ICS xxxxxxx
X xx
备案号：

JT

中华人民共和国交通运输行业标准

JT/T xxx—xxxx

公共交通IC卡技术规范
第6部分：检测

Technical specification on public transport fare system

—Part 6 :Test and certification

（征求意见稿）

20xx-xx-xx 发布

20xx-xx-xx 实施

中华人民共和国交通运输部 发布

目　　次

前　言

JT/T xxx《公共交通IC卡技术规范》由6个规范组成：

——第1部分：卡片；

——第2部分：读写终端；

——第3部分：信息接口；

——第4部分：非接触通讯接口；

——第5部分：安全；

——第6部分：检测；

本部分为JT/T xxx的第6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司提出。

本部分由全国城市客运标准化技术委员会（SAC/TC529）归口。

本部分主要起草单位：中国交通通信信息中心、交通运输部科学研究院、南京市市民卡有限公司、北京市政交通一卡通有限公司、银行卡检测中心。

本部分主要起草人：　汪宏宇、李岚、唐猛、王一路、张永军、刘好德、谷云辉、钱贞国。

公共交通IC卡技术规范

第6部分：检测

1 范围

JT/Txxx的本部分规定了公共交通IC卡卡片物理检测要求、公共交通IC卡卡片非接电特性和通讯协议检测要求、公共交通IC卡卡片应用检测要求、终端电气特性和通讯协议检测要求、终端应用内核部分检测要求、系统安全及功能检测要求、SAM卡电气特性和通讯协议检测要求、SAM卡应用功能及安全检测要求、公共交通IC卡卡片安全检测要求、公共交通IC卡卡片芯片安全检测要求。

本部分适用于公共交通IC卡片进行合规检测，要求检测内容包括卡片内部处理细节、卡片使用数据元、卡片支持指令集、终端内部处理细节等。使用对象主要是与公共交通IC卡应用相关的卡片、终端制造、检测、发行、受理，以及应用系统的研制、开发、集成和维护等部门（单位）。

2 规范性引用文件

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

GB/T 14916 识别卡 物理特性

GB/T 15120 识别卡 记录技术

3 术语和定义

下列术语和定义适用于本文件。

3.1

半字节 nibble

一个字节的高四位或低四位。

3.2

保护时间 guardtime

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

3.3

报文认证码 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。

3.4

发卡机构行为代码 issuer action code

发卡机构根据TVR的内容选择的动作。

3.5

加密算法 cryptographic algorithm

隐藏或显现数据信息内容的变换算法。

3.6

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。

3.7

静止状态 inactive

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

3.8

卡片 card

如无特殊说明在本部分中特指公共交通 IC 卡。

3.9

块 block

包含两个或三个域（头域、信息域、尾域）的字符组。

3.10

冷复位 cold reset

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

3.11

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。

3.12

认证 authentication

确认一个实体所宣称的身份的措施。

3.13

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。

3.14

支付系统环境 payment system environment

当符合本部分的支付系统应用被选择，IC 卡中所确立的逻辑条件。

3.15

终端行为代码 terminal action code

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

3.16

状态　H state H

高电平状态。根据 IC 卡中的逻辑约定，可以是逻辑 1 或逻辑 0。

3.17

状态　L state L

低电平状态。根据 IC 卡中的逻辑约定，可以是逻辑 1 或逻辑 0。

4　符号和缩略语

以下缩略语表示适用于本文件：

AC	应用密文（Application Cryptogram）
ACK	确认（Acknowledgment）
ADA	应用缺省行为（Application Default Action）
ADF	应用数据文件（Application Definition File）
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）
BER	基本编码规则（Basic Encoding Rules）
BGT	块保护时间（Block Guard Time）
CA	认证中心（Certificate Authority）
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 Byte of the Command Message）
CLK	时钟（CLK）
Cn	压缩数字格式（Compress Numeric）
CVM	持卡人验证方法（Cardholder Verification Method）
CWT	字符等待时间（Character Waiting Time）
DC	直流（Direct Current）
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）
EDC	错误检测代码（Error Detection Code）
EF	基本文件（Elementary File）
EMV	Europay MasterCard VISA
etu	基本时间单元（Elementary Time Unit）
FCI	文件控制信息（File Control Information）

GND	地（Ground）
GPO	获取处理选项（GET PROCESSING OPTIONS）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
ICS	功能一致性声明（Implementation Conformance Statement）
IFS	信息域大小（Information Field Size）
IFSC	IC 卡信息域大小（Information Field Size for the ICC）
IIH	高电平输入电流（High Level Input Current）
INF	信息域（Information Field）
INS	命令报文的指令字节（Instruction Byte of Command Message）
I/O	输入/输出（Input/Output）
IOH	高电平输出电流（High Level Output Current）
IOL	低电平输出电流（Low Level Output Current）
ISO	国际标准化组织（International Organization for Standardization）
kΩ	千欧
Lc	终端应用层（TAL）在情况 3 或情况 4 命令中发出数据的实际长度（Exact Length of Data Sent by the TAL in a Case 3 or 4 Command）
LCOL	连续脱机交易下限
Le	在情况 2 或情况 4 命令中返回给终端应用层（TAL）的数据最大期望长度（Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command）
LEN	长度（Length）
LOATC	上次联机交易计数器
Lr	响应数据域的长度（Length of Response Data Field）
LRC	冗余校验（Longitudinal Redundancy Check）
l.s.	最低位
M	必备（Mandatory）
mA	毫安
MAC	报文认证码（Message Authentication Code）
MDK	主密钥（Master DEA Key）
MF	主文件（Mater File）
MHz	兆赫
m.s.	最高位
mΩ	毫欧
MΩ	兆欧
N	数字型（Numeric）
NAD	节点地址（Node Address）
NAK	否定的确认（Negative Acknowledgment）
nAs	纳安秒
ns	纳秒
O	可选（Optional）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）

P3	参数 3（Parameter 3）
PAN	主账号（Primary Account Number）
PCB	协议控制字节（Protocol Control Byte）
pF	皮法
PIN	个人密码（Personal Identification Number）
R-block	接收就绪块（Receive Ready Block）
RFU	保留（Reserved for Future Use）
RID	注册应用提供商标签（Registered Application Provider Identifier）
RST	复位（Reset）
R-TPDU	响应 TPDU（Response TPDU）
SDA	静态数据认证（Static Data Authentication）
SFI	短文件标签符（Short File Identifier）
SW1	状态字 1（Status Word One）
SW2	状态字 2（Status Word Two）
TAC	终端行为代码（Terminal Action Code）
TAL	终端应用层（Terminal Application Layer）
TC	交易证书（Transaction Certificate）
tF	信号幅度从 90%下降到 10%的时间（Fall Time Between 90% and 10% of Signal Amplitude）
TLV	标签、长度、值（Tag Length Value）
TPDU	传输协议数据单元（Transport Protocol Data Unit）
tR	信号幅度从 10%上升到 90%的时间（Rise Time Between 10% and 90% of Signal Amplitude）
TSI	交易状态信息（Transaction Status Information）
TVR	终端验证结果（Terminal Verification Results）
UCOL	连续脱机交易上限
V	伏特（Volt）
Vcc	VCC 触点上的测得电压（Voltage Measured on VCC Contact）
VCC	电源电压（Supply Voltage）
V_{IH}	高电平输入电压（High Level Input Voltage）
V_{IL}	低电平输入电压（Low Level Input Voltage）
$V_{I/O}$	I/O 触点上的测得电压（Voltage Measured on I/O Contact）
V_{OH}	高电平输出电压（High Level Output Voltage）
V_{OL}	低电平输出电压（Low Level Output Voltage）
V_{PP}	VCC 触点上的测得电压（Voltage measured on VPP contact）
VPP	编程电压（Programming Voltage）
V_{RST}	RST 触点上的测得电压（Voltage measured on RST contact）
WI	等待时间整数（Waiting Time Integer）
WTX	等待时间扩展（Waiting Time Extension）

5 公共交通 IC 卡卡片物理检测要求

5.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度40%-60%之间。如无特殊说明，后续案例均采用此环境条件。

5.2 测试内容

5.2.1 公共交通 IC 卡卡面设计要素测试

测试目的：检查公共交通IC卡卡面（正面、背面）包含的设计要素是否符合规范要求，保证卡片表面设计要素统一完整。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：检查公共交通IC卡正面包含的设计要素；检查公共交通IC卡背面包含的设计要素。

5.2.2 公共交通 IC 卡卡面字符印刷

测试目的：检查公共交通IC卡卡面（正面、背面）包含的卡号、有效期等字符属性是否满足规范要求。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：检查公共交通IC卡正面包含的字符属性；检查公共交通IC卡背面包含的字符属性。

5.2.3 公共交通 IC 卡卡片长宽尺寸

测试目的：检查卡片长宽尺寸是否符合规范要求，保证卡片能够正常插入终端的读卡模块。。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：使用视频测量仪测量卡片长宽尺寸。

5.2.4 公共交通 IC 卡卡片厚度

测试目的：检查卡片厚度是否符合规范要求，不会由于过薄或过厚而影响卡片的插拔。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：使用千分尺测量并记录卡片厚度。

5.2.5 公共交通 IC 卡卡片翘曲

测试目的：检查卡片翘曲是否符合规范要求，保证卡片平整度在常温下维持在一定的范围内，没有明显的翘曲变形。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：使用卡片翘曲测量仪测量卡片翘曲。

5.2.6 公共交通 IC 卡卡片切边质量

测试目的：检查卡片切边质量是否符合规范要求，保证卡片边缘的毛刺长度在一定要求范围内，不会因为毛刺过长无法正常插入读卡模块，或者过度磨损读卡模块。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：使用切边测量仪测量卡片切边毛刺长度质量。

5.2.7 公共交通 IC 卡卡片弯曲刚度

测试目的：检查卡片的弹性型变量和塑性型变量是否符合规范要求，保证持卡人在一定力度范围内不小心弯折卡片时（例如卡片放在裤袋内坐下或起立时），不会引起卡片的严重变形。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：将卡片左边边缘在刚度测量仪上夹好（正面朝上），在电子测微计上读出初始位置的读数h1；在卡片右边边缘加载0.7N的砝码，锁紧砝码，一分钟后记录下卡片的位置h2；除去砝码的作用力，一分钟后记录下卡片恢复的高度h3，计算h2—h1和h3—h1。

5.2.8 公共交通 IC 卡卡片层间剥离强度

测试目的：检查卡片层间剥离强度是否符合规范要求，保证卡片层间粘结强度符合规范要求。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：使用拉伸试验机测量卡片层间剥离强度。

5.2.9 公共交通 IC 卡卡片温湿条件下尺寸稳定性

测试目的：保证卡片大小在高温严寒、干燥潮湿条件下不会因为热胀冷缩而发生严重改变，也不会出现高低不平现象。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：将卡水平放置于高低温试验箱内，依次置于下列环境下各60分钟：（a）-35℃±3℃；（b）50℃±3℃，相对湿度95%±5%；将卡取出，放在实验室环境条件下保持24小时，再使用视频测量仪测量卡片尺寸。

5.2.10 公共交通 IC 卡卡片温湿条件下整卡翘曲稳定性

测试目的：保证卡片平整度在高温严寒、干燥潮湿条件下不会因为热胀冷缩而发生严重改变，也不应有明显的翘曲变形。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：将卡水平放置于高低温试验箱内，依次置于下列环境下各60分钟：（a）-35℃±3℃；（b）50℃±3℃，相对湿度95%±5%；将卡取出，放在实验室环境条件下保持24小时，再使用整卡翘曲测量仪测量卡片翘曲。

5.2.11 公共交通 IC 卡卡片动态弯扭

测试目的：检查芯片封装抗卡片弯曲扭曲特性是否符合规范要求，保证在一定机械外力的作用下对卡片进行弯折和扭曲，卡片不发生严重形变，芯片不发生脱落，且保持正常的读写功能。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：使用弯扭特性测试仪对卡片分别进行四个方向的弯曲，每250次换一个方向；再对卡进行1000次扭曲后卡片无破裂开胶现象。ATR正确并读写功能（执行SELECT命令）正常。

5.2.12 公共交通 IC 卡卡片抗静电特性

测试目的：模拟日常生活中穿着毛衣带有静电的持卡人无意中电击卡片的情况，保证卡片经一定强度的静电电击后仍然能正常工作。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：使用模拟静电发生器，通过放电尖端在卡片表面进行空气放电，首先使用+6000V的静电测试，+6000V测完，需重新测试ATR和读写，如未出现异常，再对卡表面进行-6000V的空气放电测试，放电完毕后需重新测试ATR和读写，检查卡片是否出现异常

5.2.13 公共交通 IC 卡卡片抗紫外特性

测试目的：检查芯片抗紫外特性是否符合规范要求，保证在日常生活中接触到一定剂量紫外光照时不会导致卡片功能失效。

测试条件：参考附录A要求，根据送检样卡进行专项检测。

测试方法步骤：使用紫外测量仪（光源波长254nm）对卡片照射总剂量为0.15Ws/mm2。

5.2.14 公共交通 IC 卡卡片抗静磁场特性

测试目的：检查非接触芯片抗静磁场特性是否符合规范要求。
测试条件：参考附录A要求，根据送检样卡进行专项检测。
测试方法步骤：使用静磁场测试仪测量芯片抗静磁场特性。

5.2.15 公共交通 IC 卡卡片耐化学性测试

测试目的：包括耐酸性人工汗、耐碱性人工汗、耐碳酸钠、耐乙醇、耐糖水、耐乙二醇、耐盐水、耐醋酸八项测试，用于模拟卡片日常使用时的环境，保证卡片接触到水、汗液等日常生活中可能遇到的弱浓度化学溶液情况下不会导致卡片功能失效。
测试条件：参考附录A要求，根据送检样卡进行专项检测。
测试方法步骤：使用化学试剂浸泡后，ATR正确并读写功能（执行SELECT命令）正常。

5.2.16 公共交通 IC 卡异形卡检测

检测目的：检测异形卡卡片相关物理规格和卡片印刷是否符合规范要求。
测试条件：根据送检样卡进行专项检测。
测试过程：通过相关物理检测设备对异形卡的物理参数进行具体检测。

5.2.17 SAM 卡检测

检测目的：检测SAM卡卡片相关物理规格是否符合规范要求。
测试条件：根据送检样卡进行专项检测。
测试过程：通过相关物理检测设备对SAM卡的物理参数进行具体检测。

6 公共交通 IC 卡卡片非接电特性和通讯协议检测要求

6.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度20%-80%之间。如无特殊说明，后续案例均采用此环境条件。

公共交通IC卡的非接触电气特性和通讯协议的检测项目主要涵盖：负载调制信号的幅度测试、TYPE A测试、TYPE B测试和块传输协议执行测试等。上述检测项目从底层硬件的角度检测了IC卡能否正确地接收或发送的信号，信号的幅值是否在规定的范围内，传输的时刻是否正确，信号持续的时长是否正确，传输的内容是否完整和正确，能否自动监测并及时纠正错误以及一些控制参数是否在允许的范围内等，保证公共交通IC卡卡片和终端的信息交换按照规范的要求可靠无误地进行。

6.2 电特性测试

6.2.1 PICC 负载调制幅值测试

测试目的：确保PICC在工作场强[Hmin，Hmax]范围内，负载调制信号的幅值符合规范要求。
具体的工作场强选择范围为：
当H=1.5A/m，对应 Vrms＝480mV时
当H=2.5A/m，对应 Vrms = 800mV时
当H=3.5A/m，对应Vrms＝1.12V时
当H=4.5A/m，对应Vrms＝1.44V时

当H=5.5A/m，对应Vrms=1.76V时

当H=6.5A/m，对应Vrms=2.08V时

当H=7.5A/m，对应Vrms=2.40V时

测试条件：根据送检样卡进行专项检测。

测试方法步骤：使用终端发出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[Hmin，Hmax]。测量卡片在12.7125Mhz和14.4075Mhz两个频率点的负载调制幅值。

6.2.2 PICC 交变磁场检测

测试目的：确保PICC在交变磁场内测试后，卡片功能正常。

测试条件：参见附录B进行个人化，并符合附录C中的功能一致性声明。

测试方法步骤：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30秒。

6.3 通讯协议测试

6.3.1 传输协议测试：TYPE A

检测目的：检测卡片是否满足规范要求的TYPE A协议要求。

测试条件：支持TYPE A协议，参见附录B进行个人化，并符合附录C中的功能一致性声明。

测试过程：对卡片进行如下方面的逐项测试：

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状态下错误的处理测试；
6) READY状态下错误的处理测试；
7) ACTIVE状态下错误的处理测试；
8) 进入ACTIVE状态之后的HALT状态下错误的处理测试；
9) 进入PROTOCOL状态之后的HALT状态下错误的处理测试；
10) 轮询和PICC复位的处理测试。

6.3.2 传输协议测试：TYPE B

检测目的：检测卡片是否满足规范要求的TYPE B协议要求。

测试条件：支持TYPE B协议，参见附录B进行个人化，并符合附录C中的功能一致性声明。

测试过程：对卡片进行如下方面的逐项测试：

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

6.3.3 块传输协议执行

测试目的：检测卡片是否满足规范中规定的块传输协议要求。
测试条件：支持TYPE A或TYPE B协议，参见附录B进行个人化，并符合附录C中的功能一致性声明。
测试方法步骤：对卡片进行如下方面的逐项测试：

1） 从PCD接收链接I块的测试
2） 块之中的PCB带RFU位的测
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
8） 块协议开始出现错误的测试

7 公共交通 IC 卡卡片应用检测要求

7.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度40%-60%之间。如无特殊说明，后续案例均采用此环境条件。

公共交通IC卡的应用功能检测主要涵盖：非接触联机交易应用检测、非接触脱机交易检测、双币非接触脱机交易检测（可选）。卡片应用检测主要判断卡片在收到终端发来的不同命令时，能否识别当前命令是否属于当前应用，能否判断交易流程是否按照规范规定的步骤进行，能否校验每条命令的正确性，能否根据命令做出正确的操作并给出相应的响应，遇到异常时能否做出及时的反馈等，同时应保证卡片在异常情况下能够具备一定的恢复机制，保证卡片内部数据的完整性和正确性。

7.2 联机交易应用检测

7.2.1 电子现金应用锁定命令

检测目的：检测卡片的应用锁定命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的应用锁定命令，判定卡片应用锁定命令执行的情况。

7.2.2 电子现金应用锁定

检测目的：检测卡片的应用锁定流程和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：在不同的卡片状态下向卡片发送应用锁定命令，判定卡片应用锁定命令执行的情况。

7.2.3 电子现金读应用数据

检测目的：检测卡片的Read Record命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送正常和异常的Read Record命令，判定卡片Read Record命令执行的情况。

7.2.4 电子现金获取应用数据

检测目的：检测卡片的Get Data命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的Get Data命令，判定卡片Get Data命令执行的情况。

7.2.5 电子现金应用选择

检测目的：检测卡片的应用选择命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向不同状态的卡片发送应用选择命令，判定卡片应用选择的执行情况。

7.2.6 电子现金应用解锁命令

检测目的：检测卡片的应用解锁命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的应用解锁命令，判定卡片应用解锁命令执行的情况。

7.2.7 电子现金应用解锁

检测目的：检测卡片的应用解锁流程和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：在不同的卡片状态下向卡片发送应用解锁命令，判定卡片应用解锁命令执行的情况。

7.2.8 电子现金卡片锁定命令

检测目的：检测卡片的卡片锁定命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的卡片锁定命令，判定卡片锁定命令执行的情况。

7.2.9 电子现金卡片锁定

检测目的：检测卡片的卡片锁定流程和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：在不同的卡片状态下向卡片发送卡片锁定命令，判定卡片锁定命令执行的情况。

7.2.10 电子现金联机批准交易

检测目的：验证卡片对联机批准交易中命令的正确响应。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过发送交易命令判断卡片联机批注交易中命令的响应的情况。

7.2.11 电子现金上次交易发卡机构脚本失败

检测目的：检测卡片对上次发卡机构脚本失败情况下的流程处理满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过发送交易命令判断卡片在上次发卡机构脚本失败情况下的交易流程处理情况。

7.2.12 电子现金卡片风险管理

检测目的：检测卡片风险管理流程处理满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过发送交易命令检测卡片风险管理处理情况。

7.2.13 电子现金双货币超累计交易金额上限检查

检测目的：检测卡片卡片执行交易金额（双货币）的频度检查满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过发送交易命令检测卡片执行交易金额（双货币）的频度检查处理情况。

7.2.14 电子现金更新卡片数据

检测目的：检测卡片的卡片PUT DATA和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：在不同的卡片状态下向卡片发送PUT DATA命令，判定卡片更新数据执行的情况。

7.2.15 电子现金 EXTERNAL AUTHENTICATE 命令

检测目的：检测卡片的EXTERNAL AUTHENTICATE命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的EXTERNAL AUTHENTICATE命令，判定卡片命令执行的情况。

7.2.16 电子现金联机交易失败

检测目的：检测卡片联机交易失败情况下执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送联机失败交易，判定卡片流程执行的情况。

7.2.17 电子现金 GET PROCESSING OPTIONS 命令

检测目的：检测卡片的GET PROCESSING OPTIONS命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和GET PROCESSING OPTIONS命令，判定卡片命令执行的情况。

7.2.18 电子现金应用初始化

检测目的：检测卡片的应用初始化流程和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
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，判定卡片命令执行的情况。

7.2.19 电子现金发卡机构认证

检测目的：检测卡片的发卡机构认证流程和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：在不同的卡片状态下向卡片发送发卡机构认证命令，判定卡片命令执行的情况。

7.2.20 电子现金发卡机构脚本处理

检测目的：检测卡片的发卡机构脚本处理流程和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
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，判定卡片命令执行的情况。

7.2.21 电子现金日志文件

检测目的：检测卡片的日志记录处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：判定卡片日志文件记录和读取执行的情况。

7.2.22 电子现金新卡

检测目的：检测卡片的新卡处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：在不同的卡片状态下判定卡片新卡流程执行的情况。

7.2.23 PIN CHANGE/UNBLOCK 命令

检测目的：检测卡片的卡片PIN CHANGE/UNBLOCK命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的PIN CHANGE/UNBLOCK命令，判定卡片命令的执行情况。

7.2.24 VERIFY 命令

检测目的：检测卡片的卡片VERIFY命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的VERIFY命令，判定卡片命令的执行情况。

7.2.25 电子现金 READ RECORD 命令

检测目的：检测卡片的命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的READ RECORD命令，判定卡片命令的执行情况。

7.2.26 电子现金 UPDATE RECORD 命令

检测目的：检测卡片的UPDATE RECORD命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的UPDATE RECORD命令，判定卡片命令的执行情况。

7.2.27 电子现金联机完成

检测目的：检测卡片联机完成情况下的交易流程处理是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向不同状态的卡片发送交易命令，判定在联机完成的情况下卡片流程的执行情况。

7.2.28 电子现金联机授权未完成

检测目的：检测卡片在联机授权未完成情况下的交易流程处理是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向不同状态的卡片发送交易命令，判定在联机授权未完成的情况下卡片流程的执行情况。

7.2.29 电子现金持卡人认证

检测目的：检测卡片持卡人认证执行流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片持卡人认证流程的执行情况。

7.2.30 电子现金 PUT DATA 连续交易限制（国际）

检测目的：检测卡片的PUT DATA 连续交易限制（国际）处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在PUT DATA 连续交易限制（国际）时的执行情况。

7.2.31 电子现金执行交易金额（双货币）频度检查

检测目的：检测卡片的执行交易金额（双货币）频度检查处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在执行交易金额（双货币）频度检查时的执行情况。

7.2.32 电子现金执行国际国家频度检查

检测目的：检测卡片的执行国际国家频度检查处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在执行国际国家频度检查时的执行情况。

7.2.33 电子现金执行指定货币交易金额检查

检测目的：检测卡片的执行指定货币交易金额检查处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在执行指定货币交易金额检查时的执行情况。

7.2.34 电子现金执行国际-货币频度检查

检测目的：检测卡片的执行国际-货币频度检查处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在执行国际-货币频度检查时的执行情况。

7.2.35 电子现金参数测试

检测目的：检测卡片支持的命令参数否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送错误参数的交易指令，判定卡片对错误参数的处理情况。

