ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0025.12—2018
代替 JR/T 0025.12—2013

中国金融集成电路（IC）卡规范 第12部分：非接触式IC卡支付规范

China financial integrated circuit card specifications—
Part 12: Contactless integrated circuit card payment specification

2018-11-28 发布　　2018-11-28 实施

中国人民银行　发布

目　　次

前　言

JR/T 0025—2018《中国金融集成电路（IC）卡规范》分为14部分：

——第1部分：总则；

——第3部分：与应用无关的IC卡与终端接口规范；

——第4部分：借记/贷记应用规范；

——第5部分：借记/贷记应用卡片规范；

——第6部分：借记/贷记应用终端规范；

——第7部分：借记/贷记应用安全规范；

——第8部分：与应用无关的非接触式规范；

——第10部分：借记/贷记应用个人化指南；

——第12部分：非接触式IC卡支付规范；

——第13部分：基于借记/贷记应用的小额支付规范；

——第14部分：非接触式IC卡小额支付扩展应用规范；

——第15部分：电子现金双币支付应用规范；

——第16部分：IC卡互联网终端规范；

——第18部分：基于安全芯片的线上支付技术规范。

本部分为JR/T 0025—2018的第12部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0025.12—2013《中国金融集成电路（IC）卡规范　第12部分：非接触式IC卡支付规范》，与JR/T 0025.12—2013相比主要技术变化如下：

——增加了CDCVM、ODA和PAR等缩略语的定义（见4）；

——修改了9F66保留位，新增定义终端支持ODA和终端支持CDCVM指示位（见6.4.4，2013年版6.4.4）；

——增加了终端对卡片响应码6986的处理要求（见6.5.3）；

——删除了“交易时间”的概念，修改并明确500ms为“交互时间”的要求（见6.6，2013年版6.6）；

——在GPO响应数据中增加了PAR和CID(9F27),在GPO联机响应数据中可选增加了AFL(见7.4.2)；

——修改了脱机批准交易的GPO响应必备和条件数据表，合并纳入联机ODA、联机（无ODA）或拒绝的要求（见7.4.2，2013年版7.4.2和7.4.4）；

——在签名推荐数据中增加了可选数据元PAR（见7.4.5）；

——修改了9F68的保留位定义，新增卡片支持联机ODA的控制位（见7.7，2013年版的7.7）；

——删除了与“小额或CTTA”及“预付”相关的内容（见2013年版的7.7、7.7.5、7.7.6、7.7.7、7.7.8、7.7.13和7.7.16）；

——增加了关于联机ODA的生成流程（见7.7.16）；

——修改了卡的风险管理过程及终端处理要求（见7.7和7.8，2013年版7.7和7.8）；

——增加了终端对TVR的置位要求（见7.8.1）；

——增加了允许应用过期的联机处理（见7.8.3.1）；

——增加了持卡人身份认证描述，增加了终端执行CDCVM方法的判断流程（见7.8.5）；

——修改了终端联机处理时决定执行 CVM 的方法（见 7.8.8）；

——修改了 qPBOC 流程下交易仅联机的实现方法（见 7.9.2，2013 年版的 7.9.1）；

——增加了对非接消费交易流程的描述（见 7.11）；

——增加了联机 ODA 的描述，定义联机 ODA 的签名格式要求（见 B.2）；

——增加了密文信息数据 9F27（见附录 C）；

——在数据元列表中增加了数据元表列“共享性”，说明该数据元是否也在标准借记/贷记流程中使用，删除了原表列“备份”，增加“获取”列，说明该数据元是否可被读取以及读取命令（见附录 C，2013 年版附录 C）；

——在数据元列表中增加了用户专用数据 9F7C 和主账号参考号 9F24 的定义，增加了 9F68、9F6C、9F79、9F77、9F6D 和 9F78 的修改要求，增加了 DF61 的定义（见附录 C）；

——在数据元列表的卡片交易属性 9F6C 中增加了 CDCVM 相关位的定义（见附录 C）；

——在发卡行任意数据 IDD 中增加了 0x06，0x07 的定义（见附录 D）；

——增加了电子现金闪卡处理机制（见附录 F）；

——增加了联机 ODA 技术实施指南（见附录 G）。

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/TC 180）归口。

本部分起草单位：中国人民银行、中国人民银行广州分行、中国人民银行成都分行、中国人民银行杭州中心支行、中国人民银行宁波市中心支行、中国工商银行、中国银行、中国建设银行、中国农业银行、交通银行、中国邮政储蓄银行、上海浦东发展银行、中国银联股份有限公司、中国金融电子化公司、中金金融认证中心有限公司、银行卡检测中心、北京中金国盛认证有限公司、中钞智能卡研究院、中钞信用卡产业发展有限公司、捷德（中国）信息科技有限公司、惠尔丰（中国）信息系统有限公司、福建联迪商用设备有限公司、东信和平科技股份有限公司。

本部分主要起草人：李伟、王永红、李晓枫、陆书春、潘润红、李兴锋、宋汉石、渠韶光、邵阔义、杨倩、聂丽琴、杜宁、周玥、张宏基、程胜、汤沁莹、黄本涛、陈卫东、王岚、沈州、张文元、李承康、刘贵辉、吕扬建、徐文伟、陈则栋、吴晓光、李春欢、洪隽、张栋、王红剑、胡吉晶、吴潇、范抒、魏猛、刘志刚、张永峰、余沁、尚可、李新、李一凡、俞益宁、周新衡、雷斌、邓少峰、张步、冯珂、李建峰、向前、涂晓军、林发全、陈文博、石文鹏、齐大鹏、陈震宇、郑元龙、聂舒、丁吉、白雪晶、李子达、沈卓群、刘世英、于海涛、翁秀诚、张萌、黎志勇、张国栋、俞益宁、曾静静、李铭铭、吴宝民、郭晶莹、章盼、张波波、汪小八、拱慧璇、柳姣娜、汤中泽、骆永刚、范琳琳。

本部分代替了JR/T 0025.12—2013。

JR/T 0025.12—2013的历次版本发布情况为：

JR/T 0025.12—2010。

引　言

本部分为JR/T 0025—2018的第12部分，与JR/T 0025.8—2018一起构成非接触式应用。

本部分主要定义了基于非接触式接口的金融支付应用。有关物理特性、射频功率和信号接口，以及初始化、冲突检测和传输协议的要求不在本部分范围之内。相关的要求在JR/T 0025.8—2018中描述。

中国金融集成电路（IC）卡规范
第12部分：非接触式IC卡支付规范

1 范围

本部分规定了非接触式IC卡应用，在非接触式快速借记/贷记应用（qPBOC）方面作出了相关要求和规定。

本部分适用于由银行发行或受理的金融非接触式IC卡。使用对象主要是与金融非接触式IC卡应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等相关部门（单位）。

2 规范性引用文件

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

JR/T 0025.12—2010 中国金融集成电路（IC）卡规范 第12部分：非接触式IC卡支付规范

JR/T 0025.12—2013 中国金融集成电路（IC）卡规范 第12部分：非接触式IC卡支付规范

JR/T 0025—2018（所有部分） 中国金融集成电路（IC）卡规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

应用文件定位器 application file locator

用于指出应用相关的文件位置和记录范围。

3.2

应用交互特征 application interchange profile

表明卡片所支持的功能。

3.3

卡片 card

具有非接触式支付应用、与支付终端交互的消费者设备。

注：术语“卡片”原意是指具有传统信用卡尺寸的支付卡，但是在本部分中，是指任何可通过非接触式界面操作处理的消费者设备（例如：移动电话或PDA）。

3.4

冲突 collision

在同一时间周期内，在同一PCD的工作场中，有两张或两张以上的PICC进行数据传输，使得PCD不能辨别数据是从哪一张PICC发出的。

3.5

消费者设备 consumer device

消费者用于支付交易的具有芯片能力的设备（例如，移动电话或PDA）。

3.6

发卡行行为代码 issuer action code

发卡行根据TVR的内容选择的动作。

3.7

路径 path

根据终端支持磁条数据模式或快速借记/贷记应用所选择的一个应用路径，卡片行为由所选择的路径唯一确定。

3.8

近距离支付系统环境 proximity payment systems environment

支持的应用标识、应用标签和应用优先指示器的一个列表，可通过非接触界面访问。该列表包括所有目录的入口，由卡片在SELECT PPSE（“2PAY.SYS.DDF01”）响应的FCI中返回。

3.9

读写器 reader

与卡片交互的受理设备。

注：该词未指明具体的实现方式。读写器在非接触式交易中通常两种形式：一种是作为一种与POS设备分离，但与之通信的读写器；一种是集成到POS设备中的读写器。除非有其他的明确说明，本部分中“读写器”一词包括以上两种形式，不会特意指明特定的操作是在哪一个物理模块（读写器或POS设备）中执行的。

3.10

联机ODA online with offline data authentication

包含脱机数据验证的联机交易。即在联机交易中，卡片支持返回签名应用数据，终端通过脱机数据认证判断卡片真伪。

4 缩略语

下列缩略语适用于本文件。

AAC——应用认证密文（Application Authentication Cryptogram）

AAR——应用授权参考（Application Authorization Referral）

AC——应用密文（Application Cryptogram）

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

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）

ARQC——授权请求密文（Authorization Request Cryptogram）

ATC——应用交易计数器（Application Transaction Counter）
ATS——Type A的选择应答（Answer To Select，Type A）
BIN——银行标识号（Bank Identification Number）
CA——认证中心（Certificate Authority）
CDA——复合动态数据认证/应用密文生成（Combined DDA/AC Generation）
CDCVM——基于消费者设备的CVM（Consumer Device CVM）
CDOL——卡片风险管理数据对象列表（Card Risk Management Data Object List）
CID——密文信息数据（Cryptogram Information Data）
CTTA——累计脱机交易总金额（Cumulative Total Transaction Amount）
CTTAL——累计脱机交易总金额限制（Cumulative Total Transaction Amount Limit）
CTTAUL——累计脱机交易总金额上限（Cumulative Total Transaction Amount Upper Limit）
CVM——持卡人验证方法（Cardholder Verification Method）
CVR——卡片验证结果（Card Verification Results）
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）
DES——数据加密标准（Data Encryption Standard）
DF——专用文件（Dedicated File）
DKI——子密钥索引（Derivation Key Index）
EC——电子现金（Electronic Cash）
FCI——文件控制信息（File Control Information）
fDDA——快速动态数据认证（Fast Dynamic Data Authentication）
FWI——帧等待时间整数（Frame Waiting Time）
GPO——获取处理选项（Get Processing Options）
HCE——主卡模拟（Host Card Emulation）
IC——集成电路（Integrated Circuit）
iCVN——替代的卡片验证值（instead Card Verification Number）
IDD——发卡行自定义数据（Issuer Defined Data）
MAC——报文鉴别码（Message Authentication Code）
MBLI——最大缓冲区长度索引（Maximum Buffer Length Index）
ODA——脱机数据认证（Offline Data Authentication）
PAN——主账号（Primary Account Number）
PAR——主账号参考号（Payment Account Reference）
PCD——接近式耦合设备（读写器）（Proximity Coupling Device）
PDA——个人数字助理（Personal Digital Assistant）
PDOL——处理选项数据对象列表（Processing Options Data Object List）
PICC——接近式集成电路卡（Proximity Integrated Circuit Card）
PIN——个人识别码（Personal Identification Number）
POS——销售点（Point Of Sale）
PPSE——近距离支付系统环境（Proximity Payment Systems Environment）
PSE——支付系统环境（Payment System Environment）
qPBOC——快速借记/贷记应用（quick PBOC）
RFU——预留（Reserved for Future Use）
RSA——一种非对称密钥算法，以三位提出者名字的首字母命名（Rivest、Sharmir、Adleman）
SDA——静态数据认证（Static Data Authentication）

SDAD——签名的动态应用数据（Signed Dynamic Application Data）
SFI——短文件标识符（Short File Identifier）
TC——交易证书（Transaction Certificate）
TLV——标签、长度、值（Tag Length Value）
TTQ——终端交易属性（Terminal Transaction Qualifiers）
TVR——终端验证结果（Terminal Verification Results）
TMS——终端管理系统（Terminal Management System）
UDK——子密钥（Unique DEA Key）

5 非接触实现方法概述

5.1 非接触式支付方式

5.1.1 概述

本条描述了两种基于非接触式界面的支付方式：
——非接触式快速借记/贷记应用（qPBOC）方式；
——非接触式标准借记/贷记应用方式。
qPBOC与借记/贷记应用的区别参见附录A。

5.1.2 非接触式快速借记/贷记应用

为了满足引入了非接触式接口而产生交易速度上的要求，需要对标准的借记/贷记应用流程进行调整和优化。qPBOC对标准的借记/贷记指令和交易流程进行了优化，体现在：
——把多条借记/贷记应用命令压缩成尽可能少的命令，以减少交易的时间；
——将卡片和终端的交互过程集中完成，当卡片离开终端的感应范围后，终端再进行脱机数据认证、终端风险管理和终端行为分析，并允许卡片离开终端的感应范围之前或之后进行密码操作，使卡片在终端感应范围停留的时间尽可能短。

5.1.3 非接触式标准借记/贷记应用

非接触式借记/贷记应用方式的处理流程与接触式借记/贷记应用处理流程完全一致，仅通讯方式不同。

5.2 非接触式标准借记/贷记与 qPBOC 的互用性

非接触应用要求终端和卡片应支持qPBOC。终端和卡片也可支持非接触式借记/贷记应用。

如果终端支持非接触式借记/贷记应用，并且终端支持的方式（置于卡盘上或插入卡槽中）能够使卡片在整个非接触式借记/贷记应用交易过程中一直处于感应区内，那么终端可向卡片表明支持非接触式借记/贷记应用。

表1描述了非接触式卡片和终端的适用范围。

表1 卡片和终端的适用范围

终端配置	非接触卡片性能	
	qPBOC	qPBOC 和非接触式借记/贷记应用
仅支持 qPBOC	qPBOC	qPBOC
支持 qPBOC 和非接触式借记/贷记应用	qPBOC	非接触式借记/贷记应用
非接触式借记/贷记应用	—	非接触式借记/贷记应用

用于DDA的IC卡公钥证书包括卡片静态数据的哈希值。qPBOC和借记/贷记应用宜采用相同的静态数据。如果签名的借记/贷记静态数据不同于签名的qPBOC静态数据，则应支持两个卡片公钥证书，这将增加实现的复杂度。

终端应读取IC卡公钥证书中包括所有静态数据元，以便完成DDA。在静态数据共享情况下，发卡行应权衡在借记/贷记静态数据元中包含特殊数据项与由此增加qPBOC交易的交互时间两者之间的得失。

qPBOC推荐签名数据见7.4.5。

5.3 总体处理概述

如果终端支持 qPBOC，在提示持卡人出示卡片和终端被激活之前，应进行预交易处理。终端检测到非接触卡片之后，尝试读取 PPSE。如果卡片是符合本部分的非接触卡片，终端则向卡片表明其可支持的非接触的种类（应支持 qPBOC 或非接触式借记/贷记应用），由卡片决定进入哪种非接触式路径。卡片应支持 qPBOC 路径，可附加选择支持非接触式借记/贷记应用路径。qPBOC 路径：利用定义在 JR/T 0025.5—2018 中的命令、功能和风险管理特征，但本部分如果对原定义有增补或修订，以本部分为准。

非接触式借记/贷记应用路径：符合 JR/T 0025.5—2018。

对于含有接触界面的双界面卡，非接触式借记/贷记应用是可选的。对于仅非接触式卡片，脚本处理（如充值交易的脚本处理）应通过非接触式借记/贷记应用路径来执行。对于此类情况，终端交易属性应指明支持非接触式借记/贷记应用。

具体见JR/T 0025.5—2018中第17章。

图1给出了卡片确定路径和交易处理的总体示意图。

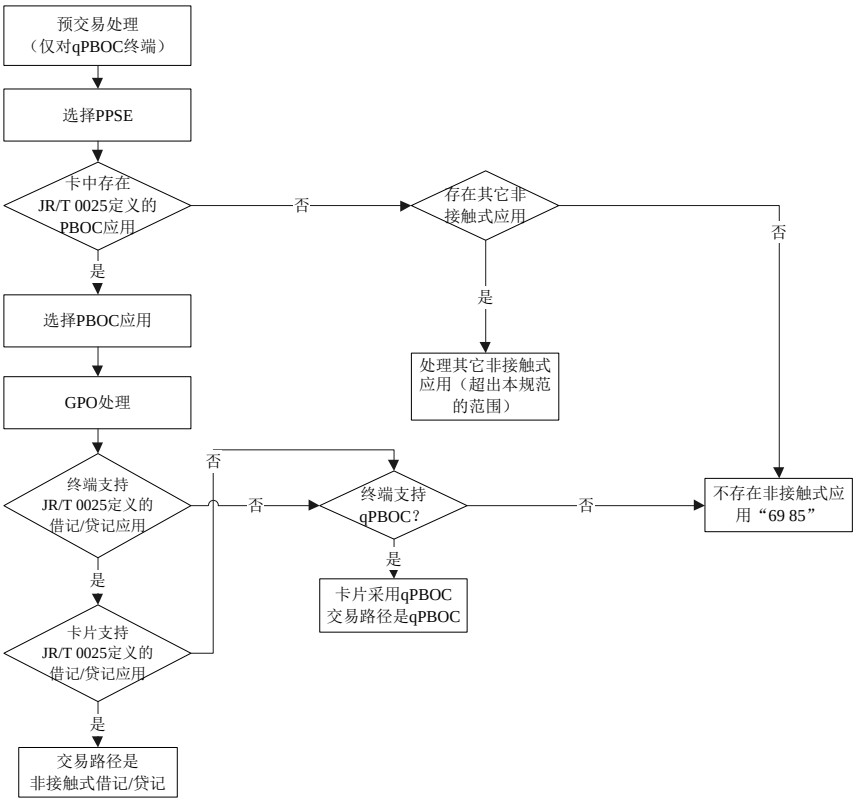


图1 总体处理流程

SM算法应用于qPBOC流程见图2。

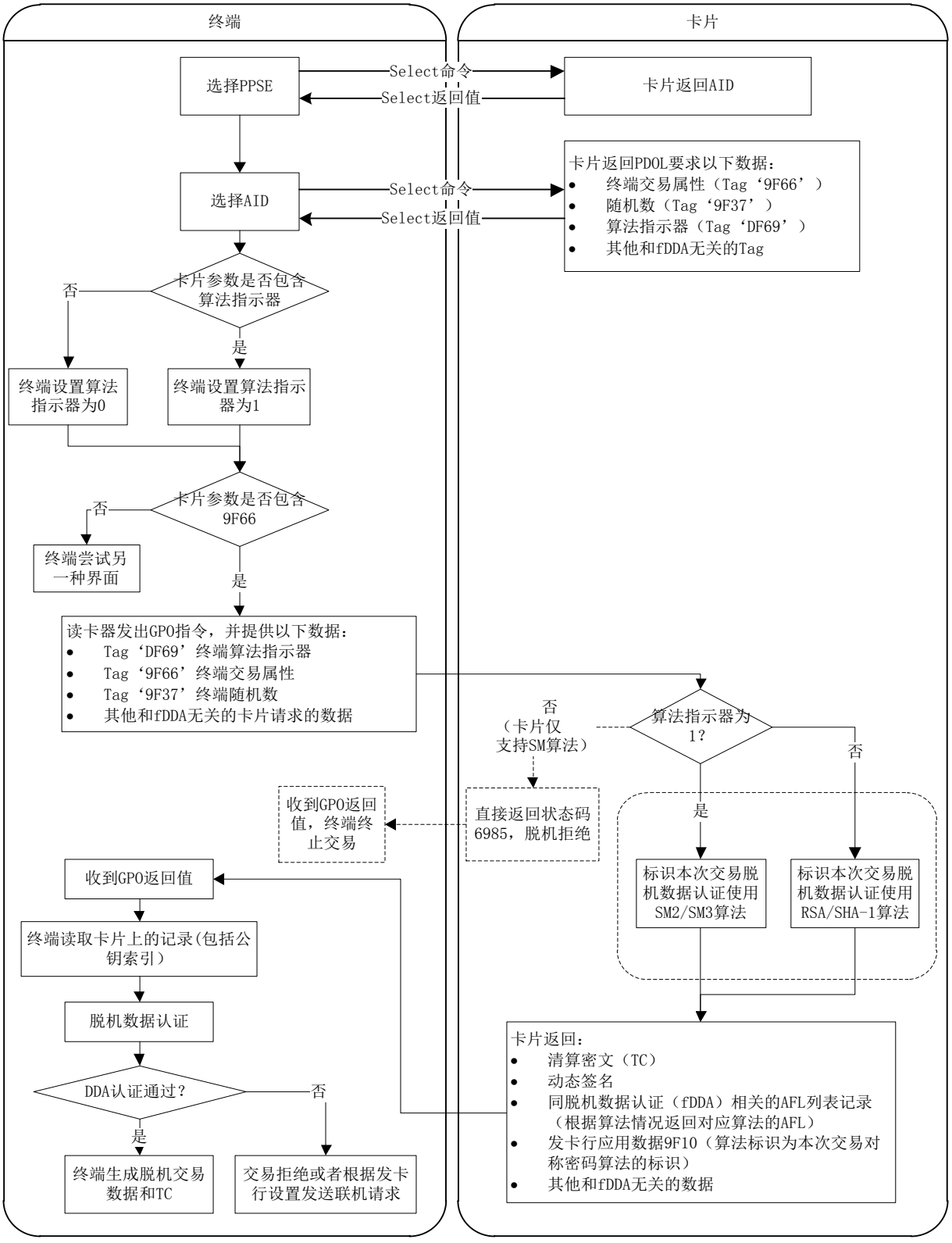


图2　SM 算法应用于 qPBOC 流程

6　非接触支付应用的通用要求

6.1　终端、卡片及收单行要求

6.1.1 概述

对qPBOC的特殊要求在第7章中定义。本条讨论所有非接触式应用应满足的要求。

qPBOC基于JR/T 0025.5—2018和JR/T 0025.6—2018，本条指出其与借记/贷记卡片应用的不同之处，并在附录A中详细描述。

6.1.2 Level1 终端要求

Level1终端要求如下：

——终端应符合 JR/T 0025.8—2018，并同时支持 Type A 和 Type B；

——对于 Type B 卡，终端应支持 MBLI=0 和 MBLI=1；

——对于 Type A 卡，终端应支持值为 8 的 FWI 和附加的值为 x“B”的 ATS – TB （1）。

6.1.3 通用终端要求

通用终端要求如下：

——终端应支持 qPBOC 和非接触式借记/贷记应用之一，或同时支持两者；

——具有脱机能力的终端应同时支持 SDA 和 DDA。如果卡片支持 DDA，则终端应执行 DDA；

——终端应支持 JR/T 0025.4—2018 中 5.3 定义的数据对象列表；

——终端应通知收单行交易是通过非接触界面完成的信息，该信息应区别是非接触式借记/贷记交易还是 qPBOC 交易，并且应包含在授权和清算报文中；

注：终端如何表示上述信息依赖于终端与收单行之间的报文格式，本部分未对该格式进行定义。收单行可正确的填写联机报文中的必备项（POS输入点方式域）来提供信息。

——如果卡片返回拒绝应用认证密文（AAC）来拒绝交易，交易不应再通过其他界面方式进行；

——当进行接触式或磁条刷卡的交易初始化时，终端应下电关闭非接触式界面；

——当进行接触式或磁条刷卡的交易初始化时，如果非接触式交易正在进行，终端应终止非接触式交易，放弃从卡片得到的所有数据，然后重新启动其他界面进行交易；

——对于非接触交易，终端应明确通知持卡人和商户出卡、交易过程及交易结果（批准、拒绝或终止）。终端信息宜包含：

- 出卡；
- 读卡成功；
- 处理中；
- 再次出卡（如果交易未完成）；
- 交易批准；
- 交易拒绝；
- 出示单一卡片（防冲突）；
- 插入或刷卡。

当提示出卡时，终端应显示授权交易金额（标签“9F02”）。如果卡片提供可用的脱机交易金额时，终端应显示该金额，以表示读卡操作成功，并可打印在交易凭条上。

6.1.4 通用终端选项

终端可按照JR/T 0025.6—2018的要求，支持读卡、显示或打印交易明细。

6.1.5 通用的卡片要求

通用的卡片要求如下：

——卡片应支持 qPBOC；

——仅含有非接触式界面的卡片应同时支持 qPBOC 和非接触式借记/贷记应用；

——卡片应符合 JR/T 0025.8—2018，至少支持 Type A 或 Type B 中的一种；
——如果接触式界面被激活，卡片不应响应非接触式界面；
——磁道 2 等价数据对于 qPBOC 是必备的；
——具有脱机能力的 qPBOC 卡片应支持 fDDA；
——为了用目前的芯片满足时间要求，卡片宜以中国余数定理模式存放与使用 RSA 私钥。

