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 0025.9—2010
代替JR/T 0025.9—2005

中国金融集成电路（IC）卡规范
第9部分：电子钱包扩展应用指南

China financial integrated circuit card specifications—
Part 9: Electronic purse extended application guide

2010-04-30 发布　　2010-04-30 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13个部分：

——第1部分：电子钱包/电子存折应用卡片规范；

——第2部分：电子钱包/电子存折应用规范；

——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；

——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。

本部分为JR/T 0025的第9部分。

本部分为金融电子钱包应用提供指导，是第2部分的补充和扩展。

本部分代替JR/T 0025.9—2005《中国金融集成电路（IC）卡规范　第9部分：电子钱包扩展应用指南》。

本部分与JR/T 0025.9—2005相比主要变化如下：

——重新起草标准的前言；

——将“规范性引用文件”、“术语和定义”、“符号和缩略语”在正文中的出现情况做了核对，对于没有出现的直接予以删除，对于出现的进行了修改和完善；

——删除了本部分中圈提的相关内容；

——将电子钱包消费的交易明细中出现的“卡片交易序号”勘误为“电子钱包脱机交易序号”（见7.3），并对规范中多处出现的“电子钱包交易序号”进行了明确，指出是“电子钱包脱机交易序号”还是“电子钱包联机交易序号”；

——与JR/T 0025.2保持一致，将加密生成MAC1的数据顺序进行了调整（见7.4.3）；

——将标准中表述不规范和错误之处进行了明确及勘误，并参照JR/T 0025的其他部分进行统一。

本部分的附录B、附录C、附录F是规范性附录，附录A、附录D、附录E是资料性附录。

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、中国农业银行、中国银行、中国建设银行、交通银行、招商银行、上海浦东发展银行、中国银联股份有限公司、中国金融电子化公司、中国印钞造币总公司、银行卡检测中心、国家电子计算机质量监督检验中心。

本部分主要起草人：姜云兵、杜宁、徐晋耀、李春欢、刘志刚、张永峰、张艳、聂舒、韩小西、张栋、回春野、吴蕃、史大鹏、边红丽、黄贵玲、李曙光、刘启滨、赵雷、詹旭波、徐文伟、黄发国、贾树辉、马小琼、赵宏鑫、林铁行、袁红斌、周兆确、向前、苏国经、周继军、赵亚东。

本部分于2005年3月首次发布，2010年4月第一次修订。

引　　言

JR/T 0025 的本部分定义的内容是 JR/T 0025.2 的补充和扩展，与 JR/T 0025.2 相同的内容在本部分中直接引用，不再重复描述。

电子钱包扩展应用指南和借记/贷记应用个人化指南是JR/T 0025的配套指南，旨在为发卡机构建设金融IC卡项目时提供指导和建议。今后视金融IC卡发展情况，出台更多的配套指南。

中国金融集成电路（IC）卡规范
第9部分：电子钱包扩展应用指南

1 范围

JR/T 0025的本部分主要包括以下内容：

——电子钱包复合应用：定义了用于电子钱包复合应用的数据元、文件、命令、交易流程及安全机制等内容；

——电子钱包灰锁应用：定义了用于电子钱包灰锁应用的数据元、文件、命令、交易流程及安全机制等内容。

本部分适用于由银行发行或受理的电子钱包IC卡，其使用对象主要是与金融电子钱包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），也可供其它行业参考。

2 规范性引用文件

下列文件中的条款通过JR/T 0025的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

JR/T 0025.2 中国金融集成电路（IC）卡规范 第2部分：电子钱包/电子存折应用规范

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

ISO/IEC 7816-4 识别卡 带触点的集成电路卡 第4部分：行业间交换用命令

3 术语和定义

下列术语和定义适用于JR/T 0025的本部分。

3.1

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）。

3.2

命令 command

终端向IC卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.3

响应 response

IC卡处理完成收到的命令报文后，回送给终端的报文。

3.4

金融交易 financial transaction

由于持卡者和商户之间的商品或服务交换行为而在持卡者、发卡机构、商户和收单行之间产生的信息交换、资金清算和结算行为。

3.5

报文 message

由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

3.6

报文鉴别码 message authentication code

对交易数据及其相关参数进行运算后产生的代码，主要用于验证报文的完整性。

3.7

明文 plaintext

未被加密的信息。

3.8

密钥 key

控制加密转换操作的符号序列。

3.9

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。

3.10

电子钱包 electronic purse

一种为方便持卡人小额消费而设计的金融IC卡应用。它支持圈存、消费等交易。消费不支持个人识别码（PIN）保护。

3.11

圈存 load

持卡人将其在银行相应账户上的资金划转到电子钱包中。

3.12

复合应用 complex application

结合电子钱包应用和其它应用的应用模式。

3.13

解扣出错计数器 GMAC count

用于防止外界对IC卡进行恶意试探，在执行解扣指令时，IC卡都会先对命令报文中的GMAC进行验证，如果正确则进行下一步的正常操作，并将出错计数器复位；连续出错3次时，IC卡自动将当前应用锁定。

3.14

灰锁交易验证码 grey-lock transaction authorization code

IC卡对电子钱包应用完成灰锁操作后，产生的一个安全验证码。

3.15

交易验证码待读标志 TAC unread flag

基于冗错考虑，当IC卡内部解扣操作已完成，而终端未读到TAC码时，交易中断，需要通过交易验证码待读标志的机制，通知下一个操作终端将这个未读TAC码取出，形成补充交易数据包上送主机。

3.16

终端随机数 terminal random

终端通过PSAM产生的随机数。

4 符号和缩略语

AID	应用标识符（Application IDentifier）
CAPP	复合应用（Complex APPlication）
CLA	命令报文的类别字节（CLAss byte of the command message）

GTAC	灰锁交易验证码（Grey-lock Transaction Authorization Code）
INS	命令报文的指令字节（INStruction byte of command message）
ISO	国际标准化组织（International Organization for Standardization）
Lc	终端发出的命令数据的实际长度（Exact Length of command data sent）
Le	响应数据中的最大期望长度（Maximum Length of data expected）
MAC	报文鉴别码（Message Authentication Code）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
PIN	个人识别码（Personal Identification Number）
PSAM	销售点终端安全存取模块（Purchase Secure Access Module）
RFU	预留（Reserved for Future Use）
SFI	短文件标识符（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）
TACUF	交易验证码待读标志（TAC Unread Flag）
TRAN	终端随机数（Terminal RANdom）

5 文件和命令

JR/T 0025的本部分继承JR/T 0025.2中有关电子钱包应用的所有定义，并增加定义了两种电子钱包应用模式：复合应用模式和灰锁应用模式。

复合应用模式支持的主要功能有复合应用（CAPP）消费、复合应用增加和复合应用删除。

灰锁应用模式支持的主要功能有灰锁应用消费、联机灰锁解扣、补扣交易和补充交易。

关于复合应用的说明见附录D。

5.1 文件

5.1.1 文件结构

见 JR/T 0025.2 的 5.1.1 条。

5.1.2 专用文件

见 JR/T 0025.2 的 5.1.2 条。

5.1.3 基本数据文件

见 JR/T 0025.2 的 5.1.3 条。

复合应用增加以下专用 EF 文件：复合应用专用文件。

5.1.4 复合应用专用文件

将采用变长记录文件，记录格式采用简单 TLV，格式新增文件的定义见附录 C。

5.1.5 文件选择

见 JR/T 0025.2 的 5.1.4 条。

5.2 命令

5.2.1 概述

见JR/T 0025.2的5.2条。

卡片具有的状态如下：

——空闲状态；

——圈存状态；

——消费/取现状态；

——复合应用消费状态 1；

——复合应用消费状态 2；
——灰锁空闲状态；
——预灰锁状态；
——联机解扣状态。
当应用选择完成后：
——如果应用为灰锁，应用进入空闲状态；
——如果应用已灰锁，应用进入灰锁空闲状态。
支持命令如下：
——CHANGE PIN（修改个人识别码）；
——CREDIT FOR LOAD（圈存）；
——DEBIT FOR PURCHASE/CASH WITHDRAW（消费/取现）；
——GET BALANCE（读余额）；
——GET TRANSACTION PROVE（取交易认证）；
——INITIALIZE FOR LOAD（圈存初始化）；
——INITIALIZE FOR PURCHASE（消费初始化）；
——RELOAD PIN（重装个人识别码）。
复合应用模式专用指令：
——INITIALIZE FOR CAPP PURCHASE（复合应用消费初始化）；
——UPDATE CAPP DATA CACHE（更新复合应用数据缓存）；
——DEBIT FOR CAPP PURCHASE（复合应用消费）。
灰锁应用模式专用指令：
——DEBIT FOR UNLOCK（解扣）；
——GET LOCK PROOF（取灰锁状态）；
——GREY LOCK（灰锁）；
——GREY UNLOCK（联机解扣）；
——INITIALIZE FOR GREY LOCK（灰锁初始化）；
——INITIALIZE FOR GREY UNLOCK（联机解扣初始化）。

表1　命令执行成功后的状态变化

状态 / 命令	空闲	圈存	消费/取现	修改	CAPP1	CAPP2	灰锁空闲	预灰锁	联机解扣
CREDIT FOR LOAD	N/A	空闲	N/A	N/A	N/A	N/A	N/A	N/A	N/A
DEBIT FOR PURCHASE/CASH WITHDRAW	N/A	N/A	空闲	N/A	N/A	N/A	N/A	N/A	N/A
DEBIT FOR CAPP PURCHASE	N/A	N/A	N/A	N/A	N/A	空闲	N/A	N/A	N/A
GET BALANCE	空闲	圈存	消费/取现	修改	CAPP1	CAPP2	灰锁空闲	预灰锁	联机解扣
GET LOCK PROOF	空闲	圈存	消费/取现	修改	CAPP1	CAPP2	灰锁空闲	预灰锁	联机解扣
GET TRANSACTION PROVE	空闲	圈存	消费/取现	修改	CAPP1	CAPP2	灰锁空闲	预灰锁	联机解扣

