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 0025.12—2013
代替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

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

2013-02-05 发布　　2013-02-05 实施

中国人民银行 发布

目　　次

前　言

JR/T 0025《中国金融集成电路（IC）卡规范》分为以下部分：

——第1部分：电子钱包/电子存折应用卡片规范（废止）；

——第2部分：电子钱包/电子存折应用规范（废止）；

——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9部分：电子钱包扩展应用指南（废止）；

——第10部分：借记/贷记应用个人化指南；

——第11部分：非接触式IC卡通讯规范；

——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；

——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17部分：借记/贷记应用安全增强规范。

本部分为JR/T 0025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—2012《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》。

本部分与JR/T 0025.12-2010相比主要变化如下：

——修订了标准的前言；

——删除了所有MSD的相关内容；

——删除了授权金额为零时，卡片必须请求联机的要求，以兼容新增补的qPBOC扩展应用；

——将原规范各章条中“PBOC应用”更改为更确切的描述“借记/贷记应用”；

——将交易日志由不记录更改为发卡机构可选地记录；

——卡片联机GPO响应数据中新增了9F63的要求，以适应不断增长的使用需求；

——将第7.7.13节中计数器增长与比较的方法做出修正，使之与JR/T 0025.5的描述保持一致；

——明确了GPO响应应遵循JR/T 0025.5中的格式2；

——明确了9F10中发卡行自定义数据的要求；

——明确了附录C.1中的TAG的取得及修改方式；

——明确了qPBOC脱机交易最后一条记录的长度；

——修订了原规范中一些排版及文字描述上的勘误。

——将原fDDA签名方法定义为“00”版本，新增了“01”版本的fDDA签名方法。新增了卡片认证相关数据（标签“9F69”）在“01”版fDDA中参与签名，并标识两种版本的fDDA。

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、中国工商银行、中国银行、中国建设银行、中国农业银行、交通银行、上海浦东发展银行、中国邮政储蓄银行、中国银联股份有限公司、中国金融电子化公司、银行卡检测中心、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。

本部分主要起草人：王永红、李晓枫、陆书春、潘润红、杜宁、陈则栋、吴晓光、李春欢、刘志刚、张永峰、汤沁莹、李新、张栋、王红剑、李一凡、余沁、周新衡、张步、冯珂、李建峰、向前、涂晓军、齐大鹏、俞益宁、曾静静、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。

本部分所代替标准的历次版本发布情况为：

JR/T 0025.12—2010。

引　言

本部分为JR/T 0025的第12部分，与JR/T 0025.8和JR/T 0025.11一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/T0025.8和JR/T 0025.11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

JR/T 0025的本部分描述了非接触式IC卡应用，在快速借记/贷记非接触式支付应用（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接受的金融非接触式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 0025.3 中国金融集成电路（IC）卡规范 第3部分：与应用无关的IC卡与终端接口规范

JR/T 0025.4 中国金融集成电路（IC）卡规范 第4部分：借记/贷记应用规范

JR/T 0025.5 中国金融集成电路（IC）卡规范 第5部分：借记/贷记应用卡片规范

JR/T 0025.6 中国金融集成电路（IC）卡规范 第6部分：借记/贷记应用终端规范

JR/T 0025.7 中国金融集成电路（IC）卡规范 第7部分：借记/贷记应用安全规范

JR/T 0025.8 中国金融集成电路（IC）卡规范 第8部分：与应用无关的非接触式规范

JR/T 0025.10 中国金融集成电路（IC）卡规范 第10部分：借记/贷记应用个人化指南

JR/T 0025.11 中国金融集成电路（IC）卡规范 第11部分：非接触式IC卡通讯规范

JR/T 0025.13 中国金融集成电路（IC）卡规范 第13部分：基于借记/贷记应用的小额支付规范

JR/T 0025.17 中国金融集成电路（IC）卡规范 第17部分：借贷记应用安全增强规范

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

本部分中“卡片”一词是指具有非接触式支付应用、与支付终端交互的消费者设备。

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，它是指任何可以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

中国余数定理（CRT） chinese remainder theorem (CRT)

RSA私钥的一种特殊表示格式，可加速签名计算速度。

3.5

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。

3.6

消费者设备 consumer device

消费者用于支付交易的卡片（PICC）或其它具有交易芯片的设备（例如，移动电话或PDA）。

3.7

集成电路 integrated circuit (IC)

具有处理和/或存储功能的电子器件。

3.8

集成电路卡（IC卡） integrated circuit(s) card (ICC)

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

3.9

发卡行行为代码 issuer action code

发卡行根据TVR的内容选择的动作。

3.10

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，卡片行为由采用所选择的路径唯一确定。

3.11

支付系统环境 payment system environment

当符合JR/T 0025的支付系统应用被选择，IC卡中所确立的逻辑条件集合。

3.12

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，可以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。

3.13

读写器 reader

本部分中“读写器”一词是指与卡片交互的受理设备。

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有以下两种形式：

——作为一种与 POS 设备分离，但与之通信的读写器；

——集成到 POS 设备中的读写器。

除非有其它的明确说明，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。

4 符号和缩略语

以下符号和缩略语表示适用于本文件。

AAC 应用认证密文（Application Authentication Cryptogram）

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）
BCD	二进制编码的十进制表示法（Binary Coded Decimal）
CDA	复合动态数据认证/应用密文生成（Combined DDA/AC Generation）
CDOL	卡片风险管理数据对象列表（Card Risk Management Data Object List）
CLA	命令报文的类别字节（Class Byte of the Command Message）
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）
CVN	卡片验证值（Card Verification Number）
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）
FCI	文件控制信息（File Control Information）
fDDA	快速 DDA（Fast DDA）
FWI	帧等待时间整数（Frame Waiting Time）
GPO	获取处理选项（Get Processing Options）
Hex	十六进制（Hexadecimal）
IAC	发卡行行为代码（Issuer Action Code）
IC	集成电路（Integrated Circuit）
iCVN	替代的 CVN，用于个人化在芯片中的磁道 2 等价数据的镜像
IDD	发卡行自定义数据（Issuer Defined Data）
Lc	终端应用层（TAL）在情况 3 或情况 4 命令中发出数据的实际长度（Exact Length of Data Sent by the TAL in a Case 3 or 4 Command）
LRC	纵向冗余校验（Longitudinal Redundancy Check）
LV	非接触快速借记/贷记的小额支付选项（Low Value）
MAC	报文鉴别码（Message Authentication Code）
MBLI	最大缓冲区长度索引（Maximum Buffer Length Index）
MDK	主密钥（Master Key）
MSI	磁条位图（Magnetic Stripe Image）
PAN	主账号（Primary Account Number）
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 IC 卡（Proximity IC Card）
PIN	个人识别码（Personal Identification Number）
PPSE	近距离支付系统环境（Proximity Payment Systems Environment）
PSE	支付系统环境（Payment System Environment）
PVKI	PIN 验证密钥索引（PIN Verification Key Index）
qPBOC	快速借记/贷记应用（quick PBOC）

RFU	预留（Reserved for Future Use）
RID	注册的应用提供商标识（Registered Application Provider Identifier）
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）
SM2	一种椭圆曲线公钥密码算法，其密钥长度为 256 比特
SFI	短文件标识符（Short File Identifier）
TAL	终端应用层（Terminal Application Layer）
TC	交易证书（Transaction Certificate）
TLV	标签、长度、值（Tag Length Value）
UDK	子密钥（Unique Key）

5 非接触实现方法概述

5.1 非接触式支付方式

本部分描述了两种基于非接触式界面的支付方式：

——快速借记/贷记（qPBOC）方式；

——非接触式借记/贷记应用方式。

qPBOC应用与借记/贷记应用的区别参见附录A。

5.1.1 快速借记/贷记非接触式支付应用

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。

qPBOC有两大特点：

——联机交易采用联机卡片认证；

——脱机交易采用脱机数据认证，并对于交易金额低于最低限额的交易采用清算密文。为限制脱机交易，可规定某一交易金额的下限。

本部分将对 qPBOC 功能要求进行定义。

5.1.2 非接触式借记/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必须支持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，那么终端只能向卡片表明支持非接触式借记/贷记应用应用。

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

非接触卡片性能 / 终端配置	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

5.2.1 支持 DDA 的 qPBOC

用于DDA的IC卡公钥证书包括卡片静态数据的哈希值。本部分建议qPBOC和借记/贷记应用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，发卡行应该权衡在借记/贷记静态数据元中包含特殊数据项与由此增加qPBOC交易的交易时间两者之间的得失。

对于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以支持的非接触的种类（应支持qPBOC或非接触式借记/贷记应用）。卡片决定进入哪种非接触式路径。卡片应支持qPBOC路径，可以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 借记/贷记应用中的命令、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 借记/贷记应用。

