Q/CUP

中国银联股份有限公司企业标准

Q/CUP 075.1—2015

银联卡销售点终端（POS）应用流程规范

Technological Process Specification for POS Terminal Accepting CUP Cards

2015-10-12 发布　　2015-10-12 实施

中国银联股份有限公司发布

目　　次

前　言

《银联卡受理终端应用流程规范》对国内受理银联卡的销售点终端应遵循的应用处理流程进行了定义。

在国内推广银联卡非接触式应用的初期，为了在商户、收银员、终端维护人员等终端应用有密切联系的从业人员形成统一理解和推广合力，本标准在名称术语、卡与终端的交互、显示和打印等方面进行统一，供各收单机构参考使用。

本规范由中国银联股份有限公司提出。

本标准的主要起草人：王兰、李伟、谭颖。

银行卡销售点终端（POS）应用流程规范

1 范围

本标准对受理银联卡的销售点终端应遵循的应用流程进行了定义，包括终端管理功能、交易功能、终端界面、交易处理流程等。

本标准不对终端与POS中心之间的交易报文接口做定义。

本标准不包含POS终端硬件要求和安全技术要求。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

《银行卡销售点（POS）终端规范》（JR/T 0001-2009）

《中国金融集成电路（IC）卡规范》（JR/T 0025-2015）

《中国银联IC卡应用规范》（Q/CUP 047-2015）

3 术语和定义

3.1

银行卡 bank card

商业银行等金融机构及邮政储汇机构向社会发行的，具有消费信用、转账结算、存取现金等全部或部分功能的信用支付工具。

3.2

磁条卡 magnetic stripe card

磁记录介质卡片，其有三条记载磁编码信息的磁道。

注：物理特性符合GB/T 14916标准，磁条记录符合GB/T 15120 、GB/T 15694-1、GB/T 19584、GB/T17552标准。

3.3

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。

3.4

销售点终端 point of sale；POS

能够接受银行卡信息，具有通讯功能，并接受柜员的指令而完成金融交易信息和有关信息交换的设备。

3.5

持卡人 card holder

卡的合法持有人，即与卡对应的银行账户相联系的客户。

3.6

发卡机构 issuer

发行银行卡，维护与卡关联的账户，并与持卡人在这两方面具有协议关系的机构。

3.7

收单机构 acquirer

与商户签有协议或为持卡人提供服务，直接或间接凭交易单据（包括电子单据或纸质单据）参加交换的清算会员单位。

3.8

交易批次号 batch number

POS从签到起至对帐完成为止的交易为一批次，交易批次号标识一批交易。

POS中心为每个POS的每个批次分配一个批次号，在签到应答报文中下传给POS终端。POS终端批结算完成后，POS中心和POS终端的批次号各自加1。

3.9

主账号 primary account number

标识发卡机构和持卡人信息的数字代码。它由发卡机构标识代码、个人账户标识和校验位组成，是银行卡金融交易的主要账号，在银行卡金融交易中等同于卡号。

3.10

个人标识码 personal identification number； PIN

即个人密码，是在联机交易中识别持卡人身份合法性的数据信息，在计算机和网络系统中任何环节都不允许PIN以明文的方式出现。

3.11

报文鉴别码 messang authentication code；MAC

MAC是用来完成消息来源正确性鉴别，防止数据被篡改或非法用户窃入的数据。

3.12

安全控制信息 security control related information

与安全相关的控制信息，用于标识密文的类型。

3.13

密钥加密密钥 key encryption key； KEK

POS终端工作时对工作密钥进行加密的密钥，由专门人员设置并直接保存在系统硬件中，只能使用，不能读取，该密钥必须与加密算法放在同一加密芯片里，又称终端主密钥。

3.14

工作密钥 working key；WK

也称为数据密钥，通常指PIN加密密钥、MAC计算的密钥和磁道数据加密密钥。工作密钥必须经常更新。在联机更新的报文中对工作密钥必须用密钥加密密钥（KEK）加密，形成密文后进行传输。

3.15

降级 fallback

在某些情况下，IC卡有可能无法在支持芯片卡的终端上使用，比如IC卡本身坏了，或终端上的读写器发生了故障。在这种情况下，支付系统允许使用卡上的磁条来进行交易

3.16

SM2 算法 SM2 cryptographic algorithm

一种椭圆曲线公钥密码算法，其密钥长度为256比特。

3.17

SM3 算法 SM3 cryptographic algorithm

一种密码杂凑算法，其输出为256比特。

3.18

SM4 算法 SM4 cryptographic algorithm

一种分组密码算法，分组长度为128比特，密钥长度为128比特。

3.19

SM 算法 SM cryptographic algorithm

包括SM2算法、SM3算法、SM4算法。

4 POS 终端交易功能

4.1 联机交易功能

POS终端可具备以下联机交易：

交易名称	定义
余额查询	持卡人在 POS 终端查询所持卡账户余额的交易。查询的结果为账户的余额。该交易不参加资金清算。
消费	指持卡人在商户购买商品或取得服务时，通过POS联机结算。在POS上输入必要的数据后，将交易请求报文上送POS中心。POS中心进行检查和处理后，将结果回送POS。 消费交易 IC 卡的受理可通过接触、非接触方式受理，非接触式受理可通过 qPBOC 流程实现。
消费撤销	指商户对持卡人于当日当批内主动发起的对消费交易的取消。消费撤销交易应提供原交易的凭证，按业务要求在 POS 上输入有关数据，收到响应后，完成消费撤销交易并打印凭证。 消费撤销交易 IC 卡的受理可通过接触、非接触方式受理，非接触式受理可通过 qPBOC 流程实现。
退货	指商户对持卡人发起退货并将退货款项退还持卡人原扣款账户的过程。退货交易应提供原交易的凭证，收到响应后，完成退货交易并打印凭证。 消费退货交易 IC 卡的受理可通过接触、非接触方式受理，非接触式受理可通过 qPBOC 流程实现。
预授权	商户通过 POS 就持卡人预计支付金额向发卡行索取付款承诺的过程。预授权获准后在响应报文中回送授权码。 预授权交易 IC 卡的受理可通过接触、非接触方式受理，非接触式受理可通过 qPBOC 流程实现。
预授权撤销	商户通过 POS 向发卡行发出取消付款承诺。 预授权撤销交易 IC 卡的受理可通过接触、非接触方式受理，非接触式受理可通过 qPBOC 流程实现。
预授权完成	持卡人对于已取得预授权的交易，在发卡行允许的范围内，做支付结算。预授权完成是依据在预授权交易中得到的授权码进行消费。 预授权完成交易 IC 卡的受理可通过接触、非接触方式受理，非接触式受理可通过 qPBOC 流程实现。
预授权完成撤销	商户对持卡人已经完成的预授权完成交易，于当日当批内主动发起的预授权完成交易的取消。预授权完成撤销交易应提供原交易的凭证，收到响应后，完成预授权完成撤销交易。 预授权完成撤销交易 IC 卡的受理可通过接触、非接触方式受理，非接触式受理可通过 qPBOC 流程实现。
自动冲正	在发生联机交易请求过程中，如果 POS 在规定时间内没有收到 POS 中心的响应信息或响应信息 MAC 校验失败，以及 IC 卡拒绝了发卡行批准的联机交易等情况下，POS 应在下笔交易前自动发送该笔交易的冲正信息，通知 POS 中心取消该笔交易。
闪付凭密	闪付凭密交易是指小额免密业务时，持卡人消费金额超出发卡行设定的当日累计限额，需通过闪付凭密交易完成非接消费交易受理。闪付凭密交易不支持 Pin ByPass，交易流程同消费。

4.2 非联机交易功能

POS终端可具备以下非联机交易功能：

交易名称	定义
电子现金余额查询	电子现金余额查询命令允许终端直接读取 IC 卡中可脱机消费的余额。
电子现金明细查询	脱机查询电子现金交易明细信息。

电子现金消费交易	持卡人使用具有电子现金账户的银行卡进行购物或获取服务，该交易为脱机类交易，经批准的交易金额实时地反映在卡片的电子现金余额中。本交易在批结前做为脱机类交易上送。该交易不能撤销。此交易在消费终端上脱机进行。

4.3 管理交易功能

POS终端可具备以下管理交易功能：

交易名称	定义
签到管理	终端的签到管理包括三种交易：POS 签到、操作员签到、收银员积分签到。
批结算管理	POS 批结算之前，先将所有未上送的离线类和 IC 卡脱机交易上送到 POS 中心，结算时将当批次交易的借记总金额、借记总笔数、贷记总金额和贷记总笔数上送 POS 中心，批结算完成后，POS 终端将打印结算总计单，失败的脱机交易和无法上送的脱机交易，打印明细单。
批上送	POS 与 POS 中心批结算对账不平时，POS 终端将当前内存中本批次的成功交易记录上送 POS 中心。
签退管理	操作员可选择“签退”功能， POS 在签退之前先进行批结算，将所有未上送交易上送。
参数传递	POS 中心如有终端参数更新，可通过联机交易或签到下发通知至 POS 终端，也可由 POS 终端主动发起。通过参数的更新实现功能和业务的控制。

5 POS 终端界面

5.1 待机界面

POS终端待机界面按确认键或取消键都可切换到功能选择主界面，进入功能选择主界面后在规定的时间内不操作，自动返回待机界面。待机界面的显示内容宜包含终端程序版本号，待机界面提示语为“请挥卡、插卡或刷卡”。

POS终端待机界面下可通过快捷键方式快速进入交易功能界面，快捷键“1”宜为电子现金交易，快捷键“9”宜为IC卡借贷记帐户交易。

5.2 用卡提示界面

对支持非接触受理的交易用卡提示语统一为“请挥卡、插卡或刷卡”。不支持非接触式受理的交易用卡提示语为“请插卡或刷卡”。可参考图1 。

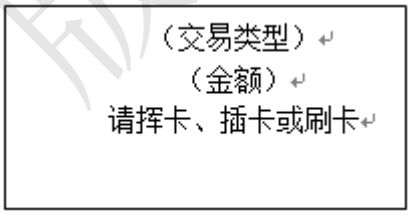


图1 用卡提示用语

5.3 功能选择主界面

操作员可以在功能选择主界面按相应的数字键选择交易或进入子界面。进入子界面后在规定的时间内不操作，自动返回待机界面。功能交易界面可参考图2 。

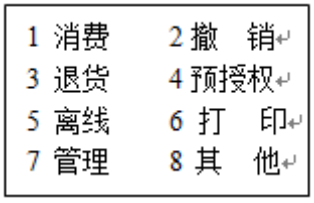


图2 功能选择主界面

5.4 闪付凭密界面

对于非接小额免签免密业务，如持卡人当天消费金额超出发卡行设定当日累计金额限定，操作员可通过POS终端闪付凭密菜单实现非接交易的受理，可参考图3 。

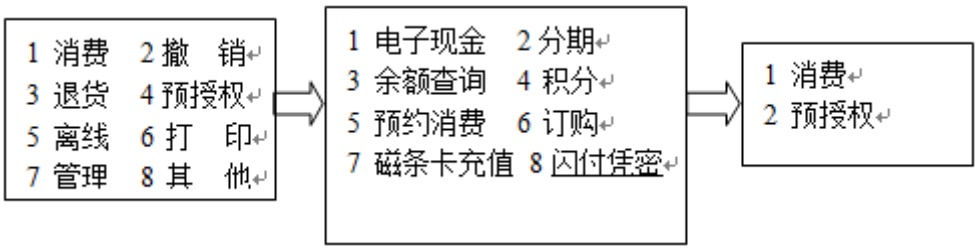


图3 闪付凭密

6 POS 终端交易处理流程

6.1 POS 终端 IC 卡受理流程

6.1.1 概述

本节主要定义了POS终端受理金融IC卡的基础处理逻辑和流程，受理银联卡的POS终端应用应遵循本节提出的相关要求。

6.1.2 基础逻辑处理流程

POS终端受理交易时，应依据卡片类型以及卡片受理方式进行逻辑判断，采用交易不同方式的受理流程。详细见图4 。

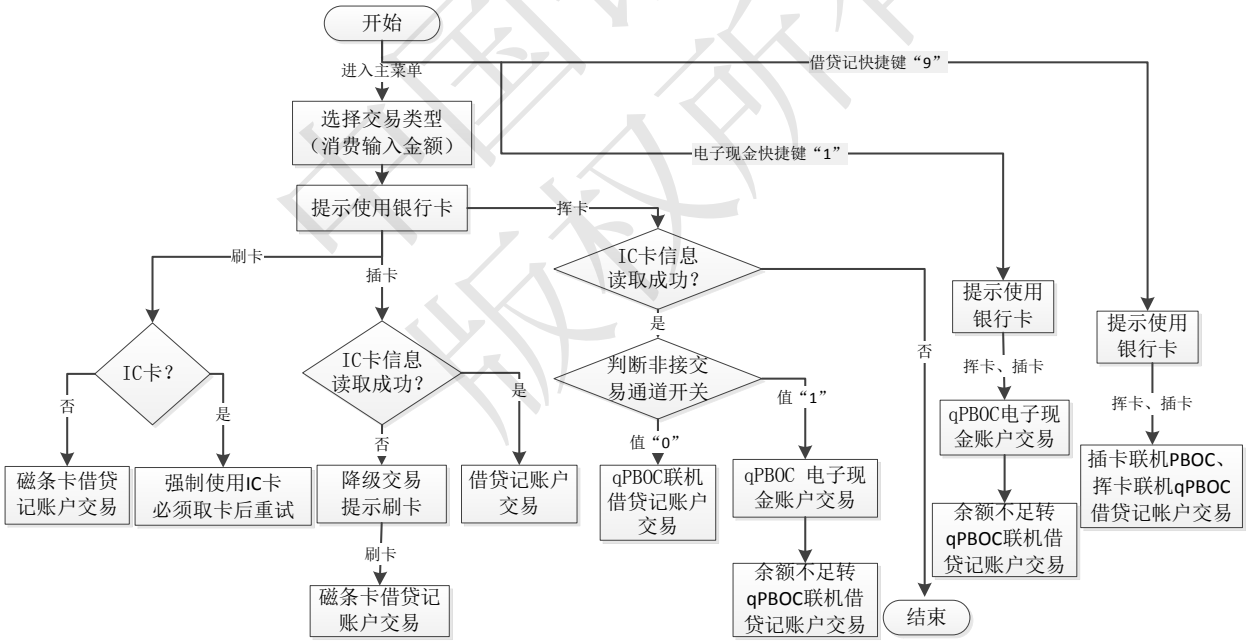


图4 读卡基础逻辑处理流程

POS终端读卡基础逻辑处理流程说明：

——终端应预先设置终端内部参数“非接交易通道开关”，IC卡非接挥卡时判断该参数取值，为‘0’，挥卡交易优先采用qPBOC联机借贷记帐户交易流程；为‘1’挥卡交易优先采用qPBOC电子现金账户交易流程，余额不足且存在借贷记主账户，转qPBOC联机借贷记主账户交易流程。

——待机界面可通过快捷键‘1’或按电子现金交易菜单，插卡、挥卡均进行电子现金交易，电子现金交易余额不足时转qPBOC联机借贷记流程。

——待机界面可通过快捷键“9”进入IC卡借贷记交易界面，插卡采用PBOC联机借贷记帐户交易流程；挥卡采用qPBOC联机借贷记帐户交易流程。

——IC卡插卡选择进行PBOC联机借贷记交易；如果读取芯片信息失败又存在磁条卡，支持降级处理。

POS终端对特殊卡片的处理：

——若卡片为纯电子现金卡，则POS在消费交易使用联机借贷记账户时（包括快捷借贷记及菜单进入挥卡优先联机借贷记），无法交易，提示“纯电子现金卡，请使用电子现金。”。授权类交易提示“授权交易不可使用电子现金”。

