对应的RID、CA公钥索引以及证书序列号进行计算的。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。

7.3.136 AQFM058-05 证书回收列表的更新，增加（1）

测试目的：确保终端能够通过增加入口更新证书回收列表。

终端配置：——支持DDA；
——支持发卡行公钥证书的回收；
——终端已装载29个证书回收列表入口，案例AQFM13500已先于此案例执行。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位7为‘0’；字节1，位5为‘0’；字节1，位1为‘0’）；
——执行交易前，证书回收列表更新已完成；
——卡中发卡行公钥证书是由与该有效入口相对应的RID、CA公钥索引及证书序列号计算得到的，该证书已装载在终端证书回收列表中。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是动态数据认证）；
c）请注意：案例AQFM13500应先于此案例执行。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.137 AQFM058-06 证书回收列表的更新，移除（2）

测试目的：确保终端能够通过删除入口更新证书回收列表。

终端配置：——支持CDA；
——支持发卡行公钥证书的回收；
——终端已装载案例AQFM13200中描述的30个证书回收列表入口。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位7为‘0’；字节1，位5为‘0’；字节1，位6为‘0’）；
——执行交易前，证书回收列表更新已完成；
——卡中发卡行公钥证书是由与该有效入口相对应的RID、CA公钥索引及证书序列号计算得到的，该证书已从终端证书回收列表中移除。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；

b）选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。金融确认信息或批上送信息中TVR的字节1，位4为‘0’（未使用DDA）。金融确认信息或批上送信息中TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’（未使用SDA）。金融确认信息或批上送信息中TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.138 AQFM058-07 证书回收列表的更新，增加（2）

测试目的：确保终端能够通过增加入口更新证书回收列表。

终端配置：——支持CDA；
——支持发卡行公钥证书的回收；
——终端已装载29个证书回收列表入口，案例AQFM13700已先于此案例执行。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位7为‘0’；字节1，位5为‘0’；字节1，位6为‘0’）；
——执行交易前，证书回收列表更新已完成；
——卡中发卡行公钥证书包含RID、CA公钥索引及证书序列号，该证书已装载在终端证书回收列表中。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是复合动态数据认证）；
c）请注意：案例AQFM13700应先于此案例执行。

通过标准：终端应该通过请求一个TC或AAC来完成交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。

7.3.139 AQFM058-10 RID、CA 公钥索引和证书序列号无效（4）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个 RID 对应三十个公钥入口，如果 RID、CA 公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——终端行为分析前不能探测到 CDA 失败；
——支持发卡行公钥证书的回收；
——CDA 总是请求，第一个 GAC 请求 ARQC；
——终端支持三个 RID；
——终端内每个 RID 装载 30 个证书回收列表入口，其中 29 个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC时请求TC。

子类案例：——案例01：终端装载30条证书回收列表入口，指定RID 1在回收列表中；
——案例02：终端装载30条证书回收列表入口，指定RID 2在回收列表中；
——案例03：终端装载30条证书回收列表入口，指定RID 3在回收列表中；
——卡中的发卡行公钥证书恢复后，RID、CA 公钥索引和证书序列号表明证书在终端证书回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC

命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.140 AQFM058-11 RID、CA 公钥索引和证书序列号无效（5）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个 RID 对应三十条公钥入口，如果 RID、CA 公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——终端行为分析前不能探测到 CDA 失败；
——支持发卡行公钥证书的回收；
——CDA 从不请求，第一个 GAC 请求 ARQC；
——CDA 总是请求，第二个 GAC 请求 TC；
——终端支持三个 RID；
——终端内每个 RID 装载 30 个证书回收列表入口，其中 29 个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC时请求TC；
——发卡行响应批准。

子类案例：——案例01：终端装载30条证书回收列表入口，指定RID 1在回收列表中；
——案例02：终端装载30条证书回收列表入口，指定RID 2在回收列表中；
——案例03：终端装载30条证书回收列表入口，指定RID 3在回收列表中；
——卡中的发卡行公钥证书恢复后，RID、CA 公钥索引和证书序列号表明证书在终端证书回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.141 AQFM058-12 RID、CA 公钥索引和证书序列号无效（6）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个 RID 对应三十条公钥入口，如果 RID、CA 公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——终端行为分析前不能探测到 CDA 失败；
——支持发卡行公钥证书的回收；
——CDA 从不请求，第一个 GAC 请求 ARQC；
——当不能联机时，正常处理缺省行为码；
——终端支持三个 RID；

——终端内每个 RID 装载 30 个证书回收列表入口，其中 29 个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC时请求TC；
——终端无法联机。

子类案例：——案例01：终端装载30条证书回收列表入口，指定RID 1在回收列表中；
——案例02：终端装载30条证书回收列表入口，指定RID 2在回收列表中；
——案例03：终端装载30条证书回收列表入口，指定RID 3在回收列表中；
——卡中的发卡行公钥证书恢复后，RID、CA 公钥索引和证书序列号表明证书在终端证书回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.142 AQFM059-00 发卡行公钥算法无法识别（1）

测试目的：如果发卡行公钥算法标识不是 01，终端动态数据认证执行失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中计算公钥证书的公钥算法标识不为‘01’。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 =‘1’（脱机数据认证已进行）。

7.3.143 AQFM059-01 发卡行公钥算法无法识别（2）

测试目的：如果发卡行公钥算法标识不是 01，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡中计算公钥证书的公钥算法标识不为‘01’。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.144 AQFM059-03 发卡行公钥算法无法识别（3）

测试目的：如果发卡行公钥算法标识不是 01，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中计算公钥证书的公钥算法标识不为‘01’。
测试流程：选择卡片应用，执行交易。
通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.145 AQFM059-04 发卡行公钥算法无法识别（4）

测试目的：如果发卡行公钥算法标识不是01，终端复合动态数据认证执行失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中计算公钥证书的公钥算法标识不为‘01’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.146 AQFM059-05 发卡行公钥算法无法识别（5）

测试目的：如果发卡行公钥算法标识不是01，终端复合动态数据认证执行失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中计算公钥证书的公钥算法标识不为‘01’；

——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.147 AQFM059-06 发卡行公钥算法无法识别（6）

测试目的：如果发卡行公钥算法标识不是01，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中计算公钥证书的公钥算法标识不为‘01’；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.148 AQFM060-00 长度为3到8位的发卡行标识（1）

测试目的：如果恢复出来的发卡行标识长度为3到8位数字，确保终端正确执行静态数据认证。

终端配置：支持SDA。

卡片配置：卡片的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

子类案例：——案例01：使用长度为3位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；
——案例02：使用长度为6位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；
——案例03：使用长度为8位数字的发卡行标识计算发卡行公钥证书。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中TVR的字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’

（SDA成功）。第一个GENERATE AC命令中TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.149 AQFM060-01 长度为 3 到 8 位的发卡行标识（2）

测试目的：如果恢复出来的发卡行标识长度为 3 到 8 位数字，确保终端正确执行动态数据认证。

终端配置：支持 DDA。

卡片配置：卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）。

子类案例：——案例 01：使用长度为 3 位数字的发卡行标识，右补‘F’至 8 位计算发卡行公钥证书；

——案例 02：使用长度为 6 位数字的发卡行标识，右补‘F’至 8 位计算发卡行公钥证书；

——案例 03：使用长度为 8 位数字的发卡行标识计算发卡行公钥证书。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 =‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 =‘1’（脱机数据认证已进行）。

7.3.150 AQFM060-02 长度为 3 到 8 位的发卡行标识（3）

测试目的：如果恢复出来的发卡行标识长度为 3 到 8 位数字，确保终端正确执行复合动态数据认证。

终端配置：——支持 CDA；

——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡的 AIP 指明复合动态数据认证（AIP 字节 1，位 1 =‘1’）；

——设置IAC和TAC使终端在第一个GENERATE AC时请求TC，且卡返回TC。

子类案例：——案例01：使用长度为3位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；

——案例 02：使用长度为 6 位数字的发卡行标识，右补‘F’至 8 位计算发卡行公钥证书；

——案例 03：使用长度为 8 位数字的发卡行标识计算发卡行公钥证书。

测试流程：选择卡片应用，执行交易完成。

通过标准：终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令或金融确认信息或批上送信息中的TVR字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。金融确认信息或批上送信息中中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.151 AQFM060-04 长度为 3 到 8 位的发卡行标识（4）

测试目的：如果恢复出来的发卡行标识长度为 3 到 8 位数字，确保终端正确执行复合动态数据认证。

终端配置：——支持 CDA；

——仅联机终端；

——CDA 总是请求，第一个 GAC 请求 ARQC 时或 CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡的 AIP 指明复合动态数据认证（AIP 字节 1，位 1 =‘1’）；

——卡在第一个GENERATE AC命令返回ARQC；

——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 时请求 ARQC，第二个 GENERATE AC 请求 TC。

子类案例：——案例 01：使用长度为 3 位数字的发卡行标识，右补‘F’至 8 位计算发卡行公钥证书；
——案例 02：使用长度为 6 位数字的发卡行标识，右补‘F’至 8 位计算发卡行公钥证书；
——案例 03：使用长度为 8 位数字的发卡行标识计算发卡行公钥证书。
测试流程：选择卡片应用，执行交易完成。
通过标准：终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令或金融确认信息或批上送信息中的TVR字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。金融确认信息或批上送信息中中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.152 AQFM060-05 长度为 3 到 8 位的发卡行标识（5）

测试目的：如果恢复出来的发卡行标识长度为 3 到 8 位数字，确保终端正确执行复合动态数据认证。
终端配置：——支持 CDA；
——仅联机终端；
——正常处理缺省行为码。
卡片配置：——卡的 AIP 指明复合动态数据认证（AIP 字节 1，位 1 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 时请求 ARQC，第二个 GENERATE AC 请求 TC；
——终端无法联机。
子类案例：——案例01：使用长度为3位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；
——案例 02：使用长度为 6 位数字的发卡行标识，右补‘F’至 8 位计算发卡行公钥证书；
——案例 03：使用长度为 8 位数字的发卡行标识计算发卡行公钥证书。
测试流程：选择卡片应用，执行交易完成。
通过标准：终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令或金融确认信息或批上送信息中的TVR字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。金融确认信息或批上送信息中中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.153 AQFM061-00 IC 卡公钥证书的长度（1）

测试目的：如果终端支持动态数据认证且 IC 卡公钥证书与发卡行公钥模长度不一致，终端动态数据认证失败。
终端配置：支持 DDA。
卡片配置：卡的 AIP 指明支持动态数据认证（AIP 字节 1，位 6 为‘1’）。
子类案例：——案例 01：卡中的 IC 卡公钥证书长度大于发卡行公钥模长度；
——案例 02：卡中的 IC 卡公钥证书长度小于发卡行公钥模长度。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 =‘1’（脱机数据认证已进行）。

7.3.154 AQFM061-01 IC 卡公钥证书的长度（2）

测试目的：如果终端支持复合动态数据认证且 IC 卡公钥证书与发卡行公钥模长度不一致，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 字节 1，位 1 为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

子类案例：——案例01：卡中的IC卡公钥证书长度大于发卡行公钥模长度；
——案例 02：卡中的 IC 卡公钥证书长度小于发卡行公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.155 AQFM061-04 IC 卡公钥证书的长度（3）

测试目的：如果终端支持复合动态数据认证且 IC 卡公钥证书与发卡行公钥模长度不一致，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 字节 1，位 1 为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

子类案例：——案例01：卡中的IC卡公钥证书长度大于发卡行公钥模长度；
——案例 02：卡中的 IC 卡公钥证书长度小于发卡行公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用)中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.156 AQFM061-05 IC 卡公钥证书的长度（4）

测试目的：如果终端支持复合动态数据认证且 IC 卡公钥证书与发卡行公钥模长度不一致，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个

GENERATE AC请求TC。

子类案例：——案例01：卡中的IC卡公钥证书长度大于发卡行公钥模长度；
——案例 02：卡中的 IC 卡公钥证书长度小于发卡行公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.157 AQFM061-06 IC卡公钥证书的长度（5）

测试目的：如果终端支持复合动态数据认证且 IC 卡公钥证书与发卡行公钥模长度不一致，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 时请求 ARQC，第二个 GENERATE AC 请求 TC；
——发卡行响应批准。

子类案例：——案例01：卡中的IC卡公钥证书长度大于发卡行公钥模长度；
——案例 02：卡中的 IC 卡公钥证书长度小于发卡行公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.158 AQFM061-07 IC卡公钥证书的长度（6）

测试目的：如果终端支持复合动态数据认证且 IC 卡公钥证书与发卡行公钥模长度不一致，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC 时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个 GENERATE AC请求TC；
——终端无法联机。

子类案例：——案例01：卡中的IC卡公钥证书长度大于发卡行公钥模长度；
——案例 02：卡中的 IC 卡公钥证书长度小于发卡行公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.159 AQFM061-08 IC卡公钥证书的长度（7）

测试目的：如果终端支持复合动态数据认证且IC卡公钥证书与发卡行公钥模长度不一致，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析之前探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机批准。

子类案例：——案例01：卡中的IC卡公钥证书长度大于发卡行公钥模长度；
——案例02：卡中的IC卡公钥证书长度小于发卡行公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.160 AQFM061-09 IC卡公钥证书的长度（8）

测试目的：如果终端支持复合动态数据认证且IC卡公钥证书与发卡行公钥模长度不一致，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析之前探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机拒绝。

子类案例：——案例01：卡中的IC卡公钥证书长度大于发卡行公钥模长度；
——案例02：卡中的IC卡公钥证书长度小于发卡行公钥模长度。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.161 AQFM063-00 恢复数据尾不是‘BC’（1）

测试目的：如果从IC卡公钥证书中恢复数据的结尾不是‘BC’，终端动态数据认证失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；

——卡中 IC 卡公钥证书被恢复，但其数据结尾不是‘BC’。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 =‘1’（脱机数据认证已进行） 。

7.3.162 AQFM063-01 恢复数据尾不是‘BC’（2）

测试目的：如果从 IC 卡公钥证书中恢复数据的结尾不是‘BC’，终端复合动态数据认证失败。

终端配置：——支持 CDA；

——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——卡中 IC 卡公钥证书被恢复，但其数据结尾不是‘BC’。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.163 AQFM063-04 恢复数据尾不是‘BC’（3）

测试目的：如果从 IC 卡公钥证书中恢复数据的结尾不是‘BC’，终端复合动态数据认证失败。

终端配置：——支持 CDA；

——仅脱机终端或有联机能力的脱机终端；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；

——卡中 IC 卡公钥证书被恢复，但其数据结尾不是‘BC’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.164 AQFM063-05 恢复数据尾不是‘BC’（4）

测试目的：如果从 IC 卡公钥证书中恢复数据的结尾不是‘BC’，终端复合动态数据认证失败。

终端配置：——支持 CDA；

——仅联机终端；

——CDA总是请求，第一个GAC请求ARQC时；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中IC卡公钥证书被恢复，但其数据结尾不是‘BC’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.165 AQFM063-06 恢复数据尾不是‘BC’（5）

测试目的：如果从IC卡公钥证书中恢复数据的结尾不是‘BC’，终端复合动态数据认证失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准；
——卡中IC卡公钥证书被恢复，但其数据结尾不是‘BC’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应在第二个GAC命令时请求AAC来拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’(CDA失败)；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.166 AQFM063-07 恢复数据尾不是‘BC’（6）

测试目的：如果从IC卡公钥证书中恢复数据的结尾不是‘BC’，终端复合动态数据认证失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机；
——卡中IC卡公钥证书被恢复，但其数据结尾不是‘BC’。测试流程：选择

卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.167 AQFM064-00 恢复数据头不是‘6A’（1）

测试目的：如果从 IC 卡公钥证书中恢复数据头不是‘6A’，终端动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；

——卡中 IC 卡公钥证书被恢复，但其数据头不是‘6A’。

测试流程：选择卡片应用，执行交易（特别是在动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 =‘1’（脱机数据认证已进行）。

7.3.168 AQFM064-01 恢复数据头不是‘6A’（2）

测试目的：如果从 IC 卡公钥证书中恢复数据头不是‘6A’，终端复合动态数据认证失败。

终端配置：——支持 CDA；

——终端行为分析前有能力探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——卡中 IC 卡公钥证书被恢复，但其数据头不是‘6A’。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.169 AQFM064-04 恢复数据头不是‘6A’（3）

测试目的：如果从 IC 卡公钥证书中恢复数据头不是‘6A’，终端复合动态数据认证失败。

终端配置：——支持 CDA；

——仅脱机终端或有联机能力的脱机终端；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；

——卡中IC卡公钥证书被恢复，但其数据头不是‘6A’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，

位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.170 AQFM064-05 恢复数据头不是‘6A’（4）

测试目的：如果从 IC 卡公钥证书中恢复数据头不是‘6A’，终端复合动态数据认证失败。
终端配置：——支持 CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中 IC 卡公钥证书被恢复，但其数据头不是‘6A’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.171 AQFM064-06 恢复数据头不是‘6A’（5）

测试目的：如果从 IC 卡公钥证书中恢复数据头不是‘6A’，终端复合动态数据认证失败。
终端配置：——支持 CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——CDA总是请求，在第二个GAC请求TC；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准；
——卡中 IC 卡公钥证书被恢复，但其数据头不是‘6A’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.172 AQFM064-07 恢复数据头不是‘6A’（6）

测试目的：如果从 IC 卡公钥证书中恢复数据头不是‘6A’，终端复合动态数据认证失败。
终端配置：——支持 CDA；
——仅联机终端；

——CDA从不请求，第一个GAC请求ARQC；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机；
——卡中IC卡公钥证书被恢复，但其数据头不是‘6A’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.173 AQFM065-00 证书格式不等于‘04’（1）

测试目的：如果从 IC 卡公钥证书中恢复得到的证书格式不等于‘04’，终端动态数据认证失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡中IC卡公钥证书被恢复，但其证书格式不是‘04’。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.174 AQFM065-01 证书格式不等于‘04’（2）

测试目的：如果从 IC 卡公钥证书中恢复得到的证书格式不等于‘04’，终端复合动态数据认证失败。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中IC卡公钥证书被恢复，但其证书格式不是‘04’。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.175 AQFM065-04 证书格式不等于‘04’（3）

测试目的：如果从 IC 卡公钥证书中恢复得到的证书格式不等于‘04’，终端复合动态数据认证失败。

终端配置：——支持CDA；

——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中 IC 卡公钥证书被恢复，但其证书格式不是‘04’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.176 AQFM065-05 证书格式不等于‘04’（4）

测试目的：如果从 IC 卡公钥证书中恢复得到的证书格式不等于‘04’，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中 IC 卡公钥证书被恢复，但其证书格式不是‘04’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.177 AQFM065-06 证书格式不等于‘04’（5）

测试目的：如果从 IC 卡公钥证书中恢复得到的证书格式不等于‘04’，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC；
——CDA 总是请求，在第二个 GAC 请求 TC；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准；
——卡中IC卡公钥证书被恢复，但其证书格式不是‘04’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。 第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.178 AQFM065-07 证书格式不等于‘04’（6）

测试目的：如果从 IC 卡公钥证书中恢复得到的证书格式不等于‘04’，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC；
——正常处理缺省行为码；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机；
——卡中 IC 卡公钥证书被恢复，但其证书格式不是‘04’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.3.179 AQFM066-00 计算的哈希结果与恢复的哈希结果的不同（1）

测试目的：如果计算得到的哈希结果与从 IC 卡公钥证书中恢复得到的哈希结果不相等，终端动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持脱机动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——计算卡中的 IC 卡公钥证书时使用错误的哈希值。

测试流程：选择卡片应用，执行交易（特别是在动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.180 AQFM066-01 计算的哈希结果与恢复的哈希结果的不同（2）

测试目的：如果计算得到的哈希结果与从 IC 卡公钥证书中恢复得到的哈希结果不相等，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡的 AIP 指明支持脱机复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——计算卡中的 IC 卡公钥证书时使用错误的哈希值。
测试流程：选择卡片应用，执行交易。
通过标准：终端GENERATE AC时不请求CDA。终端应该通过设置TAC和IAC来请求一个TC完成交易。第一个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.3.181 AQFM066-04 计算的哈希结果与恢复的哈希结果的不同（3）

测试目的：如果计算得到的哈希结果与从 IC 卡公钥证书中恢复得到的哈希结果不相等，终端复合动态数据认证失败。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的 AIP 指明支持脱机复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——计算卡中的 IC 卡公钥证书时使用错误的哈希值。
测试流程：选择卡片应用，执行交易。
通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TVR字节1，位3 为‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）；或金融确认信息或批上送信息(当终端有存储拒绝或终止交易能力时此通过标准适用)中TSI字节1，位8 为‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 为‘1’（脱机数据认证已拒绝）。

7.3.182 AQFM066-05 计算的哈希结果与恢复的哈希结果的不同（4）

测试目的：如果计算得到的哈希结果与从 IC 卡公钥证书中恢复得到的哈希结果不相等，终端复合动态数据认证失败。
终端配置：——支持 CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的 AIP 指明支持脱机复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——计算卡中的 IC 卡公钥证书时使用错误的哈希值。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC

命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.3.183 AQFM066-06 计算的哈希结果与恢复的哈希结果的不同（5）

测试目的：如果计算得到的哈希结果与从 IC 卡公钥证书中恢复得到的哈希结果不相等，**终端复合动态数据认证失败**。

终端配置：——支持 CDA；
——仅联机终端；
——CDA总是不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持脱机复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准交易；
——计算卡中的 IC 卡公钥证书时使用错误的哈希值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TVR字节1，位3 为‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TSI字节1，位8 为‘1’（脱机数据认证已完成）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 为‘1’（脱机数据认证已完成）。

7.3.184 AQFM066-07 计算的哈希结果与恢复的哈希结果的不同（6）

测试目的：如果计算得到的哈希结果与从 IC 卡公钥证书中恢复得到的哈希结果不相等，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA总是不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的 AIP 指明支持脱机复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机；
——计算卡中的 IC 卡公钥证书时使用错误的哈希值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TVR字节1，位3 为‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TSI字节1，位

8 为‘1’（脱机数据认证已完成）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 为‘1’（脱机数据认证已完成）。

7.3.185 AQFM066-08 计算的哈希结果与恢复的哈希结果的不同（7）

测试目的：如果计算得到的哈希结果与从 IC 卡公钥证书中恢复得到的哈希结果不相等，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的 AIP 指明支持脱机复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机批准；
——计算卡中的 IC 卡公钥证书时使用错误的哈希值。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.3.186 AQFM066-09 计算的哈希结果与恢复的哈希结果的不同（8）

测试目的：如果计算得到的哈希结果与从 IC 卡公钥证书中恢复得到的哈希结果不相等，终端复合动态数据认证失败。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析有能力探测到CDA失败。

卡片配置：——卡的 AIP 指明支持脱机复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机拒绝；
——计算卡中的 IC 卡公钥证书时使用错误的哈希值。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.3.187 AQFM067-00 恢复的 PAN 不等于读取的 PAN（1）

测试目的：如果恢复的 PAN 不等于读取的 PAN，终端脱机数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡中的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——计算 IC 卡公钥证书中的 PAN 不等于卡中的 PAN。

测试流程：选择卡片应用，执行交易（特别是 DDA 中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.188 AQFM067-01 恢复的 PAN 不等于读取的 PAN（2）

测试目的：如果恢复的 PAN 不等于读取的 PAN，终端复合脱机数据认证失败。
终端配置：——支持 CDA；
——终端行为分析前有能力探测到 CDA 失败。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——计算 IC 卡公钥证书中的 PAN 不等于卡中的 PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端在 GAC 时不请求 CDA。终端根据 TAC 和 IAC 的设置，通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1,位 4 为‘0’(未使用 DDA)。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.189 AQFM067-04 恢复的 PAN 不等于读取的 PAN（3）

测试目的：如果恢复的 PAN 不等于读取的 PAN，终端复合脱机数据认证失败。
终端配置：——支持 CDA；
——仅脱机或有联机能力的脱机终端；
——终端行为分析前不能探测到 CDA 失败。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——通过设置 IAC 和 TAC,终端在第一个 GAC 时请求 TC；
——计算 IC 卡公钥证书中的发卡行 ID 不等于卡中的 PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应拒绝交易。第二个 GENERATE AC 中 TVR 的字节 1，位 3 为‘1’（CDA 失败）或是包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示 TVR。终端根据 TAC 和 IAC 的设置，通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第二个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）或者或是包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示 TSI。

7.3.190 AQFM067-05 恢复的 PAN 不等于读取的 PAN（4）

测试目的：如果恢复的 PAN 不等于读取的 PAN，终端复合脱机数据认证失败。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC；
——终端行为分析前不能探测到 CDA 失败。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——第一个 GAC 时卡返回 ARQC；
——通过设置 IAC 和 TAC,终端在第一个 GAC 时请求 ARQC，在第二个 GAC 时请求 TC；
——计算发卡行公钥证书中的 PAN 不等于卡中的 PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端通过第二个 GAC 请求 AAC 拒绝交易。第二个 GENERATE AC 中 TVR 的字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第二个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.191 AQFM067-06 恢复的 PAN 不等于读取的 PAN（5）

测试目的：如果恢复的PAN不等于读取的PAN，终端复合脱机数据认证失败。。
终端配置：——支持CDA；
——仅联机；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——第一个GAC时卡返回ARQC；
——通过设置IAC和TAC,终端在第一个GAC时请求ARQC,在第二个GAC时请求TC；
——发卡行公钥证书中的PAN不等于卡中的PAN；
——发卡行批准交易。
测试流程：选择卡片应用，执行交易。
通过标准：终端拒绝交易。TVR的字节1，位3为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC中TVR的字节1，位7为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4为‘0’（未使用DDA）。TSI的字节1，位8为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.3.192 AQFM067-07 恢复的PAN不等于读取的PAN（6）

测试目的：如果恢复的PAN不等于读取的PAN，终端复合脱机数据认证失败。。
终端配置：——支持CDA；
——仅联机；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败；
——终端不能联机。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——第一个GAC时卡返回ARQC；
——通过设置IAC和TAC,终端在第一个GAC时请求ARQC,在第二个GAC时请求TC；
——计算发卡行公钥证书中的发卡行 ID 不等于卡中的PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端拒绝交易。TVR的字节1，位3为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC中TVR的字节1，位7为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4为‘0’（未使用DDA）。TSI的字节1，位8为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.3.193 AQFM068-00 证书失效日期早于今天日期（1）

测试目的：如果证书失效日期早于今天日期，则终端脱机数据认证失败。
终端配置：支持DDA。
卡片配置：——卡中发卡行公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持DDA（AIP的字节1，位6为‘1’）。
测试流程：选择卡片应用，执行交易（特别是DDA）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR

字节1，位4 为‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.3.194 AQFM068-01 证书失效日期早于今天日期（2）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。
终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端在GAC时不会请求CDA。终端根据TAC和IAC设置，应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.3.195 AQFM068-04 证书失效日期早于今天日期（3）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——通过设置IAC和TAC，终端在第一个GAC时请求TC。
测试流程：选择卡片应用，执行交易。
通过标准：终端拒绝交易并且不执行2nd GAC当卡返回TC时，或者拒绝交易通过执行2nd GAC请求AAC当卡在1st GAC时返回ARQC。TVR字节1，位3 为‘1’（CDA失败）包含在2nd GAC或者金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8为‘1’（脱机数据认证已完成）包含在2nd GAC或者金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.3.196 AQFM068-05 证书失效日期早于今天日期（4）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败；
卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC；
——卡在1st GAC时返回ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端通过执行第二个 GAC时请求AAC拒绝交易。第二个GENERATE AC命令中的

TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已进行）。

7.3.197 AQFM068-06 证书失效日期早于今天日期（5）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC；
——卡在第一个 GAC时返回ARQC；
——发卡行批准交易。

测试流程：选择卡片应用，执行交易。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.3.198 AQFM068-07 证书失效日期早于今天日期（6）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端不能联机；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC；
——卡在第一个 GAC时返回ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文中。

7.3.199 AQFM069-00 IC卡公钥算法无法识别 （1）

测试目的：如果 IC 卡公钥算法标识不是 01，终端动态数据认证执行失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中计算 IC 卡公钥证书的 IC 卡公钥算法标识不为‘01’。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.200 AQFM069-01 IC 卡公钥算法无法识别（2）

测试目的：如果 IC 卡公钥算法标识不是 01，终端复合动态数据认证执行失败。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡中计算 IC 卡公钥证书的 IC 卡公钥算法标识不为‘01’；
——通过设置 IAC 和 TAC，终端在第一个 GAC 时请求 TC。
测试流程：选择卡片应用，执行交易。
通过标准：终端在 GAC 时不应请求 CDA。终端应根据 TAC 和 IAC 设置，通过请求一个 TC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.201 AQFM069-04 IC 卡公钥算法无法识别（3）

测试目的：如果 IC 卡公钥算法标识不是 01，终端复合动态数据认证执行失败。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到 CDA 失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡中计算 IC 卡公钥证书的 IC 卡公钥算法标识不为‘01’；
——通过设置 IAC 和 TAC，终端在第一个 GAC 时请求 TC。
子类案例：——案例 01：第一个 GAC 明文和恢复的 CID 为 TC；
——案例 02：第一个 GAC 明文和恢复的 CID 为 ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：案例 01：终端应该拒绝交易且不执行第二个 GAC。案例 01：终端通过立即发送第二个 GAC 请求 AAC 来完成交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在第二个 GAC 中或金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示 TVR 值。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含第二个 GAC 中或金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示 TSI 值。

7.3.202 AQFM069-05 IC 卡公钥算法无法识别（4）

测试目的：如果 IC 卡公钥算法标识不是 01，终端复合动态数据认证执行失败。
终端配置：——支持 CDA；
——仅联机终端 ；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥算法标识不为‘01’；
——卡在第一个GAC时返回ARQC；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易通过第二个GAC请求AAC。第二个GENERATE AC命令中TVR的字节1，位3为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位7为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4为‘0’（未使用DDA）。第二个GENERATE AC命令中TSI的字节1，位8为‘1’（脱机数据认证已完成）。

7.3.203 AQFM069-06 IC卡公钥算法无法识别（5）

测试目的：如果IC卡公钥算法标识不是01，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥算法标识不为‘01’；
——卡在第一个GAC时返回ARQC；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC；
——发卡行批准交易。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易。TVR字节1，位3为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中TVR的字节1，位7为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4为‘0’（未使用DDA）。TSI字节1，位8为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.3.204 AQFM069-07 IC卡公钥算法无法识别（6）

测试目的：如果IC卡公钥算法标识不是01，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败；
——终端不能联机。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥算法标识不为‘01’；
——卡在第一个GAC时返回ARQC；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易。TVR字节1，位3为‘1’（CDA失败）包含在金融确认报

文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示 TVR 值。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示 TSI 值。

7.3.205 AQFM069-08 IC 卡公钥算法无法识别（7）

测试目的：如果 IC 卡公钥算法标识不是 01，终端复合动态数据认证执行失败。
终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡中计算 IC 卡公钥证书的 IC 卡公钥算法标识不为‘01’；
——通过设置 IAC 和 TAC，终端在第一个 GAC 时请求 ARQC；
——交易联机接受。
测试流程：选择卡片应用，执行交易。
通过标准：终端在 1st GAC 和 2nd GAC 时不应请求 CDA。终端应该完成交易通过请求 TC。第一个 GENERATE AC 命令中 TVR 字节 1，位 3 =‘1’（CDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.206 AQFM069-09 IC 卡公钥算法无法识别（8）

测试目的：如果 IC 卡公钥算法标识不是 01，终端复合动态数据认证执行失败。
终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡中计算 IC 卡公钥证书的 IC 卡公钥算法标识不为‘01’；
——通过设置 IAC 和 TAC，终端在第一个 GAC 时请求 ARQC；
——交易联机拒绝。
测试流程：选择卡片应用，执行交易。
通过标准：终端在 1st GAC 和 2nd GAC 时不应请求 CDA。终端应该通过请求 AAC 完成交易。第一个 GENERATE AC 命令中 TVR 字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.207 AQFM071-00 动态签名的生成

测试目的：——确保终端支持有效的 DDOL；
——如果支持动态数据认证，终端能发送一个包含 DDOL 中指定数据元的 EXTERNAL AUTHENTICATE 命令。
终端配置：支持 DDA。
卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中存在 DDOL；
——卡计算的动态签名是正确的。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节

1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。卡片收到的 EXTERNAL AUTHENTICATE 命令数据域是按照 JR/T 0025.4—2013 5.3 条定义的规则将 DDOL 的数据元连接起来得到的。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.208 AQFM072-00 缺省 DDOL

测试目的：如果支持动态数据认证且卡片中没有 DDOL，终端能使用其缺省 DDOL。

终端配置：——支持 DDA；
——终端含有缺省 DDOL。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中不存在 DDOL；
——卡计算的动态签名是正确的。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。卡片收到的 INTERNAL AUTHENTICATE 命令数据域是 JR/T0025.4—2013 5.3 条定义的规则将缺省 DDOL 的数据元连接起来得到的。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.209 AQFM074-00 不可预知数的来源

测试目的：如果支持动态数据认证且 DDOL 中请求不可预知数，终端发送的 INTERNAL AUTHENTICATE 命令中含有 4 个字节的不可预知数。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——DDOL请求4个字节的不可预知数（‘9F37’）；
——卡计算的动态签名是正确的。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。卡片收到的 INTERNAL AUTHENTICATE 命令的数据域中含有不可预知数。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.210 AQFM075-00 DDOL 中不含不可预知数

测试目的：如果支持动态数据认证且卡片的 DDOL 不请求不可预知数，终端动态数据认证失败。

终端配置：——支持 DDA；
——终端缺省的 DDOL 请求 4 个字节的不可预知数（‘9F37’）。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中的 DDOL 不请求 4 个字节的不可预知数（‘9F37’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.211 AQFM076-00 缺省 DDOL 不含有不可预知数

测试目的：如果支持动态数据认证，卡中不含有 DDOL 且终端中的缺省 DDOL 不请求不可预知数，终端动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中没有 DDOL；
——终端缺省 DDOL 不请求不可预知数（‘9F37’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.212 AQFM078-00 签名的动态应用数据长度不正确

测试目的：如果支持动态数据认证且签名的动态应用数据长度与 IC 卡公钥模长度不一致，终端动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡计算的签名的动态应用数据长度与 IC 卡公钥模长度不一致。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.213 AQFM079-00 恢复功能

测试目的：确保终端能够按照 JR/T0025.7—2013 5.3.5 的要求执行动态数据认证，恢复签名动态应用数据。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡计算的签名的动态应用数据是正确的；
——发卡行公钥证书有效；
——IC 卡公钥证书有效。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.214 AQFM080-00 恢复数据尾不是'BC'

测试目的：确保如果从签名的动态应用数据中恢复的数据尾不是‘BC’，终端动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中签名动态应用数据不是使用‘BC’结尾的数据计算得到。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.215 AQFM081-00 恢复数据头不等于'6A'

测试目的：如果从签名的动态应用数据中恢复的数据头不是‘6A’，终端将动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中签名动态应用数据不是使用‘6A’开头的数据计算得到。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.216 AQFM082-00 证书格式不等于'05'

测试目的：如果从签名的动态应用数据中恢复的证书格式不等于‘05’，终端将动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中签名动态应用数据不是使用‘05’的证书格式计算得到。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.217 AQFM083-00 计算的哈希结果与恢复的哈希结果的不同

测试目的：如果计算得到的哈希结果与从签名的动态应用数据中恢复出的哈希结果不相等，终端动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中签名动态应用数据使用错误的哈希值计算得到。

子类案例：——案例 01：哈希结果的第 11 个字节出错；
——案例 02：哈希结果的第 1 个字节出错；
——案例 03：哈希结果的最后一个字节出错。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.218 AQFM085-00 在动态数据认证中的 SDA 标签列表（1）

测试目的：执行 DDA 时，确保终端的 SDA 标签列表仅含有 AIP。

终端配置：支持 DDA。
卡片配置：卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）。
子类案例：——案例 1：SDA 包含 AFL 以及用此 AFL 值计算证书和哈希结果；
——案例 2：SDA 包含 AFL 和 AIP 以及用此 AFL 值和 AIP 值计算证书和哈希结果。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘1’（DDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.219 AQFM085-01 在动态数据认证中的 SDA 标签列表（2）

测试目的：执行 CDA 时，确保终端的 SDA 标签列表仅含有 AIP。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——通过设置 TAC 和 IAC，终端第一个 GAC 请求 TC。
子类案例：——案例 1：SDA 包含 AFL 以及用此 AFL 值计算证书和哈希结果；
——案例 2：SDA 包含 AFL 和 AIP 以及用此 AFL 值和 AIP 值计算证书和哈希结果。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端在 GAC 时不应该请求 CDA。终端完成交易，通过 TAC 和 IAC 的设置请求 TC。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1,位 4 为‘0’(未使用 DDA)。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.220 AQFM085-02 在动态数据认证中的 SDA 标签列表（3）

测试目的：执行 DDA 时，确保终端的 SDA 标签列表仅含有 AIP。
终端配置：支持 DDA。
卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——SDA 标签列标包含 AIP。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.221 AQFM085-03 在动态数据认证中的 SDA 标签列表（4）

测试目的：执行 CDA 时，确保终端的 SDA 标签列表仅含有 AIP。
终端配置：支持 CDA。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——SDA 标签列表包含 AIP。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。金融确认报文或批数据采集报文中的 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR

的字节 1，位 4 为‘0’（未使用 DDA）。金融确认报文或批数据采集报文中的 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）（该通过标准仅应用于假如终端请求 CDA）。

7.3.222 AQFM085-04 在动态数据认证中的 SDA 标签列表（5）

测试目的：执行 CDA 时，确保终端的 SDA 标签列表仅含有 AIP。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——通过设置 TAC 和 IAC，终端第一个 GAC 请求 TC。

子类案例：——案例 1：SDA 包含 AFL 以及用此 AFL 值计算证书和哈希结果；
——案例 2：SDA 包含 AFL 和 AIP 以及用此 AFL 值和 AIP 值计算证书和哈希结果。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端拒绝交易并且不执行2nd GAC当卡返回TC时，或者拒绝交易通过执行2nd GAC请求AAC当卡在1st GAC时返回ARQC。TVR字节1，位3 为‘1’（CDA失败）包含在第二个 GAC或者金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在第二个 GAC或者金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.3.223 AQFM085-05 在动态数据认证中的 SDA 标签列表（6）

测试目的：执行 CDA 时，确保终端的 SDA 标签列表仅含有 AIP。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——通过设置 TAC 和 IAC，终端第一个 GAC 请求 ARQC，第二个 GAC 请求 TC。

子类案例：——案例 1：SDA 包含 AFL 以及用此 AFL 值计算证书和哈希结果；
——案例 2：SDA 包含 AFL 和 AIP 以及用此 AFL 值和 AIP 值计算证书和哈希结果。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应该通过第二个 GAC 请求 AAC 拒绝交易。第二个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第二个 GENERATE AC 命令中的 TSI 的字节 1，位 8 为‘1’（脱机数据认证未完成）。

7.3.224 AQFM085-06 在动态数据认证中的 SDA 标签列表（7）

测试目的：执行 CDA 时，确保终端的 SDA 标签列表仅含有 AIP。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一次 GAC 时返回 ARQC；
——通过设置 TAC 和 IAC，终端第一个 GAC 请求 ARQC，第二个 GAC 请求 TC；
——发卡行批准交易

子类案例：——案例 1：SDA 包含 AFL 以及用此 AFL 值计算证书和哈希结果；
——案例 2：SDA 包含 AFL 和 AIP 以及用此 AFL 值和 AIP 值计算证书和哈希结果。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.3.225 AQFM085-07 在动态数据认证中的 SDA 标签列表（8）

测试目的：执行 CDA 时，确保终端的 SDA 标签列表仅含有 AIP。

终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——CDA 从不请求，第一个 GAC 请求 ARQC 时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一次 GAC 时返回 ARQC；
——通过设置 TAC 和 IAC，终端第一个 GAC 请求 ARQC，第二个 GAC 请求 TC。

子类案例：——案例 1：SDA 包含 AFL 以及用此 AFL 值计算证书和哈希结果；
——案例 2：SDA 包含 AFL 和 AIP 以及用此 AFL 值和 AIP 值计算证书和哈希结果。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.3.226 AQFM085-08 在动态数据认证中的 SDA 标签列表（9）

测试目的：执行 CDA 时，确保终端的 SDA 标签列表仅含有 AIP。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。

卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——交易联机接受；
——通过设置 TAC 和 IAC，终端第一个 GAC 请求 ARQC。

子类案例：——案例 1：SDA 包含 AFL 以及用此 AFL 值计算证书和哈希结果；
——案例 2：SDA 包含 AFL 和 AIP 以及用此 AFL 值和 AIP 值计算证书和哈希结果。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端在 1st GAC 和 2nd GAC 时不应该请求 CDA。终端应通过请求一个 TC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.227 AQFM085-09 在动态数据认证中的 SDA 标签列表（10）

测试目的：执行 CDA 时，确保终端的 SDA 标签列表仅含有 AIP。
终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。
卡片配置：——卡的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——通过设置 TAC 和 IAC，终端第一个 GAC 请求 ARQC；
——交易联机拒绝。
子类案例：——案例 1：SDA 包含 AFL 以及用此 AFL 值计算证书和哈希结果；
——案例 2：SDA 包含 AFL 和 AIP 以及用此 AFL 值和 AIP 值计算证书和哈希结果。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端在 1st GAC 和 2nd GAC 时不应该请求 CDA。终端应通过请求一个 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.228 AQFM086-00 储存在 IC 卡中的动态数据

测试目的：在动态数据认证过程中，终端包含标签为‘9F4C’的动态数字。
终端配置：支持 DDA。
卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——CDOL1 请求 IC 卡动态数字（标签为‘9F4C’）。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。标签为‘9F4C’的值和在 DDA 过程中使用的应相同（在第一个 GENERATE AC 中收到）。

7.3.229 AQFM086-01 IC 卡中的动态数据（1）

测试目的：在动态数据认证过程中，终端支持 IC 卡动态数据包含长度（28 字节）的值和可选的附加动态数据，总长度在 $L_{DD} \leqq Nic25$。
终端配置：支持 DDA。
卡片配置：——卡的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——CDOL1 请求 IC 卡动态数字（标签为‘9F4C’）；
——NIC 长度=247 字节，NI 长度=247 长度，NCA 长度=248 长度。
子类案例：——案例 01：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=2）不包含附加动态数据（LDD=3）；
——案例 02：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）不包含附加动态数据（LDD=9）；
——案例 03：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度

=8）+附加动态数据（长度=213 字节，值=AA--AA），没有填充（LDD=222）；

——案例 04：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=2）+附加动态数据（长度=219 字节，值=AA--AA），没有填充（LDD=222）；

——案例 05：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=4 字节，值=12345678）（LDD=9）；

——案例 06：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=9 字节，值=112233445566778FFF）（LDD=14）；

——案例 07：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=8 字节，值=TLV 所有的标签数据 5F508104AABBCCDD）（LDD=17）；

——案例 08：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=4 字节，值=1234BBBB）（LDD=9）；

——案例 09：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=6 字节，值=TLV“失效数据”数据：“5F2403400101”）（LDD=15）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。标签为‘9F4C’的值和在 DDA 过程中使用的应相同（在第一个 GENERATE AC 中收到）。

7.3.230 AQFM086-02 IC 卡中的动态数据（2）

测试目的：在动态数据认证过程中，终端支持 IC 卡动态数据包含长度（28 字节）的值和可选的附加动态数据，总长度在 $L_{DD} \leqq Nic25$。

终端配置：——支持 CDA；

——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡的 AIP 指明 CDA（AIP 的字节 1，位 1 为‘1’）；

——终端通过 IAC 和 TAC 的设置在第一个 GAC 时请求 TC；

——卡在第一个 GAC 时返回 TC；

——NIC 长度=238 字节，NI 长度=247 长度，NCA 长度=248 长度。

子类案例：——案例 01：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=2）不包含附加动态数据（LDD=32）；

——案例 02：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）不包含附加动态数据（LDD=38）；

——案例 03：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=175 字节，值=AA--AA），没有填充（LDD=213）；

——案例 04：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=2）+附加动态数据（长度=181 字节，值=AA--AA），没有填充（LDD=213）；

——案例 05：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=4 字节，值=12345678）（LDD=38）；

——案例 06：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=9 字节，值=112233445566778FFF）

（LDD=43）；

——案例 07：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=8 字节，值=TLV 所有的标签数据 5F508104AABBCCDD）（LDD=46）；

——案例 08：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=4 字节，值=1234BBBB）（LDD=38）；

——案例 09：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=6 字节，值=TLV“失效数据”数据：“5F2403400101”）（LDD=44）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。TVR 的字节 1，位 3 为‘0’（CDA 成功）包含在金融确认报文或者批上送报文。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或者批上送报文。

7.3.231 AQFM086-03 IC 卡中的动态数据（3）

测试目的：在动态数据认证过程中，终端支持 IC 卡动态数据包含长度（28 字节）的值和可选的附加动态数据，总长度在 $L_{DD} \leqq Nic25$。

终端配置：——支持 CDA；

——仅联机终端或有联机能力的脱机终端；

——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡的 AIP 指明支持 CDA （AIP 的字节 1，位 1 为‘1’）；

——终端通过 IAC 和 TAC 的设置在第一个 GAC 时请求 ARQC；

——卡在第一个 GAC 时返回 ARQC；

——CDOL2 请求 IC 卡动态数字（标签为‘9F4C’）；

——NIC 长度=238 字节，NI 长度=247 长度，NCA 长度=248 长度。

子类案例：——案例 01：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=2）不包含附加动态数据（LDD=32）；

——案例 02：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）不包含附加动态数据（LDD=38）；

——案例 03：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=175 字节，值=AA--AA），没有填充（LDD=213）；

——案例 04：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=2）+附加动态数据（长度=181 字节，值=AA--AA），没有填充（LDD=213）；

——案例 05：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=4 字节，值=12345678）（LDD=38）；

——案例 06：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=9 字节，值=112233445566778FFF）（LDD=43）；

——案例 07：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=8 字节，值=TLV 所有的标签数据 5F508104AABBCCDD）（LDD=46）；

——案例 08：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=4 字节，值=1234BBBB）（LDD=38）；

——案例 09：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=6 字节，值=TLV“失效数据”数据：

“5F2403400101”）（LDD=44）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或者批上送报文。在第二个 GENERATE AC 中收到标签为‘9F4C’的值和在动态签名使用的应相同。

7.3.232 AQFM086-04 IC 卡中的动态数据（4）

测试目的：在动态数据认证过程中，终端支持 IC 卡动态数据包含长度（28 字节）的值和可选的附加动态数据，总长度在 $L_{DD} \leqq Nic25$。

终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡的 AIP 指明支持 CDA （AIP 的字节 1，位 1 为‘1’）；
——终端通过 IAC 和 TAC 的设置在第一个 GAC 时请求 ARQC, 第二个 GAC 时请求 TC；
——卡在第一个 GAC 时返回 ARQC；
——CDOL2 请求 IC 卡动态数字（标签为‘9F4C’）；
——NIC 长度=238 字节，NI 长度=247 长度，NCA 长度=248 长度。

子类案例：——案例 01：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=2）不包含附加动态数据（L_{DD}=32）；
——案例 02：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）不包含附加动态数据（L_{DD}=38）；
——案例 03：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=175 字节，值=AA--AA）,没有填充（L_{DD}=213）；
——案例 04：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=2）+附加动态数据（长度=181 字节，值=AA--AA）,没有填充（L_{DD}=213）；
——案例 05：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=4 字节，值=12345678）（L_{DD}=38）；
——案例 06：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=9 字节，值=112233445566778FFF）（L_{DD}=43）；
——案例 07：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=8 字节，值=TLV 所有的标签数据 5F508104AABBCCDD）（L_{DD}=46）；
——案例 08：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=4）+附加动态数据（长度=4 字节，值=1234BBBB）（L_{DD}=38）；
——案例 09：被用在动态签名计算的 IC 卡动态数据=IC 卡动态数字（长度=8）+附加动态数据（长度=6 字节，值=TLV“失效数据”数据：“5F2403400101”）（L_{DD}=44）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。TVR 的字节 1，位 3 为‘0’（CDA 成功）包含在金融确认报文或者批上送报文。第一个 GENERATE AC 命令中 TVR 的字

节 1，位 7 为‘0’（未使用 SDA）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或者批上送报文。

7.3.233 AQFM119-00 在复合动态数据认证中的 PDOL

测试目的：确保在复合动态数据认证中可以使用 PDOL。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC。
子类案例：——案例 01：卡中存在 PDOL；
——案例 02：卡中的 PDOL 是空的；
——案例 03：卡中没有 PDOL。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应通过请求一个 TC 来完成交易。在金融确认报文或批数据采集报文中的 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。在金融确认报文或批数据采集报文中的 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.234 AQFM119-01 在复合动态数据认证中的 PDOL

测试目的：确保在复合动态数据认证中可以使用 PDOL。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC。
子类案例：——案例 01：卡中存在 PDOL；
——案例 02：卡中的 PDOL 是空的；
——案例 03：卡中没有 PDOL。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。在金融确认报文或批数据采集报文中的 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。在金融确认报文或批数据采集报文中的 TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.235 AQFM122-00 响应 AAC 为格式 1 或格式 2（1）

测试目的：——终端执行 CDA 时，若卡片在 GENERATE AC 命令中返回 AAC，则终端可以接受卡片返回的格式 1 或格式 2 的数据；
——若卡片返回 AAC，确保终端设置 TVR‘复合动态数据认证失败’位为 1。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC；
——卡中的 AIP 指明支持 CDA （AIP 的字节 1，位 1 为 1）。
子类案例：——案例 01：第一个 GENERATE AC 命令，卡片以格式 1 返回 AAC；
——案例 02：第一个 GENERATE AC 命令，卡片以格式 2 返回 AAC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于有存储拒绝交易能力的终端： TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。第一个 GENERATE AC 命令中 TVR 的字节 1,位 7 为‘0’(未使用 SDA)。第一个 GENERATE

AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.236 AQFM122-01 响应 AAC 为格式 1 或格式 2（2）

测试目的：——终端执行 CDA 时，若卡片在 GENERATE AC 命令中返回 AAC，则终端可以接受卡片返回的格式 1 或格式 2 的数据；
——若卡片返回 AAC，确保终端设置 TVR 复合动态数据认证失败’位为 1。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC；
——卡中的 AIP 指明支持 CDA （AIP 的字节 1，位 1 为‘1’）；
——卡在第一次 GAC 时返回 ARQC。
子类案例：——案例 01：第一个 GENERATE AC 命令，卡片以格式 1 返回 AAC；
——案例 02：第一个 GENERATE AC 命令，卡片以格式 2 返回 AAC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于有存储拒绝交易能力的终端： TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。第一个 GENERATE AC 命令中 TVR 的字节 1,位 7 为‘0’(未使用 SDA)。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.237 AQFM122-02 IC 卡响应 AAR（1）

测试目的：即使在 CDA 的过程中，确保终端将 AAR 视为逻辑错误并终止交易（当动态签名不存在的情况）。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——在第一个 GENERATE AC 中卡响应无数据签名的 AAR。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应终止交易。

7.3.238 AQFM122-03 IC 卡响应 AAR（2）

测试目的：即使在 CDA 的过程中，确保终端将 AAR 视为逻辑错误并终止交易（当动态签名存在的情况）。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——在第一个 GENERATE AC 中卡响应有数据签名的 AAR。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应终止交易。

7.3.239 AQFM122-04 响应 AAC 为格式 1 或格式 2（3）

测试目的：——终端执行 CDA 时，若卡片在 GENERATE AC 命令中返回 AAC，则终端可以接受卡片返回的格式 1 或格式 2 的数据；
——若卡片返回 AAC，确保终端设置 TVR 复合动态数据认证失败’位为 1。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡中的 AIP 指明支持 CDA （AIP 的字节 1，位 1 为‘1’）。

子类案例：——案例 01：第一个 GENERATE AC 命令，卡片以格式 1 返回 AAC；
——案例 02：第一个 GENERATE AC 命令，卡片以格式 2 返回 AAC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于有存储拒绝交易能力的终端： TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。第一个 GENERATE AC 命令中 TVR 的字节 1,位 7 为‘0’(未使用 SDA)。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA)。

7.3.240 AQFM122-05 响应 AAC 为格式 1 或格式 2（4）

测试目的：——终端执行 CDA 时，若卡片在 GENERATE AC 命令中返回 AAC，则终端可以接受卡片返回的格式 1 或格式 2 的数据；
——若卡片返回 AAC，确保终端设置 TVR 复合动态数据认证失败’位为 1。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡中的 AIP 指明支持 CDA （AIP 的字节 1，位 1 为‘1’)；
——卡在第一个 GAC 中返回 ARQC。
子类案例：——案例 01：第一个 GENERATE AC 命令，卡片以格式 1 返回 AAC；
——案例 02：第一个 GENERATE AC 命令，卡片以格式 2 返回 AAC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于有存储拒绝交易能力的终端： TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。第一个 GENERATE AC 命令中 TVR 的字节 1,位 7 为‘0’(未使用 SDA)。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA)。

7.3.241 AQFM122-06 IC 卡响应 AAR（3）

测试目的：即使在 CDA 的过程中，确保终端将 AAR 视为逻辑错误并终止交易（当动态签名存在的情况）。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’)；
——在第一个 GENERATE AC 中卡响应有不包含数据签名的 AAR。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应终止交易。

7.3.242 AQFM122-07 IC 卡响应 AAR（4）

测试目的：即使在 CDA 的过程中，确保终端将 AAR 视为逻辑错误并终止交易（当动态签名存在的情况）。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’)；
——在第一个 GENERATE AC 中卡响应有数据签名的 AAR。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应终止交易。

7.3.243 AQFM122-08 响应 AAC 为格式 1 或格式 2（5）

测试目的：终端执行 CDA 时，若卡片在 GENERATE AC 命令中返回 AAC，则终端可以接受卡片返回的格式 1 或格式 2 的数据。

终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码；
——CDA 从不请求，第一个 GAC 请求 ARQC 时。

卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡中的 AIP 指明支持 CDA （AIP 的字节 1，位 1 为‘1’）；
——卡在第一个 GAC 中返回 ARQC。

子类案例：——案例 01：第二个 GENERATE AC 命令，卡片以格式 1 返回 AAC；
——案例 02：第二个 GENERATE AC 命令，卡片以格式 2 返回 AAC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于包含金融确认报文或是批上送报文的有存储拒绝交易能力的终端：TSI 的字节 1，位 8 为‘1’（脱机数据认证已完成）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.244 AQFM123-00 签名的动态应用数据长度（1）

测试目的：确保终端在复合动态数据认证过程中比较签名的动态应用数据长度和 IC 卡公钥长度。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证 （AIP 的字节 1，位 1 为‘1’）；
——签名动态应用数据的长度与 IC 卡公钥长度不一致；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC。

子类案例：——案例 1：卡片在第一次 GAC 返回 TC；
——案例 2：卡片在第一次 GAC 返回 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：案例 01：终端拒绝交易且不执行第二个 GAC。案例 02：终端完成交易通过立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.245 AQFM123-01 签名的动态应用数据长度（2）

测试目的：确保终端在复合动态数据认证过程中比较签名的动态应用数据长度和 IC 卡公钥长度。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证 （AIP 的字节 1，位 1 为‘1’）；
——签名动态应用数据的长度与 IC 卡公钥长度不一致；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡片在第一次 GAC 返回 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端完成交易通过立即执行第二个 GAC 请求 AAC。第二个 GENERATE AC 命令中 TVR 字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。第二个 GENERATE AC 命令中 TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.246 AQFM123-02 签名的动态应用数据长度（3）

测试目的：确保终端在复合动态数据认证过程中比较签名的动态应用数据长度和 IC 卡公钥长度。

终端配置：——支持 CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——终端不能联机。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证 （AIP 的字节 1，位 1 为‘1’）；
——签名动态应用数据的长度与 IC 卡公钥长度不一致；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC，在第二次 GAC 请求 TC；
——卡片在第一次 GAC 返回 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.247 AQFM123-03 签名的动态应用数据长度（4）

测试目的：确保终端在复合动态数据认证过程中比较签名的动态应用数据长度和 IC 卡公钥长度。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证 （AIP 的字节 1，位 1 为‘1’）；
——签名动态应用数据的长度与 IC 卡公钥长度不一致；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC，在第二次 GAC 请求 TC；
——卡片在第一次 GAC 返回 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已进行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.248 AQFM124-00 恢复的数据尾不是‘BC’（1）

测试目的：确保终端在复合动态数据认证过程中对恢复数据尾进行检查。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC；
——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——数据尾不是‘BC’。
子类案例：——案例 1：卡在第一次 GAC 响应 TC；
——案例 2：卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：案例 01：终端拒绝交易不应该执行第二个 GAC。案例 02：终端完成交易应该立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.249 AQFM124-01 恢复的数据尾不是‘BC’（2）

测试目的：确保终端在复合动态数据认证过程中对恢复数据尾进行检查。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——数据尾不是‘BC’；
——卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端完成交易通过立即执行第二个 GAC 请求 AAC。第二个 GENERATE AC 命令中的 TVR 字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。第二个 GENERATE AC 命令中的 TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.250 AQFM125-00 恢复的数据头不是‘6A’（1）

测试目的：确保终端在复合动态数据认证过程中对恢复数据头进行检查。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——数据头不是‘6A’。
子类案例：——案例 1：卡在第一次 GAC 响应 TC；
——案例 2：卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：案例 01：终端拒绝交易不应该执行第二个 GAC。案例 02：终端完成交易应该立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.251 AQFM125-01 恢复的数据头不是‘6A’（2）

测试目的：确保终端在复合动态数据认证过程中对恢复数据头进行检查。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——数据头不是‘6A’；
——卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端完成交易通过立即执行第二个 GAC 请求 AAC。第二个 GENERATE AC 命令中的 TVR 字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。第二个 GENERATE AC 命令中的 TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）。

7.3.252 AQFM125-02 恢复的数据头不是‘6A’（3）

测试目的：确保终端在复合动态数据认证过程中对恢复数据头进行检查。
终端配置：——支持 CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——终端不能联机。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC，在第二次 GAC 请求 TC；
——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——在第二个 GAC，数据头不是‘6A’；
——卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.253 AQFM125-03 恢复的数据头不是‘6A’（4）

测试目的：确保终端在复合动态数据认证过程中对恢复数据头进行检查。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC，在第二次 GAC 请求 TC；
——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——在第二个 GAC，数据头不是‘6A’；
——卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.254 AQFM126-00 恢复的签名数据格式不等于‘05’（1）

测试目的：确保终端在复合动态数据认证过程中对恢复的数据签名格式进行检查。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——签名的数据格式不是‘05’；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 TC。
子类案例：——案例 1：卡在第一次 GAC 响应 TC；
——案例 2：卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：案例 01：终端拒绝交易不应该执行第二个 GAC。案例 02：终端完成交易应该立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.255 AQFM126-01 恢复的签名数据格式不等于‘05’（2）

测试目的：确保终端在复合动态数据认证过程中对恢复的数据签名格式进行检查。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——签名的数据格式不是‘05’；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC；
——卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端完成交易通过立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.256 AQFM126-02 恢复的签名数据格式不等于‘05’（3）

测试目的：确保终端在复合动态数据认证过程中对恢复的数据签名格式进行检查。
终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——在第二个 GAC，签名的数据格式不是‘05’；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC，在第二次 GAC 请求 TC；
——卡在第一次 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个

GENERATE AC 命令中的 TVR 字节 1,位 7 为‘0’(未使用 SDA)。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已进行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.257 AQFM126-03 恢复的签名数据格式不等于‘05’（4）

测试目的：确保终端在复合动态数据认证过程中对恢复的数据签名格式进行检查。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——在第二个 GAC，签名的数据格式不是‘05’；
——通过设置 TAC 和 IAC，终端在第一次 GAC 请求 ARQC，在第二次 GAC 请求 TC；
——卡在第一次 GAC 响应 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1,位 7 为‘0’(未使用 SDA)。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已进行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.258 AQFM127-00 恢复的 CID 与从 GENERATE AC 中获取的 CID 不一致（1）

测试目的：确保终端检查在复合动态数据认证过程恢复得到的 CID 和 GENERATE AC 命令返回的 CID 是否相同。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端的第一个 GENERATE AC 命令请求 TC；
——卡片在第一个 GAC 返回 TC；
——签名数据中的 CID 为 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端完成交易通过立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’(CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.259 AQFM127-01 恢复的 CID 与从 GENERATE AC 中获取的 CID 不一致（2）

测试目的：确保终端检查在复合动态数据认证过程恢复得到的 CID 和 GENERATE AC 命令返回的 CID 是否相同。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENERATE AC 中请求一个 TC；
——卡在第一个 GAC 响应 ARQC；
——签名数据中的 CID 是 TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易不应该执行第二个 GAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.260 AQFM127-02 恢复的 CID 与从 GENERATE AC 中获取的 CID 不一致（3）

测试目的：确保终端检查在复合动态数据认证过程恢复得到的 CID 和 GENERATE AC 命令返回的 CID 是否相同。

终端配置：——支持 CD；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENERATE AC 中请求一个 ARQC；
——卡在第一个 GAC 响应 ARQC；
——签名数据中的 CID 是 TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易不应该执行第二个 GAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.261 AQFM128-00 比较哈希结果 （1）

测试目的：确保终端在复合动态数据认证中比较哈希结果。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——哈希结果是错误的；
——设置 TAC 和 IAC 使终端在第一个 GENERATE AC 中请求一个 TC。

子类案例：——案例 1：卡在第一个 GAC 响应 TC；
——案例 2：卡在第一个 GAC 响应 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：案例 01：终端拒绝交易不应该执行第二个 GAC。案例 02：终端完成交易应该立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.262 AQFM128-01 比较哈希结果 （2）

测试目的：确保终端在复合动态数据认证中比较哈希结果。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——哈希结果是错误的；

——设置 TAC 和 IAC 使终端在第一个 GENERATE AC 中请求一个 ARQC；
——卡在第一个 GAC 响应 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端完成交易通过立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 =‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.263 AQFM128-02 比较哈希结果 （3）

测试目的：确保终端在复合动态数据认证中比较哈希结果。

终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——在第二个 GAC,哈希结果是错误的；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC, 在第二个 GAC 中请求 TC；
——卡在第一个 GAC 响应 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1,位 7 为‘0’(未使用 SDA)。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 =‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.264 AQFM128-03 比较哈希结果 （4）

测试目的：确保终端在复合动态数据认证中比较哈希结果。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——在第二个 GAC 响应中,哈希结果是错误的；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC, 在第二个 GAC 中请求 TC；
——卡在第一个 GAC 响应 ARQC；
——发卡行批准交易。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1,位 7 为‘0’(未使用 SDA)。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.265 AQFM129-00 比较交易数据哈希值（1）

测试目的：确保终端在复合动态数据认证中比较交易数据哈希值。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——哈希数据结果是错误的；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 TC。
子类案例：——案例 01：卡在第一个 GAC 响应 TC；
——案例 02：卡在第一个 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：案例 01：终端拒绝交易不应该执行第二个 GAC。案例 02：终端完成交易应该立即执行第二个 GAC 请求 AAC。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.266 AQFM129-01 比较交易数据哈希值（2）

测试目的：确保终端在复合动态数据认证中比较交易数据哈希值。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——哈希数据结果是错误的；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC；
——卡在第一个 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端完成交易通过立即执行第二个 GAC 请求 AAC。第二个 GENERATE AC 命令中的 TVR 字节 1，位 3 为‘1’（CDA 失败）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。第二个 GENERATE AC 命令中的 TSI 字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.3.267 AQFM129-02 比较交易数据哈希值（3）

测试目的：确保终端在复合动态数据认证中比较交易数据哈希值。
终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——在第二个 GAC 返回哈希数据结果是错误的；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC，在第二个 GAC 中请求 TC；
——卡在第一个 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.268 AQFM129-03 比较交易数据哈希值（4）

测试目的：确保终端在复合动态数据认证中比较交易数据哈希值。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——在第二个 GAC 返回哈希数据结果是错误的；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC，在第二个 GAC 中请求 TC；
——卡在第一个 GAC 响应 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.269 AQFM130-00 在 CDA 中的发卡行应用数据（1）

测试目的：确保终端复合动态数据认证中可以使用发卡行应用数据。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 TC；
——卡对第一个 GENERATE AC 的响应是 ARQC，第二个 GENERATE AC 的响应是 TC；
——第一个 GENERATE AC 命令的响应中存在发卡行应用数据。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。第二个 GENERATE AC 命令中字节 1，位 3 为‘0’（复合动态数据执行成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。金融确认报文或批数据采集报文中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.3.270 AQFM130-01 在 CDA 中的发卡行应用数据（2）

测试目的：确保终端在复合动态数据认证中可以使用发卡行应用数据。
终端配置：——支持 CDA；
——终端不能联机；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 TC，在第二个 GAC 中请求 TC；
——卡中的 AIP 指明支持复合动态数据认证（AIP 的第 1 个字节，位 1 为‘1’）；
——卡对第一个 GENERATE AC 的响应是 ARQC，对第二个 GENERATE AC 的响应是 TC；
——第二个 GENERATE AC 命令的响应中存在发卡行应用数据。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。TVR，TSI （包含在金融确认信息或批数据获取信息中或是其他中应该：TVR 的字节 1，位 3 为‘0’（CDA 成功）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC 命令中 TVR 的字节 1，位

7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.271 AQFM130-02 在 CDA 中的发卡行应用数据（3）

测试目的：确保终端复合动态数据认证中可以使用发卡行应用数据。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC；
——卡对第一个 GENERATE AC 的响应是 ARQC，第二个 GENERATE AC 的响应是 TC；
——第一个 GENERATE AC 命令的响应中存在发卡行应用数据。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应完成交易。第二个 GENERATE AC 命令中字节 1，位 3 为‘0’（复合动态数据执行成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。金融确认报文或批数据采集报文中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.3.272 AQFM130-03 在 CDA 中的发卡行应用数据（4）

测试目的：确保终端在复合动态数据认证中可以使用发卡行应用数据。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC；
——卡中的 AIP 指明支持复合动态数据认证(AIP 的第 1 个字节,位 1 为‘1’)；
——卡对第一个 GENERATE AC 的响应是 ARQC，对第二个 GENERATE AC 的响应是 TC；
——第二个 GENERATE AC 命令的响应中存在发卡行应用数据。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应完成交易。TVR，TSI （包含在金融确认信息或批数据获取信息中或是其他中应该：TVR 的字节 1，位 3 为‘0’（CDA 成功）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.273 AQFM130-04 在 CDA 中的发卡行应用数据（5）

测试目的：确保终端在复合动态数据认证中可以使用发卡行应用数据。

终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC, 在第二个 GAC 中请求 TC；
——卡中的 AIP 指明支持复合动态数据认证(AIP 的第 1 个字节,位 1 为‘1’)；
——卡对第一个 GENERATE AC 的响应是 ARQC，对第二个 GENERATE AC 的响应是 TC；
——第二个 GENERATE AC 命令的响应中存在发卡行应用数据。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应完成交易。TVR，TSI （包含在金融确认信息或批数据获取信息中或是其他中应该：TVR 的字节 1，位 3 为‘0’（CDA 成功）。TSI 的字节 1，位 8 =‘1’（脱机数据认证已执行）；第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）；第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.274 AQFM131-00 IC 卡动态数字的存储（1）

测试目的：确保在复合动态数据认证中，终端在标签‘9F4C’中存储 IC 卡动态数字。

终端配置：——支持 CDA；
——终端不能联机；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——CDOL2 请求 IC 卡动态数字（标签为‘9F4C’）；
——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 TC；
——卡第一个 GENERATE AC 的响应是 ARQC，第二个 GENERATE AC 的响应是 TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应完成交易。第二个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。储存在标签‘9F4C’中的 IC 卡动态数字与在复合动态数据认证的第 2 个 GENERATE AC 命令中收到的一致。TVR，TSI （包含在金融确认报文或批上送数据报文中或是其他中）有：TVR 的字节 1，位 3 为‘0’（CDA 成功）；TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.3.275 AQFM131-01 IC 卡动态数字的存储（2）

测试目的：确保在复合动态数据认证中，终端在标签‘9F4C’中存储 IC 卡动态数字。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时 或 CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——CDOL2 请求 IC 卡动态数字（标签为‘9F4C’）；
——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC；
——卡第一个 GENERATE AC 的响应是 ARQC，第二个 GENERATE AC 的响应是 TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应完成交易。第二个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。TVR，TSI 和 IC 卡动态数字 （包含在金融确认报文或批上送数据报文中或是其他中）有：TVR 的字节 1，位 3 为‘0’（CDA 成功）；TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）；存储在‘9F4C’中的 IC 卡动态数同在复合动态数据认证中使用的一样。

7.3.276 AQFM133-00 终端产生的不可预知数

测试目的：确保在复合动态数据认证中，对于不同交易终端产生一个不同的随机数。

终端配置：支持 CDA。

卡片配置：——CDOL1 和 CDOL2 中包含有终端产生的不可预知数（标签为‘9F37’）；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）。

测试流程：至少进行三个交易。比较由终端产生的不可预知数的值。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。在金融确认报文中或是批上送数据报文中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。金融确认报文或批上送数据报文中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）（该通过标准仅用于 CDA 被请求）。比较本次交易和上次交易中标签为‘9F37’的数据。它们应不同。

7.3.277 AQFM133-01 CDOL 中不包含不可预测数（1）

测试目的：确保在复合动态数据认证中，终端不会校验 CDOL1 和 CDOL2 中是否存在不可预测数。

终端配置：支持 CDA。

卡片配置：——CDOL1 和 CDOL2 中不包含有终端产生的不可预知数（标签为‘9F37’）；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。TVR 字节 1，位 3 为‘1’（CDA 失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易并且 CDA 被请求）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 3 为‘0’（CDA 未失败）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。TSI 字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易并且 CDA 被请求）。

7.3.278 AQFM133-02 CDOL 中不包含不可预测数（2）

测试目的：确保在 CDOL1 和 CDOL2 中不含有 9F37 而且不执行 CDA 时，终端能够忽略 9F37 的不存在并且继续完成交易，在联机交易中 CDA 不会失败。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC 时；
——CDA 从不请求，在第二个 GAC 请求 TC 时。

卡片配置：——CDOL1 和 CDOL2 中不包含有终端产生的不可预知数（标签为‘9F37’）；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 ARQC，在第二个 GAC 中请求 TC；
——卡在第一个 GAC 中响应 ARQC；
——发卡行批准交易。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个 TC 来完成交易。第一个和第二个 GENERATE AC 命令中的 TVR 字节 1，位 3 为‘0’（未使用 CDA）。第一个和第二个 GENERATE AC 命令中的 TVR 字节 1，位 7 为‘0’（未使用 SDA）。第一个和第二个 GENERATE AC 命令中的 TVR 字节 1，位 4 为‘0’（未使用 DDA）。

7.3.279 AQFM134-00 以格式 2 的 TC 或者 ARQC 响应 GENERATE AC （1）

测试目的：——确保终端在 CDA 中可以使用 IC 卡响应格式 2；
——确保终端在标签‘9F26’中存储用于复合动态数据认证的应用密文。

终端配置：——支持 CDA；
——终端不能联机；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——卡以格式 2 响应 GENERATE AC；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 TC，在第二个 GAC 中请求 TC。

子类案例：——案例 01：卡在第一个 GENERATE AC 响应一个 TC；
——案例 03：卡在第一个 GENERATE AC 响应 ARQC,在第 2 个 GENERATE AC 响应 TC。

注：这里的子案例序号不是线性连续的，中间缺失的编号被分配给了早期的一些子案例，但这些子案例不再适用。为避免混淆，不调整子案例编号为线性连续的。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个 TC 来完成交易。金融确认报文或批上送数据报文信息中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。 金融确认报文或批上送数据报文信息中 TSI 的字节 1，位 8 为‘1’ （脱机数据认证已执行）。金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.280 AQFM134-01 以不是格式 2 的 TC 或者 ARQC 响应 GENERATE AC （隐含的）（1）

测试目的：确保在执行复合动态数据认证，卡片响应 TC 或 ARQC 时，终端不使用格式 1 的响应。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）。

子类案例：——案例 01：IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 TC。卡使用格式 1 编码响应 TC；
——案例 02：IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 TC,卡以格式 1 编码响应 ARQC；
——案例 03：IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 TC，在第二个 GENERATE AC 请求 TC，卡片在第一个 GENERATE AC 以格式 2 编码响应 ARQC，卡片在第二个 GENERATE AC 以格式 1 编码响应 TC。终端不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端拒绝或终止交易。案例 03：终端应拒绝或终止交易。TSI 字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.3.281 AQFM134-03 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（1）

测试目的：确保在 CDA 中，终端不支持以 TC 格式的响应 AAC（使用 AAC 生成签名）。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GAC 中请求 TC。

子类案例：——案例 01：第一个 GENERATE AC 命令，卡片返回格式 2 含数字签名的 AAC（同返回 TC 的过程一样）；
——案例 02：卡第一个 GAC 返回 ARQC，第二个 GENERATE AC 命令，卡片返回格式 2 含数字签名的 AAC（同返回 TC 的过程一样）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端拒绝或终止交易。通过标准仅适用在终端存储拒绝交易的情况下：TVR 的字节 1，位 3 为‘0’（CDA 未失败）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，

位 4 为‘0’（未使用 DDA）。

7.3.282 AQFM134-04 GENERATE AC 命令中复合动态数据认证参考控制参数（1）

测试目的：确保 GENERATE AC 命令中的参考控制参数请求复合动态数据认证。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端处理交易到完成。P1 =参考控制参数（50 TC）。

7.3.283 AQFM134-05 以格式 2 的 TC 或者 ARQC 响应 GENERATE AC （2）

测试目的：——确保终端在 CDA 中可以使用 IC 卡响应格式 2；
——确保终端在标签‘9F26’中存储用于复合动态数据认证的应用密文。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡以格式 2 响应 GENERATE AC；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC。
子类案例：——案例 01：卡响应一个 ARQC；
——案例 02：卡在第 1 个 GAC 响应 ARQC，在第 2 个 GAC 响应 TC；
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应通过请求一个 TC 来完成交易。金融确认报文或批上送数据报文信息中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。金融确认报文或批上送数据报文信息中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.284 AQFM134-06 以不是格式 1 的 TC 或者 ARQC 响应 GENERATE AC （隐含的）（2）

测试目的：确保在执行复合动态数据认证，卡片响应 TC 或 ARQC 时，终端不使用格式 1 的响应。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）。
子类案例：——案例 01：IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC。卡使用格式 1 编码响应 TC；
——案例 02：IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC，在第二个 GENERATE AC 请求 TC，卡对第一个 GAC 以格式 2 编码响应 ARQC，对第二个 GAC 以格式 1 编码响应 TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端拒绝或终止交易。本通过标准只在终端能存储被拒绝的交易情况下适用：TSI 的字节 1，位 8 =‘1’（脱机数据认证已执行），应包含在金融确认报文或批上送数据报文信息中。

7.3.285 AQFM134-07 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（2）

测试目的：确保在 CDA 中，终端不支持以 TC 格式的响应 AAC（使用 AAC 生成签名）。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC；
——第一个 GENERATE AC 命令，卡片返回格式 2 含数字签名的 AAC （同返回 TC 的过程一样）。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：交易应被拒绝。通过标准仅适用在终端存储拒绝交易的情况下：TVR 的字节 1，位 3 为‘1’（CDA 失败），应包含在金融确认报文或批上送数据报文信息中。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.286 AQFM134-08 GENERATE AC 命令中复合动态数据认证参考控制参数（2）

测试目的：确保 GENERATE AC 命令中的参考控制参数请求复合动态数据认证。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，第二个 GENERATE AC 请求 TC；
——发卡行批准交易。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端处理交易到完成。第一个 GAC，P1 90 –ARQC。第二个 GAC，P1 50 – TC（当不支持 CDA 的 GAC2 TC，P1 为‘40’）。

7.3.287 AQFM134-09 以格式 2 的 TC 或者 ARQC 响应 GENERATE AC （3）

测试目的：——确保终端在 CDA 中可以使用 IC 卡响应格式 2；
——确保终端在标签‘9F26’中存储用于复合动态数据认证的应用密文。
终端配置：——支持 CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡以格式 2 响应 GENERATE AC；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，第二个 GENERATE AC 请求 TC。
子类案例：——案例 01：卡在第一个 GENERATE AC 响应一个 ARQC；
——案例 02：卡在第 2 个 GENERATE AC 响应一个 TC，终端不能联机。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应通过请求一个 TC 来完成交易。金融确认报文或批上送数据报文信息中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。 金融确认报文或批上送数据报文信息中 TSI 的字节 1，位 8 为‘1’ （脱机数据认证已执行）。金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。案例 01：如果终端支持 CDA 为 mode1/4,金融确认报文或批上送

数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。如果终端支持 CDA 为其他类型,金融确认报文或批上送数据报文信息中包含的应用密文(标签为‘9F26’)与第二个 GAC 响应的一样。案例 02：金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。

7.3.288 AQFM134-10 以不是格式 1 的 TC 或者 ARQC 响应 GENERATE AC （隐含的）（3）

测试目的：确保在执行复合动态数据认证，卡片响应 TC 或 ARQC 时，终端不使用格式 1 的响应。

终端配置：——支持 CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——支持 CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）。

子类案例：——案例 01：IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC，卡使用格式 1 编码响应 ARQC；
——案例 02：IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC, 在第二个 GENERATE AC 请求 TC,卡以格式 2 编码响应 ARQC,以格式 1 编码响应 TC。终端不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端拒绝或中止交易。本通过标准只在终端能存储被拒绝的交易情况下适用：TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行），应包含在金融确认报文或批上送数据报文信息中。

7.3.289 AQFM134-11 以格式 2 的 TC 或者 ARQC 响应 GENERATE AC （4）

测试目的：——确保终端在 CDA 中可以使用 IC 卡响应格式 2；
——确保终端在标签‘9F26’中存储用于复合动态数据认证的应用密文。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡以格式 2 响应 GENERATE AC；
——IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC；
——发卡行批准交易；
——卡在第 2 个 GENERATE AC 响应一个 TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个 TC 来完成交易。金融确认报文或批上送数据报文信息中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。 金融确认报文或批上送数据报文信息中 TSI 的字节 1，位 8 为‘1’ （脱机数据认证已执行）。金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.290 AQFM134-12 以不是格式 1 的 TC 或者 ARQC 响应 GENERATE AC （隐含的）（4）

测试目的：确保在执行复合动态数据认证，卡片响应 TC 或 ARQC 时，终端不使用格式 1 的响应。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC，在第二个 GENERATE AC 请求 TC。卡在第一个 GENERATE AC 以格式 2 编码响应 ARQC，卡片在第二个 GENERATE AC 以格式 1 编码响应 TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端拒绝或终止交易。本通过标准只在终端能存储被拒绝的交易情况下适用：TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行），应包含在金融确认报文或批上送数据报文信息中。

7.3.291 AQFM134-13 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（3）

测试目的：确保在 CDA 中，终端不支持以 TC 格式的响应 AAC（使用 AAC 生成签名）。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求在第二个 GAC 请求 TC 时。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC；
——发卡行批准交易；
——第二个 GENERATE AC 命令，卡片返回格式 2 含数字签名的 AAC （同返回 TC 的过程一样）。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：交易应被拒绝。通过标准仅适用在终端存储拒绝交易的情况下：TVR 的字节 1，位 3 为‘0’（CDA 未失败），应包含在金融确认报文或批上送数据报文信息中。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.292 AQFM134-14 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（4）

测试目的：确保在 CDA 中，终端不支持以 TC 格式的响应 AAC（使用 AAC 生成签名）。
终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC，在第二个 GENERATE AC 请求 TC；
——第二个 GENERATE AC 命令，卡片返回格式 2 含数字签名的 AAC （同返回 TC 的过程一样）。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：交易应被拒绝。通过标准仅适用在终端存储拒绝交易的情况下：TVR 的字节 1，位 3 为‘0’（CDA 未失败），应包含在金融确认报文或批上送数据报文信息中。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.293 AQFM134-15 GENERATE AC 命令中复合动态数据认证参考控制参数（3）

测试目的：确保 GENERATE AC 命令中的参考控制参数请求复合动态数据认证。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，第二

个 GENERATE AC 请求 TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端处理交易到完成。P1 =参考控制参数 （50 TC，90 ARQC）。

7.3.294 AQFM134-16 GENERATE AC 命令中复合动态数据认证参考控制参数（4）

测试目的：确保 GENERATE AC 命令中的参考控制参数请求复合动态数据认证。
终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，第二个 GENERATE AC 请求 TC；
——发卡行批准交易。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端处理交易到完成。第二个 GAC，P1 为‘50’ – TC。

7.3.295 AQFM134-17 GENERATE AC 命令中复合动态数据认证参考控制参数（5）

测试目的：确保 GENERATE AC 命令中的参考控制参数请求复合动态数据认证。
终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，第二个 GENERATE AC 请求 TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端处理交易到完成。第二个 GAC，P1 50 – TC。

7.3.296 AQFM134-18 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（3）

测试目的：确保在 CDA 中，终端不支持以 TC 格式的响应 AAC（使用 AAC 生成签名）。
终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——CDA 总是请求，在第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——IAC 和 TAC 设置使得终端在第一个 GENERATE AC 请求 ARQC；
——第二个 GENERATE AC 命令，卡片返回格式 2 含数字签名的 AAC （同返回 TC 的过程一样）。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：交易应被拒绝。通过标准仅适用在终端存储拒绝交易的情况下：TVR 的字节 1，位 3 为‘0’（CDA 未失败），应包含在金融确认报文或批上送数据报文信息中。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.297 AQFM135-00 在复合动态数据认证中，GENERATE AC 响应中缺少必备的数据对象（1）

测试目的：——确保终端检查 JR/T0025.7—2013 中 5.3.6 条表 18 中数据的存在；
——通过执行 CDA 验证。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 TC；
——卡以格式 2 对 GENERATE AC 命令响应。

子类案例：——案例 01：卡响应第一个 GENERATE AC 的 TC 中不存在签名的动态应用数据（标签为‘9F4B’）；
——案例 02：卡响应第一个 GENERATE AC 的 TC 中不存在密文信息数据（标签为‘9F27’）；
——案例 03：卡响应第一个 GENERATE AC 的 TC 中不存在应用交易计数器（标签为‘9F36’）；
——案例 04：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC 的 TC 中不存在签名的动态应用数据（标签为‘9F4B’），终端不能联机；
——案例 05：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC 的 TC 中不存在密文信息数据（标签为‘9F27’），终端不能联机；
——案例 06：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC 的 TC 中不存在应用交易计数器（标签为‘9F36’），终端不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应终止交易。

7.3.298 AQFM135-01 在复合动态数据认证中，GENERATE AC 响应中缺少必备的数据对象（2）

测试目的：——确保终端检查 JR/T0025.7—2013 中 5.3.6 条表 18 中数据的存在；
——通过执行 CDA 验证。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC；
——卡以格式 2 对 GENERATE AC 命令响应。

子类案例：——案例 01：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC 的 TC 中不存在签名的动态应用数据（标签为‘9F4B’）；
——案例 02：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC 的 TC 中不存在密文信息数据（标签为‘9F27’）；
——案例 03：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC 的 TC 中不存在应用交易计数器（标签为‘9F36’）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应终止交易。

7.3.299 AQFM135-02 在复合动态数据认证中，GENERATE AC 响应中缺少必备的数据对象（3）

测试目的：——确保终端检查 JR/T0025.7—2013 中 5.3.6 条表 18 中数据的存在；
——通过执行 CDA 验证。

终端配置：——支持 CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，在第二个 GENERATE AC 命令中请求 TC；
——卡以格式 2 对 GENERATE AC 命令响应。

子类案例：——案例 01：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC

的 TC 中不存在签名的动态应用数据（标签为‘9F4B’）；
——案例 02：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC 的 TC 中不存在密文信息数据（标签为‘9F27’）；
——案例 03：卡在第一个 GENERATE AC 响应 ARQC，响应第二个 GENERATE AC 的 TC 中不存在应用交易计数器（标签为‘9F36’）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应终止交易。

7.3.300 AQFM136-00 用于交易数据哈希计算的 CDOL2 的值 （1）

测试目的：执行复合动态数据认证时，终端保存第 2 个 GENERATE AC 命令中由 CDOL2 指定的数据元的值。

终端配置：——支持 CDA；
——仅脱机终端；
——有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为 ‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 TC，在第二个 GENERATE AC 命令中请求 TC；
——交易不能联机；
——卡在第 1 个 GENERATE AC 时返回 ARQC，且动态签名正确；
——卡在第 2 个 GENERATE AC 时返回 TC，且动态签名正确。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR 和 TSI （包含在金融确认报文或者批数据采集报文数据或者其他中） 有：TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。TVR 的字节 1，位 4 为‘0’（DDA 未失败）。TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.301 AQFM136-01 用于交易数据哈希计算的 CDOL2 的值 （2）

测试目的：执行复合动态数据认证时，终端保存第 2 个 GENERATE AC 命令中由 CDOL2 指定的数据元的值。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为 ‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC；
——卡在第 1 个 GENERATE AC 时返回 ARQC，且动态签名正确；
——卡在第 2 个 GENERATE AC 时返回 TC，且动态签名正确。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR 和 TSI （包含在金融确认报文或者批数据采集报文数据或者其他中） 有：TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。TVR 的字节 1，位 4 为‘0’（DDA 未失败）。TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.302 AQFM136-02 用于交易数据哈希计算的 CDOL2 的值 （3）

测试目的：执行复合动态数据认证时，终端保存第 2 个 GENERATE AC 命令中由 CDOL2 指定的数据元的值。

终端配置：——支持 CDA；
——仅联机终端；

——当不能联机时，正常处理缺省行为码；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为 ‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，在第二个 GENERATE AC 命令中请求 TC；
——交易不能联机；
——卡在第 1 个 GENERATE AC 时返回 ARQC，且动态签名正确；
——卡在第 2 个 GENERATE AC 时返回 TC，且动态签名正确。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR 和 TSI （包含在金融确认报文或者批数据采集报文数据或者其他中） 有：TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。TVR 的字节 1，位 4 为‘0’（DDA 未失败）。TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.303 AQFM137-00 用于交易数据哈希计算的 PDOL 的值 （1）

测试目的：确保终端储存 PDOL 指定的数据元的值，用于复合动态数据认证的第 2 个 GENERATE AC 中。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，在第二个 GENERATE AC 命令中请求 TC；
——交易不能联机；
——第一个 GENERATE AC 中卡片返回 ARQC，动态签名正确；
——第二个 GENERATE AC 中卡片返回 TC，动态签名正确；
——卡中存在 PDOL（由 PDOL 指定的数据元的值将在第 1 个 GENERATE AC 命令和第 2 个 GENERATE AC 之间变化）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR 和 TSI （包含在金融确认报文或者批数据采集报文数据或者其他中） 有：第一个 GENERATE AC 中 TVR 的字节 1，位 3 =‘0’（CDA 成功）。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）的。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。

7.3.304 AQFM137-01 用于交易数据哈希计算的 PDOL 的值 （2）

测试目的：确保终端储存 PDOL 指定的数据元的值，用于复合动态数据认证的第 2 个 GENERATE AC 中。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC；
——交易不能联机；
——第一个 GENERATE AC 中卡片返回 ARQC，动态签名正确；
——第二个 GENERATE AC 中卡片返回 TC，动态签名正确；
——卡中存在 PDOL（由 PDOL 指定的数据元的值将在第 1 个 GENERATE AC 命令和第 2 个 GENERATE AC 之间变化）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR 和 TSI （包含在金融确认报文或者批数据采集报文或者其他中） 有：第 1 个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第 1 个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）的。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。

7.3.305 AQFM137-02 用于交易数据哈希计算的 PDOL 的值 （3）

测试目的：确保终端储存 PDOL 指定的数据元的值，用于复合动态数据认证的第 2 个 GENERATE AC 中。

终端配置：——支持 CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 IAC 和 TAC 使终端在第一个 GENERATE AC 命令中请求 ARQC，在第一个 GENERATE AC 命令中请求 TC；
——交易不能联机；
——第一个 GENERATE AC 中卡片返回 ARQC，动态签名正确；
——第二个 GENERATE AC 中卡片返回 TC，动态签名正确；
——卡中存在 PDOL（由 PDOL 指定的数据元的值将在第 1 个 GENERATE AC 命令和第 2 个 GENERATE AC 之间变化）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR 和 TSI （包含在金融确认报文或者批数据采集报文或者其他中） 有：第 1 个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第 1 个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）的。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。

7.3.306 AQFM138-00 第 1 次复合动态数据认证生成时，请求 AAC

测试目的：确保当终端第一个 GENERATE AC 请求 AAC 时，不请求复合动态数据认证。

终端配置：支持 CDA。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 AAC。

测试流程：选择卡片应用，执行交易（在特殊的 CDA 中）。

通过标准：终端将处理交易直至结束，交易被拒绝。第 1 个 GENERATE AC 命令的 P1 =‘00’。

7.3.307 AQFM138-01 第 2 次复合动态数据认证生成时，请求 AAC

测试目的：确保当终端第二个 GENERATE AC 请求 AAC 时，不请求复合动态数据认证。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡在第一个 GENARATE AC 命令中返回 ARQC；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 AAC；
——设置 TAC 和 IAC 或通过发卡行返回拒绝，使得终端在第二个 GENERATE AC 命令中请求 AAC。

测试流程：选择卡片应用，执行交易（在特殊的 CDA 中）。

通过标准：终端将处理交易直至结束，交易被拒绝。第 2 个 GENERATE AC 命令的 P1 =‘00’。

7.3.308 AQFM139-00 用于交易数据哈希计算的 CDOL1 的值（1）

测试目的：确保终端存储第一个 GENERATE AC 命令中发送的 CDOL1 指定的数据，用于复

合动态数据认证。

终端配置：——支持 CDA；

——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 TC；

——第 1 个 GENERATE AC 命令，卡片返回 ARQC 且复合动态数据认证正确；

——第 2 个 GENERATE AC 命令，卡片返回 TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应完成交易。第二个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。金融确认报文或批数据采集报文数据的 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.3.309 AQFM139-01 用于交易数据哈希计算的 CDOL1 的值（2）

测试目的：确保终端在第二个 GAC 执行 CDA 时会存储 CDOL1 指定的数据，用于复合动态数据认证。

终端配置：——支持 CDA；

——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 TC，在第二个 GENARATE AC 命令中请求 TC；

——交易不能联机；

——第 1 个 GENERATE AC 命令，卡片返回 ARQC，复合动态数据认证正确；

——第 2 个 GENERATE AC 命令，卡片返回 TC，复合动态数据认证正确。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。TVR 和 TSI（包含在金融确认报文或批上送数据报文或其他）有：TVR 的字节 1，位 3 为‘0’（CDA 成功）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.310 AQFM139-02 用于交易数据哈希计算的 CDOL1 的值（3）

