ICS 35.240.40
A 11
备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0025.14—2013

中国金融集成电路（IC）卡规范 第14部分：非接触式IC卡小额支付扩展应用规范

China financial integrated circuit card specifications—
Part 14：Comprehensive application specification based on contactless low-value payment application

2013-02-05 发布　　2013-02-05 实施

中国人民银行 发布

目　　次

前　言

JR/T 0025《中国金融集成电路（IC）卡规范》分为以下部分：

——第1部分：电子钱包/电子存折应用卡片规范（废止）；

——第2部分：电子钱包/电子存折应用规范（废止）；

——第3部分：与应用无关的IC卡与终端接口规范；

——第4部分：借记/贷记应用规范；

——第5部分：借记/贷记应用卡片规范；

——第6部分：借记/贷记应用终端规范；

——第7部分：借记/贷记应用安全规范；

——第8部分：与应用无关的非接触式规范；

——第9部分：电子钱包扩展应用指南（废止）；

——第10部分：借记/贷记应用个人化指南；

——第11部分：非接触式IC卡通讯规范；

——第12部分：非接触式IC卡支付规范；

——第13部分：基于借记/贷记应用的小额支付规范；

——第14部分：非接触式IC卡小额支付扩展应用规范；

——第15部分：电子现金双币支付应用规范；

——第16部分：IC卡互联网终端规范；

——第17部分：借记/贷记应用安全增强规范。

本部分为JR/T 0025的第14部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分主要起草单位：中国人民银行、中国工商银行、中国银行、中国建设银行、中国农业银行、交通银行、上海浦东发展银行、中国邮政储蓄银行、中国银联股份有限公司、中国金融电子化公司、银行卡检测中心、中钞信用卡产业发展有限公司、捷德(中国)信息科技有限公司、惠尔丰（中国）信息系统有限公司、福建联迪商用设备有限公司。

本部分主要起草人：王永红、李晓枫、陆书春、潘润红、杜宁、陈则栋、吴晓光、李春欢、刘志刚、张永峰、汤沁莹、李新、张栋、王红剑、李一凡、余沁、周新衡、张步、冯珂、李建峰、向前、涂晓军、齐大鹏、俞益宁、曾静静、陈震宇、郑元龙、聂舒、丁吉、白雪晶、李子达、沈卓群、刘世英、于海涛、翁秀诚。

本部分为首次发布。

引　言

本部分为 JR/T 0025 的第 14 部分，与第 4 部分、第 5 部分、第 6 部分、第 7 部分、第 12 部分以及第 13 部分一起构成基于借记/贷记的小额支付扩展应用。

本部分主要定义了与小额支付扩展应用有关的内容，即小额支付扩展应用的技术实现与所支持的交易类型等。本部分未特别说明的内容，与标准借记/贷记应用以及小额支付应用一致，相关要求在JR/T 0025.4、JR/T 0025.5、JR/T 0025.6、JR/T 0025.7、JR/T 0025.12、JR/T 0025.13和JR/T 0025.17中描述。

中国金融集成电路（IC）卡规范
第14部分：非接触式IC卡小额支付扩展应用规范

1 范围

本部分对基于非接触IC卡小额支付的扩展应用做出了相关要求和规定，主要应用于分段扣费、脱机预授权、单次扣款优惠等特定的小额支付场景。

本部分适用于开展快速借记/贷记非接触式支付应用（qPBOC）的地区、发卡机构以及商户。其使用对象主要是与金融IC卡应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等相关部门（单位）。

有关快速借记/贷记非接触式支付应用（qPBOC）方面的要求在JR/T 0025.12进行了定义。有关物理特性、射频功率和信号接口、初始化、冲突检测和传输协议的要求在JR/T 0025.8和JR/T 0025.11进行了定义。

2 规范性引用文件

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

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

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

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

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

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

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

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

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

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

CAPP记录 CAPP records

扩展应用专用文件的记录，包括扩展应用循环记录文件和扩展应用专用文件的记录。

3.2

命令 command

终端向IC卡发出的一条报文，该报文启动一个操作或请求一个响应。

3.3

扩展应用专用文件 comprehensive application specified file

扩展应用专用文件用于存储特定的行业应用信息，通常情况下是变长记录结构文件。

3.4

扩展应用循环记录文件 comprehensive application cyclic file

扩展应用循环记录文件作为一些日志类的数据记录存储，是循环记录结构文件。每次交易，UPDATE CAPP DATACACHE命令只更新第一条记录。

3.5

密文 cryptogram

密码加密运算的结果。

3.6

押金抵扣 deposit deduction

押金抵扣是指发卡行可以给予持卡人一定的押金额度，该金额不计入电子现金的实际金额，但是当持卡人卡片内电子现金余额不足且小于押金额度时，持卡人可以选择使用押金来完成交易。

3.7

电子现金（EC） electronic cash (EC)

基于借记/贷记应用上实现的小额支付功能。

3.8

电子现金余额 electronic cash balance

一个计数器，表示卡片上可脱机消费的金额。

3.9

电子现金余额上限 electronic cash funds limit

持卡人可用来脱机消费的最大金额。

3.10

ID号 identify number

用于区分同一行业在不同地区的应用。

3.11

圈存 load

增加卡中电子现金余额的过程。圈存有多种实现方式，可以从主账户中划入金额，也可以现金存款，又或者从其它账户转入金额，但圈存后的电子现金余额不能超过电子现金余额上限。

3.12

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

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

3.13

响应 response

IC卡处理完收到的命令报文后，返回给终端的报文。

3.14

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。

3.15

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。

3.16

脚本 script

发卡行向终端发送的命令或命令序列，目的是向IC卡连续输入命令。

3.17

分段扣费 section purchase

分段扣费是在原来的标准qPBOC交易流程的基础上，在GPO命令处理和READ RECORD命令处理之间，增加了更新扩展应用数据的UPDATE CAPP DATA CACHE命令。以满足脱机小额快速支付应用中可能遇到的分时、分段计费的需求。

3.18

终端 terminal

在交易点安装、用于与IC卡配合共同完成金融交易的设备。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）。

4 符号和缩略语

下列符号和缩略语表示适用于本文件。

AC	应用密文(Application Cryptogram)
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）
APDU	应用协议数据单元（Application Protocol Data Unit）
ATC	应用交易计数器（Application Transaction Counter）
C	条件（Condition）
CAPP	扩展应用（Comprehensive Application）
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)
cn	压缩数字型（Compressed Numeric）
DDA	动态数据认证（Dynamic Data Authentication）
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）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
IDD	发卡行自定义数据（Issuer Defined Data）
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）
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)
PPSE	近距离支付系统环境（Proximity Payment Systems Environment）
qPBOC	快速借记/贷记应用（quick PBOC）
RFU	预留（Reserved f or Future Use）
R-MAC	响应数据的报文鉴别码（Response Message Authentication Code）
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）
TVR	终端验证结果（Terminal Verification Results）
YYYYMMDD	年、月、日（Year, Month, Day）