7.2.36 电子现金稳定性测试

检测目的：检测卡片最小交易稳定性是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，执行规定笔数的交易。

7.2.37 电子现金自助终端受理测试

检测目的：检测卡片在模拟自助终端上交易流程处理是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在GPO GAC数据不一致情况下的流程的执行情况。

7.2.38 电子钱包应用状态测试

检测目的：检测卡片的电子钱包应用在不同状态下的命令执行流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送指令将卡片设置为不同的应用状态，判定卡片在不同状态下的命令执行的情况。

7.2.39 电子钱包应用锁定命令

检测目的：检测卡片的电子钱包应用锁定命令和执行流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送正常和异常的电子钱包应用锁定命令，判定卡片应用锁定命令执行的情况。

7.2.40 电子钱包应用锁定

检测目的：检测卡片的电子钱包应用锁定流程和执行流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

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，判定卡片电子钱包应用锁定命令执行的情况。

7.2.41 电子钱包应用解锁命令

检测目的：检测卡片的电子钱包应用解锁命令和执行流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送正常和异常的电子钱包应用解锁命令，判定卡片电子钱包应用解锁命令执行的情况。

7.2.42 电子钱包应用解锁

检测目的：检测卡片的电子钱包应用解锁流程和执行流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

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，判定电子钱包卡片应用解锁命令执行的情况。

7.2.43 电子钱包圈存初始化命令

检测目的： 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是否满足规范需求。

检测条件：根据附录B个人化要求个人化好的卡片。

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，判定卡片电子钱包圈存初始化命令的执行情况。

7.2.44 电子钱包圈存流程

检测目的：检测卡片的电子钱包的圈存交易流程和执行流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：在不同情况下对卡片发送电子钱包圈存命令,判定卡片电子钱包圈存命令的执行情况。

7.2.45 电子钱包圈提流程

检测目的：检测卡片的电子钱包的圈提交易流程和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：在不同情况下对卡片发送电子钱包圈提命令,判定卡片电子钱包圈提命令的执行情况。

7.2.46 电子钱包修改透支命令

检测目的：检测卡片的电子钱包的修改透支限额交易流程和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：在不同情况执行电子钱包修改透支交易,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。

7.2.47 电子钱包 READ RECORD 命令

检测目的：检测卡片的命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的READ RECORD命令，判定卡片命令的执行情况。

7.2.48 电子钱包 UPDATE RECORD 命令

检测目的：检测卡片的UPDATE RECORD命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的UPDATE RECORD命令，判定卡片命令的执行情况。

7.2.49 电子钱包 READ BINARY 命令

检测目的：检测卡片的命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的READ BINARY命令，判定卡片命令的执行情况。

7.2.50 电子钱包 UPDATE BINARY 命令

检测目的：检测卡片的命令和执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的UPDATE BINARY命令，判定卡片命令的执行情况。

7.2.51 稳定性测试

检测目的：检测卡片最小交易稳定性是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，执行规定笔数的交易。

7.3 脱机交易应用检测

7.3.1 PPSE 选择

检测目的：检测卡片PPSE选择执行流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的PPSE选择命令，判定卡片命令的执行情况。

7.3.2 终端或卡请求 CVM

检测目的：检测卡片的CVM流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在终端或卡片请求CVM时的执行情况。

7.3.3 电子现金检查联机处理请求

检测目的：检测卡片的在卡片或终端请求联机时的处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在终端或卡片请求联机时的执行情况。

7.3.4 电子现金小额检查

检测目的：检测卡片小额检查流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片小额检查的执行情况。

7.3.5 电子现金小额和 CTTA 检查

检测目的：检测卡片小额和CTTA检查流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片小额和CTTA检查的执行情况。

7.3.6 电子现金没有任何脱机选项被支持

检测目的：检测卡片在没有任何脱机选项被支持时的流程处理是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片没有任何脱机选项被支持时的执行情况。

7.3.7 电子现金脱机下的货币不匹配

检测目的：检测卡片的在脱机处理时的处于货币不匹配状态下的处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在终端或卡片脱机完成时的执行情况。

7.3.8 电子现金预付

检测目的：检测卡片的预付处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片的预付处理流程。

7.3.9 电子现金动态数据认证

检测目的：检测卡片的动态数据认证处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片的动态数据认证处理流程。

7.3.10 电子现金闪卡测试

检测目的：检测卡片的闪卡流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片的闪卡处理流程。

7.3.11 电子现金永久锁定应用

检测目的：检测卡片在永久锁定应用状态下的处理流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送交易指令，判定卡片在永久锁定应用状态下的处理流程。

7.3.12 电子钱包消费交易

检测目的：检测卡片在电子钱包消费的处理流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送指令，判定在不同的情况下，消费流程中涉及的命令（初始化消费、消费）是否满足规范要求。

7.3.13 电子钱包复合应用消费交易（未使用互联互通文件）

检测目的：检测卡片在电子钱包复合应用消费的处理流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送指令，判定在不同的情况下，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、更新缓存数据、复合应用消费）是否满足规范要求。

7.3.14 电子钱包复合应用消费交易（使用互联互通文件）

检测目的：检测卡片在电子钱包复合应用消费（使用互联互通文件）的处理流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送指令，判定在不同的情况下，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、更新缓存数据、复合应用消费）是否满足规范要求，并结合电子现金端对互联互通文件进行核实。

7.3.15 电子现金查询余额

检测目的：检测卡片查询余额处理流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送交易指令，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。

7.3.16 电子现金稳定性测试

检测目的：检测卡片在稳定性处理交易方面是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送交易指令，判定卡片正确执行指定笔数的交易。

7.3.17 电子现金分段扣费功能测试（未使用互联互通文件）

检测目的：检测卡片的分段扣费处理流程是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送交易指令，判定卡片的分段扣费处理流程。

7.3.18 电子现金分段扣费功能测试（使用互联互通文件）

检测目的：检测卡片的分段扣费处理流程（使用互联互通文件）是否满足规范要求。

测试条件：根据附录B个人化要求个人化好的卡片。

测试过程：通过向卡片发送交易指令，判定卡片的分段扣费处理流程，并在电子钱包端确认文件数据的正确性。

7.3.19 电子现金脱机预授权及预授权完成功能测试

检测目的：检测卡片的脱机预授权及预授权完成处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片的脱机预授权及预授权完成处理流程。

7.3.20 电子现金押金抵扣功能测试

检测目的：检测卡片的押金抵扣处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片的押金抵扣处理流程。

7.3.21 电子现金交易时间测试

检测目的：检测卡片的交易时间处理满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常的交易命令，判定卡片交易执行所耗费的时间情况。

7.3.22 电子现金增强性安全性测试

检测目的：检测卡片的安全报文是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常的交易命令，判定卡片交易执行中安全信息的生成情况。

7.3.23 电子现金双币应用测试

检测目的：检测卡片在具备双币应用配置时的交易处理流程是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送正常和异常的交易命令，判定卡片双币交易流程的执行情况。其中应包括新增的数据元、异常响应和交易流程测试。

7.3.24 电子现金共享余额测试

检测目的：检测卡片在模拟交易流程及余额共享处理是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令，判定卡片在进行余额改动操作后在电子钱包端的同步共享。

7.3.25 电子现金文件共享测试

检测目的：检测卡片在模拟交易流程及文件共享处理是否满足规范要求。
测试条件：根据附录B个人化要求个人化好的卡片。
测试过程：通过向卡片发送交易指令和文件修改指令，判定卡片在进行文件改动操作后在电子钱包端的同步共享。

8 终端电气特性和通讯协议检测要求

8.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度20%-80%之间。如无特殊说明，后续案例均采用此环境条件。

针对专用级别的终端设备，选择的最低温度应在-30℃至-20℃（根据终端实际使用的环境温度决定），最高温度应该在60℃至90℃（根据终端实际使用的环境温度决定）。

非接触式终端电气特性和通讯协议检测项目主要包括：载波频率测试、PCD最大最小场强测试、PCD到PICC的传输功率测试、调制指数和波形测试、轮询测试、Type A及Type B协议测试等，主要检验读卡器与卡片没有机械接触的情况下，通过能量的交换进行终端和卡片的通讯过程中，终端的工作频率是否正常，场强的大小是否在一定的范围内，终端发送的信号波形的幅值以及上升下降时间，终端检测多张卡片同时出现的防冲突机制，终端捕捉信号的灵敏度，终端能否不受某些信号的干扰等。

8.2 电气特性测试

8.2.1 PCD 场强测试

测试目的：检测终端的PCD场强是否满足规范要求。

测试条件：送检支持的终端样品，具体要求可参考附录D。

测试方法步骤：在非接检测环境下对终端的场强进行测试。

8.2.2 载波频率测试

测试目的：检测终端的载波频率是否满足规范中规定要求。

测试条件：送检支持的终端样品，具体要求可参考附录D。

测试方法步骤：在非接检测环境下对终端的载波频率进行波形截取。

8.2.3 场复位测试

测试目的：检测终端复位时的场强和复位时间。

测试条件：送检支持的终端样品，并且终端支持连续复位模式，具体要求可参考附录D。

测试方法步骤：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。

8.2.4 TYPE A、B 通信的 PCD 到 PICC 波形测试

测试目的：检测终端的Type A 波形的t1到t4时间是否满足规范中规定要求，验证V4到V2单调下降和上升是否符合要求，验证波形上冲和下冲是否符合要求。验证TYPE B 波形的负载调试幅度和上升下降沿时间。

测试条件：送检支持的终端样品，并且终端支持循环寻卡模式，具体要求可参考附录D。

测试方法步骤：在非接检测环境下对终端的发出的TypeA波形的1时间和单调性进行检测，对TYPE B终端的负载调试幅度的上升下降沿时间进行检测。

8.2.5 验证最小调制下的负载调制 $V_{S1,pp}$ 接收灵敏度测试

测试目的：此测试验证，当测试 PICC 距离被测设备天线平面距离小于等于 2 厘米时，应用最小负载调制特性时，PCD 功能是否正常。

测试条件：送检支持的终端样品，并且终端支持循环寻卡模式，具体要求可参考附录 D。

测试方法步骤：在非接检测环境下对终端的发出的 TypeA、B 波进行响应，PCD 应在测试 PICC 应用最小负载调制特性时功能正常。观察到所有响应。

8.2.6 验证最大调制下的负载调制 $V_{S2,pp}$ 接受灵敏度测试

测试目的：此测试验证，当测试 PICC 距离被测设备天线平面距离大于 2 厘米时，应用最

大负载调制特性时，PCD 功能是否正常。

测试条件：送检支持的终端样品，并且终端支持循环寻卡模式，具体要求可参考附录 D。

测试方法步骤：在非接检测环境下对终端的发出的 TypeA、B 波进行响应，PCD 应在测试 PICC 应用最大负载调制特性时功能正常。观察到所有响应。

8.2.7 TYPE A、B 通信的比特电平编码信号接口

测试目的：此测试验证在初始化期间 PCD 到 PICC 的比特率和比特编码和去同步。

测试条件：送检支持的终端样品，并且终端支持循环寻卡模式，具体要求可参考附录 D。

测试方法步骤：在非接检测环境下对终端的发出的 TYPEA、B 波进行测量，确定波形速率是否符合规范。

8.3 通讯协议测试

8.3.1 Type A 测试

测试目的：检测终端对Type A协议的支持是否满足规范要求。

测试条件：支持TYPE A的送检终端，具体要求可参考附录D。

测试方法步骤：

——在非接检测环境下对终端的Type A协议功能进行如下逐项检测：

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SAK和ATS中的TA测试
8) 支持的TL和各种长度的历史字节测试
9) 支持的SFGI测试
10) 支持的TC测试
11) 对HALT命令的Type A桢应答测试
12) ATQA的不同值测试
13) 可能情况下的FWT下的非链接I块交互测试
14) FSC=256字节的链接块传输测试
15) FSC=16-128字节的链接块传输测试
16) 非链接I块，对桢等待时间扩展的请求处理测试
17) 链接I块，对桢等待时间扩展的请求处理测试
18) 长度不规则情况下链接I块处理测试
19) 最小帧延迟时间情况下的时序处理测试
20) WUPA响应错误的处理测试
21) ANTICOLLISION CL1后错误处理测试
22) 轮询到1个Type A卡和1个Type B卡测试
23) 冲突探测WUPA后一个错误测试
24) 冲突探测SELECT CL1后一个错误测试
25) 激活RATS后错误测试测试
26) 激活RATS响应带噪声测试

27） 冲突探测ANTICOLLISION CL1后超时测试
28） 冲突探测WUPA后超时测试
29） 冲突探测SELECT CL1后超时测试
30） 激活RATS后超时测试
31） 忽略所有传输错误（不包括循环冗余校验错误或奇偶校验错误）并在tRECOVERY时间内接受正确的序列测试
32） 激活RATS后遵守不回应期测试
33） 非链接I块的错误通知测试
34） 非链接I块响应超时测试
35） 非链接I块响应传输错误测试
36） 非链接I块响应协议错误测试
37） 链接I块错误通知测试
38） 链接I块响应超时测试
39） 链接I块响应传输错误测试
40） 链接I块响应协议错误测试
41） R（ACK）块后超时测试
42） R（ACK）响应传输错误测试
43） R（ACK）响应协议错误测试
44） S（WTX）响应块后超时测试
45） S（WTX）请求后再次使用FWT扩展测试
46） 非链接I块响应带噪声测试
47） 链接I块响应带噪声测试
48） R（ACK）块响应带噪声测试
49） R（NAK）指出传输错误的响应协议错测试
50） 移出后WUPA响应错测试
51） S（WTX）响应块后连续超时测试
52） 忽略所有传输错误（不包括循环冗余校验错误或奇偶校验错误）并在tRECOVERY时间内接受正确的序列测试
53） Type A协议下的不响应时间测试

8.3.2 Type B 测试

测试目的：检测终端对Type B协议的支持是否满足规范要求。
测试条件：支持TYPE B协议的送检终端，具体要求可参考附录D。
测试方法步骤：
——在非接检测环境下对终端的Type A协议功能进行如下逐项检测：

1） Type B预测确定TR1PUTMIN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SOS和EOS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
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，对桢等待时间扩展的请求处理测试
18） 链接I块，对桢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type B卡然后一个type A卡测试
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（不包括循环冗余校验错误或奇偶校验错误）并在tRECOVERY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
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（不包括循环冗余校验错误或奇偶校验错误）并在tRECOVERY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

9 终端应用内核部分检测要求

9.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度20%-80%之间。如无特殊说明，后续案例均采用此环境条件。

在终端应用内核测试过程中，对于交易的每一个步骤，终端首先会进行一系列的检查操作，然后发送相应的命令及数据，以终端能否判断交易金额是否超限，能否判断卡片是否或过期，终端发送命令的格式是否合法，卡片要求终端发送的数据与终端实际发送的数据是否一致等；当终端收到卡片的响应后，则验证终端能否校验这些响应数据的合法性，能否察觉必备数据是否缺失，数据的加密是否存在问题，能否判断这些数据指明了卡片的哪些功能，能否获取卡片对于当前命令所进行的操作的信息等。

9.2 数据元和命令

测试目的：检测终端对数据元和命令的支持是否满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：

——通过选择卡片应用，执行交易检测终端对如下数据元和命令的支持情况：

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
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

9.3 应用选择

测试目的：检测终端对应用选择的处理支持是否满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：

——通过选择卡片应用，执行交易检测终端如下应用选择处理时的支持情况：

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

9.4 密钥安全检测

测试目的：检测终端对密钥的选择和加密解密安全方面的处理支持是否满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：

——通过选择卡片应用，执行交易检测终端在如下处理过程时时的支持情况：

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

9.5 数据对象

测试目的：检测终端不同类型的数据对象支持是否满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：

——通过选择卡片应用，执行交易检测终端对如下类型的数据对象支持情况：

1) 长度域：1字节
2) 长度域：2字节
3) 在an格式的数据对象中“空格”字符的识别
4) 应用选择时接受IC卡中格式错误的应用选择数据对象。

9.6 认可的加密算法

测试目的：检测终端不同类型的加密算法是否满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：通过选择卡片应用，执行交易检测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。

9.7 交易接口文件

测试目的：检测终端对交易接口文件的读取处理是否满足规范要求。
测试条件：根据送检终端进行专项检测，具体要求可参考附录E。
测试方法步骤：通过选择卡片应用，执行交易检测终端对不同类型的加密算法的执行情况。

9.8 交易过程中使用的功能

测试目的：检测终端对交易过程中的流程处理是否满足规范要求。
测试条件：根据送检终端进行专项检测，具体要求可参考附录E。
测试方法步骤：
——通过选择卡片应用，执行交易检测终端交易过程中不同情况下的流程执行情况：

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

9.9 生成应用密文命令编码

测试目的：检测终端对交易过程中GAC密文的处理是否满足规范要求。
测试条件：根据送检终端进行专项检测，具体要求可参考附录E。
测试方法步骤：通过选择卡片应用，执行交易检测终端交易过程中不同情况下的GAC流程执行情况。

9.10 IC卡中错误和缺少的数据

测试目的：检测终端在IC卡出现缺少数据和内部数据错误情况下的支持是否满足规范要求。
测试条件：根据送检终端进行专项检测，具体要求可参考附录E。
测试方法步骤：
——通过选择卡片应用，执行交易检测终端对如下类型错误和缺失时的支持情况：

1) 必备数据对象丢失：FCI、DF名、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

9.11 终端总体要求

测试目的：检测终端在不同商户要求情况下的处理是否满足规范要求。
测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：通过选择卡片应用，执行交易检测终端对如不同商户要求配置的支持情况。

9.12 软件体系结构

测试目的：检测终端软件体系结构是否满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：通过选择卡片应用，执行交易检测终端数据元的初始化、支持语言和失败显示错误信息的处理情况。

9.13 持卡人和商户界面

测试目的：检测终端在不同情况下的界面显示是否满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：通过选择卡片应用，执行交易检测终端对不同情况下的商户显示界面支持情况。

9.14 终端数据元的编码

测试目的：检测终端必备数据元编码是否满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：通过选择卡片应用，执行交易检测终端对下列类型数据元的编码情况：

1) 终端类型
2) 终端性能
3) 终端附加性能
4) 账户类型

9.15 综合测试

测试目的：检测终端在不同交易流程下的处理满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：通过选择卡片应用，执行交易检测终端对不同交易流程下的过程处理情况。

9.16 补充测试

测试目的：检测终端在特殊规定情况下的处理满足规范要求。

测试条件：根据送检终端进行专项检测，具体要求可参考附录E。

测试方法步骤：

——通过选择卡片应用，执行交易检测终端对下列情况的过程处理情况：

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
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

10 系统安全及功能检测要求

10.1 一般要求

本章针对公共交通IC卡涉及的业务系统、发卡系统系统、清算系统的系统安全性和系统功能性检测事宜进行描述。

原则要求检测系统为实际生产系统或与生产系统为完全一致的准生产系统或测试系统。

10.2 交易处理检测

10.2.1 交易处理

检测目的：能够正常进行交易处理。

测试条件：相关要求可参考附录F。

测试过程：模拟交易处理。

10.2.2 管理类交易

检测目的：能够正常进行管理类交易处理。

测试条件：相关要求可参考附录F。

测试过程：模拟管理类交易。

10.3 报文接口规范检测

检测目的：报文结构、报文头、报文类型、报文位图、报文域、关键信息域和报文关联、报文格式。

测试条件：相关设计文档，具体要求可参考附录F。

测试过程：查看相关设计文档。

10.4 文件接口规范检测

检测目的：交易明细文件名称、记录格式。

测试条件：相关设计文档，具体要求可参考附录F。

测试过程：查看相关设计文档。

10.5 通信接口规范检测

检测目的：网络接口、通信接口。

测试条件：相关设计文档，具体要求可参考附录F。

测试过程：查看相关设计文档。

10.6 联网通信安全规范检测

检测目的：交易渠道依赖性、磁密依赖性、硬件加密机、密钥管理、公共交通IC卡前置设备、终端机具、个人标识码、网络、联网通信安全管理。

测试条件：相关设计文档，具体要求可参考附录F。

测试过程：查看相关设计文档。

10.7 功能测试

10.7.1 账户管理

检测目的：开户、黑名单检查、账户信息维护、账户信息查询、销户。
测试条件：测试环境，具体要求可参考附录F。
测试过程：模拟进行账户管理类测试。

10.7.2 密钥和证书管理

检测目的：公共交通IC卡密钥管理、公共交通IC卡证书管理。
测试条件：密钥管理相关文档，具体要求可参考附录F。
测试过程：查看密钥管理相关文档，查看密钥管理系统。

10.7.3 卡片管理

检测目的：制卡、开卡、黑名单检查、卡信息查询、卡交易明细查询、卡片信息维护、卡参数维护、卡状态控制、销卡。
测试条件：测试环境，具体要求可参考附录F。
测试过程：模拟进行卡片管理类测试。

10.7.4 密码功能

检测目的：修改密码、密码错误次数检查。
测试条件：测试环境，具体要求可参考附录F。
测试过程：模拟进行密码功能测试。

10.7.5 交易处理

检测目的：交易类测试、单次最高消费限额、单日最高消费次数。
测试条件：测试环境，具体要求可参考附录F。
测试过程：模拟进行交易测试。

10.8 安全性测试

10.8.1 网络安全性测试

10.10.1.1 结构安全

检测目的：网络冗余和备份、网络安全路由器、网络安全防火墙、网络拓扑结构、IP子网划分、QoS保证。
测试条件：提供网络拓扑图、网络设备配置文件，网络管理员。
测试过程：查看网络拓扑图、网络设备配置文件，访谈网络管理员。

10.10.1.2 网络访问控制

检测目的：网络域安全隔离和限制、地址转换和绑定、内容过滤、访问控制、流量控制、会话控制。
测试条件：网络设备配置文件。
测试过程：查看网络设备配置文件，访谈网络管理员。

10.10.1.3 网络安全审计

检测目的：日志信息、网络系统故障分析、网络对象操作审计、日志权限和保护。
测试条件：网络管理员。
测试过程：查看日志信息、故障知识库，访谈网络管理员。

10.10.1.4 网络入侵防范

检测目的：ARP外部欺骗、访问权限设置、DoS/DDoS攻击、安全设备配置、网络入侵防范设备。

测试条件：网络设备配置文件，网络管理员。

测试过程：查看网络设备配置文件，访谈网络管理员。

10.10.1.5 恶意代码防范

检测目的：防范软件安全部署、定时在线更新、控制措施、定期安装必要补丁。

测试条件：网络设备配置文件，网络管理员。

测试过程：查看网络设备配置文件，访谈网络管理员。

10.10.1.6 网络设备防护

检测目的：设备登录设置、设备登录口令安全性、登录地址限制、远程管理安全、设备用户设置策略、权限分离、最小化服务。

测试条件：网络设备配置文件，网络管理员。

测试过程：查看网络设备配置文件，访谈网络管理员。

10.10.1.7 网络安全管理

检测目的：网络设备运维手册、设备参数配置、网络事故管理、漏洞扫描、网络数据传输加密、安全产品管理。

测试条件：运维相关文档，网络管理员。

测试过程：查看网络设备配置文件，查看运维相关文档，访谈网络管理员。

10.10.1.8 网络相关人员安全管理

检测目的：网络安全人员管理配备、网络安全管理人员责任划分规则、网络安全关键岗位人员管理。

测试条件：相关文档，网络主管。

测试过程：查看责任划分相关文档，访谈网络主管。

10.8.2 主机安全性测试

10.10.2.1 身份鉴别

检测目的：系统与应用管理员用户设置、系统与应用管理员口令安全性、登录策略、非法访问警示。

测试条件：系统配置文件，主机管理员。

测试过程：查看用户设置配置文件，访谈主机管理员。

10.10.2.2 自主访问控制

检测目的：自主访问控制范围、主机信任关系、默认过期用户。

测试条件：系统配置文件，主机管理员。

测试过程：查看系统配置文件，访谈主机管理员。

10.10.2.3 强制访问控制

检测目的：资源访问记录、重要系统文件强制访问控制范围、共享目录、远程登录控制。

测试条件：系统配置文件，主机管理员。

测试过程：查看系统配置文件，访谈主机管理员。

10.10.2.4 安全审计

检测目的：日志信息、日志保护、系统信息分析、对象操作审计、日志权限、关键数据删除制度和记录。

测试条件：日志文件，安全管理员

测试过程：查看系统日志文件及系统，访谈安全管理员。

10.10.2.5 系统保护

检测目的：系统备份、故障恢复策略、安全配置、磁盘空间安全、主机加固、安全产品管理。

测试条件：主机管理员。

测试过程：访谈主机管理员。

10.10.2.6 剩余信息保护

检测目的：过期信息、文档处理。

测试条件：相关制度。

测试过程：查看相关制度。

10.10.2.7 入侵防范

检测目的：入侵防范记录、关闭服务、最小安装原则。

测试条件：主机配置文件，主机管理员。

测试过程：查看主机配置文件，访谈主机管理员。

10.10.2.8 恶意代码防范

检测目的：防范软件安装部署、定时在线更新、控制措施、定期安装系统必要补丁、漏洞扫描。

测试条件：安全管理员。

测试过程：访谈安全管理员。

10.10.2.9 资源控制

检测目的：连接控制、资源监控和预警。

测试条件：安全管理员。

测试过程：访谈安全管理员。

10.10.2.10 主机安全人员管理

检测目的：主机安全人员管理配备、主机安全管理人员责任划分规则、主机安全关键岗位人员管理。

测试条件：相关文档，主机主管。

测试过程：查看责任划分相关文档，访谈主机主管。

10.8.3 应用安全性测试

10.10.3.1 身份鉴别

检测目的：系统与普通用户设置、系统与普通用户口令安全性、登录访问安全策略、非法访问警示和记录、客户端鉴别信息安全、口令有效期限制、限制认证会话时间、身份标识唯一性、及时清除鉴别信息。