6.1.6 通用卡片选项

卡片可选支持非接触界面借记/贷记应用。

卡片应支持记录交易日志的功能，该功能可在个人化时通过卡片附加处理开启或关闭（详见表12），交易日志的定义见JR/T 0025.5—2018第18章。

是否启用交易日志功能由发卡机构决定。

6.1.7 卡片验证值要求

除了非接触风险管理特征外，当不使用dCVN时，qPBOC宜采用iCVN。发卡行应对芯片卡中的磁道数据用iCVN进行编码。iCVN用于防止复制芯片数据，并基于芯片数据制作空白塑料磁条卡。在非接触交易采用iCVN具有同样的用途。

6.1.8 收单行要求

收单行应在给发卡行授权报文中表明交易是非接触的。域22（POS输入方式）用于标识交易采用非接触式界面。

6.2 激活非接触界面（支持 qPBOC 的终端）前的处理要求

6.2.1 预处理前的处理要求

为了使卡片保持在感应区的时间最小化，具有qPBOC能力的终端使用非接触界面，直到qPBOC交易预处理完成后才可上电。

6.2.2 具有 qPBOC 能力终端的交易预处理

除非交易预处理已经完成，否则支持qPBOC设备的非接触界面不能上电。在某些应用场景下，为更进一步提高交易速度，可不执行交易预处理。通常为消费金额固定的终端，即消费金额已预先存储在终端中，而无需在交易过程中通过人机交互输入。例如自动贩卖机、景区门票销售机等。不进行交易预处理的终端可对非接触界面立即上电。在下面的例子中，全部或部分检查可省去：

——自动售货机可能不支持任何的检查；
——仅支持脱机的终端可能不需要联机应用密文，但可获得授权金额（标签“9F02”），并检查是否超过最低限额；
——支持状态检查的售货机可能不支持非接触方式。

终端采用终端交易属性（标签“9F66”）表示其非接触能力和交易对卡片的要求。终端交易属性由卡片在SELECT命令响应中提出申请，终端通过GPO命令提供。详细内容见6.4.4关于终端交易属性的部分。如果以下检查被执行，则应按照如下要求进行：

——终端应获取授权金额（标签“9F02”）；
——如果终端配置为支持状态检查，并且授权金额为一个货币单位（这是状态检查要求的），则终端用终端交易属性字节 2 中的第 8 位表示需要联机应用密文。支持状态检查应是一可配置的选项，在实施时应打开才能操作。这种检查的缺省行为为关闭；
——如果授权金额为零，除非终端支持 qPBOC 扩展应用，具有联机能力的终端应在终端交易属性字节 2 的第 8 位表示要求联机应用密文；

——如果授权金额为零，除非终端支持 qPBOC 扩展应用，仅支持脱机的终端应终止交易，提示持卡人使用另一种界面（如果存在）；

——如果授权金额大于或等于终端非接触交易限额（如果存在），则终端应终止交易，并提示持卡人采用另一种界面方式；

——如果授权金额大于或等于终端执行 CVM 限额（如果存在），则终端应在终端交易属性中表示要求 CVM（第 2 字节第 7 位）以及支持的 CVM 种类。

与这些指示器对应的卡片行为的详细描述见 7.7.4 ；

——如果授权金额（标签“9F02”）大于非接触终端脱机最低限额或（如果非接触终端脱机最低限额不存在）可用的终端最低限额（标签“9F1B”），则终端应在终端交易属性第 2 字节第 8 位表示需要联机应用密文；

——在预交易处理成功完成后，终端应要求出卡，并对非接触界面上电，开始检测处理。

上述处理描述（假定支持所有的检查）如图3所示。

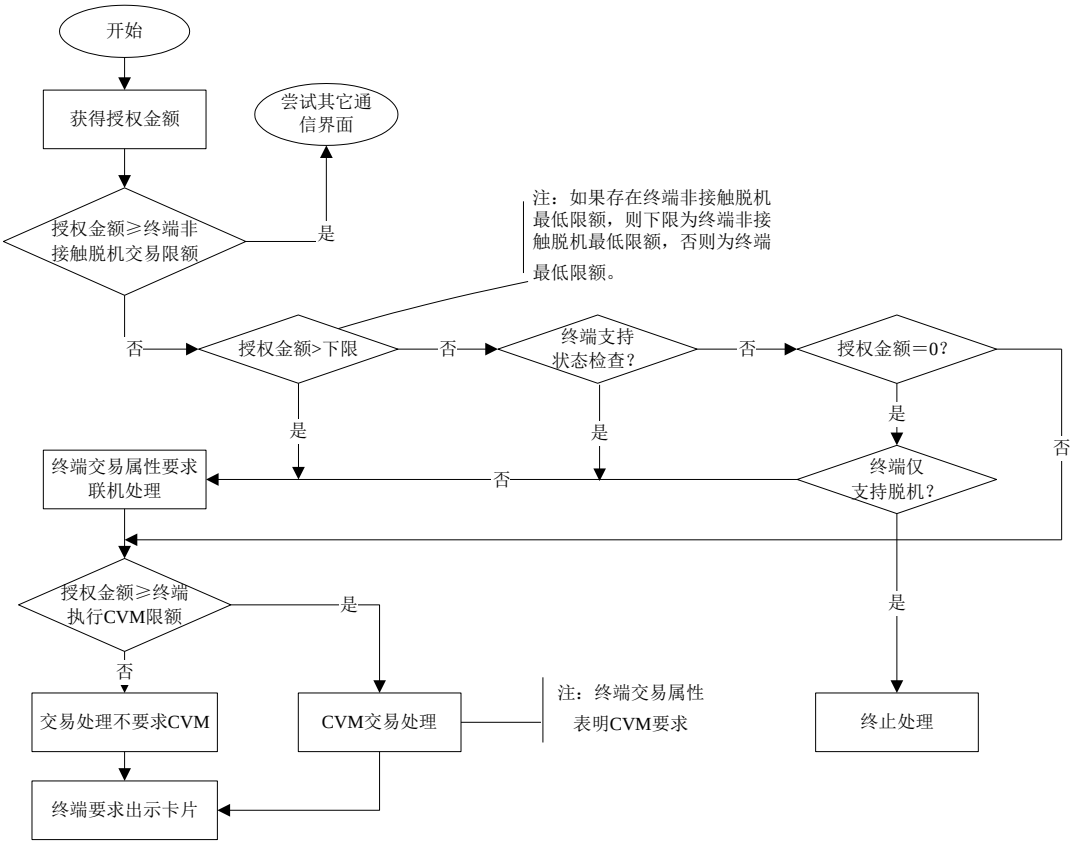


图3　具有 qPBOC 能力终端的预交易处理

6.3　卡片检测处理要求

当非接触式卡进入终端的感应范围，终端与卡片进行通信的初始化（qPBOC终端应按照6.2.2的描述，在初始化交易前执行qPBOC预处理）。

终端可按照商户的命令或预定义超时之后，通过停止检测处理和关闭非接触界面来终止交易。

如果在应用选择前，同时检测到多个非接触卡，则终端应将此情况向持卡人显示，并且要求只放置一张卡。

卡片检测处理和应用选择包含在图4中。

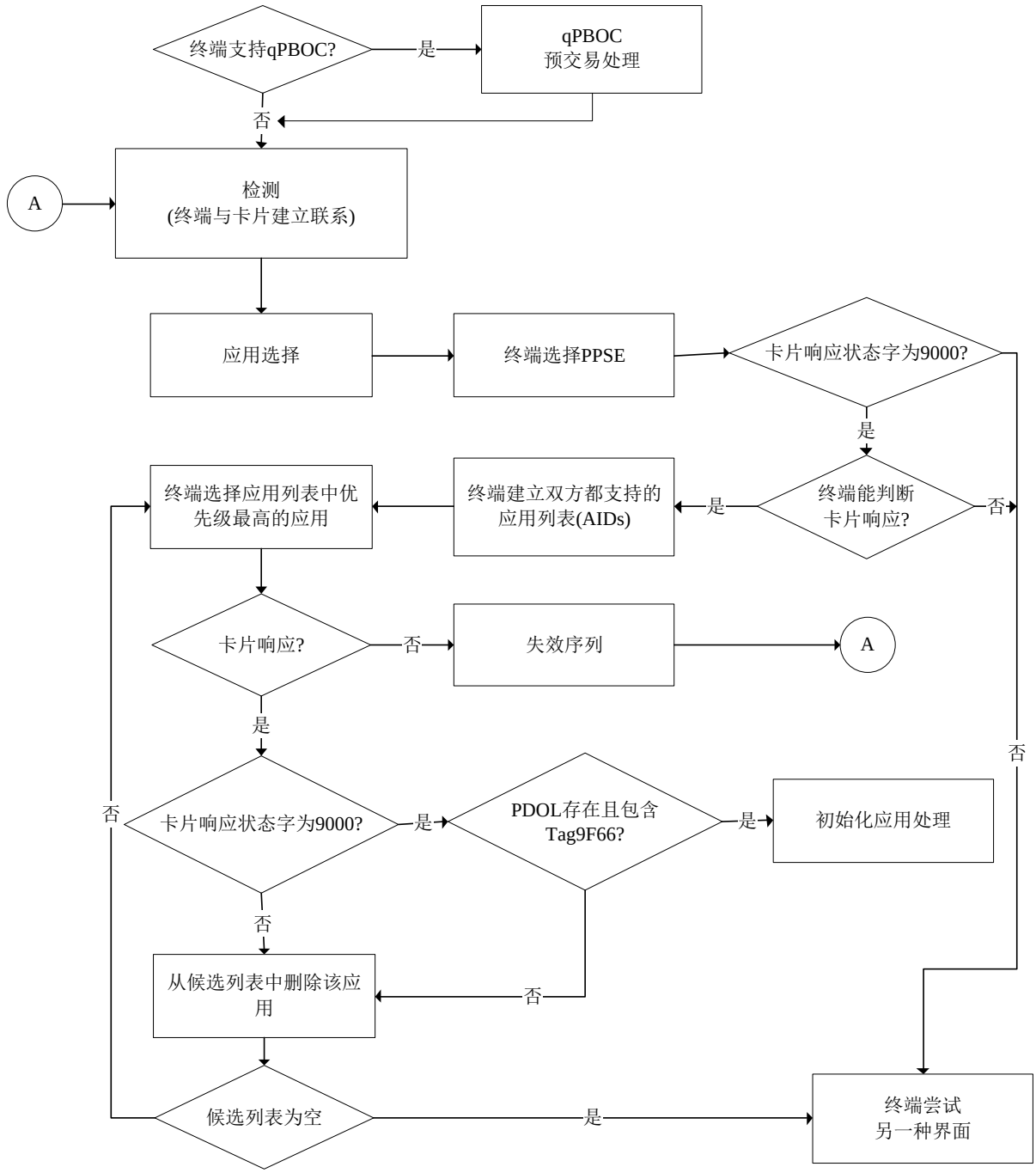


图4　卡片检测和应用选择流程

6.4　应用选择要求

6.4.1　终端应用选择要求

本条描述了终端从具有多个非接触应用的列表中进行选择的行为。为满足时间要求，在 FCI 中尽可能只列出一个应用。如果要求一个以上的应用，应用的数量要尽可能少。终端应用选择要求具体如下：

——所有非接触终端应使用 PPSE 目录选择方法；

——终端采用文件名称“2PAY.SYS.DDF01”来选择 PPSE；

——终端应支持最大长度为 16 字节的 DF 文件名（AID）；

——终端访问卡片应用中的路径应采用一个借记/贷记的 AID。路径不能被直接访问；
——终端应建立包含在FCI中，并且终端支持的应用列表。终端应判断应用优先指示器的bits 4—1（表示应用被选择的顺序），并选择优先级最高的应用来处理交易；
——如果只有一个应用包含在 FCI 中，并被终端支持，则终端应选择该应用，而不考虑可能出现的应用优先级指示器的设置；
——如果卡片对 SELECT 命令的响应状态字不是“9000”，或终端在 PPSE 存在错误格式的情况下，不能从 FCI 中取得 AID，则终端应关闭非接触界面，并尝试用另一种界面处理交易；
——如果 FCI 没有按照本部分进行个人化（例如，应用优先级不存在），但终端在共同支持的应用列表中至少存在一个应用，则终端可从共同支持应用的列表中选择任意一个应用；
——如果卡片对终端发出的 SELECT 命令响应失败，则终端应发起一个失效指令序列，并且应按照6.3 的要求返回到卡片检测处理。

6.4.2 卡片应用选择要求

本条描述了多个非接触应用的行为。为了将应用选择时间最小化，宜对个人化在FCI中的应用数量进行限制。卡片应用选择要求具体如下：

——应使用文件名“2PAY.SYS.DDF01”将 PPSE 个人化到所有的非接触卡片中；
——应在具有借记/贷记应用 AID 的单个卡片应用中，支持非接触式借记/贷记应用和 qPBOC 路径；
——如果一个以上的应用被个人化到 FCI 中，则应用优先指示器应被个人化到所有的应用中。在本部分中，应用优先指示器 Bits 8—5 应设为“0000”；
——卡片中的非接触金融应用的 AID，应在 SELECT PPSE 命令响应的 FCI 中返回。FCI 的完整格式在表 2 中描述；
——所有非接触支付应用的个人化都应存在 PDOL，该 PDOL 至少要包含表 3 中所描述的标签为“9F66”（终端交易属性）的数据元；
——如果支持单一的非接触应用，AID 的长度应至少有 7 字节；
——如果支持多个具有相同 PBOC AID 的非接触应用，应支持至少 8 字节长度的 AID，以便通过扩展字节进行区分，例如：A0 00 00 03 33 01 01 01 和 A0 00 00 03 33 01 01 02。

6.4.3 近距离支付系统环境（PPSE）

表2定义了单一应用和多个应用的PPSE格式。宜对个人化的应用的数量进行限制。

表2 近距离支付系统环境（PPSE）

标签	值				长度	出现条件
“6F”	FCI 模板				变长	M
	“84”	“2PAY.SYS.DDF01”			0E	M
	“A5”	FCI 专用模板			变长	M
		“BF0C”	FCI 发卡行自定义数据		变长	M
			“61”	目录入口	变长	M
				“4F” DF 名（AID）	07—08	M
				“50” 应用标签	04—10	O
				“87” 应用优先指示器	01	C[a]
			“61”	目录入口	变长	C[a]
				“4F” DF 名（AID）	07—08	C
				“50” 应用标签	04—10	C

标签	值				长度	出现条件
			“87”	应用优先指示器	01	C
		“61”	目录入口		变长	C*
			“4F”	DF 名（AID）	07—08	C
			“50”	应用标签	04—10	C
			“87”	应用优先指示器	01	C
[a] 如果一个以上的应用个人化到卡片中，则每个应用的个人化应具有应用优先指示器。应用优先指示器的 Bit 8—5 位应置为‘0000’。						

6.4.4 终端交易属性

表3描述了终端在GPO命令中提供的“终端交易属性”，卡片用此数据项表示的终端功能决定处理选择。“终端交易属性”的设置决定了交易的类型（qPBOC和非接触式借记/贷记应用）、终端是否支持联机处理或对联机处理的要求、终端支持持卡人验证方法的类型或终端对此项的要求。

字节2作为动态数据元，由终端按照交易条件（例如，授权金额（标签“9F02”）大于最低限额、授权金额大于CVM要求限制）设置。详细内容见6.2.2。

表3 终端交易属性（标签为“9F66”）

字节	位	定义
1	8	预留
	7	1 – 支持非接触式借记/贷记应用 0 – 不支持非接触式借记/贷记应用
	6	1 – 支持 qPBOC 0 – 不支持 qPBOC
	5	1 – 支持接触式借记/贷记应用 0 – 不支持接触式借记/贷记应用
	4	1 – 终端仅支持脱机 0 – 终端具有联机能力
	3	1 – 支持联机 PIN 0 – 不支持联机 PIN
	2	1 – 支持签名 0 – 不支持签名
	1	1 –支持联机授权交易的脱机数据认证 0 –不支持联机授权交易的脱机数据认证
2	8	1 – 要求联机密文 0 – 不要求联机密文
	7	1 – 要求 CVM 0 – 不要求 CVM
	6—1	预留
3	8	预留
	7	1 —终端支持 CDCVM 0 —终端不支持 CDCVM
	6—1	预留
4	8	1 – 终端支持“01”版本的 fDDA（见附录 B）

		0 - 终端仅支持“00”版本的 fDDA
	7—1	预留

6.4.5 SELECT 命令

SELECT命令报文编码见表4。

表4 SELECT 命令报文

代码	值
CLA	“00”
INS	“A4”
P1	引用控制参数（见表 5）
P2	SELECT 命令选项（见表 6）
Lc	“05” - “10”
Data	文件名（见 6.4.1）
Le	“00”

表5 SELECT 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0				
					1			通过名称选择
						0	0	

表6 SELECT 命令可选参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
						0	0	第 1 个或仅有一个
						1	0	下一个（未用）

6.5 初始应用处理要求

6.5.1 终端初始化应用处理的通用要求

终端初始化应用处理的通用要求如下：

——在初始应用处理阶段，终端向卡片发出 GPO 命令，命令中包括卡片在应用选择时返回 PDOL 中所要求的所有数据。初始应用处理见图 5 所示。GPO 命令详细描述见 6.5.5；

——所有终端应按照卡片在 PDOL 中的要求，在 GPO 命令中提供标签为“9F66”的数据项（终端交易属性）；

——所有终端应支持采用 JR/T 0025.5—2018 的格式 2 的 GPO 响应；

——如果 PDOL 在卡片的响应中不存在或标签为“9F66”的数据项（终端交易属性）在 PDOL 中不存在，则终端将该应用从候选列表中删除并返回选择应用步骤。

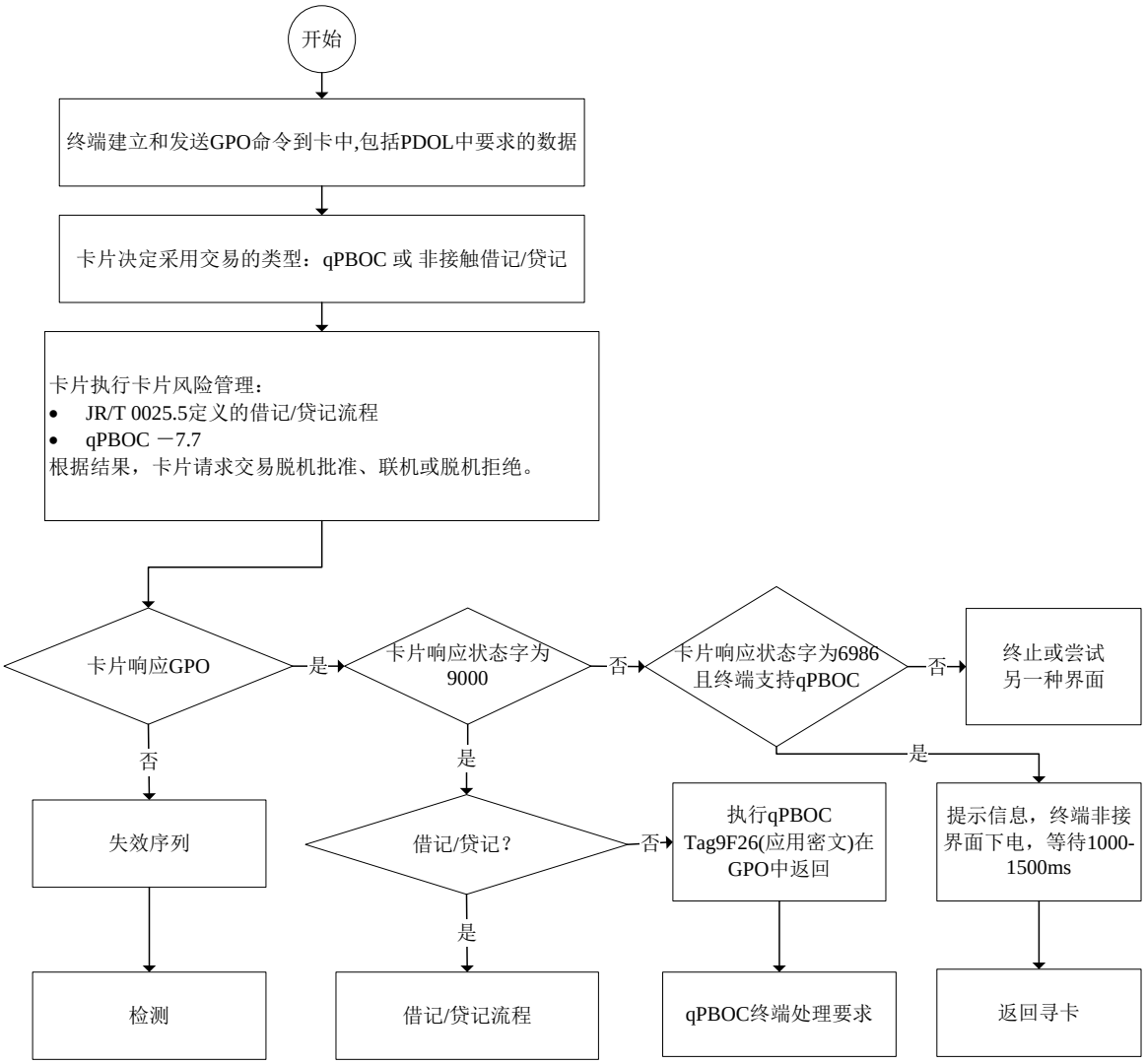


图5　初始应用处理流程

6.5.2　GPO 命令无响应

如果卡片响应终端发出的GPO命令失败，则终端应按JR/T 0025.8—2018中有关终端主循环的描述关闭工作场，并返回到6.3的检测处理。

6.5.3　GPO 命令响应的错误码

如果卡片响应GPO命令的状态字为“6986”，并且终端支持qPBOC流程，则终端应提示用户查看用户设备获取后续指令，并立即关闭非接触界面。在等待1000毫秒到1500毫秒后，终端应重新激活非接触界面，并进入卡片检测处理（见6.3），等待卡片进入。

如果卡片响应GPO命令的为其他非 “9000”的状态字，则终端应终止非接触交易，并尝试采用另一种界面进行交易。

注：根据JR/T 0025—2018，ID—1型卡片不会返回“6986”，但是对于支持CDCVM的用户支付设备例如手机等可能会返回“6986”，用于指示用户和终端执行进一步的动作。

6.5.4　GPO 命令的成功响应

终端通过应用交互特征（见附录C）和卡片响应GPO命令提供的数据元决定是否按照非接触式借记/贷记应用或qPBOC进行交易。

如果卡片响应 GPO 命令的状态字为“9000”，假设终端仅支持一种非接触选项（qPBOC 或非接触式借记/贷记应用），则终端应按此选项继续处理，不必判断 AIP。如果卡片响应 GPO 命令的状态字为“9000”，并且 AIP 第 2 字节第 8 位置‘0’，假设终端支持 qPBOC，并且应用密文（标签“9F26”）在 GPO 命令响应中出现，则终端应按照 qPBOC 处理交易。如果标签为“9F26”的数据项不出现，则终端应按照非接触式借记/贷记应用处理交易。

6.5.5 GPO 命令

获取处理选项（GET PROCESSING OPTIONS）命令格式如表7所示。

表7 GPO 命令

编码	值
CLA	“80”
INS	“A8”
P1	“00”；其他值预留
P2	“00”；其他值预留
Lc	变长
数据域	处理选项数据对象列表（PDOL）相关数据
Le	“00”

