ICS 03.220.20;35.240.15
R 07
备案号:

JT

中华人民共和国交通运输行业标准

JT/T 978.7—2015

城市公共交通IC卡技术规范 第7部分:检测项目

Technical specification on IC card for urban public transport—Part7:Test items

2015-05-21 发布　　2015-07-15 实施

中华人民共和国交通运输部　发布

目　　次

前　言

JT/T 978《城市公共交通IC卡技术规范》由7个部分组成：

——第1部分：总则

——第2部分：卡片；

——第3部分：读写终端；

——第4部分：信息接口；

——第5部分：非接触接口通信；

——第6部分：安全；

——第7部分：检测项目。

本部分为JT/T 978的第7部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由中华人民共和国交通运输部运输服务司提出。

本部分由全国城市客运标准化技术委员会(SAC/TC 529)归口。

本部分起草单位：中国交通通信信息中心、交通运输部科学研究院、北京市政交通一卡通有限公司、南京市市民卡有限公司、武汉城市一卡通有限公司、哈尔滨市城市通智能卡有限责任公司、银川市公共交通有限公司、泰州市凤城一卡通有限公司、银行卡检测中心、中钞信用卡产业发展有限公司、北京中电华大电子设计有限责任公司、天津市通卡公用网络系统有限公司。

本部分主要起草人：汪宏宇、李岚、唐猛、王一路、刘好德、谷云辉、陈文革、肖震宇、熊剑、李勇、嵇云峰、张策、王睿、周亮。

城市公共交通 IC 卡技术规范

第 7 部分:检测项目

1 范围

JT/T 978 的本部分规定了城市公共交通 IC 卡的卡片检测、SAM 卡检测、终端检测和系统检测基本要求。

本部分适用于城市公共交通 IC 卡卡片、终端及密钥管理系统的检测。

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。

GB/T 14916 识别卡 物理特性

GB/T 16649.1 识别卡 带触点的集成电路卡 第 1 部分:物理特性

GB/T 17554.1 识别卡 测试方法 第 1 部分:一般特性测试

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 28035—2011 软件系统验收规范

JT/T 978.1 城市公共交通 IC 卡技术规范 第 1 部分:总则

JT/T 978.2 城市公共交通 IC 卡技术规范 第 2 部分:卡片

JT/T 978.3 城市公共交通 IC 卡技术规范 第 3 部分:读写终端

JT/T 978.4 城市公共交通 IC 卡技术规范 第 4 部分:信息接口

JT/T 978.5 城市公共交通 IC 卡技术规范 第 5 部分:非接触接口通信

JT/T 978.6 城市公共交通 IC 卡技术规范 第 6 部分:安全

3 术语和定义

JT/T 978.1 ~JT/T 978.6 界定的及下列术语和定义适用于本文件。

3.1

保护时间 guard time

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

3.2

接口设备 interface device

终端上插入卡片的部分,包括其中的机械和电气部分。

3.3

静止状态 inactive

当卡片上的电源电压(VCC)和其他信号相对于地的电压值小于或等于 0.4V 时,则称电源电压和这些信号处于静止状态。

3.4

冷复位 cold reset

当卡片的电源电压(VCC)和其他信号从静止状态中复苏且申请复位信号时,卡片产生的复位。

3.5

热复位 warm reset

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

3.6

T=0 协议 T=0 protocol

异步半双工字符传输协议。

3.7

T=1 协议 T=1 protocol

异步半双工块传输协议。

3.8

单粒子效应 SEE single event effect

宇宙空间中单个高能粒子入射到半导体器件或集成电路中时诱发的一种现象。

4 符号和缩略语

下列符号和缩略语适用于本文件。

AC——应用密文(Application Cryptogram)

ACK——确认(Acknowledgment)

ADC——Type B 的应用数据编码(Application Data Coding, Type B)

ADA——应用缺省行为(Application Default Action)

ADF——应用数据文件(Application Definition 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)

ATC——应用交易序号(Application Transaction Counter)

ATR——复位应答(Answer to Reset)

AUC——应用用途控制(Application Usage Control)

ATQA——Type A 的请求应答(Answer to Request, Type A)

ATQB——Type B 的请求应答(Answer to Request, Type B)

ATTRIB——Type B 的 PICC 选择命令(PICC Selection Command, Type B)

ATS——选择应答(Answer to Select)

BGT——块保护时间(Block Guard Time)

CAPP——扩展应用(Comprehensive Application)/复合应用(Complex Application)

CDA——复合动态数据认证/应用密文生成(Combined DDA/AC Generation)

CDOL——卡片风险管理数据对象列表(Card Rish Management Data Object List)

CLK——时钟(Clock)

CTTA——累计脱机交易总金额(Cumulative Total Transaction Amount)

CTTAL——累计脱机交易总金额限制(Cumulative Total Transaction Amount Limit)

CTTAUL——累计脱机交易总金额上限(Cumulative Total Transaction Amount Upper Limit)

CVM——持卡人验证方法(Cardholder Verification Method)

CWT——字符等待时间(Character Waiting Time)
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)
EGT——Type B 的额外保护时间(Extra Guard Time, Type B)
EOF——帧结束(End of Frame)
f_c——载波频率(工作场的频率)
FCI——文件控制信息(File Control Information)
FDT——帧延迟时间(Frame Delay Time)
FO——帧选择(Frame Option)
FWT——帧等待时间(帧等待时间)(Frame Waiting Time)
GAC——生成应用密文(Generate AC)
GND——地(Ground)
GPO——获取处理选项(Get Processing Options)
IC——集成电路(Integrated Circuit)
ICC——集成电路卡(Integrated Circuit Card)
INF——信息域(Information Field)
I/O——输入/输出(Input/Output)
L_e——响应数据中的最大期望长度
LEN——长度(Length)
LOATC——上次联机交易计数器(Last Online ATC)
LRC——冗余校验(Longitudinal Redundancy Check)
MAC——报文认证码(Message Authentication Code)
MDK——主密钥(Master DEA Key)
NAD——节点地址(Node Address)
NAK——否定的确认(Negative Acknowledgment)
PAN——主账号(Primary Account Number)
PANSN——主账号索引号(PAN Sequnce Number)
PCB——协议控制字节(Protocol Control Byte)
PCD——接近式耦合设备(Proximity Coupling Device)
PDOL——处理选项数据对象列表(Processing Options Data Object List)
PICC——近距离接近式 IC 卡(Proximity ICC)
PIN——个人密码(Personal Identification Number)
PSE——支付系统环境(Payment Systems Environment)
PPSE——近距离支付系统环境(Proximity Payment Systems Environment)
RAM——随机存取存储器(Random - Access Memory)
RATS——Type A 的选择应答请求(Request for Answer to Select, Type A)
REQB——Type B 的请求命令(Request Command, Type B)
RFU——保留(Reserved for Future Use)
RID——注册应用提供商标签(Registered Application Provider Identifier)
RSA——Rivest、Sharmir 和 Adleman 提出的一种非对称密钥算法的简称

RST——复位(Reset)
SDA——静态数据认证(Static Data Authentication)
SFI——短文件标签符(Short File Identifier)
SFGI——启动帧保护时间整数(Start - up Frame Guard Time Integer)
SFGT——启动帧保护时间(Start - up Frame Guard Time)
SHA——安全哈希算法(Secure Hash Algorithm)
SM2——SM2 椭圆曲线公钥密码算法(Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves)
SM4——SM4 分组密码加密算法(SM4 Cryptographic Algorithm)
SOF——帧开始(Start of Frame)
TAC——终端行为代码(Terminal Action Code)
TAL——终端应用层(Terminal Application Layer)
TC——交易证书(Transaction Certificate)
t_F——信号幅度从 90% 下降到 10% 的时间(Fall Time Between 90% and 10% of Signal Amplitude)
TLV——标签、长度、值(Tag,Length,Value)
t_R——信号幅度从 10% 上升到 90% 的时间(Rise Time Between 10% and 90% of Signal Amplitude)
TSI——交易状态信息(Transaction Status Information)
TVR——终端验证结果(Terminal Verification Results)
UID——Type A 的唯一标识符 (Unique Identifier, Type A)
VCC——电源电压(Supply Voltage)
V_{OH}——高电平输出电压
V_{OL}——低电平输出电压
WTX——等待时间扩展(Waiting Time Extension)
WUPA——Type A 的 PICC 唤醒命令(Wake-up Command, Type A)
WUPB——Type B 的 PICC 唤醒命令(Wake-up Command, Type B)
XRAM——外部随机存储器(Expanded RAM)

5 卡片检测

5.1 物理特性

5.1.1 一般要求

检测应符合 GB/T 14916 的要求。

5.1.2 通用物理特性

检测内容:卡片产品通用物理特性检测内容应符合 GB/T 14916、GB/T 16649.1 的要求。
测试条件:测试条件应符合 GB/T 14916 及 GB/T 16649.1 的要求。
测试过程:测试过程应符合 GB/T 17554.1 的要求。

5.1.3 卡片工作温度测试

检测内容:卡片产品在交通应用场景极限工作温度下的卡片功能。
测试条件:低温 -35℃ ±3℃;高温 70℃ ±3℃,相对湿度 95% ±5%。
测试过程:卡片在低温和高温环境下各放置 24h,然后再在实验室环境下静置 24h 后对卡片进行应

用选择,查看卡片的功能响应。

5.2 非接触式电特性和通信协议

5.2.1 一般要求

检测环境为常温 23℃ ±3℃,湿度 40% ~80%。

参见附录 A 进行卡片准备。

本章检测结果应符合 JT/T 978.5 的要求。

5.2.2 电特性

5.2.2.1 PICC 负载调制幅值检测

检测内容:PICC 在最大工作场强(H_{max})及最小工作场强(H_{min})之间,负载调制信号的幅值。

测试条件:

a) 当 $H=1.5A/m$,对应 $V_{rms}=480mV$ 时;

b) 当 $H=2.5A/m$,对应 $V_{rms}=800mV$ 时;

c) 当 $H=3.5A/m$,对应 $V_{rms}=1.12V$ 时;

d) 当 $H=4.5A/m$,对应 $V_{rms}=1.44V$ 时;

e) 当 $H=5.5A/m$,对应 $V_{rms}=1.76V$ 时;

f) 当 $H=6.5A/m$,对应 $V_{rms}=2.08V$ 时;

g) 当 $H=7.5A/m$,对应 $V_{rms}=2.40V$ 时。

测试过程:使终端发出 WUPA、WUPB 指令,调节功率放大器,使终端发出信号满足 PICC 工作场为 $[H_{min},H_{max}]$。测量卡片在 12.7125MHz 和 14.4075MHz 两个频率点的负载调制幅值。

5.2.2.2 PICC 交变磁场检测

检测内容:检测 PICC 在交变磁场内测试后的卡片功能。

测试条件:默认环境条件。

测试过程:将待测样卡置于频率为 13.56MHz、平均场强为 10A/m、最大场强为 12A/m 的交变磁场中,平均时间 30s。

5.2.3 通信协议

5.2.3.1 Type A 传输协议

检测内容:检测卡片 Type A 协议。

测试条件:卡片支持 Type A 协议。

测试过程:按照表 1 的测试项目对卡片进行逐项测试。

表 1 Type A 传输协议测试项目

序 号	测 试 项 目
1	基本交换和时间测试
2	从 PCD 到 PICC 最短和较长帧延迟时间基本交换测试
3	防冲突状态机的正确处理测试
4	RATS 中所含变量的正确处理测试
5	IDLE 状态下的错误处理测试

表1（续）

序　号	测 试 项 目
6	READY 状态下的错误处理测试
7	ACTIVE 状态下的错误处理测试
8	进入 ACTIVE 状态之后的 HALT 状态下的错误处理测试
9	进入 PROTOCOL 状态之后的 HALT 状态下的错误处理测试
10	轮询和 PICC 复位的处理测试