GREY LOCK	N/A	N/A	N/A	N/A	N/A	N/A	N/A	灰锁空闲	N/A
GREY UNLOCK	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	空闲
INITIALIZE FOR LOAD	圈存	圈存	圈存	圈存	N/A	N/A	N/A	圈存	N/A
INITIALIZE FOR GREY LOCK	预灰锁	预灰锁	预灰锁	预灰锁	N/A	N/A	N/A	预灰锁	N/A
INITIALIZE FOR GREY UNLOCK	N/A	N/A	N/A	N/A	N/A	N/A	联机解扣	N/A	联机解扣
INITIALIZE FOR PURCHASE	消费/取现	消费/取现	消费/取现	消费/取现	N/A	N/A	消费/取现	N/A	消费/取现
INITIALIZE FOR CAPP PURCHASE	CAPP1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
INITIALIZE FOR WITHDRAW	消费/取现	消费/取现	消费/取现	消费/取现	N/A	N/A	N/A	N/A	N/A
INITIALIZE FOR UPDATE	修改	修改	修改	修改	N/A	N/A	N/A	修改	N/A
UPDATE CAPP DATA CACHE	N/A	N/A	N/A	N/A	CAPP2	CAPP2	N/A	N/A	N/A
UPDATE OVERDRAW LIMIT	N/A	N/A	N/A	空闲	N/A	N/A	N/A	N/A	N/A

表2　命令的类别字节和指令字节

命　　令	CLA	INS	P1	P2
CHANGE PIN（修改个人识别码）	‘80’	‘5E’	‘01’	‘00’
CREDIT FOR LOAD（圈存）	‘80’	‘52’	‘00’	‘00’
DEBIT FOR PURCHASE/CASH WITHDRAW（消费/取现）	‘80’	‘54’	‘01’	‘00’
DEBIT FOR CAPP PURCHASE	‘80’	‘54’	‘01’	‘00’
GET BALANCE（读余额）	‘80’	‘5C’	‘00’	‘0X’
GET TRANSACTION PROVE（取交易认证）	‘80’	‘5A’	‘00’	‘XX’
INITIALIZE FOR CASH WITHDRAW（取现初始化）	‘80’	‘50’	‘02’	‘01’
INITIALIZE FOR LOAD（圈存初始化）	‘80’	‘50’	‘00’	‘0X’
INITIALIZE FOR PURCHASE（消费初始化）	‘80’	‘50’	‘01’	‘0X’
INITIALIZE FOR CAPP PURCHASE	‘80’	‘50’	‘03’	‘02’
INITIALIZE FOR UPDATE（修改初始化）	‘80’	‘50’	‘04’	‘01’
RELOAD PIN（重装个人识别码）	‘80’	‘5E’	‘00’	‘00’
UPDATE CAPP DATA CACHE（更新复合应用数据缓存）	‘80’	‘DC’	‘XX’	‘XX’
UPDATE OVERDRAW LIMIT（修改透支限额）	‘80’	‘58’	‘00’	‘00’
DEBIT FOR UNLOCK（解扣）	‘E0’	‘7E’	‘08’	‘01’
GET LOCK PROOF（取灰锁状态）	‘E0’	‘CA’	‘0X’	‘00’
GREY LOCK（灰锁）	‘E0’	‘7C’	‘08’	‘00’
GREY UNLOCK（联机解扣）	‘E0’	‘7E’	‘09’	‘00’
INITIALIZE FOR GREY LOCK（灰锁初始化）	‘E0’	‘7A’	‘08’	‘01’
INITIALIZE FOR GREY UNLOCK（联机解扣初始化）	‘E0’	‘7A’	‘09’	‘01’

5.2.2 CHANGE PIN 命令

见JR/T 0025.2的5.2.1条。

5.2.3 CREDIT FOR LOAD 命令

见JR/T 0025.2的5.2.2条。

5.2.4 DEBIT FOR PURCHASE/CASH WITHDRAW 命令

见JR/T 0025.2的5.2.3条。

5.2.5 DEBIT FOR UNLOAD 命令

见JR/T 0025.2的5.2.4条。

5.2.6 GET BALANCE 命令

见JR/T 0025.2的5.2.5条。

5.2.7 GET TRANSACTION PROVE 命令

见JR/T 0025.2的5.2.6条。

5.2.8 INITIALIZE FOR LOAD 命令

见JR/T 0025.2的5.2.8条。

响应报文的状态字增加：

SW1	SW2	说明
‘94’	‘08’	应用灰锁锁定

5.2.9 INITIALIZE FOR PURCHASE 命令

见JR/T 0025.2的5.2.9条。

响应报文的状态字增加：

SW1	SW2	说明
‘94’	‘08’	应用灰锁锁定

5.2.10 INITIALIZE FOR UNLOAD 命令

见JR/T 0025.2的5.2.10条。

响应报文的状态字增加：

SW1	SW2	说明
‘94’	‘08’	应用灰锁锁定

5.2.11 RELOAD PIN 命令

见JR/T 0025.2的5.2.12条。

5.2.12 INITIALIZE FOR CAPP PURCHASE 命令

5.2.12.1 定义和范围

INITIALIZE FOR CAPP PURCHASE命令用于初始化复合应用消费交易。

5.2.12.2 命令报文

INITIALIZE FOR CAPP PURCHASE命令报文见表3。

表3 INITIALIZE FOR CAPP PURCHASE 命令报文格式

代码	值
CLA	‘80’
INS	‘50’
P1	‘03’
P2	‘02’
Lc	‘0B’
Data	见 5.2.12.3
Le	‘0F’

5.2.12.3 命令报文数据域

此命令报文的数据域定义见表4。

表4 INITIALIZE FOR CAPP PURCHASE 命令报文的数据域定义

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

5.2.12.4 响应报文数据域

此命令执行成功的响应报文数据域见表5。

表5 INITIALIZE FOR CAPP PURCHASE 命令执行成功的响应报文数据域

说明	长度（字节）
电子钱包余额	4
电子钱包交易序号	2
透支限额	3
密钥算法版本号（DPK）	1
密钥标识（DPK）	1
伪随机数（IC 卡）	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

5.2.12.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表6。

表6 INITIALIZE FOR CAPP PURCHASE 命令可能回送的错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持
‘94’	‘02’	交易计数器达到最大值
‘94’	‘08’	应用灰锁锁定

5.2.13 UPDATE CAPP DATA CACHE 命令

5.2.13.1 定义和范围

UPDATE CAPP DATA CACHE命令用于复合应用消费交易中更新复合应用数据缓存，缓存数据将被DEBIT FOR CAPP PURCHASE命令用于改写复合应用专用文件中相关记录。

5.2.13.2 命令报文

此命令报文见表7。

表7 UPDATE CAPP DATA CACHE 命令报文

代码	值
CLA	‘80’
INS	‘DC’
P1	复合应用类型标识符
P2	见表 8
Lc	后续数据域的长度

Data	见 5.2.13.3
Le	不存在

此命令报文中的引用控制参数P2定义见表8。

表8 UPDATE CAPP DATA CACHE 命令报文中的引用控制参数 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	第一个标识符出现的记录
—	—	—	—	—	x	x	x	RFU
其它值								RFU

5.2.13.3 命令报文数据域

此命令报文数据域由更新原有记录的新记录组成。

5.2.13.4 响应报文数据域

响应报文数据域不存在。

5.2.13.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态字见表10。

表9 UPDATE CAPP DATA CACHE 可能回送的错误状态字

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’	‘82’	不满足安全状态
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF）
‘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’	复合应用禁止

5.2.14 DEBIT FOR CAPP PURCHASE 命令

5.2.14.1 定义和范围

DEBIT FOR CAPP PURCHASE命令用于复合应用消费交易。

5.2.14.2 命令报文

此命令报文见表 10。

表10 DEBIT FOR CAPP PURCHASE 命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
Lc	‘0F’

Data	见 5.2.14.3
Le	‘08’

5.2.14.3 命令报文数据域

此命令报文的数据域定义见表11。

表11 DEBIT FOR CAPP PURCHASE 命令报文的数据域定义

说明	长度（字节）
终端交易序号	4
交易日期	4
交易时间	3
MAC1	4

5.2.14.4 响应报文数据域

此命令执行成功的响应报文数据域见表12。

表12 DEBIT FOR CAPP PURCHASE 命令执行成功的响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

5.2.14.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表13。

表13 DEBIT FOR CAPP PURCHASE 可能回送的错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘93’	‘01’	金额不足
‘93’	‘02’	MAC 无效

5.2.15 DEBIT FOR UNLOCK 命令

5.2.15.1 定义和范围

DEBIT FOR UNLOCK命令用于对电子钱包进行解扣操作。

5.2.15.2 命令报文

DEBIT FOR UNLOCK命令报文见表14。

表14 DEBIT FOR UNLOCK 命令报文

代码	值
CLA	‘E0’
INS	‘7E’
P1	‘08’
P2	‘01’
Lc	‘1B’
Data	见 5.2.15.3
Le	‘04’

5.2.15.3 命令报文数据域

此命令报文的数据域定义见表15。

表15 DEBIT FOR UNLOCK 命令报文的数据域定义

说明	长度（字节）
交易金额	4
交易序号	2
终端机编号	6
终端交易序号	4
交易日期（终端）	4
交易时间（终端）	3
GMAC	4

5.2.15.4 响应报文数据域

此命令执行成功的响应报文数据域见16表。

表16 DEBIT FOR UNLOCK 命令执行成功的响应报文数据域

说明	长度（字节）
TAC	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

5.2.15.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表17。

表17 DEBIT FOR UNLOCK 可能回送的错误状态

SW1	SW2	说明
‘64’	‘00’	状态标志位未改变
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘93’	‘01’	金额不足
‘93’	‘02’	MAC 无效
‘94’	‘06’	所需 MAC 和 TAC 不可用

5.2.16 GET LOCK PROOF 命令

5.2.16.1 定义和范围

GET LOCK PROOF命令用于读取电子钱包应用的灰锁状态以及相关的证明码。

5.2.16.2 命令报文

GET LOCK PROOF命令报文见表18。

表18 GET LOCK PROOF 命令报文

代码	值
CLA	‘E0’
INS	‘CA’
P1	‘00’：普通读取 ‘01’：清除 TACUF（交易验证码待读标志）
P2	‘00’

Lc	不存在
Data	不存在
Le	‘1E’或不存在

5.2.16.3 命令报文数据域

此命令报文的数据域不存在。

5.2.16.4 响应报文数据域

此命令执行成果，根据P1的参数、电子钱包应用的灰锁状态和TACUF，形成不同的响应报文数据域，其关系见表19。

表19 参数、状态与 GET LOCK PROOF 响应报文数据域的关系

P1 参数	TACUF	灰锁状态	响应报文数据域	
			数据域列表	报文中的状态字
‘00’	标志复位	无灰锁	表 20	‘00’
		有灰锁	表 21	‘01’
	标志置位	不影响	表 22	‘10’
‘01’	将 TACUF 标志复位	不影响	不存在	

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表20 正常状态 GET LOCK PROOF 命令执行成功的响应报文数据域