测试目的：确保终端存储第一个 GENERATE AC 命令中发送的 CDOL1 指定的数据，用于复合动态数据认证。

终端配置：——支持 CDA；

——仅联机终端；

——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC；

——第 1 个 GENERATE AC 命令，卡片返回 ARQC 且复合动态数据认证正确；

——第 2 个 GENERATE AC 命令，卡片返回 TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应完成交易。第二个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。金融确认报文或批数据采集报文数据的 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.3.311 AQFM139-03 用于交易数据哈希计算的 CDOL1 的值（4）

测试目的：确保终端存储 CDOL1 指定的数据，用于复合动态数据认证。

终端配置：——支持 CDA；

——仅联机终端；

——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC；
——发卡行批准交易；
——第 2 个 GENERATE AC 命令，卡片返回 TC，复合动态数据认证正确。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个 TC 来完成交易。TVR 和 TSI（包含在金融确认报文或批上送数据报文或其他）有：TVR 的字节 1，位 3 为‘0’（CDA 成功）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.312 AQFM139-04 用于交易数据哈希计算的 CDOL1 的值（5）

测试目的：确保终端存储 CDOL1 指定的数据，用于复合动态数据认证。
终端配置：——支持 CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，在第二个 GENARATE AC 命令中请求 TC；
——交易不能联机；
——第 1 个 GENERATE AC 命令，卡片返回 ARQC，复合动态数据认证正确；
——第 2 个 GENERATE AC 命令，卡片返回 TC，复合动态数据认证正确。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端应通过请求一个 TC 来完成交易。TVR 和 TSI（包含在金融确认报文或批上送数据报文或其他）有：TVR 的字节 1，位 3 为‘0’（CDA 成功）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。

7.3.313 AQFM140-00 终端请求 ARQC 时，不请求 CDA

测试目的：确保终端请求 ARQC 不带 CDA 时，不会执行带 CDA 的 GAC。
终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端完成交易且第一个 GAC 未请求 CDA。P1 =参考控制参数 （80 ARQC）。第一个 GENERATE AC 中 TVR 的字节 1，位 8 为‘1’（脱机数据认证未执行）。

7.3.314 AQFM141-00 不能联机，脱机接受时，GAC 命令中 CDA 的处理（1）

测试目的：确保终端不能联机，请求 TC 时，终端能够执行第二个 GAC 带 CDA。
终端配置：——支持 CDA；
——有联机能力的脱机终端 或 （仅联机终端 和 支持当不能联机时，正常处理缺省行为码；
——CDA 从不请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，在第二个 GENARATE AC 命令中请求 TC；
——交易不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端完成交易。第二个 GENERATE AC 中请求 TC 带 CDA。第一个 GENERATE AC 中 TVR 的字节 1，位 8 为‘1’（脱机数据认证未执行）。TVR（包含在第二个 GAC 或金融确认报文或批上送数据报文或其他）有：TVR 的字节 1，位 8 为‘0’（脱机数据认证已执行）。

7.3.315 AQFM141-01 不能联机，脱机拒绝时，GAC 命令中 CDA 的处理（1）

测试目的：确保终端不能联机，请求 AAC 时，终端能够执行第二个 GAC 不带 CDA。

终端配置：——支持 CDA；
——有联机能力的脱机终端 或 （仅联机终端 和 支持当不能联机时，正常处理缺省行为码 ）；
——CDA 从不请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，在第二个 GENARATE AC 命令中请求 AAC；
——交易不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端完成交易。第二个 GENERATE AC 中请求不带 CDA。第一个 GENERATE AC 中 TVR 的字节 1，位 8 为‘1’（脱机数据认证未执行）。TVR（包含在第二个 GAC 或金融确认报文或批上送数据报文或其他）有：TVR 的字节 1，位 8 为‘0’（脱机数据认证已执行）。

7.3.316 AQFM141-02 不能联机，脱机接受时，GAC 命令中 CDA 的处理（2）

测试目的：确保终端不能联机，请求 TC 时，终端能够执行第二个 GAC 带 CDA。

终端配置：——支持 CDA；
——有联机能力的脱机终端 或 （仅联机终端 和当不能联机时，正常处理缺省行为码）；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，在第二个 GENARATE AC 命令中请求 TC；
——交易不能联机；
——TAC/IAC 缺省 B1b8=1,其他位全填 0。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端完成交易。第二个 GENERATE AC 中请求 TC 带 CDA。第一个 GENERATE AC 中 TVR 的字节 1，位 8 =‘1’（脱机数据认证未执行）。TVR（包含在第二个 GAC 或金融确认报文或批上送数据报文或其他）有：TVR 的字节 1，位 8 为‘0’（脱机数据认证已执行）。TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行），在通过成功完成 TC 在第二个 GAC 和金融确认报文或批上送数据报文。

7.3.317 AQFM141-03 不能联机，脱机拒绝时，GAC 命令中 CDA 的处理（2）

测试目的：确保终端不能联机，请求 AAC 时，终端能够执行第二个 GAC 带 CDA。

终端配置：——支持 CDA；
——有联机能力的脱机终端 或 （仅联机终端 和 支持当不能联机时，正常处理缺省行为码 ）；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；

——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，在第二个 GENARATE AC 命令中请求 AAC；
——交易不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端完成交易。终端第二个 GENERATE AC 中请求不带 CDA。TVR 的字节 1，位 8 为‘0’（脱机数据认证已执行）包含在金融确认报文或批上送数据报文（假如终端有能力存储拒绝交易）。

7.3.318 AQFM142-00 联机不请求 CDA 的终端，2nd GAC 不应请求 CDA

测试目的：联机不请求 CDA 的终端，成功地联机接受 2nd GAC 不应请求 CDA。

终端配置：——支持 CDA；
——有联机能力的脱机终端 或 仅联机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC 时；
——CDA 从不请求，在第二个 GAC 请求 TC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，在第二个 GENARATE AC 命令中请求 TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端完成交易。终端第二个 GENERATE AC 中请求不带 CDA。第一个 GENERATE AC 中 TVR 的字节 1，位 8 为‘1’（脱机数据认证未执行）。TVR（包含在第二个 GAC 或金融确认报文或批上送数据报文或其他）有：TVR 的字节 1，位 8 为‘0’（脱机数据认证已执行）。

7.3.319 AQFM143-00 执行 CDA 时，格式 1 返回 TC 或 ARQC

测试目的：确保终端能够使用卡以格式 1 的返回，不带 CDA 但 AIP 支持 CDA。

终端配置：——支持 CDA；
——有联机能力的脱机终端 或 仅联机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC 时。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——卡以格式 1 返回 GAC 不带 CDA；
——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，不请求 CDA；
——卡在第一个 GAC 响应 ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端通过一个 TC 或 AAC 来完成交易。终端应该接受格式 1 的响应。

7.3.320 AQFM144-00 超长数据作为静态签名数据的哈希输入 SDA

测试目的：确保终端能够正确地执行 SDA，如果超长数据作为静态签名数据的哈希输入 SDA。

终端配置：支持 SDA。

卡片配置：——卡中的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——NI 长度=247 字节，NCA 长度=248 字节；
——发卡行公钥指数为 3；
——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充 00，直到最大的记录长度（在 70 模版中为 252 字节），其他的文件（SFI 的 1 到 10）包含 3 个签名记录，一个 127 字节长（私有标签和单字节长度），一个 127 字节长（私有标签和双字节长度）和一个最大记录长度（在 70 模版中为 252 字节），签名卡中的所有允许的记录中的所有文件（部分数据如 AFL，发卡行证书和不能包含 SSAD），建立正确的 AFL 应该包

含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是 SDA）。

通过标准：终端通过一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（SDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘0’（脱机数据认证已执行）。

7.3.321 AQFM144-01 超长数据作为 IC 卡公钥证书的哈希输入 DDA

测试目的：确保终端能够正确地执行 DDA，如果超长数据作为 IC 卡公钥证书的哈希输入 DDA。

终端配置：支持 DDA。

卡片配置：——卡中的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；

——NIC 长度=247 字节,NI 长度=247 字节，NCA 长度=248 字节；

——发卡行公钥指数为 3；

——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充 00，直到最大的记录长度（在 70 模版中为 252 字节），其他的文件（SFI 的 1 到 10）包含 3 个签名记录，一个 127 字节长（私有标签和单字节长度），一个 127 字节长（私有标签和双字节长度）和一个最大记录长度（在 70 模版中为 252 字节），签名卡中的所有允许的记录中的所有文件（部分数据如 AFL，发卡行证书和不能包含 SSAD），建立正确的 AFL 应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是 DDA）。

通过标准：终端通过一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.3.322 AQFM144-02 超长数据作为 IC 卡公钥证书的哈希输入 CDA（1）

测试目的：确保终端能够正确地执行 CDA，如果超长数据作为 IC 卡公钥证书的哈希输入 CDA。

终端配置：——支持 CDA；

——仅脱机终端或有联机能力的脱机终端。

卡片配置：——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 TC；

——卡在第一个 GAC 返回 TC；

——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；

——NIC 长度=238 字节,NI 长度=247 字节，NCA 长度=248 字节；

——IC 卡公钥指数为 3。

——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充 00，直到最大的记录长度（在 70 模版中为 252 字节），其他的文件（SFI 的 1 到 10）包含 3 个签名记录，一个 127 字节长（私有标签和单字节长度），一个 127 字节长（私有标签和双字节长度）和一个最大记录长度（在 70 模版中为 252 字节），签名卡中的所有允许的记录中的所有文件（部分数据如 AFL，发卡行证书和不能包含 SSAD），建立正确的 AFL 应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是 CDA）。

通过标准：终端通过一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，

位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.3.323 AQFM144-03 超长数据作为 IC 卡公钥证书的哈希输入 CDA（2）

测试目的：确保终端能够正确地执行 CDA，如果超长数据作为 IC 卡公钥证书的哈希输入 CDA。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，第二个 GENERATE AC 命令请求 TC；
——卡在第一个 GAC 返回 ARQC；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——NIC 长度=238 字节，NI 长度=247 字节，NCA 长度=248 字节；
——IC 卡公钥指数为 3；
——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充 00，直到最大的记录长度（在 70 模版中为 252 字节），其他的文件（SFI 的 1 到 10）包含 3 个签名记录，一个 127 字节长（私有标签和单字节长度），一个 127 字节长（私有标签和双字节长度）和一个最大记录长度（在 70 模版中为 252 字节），签名卡中的所有允许的记录中的所有文件（部分数据如 AFL，发卡行证书和不能包含 SSAD），建立正确的 AFL 应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是 CDA）。

通过标准：终端通过一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.3.324 AQFM144-04 超长数据作为 IC 卡公钥证书的哈希输入 CDA（3）

测试目的：确保终端能够正确地执行 CDA，如果超长数据作为 IC 卡公钥证书的哈希输入 CDA。

终端配置：——支持 CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC，在第二个 GENARATE AC 命令中请求 TC；
——卡在第一个 GAC 返回 ARQC；
——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——NIC 长度=238 字节，NI 长度=247 字节，NCA 长度=248 字节；
——IC 卡公钥指数为 3；
——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充 00，直到最大的记录长度（在 70 模版中为 252 字节），其他的文件（SFI 的 1 到 10）包含 3 个签名记录，一个 127 字节长（私有标签和单字节长度），一个 127 字节长（私有标签和双字节长度）和一个最大记录长度（在 70 模版中为 252 字节），签名卡中的所有允许的记录中的所有文件（部

分数据如 AFL，发卡行证书和不能包含 SSAD)，建立正确的 AFL 应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是 CDA)。

通过标准：终端通过一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA)。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功)。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA)。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.3.325 AQFM144-05 超长数据作为 IC 卡公钥证书的哈希输入 CDA（4）

测试目的：确保终端能够正确地执行 CDA，如果超长数据作为 IC 卡公钥证书的哈希输入 CDA。

终端配置：——支持 CDA

——仅联机终端；

——CDA 总是请求，第一个 GAC 请求 ARQC 时；

——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC, 在第二个 GENARATE AC 命令中请求 TC；

——卡在第一个 GAC 返回 ARQC；

——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’)；

——NIC 长度=238 字节,NI 长度=247 字节，NCA 长度=248 字节；

——IC 卡公钥指数为 3；

——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充 00，直到最大的记录长度（在 70 模版中为 252 字节)，其他的文件（SFI 的 1 到 10）包含 3 个签名记录，一个 127 字节长（私有标签和单字节长度)，一个 127 字节长（私有标签和双字节长度）和一个最大记录长度（在 70 模版中为 252 字节)，签名卡中的所有允许的记录中的所有文件（部分数据如 AFL，发卡行证书和不能包含 SSAD)，建立正确的 AFL 应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是 CDA)。

通过标准：终端通过一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA)。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功)。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’(未使用 DDA)。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.3.326 AQFM144-06 超长数据作为 IC 卡公钥证书的哈希输入 CDA（5）

测试目的：确保终端能够正确地执行 CDA，如果超长数据作为 IC 卡公钥证书的哈希输入 CDA。

终端配置：——支持 CDA；

——仅联机终端或有联机能力的脱机终端；

——CDA 总是请求，在第二个 GAC 请求 TC 时。

卡片配置：——设置 TAC 和 IAC 使终端在第一个 GENARATE AC 命令中请求 ARQC, 在第二个 GENARATE AC 命令中请求 TC；

——卡在第一个 GAC 返回 ARQC；

——卡中的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’)；

——NIC 长度=238 字节,NI 长度=247 字节，NCA 长度=248 字节；

——IC 卡公钥指数为 3；

——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数

据和包含在单独的记录中的签名数据为私有标签，需要填充 00，直到最大的记录长度（在 70 模版中为 252 字节），其他的文件（SFI 的 1 到 10）包含 3 个签名记录，一个 127 字节长（私有标签和单字节长度），一个 127 字节长（私有标签和双字节长度）和一个最大记录长度（在 70 模版中为 252 字节），签名卡中的所有允许的记录中的所有文件（部分数据如 AFL，发卡行证书和不能包含 SSAD），建立正确的 AFL 应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是 CDA）。

通过标准：终端通过一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.3.327 AQFM145-00 终端生成的随机数

测试目的：确保终端每一笔交易生成的随机数都不相同。

终端配置：不支持 DDA。

卡片配置：测试工具将会存储终端已经执行的每一个案例在 CDOL1 中返回的随机数。

测试流程：测试应按照如下规则执行：

a）在不重启终端的情况下，应连续执行 500 个测试脚本（从 YSMLxxx-xx 至 ZHCSxxx-xx，或任意执行了完整借记/贷记交易的测试脚本）；

b）然后终端应切断电源并重新开机；

c）在不重启终端的情况下，应接着连续执行 500 个其它的测试脚本（从 YSMLxxx-xx 至 ZHCSxxx-xx，step1 之外的，或任意执行了完整借记/贷记交易的测试脚本）。

通过标准：对于测试脚本，终端随机数（9F37）的存储应该：不能和先前的随机数重复（包括递增）；不能某一个 bit 固定，例如：第 i 个 bit 不能 1000 次都相同。（1<=i<=32） len(9F37)=4byte*8bits=32bits；平均权重应该在 15 到 17 之间(例如:所用 bit 中 1 的个数(全为 1,bit 的总和为 32000,32bits*1000 笔)应该在 15000 到 17000 之间。

7.3.328 AQFM145-01 终端生成的随机数（2）

测试目的：对于终端支持 DDA，确保终端每一笔交易生成的随机数都不相同。

终端配置：支持 DDA。

卡片配置：——测试工具将会存储终端已经执行的 600 个案例在 CDOL1 中返回的随机数；

——工具将会存储终端执行剩下的 400 个案例在 DDOL 中返回的随机数（对于这 400 个案例在 CDOL1 中返回的随机数将不会存储用于该案例的测试），为了达到 400 个 DDA 案例（仅有 200 个案例专门用于测试 DDA），可能需要选择存在 DDA 的案例，连续测试已达到剩下的 200 次。

测试流程：测试应按照如下规则执行：

a）在不重启终端的情况下，应连续执行 500 个测试脚本（从 YSMLxxx-xx 至 ZHCSxxx-xx，或任意执行了完整借记/贷记交易的测试脚本），300 个随机数来自 CDOL1，200 个来自 DDOL；

b）然后终端应切断电源并重新开机；

c）在不重启终端的情况下，应接着连续执行 500 个其它的测试脚本（从 YSMLxxx-xx 至 ZHCSxxx-xx，或任意执行了完整借记/贷记交易的测试脚本），300 个随机数来自 CDOL1，200 个来自 DDOL。

通过标准：对于测试脚本，终端随机数（9F37）的存储应该：不能和先前的随机数重复（包括递增）；不能某一个 bit 固定，例如：第 i 个 bit 不能 1000 次都相同。（1<=i<=32） len(9F37)=4byte*8bits=32bits；平均权重应该在 15 到 17

之间(例如:所用 bit 中 1 的个数(全为 1,bit 的总和为 32000,32bits*1000 笔)应该在 15000 到 17000 之间。

7.4 数据对象（SJDX）

7.4.1 SJDX001-00 长度域：1 字节

测试目的：确保终端支持长度域是一个字节（位 8 =0）的数据对象。
终端配置：N/A。
卡片配置：卡中包含将被读取的且长度域为一个字节的数据对象（例如 PAN）。
测试流程：选择卡片应用，执行交易。
通过标准：终端将进行交易直至完成为止，并且正确管理其接收到的长度域为 1 个字节的数据对象。

7.4.2 SJDX001-01 长度域：2 字节 （1）

测试目的：确保终端支持长度域是两个字节（81xx）的数据对象。
终端配置：N/A。
卡片配置：卡中含有长度域为两个字节的数据对象。
子类案例：——案例 01：卡中含有 PAN;
——案例 02：卡中含有长度大于 127 字节的发卡行公钥。
测试流程：选择卡片应用，执行交易。
通过标准：终端将进行交易直至完成为止并且正确管理其接收到长度域为 2 字节长度的数据对象。

7.4.3 SJDX001-02 长度域：2 字节（2）

测试目的：确保终端支持长度域是两个字节（81xx）的数据对象。
终端配置：N/A。
子类案例：——案例 01：卡中含有 70 模版，模版长度<128 字节，长度域为 2 个字节，包含原始数据对象，长度<128 字节，长度域为 2 个字节；
——案例 02：卡中含有 70 模版，模版长度〉127 字节，包含原始数据对象，长度<128 字节，长度域为 2 个字节；
——案例 03：卡中含有 70 模版，模版长度〉127 字节，包含原始数据对象，长度〉127 字节。
测试流程：选择卡片应用，执行交易。
通过标准：终端将进行交易直至完成为止并且正确管理其接收到长度域为 2 字节长度的数据对象。

7.4.4 SJDX003-00 在 an 格式的数据对象中“空格”字符的识别

测试目的：确保终端接受 IC 卡中含有“空格”的 an 类型的数据对象。
终端配置：N/A。
卡片配置：——卡将包含以下数据对象而且在每个数据对象中至少存在一个“空格”字符：首选的应用名，应用标签；
——卡中含有发卡行代码索引表。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。如果终端有显示屏并且支持持卡人确认，如果终端支持卡中的发卡行代码索引表，终端应显示带有空格的应用首选名。如果终端有显示屏并且支持持卡人确认，如果不能支持应用首选名，终端将用通用字符集显示带有空格的应用标签。

7.4.5 SJDX003-01 接受选择数据对象格式错误—PSE 选择

测试目的：终端进行 PSE 时，接受 IC 卡中格式错误的应用选择数据对象。

终端配置：支持 PSE。
卡片配置：——卡支持 PSE；
——卡包含下列指定值格式错误的数据对象；
——PSE 的 FCI 包含的首选语言为 ‘23 33’；
——PSE 的 FCI 包含发卡行代码表索引为‘F1’；
——ADF 入口包含应用标签为‘-00 00 00 41 50 50 20 7F 7F 7F’；
——ADF 入口包含应用首选名为‘01 02 03 41 42 43 44 7F 7F 7F’。
测试流程：选择卡片的 PSE，执行交易完成。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.4.6 SJDX003-02 接受选择数据对象格式错误—AID 列表选择

测试目的：终端进行 AID 列表应用选择时，接受 IC 卡中格式错误的应用选择数据对象。
终端配置：N/A。
卡片配置：——卡不含有 PSE；
——终端中包含一个 AID 与卡中的 AID 完全匹配；
子类案例：卡包含下列指定值格式错误的数据对象：
——案例 01：ADF 的 FCI 包含应用标签值为‘-00 00 00 41 50 50 20 7F 7F 7F’；ADF 的 FCI 包含首选语言为 ‘23 33’；ADF 的 FCI 包含发卡行代码表索引为‘F1’；ADF 的 FCI 包含应用首选名为‘01 02 03 41 42 43 44 7F 7F 7F’；
——案例 02：SELECT 命令的响应包含一个格式错误的应用标签，不正确的长度；
——案例 03：SELECT 命令的响应包含一个首选语言为“5F 2D 05 xx xx xx xx yy”，x 的值应该与 ISO 639 一致，yy 为“00”和“FF”之外的值。
测试流程：使用 AID 列表选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.4.7 SJDX003-03 接受选择数据对象格式错误—最终选择

测试目的：终端进行最终选择时，接受 IC 卡中格式错误的应用选择数据对象。
终端配置：N/A。
卡片配置：——卡包含下列指定值格式错误的数据对象；
——最终选择的一个 ADF 的 FCI 包含应用标签为‘-00 00 00 41 50 50 20 7F 7F 7F’；
——最终选择的一个 ADF 的 FCI 包含首选语言为‘23 33’；
——最终选择的一个 ADF 的 FCI 包含发卡行代码表索引为‘F1’；
——最终选择的一个 ADF 的 FCI 入口包含应用首选名为‘01 02 03 41 42 43 44 7F 7F 7F’。
测试流程：用 AID 列表选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.4.8 SJDX003-04 对于 PSE 的 FCI 和 ADF 的 FCI 的不一致选择数据

测试目的：确保如果在应用选择中位于几个地方的数据有不一样的值，终端不终止交易。
终端配置：支持 PSE。
卡片配置：——卡包含 PSE；
——卡在指定的位置包含以下数据对象；
——PSE 的 FCI 包含首选语言=‘65 6E’；
——PSE 的 FCI 包含发卡行代码表索引=‘01’；
——响应最终选择 ADF 的 FCI 包含首选语言=‘66 72’；
——响应最终选择 ADF 的 FCI 包含发卡行代码表索引=‘02’。
测试流程：用 PSE 方式进行应用选择。

通过标准：终端执行 PSE 方式应用选择，通过请求一个 TC 或 AAC 来完成交易。终端可以使用其中任意位置的数据。

7.4.9 SJDX003-05 在 AID 列表和最终选择 ADF 之间的不一致选择数据

测试目的：确保如果在应用选择中位于几个地方的数据有不一样的值，终端不终止交易。

终端配置：N/A。

卡片配置：——卡不包含 PSE；

——卡中包含 2 个终端支持的 ADF；

——卡在一个给定的位置，将包含以下数据对象；

——ADF1：ADF 的 FCI 包含应用标签为‘45 4D 56 43 4F 30 30 31’；ADF 的 FCI 包含应用首选名为‘45 4D 56 43 4F 30 30 31 54 45 53 54’；ADF 的 FCI 包含首选语言为‘65 6E’；ADF 的 FCI 包含发卡行代码表索引为‘01’；

——ADF2：ADF 的 FCI 包含应用标签为‘45 4D 56 43 4F 30 30 31’；ADF 的 FCI 包含应用首选名为‘45 4D 56 43 4F 30 30 31 54 45 53 54’；ADF 的 FCI 包含首选语言为‘65 6E’；

——响应最终 SELECT ADF 的 FCI 包含首选语言=‘66 72’；

——响应最终 SELECT ADF 的 FCI 包含发卡行代码表索引=‘02’。

测试流程：用 AID 列表方式进行应用选择。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。终端可以使用其中任意位置的数据。

7.4.10 SJDX003-06 数据不一致：在 PSE 或者最终选择中仅有一次出现

测试目的：确保如果卡片中应该在两个地方都存在数据对象，仅在一种情况下出现（在 PSE 或者最终选择里）的，终端不终止交易。

终端配置：支持 PSE。

卡片配置：卡支持 PSE。

子类案例：——案例 01：PSE 的 FCI：不存在首选语言和发卡行代码表索引。响应最终 SELECT ADF 的 FCI 包含：首选语言=‘65 6E’和发卡行代码表索引=‘01’；

——案例 02：PSE 的 FCI 包含：首选语言=‘65 6E’和发卡行代码表索引=‘01’。响应最终 SELECT ADF 的 FCI：不存在首选语言和发卡行代码表索引。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.4.11 SJDX003-07 数据不一致：在 SELECT ADF 或者最终选择中仅有一次出现

测试目的：确保如果卡片中应该在两个地方都存在数据对象，仅在一种情况下出现（在 ADF 或者最终选择里）的，终端不终止交易。

终端配置：N/A。

卡片配置：卡不支持 PSE。

子类案例：——案例 01：ADF 的 FCI 不包含：应用标签、应用首选名、首选语言和发卡行代码表索引。响应最终 SELECT ADF 的 FCI 包含：应用标签=‘45 4D 56 43 4F 30 30 31’，应用首选名=‘45 4D 56 43 4F 30 30 31 54 45 53 54’，首选语言=‘65 6E’和发卡行代码表索引=‘01’；

——案例 02：ADF 的 FCI：应用标签=’45 4D 56 43 4F 30 30 31’，应用首选名=‘45 4D 56 43 4F 30 30 31 54 45 53 54’，首选语言=‘65 6E’和发卡行代码表索引=‘01’。响应最终 SELECT 的 ADF 的 FCI 不包含：应用标签、应用首选名、首选语言和发卡行代码表索引。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.4.12 SJDX003-08 AID 列表选择格式错误

测试目的：确保终端在进行 AID 列表选择时，发现 IC 卡片返回的重要数据对象的格式错误时，继续处理交易。

终端配置：N/A。

卡片配置：——卡不含有 PSE；
——终端中包含至少两个 AID 与卡中的 AID 完全匹配；
——卡包含下列指定值格式错误的数据对象。

子类案例：——案例 01：卡片对与终端完全匹配的两个 AID 中的一个，返回的 SELECT 响应包含格式错误的 FCI 模版，无法正确解析；
——案例 02：卡片对与终端完全匹配的两个 AID 中的一个，返回的 SELECT 响应 DF 名长于 16 个字节；
——案例 03：卡片对与终端完全匹配的两个 AID 中的一个，返回的 SELECT 响应包含格式错误的 FCI 专用模版，无法正确解析；
——案例 04：卡片对与终端完全匹配的两个 AID 中的一个，返回的 SELECT 响应应用优先指示位多于 1 个字节；
——案例 05：卡片对与终端完全匹配的两个 AID 中的一个，返回的 SELECT 响应 PDOL 重复；
——案例 06：卡片对与终端完全匹配的两个 AID 中的一个，返回的 SELECT 响应包含格式错误的发卡行自定义数据(FCI),无法正确解析。

测试流程：使用 AID 列表选择卡片应用，执行交易。

通过标准：AID/DF 名格式错误的不加入候选列表。终端应通过请求一个 TC 或 AAC 来完成交易。

7.4.13 SJDX003-09 接受选择 IC 卡返回的格式错误

测试目的：确保终端在进行应用选择时，能够接受选择 IC 卡返回的格式错误。

终端配置：N/A。

卡片配置：——终端中包含至少 1 个 AID 与卡中的 AID 完全匹配；
——卡包含下列指定值格式错误的数据对象。

子类案例：——案例 01：模版 FCI 响应包含的应用首选名称的长度=1（值也为 1 字节）且非 ans 格式；
——案例 02：模版 FCI 响应包含的应用首选名称的长度=17（值也为 17 字节）。

测试流程：使用 AID 列表选择卡片应用，执行交易。

通过标准：终端应通过请求一个 TC 来完成交易。

7.5 认可的加密算法（JMSF）

7.5.1 JMSF001-00 CA，发卡行和 IC 卡的公钥长度之间的关系（1）

测试目的：确保如果终端支持静态数据认证，应支持发卡行公钥模不大于 CA 公钥模（$N_I<=N_{CA}$）。

终端配置：支持 SDA。

卡片配置：卡中的 AIP 指明支持静态数据认证（AIP 的字节 1，位 7 为‘1’）。

子类案例：——案例 01：当 $N_I<N_{CA}$ 时，卡中的静态签名有效；
——案例 02：当 $N_I=N_{CA}$ 时，卡中的静态签名有效。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（SDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位

4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.5.2 JMSF001-01 CA，发卡行和 IC 卡的公钥长度之间的关系（2）

测试目的：确保如果终端支持动态数据认证，应支持长度为 N_{IC} <=N_I <=N_{CA}-的公钥模。
终端配置：支持 DDA。
卡片配置：卡中的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）。
子类案例：——案例 01：当 N_{IC}<N_I<N_{CA} 时，卡中的动态签名有效；
——案例 02：当 N_{IC} =N_I =N_{CA} 时，卡中的动态签名有效。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.5.3 JMSF001-02 CA，发卡行和 IC 卡的公钥长度之间的关系（3）

测试目的：确保如果终端支持 CDA，应支持长度为 N_{IC} <=N_I <=N_{CA}-公钥模。
终端配置：支持 CDA。
卡片配置：卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）。
子类案例：——案例 01：当 N_{IC}<N_I<N_{CA} 时，卡中的动态签名有效；
——案例 02：当 N_{IC} =N_I =N_{CA} 时，卡中的动态签名有效。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。在金融确认信息中或者批数据获取的信息中 TVR 的第 1 个字节的 3 位为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。在金融确认信息中或者批数据获取的信息中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）（该通过标准仅用于 CDA 被请求）。

7.5.4 JMSF003-00 模大小的上限（1）

测试目的：确保如果终端支持静态数据认证，应支持如下定义的最大公钥模长度：N_I 的最大长度是 248 字节；N_{CA} 的最大长度是 248 字节。
终端配置：支持 SDA。
卡片配置：——卡中的 AIP 指明支持静态数据认证（AIP 的字节 1，位 7 为‘1’）；
——N_I 长度 =248 字节，N_{CA} 长度=248 字节；
——卡中的静态签名有效。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（SDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.5.5 JMSF003-01 模大小的上限（2）

测试目的：确保如果终端支持动态数据认证，应支持如下定义的最大公钥模长度：N_{IC} 的最大长度是 247 字节；N_I 的最大长度是 247 字节；N_{CA} 的最大长度是 248 字节。
终端配置：支持 DDA。
卡片配置：——卡中的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；

——N_{IC}长度=247 字节，N_I长度=247 字节，N_{CA}长度=248 字节；
——卡计算的动态签名有效。

子类案例：——案例 01：内部认证响应域为格式 1；
——案例 02：内部认证响应域为格式 2。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.5.6 JMSF003-02 模大小的上限（3）

测试目的：确保如果终端支持复合动态数据认证，应支持如下定义的最大公钥模长度：N_{IC}的最大长度是 238 字节；N_I的最大长度是 247 字节；N_{CA}的最大长度是 248 字节。

终端配置：支持 CDA。

卡片配置：——卡中的 AIP 指明支持复合动态数据认证（AIP 的字节 1，位 1 为‘1’）；
——N_{IC}长度=238 字节，N_I长度=247 字节，N_{CA}长度=248 字节；
——卡计算的动态签名有效，并且卡以格式 2 响应 GENERATE AC 且不存在 IAD。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个 TC 来完成交易。在金融确认信息或批数据获取信息中 TVR 的字节 1，位 3 为‘0’（CDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。在金融确认信息或批数据获取信息中 TSI 的字节 1,位 8 为‘1’（脱机数据认证已执行）（该通过标准仅用于 CDA 被请求）。

7.6 金融交易接口文件（JKWJ）

7.6.1 JKWJ001-00 READ RECORD：SFI 从 1 到 10

测试目的：确保终端用 READ RECORD 命令可以读取 SFI 是 1 到 10（0X01 到 0X0A）的文件里的数据。

终端配置：N/A。

子类案例：——案例 01：PAN 位于 SFI 为 01 的文件里；
——案例 02：PAN 位于 SFI 为 02 的文件里；
——案例 03：PAN 位于 SFI 为 03 的文件里；
——案例 04：PAN 位于 SFI 为 04 的文件里；
——案例 05：PAN 位于 SFI 为 05 的文件里；
——案例 06：PAN 位于 SFI 为 06 的文件里；
——案例 07：PAN 位于 SFI 为 07 的文件里；
——案例 08：PAN 位于 SFI 为 08 的文件里；
——案例 09：PAN 位于 SFI 为 09 的文件里；
——案例 10：PAN 位于 SFI 为 10 的文件里。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.2 JKWJ002-00 READ RECORD：线性文件

测试目的：确保终端可以用 READ RECORD 读取线性结构文件中的数据以及固定和可变长度的记录。

终端配置：N/A。

卡片配置：——一个必备的数据元（例如：PAN）位于线性结构文件和固定长度记录里；
——另一个必备的数据元（例如：失效日期）位于线性结构文件和可变长度的记录里。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.3 JKWJ003-00 READ RECORD：含有多个记录的文件

测试目的：确保终端可以用 READ RECORD 读取含有多个记录的文件中的数据。
终端配置：N/A。
卡片配置：——一个必备的数据元（例如：PAN）位于文件的第一条记录中；
——另一个必备的数据元（例如：失效日期）位于相同文件的第二条记录中；
——另一个必备的数据元（例如：CDOL1 和 CDOL2）位于相同文件的第三条记录中。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.4 JKWJ004-00 READ RECORD：记录长从 1 到 254 字节

测试目的：确保终端可以用 READ RECORD 读取记录长从 1 到 254 字节的文件中的数据。
终端配置：N/A。
卡片配置：——一个单独记录中仅含有模板和等于 00 的长度（70 00）；
——一个具有“平均长度”的数据元位于一个单独的记录里（例如：签名静态应用数据或者 CDOL1）；
——一个具有最大长度（包括标签、长度和模板的总长度是 254）的数据元位于一个单独的记录里（例如：CDOL1）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.5 JKWJ005-00 记录数据格式

测试目的：确保终端可以解析从记录中读取的模板为 70 的数据。
终端配置：N/A。
卡片配置：必备数据元（PAN， 失效日期， CDOL1 和 CDOL2）位于一个记录的模板 0X70 里。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.6 JKWJ007-00 使用 READ RECORD 命令访问无条件限制的文件

测试目的：确保终端可以用 READ RECORD 命令访问文件。
终端配置：N/A。
卡片配置：必备数据元位于使用 READ RECOED 能访问的文件里。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.7 JKWJ009-00 必备数据对象：应用失效日期

测试目的：确保终端检查在卡中存在可以使用的必备数据对象应用失效日期。
终端配置：N/A。
卡片配置：卡中存在应用失效日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.8 JKWJ010-00 必备数据对象：PAN

测试目的：确保终端检查在卡中存在可以使用的必备数据对象 PAN。
终端配置：N/A。
卡片配置：卡中存在 PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.9 JKWJ010-01 必备数据对象长度：PAN

测试目的：确保终端接受不同长度最大至 19 位的 PAN。
终端配置：N/A。
卡片配置：CDOL1 请求 PAN。
子类案例：根据 PAN 的长度变化将进行 10 个测试：
——案例 01：卡包含长度为 5 个字节（CN 10）的 PAN；
——案例 02：卡包含长度为 6 个字节（CN 11）的 PAN；
——案例 03：卡包含长度为 6 个字节（CN 12）的 PAN；
——案例 04：卡包含长度为 7 个字节（CN 13）的 PAN；
——案例 05：卡包含长度为 7 个字节（CN 14）的 PAN；
——案例 06：卡包含长度为 8 个字节（CN 15）的 PAN；
——案例 07：卡包含长度为 8 个字节（CN 16）的 PAN；
——案例 08：卡包含长度为 9 个字节（CN 17）的 PAN；
——案例 09：卡包含长度为 9 个字节（CN 18）的 PAN；
——案例 10：卡包含长度为 10 个字节（CN 19）的 PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。
第一个 GENERATE AC 将含有从卡中读取的 PAN。

7.6.10 JKWJ011-00 数据对象的填充：2 磁道等价数据

测试目的：确保终端接受最大为 19 字节（需要时，以‘F’填充）的长度变化的 2 磁道等价数据。
终端配置：N/A。
卡片配置：CDOL1 请求 2 磁道等价数据；
子类案例：对于 2 磁道等价数据的不同长度将进行 3 个测试：
——案例 01：卡含有 15 字节长的 2 磁道等价数据，使用了 14-5 个字节，最后的用‘F’填充；
——案例 02：卡含有 16 字节长的 2 磁道等价数据，使用了所有字节，没有进行填充；
——案例 03：卡含有 19 字节长的 2 磁道等价数据，使用了 18-5 个字节，最后的用‘F’填充。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 将含有从卡中读取的 2 磁道等价数据。

7.6.11 JKWJ013-00 可选数据对象

测试目的：终端接受存在和不存在的可选数据对象。
终端配置：N/A。
卡片配置：——测试卡片所有的可选数据对象是否存在，可通过 READ RECORD 读取（卡片可选数据对象参见 JR/T0025.5—2013 附录 A）；
——对必备数据对象的存在不进行测试；
子类案例：对含有自定义数据对象的私有模板（例如 FCI 模板）进行测试：
——案例 01：不存在可选数据对象；
——案例 02：所有可选数据对象存在；

测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.6.12 JKWJ014-00 用于脱机静态数据认证的必备数据对象（1）

测试目的：终端确保用于脱机静态数据认证（如果支持）的必备数据对象在卡中的存在，并且能使用这些对象。
终端配置：支持 SDA。
卡片配置：——卡中的 AIP 指明支持静态数据认证（AIP 的字节 1，位 7 为‘1’）；
——卡中存在 CA 公钥索引；
——卡中存在发卡行公钥证书；
——卡中存在签名的静态应用数据；
——卡中存在发卡行公钥余项（用在这个案例中的发卡行公钥允许发卡行公钥余项的存在）；
——卡中存在发卡行公钥指数。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（静态数据认证成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 6 为‘0’（无 IC 卡数据缺失）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.6.13 JKWJ015-00 用于脱机动态数据认证的必备数据对象（2）

测试目的：终端确保用于脱机动态数据认证（如果支持）的必备数据对象在卡中的存在，并且能使用这些对象。
终端配置：支持 DDA。
卡片配置：——卡中的 AIP 指明支持动态数据认证（AIP 的字节 1，位 6 为‘1’）；
——卡中存在 CA 公钥索引；
——卡中存在发卡行公钥证书；
——卡中存在发卡行公钥余项（本案例中满足发卡行公钥余项存在的条件）；
——卡中存在发卡行公钥指数；
——卡中存在 IC 卡公钥证书；
——卡中存在 IC 卡公钥余项（本案例中满足 IC 卡公钥余项存在的条件）；
——卡中存在 IC 卡公钥指数；
——卡中存在 DDOL。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（DDA 成功）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 6 为‘0’（无 IC 卡数据缺失）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘1’（脱机数据认证已执行）。

7.6.14 JKWJ017-00 GET DATA （PIN 重试次数）

测试目的：确保终端能够用 GET DATA 命令获取 PIN 重试次数。
终端配置：支持 GET DATA 获取 PIN 重试次数和脱机明文 PIN 校验。
卡片配置：——卡中的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——卡中的 CVM 是‘明文 PIN，总是’（01 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。卡在收到 VERIFY 命令之前应收

到一个 GET DATA 命令（80 CA 9F 17 00）。

7.6.15 JKWJ020-00 IC 卡中不存在 LCOL 或者 UCOL 数据对象

测试目的：确保卡中不存在 LCOL 或者 UCOL 时，终端放弃频度检查。
终端配置：支持频度检查。
卡片配置：卡中的 AIP 指明支持终端风险管理（AIP 的字节 1，位 4 为‘1’）。
子类案例：——案例 01：卡中不存在连续脱机交易下限；
——案例 02：卡中不存在连续脱机交易上限。
测试流程：选择卡片应用，执行交易。
通过标准：终端放弃频度检查，终端应通过请求一个 TC 或 AAC 来完成交易。卡不应收到获取 ATC 的 GET DATA 命令（80 CA 9F 36 00）。卡不应收到获取 LOATC 的 GET DATA 命令（80 CA 9F 13 00）。

7.6.16 JKWJ021-00 由 GET PROCESSING OPTIONS 命令获取的数据

测试目的：确保终端用 GET PROCESSING OPTIONS 命令能够获取并且正确识别 AFL 和 AIP。
终端配置：N/A。
卡片配置：——卡中存在 AFL 和 AIP；
——AIP 指明支持 SDA（AIP 的字节 1，位 7 为 1）；
——AIP 指明支持 DDA（AIP 的字节 1，位 6 为 1）；
——AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为 1）；
——AIP 指明支持发卡行认证（AIP 的字节 1，位 3 为 1）；
——AIP 指明支持 CDA（AIP 的字节 1，位 1 为 1）；
——联机响应报文中包含发卡行认证数据；
——卡片收到 EXTERNAL AUTHENTICATE 命令后响应状态码 9000 没有数据域；
——如果终端有联机能力，发卡行认证将通过 CDOL2 来完成。
测试流程：选择卡片应用，执行交易。
通过标准：终端将进行交易直到完成。卡应收到一个 GET PROCESSING OPTIONS 命令。卡应收到一系列的 READ RECORD，命令中的 P1、P2 与 AFL 中定义的文件和记录一致。在第一个 GENERATE AC 和第二个 GENERATE AC 卡收到的 TVR，TSI 和命令应反映出在 AIP 中指明支持的功能（脱机数据认证，持卡人确认，终端风险管理和发卡行认证）和终端配置项。

7.6.17 JKWJ023-00 在 AIP 中没有指定的功能：脱机静态数据认证

测试目的：确保如果 AIP 中指明不支持脱机静态数据认证，终端将不执行脱机静态数据认证。
终端配置：支持 SDA。
卡片配置：——卡中的 AIP 指明不支持静态数据认证（AIP 的字节 1，位 7 为‘0’）；
——卡中的 AIP 指明不支持动态数据认证（AIP 的字节 1，位 6 为‘0’）；
——卡中的 AIP 指明不支持复合动态数据认证（AIP 的字节 1，位 1 为‘0’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 8 =‘1’（脱机数据认证未执行）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘0’（脱机数据认证未进行）。

7.6.18 JKWJ025-00 在 AIP 中没有指定的功能：DDA

测试目的：确保如果 AIP 中指明不支持脱机动态数据认证，终端将不进行脱机动态数据认证。
终端配置：支持 DDA。

卡片配置：——卡中的 AIP 指明不支持静态数据认证（AIP 的字节 1，位 7 为‘0’）；
——卡中的 AIP 指明不支持动态数据认证（AIP 的字节 1，位 6 为‘0’）；
——卡中的 AIP 指明不支持复合动态数据认证（AIP 的字节 1，位 1 为‘0’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的字节 1，位 8 为‘1’（脱机数据认证未执行）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 3 为‘0’（未使用 CDA）。第一个 GENERATE AC 命令中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 命令中 TSI 的字节 1，位 8 为‘0’（脱机数据认证未执行）。

7.6.19 JKWJ027-00 在 AIP 中没有指定的功能：持卡人认证

测试目的：确保如果 AIP 中指明不支持持卡人认证，终端将不执行持卡人认证。
终端配置：N/A。
卡片配置：——卡中的 AIP 指明不支持持卡人认证（AIP 的字节 1，位 5 为‘0’）；
——卡中存在 CVM 列表且指明‘CVM 失败，总是’（-00 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 命令中 TVR 的第 3 个字节的第 8 位为‘0’（持卡人认证成功）。在第一个 GENERATE AC 命令中 TSI 的字节 1，位 7 为‘0’（未执行持卡人认证）。CVM 结果=（3F 00 00），没有 CVM 执行。

7.6.20 JKWJ028-00 在 AIP 中指定的功能：终端风险管理

测试目的：确保如果 AIP 中指明支持终端风险管理，终端应进行风险管理。
终端配置：支持（“频度检查”或 “最低限额检查”）或“随机选择检查”。
卡片配置：卡中的 AIP 指明支持 TRM （AIP 的字节 1，位 4 为‘1’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端将处理交易直到完成。第一个 GENERATE AC 命令中 TSI 的字节 1，位 4 为‘1’（已执行终端风险管理）。

7.6.21 JKWJ028-01 在 AIP 中指定的功能：终端风险管理（2）

测试目的：确保如果 AIP 中指明不支持终端风险管理，终端应进行风险管理。
终端配置：支持（“频度检查”或 “最低限额检查”）或“随机选择检查”。
卡片配置：卡中的 AIP 指明支持 TRM （AIP 的字节 1，位 4 为‘0’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端将处理交易直到完成。第一个 GENERATE AC 命令中 TSI 的字节 1，位 4 为‘1’（已执行终端风险管理）。

7.6.22 JKWJ031-00 在 AIP 中没有指定的功能：发卡行认证

测试目的：确保如果 AIP 中指明不支持发卡行认证，终端不进行发卡行认证。
终端配置：支持（仅联机终端或有联机能力的脱机终端）。
卡片配置：——卡片返回的 AIP 指明不支持发卡行认证（AIP 的字节 1，位 3 为‘0’）；
——设置卡参数使得交易联机进行；
——在授权响应信息中收到发卡行认证数据。
测试流程：选择卡片应用，执行交易。
通过标准：终端应完成交易。第一个 GENERATE AC 后，卡不应收到 EXTERNAL AUTHENTICATE 命令。第二个 GENERATE AC 中收到 TSI 的字节 1，位 5 为‘0’（发卡行认证未进行）。

7.6.23 JKWJ034-00 在 AIP 中没有指定的功能：CDA

测试目的：确保如果 AIP 中指明不支持 CDA，终端不进行 CDA。

终端配置：支持 CDA。

卡片配置：——卡中的 AIP 指明不支持 CDA（AIP 的第 1 个字节的第 1 位为‘0’）；
——卡中的 AIP 指明不支持动态数据认证（AIP 的字节 1，位 6 为‘0’）；
——卡中的 AIP 指明不支持静态数据认证（AIP 的字节 1，位 7 为‘0’）；
——卡响应 TC。

测试流程：选择卡片应用，执行交易。

通过标准：在第一个 GENERATE AC 命令中终端不请求 CDA。终端应通过请求一个 TC 来完成交易。 第一个 GENERATE AC 中 TVR 的字节 1，位 7 为‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 为‘0’（未使用 DDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 8 为‘1’（脱机数据认证未执行）。第一个 GENERATE AC 中 TSI 的字节 1，位 8 为‘0’（脱机数据认证未执行）。

7.6.24 JKWJ035-00 记录数据格式：终端忽略 SFI 为 1 至 30 的私有数据

测试目的：确保终端不会终止交易，忽略相关 AFL 中 SFI 为 1 至 30 的私有数据在文件中的存在。

终端配置：N/A。

卡片配置：——终端在第一个 GAC 请求一个 TC 或 ARQC；
——卡返回 ARQC。

子类案例：——案例 01：私有数据（9F 7E）存储在 70 模版 SFI2 的文件中，AFL 涉及到这个文件，这个数据没有被签名；
——案例 02：私有数据（9F 7E）存储在 70 模版 SFI12 的文件中，AFL 涉及到这个文件，这个数据没有被签名；
——案例 03：私有数据（9F 7E）存储在 70 模版 SFI22 的文件中，AFL 涉及到这个文件，这个数据没有被签名。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个 TC 来完成交易。

7.7 交易过程中使用的功能（SYGN）

7.7.1 SYGN002-00 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。

终端配置：N/A。

卡片配置：——第一个交易应将 TVR 如下位置位： 字节 2 位 8 位 4（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功，未知的 CVM）；TSI 如下位置位：字节 1 bit7 位 6（持卡人验证执行，卡片风险管理执行）；
——第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。

通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.2 SYGN002-01 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。

终端配置：支持 SDA。

子类案例：——案例 01：第一个交易应将 TVR 如下位置位： 字节 1 位 7（SDA 失败），字节 2 位 8 位 5（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功，未知的 CVM）；TSI 如下位置位：字节 1 位 8 位 6（脱机数据认证执行，持卡人验证执行，卡片风险管理执行）；第二

个交易 PDOL 请求 TVR 和 TSI。

——案例 02：第一个交易应将 TVR 如下位置位：字节 1 位 8（脱机数据认证未执行）；第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。

通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.3 SYGN002-02 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。

终端配置：支持异常文件。

卡片配置：——第一个交易应将 TVR 如下位置位： 字节 1 位 5（卡片出现在异常文件中），字节 2 位 8 位 4（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功，未知的 CVM）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行）；

——第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。

通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.4 SYGN002-03 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。

终端配置：支持 DDA。

子类案例：——案例 01：第一个交易应将 TVR 如下位置位： 字节 1 位 4（DDA 失败），字节 2 位 8 位 5（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功，未知的 CVM）；TSI 如下位置位：字节 1 位 8 位 6（脱机数据认证执行，持卡人验证执行，卡片风险管理执行）；第二个交易 PDOL 请求 TVR 和 TSI；

——案例 02：第一个交易应将 TVR 如下位置位：字节 1 位 8（脱机数据认证未执行）；第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。

通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.5 SYGN002-04 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。

终端配置：支持 CDA。

子类案例：——案例 01：第一个交易应将 TVR 如下位置位： 字节 1 位 3（CDA 失败），字节 2 位 8 位 5（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功，未知的 CVM）；TSI 如下位置位：字节 1 位 8 位 6（脱机数据认证执行，持卡人验证执行，卡片风险管理执行）；第二个交易 PDOL 请求 TVR 和 TSI。

——案例 02：第一个交易应将 TVR 如下位置位：字节 1 位 8（脱机数据认证未执行）；第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。

通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.6 SYGN002-05 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。
终端配置：支持脱机明文 PIN。
卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 5（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8、位 6（持卡人验证不成功，PIN 尝试次数超限）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行）；
——第二个交易 PDOL 请求 TVR 和 TSI。
测试流程：选择卡片应用，执行交易。
通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.7 SYGN002-06 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。
终端配置：不支持脱机明文 PIN。
卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 5（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8、位 5（持卡人验证不成功，需要输入 PIN 但 PIN pad 不存在或工作不正常）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行）；
——第二个交易 PDOL 请求 TVR 和 TSI。
测试流程：选择卡片应用，执行交易。
通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.8 SYGN002-07 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 5（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8（持卡人验证不成功）,字节 5 位 6 位 5（最终 GENETRATE AC 之前发卡行脚本执行失败，最终 GENETRATE AC 之后发卡行脚本执行失败）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行），字节 1 位 3（发卡行脚本已执行）；
——第二个交易 PDOL 请求 TVR 和 TSI。
测试流程：选择卡片应用，执行交易。
通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.9 SYGN002-08 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 4（ICC 有不同的应用

版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功,未知 CVM）,字节 5 位 7 位 5（发卡行认证失败，最终 GENETRATE AC 之前发卡行脚本执行失败，最终 GENETRATE AC 之后发卡行脚本执行失败）；TSI 如下位置位：字节 1 位 7 位 5（持卡人验证执行，卡片风险管理执行，发卡行认证执行），字节 1 位 3（发卡行脚本已执行）；

——第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。

通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.10 SYGN002-09 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。

终端配置：支持最低限额检查。

卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 4（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7(持卡人验证不成功,未知 CVM),字节 4 位 8(交易超过最低限额）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行），字节 1 位 4（终端风险管理执行）；

——第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。

通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.11 SYGN002-10 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。

终端配置：支持频度检查。

卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 4（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功,未知 CVM）,字节 4 位 7 位 6（超过连续脱机交易下限，超过连续脱机交易上限）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行），字节 1 位 4（终端风险管理执行）；

——第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。

通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.12 SYGN002-11 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。

终端配置：支持随机交易选择。

卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 4（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功,未知 CVM）,字节 4 位 5（交易被随机选择联机处理）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行），字节 1 位 4（终端风险管理执行）；

——第二个交易 PDOL 请求 TVR 和 TSI。

测试流程：选择卡片应用，执行交易。
通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.13 SYGN002-12 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。
终端配置：——终端是有人终端；
——支持强制联机。
卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 4（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功,未知 CVM）,字节 4 位 4（商户强制交易联机）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行），字节 1 位 4（终端风险管理执行）；
——第二个交易 PDOL 请求 TVR 和 TSI。
测试流程：选择卡片应用，执行交易。
通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.14 SYGN002-13 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。
终端配置：支持联机密文 PIN。
卡片配置：——第一个交易应将 TVR 如下位置位：字节 2 位 8 位 5（ICC 有不同的应用版本，过期应用，应用尚未生效，请求的服务不被允许），字节 3 位 8 位 7（持卡人验证不成功,未知 CVM）,字节 3 位 3（输入联机 PIN），字节 5 位 6 位 5（最终 GENETRATE AC 之前发卡行脚本执行失败，最终 GENETRATE AC 之后发卡行脚本执行失败）；TSI 如下位置位：字节 1 位 7 位 6（持卡人验证执行，卡片风险管理执行），字节 1 位 3（发卡行脚本已执行）；
——第二个交易 PDOL 请求 TVR 和 TSI。
测试流程：选择卡片应用，执行交易。
通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.15 SYGN002-14 TSI 和 TVR 的所有位都设置为 0

测试目的：确保当终端开始交易时，TSI和TVR的所有位都设置为0。
终端配置：支持缺省 TDOL。
卡片配置：——第一个交易应将 TVR 如下位置位：字节 5 位 8 位 5（缺省 TDOL 已使用）；
——第二个交易 PDOL 请求 TVR 和 TSI。
测试流程：选择卡片应用，执行交易。
通过标准：在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TSI应被设置为0。在第二个交易中，终端发送的GET PROCESSING OPTIONS中包含的TVR应被设置为0。

7.7.16 SYGN005-00 PDOL 中列出标签的处理规则（1）

测试目的：确保如果在选定ADF的FCI中存在PDOL，并且它包含的数据元没有在JR/T0025.6—2013 8.2表40中定义，或不是终端数据元，终端发送一个GET PROCESSING OPTIONS命令，其PDOL包含一个指定的标签和长度以及值全为十

六进制‘0’的数据元。

终端配置：N/A。

卡片配置：卡在选定ADF的FCI中返回PDOL。

子类案例：——案例01：PDOL请求一个数据元，该数据元在JR/T0025.6—2013 8.2表40中没有定义；

——案例02：PDOL请求一个数据元，该数据元是来自卡片的。

测试流程：选择卡片应用，执行交易。

通过标准：卡应收到一个GET PROCESSING OPTIONS 命令，其数据域包含标签为‘83’的数据对象。在子案例条件下，PDOL的数据元应在模板‘83’中被具有相同长度和值为十六进制‘0’的数据元替代。

7.7.17 SYGN006-00 PDOL 中列出标签的处理规则（2）

测试目的：确保如果在选定ADF的FCI中存在PDOL，并且它包含的数据元是结构数据对象，终端发送一个GET PROCESSING OPTIONS命令，其PDOL包含一个指定的标签和长度以及值全为十六进制‘0’的数据元。

终端配置：N/A。

卡片配置：卡在选定ADF的FCI中返回PDOL，其包含的数据元是结构数据对象。

测试流程：选择卡片应用，执行交易。

通过标准：卡应收到一个GET PROCESSING OPTIONS 命令，数据域包含标签为‘83’的数据对象。PDOL中的结构数据元应在模板‘83’中被具有相同长度和值为十六进制‘0’的数据元替代。

7.7.18 SYGN007-00 PDOL 中列出标签的处理规则（3）

测试目的：确保如果在选定ADF的FCI中存在PDOL，并且它包含终端中不存在的数据元，终端发送一个GET PROCESSING OPTIONS命令，其PDOL包含一个指定的标签和长度以及值全为十六进制‘0’的数据元。

终端配置：N/A。

卡片配置：卡在选定ADF的FCI中返回PDOL，并且PDOL中含有一个终端此时不能提供的数据元：ARC（标签‘8A’）。

测试流程：选择卡片应用，执行交易。

通过标准：卡应收到一个数据域包含标签为‘83’的数据对象的GET PROCESSING OPTIONS命令。PDOL中终端此刻不能提供数据元应在模板‘83’中被具有相同长度和值为十六进制‘0’的数据元替代。

7.7.19 SYGN009-00 READ RECORD 命令的执行

测试目的：确保终端总是在GET PROCESSING OPTIONS命令之后立刻发送READ RECORD命令。

终端配置：N/A。

测试流程：选择卡片应用，执行交易。

通过标准：卡应在GET PROCESSING OPTIONS命令之后紧接着收到一系列的READ RECORD命令。

7.7.20 SYGN010-00 READ RECORD 读取 AFL 指定的每个记录

测试目的：确保终端能够解释AFL并且可以对记录号从开始到截止（包括截止）的每个记录发送READ RECORD命令。

终端配置：N/A。

子类案例：——案例 01：卡中的 AFL 文件 1－记录 1 至 5 记录；

——案例02：卡中的AFL文件1－记录1至5，文件2－记录2至3，文件3－记录3至3；

——案例03：卡中的AFL文件1－记录3至3，文件2－记录2至2，文件5－记录

3至3；
——案例04：卡中的AFL文件2－记录3至5，文件2－记录6至6，文件2－记录1至2；
——案例05：卡中的AFL文件3－记录1至2，文件2－记录2至3，文件1－记录3至3；
——案例06：卡中的AFL文件3－记录1至1。

测试流程：选择卡片应用，执行交易。

通过标准：卡应接收到依据AFL发送的一系列的READ RECORD命令。

7.7.21 SYGN010-01 READ RECORD 读取 AFL 指定的每个记录（2）

测试目的：确保终端能够解释AFL并且可以对记录号从开始到截止（包括截止）的每个记录发送RED RECORD命令。

终端配置：N/A。

子类案例：——案例 01：具有 128 字节长度的 AFL；
——案例02：卡片响应的GET PROCESSING OPTIONS命令是在模版1格式并包含62个文件入口的AFL（248字节长度）。

测试流程：选择卡片应用，执行交易。

通过标准：卡应接收到依据 AFL 发送的一系列 READ RECORD 命令。

7.7.22 SYGN011-00 数据对象的处理

测试目的：确保终端在读取应用数据时能储存所有被读取的数据元。

终端配置：N/A。

卡片配置：CDOL1 请求所有在 AFL 中指定的文件中读取的数据元，CDOL1 和 CDOL2 除外。

子类案例：如下的 AFL 组合将被测试：
——案例 01：卡中的 AFL 文件 1－记录 1 至 5；
——案例 02：卡中的 AFL 文件 1－记录 1 至 5，文件 2－记录 2 至 3，文件 3－记录 3 至 3；
——案例 03：卡中的 AFL 文件 1－记录 3 至 3，文件 2－记录 2 至 2，文件 5－记录 3 至 3。

测试流程：选择卡片应用，执行交易。

通过标准：卡应在GENERATE AC的数据域中收到终端在读取应用数据时储存的数值正确的数据元。

7.7.23 SYGN012-00 数据对象的处理（不可识别的数据对象）

测试目的：确保终端在读取应用数据时忽略不可识别的数据元。

终端配置：N/A。

卡片配置：读取的记录包括非借记/贷记应用数据对象。

测试流程：选择卡片应用，执行交易。

通过标准：终端应接受卡片，通过请求一个TC或AAC来完成交易。

7.7.24 SYGN012-01 参与脱机数据认证的不可识别的数据对象（1）

测试目的：确保对于AFL指明要用于脱机数据认证的记录，即使其中包括终端无法识别的数据，终端也要将其数据加到脱机认证的数据列表中参与脱机数据认证。

终端配置：支持 SDA。

卡片配置：——在AFL列出的一个参与数据认证的记录，该记录包含非借记/贷记应用数据对象；
——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——发卡行公钥证书和签名的静态应用数据有效。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节1，

位7 为‘0’（SDA成功）。第一个 GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个 GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个 GENERATE AC的TSI字节1，位8 为‘1’（脱机数据认证已执行）。

7.7.25 SYGN012-02 参与脱机数据认证的不可识别的数据对象（2）

测试目的：确保对于AFL指明要用于脱机数据认证的记录，即使其中包括终端无法识别的数据，终端也要将其数据加到脱机认证的数据列表中参与脱机数据认证。
终端配置：支持 DDA。
卡片配置：——AFL列出的一个参与数据认证的记录中包含非借记/贷记应用数据对象；
——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；
——发卡行公钥证书、IC 卡公钥证书和动态数据签名有效。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节1，位4 为‘0’（动态数据认证成功）。第一个 GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个 GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个 GENERATE AC的TSI字节1，位8 为‘1’（脱机数据认证已执行）。

7.7.26 SYGN012-03 参与脱机数据认证的不可识别的数据对象（3）

测试目的：确保对于AFL指明要用于脱机数据认证的记录，即使其中包括终端无法识别的数据，终端也要将其数据加到脱机认证的数据列表中参与脱机数据认证。通过执行CDA验证。
终端配置：支持 CDA。
卡片配置：——AFL列出的一个参与数据认证的记录中包含非借记/贷记应用数据对象；
——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——发卡行公钥证书、IC 卡公钥证书和动态数据签名有效。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应通过请求一个TC或AAC来完成交易。包含在金融确认信息或批数据获取信息中的TVR字节1，位3 为‘0’（CDA成功）。第一个 GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个 GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。金融交易确认报文或批上送报文中的TSI字节1，位8 为‘1’（脱机数据认证已执行），此项通过标准仅适用于CDA被请求时。

7.7.27 SYGN012-04 数据对象处理（私有数据对象在可读记录里）

测试目的：确保终端应忽略在读应用数据中的私有数据对象。
终端配置：N/A。
卡片配置：——可读记录（SFI 从 1 到 10）包含私有数据对象；
——记录包含 100 个私有标签有 DF09、DF10、DF11、DF21。
测试流程：选择卡片应用，执行交易直到接受交易。
通过标准：终端应接受卡片响应并请求 TC 处理至交易结束。

7.7.28 SYGN012-05 数据对象处理（私有数据对象在 PSE 可读记录里）

测试目的：确保终端应忽略在 PSE 读应用数据模板‘BF0C’中的私有数据对象。
终端配置：支持 PSE。
卡片配置：PSE ‘BF0C’模板中包含标签 DF09、DF10、DF11、DF21。
测试流程：选择卡片应用，执行交易指导接受交易。
通过标准：终端应接受卡片响应并请求 TC 处理至交易结束。

7.7.29 SYGN013-00 记录的数据格式：强制数据：应用失效日期

测试目的：确保如果缺少应用失效日期，终端终止交易。
终端配置：N/A。

卡片配置：卡中缺少应用失效日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.7.30 SYGN014-00 记录的数据格式：强制数据：PAN

测试目的：确保如果缺少PAN，终端终止交易。
终端配置：N/A。
卡片配置：卡中缺少 PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.7.31 SYGN015-00 记录的数据格式：强制数据：CDOL1

测试目的：确保如果缺少CDOL1，终端将终止交易。
终端配置：N/A。
卡片配置：卡中缺少 CDOL1。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.7.32 SYGN016-00 记录的数据格式：强制数据： CDOL2

测试目的：确保如果缺少CDOL2，终端终止交易。
终端配置：N/A。
卡片配置：卡中缺少 CDOL2。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.7.33 SYGN017-00 记录的数据格式：唯一的数据对象

测试目的：确保如果读记录时数据对象重复，终端终止交易。
终端配置：N/A。
子类案例：——案例 01：卡中的 PAN 重复；
——案例 02：卡中的失效日期重复；
——案例 03：卡中的 AUC 重复；
——案例 04：卡中的发卡行公钥指数重复；
——案例 05：卡中的 CDOL1 重复。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.7.34 SYGN018-00 记录数据格式：参与脱机数据认证的私有数据（1）

测试目的：确保在脱机静态数据认证中，终端可以读取包含位于私有文件中的数据对象，该私有文件是 TLV 编码结构。
终端配置：支持 SDA。
卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——位于私有文件的借记/贷记应用数据对象是记录标签为‘70’的TLV编码结构；
——静态签名应用数据是有效的，其计算时包含私有文件中的‘70’标签及其记录长度。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节1，位7 为‘0’（SDA成功）。第一个 GENERATE AC的TVR字节1，位3 为‘0’（未使

用CDA）。第一个 GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个 GENERATE AC的TSI字节1，位8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.35 SYGN018-01 记录数据格式：参与脱机数据认证的自定义数据（2）

测试目的：确保在脱机静态数据认证中，终端可以读取包含在私有文件中的数据对象，该私有文件是 TLV 编码结构。

终端配置：支持 DDA。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；
——位于私有文件的借记/贷记应用数据对象是记录标签为‘70’的TLV编码结构；
——IC卡公钥证书是有效的，其计算时包含私有文件中的‘70’标签及其记录长度。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节1，位4 为‘0’（DDA成功）。第一个 GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个 GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个 GENERATE AC的TSI字节1，位8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.36 SYGN018-02 参与脱机数据认证的非 TLV 编码的私有数据（1）

测试目的：确保如果位于私有文件的数据对象是非 TLV 编码的标签为‘70’的记录，终端应判断动态数据认证失败。

终端配置：支持 DDA。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件列于AFL（SFI为1130）中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；
——位于私有文件的借记/贷记应用数据对象是非‘70’标签编码 的记录；
——IC卡公钥证书有效；
——签名的静态应用数据有效；

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节1，位4 为‘1’（DDA失败）。第一个 GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个 GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个 GENERATE AC的TSI字节1，位8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.37 SYGN018-03 记录数据格式：参与脱机数据认证的非 TLV 编码的自定义数据（2）

测试目的：确保如果位于私有文件的数据对象是非 TLV 编码的标签为‘70’的记录，终端应判断 CDA 失败。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件列于AFL（SFI为1130）中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——位于私有文件的借记/贷记应用数据对象是**非**TLV**标签编码的**的记录；
——IAC和TAC的设置应确保终端第一次GENERATE AC请求TC；

——IC卡公钥证书有效；
——签名的静态应用数据有效。
测试流程：选择卡片应用，执行交易。
通过标准：GENERATE AC命令中终端不请求CDA。终端应根据TAC和IAC的设置通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节1，位3 为‘1’（CDA失败）。第一个 GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个 GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个 GENERATE AC的TSI字节1，位8 为‘1’（脱机数据认证已执行）。第一个 GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.38 SYGN018-04 记录数据格式：参与脱机数据认证的自定义数据（3）

测试目的：确保在执行 CDA 时，终端可以读取包含于私有文件中的数据对象，该私有文件是 TLV 编码结构。
终端配置：支持 CDA。
卡片配置：——GENERATE一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件列于AFL中，并且此数据包含于被签名的数据中；
——GENERATE卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——位于私有文件的借记/贷记应用数据对象是记录标签为‘70’的TLV编码结构；
——IC卡公钥证书是有效的，其计算时包含私有文件中的‘70’标签及其记录长度。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。包含在金融确认信息或批数据获取信息中的TVR字节1，位3 为‘0’（CDA成功）。第一个 GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个 GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。金融交易确认报文或批上送报文中的TSI字节1，位8 为‘1’（脱机数据认证已执行），此项通过标准仅适用于CDA被请求时。第一个 GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.39 SYGN018-05 记录数据格式：参与脱机数据认证的非 TLV 编码的私有数据（4）

测试目的：确保当位于私有文件中的数据对象是记录标签为‘70’的非 TLV 编码结构时，终端执行 CDA 失败。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到 CDA 失败。
卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件（SFI1130）列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——位于私有文件的借记/贷记应用数据对象是记录标签为‘70’的非TLV编码结构；
——IAC和TAC的设置应确保终端第一次GENERATE AC请求TC；
——IC卡公钥证书是有效的；
——签名的动态应用数据有效。
测试流程：选择卡片应用，执行交易。
通过标准：当卡片响应TC终端应拒绝交易且不应执行第二次GENERATE AC命令，或当卡片在第一次GENERATE AC响应ARQC时终端应发送第二次GENERATE AC命令请求AAC拒绝交易。终端应在第二次GENERATE AC命令中或金融确认报文或批上送报文中将如下位置位：TVR字节1 位3为‘1’（执行CDA失败）。此项通过标准仅适用于终端有能力保存拒绝交易或中止交易，或者是终端有能力以任一形式显示TVR的值。第一个 GENERATE AC的TVR字节1 位7为’0’（SDA未执行）。

第一个 GENERATE AC的TVR字节1 位4为'0'（DDA未执行）。终端应在第二次GENERATE AC命令中或金融确认报文或批上送报文中将如下位置位：TSI 字节1 位8为'1'（脱机数据认证执行）。此项通过标准仅适用于终端有能力保存拒绝交易或中止交易，或者是终端有能力以任一形式显示TSI的值。第一个 GENERATE AC的TVR字节1，位2 为'0'（SDA未执行）。

7.7.40 SYGN018-06 记录数据格式：参与脱机数据认证的非 TLV 编码的自定义数据（5）

测试目的：确保当位于私有文件中的数据对象是记录标签为'70'的非 TLV 编码结构时，终端执行 CDA 失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件（SFI1130）列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持CDA（AIP 字节1，位1 ='1'）；
——位于私有文件的借记/贷记应用数据对象是记录标签为'70'的非TLV编码结构；
——第一次GENERATE AC卡片返回ARQC；
——IAC和TAC的设置应确保终端第一次GENERATE AC请求ARQC，第二次GENERATE AC请求TC；
——IC卡公钥证书是有效的；
——签名的静态应用数据有效。

测试流程：选择卡片应用，执行交易。

通过标准：终端发送第二次GENERATE AC命令请求AAC拒绝交易。终端应在第一次GENERATE AC命令中TVR字节1 位3为'1'（执行CDA失败）。第一个 GENERATE AC的TVR字节1 位7为'0'（SDA未执行）。第一个 GENERATE AC的TVR字节1 位4为'0'（DDA未执行）。终端应在第一次GENERATE AC命令中TSI 字节1 位8为'1'（脱机数据认证执行）。第一个 GENERATE AC的TVR字节1，位2 为'0'（SDA未执行）。

7.7.41 SYGN018-07 记录数据格式：参与脱机数据认证的非 TLV 编码的私有数据（6）

测试目的：确保当位于私有文件中的数据对象是记录标签为'70'的非 TLV 编码结构时，终端执行 CDA 失败。

终端配置：——支持 CDA；
——仅联机终端；
——CDA 从不请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件（SFI1130）列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持CDA（AIP 字节1，位1 为'1'）；
——位于私有文件的借记/贷记应用数据对象是记录标签为'70'的非TLV编码结构；
——第一次GENERATE AC卡片返回ARQC；
——IAC和TAC的设置应确保终端第一次GENERATE AC请求ARQC，第二次GENERATE AC请求TC；
——IC卡公钥证书是有效的；
——签名的静态应用数据有效；
——发卡行响应批准交易。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。终端应在第二次GENERATE AC命令中或金融确认报文或批上送报文中将如下位置位：TVR字节1 位3为‘1’（执行CDA失败）。此项通过标准仅适用于终端有能力保存拒绝交易或终止交易，或者是终端有能力以任一形式显示TVR的值。第一个 GENERATE AC的TVR字节1 位7为’0’（SDA未执行）。第一个 GENERATE AC的TVR字节1 位4为’0’（DDA未执行）。终端应在第二次GENERATE AC命令中或金融确认报文或批上送报文中将如下位置位：TSI 字节1 位8为‘1’（脱机数据认证执行）。此项通过标准仅适用于终端有能力保存拒绝交易或中止交易，或者是终端有能力以任一形式显示TSI的值。第一个 GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.42 SYGN018-08 记录数据格式：参与脱机数据认证的非 TLV 编码的自定义数据（7）

测试目的：确保当位于私有文件中的数据对象是记录标签为‘70’的非 TLV 编码结构时，终端执行 CDA 失败

终端配置：——支持 CDA；
——仅联机终端；
——终端无法联机；
——CDA 从不请求，第一个 GAC 请求 ARQC 时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到 CDA 失败。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件（SFI1130）列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——位于私有文件的借记/贷记应用数据对象是记录标签为‘70’的非TLV编码结构；
——第一次GENERATE AC卡片返回ARQC；
——IAC和TAC的设置应确保终端第一次GENERATE AC请求ARQC，第二次GENERATE AC请求TC；
——IC卡公钥证书是有效的；
——签名的静态应用数据有效。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。终端应在第二次GENERATE AC命令中或金融确认报文或批上送报文中将如下位置位：TVR字节1 位3为‘1’（执行CDA失败）。此项通过标准仅适用于终端有能力保存拒绝交易或中止交易，或者是终端有能力以任一形式显示TVR的值。第一个 GENERATE AC的TVR字节1 位7为’0’（SDA未执行）。第一个 GENERATE AC的TVR字节1 位4为’0’（DDA未执行）。终端应在第二次GENERATE AC命令中或金融确认报文或批上送报文中将如下位置位：TSI 字节1 位8为‘1’（脱机数据认证执行）。此项通过标准仅适用于终端有能力保存拒绝交易或中止交易，或者是终端有能力以任一形式显示TSI的值。第一个 GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.43 SYGN018-09 记录数据格式：参与脱机数据认证的非 TLV 编码的私有数据（8）

测试目的：确保当位于私有文件中的数据对象是记录标签为‘70’的非 TLV 编码结构时，终端执行 CDA 失败。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件（SFI1130）列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；

——位于私有文件的借记/贷记应用数据对象是记录标签为‘70’的非TLV编码结构；
——IAC和TAC的设置应确保终端第一次GENERATE AC请求ARQC；
——交易联机批准；
——IC卡公钥证书是有效的；
——签名的静态应用数据有效。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一次、第二次GENERATE AC命令均不请求CDA。终端通过请求TC，完成交易。终端应在第一次GENERATE AC命令中TVR字节1 位3为‘1’（执行CDA失败）。第一个 GENERATE AC的TVR字节1 位7为’0’（SDA未执行）。第一个GENERATE AC的TVR字节1 位4为’0’（DDA未执行）。终端应在第一次GENERATE AC命令中TSI 字节1 位8为‘1’（脱机数据认证执行）。第一个 GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.44 SYGN018-10 记录数据格式：参与脱机数据认证的非 TLV 编码的自定义数据（9）

测试目的：确保当位于私有文件中的数据对象是记录标签为‘70’的非 TLV 编码结构时，终端执行 CDA 失败。

终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到 CDA 失败。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件（SFI1130）列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——位于私有文件的借记/贷记应用数据对象是记录标签为‘70’的非TLV编码结构；
——IAC和TAC的设置应确保终端第一次GENERATE AC请求ARQC；
——交易联机拒绝；
——IC卡公钥证书是有效的；
——签名的静态应用数据有效。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一次、第二次GENERATE AC命令均不请求CDA。终端通过请求AAC，完成交易。终端应在第一次GENERATE AC命令中TVR字节1 位3为‘1’（执行CDA失败）。第一个GENERATE AC的TVR字节1 位7为’0’（SDA未执行）。第一个GENERATE AC的TVR字节1 位4为’0’（DDA未执行）。终端应在第一次GENERATE AC命令中TSI 字节1 位8为‘1’（脱机数据认证执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.45 SYGN019-00 记录数据格式：参与脱机数据认证的非 TLV 编码的私有数据（10）

测试目的：确保当位于私有文件中的数据对象是记录标签为‘70’的非 TLV 编码结构时，终端执行 SDA 失败。

终端配置：支持 SDA。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录里，该文件列于AFL中，并且此数据包含于被签名的数据中；
——卡中的AIP指明支持SDA（AIP 字节1，位7 为‘1’）；
——位于私有文件的借记/贷记应用数据对象是记录标签为‘70’的非TLV编码结构；
——签名的静态应用数据有效。

测试流程：选择卡片应用，执行交易。

通过标准：终端通过请求TC或AAC完成交易。终端应在第一次GENERATE AC命令中TVR字节1 位7为‘1’（执行SDA失败）。第一个GENERATE AC的TVR字节1 位3为’0’

（CDA未执行）。第一个GENERATE AC的TVR字节1 位4为'0'（DDA未执行）。终端应在第一次GENERATE AC命令中TSI 字节1 位8为'1'（脱机数据认证执行）。第一个GENERATE AC的TVR字节1，位2 为'1'（SDA执行）。

7.7.46 SYGN020-00 支持脱机静态数据认证

测试目的：确保如果卡片和终端都支持脱机静态数据认证，终端在读应用数据后和终端行为分析结束前的任何时间进行脱机静态数据认证。

终端配置：支持 SDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为'1'）；
——签名的静态数据无效；
——IAC 拒绝字节1，位7 为'1'（SDA失败）。

测试流程：选择卡片应用，执行交易。

通过标准：终端发出第一个 GENERATE AC请求AAC。第一个GENERATE AC的TVR字节1，位7 为'1'（静态数据认证失败）。第一个GENERATE AC的TVR字节1，位3 为'0'（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为'0'（未使用DDA）。第一个GENERATE AC的TVR字节1，位2 为'1'（SDA执行）。

7.7.47 SYGN021-00 终端和卡片支持 CDA（TC，第一个 GENERATE AC）

测试目的：确保如果卡片和终端都支持 CDA，终端执行 CDA。

终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 为'1'）；
——TAC和IAC的设置应确保终端第一次GENERATE AC请求TC；
——卡响应第一个GENERATE AC命令TC；
——由卡生成的复合动态签名有效。

测试流程：选择卡片应用，执行交易。

通过标准：终端应完成交易。TVR和TSI （包含在金融确认信息或者批数据获取信息或其他中）应设置为：TVR字节1，位3 为'0'（CDA成功）。TSI 字节1，位8 为'1'（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位7 为'0'（未使用SDA）。第一个GENERATE AC的TVR字节1，位4 为'0'（未使用DDA）。第一个GENERATE AC的TVR字节1，位2 为'0'（SDA未执行）。

7.7.48 SYGN021-01 终端和卡片支持 CDA（TC，第二个 GENERATE AC）

测试目的：确保如果卡片和终端都支持CDA，终端执行CDA。

终端配置：——支持 CDA；
——终端不能联机；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 为'1'）；
——TAC和IAC的设置应确保终端第一次GENERATE AC和第二次GENERATE AC均请求TC；
——第一个GENERATE AC卡应答ARQC，第二个GENERATE AC卡应答TC；
——由卡生成的复合动态签名有效。

测试流程：选择卡片应用，执行交易（特别是CDA）。

通过标准：终端应完成交易。TVR和TSI（包含在金融确认信息或者批数据获取信息或其他中）应设置为：TVR字节1，位3 为'0'（CDA成功）。TSI字节1，位8 为'1'（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位7为'0'（未使用SDA）。第一个GENERATE AC的TVR字节1，位4为'0'（未使用DDA）。第一个GENERATE AC的TVR字节1，位2为'0'（SDA未执行）。

7.7.49 SYGN021-02 终端和卡片支持 CDA（ARQC）（1）

测试目的：确保如果卡片和终端都支持 CDA，终端执行 CDA。
终端配置：——支持 CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——TAC和IAC的设置应确保终端第一次GENERATE AC请求TC；
——第一个GENERATE AC卡应答ARQC；
——由卡生成的复合动态签名有效。
测试流程：选择卡片应用，执行交易（特别是CDA）。
通过标准：终端应通过请求TC或者AAC完成交易。TVR和 TSI （包含在金融确认信息或者批数据获取信息或其他中）应设置为：TVR字节1，位3 为‘0’（CDA成功）。TSI 字节1，位8 =‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.50 SYGN021-03 终端和卡片支持 CDA（TC，第二个 GENERATE AC）（1）

测试目的：确保如果卡片和终端都支持 CDA，终端执行 CDA。
终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时；
——CDA 总是请求，在第二个 GAC 请求 TC 时。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——TAC和IAC的设置应确保终端第一次GENERATE AC请求ARQC；
——第一个GENERATE AC卡应答ARQC，第二次GENERATE AC卡应答TC；
——由卡生成的复合动态签名有效。
测试流程：选择卡片应用，执行交易（特别是CDA）。
通过标准：终端应完成交易。TVR和 TSI（包含在金融确认信息或者批数据获取信息或其他中）应设置为：TVR字节1，位3 为‘0’（CDA成功）。TSI 字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.51 SYGN021-04 终端和卡片支持 CDA（ARQC）（2）

测试目的：确保如果卡片和终端都支持 CDA，终端执行 CDA。
终端配置：——支持 CDA；
——仅联机终端或有联机能力的脱机终端；
——CDA 总是请求，第一个 GAC 请求 ARQC 时。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——TAC和IAC的设置应确保终端第一次GENERATE AC请求ARQC；
——第一个GENERATE AC卡应答ARQC；
——由卡生成的复合动态签名有效。
测试流程：选择卡片应用，执行交易（特别是CDA）。
通过标准：终端应通过请求TC或者AAC，完成交易。TVR和TSI（包含在金融确认信息或者批数据获取信息或其他中）应设置为：TVR字节1，位3 为‘0’（CDA成功）。TSI 字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.52 SYGN021-05 终端和卡片支持 CDA（TC，第二个 GENERATE AC）（2）

测试目的：确保如果卡片和终端都支持 CDA，终端执行 CDA。
终端配置：——支持 CDA；

——仅联机终端；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——TAC和IAC的设置应确保终端第一次GENERATE AC请求ARQC，第二次GENERATE AC请求TC；
——交易不能联机；
——第一个GENERATE AC卡应答ARQC，第二次GENERATE AC卡应答TC；
——由卡生成的复合动态签名有效。

测试流程：选择卡片应用，执行交易（特别是CDA）。

通过标准：终端应完成交易。TVR和TSI（包含在金融确认信息或者批数据获取信息或其他中）应设置为：TVR字节1，位3 为‘0’（CDA成功）。TSI 字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.53 SYGN022-00 终端和卡片支持 SDA（1）

测试目的：确保如果卡片和终端都支持 SDA，并且不同时支持 DDA 或 CDA，终端进行脱机静态数据认证。

终端配置：——支持 SDA；
——不支持 DDA；
——不支持 CDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；
——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——卡中的静态签名无效。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘1’（SDA失败）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.54 SYGN022-01 终端和卡片支持 SDA（2）

测试目的：确保如果卡片和终端都支持 SDA，并且不同时支持 DDA 或 CDA，终端进行脱机静态数据认证。

终端配置：——支持 SDA；
——支持 DDA；
——不支持 CDA。

卡片配置：——卡中的AIP指明支静态数据认证（AIP 字节1，位7 为‘1’）；
——卡中的AIP指明不支持动态数据认证（AIP 字节1，位6 为‘0’）；
——卡中的AIP指明不支持CDA（AIP 字节1，位1 为‘0’）；
——卡中的静态签名无效。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘1’（SDA失败）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.55 SYGN022-02 终端和卡片支持 SDA（3）

测试目的：确保如果卡片和终端都支持 SDA，并且不同时支持 DDA 或 CDA，终端进行脱机静态数据认证。

终端配置：——支持 SDA；
——支持 DDA；
——支持 CDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——卡中的AIP指明不支持动态数据认证（AIP 字节1，位6 为‘0’）；
——卡中的AIP指明不支持CDA（AIP 字节1，位1 为‘0’）；
——卡中的静态签名无效。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘1’（SDA失败）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.56 SYGN023-00 支持 DDA 和 SDA（1）

测试目的：确保如果卡片和终端都支持脱机静态数据认证和脱机动态数据认证，并且不同时支持复合动态数据认证，终端只进行脱机动态数据认证。

终端配置：——支持 SDA；
——支持 DDA；
——不支持 CDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；
——卡中的AIP指明支持复合动态数据认证（AIP 字节1，位1 为‘1’）；
——由卡生成的动态签名无效。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘1’（DDA失败）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.57 SYGN023-01 支持 DDA 和 SDA（2）

测试目的：确保如果卡片和终端都支持脱机静态数据认证和脱机动态数据认证，并且不同时支持复合动态数据认证，终端只进行脱机动态数据认证。

终端配置：——支持 SDA；
——支持 DDA；
——支持 CDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；
——卡中的AIP指明不支持复合动态数据认证（AIP 字节1，位1 为‘0’）；
——由卡生成的动态签名无效。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘1’（DDA失败）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.58 SYGN024-00 既不执行 DDA、也不执行 SDA 和 CDA（1）

测试目的：确保如果脱机静态数据认证、脱机动态数据认证、复合动态数据认证都未执行，终端设置 TVR 中的“脱机数据认证未执行”位为‘1’。

终端配置：——不支持 SDA；
——不支持 DDA；
——不支持 CDA。

子类案例：——案例01：卡不支持SDA、DDA或CDA；
——案例02：卡支持SDA、DDA和CDA。

测试流程：选择卡片应用，执行交易。

通过标准：终端应来完成交易。第一个GENERATE AC的TVR字节1，位8 为‘1’（脱机数据认证未执行）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1，位8 为‘0’（脱机数据认证未执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.59 SYGN024-01 既不执行 DDA、也不执行 SDA 和 CDA（2）

测试目的：确保如果脱机静态数据认证、脱机动态数据认证、复合动态数据认证都未执行，终端设置 TVR 中的“脱机数据认证未执行”位为‘1’。

终端配置：——支持 SDA；
——不支持 DDA；
——不支持 CDA。

子类案例：——案例01：卡不支持SDA、DDA或CDA；
——案例02：卡不支持SDA、支持DDA和CDA。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或者AAC来完成交易。第一个GENERATE AC的TVR字节1，位8 为‘1’（脱机数据认证未执行）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1，位8 为‘0’（脱机数据认证未执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.60 SYGN024-03 既不执行 DDA、也不执行 SDA 和 CDA（3）

测试目的：确保如果脱机静态数据认证、脱机动态数据认证、复合动态数据认证都未执行，终端设置 TVR 中的“脱机数据认证未执行”位为‘1’。

终端配置：——支持 SDA；
——支持 DDA；
——支持 CDA。

卡片配置：卡片不支持SDA、不支持DDA、不支持CDA。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或者AAC来完成交易。第一个GENERATE AC的TVR字节1，位8 为‘1’（脱机数据认证未执行）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1，位8 为‘0’（脱机数据认证未执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.61 SYGN025-00 处理输入数据的规则 （1）

测试目的：确保如果进行脱机静态数据认证，终端连接由 AFL 指定的记录中获得的数据

和静态数据认证标签列表中获得的数据，并且使用这些数据作为要被签名的输入。

终端配置：支持 SDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——AFL指明了包含在静态签名中的数据；
——卡支持静态数据认证签名列表。

子类案例：——案例01：卡片中由AFL指定的、用于静态签名的一条记录，其右边用‘00’填充（最后的数据对象之后,但仍在记录模板中）；
——案例03：卡片中由AFL指定的、用于静态签名的一条记录，无填充；
——案例04：卡片中由AFL指定的、用于静态签名的一条记录，其右边用值为‘00’的50个字节填充（最后的数据对象之后,但仍在记录模板中）；
——案例06：卡片中由AFL指定的25条记录用于静态签名的输入。

注：这里的子案例序号不是线性连续的，中间缺失的编号被分配给了早期的一些子案例，但这些子案例不再适用。为避免混淆，不调整子案例编号为线性连续的。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（SDA成功）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.62 SYGN025-01 处理输入数据的规则（2）

测试目的：确保如果进行脱机动态数据认证，终端连接由 AFL 指定的记录中获得的数据和静态数据认证标签列表中获得的数据，并且使用这个连接的数据作为要被签名的输入。

终端配置：支持 DDA。

卡片配置：——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；
——发卡行公钥证书，IC卡公钥证书和动态签名有效。

子类案例：——案例01：卡片中由AFL指定的、用于静态签名的一条记录，其右边用‘00’填充（最后的数据对象之后,但仍在记录模板中）；
——案例03：卡片中由AFL指定的、用于静态签名的一条记录，无填充；
——案例04：卡片中由AFL指定的、用于静态签名的一条记录，其右边用值为‘00’的50个字节填充（最后的数据对象之后,但仍在记录模板中）；
——案例06：卡片中由AFL指定的25条记录用于静态签名的输入。

注：这里的子案例序号不是线性连续的，中间缺失的编号被分配给了早期的一些子案例，但这些子案例不再适用。为避免混淆，不调整子案例编号为线性连续的。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC的TSI字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.63 SYGN025-02 处理输入数据的规则（3）

测试目的：确保如果进行脱机动态数据认证，终端连接由 AFL 指定的记录中获得的数据和静态数据认证标签列表中获得的数据，并且使用这个连接的数据作为要被签名的输入。

终端配置：支持 CDA。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——发卡行公钥证书，IC卡公钥证书和动态签名有效；
——卡片返回静态数据认证签名列表。

子类案例：——案例01：卡片中由AFL指定的、用于静态签名的一条记录，其右边用‘00’填充（最后的数据对象之后,但仍在记录模板中）；
——案例03：卡片中由AFL指定的、用于静态签名的一条记录，无填充；
——案例04：卡片中由AFL指定的、用于静态签名的一条记录，其右边用值为‘00’的50个字节填充（最后的数据对象之后,但仍在记录模板中）；
——案例06：卡片中由AFL指定的25条记录用于静态签名的输入。

注：这里的子案例序号不是线性连续的，中间缺失的编号被分配给了早期的一些子案例，但这些子案例不再适用。为避免混淆，不调整子案例编号为线性连续的。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。金融确认报文或批上送报文中的TSI 字节1，位8 为‘1’（脱机数据认证已执行），此通过标准仅适用于请求CDA。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.64 SYGN025-03 处理输入数据的规则（4）

测试目的：确保如果进行脱机静态数据认证，终端连接由 AFL 指定的记录中获得的数据和静态数据认证标签列表中获得的数据，并且使用这个连接的数据作为要被签名的输入，尽管这个数据存在 FF 填充值。

终端配置：支持 SDA。

卡片配置：——卡中的AIP指明支持SDA（AIP 字节1，位7 为‘1’）；
——AFL指明包含在静态签名中的数据；
——卡片返回静态数据认证签名列表。

子类案例：——案例01：卡片中由AFL指定的、用于静态签名的一条记录，其左边用‘FF’填充（第一个数据对象之前,但仍在记录模板中）；
——案例02：卡片中由AFL指定的、用于静态签名的一条记录，其左边用值为‘FF’的50个字节填充（第一个数据对象之前,但仍在记录模板中）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（SDA成功）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.65 SYGN025-04 处理输入数据的规则（5）

测试目的：确保如果进行脱机动态数据认证，终端连接由 AFL 指定的记录中获得的数据和静态数据认证标签列表中获得的数据，并且使用这个连接的数据作为要被签名的输入，尽管这个数据存在 FF 填充值。

终端配置：支持 DDA。

卡片配置：——卡中的AIP指明支持DDA（AIP 字节1，位6 为‘1’）；
——发卡行公钥证书、卡片公钥证书以及动态签名有效。

子类案例：——案例01：卡片中由AFL指定的、用于静态签名的一条记录，其左边用‘FF’填充（第一个数据对象之前,但仍在记录模板中）；
——案例02：卡片中由AFL指定的、用于静态签名的一条记录，其左边用值

为‘FF’的50个字节填充（第一个数据对象之前,但仍在记录模板中）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.66 SYGN025-05 处理输入数据的规则（6）

测试目的：确保如果进行脱机动态数据认证，终端连接由 AFL 指定的记录中获得的数据和静态数据认证标签列表中获得的数据，并且使用这个连接的数据作为要被签名的输入，尽管这个数据存在 FF 填充值。