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。

具体参见JR/T 0025.17 10.5。

图1给出了卡片确定路径和交易处理的总体示意图。

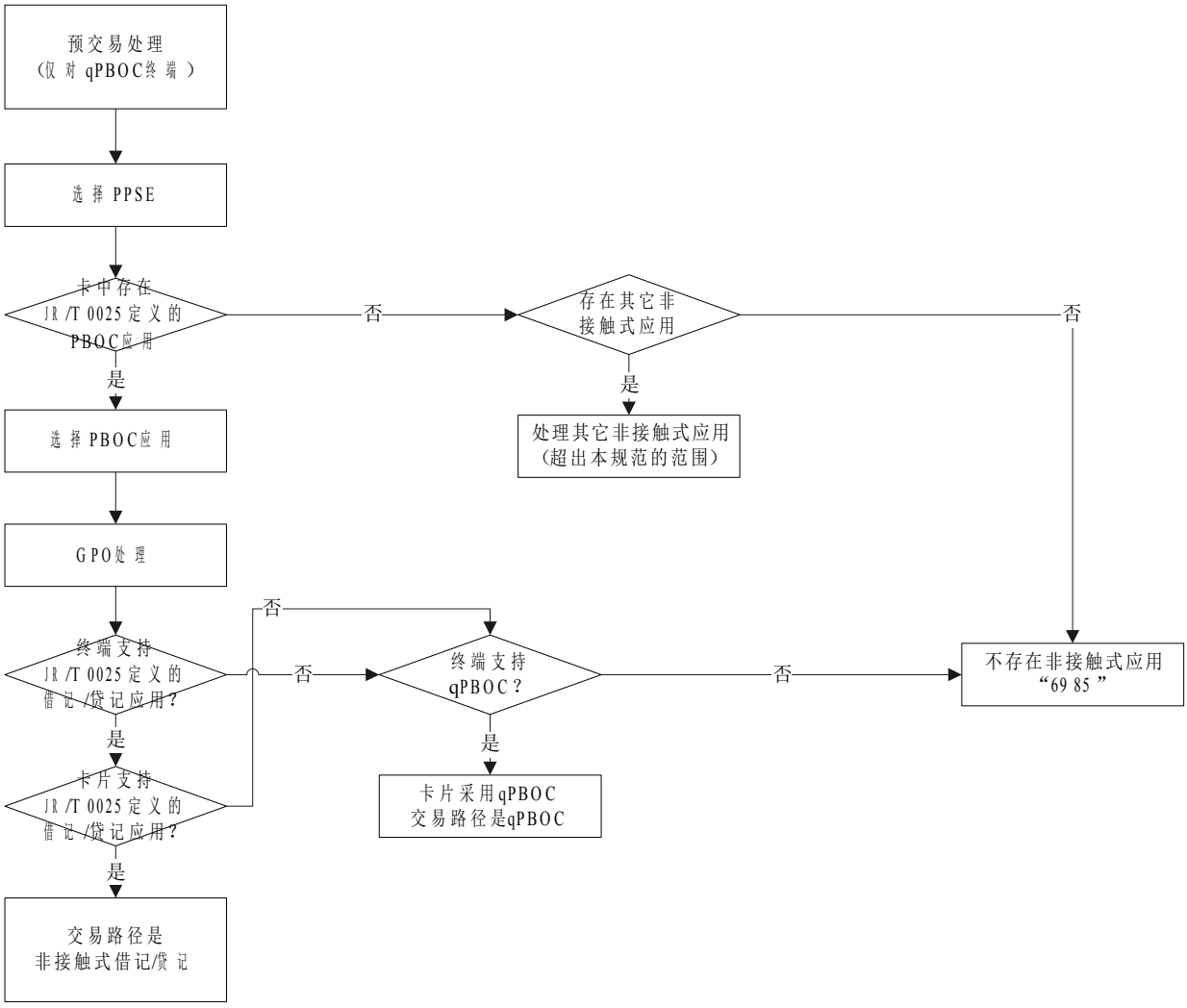

图1　总体处理流程

SM算法应用于qPBOC流程见图2。

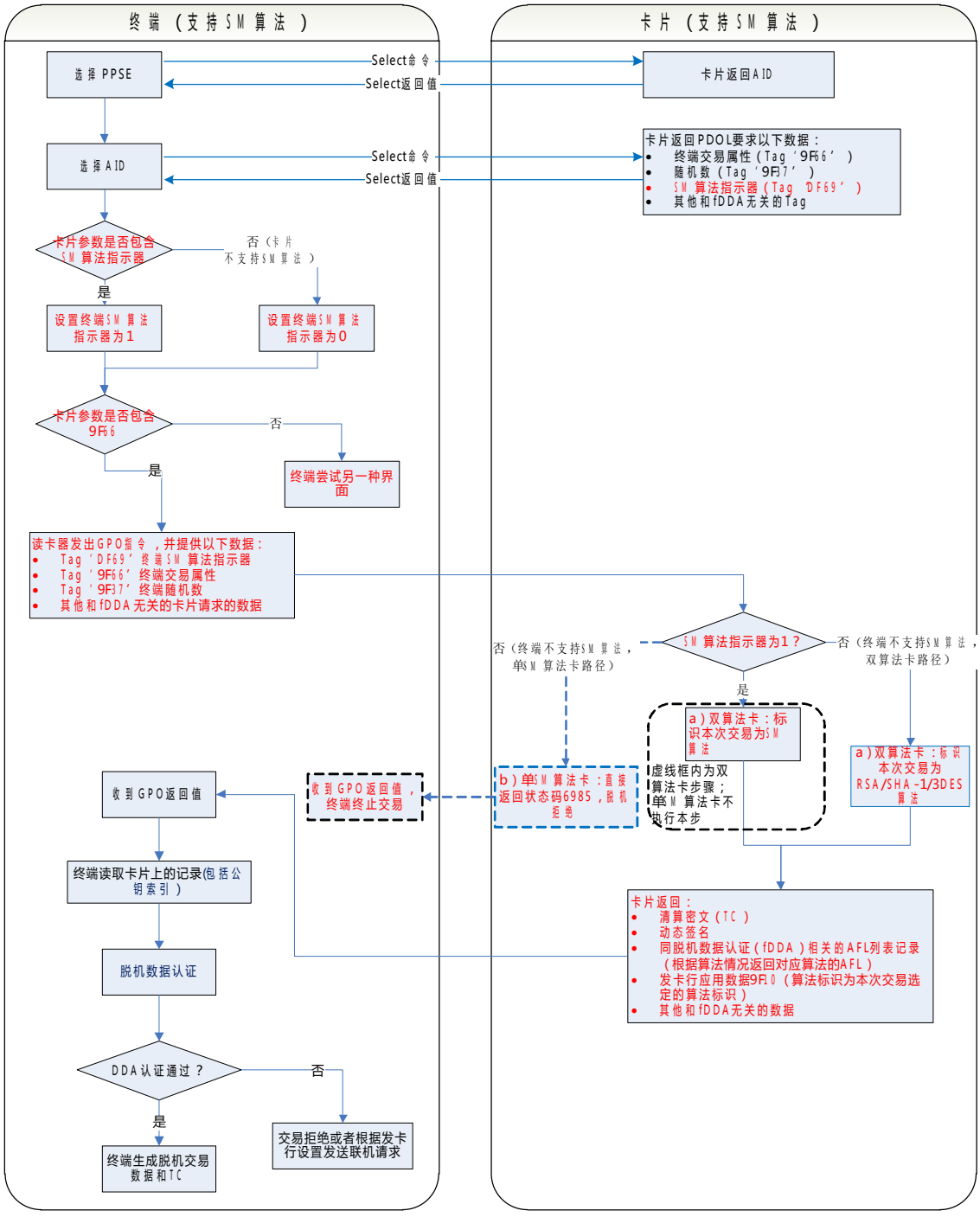

图 2　SM 算法应用于 qPBOC 流程

6　qPBOC 的通用要求

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

6.1　通用要求

qPBOC是基于借记/贷记卡片和终端应用规范的，本部分指出不同之处，并在附录A中详细描述。

6.1.1　Level1 终端要求

Level1终端要求如下：

——终端应符合 JR/T 0025.11，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)。

6.1.2 通用终端要求

——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 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/贷记应用还是 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，交易不应再通过其它界面方式进行；

——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，然后重新启动其它界面进行交易；

——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；
- 交易结果——批准、拒绝或终止。

推荐的终端信息有：

- 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。

6.1.3 通用终端选项

终端可以按照JR/T 0025.6的要求，支持读卡、显示或打印交易明细。

6.1.4 通用的卡片要求

——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；

——卡片应该符合规范照 JR/T 0025.11,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；

——具有脱机能力的卡片（qPBOC）应支持 DDA。

注： 为了用目前的芯片满足时间要求，推荐卡片以中国余数定理模式存放与使用RSA私钥。

6.1.5 通用卡片选项

卡片可选支持非接触界面借记/贷记应用应用。

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13），交易日志的定义见JR/T 0025.5第18章。

是否启用交易日志功能由发卡机构决定。

6.1.6 推荐卡片采用 iCVN

除了非接触风险管理特征外，当不使用dCVN时，推荐qPBOC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。

6.1.7 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

为了使卡片保持在感应区的时间最小化，qPBOC终端在提示持卡人出卡和激活非接触界面前，应执行下列处理。

6.2.1 预处理前的处理要求

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以上电。

6.2.2 具有 qPBOC 能力终端中的交易预处理

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。对于交易金额固定的一些设备，非接触界面可以立即上电。在下面的例子中，全部或部分检查可以省去：

——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，但可以获得授权金额（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。

如果下面描述的检查被执行，则应按照要求执行。

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。

——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。本部分当前版本支持联机 PIN（第 1 字节第 3 位）和签名（第 1 字节第 2 位）；

