ICS 35.240.40
A 11
备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0045.3—2014
代替JR/T 0045.3—2008

中国金融集成电路（IC）卡检测规范 第3部分：借记/贷记应用个人化检测规范

China financial integrated circuit card test specifications—
Part 3: Debit/Credit personalization test specification

2014-07-30 发布　　2014-07-30 实施

中国人民银行　发布

目　次

前　言

JR/T 0045 《中国金融集成电路（IC）卡检测规范》 分为5个部分：

——第 1 部分：借记/贷记应用卡片检测规范；

——第 2 部分：借记/贷记应用终端检测规范；

——第 3 部分：借记/贷记应用个人化检测规范；

——第 4 部分：非接触卡片检测规范；

——第 5 部分：非接触终端检测规范。

本部分为JR/T 0045的第3部分。

本部分依据GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0045.3—2008《中国金融集成电路（IC）卡检测规范　第3部分：借记/贷记应用个人化检测规范》。

本部分与JR/T 0045.3—2008相比主要变化如下：

——修改了标准的前言；

——在第 4.15 条个人化数据与 ICS 的一致性中，增加了许多案例；

——修改了附录 E；

——对近几年 IC 卡实际使用中遇到的问题，设计了一些新的案例；

——对原标准在文字描述上的勘误做出修正。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分主要起草单位：中国人民银行、中国银联股份有限公司、银行卡检测中心、中国金融电子化公司。

本部分主要起草人：王永红、李晓枫、陆书春、潘润红、杜宁、李兴锋、陈则栋、李新、汤沁莹、齐大鹏、李春欢、刘志刚、张永峰、余沁、张艳。

本部分于2008年首次发布，本次为第一次修订。

引　言

本部分的主要依据是 JR/T 0025.10，在此基础上制定了中国金融集成电路（IC）卡借记/贷记应用卡片个人化的相关检测案例。

本部分对金融借记/贷记的卡片个人化检测提供了指导意见和检测方法。

中国金融集成电路（IC）卡检测规范
第3部分：借记/贷记应用个人化检测规范

1 范围

本部分从卡片检测的角度描述了对借记/贷记卡片个人化的要求。

本部分适用于由银行发行或受理的金融借记/贷记应用的IC卡。其使用对象主要是与金融借记/贷记IC卡应用相关的卡片、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 符号和缩略语

下列符号和缩略语适用于本文件。

ADA	应用默认行为(Application Default Action)
AFL	应用文件定位器(Application File Locator)
AIP	应用交互特征(Application Interchange Profile)
ATC	应用交易计数器(Application Transaction Counter)
AUC	应用使用控制(Application Usage Control)
BIN	银行标识号(Bank Identification Number)
CA	认证中心(Certificate Authority)
CDA	复合DDA/AC 生成(Combined DDA/AC Generation)
CDOL	卡风险管理数据对象列表（Card Risk Management Data Object List）
CID	密文信息数据(Cryptogram Information Data)
C-MAC	指令讯息认证码（Command-Message Authentication Code）
CVM	持卡人验证方式(Cardholder Verification Method)
DDA	动态数据认证(Dynamic Data Authentication)
DDOL	动态数据认证数据对象列表（Dynamic Data Authentication Data Object List）
ENC MDK	数据加密的DEA主密钥(Master Data Encipherment DEA Key)
ENC UDK	独有的数据加密DEA子密钥(Unique Data Encipherment DEA Key)
GPO	获取处理选项(Get Processing Options)
IAC	发卡行行为代码(Issuer Action Code)
IAD	发卡行应用数据(Issuer Application Data)
IC	集成电路(Integrated Circuit Card)
ICC	集成电路卡(Integrated Circuit Card)
ICS	实现一致性声明(Implementation Conformance Statement
MAC	报文认证码(Message Authentication Code)
MAC MDK	报文认证码DEA主密钥
MAC UDK	报文认证码DEA独有子密钥

MDK	中国金融集成电路（IC）卡借记/贷记应用的主分散密钥(Master Derivation Key)
PAN	应用主账号(Primary Account Number)
PIN	个人密码(Personal Identification Number)
RFU	保留为将来使用(Reserved for Future Use)
RSA	Rivest, Sharmir, and Adleman 提出的一种非对称密钥算法
SAD	已签名的静态应用数据(Signed Static Application Data)
SDA	静态数据认证(Static Data Authentication)
SFI	短文件标识符(Short File Identifier)
UDK	由 MDK 产生的中国金融集成电路（IC）卡独有密钥

3 测试条件

默认环境条件（温度，湿度等）是指常温20±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。

测试前，被测样品应被个人化完成。被测样品宜采用附录A表A.1中的CA公钥，被测样品的发卡行公私钥对及IC卡公私钥对宜由发卡机构产生，如因故无法自行产生，则可采用附录B表B.1、附录C表C.1中的公私钥对。被测样品中的对称密钥宜由发卡机构产生，如因故无法自行产生，则可采用附录D表D.1中的密钥。

4 个人化测试案例

4.1 复位应答（FWYD）

4.1.1 FWYD001-00

测试目的：验证卡返回的 ATR 的 TS 符合规范要求。
测试条件：强制。
测试流程：卡片上电（ATR）。
通过标准：起始字符 TS 应为‘3B’或‘3F’。

4.1.2 FWYD002-00

测试目的：验证卡返回的 ATR 的 T0 和历史字符符合规范要求。
测试条件：强制。
测试流程：卡片上电（ATR）。
通过标准：TA1 到 TD1 的存在与 T0 高半字节位 5-位 8 的值一致。历史字符的个数与低半字节位 1-位 4 表示的值一致。使用 T=0 协议时，推荐 T0=‘6X’；使用 T=1 协议时，推荐 T0=‘EX’。

4.1.3 FWYD003-00

测试目的：验证卡返回的 ATR 的 TA1 符合规范要求。
测试条件：强制。
测试流程：卡片上电（ATR）。
通过标准：满足以下情况中的任意一条：

——ATR 中不存在 TA1；

——ATR 中存在 TA1(T0 的位 5 设为‘1’)，则 TA1 的值应在‘11’到‘13’之间。

4.1.4 FWYD004-00

测试目的：验证卡返回的 ATR 的 TB1 符合规范要求。

测试条件：强制。

测试流程：卡片上电（ATR）。

通过标准：ATR 中应存在 TB1(T0 的位 6 设为‘1’)，且 TB1 应为‘00’。

4.1.5 FWYD005-00

测试目的：验证卡返回的 ATR 的 TC1 符合规范要求。

测试条件：强制。

测试流程：卡片上电（ATR）。

通过标准：TC1 应存在，且 TC1 的值应在‘00’到‘FF’之间。

4.1.6 FWYD006-00

测试目的：验证卡返回的 ATR 的 TD1 符合规范要求。

测试条件：强制。

测试流程：卡片上电（ATR）。

通过标准：当选用 T=0 协议时，IC 卡不回送 TD1，或 TD1 存在且 TA2 到 TD2 的存在与 TD1 的高半字节一致且 TD1 的低半字节的值为‘0’或‘1’。当选用 T=1 协议时，推荐 IC 卡回送 TD1=‘81’。

4.1.7 FWYD007-00

测试目的：验证卡返回的 ATR 的 TA2 符合规范要求。

测试条件：ATR 中返回 TD1。

测试流程：卡片上电（ATR）。

通过标准：满足以下情况中的任意一条：

——ATR 中不包含 TA2；

——ATR 中存在 TA2，且 TA2 的低 4 位应等于 TD1 的低 4 位；位 8 应表明 IC 卡是否有能力改变它的操作模式；位 7-位 6 应等于‘00’；位 5 应表明在复位应答后是按接口字节提供的传输参数进行，还是按终端默认的传输参数进行。

4.1.8 FWYD008-00

测试目的：验证卡返回的 ATR 的 TB2 符合规范要求。

测试条件：ATR 中返回 TD1。

测试流程：卡片上电（ATR）。

通过标准：ATR 中应不存在 TB2。

4.1.9 FWYD009-00

测试目的：验证卡返回的 ATR 的 TC2 符合规范要求。

测试条件：ATR 中返回 TD1。
测试流程：卡片上电（ATR）。
通过标准：满足以下情况中的任意一条：
——ATR 中不包含 TC2；
——TC2 存在，且 TC2=‘0A’。

4.1.10 FWYD010-00

测试目的：验证卡返回的 ATR 的 TD2 符合规范要求。
测试条件：ATR 中返回 TD1。
测试流程：卡片上电（ATR）。
通过标准：如果 ATR 含 TD2，则 TD2 的高半字节与 TA3 到 TD3 的存在一致，低半字节的值为‘1’或‘E’（如果 TD1 的低半字节为‘0’）。
注：推荐使用 T=0 协议时不回送 TD2，使用 T=1 协议时，TD2=‘31’。

4.1.11 FWYD011-00

测试目的：验证卡返回的 ATR 的 TA3 符合规范要求。
测试条件：TD2 指明使用 T=1 协议。
测试流程：卡片上电（ATR）。
通过标准：满足以下情况中的任意一条：
——TA3 不存在；
——如果 TA3 存在，TA3 应在‘10’到‘FE’之间。

4.1.12 FWYD012-00

测试目的：验证卡返回的 ATR 的 TB3 符合规范要求。
测试条件：TD2 指明使用 T=1 协议。
测试流程：卡片上电（ATR）。
通过标准：TB3 应存在，T3 的高半字节表示 BWI，取值为‘0’到‘4’，TB3 的低半字节表示 CWI，取值为‘0’到‘5’。

4.1.13 FWYD013-00

测试目的：验证卡返回的 ATR 的 TC3 符合规范要求。
测试条件：TD2 指明使用 T=1 协议。
测试流程：卡片上电（ATR）。
通过标准：满足以下情况中的任意一条：
——TC3 不存在；
——TC3 存在，且 TC3 =‘00’。

4.1.14 FWYD014-00

测试目的：验证卡返回的 ATR 的 TCK 符合规范要求。
测试条件：强制。
测试流程：卡片上电（ATR）。
通过标准：仅 T=0 协议时，IC 卡不回送 TCK。在非仅 T=0 情况下 TCK 的值应使从 T0 到包括 TCK 在内的所有字节进行异或运算的结果为零。

4.2 IC 文件中强制数据的读取（SJDQ）

4.2.1 SJDQ001-00

测试目的：验证应用数据中含 2 磁道等价数据。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘57’的 2 磁道等价数据。