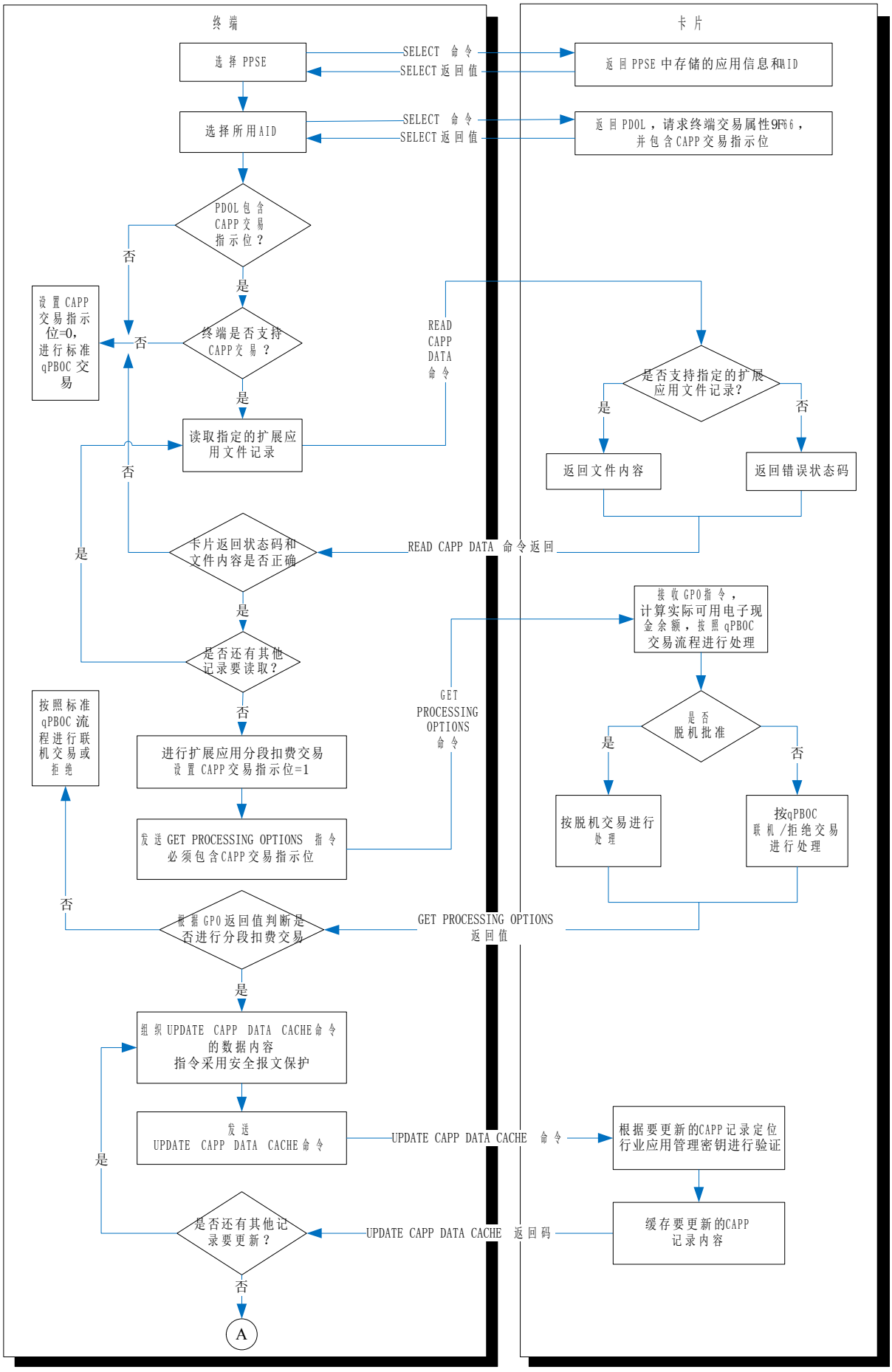
5 标准分时分段扣费交易流程

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qPBOC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。符合本规范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必须确保同时执行，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。

5.1 分段扣费交易流程图

分段扣费交易流程见图1所示。


终端
卡片
选择PPSE
SELECT 命令
SELECT返回值
返回PPSE中存储的应用信息和AID
选择所用AID
SELECT 命令
SELECT返回值
返回PDOL，请求终端交易属性9F66，并包含CAPP交易指示位
PDOL包含CAPP交易指示位？
否
是
设置CAPP交易指示位=0，进行标准qPBOC交易
终端是否支持CAPP交易？
否
是
READ CAPP DATA 命令
是否支持指定的扩展应用文件记录？
是
否
读取指定的扩展应用文件记录
返回文件内容
返回错误状态码
否
卡片返回状态码和文件内容是否正确
READ CAPP DATA 命令返回
是
是
是否还有其他记录要读取？
否
接收GPO指令，计算实际可用电子现金余额，按照qPBOC交易流程进行处理
GET PROCESSING OPTIONS 命令
按照标准qPBOC流程进行联机交易或拒绝
进行扩展应用分段扣费交易
设置CAPP交易指示位=1
是否脱机批准
是
否
按脱机交易进行处理
按qPBOC联机/拒绝交易进行处理
发送GET PROCESSING OPTIONS 指令
必须包含CAPP交易指示位
否
根据GPO返回值判断是否进行分段扣费交易
GET PROCESSING OPTIONS 返回值
是
组织UPDATE CAPP DATA CACHE命令的数据内容
指令采用安全报文保护
发送UPDATE CAPP DATA CACHE命令
UPDATE CAPP DATA CACHE 命令
根据要更新的CAPP记录定位行业应用管理密钥进行验证
是
是否还有其他记录要更新？
UPDATE CAPP DATA CACHE 返回码
缓存要更新的CAPP记录内容
否
A

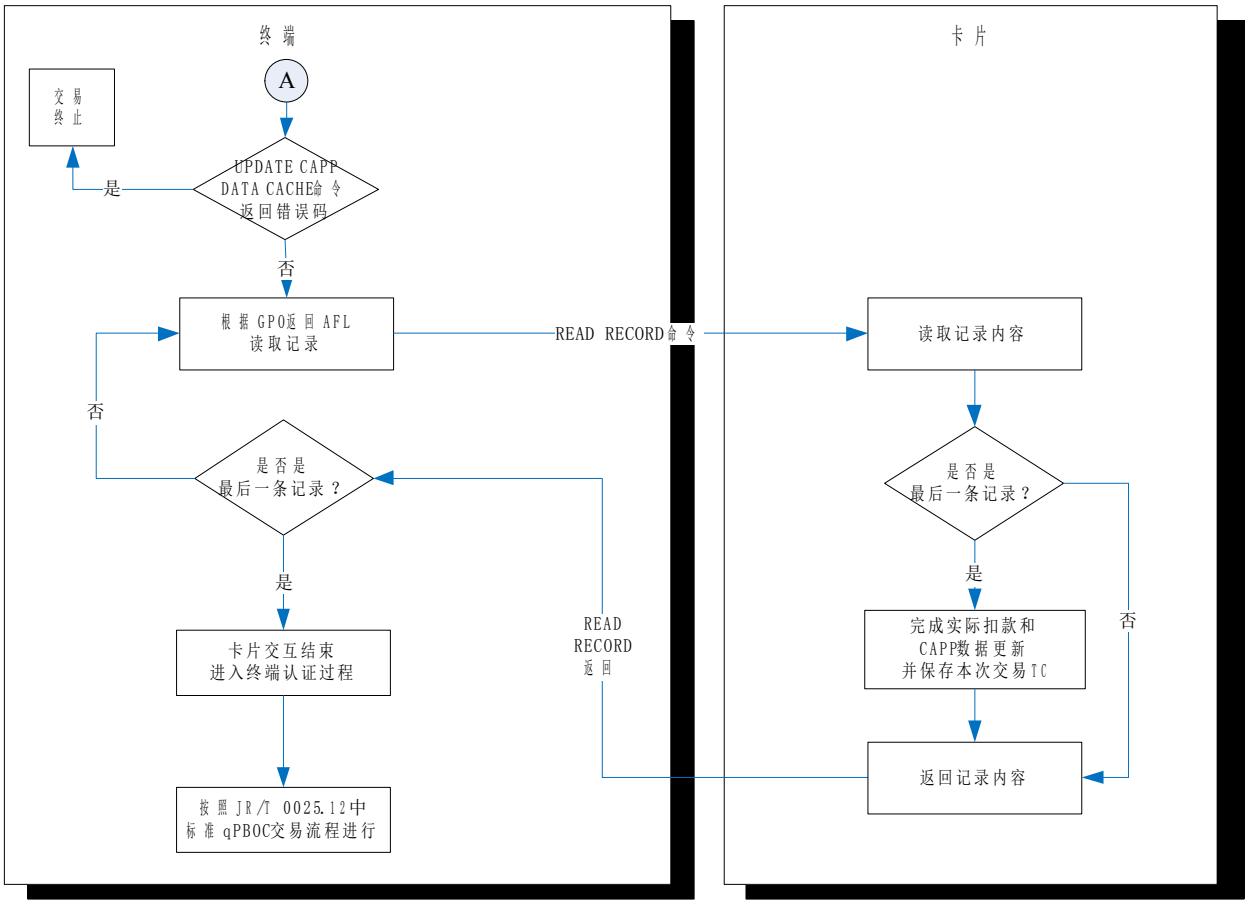


图 1.　　分段扣费交易流程图

5.2　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：

5.2.1　应用选择

终端按照 qPBOC 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，则其中必须包括请求 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：

1）　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 qPBOC 交易或根据需要终止交易；

2）　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。

3）　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，则终端应检查并验证卡片返回的 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 qPBOC 交易或根据需要终止交易。

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

5.2.2 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。

算法选择具体见 JR/T 0025.17 10.3.3。

当收到 GPO 命令时，卡片将按如下流程顺序处理：

按标准 qPBOC 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 qPBOC 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 qPBOC 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）。

5.2.3 分段扣费处理

收到 GPO 命令响应数据后，终端将作如下处理：

——终端组织更新 CAPP 记录的内容，通过安全模块计算相应的 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，则终端应检查并验证 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，则终端应终止此次分段扣费交易。

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。

5.2.4 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，并保存本次交易应用密文（TC），交易正常完成。

5.2.5 终端行为分析

见 JR/T 0025.12。

5.2.6 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。

5.2.7 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，发卡行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。

1）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。

2）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）。

3）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。

4）圈存操作

发卡行后台圈存流程保持与现有流程一致。

卡片收到发卡行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：

- 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；
- 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。