——卡片或者手机内卡片应用只支持联机借贷记应用，通过快捷键‘1’和电子现金菜单进入电子现金时，终端无电子现金应用转qPBOC联机借贷记账户交易。

6.1.3 小额免密业务处理流程

对于消费、预授权交易，通过非接触式发起的联机借贷记帐户交易，如金额小于一定金额，可免输入密码。非接小额免签处理流程中的外卡指境外发行的银联卡。详细见图5 。

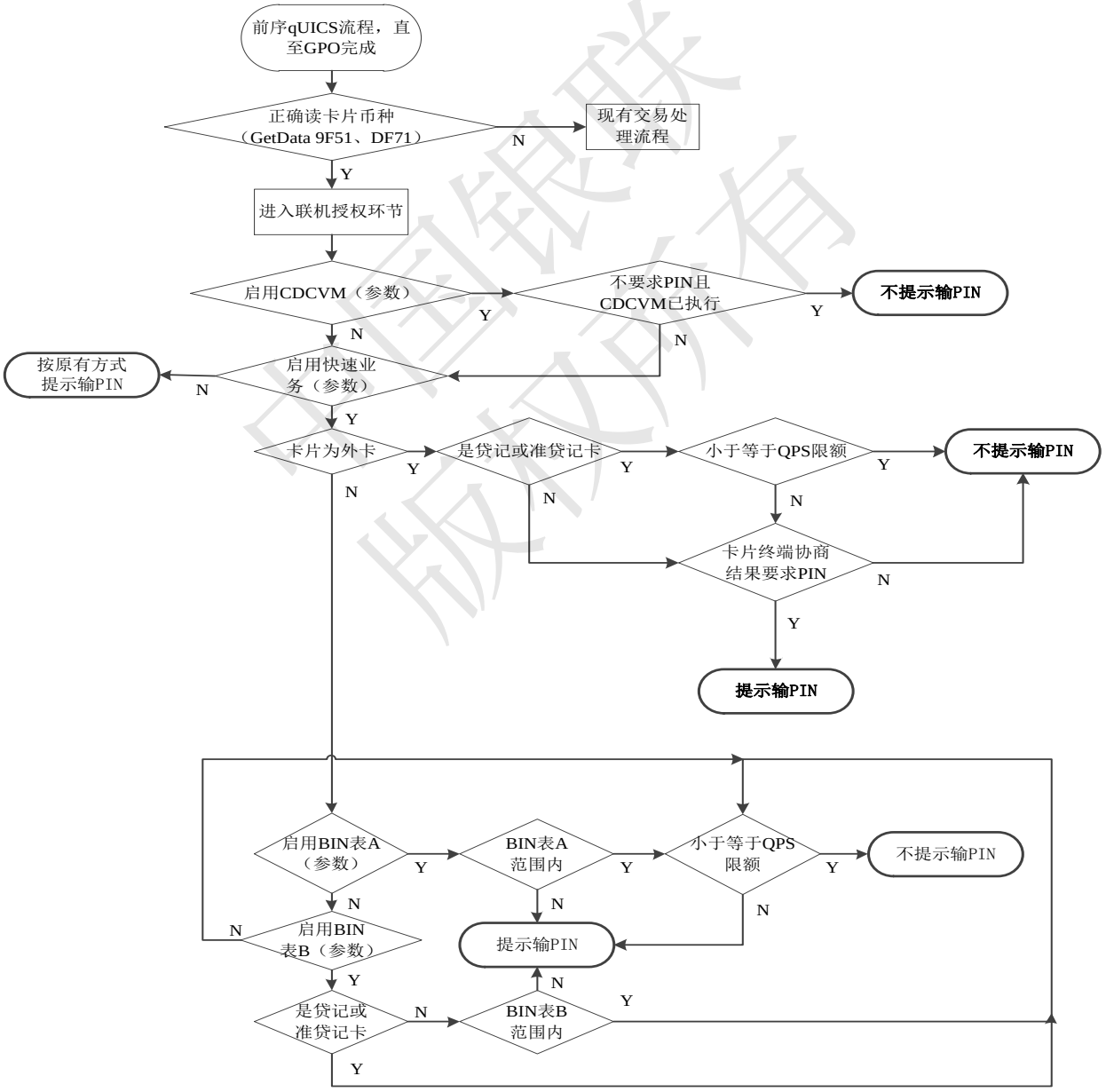


图5 非接小额免密处理流程

小额免密流程说明：

——POS终端小额免密业务功能，需加载两张bin表，bin表A和bin表B。bin表中分别放置小额免密业务试点一期和试点二期的卡bin。同时通过配置bin表开关等免密的业务参数，选择不同bin表的启用，实现试点一期二期的切换。小额免密控制参数可参见7.6 。

——POS终端对境内卡、境外发行的银联卡采用不同的处理逻辑，境内卡通过卡bin表及小额免密控制开关判断是否免密；境外发行的银联卡，贷记卡仅判断交易金额，借记卡以CVM要求为准。

——满足小额免密业务需求，需要对POS终端的和收单系统同时进行改造，收单平台应同时加载商户白名单、bin表等，后台判断是否为小额免密交易，对免密的交易在交易报文中进行标识。收单系统改造详细内容可参见附录H。

——小额免密交易发卡行如设置了当日交易限额，对当天交易金额超限的卡片，可通过新增的“闪付凭密”菜单进入完成消费。闪付凭密交易不支持Pin ByPass。

6.1.4 小额免签业务处理流程

对于消费、预授权交易，通过IC卡接触式、非接触式以及磁条刷卡交易，小于一定金额，予以免签名处理。详细见图6 。

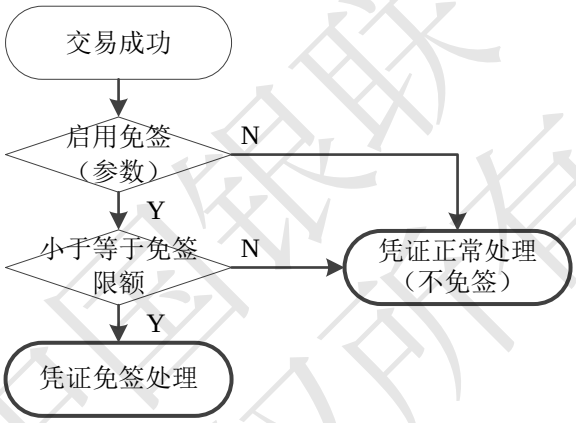


图6 小额免签处理流程

POS终端如支持小额免签业务，终端签购单应打印免签提示信息，宜打印“交易金额未超过XXX元，无需签名”。

6.2 POS 终端交易流程

POS终端可受理的交易流程可参考附录BB.1 。

7 POS 终端参数化控制

7.1 概述

本节主要定义了POS终端应用要具备的控制参数，受理银联卡的POS终端应用可参考以下参数设计、类型和取值等要求。详细可参考附录F。

根据初始和变更的方式，POS终端参数可分为出厂参数、下发参数、可设定参数和联机可更改参数四类。出厂参数不可更改，其他参数宜支持通过收单POS中心远程参数等能力更新POS，灵活实现对POS终端的业务功能控制。

7.2 出厂参数

出厂参数主要是与硬件相关的、影响硬件设备使用和运作的基本参数。出厂的参数应当在设备出厂时全部写入，不允许更改。

7.3 下发参数

下发参数主要是用于设备自身管理和配置的参数。该部分参数可以通过PC工具或POS界面进行设定，可能随着程序版本的更换而发生变化。

7.4 可设定参数

可设定参数主要是与交易内容直接相关并需要长期存放在POS终端中使用的应用参数，这些参数在收单机构的控制下可以进行配置。

7.5 联机可更改参数

联机可更改参数可以通过POS参数传递获得。

7.6 业务控制参数

某些参数既可出现在可设定参数，又出现在联机可更改参数。通过收单机构的业务配置，实现灵活的业务控制。例如非接交易业务控制参数可即通过POS中心配置，也可由收单机构在终端侧配置。

名称	内容	默认值
非接交易通道开关	0-非接联机优先，1-电子现金优先	0
闪卡当笔处理时间	10s	10s
闪卡全处理时间	60s	60s
非接小额免密开关	0-关闭，1 开启	1
非接小额免密限额	300 元	300 元
bin 表 A	0-关闭，1 开启	1
bin 表 B	0-关闭，1 开启	0
小额免签开关	0-关闭，1 开启	1
免签限额	300 元	300 元

8 POS 终端支持 SM 算法

8.1 概述

POS终端支持SM算法分为两种，一种为POS终端可受理双算法IC卡，PIN、磁道信息、MAC等数据加密仍采用3DES算法；另一种为POS终端可受理双算法IC卡，PIN、磁道信息、MAC数据加密也采用SM4算法。PIN、MAC以及磁道信息数据的SM4算法加密方法可参考附录C、附录D、附录E。

8.2 POS 终端支持 SM 算法的软硬件要求

仅支持双算法IC卡受理的POS终端，POS终端硬件无特殊要求，应用软件应具备对支持SM2算法的IC卡公钥参数下载功能。

POS终端如支持PIN、磁道信息等数据信息加密，硬件上应具备专用SM算法芯片存放加密密钥，应用软件应具备对支持SM2算法的IC卡公钥参数下载功能。

8.3 SM4 算法交易报文要求

8.3.1 不支持数据信息使用 SM4 算法加密

POS终端受理双算法IC卡，信息数据采用3DES算法，POS终端应从收单平台POS中心准确下载SM2算法IC卡公钥参数。POS终端交易报文应包含备以下特殊内容：

——通知收单侧POS中心需要下载SM2算法公钥

——收单侧POS中心通过联机交易通知POS终端发起包含SM2算法公钥的参数下载

——POS终端通过参数传递交易获取到SM2算法公钥参数

8.3.2 支持数据信息使用 SM4 算法加密

POS终端受理国密IC卡，信息数据采用SM4算法，POS终端应从收单平台POS中心准确下载SM2算法IC卡公钥参数，同时对PIN、MAC、磁道数据进行SM4算法加密。POS终端交易报文应包含备以下特殊内容：

——通知收单侧POS中心需要下载SM2算法公钥

——收单侧POS中心通过联机交易通知POS终端发起包含SM2算法公钥的参数下载

——POS终端通过参数传递交易获取到SM2算法公钥参数

——报文包含使用SM4算法计算的128bit的PIN密文数据

——报文包含使用SM4算法计算的64bit的MAC密文数据

附录 A
（资料性附录）
对应答码的处理

交易返回 POS 终端时都有 39 域，POS 终端和终端操作员根据应答码要采取相应的操作，可以把操作分为以下几类：

A：交易成功

B：交易失败，可重试

C：交易失败，不需要重试

D：交易失败，终端操作员处理

E：交易失败，系统故障，不需要重试

注 1：如果 39 域的内容不能在下表中找到，就显示“交易失败”

C.1 应答码表

代码	意义	类别	采取的措施	终端显示内容（推荐）
0	承兑或交易成功	A	成功	交易成功
1	查发卡方	C	失败	请持卡人与发卡银行联系
3	无效商户	C	失败	无效商户
4	没收卡	D	吞卡、没收	此卡为无效卡（POS）
5	身份认证失败	C	失败	持卡人认证失败
10	部分金额批准	A	成功，需提示	显示部分批准金额，提示操作员
11	重要人物批准（VIP）	A	成功	此为 VIP 客户
12	无效的关联交易	C	失败	无效交易
13	无效金额	B	失败	无效金额
14	无效卡号（无此账号）	B	失败	无效卡号
15	无此发卡方	C	失败	此卡无对应发卡方
21	卡未初始化	C	失败	该卡未初始化或睡眠卡

代码	意义	类别	采取的措施	终端显示内容（推荐）
22	故障怀疑，关联交易错误	C	失败	操作有误，或超出交易允许天数
25	找不到原始交易	C	失败	没有原始交易，请联系发卡方
30	报文格式错误	C	失败	请重试
34	有作弊嫌疑	D	吞卡、没收	作弊卡,吞卡
38	超过允许的 PIN 试输入	D	失败	密码错误次数超限，请与发卡方联系
40	请求的功能尚不支持	C	失败	发卡方不支持的交易
41	挂失卡	D	吞卡、没收	挂失卡（POS）
43	被窃卡	D	吞卡、没收	被窃卡（POS）
45	不允许降级交易	C	失败	请使用芯片
51	资金不足	C	失败	可用余额不足
54	过期的卡	C	失败	该卡已过期
55	不正确的 PIN	C	失败	密码错
57	不允许持卡人进行的交易	C	失败	不允许此卡交易
58	不允许终端进行的交易	C	失败	发卡方不允许该卡在本终端进行此交易
59	有作弊嫌疑	C	失败	卡片校验错
61	超出金额限制	C	失败	交易金额超限
62	受限制的卡	C	失败	受限制的卡
64	原始金额错误	C	失败	交易金额与原交易不匹配
65	超出取款/消费次数限制	C	失败	超出取款次数限制

代码	意义	类别	采取的措施	终端显示内容（推荐）
68	发卡行响应超时	B	失败	交易超时，请重试
75	允许的输入 PIN 次数超限	C	失败	密码错误次数超限
90	正在日终处理	C	失败	系统日切，请稍后重试
91	发卡方不能操作	C	失败	发卡方状态不正常，请稍后重试
92	金融机构或中间网络设施找不到或无法达到	C	失败	发卡方线路异常，请稍后重试
94	重复交易	C	失败	拒绝，重复交易，请稍后重试
96	银联处理中心系统异常、失效	C	失败	拒绝，交换中心异常，请稍后重试
97	ATM/POS 终端号找不到	D	失败	终端号未登记
98	银联处理中心收不到发卡方应答	E	失败	发卡方超时
99	PIN 格式错	B	失败	PIN 格式错，请重新签到
A0	MAC 鉴别失败	B	失败	MAC 校验错，请重新签到
A1	转账货币不一致	C	失败	转账货币不一致
A2	有缺陷的成功	A	成功	交易成功，请向资金转入行确认
A3	资金到账行无此账户	C	失败	资金到账行账号不正确
A4	有缺陷的成功	A	成功	交易成功，请向资金到账行确认
A5	有缺陷的成功	A	成功	交易成功，请向资金到账行确认
A6	有缺陷的成功	A	成功	交易成功，请向资金到账行确认
A7	安全处理失败	C		安全处理失败