6.5.6 非接触交易次序

卡片和终端都支持的最适当方法的要求，决定了处理选择的顺序。qPBOC支持快速联机和脱机交易，不需要卡片插入插槽或放在卡盘上。

非接触式借记/贷记应用：如果卡片支持非接触式借记/贷记应用且“终端交易属性”第 1 字节第 7 位=‘1’（支持非接触式借记/贷记应用），则卡片应使用非接触式借记/贷记应用路径，终端应按照非接触式借记/贷记应用处理交易。

qPBOC：如果卡片支持 qPBOC 且“终端交易属性”第 1 字节第 6 位=‘1’（支持非接触 qPBOC），则卡片应使用 qPBOC 路径，终端应按照 qPBOC 处理交易。

如果没有匹配的非接触交易路径，则卡片应在响应中返回一个指示器（状态字=“6985”）来终止交易，并尝试采用另一种界面。

6.6 交互时间

基于卡片和终端之间的交互，qPBOC的交互总时间不应超过500ms。这个时间从终端寻卡开始计算，直至最后一条记录被返回给终端为止。不包括联机认证和qPBOC终端脱机数据认证中验证静态或动态签名所需的时间。在这500ms中，卡片处理命令以及传输响应所占用的时间总和不应超过400ms，终端处理命令以及传输命令所占用的时间总和不应超过100ms。

6.7 个人化

所有非接触应用宜采用JR/T 0025.10—2018中的个人化方法。

7 qPBOC 要求

7.1 概述

7.1.1 qPBOC 概述

qPBOC基于借记/贷记应用概念，使用现有的借记/贷记系统和操作规则，支持联机和脱机交易。通过减少命令和响应次数，qPBOC降低了终端和卡片之间的处理时间。qPBOC还提供了脱机快速小额支付特性、脱机数据认证、更多的发卡行自定义数据（见附录D）以及使用现有密文算法（版本01，见JR/T 0025.5—2018附录E）或新的精简算法（版本17，见附录E）的联机卡片认证。

除了实现本条描述的所有要求和元素的完全qPBOC路径外，还定义了一个改进的卡片qPBOC路径版本，以提供尽可能快的交互时间。

7.1.2 qPBOC 处理流程

图6描述了qPBOC的处理要求及qPBOC处理流程。

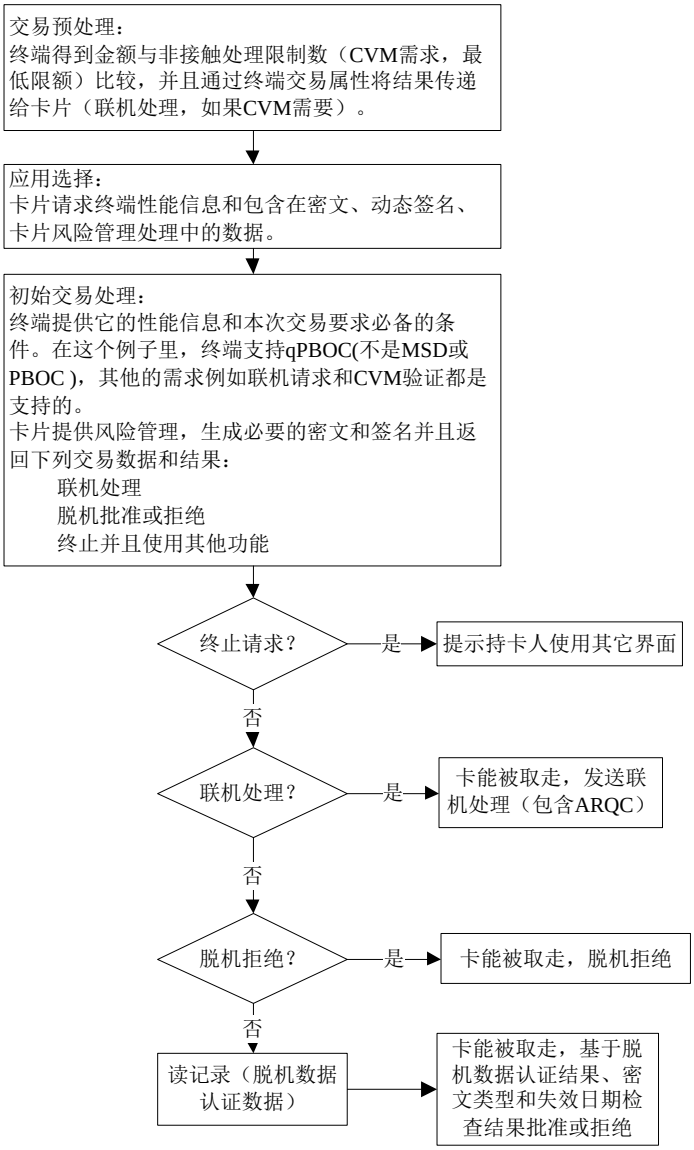


图6 qPBOC 处理流程

7.1.3 联机 ODA

联机ODA是指卡片在返回ARQC时携带签名数据，其中签名数据用于脱机数据认证判断卡片真伪，ARQC等其他数据则暂存用于后续发起联机交易。

联机ODA主要适用于卡片通过非接触方式在特定行业（如交通等）终端上进行联机交易时，通过脱机数据认证、延迟联机交易，终端无需实时联机，持卡人无需输入账户交易密码和签名，实现非接触式支付功能。

7.2 qPBOC 基于借记/贷记功能

qPBOC使用借记/贷记应用的方法进行应用选择、初始化交易处理以及读记录以得到应用数据。qPBOC采用了JR/T 0025—2018借记/贷记应用命令子集：SELECT、GPO、READ RECORD和GET DATA命令和要求。GPO命令响应采用JR/T 0025.5—2018中B.8的编码，但并不完全符合该编码，因为该响应不一定总是包含AFL。

qPBOC提供脱机数据认证支持（SDA或fDDA），符合JR/T 0025—2018借记/贷记应用的相关处理，但有如下例外：

——动态签名生成由 GPO 命令发起，不再使用内部认证命令，也不使用 DDOL；

——SDA 或 fDDA 的结果也不再放在终端验证结果（TVR）中联机发送给发卡行，或通过联机授权或清算密文进行保护。

SDA验证了重要的应用数据没有被非法更改，fDDA则不仅验证了卡片数据没有被非法更改而且验证卡片本身是有效卡（不是拷贝数据复制的伪卡）。关于fDDA的要求见附录B。

SDA不提供防复制保护。因此终端宜具有在需要的情况下，能够迅速地屏蔽SDA支持功能的能力。如果SDA被屏蔽，除非卡片支持fDDA，否则交易不能被脱机批准。交易会按照卡片交易属性（标签“9F6C”）中的卡片设置联机发送、终止或拒绝交易。

qPBOC不要求所有借记/贷记应用必备数据包含在卡片中，或者如果包含在卡片中，也不要求将其读出。在qPBOC处理中，借记/贷记应用的计数器和指示器以及其他本部分中未涉及到的变量不会受到影响。qPBOC的要求及处理在下面概述。

7.3 有关 PDOL 内容的 qPBOC 要求

7.3.1 通用要求

qPBOC不支持借记/贷记应用中的CDOL、DDOL或缺省DDOL。所有卡片处理必需的数据在PDOL中请求。

卡片请求终端交易属性以便非接触应用能决定使用哪个卡片路径（非接触式借记/贷记应用或qPBOC）。不可预知数、授权金额与卡片的ATC一起，用于计算密文（版本01或版本17）。不可预知数和ATC也用于在脱机交易中计算动态签名。

一个卡片应用包含单一的PDOL，PDOL包含了与所有路径（qPBOC以及非接触式借记/贷记应用）相关的标签，也可包含本部分未描述的标签来作为最低要求。发卡行应在PDOL请求附加数据带来的好处与附加数据传输和处理对交易性能带来的影响之间权衡利弊。

qPBOC中的PDOL最基本内容依赖于支持的密文版本（01或17），以及卡片是否支持脱机qPBOC交易。

7.3.2 采用密文版本 17 的仅联机 qPBOC

密文版本17仅联机qPBOC最基本的PDOL内容见表8所示。

表8 仅联机 qPBOC 的最基本 PDOL 内容

PDOL 中的标签	数据元名称
“9F66”	终端交易属性
“9F02”	授权金额
“9F37”	不可预知数

如果联机卡片执行支持卡片附加处理，则交易货币代码（标签“5F2A”）也应包括在PDOL中。

不可预知数、授权金额与卡片中的ATC一起用于计算密文。

7.3.3 采用密文版本 17 的可脱机 qPBOC

密文版本17联机和脱机qPBOC最基本的PDOL内容见表9所示。

表9 联机和脱机 qPBOC 的最基本 PDOL 内容

PDOL 中的标签	数据元名称
“9F66”	终端交易属性
“9F02”	授权金额
“9F37”	不可预知数
“5F2A”	交易货币代码

不可预知数、授权金额与卡片中的ATC一起用于计算密文。不可预知数和ATC还用于计算脱机交易的动态签名。

7.3.4 采用密文版本 01 的 qPBOC

在密文版本01中脱机与联机使用相同的数据标签。其最基本的PDOL内容见表10所示。

表10 应用密文版本 01 的 qPBOC 最基本 PDOL 内容

PDOL 中的标签	数据元名称
“9F66”	终端交易属性
“9F02”	授权金额
“9F03”	其他金额
“9F1A”	终端国家代码
“95”	终端验证结果（TVR）[a]
“5F2A”	交易货币代码
“9A”	交易日期
“9C”	交易类型
“9F37”	不可预知数
[a] 为了 TVR 会被 qPBOC 终端填为 0（所请求的数据对于终端无法提供时，同样按此情况处理）。	

上面所有数据除了终端交易属性外，都用于卡片密文计算。

7.4 卡片接收 GPO 命令

7.4.1 防拔保护

如果卡片支持脱机交易，则要求在计数器更新后，交易结束前提供交易防拔保护。为了提供这种保护，卡片应定义一个交易防拔保护状态，卡片在计数器更新之后设置交易防拔保护状态，并在处理最后一条命令时将该状态清除，作为最后一步操作。在交易开始时如果防拔保护状态被设置（应用被选中时），卡片就知道上一笔交易没有完成，并因此恢复脱机计数器到先前的值。

如果交易防拔保护状态被设置，卡片应恢复到最近一笔成功完成的交易结束时的值，并清除交易防拔保护状态。

交易防拔保护状态的设置和清除由卡片供应商自主实现。

7.4.2 卡片 GPO 响应

卡片的GPO响应中包括应用交互特征，以指示卡片对风险管理特征的支持。还包括密文及相关的数据元、2磁道等价数据以及列在表11中用于联机交易的所有必备数据。响应数据按照JR/T 0025.5—2018附录B中定义的格式2编码，即含有标签和长度的TLV编码，响应数据的具体内容见表11。

表11　GPO 响应必备和条件数据

标签	数据元名称	条件（M：必备，C：条件，O：可选）		
		联机（ODA）	联机（无 ODA）或拒绝	脱机批准
“82”	AIP	M	M	M
“94”	AFL	M	无	M
“9F36”	ATC	M	M	M
“9F26”	应用密文	M	M	M
“9F27”	密文信息数据	M	M	M
“9F10”	发卡行应用数据 标签“9F10”中的发卡行自定义数据也可包含可用脱机消费金额。附录 D 中详细说明了如何包含可用脱机消费金额。	M	M	M
“57”	2 磁道等价数据 除非作为待签名的静态数据一部分，2 磁道等价数据是必需的。	C 如果 2 磁道等价数据不是待签名的静态数据部分。	C 如果 2 磁道等价数据不是待签名的静态数据部分。	C 如果 2 磁道等价数据不是待签名的静态数据部分。
“5F34”	应用 PAN 序列号	C 如果卡片中出现。	C 如果卡片中出现。	C 如果卡片中出现。
“9F4B”	签名的动态应用数据	C 卡片动态签名数据可以在 GPO 中返回，也可以在 Read Record 中返回。	无	C 卡片动态签名数据可以在 GPO 中返回，也可以在 Read Record 中返回。
“9F24”	应用主账号参考号（PAR）	无	C 如果应用主账号是支付标记，则存在。	无
“9F63”	产品标识信息	C 如果卡片中出现，可以在 GPO 中返回，也可以在 Read Record 中返回。	C 如果卡片中出现。	C 如果卡片中出现，可以在 GPO 中返回，也可以在 Read Record 中返回。

标签	数据元名称	条件（M：必备，C：条件，O：可选）		
		联机（ODA）	联机（无 ODA）或拒绝	脱机批准
“9F6C”	卡片交易属性	C 如果卡片中出现。	C 如果卡片中出现。	C 如果卡片中出现。
“9F5D”	可用脱机消费金额 除非标签“9F5D”已被个人化值为‘1’，卡片不应在 GPO 响应中返回该数据元。而且，发卡行也应将卡片附加处理（第 1 字节第 1 位）个人化值为‘1’，以指示该金额将被计算并包括在所有非接触交易中。 将标签“9F5D”个人化值为‘1’，也表示可用 GET DATA 命令读出该数据元。 内容按照发卡行指示及卡片附加处理章条部分（小额、小额和 CTTA）定义进行计算。	C 如果允许脱机金额显示，可以在 GPO 中返回，也可以在 Read Record 中返回。	C 如果允许脱机金额显示。	C 如果允许脱机金额显示，可以在 GPO 中返回，也可以在 Read Record 中返回。
“5F20” 或 “9F0B”	持卡人姓名 持卡人姓名在借记/贷记应用中是要求的数据元。 （若持卡人姓名小于或等于 26 个字节时使用“5F20”，若持卡人姓名大于 26 个字节时使用“9F0B”）	O	O	O
“9F7C”	用户专用数据	O	O	O

任何附加数据，包括持卡人姓名（标签“5F20”），既可在 GPO 响应中返回，也可在 READ RECORD 命令中返回。

对于脱机交易，如果作为脱机数据认证中的待签名静态数据的一部分，应用失效日期（标签“5F24”）、应用 PAN（标签“5A”）和 SDA 标签列表（标签“9F4A”）应包含在一条记录中。

当 ATC 达到最大值(65535)时,应用应被永远锁定,密文计算被禁止,GPO 命令宜返回状态字“6985”。

PAN 和失效日期由终端从 2 磁道等价数据中得到。对于联机交易，可用脱机消费金额根据卡片配置可从两处返回：可包含在附录 D 描述的标签 9F10（联机发送给发卡行）的发卡行自定义数据部分，或者作为 GPO 响应的标签数据元返回（由终端显示或打印出）。

除发卡行有特殊业务需求外，非接触界面下记录中不应包含持卡人姓名（标签“5F20”）和持卡人姓名扩展（标签“9F0B”），以保证持卡人姓名信息不在非接触界面下被读取。否则，应由发卡行承担持卡人信息保护责任。

7.4.3 应用文件定位器

AFL包含当前所选应用的文件和相关记录列表，中间没有分隔符。终端应只读取AFL指定的记录。列表中每个项对应一个要读取的文件见JR/T 0025.5—2018中的表9。

当卡片请求拒绝交易时，AFL不应返回。

7.4.4 应用交互特征

应用交互特征指示卡片支持的应用功能，按照表C.1编码。终端应只尝试执行IC卡支持的功能。如果卡片没有返回密文信息数据，终端根据以下原则构建密文信息数据：

——将密文信息数据置为‘00’；

——将发卡行应用数据（“9F10”）第5字节第6—5位的值赋给密文信息数据的8—7位。

7.4.5 qPBOC推荐签名数据

如卡片支持qPBOC，则下面这些静态数据元宜用于签名：

——应用PAN；

——PAR（如存在）；

——应用失效日期；

——AIP（如果支持fDDA）；

——应用版本号；

——SDA标签列表（如果支持fDDA）。

卡片在个人化时应将应用版本号（标签“9F08”）设置为JR/T 0025—2018的版本号，应将应用版本号（标签“9F08”）加入到签名用的静态数据中，以标识卡片真实的应用版本。如果在同一张卡上都支持qPBOC和借记/贷记应用（接触），也可增加JR/T 0025.5—2018中推荐的附加数据元。

7.5 qPBOC卡片要求

除了所有非接触应用的卡片要求外，qPBOC还应遵守下面的要求：

——收到GPO命令，卡片应立即设置发卡行应用数据（标签“9F10”）的CVR部分为“03000000”；CVR是发卡行应用数据的第4－7字节部分，后续置位时应注意：

- CVR字节1，设置为“03”；
- CVR字节2，其中位4、3、2、1为保留位，设置为“0”；
- CVR字节3，其中位8、4、3、2、1为保留位，设置为“0”；
- CVR字节4，所有位均为保留位，设置为“0”。

——卡片应支持算法选择，并且在收到GPO指令以后，需要根据终端发送的DF69进行判定，如果发现卡片不能支持终端要求的算法，那么卡片需要返回GPO指令的状态码为6985，从而实现脱机拒绝；

——收到GPO命令，卡片对密文信息数据进行初始化，将其置为“00”；

——如果卡片在同一笔交易中收到多次GPO命令，则卡片应以“6985”响应第二次及后续收到的GPO命令；

——如果本次交易卡片以非“9000”响应过GPO命令，则卡片不应返回卡片认证相关数据；

——如果终端和卡片均支持并选择了SM算法进行交易处理，那么卡片需要返回采用SM算法计算TC、动态认证数据、SM算法的发卡行自定义数据（“9F10”）、SM算法对应的AFL等数据给终端，终端再进行数据读取以及完成fDDA认证操作；

——卡片应在计算密文和动态签名之前增加ATC的值；

——如果卡片的可用脱机消费金额（标签“9F5D”）被个人化为1，则卡片应允许读取该数据元。卡片的行为应在个人化时指明并存储在内部卡片指示器中；

——对于联机交易，卡片应在GPO响应中返回联机密文，以及表11中生成密文的数据元；

——对于脱机交易，卡片应在GPO响应中返回表11中的数据元；

——动态签名可以在GPO响应中返回，也可以在READ RECORD命令中返回；

——如果一个卡片数据元在GPO响应中被返回了，那么卡片不应在读记录时也返回该数据元。即同一个数据元在同一个交易中应只被返回一次；

——qPBOC脱机批准的交易，AFL指明的终端应读取的最后一条记录的70模板的长度不应超过32字节。如卡片执行的是“01”版本的fDDA，则宜在这条记录中仅放置电子现金发卡行授权码（标签“9F74”）和卡片认证相关数据（标签“9F69”），其中卡片认证相关数据仅在卡片执行“01”版本的fDDA时出现；

——符合 JR/T 0025—2018 的卡片应同时支持“00”版本和“01”版本的 fDDA。如终端支持“01”版本的 fDDA（终端交易属性第 4 字节第 8 位为‘1’），则卡片应执行“01”版本的 fDDA；
——如果应用主账号是支付标记，且交易类型为脱机批准或联机（ODA），则 PAR 应在 READ RECORD 指令中返回。

7.6 qPBOC 终端要求

除了对于所有非接触应用的终端要求外，支持qPBOC的终端还应符合下面这些要求：
——终端应支持 6.2.2 所描述的 qPBOC 交易预处理；
——终端应根据系统算法支持情况，设置算法指示器，发送 GPO 指令至卡片；
——脱机数据认证过程中，终端根据公钥索引检查算法类型；
——仅支持 qPBOC 的终端不应查询 AIP 来决定卡片是请求非接触式借记/贷记应用或 qPBOC，而应默认 qPBOC 处理；
——支持 qPBOC 的终端应按 JR/T 0025—2018 借记/贷记应用的规则读记录，并处理记录或 PDOL 中不认识的标签编码的数据元；
——如果 qPBOC 必备数据元没有被 GPO 返回（见表 11），支持 qPBOC 的终端应终止交易，但如果没有返回的数据元是 9F27，终端应按 7.4.4 处理；
——如果 JR/T 0025—2018 借记/贷记应用必备但 qPBOC 不要求的数据元不存在，支持 qPBOC 的终端不应因此拒绝交易；
——支持 qPBOC 的终端应在任何要求磁道数据的 qPBOC 联机报文中提供 2 磁道等价数据；
——如果卡片交易属性（标签“9F6C”）数据元在卡片中未提供，支持签名的终端应认为支持签名。如果终端要求 CVM，应在单据上打印签名行；
——支持超过一个 CVM 的终端应查询卡片交易属性（标签“9F6C”）的第 1 字节第 8 位和第 7 位决定卡片选择哪个 CVM。如果位 8=‘1’，终端应执行联机 PIN 校验，不再查询位 7；如果位 8=‘0’，终端应查询位 7。除非终端支持联机 PIN，否则卡片不会设置第 8 位；当前的卡片逻辑不会将位 8 和位 7 都设置。不过以后增加的 CVM 也许会要求卡片逻辑改变。如果位 7=‘1’，终端应在单据上打印签名行；
——对于支持 qPBOC 和非接触式借记/贷记应用的终端，如果 AIP 中第 2 字节第 8 位为零，终端按如下处理：
- 如果应用密文（标签“9F26”）没有出现在 GPO 响应中按借记/贷记应用流程处理；
- 如果应用密文（标签“9F26”）出现在 GPO 响应中按 qPBOC 处理。

——符合 JR/T 0025—2018 的终端，应同时支持“00”版本和“01”版本的 fDDA 验证，并应在终端交易属性（第 4 字节第 8 位置为‘1’）中表明此能力；
——在如下的任何情形中，脱机数据认证失败：
- AIP 中未指示支持 fDDA；
- 或支持 fDDA，但 fDDA 要求的数据缺失。

7.7 qPBOC 卡的风险管理过程

7.7.1 通用要求

终端交易属性（标签“9F66”，第1字节第6位=‘1’）指明了终端能通过非接触接口来处理qPBOC交易。

卡的行为是由卡附加处理（标签“9F68”）中个人化的一系列要求来控制。这些数据元的内容如表12所示，并在表12描述的卡片处理中用到。

表12　卡片附加处理（标签“9F68”）

字节	位	说明
1	8	1 – 支持小额检查 0 – 不支持小额检查
	7	1 – 支持小额和 CTTA 检查 0 – 不支持小额和 CTTA 检查
	6	0 – 预留
	5	1 – 支持新卡检查 0 – 不支持新卡检查
	4	1 – 支持 PIN 重试次数超过检查 0 – 不支持 PIN 重试次数超过检查
	3	1 – 允许货币不匹配的脱机交易 0 – 不允许货币不匹配的脱机交易
	2	1 – 卡优先选择接触式借记/贷记联机 0 – 卡片不选择接触式式借记/贷记联机
	1	1 – 返回可用脱机消费金额 0 – 不返回可用脱机消费金额
2	8	RFU
	7	1 – 不允许不匹配货币的交易 0 – 允许不匹配货币的交易
	6	1 – 如果是新卡且终端仅支持脱机则拒绝交易 0 – 如果是新卡且终端仅支持脱机不拒绝交易
	5	1 –qPBOC 记录交易日志，记录方式见 7.12 条，应用缺省行为（ADA）字节 3（标签 9F52） 0 –qPBOC 不记录交易日志
	4—1	RFU
3	8	1 – 匹配货币的交易支持联机 PIN 0 – 匹配货币的交易不支持联机 PIN
	7	1 – 不匹配货币的交易支持联机 PIN 0 – 不匹配货币的交易不支持联机 PIN
	6	1 – 对于不匹配货币交易，卡要求 CVM 0 – 对于不匹配货币交易，卡不要求 CVM
	5	1 – 支持签名 0 – 不支持签名
	4—1	预留
4	8—7	预留
	6	1 –支持联机授权交易的脱机数据认证 0 –不支持联机授权交易的脱机数据认证
	5—1	预留

这部分使用类伪代码语言来解释卡的处理过程，没有指明具体实现细节。本部分中详细说明的功能和时间要求应被满足，但是实现的细节由应用开发者自行决定。

7.7.2　设置货币匹配或不匹配

货币被比较一次同时保存结果。进行如下处理：

——将匹配货币位（内部卡片指示器）设置为‘0’；

——如果使用的货币代码（标签“9F51”）等于交易货币代码（标签“5F2A”），将匹配货币位设置为‘1’；

——如果匹配货币位=‘0’而且不允许不匹配货币交易（卡片附加处理的第 2 字节第 7 位=‘1’），拒绝交易，具体步骤见 7.7.18 。

7.7.3 终端仅支持脱机

如果终端仅支持脱机，跳过联机请求检查。

如果终端仅支持脱机（终端交易属性，第 1 字节第 4 位=‘1’），卡片需要尝试如下脱机处理：

——将仅脱机终端位（内部卡指示器）设置为‘1’；

——如果上次联机 ATC 寄存器为‘0’，并且如果是新卡且终端仅支持脱机（卡片附加处理的第 2 字节第 6 位=‘1’），就拒绝交易，具体步骤见 7.7.18 。