- 与这些指示器对应的卡片行为的详细描述见 7.7.3。

——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。

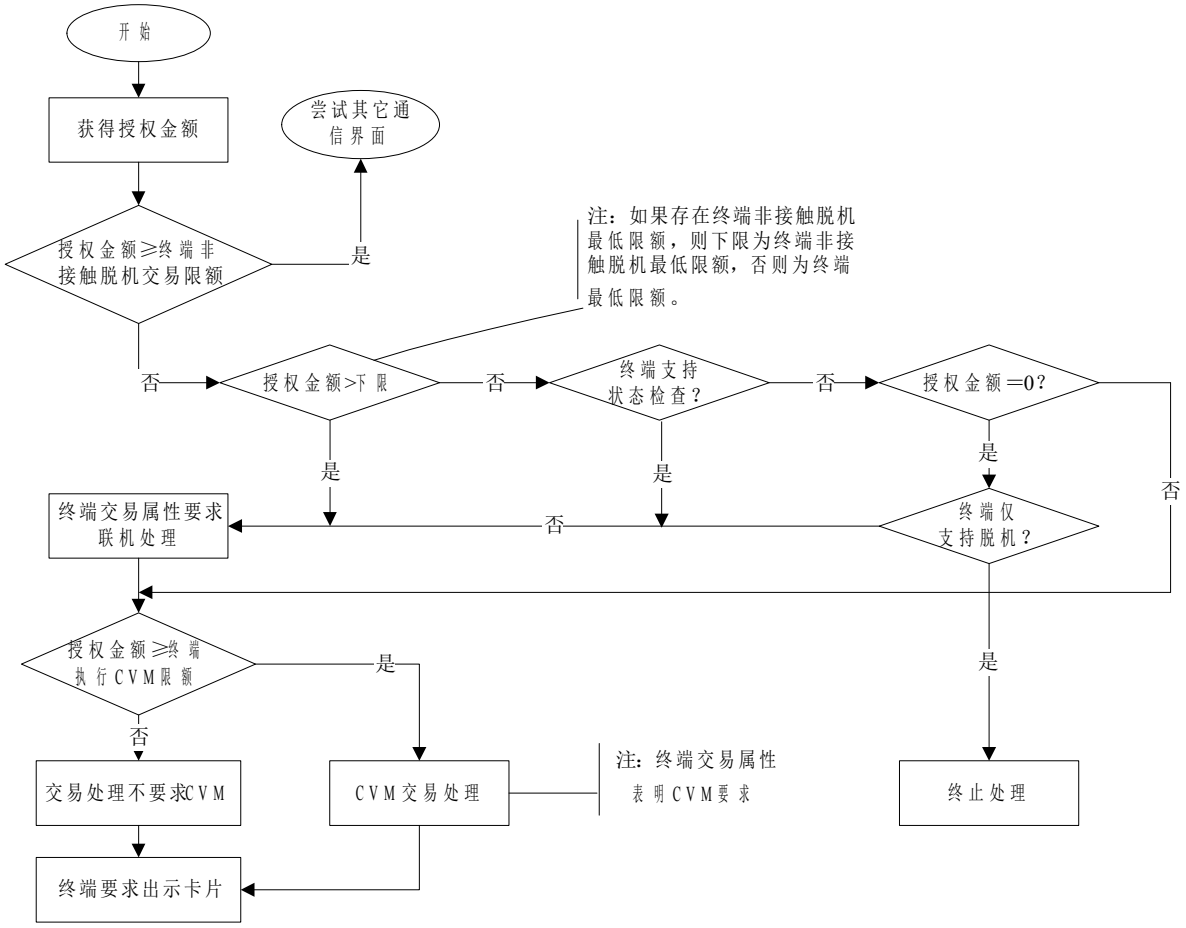

图 3　具有 qPBOC 能力终端的预交易处理

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部分的描述，在初始化交易前执行qPBOC预处理）。

终端可以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。

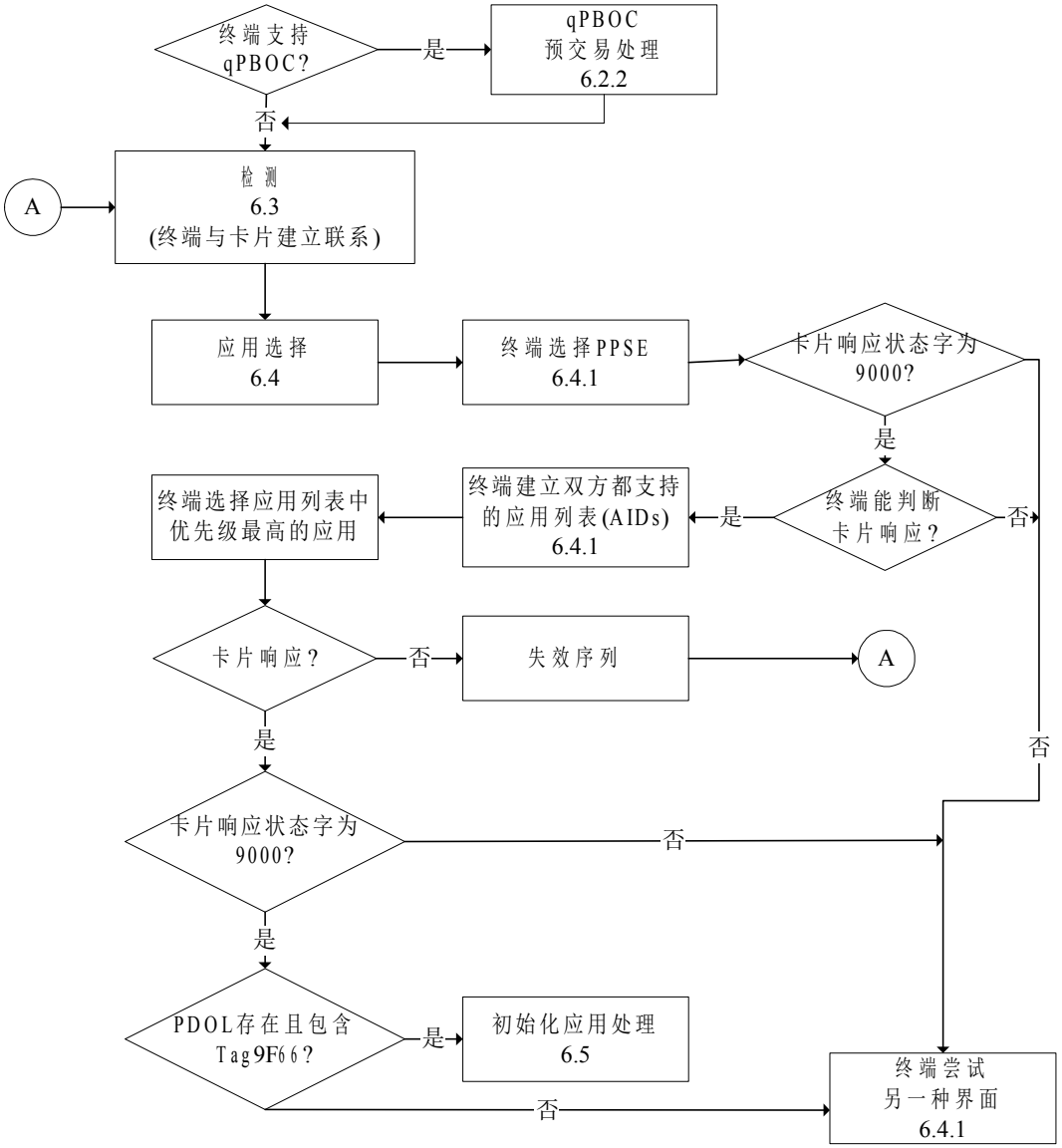

图 4　卡片检测和应用选择流程

6.4　应用选择要求

所有非接触卡片应符合下列选择非接触支付应用的要求。在初始化应用处理阶段，确定用于处理交易的方法（qPBOC或非接触式借记/贷记应用）。

6.4.1　终端应用选择要求

下列的终端要求允许选择非接触应用。本部分描述了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。

——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，则终端可以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

下面的卡片要求允许选择非接触应用。本部分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，建议对个人化在FCI中的应用数量进行限制。

——应使用文件名“2PAY. SYS. DDF01”将 PPSE 个人化到所有的非接触卡片中；

——应当在具有借记/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

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。建议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*
			“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
			“61”	目录入口		变长	C*
				“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

*条件——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	预留
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	8-1	预留
4	8	1 – 终端支持“01”版本的 fDDA
		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

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。

6.5.1　终端初始化应用处理的通用要求

——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 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，则终端应关闭非接触界面，并尝试另一种界面进行交易。

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中的描述初始化失效序列，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命令的状态字不为“9000”，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。

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。

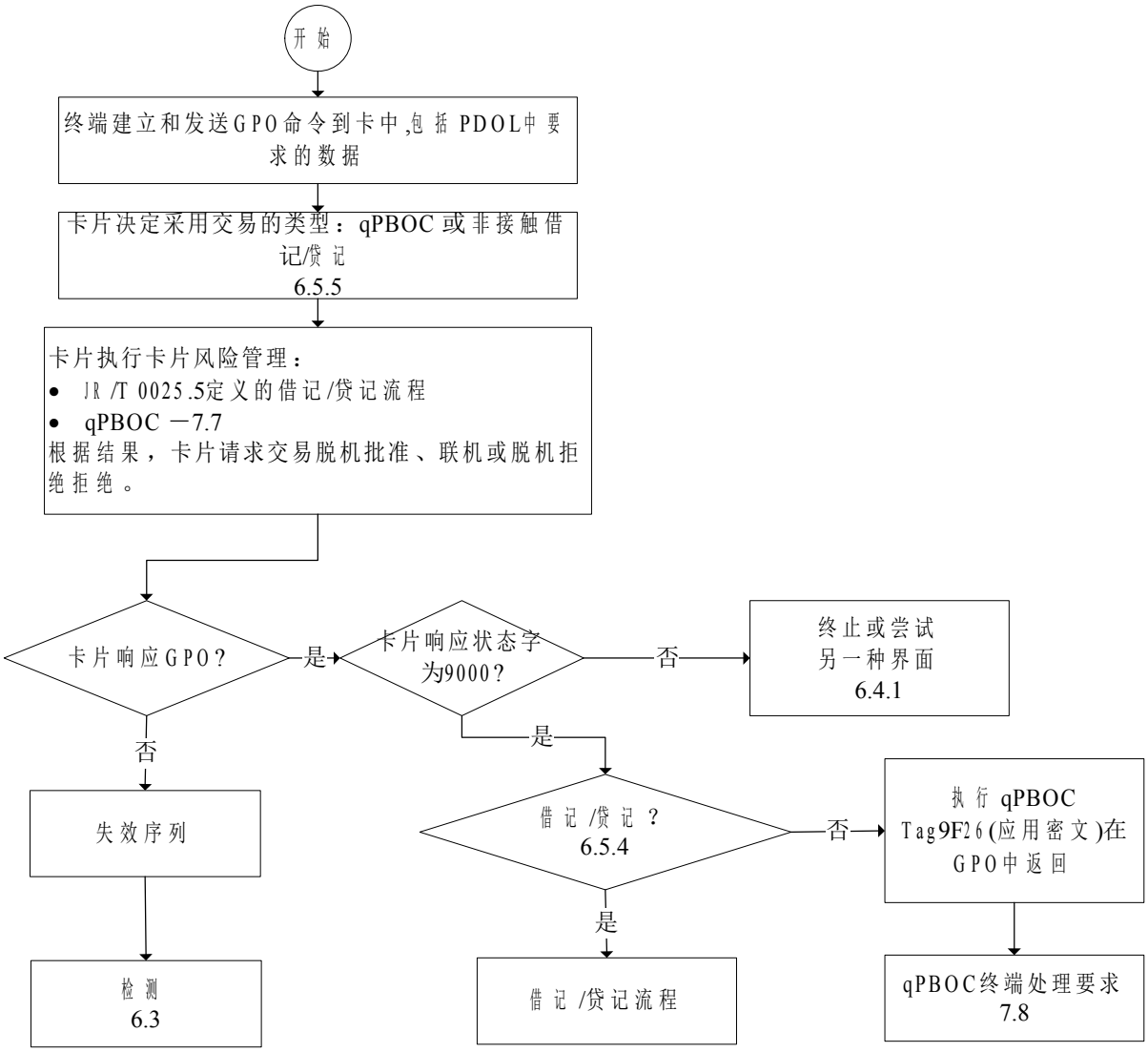

图5　初始应用处理流程

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”；其它值预留
P2	“00”；其它值预留
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。

——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；

——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；

——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 交易时间

基于卡片和终端之间的交互，qPBOC的交易时间不能超过500毫秒。这个时间不包括联机认证或qPBOC终端脱机数据认证中验证静态或动态签名所需的时间。

6.7 个人化

推荐所有非接触应用采用JR/T 0025.10中的个人化方法。

7 qPBOC要求

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。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。它还提供了脱机快速小额支付特性、脱机数据认证以及使用现有密文算法（版本01）或新的精简算法（版本17）的联机卡片认证。

除了实现本章描述的所有需求和元素的完全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易时间。

7.1 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借记/贷记应用命令子集：SELECT、GPO、READ RECORD和GET DATA命令和需求。GPO命令响应采用JR/T 0025.5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（INTERNAL AUTHENTICATE）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。因此推荐终端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它本部分中未涉及到的变量不会受到影响。QPBOC的需求及推荐处理在下面概述。

7.2 qPBOC处理概述

下面的内容详细描述了qPBOC的处理需求，图6概述了qPBOC如何工作。

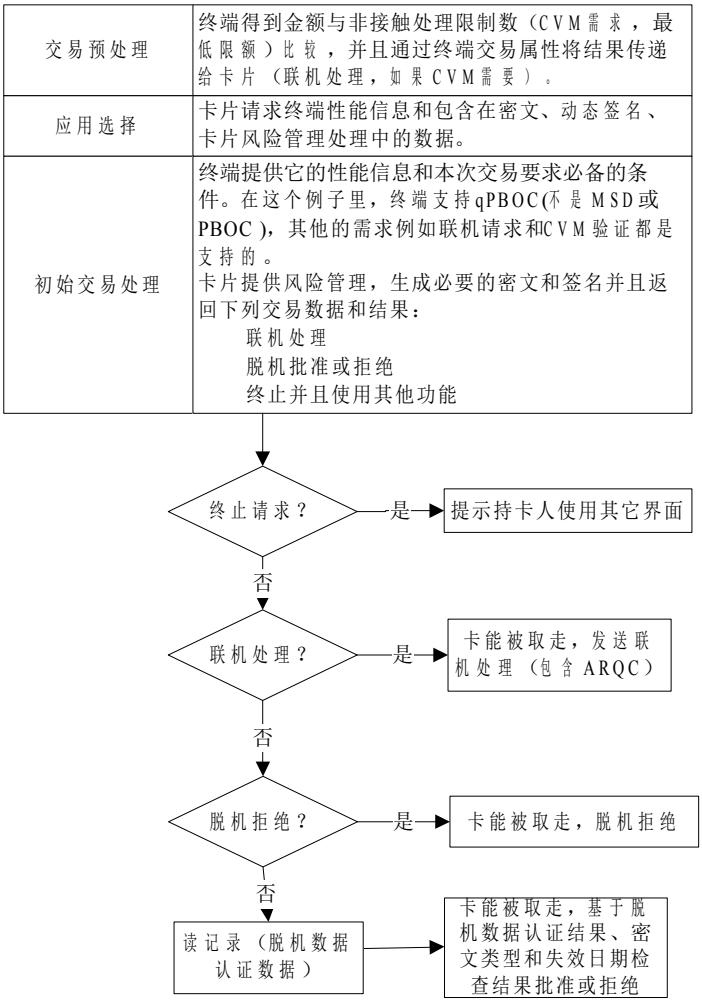

图 6　qPBOC 处理流程概况

7.3　有关 PDOL 内容的 qPBOC 需求

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/贷记应用应用）相关的标签，也可以包含本部分未描述的标签来作为最低需求。发卡行应当在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。

7.3.1　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”）也应当包括在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。

7.3.2 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。

7.3.3 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”	其它金额
“9F1A”	终端国家代码
“95”	终端验证结果（TVR） 注： 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）
“5F2A”	交易货币代码
“9A”	交易日期
“9C”	交易类型
“9F37”	不可预知数

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

卡片接收GPO命令，并检查交易防拔位（卡片内部指示器）。

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，卡片在计数器更新后设置了一个内部指示器，并在处理交易最后一条命令时将其清除，作为最后一步操作。在交易开始时如果该标志已置位（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。

如果交易防拔位（下同）＝‘1’，卡片应当恢复到最近一笔成功完成的交易结束时的值，并设置交易防拔位为‘0’。

管理交易防拔处理的方式由厂商自定。

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参照本部分的表11和表12。

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

7.4.3 应用文件定位器（AFL）

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。终端应当只读取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中的表9。