终端配置：支持 CDA。

卡片配置：——卡中的AIP指明支持DDA（AIP 字节1，位1 为‘1’）；

——发卡行公钥证书、卡片公钥证书以及动态签名有效。

子类案例：——案例01：卡片中由AFL指定的、用于静态签名的一条记录，其左边用‘FF’填充（第一个数据对象之前,但仍在记录模板中）；

——案例02：卡片中由AFL指定的、用于静态签名的一条记录，其左边用值为‘FF’的50个字节填充（第一个数据对象之前,但仍在记录模板中）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。金融确认报文或批上送报文的TSI 字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.67 SYGN026-00 执行 DDA 时，处理由 AFL 指定的记录的规则（1）

测试目的：确保当终端执行动态数据认证，建立要被签名的数据时，对于 AFL 指定的 SFI 是 1 到 10 的文里记录的标签‘70’和长度不参与动态数据认证。

终端配置：支持 DDA。

卡片配置：——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；

——参加动态数据认证的记录位于：SFI为1的文件，记录1；SFI为3的文件，记录2和3；SFI为10的文件，记录5；

——卡产生的动态签名有效。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.68 SYGN026-01 执行 CDA 时，处理由 AFL 指定的记录的规则（1）

测试目的：确保当终端执行 CDA，建立要被签名的数据时，对于 AFL 指定的 SFI 是 1 到 10 的文件里记录的标签‘70’和长度不参与复合动态数据认证。

终端配置：支持 CDA。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP 字节1，位1 为‘1’）；

——参加动态数据认证的记录位于：SFI为1的文件，记录1；SFI为3的文件，记录2和3；SFI为10的文件，记录5；

——卡产生的动态签名有效。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。包含在金融确认信息或者批数据获取信息中的TVR字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。包含在金融确认信息或者批数据获取信息中的TSI字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.69 SYGN027-00 执行 DDA 时，处理由 AFL 指定的记录的规则（2）

测试目的：确保当终端执行动态数据认证，建立要被签名的数据时，对于 AFL 指定的 SFI 是 1 到 10 的文件里记录的标签‘70’和长度不参与动态数据认证。

终端配置：支持 DDA。

卡片配置：——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；

——参加动态数据认证的记录位于：SFI为11的文件，记录1；SFI为15的文件，记录2和3；SFI为30的文件，记录5；

——SFI1130的记录为TLV编码；

——卡产生的动态签名有效。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.70 SYGN027-01 执行 CDA 时，处理由 AFL 指定的记录的规则（2）

测试目的：确保当终端执行 CDA，建立要被签名的数据时，对于 AFL 指定的 SFI 是 11 到 30 的文件里记录的标签‘70’和长度不参与复合动态数据认证。

终端配置：支持 CDA。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP 字节1，位1 为‘1’）；

——参加动态数据认证的记录位于：SFI为11的文件，记录1；SFI为15的文件，记录2和3；SFI为30的文件，记录5；SFI1130的记录为TLV编码；卡产生的动态签名有效；

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。包含在金融确认信息或者批数据获取信息中的TVR字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。包含在金融确认信息或者批数据获取信息中的TSI 字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.71 SYGN028-00 执行 SDA 时，处理由 AFL 指定的记录的规则（1）

测试目的：确保当终端执行静态数据认证，建立要被签名的数据时，对于 AFL 指定的 SFI 是 1 到 10 的文件里记录的标签‘70’和长度不参与静态数据认证。

终端配置：支持 SDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；

——参加静态数据认证的记录位于：SFI为1的文件，记录1；SFI为3的文件，记录2和3；SFI为10的文件，记录5；

——卡中的静态签名有效。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（SDA成功）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.72 SYGN029-00 执行 SDA 时，处理由 AFL 指定的记录的规则（2）

测试目的：确保当终端执行静态数据认证，建立要被签名的数据时，对于 AFL 指定的 SFI 是 11 到 30 的文件里记录的标签‘70’和长度不参与静态数据认证。

终端配置：支持 SDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——参加静态数据认证的记录位于：SFI为11的文件，记录1；SFI为15的文件，记录2和3；SFI为30的文件，记录5；
——卡中的静态签名有效；
——SFI1130的记录为TLV编码。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（SDA成功）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.73 SYGN030-00 在脱机静态数据认证中处理 AIP（1）

测试目的：——确保当终端执行脱机静态数据认证时，终端检查AIP从而进行数据认证；
——确保终端在完成脱机静态数据认证过程后设置 TSI 的“脱机数据认证已进行”位为‘1’。

终端配置：支持 SDA。

卡片配置：——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）；
——卡片中的发卡行公钥证书和静态签名有效。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（SDA成功）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.74 SYGN030-01 在脱机静态数据认证中处理 AIP（2）

测试目的：——确保当终端执行脱机动态数据认证时，终端检查AIP从而进行数据认证；
——确保终端在完成脱机动态数据认证过程后设置 TSI 的“脱机数据认证已进行”位为‘1’。

终端配置：支持 DDA。

卡片配置：——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）；
——发卡行公钥证书和卡片公钥证书有效；
——卡片中的动态签名有效。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC的TSI 字节1,位8 为‘1’(脱机数据认证已执行)。第一个GENERATE

AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.75 SYGN030-02 在脱机数据认证（复合动态数据认证）中处理 AIP

测试目的：——确保当终端执行脱机复合动态数据认证时，终端检查AIP从而进行数据认证；
——确保终端在复合动态数据认证过程中，验证JR/T 0025.7—2013 11.2条描述的签名；
——确保终端在完成脱机动态数据认证过程后设置TSI的“脱机数据认证已进行”位为‘1’。
终端配置：支持 CDA。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 为‘1’）；
——卡片中的发卡行公钥证书和IC卡公钥证书有效；
——卡片计算的动态签名有效。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应通过请求一个TC或AAC来完成交易。包含在金融确认信息或者批数据获取信息中的TVR字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。包含在金融确认信息或者批数据获取信息中的TSI字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.76 SYGN032-00 脱机静态数据认证失败

测试目的：——确保如果进行了静态数据认证但是没有成功，终端在TVR中设置“脱机静态数据认证失败”位为‘1’；
——确保终端在完成脱机静态数据认证过程后设置TSI的“脱机数据认证已进行”位为‘1’。
终端配置：支持 SDA。
卡片配置：——卡片签名的静态应用数据无效；
——卡中的AIP指明支持静态数据认证（AIP 字节1，位7 为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位7 为‘1’（SDA失败）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC的TSI字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位2 为‘1’（SDA执行）。

7.7.77 SYGN033-00 脱机动态数据认证失败

测试目的：——确保如果进行了动态数据认证但是没有成功，终端在TVR中设置“脱机动态数据认证失败”位为‘1’；
——确保终端在完成脱机静态数据认证过程后设置TSI的“脱机数据认证已进行”位为‘1’。
终端配置：支持 DDA。
卡片配置：——卡片的数据签名无效；
——卡中的AIP指明支持动态数据认证（AIP 字节1，位6 为‘1’）。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节1，位4 为‘1’（DDA失败）。第一个GENERATE AC的TVR字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC的TSI字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC的TVR字节1，位2 为‘0’（SDA未执行）。

7.7.78 SYGN035-00 执行处理限制功能

测试目的：确保终端在读取应用数据之后、完成终端行为分析之前执行处理限制功能。
终端配置：支持现金 或者 返现 或者 货币 或者 服务。
卡片配置：——卡片和终端的应用版本号不同；
——发卡行国家代码和终端国家代码相同；
——AUC中的国内交易无效；
——卡中的应用失效日期已过期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位8 为‘1’（卡片和终端应用版本不一致）。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。第一个GENERATE AC的TVR字节2，位7 为‘1’（应用已过期）。

7.7.79 SYGN036-00 由支付系统指配的应用版本号

测试目的：确保终端保存一个由支付系统分配的应用版本号。
卡片配置：——CDOL1请求应用版本号（9F09）；
——所有终端支持的应用都要进行测试。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。卡片应收到所选择应用的应用版本号的值。

7.7.80 SYGN037-00 IC卡中不存在应用版本号

测试目的：确保如果IC卡中不存在应用版本号，终端继续进行交易直到结束。
卡片配置：卡中不存在应用版本号。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。终端应认为IC卡和终端的应用兼容。第一个GENERATE AC的TVR字节2，位8 为‘0’（卡片和终端应用版本一致）。

7.7.81 SYGN039-00 卡中存在的应用版本号与终端的一致（隐含的）

测试目的：确保如果卡中的应用版本号与终端的一致，终端在TVR设置中，不设置“IC卡和终端应用版本号不一致”位为‘1’。
卡片配置：卡片和终端应用版本号相同。
测试流程：选择卡片应用，执行交易。
通过标准：终端应来完成交易。第一个 GENERATE AC的TVR字节2，位8 为‘0’（卡片和终端应用版本一致）。

7.7.82 SYGN041-00 卡中存在AUC并且交易在 ATM 上进行

测试目的：确保如果终端是ATM并且卡片中的AUC“在ATM上有效”位不是‘1’，终端应设置TVR“卡片不允许所请求的服务”位为‘1’。
终端配置：支持 ATM。
卡片配置：——卡中存在AUC；
——在AUC中“在ATM上有效”位不是‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。

7.7.83 SYGN042-00 卡中存在AUC并且交易在 ATM 上进行（隐含的）

测试目的：确保如果终端是 ATM 并且卡片中的 AUC “在 ATM 上有效”位是 ‘1’，终端将不设置 TVR “卡片不允许所请求的服务”位为 ‘1’。
终端配置：支持 ATM。

卡片配置：——卡中存在AUC；
——AUC中 “在ATM上有效”位是‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。

7.7.84 SYGN043-00 卡中存在 AUC 并且交易在非 ATM 终端上进行

测试目的：确保如果终端不是 ATM 且卡片中 AUC “在非 ATM 终端上有效”位不是 ‘1’，终端应设置 TVR “卡片不允许所请求的服务”位为 ‘1’。
终端配置：不支持 ATM。
卡片配置：——卡中存在AUC；
——AUC中 “在非ATM终端上有效”位不是‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。

7.7.85 SYGN044-00 卡中存在 AUC 并且交易在非 ATM 终端上进行（隐含的）

测试目的：确保如果终端不是 ATM 且卡片中 AUC “在非 ATM 终端上有效”位是 ‘1’，终端应不设置 TVR “卡片不允许所请求的服务”位为 ‘1’。
终端配置：不支持 ATM。
卡片配置：——卡中存在AUC；
——AUC中 “在非ATM终端上有效”位是‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。

7.7.86 SYGN045-00 交易类型为现金交易，发卡行国家代码=终端国家代码

测试目的：确保如果发卡行国家代码与终端国家代码相同，交易类型为现金交易，卡片中 AUC “国内现金交易有效”位不是 ‘1’，终端应设置 TVR “卡片不允许所请求的服务”位为 ‘1’。
终端配置：支持现金。
卡片配置：——交易类型为现金交易；
——卡中存在AUC；
——发卡行国家代码与终端国家代码相同；
——AUC中不设置“国内现金交易有效”位为‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。交易类型应显示为现金交易。

7.7.87 SYGN046-00 交易类型为现金交易，发卡行国家代码=终端国家代码（隐含的）

测试目的：确保如果发卡行国家代码与终端国家代码相同，交易类型为现金交易，卡片中 AUC 设置 “国内现金交易有效”位为 ‘1’，终端应不设置 TVR “卡片不允许所请求的服务”位为 ‘1’。
终端配置：支持现金。
卡片配置：——交易类型为现金交易；
——卡中存在AUC；
——发卡行国家代码与终端国家代码相同；
——AUC中设置“国内现金交易有效”位为‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，

位5 为‘0’（卡片允许所请求的服务）。交易类型应显示为现金交易。

7.7.88 SYGN047-00 交易类型为现金交易，发卡行国家代码≠终端国家代码

测试目的：确保如果发卡行国家代码与终端国家代码不同，交易类型为现金交易，卡片中 AUC 不设置“国际现金交易有效”位为‘1’，终端应设置 TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持现金。

卡片配置：——交易类型为现金交易；
——卡中存在AUC；
——发卡行国家代码与终端国家代码不同；
——AUC中不设置“国际现金交易有效”位为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。交易类型应显示为现金交易。

7.7.89 SYGN048-00 交易类型为现金交易，发卡行国家代码≠终端国家代码（隐含的）

测试目的：确保如果发卡行国家代码与终端国家代码不同，交易类型为现金交易，卡片中 AUC 设置“国际现金交易有效”位为‘1’，终端应不设置 TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持现金。

卡片配置：——交易类型为现金交易；
——卡中存在AUC；
——发卡行国家代码与终端国家代码不同；
——AUC中设置“国际现金交易有效”位为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。交易类型应显示为现金交易。

7.7.90 SYGN049-00 交易类型为货物和服务的消费交易，发卡行国家代码=终端国家代码

测试目的：确保如果发卡行国家代码与终端国家代码相同，交易类型为货物和服务的消费交易，卡片中 AUC 不设置“国内货物有效”位为‘1’，终端应设置 TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持货物或服务。

卡片配置：——交易类型为货物和服务的消费交易；
——卡中存在AUC；
——发卡行国家代码与终端国家代码相同；
——AUC中不设置“国内货物有效”位为‘1’；
——AUC中不设置“国内服务有效”位为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。交易类型应显示为货物和服务的消费交易。

7.7.91 SYGN050-00 交易类型为货物和服务的消费交易，发卡行国家代码=终端国家代码（隐含的）

测试目的：确保如果发卡行国家代码与终端国家代码相同，交易类型为货物和服务的消费交易，卡片中 AUC 设置“国内货物有效”位为‘1’，终端应不设置 TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持货物或服务。

卡片配置：——交易类型为货物和服务的消费交易（交易类型为‘00’）；

——卡中存在AUC；
——发卡行国家代码与终端国家代码相同；
——AUC中设置“国内货物有效”位为‘1’；
——AUC中不设置“国内服务有效”位为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。交易类型应显示为货物和服务的消费交易。

7.7.92 SYGN051-00 交易类型为货物和服务的消费交易，发卡行国家代码≠终端国家代码

测试目的：确保如果发卡行国家代码与终端国家代码不同，交易类型为货物和服务的消费交易，卡片中 AUC “国际货物有效”位不是 ‘1’，终端应设置 TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持货物或服务。

卡片配置：——交易类型为货物和服务的消费交易（交易类型为‘00’）；
——卡中存在AUC；
——发卡行国家代码与终端国家代码不同；
——AUC中不设置“国际货物有效”位为‘1’；
——AUC中不设置“国际服务有效”位为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。交易类型应显示为货物和服务的消费交易。

7.7.93 SYGN052-00 交易类型为货物和服务的消费交易，发卡行国家代码≠终端国家代码（隐含的）

测试目的：确保如果发卡行国家代码与终端国家代码不同，交易类型为货物和服务的消费交易，卡片中 AUC 设置“国际货物有效”位为‘1’，终端应不设置 TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持货物或服务。

卡片配置：——交易类型为货物和服务的消费交易（交易类型为‘00’）；
——卡中存在AUC；
——发卡行国家代码与终端国家代码不同；
——AUC中设置“国际货物有效”位为‘1’；
——AUC中不设置“国际服务有效”位为‘1’；
——案例1：交易类型是货物的消费交易；
——案例2：交易类型是服务的消费交易。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。交易类型应显示为货物和服务的消费交易。

7.7.94 SYGN053-00 交易类型为货物和服务的消费交易，发卡行国家代码=终端国家代码

测试目的：确保如果发卡行国家代码与终端国家代码相同，交易类型为货物和服务的消费交易，卡片中 AUC “国内服务有效”位不是 ‘1’，终端应设置 TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持货物或服务。

卡片配置：——交易类型为货物和服务的消费交易（交易类型为‘00’）；
——卡中存在AUC；
——发卡行国家代码与终端国家代码相同；

——AUC中不设置“国内服务有效”位为‘1’；
——AUC中不设置“国内货物有效”位为‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。交易类型应显示为货物和服务的消费交易。

7.7.95 SYGN054-00 交易类型为货物和服务的消费交易，发卡行国家代码=终端国家代码（隐含的）

测试目的：确保如果发卡行国家代码与终端国家代码相同，交易类型为货物和服务的消费交易，卡片中 AUC 设置“国内服务有效”位为‘1’，终端应不设置 TVR“卡片不允许所请求的服务”位为‘1’。
终端配置：支持货物或服务。
卡片配置：——交易类型为货物和服务的消费交易（交易类型为‘00’）；
——卡中存在AUC；
——发卡行国家代码与终端国家代码相同；
——AUC中设置“国内服务有效”位为‘1’；
——AUC中不设置“国内货物有效”位为‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 2，位 5 为‘0’（卡片允许所请求的服务）。交易类型应显示为货物和服务的消费交易。

7.7.96 SYGN056-00 交易类型为货物和服务的消费交易，发卡行国家代码≠终端国家代码（隐含的）

测试目的：确保如果发卡行国家代码与终端国家代码不同，交易类型为货物和服务的消费交易，卡片中 AUC 设置“国际服务有效”位为‘1’，终端应不设置 TVR“卡片不允许所请求的服务”位为‘1’。
终端配置：支持货物或服务。
卡片配置：——交易类型为货物和服务的消费交易（交易类型为‘00’）；
——卡中存在AUC；
——发卡行国家代码与终端国家代码不同；
——AUC中设置“国际服务有效”位为‘1’；
——AUC中不设置“国际货物有效”位为‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。交易类型应显示为货物和服务的消费交易。

7.7.97 SYGN057-00 交易类型为返现，发卡行国家代码=终端国家代码

测试目的：确保如果发卡行国家代码与终端国家代码相同，交易类型为返现，卡片中 AUC“允许国内返现”位不是‘1’，终端应设置TVR“卡片不允许所请求的服务”位为‘1’。
终端配置：支持返现。
卡片配置：——交易有返现金额；
——卡中存在AUC；
——发卡行国家代码与终端国家代码相同；
——AUC中不设置“允许国内返现”位为‘1’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，

位5 为‘1’（卡片不允许所请求的服务）。

7.7.98 SYGN058-00 交易类型为返现，发卡行国家代码=终端国家代码（隐含的）

测试目的：确保如果发卡行国家代码与终端国家代码相同，交易类型为返现，卡片中AUC设置“允许国内返现”位为‘1’，终端应不设置TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持返现。

卡片配置：——交易有返现金额；
——卡中存在AUC；
——发卡行国家代码与终端国家代码相同；
——AUC中设置“允许国内返现”位为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。

7.7.99 SYGN059-00 交易类型为返现，发卡行国家代码≠终端国家代码

测试目的：确保如果发卡行国家代码与终端国家代码不同，交易类型为返现，卡片中AUC“允许国际返现”位不是‘1’，终端应设置TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持返现。

卡片配置：——交易有返现金额；
——卡中存在AUC；
——发卡行国家代码与终端国家代码不同；
——AUC中不设置“允许国际返现”位为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘1’（卡片不允许所请求的服务）。

7.7.100 SYGN060-00 交易类型为返现，发卡行国家代码≠终端国家代码（隐含的）

测试目的：确保如果发卡行国家代码与终端国家代码不同，交易类型为返现，卡片中AUC设置“允许国际返现”位为‘1’，终端应不设置TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：支持返现。

卡片配置：——交易有返现金额；
——卡中存在AUC；
——发卡行国家代码与终端国家代码不同；
——AUC中设置“允许国际返现”位为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。

7.7.101 SYGN061-00 卡中不存在 AUC（隐含的）

测试目的：确保如果卡中不存在AUC，终端应不设置TVR“卡片不允许所请求的服务”位为‘1’。

终端配置：N/A。

卡片配置：卡片中不存在AUC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。

7.7.102 SYGN062-00 卡中存在AUC，但发卡行国家代码不存在（隐含的）

测试目的：确保如果卡中存在AUC但不存在发卡行国家代码，终端应跳过规范描述的检查。
终端配置：N/A。
卡片配置：——卡中存在AUC；
——AUC中“ATM有效”和“在非ATM终端上有效”置位；
——卡中不存在发卡行国家代码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位5 为‘0’（卡片允许所请求的服务）。

7.7.103 SYGN063-00 当前日期早于应用生效日期

测试目的：确保如果今天日期早于应用生效日期，终端将设置TVR中“应用尚未生效”位为‘1’。
终端配置：N/A。
卡片配置：——卡中存在应用生效日期；
——当前日期早于应用生效日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位6 为‘1’（应用尚未生效）。

7.7.104 SYGN064-00 当前日期晚于应用生效日期（隐含的）

测试目的：确保如果今天日期晚于或等于应用生效日期，终端将不设置TVR中“应用尚未生效”位为‘1’。
终端配置：N/A。
卡片配置：——卡中存在应用生效日期；
——当前日期晚于应用生效日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位6 为‘0’（应用已经生效）。

7.7.105 SYGN064-01 当前日期等于应用生效日期（隐含的）

测试目的：确保如果当前日期晚于或等于应用生效日期，终端将不设置TVR中“应用尚未生效”位为‘1’。
终端配置：N/A。
卡片配置：——卡中存在应用生效日期；
——当前日期等于应用生效日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位6 为‘0’（应用已经生效）。

7.7.106 SYGN065-00 当前日期晚于应用失效日期

测试目的：确保如果当前日期晚于应用失效日期，终端将设置TVR中“应用已过期”位为‘1’。
终端配置：N/A。
卡片配置：当前日期晚于应用失效日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位7 为‘1’（应用已过期）。

7.7.107 SYGN066-00 当前日期早于应用失效日期（隐含的）

测试目的：确保如果当前日期早于或等于应用失效日期，终端将不设置TVR中“应用已过期”位为‘1’。
终端配置：N/A。
卡片配置：当前日期早于应用失效日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位7 为‘0’（应用未过期）。

7.7.108 SYGN066-01 当前日期等于应用失效日期（隐含的）

测试目的：确保如果当前日期早于或等于应用失效日期，终端将不设置TVR中“应用已过期”位为‘1’。
终端配置：N/A。
卡片配置：当前日期等于应用失效日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节2，位7 为‘0’（应用未过期）。

7.7.109 SYGN068-00 AIP 中指明支持持卡人认证

测试目的：——确保如果AIP指明卡支持持卡人认证，终端应在读应用数据之后终端行为分析之前执行持卡人认证；
——确保如果持卡人认证已执行（不管成功与否），终端都应将TSI中“持卡人认证已执行”位置‘1’；
——确保如果CVM列表的所有持卡人认证均不成功，终端应将TVR中“持卡人认证未成功”位置‘1’。
终端配置：N/A。
卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 为‘1’）；
——卡中CVM为“CVM失败，总是”（0000）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM结果为“-00 00 01”。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.110 SYGN069-00 支持 CVR 条件：总是

测试目的：确保终端支持CVM条件“总是”。
终端配置：N/A。
卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 为‘1’）；
——卡中CVM为“CVM失败，总是”（0000）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 =‘1’（持卡人认证失败）。CVM结果为“-00 00 01”。第一个GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已执行）。

7.7.111 SYGN070-00 支持 CVR 条件：如果是自助现金交易

测试目的：确保终端支持CVM条件“如果是自助现金交易”。
终端配置：——支持现金交易；
——支持自助终端。
卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 为‘1’）；
——交易类型是现金交易；

——卡中CVM为“CVM失败，如果是自助现金交易”（-00 01），之后是“CVM失败，总是”（-00 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM结果为“-00 01 01”（如果是自助现金交易，CVM失败）。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.112 SYGN070-01 支持 CVR 条件：如果是人工现金交易

测试目的：确保终端支持CVM条件“如果是人工现金交易”。

终端配置：——支持现金；

——终端是有人终端。

卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 =‘1’）；

——交易类型是现金；

——卡中CVM为“CVM失败，如果是人工现金”（-00 04），之后是“CVM失败，总是”（-00 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM结果为“-00 04 01”（如果是人工现金，CVM失败）。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.113 SYGN070-02 支持 CVR 条件：如果是返现交易

测试目的：确保终端支持CVM条件“如果是返现交易”。

终端配置：支持返现。

卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 =‘1’）；

——交易类型是返现；

——卡中CVM为“CVM失败，如果是人工现金”（-00 05），之后是“CVM失败，总是”（-00 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM结果为“-00 05 01”（如果是返现，CVM失败）。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.114 SYGN071-00 支持 CVR 条件：如果不是自助现金交易、不是人工现金交易、也不是返现交易

测试目的：确保终端支持CVM条件“如果不是自助现金交易、不是人工现金交易、也不是返现交易”。

终端配置：支持货物或服务。

卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 为‘1’）；

——卡中CVM为“CVM失败，如果不是自助现金交易、不是人工现金交易、也不是返现交易”（-00 02），之后是“CVM失败，总是”（-00 00）；

——CDOL1请求授权金额和其他金额；

——交易类型是货物和服务。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM结果为“-00 02 01”（如果不是自助现金交易、不是人工现金交易、也不是返现交易，CVM失败）。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.115 SYGN073-00 支持 CVR 条件：如果终端支持该 CVM 且 CVM 为脱机 PIN

测试目的：确保终端支持CVM条件“如果终端支持该CVM”且CVM类型为脱机PIN。
终端配置：支持脱机明文 PIN。
卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 = ‘1’）；
——卡中CVM为“执行明文PIN校验，如果终端支持该CVM”（01 03）；
——持卡人输入错误的PIN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为 ‘1’（持卡人认证失败）。CVM结果为“01 03 01”。第一个GENERATE AC的TSI字节1，位7 为 ‘1’（持卡人认证已执行）。

7.7.116 SYGN074-00 支持 CVR 条件：如果终端支持该 CVM 且 CVM 为联机 PIN

测试目的：确保终端支持CVM条件“如果终端支持该CVM”且CVM类型为联机PIN。
终端配置：支持联机加密 PIN。
卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 为‘1’）；
——卡中CVM为“执行联机密文PIN校验，如果终端支持该CVM”（02 03）；
——持卡人输入有效的PIN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证成功）。第一个GENERATE AC的TVR字节3，位3 为‘1’（输入联机PIN）。加密PIN数据在授权请求报文中上送。CVM结果为“02 03 00”。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.117 SYGN075-00 支持 CVR 条件：如果终端支持该 CVM，CVM 为签名

测试目的：确保终端支持CVM条件“如果终端支持该CVM”且CVM类型为签名。
终端配置：支持签名。
卡片配置：——卡中的AIP指明支持持卡人认证 （AIP 字节1，位5 为‘1’）；
——卡中CVM为“签名，如果终端支持该CVM”（1E 03）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证成功）。CVM结果为“1E 03 00”。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.118 SYGN077-00 支持 CVR 条件：如果交易以应用货币进行且金额小于 X，而实际交易金额小于 X

测试目的：当实际交易金额小于 X 时确保终端支持 CVM 条件“如果交易以应用货币进行且金额小于 X”。
终端配置：支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额小于X，CVM失败”（-00 06）
接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额小于X；
——交易货币代码=应用货币代码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果为-00 06 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.119 SYGN077-01 支持CVR条件：如果交易以应用货币进行且金额小于X， 而实际交易金额大于X

测试目的：当实际交易金额大于X时确保终端支持CVM条件“如果交易以应用货币进行，金额小于X”。
终端配置：支持CVM执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额小于X， CVM失败”（-00 06）接下来是“CVM失败，总是”（-00 00）；
——CVM前已知交易金额；
——交易金额大于X；
——交易货币代码=应用货币代码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.120 SYGN077-02 支持CVR条件：如果交易以应用货币进行且金额小于X， 而实际交易金额等于X

测试目的：当实际交易金额等于X时确保终端支持CVM条件“如果交易以应用货币进行，金额小于X”。
终端配置：支持CVM执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额小于X，CVM失败”（-00 06）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额等于X；
——交易货币代码=应用货币代码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.121 SYGN078-00 支持CVR条件：如果交易以应用货币进行且金额大于X， 而实际交易金额大于X

测试目的：当实际交易金额大于X时确保终端支持CVM条件“如果交易以应用货币进行，金额大于X”。
终端配置：支持CVM执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额大于X，CVM失败”（-00 07）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额大于X；
——交易货币代码=应用货币代码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 07 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.122 SYGN078-01 支持CVR条件：如果交易以应用货币进行且金额大于X， 而实际交易金额小于X

测试目的：当实际交易金额小于 X 时确保终端支持 CVM 条件“如果交易以应用货币进行，金额大于 X”。

终端配置：支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额大于X，CVM失败”（-00 07）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额小于X；
——交易货币代码=应用货币代码。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC 的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.123 SYGN078-02 支持 CVR 条件：如果交易以应用货币进行且金额大于 X， 而实际交易金额等于 X

测试目的：当实际交易金额等于 X 时确保终端支持 CVM 条件“如果交易以应用货币进行，金额大于 X”。

终端配置：支持 CVM 执行前已知交易金额。

卡片配置：——卡中 AIP 指明支持持卡人认证（AIP 字节 1，位 5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额大于X， CVM失败”（-00 07）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额等于X；
——交易货币代码=应用货币代码。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC 的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.124 SYGN079-00 支持 CVR 条件：如果交易以应用货币进行且金额小于 Y， 而实际交易金额小于 Y

测试目的：当实际交易金额小于 Y 时确保终端支持 CVM 条件“如果交易以应用货币进行，金额小于 Y”。

终端配置：支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额小于Y， CVM失败”（-00 08）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额小于Y；
——交易货币代码=应用货币代码。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 08 01。第一个 GENERATE AC 的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.125 SYGN079-01 支持 CVR 条件：如果交易以应用货币进行且金额小于 Y， 而实际交易金额大于 Y

测试目的：当实际交易金额大于 Y 时确保终端支持 CVM 条件“如果交易以应用货币进行，金额小于 Y”。

终端配置：支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额小于Y，CVM失败”（-00 08）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额大于Y；
——交易货币代码=应用货币代码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC 的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.126 SYGN079-02 支持 CVR 条件：如果交易以应用货币进行且金额小于 Y， 而实际交易金额等于 Y

测试目的：当实际交易金额等于 Y 时确保终端支持 CVM 条件“如果交易以应用货币进行，金额小于 Y”。
终端配置：支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额小于Y，CVM失败”（-00 08）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额等于Y；
——交易货币代码=应用货币代码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC 的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.127 SYGN080-00 支持 CVR 条件：如果交易以应用货币进行且金额大于 Y， 而实际交易金额大于 Y

测试目的：当实际交易金额大于 Y 时确保终端支持 CVM 条件“如果交易以应用货币进行，金额大于 Y”。
终端配置：支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额大于Y，CVM失败”（-00 09）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额大于Y；
——交易货币代码=应用货币代码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 09 01。第一个 GENERATE AC 的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.128 SYGN080-01 支持 CVR 条件：如果交易以应用货币进行且金额大于 Y， 而实际交易金额等于 Y

测试目的：当实际交易金额等于 Y 时确保终端支持 CVM 条件“如果交易以应用货币进行，金额大于 Y”。
终端配置：支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；

——卡中CVM为“CVM失败，如果交易以应用货币进行，金额大于Y”（-00 09）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额等于Y；
——交易货币代码=应用货币代码。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.129 SYGN080-02 支持 CVR 条件：如果交易以应用货币进行且金额大于 Y， 而实际交易金额小于 Y

测试目的：当实际交易金额小于 Y 时确保终端支持 CVM 条件“如果交易以应用货币进行，金额大于 Y”。

终端配置：支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡中CVM为“如果交易以应用货币进行，金额大于Y， CVM失败”（-00 09）接下来是“CVM失败，总是”（-00 00）；
——CVM执行前已知交易金额；
——交易金额小于Y；
——交易货币代码=应用货币代码。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已进行）。

7.7.130 SYGN081-01 随机交易选择：随机选择中金额小于阈值

测试目的：确保终端在随机选择中交易金额小于阈值时执行随机交易选择检查。

终端配置：支持随机交易选择。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 为‘1’）；
——交易金额小于阈值；
——随机数≤TP （执行多次交易直到测试条件满足）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位5 为‘1’（交易被随机选择联机处理）。

7.7.131 SYGN081-02 随机交易选择：随机选择中金额小于阈值

测试目的：确保终端在随机选择中交易金额小于阈值时执行随机交易选择检查。

终端配置：支持随机交易选择。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 为‘1’）；
——交易金额小于阈值；
——随机数>TP （执行多次交易直到测试条件满足）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位5 为‘0’（交易未被随机选择联机处理）。

7.7.132 SYGN081-03 随机交易选择：阈值≤交易金额＜最低限额

测试目的：确保终端在随机选择中阈值≤交易金额＜最低限额时执行随机交易选择检查。

终端配置：支持随机交易选择。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 为‘1’）；

——随机数≤TP （执行多次交易直到测试条件满足）。

子类案例：——案例01：阈值=交易金额＜最低限额；

——案例02：阈值＜交易金额＜最低限额。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位5 为‘1’（交易被随机选择联机处理）。

7.7.133 SYGN081-04 随机交易选择：阈值≤交易金额＜最低限额

测试目的：确保终端在随机选择中阈值≤交易金额＜最低限额时执行随机交易选择检查。

终端配置：支持随机交易选择。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 为‘1’）；

——随机数＞TP （执行多次交易直到测试条件满足）。

子类案例：——案例01：阈值=交易金额＜最低限额；

——案例02：阈值＜交易金额＜最低限额。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位5 为‘0’（交易未被随机选择联机处理）。

7.7.134 SYGN082-01 卡中不存在 CVM 列表

测试目的：当卡中不存在 CVM 列表时，终端不将 TSI“持卡人认证已执行”位置 1；如果 AIP 支持持卡人认证而 CVM 不存在，终端将 TVR 中“IC 卡数据缺失”位置 1；如果 CVM 不存在或 CVM 条件不满足，终端将 CVM 结果字节 1 设为“无 CVM 执行”。

终端配置：N/A。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；

——卡中无CVM列表。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理并完成交易。第一个GENERATE AC的TSI字节1，位7 为‘0’（持卡人认证未执行）。第一个GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证未失败）。第一个GENERATE AC的TVR字节1，位6 为‘1’（IC卡数据缺失）。CVM结果3F 00 00。

7.7.135 SYGN083-00 持卡人认证规则的第二字节不满足

测试目的：当 CVM 列表中持卡人认证规则的第二字节不满足，终端应跳过处理下一个 CVM。当最后一个 CVM 方式执行失败时，确保终端设置 CVM 结果为失败。

如果卡片中存在 CVM 列表，确保终端应按 CVM 列表中的顺序依次执行每种 CVM 方式，直至持卡人验证执行完成。

终端配置：N/A。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；

——CVM列表是“CVM失败，子案例的条件”，后跟“CVM失败，总是”（-00 00）。

子类案例：——案例01：测试条件是自助现金（-00 01）但交易不是现金交易；

——案例02：测试条件是自助现金，终端支持人工操作（-00 01）；

——案例03：测试条件是人工现金（-00 04）但交易不是现金交易；

——案例04：测试条件是人工现金，终端支持无人操作（-00 04）；

——案例05：测试条件是返现消费（-00 05）但交易不是返现；

——案例06：测试条件是金额小于X（-00 06）但实际交易金额大于X；

——案例07：测试条件是金额大于X（-00 07）但实际交易金额小于X；

——案例08：测试条件是金额小于Y（-00 08）但实际交易金额大于Y；

——案例09：测试条件是金额大于Y（-00 09）但实际交易金额小于Y。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理并完成交易。第一个GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM结果=-00 00 01。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.136 SYGN083-01 如果没有支持的CVR条件：终端支持CVM而CVM是脱机明文PIN

测试目的：——当CVM是脱机明文PIN ，CVM条件是“如果终端支持该CVM”时，如果终端不支持脱机明文PIN，应执行下一个CVM；
——如果卡片中存在CVM列表，确保终端应按CVM列表中的顺序依次执行每种CVM方式，直至持卡人验证执行完成。

终端配置：不支持明文PIN。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是明文PIN校验，如果终端支持该CVM（01 03），后跟CVM失败，总是（-00 00）；
——CDOL1请求CVM结果。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。第一个GENERATE AC的TVR字节3，位5 为‘0’（‘要求输入PIN但PIN pad不存在或不能正常工作’不置位）。

7.7.137 SYGN083-02 如果没有支持的CVR条件：终端支持CVM而CVM是脱机密文PIN

测试目的：——当CVM是脱机密文PIN ，CVM条件是“如果终端支持该CVM”时，如果终端不支持脱机密文PIN，应执行下一个CVM；
——如果卡片中存在CVM列表，确保终端应按CVM列表中的顺序依次执行每种CVM方式，直至持卡人验证执行完成。

终端配置：不支持密文PIN。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是密文PIN校验，如果终端支持该CVM（04 03），后跟CVM失败，总是（-00 00）；
——CDOL1请求CVM结果。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。第一个 GENERATE AC的TVR字节3，位5 为‘0’（‘要求输入PIN但PIN pad不存在或不能正常工作’不置位）。

7.7.138 SYGN083-03 如果没有支持的CVR条件：如果终端支持该CVM而CVM是联机密文PIN

测试目的：当CVM是联机密文PIN ，CVM条件是“如果终端支持该CVM”时，如果终端不支持联机密文PIN，应执行下一个CVM。

终端配置：不支持联机密文PIN。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是联机密文PIN，如果终端支持该CVM（02 03），后跟CVM失败，总是（-00 00 ）；
——CDOL1请求CVM结果。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位3 为‘0’（输入联机PIN）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.139 SYGN083-04 如果没有支持的CVR条件：终端支持CVM而CVM是签名

测试目的：当CVM是签名，CVM条件是“如果终端支持该CVM”时，如果终端不支持签名，应执行下一个CVM。
终端配置：不支持签名。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 ‘1’）；
——CVM列表是签名，如果终端支持该CVM（1E 03），后跟“CVM失败，总是”（-00 00 ）；
——CDOL1请求CVM结果。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.140 SYGN083-05 如果没有支持的CVR条件：终端支持CVM而CVM是脱机明文PIN和签名

测试目的：当CVM是脱机明文PIN和签名，CVM条件是“如果终端支持该CVM”时，如果终端不支持脱机明文PIN或签名，应执行下一个CVM。
终端配置：不支持脱机明文PIN或不支持签名。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是脱机明文PIN和签名，如果终端支持该CVM（03 03），后跟“CVM失败，总是”（-00 00 ）；
——CDOL1请求CVM结果。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.141 SYGN083-06 如果没有支持的CVR条件：终端支持CVM而CVM是脱机密文PIN

测试目的：当CVM是脱机密文PIN和签名，CVM条件是“如果终端支持该CVM”时，如果终端不支持脱机密文PIN或签名，应执行下一个CVM。
终端配置：不支持密文PIN或者不支持签名。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是密文PIN校验和签名，如果终端支持该CVM（05 03），后跟CVM失败，总是（-00 00）；
——CDOL1请求CVM结果。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.142 SYGN083-07 如果没有支持的CVR条件：终端支持CVM而CVM是无需CVM

测试目的：当CVM是无需CVM，CVM条件是“如果终端支持该CVM”时，如果终端不支持无需CVM，应执行下一个CVM。
终端配置：不支持无需CVM。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是无需CVM，如果终端支持该CVM（1F 03），后跟“CVM失败，总是”（-00 00 ）；
——CDOL1请求CVM结果。
测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.143 SYGN084-00 CVM 条件中所需的 IC 卡数据缺失

测试目的：当持卡人认证条件码中所需的 IC 卡数据不存在，终端应执行下一个 CVM。
终端配置：支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是CVM失败，如果交易金额小于X（-00 06），后跟“CVM失败，总是”（-00 00 ）；
——卡中应用货币代码不存在；
——CVM执行前已知交易金额；
——交易金额小于X；
——CDOL1请求CVM结果。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.144 SYGN084-01 CVM 条件中所需的 IC 卡数据缺失（授权金额）

测试目的：当持卡人认证条件码中所需的 IC 卡数据不存在，终端应执行下一个 CVM。
终端配置：不支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是CVM失败，如果交易金额小于X（-00 06），后跟“CVM失败，总是”（-00 00 ）；
——卡中应用货币代码存在；
——交易货币代码=应用货币代码；
——CVM执行前未知交易金额；
——交易金额小于X。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.145 SYGN085-00 CVM 条件码超出终端识别范围

测试目的：当持卡人认证条件码超出终端识别范围，终端应执行下一个 CVM。
终端配置：N/A。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：——案例01：CVM列表是CVM失败（-00 0A），后跟“CVM失败，总是”（-00 00）；
——案例02：CVM列表是联机密文PIN（02 0A），后跟“CVM失败，总是”（-00 00）；
——案例03：CVM列表是脱机明文PIN和签名（03 0A），后跟“CVM失败，总是”（-00 00）；
——案例04：CVM列表是脱机密文PIN（04 0A），后跟“CVM失败，总是”（-00 00）；
——案例05：CVM列表是脱机密文PIN和签名（05 0A），后跟“CVM失败，总是”（-00 00）；
——案例06：CVM列表是（3F 0A），后跟“CVM失败，总是”（-00 00）；
——案例07：CVM列表是（07 0A），后跟“CVM失败，总是”（-00 00）。
测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.146 SYGN086-00 CVM 条件码现金交易的交易类型不满足

测试目的：当持卡人认证条件码交易类型不满足，终端应执行下一个 CVM。
终端配置：N/A。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡支持持卡人认证；
——交易类型不是现金；
——CVM条件是CVM失败，如果测试条件不满足，后跟“CVM失败，总是”。
子类案例：——案例01：终端支持自助终端，CVM条件是如果是自助现金（-00 01）；
——案例02：终端支持服务员终端，CVM条件是如果是人工现金（-00 04）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.147 SYGN086-01 CVM 终端类型不满足现金交易的持卡人验证规则

测试目的：当持卡人认证终端类型不满足，终端应执行下一个 CVM。
终端配置：N/A。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——卡支持持卡人认证；
——交易类型是现金；
——CVM列表是CVM失败，子案例中的条件，后跟“CVM失败，总是”。
子类案例：——案例01：终端支持服务员终端，CVM条件是如果是自助现金（-00 01）；
——案例02：终端支持自助终端，CVM条件是如果是人工现金（-00 04）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 00 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.148 SYGN087-00 CVM 条件码满足，测试条件是 CVM 失败

测试目的：当持卡人认证条件码交易类型满足，CVM 代码是 CVM 失败。
终端配置：N/A。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：CVM列表是CVM失败，后跟以下测试条件：
——案例01：测试条件是总是（-00 00）；
——案例02：自助终端且支持现金，测试条件是自助现金，交易是现金（-00 01）；
——案例03：测试条件是非自助现金，非人工现金，非返现，交易非现金非返现（-00 02）；
——案例04：终端是服务员终端且支持现金，测试条件是人工现金，交易是现金（-00 04）；
——案例05：测试条件是返现，交易是返现（-00 05）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（可识别的CVM）。CVM 结果=-00 XX 01。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.149 SYGN087-01 CVM 条件码满足，测试条件是 CVM 失败

测试目的：当持卡人认证条件码交易类型满足，CVM 代码是 CVM 失败。
终端配置：支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额；
——交易货币代码=应用货币代码。
子类案例：CVM条件是CVM失败，后跟以下测试条件：
——案例01：CVM条件是交易金额小于X（实际交易金额小于X）（-00 06）；
——案例02：CVM条件是交易金额大于Y（实际交易金额大于Y）（-00 09）；
——案例03：CVM条件是交易金额大于X（实际交易金额大于X）（-00 07）；
——案例04：CVM条件是交易金额小于Y（实际交易金额小于Y）（-00 08）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=-00 XX 01。第一个 GENERATE AC 的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.150 SYGN087-02 CVM 条件码满足，测试条件是 CVM 失败（2）

测试目的：当 CVM 码为‘CVM 失败’且字节 1 位 7=1 时，确保终端中止 CVM 处理。
终端配置：N/A。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM列表是‘CVM失败，总是’（40 00），后续的CVM依次为‘执行脱机明文PIN验证，总是’（01 00），‘执行联机密文PIN验证，总是’（02 00），‘执行脱机明文PIN验证加签名，总是’（03 00），‘执行脱机密文PIN验证，总是’（04 00），‘执行脱机密文PIN验证加签名，总是’（05 00），‘执行签名，总是’（1E 00），‘执行NO CVM，总是’（1F 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。CVM 结果=40 00 01。第一个 GENERATE AC 的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.151 SYGN088-00 CVM 条件码满足，代码是明文 PIN 校验（终端支持明文 PIN）

测试目的：确保当CVM是明文PIN校验，CVM条件码满足，且终端支持明文PIN时执行该CVM。确保当最后一个CVM执行不成功时，终端将CVM结果设为“失败”。
终端配置：支持明文PIN。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：CVM是明文PIN，后跟测试条件满足：
——案例01：测试条件是总是（01 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（01 01）；
——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（01 04）；
——案例04：测试条件是返现交易（实际交易是返现）（01 05）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（01 02）。
测试流程：持卡人输入错误的PIN。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。终端请求输入PIN。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=01 XX 01。

7.7.152 SYGN088-01 CVM 条件码满足，代码是明文 PIN 校验（终端不支持明文 PIN）

测试目的：确保当CVM是明文PIN校验，CVM条件码满足，且终端不支持明文PIN时仍执行该CVM。
终端配置：终端不支持明文PIN。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：CVM是明文PIN，后跟测试条件满足：
——案例01：测试条件是总是（01 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（01 01）；
——案例03：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（01 02）；
——案例04：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（01 04）；
——案例05：测试条件是返现交易（实际交易是返现）（01 05）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（可识别的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.153 SYGN088-02 CVM条件码满足，代码是明文PIN校验（终端支持明文PIN）（2）

测试目的：确保当CVM是明文PIN校验，CVM条件码满足，且终端支持明文PIN时执行该CVM。
终端配置：支持明文PIN，且支持CVM执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额。
子类案例：CVM是明文PIN，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（01 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（01 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（01 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（01 08）。
测试流程：持卡人输入有效PIN。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。终端请求输入PIN。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=01 XX 01。

7.7.154 SYGN088-03 CVM条件码满足，代码是明文PIN校验（终端不支持明文PIN）（2）

测试目的：确保当CVM是明文PIN校验，CVM条件码满足，且终端不支持明文PIN时仍执行该CVM。
终端配置：终端不支持明文PIN，且支持CVM执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额。
子类案例：CVM是明文PIN，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（01 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（01 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（01 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（01 08）。
测试流程：持卡人输入有效PIN。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’

（要求输入PIN，但密码键盘不存在或工作不正常）（当终端不支持密文PIN时）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。第一个 GENERATE AC的TVR字节3，位7 为‘0’（可识别的CVM）。

7.7.155 SYGN089-00 CVM 条件码满足，代码是联机密文 PIN 校验（终端支持联机密文 PIN）

测试目的：确保当 CVM 是联机密文 PIN 校验，CVM 条件码满足，且终端支持联机密文 PIN 时执行该 CVM。确保当最后一个 CVM 执行不成功时终端将 CVM 结果设为“失败”。

终端配置：支持联机密文 PIN。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。

子类案例：CVM是联机密文PIN，后跟测试条件满足：

——案例01：测试条件是总是（02 00）；

——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（02 01）；

——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（02 04）；

——案例04：测试条件是返现交易（实际交易是返现）（02 05）；

——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（02 02）。

测试流程：持卡人输入有效PIN。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证成功）。第一个 GENERATE AC的TVR字节3，位3 为‘1’（输入联机PIN）。终端请求输入PIN。授权请求报文中包含密文PIN。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=02 XX 00。

7.7.156 SYGN089-01 CVM 条件码满足，代码是联机密文 PIN 校验（终端不支持联机密文 PIN）

测试目的：确保当 CVM 是联机密文 PIN 校验，CVM 条件码满足，且终端不支持联机密文 PIN 时仍执行该 CVM。

终端配置：终端不支持联机密文 PIN。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。

子类案例：CVM是联机密文PIN，后跟测试条件满足：

——案例01：测试条件是总是（02 00）；

——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（02 01）；

——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（02 04）；

——案例04：测试条件是返现交易（实际交易是返现）（02 05）；

——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（02 02）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位3 为‘0’（未输入联机PIN）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（可识别的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.157 SYGN089-02 CVM 条件码满足，代码是联机密文 PIN 校验（终端支持联机密文 PIN）（2）

测试目的：确保当 CVM 是联机密文 PIN 校验，CVM 条件码满足，且终端支持联机密文 PIN 时执行该 CVM。

终端配置：支持密文 PIN，且支持 CVM 执行前已知交易金额

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额；
——交易在应用货币下进行。

子类案例：CVM是联机密文PIN，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（02 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（02 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（02 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（02 08）。

测试流程：持卡人输入有效PIN。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证成功）。第一个 GENERATE AC的TVR字节3，位3 为‘1’（输入联机PIN）。终端请求持卡人输入PIN。授权请求报文中包含密文PIN。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=02 XX 00。

7.7.158 SYGN089-03 CVM 条件码满足，代码是联机密文 PIN 校验（终端不支持联机密文 PIN）（2）

测试目的：确保当 CVM 是联机密文 PIN 校验，CVM 条件码满足，且终端不支持联机密文 PIN 时仍执行该 CVM。

终端配置：终端不支持联机密文 PIN、支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额；
——交易在应用货币下进行。

子类案例：CVM是联机密文PIN，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（02 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（02 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（02 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（02 08）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位3 为‘0’（未输入联机PIN）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。第一个 GENERATE AC的TVR字节3，位7 为‘0’（可识别的CVM）。

7.7.159 SYGN090-00 CVM 条件码满足，代码是明文 PIN 校验和签名（终端支持明文 PIN 和签名）

测试目的：确保当 CVM 是明文 PIN 校验和签名，CVM 条件码满足，且终端支持明文 PIN 校验和签名时执行该 CVM。

终端配置：支持明文 PIN 校验和签名。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。

子类案例：CVM是明文PIN校验和签名，后跟测试条件满足：
——案例01：测试条件是总是（03 00）；

——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（03 01）；
——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（03 04）；
——案例04：测试条件是返现交易（实际交易是返现）（03 05）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（03 02）。

测试流程：输入错误的PIN。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。终端请求输入PIN。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=03 XX 01。

7.7.160 SYGN090-01 CVM 条件码满足，代码是明文 PIN 校验和签名（终端不支持明文 PIN 和签名）

测试目的：确保当 CVM 是明文 PIN 校验和签名，CVM 条件码满足，且终端不支持明文 PIN 校验或签名时仍执行该 CVM。

终端配置：终端不支持明文 PIN 校验或签名。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。

子类案例：CVM是明文PIN校验和签名，后跟测试条件满足：
——案例01：测试条件是总是（03 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（03 01）；
——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（03 04）；
——案例04：测试条件是返现交易（实际交易是返现）（03 05）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（03 02）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（可识别的CVM）。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.161 SYGN090-02 CVM 条件码满足，代码是明文 PIN 校验和签名（终端支持明文 PIN 和签名）（2）

测试目的：确保当 CVM 是明文 PIN 校验和签名，CVM 条件码满足，且终端支持明文 PIN 校验和签名时执行该 CVM。

终端配置：——支持明文 PIN 校验和签名；
——支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额。

子类案例：CVM是明文PIN校验和签名，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（03 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（03 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（03 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（03 08）。

测试流程：输入错误的PIN。

通过标准：终端应通过请求一个TC或AAC来完成交易。终端应请求持卡人输入PIN。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE

AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=03 XX 01。

7.7.162 SYGN090-03 CVM 条件码满足，代码是明文 PIN 校验和签名（终端不支持明文 PIN 和签名）（2）

测试目的：确保当 CVM 是明文 PIN 校验和签名，CVM 条件码满足，且终端不支持明文 PIN 校验或签名时仍执行该 CVM。

终端配置：——终端不支持明文 PIN 校验或签名；
——支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额。

子类案例：CVM是明文PIN校验和签名，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（03 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（03 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（03 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（03 08）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。第一个 GENERATE AC的TVR字节3，位7 为‘0’（可识别的CVM）。

7.7.163 SYGN091-01 CVM 条件码满足，代码是密文 PIN 校验

测试目的：确保当 CVM 是脱机密文 PIN 校验，CVM 条件码满足，且终端不支持脱机密文 PIN 校验时仍执行该 CVM。

终端配置：不支持脱机密文 PIN。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）。

子类案例：CVM是密文PIN校验，后跟测试条件满足：
——案例01：测试条件是总是（04 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（04 01）；
——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（04 04）；
——案例04：测试条件是返现交易（实际交易是返现）（04 05）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（04 02）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（已知的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.164 SYGN091-03 CVM 条件码满足，代码是密文 PIN 校验

测试目的：确保当 CVM 是脱机密文 PIN 校验，CVM 条件码满足，且终端不支持脱机密文 PIN 校验时仍执行该 CVM。

终端配置：——不支持脱机密文 PIN；
——支持 CVM 执行前已知交易金额。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）。

子类案例：CVM是密文PIN校验，后跟测试条件满足：

——案例01：测试条件是金额小于X（实际金额小于X）（04 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（04 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（04 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（04 08）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（已知的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.165 SYGN092-01 CVM 条件码满足，代码是密文 PIN 校验和签名

测试目的：确保当 CVM 是脱机密文 PIN 校验和签名，CVM 条件码满足，且终端不支持脱机密文 PIN 校验或签名时仍执行该 CVM。

终端配置：支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）；
——CVM执行前已知交易金额。

子类案例：CVM是密文PIN校验和签名，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（05 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（05 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（05 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（05 08）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（已知的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.166 SYGN092-03 CVM 条件码满足，代码是密文 PIN 校验和签名（2）

测试目的：确保当 CVM 是脱机密文 PIN 校验和签名，CVM 条件码满足，且终端不支持脱机密文 PIN 校验或签名时仍执行该 CVM。

终端配置：支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）；
——CVM执行前已知交易金额。

子类案例：——CVM是密文PIN校验和签名，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（05 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（05 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（05 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（05 08）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（已知的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.167 SYGN093-00 CVM 条件码满足，代码是签名（终端支持签名）

测试目的：——确保当 CVM 是签名，CVM 条件码满足，且终端支持签名时执行该 CVM；
——确保当最后一个 CVM 执行不成功时终端将 CVM 结果设为“失败”。

终端配置：支持签名。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——批准交易继续处理。
子类案例：CVM是签名，后跟测试条件满足：
——案例01：测试条件是总是（1E 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（1E 01）；
——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（1E 04）；
——案例04：测试条件是返现交易（实际交易是返现）（1E 05）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（1E 02）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 =‘0’（持卡人认证成功）。终端打印带签名线的交易凭证。第一个 GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已执行）。CVM 结果=1E XX 00。

7.7.168 SYGN093-01 CVM 条件码满足，代码是签名（终端不支持签名）

测试目的：确保当 CVM 是签名，CVM 条件码满足，且终端不支持签名时仍执行该 CVM。
终端配置：终端不支持签名。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：CVM是签名，后跟测试条件满足：
——案例01：测试条件是总是（1E 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（1E 01）；
——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（1E 04）；
——案例04：测试条件是返现交易（实际交易是返现）（1E 05）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非无人现金、非人工现金和非返现交易）（1E 02）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（已知的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.169 SYGN093-02 CVM 条件码满足，代码是签名（终端支持签名）

测试目的：确保当 CVM 是签名，CVM 条件码满足，且终端支持签名时执行该 CVM。
终端配置：支持签名，且支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额；
——批准交易继续处理。
子类案例：CVM是签名，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（1E 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（1E 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（1E 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（1E 08）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。终端打印带签名线的交易凭证。

第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=1E XX 00。

7.7.170 SYGN093-03 CVM 条件码满足，代码是签名（终端不支持签名）

测试目的：确保当 CVM 是签名，CVM 条件码满足，且终端不支持签名时仍执行该 CVM。
终端配置：不支持签名，且支持 CVM 执行前已知交易金额。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额。
子类案例：CVM是签名，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（1E 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（1E 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（1E 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（1E 08）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（已知的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.171 SYGN094-00 CVM 条件码满足，代码是无需 CVM（终端支持无需 CVM）

测试目的：确保当 CVM 是无需 CVM，CVM 条件码满足，且终端支持无需 CVM 时执行该 CVM。
终端配置：支持无需 CVM。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：CVM是无需CVM，后跟测试条件满足：
——案例01：测试条件是总是（1F 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（1F 01）；
——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（1F 04）；
——案例04：测试条件是返现交易（实际交易是返现）（1F 05）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（1F 02）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证成功）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=1F XX 02。

7.7.172 SYGN094-01 CVM 条件码满足，代码是无需 CVM（终端不支持无需 CVM）

测试目的：确保当 CVM 是无需 CVM，CVM 条件码满足，且终端不支持无需 CVM 时仍执行该 CVM。
终端配置：不支持无需 CVM。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：CVM是无需CVM，后跟测试条件满足：
——案例01：测试条件是总是（1F 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（1F 01）；
——案例03：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（1F 04）；
——案例04：测试条件是返现交易（实际交易是返现）（1F 05）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易

非自助现金、非人工现金和非返现交易）（1F 02）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位7 为‘0’（已知的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.173 SYGN094-02 CVM 条件码满足，代码是无需 CVM（终端支持无需 CVM）

测试目的：确保当 CVM 是无需 CVM，CVM 条件码满足，且终端支持无需 CVM 时执行该 CVM。

终端配置：支持无需 CVM，且支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额；
——交易货币代码=应用货币代码。

子类案例：CVM是无需CVM，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（1F 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（1F 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（1F 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（1F 08）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证成功）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=1F XX 02。

7.7.174 SYGN094-03 CVM 条件码满足，代码是无需 CVM（终端不支持无需 CVM）

测试目的：确保当 CVM 是无需 CVM，CVM 条件码满足，且终端不支持无需 CVM 时仍执行该 CVM。

终端配置：不支持无需 CVM，且支持 CVM 执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM执行前已知交易金额。

子类案例：CVM是密文PIN校验和签名，后跟测试条件满足：
——案例01：测试条件是金额小于X（实际金额小于X）（1F 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（1F 09）；
——案例03：测试条件是金额大于X（实际金额大于X）（1F 07）；
——案例04：测试条件是金额小于Y（实际金额小于Y）（1F 08）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。第一个 GENERATE AC的TVR字节3，位7 为‘0’（已知的CVM）。

7.7.175 SYGN095-00 CVM 条件码满足，代码是终端未知

测试目的：确保当 CVM 条件码满足，但终端无法识别该 CVM 时，设置 TVR“未知的 CVM”位为‘1’。

终端配置：N/A。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。

子类案例：CVM是RFU，后跟测试条件满足：
——案例01：测试条件是总是（3F 00）；
——案例02：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（3F 01）；
——案例03：CVM是RFU，总是（07 00）；

——案例04：自助终端且支持现金，测试条件是自助现金（实际交易Cash）（07 01）；
——案例05：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（07 02）；
——案例06：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（07 04）；
——案例07：测试条件是非自助现金、非人工现金和非返现交易（实际交易非自助现金、非人工现金和非返现交易）（3F 02）；
——案例08：测试条件是返现交易（实际交易是返现）（07 05）；
——案例09：服务员终端且支持现金，测试条件是人工现金（实际交易Cash）（3F 04）；
——案例10：测试条件是返现交易（实际交易是返现）（3F 05）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位7 为‘1’（未知的CVM）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.176 SYGN095-01 CVM 条件码满足，代码是终端未知

测试目的：确保当 CVM 条件码满足，但终端无法识别该 CVM 时，设置 TVR“未知的 CVM”位为‘1’。

终端配置：N/A。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。

子类案例：CVM是RFU，后跟测试条件满足：
——案例01：测试条件是金额大于X（实际金额大于X）（3F 07）；
——案例02：测试条件是金额小于Y（实际金额小于Y）（3F 08）；
——案例03：测试条件是金额小于X（实际金额小于X）（47 06）；
——案例04：测试条件是金额大于Y（实际金额大于Y）（47 09）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位7 为‘1’（未知的CVM）。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.177 SYGN096-00 CVM 执行成功

测试目的：当 CVM 执行成功，终端不将 TVR“持卡人认证失败”位置‘1’。当持卡人认证已执行（无论成功与失败），终端将 TSI“持卡人认证已执行”位置‘1’。

终端配置：支持联机密文 PIN 或签名。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM为联机密文PIN（02 03），后跟签名，总是（1E 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证成功）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。当执行联机密文PIN，CVM 结果=02 03 00。当执行签名，CVM 结果=1E 00 00。

7.7.178 SYGN096-01 CVM 执行成功

测试目的：当 CVM 执行成功，终端不将 TVR“持卡人认证失败”位置‘1’。当持卡人认证已执行（无论成功与失败），终端将 TSI“持卡人认证已执行”位置‘1’。

终端配置：支持无需 CVM。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM为无需CVM（1F 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘0’（持卡人认证成功）。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=1F 00 02。

7.7.179 SYGN096-02 CVM 执行失败，执行下一个 CVR

测试目的：如果当前 CVM 执行不成功，且该 CVM 中“如果此 CVM 失败，应用后续的”位为‘1’，终端应执行 CVM 列表中下一 CVR。
终端配置：N/A。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：——案例01：明文PIN校验总是（41 00），CVM失败（-00 00）。当终端支持脱机PIN时，输入错误PIN；
——案例02：如果终端不支持执行签名，CVM是签名总是（5E 00），CVM失败（-00 00）；
——案例03：如果终端不支持执行联机密文PIN， CVM是联机PIN总是（42 00），CVM失败（-00 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=-00 00 01。

7.7.180 SYGN097-00 CVM 执行失败且 CVM 列表中无下一个 CVR

测试目的：如果当前 CVM 执行不成功，且该 CVM 中“如果此 CVM 失败，应用后续的”位为‘1’，终端应执行 CVM 列表中下一 CVR，但如果 CVM 列表中无下一个 CVR，终端应将 TVR 中“持卡人认证失败”位置‘1’。
终端配置：N/A。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）。
子类案例：——案例01：CVM是“明文PIN总是”（41 00），当终端支持脱机PIN时，输入错误PIN；
——案例02：CVM是“CVM失败，总是”（40 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=41 00 01或CVM 结果=3F 00 01（如果终端不支持脱机明文PIN）（案例01）。CVM 结果=40 00 01（案例02）。

7.7.181 SYGN098-00 CVM 执行失败，不执行 CVM 列表中下一个 CVR

测试目的：——如果当前 CVM 执行不成功，且该 CVM 中“如果此 CVM 失败，应用后续的”位不为‘1’，终端应设置 TVR 中“持卡人认证失败”位为‘1’；
——确保终端按照在 CVM 列表中的出现顺序执行每一个认证方法。
终端配置：N/A。
卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’。
子类案例：——案例01：终端支持明文PIN校验：CVM是明文PIN校验，如果终端支持（01 03），且“如果此CVM失败，使用后续的CVR”位未置1，后跟无需CVM （1F 00），持卡人输入错误PIN；
——案例02：终端不支持签名：CVM是签名，如果终端支持（1E 00），且“如果此CVM失败，使用后续的CVR”位未置1，后跟当金额小于X时无需CVM（1F 06）；

——案例03：CVM是“CVM失败总是”（-00 00），后跟“签名总是”（1E 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=01 03 01（案例01）。CVM 结果=3F 00 01（案例02）。CVM 结果=-00 00 01（案例03）。

7.7.182 SYGN099-00 无支持的 CVR 条件：如果是自助现金交易，而交易类型非现金

测试目的：如果交易类型不是现金，CVM 条件是自助现金时终端应执行下一 CVM。

终端配置：N/A。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；

——CVM列表是：如果是自助现金CVM失败（-00 01），CVM失败总是（-00 00）。

子类案例：——案例01：支持商品，交易是商品；

——案例02：支持服务，交易是服务；

——案例03：支持返现，交易是返现；

——案例04：支持咨询，交易是咨询；

——案例05：支持转帐，交易是转帐；

——案例06：支持支付，交易是支付；

——案例07：支持管理，交易是管理；

——案例08：支持现金存款，交易是现金存款。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=-00 00 01。

7.7.183 SYGN100-00 无支持的 CVR 条件：如果非自助现金交易、非人工现金交易、非返现交易，而交易类型自助现金

测试目的：如果交易类型是自助现金，CVM 条件是非自助现金、非人工现金、非返现时终端应执行下一 CVM。

终端配置：N/A。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；

——CVM 列表是：如果是非自助现金、非人工现金、非返现时 CVM 失败（-00 02），CVM 失败总是（-00 00）。

子类案例：——案例 01：自助终端支持现金，交易是现金；

——案例 02：服务员终端支持现金，交易是现金；

——案例 03：支持返现，交易是返现。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=-00 00 01。

7.7.184 SYGN100-01 无支持的 CVR 条件：如果是人工现金交易，而交易类型非人工现金

测试目的：如果交易类型不是人工现金，CVM 条件是人工现金时终端应执行下一 CVM。

终端配置：N/A。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；

——CVM 列表是：如果是人工现金 CVM 失败（-00 04），CVM 失败，总是（-00 00）。

子类案例：——案例 01：支持商品，交易是商品；

——案例 02：支持服务，交易是服务；

——案例 03：支持返现，交易是返现；

——案例 04：支持咨询，交易是咨询；
——案例 05：支持转帐，交易是转帐；
——案例 06：支持支付，交易是支付；
——案例 07：支持管理，交易是管理；
——案例 08：支持现金存款，交易是现金存款。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=-00 00 01。

7.7.185 SYGN100-02 无支持的 CVR 条件：如果是返现交易，而交易类型非返现

测试目的：如果交易类型不是返现，CVM 条件是返现时终端应执行下一 CVM。

终端配置：N/A。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM 列表是：如果是返现 CVM 失败（-00 05），CVM 失败总是（-00 00）。

子类案例：——案例 01：支持商品，交易是商品；
——案例 02：支持服务，交易是服务；
——案例 03：支持返现，交易是返现；
——案例 04：支持咨询，交易是咨询；
——案例 05：支持转帐，交易是转帐；
——案例 06：支持支付，交易是支付；
——案例 07：支持管理，交易是管理；
——案例 08：支持现金存款，交易是现金存款。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=-00 00 01。

7.7.186 SYGN100-03 无支持的 CVR 条件：如果是自助现金交易，而交易类型非现金

测试目的：如果交易类型不是现金，CVM 条件是自助现金时终端应执行下一 CVM。

终端配置：服务员终端，支持现金。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM 列表是：如果是自助现金 CVM 失败（-00 01），CVM 失败总是（-00 00）。

子类案例：——案例 01：交易类型是非现金；
——案例 02：交易类型是现金。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=-00 00 01。

7.7.187 SYGN100-04 无支持的 CVR 条件：如果是人工现金交易，而交易类型非人工现金

测试目的：如果交易类型不是人工现金，CVM 条件是人工现金时终端应执行下一 CVM。

终端配置：支持现金。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）；
——CVM 列表是：如果是人工现金 CVM 失败（-00 04），CVM 失败总是（-00 00）。

子类案例：——案例 01：交易类型是非现金；
——案例 02：交易类型是现金。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=-00 00 01。

7.7.188 SYGN100-05 CVM 选择脱机 PIN，终端不支持脱机 PIN（1）

测试目的：如果CVM选择脱机PIN,但终端不支持脱机明文PIN和脱机密文PIN,将TVR“请求 PIN 输入，但要求输入 PIN，但密码键盘不存在或工作不正常”位置‘1’。

终端配置：不支持脱机明文 PIN 和脱机密文 PIN。

卡片配置：卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）。

子类案例：——案例01：CVM是“明文PIN校验，总是”（01 00）；
——案例 02：CVM 是“密文 PIN 校验，总是”（04 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。

7.7.189 SYGN103-00 CVM 选择脱机 PIN，终端不支持脱机 PIN（2）

测试目的：如果 CVM 选择脱机 PIN，但终端支持脱机明文 PIN，不支持脱机密文 PIN，不将 TVR“请求 PIN 输入，但要求输入 PIN，但密码键盘不存在或工作不正常”位置‘1’。

终端配置：支持脱机明文 PIN。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 为‘1’）；
——CVM 是“脱机密文 PIN 校验，总是”（04 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 为‘0’（未设置要求输入PIN,但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已执行）。CVM 结果=3F 00 01。

7.7.190 SYGN103-02 CVM 选择脱机 PIN，PIN 重试次数为 0

测试目的：如果 CVM 选择脱机 PIN，但 PIN 重试次数为 0，VERIFY 命令响应 63C0，终端将 TVR“PIN 重试次数超限”位置‘1’。

终端配置：支持脱机明文 PIN。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）；
——CVM 是“脱机明文 PIN 校验，总是”（01 00）；
——VERIFY 命令响应 63C0。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 为‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位6 为‘1’（PIN重试次数超限）。第一个 GENERATE AC的TSI字节1，位7 为‘1’（持卡人认证已进行）。CVM 结果=01 00 01。

7.7.191 SYGN107-00 CVM 选择脱机 PIN，脱机 PIN 校验成功

测试目的：如果 VERIFY 命令响应 9000，终端认为 CVM 成功，并设置 CVM 结果第 3 字节为成功。确认终端能够识别 VERIFY 命令响应数据。

终端配置：支持脱机明文 PIN。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）；
——CVM 是“脱机明文 PIN 校验，总是”（01 00）；
——VERIFY 命令响应 9000。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 =‘0’（持卡人认证成功）。第一个 GENERATE AC的TVR字节3，位6 =‘0’（PIN重试次数未超限）。第一个 GENERATE AC的TVR字节3，位5 =‘0’（未设置要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位4 =‘0’（PIN已输入）。第一个 GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已进行）。CVM 结果=01 00 02。

7.7.192 SYGN108-00 CVM 选择联机 PIN，终端不支持联机 PIN

测试目的：如果 CVM 选择联机 PIN，终端不支持联机 PIN，终端将 TVR“要求输入 PIN，但密码键盘不存在或工作不正常”位置 1。

终端配置：不支持联机密文 PIN。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）；

——CVM 是“联机密文 PIN 校验，总是”（02 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 =‘1’（持卡人认证失败）。第一个 GENERATE AC的TVR字节3，位5 =‘1’（要求输入PIN，但密码键盘不存在或工作不正常）。第一个 GENERATE AC的TVR字节3，位3 =‘0’（未输入联机PIN）。第一个 GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已进行）。CVM 结果=3F 00 01。

7.7.193 SYGN109-00 CVM 选择联机 PIN，联机 PIN 校验成功

测试目的：如果 CVM 选择联机 PIN，发卡行响应成功，终端认为 CVM 成功，确认密码键盘输出为密文 PIN，CVM 结果第 3 字节为”未知”。

终端配置：不支持联机密文 PIN。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）；

——CVM 是“联机密文 PIN 校验，总是”（02 00）；

——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 =‘0’（持卡人认证成功）。第一个 GENERATE AC的TVR字节3，位3 =‘1’（输入联机PIN）。第一个 GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已进行）。CVM 结果=02 00 00。授权或金融报文含密文PIN信息。

7.7.194 SYGN112-00 CVM 需要签名（打印），终端支持签名测试流程，CVM 结果为“未知”

测试目的：如果 CVM 选择签名，终端支持签名，终端认为 CVM 成功且设置 CVM 结果第 3 字节为“未知”。

终端配置：支持签名。

卡片配置：——卡中AIP指明支持持卡人认证（AIP字节1，位5 =‘1’）；

——CVM 是“签名，总是”（1E 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 =‘0’（持卡人认证成功）。第一个 GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已进行）。CVM 结果=1E 00 00。

7.7.195 SYGN113-00 复合 CVM：成功

测试目的：如果 CVM 需要多种方法认证（例如脱机 PIN 和签名），如果所有 CVM 均成功，终端认为 CVM 成功。

终端配置：支持明文 PIN 和签名。

卡片配置：——卡中AIP指明支持持卡人认证（AIP字节1，位5 =‘1’）；

——CVM 是“明文 PIN 校验和签名，总是”（03 00）；
——持卡人输入有效 PIN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 =‘0’（持卡人认证成功）。第一个 GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已进行）。CVM 结果=03 00 00。

7.7.196 SYGN114-00 复合 CVM：失败

测试目的：如果 CVM 需要多种方法认证（例如脱机 PIN 和签名），如果有一种方法失败，终端认为 CVM 失败。
终端配置：支持明文 PIN。
卡片配置：——卡中AIP指明支持持卡人认证（AIP字节1，位5 =1）；
——CVM 是“明文 PIN 校验和签名，总是”（03 00）。
子类案例：——案例 01：终端支持签名，PIN 输入错误；
——案例 02：终端不支持签名。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 =‘1’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已进行）。CVM 结果=03 00 01（案例01）。CVM 结果=3F 00 01（案例02）。

7.7.197 SYGN115-00 支持多重 CVR，终端至少支持一条

测试目的：确保当 CVM 列表中包括多个 CVM 时（其中至少有一个是终端支持的），终端应该执行列表中它所支持的第一个 CVM。
终端配置：N/A。
卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 =‘1’）；
——CVM 列表包括如下 CVR（至少 10 个）：如果终端支持该 CVM，联机密文 PIN（02 03）；如果终端支持该 CVM，脱机密文 PIN（04 03）；如果终端支持该 CVM，联机明文 PIN（01 03）；CVM 是签名（1E 03）；CVM 是无需 CVM（1F 03）；CDOL1 请求 CVM 结果；CVM 选择执行成功。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节3，位8 =‘0’（持卡人认证失败）。第一个 GENERATE AC的TSI字节1，位7 =‘1’（持卡人认证已进行）。CVM结果第一、二字节为支持的CVM，最后字节如果是签名或联机密文PIN为‘00’，其他为‘02’。

7.7.198 SYGN115-01 AIP 中指明支持风险管理

测试目的：如果卡支持终端风险管理，终端在读应用数据后第一个 GENERATE AC 命令前执行风险管理。
终端配置：支持频度检查和最低限额检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——交易金额大于终端最低限额；
——卡中存在连续脱机交易下限、连续脱机交易上限；
——GET DATA 命令未返回 ATC；
——CDOL1 请求最低限额和授权金额。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位8 =‘1’（交易超过最低限额）。第一个 GENERATE AC的TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节2，位4 =‘0’（非新

卡)。第一个 GENERATE AC的TVR字节1，位6 ='1'（IC卡数据缺失)。第一个GENERATE AC的TSI字节1，位4 ='1'（终端风险管理已进行)。

7.7.199 SYGN116-00 存在相同 PAN 的交易日志文件入口，终端最低限额超限

测试目的：如果卡中存在相同 PAN 的交易日志，且最近日志中相同 PAN 的交易总额大于等于终端最低限额，则终端应将 TVR"交易超过最低限额"位置'1'。

终端配置：支持最低限额检查和交易日志。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 ='1')；
——如果终端支持交易日志，卡中存在相同 PAN 的交易日志（其中一笔相同 PAN 的交易金额小于最低限额)；
——CDOL1 请求最低限额和授权金额。

子类案例：——案例 01：相同 PAN 交易总额（含返现金额）=最低限额；
——案例 02：相同 PAN 交易总额（含返现金额）> 最低限额。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位8 ='1'（交易超过最低限额)。第一个 GENERATE AC的交易金额与输入一致，相同PAN交易总额（含当笔交易)（案例01）=最低限额（案例02）> 最低限额。第一个 GENERATE AC的TSI字节1，位4 ='1'（终端风险管理已进行)。

7.7.200 SYGN119-00 存在相同 PAN 的交易日志文件入口，终端最低限额未超限

测试目的：如果卡中存在相同 PAN 的交易日志，且最近日志中相同 PAN 的交易总额小于终端最低限额，则终端不将 TVR"交易超过最低限额"位置'1'。

终端配置：支持最低限额检查和交易日志。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 ='1')；
——如果终端支持交易日志，卡中存在相同 PAN 的交易日志（另一笔相同 PAN 的交易金额小于最低限额)；
——相同 PAN 交易总额（含返现金额）< 最低限额；
——CDOL1 请求最低限额和授权金额。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位8 ='0'（交易未超过最低限额)。第一个 GENERATE AC的交易金额与输入一致，相同PAN交易总额 < 最低限额。第一个 GENERATE AC的TSI字节1，位4 ='1'（终端风险管理已进行)。

7.7.201 SYGN120-00 交易日志不存在，终端最低限额超限

测试目的：如果卡中不存在交易日志，交易金额大于或等于终端最低限额，则终端将TVR"交易超过最低限额"位置'1'。

终端配置：支持最低限额检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 ='1')；
——交易日志不存在；
——CDOL1 请求最低限额和授权金额。

子类案例：——案例 01：交易金额（含返现金额）=最低限额；
——案例 02：交易金额（含返现金额）> 最低限额。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位8 ='1'（交易超过最低限额)。第一个 GENERATE AC的交易金额与输入一致，交易金额（案例01）=最低限额交易金额（案例02）> 最低限额。第一个 GENERATE AC的TSI字节1，位4 ='1'（终端风险管理已进行)。

7.7.202 SYGN124-00 交易日志不存在，终端最低限额未超限

测试目的：如果卡中不存在交易日志，交易金额小于终端最低限额，则终端不将 TVR“交易超过最低限额”位置‘1’。
终端配置：支持最低限额检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——交易日志不存在；
——交易金额 < 最低限额（交易金额含返现金额）；
——CDOL1 请求最低限额和授权金额。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位8 =‘0’（交易未超过最低限额）。第一个 GENERATE AC的交易金额与输入一致，交易金额 < 最低限额。第一个 GENERATE AC的TSI字节1，位4 =‘1’（终端风险管理已进行）。

7.7.203 SYGN127-00 相同 PAN 的交易日志不存在，终端最低限额超限

测试目的：如果卡中不存在相同 PAN 的交易日志，交易金额大于或等于终端最低限额，则终端将 TVR“交易超过最低限额”位置‘1’。
终端配置：支持最低限额检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——相同 PAN 的交易日志不存在（前次交易是另一 PAN，交易金额小于最低限额）；
——CDOL1 请求最低限额和授权金额。
子类案例：——案例 01：交易金额（含返现金额）=最低限额；
——案例 02：交易金额（含返现金额）> 最低限额。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位8 =‘1’（交易超过最低限额）。第一个 GENERATE AC的交易金额与输入一致，交易金额（案例01）=或（案例02）> 最低限额。第一个 GENERATE AC的TSI字节1，位4 =‘1’（终端风险管理已进行）。

7.7.204 SYGN128-00 相同 PAN 的交易日志不存在，终端最低限额未超限（缺省）

测试目的：如果不存在相同 PAN 的交易日志，交易金额小于终端最低限额，则终端不将 TVR“交易超过最低限额”位置‘1’。
终端配置：支持最低限额检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——相同 PAN 的交易日志不存在（上一笔交易是另一 PAN，交易金额小于最低限额）；
——交易金额（含返现金额） < 最低限额；
——CDOL1 请求最低限额和授权金额。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位8 =‘0’（交易未超过最低限额）。第一个 GENERATE AC的交易金额与输入一致，交易金额 < 最低限额。第一个 GENERATE AC的TSI字节1，位4 =‘1’（终端风险管理已进行）。

7.7.205 SYGN137-00 卡中存在连续脱机交易下限和上限

测试目的：如果卡中存在连续脱机交易下限和上限，则终端应进行频度检查。
终端配置：支持频度检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和上限；
——GET DATA 命令取 ATC 返回‘6A88’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节2，位4 =‘0’（非新卡）。第一个 GENERATE AC的TVR字节1，位6 =‘1’（IC卡数据缺失）。

7.7.206 SYGN138-00 卡中不存在连续脱机交易下限

测试目的：如果卡中不存在连续脱机交易下限或连续脱机交易上限，则终端应不进行频度检查。

终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中不存在连续脱机交易下限。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =‘0’（未超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘0’（未超过连续脱机交易上限）。终端不执行GET DATA命令取ATC或LOATC。

7.7.207 SYGN138-01 IC 卡中缺少连续脱机交易上限

测试目的：确保当卡中没有连续脱机交易下限或连续脱机交易上限时，终端不执行频度检查。

终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中缺少连续脱机交易上限。

测试流程：选择卡片应用，执行交易。

通过标准：终端应来完成交易，请求TC或AAC。第一个 GENERATE AC的TVR字节4，位7 =‘0’（未超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘0’（未超过连续脱机交易上限）。终端应不发出GET DATA 命令来取ATC或LOATC。

7.7.208 SYGN139-00 GET DATA 命令取 ATC 和 LOATC 寄存器

测试目的：确保当终端执行频度检查时，终端使用GET DATA命令读取ATC和LOATC。

终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应该接收到两个GET DATA命令来取ATC和LOATC。

7.7.209 SYGN140-00 IC 卡中不存在 ATC 寄存器

测试目的：确保当卡在GET DATA命令的响应中没返回ATC时，终端将TVR中“超过连续脱机交易下限”和“超过连续脱机交易上限”位置为‘1’，并且不将TVR中“新卡”位置‘1’。

终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 返回状态码‘6A88’，数据中没有 ATC；
——如返回，LOATC 大于 0。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =1（超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘1’

（超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节2，位4 =‘0’（非新卡）。第一个 GENERATE AC的TVR字节1位6 =‘1’（IC卡数据缺失）。

7.7.210 SYGN140-01 IC卡中不存在LOATC寄存器 LOATC > 0

测试目的：确保当卡在GET DATA命令的响应中没返回LOATC时，终端将TVR中“超过连续脱机交易下限”位和“超过连续脱机交易上限”位置为‘1’，并且不将TVR中“新卡”位置为‘1’。

终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 返回状态码‘6A88’，数据中没有 LOATC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4位7 =‘1’（超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节2，位4 =‘0’（非新卡）。第一个 GENERATE AC的TVR字节1，位6 =‘1’（IC卡数据缺失）。

7.7.211 SYGN140-02 IC卡中 ATC < LOATC寄存器

测试目的：确保当ATC小于LOATC时，终端将TVR中“超过连续脱机交易下限”位和“超过连续脱机交易上限”位置为‘1’，并且不将TVR中“新卡”位置为‘1’。

终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——卡中的 LOATC 是‘FFFF’；
——卡中的 ATC 是‘0000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节2，位4 =‘0’（非新卡）。

7.7.212 SYGN140-03 IC卡中 ATC = LOATC

测试目的：确保当ATC等于LOATC时，终端将TVR中“超过连续脱机交易下限”位和“超过连续脱机交易上限”位置为‘1’，并且不将TVR中“新卡”位置为‘1’。

终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——卡中的 LOATC 是‘FFFF’；
——卡中的 ATC 是‘FFFF’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节2，位4 =‘0’（非新卡）。

7.7.213 SYGN140-04 IC卡中不存在ATC寄存器 - LOATC =0

测试目的：确保当卡在GET DATA命令的响应中没返回ATC时，终端将TVR中“超过连续脱机交易下限”位和“超过连续脱机交易上限”位置为‘1’，并且将TVR中“新卡”位置为‘1’（LOATC=0）。

终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——卡中的 LOATC 是‘0000’；
——GET DATA返回状态码‘6A88’，数据域中没有ATC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个 GENERATE AC的TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节2，位4 =‘1’（新卡）。第一个 GENERATE AC的TVR字节1，位6 =‘1’（IC卡数据缺失）。

7.7.214 SYGN141-00 （ATC-LOATC 寄存器）> 连续脱机交易下限

测试目的：确保当ATC和LOATC寄存器之间的差大于连续脱机交易下限时，终端将TVR中“超过连续脱机交易下限”位置为‘1’。
终端配置：支持频度检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——ATC – LOATC > 连续脱机交易下限。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =‘1’（超过连续脱机交易下限）。

7.7.215 SYGN142-00 （ATC-LOATC 寄存器）=连续脱机交易下限（缺省）

测试目的：确保当ATC和LOATC寄存器之间的差等于连续脱机交易下限时，终端应不将TVR中“超过连续脱机交易下限”位置为‘1’。
终端配置：支持频度检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——ATC – LOATC =连续脱机交易下限。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =‘0’（未超过连续脱机交易下限）。

7.7.216 SYGN143-00 （ATC-LOATC 寄存器）< 连续脱机交易下限（缺省）

测试目的：确保当ATC和LOATC寄存器之间的差小于连续脱机交易下限时，终端应不将TVR中“超过连续脱机交易下限”位置为‘1’。
终端配置：支持频度检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——ATC – LOATC < 连续脱机交易下限。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位7 =‘0’（未超过连续脱机交易下限）。

7.7.217 SYGN144-00 （ATC-LOATC 寄存器）>连续脱机交易上限

测试目的：确保当ATC和LOATC寄存器之间的差大于连续脱机交易下限时，终端将TVR中“超过连续脱机交易上限”位置为‘1’。
终端配置：支持频度检查。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——ATC – LOATC > 连续脱机交易下限。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC的TVR字节4，位6 =‘1’（超过连续脱机交易上限）。

7.7.218 SYGN145-00 （ATC-LOATC 寄存器）=连续脱机交易上限（缺省）

测试目的：确保当 ATC 和 LOATC 寄存器之间的差等于连续脱机交易上限时，终端应不将 TVR 中“超过连续脱机交易上限”位置为‘1’。
终端配置：支持频度检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——ATC – LOATC =连续脱机交易上限。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位6 =‘0’（未超过连续脱机交易上限）。

7.7.219 SYGN146-00 （ATC-LOATC 寄存器）< 连续脱机交易上限（缺省）

测试目的：确保当ATC和LOATC寄存器之间的差小于连续脱机交易上限时，终端应不将TVR中“超过连续脱机交易上限”位置为‘1’。
终端配置：支持频度检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——ATC – LOATC < 连续脱机交易上限。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节4，位6 =‘0’（未超过连续脱机交易上限）。

7.7.220 SYGN147-00 LOATC 寄存器=0

测试目的：确保当LOATC寄存器为0时，终端将TVR中“新卡”位置为‘1’。
终端配置：支持频度检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——GET DATA 返回的 LOATC 寄存器=0。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节2，位4 =‘1’（新卡）。

7.7.221 SYGN147-01 ATC 和 LOATC 寄存器=0

测试目的：确保当ATC和LOATC寄存器为0时，终端将TVR中“新卡”位置为‘1’。
终端配置：支持频度检查。
卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 =‘1’）；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——GET DATA 返回的条 ATC 和 LOATC 寄存器=0。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TVR字节2，位4 ='1'（新卡）。第一个 GENERATE AC的TVR字节4，位6 ='1'（超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节4，位7 ='1'（超过连续脱机交易下限）。

7.7.222 SYGN148-00 终端风险管理完成

测试目的：确保当终端风险管理完成时，终端将TSI中"终端风险管理已进行"位置为'1'。

终端配置：支持频度检查或支持最低限额检查或支持随机交易选择。

卡片配置：——卡中AIP指明支持终端风险管理（AIP 字节1，位4 ='1'）；
——终端支持最少一种终端风险管理；
——最低限额检查；
——随机交易选择；
——频度检查；
——卡中存在连续脱机交易下限和连续脱机交易上限；
——GET DATA 响应数据中返回 ATC 和 LOATC；
——ATC – LOATC < 连续脱机交易下限和连续脱机交易上限。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC的TSI字节1，位4 ='1'（终端风险管理已进行）。第一个 GENERATE AC的TVR字节4，位6 ='0'（未超过连续脱机交易上限）。第一个 GENERATE AC的TVR字节4，位7 ='0'（未超过连续脱机交易下限）。

7.7.223 SYGN150-00 TAC 拒绝位置为 1

测试目的：确保如果TVR中的一个位被置为'1'，TAC拒绝中相应位也被置为'1'，终端发一个GENERATE AC请求AAC。

终端配置：——TAC拒绝中的一位被置为'1'， TVR中相应的位也置'1'；
——TAC 缺省所有位置为'0'。

卡片配置：——发卡行行为代码IAC所有位设为'0'；
——卡中的 AIP 被设定为支持 TAC 中涉及的功能，并使其执行失败。

测试流程：选择卡片应用，执行交易。

通过标准：终端应完成交易。第一个 GENERATE AC命令请求AAC。

7.7.224 SYGN151-00 TAC 拒绝位置为 0（1）

测试目的：确保如果TVR中的一个位被置为'1'，TAC拒绝中相应位为'0'，终端发一个GENERATE AC请求TC。

终端配置：——支持仅脱机或支持脱机/联机能力；
——TAC 拒绝中的一位被置为'0'，TVR 相应的位被置'1'；
——TAC 联机和缺省所有位置为'0'。

卡片配置：——发卡行行为代码IAC所有位设为'0'；
——卡中的 AIP 被设定为支持 TAC 中涉及的功能，并使其执行失败。

测试流程：选择卡片应用，执行交易。

通过标准：终端应完成交易。第一个 GENERATE AC命令请求TC。

7.7.225 SYGN151-01 TAC 拒绝位置为 0（2）

测试目的：确保如果 TVR 中的一个位被置为'1'，TAC 拒绝中相应位为'0'，终端发一个 GENERATE AC 请求 ARQC。

终端配置：——支持仅联机或支持脱机/联机能力；
——TAC拒绝中的一位被置为'0'，TVR相应的位被置为'1'；
——TAC 联机和缺省所有位置为'0'。

卡片配置：——发卡行行为代码IAC缺省和拒绝所有位设为‘0’；
——发卡行行为代码 IAC 联机有一位设为‘1’，确保终端请求 ARQC；
——卡中的 AIP 被设定为支持 TAC 中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC命令请求ARQC。

7.7.226 SYGN152-00 TAC 联机处理位置为 1

测试目的：确保如果TVR中的一个位被置为‘1’，TAC联机中相应位为‘1’，并且终端有联机能力，终端应发送一个GENERATE AC请求ARQC。
终端配置：——支持脱机/联机能力；
——TAC 联机中的一位被置为‘1’，TVR 相应的位被置‘1’；
——TAC 拒绝所有位置为‘0’；
卡片配置：——发卡行行为代码IAC所有位设为‘0’；
——卡中的 AIP 被设定为支持 TAC 中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC命令请求ARQC。

7.7.227 SYGN153-00 TAC 联机处理位置为 0

测试目的：确保如果TVR中的一个位被置为‘1’，TAC联机中相应位为‘0’，并且终端有联机能力，终端应发送一个GENERATE AC请求TC。
终端配置：——支持脱机/联机能力；
——TAC 联机中的一位被置为‘0’，TVR 中相应的位被置‘1’；
——TAC 拒绝所有位置为‘0’。
卡片配置：——发卡行行为代码IAC所有位设为‘0’；
——卡中的 AIP 被设定为支持 TAC 中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。
第一个 GENERATE AC 命令请求 TC。

7.7.228 SYGN154-00 TAC 缺省处理位置为 1，并且终端不能联机

测试目的：确保如果TVR中的一个位被置为‘1’，TAC缺省中相应位为‘1’，并且终端在第一次GENERATE AC请求联机，但不能联机，终端应发送第二个GENERATE AC请求AAC。
终端配置：——支持脱机/联机能力，或（支持仅联机且支持正常行为代码处理），或（支持仅脱机且终端在第一个GENERATE AC后检查缺省行为代码）；
——支持正常的缺省行为代码处理；
——终端不能联机；
——TAC 拒绝所有位置为‘0’；
——TAC 缺省中的一位被置为‘1’，TVR 中相应的位被置‘1’。
卡片配置：——卡在第一个 GENERATE AC后返回ARQC；
——发卡行行为代码 IAC 所有位设为‘0’；
——卡中的 AIP 被设定为支持 TAC 中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。第二个 GENERATE AC命令请求AAC。

7.7.229 SYGN155-00 TAC 缺省处理位置为 0，并且终端不能联机

测试目的：确保如果TVR中的一个位被置为‘1’，IAC缺省和TAC缺省中相应位均为‘0’，并且在第一次GENERATE AC中要求联机，但终端不能联机，终端应发送第二个