4.2.2 SJDQ002-00

测试目的：验证应用数据中含持卡人证件号。
测试条件：可选。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘9F61’的持卡人证件号。

4.2.3 SJDQ003-00

测试目的：验证应用数据中含持卡人证件类型。
测试条件：可选。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘9F62’的持卡人证件类型。

4.2.4 SJDQ004-00

测试目的：验证应用数据中含应用主账号（PAN）。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘5A’的应用主账号（PAN）。

4.2.5 SJDQ005-00

测试目的：验证应用数据中含发卡行行为码（IAC）缺省。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘9F0D’的发卡行行为码（IAC）缺省。

4.2.6 SJDQ006-00

测试目的：验证应用数据中含发卡行行为码（IAC）拒绝。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘9F0E’的发卡行行为码（IAC）拒绝。

4.2.7 SJDQ007-00

测试目的：验证应用数据中含发卡行行为码（IAC）联机。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘9F0F’的发卡行行为码（IAC）联机。

4.2.8 SJDQ008-00

测试目的：验证应用数据中含应用失效日期。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘5F24’的应用失效日期。失效日期格式为 YYMMDD。

4.2.9 SJDQ009-00

测试目的：验证应用数据中含卡片风险管理数据对象列表 1（CDOL1）。
测试条件：强制。

测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘8C’的卡片风险管理数据对象列表 1（CDOL1）。

4.2.10 SJDQ010-00

测试目的：验证应用数据中含卡片风险管理数据对象列表 2（CDOL2）。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘8D’的卡片风险管理数据对象列表 2（CDOL2）。

4.2.11 SJDQ011-00

测试目的：验证应用数据中含应用版本号。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读 SFI 在 1 到 10 之间的文件的应用数据。
通过标准：读应用数据过程中，应能够获得标签=‘9F08’的应用版本号。

4.2.12 SJDQ012-00

测试目的：验证卡片中含有发卡行应用数据。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)执行 VERIFY 命令；
e)第一个 GENERATE AC 命令请求 TC。
通过标准：卡对 GENERATE AC 命令响应中应含有‘9F10’的发卡行应用数据。

4.2.13 SJDQ013-00

测试目的：验证 qPBOC 时卡片不在读记录时返回主账号序列号‘5F34’。
测试条件：支持 qPBOC。
测试流程：a)卡片上电（ATR）；

b)选择 PPSE；
c)选择 PBOC 借记/贷记应用；
d)执行 GET PROCESSING OPTIONS 命令，给出 9F66 中终端支持非接触借记/贷记位为零，支持 qPBOC 位为一，使卡片进入 qPBOC 流程；给出的授权金额小于 qPBOC 脱机消费可用余额 9F5D；
e)根据 AFL 读记录。

通过标准：在读取应用数据阶段，卡片不应返回主账号序列号‘5F34’。

4.2.14 SJDQ014-00

测试目的：验证数据认证相关数据（9F69）的合法性。
测试条件：支持 fDDA。
测试流程：a)卡片上电（ATR）；
b)选择 qPBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：卡片应返回 9F69 且 9F69 的格式符合规范要求。

4.3 磁条与 IC 数据的一致性（CTSJ）

4.3.1 CTSJ001-00

测试目的：验证磁条第 2 磁道的应用主账号数据与卡片芯片内的应用主账号一致。
测试条件：支持磁条。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)比较芯片中与磁条中的应用主账号。
通过标准：从磁条中读出的应用主账号应与芯片中的应用主账号一致。

4.3.2 CTSJ002-00

测试目的：验证磁条第 2 磁道的数据中的部分值与卡片芯片内的 2 磁等价数据中的对应值一致。
测试条件：支持磁条。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)比较芯片中与磁条中 2 磁数据。
通过标准：从磁条中读出的 2 磁数据中的服务码、失效日期、主账号应与芯片中的 2 磁等价数据中的对应值一致。

4.3.3 CTSJ003-00

测试目的：验证磁条第 2 磁道的失效日期与卡片芯片内的失效日期一致。
测试条件：支持磁条。

测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)读出磁条第 2 磁道中的失效日期并进行比较。
通过标准：从 IC 芯片中读出的标签=‘5F24’的失效日期（YYMMDD）的年月值应与第 2 磁道中的失效日期（YYMM）的值一致。

4.3.4 CTSJ004-00

测试目的：验证磁条第 2 磁道的服务代码与卡片芯片内的服务代码一致。
测试条件：支持磁条，IC 芯片中存在服务代码标签=‘5F30’。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)读出磁条第 2 磁道中的服务代码并进行比较。
通过标准：从磁条和 IC 芯片中获得的标签=‘5F30’的服务代码应一致。

4.4 应用选择（YYXZ）

4.4.1 YYXZ001-00

测试目的：验证 PSE 应用选择返回的文件控制信息（FCI）的有效性。
测试条件：支持 PSE。
测试流程：a)卡片上电（ATR）；
b)选择 PSE。
通过标准：成功选择 PSE 后应使用标签=‘6F’的 FCI 模板回送 FCI 数据。且 FCI 的数据格式应正确。

4.4.2 YYXZ002-00

测试目的：验证选择 PSE 的应答报文(FCI)返回的目录基本文件的 SFI 的有效性。
测试条件：支持 PSE。
测试流程：a)卡片上电（ATR）；
b)选择 PSE 应用；
c)根据返回的 SFI，发 READ RECORD 命令读目录文件，直到卡返回‘6A83’。
通过标准：SFI 的值应在 1-10 之间。

4.4.3 YYXZ003-00

测试目的：验证 PSE 目录文件下的记录编码是否正确。
测试条件：支持 PSE。
测试流程：a)卡片上电（ATR）；
b)选择 PSE 应用；
c)根据返回的 SFI，发 READ RECORD 命令读目录文件，直到卡返回‘6A83’。
通过标准：支付系统目录包括正确的 ADF 入口。

4.4.4 YYXZ004-00

测试目的：验证选择 ADF 的应答报文 (FCI)的有效性。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 ADF。
通过标准：成功选择 ADF 后应使用标签=‘6F’的 FCI 模板回送的 FCI 数据；FCI 中的数据格式应正确。

4.4.5 YYXZ005-00

测试目的：验证 PPSE 应用选择返回的文件控制信息（FCI）的有效性。
测试条件：支持非接触借记/贷记或 qPBOC。
测试流程：a)卡片上电（ATR）；
b)选择 PPSE。
通过标准：成功选择 PPSE 后应使用标签=‘6F’的 FCI 模板回送 FCI 数据。

4.4.6 YYXZ006-00

测试目的：验证非接触交易，应用选择最终选择后，返回 PDOL 中应含有 9F66。
测试条件：支持非接触借记/贷记或 qPBOC。
测试流程：a)卡片上电（ATR）；
b)选择 PPSE；
c)选择卡片和终端共同支持的金融应用。
通过标准：成功选择 PPSE；卡片在最终选择时返回的 PDOL 应含有 9F66。

4.5 应用初始化（YYCS）

4.5.1 YYCS001-00

测试目的：验证 AIP 的内容与卡支持的功能一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令。
通过标准：卡片收到 GET PROCESSING OPTIONS 命令后，响应数据中应含有 AIP(标签=‘82’）。卡片响应的 AIP 应与 ICS 中填写的 AIP 值一致。

4.5.2 YYCS002-00

测试目的：验证 AFL 的编码正确，并且与实际文件一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令。
通过标准：卡片收到 GET PROCESSING OPTIONS 命令后，响应数据中应含有 AFL(标签=‘94’)；AFL 的长度为 4 个字节的倍数；每四个字节中的第一个字节表示 SFI，其取值范围应为 1-30；每四个字节中的第二个字节表示记录的起始序

号，其值应大于0；每四个字节中的第三个字节表示记录的截止序号，其值应不小于起始序号；每四个字节中的第四个字节表示参与脱机数据认证的连续记录的个数，其取值范围应0到（截至序号-起始序号+1）；AFL的编码应与卡中文件实际情况一致。

4.5.3 YYCS003-00

测试目的：验证qPBOC时卡片在GPO时返回主账号序列号‘5F34’。

测试条件：支持qPBOC。

测试流程：a)卡片上电（ATR）；

b)选择PPSE；

c)选择PBOC借记/贷记应用；

d)执行GET PROCESSING OPTIONS命令，给出9F66中终端支持非接触借记/贷记位为零，支持qPBOC位为一，使卡片进入qPBOC流程；给出的授权金额小于qPBOC脱机消费可用余额9F5D；

e)卡片复位（ATR）；

f)选择PPSE；

g)选择PBOC借记/贷记应用；

h)执行GET PROCESSING OPTIONS命令，给出9F66中终端支持非接触借记/贷记位为零，支持qPBOC位为一，使卡片进入qPBOC流程；给出的授权金额大于qPBOC脱机消费可用余额9F5D但小于终端非接触交易限额。

通过标准：卡片收到GET PROCESSING OPTIONS命令后，响应数据中应含有主账号序列号‘5F34’；卡片响应的主账号序列号‘5F34’的值与ICS中填写的值一致。

4.6 静态数据认证SDA（JTSJ）

4.6.1 JTSJ001-00

测试目的：验证如果支持SDA，卡片中的SDA相关数据的有效性。

测试条件：支持SDA。

测试流程：a)卡片上电（ATR）；

b)选择PBOC借记/贷记应用；

c)执行GET PROCESSING OPTIONS命令；

d)根据卡片响应的AFL，发READ RECORD命令读应用数据。

通过标准：根据AFL指定的文件记录中应包含以下数据：

——认证中心公钥索引；

——发卡行公钥证书；

——发卡行公钥指数；

——发卡行公钥余项（当$N_I > N_{CA}-36$时，应存在）；

——签名静态应用数据。

4.6.2 JTSJ002-00

测试目的：验证认证中心公钥索引的有效性。

测试条件：支持SDA。

测试流程：a)卡片上电（ATR）；

b)选择PBOC借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：卡中的认证中心公钥索引格式应为‘b8’。

4.6.3 JTSJ003-00

测试目的：验证发卡行公钥证书的有效性。
测试条件：支持 SDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：卡中的发卡行公钥证书是有效的。

4.6.4 JTSJ004-00

测试目的：验证发卡行公钥指数的有效性。
测试条件：支持 SDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：发卡行公钥指数应与发卡行公钥证书恢复数据中的发卡行公钥指数长度一致；发卡行公钥指数应为 3 或 2^16+1。