5.2.3.2　Type B 传输协议

检测内容：检测卡片 Type B 协议。

测试条件：卡片支持 Type B 协议。

测试过程：按照表2的测试项目对卡片进行逐项测试。

表2　Type B 传输协议测试项目

序　号	测 试 项 目
1	从 PCD 到 PICC 最短帧延迟时间基本交换测试
2	支持 SFGT 的 PCD，从 PCD 到 PICC 最小 SFGT 时基本交换测试
3	PCD 最小和最大 EGT 交换测试
4	最小和最大 S 序列、E 序列的交换测试
5	防冲突状态机的正确处理测试
6	在 ATTRIB 命令中发送的上层信息域的正确处理测试
7	在 WUPB/REQB/ATTRIB 命令中发送含 RFU 值的正确处理测试
8	在 IDLE 状态下的错误处理测试
9	在 READY 状态下的错误处理测试
10	在 READY 状态后的 HALT 状态下的错误处理测试
11	在 ACTIVE 状态后的 HALT 状态下的错误处理测试
12	在 HALT 状态下的发 WUPA 的处理测试
13	轮询和 PICC 复位的处理测试

5.2.3.3　块传输协议

检测内容：检测卡片的块传输协议。

测试条件：卡片支持 Type A 或 Type B 协议。

测试过程：按照表3的测试项目对卡片进行逐项测试。

表3　块传输协议测试项目

序　号	测 试 项 目
1	从 PCD 接收链接 I 块的测试
2	块之中的 PCB 带 RFU 位的测试

表3（续）

序　号	测 试 项 目
3	未指明链接I块的错误指示测试
4	接收非链接I块后的错误测试
5	接收链接I块后的错误指示及错误测试
6	PICC复位的块协议测试
7	块协议中的命令处理测试

5.3 应用功能

5.3.1 一般要求

检测环境为常温23℃ ±3℃。

参见附录A进行卡片准备，异形卡也应满足本章应用功能检测要求。

本章检测项目应符合JT/T 978.2和JT/T 978.3的要求。

5.3.2 联机交易应用

5.3.2.1 电子现金应用锁定命令

检测内容：检测卡片的应用锁定命令。

测试条件：默认环境条件。

测试过程：向卡片发送正常和异常的应用锁定命令并接收响应。

5.3.2.2 电子现金应用锁定流程

检测内容：检测卡片的应用锁定执行流程。

测试条件：默认环境条件。

测试过程：在不同的卡片状态下向卡片发送应用锁定命令并接收响应。

5.3.2.3 电子现金读应用数据

检测内容：检测卡片的READ RECORD命令和执行流程。

测试条件：默认环境条件。

测试过程：向卡片发送正常和异常的READ RECORD命令并接收响应。

5.3.2.4 电子现金获取应用数据

检测内容：检测卡片的GET DATA命令和执行流程。

测试条件：默认环境条件。

测试过程：向卡片发送正常和异常的GET DATA命令并接收响应。

5.3.2.5 电子现金应用选择

检测内容：检测卡片的应用选择命令和执行流程。

测试条件：默认环境条件。

测试过程：向不同状态的卡片发送应用选择命令并接收响应。

5.3.2.6 电子现金应用解锁命令

检测内容：检测卡片的应用解锁命令。

测试条件：默认环境条件。

测试过程：向卡片发送正常和异常的应用解锁命令并接收响应。

5.3.2.7 电子现金应用解锁流程

检测内容:检测卡片的应用解锁流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同的卡片状态下向卡片发送应用解锁命令并接收响应。

5.3.2.8 电子现金卡片锁定命令

检测内容:检测卡片锁定命令和卡片锁定命令执行的情况。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的卡片锁定命令并接收响应。

5.3.2.9 电子现金卡片锁定流程

检测内容:检测卡片锁定流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同的卡片状态下向卡片发送卡片锁定命令并接收响应。

5.3.2.10 电子现金联机批准交易

检测内容:检测卡片对联机批准交易中命令的正确响应。

测试条件:默认环境条件。

测试过程:发送交易命令并接收响应。

5.3.2.11 电子现金上次交易发卡机构脚本失败

检测内容:检测卡片对上次发卡机构执行脚本失败情况下的处理流程。

测试条件:默认环境条件。

测试过程:在上次发卡机构脚本失败情况下发送交易命令并接收响应。

5.3.2.12 电子现金卡片风险管理

检测内容:检测卡片风险管理处理流程。

测试条件:默认环境条件。

测试过程:在满足风险管理的条件下发送交易命令并接收响应。

5.3.2.13 电子现金双货币超累计交易金额上限检查

检测内容:检测卡片执行交易金额(双货币)的频度检查处理情况。

测试条件:默认环境条件。

测试过程:发送第二货币交易命令并接收响应。

5.3.2.14 电子现金更新卡片数据

检测内容:检测卡片 PUT DATA 和执行流程。

测试条件:默认环境条件。

测试过程:在不同的卡片状态下向卡片发送 PUT DATA 命令并接收响应。

5.3.2.15 电子现金 EXTERNAL AUTHENTICATE 命令

检测内容:检测卡片的 EXTERNAL AUTHENTICATE 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 EXTERNAL AUTHENTICATE 命令并接收响应。

5.3.2.16 电子现金联机交易失败

检测内容:检测卡片联机交易失败情况下执行流程。

测试条件:默认环境条件。

测试过程:在联机失败交易时向卡片发送交易指令并接收响应。

5.3.2.17 电子现金 GET PROCESSING OPTIONS 命令

检测内容:检测卡片的 GET PROCESSING OPTIONS 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 GET PROCESSING OPTIONS 命令并接收响应。

5.3.2.18 电子现金应用初始化

检测内容:检测卡片的应用初始化流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同的卡片状态下向卡片发送应用初始化命令并接收响应。

5.3.2.19 电子现金发卡机构认证

检测内容:检测卡片的发卡机构认证流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同的卡片状态下向卡片发送卡机构认证命令并接收响应。

5.3.2.20 电子现金发卡机构脚本处理

检测内容:检测卡片的发卡机构脚本处理流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同的卡片状态下向卡片发送不同的发卡机构脚本指令并接收响应。

5.3.2.21 电子现金日志文件

检测内容:检测卡片的日志记录处理流程。

测试条件:默认环境条件。

测试过程:发送交易指令进行交易并读取卡片日志文件记录。

5.3.2.22 电子现金新卡

检测内容:检测卡片的新卡处理流程。

测试条件:默认环境条件,新卡。

测试过程:在新卡状态下发送不同的交易指令并接收响应。

5.3.2.23 PIN CHANGE/UNBLOCK 命令

检测内容:检测卡片 PIN CHANGE/UNBLOCK 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 PIN CHANGE/UNBLOCK 命令并接收响应。

5.3.2.24 VERIFY 命令

检测内容:检测卡片 VERIFY 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 VERIFY 命令并接收响应。

5.3.2.25 电子现金 UPDATE RECORD 命令

检测内容:检测卡片的 UPDATE RECORD 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 UPDATE RECORD 命令并接收响应。

5.3.2.26 电子现金联机完成

检测内容:检测卡片联机完成情况下的交易流程处理,判定在联机完成的情况下卡片流程的执行情况。

测试条件:默认环境条件。

测试过程:向已经完成联机交易的卡片在重新上电的基础上发送交易命令并接收响应。

5.3.2.27 电子现金联机授权未完成

检测内容:检测卡片在联机授权未完成情况下的交易流程处理。

测试条件:默认环境条件。

测试过程:在联机授权未完成的情况下向卡片发送交易命令并接收响应。

5.3.2.28 电子现金持卡人认证

检测内容:检测卡片持卡人认证执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令实现持卡人认证执行流程并接收响应。

5.3.2.29 电子现金 PUT DATA 连续国际交易限制

检测内容:检测卡片的 PUT DATA 连续国际交易限制处理流程,判定卡片在 PUT DATA 连续国际交易限制时的执行情况。

测试条件:默认环境条件。

测试过程:向卡片发送 PUT DATA 连续国际交易限制处理交易指令并接收响应。

5.3.2.30 电子现金执行交易金额(双货币)频度检查

检测内容:检测卡片的执行交易金额(双货币)频度检查处理流程,判定卡片在执行交易金额(双货币)频度检查时的执行情况。

测试条件:默认环境条件。

测试过程:向卡片发送第二货币交易指令并接收响应。

5.3.2.31 电子现金执行国际国家频度检查

检测内容:检测卡片的执行国际国家频度检查处理流程,判定卡片在执行国际国家频度检查时的执行情况。

测试条件:默认环境条件。

测试过程:向卡片发送不同国家代码的交易指令并接收响应。

5.3.2.32 电子现金执行指定货币交易金额检查

检测内容:检测卡片的执行指定货币交易金额检查处理流程,判定卡片在执行指定货币交易金额检查时的执行情况。

测试条件:默认环境条件。

测试过程:向卡片发送指定货币交易金额的交易指令并接收响应。

5.3.2.33 电子现金执行国际货币频度检查

检测内容:检测卡片的执行国际货币频度检查处理流程,判定卡片在执行国际货币频度检查时的执行情况。

测试条件:默认环境条件。

测试过程:向卡片发送国际货币交易指令并接收响应。

5.3.2.34 电子现金参数测试

检测内容:检测卡片支持的命令参数,判定卡片对错误参数的处理情况。

测试条件:默认环境条件。

测试过程:向卡片发送错误参数的交易指令并接收响应。

5.3.2.35 电子现金稳定性测试

检测内容:检测卡片最小交易稳定性,执行规定笔数的交易。

测试条件:默认环境条件。

测试过程:向卡片发送指定交易笔数的联机交易指令并接收响应。

5.3.2.36 电子现金自助终端受理测试

检测内容:检测卡片在模拟自助终端上交易流程处理,判定卡片在 GPO GAC 数据不一致情况下的流程执行情况。

测试条件:默认环境条件。

测试过程:向卡片发送 GPO 与 GAC 数据不一致的交易指令并接收响应。

5.3.3 脱机交易应用

5.3.3.1 PPSE 选择

检测内容:检测卡片 PPSE 选择执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 PPSE 选择命令并接收响应。

5.3.3.2 电子钱包应用状态测试

检测内容:检测卡片的电子钱包应用在不同状态下的命令执行流程,判定卡片在不同状态下的命令执行的情况。

测试条件:默认环境条件。

测试过程:向卡片发送指令将卡片设置为不同的应用状态并接收响应。

5.3.3.3 电子钱包应用锁定命令

检测内容:检测卡片电子钱包应用锁定命令。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的电子钱包应用锁定命令并接收响应。

5.3.3.4 电子钱包应用锁定流程

检测内容:检测卡片的电子钱包应用锁定流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同的卡片状态下向卡片发送电子钱包应用锁定命令并接收响应。

5.3.3.5 电子钱包应用解锁命令

检测内容:检测卡片的电子钱包应用解锁命令。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的电子钱包应用解锁命令并接收响应。

5.3.3.6 电子钱包应用解锁流程

检测内容:检测卡片的电子钱包应用解锁流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同的卡片状态下向卡片发送电子钱包应用解锁命令并接收响应。

5.3.3.7 电子钱包圈存初始化命令

检测内容:检测卡片的电子钱包圈存交易流程和电子钱包圈存初始化命令处理流程。

检测条件:默认环境条件。

测试过程:在不同情况下对卡片发送电子钱包圈存初始化命令并接收响应。

5.3.3.8 电子钱包圈存流程

检测内容:检测卡片的电子钱包圈存交易流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同情况下对卡片发送电子钱包圈存命令并接收响应。

5.3.3.9 电子钱包圈提流程

检测内容:检测卡片的电子钱包圈提交易流程和执行流程。

测试条件:默认环境条件。

测试过程:在不同情况下对卡片发送电子钱包圈提命令并接收响应。

5.3.3.10 电子钱包修改透支流程

检测内容:检测卡片的电子钱包修改透支限额交易流程和执行流程,判定卡片涉及电子钱包修改透支限额交易(修改初始化命令、修改透支限额命令)的执行情况。

测试条件:默认环境条件。

测试过程:在不同情况执行电子钱包修改透支交易并接收响应。

5.3.3.11 电子钱包度记录命令

检测内容:检测卡片的 READ RECORD 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 READ RECORD 命令并接收响应。