测试条件：系统配置文件，系统管理员。

测试过程：查看系统配置文件，访谈系统管理员。

10.10.3.2 访问控制

检测目的：访问权限设置、自主访问控制范围、业务操作日志、关键数据存放、异常中断防护、数据库安全配置。

测试条件：系统配置文件，数据库配置信息，系统管理员，数据库管理员。

测试过程：查看系统配置文件、数据库配置文件，访谈系统管理员、数据库管理员。

10.10.3.3 安全审计

检测目的：日志信息、日志保护、系统信息查询与分析、对象操作审计、日志权限、审计工具、事件报警。

测试条件：日志信息，安全管理员。

测试过程：查看日志信息，访谈安全管理员。

10.10.3.4 剩余信息保护

检测目的：过期信息、文档处理。

测试条件：相关制度。

测试过程：查看相关制度。

10.10.3.5 资源控制

检测目的：连接控制、会话控制、进程资源分配、资源检测预警。

测试条件：系统配置文件，系统管理员。

测试过程：查看系统配置文件，访谈系统管理员。

10.10.3.6 应用容错

检测目的：数据有效性检验、容错机制、故障机制、回退机制。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.10.3.7 通信完整性

检测目的：通信报文有效性、通信完整性。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.10.3.8 通信保密性

检测目的：报文或会话加密、通信异常处理。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.10.3.9 抗抵赖

检测目的：原发和接收证据。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.10.3.10 编码安全

检测目的：编码规范约束、源代码管理、版本管理。

测试条件：相关制度，系统管理员。

测试过程：查看相关制度，访谈系统管理员。

10.10.3.11 脱机数据认证

检测目的：密钥和证书、静态数据认证、动态数据认证。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.10.3.12 安全报文

检测目的：报文格式、报文完整性验证、报文私密性、密钥管理。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.10.3.13 公共交通 IC 卡卡片安全

检测目的：共存应用、密钥的独立性、公共交通IC卡卡片内部安全体系、卡片中密钥的种类。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.10.3.14 终端安全

检测目的：终端数据安全性、终端设备安全性、终端密钥管理要求。

测试条件：终端安全检测报告。

测试过程：查看终端安全检测报告。

10.10.3.15 安全机制

检测目的：对称加密机制、非对称加密机制。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.10.3.16 认可的算法

检测目的：对称加密算法、非对称加密算法、哈希算法。

测试条件：系统管理员配合。

测试过程：访谈系统管理员。

10.8.4 数据安全性测试

10.10.4.1 数据完整性

检测目的：重要数据更改机制、数据备份和审计记录定期查验、保障传输过程中的数据完整性安全、定期随机抽取备份数据进行加压还原以检查其内容有效性。

测试条件：相关制度、记录，数据库管理员

测试过程：查看相关制度、记录，访谈数据库管理员。

10.10.4.2 交易数据以及客户数据的安全性

检测目的：数据物理存储、数据交换安全性、加密传输、加密存储、数据访问控制、数据备份机制、本地备份、异地备份、备份数据的恢复、数据销毁制度和记录。

测试条件：相关制度、记录，数据库管理员。

测试过程：查看相关制度、记录，访谈数据库管理员。

10.8.5 运维安全性测试

10.10.5.1 环境管理

检测目的：机房基本设施定期维护、机房出入管理制度化和文档化、办公环境的保密性措施、机房安全管理制度、机房进出登记表。

测试条件：相关制度，运维管理员。

测试过程：查看相关制度，访谈运维管理员。

10.10.5.2 介质管理

检测目的：介质的存放环境保护措施、介质的使用管理文档化、维修或销毁介质之前清楚敏感数据、介质管理记录、介质的分类与标识。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度，访谈运维管理员。

10.10.5.3 设备管理

检测目的：设备管理的责任人或部门、设施设备定期维护、设备选型采购发放等审批控制、设备配置标准化、设备的操作规程、设备的操作日志、设备使用管理文档、设备标识。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度，访谈运维管理员。

10.10.5.4 人员管理

检测目的：人员录用、人员转岗离岗、人员考核、安全意识教育和培训、外部人员访问管理、职责分离。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度，访谈运维管理员。

10.10.5.5 监控管理

检测目的：主要网络设备的各项指标监控情况、主要服务器的各项指标监控情况、应用运行各项指标监控情况、异常处理机制。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度、记录，访谈运维管理员。

10.10.5.6 变更管理

检测目的：变更方案、变更制度化管理、重要系统变更的批准、重要系统变更的通知。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度、记录，访谈运维管理员。

10.10.5.7 安全事件处置

检测目的：安全事件报告和处置、安全事件的分类和分级、安全事件记录和采取的措施。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度、记录，访谈运维管理员。

10.10.5.8 应急预案管理

检测目的：制定不同事件的应急预案、相关人员应急预案培训、定期演练。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度、记录，访谈运维管理员。

10.8.6 业务连续性测试

10.10.6.1 业务连续性需求分析

检测目的：业务中断影响分析、灾难恢复时间目标和恢复点目标。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度、记录，访谈运维管理员。

10.10.6.2 业务连续性技术环境

检测目的：备份机房、网络双链路、网络设备和服务器备份、高可靠的磁盘阵列、远程数据库备份。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度、具体设备，访谈运维管理员。

10.10.6.3 业务连续性管理

检测目的：业务连续性管理制度、应急响应流程、恢复预案、数据备份和恢复制度。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度，访谈运维管理员。

10.10.6.4 备份与恢复管理

检测目的：备份数据范围和备份频率、备份和恢复手册、备份记录和定期恢复测试记录、定期数据备份恢复性测试。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度，访谈运维管理员。

10.10.6.5 日常维护

检测目的：每年业务连续性演练、定期业务连续性培训。

测试条件：相关制度，运维管理员配合。

测试过程：查看相关制度，访谈运维管理员。

10.9 文档测试

10.9.1 用户文档

检测目的：用户手册、操作手册。

测试条件：相关文档，具体要求可参考附录F。

测试过程：查看相关文档。

10.9.2 开发文档

检测目的：需求说明书、需求分析文档、总体设计方案、数据库设计文档、概要设计文档、详细设计文档、工程实施方案。

测试条件：相关文档，具体要求可参考附录F。

测试过程：查看相关文档。

10.9.3 管理文档

检测目的：测试报告、系统运维手册、系统应急手册、运维管理制度、安全管理制度、安全审计报告。

测试条件：相关文档，具体要求可参考附录F。

测试过程：查看相关文档。

11 SAM卡电气特性和通讯协议检测要求

11.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度40%-60%之间。如无特殊说明，后续案例均采用此环境条件。

测试内容主要包括SAM卡的电特性测试、复位应答测试、字符传输测试、T=0协议测试、T=1协议测试等；上述检测项目从底层硬件的角度检测了SAM在接触界面下能否正确地接收或发送的信号，信号的幅值是否在规定的范围内，传输的时刻是否正确，信号持续的时长是否正确，传输的内容是否完整和正确，能否自动监测并及时纠正错误以及一些控制参数是否在允许的范围内等，保证卡片和终端的信息交换按照规范的要求可靠无误地进行。

11.2 电特性测试

11.2.1 卡片[1]电阻测试

测试目的：确保任意IC卡触点的电阻在允许范围内。

测试条件：默认环境条件，具体要求参考附录G。

测试过程：通过测量芯片各管脚的电阻情况。

11.2.2 卡片在不同环境条件下的测试

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

测试条件：默认环境条件，具体要求参考附录G。

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。

11.2.3 卡片在传输模式下的高低电压测试

测试目的：确保I/O触点在传输模式下信号的高低电压都在规定范围内。

测试条件：温度= 23℃±3℃

Vcc=4.5V，5V 和 5.5V（±25mV）（CLASSA）

Vcc=2.7V，3V 和 3.3V（±15mV）（CLASSB）

测试过程：IC卡复位。

在 ATR 字符帧传送过程中监控 V_{OH} 和 V_{OL}。

对所有 Vcc 条件都重复上述测试。

1) [1] 本章节中的“卡片”如无特殊说明则特指 SAM 卡片。

11.2.4 卡片 I/O 触点在传输模式下信号的下降时间测试

测试目的：确保I/O触点在传输模式下信号的下降时间在规定范围内。

测试条件：温度=23℃±3℃

Vcc=4.5V，5V 和 5.5V（±25mV）（CLASSA）

Vcc=2.7V，3V 和 3.3V（±15mV）（CLASSB）

测试过程：IC卡复位。

在 ATR 字符帧传送过程中测量 t_F 在 90% 到 10% 点信号的下降沿。

对所有 Vcc 条件都重复上述测试。

11.2.5 激活时序过程测试

测试目的：确保在一个激活时序过程中IC卡能正确的控制I/O信号。

测试条件：温度= 23℃±3℃

Vcc=4.5V，5V 和 5.5V（±25mV）（CLASSA）

Vcc=2.7V，3V 和 3.3V（±15mV）（CLASSB）

测试过程：通过发送正常的激活时序并记录相关时间。

11.2.6 复位应答测试

测试目的：确保卡复位应答相关参数在指定的时间范围内。

测试条件：默认环境条件，具体要求参考附录G。

测试过程：通过发送冷热复位信号，来判断相关的时间参数和ATR响应间隔。

11.2.7 字符传输测试

测试目的：确保卡片返回的字符中每一位和字符持续时间在规范规定范围，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：默认环境条件，具体要求参考附录G。

测试过程：通过正常流程信号，来判断相关的时间参数和字符响应间隔。

11.3 通讯协议测试

11.3.1 T=0 协议测试

检测目的：检测卡片是否满足规范要求的T=0的协议要求。

测试条件：支持T=0协议并根据附录G的相关要求个人化好的卡片。

测试过程：

——对卡片进行下列单项的测试：

1) IC卡发送的同向字符间隔测试；
2) IC卡从终端接收到字符同返回字符间的时间间隔测试；
3) TC1指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Le>卡响应数据测试
8) 命令情况2的Le=卡响应数据测试
9) 命令情况2的Le<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

11.3.2 T=1 协议测试

检测目的：检测卡片是否满足规范要求的T=1的协议要求。
测试条件：支持T=1协议并并根据附录G的相关要求个人化好的卡片。
测试过程：
——对卡片进行下列单项的测试：

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
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

12 SAM 卡应用功能及安全检测要求

12.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度40%-60%之间。如无特殊说明，后续案例均采用此环境条件。

SAM卡功能检测主要涵盖：SAM卡针对安全存储和应用之间的功能接口，应用检测主要判断卡片在收到终端发来的不同命令时，能否识别当前命令是否属于SAM卡应用，能否校验每条命令的正确性，能否根据命令做出正确的操作并给出相应的响应，遇到异常时能否做出及时的反馈等。

12.2 功能检测

12.2.1 INIT_FOR_DESCRYPT 命令

检测目的：检测SAM卡的卡片[2]INIT_FOR_DESCRYPT命令和执行流程是否满足规范要求。

测试条件：已经个人化好密钥的卡片，具体要求参考附录G。

测试过程：通过向卡片发送正常和异常的INIT_FOR_DESCRYPT命令，判定卡片命令的执行情况。

12.2.2 DES Crypt 命令

检测目的：检测SAM卡的卡片DES Crypt命令和执行流程是否满足规范要求。

测试条件：已经个人化好密钥的卡片，具体要求参考附录G。

测试过程：通过向卡片发送正常和异常的DES Crypt命令，判定卡片命令的执行情况。

12.3 逻辑安全性测试

12.3.1 敏感信息存储安全性测试

检测目的：敏感信息应采用安全方式存储，不应存在任何机制，允许输出敏感信息。

测试条件：测试样卡，具体要求参考附录G。

测试过程：执行相关指令。

12.3.2 逻辑异常攻击测试

检测目的：IC功能应不受逻辑异常的影响，比如非预期命令，未知命令等，这些逻辑异常可能会导致SAM卡功能紊乱或输出敏感信息。

测试条件：测试样卡，具体要求参考附录G。

测试过程：执行相关指令。

12.3.3 后门命令测试

检测目的：不应存在未公开的命令。这些命令可能导致SAM卡敏感信息的泄露，严重影响SAM卡的安全性。

测试条件：测试样卡，具体要求参考附录G。

测试过程：执行相关指令。

12.3.4 随机数的随机性测试

检测目的：随机数发生器具有足够的随机性，其随机性指标符合相关规范要求。

测试条件：随机数文件，具体要求参考附录G。

测试过程：验证随机数的随机性。

---

2) [2]本章节中的“卡片”如无特殊说明则特指 SAM 卡片。

12.3.5 TIMING 攻击测试

检测目的：SAM卡在安全运算过程中，时间特征不能泄露敏感信息。
测试条件：测试样卡，具体要求参考附录G。
测试过程：执行PIN校验指令验证。

12.3.6 SPA/DPA 攻击测试

检测目的：SAM卡在安全运算过程中，功率变化特征不能泄露敏感信息。
测试条件：测试样卡，具体要求参考附录G。
测试过程：采集安全运算过程中功率变化。

12.3.7 加密算法测试

检测目的：SAM卡中使用的加密算法应该符合相关规范要求。
测试条件：测试样卡，具体要求参考附录G。
测试过程：验证算法正确性。

12.3.8 SAM 卡 COS 认证

检测目的：SAM卡COS及对COS的任何改动都应经过归档和审计的流程。
测试条件：相关文档，具体要求参考附录G。
测试过程：查看相关文档。

12.4 防故障攻击测试

12.4.1 高低温测试

检测目的：在高温或低温环境下，SAM卡的功能不应发生紊乱或泄露敏感信息。
测试条件：测试样卡，具体要求参考附录G。
测试过程：在高温或低温条件下进行指令测试。

12.4.2 电压测试

检测目的：当电压超过SAM卡工作电压范围时，SAM卡应安全失效。
测试条件：测试样卡，具体要求参考附录G。
测试过程：在一定电压下进行指令测试。

12.4.3 强光干扰测试

检测目的：SAM卡在运行过程中的特定时刻，如果受到强光干扰，SAM卡功能不应发生紊乱或泄露敏感信息。
测试条件：测试样卡，具体要求参考附录G。
测试过程：利用强光进行干扰测试。

12.4.4 电磁干扰测试

检测目的：SAM卡在运行过程中的特定时刻，如果受到电磁干扰，SAM卡功能应不发生紊乱或泄露敏感信息。
测试条件：测试样卡，具体要求参考附录G。
测试过程：利用电磁进行干扰测试。

12.4.5 紫外线干扰测试

检测目的：SAM卡在运行过程中的特定时刻，如果受到紫外线干扰，SAM卡功能应不发生紊乱或泄露敏感信息。

测试条件：测试样卡，具体要求参考附录G。

测试过程：利用紫外线进行干扰测试。

12.4.6 静电干扰测试

检测目的：SAM卡在运行过程中的特定时刻，如果受到静电干扰，SAM卡功能应不发生紊乱或泄露敏感信息。

测试条件：测试样卡，具体要求参考附录G。

测试过程：利用静电进行干扰测试。

12.4.7 疲劳测试

检测目的：SAM卡在进行连续高强度操作后，功能不应发生紊乱。

测试条件：测试样卡，具体要求参考附录G。

测试过程：连续进行SAM卡高强度操作。

13 公共交通IC卡卡片安全检测要求

13.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度40%-60%之间。如无特殊说明，后续案例均采用此环境条件。

13.2 公共交通IC卡安全检测

13.2.1 逻辑安全性测试

13.2.1.1 敏感信息存储安全性测试

检测目的：敏感信息应采用安全方式存储，不应存在任何机制，允许输出敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：执行相关指令。

13.2.1.2 逻辑异常攻击测试

检测目的：IC功能应不受逻辑异常的影响，比如非预期命令，未知命令等，这些逻辑异常可能会导致公共交通IC卡功能紊乱或输出敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：执行相关指令。

13.2.1.3 后门命令测试

检测目的：不应存在未公开的命令。这些命令可能导致公共交通IC卡敏感信息的泄露，严重影响公共交通IC卡的安全性。

测试条件：测试样卡（参考附录H的要求）。

测试过程：执行相关指令。

13.2.1.4 随机数的随机性测试

检测目的：随机数发生器具有足够的随机性，其随机性指标符合相关规范要求。

测试条件：随机数文件（参考附录H的要求）。

测试过程：验证随机数的随机性。

13.2.1.5 TIMING攻击测试

检测目的：公共交通IC卡在安全运算过程中，时间特征不能泄露敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：执行PIN校验指令验证。

13.2.1.6 SPA/DPA攻击测试

检测目的：公共交通IC卡在安全运算过程中，功率变化特征不能泄露敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：采集安全运算过程中功率变化。

13.2.1.7 加密算法测试

检测目的：公共交通IC卡中使用的加密算法应该符合相关规范要求。

测试条件：测试样卡（参考附录H的要求）。

测试过程：验证算法正确性。

13.2.1.8 公共交通IC卡COS认证

检测目的：公共交通IC卡COS及对COS的任何改动都应经过归档和审计的流程。

测试条件：相关文档（参考附录H的要求）。

测试过程：查看相关文档。

13.2.2 防故障攻击测试

13.2.2.1 高低温测试

检测目的：在高温或低温环境下，公共交通IC卡的功能不应发生紊乱或泄露敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：在高温或低温条件下进行指令测试。

13.2.2.2 电压测试

检测目的：当电压超过公共交通IC卡工作电压范围时，公共交通IC卡应安全失效。

测试条件：测试样卡（参考附录H的要求）。

测试过程：在一定电压下进行指令测试。

13.2.2.3 强光干扰测试

检测目的：公共交通IC卡在运行过程中的特定时刻，如果受到强光干扰，公共交通IC卡功能不应发生紊乱或泄露敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：利用强光进行干扰测试。

13.2.2.4 电磁干扰测试

检测目的：公共交通IC卡在运行过程中的特定时刻，如果受到电磁干扰，公共交通IC卡功能应不发生紊乱或泄露敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：利用电磁进行干扰测试。

13.2.2.5 紫外线干扰测试

检测目的：公共交通IC卡在运行过程中的特定时刻，如果受到紫外线干扰，公共交通IC卡功能应不发生紊乱或泄露敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：利用紫外线进行干扰测试。

13.2.2.6 静电干扰测试

检测目的：公共交通IC卡在运行过程中的特定时刻，如果受到静电干扰，公共交通IC卡功能应不发生紊乱或泄露敏感信息。

测试条件：测试样卡（参考附录H的要求）。

测试过程：利用静电进行干扰测试。

13.2.2.7 疲劳测试

检测目的：公共交通IC卡在进行连续高强度操作后，功能不应发生紊乱。

测试条件：测试样卡（参考附录H的要求）。

测试过程：连续进行公共交通IC卡高强度操作。

14 公共交通IC卡卡片芯片安全检测要求

14.1 一般要求

默认环境条件（温度，湿度等）是指常温23±3℃，湿度40%-60%之间。如无特殊说明，后续案例均采用此环境条件。

14.2 芯片检测项目

14.2.1 芯片表面准备

检测目的：验证安全芯片是否具备足够的保护能力以防止安全芯片表面覆盖层被移除。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：尝试在不损坏安全芯片的前提下使安全芯片表面暴露。

14.2.2 芯片背部准备

检测目的：验证安全芯片是否具备足够的保护能力以防止安全芯片背部覆盖层被移除。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：尝试在不损坏安全芯片的前提下使安全芯片背部暴露。

14.2.3 传感器功能验证

检测目的：芯片应具备电压、频率和温度传感器等环境传感器或等效安全防护机制，并且这些环境传感器或等效安全防护机制均工作正常。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：尝试验证芯片环境传感器或等效安全防御机制的有效性。

14.2.4 芯片表面简要分析

检测目的：验证安全芯片硬件设计是否具备相应的复杂性。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考公开性的文档尝试分析安全芯片标识信息、表面构造和设计规则等。

14.2.5 芯片表面详细分析

检测目的：验证安全芯片硬件设计是否具备足够的复杂性。

测试条件：测试样卡、测试材料（参考附录I的要求）。测试条件：参考设计文档尝试分析安全芯片功能模块和安全敏感区域等。

14.2.6 传输系统的物理位置探测

检测目的：验证安全芯片是否具备足够的保护能力以防止其传输系统的物理位置被探测。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试通过反向工程定位传输系统的位置。

14.2.7 传输系统的FIB修改

检测目的：验证安全芯片是否具备足够的保护能力以防止通过FIB修改传输系统。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：尝试使用FIB系统对传输系统进行连线或修改。

14.2.8 逻辑建立模块的干扰

检测目的：验证安全芯片是否具备足够的保护能力以防止逻辑建立模块被干扰。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档尝试旁路或使逻辑模块的功能或安全性暂时失准或失效。

14.2.9 逻辑建立模块的修改

检测目的：验证安全芯片是否具备足够的保护能力以防止逻辑建立模块被修改。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档尝试对逻辑模块的功能或安全性进行永久的修改。

14.2.10 测试模式的重激活

检测目的：验证安全芯片是否具备足够的保护能力以防止测试模式被重激活或被旁路。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档尝试使安全芯片在测试模式下运行。

14.2.11 利用片上测试特性

检测目的：验证安全芯片是否具备足够的保护能力以防止滥用测试特性以获取及修改相关敏感信息。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档尝试滥用测试特性以获取及修改相关敏感信息。

14.2.12 非易失性 ROM 信息的泄露

检测目的：验证安全芯片是否具备足够的保护能力以防止通过形象化获取非易失性ROM的内容。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档尝试利用在工艺上的差异形象化ROM，并恢复出ROM中的数据。

14.2.13 被动探测

检测目的：验证安全芯片是否具备足够的保护能力以防止通过被动探测获取安全芯片中敏感信息。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：尝试对安全芯片进行被动探测，窃听数据总线和控制线，并记录数据。

14.2.14 主动探测

检测目的：验证安全芯片是否具备足够的保护能力以防止通过主动探测来改变安全芯片的程序流程、实现功能或敏感信息。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档尝试对安全芯片进行主动探测，观察安全芯片运行状况。

14.2.15 非易失性 ROM 信息的产生

检测目的：验证安全芯片是否具备足够的保护能力以防止通过主动及被动探测来获取非易失性ROM内容。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档，通过反向工程定位ROM的控制和地址总线，进而实施恶意操作。

14.2.16 直接读取非易失性可编程存储器

检测目的：验证安全芯片是否具备足够的保护能力以防止通过主动及被动探测直接读取EEPROM或Flash的内容。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档尝试通过主动及被动探测直接读取EEPROM或Flash单元的内容。