4.6.5 JTSJ005-00

测试目的：验证发卡行公钥余项有效性。
测试条件：支持 SDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：当 $N_I > N_{CA}-36$ 时，发卡行公钥余项应存在，且长度为 $N_I - N_{CA} + 36$ 个字节；当 $N_I \leqslant N_{CA} - 36$ 时，发卡行公钥余项应不存在。

4.6.6 JTSJ006-00

测试目的：验证签名的静态应用数据有效性。
测试条件：支持 SDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：签名的静态应用数据有效；数据认证码应与 ICS 填写一致。

4.6.7 JTSJ007-00

测试目的：验证 SDA 标签列表的有效性。
测试条件：支持 SDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：卡中如含有‘9F4A’（静态数据认证标签列表），其值应为‘82’；支持 DDA、fDDA 或 CDA 的卡片，应含有 9F4A。

4.7 动态数据认证 DDA（DTSJ）

4.7.1 DTSJ001-00

测试目的：验证如果支持 DDA，卡片中的 DDA 相关数据的有效性。
测试条件：支持 DDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：根据 AFL 指定的文件记录中应包含以下数据：
——认证中心公钥索引；
——发卡行公钥证书；
——发卡行公钥指数；
——发卡行公钥余项（当 $N_I > N_{CA}-36$ 时，应存在）；
——IC 卡公钥证书；
——IC 卡公钥指数；
——IC 卡公钥余项(当 $N_{IC}>N_I-42$ 时，应存在)。

4.7.2 DTSJ002-00

测试目的：验证发卡行公钥证书有效性。
测试条件：支持 DDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：卡中的发卡行公钥证书是有效的。

4.7.3 DTSJ003-00

测试目的：验证发卡行公钥指数有效性。
测试条件：支持 DDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：发卡行公钥指数应与发卡行公钥证书恢复数据中的发卡行公钥指数长度一

致；发卡行公钥指数应为 3 或 2^16+1。

4.7.4 DTSJ004-00

测试目的：验证发卡行公钥余项有效性。
测试条件：支持 DDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：当 $N_I > N_{CA}-36$ 时，发卡行公钥余项应存在，且长度为 $N_I - N_{CA} +36$ 个字节；当 $N_I \leqslant N_{CA} - 36$ 时，发卡行公钥余项应不存在。

4.7.5 DTSJ005-00

测试目的：验证 IC 卡公钥证书有效性。
测试条件：支持 DDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：卡中的 IC 卡公钥证书是有效的。

4.7.6 DTSJ006-00

测试目的：验证 IC 卡公钥指数有效性。
测试条件：支持 DDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：IC 卡公钥指数应为 3 或 2^16+1；IC 卡公钥指数应与 IC 卡公钥证书恢复数据中指明的 IC 卡公钥指数长度一致。

4.7.7 DTSJ007-00

测试目的：验证 IC 卡公钥余项有效性。
测试条件：支持 DDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：当 $N_{IC}>N_I - 42$ 时，IC 卡公钥余项应存在，且长度为 $N_{IC} - N_I +42$ 个字节；当 $N_{IC} \leqslant N_I - 42$ 时，IC 卡公钥余项应不存在。

4.7.8 DTSJ008-00

测试目的：验证动态数据认证数据对象列表 DDOL 的有效性。

测试条件：支持 DDA，卡片记录中包含 DDOL。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；

d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。

通过标准：DDOL 中应含有‘9F3704’。

4.7.9 DTSJ009-00

测试目的：验证 IC 卡私钥签署的签名动态应用数据的有效性。

测试条件：支持 DDA。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；

d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；

e)执行内部认证命令。

通过标准：卡片应正确返回的签名动态应用数据。

4.8 复合动态数据认证 CDA（FHSJ）

4.8.1 FHSJ001-00

测试目的：验证如果支持 CDA，卡片中的 CDA 相关数据的有效性。

测试条件：支持 CDA。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；

d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。

通过标准：根据 AFL 指定的文件记录中应包含以下数据：

——认证中心公钥索引；

——发卡行公钥证书；

——发卡行公钥指数；

——发卡行公钥余项（当 $N_I > N_{CA}-36$ 时，应存在）；

——IC 卡公钥证书；

——IC 卡公钥指数；

——IC 卡公钥余项(当 $N_{IC}>N_I-42$ 时，应存在)。

4.8.2 FHSJ002-00

测试目的：验证发卡行公钥证书有效性。

测试条件：支持 CDA。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；

d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。

通过标准：卡中的发卡行公钥证书是有效的。

4.8.3 FHSJ003-00

测试目的：验证发卡行公钥指数有效性。
测试条件：支持 CDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：发卡行公钥指数应与发卡行公钥证书恢复数据中的发卡行公钥指数长度一致；发卡行公钥指数应为 3 或 2^16+1。

4.8.4 FHSJ004-00

测试目的：验证发卡行公钥余项有效性。
测试条件：支持 CDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：当 $N_I > N_{CA}-36$ 时，发卡行公钥余项应存在，且长度为 $N_I - N_{CA}+36$ 个字节；当 $N_I \leqslant N_{CA} - 36$ 时，发卡行公钥余项应不存在。

4.8.5 FHSJ005-00

测试目的：验证 IC 卡公钥证书有效性。
测试条件：支持 CDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：卡中的 IC 卡公钥证书是有效的。

4.8.6 FHSJ006-00

测试目的：验证 IC 卡公钥指数有效性。
测试条件：支持 CDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：IC 卡公钥指数应为 3 或 2^16+1；IC 卡公钥指数应与 IC 卡公钥证书恢复数据中指明的 IC 卡公钥指数长度一致。

4.8.7 FHSJ007-00

测试目的：验证 IC 卡公钥余项有效性。
测试条件：支持 CDA。
测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。

通过标准：当 $N_{IC}>N_I-42$ 时，IC 卡公钥余项应存在，且长度为 $N_{IC}-N_I+42$ 个字节；当 $N_{IC}\leqslant N_I-42$ 时，IC 卡公钥余项应不存在。

4.8.8 FHSJ008-00

测试目的：验证动态数据认证数据对象列表 DDOL 的有效性。
测试条件：支持 CDA，卡片记录中包含 DDOL。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：DDOL 中应含有‘9F3704’。

4.8.9 FHSJ009-00

测试目的：验证 IC 卡正确处理请求的复合动态数据认证，且私钥签署的签名动态应用数据是有效的。
测试条件：支持 CDA。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)执行 GENERATE AC 请求 TC/CDA。
通过标准：卡片应使用 77 模板正确返回的签名动态应用数据。

4.9 持卡人认证（CKRZ）

4.9.1 CKRZ001-00

测试目的：验证持卡人验证方式列表的有效性。
测试条件：支持持卡人认证。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读（SFI 在 1-10 范围内）应用数据。
通过标准：读出的应用数据中应包含标签=‘8E’的持卡人验证方式列表；持卡人验证方式列表应与 ICS 填写一致。

4.9.2 CKRZ002-00

测试目的：确保持卡人验证方式列表中指定的认证方法所需的数据存在且有效。
测试条件：支持持卡人认证。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)根据持卡人验证方式列表中指定的认证方法执行持卡人认证。

通过标准：指定的持卡人认证方法应能够正确执行。

4.9.3 CKRZ003-00

测试目的：验证如果支持 PIN 验证，则应能够正确取得 PIN 尝试计数器。
测试条件：支持持卡人认证，且支持 PIN 验证方式。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)GET DATA 取 PIN 尝试次数‘9F17’；
f)VERIFY 命令正确的 PIN。
通过标准：卡应正确响应 GET DATA 命令，返回 PIN 尝试次数应与 ICS 填写一致；卡应正确响应 VERIFY 命令，返回状态字‘9000’。

4.10 终端风险管理（FXGL）

4.10.1 FXGL001-00

测试目的：验证进行终端风险管理之频度检查的卡片数据。
测试条件：可选。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：记录文件中应含有连续脱机交易下限标签=‘9F14’和连续脱机交易上限标签=‘9F23’。

4.10.2 FXGL002-00

测试目的：应用交易交易计数器(ATC)是否被初始化为零。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)执行 VERIFY 命令；
f)GET DATA 取‘9F36’。
通过标准：卡片响应 GET DATA 命令的 ATC 应为‘0001’。

4.10.3 FXGL003-00

测试目的：上次联机应用交易交易计数器(LOATC)是否被初始化为零。
测试条件：强制。
测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)执行 VERIFY 命令；
f)GET DATA 取‘9F13 ’。

通过标准：卡片响应 GET DATA 命令的 LOATC 为‘0000’。

4.11 交易日志（JYRZ）

4.11.1 JYRZ001-00

测试目的：验证交易日志入口的有效性。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用。
通过标准：PBOC 借记/贷记应用选择返回的 FCI 中应包含交易日志入口标签=‘9F4D’；交易日志入口推荐为‘0B0A’。

4.11.2 JYRZ002-00

测试目的：验证交易日志格式有效性。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取日志格式‘9F4F’；
d)执行 READ RECORD 命令读交易日志。
通过标准：卡片应正确响应 GET DATA 命令，返回交易日志格式；依据卡片返回的交易日志格式，交易日志文件应能够被正确解析。

4.11.3 JYRZ003-00

测试目的：验证交易日志文件中的终端数据元是否包括在 PDOL 或 CDOL 中。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)GET DATA 取交易日志格式‘9F4F’。
通过标准：交易日志格式 9F4F 中涉及的终端数据对象应包含在 PDOL 或 CDOL 中。

4.11.4 JYRZ004-00

测试目的：验证交易日志文件是否有效。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；

e)执行 VERIFY 命令；
f)执行第一个 GENERATE AC 请求 TC；
g)执行 EXTERNAL AUTHENTICATE 命令（如在第一个 GENERATE AC 命令卡返回 ARQC）；
h)执行第二个 GENERATE AC 请求 TC（如在第一个 GENERATE AC 命令卡返回 ARQC）
i)查询交易日志；
j)卡片上电（ATR）；
k)选择 PBOC 借记/贷记应用；
l)GET DATA 取日志格式 9F4F；
m)执行 READ RECORD 命令读交易日志（SFI=11）直到返回‘6A83’。