如果终端仅支持脱机且支持 PIN 尝试超过检查（卡片附加处理的第 1 字节第 4 位），则当脱机 PIN 尝试计数器（标签“9F17”）存在并等于 0（没有剩余的 PIN 尝试），卡片应将 CVR 的第 3 字节第 7 位设置为‘1’（PIN 尝试上限超过），并拒绝交易，具体步骤见 7.7.18 。

如果终端仅支持脱机，并且下面有一种情况满足：

——在终端交易属性中终端要求 CVM（第 2 字节第 7 位=‘1’）；

——匹配货币位=‘1’，且授权金额大于卡片 CVM 限额；

——匹配货币位=‘0’，而对于不匹配货币交易卡片请求 CVM 位=‘1’（卡片附加处理的第 3 字节第 6 位）。

则：

——如果卡和终端都支持签名，即终端交易属性中支持签名（第 1 字节第 2 位=‘1’），且卡片附加处理也支持签名（第 3 字节第 5 位=‘1’），于是在卡片交易属性中设置需要签名并尝试脱机处理。将卡片交易属性的第 1 字节第 7 位置为‘1’，并进行脱机货币检查，具体步骤见 7.7.6 ；

——如果卡或终端至少一个不支持签名，即终端交易属性中不支持签名（第 1 字节第 2 位=‘0’），或卡片附加处理不支持签名（第 3 字节第 5 位=‘0’），终止非接触交易，具体步骤见 7.7.17 。

仅支持脱机终端的处理流程见图 7 所示。

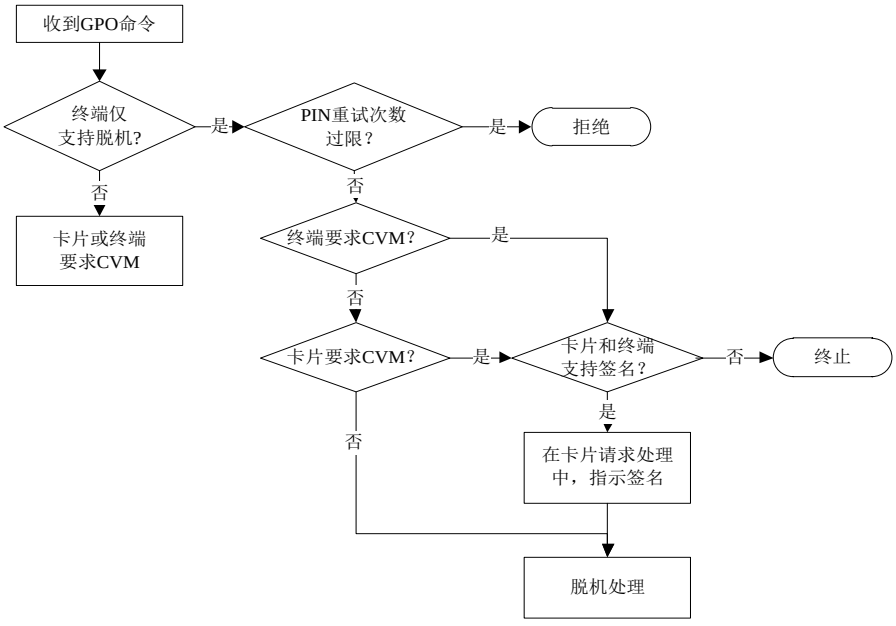


图7 终端仅支持脱机

7.7.4 终端或卡请求 CVM

终端可请求CVM（总是或者对超过终端CVM请求上限的交易）。卡同样也可请求CVM。如果卡或终端请求CVM，而卡不支持任何一种终端在终端交易属性中指明的CVM，则交易将被终止。

如果请求CVM而且联机PIN同时被终端和卡所支持，则交易将通过联机来处理。

如果请求CVM但没有被卡和终端同时支持的CVM，则交易被终止。

如果不请求 CVM，即如果终端交易属性的 CVM 请求位为‘0’，而且下面任一情况满足：

——匹配货币位=‘1’，同时授权金额小于或等于卡片 CVM 限额；

——匹配货币位=‘0’，且不匹配货币交易卡片请求 CVM 位=‘0’（卡片附加处理的第 3 字节第 6 位）。

则卡继续进行风险管理处理，检查联机处理请求，具体步骤见7.7.5 。

如果请求 CVM，即如果终端交易属性的 CVM 请求位（第 2 字节第 7 位）为‘1’，或如果终端交易属性的 CVM 请求位（第 2 字节第 7 位）为‘0’，而且下面任一情况满足：

——匹配货币位=‘1’，同时授权金额大于卡片 CVM 限额；

——匹配货币位=‘0’，且不匹配货币交易卡片请求 CVM 位=‘1’（卡片附加处理的第 3 字节第 6 位）。

则按照下列步骤继续：

——如果卡和终端均支持联机 PIN，并且在终端交易属性（第 1 字节第 3 位）中支持联机 PIN，同时下面任一情况满足：

- 匹配货币位=‘1’，同时对于匹配货币，联机 PIN 支持位=‘1’（卡片附加处理的第 3 字节第 8 位）；
- 匹配货币位=‘0’，同时对于不匹配货币，联机 PIN 支持位=‘1’（卡片附加处理的第 3 字节第 7 位）。

——如果卡和终端均支持联机 PIN，则：

- 卡要将卡交易属性（标签“9F6C”，第 1 字节第 8 位）设置为‘1’，并请求联机处理；
- 如果返回可用脱机消费金额位=‘1’，则卡要通过卡片附加处理指明的脱机小额选项（小额、小额和 CTTA）计算可用脱机消费金额。如果没有指明任何一个选项，则卡要将可用脱机消费金额设置为零。

完成联机处理，具体步骤见7.7.16 ；

——如果卡和终端均支持签名，即如果终端交易属性（第 1 字节第 2 位）支持签名同时卡片附加处理的签名支持位=‘1’（第 3 字节第 5 位）：

- 卡将卡片交易属性的签名请求位设置为‘1’，然后继续卡片风险管理处理；
- 检查联机处理请求，具体步骤见 7.7.5 。

——如果无共同的 CVM，卡片应终止非接触式交易，具体步骤见 7.7.17 。

卡片 CVM 处理流程见图 8 所示。

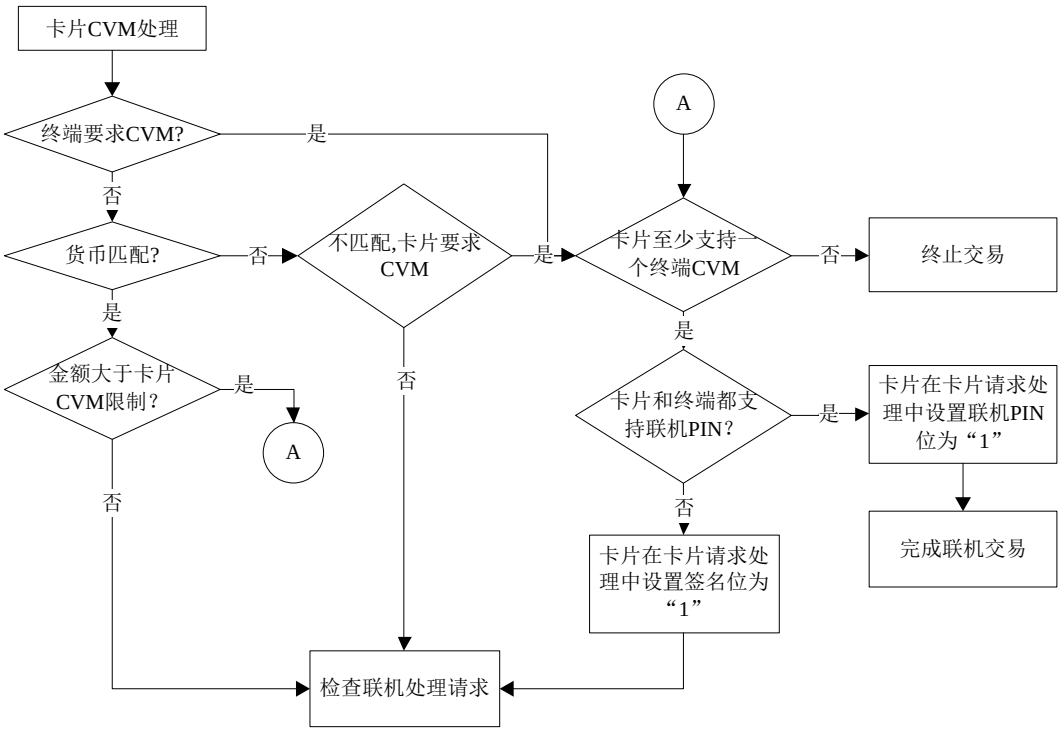


图8　卡片 CVM 处理流程

7.7.5　检查联机处理请求

卡片和终端可基于交易条件请求联机处理。如果先前的“终端或卡请求CVM”检查没有指示需要联机处理，或终止非接触交易，执行该检查决定是否存在其他的条件导致联机处理。

如果终端请求联机处理（终端交易属性的第2字节第8位=‘1’），则卡要按以下步骤请求联机处理：

——如果返回可用脱机消费金额位=‘1’，则卡要通过卡片附加处理指明的脱机小额选项（小额、小额和 CTTA）计算可用脱机消费金额。如果没有指明任何一个选项，则卡将可用脱机消费金额设置为零；

——完成联机交易，具体步骤见 7.7.16　。

如果不允许不匹配货币的脱机交易（卡片附加处理的第1字节第3位=‘0’）同时匹配货币位=‘0’，则卡片应按以下步骤请求联机处理：

——如果返回可用脱机消费金额位=‘1’，则卡要通过卡片附加处理指明的脱机小额选项（小额、小额和 CTTA）计算可用脱机消费金额。如果没有指明任何一个选项，则卡将可用脱机消费金额设置为零；

——完成联机交易，具体步骤见 7.7.16　。

如果支持新卡检查（卡片附加处理的第1字节第5位=‘1’）同时上次联机ATC寄存器为零（新卡没完成联机处理），则卡应按以下步骤请求联机处理：

——如果返回可用脱机消费金额位=‘1’，则卡要通过卡片附加处理指明的脱机小额选项（小额、小额和 CTTA）计算可用脱机消费金额。如果没有指明任何一个选项，则卡将可用脱机消费金额设置为零；

——将 CVR 的第 3 字节第 5 位设置为‘1’（新卡）；

——完成联机交易，具体步骤见 7.7.16　。

如果支持PIN尝试超过检查（卡片附加处理的第1字节第4位=‘1’）同时脱机PIN尝试计数器（标签“9F17”）存在并等于零（没有剩余的PIN尝试），则卡应按以下步骤请求联机处理：

——如果返回可用脱机消费金额位=‘1’，则卡要通过卡片附加处理指明的脱机小额选项（小额、小额和 CTTA）计算可用脱机消费金额。如果没有指明任何一个选项，则卡要将可用脱机消费金额设置为零；

——将 CVR 的第 3 字节第 7 位设置为‘1’（PIN 尝试上限超过）；

——完成联机交易，具体步骤见 7.7.16 。

检查联机处理请求见图 9 所示。

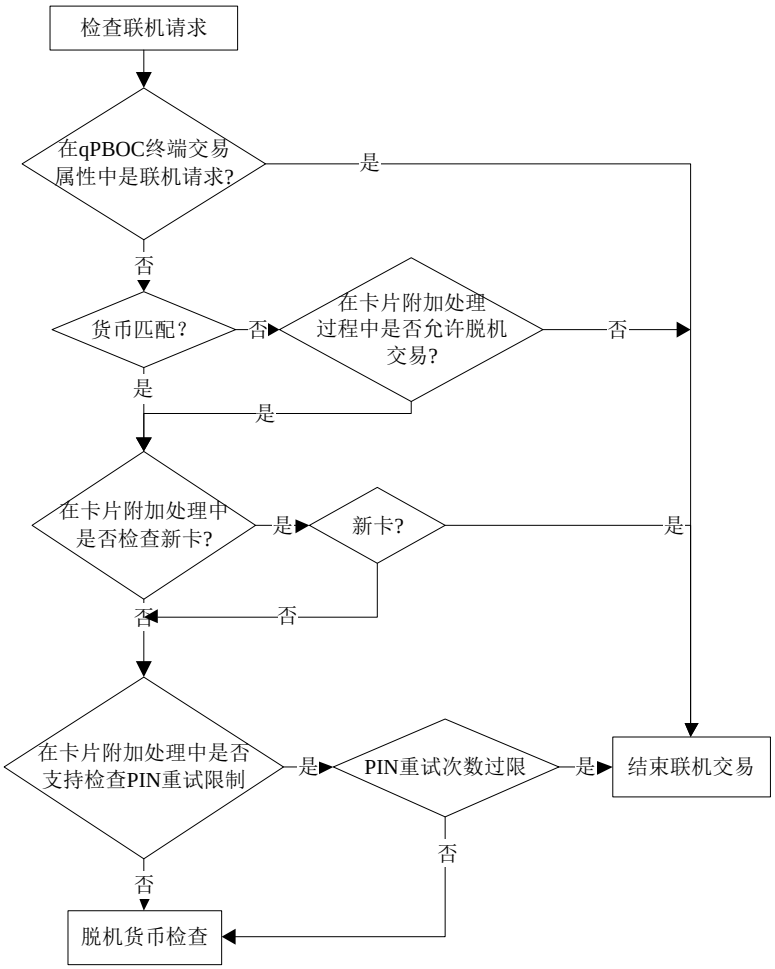


图9 检查联机处理请求

7.7.6 脱机货币检查

当交易货币匹配应用货币，执行脱机消费检查。如果货币不匹配，跳过这些检查并执行不匹配货币处理。

检查处理是匹配还是非匹配货币，以及是否支持脱机消费检查类型的相应检查。

小额检查、小额和CTTA检查是qPBOC的两种检查脱机消费的方法。JR/T 0025—2018定义的电子现金相关数据（电子现金余额、电子现金余额上限和电子现金单笔交易限额）用于执行小额处理，但处理这些相关标签的功能性要求在7.7.7和7.7.8中详细描述。

如果货币匹配位=‘0’，则脱机下的货币不匹配，具体步骤见 7.7.14 。

否则匹配货币的标志为‘1’，则卡和终端的货币相匹配。检查支持哪种脱机消费检查选项。如果没有支持任何一种，对于仅支持脱机的终端则拒绝交易，对于支持联机的终端则进行联机处理，具体见7.7.10 。

7.7.7 匹配货币交易的小额检查

这个检查通过卡上的小额上限（电子现金余额上限）来实现。非接触交易的脱机消费可用总资金就是电子现金余额。执行这个选项能够来提供等于电子现金余额的可用脱机消费金额。

如果支持小额检查（卡片附加处理的第 1 字节第 8 位=‘1’），则电子现金余额就是总的脱机可消费额，接着执行小额检查，具体步骤见 7.7.11 。

7.7.8 匹配货币交易的小额和 CTTA 检查

此部分检查CTTA是否超过累计脱机交易金额上限（CTTAUL）或者在CTTAUL不存在的情况下是否超过累计脱机交易金额限制数CTTAL。如果CTTA可用资金——CTTAUL（如果不存在用CTTAL）减去CTTA是可用的，同样会检查交易金额是否超过电子现金单笔交易限额。只有当小额和CTTA检查通过时，脱机交易才会发生。

对于这个选项，可用脱机消费金额等于可使用的CTTA资金。

如果支持小额和 CTTA 检查（卡片附加处理的第 1 字节第 7 位=‘1’），则资金应在小额和 CTTA 中均可用。CTTA 可用资金是可使用的总脱机消费额，并执行小额和 CTTA 检查，具体步骤见 7.7.12 。

7.7.9 匹配货币交易的小额或 CTTA 检查

JR/T 0025—2018不再支持此检查。

7.7.10 没有任何脱机选项被支持

没有指示脱机消费检查。

如果是终端仅支持脱机（终端交易属性，第 1 字节第 4 位=‘1’），则卡片应拒绝交易，具体步骤见 7.7.18 。

如果终端支持联机（终端交易属性，第 1 字节第 4 位=‘0’），则卡片应请求联机处理。

如果返回可用脱机消费金额=‘1’，则卡要通过卡片附加处理指明的脱机小额选项（小额、小额和CTTA）计算可用脱机消费金额。如果没有指明任何一个选项，则卡要将可用脱机消费金额设置为零，完成联机交易，具体步骤见7.7.16 。

脱机货币检查处理流程见图 10 所示。

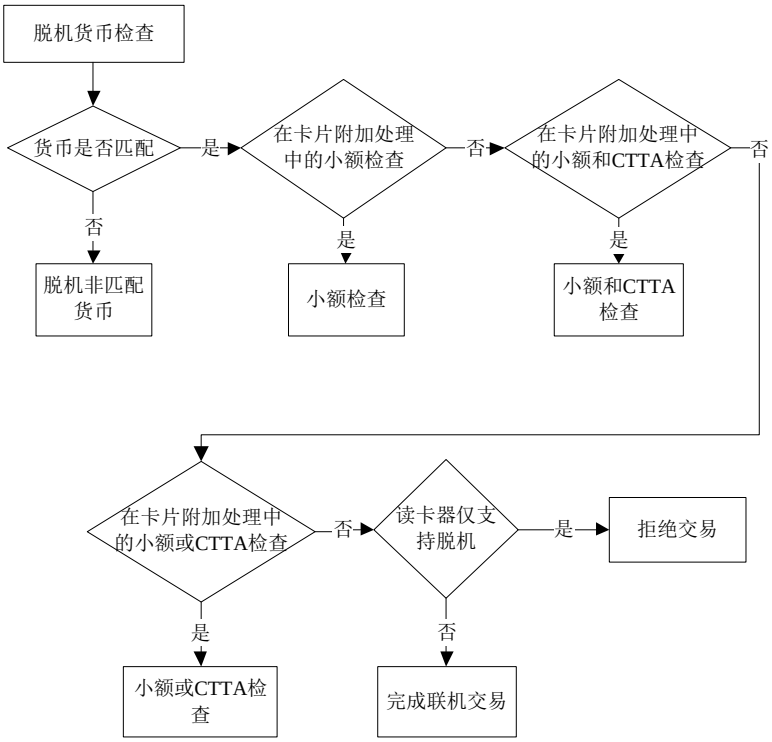


图10　脱机货币检查处理流程

7.7.11　小额检查

7.7.11.1　概述

检查交易是否能够脱机处理。

如果授权金额（标签“9F02”）小于或等于电子现金单笔交易限额，同时在交易的电子现金余额中有足够的脱机消费可用金额，则交易进行脱机处理，见7.7.11.4。

否则（即如果授权金额大于电子现金单笔交易限额或者交易没有足够的脱机消费可用金额）：

——如果终端具有联机处理能力，则卡片请求联机处理，见 7.7.11.2；

——如果终端不具有联机处理能力，则卡片请求拒绝，见 7.7.11.3。

7.7.11.2　终端可联机

当终端具有联机能力时（终端交易属性，第1字节第4位=‘0’）：

——如果授权金额（标签“9F02”）大于电子现金单笔交易限额（如果存在，标签“9F78”），则卡应准备返回可用脱机消费金额（如支持的话），并请求联机处理：

- 如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’）同时匹配货币位=‘1’，则卡应设置可用脱机消费金额（标签“9F5D”）为电子现金余额值，并在 GPO 响应中返回可用脱机消费金额；
- 设置 CVR 的第 3 字节第 6 位为‘1’（频度检查计数器超过）；
- 完成联机交易，具体步骤见 7.7.16　。

——如果授权金额（标签“9F02”）大于电子现金余额减去电子现金重置阈值（如果存在，标签“9F6D”），则卡应准备返回可用脱机消费金额（如支持获取），并请求联机处理：

- 如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’）同时匹配货币位=‘1’，则卡应设置可用脱机消费金额（标签“9F5D”）为电子现金余额值，并在 GPO 响应中返回可用脱机消费金额；

- 设置 CVR 的第 3 字节第 6 位为‘1’（频度检查计数器超过）；
- 完成联机交易，具体步骤见 7.7.16 。

7.7.11.3 终端仅脱机

仅当终端支持脱机时（终端交易属性，第1字节第4位=‘1’），如果授权金额大于电子现金余额或者大于电子现金单笔交易限额（如果存在），则卡应准备返回可用脱机消费金额（如支持获取），同时拒绝交易，且：

——如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’），则卡应设置可用脱机消费金额（标签“9F5D”）为电子现金余额值，同时在 GPO 响应中返回可用脱机消费金额；

——设置 CVR 的第 3 字节第 6 位为‘1’（频度检查计数器超过）；

——拒绝交易，具体步骤见 7.7.18 。

7.7.11.4 交易被允许脱机完成

如果前面的步骤都不符合，则卡应完成下列的处理过程：

——保存当前电子现金余额值；

——设置交易防拔保护状态，来指示计数器正在被更新。这个状态只有在最后一条读记录命令响应之前才被清除。防拔保护，具体步骤见 7.4.1 ；

——计算新的电子现金余额，等于电子现金余额减去授权金额（标签“9F02”）；

——如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’），则卡应设置可用脱机消费金额（标签“9F5D”）为电子现金余额值，同时在 GPO 响应中返回可用脱机消费金额；

——在密文信息数据及 CVR 中请求脱机批准；

——完成脱机交易，具体步骤见 7.7.15 。

7.7.11.5 流程图

小额检查处理流程见图 11 所示。

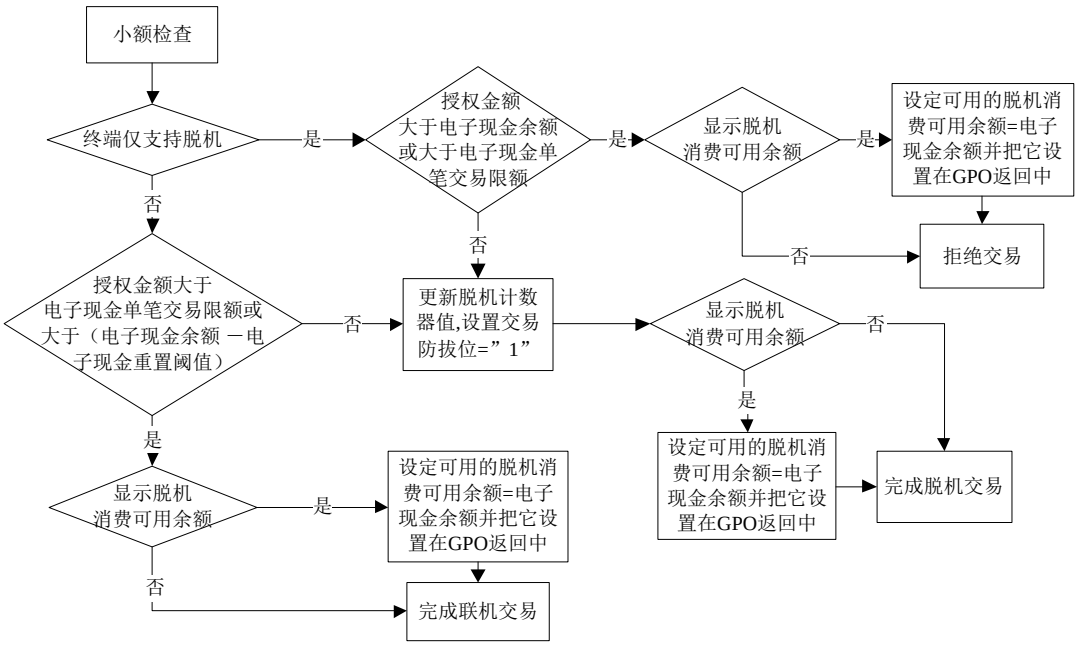


图11 小额检查处理流程

7.7.12 小额和 CTTA 检查

7.7.12.1 概述

此检查的目的是检查交易能否被脱机处理

如果授权金额（标签“9F02”）小于或等于电子现金单笔交易限额，并且交易的电子现金余额和CTTA可用资金都有足够的脱机资金，则交易脱机处理，见7.7.12.4。

如果授权金额（标签“9F02”）大于电子现金单笔交易限额或者交易没有足够的可用脱机消费金额：

——如果终端具有联机处理能力，则卡片请求联机处理，见 7.7.12.2；

——如果终端不具有联机处理能力，则卡片请求拒绝，见 7.7.12.3。

7.7.12.2 终端可联机

当终端具有联机能力时（终端交易属性，第1字节第4位=‘0’）：

——如果授权金额（标签“9F02”）大于电子现金单笔交易限额（如果存在，标签“9F78”），则卡片应准备返回可用脱机消费金额（如支持的话），并请求联机处理：

- 如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’），则卡片应计算可用脱机消费金额（标签“9F5D”），等于 CTTAUL（或者是 CTTAL，如果 CTTAUL 不存在）减去 CTTA，然后在 GPO 响应中返回该值；
- 设置 CVR 的第 3 字节第 6 位为‘1’（频度检查计数器超过）；
- 完成联机交易，具体步骤见 7.7.16 。