5.3.3.12 电子钱包更新记录命令

检测内容:检测卡片的 UPDATE RECORD 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 UPDATE RECORD 命令并接收响应。

5.3.3.13 电子钱包 READ BINARY 命令

检测内容:检测卡片的 READ BINARY 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 READ BINARY 命令并接收响应。

5.3.3.14 电子钱包 UPDATE BINARY 命令

检测内容:检测卡片的 UPDATE BINARY 命令和执行流程。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的 UPDATE BINARY 命令并接收响应。

5.3.3.15 电子钱包消费交易

检测内容:检测卡片在电子钱包消费的处理流程,消费流程中涉及的命令(初始化消费命令、消费命令)。

测试条件:默认环境条件。

测试过程:向卡片发送电子钱包消费交易指令并接收响应。

5.3.3.16 电子钱包复合应用消费交易(未使用共享文件)

检测内容:检测卡片在电子钱包复合应用消费(未使用共享文件)的处理流程,电子钱包复合应用消费流程中涉及的命令(初始化复合应用消费命令、更新缓存数据命令、复合应用消费命令)。

测试条件:默认环境条件。

测试过程:向卡片发送复合应用消费指令并接收响应。

5.3.3.17 电子钱包复合应用消费交易(使用共享文件)

检测内容:检测卡片在电子钱包复合应用消费(使用共享文件)的处理流程;电子钱包复合应用消费流程中涉及的命令(初始化复合应用消费命令、更新缓存数据命令、复合应用消费命令),并结合电子现金端共享文件进行核实。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令并接收响应。

5.3.3.18 电子钱包共享余额测试

检测内容:检测卡片电子钱包应用在模拟交易流程及余额共享处理,判定卡片在进行余额改动操作后在电子现金端的同步共享。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令并接收响应同时在电子现金端发送余额读取指令。

5.3.3.19 电子钱包文件共享测试

检测内容:检测卡片电子钱包应用在模拟交易流程及文件共享处理,判定卡片在进行文件改动操作后在电子现金端的同步共享。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令和文件修改指令并接收响应然后在电子现金端进行读取。

5.3.3.20 电子现金终端或卡请求 CVM

检测内容:检测卡片的 CVM 流程,判定卡片在终端或卡片请求 CVM 时的执行情况。

测试条件:默认环境条件。

测试过程:在 CVM 流程中向卡片发送交易指令并接收响应。

5.3.3.21 电子现金检查联机处理请求

检测内容:检测在卡片或终端请求联机时的处理流程,判定卡片在终端或卡片请求联机时的执行情况。

测试条件:默认环境条件。

测试过程:在卡片或终端请求联机时向卡片发送交易指令并接收响应。

5.3.3.22 电子现金小额检查

检测内容:检测卡片小额检查流程,判定卡片小额检查的执行情况。

测试条件:默认环境条件。

测试过程:在小额检查执行过程中向卡片发送交易指令并接收响应。

5.3.3.23 电子现金小额和 CTTA 检查

检测内容:检测卡片小额和 CTTA 检查流程,判定卡片小额和 CTTA 检查的执行情况。

测试条件:默认环境条件。

测试过程:在小额和 CTTA 检查过程中向卡片发送交易指令并接收响应。

5.3.3.24 电子现金没有任何脱机选项被支持

检测内容:检测卡片在没有任何脱机选项被支持时的流程处理,判定卡片没有任何脱机选项被支持时的执行情况。

测试条件:默认环境条件。

测试过程:在没有任何脱机选项被支持时向卡片发送交易指令并接收响应。

5.3.3.25 电子现金脱机下的货币不匹配

检测内容:检测卡片的在脱机处理时处于货币不匹配状态下的处理流程,判定卡片在终端或卡片脱机交易完成时的执行情况。

测试条件:默认环境条件。

测试过程:在卡片处于货币不匹配状态下向卡片发送交易指令并接收响应。

5.3.3.26 电子现金预付

检测内容:检测卡片的电子现金预付处理流程,判定卡片的预付处理流程。

测试条件:默认环境条件。

测试过程:向支持预付的卡片发送交易指令并接收响应。

5.3.3.27 电子现金动态数据认证

检测内容:检测卡片的电子现金动态数据认证处理流程,判定卡片的动态数据认证处理流程。

测试条件:默认环境条件。

测试过程:向卡片发送触发动态数据认证的交易指令并接收响应。

5.3.3.28 电子现金闪卡测试

检测内容:检测卡片的电子现金闪卡流程,判定卡片的闪卡处理流程。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令模拟闪卡流程并接收响应。

5.3.3.29 电子现金永久锁定应用

检测内容:检测卡片在电子现金永久锁定应用状态下的处理流程。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令达到永久锁定状态,并接受卡片响应。

5.3.3.30 电子现金查询余额

检测内容:检测卡片查询电子现金余额处理流程,判定卡片查询余额的处理流程,并同时在电子钱包端与电子现金端进行核实。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令并接收响应同时在电子钱包端进行核实。

5.3.3.31 电子现金稳定性测试

检测内容:检测卡片的电子现金稳定性处理交易方面。

测试条件:默认环境条件。

测试过程:向卡片发送指定笔数脱机交易指令并接收响应。

5.3.3.32 电子现金分段扣费功能测试(未使用共享文件)

检测内容:检测卡片电子现金的分段扣费处理流程(未使用共享文件),判定卡片的分段扣费处理流程。

测试条件:默认环境条件。

测试过程:向卡片发送分段扣费交易指令(未使用共享文件)并接收响应。

5.3.3.33 电子现金分段扣费功能测试(使用共享文件)

检测内容:检测卡片电子现金的分段扣费处理流程(使用共享文件)。

测试条件:默认环境条件。

测试过程:向卡片发送分段扣费交易指令(使用共享文件)并接收响应。

5.3.3.34 电子现金脱机预授权及预授权完成功能测试

检测内容:检测卡片电子现金的脱机预授权及预授权完成处理流程。

测试条件:默认环境条件。

测试过程:向卡片发送脱机预授权及预授权完成交易指令并接收响应。

5.3.3.35 电子现金押金抵扣功能测试

检测内容:检测卡片电子现金的押金抵扣处理流程。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令实现押金抵扣功能并接收响应。

5.3.3.36 电子现金交易时间测试

检测内容:检测卡片电子现金的交易时间处理。

测试条件:默认环境条件。

测试过程:向卡片发送交易命令并接收响应,同时记录整个过程的交易时间。

5.3.3.37 电子现金增强性安全性测试

检测内容:检测卡片电子现金的安全报文,判定卡片交易执行中安全信息的生成情况。

测试条件:默认环境条件。

测试过程:向卡片发送交易命令并接收附带安全报文的卡片响应。

5.3.3.38 电子现金双币应用测试

检测内容:检测卡片在具备双币应用配置时的交易处理流程,其中应包括新增的数据元、异常响应和交易流程测试。

测试条件:默认环境条件。

测试过程:向卡片发送正常和异常的第二货币交易命令并接收响应。

5.3.3.39 电子现金共享余额测试

检测内容:检测卡片电子现金应用在模拟交易流程及余额共享处理。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令并接收响应,同时在电子钱包端进行核实。

5.3.3.40 电子现金文件共享测试

检测内容:检测卡片电子现金应用在模拟交易流程及文件共享处理。

测试条件:默认环境条件。

测试过程:向卡片发送交易指令和文件修改指令,同时在电子钱包端进行核实。

5.3.3.41 脱机交易稳定性测试

检测内容:检测卡片电子钱包、电子现金应用在脱机状态下的稳定性。

测试条件:默认环境条件。

测试过程:循环向卡片发送电子钱包和电子现金混合交易指令并接收响应。

6 SAM 卡检测

6.1 接触式电气特性和通信协议

6.1.1 一般要求

检测环境为常温 23℃ ±3℃,湿度 40% ~60%。

本章检测结果应符合 GB 16649.3 的要求。

6.1.2 电特性

6.1.2.1 卡片电阻测试

检测内容:检测 SAM 卡卡片触点的电阻。

测试条件:默认检测环境。

测试过程:使用电阻测量设备测量 SAM 卡片各管脚的电阻。

6.1.2.2 卡片在不同环境条件下的测试

检测内容:当供电电压和输入信号在允许的范围内变化时,卡片应能够正确操作。

测试条件:

a) 电压选择如下:
   1) 类型 A:5V ±0.5V;
   2) 类型 B:3V ±0.3V;
   3) 类型 C:1.8V ±0.18V。
b) 信号类型选择如下:
   1) 典型的常规平均条件;
   2) 最小时钟频率;
   3) 最大时钟频率;
   4) 最小占空比;
   5) 最大占空比;
   6) 最低供电电压加最小信号幅度;
   7) 最高供电电压加最大信号幅度;
   8) 在最大时钟频率下减缓上升和下降时间;
   9) 在最大时钟频率,最小信号幅度下减缓上升和下降时间;
   10) 在最小时钟频率,最小信号幅度下减缓上升和下降时间;
   11) 最高供电电压加最小信号幅度。

测试过程:通过设置不同的电压和输入信号组合,并监控卡片的功能响应。

6.1.2.3 卡片在传输模式下的高低电压测试

检测内容:检测 I/O 触点在传输模式下信号的高低电压。

测试条件:默认检测环境。

$$V_{cc} = 4.5\text{V},5\text{V} \text{ 和 } 5.5\text{V}(\pm 25\text{mV})$$

V_{cc} = 2.7V,3V 和 3.3V(±15mV)

测试过程:首先进行卡片复位;然后在 ATR 字符帧传送过程中监控 VOH 和 VOL;最后对所有 V_{cc} 条件都重复上述测试。

6.1.2.4 卡片 I/O 触点在传输模式下信号的下降时间测试

检测内容:检测 I/O 触点在传输模式下信号的下降时间。

测试条件:默认检测环境。

V_{cc} = 4.5V,5V 和 5.5V(±25mV)

V_{cc} = 2.7V,3V 和 3.3V(±15mV)

测试过程:首先进行卡片复位;然后在 ATR 字符帧传送过程中测量 t_F 在 90% ~10% 点信号的下降沿;最后对所有 V_{cc} 条件都重复上述测试。

6.1.2.5 激活时序过程测试

检测内容:在一个激活时序过程中卡片正确控制 I/O 信号的时序。

测试条件:默认检测环境。

V_{cc} = 4.5V,5V 和 5.5V(±25mV)

V_{cc} = 2.7V,3V 和 3.3V(±15mV)

测试过程:通过发送正常的激活时序并记录相关时间。

6.1.2.6 复位应答测试

检测内容:卡复位应答相关参数。

测试条件:默认检测环境。

测试过程:通过发送冷热复位信号,截取相关的时间参数和 ATR 响应间隔。

6.1.2.7 字符传输测试

检测内容:卡片返回的字符中每一位和字符持续时间在本规范规定范围,同时卡片应能正确处理位持续时间和总的持续时间达到规定的边界值的字符。

测试条件:默认检测环境。

测试过程:通过正常流程信号,截取相关的时间参数和字符响应间隔。

6.1.3 通信协议

6.1.3.1 T=0 协议

检测内容:检测卡片 T=0 协议。

测试条件:支持 T=0 协议的卡片。

测试过程:按照表 4 的测试项目对卡片进行逐项测试。

表 4 T=0 协议测试项目

序 号	测 试 项 目
1	卡片发送的同向字符间隔测试
2	卡片从终端接收到字符同返回字符间的时间间隔测试
3	字节接口(1)定的字符间的最小时间间隔测试
4	接收时的最小保护时间测试
5	过程字节的传输测试
6	命令情况 2 正常流程测试
7	命令情况 2 的 L_e > 卡响应数据测试

表 4（续）

序　号	测 试 项 目
8	命令情况 2 的 L_e = 卡响应数据测试
9	命令情况 2 的 L_e < 卡响应数据测试
10	卡传输时单次字符循环发送测试
11	卡传输时多次字符循环发送测试
12	卡接收时单次字符循环发送测试
13	卡接收时多次字符循环发送测试

