ICS xxxxxxx
X xx
备案号:

JT

中华人民共和国交通运输行业标准

JT/T xxxxx—xxxx

公共交通IC卡技术规范
第2部分：读写终端

Technical specification on public transport fare system

—Part 2 :Terminal

（征求意见稿）

20xx-xx-xx 发布　　20xx-xx-xx 实施

中华人民共和国交通运输部　发布

目　　次

前　言

JT/T xxx《公共交通IC卡技术规范》由6个规范组成：

——第1部分：卡片；

——第2部分：读写终端；

——第3部分：信息接口；

——第4部分：非接触通讯接口；

——第5部分：安全；

——第6部分：检测；

本部分为JT/T xxx的第2部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中华人民共和国交通运输部运输司提出。

本部分由全国城市客运标准化技术委员会(SAC/TC529)归口。

本部分主要起草单位：交通运输部公路科学研究院、中国交通通信信息中心、交通运输部科学研究院、北京市政交通一卡通有限公司、南京市市民卡有限公司、武汉城市一卡通有限公司、中钞信用卡产业发展有限公司、天津市通卡公用网络系统有限公司、天津环球磁卡股份有限公司、银行卡检测中心。

本部分主要起草人：杨蕴、王立岩、梅新明、王刚、汪宏宇、李岚、唐猛、沈伟彬、张永军、刘好德、谷云辉、钱贞国。

公共交通IC卡技术规范

第2部分：读写终端

1 范围

JT/Txxx的本部分规定了公共交通互联互通使用的终端，其数据对象列表、终端技术要求、终端应用技术要求、电子现金交易流程、电子钱包交易流程。本部分适用于开展公共交通互联互通业务的地区、发卡机构以及收单机构。其使用对象主要是参与公共交通互联互通的终端，包括公交、地铁、出租等公共交通领域所使用的终端。

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，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2659 世界各国和地区名称代码

GB/T 12406 表示货币和资金的代码

GB/T 15150 产生报文的银行卡 交换报文规范 金融交易内容

GB/T 15273 信息处理八位单字节编码图形字符集

GB/T 16649.5 识别卡 带触点的集成电路卡 第5部分：应用标识符的编号系统和注册程序

3 术语和定义

下列术语和定义适用于本文件。

3.1

终端 terminal

在交易点安装、用于与公共交通IC卡配合共同完成交易的设备。它应包括接口设备，也可包括其它的部件和接口（如与主机的通讯）。

3.2

终端随机数 terminal random

终端通过SAM卡产生的随机数。

3.3

数据完整性 data integrity

数据不受未经许可的方法变更或破坏的属性。

3.4

ID号 identify number

用于区分同一行业在不同地区的应用。

3.5

接口设备 interface device

终端上与公共交通IC卡进行通讯处理的部分，包括其中的机械和电气部分。

3.6

圈存 load

增加卡中电子现金/电子钱包余额的过程,圈存后的电子现金余额不能超过电子现金/电子钱包余额上限。

3.7

圈提 unload

持卡人将电子钱包中的全部金额提取。圈提交易应在特定的终端上联机进行。

3.8

支付系统环境 payment system environment

当符合本部分的支付系统应用被选择，或者用于支付系统应用目的的目录定义文件（DDF）被选择后，公共交通IC卡中所确立的逻辑条件集合。

3.9

脱机预授权交易 offline pre-authorization

脱机预授权交易是指受理方将预估的消费金置入交易命令中发送给卡片,卡片通过风险控制和额度检查，批准交易，并冻结卡内对应电子现金额度。

3.10

脱机预授权完成交易 offline pre-authorization completion

脱机预授权完成交易是指受理方在预授权有效期内以发送交易命令发送给卡片,卡片通过风险控制和额度检查，批准交易，并返还卡内对应的电子现金额度。

4 缩略语

下列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）
ARPC 授权响应密文（Authorization Response Cryptogram）
ARQC 授权请求密文（Authorization Request Cryptogram）
ATC 应用交易计数器（Application Transaction Counter）
ATI 应用类型标识（Application Type Identifier）
APDU 应用协议数据单元（Application Protocol Data Unit）
AUC 应用用途控制（Application Usage Control）

BER	基本编码规则（Basic Encoding Rules）
C	条件（Condition）
CAPP	扩展应用（Comprehensive Application）/复合应用（Complex APPlication）
CAM	卡片认证方法（Card Authentication Method）
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)
CID	密文信息数据（Cryptogram Information Data）
Cn	压缩数字型（Compressed Numeric）
CVM	持卡人验证方法（Cardholder Verification Method）
CVR	卡片验证结果（Card Verification Results）
DDA	动态数据认证（Dynamic Data Authentication）
DDOL	动态数据认证数据对象列表（Dynamic Data Authentication Data Object List）
DEA	数据加密算法（Data Encryption Algorithm）
DES	数据加密标准（Data Encryption Standard）
DF	专用文件（Dedicated File）
EC	电子现金（Electronic Cash）
EF	基本文件（Elementary File）
FCI	文件控制信息（File Control Information）
fDDA	快速动态数据认证（Fast DDA）
GPO	获取处理选项（Get Processing Options）
IAC	发卡机构行为代码（Issuer Action Code）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
IFD	接口设备（Interface Device）
INS	命令报文的指令字节（Instruction Byte of Command Message）
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）
Le	响应数据中的最大期望长度（Maximum Length of Data Expected）
M	必备（Mandatory）
MAC	报文鉴别码（Message Authentication Code）
MDK	主密钥（Master DEA Key）
N	数字型（Numeric）
O	可选（Optional）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
PAN	主账号（Primary Account Number）
PDOL	处理选项数据对象列表(Processing Options Data Object List)
PIN	个人识别码（Personal Identification Number）
PPSE	近距离支付系统环境（Proximity Payment Systems Environment）
RFU	

RID	注册的应用提供商标识（Registered Application Provider Identifier）
R-MAC	响应数据的报文鉴别码（Response Message Authentication Code）
SAM	安全认证模块（Secure Authentication Module）
SFI	短文件标示符（Short File Identifier）
SW1	状态字 1（Status Word One）
SW2	状态字 2（Status Word Two）
TAC	交易验证码（Transaction Authorization Cryptogram）
TC	交易证书（Transaction Certificate）
TLV	标签、长度、值（Tag Length Value）
TSI	交易状态信息（Transaction Status Information）
TDOL	交易证书数据对象列表（Transaction Certificate Data Object List）
TRAN	终端随机数（Terminal RANdom）
TTI	交易类型标识（Transaction Type Identifier）
TVR	终端验证结果（Terminal Verification Results）
UDK	子密钥（Unique DEA Key）

5 数据对象列表

5.1 数据元

定义并解释公共交通IC卡电子现金和电子钱包应用数据交换过程中终端所需的相关数据元。包括数据元的名称、标识及功能等，见附录A。

5.2 数据对象列表

终端处理电子现金应用，应卡片的要求需要建立可变的数据元列表用来向卡片发送。为了减少公共交通IC卡内对这些数据的处理，这个列表不需要进行TLV编码，而只是把若干数据单元连接成一个复合域。因此，需要在公共交通IC卡内包含一个数据对象列表（DOL）来定义复合域中的数据格式。本部分用的DOL包括：

——卡风险管理数据对象列表 1（CDOL1）：在第一次 GENERATE AC 命令中需要传送给卡片的数据对象列表。CDOL1 是终端在读应用记录处理过程中从卡片中读出的；

——卡风险管理数据对象列表 2（CDOL2）：在第二次 GENERATE AC 命令中需要传送给卡片的数据对象列表。CDOL2 是终端在读应用记录处理过程中从卡片中读出的；

——交易证书数据对象列表（TDOL）：列出生成交易证书（TC）哈希计算的数据对象（标签和长度）；

——动态脱机数据认证对象列表（DDOL）：指定在 INTERNAL AUTHENTICATE 指令中，卡片要求终端送入卡片的终端数据标签和长度列表。

一个DOL是用一些条目连接而成的列表。每个条目代表一个加入复合域的单个数据元。每个条目的格式包括1~2个字节的标签来表明需要的数据对象，然后是1个字节的长度部分，表明本数据对象在命令数据中占据的字节长度。

终端应完成下列步骤以建立结构域：

——从公共交通 IC 卡中读取 DOL。

——连接 DOL 中列出的所有数据单元。按照下列规则进行连接：

1） 如果 DOL 中指出的数据对象的标签无法识别，终端将提供一个长度为 DOL 指定长度的数据元，并把该数据元所有的数值部分设置为 16 进制的 0。

2) 如果该列表上的一个数据对象在终端上可以识别，但属于公共交通 IC 卡上不出现的可选静态数据，那么在命令区域上代表数据对象的部分应用 16 进制的 0 来填满。
3) 如果在 DOL 条目中指出的长度小于实际数据对象的长度,则需要将实际的数据对象削减至 DOL 指出的长度。如果数据对象是数字格式（n）的，则从数据单元的的最左端开始削减字节。如果数据对象是其它格式的，则从数据单元的最右端开始削减字节。如果指出的长度比实际的数据长度大，需要把实际的数据填充至指定长度：
   - 如果数据对象是数字格式（n）的，则从数据单元头部开始填充 16 进制的 0;
   - 如果数据对象是压缩数字型（cn）的，则在数据单元的末尾填充 16 进制的 FF;
   - 如果数据对象是其它格式的，则在数据单元的末尾填充 16 进制的 0。
4) 如果 DOL 中某个数据对象在终端可以识别，但不适用于当前交易，代表该数据对象的命令域部分将填充 16 进制的 0。

——数据单元在表上的连接顺序应该与在 DOL 中出现的顺序一一对应。

6 终端技术要求

6.1 功能要求

6.1.1 通用要求

支持电子钱包和/或电子现金应用的终端应符合JT/T XXX.1和JT/T XXX.3的规定。它应支持JT/T XXX.1和本部分所定义的电子现金和/或电子钱包应用的所有文件和命令。支持电子现金和/或钱包应用的终端应该是可以在有人或无人环境中运行的联机终端或脱机终端。此处所指的终端也包括其他能够读取电子现金和/或电子钱包余额和/或交易明细的终端（如手持终端）。

6.1.2 基本交易类型

电子现金应用支持的基本交易类型见表1、表2。

表1 字节 1：交易类型

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	现金
X	1	x	x	x	x	x	x	商品
X	x	1	x	x	x	x	x	服务
X	x	x	1	x	x	x	x	RFU
X	x	x	x	1	x	x	x	查询
X	x	x	x	x	1	x	x	RFU
X	x	x	x	x	x	1	x	付款
X	x	x	x	x	x	x	1	管理

表2 字节 2：交易类型

b8	b7	b6	b5	b4	b3	b2	b1	意义
1	x	x	x	x	x	x	x	RFU
X	0	x	x	x	x	x	x	RFU
X	x	0	x	x	x	x	x	RFU
X	x	x	0	x	x	x	x	RFU

X	x	x	x	0	x	x	x	RFU
X	x	x	x	x	0	x	x	RFU
X	x	x	x	x	x	0	x	RFU
X	x	x	x	x	x	x	0	RFU

电子钱包应用支持的基本交易类型定义如下：

——02：电子钱包圈存

——03：电子钱包圈提

——06：电子钱包消费

——07：电子钱包修改透支限额

——09：复合应用消费

6.1.3 快速支付交易类型

公共交通 IC 卡应用主要应用于城际客运、轮渡、轨道交通、公共汽电车、停车收费咪表、城际铁路、出租车等与道路运输应用相关的支付场景，主要包括圈存交易和快速支付交易两种交易大类，圈存交易为联机交易，快速支付交易为脱机交易。

在以上场景中，快速支付交易又根据扣费方式的不同，可以分为标准快速支付交易、分时分段扣费交易、单次扣款优惠交易等不同的扣款交易类型。对于电子现金应用，还可以支持脱机预授权交易这一专用的交易类型。

标准快速支付交易适用于单一票价的公共汽电车、轨道交通、轮渡以及单次快速支付的出租车应用场景。

分时分段扣费交易适用于单笔交易金额较小的分段计价公共汽电车、轨道交通、城际客运班车、轮渡以及分时计价停车场应用场景。

单次扣款优惠适用于存在换乘优惠等特殊要求的快速支付交易场景。

脱机预授权交易适用于单笔交易金额较大的分段计价城际客运班车、城际铁路和分时计价停车场等应用场景，预先冻结一部分金额作为预授权的保证金，确保基本收益。

具体的交易应用类型标识详见表 3。

表3 快速支付交易应用类型列表

应用类型	快速支付交易类型标识
城际客运应用	0x01
轮渡应用	0x02
轨道交通应用	0x03
公共汽电车应用	0x04
停车收费咪表应用	0x05
城际铁路铁路应用	0x06
出租车应用	0x07
公共交通 IC 卡联网通用应用	0x08

6.1.4 交易输入方式

终端支持非接触式读取芯片卡。

6.1.5 下载管理

终端应支持对应用程序、密钥和参数等数据的下载，更新和删除。

下载的通讯端口可灵活扩展,包括串行通讯口（RS232、RS485）、Modem通讯口、USB口、红外、GPRS、CDMA和TCI/IP网络端口或其它类型的通讯端口等中的一种或几种。下载的方式可为本地下载或远程下载等方式。

终端应保证下载控制的安全。只有经过授权或认可的一方才能向终端下载数据，未经授权，不得更改终端中的内容。终端还应能够确认下载数据的安全，能验证终端下载程序的完整性和正确性，确保敏感数据在下载过程中不会泄漏。

6.2 硬件要求

6.2.1 存储空间

终端应当具有足够的存储空间来存放应用程序、密钥、交易数据和其它参数等，并确保在掉电后这些数据不会丢失。

6.2.2 公共交通 IC 卡读卡器

终端应提供公共交通IC卡读卡器的接口，用来与公共交通IC卡进行命令数据传递通讯。该读卡器模块包括机械、电气和逻辑协议等部分。建议终端的读卡器位置有明显刷卡标识。

6.2.3 SAM 卡读写器及卡槽

支持电子钱包或分时分段等扩展应用的可脱机终端应提供符合标准SAM卡接口的SAM卡读写器及卡槽，用来接受SAM卡插入并与SAM卡进行命令数据传递通讯。该模块包括机械、电气和逻辑协议等部分。SAM卡交易指令见本部分附录B。

互联互通SAM卡应用的AID为：0xA0000006324D4F542E435053414D3031。

6.2.4 显示

有服务员的终端应配置有显示给服务员的显示屏，可选带有显示给持卡人的显示屏。以供监测交易过程、输入数据、设置选项或确认交易数据。终端应支持GB/T 15273的基本字符集。建议显示屏应具备中文显示能力。

6.2.5 打印机

圈存终端配置有能打印交易单据的打印机，根据公共交通IC卡系统要求可以是针式或热敏打印机。对每笔批准的交易，不论是脱机、联机或语音授权都能打印出交易单据。脱机终端打印功能可选。

打印单据格式由各收单机构自定，但应包含如下数据：卡号、应用标识符AID、交易日期时间、金额、收单机构代码。

6.2.6 时钟

能处理脱机交易的终端应配有时钟模块，用来提供当地日期和时间。

日期用于应用生效日期、应用失效日期以及脱机数据认证中的证书有效期检查。时间用于确保交易唯一性识别以及作为应用密文生成算法中的输入数据。

6.2.7 与后台通信模块

有联机通讯能力的终端应当配置有与收单机构主机后台通信的模块。用于向主机发送交易数据包获取授权，或由主机对终端进行管理的功能。根据收单机构的要求可采用PSTN Modem拨号、GSM、GPRS、CDMA和TCP/IP等方式。通信模块与收单机构主机的通信速度应能满足实时传送公共交通IC卡交易数据的要求。

6.2.8 键盘

终端应带有用于输入交易金额、选择命令和执行功能的按键键盘。支持数字键、字母键、命令键和功能键。如果采用了带颜色的命令键，推荐使用下面的颜色分配。

命令键颜色：确认－绿色；取消－红色；清除－黄色。

6.2.9 硬件协处理器

对于支持电子现金应用的终端，推荐使用支持非对称密码算法签名验证的硬件协处理器。

6.2.10 蜂鸣器

终端应支持能够通过声音提示持卡人的相关操作，当持卡人刷卡完成或者刷卡失败是能有明确提示。

6.2.11 操作指示灯

终端应能够通过操作指示灯提示持卡人本终端的工作状态。

6.2.12 语音提示功能

在必要的条件下，终端应能支持通过语音提示持卡人进行相关的操作或通过语音反馈操作结果。

6.3 终端类型

本部分所覆盖的终端类型包括车载终端、闸机、自助终端等。

对各种终端类型的硬件要求见表4。

表4 终端类型的硬件要求

项目号	硬件设备	有服务员			无人服务（自助）		
		仅联机	联机/脱机	仅脱机	仅联机	联机/脱机	仅脱机
1	存储空间	必备	必备	必备	必备	必备	必备
2	公共交通 IC 卡读卡器	必备	必备	必备	必备	必备	必备
3	SAM 卡读写器及卡槽	可选	必备	必备	可选	必备	必备
4	显示屏	推荐	推荐	必备	必备	必备	必备
5	打印机	推荐	推荐	可选	必备	推荐	可选
6	时钟	必备	必备	必备	必备	必备	必备
7	主机通信模块	必备	必备	推荐	必备	必备	推荐
8	键盘	推荐	推荐	可选	必备	必备	可选
10	硬件协处理器	可选	可选	可选	可选	可选	可选
11	蜂鸣器	必备	必备	必备	必备	必备	必备
12	操作指示灯	必备	必备	必备	必备	必备	必备
13	语音提示功能	可选	可选	可选	可选	可选	可选

7 终端应用技术要求

本章讨论所有非接触式终端应用应满足的要求。

7.1 电子现金应用终端通用要求

7.1.1 终端通讯要求

——终端应符合 JT/T XXX.4，并同时支持 Type A 和 Type B；
——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)；
——对于 Type B 卡，终端应支持 MBLI＝0 和 MBLI＝1。

7.1.2 通用终端要求

——具有脱机能力的终端应支持 fDDA；
——终端应支持 5.2 定义的数据对象列表；
——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；
——终端应明确通知持卡人：
1) 刷卡
2) 交易过程
3) 交易结果——批准、拒绝或终止
——推荐的终端信息有：
1) 刷卡
2) 读卡成功
3) 处理中
4) 再次刷卡[如果交易未完成]
5) 交易批准
6) 交易拒绝
7) 出示单一卡片[防冲突]
——当提示刷卡时，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。

7.2 电子钱包应用终端通用要求

7.2.1 终端通讯要求

——终端应符合 JT/T XXX.4，并至少支持 Type A，可选支持 Type B；
——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)；
——对于 Type B 卡，终端应支持 MBLI＝0 和 MBLI＝1。

7.2.2 通用终端要求

——具有脱机能力的终端应支持 SAM 卡；
——终端应明确通知持卡人：
1) 刷卡
2) 交易过程
3) 交易结果——批准、拒绝或终止
——推荐的终端信息有：
1) 刷卡
2) 读卡成功
3) 处理中

4) 再次刷卡[如果交易未完成]
5) 交易批准
6) 交易拒绝
7) 出示单一卡片[防冲突]

——当提示刷卡时，终端应显示当前交易金额。

——终端应显示交易后的可用余额，以表示读卡操作成功。

7.3 激活非接触界面前的处理要求

为了使卡片保持在感应区的时间最小化，公共交通IC卡应用终端在提示持卡人刷卡和激活非接触界面前，应执行下列处理。

7.3.1 预处理前的处理要求

具有公共交通IC卡应用能力的终端应在交易预处理完成后再将非接触界面上电。

7.3.2 具有公共交通 IC 卡应用能力终端中的交易预处理

除非交易预处理已经完成，否则支持公共交通IC卡应用终端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：

——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”）/交易金额，并检查是否超过最低限额；

对于支持电子现金的终端，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。

——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，除非终端支持公共交通 IC 卡应用扩展应用，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，除非终端支持公共交通 IC 卡应用扩展应用，仅支持脱机的终端应终止交易。；

——如果授权金额大于或等于终端非接触交易限额（如果存在），则终端应提示交易终止；

——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）；

——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，终端应要求刷卡，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1所示。

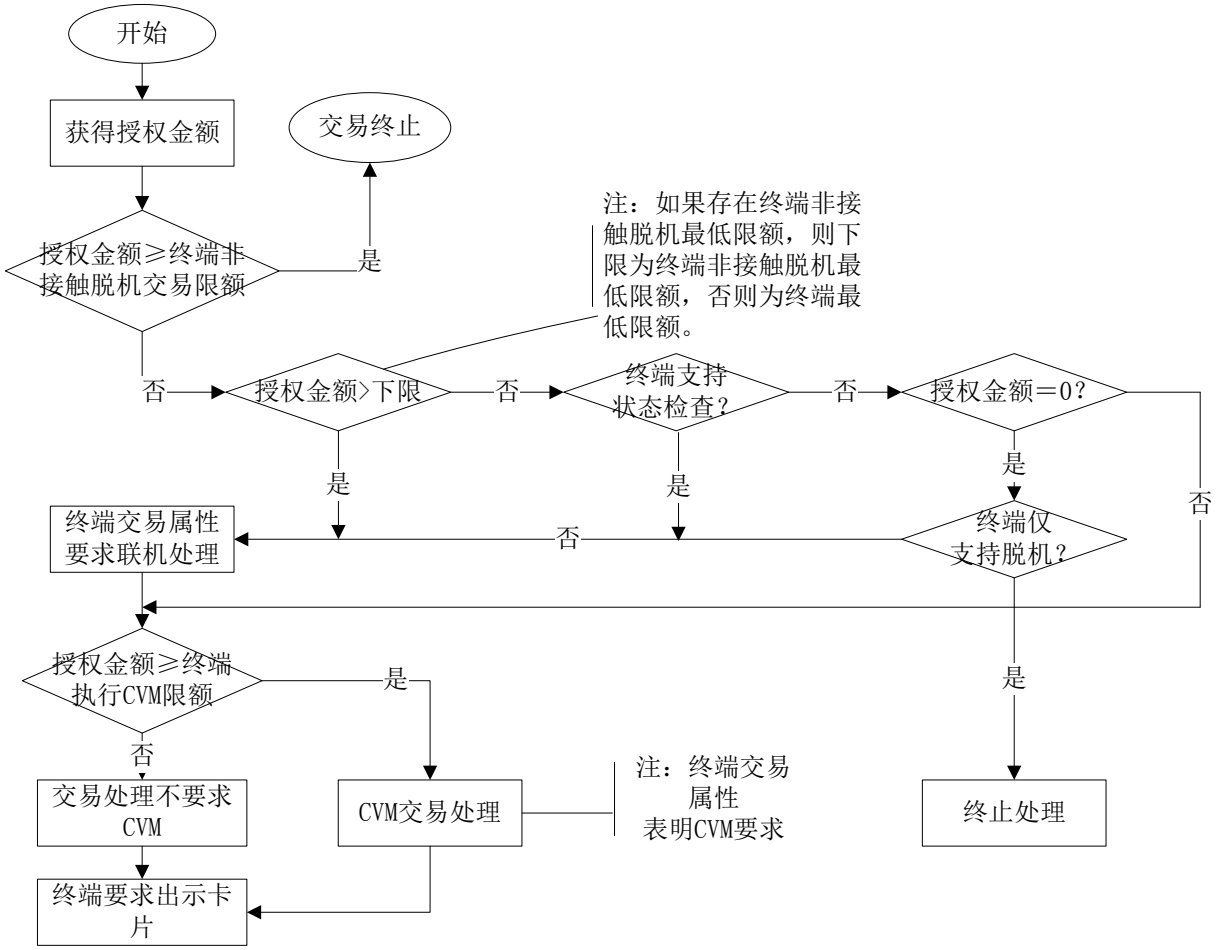


图1　具有公共交通 IC 卡应用能力终端的预交易处理

7.4　卡片检测处理要求

当卡片进入终端的感应范围，终端与卡片进行通信的初始化（公共交通IC卡应用终端应按照7.3.2部分的描述，在初始化交易前执行公共交通IC卡应用预处理）。

终端可以按照操作员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2中。

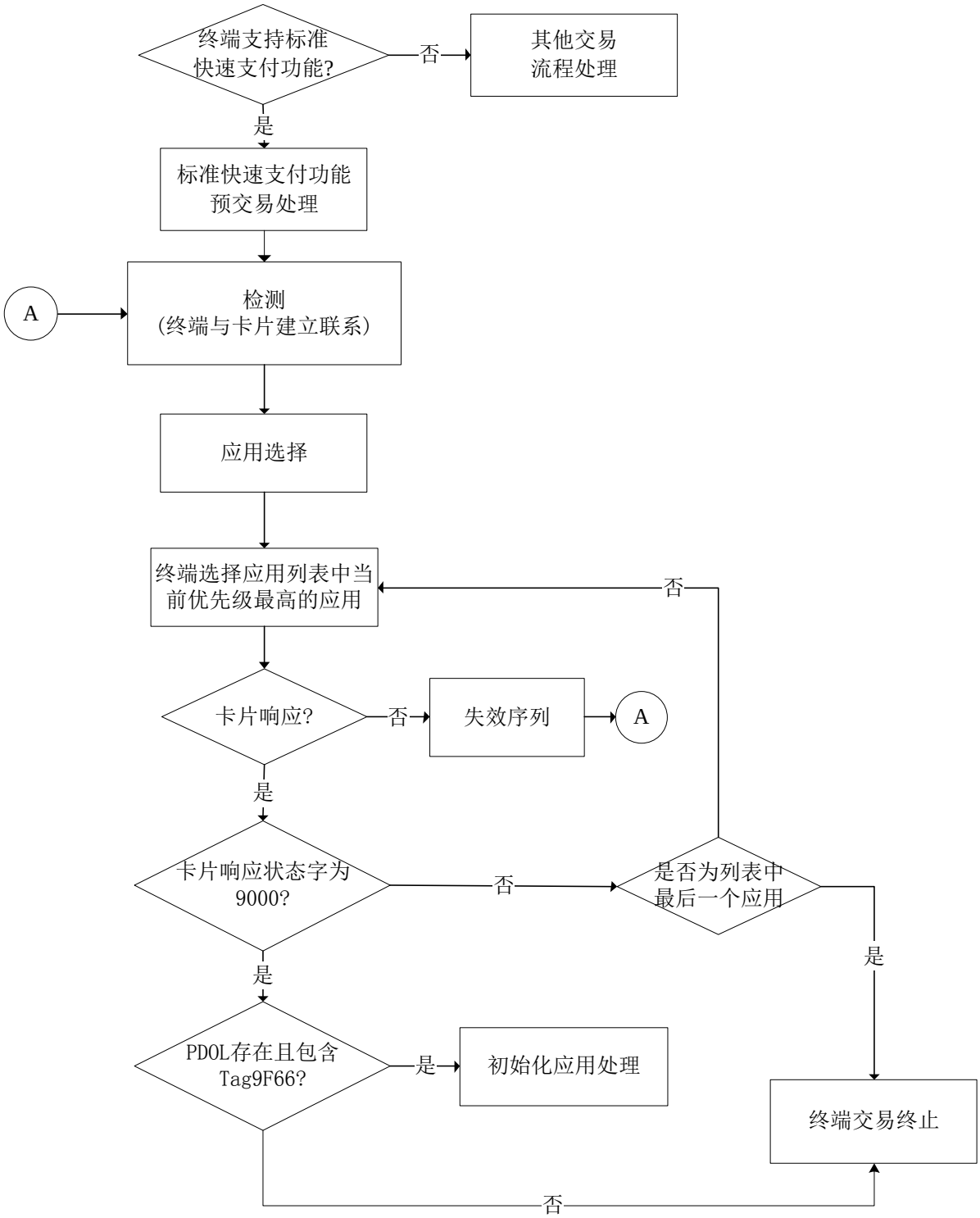


图2　卡片检测和应用选择流程

7.5　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（非接触式公共交通IC卡应用）。

7.5.1　终端应用选择要求

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。为更好地满足时间要求，终端支持

的应用列表中，建议将公共交通 IC 卡电子现金应用或电子钱包应用作为最高优先级。如果要求一个以上的应用，应用的数量要尽可能少。

——所有终端可以直接通过应用 AID 的进行应用快速直选，可选支持使用 PPSE 目录选择方法；

——如果使用 PPSE 目录选择法，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 字节的应用名称（AID）；

——终端访问卡片应用中的路径应采用一个公共交通 IC 卡应用的 AID，访问电子现金应用或者电子钱包应用；

——如果使用 PPSE 目录选择法，终端应建立包含在 FCI 中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；

——如果使用 PPSE 目录选择法，且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，并终止交易；

——如果使用 PPSE 目录选择法，且 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 7.3 的要求返回到卡片检测处理。

7.5.2 电子现金终端交易属性

表5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：公共交通IC卡联机处理交易（以下简称“联机交易”）和公共交通IC卡快速支付交易（以下简称“快速支付交易”）、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。

表5 终端交易属性（标签为“9F66”）

字节	位	定义
1	8	预留
	7	1 – 支持联机处理功能 0 – 不支持联机处理功能
	6	1 – 支持快速支付功能 0 – 不支持快速支付功能
	5	预留
	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

7.5.3 电子钱包终端有效性检查

对于SELECT命令回送的数据，终端将对这些数据进行以下检查：

——该卡是否在终端存储的黑名单卡之列（使用发卡机构编码和应用主账号）；

——终端是否支持该发卡机构编码；

——终端是否支持 IC 卡上的应用[使用应用类型标识（ATI）来检查]；

——应用是否在有效期内。

如果以上任一条件不满足时，终端所做的处理不属于本部分的范围。

终端根据应用选择时获得的应用类型标识判别IC卡支持电子钱包的情况，自动选择电子钱包，进行后续交易。

如果IC卡不支持电子钱包应用，则该过程终止。

7.6 电子现金终端初始应用处理要求

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3所示。

7.6.1 电子现金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的 GPO 响应报文中,数据对象是一个标签为‘77’的基本数据对象。数据域可以包含多个 BER-TLV 编码的对象；

——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，并终止交易。

7.6.2 GPO 命令无响应

如果卡片响应终端发出的GPO命令失败，则终端应初始化失效序列，并返回到7.3的检测处理。

7.6.3 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，并终止交易。

7.6.4 GPO 命令的成功响应

终端通过应用交互特征和卡片响应GPO命令提供的数据元决定是否按照快速支付功能或联机处理功能进行交易。

——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（联机处理功能和快速支付功能），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’，假设终端支持快速支付功能，并且应用密文（标签“9F26”）在 GPO 命令响应中出现，则终端应按照快速支付功能处理交易。如果标签为“9F26”的数据项不出现，则终端应按照联机处理功能处理交易。

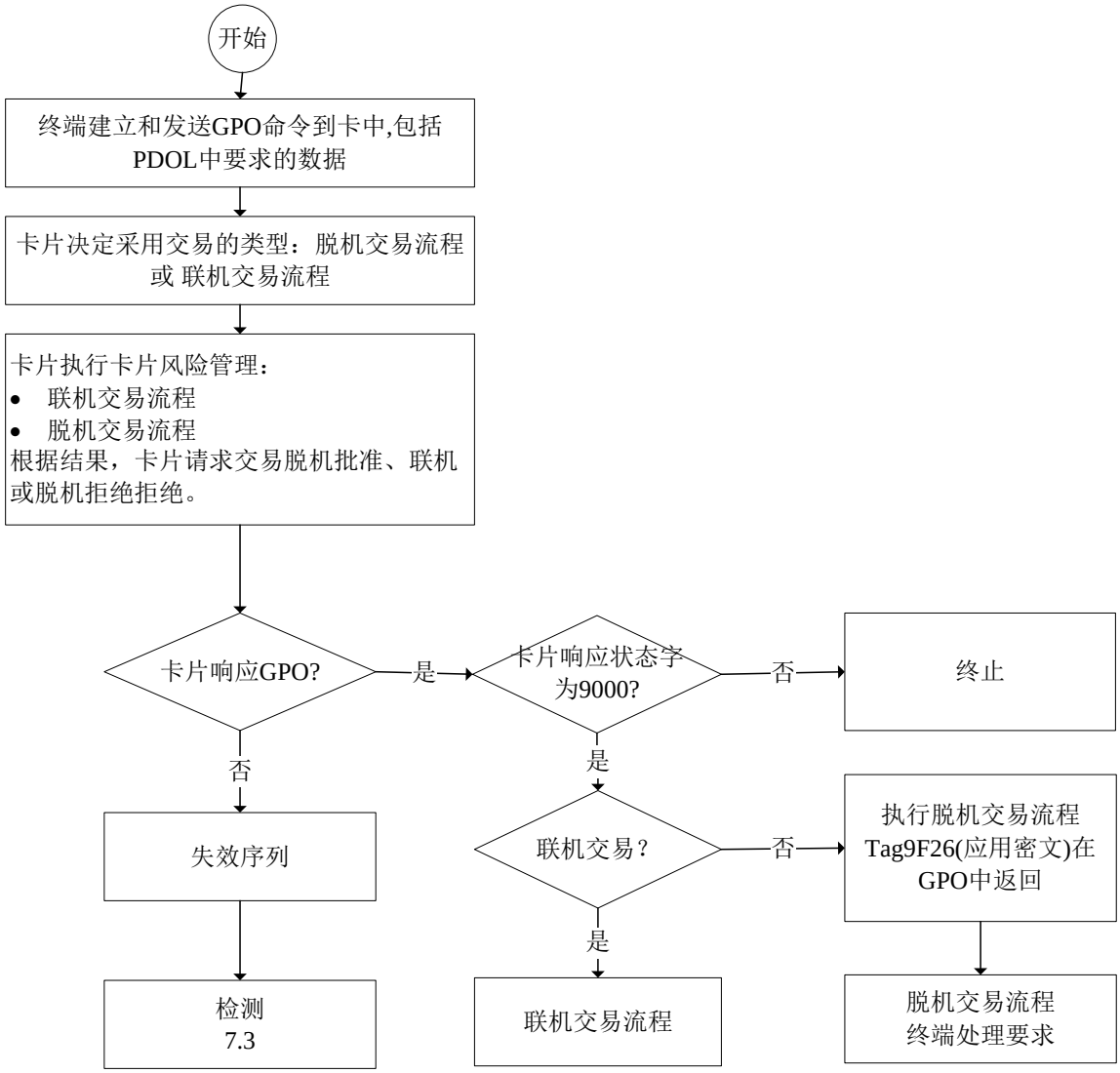


图3　初始应用处理流程

7.6.5　电子现金非接触交易次序

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。快速支付功能支持脱机和快速联机交易，不需要卡片放在卡盘上。

——标准快速支付功能：如果卡片支持公共交通 IC 卡应用且“终端交易属性”第 1 字节第 6 位＝‘1’（支持快速支付功能），则卡片应使用标准快速支付功能路径，终端应按照标准快速支付功能处理交易；

——联机处理功能：如果卡片支持联机处理功能且“终端交易属性”第 1 字节第 7 位＝‘1’（支持联机处理功能），则卡片应使用联机处理功能路径，终端应按照联机处理功能处理交易。

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。

8 电子现金交易流程

8.1 电子现金联机交易处理流程

8.1.1 功能概述

以下功能在公共交通IC卡应用交易处理中得到使用。标记为必备（M）的功能应该在所有交易中得到执行。标记为可选（O）的功能是可选择的并根据卡或终端的参数决定。联机交易包括：圈存、圈提、应用锁定及解锁、卡片锁定以及其他的发卡机构脚本下发。交易流程实例见图4。

8.1.1.1 应用选择

此为必备项，当卡片连接终端时，终端决定哪些应用由卡片和终端共同支持，终端有两种选择应用的方式：

——终端检测终端和卡片都支持的应用并将这些应用显示，供用户选择；

——终端根据发卡机构事先定义的优先级别自动选择卡片上优先级最高的应用。

终端发送SELECT命令选择应用，卡片返回文件控制信息（FCI），则其中应包括PDOL。

8.1.1.2 应用初始化

此为必备项，在终端选择应用之后，应读取卡片中的应用数据。由这些数据得知卡片具备的功能以及需要提供给卡片哪些支持。终端读取卡指示的数据并使用支持的功能列表来决定要执行的处理。

8.1.1.3 读应用数据

此为必备项，终端使用读记录命令（READ RECORD）读出交易处理中使用的卡片数据，卡片在应用初始化的响应中提供AFL标记了这些数据所在的文件与记录号，终端应该存储读出的所有可以识别的数据对象，不论是必备还是可选数据，以备将来交易使用。终端无法识别的数据对象不必存储，但是包含这种数据对象的记录可能仍然要以整体形式参与脱机数据认证过程，这取决于AFL的编码。

8.1.1.4 脱机数据认证

此外可选项,终端根据卡片和终端对这些方法的支持,决定是否使用动态数据认证来脱机认证卡片。如果终端支持脱机数据认证功能，并且检测到卡片支持动态数据认证（DDA），则终端需进行脱机数据认证。

动态数据认证（DDA）主要是用于防止伪造卡片。动态数据认证有标准动态数据认证（DDA）和复合动态数据认证（DDA/AC-CDA）两种。终端要求卡片提供由公共交通IC卡私钥加密动态交易数据生成的密文，动态交易数据是由终端和卡片为当前交易产生的唯一数据。终端用从卡片数据中获取的公共交通IC卡公钥来解密动态签名。还原的数据与原始数据匹配证实了此卡不是由合法卡复制出的赝品卡。复合动态数据认证/应用密文生成把动态签名生成与卡片的应用密文生成相结合，确保卡片行为分析时返回的应用密文来自于有效卡。

8.1.1.5 处理限制

此为必备项，终端执行交易处理限制判断交易是否允许进行。终端检查卡片的生效日期是否达到，卡是否超过失效日期，卡片和终端的应用版本是否匹配，应用用途控制（AUC）限制是否生效。发卡机构可以使用AUC限制卡片的应用，包括：国内、国外、现金、商品、服务或返现。

8.1.1.6 持卡人验证

终端应具备持卡人身份验证功能。持卡人验证可以用来确保持卡人是合法而且卡片没有遗失或被盗。终端使用卡片中的持卡人验证方法（CVM）列表数据决定验证的执行方法。CVM列表建立了持卡人验证方法优先级别，根据终端能力和交易特性提示用户采用特定的持卡人验证方法。如果持卡人验证方法是脱机PIN，终端提示持卡人输入PIN并传送持卡人输入的PIN到卡片中，卡片比较输入的PIN和卡片中的PIN值。CVM也可能指定联机PIN、签名或不需要持卡人验证。