14.2.17 非易失性可编程存储器信号的产生

检测目的：验证安全芯片是否具备足够的保护能力以防止通过探测获取EEPROM或Flash的内容。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考详细设计文档尝试通过反向工程定位EEPROM或Flash控制和地址总线，进而进行恶意操作。

14.2.18 电压对比

检测目的：验证安全芯片是否具备足够的保护能力以防止通过形象化安全芯片表面电压以恢复存储器中敏感信息及其位置。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试通过形象化安全芯片表面的电压恢复存储器中的秘密信息的位置及内容。

14.2.19 供电电源操纵

检测目的：验证安全芯片是否具备足够的保护能力以防止通过供电电源操纵改变安全芯片程序流程，或导致安全芯片进入一个非预期或未定义的状态。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试操纵安全芯片供电电源，观察安全芯片运行状态。

14.2.20 其他非侵入式操纵

检测目的：验证安全芯片是否具备足够的保护能力以防止通过外部参数操纵改变安全芯片程序流程或导致安全芯片进入一个非预期或未定义的状态。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试改变安全芯片各类参数（比如时钟、复位或I/O信号），观察并记录安全芯片运行情况。

14.2.21 电磁操纵

检测目的：验证安全芯片是否具备足够的保护能力以防止通过电磁操纵改变安全芯片程序流程或导致安全芯片进入一个非预期或者未定义的状态。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试使用高压在安全芯片表面产生一个电场，观察并记录安全芯片运行情况。参考设计文档尝试使用强磁场在安全芯片的连线中引起电流，观察并记录安全芯片运行情况。

14.2.22 光注入

检测目的：验证安全芯片是否具备足够的保护能力以防止通过光注入引起安全芯片运行中的错误、改变安全芯片程序流程或导致安全芯片进入一个非预期或者未定义的状态。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试对安全芯片表面进行光注入，干扰安全芯片运行，观察并记录安全芯片运行情况。

14.2.23 放射线注入

检测目的：验证安全芯片是否具备足够的保护能力以防止通过放射线注入而导致单粒子效应对安全芯片的影响。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试通过放射线注入干扰安全芯片运行，观察并记录安全芯片运行情况。

14.2.24 形象化功耗信息

检测目的：验证安全芯片是否具备足够的保护能力以防止通过形象化重现功耗中隐含的信息，来获取安全芯片上运行的程序信息。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：：参考设计文档尝试通过形象化功率消耗中隐藏的重复信息获取安全芯片上运行的程序信息。

14.2.25 简单功耗分析

检测目的：验证安全芯片是否具备足够的保护能力以防止通过简单功耗分析获取密钥信息。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试对安全芯片进行简单功耗分析。

14.2.26 差分功耗分析

检测目的：验证安全芯片是否具备足够的保护能力以防止通过差分功耗分析获取密钥信息。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试对安全芯片进行差分功耗分析。

14.2.27 电磁分析

检测目的：验证安全芯片是否具备足够的保护能力以防止通过电磁辐射分析获取密钥信息或程序信息。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试对安全芯片进行电磁辐射分析。

14.2.28 随机数发生器测试

检测目的：芯片随机数发生器输出的随机数应具备足够的随机性。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：对随机数发生器输出的随机数随机性进行合规验证。

14.2.29 差分错误分析

检测目的：验证安全芯片是否具备足够的保护能力以防止通过差分错误分析获取密钥信息。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试对安全芯片进行错误注入并进行密钥获取分析。

14.2.30 中断处理

检测目的：验证安全芯片是否具备足够的保护能力以防止强制中断导致安全芯片进入非预期或未定义状态。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试在敏感操作过程中，执行各类中断，观察并记录安全芯片运行情况。

14.2.31 传输信息分析

检测目的：验证安全芯片是否具备足够的能力以防止安全芯片中的传输信息被反向工程或分析。

测试条件：测试样卡、测试材料（参考附录I的要求）。

测试过程：参考设计文档尝试对安全芯片中的传输信息进行反向工程或分析。

附 录 A
公共交通 IC 卡卡片物理送检要求
（资料性附录）

A.1 送检样卡数量要求

30 张/每种

A.2 样卡外观要求及检测内容

1、检测样卡正面应包括烫印的 xx 全息防伪标志、印刷的 XX 标识等。
2、检测样卡卡面色值：XXXX

A.3 物理测试要求

A.3.1 整卡翘曲测试

对于未打凸字的卡，翘曲最大值应满足 GB/T 14916 的要求；
对于已打凸字的卡，翘曲最大值应满足 GB/T 14916 的要求。

A.3.2 卡片切边质量测试

每张卡的毛刺长度值，应应满足 GB/T 14916 的要求。

A.3.3 磁条区变形测试

磁条区的最大变形量应满足 GB/T 15120 的要求。

A.3.4 卡片弯曲刚度测试

弹性变形量应满足 GB/T 14916 的要求。
塑性变形量应满足 GB/T 14916 的要求。

A.3.5 磁条表面粗糙度测试

磁条纵向和横向的粗糙度值均应满足 GB/T 15120 的要求。

A.3.6 磁条表面轮廓度测试

磁条轮廓度应满足 GB/T 15120 的要求。

A.3.7 磁条高度测试

磁条高度应满足 GB/T 15120 的要求。

A.3.8 卡片尺寸测试

应满足 GB/T 14916 的要求。

A.3.9 卡厚度测试

卡厚度的最大值和最小值与标准值比较，应满足 GB/T 14916 的要求。

A.3.10 温湿度条件下卡的尺寸稳定性和翘曲稳定性测试

将卡依次置于下列环境下各 60 分钟：

（a）-35℃±3℃；

（b）50℃±3℃，相对湿度 95%±5%

将卡取出，放在实验室环境条件下保持 24 小时，再测卡片尺寸及卡片翘曲，要求卡片尺寸值和最大翘曲值的测量的结果应与原测量值一致。

A.3.11 标识及全息防伪标志的测试

A 限国内通用的卡面设计尺寸参考要求见图 1：

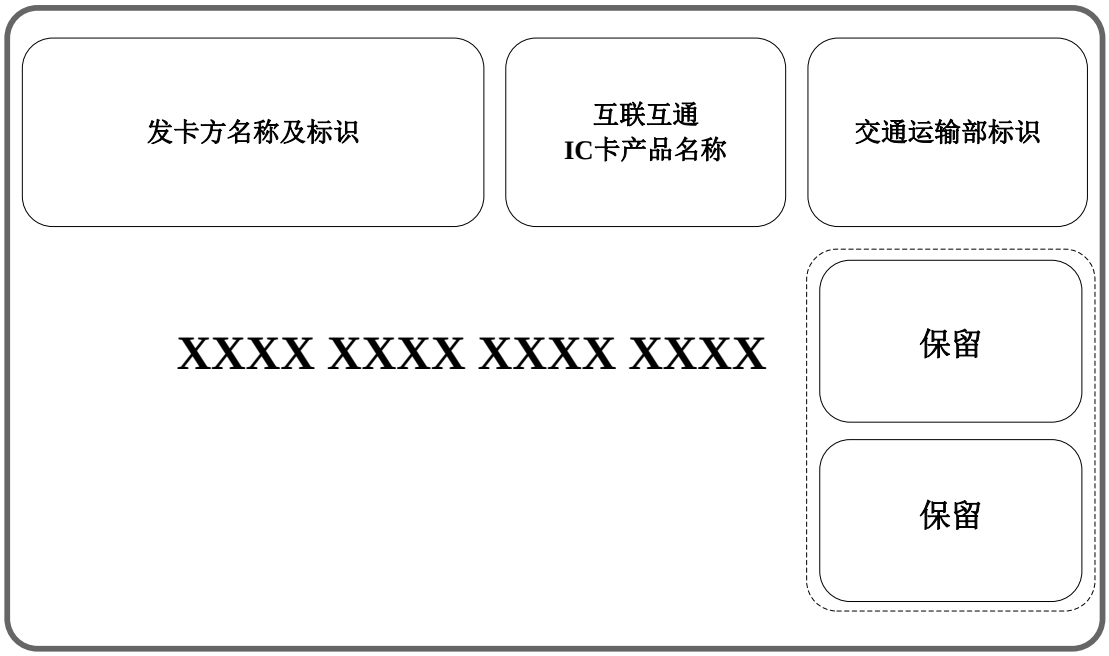

图 A.1 卡面设计图

表 A.1 新标识规格及尺寸表

新标识规格及尺寸		
A	新标识的高度	xxmm
B	新标识的投影宽度	xxmm
C	新标识三色图案与上、下边框间的距离	xxmm
D	新标识三色图案与标识边框间的底色	白色（☆2）
E	缩微文字在新标识三色图案与标识边框间居中印刷	圆黑，0.7Pt
F	新标识右上端外框边沿垂直线与同侧卡片边沿间的距离	xxmm
G	新标识下方水平外框边沿与同侧卡片边沿间的距离	xxmm
H	新标识上方水平外框边沿与全息防伪标志间的距离	xxmm
I	新标识右上角、左下角的圆角半径	xxmm
备注☆	1、A～B，F～J 尺寸的公差为±0.30mm，C 尺寸的公差为±0.15mm	

	2、标识在白色或浅色背景下使用，无法突出显示标识的覆盖区域时，新标识三色图案与标识边框间的底色应采用浅灰色或批准的其他对比色。 3、新标识三色图案与标识的外边框应居中对齐。 4、xx 标识在卡上的使用规格及尺寸要求同新标识。	

附 录 B
公共交通 IC 卡卡片应用送检要求
（资料性附录）

B.1 范围

本部分适用于公共交通 IC 卡的卡片制造商、应用设计商和个人化技术人员。

B.2 技术要求

B.2.1 个人化要求

送检送检厂商可以选择以下两种方式的一种进行送检（个人化数据见第 3 部分）。

请送检送检厂商在送检时声明卡片实际支持的算法类型，具体可选的类型包括国际算法（对称加密算法基于 DES、非对称加密算法基于 RSA、哈希算法基于 SHA-1）、国密（SM）算法（对称基于 SM4、非对称基于 SM2、哈希算法基于 SM3）、同时支持双算法（同时支持上述两类卡片所涉及的加密方式，根据规范规定进行选择）。具体每种类型的卡片送检张数详见本部分第 2.2 条和 2.3 条规定，请特别注意支持不同算法类型中卡片[3]PDOL 数据的不同。

根据卡片的功能界面不同可分为接触界面和非接触界面，请在个人化时注意两者相同特征中不同个人化数据的要求，主要区别在 PDOL 个人化数据的不同，同时非接界面需要将 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。

B.2.2 方式一

提交卡片个人化工具（可以是软件或者装有该软件的笔记本电脑），并且参照本部分第 3 节的个人化数据要求，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，此种方式需提供 30 张测试卡片。推荐送检厂商采用方式一送检。

B.2.3 方式二

B.2.3.1 概述

将送检样卡按照本部分第 3 节的个人化数据要求，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。总计需要约 500 张卡片。

注 ：测试中如测试样卡不够，可能需送检厂商另外提供样卡。

B.2.3.2 单国际算法卡

针对送检的卡片，如果卡片为不支持国密算法的单国际算法卡片，则联机应用需个人化 1-26 号特征进行送检。PDOL 请选择基本特征中的 PDOL（若卡片不支持国密）项。下面的表格列出了每种卡片特征应制作的卡片张数。

表 B.1 单国际特征卡数量

特征	仅非接触式
1	50
2	5
3	6
4	1
5	1

3) [3] 本章节中的卡片如无特殊说明则特指公共交通 IC 卡。

6	1
7	1
8	4
9	6
10	15
11	1
12	1
13	1
14	1
15	1
16	3
17	1
18	1
19	1
20	1
21	1
22	1
23	1
24	1
25	1
26	1

卡片特征	单币	双币
31	2	4
32	12	24
33	6	12
34	17	34
35	12	24
36	2	4
37	10	20
38	2	4
39	6	12
40	3	6
41	7	14
42	7	14
43	11	22
44	3	6
45	7	14
46	50	N/A
47	30	N/A
48	1	2
49	1	2

B.2.3.3 单国密算法卡片

如果送检卡片为仅支持国密算法的单算法卡片，联机卡片需进行卡片特征为1至26的个人化操作，电子现金卡片需进行特征值为29、30的个人化操作，个人化数据中PDOL需选择基础数据中的PDOL（若卡片支持国密）。同时针对单国密算法卡片，静态认证数据对象和动态数据认证对象须按照个人化数据中AIP中支持的脱机数据认证类型和B.3.4条中的具体的密钥对应关系进行个人化操作。下面的表格列出了每种卡片特征应制作的卡片张数。

表B.2 单国密特征卡数量

特征	仅非接触式
1	50
2	5
3	6
4	1
5	1
6	1
7	1
8	4
9	6
10	15
11	1
12	1
13	1
14	1
15	1
16	3
17	1
18	1
19	1
20	1
21	1
22	1
23	1
24	1
25	1
26	1

卡片特征	单币	双币
31	2	4
32	12	24
33	6	12
34	17	34
35	12	24
36	2	4

37	10	20
38	2	4
39	6	12
40	3	6
41	7	14
42	7	14
43	11	22
44	3	6
45	7	14
46	50	N/A
47	30	N/A
48	1	2
49	1	2

B. 2. 3. 4 双算法卡片

针对同时支持国产加密算法和国际算法的双算法卡，联机卡片按照 1 至 26 号卡片特征进行卡片个人化，与单独支持国密算法卡的不同之处在于除了静态数据和动态数据认证对象应同时个人化国际算法和国密算法两种类型，具体可见 B.3.4 条中的具体对应关系。

除此之外，考虑到具体的市场需求：卡片支持两种非对称算法但仅支持一种对称算法，卡片仅针对非对称算法进行切换，因此还应准备个人化特征 27、28 用于测试联机应用。这两个特征的基于国际算法和国密算法的静态和动态认证必备数据对象与其他特征的双算法卡相同。

下面的表格列出了每种卡片特征应制作的卡片张数。

表 B.3 双算法特征卡数量

特征	仅非接触式
1	100
2	8
3	10
4	1
5	1
6	1
7	1
8	6
9	8
10	30
11	1
12	1
13	1
14	1
15	1
16	6
17	1
18	1

19	1
20	1
21	1
22	1
23	1
24	1
25	1
26	1
27	1
28	1

特征	仅非接触式	仅非接触式
币种	单币	双币
29	12	24
30	12	24
51	12	24
52	12	24

卡片特征	单币	双币
31	2	4
32	22	44
33	10	20
34	32	64
35	22	44
36	2	4
37	18	36
38	2	4
39	12	24
40	6	12
41	12	24
42	12	24
43	22	44
44	6	12
45	14	28
46	50	N/A
47	30	N/A
48	2	4
49	2	4

B.2.4 文档要求

个人化数据要求

送检厂商在送检时应提交以下文档：

——芯片资料（请按附件 1 的表格填写），包括：

——芯片型号；
——芯片基本性能（CPU 位数、ROM 及 E2PROM 容量）。
——卡片技术参数手册（至少应包括以下内容）
——卡片文件管理结构；
——卡片安全特性；
——卡片指令集（包括规范中未定义的个人化指令）；
——卡片 ATR 的说明；
——COS 版本号及从卡片中读取该版本号的方法；
——卡片内部所有文件的结构图和相应的文件标识符 FID。
如是硬掩膜产品，应提交芯片制造商出具的硬掩膜证明。
如果卡内含有多个应用，应注明受检卡内含有几个应用，各为何种应用。
非接触 C 卡电气特性和协议测试功能一致性声明。

B. 3 数据要求

B. 3. 1 概述

本部分第 3.2 条列出了个人化数据的公共部分，称为基本特征，第 3.5 条列出的每个个人化特征都继承于基本特征。

本部分第 3.3 条列出了所有可能被用到的公钥证书、非对称公私钥对、对称密钥等信息。

本部分第 3.5 条列出了针对不同测试点所涉及的各种个人化数据，称为卡片特征，卡片特征继承自基本特征。

本部分第 3.4 条列出了卡片特征与选用的密钥之间的关系。

基本特征和卡片特征为测试时所必需的数据对象，可能并不能涵盖规范中规定的所有数据对象，对于没有在此定义的数据对象，送检厂商可自行为其赋值。

根据卡片功能的不同，送检厂商可能不需要支持本部分中列出的全部卡片特征。表 4 列出了支持不同功能的卡片所应支持的卡片特征。

表 B.4 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 至卡片特征 45，卡片特征 48 和卡片特征 49
脱机交易扩展应用	卡片特征 31 至卡片特征 49
非接触式联机交易应用	卡片特征 1 至卡片特征 26（加入 PPSE 并采用非接界面下的 PDOL 个人化数据）
仅支持国密算法的卡片	
脱机交易应用	卡片特征 31 至卡片特征 45，卡片特征 48 和卡片特征 49
脱机交易扩展应用	卡片特征 31 至卡片特征 47
非接触式联机交易应用	卡片特征 1 至卡片特征 26（加入 PPSE 并采用非接界面下支持国密算法的 PDOL 个人化数据）
支持国际算法和国密算法的卡片	
脱机交易	卡片特征 31 至卡片特征 45，卡片特征 48 和卡片特征 49
脱机交易扩展	卡片特征 31 至卡片特征 49
非接触式联机交易应用	卡片特征 1 至卡片特征 28（与仅支持国密算法的卡片特征相比加入了国际对称与非对称算法相关的必备数据）

B.3.2 基本特征

B.3.2.1 联机交易应用测试基本特征

表 5 列出了支持联机应用功能的卡片的基本特征，数据分组可由送检厂商自行设计。但 SFI=1 的文件的 1 号记录除外，SFI 1 的 1 号记录应存储以下数据：

70 13 57 11 38 88 88 01 00 00 11 17 D3 01 22 01

01 23 45 67 89

表 B.5 联机应用基本特征

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
应用交互特征	82	5C 00
应用标签	50	50 42 4F 43 20 43 72 65 64 69 74
应用主帐号	5A	38 88 88 01 00 00 11 17
应用主帐号序列号	5F34	01
应用首选名称	9F12	43 41 52 44 20 49 4D 41 47 45 20 30 30 30 31
应用优先指示器	87	01
应用用途控制	9F07	FF C0
应用版本号	9F08	00 30
CDOL1	8C	9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9F 21 03 9C 01 9F 37 04
CDOL2	8D	8A 02 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9F 21 03 9C 01 9F 37 04
持卡人姓名	5F20	46 55 4C 4C 20 46 55 4E 43 54 49 4F 4E 41 4C
CVM 列表	8E	00 00 00 00 00 00 00 00 41 03 42 03 5E 03 43 03 1F 00
CA 公钥模索引	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
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）	9F 38	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 33 03 9F 4E 14 9F 7A 01
PDOL 非接触界面（若卡片支持国密）	9F 38	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 9F 33 03 9F 4E 14 9F 7A 01 DF 69 01
PIN尝试计数器	9F17	03
PIN尝试限制数	--	03
参考 PIN 数据	--	12 34
第二应用货币代码	9F76	00 00
服务码	5F30	02 01
磁道 2 等效数据	57	38 88 88 01 00 00 11 17 D3 01 22 01 01 23 45 67 89
产品标识信息	9F63	11 22 33 44 55 66 77 88 00 00 00 00 00 00 00 00

B.3.2.2 脱机交易应用测试基本特征

读记录时卡片至少应返回以下数据，以下数据至少分四条记录存储：

93：签名的静态应用数据

8F：CA 公钥模索引

90：发卡机构公钥证书

92：发卡机构公钥余项

9F32：发卡机构公钥指数

9F46：IC 卡公钥证书

9F47：IC 卡公钥指数

9F48：IC 卡公钥余项

5F24：应用失效期

5F25：应用生效期

5A：应用主帐号

9F74：电子现金发卡机构授权码

9F08：应用版本号

表 6 定义了脱机交易的基本特征，表 7 定义了双币脱机交易的基本特征，表 7 未定义的数据见表 6，表 6 未定义的数据在表 4 中规定。

表 B.6 脱机交易基本特征表

数据	标签 — T	长度 — L	数值 – V
电子现金余额	9F79	06	00 00 00 01 00 00
电子现金余额上限	9F77	06	00 00 00 01 50 00
电子现金发卡机构授权码	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）	9F38		9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04
PDOL 非接触式（若卡片支持国密）	9F38		9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04 DF 69 01
产品标识信息	9F63	10	11 22 33 44 55 66 77 88 00 00 00 00 00 00 00 00
连续交易限制数（国际-货币）	9F53	01	03
密文版本		01	0X01，0X17
发卡机构应用数据	9F10	0x13	07 01 01 03 00 00 00 xx 0A 01 xx xx xx xx xx yy yy yy yy
脱机可用余额	9F5D	06	00 00 00 00 00 01

表 B.7 双币脱机交易基本特征表

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

B.3.2.3 扩展交易测试基本特征

表 8 定义了脱机交易扩展的基本特征，表 8 中未定义的数据在表 6 和表 4 中定义。

表 B.8 脱机交易扩展基本特征表

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
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
来自从应用提供商、发卡机构或交通 IC 卡供应商的 1 个或多个附加（专用）数据元	DF11（前20字节与电子钱包的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
电子现金分段扣费抵扣限额	DF62	00 00 00 00 00 0
电子现金分段扣费已抵扣额	DF63	00 00 00 00 00 0

除此之外，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。如下：

变长文件，其 SFI=0x1A

该文件至少可开通 14 个行业应用，即至少可 Append 14 条记录。每个记录不超过 128 字节，举例如下。

表 B.9 行业应用记录格式表

记录名称	行业应用信息	记录大小	128
字节	数据元	长度（bytes）	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	

开通密钥：191A5F026001DF259A03019C37049F11

循环文件，其 SFI=0x1E

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

B.3.3 密钥信息

B.3.3.1 对称密钥-3DES

B.3.3.1.1 电子钱包对称密钥

表 B.10 电子钱包对称密钥表-3DES

密钥名称	密钥值（HEX）
圈存主密钥（MLK_01）	D3D6E8836832FDD4706D0671BB8BD28B
圈存主密钥（MLK_02）	B117DE007E79E786634B73A483AE9746
圈提主密钥（MULK_01）	E938FDDAAE9E5C8CE6A137B7F162E57E
圈提主密钥（MULK_02）	EFFA773C95533A0371BBA0B2D545734A
消费主密钥（MPK_01）	70E9BEA697723DF83605EBBCB7C2C7C4
消费主密钥（MPK_02）	6F153B35A97E1B56A1F8A3CE7AC5DAE2
应用解锁主密钥（MUBK）	07C3EAA0997CE026B8629A77CCB5AC9A
应用锁定主密钥（MBK）	48396B19B5E9765FDA25EC5C394058A0
应用主控密钥（MAMK）	0F6FF9CC72204371093916F9E8BBF062
TAC 主密钥（MTK）	138D34F84B2031FF479E71BEFF107A76

B.3.3.1.2 电子现金对称密钥

表 11 定义了 DES 算法适用的对称密钥，送检厂商在使用此类密钥时无需使用 PAN 和 PANSN 分散这些密钥。

表 B.11 电子现金对称密钥表-3DES

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

B.3.3.2 对称密钥-SM4

表 12 定义了 SM4 算法适用的对称密钥，送检厂商在使用此类密钥时无需使用 PAN 和 PANSN 分散这些密钥。

表 B.12 电子现金对称密钥表-SM4

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

B.3.3.3 发卡机构公私钥对及证书RSA-1152位

CA 公钥模索引

标签 = 8F

长度 = 01

值 = 23

CA 公钥

C5F788D993CF8D3C7FEB4E542EEA267FEA8555CF06F3EA9AFDB4F1AC2EE3998820017041B0EFEC5DF2B6A9F4533E492A5514BEA621C772DADD5D82D4EEF04A67DA9A64520DFF00BB19F1D0E4E9FB47F0C4A6468FADA3CC812C734EEA0C53914F9E26332BF7945B091453F97277D3C955482F5C179C94A85294BC812B68045D171AEB2C4065C15B94E39070F456BE2745