GENERATE AC请求TC。

终端配置：——仅联机且支持正常的缺省行为代码处理或支持脱机/联机；
——TAC拒绝所有位置为‘0’；
——终端有联机功能但不能联机；
——TAC缺省中的一位被置为‘0’，TVR中相应的位被置‘1’。

卡片配置：——卡在第一个GENERATE AC后返回ARQC；
——发卡行行为代码IAC所有位设为0；
——卡中的AIP被设定为支持TAC中涉及的功能，并使其执行失败。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理交易直到完成。第二个 GENERATE AC命令请求TC。

7.7.230 SYGN156-00 TAC 缺省处理位置为 1，并且终端无联机能力

测试目的：确保如果TVR中的一个位被置为‘1’，TAC缺省中相应位为‘1’，并且终端无联机能力，终端跳过联机行为代码检查，发送第一次GENERATE AC请求AAC。

终端配置：——支持仅脱机且缺省行为代码先于第一个GENERATE AC ；
——TAC拒绝所有位置为‘0’；
——TAC联机所有位置为‘1’；
——TAC缺省中的一位被置为‘1’，TVR中相应的位被置‘1’。

卡片配置：——发卡行行为代码IAC所有位设为‘0’；
——卡中的AIP被设定为支持TAC中涉及的功能，并使其执行失败。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求AAC来完成交易。第一个 GENERATE AC命令请求AAC。

7.7.231 SYGN157-00 TAC 缺省处理位置为 0，并且终端无联机能力

测试目的：确保如果TVR中的一个位被置为‘1’，IAC缺省和TAC缺省中相应位为‘0’，并且终端无联机能力，终端跳过联机行为代码检查，发送第一次GENERATE AC请求TC。

终端配置：——支持仅脱机且缺省行为代码先于第一个 GENERATE AC；
——TAC拒绝所有位置为‘0’；
——TAC联机所有位置为‘1’；
——TAC缺省中的一位被置为‘0’，TVR中相应的位被置‘1’。

卡片配置：——IAC拒绝所有位置为‘0’；
——IAC缺省所有位置为‘0’；
——卡中的AIP被设定为支持TAC中涉及的功能，并使其执行失败。

测试流程：选择卡片应用，执行交易。

通过标准：第一个 GENERATE AC命令请求TC。

7.7.232 SYGN157-01 仅联机终端跳过缺省行为码处理

测试目的：确保仅联机终端请求联机，但联机无法完成时，终端跳过TAC缺省的处理。

终端配置：——仅联机且支持跳过正常的缺省行为代码处理；
——TAC拒绝所有位置为‘0’；
——TAC缺省所有位置为‘0’。

卡片配置：——IAC拒绝所有位置为‘0’；
——IAC联机所有位置为‘0’；
——IAC缺省所有位置为‘0’；
——卡在第一个GENERATE AC后返回ARQC；
——终端有联机功能但不能联机。

测试流程：选择卡片应用，执行交易。

通过标准：卡片应收到第2个GENERATE AC请求AAC。

7.7.233 SYGN158-00 终端行为分析、TVR 和 IAC 拒绝检查请求 AAC

测试目的：确保终端在第一次GENERATE AC命令之前执行行为分析。
如果终端TVR某一位被置‘1’，而IAC拒绝中的相应位也被置‘1’，终端应发送GENERATE AC请求AAC。
终端配置：TAC所有位置为0。
卡片配置：IAC拒绝有一位被置为‘1’，TVR中相应的位被置为‘1’。
IAC缺省所有位置为‘0’。
卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。
第一个 GENERATE AC 命令请求 AAC。

7.7.234 SYGN159-00 终端行为分析、TVR 和 IAC 拒绝检查请求 TC（缺省）

测试目的：——确保终端在第一次GENERATE AC命令之前执行行为分析；
——如果终端TVR某一位被置‘1’，而IAC拒绝中的相应位被置‘0’，终端应发送GENERATE AC请求TC。
终端配置：——支持仅脱机或支持脱机/联机能力；
——TAC所有位置为‘0’。
卡片配置：——IAC拒绝有一位被置为‘0’，TVR中相应的位被置为‘1’；
——IAC联机和却省所有位置为‘0’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。第一个 GENERATE AC命令请求TC。

7.7.235 SYGN159-01 终端行为分析、TVR 和 IAC 拒绝检查请求 ARQC（缺省）

测试目的：——确保终端在第一次GENERATE AC命令之前执行行为分析；
——如果终端TVR某一位被置‘1’，而IAC拒绝中的相应位被置‘0’，终端应发送GENERATE AC请求ARQC。
终端配置：——仅联机或支持脱机/联机能力；
——TAC拒绝和缺省中所有位置为‘0’；
——TAC联机有一位置为‘1’，确保终端请求ARQC。
卡片配置：——IAC拒绝有一位被置为‘0’，TVR中相应的位被置为‘1’；
——IAC联机和缺省所有位置为‘0’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC命令请求ARQC。

7.7.236 SYGN160-00 终端有联机能力，TVR 和 IAC 联机检查请求 ARQC

测试目的：确保如果TVR中的一个位被置为‘1’，IAC联机中相应位为‘1’，并且终端有联机能力，终端应发送一个GENERATE AC请求ARQC。
终端配置：——仅联机或支持脱机/联机能力；
——TAC中所有位置为‘0’。
卡片配置：——IAC拒绝和缺省所有位置为‘0’；
——IAC联机有一位被置为‘1’，TVR中相应的位被置为‘1’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC请求ARQC。

7.7.237 SYGN160-01 仅联机终端请求 ARQC，即使 TVR 和 IAC 联机 TAC 联机检查无匹配

测试目的：确保如果TVR中的一个位被置为‘1’，IAC联机中相应位为‘0’，仅联机终端应发送一个GENERATE AC请求ARQC。
终端配置：——支持仅联机；
——TAC中所有位置为‘0’；
卡片配置：——IAC中所有位置为‘0’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。
卡片收到第一个 GENERATE AC 终端请求 ARQC。

7.7.238 SYGN161-00 终端有联机能力，TVR 和 IAC 联机检查请求 TC（缺省）

测试目的：确保如果TVR中的一个位被置为‘1’，IAC联机中相应位为‘0’，并且终端有联机能力，终端应发送一个GENERATE AC请求TC。
终端配置：——支持脱机/联机；
——TAC中所有位置为‘0’。
卡片配置：——IAC拒绝和缺省所有位置为‘0’；
——IAC联机有一位被置为‘0’，TVR中相应的位被置为‘1’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。第一个 GENERATE AC命令请求TC。

7.7.239 SYGN162-00 终端不能联机，TVR 和 IAC 缺省检查请求 AAC

测试目的：确保如果TVR中的一个位被置为‘1’，IAC缺省中相应位为‘1’，并且第一次GENERATE AC中要求联机，但终端不能联机，终端应发送第二个GENERATE AC请求AAC。
终端配置：——仅联机且支持正常的缺省行为代码处理或支持脱机/联机能力；
——终端不能联机；
——TAC中所有位置为‘0’。
卡片配置：——IAC拒绝所有位置为‘0’；
——对于第一个GENERATE AC命令，卡片返回ARQC；
——IAC缺省有一位被置为‘1’，TVR中相应的位被置为‘1’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。第二个 GENERATE AC命令请求AAC。

7.7.240 SYGN163-00 终端不能联机，TVR 和缺省行为码检查请求 TC

测试目的：确保如果TVR中的一个位被置为‘1’，IAC缺省中相应位为‘0’，并且第一次GENERATE AC中要求联机，但终端不能联机，终端应发送第二个GENERATE AC请求TC。
终端配置：——仅联机且支持正常的缺省行为代码处理或支持脱机/联机能力；
——终端不能联机；
——TAC中所有位置为‘0’。
卡片配置：——IAC拒绝所有位置为‘0’；
——对于第一个GENERATE AC命令，卡片返回ARQC；
——IAC缺省有一位被置为‘0’，TVR中相应的位被置为‘1’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。第二个 GENERATE AC命令请求TC。

7.7.241 SYGN164-00 终端无联机能力，TVR 和 IAC 缺省检查请求 AAC

测试目的：确保如果TVR中的一个位被置为‘1’，IAC缺省中相应位为‘1’，并且终端无联机能力，终端跳过联机行为代码检查，发送第一次GENERATE AC请求AAC。
终端配置：——支持仅脱机且缺省行为代码先于第一个GENERATE AC；
——TAC中所有位置为‘0’。
卡片配置：——IAC拒绝所有位置为‘0’；
——IAC缺省有一位被置为‘1’，TVR中相应的位被置为‘1’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。第一个 GENERATE AC命令请求AAC。

7.7.242 SYGN165-00 终端无联机能力，TVR 和缺省行为码检查请求 TC

测试目的：确保如果TVR中的一个位被置为‘1’，IAC缺省中相应位为‘0’，并且终端无联机能力，终端跳过联机行为代码检查，发送第一次或第二次GENERATE AC请求TC。
终端配置：——支持仅脱机且缺省行为代码先于第一个GENERATE AC；
——TAC中所有位置为‘0’。
卡片配置：——IAC拒绝所有位置为‘0’；
——IAC缺省有一位被置为‘0’，TVR中相应的位被置为‘1’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。第一个GENERATE AC命令请求TC。

7.7.243 SYGN166-00 IC 卡中无 IAC 拒绝

测试目的：确保当IC卡中不存在IAC拒绝时，终端使用所有位被置为0的缺省值。
终端配置：——支持脱机/联机能力；
——TAC拒绝中所有位置为‘0’；
——TAC联机中所有位置为‘0’；
——TAC缺省中所有位置为‘0’。
卡片配置：——IAC拒绝在卡中不存在；
——IAC联机中所有位置为‘0’；
——IAC缺省所有位被置为‘0’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求TC来完成交易。第一个GENERATE AC命令请求TC。

7.7.244 SYGN166-01 终端中不存在 TAC 拒绝

测试目的：确保当终端中不存在TAC拒绝时，终端使用所有位被置为0的缺省值。
终端配置：——支持脱机/联机能力；
——TAC拒绝不存在；
——TAC联机中所有位置为‘0’；
——TAC缺省中所有位置为‘0’。
卡片配置：——IAC拒绝中所有位置为‘0’；
——IAC联机中所有位置为‘0’；
——IAC缺省所有位被置为‘0’；
——卡中的AIP被设定为支持TAC中涉及的功能，并使其执行失败。
测试流程：选择卡片应用，执行交易。通过标准：第一个 GENERATE AC命令请求TC。

7.7.245 SYGN167-00 IC 卡中不存在 IAC 联机

测试目的：确保当卡中不存在IAC联机时，终端使用所有位被置为1的缺省值。
终端配置：——支持脱机/联机能力；

——TAC联机中所有位置为‘0’；
——TAC拒绝中所有位置为‘0’；
——TAC缺省中所有位置为‘0’。

卡片配置：——卡中不存在IAC联机；
——IAC拒绝中所有位置为‘0’；
——IAC缺省所有位被置为‘0’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个 GENERATE AC命令请求ARQC。

7.7.246 SYGN167-01 终端中不存在 TAC 联机

测试目的：确保当终端中不存在TAC联机时，终端使用所有位被置为‘0’的缺省值。

终端配置：——支持仅脱机或支持脱机/联机能力；
——TAC联机不存在；
——TAC拒绝中所有位置为‘0’；
——TAC缺省中所有位置为‘0’。

卡片配置：——IAC拒绝中所有位置为‘0’；
——IAC联机中所有位置为‘0’；
——IAC缺省所有位被置为‘0’；
——卡中的AIP被设定为支持TAC中涉及的功能，并使其执行失败。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理交易直到完成。第一个 GENERATE AC命令请求密文TC。

7.7.247 SYGN168-00 IC 卡中不存在 IAC 缺省，且终端不能联机

测试目的：确保当卡中不存在IAC缺省且终端不能联机时，终端使用所有位被置为1的缺省值。

终端配置：——仅联机且支持正常的缺省行为代码处理或支持脱机/联机能力；
——TAC 缺省中所有位置为‘0’；
——TAC 拒绝中所有位置为‘0’；
——终端不能联机（例如发卡行无响应）。

卡片配置：——卡中不存在IAC缺省；
——IAC拒绝中所有位置为‘0’；
——对于第一个GENERATE AC命令，卡请求ARQC；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败。

测试流程：选择卡片应用，执行交易。

通过标准：第二个 GENERATE AC 命令请求AAC。

7.7.248 SYGN168-01 终端中不存在 TAC 缺省，且终端不能联机

测试目的：确保当终端中不存在TAC缺省时，终端使用所有位被置为‘0’的缺省值。

终端配置：——仅联机且支持正常的缺省行为代码处理或支持脱机/联机能力；
——TAC缺省不存在；
——TAC拒绝中所有位置为‘0’；
——TAC联机中所有位置为‘0’；
——终端不能联机（例如发卡行无响应）。

卡片配置：——IAC拒绝中所有位置为‘0’；
——IAC联机中所有位置为‘0’；
——IAC缺省中所有位置为‘0’；
——对于第一个GENERATE AC命令，卡请求ARQC；
——卡中的AIP被设定为支持在第二次风险管理中执行失败的功能（例如超

过最低限额）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。第二个 GENERATE AC命令请求TC。

7.7.249 SYGN169-00 IC卡中不存在IAC缺省，且终端仅脱机（1）

测试目的：确保当卡中不存在IAC缺省且终端为仅脱机时，终端使用所有位被置为‘1’的缺省值。
终端配置：——支持仅脱机且缺省行为代码先于第一个GENERATE AC；
——TAC缺省中所有位置为‘0’；
——TAC拒绝中所有位置为‘0’；
——TAC联机中所有位置为‘0’。
卡片配置：——IAC缺省在卡中不存在；
——IAC拒绝中所有位置为‘0’；
——IAC联机中所有位置为‘0’；
——AIP应被设定执行IAC涉及的功能，卡执行此功能失败（例如SDA失败后，TVR第一字节的第七位被置为‘1’）。
测试流程：选择卡片应用，执行交易。
通过标准：第一个 GENERATE AC 命令请求AAC。

7.7.250 SYGN169-02 IC卡中不存在IAC缺省，且终端仅脱机（2）

测试目的：确保当卡中不存在IAC缺省且终端仅脱机时，终端使用所有位被置为‘1’的缺省值。
终端配置：——支持仅脱机且不支持缺省行为代码先于第一个GENERATE AC；
——TAC缺省中所有位置为‘0’；
——TAC拒绝中所有位置为‘0’。
卡片配置：——IAC缺省在卡中不存在；
——IAC拒绝中所有位置为‘0’；
——IAC联机中所有位置为‘1’；
——卡中的AIP被设定为支持IAC中涉及的功能，并使其执行失败（例如SDA失败后，TVR第一字节的第七位被置为‘1’）；
——第一个GENERATE AC卡响应ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：第二个 GENERATE AC命令请求AAC。

7.7.251 SYGN170-00 卡片行为分析功能完成

测试目的：确保在卡片返回ARQC后，终端将TSI中的“卡片风险管理已进行”位设置成‘1’。
终端配置：N/A。
卡片配置：第一个 GENERATE AC命令后，卡返回ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第二个 GENERATE AC命令中TSI字节1，位6 =‘1’，（卡片风险管理已进行）。

7.7.252 SYGN175-00 GENERATE AC命令响应以一个公钥信封返回

测试目的：确保当交易符合CDA时，IC卡响应TC或ARQC，如果IC卡使用在JR/T0025.7—2013 5.3条中定义的公钥来响应GENERATE AC响应，终端应能正确解释该响应。
终端配置：支持CDA且支持仅脱机或支持仅脱机/联机。
卡片配置：——卡中AIP指明支持CDA（AIP 字节1，位7 =‘1’）；
——设定TAC和IAC，使得终端第一个 GENERATE AC请求TC；
——卡在一个公钥信封中返回GENERATE AC命令响应。

子类案例：——案例01：第一个GENERATE AC卡响应ARQC；
——案例02：第一个GENERATE AC卡响应TC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。终端应正确处理卡的响应。第一个 GENERATE AC TVR字节1，位7 =‘0’（未使用SDA）。第一个 GENERATE AC TVR字节1，位4 =‘0’（未使用DDA）。第一个 GENERATE AC TVR字节1，位3 =‘0’（CDA未执行）。在金融确认报文或批数据采集报文中TVR字节1，位3 =‘0’（CDA成功）。

7.7.253 SYGN175-01 GENERATE AC 命令响应以一个公钥信封返回

测试目的：确保当交易符合CDA时，IC卡响应ARQC，如果IC卡使用在JR/T0025.7—2013 5.3条中定义的公钥来响应GENERATE AC响应，终端应能正确解释该响应。
终端配置：支持CDA且仅联机终端且CDA总是请求，第一个GAC请求ARQC时
卡片配置：——卡中AIP指明支持CDA（AIP 字节1，位7 =‘1’）；
——设定TAC和IAC，使得终端第一个 GENERATE AC请求ARQC；
——卡在一个公钥信封中返回GENERATE AC命令响应；
——第一个 GENERATE AC命令，卡返回ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。终端应正确处理卡的响应。第一个 GENERATE AC TVR字节1，位7 =‘0’（未使用SDA）。第一个 GENERATE AC TVR字节1，位4 =‘0’（未使用DDA）。第一个 GENERATE AC TVR字节1，位3 =‘0’（CDA未执行）。在金融确认报文或批数据采集报文中TVR字节1，位3 =‘0’（CDA成功）。

7.7.254 SYGN177-00 在卡片行为分析中的通知报文（密文信息数据：通知请求）

测试目的：——验证终端正确处理卡在GENERATE AC命令响应中的通知请求（密文信息数据：请求通知）；
——确保如果在密文信息数据中“请求通知”位被设为‘1’，且交易没有被捕获时，终端创建并发送一个通知报文给发卡行；
——确保终端实时传送一个类似于授权报文或金融交易报文的联机通知。
终端配置：支持通知。
卡片配置：——卡在GENERATE AC的响应中，密文信息数据（CID）的第四位设为‘1’；
——交易没有被捕获。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个AAC来完成交易。终端应准备一个脱机通知报文，或发送一个联机通知报文。

7.7.255 SYGN178-00 联机处理功能执行

测试目的：确保当卡对第一个 GENERATE AC返回ARQC时，终端执行联机处理功能。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——第一个 GENERATE AC 返回ARQC；
——卡应设置使终端在第一个GENERATE AC中不请求AAC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。终端应准备并发送授权或金融请求报文给发卡行。

7.7.256 SYGN180-00 从发卡行接收到 IAD，AIP 中指明支持发卡行认证

测试目的：确保当卡在AIP中指明支持发卡行认证且授权响应报文中存在IAD时，终端接收到IAD后应发送一个EXTERNAL AUTHENTICATE命令。
终端配置：仅联机或支持脱机/联机能力。

卡片配置：——卡对第一个 GENERATE AC 返回ARQC；
——卡中AIP指明支持发卡行认证（AIP 字节1，位3 =‘1’）。
子类案例：——案例01：发卡行返回10个字节的IAD，有效的密文（ARPC）和2个字节私有数据；
——案例02：发卡行返回8个字节的IAD，仅包含有效的密文（ARPC）；
——案例03：发卡行返回16个字节的IAD，有效的密文（ARPC）和8个字节私有数据。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第一个GENERATE AC后接收到EXTERNAL AUTHENTICATE命令。卡接收EXTERNAL AUTHENTICATE命令的数据域应包含从发卡行返回到的IAD。

7.7.257 SYGN180-01 发卡行认证失败

测试目的：确保当终端收到EXTERNAL AUTHENTICATE命令的响应为‘6985’时，终端将TVR发卡行认证失败位置1或终止交易。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——卡的参数设置使得交易联机执行；
——卡中AIP指明支持发卡行认证（AIP 字节1，位3 =‘1’）；
——终端收到模拟后台响应的发卡行认证数据；
——EXTERNAL AUTHENTICATE命令，卡响应‘6985’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应：处理交易直到完成，且第二个 GENERATE AC命令中TVR字节5，位7 =‘1’，（发卡行认证失败）。第二个 GENERATE AC命令中TSI字节1，位5 =‘1’，（发卡行认证已进行）或者，终止交易。

7.7.258 SYGN182-00 从发卡行接收到 IAD,AIP 中指明不支持发卡行认证（第二个 GENERATE AC）

测试目的：确保当卡在AIP中指明不支持发卡行认证且授权响应报文中存在IAD时，终端不发送EXTERNAL AUTHENTICATE命令，但应接受卡请求的在CDOL2中发送IAD。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——卡对第一个GENERATE AC返ARQC；
——卡中AIP指明发卡行认证不支持（AIP 字节1，位3 =‘0’）；
——授权响应报文中包括IAD；
——CDOL2中包括IAD。
子类案例：——案例01：发卡行返回10个字节的IAD，有效的密文（ARPC）和2个字节私有数据；
——案例02：发卡行返回8个字节的IAD，仅包含有效的密文（ARPC）；
——案例03：发卡行返回16个字节的IAD，有效的密文（ARPC）和8个字节私有数据。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡在第一个 GENERATE AC命令后不应收到EXTERNAL AUTHENTICATE命令。卡接收到第二个 GENERATE AC命令中的CDOL2包含授权响应报文中的IAD。

7.7.259 SYGN183-00 未从发卡行接收到 IAD

测试目的：确保当卡在AIP中指明支持发卡行认证且授权响应报文中不存在IAD时，终端不发送EXTERNAL AUTHENTICATE命令，并将TSI中“发卡行认证已进行”位设置为‘0’。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——设置卡的参数使得交易联机进行；

——卡中AIP指明支持发卡行认证（AIP 字节1，位3 =‘1’）；
——授权响应报文中不包括IAD。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡在第一个 GENERATE AC后不应收到EXTERNAL AUTHENTICATE命令。第二个 GENERATE AC中的TSI字节1，位5 =‘0’（发卡行认证未进行）。

7.7.260 SYGN187-00 发卡行脚本可能包含多个发卡行脚本命令（1）

测试目的：——确保终端能够接收和管理包含多条命令的发卡行脚本；
——确保终端按照在脚本中出现的顺序来执行脚本命令。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包括一个标签‘71’的发卡行脚本（包含三条命令）；
——对脚本中的每一条命令，卡片返回‘9000’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前接收到授权响应中的一系列脚本命令。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，带标签‘71’的第一个发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。

7.7.261 SYGN187-01 发卡行脚本可能包含多个发卡行脚本命令（2）

测试目的：——确保终端能够接收和管理包含多条命令的发卡行脚本；
——确保终端按照在脚本中出现的顺序来执行脚本命令。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——对第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包括一个标签‘72’的发卡行脚本（包含三条命令）；
——对脚本中的每一条命令，卡片返回‘9000’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之后接收到授权响应中的一系列脚本命令。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘72’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.262 SYGN187-02 发卡行脚本可能包含多个发卡行脚本命令（3）

测试目的：——确保终端能够接收和管理包含多条命令的发卡行脚本；
——确保终端按照在脚本中出现的顺序来执行脚本命令。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包括一个标签‘71’的发卡行脚本（包含三条命令），和一个标签‘72’的发卡行脚本（包含三条命令）；
——对脚本中的每一条命令，卡片返回‘9000’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前和之后接收到授权响应中的一系列脚本命令。在金融确认报文或批数据采集

报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘71’的发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，标签‘72’的发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。

7.7.263 SYGN188-00 终端不能识别发卡行脚本命令（1）

测试目的：确保终端能够发送脚本中的非借记/贷记应用命令。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——对第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包括一个标签‘71’的发卡行脚本（包含三条非借记/贷记应用命令）；
——对脚本中的每一条命令，卡片返回‘9000’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前收到授权响应中的一系列非借记/贷记应用脚本命令。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘71’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.264 SYGN188-01 终端不能识别发卡行脚本命令（2）

测试目的：确保终端能够发送脚本中的无法识别的命令。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包括一个标签‘72’的发卡行脚本（包含三条非借记/贷记应用命令）；
——对脚本中的每一条命令，卡片返回‘9000’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之后收到授权响应中的一系列非借记/贷记应用脚本命令。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘72’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.265 SYGN188-02 终端不能识别发卡行脚本命令（3）

测试目的：确保终端能够发送脚本中的无法识别的命令。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包括一个标签‘71’的发卡行脚本（包含非借记/贷记应用三条命令），和一个标签‘72’的发卡行脚本（包含三条非借记/贷记应用命令）；
——对脚本中的每一条命令，卡片返回‘9000’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前

和之后收到授权响应中的一系列非借记/贷记应用脚本命令。在金融确认报文或批数据采集报文中TVR字节5，位5 ='0'（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 ='0'（最后一次GENERATE AC命令之前脚本处理成功）。第二个 GENERATE AC中的TSI字节1，位3 ='1'（脚本处理已进行）。在金融确认报文或批数据采集报文中，标签'71'发卡行脚本结果的字节1应被设置成'20'，脚本执行成功。在金融确认报文或批数据采集报文中，标签'72'发卡行脚本结果的字节1应被设置成'20'，脚本执行成功。

7.7.266 SYGN189-00 标签'71'的发卡行脚本执行

测试目的：——确保终端在第二个 GENERATE AC之前处理标签71的脚本；
——确保终端执行授权响应中的发卡行脚本后，将TSI中的"脚本处理已进行"位设置成'1'。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包括一个标签'71'的发卡行脚本；
——对脚本中的每一条命令，卡片返回'9000'。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个GENERATE AC之前收到授权响应中的一系列脚本命令。第二个 GENERATE AC中的TVR字节5，位6 ='0'（最后一次GENERATE AC命令之前脚本处理成功）。在金融确认报文或批数据采集报文中TVR字节5，位5 ='0'（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 ='1'（脚本处理已进行）。在金融确认报文或批数据采集报文中，标签'71'发卡行脚本结果的字节1应被设置成'20'，脚本执行成功。

7.7.267 SYGN190-00 标签'72'的发卡行脚本执行

测试目的：——确保终端在第二个 GENERATE AC之后处理标签72的发卡行脚本；
——确保终端执行授权响应中的发卡行脚本后，将TSI中的"脚本处理已进行"位设置成'1'。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包括一个标签'72'的发卡行脚本；
——对脚本中的每一条命令，卡片返回'9000'。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个GENERATE AC之后收到授权响应中的一系列脚本命令。在金融确认报文或批数据采集报文中TVR字节5，位5 ='0'（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 ='0'（最后一次GENERATE AC命令之前脚本处理未进行）。TSI字节1，位3 ='1'（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，标签'72'发卡行脚本结果的字节1应被设置成'20'，脚本执行成功。

7.7.268 SYGN191-00 发卡行脚本格式（1）

测试目的：确保终端能够识别脚本格式（一个结构数据对象包含一个脚本标识符和一系列发卡行脚本命令APDU）。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：第一个 GENERATE AC卡片返回ARQC。

子类案例：——案例01：授权响应报文中包括一个含有脚本标识符的标签'71'发卡行脚本，对脚本中的每一条命令，卡片返回'9000'；

——案例02：授权响应报文中包括一个含有长度为0脚本标识符的标签‘71’发卡行脚本，对脚本中的每一条命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个GENERATE AC之前收到授权响应中的一系列脚本命令的APDU。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘71’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.269 SYGN191-01 发卡行脚本格式（2）

测试目的：确保终端能够识别脚本格式（一个结构数据对象包含一个脚本标识符和一系列发卡行脚本命令APDU）。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：第一个 GENERATE AC卡片返回ARQC。

子类案例：——案例01：授权响应报文中包括一个含有脚本标识符的标签‘72’发卡行脚本，对脚本中的每一条命令，卡片返回‘9000’；

——案例02：授权响应报文中包括一个含有长度为0脚本标识符的标签‘72’发卡行脚本，对脚本中的每一条命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之后收到授权响应中的一系列脚本命令的APDU。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘72’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.270 SYGN192-00 发卡行脚本中的脚本标识符（1）

测试目的：确保终端能够接收和管理没有脚本标识的发卡行脚本。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；

——授权响应报文中包含一个无脚本标识符的标签‘71’发卡行脚本；

——对脚本中的每一条命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前收到授权响应中的一系列脚本命令的APDU。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘71’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.271 SYGN192-01 发卡行脚本中的脚本标识符（2）

测试目的：确保终端能够接收和管理没有脚本标识的发卡行脚本。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；

——授权响应报文中包含一个无脚本标识符的标签‘72’发卡行脚本；

——对脚本中的每一条命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之后收到授权响应中的一系列脚本命令的APDU。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘72’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.272 SYGN193-00 发卡行脚本处理（1）

测试目的：——确保终端以在授权响应中出现的顺序来处理发卡行脚本；
——确保终端能够接收和管理一个授权响应报文中包含的多个发卡行脚本；
——确保终端在发卡行脚本结果中指明脚本执行结果。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含三个标签‘71’的发卡行脚本；
——对脚本中的每一条命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前收到与授权响应报文中脚本顺序一致的脚本命令APDU。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，第一个标签‘71’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第二个标签‘71’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第三个标签‘71’发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.273 SYGN193-01 发卡行脚本处理（2）

测试目的：——确保终端以在授权响应中出现的顺序来处理发卡行脚本；
——确保终端能够接收和管理一个授权响应报文中包含的多个发卡行脚本；
——确保终端在发卡行脚本结果中指明脚本执行结果。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含三个标签‘72’的发卡行脚本；
——对脚本中的每一条命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之后收到与授权响应报文中脚本顺序一致的脚本命令APDU。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，第一个标签‘72’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第二个标签‘72’ 的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第三个标签‘72’ 的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.274 SYGN193-02 发卡行脚本处理（3）

测试目的：——确保终端以在授权响应中出现的顺序来处理发卡行脚本；
——确保终端能够接收和管理一个授权响应报文中包含的多个发卡行脚本；
——确保终端在发卡行脚本结果中指明脚本执行结果。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含四个标签‘71’的发卡行脚本和四个标签‘72’的发卡行脚本；
——对脚本中的每一条命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前和之后收到与授权响应报文中脚本顺序一致的脚本命令APDU。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，第一个标签‘71’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第二个标签‘71’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第三个标签‘71’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第四个标签‘71’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第一个标签‘72’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第二个标签‘72’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第三个标签‘72’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，第四个标签‘72’的发卡行脚本结果的字节1应被设置成‘20’，脚本执行成功。

7.7.275 SYGN194-00 发卡行脚本命令未按 TLV 格式编码以及发卡行脚本标签是‘71’

测试目的：确保如果在标签‘71’的脚本中的命令未以标签‘86’进行TLV格式编码时，终端将TVR中的“在第二个GENERATE AC命令之前脚本处理失败”位设置为‘1’。

终端配置：仅联机或支持脱机/联机能力，不支持脚本飞。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含一个标签‘71’的发卡行脚本。

子类案例：——案例01：发卡行脚本中的命令未以标签‘86’进行TLV编码；
——案例02：发卡行脚本中的命令以标签‘86’进行编码，但标签‘86’的长度值不正确。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第二个 GENERATE AC中的TVR字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘00’，脚本未被执行。

7.7.276 SYGN194-01 发卡行脚本命令未按 TLV 格式编码以及发卡行脚本标签是‘71’

测试目的：确保如果在标签‘71’的脚本中的命令未以标签‘86’进行TLV格式编码时，终端将TVR中的“在第二个GENERATE AC命令之前脚本处理失败”位设置为‘1’。

终端配置：仅联机或支持脱机/联机能力，支持脚本飞。
卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含一个标签‘71’的发卡行脚本。
子类案例：——案例01：发卡行脚本中的命令未以标签‘86’进行TLV编码；
——案例02：发卡行脚本中的命令以标签‘86’进行编码，但标签‘86’的长度值不正确。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第二个 GENERATE AC中的TVR字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。案例1：在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘00’，脚本未被执行。案例2：在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘1x’或‘00’。

7.7.277 SYGN195-00 发卡行脚本命令未按 TLV 格式编码以及发卡行脚本标签是‘72’

测试目的：确保如果在标签‘72’脚本中的命令未以标签‘86’进行TLV格式编码时，终端将TVR中的“在第二个GENERATE AC之后脚本处理失败”位设置为‘1’。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含一个标签‘72’的发卡行脚本。
子类案例：——案例01：发卡行脚本中的命令未以标签‘86’进行TLV编码；
——案例02：发卡行脚本中的命令以标签‘86’进行编码，但标签‘86’的长度值不正确。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘00’，脚本未被执行。

7.7.278 SYGN195-01 发卡行脚本命令未按 TLV 格式编码以及发卡行脚本标签是‘71’和‘72’（1）

测试目的：确保如果标签‘71’和‘72’的脚本中的命令未以标签‘86’进行TLV格式编码时，终端将TVR中的“在第二个GENERATE AC命令之后脚本处理失败”位和“在第二个GENERATE AC命令之前脚本处理失败”位设置为‘1’。
终端配置：仅联机或支持脱机/联机能力，不支持脚本飞
卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含一个标签‘71’的发卡行脚本和一个标签‘72’的发卡行脚本。
子类案例：——案例01：发卡行脚本中的命令未以标签‘86’进行TLV编码；
——案例02：发卡行脚本中的命令以标签‘86’进行编码，但标签‘86’的长度值不正确。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。第二个 GENERATE AC中的TVR字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，发卡行脚本结果字节

1应被设置成‘00’，标识为‘71’的脚本未被执行。在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘00’，标识为‘72’的脚本未被执行。

7.7.279 SYGN195-02 发卡行脚本命令未按 TLV 格式编码以及发卡行脚本标签是‘71’和‘72’（2）

测试目的：确保如果终端收到标签‘71’和‘72’的脚本，如果在标签‘72’脚本中的命令未以标签‘86’进行TLV格式编码时，终端将TVR中的“在第二个 GENERATE AC之后脚本处理失败”位设置为‘1’。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含一个标签‘71’的发卡行脚本。

子类案例：授权响应报文中包含一个标签‘72’的发卡行脚本，包括如下命令：
——案例01：发卡行脚本中的命令未以标签‘86’进行TLV编码；
——案例02：发卡行脚本中的命令以标签‘86’进行编码，但标签‘86’的长度值不正确。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。金融确认报文或批数据采集报文中TVR字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘71’的发卡行脚本结果字节1应被设置成‘2X’，脚本执行成功。在金融确认报文或批数据采集报文中，标签‘72’的发卡行脚本结果字节1应被设置成‘00’，脚本未执行。

7.7.280 SYGN195-03 发卡行脚本命令未按 TLV 格式编码以及发卡行脚本标签是‘71’和‘72’（3）

测试目的：确保如果终端收到标签‘71’和‘72’的脚本，如果在标签‘71’脚本中的命令未以标签‘86’进行TLV格式编码时，终端将TVR中的“在第二个 GENERATE AC之前脚本处理失败”位设置为‘1’。

终端配置：仅联机或脱机/联机都支持。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含一个标签‘72’ 命令的发卡行脚本。

子类案例：授权响应报文中也包含一个标签‘71’的发卡行脚本，包括如下命令：
——案例01：发卡行脚本中的命令未以标签‘86’进行TLV编码；
——案例02：发卡行脚本中的命令以标签‘86’进行编码，但标签‘86’的长度值不正确。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘71’的发卡行脚本结果的字节1应被设置成‘00’，脚本未执行。在金融确认报文或批数据采集报文中，标签‘72’的发卡行脚本结果的字节1应被设置成‘2X’，脚本执行成功。

7.7.281 SYGN195-04 发卡行脚本命令未按 TLV 格式编码以及发卡行脚本标签是‘71’和‘72’（4）

测试目的：确保如果标签‘71’和‘72’的脚本中的命令未以标签‘86’进行TLV格式编码时，

终端将TVR中的“在第二个GENERATE AC命令之后脚本处理失败”位和“在第二个GENERATE AC命令之前脚本处理失败”位设置为‘1’。

终端配置：仅联机或脱机/联机都支持，支持脚本飞。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；

——授权响应报文中包含一个标签‘71’的发卡行脚本和一个标签‘72’的发卡行脚本。

子类案例：——案例01：发卡行脚本中的命令未以标签‘86’进行TLV编码；

——案例02：发卡行脚本中的命令以标签‘86’进行编码，但标签‘86’的长度值不正确。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第二个 GENERATE AC中的TVR字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。案例1：在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘00’，标识为‘71’的脚本未被执行。案例2：在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘00’或‘1x’，标识‘71’的脚本。在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘00’或‘1x’，标识‘72’的脚本。

7.7.282 SYGN197-00 状态码中 SW1 等于‘90’‘62’或‘63’（1）

测试目的：确保当卡片返回的状态码中SW1等于‘90’‘62’或‘63’时，终端继续执行脚本中的下一条命令。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；

——授权响应报文中包含一个标签‘71’的发卡行脚本，包含以下命令：对脚本命令1，卡片返回‘9000’；对脚本命令2，卡片返回‘62XX’；对脚本命令3，卡片返回‘63XX’；对其他两个脚本命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前收到脚本中所有的命令。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。

7.7.283 SYGN197-01 状态码中 SW1 等于‘90’‘62’或‘63’（2）

测试目的：确保当卡片返回的状态码中SW1等于‘90’‘62’或‘63’时，终端继续执行脚本中的下一条命令。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；

——授权响应报文中包含一个标签‘72’的发卡行脚本，包含以下命令：对脚本命令1，卡片返回‘9000’；对脚本命令2，卡片返回‘62XX’；对脚本命令3，卡片返回‘63XX’；对其他两个脚本命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之后收到脚本中所有的命令。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。

TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。

7.7.284 SYGN197-02 状态码中 SW1 等于‘90’‘62’或‘63’（3）

测试目的：确保当卡片返回的状态码中SW1等于‘90’‘62’或‘63’时，终端继续执行脚本中的下一条命令。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；

——授权响应报文中包含一个标签‘71’的发卡行脚本，包含以下命令：对脚本命令1，卡片返回‘9000’；对脚本命令2，卡片返回‘62XX’；对脚本命令3，卡片返回‘63XX’；对其他两个脚本命令，卡片返回‘9000’；

——授权响应报文中也包含一个标签‘72’的发卡行脚本，包含以下命令：对脚本命令1，卡片返回‘9000’；对脚本命令2，卡片返回‘62XX’；对脚本命令3，卡片返回‘63XX’；对其他两个脚本命令，卡片返回‘9000’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。卡应在第二个 GENERATE AC之前和之后接收到脚本中所有的命令。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。第二个GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，标签‘71’的发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。在金融确认报文或批数据采集报文中，标签‘72’的发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。

7.7.285 SYGN199-00 状态码中 SW1 不等于‘90’‘62’或‘63’以及发卡行脚本标签为‘71’

测试目的：——确保对于标签‘71’的脚本，如果卡对脚本命令返回的状态码中SW1不等于‘90’‘62’或‘63’时，终端将TVR中的“在第二个 GENERATE AC之前脚本处理失败”位置为1；

——确保终端在发卡行脚本结果中指出脚本执行失败。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；

——授权响应报文中包含一个标签‘71’的发卡行脚本（包含三条命令）：对脚本命令1和脚本命令3（如果终端发送），卡片返回‘9000’。

子类案例：对脚本命令2，卡片返回以下状态：

——案例01：SW1SW2是‘69XX’；

——案例02：SW1SW2是‘6AXX’；

——案例03：SW1SW2是‘64XX’；

——案例04：SW1SW2是‘65XX’；

——案例05：SW1SW2是‘6DXX’；

——案例06：SW1SW2是‘6EXX’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第二个 GENERATE AC中的TVR字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。第二个 GENERATE AC中的TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘1X’，脚本执行失败，X等于2表示第二个命令失败。卡不应收到脚本命令3。

7.7.286 SYGN200-00 状态码中 SW1 不等于‘90’‘62’或‘63’以及发卡行脚本标签为‘72’

测试目的：——确保对于标签‘72’的脚本，如果卡对脚本命令返回的状态码中SW1不等于‘90’‘62’或‘63’时，终端将TVR中的“在第二个 GENERATE AC之后脚本处理失败”位置为1；
——确保终端在发卡行脚本结果中指出脚本执行失败。
终端配置：仅联机或支持脱机/联机能力。
卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文中包含一个标签‘72’的发卡行脚本（包含三条命令）：对脚本命令1和脚本命令3（如果终端发送），卡片返回‘9000’；
子类案例：对脚本命令2，卡片返回以下状态：
——案例01：SW1SW2是‘6983’；
——案例02：SW1SW2是‘6AXX’；
——案例03：SW1SW2是‘64XX’；
——案例04：SW1SW2是‘65XX’；
——案例05：SW1SW2是‘6DXX’；
——案例06：SW1SW2是‘6EXX’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。第二个 GENERATE AC中的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。TSI字节1，位3 =‘1’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理已进行）。在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘1X’，脚本执行失败，X等于2表示第二个命令失败。卡不应收到脚本命令3。

7.7.287 SYGN200-01 状态码中 SW1 不等于‘90’‘62’或‘63’以及发卡行脚本标签为‘71’和‘72’

测试目的：确保对于标签‘71’的脚本，如果卡对脚本命令返回的状态码中 SW1 不等于‘90’‘62’或‘63’时，终端将 TVR 中的“在第二个 GENERATE AC 之前脚本处理失败”位置为‘1’。对于标签‘72’的脚本，如果卡对脚本命令返回的状态码中 SW1 不等于‘90’‘62’或‘63’时，终端将 TVR 中的“在第二个 GENERATE AC 之后脚本处理失败”位置为‘1’。
终端配置：仅联机或支持脱机/联机能力。
子类案例：授权响应报文包含以下脚本：
——案例 01：脚本‘71’包含三条命令：对脚本命令 2，卡片返回‘69XX’，脚本‘72’包含两条命令，对每一条命令，卡片返回‘9000’；
——案例 02：脚本‘71’包含两条命令：对每一条命令，卡片返回‘9000’，脚本‘72’包含两条命令：对命令 1，卡片返回‘69XX’；
——案例 03：脚本‘71’包含两条命令：对命令 1，卡片返回‘6AXX’；脚本‘72’包含两条命令：对命令 1，卡片返回‘6900’；
——案例 04：脚本‘71’包含两条命令：对命令 1，卡片返回‘6AXX’；脚本‘72’包含三条命令：对命令 2，卡片返回‘6AXX’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个TC或AAC来完成交易。TVR字节5，位5 =‘1’（最后一次 GENERATE AC命令之后脚本处理失败，在批上送数据中，适用于子案例02、03、04）。TVR字节5，位5 =‘0’（最后一次 GENERATE AC命令之后脚本处理成功，在批上送数据中，适用于子案例01）。TVR字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败，在批上送数据中，适用于子案例01、03、04）。TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功，在批上送数据中，适用于子案例02）。第二个 GENERATE AC中的TSI字节1，位3 =‘1’（脚本处理已进行）。对于有错误的脚本，在金融确认报文或批

数据采集报文中，发卡行脚本结果字节1应被设置成‘1X’，X是失败命令的序号。对于正确的脚本案例，在金融确认报文或批数据采集报文中，发卡行脚本结果字节1应被设置成‘20’，脚本执行成功。在脚本中某一命令失败后，卡不应收到该脚本中的其它脚本命令。后续脚本应继续执行。

7.7.288 SYGN202-00 发卡行脚本未执行（缺省）

测试目的：确保如果在授权响应中未收到脚本时，终端不将TSI中的“脚本处理已进行”位置为‘1’。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——授权响应报文不包含任何发卡行脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第二个 GENERATE AC中的TSI字节1，位3 =‘0’（脚本处理未进行）。TSI字节1，位3 =‘0’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理未进行）。在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。第二个 GENERATE AC的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。在金融确认报文或批数据采集报文中不包含发卡行脚本结果。

7.7.289 SYGN202-01 无脚本时不执行脚本

测试目的：确保如果在授权响应中未收到脚本时，终端不将TSI中的“脚本处理已进行”位置为‘1’。

终端配置：仅联机或支持脱机/联机能力。

卡片配置：——第一个 GENERATE AC卡片返回ARQC；
——每个案例进行2笔交易。

子类案例：——案例01：第一笔交易的授权响应报文中包含脚本‘71’，第二笔交易的授权响应报文中不包含脚本；
——案例02：第一笔交易的授权响应报文中包含脚本‘72’，第二笔交易的授权响应报文中不包含脚本；
——案例03：第一笔交易的授权响应报文中包含脚本‘71’和脚本‘72’，第二笔交易的授权响应报文中不包含脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成两笔交易。第二笔交易中，第二个 GENERATE AC中的TSI字节1，位3 =‘0’（脚本处理未进行）。第二笔交易中，TSI字节1，位3 =‘0’（如果出现在金融确认报文或批数据采集报文中，表明脚本处理未进行）。第二笔交易中，在金融确认报文或批数据采集报文中TVR字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。在第二笔交易中，第二个 GENERATE AC的TVR字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。在金融确认报文或批数据采集报文中，第二笔交易不包含发卡行脚本结果。

7.7.290 SYGN203-00 当卡响应 TC 时，CDA 失败（1）

测试目的：——确保当卡响应TC，而CDA执行失败（第一个 GENERATE AC）时，终端拒绝交易；
——确保当CDA执行但不成功时，终端将TVR中“CDA失败”位设置为‘1’；
——确保终端在脱机数据认证完成后将TSI中“脱机数据认证已进行”位置为‘1’。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持CDA；
——设置TAC和IAC，确保第一次GENERATE AC请求TC；
——卡对第一个 GENERATE AC返回TC；
——数字签名无效。
测试流程：选择卡片应用，执行CDA交易完成。
通过标准：终端应拒绝交易，且不执行第二个 GENERATE AC命令。以下通过标准仅适用于当终端有存储失败交易能力时：在金融确认报文或批数据采集报文中TSI字节1，位8 =‘1’（脱机数据认证已进行）。第一个GENERATE AC的TVR字节1，位2 =‘0’（SDA未执行）。

7.7.291 SYGN203-01 当卡响应 TC 时，CDA 失败（2）

测试目的：确保当卡响应TC而CDA执行失败（第二个 GENERATE AC）时，终端拒绝交易。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个和第二个GENERATE AC中请求TC；
——终端无法联机；
——卡对第二个 GENERATE AC返回TC，数字签名无效；
——卡对第一个 GENERATE AC返回ARQC，数字签名有效。
测试流程：选择卡片应用，执行CDA交易完成。
通过标准：终端应在第二个 GENERATE AC后拒绝交易。以下通过标准仅适用于当终端有存储失败交易能力时：TSI字节1，位8 =‘1’（脱机数据认证已进行）。第一个 GENERATE AC中的TVR字节1，位7 =‘0’（未使用SDA）。第一个 GENERATE AC中的TVR字节1，位4 =‘0’（未使用DDA）。第一个 GENERATE AC中的 TVR字节1，位2 =‘0’（SDA未执行）。

7.7.292 SYGN203-02 当卡响应 TC 时，CDA 失败（3）

测试目的：确保当卡响应TC而CDA执行失败（第二个 GENERATE AC）时，终端拒绝交易。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个GENERATE AC中请求ARQC；
——卡对第二个 GENERATE AC返回TC，数字签名无效；
——发卡行响应接受；
——卡对第一个 GENERATE AC返回ARQC，数字签名有效（当请求CDA时）。
测试流程：选择卡片应用，执行CDA交易完成。
通过标准：终端应在第二个 GENERATE AC后拒绝交易。以下通过标准仅适用于当终端有存储失败交易能力时：TSI字节1，位8 =‘1’（脱机数据认证已进行）。第一个 GENERATE AC中的TVR字节1，位7 =‘0’（未使用SDA）。第一个 GENERATE AC中的TVR字节1，位4 =‘0’（未使用DDA）。第一个 GENERATE AC中的 TVR字节1，位2 = ‘0’（SDA未执行）。

7.7.293 SYGN203-03 当卡响应 TC 时，CDA 失败（4）

测试目的：确保当卡响应 TC 而 CDA 执行失败（第二个 GENERATE AC）时，终端拒绝交易。
终端配置：——支持CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；

——TAC和IAC设定，保证终端在第一个GENERATE AC中请求ARQC，在第二个GENERATE AC中请求TC；
——终端无法联机；
——卡对第二个 GENERATE AC返回TC，数字签名无效；
——卡对第一个 GENERATE AC返回ARQC，数字签名有效（当请求CDA时）。

测试流程：选择卡片应用，执行CDA交易完成。

通过标准：终端应在第二个 GENERATE AC后拒绝交易。以下通过标准仅适用于当终端有存储失败交易能力时：TSI字节1，位8 =‘1’（脱机数据认证已进行）。第一个 GENERATE AC中的TVR字节1，位7 =‘0’（未使用SDA）。第一个 GENERATE AC中的TVR字节1，位4 =‘0’（未使用DDA）。第一个 GENERATE AC中的 TVR字节1，位2 = ‘0’（SDA未执行）。

7.8 生成应用密文命令编码（SCMW）

7.8.1 SCMW001-00 第一个 GENERATE AC 的 CDOL1

测试目的：——确保终端支持有效的CDOL1；
——确保终端检查卡中存在必备的数据对象CDOL1并使用；
——确保终端能够按照CDOL1指定的数据对象建立GENERATE AC的数据域。

终端配置：N/A。

子类案例：——案例01：CDOL1包括日期、终端类型、PAN；
——案例02：CDOL1包括交易金额、终端类型、交易金额；
——案例03：CDOL1包括发卡行认证数据、交易金额。

测试流程：选择卡片应用，执行交易。

通过标准：终端应发送第一个 GENERATE AC 命令，其数据域应按照 CDOL1 要求正确编码。

7.8.2 SCMW002-00 第二个 GENERATE AC 的 CDOL2

测试目的：——确保终端支持有效的CDOL2；
——确保终端检查卡中存在必备的数据对象CDOL2并使用；
——确保终端能够按照CDOL2指定的数据对象建立GENERATE AC的数据域。

终端配置：N/A。

卡片配置：第一个 GENERATE AC返回ARQC。

子类案例：——案例01：CDOL2包括日期、终端类型、PAN；
——案例02：CDOL2包括交易金额、终端类型、交易金额；
——案例03：CDOL2包括发卡行认证数据、交易金额。

测试流程：选择卡片应用，执行交易。

通过标准：终端应发送第二个 GENERATE AC 命令，其数据域应按照 CDOL2 要求正确编码。

7.8.3 SCMW003-00 CDOL 请求一个 TC 哈希值且 TDOL 在卡中出现

测试目的：——确保终端支持有效的TDOL；
——确保如果CDOL中请求TC哈希值时，终端能够按照卡提供的TDOL计算TC哈希值。

终端配置：N/A。

卡片配置：——卡包括TDOL；
——CDOL1请求TC哈希值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应发送一个 GENERATE AC 命令，其数据域部分应包含正确的 TC 哈希值，该值由终端使用卡中的 TDOL 计算。

7.8.4 SCMW004-00 CDOL 请求一个 TC 哈希值且 TDOL 未在卡中出现

测试目的：确保如果CDOL中请求TC哈希值，且卡未提供TDOL时，终端能够按照终端中缺

省的TDOL计算TC哈希值，并将TVR中的“使用缺省TDOL”位设置为‘1’。

终端配置：——支持缺省TDOL；

——缺省TDOL值已知。

卡片配置：——卡不包括TDOL；

——CDOL1请求TC 哈希值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应发送一个 GENERATE AC 命令， 其数据域部分应包含正确的 TC 哈希值，该值由终端使用卡中的 TDOL 计算。第一个 GENERATE AC 的 TVR 字节 5，位 8 =‘1’（使用缺省的 TDOL）。

7.8.5 SCMW005-00 CDOL 请求一个 TC 哈希值且 TDOL 和缺省 TDOL 都未出现

测试目的：确保如果CDOL中请求TC哈希值，卡未提供TDOL，且终端不支持缺省TDOL时，终端能够使用没有数据对象的TDOL计算TC哈希值。

终端配置：不支持缺省TDOL。

卡片配置：——卡不包括TDOL；

——CDOL1请求TC哈希值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应发送一个 GENERATE AC 命令， 其数据域部分应包含正确的 TC 哈希值，该值由终端使用不含任何数据对象的 TDOL 计算（即哈希算法的输入为空）。第一个 GENERATE AC 的 TVR 字节 5，位 8 =‘0’（未使用缺省的 TDOL）。

7.8.6 SCMW005-01 CDOL 请求一个 TC 哈希值且 TDOL 和缺省 TDOL 都未出现

测试目的：确保如果CDOL中请求TC哈希值，卡未提供TDOL，且终端支持但不存在缺省TDOL时，终端能够使用没有数据域的TDOL计算TC哈希值。

终端配置：支持缺省TDOL但无缺省TDOL。

卡片配置：——卡不含TDOL；

——CDOL1请求TC哈希值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应发送一个 GENERATE AC 命令， 其数据域部分应包含正确的 TC 哈希值，该值由终端使用不含任何数据对象的 TDOL 计算（即哈希算法的输入为空）。第一个 GENERATE AC 的 TVR 字节 5，位 8 =‘0’（未使用缺省的 TDOL）。

7.8.7 SCMW006-00 CDOL 在第二个 GENERATE AC 中请求一个 TC 哈希值

测试目的：确保如果CDOL2中请求TC哈希值时，终端能够根据TDOL 要求使用当前的数据计算 TC哈希值。

终端配置：仅联机终端或有联机能力的脱机终端。

卡片配置：——卡包括TDOL；

——TDOL请求TSI；

——CDOL2请求TC哈希值；

——第一个 GENERATE AC卡片返回ARQC；

——支持发卡行认证并执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应发送一个 GENERATE AC 命令， 其数据域部分应包含正确的 TC 哈希值，该值由终端使用卡中的 TDOL 计算（特别的，TDOL 所请求的 TSI 应使用当前值，“发卡行认证已进行”位被置‘1’）。第一个 GENERATE AC 的 TSI 字节 1，位 5 =‘0’（发卡行认证未进行）。第二个 GENERATE AC 的 TSI 字节 1，位 5 =‘1’（发卡行认证已进行）。

7.8.8 SCMW007-00 终端在第一个 GENERATE AC 请求 TC

测试目的：确保终端在第一个 GENERATE AC请求TC时，能够接受卡响应返回的AAC或ARQC

或TC。
终端配置：仅脱机终端或有联机能力的脱机终端。
卡片配置：IAC和TAC设置以确保终端在第一个 GENERATE AC请求TC。
子类案例：——案例01：第一个 GENERATE AC卡片返回AAC；
——案例02：第一个 GENERATE AC卡片返回ARQC；
——案例03：第一个 GENERATE AC卡片返回TC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应按照接收到的密文类型来处理并完成交易。

7.8.9 SCMW008-00 终端在第一个 GENERATE AC 请求 ARQC

测试目的：确保终端在第一个 GENERATE AC请求ARQC时，终端接受卡响应中返回的AAC或ARQC。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：IAC和TAC设置使终端在第一个 GENERATE AC请求ARQC。
子类案例：——案例01：第一个 GENERATE AC卡片返回AAC；
——案例02：第一个 GENERATE AC卡片返回ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应按照接收到的密文类型来处理并完成交易。

7.8.10 SCMW009-00 终端在第一个 GENERATE AC 请求 AAC

测试目的：确保如果终端在第一个 GENERATE AC请求AAC时，终端仅接受卡响应中返回的AAC。
终端配置：N/A。
卡片配置：——IAC和TAC设置使终端在第一个 GENERATE AC请求AAC；
——第一个 GENERATE AC卡片返回AAC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应按照接收到的密文类型来处理并完成交易。

7.8.11 SCMW010-00 第一个 GENERATE AC 卡响应 ARQC

测试目的：确保第一个 GENERATE AC卡响应ARQC，并且终端有联机能力时，终端应准备并发送一个授权或金融请求报文。
终端配置：——仅联机终端或有联机能力的脱机终端；
——TAC拒绝所有位设置成‘0’。
卡片配置：——IAC拒绝所有位设置成0以确保终端在第一个 GENERATE AC中不请求AAC；
——第一个 GENERATE AC中卡响应ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应准备并发送一个授权或金融请求报文。

7.8.12 SCMW012-00 第一个 GENERATE AC 卡响应 TC

测试目的：确保第一个 GENERATE AC卡响应TC时，终端脱机批准交易。
终端配置：——仅脱机终端或有联机能力的脱机终端；
——TAC的所有位设置为‘0’。
卡片配置：——IAC所有位设置为‘0’；
——第一个 GENERATE AC卡片返回TC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应脱机批准交易。

7.8.13 SCMW013-00 第一个 GENERATE AC 卡响应 AAC

测试目的：确保第一个 GENERATE AC卡响应AAC时，终端脱机拒绝交易。
终端配置：N/A

子类案例：设置IAC和TAC，使得在第一个GENERATE AC中：
——案例01：终端请求AAC，卡响应AAC；
——案例02：终端请求ARQC，卡响应AAC；
——案例03：终端请求TC，卡响应AAC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应脱机拒绝交易。

7.8.14 SCMW015-00 第二个 GENERATE AC 终端请求 AAC

测试目的：——确保终端在第二个 GENERATE AC中请求AAC时，接受卡响应返回的AAC；
——确保如果卡对GENERATE AC命令响应拒绝（AAC）时，终端拒绝交易。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：——IAC设置使终端在第一个GENERATE AC中请求ARQC；
——后台应在授权响应中返回拒绝响应；
——第二个 GENERATE AC卡片返回AAC。
子类案例：——案例01：第二个 GENERATE AC卡片返回AAC；
——案例02：第二个 GENERATE AC卡片返回ARQC；
——案例03：第二个 GENERATE AC卡片返回TC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应拒绝交易。

7.8.15 SCMW016-00 第二个 GENERATE AC 终端请求 TC

测试目的：确保如果终端在第二个 GENERATE AC请求TC时，应接受卡响应返回的AAC或TC。
终端配置：——仅联机终端或有联机能力的脱机终端；
——TAC设置确保终端在第二个 GENERATE AC中请求TC。
卡片配置：IAC设置确保终端在第一个 GENERATE AC中请求ARQC，第二个 GENERATE AC中请求TC。
子类案例：——案例01：第二个 GENERATE AC卡片返回TC；
——案例02：第二个 GENERATE AC卡片返回AAC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应依据卡的响应拒绝或接受交易。

7.8.16 SCMW017-00 比请求的更高级的密文（1）

测试目的：确保卡在第一个 GENERATE AC中返回的密文比所请求的密文更高级时，终端终止交易。
终端配置：N/A。
子类案例：设定IAC和TAC，使得终端：
——案例 01：第一个 GENERATE AC 请求 AAC，卡片返回 TC；
——案例 02：第一个 GENERATE AC 请求 AAC，卡片返回 ARQC；
——案例 03：第一个 GENERATE AC 请求 ARQC，卡片返回 TC（终端仅联机或支持脱机/联机能力）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.8.17 SCMW018-00 比请求的更高级的密文（2）

测试目的：确保卡在第二个 GENERATE AC中返回的密文比所请求的密文更高级时，终端应完成交易并把返回的密文视为AAC。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：设置TAC和IAC，使终端在第一次GENERATE AC时，请求ARQC。
子类案例：——案例01：发卡行返回拒绝的授权响应码，使得终端请求拒绝，卡片返回

TC；
——案例02：发卡行返回拒绝的授权响应码，使得终端请求拒绝，卡片返回ARQC；
——案例03：发卡行返回批准的授权响应码，使得终端请求接受，卡片返回ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：在所有的情况下，终端应把密文视为 AAC 完成交易（拒绝交易）。

7.8.18 SCMW018-01 比请求的更高级的密文（3）

测试目的：确保卡在第二个 GENERATE AC中返回的密文比所请求的密文更高级时，终端应把返回的密文视为AAC来完成交易。
终端配置：仅脱机终端。
卡片配置：——在第一个GENERAE AC前，TAC/IAC拒绝，TAC/IAC联机和TAC/IAD缺省均与TVR无匹配位，终端请求TC，卡响应ARQC；
——在第二个GENERATE AC前，TAC/IAC缺省与TVR无匹配位，终端请求TC，卡响应ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：在所有的情况下，终端应把密文视为AAC完成交易（拒绝交易）。

7.9 IC卡中错误和缺少的数据（CQSJ）

7.9.1 CQSJ001-00 必备数据对象丢失：FCI（1）

测试目的：确保在“PSE选择”过程中的选择命令响应的FCI中缺少强制数据时，终端转到“AID列表”方式。
终端配置：支持PSE。
卡片配置：——卡内含有PSE；
——选择PSE的响应中不包含FCI标签（标签‘6F’）（缺失所有数据：TLV）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应切换成 AID 列表选择，对支持的每一个 AID 逐项发送选择命令。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.2 CQSJ001-01 必备数据对象丢失：最终选择

测试目的：确保如果在最终选择命令中，响应数据缺少必备数据对象时，终端继续最终选择。
终端配置：N/A。
子类案例：——案例01：最终选择的响应中不包含FCI标签（标签‘6F’）（缺失所有数据：TLV）；
——案例02：最终选择的响应中不包含DF名（标签‘84’）（缺失所有数据：TLV）；
——案例03：最终选择的响应中不包含FCI私有模版（标签‘A5’）（缺失所有数据：TLV）。
测试流程：选择卡片应用，执行交易。
通过标准：终端将当前最终选择的应用从候选列表中删除。终端重启最终选择过程。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.3 CQSJ001-02 必备数据对象丢失：FCI （2）

测试目的：确保SELECT ADF命令的响应数据缺少必备数据对象FCI时，终端将其从候选列表中删除。
终端配置：N/A。
卡片配置：——卡内不含有PS；

——卡与终端同时支持两个无优先级的 ADF；
——在建立候选列表时，SELECT ADF1 命令的响应数据不含 FCI（标签‘6F’）（缺失所有数据：TLV）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应使用 ADF2，并通过请求一个 TC 或 AAC 来完成交易。

7.9.4 CQSJ002-00 必备数据对象丢失：DF 名（1）

测试目的：确保如果当终端支持PSE选择，但SELECT PSE或SELECT ADF命令的响应数据中缺少必备数据对象DF名时，终端切换到AID列表方式。
终端配置：支持PSE。
卡片配置：——卡内含有PSE。
——卡在 SELECT PSE 命令的响应中不包含 DF 名（标签‘84’）（缺失所有数据：TLV）。
测试流程：卡执行PSE应用选择过程。
通过标准：终端应清除 PSE 候选列表。终端应切换成 AID 列表选择，对它所支持的每一个 AID 逐项选择。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.5 CQSJ002-01 必备数据对象丢失：DF 名（2）

测试目的：确保如果SELECT ADF命令的响应数据中缺少必备数据对象DF名时，终端应将该应用从候选列表中删除。
终端配置：N/A。
卡片配置：——卡不含PSE。
——卡与终端同时支持两个具有相同优先级的 ADF。
——在建立候选列表时，SELECT ADF1 命令的响应数据不含 DF 名(标签‘84’)（缺失所有数据：TLV）。
测试流程：卡执行应用选择。
通过标准：终端应在 ADF2 中来完成交易，请求 TC 或 AAC。

7.9.6 CQSJ003-00 必备数据对象丢失：SFI

测试目的：确保如果终端支持PSE选择，但SELECT PSE命令的响应数据中缺少必备数据对象SFI（标签‘88’）时，终端切换成AID列表方式。
终端配置：支持PSE。
卡片配置：——卡内含有PSE；
——卡在SELECT PSE命令的响应中不包含SFI（标签‘88’）（缺失所有数据：TLV）。
测试流程：卡执行PSE的应用选择过程。
通过标准：终端应清除 PSE 候选列表。终端应切换成 AID 列表选择，对它所支持的每一个 AID 逐项选择。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.7 CQSJ004-00 目录入口缺少必备数据对象：ADF 名

测试目的：确保如果终端支持PSE选择，且支付系统目录的ADF入口缺少必备数据对象ADF名（标签‘4F’）时，终端切换成AID列表方式。
终端配置：支持PSE。
卡片配置：——卡的支付体系目录中包含一个ADF入口；
——在这个入口不含ADF名（标签‘4F’）（缺失所有数据：TLV）。
测试流程：卡执行应用选择过程。
通过标准：终端应清除 PSE 候选列表。终端应切换成 AID 列表选择，对它所支持的每一个 AID 逐项选择。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.8 CQSJ005-00 目录入口缺少必备数据对象：应用标签

测试目的：确保当终端进行PSE选择时，如果ADF入口中不含必备数据对象应用标签（标签‘50’）时，终端切换成AID列表方式。
终端配置：支持PSE。
卡片配置：——卡的PSE目录文件包含一个ADF入口；
——在这个入口中不含应用标签（标签‘50’）（缺失所有数据：TLV）。
测试流程：卡执行应用选择过程。
通过标准：终端应清除 PSE 候选列表。终端应切换成 AID 列表选择，对它所支持的每一个 AID 逐项选择。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.9 CQSJ006-00 缺少必备数据对象：FCI 专有模版（1）

测试目的：确保如果SELECT PSE或SELECT ADF命令的响应数据中缺少必备数据对象FCI专有模版（标签‘A5’）时，终端切换成AID列表方式。
终端配置：支持PSE。
卡片配置：——卡内含有PSE；
——卡在SELECT PSE的响应中不包含FCI专有模版（标签‘A5’）（缺失所有数据：TLV）。
测试流程：卡执行应用选择过程。
通过标准：终端应清除 PSE 候选列表。终端应切换成 AID 列表选择，对它所支持的每一个 AID 逐项选择。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.10 CQSJ006-01 缺少必备数据对象：FCI 专有模版（2）

测试目的：确保如果在SELECT ADF命令的响应数据中缺少必备数据对象FCI专有模版（标签‘A5’）时，终端将应用从候选列表中删除。
终端配置：N/A。
卡片配置：——卡不包含PSE；
——卡与终端同时支持两个无优先级的ADF；
——在建立候选列表时， SELECT ADF1命令的响应数据不含FCI专有模版（缺失所有数据：TLV）。
测试流程：卡执行应用选择过程。
通过标准：终端应选择 ADF2 应用，并通过请求一个 TC 或 AAC 来完成交易。

7.9.11 CQSJ006-02 缺少必备数据对象：应用标签（1）

测试目的：如果在SELECT ADF命令的响应数据中缺少必备数据对象应用标签（标签‘50’）时，确保终端继续交易。
终端配置：不支持持卡人确认。
卡片配置：——卡不包含PSE；
——卡与终端支持两个ADF，ADF1具有最高优先级；
——在建立候选列表时， SELECT ADF1命令的响应数据FCI私有模版（L＝5）中不含应用标签（存在标签，但数据长度为0），只含应用优先级指示器。
测试流程：卡执行应用选择过程。
通过标准：终端应选择 ADF1 应用，并通过请求一个 TC 或 AAC 来完成交易。

7.9.12 CQSJ006-03 缺少必备数据对象：应用标签（2）

测试目的：如果在SELECT ADF命令的响应数据中缺少必备数据对象应用标签（标签‘50’）时，确保终端继续交易。
终端配置：支持持卡人确认。
卡片配置：——卡不包含PSE；
——卡与终端同时支持两个ADF；
——在建立候选列表时， SELECT ADF1命令的响应数据FCI私有模版（L＝2）

中不含应用标签（存在标签，但数据长度为0）。

测试流程：卡执行应用选择过程。

通过标准：终端应选择 ADF1 应用，并通过请求一个 TC 或 AAC 来完成交易。终端应显示候选列表给持卡人选择，候选列表包含两个应用 ADF1，ADF2 应用。

7.9.13 CQSJ007-00 缺少必备数据对象：AFL

测试目的：确保在GET PROCESSING OPTIONS命令的响应数据中缺少必备数据对象AFL时，终端终止交易。

终端配置：N/A。

子类案例：——案例01：卡对GET PROCESSING OPTIONS命令的响应格式1，且不包含AFL；

——案例02：卡对GET PROCESSING OPTIONS命令的响应格式2，且AFL值域为空（9400）；

——案例03：卡对GET PROCESSING OPTIONS命令的响应格式2，且不包含完整的TLV格式的数据对象AFL。

测试流程：选择卡中应用，执行交易。

通过标准：终端应终止交易。

7.9.14 CQSJ008-00 缺少必备数据对象：AIP

测试目的：确保在GET PROCESSING OPTIONS命令的响应数据中缺少必备数据对象AIP时，终端终止交易。

终端配置：N/A。

卡片配置：AFL长度为4个字节。

子类案例：——案例01：卡对GET PROCESSING OPTIONS命令的响应格式1，且不包含AIP；

——案例02：卡对GET PROCESSING OPTIONS命令的响应格式2，且AIP值域为空（8200）；

——案例03：卡对GET PROCESSING OPTIONS命令的响应格式2，且不包含完整的TLV格式的数据对象AIP。

测试流程：选择卡中应用，执行交易。

通过标准：终端应终止交易。

7.9.15 CQSJ009-00 缺少必备数据对象：CDOL1

测试目的：确保如果卡缺少必备数据对象CDOL1，终端应终止交易。

终端配置：N/A。

子类案例：——案例01：卡不包含CDOL1 （缺失所有数据：TLV）；

——案例02：卡包含的CDOL1的长度等于0。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应终止交易。

7.9.16 CQSJ010-00 缺少必备数据对象：CDOL2

测试目的：确保如果卡缺少必备数据对象CDOL2，终端应终止交易。

终端配置：N/A。

子类案例：——案例01：卡不包含CDOL2 （缺失所有数据：TLV）；

——案例02：卡包含的CDOL2的长度等于0。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应终止交易。

7.9.17 CQSJ011-00 缺少必备数据对象：PAN

测试目的：确保如果卡缺少必备数据对象PAN，终端应终止交易。

终端配置：N/A。

子类案例：——案例01：卡不包含PAN （缺失所有数据：TLV）；

——案例02：卡包含的PAN的长度等于0。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.18 CQSJ012-00 缺少必备数据对象：应用生效日期

测试目的：确保如果卡缺少必备数据对象应用生效日期，终端应终止交易。
终端配置：N/A。
子类案例：——案例01：卡不包含应用生效日期（缺失所有数据：TLV）；
——案例02：卡包含的应用生效日期的长度等于0。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.19 CQSJ013-00 GET DATA 未返回 ATC，且 LCOL 和 UCOL 都存在

测试目的：确保如果卡中同时存在连续脱机限制上限和连续脱机限制下限，但GET DATA命令未返回ATC时，终端将TVR中的“IC卡数据缺失”位置‘1’。
终端配置：支持频度检查。
卡片配置：——卡中的AIP指明支持TRM（AIP 字节1，位4 =‘1’）；
——连续脱机限制上限和连续脱机限制下限同时存在；
——GET DATA命令未返回ATC。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 4，位 7 =‘1’（超过连续脱机限制下限）。第一个 GENERATE AC 的 TVR 字节 4，位 6 =‘1’(超过连续脱机限制上限)。第一个 GENERATE AC 的 TVR 字节 2，位 4 =‘0’（非新卡）。

7.9.20 CQSJ014-00 GET DATA 未返回 LOATC 寄存器，且 LCOL 和 UCOL 都存在

测试目的：确保如果卡中同时存在连续脱机限制上限和连续脱机限制下限，但GET DATA命令未返回LOATC时，终端将TVR中的“IC卡数据缺失”位置‘1’。
终端配置：支持频度检查。
卡片配置：——卡中的AIP指明支持TRM（AIP 字节1，位4 =‘1’）；
——连续脱机限制上限和连续脱机限制下限同时存在；
——GET DATA命令未返回LOATC。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 4，位 7 =‘1’（超过连续脱机限制下限）。第一个 GENERATE AC 的 TVR 字节 4，位 6 =‘1’(超过连续脱机限制上限)。第一个 GENERATE AC 的 TVR 字节 2，位 4 =‘0’（非新卡）。

7.9.21 CQSJ019-00 发卡行公钥证书不存在且在 AIP 中指明支持 SDA（1）

测试目的：确保如果AIP指明支持脱机静态数据认证，但卡中缺少发卡行公钥证书时，终端应将TVR中的“IC卡数据缺失”位置‘1’。
终端配置：支持SDA。
卡片配置：——卡中的AIP指明支持脱机静态数据认证（AIP 字节1，位7 =‘1’）；
——卡中不存在发卡行公钥证书（缺失所有数据：TLV）。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’(已进行脱机数据认证)。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘1’

（ 脱机静态数据认证失败）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.22 CQSJ021-00 发卡行公钥指数不存在且在 AIP 中指明支持 SDA（2）

测试目的：确保如果AIP指明支持脱机静态数据认证，但卡中缺少发卡行公钥指数时，终端应将TVR中的“IC卡数据缺失”位置‘1’。

终端配置：支持SDA。

卡片配置：——卡中的AIP指明支持脱机静态数据认证（AIP 字节1，位7 =‘1’）；
——卡中不存在发卡行公钥指数（缺失所有数据：TLV）。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（已进行脱机数据认证）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘1’（ 脱机静态数据认证失败）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.23 CQSJ023-00 发卡行公钥余数不存在且在 AIP 中指明支持 SDA（3）

测试目的：确保如果AIP指明支持脱机静态数据认证，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端应将TVR中的“IC卡数据缺失”位置‘1’。

终端配置：支持SDA。

卡片配置：——卡中的AIP指明支持脱机静态数据认证（AIP 字节1，位7 =‘1’）；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I > N_{CA}36$。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（已进行脱机数据认证）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘1’（ 脱机静态数据认证失败）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.24 CQSJ023-01 发卡行公钥余数不存在且在 AIP 中指明支持 SDA（隐含）（4）

测试目的：确保如果AIP中指明支持脱机静态数据认证，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数不应当存在时，终端执行SDA。

终端配置：支持SDA。

卡片配置：——卡中的AIP指明支持脱机静态数据认证（AIP 字节1，位7 =‘1’）；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I < N_{CA}36$。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（SDA 成功）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘1’（脱机数据认证已进行）。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘0’（IC 卡数据未缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.25 CQSJ024-00 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（1）

测试目的：确保AIP中指明支持脱机动态数据认证，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：支持DDA。

卡片配置：——卡中的AIP指明支持脱机动态数据认证（AIP字节1，位6 =‘1’）；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I>N_{CA}36$。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（已进行脱机数据认证）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘1’（ 脱机动态数据认证失败）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。

7.9.26 CQSJ024-01 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（2）

测试目的：确保如果AIP中指明支持CDA，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。
终端配置：——支持CDA；
——仅脱机或支持脱机/联机；
——TAA前能检测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP TVR字节1，位1 =‘1’）；
——设置TAC和IAC，使得第一次GENERATE AC中请求TC；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I>N_{CA}36$。
测试流程：选择卡片中应用，执行交易。
通过标准：终端在第一个 GENERATE AC 中不请求 CDA。终端应根据 TAC 和 IAC 在设置，请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（已进行脱机数据认证）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.27 CQSJ024-02 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（隐含）（3）

测试目的：确保如果AIP中指明支持脱机动态数据认证，卡中缺少发卡行公钥余数，但恢复的发卡行公钥长度表明发卡行公钥余数应不存在时，终端执行动态数据认证。
终端配置：支持DDA。
卡片配置：——卡中的AIP指明支持脱机动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I<N_{CA}36$。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（DDA 成功）。第一个 GENERATE AC 的 TSI 字节 1，位 8 =‘1’（脱机数据认证已进行）。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘0’（IC 卡数据未缺失）。

7.9.28 CQSJ024-03 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（隐含）（4）

测试目的：确保如果AIP中指明支持CDA，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应不存在时，终端执行CDA。
终端配置：支持CDA。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I<N_{CA}36$。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应处理交易直到完成，生成一个 TC 或 AAC。在金融确认报文或批数据采集报文中包含的 TVR 字节 1，位 3 =‘0’（CDA 成功）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。在金融确认报文或批数据采集报文中包含的 TSI 字节 1，位 8 =‘1’（脱机数据认证已进行）（该通过条件仅适用于 CDA 被请求时）。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘0’（IC 卡数据未缺失）。

7.9.29 CQSJ024-04 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（5）

测试目的：确保如果AIP中指明支持CDA，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——支持仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求TC；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I > N_{CA} - 36$。

测试流程：选择卡片中应用，执行交易。

通过标准：卡片返回 TC 时，终端应拒绝交易，并且不发送第二个 GENERATE AC 命令；或当第一个 GENERATE AC 卡片响应 ARQC 时，终端发送第二个 GENERATE AC 命令请求 AAC。第二个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失），或出现在批数据采集中在 TVR（仅适用于终端有能力保存拒绝或异常终止的交易，）或终端有能力以任何形式显示 TVR 值（如：打印在凭条中）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（ 已进行脱机数据认证）。第二个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败），或出现在金融确认报文或批数据采集报文中在 TVR（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值（如：打印在凭条中）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.30 CQSJ024-05 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（6）

测试目的：确保如果AIP中指明支持CDA，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——第一个GENERATE AC命令，卡片响应ARQC；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC，在第二个GENERATE AC命令中请求TC；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I > N_{CA} - 36$。

测试流程：选择卡片中应用，执行交易。

通过标准：终端发送第二个 GENERATE AC 命令请求 AAC，拒绝交易。第二个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（ 已进行脱机数据认证）。第二个 GENERATE AC 的 TVR 字

节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（ 未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（ 未使用 DDA）。

7.9.31 CQSJ024-06 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（7）

测试目的：确保如果AIP中指明支持CDA，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——第一个GENERATE AC命令，卡片响应ARQC；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC，在第二个GENERATE AC命令中请求TC；
——发卡行批准交易；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I > N_{CA}36$。

测试流程：选择卡片中应用，执行交易。

通过标准：终端拒绝交易。TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失），包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值（如：打印在凭条中）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘1’（ 未进行脱机数据认证）。TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败），包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值(如:打印在凭条中)。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.32 CQSJ024-07 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（8）

测试目的：确保如果AIP中指明支持CDA，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——第一个GENERATE AC命令，卡片响应ARQC；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC。
——终端无法联机；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足$N_I > N_{CA}36$。

测试流程：选择卡片中应用，执行交易。

通过标准：终端拒绝交易。TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失），包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值（如：打印在凭条中）。第一个

GENERATE AC 的 TVR 字节 1，位 8 =‘1’（ 未进行脱机数据认证）。TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败），包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值(如:打印在凭条中)。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.33 CQSJ024-08 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（9）

测试目的：确保如果AIP中指明支持CDA，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC；
——终端联机批准；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足N_I>N_{CA}36。

测试流程：选择卡片中应用，执行交易。

通过标准：第一个 GENERATE AC 和第二个 GENERATE AC 均不请求 CDA。终端应完成交易，最终请求 TC。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（ 已进行脱机数据认证）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.34 CQSJ024-09 发卡行公钥余数不存在且在 AIP 中指明支持 DDA（10）

测试目的：确保如果AIP中指明支持CDA，卡中缺少发卡行公钥余数，但被恢复的发卡行公钥长度表明发卡行公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC；
——终端联机拒绝；
——卡中不存在发卡行公钥余数（缺失所有数据：TLV）；
——发卡行公钥和CA公钥的长度满足N_I>N_{CA}36。

测试流程：选择卡片中应用，执行交易。

通过标准：第一个 GENERATE AC 和第二个 GENERATE AC 均不请求 CDA。终端应完成交易，最终请求 AAC。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（ 已进行脱机数据认证）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.35 CQSJ028-00 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（1）

测试目的：确保如果AIP中指明支持脱机动态数据认证，卡中缺少IC卡公钥余数，但被恢复的IC卡公钥长度表明IC卡公钥余数应当存在时，终端将TVR中“IC卡数据

缺失”位置‘1’。

终端配置：支持DDA。

卡片配置：——卡中的AIP指明支持脱机动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中不存在IC卡公钥余数（缺失所有数据：TLV）；
——IC卡公钥和发卡行公钥的长度满足N_{ICC}>N_I42。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’(已进行脱机数据认证)。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘1’（DDA 失败）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。

7.9.36 CQSJ028-01 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（2）

测试目的：确保如果AIP中指明支持CDA，卡中缺少IC卡公钥余数，但被恢复的IC卡公钥长度表明IC卡公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求TC；
——卡中不存在IC卡公钥余数（缺失所有数据：TLV）；
——IC卡公钥和发卡行公钥的长度满足N_{ICC}>N_I42。

测试流程：选择卡片中应用，执行交易。

通过标准：终端在 GENERATE AC 命令中不请求 CDA。终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’(已进行脱机数据认证)。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’(复合动态数据认证/应用密文生成失败)。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.37 CQSJ028-02 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（隐含）（3）

测试目的：确保如果AIP中指明支持脱机动态数据认证，卡中缺少IC卡公钥余数，且被恢复的IC卡公钥长度表明IC卡公钥余数应不存在时，终端将执行动态数据认证。

终端配置：支持DDA。

卡片配置：——卡中的AIP指明支持脱机动态数据认证（AIP 字节1，位6 =‘1’）；
——IC卡公钥和发卡行公钥的长度满足N_{ICC}<N_I42。

子类案例：——案例01：卡中不存在IC卡公钥余项（缺失所有数据：TLV）；
——案例02：卡中IC卡公钥余项的长度等于0。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（DDA 成功）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘1’（脱机数据认证已进行）。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘0’（IC 卡数据未缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘0’(未使用 CDA)。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。

7.9.38 CQSJ028-03 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（隐含）（4）

测试目的：确保如果AIP中指明支持CDA，卡中缺少IC卡公钥余数，且被恢复的IC卡公钥长度表明IC卡公钥余数应不存在时，终端将执行CDA。

终端配置：支持CDA。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——IC卡公钥和发卡行公钥的长度满足N_{ICC}<N_I42。
子类案例：——案例01：卡中不存在IC卡公钥余项（缺失所有数据：TLV）；
——案例02：卡中IC卡公钥余项的长度等于0。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应处理交易直到完成，生成一个 TC 或 AAC。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘0’（CDA 成功）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。在金融确认报文或批数据采集报文中包含的 TSI 字节 1，位 8 =‘1’（脱机数据认证已进行）（仅当交易请求了 CDA 时，验证此标准）。在金融确认报文或批数据采集报文中包含的 TVR 字节 1，位 6 =‘0’（IC 卡数据未缺失）。

7.9.39 CQSJ028-04 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（5）

测试目的：确保如果AIP中指明支持CDA，卡中缺少IC卡公钥余数，但被恢复的IC卡公钥长度表明IC卡公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。
终端配置：——支持CDA；
——支持仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求TC；
——卡中不存在IC卡公钥余数（缺失所有数据：TLV）；
——IC卡公钥和发卡行公钥的长度满足N_{ICC}<N_I42。
测试流程：选择卡片中应用，执行交易。
通过标准：卡片返回 TC 时，终端应拒绝交易，并且不发送第二个 GENERATE AC 命令；或当第一个 GENERATE AC 卡片响应 ARQC 时，终端发送第二个 GENERATE AC 命令请求 AAC。第二个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失），或 TVR 包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值（如：打印在凭条中）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（ 已进行脱机数据认证）。第二个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败），或 TVR 包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值（如：打印在凭条中）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.40 CQSJ028-05 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（6）

测试目的：确保如果AIP中指明支持CDA，卡中缺少IC卡公钥余数，但被恢复的IC卡公钥长度表明IC卡公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——第一个GENERATE AC命令，卡片响应ARQC；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC，在第二个GENERATE AC命令中请求TC；
——卡中不存在IC卡公钥余数（缺失所有数据：TLV）；
——IC卡公钥和发卡行公钥的长度满足N_{ICC}>N_I42。
测试流程：选择卡片中应用，执行交易。

通过标准：终端发送第二个 GENERATE AC 命令请求 AAC，拒绝交易。第二个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（ 已进行脱机数据认证）。第二个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（ 未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（ 未使用 DDA）。

7.9.41 CQSJ028-06 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（6）

测试目的：确保如果AIP中指明支持CDA，卡中缺少IC卡公钥余数，但被恢复的IC卡公钥长度表明IC卡公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——第一个GENERATE AC命令，卡片响应ARQC；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC，在第二个GENERATE AC命令中请求TC；
——发卡行批准交易；
——卡中不存在IC卡公钥余数（缺失所有数据：TLV）；
——IC卡公钥和发卡行公钥的长度满足$N_{ICC}>N_I42$。

测试流程：选择卡片中应用，执行交易。

通过标准：终端拒绝交易。TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失），包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值（如：打印在凭条中）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘1’（ 未进行脱机数据认证）。TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败)），包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值(如:打印在凭条中)。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.42 CQSJ028-08 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（7）

测试目的：确保如果AIP中指明支持CDA，卡中缺少IC卡公钥余数，但被恢复的IC卡公钥长度表明IC卡公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——第一个GENERATE AC命令，卡片响应ARQC；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC，在第二个GENERATE AC命令中请求TC；
——终端无法联机；
——卡中不存在IC卡公钥余数（缺失所有数据：TLV）；
——IC卡公钥和发卡行公钥的长度满足$N_{ICC}>N_I42$。

测试流程：选择卡片中应用，执行交易。

通过标准：终端拒绝交易。TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失），包含于金融确认

报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值（如：打印在凭条中）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘1’（ 未进行脱机数据认证）。TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败），包含于金融确认报文或批数据采集报文中（仅适用于终端有能力保存拒绝或异常终止的交易），或终端有能力以任何形式显示 TVR 值(如:打印在凭条中)。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.43 CQSJ028-09 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（8）

测试目的：确保如果AIP中指明支持CDA，卡中缺少IC卡公钥余数，但被恢复的IC卡公钥长度表明IC卡公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC；
——交易联机批准；
——卡中不存在IC卡公钥余数（缺失所有数据：TLV）；
——IC卡公钥和发卡行公钥的长度满足$N_{ICC}>N_I42$。

测试流程：选择卡片中应用，执行交易。

通过标准：第一个 GENERATE AC 和第二个 GENERATE AC 均不请求 CDA。终端应完成交易，最终请求 TC。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（ 已进行脱机数据认证）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.44 CQSJ028-10 IC 卡公钥余数不存在且在 AIP 中指明支持 DDA（9）

测试目的：确保如果AIP中指明支持CDA，卡中缺少IC卡公钥余数，但被恢复的IC卡公钥长度表明IC卡公钥余数应当存在时，终端将TVR中“IC卡数据缺失”位置‘1’。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前能探测到CDA失败。

卡片配置：——卡中的AIP指明支持CDA（AIP 字节1，位1 =‘1’）；
——TAC和IAC设定，保证终端在第一个GENERATE AC命令中请求ARQC；
——交易联机拒绝；
——卡中不存在IC卡公钥余数（缺失所有数据：TLV）；
——IC卡公钥和发卡行公钥的长度满足$N_{ICC}>N_I42$。

测试流程：选择卡片中应用，执行交易。

通过标准：第一个 GENERATE AC 和第二个 GENERATE AC 均不请求 CDA。终端应完成交易，最终请求 AAC。第一个 GENERATE AC 的 TVR 字节 1，位 6 =‘1’（ IC 卡数据缺失）。第一个 GENERATE AC 的 TVR 字节 1，位 8 =‘0’（ 已进行脱机数据认证）。第一个 GENERATE AC 的 TVR 字节 1，位 3 =‘1’（ 复合动态数据认证/应用密文生成失败）。第一个 GENERATE AC 的 TVR 字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 的 TVR 字节 1，位 4 =‘0’（未使用 DDA）。

7.9.45 CQSJ029-00 结构数据对象无法正确解析：PSE 的 FCI

测试目的：确保如果终端支持PSE选择，且PSE的FCI模版无法正确解析时，终端切换成AID列表方式。

终端配置：支持PSE。
卡片配置：卡包含PSE。
子类案例：——案例01：在SELECT PSE的响应中返回的FCI模版‘6F’有一个错误标签‘6A’；
——案例 02：在 SELECT PSE 的响应中返回的 FCI 模版‘6F’有一个错误的长度，但值域的长度正确；
——案例 03：在 SELECT PSE 的响应中返回的 FCI 含一个带有错误标签‘85’的 DF 名；
——案例 04：在 SELECT PSE 的响应中返回的 FCI 含一个带有长度错误但值域长度正确的 DF 名；
——案例 05：在 SELECT PSE 的响应中返回的 FCI 含一个值域长度比长度域定义的长（+1）的 SFI 目录文件数据对象。
测试流程：卡执行PSE应用选择过程。
通过标准：终端应清除 PSE 候选列表。终端应切换成 AID 列表选择，对它所支持的每一个 AID 逐项选择。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.46 CQSJ029-05 结构数据对象无法正确解析：支付系统目录中的记录

测试目的：确保如果支付系统目录文件中的记录未能解析正确，终端应切换成AID列表方式。
终端配置：支持PSE。
子类案例：在READ RECORD命令的响应中返回的记录未能解析正确：
——案例 01：返回的记录有一个错误长度，但值域的长度正确；
——案例 02：返回的记录有一个错误的标签‘74’；
——案例 03：返回的记录包含一个位置不正确的数据对象：‘4F’ADF 名位于应用模版下，但在应用模版‘61’之前；
——案例 04：返回的记录包含一个位置不正确的数据对象：‘4F’ADF 名位于记录模版下，但在应用模版‘61’之后。
测试流程：卡执行PSE应用选择过程。
通过标准：终端应清除 PSE 候选列表。终端应切换成 AID 列表选择，对它所支持的每一个 AID 逐项选择。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.47 CQSJ030-00 结构数据对象无法正确解析：记录模版

测试目的：确保如果记录模版无法正确解析时，终端中断处理。
终端配置：N/A。
卡片配置：在读应用数据中的READ RECORD命令响应的记录模版无法正确解析。
子类案例：——案例01：在一个AEF 文件读记录的响应中返回卡的记录有一个错误长度，但值域的长度正确；
——案例 02：在一个 AEF 文件读记录的响应中返回卡的记录有一个错误的标签‘74’；
——案例 03：在一个 AEF 文件读记录的响应中返回卡的记录没有模版，直接是基本数据对象 CDOL1；
——案例 04：在 AEF 记录的响应中返回卡的记录长度正确，但值域长度是这个长度+1。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.9.48 CQSJ032-00 结构数据对象无法正确解析：ADF 的 FCI