——如果授权金额（标签“9F02”）大于电子现金余额（标签“9F79”）减去电子现金重置阈值（标签“9F6D”），则卡应准备返回可用脱机消费金额（如支持取回），并请求联机处理：

- 如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’），则卡片应计算可用脱机消费金额（标签“9F5D”），等于 CTTAUL（或者是 CTTAL，如果 CTTAUL 不存在）减去 CTTA，然后在 GPO 响应中返回该值；
- 设置 CVR 的第 3 字节第 6 位为‘1’（频度检查计数器超过）；
- 完成联机交易，具体步骤见 7.7.16 。

——如果授权金额（标签“9F02”）加上 CTTA 大于 CTTAUL/CTTAL（标签“9F54”），则卡片应准备返回可用脱机消费金额（如支持取回），并请求联机处理：

- 如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’），则卡片应计算可用脱机消费金额（标签“9F5D”），等于 CTTAUL（或者是 CTTAL，如果 CTTAUL 不存在）减去 CTTA，然后在 GPO 响应中返回该值；
- 设置 CVR 的第 3 字节第 6 位为‘1’（频度检查计数器超过）；
- 完成联机交易，具体步骤见 7.7.16 。

7.7.12.3 终端仅脱机

当终端仅支持脱机时（终端交易属性，第1字节第4位=‘1’），如果授权金额（标签“9F02”）大于电子现金余额，或者授权金额大于电子现金单笔交易限额，或者授权金额加上CTTA大于CTTAUL（或者是CTTAL，如果CTTAUL不存在），则卡片应准备返回可用脱机消费金额（如果支持的话），并拒绝交易，且：

——如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’），则卡片应计算可用脱机消费金额（标签“9F5D”），等于 CTTAUL（或者是 CTTAL，如果 CTTAUL 不存在）减去 CTTA，然后在 GPO 响应中返回该值；

——设置 CVR 的第 3 字节第 6 位为‘1’（频度检查计数器超过）；

——拒绝交易，具体步骤见 7.7.18 。

7.7.12.4 交易被允许脱机完成

如果前面步骤都不符合，则卡片应：

——保存 CTTA 当前值；

——保存电子现金余额当前值；

——将交易防拔位（内部卡片指示器）设置为‘1’来指示计数器正在被更新。这个指示器只有在最后一条读记录命令响应之前才被重置为‘0’。防拔保护，具体步骤见 7.4.1 ；

——计算新的 CTTA 等于 CTTA 加上授权金额（标签“9F02”）；

——计算新的电子现金余额，等于电子现金余额减去授权金额（标签“9F02”）；

——如果允许返回可用脱机消费金额（卡片附加处理的第 1 字节第 1 位=‘1’），则卡片应计算可用脱机消费金额（标签“9F5D”），等于 CTTAUL（或者是 CTTAL，如果 CTTAUL 不存在）减去 CTTA，然后在 GPO 响应中提供该值；

——请求脱机批准；

——完成脱机交易，具体步骤见 7.7.15 。

7.7.12.5 流程图

小额和 CTTA 检查处理流程见图 12 所示。

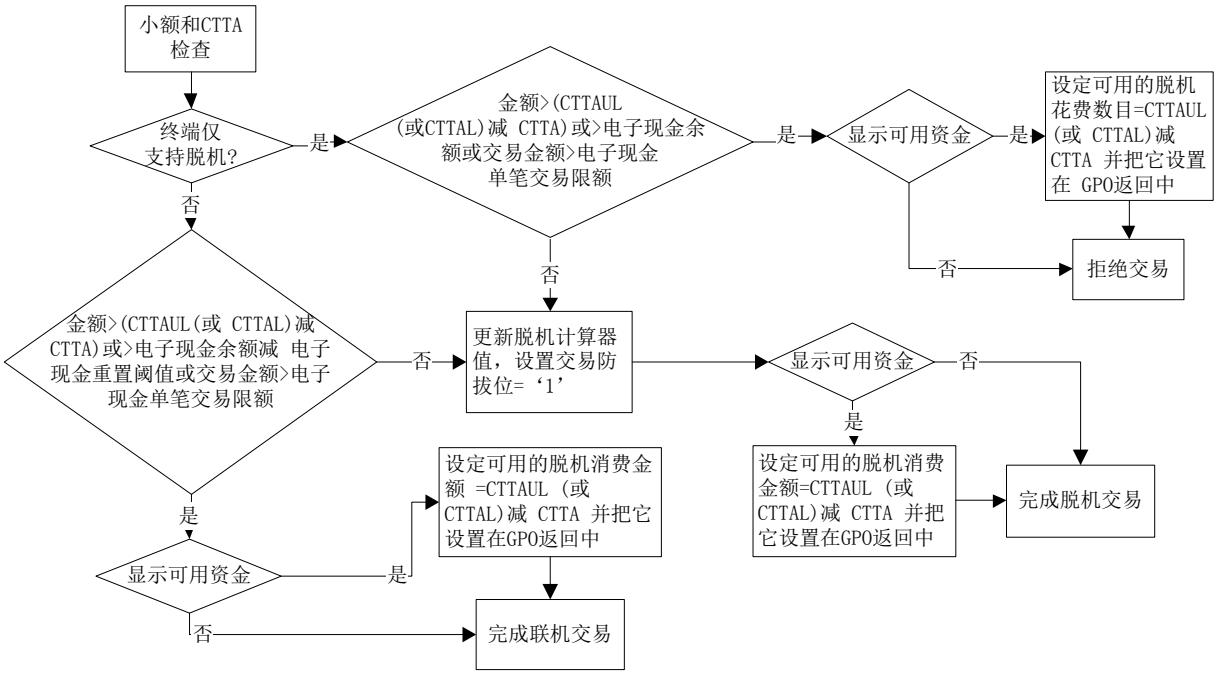


图12 小额和 CTTA 检查处理流程

7.7.13 小额或 CTTA 检查

JR/T 0025—2018不再支持此检查。

7.7.14 脱机下的货币不匹配

如果应用货币与交易货币不匹配，要检查这些交易的上限是否超额。7.7.6 已讲述了货币检查，如果货币不匹配：

——如果连续交易计数器（国际—货币）小于连续脱机交易限制数（国际—货币）（标签“9F53”），

那么卡片应：

- 存储连续交易计数器的当前值（国际）；
- 设置交易防拔保护状态，以指示计数器正被更新。该状态在最后一个读记录响应前被清除。防拔保护，具体步骤见 7.4.1 ；
- 连续交易计数器（国际—货币）加 1；
- 请求脱机批准；
- 完成脱机交易，具体步骤见 7.7.15 。

——如果前面的条件不满足，且仅脱机终端位=‘0’，那么卡片应请求联机处理：

- 将 CVR 第 3 字节第 6 位置为‘1’（频度检查计数器超过）；
- 完成联机交易，具体步骤见 7.7.16 。

——如果前面的条件不满足，且仅脱机终端位=‘1’，那么卡片应请求拒绝交易：

- 将 CVR 第 3 字节第 6 位置为‘1’（频度检查计数器超过）；
- 拒绝交易，具体步骤见 7.7.18 。

脱机下货币不匹配处理流程见图 13 所示。

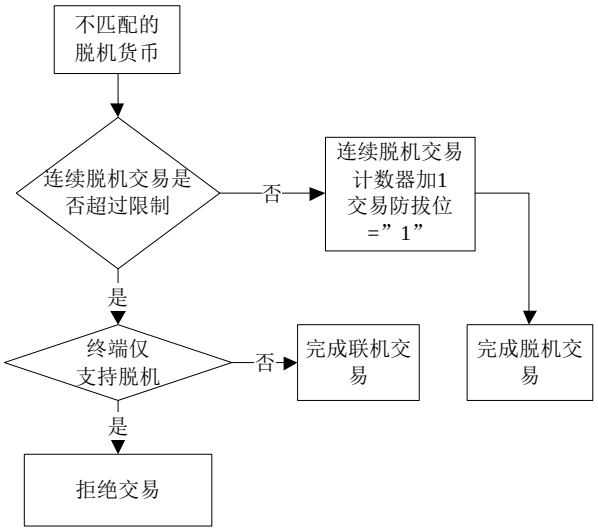


图13 不匹配的脱机货币

7.7.15 完成脱机交易

交易可脱机完成。在GPO响应中提供可供终端读取的附加数据指针和批准密文。

卡片应：

——生成动态应用数据签名（SDAD—标签“9F4B”）：

- 如果终端支持“01”版本的 fDDA（终端交易属性第 4 字节第 8 位为‘1’），则应生成 4 个字节的不可预知数，并按照附录 B 执行 “01” 版本的 fDDA；
- 如果终端不支持“01”版本的 fDDA（终端交易属性第 4 字节第 8 位为‘0’），则根据附录 B，执行 “00” 版本的 fDDA。

——在 GPO 响应中返回一个指示 fDDA 所需数据的 SFI 和记录号的 AFL，注意并非所有借记/贷记必备数据（如 CDOLs）都要存在于 AFL 标识的记录中；

——卡片应将密文信息数据（“9F27”）第 8—7 位及 CVR 字节 2 的第 6—5 位置为“01”，以指示一个脱机批准密文，按密文版本 01 生成应用密文。密文 17 用跟密文 01 同样的方式生成，但是使用不同的卡片和终端数据元作为密文输入；

——卡片应根据 7.4 建立 GPO 响应；

——结束 qPBOC 卡片的 GPO 处理，具体步骤见 7.7.19 。

完成脱机交易处理流程见图 14 所示。

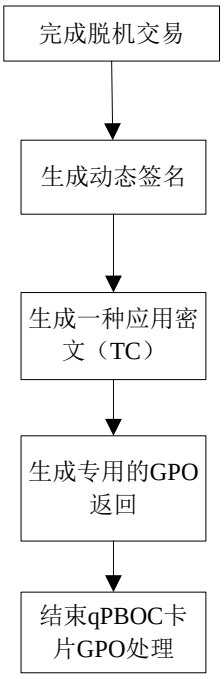


图14　完成脱机交易

7.7.16　完成联机交易

7.7.16.1　完成联机交易开始

在完成联机交易开始时，卡片应检查卡片附加处理第1字节第2位，以判断是否应进入接触式借记贷记交易，如果该位为1：

——如果终端也支持接触借记/贷记（终端交易属性第1字节第5位），那么卡片应终止非接触式交易，具体步骤见7.7.17　；

——如果终端不支持接触式借记/贷记，那么应继续完成联机交易，见7.7.16.2。

7.7.16.2　继续完成联机交易

卡片应：

——根据密文版本 01，卡片产生应用密文（ARQC）。密文版本 17 和密文版本 01 的生成方式相同，但是作为密文输入的卡片和终端的数据元不同；

——如卡片支持联机授权交易的脱机数据认证功能（CAP 的第 4 字节的第 6 位是 1）且终端支持联机授权交易的脱机数据认证功能（TTQ 的第 1 字节的第 1 位是 1），那么卡片应生成动态签名，并根据表 11 中的数据元返回数据：

- 生成签名格式为“95”的应用数据签名（SDAD—标签“9F4B”）：
  - 如果终端支持“01”版本的 fDDA（终端交易属性第 4 字节第 8 位为‘1’），则按照附录 B 执行 “01” 版本的 fDDA；
  - 如果终端不支持“01”版本的 fDDA（终端交易属性第 4 字节第 8 位为‘0’），则根据附录 B，执行 “00” 版本的 fDDA。
- 在 GPO 响应中返回一个指示 fDDA 所需数据的 SFI 和记录号的 AFL，注意并非所有借记/贷记必备数据（如 CDOLs）都要存在于 AFL 标识的记录中。

——卡片应将密文信息数据（“9F27”）第 8—7 位及 CVR 中的位置为‘10’，指示一个 ARQC，然

后根据 7.4 所描述的将密文和相关数据包含 GPO 响应中（注意对于联机交易，AFL 不返回）；

——发卡行个人化卡片时，如果要求在发卡行应用数据（标签“9F10”）的发卡行自定数据中提供可用脱机消费金额，那么卡片应包括该信息以便联机授权，见附录 D；

——如果允许返回可用脱机消费金额（卡片附加处理，第 1 字节第 1 位=‘1’），而且匹配货币位=‘1’，那么卡片应在 GPO 响应中包含这些数据；

——结束 qPBOC 卡的 GPO 处理，具体步骤见 7.7.19 。

7.7.16.3 流程图

完成联机处理流程见图 15 所示。

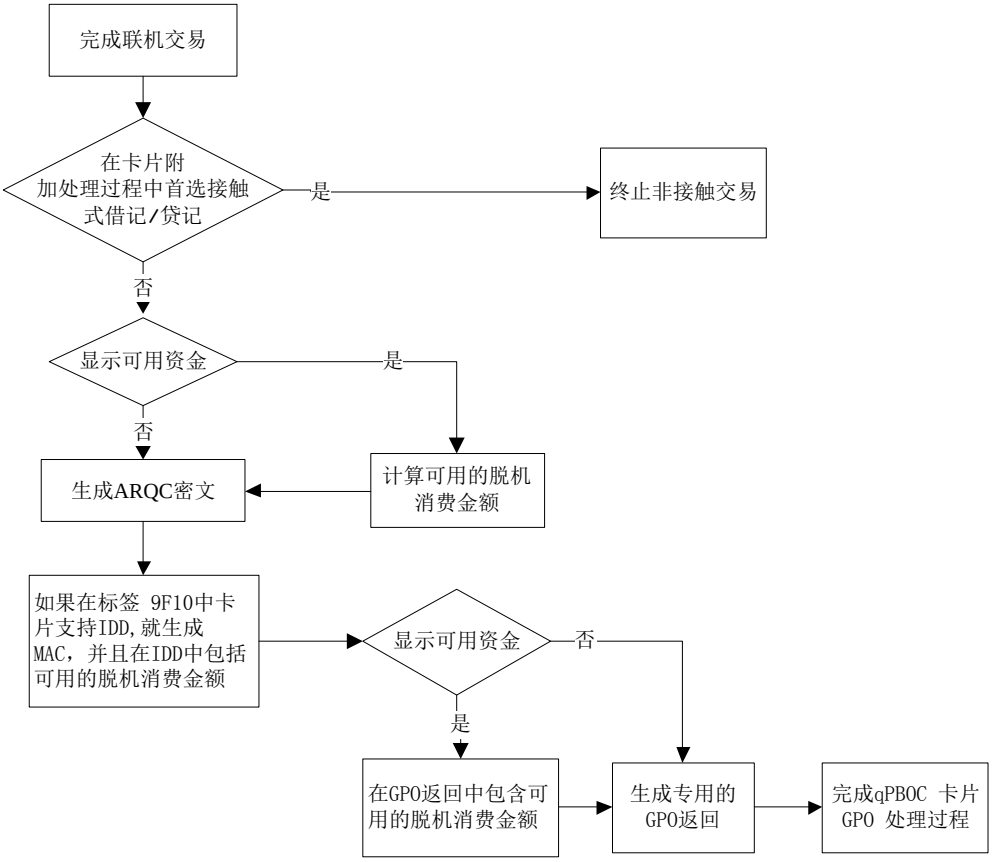


图15 完成联机交易

7.7.17 终止非接触式交易

卡片已请求终止非接触式交易。在GPO响应中返回错误代码：SW1 SW2=x“6985”。

7.7.18 拒绝交易

终端在仅脱机且脱机交易因为超出脱机交易上限不能完成时，应拒绝交易，相关要求如下：

——如果返回可用脱机消费金额位=‘1’，那么卡片应在 GPO 响应中包含可用脱机消费金额；

——卡片应将密文信息数据（“9F27”）第 8—7 位及 CVR 中的位置为“00”，指示一个 AAC 密文，生成 AAC 密文，然后根据 7.4 所描述的，在 GPO 响应中包括 CVR 和密文以及相关数据；

——密文根据密文版本 01 产生。密文版本 17 跟密文版本 01 的生成方式相同，但是作为密文输入的卡片和终端的数据元不同；

——结束 qPBOC 卡的 GPO 处理，具体步骤见 7.7.19 。

7.7.19 结束 qPBOC 卡的 GPO 处理

卡片按7.4.2 所述，格式化GPO命令响应并返回给终端。

7.8 qPBOC 终端处理要求

7.8.1 通用要求

当终端接收到来自卡片的正确的GPO命令响应，终端将继续进行读数据处理、处理限制检查、脱机数据认证，持卡人认证，最后根据密文信息数据（标签“9F27”）来确定卡片提供的密文类型。如果未返回密文信息数据（标签“9F27”），则根据发卡行应用数据（标签“9F10”）进行判断。根据密文类型，判断交易拒绝、联机处理或脱机批准。

终端在上述终端处理过程中不对终端状态结果（TVR）置位，以确保用于生成ARQC的TVR与最后联机上送的TVR的值保持一致。

终端所支持的持卡人身份认证方式应包括但不限于联机PIN，签名和CDCVM。

7.8.2 读数据处理

如果卡片在GPO命令的响应数据中返回了AFL，则交易将继续进行。

在读数据处理阶段，终端应：

——对AFL中的每一条记录都发送READ RECORD命令；

——为了提高交易的运行速度，应按照AFL中的顺序读取卡片记录；

——卡片不会知道终端是否成功接受到最后一条READ RECORD命令的响应。这意味着中断仍可能发生，而一旦发生，将会不正常影响脱机可用余额。出现这种情形的时间窗已经减小到最小。如果脱机数据认证检查失败，终端仍可拒绝交易，但这对于真正的卡很少发生。如果终端支持闪卡处理机制，且终端判断出终止交易是因闪卡造成的，可尝试参见附录F中提示的机制进行处理。

在读数据处理阶段，卡片应：

——知道最后一条记录被读取；

——在响应最后一条 READ RECORD 命令前，卡片应清除交易防拔保护状态；

——在响应最后一条 READ RECORD 命令前，卡片应检查卡片附加处理（9F68）第 2 字节第 5 位，若该位为‘1’，则卡片应记录一条交易日志，记录交易日志的方法见 JR/T 0025.5—2018 第 18 章；

——一旦所有指示的记录都被读取，终端应提示持卡人和商户可将卡移开，但交易仍在处理；

——如果卡片响应 READ RECORD 命令失败，那么终端应丢弃当前交易数据并返回检测处理。

7.8.3 处理限制检查

7.8.3.1 有效期检查

如果卡片返回AFL时，当终端在获得卡片的失效日期后，应立即进行有效期的检查。如果卡片失效，终端需要检查卡片交易属性（9F6C）字节1的第4位，若该位为‘1’，则终端进行联机处理；否则终端应终止交易并提示持卡人“卡片过有效期，交易失败”。此时卡片由于没有检测到最后一条记录被读取，因此卡片的交易防拔保护状态不能被清除。在下次交易时，卡片应能恢复脱机计数器到先前的值。

在个人化时，卡片失效日期不应在最后一条记录中。

7.8.3.2 异常文件检查

如果卡片返回AFL，那么终端应执行此检查：如果终端存在终端异常文件（如果存在），且应用PAN在终端异常文件中出现，那么终端应脱机拒绝交易。

7.8.4 脱机数据认证

如果卡片返回AFL，那么终端应根据JR/T 0025.7—2018和附录B fDDA的定义验证DDA动态签名。

如果返回 TC 但 fDDA 失败，或者脱机数据认证未执行，那么终端应查询卡片交易属性：

——如果卡片交易属性第 1 字节的第 6 位=‘1’，可联机终端应通知持卡人交易正在进行，并生成给收单行的联机报文，然后用卡片提供的 TC 联机发送交易，具体步骤见 7.8.8 ；

——如果卡片交易属性的第 1 字节的第 5 位=‘1’，支持接触式借记/贷记应用的终端应终止交易并请求持卡人采用接触式借记/贷记接口，具体步骤见 7.8.10 ；

——如果以上的条件都不满足，终端应拒绝交易，也不应尝试用另外的接口进行交易，具体步骤见 7.8.9 。为了简化交易处理，在卡片个人化时，宜设置卡片交易属性的第 1 字节的第 6 位=‘0’，无需请求联机处理。

如果返回 ARQC 但 fDDA 失败，参见附录 B 的要求。

如果返回 TC 并且 fDDA 被执行并通过，那么终端应批准交易，具体步骤见 7.8.7 。

如果返回 ARQC 并且 fDDA 被执行并通过，那么终端应将交易联机发送，具体步骤见 7.8.8 。

7.8.5 持卡人身份认证

7.8.5.1 卡片未返回卡片交易属性

如果终端要求进行CVM 验证而卡片未返回卡片交易属性（Tag “9F6C”），则：

——如终端支持签名，则执行签名验证方式；

——如终端仅支持联机 PIN 和 CDCVM，则执行联机 PIN；

——如终端仅支持 CDCVM，则终端做交易拒绝处理。

7.8.5.2 卡片返回卡片交易属性

如卡片返回了卡片交易属性（Tag “9F6C”），终端应检查卡片交易属性并决定执行的CVM方法。

如果卡片交易属性要求联机 PIN（卡片交易属性第 1 字节第 8 位=‘1’），并且终端也支持联机 PIN，则终端执行联机 PIN，终端无需再检查其他卡片交易属剩余位。否则如卡片交易属性未要求联机 PIN，或终端不支持联机 PIN，则：

——如果卡片交易属性的 CDCVM 执行标识位为‘1’（卡片交易属性第 2 字节第 8 位），则：

- 如果卡片同时返回了卡片验证相关数据（Tag “9F6C”），则：
  - 如卡片验证相关数据第 6、7 字节分别与卡片交易属性第 1、2 字节匹配，则完成 CVM 处理，终端无需再查询卡片交易属性剩余位；
  - 否则（即不匹配），终端拒绝交易，并完成 CVM 处理。
- 如果卡片未返回卡片验证相关数据（Tag “9F6C”），则：
  - 如果卡片返回的密文类型为 ARQC，则完成 CVM 处理，终端不应再查询卡片交易属性剩余位（对于 qPBOC 联机交易，GPO 应答中通常不包含卡片认证相关数据。因此，终端不能确保卡片交易属性是否未被应用程序篡改。但发卡机构可通过卡片验证结果 CVR 第 2 字节第 3 位来确定 CDCVM 是否成功执行）；
  - 如果卡片返回的密文类型不是 ARQC，终端拒绝交易，并结束 CVM 处理。

——如果既未要求联机 PIN，又未执行 CDCVM，同时卡片交易属性要求签名（卡片交易属性第 1 字节第 7 位=‘1’），并终端支持签名， 则执行签名方式验证持卡人。

如果非以上所有情况，终端没有找到共同支持的 CVM，则不执行 CVM 处理。

如果终端请求了 CVM，则最后没有执行 CVM，则终端应将交易做拒绝处理。

7.8.6 密文类型检查

如果返回 ARQC（密文信息数据（标签“9F27”）的第 8—7 位=‘10’），那么终端应将交易联机发送，具体步骤见 7.8.8 。

如果返回 AAC（密文信息数据（标签“9F27”）的第 8—7 位=‘00’），那么终端应拒绝交易，具体步骤见 7.8.9 。

如果返回 TC（密文信息数据（标签“9F27”）的第 8—7 位=‘01’），那么终端应检查终端异常文件（如果存在），如果应用 PAN 在终端异常文件中出现，那么终端应脱机拒绝交易，具体步骤见 7.8.9 ，否则终端应批准脱机交易，具体步骤见 7.8.7 。