通过标准：交易日志中应存在一笔交易记录；交易日志的内容应正确。

4.12 圈存日志（QCRZ）

4.12.1 QCRZ001-00

测试目的：验证圈存日志入口的有效性。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用。
通过标准：PBOC 借记/贷记应用选择返回的 FCI 中应包含圈存日志入口标签=‘DF4D’；圈存日志入口推荐为‘0C0A’。

4.12.2 QCRZ002-00

测试目的：验证圈存日志格式有效性。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取日志格式‘DF4F’；
d)执行 READ RECORD 命令读交易日志。
通过标准：卡片应正确响应 GET DATA 命令，返回日志格式；依据卡片返回的圈存日志格式，交易日志文件应能够被正确解析。

4.12.3 QCRZ003-00

测试目的：验证圈存日志文件中的终端数据元是否包括在 PDOL 或 CDOL 中。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)GET DATA 取日志格式‘DF4F’。
通过标准：日志格式 DF4F 中涉及的终端数据对象应包含在 PDOL 或 CDOL 中。

4.12.4 QCRZ004-00

测试目的：验证圈存日志文件是否有效。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)执行 VERIFY 命令；
f)执行第一个 GENERATE AC 请求 ARQC；
g)执行 EXTERNAL AUTHENTICATE 命令；
h)执行第二个 GENERATE AC 请求 TC；
i)执行 Put Data 9F79 和 Put Data DF79；
j)查询圈存交易日志；
k)卡片上电（ATR）；
l)选择 PBOC 借记/贷记应用；
m)GET DATA 取圈存日志格式 DF4F；
n)执行 READ RECORD 命令读圈存日志直到返回‘6A83’。
通过标准：圈存日志中应存在一笔交易记录；圈存日志的内容应正确。

4.13 其他数据检查（KXSJ）

4.13.1 KXSJ001-00

测试目的：验证卡片中的应用生效日期是否有效。
测试条件：卡中存在应用生效日期。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：记录文件应能够取得应用生效日期‘5F25’；应用生效日期的格式应为‘YYMMDD’；应用生效日期‘5F25’应不晚于应用失效日期‘5F24’。

4.13.2 KXSJ002-00

测试目的：验证卡片中的应用用途控制（AUC）是否有效。
测试条件：卡中存在应用用途控制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：应用用途控制的编码正确。

4.13.3 KXSJ003-00

测试目的：验证发卡行公钥证书的有效期是否有效
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；

d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。

通过标准：发卡行公钥证书的有效期的年年月月值小于等于应用失效日期‘5F24’中的年年月月值。

4.13.4 KXSJ004-00

测试目的：验证 CDOL1 和 CDOL2 被放置在了 AFL 中指明的参与脱机数据验证的记录中。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；

d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。

通过标准：验证 CDOL1 和 CDOL2 被放置在了 AFL 中指明的参与脱机数据验证的记录中。

4.14 密钥的有效性（MYYX）

4.14.1 MYYX001-00

测试目的：验证卡内应用密文密钥分散得是否正确。

测试条件：强制。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；

d)执行 Verify 命令；

e)执行第一个 GENERATE AC 命令请求 TC。

通过标准：卡片响应 GENERATE AC 命令的应用密文应正确。

4.14.2 MYYX002-00

测试目的：验证卡内安全报文认证（MAC）密钥分散得是否正确。

测试条件：强制。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；

d)执行 Verify 命令；

e)执行第一个 GENERATE AC 命令请求 ARQC；

f)执行外部认证命令，ARPC 正确；

g)执行第二个 GENERATE AC 请求 TC；

h)执行脚本命令 APPLICATION UNBLOCK，MAC 错误。

i)卡片上电（ATR）；

j)选择 PBOC 借记/贷记应用；

k)执行 GET PROCESSING OPTIONS 命令；

l)执行 Verify 命令；

m)执行第一个 GENERATE AC 命令请求 ARQC；

n)执行外部认证命令，ARPC 正确；

o)执行第二个 GENERATE AC 请求 TC；

p)执行脚本命令 APPLICATION UNBLOCK，MAC 正确。

通过标准：交易 1 中脚本命令 APPLICATION UNBLOCK 卡片响应状态字应不是‘9000’，

推荐卡片响应状态字‘6988’；交易 2 中脚本命令 APPLICATION UNBLOCK 卡片响应状态字为‘9000’。

4.14.3 MYYX003-00

测试目的：验证卡内安全报文加密密钥分散得是否正确。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)执行 Verify 命令；
e)第一个 GENERATE AC 命令请求 ARQC；
f)执行外部认证命令，ARPC 正确；
g)第二个 GENERATE AC 请求 TC；
h)执行 PIN CHANGE/UNBLOCK 命令，PIN 加密错误。
i)卡片上电（ATR）；
j)选择 PBOC 借记/贷记应用；
k)执行 GET PROCESSING OPTIONS 命令；
l)执行 Verify 命令；
m)第一个 GENERATE AC 命令请求 ARQC；
n)执行外部认证命令，ARPC 正确；
o)第二个 GENERATE AC 请求 TC；
p)执行 PIN CHANGE/UNBLOCK 命令，PIN 加密正确。
通过标准：交易 1 中脚本命令 PIN CHANGE/UNBLOCK 卡响应状态字应不是‘9000’；交易 2 中脚本命令 PIN CHANGE/UNBLOCK 卡响应状态字应为‘9000’。

4.15 个人化数据与 ICS 的一致性（SJYZ）

4.15.1 SJYZ001-00

测试目的：验证应用货币代码与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)GET DATA 取 9F51。
通过标准：响应数据的应用货币代码‘9F42’应与 ICS 填写一致；响应数据的应用货币代码‘9F51’应与 ICS 填写一致；响应数据的应用货币代码‘9F42’应与响应数据的应用货币代码‘9F51’一致。

4.15.2 SJYZ002-00

测试目的：验证应用货币指数与 ICS 一致。
测试条件：卡片中存在应用货币指数‘9F44’。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的应用货币指数‘9F44’应与 ICS 填写一致。

4.15.3 SJYZ003-00

测试目的：验证应用生效日期与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的应用生效日期‘5F25’应与 ICS 填写一致。

4.15.4 SJYZ004-00

测试目的：验证应用失效日期与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的应用失效日期‘5F24’应与 ICS 填写一致。

4.15.5 SJYZ006-00

测试目的：验证应用标识与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PSE（如支持 PSE）；
c)执行 READ REACORD 命令读 DIR 目录文件(如支持 PSE)；
d)选择 PBOC 借记/贷记应用。
通过标准：响应数据的应用标识‘4F’应与 ICS 填写一致。

4.15.6 SJYZ008-00

测试目的：验证应用标签与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PSE（如支持 PSE）；
c)执行 READ REACORD 命令读 DIR 目录文件(如支持 PSE)；
d)选择 PBOC 借记/贷记应用。
通过标准：响应数据的应用标签‘50’应与 ICS 填写一致。

4.15.7 SJYZ009-00

测试目的：验证应用首选名与 ICS 一致。
测试条件：卡片中存在应用首选名‘9F12’。

测试流程：a)卡片上电（ATR）；
b)选择 PSE（如支持 PSE）；
c)执行 READ REACORD 命令读 DIR 目录文件(如支持 PSE)；
d)选择 PBOC 借记/贷记应用。
通过标准：响应数据的应用首选名‘9F12’应与 ICS 填写一致。

4.15.8 SJYZ010-00

测试目的：验证应用主账号与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的应用主账号‘5A’应与 ICS 填写一致。

4.15.9 SJYZ011-00

测试目的：验证应用主账号序列号与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的应用主账号序列号‘5F34’应与 ICS 填写一致。

4.15.10 SJYZ012-00

测试目的：验证应用优先级指示器与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用。
通过标准：响应数据的应用优先级指示器‘87’应与 ICS 填写一致。

4.15.11 SJYZ013-00

测试目的：验证应用用途控制(AUC)与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的应用用途控制‘9F07’应与 ICS 填写一致。

4.15.12 SJYZ014-00

测试目的：验证应用版本号与 ICS 一致。
测试条件：强制。

测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的应用版本号‘9F08’应与 ICS 填写一致。

4.15.13 SJYZ015-00

测试目的：验证 CDOL1 与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的 CDOL1‘8C’应与 ICS 填写一致。

4.15.14 SJYZ016-00

测试目的：验证 CDOL2 与 ICS 一致。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的 CDOL2‘8D’应与 ICS 填写一致。

4.15.15 SJYZ017-00

测试目的：验证持卡人姓名与 ICS 一致。
测试条件：卡片中存在持卡人姓名‘5F20’。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的持卡人姓名‘5F20’应与 ICS 填写一致。

4.15.16 SJYZ018-00

测试目的：验证第一次 GAC 命令中发卡行应用数据‘9F10’正确。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)执行 VERIFY 命令；
f)执行第一个 GENERATE AC 请求 TC。
通过标准：卡片在第一个 GENERATE AC 响应数据中的发卡行应用数据正确。

4.15.17 SJYZ018-01

测试目的：验证第二次 GAC 命令中发卡行应用数据‘9F10’正确。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)执行 VERIFY 命令 ；
f)执行第一个 GENERATE AC 请求 ARQC；
g)执行 EXTERNAL AUTHENTICATE 命令（如卡片支持发卡行认证）；
h)执行第二个 GENERATE AC 请求 TC。
通过标准：卡片在第二个 GENERATE AC 响应数据中的发卡行应用数据应正确。

4.15.18 SJYZ018-02

测试目的：验证快速借记贷记时 GPO 命令中发卡行应用数据‘9F10’正确。
测试条件：强制。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：卡片在 GPO 响应数据中的发卡行应用数据应正确。

4.15.19 SJYZ020-00

测试目的：验证卡产品信息‘9F63’与 ICS 一致。
测试条件：卡片中存在卡产品信息‘9F63’
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。
通过标准：响应数据的卡产品信息‘9F63’应与 ICS 填写一致。

4.15.20 SJYZ021-00

测试目的：验证发卡行认证指示位‘9F56’与 ICS 一致。
测试条件：卡片中存在发卡行认证指示位‘9F56’。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取发卡行认证指示位‘9F56’。
通过标准：响应数据的发卡行认证指示位‘9F56’应与 ICS 填写一致。

4.15.21 SJYZ022-00

测试目的：验证连续脱机交易限制数(国际-货币)‘9F53’与 ICS 一致。
测试条件：卡片中存在连续脱机交易限制数(国际-货币) ‘9F53’。
测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取连续脱机交易限制数(国际-货币) ‘9F53’。