测试目的：确保如果在最终选择中ADF模版的FCI无法正确解析时，终端将该应用从候选列表中移除。
终端配置：N/A。
卡片配置：——卡不包含PSE；

——卡片和终端共同支持两个优先级相同的ADF。

子类案例：最终选择中返回如下的FCI模版：

——案例01：在选择ADF1的响应中返回卡的FCI模版‘6F’有一个错误标签‘6A’；

——案例02：选择ADF1返回的FCI模版‘6F’的长度错误，但值域长度正确；

——案例03：选择ADF1的响应中返回的FCI包含DF名的标签不是‘84’而是‘85’；

——案例04：在选择ADF1返回卡的FCI包含DF名的长度错误，但值域长度正确；

——案例05：在选择ADF1返回的FCI包含的PDOL的长度要比标记长度长 1。

测试流程：卡执行应用选择过程。

通过标准：终端应在ADF2下执行交易直到完成，生成一个TC或AAC。

7.9.49 CQSJ033-00 结构数据对象无法正确解析：GET PROCESSING OPTIONS响应模版

测试目的：确保如果GET PROCESSING OPTIONS响应模版无法正确解析时，终端应终止交易。

终端配置：N/A。

子类案例：——案例01：卡在GET PROCESSING OPTIONS命令响应中的模版‘77’有一个错误标签‘70’；

——案例02：卡在GET PROCESSING OPTIONS命令响应中的模版‘77’的长度错误，但值域长度正确；

——案例03：卡在GET PROCESSING OPTIONS命令响应中的模版‘80’有一个错误标签‘70’；

——案例04：卡在GET PROCESSING OPTIONS命令响应中的模版‘80’的长度错误，但值域长度正确；

——案例05：卡在GET PROCESSING OPTIONS命令响应中的模版‘77’包含的AFL有一个错误的标签‘74’；

——案例06：卡在GET PROCESSING OPTIONS命令响应中的模版‘77’包含的AIP的长度域‘03’错误，但值域长度正确；

——案例07：卡在GET PROCESSING OPTIONS命令响应中的模版‘77’不包含AIP。

测试流程：选择卡片应用，执行交易。

通过标准：终端应终止交易。

7.9.50 CQSJ034-00 结构数据对象无法正确解析：GENERATE AC响应模版‘77’

测试目的：确保如果GENERATE AC响应模版无法正确解析时，终端应终止交易。

终端配置：N/A。

子类案例：——案例01：卡在GENERATE AC响应中的模版‘77’有一个错误标签‘9D27’的CID；

——案例02：卡在GENERATE AC响应中的模版‘77’有一个错误长度‘03’的ATC，但值域的长度正确；

——案例03：卡在GENERATE AC响应中的模版‘77’包含的应用密文值域长度错误：标签‘9F26’，长度域‘08’，值为9个字节；

——案例04：卡在GENERATE AC响应中的模版‘77’包含的长度不正确：总长度+1；

——案例05：卡在GENERATE AC响应中的模版包含错误的标签‘70’；

——案例06：卡在GENERATE AC响应中的模版‘80’包含的长度不正确：总长度+1。

测试流程：选择卡片应用，执行交易。

通过标准：终端应终止交易。

7.9.51 CQSJ035-00 结构数据对象无法正确解析：INTERNAL AUTHENTICATE 响应模版

测试目的：确保如果对动态数据认证的INTERNAL AUTHENTICATE响应模版无法正确解析时，终端应终止交易。
终端配置：支持DDA。
卡片配置：卡中的AIP指明支持动态数据认证（AIP字节1，位6为1）。
子类案例：——案例01：卡在内部认证响应中的模版‘77’的长度域错误：总长+1；
——案例02：卡在内部认证响应中的模版‘77’包含一个带有错误标签‘8F4B’的签名动态应用数据；
——案例03：卡在内部认证响应中的模版‘77’包含一个带有错误长度（值域+1），但值的长度正确的签名动态应用数据；
——案例04：卡在内部认证响应中的模版‘77’包含一个未知标签‘70’；
——案例05：卡在内部认证响应中的模版‘80’的长度域错误：总长+1；
——案例06：卡在内部认证响应中的模版‘80’包含一个错误标签‘79’。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应终止交易。

7.9.52 CQSJ036-00 日期超出范围：应用生效日期（1）

测试目的：确保如果卡提供的日期超出范围时，终端应终止交易。
终端配置：N/A。
子类案例：——案例01：日期中月份是13；
——案例02：日期中月份是00；
——案例03：日期中月份是99；
——案例04：日期中日是00；
——案例05：日期中日是32；
——案例06：日期中日是99；
——案例07：日期是310212（2012年2月31日）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.9.53 CQSJ036-01 日期超出范围：应用失效日期（2）

测试目的：确保如果卡提供的日期超出范围时，终端应终止交易。
终端配置：N/A。
子类案例：——案例01：日期中月份是13；
——案例02：日期中月份是00；
——案例03：日期中月份是99；
——案例04：日期中日是00；
——案例05：日期中日是32；
——案例06：日期中日是99；
——案例07：日期是310206（2006年2月31日）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.9.54 CQSJ037-00 数据应在规定的范围之内却没在：SFI

测试目的：确保如果终端支持PSE选择，且卡返回的FCI中的SFI不在支持的值范围内时，终端应切换成AID列表方式。
终端配置：支持PSE。
卡片配置：卡在选择PSE的响应中SW1SW2 =‘9000’。
子类案例：——案例01：卡片返回目录文件的SFI是00；
——案例02：卡片返回目录文件的SFI是11；

——案例03：卡片返回目录文件的SFI是31。

测试流程：卡执行PSE应用选择过程。

通过标准：终端应清除 PSE 候选列表。终端应切换成 AID 列表选择，对它所支持的每一个 AID 逐项选择。终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.55 CQSJ044-00 CVM 列表无持卡人认证规则

测试目的：——确保如果CVM列表不包含任何持卡人认证规则时，终端应继续交易直到完成；

——确保终端认为CVM列表不包含任何持卡人认证规则和CVM列表不存在是一样的处理方式。

终端配置：N/A。

卡片配置：卡中的AIP指明支持持卡人验证（AIP 字节1，位5 =‘1’）。

子类案例：——案例01：CVM列表不包含任何持卡人认证规则（长度为0）；

——案例02：CVM列表不包含任何持卡人认证规则，但包含8个字节的金额X和金额Y（长度为8，值＝0000000000000000）。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应执行交易直到完成。TVR 字节 1，位 6 =‘1’（IC 卡数据缺失）。第一个 GENERATE AC 中，TVR 字节 3，位 8 =‘0’（持卡人认证未失败）。TSI 字节 1，位 7 =‘0’（持卡人认证未进行）。CVM 结果（3F 00 00）。

7.9.56 CQSJ045-00 CVM 列表中存在格式错误

测试目的：确保终端终止交易，如果CVM列表中存在格式错误。

终端配置：N/A。

卡片配置：卡中的AIP指明支持持卡人验证（AIP 字节1，位5 =‘1’）。

子类案例：——案例01：CVM列表为持卡人验证失败，总是。CVM方法存在，但CVM执行条件缺失；

——案例02：CVM列表为持卡人验证失败，总是。CVM列表长度字节错误：“8E0E0000000100000002000”。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应终止交易。

7.9.57 CQSJ047-00 AFL 有一个错误的 SFI

测试目的：确保如果AFL中的SFI有一个值是0或31时，终端应终止交易。

终端配置：N/A。

子类案例：——案例01：AFL中的SFI是0；

——案例02：AFL中的SFI是31。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应终止交易。

7.9.58 CQSJ048-00 AFL 有一个错误的起始记录号

测试目的：确保如果AFL中的起始记录号是0时，终端应终止交易。

终端配置：N/A。

卡片配置：AFL中的起始记录号是0。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应终止交易。

7.9.59 CQSJ049-00 AFL 有一个错误的结束记录号

测试目的：确保如果AFL中的起始记录号的值大于结束记录号值时，终端应终止交易。

终端配置：N/A。

卡片配置：AFL中的起始记录号的值大于结束记录号值。

测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.60 CQSJ050-00 有一个错误的记录号的 AFL 参加脱机数据认证

测试目的：确保如果参加脱机数据认证的AFL入口有一个错误的记录号时，终端应终止交易。
终端配置：N/A。
卡片配置：结束记录号起始记录号+1<参加脱机数据认证的记录数。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.61 CQSJ054-00 ISO 填充：在数据对象间的填充

测试目的：确保如果在模版中两个数据对象间的填充为‘0x00’或‘0xFF’时，终端应忽略填充。
终端配置：N/A。
卡片配置：填充字节的长度包括在模版长度中。
子类案例：——案例01：卡中的记录模版‘70’包含的两个数据对象，在其间有50个字节的填充‘00’；
——案例02：卡中的记录模版‘70’包含的两个数据对象，第一个数据对象之前填充‘0000’；
——案例03：卡中的记录模版‘70’包含的两个数据对象，第二个数据对象之后填充200个字节的‘00’；
——案例13：卡在GET PROCESSING OPTIONS的响应中模版‘77’包含AFL和AIP，二者之间填充‘0000’；
——案例14：卡在GET PROCESSING OPTIONS的响应中模版‘77’包含AFL和AIP，在两个数据对象之后有50个字节的填充‘00’；
——案例15：卡在GET PROCESSING OPTIONS的响应中模版‘77’包含AFL和AIP，在两个数据对象之前有一个填充‘0000’；
——案例19：卡的一个记录模版‘70’包含一个251个字节的填充‘00’。
注：这里的子案例序号不是线性连续的，中间缺失的编号被分配给了早期的一些子案例，但这些子案例不再适用。为避免混淆，不调整子案例编号为线性连续的。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.62 CQSJ054-01 ISO 填充：在数据对象间的填充

测试目的：本测试用于向后兼容，确保如果在模版中两个数据对象间的填充为‘0xFF’时，终端应忽略填充。
终端配置：N/A。
卡片配置：填充字节的长度包括在模版长度中。
子类案例：——案例01：卡中的记录模版‘70’包含的两个数据对象，在其间填充‘FFFF’；
——案例02：卡中的记录模版‘70’包含的两个数据对象，第一个数据对象之前填充50个字节的‘FF’；
——案例03：卡中的记录模版‘70’包含的两个数据对象，第二个数据对象之后填充‘FFFF’；
——案例04：卡在选择ADF的响应中FCI模版‘6F’包含DF名和FCI专有模版，二者之间填充50个字节的‘FF’；
——案例05：卡在选择ADF的响应中FCI模版‘6F’包含DF名和FCI专有模版，在DF名前填充‘FFFF’；
——案例06：卡在选择ADF的响应中FCI模版‘6F’包含DF名和FCI专有模版，在FCI专有模版之后有一个填充‘FFFF’但在FCI专有模版之内

（FCI专有模板长度包含了填充字节）；

——案例07：卡在GET PROCESSING OPTIONS的响应中模版‘77’包含AFL和AIP，二者之间填充200个字节的‘FF’；

——案例08：卡在GET PROCESSING OPTIONS的响应中模版‘77’包含AFL和AIP，在两个数据对象之后有一个填充‘FFFF’；

——案例09：卡在GET PROCESSING OPTIONS OPTION的响应中模版‘77’包含AFL和AIP，在两个数据对象之前有一个填充‘FFFF’。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.63 CQSJ054-02 填充：在数据对象间的填充

测试目的：确保如果在模版中两个数据对象间的填充为‘0x00’’时，终端应忽略非ISO填充。

终端配置：N/A。

卡片配置：填充字节的长度包括在模版长度中。

子类案例：——案例01：卡在选择ADF的响应中FCI模版‘6F’包含DF名和FCI专有模版，二者之间填充‘0000’；

——案例02：卡在选择ADF的响应中FCI模版‘6F’包含DF名和FCI专有模版，在DF名前填充200个字节‘00’；

——案例03：卡在选择ADF的响应中FCI模版‘6F’包含DF名和FCI专有模版，在FCI专有模版之后有一个填充‘0000’但在FCI专有模版之内（FCI专有模板长度包含了填充字节）；

——案例04：卡在选择ADF的响应中FCI专有模版‘A5’包含应用标签和语言参考，二者之间填充‘0000’；

——案例05：卡在选择ADF的响应中FCI专有模版‘A5’包含应用标签和语言参考，在应用标签填充200个字节‘00’；

——案例06：卡在选择ADF的响应中FCI专有模版‘A5’包含应用标签和语言参考，在最后数据之后有一个填充‘0000’但在FCI专有模版之内（FCI专有模板长度包含了填充字节）。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.9.64 CQSJ055-00 应用标签和应用优先名的格式是‘ans’

测试目的：确保终端支持新‘ans’格式的应用标签和应用优先名。

终端配置：N/A。

卡片配置：卡包含一个ADF。

子类案例：——案例01：ADF的FCI包含ans格式的应用标签和应用优先名且其中包含空格字符；

——案例02：ADF的FCI包含ans格式的应用标签和应用优先名且其中含“&”字符。

测试流程：选择卡片中应用，执行交易。

通过标准：终端应接受卡片，且通过请求一个 TC 或 AAC 来完成交易。

7.9.65 CQSJ056-00 强制数据缺失，格式 1,GENERATE AC 命令,响应 TC

测试目的：确保终端检查强制数据存在,当执行GENERATE AC命令,不请求CDA时。

终端配置：——仅脱机终端或有联机能力的脱机终端；

——不支持CDA。

卡片配置：——TAC/IAC设定,保证终端第一个GENERATE AC请求TC；

——第一个GENERATE AC，卡响应TC,格式1。

子类案例：——案例01：第一个GENERATE AC命令响应中，应用密文值不存在；

——案例02：第一个GENERATE AC命令响应中，密文信息数据不存在；
——案例03：第一个GENERATE AC命令响应中，应用计数器不存在。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.66 CQSJ057-00 强制数据缺失，格式1,GENERATE AC命令,响应ARQC

测试目的：确保终端检查强制数据存在,当执行GENERATE AC命令,不请求CDA时。
终端配置：——仅联机终端或有联机能力的脱机终端；
——不支持CDA。
卡片配置：——TAC/IAC设定,保证终端第一个GENERATE AC请求ARQC,第二个GENERATE AC请求TC；
——第一个GENERATE AC，卡响应ARQC,格式1，无可选数据；
——第一个GENERATE AC，卡响应ARQC，第二个GENERATE AC响应TC。
子类案例：——案例01：第二个GENERATE AC命令响应中，应用密文值不存在；
——案例02：第二个GENERATE AC命令响应中，密文信息数据不存在；
——案例03：第二个GENERATE AC命令响应中，应用计数器不存在。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.67 CQSJ058-00 强制数据缺失，格式2,GENERATE AC命令,响应TC

测试目的：确保终端检查强制数据存在,当执行GENERATE AC命令时。
终端配置：仅脱机终端或有联机能力的脱机终端。
卡片配置：——TAC/IAC设定,保证终端第一个GENERATE AC请求TC；
——第一个GENERATE AC，卡响应TC,格式2。
子类案例：——案例01：第一个GENERATE AC命令响应的TLV数据中，应用密文值域不存在（9F2600）；
——案例02：第一个GENERATE AC命令响应的TLV数据中，应用密文值不存在；
——案例03：第一个GENERATE AC命令响应中，密文信息数据域不存在（9F2700）；
——案例04：第一个GENERATE AC命令响应中，密文信息数据不存在；
——案例05：第一个GENERATE AC命令响应中，应用计数器值域不存在（9F3600）；
——案例06：第一个GENERATE AC命令响应中，应用计数器不存在。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.68 CQSJ059-00 强制数据缺失，格式2,GENERATE AC命令,响应ARQC

测试目的：确保终端检查强制数据存在,当执行GENERATE AC命令时。
终端配置：仅联机终端或有联机能力的脱机终端。
卡片配置：——TAC/IAC设定,保证终端第一个GENERATE AC请求ARQC,第二个GENERATE AC请求TC；
——第一个GENERATE AC，卡响应ARQC,格式2。
子类案例：——案例01：第二个GENERATE AC命令响应中,应用密文值域不存在(9F2600)；
——案例02：第二个GENERATE AC命令响应中，应用密文值不存在；
——案例03：第二个GENERATE AC命令响应中，密文信息数据域不存在（9F2700）；
——案例04：第二个GENERATE AC命令响应中，密文信息数据不存在；
——案例05：第二个GENERATE AC命令响应中，应用计数器值域不存在（9F3600）；
——案例06：第二个GENERATE AC命令响应中，应用计数器不存在。

测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.69 CQSJ060-00 强制数据缺失，格式1,内部认证命令

测试目的：确保终端检查强制数据存在,当执行内部认证命令时。
终端配置：支持DDA。
卡片配置：——卡的AIP指明支持DDA（AIP的第1字节第6位为‘1’）；
——卡以格式1响应内部认证命令；
——缺少动态应用签名数据。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.9.70 CQSJ061-00 强制数据缺失，格式2,内部认证命令

测试目的：确保终端检查强制数据存在,当执行内部认证命令时。
终端配置：支持DDA。
卡片配置：——卡的AIP指明支持DDA（AIP的第1字节第6位为‘1’）；
——卡以格式2响应内部认证命令。
子类案例：——案例01：内部认证命令响应中,动态应用签名数据值域不存在（9F4B00）；
——案例02：内部认证命令响应中，动态应用签名数据不存在。
测试流程：选择卡片中应用，执行交易。
通过标准：终端应终止交易。

7.10 终端总体要求（ZTYQ）

7.10.1 ZTYQ001-00 商户控制终端提供金额

测试目的：确保终端显示输入金额信息，并且如果PDOL包含金额域时，终端在能够在初始化应用过程中提供交易金额。
终端配置：支持终端类型X1 或者 支持终端类型X2 或者 支持终端类型X3。
卡片配置：PDOL请求授权金额。
子类案例：——案例01：PDOL请求数字型授权金额（tag “9F02”）；
——案例02：PDOL请求二进制型授权金额（tag “81”）；
——案例03：PDOL请求数字型其他金额（tag “9F03”），返现交易；
——案例04：PDOL请求二进制型其他金额（tag “9F04”），返现交易。
测试流程：选择卡片应用，执行交易。
通过标准：终端应在发送 GET PROCESSING OPTIONS 命令之前得到金额。卡应接收到一个数据域包含交易金额的 GET PROCESSING OPTIONS 命令。

7.10.2 ZTYQ002-00 商户控制终端获取金额如果不可用

测试目的：确保如果PDOL包含金额域但不可用时，终端在初始化应用过程中提示“输入金额”以获取交易金额。
终端配置：支持终端类型X1 或者 支持终端类型X2 或者 支持终端类型X3。
卡片配置：PDOL请求授权金额。
子类案例：——案例01：PDOL请求金额为数字型（tag “9F02”）；
——案例02：PDOL请求金额为二进制型（tag “81”）；
——案例03：PDOL请求数字型其他金额（tag “9F03”），返现交易；
——案例04：PDOL请求二进制型其他金额（tag “9F04”），返现交易。
测试流程：选择卡片应用，执行交易。
通过标准：终端应在发GET PROCESSING OPTIONS命令前获得交易金额。终端应显示“输入金额”信息。卡应接收到一个数据域包含交易金额的GET PROCESSING OPTIONS命令。

7.10.3 ZTYQ003-00 PDOL 请求授权金额和其他金额

测试目的：确保终端可以正确处理请求授权金额和其他金额在PDOL。
终端配置：不支持终端类型X1且不支持终端类型X2且不支持终端类型X3。
测试条件：交易金额大于零。
子类案例：——案例01：PDOL请求金额为数字型（tag “9F02”）；
——案例02：PDOL请求金额为二进制型（tag “81”）；
——案例03：PDOL请求数字型其他金额（tag “9F03”）；
——案例04：PDOL请求二进制型其他金额（tag “9F04”）。
测试流程：选择卡片应用，执行交易。
通过标准：GET PROCESSING OPTIONS 命令包含 PDOL 相应的交易金额 。如果终端不能得到金额则金额域应填充十六进制的零。终端应能完成交易。

7.10.4 ZTYQ004-00 仅联机的终端不支持数据认证设置位

测试目的：确保根据终端性能，如果仅联机的终端不支持任何形式的数据认证时，将TVR中的“未进行脱机数据认证”位设置成‘1’。
终端配置：仅联机终端、不支持SDA。
卡片配置：N/A。
测试流程：选择卡片应用，执行交易。
通过标准：第一个 GENERATE AC 中 TVR 的字节 1，位 8 =‘1’（未进行脱机数据认证）。第一个 GENERATE AC 中 TVR 的字节 1，位 7 =‘0’（未使用 SDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 3 =‘0’（未使用 CDA）。第一个 GENERATE AC 中 TVR 的字节 1，位 4 =‘0’（未使用 DDA）。

7.10.5 ZTYQ006-00 卡片和终端的应用版本号不同

测试目的：确保当卡片和终端的应用版本号不同时，终端应尝试继续处理交易。如果不能继续，终端终止交易。
终端配置：N/A。
卡片配置：卡片和终端有不同的应用版本号。
测试流程：选择卡片应用，执行交易。
通过标准：终端应尝试通过请求一个 TC 或 AAC 来完成交易，如果不能，终端应终止交易。第一个 GENERATE AC 中 TVR 字节 2，位 8 =‘1’（IC 卡和终端应用版本不一致）。

7.10.6 ZTYQ009-00 终端识别 CVM 码（支持‘无需 CVM’）当无需 CVM 时 CVM 被设置

测试目的：——确保当终端支持CVM码“无需CVM”时，终端应能识别此CVM；
——确保当可用的 CVM 是“无需 CVM”时，终端应将 CVM 结果的第 3 字节设置成‘成功’。
终端配置：支持无需CVM。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的第1字节第5位为‘1’）；
——CVM 列表是“无需 CVM，总是”（1F 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 字节 3，位 8 =‘0’（持卡人认证成功）。终端应将 CVM 结果第 3 字节设置成‘成功’。在第一个 GENERATE AC 中接收到的 TSI 字节 1，位 7 =‘1’（持卡人认证已进行）。CVM 结果=1F 00 02。

7.10.7 ZTYQ009-05 终端识别 CVM 码（不支持‘无需 CVM’）

测试目的：确保当终端不支持CVM码“无需CVM”时，终端应识别此CVM。
终端配置：不支持无需CVM。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的第1字节第5位为‘1’）；
——CDOL1请求CVM结果；
——CVM列表是“无需CVM，总是”（1F 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。第一个 GENERATE AC 中 TVR 字节 3，位 8 =‘1’（持卡人认证失败）。终端应将 CVM 结果第 3 字节设置成‘失败’。在第一个 GENERATE AC 中接收到的 TSI 字节 1，位 7 =‘1’（持卡人认证已进行）。CVM 结果=3F 00 01。

7.10.8 ZTYQ010-00 终端识别 CVM 码（‘CVM 失败处理’）—当 CVM 是‘CVM 失败处理’时，CVM 被设置

测试目的：——确保终端能识别CVM码“CVM失败”；
——确保当可用的CVM是“CVM失败”时，终端应将CVM结果的第3字节设置成‘失败’。
终端配置：N/A。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的第一字节第五位为‘1’）；
——CVM列表是“CVM失败，总是”（-00 00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。在第一个 GENERATE AC 中 TVR 字节 3，位 8 =‘1’（持卡人认证失败）。在第一个 GENERATE AC 中接收到的 TSI 字节 1，位 7 =‘1’（持卡人认证已进行）。在第一个 GENERATE AC 中接收到的 CVM 结果=-00 00 01。

7.10.9 ZTYQ011-00 支持的 CVM

测试目的：确保终端支持的CVM在终端性能中指明。
终端配置：N/A。
卡片配置：PDOL请求终端性能。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个 TC 或 AAC 来完成交易。由终端返回的终端性能应该反映终端支持的 CVM。

7.10.10 ZTYQ013-00 卡没有得到 PIN 重试次数

测试目的：确保终端在PIN重试次数没有得到，或者卡不支持GET DATA命令的情况下，能够提示输入PIN。
终端配置：支持脱机明文PIN校验、支持Get Data命令取PIN重试次数。
卡片配置：——卡的AIP指明支持持卡人认证。（AIP 字节1，位5 =‘1’）；
——卡在Get Data命令不返回PIN重试次数；
——CVM列表是“明文PIN” （01 00）。
子类案例：——案例01：Get Data 命令中PIN重试次数返回长度为0；
——案例02：Get Data（取PIN重试次数）命令卡片返回的状态码不是‘9000’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端在收到Get Data命令的应答后，应该显示“Enter PIN”。

7.10.11 ZTYQ016-00 终端提示输入 PIN （PIN 重试次数 >0）

测试目的：确保终端在Get Data命令返回的PIN重试次数不为0的情况下能够提示输入PIN。
终端配置：支持脱机明文PIN校验、支持Get Data命令取PIN重试次数。
卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；

——卡在Get Data命令返回的PIN重试次数大于0；
——CVM列表是“明文PIN”（01 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端在收到Get Data命令的应答后，应该显示“Enter PIN”。

7.10.12 ZTYQ018-00 脱机PIN校验不成功

测试目的：确保如果IC卡脱机PIN验证不成功，终端不设置CVM结果，继续对CVM列表处理。

终端配置：支持脱机明文PIN校验。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；
——如果终端支持Get Data命令取PIN重试次数，卡片返回的PIN重试次数大于0；
——CVM列表是“明文PIN”（41 00），然后是“CVM失败”（-00 00）；
——卡在VERIFY 命令返回的状态码为‘63C0’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节3，位8 =‘1’（持卡人认证失败）。第一个GENERATE AC命令中TSI字节1，位7 =‘1’（持卡人认证已进行）。CVM 结果（-00 00 01）“CVM失败，总是，执行失败”。

7.10.13 ZTYQ020-00 联机PIN校验当终端支持Get Data命令取回PIN重试次数且PIN重试次数超限

测试目的：确保终端即使是在PIN重试次数超限的情况下，也允许输入PIN用于联机PIN的校验。

终端配置：支持Get Data命令取PIN重试次数、支持联机密文PIN校验、支持脱机明文PIN校验。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；
——CVM 列表要求是“明文 PIN ，如果终端支持”（41 03），然后是“脱机密文 PIN，如果终端支持”（44 03），然后是“联机密文 PIN，总是”（02 00）；
——卡在 GET DATA 命令返回 PIN 重试次数为 0 。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节3，位8 =‘0’（持卡人认证成功）。第一个GENERATE AC命令中TVR字节3，位6 =‘1’（PIN重试次数超限）。第一个GENERATE AC命令中TVR字节3，位3 =‘1’（输入联机PIN）。终端应显示“Enter PIN”。授权或金融请求报文应包含密文PIN。

7.10.14 ZTYQ020-01 联机PIN校验当终端不支持Get Data命令取回PIN重试次数且PIN重试次数超限

测试目的：确保终端即使在PIN重试次数超限的情况下，允许输入PIN用于联机PIN的校验。

终端配置：不支持Get Data命令取PIN重试次数，支持联机密文PIN校验、支持脱机明文PIN校验。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；
——卡在 VERIFY 命令返回‘63C0’。

子类案例：——案例 01：CVM 列表要求“明文 PIN 校验，如果支持”（41 03），然后是“联机密文 PIN 校验，总是”（02 00）；
——案例 03：CVM 列表要求“明文 PIN 校验，如果支持”（41 03），然后是

“密文 PIN 脱机校验，如果支持”（4403），然后是“联机密文 PIN 校验，总是”（02 00）。

注：这里的子案例序号不是线性连续的，中间缺失的编号被分配给了早期的一些子案例，但这些子案例不再适用。为避免混淆，不调整子案例编号为线性连续的。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节3，位8 =‘0’（持卡人认证成功）。第一个GENERATE AC命令中TVR字节3，位6 =‘1’（PIN重试次数超限）。第一个GENERATE AC命令中TVR字节3，位3 =‘1’（输入联机PIN）。终端应显示“Enter PIN”。授权或金融请求报文应包含密文PIN。

7.10.15 ZTYQ022-00 当在一个服务员终端 PIN 输入被绕过时，TVR 应被设置

测试目的：确保一个服务员终端绕过PIN输入时，设置TVR中“要求输入PIN， PIN pad 存在，但PIN没有输入” 位为 ‘1’并且“PIN重试次数超限”位不设为 ‘1’。

终端配置：支持绕过PIN并且支持服务员终端、支持脱机明文PIN校验或联机密文PIN校验。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；

——商户强制绕过 PIN 输入。

子类案例：根据终端的配置，决定以下子案例的执行：

——案例 01：CVM 列表是“明文 PIN 校验，总是”；

——案例 03：CVM 列表是 “联机密文 PIN 校验，总是”。

注：这里的子案例序号不是线性连续的，中间缺失的编号被分配给了早期的一些子案例，但这些子案例不再适用。为避免混淆，不调整子案例编号为线性连续的。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节3，位4 =‘1’（要求输入PIN，密码键盘存在，但未输入PIN）。第一个GENERATE AC命令中TVR字节3，位6 =‘0’（PIN重试次数未超限）。

7.10.16 ZTYQ023-00 一个服务员终端绕过 PIN 输入后 CVM 不成功

测试目的：如果PIN输入被绕过，确保终端认为CVM不成功并且继续CVM处理。

终端配置：支持绕过PIN并且支持服务员终端、支持脱机明文PIN校验或联机密文PIN校验。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；

——商户强制绕过 PIN 输入。

子类案例：——根据终端的配置，决定以下子案例的执行：

——案例 01：CVM 列表是“卡进行明文 PIN 验证，总是 ”（41 00），然后是“CVM 失败，总是”（-00 00）；

——案例 03：CVM 列表是“联机密文 PIN 校验”（42 00），然后是 “CVM 失败，总是”（-00 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应不显示关于PIN尝试计数器的信息。第一个GENERATE AC命令中TVR字节3，位8 =‘1’（持卡人认证失败）。第一个GENERATE AC命令中TSI字节1，位 7 =‘1’（持卡人认证已进行）。第一个GENERATE AC命令中TVR字节3，位4 =‘1’（要求输入PIN，密码键盘存在，但未输入PIN）。CVM 结果是（-00 00 01）。

7.10.17 ZTYQ024-00 绕过 PIN 输入绕过所有的 PIN 输入方式

测试目的：确保当一种绕过PIN输入被执行则终端认为绕过其他任何在CVM里面的PIN输入。

终端配置：支持连续绕过PIN输入并且支持绕过PIN输入并且有人终端，并且支持脱机明

文PIN并且支持联机密文PIN。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；
——CVM 是“卡进行脱机明文 PIN 校验如果支持则执行”（41 03）并且“卡进行联机密文 PIN 校验如果支持则执行”（42 03）且“CVM 失败，总是”（-00 00）；
——商户强制绕过 PIN 输入。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在第一次GENERATE AC 命令中TVR字节3，位4 =‘1’（要求输入PIN，密码键盘存在，但未输入PIN）。在第一次GENERATE AC 命令中TVR字节3，位8 =‘1’（持卡人验证失败）。在第一次GENERATE AC 命令中TSI字节1，位7 =‘1’（持卡人验证已执行）。CVM 结果是（-00 00 01）。终端不尝试第二种PIN输入方式。

7.10.18 ZTYQ024-01 绕过 PIN 输入不绕过所有的 PIN 输入方式

测试目的：确保当一种绕过PIN输入被执行则终端不认为绕过其他任何在CVM里面的PIN输入。

终端配置：支持绕过PIN输入并且有人终端，并且支持脱机明文PIN并且支持联机密文PIN并且不支持连续绕过PIN输入。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；
——CVM 是“卡进行脱机明文 PIN 校验如果支持则执行”（41 03）并且“卡进行联机密文 PIN 校验如果支持则执行”（42 03）且“CVM 失败，总是”（-00 00）；
——商户强制绕过 PIN 输入，并在第二个 PIN 验证方法中输入正确的 PIN。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在第一次GENERATE AC 命令中TVR字节3，位4 =‘1’（要求输入PIN，密码键盘存在，但未输入PIN）。在第一次GENERATE AC 命令中TVR字节3，位8 =‘0’（持卡人验证失败）。在第一次GENERATE AC 命令中TSI字节1，位7 =‘1’（持卡人验证已执行）。CVM 结果是（-00 00 01）。终端尝试第二种PIN输入方式。

7.10.19 ZTYQ025-00 终端打印有用于持卡人签名带线的单据

测试目的：确保当签名是可适用的CVM时，终端打印带有签名线的凭证。

终端配置：支持签名。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；
——CVM 是“签名，总是”（1E 00）。

子类案例：——案例 01：脱机交易；
——案例 02：联机交易。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应打印带有持卡人签名线的凭证。

7.10.20 ZTYQ028-00 CVM 结果设置为最后执行的 CVM 的方法代码和条件代码（1）

测试目的：确保终端根据最后执行的CVM，设置CVM 结果的字节1和字节2。

终端配置：N/A。

卡片配置：——卡的AIP指明支持持卡人认证 （AIP 字节1，位5 =‘1’）；
——CVM 列表为“CVM 失败，总是”（0000）接着是“无需 CVM，总是”（1F00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。CVM 结果 =-00 00 01。在第一个GENERATE AC命令中的TSI字节1，位7 =‘1’（持卡人认证已执行）。

7.10.21 ZTYQ028-01 CVM结果设置为最后执行的CVM的方法代码和条件代码（2）

测试目的：确保终端根据最后执行的CVM，设置CVM 结果的字节1和字节2。
终端配置：支持脱机明文PIN。
卡片配置：卡的AIP指明支持持卡人认证 （AIP 字节1，位5 =‘1’）。
子类案例：——案例01：CVM 列表为“脱机明文PIN校验，总是”（41 00） 接着“签名，总是“（1E 00）并且输入正确的PIN；
——案例02：CVM 列表为“脱机明文PIN校验，总是”（41 00） 接着“签名，总是“（1E 00）并且输入错误的PIN；
——案例03：CVM列表为“CVM失败，总是”（0000）接着“无需CVM，总是”（1F00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。在第一个GENERATE AC命令中的TSI字节1，位7 =‘1’（持卡人认证已执行）。案例01：CVM 结果应设置为 41 00 02。案例02：CVM 结果应设置为 1E 00 00（如果终端支持签名）或 1E 00 01（如果终端不支持签名）。案例03：CVM 结果应设置为 00 00 01。

7.10.22 ZTYQ028-02 CVM结果设置为最后执行的CVM的方法代码和条件代码（3）

测试目的：确保终端根据最后执行的CVM，设置CVM 结果的字节1和字节2。
终端配置：支持联机密文PIN。
卡片配置：卡的AIP指明支持持卡人认证 （AIP 字节1，位5 =‘1’）。
子类案例：——案例01：CVM 列表为“联机密文PIN校验，总是”（42 00） 接着“CVM失败，总是“（0000）并且输入错误的PIN；
——案例02：CVM 列表为“联机密文PIN校验，总是”（42 00），接着“CVM失败，总是“（0000）并且输入正确的PIN；
——案例03：CVM列表为“CVM失败，总是”（0000）接着“无需CVM，总是”（1F00）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。在第一个GENERATE AC命令中的TSI字节1，位7 =‘1’（持卡人认证已执行）。案例01：CVM 结果应设置为 42 00 00。案例02：CVM 结果应设置为 42 00 00。案例03：CVM 结果应设置为 00 00 01。

7.10.23 ZTYQ028-04 CVM结果设置为最后执行的CVM的方法代码和条件代码（4）

测试目的：确保终端根据最后执行的CVM，设置CVM 结果的字节1和字节2。
终端配置：支持无需CVM。
卡片配置：——卡的AIP指明支持持卡人认证 （AIP 字节1，位5 =‘1’）；
——CVM列表是 “无需CVM，总是”（1F00），接着是“CVM失败，总是”（0000）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。CVM 结果应设置为 1F 00 02。在第一个GENERATE AC命令中的TSI字节1，位7 =‘1’ （持卡人认证已执行）。

7.10.24 ZTYQ030-00 当无CVM执行时的CVM结果（1）

测试目的：确保终端在没有CVM存在或没有CVM条件满足的情况下设置CVM 结果字节1为“没有 CVM 执行” 。
终端配置：不支持无需CVM。
卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；
——卡片的CVM列表是无需CVM，如果终端支持此CVM（1F 03）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。在第一个GENERATE AC命令中TVR字节3，位8 =‘1’（持卡人验证失败）。在第一个GENERATE AC命令中TVR字节

3，位7 =‘0’（未知的CVM）。TSI字节1，位7 =‘1’（持卡人验证已执行）。CVM结果是 （3F 00 01）。

7.10.25 ZTYQ030-01 当无 CVM 执行时的 CVM 结果（2）

测试目的：确保终端在没有CVM存在或没有CVM条件满足的情况下设置CVM 结果字节1为“没有 CVM 执行” 。

终端配置：支持CVM前已知交易金额。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；

——卡片中如果金额低于 X（-00 06）则 CVM 失败，但金额高于 X，没有 CVM 满足条件。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在第一个GENERATE AC命令中TVR字节3，位8 =‘1’（持卡人验证失败）。TSI字节1，位7 =‘1’（持卡人验证已执行）。CVM 结果是 （3F 00 01）。

7.10.26 ZTYQ030-02 当无 CVM 执行时的 CVM 结果（3）

测试目的：确保终端在没有CVM存在或没有CVM条件满足的情况下设置CVM 结果字节1为“没有 CVM 执行” 。

终端配置：不支持签名。

卡片配置：——卡的AIP指明支持持卡人认证，（AIP 字节1，位5 =‘1’）；

——卡片中 CVM 列表是签名，如果终端支持这个 CVM（1E 03）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在第一个GENERATE AC命令中TVR字节3，位8 =‘1’（持卡人验证失败）。在第一个GENERATE AC命令中TVR字节3，位7 =‘0’（未知的CVM）。TSI字节1，位7 =‘1’（持卡人验证已执行）。CVM结果是 （3F 00 01）。

7.10.27 ZTYQ031-00 终端异常文件的检查

测试目的：确保当终端有异常文件时，应检查卡片的PAN是否存在于异常文件中，如果不存在，应不设置TVR中“卡出现在异常文件中”位为‘1’。

终端配置：支持异常文件。

子类案例：——案例1：卡片的PAN不在异常文件中；

——案例 2：卡片的 PAN 序列号不在异常文件中。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在第一个GENERATE AC命令中TVR字节1，位5 =‘0’ （卡没有出现在异常文件中）。

7.10.28 ZTYQ032-00 如果与异常文件中记录匹配，设置 TVR

测试目的：确保终端当有异常文件时，应检查卡片的PAN是否存在于异常文件中，如果存在，应设置TVR中“卡出现在异常文件中”位为‘1’。

终端配置：支持异常文件。

卡片配置：终端支持异常文件数据也在卡片中出现（例如卡主账号和卡序号）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节1，位5 =‘1’（卡出现在异常文件中）。

7.10.29 ZTYQ033-00 当终端脱机接受交易时授权响应码的设置

测试目的：确保当终端行为分析的结果为脱机接受时，终端设置授权响应码为”脱机批准”。

终端配置：支持仅脱机或脱机/联机能力。

卡片配置：——卡的参数设置使得交易脱机批准；
——CDOL1 请求授权响应码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC来完成交易。无论卡的应答是什么，授权响应码应该是”脱机批准”。

7.10.30 ZTYQ034-00 当交易脱机拒绝时授权响应码的设置

测试目的：确保当终端行为分析的结果为脱机拒绝时，终端设置授权响应码为‘脱机拒绝’。
终端配置：N/A。
卡片配置：——卡的参数设置使得交易脱机拒绝；
——CDOL1 请求授权响应码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个AAC来完成交易。无论卡的应答是什么，授权响应码应该是‘脱机拒绝’。

7.10.31 ZTYQ035-00 当选择交易联机时授权响应码不设置

测试目的：确保在终端行为分析结果为联机情况下，终端不设置授权响应码。
终端配置：支持仅联机或脱机/联机能力。
卡片配置：——卡的参数设置使得交易联机；
——CDOL1 请求授权响应码。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。应该不设置授权响应码。

7.10.32 ZTYQ036-00 当卡接受交易时，终端完成交易（1）

测试目的：确保当卡对GENERATE AC命令返回批准的情况下，终端完成交易。
终端配置：——支持仅脱机或脱机/联机；
——TAC联机、TAC缺省、TAC拒绝全设为‘0’。
卡片配置：——IAC联机、IAC缺省、IAC拒绝全设为‘0’；
——卡片返回 TC 给第一个 GENERATE AC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。

7.10.33 ZTYQ036-01 当卡接受交易时，终端完成交易（2）

测试目的：确保当卡对GENERATE AC命令返回批准的情况下，终端完成交易。
终端配置：TAC联机、TAC缺省、TAC拒绝全设为‘0’。
卡片配置：——IAC联机、IAC缺省、IAC拒绝全设为‘0’；
——卡片返回 ARQC 给第一个 GENERATE AC；
——卡片返回 TC 给第二个 GENERATE AC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。

7.10.34 ZTYQ038-00 终端传送授权或金融交易请求报文

测试目的：确保如果卡在第一个GENERATE AC返回请求联机，终端传送一个金融或授权请求报文。
终端配置：支持仅联机或脱机/联机功能。
卡片配置：卡在第一个GENERATE AC命令返回ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。终端应生成并传送一个金融或授权请求报文到发卡行。

7.10.35 ZTYQ040-00 卡请求通知且终端支持同时交易被捕获

测试目的：确保卡请求通知但交易被捕获时，终端不生成通知。
终端配置：支持通知并且支持联机数据捕获或批数据捕获。
卡片配置：——卡在第一个GENERATE AC命令响应中请求通知；
——交易被捕获（批上送或联机数据捕获）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端不应该传送通知消息。

7.10.36 ZTYQ042-00 如果卡指出'服务不允许'（CID：服务不允许），终端终止交易。

测试目的：——确保终端可以正确的识别卡在GENERATEAC命令的应答中要求生成通知及生成通知的原因为服务不允许；
——确保当卡在GENERATE AC命令应答中指示服务不允许的情况下，终端显示'不接受'报文并且终止交易。
终端配置：N/A。
卡片配置：TAC/IAC被设置使得终端在第一个GENERATE AC请求TC或ARQC。
子类案例：——案例01：卡片返回'服务不允许'在第一个GENERATE AC命令，AAC（CID=01）；
——案例 02：卡片返回'服务不允许'在第一个 GENERATE AC 命令，ARQC（CID=81）；
——案例 03：卡片返回'服务不允许'在第一个 GENERATE AC 命令，AAC 并且要求生成通知（CID=09）；
——案例 04：卡片返回'服务不允许'在第一个 GENERATE AC 命令，ARQC 并且要求生成通知（CID=89）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易，并显示"交易不接受"。

7.10.37 ZTYQ042-01 如果卡指出'服务不允许'（CID：服务不允许），终端终止交易。

测试目的：确保终端可以正确的识别卡在GENERATEAC命令的应答中要求生成通知及生成通知的原因为服务不允许。
终端配置：支持仅脱机或脱机/联机。
卡片配置：测试条件被设置以便终端请求交易联机完成。
子类案例：——案例01：卡片返回'服务不允许'在第二个GENERATE AC命令，AAC （CID=01）；
——案例 02：卡片返回'服务不允许'在第二个 GENERATE AC 命令，TC （CID=41）；
——案例 03：卡片返回'服务不允许' 在第二个 GENERATE AC 命令，AAC 并且要求生成通知（CID=09）；
——案例 04：卡片返回'服务不允许' 在第二个 GENERATE AC 命令，TC 并且要求生成通知（CID =49）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易，并显示"交易不接受"。

7.10.38 ZTYQ042-06 CDA 失败，IC 卡片返回 ARQC

测试目的：确保如果CDA失败并且卡片返回ARQC，终端应设置TVR中"CDA失败"位为'1'并通过发送第二个GENERATE AC命令请求AAC来完成交易。
终端配置：——支持CDA；
——仅脱机或支持脱机/联机能力。
卡片配置：——卡的AIP指明支持CDA（AIP 字节1，位1 ='1'）；
——设置TAC和IAC使得第一次GENERATE AC命令请求TC；

——卡中的CDA签名错误；
——卡在第一个GENERATE AC命令中返回ARQC。

测试流程：选择卡片应用，执行交易 （执行CDA）。

通过标准：终端应处理交易直到完成并且执行第二个GENERATE AC命令请求AAC。第二个GENERATE AC中TSI字节1，位8 =‘1’（脱机数据认证已执行）。

7.10.39 ZTYQ042-07 如果卡指出‘服务不允许’（CID：服务不允许），联机能力终端终止交易

测试目的：——确保终端可以正确的识别卡在GENERATEAC命令的应答中要求生成通知及生成通知的原因为服务不允许；
——确保当卡在GENERATE AC命令应答中指示服务不允许的情况下，终端显示‘不接受’报文并且终止交易。

终端配置：支持仅脱机或脱机/联机。

卡片配置：TAC/IAC被设置以便终端在第一次GENERATE AC命令中请求TC。

子类案例：——案例01：卡片返回‘服务不允许’在第一个GENERATE AC命令，应用密文TC （CID =41）；
——案例02：卡片返回‘服务不允许’在第一个GENERATE AC命令，应用密文TC且要求生成通知（CID =49）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应终止交易，并显示“交易不接受”。

7.10.40 ZTYQ042-08 复合动态数据认证/应用密文生成失败并且卡片请求ARQC。

测试目的：确保在生成DDA应用密文时候失败，且卡片请求ARQC，终端设置复合动态数据认证/应用密文生成失败位为1，并且立即发送第二次GENERATE AC命令请求AAC以完成交易。

终端配置：支持复合动态数据认证并且支持仅联机终端并且在支持复合动态数据认证在第一次GENERATE AC请求ARQC。

卡片配置：——卡片AIP指明支持复合动态数据认证（AIP第1字节位1 = ‘1’）；
——设置TAC和IAC使得第一次GENERATE AC命令中请求ARQC；
——在卡片中复合动态数据认证/应用密文生成失败；
——卡片在第一次GENERATE AC命令中请求ARQC。

测试流程：选择卡片应用，执行交易（CDA）。

通过标准：终端在第二次GENERATE AC命令中请求AAC以完成交易。第二次GENERATE AC命令中TSI字节1，位8 =‘1’（脱机数据认证已执行）。

7.10.41 ZTYQ043-00 终端决定交易接受或拒绝后发第二个GENERATE AC

测试目的：确保如果交易是联机的，终端应发出第二个GENERATE AC命令指出ARC的内容。

终端配置：支持仅联机或脱机/联机能力。

卡片配置：卡参数被设置使得交易联机。

子类案例：——案例01：发卡方返回ARC为交易批准；
——案例02：发卡方返回ARC为交易拒绝。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理交易直到完成。卡应该收到第二个GENERATE AC命令请求TC（测试1）和AAC（测试2）。

7.10.42 ZTYQ044-00 ARC是 ’联机批准’

测试目的：确保如果交易联机执行并被联机捕获，发卡行返回ARC是联机批准，则在第二个GENERATE AC命令卡片返回AAC的情况下，终端应发起一个冲正报文。

终端配置：支持联机数据捕获、支持仅联机或脱机/联机能力。

卡片配置：——卡参数设置使得交易联机；

——交易被联机捕获 （金融报文）；
——返回的ARC是‘联机批准’；
——卡对第二个GENERATE AC返回AAC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该生成并实时传输一个冲正报文。

7.10.43 ZTYQ045-00 终端支持在授权或金融交易应答中的发卡行脚本（1）

测试目的：当终端收到授权或金融交易应答包含一个或多个脚本，总长度小于或等于128字节时，终端应能管理并执行这些脚本。

终端配置：支持仅联机或脱机/联机能力。

卡片配置：卡参数设置使得交易联机执行。

子类案例：——案例01：发卡方应答中包含三个‘71’的脚本，总长为128字节。例如：’71 28 9F 18 04 00 00 00 01 86 1F {31个字节的命令}’+’71 29 9F 18 04 00 00 00 02 86 20 {32个字节的命令}’+’71 29 9F 18 04 00 00 00 03 86 20 {32个字节的命令}’；

——案例02：发卡方应答中包含一个‘71’的脚本，总长为128字节。例如：’72 7E 9F 18 04 00 00 00 01 86 75 {117个字节的命令}’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应收到根据应答发送的脚本中的命令。

7.10.44 ZTYQ045-01 终端支持在授权或金融交易应答中的发卡方脚本（2）

测试目的：当终端收到授权或金融应答包含一个或多个脚本，总长小于或等于128字节时，终端应能管理并执行这些脚本。

终端配置：支持仅联机或脱机/联机能力。

卡片配置：卡参数设置位交易联机执行。

子类案例：——案例01：发卡方应答中包含一个‘72’的脚本，总长为128字节。例如：’71 28 9F 18 04 00 00 00 01 86 1F {31个字节的命令}’+’71 29 9F 18 04 00 00 00 02 86 20 {32个字节的命令}’+’71 29 9F 18 04 00 00 00 03 86 20 {32个字节的命令}’；

——案例02：发卡方应答中包含三个‘72’的脚本，总长为128字节。例如：’72 7E 9F 18 04 00 00 00 01 86 75 {117个字节的命令}’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应收到根据应答发送的脚本中的命令。

7.10.45 ZTYQ045-02 终端支持在授权或金融交易应答中的发卡方脚本（3）

测试目的；当终端收到授权或金融应答包含一个或多个脚本，总长小于或等于128字节时，终端应能管理并执行这些脚本。

终端配置：支持仅联机或脱机/联机能力。

卡片配置：卡参数设置位交易联机执行。

子类案例：——案例01：发卡方应答中包含一个‘71’和一个‘72’的脚本，总长为128字节。例如：’71 3E 9F 18 04 00 00 00 01 86 35 {53个字节的命令}’ +’72 3E 9F 18 04 00 00 00 02 86 35 {53个字节的命令}’；

——案例02：发卡方应答中包含一个‘71’和两个‘72’的脚本，总长为128字节。例如：’71 28 9F 18 04 00 00 00 01 86 1F {31个字节的命令}’+’72 29 9F 18 04 00 00 00 02 86 20 {32个字节的命令’ +’72 29 9F 18 04 00 00 00 03 86 20 {32个

字节的命令}’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应收到根据应答发送的脚本中的命令。

7.10.46 ZTYQ048-00 终端记录脚本标识

测试目的：确保终端在发卡方脚本结果中设置了脚本的执行结果。

终端配置：支持仅联机或脱机/联机能力。

卡片配置：——卡参数设置使得交易联机执行；
——所有的脚本都有一个脚本标识。

子类案例：——案例 01：发卡方脚本应答包含三个‘71’的脚本：前两个成功最后一个失败；
——案例 02：发卡方脚本应答包含三个‘71’的脚本：都成功；
——案例 03：发卡方脚本应答包含三个‘72’的脚本：前两个成功最后一个失败；
——案例 04：发卡方脚本应答包含三个‘72’的脚本：都成功；
——案例 05：发卡方脚本应答包含两个‘71’的脚本和一个‘72’的脚本，前两个‘71’的脚本成功并且最后一个 72 的脚本失败；
——案例 06：发卡方脚本应答包含一个‘71’的脚本，一个‘72’的脚本，两个脚本都成功；
——案例 07：发卡方脚本应答包含两个‘71’的脚本和一个‘72’的脚本，第一个‘71’的脚本失败并且后两个脚本成功；
——案例 08：发卡方脚本应答包含一个‘71’的脚本和两个‘72’的脚本，第一个‘71’的脚本成功， 第一个‘72’的脚本失败并且最后一个 72 的脚本成功。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第二个GENERATE AC中，TVR字节5，位6 =‘0’（脚本处理在最后一个GENERATE AC前未使用或成功执行），案例02，03，04，05，06和09。第二个GENERATE AC中，TVR字节5，位6 =‘1’（脚本处理在最后一个GENERATE AC前失败），案例01和07。金融确认报文或批批数据捕获报文中,TVR字节5,位5 =‘0’(脚本处理在最后一个GENERATE AC后未使用或成功执行），案例01，02，04，06和07。金融确认报文或批批数据捕获报文中，TVR字节5，位5 =‘1’（脚本处理在最后一个GENERATE AC后失败），案例03，05和08。发卡方脚本结果（包含在金融确认报文中或批数据采集报文中）：案例01发卡方脚本执行结果：20 xx xx xx xx 20 yy yy yy yy 1x zz zz zz zz。案例02发卡方脚本执行结果：20 xx xx xx xx 20 yy yy yy yy 20 zz zz zz zz。案例03发卡方脚本执行结果：20 xx xx xx xx 20 yy yy yy yy 1x zz zz zz zz。案例04发卡方脚本执行结果：20 xx xx xx xx 20 yy yy yy yy 20 zz zz zz zz。案例05发卡方脚本执行结果：20 xx xx xx xx 20 yy yy yy yy 1x zz zz zz zz。案例06发卡方脚本执行结果：20 xx xx xx xx 20 yy yy yy yy。案例07发卡方脚本执行结果：1x xx xx xx xx 20 yy yy yy yy 20 zz zz zz zz。案例08发卡方脚本执行结果：20 xx xx xx xx 1x yy yy yy yy 20 zz zz zz zz。

7.10.47 ZTYQ052-00 当交易没有报文产生时终端产生一个通知

测试目的：对于交易联机拒绝交易，当交易无法被发卡行捕获时，确保终端产生一个通知报文包括发卡方脚本结果。

终端配置：支持仅联机或脱机/联机能力、支持通知。

卡片配置：——卡参数被设置使得交易联机进行；
——最后 GENERATE AC 命令返回 AAC。

子类案例：——案例 01：发卡方脚本应答包含一个‘71’ 的脚本；
——案例 02：发卡方脚本应答包含三个‘71’ 的脚本；
——案例 03：发卡方脚本应答包含一个‘72’ 的脚本；
——案例 04：发卡方脚本应答包含三个‘72’ 的脚本；
——案例 05：发卡方脚本应答包含两个‘71’ 的脚本和一个‘72’的脚本；
——案例 06：发卡方脚本应答包含两个‘72’ 的脚本和一个‘71’的脚本。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应生成一个包含发卡方脚本结果的通知报文。

7.10.48 ZTYQ055-00 终端支持 DDA 应也支持 SDA（1）

测试目的：确保终端在支持DDA的情况下也支持SDA。
终端配置：——支持DDA；
——终端中含有卡指定的 CA 公钥。
卡片配置：——卡中AIP指明支持SDA （AIP字节1，位7 =‘1’）；
——卡中的静态签名数据正确；
——CDOL1 请求终端能力。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端性能应指明支持SDA。第一个GENERATE AC命令中TVR字节1，位7 =‘0’ （SDA成功）。第一个GENERATE AC命令中TSI字节1，位8 =‘1’ （脱机数据认证已进行）。第一个GENERATE AC命令中TVR字节1，位3 =‘0’ （未使用CDA）。第一个GENERATE AC命令中TVR字节1，位4 =‘0’ （未使用SDA）。

7.10.49 ZTYQ055-01 终端支持 CDA 应也支持 SDA （2）

测试目的：确保终端在支持CDA的情况下也支持SDA。
终端配置：——支持CDA；
——终端中含有卡指定的 CA 公钥。
卡片配置：——卡中AIP指明支持SDA （AIP字节1，位7 =‘1’）；
——卡中的静态签名数据正确；
——CDOL1 请求终端能力。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端性能应指明支持SDA。金融确认报文或批数据采集报文中TVR字节1，位7 =‘0’ （SDA成功）。第一个GENERATE AC命令中TVR字节1，位3 =‘0’ （未使用SDA）。第一个GENERATE AC命令中TVR字节1，位4 =‘0’ （未使用DDA）。金融确认报文或批数据采集报文中TSI字节1，位8 =‘1’ （脱机数据认证已进行）。

7.10.50 ZTYQ056-00 仅脱机的终端应该支持 SDA

测试目的：确保仅脱机能力的终端支持SDA。
终端配置：——支持仅脱机；
——终端中含有卡指定的 CA 公钥。
卡片配置：——卡中AIP指明支持SDA （AIP字节1，位7 =‘1’）；
——卡中的静态签名数据正确；
——CDOL1 请求终端性能。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端性能应指明支持SDA。第一个GENERATE AC命令中TVR字节1，位7 =‘0’ （SDA成功）。第一个GENERATE AC命令中TSI字节1，位8 =‘1’ （脱机数据认证已进行）。

7.10.51 ZTYQ057-00 有联机能力的脱机终端应支持 SDA

测试目的：如果终端是有联机能力的脱机终端，确保终端支持SDA。
终端配置：——有联机能力的脱机终端；
——终端中含有卡指定的 CA 公钥。
卡片配置：——卡中AIP指明支持SDA （AIP字节1，位7 =‘1’）；
——卡中的静态签名数据正确；
——CDOL1 请求终端能力。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端性能应指明支持SDA。第一个GENERATE AC命令中TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.10.52 ZTYQ058-00 仅支持脱机的终端应支持终端风险管理

测试目的：如果终端仅支持脱机，确保终端支持终端风险管理。
终端配置：仅脱机终端。
卡片配置：——卡的AIP指明支持TRM （AIP 字节1，位4 =‘1’）；
——交易金额超过终端最低限额；
——卡中 LCOL 和 UCOL 存在；
——GET DATA 命令没有返回 ATC 。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节4，位8 =‘1’（交易超过最低限额）。第一个GENERATE AC命令中TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个GENERATE AC命令中TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个GENERATE AC命令中TSI字节1，位4 =‘1’（终端风险管理已进行）。

7.10.53 ZTYQ059-00 有联机功能的脱机终端应支持终端风险管理

测试目的：如果终端是仅联机能力的脱机终端，确保终端支持终端风险管理。
终端配置：支持仅脱机或脱机/联机能力。
卡片配置：——卡的AIP指明支持TRM （AIP 字节1，位4 =‘1’）；
——交易金额超过终端最低限额；
——卡中 LCOL 和 UCOL 存在；
——GET DATA 命令没有返回 ATC 。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节4，位8 =‘1’（交易超过最低限额）。第一个GENERATE AC命令中TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个GENERATE AC命令中TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个GENERATE AC命令中TSI字节1，位4 =‘1’（终端风险管理已进行）。

7.10.54 ZTYQ060-00 金融机构控制的终端应支持终端风险管理

测试目的：确保金融机构控制的终端支持终端风险管理。
终端配置：终端类型为1x并且支持频度检查或者支持最低限额检查或者支持随机交易选择或者支持异常文件或者支持交易日志。
卡片配置：——卡的AIP指明支持TRM （AIP 字节1，位4 =‘1’）；
——交易金额超过终端最低限额；
——卡中 LCOL 和 UCOL 存在；
——GET DATA 命令没有返回 ATC；
——CDOL1 请求终端类型。

测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节4，位8 =‘1’（交易超过最低限额）。第一个GENERATE AC命令中TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个GENERATE AC命令中TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个GENERATE AC命令中TSI字节1，位4 =‘1’（终端风险管理已进行）。

7.10.55 ZTYQ061-00 商户控制终端支持终端风险管理

测试目的：确保商户控制终端支持TRM。
终端配置：终端类型为2x并且支持频度检查。
卡片配置：——卡的AIP指明支持TRM （AIP 字节1，位4 =‘1’）；
——交易金额超过终端最低限额；
——卡中 LCOL 和 UCOL 存在；
——GET DATA 命令没有返回 ATC；
——CDOL1 请求终端类型。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节4，位8 =‘1’（交易超过最低限额）。第一个GENERATE AC命令中TVR字节4，位7 =‘1’（超过连续脱机交易下限）。第一个GENERATE AC命令中TVR字节4，位6 =‘1’（超过连续脱机交易上限）。第一个GENERATE AC命令中TSI字节1，位4 =‘1’（终端风险管理已进行）。

7.10.56 ZTYQ062-00 终端显示交易总计

测试目的：确保终端显示交易金额给持卡人。
终端配置：N/A。
卡片配置：N/A。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应显示交易金额给持卡人，或将其打印在签购单上。

7.10.57 ZTYQ063-00 返现金额在其他金额数据对象中被传输

测试目的：如果终端支持返现交易，确保终端使用其他金额数据对象存放返现金额。
终端配置：支持返现交易。
卡片配置：——持卡人要求返现；
——卡中 AUC 显示支持返现交易；
——CDOL1 请求其他金额域（数字格式或二进制格式）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。其他金额应包含返现的值。

7.10.58 ZTYQ064-00 消费和返现传输授权金额

测试目的：确保终端在授权金额中包括消费金额和返现金额。
终端配置：支持返现。
卡片配置：——持卡人要求返现；
——卡中 AUC 显示支持返现交易；
——CDOL1 请求授权金额域和其他金额域，（数字格式或二进制格式）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。授权金额应为返现金额和消费金额的和。

7.10.59 ZTYQ066-00 授权金额用十进制表示

测试目的：确保终端存储用十进制表示的授权金额。
终端配置：N/A。
卡片配置：——消费金额是十进制的值；
——CDOL1 请求授权金额。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。授权金额应为十进制表示。

7.10.60 ZTYQ067-00 其他金额使用十进制表示

测试目的：确保终端以十进制方式保存其他金额。
终端配置：支持返现。
卡片配置：——返现交易；
——消费金额是十进制值；
——卡中的 AUC 显示支持返现；
——CDOL1 请求其他金额。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。其他金额应为十进制表示。

7.10.61 ZTYQ074-00 当发卡方发起语音授权终端显示相关信息

测试目的：确保如果发卡方返回的ARC显示语音授权，一个服务员终端显示“打电话给发卡行”的提示信息。
终端配置：支持仅联机或脱机/联机能力、支持发卡方语音授权。
卡片配置：——卡参数被设置使得交易联机执行；
——应答中返回的 ARC 指示语音授权。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应显示一个“打电话给发卡行”的提示信息。

7.10.62 ZTYQ075-00 数据显示或打印执行发卡方授权参考

测试目的：确保如果发卡方返回的ARC， 指示一个语音授权， 一个服务员终端显示或打印正确的应用数据如PAN。
终端配置：支持仅联机或脱机/联机能力、支持发卡方发起的语音参考。
卡片配置：——卡参数被设置使得交易联机进行；
——应答中返回的 ARC 指示语音授权。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应显示或打印PAN 和其他应用数据。

7.10.63 ZTYQ076-00 信息提示操作员对发卡方的授权参考选择接受或拒绝

测试目的：确保如果发卡方返回的ARC，指示一个语音授权，一个服务员终端显示信息提示操作员输入银行的应答。
终端配置：支持仅联机或脱机/联机能力、支持发卡方发起的语音参考。
卡片配置：——卡参数被设置使得交易联机进行；
——应答中返回的 ARC 指示语音授权。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应显示一个信息提示操作员输入银行的应答。

7.10.64 ZTYQ077-00 当发卡方发起语音授权时 ARC

测试目的：确保如果发卡行返回ARC指示一个语音授权，则服务员终端应不改变接收到的ARC。

终端配置：支持仅联机或脱机/联机能力、支持发卡方发起的语音授权。
卡片配置：——卡参数被设置为交易联机执行；
——应答中返回的 ARC 指示语音授权；
——CDOL2 请求 ARC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。ARC应和从发卡方返回的一致。

7.10.65 ZTYQ078-00 终端发出第二个 GENERATE AC

测试目的：确保如果发卡方返回ARC指示一个语音授权，服务员终端应发第二个GENERATE AC命令，其中包含的ARC与根据银行应答输入的交易结果一致。
终端配置：支持仅联机或脱机/联机能力、支持发卡方发起的语音参考。
卡片配置：——卡参数被设置为交易联机执行；
——应答中返回的 ARC 指示语音授权。
子类案例：——案例 01：银行返回交易成功；
——案例 02：银行返回交易拒绝。
测试流程：选择卡片应用，执行交易。
通过标准：终端应能完成交易。卡应收到EXTERNAL AUTHENTICATE 命令。-xy=01：卡应收到第二个GENERATE AC命令请求TC。-xy=02：卡应收到第二个GENERATE AC命令请求AAC。

7.10.66 ZTYQ079-00 当商户强制交易联机 TVR 设置

测试目的：确保如果一个交易被强制联机，一个服务员终端设置TVR中“商户强制联机”位为‘1’。
终端配置：支持服务员终端、支持强制联机。
卡片配置：N/A。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第二个GENERATE AC命令中TVR字节4，位4 =‘1’ （商户要求联机交易）。

7.10.67 ZTYQ080-00 操作员强制交易批准

测试目的：确保如果操作员强制交易批准，终端发送联机金融通知或生成一个批上送数据捕获入口。
终端配置：支持服务员终端、支持强制批准。
子类案例：——案例 01：卡在第一个 GENERATE AC 命令应答是一个 AAC；
——案例 02：卡在第一个 GENERATE AC 命令应答是 ARQC，第二个 GENERATE AC 命令应答是一个 AAC。
测试条件：操作员强制交易接受。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。终端应发送联机金融通知或产生一个批数据采集入口。

7.10.68 ZTYQ081-00 当交易强制接受后 ARC

测试目的：确保如果操作员强制交易批准，终端应不修改ARC。
终端配置：支持服务员终端、支持强制批准、仅联机终端或有联机能力的脱机终端。
卡片配置：——卡参数设置使得交易联机执行；
——操作员强制交易接受。
子类案例：——案例01：发卡行拒绝（发卡行返回ARC指示拒绝）；
——案例 02：发卡行批准(发卡行返回 ARC 指示批准)，卡在第二个 GENERATE AC 命令应答是 AAC。
测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。联机金融通知或批数据采集入口中的ARC应和从发卡方收到的一致。

7.10.69 ZTYQ082-00 当操作员强制交易批准，终端配置指示器

测试目的：确保如果操作员强制交易批准，终端在联机通知或批数据采集中设置指示器。
终端配置：支持服务员终端、支持强制批准、仅联机终端或有联机能力的脱机终端。
卡片配置：卡参数设置使得交易联机执行。
子类案例：——案例01：操作员强制接受一个卡片请求脱机拒绝的交易。（即，第一个GENERATE AC请求ARQC，卡片响应AAC）；
——案例 02：操作员强制接受一个终端请求脱机拒绝的交易。（即，第一个 GENERATE AC 请求 AAC）；
——案例 03：操作员强制接受一个卡片请求联机拒绝的交易。（即，第二个 GENERATE AC 请求 TC，卡片响应 AAC）；
——案例 04：操作员强制接受一个终端请求联机拒绝的交易。（即，第二个 GENERATE AC 请求 AAC）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。终端应在操作员强制接受交易的联机通知或批数据采集中设置指示器标记该交易是强制接受。

7.10.70 ZTYQ083-00 终端维护交易序列号

测试目的：确保终端维护交易序列号。
终端配置：N/A。
卡片配置：——最少执行4个交易；
——如果终端有联机能力：两个交易联机执行另两个交易脱机执行；
——CDOL1 请求交易序列号。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。每个交易的交易序列号应按1递增。

7.10.71 ZTYQ086-00 终端读磁条上的服务代码

测试目的：如果读磁条的服务代码以‘2’或‘6’开始，并且如果终端不是一个IC和磁条的复合读卡器，确保终端显示一个信息“使用芯片卡交易”。
终端配置：支持磁条阅读器并且不支持磁条/IC复合读卡器。
卡片配置：服务代码‘5F30’在磁条中，不在芯片内。
子类案例：——案例01：卡磁条的服务代码以‘2’开头；
——案例 02：卡磁条的服务代码以‘6’开头。
测试流程：选择卡片应用，执行交易（先使用磁条，提示后插入IC卡）。
通过标准：终端应提示用户插入IC卡。授权请求，金融交易或批数据采集报文中不包括磁条数据（服务代码‘5F30’）。终端应处理交易直到完成。

7.10.72 ZTYQ087-00 终端读磁条上的服务代码

测试目的：如果读磁条的服务代码以‘2’或‘6’开始，确保终端转为IC操作。
终端配置：支持IC卡和磁条的复合读卡器并且磁条先读。
卡片配置：卡是磁条IC复合卡。
子类案例：——案例01：卡磁条的服务代码以‘2’开头；
——案例 02：卡磁条的服务代码以‘6’开头。
测试流程：选择卡片应用，执行交易（使用磁条）。
通过标准：终端应转入IC卡操作并且应发送借记/贷记应用命令到卡。

7.10.73 ZTYQ091-00 POS 输入模式代码

测试目的：如果如果服务代码‘2’或‘6’开头，终端读IC卡失败，确保终端应在交易报文中设置POS输入模式为‘磁条读取，上次交易读IC卡不成功’。
终端配置：支持磁条阅读器并且是服务员终端。
卡片配置：卡芯片功能无法使用。
子类案例：——案例01：卡磁条的服务代码以‘2’开头；
——案例 02：卡磁条的服务代码以‘6’开头。
测试流程：交易先从卡的芯片开始。
通过标准：交易报文（金融或批上送）应有终端输入模式设为‘磁条读取，上次交易读IC卡不成功’。

7.10.74 ZTYQ092-00 SDA 相关数据计算

测试目的：确保终端可以正确的计算SDA的相关的日期，当日期在2000年前、在2000年以及在2000年后。
终端配置：支持SDA。
卡片配置：卡中AIP指明SDA支持（AIP字节1，位7 =‘1’）。
子类案例：卡中的发卡行公钥证书使用以下不同的证书有效期计算：
——案例 01：证书失效日期为 101010；
——案例 02：证书失效日期为 991231；
——案例 03：证书失效日期为 000101；
——案例 04：证书失效日期为 120229；
——案例 05：证书失效日期为 010101；
——案例 06：证书失效日期为 160229；
——案例 07：证书失效日期为 200229；
——案例 08：证书失效日期为 491231。
测试流程：选择卡片应用，执行交易（尤其是SDA）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TSI字节1，位8 =‘1’（脱机数据认证已进行）。第一个GENERATE AC命令中TVR字节1，位7应根据证书失效日期设置（如果早于今天日期为‘1’，等于或晚于为‘0’）。第一个GENERATE AC命令中TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中TVR字节1，位4 =‘0’（未使用DDA）。

7.10.75 ZTYQ093-00 处理限制相关日期的计算

测试目的：确保终端可以正确的计算处理限制的相关的日期，当日期在2000年前、在2000年以及在2000年后。
终端配置：N/A。
子类案例：——案例01：应用的失效日期为900101；
——案例 02：应用的失效日期为 991231；
——案例 03：应用的失效日期为 000101；
——案例 04：应用的启用日期为 000112；
——案例 05：应用的启用日期为 000101；
——案例 06：应用的失效日期为 001201；
——案例 07：应用的失效日期为 010101；
——案例 08：应用的失效日期为 120229；
——案例 09：应用的启用日期为 120229；
——案例 10：应用的启用日期为 010101；
——案例 11：应用的启用日期为 900101；
——案例 12：应用的启用日期为 001201。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节2，位7应根据应用失效日期设置（如果在今天日期之前为‘1’，之后为

‘0’)。第一个GENERATE AC命令中TVR字节2，位6应根据应用启用日期设置（如果在今天日期之前为‘0’，之后为‘1’)。

7.10.76 ZTYQ094-00 计算，存储，并且显示 2000 年后的日期域

测试目的：确保终端可以正确的计算并存储2000年的日期域。
终端配置：支持内部日期管理。
卡片配置：CDOL1请求交易日期和交易时间。
子类案例：——案例01：终端的内部日期设置为31/12/2020 23h59min；
——案例 02：终端的内部日期设置为 28/02/2013 23h59min；
——案例 03：终端的内部日期设置为 28/02/2012 23h59min。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。交易日期应被更新为正确的值：案例01为01/01/2021；案例02为01/03/2013；案例03为29/02/2012。

7.10.77 ZTYQ094-01 计算，存储，并且显示 2000 年后的日期域

测试目的：确保终端可以正确的计算并存储2000年的日期域。
终端配置：仅联机终端并不支持内部日期管理。
卡片配置：CDOL1请求交易日期和交易时间。
子类案例：——案例01：终端的内部日期设置为31/12/2020 23h59min；
——案例 02：终端的内部日期设置为 28/02/2013 23h59min；
——案例 03：终端的内部日期设置为 28/02/2012 23h59min。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。交易日期应被更新为正确的值：案例01为01/01/2020；案例02为01/03/2013；案例03为29/02/2012。

7.10.78 ZTYQ095-00 年份处理

测试目的：确保终端可以正确的处理两位的年份。
终端配置：N/A。
子类案例：——案例01：应用的失效日期年为00；
——案例 02：应用的失效日期年为 10；
——案例 03：应用的失效日期年为 49；
——案例 04：应用的失效日期年为 50；
——案例 05：应用的失效日期年为 67；
——案例 06：应用的失效日期年为 99。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节2，位7应根据应用失效日期设置（今天日期之前设置为‘1’，之后为‘0’)。

7.10.79 ZTYQ102-00 服务员终端显示给操作员

测试目的：确保如果终端是服务员终端，应有正确显示给服务员。
终端配置：支持服务员终端。
卡片配置：N/A。
测试流程：测试员目测。
通过标准：终端应有一个显示给操作员。

7.10.80 ZTYQ103-00 字母数字字符的显示

测试目的：确保如果终端有显示，应能够至少显示32个字母数字字符（两行，每行16个)。
终端配置：支持显示。
卡片配置：N/A。

测试流程：测试员目测。
通过标准：终端应能够至少显示32个字母数字字符（每行16个）。

7.10.81 ZTYQ105-00 捕获交易和通知的存储

测试目的：确保当终端支持批数据捕获，交易记录和通知应在终端中正确存储，不会被擦除或更改直到下一次系统结算。
终端配置：支持批数据捕获。
卡片配置：N/A。
测试流程：——终端执行多个交易；
——存储的交易在与收单行对帐前应可以被读取。
通过标准：终端中存储的交易记录和通知应不被擦除或修改。

7.10.82 ZTYQ106-00 本地时钟的日期和时间

测试目的：确保支持仅脱机和有联机能力的脱机终端应有记录本地日期和时间的时钟。
终端配置：仅脱机终端或有联机能力的脱机终端。
卡片配置：CDOL1请求交易日期和交易时间。
测试流程：终端执行多个交易。
通过标准：交易日期和时间应该是连贯的。

7.10.83 ZTYQ107-00 终端打印机的性能

测试目的：确保如果打印机存在，打印机应能够每行至少打印20个字符。
终端配置：支持打印。
卡片配置：卡中的AID长10个字节（20个字符，例如‘A0 00 00 00 09 08 07 06 05 04’）。
测试流程：选择卡片应用，执行交易。
通过标准：AID应被正确打印在凭证上。

7.10.84 ZTYQ109-00 磁条阅读器使用磁道一或/及磁道二

测试目的：确保如果存在，终端磁条阅读器能够读取完整的磁道一或/及磁道二。
终端配置：支持磁条阅读器。
卡片配置：N/A。
测试流程：交易用卡的磁条执行。
通过标准：终端应能读取磁道一或磁道二或两个均可读取。

7.10.85 ZTYQ129-00 PIN PAD 应支持输入 412 位 PIN

测试目的：确保终端的PIN PAD支持412位PIN。
终端配置：支持脱机明文PIN。
卡片配置：——卡中AIP指明支持持卡人认证（AIP字节1，位5 =‘1’）；
——卡中的 CVM 是“明文 PIN 校验，总是”（0100）。
子类案例：——案例 01：卡中的 PIN 长度为 4 位；
——案例 02：卡中的 PIN 长度为 5 位；
——案例 03：卡中的 PIN 长度为 6 位；
——案例 04：卡中的 PIN 长度为 9 位；
——案例 05：卡中的 PIN 长度为 12 位；
——PIN 输入正确。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节3，位8 =‘0’（持卡人认证成功）。第一个GENERATE AC命令中TSI字节1，位7 =‘1’（持卡人认证已执行）。卡收到的PIN应该与输入的一致。

7.10.86 ZTYQ129-02 PIN PAD 应支持输入 412 位 PIN（联机 PIN）

测试目的：确保终端的PIN PAD支持412位PIN，当CVM要求执行联机PIN。
终端配置：支持联机密文PIN。
卡片配置：——卡中AIP指明支持持卡人认证（AIP字节1，位5 =‘1’）；
——卡中的CVM是“联机密文PIN校验，总是”（0200）。
子类案例：——案例01：卡中的PIN长度为4位；
——案例02：卡中的PIN长度为5位；
——案例03：卡中的PIN长度为6位；
——案例04：卡中的PIN长度为9位；
——案例05：卡中的PIN长度为12位。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR字节3，位8 =‘0’（持卡人认证成功）。第一个GENERATE AC命令中TVR字节3，位3 =‘1’（输入联机PIN）。第一个GENERATE AC命令中TSI字节1，位7 =‘1’（持卡人认证已进行）。联机报文中的PIN应该和密码键盘上输入的一致。

7.10.87 ZTYQ130-00 PIN PAD上输入的显示保护输入PIN的值（1）

测试目的：——确保当密码键盘有显示时，每一位输入的PIN都应被显示；
——确保当密码键盘有显示时，输入的PIN的值应有一定的保护，不能被显示出来，防止看或听的方式获取。
终端配置：支持脱机明文PIN校验。
卡片配置：——卡中AIP指明支持持卡人认证（AIP字节1，位5 =‘1’）；
——卡中的CVM是“明文PIN校验，总是”（0100）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。PIN每一位的输入应有一个显示。输入的PIN的每一位的值不能被显示。输入的PIN的每一位的值应有一定的保护，防止通过听或看的方式获取。

7.10.88 ZTYQ130-02 PIN PAD上输入的显示保护输入PIN的值（2）

测试目的：——确保当密码键盘有显示时，每一位输入的PIN都应被显示；
——确保当密码键盘有显示时，输入的PIN的值应有一定的保护，不能被显示出来，防止看或听的方式获取。
终端配置：支持联机密文PIN校验。
卡片配置：——卡中AIP指明支持持卡人认证（AIP字节1，位5 =‘1’）；
——卡中的CVM是“联机密文PIN校验，总是”（0200）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。PIN每一位的输入应有一个显示。输入的PIN的值不能被显示。输入PIN的值应有一定的保护，防止通过听或看的方式获取。

7.10.89 ZTYQ137-00 联机验证中PIN的保护

测试目的：确保如果终端支持联机PIN校验，终端应根据ISO95641对联机的PIN进行加密并且根据支付系统规则进行传输。
终端配置：支持联机密文PIN校验。
卡片配置：——卡中AIP指明支持持卡人认证（AIP字节1，位5 =‘1’）；
——卡中的CVM是“联机密文PIN校验，总是”（0200）；
——持卡人输入一个有效PIN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。金融或授权请求报文中的密文PIN数据包含根据ISO95641加密的PIN输入数据。

7.11 软件体系结构（TXJG）

7.11.1 TXJG004-00 终端中数据元的初始化

测试目的：确保列在数据元表中的数据元在终端内被初始化或在交易时获得数值。
终端配置：N/A。
卡片配置：CDOL1要求（若长度太长而不能返回所有数据，则可通过执行若干个测试）：
——账户类型；
——收单行标识符；
——终端附加性能；
——授权金额（二进制型）；
——授权金额（数字型）；
——其他金额（二进制型）；
——其他金额（数字型）；
——货币参考金额；
——应用标识符；
——应用版本号；
——CVM 结果；
——CA 公钥索引；
——IFD 序列号；
——商户种类码；
——商户标识符；
——商户名称和位置；
——POS 输入模式；
——终端性能；
——终端国家代码；
——终端最低限额；
——终端标识；
——TRM 数据；
——终端类型；
——终端验证结果；
——交易货币代码；
——交易货币指数；
——交易日期；
——交易参考货币代码；
——交易参考货币指数；
——交易序列号；
——交易状态信息；
——交易时间；
——交易类型。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端返回的数据元应该有正确的格式和相应的数值：

7.11.2 TXJG012-00 终端支持的语言

测试目的：确保终端有初始化的参数，以至处理卡的优先语言时，能够识别所支持的语言。
终端配置：N/A。
子类案例：——案例01：卡的优选语言（小写字母编码）与终端支持的一种语言匹配；
——案例 02：卡的优选语言（小写字母编码）与终端支持的所有语言匹配

（如果支持多语言）；
——案例 03：卡的优选语言（小写字母编码）与终端支持的一种语言匹配，卡优选语言（小写字母编码）中的另外一种，终端不支持；
——案例 04：卡的优选语言（大写字母编码）与终端支持的一种语言匹配；
——案例 05：卡的优选语言（大写字母编码）与终端支持的所有语言匹配（如果支持多语言）；
——案例 06：卡的优选语言（大写字母编码）与终端支持的一种语言匹配，卡优选语言（大写字母编码）中的另外一种，终端不支持。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。如果终端支持的语言与卡片中优先语言匹配，则该语言应该被使用。

7.11.3 TXJG016-00 如果验证失败，终端显示错误消息

测试目的：——确保如果在CA公钥下载时，校验和验证失败，终端不应接受该CA公钥；
——确保如果CA下载时，需要操作员行为，则终端显示一个错误消息提示处理失败。

终端配置：支持SDA或支持DDA或支持CDA、支持CAPK校验。

卡片配置：——CA公钥通过CA公钥校验和校验；
——CA公钥校验和是错误的。

测试流程：下载 CA 公钥 。

通过标准：CA公钥下载被拒绝。如果需要操作员行为，则终端应显示一个错误消息。

7.12 持卡人和商户界面（CSJM）

7.12.1 CSJM001-00 终端支持本地语言

测试目的：确保终端支持在终端位置或区域内使用的本地语言。

终端配置：支持显示。

卡片配置：卡首选语言根据终端所在位置和区域的本地语言设置。

子类案例：——案例01：卡的首选语言用小写字母进行编码；
——案例02：卡的首选语言用大写字母进行编码。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。信息的显示应该使用终端所在位置或区域的本地语言。

7.12.2 CSJM002-00 终端用本地语言的显示信息

测试目的：确保终端显示给服务员的消息是使用终端所在位置或区域内的本地语言。

终端配置：——服务员终端；
——支持显示。

卡片配置：N/A。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。给服务员显示消息使用的语言应该是终端所在位置或区域的本地语言或者是服务员选择的语言。

7.12.3 CSJM003-00 终端对相关字符集的支持

测试目的：确保终端显示的信息是使用定义在ISO 8859中的相关字符集。

终端配置：——支持显示；
——支持发卡行代码表；
——支持至少一个发卡行代码表索引。

子类案例：——案例01：终端支持卡的优选语言中的一种；
——案例02：终端支持卡中列出的所有首选语言（如果支持多语言）；

——案例03：终端支持卡的首选语言中的一种，另一种不支持；
——案例04：卡的首选语言为西班牙语；
——案例05：卡的首选语言为中文（汉语）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应使用共同支持的语言和相关字符集。

7.12.4 CSJM005-00 终端使用优先级最高的语言

测试目的：确保终端在交易的开始前，和卡中的首选语言进行比较，如果有相匹配的，则使用优先级最高的语言显示消息给持卡人。

终端配置：——支持显示；
——支持多种语言。

子类案例：——案例01：卡有语言1和语言2（按优先的顺序）作为优选语言，它们都被终端所支持；
——案例02：卡有语言1和语言2（按优先的顺序）作为优选语言，只有一个是终端所支持的；
——案例03：卡有语言1、语言2和语言3（按优先的顺序）作为优选语言，它们都是终端所支持的；
——案例04：卡有语言1、语言2和语言3（按优先的顺序）作为优选语言，它们中最后两个是终端所支持的；
——案例05：卡有语言1、语言2和语言3（语言3优先级最高，语言1最低，卡片按1，2和3的顺序返回三种语言）作为优选语言，它们都被终端所支持。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC来完成交易。终端应该在语言选择后使用终端和卡共同支持的优先级最高的语言显示的后续信息给持卡人。

7.12.5 CSJM006-00 终端允许持卡人选择语言

测试目的：确保终端在交易开始前，和卡的首选语言进行比较，如果没有相匹配的，且终端支持多语言，则终端允许持卡人选择语言。

终端配置：——支持功能键或支持键盘；
——支持显示；
——支持多种语言。

卡片配置：卡的首选语言值与终端支持的语言没有相匹配的并且终端有几种语言。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该处理交易直到完成。终端应该允许持卡人在终端发送GPO命令之前从终端支持的语言中选择他期望使用的语言。终端应该在语言选择之后使用持卡人所选择的语言来显示后续信息给持卡人。

7.12.6 CSJM006-01 终端允许持卡人选择语言（2）

测试目的：确保卡没有提供语言优先级，如果终端有方法允许持卡人选择他们的首选语言，那么终端应该使用持卡人选择的语言。

终端配置：——支持功能键或支持键盘；
——支持显示；
——支持多种语言；

卡片配置：卡片不包含语言优先级数据对象。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该处理交易直到完成。终端应该允许持卡人在终端发送GPO命令之前从终端支持的语言中选择他期望使用的语言。终端应该在语言选择之后使用持卡人所选择的语言来显示后续信息给持卡人。

7.12.7 CSJM006-02 终端使用当地语言

测试目的：确保卡片没有提供语言优先级，并且终端也没有方法让持卡人去选择他们的首选语言时，终端应该使用当地语言。
终端配置：——不支持功能键；
——不支持键盘；
——支持显示；
——支持多种语言。
卡片配置：卡片不包含语言优先级数据对象。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该处理交易直到完成。终端应该使用当地所支持的语言。GPO命令之后的所有信息应该用当地语言来显示给持卡人。

7.12.8 CSJM006-03 终端使用当地语言

测试目的：确保终端和卡片的语言优先级不匹配时，终端使用当地语言。
终端配置：——不支持功能键；
——不支持键盘；
——支持显示；
——支持多种语言。
卡片配置：卡片中的优先级和终端中的几个语言不匹配。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该处理交易直到完成。终端应该使用当地所支持的语言。GPO命令之后的所有信息应该用当地语言来显示给持卡人。

7.12.9 CSJM008-00 终端用支持的语言显示信息

测试目的：确保如果与卡中的优选语言没有相匹配的，且终端仅支持一种语言（当地语言），终端应该使用它支持的语言。
终端配置：——支持显示；
——不支持多种语言。
卡片配置：——案例01：卡的三个首选语言值与终端中支持的无相互匹配；
——案例02：卡中没有语言优先级数据。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。显示给持卡人的信息应该使用终端支持的语言。

7.12.10 CSJM008-01 终端用支持的语言显示信息

测试目的：确保如果与卡的优选语言中只有一个与终端的匹配，终端应该使用这个支持的语言。
终端配置：——支持显示；
——不支持多种语言。
卡片配置：卡的有限语言中有一个与终端匹配。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC来完成交易。终端不提示让持卡人选择语言。显示给持卡人的信息应该使用终端支持的语言。

7.12.11 CSJM011-00 终端对 AID 列表选择方式的支持

测试目的：确保终端支持AID列表选择应用方式。
终端配置：N/A。
卡片配置：——卡不支持PSE；
——终端和卡至少有一种相互匹配的应用。

测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。对于每个终端支持的应用，卡都应收到一个SELECT命令。

7.12.12 CSJM013-00 终端创建候选应用列表（1）

测试目的：确保如果终端支持持卡人选择应用，并且应用首选名称存在，发卡行代码表索引被使用，则终端使用应用首选名称显示共同支持的应用。
终端配置：——支持持卡人确认；
——支持发卡行代码表索引。
卡片配置：——卡片和终端有三种共同支持的应用；
——卡的应用有应用优先指示符指明的优先顺序；
——卡的应用有应用首选名称和发卡行代码列表索引。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端使用应用首选名称和发卡行代码表索引显示共同支持的应用。

7.12.13 CSJM014-00 终端创建候选应用列表（2）

测试目的：确保如果终端支持持卡人选择应用，应用首选名称不存在，则终端使用应用标签显示共同支持的应用。
终端配置：支持持卡人确认。
卡片配置：——卡片和终端有三种共同支持的应用；
——卡的应用有应用优先指示符指明的优先顺序；
——卡的应用没有应用首选名称。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该使用应用标签和发卡行代码表索引显示共同支持的应用。

7.12.14 CSJM015-05 终端显示应用列表

测试目的：确保如果支持持卡人确认的终端在最终应用选择时卡片返回不是‘9000’，终端应显示“请重新选择应用”的提示，并且显示给持卡人其它可选择的应用。
终端配置：支持持卡人确认。
卡片配置：——卡片和终端有三种共同支持的应用；
——卡片返回不是‘9000’的状态码作为对最终SELECT命令的响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应显示给持卡人终端和卡共同支持的应用列表，除了这个应用。终端应该显示‘请重新选择应用’。

7.12.15 CSJM016-00 终端选择下一个最高优先级应用

测试目的：确保如果终端不支持持卡人应用选择，且最终应用返回不是‘9000’的状态码，则终端选择次高优先级且不要求持卡人确认的应用。
终端配置：不支持持卡人确认。
卡片配置：——卡片和终端有三种共同支持的应用；
——卡的应用有优先顺序；
——在共同支持的应用列表中，带有最高优先级的应用要求持卡人确认；
——卡片返回不是‘9000’的状态码，作为对相互支持的应用列表中第二高优先级的应用最终选择的响应（在终端寻找共同支持应用期间，如果处理正确，则会发送这个SELECT命令）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。在应用最终选择阶段，终端应该绕过需持卡人确认的最高优选级的应用，选择第二优先级的应用，且卡返

回在状态不为‘9000’。卡应该接收另一个SELECT命令选择共同支持的应用列表中的第三高优先级的应用。

7.12.16 CSJM017-00 凭证上的应用标识

测试目的：确保终端打印部分应用PAN（或者全部PAN，若支付系统允许）和AID在交易凭证上。
终端配置：支持打印。
卡片配置：N/A。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该打印部分应用PAN（或者全部PAN，若支付系统允许）和AID的交易凭证。

7.12.17 CSJM018-00 打印在凭证上的数据

测试目的：确保终端用十六进制字符在凭证上打印AID。
终端配置：支持打印。
卡片配置：N/A。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该用十六进制格式打印AID。

7.12.18 CSJM019-00 授权报文使用

测试目的：确保当交易是批数据捕获时，终端使用一个授权请求报文。
终端配置：——支持批数据捕获；
——支持仅联机或脱机/联机。
卡片配置：卡片的参数被设置从而使交易是联机执行的。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该准备并且传输授权请求报文。如果终端同时支持批数据捕获和联机数据捕获那么CSJM01800和CSJM01900两个中有一个通过是可以接受的。

7.12.19 CSJM020-00 金融交易报文使用

测试目的：确保当收单行执行联机数据捕获时，终端使用一个金融交易报文。
终端配置：——支持联机数据捕获；
——支持仅联机或脱机/联机。
卡片配置：卡片的参数被设置从而使交易是联机执行的。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该准备并且传输金融交易报文。如果终端同时支持批数据捕获和联机数据捕获那么CSJM01800和CSJM01900两个中有一个通过是可以接受的。

7.12.20 CSJM021-00 脱机通知报文传送

测试目的：确保当支持批数据捕获时，终端在批数据文件中传送脱机通知。
终端配置：——支持批数据捕获；
——支持通知。
卡片配置：——卡在响应第一个 GENERATE AC AAC时，请求生成通知；
——交易没有被捕获。
测试流程：选择卡片应用，执行交易。
通过标准：终端应传递脱机通知。如果终端同时支持批数据捕获和联机数据捕获那么CSJM02000和CSJM02100两个中有一个通过是可以接受的。

7.12.21 CSJM022-00 联机通知报文传输

测试目的：确保终端实时传输类似授权报文或金融交易报文的联机通知。
终端配置：——支持联机数据捕获；
——支持仅联机或脱机/联机；
——支持通知。
卡片配置：——卡在第一个GENERATE AC时请求生成通知；
——卡片返回应用密文AAC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应准备并且实时传输一个通知报文。如果终端同时支持批数据捕获和联机数据捕获那么CSJM02000和CSJM02100两个中有一个通过是可以接受的。

7.12.22 CSJM023-00 冲正的使用

测试目的：确保终端实时传输冲正报文。
终端配置：——支持联机数据捕获；
——支持仅联机或脱机/联机。
卡片配置：——卡片返回ARQC来响应第一个GENERATE AC；
——返回发卡行长度错误的授权响应给终端。
测试流程：选择卡片应用，执行交易。
通过标准：终端应准备并且实时传输冲正报文到发卡行。

7.12.23 CSJM025-00 当不能联机时，终端发送第二个 GENERATE AC 命令（1）

测试目的：确保如果终端在不能联机时脱机接受交易，则终端设置ARC为‘不能联机进行，脱机接受’，并发送第二个GENERATE AC命令请求TC。
终端配置：——支持仅脱机或支持脱机/联机或；
——仅联机且支持正常的缺省行为代码处理；
——终端不能联机进行（例如，未接收到发卡行的响应）；
——终端行为代码缺省、拒绝、联机所有位设为‘0’。
卡片配置：——所有发卡行行为代码拒绝和联机所有位都设置为‘0’；
——所有发卡行行为代码缺省位都设置为‘0’；
——第一个GENERATE AC命令卡响应为ARQC；
——CDOL2请求ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。终端应发第二个GENERATE AC命令请求TC。ARC应被设置成表示‘不能联机进行，脱机接受’。