5）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。

6）更新分段扣费抵扣限额操作

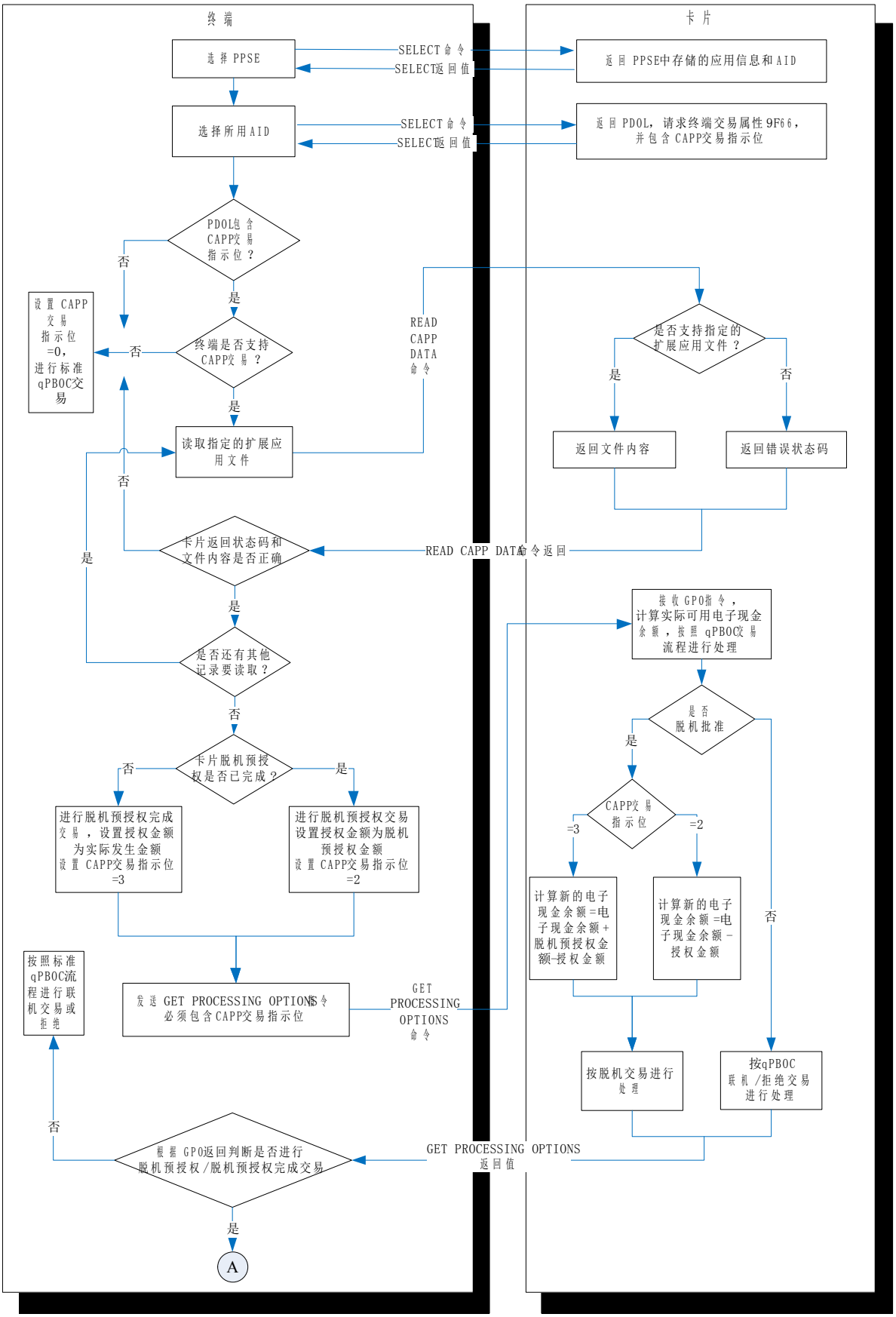
——卡片收到发卡行发送的修改分段扣费抵扣限额（DF62）的脚本命令时，如果修改分段扣费抵扣限额的脚本中指定的分段扣费抵扣限额（DF62）小于分段扣费已抵扣金额（DF63），则返回 6A80；否则，用脚本中指定的值完成分段扣费抵扣限额（DF62）的更新。

6 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。

6.1 脱机预授权交易流程图

脱机预授权交易见图2所示。



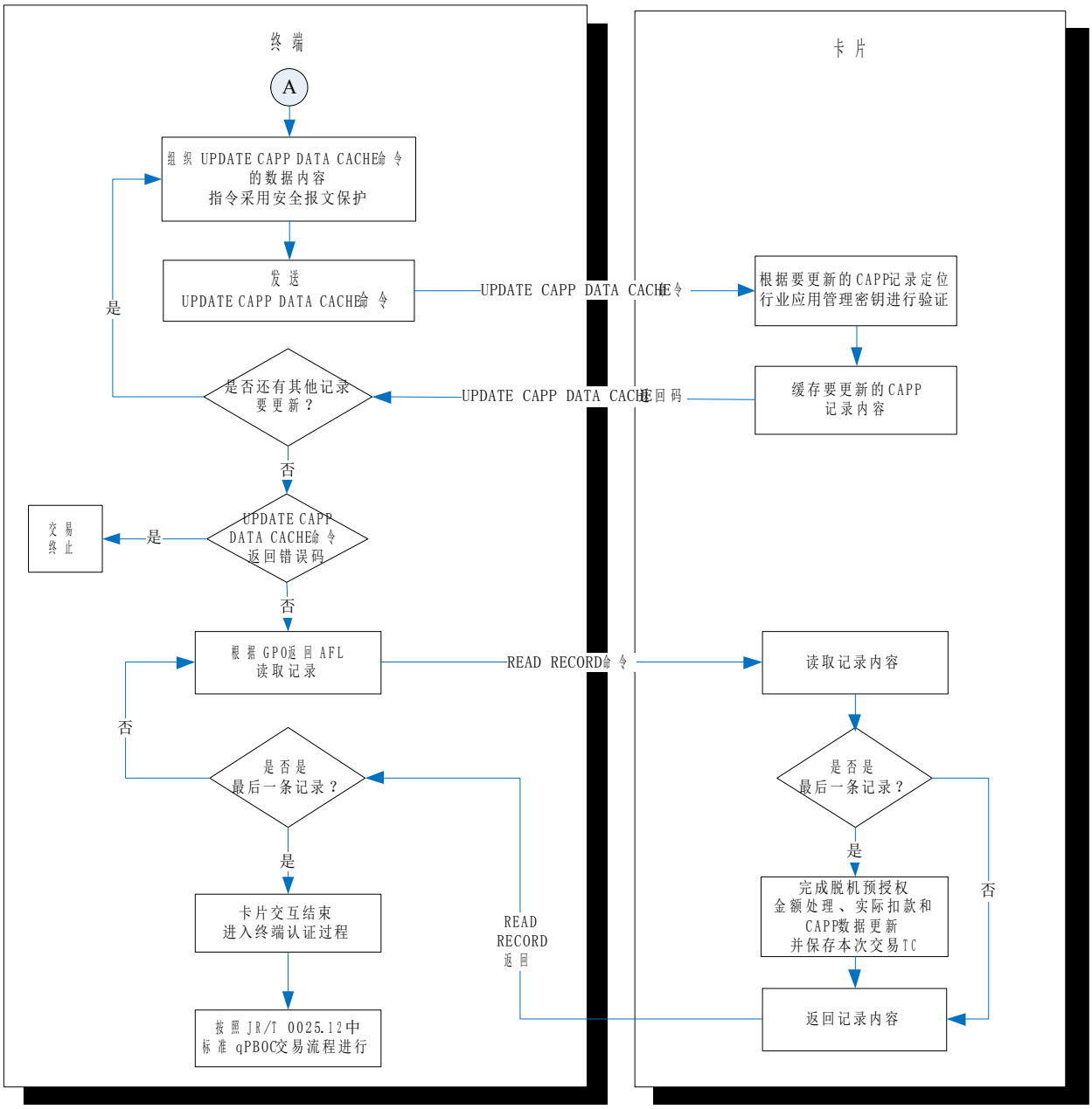


图 2.　　脱机预授权交易流程图

6.2　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：

6.2.1　应用选择

终端按照 qPBOC 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：

1）　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 qPBOC 交易或根据需要终止交易；

2） 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。

3） 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，则终端应检查并验证卡片返回的 R-MAC 值。如 R-MAC 验证错误，则终止交易；

4） 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 qPBOC 交易或根据需要终止交易；

5） 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；

6） 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。

6.2.2 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。

当收到 GPO 命令时，卡片将按如下顺序进行处理：

1） 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 qPBOC 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 qPBOC 联机/拒绝交易流程处理 GPO 命令；

2） 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’；

3） 与标准 qPBOC 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）。

6.2.3 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，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；

——终端通过安全模块计算相应的 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，则终端应检查并验证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，则终端均应终止此次脱机预授权交易。

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。

6.2.4 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；

——卡片必须在验证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；

6.2.5 终端行为分析

见JR/T 0025.12。

6.2.6 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。

6.2.7 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。

6.2.8 脱机预授权未完成状态下的圈存与查询操作

——圈存操作

- 发卡行后台圈存流程与现有流程保持一致；

- 为了避免圈存时发卡行下发圈存脚本导致卡片金额超限，卡片在收到GENERATE AC指令后，返回的发卡行应用数据（9F10）中如包含发卡行自定义数据项，则卡片在计算发卡行自定义数据项时，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；
- 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