当卡片请求联机处理或拒绝交易时，AFL不应当返回。

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，按照附录C的表C.1编码。终端应当只尝试执行IC卡支持的功能。详细要求在表11中说明。

对于所有qPBOC联机交易，表11中列出的必备数据元应包含在GPO返回中。

表 11 qPBOC 联机交易或拒绝交易的 GPO 响应数据

标签	必备（M） 可选（O） 条件（C）	数据元名称
“82”	M	AIP
“9F36”	M	ATC
“57”	M	2 磁道等价数据
“9F10”	M	发卡行应用数据 标签“9F10”中的发卡行自定义数据也可以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
“9F26”	M	应用密文
“9F63”	C 如果卡片中出现	产品标识信息
“5F34”	C 如果卡片中出现	应用 PAN 序列号
“9F6C”	C 如果卡片中出现	卡片交易属性
“9F5D”	C 如果允许脱机金额显示	可用脱机消费金额 除非标签“9F5D”已被个人化为值 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、小额或 CTTA）定义进行计算
“5F20”	O	持卡人姓名 注： 持卡人姓名在借记/贷记应用中是要求的数据元。

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：可以包含在附录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）。

——表 12 中列出的数据元在脱机交易的 GPO 响应中是必备或条件的。

表 12 脱机批准交易的 GPO 响应必备和条件数据

标签	必备（M）或条件（C）	数据元名称
“82”	M	AIP
“94”	M	AFL
“9F36”	M	ATC

“9F26”	M	应用密文
“9F10”	M	发卡行应用数据 标签“9F10”中的发卡行自定义数据也可以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
“57”	C 如果2磁道等价数据不是待签名的静态数据部分	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
“5F34”	C 如果卡片中出现	应用 PAN 序列号
“9F4B”	C 如果支持 fDDA 且 IC 卡的私钥长度小于等于 1024 位	签名的动态应用数据
“9F6C”	C 如果卡片中出现	卡片交易属性
“9F5D”	C 如果允许返回可用脱机消费金额且 IC 卡私钥的长度小于等于 1024 位	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、小额或 CTTA）定义进行计算。

——任何附加数据，包括持卡人姓名（标签“5F20”），应当用 READ RECORD 命令读取；

——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”）应当包含在一条记录中。

7.4.5 qPBOC 推荐签名数据

如卡片支持qPBOC，则推荐下面这些静态数据元用于签名：

——应用 PAN；

——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”）设置为本规范的本版本，强烈建议将应用版本号（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/贷记应用应用（接触），也可以增加JR/T 0025.5中推荐的附加数据元。

7.5 qPBOC 卡片需求

除了所有非接触应用的卡片需求外，qPBOC还应当遵守下面的要求：

——收到 GPO 命令，卡片应当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；

CVR字节2，位4、3、2、1未使用，仍保留设置为“0”；

CVR字节3，位8、4、3、2、1未使用，仍保留设置为“0”；

CVR字节4未使用，所有位仍保留设置为“0”；

——卡片应当支持算法选择，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。

——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。

——卡片应当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，则卡片应当允许读取该数据元。卡片的行为应当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，卡片应当在 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，卡片应当在 GPO 响应中返回表 12 中的数据元；

——如果 IC 卡私钥的长度小于等于 1024 位，应当生成动态签名并在 GPO 响应中返回；

——如果 IC 卡私钥的长度大于 1024 位，卡片应当在 GPO 时生成动态签名并在 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当只被返回一次；

——qPBOC 脱机批准的交易，AFL 指明的终端须读取的最后一条记录的 70 模板的长度应不超过 32 字节。如卡片执行的是“01”版本的 fDDA，则建议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。

——符合本规范的卡片应同时支持“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。

注： 如果IC卡私钥的长度大于1024位，GPO相应中没有足够空间返回动态签名。

——为了确保 GPO 响应能成功传送给终端，对于 IC 卡私钥的长度等于 1024 位的情形，AFL 包含的分支不应当超过 4 个。

注： 如果IC卡私钥的长度更短，可能会有足够空间包含更多的分支。如果IC卡私钥的长度更长，签名在记录中传送，也会有足够空间传送更大的AFL。

7.6 qPBOC 终端需求

除了对于所有非接触应用的终端需求外，支持qPBOC的终端还应当符合下面这些要求：

——终端应当支持 6.2.2 所描述的 qPBOC 交易预处理；

——终端应当根据系统算法支持情况，设置 SM 算法支持指示器标签，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 的终端不应当查询 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 的终端应当按 JR/T 0025 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 和 12），支持 qPBOC 的终端应当终止交易；

——如果 JR/T 0025 借记/贷记应用必备但 qPBOC 不要求的数据元不存在，支持 qPBOC 的终端不应当因此拒绝交易；

——支持 qPBOC 的终端应当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，支持签名的终端应当认为支持签名。如果终端要求 CVM，应当在单据上打印签名行；

——支持超过一个 CVM 的终端应当查询卡片交易属性（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’，终端应当执行联机 PIN 校验，不再查询位 7；如

果位 8＝‘0’，终端应当查询位 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’，终端应当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。

——符合本规范的终端，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

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”）中个人化的一系列需求来控制。这些数据元的内容如表13所示，并在表13描述的卡片处理中用到。

表 13　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	1 – 支持小额或 CTTA 检查 0 – 不支持小额或 CTTA 检查
	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	1 – 支持预付 0 – 不支持预付
	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 脱机批准的交易，卡片记录交易日志 0 – qPBOC 脱机批准的交易，卡片不记录交易日志
	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	8-1	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。

7.7.1 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。接下来的处理步骤见 7.7.17——拒绝交易。

7.7.2 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，接下来的处理步骤看 7.7.17——拒绝交易。

脱机 PIN 尝试上限超过

——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），卡片应当拒绝交易：

- 将 CVR 的第 3 字节第 7 位设置为‘1’（PIN 尝试上限超过）；
- 接下来的处理步骤看 7.7.17——拒绝交易。

要求 CVM

——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：

卡和终端都支持签名

如果在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’；
- 接下来的处理步骤看 7.7.5——脱机货币检查。

卡或终端至少一个不支持签名

如果在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。

- 接下来的处理步骤看 7.7.16——终止非接触式交易。

仅支持脱机终端的处理流程见图 7 所示。

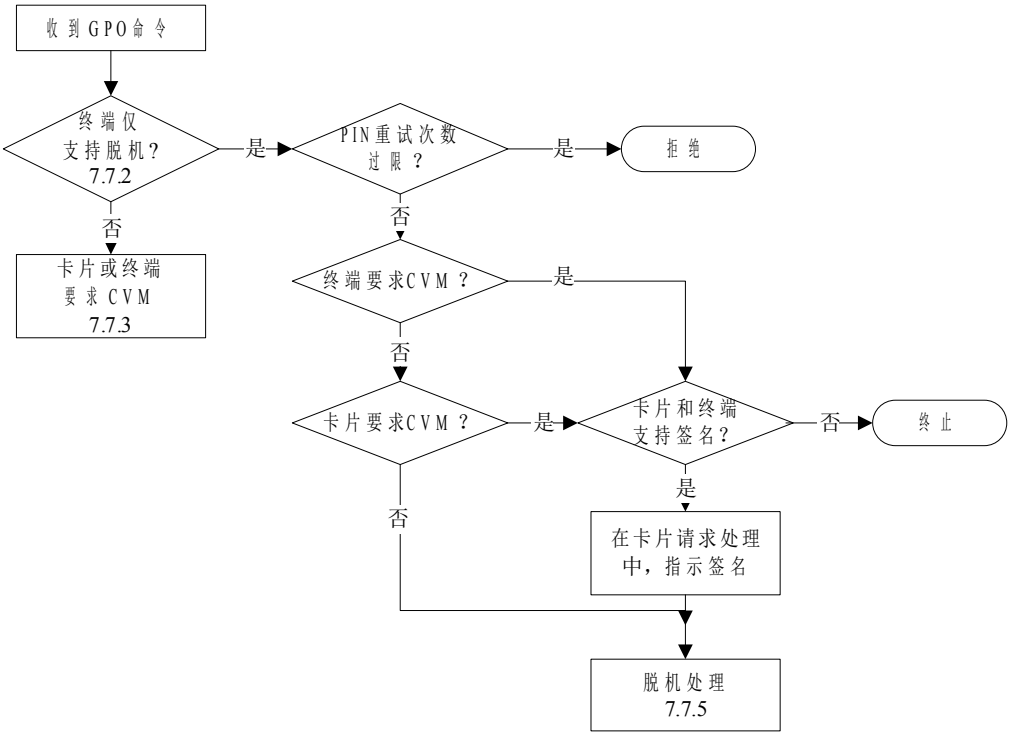

图 7　仅支持脱机终端

7.7.3　终端或卡请求 CVM

终端可以请求CVM（总是或者对超过终端CVM请求上限的交易）。卡同样也可以请求CVM。目前qPBOC支持两种方式验证持卡人：联机PIN和签名。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。

无需 CVM

——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，继续7.7.4——检查联机处理请求。

结束无需 CVM

要求 CVM

——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）。

接着按照下面的步骤继续。

卡和终端均支持联机 PIN

——如果在终端交易属性（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）。

——卡和终端均支持联机 PIN；

- 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、小额或 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。

按7.7.15的步骤继续处理——完成联机处理。

卡和终端均支持签名

——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；
- 按 7.7.4 继续处理——检查联机处理请求。

无共同的 CVM

——卡片应当终止交易：

按7.7.16的步骤继续处理——终止非接触式交易。

结束要求 CVM

卡片 CVM 处理流程见图 8 所示。

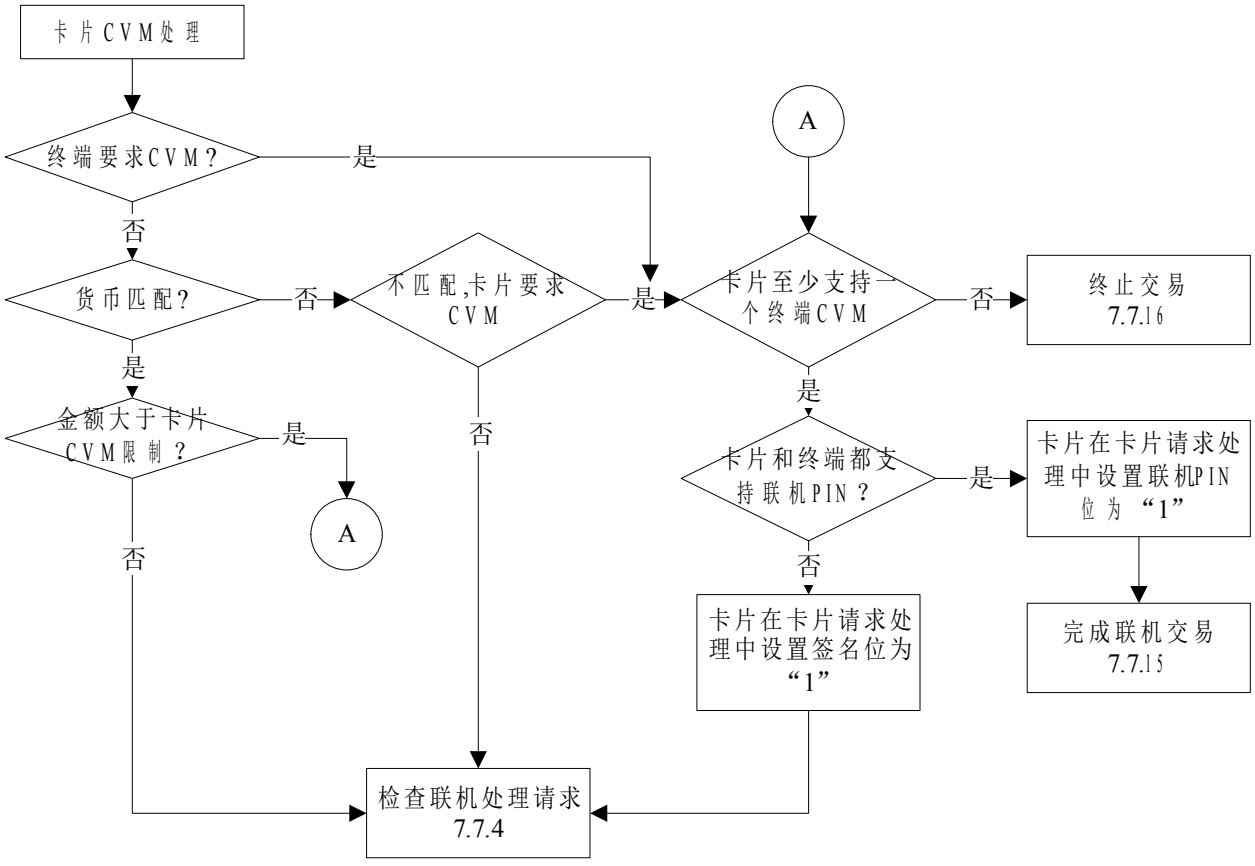

图 8　卡片 CVM 流程

7.7.4　检查联机处理请求

卡片和终端可以基于交易条件请求联机处理。如果先前的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它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’），则卡也要请求联机处理；