7.12.24 CSJM026-00 当不能联机时，终端发送第二个 GENERATE AC 命令（2）

测试目的：确保如果终端在不能联机时脱机拒绝交易，则终端设置ARC为‘不能联机进行，脱机拒绝’，并发送第二个GENERATE AC命令请求AAC。
终端配置：——不支持第一个GAC前处理缺省行为代码；
——如果有联机能力，但终端不能联机进行（例如，未收到发卡行响应）；
——终端行为代码缺省、联机所有位设为‘0’。
卡片配置：——发卡行行为代码拒绝和联机所有位都设置为‘0’；
——第一个GENERATE AC命令卡响应为ARQC；
——CDOL2请求授权响应码ARC。
子类案例：——案例01：卡的SDA失败，发卡行行为代码缺省设置为 ‘40 00 00 00 00’（支持SDA）；
——案例02：金额超出最低限额，发卡行行为代码缺省设置为‘-00 00 00 80 00’（终端风险管理，支持最低限额检查）；

——案例03：卡的应用过期，发卡行行为代码缺省设置为‘-00 40 00 00 00’；
——案例04：LOATC ＝ 0，发卡行行为代码缺省设置为‘-00 08 00 00 00’（终端风险管理，支持频度检查）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理交易直到完成。终端发第二个GENERATE AC命令请求AAC。ARC应被设置成表示‘不能联机进行，脱机拒绝’。

7.12.25 CSJM028-00 终端基于授权响应码继续处理（1）

测试目的：确保如果交易是联机执行时，终端应该根据ARC继续处理交易。

终端配置：支持仅联机或脱机/联机。

卡片配置：——第一个GENERATE AC命令卡响应ARQC；
——CDOL2请求授权响应码ARC。

子类案例：——案例1：授权响应码是联机批准；
——案例2：授权响应码是联机拒绝。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理交易直到完成。授权响应码应该与发卡行返回的一致。依据收到的ARC，终端应该：发送第二个GENERATE AC命令请求TC或发送第二个GENERATE AC命令请求AAC。

7.12.26 CSJM028-01 终端基于授权响应码继续处理（2）

测试目的：确保如果交易是联机执行时，终端应该根据ARC继续处理交易。

终端配置：——支持仅联机或脱机/联机；
——支持发卡行发起的语音授权。

卡片配置：——第一个GENERATE AC命令卡响应ARQC；
——CDOL2请求授权响应码ARC；
——授权响应码是语音授权。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理交易直到完成。授权响应码应该与发卡行返回的相同。依据收到的ARC，终端应该显示“打电话给发卡行”。

7.12.27 CSJM030-00 终端发送第二个 GENERATE AC 命令（1）

测试目的：确保如果终端在接收到的授权响应不正确的情况下脱机批准交易，终端设置ARC为“不能联机进行，脱机接受”，并发送第二个GENERATE AC请求TC。

终端配置：——支持脱机/联机能力；
——或仅联机且支持正常的缺省行为代码处理；
——终端行为代码拒绝和联机所有位都设置为‘0’。

卡片配置：——发卡行行为代码拒绝和联机所有位都设置为‘0’；
——发卡行行为代码缺省所有位都设置为‘0’；
——第一个GENERATE AC命令卡响应ARQC；
——CDOL2请求授权响应码ARC。

子类案例：——案例01：未收到发卡行的授权响应；
——案例02：发卡行返回长度错误的授权响应。

测试流程：选择卡片应用，执行交易。

通过标准：终端应处理交易直到完成。终端在未收到授权响应或授权响应不正确的情况下，可以重发授权请求。ARC应被设置成表示“不能联机进行，脱机接受”。终端应该发送第二个GENERATE AC命令来请求TC。

7.12.28 CSJM031-00 终端发送第二个 GENERATE AC 命令（2）

测试目的：确保如果终端在接收到的授权响应不正确的情况下脱机拒绝交易，终端设置ARC为“不能联机进行，脱机拒绝”，并发送第二个GENERATE AC请求AAC。

终端配置：——支持仅联机或脱机/联机；
——终端行为代码拒绝和联机的所有位都设置为‘0’。
卡片配置：——发卡行行为代码拒绝和联机所有位都设置为‘0’；
——发卡行行为代码缺省设置为‘-00 40 00 00 00’；
——卡片应用已过期；
——第一个GENERATE AC命令卡响应为ARQC；
——CDOL2请求授权响应码ARC。
子类案例：——案例01：未收到发卡行的授权响应；
——案例02：发卡行返回无效长度的授权响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。终端在未收到授权响应或授权响应不正确的情况下，可以重发授权请求。ARC应被设置成表示“不能联机进行，脱机拒绝”。终端应该发送第二个GENERATE AC命令来请求AAC。

7.12.29 CSJM032-00 终端发送冲正报文

测试目的：确保如果执行联机数据捕获，在接收到的授权响应不正确时，终端应该发送冲正报文给发卡行。
终端配置：——支持联机数据捕获，支持仅联机或脱机/联机；
——终端行为代码拒绝和联机所有位都设置为‘0’；
——终端行为代码缺省所有位都设置为‘1’。
卡片配置：——发卡行行为代码拒绝和联机所有位都设置为‘0’；
——发卡行行为代码缺省所有位都设置为‘0’；
——第一个GENERATE AC命令卡响应ARQC；
——卡的AIP中标记的某种与TAC缺省位相关的功能执行失败。
子类案例：——案例01：未收到发卡行的授权响应；
——案例02：发卡行返回无效长度的授权响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该处理交易直到完成。终端应该发送第二个GENERATE AC命令请求AAC。在未收到授权响应或授权响应不正确情况下，终端可以重发授权请求报文。终端应该准备并且发送一个冲正报文。

7.12.30 CSJM033-00 终端创建金融记录

测试目的：确保终端应该创建一个金融记录，如果冲正已经发出，且交易最终被批准。
终端配置：——支持联机数据捕获；
——支持仅联机或脱机/联机且支持当不能联机时，正常处理缺省行为码；
——终端行为代码拒绝、拒绝和联机所有位都设置为‘0’。
卡片配置：——执行联机数据捕获；
——发卡行行为代码拒绝和联机所有位都设置为‘0’；
——发卡行行为代码缺省所有位都设置为‘0’；
——第一个GENERATE AC命令卡响应ARQC。
子类案例：——案例01：未收到发卡行的授权响应；
——案例02：发卡行返回长度错误的授权响应。
测试流程：选择卡片应用，执行交易。
通过标准：终端应处理交易直到完成。在收到第一个GENERATE AC命令响应后，终端应该发送一个金融交易请求报文。在未收到授权响应或授权响应不正确情况下，终端可以重发授权请求。卡应该接收到第二个GENERATE AC命令请求TC。在收到第二个GENERATE AC命令的响应后，终端应该发送一个冲正报文。在收到第二个GENERATE AC命令的响应后，终端应该创建一个金融记录并发送给发卡行。

7.12.31 CSJM034-00 终端终止发卡行脚本处理（1）

测试目的：确保终端终止脚本处理，如果出现一个脚本长度错误或格式错误。
终端配置：——支持仅联机或脱机/联机；
——不支持脚本飞。
卡片配置：——卡的参数被设置从而使交易联机执行；
——所有接收到的脚本都有一个唯一的脚本标识符。
子类案例：——案例01：发卡行脚本响应包含2个‘71’脚本：一个‘71’脚本格式错误：带有3个脚本命令，第一个标签 86的长度大于命令本身长度。另一个是正确的‘71’脚本；
——案例02：发卡行脚本响应包含2个‘71’脚本：一个‘71’脚本带有格式错误：脚本命令标签不正确，接下来是一个正确的‘71’脚本。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端不应该发送第一个脚本的任何命令。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。在金融确认报文或批数据捕获报文中，TVR的字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。在接收到第二个GENERATE AC命令时，TSI 的字节1，位3 =‘1’（脚本处理已进行）。包含在金融确认报文或批数据捕获报文中的发卡行脚本结果应该设置成：‘-00 xx xx xx xx 20 yy yy yy yy’。

7.12.32 CSJM034-01 终端终止发卡行脚本处理（2）

测试目的：确保终端终止脚本处理，如果出现一个脚本长度错误或格式错误。
终端配置：支持仅联机或脱机/联机。
卡片配置：卡的参数被设置从而使交易联机执行。
子类案例：——案例01：发卡行脚本响应包含2个‘72’脚本：一个‘72’脚本格式错误：带有3个脚本命令，第一个标签 86的长度大于命令本身长度。另一个是正确的‘72’脚本；
——案例02：发卡行脚本响应包含2个‘72’脚本：一个‘72’脚本带有格式错误：脚本命令标签不正确，接下来是一个正确的‘72’脚本。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端不应该发送第一个脚本的任何命令。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。包含在金融确认报文或批数据捕获报文中的TVR的字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。包含在金融确认报文或批数据捕获报文中的TSI 的字节1，位3 =‘1’（脚本处理已进行）。包含在金融确认信息或批数据捕获消息中的发卡行脚本结果应该设置成：‘-00 xx xx xx xx 20 yy yy yy yy’。

7.12.33 CSJM034-02 终端终止超过设备长度的发卡行脚本处理（1）

测试目的：确保终端终止脚本处理，如果发卡行脚本长度超过设备限制。
终端配置：——支持仅联机或脱机/联机；
——支持设备脚本限制＝>128字节。
卡片配置：——卡的参数被设置从而使交易联机执行；
——收到的所有脚本有唯一的脚本标识；
——发卡行下发两个‘71’脚本（总长度超过128字节）。第一个脚本长度100个字节，第二个脚本长度至少29个字节。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该处理交易直到完成。终端应该处理第一个发卡行脚本并且终止第二个的处理。在接收到的第二个GENERATE AC命令中，TVR的字节5，位6 =‘1’

（最后一次GENERATE AC命令之前脚本处理失败）。包含在金融确认报文或批数据获取报文中的TVR字节5，位5 ='0'（最后一次GENERATE AC命令之后脚本处理未进行）。在接收到的第二个GENERATE AC命令中，TSI的字节1，位3 ='1'（脚本处理已进行）。包含在金融确认报文或批数据捕获报文中的发卡行脚本结果应该等于：'20 xx xx xx xx 00 yy yy yy yy'。

7.12.34 CSJM034-03 终端终止超过设备长度的发卡行脚本处理（2）

测试目的：确保如果发卡行脚本长度超过设备限制，终端终止脚本处理。

终端配置：——支持仅联机或脱机/联机；
——支持设备脚本限制=>128字节。

卡片配置：——卡的参数被设置从而使交易联机执行；
——收到的所有脚本有唯一的脚本标识；
——发卡行下发两个'72'脚本（总长度网络/终端支持的最大长度，如超过128字节）第一个脚本长度100个字节，第二个脚本长度至少29个字节。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该处理交易直到完成。终端应该处理第一个发卡行脚本并且终止第二个的处理。包含在金融确认报文或批数据获取报文中的TVR的字节5，位6 ='0'（最后一次GENERATE AC命令之前脚本处理未进行）。包含在金融确认报文或批数据获取报文中的TVR字节5，位5 ='1'（最后一次GENERATE AC命令之后脚本处理失败）。包含在金融确认报文或批数据获取报文中的TSI的字节1，位3 ='1'（脚本处理已进行）。包含在金融确认报文或批数据捕获报文中的发卡行脚本结果应该等于：'20 xx xx xx xx 00 yy yy yy yy'。

7.12.35 CSJM034-04 终端终止超过设备长度的发卡行脚本处理（3）

测试目的：确保如果发卡行脚本长度或格式错误，终端终止脚本处理。

终端配置：——支持仅联机或脱机/联机；
——支持脚本飞。

卡片配置：——卡的参数被设置从而使交易联机执行；
——所有接收到的脚本都有一个唯一的标识。

子类案例：——案例01：发卡行脚本响应包含2个'71'脚本：一个'71'脚本格式错误：带有3个脚本命令，第一个标签 86的长度大于命令本身长度。另一个是正确的'71'脚本；
——案例02：发卡行脚本响应包含2个'71'脚本：一个'71'脚本带有格式错误：脚本命令标签不正确，接下来是一个正确的'71'脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在第二次GAC中的TVR的字节5，位6 ='1'（最后一次GENERATE AC命令之前脚本处理未进行）。包含在金融确认报文或批数据获取报文中的TVR字节5，位5 ='0'（最后一次GENERATE AC命令之后脚本处理失败）。包含在第二次GAC中的中的TSI的字节1，位3 ='1'（脚本处理已进行）。包含在金融确认报文或批数据捕获报文中的第一个发卡行脚本结果应该设置成'00'或者'1x'。

7.12.36 CSJM035-00 发卡行脚本结果的设置（1）

测试目的：确保终端终止发卡行脚本的处理，并在发卡行脚本结果中设置脚本错误，如果发卡行脚本不能正确的解析。

终端配置：——支持仅联机或脱机/联机；
——不支持脚本飞。

卡片配置：卡的参数被设置从而使交易联机执行。

子类案例：——案例01：发卡行发送'71'的脚本：脚本标识（'44 33 22 11'）可读，有一个格式错误，3个脚本命令中的第一个标签 86的长度大于命

令本身长度；

——案例 02：发卡行发送‘71’的脚本：脚本标识（‘44 33 22 11’）可读，一个格式错误：脚本命令标签不正确。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该终止不能解析的发卡行脚本处理，并继续后来可读的脚本。案例01：发卡行脚本结果（包含在金融确认报文或批数据捕获报文中）设置为‘-00 44 33 22 11’，错误脚本未执行。案例02：发卡行脚本结果（包含在金融确认报文或批数据捕获报文中）设置为‘-00 00 00 00 00’。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。包含在金融确认报文或批数据捕获报文中的TVR的字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理未进行）。包含在金融确认报文或批数据捕获报文中的TSI 的字节1，位3 =‘1’（脚本处理已进行）。

7.12.37 CSJM035-01 发卡行脚本结果的设置（2）

测试目的：确保终端终止发卡行脚本处理，且在发卡行脚本结果中报告脚本错误，如果发卡行脚本不能正确的解析。

终端配置：——支持仅联机或脱机/联机；

——不支持脚本飞。

卡片配置：卡的参数被设置从而使交易联机执行。

子类案例：——案例01：发卡行发送‘72’脚本：脚本标识（‘44 33 22 11’）可读，脚本格式错误，3个脚本命令中的第一个标签‘ 86’的长度大于命令本身长度；

——案例 02：发卡行发送‘72’的脚本：脚本标识（‘44 33 22 11’）可读，一个格式错误：脚本命令标签不正确。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该终止不能解析的发卡行脚本处理，并继续后来可读的脚本。案例01：发卡行脚本结果（包含在金融确认报文或批数据捕获报文中）设置为‘-00 44 33 22 11’，错误脚本未执行。案例02：发卡行脚本结果（包含在金融确认报文或批数据捕获报文中）设置为‘-00 00 00 00 00’，错误脚本未执行。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。包含在金融确认报文或批数据捕获报文中的TVR的字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。包含在金融确认报文或批数据捕获报文中的TSI 的字节1，位3 =‘1’（脚本处理已进行）。

7.12.38 CSJM035-02 发卡行脚本结果的设置（3）

测试目的：确保终端终止发卡行脚本处理，且在发卡行脚本结果中报告脚本错误，如果发卡行脚本不能正确的解析。

终端配置：支持仅联机或脱机/联机。

卡片配置：卡的参数被设置从而使交易联机执行。

子类案例：——案例01：发卡行发送回一个‘71’脚本和一个‘72’脚本，都带有可读脚本标识：脚本‘71’有一个语法错误，脚本‘72’正确；

——案例 02：发卡行发送回一个‘71’脚本和一个‘72’脚本，都带有可读脚本标识：脚本‘71’ 正确，脚本‘72’有一个语法错误；

——案例 03：发卡行发送回两个‘71’脚本和一个‘72’脚本，都带有可读脚本标识：第一个脚本‘71’正确，第二个脚本‘71’有一个语法错误，脚本‘72’正确；

——案例 04：发卡行发送回两个‘71’脚本和两个‘72’脚本，都带有可读脚本标识：第一个脚本‘71’正确，第二个脚本‘71’有一个语法错误，

第一个脚本‘72’正确，第二个脚本‘72’有一个语法错误。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该终止无法正确解析的发卡行脚本处理，并继续处理后面可读的脚本。每个错误的脚本的发卡行脚本结果（包含在金融确认消息或批数据捕获消息中）设置为‘00’，错误脚本未执行。根据每个子案例，TVR的字节5，位5和位6应设为正确的值 。包含在金融确认报文或批数据捕获报文中的TSI 的字节1，位3 =‘1’（脚本处理已进行）。

7.12.39 CSJM035-03 发卡行脚本结果的设置（4）

测试目的：确保终端终止发卡行脚本处理，且在发卡行脚本结果中报告脚本错误，如果发卡行脚本不能正确的解析。

终端配置：——支持仅联机或脱机/联机；

——支持脚本飞。

卡片配置：卡的参数被设置从而使交易联机执行。

子类案例：——案例01：发卡行发送‘71’脚本：脚本标识（‘44 33 22 11’）可读，脚本格式错误，3个脚本命令中的第一个标签‘ 86’的长度大于命令本身长度；

——案例 02：发卡行发送‘71’的脚本：脚本标识（‘44 33 22 11’）可读，一个格式错误：脚本命令标签不正确。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该终止不能解析的发卡行脚本处理，并继续后来可读的脚本。案例01：发卡行脚本结果（包含在金融确认报文或批数据捕获报文中）设置为‘1x 44 33 22 11’或‘-00 44 33 22 11’。案例02：发卡行脚本结果（包含在金融确认报文或批数据捕获报文中）设置为‘-00 00 00 00 00’，失败的脚本未被执行。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理未进行）。包含在金融确认报文或批数据捕获报文中的TVR的字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理失败）。包含在金融确认报文或批数据捕获报文中的TSI 的字节1，位3 =‘1’（脚本处理已进行）。

7.12.40 CSJM035-04 发卡行脚本结果的设置（5）

测试目的：确保终端终止发卡行脚本处理，且在发卡行脚本结果中报告脚本错误，如果发卡行脚本不能正确的解析。

终端配置：——支持仅联机或脱机/联机；

——支持脚本飞。

卡片配置：卡的参数被设置从而使交易联机执行。

子类案例：——案例01：发卡行发送‘72’脚本：脚本标识（‘44 33 22 11’）可读，脚本格式错误，3个脚本命令中的第一个标签‘ 86’的长度大于命令本身长度；

——案例 02：发卡行发送‘72’的脚本：脚本标识（‘44 33 22 11’）可读，一个格式错误：脚本命令标签不正确。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该终止不能解析的发卡行脚本处理，并继续后来可读的脚本。案例01：发卡行脚本结果（包含在金融确认报文或批数据捕获报文中）设置为‘1x 44 33 22 11’或‘-00 44 33 22 11’。案例02：发卡行脚本结果（包含在金融确认报文或批数据捕获报文中）设置为‘-00 00 00 00 00’，失败的脚本未被执行。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理未进行）。包含在金融确认报文或批数据捕获报文中的TVR的字节5，位5

='1'（最后一次GENERATE AC命令之后脚本处理失败）。包含在金融确认报文或批数据捕获报文中的TSI 的字节1，位3 ='1'（脚本处理已进行）。

7.12.41 CSJM036-00 终端继续处理后面的发卡行脚本（1）

测试目的：确保终端继续处理后面的脚本，如果当前脚本有一个语法错误。
终端配置：支持仅联机或脱机/联机。
卡片配置：卡的参数被设置从而使交易联机执行。
子类案例：——案例01：发卡行返回两个'71'脚本：脚本1有一个语法错误， 脚本2正确；
——案例 02：发卡行返回三个'71'脚本：脚本 3 有一个语法错误，脚本 1 和 2 正确；
——案例 03：发卡行返回两个'71'脚本：脚本 1 正确，脚本 2 有一个语法错误。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该仅收到来自正确脚本的脚本命令。

7.12.42 CSJM036-01 终端继续处理后面的发卡行脚本（2）

测试目的：确保终端继续处理后面的脚本，如果当前脚本有一个语法错误。
终端配置：支持仅联机或脱机/联机。
卡片配置：卡的参数被设置从而使交易联机执行。
子类案例：——案例01：发卡行返回两个'72' 脚本：脚本1有一个语法错误，脚本2正确；
——案例 02：发卡行返回三个'72'脚本：脚本 3 有一个语法错误，脚本 1 和 2 正确；
——案例 03：发卡行返回两个'72'脚本：脚本 1 正确，脚本 2 有一个语法错误。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该仅收到来自正确脚本的脚本命令。

7.12.43 CSJM036-02 终端继续处理后面的发卡行脚本（3）

测试目的：确保终端继续处理后面的脚本，如果当前脚本有一个语法错误。
终端配置：支持仅联机或脱机/联机。
卡片配置：卡的参数被设置从而使交易联机执行。
子类案例：——案例01：发卡行返回一个'71'脚本和一个'72'脚本：脚本'71'有一个语法错误，脚本'72'正确；
——案例 02：发卡行返回一个'71'脚本和一个'72'脚本：脚本'71' 正确，脚本'72' 有一个语法错误；
——案例 03：发卡行返回两个'71'脚本和一个'72'脚本：第一个脚本'71'正确，第二个脚本'71' 有一个语法错误，脚本'72'正确。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。卡应该仅收到来自正确脚本的脚本命令。

7.12.44 CSJM037-00 报文中的所有数据来自芯片（1）

测试目的：确保当一个数据存在于磁条不在IC卡中时，终端不使用磁条中的数据生成授权或金融交易报文。
终端配置：支持磁条/IC复合读卡器并且磁条先读。
卡片配置：磁条中存在数据，在IC中不存在：二磁等价数据'57'，服务代码'5F30'。

测试流程：选择卡片应用，执行交易。
通过标准：授权报文，金融交易报文，批数据报文中不应该包含这个磁条数据（服务代码‘5F30’）。

7.12.45 CSJM038-00 报文中的所有数据来自芯片（2）

测试目的：确保当一个数据存在于磁条不在IC卡中时，终端不使用磁条中的数据生成授权或金融交易报文。
终端配置：支持磁条/IC复合读卡器并且磁条先读。
卡片配置：一个数据，在IC和磁条中数值不同：二磁等价数据‘57’。
测试流程：选择卡片应用，执行交易。
通过标准：对于联机交易的授权报文或金融交易报文，应该包含IC中的数据。对于脱机交易，须在批数据报文中检查该数据。

7.13 终端数据元的编码（YSBM）

7.13.1 YSBM001-00 终端类型

测试目的：确保终端的终端类型是依照它的实际类型进行的编码。
终端配置：N/A。
卡片配置：CDOL1请求终端类型和终端性能。
测试流程：选择卡片应用，执行交易。
通过标准：终端性能应该依照下面进行编码：
——有服务员的终端 x1 或 x2 或 x3；
——无人服务的终端 x4 或 x5 或 x6；
——金融机构操作的终端 1x；
——商户操作的终端 2x；
——持卡人操作的终端 3x；
——仅联机的终端 x1 或 x4；
——支持脱机和联机的终端 x2 或 x5；
——仅支持脱机的终端 x3 或 x6。

7.13.2 YSBM002-00 终端性能

测试目的：确保终端性能是依照它的实际性能进行编码的。
终端配置：N/A。
卡片配置：CDOL1请求终端性能。
测试流程：选择卡片应用，执行交易。
通过标准：终端性能应该依照下面进行编码：
——人工密钥输入 字节 1，位 8 ＝‘1’；
——磁条 字节 1，位 7 ＝‘1’；
——带触点的 IC 字节 1，位 6 ＝‘1’；
——明文 PIN 由 IC 卡验证 字节 2，位 8 ＝‘1’；
——联机密文 PIN 字节 2，位 7 ＝‘1’；
——签名 字节 2，位 6 ＝‘1’；
——RFU 字节 2，位 5 ＝‘1’；
——不要求 CVM 字节 2，位 4 ＝‘1’；
——持卡人证件验证 字节 2，位 1 ＝‘1’；
——SDA 字节 3，位 8 ＝‘1’；
——DDA 字节 3，位 7 ＝‘1’；
——吞卡 字节 3，位 6 ＝‘1’；
——CDA 字节 3，位 4 ＝‘1’。

7.13.3 YSBM003-00 终端附加性能

测试目的：确保终端附加性能是依照它的实际性能进行编码。
终端配置：N/A。
卡片配置：CDOL1请求终端附加性能。
测试流程：选择卡片应用，执行交易。
通过标准：交易类型性能应该依照下面指出的终端支持的特征进行编码：
——现金存款 字节2，位8 ＝ ‘1’；
——现金 字节1，位8 ＝ ‘1’；
——商品 字节1，位7 ＝ ‘1’；
——服务 字节1，位6 ＝ ‘1’；
——返现 字节1，位5 ＝ ‘1’；
——查询 字节1，位4 ＝ ‘1’；
——转账 字节1，位3 ＝ ‘1’；
——付款 字节1，位2 ＝ ‘1’；
——管理 字节1，位1 ＝ ‘1’；
——数字键 字节3，位8 ＝ ‘1’；
——字母和特殊字符键 字节3，位7 ＝ ‘1’；
——命令键 字节3，位6 ＝ ‘1’；
——功能键 字节3，位5 ＝ ‘1’；
——打印，给服务员 字节4，位8 ＝ ‘1’；
——打印，给持卡人 字节4，位7 ＝ ‘1’；
——显示，给服务员 字节4，位6 ＝ ‘1’；
——显示，给持卡人 字节4，位5 ＝ ‘1’；
——编码表10 字节4，位2 ＝ ‘1’；
——编码表9 字节4，位1 ＝ ‘1’；
——编码表8 字节5，位8 ＝ ‘1’；
——编码表7 字节5，位7 ＝ ‘1’；
——编码表6 字节5，位6 ＝ ‘1’；
——编码表5 字节5，位5 ＝ ‘1’；
——编码表4 字节5，位4 ＝ ‘1’；
——编码表3 字节5，位3 ＝ ‘1’；
——编码表2 字节5，位2 ＝ ‘1’；
——编码表1 字节5，位1 ＝‘1’。

7.13.4 YSBM004-00 账户类型

测试目的：确保终端存储账户类型到指定的标签中，当某种账户类型被选择。
终端配置：支持账户类型。
卡片配置：——PDOL请求账户类型（‘5F57’）；
——某种账户类型被选中。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该在PDOL中发送选中的账户类型。

7.14 命令语法（MLYF）

7.14.1 MLYF001-00 强制命令

测试目的：确保在交易流程中，终端在适当时机正确发送强制的基本命令。
终端配置：N/A。
卡片配置：——卡包含值为‘0000’的AIP——卡不支持附加功能；
——卡包含以下强制的数据对象（应用失效日期，应用PAN，CDOL1 和

CDOL2）。

子类案例：——案例1：卡请求一个交易，使用T=0协议；

——案例2：卡请求一个交易，使用T=1协议。

测试流程：终端应该执行以下功能，作为基本借记/贷记应用交易的一部分：

a）应用选择；

b）应用初始化；

c）读应用数据；

d）终端行为分析；

e）完成。

通过标准：——两种协议下，终端应接受卡片并来完成交易。终端发送的命令应符合正确格式。 终端应该发送以下指定的所有强制命令。每个命令都应该包含正确的语法并在适当的时候发送(包括以下的命令和遵循以下的命令语法)；

——SELECT：强制命令；-00 A0 04 00 Lc 命令数据 Le；Lc ＝ 05 10（命令数据的长度）；命令数据 ＝ 文件名；Le ＝（不存在 T ＝ 0）；

——GET PROCESSING OPTIONS：强制命令；80 A8 00 00 Lc 命令数据 Le；Lc ＝ 可变（命令数据的长度）；命令数据 ＝（PDOL 中指定）；Le ＝（不存在 T ＝ 0）；

——Read Record：强制命令；-00 B2 P1 P2 00；P1 ＝ 记录号；P2 ＝ 控制参数 SFI；由 AFL 决定发送若干个 Read Record 命令；

——GENERATE AC：强制命令；80 AE P1 00 Lc 命令数据 Le；P1 ＝控制参数（00AAC，40TC，80ARQC）；Le ＝ 00（不存在 T ＝ 0）。

7.14.2 MLYF002-00 SELECT NEXT 命令

测试目的：确保在交易流程中，终端在适当时机正确发送SELECT NEXT命令。

终端配置：N/A。

卡片配置：——卡包含比终端存储的AID长的DF名称；

——卡包含值为‘-00 00’的 AIP——卡不支持附加功能；

——卡包含以下强制的数据对象（应用失效日期，应用 PAN，CDOL1 和 CDOL2）。

子类案例：——案例 1：卡请求一个交易，使用 T=0 协议；

——案例 2：卡请求一个交易，使用 T=1 协议。

测试流程：终端应该执行以下功能作为基本借记/贷记应用交易的一部分：

a）应用选择；

b）应用初始化；

c）读应用数据；

d）终端行为分析；

e）完成。

通过标准：——两种协议下，终端应接受卡片并来完成交易。终端发送的命令应符合正确格式。终端应该发送以下指定的所有强制命令。终端在收到一个比终端中存储AID长的DF名时，应发送SELECT NEXT 命令。每个命令都应包含正确的语法并在适当的时候发送(包括以下的命令和遵循以下的命令语法)；

——SELECT：强制命令；-00 A0 04 00 Lc 命令数据 Le；Lc ＝ 05 10（命令数据的长度）；命令数据 ＝ 文件名；Le ＝（不存在 T ＝ 0）；

——SELECT NEXT：强制命令；-00 A0 04 02 Lc 命令数据 Le；Lc ＝ 05 10（命令数据的长度）；命令数据 ＝ 文件名；Le ＝（不存在 T ＝ 0）；

——GET PROCESSING OPTIONS：强制命令；80 A8 00 00 Lc 命令数据 Le；Lc ＝ 可变(命令数据的长度)；命令数据 ＝(PDOL 指定的数据对象)；

Le ＝（不存在 T ＝ 0）；

——Read Record：强制命令；-00 B2 P1 P2 00；P1 ＝ 记录号；P2 ＝ 控制参数 SFI；由 AFL 决定发送若干个 Read Record 命令；

——GENERATE AC：强制命令；80 AE P1 00 Lc 命令数据 Le；P1 ＝控制参数（00AAC，40TC，80ARQC）；Le ＝ 00（不存在 T ＝ 0）。

7.14.3 MLYF003-00 INTERNAL AUTHENTICATE 命令

测试目的：确保如果终端支持DDA，应该正确发送INTERNAL AUTHENTICATE命令。

终端配置：支持DDA。

卡片配置：——卡包含支持DDA所应的数据对象；

——卡包含值为‘20 00’的 AIP－支持 DDA；

——卡包含以下强制的数据对象（应用失效日期，应用 PAN，CDOL1 和 CDOL2）。

子类案例：——案例 1：卡请求一个交易，使用 T=0 协议；

——案例 2：卡请求一个交易，使用 T=1 协议。

测试流程：终端应该执行以下功能作为基本借记/贷记应用交易的一部分：

a）应用选择；

b）应用初始化；

c）读应用数据；

d）脱机数据认证；

e）终端行为分析；

f）完成。

通过标准：——两种协议下，终端应接受卡片并来完成交易。终端发送的命令应该符合正确命令格式。终端应该发送如下的强制命令。终端应该在读应用数据后，第一个 GENERATE AC命令前，发送INTERNAL AUTHENTICATE命令。每个命令都应包含正确的语法并在适当的时候发送(包括以下的命令和遵循以下的命令语法)；

——SELECT：强制命令；-00 A0 04 00 Lc 命令数据 Le；Lc ＝ 05 10（命令数据的长度）；命令数据 ＝ 文件名；Le ＝（不存在 T ＝ 0）；

——GET PROCESSING OPTIONS：强制命令；80 A8 00 00 Lc 命令数据 Le；Lc ＝ 可变(命令数据的长度)；命令数据 ＝(PDOL 指定的数据对象)；Le ＝（不存在 T ＝ 0）；

——Read Record：强制命令；-00 B2 P1 P2 00；P1 ＝ 记录号；P2 ＝ 控制参数 SFI；由 AFL 决定发送若干个 Read Record 命令；

——INTERNAL AUTHENTICATE：强制命令（如果终端支持 DDA）；-00 88 00 00 Lc 命令数据 Le；Lc ＝（命令数据的长度）；命令数据 ＝ 认证相关数据的长度；Le ＝ 00（不存在 T ＝ 0）；

——GENERATE AC：强制命令；80 AE P1 00 Lc 命令数据 Le；P1 ＝ 控制参数（00AAC，40TC，80ARQC）；Le ＝ 00（不存在 T ＝ 0）。

7.14.4 MLYF004-00 VERIFY 命令

测试目的：确保终端支持持卡人认证形式，由IC卡的明文验证，以及在交易流程中，发送正确形式的VERIFY命令并在适当的时机发送。如果终端支持取PIN重试次数的Get Data，则Get Data命令应该在VERIFY命令前发送。

终端配置：支持明文PIN。

卡片配置：——卡包含CVM列表，CVM要求‘卡片执行明文PIN验证’（0100）；

——卡包含值为‘10 00’的 AIP－支持持卡人认证；

——卡包含以下强制的数据对象（应用失效日期，应用 PAN，CDOL1 和 CDOL2）。

子类案例：——案例 1：卡请求一个交易，使用 T=0 协议；

——案例 2：卡请求一个交易，使用 T=1 协议。

测试流程：终端应该执行以下功能作为基本借记/贷记应用交易的一部分：

a）应用选择；
b）应用初始化；
c）读应用数据；
d）持卡人确认；
e）终端行为分析；
f）完成。

通过标准：——两种协议下，终端应接受卡片并来完成交易。终端应该发送符合正确格式的命令。 终端应该发送如下指定的所有强制命令。如果终端支持取PIN重试次数的Get Data，则它应该在VERIFY命令前发送。终端应该在读应用后，第一个GENERATE AC命令前，发送VERIFY命令。每个命令都应包含正确的语法并在适当的时候发送(包括以下的命令和遵循以下的命令语法)；

——SELECT：强制命令；-00 A0 04 00 Lc 命令数据 Le；Lc ＝ 05 10（命令数据的长度）；命令数据 ＝ 文件名；Le ＝（不存在 T ＝ 0）；

——GET PROCESSING OPTIONS：强制命令；80 A8 00 00 Lc 命令数据 Le；Lc ＝ 可变(命令数据的长度)；命令数据 ＝(PDOL 指定的数据对象)；Le ＝（不存在 T ＝ 0）；

——Read Record：强制命令；-00 B2 P1 P2 00；P1 ＝ 记录号；P2 ＝ 控制参数 SFI；由 AFL 决定发送若干个 Read Record 命令；

——Get Data For PIN Try Counter：如果终端支持；80 CA 9F 17 00；Lc ＝ 不存在；命令数据 ＝ 不存在；

——VERIFY 命令；-00 20 00 P2 Lc 命令数据 Le；P2 ＝（80 – 明文）；命令数据 ＝ 交易 PIN 数据；Le ＝（不存在 ）；

——GENERATE AC：强制命令；80 AE P1 00 Lc 命令数据 Le；P1 ＝ 控制参数（00AAC，40TC，80ARQC）；Le ＝ 00（不存在 T ＝ 0）。

7.14.5 MLYF006-00 Get Data 命令

测试目的：确保如果终端支持频度检查作为TRM的一部分，则在交易测试流程期间，终端应该发送正确形式的Get Data命令并在适当时机发送。

终端配置：支持频度检查。

卡片配置：——卡的AIP指明支持TRM；

——卡包含以下强制的数据对象（应用失效日期，应用PAN，CDOL1 和CDOL2）；

——卡中包含UCOL和LCOL。

子类案例：——案例1：卡请求一个交易，使用T=0协议；

——案例2：卡请求一个交易，使用T=1协议。

测试流程：终端应该执行以下功能作为基本借记/贷记应用交易的一部分：

a）应用选择；
b）应用初始化；
c）读应用数据；
d）终端风险管理；
e）终端行为分析；
f）完成。

通过标准：——两种协议下，终端应接受卡片并来完成交易。终端应该发送正确格式的命令。终端应该发送以下指定的所有强制命令。终端应该在读应用数据后，在第一个 GENERATE AC命令前发送Get Data命令取应用交易计数器ATC和上次联机应用交易计数器LOATC。每个命令都应包含正确的语法并

在适当的时候发送（包括以下的命令和遵循以下的命令语法）；

——SELECT：强制命令；-00 A0 04 00 Lc 命令数据 Le；Lc ＝ 05　10（命令数据的长度）；命令数据 ＝ 文件名；Le ＝（不存在 T ＝ 0）；

——GET PROCESSING OPTIONS：强制命令；80 A8 00 00 Lc 命令数据 Le；Lc ＝ 可变（命令数据的长度）；命令数据 ＝（PDOL）；Le ＝（不存在 T ＝ 0）；

——Read Record：强制命令；-00 B2 P1 P2 00；P1 ＝ 记录号；P2 ＝控制参数 SFI；由 AFL 决定发送若干个 Read Record 命令；

——Get Data For ATC：强制命令；80 CA 9F 36 00；Lc ＝ 不存在；命令数据 ＝ 不存在；

——Get Data For 最终联机 ATC：强制命令；80 CA 9F 13 00；Lc ＝ 不存在；命令数据 ＝ 不存在；

——GENERATE AC：强制命令；80 AE P1 00 Lc 命令数据 Le；P1 ＝控制参数（00AAC，40TC，80ARQC）；Le ＝ 00（不存在 T ＝ 0）。

7.14.6　MLYF007-00 External Authenticate 命令

测试目的：确保带有联机能力的终端能够发送External Authenticate命令，在第一个GENERATE AC命令后，第二个GENERATE AC命令前。在交易流程期间，命令应该在适当时机正确发送。

终端配置：支持联机或脱机/联机。

卡片配置：——卡包含值为‘04 00’的AIP－支持发卡行认证；

——卡包含以下强制的数据对象（应用失效日期，应用PAN，CDOL1 和CDOL2）；

——第一个GENERATE AC－ARQC；

——发卡行认证数据 － 作为响应从host返回。

子类案例：——案例1：卡请求一个交易，使用T=0协议；

——案例2：卡请求一个交易，使用T=1协议。

测试流程：终端应该执行以下功能作为基本借记/贷记应用交易的一部分：

a）应用选择；

b）应用初始化；

c）读应用数据；

d）终端行为分析；

e）联机处理；

f）发卡行认证；

g）完成。

通过标准：——两种协议下，终端应接受卡片并来完成交易。终端应该发送正确格式的命令。终端应该发送如下指定的所有强制命令。终端应该在第一个GENERATE AC命令后，第二个GENERATE AC命令前，发送External Authenticate命令。每个命令都应包含正确的语法并在适当的时候发送（包括以下的命令和遵循以下的命令语法）；

——SELECT：强制命令；-00 A0 04 00 Lc 命令数据 Le；Lc ＝ 05　10（命令数据的长度）；命令数据 ＝ 文件名；Le ＝（不存在 T ＝ 0）；

——GET PROCESSING OPTIONS：强制命令；80 A8 00 00 Lc 命令数据 Le；Lc ＝ 可变（命令数据的长度）；命令数据 ＝（PDOL）；Le ＝（不存在 T ＝ 0）；

——Read Record：强制命令；-00 B2 P1 P2 00；P1 ＝ 记录号；P2 ＝ 控制参数 SFI；由 AFL 决定发送若干个 Read Record 命令；

——第一个 GENERATE AC：强制命令；80 AE P1 00 Lc 命令数据 Le；P1 ＝控制参数（00AAC，40TC，80ARQC）；注意：对于这个测试 P1 ＝ 80；

Le ＝ 00（不存在 T ＝ 0）；

——External Authenticate：强制命令；-00 82 00 00 Lc 命令数据 Le；Lc ＝ 8　16（命令数据的长度）；命令数据 ＝发卡行认证数据；Le ＝不存在；

——第二个 GENERATE AC：强制命令；80 AE P1 00 Lc 命令数据 Le；P1 ＝控制参数（00AAC，40TC，80ARQC）；Le ＝ 00（不存在 T ＝ 0）。

7.14.7 MLYF014-00 交易流程中的功能组合测试：脱机 PIN 和 PIN 重试次数超限生成通知

测试目的：确保当要求PIN重试次数超限生成通知，及PIN脱机认证失败时，终端能够执行交易。

终端配置：支持通知且支持明文PIN。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的 字节1，位5为1）；

——CVM 要求是‘脱机明文 PIN 验证’（0100）；

——卡响应 GENERATE AC 命令的 CID 的 2、4 位为 1；

——卡响应 GENERATE AC 的密文类型为 AAC；

——持卡人输入一个错误的 PIN。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该处理交易，直到完成并且拒绝。终端应该发送一个通知报文只有当它不能存储在批数据文件中时。第一个GENERATE AC命令中的TVR字节3，位8 =‘1’（i-e持卡人认证失败）。在接收到第一个GENERATE AC命令时，TSI的字节1，位7 =‘1’（持卡人认证完成）。

7.14.8 MLYF014-01 交易流程中的功能组合测试：脱机 PIN 和 PIN 重试次数超限的通知（2）

测试目的：确保当要求PIN重试次数超限生成通知，及PIN脱机认证正确时，终端能够执行交易。

终端配置：支持通知且支持明文PIN。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的 字节1，位5为1）；

——CVM 要求是‘执行脱机明文 PIN 验证’（0100）；

——卡中 PIN 验证正确的出现；

——卡响应 GENERATE AC 命令的 CID 的 2、4 位设为 1；

——卡响应 GENERATE AC 的密文类型为 TC；

——持卡人输入一个有效的 PIN。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该来完成交易并且获得批准。在接收到的第一个GENERATE AC命令中，TVR的字节3，位8 =‘0’（持卡人认证成功）。在接收到的第一个GENERATE AC命令中，TSI的字节1，位7 =‘1’（持卡人认证完成）。

7.14.9 MLYF015-00 交易流程中的功能组合测试：SDA、用 1 个或 2 个字节编码的记录长度

测试目的：确保终端支持SDA，且用于SDA计算中的记录用1或2字节长度来编码。

终端配置：——支持SDA；

——终端包含卡指定的 CA 公钥。

卡片配置：——卡的AIP指明支持SDA（AIP的 字节1，位7为1）；

——卡中的签名静态应用数据是正确的。

子类案例：——案例01：在AFL中列出的，参加数据认证的记录长度用1字节编码（位8＝0）；

——案例02：在AFL中列出的，参加数据认证的记录长度用2字节编码（81xx）；

——案例03：参加数据认证的数据对象的长度用1字节编码（位8＝0）；

——案例04：参加数据认证的数据对象的长度用2字节编码（81xx）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端性能应该指示支持SDA。第

一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。在接收到第一个GENERATE AC命令时，TSI的字节1，位8 =‘1’（脱机数据认证完成）。第一个 GENERATE AC命令中的 TVR字节1，位2 = ‘1’（SDA执行）。

7.14.10 MLYF015-01 交易流程中的功能组合测试：SDA 和私有文件的记录长度用 1 或 2 字节编码

测试目的：确保终端支持SDA，参与SDA计算的中的私有文件的记录长度用1个或2个字节来编码。

终端配置：支持SDA。

卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录中，列在AFL中，并且包含在签名数据中；
——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为 1）；
——私有文件中的借记/贷记应用数据对象是 TLV 格式，且记录标签是‘70’；
——签名静态应用数据是正确的（标签‘70’以及包含在私有文件中的记录的长度参与计算）。

子类案例：——案例 01：参加数据认证的私有文件中的记录长度用 1 字节编码（位 8＝0）；
——案例 02：参加数据认证的私有文件中的记录长度用 2 字节编码（81xx）。

测试流程：选择卡片应用，执行交易（SDA被执行）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。在接收到第一个GENERATE AC命令时，TSI的字节1，位8 =‘1’（脱机数据认证完成）。第一个 GENERATE AC命令中的 TVR字节1，位2 = ‘1’（SDA执行）。

7.14.11 MLYF015-02 交易流程中的功能组合测试：DDA 和用 1 个或 2 个字节编码的记录长度

测试目的：确保终端支持DDA，且参与DDA计算的记录长度用1个或2个字节来编码。

终端配置：——支持DDA；
——终端包含卡指定的 CA 公钥。

卡片配置：——卡的AIP指明支持DDA（AIP的 字节1，位6为1）；
——卡签名的动态应用数据是正确的。

子类案例：——案例 01：在 AFL 中列出的，参加数据认证的记录长度用 1 字节编码（位 8＝0）；
——案例 02：在 AFL 中列出的，参加数据认证的记录长度用 2 字节编码（81xx）；
——案例 03：参加数据认证的数据对象长度用 1 字节编码（位 8＝0）；
——案例 04：参加数据认证的数据对象长度用 2 字节编码（81xx）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。终端性能应该指示支持DDA。在接收到的第一个GENERATE AC命令中，TVR的字节1，位4 =‘0’（DDA成功）。在接收到的第一个GENERATE AC命令中，TVR的字节1，位3 =‘0’（未使用CDA）。在接收到的第一个GENERATE AC命令中，TVR的字节1，位7 =‘0’（未使用SDA）。在接收到的第一个GENERATE AC命令中，TSI的字节1，位8 =‘1’（脱机数据认证完成）。在接收到的第一个 GENERATE AC命令中，TVR的字节 1，位2 = ‘0’（SDA未执行）。

7.14.12 MLYF015-03 交易流程中的功能组合测试：DDA 和私有文件的记录长度用 1 或 2 字节编码

测试目的：确保终端支持DDA，且参与DDA计算的私有文件的记录长度用1或2字节来编码。
终端配置：支持DDA。
卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录中，列在AFL中，并且包含在签名数据中；
——卡的 AIP 指明支持 DDA（AIP 的 字节 1，位 6 为 1）；
——私有文件中的借记/贷记应用数据对象是 TLV 格式，且记录标签是‘70’；
——签名动态应用数据是正确的（标签‘70’以及包含在私有文件中的记录的长度参与计算）。
子类案例：——案例 01：参加数据认证的私有文件中的记录长度用 1 字节编码（位 8＝0）；
——案例 02：参加数据认证的私有文件中的记录长度用 2 字节编码(81xx)。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’(DDA成功)。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。在接收到第一个GENERATE AC命令时，TSI的字节1，位8 =‘1’（脱机数据认证完成）。第一个 GENERATE AC命令中的 TVR字节1，位2 = ‘0’（SDA未执行）。

7.14.13 MLYF015-04 交易流程中的功能组合测试：CDA 和用 1 或 2 个字节编码的记录长度

测试目的：确保终端支持CDA，且参与CDA计算的私有文件的记录长度用1或2字节来编码。
终端配置：——支持CDA；
——终端包含卡指定的CA公钥。
卡片配置：卡的AIP指明支持CDA（AIP的 字节1，位1为1）。
子类案例：——案例01：在AFL中列出的，参加数据认证的记录长度用1字节编码（位8＝0）；
——案例02：在AFL中列出的，参加数据认证的记录长度用2字节编码(81xx)；
——案例03：参加数据认证的数据对象长度用1字节编码（位8＝0）；
——案例04：参加数据认证的数据对象长度用2字节编码（81xx）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端性能应该指示支持CDA。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’(未使用DDA)。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（CDA成功）。包含在金融确认信息或是批数据捕获信息中的TSI的字节1，位8 =‘1’（脱机数据认证完成）（本通过标准仅适用于终端请求CDA的情况）。第一个GENERATE AC命令中的TVR字节1，位2 = ‘0’(SDA未执行)。

7.14.14 MLYF015-05 交易流程中的功能组合测试：CDA 和私有文件的记录长度用 1 或 2 字节编码

测试目的：确保终端支持CDA，且参与CDA计算的私有文件的记录长度用1或2字节来编码。
终端配置：支持CDA。
卡片配置：——一个借记/贷记应用数据对象包含在一个私有文件的记录中，列在AFL中，并且包含在签名数据中；
——卡的 AIP 指明支持 CDA（AIP 的 字节 1，位 6 为 1）；
——私有文件中的借记/贷记应用数据对象是 TLV 格式，且记录标签是‘70’；
——签名动态应用数据是正确的（标签‘70’以及包含在私有文件中的记录的

长度参与计算）。

子类案例：——案例 01：参加数据认证的私有文件中的记录长度用 1 字节编码（位 8 ＝0）；

——案例 02：参加数据认证的私有文件中的记录长度用 2 字节编码(81xx)。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA)。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA未使用)。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（CDA成功)。包含在金融确认信息或是批数据捕获信息中的TSI的字节1，位8 =‘1’（脱机数据认证完成)（本通过标准仅适用于终端请求CDA的情况)。第一个GENERATE AC命令中的TVR字节1，位2 = ‘0’（SDA未执行)。

7.14.15 MLYF016-00 组合测试：SDA 标签列表和 SDA 中的 AFL

测试目的：确保终端支持SDA标签列表和AFL中标记的记录参与静态数据认证。

终端配置：支持SDA。

卡片配置：——卡的AIP指明支持SDA（AIP的 字节1，位7为1）；

——SDA 签名对于每个子案例都是正确的。

子类案例：——案例 01：SDA 标签列表包含标签‘82’（AIP），且一个 AFL 标记的借记/贷记应用文件的记录，参与静态数据认证；

——案例 02：SDA 标签列表包含标签‘82’（AIP），且一个 AFL 标记的私有文件的记录，参与静态数据认证；

——案例 03：SDA 标签列表包含标签‘82’（AIP），且 AFL 标记的一个私有文件的记录和一个借记/贷记应用文件记录，参与静态数据认证；

——案例 04：SDA 标签列表包含标签‘82’（AIP），且 AFL 没有标记参与静态数据认证的记录；

——案例 05：SDA 标签列表不存在，且一个 AFL 标记的借记/贷记应用文件的记录，参与静态数据认证；

——案例 06：SDA 标签列表不存在，且一个 AFL 标记的私有文件的记录，参与静态数据认证；

——案例 07：SDA 标签列表不存在，且 AFL 标记的一个私有文件的记录和一个借记/贷记应用文件记录，参与静态数据认证。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功)。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA)。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA)。在接收到第一个GENERATE AC命令时，TSI的字节1，位8 =‘1’（脱机数据认证完成)。第一个GENERATE AC命令中的TVR字节1，位2 = ‘1’（SDA执行)。

7.14.16 MLYF016-03 组合测试：SDA 标签列表和 DDA 中的 AFL

测试目的：确保终端支持SDA标签列表，和AFL中标记的记录参与动态数据认证。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持DDA（AIP的 字节1，位6为1）；

——每个子案例的SDA签名都是正确的。

子类案例：——案例 01：SDA 标签列表包含标签‘82’（AIP），且一个 AFL 标记的借记/贷记应用文件的记录，参与动态数据认证；

——案例 02：SDA 标签列表包含标签‘82’（AIP），且一个 AFL 标记的私有文件的记录，参与动态数据认证；

——案例 03：SDA 标签列表包含标签‘82’（AIP），且 AFL 标记的一个私有

文件的记录和一个借记/贷记应用文件记录，参与动态数据认证；

——案例 04：SDA 标签列表包含标签‘82’（AIP），且 AFL 没有标记参与动态数据认证的记录；

——案例 05：SDA 标签列表不存在，且一个 AFL 标记的借记/贷记应用文件的记录，参与动态数据认证；

——案例 06：SDA 标签列表不存在，且一个 AFL 标记的私有文件的记录，参与动态数据认证；

——案例 07：SDA 标签列表不存在，且 AFL 标记的一个私有文件的记录和一个借记/贷记应用文件记录，参与动态数据认证。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。在接收到第一个GENERATE AC命令时，TSI的字节1，位8 =‘1’（脱机数据认证完成）。第一个GENERATE AC命令中的TVR字节1，位2 = ‘0’（SDA未执行）。

7.14.17 MLYF016-05 组合测试：SDA 标签列表和 CDA 中的 AFL

测试目的：确保终端支持SDA标签列表，和AFL中标记的记录参与复合动态数据认证。

终端配置：支持CDA。

卡片配置：卡的AIP指明支持CDA（AIP的 字节1，位1为1）。

子类案例：——案例01：SDA标签列表包含标签‘82’（AIP），且一个AFL标记的借记/贷记应用文件的记录，参与复合动态数据认证；

——案例 02：SDA 标签列表包含标签‘82’（AIP），且一个 AFL 标记的私有文件的记录，参与复合动态数据认证；

——案例 03：SDA 标签列表包含标签‘82’（AIP），且 AFL 标记的一个私有文件的记录和一个借记/贷记应用文件记录，参与复合动态数据认证；

——案例 04：SDA 标签列表包含标签‘82’（AIP），且 AFL 没有标记参与复合动态数据认证的记录；

——案例 05：SDA 标签列表不存在，且一个 AFL 标记的借记/贷记应用文件的记录，参与复合动态数据认证；

——案例 06：SDA 标签列表不存在，且一个 AFL 标记的私有文件的记录，参与复合动态数据认证；

——案例 07：SDA 标签列表不存在，且 AFL 标记的一个私有文件的记录和一个借记/贷记应用文件记录，参与复合动态数据认证。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。如果终端有存储拒绝交易的能力，包含在金融确认报文或是批数据获取报文中的TVR字节1，位3 =‘0’（CDA成功或未使用）。如果终端有存储拒绝交易的能力，包含在金融确认报文或是批数据获取报文中的TVR字节1，位4 =‘0’（未使用DDA）。如果终端有存储拒绝交易的能力，包含在金融确认报文或是批数据获取报文中的TVR字节1，位7 =‘0’（未使用SDA）。如果终端有存储拒绝交易的能力，包含在金融确认报文或是批数据获取报文中的TVR字节1，位2 =‘0’（SDA未执行）。

7.15 综合测试（ZHCS）

7.15.1 ZHCS011-00 交易流程中的功能组合测试：发卡行认证和脚本处理（1）

测试目的：确保终端在同一个交易中能够执行发卡行认证和发卡行脚本处理。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置从而使交易联机执行；

——卡的 AIP 指明支持发卡行认证（AIP 的 字节 1 位 3 为‘1’）。

子类案例：从发卡行返回的报文包含以下脚本：

——案例 01：一个‘71’脚本；

——案例 02：一个‘72’脚本；

——案例 03：一个‘71’脚本和一个‘72’脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘0’（最后一次GENERATE AC命令之前脚本处理成功（子案例01和03））。包含在金融确认报文或是批数据获取报文中的TVR的字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功（子案例02和03））。包含在金融确认报文或是批数据获取报文中的TSI的字节1，位3 =‘1’（脚本处理已进行）。在接收到第二个GENERATE AC命令时，TVR的字节5，位7 =‘0’（发卡行认证成功）。在接收到第二个GENERATE AC命令时，TSI的字节1，位5 =‘1’（发卡行认证已进行）。

7.15.2 ZHCS011-01 交易流程中的功能组合测试：发卡行认证和脚本处理（2）

测试目的：确保终端在同一个交易中能够执行发卡行认证和处理带有错误的发卡行脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置从而使交易联机执行；

——卡的AIP指明支持发卡行认证（AIP的 字节1，位3为‘1’）；

——授权响应报文包含一个‘71’的发卡行脚本，包含以下命令：卡片返回‘9000’给脚本命令1；卡片返回‘6983’给脚本命令2。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在接收到第二个GENERATE AC命令时，TSI的字节1，位3 =‘1’（脚本处理已进行）。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。在接收到第二个GENERATE AC命令时，TVR的字节5，位7 =‘0’（发卡行认证成功）。在接收到第二个GENERATE AC命令时，TSI的字节1，位5 =‘1’（发卡行认证已进行）。

7.15.3 ZHCS011-02 交易流程中的功能组合测试：发卡行认证和脚本处理（3）

测试目的：确保终端在同一个交易中能够执行发卡行认证和处理带有错误的发卡行脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置从而使交易联机执行；

——卡的 AIP 指明支持发卡行认证（AIP 的 字节 1，位 3 为‘1’）；

——授权响应报文包含一个‘72’的发卡行脚本，带有以下命令：卡片返回‘9000’给脚本命令 1；卡片返回‘6983’给脚本命令 2。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认报文或是批数据获取报文中的TSI的字节1，位3 =‘1’（脚本处理已进行）。包含在金融确认报文或是批数据获取报文中的TVR的字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。在接收到第二个GENERATE AC命令时，TVR的字节5，位7 =‘0’（发卡行认证成功）。在接收到第二个GENERATE AC命令时，TSI的字节1，位5 =‘1’（发卡行认证已进行）。

7.15.4 ZHCS011-03 交易流程中的功能组合测试：发卡行认证和脚本处理（4）

测试目的：确保终端在同一个交易中能够执行发卡行认证和处理带有错误的发卡行脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置从而使交易联机执行；
——卡的AIP指明支持发卡行认证（AIP的 字节1，位3为‘1’）；
——授权响应报文包含一个‘71’的发卡行脚本，带有以下命令：卡片返回‘9000’给脚本命令1；卡片返回‘6983’给脚本命令2；
——授权响应报文包含一个‘72’的发卡行脚本，带有以下命令：卡片返回‘9000’给脚本命令1；卡片返回‘6983’给脚本命令2。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认报文或是批数据获取报文中的TSI的字节1，位3 =‘1’（脚本处理已进行）。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。包含在金融确认报文或是批数据获取报文中的TVR的字节5，位5 =‘1’（最后一次GENERATE AC命令之后脚本处理失败）。在接收到第二个GENERATE AC命令时，TVR的字节5，位7 =‘0’（发卡行认证成功）。在接收到第二个GENERATE AC命令时，TSI的字节1，位5 =‘1’（发卡行认证已进行）。

7.15.5 ZHCS011-04 交易流程中的功能组合测试：发卡行认证和脚本处理（5）

测试目的：确保终端在同一个交易中能够执行发卡行认证和处理带有错误的发卡行脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置从而使交易联机执行；
——卡的AIP指明支持发卡行认证（AIP的 字节1，位3为‘1’）；
——授权响应报文包含一个‘71’的发卡行脚本，带有以下命令：卡片返回‘9000’给脚本命令1；卡片返回‘6983’给脚本命令2；
——授权响应报文包含一个‘72’的发卡行脚本，带有以下命令：卡片返回‘9000’给脚本命令1；卡片返回‘9000’给脚本命令2。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认报文或是批数据获取报文中的TSI的字节1，位3 =‘1’（脚本处理已进行）。在接收到第二个GENERATE AC命令时，TVR的字节5，位6 =‘1’（最后一次GENERATE AC命令之前脚本处理失败）。包含在金融确认报文或是批数据获取报文中的TVR的字节5，位5 =‘0’（最后一次GENERATE AC命令之后脚本处理成功）。在接收到第二个GENERATE AC命令时，TVR的字节5，位7 =‘0’（发卡行认证成功）。在接收到第二个GENERATE AC命令时，TSI的字节1，位5 =‘1’（发卡行认证已进行）。

7.15.6 ZHCS012-00 交易流程中的功能组合测试：发卡行认证和生成通知（1）

测试目的：确保如果密文信息数据中的‘请求通知’位设置为‘1’，则终端执行发卡行认证并生成通知报文给发卡行。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置以致交易联机执行；
——卡的AIP指明支持发卡行认证（AIP的 字节1，位3为‘1’）；
——卡响应第一个GENERATE AC的CID的位4被置为‘1’；
——卡响应AAC（CID=‘08’）给第二个GENERATE AC；
——交易未被捕获。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该来完成交易并且被拒绝。如果支持生成通知且数据未被捕获，则终

端应该发送一个通知。

7.15.7 ZHCS012-01 交易流程中的功能组合测试：发卡行认证和生成通知（2）

测试目的：确保如果密文信息数据中的“需要通知”位和“发卡行认证失败”位设为‘1’，则终端执行发卡行认证并生成通知给发卡行。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置从而使交易联机执行；
——卡的AIP指明支持发卡行认证（AIP的 字节1，位3为‘1’）；
——卡响应第一个GENERATE AC的CID 位1、2、4被置为‘1’；
——卡响应AAC （CID=‘0B’）给第二个GENERATE AC；
——交易未被捕获。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该处理交易，直到完成并且被拒绝。如果支持通知且支持联机数据捕获，则终端应该发送一个联机通知，如果终端支持通知且支持批数据捕获，则终端应该发送一个离线通知，如果终端不支持通知，则不应发送通知。

7.15.8 ZHCS013-00 交易流程中的功能组合测试：第一个和第二个 GENERATE AC 请求通知（1）

测试目的：——确保在第一个和第二个GENERATE AC，终端支持生成通知给发卡行；
——确保如果终端不支持通知，忽略通知请求继续完成交易。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置从而使交易联机执行；
——卡响应第一个 GENERATE AC 的 CID 位 4 被置为‘1’；
——卡响应 TC 给第二个 GENERATE AC；
——卡响应第二个 GENERATE AC 的 CID 位 4 被置为‘1’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC来完成交易。如果终端支持通知且不支持批数据捕获，则应发送一个通知。

7.15.9 ZHCS013-01 交易流程中的功能组合测试：第一个和第二个 GENERATE AC 请求通知（2）

测试目的：确保在第一个和第二个GENERATE AC期间，终端支持给发卡行的通知消息。

终端配置：支持仅联机或脱机/联机、支持通知。

卡片配置：——卡的参数被设置从而使交易联机执行；
——卡用 CID 位 4 设置为‘1’来答复第一个 GENERATE AC；
——卡答复第二个 GENERATE AC 为 AAC；
——卡用 CID 位 4 设置为‘1’来答复第二个 GENERATE AC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该来完成交易并且交易拒绝。如果支持通知且支持联机数据捕获，则终端应该发送一个联机通知，如果终端支持通知且支持批数据捕获，则终端应该发送一个离线通知，如果终端不支持通知，则不应发送通知。

7.15.10 ZHCS017-00 综合测试：以不同格式响应 GET PROCESSING OPTIONS 和 GENERATE AC 命令（1）

测试目的：确保终端在同一个交易中能够支持 GET PROCESSING OPTIONS 和 GENERATE AC 的响应模版格式为 1 和 2 的响应。

终端配置：N/A。

子类案例：——案例 01：卡以格式 1 响应 GET PROCESSING OPTIONS 命令，以格式 2 响应 GENERATE AC 命令；
——案例 02：卡以格式 2 响应 GET PROCESSING OPTIONS 命令，以格式 1 响

应 GENERATE AC 命令。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该能够通过请求产生TC或AAC，处理交易到完成。

7.15.11 ZHCS017-01 综合测试：以不同格式响应 GET PROCESSING OPTIONS 和 GENERATE AC 命令（2）

测试目的：确保终端在同一个交易中能够支持GET PROCESSING OPTIONS和GENERATE AC命令的响应模版格式为1和2的响应。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的参数被设置从而使交易联机执行；

——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）。

子类案例：——案例 01：以响应模版格式 1 响应 GET PROCESSING OPTIONS 命令，以响应模版格式 2 响应第一个 GENERATE AC 命令，以响应模版格式 1 响应第二个 GENERATE AC 命令；

——案例 02：以响应模版格式 2 响应 GET PROCESSING OPTIONS 命令，以响应模版格式 1 响应第一个 GENERATE AC 命令，以响应模版格式 2 响应第二个 GENERATE AC 命令；

——案例 03：以响应模版格式 1 响应 GET PROCESSING OPTIONS 命令，以响应模版格式 1 响应第一个 GENERATE AC 命令，以响应模版格式 2 响应第二个 GENERATE AC 命令。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该接受卡，通过请求TC或AAC来完成交易。

7.15.12 ZHCS018-00 综合测试：不同响应模版格式的 GET PROCESSING OPTIONS 和 GENERATE AC，CDA（1）

测试目的：确保终端接受响应模版格式1和2响应GET PROCESSING OPTIONS命令，响应模版格式2响应请求CDA的GENERATE AC命令。

终端配置：支持CDA。

卡片配置：——卡的AIP指明支持CDA（AIP的 字节1，位1为‘1’）；

——联机、拒绝和默认IAC以及联机、拒绝和默认TAC被设置从而使终端在第一次GAC和第二次GAC都请求TC；

——如果终端联机处理，应使其不能联机。

子类案例：——案例01：以响应模版格式1响应GET PROCESSING OPTIONS命令，以响应模版格式2响应GENERATE AC命令；

——案例 02：以响应模版格式 2 响应 GET PROCESSING OPTIONS 命令，以响应模版格式 2 响应 GENERATE AC 命令。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求TC来完成交易。包含在金融确认报文或批数据获取报文中的TVR字节1，位3 =‘0’（CDA成功或未使用）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。

7.15.13 ZHCS018-01 综合测试：不同响应模版格式的 GET PROCESSING OPTIONS 和 GENERATE AC，CDA（2）

测试目的：确保终端接受响应模版格式1和2响应GET PROCESSING OPTIONS命令，响应模版格式2响应请求CDA的GENERATE AC命令。

终端配置：支持CDA。

卡片配置：——卡的参数被设置从而使交易联机执行；

——卡的 AIP 指明支持 CDA（AIP 的 字节 1，位 1 为‘1’）；

——联机、拒绝和默认IAC以及联机、拒绝和默认TAC被设置从而使终端在第

一次GAC请求ARQC,第二次GAC请求TC；

——如果终端联机处理，应使其不能联机。

子类案例：——案例01：以响应模版格式1响应GET PROCESSING OPTIONS命令，以响应模版格式2响应第一个和第二个GENERATE AC命令；

——案例 02：以响应模版格式 2 响应 GET PROCESSING OPTIONS 命令，以响应模版格式 2 响应第一个和第二个 GENERATE AC 命令。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求TC或者AAC（如果终端支持当不能联机时，跳过缺省行为码的处理）来完成交易。包含在金融确认报文或批数据获取报文中的TVR字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。

7.15.14 ZHCS019-00 综合测试：不同响应模版格式的 GET PROCESSING OPTIONS、INTERNAL AUTHENTICATE 和 GENERATE AC（1）

测试目的：确保终端在同一个交易中接受对于GET PROCESSING OPTIONS、INTERNAL AUTHENTICATE和GENERATE AC命令的响应模版格式为1和2的响应。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持DDA（AIP的 字节1，位6为‘1’）；

——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）。

子类案例：——案例 01：给 GET PROCESSING OPTIONS 的响应为响应模版格式 1，给 INTERNAL AUTHENTICATE 的响应为响应模版格式 2，给 GENERATE AC 的响应为响应模版格式 1；

——案例 02：给 GET PROCESSING OPTIONS 的响应为响应模版格式 2，给 INTERNALAUTHENTICATE 的响应为响应模版格式 1，给 GENERATE AC 的响应为响应模版格式 2；

——案例 03：给 GET PROCESSING OPTIONS 的响应为响应模版格式 1，给 INTERNAL AUTHENTICATE 的响应为响应模版格式 1，给 GENERATE AC 的响应为响应模版格式 2。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.15 ZHCS019-01 综合测试：不同响应模版格式的 GET PROCESSING OPTIONS、INTERNAL AUTHENTICATE 和 GENERATE AC（2）

测试目的：确保终端在同一个交易中接受对于GET PROCESSING OPTIONS、INTERNALAUTHENTICATE和GENERATE AC命令的响应模版格式为1和2的响应。

终端配置：——支持DDA；

——支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持DDA（AIP的 字节1，位6为‘1’）；

——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）；

——卡的参数被设置以至交易联机进行。

子类案例：——案例 01：给 GET PROCESSING OPTIONS 的响应为格式 1，给 INTERNAL AUTHENTICATE 的响应为格式 2，给第一个 GENERATE AC 的响应为格式 1，给第二个 GENERATE AC 的响应为格式 2；

——案例 02：给 GET PROCESSING OPTIONS 的响应为格式 2，给 INTERNAL AUTHENTICATE 的响应为格式 1，给第一个 GENERATE AC 的响应为格式 2，给第二个 GENERATE AC 的响应为格式 1；

——案例 03：给 GET PROCESSING OPTIONS 的响应为格式 1，给 INTERNAL AUTHENTICATE 的响应为格式 1，给第一个 GENERATE AC 的响应为格式 2，给第二个 GENERATE AC 的响应为格式 2。

测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.16 ZHCS020-00 交易流程中的功能组合测试：PSE，空的 PDOL，SDA，明文 PIN，发卡行认证，GENERATE AC 响应模版格式 1，脚本

测试目的：确保终端在同一个交易中能够支持以下卡的功能：PSE，带有空PDOL的GET PROCESSING OPTIONS命令，SDA，明文PIN，发卡行认证， GENERATE AC格式1，脚本。
终端配置：支持仅联机或脱机/联机性能。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的 字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的 字节 1，位 3 为‘1’）；
——卡支持 PSE；
——ADF 的 FCI 响应包含一个空的 PDOL；
——CVM 要求“脱机明文 PIN 验证，如果终端支持”（0103），下面是“纸张签名如果终端支持”（1E03），下面是“联机 PIN，如果终端支持”（0203），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回的响应模版格式为 1。
子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答一个‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答一个‘71’的脚本。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.17 ZHCS020-01 交易流程中的功能组合测试：PSE，空的 PDOL，SDA，明文 PIN，发卡行认证，GENERATE AC 格式 1

测试目的：确保终端在同一个交易中能够支持以下卡的功能：PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，明文PIN，发卡行认证，GENERATE AC格式1。
终端配置：支持仅脱机。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的 字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的 字节 1，位 3 为‘1’）；
——卡支持 PSE；
——ADF 的 FCI 响应包含一个空 PDOL；
——CVM 要求“脱机明文 PIN 验证，如果终端支持该 CVM”（0103），接着是“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 1；
——卡的参数被设置从而使交易脱机执行。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.18 ZHCS021-00 交易流程中的功能组合测试：无 PSE，PDOL 空，SDA，明文 PIN，发卡行认证，GENERATE AC 格式 1，脚本

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，明文PIN，发卡行认证， GENERATE AC格式1，脚本。
终端配置：支持仅联机或脱机/联机性能。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的 字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的 字节 1，位 3 为‘1’）；

——卡不支持 PSE；
——ADF 的 FCI 响应包含一个空 PDOL；
——CVM 要求“脱机明文 PIN 验证，如果终端支持”（0103），接着是“纸张签名，如果终端支持”（1E03），接着是“联机 PIN，如果终端支持该 CVM”（0203），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 1。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.19 ZHCS021-01 交易流程中的功能组合测试：无 PSE，空的 PDOL，SDA，明文 PIN，发卡行认证，GENERATE AC 格式 1

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，明文PIN，发卡行认证， GENERATE AC格式1。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的 字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的 字节 1，位 3 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“脱机明文 PIN 验证，如果终端支持该 CVM”（0103），接着是“纸张签名，如果终端支持该 CVM”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回响应为格式 1；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.20 ZHCS022-00 交易流程中的功能组合测试：PSE，空的 PDOL，SDA，纸张签名，发卡行认证，GENERATE AC 格式 1，脚本

测试目的：确保终端在同一个交易中能够支持以下卡的功能：PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，纸张签名，发卡行认证， GENERATE AC格式1，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的 字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的 字节 1，位 3 为‘1’）；
——卡支持 PSE；
——卡 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“纸张签名，如果终端支持该 CVM”（1E03），接着是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 1。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.21 ZHCS022-01 交易流程中的功能组合测试：PSE，空的 PDOL，SDA，纸张签名，发卡行认证，GENERATE AC 格式 1

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，纸张签名，发卡行认证， GENERATE AC格式1。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的 字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的字节 1，位 3 为‘1’）；
——卡支持 PSE；
——卡的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 1；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.22 ZHCS023-00 交易流程中的功能组合测试：无 PSE，空的 PDOL，SDA，纸张签名，发卡行认证，GENERATE AC 格式 1，脚本（1）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，纸张签名，发卡行认证， GENERATE AC格式1，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的字节 1，位 3 为‘1’）；
——卡不支持 PSE；
——卡的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“纸张签名，如果终端支持该 CVM”（1E03），接着是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 1。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.23 ZHCS023-01 交易流程中的功能组合测试：无 PSE，空的 PDOL，SDA，纸张签名，发卡行认证，GENERATE AC 格式 1，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，纸张签名，发卡行认证， GENERATE AC格式1，脚本。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的字节 1，位 3 为‘1’）；
——卡不支持 PSE；
——卡的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“纸张签名，如果终端支持该 CVM”（1E03），接着是“无需 CVM，

总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 1；
——卡的参数被设置从而使交易脱机执行。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.24 ZHCS024-00 交易流程中的功能组合测试：无 PSE，空的 PDOL，SDA，纸张签名，无发卡行认证，GENERATE AC 格式 1，脚本（1）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，纸张签名，无发卡行认证， GENERATE AC格式1，脚本。
终端配置：支持仅联机或脱机/联机。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“纸张签名，如果终端支持”（1E03），接着是“无需 CVM”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 1，IAD 不存在。
子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答 71 的脚本。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.25 ZHCS024-01 交易流程中的功能组合测试：无 PSE，空的 PDOL，SDA，纸张签名，无发卡行认证，GENERATE AC 格式 1，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，纸张签名，无发卡行认证， GENERATE AC格式1，脚本。
终端配置：支持仅脱机。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“纸张签名，如果终端支持”（1E03），接着是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 1，IAD 不存在；
——卡的参数被设置从而使交易脱机执行。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.26 ZHCS025-00 交易流程中的功能组合测试：PSE，空的 PDOL，SDA，纸张签名，无发卡行认证，GENERATE AC 格式 1，脚本（1）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，纸张签名，无发卡行认证， GENERATE AC格式1，脚本。
终端配置：支持仅联机或脱机/联机。
卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡支持 PSE；

——卡的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“纸张签名，如果终端支持”（1E03），接着是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 1，IAD 不存在。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.27 ZHCS025-01 交易流程中的功能组合测试：PSE，空的 PDOL，SDA，纸张签名，无发卡行认证，GENERATE AC 格式 1，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，纸张签名，无发卡行认证， GENERATE AC格式1，脚本。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡支持 PSE；
——卡的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“纸张签名，如果终端支持”（1E03），接着是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 1，IAD 不存在；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.28 ZHCS026-00 交易流程中的功能组合测试：无 PSE，空的 PDOL，SDA，明文 PIN，无发卡行认证，GENERATE AC 格式 2，脚本（1）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，明文PIN，无发卡行认证（IAD存在）， GENERATE AC格式2，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“脱机明文 PIN 验证，如果终端支持”（0103），接着是“纸张签名，如果终端支持该 CVM”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 2，IAD 存在。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.29 ZHCS026-01 交易流程中的功能组合测试：无 PSE，空的 PDOL，SDA，明文 PIN，无发卡行认证，GENERATE AC 格式 2，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS，SDA，明文PIN，无发卡行认证（IAD存在）， GENERATE

AC格式2，脚本。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“脱机明文 PIN 验证，如果终端支持”（0103），接着是“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 2，IAD 存在；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.30 ZHCS027-00 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 2，SDA，明文 PIN，无发卡行认证，GENERATE AC 格式 2，脚本（1）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE， GET PROCESSING OPTIONS格式2，SDA，明文PIN，无发卡行认证（IAD存在），GENERATE AC格式2，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个有效的 PDOL；
——卡对 GET PROCESSING OPTIONS 返回响应模版格式 2；
——CVM 要求“脱机明文 PIN 验证，如果终端支持该 CVM”（0103），接着是“纸张签名，如果终端支持该 CVM”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 2，IAD 存在。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.31 ZHCS027-01 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 2，SDA，明文 PIN，无发卡行认证，GENERATE AC 格式 2，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，GET PROCESSING OPTIONS格式2，SDA，明文PIN，无发卡行认证（IAD存在），GENERATE AC格式2，脚本。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个有效的 PDOL；
——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 2；
——CVM 要求“脱机明文 PIN 验证，如果终端支持”（0103），接着是“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 2，IAD 存在；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.32 ZHCS028-00 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 1，SDA，纸张签名，无发卡行认证，GENERATE AC 格式 1，脚本（1）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，GET PROCESSING OPTIONS格式1，SDA，纸张签名，无发卡行认证（IAD存在），GENERATE AC格式1，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个有效的 PDOL；
——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 1；
——CVM 要求“纸张签名，如果终端支持该 CVM”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 1，IAD 存在。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.33 ZHCS028-01 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 1，SDA，纸张签名，无发卡行认证，GENERATE AC 格式 1，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，GET PROCESSING OPTIONS格式1，SDA，纸张签名，无发卡行认证（IAD存在），GENERATE AC格式1，脚本。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个有效的 PDOL；
——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 1；
——CVM 要求“纸张签名，如果终端支持该 CVM”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回响应模版格式 1，IAD 存在；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.34 ZHCS029-00 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 1，TRM，SDA，DDA，纸张签名，无发卡行认证，GENERATE AC 格式 1，脚本

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，GET PROCESSING OPTIONS格式1,TRM,SDA,DDA,纸张签名,无发卡行认证(IAD存在)，GENERATE AC格式1，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持终端风险管理TRM（AIP的字节1，位4为‘1’）；
——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；

——卡片返回的 ADF FCI 响应包含一个有效的 PDOL；
——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 1；
——CVM 要求“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 1，IAD 存在。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.35 ZHCS029-01 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 1，TRM，SDA，DDA，纸张签名，无发卡行认证，GENERATE AC 格式 1

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE， GET PROCESSING OPTIONS格式1,TRM,SDA,DDA,纸张签名,无发卡行认证(IAD存在)，GENERATE AC格式1。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持TRM（AIP的字节1，位4为‘1’）；
——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个有效的 PDOL；
——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 1；
——CVM 要求“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回响应模版格式 1，IAD 存在；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.36 ZHCS030-00 交易流程中的功能组合测试：无 PSE，PDOL 空，SDA，DDA，明文 PIN，发卡行认证，GENERATE AC 格式 1，脚本（1）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE， 带有空PDOL的GET PROCESSING OPTIONS，SDA，DDA，明文PIN，发卡行认证， GENERATE AC格式1，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持发卡行认证（AIP的字节1，位3为‘1’）；
——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“脱机明文 PIN 验证，如果终端支持该 CVM”（0103），接着是“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回响应模版格式 1。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.37 ZHCS030-01 交易流程中的功能组合测试：无 PSE，PDOL 空，SDA，DDA，明文 PIN，发卡行认证，GENERATE AC 格式 1，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，带有空PDOL的GET PROCESSING OPTIONS Option，SDA，DDA，明文PIN，发卡行认证， GENERATE AC格式1，脚本。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持发卡行认证（AIP的字节1，位3为‘1’）；
——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡片返回的 ADF FCI 响应包含一个空 PDOL；
——CVM 要求“脱机明文 PIN 验证，如果终端支持该 CVM”（0103），接着是“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 1；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.38 ZHCS031-00 交易流程中的功能组合测试：PSE，GET PROCESSING OPTIONS Option 格式 2，SDA，DDA，密文 PIN，发卡行认证，GENERATE AC 格式 2，脚本

测试目的：确保终端在同一个交易中能够支持以下卡的功能： PSE，GET PROCESSING OPTIONS格式2，SDA，DDA，密文PIN，发卡行认证，GENERATE AC格式2，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持发卡行认证（AIP的字节1，位3为‘1’）；
——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡支持 PSE；
——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 2；
——CVM 要求“离线密文 PIN 验证，如果终端支持”（0403），下面是“纸质签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 2。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.39 ZHCS031-01 交易流程中的功能组合测试：PSE，GET PROCESSING OPTIONS Option 格式 2，SDA，DDA，密文 PIN，发卡行认证，GENERATE AC 格式 2，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：PSE，GET PROCESSING OPTIONS格式2，SDA，DDA，密文PIN，发卡行认证，GENERATE AC格式2，脚本。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持发卡行认证（AIP的字节1，位3为‘1’）；
——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；

——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡支持 PSE；
——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 2；
——CVM 要求“离线密文 PIN 验证，如果终端支持”（0403），下面是“纸质签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 2。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.40 ZHCS032-00 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 2，TRM，SDA，DDA，CDA，密文 PIN，发卡行认证，GENERATE AC 格式 2，脚本

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，GET PROCESSING OPTIONS格式2，TRM，SDA，DDA，CDA，密文PIN，发卡行认证， GENERATE AC格式2，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持终端风险管理TRM（AIP的字节1，位4为‘1’）；
——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的字节 1，位 3 为‘1’）；
——卡不支持 PSE；
——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 2；
——CVM 要求“离线密文 PIN 验证，如果终端支持”（0403），下面是“纸质签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 2。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答‘72’的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.41 ZHCS032-01 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 2，TRM，SDA，DDA，CDA，密文 PIN，发卡行认证，GENERATE AC 格式 2，脚本

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE，GET PROCESSING OPTIONS格式2，TRM，SDA，DDA，CDA，密文PIN，发卡行认证， GENERATE AC格式2，脚本。

终端配置：支持仅联机或脱机/联机。

卡片配置：——卡的AIP指明支持终端风险管理TRM（AIP的字节1，位4为‘1’）；
——卡的 AIP 指明支持持卡人认证（AIP 的字节 1，位 5 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——卡的 AIP 指明支持发卡行认证（AIP 的字节 1，位 3 为‘1’）；
——卡不支持 PSE；

——卡对 GET PROCESSING OPTIONS 命令返回响应模版格式 2；
——CVM 要求“离线密文 PIN 验证，如果终端支持”（0403），下面是“纸质签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回为响应模版格式 2；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.42 ZHCS033-00 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS Option 格式 2，SDA，DDA，CDA，纸张签名，无发卡行认证，GENERATE AC 格式 2，脚本（1）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE， GET PROCESSING OPTIONS为格式2，SDA，DDA，CDA，纸张签名，无发卡行认证， GENERATE AC格式2，脚本。

终端配置：支持仅联机或支持脱机/联机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡对 GET PROCESSING OPTIONS 返回响应模版格式 2；
——CVM 要求“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 2。

子类案例：——案例 01：卡的参数被设置从而使交易联机执行，卡应答 72 的脚本；
——案例 02：卡的参数被设置从而使交易脱机执行；
——案例 03：卡的参数被设置从而使交易联机执行，卡应答‘71’的脚本。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.43 ZHCS033-01 交易流程中的功能组合测试：无 PSE，GET PROCESSING OPTIONS 格式 2，SDA，DDA，CDA，纸张签名，无发卡行认证，GENERATE AC 格式 2，脚本（2）

测试目的：确保终端在同一个交易中能够支持以下卡的功能：无PSE， GET PROCESSING OPTIONS为格式2，SDA，DDA，CDA，纸张签名，无发卡行认证，GENERATE AC格式2，脚本。

终端配置：支持仅脱机。

卡片配置：——卡的AIP指明支持持卡人认证（AIP的字节1，位5为‘1’）；
——卡的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡的 AIP 指明支持 SDA（AIP 的字节 1，位 7 为‘1’）；
——卡不支持 PSE；
——卡对 GET PROCESSING OPTIONS 返回响应模版格式 2；
——CVM 要求“纸张签名，如果终端支持”（1E03），下面是“无需 CVM，总是”（1F00）；
——卡对 GENERATE AC 命令返回命令响应模版格式 2；
——卡的参数被设置从而使交易脱机执行。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.44 ZHCS034-00 交易流程中的功能组合测试：自定义数据和借记/贷记应用数据

测试目的：确保在以下数据配置卡上，终端能够正确执行交易。
终端配置：N/A。
卡片配置：——卡的AIP ＝‘7D00’；
——卡的语言优先选择 ＝‘6A 61 65 6E’；
——卡的应用版本号 ＝‘0200’；
——卡的 AFL 长度为 20 字节；
——卡的 CDOL1 和 CDOL2 的长度为 128 字节；
——卡的 CVM 列表 ＝‘-00 00 00 00 00 00 00 00 41 03 1E 03 02 03 1F 03’；
——卡中的一个记录包含自定义数据标签为‘9F54’；
——卡中的一个记录包含自定义数据标签为‘DF4F’；
——卡中的一个记录包含自定义数据标签为‘9F55’。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。

7.15.45 ZHCS035-00 交易流程中的功能组合测试：SDA、密钥余数不存在、自定义数据和借记/贷记应用数据

测试目的：确保在以下数据配置的卡上：SDA、密钥余数不存在、自定义数据和借记/贷记应用数据，终端能够正确执行交易。
终端配置：支持SDA。
卡片配置：——CA公钥的长度为1984位；
——卡的AIP ＝‘5C00’；
——卡的语言优先选择 ＝‘6A 61 65 6E’；
——卡的应用版本号 ＝‘0200’；
——卡的 AFL 长度为 20 字节；
——卡的 CDOL1 和 CDOL2 的长度为 128 字节；
——卡的 CVM 列表 ＝ ‘-00 00 00 00 00 00 00 00 41 03 1E 03 02 03 1F 03’；
——卡中的一个记录包含自定义数据标签为‘9F54’；
——卡中的一个记录包含自定义数据标签为‘DF4F’；
——卡中的一个记录包含自定义数据标签为‘9F55’；
——发卡行公钥的长度为 1744 位；
——卡中不存在发卡行公钥余数。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。在收到的第一个GENERATE AC命令中，TVR的字节1，位6 =‘1’（IC卡数据缺失）。

7.15.46 ZHCS036-00 交易流程中的功能组合测试：DDA、密钥余数不存在、自定义数据和借记/贷记应用数据

测试目的：确保在以下数据配置卡上：DDA、密钥余数不存在、自定义数据和借记/贷记应用数据，终端能够正确执行交易。
终端配置：支持DDA。
卡片配置：——CA公钥的长度为1984位；
——卡的AIP ＝‘7C00’；
——卡的语言优先选择 ＝‘6A 61 65 6E’；
——卡的应用版本号 ＝‘0200’；
——卡的 AFL 长度为 20 字节；
——卡的 CDOL1 和 CDOL2 的长度为 128 字节；
——卡的 CVM 列表 ＝ ‘-00 00 00 00 00 00 00 00 41 03 1E 03 02 03 1F 03’；
——卡中的一个记录包含自定义数据标签为‘9F54’；

——卡中的一个记录包含自定义数据标签为‘DF4F’；
——卡中的一个记录包含自定义数据标签为‘9F55’；
——发卡行公钥的长度为 1744 位；
——IC 卡公钥的长度为 1504 位。

子类案例：——案例 01：卡中不存在发卡行公钥余数；
——案例 02：卡中不存在 IC 卡公钥余数。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在收到的第一个GENERATE AC命令中，TVR的字节1，位6 =‘1’（IC卡数据缺失）。

7.15.47 ZHCS037-00 交易流程中的功能组合测试：CDA、密钥余数不存在、自定义数据和借记/贷记应用数据

测试目的：确保在以下数据配置卡上：CDA、密钥余数不存在、自定义数据和借记/贷记应用数据，终端能够正确执行交易。

终端配置：——支持CDA；
——支持仅脱机或脱机/联机。

卡片配置：——CA公钥的长度为1984位；
——卡的AIP ＝ ‘7D00’；
——卡的语言优先选择 ＝ ‘6A 61 65 6E’；
——卡的应用版本号 ＝‘0200’；
——卡的 AFL 长度为 20 字节；
——卡的 CDOL1 和 CDOL2 的长度为 128 字节；
——卡的 CVM 列表 ＝ ‘-00 00 00 00 00 00 00 00 41 03 1E 03 02 03 1F 03’；
——卡中的一个记录包含自定义数据标签为‘9F54’；
——卡中的一个记录包含自定义数据标签为‘DF4F’；
——卡中的一个记录包含自定义数据标签为‘9F55’；
——发卡行公钥的长度为 1744 位；
——IC 卡公钥的长度为 1504 位；
——联机、拒绝和默认 IAC 以及联机、拒绝和默认 TAC 被设置从而使终端——在第一次 GAC 请求 TC；
——如果交易需要联机处理，终端无法联机。

子类案例：——案例 01：卡中不存在发卡行公钥余数；
——案例 02：卡中不存在 IC 卡公钥余数。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在收到的第一个GENERATE AC命令中或包含在金融确认报文或批数据获取报文中，TVR的字节1，位6 =‘1’（IC卡数据缺失）。

7.15.48 ZHCS038-00 交易流程中的功能组合测试：LCOL＝00、UCOL＝FF 自定义数据和借记/贷记应用数据

测试目的：确保在以下数据配置卡上，终端能够正确执行交易。

终端配置：支持频度检查。

卡片配置：——卡的AIP ＝ ‘7D00’；
——卡的语言优先选择 ＝ ‘6A 61 65 6E’；
——卡的应用版本号 ＝ ‘0200’；
——卡的 AFL 长度为 20 字节；
——卡的 CDOL1 和 CDOL2 的长度为 131 字节（1 个字节标签，2 个字节长度，128 字节数值）；
——卡的 CVM 列表 ＝ ‘-00 00 00 00 00 00 00 00 41 03 1E 03 02 03 1F

03’；
——卡中的一个记录包含自定义数据标签为‘9F54’；
——卡中的一个记录包含自定义数据标签为‘DF4F’；
——卡中的一个记录包含自定义数据标签为‘9F55’；
——LCOL＝00；
——UCOL＝FF；
——ATC 和 LOATC 由 GET DATA 取回；
——ATC – LOATC ＝ UCOL。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。在接收到的第一个GENERATE AC命令中，TVR的字节4，位6 =‘0’（未超过连续脱机交易上限）。在接收到的第一个GENERATE AC命令中，TVR的字节4，位7 =‘1’（超过连续脱机交易下限）。

7.15.49 ZHCS038-01 交易流程中的功能组合测试：LCOL＝00、UCOL＝FF 自定义数据和借记/贷记应用数据

测试目的：确保在以下数据配置卡上，终端能够正确执行交易。

终端配置：支持频度检查。

卡片配置：——卡的AIP ＝ ‘7D00’；
——卡的语言优先选择 ＝ ‘6A 61 65 6E’；
——卡的应用版本号 ＝ ‘0200’；
——卡的发卡行标识符 ＝ ‘35 4F FF FF’；
——卡的 AFL 长度为 20 字节；
——卡的 CDOL1 和 CDOL2 的长度为 131 字节（1 个字节标签，2 个字节长度，128 字节数值）；
——卡的 CVM 列表 ＝ ‘-00 00 00 00 00 00 00 00 41 03 1E 03 02 03 1F 03’；
——卡中的一个记录包含自定义数据标签为‘9F54’；
——卡中的一个记录包含自定义数据标签为‘DF4F’；
——卡中的一个记录包含自定义数据标签为‘9F55’；
——LCOL ＝ 00；
——UCOL ＝ FF；
——ATC 和 LOATC 由 GET DATA 取回。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节4，位6 =‘0’（未超过连续脱机交易上限）。第一个GENERATE AC命令中的TVR字节4，位7 =‘1’（超过连续脱机交易下限）。

7.15.50 ZHCS039-00 IC 卡仅支持 DDA

测试目的：确保终端接受下面卡片配置中的卡片，正确执行交易。

终端配置：支持DDA。

卡片配置：——卡的AIP为‘3C 00’；
——卡的 AFL 指明没有记录参与静态数据认证（即，每个入口的第 4 字节为‘00’）；
——卡中无已签名的静态应用数据（标签‘93’）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位6 =‘0’（IC卡数据未缺失）。第一个GENERATE AC命令中的TVR字节1，位8 =‘0’（脱机数据认证已进行）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.15.51 ZHCS040-00 符合 CPA 规范的卡片