通过标准：响应数据的连续脱机交易限制数(国际-货币) ‘9F53’应与 ICS 填写一致；借记卡若存在该值，则应为全零。

4.15.22 SJYZ023-00

测试目的：验证累计脱机交易金额限制数‘9F54’与 ICS 一致。

测试条件：卡片中存在累计脱机交易金额限制数‘9F54’。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取累计脱机交易金额限制数‘9F54’。

通过标准：响应数据的累计脱机交易金额限制数‘9F54’应与 ICS 填写一致；借记卡若存在该值，则应为全零。

4.15.23 SJYZ024-00

测试目的：验证累计脱机交易金额上限‘9F5C’与 ICS 一致。

测试条件：卡片中存在累计脱机交易金额上限‘9F5C’。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取累计脱机交易金额上限‘9F5C’。

通过标准：响应数据的累计脱机交易金额上限‘9F5C’应与 ICS 填写一致；借记卡若存在该值，则应为全零。

4.15.24 SJYZ025-00

测试目的：验证连续脱机交易下限‘9F58’与 ICS 一致。

测试条件：卡片中存在连续脱机交易下限‘9F58’。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取连续脱机交易下限‘9F58’。

通过标准：响应数据的连续脱机交易下限‘9F58’ 应与 ICS 填写一致；借记卡若存在该值，则应为全零。

4.15.25 SJYZ026-00

测试目的：验证连续脱机交易上限‘9F59’与 ICS 一致。

测试条件：卡片中存在连续脱机交易上限‘9F59’ 。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取连续脱机交易上限‘9F59’。

通过标准：响应数据的连续脱机交易上限‘9F59’ 应与 ICS 填写一致；借记卡若存在该值，则应为全零。

4.15.26 SJYZ027-00

测试目的：验证连续脱机交易限制数(国际-国家)‘9F72’与 ICS 一致。

测试条件：卡片中存在连续脱机交易限制数(国际-国家)‘9F72’ 。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取连续脱机交易限制数(国际-国家)‘9F72’ 。

通过标准：响应数据的连续脱机交易限制数(国际-国家)‘9F72’ 应与 ICS 填写一致；借记卡若存在该值，则应为全零。

4.15.27 SJYZ028-00

测试目的：验证连续脱机交易限制数(双货币)‘9F75’与 ICS 一致。

测试条件：卡片中存在连续脱机交易限制数(双货币)‘9F75’。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取连续脱机交易限制数(双货币)‘9F75’。

通过标准：响应数据的连续脱机交易限制数(双货币)‘9F75’应与 ICS 填写一致；借记卡若存在该值，则应为全零。

4.15.28 SJYZ029-00

测试目的：验证发卡行国家代码‘5F28’与 ICS 一致。

测试条件：强制。

测试流程：a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)执行 GET PROCESSING OPTIONS 命令；

d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据。

通过标准：响应数据的发卡行国家代码‘5F28’应与 ICS 填写一致。

4.15.29 SJYZ031-00

测试目的：验证卡片附加处理‘9F68’与 ICS 一致。

测试条件：卡片支持 qPBOC。

测试流程：a)卡片上电（ATR）；

b)选择 PPSE；

c)选择 PBOC 借记/贷记应用；

d)GET DATA 取卡片附加处理‘9F68’。

通过标准：响应数据的卡片附加处理‘9F68’应与 ICS 填写一致。

4.15.30 SJYZ032-00

测试目的：验证卡片交易属性‘9F6C’与 ICS 一致。

测试条件：卡片支持 qPBOC。

测试流程：a)卡片上电（ATR）；

b)选择 PPSE；

c)选择 PBOC 借记/贷记应用；

d)执行 GPO，等待卡片返回 qPBOC 流程的 GPO 响应。

通过标准：响应数据的卡片交易属性‘9F6C’中的第一字节第 5 位和第 6 位应与 ICS 填写一致。

4.15.31 SJYZ033-00

测试目的：验证卡片 CVM 限额‘9F6B’与 ICS 一致。
测试条件：卡片支持 qPBOC。
测试流程：a)卡片上电（ATR）；
b)选择 PPSE；
c)选择 PBOC 借记/贷记应用；
d)GET DATA 取卡片 CVM 限额‘9F6B’。
通过标准：响应数据的卡片 CVM 限额‘9F6B’应与 ICS 填写一致。

4.15.32 SJYZ034-00

测试目的：验证电子现金余额上限‘9F77’与 ICS 一致。
测试条件：卡片支持电子现金。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取电子现金余额上限‘9F77’。
通过标准：响应数据的电子现金余额上限‘9F77’ 应与 ICS 填写一致。

4.15.33 SJYZ035-00

测试目的：验证电子现金单笔交易限额‘9F78’与 ICS 一致。
测试条件：卡片支持电子现金。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取电子现金单笔交易限额‘9F78’。
通过标准：响应数据的电子现金单笔交易限额‘9F78’应与 ICS 填写一致。

4.15.34 SJYZ036-00

测试目的：验证电子现金重置阈值‘9F6D’与 ICS 一致。
测试条件：卡片支持电子现金。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取电子现金重置阈值‘9F6D’。
通过标准：响应数据的电子现金重置阈值‘9F6D’应与 ICS 填写一致。

4.15.35 SJYA037-00

测试目的：验证电子现金发卡行授权码‘9F74’的返回时机正确。
测试条件：强制。
测试流程：a)1 笔借记贷记交易；
b)1 笔基于借记贷记的小额支付交易；
c)1 笔快速借记贷记交易。
通过标准：流程 a 时在读取应用数据阶段，卡片不应返回电子现金发卡行授权码‘9F74’；流程 b 和流程 c 时，在读取应用数据阶段，卡片应返回电子现金发卡行授权码‘9F74’。

4.16 第二货币相关数据

4.16.1 DEHB001-00

测试目的：验证第二币种电子现金应用货币代码与 ICS 一致。
测试条件：卡片支持双币电子现金或双币 qPBOC。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)执行 GET PROCESSING OPTIONS 命令；
d)根据卡片响应的 AFL，发 READ RECORD 命令读应用数据；
e)GET DATA 取 DF71。
通过标准：第二币种电子现金应用货币代码‘DF71’应与 ICS 填写一致。

4.16.2 DEHB002-00

测试目的：验证第二币种卡片 CVM 限额‘DF72’与 ICS 一致。
测试条件：卡片支持双币 qPBOC。
测试流程：a)卡片上电（ATR）；
b)选择 PPSE；
c)选择 PBOC 借记/贷记应用；
d)GET DATA 取第二币种卡片 CVM 限额‘DF72’。
通过标准：响应数据的第二币种卡片 CVM 限额‘DF72’应与 ICS 填写一致。

4.16.3 DEHB003-00

测试目的：验证第二币种电子现金余额上限‘DF77’与 ICS 一致
测试条件：卡片支持双币电子现金。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取第二币种电子现金余额上限‘DF77’。
通过标准：响应数据的第二币种电子现金余额上限‘DF77’ 应与 ICS 填写一致。

4.16.4 DEHB004-00

测试目的：验证第二币种电子现金单笔交易限额‘DF78’与 ICS 一致。
测试条件：卡片支持双币电子现金。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取第二币种电子现金单笔交易限额‘DF78’。
通过标准：响应数据的第二币种电子现金单笔交易限额‘DF78’应与 ICS 填写一致。

4.16.5 DEHB005-00

测试目的：验证第二币种电子现金重置阈值‘DF76’与 ICS 一致。
测试条件：卡片支持双币电子现金。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取第二币种电子现金重置阈值‘DF76’。

通过标准：响应数据的第二币种电子现金重置阈值‘DF76’应与 ICS 填写一致。

4.17 扩展应用相关数据（KZYY）

4.17.1 KZYY001-00

测试目的：扩展应用标识‘DF61’正确。
测试条件：支持扩展应用。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用。
通过标准：应用选择时，卡片返回的 DF61 正确。

4.17.2 KZYY002-00

测试目的：分段扣费押金抵扣限额‘DF62’正确。
测试条件：支持扩展应用。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用；
c)GET DATA 取分段扣费押金抵扣限额 DF62。
通过标准：卡片返回的 DF62 正确。

4.17.3 KZYY003-00

测试目的：PDOL 中含 CAPP 交易指示位‘DF60’。
测试条件：支持扩展应用。
测试流程：a)卡片上电（ATR）；
b)选择 PBOC 借记/贷记应用。
通过标准：PDOL 中含 CAPP 交易指示位‘DF60’。

4.17.4 KZYY004-XX

测试目的：扩展应用变长文件被正确初始化。
测试条件：支持扩展应用。
子类案例：——XX=00：扩展应用变长文件 0x15 被正确初始化；
——XX=01：扩展应用变长文件 0x16 被正确初始化；
——XX=02：扩展应用变长文件 0x17 被正确初始化；
——XX=03：扩展应用变长文件 0x18 被正确初始化；
——XX=04：扩展应用变长文件 0x19 被正确初始化；
——XX=05：扩展应用变长文件 0x1A 被正确初始化；
——XX=06：扩展应用变长文件 0x1B 被正确初始化。
测试流程：a)卡片上电（ATR）；
b)选择 UICS 借记/贷记应用；
c)GET DATA 取 ATC；
d)对子类案例中的每一个扩展应用文件进行 APPEND RECORD 操作。
通过标准：APPEND RECRD 成功。