6.1.3.2　T = 1 协议

检测内容：检测卡片 T = 1 协议。

测试条件：支持 T = 1 协议的卡片。

测试过程：按照表 5 的测试项目对卡片进行逐项测试。

表 5　T = 1 协议测试项目

序　号	测 试 项 目
1	同向最小字符间隔的接收测试
2	同向最大字符间隔的接收测试（CWT）
3	反向最小字符间隔的接收测试（BGT）
4	反向最大字符间隔的接收测试（BGT）
5	来自卡的最小标准字符间隔测试
6	来自卡的最大标准字符间隔测试
7	块保护时间测试
8	I 块序列号测试
9	LRC 错误测试
10	奇偶校验错误测试
11	S 块的单次纠错测试
12	I 块的单次纠错测试（seq = 0）
13	I 块的单次纠错测试（seq = 1）
14	S 块的多次纠错测试
15	I 块的多次纠错测试（seq = 0）
16	I 块的多次纠错测试（seq = 1）
17	传输错误次数超出测试
18	来自卡的 S 块单次重发测试
19	来自卡的 I 块单次重发测试
20	命令结构错误测试（seq = 0）- PCB = C5 INF = 10
21	命令结构错误测试（seq = 0）- PCB = E5 INF = 10
22	命令结构错误测试（seq = 0）- PCB b7 = 1

表5（续）

序　号	测 试 项 目
23	命令结构错误测试(seq=0) – R 块 PCB b5=0
24	命令结构错误测试(seq=0) – R 块 LEN=1
25	命令结构错误测试(seq=0) – I 块 NAD=01
26	命令结构错误测试(seq=1) – PCB=C5 INF=10
27	命令结构错误测试(seq=1) – PCB=E5 INF=10
28	命令结构错误测试(seq=1) – PCB b7=1
29	命令结构错误测试(seq=1) – R 块 PCB b5=0
30	命令结构错误测试(seq=1) – R 块 LEN=1
31	命令结构错误测试(seq=1) – I 块 PCB b5=0
32	字符超出的命令结构错误测试
33	特定 11 测试

6.2　应用功能

6.2.1　一般要求

检测环境为常温 23℃ ±3℃。

本章检测项目应符合 JT/T 978.3 的相关要求。

6.2.2　功能检测

6.2.2.1　INIT_FOR_DESCRYPT 命令

检测内容:检测 SAM 卡的卡片 INIT_FOR_DESCRYPT 命令和执行流程。

测试条件:默认检测环境。

测试过程:向卡片发送正常和异常的 INIT_FOR_DESCRYPT 命令并接收卡片响应。

6.2.2.2　DES CRYPT 命令

检测内容:检测 SAM 卡的卡片 DES CRYPT 命令和执行流程。

测试条件:默认检测环境。

测试过程:向卡片发送正常和异常的 DES CRYPT 命令并接收卡片响应。

7　终端检测

7.1　非接触电气特性和通信协议

7.1.1　一般要求

检测环境为常温 23℃ ±3℃,湿度 40% ~60%。

本章检测项目应符合 JT/T 978.5 的要求。

7.1.2　电气特性

7.1.2.1　PCD 场强测试

检测内容:检测终端的 PCD 场强。

测试条件:默认检测环境。

测试过程:开启终端并将终端设置为场强打开状态,使用场强探测仪在非接触检测环境下对终端的场强进行测量并记录。

7.1.2.2 载波频率测试

检测内容:检测终端的载波频率。

测试条件:默认检测环境。

测试过程:开启终端并将终端设置为场强打开状态,使用非接触探测设备在非接触检测环境下对终端的载波频率进行波形截取。

7.1.2.3 场复位测试

检测内容:检测终端复位时的场强和复位时间。

测试条件:默认检测环境,并且终端支持连续复位模式。

测试过程:开启终端,将中断设置为循环复位状态,使用非接触探测设备在终端复位过程中截取终端发出的复位波形,测量复位期间的幅值和低电平的持续时间。

7.1.2.4 Type A、Type B 通信的 PCD 到 PICC 波形测试

检测内容:检测终端的 Type A 波形的 $t_1 \sim t_4$ 时间,验证 $V_4 \sim V_2$ 单调下降和上升应符合要求,检测波形上冲和下冲时间。检测 Type B 波形的负载调试幅度和上升下降沿时间。

测试条件:默认检测环境,并且终端支持循环寻卡模式。

测试过程:在非接触检测环境下对终端的发出的 Type A 波形的 1 时间和单调性进行截取,对 Type B 终端的负载调试幅度的上升下降沿时间进行测量并记录。

7.1.2.5 验证最小调制下的负载调制接收灵敏度测试

检测内容:当测试 PICC 距离被测设备天线平面不大于 2cm 时,应用最小负载调制特性时的 PCD 功能状态。

测试条件:默认检测环境,并且终端支持循环寻卡模式。

测试过程:在非接触检测环境下对终端的发出的 Type A、Type B 波进行响应,验证 PCD 在测试 PICC 应用最小负载调制特性时功能。

7.1.2.6 验证最大调制下的负载调制接收灵敏度测试

检测内容:当测试 PICC 距离被测设备天线平面距离大于 2cm 时,应用最大负载调制特性时的 PCD 功能状态。

测试条件:默认检测环境,并且终端支持循环寻卡模式。

测试过程:在非接触检测环境下对终端的发出的 Type A、Type B 波进行响应,验证 PCD 应在测试 PICC 应用最大负载调制特性时功能正常。

7.1.2.7 Type A、Type B 通信的比特电平编码信号接口测试

检测内容:在初始化期间 PCD 到 PICC 的比特率和比特编码同步情况。

测试条件:默认检测环境,并且终端支持循环寻卡模式。

测试过程:在非接触检测环境下对终端的发出的 Type A、Type B 波形进行测量,确定波形速率是否符合规范。

7.1.3 通信协议

7.1.3.1 Type A 测试

检测内容:检测终端的 Type A 协议。

测试条件:支持 Type A 的终端。

测试过程:在非接触检测环境下对终端的 Type A 协议功能按照表 6 所示测试项目进行逐项检测。

表 6　Type A 功能测试项目

序　号	测 试 项 目
1	轮询的执行及时间验证
2	基本的 Type A 交互和时间测量
3	Type A 正确的移出测试
4	基本的 Type A 交互,使用最小或最大的 FDT 测试
5	2 级和 3 级长度的 UID 测试
6	支持的 ATQA 的值测试
7	支持的各种长度的历史字节测试
8	支持的 SFGI 测试
9	支持的 TC 测试
10	对 HALT 命令的 Type A 帧应答测试
11	ATQA 的不同值测试
12	可能情况下的 FWT 下的非链接 I 块交互测试
13	FSC = 256 字节的链接块传输测试
14	FSC = 16 – 128 字节的链接块传输测试
15	非链接 I 块,对帧等待时间扩展的请求处理测试
16	链接 I 块,对帧等待时间扩展的请求处理测试
17	长度不规则情况下链接 I 块处理测试
18	最小帧延迟时间情况下的时序处理测试
19	WUPA 响应错误的处理测试
20	ANTICOLLISION CL1 后错误处理测试
21	轮询到 1 个 Type A 卡和 1 个 Type B 卡测试
22	冲突探测 WUPA 后一个错误测试
23	冲突探测 SELECT CL1 后一个错误测试
24	激活 RATS 后错误测试测试
25	激活 RATS 响应带噪声测试
26	冲突探测 ANTICOLLISION CL1 后超时测试
27	冲突探测 WUPA 后超时测试
28	冲突探测 SELECT CL1 后超时测试
29	激活 RATS 后超时测试
30	忽略所有传输错误并在 RECOVERY 时间内接受正确的序列测试
31	激活 RATS 后遵守不回应期测试
32	非链接 I 块的错误通知测试
33	非链接 I 块响应超时测试
34	非链接 I 块响应传输错误测试

表6（续）

序　号	测 试 项 目
35	非链接I块响应协议错误测试
36	链接I块错误通知测试
37	链接I块响应超时测试
38	链接I块响应传输错误测试
39	链接I块响应协议错误测试
40	R(ACK)块后超时测试
41	R(ACK)响应传输错误测试
42	R(ACK)响应协议错误测试
43	S(WTX)响应块后超时测试
44	S(WTX)请求后再次使用FWT扩展测试
45	非链接I块响应带噪声测试
46	链接I块响应带噪声测试
47	R(ACK)块响应带噪声测试
48	R(NAK)指出传输错误的响应协议错测试
49	移出后WUPA响应错测试
50	S(WTX)响应块后连续超时测试
51	忽略所有传输错误并在1 280/f_c时间内接受正确的序列测试
52	Type A协议下的不响应时间测试

7.1.3.2 Type B测试

检测内容：检测终端的Type B协议。

测试条件：支持Type B协议的终端。

测试过程：在非接触检测环境下对终端的Type B协议功能按照表7所示测试项目进行逐项检测。

表7　Type B功能测试项目

序　号	测 试 项 目
1	Type B预测确定TR1最小值测试
2	基本的Type B交互和时间测量测试
3	Type B使用支持的SOF和EOF交互测试
4	Type B正确的移出测试
5	基本的Type B交互，使用最小或最大的FDT测试
6	基本的Type B交互，使用最小或最大的字符间延迟测试
7	支持的ADC值测试
8	支持的FO值测试
9	支持的位速率测试
10	支持的ADF值测试

表 7（续）

序　号	测 试 项 目
11	支持的 ATQB 中协议类型 b4 – b2 值测试
12	支持的 ATTRIB 响应中 MBLI 的值测试
13	不同的 ATQB 值测试
14	可能的 FWT 值下的非链接 I 块交互测试
15	FSC = 256 双方向链接块传输测试
16	FSC = 16 – 128 字节链接块传输测试
17	非链接 I 块，对帧等待时间扩展的请求处理测试
18	链接 I 块，对帧等待时间扩展的请求处理测试
19	长度不规则情况下链接 I 块处理测试
20	最小帧延迟时间情况下的时序处理测试
21	WUPB 响应错误的处理测试
22	轮询，探测到一个 Type B 卡然后探测一个 Type A 卡
23	冲突探测 WUPB 响应错误测试
24	激活，ATTRIB 响应带噪声测试
25	激活，ATTRIB 响应错误测试
26	冲突探测，WUPB 后超时测试
27	激活，ATTRIB 响应超时测试
28	忽略所有传输错误并在 1 280/f_c 时间内接受正确的序列测试
29	激活 ATTRIB 后遵守不回应期测试
30	非链接 I 块的错误通知测试
31	非链接 I 块响应超时测试
32	非链接 I 块响应传输错误测试
33	非链接 I 块响应协议错误测试
34	链接 I 块错误通知测试
35	链接 I 块响应超时测试
36	链接 I 块响应传输错误测试
37	链接 I 块响应协议错误测试
38	R(ACK)块后超时测试
39	R(ACK)响应传输错误测试
40	R(ACK)响应协议错误测试
41	S(WTX)响应块后超时测试
42	S(WTX)请求后再次使用 FWT 扩展测试
43	非链接 I 块对噪声响应的处理测试
44	带链接 I 块对噪声响应的处理测试

表 7（续）

序　号	测 试 项 目
45	R(ACK)块对噪声响应的处理测试
46	R(NAK)指出传输错误的响应协议错测试
47	移出,WUPB 响应错测试
48	S(WTX)响应块后连续超时测试
49	忽略所有传输错误并在 1 280/f_c 时间内接受正确的序列测试
50	Type B 协议下的不响应时间测试