说明	长度（字节）
状态字（＝‘00’表示当前应用无灰锁）	1
上次发生的解扣、联机解扣的交易类型标识	1
上次解扣、联机解扣的电子钱包（‘01’）	1
上次解扣、联机解扣的电子钱包余额	4
上次解扣、联机解扣的电子钱包的交易序号	2
上次解扣、联机解扣的终端机编号	6
上次解扣、联机解扣的日期	4
上次解扣、联机解扣的时间	3
上次解扣、联机解扣的交易金额	4
上次解扣的 TAC 或联机解扣的 MAC3	4

表21 灰锁状态 GET LOCK PROOF 命令执行成功的响应报文数据域

说明	长度（字节）
状态字（＝‘01’表示当前应用已灰锁）	1
灰锁的交易类型标识	1
被灰锁的电子钱包（‘01’）	1
被灰锁的电子钱包余额	4
被灰锁的电子钱包交易序号	2
执行 GREY LOCK 时的终端机编号	6
执行 GREY LOCK 时的日期	4
执行 GREY LOCK 时的时间	3
灰锁时的 MAC2	4
灰锁时的 GTAC	4

表22 TAC 未读时 GET LOCK PROOF 命令执行成功的响应报文数据域

说明	长度（字节）

状态字（＝‘10’表示当前应用 TAC 未读）	1
上次解扣的交易类型标识	1
上次解扣的电子钱包（‘01’）	1
上次解扣的电子钱包余额	4
上次解扣的电子钱包交易序号	2
上次执行解扣的终端机编号	6
上次执行解扣的日期	4
上次执行解扣的时间	3
解扣交易金额	4
上次解扣的 TAC	4

5.2.16.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表23。

表23 GET LOCK PROOF 可能回送的错误状态

SW1	SW2	说明
‘64’	‘00’	状态标志位未改变
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1、P2 参数不正确

5.2.17 GREY LOCK 命令

5.2.17.1 定义和范围

GREY LOCK命令用于灰锁电子钱包。

5.2.17.2 命令报文

GREY LOCK命令报文见24表。

表24 GREY LOCK 命令报文

代码	值
CLA	‘E0’
INS	‘7C’
P1	‘08’
P2	‘00’
Lc	‘13’
Data	见 5.2.17.3
Le	‘08’

5.2.17.3 命令报文数据域

此命令报文的数据域定义见表25。

表25 GREY LOCK 命令报文的数据域定义

说明	长度（字节）
终端交易序号	4
终端随机数	4
交易日期（终端）	4
交易时间（终端）	3
MAC1	4

5.2.17.4 响应报文数据域

此命令执行成功的响应报文数据域见表26。

表26 GREY LOCK 命令执行成功的响应报文数据域

说明	长度（字节）
GTAC	4
MAC2	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

5.2.17.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表27。

表27 GREY LOCK 可能回送的错误状态

SW1	SW2	说明
‘64’	‘00’	状态标志位未改变
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘93’	‘02’	MAC 无效

5.2.18 GREY UNLOCK 命令

5.2.18.1 定义和范围

GREY UNLOCK命令用于联机解扣交易。

5.2.18.2 命令报文

GREY UNLOCK命令报文见表28。

表28 GREY UNLOCK 命令报文

代码	值
CLA	‘E0’
INS	‘7E’
P1	‘09’
P2	‘00’
Lc	‘0F’
Data	见 5.2.18.3
Le	‘04’

5.2.18.3 命令报文数据域

此命令报文的数据域定义见表29。

表29 GREY UNLOCK 命令报文的数据域定义

说明	长度（字节）
交易金额	4
交易日期（主机）	4
交易时间（主机）	3
MAC2	4

5.2.18.4 响应报文数据域

此命令执行成功的响应报文数据域见表30。

表30 GREY UNLOCK 命令执行成功的响应报文数据域

说明	长度（字节）
MAC3	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

5.2.18.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表31。

表31 GREY LOCK 可能回送的错误状态

SW1	SW2	说明
‘64’	‘00’	状态标志位未改变
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘93’	‘02’	MAC 无效
‘94’	‘01’	金额不足

5.2.19 INITIALIZE FOR GREY LOCK 命令

5.2.19.1 定义和范围

INITIALIZE FOR GREY LOCK命令用于初始化灰锁操作。

5.2.19.2 命令报文

INITIALIZE FOR GREY LOCK命令报文见表32。

表32 INITIALIZE FOR GREY LOCK 命令报文

代码	值
CLA	‘E0’
INS	‘7A’
P1	‘08’
P2	‘01’
Lc	‘07’
Data	见 5.2.19.3
Le	‘0F’

5.2.19.3 命令报文数据域

此命令报文的数据域定义见表33。

表33 INITIALIZE FOR GREY LOCK 命令报文的数据域定义

说明	长度（字节）
密钥索引号	1
终端机编号	6

5.2.19.4 响应报文数据域

此命令执行成功的响应报文数据域见表34。

表34 INITIALIZE FOR GREY LOCK 命令执行成功的响应报文数据域

说明	长度（字节）
电子钱包余额	4
电子钱包交易序号	2

透支限额	3（全0）
密钥版本号	1
算法标识	1
伪随机数	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

5.2.19.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表35。

表35 INITIALIZE FOR GREY LOCK 可能回送的错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘94’	‘03’	密钥索引号不支持

5.2.20 INITIALIZE FOR GREY UNLOCK 命令

5.2.20.1 定义和范围

INITIALIZE FOR GREY UNLOCK命令用于初始化联机解扣交易。

5.2.20.2 命令报文

INITIALIZE FOR GREY UNLOCK命令报文见表36。

表36 INITIALIZE FOR GREY UNLOCK 命令报文

代码	值
CLA	‘E0’
INS	‘7A’
P1	‘09’
P2	‘01’
Lc	‘07’
Data	见5.2.20.3
Le	‘12’

5.2.20.3 命令报文数据域

此命令报文的数据域定义见表37。

表37 INITIALIZE FOR GREY UNLOCK 命令报文的数据域定义

说明	长度（字节）
密钥索引号	1
终端机编号	6

5.2.20.4 响应报文数据域

此命令执行成功的响应报文数据域见表38。

表38 INITIALIZE FOR GREY UNLOCK 命令执行成功的响应报文数据域

说明	长度（字节）
电子钱包余额	4
电子钱包脱机交易序号	2
电子钱包联机交易序号	2
密钥版本号	1

密钥算法	1
伪随机数	4
MAC1	4

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

5.2.20.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态见表39。

表39 INITIALIZE FOR GREY LOCK 可能回送的错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1、P2 参数不正确
‘94’	‘03’	密钥索引号不支持

6 安全

见JR/T 0025.2的5.3条。

补充定义如下：

——复合应用专用文件受应用维护密钥保护，在非交易情况下，需经过应用维护密钥验证或使用应用维护密钥生成 MAC 的安全报文，对文件进行维护；

——复合应用消费受消费/取现密钥保护。

7 交易流程

本章描述电子钱包应用的交易流程，是卡片被终端激活并选择而与终端相互作用后，所进行的交易处理过程。

消费交易要求终端必须具备交易安全存取模块（PSAM）。JR/T 0025假定终端与PSAM之间是以安全方式进行通信的，因此不定义如何与PSAM通信相关的命令－响应对。

7.1 交易预处理

7.1.1 标准的交易预处理（步骤 1.1）

见JR/T 0025.2的5.5.1条。

补充定义如下：

——“选择 IC 卡”部分：对于非接触式 IC 卡，终端应具有检测 IC 卡是否进入射频有效场强范围内的能力。一旦终端检测到有效 IC 卡进入，终端应具备分辨多张有效 IC 卡进入的情况，并依次逐卡自动选择或人工选择一张特定 IC 卡。当卡片选定后，终端将继续专项应用选择功能。终端应根据支持的应用自动选择卡片上的应用；

——“提示输入个人识别码（PIN）”和“校验 PIN”部分：JR/T 0025 定义的应用中的消费交易、复合应用消费交易、灰锁消费交易的交易预处理无需此部分；

——“交易类型选择”部分：对电子钱包应用来说，持卡人应能选择如下交易类型：圈存、 消费、查询余额、复合应用消费交易和灰锁消费交易。

以下补充交易预处理步骤为可选项。

7.1.2 发出 GET LOCK PROOF（P1＝‘00’）命令（步骤 1.2）

终端发出GET LOCK PROOF（P1＝‘00’）命令对电子钱包的状态进行查询。

7.1.3 判断 TACUF（交易验证码待读标志）（步骤 1.3）

IC卡收到GET LOCK PROOF（P1＝‘00’）命令后，首先根据TACUF判断上次的解扣交易的TAC码是否未被终端正确读取。如果TACUF为1，即上次的解扣交易的TAC码有待读取，则进入7.1.4条所描述的步骤。否则，进入7.1.5条所描述的步骤进行灰锁标志的判断。

如果应用未发生过灰锁、解扣、联机解扣交易，则IC卡返回‘6985’出错信息给终端，但不回送其他数据，同时结束交易预处理流程。

7.1.4 返回 TAC 码（步骤 1.4）

IC卡将上次的解扣交易的产生的未成功读取的TAC码返回给终端，以供终端形成补充交易数据包，进入7.1.9条所描述的步骤。详细的响应报文见5.2.16条中的表22。

7.1.5 判断灰锁标志（步骤 1.5）

IC卡对所选择的电子钱包应用进行灰锁判断，如果当前应用中的电子钱包应用无灰锁，则进入7.1.6条所描述的步骤，返回正常信息给终端。否则进入7.1.7条所描述的步骤，返回灰锁信息给终端。