附录 B
（资料性附录）
POS 终端交易流程

B.1　交易流程

B.1.1　余额查询

B.1.1.1　联机余额查询交易处理流程

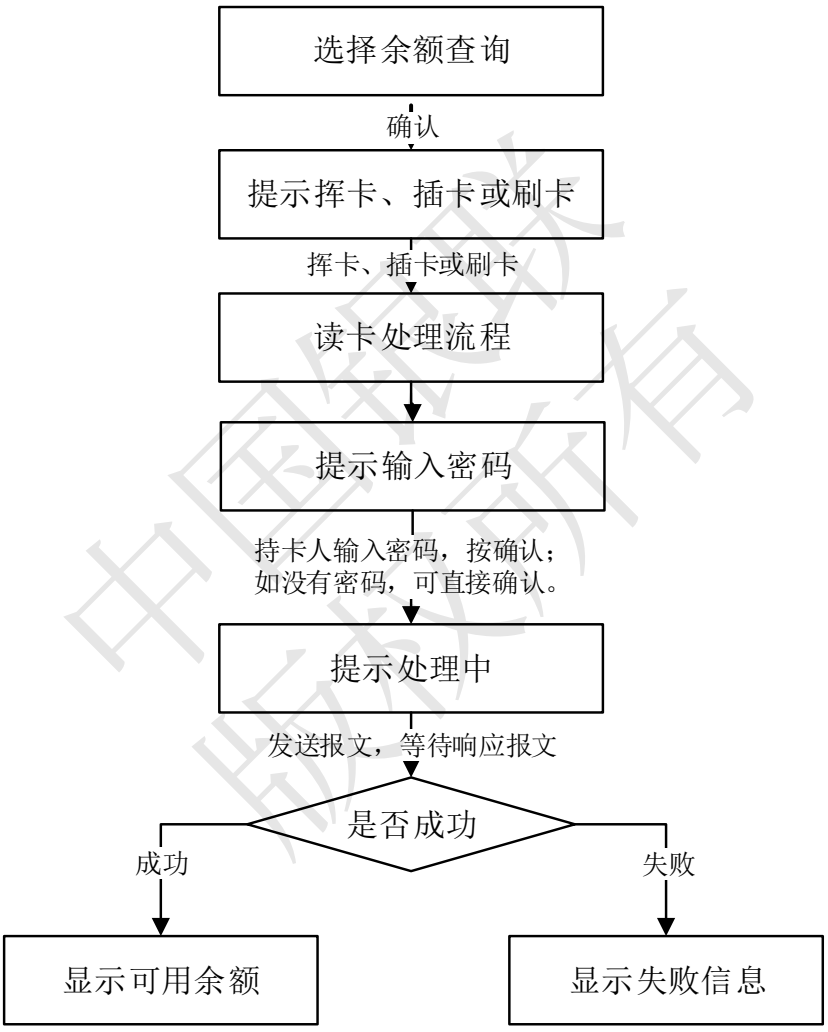


图7　银行卡余额查询交易处理流程

B.1.1.2　电子现金的IC卡余额查询交易处理流程

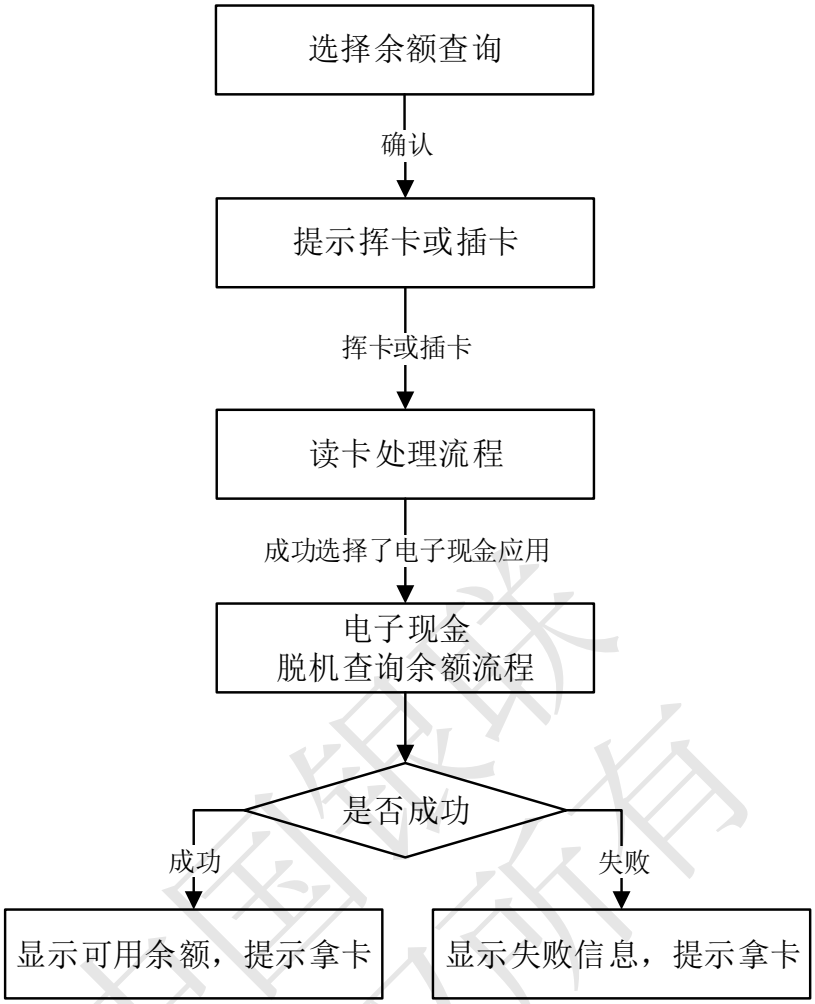


图8　IC 卡电子现金余额查询交易处理流程

B.1.2　消费

B.1.2.1　银行卡消费交易处理流程

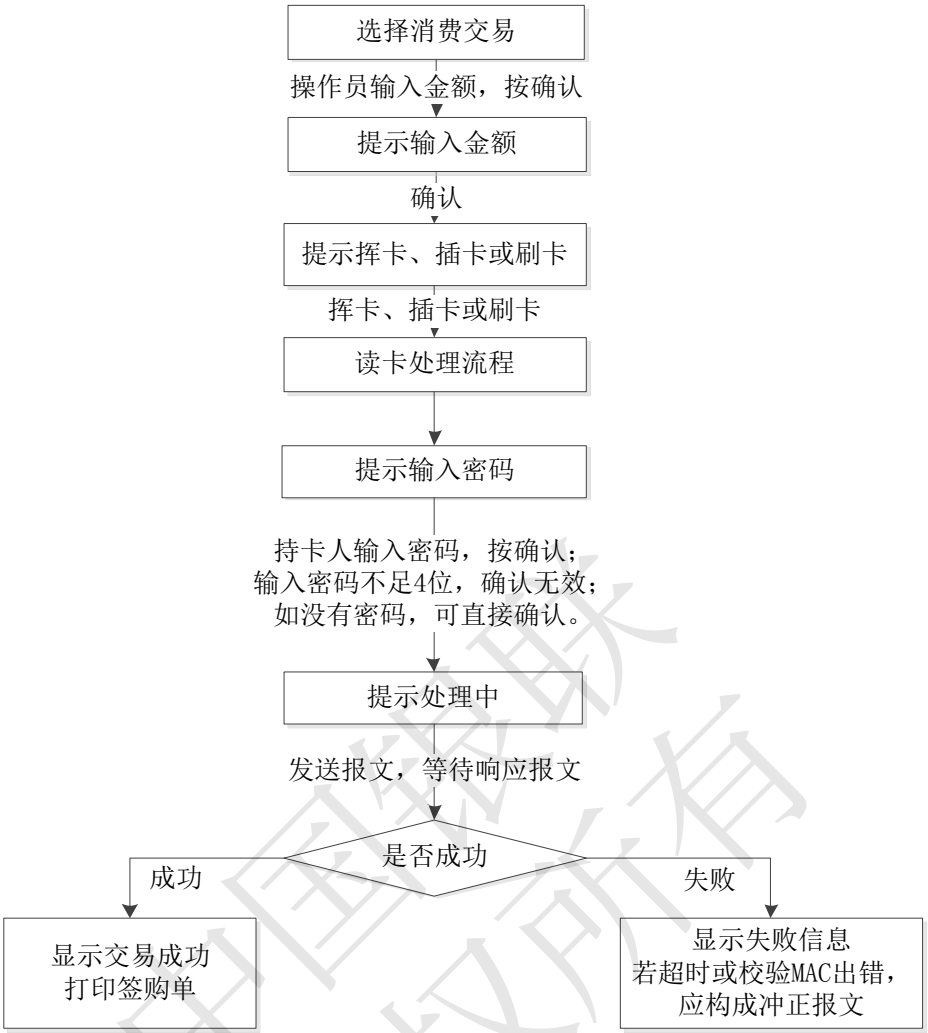


图9　银行卡消费交易处理流程

B.1.2.2　IC卡脱机消费交易处理流程

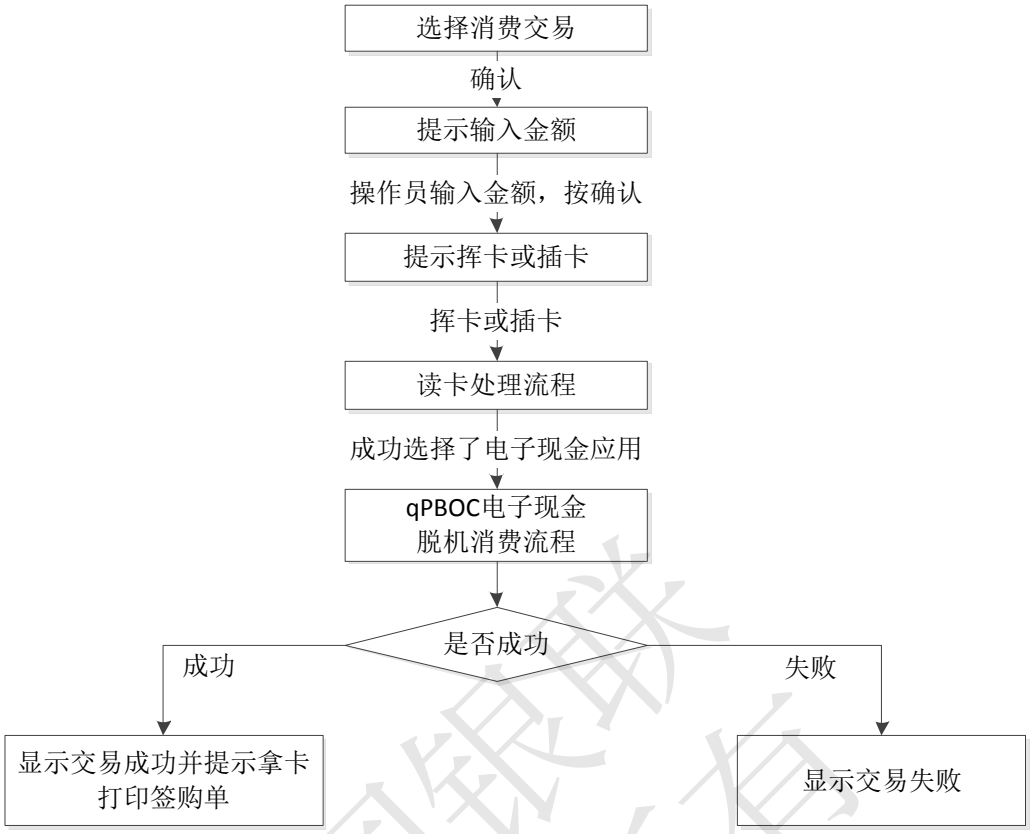


图10　IC 卡脱机消费交易处理流程

B.1.3　消费撤销

B.1.3.1　银行卡消费撤销交易处理流程

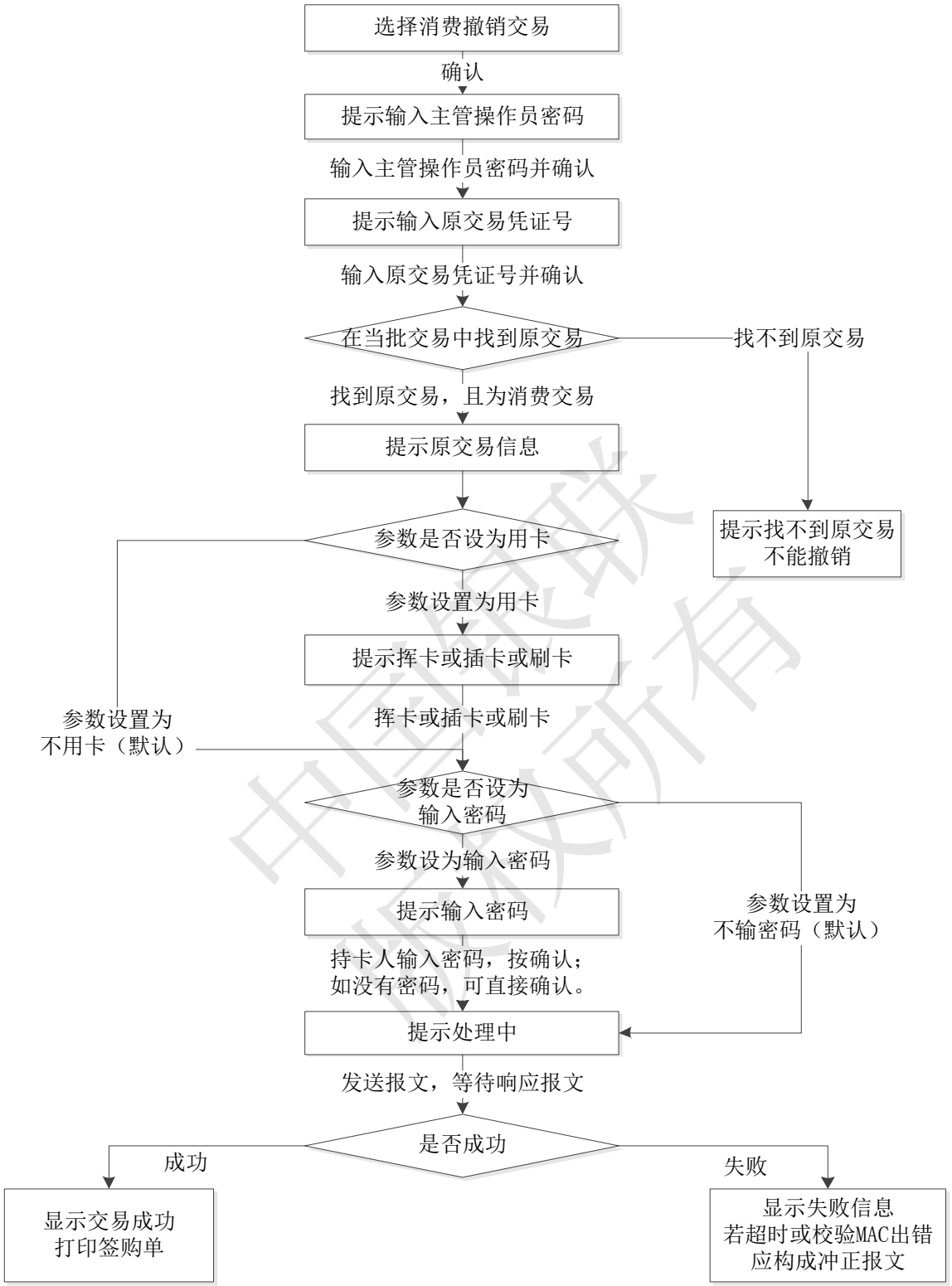


图11　银行卡消费撤销交易处理流程

B.1.4　退货

B.1.4.1　银行卡退货交易处理流程

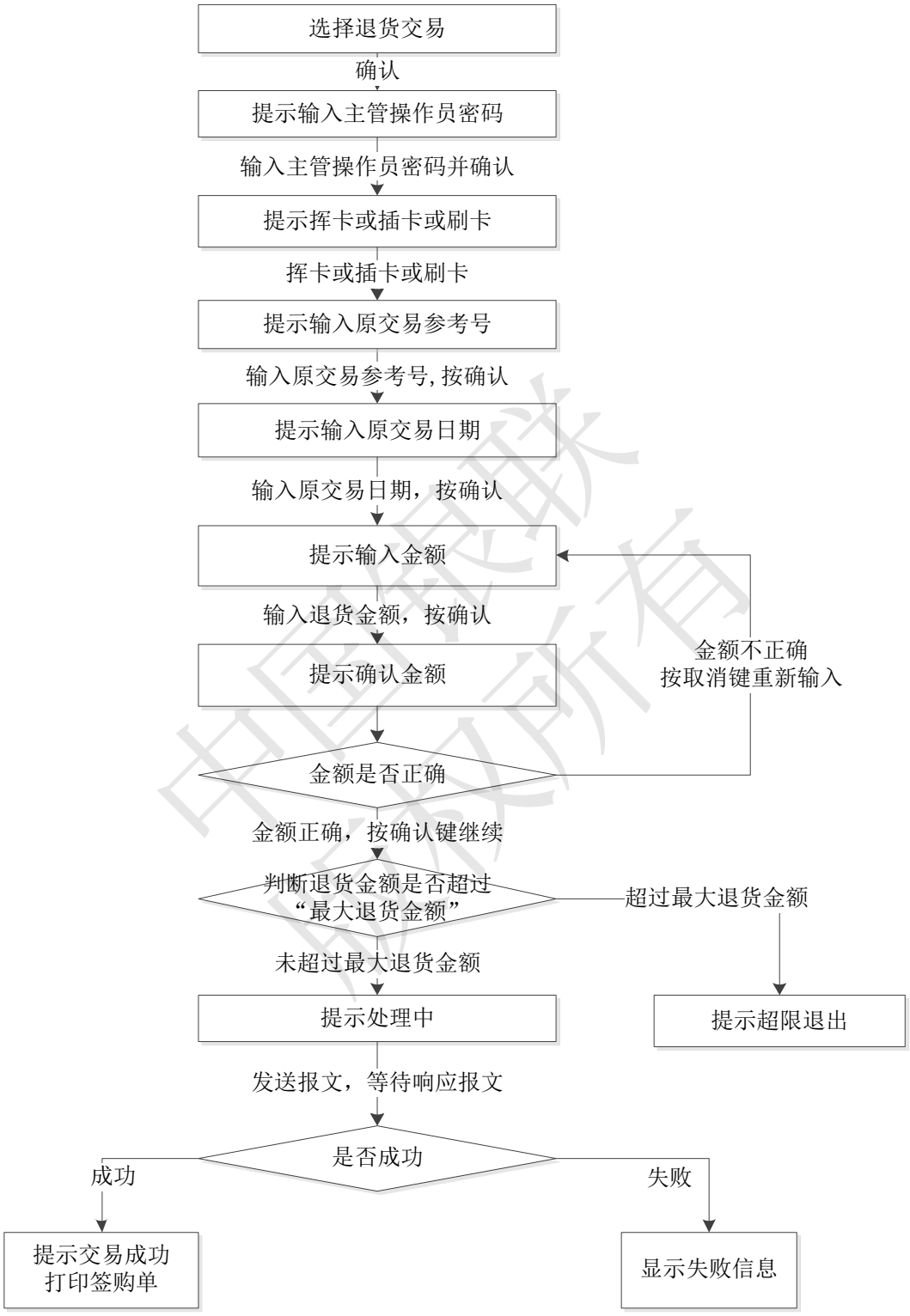


图12　银行卡退货交易处理流程

B.1.4.2　IC卡电子现金退货交易处理流程