8.1.1.7 终端风险管理

此为必备项，终端应具备风险管理功能。终端风险管理检查交易是否超过了最低限额，账号是否在终端异常文件中，连续脱机交易次数是否超过了限制次数，是否新卡，以及商户是否强制进行联机，有些交易可能被随机的选择联机处理。

终端风险管理也包括可选的频度检查，终端使用卡片中的数据进行检查。在终端行为分析过程中要考虑终端频度检查的结果。

8.1.1.8 终端行为分析

此为必备项，终端应具备终端行为分析功能。终端行为分析根据脱机数据认证、处理限制、持卡人验证、终端风险管理的结果以及终端和卡片中设置的风险管理参数决定如何继续交易（脱机批准、脱机拒绝和联机授权）。再由卡返回给终端的发卡机构行为代码（IAC）域设立卡片规则，在终端行为代码（TAC）设立终端规则。决定交易处理之后，终端向卡片请求应用密文。不同的应用密文对应不同的交易处理：以交易证书（TC）为批准，授权请求密文（ARQC）为联机请求，应用认证密文（AAC）为拒绝。

8.1.1.9 卡片行为分析

此为必备项，公共交通IC卡可以执行发卡机构定义的风险管理算法以防止发卡机构被欺诈。当卡片收到终端的应用密文请求时，卡片就执行卡风险管理检查，来决定是否要改变终端设定的交易处理，检查可能包括：先前未完成的联机交易、上一笔交易发卡机构认证失败或脱机数据认证失败、达到了交易笔数或金额的限制等。卡片可以将终端请求的脱机接受改成联机授权或脱机拒绝。卡片不能推翻终端做出的拒绝交易的决定。公共交通IC卡可以决定以下方式继续交易：

——同意脱机完成(TC)；

——联机授权(ARQC)；

——拒绝交易(AAC)。

完成检查后，卡片使用应用数据及一个存储在卡上的应用密文过程密钥生成应用密文。它再将这个密文返回到终端。对于脱机批准的交易，TC以及生成TC的数据通过清算消息传送给发卡机构，以备未来发生持卡人争议或退单时使用。当持卡人对交易有争议时，TC可以作为交易的证据还可验证商户或收单机构（是否）未改动交易数据。

当卡片作出接受交易的结论（卡片返回TC）后，卡片会记录交易日志。

8.1.1.10 联机处理

此为可选项，如果卡片或终端决定交易需要进行联机授权，同时终端具备联机能力，终端将卡片产生的ARQC报文送至发卡机构进行联机授权。此报文包括ARQC密文，用来生成ARQC的数据以及表示脱机处理结果的指示器。在联机处理中，发卡机构在联机卡片认证方法（CAM）过程中验证ARQC来认证卡片。发卡机构可以在它的授权决定中考虑这些CAM结果和脱机处理结果。

传送回终端的授权响应信息可以包括发卡机构生成的授权响应密文（ARPC）（由ARQC、授权响应码和卡片应用密文过程密钥产生）。此响应也可以包括发卡机构脚本，对卡片进行发卡后更新。

如果授权响应包含ARPC而且卡片支持发卡机构认证，卡片通过确认ARPC而执行发卡机构认证，来校验响应是否是来自真实的发卡机构（或其代理）。要在卡片里重新设置某些相关的安全参数必需成功地得到发卡机构认证。这阻止了犯罪者通过模拟联机处理来剽窃卡片的安全特性，以及通过欺诈性地批准交易来重设卡片的计数器和指示器。如果发卡机构认证失败，随后的卡片交易将发送联机授权，直到发卡机构认证成功。如果发卡机构认证失败，发卡机构有权设置卡片拒绝交易。

8.1.1.11 交易结束

此为必备项，除非交易在前几个步骤因处理异常被终止，否则终端应执行此功能用来结束交易。

卡和终端执行最后处理来完成交易。一个经发卡机构认可的交易可能根据卡片中的发卡机构认证结果和发卡机构写入的参数而被拒绝。卡片使用交易处理、发卡机构校验结果、以及发卡机构写入的规则来决定是否重设基于芯片卡计数器和指示器。卡片生成TC来认可交易，生成AAC来拒绝交易。

如果终端在授权消息之后传送清算信息，则TC应包括在该清算信息里。对于发卡机构批准而卡片拒绝的交易，终端应发起冲正。

当卡片作出接受交易的结论（卡片返回TC）后，卡片会记录交易日志。

8.1.1.12 发卡机构脚本处理

此为可选项，如果发卡机构在授权响应报文中包含了脚本，虽然终端可能对脚本不能理解，但终端仍需要将这些脚本命令发送给公共交通IC卡。在使用这些更新之前，卡片执行安全检查以确保脚本来自有效的发卡机构，且在传输中未有变动。这些命令对当前交易并不产生影响，主要会影响卡片的后续功能，如卡片应用解锁、卡片锁定、修改PIN等。

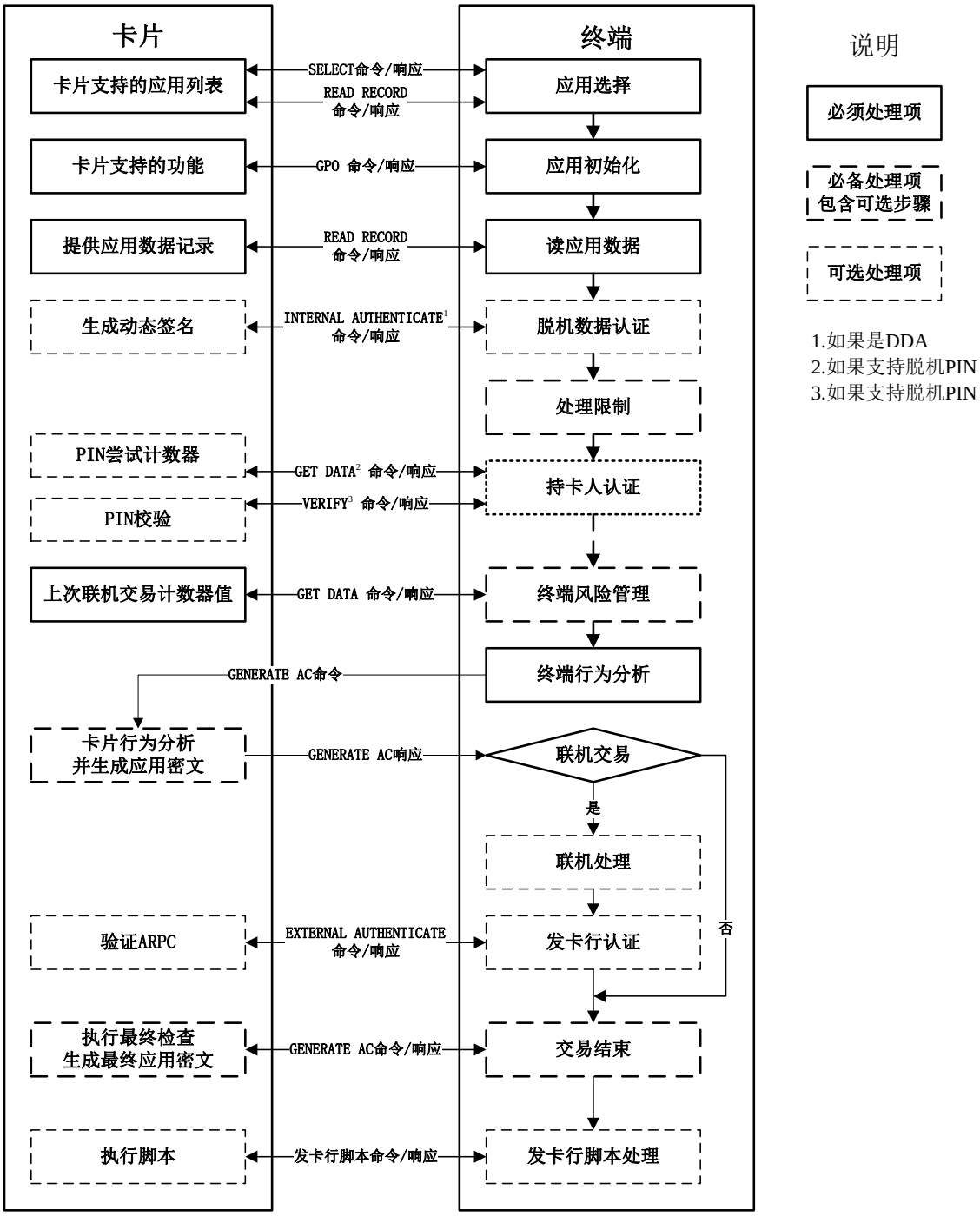


图4　交易流程实例

8.1.2　交易步骤

8.1.2.1　应用选择

8.1.2.1.1　描述

应用选择是一个过程，它决定哪个由卡片和终端共同支持的应用将被用于进行交易。这个过程分为两步骤：

——终端建立一个共同支持的应用的候选列表；

——列表中的某个应用被选择并确认用来处理交易。

8.1.2.1.2 卡片数据

同6.5应用选择要求中描述。

8.1.2.1.3 终端数据

同6.5应用选择要求中描述。

8.1.2.1.4 命令

SELECT。

终端发送选择（SELECT）命令给卡片获取卡片支持的应用信息。应用信息包括发卡机构参数，例如：选择应用的优先级别，应用名称，首选语言。命令中可以包括支付系统环境目录名称（用于目录选择方式），或者一个被请求的AID（用于AID列表选择方式）。

命令的P1参数表明应用是按照名称方式选择的。P2参数表明在支持AID后缀的情况下是否有另外使用同样AID的应用被请求（当卡片支持多应用使用同样AID的时候）。

命令可以有下列SW1 SW2返回状态字：

——9000：选择（SELECT）命令成功返回；

——6A82：在命令包含支付系统环境名称情况下，卡片不支持目录选择方式；在命令包含AID的情况下，表示选择的文件没有找到或已经是相同AID的最后一个文件而P2参数指定还有下一个相同AID的应用可选；

——6A81：卡片锁定或命令不支持；

——6283：选择文件无效。

如果卡片包括一个PDOL，PDOL作为FCI的一部分包括在选择（SELECT）命令的响应信息中。在应用初始化处理中终端将PDOL中指定的数据送入卡片。

在卡片对SELECT命令的响应中可能包含交易日志入口（Log Entry），如果出现该数据元则表示该卡片支持交易日志。

READ RECORD

终端发送READ RECORD命令到卡片，读取PPSE中的记录（如果支持目录选择）或其他AID选择方法列表中的DDF。命令包括读取文件的短文件标识（SFI）以及文件里的记录号。

卡片在响应信息中返回请求的记录内容。SW1 SW2可以有下列返回值：

——9000：成功执行；

——6A83：记录号不存在。

8.1.2.1.5 建立候选应用列表

终端通过两个途径建立共同支持应用的列表。

——目录选择方式对于终端和卡片都是可选要求。终端从卡片中读取支付系统环境文件。此文件列出卡片支持的所有支付应用。终端将卡片列表和终端列表中都有的应用加入候选列表中；

——AID 列表选择方法对于卡片和终端都是必备的。在 AID 列表选择方法中，终端对终端应用列表中包含的每个应用都向卡片发送一个 SELECT 命令。如果卡片响应表示卡也支持该应用，终端就将应用添加到候选目录中。

8.1.2.1.6 标识并选出应用

如果没有共同支持的应用，交易将被终止。如果至少有一个共同支持的应用，处理过程将如以下章条所述。

——终端决定应用

如果终端不支持持卡人选择应用或确认应用，终端会向不要求确认的具有最高优先级的应用发送一个SELECT命令。如果卡片中有超过一个应用有最高优先级，终端可以向其中任意一个发布SELECT命令。

如果用目录选择法来建立应用列表，SELECT命令的响应可能说明该应用已被锁定。如果发生此种情况，而且在可用应用列表上有更多可用的应用，终端应该向下一个优先级最高的应用发送SELECT命令。

——持卡人决定应用

a) 终端支持持卡人确认

1) 若终端不支持显示供持卡人选择的应用列表，而支持持卡人应用确认，它首先将优先级最高的应用提供给持卡人确认。如果超过一个应用有同样的优先级，终端可以根据遇到的先后次序或自行选择其中一个应用。如果持卡人确认这个选择，终端就用 SELECT 命令执行选择应用。

2) 如果持卡人不确认，终端会提供下一个优先级最高的应用，直到持卡人确认或不再有更多的可用应用为止。

3) 如果用目录选择法来建立应用列表，卡片对 SELECT 命令的响应可能说明该应用已被锁定。如果发生此种情况，而且在应用列表上有更多可用的应用，终端应该将该应用从可用应用列表中移出并选择下一个可用的应用进行持卡人确认。

b) 终端支持持卡人选择

1) 支持持卡人选择的终端将向持卡人按优先级顺序给出应用列表以供选择。如果超过一个应用有同样的优先级，终端可以按读出的顺序或自行选择一个处理。持卡人从列表中选择应用，终端用 SELECT 命令选择应用。

2) 如果用目录选择法建立应用列表，卡对 SELECT 命令的响应可能说明应用已被锁定。如果发生此种情况，而且在应用列表上有更多可用的应用，终端应该显示“重试”并显示已排除了被拒绝应用的可用应用列表。

3) 如果持卡人不选择应用，终端就终止交易。

8.1.2.1.7 流程图

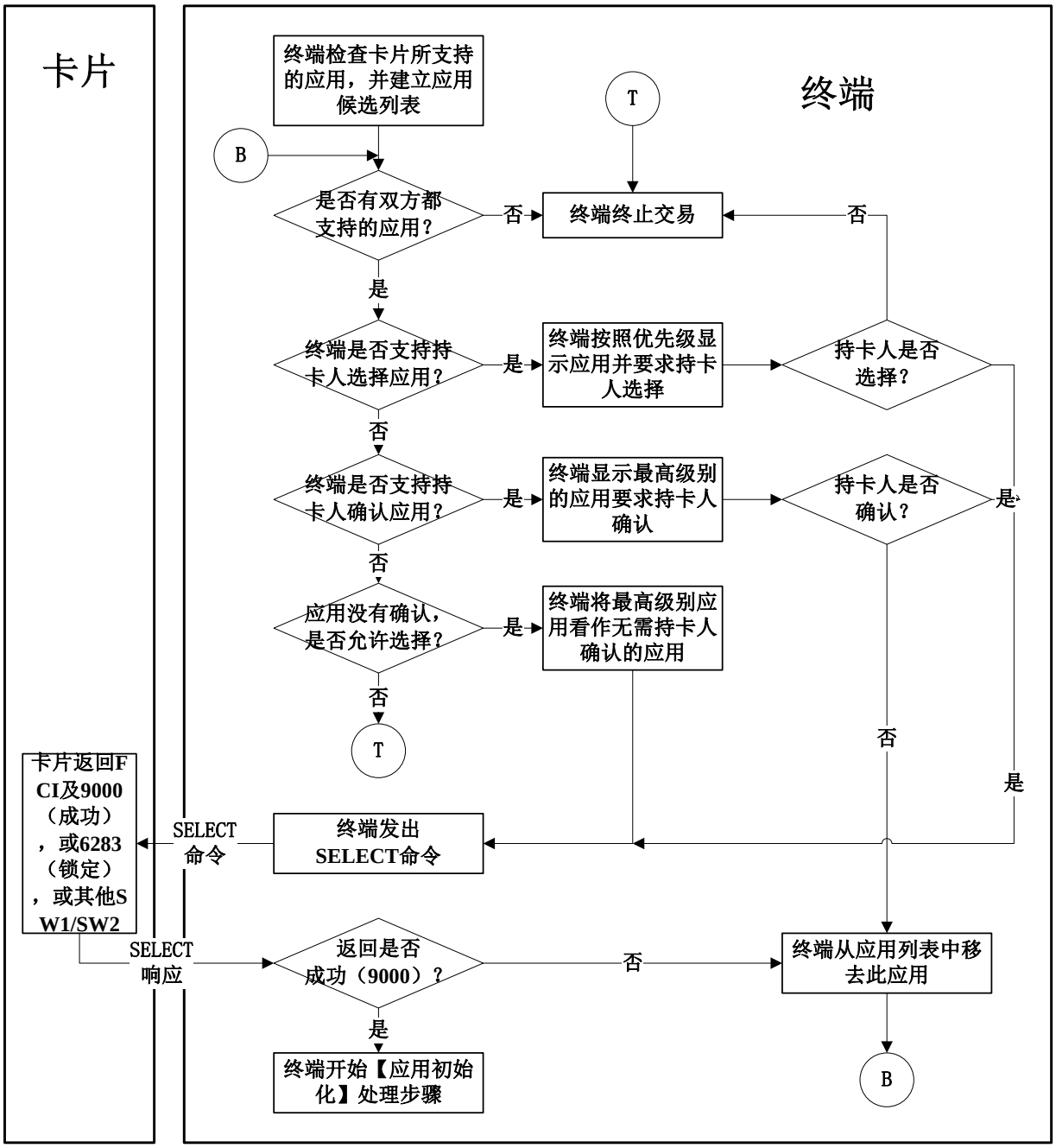


图5　应用选择处理流程图

8.1.2.1.8　后续相关处理

——初始化应用处理

终端发送获取处理选项（GPO）命令给卡片，如果在应用选择时选择（SELECT）命令的响应信息中包括PDOL，GPO命令中包括PDOL中指定的终端数据，例如交易日志记录里需要的终端数据。

如果某些限制不允许选择的应用做初始化，终端终止应用并返回应用选择步骤选择另一个应用。

——读交易明细记录

对于需要访问交易明细记录的终端，可通过发送GET DATA命令从卡片获取日志格式（Log Format）数据元，然后发送READ RECORD命令到卡片，逐条读取交易记录。

8.1.2.2　应用初始化

8.1.2.2.1 描述

本交易前提是同7.6初始应用处理要求中进入了非接触式公共交通IC卡应用流程。

在应用初始化处理中，终端向卡片发送GPO命令，表示交易处理开始。当发此命令时，终端向卡提供处理选项数据对象列表（PDOL）请求的数据元。PDOL是卡片在应用选择时提供给终端的标签和数据元长度的列表，处理选项数据对象列表（PDOL）是可选数据元。

8.1.2.2.2 卡片数据

表6 初始化应用处理—卡片数据

数据元	说明
应用文件定位器（AFL）	说明终端作交易处理要读出的卡片数据存放的文件位置和记录范围。对每个要读出的文件，AFL包括下列信息： 字节 1——短文件标识符（一个文件的数字标签） 字节 2——第 1 个要读出的记录号 字节 3——最后一个要读出的记录号 字节 4——存放用于脱机数据认证的数据的连续记录个数，字节 2 指出的是第 1 条要读的记录号
应用交互特征（AIP）	指示在此应用中卡片支持特定功能的能力列表，包括静态数据认证（SDA）、动态数据认证（标准DDA）、持卡人验证、发卡机构认证以及复合动态数据认证（DDA/AC）。 AIP 在个人化时应被写入卡中用来指明支持终端风险管理和持卡人验证
应用交易计数器（ATC）	应用个人化后，卡片应用交易计数器启动
卡片验证结果（CVR）	专用数据，表明从卡片角度来看本次和前次交易的脱机处理结果。数据存放在卡片中，作为发卡机构应用数据的一部分联机上送
文件控制信息（FCI）	FCI 是卡片相关应用的信息，在终端发送的 SELECT 命令的响应中。
密文信息数据（CID）	指明卡片返回的密文类型和终端需要进行的后续处理行为。在应用初始化处理时被初始为全 0
处理选项数据对象列表（PDOL）	PDOL 是卡片请求的终端数据元的标签和长度的可选列表。它是终端在 SELECT 命令响应中得到的卡片 FCI 的一部分。终端在 GPO 命令中向卡片提供该列表所请求的数据元。

8.1.2.2.3 终端数据

终端将卡片需要的数据元通过PDOL传送给卡片。

8.1.2.2.4 命令

——GPO

终端使用获取处理选项（GPO）命令通知卡片交易开始。

命令中包含卡片在PDOL中列出的终端数据元的值部分，PDOL是卡片在应用选择阶段返回的可选数据。

卡片响应数据内容为AIP和AFL。AIP列出了交易在处理过程中执行的功能；AFL列出交易需要的数据存放的短文件标识符、记录号、记录个数以及脱机数据认证需要数据的存放位置。

对应用初始化，终端：

a) 从 SELECT 命令响应中的文件控制信息（FCI）中提取处理选项数据对象列表（若存在）。
b) 向卡片发送 GPO 命令。在这个命令中，终端组织所有卡片在 PDOL 中请求的数据元并传递给卡片。

终端对卡片GPO命令响应进行如下处理：

a) 接收卡片对 GPO 命令的响应

b) 如果卡片响应为“使用条件不满足”，终端：

1) 将该应用从可用应用列表里删除；

2) 返回应用选择。

c) 如果卡片用 AIP 和 AFL 做出响应，终端开始读取应用数据。

8.1.2.2.5 流程图

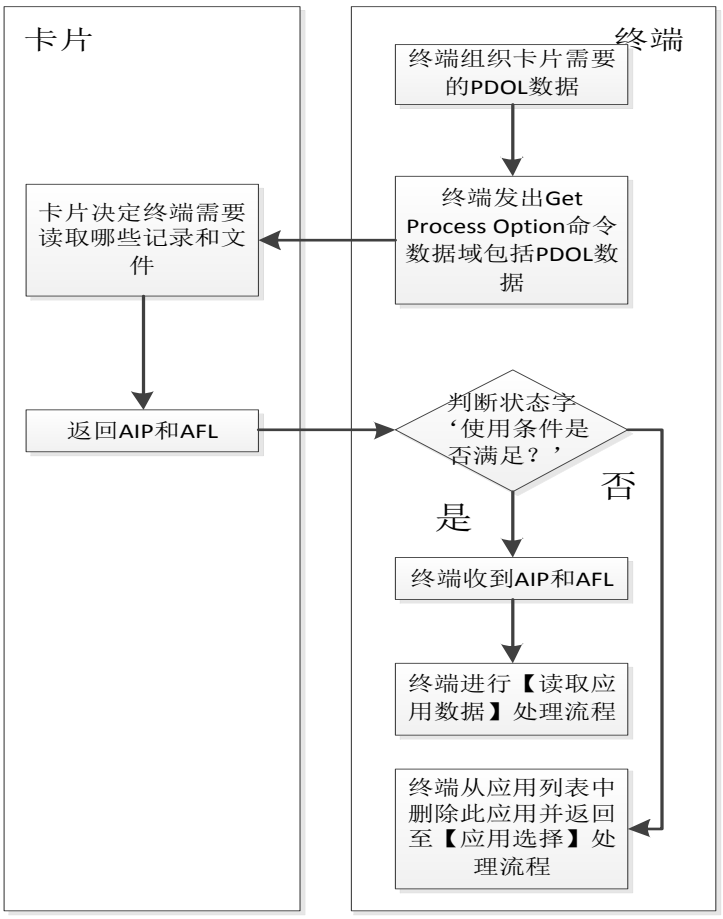


图6 应用初始化处理流程图

8.1.2.2.6 前期相关处理

——应用选择

卡片在SELECT命令响应中将PDOL（若存在）作为FCI的一部分提供给终端。

8.1.2.2.7 后续相关处理

——读取应用数据

终端使用GPO命令响应中由卡片提供的AFL，来确定从卡片读取哪些应用数据以及哪些应用数据将要用到脱机数据认证中。

——脱机数据认证

终端使用GPO命令响应中由卡片提供的AIP，来确定卡片是否支持脱机数据认证的类型。

——持卡人验证

终端使用GPO命令响应中由卡片提供的AIP，来确定卡片是否支持持卡人验证。

——联机处理

终端使用GPO命令响应中由卡片提供的AIP，来确定卡片是否支持发卡机构认证。

8.1.2.3 读应用数据

8.1.2.3.1 描述

读取应用数据时，终端读取交易处理中必要的卡片数据，并决定动态数据认证（DDA）中使用的数据。

8.1.2.3.2 卡片数据

表7 读应用数据—卡片数据

数据元	说明
应用文件定位器（AFL）	指示包含终端将要读取的用来交易处理的卡片数据的文件和记录范围。 每个条目指定了要从文件读取的最初记录和最终记录号以及哪些记录要用在脱机数据认证中。

表8 读应用数据—卡片文件

数据元	说明
应用基本文件（AEF）	卡片数据文件，包括应用处理使用的数据。一个 AEF 包括一系列用记录号标识的记录。每个 AEF 用 SFI 唯一标识。终端使用读记录（READ RECORD）命令读取记录内容，命令中包括 SFI 和记录号。
短文件标识符（SFI）	SFI 是用来唯一标识应用定义文件的符号。在 AFL 里列出，终端用它来标识要读取的文件。

表9列出了读记录时，公共交通IC卡中应具备的数据对象。本部分中定义的其它公共交通IC卡数据对象都是可选的。

表9 读应用数据—卡片必备数据对象

标签	值	存在性
‘5F24’	应用失效日期	必备
‘5A’	应用主账号	必备
‘8C’	卡片风险管理数据对象列表 1	必备
‘8D’	卡片风险管理数据对象列表 2	必备

8.1.2.3.3 终端数据

读取应用数据功能中不使用终端数据。

8.1.2.3.4 命令

——READ RECORD

终端为每个要读取的记录向卡片发送一条READ RECORD命令给卡片。此命令包括标识文件的一个短文件标识符（SFI）以及一个记录号来标识文件里的记录。

卡片在READ RECORD命令的响应提供被请求的记录。

8.1.2.3.5 处理流程

终端根据卡片的应用文件定位器（AFL）决定从卡片读取哪些记录。

对于每个AFL条目，终端用READ RECORD命令请求读取首条指定的记录。当此记录从卡返回，终端就为随后的处理保留该数据对象。如果AFL条目指明脱机数据认证时对静态数据的认证需要此记录，终端将记录数据放入静态数据认证输入列表。终端继续读取文件记录直到最后一条指定要读取的记录为止。

8.1.2.3.6 流程图

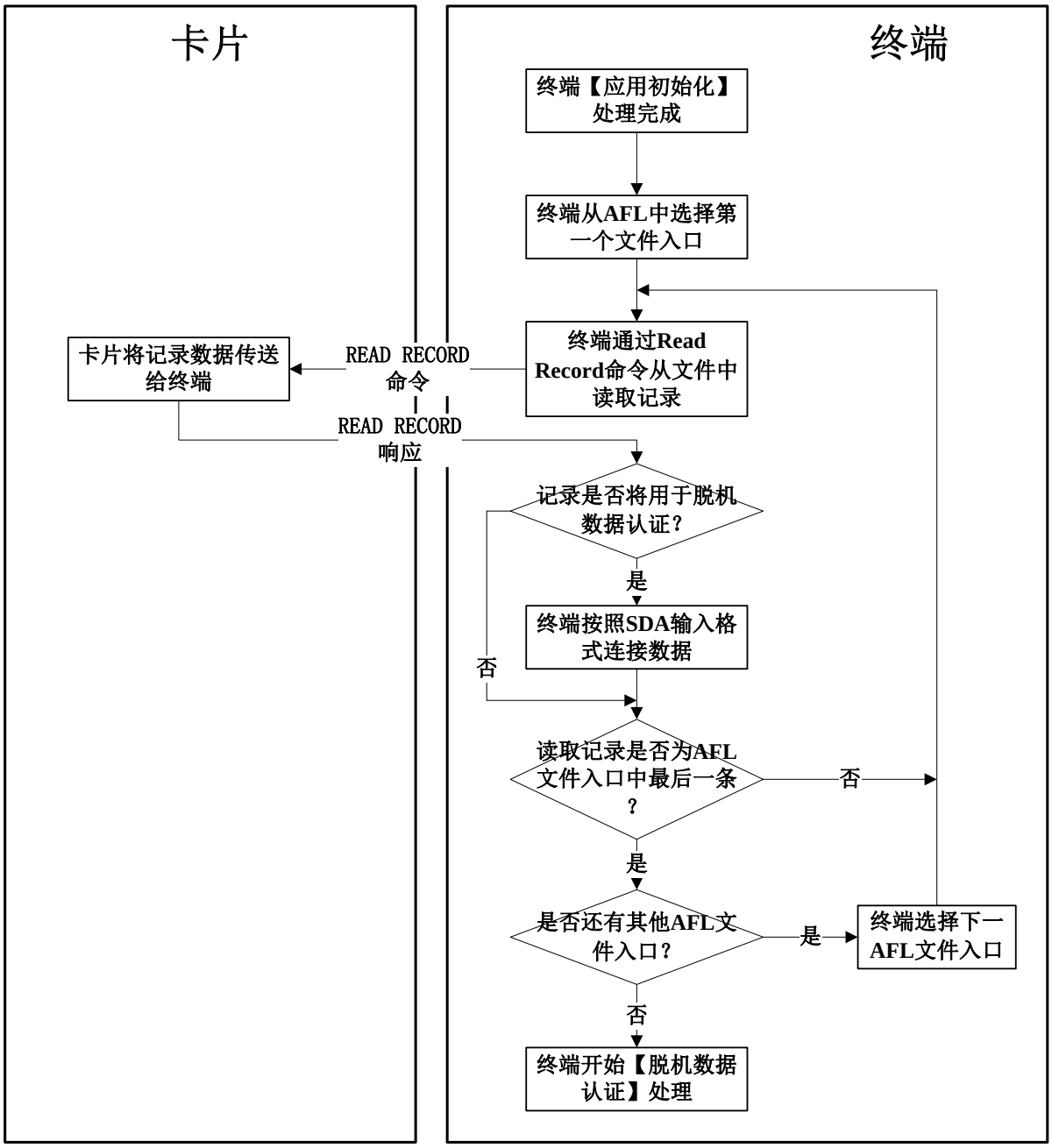


图7 读应用数据处理流程图

8.1.2.3.7 前期相关处理

终端使用应用初始化时卡片提供的AFL，以读取应用数据。

8.1.2.3.8 后续相关处理

——脱机数据认证

终端使用在读应用数据处理中建立的一个DDA中使用的IC卡公钥验证。

——其他功能

其他功能用读取应用数据时得到的数据进行处理。

8.1.2.4 脱机数据认证

8.1.2.4.1 描述

脱机数据认证是终端使用非对称公钥技术认证来自卡片数据的处理过程。

在动态数据认证（DDA）处理中，终端不仅认证静态的卡数据，也认证卡片使用能够唯一标识一笔交易的交易数据生成的签名。动态数据认证除了确保发卡机构选择的卡片数据元自卡片个人化以来没有受到改变，还确认卡片是否属于伪卡（非法复制）。

脱机数据认证结果决定了卡片和终端是脱机批准交易、进行联机认证还是脱机拒绝交易。联机认证系统在它们的认证响应决定中可以使用脱机数据认证结果。

所有脱机交易的终端应支持动态数据认证（DDA），复合动态数据认证CDA可选支持。

8.1.2.4.2 密钥及认证

密钥及认证见JT/T XXX.2。

8.1.2.4.3 确定脱机数据认证的方法

任何交易只执行一种脱机数据认证方法，复合动态数据认证/应用密文生成优先权最高，标准动态数据认证其次。表10表明了根据卡片和终端的共同支持情况决定所要执行的脱机数据认证方法。

表10 脱机数据认证处理优先权

卡应用交互特征（AIP）表明卡支持	标准动态数据认证（DDA）	标准动态数据认证（DDA）及复合动态数据认证/应用密文生成（CDA）
标准动态数据认证	标准动态数据认证	标准动态数据认证
标准动态数据认证 复合 DDA/应用密文生成	标准动态数据认证	复合动态数据认证/应用密文生成

8.1.2.4.4 动态数据认证

如果要执行脱机动态数据认证，终端用发卡机构公钥和认证中心公钥验证卡片的静态数据，处理过程和静态数据认证相似。验证了静态数据后，终端向卡片申请动态签名。这要求使用内部认证命令实现标准动态数据认证以及使用第一个AC生成命令实现复合动态数据认证/应用密文生成。

卡片用公共交通IC卡私钥对终端随机数和来自卡片的动态数据进行签名，生成一个数字签名，叫做签名动态应用数据。用复合动态数据认证/应用密文生成方法产生的签名数据包括应用密文。卡片把这个动态签名发送给终端。

终端用已从公共交通IC卡公钥证书中恢复的公共交通IC卡公钥将卡片的签名解密。恢复的数据被用来与实际的数据比较来确定动态数据认证是否通过。成功的动态数据认证意味着卡片数据没有被改变且不是伪卡。

——动态数据认证处理的数据元

终端将用表11中描述的附加动态数据认证数据进行动态数据认证。

表11 动态数据认证中使用的终端数据

数据元	说明
缺省动态数据认证数据对象列表（缺省 DDOL）	如果卡片不提供动态数据认证数据对象列表，则终端使用缺省的动态数据认证数据对象列表，该列表包含终端不可预知数字的标签。
不可预知数字	由终端生成的不可预知的、唯一标识一笔交易的数字，该数字通过内部认证命令发送到卡片。

表12中描述的数据也用于动态数据认证。

表12 动态数据认证中使用的卡片数据

数据元	说明
动态数据认证失败指示器	内部指示器，如果标准动态数据认证失败且交易被脱机拒绝，则它由卡片设置并保存。
动态数据认证数据对象列表（DDOL）	动态数据认证处理中，要传递给卡片的终端数据对象的标签列表。
公共交通 IC 卡动态数字	卡片生成的唯一数字，并作为复合动态数据认证/应用密文生成中动态签名的部分由终端验证。
公共交通 IC 卡私钥	卡片用它生成动态签名。
公共交通 IC 卡公钥证书	公共交通 IC 卡公钥证书包含用发卡机构私钥签名的公共交通 IC 卡公钥。
公共交通 IC 卡公钥指数	在非对称算法中使用该指数来恢复签名动态应用数据。
公共交通 IC 卡公钥余项	如果有必要，公共交通 IC 卡公钥余项包含公共交通 IC 卡公钥未列入公共交通 IC 卡公钥证书的部分。

所有在标准动态数据认证中使用的数据元，除动态数据认证数据对象列表以外，都用于复合动态数据认证/应用密文生成。此外，表13中描述的数据也被使用。

表13 复合动态数据认证/应用密文生成中使用的卡片数据

数据元	说明
应用密文	卡片在 GENERATE AC 命令响应里返回的加密密文。如果复合动态数据认证/应用密文生成在 ARQC 或 TC 中返回，ARQC 或 TC 是动态签名验证的一部分。
密文信息数据	卡片提供密文类型信息，终端在复合动态数据认证/应用密文生成中验证。

——标准动态数据认证处理流程

这个处理过程，除了动态签名由卡片生成以外，其他都是由终端执行的。以下概述了这个处理过程。

1） 认证中心公钥的获取

终端用认证中心公钥索引（PKI）以及卡中的注册的应用提供商标识来获取储存在终端中的认证中心公钥以及相关信息。

2） 发卡机构公钥的获取

终端用认证中心公钥从发卡机构公钥证书中将发卡机构公钥恢复。发卡机构公钥证书的格式是经过验证的。

3） 公共交通 IC 卡公钥的获取

终端用发卡机构公钥解密包含公共交通IC卡公钥和静态应用数据哈希值的公共交通IC卡公钥证书。终端把此哈希值与被恢复数据的哈希值相比较来验证它。如果这些哈希值不相等，则动态数据认证失败。

4） 动态签名生成（仅标准动态数据认证）

终端传送包括动态随机数的INTERNAL AUTHENTICATE命令到卡。

一收到INTERNAL AUTHENTICATE命令，卡片使用公共交通IC卡私钥加密终端、卡片动态数据的哈希值来生成一个动态签名。卡片再把此动态签名传递给终端。

5） 动态签名校验（仅标准动态数据认证）

终端用从公共交通IC卡公钥证书恢复的公共交通IC卡公钥并解密动态签名。如果终端生成的实际动态数据哈希值与恢复的哈希值不一致，则动态数据认证失败。

8.1.2.4.5 处理流程

对于复合动态数据认证/应用密文生成，终端执行标准动态数据认证的步骤a)到c)。终端要求使用第一个GENERATE AC命令生成的动态密文。不使用INTERNAL AUTHENTICATE命令。对此密文的要求和认证包括以下步骤：

——动态签名生成（仅复合动态数据认证/应用密文生成）

终端行为分析中，如果终端要求一个联机密文（授权请求密文）或脱机批准密文（交易证书），第一个GENERATE AC命令表明复合动态数据认证/应用密文生成即将被执行。如果卡片决定的应用密文是一个交易证书或授权请求密文，卡片就用公共交通IC卡私钥签名应用密文及相关数据，并在GENERATE AC命令响应中把动态签名返回给终端。

——动态签名校验（仅复合动态数据认证/应用密文生成）

卡片行为分析中，如果最初的GENERATE AC响应包含一个交易证书或授权请求密文，终端使用恢复公共交通IC卡公钥将动态签名解密。如果签名成功地恢复了，处理就根据所收到的密文的类型继续下去。如果签名恢复失败，则交易就脱机拒绝。