- 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、小额或 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；
- 按 7.7.15 继续处理——完成联机交易。

——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、小额或 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；
- 按 7.7.15 继续处理——完成联机交易。

——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、小额或 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）；
- 按 7.7.15 继续处理——完成联机交易。

——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、小额或 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）；
- 按 7.7.15 继续处理——完成联机交易。

检查联机处理请求见图 9 所示。

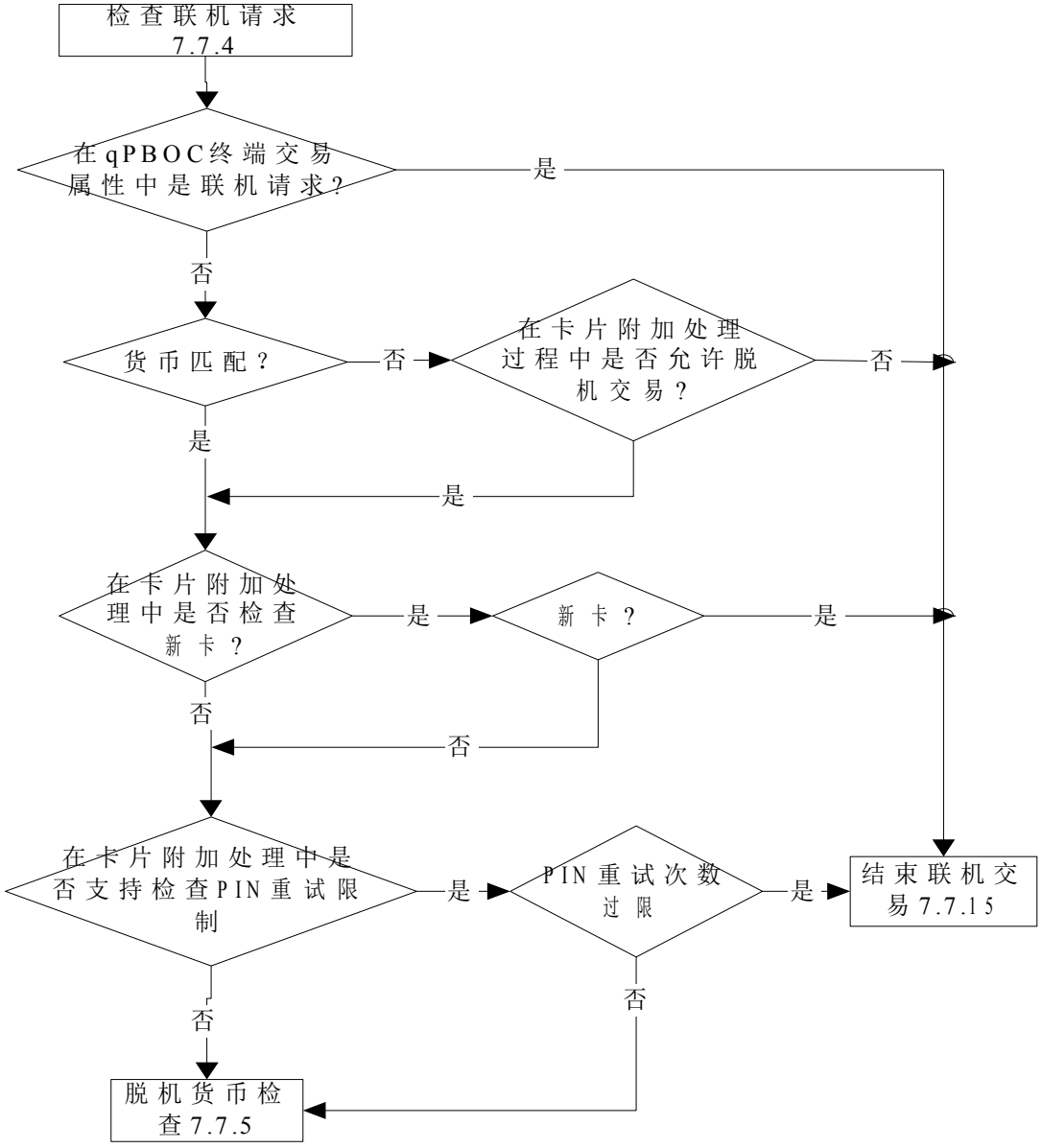

图9　检查联机处理请求

7.7.5　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、小额或CTTA检查是qPBOC的三种检查脱机消费的方法。JR/T 0025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需求在下面三种方法中详细描述。

——如果货币匹配位=‘0’：

继续进行的步骤见7.7.13——脱机下的货币不匹配。

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7.7.9的描述。

7.7.6 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。

继续进行的步骤见7.7.10——小额检查。

7.7.7 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。

继续进行的步骤见7.7.11——小额和CTTA检查。

7.7.8 匹配货币交易的小额或 CTTA 检查

此部分检查是否超过电子现金单笔交易限额（如果存在）。如果小额资金不可用，则检查是否超过累计交易总额上限（CTTAL）。只有小额或者CTTA资金任一可用，脱机处理才会发生。

——如果支持小额或 CTTA 检查（卡片附加处理的第 1 字节第 6 位=‘1’），则脱机资金应在小额或者 CTTA 中可用。

继续进行的步骤见7.7.12——小额或CTTA检查。

7.7.9 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’），则卡片应当拒绝交易；

继续进行的步骤见7.7.17——拒绝交易；

——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、小额或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。

继续进行的步骤见7.7.15——完成联机交易。

脱机货币检查处理流程见图 10 所示。

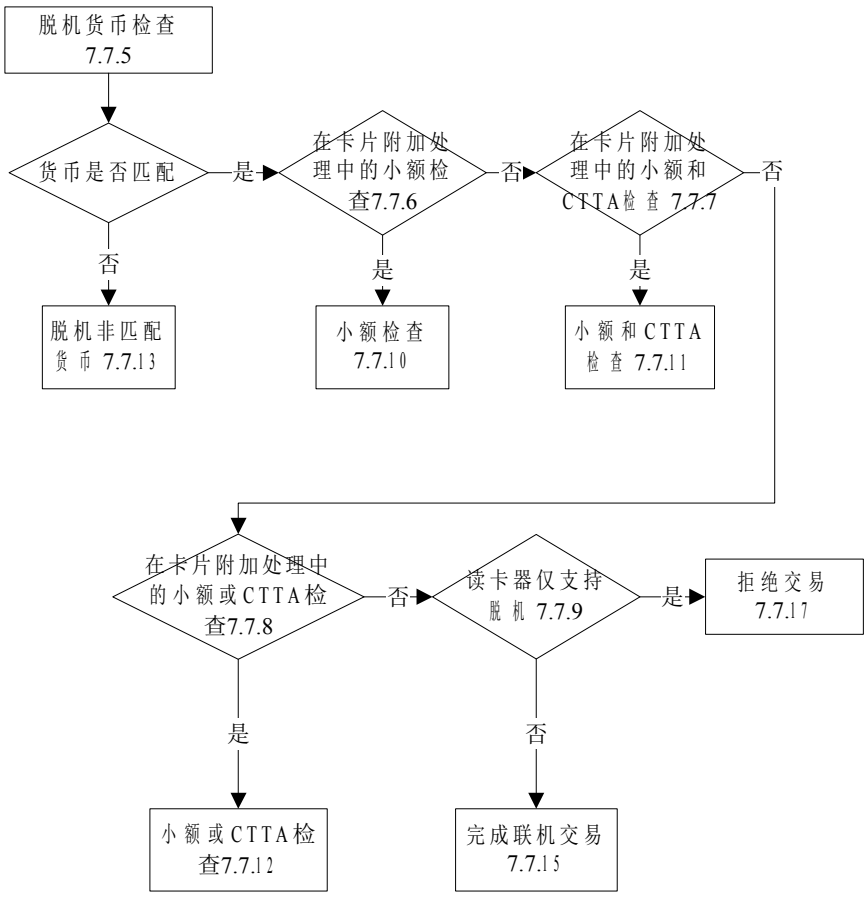

图 10　脱机货币检查

7.7.10　小额检查

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。

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；

——如果终端不具有联机处理能力，则卡片请求拒绝。

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’），适用下面的需求。

——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）；
- 继续进行的步骤见 7.7.15——完成联机交易。

——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）；
- 继续进行的步骤见 7.7.15——完成联机交易。

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’），适用下面需求。

——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。

- 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）；
- 继续进行的步骤见 7.7.17——拒绝交易。

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；
- 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’。见 7.4.1——防拔保护；
- 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 CVR 中请求脱机批准；
- 继续进行的步骤见 7.7.14——完成脱机交易。

小额检查处理流程见图 11 所示。

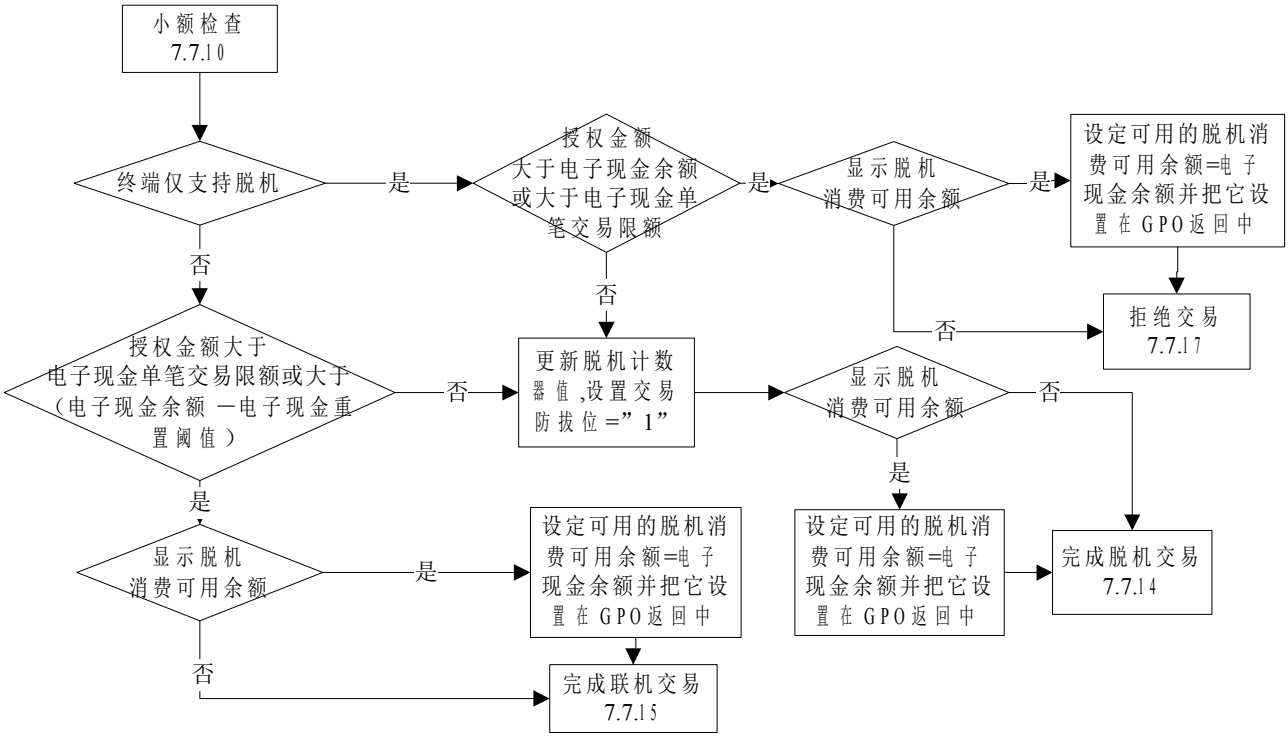

图 11　小额检查

7.7.11　小额和 CTTA 检查

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。

否则[即，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；

——如果终端不具有联机处理能力，则卡片请求拒绝。

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’），适用下面需求。

——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”），则卡片应当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）；
- 继续进行的步骤见 7.7.15——完成联机交易。