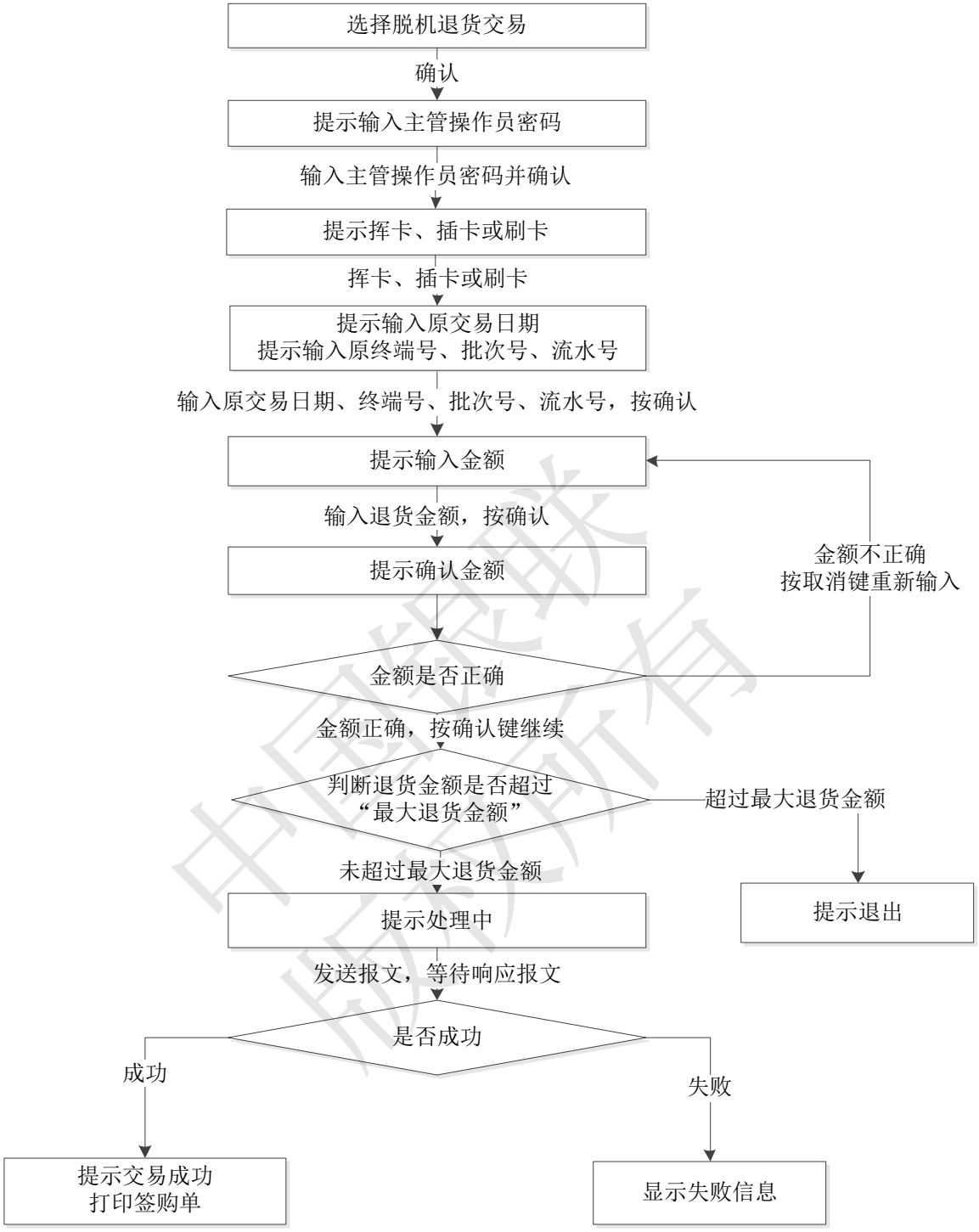


图13　IC 卡电子现金退货交易处理流程

B.1.5　预授权

B.1.5.1　银行卡预授权交易处理流程

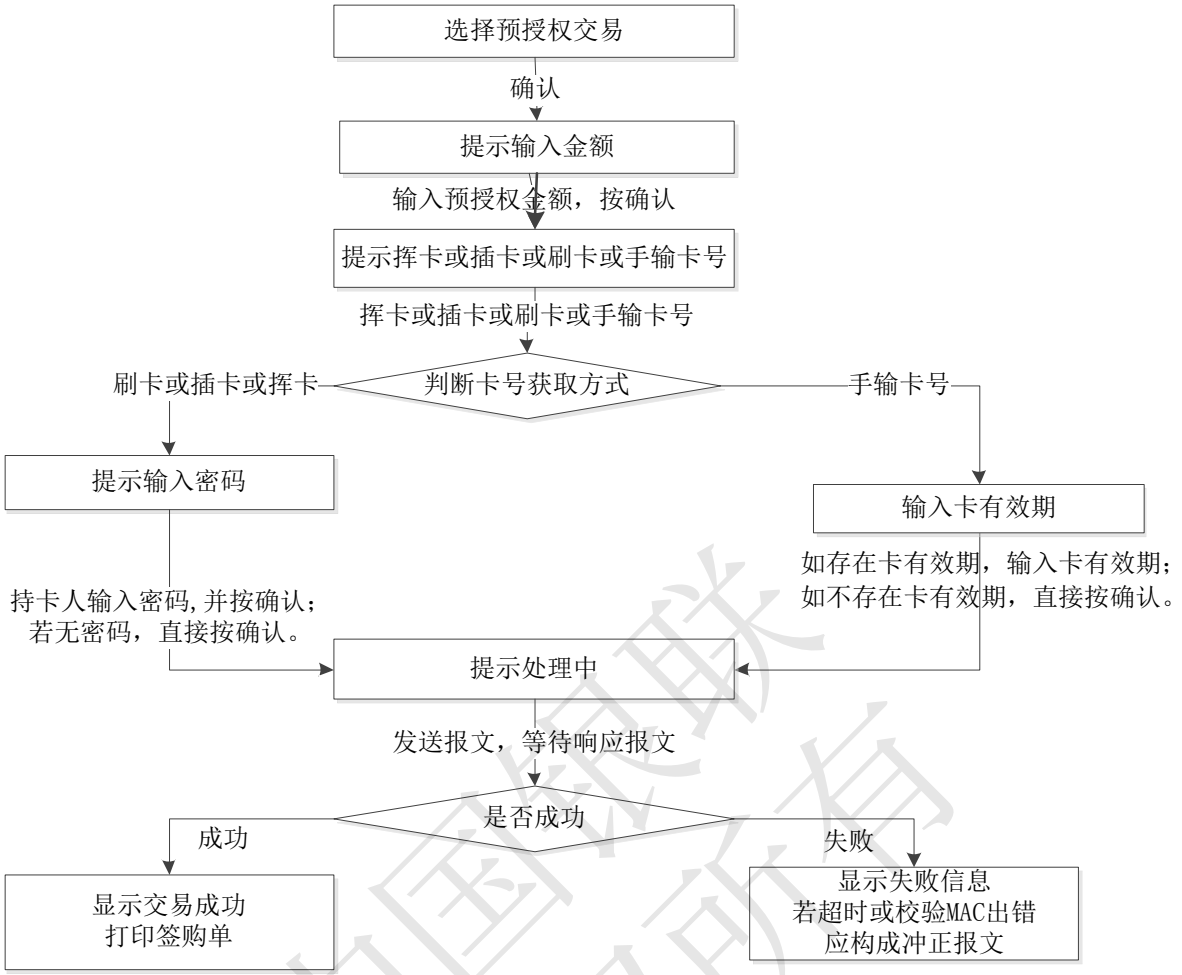


图14　银行卡预授权交易处理流程

B.1.6　预授权撤销

B.1.6.1　银行卡预授权撤销交易处理流程

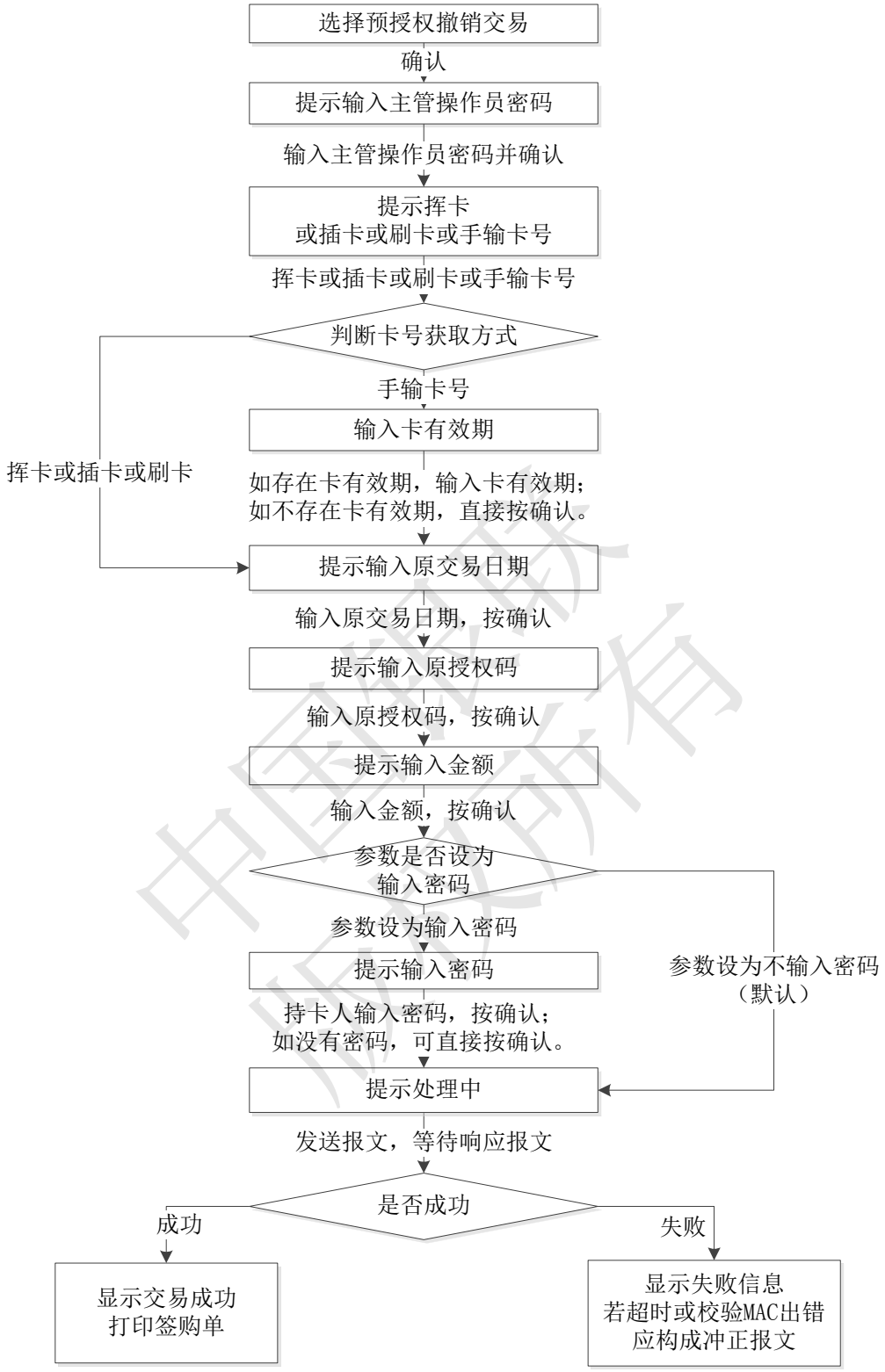


图15　银行卡预授权撤销交易处理流程

B.1.7　预授权完成

B.1.7.1　银行卡预授权完成（通知）交易处理流程

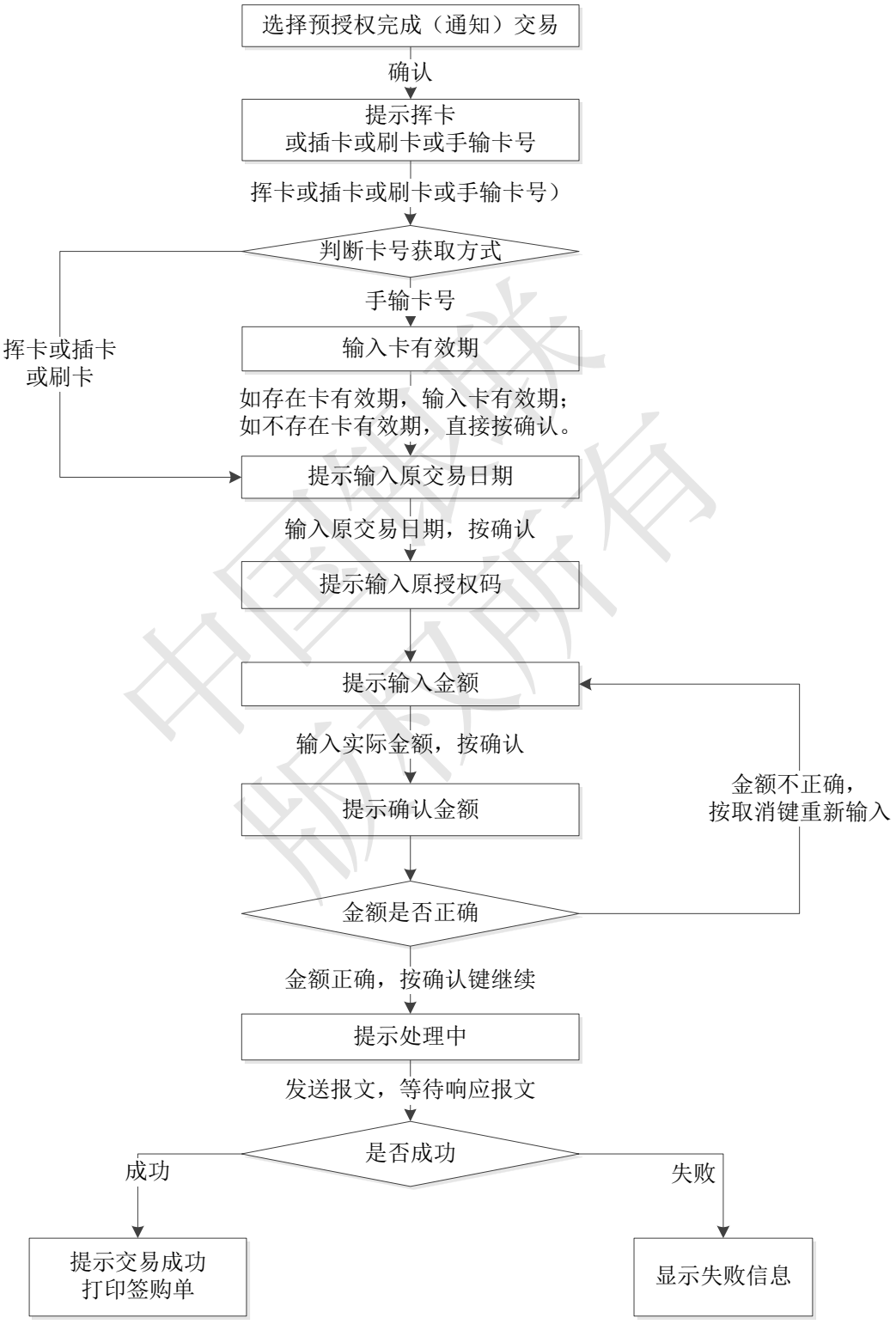

选择预授权完成（通知）交易
确认
提示挥卡
或插卡或刷卡或手输卡号
挥卡或插卡或刷卡或手输卡号）
判断卡号获取方式
手输卡号
挥卡或插卡
或刷卡
输入卡有效期
如存在卡有效期，输入卡有效期；
如不存在卡有效期，直接按确认。
提示输入原交易日期
输入原交易日期，按确认
提示输入原授权码
提示输入金额
输入实际金额，按确认
提示确认金额
金额不正确，
按取消键重新输入
金额是否正确
金额正确，按确认键继续
提示处理中
发送报文，等待响应报文
是否成功
成功
失败
提示交易成功
打印签购单
显示失败信息