7.1.6 返回正常信息（步骤 1.6）

IC卡将正常信息返回给终端，详细的响应报文见5.2.16条中的表20。交易预处理流程完成。

7.1.7 返回灰锁信息（步骤 1.7）

IC卡将上次的灰锁交易的产生日期、时间、MAC2、GTAC等返回给终端，详细的响应报文见5.2.16条中的表21。终端进入7.1.8条启动补扣交易流程。

7.1.8 进行补扣交易（步骤 1.8）

补扣交易的详细描述见7.9，完成后交易预处理流程结束。

7.1.9 进行补充交易（步骤 1.9）

补充交易的详细描述见7.10，完成后交易预处理流程结束。

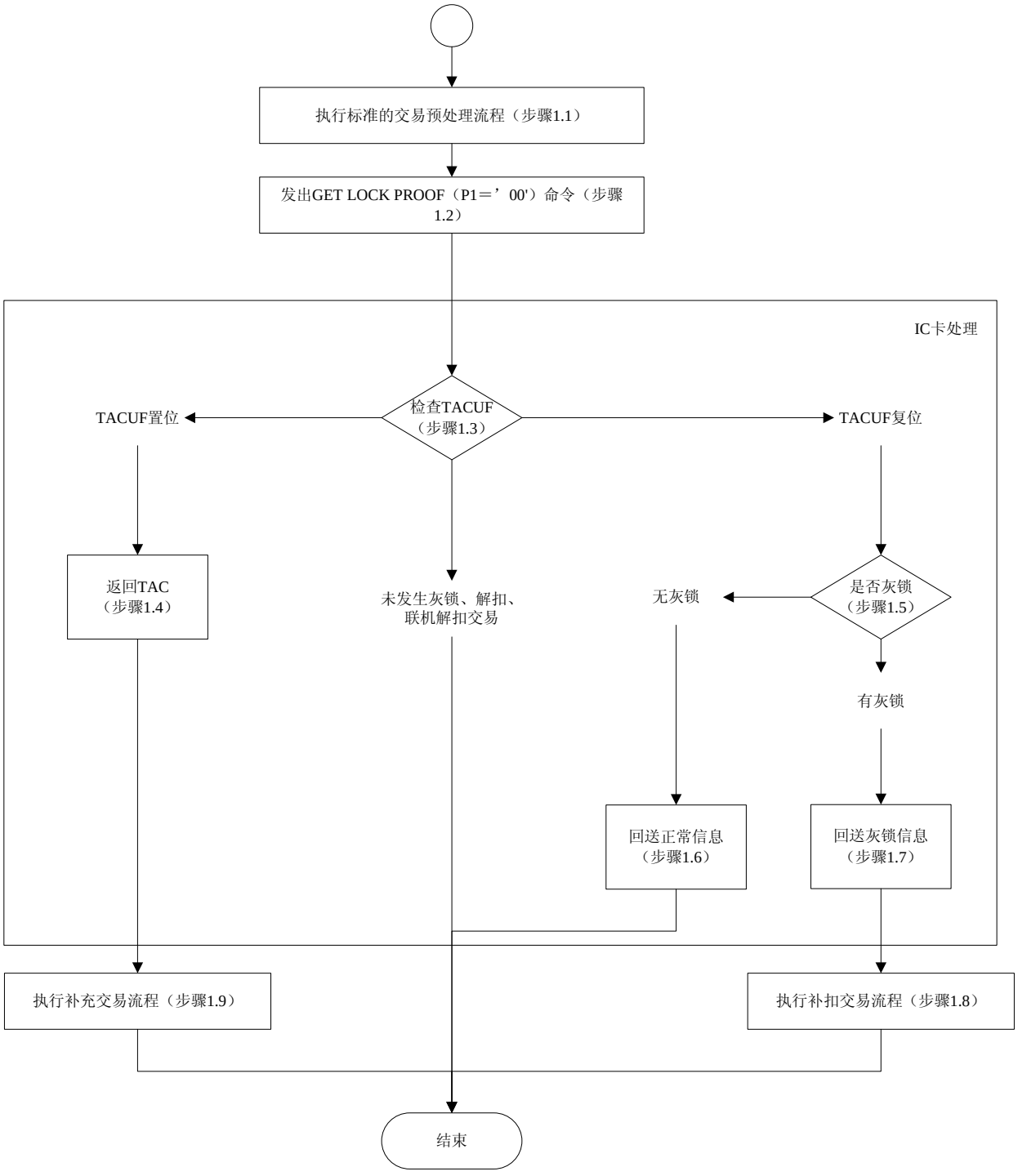

图1　加入灰锁机制的交易预处理流程

7.2　圈存交易

见JR/T 0025.2的5.5.2条。

补充定义如下：

——“交易处理”部分，交易明细定义为：

- 电子钱包联机交易序号；
- 交易金额；
- 交易类型标识；
- 终端机编号；

- 交易日期；
- 交易时间。

——“处理 INITIALIZE FOR LOAD”部分，增加一检查过程：检查钱包是否被灰锁。如果灰锁，则回送状态字‘9408’（钱包灰锁锁定），但不回送其它信息，同时终止命令的处理过程。

7.3 消费交易

见JR/T 0025.2的5.5.4条。

补充定义如下：

——“交易处理”：IC 卡从电子钱包余额中扣减消费的金额，电子钱包脱机交易序号加 1，更新电子钱包消费交易记录。IC 卡必须成功地完成以上所有步骤或者一个也不完成。

——对于电子钱包消费交易，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‘06’；
- 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）。

——“处理 INITIALIZE FOR PURCHASE”部分增加一检查过程：检查钱包是否被灰锁。如果灰锁，则回送状态字‘9408’（钱包灰锁锁定），但不回送其它信息，同时终止命令的处理过程。

7.4 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进行购物或获取服务。此交易可以在终端设备或其它读卡设备上脱机进行。此交易无需提交个人识别码（PIN）。

复合应用消费交易允许消费金额为0。

7.4.1 发出 INITIALIZE FOR CAPP PURCHASE 命令（步骤 4.1）

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

7.4.2 处理 INITIALIZE FOR CAPP PURCHASE 命令（步骤 4.2）

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；

——检查钱包是否被灰锁，如果灰锁，则回送状态字‘9408’（钱包灰锁锁定），但不回送其它信息，同时终止命令的处理过程；

——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在 JR/T 0025 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JR/T 0025.2的附录B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。

7.4.3 产生 MAC1（步骤 4.3）

使用伪随机数（ICC）和IC卡回送的电子钱包脱机交易序号，终端的安全存取模块（PSAM）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PSAM的合法性。

MAC1的计算机制见JR/T 0025.2的附录B。用SESPK对以下数据进行加密产生MAC1（按所列顺序）：

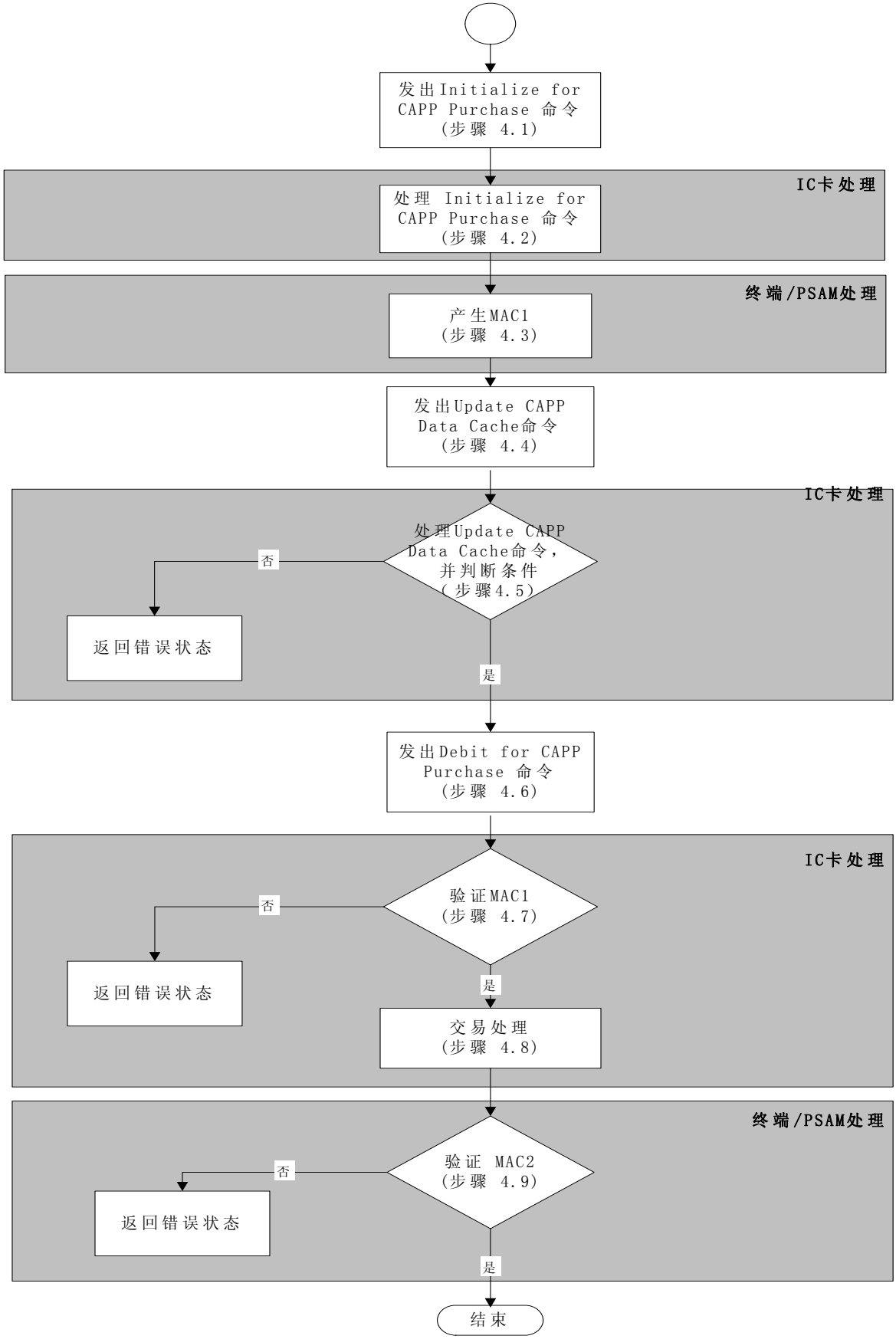

图2　复合消费交易流程

——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）。

7.4.4 发出 UPDATE CAPP DATA CACHE 命令（步骤 4.4）

终端发出UPDATE CAPP DATA CACHE命令。

7.4.5 处理 UPDATE CAPP DATA CACHE 命令（步骤 4.5）

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。

7.4.6 发出 DEBIT FOR CAPP PURCHASE 命令（步骤 4.6）

终端发出DEBIT FOR CAPP PURCHASE命令。

7.4.7 验证 MAC1（步骤 4.7）

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7.4.8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JR/T 0025范围内。

7.4.8 交易处理（步骤 4.8）

IC卡从电子钱包余额中扣减消费的金额，电子钱包脱机交易序号加1，根据7.4.5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卡必须成功地完成以上所有步骤或者一个也不完成。

在根据7.4.5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卡产生一个报文签别码 （MAC2）供PSAM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PSAM产生MAC2的输入数据。MAC2的计算机制见JR/T 0025.2的附录B。用SESPK对以下数据进行加密产生MAC2：交易金额。

IC卡按照JR/T 0025.2的附录B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，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‘09’；

——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）。

7.4.9 验证 MAC2 （步骤 4.9）

在收到IC卡（经过终端）传来的MAC2后，PSAM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JR/T 0025的范围之内。

7.5 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。此交易一般脱机进行。此交易无需提交个人识别码（PIN）。

终端利用GET BALANCE命令实现查询余额交易。

7.6 查询明细交易

持卡人可以通过终端或其他读卡设备读取卡片中的交易明细记录。此交易一般采用脱机方式处理。交易时无需提交个人识别码（PIN）。

终端发出一个READ RECORD命令来获得交易明细。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。