7.8.7 批准脱机交易

处理要求如下：

——终端应执行下电时序并下电；

——终端应提示持卡人和商户交易已被批准；

——如果卡（在卡片交易属性中）或终端要求一个 CVM（签名），那么终端应在收据上打印签名行；

——如果卡片提供了可用脱机消费金额，而且终端能够显示或打印，那么终端应将其显示或打印出来；

——终端应用 GPO 响应所提供的脱机批准密文和相关数据清分交易，关于密文版本 17 所需数据见附录 E。

7.8.8 终端联机处理

处理要求如下：

——终端应执行下电时序并下电；

——终端应提示持卡人和商户移开卡片，交易正在请求授权；

——终端应根据卡片返回的卡片交易属性“9F6C”决定本次交易执行的 CVM 方法；

——终端应给收单行发送一个联机授权请求报文，报文中包括卡片在 GPO 响应中提供的联机密文（ARQC）以及其他必需信息；

——在发卡行完全迁移的情况下，终端应能够提供带有基本 IC 卡交易信息的联机报文，关于支持密文版本 17 时联机报文应提供的最基本数据见附录 E；

——终端应根据发卡行的响应批准或拒绝交易；

——终端应提示持卡人和商户交易被批准或拒绝；

——如果联机交易不能完成，终端应拒绝交易并提示持卡人和商户交易被拒绝；

——如果交易被批准，那么终端应清分交易，并包括卡片 GPO 响应所提供的密文（ARQC）和相关数据，关于密文版本 17 所需数据见附录 E；

——如果终端支持联机 ODA 功能，参见附录 G 的要求；

——终端不应因发卡行返回脚本而拒绝交易。

7.8.9 终端脱机拒绝

处理要求如下：

——终端应执行下电时序并下电；

——终端应拒绝交易并提示持卡人和商户交易被拒绝；

——如果提供了可用脱机消费金额，而且终端能够显示或打印，那么终端应将其显示或打印出来；

——终端不应尝试用另外的接口进行交易。

7.8.10 脱机数据认证失败且终端终止交易

处理要求如下：

——终端应执行下电时序并下电；

——终端应终止非接触式交易。

qPBOC 终端处理流程见图 16 所示。

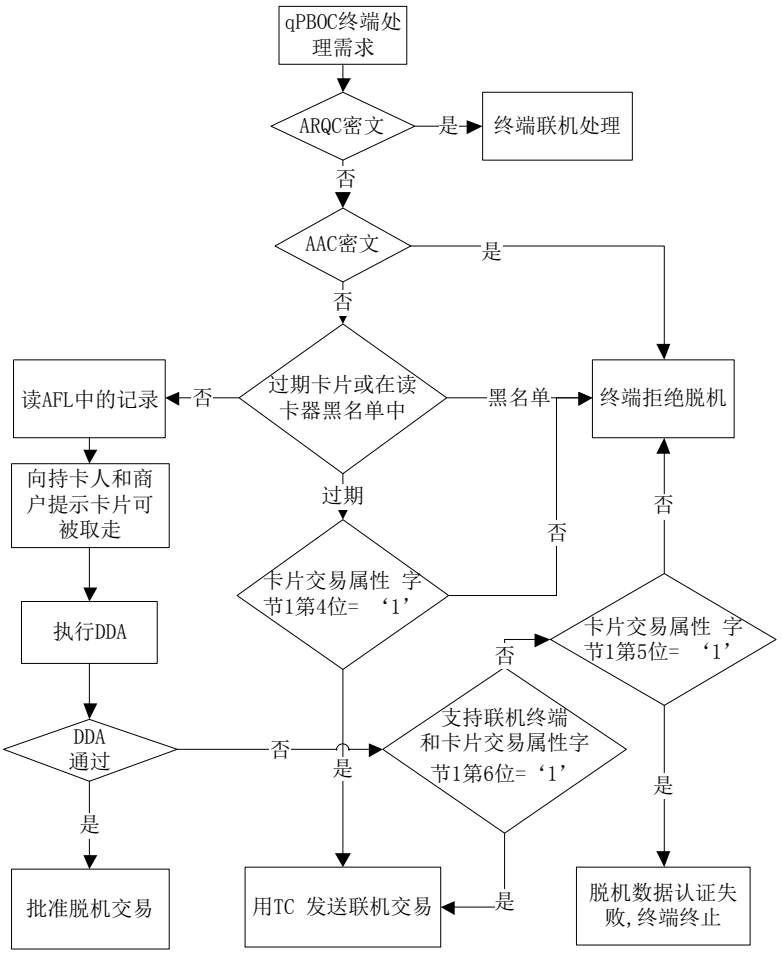


图16　qPBOC 终端处理流程

7.9　qPBOC 的简化功能

7.9.1　概述

卡片应能支持联机密文。如果支持脱机，则卡片也应支持脱机数据认证。

7.9.2　仅联机 qPBOC 的最小功能

7.9.2.1　通过流程控制实现

仅联机 qPBOC 流程是一个简化的、支持卡片侧路径，可实现并加快交易速度。 仅联机 qPBOC 流程具有下特点：

——仅联机 qPBOC 流程不支持脱机处理，卡片不对 GPO 的脱机应答进行个人化；

——GPO 命令的后续处理需要依据终端能力，当满足以下条件时，卡片按照后续要求处理，否则应返回“6985”：

- 终端交易属性（标签“9F66”）表明终端支持 qPBOC 路径（终端交易属性第 1 字节第 7 位为‘0’且第 1 字节第 6 位为‘1’）；

- 终端交易属性（标签“9F66”）表明终端具备联机能力（终端交易属性第 1 字节第 4 位为‘0’）。

——卡片执行以下风险管理：

- 若应用被锁，卡片脱机拒绝交易或 GPO 返回 SW1 SW2 = “6985”；
- 持卡人检查，若终端要求执行持卡人检查（终端交易属性第 2 字节第 7 位为 1），卡片应根据终端和卡片共同支持的持卡人验证方式选择 CVM。若终端和卡片同时支持两种方式（联机 PIN 和签名），则按优先处理联机 PIN 的方式进行处理。

——卡片应根据表 11（联机（无 ODA）或拒绝）规定的格式响应 GPO 命令，而且应包括表 11（联机（无 ODA）或拒绝）中所列的必备数据；

——卡片 qPBOC 路径应支持密文版本 17；

——仅联机 qPBOC 的 PDOL 内容应满足表 11（联机（无 ODA）或拒绝）的要求。

7.9.2.2 通过个人化参数控制实现

利用 qPBOC 流程，发卡行和收单行可通过参数设置的方法达到交易仅联机的目的。从实现上来说，由于依然采用 qPBOC 流程，并不简化个人化的工序，且依然执行所要求的风险管理步骤，因此交易速度提高较小。但无需重新个人化现有的卡片就能实现交易联机。

发卡行可通过实现下列设置中的至少一种来实现交易仅联机：

——设置电子现金余额为 0；

——设置电子现金单笔交易限额为 0；

——对于符合 JR/T 0025—2018 的卡片，设置卡片附加处理中“小额检查=0”且“小额和 CTTA 检查=0”；

——对于符合 JR/T 0025.12—2010 或 JR/T 0025.12—2013 版规范的卡片，设置卡片附加处理中“小额检查=0”且“小额和 CTTA 检查=0”。

收单行可将终端非接脱机交易最低限额设置为0来实现交易仅联机。

7.9.3 qPBOC 联机和脱机的最小功能

卡片应支持脱机数据认证并使用 fDDA。

卡片应支持小额检查。如果卡片附加处理不存在，应执行默认的小额检查，且电子现金余额和电子现金余额上限应出现在卡中。

7.10 对密文版本 17 的要求

在实现密文版本17的时候，个人化PDOL时至少要包含表13中列出的数据。

表13 PDOL 的最小数据集

PDOL中的数据标识	数据名称
“9F66”	终端交易属性
“9F02”	授权金额
“9F37”	随机数

个人化PDOL的时候，也可增加其他的数据标识，但是发卡方应明白qPBOC的终端可能不具有所有的借记/贷记终端数据。

正如前面提到的，每个应用有一个单独的PDOL。PDOL的最小数据集包含了支持所有应用路径数据的数据标签。密文版本17要求的数据标签是密文版本01要求的一个子集。每个路径应分析GPO指令中的数据，来获得进行处理所要求的信息。

卡片使用格式2来回应GPO，同时要求一个密文并返回与之相关的数据、AIP和2磁道数据。如果卡上有持卡人姓名、主账号序列号和一磁道等价数据，这些数据也会被包含在内。

7.11 非接消费交易流程

7.11.1 概述

本条规范了非接金融IC卡和移动金融近场支付消费、预授权类、联机消费反向类等非接交易流程，明确了非接读卡器场强、非接标识、终端程序远程更新的技术要求。

7.11.2 非接消费交易

7.11.2.1 非接消费交易流程

非接消费交易流程如图 17 所示。

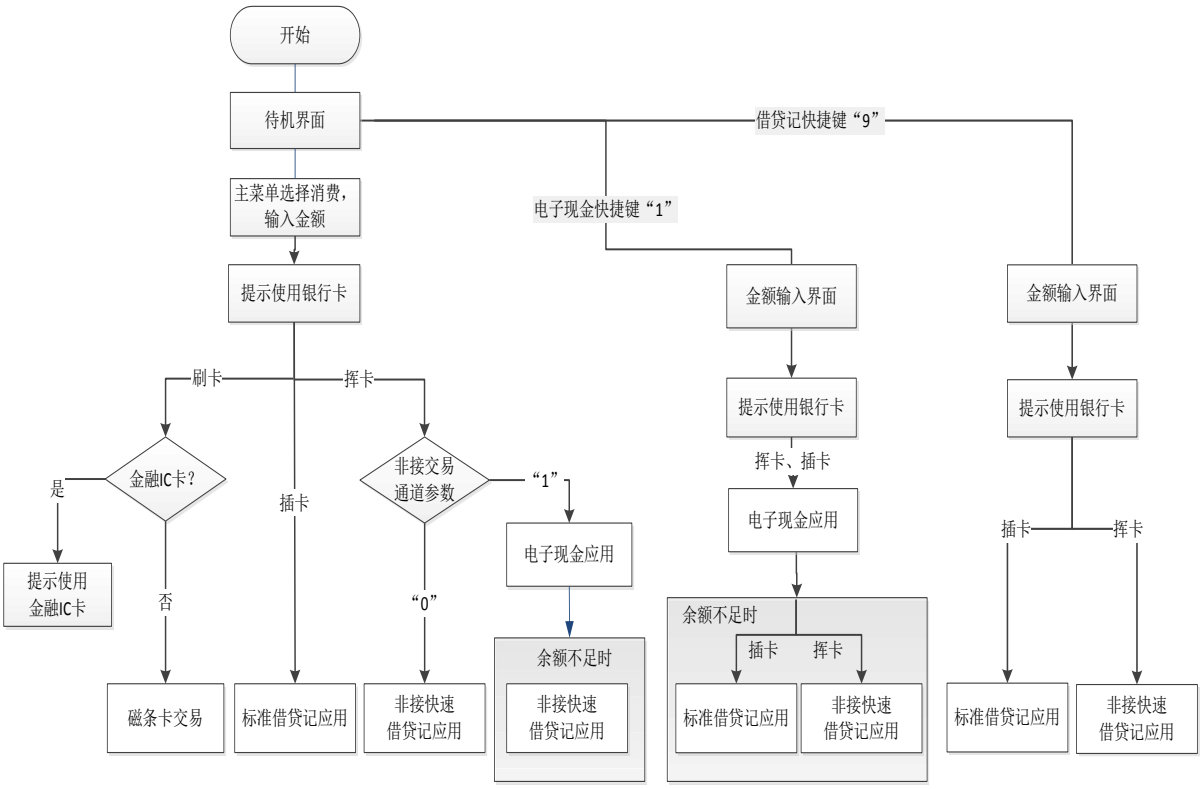


图17 非接消费交易流程

7.11.2.2 新增参数及快捷键

新增的参数及快捷键如下：

——“非接消费交易通道”参数：‘0’表示在非接触界面下交易优先采用非接快速借记/贷记应用；‘1’表示优先采用电子现金应用；

——电子现金快捷键‘1’：在 POS 待机界面，按‘1’键，进入电子现金交易流程；

——借记/贷记快捷键‘9’：在 POS 待机界面，按‘9’键，进入借记/贷记交易流程；

——“快捷受理交易开关”参数：‘1’表示消费；‘2’表示预授权。该参数适用于：判断待机界面下插卡、刷卡进入消费交易或预授权交易流程；判断按“借记/贷记快捷键‘9’”后，进入消费交易或预授权交易流程。

上述终端参数宜支持远程更新。

7.11.2.3 消费交易流程

处理要求如下：

——对于非接消费交易通道参数设置为“非接快速借记/贷记应用优先”的终端，持卡人挥卡时，终端自动采用非接快速借记/贷记交易流程，交易由借记/贷记主账户完成；

——对于非接消费交易通道参数设置为“电子现金应用优先”的终端，持卡人挥卡时，终端自动采用电子现金交易流程，交易由电子现金账户完成。若卡片电子现金余额不足，终端自动转非接快速借记/贷记交易流程，交易由借记/贷记主账户完成；

——终端待机界面按快捷键‘1’：进入电子现金交易界面，挥卡、插卡均进行电子现金交易。电子现金交易余额不足时，若挥卡则转为非接快速借记/贷记应用，若插卡则转为标准借记/贷记应用；

——终端待机界面按快捷键‘9’：进入金融 IC 卡借记/贷记交易流程，插卡采用标准借记/贷记应用；挥卡采用非接快速借记/贷记应用；

——若卡片仅支持联机借记/贷记交易（包括普通金融 IC 卡和手机内置卡片应用），在终端进行电子现金非接交易时，如终端判断卡片内无电子现金应用，自动转非接快速借记/贷记交易流程。

7.11.3 非接预授权类与联机消费反向类交易

非接预授权类交易：对于开通非接预授权类功能的 POS 终端，预授权、预授权撤销、预授权完成、预授权完成撤销交易应采用非接快速借记/贷记交易流程，并采用“先输金额，再提示用卡”操作流程。

联机消费反向类交易：对于开通联机消费反向类交易功能的 POS 终端，采用非接快速借记/贷记交易流程完成联机消费的，其撤销、退货等反向类交易应采用非接快速借记/贷记交易流程。

7.11.4 非接读卡器硬件要求

非接读卡器硬件要求如下：

——非接读卡器中心点场强要求。非接读卡器应符合相关金融行业标准，在距读卡中心点 0 厘米至 4 厘米范围内能够正确读取符合相关金融行业标准要求的金融 IC 卡及移动设备；

——非接读卡器非接标识要求。非接读卡器应具备明显的标识，标明非接读卡区域。如果读卡区域在显示屏下方，提示使用银行卡时，应在显示屏上显示非接读卡标识。非接标识应标识场强最强的场强中心点位置，场强中心点应在终端正面。

7.11.5 终端程序远程更新

收单机构宜建设终端管理系统（TMS），实现终端程序及参数远程更新功能。

7.12 qPBOC 卡片交易日志控制

卡片在默认情况下应记录所有联机请求交易、脱机批准交易的交易日志，发卡方可通过配置卡片附加处理控制卡片在非接界面下是否记录交易日志，当记录交易日志时通过应用缺省行为（ADA）字节 3（标签“9F52”）的 6—8 位，控制交易日志的记录方式：

——位 8=‘0’：脱机批准交易记录交易日志；

——位 7=‘0’：联机请求交易记录交易日志；

——位 6=‘0’：脱机拒绝不记录交易日志。

当非接触应用选择的 FCI 中未个人化交易日志入口时，卡片应不允许通过非接触界面读取交易日志，此时当卡片收到读取交易日志的 READ RECORD 命令时，应返回“6A82”。

当非接触应用选择的 FCI 中未个人化圈存日志入口时，卡片应不允许通过非接触界面读取圈存日志，此时当卡片收到读取圈存日志的 READ RECORD 命令时，应返回“6A82”。

除发卡行有特殊业务需求外，非接触界面下 FCI 信息中不应包含交易日志入口和圈存日志入口，以保证交易日志和圈存日志不在非接触界面下被读取。否则，如造成持卡人隐私泄露，由发卡行承担相应责任。

附 录 A
（资料性附录）
qPBOC 和借记/贷记应用的比较

本附录列出了qPBOC与标准借记/贷记的比较。

qPBOC的要求是与接触式借记/贷记应用不同的。对于应用选择，前两者使用PPSE而后者使用PSE。当PPSE被选择后，非接触应用的列表在Select指令的应答中被返回。在借记/贷记应用中，PSE被选择后，将使用Read Record指令来获得卡上的接触式应用列表。

借记/贷记应用中PSE的使用不是必备的（目录选择方式）。在借记/贷记应用中，AID列表的方法是必备的，而在qPBOC中，这个方法是不宜使用的。

对qPBOC而言，PDOL最好存在，并且要求提供终端数据元——终端交易属性，这个数据将指示终端支持接触式借记/贷记应用、非接触式借记/贷记应用还是qPBOC或者三者都支持。

qPBOC不遵循借记/贷记应用处理规定，也不必支持借记/贷记应用的必备数据和要求。GPO指令被用来向终端提供密文、密文数据和动态签名。

如果qPBOC支持fDDA，那么fDDA相关的数据也需要从芯片中读出。卡片应用可能同时也支持dCVN，但是对于终端而言dCVN是透明的，表A.1详细列出了qPBOC和借记/贷记应用处理。

表A.1 qPBOC 和非接触式借记/贷记应用的比较

qPBOC 终端		借记/贷记应用设备	
命令	描述	命令	描述
选择 SELECT	必备：选择 PPSE（2PAY.SYS.DDF01），无选项； 对选择 PPSE 的响应包含用于所有非接触应用的 AIDs（和有限的附加信息）； 要求 PDOL 并包括标签“9F66”最小值和用于加密的终端数据标签； 流程由本部分中图 4 描述。	选择 SELECT	接触式 PBOC； 必备：选择 AID； 选项：选择 PSE（1PAY.SYS.DDF01）； 对于目录文件读记录，目录文件是与卡内 PSE 提供的 AIDs 和应用信息相关； PDOL 可选； 流程由 JR/T 0025.5—2018 描述。
获取处理选项 GPO	终端发送数据值标签“9F66”，表示支持非接触式借记/贷记应用或 qPBOC，发送用于加密的终端数据和其他卡片要求的数据用于完成交易。 **脱机/联机（ODA）：** 对于该类交易，作为对 GPO 的响应，卡片返回密文，卡片密文数据，其他交易数据和动态签名，一个包含脱机数据认证（DDA/SDA）的 AFL 也返回。 **联机（无 ODA）：** 对于联机交易，没有 AFL 返回； 作为对 GPO 的响应，卡片返回密文，卡片密文数据。	获取处理选项 GPO	如果交易条件满足，卡片对 AFL 和 AIP 响应；如果有 PDOL 的话，终端提供卡片 PDOL 中请求的数据，而且卡片可能有其他逻辑来决定返回怎样的 AFL 或 AIP。

读记录 READ RECORD	OFFLINE： 如果 GPO 中返回的密文并非 AAC，终端读取 AFL 指出的记录。AFL 也指出哪条记录被签名用于脱机数据认证，终端检查卡片是否到失效期，如果未到失效期则执行脱机数据认证（SDA/DDA），如果失败则拒绝此交易； 如果脱机数据认证通过而且卡片未失效，则使用 GPO 中的返回密文完成交易； 脱机数据认证是兼容 JR/T 0025.6—2018 的，除非在 GPO 中产生动态签名或在读完最后一条记录后卡片不再需要保留在域中。 ONLINE： 卡片离开后，终端发送由卡片提供的密文。密文是对 GPO、联机和发卡行响应的批准或拒绝； AFL 未被返回，而且没有其他记录可被读出。	读记录 READ RECORD	设备使用 AFL 来决定读取哪条记录并读出这些记录。AFL 也指出哪条记录将被签名； 如果必备数据元素丢失，交易将被终止。
N/A	N/A	内部认证 INTERNAL AUTHENTICATE	设备检查 AIP 来确定卡片支持哪一种风险管理特性； 如果 AIP 需要支持 DDA，内部认证命令发送到卡片； 依据 JR/T 0025.6—2018 执行 DDA； 设置 JR/T 0025.6—2018 规定的指示器。
N/A	N/A	N/A	处理限制。
N/A	N/A	N/A	持卡人验证。
N/A	N/A	获取随机数 GET CHALLENGE	可选脱机加密 PIN。
N/A	N/A	校验 VERIFY	可选脱机 PIN 校验（明文或密文）。
N/A	N/A	N/A	终端风险管理。
N/A	N/A	生成应用密文（第 1 次）	脱机批准或拒绝或请求联机处理。
N/A	N/A	外部认证	如果联机处理和发卡行认证。
N/A	N/A	生成应用密文（第 2 次） Generate AC (2nd)	批准或拒绝。
N/A	N/A	发卡行脚本命令	设备发送发卡行脚本命令到卡片。

附 录 B
（规范性附录）
快速 DDA

B.1 DDA介绍

在非接触支付环境中，快速交易速度（1秒或者更低）是业务上的需要。DDA作为一种动态数据认证方法，用于脱机预防伪卡。

除了在大多数PBOC接触芯片应用中使用的不可预知数（终端）被签名外，fDDA也对其他的交易动态数据进行签名。授权金额、交易货币代码和不可预知数（卡片）在进行fDDA时都被用来签名。

卡片使用PDOL从终端获取数据用于fDDA。在GPO命令中卡片接收从读卡器请求的数据。这些终端数据元素与卡片数据一起产生动态签名。

在GPO中返回的AFL指向了包含证书和其他fDDA相关数据的记录。一旦最后一条记录被读卡器读取，卡片不需要再停留在场中。读卡器然后验证卡片返回的动态签名。如果签名验证失败，交易将根据卡片交易属性被脱机拒绝，请求联机授权或者终止。

为了适应可能出现的新fDDA算法和输入，定义了卡片数据元素fDDA版本（标签9F69的一部分）用于标识卡片使用的fDDA版本。fDDA版本号由卡片返回，读卡器使用其来决定要执行的fDDA算法。JR/T 0025.12—2010中定义的fDDA算法在JR/T 0025—2013中将其定义为“00”版的fDDA。JR/T 0025—2013中定义的fDDA算法，其版本定义为“01”。

对于符合JR/T 0025—2018的卡片应同时支持“00”和“01”两种版本的fDDA，具体使用的版本应根据终端能力（终端交易属性中指明）来决定。

对于符合JR/T 0025—2018的读卡器应同时支持“00”和“01”两种版本的fDDA。在GPO命令中，读卡器应向卡片表明支持“01”版本fDDA的能力（终端交易属性第4字节第8位为‘1’）。

对于版本“01”的fDDA，卡片应将从读卡器GPO命令中取得的不可预知数（终端）、授权金额、交易货币代码，连接上卡片ATC和卡片认证相关数据共同用于动态签名的计算。

B.2 动态签名的产生

数据的连接和动态签名的产生与JR/T 0025.7—2018中第5章一致，以下内容除外：

——对于联机授权交易中的 ODA 签名，IC 卡动态签名应使用签名格式“95”，见表 B.1；

——对于脱机批准交易中的 ODA 签名，IC 卡动态签名仍使用签名格式“05”；

——对于支持联机 ODA 的终端，在进行联机 ODA 的动态签名验证过程中，终端应支持使用签名数据格式“95”进行数据验证。对于传统金融 POS 终端（不支持联机 ODA），在动态签名验证过程中，如签名数据格式不是“05”，则动态数据认证失败（对于基于主机模拟技术（HCE）的移动支付产品，除了在签名数据格式时候使用 95 用于与传统脱机授权交易进行区分之外，IC 卡公钥证书中证书格式应使用 94 用于区别基于 SE 的 IC 卡/移动支付产品。对于支持联机 ODA 的行业终端应支持 94 和 04 两个值）。

表 B.1 从签名的动态数据恢复的数据格式（联机 ODA）

字段名	长度	描述	格式
恢复数据头	1	十六进制，值为‘6A’。	b
签名数据格式	1	十六进制，值为‘95’。	b

字段名	长度	描述	格式
哈希算法标识	1	标识用于在数字签名方案中产生哈希结果的哈希算法。	b
IC 卡动态数据长度	1	标识 IC 卡动态数据的字节长度。	b
IC 卡动态数据	L_{DD}	由 IC 卡生成和/或存储在 IC 卡上的动态数据。	—
填充字节	N_{IC}—L_{DD} - 25	（N_{IC}—L_{DD} - 25）个值为‘BB’的填充字节。	b
哈希结果	20	动态应用数据以及相关信息的哈希值。	b