CA 公钥模指数

010001

发卡机构公钥

C035D8F6D8E3E2EBAE78AD5BE456A7C06C2051B6E8271C8AF661113203893B42F0AB631CB5BFEB0894CDE3A1FC9BACFF6BF8D5E28CD918BAF22C73DFC31352ABC3F9F1BF5EDCF79A3B1727F8E958AABC098AC6B1FD5A98095715DBA46F2510249B8EEE8FF7EA33C03A6F7943DA7D9ED0CB4FB9A1182967B17314701AC51969D44B85798C8ECE039CD0C11714E9CC19EB

发卡机构私钥

8023E5F9E5ED41F2745073929839C52AF2C03679F01A13074EEB60CC025B7CD74B1CECBDCE7FF205B889426BFDBD1DFF9D508E970890BB274C1DA2952CB78C7282A6A12A3F3DFA65A9641C858DD4851F32571E4B29E961F40158387F76C9BD79C004CCB9AE8FED07FAF5D79A6B81C4EDA48E8611E800D6A09E5CB95189F146031F98029475BCD98B36DE50A736F77CAB

发卡机构公钥证书 = （1152 位 s, 144 字节 s, 0x90）

标签= 90

长度= 90

值=

A9CD4E3FD4CB485C86959B86021655A894BBCD7749F8E7086CE386636093CD6639EE7EF762FB738F270EA7F71E7D5F5CDACCE2DC1B677AD74E583B51970270364F348AAD3023FE0C4AC2654363DAB3FAE2E9E137414C67C52CADEC3274646B0F446D79DBD440859D995E7903DA83C4C33340BE4C850B5CBFC9FA1175D8048349D3266E6DB05B6DDB6DF1F55CB282D702

发卡机构公钥余项

标签= 92

长度= 24

数值=DA7D9ED0CB4FB9A1182967B17314701AC51969D44B85798C8ECE039CD0C11714E9CC19EB

发卡机构公钥指数

标签= 9F32

长度= 01

值= 03

哈希输入数据：

02388888FF123000000101019001C035D8F6D8E3E2EBAE78AD5BE456A7C06C2051B6E8271C8AF661
113203893B42F0AB631CB5BFEB0894CDE3A1FC9BACFF6BF8D5E28CD918BAF22C73DFC31352AB
C3F9F1BF5EDCF79A3B1727F8E958AABC098AC6B1FD5A98095715DBA46F2510249B8EEE8FF7EA3
3C03A6F7943DA7D9ED0CB4FB9A1182967B17314701AC51969D44B85798C8ECE039CD0C11714E9C
C19EB03

参与脱机数据认证的静态数据为：

5A0838888801000011175F24033012315F25039507019F08020030

认证中心签名的发卡机构公钥证书输入数据 ：

6A02388888FF123000000101019001C035D8F6D8E3E2EBAE78AD5BE456A7C06C2051B6E8271C8AF6
61113203893B42F0AB631CB5BFEB0894CDE3A1FC9BACFF6BF8D5E28CD918BAF22C73DFC31352A
BC3F9F1BF5EDCF79A3B1727F8E958AABC098AC6B1FD5A98095715DBA46F2510249B8EEE8FF7EA
33C03A6F794383A24B3CA3244EDDBB814F65237CA6CF53AF4077BC

数据验证代码

DA C1

参与签名的记录数据为：

5A0838888801000011175F24033012315F25039507019F08020030

B.3.3.4 发卡机构公私钥对及证书RSA-1280位

暂无，此条保留给将来使用。

B.3.3.5 发卡机构公私钥对及证书RSA-1408位

CA 公钥模索引

标签 = 8F

长度 = 01

值 = 24

CA 公钥模

C82208F7604FE17ABA1839873F2DF77FF6304A6292986015DD1223F90FC0314E0E14836D4168565AE
E4E255F932307F60AFC11000DB545C4BB21FBC6DDF8B27E7AFB29D243D9E00E423226D6D22DE12
98FE67384BA761EE0B24C3775717942ACC042885121375340E0F3FF47E66CD91A18CC8B04EC0B285
DCE8A4067E8142406DD469412CBF8B268B369C3D1B89F71F9076EC5BF10D00BF94115406BC9FB39
DFB829EAC599F1D1BA94868501E2A1E59B

CA 指数

010001

发卡机构公钥

CE69697219A3AB2438210B449809119F52E12291F7D642B6C8D72828482FE4B6AB1FB7D3B4A685DF
971F8EFD898E82BB8F31D9A639B7F76215CDA8FF9A6387E2375D619DB4E0440BBAEB4232BF620E
A73BAAF60F4195D4571F82C2BAC6B17196CEFA5D3A3C59EDA526BE69705DB89058D72903F2A6A
FF949FF8BF6D2FF44968D24D8F8DB2437C0ECAA63B57BAFC9AAD1082B549F009EAD566BE0EB61
0EB8897033EF2296330DD3C3B04BB7C1D7E3C481

发卡机构私钥

899B9BA1666D1CC2D016078310060BBF8C96170BFA8ED72485E4C570301FEDCF1CBFCFE2786F03E
A64BFB4A9065F01D25F7691197BCFFA4163DE70AA66ED05417A3E4113CDEAD807D1F22C21D4EC
09C4D271F95F810E8D8E3786DE863D69AD7D2FFDBEBF85D2CED352245504F751FB439F7D82F8BF
A759C5D66AD8D67CEE9E562109F6D24F154163A69C0FD8D5A592DA761BDDCF5E177FE3AF023AE
50A5FE146F34B648CC12FA2D08217B7C27B20A12B

发卡机构公钥证书 = （1408 位 s, 176 字节 s, 0xB0）

标签= 90

长度= B0
值=
4E3518A497AEDC0EF0F665474C59C9CD1592A271087090E95D2CBD22B041019CF81D8C036D29F0A
00FFEA13895B773FEBDC092D8F4FC6E9D6267FEAD38C46A53997A3F5D75A3AF40C06D160BDA67
514D273C033411EABED67CCAF301FD6709BADDBC9C9CB1A733C3E44024D5BD89CEC38DFBC479
76C8BC23EAED1D475AA41887EC04941F29DEECBC4139B8BFF2B709FB0922AE095E840E52C4CB08
5D9AB1B921F10BE1DD23C22A12228350C03BDE07EE
发卡机构公钥余项
标签= 92
长度= 24
数值=AFC9AAD1082B549F009EAD566BE0EB610EB8897033EF2296330DD3C3B04BB7C1D7E3C481
发卡机构公钥指数
标签= 9F32
长度= 01
值= 03
认证中心签名的发卡机构公钥数据：
6A02388888FF12300000010101B001CE69697219A3AB2438210B449809119F52E12291F7D642B6C8D7
2828482FE4B6AB1FB7D3B4A685DF971F8EFD898E82BB8F31D9A639B7F76215CDA8FF9A6387E237
5D619DB4E0440BBAEB4232BF620EA73BAAF60F4195D4571F82C2BAC6B17196CEFA5D3A3C59ED
A526BE69705DB89058D72903F2A6AFF949FF8BF6D2FF44968D24D8F8DB2437C0ECAA63B57BC670
86BAFBC04C7F7EFE6264A6D72F525251912CBC
哈希输入数据：
02388888FF12300000010101B001CE69697219A3AB2438210B449809119F52E12291F7D642B6C8D72828
8482FE4B6AB1FB7D3B4A685DF971F8EFD898E82BB8F31D9A639B7F76215CDA8FF9A6387E2375D6
19DB4E0440BBAEB4232BF620EA73BAAF60F4195D4571F82C2BAC6B17196CEFA5D3A3C59EDA52
6BE69705DB89058D72903F2A6AFF949FF8BF6D2FF44968D24D8F8DB2437C0ECAA63B57BAFC9AA
D1082B549F009EAD566BE0EB610EB8897033EF2296330DD3C3B04BB7C1D7E3C48103
发卡机构认证哈希结果：
C67086BAFBC04C7F7EFE6264A6D72F525251912C
数据验证代码
DA C1
参与签名的记录数据为：
5A0838888801000011175F24033012315F25039507019F08020030

B.3.3.6 发卡机构公私钥对及证书RSA-1984位

CA 公钥模索引
标签 = 8F
长度 = 01
值 = 24
CA 公钥模
B126D0A69696AF80731C6588F532CCF0FAC9A8B011372FE42B40531FD95E507554637C84D20927C2
4A3D156BA7B527F8052B42052D6A567821136AFAA6ACC7011A415E2E3D4947E11250F730B44B75E
19D5A8CB30E238892EDE3EAEB54E6277388B89E53AC7F2739542F5D1EE1287BC543066821783387E
1A54105D057E1B377591B181E97044985087461OEAAEDBA50E32DDA712342841AC9B3634422A0C97
D8953A561CABB364D919186B086BCC4F3CA1A3E98EEC6A4C2960AE2BED6E1B8C18A5E73883A28
57CD46DFEA8D6A4F11B1B222F5263A78E00C4F2ADA856B0487A6513BDF1CE7C5FFB4EC01A3E69

BD94F718F6BC35FCC6C620B
CA 指数
010001
发卡机构公钥证书 = （1984 位 s, 248 字节 s, 0xF8）
标签= 90
长度= F8
值=
193B971359D3E89A2A571AE2122D26430425305DCFB35EFE7C782D2FC8D64C07183BAAAF5E0B31
BF224B5C7348E7064F6420334007A7D935C8647B6F33BAED4877E357AFD3705E040ECAA8007643A3
32E3F7FEB0665D9C755DCC4C9B712B50BF5B99472EDEE9D7E5ADC54D92E0BD50AB4657BCC1336
E505A90B4BA5B5420C9E8F6CDFC43AD22056795EEDFA0DCE0CC9AECA4D961EDBD551B8A9725
93A19E561877F073BF967635153BFFD19D4B32E2214FCC207B368EF6C04CE53E4F04ADB3C32B5F97
E811CAE5783BB582EEDDCDE2EB25A04B4AB454DD9F644FB3BC4FBFAA3287AA7C732DF7523C8
F584CC094923D15E7110E1709F79926
发卡机构公钥余项
标签= 92
长度= 24
数值=B1F73EAC3DAAFF10F54AFE269D55BCCA7AC1AB3E6977620404306252057830 9C2E98184D
发卡机构公钥指数
标签= 9F32
长度= 01
值= 03
发卡机构公钥：
BE41AACA0C6A8B8938FE69E1564640985B0CCA43B034CE1D62C8E3E777912047F1523AA79761217
5207CDA361152EC984BDFBB3C3B57476014D84F3949A151CCC71B20F8682B68331D55AA702082B5
815BF9EFC278B95A970C1486DDE544B197E4329A9894376684B708185DBE91D343AC6D35CFD4BD
B46A0984020011085272F2F4286294A130723600253270FF4A59BADBB0956ED5D28AF817F1E7D1032
53EEF2548F36689A7A25A60D2BDE2CAF5C9F1B3F583FD15344750A97E08713A31E54EFEE41B025F
9C5AD64A313793C66C00D7867FEAB1F73EAC3DAAFF10F54AFE269D55BCCA7AC1AB3E69776204
043062520578309C2E98184D
发卡机构私钥：
7ED671DC084707B0D0A99BEB8ED98065920886D7CACDDEBE41DB429A4FB615854B8C271A64EB6
BA36AFDE6CEB637486587EA7CD2D23A2F95633ADF7B866B8BDDDA1215FAF01CF022138E71A015
AC7900E7FBF52C507B91BA080DAF3E98D8766542CC671062CF99ADCF5ABAE929B68CD7C848CE8
A8DD3CD9C0658015439986990A2421D4443678B12BABAE019B2779D6C535BA1DC856914576EE91B
CEB4A71EE302D919C252B3BC3F4EC7722EE15408945D293A5890E79B3F084FCFA71C6FCB9BCEB3
1D32E695193AC7B9BD0EE03A8FBEB8236C7DF505E3B0D64C9A1C23B4BBEFD6EA9432BA6A0A0C
2EA5C4541F71980E511FB2A513C89313
认证中心签名的发卡机构公钥数据：
6A02388888FF12300000010101F801BE41AACA0C6A8B8938FE69E1564640985B0CCA43B034CE1D62
C8E3E777912047F1523AA797612175207CDA361152EC984BDFBB3C3B57476014D84F3949A151CCC7
1B20F8682B68331D55AA702082B5815BF9EFC278B95A970C1486DDE544B197E4329A9894376684B7
08185DBE91D343AC6D35CFD4BDB46A0984020011085272F2F4286294A130723600253270FF4A59BA
DBB0956ED5D28AF817F1E7D103253EEF2548F36689A7A25A60D2BDE2CAF5C9F1B3F583FD153447
50A97E08713A31E54EFEE41B025F9C5AD64A313793C66C00D7867FEAB2E7D3E02B336DD0F21786B

C0FB0737664BF317ABC
哈希输入数据：
02388888FF12300000010101F801BE41AACA0C6A8B8938FE69E1564640985B0CCA43B034CE1D62C8
E3E777912047F1523AA797612175207CDA361152EC984BDFBB3C3B57476014D84F3949A151CCC71B
20F8682B68331D55AA702082B5815BF9EFC278B95A970C1486DDE544B197E4329A9894376684B7081
85DBE91D343AC6D35CFD4BDB46A0984020011085272F2F4286294A130723600253270FF4A59BADB
B0956ED5D28AF817F1E7D103253EEF2548F36689A7A25A60D2BDE2CAF5C9F1B3F583FD15344750A
97E08713A31E54EFEE41B025F9C5AD64A313793C66C00D7867FEAB1F73EAC3DAAFF10F54AFE269
D55BCCA7AC1AB3E69776204043062520578309C2E98184D03
发卡机构认证哈希结果：
B2E7D3E02B336DD0F21786BC0FB0737664BF317A
数据验证代码
DA C1
参与签名的记录数据为：
5A0838888801000011175F24033012315F25039507019F08020030

B.3.3.7 发卡机构公私钥对及证书-SM2-推荐曲线-索引57

CA 公钥模索引
标签= 8F
长度= 01
值= 57
【CA 公钥模】
2C631314565FA083830F81A930F60AB75290D9A1C273C2D72987364C26B0BBD6C3730C57A6884CA
D05F24BBA45D026633DE271F4FFD474929FDFB898A1E4F196
【发卡机构公钥】
9F483BF2CC71C5093728318061E3F768EA7C170F82DD8C4B979FBD8C76A129F93FB5746E96F5E49B
987FFB521E473B25E1B017C30BE3FC638BA14D5FA4AADC16
【发卡机构私钥】
1F34E60E7FAC21CC2B26DD34462B64A6FAE2495ED1DD383B8138BEA100FF9B7A
【参与脱机数据认证的静态数据】：
5A0838888801000011175F24033012315F25039507019F08020030
【9F4A 数据】：82
【AIP 数据】：根据卡片特征而定
【证书格式】：12
【发卡机构标识】：38888801
【证书失效日期】：1220
【证书序列号】：000001
【发卡机构公钥签名算法标识】：04
【发卡机构公钥加密算法标识】：00
【发卡机构公钥参数标识】：11
【发卡机构公钥长度】：40
【CA 哈希值】：
D80D666CCDB048514079AD72F1B20C984DD8BE75E82E8F4B367BF6E93C3E189FFE8F9B39EC1EFC
28B9F301ACD797467819E5F5D3B34F5CD0B5A9B25882B3EA0E
【发卡机构公钥证书 Tag_90 】：
123888880112200000001040011409F483BF2CC71C5093728318061E3F768EA7C170F82DD8C4B979FBD

8C76A129F93FB5746E96F5E49B987FFB521E473B25E1B017C30BE3FC638BA14D5FA4AADC16D80D
666CCDB048514079AD72F1B20C984DD8BE75E82E8F4B367BF6E93C3E189FFE8F9B39EC1EFC28B9
F301ACD797467819E5F5D3B34F5CD0B5A9B25882B3EA0E
签名的静态应用数据：
【签名数据格式】：13
【数据验证代码】：DAC1

B.3.3.8 发卡机构公私钥对及证书-SM2-推荐曲线-索引58

暂无，此条保留给将来使用

B.3.3.9 IC卡公私钥对-768位

E=
03
N=
C5BD39EFF93AC495A771653D66341F660E8DF31237C0A28729661C45C9F4384CF26F687B69FB717C
7595B4D26B533459BC1FC4367623654C29BAEF473FD085C191EC9626E579E2333322944AC7C31E850
928FD8B098289DD917D3A288B7BDD55
P=
FC03512FED42394B442611AAC061B66523EC90FB6745D31297CA310E1F6833FFFFCC5ED34BF8AC3
B52C7AA754FCF298B
Q=
C8DE1801D80CDFCB0FC2FE4E6C7B1DCB99C9FBED69F4B9EA3EEAD4166BDE9CA582E587A870D
7823EF64D73C320F5309F
d mod （p-1）=
24E27767845A44F87728FB3CFA9B528ECB0B3CCD0EF871442F63307AD8ADEFAE704A0136FBCF91
A5BD1FEC1AEF6B6AB1
d mod q-1=
BB1B1E73C143A4C72B4470CCAE82346BEE3256E87CF548A4E9BCA698C81C52005EA0DE2FCA050
53F0F01709EC7B97D73
1/q mod p=
A682730F9213805749E474FB08D6C00888592B188C7BD6D15CC8643854754ED4C8C32300D1631FF59
9F744C07C90F1BE

B.3.3.10 IC卡公私钥对-1152位

E=
03
N=
C345B4CD6FFC58E5C7ACFDFD6D0EA4EA9CEB288F30E5CAE9499D38A6FD0E378194A45A79E25E
6DDE3DE5AA42584D450B350892B689F05E5B1A54B401CC9E486B43F6290A7C3863F3790EC4BBB34
E078D7D98E247E89EFAB315C8F0A6E9B2A4802473C24800F16CF499D63F940099FA6B759F06226DE
4A07C2E47A387D3A72A2FEB78028C04E5E903AC0BE73A7AF73FE5
D=
822E7888F552E5EE851DFEA8F35F189C689CC5B4CB43DC9B8668D06F535ECFABB86D91A696E99E
942943C6D6E588D8B2235B0C79B14AE992118DCD568869859CD7F970B1A82597F67A4E5FB9B1BF6
E1096942D3ECD2258A0D1CDD48BBB60E799B09BB0FA9A5A1A2E9B39BD379792AA0135C9E4C9D
6D642366EDB452A5A4E8D3186F60747EB2B9C10A579B490C5985873
P=

F824ECAFB6C399C804E97C3F0577360F4DB2B35FD686AF75DA8F7356E446797322845249C02223984
7497AF19CFC0DE4CE7D15B9FCA96566383EEF7CF39019797C5340FA7BFA9027
Q=
C974487571EB48AC96D1222AAF743FB28D617E757A1A99A3C0FAC5793523CC3B8E7B5176DD1BD7
D15DA6B4020EA72F45B981A60E4F87F0FF68C8082330946571378217 66D6982B13
d mod （p-1）=
A56DF31FCF2D1130034652D4AE4F795F8921CCEA8F0474F93C5FA239ED8450F76C5836DBD56C17B
ADA30FCA11352B3EDDEFE0E7BFDC643997AD49FA8A26010FBA83780A6FD51B56F
d mod q-1=
864D85A3A14785C8648B6C1C74F82A7708EBA9A3A6BC666D2B51D8FB78C28827B452364F3E128FE
0E919CD56B46F74D926566EB435054B54F0855AC22062EE4B7A56BA448F101CB7
1/q mod p=
55FC824EF4466D5C0FAE99FE250633410E762A8402F6CF6F0C71CACCC9D16A9652E2CC74F546445
C6B9DFD33F5D699799F8CD7908CBC03E9DE6A350B75A2165FD73782B8B0309009

B.3.3.11 IC卡公私钥对-1280位

E=
01 00 01
N=
D0 1B E7 8B 92 64 3C 6C 35 20 AA 59 FD 28 08 48 69 F8 05 E7 FC 94 F4 28 98 69 9C A8 97 0E 50 92 3C 90 96 25 F4 5B 40 47 2B 42 95 D6 DA 94 23 DB 16 1B F5 CE AB 58 06 C0 2F 7E C0 25 B5 12 AA 32 1F 6D 68 71 5A 5F EE E6 92 3F 95 14 34 82 1D 9B 92 31 31 0C 47 31 94 69 F0 D8 01 46 3A 00 EA 8B 22 22 5E 3D 33 3A B1 71 86 59 F8 9D E4 29 3F 58 D5 CB 54 1F E1 40 CF D3 E5 9E 11 E3 8C 4B DC A2 83 2F 61 99 51 CA D7 77 23 6D 7C B7 75 76 C8 E4 C5 F9 02 F9 0F 38 49 94 3D 4C 7D 0F 04 94 79 B9
D=
01 BC 64 84 B8 31 38 85 23 E1 A4 8A 20 F5 21 DC 8E 1B 10 DC 36 87 27 8C E4 78 92 63 4A F4 9B 9C C7 54 8D 6C 13 A0 64 90 DE 13 82 C7 20 06 4C 50 EF 86 46 D9 4A 79 EE D4 7B 90 F0 6E B5 6B F5 1A 25 EE 4B B3 66 5A EB D5 E5 DD 11 E9 46 91 84 9D B1 10 9C A3 9D 68 24 21 8F 08 D7 FD 99 7E 5E E2 82 D3 75 29 F8 B0 D5 0D 00 3D A6 DE 27 14 5E 12 AD 7F 33 B3 77 5C BB 1C 05 A0 E3 5F E2 3E C0 F5 B5 52 3C F8 FB 54 92 B9 E7 4B 8F F9 CB F8 E7 DF D2 3A D6 97 BD 78 5B 7F 54 96 74 CC 6B C8 96 61
P=
D6 27 02 8E 7F 01 5F 22 22 56 AB 78 7E E1 F3 28 2F 37 2C 1F EA 6B 7D E7 49 B4 BA 6F B1 12 56 D5 92 4F F3 45 EE F2 17 A4 D0 FB D5 0C 99 72 3D C5 B6 88 66 6E C4 0F AB 01 CA CC 9D 70 15 23 13 A1 4E 12 6A A0 70 CB 46 90 DF 0A B9 33 99 D6 44 CF
Q=
F8 C6 92 E9 77 C1 98 63 0B D1 B6 B0 50 5D 3A 68 64 42 9D 76 F3 D4 01 5A CD 82 B1 C8 C2 C4 92 CB 45 19 69 97 93 4E CF 8E E4 21 24 C0 56 24 4B 9A 2B 95 AC 3B E5 0A C1 C6 D1 B2 B2 4F 84 86 5B 02 CB 92 8A A6 A3 60 12 25 0B A0 05 F1 9F 58 0A F7
d mod （p-1）=
82 1F 0F E9 9F 78 28 E2 E7 B4 7B D9 EA 56 C6 55 7B 62 ED B7 B2 CB 7F A3 E2 60 23 0C 2C AE 74 FE AE 39 50 1B 05 16 2A 91 A5 BD EE F5 09 E3 A5 6F 15 FB 09 2A 72 8D 06 9E 3F 28 56 DD 3C AA A4 89 D5 93 51 20 8D 88 A6 26 EE AF 68 5A D7 35 9F 77
d mod （q-1）=
94 E3 8B 93 8D 27 E1 83 0D D4 D2 68 CD 80 2E 6F C1 E9 98 82 53 C5 C3 95 CB BF 77 95 B6 F3 9D 03 68 F4 9F 9C A6 FE 18 FC E5 0D ED 07 EB C6 47 35 1A F6 B6 21 16 A0 8C 7E E8 8B F1 69 E3 DF E1 62 57 E1 F9 77 67 FA 1C 81 ED 66 35 88 79 9C 60 DB

1/p mod q=
77 55 9B F3 47 48 68 88 2A 20 EF 90 7F E7 1E 7B 99 65 87 1B 66 B4 70 EF 28 0F 1F E0 EF 01 0C E7 39 F6 C0 5B 66 D3 2A 5E 1E 30 FD F1 9E DA 68 B5 4B 86 62 DD 20 18 70 5D 15 B6 DA 2B 42 D6 43 6D F7 39 95 B1 78 30 8C AF 5F 3C 8A 52 2F 16 FC 85
1/q mod p=
6F 6D 22 AD 15 66 B9 57 2D 08 B5 78 95 44 A6 73 3A C1 A6 03 74 50 C8 58 4D BA 3E 8A 64 AD F2 FE 56 2B BE 84 90 31 03 AD A5 F6 CD F8 A4 73 00 34 C7 A4 04 CD B1 B6 F1 B1 E8 3B 95 14 B9 59 7A 21 A7 FB 9A 9B 2E 83 89 52 16 92 DB 23 DE BB A8 89