7.7 灰锁消费交易

灰锁消费交易允许持卡人使用电子钱包进行灰锁消费。此交易可以脱机进行。

7.7.1 发出 INITIALIZE FOR GREY LOCK 命令（步骤 7.1）

终端发出INITIALIZE FOR GREY LOCK命令启动灰锁消费交易。

7.7.2 处理 INITIALIZE FOR GREY LOCK 命令（步骤 7.2）

IC卡收到INITIALIZE FOR GREY LOCK命令后，将进行以下操作：检查命令中包含的密钥索引号是否被IC卡支持。如果不支持，返回状态字“9403”（不支持的密钥索引号）且不返回其他数据。

在通过以上检查之后，IC卡将产生一个伪随机数，这个伪随机数将包含在本命令的响应报文中返回终端。

之后，IC卡将内部的TACUF复位。

7.7.3 计算 MAC1（步骤 7.3）

使用IC卡返回的伪随机数和电子钱包脱机交易序号，终端的安全存取模块（PSAM）将产生一个终端随机数（TRAN），一个过程密钥（GSESPK）和一个报文鉴别码（MAC1），供IC卡来验证PSAM的合法性。

过程密钥GSESPK被用于电子钱包的灰锁消费交易。

过程密钥的产生分两步：

——用 DPK 密钥并按照 JR/T 0025.2 的附录 B 中的机制产生的中间密钥；

——用中间密钥采用下述的算法产生过程密钥。

用来产生中间密钥的输入数据如下：

TMPCK：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。

用中间密钥对终端随机数（TRAN）加密，运算的结果产生过程密钥：

GSESPK =DES（TMPCK，TRAN || ‘80000000’）。

MAC1的计算机制见JR/T 0025.2的附录B。

用GSESPK对以下数据进行加密产生MAC1（按所列顺序）：

——交易类型标识；

——终端机编号；

——交易日期；

——交易时间。

7.7.4 发出 GREY LOCK 命令（步骤 7.4）

终端发出GREY LOCK命令。

7.7.5 验证 MAC1（步骤 7.5）

IC卡收到GREY LOCK命令后，将产生同样的过程密钥（GSESPK）并验证MAC1是否有效。如果MAC1是有效的，交易处理将继续执行7.7.6条。如果MAC1是无效的，IC卡返回错误状态字“9302”（MAC无效）给终端。

7.7.6 灰锁处理（步骤 7.6）

IC卡将电子钱包脱机交易序号加1，并将电子钱包应用灰锁。

IC卡产生一个报文鉴别码(MAC2)供PSAM对IC卡合法性进行检查，并同时将MAC2写入内部文件。MAC2将包含在从卡传送到PSAM（通过终端）GREY LOCK的命令响应报文和GET LOCK PROOF的命令响应报文中。

MAC2的计算机制见JR/T 0025.2的附录B。用GSESPK对以下这些数据进行加密产生MAC2：

——电子钱包余额；

——电子钱包脱机交易序号（加 1 前）。

IC卡也应该用和JR/T 0025.2的附录B中相同的机制直接用密钥DTK产生一个GTAC。GTAC将包含在从卡传送到PSAM（通过终端）的GREY LOCK的命令响应报文和GET LOCK PROOF的命令响应报文中。如果之后出现交易异常中断等，使DEBIT FOR UNLOCK指令无法当时执行成功，GTAC可供终端纳入终端异常交易数据中，以便后来上传给主机进行灰锁验证。

下面是用来生成GTAC的要素：

——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）。

IC卡应把GSESPK存贮到安全的内部文件中（或者，IC卡也可以将终端随机数、伪随机数（ICC）、终端交易序号等，写入内部文件，通过计算重新获得），以备交易中途IC卡掉电后，在后续交易流程中恢复过程密钥GSESPK。

IC卡将用以下数据组成的一个记录来更新内部专用明细。这个明细记录中的数据将包含在GET LOCK PROOF的命令响应报文中，由IC卡返回给终端：

——交易类型标识（‘91’＝电子钱包灰锁）；

——电子钱包代号（‘01’＝电子钱包）；

——电子钱包余额；

——电子钱包脱机交易序号；

——终端机编号；

——交易日期；

——交易时间；

——MAC2；

——GTAC。

IC卡必须全部成功地完成以上几个步骤或者一个也不完成，如果脱机交易序号的更新、电子钱包应用灰锁状态的设置没有成功，交易明细也不应更新。

7.7.7 验证 MAC2（步骤 7.7）

在收到IC卡(经终端)传来的MAC2后，PSAM要验证MAC2的有效性。MAC2如果有效，交易继续进行7.7.8条所描述的步骤；如果MAC2是无效的，终端应停止交易并采取相应的措施。

7.7.8 持卡人进行消费行为（步骤 7.8）

持卡人进行消费行为。在进行消费过程中，允许终端对IC卡下电。若下电以后，IC卡重新上电，经过交易预处理（选择应用、验证个人识别码等）后应可以继续执行7.7.9条所描述的步骤而不受影响。

7.7.9 产生 GMAC（步骤 7.9）

安全存取模块（PSAM）根据专用消费的金额，用过程密钥（GSESPK）产生一个报文鉴别码（GMAC），供IC卡来验证PSAM的合法性。GMAC的计算机制见JR/T 0025.2的附录B。

用GSESPK对以下数据进行加密产生GMAC：交易金额。

7.7.10 发出 DEBIT FOR UNLOCK 命令（步骤 7.10）

终端发出DEBIT FOR UNLOCK命令。

7.7.11 检查脱机交易序号和余额（步骤 7.11）

收到DEBIT FOR UNLOCK命令后，1C卡将进行以下操作：

——检查脱机交易序号是否匹配，如果脱机交易序号不匹配，IC 卡将返回“9406”（脱机交易序号错），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”（金额不足），但不回送其他数据，IC 卡不操作内部出错计数器，终端应采取相应的措施。

通过上面的检查后，IC卡进入7.7.12条。

7.7.12 验证 GMAC（步骤 7.12）

IC卡验证GMAC的有效性。如果GMAC是有效的，将1C卡内部的解扣出错计数器复位，交易处理将继续执行7.7.13条。如果GMAC是无效的，IC卡返回错误状态字“9302”（MAC无效）给终端，同时操作解扣出错计数器，3次出错则临时锁住应用以防止恶意试探。该解扣出错计数器将在应用解锁命令执行成功后被复位。

7.7.13 交易处理（步骤 7.13）

1C卡从卡上的电子钱包余额中减去灰锁消费的交易金额(如果交易金额为0,则省略对余额的修改)、将电子钱包解锁、并将卡内的TACUF（交易验证码待读标志）置位。

IC卡应该用和JR/T 0025.2的附录B中描述的机制直接用密钥DTK产生一个TAC。TAC将被写入终端交易数据包，以便后来传给主机进行交易验证。

下面是用来生成TAC的要素（按所列顺序）：

——交易金额；

——交易类型标识（‘93’=电子钱包解扣）；

——终端机编号（发出 DEBIT FOR UNLOCK 命令的终端）；

——终端交易序号（发出 DEBIT FOR UNLOCK 命令的终端）；

——交易日期（发出 DEBIT FOR UNLOCK 命令的日期）；

——交易时间（发出 DEBIT FOR UNLOCK 命令的时间）。

对于电子钱包的灰锁消费交易，IC卡将用以下数据组成的一个记录更新标准交易明细：

——电子钱包脱机交易序号；

——交易金额；

——交易类型标识（‘93’=电子钱包解扣）；

——终端机编号（发出 DEBIT FOR UNLOCK 命令的终端）；

——交易日期（发出 DEBIT FOR UNLOCK 命令的日期）；

——交易时间（发出 DEBIT FOR UNLOCK 命令的时间）。

对于电子钱包的灰锁消费交易，IC卡将用以下数据组成的一个记录更新内部专用明细文件，以便以后终端可以通过GET LOCK PROOF命令得到：

——交易类型标识；

——电子钱包代号（‘01’=ET）；

——电子钱包余额；

——电子钱包脱机交易序号；

——终端机编号（发出 DEBIT FOR UNLOCK 命令的终端）；

——交易日期（发出 DEBIT FOR UNLOCK 命令的日期）；

——交易时间（发出 DEBIT FOR UNLOCK 命令的时间）；

——交易金额；

——TAC。

IC卡必须全部成功地完成以上几个步骤或者一个也不完成，如果余额的更新、TACUF的置位、电子钱包应用的灰锁状态的恢复没有成功，标准交易明细和内部专用明细也不应被更新。

7.7.14 回送确认（步骤 7.14）

IC卡在DEBIT FOR UNLOCK命令的响应报文中回送TAC码和SW1 SW2＝“9000”，表明余额已被更新而且电子钱包应用已解锁。

7.7.15 读取 TAC 码（步骤 7.15）

终端读取由IC卡发来的TAC码，合成完整的交易成交数据包。

7.7.16 发出 GET LOCK PROOF（P1＝‘01’）命令（步骤 7.16）

终端发出GET LOCK PROOF（P1＝‘01’）命令。

7.7.17 处理 GET LOCK PROOF（P1=‘01’）命令（步骤 7.17）

IC卡将内部的TACUF（交易验证码待读标志）复位。

7.8 联机解扣交易

联机解扣交易允许将IC卡上的电子钱包应用解锁并扣除相应的交易金额。本交易必须在联机的终端上进行。

7.8.1 发出 INITIALIZE FOR GREY UNLOCK 命令（步骤 8.1）

终端发出INITIALIZE FOR GREY UNLOCK命令启动联机解扣交易。

7.8.2 处理 INITIALIZE FOR GREY UNLOCK 命令（步骤 8.2）

IC卡收到INITIALIZE FOR GREY UNLOCK命令后，将进行以下操作：检查IC卡是否支持命令中包含的密钥索引号。如果不支持，返回状态字“9403”（不支持的密钥索引号），且不返回其他数据。

在通过以上检查之后，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），供主机来验证联机解扣交易和IC卡的合法性。