图16　银行卡预授权完成（通知）交易处理流程

B.1.7.2　银行卡预授权完成（请求）交易处理流程

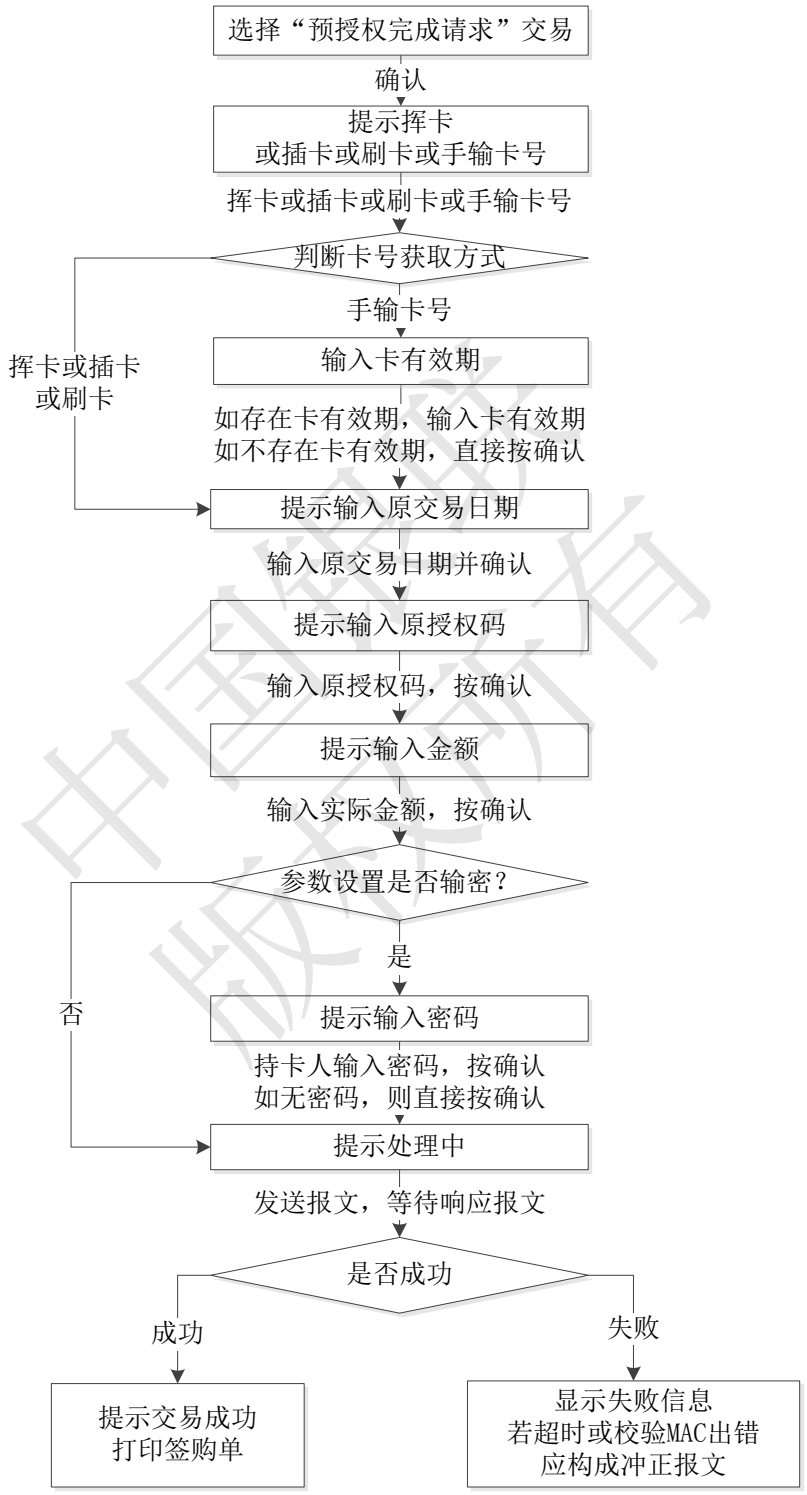


图17　银行卡预授权完成（请求）交易处理流程

B.1.8　预授权完成（请求）撤销

B.1.8.1　银行卡预授权完成（请求）撤销交易处理流程

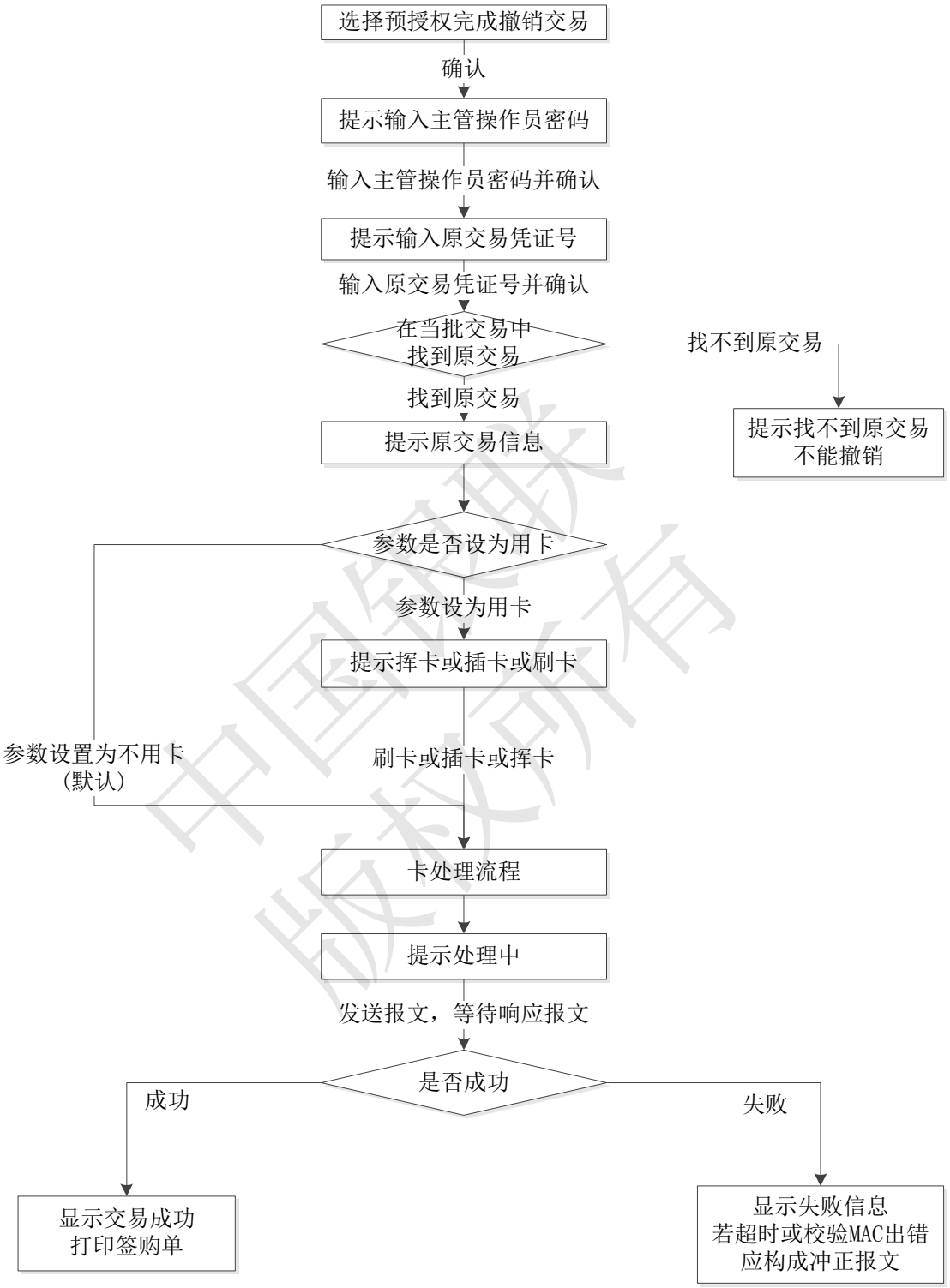


图18　银行卡预授权完成（请求）撤销交易处理流程

附录 C
（资料性附录）
个人标识码（PIN）的加密和解密方法

C.1 用于PIN加、解密的主账号PAN取法

C.1.1 手输卡号

如为手输卡号，从所输卡号（2域）右边数第二位开始，向左取12位，作为参与PIN加、解密的PAN。

C.1.2 刷卡方式

如为刷卡方式，从磁道2（35域）分隔符‘＝’左边第二位开始，向左取12个字符，作为参与PIN加密的PAN；如只有磁道3（36域），则从磁道3分隔符‘＝’左边第二位开始，向左取12个字符，作为参与PIN加、解密的PAN。

C.2 PIN的长度

PIN的长度为4-12位数字。

C.3 PIN的字符集

PIN用数字字符表示，下表给出了它的二进制对照表：

表 C.1 PIN 字符二进制表示

PIN 字符	二进制表示
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

C.4 PIN格式

PIN的格式应符合ANSI X9.8 Format（带主账号信息）
PIN BLOCK格式等于PIN按位异或主账号(PAN)

C.4.1 3DES算法的PINBLOCK示例

PIN格式：

表 C.2 PIN 格式

位置	长度	说明
1	1 BYTE	PIN 长度

2	7 BYTE	4-12 位 PIN(每个字符占 4 个 BIT，不足右补 F)

PAN格式：

表 C.3 PAN 格式

位置	长度	说明
1	2 BYTE	%H0000
3	6 BYTE	取主账号的右 12 位（参见 C.1）

示例 1

例如：明文PIN为： 123456，

假设： 磁卡上的PAN：1234 5678 9012 3456 78

截取下的PAN：6789 0123 4567

则用于PIN加密的PAN为：0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

PIN BLOCK为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

异或：0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

结果为：0x06 0x12 0x53 0xDF 0xFE 0xDC 0xBA 0x98

示例 2

假设： 磁卡上PAN：1234 5678 9012 3456

截取下的PAN：4567 8901 2345

则用于PIN加密的主账号为：0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

PIN BLOCK为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

异或：0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

结果为：0x06 0x12 0x71 0x31 0x76 0xFE 0xDC 0xBA

C.4.2 SM4算法的PINBLOCK示例

PIN BLOCK为PIN按位异或主账号（PAN）。

其中，PIN格式如下表所示：

表1 PIN格式

位置	长度	说明
1	1 BYTE	PIN 长度
2	15 BYTE	4-12 位数字的 PIN（每个字符占 4 个 BIT），不足部分右补 F）

PAN格式如下表所示：

表2 PAN格式

位置	长度	说明
1	2 BYTE	%H0000
3	14BYTE	取主账号的右 12 位（不包括最右边的校验位），主账号不足 12 位左补 0

示例

示例（一）示例 1

示例PIN 明文：123456

示例磁卡上的 PAN：1234 5678 9012 3456 78

示例截取下的 PAN：6789 0123 4567

示例则用于 PIN 加密的 PAN 为：0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

示例则 PIN BLOCK 为： 0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF

示例异或：0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

示例结果为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x98 0x76 0xFE 0xDC 0xBA 0x98

示例（二）示例 2

示例PIN 明文：123456

示例磁卡上 PAN：1234 5678 9012 3456

示例截取下的 PAN：4567 8901 2345

示例则用于 PIN 加密的主账号为：0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

示例则 PIN BLOCK 为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF

示例异或：0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

示例结果为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0xBA 0x98 0x76 0xFE 0xDC 0xBA

示例

示例 PIN 的类型（类型 2）、算法格式（3DES 或 SM4）必须在消息报文的域 53（SECURITY -RELATED－CONTROL－INFORMATION）中标明。

附录 D
（资料性附录）
POS 终端 MAC 的算法

D.1 概述

POS终端采用ECB的加密方式。

D.2 基于 3DES的MAC算法

POS终端采用ECB的加密方式，简述如下：

a) 将欲发送给POS中心的消息中，从消息类型（MTI）到63域之间的部分构成MAC ELEMEMENT BLOCK （MAB）。

b) 对MAB，按每8个字节做异或（不管信息中的字符格式），如果最后不满8个字节，则添加“0X00”。

示例：

MAB = M1 M2 M3 M4

其中：

M1 = MS11 MS12 MS13 MS14 MS15 MS16 MS17 MS18

M2 = MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28

M3 = MS31 MS32 MS33 MS34 MS35 MS36 MS37 MS38

M4 = MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48

按如下规则进行异或运算：

MS11 MS12 MS13 MS14 MS15 MS16 MS17 MS18
XOR） MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28

TEMP BLOCK1 =TM11 TM12 TM13 TM14 TM15 TM16 TM17 TM18

然后，进行下一步的运算：

TM11 TM12 TM13 TM14 TM15 TM16 TM17 TM18
XOR） MS31 MS32 MS33 MS34 MS35 MS36 MS37 MS38

TEMP BLOCK2 =TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28

再进行下一步的运算：

TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28
XOR） MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48

RESULT BLOCK = TM31 TM32 TM33 TM34 TM35 TM36 TM37 TM38

c) 将异或运算后的最后8个字节（RESULT BLOCK）转换成16 个HEXDECIMAL：

RESULT BLOCK = TM31 TM32 TM33 TM34 TM35 TM36 TM37 TM38
= TM311 TM312 TM321 TM322 TM331 TM332 TM341 TM342 ||
TM351 TM352 TM361 TM362 TM371 TM372 TM381 TM382

d) 取前8 个字节用MAK加密：

ENC BLOCK1 = eMAK（TM311 TM312 TM321 TM322 TM331 TM332 TM341 TM342）

= EN11 EN12 EN13 EN14 EN15 EN16 EN17 EN18

e) 将加密后的结果与后8 个字节异或：

EN11 EN12 EN13 EN14 EN15 EN16 EN17 EN18

XOR） TM351 TM352 TM361 TM362 TM371 TM372 TM381 TM382

TEMP BLOCK=TE11 TE12 TE13 TE14 TE15 TE16 TE17 TE18

f) 用异或的结果TEMP BLOCK 再进行一次单倍长密钥算法运算。

ENC BLOCK2 = eMAK（TE11 TE12 TE13 TE14 TE15 TE16 TE17 TE18）

= EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28

g) 将运算后的结果（ENC BLOCK2）转换成16 个HEXDECIMAL：

ENC BLOCK2 = EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28

= EM211 EM212 EM221 EM222 EM231 EM232 EM241 EM242 ||

EM251 EM252 EM261 EM262 EM271 EM272 EM281 EM282

示例：

ENC RESULT= %H84, %H56, %HB1, %HCD, %H5A, %H3F, %H84, %H84

转换成16 个HEXDECIMAL:

“8456B1CD5A3F8484”

h) 取前8个字节作为MAC值。

取”8456B1CD”为MAC值。

D.3 基于SM4 的MAC算法

a) 将欲发送给POS中心的消息中，从消息类型（MTI）到63域之间的部分构成MAC ELEMEMENT BLOCK （MAB）。

b) SM4算法的MAB，按每16个字节做异或（不管信息中的字符格式），如果最后不满16个字节，则添加“0X00”。

示例：

MAB = M1 M2 M3M4

其中：

M1 = MS01 MS02 MS03 MS04 MS05 MS06 MS07 MS08 MS09 MS10 MS11 MS12 MS13 MS14 MS15 MS16

M2 = MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28 MS29 MS30 MS31 MS32 MS33 MS34 MS35 MS36

M3= MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48 MS49 MS50 MS51 MS52 MS53 MS54 MS55 MS56

M4= MS61 MS62 MS63 MS64 MS65 MS66 MS67 MS68 MS69 MS70 MS71 MS72 MS73 MS74 MS75 MS76

按如下规则进行异或运算：

MS01 MS02 MS03 MS04 MS05 MS06 MS07 MS08 MS09 MS10 MS11 MS12 MS13 MS14 MS15 MS16

XOR）

MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28 MS29 MS30 MS30 MS32 MS33 MS34 MS35 MS36

RESULT BLOCK1 = TM01 TM02 TM03 TM04 TM05 TM06 TM07 TM08 TM09 TM10 TM11 TM12 TM13 TM14 TM15 TM16

进行下一次异或

TM01 TM02 TM03 TM04 TM05 TM06 TM07 TM08 TM09 TM10 TM11 TM12 TM13 TM14 TM15 TM16

XOR）

MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48 MS49 MS50 MS51 MS52 MS53 MS54 MS55 MS56

RESULT BLOCK2 = TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28 TM29 TM30 TM31 TM32 TM33 TM34 TM35 TM36

再进行一次异或运算

TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28 TM29 TM30 TM31 TM32 TM33 TM34 TM35 TM36

XOR）

MS61 MS62 MS63 MS64 MS65 MS66 MS67 MS68 MS69 MS70 MS71 MS72 MS73 MS74 MS75 MS76

RESULT BLOCK = TM41 TM42 TM43 TM44 TM45 TM46 TM47 TM48 TM49 TM50 TM51 TM52 TM53 TM54 TM55 TM56

c) 将异或运算后的最后16个字节（RESULT BLOCK）转换成32 个HEXDECIMAL：

RESULT BLOCK = TM41 TM42 TM43 TM44 TM45 TM46 TM47 TM48 TM49 TM50 TM51 TM52 TM53 TM54 TM55 TM56

= TM011 TM012 TM021 TM022 TM031 TM032 TM041 TM041 TM051 TM052 TM061 TM062 TM071 TM072 TM081 TM082 || TM091 TM092 TM101 TM102 TM111 TM112 TM121 TM122 TM131 TM132 TM141 TM142 TM151 TM152 TM161 TM162

d) 取前16 个字节用SM4加密：

ENC BLOCK1 = SM4K（TM011 TM012 TM021 TM022 TM031 TM032 TM041 TM041 TM051 TM052 TM061 TM062 TM071 TM072 TM081 TM082）

= EN 011 EN 012 EN 021 EN 022 EN 031 EN 032 EN 041 EN 041 EN 051 EN 052 EN 061 EN 062 EN 071 EN 072 EN 081 EN 082

e) 将加密后的结果与后16 个字节异或：

EN 011 EN 012 EN 021 EN 022 EN 031 EN 032 EN 041 EN 041 EN 051 EN 052 EN 061 EN 062 EN 071 EN 072 EN 081 EN 082

XOR）TM091 TM092 TM101 TM102 TM111 TM112 TM121 TM122 TM131 TM132 TM141 TM142 TM151 TM152 TM161 TM162

TEMP BLOCK=TE01 TE02 TE03 TE04 TE05 TE06 TE07 TE08 TE09 TE10 TE11 TE12 TE13 TE14 TE15 TE16

f) 用异或的结果TEMP BLOCK 再进行一次SM4密钥算法运算。

ENC BLOCK2 = SM4K（TE01 TE02 TE03 TE04 TE05 TE06 TE07 TE08 TE09 TE10 TE11 TE12 TE13 TE14 TE15 TE16）

= EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28 EN29 EN30 EN31 EN32 EN33 EN34 EN35 EN36

g) 将运算后的结果（ENC BLOCK2）转换成32 个HEXDECIMAL：

ENC BLOCK2 = EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28 EN29 EN30 EN31 EN32 EN33 EN34 EN35 EN36