终端动态数据元素不在DDOL中指定（DDOL对于qPBOC是一个不可识别的数据）。JR/T 0025.7—2018中第5章表16或表30中的终端动态数据应由表B.2指定的数据元素按顺序连接构成。如果任何要求的数据元素缺失，则fDDA失败。

在把卡片认证相关数据包含在终端动态数据之前，卡片应产生并填充不可预知数（卡片）和卡片交易属性到卡片认证相关数据中。

注：如果卡片交易属性没有被个人化，则使用数值“0”替代，被用于卡片认证相关数据中。

IC卡动态数据应包含表B.3中的内容。

表 B.2　用于输入 DDA 哈希算法的终端动态数据

标签	数据元素	长度	数据来源	版本“00”	版本“01”
9F37	不可预知数	4 字节	终端	√	√
9F02	授权金额	6 字节	终端		√
5F2A	交易货币代码	2 字节	终端		√
9F69	卡片认证相关数据	可变	卡片		√

表 B.3　用于输入 DDA 哈希算法的 IC 卡动态数据

标签	数据元素	长度	数据来源	版本“00”	版本“01”
9F36	应用交易计数器（ATC）	2 字节	卡片	√	√

B.3　动态签名的验证

为验证fDDA动态签名，读卡器应先后恢复出CA公钥、发卡行公钥和IC卡公钥。这一过程见JR/T 0025.7—2018中第5章。

验证动态签名过程与JR/T 0025.7—2018中第5章一致，以下内容除外：

——终端根据卡片返回的卡片认证相关数据（标签“9F69”）决定使用的 fDDA 签名算法；如未返回，则视为使用“00”版本的 fDDA 签名算法；卡片认证相关数据是变长数据，读卡器应使用卡片返回的整个卡片认证相关数据进行动态签名认证；

——输入哈希算法的终端动态数据元素不在 DDOL 中指定（DDOL 对于 qPBOC 是一个不可识别的数据），而是由表 B.1 指定的数据元素按顺序连接构成。终端可将表 B.1 指定的标签理解为“01”版本的 fDDA 缺省的 DDOL。

在下列情况，fDDA应失败：

——应用交互特征（AIP）指示卡片不支持 DDA（AIP 字节 1 第 6 位为‘0’）；

——支持 fDDA，但是支持 fDDA 所要求数据缺失；

——卡片请求的 fDDA 版本读卡器不支持。“00”版 fDDA 和“01”版 fDDA 是本部分所支持的 fDDA 版本；

——如终端支持“01”版本的 fDDA（终端交易属性第 4 字节第 8 位为‘1’），且卡片返回的应用版本号（标签“9F08”）标明卡片支持“01”版本的 fDDA，但是却返回了“00”版本的 fDDA 签名。

快速DDA（fDDA）qPBOC示例见图B.1所示。

图 B.1　快速 DDA（fDDA）qPBOC 示例

相关处理流程如下：

——终端选择 PPSE；

——卡片返回唯一借记/贷记 AID；

——终端选择借记/贷记 AID；

——卡片返回请求：

- 终端交易属性（标签“9F66”）；
- 不可预知数（标签“9F37”）；
- 授权金额（标签“9F02”）；
- 交易货币代码（标签“5F2A”）；
- 其他 PDOL 中指定的标签。

——终端发出 GPO，提供：

- 标签“9F66”指明仅支持 qPBOC；
- 标签“9F37”不可预知数；
- 标签“9F02”授权金额；
- 标签“5F2A”交易货币代码；
- 其他 PDOL 中指定的标签。

——卡片响应：

- 交易证书（TC）；
- 动态签名；
- 同脱机数据认证（fDDA）相关的 AFL 列表记录；
- 其他和 fDDA 无关的数据。

——终端读取 AFL 指定的记录；

——卡片提供证书和数据，用来认证静态数据的签名，同时卡片认证相关数据被添加在最后一条记录中返回（如果卡片已被个人化为支持“01”版本的 fDDA），此时卡片可离开通讯区域；

——终端认证动态签名；

——如果 fDDA 认证通过，终端提供清算信息：

- 交易证书（TC）；
- 相关数据。

——如果fDDA认证失败，交易被拒绝、终止或者根据发卡行设置发送联机请求。

附 录 C
（规范性附录）
数据元

C.1 名字

该数据元的名字。

C.2 格式、标签与长度

格式、标签与长度的要求如下：

——数据元的格式遵守 JR/T 0025.5—2018 的 A.1；

——数据元的标签是十六进制的表示数据元的唯一编码，标签的使用应遵守 JR/T 0025.5—2018 的 A.3；

——数据元的长度值用十进制表示。

C.3 共享性

Y：表示该数据元同时也在标准借记/贷记流程中被使用，无论是标准借记/贷记流程完成的交易还是 qPBOC 流程完成的交易都会影响该数据元。

N：表示该数据元只在 qPBOC 中使用。

C.4 要求

要求列表示该数据元在 qPBOC 中存在的条件是必备、有条件或是可选，并指明该数据元是卡片数据还是终端数据。

C.5 获取

获取列指明该数据元是否能被终端读取，或通过命令返回。若能，给出读取的命令。获取列中“SD”表示数据元是只可在专门的设备上获取。

C.6 值

该数据元各位的取值见表 C.1。若无特别说明，取值被设置为预留（字节或比特位），应被置为 0。

表 C.1　数据元

名字	格式 标签 长度	共享性	要求	描述	获取	值
可用脱机消费金额 Available Offline Spending Amount	F：n 12 T：“9F5D” L：6	N	可选卡片数据元	一个计算区域，用来允许终端打印或显示卡内的可用的脱机交易额度，除非此标签被个人化为‘1’，否则卡片将不会允许此标签被包括在可被终端读出的记录中或对GPO 的响应中； 对于此数据的个人化并不影响其包含在发卡行定义数据中。	GET DATA GPO READ RECORD	如果个人化的值大于零，对此数据元的获取数据（GET DATA）操作被允许； 如果此数据元被个人化为‘1’并且卡片应用处理（第1字节第1位）有值为‘1’，则此数据元包含在GPO中，并且允许读记录（READ RECORD）； 此数据元可以通过读记录指令（READ RECORD），也可以通过GPO读出。
卡片附加处理 Card Additional Processes	F：b 32 T：“9F68” L：4	N	条件卡片数据元如果支持脱机，并且是小额选项而不是默认值或没有卡片风险管理选项所支持。	指出卡片处理需求和参数选择。	GET DATA (SD)	详见表12卡片附加处理； 此标签应可被 PUT DATA 命令修改。
卡片CVM限额 Card CVM Limit	F：n 12 T：“9F6B” L： 6	N	可选卡片数据元	如果出现表示当卡片和终端货币类型匹配且一个非接触交易超过这个值，则需要由卡片提供CVM。 本部分定义	GET DATA (SD)	此标签应可被 PUT DATA 命令修改。

名字	格式 标签 长度	共享性	要求	描述	获取	值
				的持卡人验证是联机PIN和签名。		
卡片内部指示器 Card Internal Indicators	F：b 16 T：- L：2		必备卡片内部数据元	用于控制卡片内部过程。	N	字节1 位8 中断 位7 脱机只支持终端 位6 匹配货币
卡片交易属性 Card Transaction Qualifiers	F：b 16 T：“9F6C” L：2	N	可选卡片数据元	在本部分中用于向设备指明卡片要求哪一个CVM。	GET DATA (SD)，GPO	此标签应可被 PUT DATA 命令修改。 字节1 位8 1= 需要联机PIN 位7 1= 需要签名 位6 1= 如果脱机数据认证失败而且终端可联机则要求联机 位5 1= 如果脱机数据认证失败而且终端支持 PBOC 则终止 位4 1= 如果应用过期，则交易联机 位3~1 保留 字节2 位8 1=执行 CDCVM（该位不适用于标准卡片交易） 位7~1 保留
应用交互特征 Application Interchange Profile (AIP)	F：b 16 T：“82” L：2	N，与标准借记/贷记流程使用的AIP是分开的	必备卡片数据元	说明此应用中卡片支持指定功能的能力。	GPO	字节1 位8 RFU 位7 1= 支持SDA 位6 1= 支持DDA 位5 1= 支持持卡人验证 位4 1= 支持终端风险管理 位3 1= 支持发卡行认证 位2 1= RFU 位1 1= 支持CDA 字节 2 位8 = 0（该位曾被用于磁条数据标识位，因此，有部

名字	格式 标签 长度	共享性	要求	描述	获取	值
						分存量卡可能有该位置1的情况） 位 7~1 RFU
密文信息数据 Cryptogram Information Data(CID)	F：b 8 T：“9F27” L：1	N	必备卡片数据元	表明卡片返回的密文类型并指出终端要进行的操作。	GPO	位 8－7： 00=AAC 01=TC 10=ARQC 11=AAR 位 6－5：RFU（00） 位 4：1=需要通知 位 3－1(原因/通知/授权参考码)： 000=无信息 001=不允许服务 010=PIN 尝试次数超过 011=发卡行认证失败 xxx=RFU 本数据在应用初始化时置为‘00’
上次联机应用交易计数器（ATC）寄存器 Last Online ATC Register	F：b 16 T：“9F13” L：2	Y	可选卡片数据元（如果执行新卡检查）	上次联机上送交易时的ATC值。	GET DATA	
非接触终端脱机最低限额 Terminal Contactless Floor Limit	F：n 12 T：－ L：6	N	可选终端数据元	指示终端中的非接触最低限额。	N/A	
非接触终端交易限额 Terminal Contactless Transaction Limit	F：n 12 T：－ L：6	N	可选终端数据元	如果非接触交易的数值大于或等于此数值，则交易终止允许在其他界面尝试此交易。	N/A	

名字	格式 标签 长度	共享性	要求	描述	获取	值
终端执行CVM限额	F：n 12 T：- L：6	N	可选终端数据元	如果非接触交易超过此值，终端要求一个持卡人验证方法（CVM）； 联机PIN和签名是本部分定义的持卡人验证方法（CVM）。	N/A	
终端交易属性 Terminal Transaction Qualifiers	F：b 32 T：“9F66” L：4	N	必备终端数据元	指示终端能力，要求和对卡片的参数选择。	N/A	详见表3终端交易属性（标签“9F66”），不应在READ RECORD命令中返回。
电子现金余额 Electronic Cash Balance	F：n 12 T：“9F79” L：6	Y（基于借记/贷记的小额支付流程使用）	可选卡片数据元	如果授权金额超过了电子现金余额，则所有交易应通过联机授权或脱机拒绝。	GET DATA	此标签应可被PUT DATA命令修改。
电子现金余额上限 Electronic Cash Balance Limit	F：n 12 T：“9F77” L：6	Y（基于借记/贷记的小额支付流程使用）	可选卡片数据元	如果授权金额加上电子现金余额超出此限制，卡片要求联机处理。	GET DATA (SD)	此标签应可被PUT DATA命令修改，不应在READ RECORD命令中返回。
电子现金重置阈值 EC Reset Threshold	F：n 12 T：“9F6D” L：6	Y（基于借记/贷记的小额支付流程使用）	可选卡片数据元	如果授权金额大于电子现金余额减去此阈值，则卡片要求联机处理。	GET DATA	此标签应可被PUT DATA命令修改，不应在READ RECORD命令中返回。
电子现金单笔交易限额 EC Single Transaction Limit	F：n 12 T：“9F78” L：6	Y（基于借记/贷记的小额支付流程使	可选卡片数据元		GET DATA (SD)	此标签应可被PUT DATA命令修改，不应在READ RECORD命令中返回。

名字	格式 标签 长度	共享性	要求	描述	获取	值
		用）				
电子现金发卡行授权码 EC Issuer Authorization Code	F：a 6 T：“9F74” L：6	Y（基于借记/贷记的小额支付流程使用）	可选卡片数据元	电子现金交易或 qPBOC 脱机批准的交易，卡片应返回此数据元。	READ RECORD	
应用版本号 Application Version Number	F：b16 T：“9F08” L：2	Y	必备数据元	支付系统给应用分配的版本号。同 JR/T 0025.5—2018 中的定义。	READ RECORD	由支付系统定义。
卡片认证相关数据 Card Authentication Related Data	F：b T：“9F69” L：var 8—16	N	可选卡片数据元 如果支持“01”或以上版本的 fDDA。	如果卡片执行的是“01”或以上版本的 fDDA，则该数据应在最后一条记录中返回；否则该数据不应在记录中出现。	READ RECORD	在 JR/T 0025—2018 中，卡片认证相关数据使用 8 个字节长度，并且被个人化到卡片中。 字节 1：fDDA 版本号（在 JR/T 0025—2018 中为“01”） 字节 2—5：卡片不可预知数 字节 6—7：卡片交易属性 字节 8：RFU（00），具体使用方法不在本部分定义。
用户专用数据 Customer Exclusive Data	F：b T：“9F7C” L：var 1—32		可选卡片数据元	包含发送到发卡方的数据。	GPO，READ RECORD	此标签应可被 PUT DATA、UPDATE RECORD 命令修改。 由一个或多个发卡方元素组成，每个元素由一个字节的专有标识、一字节长度、内容组成，JR/T 0025—2018 目前定义的标识： “01”—发卡方专有标识 “02”—“FF”—RFU 既可在 GPO 响应中返回，也可在 ReadRecord 中返回。

名字	格式 标签 长度	共享性	要求	描述	获取	值
主账号参考号 Payment Account Reference	F：ans T：“9F24” L：29		如果应用主账号为支付标记，则存在。	PAR 由卡组织（具有BIN管理权的机构）分配以及管理。	GPO READ RECORD	
行业应用扩展标识 Industrial Application Extension Label	F：b8 T：DF61 L：1		如果卡片支持行业应用，发卡行在 BFOC 中进行个人化，支持取数据（Get Data）和设置数据（Put Data）命令。	用于区别卡片支持扩展应用的能力。	SELECT DATA（在文件控制信息（FCI）中发卡行自定义数据 BFOC 中返回）	位 7:1=卡片支持联机 ODA 功能（存量终端不应由于无法识别 DF61 中新增标识位而拒绝交易）。 其他位的定义见 JR/T 0025.14—2018。

注：在本部分中引用而没有在借记/贷记应用中定义的或经修改的数据元在本附录中定义。

附 录 D
（规范性附录）
“9F10”中的发卡行自定义数据

D.1 发卡行自定义数据选项

为了使得发卡行可在主机端更紧密地跟踪资金，引入了在发卡方应用数据（“9F10”）的发卡行自定义数据部分中允许加入特殊数据的选项。对于借记/贷记交易，这一数据通过Generate AC的应答提供给终端，并联机发送给发卡行。对于qPBOC交易，这一数据通过GPO指令的应答提供给终端，并联机发送给发卡行。

累计交易总金额、在CTTA基础上增加的累计交易总金额限制（CTTAL）、电子现金余额、可用脱机消费金额和能够个人化不超过15个字节的静态数据，是发卡行可选择联机发送的5个数据选项，发卡行可在这5个选项中选择任意一个联机发送。同时如果该数据存在，在发送的指令中会被加上校验码，以保证数据完整性。

D.2 发卡行自定义数据的个人化

如果存在发卡行自定义数据（IDD），应在发卡行应用数据（标签“9F10”）中的自定义数据之后被返回。

发卡行自定义数据（IDD）根据表D.1中描述的在个人化时选择的选项不同，会有所变化。

表 D.1 发卡行任意数据（IDD）

发卡行自定义数据选项	长度（字节）	IDD ID	金额域	MAC 字节数
电子现金余额	10	0x01	标签“9F79”的值（低 5 位字节）	4
累计交易总金额（CTTA）	10	0x02	值，此数据无标签（低 5 位字节）	4
电子现金余额和 CTTA	15	0x03	值（10 字节，“9F79”值在第 1 位置）	4
CTTA 和 CTTAL	15	0x04	值（10 字节，CTTA 值在第 1 位置）	4
可用脱机消费金额	10	0x05	标签“9F5D”的值（低 5 位字节）	4
预留给第 14 部分	保留	0x06	保留	4
卡组织保留	保留	0x07	保留	保留
静态	1 to 15	N/A	发卡行指定固定数据	无

发卡行自定义数据（IDD）的 ID 值用于选择在发卡行自定义数据域中返回的数据的类型。缺省的情况下，发卡行自定义数据不会被返回。如果发卡行希望收到发卡行自定义数据，在“9F10”个人化值中，需要添加以上相应的数据的长度和标示符字节（在借记/贷记应用的自定义数据之后）。

例如，0x0A02表示在生成交易密文的指令应答中，将返回10个字节的发卡行自定义数据，包括数据类型标示符（0x02），累计交易总额和校验码。返回电子现金余额的选项，只有当应用被个人化为电子现金的时候才会有效。

D.3 发卡行应用数据个人化案例

借记/贷记自定义数据（必备）

长度： 0x 07

取值： 0x 01100300000001（假设密文版本号为 10）

发卡行自定义数据

长度： 0x 0A（在 GENERATE AC 指令的应答中期待的返回值的长度）

取值： 0x 02（请求 CTTA 的 ID 值）

以上案例的 TLV 值

9F10 0A

07 01100300000001

0A 02

卡片上的应用使用个人化的发卡行自定义数据的长度和ID（0x0A02），当对第1次生成应用密文返回联机密文请求时，激活内部代码，从而在发卡行自定义数据中提供累计交易总额的一个指示器。

D.4 生成应用密文返回的发卡行应用数据

借记/贷记自定义数据

长度： 0x 07

取值： 0x 01100300000001（例子）

发卡行自定义数据

长度： 0x 0A

取值： 0x 02（ID）累计交易金额（5 个字节）

验证码：4个字节，解释见D.5

D.5 校验码的计算

被进行校验码计算的数据包括2个字节的应用交易计数器，加上一或两个5字节的金额域和补位字符0x00，具体数据构成规则如表D.2所示：

对发卡行自定义数据ID选项为0x01，数据为8字节，包含应用交易计数器、电子现金余额和一个字节的补位。

对发卡行自定义数据ID选项为0x02，数据为8字节，包含应用交易计数器、CTTA金额和一个字节的补位。

对发卡行自定义数据ID选项为0x03，数据为16字节，包含应用交易计数器、电子现金余额、CTTA和四个字节的补位。

对发卡行自定义数据ID选项为0x04，数据为16字节，包含应用交易计数器、CTTA、CTTAL和四个字节的补位。

对发卡行自定义数据ID选项为0x05，数据为8字节，包含应用交易计数器、可用脱机消费金额和一个字节的补位。

四字节的校验码是通过从MAC UDK分散得来的过程密钥计算得来的。密钥分散方法和MAC计算方法见JR/T 0025.7—2018。

表 D.2 MAC 计算

IDD ID 选项	数据块长度	元素	
0x01	8 bytes	ATC 电子现金余额 填充	2 字节 低 5 位字节 1 字节

IDD ID 选项	数据块长度	元素	
0x02	8 bytes	ATC CTTA 金额 填充	2 字节 低 5 位字节 1 字节
0x03	16 bytes	ATC 电子现金余额 CTTA 填充	2 字节 低 5 位字节 低 5 位字节 4 字节
0x04	16 bytes	ATC CTTA CTTAL 填充	2 字节 低 5 位字节 低 5 位字节 4 字节
0x05	8 bytes	ATC 可用脱机消费金额 填充	2 字节 低 5 位字节 1 字节

附 录 E
（规范性附录）
密文版本 17

密文版本17使用和密文版本01相同的算法和参数，不同点是不支持密文版本01要求的所有数据。表E.1列出了根据需要的顺序排列的密文版本17要求的数据。

表 E.1 包含在密文版本 17 中的数据元

标签	数据元	来自终端的数据	由卡片输入
“9F02”	授权金额*	✓	
“9F37”	不可预知数	✓	
“9F36”	应用交易计数器（ATC）		✓
“9F10”	发卡行应用数据（字节 5） 根据 PBOC 定义，字节 5 是 CVR 的第 1 个数据字节，CVR 的固定长度为“03”。 只有字节 5 是参与密文运算的，但是发卡行应用数据的前 8 个字节应在报文中出现。对于 qPBOC 联机交易，发卡行自定义数据（IDD）可能被包括。 字节 1 -“07” 字节 2 - DKI 字节 3 - 密文版本号 字节 4 -“03” 字节 5 - CVR bits 位 8—7 “10” bits 位 6—5 “00” (AAC) “01” (TC) “10” (ARQC) “11” RFU bits 位 4—1 “0000” 字节 6 -“00000000” 如果 PIN 尝试超限，频度检查超限或卡片为新卡，位 7，6 和 5 可能被设置。 字节 7 -“00000000” 字节 8 - 算法标识 字节 9 - Length of IDD 字节 10—23 - IDD		✓

对于 qPBOC，终端到收单机构的报文中含有这些数据。收单机构将这些数据装入报文中的 55 域。

应用密文和表 E.1 中的数据应出现在终端到收单机构的报文中，以及收单机构到交换中心的认证清算报文中。

附 录 F
（资料性附录）
电子现金“闪卡”处理机制

F.1 电子现金交易闪卡介绍

在非接电子现金脱机消费时，发生卡片内的金额已扣除但终端交易未成功的现象，通常称为“闪卡”。其原因为卡片已返回最后一条记录，但终端未收到，导致卡片扣款，终端交易未成功。

当笔闪卡重挥处理时间（T1）：指当终端发生闪卡交易，在T1时间内，终端通过语音或“蜂鸣提示配以屏幕显示”等方式，明确告知持卡人“请重新挥卡”以完成当笔闪卡交易。T1默认取值10秒，收单机构可视实际应用场景进行调整。

当笔闪卡交易处理流程：指当终端发生闪卡交易，在T1时间内，终端对当笔闪卡交易的处理流程。若当笔闪卡交易处理成功，则终端打印签购单并上送成功的电子现金交易报文；若当笔闪卡交易处理失败，则终端保留当笔闪卡交易信息，并转入“全部闪卡交易处理流程”。

闪卡记录可处理时间（T2）：指当终端发生闪卡交易，且当笔闪卡交易处理流程失败，则在T2时间内，可在后续电子现金交易中继续处理该笔闪卡交易。T2默认取值60秒，收单机构视实际应用场景进行调整。

全部闪卡交易处理流程：指当终端发生闪卡交易，且当笔闪卡交易处理流程失败，则终端保留当笔闪卡交易信息，在T2时间内的电子现金交易中继续处理闪卡交易。若在T2时间内处理闪卡交易成功，则终端打印签购单并上送成功的电子现金交易，若终端处理闪卡交易失败，则终端上送失败交易记录，并在终端本地删除相应的闪卡记录。

F.2 电子现金交易闪卡处理要求

F.2.1 终端技术要求

终端技术要求如下：

——终端在发生交易异常时，应以语音或“蜂鸣提示配以屏幕显示”等方式提示重新挥卡，界面和指示灯配合提示。其中，在无人值守终端宜采用语音提示；

——终端应支持参数设置可保存的闪卡记录数，最少 1 条，最多 3 条（默认值）；

——终端读取卡片最后一条记录失败时，如已获取卡片电子现金余额，则终端应立即保存闪卡记录，保存失败交易记录，进入“当笔闪卡交易处理流程”；如终端未获取卡片电子现金余额，则按原有方式提示交易失败；

——发生闪卡后，终端进入“当笔闪卡交易处理流程”，即通过要求持卡人重新挥卡，处理当前刚发生的一笔闪卡交易。在超过 T1 或按“取消”键时，回到初始界面，进入“全部闪卡交易处理流程”，对所有闪卡记录进行匹配和处理；

——终端应支持 T1 参数的配置，参考取值为 10 秒，收单机构视实际应用场景进行调整。对于无人值守终端，特别是交易速率快、人流量大的场景（如闸机类终端设备），宜减小 T1 取值；

——终端应支持 T2 参数的配置，对于有人值守终端（如超市、食堂等）或消费金额固定的无人值守终端（如公交），参考取值为 60 秒；对于消费金额不固定的无人值守终端（如自助售货机），参考取值为 10 秒。收单机构可视实际应用场景进行调整。终端应删除超过 T2 的闪卡记录。