过程密钥SESULK被用于电子钱包的联机解扣交易。过程密钥是用DULK密钥并按照JR/T 0025.2的附录B中的机制产生的。

用来产生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JR/T 0025.2的附录B。

用SESUlK对以下数据加密产生MAC1（按所列顺序）：

——电子钱包余额；

——电子钱包脱机交易序号；

——交易类型标识；

——终端机编号。

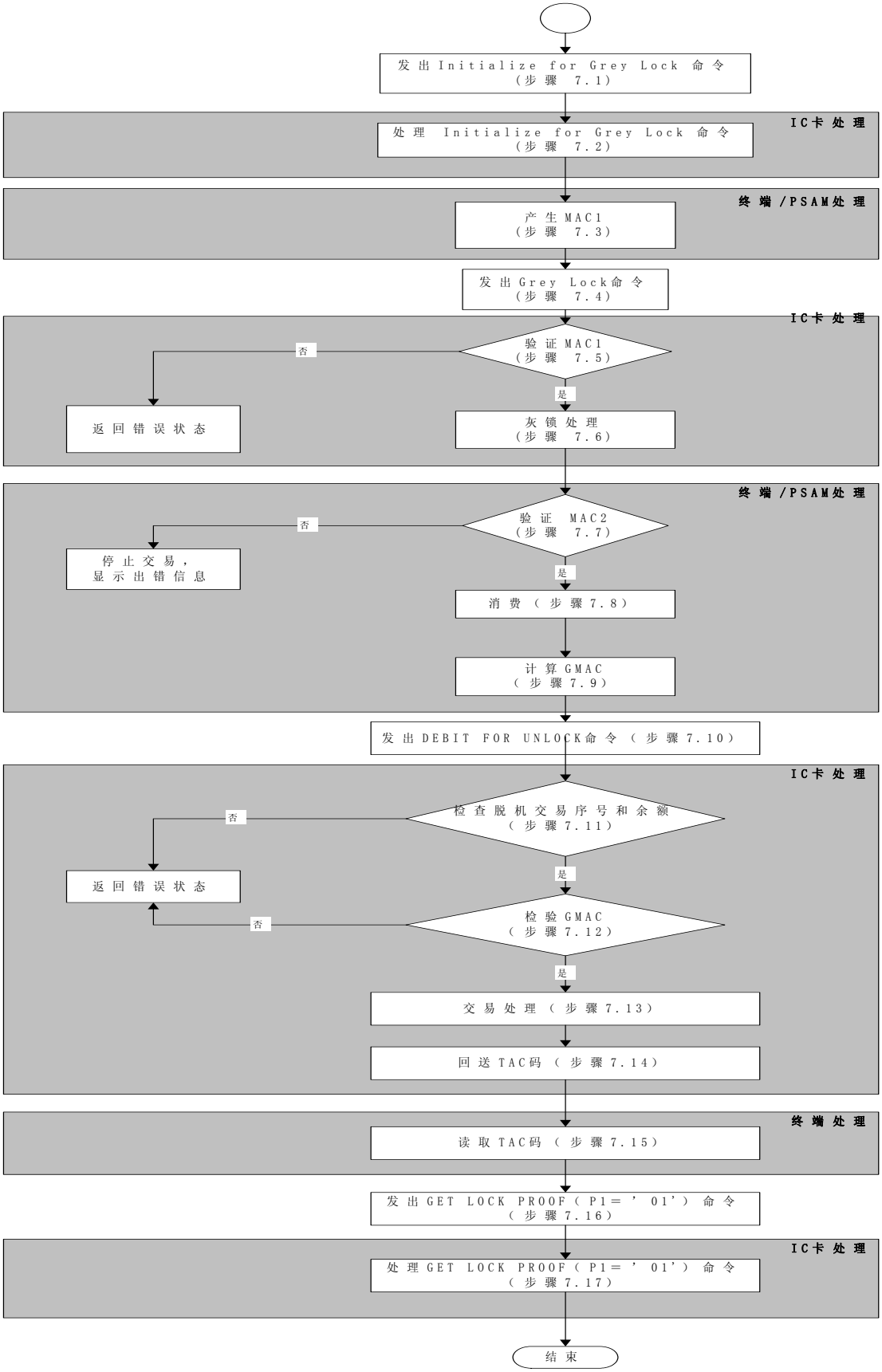

图3 灰锁消费交易流程

IC卡将把5.2.20.4定义的INITIALIZE FOR GREY UNLOCK命令的响应报文送给终端处理。

如果IC卡返回的状态不是“9000”，终端将终止交易。

在收到INITIALIZE FOR GREY UNLOCK命令的响应报文后，终端将一个包含表38中数据的联机解扣许可请求数据包送往发卡方主机。

7.8.3 验证 MAC1（步骤 8.3）

主机将生成SESULK并且确认MAC1是否有效。如果MAC1有效，交易处理将按7.8.5条描述的步骤继续执行，否则主机返回一个错误状态字，交易处理将转至7.8.4条描述的步骤。

7.8.4 回送错误状态（步骤 8.4）

如果出现使联机解扣交易不能被接受的情况，则主机应通知终端。终端将采取相应的措施。

7.8.5 主机处理（步骤 8.5）

在确认能够进行联机解扣交易后，主机将产生一个报文鉴别码（MAC2），供IC卡对主机合法性进行检查。

MAC2的计算机制见JR/T 0025.2的附录B。

用SESULK对以下数据进行加密产生MAC2（按所列顺序）：

——应补扣的交易金额；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

主机发送一个联机解扣交易接受报文给终端，其中至少包括MAC2、交易日期（主机）和交易时间（主机）。

7.8.6 发出 GREY UNLOCK 命令（步骤 8.6）

终端收到主机的联机解扣交易响应报文后，向IC卡发出GREY UNLOCK命令，以更新卡上电子钱包余额、并将电子钱包应用解锁。

7.8.7 验证 MAC2（步骤 8.7）

收到GREY UNLOCK命令后，IC卡先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”（金额不足），但不回送其他数据。IC卡还要验证MAC2的有效性。如果MAC2是有效的，交易处理将继续执行7.8.8条所描述的步骤；否则IC卡返回错误状态字“9302”（MAC无效）给终端。

7.8.8 交易处理（步骤 8.8）

IC卡从卡上的电子钱包余额中减去交易金额（如果交易金额为0，则省略对余额的修改），将电子钱包联机交易序号加1，将内部的解扣出错计数器复位，并将电子钱包应用解锁。

IC卡产生一个报文鉴别码（MAC3），包含在从卡传送到主机（通过终端）的GREY UNLOCK命令的响应报文中，以供主机对联机解扣交易的成功的合法性进行检查。MAC3的计算机制见JR/T 0025.2的附录B。

用SESULK对以下数据进行加密产生MAC3（按所列的顺序）：

——电子钱包余额；

——电子钱包联机交易序号（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）。

在对电子钱包的联机解扣交易中，IC卡用以下数据组成的一个记录来更新标准交易明细：

——电子钱包联机交易序号；

——交易金额；

——交易类型标识（‘95’=电子钱包联机解扣）；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

对于电子钱包的联机解扣交易，IC卡将用以下数据组成的一个记录更新内部专用明细文件，以便以后终端可以通过GET LOCK PROOF命令得到：

——交易类型标识；

——电子钱包代号（‘01’=电子钱包）；

——电子钱包余额；

——电子钱包联机交易序号；

——终端机编号；

——交易日期；

——交易时间；

——交易金额；

——MAC3。

IC卡必须全部成功地完成以上几个步骤或者一个也不完成，如果上述的操作没有成功，标准交易明细和内部专用明细也不应更新。

7.8.9 验证 MAC3（步骤 8.9）

主机收到从IC卡（经过终端）传来的MAC3后，应验证MAC3的有效性。

如果MAC3正确，则执行7.8.10中描述的步骤，否则主机发给终端错误状态字。

7.8.10 显示完成（步骤 8.10）

在收到主机的完成报文后，终端做相应的处理，显示完成信息。

7.9 补扣交易

补扣交易允许持卡人在灰锁的电子钱包应用中，对电子钱包补扣上次消费交易未扣除的交易额，并将电子钱包应用解锁。

本交易必须在拥有该电子钱包的上次异常交易记录的终端上进行。异常交易记录至少包括灰锁的电子钱包应用的应用序列号、灰锁的电子钱包脱机交易序号、应扣的交易金额、GMAC。拥有异常交易记录的终端可以是产生灰卡的终端，也可以是通过网络通讯得到异常交易记录的其他终端。

在交易预处理流程中发现电子钱包应用已灰锁时，进入本交易流程。

交易预处理流程中，终端收到IC卡返回的GET LOCK PROOF（P1＝‘00’）的命令响应报文后，得到上次的灰锁操作的产生日期、时间、MAC2、GTAC等数据。这些数据是终端进行补扣交易的依据。详细的响应报文参见5.2.16.4条中的表21。

7.9.1 查找异常交易记录（步骤 9.1）

终端得到IC卡的响应报文后，在异常交易记录中进行查找，如果有符合条件的异常交易记录，就进入7.9.2条所描述的步骤；否则显示相应的提示信息。

7.9.2 发出 DEBIT FOR UNLOCK 命令（步骤 9.2）

终端发出DEBIT FOR UNLOCK命令。

7.9.3 检查脱机交易序号和余额（步骤 9.3）

IC卡收到DEBIT FOR UNLOCK命令后，将进行以下操作：

——检查脱机交易序号是否匹配，如果脱机交易序号不匹配，IC 卡将返回“9406”（脱机交易序号错），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”。（金额不足），但不回送其他数据，IC 卡不操作内部出错计数器，终端应采取相应的措施。