= EN211 EN212 EN221 EN222 EN231 EN232 EN241 EN242 EN251 EN252 EN261 EN262 EN271 EN272 EN281 EN282||

EN291 EN292 EN301 EN302 EN311 EN312 EN321 EN322 EN331 EN332 EN341 EN342 EN351 EN352 EN361EN362

ENC RESULT

= %H84, %H56, %HB1, %HCD, %H5A, %H3F, %H84, %H84%H84, %H56, %HB1, %HCD, %H5A, %H3F, %H84, %H84

转换成32 个HEXDECIMAL：

“8456B1CD5A3F84848456B1CD5A3F8484”

h) 取前8个字节作为MAC值。

取“8456B1CD”为MAC值。

附录 E
（资料性附录）
磁道信息加密算法

E.1 基本要求

PIN输入设备需对下列磁道信息中敏感信息进行加密：

发卡方信息（包括卡片验证码CVN等信息）。

加密采用双倍长密钥算法，磁道信息加密密钥TDK通过POS签到交易获得，存储在PIN输入设备中。

E.2 数据源构成

E.2.1 二磁道数据源

E.2.1.1 基于3DES密钥加密方式

二磁道数据（35域）从结束标志“？”向左第2个字节开始，再向左取8个字节作为参与加密的二磁道中发卡方信息，记为TDB2。

E.2.1.2 基于SM4密钥加密方式

二磁道数据（35域）从结束标志“？”向左第2个字节开始，再向左取16个字节作为参与加密的二磁道中发卡方信息，记为TDB2。

E.2.2 三磁道数据源

E.2.2.1 基于3DES密钥加密方式

类似二磁道数据源构造方法，三磁道数据（36域，如果存在）磁道信息块构造方法如下：

三磁道数据（36域）从结束标志“？”向左第2个字节开始，再向左取8个字节作为参与加密的三磁道中发卡方信息（若不足右补足F），记为TDB3。

E.2.2.2 基于SM4密钥加密方式

类似二磁道数据源构造方法，三磁道数据（36域，如果存在）磁道信息块构造方法如下：

三磁道数据（36域）从结束标志“？”向左第2个字节开始，再向左取16个字节作为参与加密的三磁道中发卡方信息（若不足右补足F），记为TDB3。

E.2.3 异常处理

对于二磁道或三磁道缺失的情况，终端应上送8字节全F。

E.3 加密方式

E.3.1 3DES加密方式

采用双倍长密钥TDK分别对TDB2，TDB3进行加密，将密文输出后按照对应位置替换原先的明文数据。

E.3.2 SM4加密方式

采用SM4密钥TDK分别对TDB2，TDB3进行加密，将密文输出后按照对应位置替换原先的明文数据。

E.4 举例

二磁道数据（37）：

12345678901234567 89＝0508201781999168302

表示为:

0x12 0x34 0x56 0x78 0x90 0x12 0x34 0x56 0x78 0x9D 0x05 0x08 0x20 0x17 0x81 0x99 0x91 0x68 0x30 0x20

三磁道数据（104）：

9912345678901234567 89=156000000000000000000037819992160000050800000000000000000000000=0000000000003=0000000000

表示为:

0x99 0x12 0x34 0x56 0x78 0x90 0x12 0x34 0x56 0x78 0x9D 0x15 0x60 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x03 0x78 0x19 0x99 0x21 0x60 0x00 0x00 0x50 0x80 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0xD0 0x00 0x00 0x00 0x00 0x00 0x3D 0x00 0x00 0x00 0x00 0x00

E.4.1 3DES算法加密方式

则TDB2表示为：0x08 0x20 0x17 0x81 0x99 0x91 0x68 0x30

则TDB3表示为：0x00 0x00 0x00 0x3D 0x00 0x00 0x00 0x00

采用TDK对TDB2、TDB3分别进行TDES加密，加密后的磁道信息为：

ENC BLOCK1 = eTDK(0x08 0x20 0x17 0x81 0x99 0x91 0x68 0x30)

ENC BLOCK2 = eTDK(0x00 0x00 0x00 0x3D 0x00 0x00 0x00 0x00)

E.4.2 SM4算法加密方式

则TDB2表示为：0x78 0x90 0x12 0x34 0x56 0x78 0x9D 0x05 0x08 0x20 0x17 0x81 0x99 0x91 0x68 0x30

则TDB3表示为：0x00 0x00 0x00 0x00 0x00 0xD0 0x00 0x00 0x00 0x00 0x00 0x3D 0x00 0x00 0x00 0x00

采用TDK对TDB2、TDB3分别进行SM4加密，加密后的磁道信息为：

ENC BLOCK1 = SM4(0x78 0x90 0x12 0x34 0x56 0x78 0x9D 0x05 0x08 0x20 0x17 0x81 0x99 0x91 0x68 0x30)

ENC BLOCK2 = SM4(0x00 0x00 0x00 0x00 0x00 0xD0 0x00 0x00 0x00 0x00 0x00 0x3D 0x00 0x00 0x00 0x00)

附录 F
（资料性附录）
终端 POS 参数

F.1 概述

根据初始和变更的方式，POS终端参数可分为出厂参数、下发参数、可设定参数和联机可更改参数四类。如果某参数既出现在可设定参数，又出现在联机可更改参数，表明该参数两者均使用。

F.2 出厂参数

出厂参数主要是与硬件相关的、影响硬件设备使用和运作的基本参数。出厂的参数应当在设备出厂时全部写入，不允许更改。

表1 出厂参数表

参数名称	用途	设置时间	关联内容
硬件版本号	标识当前设备硬件版本	出厂	与硬件设备相关的其他参数
设备序列号	当前设备唯一标识	出厂	设备管理数据库，需要遵循银联的规范
操作系统版本号	标识当前设备操作系统	出厂或升级时	硬件版本、应用软件版本
内存状态	标识内存使用状况	程序下装后	应用软件使用
通讯端口类型	识别可用的通讯端口种类	出厂	操作系统、应用软件使用
通讯端口参数	根据具体应用更改设置	出厂或应用时	操作系统、应用软件使用
MODEM 类型	识别可用的 MODEM 种类	出厂	操作系统、应用软件使用
MODEM 参数	根据具体应用更改设置	出厂或应用时	操作系统、应用软件使用
打印机类型	识别可用的打印机种类	出厂	操作系统、应用软件使用
打印机参数	根据具体应用更改设置	出厂或应用时	操作系统、应用软件使用
密码键盘类型	识别可用的密码键盘种类	出厂	操作系统、应用软件使用
密码键盘参数	根据具体应用更改设置	出厂或应用时	操作系统、应用软件使用
磁卡阅读器参数	根据具体设备、应用更改	出厂或升级时	操作系统、应用软件版本
IC 卡阅读器（包括非接卡读写模块）参数	根据具体设备、应用更改	出厂或升级时	操作系统、应用软件版本
根据具体设备的差异，通讯端口参数、MODEM 参数、打印机参数、密码键盘参数和 IC 卡阅读器参数等项目可以包括多个子项目。			

F.3 下发参数

下发参数主要是用于设备自身管理和配置的参数。该部分参数可以通过PC工具或POS界面进行设定，可能随着程序版本的更换而发生变化。

表2 下发参数表

参数名称	用途	设置时间	关联内容
电话号码	用于设备管理及正常交易	安装或调整时	交易号码、管理号码、拨号参数
拨号参数	设置电话拨号参数	安装或调整时	拨号方式、交换机前缀、电话号码
终端编号	标识当前设备逻辑编号	安装或调整时	设备管理数据库、交易应用
商户编号	标识使用设备的商户编号	安装或调整时	设备管理数据库、交易应用

参数名称	用途	设置时间	关联内容
商户名称	标识商户的中文或英文名	安装或调整时	设备管理数据库、交易应用
超时时间	通讯响应超时时间	安装或调整时	交易应用
重试次数	通讯失败重试次数	安装或调整时	交易应用
TPDU	交易报文的目的地址	安装或调整时	交易应用
AID 列表	终端支持的借/贷记应用列表，如 ISO/IEC 7816-5 所述，指明应用	安装或调整时	交易应用
应用选择指示符	指示应用选择时终端上的 AID 与卡片中的 AID 是完全匹配还是部分匹配	安装或调整时	交易应用
认证中心公钥 RID	与公钥索引一起标识认证中心的公钥	安装或调整时	交易应用
认证中心公钥索引	与 RID 一起标识认证中心的公钥	安装或调整时	交易应用
认证中心公钥模	公钥模值	安装或调整时	交易应用
认证中心公钥指数	公钥指数	安装或调整时	交易应用
认证中心公钥校验值	验证认证中心公钥用	安装或调整时	交易应用
认证中心公钥有效期	认证中心规定的有效期限	安装或调整时	交易应用
认证中心公钥哈什算法标识	标识用于在数字签名方案中产生哈什结果的哈什算法	安装或调整时	交易应用
认证中心公钥算法标识	标识使用在认证中心公钥上的数字签名算法	安装或调整时	交易应用
TAC－缺省	标识如果交易可以联机完成但终端没有联机交易能力时，拒绝交易的收单行条件	安装或调整时	交易应用
TAC－联机	标识联机交易的收单行条件	安装或调整时	交易应用
TAC－拒绝	标识不作联机尝试即拒绝交易的收单行条件	安装或调整时	交易应用
应用版本号	应用当前的版本号	安装或调整时	交易应用
终端联机 PIN 支持能力	指示终端在每个 AID 的要求下是否支持联机 PIN 的输入。	安装或调整时	交易应用
缺省 DDOL	卡片中无 DDOL 时用于构造内部认证命令的 DDOL	安装或调整时	交易应用
终端最低限额	IC 卡消费时终端允许的最低脱机限额	安装或调整时	交易应用
偏置随机选择的阈值	在终端风险管理中用于随机交易选择的值	安装或调整时	交易应用
偏置随机选择的最大目标百分数	用于偏置随机选择的最大目标百分数	安装或调整时	交易应用
随机选择的目标百分数	用于随机选择的目标百分数	安装或调整时	交易应用
终端电子现金交易限额	终端使用此数据元（如果存在的话）判断一个交易的处理方式，当授权金额小于该限额时允许电子	安装或调整时	交易应用

参数名称	用途	设置时间	关联内容
	现金交易，否则设置终端行为代码并据此确认交易方式（小额支付参数）		
非接触读写器脱机最低限额	在 AID 联合中，用来指示读写器中非接触脱机交易的最低限额	安装或调整时	交易应用
非接触读写器交易限额	如果非接触交易的金额大于或等于此数值，则交易终止。允许在其他界面尝试此交易	安装或调整时	交易应用
读写器持卡人验证方法（CVM）所需限制	如果非接触交易超过此值，读写器要求一个持卡人验证方法（CVM）	安装或调整时	交易应用
终端国家代码	标识根据 ISO3166 表示的终端国家代码	安装时	交易应用
收单行标识	标识收单行	安装时	交易应用
商户分类码	商户分类码值	安装时	交易应用
交易货币代码	表示根据 ISO 4217 规定的交易货币代码	安装时	交易应用
交易货币指数	表示根据 ISO 4217 规定的从交易金额右起的隐含小数点位置	安装时	交易应用
终端性能	表示终端的卡片数据输入，CVM 和安全能力	安装时	交易应用
附加终端性能	表明终端的数据输入输出能力	安装时	交易应用
商户标识	和收单行标识一起唯一地标识一个特定地商户	安装时	交易应用
终端类型	表明终端环境、通讯能力和操作控制	安装时	交易应用

F.4 可设定参数

可设定参数主要是与交易内容直接相关并需要长期存放在POS终端中使用的应用参数，这些参数在收单机构的控制下可以进行配置，不允许商户私自修改已经配置好的参数，包括以下几类：

—— 基本参数类：

- 交易应用密钥：根据业务需求所要使用的所有密钥。
- 当前重要编号：当前流水号、当前批次号、当前操作员号。
- 最大日志笔数：允许当批交易保存的最大交易笔数。
- 操作员管理表：操作员号、操作员密码、操作员属性。
- 日期与时间表：实时时钟的日期和时间，在每次签到交易成功后调整。

—— 交易/状态控制类：

- 终端支持的交易类型：终端支持哪些交易，不支持的交易不出现在界面中，该部分参数可以通过参数文件导入等方式进行配置。
- 消费撤销交易是否出现卡：根据该参数的值确定消费撤销交易是否需要进行刷卡或插卡或挥卡。1：用卡；0：不用卡。默认值为 0。
- 预授权完成撤销交易是否出现卡：根据该参数的值确定预授权完成撤销交易是否需要进行刷卡或插卡或挥卡。1：用卡；0：不用卡。默认值为 0。

- 撤销类交易是否允许持卡人输入密码[1]：根据该参数的值确定撤销类交易是否需要输入密码。1：输入；0：不输入。默认值为 0。
- 预授权完成（请求）交易是否允许持卡人输入密码：根据该参数的值确定预授权完成（请求）交易是否需要输入密码。1：输入；0：不输入。默认值为 0。
- 退货交易最大金额：根据该参数的值判断退货交易的最大允许金额，默认为 1000.00 元。
- 预授权完成方式参数：根据该参数的值确定预授权完成的方式，并且显示相应的界面提示。参数为 0 时，终端同时支持预授权完成（请求）和预授权完成（通知）；参数为 1 时，终端只支持预授权完成（请求）；参数为 2 时，终端只支持预授权完成（通知）。默认值为 0。
- 终端默认交易参数：根据该参数的值确定在终端显示待机界面时刷卡、插卡或挥卡可直接进入的默认交易。1：消费；0：预授权。默认值为 1。

F.5 联机可更改参数

联机可更改参数可以通过POS参数传递获得。

包括超时时间（默认60秒）、重试次数（默认3次）、三个交易电话号码、一个管理号码、是否支持小费（默认为否）、小费百分比（默认为0）、是否支持手工输入卡号[2]、POS终端应用类型（默认为60）、商户名称（中文简称）、交易重发次数（默认为3次）、主密钥INDEX（一机一密为空）、交易类型位图。

[1] 该参数应针对消费撤销、预授权撤销、预授权完成撤销交易分别设置。

[2] 如需在 POS 终端中设置该参数，应按照《业务规则》要求，只能对可以手输卡号进行的交易设置该参数。对必须刷卡进行的交易（目前有余额查询、消费、退货、预授权（境内卡）），不可设置该参数，若该商户为外卡商户，允许设置预授权交易进行手输卡号。

附录 G
（资料性附录）
非接电子现金“闪卡”处理解决方案

G.1 电子现金“闪卡”处理

G.1.1 终端要求

G.1.1.1 终端提示要求

在交易过程中，终端应通过语音（默认为中文普通话）或蜂鸣提示和屏幕显示（默认为汉字）等方式，明确告知持卡人“请重刷”。

1、语音或蜂鸣提示

终端应在发生“闪卡”时以语音或蜂鸣方式提示重刷。界面和指示灯配合提示。其中在无人值守终端推荐优先采用语音提示。

如采用语音提示，应提示“请重新挥卡”。

如采用蜂鸣提示，采用如下方式：

状态	含义	指示灯状态	界面提示信息	蜂鸣
交易失败	交易过程发生错误（疑似闪卡）	红灯常亮	见下节“屏幕提示”	长蜂鸣音。

“闪卡”发生后，在当笔闪卡重刷处理流程中，如未发生超时或未按“取消”键，在等待卡片重刷过程中，建议持续蜂鸣状态。

2、屏幕显示

（1）“请重新挥卡”提示

“闪卡”处理流程中提示持卡人重新将卡片放置感应区时，终端应包括如下屏幕显示提示：

扣款失败，再次放卡

图19 “请重新挥卡”提示

终端应在界面超时时间（建议10秒）内保持显示状态，直至卡片放回或显示超时或按“退出”键。卡号显示应遵循屏蔽规则。

（2）“读卡失败”提示（仅用于“全部闪卡待处理流程”）

“闪卡”处理过程中，终端读取数据（包括卡号、ATC、货币代码、余额、最后一条记录等）失败时显示提示：

读卡失败

图20 “读卡失败”提示

仅在该界面超时时间内（建议2秒）保持显示。仅在“全部闪卡待处理流程”中使用，具体使用见处理流程要求。

（3）“卡号不一致”提示（仅用于“当笔闪卡重刷处理流程”）

“当笔闪卡重刷处理流程”中，当再次挥卡，终端比对卡号不一致时，提示换用原卡。

卡号不一致 请使用原卡片

图21 “卡号不一致”提示

仅在该界面超时时间内（建议2秒）保持显示，随后转入“请重新挥卡”提示界面。仅在“当笔闪卡重刷处理流程”中使用，具体使用见处理流程要求。

G.1.1.2 终端闪卡要求

终端应满足如下闪卡要求：

——终端应支持参数设置可保存的闪卡记录条数，最少1条，最多3条（默认值）。

——终端应支持对闪卡记录的断电保护。

——终端应确保所存储交易信息安全性，应对敏感数据进行加密存储。

——终端应按要求以文字和语音（或蜂鸣）方式提示交易状态和操作要求，按处理流程进行相应处理。

——发生闪卡后，终端进入“当笔闪卡重刷处理流程”，即通过要求持卡人重新挥卡，针对性地处理当前刚发生的这一笔闪卡交易，在超过“当笔重刷处理时间”T1或按“取消”键时，回到初始界面，进入“全部闪卡待处理流程”，对所有闪卡记录进行匹配和处理。