8.1.2.4.6 流程图

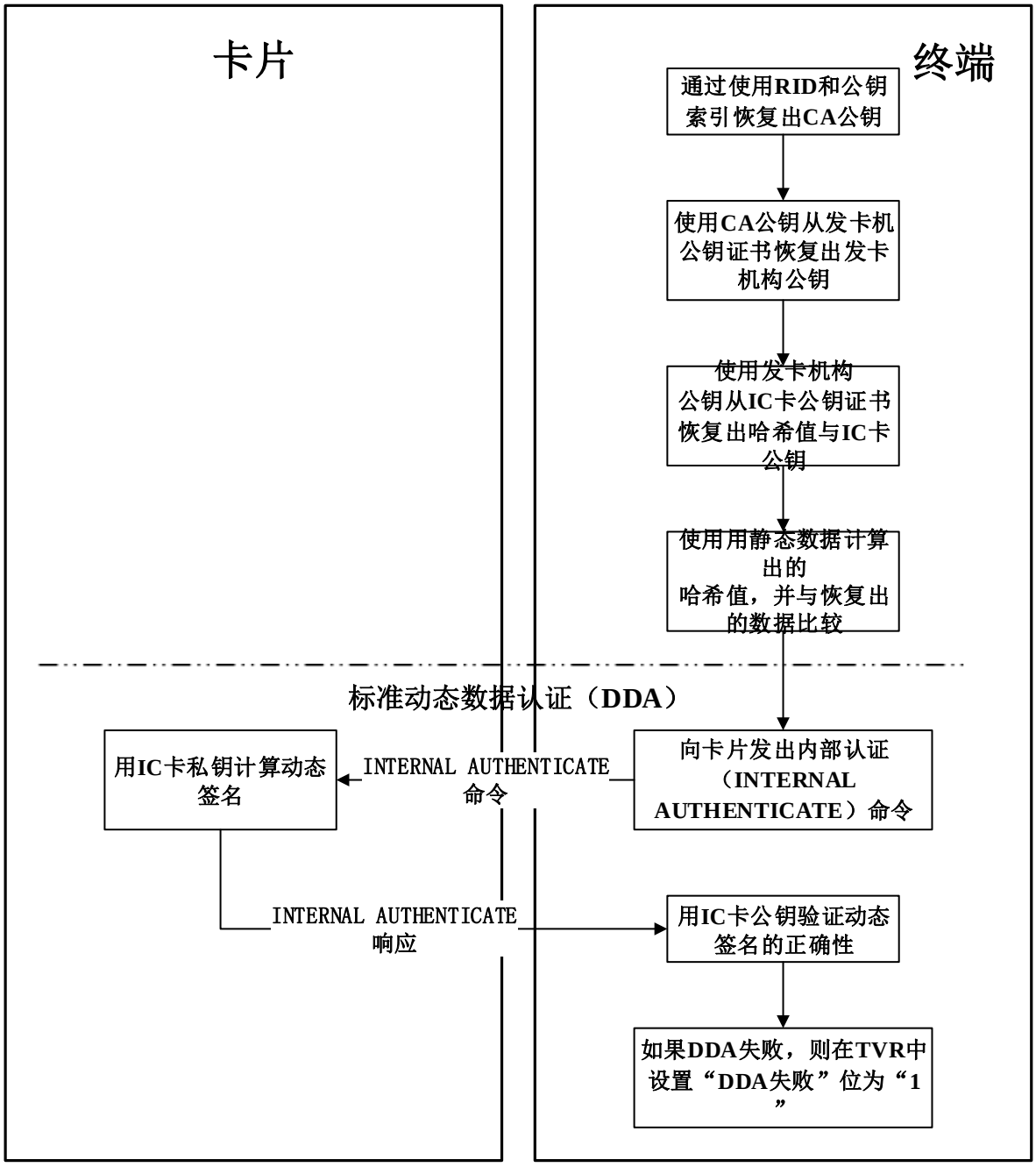


图8　脱机数据认证处理流程图

8.1.2.4.7　前期相关处理

——读取应用数据

终端从卡片读取应用数据，此数据包括为支持脱机数据认证方法所要求的数据。应用文件定位器和动态数据认证中认证公共交通IC卡公钥证书的数据。

8.1.2.4.8　后续相关处理

——终端行为分析

终端用脱机数据认证结果，卡片和终端参数来决定交易是否要被脱机拒绝，还是进行联机认证，或脱机批准。当要执行复合动态数据认证/应用密文生成且交易要被发送联机或脱机批准时，终端在GENERATE AC命令里设置了复合动态数据认证/应用密文生成指示器。

——卡片行为分析

如果上笔交易动态数据认证失败且交易被脱机拒绝，卡片也在CVR设置一个类似的指示器。

如果动态数据认证失败了，且要脱机拒绝交易，就动态数据认证失败指示器。

复合动态数据认证/应用密文生成。

如果从终端收到GENERATE AC命令表明将要执行复合动态数据认证/应用密文生成，卡片就返回授权请求密文和交易证书应用密文，该密文用公共交通IC卡私钥签名。

——联机处理

复合动态数据认证/应用密文生成。

当返回的应用密文是动态签名，终端用公共交通IC卡公钥解密此签名。如果解密成功，终端就根据应用密文把处理继续下去。如果解密失败，则交易就脱机拒绝。

——交易结束

联机认证后，卡片允许根据发卡机构认证选项和结果来重设动态数据认证失败指示器。

如果动态数据认证失败了，且因联机认证不能完成，交易要被脱机拒绝，就设置动态数据认证失败指示器。

——复合动态数据认证/应用密文生成

如果复合动态数据认证/应用密文生成失败且返回的应用密文是ARQC，则终端发送第二个GENERATE AC命令请求AAC。如果复合动态数据认证/应用密文生成失败且返回的应用密文是TC，则交易被脱机拒绝并不要求第二个GENERATE AC命令了。

8.1.2.5 处理限制

8.1.2.5.1 描述

终端使用终端和卡片的数据元执行处理限制功能，终端应支持对应用版本、生效日期和失效日期以及交易点条件的有关检查。

8.1.2.5.2 卡片数据

表14列出并描述了处理限制中用到的卡数据元。

表14 处理限制—卡片数据

数据元	说明
应用版本号	该数据元（标签”9F08”）显示了卡片的应用版本。终端将其用于应用版本号的检查。
应用用途控制（AUC）	AUC 是可选数据元，它表明了发卡机构有关卡片应用在地域以及所允许的服务方面的所有限制，由终端用于应用用途控制检查。
发卡机构国家代码	发卡机构国家代码是本部分的数据元，表明发卡的国家，由终端用于应用用途控制检查。
应用生效日期	应用生效日期是应用开始使用的日期。
应用失效日期	应用失效日期过后，应用即被禁止。

8.1.2.5.3 终端数据

表15列出并描述了处理限制中用到的终端数据元。

表15 处理限制—终端数据

数据元	说明
应用版本号	该数据元（终端标签”9F09”）表明了终端的应用版本，它被终端用于应用版本号的检查，遵循此规范的卡应用版本号待定。
终端性能	表明终端关于卡片数据输入，持卡人验证和安全的性能。由终端用于应用用途控制的检查。
终端国家代码	该数据元表明终端所在的国家，由终端用于应用用途控制检查。
交易日期	这是终端提供的交易发生的当地日期，由终端用于应用生效期和失效日期检查。
交易类型	该数据元表明交易的类型，由终端用于应用用途控制检查。

8.1.2.5.4 应用版本号检查

终端把卡片的应用版本号和终端的应用版本号相比较，看它们是否相同。如果不相同，终端在终端验证结果（TVR）里显示出应用版本不一致。

8.1.2.5.5 应用用途控制检查

在应用用途控制处理中，终端检查交易发生地的不同情况，决定交易是否继续进行。如果在读应用数据步骤中终端读取到应用用途控制（AUC）和发卡机构国家代码数据，终端检查下列应用限制:

步骤1：国内和国际检查：

——国内

终端比较发卡机构国家代码和终端国家代码。如果相同，认为是国内交易。如果是国内交易，AUC中对应的国内交易类型指示位应为“1”表明请求的服务允许进行。

示例：如果是一个现金交易，AUC中“国内现金交易有效”指示位应为“1”。

——国际

如果国家代码不同，认为是国际交易。如果是国际交易，AUC中对应的国际交易类型指示位应为“1”表明请求的服务允许进行。

示例：如果是一个现金交易，AUC中“国际现金交易有效”指示位应为“1”。

如果上述任何终端执行的检查失败，终端在TVR中标明“卡片产品不允许请求的服务”。

8.1.2.5.6 有效期检查

——应用生效日期检查

应用生效日期检查通过验证卡片的应用生效日期（如果存在）早于等于终端的当前交易日期，确认应用已经生效。如果生效日期晚于交易日期，终端就在终端验证结果中指示应用还未生效。

——应用失效日期检查

应用失效日期检查是必备的。检查确保应用没有过期。如果应用失效日期小于交易日期，终端要在TVR中标明应用已经过期。

8.1.2.5.7 流程图

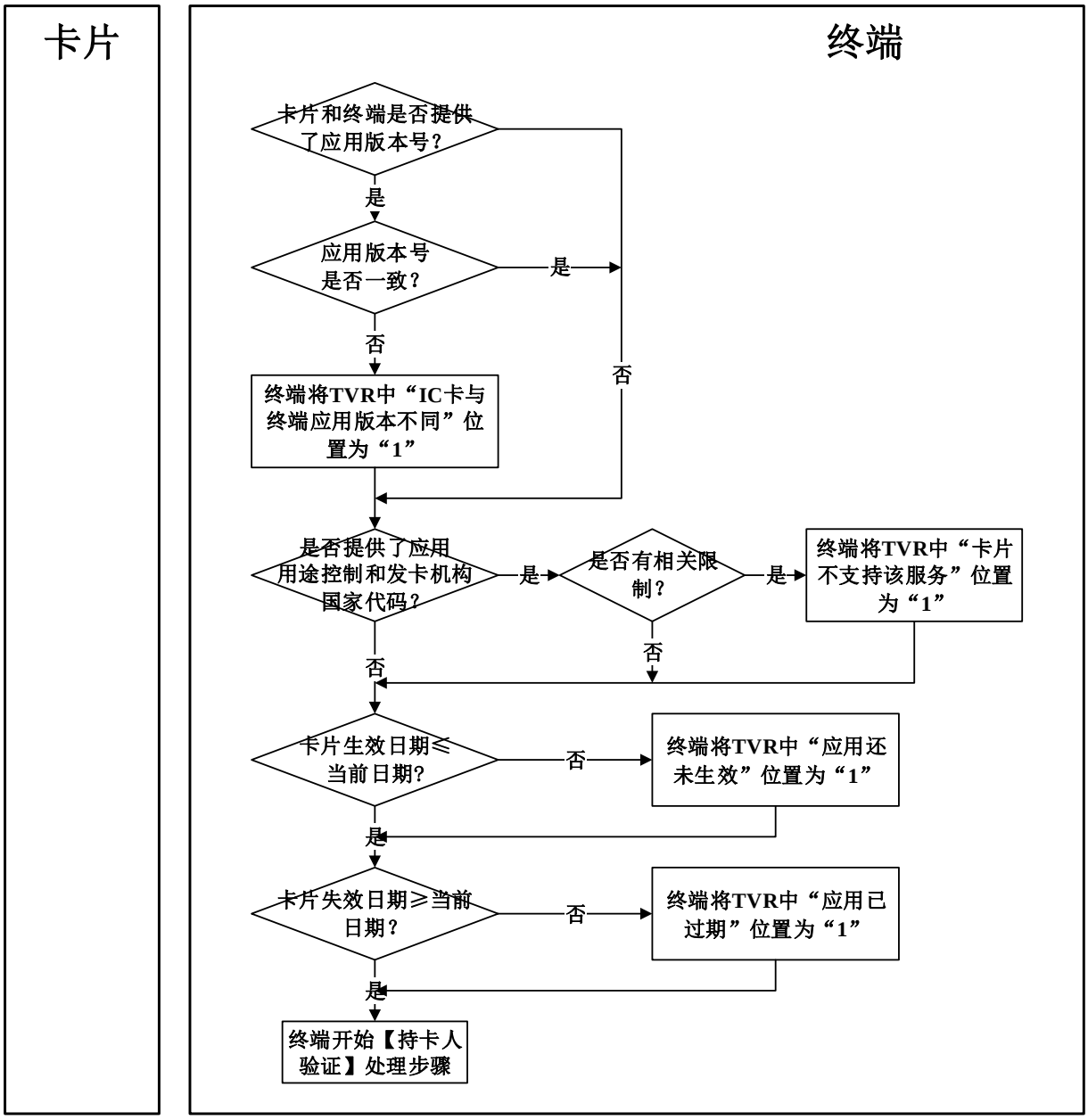


图9　处理限制流程图

8.1.2.5.8　前期相关处理

——读取应用数据

终端使用READ RECORD命令获得应用版本号以及卡片的应用失效日期。如果存在，应用用途控制、发卡机构国家代码和应用生效日期，则它们也被从卡中读取出来。

8.1.2.5.9　后续相关处理

——终端行为分析

终端行为分析中，终端检查发卡机构行为代码和终端行为代码以决定如果应用版本不一致、卡未生效或卡已失效、或卡不支持所请求的服务时，应采取怎样的处理。

8.1.2.6　持卡人验证

持卡人验证功能为可选项。

8.1.2.6.1 描述

持卡人验证用来确保持卡人是合法的，卡片不是丢失的或被盗的。

在持卡人验证处理中，终端决定要使用的持卡人验证方法（CVM）并执行选定的持卡人验证。CVM处理允许增加其它持卡人验证方法，例如生物识别等。如果使用脱机PIN方式，卡片要验证卡片内部的脱机PIN。脱机PIN验证结果包括在联机授权信息中，发卡机构作授权决定的时候要考虑其验证结果。

支持的持卡人验证方法有：

——脱机明文 PIN 验证；

——联机 PIN 验证；

——签名；

——CVM 失败；

——无需 CVM；

——签名与脱机明文 PIN 验证组合；

——身份证件验证。

签名、身份证件验证可以和脱机PIN验证方式结合起来。持卡人验证方法处理被设计为可支持附加的持卡人验证，比如被采用的生物识别技术。用脱机PIN方式在卡片内部完成了PIN的确认。脱机PIN验证结果包括在联机授权报文中，在发卡机构的授权决定里应予以考虑。

8.1.2.6.2 卡片数据

终端将表16和表17中描述的卡片数据用于持卡人验证方法列表处理。

表16 持卡人验证方法列表处理—卡片数据

数据元	说明
应用交互特征（AIP）	包含一个指示器，标明卡片是否支持持卡人验证。此指示器应设置为“1”。
持卡人验证方法（CVM）列表	卡片应用持卡人验证方法列表先后顺序。卡片可以包含多种的持卡人验证方法列表以用于不同的环境，比如国际和国内交易。持卡人验证方法列表包含以下部分： ——金额 X—可能在持卡人验证方法使用条件中用到的金额； ——金额 Y—可能在持卡人验证方法用法条件中用到的第二个金额。 持卡人验证方法条目—持卡人验证方法列表可能包括不止一个条目，每个条目包含以下子域： ——持卡人验证方法代码子域：如果持卡人验证失败，即指定要采取的行动。可以选择处理下一个持卡人验证方法或中止持卡人验证处理。 ——持卡人验证方法类型子域：持卡人验证方法要执行的类型，例如脱机 PIN 验证。 ——持卡人验证方法条件子域：当要用到持卡人验证方法条目时的条件，例如，如果终端支持该持卡人验证方法类型（脱机 PIN）。

表17 脱机 PIN 验证处理—卡片数据

数据元	说明
应用缺省行为（ADA）	如果脱机 PIN 重试次数超限，卡片用该数据元来决定要采取怎样的行动。
卡片验证结果（CVR）	包含卡片为下列情况设置的指示器： ——执行了脱机 PIN 验证； ——脱机 PIN 验证失败； ——PIN 重试次数超限； ——因 PIN 重试次数超限，应用锁定。
PIN 重试次数计数器	剩余的脱机 PIN 重试次数。每次持卡人脱机 PIN 验证失败时，PIN 重试次数计数器都减 1。如果持卡人输入与存储在卡中参考 PIN 一致的 PIN 或重置 PIN 重试次数计数器的脚本命令执行成功，PIN 重试次数计数器被重置为 PIN 重试次数上限。卡片使用取数据（GET DATA）命令返回 PIN 尝试计数器（可选）。在验证命令中返回给终端。
PIN 重试次数上限	针对某一应用，发卡机构指定的所能允许的连续输入错误 PIN 的最大次数。
参考 PIN	持卡人 PIN，储存在卡片的安全位置。
持卡人证件号	用于证件验证
持卡人证件类型	用于标识证件类型

8.1.2.6.3 终端数据

表18中描述的终端数据用于持卡人验证处理。

表18 持卡人验证处理—终端数据

数据元	说明
加密个人识别码（PIN）数据	在密码键盘加密交易 PIN 用于联机验证。
密码键盘保密密钥	密码键盘使用加密输入的脱机 PIN 的保密密钥，且读卡器用此密钥来给加密 PIN 解密。当密码键盘和读卡器没有集成为一个不受外界干预的一体设备，这个密钥是必需的。此密钥和用于脱机加密 PIN 的密钥不同。
终端性能	标明了终端支持的持卡人验证方法。
终端验证结果（TVR）	在终端验证结果里为下列情况设置指示器： 持卡人验证不成功； 不可识别的持卡人验证方法； PIN 输入次数超限； 需要 PIN 输入而没有密码键盘或密码键盘不能工作； 需要 PIN 输入，有密码键盘但 PIN 没有输入； 输入联机 PIN。
交易个人识别码（PIN）	包含持卡人为 PIN 验证输入的数据。

8.1.2.6.4 命令

以下命令用于脱机PIN处理：

——GET DATA

终端用这条命令从卡片获取PIN重试计数器以便决定在先前的交易中PIN输入次数是否超限，或接近超限。可选。

如果卡片不支持用取数据（GET DATA）命令返回PIN尝试计数器，卡片返回“6A88”；

——VERIFY

用于脱机明文PIN验证。

VERIFY命令包括持卡人输入的PIN并开始卡片对这个PIN与储存在卡上的参考PIN的比较。

如果卡片和终端支持脱机PIN处理，则它们支持VERIFY命令。

卡片的响应指出下列情况中的一种，命令的响应状态字SW1 SW2可能有如下返回值：

1) “9000”验证成功；
2) “63Cx”PIN 不匹配，“x”表明剩余的次数；
3) “6984”当在上次交易中尝试次数限制数已经超过，本次交易第 1 次处理验证（VERIFY）命令时返回。
4) “6983”当在本次交易中尝试次数限制数超过，卡片再次收到验证（VERIFY）命令时返回。

8.1.2.6.5 处理流程

持卡人验证处理分成两部分，为卡片的持卡人验证方法列表处理与执行持卡人验证。

——持卡人验证方法列表处理

卡片在持卡人验证方法列表处理中，提供给终端持卡人验证方法列表以及其他必需数据。

终端执行下列步骤：

a)决定是否执行持卡人验证—如果卡片支持持卡人验证（如应用交互特征所说明），且读取应用数据时，卡片提供一个持卡人验证方法列表，那么终端就继续持卡人验证。反之，终端就进行终端风险管理。

b)处理持卡人验证列表条目—由持卡人验证方法列表中的第一个条目开始，终端执行以下行为：

1) 检查持卡人验证条件是否符合。如果不符合，终端进行下一个持卡人验证方法列表条目。
2) 如果持卡人验证条件符合，终端将进一步检查此 CVM 代码是否可以识别。
   如果可以识别，终端判断是否支持此 CVM，如果支持，则进入步骤 4）；如果终端不支持此 CVM 代码，则进行判断，此 CVM 是否和 PIN 验证相关，如果为 PIN 验证则终端设置 TVR “要求输入 PIN，但密码键盘不存在或不工作”位为 1，进入步骤 3）。
   如果此 CVM 代码无法被终端识别，终端将在 TVR 中设置“未识别 CVM”位为 1，进入步骤 3）。
3) 终端检查 CVM 代码 bit7 位。如果为 1，则继续处理下一个 CVM 条目；如果 CVM 列表中无未处理的 CVM 条目，则持卡人验证失败，终端结束持卡人验证。如果为 0，则持卡人验证失败，终端设置持卡人验证不成功标志为“1”，结束持卡人验证。
4) 执行指定的持卡人验证方法。如果持卡人验证不成功（例如脱机 PIN 验证失败），终端进入步骤 3）。如果持卡人验证成功，终端进行终端风险管理。

c)如果终端到达了持卡人验证方法列表的末端还没有一个成功的持卡人验证，则持卡人验证处理失败—终端在终端验证结果里设置持卡人验证不成功标志“1”并进行终端风险管理。

——持卡人验证处理

a) 联机 PIN 验证

在联机PIN验证处理过程中，输入后的PIN被加密，并包含在联机授权报文里，由发卡机构的联机系统加以验证。

联机PIN处理流程不在本部分中描述。

b) 签名

当选择签名作为持卡人验证方法时，终端打印一张附有给持卡人签名档的收据。

c) 无需 CVM

当持卡人验证方法是“无需CVM”时，持卡人验证成功。

d) 持卡人验证失败

当持卡人验证方法是“持卡人验证失败”时，认为持卡人验证处理失败。

e） 持卡人证件验证

终端提示持卡人出示身份证件，并将卡片中得到的证件类型和证件号码显示给服务员，进行持卡人身份比对验证。

图11和图12概述了PIN验证处理流程。

8.1.2.6.6 流程图

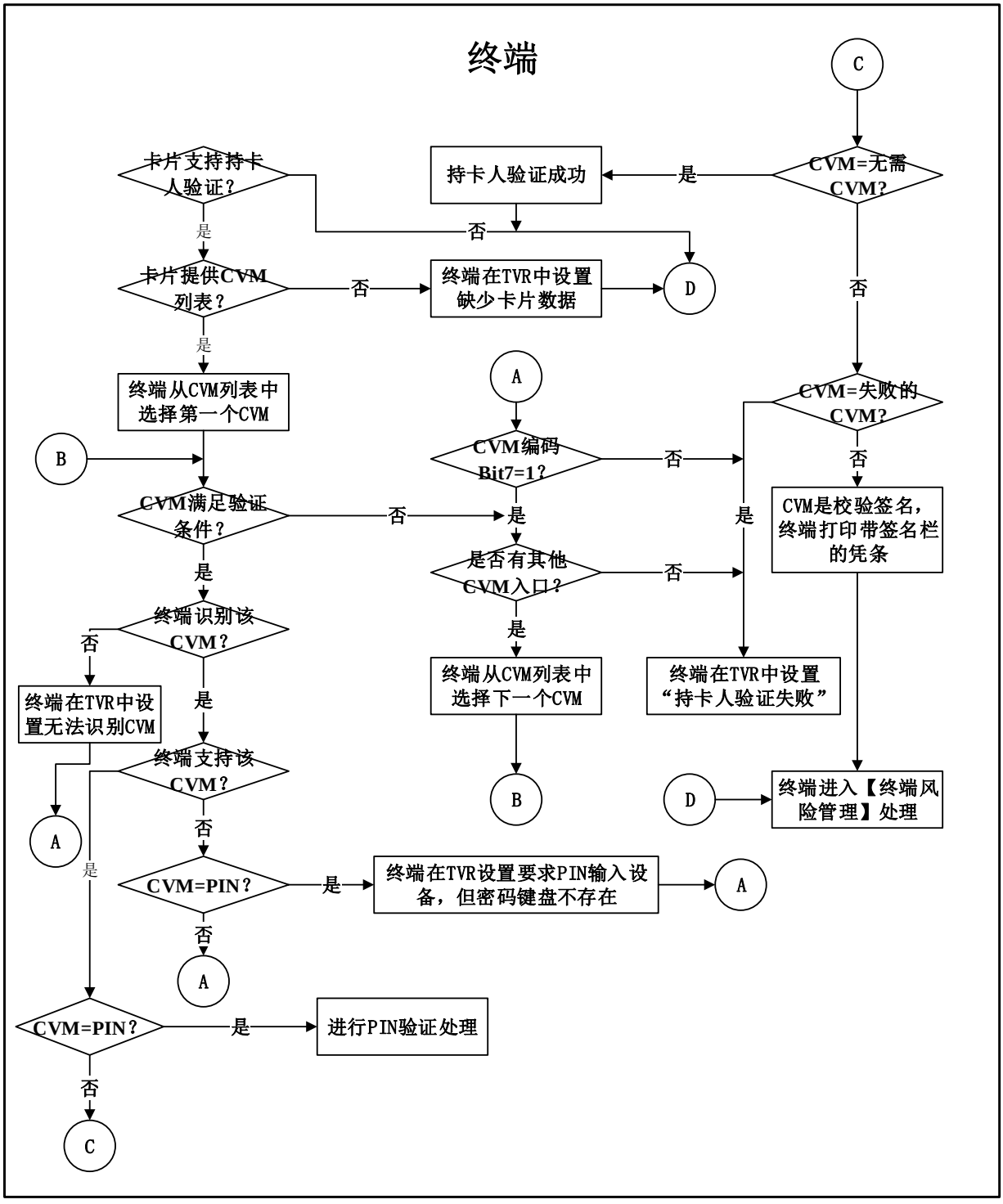


图10 持卡人验证方法列表处理流程图

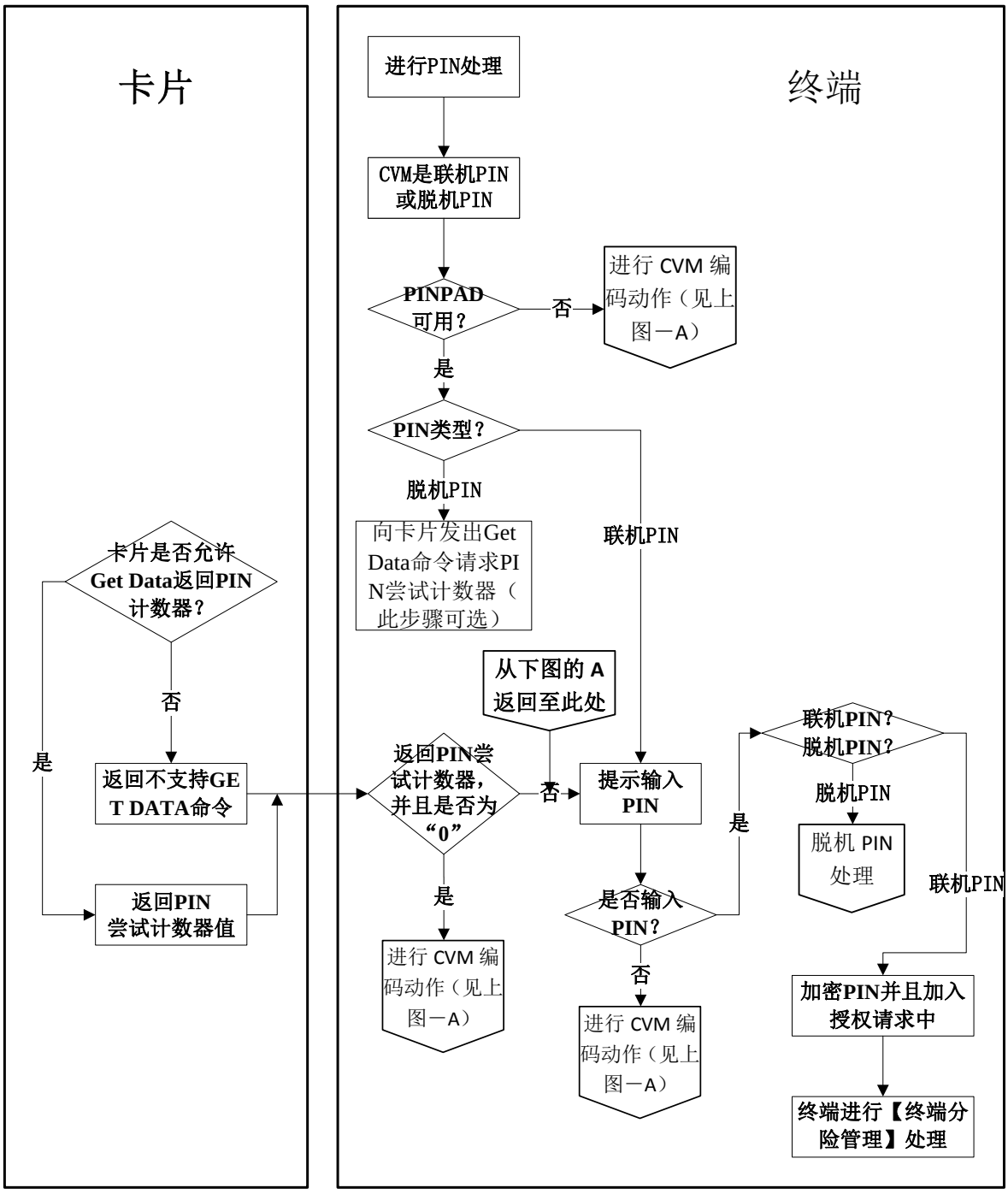


图11　PIN 验证处理流程图（1）

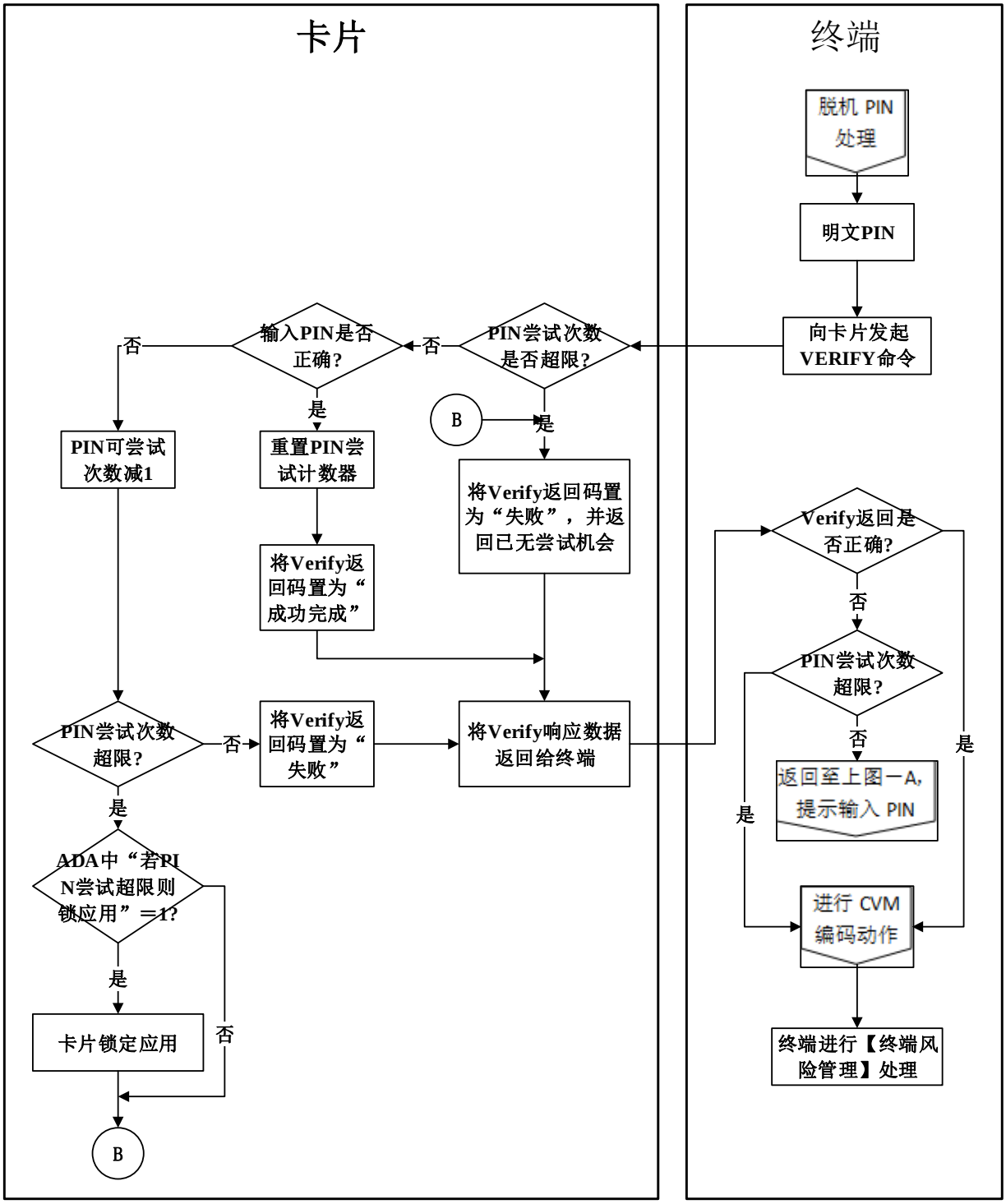


图12　PIN 验证处理流程图（2）

8.1.2.6.7　前期相关处理

——初始化应用处理

从卡片中获取应用交互特征（AIP），指示卡片是否支持持卡人验证。

——读取应用数据

终端从卡片中读取持卡人验证方法列表以及其他持卡人验证处理中使用的数据。

8.1.2.6.8 后续相关处理

——终端行为分析

终端使用持卡人验证结果，以及发卡机构行为代码和终端行为代码来决定交易是被脱机拒绝、是联机发送授权请求、还是脱机批准。

——卡片行为分析

当PIN尝试次数超限时，卡片使用持卡人验证结果与应用缺省行为中的参数来决定是拒绝交易，还是进行联机授权请求。

——联机处理

授权请求报文中不包括脱机PIN，但包括脱机PIN验证结果在内的持卡人验证结果，发卡机构的授权决定中应该考虑这些结果。

——交易结束

联机获取授权的尝试失败后，卡使用持卡人验证结果和应用缺省行为中的参数来决定是否拒绝交易。

——发卡机构脚本命令处理

PIN CHANGE/UNBLOCK命令可以用于重新设置PIN重试次数计数器，使其与PIN重试次数上限相等。

APPLICATION UNBLOCK命令可用来解锁在持卡人验证处理中锁定的应用。

8.1.2.7 终端风险管理

8.1.2.7.1 描述

终端风险管理使大额交易联机授权，并确保芯片交易能够周期性地进行联机以防止在脱机环境中也许无法觉察的风险。

发卡机构需要支持终端风险管理。无论卡片是否支持，终端都需要支持终端风险管理。

8.1.2.7.2 卡片数据

表19列出并描述了终端风险管理中使用的卡片数据元。

表19 终端风险管理—卡数据

数据元	说明
应用主账号（PAN）	终端异常文件检查时使用的有效的持卡人账号。
应用交易计数器（ATC）	自卡片个人化以后处理的交易数量，在终端频度检查中使用。
上次联机 ATC 寄存器	上次联机 ATC 的值。如果卡片要求终端进行终端频度检查或新卡检查，则这个数据元以及下面所列出的数据元都应提供。
连续脱机交易下限	如果终端可以联机，该数据元（标签“9F14”）是发卡机构定义的在交易应联机之前所允许的最大连续脱机交易笔数，它用于终端频度检查。
连续脱机交易上限	该数据元（标签“9F23”）是发卡机构定义的在脱机交易应被拒绝之前所允许的最大连续脱机交易笔数。它用于终端频度检查。

8.1.2.7.3 终端数据

表20列出并描述了终端风险管理中使用的终端数据元。

表20 终端风险管理—终端数据

数据元	说明
授权金额	该数值型数据元（标签“9F02”）存储了当前交易金额（不包括调账交易）。用于最低限额检查。
用于偏置随机选择的最大目标百分数	用于随机选择交易联机处理。
用来随机选择的目标百分数	用于随机选择交易联机处理。
终端最低限额	该数据元（标签“9F1B”）表示与应用标识符相关联的终端最低限额。用于最低限额检查和随机选择交易联机处理。
终端验证结果（TVR）	记录终端脱机处理结果的一系列指示器。它们用来记录终端风险管理检查的结果。
偏置随机选择与阈值	用于随机选择交易联机处理的数值。
交易日志	终端上存储的被接受的交易的交易日志，用来防止使用分次消费的方法企图躲过最低限额检查。这个日志至少包含了应用的主账号和交易金额，并可选包含应用主账号序列号和交易日期。而交易数量的储存和日志的维护由具体应用定义。如果该日志存在，则终端最低限额检查将可能使用到这个日志
交易状态信息（TSI）	标明终端执行的功能，联机授权和清算报文中不提供此数据元，终端用它来表示已经执行了终端风险管理。

8.1.2.7.4 命令

——GET DATA

如果终端尚未获取上次联机ATC寄存器和应用交易计数器，则发送取数据（GET DATA）命令从卡片中读取。这些数据在终端频度检查和新卡检查时使用。

如果卡片支持终端频度检查或新卡检查，卡片要返回这些数据给终端。

如果卡片不支持终端频度检查或新卡检查，这些数据要存储为专用数据元并不能返回给终端。此时卡片响应SW1 SW2=“6A88”。

8.1.2.7.5 终端异常文件检查

如果终端异常文件存在，终端应检查应用主账号（PAN）是否列在终端异常文件中。

如果卡号列在终端异常文件中，终端在终端验证结果（TVR）中设置“卡号出现在终端异常文件中”的位为“1”。

8.1.2.7.6 商户强制交易联机

在可以联机的终端，商户可以将终端设置为交易应该联机处理。

如果商户强制交易联机，终端将终端验证结果（TVR）中“商户强制交易联机”的位设置成“1”。

8.1.2.7.7 最低限额检查

执行最低限额检查，可以使超过终端最低限额的交易执行联机授权。

终端将授权金额和终端最低限额进行比较，如果交易额大于等于最低限额，终端将终端验证结果（TVR）中“交易金额超过最低限额”的位设置成“1”。即使终端最低限额为0，终端也应执行最低限额检查，并将终端验证结果中“交易金额超过最低限额”的位设置成“1”。

如果终端包含一个交易日志，终端就检查同一张卡片先前的交易金额加上现在的交易金额是否超过了最低限额。

8.1.2.7.8 随机交易选择

可以支持脱机和联机交易的终端会随机选择交易进行联机处理。

如果随机选择了一个交易，终端会标注在终端验证结果中。

8.1.2.7.9 终端频度检查

频度检查允许发卡机构在一个预先设定的连续脱机交易的数量之后要求进行联机处理。允许脱机的终端应支持终端频度检查。发卡机构可以选择终端不支持频度检查。

如果卡片在读取应用数据处理时提供连续脱机交易下限（标签“9F14”）和连续脱机交易上限（标签“9F23”），终端将执行终端频度检查。如果这些数据中的任意一个都没有出现在卡里，终端将避开这个处理。

终端发送GET DATA命令向卡读取上次联机ATC寄存器与交易计数器（ATC）。卡在命令响应中返回这些数据元。

终端将ATC与上次联机ATC寄存器对比：

——如果 ATC 减去上次联机 ATC 寄存器大于连续脱机交易下限值，终端将终端验证结果中“超过连续脱机交易下限”的位设置成“1”。

——如果 ATC 减去上次联机 ATC 寄存器大于连续脱机交易上限值，终端将终端验证结果中“超过连续脱机交易上限”的位设置成“1”。

注：卡片行为分析中，卡片可执行相似的频度检查。卡的频度检查不会影响终端验证结果。

8.1.2.7.10 新卡检查

在终端所做的新卡检查中，如果存在连续脱机交易上限值和连续脱机交易下限值，终端就检查上次联机ATC寄存器（如果卡提供的话）。根据发卡机构认证结果和卡片参数，交易被联机批准后，该寄存器被重新复位。