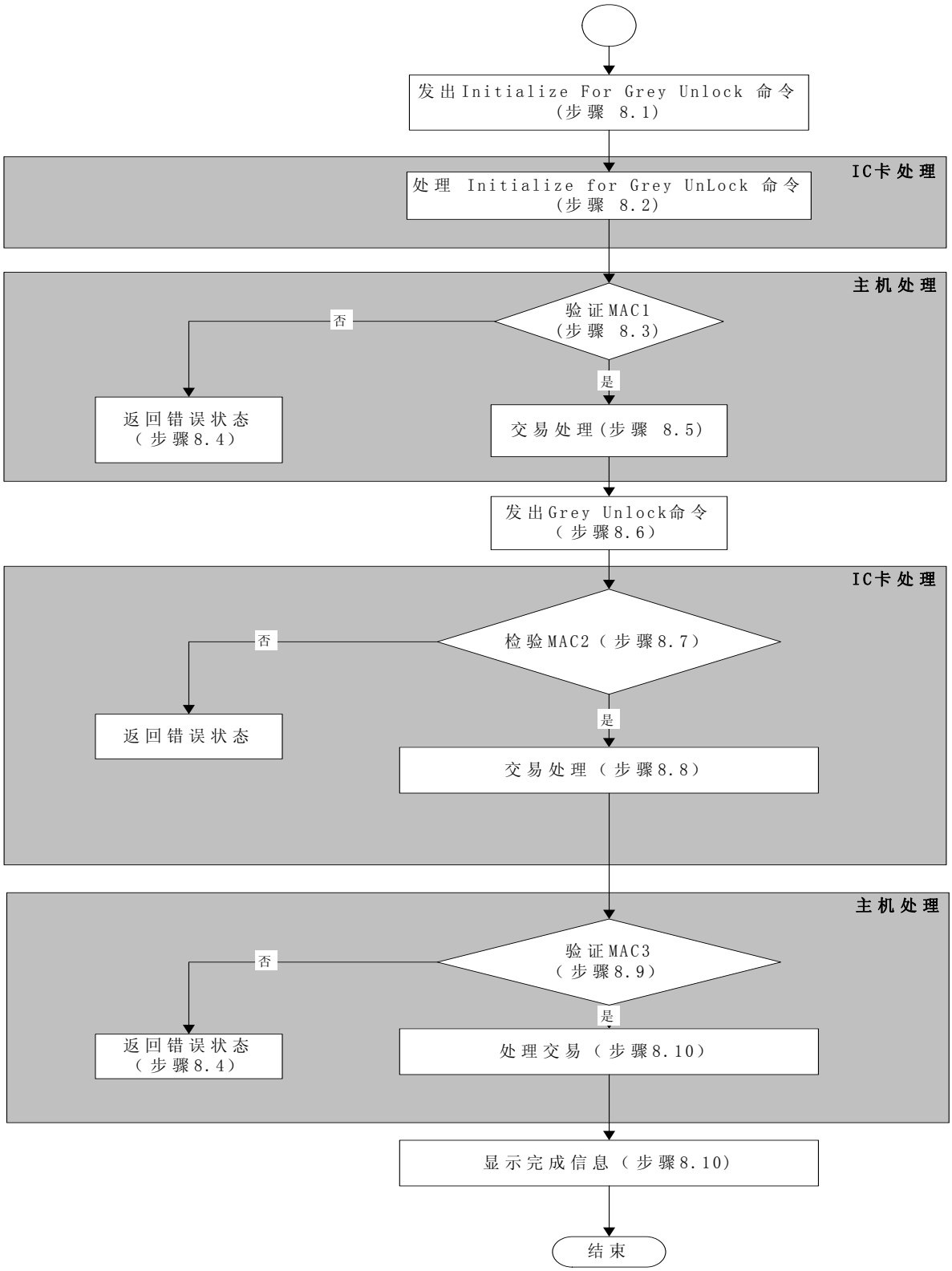

图4 联机解扣交易流程

通过上面的检查后，IC卡进入7.9.4条所描述的步骤。

7.9.4 验证 GMAC（步骤 9.4）

IC卡验证GMAC的有效性。如果GMAC是有效的，将IC卡内部的解扣出错计数器复位，交易处理将继续执行7.9.5条。如果GMAC是无效的，IC卡返回错误状态字“9302”（MAC无效）给终端，同时操作内部的解扣出错计数器，出错达到3次则临时锁住应用以防止恶意试探。

7.9.5 交易处理（步骤9.5）

IC卡从卡上的电子钱包余额中减去灰锁消费的交易金额(如果交易金额为0,则省略对余额的修改)、将电子钱包应用解锁，并将卡内的TACUF（交易验证码待读标志）置位。

IC卡应该用和JR/T 0025.2的附录B中相同的机制直接用密钥DTK产生一个TAC。TAC将被写入终端交易数据包，以便后来传给主机进行交易验证。

下面是用来生成TAC的要素：

——交易金额；

——交易类型标识；

——终端机编号（发出DEBIT FOR UNLOCK命令的终端）；

——终端交易序号（发出DEBIT FOR UNLOCK命令的终端）；

——交易日期（发出DEBIT FOR UNLOCK命令的日期）；

——交易时间（发出DEBIT FOR UNLOCK命令的时间）。

对于电子钱包的补扣交易，IC卡将用以下数据组成的一个记录更新标准交易明细：

——电子钱包脱机交易序号；

——交易金额；

——交易类型标识（电子钱包解扣）；

——终端机编号（发出DEBIT FOR UNLOCK命令的终端）；

——交易日期（发出DEBIT FOR UNLOCK命令的日期）；

——交易时间（发出DEBIT FOR UNLOCK命令的时间）。

对于电子钱包的补扣交易，IC卡将用以下数据组成的一个记录更新内部专用明细文件，以便以后终端可以通过GET LOCK PROOF命令得到：

——交易类型标识；

——电子钱包代号（‘01’=电子钱包）；

——电子钱包余额；

——电子钱包脱机交易序号；

——终端机编号（发出DEBIT FOR UNLOCK命令的终端）；

——交易日期（发出DEBIT FOR UNLOCK命令的日期）；

——交易时间（发出DEBIT FOR UNLOCK命令的时间）；

——交易金额；

——TAC。

IC卡必须全部成功地完成以上几个步骤或者一个也不完成，如果余额的更新、TACUF的置位、电子钱包应用解锁未成功，标准交易明细和内部专用明细也不应被更新。

7.9.6 回送TAC码（步骤9.6）

IC卡在DEBIT FOR UNLOCK命令的响应报文中回送TAC码，表明余额已被更新而且电子钱包应用已解锁。

7.9.7 读取TAC码（步骤9.7）

终端读取由IC卡发来的TAC码，合成完整的交易成交数据包。

7.9.8 发出GET LOCK PROOF（P1＝‘01’）命令（步骤9.8）

终端发出GET LOCK PROOF（P1＝‘01’）命令。

7.9.9 处理GET LOCK PROOF（P1＝‘01’）命令（步骤9.9）

IC卡将内部的TACUF（交易验证码待读标志）复位。

7.10 补充交易

补充交易允许终端读取上次灰锁消费交易或补扣交易中未获得的TAC，上送主机以供验证。

在交易预处理流程中发现电子钱包解扣操作已完成而TAC未成功读取，则进入本交易流程。

交易预处理流程中，终端收到IC卡返回的GET LOCK PROOF（P1＝‘00’）的命令响应报文后，得到上次的灰锁操作的产生日期、时间、TAC等数据。这些数据是终端进行补充交易的依据。