F.2.2 卡片技术要求

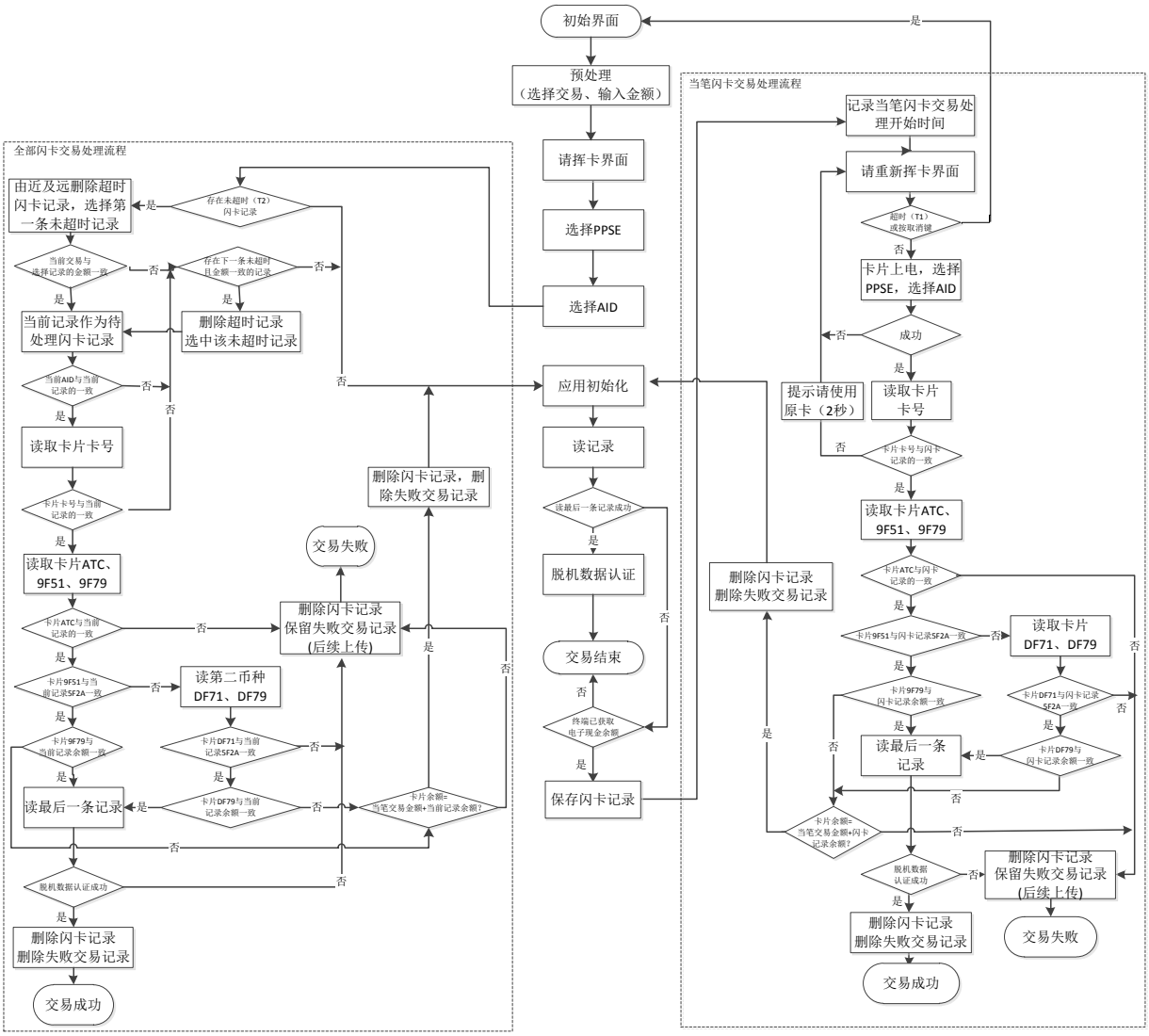
卡片技术要求如下：

——如卡片收到读最后一条记录的指令，应确保保存最后一条记录的数据，在卡片重新上电并完成应用选择后，终端可获取该最后一条记录；

——如卡片未收到读最后一条记录的指令，在卡片重新上电并完成应用选择后，卡片应立即删除上一次交易的记录数据，该操作与卡片防拔回滚应为一个原子操作。

F.3 电子现金交易闪卡处理流程

电子现金扩展应用的闪卡处理可参考图F.1所示流程。



注 1：当笔闪卡交易处理过程中，在读取数据失败（如卡号、ATC、9F51、9F79 等）时，如未超T1 则退回重新挥卡界面；如T1 超时则保留闪卡记录和失败交易记录，回到初始界面。

注 2：全部闪卡交易处理过程中，在读取数据失败（如卡号、ATC、9F51、9F79 等）时，界面提示读卡失败，回到终端初始界面，闪卡记录和失败交易记录均无变化。

图 F.1 电子现金非接消费闪卡处理流程

对于当笔闪卡交易处理，终端提示持卡人重新将卡片放置在非接感应区，终端将卡片的卡号、应用交易计数器、应用货币代码、电子现金余额等要素与终端保存的闪卡记录进行比较，并做相应处理。对于全部闪卡交易处理，持卡人将卡片放置在非接感应区时，终端将卡片的卡号、应用交易计数器、应用货币代码、电子现金余额等要素与全部闪卡记录逐一比较，并做相应处理。具体流程如图F.1所示。

附 录 G
（资料性附录）
联机 ODA 技术实施指南

G.1 实施要点

G.1.1 适用范围

G.1.1.1 终端及渠道范围

适用于经过特定改造的，支持联机ODA功能的非接触式终端。仅涉及线下渠道。

G.1.1.2 卡片范围

适用于支持qPBOC联机ODA功能或非接触式借记/贷记应用的卡片（包括纯芯片卡、磁条芯片复合卡和消费者设备）。借记卡和贷记卡均支持联机ODA功能。

G.1.1.3 交易类型范围

适用于通过非接触式方式读取IC卡信息，使用qPBOC或非接触式借记/贷记流程，以联机方式发起的在特定行业及商户进行的自助消费等交易。

G.1.1.4 商户范围

联机ODA仅适用于金额小、对交易速度有较高需求或不具备长期实时联机环境的场景，如地铁、公交、停车场等，且要求商户具备一定资质。

G.1.1.5 交易场景范围

适用于商户与持卡人面对面发起的现场有卡消费业务，以及持卡人通过自助终端发起的有卡自助消费业务。

G.1.2 交易处理场景

交易处理场景如下：

——终端发起交易，或持卡人操作自助终端确认交易信息；

——持卡人在终端非接感应区附近挥卡；

——脱机数据认证以及其他相关检查通过后，终端给出成功提示，商户向持卡人提供商品或者服务；

——终端将相关交易数据进行留存。终端应与后台系统相连，并在一定时间内将交易数据上传至后台系统；

——后台系统应在规定时限内完成对交易数据的处理，并将交易数据上传至交换系统，该系统对交易数据按照一定规则进行检查处理后发起联机交易处理；

——对请款失败等满足黑名单规则的情况，将相应卡号加入黑名单并更新至所有终端。终端将拒绝黑名单内的卡片再次发起交易。

G.1.3 交易处理参考要求

G.1.3.1 交易数据上传期限要求

考虑到金融交易的时效性，商户原则上应尽快通过后台系统上传交易数据至交换系统，发起联机交易。

对于首次扣款失败的交易，在一定时限内将尝试多次扣款，直至扣款成功或超过时限。考虑到风险敞口以及业务开展的需要，应设置最大上传期限。

G.1.3.2 交易处理基本要求

发卡银行对于收到的联机ODA交易，不校验交易顺序（ATC计数器）、不比对交易实际发生时间与报文上送时间、不比对交易授权金额与实际结算金额；对于尚未取得成功应答的延迟请款交易，收单系统可在原交易发生日起一定期限内，多次发起延迟请款、直至取得成功应答。

信用卡发卡银行宜根据本行授权与风控逻辑，对联机ODA交易提供一定幅度的超额授信服务。

发卡银行应根据交易验证逻辑进行检查，且对其他交易信息进行验证，对验证通过的，应给予成功交易应答。

对于实体卡账户处于挂失、冻结或注销等异常状态下，收单机构上送的联机ODA交易，发卡银行应根据卡片状态拒绝交易。

G.1.3.3 交易限额要求

考虑到联机ODA业务主要应用于小额交易场景，收单机构宜根据实际业务需求设置单笔交易限额，同时设置合理的单卡日累计交易限额，以减少风险敞口。

G.1.3.4 防重复交易要求

终端应有相关机制防止重复交易。

G.1.3.5 交易凭证要求

商户及收单机构可不打印、不保留交易凭证。

收单机构应保存交易流水等电子凭证，保存期至少为一年。

G.1.3.6 退货处理要求

对于商户不打印交易凭证的，商户不得以无交易凭证为理由拒绝持卡人的退货请求。退货时以商户保存的交易流水为退货凭证。

G.1.3.7 支付信息安全管理要求

支付信息安全管理要求如下：

——采集支付信息应遵循“业务必须”和“最小化”原则，不得收集与所提供服务无关的支付信息；

——从行业终端采集磁道信息（或芯片中等效磁道信息）时应进行加密保护，包括但不限于使用安全芯片实现硬加密。该信息仅用于完成银行卡交易，不得用于除此之外的任何其他用途；

——行业终端仅限于保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除；

——应加强支付信息保护，信息保护要求应依据国家和行业有关规范实施。

G.2 技术要点

G.2.1 应用系统架构

应用系统架构如图G.1所示。

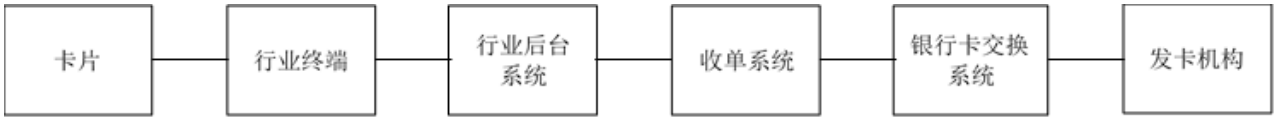


图 G.1　应用系统架构图

行业终端处理要求如下：

——按照 JR/T 0025—2018 与卡片进行交互；

——收集并保存联机交易所需交易数据及交易要素；

——按照商户要求进行相应检查；

——与行业后台系统通信并进行数据传输。

行业后台系统处理要求如下：

——与行业终端通信并进行数据传输；

——数据汇总与相关处理；

——与交换系统通信并进行数据传输。

收单系统处理要求如下：

——交易合规性检查（预防重复上送交易与超期上送交易）；

——发起延迟请款交易。

银行卡交换系统进行转接清算处理。

发卡行进行交易授权处理。

G.2.2　交易阶段概述

G.2.2.1　第一阶段：卡片与终端交互阶段

行业终端应在联机交易时进行脱机数据认证验证卡片真伪，并在验证成功以及其他相关检查通过后对相关交易数据进行留存。

G.2.2.2　第二阶段：延迟联机请款阶段

行业终端应在一定时间内将留存的相关交易数据上传至行业后台系统，由行业后台系统上送交易至银行卡交换系统完成请款。

G.2.3　卡片与终端交互技术方案

G.2.3.1　综述

不同的卡片类型与终端交互的流程不相同，现将卡片分为两类。

第一类为不支持联机ODA功能的已发行存量卡片。可通过非接触式借记/贷记应用流程进行交互，完成终端对卡片的真伪判断及联机授权交易请求。

第二类为支持联机ODA的新增卡片，包括芯片卡和消费者设备。卡片可通过qPBOC流程进行交互，从而实现终端对卡片的真伪判断及联机授权交易请求。

G.2.3.2　存量卡

G.2.3.2.1　存量卡的识别

终端根据SELECT AID返回的FCI信息，使用BF0C中的DF61（行业应用扩展标识）中的保留位（第1字节第7位）来识别是否为存量卡。如果select命令返回的DF61未置位或未返回DF61，则说明该卡为存量卡。

G.2.3.2.2 存量卡与终端交互流程

存量卡与终端交互流程如下：

——终端对卡片发出 SELECT AID/SELECT PPSE 指令进行应用选择；

——卡片返回 FCI 信息，DF61 第 1 字节第 7 位为 0 或不返回 DF61；

——终端将 tag 9F66 第 1 字节第 7 位置 1（非接 PBOC），进入非接触式借记/贷记应用流程并执行脱机数据认证；

——终端根据脱机数据认证结果对卡片真伪进行判断，若脱机数据认证失败则为伪卡，则拒绝交易；

——若脱机数据认证成功，则认定卡片为真卡，终端判断卡片是否按要求返回了 ARQC，若未返回 ARQC，则拒绝交易；

——当确认卡片已按要求返回 ARQC 后，终端可执行新卡检查；

——将卡号与黑名单进行比对，若卡号在黑名单中，则拒绝交易；

——终端可根据行业商户要求，进行其他检查，若不通过，则拒绝交易；

——在通过各项检查后，交易成功，终端对联机交易数据以及相关交易要素进行留存。

具体如图 G.2 所示。

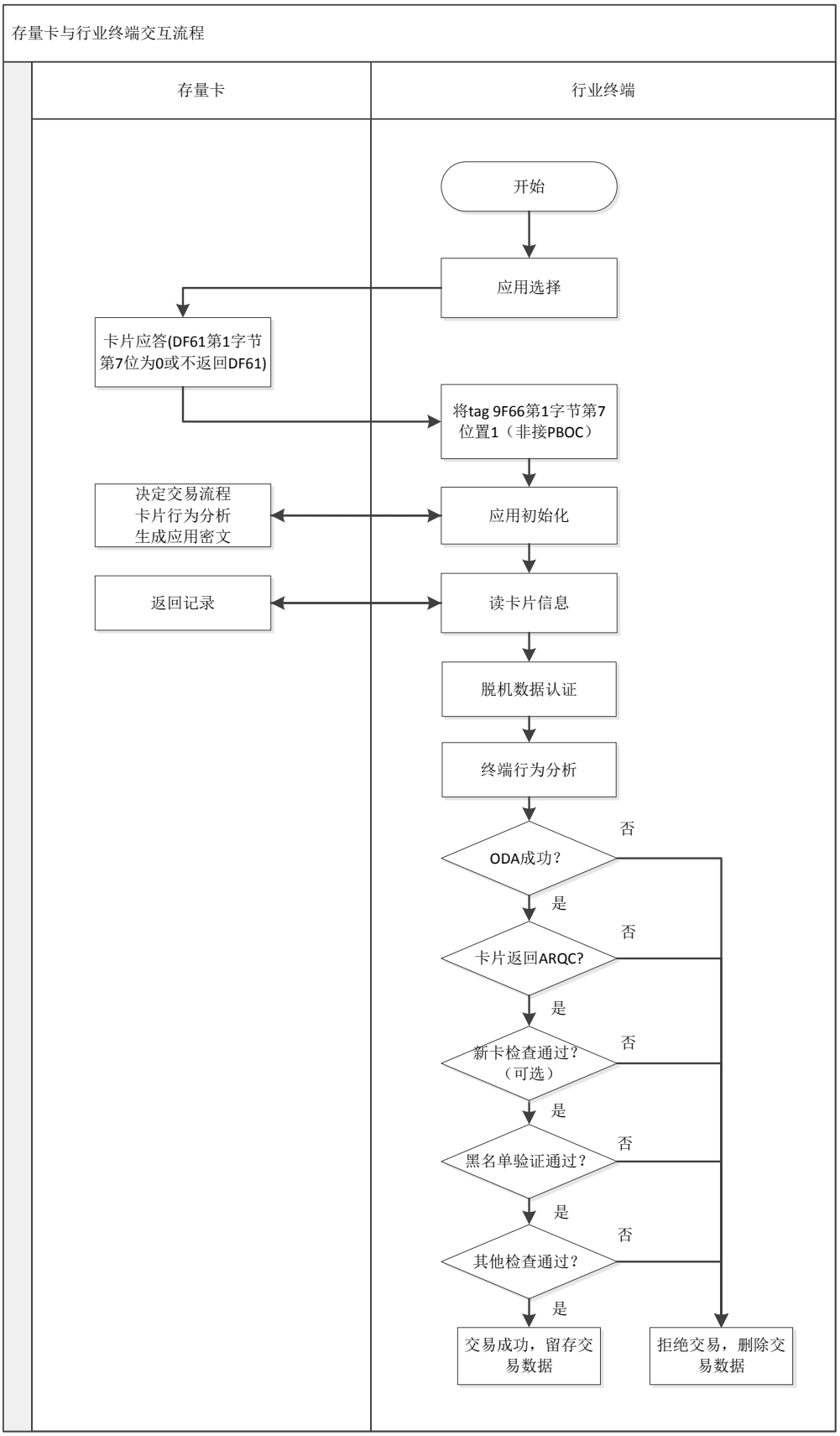


图 G.2　存量卡与行业终端交互流程

G.2.3.3 新增卡

G.2.3.3.1 新增卡的识别

终端根据SELECT AID返回的FCI信息，使用BF0C中的DF61（行业应用扩展标识）中的保留位（第1字节第7位)来识别是否为新增卡。如果select命令返回的DF61已置位，则说明该卡为新增卡，支持qPBOC流程进行联机ODA交易。

若行业终端有识别特定消费者设备的需求，则终端可根据卡片GPO应答中的tag 9F63中特定位的值进行识别，并进入相应流程进行处理。

G.2.3.3.2 新增卡与终端交互流程

新增卡与终端交互流程如下：

——终端对卡片发出 SELECT AID/SELECT PPSE 指令进行应用选择；

——卡片返回 FCI 信息，DF61 第 1 字节第 7 位置为‘1’；

——终端将 tag 9F66 第 1 字节第 7 位置‘0’（qPBOC）、第 1 字节第 1 位置‘1’（联机 ODA）、第 1 字节第 6 位置‘1’、第 2 字节第 8 位置‘1’（要求联机），进入 qPBOC 流程；

——卡片返回 AFL，终端使用 READ RECORD 读取相应数据，并执行脱机数据认证；

——终端根据脱机数据认证结果对卡片真伪进行判断，若脱机数据认证失败则为伪卡，则拒绝交易；

——若脱机数据认证成功，则认定卡片为真卡，终端判断卡片是否按要求返回了 ARQC，若未返回 ARQC，则拒绝交易；

——当确认卡片已按要求返回 ARQC 后，终端可执行新卡检查；

——将卡号与黑名单进行比对，若卡号在黑名单中，则拒绝交易；

——终端可根据行业商户要求，进行其他检查，若不通过，则拒绝交易；

——在通过各项检查后，交易成功，终端对联机交易数据以及相关交易要素进行留存。

具体如图 G.3 所示。

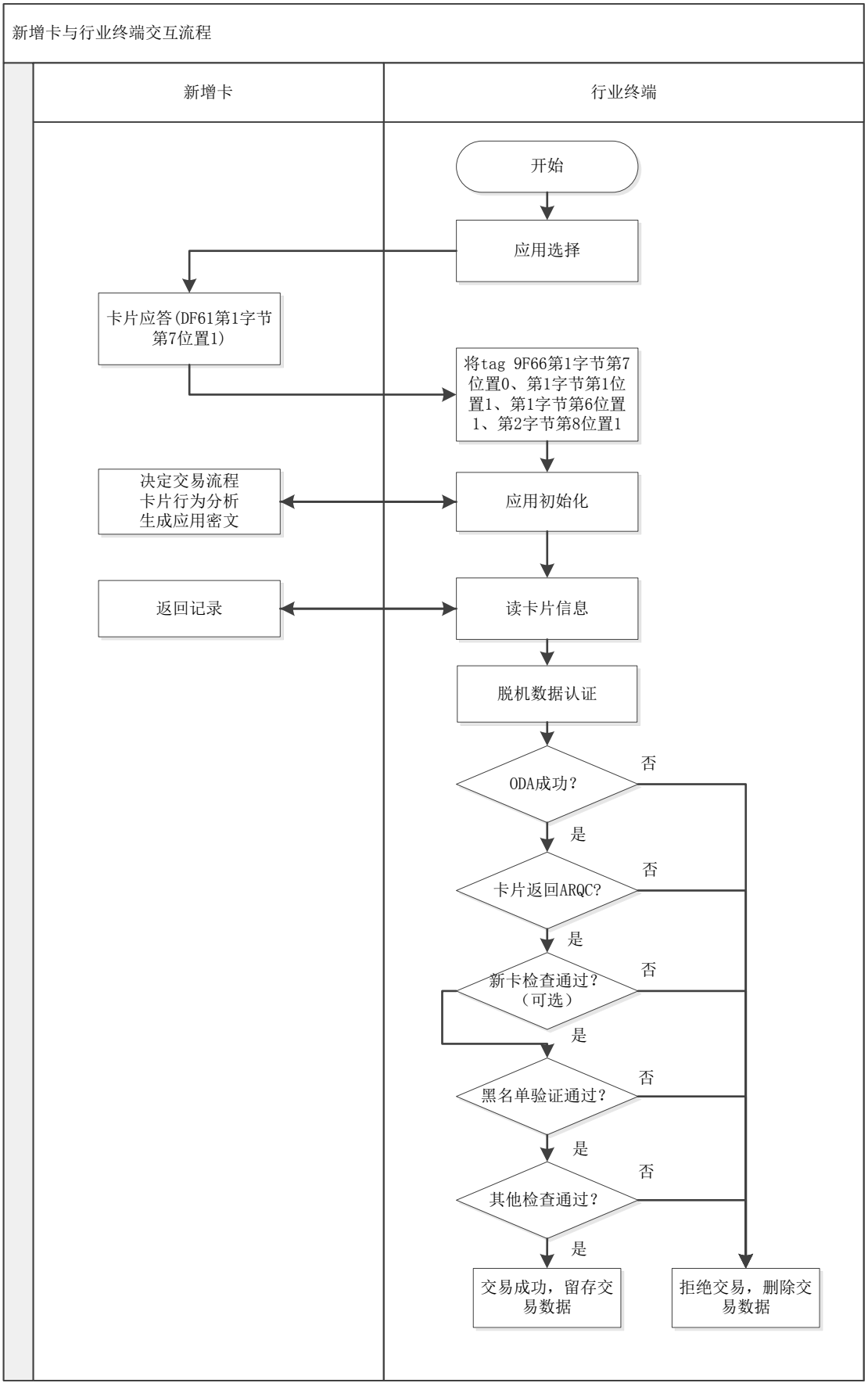


图 G.3　新增卡与行业终端交互流程

G.2.4 技术改造要点

G.2.4.1 卡片启用DF61新标识位标明支持联机ODA功能

启用BF0C中的DF61（行业应用扩展标识）中第1字节第7位（原保留位）来表示是否支持联机ODA功能。对于支持联机ODA功能的卡片将该位设置为1。数据元定义见附录C。

注1：联机 ODA 交易流程中卡片脱机数据认证与现有 qPBOC 脱机交易中脱机数据认证保持一致，包括卡片使用同一套 AFL 进行交易。

注2：卡片个人化时应确保 DF61 第 1 字节的第 7 位和 9F68 第 4 字节第 6 位保持一致。

G.2.4.2 卡片附加处理

卡片附加处理（tag 9F68）采用第4字节的第6位来标识卡片是否支持qPBOC联机授权交易的脱机数据认证功能。若为支持联机ODA的新卡，则卡片附加处理（CAP Tag 9F68）的第4字节的第6位“支持联机授权交易的脱机数据认证”应设置为1。

G.2.4.3 卡片返回数据元要求

对于qPBOC联机带脱机数据认证的交易，即当卡片支持联机授权交易的脱机数据认证功能（CAP的第4字节的第6位是1）且终端支持联机授权交易的脱机数据认证功能（TTQ的第1字节的第1位是1），那么卡片应在GPO响应中返回本部分表11中的数据元。

G.2.4.4 联机ODA签名和验证要求

内容见附录B。

G.2.4.5 终端改造方案

终端或其后台系统应具备联网能力，且终端应支持qPBOC，即终端交易属性（“9F66”）字节1的第4位应置0，第6位置1。如终端不支持电子现金交易，则“终端非接脱机交易最低限额”应设置为0。

终端应支持 qPBOC 联机交易的脱机数据认证功能，且应具备通过参数设置方式来开启和关闭这一功能的能力。当功能开启时，且终端判断卡片 DF61 支持联机 ODA 后，终端交易属性（TTQ Tag 9F66）的第 1 字节的第 1 位“支持联机授权交易的脱机数据认证”应设置为 1。

参 考 文 献

[1] EMV 支付系统集成电路卡规范[S/OL]. 4.3