- 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。

7 单次扣款优惠流程

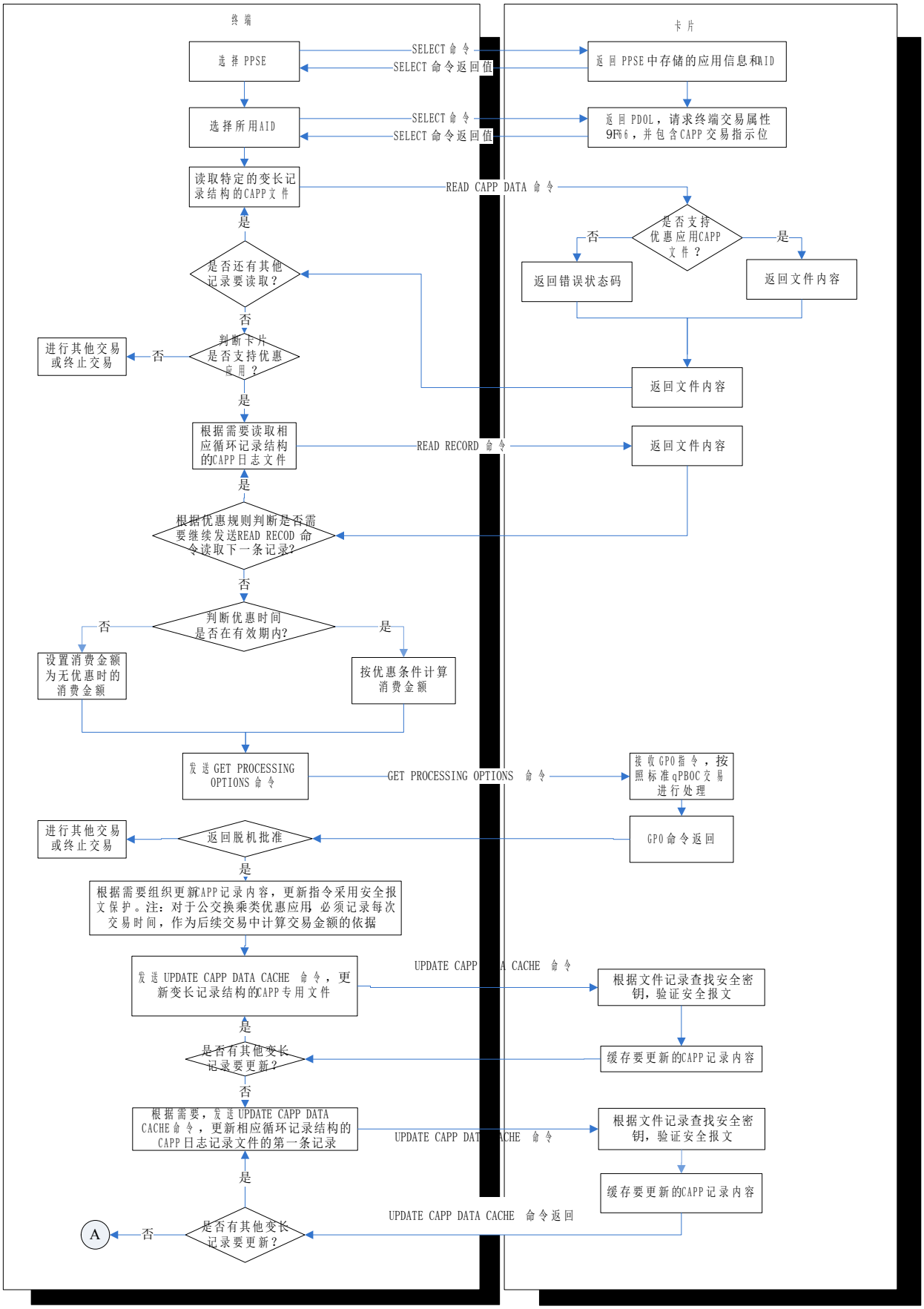
单次扣款优惠是指在交易时根据读取的扩展应用专用文件信息，判断卡片是否需要进行优惠处理的过程。单次扣款优惠多用于公交换乘优惠、学生卡、老人卡等场景。

——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3所示。


终端
卡片
选择PPSE
SELECT命令
SELECT命令返回值
返回PPSE中存储的应用信息和AID
选择所用AID
SELECT命令
SELECT命令返回值
返回PDOL，请求终端交易属性9F66，并包含CAPP交易指示位
读取特定的变长记录结构的CAPP文件
READ CAPP DATA命令
是否支持优惠应用CAPP文件？
否
是
返回错误状态码
返回文件内容
是
是否还有其他记录要读取？
否
判断卡片是否支持优惠应用？
否
进行其他交易或终止交易
返回文件内容
是
根据需要读取相应循环记录结构的CAPP日志文件
READ RECORD命令
返回文件内容
是
根据优惠规则判断是否需要继续发送READ RECOD命令读取下一条记录?
否
判断优惠时间是否在有效期内?
否
是
设置消费金额为无优惠时的消费金额
按优惠条件计算消费金额
发送GET PROCESSING OPTIONS命令
GET PROCESSING OPTIONS命令
接收GPO指令，按照标准qPBOC交易进行处理
进行其他交易或终止交易
返回脱机批准
GPO命令返回
是
根据需要组织更新CAPP记录内容，更新指令采用安全报文保护。注：对于公交换乘类优惠应用，必须记录每次交易时间，作为后续交易中计算交易金额的依据
发送UPDATE CAPP DATA CACHE命令，更新变长记录结构的CAPP专用文件
UPDATE CAPP DATA CACHE命令
根据文件记录查找安全密钥，验证安全报文
是
是否有其他变长记录要更新？
缓存要更新的CAPP记录内容
否
根据需要，发送UPDATE CAPP DATA CACHE命令，更新相应循环记录结构的CAPP日志记录文件的第一条记录
UPDATE CAPP DATA CACHE命令
根据文件记录查找安全密钥，验证安全报文
是
缓存要更新的CAPP记录内容
UPDATE CAPP DATA CACHE命令返回
A
否
是否有其他变长记录要更新？

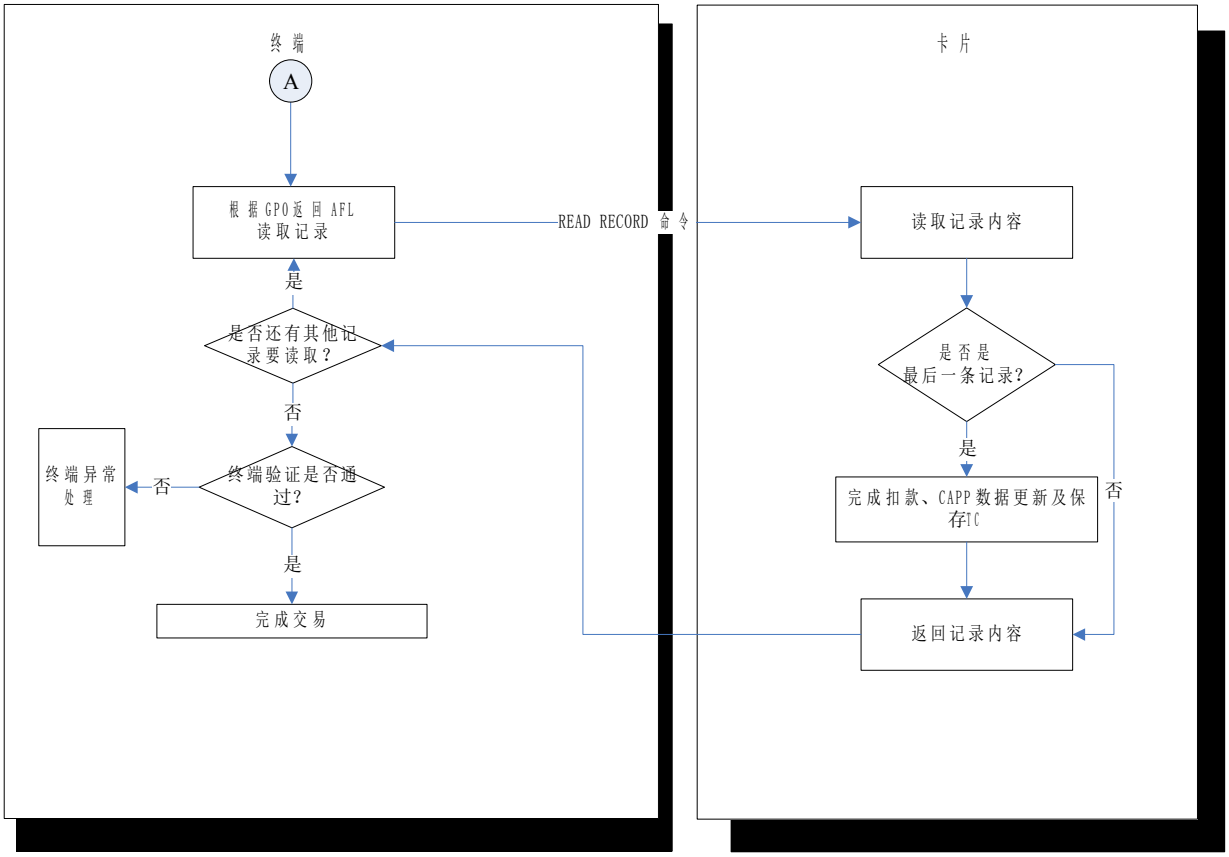


图 3.　　单次扣款优惠交易流程

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

持卡人使用非接触式金融 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：

- 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。
- 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。
- 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，则终端应检查并验证 R-MAC。具体方法同分段扣费和脱机预授权交易流程中描述。

8　安全性要求

8.1　密钥说明

对支持非接触小额支付扩展应用的卡片，在个人化时需创建本部分定义的扩展应用专用文件（详见附录 B）。每个扩展应用文件对应一个应用开通密钥，每个行业应用的开通都由此密钥以安全报文的方式保护，卡片的应用开通密钥由同一个应用开通主密钥分散得到。扩展应用专用文件中每一条记录代表一个特定行业在特定地区的应用，由行业定义的行业应用管理密钥针对每一条记录进行保护。密钥类型见表 1 所示。