——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”），则卡应当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）；

- 继续进行的步骤见 7.7.15——完成联机交易。

——如果授权金额（标签“9F02”）加上 CTTA 大于 CTTAUL/CTTAL（标签“9F54”），则卡片应当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）；
- 继续进行的步骤见 7.7.15——完成联机交易。

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’），应用下面需求。

——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），则卡片应当准备返回可用脱机消费金额（如果支持的话），并拒绝交易。

- 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）；
- 继续进行的步骤见 7.7.17——拒绝交易。

交易被允许脱机完成

——如果前面步骤都不符合，则卡片应当：

- 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’。见 7.4.1——防拔保护；
- 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；
- 继续进行的步骤见.7.14——完成脱机交易。

小额和 CTTA 检查处理流程见图 12 所示。

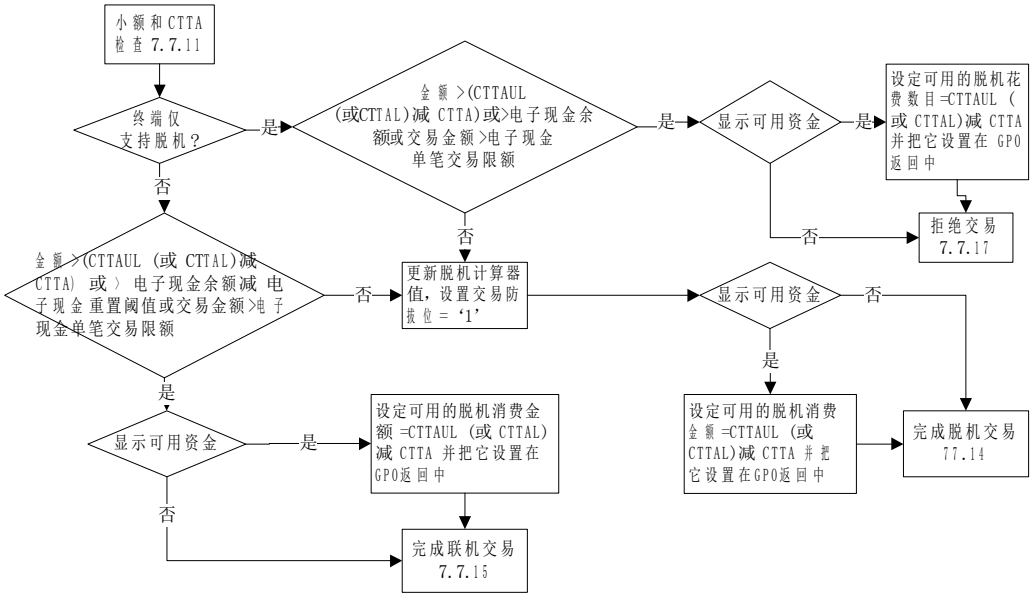

图 12　小额和 CTTA 检查

7.7.12　小额或 CTTA 检查

此检查交易能否脱机处理。

如果授权金额（标签“9F02”）小于或等于单笔交易限额，并且电子现金余额或者CTTA中有足够的脱机资金，那么交易可以脱机处理。

否则（即如果授权金额（标签“9F02”）大于电子现金单笔交易限额或者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，那么卡片请求联机处理；

——如果终端不具有许联机处理能力，那么卡片将请求拒绝。

对于该选项，可用脱机消费金额等于CTTA可用余额和电子现金余额的总和。

可联机终端

以下只适用于终端可联机的情况（终端交易属性字节1第4位＝‘0’）。

如果仅脱机终端位（卡片内部的指示器）=‘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”），那么卡片应准备返回可用脱机消费金额（如果支持的话），并请求联机处理；

- 如果支持返回可用脱机消费金额（卡片附加处理，字节 1 第 1 位=‘1’），那么卡片应将可用脱机消费金额（标签“9F5D”）的值设为电子现金余额加上 CTTAUL（或者是 CTTAL 如果 CTTAUL 不存在），再减去 CTTA，然后在 GPO 响应中返回。
- 将 CVR 第 3 字节第 6 位置为‘1’（频度检查计数器超过）。
- 继续见 7.7.15——完成联机交易。

——如果授权金额（标签“9F02”）大于电子现金余额（标签“9F79”），而且授权金额（标签“9F02”）加上 CTTA（无标签）大于 CTTAUL/CTTAL（标签“9F54”），那么卡片应准备返回可用脱机消费金额（如果支持的话），并请求联机处理。

- 如果支持返回可用脱机消费金额（卡片附加处理，第 1 字节第 1 位=‘1’），那么卡片应将可用脱机消费金额（标签“9F5D”）的值设为电子现金余额加上 CTTAUL（或者是 CTTAL 如果 CTTAUL 不存在），再减去 CTTA，然后在 GPO 响应中返回。
- 将 CVR 第 3 字节第 6 位置为‘1’（频度检查计数器超过）。
- 继续见 7.7.15——完成联机交易。

仅脱机终端

以下只适用于终端仅脱机的情况（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单笔交易限额，或者授权金额大于电子现金余额并且授权金额加上CTTA大于CTTAUL/CTTAL，那么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。

- 如果支持返回可用脱机消费金额（卡片附加处理，第1字节第1位=‘1’），那么卡片应将可用脱机消费金额（标签“9F5D”）的值设为电子现金余额加上CTTAUL（或者是CTTAL如果CTTAUL不存在），再减去CTTA，然后在GPO响应中返回。
- 将CVR第3字节第6位置为‘1’（频度检查计数器超过）。
- 继续见7.7.17—拒绝交易。

交易被允许脱机完成

——如果都不是前面步骤的情况，那么卡片应完成以下处理：

- 置交易防拔位（卡片内部的指示器）为‘1’，以指示计数器正被更新。该指示器在最后一个READ RECORD响应前被复位为‘0’。见7.4.1——防拔保护。

电子现金资金可用

- 如果授权金额（标签“9F02”）不大于电子现金余额（标签“9F79”），那么保存电子现金余额值，并计算新的电子现金余额=电子现金余额－授权金额（标签“9F02”）。

电子现金资金不可用从而用CTTA资金

- 如果授权金额（标签“9F02”）大于电子现金余额（标签“9F79”），那么保存CTTA，并计算新的CTTA=CTTA加上授权金额。

- 如果支持返回可用脱机消费金额（卡片附加处理，第1字节第1位=‘1’），那么卡片应将可用脱机消费金额（标签“9F5D”）的值设为电子现金余额加上CTTAUL（或者是CTTAL如果CTTAUL不存在），再减去CTTA，然后在GPO响应中返回。
- 请求脱机批准。
- 继续见7.7.14——完成脱机交易。

小额或CTTA检查处理流程见图13所示。

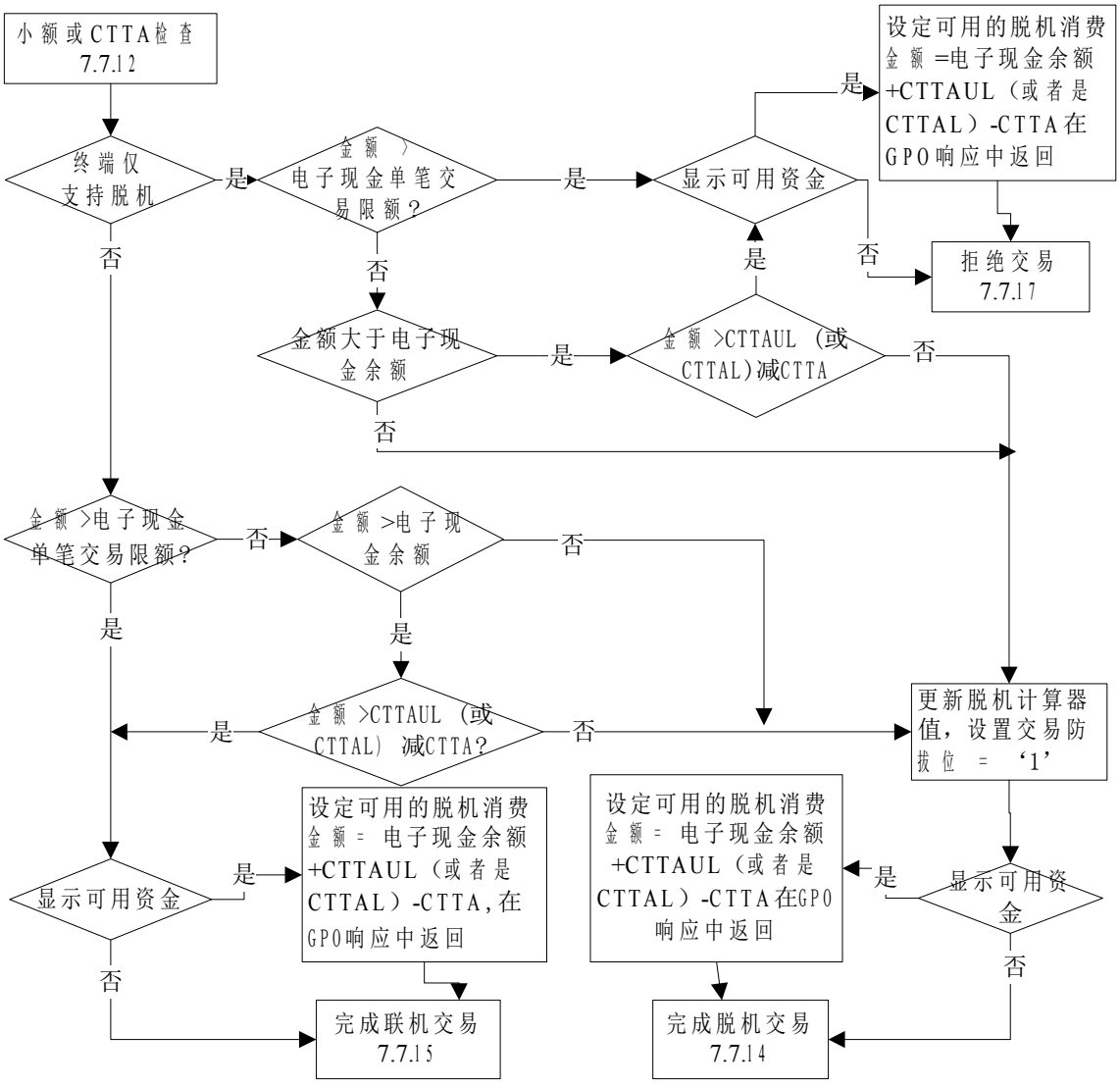

图 13　小额或 CTTA 检查

7.7.13　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。7.7.5已讲述了货币检查，如果货币不匹配则见本条。