终端发送GET DATA命令向卡片读取上次联机ATC寄存器（如果该数据元并未出现在终端里）。卡片用上次联机ATC寄存器作为对GET DATA命令的响应。

终端检查上次联机ATC寄存器，如果序号为0，终端将TVR中的“新卡”位置设为“1”。

注：卡片行为分析中，卡片可执行相似的新卡检查。

8.1.2.7.11 流程图

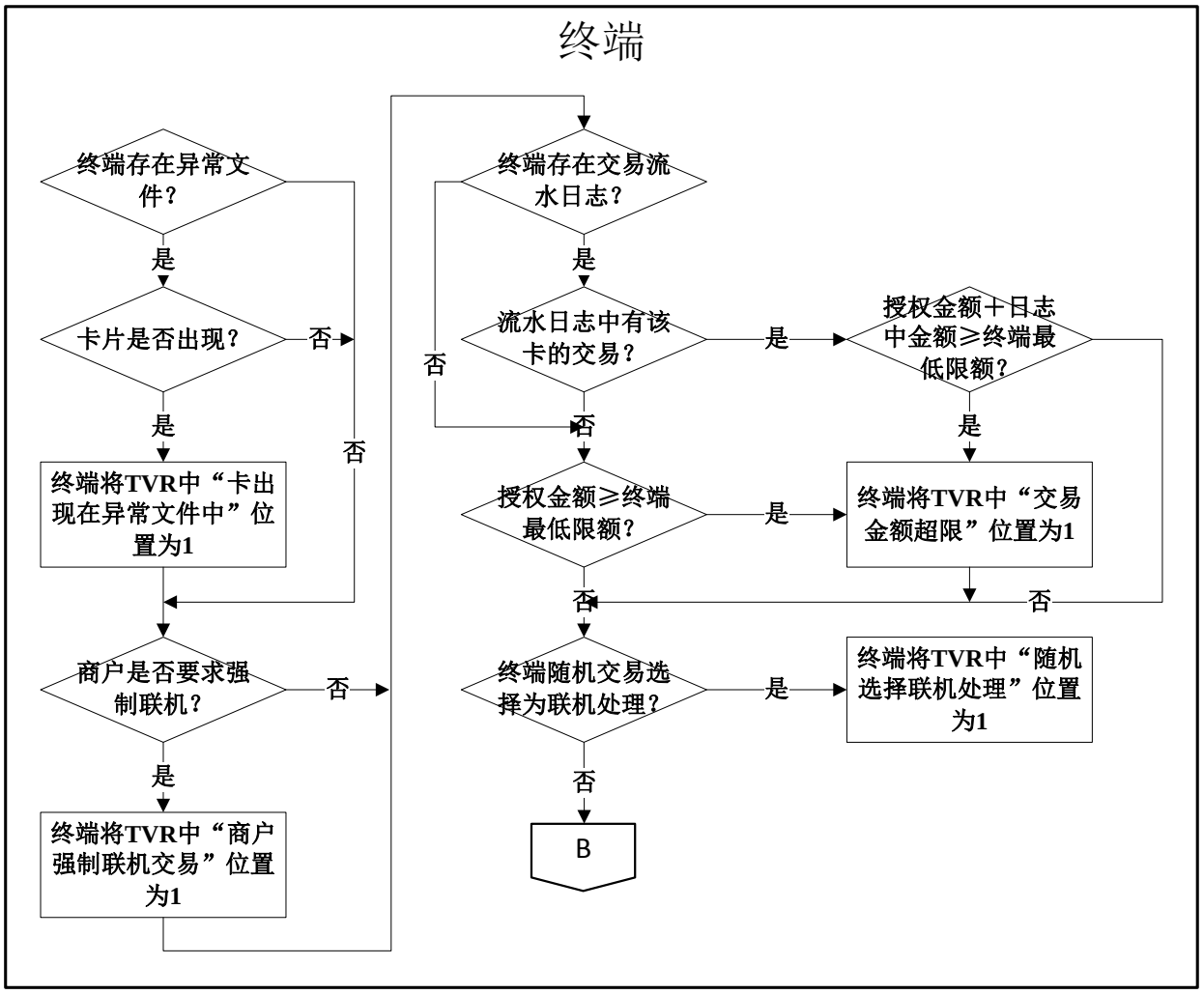


图13　终端风险管理处理流程图（1）

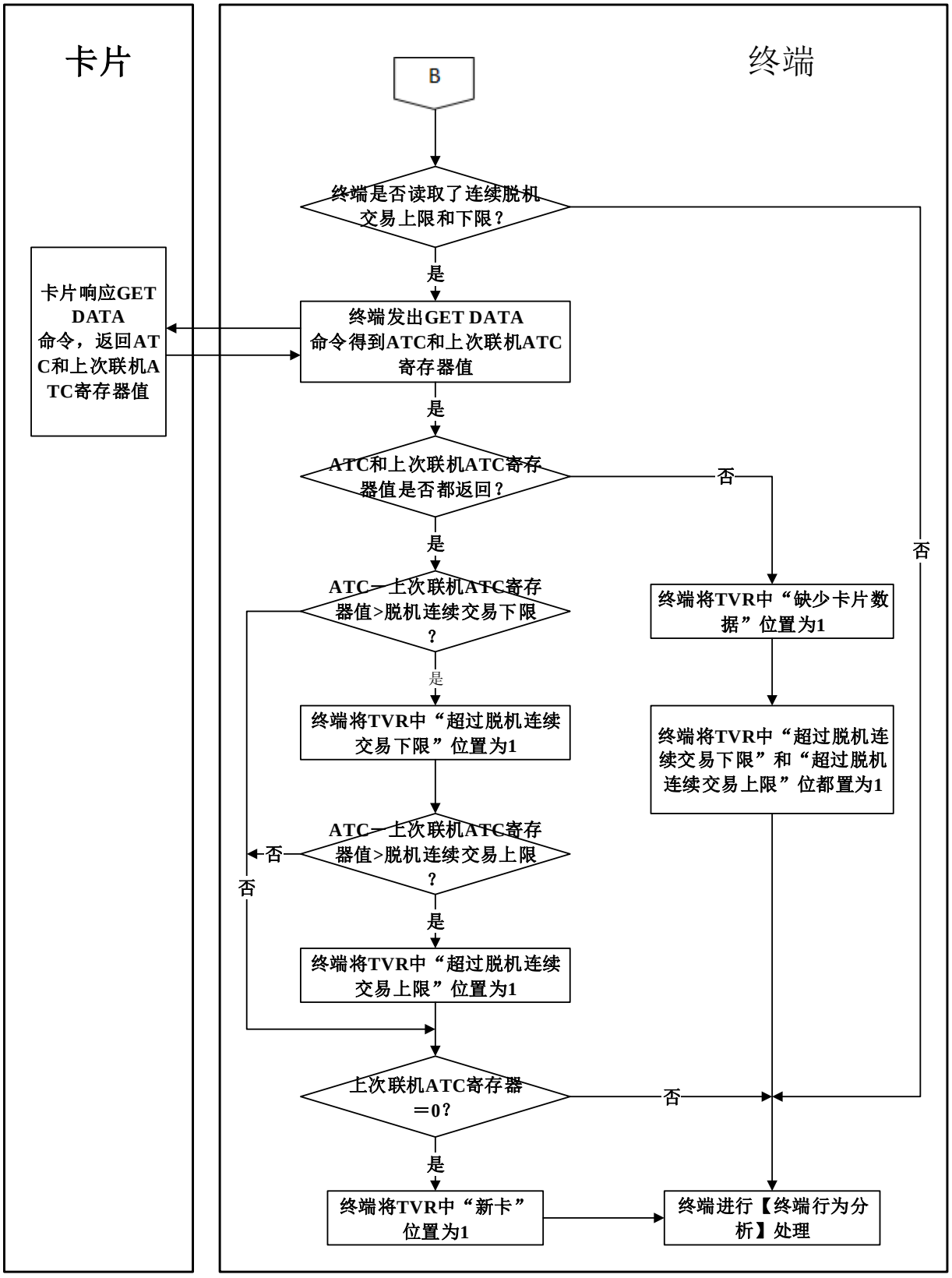


图14　终端风险管理处理流程图（2）

8.1.2.7.12 前期相关处理

——读取应用数据

下列数据从卡片中读取：

1) 主账号用于检查终端异常文件；
2) 如果卡上存在连续脱机交易上限值和下限值，它们用于终端频度检查。

8.1.2.7.13 后续相关处理

——终端行为分析

终端根据卡片和终端的设置来决定采取怎样的行动，如果：

1) 卡片在终端异常文件上；
2) 商户强制交易联机；
3) 超过了最低限额；
4) 交易被随机选择进行联机处理；
5) 频度检查金额或笔数超限；
6) 新卡。

8.1.2.8 终端行为分析

8.1.2.8.1 描述

终端行为分析中，终端把发卡机构设置在卡片里及收单机构设置在终端里的规则应用于脱机处理结果，以决定交易是应该被脱机批准、应该被脱机拒绝，还是请求联机授权。

终端行为分析牵涉到两个步骤：

——**检查脱机处理结果**—终端检查由终端记录在终端验证结果里的脱机处理结果，决定交易要请求联机授权、脱机批准，还是脱机拒绝。此过程考虑了卡片中发卡机构定义的规则，即发卡机构行为代码（IAC）以及终端定义的规则，即终端行为代码（TAC）。

——**请求密文处理**—终端要求一个来自卡片的密文。

终端行为分析中，脱机批准或申请联机处理的决定并不是最终的。卡片可以不考虑终端的决定，但脱机拒绝的决定是不可以忽略的。

8.1.2.8.2 卡片数据

表21和表22所描述是先前从卡片收到并在终端行为分析中使用的卡片数据元。这些数据元及其用法的详细说明见JT/T XXX.1附录C。

表21 检查脱机处理结果—卡片数据

数据元	说明
发卡机构行为代码（IAC）	发卡机构行为代码是三种数据元，即发卡机构行为代码-拒绝，发卡机构行为代码-联机，发卡机构行为代码-缺省。每个发卡机构行为代码由一系列与终端验证结果（TVR）中的比特位相对应的比特位组成： ——发卡机构行为代码-拒绝位设置为“1”反映了交易被脱机拒绝的终端验证结果条件； ——发卡机构行为代码-联机位设置为“1”代表需要联机授权条件； ——发卡机构行为代码-缺省位设置为“1”是当联机处理不可行时脱机拒绝所需的条件。 类似的终端行为代码（TAC）在终端里定义。IAC 数据建议作为静态脱机数据认证用数据。

表22 要求密文处理—卡片数据

数据元	说明
卡片风险管理数据对象列表 1（CDOL1）	卡片风险管理数据对象列表 1 包含了终端数据对象的标签和长度，卡片需要用它们来生成第一个应用密文，以及进行其他处理。
交易证书数据对象列表 TDOL	列出生成交易证书（TC）哈希计算的数据对象（标签和长度）。

8.1.2.8.3 终端数据

终端数据元及其用法的详细说明见附录A。

表23 检查脱机处理结果—终端数据

数据元	说明
终端行为代码（TAC）	终端行为代码是三种数据元，即终端行为代码-拒绝，终端行为代码-联机，终端行为代码-缺省。和发卡机构行为代码相似，每个终端行为代码由一系列与终端验证结果（TVR）中的比特位相对应的比特位组成： • 终端行为代码-拒绝比特位设置为“1”反映了交易被脱机拒绝的终端验证结果条件； • 终端行为代码-联机比特位设置为“1”代表了联机授权条件； • 终端行为代码-缺省比特位设置为“1”是当联机处理不可行时脱机拒绝所需的条件。
终端验证结果（TVR）	终端验证结果是在交易处理期间被用来代表脱机处理结果而设置的一系列比特位。

表24 要求密文处理—终端数据

数据元	说明
终端数据元	在卡片风险管理数据对象列表 1 中得以详细说明的终端数据元包括在 GENERATE AC 命令中。
交易证书（TC）哈希结果	可选。作为输入数据使用生成应用密文（GENERATE AC）命令送入卡片。

8.1.2.8.4 命令

——GENERATE AC

终端发送GENERATE AC命令向卡申请一个应用密文。命令中的P1参数标明了密文类型以及是否执行CDA。命令的数据部分包括卡片在CDOL1中要求的终端数据元。CDOL1是终端在读应用记录处理过程中从卡片中读出的。如果执行复合动态数据验证/应用密文生成，终端也会出现此命令。

该命令指明了下列应用密文中的一种：

1) 交易证书（TC）——用于批准；
2) 应用认证密文（AAC）——用于拒绝；
3) 授权请求密文（ARQC）——进行联机。

此命令也包括卡在卡风险管理数据对象列表1里要求的终端数据对象。

当卡片接到GENERATE AC命令，它进行卡片行为分析。终端行为分析期间不返回对此命令的响应。

8.1.2.8.5 处理流程

终端行为分析处理有两个步骤：

——脱机处理结果的检查

终端检查脱机处理的结果以决定是否交易需要联机、被脱机批准，或被脱机拒绝。这个过程中使用了卡片中发卡机构定义的规则（发卡机构行为代码）以及本部分定义的规则（终端行为代码）。

——请求密文处理

终端行为分析的第二阶段包括向卡片申请一个应用密文。检查脱机处理结果的步骤决定了将申请的密文类型：

1) 脱机批准——TC（交易证书）；
2) 进行联机授权——ARQC（授权请求密文）；
3) 脱机拒绝——AAC（应用认证密文）。

如果执行复合动态数据验证/应用密文生成，终端也会出现此命令。

8.1.2.8.6 流程图

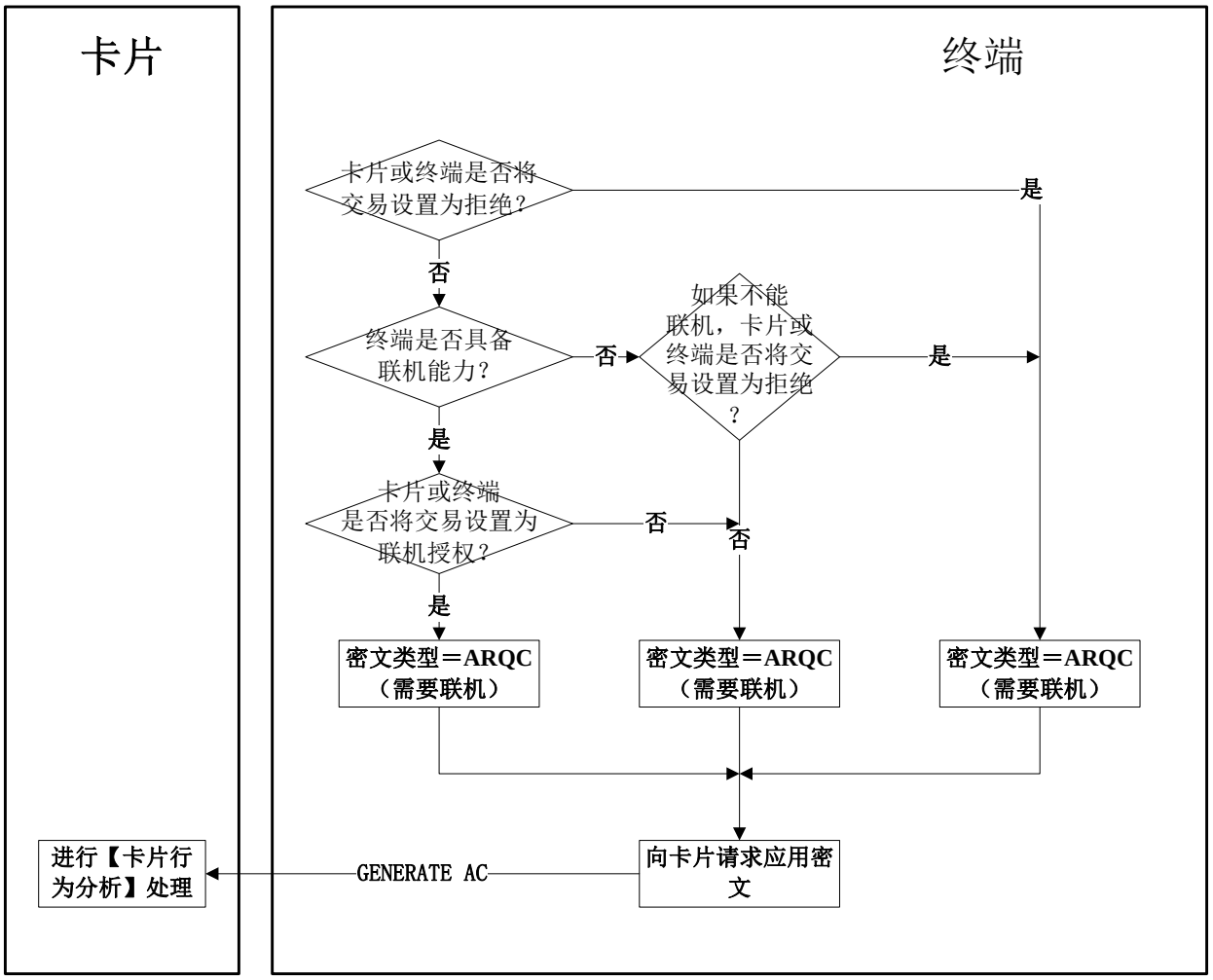


图15 终端行为分析处理流程图

8.1.2.8.7 前期相关处理

——读取应用数据

终端从卡片读取应用数据。此数据包括卡片风险管理数据对象列表1和发卡机构行为代码。

——脱机数据认证，处理限制，持卡人验证及终端风险管理

根据处理结果，这些脱机功能在终端验证结果设置比特位。终端行为分析中，这些比特位设置与发卡机构行为代码和终端行为代码共同使用来决定交易处理。

8.1.2.8.8 后续相关处理

——卡片行为分析

卡片行为分析中，卡片执行附加的风险管理来决定是否否定终端行为分析中脱机批准或请求联机的决定。

8.1.2.9 卡片行为分析

8.1.2.9.1 描述

卡行为分析允许发卡机构执行频度检查以及其他的卡片内部的风险管理。本条描述的所专有的卡片风险管理特性包括如下检查：

——上次交易的行为；

——新卡；

——脱机交易计数和累计脱机金额。

卡片行为分析结束后，卡片返回一个应用密文给终端。AAC表示交易拒绝，ARQC表示请求联机授权，TC表示脱机交易接受。如果卡片和终端都支持CDA，卡片返回的ARQC或TC要作为签名的动态应用数据的一部分。

8.1.2.9.2 卡片数据

表25列出并描述了卡行为分析中用到的卡数据元。

表25 卡片行为分析－卡片数据

数据元	说明
应用密文	卡响应 GENERATE AC 命令而返回的密文。 ——返回请求拒绝的应用认证密文称为 AAC ——返回请求批准的交易证书称为 TC ——联机处理申请的授权请求密文称为 ARQC
应用货币代码	指明和应用有关的国内货币，是卡片指定货币
应用缺省行为（ADA）	发卡机构定义的指示器，指定在一些特殊条件下的卡片行为。如果卡片中没有则缺 省认为为零
应用交互特征（AIP）	包括表明卡片支持 CDA 和发卡机构认证能力的指示器
卡风险管理数据对象列表中要求的数据（CDOL1）	卡风险管理数据对象列表 1 中要求的数据见 JT/T XXX.1 附录 C。
卡片验证结果（CVR）	表明当前和上次交易的脱机处理结果。此数据作为发卡机构应用数据的一部分联机上送
密文信息数据（CID）	在生成应用密文（GENERATE AC）命令中返回给终端，CID 指出了卡片返回的密文的类型。CID 还包括了是否要生成通知的标识位，以及生成通知的原因的代码
连续脱机交易计数器（国际-货币）	每次使用非卡片指定货币的脱机交易，计数器加 1
连续脱机交易限制次数（国际-货币）	使用卡片非指定货币的脱机交易的限制次数，超过则请求联机处理
连续脱机交易计数器（国际-国家）	每次发卡机构国家代码和终端国家代码不同的脱机交易，计数器加 1
连续脱机交易限制次数（国际-国家）	发卡机构国家代码和终端国家代码不同的脱机交易的限制次数,超过请求联机处理
累计脱机交易金额	记录自从上次联机处理以来，使用卡片指定货币的脱机交易总金额
累计脱机交易金额限制	累计脱机交易金额的限制数。如果超过请求联机处理
累计脱机交易金额（双货币）	记录自从上次联机处理以来，使用卡片指定货币和第 2 货币的脱机交易总金额
累计脱机交易金额限额（双货币）	累计脱机交易金额（双货币）的限制数。如果超过请求联机处理
货币转换因子	用来将第二应用货币转换成应用指定货币的汇率值。此数据元有四个字节，第一个高半字节表示小数点的位置，后面 7 个半字节表示汇率值
DDA 失败指示位	当上次交易 DDA 失败而且交易拒绝时设置的卡片内部应用指示位。
发卡机构认证失败指示位	当上次联机交易出现下面两种情况之一时设置的卡片内部应用指示位： ——发卡机构认证执行并失败；

	——发卡机构认证强制但没执行。
发卡机构认证指示位	指明卡片支持的发卡机构认证是强制还是可选的指示位。
发卡机构国家代码（“9F57”）	表明发卡机构的国家。
发卡机构脚本命令计数器	记录上次联机交易中，有安全报文的发卡机构脚本命令的个数。
发卡机构脚本失败指示位	在上次联机交易中，发卡机构脚本处理失败时设置。
连续脱机交易下限（“9F58”）	在申请联机授权之前，卡片允许的最大连续脱机交易限制数。
卡片请求脱机拒绝指示位	当卡片风险管理检查决定交易拒绝时设置的卡片内部应用指示位
联机授权指示位	当申请联机的交易无法联机或联机授权被中止时设置的内部应用指示位。
卡片请求联机指示位	当卡片风险管理检查决定交易要联机上送时设置的卡片内部应用指示位。
PIN 尝试次数计数器	记录 PIN 剩余的尝试次数。
第二应用货币代码	用于双货币频度检查。可以使用货币转换因子转换为本地货币（卡片指定货币）。
SDA 失败指示位	当上次交易 SDA 失败而且交易拒绝时设置的卡片内部应用指示位。
交易日志文件短文件标识符	当卡片作出接受交易的决定后，卡片内部自动记录交易日志，交易日志文件的短文件标识符标识此文件。

8.1.2.9.3 终端数据

表26列出在卡片风险管理处理中是使用的终端数据。

表26 卡片行为分析——终端数据

数据元	描述
授权金额	交易的金额。
交易货币代码	表明交易的货币类型，在 CDOL1 中。
终端国家代码	表明终端的国家，在 CDOL1 中。
终端认证结果（TVR）	终端记录脱机处理结果的一系列指示器。

8.1.2.9.4 命令

——GENERATE AC

终端使用生成应用密文（GENERATE AC）命令请求卡片提供一个应用密文。

命令中的P1参数表明了密文类型以及是否执行CDA。命令的数据部分包括CDOL1中指定的终端数据。

命令的响应信息包括应用密文和密文信息数据。如果卡片执行CDA，而且密文类型为ARQC或TC，密文要作为签名的动态应用数据使用IC卡私钥签名。

8.1.2.9.5 处理流程

终端行为分析之后，终端向卡发送GENERATE AC命令，向卡片提供在卡片风险管理数据对象列表（CDOL1）中要求的数据并请求一个应用密文。在8.1.2.8阐述了终端行为分析处理过程。

卡片收到终端发来的生成应用密文（GENERATE AC）命令。命令的数据部分包括CDOL1中卡片指定的终端数据。如果CDOL1和PDOL中均含有某个标签（这些标签包括但不仅限于交易货币代码‘5F2A’、授权金额‘9F02’，但不包括终端验证结果‘95’，交易状态信息‘9B’和不可预知数‘9F37’），但终端在生成应用密文（GENERATE AC）命令中给出的标签的值与取处理选项（GPO）命令中给出的标签的值不一致，卡片应当以生成应用密文（GENERATE AC）命令中收到的该值为准，在该笔交易的后续所有流程中均应使用该值。卡片不应因生成应用密文（GENERATE AC）命令中某个标签的值与取处理选项（GPO）命令中某个标签的值不一致而以非‘9000’响应生成应用密文（GENERATE AC）命令）。

——卡片风险管理

如果卡片支持并且要求的数据可用，则卡片执行下列卡片风险管理行为：

a) 上次交易行为：
   1) 联机授权未完成
   2) 上次联机交易时，发卡机构认证失败
   3) 上次交易静态数据认证失败
   4) 上次交易动态数据认证失败
   5) 上次交易发卡机构脚本命令执行情况
   6) 上次交易 PIN 重试次数超限
b) 新卡检查
c) 频度检查查看以下项目的脱机处理次数是否超限：
   7) 全部连续脱机交易笔数
   8) 根据货币种类统计的全部连续脱机国际交易笔数
   9) 根据国家统计的全部连续脱机国际交易笔数
   10) 指定货币的全部脱机交易累计金额
   11) 指定货币和第二货币的全部脱机交易金额

——卡片响应决定

根据卡片风险管理的结果，卡片决定交易响应。卡片返回的密文可以与终端请求密文类型不同：

a) 卡片可以不考虑终端已批准脱机的决定，而申请联机授权或拒绝脱机
b) 卡片可以不考虑终端申请联机授权的决定，而拒绝交易

表27 卡片行为分析－卡片对 GENERATE AC 命令的响应

终端请求类型	卡片响应类型		
	AAC	ARQC	TC
AAC	拒绝	—	—
ARQC	拒绝	申请联机	—
TC	拒绝	申请联机	批准

——标准 GENERATE AC 的响应

卡片利用终端和卡片提供的数据生成一个基于对称算法的密文。JT/T XXX.1附录C中详述了所要求的数据，JT/T XXX.5中详述了密文生成过程中所需的对称密钥和算法。

卡片在GENERATE AC响应中将此密文返回给终端。这个响应中的密文类型表明了卡片对于此交易的处理决定（脱机批准、脱机拒绝、申请联机授权）。

——复合动态数据认证/应用密文生成的 GENERATE AC 响应

如果终端在GENERATE AC命令中表明将执行CDA，并且卡片在GENERATE AC响应中返回的密文类型是批准（TC）或请求联机（ARQC），则卡片用公共交通IC卡私钥将应用密文、密文信息数据以及其他的数据加密。在GENERATE AC响应中，卡片将这签名数据返回给终端。

8.1.2.9.6 流程图

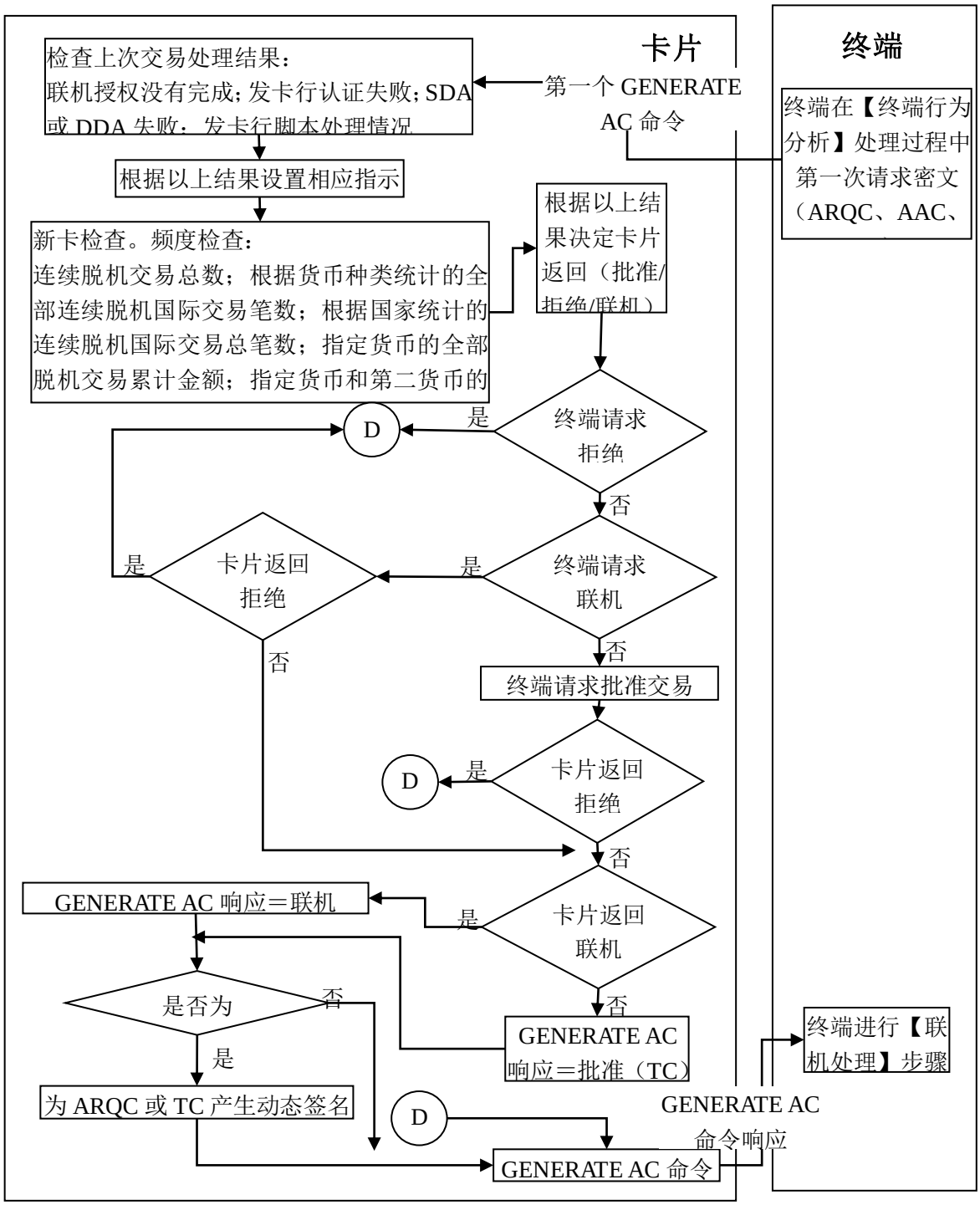


图16 卡片行为分析处理流程图

8.1.2.9.7 前期相关处理

——读取应用数据

终端从卡片读取卡片风险管理数据对象列表1（CDOL1）。

8.1.2.9.8 后继相关处理

——交易结束

如果要求联机处理，但终端无法将交易联机发送，则卡片和终端执行其他的处理来决定是脱机批准或拒绝交易。

终端在执行另外的分析（类似于终端行为分析）中使用发卡机构行为代码（IAC）-拒绝和终端行为码（TAC）-拒绝来以决定在最终GENERATE AC命令中要请求的密文类型（AAC或TC）。

卡也执行下列的卡风险管理检查，以决定最终的交易处理结果：

1) 对于全部连续脱机交易（上限）的频度检查
2) 新卡
3) 没有执行脱机 PIN 验证

8.1.2.10 联机处理

8.1.2.10.1 描述

联机处理允许发卡机构主机根据发卡机构设置的主机风险管理参数判断交易是允许或拒绝。与传统的联机欺诈检查和信用检查相比，主机授权系统还需额外通过利用卡片产生的动态密文执行联机卡片授权，同时还需在决定授权时考虑脱机处理的结果。

发卡机构返回的数据可以包括发卡机构生成的密文和给卡片的更新数据。其中发卡机构产生的密文用于卡片认证返回数据真实性。

8.1.2.10.2 卡片数据

终端所用到的卡片数据见表28。

表28 联机处理－终端使用的卡片数据

数据元	描述
GENERATE AC 命令返回数据	返回数据中包括： ——密文类型（如果交易需要联机授权，则是授权请求密文 ARQC）； ——应用密文（AC）； ——应用交易计数器（ATC）； ——发卡机构应用数据。
应用交互特征（AIP）	终端在应用初始化处理时从卡片得到 AIP，其中一位指明卡片是否支持发卡机构认证。

在发卡机构授权过程中卡片内部使用的数据见表29。

表29 联机处理－卡片内部使用数据

数据元	描述
授权请求密文（ARQC）	由卡片在此交易的较早步骤产生。ARQC 和授权响应码将在授权响应密文（ARPC）确认处理中作为输入数据。
应用密文过程密钥（UDK）	是 ARPC 确认处理中使用的 DES 密钥，与产生 ARQC 使用的是同一密钥。
卡片验证结果（CVR）	如果发卡机构认证失败，相应位将置为 1。
发卡机构认证失败指示器	如果发卡机构认证失败该位将置为 1。

8.1.2.10.3 终端数据

根据发卡机构认证状态，终端需改变的数据元见表30。

表30 联机处理－终端需改变数据

数据元	描述
终端验证结果（TVR）	当发卡机构认证失败时，其中相应位将置为1。
交易状态信息（TSI）	当发卡机构认证执行过后，其中相应位置为1。

8.1.2.10.4 联机响应数据

表31是发卡机构可能返回给收单机构的响应数据，如果存在的话，收单机构应将数据传送给终端。

表31 联机处理－发卡机构可能返回的响应数据

数据元	描述
发卡机构认证数据	包括以下子项： ——授权响应密文（ARPC）：由发卡机构主机系统产生的密文； ——授权响应码：在产生ARPC时用到的响应码。
发卡机构脚本	由发卡机构发送给卡片的一些命令数据，用于更新卡片数据。

8.1.2.10.5 命令

联机处理过程使用外部认证（EXTERNAL AUTHENTICATE）命令。

如果执行了发卡机构认证，终端应使用从发卡机构请求到的发卡机构认证数据通过外部认证（EXTERNAL AUTHENTICATE）命令验证授权响应密文（ARPC）的正确性。通过命令的返回可以知道认证是否通过。

外部认证命令的响应码说明发卡机构认证数据验证是否通过。如果验证通过，SW1 SW2=“9000”，如果失败，返回“6300”。

一次交易中，卡片允许处理一次外部认证命令，后续的外部认证命令卡片一律返回“6985”

8.1.2.10.6 处理流程

标准的联机处理包括联机请求、联机响应，如果需要，可以执行发卡机构认证。

——联机请求

如果卡片在GENERATE AC向终端返回ARQC，同时终端具备联机能力，则终端发出联机授权报文。

如果卡片没有返回ARQC或终端不具备联机能力，则转至完成处理步骤。

——联机响应

联机请求报文成功发送给发卡机构后，终端接受发卡机构返回的响应报文，其中可以包括用于更改卡片信息的发卡机构命令脚本或密文，也可以两者皆有，用于确认响应报文确实是从合法的发卡机构返回的。如果联机响应中包括发卡机构认证数据，同时卡片支持发卡机构认证，则执行发卡机构认证。否则，转至完成处理步骤。

——发卡机构认证

终端向卡片发出外部认证（EXTERNAL AUTHENTICATE）命令用于执行发卡机构认证，卡片用先前生成的ARQC，发卡机构授权响应码以及存储在卡片特定安全区域的子密钥（UDK）验证ARPC的合法性。

卡片和终端都要记录发卡机构认证结果：

1) 卡片在卡片验证结（CVR）中设置发卡机构认证结果以及发卡机构认证失败标识，并且在外部认证命令（EXTERNAL AUTHENTICATE）响应报文中将结果返回给终端。
2) 终端在进行完成处理之前，将在终端验证结果（TVR）中设置发卡机构认证结果和交易状态信息（TSI）。

8.1.2.10.7 流程图

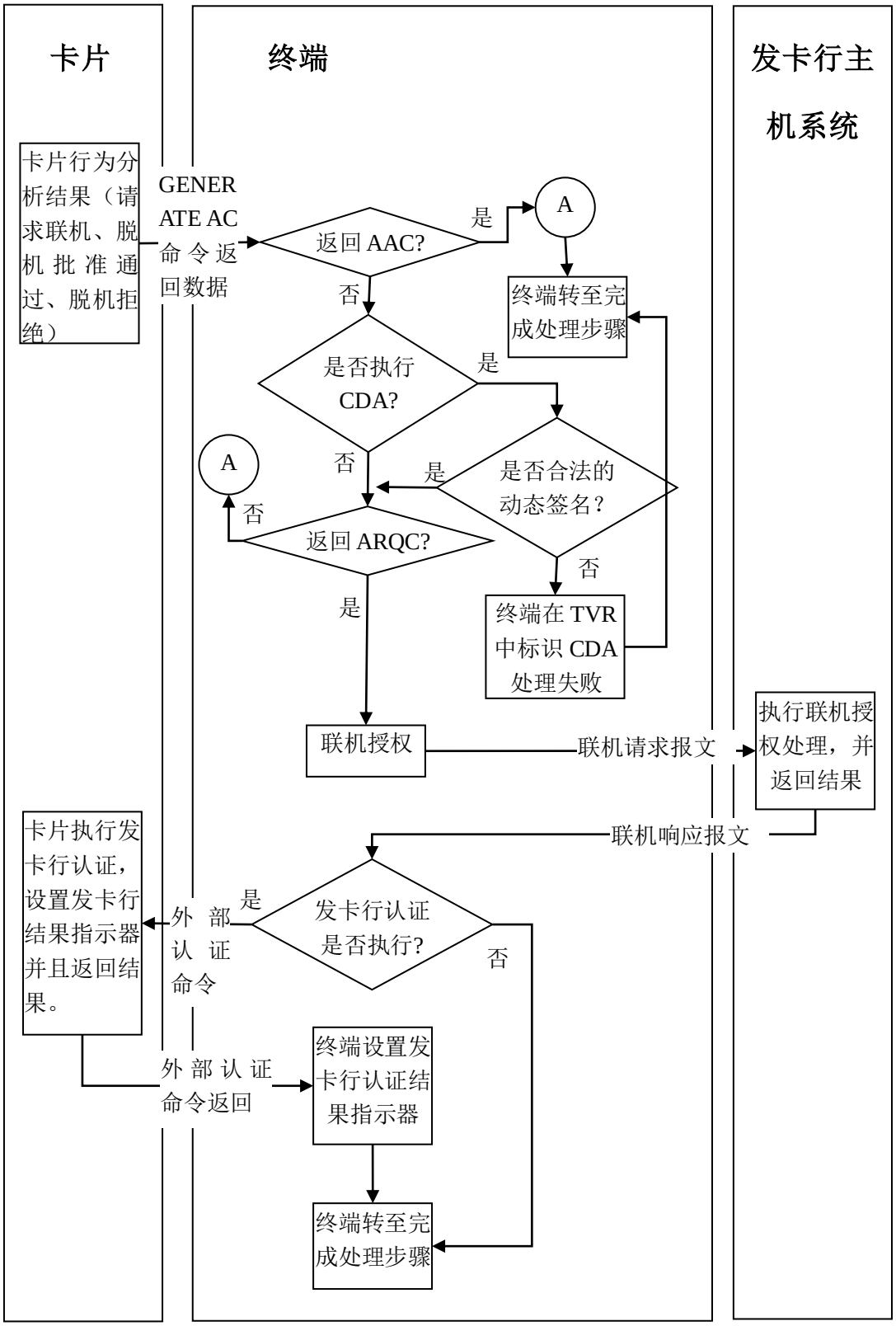


图17 联机处理流程图

8.1.2.10.8 前期相关操作

——卡片行为分析

如果经过卡片分析后需要联机授权，则卡片返回的密文类型为ARQC。

8.1.2.10.9 后续相关操作

——交易结束

在完成处理过程中，卡片参考发卡机构认证结果和卡片参数交易如何处理以及是否重置相关指示器和计数器。

——发卡机构脚本处理

如果联机处理范围报文中包括发卡机构命令脚本，终端需要将这些命令脚本发给卡片执行。

8.1.2.11 交易结束

8.1.2.11.1 描述

终端和卡片执行完成来结束交易处理，主要包括以下动作：

——如果要求联机处理，但终端并不支持联机处理或联机授权无法完成，则终端和卡片通过其他的分析决定交易是否可以脱机完成或拒绝。

——如果终端执行 CDA 失败，则终端按照以下方式处理：

1) 如果卡片请求 ARQC，则终端在第二次产生应用密文（GENERATE AC）时请求 AAC（拒绝密文）；
2) 如果卡片请求 TC 并且 CDA 执行失败，终端拒绝交易并返回响应码。