表 1　密钥类型说明

密钥类型	用途	长度	管理方
应用开通密钥	用于开通行业应用	16 字节	发卡行
行业应用管理密钥	用于行业应用记录的数据修改权限控制	16 字节	行业合作方

注 1：行业应用的开通过程，参见附录 F。

注 2：行业应用管理密钥的生成和管理，由行业合作方自行定义。

8.2　安全机制

终端使用 APPEND RECORD 指令在指定行业应用的扩展应用文件中新增应用记录，即开通新的行业应用。使用 APPEND RECORD 命令在扩展应用文件中新增应用记录，使用 UPDATE CAPP DATA CACHE 命令更新应用文件数据，这两条指令都强制带有安全报文，以便卡片确认指令来自于合法的终端。

安全报文以‘00’‖‘00’‖‘00’‖‘00’‖‘00’‖‘00’‖ATC 作为初始向量参与 MAC 运算。MAC 的计算方法见 JR/T0025.7 或 JR/T 0025.17 中关于报文鉴别码的描述。终端在发送 APPEND RECORD 和 UPDATE CAPP DATA CACHE 指令之前，可以通过发送 GET DATA 指令，或者通过发送 GPO 指令获取 ATC。

在 APPEND RECORD 指令中，附带有行业应用管理密钥设置，详见附录 A.3。行业应用开通后，此行业应用的应用数据的修改权限，由对应的行业应用管理密钥以安全报文的方式控制。终端通过 UPDATE CAPP DATA CACHE 指令修改行业应用数据。扩展应用支持应用失效功能，即行业终端在更新应用数据时将应用有效标识置零。

9　扩展应用个人化要求

对于仅支持分时、分段扣费功能的卡片，发卡行在个人化数据时应在 SELECT AID 返回的文件控制信息（FCI）中的发卡行自定义数据（BF0C）中写入分时、分段扣费标识（DF61）=0x01。对于同时支持分时、分段扣费功能和脱机预授权功能的卡片（DF61）=0x02。

个人化用于非接触界面的 PDOL 时，需要包含 CAPP 交易指示位。在非接触界面下，若卡片返回的 PDOL 中出现 CAPP 交易指示位，则表明卡片支持基于非接触小额支付的扩展应用；若终端决定执行特定扩展应用功能，则在 GPO 命令中提供 CAPP 交易指示位，并设置为相应数值；若终端不支持扩展应用，则将 CAPP 交易指示位设置为“0”。终端将设置后的 CAPP 交易指示位通过 GPO 指令发送给卡片。

发卡行在个人化时预先创建扩展应用文件，预置应用开通密钥。在使用前，由持卡人在专用设备上进行开通，即创建对应扩展应用文件的行业应用记录，并将行业应用管理密钥写入卡片。

对于循环记录文件，文件由发卡行个人化时预先创建，如果行业有使用循环记录文件的需求，则可以在持卡人开通业务时，通过 APPEND RECORD 命令新增一条记录，以后通过 UPDATE CAPP DATA CACHE 来更新该文件中的记录。该文件对应一条行业应用管理密钥。

附 录 A
（规范性附录）
新增扩展应用专用指令

A.1 READ CAPP DATA（读取扩展应用数据）命令

A.1.1 定义和范围

READ CAPP DATA 命令用于扩展应用交易中，终端判断卡片是否支持相应行业应用，同时可获得上笔扩展应用交易信息。

终端通过扩展应用的所属的 ID 号（ID 号由支付系统定义，不足位数后补 0）和扩展应用行业类型，决定读取某一扩展应用文件的指定记录，在同一个 SFI 下，ID 应保持唯一。

卡片在接收到 READ CAPP DATA 命令后，将进行以下操作：

——根据 P2 指定的 SFI 选取相应的 EF 文件。如果文件不存在，卡片回送状态码‘6A82’（未找到文件）。

——如果 EF 文件不是变长记录文件，卡片回送状态字‘6981’（文件类型不符）。

A.1.2 命令报文

此命令报文见表 A.1：

表 A.1 READ CAPP DATA 命令报文

代码	值
CLA	‘80’
INS	‘B4’
P1	‘00’
P2	见表 A.2
Lc	‘02’或‘0A’
Data	详见说明
Le	‘00’

此命令报文中的引用控制参数 P2 定义如表 A.2 所示：

表 A.2 READ CAPP DATA 命令报文中引用控制参数 P2 定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0	0	0	0	0	—	—	—	RFU
X	X	X	X	X	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	0	0	0	第一个区号出现的记录
—	—	—	—	—	0	0	1	同一区号的下一条记录
—	—	—	—	—	X	X	X	RFU
其它值								RFU

A.1.3 命令报文数据域

当卡片不支持扩展应用记录的 R-MAC 保护时，命令报文数据域包括 2 个字节的 ID 号；当卡片支持扩展应用记录的 R-MAC 保护时，命令报文数据域包括 2 个字节的 ID 号和 8 个字节的终端随机数。

A.1.4 响应报文数据域

当卡片不支持扩展应用记录的 R-MAC 保护时，响应报文数据包括指定 ID 号的记录内容；当卡片支持扩展应用记录的 R-MAC 保护时，响应报文数据域包括指定 ID 号的记录内容和 4 个字节的 R-MAC 值。

响应报文数据中的 R-MAC，由卡片根据 JR/T0025.7 中关于报文鉴别码的描述，使用行业应用管理密钥对响应数据进行加密生成，其初始向量为命令报文数据域中的终端随机数。

A.1.5 响应报文的状态码

命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 A.3：

表 A.3 READ CAPP DATA 错误状态码表

SW1	SW2	含 义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF 文件）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够
‘94’	‘07’	应用禁止

A.2 UPDATE CAPP DATA CACHE(更新数据缓存)命令

A.2.1 定义和范围

UPDATE CAPP DATA CACHE 命令用于扩展应用交易中更新应用数据缓存。

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

——根据 P2 指定的 SFI 选取相应的 EF 文件。如果文件不存在，卡片回送状态码‘6A82’（未找到文件）。终端应终止此次扩展应用交易。

——检查扩展应用专用文件的使用条件，若该命令的前续命令不是 GPO 命令或另一条 UPDATE CAPP DATA CACHE 命令，则回送状态码‘6985’(使用条件不满足)。终端应终止此次扩展应用交易。

——若待更新的扩展应用专用文件是变长记录文件，则根据命令数据域中的 ID 号，查询扩展应用专用文件中是否存在相同 ID 号的记录。如果不存在，则回送状态码‘6A83’（未找到记录）。终端应终止此次扩展应用交易。

——检查命令中的数据域长度是否大于扩展应用专用文件中相应记录的长度。如果大于，则回送状态码‘6A84’（文件中存储空间不够）；如果小于，则回送状态‘6A80’(数据域不正确)。终端应终止此次扩展应用交易。

在通过以上检查后，卡片应暂存命令中的 SFI、记录号和应用数据。扩展应用专用文件中相应记录的数据不得通过此命令更新。

允许多次执行 UPDATE CAPP DATA CACHE 命令，来完成多条记录的更新。

扩展应用专用文件可以是变长记录结构，也可以是循环记录结构。若是变长记录结构，在使用 UPDATE CAPP DATA CACHE 命令更新扩展应用数据之前，必须保证文件中存在相应的记录；若是循环记录结构，每次执行该指令，将更新最新的一条记录，然后循环使用。

该命令必须采用安全报文方式。

A.2.2 命令报文

此命令报文见表 A.4：

表 A.4 UPDATE CAPP DATA CACHE 命令报文

代码	值
CLA	‘84’
INS	‘DE’
P1	‘00’
P2	见表 A.5
Lc	后续数据域的长度
Data	详见说明
Le	‘00’

此命令报文中的引用控制参数 P2 定义如表 A.5：

表 A.5　UPDATE CAPP DATA CACHE 命令报文中引用控制参数 P2 定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0	0	0	0	0	—	—	—	RFU
X	X	X	X	X	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	0	0	0	第一个 ID 号出现的记录(变长记录文件) 或最新的一条记录(循环记录文件)
—	—	—	—	—	0	0	1	下一个 ID 号出现的记录（变长记录文件）
—	—	—	—	—	X	X	X	RFU
其它值								RFU

A.2.3　命令报文数据域

命令报文数据域包含记录内容和安全报文。

若当前文件为变长记录文件，记录内容包含 ID 号、记录长度等扩展应用信息和扩展应用数据；若当前文件是循环记录文件，命令报文数据域包含扩展应用数据。

A.2.4　响应报文数据域

当卡片不支持扩展应用记录的 R-MAC 保护时，响应报文数据域不存在；当卡片支持扩展应用记录的 R-MAC 保护时，响应报文数据为 4 字节的 R-MAC 值。

响应报文数据中的 R-MAC，由卡片根据 JR/T0025.7 中关于报文鉴别码的描述，使用行业应用管理密钥对响应报文的状态码进行加密生成，其初始向量为‘00’‖‘00’‖‘00’‖‘00’‖命令报文数据域中的 MAC。

A.2.5　响应报文的状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 A.6：

表 A.6　UPDATE CAPP DATA CACHE 错误状态码表

SW1	SW2	含　义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF 文件）
‘6A’	‘80’	数据域不正确
‘6A’	‘81’	不支持此功能

‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够
‘94’	‘07’	应用禁止

A.3 APPEND RECORD(新增记录)命令

A.3.1 定义和范围

APPEND RECORD 命令用于扩展应用开通时，向扩展应用文件中增加行业应用记录。可以用于向循环记录文件中添加记录，也可以用于向扩展应用循环记录文件中初始化第一条记录，记录空间在 APPEND RECORD 命令时动态分配。