——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”），那么卡片应当：

- 存储连续交易计数器的当前值（国际）；
- 置交易防拔位（卡片内部指示器）为‘1’，以指示计数器正被更新。该指示器在最后一个读记录响应前复位为‘0’。见 7.4.1——防拔保护；
- 连续交易计数器（国际—货币）加 1；
- 请求脱机批准；
- 继续见 7.7.14——完成脱机交易。

——如果前面的条件不满足，且仅脱机终端位=‘0’，那么卡片应当请求联机处理；

- 将 CVR 第 3 字节第 6 位置为‘1’（频度检查计数器超过）；
- 继续见 7.7.15——完成联机交易。

——如果前面的条件不满足，且仅脱机终端位＝‘1’，那么卡片应当请求拒绝交易；

- 将 CVR 第 3 字节第 6 位置为‘1’（频度检查计数器超过）；
- 继续见 7.7.17——拒绝交易。

脱机下货币不匹配处理流程见图 14 所示。

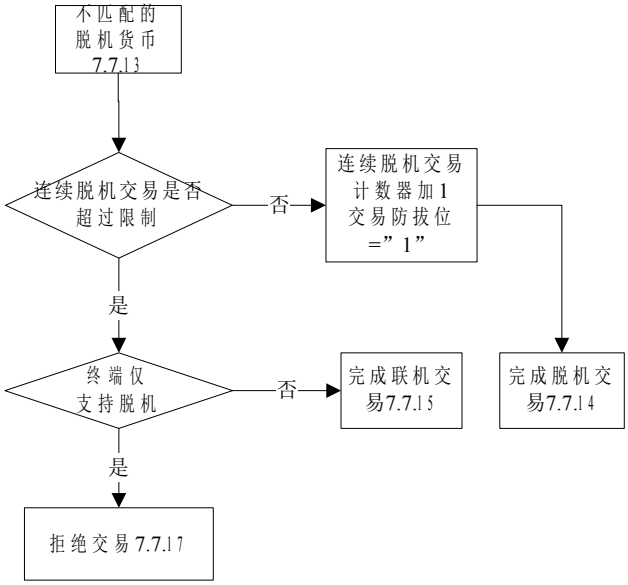

图 14　不匹配的脱机货币

7.7.14　完成脱机交易

交易可以脱机完成。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。

——卡片应当：

- 生成动态应用数据签名（SDAD—标签“9F4B”）：

a) 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；

b) 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：　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 CVR 字节 2 的第 6-5 位置为“01”，以指示一个脱机批准密文（TC），按 JR/T 0025.5 附录 E 的密文版本 01 生成应用密文（TC）。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（见本部分附录 E）。

注：　qPBOC中不使用CDOLs，密文使用PDOL请求的数据生成。

——卡片应当根据 7.4 条建立 GPO 响应；

——继续见 7.7.18——结束 qPBOC 卡片的 GPO 处理。

完成脱机交易处理流程见图 15 所示。

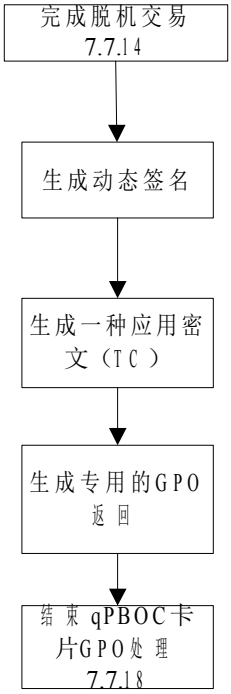

图 15　完成脱机交易

7.7.15　完成联机交易

卡片或终端请求交易需要联机进行授权。在完成联机交易之前，确认其它检查不要求终止或拒绝交易。

卡片要求接触式借记/贷记联机

如果卡片要求接触式借记/贷记联机（卡片附加处理，第1字节第2位），而且终端支持接触借记/贷记（终端交易属性第1字节第5位），那么卡片应当请求交易终止；如果终端不支持接触式借记/贷记，继续完成联机交易。

继续见7.7.16——终止非接触式交易。

预付

对于预付卡，可用脱机消费金额反应了消费者的预付消费能力。对于此类卡片，在成功完成交易之后，不管是联机还是脱机，可用脱机消费金额都需要更新。

预付是一个可选检查，在假设如果卡上余额可用，发卡行将批准联机交易的情况下，允许在联机交易中从脱机预付额资金中减去授权金额（标签“9F02”）。如果执行了该可选检查，有时脱机预付额将会小于正确额度（例如联机交易被拒绝）。脱机预付额不会大于正确额度，以保护发卡行避免非授权消费。

检查预付支持

如果支持预付（卡片附加处理，第2字节第8位=‘1’）：

如果授权金额为零，继续见7.7.17——拒绝交易。如果授权金额大于零，继续如下处理：

小额和 CTTA 预付

如果支持小额和CTTA检查（卡片附加处理，第1字节第7位=‘1’）：

预付且资金不足

如果授权金额（标签“9F02”）大于电子现金余额（标签“9F79”），或者授权金额加上CTTA大于CTTAUL（如果CTTAUL不存在，使用CTTAL），那么卡片应当请求拒绝交易：

继续见7.7.17——拒绝交易。

预付且资金可用

如果授权金额（标签“9F02”）不大于电子现金余额（标签“9F79”），而且授权金额加上CTTA不大于CTTAUL（如果CTTAUL不存在，使用CTTAL），那么卡片将请求一个联机密文：

卡片应当设置CTTA=CTTA+授权金额。

设置电子现金余额=电子现金余额—授权金额。

设置可用脱机消费金额=CTTAUL（如果CTTAUL不存在，使用CTTAL）－CTTA。

结束小额和CTTA预付

小额预付

如果支持小额检查（卡片附加处理，第1字节第8位=‘1’）：

预付且资金不足

如果授权金额（标签“9F02”）大于电子现金余额（标签“9F79”），那么卡片应请求拒绝：

继续见7.7.17——拒绝交易。

预付且资金可用

如果授权金额（标签“9F02”）不大于电子现金余额（标签“9F79”），那么卡片将请求一个联机密文：

卡片应设置电子现金余额=电子现金余额—授权金额，设置可用脱机消费金额=电子现金余额。

继续见7.7.15——完成联机交易。

结束小额预付

结束预付

继续完成联机交易

具体如下：

——根据 JR/T 0025.5 附录 E 的密文版本 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（见本部分附录 E）；

注： qPBOC中不使用CDOL，密文由PDOL请求的数据生成；

——卡片应在 CVR 中指示一个 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，那么卡片应当包括它以便联机授权，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；

——继续见 7.7.18——结束 qPBOC 卡的 GPO 处理。

完成联机处理流程见图 16 所示。

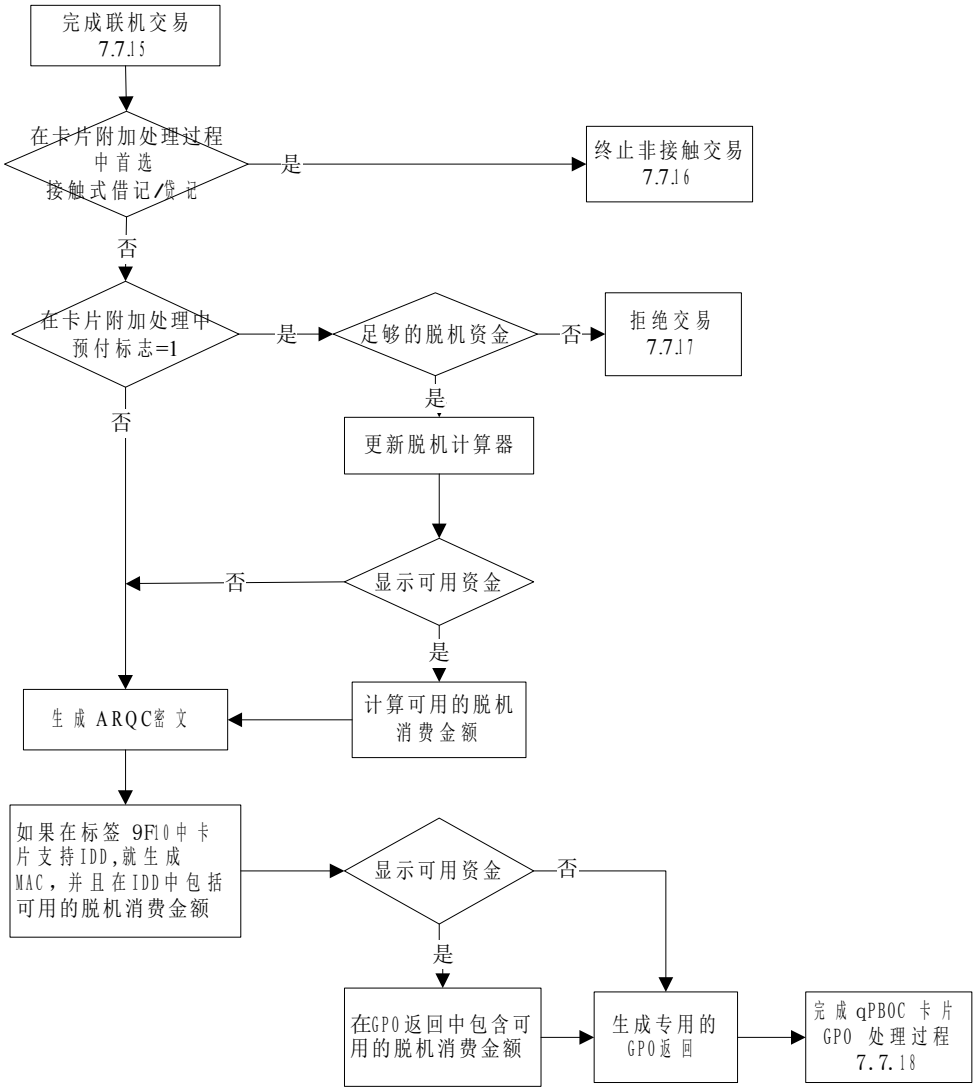

图 16　完成联机交易

7.7.16　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”

7.7.17　拒绝交易

无论在终端是仅脱机终端且脱机交易因为超出脱机交易上限不能完成，还是卡片用了预付选项且交易没有足够的资金等情况下，都要拒绝交易。

——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；

——卡片应当在 CVR 中指示一个 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 JR/T 0025.5 附录 E 的密文版本 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（见本部分附录 E）。

——继续见 7.7.18——结束 qPBOC 卡 GPO 处理。

7.7.18　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。

7.7.19 脱机交易的 READ RECORD 命令处理

对于脱机交易，交易将继续进行。终端对AFL中的每一条记录都发送READ RECORD命令。当卡成功返回最后一条记录后，交易防拔位被复位为零，用来指示终端已经完成与卡片的交易。

——卡片应当能够知道最后一条记录被读取；

——在响应最后一条 READ RECORD 命令前，卡片应当设置交易防拔位（卡片内部指示器）为零；

注：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，终端仍可以拒绝交易，但这对于真正的卡很少发生。

——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’，则卡片应当记录一条交易日志，记录交易日志的方法见 JR/T 0025.5 第 18 章。

为了提高交易的运行速度，终端应按照AFL中的顺序读取卡片记录。

7.7.20 有效期检查

终端通过READ RECORD命令获得卡片数据时，当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，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位不能复位为零。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 qPBOC 终端处理需求

当终端接收到来自卡片的正确的GPO命令响应，它将检查发卡行应用数据（标签“9F10”）来确定卡片提供的密文类型。根据密文类型，判断交易拒绝、联机处理或脱机批准。

7.8.1 密文类型检查

——如果返回 ARQC（发卡行应用数据（标签“9F10”）字节 5 的第 6-5 位=“10”），那么终端应将交易联机发送；

继续见7.8.3——终端联机处理。

——如果返回 AAC（发卡行应用数据（标签“9F10”）字节 5 的第 6-5 位=“00”），那么终端应拒绝交易；

继续见7.8.4——终端脱机拒绝。

——如果返回 TC（发卡行应用数据（标签“9F10”）字节 5 的第 6-5 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；