B.3.3.12 IC卡公私钥对-1408位

E=
03
N=
B231678044B98D5CF9DF30B9541E94C2BECD7352FC9D96F86D197518333E2D1D1AA584E12A1DEC60F11B3CD2AEB3630184FFFD3998E5C149862C5063149404E5C4FDB9FF30416B846BEF1F656BB40CF9092888AB904A2C7659A3F14CFC3F930532D869D014E669C533B763A88114156DC2061A5316780B173BD04BE8471E975EE318CA9D327BF28AEE954ECDC5B4C0FAD9EFCB659FE3C01E431F3440B3E0167DD5DCDE431E1378745DAE9D4C50432D7D
D=
76CB9A5583265E3DFBEA207B8D69B881D488F78CA8690F5048BBA365777EC8BE11C3ADEB71694840A0BCD3371F2242010355537BBB43D631041D8AECB862ADEE8353D154CAD647AD9D4A14EE47CD5DFB5B705B1D0ADC1DA31ECF91F87CAD95B0D5272581329781A0EECD9C1981354F71ACF7E1D8A4B338CEF08EB808835E9C5F71E32E1932024DB204A87A2E134650170848934899F163045B3FCC588E2C561F3260FF6033B33AEFA641B0AA9A52A693
P=
DD289AD283534834B4BEC487401CE9E755ACBA1C4B6816C36BC38E3E59C5BED25167C20CF8F877D3EDBD1208F48A9309E1E438813AC31CDF170B81508E38360788F69AF6E673668ACD3C9F279A539FFF88EDB9E3E298B48B
Q=
CE43FB85BDE7EA473E5EED0708E63D6C77D63F65F3DC077FD2CEB94FC5A5770E819275CE891834FBCA86F36E72EDEAF605B45F076E082BF936776D282AC175903148E6C4F82A2EC43D0EC00B3633000D5B5E5A68862E7F17
d mod （p-1）=
9370673702378578787F2DAF8013469A391DD1683245648247D7B429912E7F36E0EFD6B350A5A537F3D3615B4DB1B75BEBED7B00D1D76894BA07AB8B097ACEAFB0A4674F444CEF07337DBF6FBC37BFFFB09E7BED41BB2307

d mod （q-1）=
8982A7AE7E9A9C2F7EE9F35A05EED39DA5397F994D3D5A5537347B8A83C3A4B45661A3DF061023528704A249A1F3F1F95922EA04F40572A6244F9E1AC72BA3B5763099D8A5717482D35F2AB224220008E7943C45AEC9AA0F
1/q mod p=
CAACCAB9F685356F8E0F3A72733BE0ED370D0F4B276F19EB009D7317A010E69AA26988ECE98306FEBDE63A29F92B9F151AE46C979D096807484A5FFA126D7C0B1E0FC0FBC2783BCAC9140C0A138036DD205262A05995FACA

B.3.3.13 IC卡公私钥对-1976位

此种长度的密钥，卡片可选支持，如不支持请按照不支持 DDA，支持 SDA 处理，AIP 设为’50 00’，SDA 需要的数据与卡片特征 33 中相同

E=

03

N=

C069B5366269430B73FD1876A2CA3B87B63DED06BC35495834893070E6281237E061AB46902A6D8C
CC6605A6C42D2A325486DD3A5AB20C061A6512B7E91BB123ECC7E05FECD181F4D819FC2D49CD5
7D266DA3A511F625DA39BCEF0FC18583281708FF01D11146DAF6DA23355EA981F85F6576FE18E3F
02BE68BD759EC4777421991AB5D512985FA3D05A77B45B76C59531977FC67394DB78B25E9F8D5927
20B726CB4FE3E8B5E8F74558ADE0C32AF8E382AF9A2FEB3D45250CF3D36B0E76C37029B216D06F
5E3B64C1DCAF2860956C2D44F0A4A02541D71685611F99899F33EE187CBE9A003733D8D9EB43EED
F1CE0837A8F12A0E0DB19

D=

804678CEEC462CB24D5365A46C86D25A797E9E047D78DB902306204B441AB6CFEAEBC784601C490
8884403C482C8C6CC3859E8D191CC08041198B72546127617F32FEAEA9DE1014DE566A81E31338FE
199E6D18B6A4193C267DF4B52BAE57700F5B54ABE0B62F3CA4916CCE3F1BABFAEA43A4A965ED
4AC7EF07E4E575986054B2005068D08424536C6657C94859842804CD533A22260404401A5B26BF7078
8AE48AB79FB980E759C23854E84B0BFF731A2D17D4A4AB5E0EF9ED2F8970D2F627C1DED92345D9
33935655612F76064D94356F6B979AD4BE23FFF992C90A58921836390B50465ABD5F4D87CC415859A
17989A580465FF5EC3

P=

0DEF93298FEE3B0CE64863BA0621203309DEA4C84214CD9A1A26C0C277A974A67FA866735A40A5
E1F95BFD17972CF11B088D20A339B79C721FB02F239C2E5C8A2E104EBEE9E138180DF6B9AF508A5
95694B68262319E997BF6D7915A71D34B32661C255A44D5322F56E45B5C3ECC12DBB43022A8BD2A
B04E56F7E5DB

Q=

0DCE9B42A0FAD81F1B3DD13DCB85A209CBB46D9992A98A18391943B89B06716D6BBE3560577924
36F128A320F5E31F9D112CEA62DF56D8EC20CAFD5021705AD45A6A60F0CC1B95A373EC47B6441F
823C20997BC416A3E51272C9BEA944B2B02A5A752C27642DF17FBC835A16AAC91D421A669314616
85ABDB0E9E71B

d mod （q-1）=

094A621BB5497CB34430427C041615775BE9C3302C0DDE66BC19D5D6FA70F86EFFC599A23C2B194
150E7FE0FBA1DF61205B36B177BCFBDA16A7574C2681EE85C1EB589D49BEB7ABAB3F9D11F8B06
E639B879AC417669BBA7F9E50B91A1378776EEBD6E3C2DE376CA39ED923D7F32B73D22CAC1C5D
371CADEE4A543E7

d mod （q-1）=

09346781C0A73ABF677E8B7E87AE6C0687CD9E6661C65C102610D7D06759A0F39D2978EAE4FB6D7
9F61B176B4E976A68B61DF1973F8F3B4815DCA8E0164AE7383C46EB4B32BD0E6CF7F2DA7982BFA
C2815BBA7D80F17EE0C4C867F1B8321CAC6E6F8C81A42C94BAA7DACE6B9C730BE2C1199B762E
B9AE729209BEF67

1/q mod p=

04D6F6AF71A11ACD2E14C2BA7620A614295638A3DA278E38875249F222E16ED2CABD32F40FDB7B
CC88B6C53CBA362021BF877CB4AAB81E45BF800FB109ED01F13A1337F70F626E01F995390BF11D5
7924EF55FDBF40B3DCBAABB9ECBC843F90F890C45922C9F8876C93ACF37F5EAEA6BFF1FE14CF4
D07D0BCCEC6BA1

B.3.3.14 IC卡公私钥对-1984位

E=

03

N=

97CF8BAD30CAE0F9A89285454DDDE967AAFBCD4BC0B78F29ECB1005286F15F6D7532A9C476607C73FF7424316DFC741894AA52EDBAF909719C7B53448343B45CF2F00A8ABFB78CEEBE848933AAED97DBE84F0730F34FB1AA1528D3D6EC75B73252A30D0C717518BE36458ADD0FBF854C65497F3F54084154B60F51561361EE8E85F742A54005524CB00FEBC334276E0E63DAD86C079A9A3DF5DD32BECADE1AB2B71F5F0A0E95A4000D01F1044A578AAD92E9FDE92E3C6AA3DCD4913DFA5552537E7DE75E241FAED455D76CB8FCAFEED3FD6DAB24D7A9C32852F866C751D7710F494A0DF11B67FAECDD87A9A4E2CC44F6F27E46E3C0CCCD0F

D=

194D41F232CC7AD446C3163637A4FC3BF1D4A2374AC94286FCC82AB86BD2E53CE8DDC6F613BABF68AA935B5D9254BE0418C70DD249D42C3D9A148DE0C08B48BA287D57171FF3ECD2751616DDF1D243F9FC0D2BDD7DE29D9C58DC234E7CBE49330DC5D78212E8D975090B9724D7F540E210E1953538AC0AE373AD3838C182F8DACD16829DD30E9698B309007E068BC76C44A7CE2113D6C7CEC6AC1B6FD27E53BF0082EB33AEBE02DC15B7942018420E0584224EBC6C49BDC0A9EF42210E363751AAC6F01165A57ED7DA3F9DFC1BEABBE6CBEE4F7253C7D3137996368D10E99D1FC187F6270856194E53E38E0CAD1439B9EA2CBEA4EE9077B3

P=

C27D0FDC2204F4BF077CE1AD370EE401D1848B2D164FC46B3F3AB9B23506FDABFF38EFC558C39EBD893B9024A0194DCA34214ECA18B26B8D4336B9A8B55C0F21C9DDF5DA0C120F64F0E46A505C74D261F2FD5B666F9E8DC44AF10BDC0269AE8B9482949B7E906B901247F7EA55D23A1F4425CD33E4A8891DC027D649

Q=

C7D30991956B3E334630E90B46CB04CD3B5C3657B19C3F3A515731B318CD9073DCAF34735B4A3D166CE602B2EA9B2A7984A9E7C26169B9F1614B3E772BDCF555DB32108F71C23790D15A4B74DBE4E66E62322C04C63940B29609C4D7770970ED57DB2DB54189DD76D71B6B2C90601B39902D1D6790C945E869422897

d mod （p-1）=

81A8B53D6C034DD4AFA896737A09ED568BADB21E0EDFD8477F7C7BCC2359FE72AA25F52E3B2D147E5B7D0AC3156633DC22C0DF3165CC47B382247BC5CE3D5F6BDBE94E915D615F98A09846E03DA336EBF75392444A69B3D831F607E8019BC9B26301B867A9B59D0AB6DAA546E3E17C14D8193377EDC5B0BE801A8EDB

d mod （q-1）=

85375BB6639CD4222ECB460784875888D23D798FCBBD7F7C363A212210890AF7E874CDA23CDC28B99DEEAC7747121C51031BEFD6EB9BD14B963229A4C7E8A38E9221605FA12C250B363C324DE7EDEEF44176C8032ED0D5CC6406833A4F5BA09E3A921E78D65BE8F9E4BCF21DB595677BB57368EFB5DB83F0462C1B0F

1/q mod p=

474B5A7EFC099D5B9E6D80AFDD7C04814A6A804414338B966AF7D0C4B92049552085A96B74CC61D06E77618540C240A7E5593AFBD00148F6939D1CA5451511D31CB09128247E3D3ECA9E49871CFB6C6614B070C7ADEE4AFFD2E62A3746D71132B6B6FE1CCC32BFAF836D87A01743E6BCB4E2C9F1FE67696EB226BB0E

B.3.3.15 IC卡公私钥对及证书-SM2-推荐曲线-索引57

【IC 卡私钥】：
4EFF3E9B796688F38E006DEB21E101C01028903A06023AC5AAB8635F8E307A53
【IC 卡公钥】：
C3AC12B81B9D175936B5BF72BB8FE3A2266BC013B2E94F5837F16AA1C01AA7323B75626AB64D02AED20CC6F440841F10EE6873BCBEA3F41D6869D0FEADD71154

B.3.3.16 IC卡公私钥对及证书-SM2-推荐曲线-索引58

【IC 卡私钥】：
E23073A44CA215D6C26CA68847B388E39520E0026E62294B557D6470440CA0AE
【IC 卡公钥】：
3AFD58A8749CBDB6F59956BE0286CAFF3123976DC4C67DD5AAA2ADCA6909B8C3EC83B847D33AA8BDD9CAFE9BBAC519524AA7DF47EA7EDD12297CF1A9BB3DA07E

B.3.3.17 IC卡公钥证书和IC卡公钥余项

送检厂商无需计算“IC 卡公钥证书（tag9F46）”和“IC 卡公钥余项（tag9F48）”，也不必在意它们的值是否正确，只需写入与 IC 卡公钥的模的长度相等的 IC 卡公钥证书和任意值的 IC 卡公钥余项即可。

B.3.3.18 签名的静态应用数据

送检厂商无需计算“签名的静态应用数据（tag93）”，不必在意其值是否正确，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（tag93）”即可。

B.3.4 电子现金卡片特征与密钥信息的对应关系

卡片特征中是否个人化动态数据认证相关数据请根据 3.5 条中卡片 AIP 的具体设置进行处理。

表 B.13 秘钥对应表

卡片特征	采用算法	发卡机构公私钥对	IC 卡公私钥对	对称密钥
1	仅国际	RSA 1152 位，见 B.3.3.3	RSA 768 位，见 B.3.3.9	3DES，见 B.3.3.1.2
2		RSA 1152 位，见 B.3.3.3	RSA 768 位，见 B.3.3.9	3DES，见 B.3.3.1.2
3		RSA 1152 位，见 B.3.3.3	RSA 1152 位，见 B.3.3.10	3DES，见 B.3.3.1.2
4		RSA 1408 位，见 B.3.3.5	RSA 1408 位，见 B.3.3.12	3DES，见 B.3.3.1.2
5		RSA 1984 位，见 B.3.3.6	RSA 768 位，见 B.3.3.9	3DES，见 B.3.3.1.2
6		RSA 1152 位，见 B.3.3.3	RSA 768 位，见 B.3.3.9	3DES，见 B.3.3.1.2
7		RSA 1152 位，见 B.3.3.3	RSA 1152 位，见 B.3.3.10	3DES，见 B.3.3.1.2
8		RSA 1408 位，见 B.3.3.5	RSA 1408 位，见 B.3.3.12	3DES，见 B.3.3.1.2
9 至 26		RSA 1152 位，见 B.3.3.3	RSA 768 位，见 B.3.3.9	3DES，见 B.3.3.1.2
1 至 26	仅国密	SM2-推荐曲线-索引 57，见 B.3.3.7	SM2-推荐曲线-索引 57，见 B.3.3.15	SM4，见 B.3.3.2
1	双算法	RSA 1152 位，见 B.3.3.3 SM2-推荐曲线-索引 57，见 B.3.3.7	RSA 768 位，见 B.3.3.9 SM2-推荐曲线-索引 57，见 B.3.3.15	3DES，见 B.3.3.1.2 SM4，见 B.3.3.2
2		RSA 1152 位，见 B.3.3.3 SM2-推荐曲线-索引 57，见 B.3.3.7	RSA 768 位，见 B.3.3.9 SM2-推荐曲线-索引 57，见 B.3.3.15	3DES，见 B.3.3.1.2 SM4，见 B.3.3.2
3		RSA 1152 位，见 B.3.3.3	RSA 1152 位，见 B.3.3.10	3DES，见 B.3.3.1.2

卡片特征	采用算法	发卡机构公私钥对	IC卡公私钥对	对称密钥
		SM2-推荐曲线-索引57，见B.3.3.7	SM2-推荐曲线-索引57，见B.3.3.15	SM4，见B.3.3.2
4		RSA 1408位，见B.3.3.5 SM2-推荐曲线-索引57，见B.3.3.7	RSA 1408位，见B.3.3.12 SM2-推荐曲线-索引57，见B.3.3.15	3DES，见B.3.3.1.2 SM4，见B.3.3.2
5		RSA 1984位，见B.3.3.6 SM2-推荐曲线-索引57，见B.3.3.7	RSA 768位，见B.3.3.9 SM2-推荐曲线-索引57，见B.3.3.15	3DES，见B.3.3.1.2 SM4，见B.3.3.2
6		RSA 1152位，见B.3.3.3 SM2-推荐曲线-索引57，见B.3.3.7	RSA 768位，见B.3.3.9 SM2-推荐曲线-索引57，见B.3.3.15	3DES，见B.3.3.1.2 SM4，见B.3.3.2
7		RSA 1152位，见B.3.3.3 SM2-推荐曲线-索引57，见B.3.3.7	RSA 1152位，见B.3.3.10 SM2-推荐曲线-索引57，见B.3.3.15	3DES，见B.3.3.1.2 SM4，见B.3.3.2
8		RSA 1408位，见B.3.3.5 SM2-推荐曲线-索引57，见B.3.3.7	RSA 1408位，见B.3.3.12 SM2-推荐曲线-索引57，见B.3.3.15	3DES，见B.3.3.1.2 SM4，见B.3.3.2
9 至 26		RSA 1152位，见B.3.3.3 SM2-推荐曲线-索引57，见B.3.3.7	RSA 768位，见B.3.3.9 SM2-推荐曲线-索引57，见B.3.3.15	3DES，见B.3.3.1.2 SM4，见B.3.3.2
27		RSA 1152位，见B.3.3.3 SM2-推荐曲线-索引57，见B.3.3.7	RSA 768位，见B.3.3.9 SM2-推荐曲线-索引57，见B.3.3.15	SM4，见B.3.3.2
28		RSA 1152位，见B.3.3.3 SM2-推荐曲线-索引57，见B.3.3.7	RSA 768位，见B.3.3.11 SM2-推荐曲线-索引57，见B.3.3.15	3DES，见B.3.3.1.2
卡片特征	采用算法	发卡机构公私钥对	IC卡公私钥对	对称密钥
31	仅国际	1152位，见B.3.3.3	768位，见B.3.3.9	3DES，见B.3.3.1.2
32				
33				
34				
35				
36				
37		1152位，见B.3.3.3	1152位，见B.3.3.10	
38				
39		1408位，见B.3.3.5	1280位，见B.3.3.11	
40				
41		1984位，见B.3.3.6	768位，见B.3.3.9	
42		1152位，见B.3.3.3	768位，见B.3.3.9	
43				
44				
45				
46				

卡片特征	采用算法	发卡机构公私钥对	IC 卡公私钥对	对称密钥
47				
48		1408 位，见 B.3.3.5	1408 位，见 B.3.3.6	3DES，见 B.3.3.1.2
49		1984 位，见 B.3.3.6	1984 位，见 B.3.3.14	3DES，见 B.3.3.1.2
31 至 49	仅国密	SM2-推荐曲线-索引 57，见 B.3.3.7	SM2-推荐曲线-索引 57，见 B.3.3.15	SM4，见 B.3.3.2
31 至 43	双算法	同时具备上述“仅国际”的密钥和“仅国密”的密钥。		
44		同时具备上述“仅国际”的密钥和“仅国密”的密钥。		SM4，见 B.3.3.2
45				3DES，见 B.3.3.1.2
46 至 49		同时具备上述“仅国际”的密钥和“仅国密”的密钥。		

B.3.5 电子现金卡片特征

B.3.5.1 卡片特征1至卡片特征19

此类特征基于本部分第 3.2.1 条规定的联机交易应用基本特征。

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

表 B.14 卡片特征 1 至卡片特征 19 表

应用首选名称 [9F 12]	AIP [82]	ADA [9F 52]	发卡机构认证指示位 [9F 56]	LCOL [9F 58]	UCOL [9F 59]
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 31 卡片特征 1	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	00	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 32 卡片特征 2	58 00 -支持 SDA -支持持卡人认证 -执行终端风险管理	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	N/A	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 33 卡片特征 3	7C 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	00 -可选	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 34 卡片特征 4	7C 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	1E 40 -如果交易拒绝脱机执行，生成通知 -如果在本次交易中 PIN 尝试次数超出而且交易拒绝，生成通知 -如果因为发卡机构认证失败或没有执行导致交易拒绝，生成通知 -如果是新卡，联机交易	80 -强制	03	07

		-如果在前次交易中 PIN 尝试次数超限，拒绝交易			
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 36 卡片特征 6	7C 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	00	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 37 卡片特征 7	7D 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证 -支持复合 CDA-GENERATE AC	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	09	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 38 卡片特征 8	7D 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证 -支持复合 CDA-GENERATE AC	80 40 -如果发卡机构认证失败，下次联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	00 -可选	03	09
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 39 卡片特征 9	79 00 -支持 SDA -支持 DDA -支持持卡人认证 -执行终端风险管理 -支持复合 CDA-GENERATE AC	80 40 -如果发卡机构认证失败，下次联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	N/A	09	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 30 卡片特征 10	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	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 -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31	5C 00 -支持 SDA -支持持卡人认证	C2 40 -如果发卡机构认证失败，下次联机交易 -如果发卡机构认证执行但失败，拒绝交易	80 -强制	09	07

32 卡片特征 12	-执行终端风险管理 -支持发卡机构认证	-如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易			
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 33 卡片特征 13	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	C6 40 -如果发卡机构认证失败，下次联机交易 -如果发卡机构认证执行但失败，拒绝交易 -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 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 34 卡片特征 14	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	92 40 -如果发卡机构认证失败，下次联机交易 -如果交易拒绝脱机执行，生成通知 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 35 卡片特征 15	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	03	00
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 36 卡片特征 16	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	83 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果是新卡，当交易无法联机时拒绝交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 37 卡片特征 17	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	82 30 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易 -如果在前次交易中 PIN 尝试次数超限，当交易无法联机时拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41 47 45 20 30 30 31 38 卡片特征 18	5C 00 -支持 SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	93 40 -如果发卡机构认证失败，下次联机交易 -如果交易拒绝脱机执行，生成通知 -如果是新卡，联机交易 -如果是新卡，当交易无法联机时拒绝交易 -如果在前次交易中 PIN 尝试次数超限，拒绝交易	80 -强制	03	07
43 41 52 44 20 49 4D 41	5C 00 -支持 SDA	82 C0 -如果发卡机构认证失败，下次联机交易	80 -强制	03	07

47 45 20 30 30 31 39 卡片特征 19	-支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	-如果是新卡，联机交易 -如果在本次交易中 PIN 尝试次数超限，应用锁定 -如果在前次交易中 PIN 尝试次数超限，拒绝交易			

B.3.5.2 卡片特征20

此特征基于本部分第 3.2.1 条规定的联机应用基本特征。

此特征用于测试执行频度检查和发卡机构脚本处理失败。

使用最大值个人化此类数据元素，以保证不引起包括此类元素的频度检查超限条件。

表 B.15 卡片特征 20 表

数据元素	值
LCOL[9F 58]	0F
UCOL[9F 59]	0F
连续交易限制数（国际）[9F 53]	0F
累计交易金额限制数[9F 54]	000099999999
累计交易金额限制数（双货币）[9F 75]	000000030000

应用首选名称 [9F 12]	AIP [82]	发卡机构认证指示位 [9F 56]	ADA [9F 52]	连续交易限制数 [9F 72]	累计交易金额上限 [9F 5C]	第二应用货币代码 [9F 76]	货币转换因子 [9F 73]
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 30 卡片特征 20	5C 00 -支持SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	80 -强制	C2 48 -如果发卡机构认证失败，下次联机交易 -如果发卡机构认证执行但失败，拒绝交易 -如果是新卡，联机交易 -如果在前次交易中PIN尝试次数超限，拒绝交易 -如果发卡机构脚本命令在前次交易中失败，联机交易	05	000000005000	0826	20000175

B.3.5.3 卡片特征24

此特征用于测试加强 ATC 处理（Enhanced ATC Processing）。

此特征除了以下标明的数据其余均按卡片特征 1 个人化。

表 B.16 卡片特征 24 表

应用首选名称	应用交易计数器

[9F 12]	[9F 36]
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 34 卡片特征 24	FF FD

B.3.5.4 卡片特征5，25，26

此类特征基于本部分第 3.2.1 条规定的联机应用基本特征。

此类特征用于测试附加频度和更新功能。

此类特征对于支持累计连续国际交易（货币）、交易金额（双货币）、更新记录和写数据的频度检查的卡片是必需的。

使用最大值个人化此类数据元素，以保证不引起包括这些元素的频度检查超限条件。

表 B.17 卡片特征 5，25，26 表

数据元素	值
LCOL[9F 58]	0F
UCOL[9F 59]	0F
连续交易限制数（国际）[9F 53]	0F
累计交易金额限制数[9F 54]	000099999999