4.17.5 KZYY005-00

测试目的：扩展应用循环文件 0x1E 被正确初始化。

测试条件：支持扩展应用。

测试流程：a)卡片上电（ATR）；

b)选择 UICS 借记/贷记应用；

c)GET DATA 取 ATC；

d)对循环文件 0x1E 进行 APPEND RECORD 操作。

通过标准：APPEND RECRD 成功。

4.17.6 KZYY006-XX

测试目的：扩展应用变长文件的初始记录被正确添加。

测试条件：支持扩展应用。

子类案例：——XX=00：扩展应用变长文件 0x15 的初始记录被正确添加；

——XX=01：扩展应用变长文件 0x16 的初始记录被正确添加；

——XX=02：扩展应用变长文件 0x17 的初始记录被正确添加；

——XX=03：扩展应用变长文件 0x18 的初始记录被正确添加；

——XX=04：扩展应用变长文件 0x19 的初始记录被正确添加；

——XX=05：扩展应用变长文件 0x1A 的初始记录被正确添加；

——XX=06：扩展应用变长文件 0x1B 的初始记录被正确添加。

测试流程：对子类案例中的每一个扩展应用文件执行下列操作：

a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取 ATC；

d)Read CAPP Data Cache 命令；

e)GPO；

f)UPDATE CAPP Data Cache 命令；

g)读记录。

通过标准：d)和 f)应成功。

4.17.7 KZYY007-00

测试目的：扩展应用循环文件 0x1E 下的初始记录被正确添加。

测试条件：支持扩展应用。

测试流程：对循环文件 0x1E 执行下列操作：

a)卡片上电（ATR）；

b)选择 PBOC 借记/贷记应用；

c)GET DATA 取 ATC；

d)Read CAPP Data Cache 命令读全部记录；

e)GPO；

f)UPDATE CAPP Data Cache 命令；

g)读记录。

通过标准：d)和 f)应成功。

附 录 A
（资料性附录）
测试 CA 公钥

表 A.1 测试 CA 公钥

索引	长度	指数	模数
0A	1024 位	3	B2 AB 1B 6E 9A C5 5A 75 AD FD 5B BC 34 49 0E 53 C4 C3 38 1F 34 E6 0E 7F AC 21 CC 2B 26 DD 34 46 2B 64 A6 FA E2 49 5E D1 DD 38 3B 81 38 BE A1 00 FF 9B 7A 11 18 17 E7 B9 86 9A 97 42 B1 9E 5C 9D AC 56 F8 B8 82 7F 11 B0 5A 08 EC CF 9E 8D 5E 85 B0 F7 CF A6 44 EF F3 E9 B7 96 68 8F 38 E0 06 DE B2 1E 10 1C 01 02 89 03 A0 60 23 AC 5A AB 86 35 F8 E3 07 A5 3A C7 42 BD CE 6A 28 3F 58 5F 48 EF
08	1152 位	3	B6 16 45 ED FD 54 98 FB 24 64 44 03 7A 0F A1 8C 0F 10 1E BD 8E FA 54 57 3C E6 E6 A7 FB F6 3E D2 1D 66 34 08 52 B0 21 1C F5 EE F6 A1 CD 98 9F 66 AF 21 A8 EB 19 DB D8 DB C3 70 6D 13 53 63 A0 D6 83 D0 46 30 4F 5A 83 6B C1 BC 63 28 21 AF E7 A2 F7 5D A3 C5 0A C7 4C 54 5A 75 45 62 20 41 37 16 96 63 CF CC 0B 06 E6 7E 21 09 EB A4 1B C6 7F F2 0C C8 AC 80 D7 B6 EE 1A 95 46 5B 3B 26 57 53 3E A5 6D 92 D5 39 E5 06 43 60 EA 48 50 FE D2 D1 BF
09	1408 位	3	EB 37 4D FC 5A 96 B7 1D 28 63 87 5E DA 2E AF B9 6B 1B 43 9D 3E CE 0B 18 26 A2 67 2E EE FA 79 90 28 67 76 F8 BD 98 9A 15 14 1A 75 C3 84 DF C1 4F EF 92 43 AA B3 27 07 65 9B E9 E4 79 7A 24 7C 2F 0B 6D 99 37 2F 38 4A F6 2F E2 3B C5 4B CD C5 7A 9A CD 1D 55 85 C3 03 F2 01 EF 4E 8B 80 6A FB 80 9D B1 A3 DB 1C D1 12 AC 88 4F 16 4A 67 B9 9C 7D 6E 5A 8A 6D F1 D3 CA E6 D7 ED 3D 5B E7 25 B2 DE 4A DE 23 FA 67 9B F4 EB 15 A9 3D 8A 6E 29 C7 FF A1 A7 0D E2 E5 4F 59 3D 90 8A 3B F9 EB BD 76 0B BF DC 8D B8 B5 44 97 E6 C5 BE 0E 4A 4D AC 29 E5
0B	1984 位	3	CF 9F DF 46 B3 56 37 8E 9A F3 11 B0 F9 81 B2 1A 1F 22 F2 50 FB 11 F5 5C 95 87 09 E3 C7 24 19 18 29 34 83 28 9E AE 68 8A 09 4C 02 C3 44 E2 99 9F 31 5A 72 84 1F 48 9E 24 B1 BA 00 56 CF AB 3B 47 9D 0E 82 64 52 37 5D CD BB 67 E9 7E C2 AA 66 F4 60 1D 77 4F EA EF 77 5A CC C6 21 BF EB 65 FB 00 53 FC 5F 39 2A A5 E1 D4 C4 1A 4D E9 FF DF DF 13 27 C4 BB 87 4F 1F 63 A5 99 EE 39 02 FE 95 E7 29 FD 78 D4 23 4D C7 E6 CF 1A BA BA A3 F6 DB 29 B7 F0 5D 1D 90 1D 2E 76 A6 06 A8 CB FF FF EC BD 91 8F A2 D2 78 BD B4 3B 04 34 F5 D4 51 34 BE 1C 27 81 D1 57 D5 01 FF 43 E5 F1 C4 70 96 7C D5

			7C E5 3B 64 D8 29 74 C8 27 59 37 C5 D8 50 2A 12 52 A8 A5 D6 08 8A 25 9B 69 4F 98 64 8D 9A F2 CB 0E FD 9D 94 3C 69 F8 96 D4 9F A3 97 02 16 2A CB 5A F2 9B 90 BA DE 00 5B C1 57

附 录 B
（资料性附录）
测试发卡行公私钥对

表 B.1 测试发卡行公私钥对

长度	公钥指数	模数	私钥指数
1024 位	3	EE 3F 92 4D 9A FF 10 F4 C9 41 E0 7A BC 1C F9 87 EC 4C 2A D0 7C 2A 1A 54 64 68 3A 48 66 70 20 58 48 59 83 64 68 CD E6 64 B9 15 B7 B9 97 64 33 73 90 BE DE 6D D7 AE E2 12 A3 8D D4 05 35 98 6C 7B 76 26 22 CA E0 0C 5A A5 DD 6B D6 FE 7D DC 45 2D 8C B5 84 84 AF 57 E1 49 2E AF C9 2F 28 24 2E 11 8F 86 C3 E8 A1 77 05 3F DE 7A B0 F0 09 F6 0A 26 56 C2 DE 02 41 DD F5 BB C6 76 E3 F3 B8 D2 B0 23	9E D5 0C 33 BC AA 0B 4D DB 81 40 51 D2 BD FB AF F2 DD 71 E0 52 C6 BC 38 42 F0 26 DA EE F5 6A E5 85 91 02 42 F0 89 44 43 26 0E 7A 7B BA 42 CC F7 B5 D4 94 49 3A 74 96 B7 17 B3 E2 AE 23 BA F2 FB AF F5 01 8D 83 4E 6F 57 78 79 31 8E 4D 47 C5 39 3B FA E6 C7 D4 44 F4 F5 E0 2A E0 CC 77 F2 C7 E3 F9 48 9B 3A A8 D7 E8 D3 4E FE 32 35 2B 67 58 34 78 FB 5E C0 B0 9D 6A 0A 98 2A D1 29 65 2D CC 1B
1152 位	3	C2 AB E7 63 CD 75 D5 7D DC D3 4C F6 32 AA 27 F5 E9 5A 52 04 56 2C 2D 39 E9 46 07 74 C7 61 B8 65 73 E9 D4 C1 B5 AC 4D AD A9 F4 2F 92 17 71 2B 73 D5 A6 6E 29 EA 8E 02 74 08 5F F6 33 CB 8E BB FA FB 13 F8 BC 82 63 84 E1 52 2F AB 4F C4 54 58 18 CB 6F 41 65 85 84 5E 7E 64 B7 21 A3 4B E4 8F AE F0 B0 78 DC BA DE BE 5F FA 22 A7 47 FF AB C8 EC F6 2F E4 B0 96 94 9F AE 88 A3 31 79 28 73 16 3B EC D9 0D 75 D8 F1 57 0F 47 ED 40 F7 86 90 B7 FB	81 C7 EF 97 DE 4E 8E 53 E8 8C DD F9 77 1C 1A A3 F0 E6 E1 58 39 72 C8 D1 46 2E AF A3 2F 96 7A EE 4D 46 8D D6 79 1D 89 1E 71 4D 75 0C 0F A0 C7 A2 8E 6E F4 1B F1 B4 01 A2 B0 3F F9 77 DD 09 D2 A7 52 0D 50 7D AC 42 58 95 0D 03 C3 ED 80 BF A7 CC 4C 57 53 B4 B4 47 EC E4 BA F8 ED 37 16 90 10 E1 9E 0E F9 14 49 28 A3 06 96 CA F7 37 F8 DE 03 7F EB 90 EE 74 60 A6 8B A5 D1 5D E3 D8 79 71 55 F1 41 95 DD 24 46 58 6F 4B 54 AE 58 A2 77 D9 2E 5B
1408 位	3	BB 15 6E E2 17 99 4E A7 57 AB 4F 73 BD 26 A9 A6 CA E5 1C 08 D6 C5 A8 E6 26 E9 D5 61 3E 54 14 02 6B 92 77 F0 7A 50 04 25 39 C4 02 2A 5D 15 D9 9F 83 33 8F CA 9B F2 E8 BE B6 88 6B 59 E1 54 7D 72 43 44 C3 A3 19 CA 33 10 6D EB 4B 28 55 02 D7 D6 D8 A0 8A A7 29 47 93 F5 69 02 07 E2 A6 C4 B6 40 A3 26 4C 21 A3 3E 55 FD E2 99 52 6F C1 09 CB 97 BD F9 4B 43 FE B3 5B A9 82 83 5E BC D5 C1 D0 3A 12 A3 8F 73 6F 1B 22 B9 94 B0 AC 95 89 EC 0B	7C B8 F4 96 BA 66 34 6F 8F C7 8A 4D 28 C4 71 19 DC 98 BD 5B 39 D9 1B 44 19 F1 38 EB 7E E2 B8 01 9D 0C 4F F5 A6 E0 02 C3 7B D8 01 71 93 63 E6 6A 57 77 B5 31 BD 4C 9B 29 CF 05 9C E6 96 38 53 A1 82 2D D7 C2 11 31 77 60 49 47 87 70 38 AC 8F E4 90 6B 07 1A 1B 85 0D 4D 20 53 A6 BE 0D 83 A7 68 B5 3D 8A BE FB E5 21 14 97 3D 88 73 BB 3B 4B F1 05 F3 6E 7B 75 A6 E0 A1 E6 2E C3 EA DC FC 01 59 67 67 F7 FA 83 85 8D 01 23 10 87 AC AE B3 6C