——发卡机构的联机确认结果有可能会因为发卡机构认证结果和卡片的一些选项而变成拒绝交易。

——交易处理过程中指示器和计数器会反应发生情况。

——联机授权后，指示器和计数器可能会根据发卡机构认证结果和卡片选项重置。

终端可以执行其他一些附加的功能以完成整个交易。例如打印凭条、记录交易数据等与终端部分不冲突的功能。

8.1.2.11.2 卡片数据

完成处理时卡片内部使用到的部分数据见表32。

表32 交易结束－卡片使用数据元

数据元	描述
应用货币代码（9F51）	指明和应用有关的国内货币。
应用缺省行为（ADA）	发卡机构定义的指示器，指定在一些特殊条件下的卡片行为。
应用交互特征（AIP）	包括表明卡片支持发卡机构认证能力的指示位。
连续脱机交易计数器（国际-货币）	记录自从上次联机授权以来，使用非指定货币的脱机交易的次数。
连续脱机交易计数器（国际-国家）	记录自从上次联机授权以来，终端国家代码和发卡机构国家代码不同的脱机交易的次数。此检查使用发卡机构国家代码决定交易是国内还是国际。
累计脱机交易金额	记录自从上次联机处理以来，使用应用指定货币的脱机交易总金额。
累计脱机交易金额（双货币）	记录自从上次联机处理以来，使用应用指定货币（应用货币代码）和第二应用货币的脱机交易总金额。如果是第二应用货币，在累加之前要先使用货币转换因子将授权金额进行转换。

累计脱机交易金额上限	累计脱机交易金额和累计脱机交易金额（双货币）的最大累计值限制数。
货币转换因子	用来将第二应用货币转换成应用指定货币的汇率值。第二应用货币金额乘以转换因子转换为应用指定货币金额。
DDA 失败指示位	标明本次或上次交易 DDA 失败。
发卡机构认证失败指示位	标明本次或上次交易发卡机构认证失败，在后续交易的卡片行为分析步骤中使用。
发卡机构认证指示位	标明发卡机构认证是强制还是可选。 如果发卡机构认证是强制的，卡片应收到并成功处理一个 ARPC（即通过发卡机构认证）来对上次联机 ATC 寄存器和脱机计数器进行复位
发卡机构国家代码（9F57）	表明发卡机构的国家。
发卡机构脚本命令计数器	记录上次联机交易中，有安全报文的发卡机构脚本命令的个数。
发卡机构脚本失败指示位	在上次联机交易中，发卡机构脚本处理失败时设置。
上次联机 ATC 寄存器	上次联机授权并满足发卡机构验证需要的交易的 ATC 值。
联机授权指示位	当申请联机的交易无法联机或联机授权被中止时设置的内部应用指示位。
第二应用货币代码	用于双货币频度检查。可以使用货币转换因子转换为应用货币。
SDA 失败指示位	标明本次或上次交易 SDA 失败。
连续脱机交易上限	如果交易无法联机，接受交易脱机的最大连续脱机交易次数。

卡片对产生应用密文（GENERATE AC）命令响应数据见表33。

表33　交易结束－GENERATE AC 命令卡片响应数据

数据元	描述
应用密文（AC）	由卡片产生的密文
应用交易计数器（ATC）	卡片记录交易次数的计数器
密文信息数据	包括下列指示位： 密文类型： -拒绝 AAC； -接受 TC； -联机上送 ARQC。 其他状态信息。
发卡机构应用数据	发卡机构定义的应用数据，包括 CVR。
卡片验证结果（CVR）	表明当前和上次交易的脱机处理结果。

表34　终端使用交易结束——终端使用的卡片数据

数据元	描述
卡片风险管理数据对象列表 2（CDOL2）	列出在第二个 GENERATE AC 命令中，卡片要求终端传送的数据对象（标签和长度）。除了密文算法中要求的数据标签外，下面列出的数据应在 CDOL2 中用于交易结束处理： ——授权金额（如果支持使用金额的频度检查）； ——授权响应码； ——终端验证结果（TVR）； ——交易货币代码（如果支持使用货币代码的检查）； ——终端国家代码（如果支持使用国家代码的检查）。 CDOL 中的数据元不能重复。

8.1.2.11.3　终端数据

在完成处理过程中终端使用到的数据元见表35。

表35 交易结束－终端使用数据

数据元	描述
授权响应码	表明交易处理结果，提交给卡片。
终端验证结果（TVR）	用来记录脱机处理结果，例如SDA执行情况等。
授权金额	当前交易金额。
终端国家代码	标明终端所在国家。
交易货币代码	标明本次交易使用的货币。

8.1.2.11.4 命令

——GENERATE AC

终端发出第二次GENERATE AC命令向卡片请求最终的应用密文，此处的GENERATE AC命令也可标识成需要执行复合动态数据认证/生成应用密文（CDA）执行。

GENERATE AC指令包含在卡片的CDOL2中详细描述的终端数据元，终端通过读取应用数据取得这些数据元。CDOL2数据包括发卡机构联机返回的授权响应码或在联机授权无法完成的情况下由终端返回的授权响应码。

GENERATE AC指令的响应信息包括卡片交易计数器、指明卡片授权决定的密文类型、应用密文和CVR指定的处理结果，发卡机构自定义的数据也可以被返回。

8.1.2.11.5 处理流程

根据先前的交易处理中所发生的情况，完成处理期间终端可能处理不同的情况：

卡片行为分析结束后，卡片可能已经：

——请求脱机批准（TC）或拒绝交易（AAC）；

——请求联机授权（ARQC）；

在联机处理时，联机授权可能已经：

——成功完成；

——由于终端或通讯原因未完成；

当卡片行为分析执行第一个GENERATE AC命令返回TC或AAC时，则交易脱机接受或拒绝。

终端应根据第一个GENERATE AC命令响应返回的CID以及TVR中显示的复合动态数据认证（CDA）结果决定交易最终结果。

表36 交易结束－终端处理结果（脱机）

第一次 GENERATE AC 返回结果	CDA 处理结果	最终交易结果
TC	CDA 不执行或成功	脱机批准通过
TC	CDA 失败	拒绝
ARQC	CDA 失败	在第二次 GENERATE AC 命令中请求 AAC
AAC	--	拒绝

当卡片行为分析执时第一个GENERATE AC命令返回ARQC（要求联机）时：

a) 由于终端不支持或其他原因造成联机授权没有完成，终端向卡片发出第二个 GENERATE AC 命令请求产生 AAC 或 TC；

b) 当联机授权完成，根据联机授权结果，终端向卡片发出第二个 GENERATE AC 命令请求 TC（批准）或 AAC（拒绝）。终端根据表 37 和表 38 情况处理交易：

表37 交易结束－终端处理结果（联机授权未完成）

终端向卡片请求数据	卡片返回	最终交易结果
AAC	AAC	拒绝
TC	TC/AAC	批准/拒绝

表38 交易结束－终端处理结果（联机授权完成）

联机授权结果	终端向卡片请求数据	卡片返回	最终交易结果
通过	TC	TC 或 AAC	除以下两种情况卡片返回 AAC（拒绝），其他情况卡片返回 TC（批准）： ——发卡机构认证失败，同时 ADA 中标识此种情况拒绝交易； ——发卡机构认证强制，但未执行，同时 ADA 中标识此种情况拒绝交易。 如果拒绝交易，应要向发卡机构发冲正交易。
拒绝	AAC	AAC	拒绝

a) 当联机授权成功，但是终端向卡片发出第二个 GENERATE AC 命令执行失败，终端应向发卡机构发出冲正交易。

8.1.2.11.6 流程图

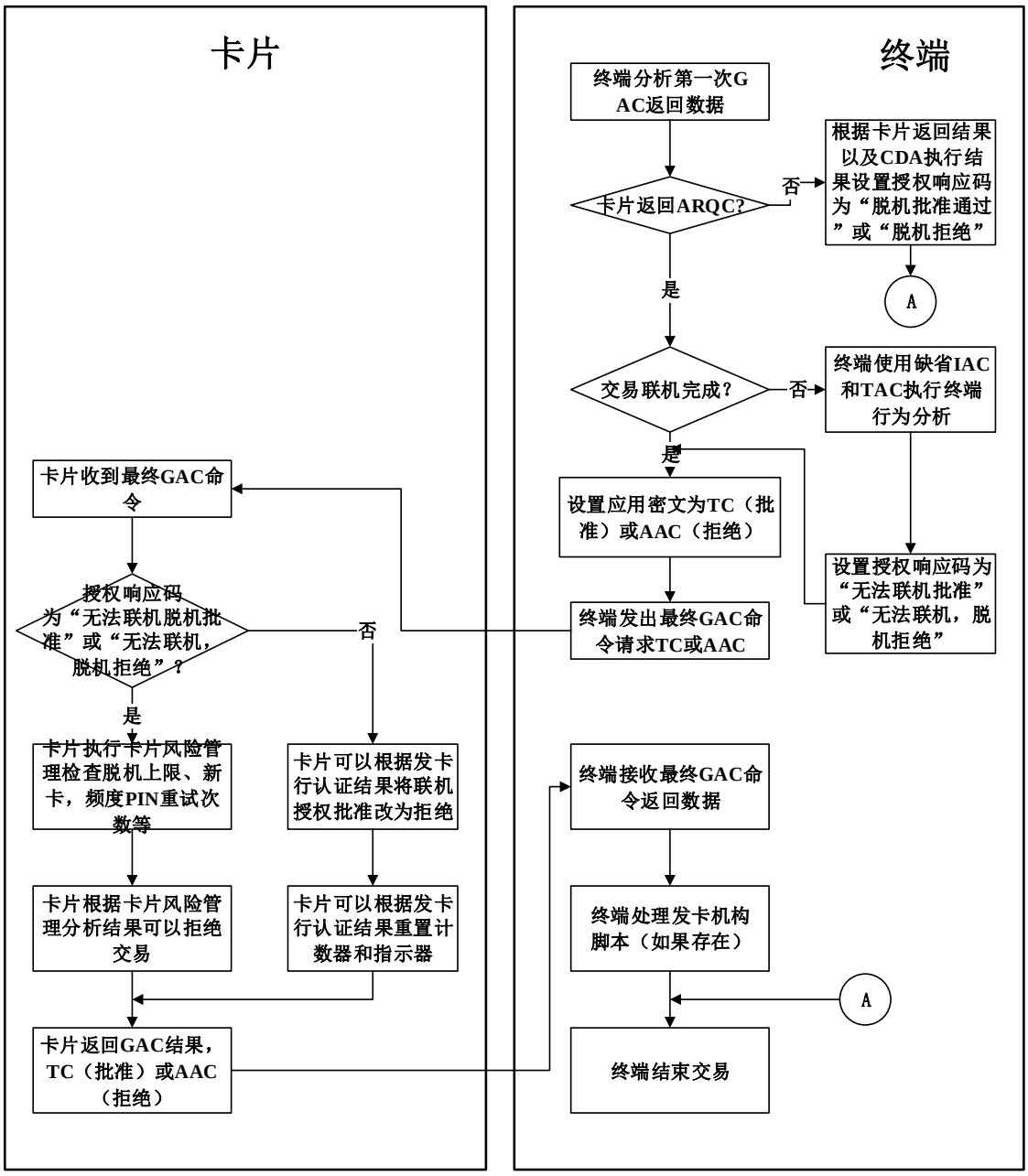


图18 交易结束处理流程图

8.1.2.11.7 前期相关操作

——联机处理

如果卡片收到终端发出的外部认证（EXTERNAL AUTHENTICATE）命令，则卡片开始进行发卡机构认证处理，同时设置指示器为发卡机构认证已执行并标识成功或失败。这些指示器将在完成处理期间被卡片用于卡片响应，并且决定哪些卡片计数器和指示器将被重置。

8.1.2.12 发卡机构脚本处理

8.1.2.12.1 描述

发卡机构脚本处理使得发卡机构不用二次发卡就可以改变卡片个人化数据。发卡机构在认证响应时在返回报文中包括了有卡片指令的脚本，终端在安全条件满足的情况下将这些指令发送给卡片。

支持的脚本命令如下：

——更改卡片参数；

——应用锁定/解锁；

——卡片锁定；

——重置 PIN 计数器；

——修改脱机 PIN。

发卡机构脚本处理通过可以锁定被盗或恶意透支卡来防止信用和欺诈风险。另外也可以根据持卡人的具体情况改变卡片参数。

8.1.2.12.2 脚本相关密钥

——报文鉴别码密钥

MAC Key是用来产生和验证命令脚本MAC的。MAC是包含在命令脚本中的密文，用于确认数据没有被篡改过（完整性），同时可以确认命令发出的发卡机构是否是合法（发卡机构认证）。MAC处理过程中用到了三个密钥：

1) MAC 主密钥（MAC MDK）：由发卡机构确定的唯一的双倍长对称密钥，用来产生卡片唯一的 MAC 认证密钥（MAC UDK）和交易 MAC 的过程密钥。
2) 卡片 MAC 子密钥（MAC UDK）：在卡片个人化时由 MAC 主密钥分散后写入卡片的双倍长对称密钥。MAC UDK 用来在交易过程中产生 MAC 过程密钥。
3) MAC 过程密钥：MAC 过程密钥是交易中唯一的双倍长对称密钥，用来在交易时产生脚本命令的 MAC 码。

——数据加密密钥

数据加密密钥用来加密脚本中的敏感数据，如脱机PIN等。数据加密用到三个密钥：

1) 数据加密主密钥（ENC MDK）：数据加密主密钥是发卡机构唯一的双倍长对称密钥，用于产生卡片唯一数据加密密钥以及交易的数据加密过程密钥。
2) 卡片数据加密子密钥（ENC UDK）：ENC UDK 是卡片个人化时由数据加密主密钥分散得到后写入卡片的双倍长对称密钥。用来产生数据加密过程密钥。
3) 数据加密过程密钥：数据加密过程密钥是交易中唯一的双倍长对称密钥，由 ENC MDK 分散而得到，用于发卡机构主机系统加密脚本中的敏感数据。

8.1.2.12.3 卡片数据

脚本处理过程中卡片使用到的计数器和指示器见表39。

表39 发卡机构脚本处理－卡片使用的计数器和指示器

数据元	描述
应用交易计数器（ATC）	自卡个人化以后处理的交易计数器，在终端频度检查中用到。
卡片验证结果（CVR）	根据本次和上次交易脱机处理结果进行设置的验证结果指示符。
发卡机构脚本命令计数器	记录第二次生成应用密文后卡片收到的有安全报文的指令的个数。在下次交易中的结束处理步骤中可能被复位。
发卡机构脚本失败指示器	如果脚本指令执行失败，指示位置“1”，失败的情况有： ——安全报文错误； ——安全报文通过但是指令执行失败； ——需要安全报文但是不存在。

	在下次交易中的结束处理步骤中可能被复位。

8.1.2.12.4 终端数据

发卡机构脚本处理过程中终端用到的数据元见表40。

表40 发卡机构脚本处理－终端使用的数据元

数据元	描述
发卡机构脚本结果	记录卡片对发卡机构脚本指令处理的结果，此结果要包括在清算报文和下次联机授权中。
终端验证结果（TVR）	TVR 中包括和脚本有关的两个指示位： ● 最后一个生成应用密文之前，发卡机构脚本失败； ● 最后一个生成应用密文之后，发卡机构脚本失败； 本部分只支持在最后一个生成应用密文命令之后，处理发卡机构脚本。
交易状态信息（TSI）	TSI 中包括一个表明执行发卡机构脚本处理标记。

8.1.2.12.5 联机响应数据

表41 发卡机构脚本处理－联机响应数据

数据元	描述
发卡机构脚本命令	脚本中的每一个发卡机构脚本指令都按照 BER-TLV 格式，用标签“86”开始。
发卡机构脚本标识	发卡机构用来唯一标识发卡机构脚本。
发卡机构脚本模板 2	仅支持发卡机构脚本模板 2。标签“72”标识模板 2，模板中包括在第二次生成应用密文指令后，传送给卡片的发卡机构专有脚本数据。

8.1.2.12.6 命令

——应用锁定（APPLICATION BLOCK）

该命令将锁定当前选择的应用。如果应用在交易过程中被锁定，卡片和终端将继续处理交易直到交易完成。在应用锁定之后，卡片将拒绝被锁的应用完成任何交易。终端可以选择被锁的应用，用于对该应用解锁。

——应用解锁（APPLICATION UNBLOCK）

该命令将已被锁定的应用解锁。对于发卡机构，应用解锁最好在专用设备上进行。

——卡片锁定（CARD BLOCK）

卡片锁定将使卡片上所有的应用永久锁定。

——PIN 修改/解锁（PIN CHANGE/UNBOLCK）

PIN修改/解锁命令可以让发卡机构在PIN解锁（重置PIN重试计数器）的同时更改卡片PIN。PIN修改/解锁应该在满足发卡机构安全要求的环境下进行。

——设置数据（PUT DATA）

PUT DATA命令数要用于更新卡片中由发卡机构设置的管理参数，如连续脱机交易次数上限、连续脱机交易次数下限、连续脱机国际交易限制、累计脱机交易总额上限等。

——修改记录（UPDATE RECORD）

修改记录命令用来修改文件中一条记录的内容。

8.1.2.12.7 处理流程

发卡机构脚本处理包括发卡机构脚本、命令执行、安全报文三方面。

——发卡机构脚本

发卡机构通过返回报文将发卡机构脚本发送给收单方。

发卡机构返回报文中如果包括标志“72”，标明在最终的GENERATE AC后需要执行发卡机构脚本

——命令执行

被推荐的发卡机构脚本命令用来处理本章先前说明的那些功能。只有命令支持安全报文，而且安全报文得以成功执行的情况下，卡片才执行被请求的命令来更新包含在卡里的数据。

在处理发卡机构脚本命令之前，发卡机构需要先成功地执行一些发卡机构认证方式。因为安全报文是一种发卡机构认证方式，所以通过为命令成功地执行安全报文，也可以满足此要求。卡片发卡机构承担着发卡机构脚本命令组织。如果一个不同于发卡机构的实体发起命令，也会发起同样的请求。

——安全报文

安全报文的原则目的是确保数据机密性，消息完整性以及发卡机构认证。数据机密性确保保密数据在从发卡机构到卡的传送中保持其秘密。消息完整性确保命令和命令数据在传送时没有被改变。发卡机构认证确保命令来自有效发卡机构。使用MAC来达到消息完整性以及发卡机构认证。使用对明文命令数据（如果有出现）的加密，来达到数据机密性。

8.1.2.12.8 流程图

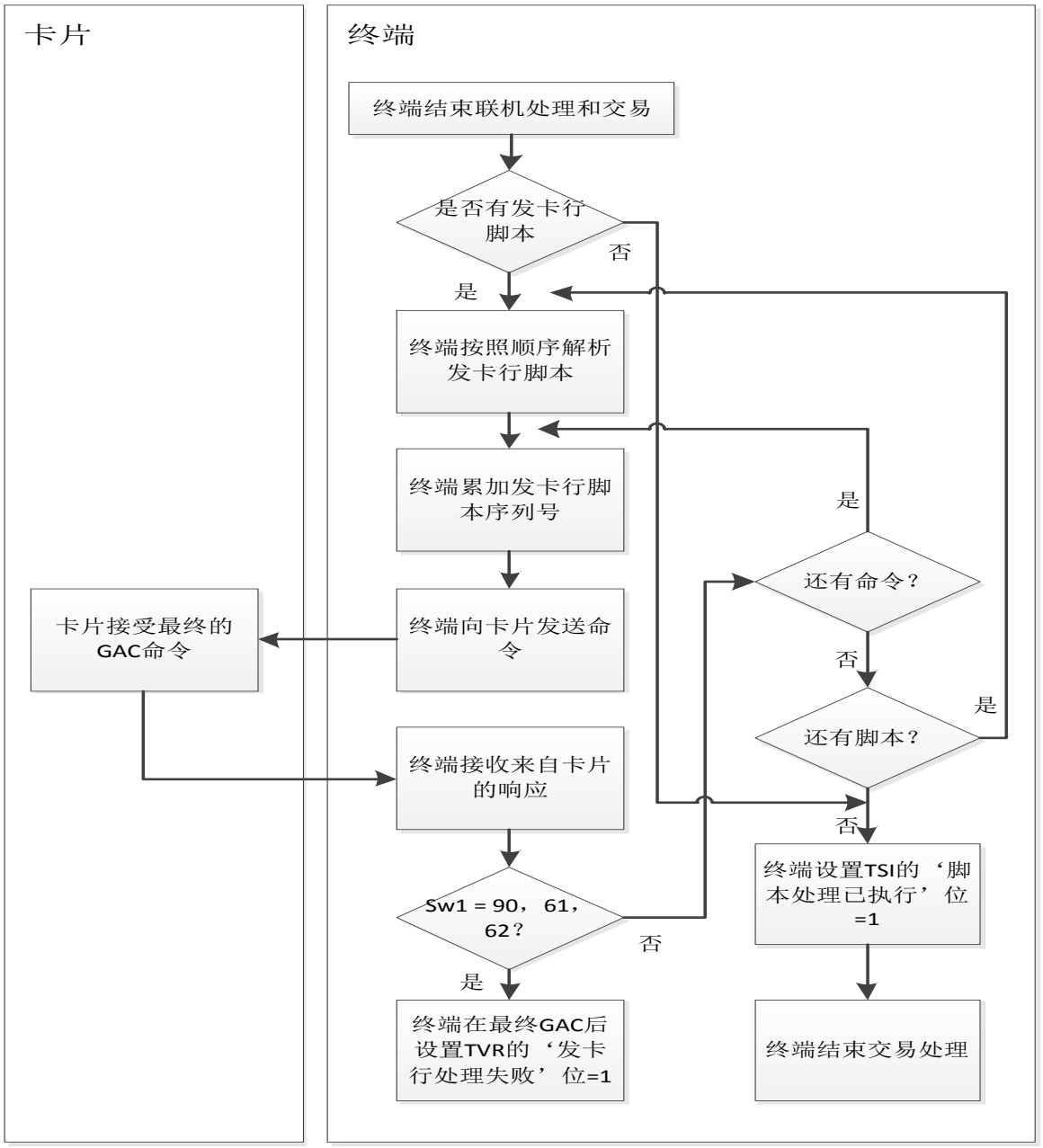


图19 发卡机构脚本处理流程图

8.1.2.12.9 前期相关操作

——联机处理

联机处理响应报文中可能包括需要在发卡机构脚本处理过程中处理的发卡机构脚本。

8.1.2.12.10 后续相关操作

——卡片行为分析（下一交易）

在下一交易的卡片行为分析时，卡片中的CVR子域将根据卡片中保存的上次交易发卡机构命令脚本失败指示器和发卡机构脚本命令计数器设置脚本运行结果。发卡机构将在下次清算记录和联机授权时收到卡片验证结果（CVR）。

——交易结束（下一交易）

当下列任何一种情况发生时，卡片将重置发卡机构脚本失败指示器和发卡机构脚本计数器为“0”：

1) 发卡机构认证成功；
2) 发卡机构认证为可选项，并且没有执行；
3) 不支持发卡机构认证。

当联机授权没有完成或发卡机构认证条件不满足时，发卡机构脚本失败指示器和发卡机构命令计数器将不会被重置。

8.1.2.13 卡片交易明细记录

8.1.2.13.1 描述

卡片可以支持交易明细记录，对于支持交易明细的卡片，在SELECT命令的响应中应包含日志入口（Log Entry）数据元，同时应支持终端通过GET DATA命令从卡片获取日志格式（Log Format）数据元，对于需要访问交易明细记录的终端可通过发送READ RECORD命令到卡片，逐条读取交易记录。

支持记录明细的卡片应通过DOL向终端获取记录交易明细所需要的终端数据元。当交易结束时，如果卡片批准交易通过并返回TC，卡片内部会记录此笔交易的交易明细供持卡人脱机查询。

交易明细是以循环记录文件形式保存在卡片的某一文件中，该交易明细文件的修改由卡片内部完成，终端只能对其进行读取操作。

8.1.2.13.2 交易明细数据元（推荐）

建议卡片交易明细中包含交易日期、交易时间、授权金额、其他金额、终端国家代码、交易货币代码、商户名称、交易类型、应用交易计数器等数据，具体格式见表42。

表42 卡片交易明细－数据格式

数据	格式	长度（字节）
交易日期	YYMMDD	3
交易时间	HHMMSS	3
授权金额	n12	6
其它金额	n12	6
终端国家代码	n3	2
交易货币代码	n3	2
商户名称	ans	20
交易类型	n2	1
应用交易计数器（ATC）	b	2

8.2 电子现金标准快速支付流程

标准快速支付交易一般由卡片进行脱机授权，与这些交易相关的清算操作使用电子现金账户。因此，圈存操作使电子现金账户金额增加，脱机交易清算使电子现金账户金额减少，电子现金闪卡处理流程参见附录C。

8.2.1 交易流程图

交易流程见图20和图21所示。

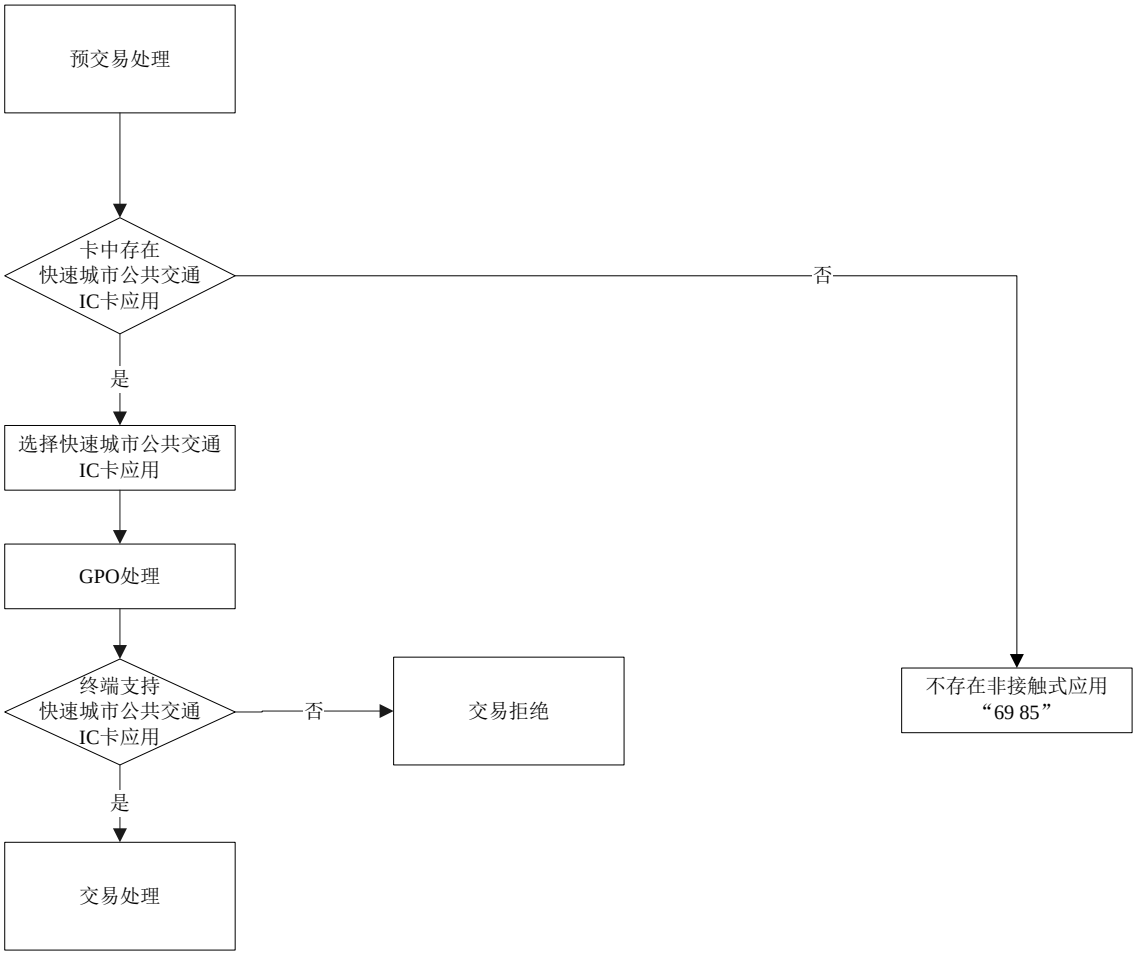


图20　交易流程图——总体流程

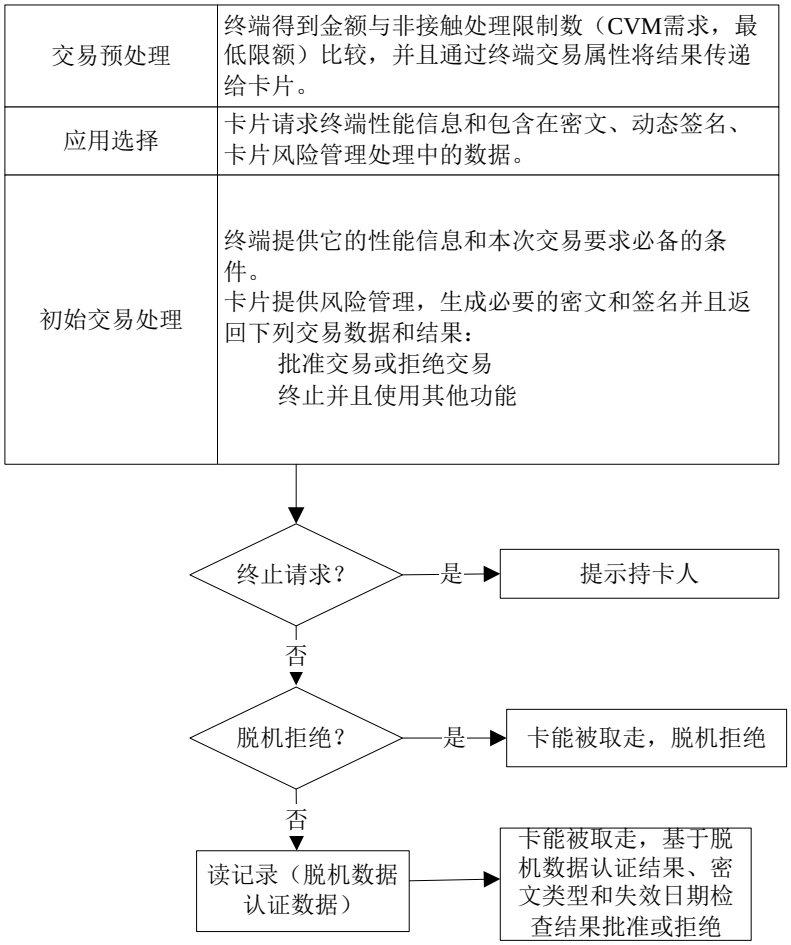


图21　交易流程图——处理流程概况

8.2.2　交易流程说明

8.2.2.1　有关 PDOL 内容的标准快速支付流程需求

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。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），详见表43和表44。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（标准快速支付交易和联机交易）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。发卡机构应当在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。

表43　密文版本 17 的标准快速支付的最基本要求

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

表44　密文版本 01 的标准快速支付的最基本要求

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） 为了 TVR 会被标准快速支付终端填为 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。

8.2.2.2 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）。

——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。

——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。响应数据按照卡片按JT/T XXX.1，格式化GPO响应，返回给终端。响应数据的具体内容参照本部分的表45。

表45 标准快速支付的 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	发卡机构应用数据 提供应用密文类型 。
“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，发卡机构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。 内容按照发卡机构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。

——标准快速支付推荐签名数据：

下面这些静态数据元推荐用于签名：

1) 应用 PAN；
2) 应用失效日期；
3) AIP；
4) SDA 标签列表。

8.2.2.3 标准快速支付的卡片需求

标准快速支付应当遵守下面的要求：

——收到 GPO 命令，卡片应当立即设置发卡机构应用数据（标签“9F10”）的 CVR 部分为“03000000”。CVR 是发卡机构应用数据的第 4—7 字节部分；

1) CVR 字节 2，位 4、3、2、1 未使用，仍保留设置为“0”
2) CVR 字节 3，位 8、4、3、2、1 未使用，仍保留设置为“0”
3) CVR 字节 4 未使用，所有位仍保留设置为“0”

——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；

——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。

——标准快速支付批准的交易，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。建议在这条记录中仅放置电子现金发卡机构授权码（9F74）。

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。

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。

8.2.2.4 标准快速支付终端需求

除了对于所有非接触应用的终端需求外，支持标准快速支付的终端还应当符合下面这些要求：

——终端应当支持 6.2.2 所描述的交易预处理；

——终端不应当查询 AIP 来决定卡片是请求联机交易或标准快速支付，而应默认标准快速支付处理；

——支持标准快速支付的终端应当按本部分规则读记录，并处理记录或 PDOL 中不认识的标签编码的数据元；

——如果标准快速支付必备数据元没有被 GPO 返回（见表 44），终端应当终止交易；

——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 AIP 中第 2 字节第 8 位为零，终端按如下处理：

1） 如果应用密文（标签“9F26”）没有出现在 GPO 响应中，终端应当终止交易；

2） 如果应用密文（标签“9F26”）出现在 GPO 响应中按标准快速支付处理。

——在如下的任何情形中，脱机数据认证失败：

1） AIP 中未指示支持 fDDA；

2） 或支持 fDDA，但 fDDA 要求的数据缺失。

8.2.2.5 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标准快速支付交易。

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。卡附加处理（标签“9F68”）的值及描述见JT/T XXX.1附录C。

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

——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：

a） 将匹配货币位（内部卡片指示器）设置为‘0’；

b） 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。

——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检查是标准快速支付的三种检查脱机消费的方法。根据电子现金相关数据（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’，继续进行的步骤见为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，则拒绝交易。

——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。

——小额检查

检查交易是否能够处理。

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）：

a) 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。

b) 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；

c) 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：拒绝交易。

——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。上文已讲述了货币检查，如果货币不匹配则见本条。

a) 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：

   1) 存储连续交易计数器的当前值（国际）；

   2) 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’。

   3) 连续交易计数器（国际—货币）加 1；

   4) 请求脱机批准；

   5) 继续见：完成脱机交易。

b) 如果前面的条件不满足’，那么卡片应当请求拒绝交易；

   1) 将 CVR 第 3 字节第 6 位置为‘1’（频度检查计数器超过）；

   继续见：拒绝交易。

——完成标准快速支付交易

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。

a) 卡片应当：

   1) 用终端提供的不可预知数作为终端动态数据，生成动态应用数据签名（SDAD—标签“9F4B”）；

   2) 返回一个指示 fDDA 所需数据的 SFI 和记录号的 AFL。

b) 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 JT/T XXX.1 附录 I 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 JT/T XXX.1 附录 I）。

c) 卡片应当根据卡片按 JT/T XXX.1 录 A 建立 GPO 响应；

   继续见：结束标准快速支付卡片的GPO处理。

——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。

a) 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；

b) 卡片应当在CVR中指示一个AAC密文，生成AAC密文，在GPO响应中包括CVR和密文以及相关数据；

c) 密文根据JT/T XXX.5要求产生。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JT/T XXX.1附录I）。

继续见：结束标准快速支付卡片的GPO处理。

——结束标准快速支付卡片的GPO处理

卡片JT/T XXX.1附录A的规定，格式化GPO响应，返回给终端。

——交易的READ RECORD命令处理

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。

a) 卡片应当能够知道最后一条记录被读取；

b) 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。

c) 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。

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。

——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。

8.2.2.6 标准快速支付终端处理需求

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

——如果返回ARQC（发卡机构应用数据（标签“9F10”）字节5的第6-5位=“10”），那么终端应拒绝交易，继续见终端脱机拒绝；

——如果返回AAC（发卡机构应用数据（标签“9F10”）字节5的第6-5位=“00”），那么终端应拒绝交易，继续见终端脱机拒绝；

——如果返回TC（发卡机构应用数据（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，继续见终端脱机拒绝；