卡片接收到 APPEND RECORD 命令后，将进行如下处理：

——判断新增记录长度是否超过文件记录最大长度限制，如果超过，卡片回送状态字‘6A80’；

——判断文件剩余空间是否足够，如果空间不足，卡片回送状态字‘6A84’；

通过以上判断，卡片将根据命令数据域的记录数据长度，分配记录空间，将新的记录数据写入文件。

A.3.2 命令报文

此命令报文见表 A.7：

表 A.7 APPEND RECORD 命令报文

代码	值
CLA	‘04’
INS	‘E2’
P1	‘00’
P2	见表 A.8
Lc	后续数据域的长度
Data	16 字节记录修改密钥（由应用开通密钥加密）+新增的记录内容 + MAC
Le	不存在

此命令报文中的引用控制参数 P2 定义见表 A.8：

表 A.8 APPEND RECORD 命令报文中引用控制参数 P2 定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0	0	0	0	0	—	—	—	RFU
X	X	X	X	X	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	X	X	X	RFU
其它值								RFU

A.3.3 命令报文数据域

此命令报文数据域由加密后的 16 字节的记录修改密钥、新增的记录内容（扩展应用数据）和 MAC 组成。

A.3.4 响应报文数据域

响应报文数据域不存在。

A.3.5 响应报文的状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 A.9 所示：

表 A.9 APPEND RECORD 错误状态码表

SW1	SW2	含 义

‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF 文件）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够
‘94’	‘07’	应用禁止

A.4 GET TRANS PROVE（取脱机交易应用密文）命令

A.4.1 定义和范围

GET TRANS PROVE 命令用于获取指定的 ATC（应用交易计数器）对应扩展应用交易的 TC(脱机交易应用密文)。使用场景为，终端在无法接收到最后一条交易指令响应数据的情况下，重新上电并发送此命令，获取上笔失败交易的 TC，如果命令响应成功，则终端判断上笔交易成功，否则，按交易失败处理。

该命令只能获取最近一笔卡片成功完成的扩展应用交易的 TC。如果最近一笔交易是脱机预授权交易，则返回的 TC 为全零。

A.4.2 命令报文

此命令报文见表 A.10：

表 A.10 GET TRANS PROVE 命令报文

代码	值
CLA	‘80’
INS	‘5A’
P1	‘00’
P2	‘00’
Lc	‘02’
Data	终端指定的交易 ATC
Le	‘08’

A.4.3 命令报文数据域

命令报文数据域由终端指定的交易 ATC 组成。

A.4.4 响应报文数据域

响应报文数据域返回终端指定交易 ATC 对应的 TC（8 字节）。

A.4.5 响应报文的状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的错误状态码见表 A.11 所示：

表 A.11 GET TRANS PROVE 错误状态码表

SW1	SW2	含义
‘65’	‘81’	内存失败
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	命令不存在

‘6E’	‘00’	命令类型不支持
‘94’	‘06’	所需 TC 不可用

附 录 B
（规范性附录）
扩展应用专用文件

B.1 扩展应用专用文件

扩展应用专用文件是变长记录结构，在换乘优惠应用模式下，应增加一个循环记录结构的扩展应用循环记录文件，用于保存相应的换乘记录等信息。

若扩展应用专用文件为变长记录结构，应按表 B.1 创建扩展应用专用文件。

表 B.1 扩展应用变长记录文件

文件名称	变长扩展应用专用文件		文件类型	变长记录文件
文件标识	SFI （规定值见附录 C）		文件大小	自定义
单条记录最大长度	自定义			
文件权限	读取	自由		
	更新	保护		
记录编码				
字节	数据元			长度（bytes）
1-2	ID 标识（区号）			2
3	记录长度（后续数据长度）			1
4	应用有效标识（0 表示无效；1 表示有效）			1
5	扩展应用标识（1 表示本应用采用分段扣费；2 表示应用采用脱机预授权消费）			1
6	应用锁定标志（0 表示应用没有锁定；1 表示应用锁定）			1
7-n	应用数据			n-7

扩展应用短文件标识符的具体定义参见附录 C。对上表中的应用数据部分，行业合作方可通过安全验证方式，保障数据安全。

B.2 扩展应用循环记录文件

扩展应用循环记录文件，为循环记录结构。每次交易通过 UPDATE CAPP DATACACHE 命令只更新第一条记录，仅作为一些日志类的数据记录存储，建议按表 B.2 信息创建扩展应用循环记录文件。

本文件也可用于行业的其他自定义应用。

表 B.2 扩展应用循环记录文件

文件名称	扩展应用循环记录文件		文件类型	循环记录文件
文件标识	SFI=0x1E		文件大小	自定义
文件权限	读取	自由		
	更新	保护		
记录编码				
字节	数据元			长度（bytes）
1-n	扩展应用数据			n

支持换乘优惠的应用应将本次交易明细记录在扩展应用循环记录文件中。在换乘优惠时，可读取循环记录文件中的内容作为换乘优惠的依据。

附 录 C
（规范性附录）
扩展应用文件短文件标识符定义

对扩展应用文件短文件标识符（SFI）以及扩展应用开通密钥，做出如下定义。详见表 C.1 所示。

表 C.1 扩展应用文件短文件标识符及开通密钥定义

扩展应用类型	扩展应用文件 SFI	开通密钥
地铁应用	0x15	预设
公交应用	0x16	预设
高速公路不停车收费	0x17	预设
停车收费咪表应用	0x18	预设
铁路（高铁）应用	0x19	预设
银行自定义应用	0x1A、0x1B、	预设
保留应用	0x13、0x14、0x1C、0x1D	预设

附 录 D
（规范性附录）
新增数据元

本部分中引用而没有在 JR/T 0025.01 - JR/T 0025.13 中定义的或经修改的数据元在本附录中定义。新增数据元见表 D.1 所示。

表 D.1 新增数据元

名字	格式 标签 长度	需求	描述	取回	值
CAPP 交易指示位	F: b8 T: DF60 L: 1	条件 如果卡片支持 CAPP 扩展应用交易，则需在 PDOL 中指明此数据	指出终端支持的 CAPP 交易类型	N/A	0：表示终端不支持扩展应用 1：表示选择或执行分段扣费交易 2：表示选择或执行脱机预授权交易 3：表示选择或执行脱机预授权完成交易
分段扣费应用标识	F: b8 T: DF61 L: 1	如果卡片仅支持分段扣费交易时，发卡行在 BF0C 中进行个人化，支持取数据（Get Data）和设置数据（Put Data）命令	用于区别卡片支持扩展应用的能力	在文件控制信息（FCI）中发卡行自定义数据 BF0C 中返回	字节 1： 位 8:1=卡片支持对扩展应用记录数据的 R-MAC 保护 位 7~3:RFU（00000） 位 2=1:表示卡片既支持分段扣费功能也支持脱机预授权功能 位 1=1:表示卡片仅支持分段扣费功能
电子现金分段扣费抵扣限额	F: n12 T: DF62 L: 6 格式：cn	如果卡片支持分段扣费抵扣功能，支持取数据（Get Data）和设置数据（Put Data）命令。	表示卡片在分段扣费交易中可抵扣的最大额度	可通过取数据（Get Data）命令返回	
电子现金分段扣费已抵扣额	F: n12 T: DF63 L: 6 格式：cn	如果卡片支持分段扣费抵扣功能，支持取数据（Get Data），不支持设置数据（Put Data）命令。	表示卡片当前已抵扣的额度	可通过取数据（Get Data）命令返回	

附 录 E
（资料性附录）
分段扣费交易应用举例

本附录以基于非接触小额支付的分段扣费交易在特定应用环境中的应用为范例，描述分段扣费交易的实际应用模式。

注：以下范例描述的前提是终端支持特定的分段扣费交易应用。

E.1 地铁/铁路/高速公路收费/停车咪表应用

地铁/铁路/高速公路收费应用是分段收费模式；停车咪表应用是分时收费模式，但以上所有应用其交易流程是一致的。本条将重点以地铁收费应用为例描述基于非接触小额支付特定分段扣费应用的交易流程。整个交易分为进闸交易（即进消费区交易）和出闸交易（即出消费区交易）。关于终端上CVM的设置，参照电子现金要求执行。

E.1.1 地铁收费应用

E.1.1.1 进闸交易流程

——描述

进闸交易的基本流程为：选择 PPSE 支付环境，然后选择 qPBOC 应用，读取扩展应用专用文件，判断上次交易是否正常完成。若上次交易正常完成，则进行零金额消费，并更新文件；否则返回错误提示，提示持卡人不能进入收费区。