7.2　应用功能

7.2.1　一般要求

检测环境为常温 23℃ ±3℃。

本章检测项目应符合 JT/T 978.2 和 JT/T 978.3 的要求。

7.2.2　数据元和命令

检测内容:检测终端对数据元和命令的支持情况。

测试条件:默认检测环境。

测试过程:选择卡片应用,按照表 8 中所示数据元和命令测试项目进行检测。

表 8　数据元和命令测试项目

序　号	测 试 项 目
1	数据元的存储
2	TLV 中的长度编码
3	DOL 对象处理
4	EXTERNAL AUTHENTICATE 状态码的处理
5	GET DATA 命令的处理
6	GET PROCESSING OPTIONS 的正常和异常处理
7	READ RECORD 的处理
8	SELECT 命令的处理
9	RFU 字节和位的编码
10	GENERATE AC 返回的数据域的格式
11	密文信息数据处理
12	CVM 列表处理
13	发卡机构脚本命令最大数据长度
14	来自终端或者发卡机构的数据
15	来自 SELECT ADF 的 FCI 中的自定义数据的响应
16	最小数据长度

表 8（续）

序　号	测 试 项 目
17	扩展应用中使用到的 CAPP 交易指示位、分段扣费应用标识、电子现金分段扣费抵扣限额、电子现金分段扣费已抵扣额支持性测试
18	READ CAPP DATA 命令处理
19	UPDATE CAPP DATA CACHE 命令处理
20	APPEND RECORD 命令处理
21	GET TRANS PROVE 命令处理

7.2.3　应用选择

检测内容：检测终端对应用选择的处理支持情况。

测试条件：默认检测环境。

测试过程：选择卡片应用，按照表 9 所示终端检测应用项目进行逐项检测。

表 9　终端检测应用项目

序　号	测 试 项 目
1	PPSE 的定义
2	支付系统目录中记录的定义
3	终端支持的应用列表
4	AID 的匹配
5	表明记录结束
6	目录入口定义
7	部分匹配的候选列表
8	部分匹配选择下一个应用
9	AID 列表选择
10	DF 名称的异常测试
11	不同情况下的最终选择测试
12	支持应用显示
13	来自候选列表的最终应用选择

7.2.4　密钥安全检测项目

检测内容：检测终端对密钥的选择和加密解密安全方面的处理支持情况。

测试条件：默认检测环境。

测试过程：选择卡片应用，按照表 10 所示的密钥安全检测项目进行逐项检测。

表 10　密钥安全检测项目

序　号	测 试 项 目
1	证书密钥相关参数测试
2	不同类型的密钥数据缺失测试
3	不同类型的证书恢复失败测试
4	证书内容异常情况下的处理过程测试
5	签名和验签的正常和异常测试
6	哈希数据的正常和异常验证测试

7.2.5　数据对象

检测内容:检测终端不同类型的数据对象支持情况。

测试条件:默认检测环境。

测试过程:选择卡片应用,执行交易检测终端对表 11 所示类型的数据对象进行逐项检测。

表 11　数 据 对 象

序　号	测 试 项 目
1	长度域:1 字节
2	长度域:2 字节
3	在 an(字母数字)格式的数据对象中“空格”字符的识别
4	应用选择时接受卡片中格式错误的应用选择数据对象

7.2.6　认可的加密算法

检测内容:检测终端不同类型的加密算法的支持情况。

测试条件:默认检测环境。

测试过程:选择卡片应用,执行交易模拟终端对不同类型的加密算法的执行情况,同时针对支持多种算法的终端也按照上述过程进行逐项算法测试。

7.2.7　交易接口文件

检测内容:检测终端对交易接口文件的读取处理情况。

测试条件:默认检测环境。

测试过程:选择卡片应用,执行交易并记录终端对不同类型的交易接口文件的处理结果。

7.2.8　交易流程检测项

检测内容:检测终端对交易过程中的流程处理情况。

测试条件:默认检测环境。

测试过程:选择卡片应用,按照表 12 所示的检测项目对检测终端交易流程进行逐项检测。

表 12　交易流程检测项目

序　号	测 试 项 目
1	初始 TSI 和 TVR 的设置
2	DOL 数据处理流程
3	GPO 流程处理
4	READ RECORD 命令的执行
5	数据对象的处理
6	记录的数据格式
7	处理输入数据的规则
8	AUC 处理限制
9	CVM 处理
10	各类限制寄存器的处理
11	发卡机构脚本处理
12	终端行为分析
13	分段扣费流程处理
14	脱机预授权交易流程处理

7.2.9　生成应用密文命令编码

检测内容:检测终端对交易过程中 GAC 密文的处理情况。

测试条件:默认检测环境。

测试过程:选择卡片应用,执行交易并记录终端交易过程中不同情况下的 GAC 处理结果。

7.2.10　卡片中错误和数据缺失检测项目

检测内容:检测终端在卡片出现缺少数据和内部数据错误情况下的支持。

测试条件:默认检测环境。

测试过程:选择卡片应用,按照表 13 所示卡片中的错误和数据缺失检测项目进行逐项检测。

表 13　卡片中的错误和数据缺失检测项目

序　号	测 试 项 目
1	必备数据对象丢失:FCI、DF、SFI、AFL、AIP、CDOL1、CDOL2、PAN 等
2	各类密钥及证书相关数据缺失
3	结构数据对象无法正常解析
4	GENERATE AC 响应中强制数据缺失

7.2.11　终端总体检测

检测内容:检测终端在不同商户要求情况下的处理情况。

测试条件:默认检测环境。

测试过程:执行交易并在交易过程中使用不同商户的配置要求并记录检测终端响应。

7.2.12 软件体系结构

检测内容:检测终端软件体系结构。

测试条件:默认检测环境。

测试过程:选择卡片应用,执行交易并在终端数据元的初始化、支持语言和失败显示错误信息情况下记录终端响应。

7.2.13 持卡人和商户界面

检测内容:检测终端在不同情况下的界面显示情况。

测试条件:默认检测环境。

测试过程:选择卡片应用,执行交易并查看检测终端对不同情况下的商户显示界面内容。

7.2.14 终端数据元的编码

检测内容:检测终端必备数据元编码。

测试条件:默认检测环境。

测试过程:选择卡片应用,执行交易并按照表 14 所示的数据元编码检测项目对终端进行逐项测试。

表 14 数据元编码检测项目

序 号	测 试 项 目
1	终端类型
2	终端性能
3	终端附加性能
4	账户类型

7.2.15 综合测试

检测内容:检测终端在不同交易流程下的处理流程。

测试条件:默认检测环境。

测试过程:选择卡片应用,执行交易并检测终端对不同交易流程下的处理。

7.2.16 补充测试

检测内容:检测终端在特殊规定情况下的处理流程。

测试条件:默认检测环境。

测试过程:选择卡片应用,按照表 15 所示的异常交流检测项目对终端进行逐项测试。

表 15 异常交易流程检测项目

序 号	测 试 项 目
1	持卡人证件出示验证,身份证
2	持卡人证件出示验证,PIN 验认证失败,执行下一个
3	核对持卡人证件失败,执行下一个
4	持卡人证件出示,护照

表 15（续）

序　号	测 试 项 目
5	持卡人证件出示,军官证
6	读交易明细
7	终端性能:持卡人证件验证位的置位
8	密文传输:从外置密码键盘到终端
9	持卡人姓名扩展
10	圈存日志读取
11	脱机交易时间

8　系统检测

8.1　一般要求

被检测的系统应为实际生产系统或准生产系统。

本章检测项目应符合 GB/T 28035 及 JT/T 978.4 的要求。

8.2　文件接口

8.2.1　文件名称检测

检测内容:检测系统各类文件名称。

测试条件:默认检测环境和相关设计文档。

测试过程:查看相关设计文档,查看相关交易、清算和反馈文件。

8.2.2　文件记录格式

检测内容:检测系统交易明细文件记录格式。

测试条件:默认检测环境和相关设计文档。

测试过程:查看相关设计文档,查看相关交易、清算和反馈文件。

8.2.3　文件类型测试

检测内容:检测系统各类文件记录类型。

测试条件:默认检测环境和相关设计文档。

测试过程:查看相关设计文档,查看相关交易、清算和其他文件。

8.2.4　文件结构测试

检测内容:检测系统各类文件记录结构。

测试条件:默认检测环境和相关设计文档。

测试过程:查看相关设计文档,查看相关交易、清算和其他文件。

8.2.5　报文结构检测

检测内容:检测系统查看报文结构。

测试条件:默认检测环境和相关设计文档。

测试过程:查看相关设计文档,模拟交易并查看报文头及报文结构。

8.2.6 报文格式检测

检测内容:检测系统查看报文格式。
测试条件:默认检测环境和相关设计文档。
测试过程:查看相关设计文档,模拟交易并查看报文格式。

8.3 通信接口

8.3.1 接口方式检测

检测内容:检测系统查看通信接口的网络接口、通信接口方式。
测试条件:默认检测环境和相关设计文档。
测试过程:查看相关设计文档,查看实际接口环境。

8.3.2 接口运行检测

检测内容:查看通信接口的网络接口、通信接口的运行效果和传送文件的格式。
测试条件:默认检测环境和相关设计文档。
测试过程:查看相关设计文档,查看实际接口环境,使用接口传送文件并查看。

附 录 A
（资料性附录）
卡片应用送检示例

A.1 技术准备

A.1.1 送检卡片个人化建议

在送检时声明卡片实际支持的算法类型。支持不同算法类型中卡片 PDOL 数据的不同，同时要将 PPSE 相关数据个人化至卡片中，以满足现行规范中非接触界面应用选择的要求。

A.1.2 卡片送检方式

可以选择以下两种方式的其中一种进行送检。

A.1.2.1 方式一

提交卡片个人化工具（软件或者装有该软件的笔记本电脑），并且参见 A.2 的个人化数据示例，将不同的个人化情况事先加入个人化工具中，测试时检测方可通过选择各种个人化配置对卡片进行个人化。

A.1.2.2 方式二

在不提供个人化工具的情况下，将送检样卡参见 A.2 的个人化数据要求，分别做好个人化，并在卡片上标记好对应的个人化的配置号。

A.2 个人化数据示例

A.2.1 概述

根据卡片功能的不同可能不需要支持本部分中列出的全部卡片特征。支持不同功能的卡片所应支持的卡片特征见表 A.1。

表 A.1 卡片支持的功能与卡片特征的对应关系

卡片支持的应用	送检时应准备的卡片特征
仅支持国际算法的卡片	
脱机交易应用	卡片特征 31～45，卡片特征 48～49
脱机交易扩展应用	卡片特征 31～49
非接触式联机交易应用	卡片特征 1～26（加入 PPSE 并采用非接触界面下的 PDOL 个人化数据）
仅支持国密算法的卡片	
脱机交易应用	卡片特征 31～45，卡片特征 48～49
脱机交易扩展应用	卡片特征 31～47
非接触式联机交易应用	卡片特征 1～26（加入 PPSE 并采用非接触界面下支持国密算法的 PDOL 个人化数据）
支持国际算法和国密算法的卡片	
脱机交易	卡片特征 31～45，卡片特征 48～49
脱机交易扩展	卡片特征 31～49
非接触式联机交易应用	卡片特征 1～28（与仅支持国密算法的卡片特征相比加入了国际对称与非对称算法相关的必备数据）

A.2.2 基本特征

A.2.2.1 联机交易应用测试基本特征

表 A.2 列出了支持联机交易应用功能的卡片基本特征,数据分组可自行设计,但除 SFI = 1 的文件的 1 号记录外,SFI 1 的 1 号记录可存储以下数据:

70 13 57 11 38 88 88 01 00 00 11 17 D3 01 22 01 01 23 45 67 89

表 A.2 联机应用卡片基本特征

数据元素	标签	数值
应用货币代码	9F51	01 56
应用货币代码	9F42	01 56
应用生效日期	5F25	14 06 12
应用失效日期	5F24	99 12 31
应用标识符	4F	A0 00 00 06 32 01 01
应用首选名称	9F12	43 41 52 44 20 49 4D 41 47 45 20 30 30 30 31
应用优先指示器	87	01
应用用途控制	9F07	FF C0
应用版本号	9F08	00 30
CDOL1	8C	9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9F 21 03 9C 01 9F 37 04
CDOL2	8D	8A 02 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9F 21 03 9C 01 9F 37 04
持卡人姓名	5F20	46 55 4C 4C 20 46 55 4E 43 54 49 4F 4E 41 4C
CVM 列表	8E	00 00 00 00 00 00 00 00 41 03 42 03 5E 03 43 03 1F 00
根公钥模索引	8F	xx
连续交易计数器(国际)		00
连续交易限制数(国际)	9F53	05
连续交易计数器(国际—国家)		00
连续交易限制数(国际—国家)	9F72	00
密文版本号		01
累计交易金额		00 00 00 00 00 00
累计交易金额限制数	9F54	00 00 00 01 00 00
数据认证代码		DA C1
分散密钥索引		01
发卡机构行为代码—缺省	9F0D	F0 20 04 00 00
发卡机构行为代码—拒绝	9F0E	00 50 88 00 00
发卡机构行为代码—联机	9F0F	F0 20 04 98 00
发卡机构应用数据	9F10	07 01 01 03 00 00 00 xx