——终端应根据JT/T XXX.1附录C的要求处理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JT/T XXX.1附录F的要求进行fDDA验证；

——如果 fDDA 失败，或者脱机数据认证未执行，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。后续见下文批准标准快速支付交易。

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。

批准标准快速支付交易：

——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。

8.3 电子现金分时分段扣费交易流程

为满足脱机小额快速支付应用中分时、分段计费的需求，在原来的标准快速支付功能应用交易流程的基础上，增加了READ CAPP DATA和UPDATE CAPP DATA CACHE命令用于扩展应用记录的读取和更新。符合本部分的卡片应支持多个分时、分段扣费交易同时存在并能进行处理。

交易扣款和扩展应用记录的更新应确保同时执行，在READ RECORD命令成功读取AFL中的最后一条记录时统一进行更新。分时扣费与分段扣费的交易机制类似，以下以分段扣费方式进行流程说明。

8.3.1 分段扣费交易流程图

分段扣费交易流程见图22和图23所示。

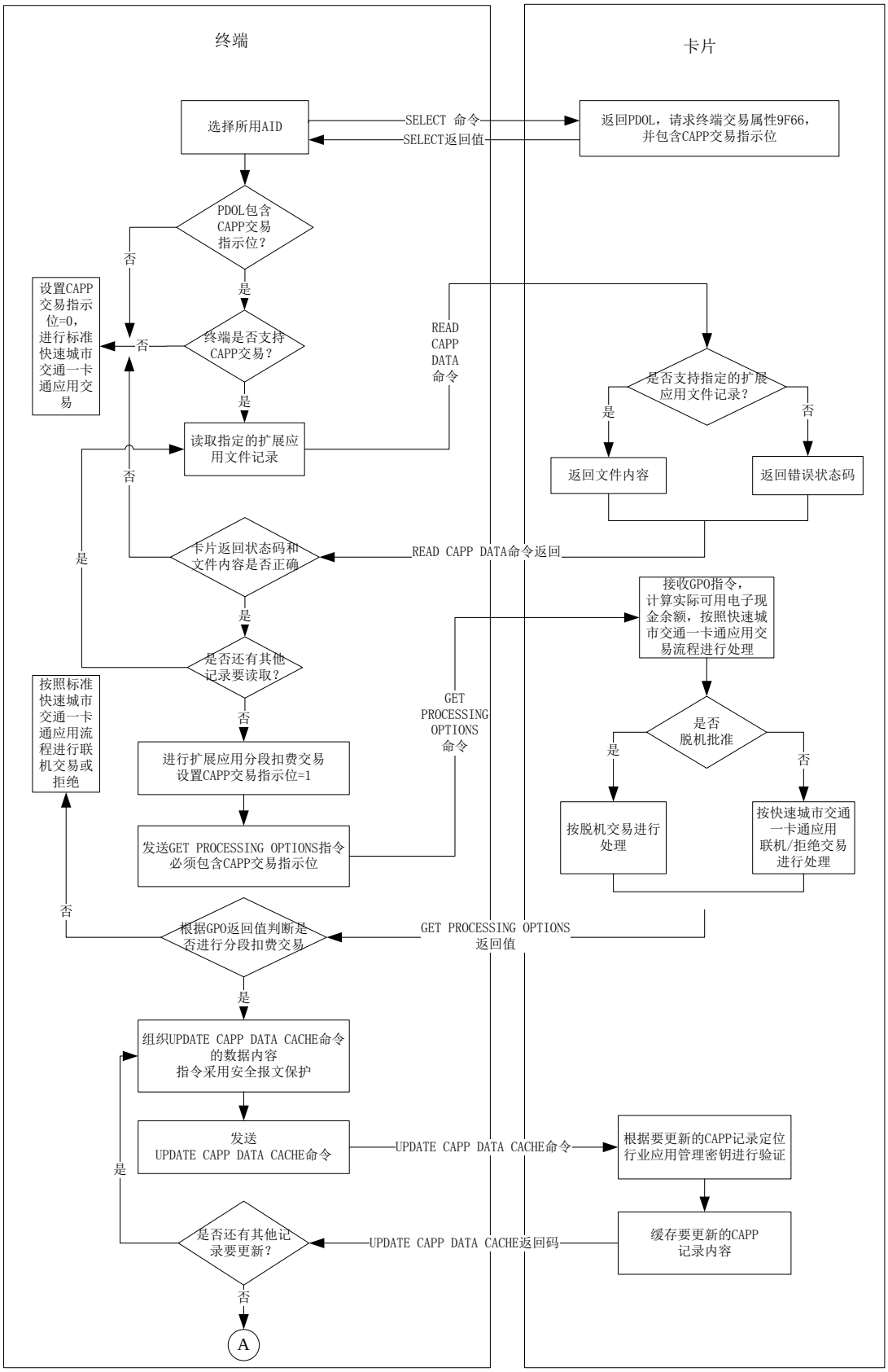


图22　分段扣费交易流程图 1

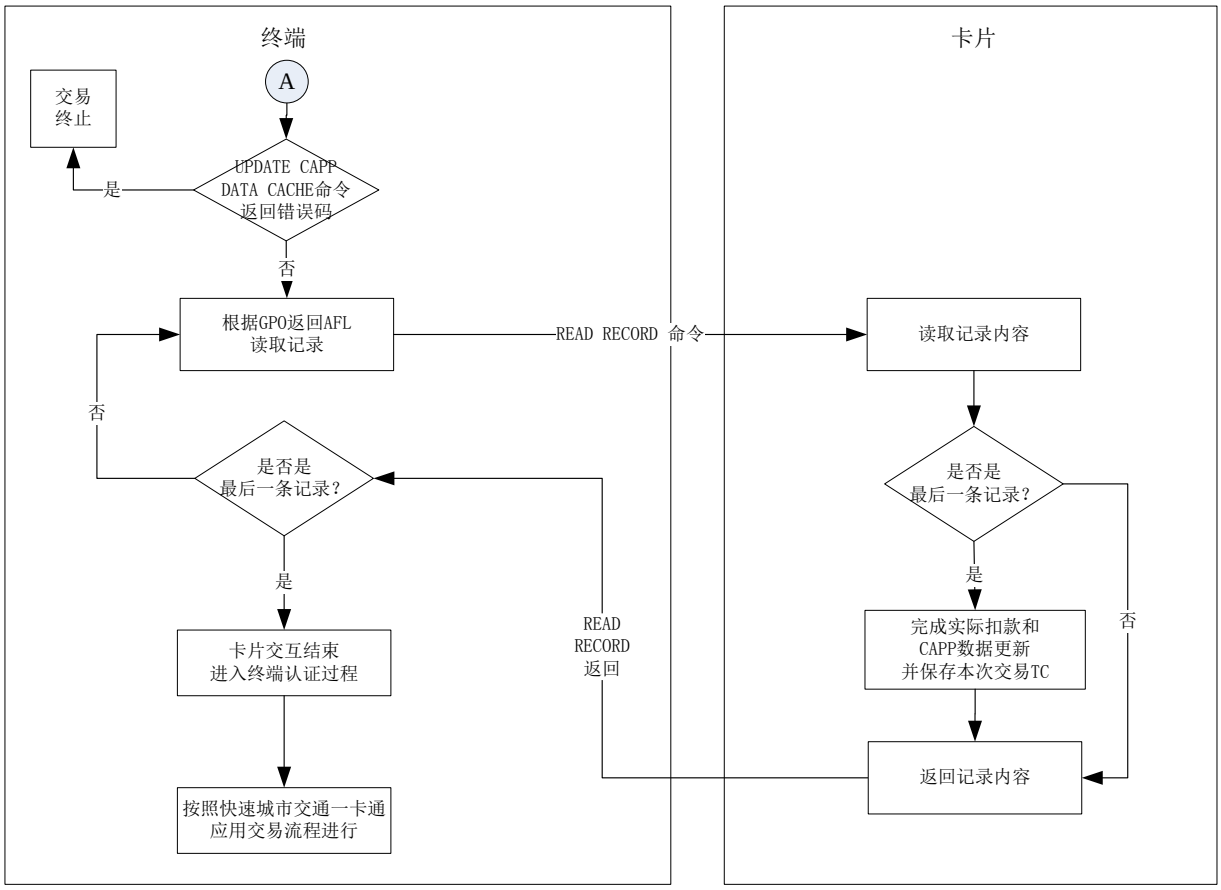


图23　分段扣费交易流程图 2

8.3.2　分段扣费交易流程说明

以下是基于非接触小额支付的分段扣费交易处理流程：

8.3.2.1　应用选择

终端按照公共交通 IC 卡应用交易流程要求，发送 SELECT PPSE 命令，选择 PPSE。根据卡片返回的应用信息和 AID，终端发送 SELECT 命令选择应用，卡片返回文件控制信息(FCI)，如果卡片支持 SM2 算法，则其中应包括请求 SM2 算法支持指示器（标签 DF69）和终端国家代码（标签 9F1A）的 PDOL。卡片返回的文件控制信息(FCI)中，包含分段扣费标识符（标签“DF61”）。如分段扣费标识符（标签“DF61”）字节 1 的第 1 位设置为‘1’，则表明卡片支持分段扣费应用；如分段扣费标识符（标签“DF61”）字节 1 的第 8 位设置为‘1’，则表明卡片支持扩展应用记录的 R-MAC 保护。

如果卡片返回的 FCI 中的 PDOL 数据中，包含 CAPP 交易指示位，终端将按如下流程进行交易处理：

a) 终端判断是否支持扩展应用：如是则继续进行后续处理；否则将 CAPP 交易指示位置“0”，进行标准快速支付交易或根据需要终止交易；

b) 终端可根据需要发送 READ CAPP DATA 命令读取指定的 CAPP 记录，以判断卡片是否支持特定扩展应用。如卡片支持扩展应用记录的 R-MAC 保护，则 READ CAPP DATA 的命令报文数据域中应包括 8 个字节的终端随机数；否则 READ CAPP DATA 命令报文数据域为空。

c) 如果卡片上存在指定的 CAPP 记录，则卡片返回文件内容。如卡片支持扩展应用记录的 R-MAC 保护，则终端应通过 SAM 卡计算并验证卡片返回的 R-MAC 值。如 R-MAC 验证错误，则终止交易。终端确认卡片支持特定的扩展应用，并将 CAPP 交易指示位置“1”，继续进行后续处理；如果卡

片上不存在指定的 CAPP 记录，则卡片返回错误状态码，表明卡片不支持特定扩展应用，终端将 CAPP 交易指示位置“0”，进行标准快速支付交易或根据需要终止交易。

d) 终端可以通过多条 READ CAPP DATA 指令，读取多个 CAPP 记录中的内容。

8.3.2.2 初始化应用

终端向卡片发送 GPO 指令，指令中的数据根据应用选择时返回的 PDOL 中的数据进行组织，需要包含 CAPP 交易指示位。

算法选择具体参见 JT/T XXX.5。

当收到 GPO 命令时，卡片将按如下流程顺序处理：

按标准快速支付交易处理，判断是否脱机批准该交易：如是，继续进行后续处理；否则，按标准快速支付功能联机/拒绝交易流程处理 GPO 命令：

——如果 CAPP 交易指示位为“1”，进入分段扣费交易流程；

——如果当前实际可用电子现金余额小于当前交易金额，则进入标准快速支付功能流程，判断拒绝交易还是请求联机；如果当前实际可用电子现金余额大于等于当前交易金额，则以当前实际可用电子现金余额替代电子现金余额（9F79）进行小额检查等相关操作（预付处理除外，仍使用电子现金余额（9F79）作为判断依据）。

8.3.2.3 分段扣费处理

收到 GPO 命令响应数据后卡片将作如下处理：

——根据 UPDATE CAPP DATA CACHE 命令所指示的文件记录查找相应的行业应用管理密钥，计算并验证安全报文；

——如果安全报文验证成功后，将 CAPP 记录数据缓存，待交易完成时一起写入卡片；

——如果安全报文验证失败，返回指定错误码。

终端将作如下处理：

——终端组织更新 CAPP 记录的内容，通过保存在 SAM 卡中制定行业文件所对应的密钥，计算相应的 MAC，对 UPDATE CAPP DATA CACHE 指令进行安全保护；

——终端发送 UPDATE CAPP DATA CACHE 命令。允许根据实际应用，发送多条 UPDATE CAPP DATA CACHE 命令；

——如果卡片支持扩展应用记录的 R-MAC 保护，则终端应通过 SAM 卡计算并验证 UPDATE CAPP DATA CACHE 命令后卡片返回的 R-MAC 值。如 R-MAC 验证错误，或卡片返回错误的状态码，或未返回 R-MAC，则终端均应终止此次分段扣费交易。

——如果卡片不支持扩展应用记录的 R-MAC 保护，则当 UPDATE CAPP DATA CACHE 命令返回错误码时，终端应终止此次分段扣费交易。

8.3.2.4 读取卡片数据内容

终端根据 GPO 返回的 AFL，向卡片发送 READ RECORD 命令，读取相应的记录内容。在最后一条记录被成功读取后，卡片同时完成小额支付的扣款和 CAPP 记录的实际更新,终端获得并保存本次交易应用密文（TC），交易正常完成。

8.3.2.5 结束处理

终端执行交易结束步骤(即终端认证过程)决定交易处理结果(交易拒绝或交易批准)。包括下列步骤：

——检查所有相关数据的有效性和合法性；

——进行脱机数据认证，即 fDDA 验证。

如果卡片的 fDDA 版本号为“01”，则卡片在产生动态签名前应将分段扣费应用标识（DF61）的值动态填充到卡片认证相关数据（9F69）的第 8 个字节中再进行动态签名的运算。终端在 fDDA 验证成功后应将卡片认证相关数据（9F69）的第 8 字节与应用选择时卡片返回的 FCI 数据中的分段扣费应用标识（DF61）相比较，如比较不一致，则应提示交易失败。

8.3.2.6 支持分段扣费押金抵扣功能的特殊处理

在分段扣费交易模式下，发卡机构可选择支持押金抵扣功能，并需在个人化时增加分段扣费抵扣限额（DF62）和分段扣费已抵扣金额（DF63）两个数据。同时，在标准分时、分段扣费交易的部分流程中，对具有押金抵扣功能的卡片进行如下特殊处理。

a） 应用选择

对于支持押金抵扣交易的终端，在进行交易前，应获取电子现金余额（9F79）进行校验。如果当前电子现金余额（9F79)大于 0，终端继续交易；如果当前电子现金余额（9F79）等于 0，表示卡内余额为 0 或者已经进行过押金抵扣交易，终端可根据自身业务逻辑决定继续交易或者终止交易。

b） 初始化应用

当收到 GPO 命令，进入分段扣费流程时，如果卡片支持分段扣费押金抵扣功能，则当前实际可用电子现金余额=电子现金余额（9F79）+分段扣费抵扣限额（DF62）-分段扣费已抵扣金额（DF63）；如果卡片不支持分段扣费押金抵扣功能，则当前实际可用电子现金余额=电子现金余额（9F79）。

c） 读取卡片数据内容

终端根据 GPO 返回的 AFL，向卡片发送 READ RECORD 命令时，如果卡片支持押金抵扣功能，且电子现金余额（9F79）小于当前交易金额，则进行押金抵扣，交易后的分段扣费已抵扣金额（DF63）=交易前分段扣费已抵扣金额（DF63）+ 交易金额 - 交易前电子现金余额（9F79）。如果交易后的分段扣费已抵扣金额（DF63）小于电子现金分段扣费抵扣限额（DF62），则在最后一个记录被成功读取后，将交易后的分段扣费已抵扣金额（DF63）进行更新，同时将交易后的电子现金余额（9F79）设置为零，完成交易；否则交易失败。

d） 圈存操作

发卡机构后台圈存流程保持与现有流程一致。

卡片收到发卡机构发送的修改余额的脚本命令时，需自动计算并同时设置电子现金余额（9F79）和分段扣费已抵扣金额（DF63）。

——如果当前电子现金余额（9F79）等于 0：

1） 当修改余额脚本中指定的金额大于分段扣费已抵扣金额（DF63），则圈存后的电子现金余额（9F79）= 修改余额脚本中指定的金额 - 分段扣费已抵扣金额（DF63），同时将分段扣费已抵扣金额（DF63）清零；

2） 当修改余额脚本中指定的金额小于等于分段扣费已抵扣金额（DF63），则圈存后的分段扣费已抵扣金额（DF63）= 圈存前分段扣费已抵扣金额（DF63）- 修改余额脚本中指定的金额，电子现金余额（9F79）值保持不变；

——如果当前电子现金余额（9F79）大于 0，按标准圈存流程处理。

e） 查询操作

——标准终端只能支持电子现金余额（9F79）的查询；

——支持分段扣费押金抵扣功能的终端，可单独查询电子现金余额（9F79）、分段扣费抵扣限额（DF62）与分段扣费已抵扣金额（DF63），根据实际业务需求显示查询余额。

f） 更新分段扣费抵扣限额操作

——卡片收到发卡机构发送的修改分段扣费抵扣限额（DF62）的脚本命令时，如果修改分段扣费抵扣限额的脚本中指定的分段扣费抵扣限额（DF62）小于分段扣费已抵扣金额（DF63），则返回 6A80；否则，用脚本中指定的值完成分段扣费抵扣限额（DF62）的更新。

8.4 电子现金脱机预授权交易流程

脱机预授权是特殊形式的分时、分段扣费交易，分为脱机预授权和脱机预授权完成两个步骤：在脱机预授权时，冻结一部分电子现金余额作为预授权金额；在脱机预授权完成时，完成实际消费金额的扣款和冻结金额的恢复。脱机预授权交易不支持押金抵扣功能。

8.4.1 脱机预授权交易流程图

脱机预授权交易见图24和图25所示。

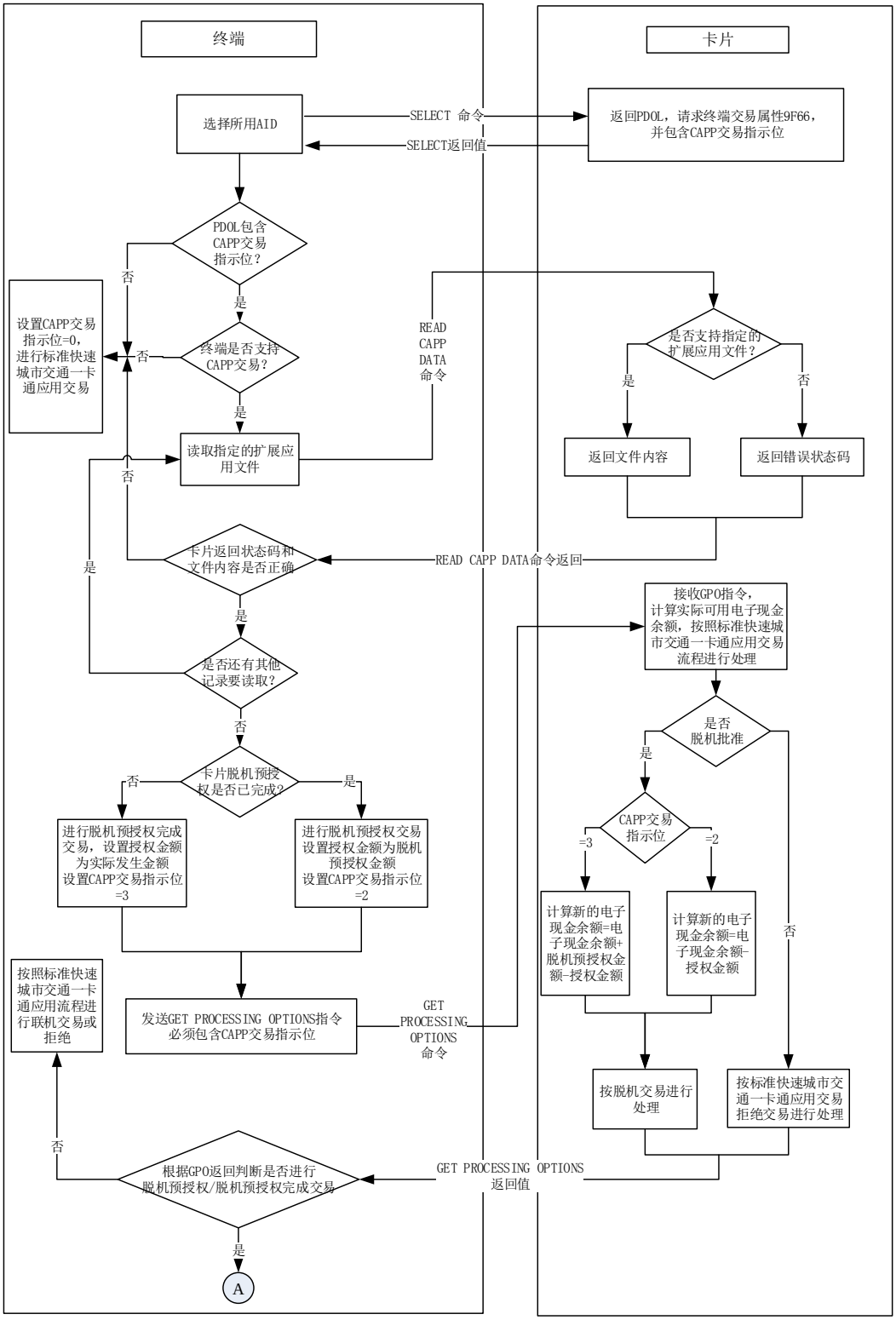


图24　脱机预授权交易流程图 1

图25　脱机预授权交易流程图 2

8.4.2　脱机预授权交易流程说明

以下是基于非接触小额支付的脱机预授权交易的处理流程：

8.4.2.1　应用选择

终端按照快速支付交易流程要求，发送 SELECT PPSE 命令，选择 PPSE。根据卡片返回的应用信息和 AID，终端发送 SELECT 命令选择应用，卡片返回文件控制信息(FCI)。卡片返回的文件控制信息(FCI)中，包含分段扣费标识符（标签“DF61”）。如分段扣费标识符（标签“DF61”）字节 1 的第 2 位设置为‘1’，则表明卡片支持脱机预授权功能；如分段扣费标识符（标签“DF61”）字节 1 的第 8 位设置为‘1’，则表明卡片支持扩展应用记录的 R-MAC 保护。如果 FCI 数据中要求的 PDOL 数据中，包含 CAPP 交易指示位，终端将按顺序作如下处理：

a) 判断终端是否支持脱机预授权应用：如是则继续进行后续处理，否则将 CAPP 交易指示位置“0”，进行标准快速支付交易或根据需要终止交易；
b) 终端发送 READ CAPP DATA 命令读取指定的扩展应用专用文件记录，或发送 READ RECORD 命令读取指定的扩展应用循环记录文件，以判断卡片是否支持脱机预授权应用。如卡片支持扩展应用记录的 R-MAC 保护，则 READ CAPP DATA 的命令报文数据域中应包括 8 个字节的终端随机数；否则 READ CAPP DATA 命令报文数据域为空。
c) 如果卡片上存在指定的脱机预授权应用文件，则卡片返回文件内容，终端确认卡片支持指定的脱机预授权应用。如卡片支持扩展应用记录的 R-MAC 保护，则终端通过 SAM 卡计算并验证卡片返回的 R-MAC 值。如 R-MAC 验证错误，则终止交易；
d) 如果卡片上不存在指定的 CAPP 记录，则卡片返回错误状态码，表明卡片不支持脱机预授权应用，终端并将 CAPP 交易指示位置“0”，进行标准快速支付交易或根据需要终止交易；
e) 终端根据读取的指定脱机预授权应用数据中的脱机预授权状态、脱机预授权金额和脱机预授权日期或者有效期判断卡片脱机预授权是否已完成，从而确定本次交易的具体子类型，（脱机预授权应用文件中的数据由行业定义，但是建议包括脱机预授权状态、脱机预授权金额和脱机预授权日期或者有效期），具体判断规则由相关行业根据实际需要自行设定；
f) 如果判断本次交易为脱机预授权交易，则终端设置 CAPP 交易指示位为“2”，并设置授权金额为新的脱机预授权金额，进行新的脱机预授权交易；如果判断结果为脱机预授权完成交易，则终端设置 CAPP 交易指示位为“3”，并设置授权金额为实际发生的交易金额，进行脱机预授权完成交易。

8.4.2.2 初始化应用

终端向卡片发送 GPO 指令，当收到 GPO 命令时，卡片将按如下顺序进行处理：

a) 在交易类型为脱机预授权完成时，参与卡片风险管理的电子现金余额应为当前电子现金余额加上脱机预授权金额，按照快速支付功能规定的卡片风险管理判断是否脱机批准该交易：如是，继续进行后续处理；否则按标准快速支付联机/拒绝交易流程处理 GPO 命令；
b) 判断 GPO 命令数据域中是否包含 CAPP 交易指示位，且设置为“2”或者“3”。如果 CAPP 交易指示位为“2”，计算新的电子现金余额=电子现金余额-脱机预授权金额，在卡片内部记录脱机预授权金额，用于脱机预授权完成交易（目前同时支持 3 个脱机预授权交易，对应 3 个不同的内部脱机预授权金额，如果卡片收到第 4 个脱机预授权交易的 GPO 命令时，则卡片返回‘6971’）；如果 CAPP 交易指示位为“3”，计算新的电子现金余额=电子现金余额+脱机预授权金额-脱机预授权完成金额；

——如果 CAPP 交易指示位为“2”，对于同一行业的同一应用（即相同 SFI 的扩展应用文件下相同 ID 的记录）不允许连续脱机预授权交易发生，如果卡片收到连续脱机预授权交易，则返回‘6972’；

——如果 CAPP 交易指示位为“3”，但是卡片无对应脱机预授权交易，则卡片返回‘6973’；

与标准快速支付交易流程不同，如果交易是脱机预授权交易，则卡片在脱机交易批准的情况下不返回应用密文（TC）。

8.4.2.3 脱机预授权处理

收到 GPO 命令响应数据后进入脱机预授权交易后，

卡片将作如下处理：

——根据 UPDATE CAPP DATA CACHE 命令所指示的文件记录查找相应的行业应用管理密钥，计算并验证安全报文；

——如果安全报文验证成功，将 CAPP 记录数据缓存，待交易完成时一起写入卡片；

——如果安全报文验证失败，返回指定错误码。

终端将作如下处理：

——当脱机预授权完成交易和脱机预授权交易发生在同一终端上时，终端使用脱机预授权完成交易生成的交易数据覆盖脱机预授权交易数据，对于以上两笔相关交易，终端只保存一条脱机预授权完成的交易记录；

——对于脱机预授权交易和脱机预授权完成交易，终端更新 CAPP 记录，具体更新内容细节由行业应用方定义；

——终端应通过 SAM 卡计算相应的 MAC，对 UPDATE CAPP DATA CACHE 指令进行安全保护；

——发送 UPDATE CAPP DATA CACHE 命令。允许根据实际应用，发送多条 UPDATE CAPP DATA CACHE 命令；

——如果卡片支持扩展应用记录的 R-MAC 保护，则终端应通过 SAM 卡计算并验证 UPDATE CAPP DATA CACHE 命令后卡片返回的 R-MAC 值。如 R-MAC 验证错误，或卡片返回错误的状态码，或未返回 R-MAC，则终端均应终止此次脱机预授权交易。

——如果卡片不支持扩展应用记录的 R-MAC 保护，则当 UPDATE CAPP DATA CACHE 命令返回错误码时，终端应终止此次脱机预授权交易。

8.4.2.4 读取卡片数据内容

——终端根据 GPO 返回的 AFL，向卡片发送 READ RECORD 命令，读取相应的记录内容；

——卡片应在验证 UPDATE CAPP DATA CACHE 指令中的 MAC 成功后，方允许更新余额；

——在最后一个记录被成功读取后，卡片检测当前 UPDATE CAPP DATA CACHE 所更新的 CAPP 记录是否与最后一条 READ CAPP DATA 的 CAPP 记录一致（即相同 SFI 的扩展应用文件下相同 ID 的记录），且更新成功。如果是，卡片同步完成脱机预授权金额的处理、电子现金余额的更新和 CAPP 记录的实际更新，并保存本次交易应用密文（TC），交易正常完成；如果否，卡片在最后一条记录时，返回‘6974’，交易失败；

8.4.2.5 结束处理

终端执行交易结束步骤(即终端认证过程)决定交易处理结果(交易拒绝或交易批准)。包括下列步骤：

——检查所有相关数据的有效性和合法性；

——进行脱机数据认证，即 fDDA 验证；

——终端在完成脱机数据认证后，保存所有相关交易信息，以便上传。建议相关信息应包含脱机预授权交易发生终端的终端编号和商户编号，以及脱机预授权完成的本机相关信息。

如果卡片的 fDDA 版本号为“01”，则卡片在产生动态签名前应将分段扣费应用标识（DF61）的值动态填充到卡片认证相关数据（9F69）的第 8 个字节中再进行动态签名的运算。终端在 fDDA 验证成功后应将卡片认证相关数据（9F69）的第 8 字节与应用选择时卡片返回的 FCI 数据中的分段扣费应用标识（DF61）相比较，如比较不一致，则应提示交易失败。

8.4.2.6 脱机预授权完成交易时的特殊处理

——脱机预授权完成交易时，如果脱机预授权完成金额大于等于脱机预授权金额，则电子现金余额=电子现金余额+脱机预授权金额-脱机预授权完成金额；

——脱机预授权完成交易时，如果脱机预授权完成金额小于脱机预授权金额，且分段扣费已抵扣金额（DF63）大于零，脱机预授权剩余金额 = 脱机预授权金额 - 脱机预授权完成金额；

——如果脱机预授权剩余金额大于分段扣费已抵扣金额（DF63），则将分段扣费已抵扣金额（DF63）清零，同时设置当前电子现金余额（9F79）= 脱机预授权剩余金额 - 分段扣费已抵扣金额（DF63）；如果脱机预授权剩余金额小于等于分段扣费已抵扣金额（DF63），则设置当前分段

扣费已抵扣金额（DF63）= 交易前分段扣费已抵扣金额（DF63）- 脱机预授权剩余金额。

8.4.2.7 脱机预授权未完成状态下的圈存与查询操作

——圈存操作

1) 发卡机构后台圈存流程与现有流程保持一致；
2) 为了避免圈存时发卡机构下发圈存脚本导致卡片金额超限，卡片在收到 GENERATE AC 指令后，返回的发卡机构应用数据（9F10）中如包含发卡机构自定义数据项，则卡片在计算发卡机构自定义数据项时，所使用的电子现金余额= 当前电子现金余额（9F79）+ 卡片未完成的一笔或多笔脱机预授权金额的总和；
3) 为了避免圈存后由于预授权完成交易导致卡片内电子现金余额（9F79）超限，卡片在收到 PUT DATA 指令进行圈存操作时，需要确保电子现金余额上限（9F77）大于等于 PUT DATA 指令设置的电子现金余额（9F79）+ 卡片未完成的一笔或多笔脱机预授权金额的总和，否则卡片以‘6A80’错误码响应 PUT DATA 指令。

——查询操作

1) 终端查询电子现金余额（9F79）流程与现有流程保持一致；

通过 GET DATA 指令或 GPO 指令获取的电子现金余额（9F79）或可用脱机消费金额（9F5D）均为当前实际可用金额，不包括未完成的一笔或多笔脱机预授权的金额。

8.5 电子现金单次扣款优惠流程

单次扣款优惠是指在交易时根据读取的扩展应用专用文件信息,判断卡片是否需要进行优惠处理的过程。单次扣款优惠多用于公交换乘优惠、学生卡、老人卡等场景。

——描述

单次扣款优惠交易的基本流程为：读取扩展应用专用文件，判断卡片是否支持优惠应用，若支持，判断优惠时间是否未过期；若是，则按优惠规则计算消费金额，并继续进行优惠交易的其它步骤。

——流程图

单次扣款优惠交易流程见图 26 和图 27 所示。

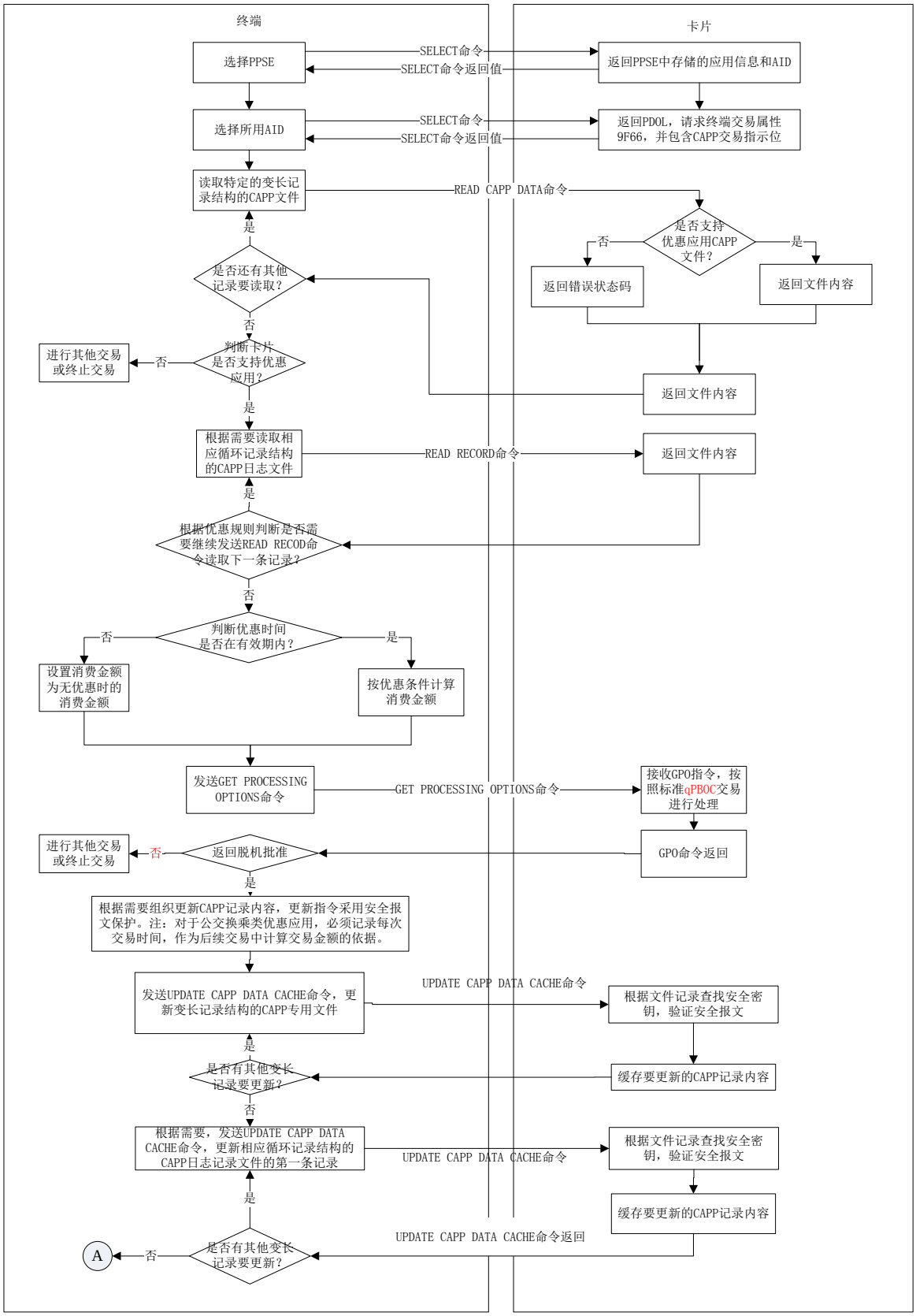


图26　单次扣款优惠交易流程 1

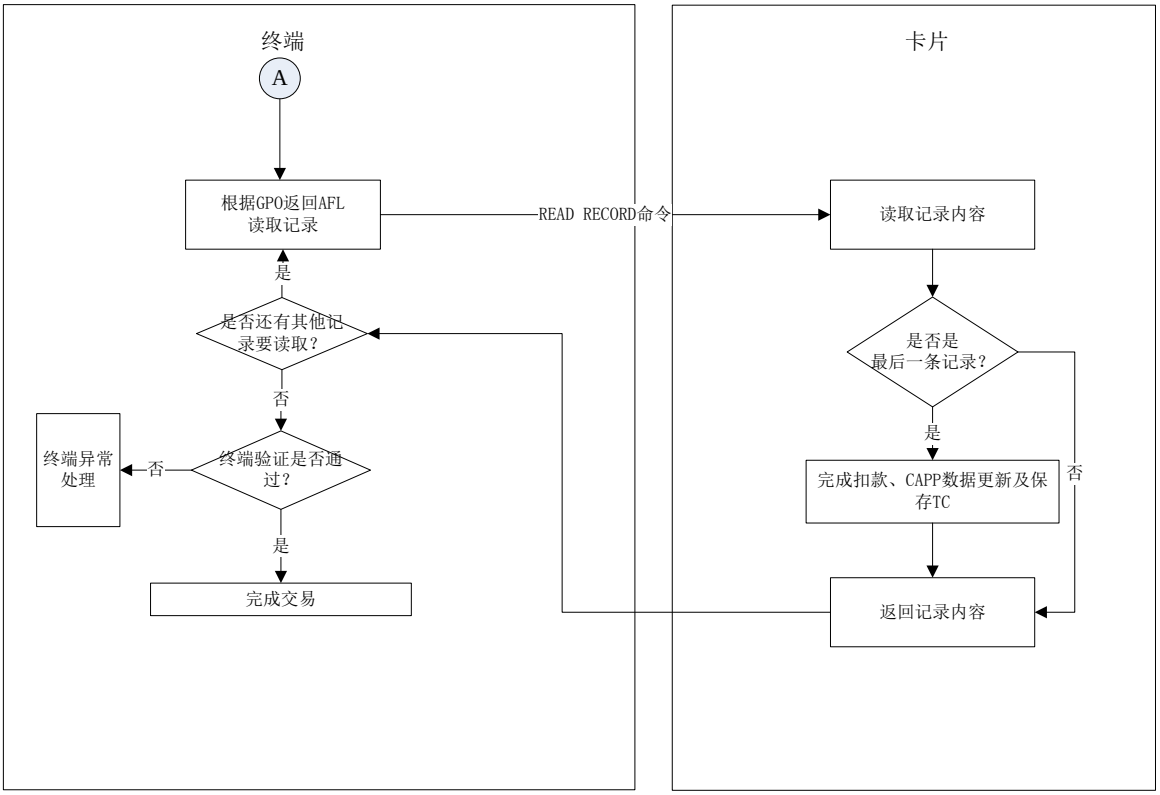


图27　单次扣款优惠交易流程 2

注：对单次扣款优惠可能追溯最近一次或多次的交易记录（例如公交换乘），故除通用的记录优惠应用的CAPP变长记录文件外，可额外增加一个使用循环记录文件结构的CAPP日志记录文件。两个文件配合使用，灵活实现不同的优惠方案。