继续见7.8.4——终端脱机拒绝。

——终端应根据 JR/T 0025.5 处理 AFL，为 AFL 中的每一个记录发送 READ RECORD 命令；

——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；

——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 AIP 指示支持 DDA，那么终端应该根据 JR/T 0025.7 或 JR/T 0025.17 和附录 B fDDA 的定义验证 DDA 动态签名。

——如果 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。继续见 7.8.3——终端联机处理。

为了简化交易处理，建议在卡片个人化时，设置卡片交易属性的第 1 字节的第 6 位=‘0’，即如果执行 fDDA 失败，或者终端未执行脱机数据认证，则直接脱机拒绝交易。

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。继续见 7.8.5。

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。继续见 7.8.4

——终端脱机拒绝。

——如果返回 TC 并且 fDDA 被执行并通过，那么终端应批准交易。继续见 7.8.2——批准脱机交易。

7.8.2 批准脱机交易

——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，那么终端应当将其显示或打印出来；

——终端应用 GPO 响应所提供的密文（TC）和相关数据清分交易。详见附录 E 关于密文版本 17 所需数据。

7.8.3 终端联机处理

——终端应提示持卡人和商户卡片可以移开，交易正在请求授权；

——终端应执行下电时序并下电；

——终端应提示持卡人输入联机 PIN，并将联机 PIN 上送发卡行，同时根据 CVM 的设置进行签名处理；

——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）以及其它必需信息；

——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。见附录 E 关于支持密文版本 17 时联机报文应提供的最基本数据；

——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；

注： 如果这些交易已被清分，将由商户承担责任。

——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。

7.8.4 终端脱机拒绝

——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，那么终端应当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。

7.8.5 脱机数据认证失败且终端终止交易

——终端应执行下电时序并下电；

——读卡应终止非接触式交易并提示用户采用接触式接口。

qPBOC 终端处理流程见图 17 所示。

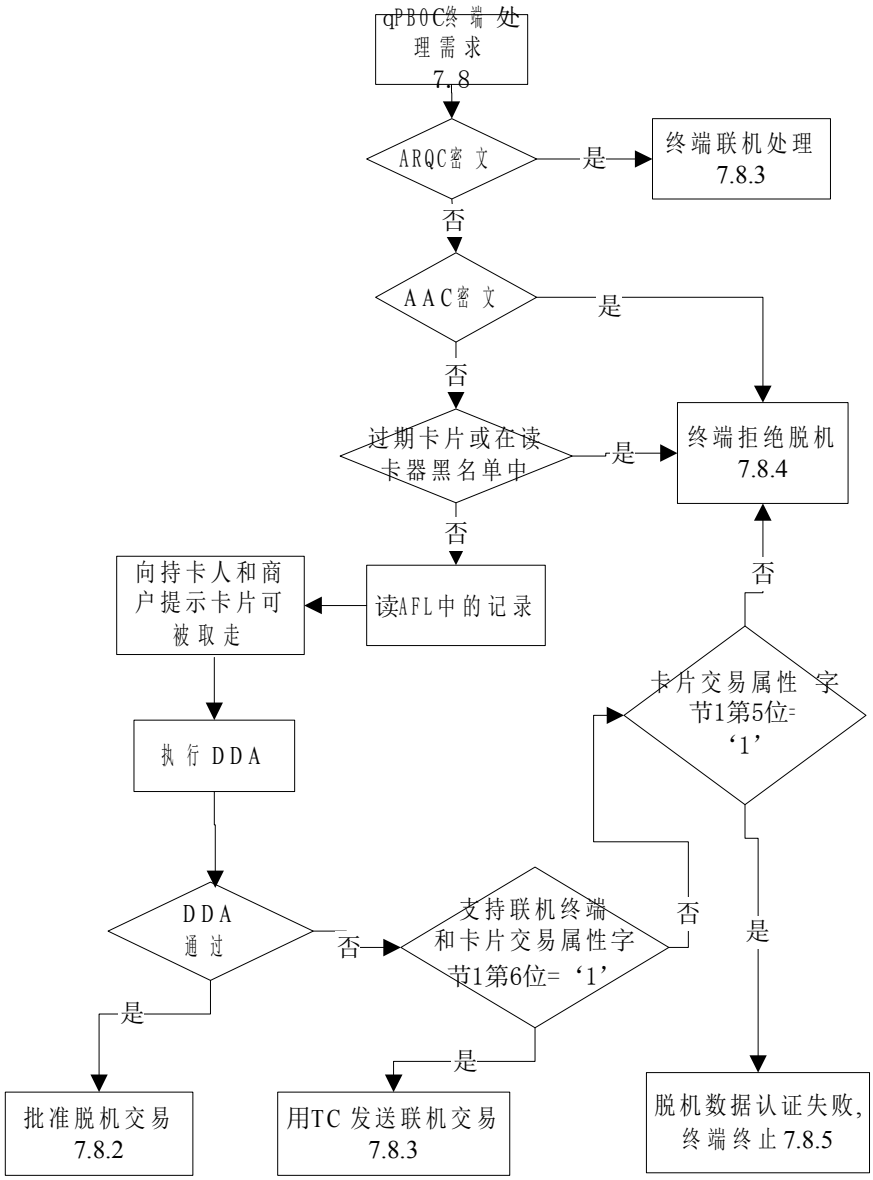

图 17　qPBOC 终端处理流程

7.9　qPBOC 的简化功能

qPBOC路径的基本行为和终端行为描述如下。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。

7.9.1　仅联机 qPBOC 的最小功能

——卡片应当根据 JR/T 0025.5 规定的格式响应 GPO 命令，而且应包括表 11 中所列的必备数据；

——卡片 qPBOC 路径应支持密文版本 17；

——简化 qPBOC 的 PDOL 应包含以下标签：

- “9F66”（终端交易属性）；
- “9F02”（授权金额）；
- “9F37”（不可预知数）。

7.9.2　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14中列出的数据。

表 14 PDOL 的最小数据集

PDOL中的数据标示	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，也可以增加其它的数据标识，但是发卡方应该明白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它相关的数据、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。

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，这个方法是不推荐的。

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.1qPBOC 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 0025.3 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它卡片要求的数据用于完成交易 **脱机** 对于脱机交易，作为对 GPO 的响应，卡片返回密文，卡片密文数据，其它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** 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，而且卡片可能有其它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 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，而且没有其它记录可被读出	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 执行 DDA 设置 JR/T 0025.6 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

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也对其它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它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，新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。原JR/T0025.12-2010中定义的fDDA算法本版规范将其定义为“00”版的fDDA。本规范中将定义一种新的fDDA算法，并将其版本定义为“01”。

对于符合本规范的卡片应同时支持“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。

对于符合本规范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.1 动态签名的产生

数据的连接和动态签名的产生与本规范第7部分5.3.5.1的第2步或第17部分5.2.4.1的第2步一致，以下内容除外：

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）。本规范第7部分5.3.5.1表13或第17部分5.2.4.1表9中的终端动态数据应由表B.1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.2中的内容。

表 B.1 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.2 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.2 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。这一过程见第7部分5.3或第17部分5.2。

验证动态签名过程与本规范第7部分5.3或第17部分5.2一致，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；
- 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。终端可以将表B.1指定的标签理解为“01”版本的fDDA缺省的DDOL。

注：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。

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”）标明卡片符合本版本规范，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

1）终端选择PPSE；

2）卡片返回唯一借记/贷记AID；

3）终端选择借记/贷记AID；

4）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”）
- 其它 PDOL 中指定的标签。

5）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
- 其它 PDOL 中指定的标签。

6）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；
- 其它和 fDDA 无关的数据。

7）终端读取AFL指定的记录；

8）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）；

此时卡片可以离开通讯区域。

9）终端认证动态签名；

10）如果fDDA认证通过，终端提供清算消息。

- 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

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。表C.1中“取回”列中SD表示数据元是只可在专门的设备上获取。

表 C.1 数据元

名字	格式 标签 长度	需求	描述	备份	获取	值
可用脱机消费金额 Available Offline Spending Amount	F: n 12 T: “9F5D” L: 6	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它包含在发卡行定义数据中	N	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） 如果IC卡的私钥的长度大于1024位，则此数据元通过读记录指令（READ RECORD）而不是通过GPO读出
卡片附加处理 Card Additional Processes	F: b 32 T: “9F68” L: 4	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	N	GET DATA (SD)	详见表13卡片附加处理

名字	格式 标签 长度	需求	描述	备份	获取	值
卡片 CVM 限额 Card CVM Limit	F: n 12 T: “9F6B” L: 6	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 本部分定义的持卡人验证是联机 PIN 和签名	N	GET DATA (SD)	此标签应可以被 PUT DATA 命令修改。
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	Y	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	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	N	GPO	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 保留 字节 2 位 8~1 保留
应用交互特征 Application Interchange Profile (AIP)	F: b 16 T: “82” L: 2	必备卡片数据元	说明此应用中卡片支持指定功能的能力	N	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 位 7~1 RFU

名字	格式 标签 长度	需求	描述	备份	获取	值
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	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	Y 或缺省为 1	GET DATA	
非接触终端脱机最低限额 Terminal Contactless Floor Limit	F: n 12 T: – L: 6	可选终端数据元	指示终端中的非接触最低限额	N/A	N/A	
非接触终端交易限额 Terminal Contactless Transaction Limit	F: n 12 T: – L: 6	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它界面尝试此交易	N/A	N/A	
终端执行 CVM 限额	F: n 12 T: – L: 6	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	N/A	
终端交易属性 Terminal Transaction Qualifiers	F: b 32 T: “9F66” L: 4	必备终端数据元	指示终端能力，需求和对卡片的参数选择	N/A	N/A	详见表 3 终端交易属性（标签“9F66”）

名字	格式 标签 长度	需求	描述	备份	获取	值
电子现金余额 Electronic Cash Balance	F: n 12 T: “9F79” L: 6	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	N	GET DATA	不应在 READ RECORD 命令中返回
电子现金余额上限 Electronic Cash Balance Limit	F: n 12 T: “9F77” L: 6	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	N	GET DATA (SD)	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	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	N	GET DATA	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	可选卡片数据元		N	GET DATA (SD)	不应在 READ RECORD 命令中返回
电子现金发卡行授权码 EC Issuer Authorization Code	F: a 6 T: “9F74” L: 6	可选卡片数据元	电子现金交易或 qPBOC 脱机批准的交易，卡片应当返回此数据元	N	READ RECORD	
应用版本号 Application Version Number	F：b16 T：“9F08” L：2	必备数据元	支付系统给应用分配的版本号。同 JR/T0025.5 中的定义。	N	READ RECORD	由支付系统定义

名字	格式 标签 长度	需求	描述	备份	获取	值
卡片认证相关数据 Card Authentication Related Data	F: b T: “9F69” L: var 8-16	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。	N/A	READ RECORD	字节 1：fDDA 版本号（在本版本规范中为“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。 注：在本版本规范中，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。

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

为了使得发卡行可以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，发卡行可以在这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
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 Gen 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 值就是

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或JR/T 0025.17。

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
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

IDD ID 选项	数据块长度	元素	
0x04	16 bytes	ATC	2 字节
		CTTA	低 5 位字节
		CTTAL	低 5 位字节
		填充	4 字节
0x05	8 bytes	ATC	2 字节
		可用脱机消费金额	低 5 位字节
		填充	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，不同点是它不支持密文版本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 x“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 个字节应当在报文中出现。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。

参考文献

[1] EMV 支付系统集成电路卡规范[S/OL]. 4.3
[2] Visa 非接触支付规范 2.1[S]. 2009