表 A.2（续）

数 据 元 素	标 签	数 值
发卡机构认证指示位	9F56	80
发卡机构代码表索引	9F11	01
发卡机构国家代码	5F28	01 56
发卡机构国家代码	9F57	01 56
首选语言	5F2D	7A 68 65 6E 66 72 64 65
日志入口	9F4D	0B 0A
日志格式	9F4F	9A 03 9F 21 03 9F 02 06 9F 03 06 9F 1A 02 5F 2A 02 9F 4E 14 9C 01 9F 36 02
联机授权指示位		00
PDOL 非接触界面(若卡片不支持国密算法)	9F38	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 33 03 9F 4E 14 9F 7A 01
PDOL 非接触界面(若卡片支持国密算法)	9F38	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 33 03 9F 4E 14 9F 7A 01 DF 69 01
PIN 尝试计数器	9F17	03
PIN 尝试限制数		03
PIN 数据(可选)		12 34
第二应用货币代码	9F76	00 00
服务码	5F30	02 01
预留		
产品标识信息	9F63	11 22 33 44 55 66 77 88 00 00 00 00 00 00 00 00

A.2.2.2 脱机交易应用测试基本特征

A.2.2.2.1 读记录时卡片至少应返回以下数据,以下数据至少分四条记录存储:

a) “93”——签名的静态应用数据;
b) “8F”——根公钥模索引;
c) “90”——发卡机构公钥证书;
d) “92”——发卡机构公钥余项;
e) “9F32”——发卡机构公钥指数;
f) “9F46”——卡片公钥证书;
g) “9F47”——卡片公钥指数;
h) “9F48”——卡片公钥余项;
i) “5F24”——应用失效期;
j) “5F25”——应用生效期;
k) “5A”——应用主账号;
l) “9F74”——电子现金发卡机构授权码;
m) “9F08”——应用版本号。

A.2.2.2.2 表 A.3 规定了脱机交易的基本特征;表 A.4 规定了双币脱机交易的基本特征。

表 A.3　脱机交易的基本特征表

数　据	标　签	长度（字节）	数　值
电子现金余额	9F79	06	00 00 00 01 00 00
电子现金余额上限	9F77	06	00 00 00 01 50 00
电子现金发卡机构授权码	9F74	06	45 43 43 31 31 31
电子现金单笔交易限额	9F78	06	00 00 00 00 10 00
电子现金重置阈值	9F6D	06	00 00 00 00 15 00
卡片交易属性	9F6C	02	30 00
卡片 CVM 限额	9F6B	06	00 00 00 00 05 00
PDOL 非接触式(若卡片不支持国密算法)	9F38		9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04
PDOL 非接触式(若卡片支持国密算法)	9F38		9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 DF 69 01
产品标识信息	9F63	10	11 22 33 44 55 66 77 88 00 00 00 00 00 00 00 00
连续交易限制数(国际—货币)	9F53	01	03
密文版本		01	0X01,0X17
发卡机构应用数据	9F10	0x13	07 01 01 03 00 00 00 xx 0A 01 xx xx xx xx xx yy yy yy yy yy
脱机可用余额	9F5D	06	00 00 00 00 00 01

表 A.4　双币脱机交易的基本特征表

数　据	标签	长度（字节）	数　值
第二币种电子现金应用货币代码	DF71	02	03 44
第二币种卡片 CVM 限额	DF72	06	00 00 00 00 05 00
第二币种电子现金余额	DF79	06	00 00 00 02 00 00
第二币种电子现金余额上限	DF77	06	00 00 00 03 00 00
第二币种电子现金单笔交易限额	DF78	06	00 00 00 00 20 00
第二币种电子现金重置阈值	DF76	06	00 00 00 00 30 00

A.2.2.3　扩展交易测试基本特征

A.2.2.3.1　表 A.5 规定了脱机交易扩展的基本特征。

表 A.5　脱机交易扩展的基本特征表

数 据 对 象	说　明	数　值
PDOL	密文版本 01	DF 60 01 9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04
	密文版本 17	DF 60 01 9F 66 04 9F 02 06 9F 37 04 5F 2A 02

表 A.5（续）

数 据 对 象	说　明	数　值
分段扣费应用标识 DF61	BF0C 模板	02
卡片附加处理 9F68	所有的卡片特征	Byte1 bit 8 = 1 支持小额检查
来自应用提供商、发卡机构或卡片供应商的 1 个或多个附加(专用)数据元	DF11 (前 20 字节与电子钱包 0x15 文件前 20 字节一致)	00 08 30 10 FF FF FF FF 00 00 38 88 88 01 00 00 11 17 01 00 00 00 00 00 00 00 00 00 00 00 00 00
电子现金分段扣费抵扣限额	DF62	00 00 00 00 00 00
电子现金分段扣费已抵扣额	DF63	00 00 00 00 00 00

A.2.2.3.2　支持脱机交易扩展应用的卡片还应初始化 2 个扩展应用专用文件：一个变长文件和一个循环文件。变长文件，其 SFI = 0x1A。

A.2.2.3.3　该文件至少可新开 14 条记录。每个记录不超过 128 字节，见表 A.6。

表 A.6　应用记录格式表

字　节	数 据 元	长度(字节)	数 据 格 式
1-2	记录 ID 标识	2	2701
3	记录长度	1	固定为 0x7D
4	应用有效标识	1	固定为 0x01
5-128	行业应用信息数据	124	

注 1：开通密钥：191A5F026001DF259A03019C37049F11，循环文件，其 SFI = 0x1E。

注 2：该文件包含 30 条循环记录，每个记录不超过 48 字节，开通密钥：191A5F026001DF259A03019C37049F11。

A.2.3　密钥信息

A.2.3.1　对称密钥—3DES

A.2.3.1.1　电子钱包对称密钥

电子钱包对称密钥见表 A.7。

表 A.7　电子钱包对称密钥表—3DES

密 钥 名 称	密钥值(十六进制)
圈存主密钥(MLK_01)	D3 D6 E8 83 68 32 FD D4 70 6D 06 71 BB 8B D2 8B
圈存主密钥(MLK_02)	B1 17 DE 00 7E 79 E7 86 63 4B 73 A4 83 AE 97 46
圈提主密钥(MULK_01)	E9 38 FD DA AE 9E 5C 8C E6 A1 37 B7 F1 62 E5 7E
圈提主密钥(MULK_02)	EF FA 77 3C 95 53 3A 03 71 BB A0 B2 D5 45 73 4A
消费主密钥(MPK_01)	70 E9 BE A6 97 72 3D F8 36 05 EB BC B7 C2 C7 C4
消费主密钥(MPK_02)	6F 15 3B 35 A9 7E 1B 56 A1 F8 A3 CE 7A C5 DA E2
应用解锁主密钥(MUBK)	07 C3 EA A0 99 7C E0 26 B8 62 9A 77 CC B5 AC 9A
应用锁定主密钥(MBK)	48 39 6B 19 B5 E9 76 5F DA 25 EC 5C 39 40 58 A0
应用主控密钥(MAMK)	0F 6F F9 CC 72 20 43 71 09 39 16 F9 E8 BB F0 62
TAC 主密钥(MTK)	13 8D 34 F8 4B 20 31 FF 47 9E 71 BE FF 10 7A 76

A.2.3.1.2 电子现金对称密钥

表 A.8 给出了 3DES 算法适用的对称密钥,在使用此类密钥时,无须使用 PAN 和 PANSN 分散这些密钥。

表 A.8 电子现金对称密钥表—3DES

密 钥 名 称	密钥值(十六进制)
应用密文密钥	11 22 33 44 00 66 77 88 11 22 33 44 55 00 77 88
安全报文认证(MAC)密钥	8B 4F 85 4F 08 31 FB F2 63 5A 21 2E 4D DD B9 2A
安全报文加密密钥	11 22 00 44 55 66 77 88 11 22 33 00 55 66 77 88

A.2.3.2 对称密钥—SM4

表 A.9 描述了 SM4 算法适用的对称密钥,在使用此类密钥时,无须使用 PAN 和 PANSN 分散这些密钥。

表 A.9 电子现金对称密钥表—SM4

密 钥 名 称	密钥值(十六进制)
应用密文密钥	11 22 33 44 00 66 77 88 11 22 33 44 55 00 77 88
安全报文认证(MAC)密钥	8B 4F 85 4F 08 31 FB F2 63 5A 21 2E 4D DD B9 2A
安全报文加密密钥	11 22 00 44 55 66 77 88 11 22 33 00 55 66 77 88

A.2.3.3 发卡机构公私钥对及证书

按照 JT/T 978.2 卡片规范的要求进行公私钥对和证书的个人化。

A.2.3.4 卡片公钥证书和卡片公钥余项

无须计算卡片公钥证书(tag“9F46”)和卡片公钥余项(tag“9F48”),只需写入与卡片公钥的模的长度相等的卡片公钥证书和任意值的卡片公钥余项。

A.2.3.5 签名的静态应用数据

无须计算签名的静态应用数据(tag“93”),只需写入与发卡机构公钥的模的长度相等的签名的静态应用数据(tag“93”)。

A.2.4 电子现金卡片特征与密钥信息的对应关系

电子现金卡片特征与密钥信息的对应关系见表 A.10。

表 A.10 密 钥 对 应 表

卡片特征	采用算法	发卡机构公私钥对	卡片公私钥对	对称密钥
1	仅支持国际算法	RSA 1024 位	RSA 1024 位	3DES,见 A.2.3.1.2
2		RSA 1024 位	RSA 1024 位	3DES,见 A.2.3.1.2
3		RSA 1152 位	RSA 1152 位	3DES,见 A.2.3.1.2
4		RSA 1408 位	RSA 1408 位	3DES,见 A.2.3.1.2
5		RSA 1984 位	RSA 1976 位	3DES,见 A.2.3.1.2
6		RSA 1024 位	RSA 1024 位	3DES,见 A.2.3.1.2
7		RSA 1152 位	RSA 1152 位	3DES,见 A.2.3.1.2

表 10（续）

卡片特征	采用算法	发卡机构公私钥对	卡片公私钥对	对称密钥
8	仅支持国际算法	RSA 1408 位	RSA 1408 位	3DES,见 A.2.3.1.2
9		RSA 1984 位	RSA 1976 位	3DES,见 A.2.3.1.2
10～27		RSA 1024 位	RSA 1024 位	3DES,见 A.2.3.1.2
1～27	仅支持国密算法	SM2—推荐曲线—索引 57	SM2—推荐曲线—索引 57	SM4,见 A.2.3.2
1	支持双算法	RSA 1024 位 SM2—推荐曲线—索引 57	RSA 1024 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
2		RSA 1024 位 SM2—推荐曲线—索引 57	RSA 1024 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
3		RSA 1152 位 SM2—推荐曲线—索引 57	RSA 1152 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
4		RSA 1408 位 SM2—推荐曲线—索引 57	RSA 1408 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
5		RSA 1984 位 SM2—推荐曲线—索引 57	RSA 1976 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
6		RSA 1024 位 SM2—推荐曲线—索引 57	RSA 1024 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
7		RSA 1152 位 SM2—推荐曲线—索引 57	RSA 1152 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
8		RSA 1408 位 SM2—推荐曲线—索引 57	RSA 1408 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
9		RSA 1984 位 SM2—推荐曲线—索引 57	RSA 1976 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
10～26		RSA 1024 位 SM2—推荐曲线—索引 57	RSA 1024 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2 SM4,见 A.2.3.2
27		RSA 1024 位 SM2—推荐曲线—索引 57	RSA 1024 位 SM2—推荐曲线—索引 57	SM4,见 A.2.3.2
28		RSA 1024 位 SM2—推荐曲线—索引 57	RSA 1024 位 SM2—推荐曲线—索引 57	3DES,见 A.2.3.1.2
31	支持国际算法	RSA 1152 位	RSA 768 位	3DES,见 A.2.3.1.2
32				
33			RSA 1024 位	
34				
35				
36				
37		RSA 1152 位	RSA 1152 位	
38				
39		RSA 1408 位	RSA 1280 位	
40				
41		RSA 1984 位	RSA 1976 位	