——流程说明

持卡人使用公共交通 IC 卡在优惠应用环境中进行单次扣款优惠交易时，终端将作如下处理：

1) 终端首先选择和激活卡片，并通过返回信息选择判断卡片是否支持基于非接触小额支付的扩展应用交易。
2) 终端发出 READ CAPP DATA 命令查询变长记录结构的优惠应用 CAPP 专用文件，判断卡片是否支持优惠应用。如支持，终端根据需要发送一条或多条 READ RECORD 命令读取循环记录结构的日志记录 CAPP 专用文件中的记录内容：如优惠规则中指明优惠需要参考最近的多次交易，则终端需要读取循环文件中的最近几条记录，作为消费金额计算的依据，否则只需读取最近一次的日志记录作为依据；如果不满足优惠条件，则交易金额为无优惠的标准值，否则根据优惠规则计算消费金额，然后进入扣费交易流程。
3) 支持优惠的终端可通过追溯最近几次的消费情况来计算优惠消费金额。但应避免设计得过于复杂，以免影响交易速度。

注：如卡片支持扩展应用记录的R-MAC保护，则终端应通过SAM卡计算并验证R-MAC。具体方法同分段扣费和脱机预授权交易流程中描述。

9　电子钱包交易流程

9.1　电子钱包圈存交易

通过圈存交易，持卡人可将其指定的资金存入电子钱包中。

9.1.1 发出初始化圈存（INITIALIZE FOR LOAD）命令（步骤1）

终端应按JT/T XXX.1附录A中的描述,发出初始化圈存（INITIALIZE FOR LOAD命）令,启动圈存交易。

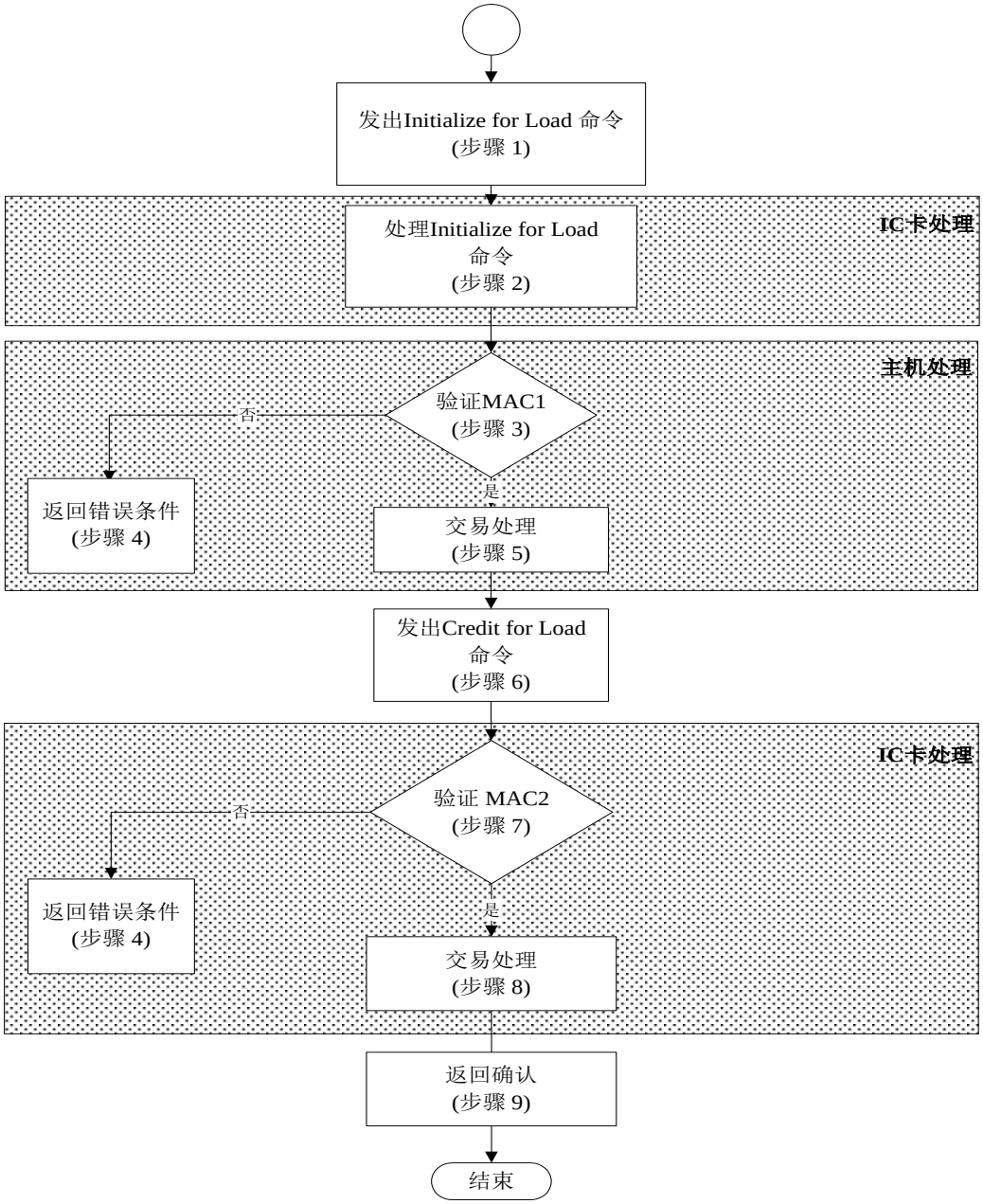


图28 圈存交易处理流程

9.1.2 处理初始化圈存（INITIALIZE FOR LOAD）命令（步骤2）

收到初始化圈存（INITIALIZE FOR LOAD）命令后，IC卡将进行以下操作：

——检查是否支持命令中包含的密钥索引号。如果不支持，则回送状态字“9403”（不支持的密钥索引），但不回送任何其他数据，同时终止命令的处理过程；

——产生一个伪随机数（ICC），过程密钥和一个报文鉴别码（MAC1），用以供主机验证圈存交易及IC卡的合法性。

过程密钥用于电子钱包圈存交易。该过程密钥是用DLK密钥按照JT/T XXX.5描述的机制产生的。用来产生过程密钥的输入数据如下：

伪随机数（ICC）||电子钱包联机交易序号||“8000”

MAC1的计算机制见JT/T XXX.5定义的内容。用过程密钥对以下数据加密产生MAC1（按所列顺序）：

——电子钱包余额（交易前）；

——交易金额；

——交易类型标识；

——终端机编号。

IC卡将把JT/T XXX.1附录A中定义的初始化圈存（INITIALIZE FOR LOAD）响应报文回送给终端处理。如果IC卡回送的状态字不是“9000”，则交易终止。

9.1.3 验证 MAC1（步骤 3）

收到初始化圈存（INITIALIZE FOR LOAD）命令响应报文后，终端把JT/T XXX.1附录A中定义的数据传给发卡方主机。主机将生成过程密钥并确认MAC1是否有效。如果MAC1有效，交易处理将按8.1.5中描述的步骤继续执行。否则，交易处理将执行8.1.4中所描述的步骤。

9.1.4 回送错误状态（步骤 4）

如果不接受圈存交易，则主机应通知终端。回送给终端的报文格式和内容，以及终端所做的处理不在本部分范围内。

9.1.5 交易处理（步骤 5）

主机产生一个报文签别码（MAC2），用于IC卡对主机进行合法性检查。JT/T XXX.5中描述了主机用来生成MAC2的机制。用过程密钥对以下数据加密产生MAC2（按所列顺序）：

——交易金额；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

成功地进行了圈存交易后，主机将电子现金交易序号加1，并向终端发送一个圈存交易接受报文，其中包括MAC2、交易日期（主机）和交易时间（主机）。

9.1.6 发出圈存（CREDIT FOR LOAD）命令（步骤 6）

终端收到主机发来的圈存交易接受报文后，发出圈存（CREDIT FOR LOAD）命令更新卡上电子钱包余额。圈存（CREDIT FOR LOAD）命令见JT/T XXX.1附录A中的描述。

9.1.7 验证 MAC2（步骤 7）

收到圈存（CREDIT FOR LOAD）命令后，IC卡应确认MAC2的有效性。如果MAC2有效，交易处理将执行9.1.8中描述的步骤。否则将向终端回送状态字“9302”（MAC无效）。终端对错误所应采取的相应措施不在本部分范围内。

9.1.8 交易处理（步骤 8）

IC卡将电子钱包交易序号加1，并且把交易金额加在电子钱包的余额上。IC卡应成功地完成以上所有操作或者一个也不完成。

在电子钱包圈存交易中，IC卡用以下数据组成的一个记录更新交易明细：

——电子钱包交易序号；
——交易金额；
——交易类型标识；
——终端机编号；
——交易日期（主机）；
——交易时间（主机）。

TAC的计算机制见JT/T XXX.5。TAC的计算不采用过程密钥方式，它用DTK左右8位字节异或运算的结果对以下数据进行加密运算来产生（按所列顺序）：

——电子钱包余额（交易后）；
——电子钱包交易序号（加 1 前）；
——交易金额；
——交易类型标识；
——终端机编号；
——交易日期（主机）；
——交易时间（主机）。

9.1.9 返回确认（步骤 9）

在成功完成步骤8后，IC卡通过CREDIT FOR LOAD命令的响应报文将TAC回送给终端。主机可以不马上验证TAC。

9.2 电子钱包圈提交易

通过圈提交易，持卡人可以把电子现金中的全部资金取回。圈提交易只能在特定终端上联机进行。

9.2.1 发出初始化圈提（INITIALIZE FOR UNLOAD）命令（步骤 1）

终端发出初始化圈提（INITIALIZE FOR UNLOAD）命令启动圈提交易。

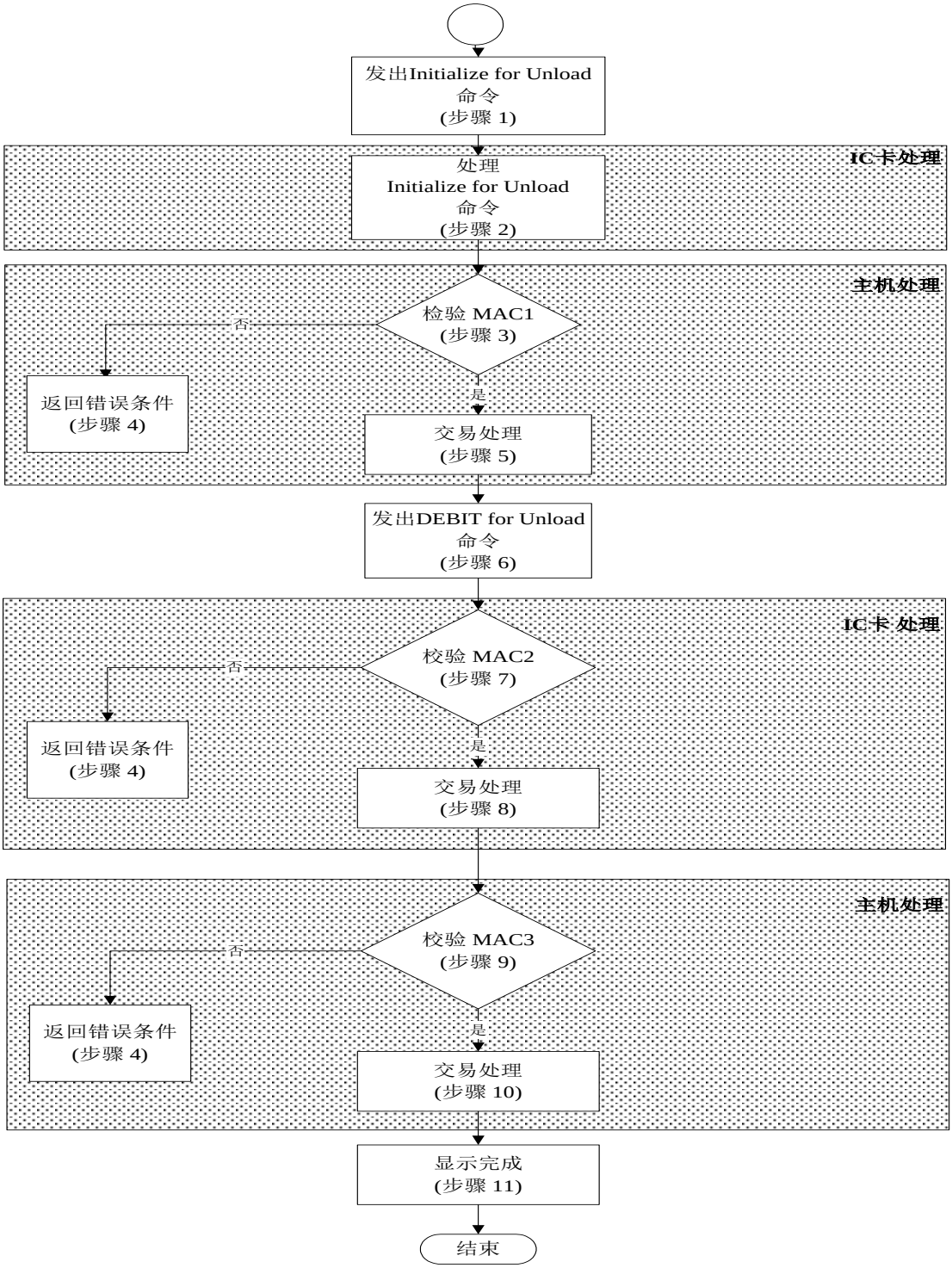


图29　圈提交易处理流程

9.2.2　处理初始化圈提（INITIALIZE FOR UNLOAD）命令（步骤 2）

收到初始化圈提（INITIALIZE FOR UNLOAD）命令后，IC卡将进行以下操作：

——检查是否支持命令中提供的密钥索引号。如果不支持，则回送状态字“9403”（不支持的密钥索引），但不回送任何其他数据，命令处理结束；

——检查命令中包含的交易金额是否超过电子现金余额。如果超过，则回送状态字“9401”（资金不足），但不回送其他数据。终端应采取的措施不在本部分范围之内。

在通过以上检查后，IC卡将产生一个伪随机数（ICC）、过程密钥SESULK和一个报文鉴别码（MAC1），供主机验证圈提交易及IC卡的合法性。

SESULK是用于电子钱包圈提交易的过程密钥。该过程密钥是利用DULK并按照JT/T XXX.5所描述的机制产生的。用来产生该过程密钥的输入数据如下：

SESULK：伪随机数（ICC）||电子钱包联机交易序号||“8000”

MAC1的计算机制见JT/T XXX.5定义的内容。用SESULK对以下数据加密产生MAC1（按所列顺序）：

——电子现金余额（交易前）；

——交易金额；

——交易类型标识；

——终端机编号。

IC卡应向终端回送JT/T XXX.1附录A中定义的初始化圈提（INITIALIZE FOR UNLOAD）命令的响应报文和状态字“9000”。

在收到初始化圈提（INITIALIZE FOR UNLOAD）的响应报文后，终端将一个包含JT/T XXX.1附录A中数据的圈提许可请求报文MAC1送往发卡方主机。

9.2.3 验证 MAC1（步骤 3）

主机将产生SESULK并验证MAC1是否有效。如果MAC1有效，将执行8.2.5中的步骤。否则终端应回送一个错误状态字，交易处理将转而执行8.2.4中所描述的步骤。

为保证执行成功，还有一些其它条件应该由主机进行检查，有关这方面的内容及主机回送的错误状态报文均不在本部分的范围之内。

9.2.4 回送错误状态（步骤 4）

如果不接受圈提交易，主机应通知终端。终端的处理方式不在本部分范围内。

9.2.5 主机处理（步骤 5）

主机确认能够进行圈提交易后，将产生一个报文签别码（MAC2），以供IC卡对主机合法性进行检查。下面列出包含在DEBIT FOR UNLOAD命令中从主机经由终端传到IC卡的数据。

MAC2的计算机制见JT/T XXX.5用SESULK对以下数据进行加密（按所列顺序）产生MAC2：

——交易金额；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

主机向终端发送一个圈提交易接受报文，其中至少应包括交易日期（主机）、交易时间（主机）和MAC2。

9.2.6 发出圈提（DEBIT FOR UNLOAD）命令（步骤 6）

终端收到主机的圈提交易接受报文后，向IC卡发出圈提（DEBIT FOR UNLOAD）命令以更新卡上电子现金余额。圈提（DEBIT FOR UNLOAD）命令见JT/T XXX.1附录A。

9.2.7 验证 MAC2（步骤 7）

IC卡应确认MAC2是有效的。如果MAC2有效，交易处理将执行8.2.8中所描述的步骤。否则向终端回送状态字“9302”（MAC无效）。终端应采取的相应措施不在本部分范围内。

9.2.8 交易处理（步骤 8）

IC卡将电子钱包交易序号加1，并从卡上的电子钱包余额中扣减交易金额。IC卡应成功地完成以上所有步骤或者一个也不完成。

IC卡将产生一个报文鉴别码（MAC3），并通过圈提（DEBIT FOR UNLOAD）命令的响应报文将以下数据经终端送往主机。

用SESULK对以下数据加密产生MAC3（按所列顺序）：

——电子钱包余额（交易后）；

——电子钱包交易序号（加 1 前）；

——交易金额；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

IC卡用以下数据组成的一个记录更新交易明细：

——电子钱包交易序号；

——交易金额；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

9.2.9 验证 MAC3（步骤 9）

主机收到（经由终端）IC卡回送的MAC3后，应确认MAC3是否有效。如果MAC3有效，交易处理将执行8.2.10中描述的步骤。否则将向终端回送一个错误状态字。终端对错误状态采取的相应措施不在本部分范围内。

9.2.10 交易处理（步骤 10）

发卡方主机将交易金额从电子钱包账户上扣减，并将主机的电子钱包交易序号加1。

主机将向终端回送一个完成报文，表示持卡人的账户已更新。报文的内容和形式不在本部分范围内。

9.2.11 显示完成（步骤 11）

在收到主机的完成报文后，终端将向持卡人显示交易完成信息。

如果需要，终端应能向持卡人提供纸质交易凭证。

9.3 电子钱包消费交易

消费交易允许持卡人使用电子钱包的余额进行支付或获取服务。此交易通常在公共交通IC卡终端上脱机进行。

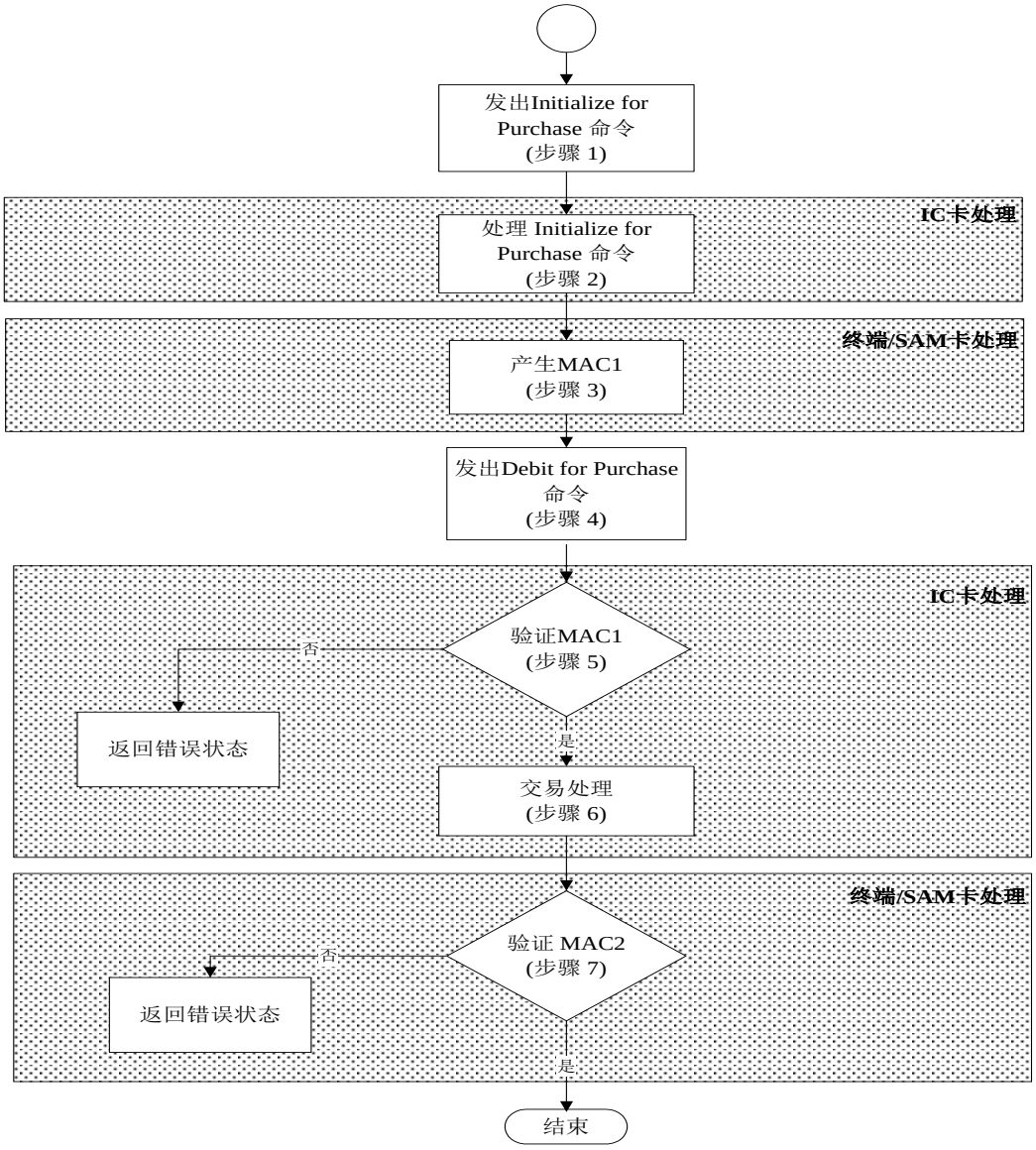


图30　消费交易处理流程

9.3.1　发出初始化消费（INITIALIZE FOR PURCHASE）命令（步骤1）

终端发出初始化消费（INITIALIZE FOR PURCHASE）命令启动消费交易。

9.3.2　处理初始化消费（INITIALIZE FOR PURCHASE）命令（步骤2）

IC卡收到初始化消费（INITIALIZE FOR PURCHASE）命令后，将进行以下操作：

——检查是否支持命令中提供的密钥索引号。如果不支持，则回送状态字“9403”（不支持的密钥索引），但不回送其他数据；

——检查电子钱包余额是否大于或等于交易金额。如果小于交易金额，则回送状态字“9401”（资金不足），但不回送其他数据。终端应采取的相应措施不在本部分的范围内。

在通过以上检查之后，IC卡将产生一个伪随机数并在8.3.5中生成过程密钥并验证MAC1。过程密钥是利用DPK并按照JT/T XXX.5所描述的机制产生的。用于产生该过程密钥的输入数据如下：

SESPK：伪随机数（ICC）||电子钱包脱机交易序号||终端交易序号的最右两个字节

9.3.3 产生 MAC1（步骤 3）

使用伪随机数（ICC）和IC卡回送的电子钱包交易序号，终端的安全存取模块（SAM卡）将产生一个过程密钥（SESPK）和一个报文鉴别码（MAC1），供IC卡来验证SAM卡的合法性。

MAC1的计算机制见JT/T XXX.5。用SESPK对以下数据进行加密产生MAC1（按所列顺序）：

——交易金额；

——交易类型标识；

——终端机编号；

——交易日期（终端）；

——交易时间（终端）。

9.3.4 发出消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令（步骤 4）

终端发出消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令。

9.3.5 验证 MAC1（步骤 5）

在收到消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令后，IC卡将验证MAC1的有效性。如果MAC1有效，交易处理将继续执行8.3.6中所描述的步骤。否则将向终端回送错误状态字‘9302’（MAC无效）。终端对错误状态的处理不在本部分范围内。

9.3.6 交易处理（步骤 6）

IC卡从电子钱包余额中扣减消费的金额，并将电子钱包交易序号加1。IC卡应成功地完成以上所有步骤或者一个也不完成。只有余额和序号的更新均成功后，交易明细才可更新。

IC卡产生一个报文鉴别码（MAC2）供SAM卡对其进行合法性检查，并通过DEBIT FOR PURCHASE命令的响应报文回送终端。MAC2的计算机制见JT/T XXX.5。用SESPK对以下数据进行加密产生MAC2：

——交易金额。

IC卡按照JT/T XXX.5中描述的机制用密钥DTK左右8位字节异或运算后的结果产生TAC。TAC将被写入终端交易明细，以便于主机进行交易验证。TAC以明文形式通过消费/取现（DEBIT FOR PURCHASE）命令的响应报文从IC卡传送到终端，下面是用来生成TAC的数据：

——交易金额；

——交易类型标识；

——终端机编号；

——终端交易序号；

——交易日期（终端）；

——交易时间（终端）。

对于电子钱包消费交易（可选），IC卡将用以下数据组成的一个记录更新交易明细。

——电子钱包交易序号；

——交易金额；

——交易类型标识；

——终端机编号；

——交易日期（终端）；

——交易时间（终端）。

9.3.7 验证 MAC2（步骤 7）

在收到IC卡（经过终端）传来的MAC2后，SAM卡要验证MAC2的有效性。MAC2验证的结果被传送到终端以便采取必要的措施。终端应采取的相应措施不在本部分的范围之内。

9.4 电子钱包复合应用消费交易

复合应用消费交易允许持卡人使用电子钱包的余额，根据卡上记录的分时分段信息，进行支付或获取服务。此交易通常在终端设备或其它读卡设备上脱机进行。

复合应用消费交易允许消费金额为0。

9.4.1 发出 INITIALIZE FOR CAPP PURCHASE 命令（步骤 1）

终端发出INITIALIZE FOR CAPP PURCHASE命令启动复合应用消费交易。

9.4.2 处理 INITIALIZE FOR CAPP PURCHASE 命令（步骤 2）

IC卡收到INITIALIZE FOR CAPP PURCHASE命令后，将进行以下操作：

——检查是否支持命令中提供的密钥索引号。如果不支持，则回送状态字‘9403’（不支持的密钥索引），但不回送其他数据；

——检查电子钱包余额是否大于或等于交易金额。如果小于交易金额，则回送状态字‘9401’，但不回送其它数据。终端应采取的措施不本部分的范围内。

在通过以上检查之后，IC卡将产生一个伪随机数（ICC）和过程密钥。过程密钥是利用DPK并按照JT/T XXX.5所描述的机制产生的。用于产生该过程密钥的输入数据如下：

SESPK：伪随机数（ICC）||电子钱包交易序号||终端交易序号的最右两个字节。

9.4.3 产生 MAC1（步骤 3）

使用伪随机数（ICC）和IC卡回送的电子钱包交易序号，终端的安全存取模块（SAM卡）将产生一个过程密钥（SESPK）和一个报文鉴别码（MAC1），供IC卡来验证SAM卡的合法性。

MAC1的计算机制见JT/T XXX.5。用SESPK对以下数据进行加密产生MAC1（按所列顺序）：

——交易金额；

——交易类型标识；

——终端机编号；

——交易日期（终端）；

——交易时间（终端）。

9.4.4 发出 UPDATE CAPP DATA CACHE 命令（步骤 4）

终端发出UPDATE CAPP DATA CACHE命令。

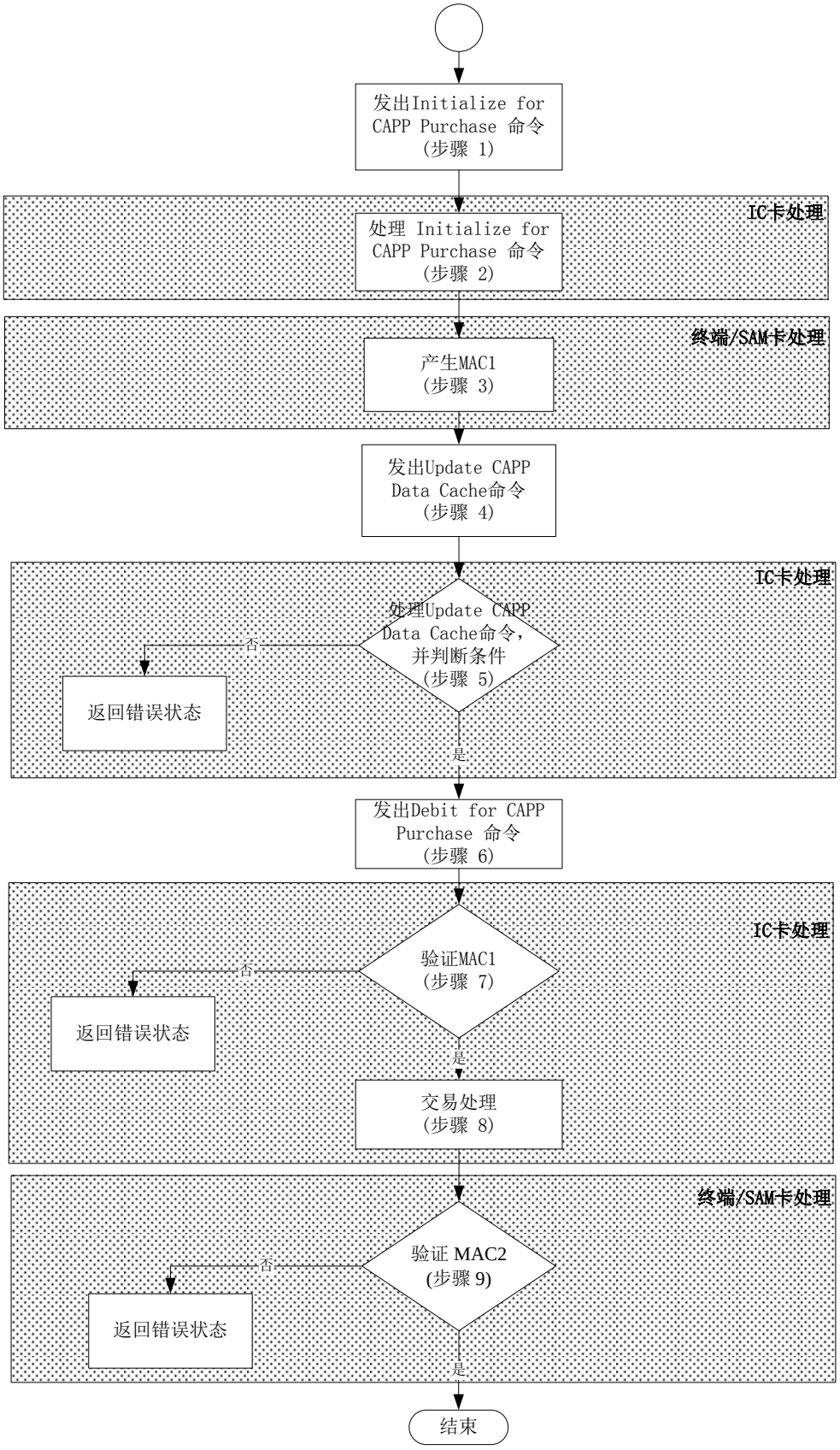


图31　复合消费交易流程

9.4.5　处理 UPDATE CAPP DATA CACHE 命令（步骤 5）

IC卡在收到UPDATE CAPP DATA CACHE命令后，将进行以下操作：

——如果命令中存在 SFI 域，检查卡片当前应用下是否存在与命令中 SFI 值相同的文件。如果不存在，回送状态字“6A82”（未找到文件），但不回送其它数据。终端应终止此次复合应用消费交易；

——根据命令中的复合应用类型标识符，查询复合应用专用文件中是否存在相同标识符的记录。如果不存在，则回送状态字“6A83”（未找到记录），但不回送其它数据。终端应终止此次复合应用消费交易；

——检查复合应用专用文件中相应记录中的应用锁定标志字节。如果应用锁定标志为设置，则回送状态字“9407”（复合应用禁止），但不回送其它数据。终端应终止此次复合应用消费交易；

——检查命令中的数据域长度是否大于复合应用专用文件中相应记录的长度。如果大于，则回送状态字“6A84”（文件中存储空间不够），但不回送其它数据。终端应终止此次复合应用消费交易。

在通过以上检查后，IC卡应暂存命令中的SFI、记录号、复合应用类型标识符和数据域。复合应用专用文件中相应记录中的数据不得通过此命令更新。

9.4.6 发出 DEBIT FOR CAPP PURCHASE 命令（步骤 6）

终端发出DEBIT FOR CAPP PURCHASE命令。

9.4.7 验证 MAC1（步骤 7）

在收到DEBIT FOR CAPP PURCHASE命令后，IC卡将验证MAC1的有效性。如果MAC1有效，交易处理将继续执行8.4.8中所描述的步骤。否则将向终端回送错误状态字“9302”（MAC无效）。终端对错误状态的处理不在本部分范围内。

9.4.8 交易处理（步骤 8）

IC卡从电子钱包余额中扣减消费的金额，电子钱包交易序号加1，根据8.4.5中暂存的数据更新复合应用专用文件，更新电子钱包消费交易记录。IC卡应成功地完成以上所有步骤或者一个也不完成。

在根据8.4.5中暂存的数据更新复合应用专用文件时，如果更新数据长度小于记录长度，IC卡应在数据后自动填充‘00’至记录尾。

IC卡产生一个报文鉴别码（MAC2）供SAM卡对其进行合法性检查，并通过DEBIT FOR CAPP PURCHASE命令响应报文回送以下数据，作为SAM卡产生MAC2的输入数据。MAC2的计算机制见JT/T XXX.5。用SESPK对以下数据进行加密产生MAC2：

——交易金额。

IC卡按照JT/T XXX.5中描述的机制直接用密钥DTK产生TAC。TAC将被写入终端交易明细，以便于主机进行交易验证，它以明文形式通过命令报文从终端传送到IC卡。下面是用来生成TAC的数据：

——交易金额；

——交易类型标识；

——终端机编号；

——终端交易序号；

——交易日期（终端）；

——交易时间（终端）。

对于电子钱包消费交易（可选），IC卡将用以下数据组成的一个记录更新交易明细：

——交易金额；

——交易类型标识；

——电子钱包脱机交易序号；

——终端机编号；
——交易日期（终端）；
——交易时间（终端）。

9.4.9 验证 MAC2 （步骤 9）

在收到IC卡（经过终端）传来的MAC2后，SAM卡要验证MAC2的有效性。MAC2验证的结果被传送到终端以便采取必要的措施。终端的采取的措施不在本部分的范围之内。

9.5 电子钱包查询交易

9.5.1 查询余额交易

持卡人可以通过终端或其他读卡设备读取电子钱包中的余额。此交易采用脱机方式进行。

终端利用查询余额（GET BALANCE）命令实现查询余额交易。

9.5.2 查询明细交易

持卡人可以通过终端或其他读卡设备读取IC卡中的交易明细记录。此交易一般采用脱机方式处理。

终端发出一个READ RECORD命令（符合JT/T XXX.1中的规定）来获得交易明细。这个命令会回送某个交易明细记录中所含的所有数据。交易明细文件为循环记录文件，且至少应包含10条记录。

交易明细中的记录使用记录号寻址。记录号范围从1到n，n是文件中记录的最大个数。最近写入的记录号为1，前一记录号为2，如此类推直到n。n代表文件中最早写入的记录。

根据本部分的要求，IC卡应支持在以下交易中记录明细：电子钱包圈存交易、电子钱包圈提交易、电子钱包消费交易（可选）、电子钱包复合应用消费交易（可选）。

9.6 电子钱包应用维护功能

以下交易应在拥有相应密钥的设备上执行。

9.6.1 安全报文

电子钱包应用涉及到的安全机制，应按照JT/T XXX.5的规定进行，并作如下改动和增补：

——在传送一个包含安全报文的命令前，主机向终端发送一个报文，要求从 IC 卡获得一个随机数。终端向 IC 卡发出一个 GET CHALLENGE 命令（见 JT/T XXX.1 附录 A）。从 IC 卡回送的随机数被送往主机以用于安全报文处理。

——从 IC 卡回送的 4 字节随机数后缀以‘00 00 00 00’，所得到的结果作为初始值。

——不采用过程密钥。除去 APPLICATION UNBLOCK 指令使用导出的应用解锁密钥（DUBK）来计算以外，均使用导出的应用维护密钥（DAMK）来计算 MAC。

——全部采用双字节密钥的对称算法。

9.6.2 应用锁定

终端发出应用锁定（APPLICATION BLOCK）命令来锁定应用。

此命令的用法由发卡方自行决定。

此命令参照JT/T XXX.1附录A。其安全机制在8.6.1中描述。在本部分所述的应用中，命令的成功执行导致IC卡中的电子钱包应用无效。在这种状态下：

——选择此应用时，对 SELECT 命令 IC 卡回送状态字“6283”(选择文件无效)和文件控制信息(FCI)，在 T=0 协议时，卡片 FCI 需用取响应（GET RESPONSE）命令取回；

——在应用被选择后，除以下情况外，IC 卡对其它命令只回送状态字“6985”(使用的条件不满足)：

1） 当用 SELECT 命令选择此应用或其他应用时；

2) 产生随机数（GET CHALLANGE）命令；
3) 应用锁定（APPLICATION BLOCK）命令；
4) 应用解锁（APPLICATION UNBLOCK）命令。