终端也可以根据实际需求进行预处理，例如可以事先获取卡片中的余额，来判断是否允许持卡人进站。

——流程图

地铁进闸交易流程见图 E.1 所示。

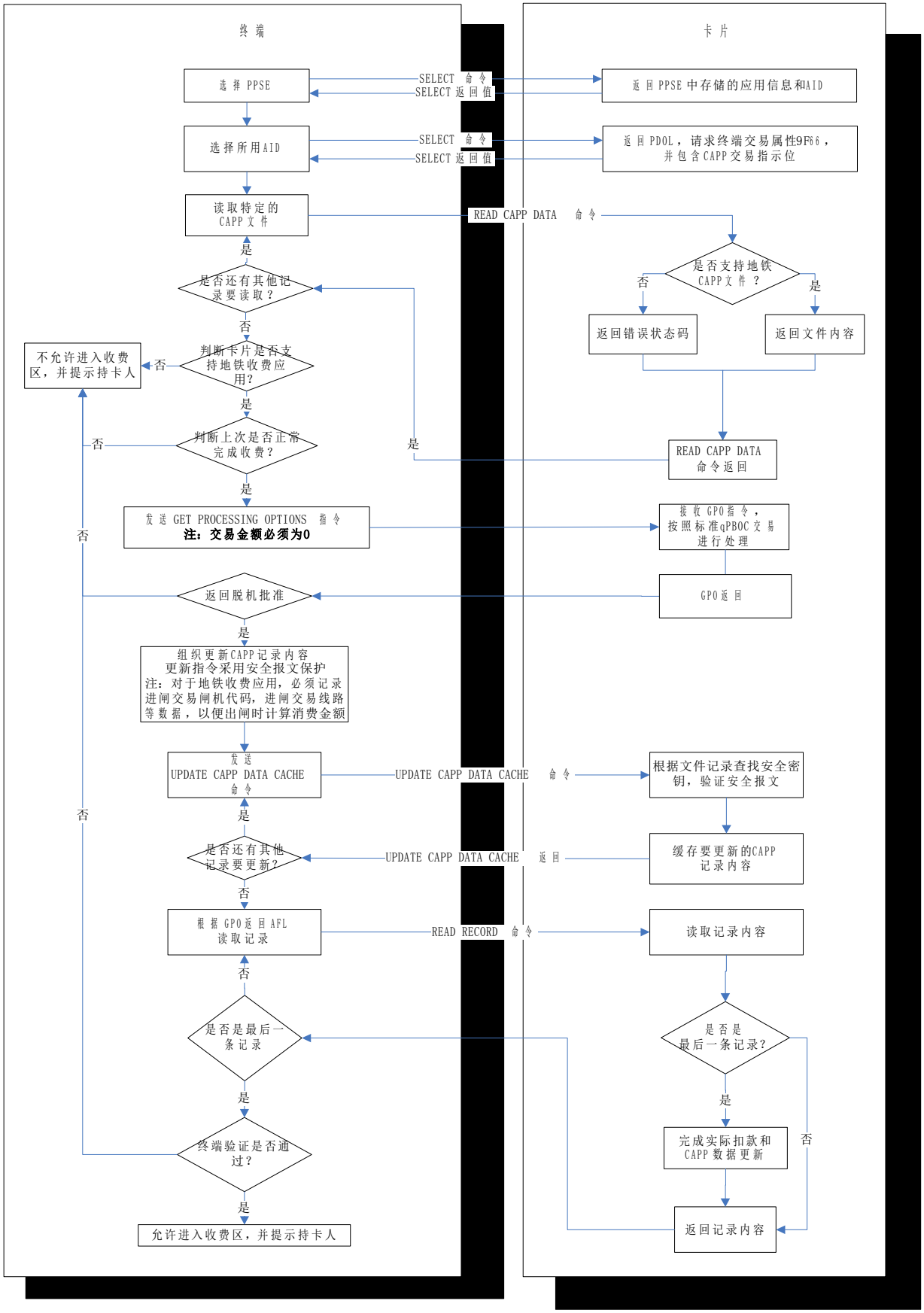


图 E.1　地铁消费应用的进闸交易流程

——流程说明

持卡人使用非接触式金融 IC 卡在地铁消费应用环境中进行进闸交易时，终端将作如下处理：

1） 终端首先选择和激活卡片，并通过 AID 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 RECORD 命令查询，判断卡片是否支持地铁收费应用。如支持，终端应读取此特定专用数据，并根据数据进行处理，如判断上次是否离开收费区等。如处理结果为不允许进行进闸交易，终端应提示持卡人。如处理结果允许进行进闸交易，终端进行分段扣费交易，其中交易金额为 0。

3） 终端根据其自身情况，在 UPDATE CAPP DATA CACHE 中更新地铁收费专用数据，填写城市代码、运营企业代码、记录格式版本号、交易标志、进收费区交易时间、进收费区交易线路代码、进收费区交易站点代码、进收费区交易闸机代码、进收费区交易序号和专用 TAC 等字段，并保留出收费区交易时间、出收费区交易线路代码、出收费区交易站点代码、出收费区交易闸机代码、出收费区交易金额、出收费区交易序号等记录原值。

4） 交易最后，终端根据交易过程中卡片返回的数据，对卡片进行动态数据认证。只有卡片通过认证，终端才允许持卡人进入收费区。

E.1.1.2 出闸交易流程

——描述

出闸交易的基本流程为：选择 PPSE 支付环境，然后选择 qPBOC 应用，读取扩展应用专用文件，判断文件内容是否正确，若正确，则根据入闸信息，计算消费金额。然后进行扣款消费，并更新扩展应用专用文件，表示正常完成交易，同时提示持卡人离开收费区。

——流程图

地铁出闸交易见流程见图 E.2 所示。

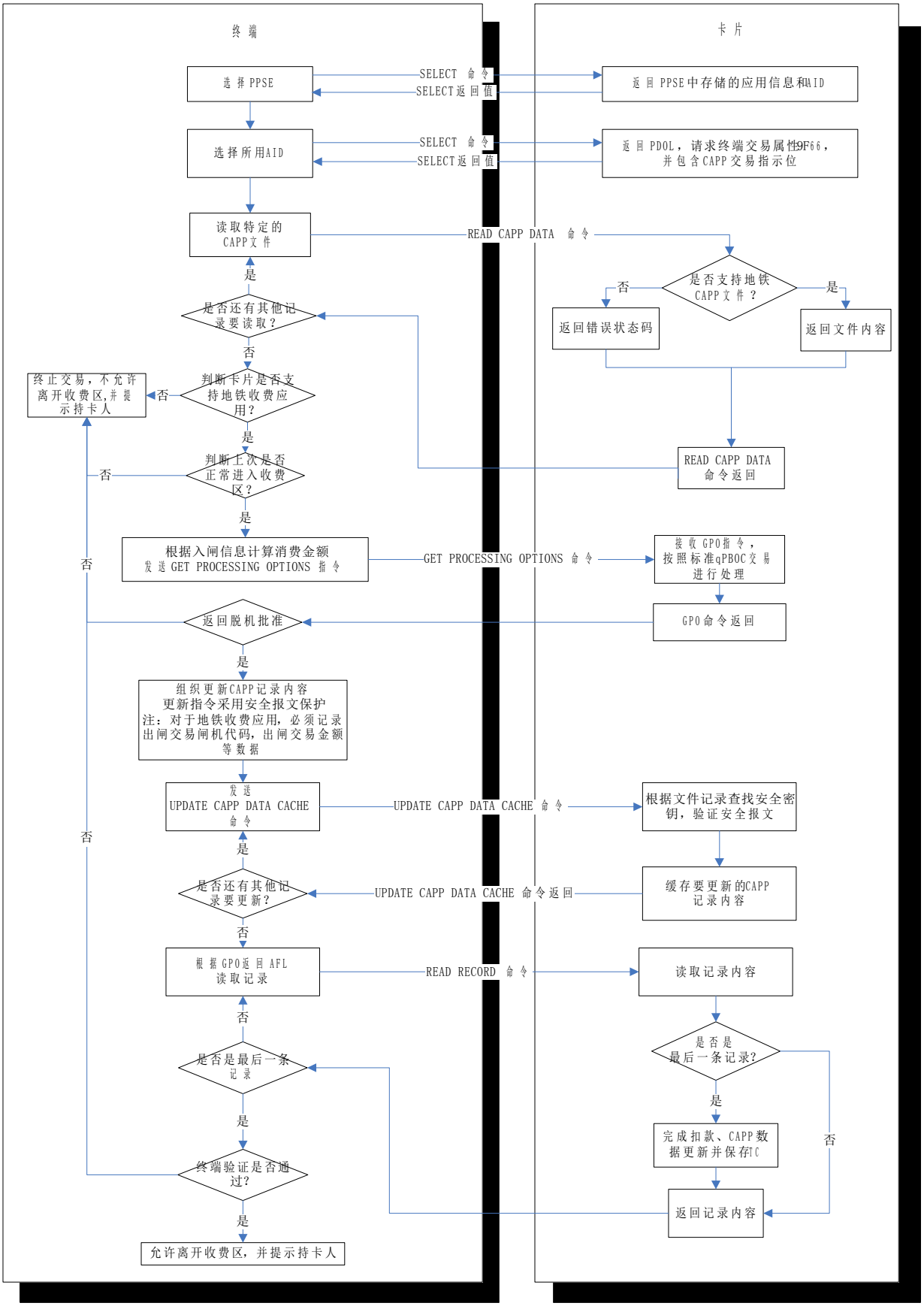


图 E.2　地铁消费应用的出闸交易流程

——流程说明

持卡人使用非接触式金融 IC 卡在地铁消费应用环境中进行出闸交易时，终端将作如下处理：

1） 终端首先选择和激活卡片，并通过 AID 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 RECORD 命令查询，判断卡片是否支持地铁收费应用。如支持，终端应读取地铁收费专用数据，并根据数据进行处理，如判断上次是否正常进入收费区等，若是，则根据扩展应用专用文件中的入闸信息计算消费金额。如处理结果为不允许进行出收费区交易，终端应提示持卡人。如处理结果允许进行出收费区交易，终端进行分段扣费交易，并更新扩展应用专用文件，其中交易金额为计算所得的消费金额。