测试目的：确保终端支持CPA卡片应用。
终端配置：N/A。
卡片配置：——卡片返回的ADF FCI响应包含一个有效的长度为128个字节的PDOL；
——CDOL1 包含总共 65 字节的 CPA 规范（2005 十二月 版本 1-0）表 155 中列出来的所有数据以及其他相关的数据；
——CDOL2 包含总共 63 字节的 CPA 规范（2005 十二月 版本 1-0）表 176 中列出来的所有数据以及其他相关的数据；
——卡对第一次和第二次 GENERATE AC 命令返回命令响应模版格式 2，发卡行认证数据长度为 32 个字节；
——第一次 GENERATE AC 返回 ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该按照PDOL正确地返回GET PROCESSING OPTIONS命令，标签83的长度字节为两个字节。终端应该按照CDOL1和CDOL2正确地返回GENERATE AC命令。

7.15.52 ZHCS040-01 符合 CPA 规范的卡片（2）

测试目的：确保终端支持CPA卡片应用。
终端配置：N/A。
卡片配置：——卡的 AIP 指明支持 CDA（AIP 的字节 1，位 1 为‘1’）；
——卡的 AIP 指明支持 DDA（AIP 的字节 1，位 6 为‘1’）；
——卡片返回的ADF FCI响应包含：
——6F 81 F0（FCI模板包含240字节数据，长度字节两个字节）；
——84 10<16个字节的DF名>；
——A5 81 DB（FCI属性模板，长度字节两个字节）；
——9F 38 81 D7（215个字节的有效PDOL）。
——CDOL1 包含总共 65 字节的 CPA 规范（2005 十二月 版本 1-0）表 155 中列出来的所有数据以及其他相关的数据；
——CDOL2 包含总共 63 字节的 CPA 规范（2005 十二月 版本 1-0）表 176 中列出来的所有数据以及其他相关的数据；
——卡对第一次和第二次 GENERATE AC 命令返回命令响应模版格式 2，发卡行认证数据长度为 32 个字节；
——第一次 GENERATE AC 返回 ARQC。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端应该按照PDOL正确地返回GET PROCESSING OPTIONS命令。终端应该按照CDOL1和CDOL2正确地返回GENERATE AC命令。

7.16 补充测试（BCCS）

7.16.1 BCCS001-00 持卡人证件出示验证，身份证（1）

测试目的：确保如果终端支持持卡人证件出示验证，当条件满足时，终端执行这种持卡人验认证方法。
终端配置：支持持卡人证件出示验证。
卡片配置：——卡中的CVM 列表是是‘20 03’；
——持卡人证件类型是身份证。
子类案例：——案例 01：持卡人证件检查验证通过；
——案例 02：持卡人证件检查验证失败。
测试流程：选择卡片应用，执行交易。

通过标准：终端应提示操作员核对持卡人证件，并正确显示持卡人证件类型和证件号。第一个 GENERATE AC 命令中的 TSI 字节 1，位 7 =‘1’（持卡人验证已执行认证已进行）。案例 01：持卡人认证验证结果为 200302。第一个 GENERATE AC 命令中的 TVR 字节 3，位 8 =‘0’（持卡人认证验证成功）。案例 02：持卡人认证验证结果为 200301。第一个 GENERATE AC 命令中的 TVR 字节 3，位 8 =‘1’（持卡人验证持卡人认证失败）。

7.16.2 BCCS002-00 持卡人证件出示验证，PIN 验认证失败，执行下一个

测试目的：确保如果终端支持持卡人证件出示验证，当条件满足时，终端执行这种持卡人认证方法。

终端配置：支持持卡人证件出示验证。

卡片配置：——卡中的CVM 列表是 ‘41 03 20 03’；
——持卡人 3 次输入密码出错；
——持卡人证件类型是身份证；
——持卡人证件检查验证通过。

测试流程：选择卡片应用，执行交易。

通过标准：终端应在输入 3 次密码不正确后，执行下一种认证持卡人验证方法，即出示持卡人证件，证件验证。终端应提示操作员核对持卡人证件，并正确显示持卡人证件类型和证件号。持卡人认证结果为 200302。第一个 GENERATE AC 命令中的 TVR 字节 3，位 8 =‘0’（持卡人认证验证成功）。第一个 GENERATE AC 命令中的 TSI 字节 1，位 7 =‘1’（持卡人认证已进行验证已执行）。

7.16.3 BCCS003-00 持卡人证件出示，护照

测试目的：确保如果终端支持持卡人证件出示验证，当条件满足时，终端执行这种持卡人验认证方法。

终端配置：支持持卡人证件验证出示。

卡片配置：——卡中的CVM 列表是‘20 03 ’；
——持卡人证件类型是护照；
——持卡人证件验证检查通过。

测试流程：选择卡片应用，执行交易。

通过标准：终端应提示操作员核对持卡人证件，并正确显示持卡人证件类型和证件号。持卡人认证结果为 200302。第一个 GENERATE AC 命令中的 TVR 字节 3，位 8 =‘0’（持卡人验证成功）。第一个 GENERATE AC 命令中的 TSI 字节 1，位 7 =‘1’（持卡人验证已执行）TVR 字节 3，位 8 =‘0’（持卡人认证成功）。TSI 字节 1，位 7 =‘1’（持卡人认证已进行）。

7.16.4 BCCS004-00 持卡人证件出示：军官证

测试目的：确保如果终端支持持卡人证件验证出示，当条件满足时，终端执行这种持卡人验证认证方法。

终端配置：支持持卡人证件验证出示。

卡片配置：——卡中的CVM 列表是‘20 03’；
——持卡人证件类型是军官证；
——持卡人证件验证检查通过。

测试流程：选择卡片应用，执行交易。

通过标准：终端应提示操作员核对持卡人证件，并正确显示持卡人证件类型和证件号。持卡人认证结果为 200302。第一个 GENERATE AC 命令中的 TVR 字节 3，位 8 =‘0’（持卡人验证成功）。第一个 GENERATE AC 命令中的 TSI 字节 1，位 7 =‘1’（持卡人验证已执行）。TVR 字节 3，位 8 =‘0’（持卡人认证成功）。TSI 字节 1，位 7 =‘1’（持卡人认证已进行）。

7.16.5 BCCS005-00 读交易日志

测试目的：确保如果终端支持读取交易日志，终端应能正确读取和显示交易日志。
终端配置：支持读取交易日志。
卡片配置：ADF的FCI中包括交易日志的入口。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该发 GET DATA 命令获取日志格式。终端应该根据日志入口读日志文件。终端应该正确显示交易日志。

7.16.6 BCCS006-00 读交易日志：应用锁定

测试目的：确保如果终端支持读取交易日志，终端应能正确读取和显示交易日志，即使是锁定的应用。
终端配置：支持读取交易日志。
卡片配置：——应用已被锁定；
——ADF 的 FCI 中包括交易日志的入口。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该发 GET DATA 命令获取日志格式。终端应该根据日志入口读日志文件。终端应该正确显示交易日志。

7.16.7 BCCS007-00 终端性能：持卡人证件验证位的置位

测试目的：确保终端性能是依照它的实际性能进行编码的，尤其是持卡人证件验证位。
终端配置：N/A。
卡片配置：CDOL1请求终端性能。
测试流程：选择卡片应用，执行交易。
通过标准：终端性能（tag9F33）应该依照终端支持的性能进行编码。Byte2bit1=1，当终端支持持卡人证件验证时；Byte2bit1=0-当终端不支持持卡人证件验证时。

7.16.8 BCCS008-00 密文传输：从外置密码键盘到终端

测试目的：确保外置密码键盘到终端间的数据以密文形式传输。
终端配置：支持外置密码键盘、支持脱机明文PIN。
卡片配置：——执行脱机明文PIN的持卡人认证方法；
——监控密码键盘传给终端的数据。
测试流程：选择卡片应用，执行交易。
通过标准：从密码键盘到终端间传输的 PIN 值应以密文形式传输。

7.16.9 BCCS009-00 持卡人姓名扩展

测试目的：确保当读记录的数据中有持卡人姓名扩展数据元时，终端能完成交易。
终端配置：N/A。
子类案例：——案例01：卡在读记录中返回数据对象持卡人姓名（tag5F20，长度0B）和持卡人姓名扩展（tag9F0B，长度04）；
——案例02：卡在读记录中返回数据对象持卡人姓名（tag5F20，长度1A）和持卡人姓名扩展（tag9F0B，长度04）；
——案例03：卡在读记录中返回数据对象持卡人姓名扩展（tag9F0B，长度1E）；
——案例04：卡在读记录中返回数据对象持卡人姓名扩展（tag9F0B，长度09）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应通过请求一个 TC 或 AAC 来完成交易。

7.16.10 BCCS010-00 逐条读取圈存明细

测试目的：确保如果终端支持逐条读取圈存明细，终端应能正确逐条读取和显示圈存明细。
终端配置：支持圈存明细（逐条读取）。
卡片配置：——取圈存日志格式命令和读日志命令卡响应9000；
——应用选择成功。
测试流程：选择应用，取圈存日志格式，读取圈存日志。
通过标准：终端应发送 GET DATA 取日志格式。终端应正确显示日志内容，tag 用中文，过程应为中文，内容与记录一致。终端应能够显示圈存日志内容列表及圈存日志格式（DF4F）推荐值。

7.16.11 BCCS010-01 逐条读取圈存明细，应用锁定

测试目的：确保如果终端支持逐条读取圈存明细，终端应能正确逐条读取和显示圈存明细。
终端配置：支持圈存明细（逐条读取）。
卡片配置：——取圈存日志格式命令和读日志命令卡响应9000；
——应用选择6283。
测试流程：选择应用，取圈存日志格式，读取圈存日志。
通过标准：终端应发送 GET DATA 取日志格式。终端应正确显示日志内容，tag 用中文，过程应为中文，内容与记录一致。终端应能够显示圈存日志内容列表及圈存日志格式（DF4F）推荐值。

7.16.12 BCCS011-00 逐条读取圈存明细,模板长度为 0

测试目的：确保如果终端支持逐条读取圈存明细，终端应能正确逐条读取和显示圈存明细，即使模板长度为0。
终端配置：支持圈存明细（逐条读取）。
卡片配置：——取圈存日志格式命令和读日志命令卡响应9000；
——案例01：DF4F长度为0，模板长度为0。
测试流程：选择应用，取圈存日志格式，读取圈存日志。
通过标准：终端应发送 GET DATA 取日志格式。终端应正确显示日志内容，tag 用中文，过程应为中文，内容与记录一致。终端应能够显示圈存日志内容列表，没有圈存日志格式（DF4F）推荐值。

7.16.13 BCCS012-00 一次性读取圈存明细

测试目的：确保如果终端支持一次性读取圈存明细，终端应能正确读取和显示圈存明细。
终端配置：支持圈存明细（一次性读取日志）。
卡片配置：——取圈存日志格式命令和读日志命令卡响应9000；
——案例01：一次性读取日志，read record P1=00。
测试流程：选择应用，读取圈存日志。
通过标准：终端不应发送 GET DATA 取日志格式。终端应正确显示日志内容，tag 用中文，过程应为中文，内容与记录一致。终端应显示 mac 数值。

7.16.14 BCCS013-00 逐条读取圈存明细，不存在圈存明细

测试目的：确保如果终端支持逐条读取圈存明细，当不存在圈存明细时，终端应显示没有圈存明细信息。
终端配置：支持圈存明细（逐条读取）。
卡片配置：记录为空，FCI中DF4D=0C00。
测试流程：选择卡片应用。
通过标准：终端不应发送 read record 命令。终端应显示没有圈存日志信息。

7.16.15 BCCS014-00 逐条读取圈存明细，根据实际显示条数

测试目的：确保如果终端支持逐条读取圈存明细，终端应根据实际条数显示圈存明细信息。
终端配置：支持圈存明细（逐条读取）。
卡片配置：取圈存日志格式命令和读日志命令卡响应9000。读取第5条记录，返回6A83。
测试流程：选择卡片应用。
通过标准：终端应发送 GET DATA 取日志格式。终端应正确显示日志内容，tag 用中文，过程应为中文，内容与记录一致。终端应能够显示圈存日志内容列表及圈存日志格式（DF4F）推荐值。仅显示四条记录。

7.16.16 BCCS015-00 逐条读取圈存明细，模板长度错

测试目的：确保如果终端支持逐条读取圈存明细，当模板长度错时，终端应终止读取圈存明细信息。
终端配置：支持圈存明细（逐条读取）。
卡片配置：——取圈存日志格式命令和读日志命令卡响应9000；
——读取第1条记录，DF4F格式要求长度与实际记录值长度不一致。
测试流程：选择卡片应用。
通过标准：终端应发送 GET DATA 取日志格式。终端应终止读取圈存日志，在第 1 条记录。

7.16.17 BCCS016-00 逐条读取圈存明细，模板返回异常状态字

测试目的：确保如果终端支持逐条读取圈存明细，当取模板返回异常状态字，终端应终止读取圈存明细信息。
终端配置：支持圈存明细（逐条读取）。
卡片配置：取圈存日志格式命令和读日志命令卡响应9000。get DF4F返回6A88。
测试流程：选择卡片应用。
通过标准：终端应终止读取圈存日志。不能发送 read record 命令。

7.17 安全方面—国际算法补充测试（R-AQFM）

7.17.1 R-AQFM002-01 终端不支持 SM 算法，PDOL 中 DF69=00

测试目的：终端不支持SM算法，PDOL中DF69应该为“00”，数据按照RSA算法返回，使用RSA数据认证，SDA成功，完成交易。
终端配置：支持SDA。
卡片配置：卡的AIP指明支持SDA（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC来完成脱机批准交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.17.2 R-AQFM002-02 终端不支持 SM 算法,GPO 命令返 6985

测试目的：终端不支持SM算法，PDOL中DF69应该为“00”，GPO命令卡片返回6985，终端应终止交易。
终端配置：N/A。
卡片配置：卡片仅支持SM算法。
测试流程：选择卡片应用，执行交易。
通过标准：终端应终止交易。

7.18 安全方面—国密算法（SM-AQFM）

7.18.1 SM-AQFM002-00 终端支持国密算法，国密算法指示位应为01

测试目的：确保如果终端支持SM算法，SM算法指示器DF69应为01。
终端配置：支持SM。
卡片配置：PDOL请求DF69。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。DF69=01。

7.18.2 SM-AQFM003-00 对于RID终端应该能够存储CA索引

测试目的：确保如果终端支持SDA，它应该能够存储66个CA公钥以及与密钥同时用到的相关信息，并能够在给定RID和CA公钥索引后定位相应密钥。
终端配置：支持SDA。
卡片配置：——终端支持3个RID（RID1、RID2和RID3）；
——对于每个RID，终端都载入62个CA公钥（密钥索引从00到05）；
——卡的AIP指明支持SDA（AIP的字节1，位7为‘1’）。
子类案例：——案例01：卡包含基于RID1、密钥索引为00的静态签名和相关数据；
——案例02：卡包含基于RID1、密钥索引为01的静态签名和相关数据；
——案例03：卡包含基于RID1、密钥索引为02的静态签名和相关数据；
——案例04：卡包含基于RID1、密钥索引为03的静态签名和相关数据；
——案例05：卡包含基于RID1、密钥索引为04的静态签名和相关数据；
——案例06：卡包含基于RID1、密钥索引为05的静态签名和相关数据；
——案例07：卡包含基于RID2、密钥索引为00的静态签名和相关数据；
——案例08：卡包含基于RID2、密钥索引为01的静态签名和相关数据；
——案例09：卡包含基于RID2、密钥索引为02的静态签名和相关数据；
——案例10：卡包含基于RID2、密钥索引为03的静态签名和相关数据；
——案例11：卡包含基于RID2、密钥索引为04的静态签名和相关数据；
——案例12：卡包含基于RID2、密钥索引为05的静态签名和相关数据；
——案例13：卡包含基于RID3、密钥索引为00的静态签名和相关数据；
——案例14：卡包含基于RID3、密钥索引为01的静态签名和相关数据；
——案例15：卡包含基于RID3、密钥索引为02的静态签名和相关数据；
——案例16：卡包含基于RID3、密钥索引为03的静态签名和相关数据；
——案例17：卡包含基于RID3、密钥索引为04的静态签名和相关数据；
——案例18：卡包含基于RID3、密钥索引为05的静态签名和相关数据。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.3 SM-AQFM004-00 SDA的算法

测试目的：对于静态数据认证，确保终端在静态数据认证中支持发卡行公钥签名算法标识为‘04’。支持发卡行公钥参数标识为‘11’。
终端配置：支持SDA。
卡片配置：——卡中发卡行公钥证书正确；
——卡中的静态签名是使用发卡行公钥签名算法标识为‘04’和发卡行公钥参数标识为‘11’计算的；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR

字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.4 SM-AQFM006-00 公钥的长度

测试目的：确保对于静态数据认证，终端支持的公钥长度为64字节。
终端配置：支持SDA。
卡片配置：——卡中的静态签名是有效的；
——使用的公钥的长度是64字节；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
子类案例：——案例01：测试针对CA公钥；
——案例02：测试针对发卡行公钥。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.5 SM-AQFM009-00 数据缺失：CA 公钥索引

测试目的：——确保如果IC卡中缺少CA公钥索引，终端的静态数据认证失败；
——确保如果在AIP中脱机静态数据认证是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。
终端配置：支持SDA。
卡片配置：——卡中缺少CA公钥索引；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.6 SM-AQFM010-00 数据缺失：发卡行公钥证书

测试目的：确保如果IC卡中缺少发卡行公钥证书，终端的静态数据认证失败。
终端配置：支持SDA。
卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.7 SM-AQFM012-00 数据缺失：签名静态应用数据

测试目的：——确保如果IC卡中缺少签名的静态应用数据，终端的静态数据认证失败；
——确保如果在AIP中SDA是支持的，且卡中缺少静态应用数据，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：支持SDA。
卡片配置：——卡中缺少静态应用数据；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.8 SM-AQFM014-00 获取用于执行 SDA 的 CA 公钥：密钥不存在

测试目的：确保如果终端支持静态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的静态数据认证失败。
终端配置：——支持SDA；
——终端不包含卡中引用的CA公钥。
卡片配置：卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.9 SM-AQFM014-01 获取用于执行 DDA 的 CA 公钥：密钥不存在

测试目的：确保如果终端支持动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的动态数据认证处理失败。
终端配置：——支持DDA；
——终端不包含卡中引用的CA公钥。
卡片配置：卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.10 SM-AQFM014-02 获取用于执行 CDA 的 CA 公钥：密钥不存在

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败；
——终端不包含卡中引用的CA公钥。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使第一个GENERATE AC请求TC。
测试流程：选择卡片应用，执行交易。
通过标准：终端第一个GENERATE AC应不请求CDA。终端应该依据TAC和IAC设置请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC

命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.11 SM-AQFM014-04 获取用于执行CDA的CA公钥：密钥不存在（2）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使第一个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.12 SM-AQFM014-05 获取用于执行CDA的CA公钥：密钥不存在（3）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC时卡返回ARQC；
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.13 SM-AQFM014-06 获取用于执行CDA的CA公钥：密钥不存在（4）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；

——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC时卡返回ARQC；
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时（万一终端请求AAC而缺少第二个GENERATE AC，此通过标准仅在终端有能力存储失败交易时生效），其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.14 SM-AQFM014-07 获取用于执行CDA的CA公钥：密钥不存在（5）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC时卡返回ARQC；
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.15 SM-AQFM014-08 获取用于执行CDA的CA公钥：密钥不存在（6）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败；
——终端不包含卡中引用的CA公钥。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC；
——交易联机批准。
测试流程：选择卡片应用，执行交易。
通过标准：终端在第一个和第二个GENERATE AC应不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.16 SM-AQFM014-09 获取用于执行 CDA 的 CA 公钥：密钥不存在（7）

测试目的：确保如果终端支持复合动态数据认证，且对于给定的RID和CA公钥索引没有可用的CA公钥，则终端的复合动态数据认证处理失败。
终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败；
——终端不包含卡中引用的CA公钥。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端第一个GENERATE AC请求ARQC；
——交易联机拒绝。
测试流程：选择卡片应用，执行交易。
通过标准：终端在第一个和第二个GENERATE AC应不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.17 SM-AQFM019-00 证书格式不等于‘12’

测试目的：确保如果从发卡行公钥证书中的证书格式不是‘12’，则终端的静态数据认证处理失败。
终端配置：支持SDA。
卡片配置：——卡中发卡行公钥证书格式不是‘12’；
——卡的AIP指明支持SDA（AIP的字节1，位7为‘1’）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.18 SM-AQFM020-00 发卡行公钥证书中的数字签名不正确

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的静态数据认证处理失败。
终端配置：支持SDA。
卡片配置：——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到；
——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。
子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；
——案例04：签名s的最后一个字节有错误。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.19 SM-AQFM021-00 发卡行标识符与 PAN 最左端 3-8 的数字不匹配

测试目的：确保如果发卡行标识符与PAN最左端3到8位数字不匹配，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

子类案例：——案例01：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；

——案例02：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；

——案例03：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.20 SM-AQFM022-00 证书失效日期早于当前日期

测试目的：确保如果证书失效日期早于今天日期，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中发卡行公钥证书计算使用的证书失效日期早于今天日期；

——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.21 SM-AQFM023-00 无效的 RID、CA 公钥索引以及证书序列号

测试目的：确保如果RID、CA公钥索引及证书序列号连接起来的结果表明是已回收的证书，则终端的静态数据认证处理失败。

终端配置：——支持SDA；

——支持发卡行公钥证书的回收；

——终端支持3个RID；

——终端内每个RID装载30个CRL入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡中发卡行公钥证书包含RID、CA公钥索引及证书序列号，该证书存在于终端的回收列表中；

——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

子类案例：——案例01：终端装载30条CRL入口，指定RID 1在回收列表中；

——案例02：终端装载30条CRL入口，指定RID 2在回收列表中；

——案例03：终端装载30条CRL入口，指定RID 3在回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 ='1'（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 ='0'（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.18.22 SM-AQFM023-01 证书回收列表更新，删除

测试目的：确保终端能够通过删除入口更新证书回收列表。

终端配置：——支持SDA；

——支持发卡行公钥证书的回收。

卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为'1'）；

——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位6为'0'；字节1，位5为'0'；字节1，位1为'0'）；

——执行PBOC交易前，证书回收列表更新已完成；

——卡中发卡行公钥证书包含RID、CA公钥索引及证书序列号，该证书已从终端证书回收列表中移除。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；

b）选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 ='0'（SDA成功）。

7.18.23 SM-AQFM023-02 证书回收列表更新，添加

测试目的：确保终端能够通过增加入口更新证书回收列表。

终端配置：——支持SDA；

——支持发卡行公钥证书的回收；

——终端已装载29个证书回收列表入口，案例SM-AQFM027-00已先于此案例执行。

卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为'1'）；

——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位6为'0'；字节1，位5为'0'；字节1，位1为'0'）；

——执行PBOC交易前，证书回收列表更新已完成；

——卡中发卡行公钥证书包含RID、CA公钥索引及证书序列号，该证书已装载在终端证书回收列表中。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；

b）选择卡片应用，执行交易（特别是静态数据认证）；

c）请注意：案例SM-AQFM027-00应先于此案例执行。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 ='1'（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 ='0'（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 ='0'（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 ='1'（脱机数据认证已进行）。

7.18.24 SM-AQFM024-00 不识别的发卡行公钥签名算法标识

测试目的：确保如果发卡行公钥签名算法不支持（不是'04'），则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中发卡行公钥证书不是使用公钥签名算法标识为'04'的算法计算的；

——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.25 SM-AQFM030-00 签名数据格式不为‘13’

测试目的：确保如果签名数据格式不是‘13’，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中签名数据格式不为‘13’；

——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.26 SM-AQFM031-00 签名的静态数据中的数字签名不正确

测试目的：确保如果从签名静态应用数据中计算出的签名与签名静态应用数据中的数字签名不同，则终端的静态数据认证处理失败。

终端配置：支持SDA。

卡片配置：——卡中签名静态应用数据的数字签名使用带有不正确的签名的数据计算得到；

——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

子类案例：——案例01：签名r的第一字节有错误；

——案例02：签名r的最后一个字节有错误；

——案例03：签名s的第一字节有错误；

——案例04：签名s的最后一个字节有错误。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.27 SM-AQFM032-00 静态数据认证中的 SDA 标签列表（1）

测试目的：确保终端在执行SDA时检查SDA标签列表只包含AIP。

终端配置：支持SDA。

卡片配置：卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

子类案例：——案例01：SDA标签列表包含AFL；

——案例02：SDA标签列表包含AFL和AIP。

测试流程：选择卡片应用，执行交易（特别是静态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘1’（SDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.28 SM-AQFM032-01 静态数据认证中的SDA标签列表（2）

测试目的：确保终端在执行SDA时检查SDA标签列表只包含AIP。
终端配置：支持SDA。
卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）；
——SDA标签列表包含标签‘82’（AIP）。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.29 SM-AQFM033-00 数据认证码的存储

测试目的：确保在执行SDA时，终端将数据认证码存储在标签‘9F45’中。
终端配置：支持SDA。
卡片配置：——卡的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）；
——CDOL1请求标签‘9F45’；
——数据认证码为‘DAC0’。
测试流程：选择卡片应用，执行交易（特别是静态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。在接收到第一个GENERATE AC命令时，标签‘9F45’中的值为‘DAC0’。

7.18.30 SM-AQFM036-00 对于RID终端应该能存储CA索引（1）

测试目的：确保如果终端支持动态数据认证，且它能够存储6个CA公钥及与密钥一起使用的相关信息，则在给定RID和CA公钥索引时，终端能够定位到相应密钥。
终端配置：支持DDA。
卡片配置：——终端支持2个RID（RID1和RID2）；
——对于每个RID，终端都载入6个CA公钥（从公钥索引00至05）；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
子类案例：——案例01：卡包含基于RID1、密钥索引01产生正确的动态签名和相关数据；
——案例02：卡包含基于RID1、密钥索引03产生正确的动态签名和相关数据；
——案例03：卡包含基于RID1、密钥索引04产生正确的动态签名和相关数据；
——案例04：卡包含基于RID2、密钥索引01产生正确的动态签名和相关数据；
——案例05：卡包含基于RID2、密钥索引03产生正确的动态签名和相关数据；
——案例06：卡包含基于RID2、密钥索引04产生正确的动态签名和相关数据。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.31 SM-AQFM036-01 对于RID终端应该能存储CA索引（2）

测试目的：确保如果终端支持复合动态数据认证，且它能够存储6个CA公钥及与密钥一起使用的相关信息，则在给定RID和CA公钥索引时，终端能够定位到相应密钥。

终端配置：支持CDA。

卡片配置：——终端支持2个RID；
——对于每个RID，终端都载入6个CA公钥（公钥索引从00至05），如测试案例SM-AQFM038-00；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

子类案例：——案例01：卡包含基于RID1、密钥索引00产生正确的动态签名和相关数据；
——案例02：卡包含基于RID1、密钥索引02产生正确的动态签名和相关数据；
——案例03：卡包含基于RID1、密钥索引05产生正确的动态签名和相关数据；
——案例04：卡包含基于RID2、密钥索引01产生正确的动态签名和相关数据；
——案例05：卡包含基于RID2、密钥索引02产生正确的动态签名和相关数据；
——案例06：卡包含基于RID2、密钥索引05产生正确的动态签名和相关数据。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息中的TSI 的字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.32 SM-AQFM037-00 DDA 的算法（1）

测试目的：对于动态数据认证，确保终端支持发卡行公钥签名算法标识为‘04’，IC卡公钥签名算法标识为‘04’，支持发卡行公钥参数标识为 ‘11’，支持IC卡公钥参数标识为 ‘11’。

终端配置：支持DDA。

卡片配置：——卡中发卡行公钥证书正确；
——卡中IC公钥证书正确；
——卡中的动态签名是使用IC公钥签名算法标识为‘04’和IC卡公钥参数标识为 ‘11’ 计算的；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.33 SM-AQFM037-01 DDA 的算法（2）

测试目的：对于CDA，确保终端支持支持发卡行公钥签名算法标识为‘04’，IC卡公钥签名算法标识为‘04’，支持发卡行公钥参数标识为 ‘11’，支持IC卡公钥参数标识为 ‘11’。

终端配置：支持CDA。

卡片配置：——卡中发卡行公钥证书正确；
——卡中IC公钥证书正确；
——卡中的动态签名是使用IC公钥签名算法标识为‘04’和IC卡公钥参数标识为 ‘11’ 计算的；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息

中的TSI 的字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.34 SM-AQFM039-00 公钥的长度

测试目的：确保对于动态数据认证，终端支持公钥长度是64字节。
终端配置：支持DDA。
卡片配置：——卡计算的动态签名是有效的；
——对于CA密钥、发卡行密钥和IC卡密钥，使用的公钥长度是64字节；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.35 SM-AQFM039-01 公钥的长度（2）

测试目的：确保对于复合动态数据认证，终端支持公钥长度是64字节。
终端配置：支持CDA。
卡片配置：——卡计算的动态签名是有效的；
——对于CA密钥、发卡行密钥和IC卡密钥，使用的公钥长度是64字节；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。包含在金融确认信息或是批数据捕获信息中的TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。包含在金融确认信息或是批数据捕获信息中的TSI 的字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.36 SM-AQFM043-00 数据缺失：CA 公钥索引（1）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端动态数据认证处理失败；
——确保如果在AIP中DDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。
终端配置：支持DDA。
卡片配置：——卡中缺少CA公钥索引；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.37 SM-AQFM043-01 数据缺失：CA 公钥索引（2）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。
终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡中缺少CA公钥索引；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.38 SM-AQFM043-02 数据缺失：CA 公钥索引（3）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.39 SM-AQFM043-03 数据缺失：CA 公钥索引（4）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡在第一个GENERATE AC命令时返回ARQC；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命

令中的TVR字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.40 SM-AQFM043-04 数据缺失：CA公钥索引（5）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡在第一个GENERATE AC命令时返回ARQC；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.41 SM-AQFM043-05 数据缺失：CA公钥索引（6）

测试目的：——确保如果IC卡中缺少CA公钥索引，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少CA公钥索引，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少CA公钥索引；
——卡在第一个GENERATE AC命令时返回ARQC；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.42 SM-AQFM044-00 数据缺失：发卡行公钥证书（1）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端动态数据认证处理失败；
——确保如果在AIP中指明支持脱机动态数据认证，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：支持DDA。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.43 SM-AQFM044-01 数据缺失：发卡行公钥证书（2）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.44 SM-AQFM044-02 数据缺失：发卡行公钥证书（3）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；

——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息(当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.45 SM-AQFM044-03 数据缺失：发卡行公钥证书（4）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前没有探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.46 SM-AQFM044-04 数据缺失：发卡行公钥证书（5）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中支持CDA，且卡中缺少发卡行公钥证书，则终端设置TVR

中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前没有探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.47 SM-AQFM044-05 数据缺失：发卡行公钥证书（6）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示

TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.48 SM-AQFM044-06 数据缺失：发卡行公钥证书（7）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.49 SM-AQFM044-07 数据缺失：发卡行公钥证书（8）

测试目的：——确保如果IC卡中缺少发卡行公钥证书，终端复合动态数据认证处理失败；
——确保如果在AIP中CDA是支持的，且卡中缺少发卡行公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中缺少发卡行公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机拒绝。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.50 SM-AQFM046-00 数据缺失：IC卡公钥证书（1）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端动态数据认证处理失败；
——确保如果在AIP中指明动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：支持DDA。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.51 SM-AQFM046-01 数据缺失：IC卡公钥证书（2）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；
——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。
终端配置：——支持CDA；
——在终端行为分析之前检测到CDA失败。
卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.52 SM-AQFM046-04 数据缺失：IC卡公钥证书（3）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；
——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。
终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。
测试流程：选择卡片应用，执行交易。
通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中或金融确认信息或批上送信息中的TVR字节1，位3 =‘1’（CDA失败）。
第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失），或包含在金融确认信息或批上送信息中（当终端有存储失败或终止交易能力时此通过标准适用）；或终端有类似打印凭证功能来显示TVR。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.53 SM-AQFM046-05 数据缺失：IC卡公钥证书（4）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；
——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时或当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第二个GENERATE AC命令中的TVR字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.54 SM-AQFM046-06 数据缺失：IC卡公钥证书（5）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；
——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.55 SM-AQFM046-07 数据缺失：IC卡公钥证书（6）

测试目的：——确保如果IC卡中缺少IC卡公钥证书，终端对复合动态数据认证处理失败；
——确保如果在AIP中指明复合动态数据认证是支持的，且卡中缺少IC卡公钥证书，则终端设置TVR中‘IC卡数据缺失’位为‘1’。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中缺少IC卡公钥证书；
——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位6 =‘1’（IC卡数据缺失）；或终端有类似打印凭证功能来显示TVR时，其字节1，位6 =‘1’（IC卡数据缺失）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.56 SM-AQFM054-00 证书格式不等于‘12’（1）

测试目的：确保如果从发卡行公钥证书中的证书格式不等于‘12’，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.57 SM-AQFM054-01 证书格式不等于‘12’（2）

测试目的：确保如果从发卡行公钥证书中的证书格式不等于‘12’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该依据TAC和IAC设置请求一个TC或AAC来完成交易。终端在GENERATE AC命令中应不请求CDA。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA

失败)。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’(未使用DDA)。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.58 SM-AQFM054-03 证书格式不等于‘12’（3）

测试目的：确保如果从发卡行公钥证书中的证书格式不等于‘12’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1)；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败)；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败)；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败)。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’(未使用DDA)。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行)；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行)；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.59 SM-AQFM054-04 证书格式不等于‘12’（4）

测试目的：确保如果从发卡行公钥证书中的证书格式不等于‘12’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1)；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败)。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA)。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA)。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行)。

7.18.60 SM-AQFM054-05 证书格式不等于‘12’（5）

测试目的：确保如果从发卡行公钥证书中的证书格式不等于‘02’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；

——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.61 SM-AQFM054-06 证书格式不等于‘12’（6）

测试目的：确保如果从发卡行公钥证书中的证书格式不等于‘02’，终端复合动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——卡中发卡行公钥证书不是使用证书格式为‘02’的数据计算得到；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.62 SM-AQFM055-00 发卡行公钥证书中的数字签名不正确（1）

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持脱机动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到。

子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；
——案例04：签名s的最后一个字节有错误。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.63 SM-AQFM055-01 发卡行公钥证书中的数字签名不正确（2）

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的动态数据认证处理失败。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到。
子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；
——案例04：签名s的最后一个字节有错误。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过请求一个TC或AAC来完成交易。终端在GENERATE AC命令中应不请求CDA。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.64 SM-AQFM055-03 发卡行公钥证书中的数字签名不正确（3）

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的动态数据认证处理失败。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证 （AIP 字节1，位1 =1）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到。
子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；
——案例04：签名s的最后一个字节有错误。
测试流程：选择卡片应用，执行交易。
通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；

或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.65 SM-AQFM055-04 发卡行公钥证书中的数字签名不正确（4）

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到。

子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；
——案例04：签名s的最后一个字节有错误。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC命令请求一个AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.66 SM-AQFM055-05 发卡行公钥证书中的数字签名不正确（5）

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——CDA总是请求，在第二个GAC请求TC；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——发卡行响应批准；
——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到。

子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；
——案例04：签名s的最后一个字节有错误。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.67 SM-AQFM055-06 发卡行公钥证书中的数字签名不正确（6）

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——终端无法联机；
——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到。

子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；
——案例04：签名s的最后一个字节有错误。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.68 SM-AQFM055-07 发卡行公钥证书中的数字签名不正确（7）

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——交易联机批准；
——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到。

子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；

——案例04：签名s的最后一个字节有错误。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.69 SM-AQFM055-08 发卡行公钥证书中的数字签名不正确（8）

测试目的：确保如果从发卡行公钥证书中计算出的签名与发卡行公钥证书中的数字签名不同，则终端的动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前探测到CDA失败。

卡片配置：——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——卡的AIP指明支持复合动态数据认证（AIP 字节1，位1 =‘1’）；
——交易联机拒绝；
——卡中发卡行公钥证书签名使用带有不正确的签名的数据计算得到。

子类案例：——案例01：签名r的第一字节有错误；
——案例02：签名r的最后一个字节有错误；
——案例03：签名s的第一字节有错误；
——案例04：签名s的最后一个字节有错误。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.70 SM-AQFM056-00 发卡行标识与 PAN 最左边的 3—8 位不匹配（1）

测试目的：确保如果发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）。

子类案例：——案例01：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.71 SM-AQFM056-01 发卡行标识与 PAN 最左边的 3—8 位不匹配（2）

测试目的：确保如果发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：——支持CDA；
——终端行为分析前探测到CDA失败。
卡片配置：卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）。
子类案例：——案例01：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端在GENERATE AC命令时不应请求CDA。终端应该依据TAC和IAC设置请求TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.72 SM-AQFM056-03 发卡行标识与 PAN 最左边的 3—8 位不匹配（3）

测试目的：确保如果发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。
终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。
子类案例：——案例01：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。
测试流程：选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.73 SM-AQFM056-04 发卡行标识与 PAN 最左边的 3—8 位不匹配（4）

测试目的：确保如果发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC。

子类案例：——案例01：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.74 SM-AQFM056-05 发卡行标识与 PAN 最左边的 3—8 位不匹配（5）

测试目的：确保如果发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——发卡行响应批准。

子类案例：——案例01：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.75 SM-AQFM056-06 发卡行标识与 PAN 最左边的 3—8 位不匹配（6）

测试目的：确保如果发卡行标识与PAN最左边的3到8位不匹配，终端动态数据认证处理失败。

终端配置：——支持CDA；

——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡在第一个GENERATE AC命令返回ARQC；
——终端无法联机。

子类案例：——案例01：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第3位数字不同；
——案例02：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：第8位数字不同；
——案例03：卡中发卡行公钥证书带有与PAN最左端3到8位数字不同的发卡行标识符：所有3到8位数字不同。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.76 SM-AQFM057-00 证书失效日期早于今天（1）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.77 SM-AQFM057-01 证书失效日期早于今天（2）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.78 SM-AQFM057-03 证书失效日期早于今天（3）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。
终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC。
测试流程：选择卡片应用，执行交易。
通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.79 SM-AQFM057-04 证书失效日期早于今天（4）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。
测试流程：选择卡片应用，执行交易。
通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.80 SM-AQFM057-05 证书失效日期早于今天（5）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。
终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——CDA总是请求，在第二个GAC请求TC；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；

——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.81 SM-AQFM057-06 证书失效日期早于今天（6）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.82 SM-AQFM057-07 证书失效日期早于今天（7）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机批准；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个

GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.83 SM-AQFM057-08 证书失效日期早于今天（8）

测试目的：确保如果证书失效日期早于今天日期，终端动态数据认证处理失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持动态数据认证（AIP 字节1，位6 =‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机拒绝；
——卡中的发卡行公钥证书计算使用的证书失效日期早于今天日期。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.84 SM-AQFM058-00 RID、CA 公钥索引和证书序列号无效（1）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个RID对应三十个公钥入口，如果RID、CA公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端动态数据认证失败。

终端配置：——支持DDA；
——支持发卡行公钥证书的回收；
——终端支持三个RID；
——终端内每个RID装载30个CRL入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡中的发卡行公钥证书恢复后，RID、CA公钥索引和证书序列号表明证书在终端证书回收列表中。

子类案例：——案例01：终端装载30条CRL入口，指定RID 1在回收列表中；
——案例02：终端装载30条CRL入口，指定RID 2在回收列表中；
——案例03：终端装载30条CRL入口，指定RID 3在回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.85 SM-AQFM058-01 RID、CA 公钥索引和证书序列号无效，CDA（2）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个RID对应三十条公钥入口，如果RID、CA公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持CDA；
——支持发卡行公钥证书的回收；
——终端行为分析前有能力探测到CDA失败；
——终端支持三个RID；

——终端内每个RID装载30个CRL入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中的发卡行公钥证书恢复后，RID、CA公钥索引和证书序列号表明证书在终端证书回收列表中。

子类案例：——案例01：终端装载30条CRL入口，指定RID 1在回收列表中；
——案例02：终端装载30条CRL入口，指定RID 2在回收列表中；
——案例03：终端装载30条CRL入口，指定RID 3在回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.86 SM-AQFM058-03 RID、CA公钥索引和证书序列号无效（3）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个RID对应三十个公钥入口，如果RID、CA公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败；
——支持发卡行公钥证书的回收；
——终端支持三个RID；
——终端内每个RID装载30个CRL入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中的发卡行公钥证书恢复后，RID、CA公钥索引和证书序列号表明证书在终端证书回收列表中。

子类案例：——案例01：终端装载30条CRL入口，指定RID 1在回收列表中；
——案例02：终端装载30条CRL入口，指定RID 2在回收列表中；
——案例03：终端装载30条CRL入口，指定RID 3在回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.87 SM-AQFM058-04 证书回收列表更新，删除（1）

测试目的：确保终端能够通过删除入口更新证书回收列表。
终端配置：——支持DDA；
——支持发卡行公钥证书的回收；
——终端已装载案例SM-AQFM132-00中描述的30个证书回收列表入口。
卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位7为‘0’；字节1，位5为‘0’；字节1，位1为‘0’）；
——执行交易前，证书回收列表更新已完成；
——一个有效的证书回收列表从终端移除，而卡片中的发卡行公钥证书是根据与该有效入口香对应的RID、CA公钥索引以及证书序列号进行计算的。
测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（DDA成功）。

7.18.88 SM-AQFM058-05 证书回收列表更新，添加（1）

测试目的：确保终端能够通过增加入口更新证书回收列表。
终端配置：——支持DDA；
——支持发卡行公钥证书的回收；
——终端已装载29个证书回收列表入口，案例SM-AQFM135-00已先于此案例执行。
卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位7为‘0’；字节1，位5为‘0’；字节1，位1为‘0’）；
——执行交易前，证书回收列表更新已完成；
——卡中发卡行公钥证书是由与该有效入口相对应的RID、CA公钥索引及证书序列号计算得到的，该证书已装载在终端证书回收列表中。
测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是动态数据认证）；
c）请注意：案例SM-AQFM135-00应先于此案例执行。
通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘1’（DDA失败）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.89 SM-AQFM058-06 证书回收列表更新，删除（2）

测试目的：确保终端能够通过删除入口更新证书回收列表。
终端配置：——支持CDA；
——支持发卡行公钥证书的回收；
——终端已装载案例SM-AQFM132-00中描述的30个证书回收列表入口。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位7为‘0’；字节1，位5为‘0’；字节1，位6为‘0’）；
——执行交易前，证书回收列表更新已完成；
——卡中发卡行公钥证书是由与该有效入口相对应的RID、CA公钥索引及证书序列号计算得到的，该证书已从终端证书回收列表中移除。
测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应该通过请求一个TC或AAC来完成交易。金融确认信息或批上送信息中

TVR的字节1，位4为‘0’（未使用DDA）。金融确认信息或批上送信息中TVR的字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.90 SM-AQFM058-07 证书回收列表更新，添加（2）

测试目的：确保终端能够通过增加入口更新证书回收列表。

终端配置：——支持CDA；
——支持发卡行公钥证书的回收；
——终端已装载29个证书回收列表入口，案例AQFM137-00已先于此案例执行。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡的AIP指明其他数据认证方式不支持（AIP的字节1，位7为‘0’；字节1，位5为‘0’；字节1，位6为‘0’）；
——执行交易前，证书回收列表更新已完成；
——卡中发卡行公钥证书包含RID、CA公钥索引及证书序列号，该证书已装载在终端证书回收列表中。

测试流程：a）证书回收列表更新过程已按照终端厂商的说明文档执行完毕；
b）选择卡片应用，执行交易（特别是复合动态数据认证）；
c）请注意：案例SM-AQFM137-00应先于此案例执行。

通过标准：终端应该通过请求一个TC或AAC来完成交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。

7.18.91 SM-AQFM058-10 RID、CA 公钥索引和证书序列号无效（4）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个RID对应三十个公钥入口，如果RID、CA公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——终端行为分析前不能探测到CDA失败；
——支持发卡行公钥证书的回收；
——CDA总是请求，第一个GAC请求ARQC；
——终端支持三个RID；
——终端内每个RID装载30个证书回收列表入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC时请求TC；
——卡中的发卡行公钥证书恢复后，RID、CA公钥索引和证书序列号表明证书在终端证书回收列表中。

子类案例：——案例01：终端装载30条证书回收列表入口，指定RID 1在回收列表中；
——案例02：终端装载30条证书回收列表入口，指定RID 2在回收列表中；
——案例03：终端装载30条证书回收列表入口，指定RID 3在回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR

字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.92 SM-AQFM058-11 RID、CA公钥索引和证书序列号无效（5）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个RID对应三十条公钥入口，如果RID、CA公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——终端行为分析前不能探测到CDA失败；
——支持发卡行公钥证书的回收；
——CDA从不请求，第一个GAC请求ARQC；
——CDA总是请求，第二个GAC请求TC；
——终端支持三个RID；
——终端内每个RID装载30个证书回收列表入口，其中29个是基于未签名的证书序列号（例如虚拟测试数据）。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC时请求TC；
——发卡行响应批准；
——卡中的发卡行公钥证书恢复后，RID、CA公钥索引和证书序列号表明证书在终端证书回收列表中。

子类案例：——案例01：终端装载30条证书回收列表入口，指定RID 1在回收列表中；
——案例02：终端装载30条证书回收列表入口，指定RID 2在回收列表中；
——案例03：终端装载30条证书回收列表入口，指定RID 3在回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.93 SM-AQFM058-12 RID、CA公钥索引和证书序列号无效（6）

测试目的：确认当终端支持发卡行公钥证书的回收，且支持每个RID对应三十条公钥入口，如果RID、CA公钥索引和证书序列号和任何其他附加数据表明证书已被回收，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——终端行为分析前不能探测到CDA失败；
——支持发卡行公钥证书的回收；
——CDA从不请求，第一个GAC请求ARQC；
——当不能联机时，正常处理缺省行为码；
——终端支持三个RID；
——终端内每个RID装载30个证书回收列表入口，其中29个是基于未签名的

证书序列号（例如虚拟测试数据）。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC时请求TC；
——终端无法联机；
——卡中的发卡行公钥证书恢复后，RID、CA公钥索引和证书序列号表明证书在终端证书回收列表中。

子类案例：——案例01：终端装载30条证书回收列表入口，指定RID 1在回收列表中；
——案例02：终端装载30条证书回收列表入口，指定RID 2在回收列表中；
——案例03：终端装载30条证书回收列表入口，指定RID 3在回收列表中。

测试流程：选择卡片应用，在每个案例中选择指定的RID，执行交易（特别是复合动态数据认证）。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.94 SM-AQFM059-00 发卡行公钥签名算法无法识别（1）

测试目的：如果发卡行公钥签名算法标识不是04，终端动态数据认证执行失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡中计算公钥证书的公钥签名算法标识不为‘04’。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.95 SM-AQFM059-01 发卡行公钥签名算法无法识别（2）

测试目的：如果发卡行公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算公钥证书的公钥签名算法标识不为‘04’。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.96 SM-AQFM059-03 发卡行公钥签名算法无法识别（3）

测试目的：如果发卡行公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；

——仅脱机终端或可联机的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中计算公钥证书签名的公钥签名算法标识不为‘04’。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.97 SM-AQFM059-04 发卡行公钥签名算法无法识别（4）

测试目的：如果发卡行公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中计算公钥证书签名的公钥签名算法标识不为‘04’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.98 SM-AQFM059-05 发卡行公钥签名算法无法识别（5）

测试目的：如果发卡行公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中计算公钥证书的公钥签名算法标识不为‘04’；
——发卡行响应批准。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.99 SM-AQFM059-06 发卡行公钥签名算法无法识别（6）

测试目的：如果发卡行公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——卡中计算公钥证书的公钥签名算法标识不为‘04’；
——终端无法联机。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.100 SM-AQFM060-00 长度为 3-8 位的发卡行标识（1）

测试目的：如果恢复出来的发卡行标识长度为3到8位数字，确保终端正确执行静态数据认证。

终端配置：支持SDA。

卡片配置：卡片的AIP指明支持静态数据认证（AIP的字节1，位7为‘1’）。

子类案例：——案例01：使用长度为3位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；
——案例02：使用长度为6位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；
——案例03：使用长度为8位数字的发卡行标识计算发卡行公钥证书。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中TVR的字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’（SDA成功）。第一个GENERATE AC命令中TSI的字节1，位8 =‘1’（脱机数据认证已

进行）。

7.18.101 SM-AQFM060-01 长度为 3-8 位的发卡行标识（2）

测试目的：如果恢复出来的发卡行标识长度为3到8位数字，确保终端正确执行动态数据认证。

终端配置：支持DDA。

卡片配置：卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。

子类案例：——案例01：使用长度为3位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；

——案例02：使用长度为6位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；

——案例03：使用长度为8位数字的发卡行标识计算发卡行公钥证书。

测试流程：选择卡片应用，执行交易。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 =‘0’（DDA成功）。第一个GENERATE AC命令中TVR的字节1，位3 =‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.102 SM-AQFM060-02 长度为 3-8 位的发卡行标识（3）

测试目的：如果恢复出来的发卡行标识长度为3到8位数字，确保终端正确执行复合动态数据认证。

终端配置：——支持CDA；

——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡的AIP指明复合动态数据认证（AIP 字节1，位1 =‘1’）；

——设置IAC和TAC使终端在第一个GENERATE AC时请求TC，且卡返回TC。

子类案例：——案例01：使用长度为3位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；

——案例02：使用长度为6位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；

——案例03：使用长度为8位数字的发卡行标识计算发卡行公钥证书。

测试流程：选择卡片应用，执行交易完成。

通过标准：终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令或金融确认信息或批上送信息中的TVR字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。金融确认信息或批上送信息中中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.103 SM-AQFM060-04 长度为 3-8 位的发卡行标识（4）

测试目的：如果恢复出来的发卡行标识长度为3到8位数字，确保终端正确执行复合动态数据认证。

终端配置：——支持CDA。

——仅联机终端。

——CDA总是请求，第一个GAC请求ARQC时或CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡的AIP指明复合动态数据认证（AIP 字节1，位1 =‘1’）。

——卡在第一个GENERATE AC命令返回ARQC。

——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC。

子类案例：——案例01：使用长度为3位数字的发卡行标识，右补‘F’至8位计算发卡行

公钥证书。

——案例02：使用长度为6位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书。

——案例03：使用长度为8位数字的发卡行标识计算发卡行公钥证书。

测试流程：选择卡片应用，执行交易完成。

通过标准：终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令或金融确认信息或批上送信息中的TVR字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。金融确认信息或批上送信息中中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.104 SM-AQFM060-05 长度为 3-8 位的发卡行标识（5）

测试目的：如果恢复出来的发卡行标识长度为3到8位数字，确保终端正确执行复合动态数据认证。

终端配置：——支持CDA；

——仅联机终端；

——正常处理缺省行为码。

卡片配置：——卡的AIP指明复合动态数据认证（AIP 字节1，位1 =‘1’）；

——卡在第一个GENERATE AC命令返回ARQC；

——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；

——终端无法联机。

子类案例：——案例01：使用长度为3位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；

——案例02：使用长度为6位数字的发卡行标识，右补‘F’至8位计算发卡行公钥证书；

——案例03：使用长度为8位数字的发卡行标识计算发卡行公钥证书。

测试流程：选择卡片应用，执行交易完成。

通过标准：终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令或金融确认信息或批上送信息中的TVR字节1，位3 =‘0’（CDA成功）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。金融确认信息或批上送信息中中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.105 SM-AQFM065-00 证书格式不等于‘14’（1）

测试目的：如果从IC卡公钥证书中恢复得到的证书格式不等于‘14’，终端动态数据认证失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；

——卡中IC卡公钥证书格式不是‘14’。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位3 =‘0’

（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.106 SM-AQFM065-01 证书格式不等于‘14’（2）

测试目的：如果从IC卡公钥证书中恢复得到的证书格式不等于‘14’，终端复合动态数据认证失败。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中IC卡公钥证书格式不是‘14’。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GENERATE AC命令中应不请求CDA。终端应该依据TAC和IAC设置请求TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.107 SM-AQFM065-04 证书格式不等于‘14’（3）

测试目的：如果从IC卡公钥证书中恢复得到的证书格式不等于‘14’，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——卡中IC卡公钥证书格式不是‘14’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）；或金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.108 SM-AQFM065-05 证书格式不等于‘14’（4）

测试目的：如果从IC卡公钥证书中恢复得到的证书格式不等于‘14’，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；

——卡中IC卡公钥证书格式不是‘14’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第一个GENERATE AC命令中的TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.109 SM-AQFM065-06 证书格式不等于‘14’（5）

测试目的：如果从IC卡公钥证书中恢复得到的证书格式不等于‘14’，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——CDA总是请求，在第二个GAC请求TC；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准；
——卡中IC卡公钥证书格式不是‘14’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.110 SM-AQFM065-07 证书格式不等于‘14’（6）

测试目的：如果从IC卡公钥证书中恢复得到的证书格式不等于‘14’，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC；
——正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机；
——卡中IC卡公钥证书格式不是‘14’。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TVR字节1，位3 =‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 =‘1’（CDA失败）。第一个GENERATE

AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 =‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储失败或终止交易能力时此通过标准适用）中TSI字节1，位8 =‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 =‘1’（脱机数据认证已进行）。

7.18.111 SM-AQFM066-00 IC卡公钥证书中的数字签名不正确（1）

测试目的：如果计算得到的签名结果与从IC卡公钥证书中得到的签名结果不相等，终端动态数据认证失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持脱机动态数据认证（AIP的字节1，位6为‘1’）；
——计算卡中的IC卡公钥证书时使用错误的签名数据。

测试流程：选择卡片应用，执行交易（特别是在动态数据认证中）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.112 SM-AQFM066-01 IC卡公钥证书中的数字签名不正确（2）

测试目的：如果计算得到的签名结果与从IC卡公钥证书中得到的签名结果不相等，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持脱机复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——计算卡中的IC卡公钥证书时使用错误的签名数据。

测试流程：选择卡片应用，执行交易。

通过标准：终端GENERATE AC时不请求CDA。终端应该通过设置TAC和IAC来请求一个TC完成交易。第一个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.113 SM-AQFM066-04 IC卡公钥证书中的数字签名不正确（3）

测试目的：如果计算得到的签名结果与从IC卡公钥证书中得到的签名结果不相等，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持脱机复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求TC；
——计算卡中的IC卡公钥证书时使用错误的签名数据。

测试流程：选择卡片应用，执行交易。

通过标准：当卡在第一个GENERATE AC返回TC时，终端应拒绝交易且不执行第二个GENERATE AC命令；或当卡在第一个GENERATE AC返回ARQC时，终端应通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）；或金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TVR字节1，位3 为‘1’（CDA失败）；

或终端有类似打印凭证功能来显示TVR时，其字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）；或金融确认信息或批上送信息(当终端有存储拒绝或终止交易能力时此通过标准适用)中TSI字节1，位8 为‘1’（脱机数据认证已进行）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 为‘1’（脱机数据认证已拒绝）。

7.18.114 SM-AQFM066-05 IC卡公钥证书中的数字签名不正确（4）

测试目的：如果计算得到的签名结果与从IC卡公钥证书中得到的签名结果不相等，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持脱机复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——计算卡中的IC卡公钥证书时使用错误的签名值。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该通过第二个GENERATE AC请求AAC来拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第二个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.115 SM-AQFM066-06 IC卡公钥证书中的数字签名不正确（5）

测试目的：如果计算得到的签名结果与从IC卡公钥证书中得到的签名结果不相等，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持脱机复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——发卡行响应批准交易；
——计算卡中的IC卡公钥证书时使用错误的签名数据。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TVR字节1，位3 为‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 =‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TSI字节1，位8为‘1’（脱机数据认证已完成）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.116 SM-AQFM066-07 IC卡公钥证书中的数字签名不正确（6）

测试目的：如果计算得到的签名结果与从IC卡公钥证书中得到的签名结果不相等，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持脱机复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENERATE AC命令返回ARQC；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC，第二个GENERATE AC请求TC；
——终端无法联机；
——计算卡中的IC卡公钥证书时使用错误的签名数据。

测试流程：选择卡片应用，执行交易。

通过标准：终端应拒绝交易。金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TVR字节1，位3 为‘1’（CDA失败）；或终端有类似打印凭证功能来显示TVR时，其字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。金融确认信息或批上送信息（当终端有存储拒绝或终止交易能力时此通过标准适用）中TSI字节1，位8 为‘1’（脱机数据认证已完成）；或终端有类似打印凭证功能来显示TSI时，其字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.117 SM-AQFM066-08 IC卡公钥证书中的数字签名不正确（7）

测试目的：如果计算得到的签名结果与从IC卡公钥证书中得到的签名结果不相等，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持脱机复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；
——交易联机批准；
——计算卡中的IC卡公钥证书时使用错误的签名数据。

测试流程：选择卡片应用，执行交易。

通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个TC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.118 SM-AQFM066-09 IC卡公钥证书中的数字签名不正确（8）

测试目的：如果计算得到的签名结果与从IC卡公钥证书中恢复得到的签名结果不相等，终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持脱机复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC时请求ARQC；

——交易联机拒绝；
——计算卡中的IC卡公钥证书时使用错误的签名数据。
测试流程：选择卡片应用，执行交易。
通过标准：终端第一个和第二个GENERATE AC时不请求CDA。终端应该通过请求一个AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.119 SM-AQFM067-00 获取的 PAN 不等于读取的 PAN（1）

测试目的：如果证书中的PAN不等于读取的PAN，终端脱机数据认证失败。
终端配置：支持 DDA。
卡片配置：——卡中的AIP指明支持DDA（AIP的字节1，位6为‘1’）；
——计算IC卡公钥证书中的PAN不等于卡中的PAN。
测试流程：选择卡片应用，执行交易（特别是DDA中）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位4 为‘1’（DDA失败）。第一个GENERATE AC中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.120 SM-AQFM067-01 获取的 PAN 不等于读取的 PAN（2）

测试目的：如果证书中的PAN不等于读取的PAN，终端复合脱机数据认证失败。
终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——计算IC卡公钥证书中的PAN不等于卡中的PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端在GAC时不请求CDA。终端根据TAC和IAC的设置，通过请求一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.121 SM-AQFM067-04 获取的 PAN 不等于读取的 PAN（3）

测试目的：如果证书中的PAN不等于读取的PAN，终端复合脱机数据认证失败。
终端配置：——支持CDA；
——仅脱机或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——通过设置IAC和TAC,终端在第一个GAC时请求TC；
——计算IC卡公钥证书中的发卡行 ID 不等于卡中的PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端应拒绝交易。第二个GENERATE AC中TVR的字节1，位3 为‘1’（CDA失败）或是包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR。终端根据TAC和IAC的设置，通过请求一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。第二个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已完成）或者或是包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如

凭条显示TSI。

7.18.122 SM-AQFM067-05 获取的 PAN 不等于读取的 PAN（4）

测试目的：如果证书中的PAN不等于读取的PAN，终端复合脱机数据认证失败。
终端配置：——支持 CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——第一个GAC时卡返回ARQC；
——通过设置IAC和TAC,终端在第一个GAC时请求ARQC,在第二个GAC时请求TC；
——计算发卡行公钥证书中的PAN不等于卡中的PAN。
测试流程：选择卡片应用，执行交易。
通过标准：终端通过第二个 GAC请求AAC拒绝交易。第二个GENERATE AC中TVR的字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。第二个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已完成）

7.18.123 SM-AQFM067-06 获取的 PAN 不等于读取的 PAN（5）

测试目的：如果证书中的PAN不等于读取的PAN，终端复合脱机数据认证失败。。
终端配置：——支持CDA；
——仅联机；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——第一个GAC时卡返回ARQC；
——通过设置IAC和TAC,终端在第一个GAC时请求ARQC,在第二个GAC时请求TC；
——发卡行公钥证书中的PAN不等于卡中的PAN；
——发卡行批准交易。
测试流程：选择卡片应用，执行交易。
通过标准：终端拒绝交易。TVR的字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。TSI的字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.124 SM-AQFM067-07 获取的 PAN 不等于读取的 PAN（6）

测试目的：如果证书中的PAN不等于读取的PAN，终端复合脱机数据认证失败。。
终端配置：——支持CDA；
——仅联机；
——终端不能联机；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；

——第一个GAC时卡返回ARQC；
——通过设置IAC和TAC,终端在第一个GAC时请求ARQC,在第二个GAC时请求TC；
——计算发卡行公钥证书中的发卡行 ID 不等于卡中的PAN。

测试流程：选择卡片应用，执行交易。

通过标准：终端拒绝交易。TVR的字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。TSI的字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.125 SM-AQFM068-00 证书失效日期早于今天（1）

测试目的：如果证书失效日期早于今天日期，则终端脱机数据认证失败。

终端配置：支持DDA。

卡片配置：——卡中发卡行公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持DDA（AIP的字节1，位6为‘1’）。

测试流程：选择卡片应用，执行交易（特别是DDA）。

通过标准：终端应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位4 为‘1’（DDA失败）。第一个GENERATE AC命令中的TVR字节1，位3为‘0’（未使用CDA）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.126 SM-AQFM068-01 证书失效日期早于今天（2）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。

终端配置：——支持CDA；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GAC时不会请求CDA。终端根据TAC和IAC设置，应该通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.127 SM-AQFM068-04 证书失效日期早于今天（3）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——通过设置IAC和TAC，终端在第一个GAC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端拒绝交易并且不执行2nd GAC当卡返回TC时，或者拒绝交易通过执行2nd GAC请求AAC当卡在1st GAC时返回ARQC。TVR字节1，位3 为‘1’（CDA失败）包含在2nd GAC或者金融确认报文或是批上送报文（该通过标准仅用于终端

有能力保存拒绝或是终止交易)或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA)。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在2nd GAC或者金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.128 SM-AQFM068-05 证书失效日期早于今天（4）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’)；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC, 在第二个GAC时请求TC；
——卡在1st GAC时返回ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端通过执行第二个 GAC时请求AAC拒绝交易。第二个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败)。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA)。第二个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已进行)。

7.18.129 SM-AQFM068-06 证书失效日期早于今天（5）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。

终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’)；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC, 在第二个GAC时请求TC；
——卡在第一个GAC时返回ARQC；
——发卡行批准交易。

测试流程：选择卡片应用，执行交易。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA)。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.130 SM-AQFM068-07 证书失效日期早于今天（6）

测试目的：如果证书失效日期早于今天日期，则终端复合动态数据认证失败。

终端配置：——支持CDA；

——仅联机终端；
——终端不能联机；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡中IC卡公钥证书计算使用的证书失效日期早于今天日期；
——卡的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC；
——卡在第一个GAC时返回ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文中。

7.18.131 SM-AQFM069-00 IC卡公钥签名算法无法识别（1）

测试目的：如果IC卡公钥签名算法标识不是04，终端动态数据认证执行失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥签名算法标识不为‘04’。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.132 SM-AQFM069-01 IC卡公钥签名算法无法识别（2）

测试目的：如果IC卡公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥签名算法标识不为‘04’；
——通过设置IAC和TAC，终端在第一个GAC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端在GAC时不应请求CDA。终端应根据TAC和IAC设置，通过请求一个TC来完成交易。第一个GENERATE AC命令中TVR的字节1，位3为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.133 SM-AQFM069-04 IC卡公钥签名算法无法识别（3）

测试目的：如果IC卡公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥签名算法标识不为‘04’；

——通过设置IAC和TAC，终端在第一个GAC时请求TC。

子类案例：——案例01：第一个GAC明文和CID为TC；

——案例01：第一个GAC明文和CID为ARQC。

测试流程：选择卡片应用，执行交易。

通过标准：案例01：终端应该拒绝交易且不执行第二个GAC。案例01：终端通过立即发送第二个GAC请求AAC来完成交易。TVR字节1，位3 为‘1’（CDA失败）包含在第二个 GAC中或金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

TSI字节1，位8 为‘1’（脱机数据认证已完成）包含第二个 GAC中或金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.134 SM-AQFM069-05 IC卡公钥签名算法无法识别（4）

测试目的：如果IC卡公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；

——仅联机终端；

——CDA总是请求，第一个GAC请求ARQC时；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——卡中计算IC卡公钥证书的IC卡公钥签名算法标识不为‘04’；

——卡在第一个GAC时返回ARQC；

——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易通过第二个GAC请求AAC。第二个GENERATE AC命令中TVR的字节1，位3为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。第二个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.135 SM-AQFM069-06 IC卡公钥签名算法无法识别（5）

测试目的：如果IC卡公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；

——仅联机终端；

——CDA从不请求，第一个GAC请求ARQC时；

——CDA总是请求，在第二个GAC请求TC时；

——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——卡中计算IC卡公钥证书的IC卡公钥签名算法标识不为‘04’；

——卡在第一个GAC时返回ARQC；

——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC；

——发卡行批准交易。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，

位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.136 SM-AQFM069-07 IC卡公钥签名算法无法识别（6）

测试目的：如果IC卡公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥签名算法标识不为‘04’；
——卡在第一个GAC时返回ARQC；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC，在第二个GAC时请求TC。

测试流程：选择卡片应用，执行交易。

通过标准：终端应该拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.137 SM-AQFM069-08 IC卡公钥签名算法无法识别（7）

测试目的：如果IC卡公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥签名算法标识不为‘04’；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC；
——交易联机接受。

测试流程：选择卡片应用，执行交易。

通过标准：终端在1st GAC和2nd GAC时不应请求CDA。终端应该完成交易通过请求TC。第一个GENERATE AC命令中TVR字节1，位3 =‘1’（CDA失败）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.138 SM-AQFM069-09 IC卡公钥签名算法无法识别（8）

测试目的：如果IC卡公钥签名算法标识不是04，终端复合动态数据认证执行失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡中计算IC卡公钥证书的IC卡公钥签名算法标识不为‘04’；
——通过设置IAC和TAC，终端在第一个GAC时请求ARQC；

——交易联机拒绝。

测试流程：选择卡片应用，执行交易。

通过标准：终端在1st GAC和2nd GAC时不应请求CDA。终端应该通过请求AAC完成交易。第一个GENERATE AC命令中TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中TSI字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.139 SM-AQFM071-00 动态签名的生成

测试目的：——确保终端支持有效的DDOL；
——如果支持动态数据认证，终端能发送一个包含DDOL中指定数据元的EXTERNAL AUTHENTICATE命令。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡中存在DDOL ；
——卡计算的动态签名是正确的。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。卡片收到的EXTERNAL AUTHENTICATE命令数据域是按照JR/T 0025.4—2013 5.3条定义的规则将DDOL的数据元连接起来得到的。第一个GENERATE AC命令中TSI的字节1，位 8 为‘1’（脱机数据认证已完成）。

7.18.140 SM-AQFM072-00 缺省 DDOL

测试目的：如果支持动态数据认证且卡片中没有DDOL，终端能使用其缺省DDOL。

终端配置：——支持DDA；
——终端含有缺省DDOL。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡中不存在DDOL ；
——卡计算的动态签名是正确的。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。卡片收到的INTERNAL AUTHENTICATE命令数据域是JR/T 0025.4—2013 5.3条定义的规则将缺省DDOL的数据元连接起来得到的。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.141 SM-AQFM074-00 不可预测数的来源

测试目的：如果支持动态数据认证且DDOL中请求不可预知数，终端发送的INTERNAL AUTHENTICATE命令中含有4个字节的不可预知数。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——DDOL请求4个字节的不可预知数（‘9F37’）；
——卡计算的动态签名是正确的。

测试流程：选择卡片应用，执行交易（特别是动态数据认证）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用

SDA)。卡片收到的INTERNAL AUTHENTICATE命令的数据域中含有不可预知数。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成)。

7.18.142 SM-AQFM075-00 DDOL 中不含不可预测数

测试目的：如果支持动态数据认证且卡片的DDOL不请求不可预知数，终端动态数据认证失败。

终端配置：——支持DDA；
——终端缺省的DDOL请求4个字节的不可预知数（‘9F37’)。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’)；
——卡中的DDOL不请求4个字节的不可预知数（‘9F37’） 。

测试流程：选择卡片应用，执行交易（特别是动态数据认证)。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’(DDA失败)。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA)。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成)。

7.18.143 SM-AQFM076-00 缺省 DDOL 不含有不可预测数

测试目的：如果支持动态数据认证，卡中不含有DDOL且终端中的缺省DDOL不请求不可预知数，终端动态数据认证失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’)；
——卡中没有DDOL；
——终端缺省DDOL不请求不可预知数（‘9F37’） 。

测试流程：选择卡片应用，执行交易（特别是动态数据认证)。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’(DDA失败)。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA)。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中TSI的字节1，位8为‘1’（脱机数据认证已完成)。

7.18.144 SM-AQFM079-00 数字签名的验证

测试目的：确保终端能够按照JR/T0025.7—2013 5.3.5的要求执行动态数据认证，验证签名动态应用数据。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’)；
——卡计算的签名的动态应用数据是正确的；
——发卡行公钥证书有效；
——IC卡公钥证书有效。

测试流程：选择卡片应用，执行交易（特别是动态数据认证)。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（DDA成功)。第一个GENERATE AC命令中TVR的字节1，位3为‘0’（未使用CDA)。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成)。

7.18.145 SM-AQFM082-00 签名的数据格式不等于'15'

测试目的：如果从签名的动态应用数据中得到的证书格式不等于‘15’，终端将动态数据认证失败。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡中签名动态应用数据不是使用‘15’的证书格式计算得到。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.146 SM-AQFM083-00 签名的动态数据中的数字签名不正确

测试目的：如果计算得到的签名结果与从签名的动态应用数据中的签名结果不相等，终端动态数据认证失败。
终端配置：支持DDA。
卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；
——卡中签名动态应用数据使用错误的签名数据计算得到。
子类案例：——案例01：签名数据r的第11个字节出错；
——案例02：签名数据r的第1个字节出错；
——案例03：签名数据r的最后一个字节出错；
——案例04：签名数据s的第11个字节出错；
——案例05：签名数据s的第1个字节出错；
——案例06：签名数据s的最后一个字节出错。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.147 SM-AQFM085-00 在动态数据认证中的 SDA 标签列表（1）

测试目的：执行DDA时，确保终端的SDA标签列表仅含有AIP。
终端配置：支持DDA。
卡片配置：卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）。
子类案例：——案例01：SDA包含AFL以及用此 AFL值计算签名；
——案例02：SDA包含AFL和AIP以及用此 AFL值和AIP值计算签名。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4为‘1’（DDA失败）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.148 SM-AQFM085-01 在动态数据认证中的 SDA 标签列表（2）

测试目的：执行CDA时，确保终端的SDA标签列表仅含有AIP。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端；
——终端行为分析前有能力探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位6为‘1’）；
——通过设置TAC和IAC，终端第一个GAC请求TC。
子类案例：——案例01：SDA包含AFL以及用此 AFL值计算签名；
——案例02：SDA包含AFL和AIP以及用此 AFL值和AIP值计算签名。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端在GAC时不应该请求CDA。终端完成交易，通过TAC和IAC的设置请求TC。第一个GENERATE AC命令中TVR的字节1,位3为‘1’(CDA失败)。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA)。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成)。

7.18.149 SM-AQFM085-02 在动态数据认证中的 SDA 标签列表（3）

测试目的：执行DDA时，确保终端的SDA标签列表仅含有AIP。
终端配置：支持DDA。
卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’)；
——SDA标签列标包含AIP。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中)。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（DDA成功)。第一个GENERATE AC命令中TVR的字节1，位3为‘0’（未使用CDA)。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成)。

7.18.150 SM-AQFM085-03 在动态数据认证中的 SDA 标签列表（4）

测试目的：执行CDA时，确保终端的SDA标签列表仅含有AIP。
终端配置：支持CDA。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’)；
——SDA标签列表包含AIP。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中)。
通过标准：终端应通过请求一个TC或AAC来完成交易。金融确认报文或批数据采集报文中的TVR的字节1，位3 为‘0’（CDA成功)。第一个GENERATE AC命令中TVR的字节1，位7 为 ‘0’（未使用SDA)。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA)。金融确认报文或批数据采集报文中的TSI的字节1，位8 为‘1’(脱机数据认证已完成)（该通过标准仅应用于假如终端请求CDA)。

7.18.151 SM-AQFM085-04 在动态数据认证中的 SDA 标签列表（5）

测试目的：执行CDA时，确保终端的SDA标签列表仅含有AIP。
终端配置：——支持CDA;
——仅脱机终端或有联机能力的脱机终端;
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’)；
——通过设置TAC和IAC，终端第一个GAC请求TC。
子类案例：——案例01：SDA包含AFL以及用此 AFL值计算签名;
——案例02：SDA包含AFL和AIP以及用此 AFL值和AIP值计算签名。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中)。
通过标准：终端拒绝交易并且不执行2nd GAC当卡返回TC时，或者拒绝交易通过执行2nd GAC请求AAC当卡在1st GAC时返回ARQC。TVR字节1，位3 为‘1’（CDA失败）包含在第二个 GAC或者金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA)。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在第二个 GAC或者金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.152 SM-AQFM085-05 在动态数据认证中的SDA标签列表（6）

测试目的：执行CDA时，确保终端的SDA标签列表仅含有AIP。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——通过设置TAC和IAC，终端第一个GAC请求ARQC，第二个GAC请求TC。
子类案例：——案例01：SDA包含AFL以及用此 AFL值计算签名；
——案例02：SDA包含AFL和AIP以及用此 AFL值和AIP值计算签名。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应该通过第二个GAC请求AAC拒绝交易。第二个GENERATE AC命令中TVR的字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI的字节1，位8 为‘1’（脱机数据认证未完成）。

7.18.153 SM-AQFM085-06 在动态数据认证中的SDA标签列表（7）

测试目的：执行CDA时，确保终端的SDA标签列表仅含有AIP。
终端配置：——支持CDA；
——仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一次GAC时返回ARQC；
——通过设置TAC和IAC，终端第一个GAC请求ARQC，第二个GAC请求TC；
——发卡行批准交易。
子类案例：——案例01：SDA包含AFL以及用此 AFL值计算签名；
——案例02：SDA包含AFL和AIP以及用此 AFL值和AIP值计算签名。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.154 SM-AQFM085-07 在动态数据认证中的SDA标签列表（8）

测试目的：执行CDA时，确保终端的SDA标签列表仅含有AIP。
终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——CDA从不请求，第一个GAC请求ARQC时；
——当不能联机时，正常处理缺省行为码；
——终端行为分析前不能探测到CDA失败。
卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一次GAC时返回ARQC；

——通过设置TAC和IAC，终端第一个GAC请求ARQC，第二个GAC请求TC。

子类案例：——案例01：SDA包含AFL以及用此 AFL值计算签名；

——案例02：SDA包含AFL和AIP以及用此 AFL值和AIP值计算签名。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TVR值。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝或是终止交易）或者终端能通过其他方式如凭条显示TSI值。

7.18.155 SM-AQFM085-08 在动态数据认证中的 SDA 标签列表（9）

测试目的：执行CDA时，确保终端的SDA标签列表仅含有AIP。

终端配置：——支持CDA；

——仅联机终端或有联机能力的脱机终端；

——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——交易联机接受；

——通过设置TAC和IAC，终端第一个GAC请求ARQC。

子类案例：——案例01：SDA包含AFL以及用此 AFL值计算签名；

——案例02：SDA包含AFL和AIP以及用此 AFL值和AIP值计算签名。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端在1st GAC和2nd GAC时不应该请求CDA。终端应通过请求一个TC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中TVR的字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.156 SM-AQFM085-09 在动态数据认证中的 SDA 标签列表（10）

测试目的：执行CDA时，确保终端的SDA标签列表仅含有AIP。

终端配置：——支持CDA；

——仅联机终端或有联机能力的脱机终端；

——终端行为分析前有能力探测到CDA失败。

卡片配置：——卡的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——通过设置TAC和IAC，终端第一个GAC请求ARQC；

——交易联机拒绝。

子类案例：——案例01：SDA包含AFL以及用此 AFL值计算签名；

——案例02：SDA包含AFL和AIP以及用此 AFL值和AIP值计算签名。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端在1st GAC和2nd GAC时不应该请求CDA。终端应通过请求一个AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中TVR的字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.157 SM-AQFM086-00 储存在 IC 卡中的动态数据

测试目的：在动态数据认证过程中，终端包含标签为‘9F4C’的动态数字。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；

——CDOL1请求IC卡动态数字（标签为‘9F4C’）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC命令中TVR的字节1，位3为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。标签为‘9F4C’的值和在DDA过程中使用的应相同（在第一个GENERATE AC中收到）。

7.18.158 SM-AQFM086-01 IC卡中的动态数据（1）

测试目的：在动态数据认证过程中，终端支持IC卡动态数据包含长度（2-8字节）的值和可选的附加动态数据，总长度在LDD≦Nic-25。

终端配置：支持DDA。

卡片配置：——卡的AIP指明支持动态数据认证（AIP的字节1，位6为‘1’）；

——CDOL1请求IC卡动态数字（标签为‘9F4C’）；

——NIC长度=247字节，NI长度=247长度，NCA长度=248长度。

子类案例：——案例01：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=2）不包含附加动态数据（LDD=3）；

——案例02：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）不包含附加动态数据（LDD=9）；

——案例03：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=213字节，值=AA--AA）,没有填充（LDD=222）；

——案例04：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=2）+附加动态数据（长度=219字节，值=AA--AA）,没有填充（LDD=222）；

——案例05：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=4字节，值=12345678）（LDD=9）；

——案例06：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=9字节，值=112233445566778FFF）（LDD=14）；

——案例07：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=8字节，值=TLV所有的标签数据5F508104AABBCCDD）（LDD=17）；

——案例08：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=4字节，值=1234BBBB）（LDD=9）；

——案例09：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=6字节，值=TLV“失效数据”数据：“5F2403400101”）（LDD=15）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个TC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TSI的字节1，位8 为‘1’（脱机数据认证已完成）。标签为‘9F4C’的值和在DDA过程中使用的应相同（在第一个GENERATE AC中收到）。

7.18.159 SM-AQFM086-02 IC卡中的动态数据（2）

测试目的：在动态数据认证过程中，终端支持IC卡动态数据包含长度（2-8字节）的值和可选的附加动态数据，总长度在LDD≦Nic-25。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡的AIP指明CDA（AIP的字节1，位1为‘1’）；
——终端通过IAC和TAC的设置在第一个GAC时请求TC；
——卡在第一个GAC时返回TC；
——NIC长度=238字节，NI长度=247长度，NCA长度=248长度。
子类案例：——案例01：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=2）不包含附加动态数据（LDD=32）；
——案例02：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）不包含附加动态数据（LDD=38）；
——案例03：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=175字节，值=AA--AA）,没有填充（LDD=213）；
——案例04：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=2）+附加动态数据（长度=181字节，值=AA--AA）,没有填充（LDD=213）；
——案例05：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=4字节，值=12345678）（LDD=38）；
——案例06：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=9字节，值=112233445566778FFF）（LDD=43）；
——案例07：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=8字节，值=TLV所有的标签数据5F508104AABBCCDD）（LDD=46）；
——案例08：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=4字节，值=1234BBBB）（LDD=38）；
——案例09：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=6字节，值=TLV“失效数据”数据：“5F2403400101”）（LDD=44）。
测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。
通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。TVR的字节1，位3 为‘0’（CDA成功）包含在金融确认报文或者批上送报文。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。TSI的字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或者批上送报文。

7.18.160 SM-AQFM086-03 IC卡中的动态数据（3）

测试目的：在动态数据认证过程中，终端支持IC卡动态数据包含长度（2-8字节）的值和可选的附加动态数据，总长度在LDD≦Nic-25。
终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——CDA总是请求，第一个GAC请求ARQC时。
卡片配置：——卡的AIP指明支持CDA （AIP的字节1，位1为‘1’）；
——终端通过IAC和TAC的设置在第一个GAC时请求ARQC；
——卡在第一个GAC时返回ARQC；
——CDOL2请求IC卡动态数字（标签为‘9F4C’）；
——NIC长度=238字节，NI长度=247长度，NCA长度=248长度。
子类案例：——案例01：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=2）不包含附加动态数据（LDD=32）；

——案例02：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）不包含附加动态数据（LDD=38）；
——案例03：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=175字节，值=AA--AA）,没有填充（LDD=213）；
——案例04：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=2）+附加动态数据（长度=181字节，值=AA--AA）,没有填充（LDD=213）；
——案例05：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=4字节，值=12345678）（LDD=38）；
——案例06：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=9字节，值=112233445566778FFF）（LDD=43）；
——案例07：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=8字节，值=TLV所有的标签数据5F508104AABBCCDD）（LDD=46）；
——案例08：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=4字节，值=1234BBBB）（LDD=38）；
——案例09：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=6字节，值=TLV“失效数据”数据：“5F2403400101”）（LDD=44）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC命令中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。TSI的字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或者批上送报文。在第二个GENERATE AC中收到标签为‘9F4C’的值和在动态签名使用的应相同。

7.18.161 SM-AQFM086-04 IC卡中的动态数据（4）

测试目的：在动态数据认证过程中，终端支持IC卡动态数据包含长度（2-8字节）的值和可选的附加动态数据，总长度在LDD≦Nic-25。

终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡的AIP指明支持CDA （AIP的字节1，位1为‘1’）；
——终端通过IAC和TAC的设置在第一个GAC时请求ARQC, 第二个GAC时请求TC；
——卡在第一个GAC时返回ARQC；
——CDOL2请求IC卡动态数字（标签为‘9F4C’）；
——NIC长度=238字节，NI长度=247长度，NCA长度=248长度。

子类案例：——案例01：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=2）不包含附加动态数据（LDD=32）；
——案例02：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）不包含附加动态数据（LDD=38）；
——案例03：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=175字节，值=AA--AA）,没有填充（LDD=213）；

——案例04：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=2）+附加动态数据（长度=181字节，值=AA--AA）,没有填充（LDD=213）；
——案例05：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=4字节，值=12345678）（LDD=38）；
——案例06：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+ 附加动态数据（长度=9字节，值=112233445566778FFF）（LDD=43）；
——案例07：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=8字节，值=TLV所有的标签数据5F508104AABBCCDD）（LDD=46）；
——案例08：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=4）+附加动态数据（长度=4字节，值=1234BBBB）（LDD=38）；
——案例09：被用在动态签名计算的IC卡动态数据=IC卡动态数字（长度=8）+附加动态数据（长度=6字节，值=TLV“失效数据”数据：“5F2403400101”）（LDD=44）。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个TC或AAC来完成交易。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。TVR的字节1，位3 为‘0’（CDA成功）包含在金融确认报文或者批上送报文。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。TSI的字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或者批上送报文。

7.18.162 SM-AQFM119-00 在复合动态数据认证中的 PDOL

测试目的：确保在复合动态数据认证中可以使用PDOL。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——通过设置TAC和IAC，终端在第一次GAC请求TC。

子类案例：——案例01：卡中存在PDOL；
——案例02：卡中的PDOL是空的；
——案例03：卡中没有PDOL。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个TC来完成交易。在金融确认报文或批数据采集报文中的TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4为‘0’（未使用DDA）。在金融确认报文或批数据采集报文中的TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.163 SM-AQFM119-01 在复合动态数据认证中的 PDOL

测试目的：确保在复合动态数据认证中可以使用PDOL。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——通过设置TAC和IAC，终端在第一次GAC请求ARQC。

子类案例：——案例01：卡中存在PDOL；
——案例02：卡中的PDOL是空的；
——案例03：卡中没有PDOL。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个TC或 AAC来完成交易。在金融确认报文或批数据采集报文中的TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4为‘0’（未使用DDA）。在金融确认报文或批数据采集报文中的TSI的字节1，位8 为‘1’（脱机数据认证已完成）。

7.18.164 SM-AQFM122-00 响应 AAC 为格式 1 或格式 2（1）

测试目的：——终端执行CDA时，若卡片在GENERATE AC命令中返回AAC，则终端可以接受卡片返回的格式1或格式2的数据；
——若卡片返回AAC，确保终端设置TVR‘复合动态数据认证失败’位为1。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求TC；
——卡中的AIP指明支持CDA （AIP的字节1，位1为1）。

子类案例：——案例01：第一个GENERATE AC命令，卡片以格式1返回AAC；
——案例02：第一个GENERATE AC命令，卡片以格式2返回AAC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于有存储拒绝交易能力的终端： TSI的字节1，位8 为‘1’（脱机数据认证已完成）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.165 SM-AQFM122-01 响应 AAC 为格式 1 或格式 2（2）

测试目的：——终端执行CDA时，若卡片在GENERATE AC命令中返回AAC，则终端可以接受卡片返回的格式1或格式2的数据；
——若卡片返回AAC，确保终端设置TVR复合动态数据认证失败’位为1。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求TC；
——卡中的AIP指明支持CDA （AIP的字节1，位1为‘1’）；
——卡在第一次GAC时返回ARQC。

子类案例：——案例01：第一个GENERATE AC命令，卡片以格式1返回AAC；
——案例02：第一个GENERATE AC命令，卡片以格式2返回AAC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于有存储拒绝交易能力的终端：TSI的字节1，位8 为‘1’（脱机数据认证已完成）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.166 SM-AQFM122-02 IC 卡响应 AAR（1）

测试目的：即使在CDA的过程中，确保终端将AAR视为逻辑错误并终止交易（当动态签名不存在的情况）。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求TC；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC 中卡响应无数据签名的AAR。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应终止交易。

7.18.167 SM-AQFM122-03 IC卡响应AAR（2）

测试目的：即使在CDA的过程中，确保终端将AAR视为逻辑错误并终止交易（当动态签名存在的情况）。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求TC；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC 中卡响应有数据签名的AAR。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应终止交易。

7.18.168 SM-AQFM122-04 响应AAC为格式1或格式2（3）

测试目的：——终端执行CDA时，若卡片在GENERATE AC命令中返回AAC，则终端可以接受卡片返回的格式1或格式2的数据；
——若卡片返回AAC，确保终端设置TVR复合动态数据认证失败’位为1。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求ARQC；
——卡中的AIP指明支持CDA （AIP的字节1，位1为‘1’）。

子类案例：——案例01：第一个GENERATE AC命令，卡片以格式1返回AAC；
——案例02：第一个GENERATE AC命令，卡片以格式2返回AAC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于有存储拒绝交易能力的终端：TSI的字节1，位8 为‘1’（脱机数据认证已完成）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.169 SM-AQFM122-05 响应AAC为格式1或格式2（4）

测试目的：——终端执行CDA时，若卡片在GENERATE AC命令中返回AAC，则终端可以接受卡片返回的格式1或格式2的数据；
——若卡片返回AAC，确保终端设置TVR复合动态数据认证失败’位为1。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求ARQC；
——卡中的AIP指明支持CDA （AIP的字节1，位1为‘1’）；
——卡在第一个GAC中返回ARQC。

子类案例：——案例01：第一个GENERATE AC命令，卡片以格式1返回AAC；
——案例02：第一个GENERATE AC命令，卡片以格式2返回AAC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于有存储拒绝交易能力的终端：TSI的字节1，位8 为‘1’（脱机数据认证已完成）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.170 SM-AQFM122-06 IC卡响应AAR（3）

测试目的：即使在CDA的过程中，确保终端将AAR视为逻辑错误并终止交易（当动态签名存在的情况）。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。
卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求ARQC；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC 中卡响应有不包含数据签名的AAR。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应终止交易。

7.18.171 SM-AQFM122-07 IC卡响应AAR（4）

测试目的：即使在CDA的过程中，确保终端将AAR视为逻辑错误并终止交易（当动态签名存在的情况）。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。
卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求ARQC；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——在第一个GENERATE AC 中卡响应有数据签名的AAR。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应终止交易。

7.18.172 SM-AQFM122-08 响应AAC为格式1或格式2（5）

测试目的：终端执行CDA时，若卡片在GENERATE AC命令中返回AAC，则终端可以接受卡片返回的格式1或格式2的数据。
终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码；
——CDA从不请求，第一个GAC请求ARQC时。
卡片配置：——通过设置TAC和IAC，终端在第一次GAC请求ARQC；
——卡中的AIP指明支持CDA （AIP的字节1，位1为‘1’）；
——卡在第一个GAC中返回ARQC。
子类案例：——案例01：第二个GENERATE AC命令，卡片以格式1返回AAC；
——案例02：第二个GENERATE AC命令，卡片以格式2返回AAC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端将进行交易直至结束。交易被拒绝。该通过标准仅适用于包含金融确认报文或是批上送报文的有存储拒绝交易能力的终端：TSI的字节1，位8 为‘1’（脱机数据认证已完成）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.173 SM-AQFM126-00 签名的数据格式不等于‘15’（1）

测试目的：确保终端在复合动态数据认证过程中对数据签名格式进行检查。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——签名的数据格式不是‘15’；
——通过设置TAC和IAC，终端在第一次GAC请求TC。
子类案例：——案例01：卡在第一次GAC响应TC；
——案例02：卡在第一次GAC响应ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：案例01：终端拒绝交易不应该执行第二个GAC。案例02：终端完成交易应该立即执行第二个GAC请求AAC。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.174 SM-AQFM126-01 签名的数据格式不等于‘15’（2）

测试目的：确保终端在复合动态数据认证过程中对数据签名格式进行检查。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——签名的数据格式不是‘15’；
——通过设置TAC和IAC，终端在第一次GAC请求ARQC；
——卡在第一次GAC响应ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端完成交易通过立即执行第二个GAC请求AAC。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.175 SM-AQFM126-02 签名的数据格式不等于‘15’（3）

测试目的：确保终端在复合动态数据认证过程中对数据签名格式进行检查。

终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——在第二个GAC，签名的数据格式不是‘15’；
——通过设置TAC和IAC，终端在第一次GAC请求ARQC，在第二次GAC请求TC；
——卡在第一次GAC响应ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝交易)。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已进行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.176 SM-AQFM126-03 签名的数据格式不等于‘15’（4）

测试目的：确保终端在复合动态数据认证过程中对数据签名格式进行检查。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；

——在第二个GAC，签名的数据格式不是‘15’；
——通过设置TAC和IAC，终端在第一次GAC请求ARQC，在第二次GAC请求TC；
——卡在第一次GAC响应ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝交易)。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA)。TSI字节1，位8 为‘1’（脱机数据认证已进行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.177 SM-AQFM127-00 动态签名中 CID 与从 GENERATE AC 中获取的 CID 不一致（1）

测试目的：确保终端检查在复合动态数据认证过程恢复得到的CID和GENERATE AC命令返回的CID是否相同。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’)；
——设置TAC和IAC使终端的第一个GENERATE AC命令请求TC；
——卡片在第一个GAC返回TC；
——签名数据中的CID为ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端完成交易通过立即执行第二个GAC请求AAC。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易)。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA)。TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.178 SM-AQFM127-01 动态签名中 CID 与从 GENERATE AC 中获取的 CID 不一致（2）

测试目的：确保终端检查在复合动态数据认证过程恢复得到的CID和GENERATE AC命令返回的CID是否相同。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’)；
——设置TAC和IAC使终端在第一个GENERATE AC中请求一个TC；
——卡在第一个GAC响应ARQC；
——签名数据中的CID是TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易不应该执行第二个GAC。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝交易)。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA)。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA)。
TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.179 SM-AQFM127-02 动态签名中 CID 与从 GENERATE AC 中获取的 CID 不一致（3）