——终端应支持“当笔重刷处理时间”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），建议减小T1取值。

——终端应支持“闪卡记录可处理时间”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（如自动售货机），参考取值为10秒。收单机构视实际应用场景进行调整。终端应删除超过闪卡可处理时间的闪卡记录。

——对于已成功恢复的交易，终端删除失败交易记录，上送成功交易记录；闪卡未恢复、且已超过闪卡记录可处理时间的，终端以失败交易上送（复用IC卡失败交易的上送报文）。

——交易金额与闪卡记录金额不匹配的，均视当前交易为新发起交易，进入正常交易处理流程应用初始化阶段。

G.2 处理流程

G.2.1 电子现金交易正常处理流程

处理流程如下图所示。

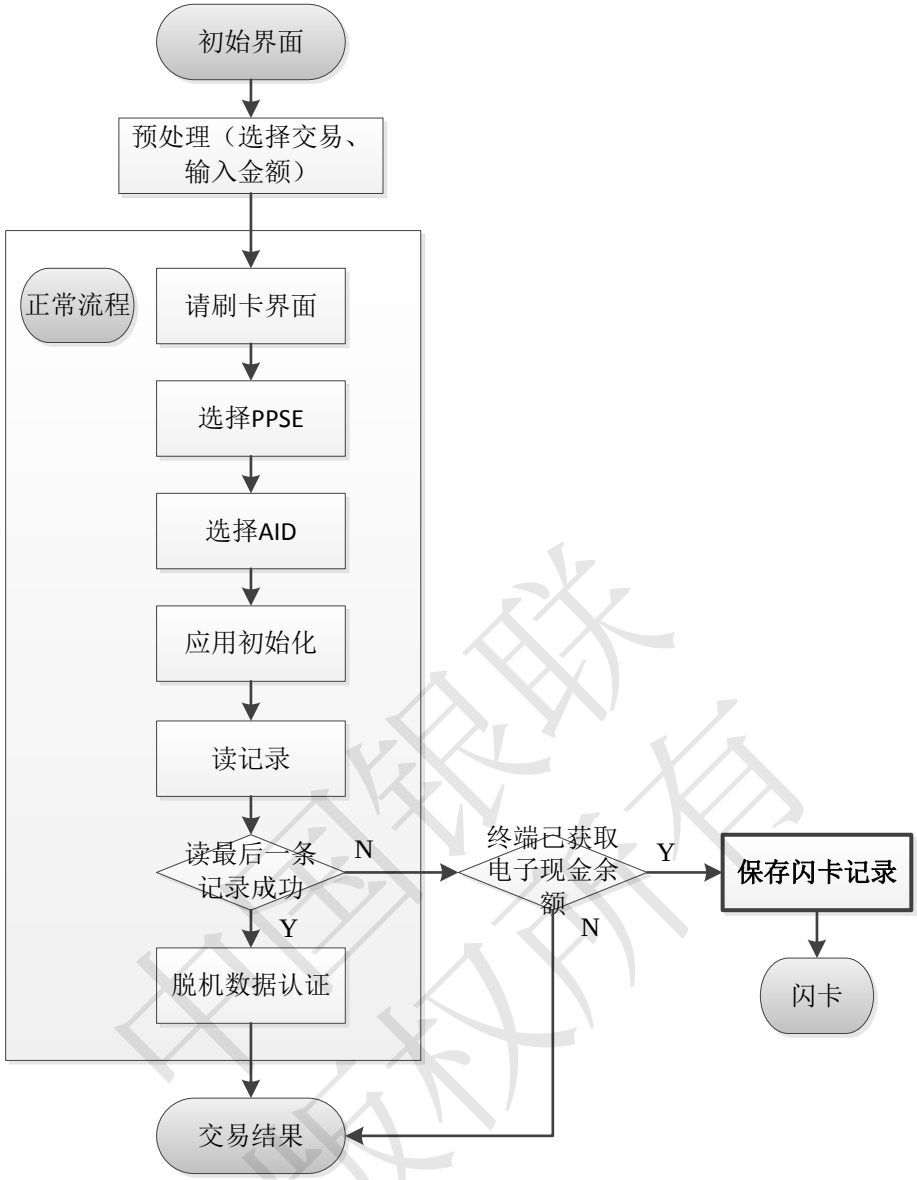


图22　电子现金脱机交易正常处理流程

电子现金脱机交易基本流程采用qPBOC流程。为支持“闪卡”处理，终端在原有基本流程的基础上还应满足如下要求：

——如读取卡片最后一条记录失败（即发生“闪卡”），如终端已获取卡片电子现金可用余额，则终端应立即保存闪卡记录（记录闪卡发生时间用于超时判断），并保存失败交易记录，并进入“当笔闪卡重刷处理流程”；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。终端是否获取卡片电子现金的判断见下一项要求。

——“闪卡”记录应具有当次交易所有信息，包括AFL、AIP、ATC、IAD、磁道二信息、主账号（tag5A或tag57）、动态签名数据、交易金额、可用余额、卡片交易属性、随机数、及其他交易数据，以上数据加上最后一条记录应为完整脱机交易数据。同时终端保存获取二磁道等效信息和主账号的文件名和记录号，以避免闪卡处理中终端遍历全部卡片记录。其中，“可用余额”是完成扣款之后的金额，选择卡片返回的tag9F5D或tag9F10中包含的电子现金余额（对仅小额检查的卡片中tag9F5D等于tag9F79，基本覆盖目前发行的非接IC卡）。若卡片未返回tag9F5D，并且在返回的tag9F10中未包含电子现金余额数据（tag9F79的值或tag9F5D的值），则认为终端未获取卡片电子现金可用余额，后续不进行闪卡处理，仅保存失败交易记录，不保存闪卡记录，提示交易失败。。注意，tag9F79是GPO中已完成授权金额扣减的

新的电子现金余额值（GPO小额检查操作中，新的tag9F79，第一币种等于GPO完成前原tag9F79减授权金额，第二币种等于GPO完成前原tagDF79减授权金额）。

G.2.2 当笔“闪卡”重刷处理流程

处理流程如图5所示。

1-界面和语音（或蜂鸣）提示重新挥卡（图1），记录重刷处理开始时间用于超时判断。

2-如超过“当笔重刷处理时间”T1或按“取消”键，终端回到初始界面，进入“全部闪卡待处理流程”；如未超时、未按“取消”键，进入步骤3。

3-对卡片上电，选择PPSE，选择AID，如成功，进入步骤4；如任意操作失败，回到步骤1，但重刷处理时间在后续整个过程中不再重置。

4-终端读取当前卡片卡号，判断是否与当前“闪卡”记录卡号一致，如一致，则终端读取卡片应用交易计数器（ATC，tag9F36）、应用货币代码（tag9F51）、电子现金余额（第一币种为tag9F79）；如不一致，提示卡号不一致，并回到步骤1。因卡片离开感应区等原因导致读取数据（卡号、ATC、货币代码、余额等）失败时，如未超过T1，退回步骤1；如T1超时，则保留闪卡记录和失败交易记录，回到终端初始界面，进入“全部闪卡待处理流程”。

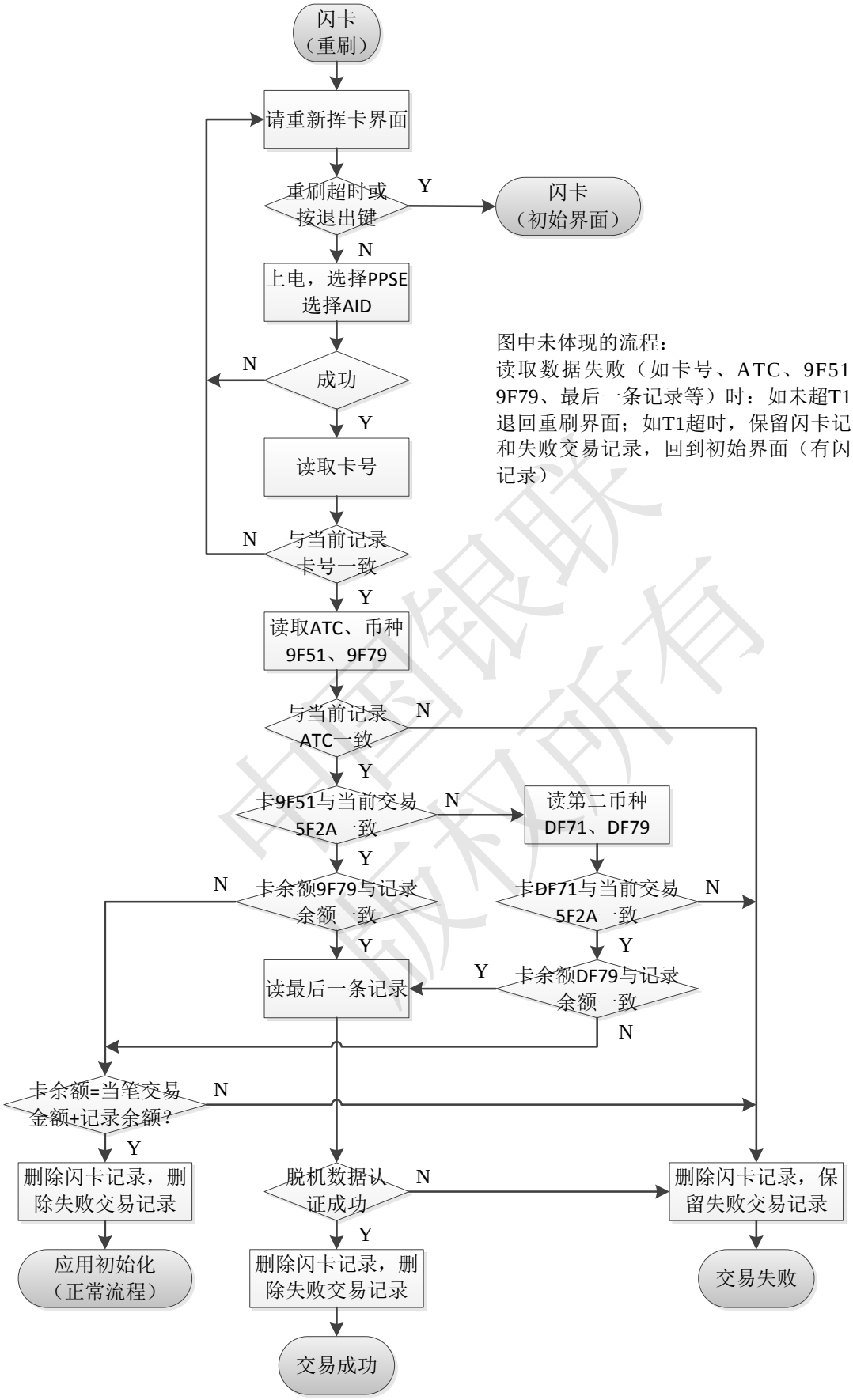
5-判断当前卡片ATC是否与当前“闪卡”记录ATC一致，如一致，进入步骤6；如不一致，则终端删除闪卡记录，保留失败交易记录（后续上送），提示交易失败。

6-判断卡片tag9F51是否与当前闪卡记录tag5F2A一致，如币种不一致，则进入步骤7；如币种一致，则继续判断卡片余额是否与记录中余额一致，如余额也一致，则终端读取卡片最后一条记录，进入步骤9；如余额不一致，则进入步骤8。因卡片离开感应区等原因导致读取最后一条记录失败时，如未超过T1，退回步骤1；如T1超时，则保留闪卡记录和失败交易记录，回到终端初始界面，进入“全部闪卡待处理流程”。

7-终端读取第二币种应用货币代码（tagDF71）和第二币种电子现金余额（tagDF79），判断卡片tagDF71是否与当前闪卡记录tag5F2A一致，如币种不一致（未获取等同于不一致），则终端删除闪卡记录，保留失败交易记录（后续上送），提示交易失败；如币种一致，则继续判断卡片第二币种余额是否与记录中余额一致，如余额也一致，则终端读取卡片最后一条记录，进入步骤9；如余额不一致（未获取等同于不一致），则进入步骤8。因卡片离开感应区等原因导致读取最后一条记录失败时，如未超过T1，退回步骤1；如T1超时，则保留闪卡记录和失败交易记录，回到终端初始界面，进入“全部闪卡待处理流程”。

8-判断卡片余额是否等于记录中余额加上当笔交易金额，如一致，则终端删除闪卡记录，删除失败交易记录，进入正常处理流程的应用初始化步骤；如不一致，则终端删除闪卡记录，保留失败交易记录（后续上送），提示交易失败。

9-终端进行脱机数据认证，如成功，则删除当前闪卡记录，删除对应失败交易记录，提示交易成功；如不成功，删除当前闪卡记录，保留对应失败交易记录（后续上送），提示交易失败。



图中未体现的流程：
读取数据失败（如卡号、ATC、9F51、9F79、最后一条记录等）时：如未超T1，退回重刷界面；如T1超时，保留闪卡记录和失败交易记录，回到初始界面（有闪卡记录）

图23　闪卡单笔处理流程

G.2.3 全部“闪卡”待处理流程

处理流程如下图所示。

图中未体现的流程：
读取数据失败（如卡号、ATC、9F51、9F79、最后一条记录等）时，界面提示读卡失败，回到请刷卡界面，闪卡记录和失败交易记录均不产生变化

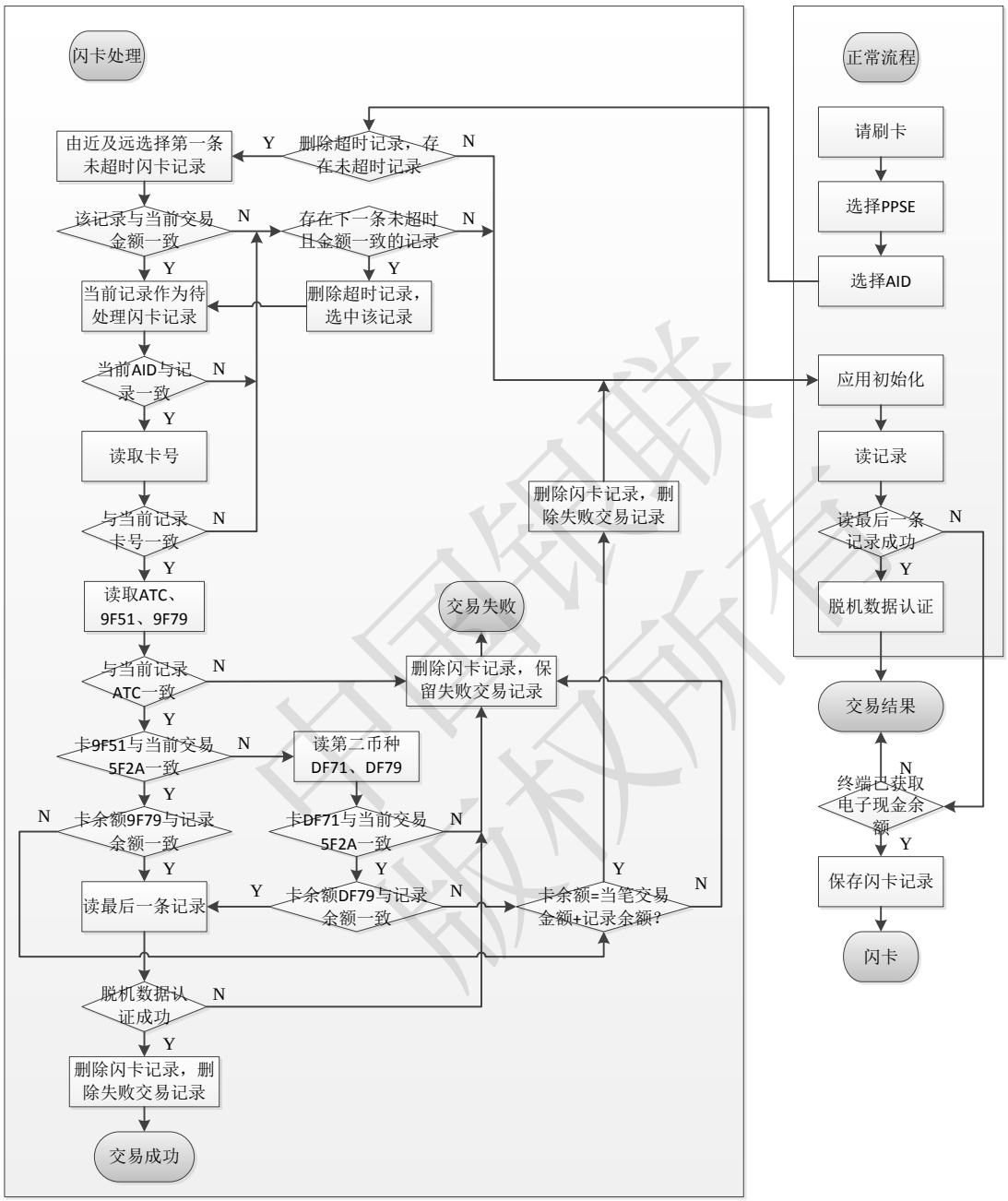


图24 全部“闪卡”待处理流程

1-终端处于初始界面，选择交易、输入交易金额，终端进行IC卡预处理，提示请刷卡（挥卡）。选择PPSE，选择AID，进入步骤2。

2-判断闪卡记录超时（“闪卡记录可处理时间”T2）情况，删除超时记录。如终端存在未超时闪卡记录，进入步骤3；如不存在，则进入应用初始化，进入正常交易流程。

3-在“闪卡”记录中以由近及远的方式选择第一条记录，判断该记录中的交易金额与当前交易的金额是否一致，如一致，将该记录作为“当前待处理（恢复）闪卡记录”，进入步骤5；如不一致，进入步骤4。