3） 终端根据其自身情况，在 UPDATE CAPP DATA CACHE 中更新地铁收费专用数据，填写出收费区交易时间、出收费区交易线路代码、出收费区交易站点代码、出收费区交易闸机代码、出收费区交易金额、出收费区交易序号、专用 TAC 等记录，并保留城市代码、运营企业代码、记录格式版本号、交易标志、进收费区交易时间、进收费区交易线路代码、进收费区交易站点代码、进收费区交易闸机代码、进收费区交易序号等字段记录原值。

4） 交易最后，终端根据交易过程中卡片返回的数据，对卡片进行动态数据认证。只有卡片通过认证，终端才允许持卡人离开收费区。

E.1.2 城际收费/高速收费应用

城际收费/高速收费应用的交易流程与地铁收费应用的交易流程一样，也将交易分为进闸交易和出闸交易，只是收费标准不同。它们都是按行驶路段收费，所以在进闸交易时，对进闸交易闸机代码和进闸交易线路代码等的记录非常重要，这些信息是出闸时计算扣款金额的依据。

E.1.3 停车咪表应用

停车咪表应用的交易流程与地铁收费应用的交易流程一样，可以将交易分为停车交易和收费交易，等同于进闸交易和出闸交易。但地铁收费应用是按旅客的乘坐路段收费，而停车咪表应用是按顾客的停车时间收费，所以对于停车咪表应用，在停车交易时，对交易咪表代码和停车交易时间等的记录非常重要，这些信息是在收费交易时，计算扣款金额的依据。

E.2 公交日票/月票交易流程说明

除分时、分段扣费交易外，扩展应用还可以通过读取扩展应用专用文件，实现公交日票/月票应用功能。

E.2.1 公交日票/月票应用

——描述

扩展应用在公交日/月票领域的应用包括以下两种类型：限定次数型和不限次数型。其中，限定次数型表示限定日/月票在当日/月内的使用次数，每次进行等额消费，消费金额为日/月票总额与限定次数的比值；不限次数型表示不限定日/月票在当日/月内的使用次数，且在第一次使用时一次性扣减当天/整月的金额，以后每次进行 0 额消费。

日/月票交易的基本流程为：读取扩展应用专用文件，判断卡片是否支持公交日/月票应用，若支持，判断公交日/月票是否已使用；若未使用，则进行日/月票消费交易；若已使用，根据初次使用时间和（/或）使用次数，判断日/月票是否已过期，如果是则提示持卡人日/月票已过期，否则继续进行日/月票消费交易。

——流程图

公交日票/月票消费交易流程见图 E.3 所示。

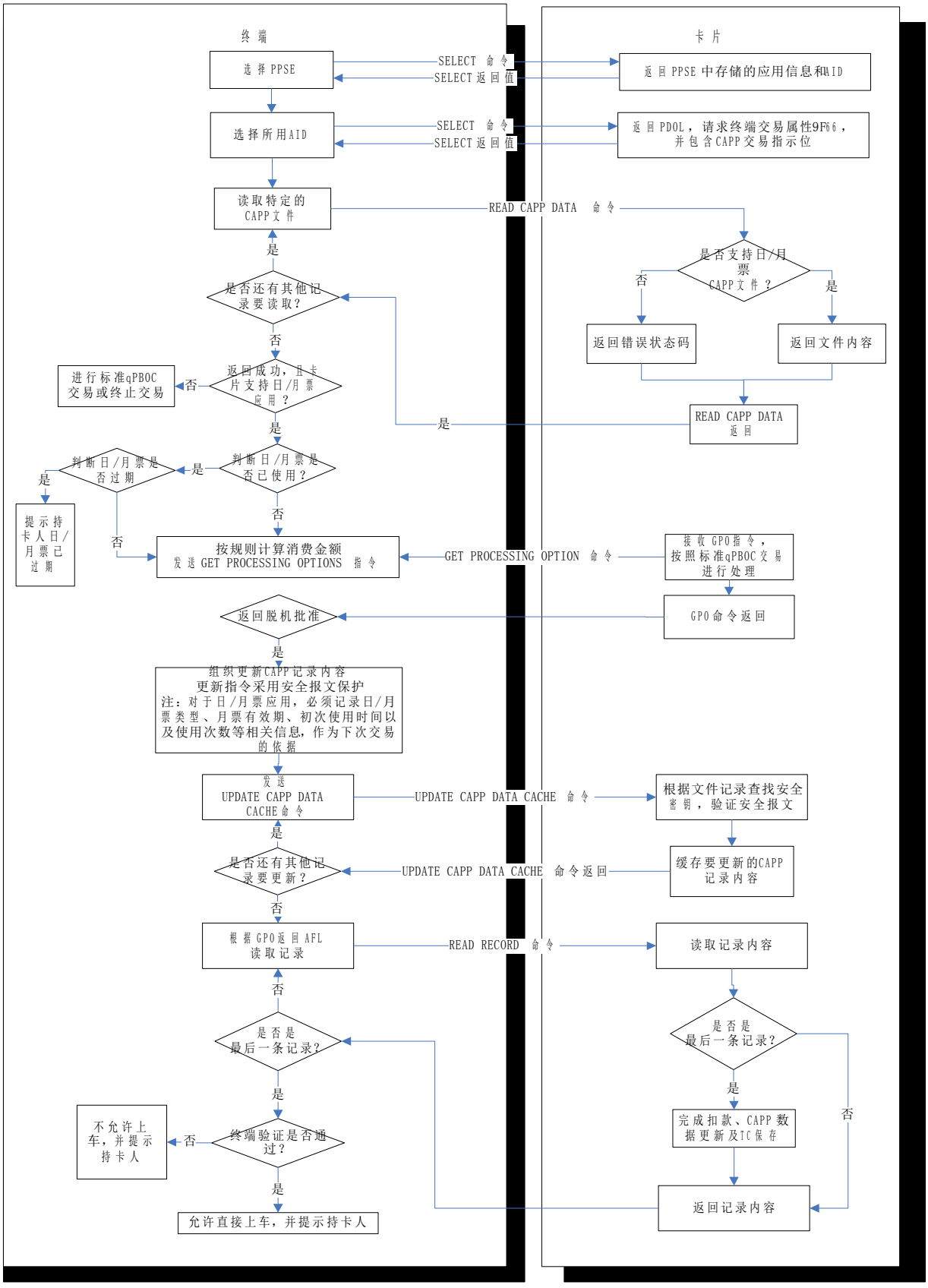


图 E.3　公交日/月票消费交易流程图

——流程说明

持卡人使用非接触式金融IC卡在日/月票应用环境中进行公交日/月票交易时，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 RECORD命令查询行业文件，判断卡片是否支持公交日/月票应用。如支持，终端应读取公交日/月票专用数据，并根据数据进行处理：首先判断公交日/月票是否已使用：若未使用，则根据规则，计算消费金额并进行日/月票消费交易；若已经使用，则根据初次使用的时间和（/或）使用的次数判断日/月票是否过期，如果过期则交易停止，并提示持卡人日/月票过期，如果未过期则根据规则，计算消费金额并进行日/月票消费交易。

3） 对于日/月票应用，扩展应用专用文件中必须记录日/月票的类型，日/月票的有效期，初次使用的时间以及使用的次数等相关信息，作为下次交易的依据。

4） 如果日/月票限定必须在某日/月使用，则可以在充值/发卡时，对CAPP文件进行更新。

附 录 F
（资料性附录）
行业应用开通指南

行业应用开通主密钥一般由发卡行管理，且各个行业应用由独立的行业应用开通主密钥控制，以确保各个行业的独立性。IC 卡应用开通密钥的分散方法见 JR/T0025.7 或 JR/T0025.17 中关于子密钥分散的描述部分，由行业应用开通主密钥通过金融应用 PAN 号、PAN 序列号进行分散得到。

行业应用管理和开通的流程如下：

1） 发卡行在其 IC 卡密钥管理系统中产生行业应用开通主密钥。

2） 发卡行在进行 IC 卡数据准备时，由行业应用开通主密钥通过金融应用 PAN 号、PAN 序列号进行分散，得到 IC 卡行业应用开通密钥。

3） 发卡行在个人化时，预先创建扩展应用文件，预置相应的 IC 卡行业应用开通密钥。

4） 持卡人在指定的终端上，在行业应用开通密钥的保护下，通过 APPEND RECORD 命令新增行业应用记录，开通行业应用。

开通行业应用可以通过如下途径：

——终端机具认证方式开通行业应用：终端上存放有行业应用开通主密钥，通过 PAN 号、PAN 序列号进行分散，获得 IC 卡行业应用开通密钥。终端在 IC 卡行业应用开通密钥的控制下，创建行业应用记录（行业应用管理密钥由发卡行、行业协商产生，通过 IC 卡行业应用开通密钥加密后写入 IC 卡）。

——发卡行后台认证方式开通行业应用：终端上不存放行业应用开通主密钥，行业应用开通主密钥存放在发卡行后台，由卡片与发卡行后台进行联机交互认证，其开通行业应用流程同终端机具认证方式。该方式适合通过远程进行行业应用开通。