表 10（续）

卡片特征	采用算法	发卡机构公私钥对	卡片公私钥对	对称密钥
42	支持国际算法	RSA 1024 位	RSA 1024 位	
43				
44				
45				
46				
47		RSA 1024 位	RSA 1024 位	3DES,见 A.2.3.1.2
48		RSA 1024 位	RSA 1408 位	3DES,见 A.2.3.1.2
49		1984 位	1984 位	3DES,见 A.2.3.1.2
31～49	仅支持国密算法	SM2—推荐曲线—索引 57	SM2—推荐曲线—索引 57	SM4,见 A.2.3.2
31～43	支持双算法	同时具备上述“仅支持国际算法”的密钥和“仅支持国密算法”的密钥		
44		同时具备上述“仅支持国际算法”的密钥和“仅支持国密算法”的密钥		SM4,见 A.2.3.2
45				3DES,见 A.2.3.1.2
46～49		同时具备上述“仅支持国际算法”的密钥和“仅支持国密算法”的密钥		

A.2.5 电子现金卡片特征

A.2.5.1 卡片特征 1～19

对卡片个人化特征 1,SFI 4 的 1 号记录应存储以下数据:70 08 9F 14 01 03 9F 23 01 07;卡片特征 1～19 见表 A.11。

表 A.11 卡片特征 1 ～19

应用首选名称“9F12”	AIP“82”	ADA“9F52”	发卡机构认证指示位“9F56”	连续脱机交易下限“9F58”	连续脱机交易上限“9F59”
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 31 卡片特征 1	5C 00 a) 支持 SDA; b) 支持持卡人认证; c) 执行终端风险管理; d) 支持发卡机构认证	82 40 a) 如果发卡机构认证失败,下次联机交易; b) 如果是新卡,联机交易; c) 如果在前次交易中 PIN 尝试次数超限,拒绝交易	80 ——强制	00	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 32 卡片特征 2	58 00 a) 支持 SDA; b) 支持持卡人认证; c) 执行终端风险管理	82 40 a) 如果发卡机构认证失败,下次联机交易; b) 如果是新卡,联机交易; c) 如果在前次交易中 PIN 尝试次数超限,拒绝交易	N/A	03	07

表 A.11（续）

应用首选名称“9F12”	AIP“82”	ADA“9F52”	发卡机构认证指示位“9F56”	连续脱机交易下限“9F58”	连续脱机交易上限“9F59”
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 33 卡片特征 3	7C 00 a) 支持 SDA； b) 支持 DDA； c) 支持持卡人认证； d) 执行终端风险管理； e) 支持发卡机构认证	82 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	00 ——可选	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 34 卡片特征 4	7C 00 a) 支持 SDA； b) 支持 DDA； c) 支持持卡人认证； d) 执行终端风险管理； e) 支持发卡机构认证	1E 40 a) 如果交易拒绝脱机执行，生成通知； b) 如果在本次交易中 PIN 尝试次数超出而且交易拒绝，生成通知； c) 如果因为发卡机构认证失败或没有执行导致交易拒绝，生成通知； d) 如果是新卡，联机交易； e) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 36 卡片特征 6	7C 00 a) 支持 SDA； b) 支持 DDA；—支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	82 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	00	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 37 卡片特征 7	7D 00 a) 支持 SDA； b) 支持 DDA； c) 支持持卡人认证； d) 执行终端风险管理； e) 支持发卡机构认证； f) 支持复合 CDA 过程中的 GENERATE AC	82 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	09	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 38 卡片特征 8	7D 00 a) 支持 SDA； b) 支持 DDA； c) 支持持卡人认证； d) 执行终端风险管理； e) 支持发卡机构认证； f) 支持复合 CDA-GENERATE AC	80 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	00 ——可选	03	09

表 A.11（续）

应用首选名称“9F12”	AIP“82”	ADA“9F52”	发卡机构认证指示位“9F56”	连续脱机交易下限“9F58”	连续脱机交易上限“9F59”
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 39 卡片特征 9	79 00 a) 支持 SDA； b) 支持 DDA； c) 支持持卡人认证； d) 执行终端风险管理； e) 支持复合 CDA-GENERATE AC	80 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	N/A	09	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 30 卡片特征 10	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	80 00 如果发卡机构认证失败，下次联机交易	80 ——强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 31 卡片特征 11	1C 00 a) 支持持卡人认证； b) 执行终端风险管理； c) 支持发卡机构认证	82 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 32 卡片特征 12	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	C2 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果发卡机构认证执行但失败，拒绝交易； c) 如果是新卡，联机交易； d) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	09	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 33 卡片特征 13	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	C6 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果发卡机构认证执行但失败，拒绝交易； c) 如果因为发卡机构认证失败或没有执行导致交易拒绝，生成通知； d) 如果是新卡，联机交易； e) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	03	07

表 A.11（续）

应用首选名称“9F12”	AIP“82”	ADA“9F52”	发卡机构认证指示位“9F56”	连续脱机交易下限“9F58”	连续脱机交易上限“9F59”
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 34 卡片特征 14	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	92 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果交易拒绝脱机执行，生成通知； c) 如果是新卡，联机交易； d) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 35 卡片特征 15	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	82 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	03	00
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 36 卡片特征 16	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	83 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果是新卡，当交易无法联机时拒绝交易； d) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 37 卡片特征 17	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	82 30 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果在前次交易中 PIN 尝试次数超限，拒绝交易； d) 如果在前次交易中 PIN 尝试次数超限，当交易无法联机时拒绝交易	80 ——强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 38 卡片特征 18	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	93 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果交易拒绝脱机执行，生成通知； c) 如果是新卡，联机交易； d) 如果是新卡，当交易无法联机时拒绝交易； e) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	03	07

表 A.11（续）

应用首选名称“9F12”	AIP“82”	ADA“9F52”	发卡机构认证指示位“9F56”	连续脱机交易下限“9F58”	连续脱机交易上限“9F59”
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 39 卡片特征 19	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	82 C0 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果在本次交易中 PIN 尝试次数超限，应用锁定； d) 如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 ——强制	03	07

A.2.5.2 卡片特征 20

卡片特征 20 见表 A.12。

表 A.12 卡 片 特 征 20

数 据 元 素				值			
连续脱机交易下限 9F58				0F			
连续脱机交易上限 9F59				0F			
连续交易限制数（国际）9F53				0F			
累计交易金额限制数 9F54				000099999999			
累计交易金额限制数（双货币）9F75				000000030000			
应用首选名称“9F12”	AIP“82”	发卡机构认证指示位“9F56”	ADA“9F52”	连续交易限制数“9F72”	累计交易金额上限“9F5C”	第二应用货币代码“9F76”	货币转换因子“9F73”
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 30 卡片特征 20	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	80 ——强制	C2 48 a) 如果发卡机构认证失败，下次联机交易； b) 如果发卡机构认证执行但失败，拒绝交易； c) 如果是新卡，联机交易； d) 如果在前次交易中；PIN 尝试次数超限，拒绝交易； e) 如果发卡机构脚本命令在前次交易中失败，联机交易	05	000000005000	0826	20000175

A.2.5.3 卡片特征 24

卡片特征 24 见表 A.13。

表 A.13 卡片特征 24

应用首选名称“9F12”	应用交易计数器“9F36”
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 34	FF FD

A.2.5.4 卡片特征 5,25,26

卡片特征 5,25,26 见表 A.14。

表 A.14 卡片特征 5,25,26

数据元素				值			
连续国际交易下限 9F58				0F			
连续脱机交易上线 9F59				0F			
连续交易限制数(国际)9F53				0F			
累计交易金额限制数 9F54				000099999999			
应用首选名称“9F12”	AIP“82”	AIA“9F 56”	ADA“9F52”	连续交易限制数“9F72”	累计交易金额限制数(双货币)“9F75”	第二应用货币代码“9F 76”	货币转换因子“9F73”
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 35 卡片特征 5	7C 00 a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证; d) 执行终端风险管理; e) 支持发卡机构认证	80 强制	82 40 a) 如果发卡机构认证失败,下次联机交易; b) 如果是新卡,联机交易; c) 如果在前次交易中;PIN 尝试次数超限,拒绝交易	0F	000000015000	0826	20000175
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 35 卡片特征 25	5C 00 a) 支持 SDA; b) 支持持卡人认证; c) 执行终端风险管理; d) 支持发卡机构认证	80 强制	82 40 a) 如果发卡机构认证失败,下次联机交易; b) 如果是新卡,联机交易; c) 如果在前次交易中;PIN 尝试次数超限,拒绝交易	03	000000015000	0826	20000175

表 A.14（续）

应用首选名称“9F12”	AIP“82”	AIA“9F 56”	ADA“9F52”	连续交易限制数“9F72”	累计交易金额限制数(双货币)“9F75”	第二应用货币代码“9F 76”	货币转换因子“9F73”
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 36 卡片特征 26	5C 00 a) 支持 SDA； b) 支持持卡人认证； c) 执行终端风险管理； d) 支持发卡机构认证	00 可选	82 40 a) 如果发卡机构认证失败，下次联机交易； b) 如果是新卡，联机交易； c) 如果在前次交易中，PIN 尝试次数超限，拒绝交易	03	000000015000	0826	20000175

A.2.5.5 卡片特征 27

卡片特征 27 见表 A.15。

表 A.15 卡 片 特 征 27

应用首选名称“9F12”	应用标识符“84”
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 37	A0 00 00 06 32 01 01

A.2.5.6 卡片特征 28

本特征仅适用于双算法模板，按卡片特征 27 个人化，对称密钥算法不同。

A.2.5.7 卡片特征 31

卡片特征 31 见表 A.16。

表 A.16 卡 片 特 征 31

	AIP“82”	卡片附加处理	卡片交易属性	LOATC
卡片特征 31	70 00——脱机交易 AIP a) 支持 SDA； b) 支持 DDA； c) 支持持卡人认证	92 70 10 00 a) 支持小额检查； b) 支持新卡检查； c) 卡优先选择接触式联机； d) 不允许不匹配货币的交易； e) 如果是新卡且读卡器仅支持脱机则拒绝交易； f) 支持签名； g) 脱机交易脱机批准的交易，卡片记录交易日志	30 00	1

A.2.5.8 卡片特征 32

卡片特征 32 见表 A.17。

表 A.17 卡 片 特 征 32

	AIP“82”	卡片附加处理	卡片交易属性	CTTAUL
卡片特征 32	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	44 00 50 00 a) 支持小额和 CTTA 检查; b) 允许货币不匹配的脱机交易; c) 不匹配货币的交易支持联机 PIN; d) 支持签名	30 00	102.00

A.2.5.9 卡片特征 33

卡片特征 33 见表 A.18。

表 A.18 卡 片 特 征 33

	AIP“82”	卡片附加处理	密文版本	卡片 CVM 限额	CTTAUL
卡片特征 33	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	41 20 80 00 a) 支持小额和 CTTA 检查; b) 返回脱机消费可用余额; c) 如果是新卡且读卡器仅支持脱机则拒绝交易; d) 匹配货币的交易支持联机 PIN	01	00 00 00 00 11 00	110