测试目的：确保终端检查在复合动态数据认证过程恢复得到的CID和GENERATE AC命令返回的CID是否相同。

终端配置：——支持CDA；
——仅联机终端；

——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENERATE AC中请求一个ARQC；
——卡在第一个GAC响应ARQC；
——签名数据中的CID是TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端拒绝交易不应该执行第二个GAC。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。
TSI字节1，位8 为‘1’（脱机数据认证已完成）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.180 SM-AQFM128-00 签名的复合动态数据中的数字签名不正确（1）

测试目的：确保终端在复合动态数据认证中比较哈希结果。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——哈希结果是错误的；
——设置TAC和IAC使终端在第一个GENERATE AC中请求一个TC。

子类案例：——案例01：卡在第一个GAC响应TC；
——案例02：卡在第一个GAC响应ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：案例01：终端拒绝交易不应该执行第二个GAC。案例02：终端完成交易应该立即执行第二个GAC请求AAC。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.181 SM-AQFM128-01 签名的复合动态数据中的数字签名不正确（2）

测试目的：确保终端在复合动态数据认证中比较哈希结果。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——哈希结果是错误的；
——设置TAC和IAC使终端在第一个GENERATE AC中请求一个ARQC；
——卡在第一个GAC响应ARQC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端完成交易通过立即执行第二个GAC请求AAC。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 =‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.182 SM-AQFM128-02 签名的复合动态数据中的数字签名不正确（3）

测试目的：确保终端在复合动态数据认证中比较哈希结果。

终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——在第二个GAC,哈希结果是错误的；
——设置TAC和IAC使终端在第一个GAC中请求ARQC，在第二个GAC中请求TC；
——卡在第一个GAC响应ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝交易)。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 =‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.183 SM-AQFM128-03 签名的复合动态数据中的数字签名不正确（4）

测试目的：确保终端在复合动态数据认证中比较哈希结果。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——在第二个GAC响应中,哈希结果是错误的；
——设置TAC和IAC使终端在第一个GAC中请求ARQC，在第二个GAC中请求TC；
——卡在第一个GAC响应ARQC；
——发卡行批准交易。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文(该通过标准仅用于终端有能力保存拒绝交易)。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.184 SM-AQFM129-00 比较交易数据哈希码（1）

测试目的：确保终端在复合动态数据认证中比较交易数据哈希值。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——哈希数据结果是错误的；
——设置TAC和IAC使终端在第一个GAC中请求TC。
子类案例：——案例01：卡在第一个GAC响应TC；
——案例02：卡在第一个GAC响应ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：案例01：终端拒绝交易不应该执行第二个GAC。案例02：终端完成交易应该立即执行第二个GAC请求AAC。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过

标准仅用于终端有能力保存拒绝交易）。

7.18.185 SM-AQFM129-01 比较交易数据哈希码（2）

测试目的：确保终端在复合动态数据认证中比较交易数据哈希值。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——哈希数据结果是错误的；
——设置TAC和IAC使终端在第一个GAC中请求ARQC；
——卡在第一个GAC响应ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端完成交易通过立即执行第二个GAC请求AAC。第二个GENERATE AC命令中的TVR字节1，位3 为‘1’（CDA失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。第二个GENERATE AC命令中的TSI字节1，位8 为‘1’（脱机数据认证已执行）。

7.18.186 SM-AQFM129-02 比较交易数据哈希码（3）

测试目的：确保终端在复合动态数据认证中比较交易数据哈希值。
终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——在第二个GAC返回哈希数据结果是错误的；
——设置TAC和IAC使终端在第一个GAC中请求ARQC，在第二个GAC中请求TC；
——卡在第一个GAC响应ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.187 SM-AQFM129-03 比较交易数据哈希码（4）

测试目的：确保终端在复合动态数据认证中比较交易数据哈希值。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——在第二个GAC返回哈希数据结果是错误的；
——设置TAC和IAC使终端在第一个GAC中请求ARQC，在第二个GAC中请求TC；
——卡在第一个GAC响应ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端拒绝交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认

证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.188 SM-AQFM130-00 在复合动态数据认证中的发卡行应用数据（1）

测试目的：确保终端复合动态数据认证中可以使用发卡行应用数据。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GAC中请求TC；
——卡对第一个GENERATE AC的响应是ARQC，第二个GENERATE AC的响应是TC；
——第一个GENERATE AC命令的响应中存在发卡行应用数据。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。第二个GENERATE AC命令中字节1，位3 为‘0’（复合动态数据执行成功）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。金融确认报文或批数据采集报文中TSI的字节1，位8 为‘1’（脱机数据认证已执行）。

7.18.189 SM-AQFM130-01 在复合动态数据认证中的发卡行应用数据（2）

测试目的：确保终端在复合动态数据认证中可以使用发卡行应用数据。
终端配置：——支持CDA；
——终端不能联机；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——设置TAC和IAC使终端在第一个GAC中请求TC，在第二个GAC中请求TC；
——卡中的AIP指明支持复合动态数据认证（AIP的第1个字节，位1为‘1’）；
——卡对第一个GENERATE AC的响应是ARQC，对第二个GENERATE AC的响应是TC；
——第二个GENERATE AC命令的响应中存在发卡行应用数据。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。TVR，TSI（包含在金融确认信息或批数据获取信息中或是其他中应该：-TVR的字节1，位3 为‘0’（CDA成功）。-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.190 SM-AQFM130-02 在复合动态数据认证中的发卡行应用数据（3）

测试目的：确保终端复合动态数据认证中可以使用发卡行应用数据。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GAC中请求ARQC；
——卡对第一个GENERATE AC的响应是ARQC，第二个GENERATE AC的响应是TC；
——第一个GENERATE AC命令的响应中存在发卡行应用数据。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。第二个GENERATE AC命令中字节1，位3 为‘0’（复合动态数据执行成功）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。金融确认报文或批数据采集报文中TSI的字节1，位8 为‘1’（脱机数据认证已执行）。

7.18.191 SM-AQFM130-03 在复合动态数据认证中的发卡行应用数据（4）

测试目的：确保终端在复合动态数据认证中可以使用发卡行应用数据。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。
卡片配置：——设置TAC和IAC使终端在第一个GAC中请求ARQC；
——卡中的AIP指明支持复合动态数据认证（AIP的第1个字节，位1为‘1’）；
——卡对第一个GENERATE AC的响应是ARQC，对第二个GENERATE AC的响应是TC；
——第二个GENERATE AC命令的响应中存在发卡行应用数据。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。TVR，TSI（包含在金融确认信息或批数据获取信息中或是其他中应该：-TVR的字节1，位3 为‘0’（CDA成功）。-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.192 SM-AQFM130-04 在复合动态数据认证中的发卡行应用数据（5）

测试目的：确保终端在复合动态数据认证中可以使用发卡行应用数据。
终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。
卡片配置：——设置TAC和IAC使终端在第一个GAC中请求ARQC, 在第二个GAC中请求TC；
——卡中的AIP指明支持复合动态数据认证（AIP的第1个字节，位1为‘1’）；
——卡对第一个GENERATE AC的响应是ARQC，对第二个GENERATE AC的响应是TC；
——第二个GENERATE AC命令的响应中存在发卡行应用数据。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。TVR，TSI（包含在金融确认信息或批数据获取信息中或是其他中应该：-TVR的字节1，位3 为‘0’（CDA成功）。-TSI的字节1，位8 =‘1’（脱机数据认证已执行）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.193 SM-AQFM131-00 储存的 IC 卡动态数字（1）

测试目的：确保在复合动态数据认证中，终端在标签‘9F4C’中存储IC卡动态数字。
终端配置：——支持CDA；
——终端不能联机；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——CDOL2请求IC卡动态数字（标签为‘9F4C’）；
——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GAC中请求TC；
——卡第一个GENERATE AC的响应是ARQC，第二个GENERATE AC的响应是TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。第二个GENERATE AC命令中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。储存在标签‘9F4C’中的IC卡动态数字与在复合动态数据认证的第2个ENERATE AC命令

中收到的一致。TVR，TSI（包含在金融确认报文或批上送数据报文中或是其他中）有：-TVR的字节1，位3 为‘0’（CDA成功）。-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。

7.18.194 SM-AQFM131-01 储存的 IC 卡动态数字（2）

测试目的：确保在复合动态数据认证中，终端在标签‘9F4C’中存储IC卡动态数字。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时 或 CDA总是请求，在第二个GAC请求TC时。
卡片配置：——CDOL2请求IC卡动态数字（标签为‘9F4C’）；
——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GAC中请求ARQC；
——卡第一个GENERATE AC的响应是ARQC，第二个GENERATE AC的响应是TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应完成交易。第二个GENERATE AC命令中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。TVR，TSI 和 IC卡动态数字 （包含在金融确认报文或批上送数据报文中或是其他中）有：-TVR的字节1，位3 为‘0’（CDA成功）。-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。-存储在‘9F4C’中的IC卡动态数同在复合动态数据认证中使用的一样。

7.18.195 SM-AQFM133-00 终端产生的不可预测数

测试目的：确保在复合动态数据认证中，对于不同交易终端产生一个不同的随机数。
终端配置：支持CDA。
卡片配置：——CDOL1和CDOL2中包含有终端产生的不可预知数（标签为‘9F37’）；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）。
测试流程：至少进行三个交易。比较由终端产生的不可预知数的值。
通过标准：终端应通过请求一个TC或AAC来完成交易。在金融确认报文中或是批上送数据报文中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。金融确认报文或批上送数据报文中TSI的字节1，位8 为‘1’（脱机数据认证已执行）（该通过标准仅用于CDA被请求）。比较本次交易和上次交易中标签为‘9F37’的数据。它们应不同。

7.18.196 SM-AQFM133-01 CDOL 中不包含不可预测数（1）

测试目的：确保在复合动态数据认证中，终端不会校验CDOL1和CDOL2中是否存在不可预测数。
终端配置：支持CDA。
卡片配置：——CDOL1和CDOL2中不包含有终端产生的不可预知数（标签为‘9F37’）；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应通过请求一个TC或AAC来完成交易。TVR字节1，位3 为‘1’（CDA失败）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易并且CDA被请求）。第一个GENERATE AC命令中的TVR字节1，位3 为‘0’（CDA未失败）。第一个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）第一个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。TSI字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易并且CDA被请求）。

7.18.197 SM-AQFM133-02 CDOL 中不包含不可预测数（2）

测试目的：确保在CDOL1和CDOL2中不含有9F37而且不执行CDA时，终端能够忽略9F37的不存在并且继续完成交易，在联机交易中CDA不会失败。

终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——CDA从不请求，第一个GAC请求ARQC时；
——CDA从不请求，在第二个GAC请求TC时。

卡片配置：——CDOL1和CDOL2中不包含有终端产生的不可预知数（标签为‘9F37’）；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GAC中请求ARQC，在第二个GAC中请求TC；
——卡在第一个GAC中响应ARQC；
——发卡行批准交易。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个TC来完成交易。第一个和第二个GENERATE AC命令中的TVR字节1，位3 为‘0’（未使用CDA）。第一个和第二个GENERATE AC命令中的TVR字节1，位7 为‘0’（未使用SDA）。第一个和第二个GENERATE AC命令中的TVR字节1，位4 为‘0’（未使用DDA）。

7.18.198 SM-AQFM134-00 以格式 2 的 TC 或者 ARQC 响应 GENERATE AC （1）

测试目的：——确保终端在CDA中可以使用IC卡响应格式2；
——确保终端在标签‘9F26’中存储用于复合动态数据认证的应用密文。

终端配置：——支持CDA；
——终端不能联机；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡以格式2响应GENERATE AC；
——设置TAC和IAC使终端在第一个GAC中请求TC，在第二个GAC中请求TC。

子类案例：——案例01：卡在第一个GENERATE AC响应一个TC；
——案例03：卡在第一个GENERATE AC响应ARQC，在第2个GENERATE AC响应TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个TC来完成交易。金融确认报文或批上送数据报文信息中TVR的字节1，位3 为‘0’（CDA成功）。金融确认报文或批上送数据报文信息中TSI的字节1，位8 为‘1’（脱机数据认证已执行）。金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.199 SM-AQFM134-01 以不是格式 2 的 TC 或者 ARQC 响应 GENERATE AC （隐含的）（1）

测试目的：确保在执行复合动态数据认证，卡片响应TC或ARQC时，终端不使用格式1的响应。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）。

子类案例：——案例01：IAC和TAC设置使得终端在第一个GENERATE AC请求TC，卡使用格式1编码响应TC；
——案例02：IAC和TAC设置使得终端在第一个GENERATE AC请求TC，卡以格式1编码响应ARQC；
——案例03：IAC和TAC设置使得终端在第一个GENERATE AC请求TC，在第二

个GENERATE AC请求TC，卡片在第一个GENERATE AC以格式2编码响应ARQC，卡片在第二个GENERATE AC以格式1编码响应TC，终端不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端拒绝或终止交易。案例03：终端应拒绝或终止交易。TSI字节1，位8为‘1’（脱机数据认证已执行）包含在金融确认报文或是批上送报文（该通过标准仅用于终端有能力保存拒绝交易）。

7.18.200 SM-AQFM134-03 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（1）

测试目的：确保在CDA中，终端不支持以TC格式的响应AAC（使用AAC生成签名）。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GAC中请求TC。

子类案例：——案例01：第一个GENERATE AC命令，卡片返回格式2含数字签名的AAC（同返回TC的过程一样）；
——案例02：卡第一个GAC返回ARQC，第二个GENERATE AC命令，卡片返回格式2含数字签名的AAC（同返回TC的过程一样）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端拒绝交易。通过标准仅适用在终端存储拒绝交易的情况下：TVR的字节1，位3为‘0’（CDA未失败）。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.201 SM-AQFM134-04 GENERATE AC 命令中复合动态数据认证参考控制参数（1）

测试目的：确保GENERATE AC命令中的参考控制参数请求复合动态数据认证。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端处理交易到完成。P1 =参考控制参数 （50 - TC）。

7.18.202 SM-AQFM134-05 以格式 2 的 TC 或者 ARQC 响应 GENERATE AC （2）

测试目的：——确保终端在CDA中可以使用IC卡响应格式2；
——确保终端在标签‘9F26’中存储用于复合动态数据认证的应用密文。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡以格式2响应GENERATE AC；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC。

子类案例：——案例01：卡响应一个ARQC；
——案例02：卡在第1个GAC响应ARQC，在第2个GAC响应TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个TC来完成交易。金融确认报文或批上送数据报文信息中TVR的字节1，位3 为‘0’（CDA成功）。金融确认报文或批上送数据报文信息中TSI的字节1，位8 为‘1’ （脱机数据认证已执行）。金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证

使用的一样。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.203 SM-AQFM134-06 以不是格式 1 的 TC 或者 ARQC 响应 GENERATE AC （隐含的）（2）

测试目的：确保在执行复合动态数据认证，卡片响应TC或ARQC时，终端不使用格式1的响应。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）。

子类案例：——案例01：IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC；卡使用格式1编码响应TC；
——案例02：IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC，在第二个GENERATE AC请求TC,卡对第一个GAC以格式2编码响应ARQC,对第二个GAC以格式1编码响应TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端拒绝或终止交易。本通过标准只在终端能存储被拒绝的交易情况下适用：TSI的字节1，位8 =‘1’（脱机数据认证已执行），应包含在金融确认报文或批上送数据报文信息中。

7.18.204 SM-AQFM134-07 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（2）

测试目的：确保在CDA中，终端不支持以TC格式的响应AAC（使用AAC生成签名）。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC。

子类案例：——案例01：第一个GENERATE AC命令，卡片返回格式2含数字签名的AAC（同返回TC的过程一样）；
——案例02：第二个GENERATE AC命令，卡片返回格式2含数字签名的AAC（同返回TC的过程一样）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应通过请求一个AAC来完成交易。交易应被拒绝。通过标准仅适用在终端存储拒绝交易的情况下：TVR的字节1，位3为‘1’（CDA失败），应包含在金融确认报文或批上送数据报文信息中。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.205 SM-AQFM134-08 GENERATE AC 命令中复合动态数据认证参考控制参数（2）

测试目的：确保GENERATE AC命令中的参考控制参数请求复合动态数据认证。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，第二个GENERATE AC请求TC；
——发卡行批准交易。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端处理交易到完成。第一个GAC，P1 90 –ARQC。第二个GAC，P1 50 – TC

（当不支持CDA的GAC2 TC，P1为‘40’）。

7.18.206 SM-AQFM134-09 以格式 2 的 TC 或者 ARQC 响应 GENERATE AC （3）

测试目的：——确保终端在CDA中可以使用IC卡响应格式2；
——确保终端在标签‘9F26’中存储用于复合动态数据认证的应用密文。

终端配置：——支持CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡以格式2响应GENERATE AC；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，第二个GENERATE AC请求TC。

子类案例：——案例01：卡在第一个GENERATE AC响应一个ARQC；
——案例02：卡在第2个GENERATE AC响应一个TC，终端不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。

通过标准：终端应通过请求一个TC来完成交易。金融确认报文或批上送数据报文信息中TVR的字节1，位3 为‘0’（CDA成功）。金融确认报文或批上送数据报文信息中TSI的字节1，位8 为‘1’（脱机数据认证已执行）。金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。案例01：如果终端支持CDA为mode1/4,金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。如果终端支持CDA为其他类型,金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与第二个GAC响应的一样。案例02：金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。

7.18.207 SM-AQFM134-10 以不是格式 1 的 TC 或者 ARQC 响应 GENERATE AC （隐含的）（3）

测试目的：确保在执行复合动态数据认证，卡片响应TC或ARQC时，终端不使用格式1的响应。

终端配置：——支持CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——支持 CDA总是请求，第一个GAC请求ARQC时。

卡片配置：卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）。

子类案例：——案例01：IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC；卡使用格式1编码响应ARQC；
——案例02：IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC，在第二个GENERATE AC请求TC,卡以格式2编码响应ARQC,以格式1编码响应TC；终端不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端拒绝或中止交易。本通过标准只在终端能存储被拒绝的交易情况下适用：TSI的字节1，位8 为‘1’（脱机数据认证已执行），应包含在金融确认报文或批上送数据报文信息中。

7.18.208 SM-AQFM134-11 以格式 2 的 TC 或者 ARQC 响应 GENERATE AC （4）

测试目的：——确保终端在CDA中可以使用IC卡响应格式2；
——确保终端在标签‘9F26’中存储用于复合动态数据认证的应用密文。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡以格式2响应GENERATE AC；
——IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC；
——发卡行批准交易；
——卡在第2个GENERATE AC响应一个TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证）。
通过标准：终端应通过请求一个TC来完成交易。金融确认报文或批上送数据报文信息中TVR的字节1，位3 为‘0’（CDA成功）。金融确认报文或批上送数据报文信息中TSI的字节1，位8 为‘1’ （脱机数据认证已执行）。金融确认报文或批上送数据报文信息中包含的应用密文（标签为‘9F26’）与在复合动态数据认证使用的一样。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.209 SM-AQFM134-12 以不是格式 1 的 TC 或者 ARQC 响应 GENERATE AC （隐含的）（4）

测试目的：确保在执行复合动态数据认证，卡片响应TC或ARQC时，终端不使用格式1的响应。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC，在第二个GENERATE AC请求TC；卡在第一个GENERATE AC以格式2编码响应ARQC，卡片在第二个GENERATE AC以格式1编码响应TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端拒绝或终止交易。本通过标准只在终端能存储被拒绝的交易情况下适用：TSI的字节1，位8 为‘1’（脱机数据认证已执行），应包含在金融确认报文或批上送数据报文信息中。

7.18.210 SM-AQFM134-13 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（3）

测试目的：确保在CDA中，终端不支持以TC格式的响应AAC（使用AAC生成签名）。
终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。
卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC；
——发卡行批准交易；
——第二个GENERATE AC命令，卡片返回格式2含数字签名的AAC （同返回TC的过程一样）。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：交易应被拒绝。通过标准仅适用在终端存储拒绝交易的情况下：TVR的字节1，位3为‘0’（CDA未失败），应包含在金融确认报文或批上送数据报文信息中。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.211 SM-AQFM134-14 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（4）

测试目的：确保在CDA中，终端不支持以TC格式的响应AAC（使用AAC生成签名）。
终端配置：——支持CDA；

——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC，在第二个GENERATE AC请求TC；
——第二个GENERATE AC命令，卡片返回格式2含数字签名的AAC （同返回TC的过程一样）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：交易应被拒绝。通过标准仅适用在终端存储拒绝交易的情况下：TVR的字节1，位3为‘0’（CDA未失败），应包含在金融确认报文或批上送数据报文信息中。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.212 SM-AQFM134-15 GENERATE AC 命令中复合动态数据认证参考控制参数（3）

测试目的：确保GENERATE AC命令中的参考控制参数请求复合动态数据认证。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端处理交易到完成。P1 =参考控制参数 （50 - TC，90 -ARQC）。

7.18.213 SM-AQFM134-16 GENERATE AC 命令中复合动态数据认证参考控制参数（4）

测试目的：确保GENERATE AC命令中的参考控制参数请求复合动态数据认证。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，第二个GENERATE AC请求TC；
——发卡行批准交易。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端处理交易到完成。第二个GAC，P1 为‘50’ – TC。

7.18.214 SM-AQFM134-17 GENERATE AC 命令中复合动态数据认证参考控制参数（5）

测试目的：确保GENERATE AC命令中的参考控制参数请求复合动态数据认证。

终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，第二个GENERATE AC请求TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端处理交易到完成。第二个GAC，P1 50 – TC。

7.18.215 SM-AQFM134-18 响应 GENERATE AC 的 AAC 不是数字签名的（隐含的）（5）

测试目的：确保在CDA中，终端不支持以TC格式的响应AAC（使用AAC生成签名）。

终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——IAC和TAC设置使得终端在第一个GENERATE AC请求ARQC，在第二个GENERATE AC请求TC；
——第二个GENERATE AC命令，卡片返回格式2含数字签名的AAC （同返回TC的过程一样）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：交易应被拒绝。通过标准仅适用在终端存储拒绝交易的情况下：TVR的字节1，位3为‘0’（CDA未失败），应包含在金融确认报文或批上送数据报文信息中。第一个GENERATE AC命令中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC命令中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.216 SM-AQFM135-00 在复合动态数据认证中，GENERATE AC 响应中缺少必备的数据对象（1）

测试目的：——确保终端检查JR/T 0025.7—2013中5.3.6条表18中数据的存在；
——通过执行CDA验证。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求TC；
——卡以格式2对GENERATE AC命令响应。

子类案例：——案例01：卡响应第一个GENERATE AC 的TC中不存在签名的动态应用数据（标签为‘9F4B’）；
——案例02：卡响应第一个GENERATE AC 的TC中不存在密文信息数据（标签为‘9F27’）；
——案例03：卡响应第一个GENERATE AC 的TC中不存在应用交易计数器（标签为‘9F36’）；
——案例04：卡在第一个GENERATE AC响应ARQC，响应第二个GENERATE AC 的TC中不存在签名的动态应用数据（标签为‘9F4B’），终端不能联机；
——案例05：卡在第一个GENERATE AC响应ARQC，响应第二个GENERATE AC 的TC中不存在密文信息数据（标签为‘9F27’） ，终端不能联机；
——案例06：卡在第一个GENERATE AC响应ARQC，响应第二个GENERATE AC 的TC中不存在应用交易计数器（标签为‘9F36’） ，终端不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应终止交易。

7.18.217 SM-AQFM135-01 在复合动态数据认证中，GENERATE AC 响应中缺少必备的数据对象（2）

测试目的：——确保终端检查JR/T 0025.7—2013 5.3.6条表18中数据的存在；
——通过执行CDA验证。

终端配置：——支持CDA；
——仅联机终端；

——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC；
——卡以格式2对GENERATE AC命令响应。

子类案例：——案例01：卡在第一个GENERATE AC响应ARQC， 响应第二个GENERATE AC 的TC中不存在签名的动态应用数据（标签为‘9F4B’）；
——案例02：卡在第一个GENERATE AC响应ARQC，响应第二个GENERATE AC 的TC中不存在密文信息数据（标签为‘9F27’）；
——案例03：卡在第一个GENERATE AC响应ARQC，响应第二个GENERATE AC 的TC中不存在应用交易计数器（标签为‘9F36’）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应终止交易。

7.18.218 SM-AQFM135-02 在复合动态数据认证中，GENERATE AC 响应中缺少必备的数据对象（3）

测试目的：——确保终端检查JR/T0025.7—2013 5.3.6条表18中数据的存在；
——通过执行CDA验证。

终端配置：——支持CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，在——第二个GENERATE AC命令中请求TC；
——卡以格式2对GENERATE AC命令响应。

子类案例：——案例01：卡在第一个GENERATE AC响应ARQC，响应第二个GENERATE AC 的TC中不存在签名的动态应用数据（标签为‘9F4B’）；
——案例02：卡在第一个GENERATE AC响应ARQC，响应第二个GENERATE AC 的TC中不存在密文信息数据（标签为‘9F27’）；
——案例03：卡在第一个GENERATE AC响应ARQC，响应第二个GENERATE AC 的TC中不存在应用交易计数器（标签为‘9F36’）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应终止交易。

7.18.219 SM-AQFM136-00 用于交易数据哈希的 CDOL2 的值（1）

测试目的：执行复合动态数据认证时，终端保存第2个GENERATE AC命令中由CDOL2指定的数据元的值。

终端配置：——支持CDA；
——仅脱机终端；
——有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为 ‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求TC，在第二个GENERATE AC命令中请求TC；
——交易不能联机；
——卡在第1个GENERATE AC时返回ARQC，且动态签名正确；
——卡在第2个GENERATE AC时返回TC，且动态签名正确。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR和 TSI （包含在金融确认报文或者批数据采集报文数据或者其他中） 有：-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。-TVR的字节1，位4 为‘0’（DDA未失败）。-TVR的字节1，位3 为‘0’

（CDA成功）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.220 SM-AQFM136-01 用于交易数据哈希的 CDOL2 的值（2）

测试目的：执行复合动态数据认证时，终端保存第2个GENERATE AC命令中由CDOL2指定的数据元的值。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为 ‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC；
——卡在第1个GENERATE AC时返回ARQC，且动态签名正确；
——卡在第2个GENERATE AC时返回TC，且动态签名正确。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR和 TSI（包含在金融确认报文或者批数据采集报文数据或者其他中） 有：-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。-TVR的字节1，位4 为‘0’（DDA未失败）。-TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.221 SM-AQFM136-02 用于交易数据哈希的 CDOL2 的值（3）

测试目的：执行复合动态数据认证时，终端保存第2个GENERATE AC命令中由CDOL2指定的数据元的值。

终端配置：——支持CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为 ‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，在第二个GENERATE AC命令中请求TC；
——交易不能联机；
——卡在第1个GENERATE AC时返回ARQC，且动态签名正确；
——卡在第2个GENERATE AC时返回TC，且动态签名正确。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR和 TSI（包含在金融确认报文或者批数据采集报文数据或者其他中） 有：-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。-TVR的字节1，位4 为‘0’（DDA未失败）。-TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.222 SM-AQFM137-00 用于交易数据哈希的 PDOL 的值（1）

测试目的：确保终端储存PDOL指定的数据元的值，用于复合动态数据认证的第2个GENERATE AC中。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，在第二个GENERATE AC命令中请求TC；
——交易不能联机；

——第一个GENERATE AC中卡片返回ARQC，动态签名正确；
——第二个GENERATE AC中卡片返回TC，动态签名正确；
——卡中存在PDOL（由PDOL指定的数据元的值将在第1个GENERATE AC命令和第2个GENERATE AC之间变化）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR和 TSI （包含在金融确认报文或者批数据采集报文或者其他中） 有：-第1个GENERATE AC中TVR的字节1，位3 =‘0’（CDA成功）。-第1个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）的。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。

7.18.223 SM-AQFM137-01 用于交易数据哈希的 PDOL 的值（2）

测试目的：确保终端储存PDOL指定的数据元的值，用于复合动态数据认证的第2个GENERATE AC中。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC；
——交易不能联机；
——第一个GENERATE AC中卡片返回ARQC，动态签名正确；
——第二个GENERATE AC中卡片返回TC，动态签名正确；
——卡中存在PDOL（由PDOL指定的数据元的值将在第1个GENERATE AC命令和第2个GENERATE AC之间变化）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR和 TSI（包含在金融确认报文或者批数据采集报文或者其他中）有：-第1个GENERATE AC中TVR的字节1，位3为‘0’（CDA成功）。-第1个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）的。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。

7.18.224 SM-AQFM137-02 用于交易数据哈希的 PDOL 的值（3）

测试目的：确保终端储存PDOL指定的数据元的值，用于复合动态数据认证的第2个GENERATE AC中。

终端配置：——支持CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置IAC和TAC使终端在第一个GENERATE AC命令中请求ARQC，在第一个GENERATE AC命令中请求TC；
——交易不能联机；
——第一个GENERATE AC中卡片返回ARQC，动态签名正确；
——第二个GENERATE AC中卡片返回TC，动态签名正确；
——卡中存在PDOL（由PDOL指定的数据元的值将在第1个GENERATE AC命令和第2个GENERATE AC之间变化）。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应处理交易直到完成。TVR和 TSI （包含在金融确认报文或者批数据采集报文或者其他中） 有：-第1个GENERATE AC中TVR的字节1，位3 为‘0’（CDA

成功）。-第1个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）的。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。

7.18.225 SM-AQFM138-00 第一个复合动态数据认证请求 AAC

测试目的：确保当终端第一个GENERATE AC请求AAC时，不请求复合动态数据认证。
终端配置：支持CDA。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求AAC。
测试流程：选择卡片应用，执行交易（在特殊的CDA中）。
通过标准：终端将处理交易直至结束，交易被拒绝。第1个GENERATE AC命令的P1 =‘00’。

7.18.226 SM-AQFM138-01 第二个复合动态数据认证请求 AAC

测试目的：确保当终端第二个GENERATE AC请求AAC时，不请求复合动态数据认证。
终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡在第一个GENARATE AC命令中返回ARQC；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求AAC；
——设置TAC和IAC或通过发卡行返回拒绝，使得终端在第二个GENERATE AC命令中请求AAC。
测试流程：选择卡片应用，执行交易（在特殊的CDA中）。
通过标准：终端将处理交易直至结束，交易被拒绝。第2个GENERATE AC命令的P1 =‘00’。

7.18.227 SM-AQFM139-00 用于交易数据哈希的 CDOL1 的值（1）

测试目的：确保终端存储第一个GENERATE AC命令中发送的CDOL1指定的数据，用于复合动态数据认证。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求TC；
——第1个GENERATE AC命令，卡片返回ARQC且复合动态数据认证正确；
——第2个GENERATE AC命令，卡片返回TC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端应完成交易。第二个GENERATE AC中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。金融确认报文或批数据采集报文数据的TSI的字节1，位8 为‘1’（脱机数据认证已执行）。

7.18.228 SM-AQFM139-01 用于交易数据哈希的 CDOL1 的值（2）

测试目的：确保终端在第二个GAC执行CDA时会存储CDOL1指定的数据，用于复合动态数据认证。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求TC，在第二个GENARATE AC命令中请求TC；
——交易不能联机；
——第1个GENERATE AC命令，卡片返回ARQC，复合动态数据认证正确；
——第2个GENERATE AC命令，卡片返回TC，复合动态数据认证正确。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个TC或AAC来完成交易。TVR和TSI（包含在金融确认报文或批上送数据报文或其他）有：-TVR的字节1，位3 为‘0’（CDA成功）。-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.229 SM-AQFM139-02 用于交易数据哈希的 CDOL1 的值（3）

测试目的：确保终端存储第一个GENERATE AC命令中发送的CDOL1指定的数据，用于复合动态数据认证。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC；
——第1个GENERATE AC命令，卡片返回ARQC且复合动态数据认证正确；
——第2个GENERATE AC命令，卡片返回TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端应完成交易。第二个GENERATE AC中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。金融确认报文或批数据采集报文数据的TSI的字节1，位8 为‘1’（脱机数据认证已执行）。

7.18.230 SM-AQFM139-03 用于交易数据哈希的 CDOL1 的值（4）

测试目的：确保终端存储CDOL1指定的数据，用于复合动态数据认证。

终端配置：——支持CDA；
——仅联机终端；
——CDA总是请求，第一个GAC请求ARQC时；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC；
——发卡行批准交易；
——第2个GENERATE AC命令，卡片返回TC，复合动态数据认证正确。

测试流程：选择卡片应用，执行交易（特别是动态数据认证中）。

通过标准：终端应通过请求一个TC来完成交易。TVR和TSI（包含在金融确认报文或批上送数据报文或其他）有：-TVR的字节1，位3 为‘0’（CDA成功）。-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.231 SM-AQFM139-04 用于交易数据哈希的 CDOL1 的值（5）

测试目的：确保终端存储CDOL1指定的数据，用于复合动态数据认证。

终端配置：——支持CDA；
——仅联机终端；
——当不能联机时，正常处理缺省行为码；
——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求TC；
——交易不能联机；

——第1个GENERATE AC命令，卡片返回ARQC，复合动态数据认证正确；
——第2个GENERATE AC命令，卡片返回TC，复合动态数据认证正确。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端应通过请求一个TC来完成交易。TVR和TSI（包含在金融确认报文或批上送数据报文或其他）有：-TVR的字节1，位3 为‘0’（CDA成功）。-TSI的字节1，位8 为‘1’（脱机数据认证已执行）。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。

7.18.232 SM-AQFM140-00 终端请求 ARQC 时，不请求 CDA

测试目的：确保终端请求ARQC不带CDA时，不会执行带CDA的GAC。
终端配置：——支持CDA；
——仅联机终端或有联机能力的脱机终端；
——CDA从不请求，第一个GAC请求ARQC时。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端完成交易且第一个GAC未请求CDA。P1 =参考控制参数 （80 -ARQC）。第一个GENERATE AC中TVR的字节1，位8 为‘1’（脱机数据认证未执行）。

7.18.233 SM-AQFM141-00 不能联机，脱机接受时，GAC 命令中 CDA 的处理（1）

测试目的：确保终端不能联机，请求TC时，终端能够执行第二个GAC带CDA。
终端配置：——支持CDA；
——有联机能力的脱机终端 或 （仅联机终端 和 支持当不能联机时，正常处理缺省行为码；
——CDA从不请求，第一个GAC请求ARQC时。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求TC；
——交易不能联机。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端完成交易。第二个GENERATE AC中请求TC带CDA。第一个GENERATE AC中TVR的字节1，位8 为‘1’（脱机数据认证未执行）。TVR（包含在第二个GAC或金融确认报文或批上送数据报文或其他）有：-TVR的字节1，位8 为‘0’（脱机数据认证已执行）。

7.18.234 SM-AQFM141-01 不能联机，脱机拒绝时，GAC 命令中 CDA 的处理（1）

测试目的：确保终端不能联机，请求AAC时，终端能够执行第二个GAC不带CDA。
终端配置：——支持CDA；
——有联机能力的脱机终端 或 （仅联机终端 和 支持当不能联机时，正常处理缺省行为码 ）；
——CDA从不请求，第一个GAC请求ARQC时。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求AAC；
——交易不能联机。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端完成交易。第二个GENERATE AC中请求不带CDA。第一个GENERATE AC中TVR的字节1，位8 为‘1’（脱机数据认证未执行）。TVR（包含在第二个GAC或金融确认报文或批上送数据报文或其他）有：- TVR的字节1，位8 为‘0’（脱

机数据认证已执行）。

7.18.235 SM-AQFM141-02 不能联机，脱机接受时，GAC 命令中 CDA 的处理（2）

测试目的：确保终端不能联机，请求TC时，终端能够执行第二个GAC带CDA。

终端配置：——支持CDA；

——有联机能力的脱机终端 或 （仅联机终端 和当不能联机时，正常处理缺省行为码）；

——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求TC；

——交易不能联机；

——TAC/IAC-缺省 B1b8=1,其他位全填0。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端完成交易。第二个GENERATE AC中请求TC带CDA。第一个GENERATE AC中TVR的字节1，位8 =‘1’（脱机数据认证未执行）。TVR（包含在第二个GAC或金融确认报文或批上送数据报文或其他）有：-TVR的字节1，位8 为‘0’（脱机数据认证已执行）。TSI的字节1，位8 为‘1’（脱机数据认证已执行），在通过成功完成TC在第二个GAC和金融确认报文或批上送数据报文。

7.18.236 SM-AQFM141-03 不能联机，脱机拒绝时，GAC 命令中 CDA 的处理（2）

测试目的：确保终端不能联机，请求 AAC 时，终端能够执行第二个 GAC 带 CDA。

终端配置：——支持CDA；

——有联机能力的脱机终端 或 （仅联机终端 和 支持当不能联机时，正常处理缺省行为码 ）；

——CDA总是请求，第一个GAC请求ARQC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求AAC；

——交易不能联机。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端完成交易。终端第二个GENERATE AC中请求不带CDA。TVR的字节1，位8 为‘0’（脱机数据认证已执行）包含在金融确认报文或批上送数据报文（假如终端有能力存储拒绝交易）。

7.18.237 SM-AQFM142-00 联机不请求 CDA 的终端，2nd GAC 不应请求 CDA

测试目的：联机不请求CDA的终端，成功地联机接受2nd GAC不应请求CDA。

终端配置：——支持CDA；

——有联机能力的脱机终端 或 仅联机终端；

——CDA从不请求，第一个GAC请求ARQC时；

——CDA从不请求，在第二个GAC请求TC时。

卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；

——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求TC。

测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。

通过标准：终端完成交易。终端第二个GENERATE AC中请求不带CDA。第一个GENERATE AC中TVR的字节1，位8 为‘1’（脱机数据认证未执行）。TVR（包含在第二个GAC或金融确认报文或批上送数据报文或其他）有：-TVR的字节1，位8 为‘0’（脱机数据认证已执行）。

7.18.238 SM-AQFM143-00 未执行 CDA 时，格式 1 返回 TC 或 ARQC

测试目的：确保终端能够使用卡以格式1的返回，不带CDA但AIP支持CDA。
终端配置：——支持CDA；
——有联机能力的脱机终端 或 仅联机终端；
——CDA从不请求，第一个GAC请求ARQC时。
卡片配置：——卡中的AIP指明支持复合动态数据认证（AIP的字节1，位1为‘1’）；
——卡以格式1返回GAC不带CDA；
——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，不请求CDA；
——卡在第一个GAC响应ARQC。
测试流程：选择卡片应用，执行交易（特别是复合动态数据认证中）。
通过标准：终端通过一个TC或AAC来完成交易。终端应该接受格式1的响应。

7.18.239 SM-AQFM144-00 超长数据作为静态签名数据的哈希输入-SDA

测试目的：确保终端能够正确地执行SDA，如果超长数据作为静态签名数据的哈希输入SDA。
终端配置：支持SDA。
卡片配置：——卡中的AIP指明支持SDA（AIP的字节1，位7为‘1’）。
——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充00，直到最大的记录长度（在70模版中为252字节）；其他的文件（SFI的1到10）包含3个签名记录，一个127字节长（私有标签和单字节长度），一个127字节长（私有标签和双字节长度）和一个最大记录长度（在70模版中为252字节）；签名卡中的所有允许的记录中的所有文件（部分数据如AFL，发卡行证书和不能包含SSAD）；为‘0’（未使用DDA）。第一个GENERATE AC中TSI的字节1，位8 为‘0’（脱机数据认证已执行）。

7.18.240 SM-AQFM144-01 超长数据作为 IC 卡公钥证书的哈希输入-DDA

测试目的：确保终端能够正确地执行DDA，如果超长数据作为IC卡公钥证书的哈希输入DDA。
终端配置：支持DDA。
卡片配置：——卡中的AIP指明支持DDA（AIP的字节1，位6为‘1’）；
——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充00，直到最大的记录长度（在70模版中为252字节）；其他的文件（SFI的1到10）包含3个签名记录，一个127字节长（私有标签和单字节长度），一个127字节长（私有标签和双字节长度）和一个最大记录长度（在70模版中为252字节）；签名卡中的所有允许的记录中的所有文件（部分数据如AFL，发卡行证书和不能包含SSAD）；建立正确的AFL应该包含上述记录中所涉及数据认证的数据。
测试流程：选择卡片应用，执行交易（特别是DDA）。
通过标准：终端通过一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位3 为‘0’（未使用CDA）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（DDA成功）。第一个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）。

7.18.241 SM-AQFM144-02 超长数据作为 IC 卡公钥证书的哈希输入-CDA（1）

测试目的：确保终端能够正确地执行CDA，如果超长数据作为IC卡公钥证书的哈希输入CDA。

终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——设置TAC和IAC使终端在第一个GENARATE AC命令中请求TC；
——卡在第一个GAC返回TC；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充00，直到最大的记录长度（在70模版中为252字节）；其他的文件（SFI的1到10）包含3个签名记录，一个127字节长（私有标签和单字节长度），一个127字节长（私有标签和双字节长度）和一个最大记录长度（在70模版中为252字节）；签名卡中的所有允许的记录中的所有文件（部分数据如AFL，发卡行证书和不能包含SSAD）；建立正确的AFL应该包含上述记录中所涉及数据认证的数据。
测试流程：选择卡片应用，执行交易（特别是CDA）。
通过标准：终端通过一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.18.242 SM-AQFM144-03 超长数据作为 IC 卡公钥证书的哈希输入-CDA（2）

测试目的：确保终端能够正确地执行CDA，如果超长数据作为IC卡公钥证书的哈希输入CDA。
终端配置：——支持CDA；
——仅脱机终端或有联机能力的脱机终端。
卡片配置：——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC,第二个GENERATE AC命令请求TC；
——卡在第一个GAC返回ARQC；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充00，直到最大的记录长度（在70模版中为252字节）；其他的文件（SFI的1到10）包含3个签名记录，一个127字节长（私有标签和单字节长度），一个127字节长（私有标签和双字节长度）和一个最大记录长度（在70模版中为252字节）；签名卡中的所有允许的记录中的所有文件（部分数据如AFL，发卡行证书和不能包含SSAD）；建立正确的AFL应该包含上述记录中所涉及数据认证的数据。
测试流程：选择卡片应用，执行交易（特别是CDA）。
通过标准：终端通过一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.18.243 SM-AQFM144-04 超长数据作为 IC 卡公钥证书的哈希输入-CDA（3）

测试目的：确保终端能够正确地执行CDA，如果超长数据作为IC卡公钥证书的哈希输入-CDA。
终端配置：——支持CDA；
——仅联机终端；
——终端不能联机；

——当不能联机时，正常处理缺省行为码。

卡片配置：——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求TC；

——卡在第一个GAC返回ARQC；

——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；

——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充00，直到最大的记录长度（在70模版中为252字节）；其他的文件（SFI的1到10）包含3个签名记录，一个127字节长（私有标签和单字节长度），一个127字节长（私有标签和双字节长度）和一个最大记录长度（在70模版中为252字节）；签名卡中的所有允许的记录中的所有文件（部分数据如AFL，发卡行证书和不能包含SSAD）；建立正确的AFL应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是CDA）。

通过标准：终端通过一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.18.244 SM-AQFM144-05 超长数据作为 IC 卡公钥证书的哈希输入-CDA（4）

测试目的：确保终端能够正确地执行CDA，如果超长数据作为IC卡公钥证书的哈希输入-CDA。

终端配置：——支持CDA；

——仅联机终端；

——CDA总是请求，第一个GAC请求ARQC时；

——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求TC；

——卡在第一个GAC返回ARQC；

——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；

——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充00，直到最大的记录长度（在70模版中为252字节）；其他的文件（SFI的1到10）包含3个签名记录，一个127字节长（私有标签和单字节长度），一个127字节长（私有标签和双字节长度）和一个最大记录长度（在70模版中为252字节）；签名卡中的所有允许的记录中的所有文件（部分数据如AFL，发卡行证书和不能包含SSAD）；建立正确的AFL应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是CDA）。

通过标准：终端通过一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

7.18.245 SM-AQFM144-06 超长数据作为 IC 卡公钥证书的哈希输入-CDA（5）

测试目的：确保终端能够正确地执行CDA，如果超长数据作为IC卡公钥证书的哈希输入CDA。

终端配置：——支持CDA；

——仅联机终端或有联机能力的脱机终端；
——CDA总是请求，在第二个GAC请求TC时。

卡片配置：——设置TAC和IAC使终端在第一个GENARATE AC命令中请求ARQC，在第二个GENARATE AC命令中请求TC；
——卡在第一个GAC返回ARQC；
——卡中的AIP指明支持CDA（AIP的字节1，位1为‘1’）；
——卡中用作计算签名的静态应用数据为：一个文件包含所有通常的签名数据和包含在单独的记录中的签名数据为私有标签，需要填充00，直到最大的记录长度（在70模版中为252字节）；其他的文件（SFI的1到10）包含3个签名记录，一个127字节长（私有标签和单字节长度），一个127字节长（私有标签和双字节长度）和一个最大记录长度（在70模版中为252字节）；签名卡中的所有允许的记录中的所有文件（部分数据如AFL，发卡行证书和不能包含SSAD）；建立正确的AFL应该包含上述记录中所涉及数据认证的数据。

测试流程：选择卡片应用，执行交易（特别是CDA）。

通过标准：终端通过一个TC或AAC来完成交易。第一个GENERATE AC中TVR的字节1，位7 为‘0’（未使用SDA）。第一个GENERATE AC中TVR的字节1，位3 为‘0’（CDA成功）。第一个GENERATE AC中TVR的字节1，位4 为‘0’（未使用DDA）。第一个GENERATE AC中TSI的字节1，位8 为‘1’（脱机数据认证已执行）包含在金融确认报文或批上送报文中。

8 基于借记贷记的小额支付应用的测试案例

8.1 应用选择（P2EA）

8.1.1 P2EA001-00 PDOL 不含电子现金终端支持指示器

测试目的：确保支持电子现金的终端，当PDOL中不含电子现金终端支持指示器时，进行标准PBOC交易。

终端配置：支持电子现金的终端。

卡片配置：——交易类型是消费；
——卡中的PDOL数据含授权金额和交易货币代码；
——卡中的PDOL数据不含电子现金终端支持指示器。

子类案例：——案例01：卡支持PSE选择；
——案例02：卡不支持PSE选择。

测试流程：选择应用，执行交易。

通过标准：终端应按照标准PBOC流程完成交易。卡在GPO命令中接收到“83”PDOL中指定的内容。

8.1.2 P2EA002-00 PDOL 不含授权金额

测试目的：确保支持电子现金的终端，当PDOL中不含授权金额时，进行标准PBOC交易。

终端配置：支持电子现金的终端。

卡片配置：——交易类型是消费；
——卡中的PDOL数据含电子现金终端支持指示器和交易货币代码。

子类案例：——案例01：卡中的PDOL数据不含授权金额；
——案例02：卡中PDOL为空；
——案例03：卡中不含PDOL。

测试流程：选择应用，执行交易。

通过标准：卡在GPO命令中接收到正确数据。终端应按照标准PBOC流程完成交易。

8.1.3 P2EA003-00 PDOL 含电子现金终端支持指示器、授权金额、交易货币代码

测试目的：如果确保支持电子现金的终端，PDOL中含电子现金终端支持指示器、交易货币代码，进行电子现金交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——卡中的PDOL数据含电子现金终端支持指示器、授权金额和交易货币代码。
子类案例：——案例01：卡支持PSE选择；
——案例02：卡不支持PSE选择。
测试流程：选择应用，执行交易。
通过标准：卡在GPO命令中接收到正确数据。终端应按照电子现金流程完成交易。交易结束，终端能显示电子现金余额。

8.1.4 P2EA004-00 PDOL 包含 DF69，支持 SM 算法终端，DF69 为 01

测试目的：确保支持SM算法的电子现金终端，GPO中DF69应为01。
终端配置：——支持电子现金的终端；
——支持国密算法。
卡片配置：交易类型是消费。
测试流程：选择应用。
通过标准：依据国密算法完成交易。GPO中DF69为01。

8.1.5 P2EA005-00 PDOL 包含 DF69，不支持 SM 算法终端，DF69 为 00

测试目的：确保不支持SM算法的电子现金终端，GPO中DF69应为00。
终端配置：支持-签名卡中的所有允许的记录中的所有文件（部分数据如AFL，发卡行证书和不能包含SSAD）。
卡片配置：交易类型是消费。
测试流程：选择应用。
通过标准：依据国际算法完成交易。GPO中DF69为00。

8.2 初始化应用（P2EB）

8.2.1 P2EB001-00 授权金额小于电子现金终端交易限额

测试目的：确保支持电子现金的终端，当授权金额小于电子现金终端交易限额时，进行电子现金交易。
终端配置：支持电子现金的终端，支持电子现金终端交易限额。
卡片配置：交易类型是消费。

测试流程：选择应用，执行交易。
通过标准：终端应按照电子现金流程完成交易。终端不置金额超限位。

8.2.2 P2EB002-00 授权金额等于电子现金终端交易限额-

测试目的：确保支持电子现金的终端，当授权金额等于电子现金终端交易限额时，进行标准PBOC交易。
终端配置：支持电子现金的终端，支持电子现金终端交易限额。
卡片配置：——交易类型是消费；
——实际交易金额等于电子现金终端交易限额，并且小于终端最低限额。
测试流程：选择应用，执行交易。
通过标准：终端应按照标准PBOC流程完成交易。终端不置金额超限位。

8.2.3 P2EB003-00 授权金额大于电子现金终端交易限额

测试目的：确保支持电子现金的终端，当授权金额大于电子现金终端交易限额时，进行标准PBOC交易。
终端配置：支持电子现金的终端，支持电子现金终端交易限额。
卡片配置：——交易类型是消费；
——实际交易金额大于电子现金终端交易限额，并且小于终端最低限额。
测试流程：选择应用，执行交易。
通过标准：终端应标准PBOC流程完成交易。终端不置金额超限位。

8.2.4 P2EB004-00 授权金额小于终端最低限额

测试目的：确保支持电子现金的终端，当电子现金终端交易限额不存在，授权金额小于终端最低限额时，进行电子现金交易。
终端配置：支持电子现金的终端，不存在电子现金终端交易限额。
卡片配置：——交易类型是消费；
——终端中不存在电子现金终端交易限额；
——实际交易金额小于终端最低限额。
测试流程：选择应用，执行交易。
通过标准：终端应按照电子现金流程完成交易。终端不置金额超限位。

8.2.5 P2EB005-00 授权金额大于终端最低限额

测试目的：确保支持电子现金的终端，当电子现金终端交易限额不存在，授权金额大于终端最低限额时，进行标准PBOC交易。
终端配置：支持电子现金的终端，不存在电子现金终端交易限额。
卡片配置：——交易类型是消费；
——终端中不存在电子现金终端交易限额；
——实际交易金额大于终端最低限额。
测试流程：选择应用，执行交易。
通过标准：终端应按照标准PBOC流程完成交易。终端置金额超限位。

8.2.6 P2EB006-00 授权金额等于终端最低限额

测试目的：确保支持电子现金的终端，当电子现金终端交易限额不存在，授权金额等于终端最低限额时，进行标准PBOC交易。
终端配置：支持电子现金的终端，不存在电子现金终端交易限额。
卡片配置：——交易类型是消费；
——终端中不存在电子现金终端交易限额；
——实际交易金额等于终端最低限额。
测试流程：选择应用，执行交易。
通过标准：终端应按照标准PBOC流程完成交易。终端置金额超限位。

8.2.7 P2EB007-00 授权金额大于终端最低限额，但小于电子现金终端交易限额

测试目的：确保支持电子现金的终端，当电子现金终端交易限额和终端最低限额都存在，授权金额大于终端最低限额，但小于电子现金终端交易限额时，进行电子现金交易。
终端配置：支持电子现金的终端，存在电子现金终端交易限额。
卡片配置：——设置最低限额小于电子现金终端交易限额；
——交易类型是消费；
——实际交易金额< 电子现金终端交易限额；
——实际交易金额>终端最低限额。
测试流程：选择应用，执行交易。
通过标准：终端应按照电子现金流程完成交易。终端不置金额超限位。

8.2.8 P2EB008-00 授权金额大于电子现金终端交易限额，但小于终端最低限额

测试目的：确保支持电子现金的终端，当电子现金终端交易限额和终端最低限额都存在，授权金额大于电子现金终端交易限额，但小于终端最低限额时，进行标准PBOC交易。
终端配置：支持电子现金的终端，存在电子现金终端交易限额
卡片配置：——设置最低限额大于电子现金终端交易限额；
——交易类型是消费；
——终端中存在电子现金终端交易限额和终端最低限额；
——实际交易金额<终端最低限额；
——实际交易金额>电子现金终端交易限额。
测试流程：选择应用，执行交易。
通过标准：终端应按照标准PBOC流程完成交易。终端不置金额超限位。

8.2.9 P2EB009-00 终端交易类型不是消费

测试目的：确保支持电子现金的终端，当终端交易类型不是消费时，进行标准PBOC交易。
终端配置：支持电子现金的终端。
卡片配置：交易类型非消费。
测试流程：选择应用，执行交易。
通过标准：终端应按照标准PBOC流程完成交易。

8.2.10 P2EB010-00 取得 EC 发卡行授权码，终端应获取电子现金余额和电子现金重置阈值

测试目的：确保支持电子现金的终端，终端从AFL中获取到EC发卡行授权码，终端应该发送GET DATA命令取电子现金余额和电子现金重置阈值。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——GPO命令卡响应AFL包含了ECC发卡行授权码所在文件的入口。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易。

8.2.11 P2EB011-00 未取得 EC 发卡行授权码，终端不读取电子现金余额和电子现金重置阈值

测试目的：确保支持电子现金的终端，终端未从AFL中获取到EC发卡行授权码，终端不应发送GET DATA命令取电子现金余额和电子现金重置阈值。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——GPO命令卡响应AFL未指明EC发卡行授权码所在文件。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易。

8.2.12 P2EB012-00GPO 命令未返回 AIP，终端交易终止

测试目的：确保支持电子现金的终端，GPO命令卡未响应AIP,交易应终止。
终端配置：支持电子现金的终端。
卡片配置：交易类型是消费。
子类案例：——案例01：GPO命令卡未响应AIP；
——案例02：GPO命令卡响应9000，数据域为空；
——案例03：GPO命令卡响应6985。
测试流程：选择应用。
通过标准：终端应交易终止。

8.2.13 P2EB013-00GPO 命令未返回 AFL，终端交易终止

测试目的：确保支持电子现金的终端，GPO命令卡未响应AFL,交易应终止。
终端配置：支持电子现金的终端。
卡片配置：交易类型是消费。
子类案例：——案例01：GPO命令卡未响应AFL；
——案例02：GPO命令卡响应AFL入口为空。
测试流程：选择应用。
通过标准：终端应交易终止。

8.3 脱机数据认证(国际算法)（P2EC）

8.3.1 P2EC001-00 静态数据认证成功

测试目的：确保支持电子现金的终端，应支持静态数据认证，且SDA能够成功。
终端配置：支持电子现金的终端，支持SDA。
卡片配置：——交易类型是消费；
——AIP支持SDA；
——授权金额小于电子现金终端限额；
——卡响应正确的静态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，置相关的脱机数据认证位。

8.3.2 P2EC002-00 静态数据认证失败

测试目的：确保支持电子现金的终端，应支持静态数据认证，且能够判断SDA失败。
终端配置：支持电子现金的终端，支持SDA。
卡片配置：——交易类型是消费；
——AIP支持支持SDA；
——授权金额小于电子现金终端限额；
——卡响应错误的静态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，置相关的脱机数据认证位。

8.3.3 P2EC003-00 标准动态数据认证成功

测试目的：确保支持电子现金的终端，应支持动态数据认证，且DDA能够成功。
终端配置：支持电子现金的终端，支持DDA。
卡片配置：——交易类型是消费；
——AIP支持支持DDA；
——授权金额小于电子现金终端限额；
——内部认证命令响应正确的动态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，按DDA流程置相关的脱机数据认证位。

8.3.4 P2EC004-00 标准动态数据认证失败

测试目的：确保支持电子现金的终端，应支持动态数据认证，且能够判断DDA失败。
终端配置：支持电子现金的终端，支持DDA。
卡片配置：——交易类型是消费；
——AIP支持DDA；
——授权金额小于电子现金终端限额；
——内部认证命领响应错误的动态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，按DDA流程置相关的脱机数据认证位。

8.3.5 P2EC005-00 复合动态数据认证成功

测试目的：确保支持电子现金的终端，应支持复合动态数据认证，且CDA能够成功。
终端配置：支持电子现金的终端，支持CDA。
卡片配置：——交易类型是消费；
——AIP支持CDA；
——授权金额小于电子现金终端限额；
——第一次GAC命令响应正确的动态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，按CDA流程置相关的脱机数据认证位。

8.3.6 P2EC006-00 复合动态数据认证失败

测试目的：确保支持电子现金的终端，应支持复合动态数据认证，且能够判断CDA失败。
终端配置：支持电子现金的终端，支持CDA。
卡片配置：——交易类型是消费；
——AIP支持CDA；
——授权金额小于电子现金终端限额；
——第一次GAC命令响应错误的动态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，按CDA流程置相关的脱机数据认证位。

8.4 脱机数据认证(国密算法)（SM-P2EC）

8.4.1 SM-P2EC001-00 静态数据认证成功

测试目的：确保支持电子现金的终端，应支持静态数据认证，且SDA能够成功。
终端配置：支持电子现金的终端，支持SDA，支持国密算法。
卡片配置：——交易类型是消费；
——AIP支持SDA；
——授权金额小于电子现金终端限额；
——卡响应正确的静态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，置相关的脱机数据认证位。

8.4.2 SM-P2EC002-00 静态数据认证失败

测试目的：确保支持电子现金的终端，应支持静态数据认证，且能够判断SDA失败。
终端配置：支持电子现金的终端，支持SDA，支持国密算法。
卡片配置：——交易类型是消费；
——AIP支持支持SDA；
——授权金额小于电子现金终端限额；
——卡响应错误的静态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，置相关的脱机数据认证位。

8.4.3 SM-P2EC003-00 标准动态数据认证成功

测试目的：确保支持电子现金的终端，应支持动态数据认证，且DDA能够成功。
终端配置：支持电子现金的终端，支持DDA，支持国密算法。
卡片配置：——交易类型是消费；
——AIP支持支持DDA；
——授权金额小于电子现金终端限额；
——内部认证命令响应正确的动态签名数据和正确的相关数据。

测试流程：选择应用，执行交易。
通过标准：终端应完成交易，按DDA流程置相关的脱机数据认证位。

8.4.4 SM-P2EC004-00 标准动态数据认证失败

测试目的：确保支持电子现金的终端，应支持动态数据认证，且能够判断DDA失败。
终端配置：支持电子现金的终端，支持DDA，支持国密算法。
卡片配置：——交易类型是消费；
——AIP支持DDA；
——授权金额小于电子现金终端限额；
——内部认证命领响应错误的动态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，按DDA流程置相关的脱机数据认证位。

8.4.5 SM-P2EC005-00 复合动态数据认证成功

测试目的：确保支持电子现金的终端，应支持复合动态数据认证，且CDA能够成功。
终端配置：支持电子现金的终端，支持CDA，支持国密算法。
卡片配置：——交易类型是消费；
——AIP支持CDA；
——授权金额小于电子现金终端限额；
——第一次GAC命令响应正确的动态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，按CDA流程置相关的脱机数据认证位。

8.4.6 SM-P2EC006-00 复合动态数据认证失败

测试目的：确保支持电子现金的终端，应支持复合动态数据认证，且能够判断CDA失败。
终端配置：支持电子现金的终端，支持CDA，支持国密算法。
卡片配置：——交易类型是消费；
——AIP支持CDA；
——授权金额小于电子现金终端限额；
——第一次GAC命令响应错误的动态签名数据和正确的相关数据。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，按CDA流程置相关的脱机数据认证位。

8.5 处理限制（P2ED）

8.5.1 P2ED001-00 卡的应用版本号与终端一致

测试目的：确保支持电子现金的终端，应能够正确判断应用版本号。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——授权金额小于电子现金终端限额；
——卡中存在应用版本号且于终端一致；
——卡返回IAC返回全零；
——设置TAC返回全零。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，正确判断应用版本号，置位。

8.5.2 P2ED002-00 卡的应用版本号与终端不一致

测试目的：确保支持电子现金的终端，应能够正确判断应用版本号。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；

——卡中存在应用版本号且于终端不一致；
——卡返回IAC返回全零；
——设置TAC返回全零。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，正确判断应用版本号，置位。

8.5.3 P2ED003-00 正确判断应用用途控制（1）

测试目的：确保支持电子现金的终端，应能够正确判断应用用途控制AUC。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——卡中存在应用用法控制；
——AUC中国内商品有效位=1；
——发卡行国家代码等于终端国家代码。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，正确判断AUC，置位。

8.5.4 P2ED004-00 正确判断应用用途控制（2）

测试目的：确保支持电子现金的终端，应能够正确判断应用用途控制AUC。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——卡中存在应用用法控制；
——AUC中国内商品有效位=0；
——发卡行国家代码等于终端国家代码；
——卡返回IAC返回全零；
——设置TAC返回全零。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，正确判断AUC，置位。

8.5.5 P2ED005-00 应用生效期检查（1）

测试目的：确保支持电子现金的终端，应能够正确判断应用有效期。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——卡中存在应用生效期；
——当前日期早于应用生效期；
——卡返回IAC返回全零；
——设置TAC返回全零。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，正确判断应用有效期，置位。

8.5.6 P2ED006-00 应用生效期检查（2）

测试目的：确保支持电子现金的终端，应能够正确判断应用有效期。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——卡中存在应用生效期；
——当前日期等于应用生效期。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，正确判断应用有效期，置位。

8.5.7 P2ED007-00 应用失效期检查（1）

测试目的：确保支持电子现金的终端，应能够正确判断应用失效期。

终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——卡中存在应用失效期；
——卡返回IAC返回全零；
——设置TAC返回全零。
子类案例：——案例1：当前日期早于应用失效期；
——案例2：当前日期等于应用失效期。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，正确判断应用失效期，置位。

8.5.8 P2ED008-00 应用失效期检查（2）

测试目的：确保支持电子现金的终端，应能够正确判断应用失效期。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——卡中存在应用失效期；
——当前日期晚于应用失效期；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，正确判断应用失效期，置位。

8.6 持卡人认证（P2EE）

8.6.1 P2EE001-00 脱机明文 PIN 校验成功

测试目的：确保支持电子现金的终端，应能够正确判断CVM列表，如果支持脱机明文PIN，应正确执行脱机明文PIN。
终端配置：支持电子现金的终端，支持脱机明文PIN。
卡片配置：——交易类型是消费；
——AIP 支持持卡人认证；
——卡中存在CVM列表，（01 00）；
——VERIFY命令卡相应9000。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。

8.6.2 P2EE002-00 脱机明文 PIN 校验失败

测试目的：确保支持电子现金的终端，应能够正确判断CVM列表，如果支持脱机明文PIN，应正确判断脱机明文PIN校验失败。
终端配置：支持电子现金的终端，支持脱机明文PIN。
卡片配置：——交易类型是消费；
——AIP支持支持持卡人认证；
——卡中存在CVM列表，（01 00）；
——VERIFY命令卡相应6983；
——卡返回IAC返回全零；
——设置TAC返回全零。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。

8.6.3 P2EE003-00 联机 PIN 校验成功

测试目的：确保支持电子现金的终端，应能够正确判断CVM列表，如果支持联机PIN，应正确执行联机PIN。

终端配置：支持电子现金的终端，支持联机PIN。
卡片配置：——交易类型是消费；
——AIP支持支持持卡人认证；
——卡中存在CVM列表，（02 00）；
——发卡行响应成功。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。

8.6.4 P2EE004-00 判断签名

测试目的：确保支持电子现金的终端，应能够正确判断CVM列表，如果支持签名，应正确判断签名。
终端配置：支持电子现金的终端，支持签名。
卡片配置：——交易类型是消费；
——AIP支持持卡人认证；
——卡中存在CVM列表，（1E 00）。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。打印签名线。

8.6.5 P2EE005-00 无需 CVM(终端支持无需 CVM)

测试目的：确保支持电子现金的终端当CVM是无需CVM，CVM条件码满足，且终端支持无需CVM时执行该CVM。
终端配置：支持无需CVM。
卡片配置：——卡中AIP指明支持持卡人认证；
——交易类型是消费；
——正常电子现金交易；
——CVM=1F 00。
测试流程：选择卡片应用，执行交易。
通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。

8.6.6 P2EE006-00 无需 CVM(终端不支持无需 CVM)

测试目的：确保支持电子现金的终端当CVM是无需CVM，CVM条件码满足，且终端支持无需CVM时执行该CVM。
终端配置：不支持无需CVM。
卡片配置：——卡中AIP指明支持持卡人认证；
——交易类型是消费；
——正常电子现金交易；
——CVM=1F 00。
测试流程：选择卡片应用，执行交易。
通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。

8.6.7 P2EE007-00 执行失败，执行下一个 CVR

测试目的：如果支持电子现金的终端当前CVM执行不成功，且该CVM中“如果此CVM失败，应用后续的”位为‘1’，终端应执行CVM列表中下一CVR。
终端配置：N/A。
卡片配置：——卡中AIP指明支持持卡人认证；
——交易类型是消费。
子类案例：——案例01：明文PIN校验总是（41 00），CVM失败（00 00）；当终端支持脱机PIN时，输入错误PIN；
——案例02：如果终端不支持执行签名，CVM是签名总是（5E 00），CVM失败（00 00）；

——案例03：如果终端不支持执行联机密文PIN， CVM是联机PIN总是（42 00），CVM失败（00 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。

8.6.8 P2EE008-00CVM 条件码满足，代码是明文 PIN 校验（终端支持明文 PIN）

测试目的：确保支持电子现金的终端，当CVM是明文PIN校验，CVM条件码满足，且终端支持明文PIN校验时执行该CVM。

终端配置：支持电子现金，支持明文PIN校验和签名、支持CVM执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 = ‘1’）；
——CVM执行前已知交易金额；
——交易类型是消费；
——设置终端国家代码为0156；
——CVM是明文PIN校验，后跟测试条件满足：输入错误的PIN。

子类案例：——案例01：测试条件是金额小于X（实际金额小于X）（01 06）；
——案例02：测试条件是金额大于Y（实际金额大于Y）（01 09）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。

8.6.9 P2EE009-00CVM 条件码不满足，代码是明文 PIN 校验（终端支持明文 PIN）

测试目的：确保支持电子现金的终端，当CVM是明文PIN校验+CVM失败，CVM条件码不满足，执行下一个CVM。

终端配置：支持电子现金，支持明文PIN校验、支持CVM执行前已知交易金额。

卡片配置：——卡中AIP指明支持持卡人认证（AIP 字节1，位5 = ‘1’）；
——CVM执行前已知交易金额；
——交易类型是消费；
——设置终端国家代码为0156；
——CVM是明文PIN校验，后跟测试条件满足。

子类案例：——案例01：测试条件是金额小于X（实际金额大于X）（01 06 00 00）；
——案例02：测试条件是金额大于Y（实际金额小于Y）（01 09 00 00）。

测试流程：选择卡片应用，执行交易。

通过标准：终端应完成交易，CVM结果正确，TVR和TSI置相应位。

8.7 终端风险管理（P2EF）

8.7.1 P2EF001-00 随机交易选择判断

测试目的：对于支持电子现金的终端，正常的电子现金脱机交易，当随机数小于TP，授权金额小于随机选择阈值，终端应不执行随机交易选择。

终端配置：支持电子现金的终端，支持随机交易选择。

卡片配置：——交易类型是消费；
——AIP支持终端风险管理；
——正常的电子现金脱机交易；
——授权金额小于随机选择阈值；
——随机数小于TP，满足随机选中的条件。

测试流程：选择应用，执行交易。

通过标准：终端应完成交易，根据情况置相关随机交易选择位。

8.7.2 P2EF002-00 随机交易选择判断（2）

测试目的：对于支持电子现金的终端，正常的电子现金脱机交易，当卡片返回的AFL指定的记录中不包含ECC发卡行授权码时，终端应执行随机交易选择。

终端配置：支持电子现金的终端，支持随机交易选择。
卡片配置：——交易类型是消费；
——AIP支持终端风险管理；
——正常的电子现金脱机交易；
——卡片返回的AFL指定的记录中不包含ECC发卡行授权码；
——授权金额小于随机选择阈值；
——随机数小于TP，满足随机选中的条件。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相关随机交易选择位。

8.7.3 P2EF003-00 偏置随机交易选择判断

测试目的：对于支持电子现金的终端，正常的电子现金脱机交易，当随机数小于TP，授权金额等于随机选择阈值，终端应不执行随机交易选择。
终端配置：支持电子现金的终端，支持随机交易选择
卡片配置：——交易类型是消费；
——AIP支持终端风险管理；
——正常的电子现金脱机交易；
——授权金额等于随机选择阈值，小于电子现金终端交易限额（不包括电子现金终端交易限额时小于最低限额）；
——随机数小于交易目标百分数，满足随机选中条件。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相关随机交易选择位。

8.7.4 P2EF004-00 偏置随机交易选择判断（2）

测试目的：对于支持电子现金的终端，正常的电子现金脱机交易，当随机数小于TP，授权金额大于随机选择阈值，小于最低限额，终端应不执行随机交易选择。
终端配置：支持电子现金的终端，支持随机交易选择。
卡片配置：——交易类型是消费；
——AIP支持终端风险管理；
——正常的电子现金脱机交易；
——授权金额大于随机选择阈值，小于电子现金终端交易限额（不包括电子现金终端交易限额时小于最低限额）；
——随机数小于交易目标百分比，满足随机即选中条件。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相关随机交易选择位。

8.7.5 P2EF005-00 偏置随机交易选择判断（3）

测试目的：对于支持电子现金的终端，正常的电子现金脱机交易，当卡片返回的AFL指定的记录中不包含ECC发卡行授权码时，终端应执行随机交易选择。
终端配置：支持电子现金的终端，支持随机交易选择。
卡片配置：——交易类型是消费；
——AIP支持终端风险管理；
——正常的电子现金脱机交易；
——卡片返回的AFL指定的记录中不包含ECC发卡行授权码；
——授权金额大于随机选择阈值，小于最低限额；
——随机数小于交易目标百分比，满足随机选中条件。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相关随机交易选择位。

8.7.6 P2EF006-00 最低限额判断（1）

测试目的：对于支持电子现金的终端，正常的电子现金脱机交易，当授权金额大于最低限额，终端应不执行最低限额检查。
终端配置：支持电子现金的终端，支持电子现金终端限额。
卡片配置：——交易类型是消费；
——AIP支持电子现金交易功能，支持终端风险管理；
——正常的电子现金脱机交易；
——授权金额大于最低限额，小于电子现金终端限额。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相关金额超限位。

8.7.7 P2EF007-00 最低限额判断（2）

测试目的：对于支持电子现金的终端，当卡片返回的AFL指定的记录中不包含ECC发卡行授权码时，终端应执行最低限额检查。
终端配置：支持电子现金的终端，支持电子现金终端限额。
卡片配置：——交易类型是消费；
——AIP支持终端风险管理；
——正常的电子现金脱机交易；
——卡片返回的AFL指定的记录中不包含ECC发卡行授权码；
——授权金额大于最低限额，小于电子现金终端限额。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相关金额超限位。

8.7.8 P2EF008-00 频度检查

测试目的：对于支持电子现金的终端，正常的电子现金脱机交易，当连续脱机交易下限与连续脱机交易上限都存在于卡中，终端应不执行频度检查。
终端配置：支持电子现金的终端，支持频度检查。
卡片配置：——交易类型是消费；
——AIP支持终端风险管理；
——正常的电子现金脱机交易；
——卡存在连续脱机交易下限和连续脱机交易上限；
——卡中连续脱机交易下限和连续脱机交易上限超限。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，判断是否执行频度检查，置相应位。

8.7.9 P2EF009-00 频度检查（2）

测试目的：对于支持电子现金的终端，当ECC发卡行授权码没有返回时，当连续脱机交易下限与连续脱机交易上限对存在于卡中，终端应执行频度检查。
终端配置：支持电子现金的终端，支持频度检查。
卡片配置：——交易类型是消费；
——AIP支持终端风险管理；
——正常的电子现金脱机交易；
——设置TAC拒绝、TAC联机、TAC缺省全为0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——卡片返回的AFL指定的记录中不包含ECC发卡行授权码；
——卡存在连续脱机交易下限和连续脱机交易上限；
——卡中连续脱机交易下限和连续脱机交易上限超限。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，判断是否执行频度检查，置相应位。

8.8 终端行为分析（P2EG）

8.8.1 P2EG001-00 电子现金余额减授权金额大于电子现金重置阈值，卡返 TC

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额大于电子现金重置阈值，终端应请求TC,卡返回TC，接收交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——终端成功取回电子现金余额和电子现金重置阈值；
——电子现金余额减授权金额大于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——第一个GAC命令卡响应TC。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，上送后台数据正确，显示余额正确。

8.8.2 P2EG002-00 电子现金余额减授权金额大于电子现金重置阈值，卡返 AAC

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额大于电子现金重置阈值，终端应请求TC，卡返回AAC。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——第一个GAC命令卡响应AAC。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，上送后台数据正确。

8.8.3 P2EG003-00 电子现金余额减授权金额大于电子现金重置阈值，卡返 ARQC

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额大于电子现金重置阈值，终端应请求TC，当卡片返回ARQC时，联机完成交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——第一个GAC命令卡响应ARQC；
——发卡行响应返回批准的应答。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，上送后台数据正确。

8.8.4 P2EG004-00 电子现金余额减授权金额小于电子现金重置阈值，联机完成

测试目的：如果支持电子现金的终端，当电子现金余额减授权金额小于电子现金重置阈值，具备联机能力的终端应请求ARQC。
终端配置：支持电子现金的终端,具备联机或脱机能力或仅联机终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额小于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——CVM List中是01 00（明文PIN，总是）；
——第一个GAC命令卡响应ARQC；
——第二个GAC命令卡响应TC。

测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，执行CVM，输入联机PIN。

8.8.5 P2EG005-00 电子现金余额减授权金额小于电子现金重置阈值，联机完成（2）

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额小于电子现金重置阈值，具备联机能力的终端应请求ARQC。
终端配置：支持电子现金的终端,具备联机和脱机能力或仅联机终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额小于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省全为0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——CVM List中是02 00（密文PIN，总是）。
测试流程：选择应用，执行交易，终端显示余额。
通过标准： 终端应完成交易，执行CVM，输入联机PIN。

8.8.6 P2EG006-00 电子现金余额减授权金额小于电子现金重置阈值，拒绝交易

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额小于电子现金重置阈值，具备联机能力的终端应请求ARQC，卡响应AAC，终端应该拒绝交易。
终端配置：支持电子现金的终端,具备联机或脱机能力或仅联机终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额小于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0。
子类案例：——案例1：第一个GAC命令卡响应AAC；
——案例2：第二个GAC命令卡响应AAC 。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，执行CVM，案例2输入联机PIN。

8.8.7 P2EG007-00 电子现金余额减授权金额小于电子现金重置阈值。无法联机，脱机接受

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额小于电子现金重置阈值，具备联机能力的终端应请求ARQC，无法联机时脱机接受。
终端配置：支持电子现金的终端,具备联机/脱机或仅联机终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额小于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——第一个GAC命令卡响应ARQC；
——无法联机（如联机未收到响应）；
——第二个GAC命令卡响应TC。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，执行CVM，输入联机PIN，上送后台数据正确。

8.8.8 P2EG008-00 电子现金余额减授权金额小于电子现金重置阈值，无法联机，脱机拒绝

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额小于电子现金重置阈值，具备联机能力的终端应请求ARQC，无法联机时脱机完成交易。
终端配置：支持电子现金的终端,具备联机/脱机或仅联机终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额小于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；

——第一个GAC命令卡响应ARQC；
——无法联机（如联机未收到响应）；
——第二个GAC命令卡响应AAC。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，不存此笔金融记录。

8.8.9 P2EG009-00 电子现金余额减授权金额等于电子现金重置阈值，脱机完成

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额等于电子现金重置阈值，终端应请求TC。
终端配置：支持电子现金的终端,具备联机和脱机能力或仅联机终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额等于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——第一个GAC命令卡响应TC。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，执行CVM，显示余额正确。

8.8.10 P2EG010-00 电子现金余额减授权金额等于电子现金重置阈值，持卡人认证

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额等于电子现金重置阈值，终端应脱机完成电子现金交易。
终端配置：支持电子现金的终端,具备联机和脱机能力或仅联机终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额等于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——CVM List 0108（明文PIN ，金额小于Y）。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，执行CVM，显示余额正确。

8.8.11 P2EG011-00 电子现金余额减授权金额等于电子现金重置阈值，拒绝交易

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额等于电子现金重置阈值，终端应请求TC，卡响应AAC，终端应该拒绝交易。
终端配置：支持电子现金的终端,具备联机和脱机能力或仅联机终端
卡片配置：——交易类型是消费；
——电子现金余额减授权金额等于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0。
子类案例：——案例1：第一个GAC命令卡响应AAC；
——案例2：第二个GAC命令卡片响应AAC。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易。

8.8.12 P2EG014-00 电子现金余额减授权金额小于等于电子现金重置阈值，发卡行拒绝交易

测试目的：对于支持电子现金的终端，当电子现金余额减授权金额小于等于电子现金重置阈值，具备联机能力的终端应请求ARQC，卡响应ARQC，发卡行返回拒绝的授权响应码，交易拒绝。
终端配置：支持电子现金的终端,具备联机或脱机能力或仅联机终端。
卡片配置：——交易类型是消费；

——电子现金余额减授权金额小于电子现金重置阈值；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——第一个GAC命令卡响应ARQC；
——发卡行返回拒绝的授权响应；
——第二个GAC命令卡响应AAC。

测试流程：选择应用，执行交易，终端显示余额。

通过标准：终端应完成交易。

8.8.13 P2EG015-00 设 TAC 和 IAC 为全零，交易脱机接受

测试目的：确保支持电子现金的终端，当TAC和IAC为全零，终端第一个GAC命令应请求TC。

终端配置：支持电子现金的终端。

卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP支持SDA，支持持卡人认证；
——卡片返回应用版本号为非0030；
——卡片返回静态签名不正确；
——卡片返回verify PIN 6983；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——卡第一个GAC响应TC。

测试流程：选择应用，执行交易。

通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.14 P2EG016-00 设 TAC 和 IAC 为全零，交易无法联机脱机接受

测试目的：确保支持电子现金的终端，当TAC和IAC为全零，终端第一个GAC命令应请求TC，交易无法联机时，脱机接受交易。

终端配置：支持电子现金的终端。

卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP=5800；
——卡片返回应用版本号为非0030；
——卡片返回静态签名不正确；
——卡片返回verify PIN 6983；
——设置TAC拒绝、TAC联机、TAC缺省为全0；
——卡返回IAC拒绝、IAC联机、IAC缺省均为0；
——卡第一个GAC响应ARQC；
——无法成功联机；
——卡第二个GAC响应TC。

测试流程：选择应用，执行交易。

通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.15 P2EG017-00 设 TAC 和 IAC 为全 1，交易无法联机，脱机接受

测试目的：对于支持电子现金的终端，TVR为全零，设置TAC、IAC为全1，终端第一个GAC命令应请求TC，交易脱机接受。

终端配置：支持电子现金的终端。

卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP=5800；

——设置TAC拒绝、TAC联机、TAC缺省所有位均为1；
——卡片返回IAC拒绝、IAC联机、IAC缺省所有位均为1；
——卡片返回Verify pin 9000；
——卡第一个GAC响应ARQC；
——无法成功联机；
——卡第二个GAC响应TC。

测试流程：选择应用，执行交易。

通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.16 P2EG018-00 设 TAC 和 IAC 为全 1，交易脱机接受

测试目的：确保支持电子现金的终端，TVR为全零，设置TAC、IAC为全1，终端第一个GAC命令应请求TC，交易无法联机时，脱机接受。

终端配置：支持电子现金的终端。

卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP支持SDA，支持持卡人认证；
——设置TAC拒绝、TAC联机、TAC缺省所有位均为1；
——卡片返回IAC拒绝、IAC联机、IAC缺省所有位均为1；
——卡片返回Verify pin 9000；
——第一个GAC命令卡响应TC。

测试流程：选择应用，执行交易。

通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.17 P2EG019-00 设 TAC 拒绝相应位，使交易拒绝（1）

测试目的：确保支持电子现金的终端，当设置与TVR置位的TAC拒绝相应位为1，终端第一个GAC命令应请求AAC，脱机拒绝交易。

终端配置：支持电子现金的终端。

卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP=7C00；
——设置TAC拒绝=0800000000；
——设置TAC联机、TAC缺省均为0；
——卡片返回IAC拒绝、IAC联机、IAC缺省均为0；
——卡片返回动态签名不正确；
——第一个GAC命令卡响应AAC。

测试流程：选择应用，执行交易。

通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.18 P2EG020-00 设 TAC 拒绝相应位，使交易拒绝（2）

测试目的：确保支持电子现金的终端，当设置与TVR置位的TAC拒绝相应位为1，终端第一个GAC命令应请求AAC，脱机拒绝交易。

终端配置：支持电子现金的终端。

卡片配置：——交易类型是消费；
——电子现金余额减授权金额小于电子现金重置阈值；
——AIP=5800；
——设置TAC拒绝=4000000000；
——设置TAC联机、TAC缺省均为0；
——卡片返回IAC拒绝、IAC联机、IAC缺省均为0；
——卡片返回静态签名数据不正确；
——第一个GAC命令卡响应AAC。

测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.19 P2EG021-00 设 TAC 联机相应位，交易联机

测试目的：确保支持电子现金的终端，当设置与TVR置位的TAC联机相应位为1，终端第一个GAC命令应请求ARQC，联机完成交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——AIP=7C00；
——设置TAC联机 =0080000000；
——设置TAC拒绝、TAC缺省均为0；
——卡片返回IAC拒绝、IAC联机、IAC缺省均为0；
——卡片返回应用版本号为非0030；
——第一个GAC命令卡响应ARQC；
——发卡行授权码响应批准交易；
——第二个GAC命令卡响应TC。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.20 P2EG022-00 设 TAC 缺省相应位，交易拒绝

测试目的：确保支持电子现金的终端，当设置与TVR置位的TAC缺省相应位为1，终端无法联机时，请求脱机拒绝交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP=7C00；
——设置TAC 缺省=0000800000；
——设置TAC拒绝、TAC联机均为0；
——卡片返回IAC拒绝、IAC联机、IAC缺省均为0；
——Verify pin卡片返回63C0；
——第一个GAC命令卡响应ARQC；
——无法成功联机；
——第二个GAC命令卡响应AAC。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.21 P2EG023-00 设 IAC 拒绝相应位，使交易拒绝（1）

测试目的：确保支持电子现金的终端，当设置与TVR置位的IAC拒绝相应位为1，终端第一个GAC命令应请求AAC，脱机拒绝交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP=7C00；
——卡片返回IAC拒绝=0800000000；
——卡片返回IAC联机、IAC缺省均为0；
——设置TAC拒绝、TAC联机、TAC缺省均为0；
——卡片返回动态签名不正确；
——第一个GAC命令卡响应AAC。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.22 P2EG024-00 设 IAC 拒绝相应位，使交易拒绝（2）

测试目的：确保支持电子现金的终端，当设置与TVR置位的IAC拒绝相应位为1，终端第一个GAC命令应请求AAC，脱机拒绝交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额小于电子现金重置阈值；
——AIP=5800；
——卡片返回IAC拒绝=4000000000；
——卡片返回IAC联机、IAC缺省均为0；
——设置TAC拒绝、TAC联机、TAC缺省均为0；
——卡片返回静态签名数据不正确；
——第一个GAC命令卡响应AAC。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.23 P2EG025-00 设 IAC 联机相应位，交易联机

测试目的：确保支持电子现金的终端，当设置与TVR置位的IAC联机相应位为1，终端第一个GAC命令应请求ARQC，联机完成交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP=7C00；
——卡片返回IAC联机 =0080000000；
——卡片返回IAC拒绝、IAC缺省均为0；
——设置TAC拒绝、TAC联机、TAC缺省均为0；
——卡片返回应用版本号为非0030；
——第一个GAC命令卡响应ARQC；
——发卡行授权码响应批准交易；
——第二个GAC命令卡响应TC。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.8.24 P2EG026-00 设 IAC 缺省相应位，交易拒绝

测试目的：确保支持电子现金的终端，当设置与TVR置位的IAC缺省相应位为1，终端无法联机时，请求脱机拒绝交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——电子现金余额减授权金额大于电子现金重置阈值；
——AIP=7C00；
——卡片返回IAC 缺省=0000800000；
——卡片返回IAC拒绝、IAC联机均为0；
——设置TAC拒绝、TAC联机、TAC缺省均为0；
——Verify pin卡片返回63C0；
——第一个GAC命令卡响应ARQC；
——无法成功联机；
——第二个GAC命令卡响应AAC。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.9 发卡行脚本处理（P2EH）

8.9.1 P2EH001-00 在 AIP 不支持发卡行认证

测试目的：确保支持电子现金的终端，当卡在AIP中指明不支持发卡行认证且授权响应报文中存在IAD时，终端不发送EXTERNAL AUTHENTICATE命令。
终端配置：支持电子现金，仅联机或支持脱机/联机能力。
卡片配置：——正常电子现金交易；
——交易类型为消费；
——卡对第一个GENERATE AC返回ARQC；
——卡中AIP指明发卡行认证不支持（AIP 字节1，位3 = ‘0’）；
——授权响应报文中包括IAD；
——发卡行返回IAD。
测试流程：选择卡片应用，执行交易。
通过标准：终端应完成交易，不应发送外部认证命令。

8.9.2 P2EH002-00AIP 支持发卡行认证

测试目的：确保支持电子现金的终端，当卡在AIP中指明支持发卡行认证且授权响应报文中存在IAD时，终端发送EXTERNAL AUTHENTICATE命令。
终端配置：支持电子现金，仅联机或支持脱机/联机能力。
卡片配置：——正常电子现金交易；
——交易类型为消费；
——卡对第一个GENERATE AC返回ARQC；
——卡中AIP指明支持发卡行认证（AIP 字节1，位3 = ‘1’）；
——授权响应报文中包括IAD；
——发卡行返回IAD；
——卡片响应EXTERNAL AUTHENTICATE命令9000。
测试流程：选择卡片应用，执行交易。
通过标准：终端应完成交易，应发送外部认证命令。

8.9.3 P2EH003-00AIP 支持发卡行认证，发卡行认证失败

测试目的：确保支持电子现金的终端，当卡在AIP中指明支持发卡行认证且授权响应报文中存在IAD时，终端发送EXTERNAL AUTHENTICATE命令。
终端配置：支持电子现金，仅联机或支持脱机/联机能力。
卡片配置：——正常电子现金交易；
——交易类型为消费；
——卡对第一个GENERATE AC返回ARQC；
——卡中AIP指明支持发卡行认证（AIP 字节1，位3 = ‘1’）；
——授权响应报文中包括IAD；
——发卡行返回IAD；
——卡片响应EXTERNAL AUTHENTICATE命令6300。
测试流程：选择卡片应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI。

8.9.4 P2EH004-00 执行 TAG=71 的脚本命令

测试目的：对于支持电子现金的终端，应能够正确处理TAG=71的发卡行的正确脚本。
终端配置：支持电子现金的终端，具备联机\脱机能力或仅联机终端。
卡片配置：——交易类型是消费；
——正常电子现金交易；
——发卡行发送TAG=71的脚本；
——卡响应每个脚本9000。
测试流程：选择应用，执行交易。

通过标准：终端应完成交易，根据情况置相应的TVR和TSI，脚本执行正确。

8.9.5 P2EH005-00 执行 TAG=72 的脚本命令

测试目的：对于支持电子现金的终端，应能够正确处理TAG=72的发卡行的正确脚本。
终端配置：支持电子现金的终端，具备联机或脱机能力或仅联机终端。
卡片配置：——交易类型是消费；
——正常电子现金交易；
——发卡行发送TAG=72的脚本；
——卡响应每个脚本9000。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI，脚本执行正确。

8.9.6 P2EH006-00 执行 TAG=71 的脚本命令失败

测试目的：对于支持电子现金的终端，应能够正确处理TAG=71的发卡行的失败脚本。
终端配置：支持电子现金的终端，具备联机和脱机能力或仅联机终端。
卡片配置：——交易类型是消费；
——正常电子现金交易；
——发卡行发送TAG=71的脚本；
——卡响应脚本非9000。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI，脚本执行正确。

8.9.7 P2EH007-00 执行 TAG=72 的脚本命令失败

测试目的：对于支持电子现金的终端，应能够正确处理TAG=72的发卡行的失败脚本。
终端配置：支持电子现金的终端，具备联机和脱机能力或仅联机终端。
测试条件：——交易类型是消费；
——正常电子现金交易；
——发卡行发送TAG=72的脚本；
——卡响应脚本非9000。
测试流程：选择应用，执行交易，终端显示余额。
通过标准：终端应完成交易，根据情况置相应的TVR和TSI，脚本执行正确。

8.10 其他情况（P2EI）

8.10.1 P2EI001-00 电子现金余额查询功能

测试目的：对于支持电子现金的终端，应具备电子现金余额查询功能。
终端配置：支持电子现金的终端。
卡片配置：支持余额查询，卡片返回余额。
测试流程：选择应用，执行查余额。
通过标准：终端应具备查余额功能。余额的显示应正确。

8.10.2 P2EI002-00 交易完成后显示电子现金余额功能（1）

测试目的：对于支持电子现金的终端，应具备在电子现金交易完成后正确显示电子现金余额的功能。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——授权金额小于电子现金终端限额。
测试流程：选择应用，执行交易，显示余额。
通过标准：终端应完成交易。交易完成后应能正确显示电子现金余额。

8.10.3 P2EI002-01 交易完成后显示电子现金余额功能（2）

测试目的：对于支持电子现金的终端，应具备在电子现金交易完成后正确显示电子现金余额的功能。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——授权金额小于电子现金终端限额；
——卡片第一个GAC返回ARQC。
测试流程：选择应用，执行交易，显示余额。
通过标准：终端应完成交易。交易完成后应能正确显示电子现金余额。

8.10.4 P2EI003-00 交易日志查询功能

测试目的：对于支持电子现金的终端，应具备交易日志查询功能。
终端配置：支持电子现金的终端。
卡片配置：取交易日志格式命令和读日志命令卡响应9000，返回日志。
测试流程：选择应用，取交易日志格式，读取交易日志。
通过标准：终端应发送GET DATA取日志格式。终端应正确显示日志内容。

8.10.5 P2EI004-00 持卡人姓名和姓名扩展

测试目的：如果卡片中返回持卡人姓名或持卡人姓名扩展数据，数据的长度不应导致终端终止交易。
终端配置：支持电子现金的终端。
卡片配置：——交易类型是消费；
——授权金额小于电子现金终端限额。
子类案例：——案例01：返回持卡人姓名和姓名扩展；
——案例02：返回持卡人姓名和姓名扩展，持卡人姓名长26个字节；
——案例03：返回持卡人姓名扩展长度超过26个字节；
——案例04：返回持卡人姓名扩展长度小于19个字节。
测试流程：选择应用，执行交易。
通过标准：终端应完成交易。