4-判断是否存在下一条未超时且金额一致的闪卡记录（依然按由近及远方式选择），如存在，将该记录作为“当前待处理闪卡记录”，并删除超时记录，进入步骤5；如不存在，则进入应用初始化，进入正常交易流程。

5-判断当前待处理闪卡记录的AID是否与当前交易选中的AID一致，如一致，进入步骤6；如不一致，进入步骤4。

6-读取卡号，判断是否与当前待处理闪卡记录中的卡号一致，如一致，则终端读取卡片应用交易计数器（ATC，tag9F36）、应用货币代码（tag9F51）、电子现金余额（tag9F79），进入步骤7；如不一致，进入步骤4。因卡片离开感应区等原因导致读取数据（卡号、ATC、货币代码、余额等）失败时，提示读卡失败（图2），保留闪卡记录和失败交易记录，回到终端初始界面，进入步骤1。

7-判断卡片ATC与当前待处理闪卡记录中的ATC是否一致，如一致，进入步骤8；如不一致，则终端删除闪卡记录，保留失败交易记录（后续上送），提示交易失败。

8-判断卡片tag9F51是否与当前闪卡记录tag5F2A一致，如币种不一致，则进入步骤9；如币种一致，则继续判断卡片余额是否与记录中余额一致，如余额也一致，则终端读取卡片最后一条记录，进入步骤11；如余额不一致，则进入步骤10。因卡片离开感应区等原因导致读取最后一条记录失败时，提示读卡失败（图2），保留闪卡记录和失败交易记录，回到终端初始界面，进入步骤1。

9-终端读取第二币种应用货币代码（tagDF71）和第二币种电子现金余额（tagDF79），判断卡片tagDF71是否与当前闪卡记录tag5F2A一致，如币种不一致（未获取等同于不一致），则终端删除闪卡记录，保留失败交易记录（后续上送），提示交易失败；如币种一致，则继续判断卡片第二币种余额是否与记录中余额一致，如余额也一致，则终端读取卡片最后一条记录，进入步骤11；如余额不一致（未获取等同于不一致），则进入步骤10。因卡片离开感应区等原因导致读取最后一条记录失败时，提示读卡失败（图2），保留闪卡记录和失败交易记录，回到终端初始界面，进入步骤1。

10-判断卡片余额是否等于记录中余额加上当笔交易金额，如一致，则终端删除闪卡记录，删除失败交易记录，进入正常处理流程的应用初始化步骤；如不一致，则终端删除闪卡记录，保留失败交易记录（后续上送），提示交易失败。

11-终端进行脱机数据认证，如成功，则删除当前闪卡记录，删除对应失败交易记录，提示交易成功；如不成功，删除当前闪卡记录，保留对应失败交易记录（后续上送），提示交易失败。

G.3 卡片注意事项

为有效实施“闪卡”处理方案、防止发生交易风险，IC卡应满足以下要求：

——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，终端可以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。

附录 H
（规范性附录）
小额非接免签免密收单技术方案

H.1 概述

通过终端和收单系统配套改造，使境内POS终端满足闪付联机小额免密产品的受理需求。同时实现以下目标：

——终端处理功能满足试点阶段一、试点阶段二和全面支持推广阶段的要求，兼容不同维度业务需求（境内/境外银联卡、借/贷记卡）。

——可通过远程更新实现不同阶段的终端处理逻辑切换，实现必要参数（如QPS限额等）的远程更新，存在变动可能性的功能点设置开关控制，避免终端反复改造。

——统筹考虑CDCVM（现阶段主要用于移动设备卡）在终端受理的应用。

试点阶段一在技术上指部分贷记卡和部分借记卡参与产品试点的阶段，试点阶段二在技术上指全部贷记卡和部分借记卡参与产品试点的阶段，全面支持推广阶段在技术上指全部卡片支持的阶段。以上阶段的划分和技术方案均针对境内发行银联卡，对境外发行银联卡各阶段处理逻辑保持一致。

H.2 功能需求

H.2.1 试点阶段一

1）受理境内发行银联卡,实现以下业务需求：

——QPS BIN表（BIN表A）范围以内，在QPS限额以下（含QPS限额，下同）：终端不提示输密（分体式终端在主机和密码键盘界面均不提示，下同）。

——免签限额以下，凭证“免签名”，免签凭证打印要求见4.5节；

——其他情况：终端提示“请输入密码”，支持PIN ByPass。

2）受理境外发行银联卡实现以下业务需求：

——终端输密提示：贷记卡在QPS限额以下，终端不提示输密；贷记卡在QPS限额以上，按《中国银联IC卡技术规范》（以下采用“qUICS规范”指代），由终端与卡片协商的CVM结果确定是否提示输密；终端支持PIN ByPass。借记卡按qUICS规范，由终端与卡片协商的CVM结果确定是否提示输密；终端支持PIN ByPass。

——凭证打印：在免签限额以下，凭证“免签名”，免签凭证打印要求见4.5节；在免签限额以上，凭证不采用免签名方案。

注意：终端与卡片协商的CVM方式包含PIN、CDCVM、签名，当卡片要求PIN且终端支持PIN时，终端提示输密；否则终端均不提示输密。

H.2.2 试点阶段二

1) 受理境内发行银联卡实现以下业务需求：

贷记卡：

——在QPS限额以下：终端不提示输密。

——其他：终端提示“请输入密码”，支持PIN ByPass，凭证不采用免签名方案。

借记卡：

——与试点阶段一一致（BIN表方式），但采用BIN表B判断。

——试点阶段二所采用的BIN表B中仅包含借记卡卡BIN，包含试点阶段一BIN表A中全部借记卡BIN号以及在试点阶段二投入试点的借记卡BIN号。

对于借贷记卡，免签限额以下，凭证“免签名”。

2）受理境外发行银联卡

与试点阶段一一致。

H.2.3 全面支持推广阶段

1) 受理境内发行银联卡

贷记卡：与试点阶段二一致。

借记卡：借记卡全部支持闪付联机小额免密后，与贷记卡处理一致。

2) 受理境外发行银联卡

与试点阶段一一致。

H.3 针对免密限额超限等交易失败的后续终端处理

如当前交易执行小额免密处理，但超过发卡行闪付小额免密限额控制，发卡行拒绝交易并返回“交易金额超限”应答码，终端交易失败并提示金额超限。因金额超限拒绝交易的应答码复用现有“交易金额超限”应答码，终端提示上不进行区分。

当操作者（收银员）发现终端“金额超限”提示后，应选择菜单中“闪付凭密”交易，该交易选项下，终端将强制提示密码输入，且不支持PIN ByPss。但是，“闪付凭密”选项下发起的所有交易均不再属于闪付小额免密交易。

H.4 凭证打印

若当笔交易符合“免签名”要求，则进行如下处理：

——热敏打印机：不打印签名栏，原签名栏区域打印“交易金额不足XX元，无需签名”，其中XX元与“免签限额”参数一致（下同）；

——针式打印机：签名栏区域空白处打印“交易金额不足XX元，无需签名”。

H.5 参数要求

H.5.1 应用参数

终端新增参数，控制快速业务金额。

表3 下发参数表

参数名称	用途	格式	取值
非接快速业务（QPS）免密限额	终端使用此数据元作为条件之一判断非接联机交易是否请求持卡人验证方法	12 位数字，表示 XXXXXXXXXX.XX	现值 0000000300.00 后续根据业务需求调整
免签限额	终端使用此数据元作为判断交易凭证是否需要进行免签处理	12 位数字，表示 XXXXXXXXXX.XX	现值 0000000300.00 后续根据业务需求调整

H.5.2 功能控制参数

终端通过功能控制参数启用或关闭某项功能、启用或取消某项处理逻辑。

终端处理逻辑中使用的新功能控制参数定义如下。

表4 功能控制参数

参数名称	含义	格式	取值
非接快速业务标识	终端使用此数据元作为是否开启非接快速功能的判断条件。	1 位数字	1-启用 0-关闭
BIN 表 A 标识	终端使用此数据元作为是否将 BIN 表 A 作为免密的判断条件，启用该标识意味着非接快速业务处于试点阶段。	1 位数字	1-启用 0-关闭
BIN 表 B 标识	在终端启用此数据元意味着非接快速业务试点结束，但仍处于试点阶段二的初期阶段，即贷记卡实现全面支持，但此时境内借记卡尚未实现全面支持，借记卡依然根据 BIN 表判断。	1 位数字	1-启用 0-关闭
CDCVM 标识	终端使用此数据元作为是否将卡片 CDCVM 执行情况作为免密的判断条件。	1 位数字	1-启用 0-关闭
免签标识	终端使用此数据元作为是否支持交易凭证免签处理的判断条件	1 位数字	1-启用 0-关闭

上述控制参数存在优先级，具体逻辑关系参见“终端处理逻辑”部分。

H.6 参数控制说明

H.6.1 QPS控制

试点之前：试点商户逐步改造终端，装载BIN表A和BIN表B，此时关闭“非接快速业务标识”，终端处理逻辑与现行方式完全一致。

试点阶段一：启用“非接快速业务标识”，启用“BIN表A标识”，关闭“BIN表B标识”，此时贷记卡和借记卡均部分参与，通过BIN表A判断是否支持本产品。

试点阶段二：启用“非接快速业务标识”，关闭“BIN表A标识”，启用“BIN表B标识”，此时境内贷记卡完成全部切换，无需卡BIN判断，但借记卡尚未实现全部切换，因而需使用BIN表B判断。

全面支持推广阶段：启用“非接快速业务标识”，关闭“BIN表A标识”，关闭“BIN表B标识”。

H.6.2 小额免签控制

小额免签与 QPS 业务相对独立，但遵循“免密必免签”原则，开通 QPS 的商户终端均支持小额免签；未开通 QPS 的商户，如纳入免签商户管理，终端亦支持小额免签。

小额免签与 CDCVM 完全独立，其是否开启与 CDCVM 业务是否开启无强关联性。

H.7 方案前提条件和注意事项

H.7.1 BIN表设置说明

BIN表A：试点阶段一过程中参与试点的贷记卡和借记卡BIN号，在试点阶段一结束、试点阶段二开始时，BIN表A通过“BIN表A标识”参数的控制而关闭使用。

BIN表B：试点阶段二过程中参与试点的借记卡BIN号，包含试点阶段一BIN表A中的全部借记卡BIN号、以及在试点阶段二投入试点的借记卡BIN号。在试点阶段二结束、全面支持推广阶段开始时，BIN表B通过“BIN表B标识”参数的控制而关闭使用。

注意，BIN表A和BIN表B均在试点开始前随程序灌装入终端，根据不同阶段的切换而启用或关闭，后续不再变更，即：如BIN表B与BIN表A的借记卡BIN号部分存在差异，则该差异必须在试点开始前提前明确，后续不再进行变更。

卡BIN可以是借记、贷记或准贷记。考虑到终端容量和交易速度的要求，卡BIN上限为100个。

H.7.2 终端IC处理内核影响

方案在正常GPO完成后插入读取卡片货币代码的步骤，改变了现有qUICS流程，需对终端内核进行改造。

方案支持CDCVM，将其做为CVM一种方式，改变了现有qUICS终端侧处理逻辑和流程，需对终端内核进行改造，具体CVM协商处理流程见6.4节“CDCVM应用说明”。

H.7.3 内外卡判断说明

本处理逻辑中的“外卡”指境外发行的银联卡。

GPO处理完成后，终端通过Get Data获取Tag 9F51、TagDF71（应用货币代码），如Tag 9F51、TagDF71其中一个为人民币，则该卡视为“内卡”处理；如Tag 9F51、TagDF71均为非人民币，则该卡视为“外卡”处理。

H.7.4 免签判断

终端在收到交易成功的联机响应报文后，根据以下条件判断是否对交易凭证做免签处理：

——功能标识检查：终端支持小额免签，即“免签标识”取值为“1”；

——交易金额检查：交易金额小于等于免签限额，交易金额以响应报文域4（交易金额）为准。

H.8 终端报文接口

H.8.1 PIN状态

终端应遵守《销售点（POS）终端应用规范》要求，域22“服务点输入方式码”应与域52“个人标识码数据”填写情况一致，即域22准确标识当前交易是否存在PIN密文。

H.9 收单侧平台要求

H.9.1 参数下载

收单处理平台应能实现前述应用和功能控制参数的远程更新，并支持收单机构或专业化服务机构配置下载任务。

H.9.2 转接报文接口

收单平台向转接平台传递的报文中使用60.2.6域作为免密标志位，取值为“1”表示当前交易为免密交易。通过对终端上送交易报文的检查来判断是否在向转接传递的报文中置免密标志位，当以下条件都满足时，收单平台置60.2.6域为“1”，否则置60.2.6域为“0”，并执行后续处理流程。具体判断逻辑如下：

——交易类型检查：仅限于普通消费、自助消费、预授权、自助预授权。

——交易金额检查：交易金额（终端报文4域）小于QPS限额。

——交易方式检查：采用非接快速流程的IC卡交易，终端上送报文中包含55域（IC卡数据），且22域（服务点输入方式）前两位取值为“07”，即快速PBOC借贷记IC卡读入（非接触式）。

——个人识别码数据检查：终端上送报文中不包含52域（个人识别码数据）。

——商户限制：商户号应属于在免密商户白名单。

——卡片范围检查：仅在试点阶段一和试点阶段二中需要执行，用于检查交易主账号是否属于非接快速业务范围（试点阶段一检查卡BIN，试点阶段二初期检查全体贷记卡和借记卡BIN表，借贷记均完成切换后不再检查）。

附录 I
（资料性附录）
CDCVM 的应用

I.1 CDCVM应用说明

I.1.1 终端与卡片协商CVM过程

本节阐述的终端与卡片协商CVM过程指qUICS流程中终端IC卡内核与卡片间交互的过程，不包括应用层处理。CDCVM的引入对终端内核处理卡片返回的交易属性标签（卡片对CVM的要求）的机制产生影响和变化，具体如下：

支持超过一个CVM的终端应当查询卡片交易属性（Tag 9F6C）的第1字节第8位（需要联机PIN标识）、第2字节第8位（CDCVM已执行标识）、以及第1字节第7位（需要签名标识），决定卡片选择哪个CVM。如第1字节位8=“1”，终端应当执行联机PIN校验，不再查询第2字节位8和第1字节位7；如第1字节位8=“0”，终端应当查询第2字节位8。如第2字节位8=“1”（卡片端CDCVM已执行），终端应认为卡片要求CDCVM作为CVM方式并且已完成校验；如第2字节位8=“0”，则终端应当检查第1字节位7。除非终端支持联机PIN，否则卡片不会设置第1字节第8位。卡片逻辑不会将第1字节位8和位7都设置，但第2字节位8可能与第1字节位8或位7同时存在。

I.1.2 CDCVM卡片数据设置

卡片向终端返回的Tag 9F6C中包含是否已完成CDCVM的信息。

表5 Tag 9F6C 取值含义

字节	位	含义
字节 1	8	需要联机 PIN
	7	需要签名
	6	如果脱机数据认证失败而且终端可联机，则要求联机
	5	如果脱机数据认证失败而且终端支持接触标准借贷记，则终止
	4-1	RFU
字节 2	8	CDCVM 是否执行，1-CDCVM 已执行，0-CDCVM 未执行
	7-1	RFU

Tag 9F6C的生成逻辑由卡片内部完成。