应用首选名称 [9F 12]	AIP [82]	AIA [9F 56]	ADA [9F 52]	连续交易限制数 [9F 72]	累计交易金额限制数(双货币)[9F 75]	第二应用货币代码 [9F 76]	货币转换因子 [9F 73]
43 41 52 44 20 49 4D 41 47 45 20 30 30 30 35 卡片特征 5	7C 00 -支持SDA -支持DDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	80 -强制	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中PIN尝试次数超限，拒绝交易	0F	000000015000	0826	20000175
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 35 卡片特征 25	5C 00 -支持SDA -支持持卡人认证 -执行终端风险管理 -支持发卡机构认证	80 -强制	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易 -如果在前次交易中PIN尝试次数超限，拒绝交易	03	000000015000	0826	20000175
43 41 52 44 20 49 4D 41 47 45 20 30 30 32 36 卡片特征 26	5C 00 -支持SDA -支持持卡人认证 -执行终端风险	00 -可选	82 40 -如果发卡机构认证失败，下次联机交易 -如果是新卡，联机交易	03	000000015000	0826	20000175

	管理 -支持发卡机构认证		-如果在前次交易中PIN尝试次数超限，拒绝交易				

B.3.5.5 卡片特征27

本特征基于本部分第 3.2.1 条规定的联机应用基本特征。

此特征除了以下标明的数据其余均按卡片特征 1 个人化。

表 B.18 卡片特征 27 表

应用首选名称 [9F 12]	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

B.3.5.6 卡片特征28

本特征仅适用于双算法模板。

本特征按卡片特征 27 个人化，仅对称密钥算法不同。

B.3.5.7 卡片特征31

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

表 B.19 卡片特征 31 表

	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 -支持SDA -支持DDA -支持持卡人认证	92 70 10 00 – 支持小额检查 – 支持新卡检查 – 卡优先选择接触式联机 – 不允许不匹配货币的交易 – 如果是新卡且读卡器仅支持脱机则拒绝交易 – 支持签名 – 脱机交易脱机批准的交易，卡片记录交易日志	30 00	1

B.3.5.8 卡片特征32

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

表 B.20 卡片特征 32 表

	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 -支持SDA -支持DDA -支持持卡人认证	44 00 50 00 – 支持小额和 CTTA 检查 – 允许货币不匹配的脱机交易 – 不匹配货币的交易支持联机 PIN – 支持签名	30 00	102.00

B.3.5.9 卡片特征33

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

表 B.21 卡片特征 33 表

	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 -支持 SDA -支持 DDA -支持持卡人认证	41 20 80 00 – 支持小额和 CTTA 检查 –返回脱机消费可用余额 –如果是新卡且读卡器仅支持脱机则拒绝交易 –匹配货币的交易支持联机 PIN	01	00 00 00 00 11 00	110

B. 3. 5. 10 卡片特征34

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

表 B.22 卡片特征 34 表

	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 -支持SDA -支持DDA -支持持卡人认证	21 00 F0 00 – 支持小额或CTTA检查 –返回脱机消费可用余额 –匹配货币的交易支持联机 PIN –不匹配货币的交易支持联机PIN –对于不匹配货币交易，卡要求CVM – 支持签名	01	50.00	102.00

B. 3. 5. 11 卡片特征35

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

表 B.23 卡片特征 35 表

	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 -支持SDA -支持DDA -支持持卡人认证	41 10 20 00 – 支持小额和 CTTA 检查 – 返回脱机消费可用余额 – 对于不匹配货币交易，卡要求 CVM – 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

B.3.5.12 卡片特征36

此特征基于本部分第3.2.2条规定的脱机交易基本特征。

表B.24 卡片特征36表

	AIP [82]	卡片附加处理	CTTAL	CTTAUL
卡片特征36	70 00 — 脱机交易 AIP -支持SDA -支持DDA -支持持卡人认证	01 00 10 00 – 返回脱机消费可用余额 – 支持签名	不存在	不存在

B.3.5.13 卡片特征37

此特征基于本部分第3.2.2条规定的脱机交易基本特征。

表B.25 卡片特征37表

	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 -支持SDA -支持DDA -支持持卡人认证	83 10 40 00 —支持小额检查 – 卡优先选择接触式联机 – 返回脱机消费可用余额 – 不匹配货币的交易支持联机PIN – 脱机交易脱机批准的交易，卡片记录交易日志	支持国密：9F 66 04 9F 02 06 9F 37 04 5F 2A 02 DF 69 01 不支持国密：9F 66 04 9F 02 06 9F 37 04 5F 2A 02	17	0	00 00 00 00 11 00

B.3.5.14 卡片特征38

此特征基于本部分第3.2.2条规定的脱机交易基本特征。

表B.26 卡片特征38表

	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 -支持SDA -支持DDA -支持持卡人认证	81 00 30 00 – 支持小额检查 卡片不选择接触式联机 – 返回脱机消费可用余额 – 对于不匹配货币交易，卡要求CVM – 支持签名	支持国密：9F 66 04 9F 02 06 9F 37 04 5F 2A 02 DF 69 01 不支持国密：9F 66 04 9F 02 06 9F 37 04 5F 2A 02	17	0

B.3.5.15 卡片特征39

此特征基于本部分第3.2.2条规定的脱机交易基本特征。

表B.27 卡片特征39表

	AIP [82]	卡片附加处理	应用交易计数器 [9F 36]	9F17	CTTAL
卡片特征39	70 00 — 脱机交易 AIP -支持SDA -支持DDA -支持持卡人认证	2C 00 F0 00 – 支持小额或CTTA检查 – 支持PIN重试次数超过检查 – 允许货币不匹配的脱机交易 – 匹配货币的交易支持联机PIN – 对于不匹配货币交易，卡要求CVM – 支持签名	FF E0	0	50.00

B.3.5.16 卡片特征40

此特征基于本部分第3.2.2条规定的脱机交易基本特征。

表B.28 卡片特征40表

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

B.3.5.17 卡片特征41

此特征基于本部分第3.2.2条规定的脱机交易基本特征。

表B.29 卡片特征41表

	AIP [82]	卡片附加处理	9F17	CTTAL	CTTAUL

卡片特征 41	50 00 — 脱机交易 AIP -支持SDA -支持DDA -支持持卡人认证	45 90 F0 00 – 支持小额和 CTTA 检查 – 允许货币不匹配的脱机交易 –返回脱机消费可用余额 – 支持预付 – 匹配货币的交易支持联机 PIN – 对于不匹配货币的交易支持联机 PIN – 对于不匹配货币交易，卡要求 CVM – 支持签名 – 脱机交易脱机批准的交易，卡片记录交易日志	3	50.00	102.00

B. 3. 5. 18 卡片特征42

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

表 B.30 卡片特征 42 表

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

B. 3. 5. 19 卡片特征43

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

此特征的非接触界面下的 PDOL 9F38 应设置为 9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04（即不含有 SM 算法支持指示器）。

表 B.31 卡片特征 43 表

	AIP [82]	卡片附加处理	PDOL	CTTAL	CTTAUL

卡片特征 43	70 00 — 脱机交易 AIP -支持SDA -支持DDA -支持持卡人认证	8D 00 30 00 – 支持小额检查 – 支持 PIN 重试次数超过检查 – 允许货币不匹配的脱机交易 – 返回脱机消费可用余额 – 对于不匹配货币交易，卡要求 CVM – 支持签名	9F 66 04 9F 02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F 37 04	不存在	不存在

B.3.5.20 卡片特征44

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

表 B.32 卡片特征 44 表

	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 -支持SDA -支持DDA -支持持卡人认证	41 20 80 00 – 支持小额和CTTA检查 –返回脱机消费可用余额 –如果是新卡且读卡器仅支持脱机则拒绝交易 –匹配货币的交易支持联机PIN	01	110

B.3.5.21 卡片特征45

此特征基于本部分第 3.2.2 条规定的脱机交易基本特征。

表 B.33 卡片特征 45 表

	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 -支持SDA -支持DDA -支持持卡人认证	51 20 80 00 – 支持小额和 CTTA 检查 – 支持新卡检查 – 返回脱机消费可用余额 – 如果是新卡且读卡器仅支持脱机则拒绝交易 – 匹配货币的交易支持联机 PIN	01	00 00 00 00 11 00	110

B.3.5.22 卡片特征46

此特征基于本部分第 3.2.3 条规定的脱机交易扩展基本特征。

表 B.34 卡片特征 46 表

数据对象	Tag	Length	Value
AIP	82	02	70 00 — 脱机交易 AIP -支持 SDA -支持持卡人认证

			-支持 DDA
卡片附加处理	9F68	04	81 00 00 00 – 支持小额检查 –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

对于卡片特征 46，除 SFI=0x19 和 SFI=0x1E 的扩展应用专用文件外，再新增三个变长文件，总共四个变长文件和一个循环文件：

变长文件，其 SFI=0x15

该文件至少可开通 4 个行业应用，即至少可 Append 4 条记录。每个记录不超过 128 字节。

开通密钥：15A912A5F029C6001DF2539A00137049

变长文件，其 SFI=0x16

该文件可开通 2 个行业应用，即可 Append 2 条记录。每个记录不超过 128 字节。

开通密钥：167312850029B6001DC2539A0013E049

变长文件，其 SFI=0x17

该文件可开通 7 个行业应用，即至少可 Append 7 条记录。每个记录不超过 128 字节。

开通密钥：191A5F026001DF259A03019C37049F11

B. 3. 5. 23 卡片特征47

此特征基于卡片特征 46，除下表规定的数据外，其余数据均按照卡片特征 46 来设置。

表 B.35 卡片特征 47 表

数据对象	Tag	Length	Value
可用脱机消费金额	9F5D	06	00 00 00 00 00 01
电子现金分段扣费透支限额	DF62	06	00 00 00 10 00 00
电子现金分段扣费已透支额	DF63	06	00 00 00 00 00 00

B. 3. 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 3.4 条。

B. 3. 6 电子钱包卡片特征

表 B.36 数据文件内容规定表

文件标识（FID）		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
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 B.37 持卡人基本信息文件表

文件标识（FID）		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	本行职工标识	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 B.38 管理信息文件表

文件标识（FID）		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	卡类型	00
12-60	预留	初始化全 00

B.3.7 芯片证明材料

芯片证明材料

芯片提供商名称	
芯片名称	
芯片型号	
CPU 处理位数	
EEPROM 容量	

ROM 容量	
RAM 容量	
XRAM 容量	
FLASH 容量	
工作电压范围	
工作时钟频率	
加密协处理器（算法位数）	

芯片或 COS 提供商（盖章）

年　　月　　日

注：以上材料存储器所对应的项（EEPROM、ROM、RAM、XRAM、FLASH）根据实际情况选择填写，没有的请标明无。其余项为必填项，如无法填写则应附加加盖芯片或 COS 提供商公章的书面说明，此页需芯片或 COS 提供商如实填写，并加盖公章。

附 录 C
公共交通IC卡卡片电特性协议送检要求
（资料性附录）

送检厂商在送检时应提交填写完毕的下列声明（送检其他信息参考附录B的相关要求）：

公共交通IC卡电特性协议测试功能一致性声明

PART I – 样品提供者标识		
注册号：	7	
公司名称：		
联系人：		
公司地址：		
电话：		
传真：		
EMAIL:		
签名和日期：		
PART IIa–卡片信息		
描述	**名称**	**版本**
COS		
样品名称		
芯片型号		
E^2PROM 容量		
卡芯片厂商		
卡封装厂商		
PART IIb – 依据规范		
规范日期版本：		
PART III – 卡片执行		
功能	**参数值**	
卡片类型	**类型 A**	是
	类型 B	否
协议参数	**DDA 支持**	否
	CID 支持	是
	Loopback 指令	否
类型 A 参数	**UID 长度**	4
	UID 动态生成	否
	FWI	0
	SFGI	0
	FSCI	2
类型 B 参数	**PUPI 动态生成**	否
	扩展 ATQB 支持	否

	FWI	否
	FSCI	否

附 录 D
终端电气特性和协议送检要求
（资料性附录）

D.1 文档要求

厂商在送检时须提交以下文档：

——Level1 测试终端功能陈述文档；

——终端的安装和使用手册；

——其它与使用相关的技术资料。

PART I – 样品提供者标识			
注册号：			
公司名称：			
联系人：			
公司地址：			
电话：			
传真：			
EMAIL:			
签名和日期：			
PART IIa – PCD 标识			
描述	**名称**	**版本**	**Check sum**
PCD 名称			
PCD 硬件名称			
PCD 软件名称			
PART IIb – PCD 所在终端标识			
PCD 所在终端名称			
PART IIc – 样品编号			
样品 1 编号			
样品 2 编号			
样品 3 编号			
PART IId – 依据规范			
规范日期版本：			
PART III – PICC 接口			
供电方式			
- **电池供电（电池作为唯一的供电方式）**			
所用电池的类型			
电池的正常电压			

- **直流电源（直流电源作为供电方式）**	
正常的直流电压	
直流供电的正常电流	
- **交流电源（交流电源作为供电方式）**	
正常的交流电压	
正常频率	
- **电池和直流（或交流）复合供电**	

	PCD 类型	**支持**	**数**	—— 备注
PART IV – 执行的协议类型				
1.	PCD 是否支持，除了 A 类型和 B 类型以外的其他类型的卡片？ 如果是，请列举所有支持的其他卡片类型，并表述他们是如何共同工作的。			
2.	正常交易结束后，卡片移出工作场，PCD 是否在 t_{PAUSE} 时间复位工作关场，并重新开始轮询和防冲突检测？ 如果是，请指明 t_{PAUSE} 的数值。 如果否，请详细描述 PCD 的工作流程。			
3.	基于无错恢复，请描述 PCD 在块交互过程中，如果出现场复位的后续工作流程。			
PART V– A 类型协议				
1.	当 PCD 检测到副载波中开始的半位持续时间和比特周期的调制方式与卡片负载调制的副载波不一致后，是否认为是传输错误？ 如果否，请描述 PCD 工作流程。			
2.	PCD 是否接受 A 类型卡片超出规范要求的 FDT？ 如果是，请描述那些指令或块支持。			
3.	PCD 是否支持不遵循 JR/T 0025 规定的 A 类型卡片（例如：SAK 字节的 b_6 = （0）$_b$）？			
4.	PCD 是否支持 A 卡返回的 ATS 超过 20 字节（例如：ATS 中 TL 字节的某值大于‘14’）？			
5.	PCD 是否支持 A 卡返回的 ATS 超过 15 个历史字			
6.	如果 A 类型卡片指明了两个方向上的位传输速率不等于 106kbps，PCD 是否支持。（例如：ATS 中 TA（1）不等于‘00’，‘08’，‘80’，‘88’）？ 如果是，请指明各方向支持的速率，并描述 PCD 工作流程.			
7.	PCD 是否支持 A 卡 SFGT>$SFGT_{MAX}$。（例如：			
PART VI– B 类型协议				
1.	EOS 之后，B 类型卡片副载波持续时间大于 t_{FSOFF} 时，PCD 是否认为是传输错误？ 如果否，请描述 PCD 工作流程。			

2.	PCD是否支持同步时间TR1<$TR1_{MIN}$的B类型卡片？			
3.	如果PCD支持同步时间TR1<$TR1_{MIN}$的B类型卡片，那么同样的最小值是否也可用于从一个命令到另一个命令之间或者从一个交易到另一个交易之			
4.	如果PCD支持的最小TR1数值是不变的，那么以us为单位的值是多少？ 如果PCD支持的最小TR1数值是变化的，那么以us为单位变化的限值是多少？			
5.	PCD是否支持同步时间TR1>$TR1_{MIN}$的B类型卡片？ 如果是，请指明PCD可接受的最大TR1的数值。			
6.	如果 B 类型卡片指明了两个方向上的位传输速率不等于 106kbps，PCD 是否支持。（例如：ATQB 位速率控制字节不等于‘00’，‘08’，‘80’，‘88’）？ 如果是，请指明各方向支持的速率，并描述 PCD 工作流程。			
7.	如果 B 类型卡片指明支持高于 106kbps 的位速率，PCD 是否建立高于 106kbps 的位速率？ 如果是，请描述 PCD 工作流程。			
8.	PCD 是否支持不遵循 JR/T 0025 规定的 B 类型卡片（例如：ATQB 中的协议字节不等于$(0001)_b$）？			
PART VII– A 和 B 类型协议				
1.	PCD是否支持S块功率水平不同于$(00)_b$的其他值（例如：S块的INF域的b_8b_7位不等于$(00)_b$）？			
2.	当收到不是对 R（NAK）进行响应的 R（ACK）块，且块号不等于当前 PCD 的块号时，PCD 是否重发上一个 I 块？			
PART VIII– 刷卡平面形状				
1.	PCD表面是否有不均匀凸起？ 如果是，请用清楚地描述Z轴的位置。（如需要请另附图片）			
2.	PCD 表面是否为凹面？ 如果是，请用清楚地描述 0cm 的测试位置。（如需要请另附图片）			

D.2 硬件要求

厂商须提交三个送检终端样品于检测方用于测试。

附 录 E
终端内核应用送检要求
（资料性附录）

E.1 文档要求

厂商在送检时须提交下列文档：

——终端的安装和使用手册

——Level2 测试终端功能陈述文档

E.2 送检终端的要求：

——提供三个送检终端

——提供用于联机交易测试的模拟后台

——如果终端外接密码键盘，为了验证外置密码键盘到终端 pin 是密文传输的，需厂商提供对外接密码键盘与终端间数据监控的方法和工具。

——每个送检终端应满足如下要求：

1) 下列 AID 应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**

终端中的 AID 应该可由 BCTC 添加或删除, 并且对应于每个 AID 的 ASI 应可配置。

CA 公钥模.

CA 公钥模必须可以独立下装，并且下列的 CA 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' and '03' 对应 RID 'A0 00 00 00 65'

CA 公钥模的值请参见 E.3。

2) 终端风险管理

如果终端支持异常文件检查，那么终端中的异常文件应该可以由测试人员配置。请预先将下列账号写入异常文件：

卡号#: 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

基于对随机交易选择的支持情况，出于测试的目的，终端应能够为每个交易显示或打印终端随机数。

3) 终端行为码

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

4) 应用版本号

存储在终端中的应用版本号应设置为'008C'

5) 终端国家代码

出于测试目的，终端的国家代码请设为 '0840'

终端内部时钟

终端的内部时钟应可以由测试人员设值。

1) 终端应能够识别并且能够产生下列授权响应码：

- 不能联机执行（脱机批准）= Y3
- 不能联机执行（脱机拒绝）= Z3
- 脱机批准 = Y1
- 脱机拒绝 = Z1

2) 证书回收列表

如果支持证书回收，则对于每个RID（ A000000003',A000000004',A000009999', A000000632” ）需要至少包含30个CRL入口（其中29个为一些没有被签名的证书序列号）

For RID 'A000000632' the signed CRL entry is for:

- CA Index '50'
- Certificate Serial Number '014455'

For RID 'A000000004' the signed CRL entry is for:

- CA Index 'FE'
- Certificate Serial Number '092355'

For RID 'A000009999' the signed CRL entry is for:

- CA Index 'E1'
- Certificate Serial Number '014394'

——厂商提供的模拟后台应满足如下要求：

1) 显示

出于测试目的，模拟主机必须提供显示终端上送的报文的窗口，并且指出上送的报文类型。

2) 授权响应码

下发的授权响应码应可以被选择或设置，Approve-00, Decline-05, Referral-01

3) 发卡机构脚本

发卡机构脚本需要按照下一章的发卡机构脚本要求，事先编写好填加到模拟主机中，以便测试时测试工程师能够通过选择不同的发卡机构脚本来给终端下发案例所要求的发卡机构脚本。另外 BCTC 应可以对下发的发卡机构脚本控制，可以选择不下发发卡机构脚本，可以编辑，和修改下发的发卡机构脚本。

4) 发卡机构认证数据

测试人员应可以对下发的发卡机构认证数据进行修改和编辑。

5) 联机密文 PIN

为了验证输入的 PIN 与上送报文中的密文 PIN 块一致，需要厂商在模拟后台中增加联机密文 PIN 的加密和解密功能。确保能够对收入的 PIN 进行加密，以验证上送报文中的 PIN 正确；能够对联机 PIN 密文进行解密，以验证解密后获取的 PIN 与输入一致。

E.3 CA公钥

E.3.1 Test Certificate Authority Public Keys For RID 'A0 00 00 06 32'

Certificate Authority Public Key '80'

Length '80'

RID : A000000632

Public Modulus is

CCDBA686E2EFB84CE2EA01209EEB53BEF21AB6D353274FF8391D7035D76E2156CAEDD07510E07DAF
CACABB7CCB0950BA2F0A3CEC313C52EE6CD09EF00401A3D6CC5F68CA5FCD0AC6132141FAFD1CFA
36A2692D02DDC27EDA4CD5BEA6FF21913B513CE78BF33E6877AA5B605BC69A534F3777CBED6376BA
649C72516A7E16AF85

Public Exponent is '010001'

Certificate Authority Public Key '57' For SM
Alg Type: SM
Public Key is
X=E8105E77861FD2EB727C84E36D3D4A5666BD0ADCE8781F0145D3D82D72B92748
Y=E22D5404C6C41F3EC8B790DE2F61CF29FAECB168C79F5C8666762D53CC26A460

Certificate Authority Public Key '58' For SM
Alg Type: SM
Public Key is
X=FFC2B1513320C275411DBADD2188203F7B62519F8C7BA98EF8AA9FD6D2E47598
Y=4E383C3E12784B42B066960EEA0C8FC8099E14128055D67A666CCA5A058C26A4

Certificate Authority Public Key '61'
Length '80'
RID : A000000632
Public Modulus is
834D2A387C5A5F176EF3E66CAAF83F194B15AAD2470C78C77D6EB38EDAE3A2F9BA1623F6A58C892C
C925632DFF48CE954B21A53E1F1E4366BE403C279B90027CBC72605DB6C79049B8992CB4912EFA270BE
CAB3A7CEFE05BFA46E4C7BBCF7C7A173BD988D989B32CB79FAC8E35FBE1860E7EA9F238A92A35935
52D03D1E38601
Public Exponent is '03'

Certificate Authority Public Key '62'
Length '80'
RID : A000000632
Public Modulus is
B5CDD1E5368819FC3EA65B80C68117BBC29F9096EBD217269B583B0745E0C16433D54B8EF387B1E6CD
DAED4923C39E370E5CADFE041773023A6BC0A033B0031B0048F18AC159773CB6695EE99F551F414883F
B05E52640E893F4816082241D7BFA3640960003AD7517895C50E184AA956367B7BFFC6D8616A7B57E2D4
47AB3E1
Public Exponent is '010001'

Certificate Authority Public Key '63'
Length '90'
RID : A000000632
Public Modulus is
867ECA26A57472DEFB6CA94289312BA39C63052518DC480B6ED491ACC37C028846F4D7B79AFAEEFA0
7FB011DAA46C06021E932D501BF52F2834ADE3AC7689E94B248B28F3FE2803669DEDA000988DA1249F
9A891558A05A1E5A7BD2C282FE18D204189A9994D4ADD86C0CE50952ED8BCEC0CE633679188285E51E
1BED840FCBFC10953939AF49DB90048912E48B44181
Public Exponent is '03'

Certificate Authority Public Key '64'
Length 'A0'
RID : A000000632
Public Modulus is
91123ECF0230E3CB245C88DDFA3EE57BC58ED00B367B3875FCB79548872680F601E8C839AC0721BAB3
B89ED21607281C8919BF726266EAB848502AD874B5107A4E654EF6D37773343F461435C86E4A8F866FB1
8C7CBA497B426290C38D196E2AFF33C0906F9296F297E156DC602A5E653CA1168F1109261114BF7BE812
7A3E8007191830134299395CE2B322228667B76E072EB7FD5D0FB3A83E8AD1D7F6FD81
Public Exponent is '03'

Certificate Authority Public Key '65'
Length 'B0'
RID : A000000632
Public Modulus is
81BA1E6B9F671CFC848CA2ACD8E17AF406B4D329D1ECA5D01BC094A87C30AF49867944C632E818507
4655FA535AD8CA42A83B41AAAEA859F432FA0B818E72DC07ED3F77FB318A475A261C0760A156E5DD
C157AE8B79BA72D89D69FFF754619E928F1516A2A72C0F86B09B8EA25F86DC5A48EBC5A16F83FBA8F
C4E3A98278912249F4E079BCBC06E7BED9AED397879D279ED9192539490126094 9BCCE6FA1169798A27
15DAE32988BEFBE9621AE15E0C1
Public Exponent is '010001'