		66 57 0D 12 52 93 CE 59 A4 4D 25 C9 24 42 6B 58 4D AE C3 89 0A 05 AE 3D C7 22 5C 9B 4E 0A CD 67 37	06 7B FF 13 A6 05 A3 1F 25 66 85 62 BD FE 3E DA 23 53 4C 60 2F 8E 65 C9 86 DB 08 5D 3A DB 89 E9 1B
1984 位	3	A5 D7 0F 5D C5 E9 D5 5C E7 B1 50 5C 9B DF A4 08 CE C4 9E 98 61 8F AF DA DC CA 6E AA 3C 0C 39 A8 5E 58 D0 07 EE 86 12 F1 55 FA 9D 64 75 A0 B0 4D E7 43 3A 77 32 A4 BE F7 15 8E 39 A6 08 18 09 C4 4B 69 6D 10 DF D6 1D DF 23 E7 31 94 47 A5 6B A3 D1 8E D3 95 77 77 3D 71 FF 67 D7 1A 37 8A 3C B1 11 38 EC EA A5 7B FE 03 10 51 E7 53 AD 1B E4 9D 92 71 12 9C 32 5D ED 09 89 02 E1 B1 DD 24 75 D7 CD 26 E8 AC CD C4 D8 91 A8 F3 11 7C F8 D9 CC CD 2D 48 A9 21 8E F6 1F 01 E1 2F 23 B0 88 ED 23 79 B9 20 87 DD A8 B9 54 E4 28 3E AA D0 11 81 CA 3C B3 A2 8A 1F C6 93 25 90 3D E1 79 E3 60 36 F5 76 45 D9 AE F8 DC C6 E1 E3 5B 16 F8 22 4F F9 74 16 07 4E 76 C9 FE 94 D5 54 EC AD 36 F5 64 B2 AC D2 38 D1 E2 ED 5F D2 FD 9E 0F 8C 28 18 CD 91 CF 3C 92 13 23 AC 5A D7 39 71	6E 8F 5F 93 D9 46 8E 3D EF CB 8A E8 67 EA 6D 5B 34 83 14 65 96 5F CA 91 E8 86 F4 71 7D 5D 7B C5 94 3B 35 5A 9F 04 0C A0 E3 FC 68 ED A3 C0 75 89 44 D7 7C 4F 77 18 7F 4F 63 B4 26 6E B0 10 06 82 DC F0 F3 60 95 39 69 3F 6D 44 CB B8 2F C3 9D 17 E1 09 E2 63 A4 FA 28 F6 AA 45 3A 11 7A 5C 28 76 0B 7B 48 9C 6E 52 A9 57 60 36 9A 37 C8 BD 43 13 B6 F6 0C 68 21 93 F3 5B B0 AC 96 75 80 5B 85 5F C4 27 22 39 05 08 03 68 68 13 D8 EE 47 05 12 E4 E6 8C 87 A5 23 DC E0 3D 90 F5 27 AB AA 9F C9 24 C5 09 F0 AE CA 04 44 DF 3A F9 88 D3 5D 75 77 6D 18 6F 8A 32 48 43 C4 90 4A 78 65 BD 11 11 E9 28 1A 5F 9F 6D 04 17 26 83 B7 06 12 DE 8B 77 FD E3 27 C0 20 72 01 5B 75 84 BD AE 4D EE C2 65 DC 85 3F 22 38 73 C2 91 3E A5 B3 A9 18 E3 3E ED A4 48 98 17 D8 B7 3C 6E 05 C3

附 录 C
（资料性附录）
测试 IC 卡公私钥对

表 C.1 测试发卡行公私钥对

长度	公钥指数	模数	私钥指数
768 位	3	C8 AD 83 9D 49 7B 8D 57 BE 2E 05 78 3A 60 A4 82 0A 62 1B 0B 7D 31 98 20 B8 F8 5A F5 F5 4C C6 82 50 B3 C9 CB E1 86 01 27 18 0B B2 93 6E 66 44 AC D2 E9 94 63 C7 5A C6 39 39 A8 5F 6A AD 8B 9E 5D 69 94 80 FE FF BF D8 DE 4A A0 4E 57 72 73 5E 52 64 92 C4 32 EF F8 5D EB B5 DE 2A E7 69 A9 C8 F3	85 C9 02 68 DB A7 B3 8F D4 1E AE 50 26 EB 18 56 B1 96 BC B2 53 76 65 6B 25 FA E7 4E A3 88 84 56 E0 77 DB DD 41 04 00 C4 BA B2 77 0C F4 44 2D C7 5D A3 A6 3C F9 5E 88 46 48 4C 95 F1 06 98 45 D8 20 40 8A 31 05 AE 79 55 51 0D 0F E2 5D 4F 80 29 F3 E4 FE 9F 8B 33 18 AB A6 D5 55 4E 3C F3 48 2B
1024 位	3	C7 1A 43 77 0C 1E 59 28 59 80 1E 3C 31 A6 BC CD 85 C6 F1 F1 1F 33 4E 8E D4 41 99 6A EA 5B 2B F9 B3 FF 58 C6 73 1D 8F AC C8 60 E6 0F 89 34 14 16 FB 66 54 4C CE D2 78 AE F8 C2 E4 E0 D4 C5 4A 76 46 4B 91 24 51 FD 26 1A 39 DB 45 94 71 4C DA 9C 02 76 6E 90 BF 12 CD 6D C2 DE 51 56 B7 E4 B6 A6 54 71 DD E4 0A 58 0F 26 E1 01 5D 82 F8 CB 78 80 DC 14 B8 78 E9 8E BD DE DD B7 13 C1 07 4C 5D A1	84 BC 2C FA 08 14 3B 70 3B AA BE D2 CB C4 7D DE 59 2F 4B F6 14 CC DF 09 E2 D6 66 47 46 E7 72 A6 77 FF 90 84 4C BE 5F C8 85 95 EE B5 06 22 B8 0F 52 44 38 33 34 8C 50 74 A5 D7 43 40 8D D8 DC 4D AB CB D2 D3 82 DA 75 80 ED 18 1A 10 C9 77 C9 46 D7 AC 39 25 06 52 77 8E D2 1D 65 A0 59 9A 9E 35 6E 95 45 FA 02 7B CD 68 4C DE 1D D4 B8 E1 BC 8E C1 71 12 4E 23 FC 7A 2C 71 7B 00 7E 68 C5 1B 2B
1152 位	3	DE D9 E1 BC 8E 74 9C AD 74 94 84 BF B4 72 44 5B C8 1F FA A8 97 07 64 8C 34 2A A3 0D 1B E6 0D 5E D0 F6 CE AB A2 5C 68 3D 45 03 CB 11 CA F9 1A 39 72 75 93 CF 2B EE AE 80 32 EF AC C4 4F DF 8D A3 1D 60 07 13 9D 45 95 E8 65 5C 74 95 CF 46 A9 D5 93 A8 3E 3C 65 B2 CB F2 AF 1E EA 02 D1 F9 69 51 A9 46 61 6B 5A B2 1C A0 BF 34 D1 2D 05 F6 AE 18 35 08 A7 AC 7A 46 91 3B DC E5 FD C3 91 4C A7 50 01 8B 13 0C A5 BA D4 9A D8 C0 22 91 AC A5 CF FD	94 91 41 28 5E F8 68 73 A3 0D AD D5 22 F6 D8 3D 30 15 51 C5 BA 04 ED B2 CD 71 C2 08 BD 44 08 E9 E0 A4 89 C7 C1 92 F0 28 D8 AD 32 0B DC A6 11 7B A1 A3 B7 DF 72 9F 1F 00 21 F5 1D D8 35 3F B3 C2 13 95 5A 0D 13 83 B9 44 5A 65 3A 29 97 B5 1F BE 20 8A 38 0A 7C D9 10 AC 53 FD 4C E9 64 64 45 33 D1 3E 9F F9 43 B2 95 06 03 6F D6 10 1F 9F 77 69 A5 21 61 DF 31 90 07 40 5E C4 8A 31 12 23 44 21 76 DB F5 96 A1 F3 F0 87 20 B0 51 7A CD CF D2 D3

附 录 D
（资料性附录）
测试发卡行对称密钥

表 D.1 测试发卡行公私钥对

名称	长度	值
应用密文主密钥	16 字节	F0 C3 4A 81 24 CE E0 A9 1A 0B 03 4A A9 7D 6E AC
安全报文认证(MAC)主密钥	16 字节	12 B1 AC 4A F0 70 CC 35 61 2B FE 2D 30 AB 60 0D
安全报文加密主密钥	16 字节	D3 0F 45 EA BC 12 AC 3E F5 6B 0C 0D 7F 86 54 DE

附 录 E
（资料性附录）
PBOC 借记/贷记 IC 卡个人化功能实现一致性声明

表 E.1 一致性声明

机构名称		
机构代码		
联系人或填表人		
地址		
电话		
传真		
Email		
发卡机构期望启用的卡片应用	□接触式 IC	□借记/贷记 □基于借记贷记应用的小额支付--□双币
	□非接触式 IC	□借记/贷记 □快速借记/贷记（qPBOC） -----□双币 □非接触式小额支付扩展--- □押金抵扣 □增强型小额支付
	□磁条	----
卡片使用地域	□仅在国内使用 □开通境外交易	
发卡机构期望卡片启用的对称算法	□总是 DES/3DES □总是 SM4 □根据 DF69 在 DES/3DES 与 SM4 间自动切换	
发卡机构期望卡片启用的非对称算法	□总是 RSA □总是 SM2 □根据 DF69 在 RSA 与 SM2 间自动切换	
发卡机构期望卡片启用的哈希算法	□总是 SHA-1 □总是 SM3 □根据 DF69 在 SHA-1 与 SM3 间自动切换	
BIN 号		
个人化模板 X 编号		
个人化模板 Y 编号		
应用标识符（AID）	□A000000333010101(借记) □A000000333010102(贷记) □A000000333010103(准贷记) □A000000333010106(纯电子现金) □其他_____	
是否使用银联 TSM 完成个人化	□是 □否	
送检样品信息（仅适用于非银联 TSM 个人化）		
卡片名称		