如果在命令参数P2中指明永久性锁定此应用，IC卡将设置一个内部标志以表明不允许执行应用解锁（APPLICATION UNBLOCK）命令。

此命令的执行并不改变电子钱包交易序号的值。

9.6.3 应用解锁

交易终端发出应用解锁（APPLICATION UNBLOCK）命令来对应用解锁，详细定义见JT/T XXX.1附录A，具体安全机制见8.6.1。

如果对某应用连续三次解锁失败，则IC卡将永久锁定此应用并回送状态字“9303”（应用永久锁定）。

如果在应用解锁（APPLICATION UNBLOCK）命令中使用了永久锁定的选项，IC卡将回送状态字“9303”（应用永久锁定）且不再对应用解锁。

应用解锁（APPLICATION UNBLOCK）命令的成功执行使应用重新恢复成有效状态。在此之后，该应用对所有命令的响应就象应用锁定和应用解锁没有执行过一样。

此命令的执行并不改变电子钱包交易序号的值。

9.6.4 二进制形式修改

终端按照JT/T XXX.1和8.6.1中所描述的安全要求，发出修改二进制（UPDATE BINARY）指令。

如果三次执行此命令均告失败，则IC卡将永久锁定此应用并回送状态字“9303”（应用永久锁定）。

9.6.5 增加复合应用

增加复合应用通过修改或增加记录的方式，修改复合应用专用文件或在复合应用专用文件中增加记录，从而启用或重启用知道的复合应用。

终端首先利用READ RECORD命令读取复合应用专用文件。如果文件不存在，则说明IC卡不支持复合应用。终端应采取的措施不在本部分的范围内。

终端应提示持卡人选择需增加的复合应用类型，并将选择结果通过对应表翻译成复合应用类型标识符和记录长度。

终端利用指定P1为复合应用类型标识符，P2的b4至b8为SFI，P2的b1至b3为0的READ RECORD命令，查询复合应用专用文件记录。如果记录不存在，则发出指定SFI的APPEND RECORD命令，命令数据域为简单TLV格式，其中Tag值为复合应用类型标识符，Length为复合应用数据长度。命令执行成功后，终端应提示持卡人增加复合应用操作成功。

如果记录存在，则终端发出指定P1为复合应用类型标识符，P2的b4至b8为SFI，P2的b1至b3为0的READ RECORD命令，获取复合应用数据。

终端检查复合应用数据中的复合应用锁定标志字节。如为锁定，则终端应将锁定标志字节设置为‘00’后，将复合应用数据通过UPDATE RECORD回写入卡片。回写成功后，终端应提示持卡人复合应用重启用成功。

如锁定标志未被设置，则终端终止处理，并提示持卡人复合应用已存在。

9.6.6 删除复合应用

删除复合应用通过设置复合应用专用文件记录中的应用锁定标志，终止卡片对指定复合应用的支持。

终端首先利用READ RECORD命令读取复合应用专用文件。如果文件不存在，则说明IC卡不支持复合应用。终端应采取的措施不在本部分的范围内。

终端利用READ RECORD命令遍历读取所有复合应用专用文件，并通过对照表，以记录号作为复合应用类型标识符获得卡片支持的所有复合应用，并提示持卡人选择。

持卡人选择后，终端应根据选择结果，发出指定P1为复合应用类型标识符，P2的b4至b8为SFI，P2的b1至b3为0的READ RECORD命令，获取复合应用数据。

终端检查复合应用数据中的复合应用锁定标志字节。如标志未被锁定，则终端应将锁定标志字节设置为‘01’标识锁定后，将复合应用数据通过UPDATE RECORD回写入卡片。回写成功后，终端应提示持卡人复合应用删除成功。

如锁定标志已被设置，则终端终止处理，并提示持卡人复合应用已删除。

附 录 A
（规范性附录）
终端和受理机构数据元

a－每个字节包含一个字符的字母数据元（A-Z，a-z）。

an－每个字节包含一个字符字母数字型数据元（A-Z，a-z，0-9）。

ans－字母数字及特殊字符型。

b－二进制（二进制数或者位组合）。

cn－压缩数字，每个字节由‘0’－‘9’中的两个数字组成，数据元左对齐，右补F。如数1234567890123可以以十六进制形式保存在8个字节的PAN数据对象中，形如‘12 34 56 78 90 12 3F FF’。

n－数字型，也称作BCD码。右对齐，左补‘0’。如，数字12345可以保存在n12的授权金额数据对象中，形如‘00 01 23 45’。

var－可变长。变长数据的格式另有说明。

表A.1列出终端和收单机构支持的数据元，并说明其来源，含义及TLV格式。

表A.1 终端和收单机构数据元

名称	描述	来源	格式	模版	标签	长度
收单机构代码	在每个公共交通 IC 卡系统中唯一标识收单机构	终端	n6-11	—	‘9F01’	4
附加终端性能	表明终端的数据输入输出能力	终端	B	—	‘9F40’	5
授权金额（二进制）	交易授权金额（不包括调整）	终端	B	—	‘81’	4
授权金额（数值型）	交易授权金额（不包括调整）	终端	n12	—	‘9F02’	6
其它金额（二进制）	与交易相关的第 2 金额，表示返现金额	终端	B	—	‘9F04’	4
其它金额（数值型）	与交易相关的第 2 金额，表示返现金额	终端	n12	—	‘9F03’	6
参考货币金额	用参考货币表示的授权金额	终端	B	—	‘9F3A’	4
应用标识（AID）	按 GB/T 16649.5 所定义，用于表示一个应用	终端	B	—	‘9F06’	5-16
应用选择指示器	指示应用选择时终端上的 AID 与卡片中的 AID 是完全匹配（长度和内容都应一样），还是部分匹配（卡片 AID 的前面部分与终端 AID 相同，长度可以更长）。终端支持的应用列表中的每个 AID 仅有一个应用选择指示器，它的格式如表 5 所示	终端	由终端决定，本数据不在接口之间传递	无	无	见格式
应用版本号	公共交通 IC 卡系统给应用分配的版本号	终端	B	—	‘9F09’	2
授权响应代码	定义发卡机构对交易联机授权的结果	发卡	An 2	—	‘8A’	2

名称	描述	来源	格式	模版	标签	长度
		机构/终端				
持卡人验证方法（CVM）结果	表示最后一次持卡人验证方法执行的结果	终端	B	—	‘9F34’	3
认证中心公钥验证和	用安全哈希算法对认证中心公钥所有部分（RID、认证中心公钥索引、认证中心公钥模、认证中心公钥指数）连接的结果进行运算所得的验证值	终端	B	—	—	20
认证中心公钥指数	认证中心公钥的指数部分	终端	B		—	1 或 3
认证中心公钥索引	与 RID 一起标识认证中心公钥	终端	B		‘9F22’	1
认证中心公钥模	认证中心公钥的模部分	终端	B		—	Nca（最大 248）
命令模版	标识命令报文中的数据域	终端	B		‘83’	var.
缺省动态数据认证数据对象列表（DDOL）	卡片中无 DDOL 时用于构造内部认证命令的 DDOL	终端	B		—	var.
缺省交易证书数据对象列表（TDOL）	卡片中无 TDOL 时用于生成 TC 哈希值的 TDOL。本部分中该值为空	终端	B		—	var.
接口设备（IFD）序列号	厂商分配给终端 IFD 的唯一、永久的序列号	终端	an8	—	‘9F1E’	8
发卡机构脚本结果	表示终端脚本处理的结果	终端	B		—	var.
偏置随机选择的最大目标百分数	在终端风险管理中用于随机交易选择的值	终端	—		—	—
商户分类码	按 GB/T 15150 卡片受理业务编码所规定的商户从事业务所进行的分类	终端	N 4	—	‘9F15’	2
商户标识	和收单机构代码一起唯一地标识一个特定的商户	终端	ans 15	—	‘9F16’	15
商户名称和位置	表明商户的名称和所处位置	终端	Ans		—	var.
报文类别	表明批数据收集记录是记录还是通知	终端	N 2		—	1
销售点（终端）输入方式	按 GB/T 15150 销售点输入模式，表示 PAN 的输入方式	终端	n 2	—	‘9F39’	1
随机选择的目标百分数	在终端风险管理中用于随机交易选择的值	终端	—		—	—
终端行为代码－缺省	收单机构设置的在交易联机无法进行的情况下能够导致交易脱机拒绝的 TVR 条件位	终端	b		—	5
终端行为代码－拒绝	收单机构设置的能够导致交易脱机拒绝的 TVR 条件位	终端	b		—	5

名称	描述	来源	格式	模版	标签	长度
终端行为代码－联机	收单机构设置的能够导致交易联机处理的 TVR 条件位	终端	b		—	5
终端性能	表示终端的卡片数据输入、CVM 支持和安全能力	终端	b		‘9F33’	3
终端国家代码	按 GB/T 2659 表示的终端国家代码	终端	n 3	—	‘9F1A’	2
终端最低限额	终端中与 AID 相关的导致交易联机处理的最低交易金额	终端	b		‘9F1B’	4
终端标识	表明终端在商户的唯一位置	终端	an 8	—	‘9F1C’	8
终端类型	指示终端环境、通讯能力和操作控制	终端	n 2	—	‘9F35’	1
终端验证结果（TVR）	用于记录终端执行各公共交通 IC 卡应用功能处理结果的一组指示位	终端	b	—	‘95’	5
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	终端	—		—	—
电子现金交易金额	交易的清算金额，包括消费和其它调整	终端	n 12		—	6
交易证书（TC）哈希值	包含在 CDOL 数据中要求送给卡片，由 TDOL 表示的数据作哈希运算的结果	终端	b	—	‘98’	20
交易货币代码	按 GB/T 12406 规定的交易货币代码	终端	n 3	—	‘5F2A’	2
交易货币指数	按 GB/T 12406 规定的从交易金额右起的隐含小数点位置	终端	n 1	—	‘5F36’	1
交易日期	交易授权的本地日期	终端	n 6 YYMMDD	—	‘9A’	3
交易参考货币代码	当交易货币代码和应用货币代码不同时，终端使用的公共货币代码	终端	n 3	—	‘9F3C’	2
交易参考货币兑换比率	从交易货币代码向交易参考货币代码兑换时的比率	终端	n 8		—	4
交易参考货币指数	表示按 GB/T 12406 规定的交易参考货币代码的交易金额右起的隐含小数点位置	终端	n 1	—	‘9F3D’	1
交易序列计数器	终端维护的每笔交易递增一的计数器	终端	n 4-8	—	‘9F41’	2-4
交易状态信息	一组表示交易完成的公共交通 IC 卡应用功能的指示位	终端	b	—	‘9B’	2
交易时间	交易授权的本地时间	终端	n 6 HHMMSS	—	‘9F21’	3
电子现金交易类型	按 GB/T 15150 定义的处理码前 2 位表示的交易类型	终端	n 2	—	‘9C’	1
不可预知数	为提供给卡片生成应用密文而由终端提供的动态变化和唯一的数据	终端	b	—	‘9F37’	4
账户类型	标识在交易中选择的账户的类型	终端	n2	—	‘5F57’	1
算法标识（DLK）	用来标识圈存交易的加密算法	终端	b	—	—	1
算法标识（DPK）	用来标识消费和取现交易的加密算法	终端	b	—	—	1
算法标识（DTK）	用来标识在交易中计算 TAC 使用的加密算法	终端	b	—	—	1

名称	描述	来源	格式	模版	标签	长度
算法标识（DUK）	用来标识在修改透支限额交易中使用的加密算法	终端	b	—	—	1
算法标识（DULK）	用来标识在圈提交易中使用的加密算法	终端	b	—	—	1
密钥索引号	为了唯一标识在一个密钥版本中的密钥索引号而分配的一个数字	终端	cn	—	—	1
SAM 卡应用标识符	按 GB/T 16649.5 所定义，用于表示用来唯一标识安装在终端中的 SAM 卡上的安全应用	终端	b	—	—	5-16
SAM 卡标识符	用来唯一标识安装在终端中的 SAM 卡的一个数字。	SAM 卡	b	—	—	4
终端机编号	用来唯一标识商户终端的一个编号。	终端	b	—	—	6
终端交易计数器	终端里的一个计数器，每当交易发生就增加。	终端	b	—	—	4
电子钱包交易金额	当前交易的金额，包括消费和圈存等	终端	b	—	—	4
电子钱包交易类型标识（TTI）	用于标识持卡人选择的交易类型（例如：圈存、圈提及消费等）而分配的一个值	终端	cn	—	—	1

当定义的数据对象长度大于实际数据对象的长度时，采用如下规则：

——格式为 n 的数据元右对齐，左补十六进制零；

——格式为 cn 的数据元左对齐，右补十六进制‘F’；

——格式为 an 的数据元左对齐，右补十六进制零；

——格式为 ans 的数据元左对齐，右补十六进制零。

当数据从一处转移到另一处时（例如从卡片到终端），无论各自内部如何存储，应按从高位到低位的顺序传递。连接数据时也使用同样的规则。

如下数据应在终端首次安装时初始化：

终端性能、终端附加性能、终端 IFD 序号、终端国家代码、终端标识、终端类型、终端交易货币和终端货币指数。

如下终端数据应允许在终端布放后通过下载更新：

终端支持应用 AID 列表、CA 公钥、终端行为代码 TAC、最低限额（Floor limit）、随机选择阈值、随机选择目标百分数、偏置随机选择最大目标百分数、商户标识、商户分类码和收单机构代码。

附 录 B
（规范性附录）
扩展应用 SAM 交易指令

B.1 扩展应用DES计算初始化（INIT_FOR_DESCRYPT）

B.1.1 定义和范围

INIT_FOR_DESCRYPT 命令用来初始化通用密钥计算过程。SAM 卡将利用卡中指定的密钥进行运算，产生一个临时密钥。运算方式由指定的密钥类型、密钥分散级数和密钥算法标识确定。

不支持计算临时密钥计算的密钥类型有：

——主控密钥

——维护密钥

——消费密钥

双长度密钥产生双长度临时密钥类型有：

——用户卡应用维护密钥

双长度密钥产生双长度临时密钥，单长度密钥产生单长度临时密钥的密钥类型有：

——MAC 密钥

——加密密钥

——MAC、加密密钥

指定密钥经过几级处理由密钥分散级数和 LC 确定，若二者不一致，则返回错误信息。

临时密钥在 SAM 卡下电后自动消失，不允许读。

临时密钥产生后，与原密钥的属性一致。

B.1.2 命令报文

INIT_FOR_DESCRYPT命令报文根据表B.1编码

表B.1 INIT_FOR_DESCRYPT 命令报文

代码	值
CLA	‘80’
INS	‘1A’
P1	密钥用途
P2	密钥版本
Lc	待处理数据的长度
Data	待处理数据
Le	不存在

B.1.3 命令报文数据域

命令报文数据域包括待处理的输入数据。 数据长度为 8 的整数倍，长度也可以是 0。密钥类型取密钥用途的低 5 位，密钥分散级数取密钥用途的高 3 位。

待处理的输入数据包括多级的分散因子，按最后一次分散因子在前、最后一次分散因子在后的顺序输入。

B.1.4 响应报文

数据域不存在。

B.1.5 响应报文的状态码

SAM卡可能回送的错误状态码见表B.2所示

表B.2 INIT_FOR_DESCRYPT 状态码表

SW1	SW2	含　义
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	85	使用条件不满足(应用被锁定)
69	86	不满足命令执行条件，当前文件不是 EF
6A	80	数据域参数错误（如：密钥分散级数与分散数不符）
6A	81	功能不支持（应用锁定）
6A	86	P1、P2 参数错
6D	00	命令不存在
93	03	应用永久锁定

B.2 扩展应用DES计算（DES Crypt）

B.2.1 定义和范围

DES Crypt 命令利用指定的密钥来进行运算。若一条命令无法传输所有的待处理数据，可分几条命令输入。

加密计算采用 ECB 模式，数据的填充在卡片外面进行，卡片只支持长度为 8 的整数倍数据的加密。

MAC 计算遵循 JT/T XXX.5 的安全机制，数据的填充在卡片外部进行，卡片只支持长度为 8 的整数倍数据的 MAC 计算。

DES Crypt 命令应在 INIT_FOR_DESCRYPT 命令成功执行后才能进行。卡片状态在执行无后续数据块计算后，复原为通用 DES 计算初始化执行前的状态

B.2.2 命令报文

DES Crypt命令报文根据表B.3编码

表B.3 DES Crypt 命令报文

代码	值
CLA	‘80’
INS	‘FA’
P1	见表 B.4
P2	‘00’
Lc	待加密数据的长度
Data	待加密数据
Le	不存在

表B.4 P1 参数说明：

B8	B7	B6	B5	B4	B3	B2	B1	意义
							X	计算模式 ——0，加密 ——1，MAC 计算
						X		后续块 ——0，无后续块 ——1，由后续块
					X			初始值（仅对 MAC 计算有效） ——0，无初试值 ——1，有初试值

P1 值计算模式如下：
——0，无后续块加密；
——1，最后一块 MAC 计算；
——2，有后续块加密；
——3，下一块 MAC 计算；
——5，唯一一块 MAC 计算；
——7，第一快 MAC 计算；
——其他，保留。

B.2.3 命令报文数据域

命令报文数据域包括要加密的数据。加密数据的长度为 8 的整数倍。在 p1 的 b3 位为 1 时，待处理数据的前 8 个字节为 MAC 计算的初试值。

B.2.4 响应报文

在 p1 的 b1 位为 0 时，响应报文数据域包括加密结果，数据长度是 8 的整数倍。
在 p1 的 b1 位为 1，且 p1 的 b2 位为 0 时，响应报文数据域包括 4 字节的 MAC。

B.2.5 响应报文的状态码

SAM 卡可能回送的错误状态码见表 B.5 所示：

表B.5 DES Crypto 状态码表

SW1	SW2	含　义
90	00	命令执行成功
64	00	标志状态位没变
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	01	命令不接受（无效状态）
69	85	使用条件不满足(应用被锁定)
69	86	不满足命令执行条件，当前文件不是 EF
6A	81	功能不支持（应用锁定）
6A	86	P1、P2 参数错

6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.3 选择文件（SELECT）

B.3.1 定义和范围

SELECT 命令通过文件名或 AID 来选择 IC 卡中的 PSE、DDF 或 ADF。
命令执行成功后，PSE、DDF 或 ADF 的路径被设定。
应用到 AEF 的后续命令将采用 SFI 方式联系到所选定的 PSE、DDF 或 ADF。
从 IC 卡的响应报文应由回送 FCI 组成。

B.3.2 命令报文

SELECT的命令报文如表B.6编码

表B.6 SELECT 命令报文

代码	数 值
CLA	‘00’
INS	‘A4’
P1	‘00’ 选择 MF 文件（Lc= ‘00’）或通过 FID 选择 MF、DF、EF ‘02’ 通过 FID 选择当前 DF 下的 EF ‘04’ 通过 DF 名选择应用
P2	‘00’ ‘02’ 下一个文件实例（P1=04h 时）
Lc	若 P1= ‘00’，不存在或 ‘02’ 若 P1= ‘02’，‘02’ 若 P1= ‘04’，‘01’ — ‘10’ DATA 域的数据长度
DATA	若 P1= ‘00’，不存在或 FID（2 字节） 若 P1= ‘02’，FID（2 字节） 若 P1= ‘04’，应用名（AID）
Le	FCI 文件中信息的长度（选择 MF、DDF、ADF 时）

B.3.3 命令报文数据域

若P1= ‘00’，不存在或FID（2字节）；
若P1= ‘02’，FID（2字节）；
若P1= ‘04’，应用名（AID）。

B.3.4 响应报文

响应报文中数据域应包括所选择的PSE、DDF或ADF的FCI。本部分不规定FCI中回送的附加标志。

表B.7 SELECT PSE 的响应报文(FCI)

标 志	内容说明	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M
‘A5’	FCI 专用数据	M

‘88’	目录基本文件的 SFI	M

表B.8 SELECT DDF 的响应报文(FCI)

标 志	内容说明	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M
‘A5’	FCI 专用数据	M
‘88’	目录基本文件的 SFI	M

表B.9 SELECT ADF 的响应报文(FCI)

标 志	内容说明	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M
‘A5’	FCI 专用数据	M
‘9F0C’	发卡机构自定数据的 FCI	O（可以不返回）

表B.10 SELECT ADF 的应答报文中的 FCI 数据专用模板

标 志		内容说明	存在方式
‘A5’		FCI 数据专用模板	M
	‘50’	应用标签	O
	‘87’	应用优先指示符	O
	‘9F08’	应用版本号	M
	‘9F12’	应用优先名称	O

B.3.5 响应报文状态码

SAM卡可能回送的错误状态码见表B.11所示：

表B.11 SELECT 状态码表

SW1	SW2	含 义
90	00	命令执行成功
62	83	选择文件无效
62	84	FCI 格式与 P2 指定不符
64	00	标志状态位没变
67	00	Lc 长度错误
6A	81	功能不支持（应用锁定）
6A	82	未找到文件
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定
61	XX	需发出 GET RESPONSE 命令

B.4 取随机数（GET CHALLENGE）

B.4.1 定义和范围

GET CHALLENGE 命令用于从 IC 卡中获得一个 4/8 个字节的随机数。该随机数服务于安全过程（如安全报文），在使用随机数的命令执行后失效。

B.4.2 命令报文

GET CHALLENGE的命令报文如表B.12编码。

表B.12 GET CHALLENGE 命令报文

代码	数 值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘04’ / ‘08’

B.4.3 命令报文数据域

数据域不存在。

B.4.4 响应报文

响应信息中的数据为4字节或者8字节随机数。

B.4.5 响应报文状态码

SAM卡可能回送的错误状态码见表B.13所示。

表B.13 GET CHALLENGE 状态码表

SW1	SW2	含 义
90	00	命令执行成功
65	81	内存失败
6A	81	功能不支持（应用锁定）
6A	88	未找到引用数据
6A	86	P1、P2 参数错
67	00	Lc 长度错误
6E	00	CLA 错
61	XX	需发出 GET RESPONSE 命令

B.5 读透明文件（READ BINARY）

B.5.1 定义和范围

READ BINARY命令用于读出透明文件的内容。

B.5.2 命令报文

READ BINARY的命令报文如表B.14编码。

表B.14 READ BINARY 命令报文

代码	数 值
CLA	‘00’
INS	‘B0’
P1	见表 B.13
P2	若 P1 的 b8=0，偏移地址低字节 若 P1 的 b8=1，偏移地址
Lc	1）不存在——明文方式
DATA	1）不存在
Le	期望返回的明文字节数

表B.15 P1 参数说明

b8	b7	b6	b5	b4	b3	b2	b1	说 明
0	–	–	–	–	–	–	–	当前的 EF 文件
	x	x	x	X	x	x	x	偏移地址高字节
1	–	–	–	–	–	–	–	用 SFI 方式
–	0	0	–	–	–	–	–	其它值保留
–	–	–	x	x	x	x	x	SFI

B.5.3 命令报文数据域

无

B.5.4 响应报文

响应信息中的数据为明文或密文数据。

B.5.5 响应报文状态码

SAM卡可能回送的错误状态码见表B.16所示。

表B.16 READ BINARY 的状态码表

SW1	SW2	含 义
90	00	命令执行成功
62	81	回送的数据可能有错
61	xx	还有 xx 字节需要返回
65	81	写 EEPROM 失败
67	00	Lc 长度错误
68	82	不支持安全报文
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	85	使用条件不满足（应用被锁定）

69	86	没有选择当前文件
6A	81	功能不支持，应用暂时锁定
6A	82	未找到文件
6A	83	记录未找到
6A	86	P1、P2 参数错
6B	00	起始地址超出范围
6C	xx	Le 长度错误。‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.6 读记录（READ RECORD）

B.6.1 定义和范围

READ RECORD命令读记录文件中指定的记录。

B.6.2 命令报文

READ RECORD命令报文如B.17编码。

表B.17 READ RECORD 命令报文

代码	数 值
CLA	‘00’
INS	‘B2’
P1	记录号（‘00’表示当前记录）或记录标识符
P2	见表 B.16
Lc	不存在——明文方式
DATA	不存在——明文方式
Le	期望返回的明文字节数

表B.18 P2 编码

b8	b7	b6	b5	b4	b3	b2	b1	说 明
0	0	0	0	0	–	–	–	当前的 EF 文件（扩展）
x	x	x	x	x	–	–	–	用 SFI 方式
1	1	1	1	1	–	–	–	保留
–	–	–	–	–	1	x	x	利用 P1 中的记录号
–	–	–	–	–	1	0	0	P1 记录号
–	–	–	–	–	0	0	0	读第一个具有 P1 指定的记录标识符的实例
–	–	–	–	–	0	1	0	读下一个具有 P1 指定的记录标识符的实例
任何其他值								保留

B.6.3 命令报文数据域

无

B.6.4 响应报文

响应信息中的数据为明文或密文数据。

B.6.5 响应报文状态码

SAM卡可能回送的错误状态码见表B.19所示。

表B.19 READ RECORD 的状态码表

SW1	SW2	含　义
90	00	命令执行成功
62	81	回送的数据可能有错
61	xx	还有 xx 字节需要返回
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	85	使用条件不满足
69	86	没有选择当前文件
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	86	P1、P2 参数错
6C	xx	Le 错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.7 MAC1 计算（INIT SAM FOR PURCHASE）

B.7.1 定义和范围

INIT SAM FOR PURCHASE 命令可支持多级消费密钥分散机制，产生JT/T XXX.1中定义的MAC1。可以利用发卡机构编码、卡片应用主账号、随机数和交易信息得到过程密钥，进而加密得到MAC。

INIT SAM FOR PURCHASE命令可支持多级消费密钥分散机制，消费密钥的分散过程由Lc和消费密钥共同确定，如果二者不一致，则返回错误信息。

B.7.2 命令报文

INIT SAM FOR PURCHASE命令报文如B.20编码。

表B.20 INIT SAM FOR PURCHASE 命令报文

代码	数　值
CLA	‘80’
INS	‘70’
P1	‘00’

P2	‘00’
Lc	‘14’ + ‘8*N’ (N = 1，2 ，3)
DATA	MAC1 计算输入数据
Le	‘08’

B.7.3 命令报文数据域

数据以下列顺序排列：
——用户卡随机数 4 字节；
——用户卡交易序号 2 字节；
——交易金额 4 字节；
——交易类型标识 1 字节；
——交易日期终端 4 字节；
——交易时间终端 3 字节；
——消费密钥版本号 1 字节；
——消费密钥算法标识 1 字节；
——用户卡应用主账号 最右 8 字节；
——发卡机构编码 8 字节（4 字节发卡机构编码左补 4 字节 0x00）。

B.7.4 响应报文

响应数据域包括以下数据按顺序返回：
——4 字节的终端脱机交易序号；
——4 字节的 MAC1。

B.7.5 响应报文状态码

SAM卡可能回送的错误状态码见表B.21所示。

表B.21 INIT SAM FOR PURCHASE 的状态码表

SW1	SW2	含 义
90	00	命令执行成功
67	00	Lc 长度错误
69	85	使用条件不满足
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

B.8 校验MAC2（CREDIT SAM FOR PURCHASE）

B.8.1 定义和范围

CREDIT SAM FOR PURCHASE命令利用INIT SAM FOR PURCHASE命令产生的过程密钥SESPKP校验MAC2。
——在此过程中，所有的中间结果只保留在卡片内部，外界无法得到；
——CREDIT SAM FOR PURCHASE 命令应在 INIT SAM FOR PURCHASE 命令成功执行后才能进行。
——若 MAC2 尝试计数器为 0 的话，消费密钥所在的应用将被锁定，只能在应用维护密钥的控制下

应用解锁后使用。

——应用下的MAC2错误计数器在应用下所有消费密钥MAC2校验错误的情况下都要被减1。

——卡片的状态在命令执行后将复原为MAC1校验前的状态。

B.8.2 命令报文

CREDIT SAM FOR PURCHASE命令报文如B.22编码。

表B.22 CREDIT SAM FOR PURCHASE 命令报文

代码	数 值
CLA	‘80’
INS	‘72’
P1	‘00’
P2	‘00’
Lc	‘04’
DATA	MAC2
Le	不存在

B.8.3 命令报文数据域

数据为4字节待校验MAC2。

B.8.4 响应报文

不存在

B.8.5 响应报文状态码

SAM卡可能回送的错误状态码见表B.23所示。

表B.23 CREDIT SAM FOR PURCHASE 的状态码表

SW1	SW2	含 义
90	00	命令执行成功
67	00	Lc长度错误
69	85	使用条件不满足
6A	86	P1、P2参数错
6D	00	命令不存在
6E	00	CLA错
93	03	应用永久锁定

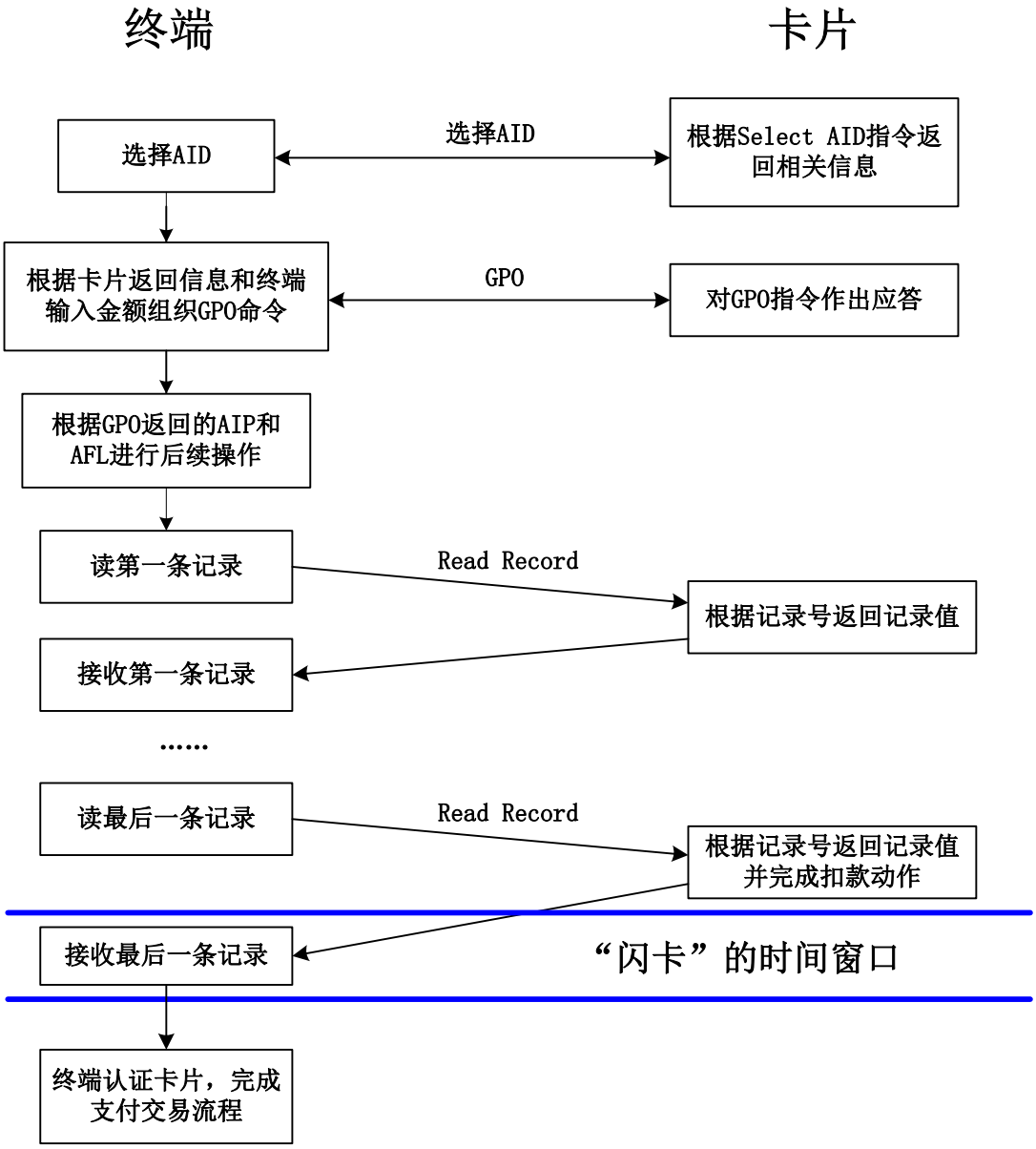
附 录 C
（资料性附录）
电子现金“闪卡”处理流程

C.1 定义和范围

“闪卡”问题是指在标准快速支付交易时，发生卡片内的金额已扣除、但终端交易未成功的现象。造成这种现象的原因有两个：一是终端在后续执行脱机数据校验时，发生失败。通常是由于终端程序错误或证书错误、或卡片是假卡。即在终端程序、参数、卡片都正确时，不会出现失败；二是卡片已返回最后一条记录，但终端未收到，导致卡片扣款、终端未成功现象。以下将就第二种原因进行分析，并提出解决方案。

C.2 “闪卡”现象出现的机理分析

标准快速支付交易中，“闪卡”现象出现的时间窗口是：终端读取卡片最后一条记录，卡片发送给终端最后一条记录并扣款成功，但这个时候，卡片离开了读卡器的磁场区，导致终端没有接收到最后一条记录，从而无法进行后续的认证和交易流程。这样的话，卡片扣款成功但终端交易未成功。

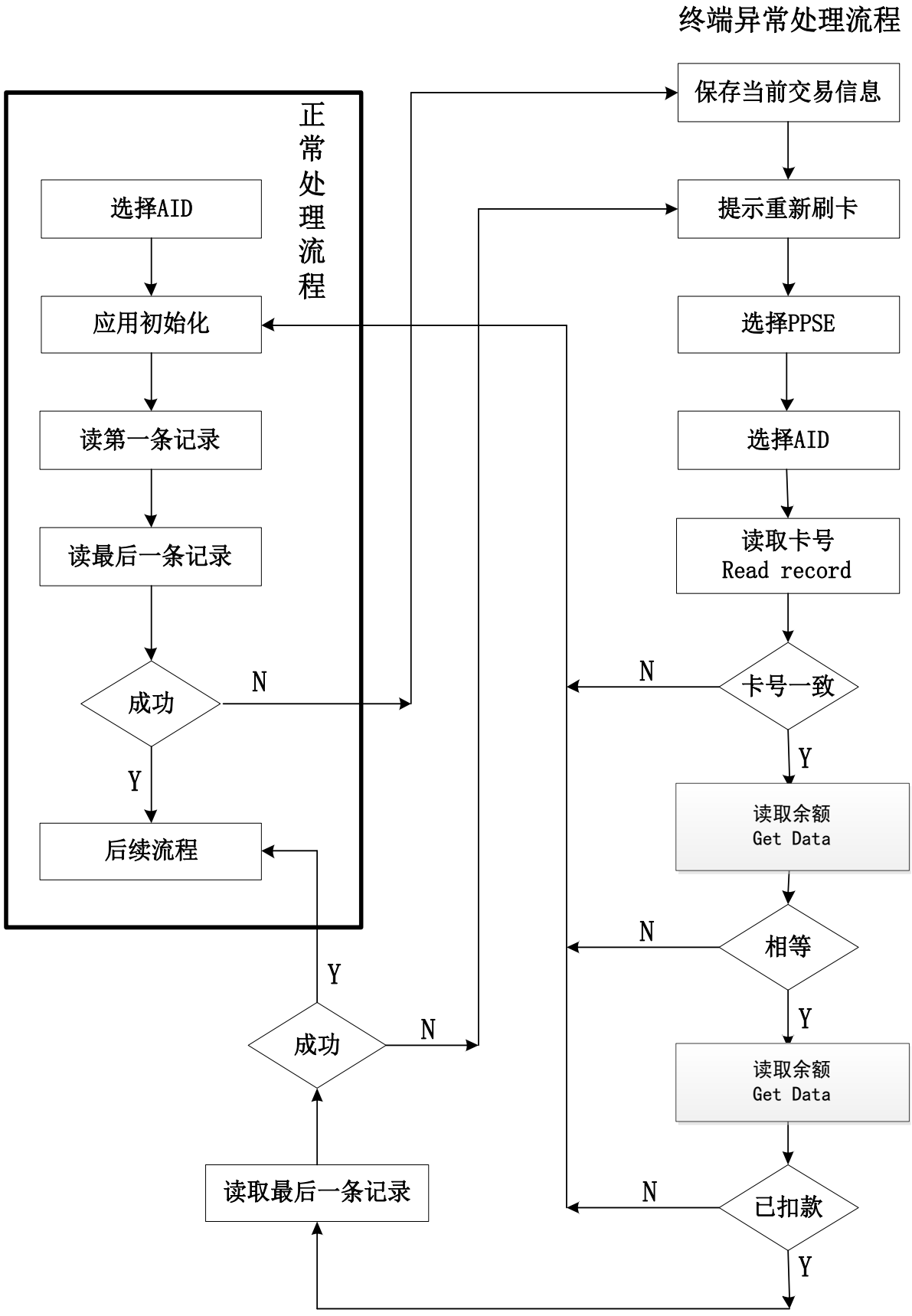


图C.1　闪卡原因分析

C.3　解决方案

正常交易时，终端执行正常交易流程，只有发生最后一笔记录没有正确读出时，才进入异常交易流程。终端只保留最近一笔异常交易的处理数据，并只在异常处理流程中使用。

交易流程如下图所示：



图C.2　增加的终端特殊处理流程

a) 终端发现最后一条记录没有读取成功，首先保存本笔交易的所有信息，包括卡号、TC、随机数、动态签名数据、卡片的记录等，并提示持卡人“请重新刷卡”；
b) 持卡人重刷卡片，终端重新对卡片进行上电，并在选择 PPSE 和 AID 后，通过读记录的方式，从卡片中读出卡号，判断是否是同一张卡，如果不是，则发起 GPO，执行正常交易流程；
c) 终端通过 Get Data 指令，读取卡片 ATC，并判断新读出的 ATC 是否与已保存的上笔交易的 ATC 相等，如果不相等，则发起 GPO，执行正常交易流程；
d) 终端通过 Get Data 指令，读取卡片当前余额，余额数据标签根据上笔交易货币代码判断是选择第一货币余额还是第二货币余额，并判断已保存的上笔交易余额减去上笔交易金额是否等于当前余额，如果不相等，则发起 GPO，执行正常交易流程；
e) 终端读取 AFL 中的最后一条记录，如果读取成功则执行正常的后续流程；如果依然读取失败，则跳转到异常处理流程中的“提示重新刷卡”。