Certificate Authority Public Key '66'
Length '60'
RID : A000000632
Public Modulus is

7F5A3945794D6B15F5F26B4A21A63A5EF35540D8C8C099151F2279780A5C18A317703C98632E804D25576
A7B460C05061E03975E50FBD7495B3ADC8E425E53DF76FA40B035E87F69ABF8765A52523F3B1A39B195
28B002239015FADBA5921051
Public Exponent is '010001'

E.3.2 Test Certificate Authority Public Keys For RID 'A0 00 00 99 99'
Certificate Authority Public Key 'E1'
Length '70'
RID : A000009999
Public Modulus is
99C5B70AA61B4F4C51B6F90B0E3BFB7A3EE0E7DB41BC466888B3EC8E9977C762407EF1D79E0AFB282
3100A020C3E8020593DB50E90DBEAC18B78D13F96BB2F57EEDDC30F256592417CDF739CA6804A10A29
D2806E774BFA751F22CF3B65B38F37F91B4DAF8AEC9B803F7610E06AC9E6B
Public Exponent is '03'

Certificate Authority Public Key 'E2'
Length '70'

RID : A000009999
Public Modulus is
BD232E348B118EB3F6446EF4DA6C3BAC9B2AE510C5AD107D38343255D21C4BDF4952A42E92C633B1C
E4BFEC39AFB6DFE147ECBB91D681DAC15FB0E198E9A7E4636BDCA107BCDA3384FCB28B06AFEF90F
099E7084511F3CC010D4343503E1E5A67264B4367DAA9A3949499272E9B5022F
Public Exponent is '03'

Certificate Authority Public Key 'E3'
Length '70'
RID : A000009999
Public Modulus is
BC01E12223E1A41E88BFFA801093C5F8CEC5CD05DBBDBB787CE87249E8808327C2D218991F97A1131E
8A25B0122ED11E709C533E8886A1259ADDFDCBB396604D24E505A2D0B5DD0384FB0002A7A1EB39BC8
A11339C7A9433A948337761BE73BC497B8E58736DA4636538AD282D3CD3DB
Public Exponent is '010001'

Certificate Authority Public Key 'E4'
Length '80'
RID : A000009999
Public Modulus is
CBF2E40F0836C9A5E390A37BE3B809BDF5D740CB1DA38CFC05D5F8D6B7745B5E9A3FA6961E55FF204
12108525E66B970F902F7FF4305DD832CD0763E3AA8B8173F84777100B1047BD1D744509312A0932ED25F
ED52A959430768CCD902FD8C8AD9123E6ADDB3F34B92E7924D729CB6473533AE2B2B55BF0E44964FD
EA8440117
Public Exponent is '03'

Certificate Authority Public Key 'E5'
Length '80'
RID : A000009999
Public Modulus is
D4FDAE94DEDBECC6D20D38B01E91826DC6954338379917B2BB8A6B36B5D3B0C5EDA60B337448BAFF
EBCC3ABDBA869E8DADEC6C870110C42F5AAB90A18F4F867F72E3386FFC7E67E7FF94EBA079E531B3
CF329517E81C5DD9B3DC65DB5F9043190BE0BE897E5FE48ADF5D3BFA0585E076E554F26EC69814797F1
5669F4A255C13
Public Exponent is '03'

Certificate Authority Public Key 'E6'
Length '80'
RID : A000009999
Public Modulus is
EBF9FAECC3E5C315709694664775D3FBDA5A504D89344DD920C55696E891D9AB622598A9D6AB8FBF3
5E4599CAB7EB22F956992F8AB2E6535DECB6B576FA0675F97C23DD4C374A66E6AF419C9D204D0B9F93
C08D789D63805660FBB629DF1B488CFA1D7A13E9B729437EEAFE718EFA859348BA0D76812A99F31CD3

64F2A4FD42F
Public Exponent is '010001'

E.3.3 Test Certificate Authority Public Keys For RID 'A0 00 00 06 32'

Certificate Authority Public Key '50'
Length '80'
RID : A000000632
Public Modulus is
D11197590057B84196C2F4D11A8F3C05408F422A35D702F90106EA5B019BB28AE607AA9CDEBCD0D81A
38D48C7EBB0062D287369EC0C42124246AC30D80CD602AB7238D51084DED4698162C59D25EAC1E6625
5B4DB2352526EF0982C3B8AD3D1CCE85B01DB5788E75E09F44BE7361366DEF9D1E1317B05E5D0FF529
0F88A0DB47
Public Exponent is '010001'

Certificate Authority Public Key '51'
Length '90'
RID : A000000632
Public Modulus is
DB5FA29D1FDA8C1634B04DCCFF148ABEE63C772035C79851D3512107586E02A917F7C7E885E7C4A7D5
29710A145334CE67DC412CB1597B77AA2543B98D19CF2CB80C522BDBEA0F1B113FA2C86216C8C610A2
D58F29CF3355CEB1BD3EF410D1EDD1F7AE0F16897979DE28C6EF293E0A19282BD1D793F1331523FC71
A228800468C01A3653D14C6B4851A5C029478E757F
Public Exponent is '03'

Certificate Authority Public Key '53'
Length 'F8'
RID : A000000632
Public Modulus is
BCD83721BE52CCCC4B6457321F22A7DC769F54EB8025913BE804D9EABBFA19B3D7C5D3CA658D768C
AF57067EEC83C7E6E9F81D0586703ED9DDDADD20675D63424980B10EB364E81EB37DB40ED100344C92
8886FF4CCC37203EE6106D5B59D1AC102E2CD2D7AC17F4D96C398E5FD993ECB4FFDF79B17547FF9FA
2AA8EEFD6CBDA124CBB17A0F8528146387135E226B005A474B9062FF264D2FF8EFA36814AA2950065B
1B04C0A1AE9B2F69D4A4AA979D6CE95FEE9485ED0A03AEE9BD953E81CFD1EF6E814DFD3C2CE37AE
FA38C1F9877371E91D6A5EB59FDEDF75D3325FA3CA66CDFBA0E57146CC789818FF06BE5FCC50ABD36
2AE4B80996D
Public Exponent is '03'

Certificate Authority Public Key '94'
Length 'F8'
RID : A000000632
Public Modulus is
D1BE39615F395AC9337E3307AA5A7AC35EAE0036BF20B92F9A45D190B2F4616ABF9D340CBF5FBB3A2
B94BD8F2F977C0A10B90E59D4201AA32669E8CBE753F536119DF4FB5E63CED87F1153CE914B124F3E6B

648CD5C97655F7AB4DF62607C95DA50517AB8BE3836672D1C71BCDE9BA7293FF3482F124F86691130A
B08177B02F459C025A1F3DFFE0884CE78122542EA1C8EA092B552B586907C83AD65E0C6F91A400E485E
11192AA4C171C5A1EF56381F4D091CC7EF6BD8604CBC4C74D5D77FFA07B641D53998CDB5C21B7BC65
E082A6513F424A4B252E0D77FA4056986A0AB0CDA6155ED9A883C69CC2992D49ECBD4797DD2864FFC
96B8D
Public Exponent is '010001'

Certificate Authority Public Key '96'
Length '80'
RID : A000000632
Public Modulus is
B74586D19A207BE6627C5B0AAFBC44A2ECF5A2942D3A26CE19C4FFAEEE920521868922E893E7838225
A3947A2614796FB2C0628CE8C11E3825A56D3B1BBAEF783A5C6A81F36F8625395126FA983C5216D3166
D48ACDE8A431212FF763A7F79D9EDB7FED76B485DE45BEB829A3D4730848A366D3324C3027032FF8D1
6A1E44D8D
Public Exponent is '03'

Certificate Authority Public Key '97'
Length '60'
RID : A000000632
Public Modulus is
AF0754EAED977043AB6F41D6312AB1E22A6809175BEB28E70D5F99B2DF18CAE73519341BBBD327D0B
8BE9D4D0E15F07D36EA3E3A05C892F5B19A3E9D3413B0D97E7AD10A5F5DE8E38860C0AD004B1E06F4
040C295ACB457A788551B6127C0B29
Public Exponent is '03'

附 录 F
系统安全检测要求
（资料性附录）

F.1 范围

本部分适用于公共交通 IC 卡的系统制造商、运营商和相关技术人员。

F.2 文档准备

进行系统检测需要相关人员填写下列文档：

——调查问卷

——基本情况问卷

——系统检测准备工作清单

检测人员需要根据工作清单上的内容准备相关的安全文档以进行现场检查。准备内容包括但不限于以下内容：

序号	文档类型	包含要素
1	开发类文档	包括但不限于：用户手册、操作手册、需求说明书、需求分析文档、总体设计方案、数据库设计文档、概要设计文档、详细设计文档、工程实施方案、测试报告。
2	管理类文档	包括但不限于： 测试报告、系统运维手册、系统应急手册、运维管理制度、安全管理制度、安全审计报告等。
3	交易处理	联机交易和管理类交易
4	报文接口	IC 卡交易报文接口
5	文件接口	普通交易明细文件、转账交易明细文件、差错交易明细文件、汇总文件
6	数据安全传输控制	密钥的管理和控制、密钥的层次、联机报文 PIN 的加密和解密、联机报文 MAC 的加密和解密、基于联机标准的 IC 卡安全要求
7	通讯接口	网络接口和通讯接口配置及参数定义
8	联网安全	硬件加密机、前置设备、终端机具、网络、联网联合安全管理、IC 卡安全等方面的安全管理
9	网络架构说明	网络拓扑图及其说明（说明中应包括：网络边界的接入方式说明、网络拓扑图中的各个区域的安全级别说明等）。
10	测试报告	内部性能测试报告（包含各种 IC 卡交易） 提供稳定处理能力（收付速度基本一致）测试数据，包括并发笔数、核心服务器 CPU、内存数据和数据库服务器 CPU、内存数据
11	风险控制	风险控制相关管理类和技术类文档

F.3 系统准备

为保证检测结果的有效性，检测要求在实际系统或与实际系统完全一致的准生产系统或测试系统上进行检测。

F.4 其他准备

包括可进行所有类型交易的检测卡片。

附 录 G
SAM 卡送检要求
（资料性附录）

G.1 功能要求

送检样卡数量和其他证明材料请参考附录 B。

送检时需完成下列声明：

SAM 卡电气特性和协议测试功能一致性声明

PART I – 样品提供者标识			
注册号：			
公司名称：			
联系人：			
公司地址：			
电话：			
传真：			
EMAIL:			
签名和日期：			
PART II a–卡片信息			
描述	**名称**	**版本**	
COS			
样品名称			
芯片型号			
E^2PROM 容量			
卡芯片厂商			
卡封装厂商			
PART II b – 依据规范			
规范日期版本：			
PART III – 卡片执行			
功能	**指令**	**参数值**	
卡片类型		**类型 A**	
		类型 B	
		类型 C c6	
卡片协议		**T=0 协议**	
		T=1 协议	
T=0 协议		**在交互过程中卡片是否会发送字节“60”来请求额外工作等待时间，如果支持，请描述在何种情况，何种指令时发出。 c13**	
		描述：	
T=1 协议		**在 CCD/CPA 过程中，卡片是否发送额外工作等**	

		待时间请求 S（WTX）块。如果支持，请描述在何种情况，何种指令时发出。 c7	
		描述：	
		IFSC 值 c8	
		发送数据时 ICC 是否会发起链接，如果支持，请描述在何种情况，何种指令时发出。	
		描述：	
		当 CCD 指令长度大于 IFSC 时，卡片是否能够接受链接块，如果支持，请列举这样的指令和卡片响应	
		描述:	
复位	冷复位	冷复位 ATR:（提供卡能支持的最长历史字节）	
	热复位	热复位 ATR:（提供卡能支持的最长历史字节）	
	动态计算	卡复位时，是否受动态计算的影响，如果影响请提供更多信息	
应用选择	PSE	PSE 是否支持，如果支持，请提供选择 PSE 的 FCI 数据：	
		以及后续 READ RECORD 和响应:	
	应用	应用名称：	
		是否存在动态计算或者内部检查,使得 SELECT 命令发生变化	
		如果是，请描述最坏的情况：	
		冷复位选择的应用是否固定	
		如果不固定，请声明 ADF 或不固定的应用选择名称	
		热复位选择的应用是否固定	
		如果不固定，请声明 ADF 或不固定的应用选择名称	
DDA	内部认证	DDA 是否支持 c9	
持卡人验证	验证	密文 PIN 是否支持 c10	
		如果支持密文 PIN，最长私钥是什么	
第一次 GAC		最大响应大小（取决于 CDA 是否支持）	
第二次 GAC		最大响应大小（取决于 CDA 是否支持）	

G.2 安全要求

G.2.1 提交评估的样品要求：

——SAM 卡 30 张。要求该 SAM 卡处于可使用状态，即除了密钥、PIN 使用测试值之外，其它如文件系统结构、文件内容、支持的指令集等都要与实际发行的卡片一致。

——随机数数据文件，用于 RNG 评估。要求十六进制的.bin 格式文件（可参考附件样例），大于 150M 字节。

G.2.2 提交评估的文档要求：

——SAM卡文件结构说明

1) SAM卡支持的文件列表

2) SAM卡各应用（包括MF）下包含的文件标识、用途以及文件类型

3) SAM卡各应用（包括MF）下各文件的访问权限

——指令集说明

1) SAM卡各应用（包括MF）下支持的指令列表

2) SAM卡支持的各条指令参数、用途及返回状态码

——SAM卡芯片参数说明

1) SAM卡芯片类型、存储器类型及容量

2) SAM卡芯片工作电压

3) SAM卡芯片工作频率

4) SAM卡芯片工作温湿度

5) SAM卡芯片的其它参数（抗静电、电磁辐射、紫外线……）

——防攻击机制说明

1) SAM卡芯片硬件提供的防攻击机制，详细说明工作过程、原理及有效性

2) SAM卡软件所采用的防攻击机制，详细说明工作过程、原理及有效性

——软件开发过程中的功能测试报告

——芯片环境适应性测试报告（可选）

附 录 H
公共交通IC卡安全送检要求
（资料性附录）

H.1 送检准备材料

H.1.1 提交评估的样品要求：

——IC卡30张。要求该IC卡处于可使用状态，即除了密钥、PIN使用测试值之外，其它如文件系统结构、文件内容、支持的指令集等都要与实际发行的卡片一致。

——随机数数据文件，用于RNG评估。要求十六进制的.bin格式文件（可参考附件样例），大于150M字节。

H.1.2 提交评估的文档要求：

——IC卡文件结构说明

1) IC卡支持的文件列表

2) IC卡各应用（包括MF）下包含的文件标识、用途以及文件类型

3) IC卡各应用（包括MF）下各文件的访问权限

——指令集说明

1) IC卡各应用（包括MF）下支持的指令列表

2) IC卡支持的各条指令参数、用途及返回状态码

——IC卡芯片参数说明

1) IC卡芯片类型、存储器类型及容量

2) IC卡芯片工作电压

3) IC卡芯片工作频率

4) IC卡芯片工作温湿度

5) IC卡芯片的其它参数（抗静电、电磁辐射、紫外线……）

——防攻击机制说明

1) IC卡芯片硬件提供的防攻击机制，详细说明工作过程、原理及有效性

2) IC卡软件所采用的防攻击机制，详细说明工作过程、原理及有效性

——软件开发过程中的功能测试报告

——芯片环境适应性测试报告（如果有）

——芯片证明材料（参见附录 B）

——送检厂商调查问卷：

安全评估文档：	
1. 确认☐	芯片数据手册
2. 确认☐	硬件设计及实现（>100 页）
3. 确认☐	安全防护策略及实现（>100 页）
4. 确认☐	芯片版图设计说明
5. 确认☐	硬件平台使用及安全指南（>30 页）
6. 确认☐	CPU 及指令集设计说明
7. 确认☐	第三方 IP 设计说明书
8. 确认☐	版本变更说明（非第一次提交时）
9. 确认☐	测试开发套件说明文档
10. 确认☐	安全相关固件说明文档（供芯片使用方 COS 开发）
11. 确认☐	启动流程源代码说明
12. 确认☐	其它，请补充
源代码：	
13. 确认☐	DES/3DES、AES、RSA 等算法 RTL 代码及对应 testbench 文件
14. 确认☐	E2、Flash 等 NVM 存储器接口仿真数据
15. 确认☐	芯片版图（包括第三方 IP）
16. 确认☐	启动流程源代码
17. 确认☐	包含算法库程序在内的安全相关固件源码（与文档 10 对应）
18. 确认☐	测试 COS 代码（可编译的工程文件），要求实现各加密算法调用工程，要求固定以下命令字：密钥更新命令：80 40 00 00Lc，DES 加密命令：80 42 00 00 00，RSA 加密命令：80 44 00 00 00，AES 加密命令：80 46 00 00 00，其它依次类推；取响应命令 80 C0 00 00 XX
19. 确认☐	测试模式下 COS 源码
辅助工具：	
20. 确认☐	测试开发套件（仿真器、开发板、COS 下载工具等）（与文档 9 对应）
21. 确认☐	随机数采集工具（含采集说明，用于 RNG 评估，能够采集至少 128M 字节十六进制随机数，并可保存为*.BIN 格式）
22. 确认☐	其它，请补充
样品：	
23. 确认☐	提供唯一版本测试 COS，7816 接口、DIP 接口样品 提供测试电路完整样品 10 颗，可以直接进入测试模式 具体数量依据选择测试项目咨询客服人员
24. 确认☐	其它，请补充
其它第三方测试报告：	
25. 确认☐	CC IC 证书/报告
26. 确认☐	EMVCo 证书/报告
27. 确认☐	传感器功能验证报告

28. 确认☐	功耗测量报告
29. 确认☐	电磁辐射报告
30. 确认☐	随机数测试报告
31. 确认☐	电压毛刺测试报告
32. 确认☐	光注入测试报告
33. 确认☐	其它，请补充
厂商自测试报告：	
34. 确认☐	传感器功能验证报告
35. 确认☐	功耗测量报告
36. 确认☐	电磁辐射报告
37. 确认☐	随机数测试报告
38. 确认☐	电压毛刺测试报告
39. 确认☐	光注入测试报告
40. 确认☐	设计阶段功耗仿真图和数据
41. 确认☐	电磁操纵测试报告
42. 确认☐	中断处理测试报告
43. 确认☐	其他操纵测试报告
44. 确认☐	其它，请补充

附 录 I
公共交通 IC 卡芯片安全送检要求
（资料性附录）

I.1 送检准备材料

I.1.1 提交评估的样品要求：

序号	测试项名称	样品数量	样品封装	备注
01	芯片表面准备	N/A	N/A	
02	芯片背部准备	N/A	N/A	
03	传感器功能验证	4	卡片	
04	芯片表面简要分析	10	卡片	
05	芯片表面详细分析	10	卡片	
06	传输系统物理位置探测	N/A	N/A	
07	传输系统的 FIB 修改	N/A	N/A	
08	逻辑建立模块的干扰	10	卡片	
09	逻辑建立模块的修改	10	卡片	
10	测试模式的重激活	16	卡片/DIP 封装	测试模式下样片 10 张，用户模式下 6 张。如为 DIP 封装，应为非陶瓷封装，建议双 die
11	利用片上测试特性			
12	非易失性 ROM 信息的泄露	6	卡片	
13	被动探测	N/A	N/A	
14	主动探测	N/A	N/A	
15	非易失性 ROM 信息的产生	8	卡片	

16	直接读取非易失性可编程存储器	8	卡片	
17	非易失性可编程信号的产生	8	卡片	
18	电压对比	8	卡片 4 张；DIP4 张	DIP 必须使用非陶瓷类封装
19	供电电源操纵	5	卡片	
20	其他非侵入性操纵	5	卡片	
21	电磁操纵	10	卡片	
22	光注入	10	卡片	
23	放射线注入	5	卡片	
24	形象化功耗信息	10	卡片	
25	简单功耗分析			
26	差分功耗分析			
27	电磁辐射分析			
28	随机数发生器测试	2	卡片	支持 pps 模式
29	差分错误分析	10	卡片	
30	中断处理	5	卡片	
31	传输信息分析	N/A	N/A	
合计		160		

I.1.2 提交评估的文档要求：

——IC 卡文件结构说明

3) IC 卡支持的文件列表

4) IC 卡各应用（包括 MF）下包含的文件标识、用途以及文件类型

5) IC 卡各应用（包括 MF）下各文件的访问权限

——指令集说明

6) IC卡各应用（包括MF）下支持的指令列表

7) IC卡支持的各条指令参数、用途及返回状态码

——IC卡芯片参数说明

8) IC卡芯片类型、存储器类型及容量

9) IC卡芯片工作电压

10) IC卡芯片工作频率

11) IC卡芯片工作温湿度

12) IC卡芯片的其它参数（抗静电、电磁辐射、紫外线……）

——防攻击机制说明

13) IC卡芯片硬件提供的防攻击机制，详细说明工作过程、原理及有效性

14) IC卡软件所采用的防攻击机制，详细说明工作过程、原理及有效性

——软件开发过程中的功能测试报告

——芯片环境适应性测试报告（如果有）

——芯片证明材料（参见附录B）

——送检厂商调查问卷

其他文档：

安全测试文档	
1. 确认☐	芯片数据手册
2. 确认☐	芯片硬件设计及实现（>100页）
3. 确认☐	芯片安全防护策略及实现（>100页）
4. 确认☐	芯片版图设计说明
5. 确认☐	芯片硬件平台使用及安全指南（>30页）
6. 确认☐	CPU及指令集设计说明
7. 确认☐	第三方IP设计说明书
8. 确认☐	版本变更说明（非第一次提交时）
9. 确认☐	测试开发套件说明文档
10. 确认☐	安全相关固件说明文档（供芯片使用方进行COS开发）
11. 确认☐	启动流程及其源代码说明
12. 确认☐	其它
源代码（提交的软硬件源代码需有详细注释）	
13. 确认☐	DES/3DES、RSA等算法RTL代码及对应testbench文件
14. 确认☐	EEPROM、Flash等非易失性存储器接口仿真数据
15. 确认☐	芯片层次化版图（包括第三方IP，保留内部模块label）
16. 确认☐	启动流程源代码

17. 确认☐	包含算法库程序在内的安全相关固件源码（与文档 10 对应）
18. 确认☐	测试 COS 代码（与附件 4 对应，可编译的工程文件），要求至少提供下列 APDU：可变多字节读写片内存储器、取随机数、DES 加解密、RSA 加解密、其他算法加解密。
19. 确认☐	测试模式实现源代码（包括软件源代码及硬件 RTL 代码），测试模式下支持的命令列表（包括激活测试模式的私有口令）及其使用说明。
20. 确认☐	其它
辅助工具	
21. 确认☐	测试开发套件（仿真器、开发板、COS 下载工具等）（与文档 9 对应）
22. 确认☐	随机数采集工具工程文件（含采集说明，用于 RNG 评估，能够采集至少 128M 字节十六进制随机数，并可保存为*.BIN 格式）
23. 确认☐	测试模式样片通信转接板
24. 确认☐	其它
样品	
25. 确认☐	提供 7816 接口、DIP 接口样品； 提供测试电路完整样品，建议双 die 封装； 具体数量及封装形式依据所选择测试项目咨询客服人员
26. 确认☐	其它
其它第三方测试报告（如果有）	
27. 确认☐	CC 证书/报告
28. 确认☐	EMVCo 证书/报告
29. 确认☐	其它
厂商自测试报告（如果有）	
30. 确认☐	传感器功能验证报告
31. 确认☐	功耗测量报告
32. 确认☐	电磁辐射报告
33. 确认☐	随机数测试报告
34. 确认☐	电压毛刺测试报告
35. 确认☐	光注入测试报告
36. 确认☐	设计阶段功耗仿真图和数据
37. 确认☐	电磁操纵测试报告
38. 确认☐	中断处理测试报告
39. 确认☐	其他操纵测试报告
40. 确认☐	其它