A.2.5.10 卡片特征 34

卡片特征 34 见表 A.19。

表 A.19 卡 片 特 征 34

	AIP“82”	卡片附加处理	密文版本	CTTAL	CTTAUL
卡片特征 34	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	21 00 F0 00 a) 支持小额或 CTTA 检查; b) 返回脱机消费可用余额; c) 匹配货币的交易支持联机 PIN; d) 不匹配货币的交易支持联机 PIN; e) 对于不匹配货币交易,卡要求 CVM; f) 支持签名	01	50.00	102.00

A.2.5.11 卡片特征 35

卡片特征 35 见表 A.20。

表 A.20 卡 片 特 征 35

	AIP“82”	卡片附加处理	卡片 CVM 限额	CTTAL	CTTAUL
卡片特征 35	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	41 10 20 00 a) 支持小额和 CTTA 检查; b) 返回脱机消费可用余额; c) 对于不匹配货币交易,卡要求 CVM; d) 脱机交易脱机批准的交易,卡片记录交易日志	00 00 00 00 11 00	70.00	不存在

A.2.5.12 卡片特征 36

卡片特征 36 见表 A.21。

表 A.21 卡 片 特 征 36

	AIP“82”	卡片附加处理	CTTAL	CTTAUL
卡片特征 36	70 00—— 脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	01 00 10 00 a) 返回脱机消费可用余额; b) 支持签名	不存在	不存在

A.2.5.13 卡片特征 37

卡片特征 37 见表 A.22。

表 A.22 卡 片 特 征 37

	AIP“82”	卡片附加处理	PDOL	密文版本	LOATC	卡片 CVM 限额和第二币种卡片 CVM 限额
卡片特征 37	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	83 10 40 00 a) 支持小额检查; b) 卡优先选择接触式联机; c) 返回脱机消费可用余额; d) 不匹配货币的交易支持联机 PIN; e) 脱机交易脱机批准的交易,卡片记录交易日志	支持国密算法:9F 66 04 9F 02 06 9F 37 04 5F 2A 02 DF 69 01 不支持国密算法:9F 66 04 9F 02 06 9F 37 04 5F 2A 02	17	0	00 00 00 00 11 00

A.2.5.14 卡片特征 38

卡片特征 38 见表 A.23。

表 A.23 卡 片 特 征 38

	AIP“82”	卡片附加处理	PDOL	密文版本	“9F17”
卡片特征 68	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	81 0 30 00 a) 支持小额检查; b) 卡片不选择接触式联机; c) 返回脱机消费可用余额; d) 对于不匹配货币交易,卡要求 CVM; e) 支持签名	支持国密算法:9F 66 04 9F 02 06 9F 37 04 5F 2A 02 DF 69 01 不支持国密算法:9F 66 04 9F 02 06 9F 37 04 5F 2A 02	17	0

A.2.5.15 卡片特征 39

卡片特征 39 见表 A.24。

表 A.24 卡 片 特 征 39

	AIP“82”	卡片附加处理	应用交易计数器“9F36”	“9F17”	CTTAL
卡片特征 39	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	2C 00 F0 00 a) 支持小额或 CTTA 检查; b) 支持 PIN 重试次数超过检查; c) 允许货币不匹配的脱机交易; d) 匹配货币的交易支持联机 PIN; e) 对于不匹配货币交易,卡要求 CVM; f) 支持签名	FF E0	0	50.00

A.2.5.16 卡片特征 40

卡片特征 40 见表 A.25。

表 A.25 卡 片 特 征 40

	AIP“82”	卡片附加处理	“9F17”	CTTAL	CTTAUL
卡片特征 40	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	24 10 B0 00 a) 支持小额或 CTTA 检查; b) 允许货币不匹配的脱机交易; c) 匹配货币的交易支持联机 PIN; d) 对于不匹配货币交易,卡要求 CVM; e) 支持签名; f) 脱机交易脱机批准的交易,卡片记录交易日志	3	50.00	102.00

A.2.5.17 卡片特征41

卡片特征41见表A.26。

表A.26 卡片特征41

	AIP“82”	卡片附加处理	“9F17”	CTTAL	CTTAUL
卡片特征41	50 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	45 90 F0 00 a) 支持小额和 CTTA 检查; b) 允许货币不匹配的脱机交易; c) 返回脱机消费可用余额; d) 支持预付; e) 匹配货币的交易支持联机 PIN; f) 对于不匹配货币的交易支持联机 PIN; g) 对于不匹配货币交易,卡要求 CVM; h) 支持签名; i) 脱机交易脱机批准的交易,卡片记录交易日志	3	50.00	102.00

A.2.5.18 卡片特征42

卡片特征42见表A.27。

表A.27 卡片特征42

	AIP“82”	卡片附加处理	PDOL	“9F17”	
卡片特征42	70 00——脱机交易 AIP a) 支持 SDA; b) 支持持卡人认证; c) 支持 DDA	85 80 F0 00 a) 支持小额检查; b) 允许货币不匹配的脱机交易; c) 返回脱机消费可用余额; d) 支持预付; e) 匹配货币的交易支持联机 PIN; f) 对于不匹配货币的交易支持联机 PIN; g) 对于不匹配货币交易,卡要求 CVM; h) 支持签名	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04	3	

A.2.5.19 卡片特征43

卡片特征43见表A.28,此特征的非接触界面下的PDOL 9F38应设置为9F 66 04 9F 02 06 9F 03 06

9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04(即不含有 SM 算法支持指示器)。

表 A.28 卡 片 特 征 43

	AIP“82”	卡片附加处理	PDOL	CTTAL	CTTAUL
卡片特征 43	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	8D 00 30 00 a) 支持小额检查; b) 支持 PIN 重试次数超过检查; c) 允许货币不匹配的脱机交易; d) 返回脱机消费可用余额; e) 对于不匹配货币交易,卡要求 CVM; f) 支持签名	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04	不存在	不存在

A.2.5.20 卡片特征 44

卡片特征 44 见表 A.29。

表 A.29 卡 片 特 征 44

	AIP“82”	卡片附加处理	密文版本	CTTAUL
卡片特征 44	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	41 20 80 00 a) 支持小额和 CTTA 检查; b) 返回脱机消费可用余额; c) 如果是新卡且读卡器仅支持脱机则拒绝交易; d) 匹配货币的交易支持联机 PIN	01	110

A.2.5.21 卡片特征 45

卡片特征 45 见表 A.30。

表 A.30 卡 片 特 征 45

	AIP“82”	卡片附加处理	密文版本	卡片 CVM 限额	CTTAUL
卡片特征 45	70 00——脱机交易 AIP a) 支持 SDA; b) 支持 DDA; c) 支持持卡人认证	51 20 80 00 a) 支持小额和 CTTA 检查; b) 支持新卡检查; c) 返回脱机消费可用余额; d) 如果是新卡且读卡器仅支持脱机则拒绝交易; e) 匹配货币的交易支持联机 PIN	01	00 00 00 00 11 00	110

A.2.5.22 卡片特征46

卡片特征46见表A.31。

表A.31 卡片特征46

数据对象	标签	长度(字节)	值
AIP	82	02	70 00 ——脱机交易AIP a) 支持SDA; b) 支持持卡人认证; c) 支持DDA
卡片附加处理	9F68	04	81 00 00 00 a) 支持小额检查; b) 返回脱机消费可用余额
电子现金余额	9F79	06	00 00 00 10 00 00
电子现金余额上限	9F77	06	00 00 00 50 00 00
电子现金单笔交易限额	9F78	06	00 00 00 10 00 00
电子现金重置阈值	9F6D	06	00 00 00 00 00 00
卡片交易属性	9F6C	02	00 00
卡片CVM限额	9F6B	06	00 00 00 10 00 00
连续交易限制数(国际—货币)	9F53	01	00

A.2.5.23 卡片特征47

卡片特征47见表A.32。

表A.32 卡片特征47

数据对象	标签	长度(字节)	值
可用脱机消费金额	9F5D	06	00 00 00 00 00 01
电子现金分段扣费透支限额	DF62	06	00 00 00 10 00 00
电子现金分段扣费已透支额	DF63	06	00 00 00 00 00 00

A.2.5.24 卡片特征48,49

数据同卡片特征31,区别在于选用的密钥长度,具体见本部分第A.2.4。

A.2.6 电子钱包卡片特征

电子钱包卡片特征见表A.33～表A.35。

表A.33 数据文件内容规定表

文件标识	0x15
文件类型	二进制数据文件
文件大小	0x1E
文件存取控制	读:自由

表 A.33（续）

文件标识		0x15
字　节	数 据 元	数　值
1～8	发卡机构代码	00 08 30 10 FF FF FF FF
9	应用类型标识	00
10	发卡机构应用版本	00
11～20	应用主账号	03 88 88 80 10 00 00 00 11 17
21～24	应用启用日期(YYYYMMDD)	20 14 06 12
25～28	应用有效日期(YYYYMMDD)	20 99 12 30
29～30	发卡机构自定义 FCI 数据	00 00

表 A.34　持卡人基本信息文件表

文 件 标 识		0x16
文件类型		二进制数据文件
文件大小		0x37
文件存取控制		读:自由
字节	数据元	数值
1	持卡人类型标识	00
2	本机构职工标识	00
3～22	持卡人姓名	初始化全 00
23～54	持卡人证件号码	初始化全 00
55	持卡人证件类型	00

表 A.35　管理信息文件表

文 件 标 识		0x17
文件类型		二进制数据文件
文件大小		0x3C
文件存取控制		读:自由
字节	数据元	数值
1～4	国际代码	00 00 00 00
5～6	省级代码	00 00
7～8	城市代码	30 10
9～10	互通卡种	FF FF
11	卡种类型	00
12～60	预留	初始化全 00

附 录 B
（资料性附录）
终端应用送检示例

B.1 文档

在送检时提交下列文档：终端的安装和使用手册、终端应用功能测试终端功能陈述文档。

B.2 送检终端

B.2.1 在送检时提交下列终端和相关内容：提供送检终端；

B.2.1.1 终端中的 AID 建议由检测方添加或删除，并且对应于每个 AID 的 ASI 应可配置，下列 AID 预先备下装到终端中：

AID1——A0 00 00 06 32 01 01

AID2——A0 00 00 06 32 10 10

AID3——A0 00 00 06 32 10 10 03

AID4——A0 00 00 06 32 10 10 04

AID5——A0 00 00 06 32 10 10 05

AID6——A0 00 00 06 32 10 10 06

AID7——A0 00 00 06 32 10 10 07

AID8——A0 00 00 00 99 90 90

AID9——A0 00 00 99 99 01

AID10——A0 00 00 00 04 10 10

AID11——A0 00 00 00 65 10 10

B.2.1.2 根公钥模建议可独立下装，并且下列的根公钥模应被预先下装到终端中：

公钥索引‘80’‘57’‘58’‘61’‘62’‘63’‘64’‘65’‘66’‘94’‘96’‘97’‘50’‘51’‘53’对应 RID‘A0 00 00 06 32’；

公钥索引‘E1’‘E2’‘E3’‘E4’‘E5’‘E6’对应 RID‘A0 00 00 99 99’；

公钥索引‘FE’‘FC’‘FB’‘FD’‘FA’‘FF’对应 RID‘A0 00 00 00 04’；

公钥索引‘02’或‘03’对应 RID‘A0 00 00 00 65’。

B.2.1.3 CA 公钥模的值请按照终端规范要求格式设置：

B.2.1.3.1 终端风险管理

终端支持异常文件检查，终端中的异常文件应该可以由测试人员配置。预先将下列账号写入异常文件：卡号为 47 61 73 90 01 01 00 10 。

基于对终端风险管理的支持情况，下列项应可由测试人员配置：最低限额、随机选择目标百分数、偏置随机选择阈值、偏置随机选择的最大目标百分数。

B.2.1.3.2 终端行为码

终端支持终端行为码，可由测试人员修改配置；如果终端不支持终端行为码，指出缺省的假设值。

B.2.1.3.3 应用版本号

存储在终端中的应用版本号设置为‘008C’。

B.2.1.3.4 终端国家代码

终端的国家代码设为‘0840’。