封装厂商		
COS/APPLET 版权商		
芯片商及型号		
COS 平台	□Java □Multos □Native □其它	
PBOC2.0 或 3.0 检测报告	PBOC2.0 或 3.0 借记/贷记（支持小额支付）IC 卡检测报告	编号
	非接触式 IC 支付卡检测报告	编号
	基于非接触小额支付扩展应用卡检测报告	编号
送检数据信息（仅适用于银联 TSM 个人化）		
发卡机构期望数据被装入哪个（些）卡商的 SIM 卡上进行测试	A B C D	
1.公共部分		
1.1 接触式应用选择		
应用优先指示器 87		
交易日志入口 9F4D		
交易日志格式 9F4F		
圈存日志入口 DF4D		
圈存日志格式 DF4F		
应用标签 50		
应用首选名称 9F12		
发卡行代码表索引 9F11		
首选语言 5F2D		
处理选项数据对象列表（PDOL）9F38		
1.2 非接触式应用选择		
应用优先指示器 87		
交易日志入口 9F4D		
交易日志格式 9F4F		
圈存日志入口 DF4D		
圈存日志格式 DF4F		
处理选项数据对象列表（PDOL）9F38		
增值功能指示器 DF61		
1.3 应用密钥		
ARQC KEY(明文主密钥-DES)		
安全报文 MAC KEY(明文主密钥-DES)		
PIN 加密 KEY(明文主密钥-DES)		
ARQC KEY(明文主密钥-SM4)		
安全报文 MAC KEY(明文主密钥-SM4)		

PIN 加密 KEY(明文主密钥-SM4)	
1.4 其他值	
脱机 PIN	
脱机 PIN 最大重试次数	
2. 借记/贷记部分	
2.1 借记/贷记 模板缺省数据	
发卡行行为代码（IAC）-拒绝 9F0E	
发卡行行为代码（IAC）-联机 9F0F	
发卡行行为代码（IAC）-缺省 9F0D	
应用交互特征（AIP）82	
持卡人验证方法列表 8E	☐我机构已知银联启用脱机 PIN 的建议，但我机构暂不启用。
当终端要求输入联机 PIN 时	☐我机构期望 PIN 未被输入的交易被受理终端直接拒绝。 ☐我机构期望 PIN 未被输入的交易联机完成。 ☐其他，测试时遇到问题请通知我。
应用用途控制（AUC）9F07	
应用版本号 9F08	
应用缺省行为（ADA）9F52	
卡片风险管理数据对象列表 1（CDOL1） 8C	
卡片风险管理数据对象列表 2（CDOL2） 8D	
2.2 借记/贷记 发卡行通用数据	
卡产品标识信息 9F63	
发卡行认证指示位 9F56	
连续脱机交易限制数（国际-货币）9F53	
累计脱机交易金额限制数 9F54	
累积脱机交易金额上限 9F5C	
连续脱机交易下限 9F58	
连续脱机交易上限 9F59	
连续脱机交易下限 9F14	
连续脱机交易上限 9F23	
连续脱机交易限制数（国际-国家）9F72	
累计脱机交易金额限制数（双货币）9F75	
发卡行应用数据 9F10	
发卡行国家代码 5F28	
发卡行国家代码 9F57	
应用货币代码 9F51	
应用货币代码 9F42	
应用生效日期 5F25	
CA 公钥索引（PKI）8F（RSA）	
发卡行公钥证书 90（RSA）	
发卡行公钥余数 92（RSA）	
发卡行公钥指数 9F32（RSA）	

CA 公钥索引（PKI）8F（SM2）	
发卡行公钥证书 90（SM2）	
动态数据认证数据对象列表（DDOL）9F49	
2.3 借记/贷记 卡或持卡人特殊数据	
应用主账号 5A	
应用主账号序列号 5F34	
持卡人姓名 5F20	
持卡人姓名扩展 9F0B	
持卡人证件号 9F61	
持卡人证件类型 9F62	
应用失效日期 5F24	
服务码 5F30	
磁条 1 自定义数据 9F1F	
磁条 2 等效数据 57	
签名的静态应用数据 93（RSA）	
签名的静态应用数据 93（SM2+SM3）	
静态数据认证标签列表 9F4A	82
数据认证码 9F45（RSA）	
IC 卡公钥证书 9F46（RSA）	
IC 卡公钥指数 9F47（RSA）	
IC 卡公钥余数 9F48（RSA）	
数据认证码 9F45（SM2）	
IC 卡公钥证书 9F46（SM2）	
3.基于借记贷记应用的小额支付部分	
3.1 基于借记贷记应用的小额支付 模板缺省数据	
发卡行行为代码（IAC）-拒绝 9F0E	
发卡行行为代码（IAC）-联机 9F0F	
发卡行行为代码（IAC）-缺省 9F0D	
应用交互特征（AIP）82	
持卡人验证方法列表 8E	
应用用途控制（AUC）9F07	
应用版本号 9F08	
应用缺省行为（ADA）9F52	
卡片风险管理数据对象列表 1（CDOL1） 8C	
卡片风险管理数据对象列表 2（CDOL2） 8D	
电子现金发卡行授权码 9F74	ECC001
3.2 基于借记贷记应用的小额支付 发卡行通用数据	
卡产品标识信息 9F63	
发卡行认证指示位 9F56	
连续脱机交易限制数（国际-货币）9F53	
累计脱机交易金额限制数 9F54	
累积脱机交易金额上限 9F5C	

连续脱机交易下限 9F58	
连续脱机交易上限 9F59	
连续脱机交易下限 9F14	
连续脱机交易上限 9F23	
连续脱机交易限制数（国际-国家）9F72	
累计脱机交易金额限制数（双货币）9F75	
发卡行应用数据 9F10	
发卡行国家代码 5F28	
发卡行国家代码 9F57	
应用货币代码 9F51	
应用货币代码 9F42	
应用生效日期 5F25	
CA 公钥索引（PKI）8F（RSA）	
发卡行公钥证书 90（RSA）	
发卡行公钥余数 92（RSA）	
发卡行公钥指数 9F32（RSA）	
CA 公钥索引（PKI）8F（SM2）	
发卡行公钥证书 90（SM2）	
动态数据认证数据对象列表（DDOL）9F49	
3.3 基于借记贷记应用的小额支付 卡或持卡人特殊数据	
应用主账号 5A	
应用主账号序列号 5F34	
持卡人姓名 5F20	
持卡人姓名扩展 9F0B	
持卡人证件号 9F61	
持卡人证件类型 9F62	
应用失效日期 5F24	
服务码 5F30	
磁条 1 自定义数据 9F1F	
磁条 2 等效数据 57	
签名的静态应用数据 93（RSA）	
签名的静态应用数据 93（SM2+SM3）	
静态数据认证标签列表 9F4A	82
数据认证码 9F45（RSA）	
IC 卡公钥证书 9F46（RSA）	
IC 卡公钥指数 9F47（RSA）	
IC 卡公钥余数 9F48（RSA）	
数据认证码 9F45（SM2）	
IC 卡公钥证书 9F46（SM2）	
电子现金余额上限 9F77	
电子现金单笔交易限额 9F78	
电子现金重置阈值 9F6D	

3.4 双币特有数据	
第二币种电子现金应用货币代码 DF71	
第二币种电子现金余额上限 DF77	
第二币种电子现金单笔交易限额 DF78	
第二币种电子现金重置阈值 DF76	
第二币种卡片 CVM 限额 DF72	
4.快速借记/贷记（qPBOC）部分	
4.1 快速借记/贷记（qPBOC）模板缺省数据	
应用交互特征（AIP）82	
卡片附加处理 9F68	
卡片交易属性 9F6C	
电子现金发卡行授权码 9F74	ECC001
卡片认证相关数据 9F69	01 xx xx xx xx yy yy zz
4.2 快速借记/贷记（qPBOC）发卡行通用数据	
卡产品标识信息 9F63	
发卡行应用数据 9F10	
CA 公钥索引（PKI）8F（RSA）	
发卡行公钥证书 90（RSA）	
发卡行公钥余数 92（RSA）	
发卡行公钥指数 9F32（RSA）	
CA 公钥索引（PKI）8F（SM2）	
发卡行公钥证书 90（SM2）	
4.3 快速借记/贷记（qPBOC）卡或持卡人特殊数据	
卡片持卡人验证方法限额 9F6B	
签名的静态应用数据 93（RSA）	
签名的静态应用数据 93（SM2+SM3）	
静态数据认证标签列表 9F4A	82
数据认证码 9F45（RSA）	
IC 卡公钥证书 9F46（RSA）	
IC 卡公钥指数 9F47（RSA）	
IC 卡公钥余数 9F48（RSA）	
数据认证码 9F45（SM2）	
IC 卡公钥证书 9F46（SM2）	
5.非接触式小额支付扩展部分	
分段扣费押金抵扣限额 DF62	
发卡机构期望使用的扩展应用变长文件 SFI	□0x15 普通地铁 □0x19 铁路(高铁) □0x16 普通公交 □0x1A 普通公交日月票 □0x17 高速公路不停车收费 □0x1B 普通地铁日月票 □0x18 停车收费咪表
发卡机构期望使用的扩展应用循环文件 SFI	□0x1E
变长文件 应用开通主密钥	
变长文件 文件最大长度	

0x15	初始行业应用记录数据	
	初始行业应用 MAC 密钥	
变长文件 0x16	应用开通主密钥	
	文件最大长度	
	初始行业应用记录数据	
	初始行业应用 MAC 密钥	
变长文件 0x17	应用开通主密钥	
	文件最大长度	
	初始行业应用记录数据	
	初始行业应用 MAC 密钥	
变长文件 0x18	应用开通主密钥	
	文件最大长度	
	初始行业应用记录数据	
	初始行业应用 MAC 密钥	
变长文件 0x19	应用开通主密钥	
	文件最大长度	
	初始行业应用记录数据	
	初始行业应用 MAC 密钥	
变长文件 0x1A	应用开通主密钥	
	文件最大长度	
	初始行业应用记录数据	
	初始行业应用 MAC 密钥	
变长文件 0x1B	应用开通主密钥	
	文件最大长度	
	初始行业应用记录数据	
	初始行业应用 MAC 密钥	
循环文件 0x1E	应用开通主密钥	
	文件最大长度	
	初始行业应用记录数据	
	初始行业应用 MAC 密钥	
	初始行业应用最大记录条数	
1) 所有信息都应填写，可适当注解。		
我机构申请上述特性的 PBOC 借贷记卡业务数据个人化验证测试。 签章：　　日期：		