详细的响应报文参见5.2.16.4中的表22。

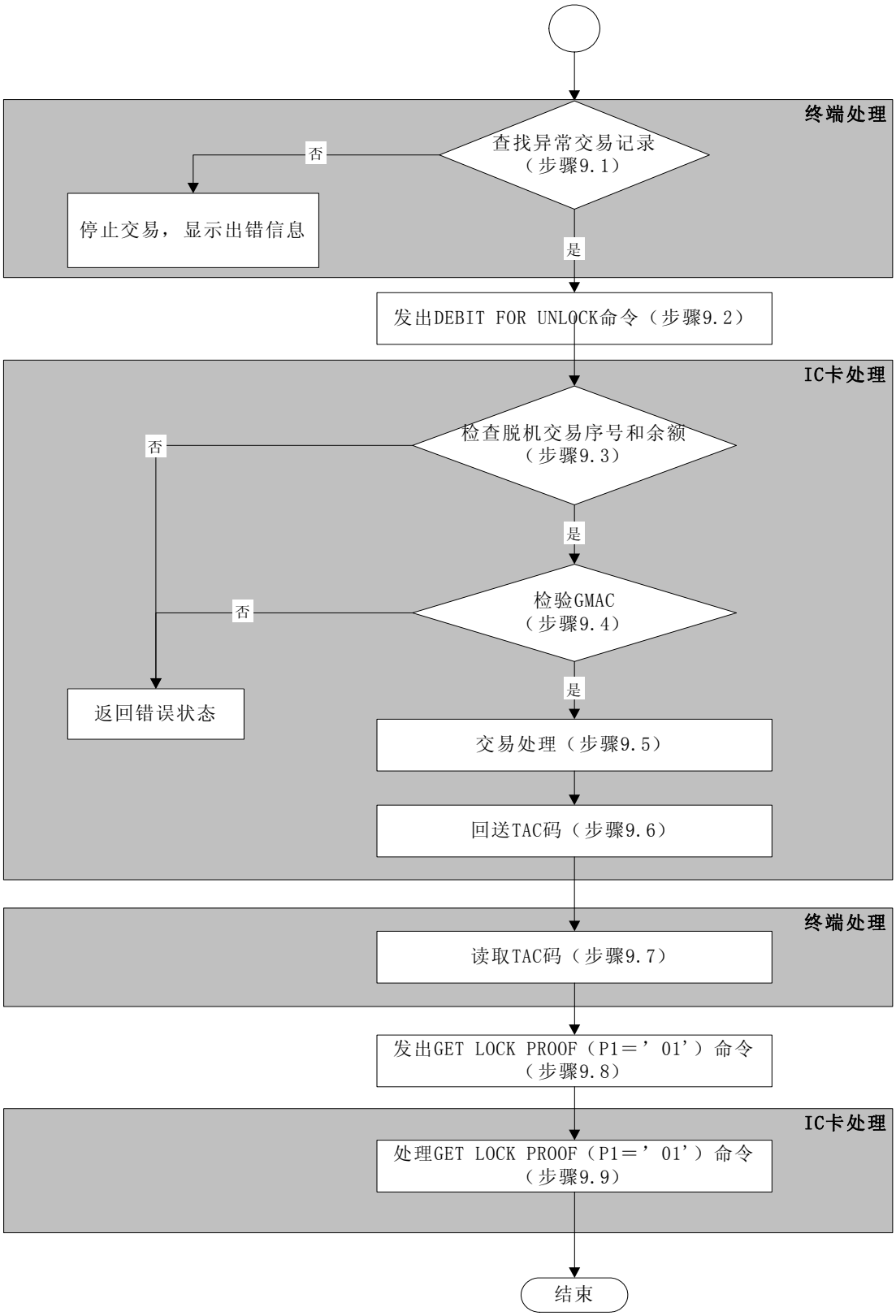

图5　补扣交易流程

7.10.1　读取 TAC（步骤 10.1）

终端通过GET LOCK PROOF命令中的响应报文，获得上次灰锁消费或补扣交易的TAC。

7.10.2　形成补充交易数据包（步骤 10.2）

终端将读到的TAC，和其他的相关数据合成一条补充交易数据包，以便上送主机。

7.10.3　发出 GET LOCK PROOF（P1＝‘01’）命令（步骤 10.3）

终端发出GET LOCK PROOF（P1＝‘01’）命令。

7.10.4　处理 GET LOCK PROOF（P1＝‘01’）命令（步骤 10.4）

IC卡将内部的TACUF复位。

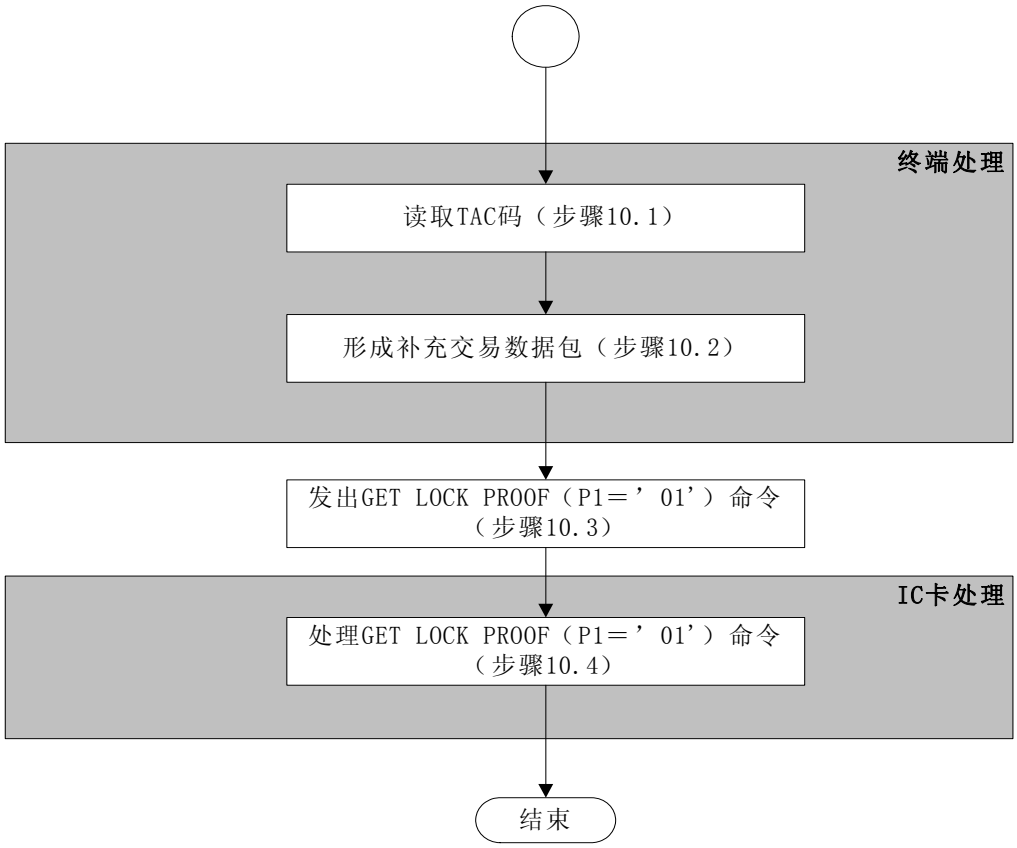

图6　补充交易流程

7.11　应用维护功能

见JR/T 0025.2的5.5.9条。

7.11.1　安全报文

见JR/T 0025.2的5.5.9.1条。

7.11.2　卡片锁定

见JR/T 0025.2的5.5.9.2条。

7.11.3　应用锁定

见JR/T 0025.2的5.5.9.3条。

7.11.4　应用解锁

见JR/T 0025.2的5.5.9.4条。

7.11.5　PIN 解锁

见JR/T 0025.2的5.5.9.5条。

7.11.6　二进制形式修改

见JR/T 0025.2的5.5.9.6条。

7.11.7 更改 PIN

见JR/T 0025.2的5.5.9.7条。

7.11.8 重装 PIN

见JR/T 0025.2的5.5.9.8条。

7.11.9 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。

首先终端必须按照7.1进行交易预处理，并必须校验个人识别码（PIN）。

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JR/T 0025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。

7.11.10 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。

首先终端必须按照7.1进行交易预处理，并必须校验个人识别码（PIN）。

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JR/T 0025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，获取符合应用数据。

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。

7.11.11 关闭非接触通道

终端发出关闭非接触通道命令来关闭卡片的非接触通信通道。

此命令参照JR/T 0025.8。安全报文的计算和JR/T 0025.2的5.5.9.1安全报文中描述的相同。命令的成功执行使得卡片的非接触通道失效。在这种情况下，以非接触方式对卡片发命令（除了激活非接触通道命令），卡片将没有响应。

此功能对接触式电子钱包是可选功能。

7.11.12 激活非接触通道

终端发出激活非接触通道命令来激活卡片的非接触通信通道。

此命令见JR/T 0025.8。安全报文的计算和JR/T 0025.2的5.5.9.1安全报文中描述的相同。命令的成功执行使得卡片的非接触通道重新激活。此命令可以以非接触方式发送给卡片。

此功能对接触式电子钱包是可选功能。

8 交易处理性能

交易处理性能要求针对非接触式金融IC卡。

交易处理性能要求主要体现在消费交易和复合应用消费交易，从卡被选择到交易处理结束允许离开磁场感应区的建议性限制为不大于500ms。

附 录 A
（资料性附录）
数据元解释

参见JR/T 0025.2的附录A。

补充规定符合JR/T 0025的卡的应用版本号与接触式金融IC卡电子钱包应用版本号。

补充数据元如下。

数据域	来源	格式	长度（字节）	值
解扣出错计数器	IC 卡	b	1	3
灰锁交易验证码	IC 卡 终端	cn	4	
交易验证码待读标志	IC 卡	b	1	00－复位 01－置位
终端随机数	终端	cn	4	

附 录 B
（规范性附录）
应用的密钥关系

电子钱包扩展应用指南的密钥引用电子钱包/电子存折应用规范中的相关密钥，见JR/T 0025.2的附录B。

附 录 C
（规范性附录）
电子钱包应用的基本数据文件

C.1 电子钱包应用的公共基本数据文件

见JR/T 0025.2附录C的表C.1。

C.2 电子钱包应用的持卡人基本数据文件

见JR/T 0025.2附录C的表C.2。

C.3 内部数据元

见JR/T 0025.2附录C的表C.3。不同点如下：增加“电子钱包消费透支限额”，长度为4字节。

C.4 交易明细

此文件必须能够容纳至少10条圈存、消费等交易记录。
交易明细必须允许卡对其循环修改。循环文件的结构应符合ISO/IEC 7816-4。
对明细中所有数据元的修改必须考虑数据完整性和安全要求。

表 C.1 交易明细

文件标识（SFI）		‘24’（十进制）
文件类型		循环
文件存取控制		读＝开放
		改写＝禁止
记录长度		23 字节
字节	数据元	长度
1－2	电子存折或电子钱包联机或脱机交易序号	2
3－5	透支限额	3
6－9	交易金额	4
10	交易类型标识	1
11－16	终端机编号	6
17－20	交易日期（终端）	4
21－23	交易时间（终端）	3

C.5 复合应用专用文件

表 C.2 复合应用专用文件

文件标识（SFI）	‘25’（十进制）
文件类型	变长记录文件
文件存取控制	读＝开放
	改写＝保护
记录长度	最大 256 字节

字节	数据元	长度
1	复合应用类型标识符	1
2	记录长度	1
3	应用锁定标志	1
4-n	复合应用数据	n-3

附 录 D
（资料性附录）
复合应用说明

复合应用是本部分在JR/T 0025.2电子钱包应用的基础上，根据部分行业应用的特定，引入的新应用模式。复合应用消费与电子钱包消费的主要差别在于前者增加了在消费交易中卡片记录非金融数据的能力，且数据写入和交易同时完成。此非金融数据主要用于作为消费金额的计算依据。因此复合应用消费主要适用于使用计程、计时或计次的金融消费领域。

本部分应保证复合应用数据在卡片中的存储的完整性和存取的安全性。

本部分不保证复合应用数据的有效性。

复合应用数据的结构和定义不在本应用规范的范围内。

每一复合应用均由唯一的复合应用类型标识符表征，其值应统一分配。对特定复合应用，其所对应的复合应用专用文件中的记录长度固定，并统一指定。

附 录 E
（资料性附录）
复合应用消费交易范例

本附录以非接触式金融IC卡电子钱包应用在一特定应用环境中的应用为范例，描述复合应用的一种实际应用模式。在这一特定应用环境中，空间被分割为收费区和非收费区。持卡人在进入收费区时，终端将在IC卡中写入特定信息；当持卡人离开收费区时，终端根据特定信息计算所需支付费用，并从电子钱包中扣除等额金额。

E.1 基础定义

以下定义复合应用所需基础定义：定义此复合应用的复合应用类型标识符为‘13’。

复合应用记录格式见表E.1。

表 E.1 复合应用专用文件

字段名	长度	字节
城市代码	4	1－4
运营企业代码	6	5－10
记录格式版本号	1	11
交易标志	1	12
进收费区交易时间	4	13－16
进收费区交易线路代码	1	17
进收费区交易站点代码	1	18
进收费区交易闸机代码	1	19
进收费区交易序号	4	20－23
出收费区交易时间	4	24－27
出收费区交易线路代码	1	28
出收费区交易站点代码	1	29
出收费区交易闸机代码	1	30
出收费区交易金额	3	31－34
出收费区交易序号	4	35－38
专用 TAC	4	39－42

E.2 交易流程

E.2.1 增加复合应用类型

持卡人如需使用非接触式金融IC卡在特定应用环境中进行交易，需先在卡片中增加相应复合应用类型，即启用此类型的复合应用。

增加复合应用操作必须在根据JR/T 0025支持复合应用的终端上联机完成。

具体处理流程为：

——终端在激活卡片后，由持卡人选择进入增加复合应用增加操作界面，终端向持卡人提示其支持的所有复合应用类型，其中包括此特定复合应用；

——当持卡人选择增加此特定复合应用后，终端使用 READ RECORD 命令查询卡片是否支持复合应用，是否支持此特定复合应用。如不支持复合应用，可联机创建复合应用专用文件。如卡片已支持此特定复合应用，终端应提示持卡人。

如卡片支持复合应用，但不支持此特定复合应用或此特定复合应用已锁定，则终端可根据7.11.9条在卡片中增加此特定复合应用，即创建以‘13’为记录号的长度为43字节的记录，并将记录内所有字节初始化为0。

E.2.2 进收费区交易流程

进收费区交易有两种实现方式：交易方式和文件改写方式。其中交易方式将完成一次完整的消费交易。文件改写方式则直接改写复合应用专用文件中的相关记录。

E.2.2.1 交易方式

持卡人使用非接触式金融IC卡在此特定应用环境中进行进收费区交易时，终端将作如下处理：

——终端首先选择和激活卡片，判断卡片为非接触式金融 IC 卡，并通过 AID 选择进入电子钱包应用目录；

——终端发出 READ RECORD 命令查询复合应用，判断卡片是否支持复合应用，是否支持此特定复合应用。

如支持，终端应读取此特定复合应用专用数据，并根据数据进行处理，如判断上次是否未出收费区等等。如处理结果为不允许进行进收费区交易，终端应提示持卡人。

如处理结果允许进行进收费区交易，终端根据7.4条进行复合应用消费交易，其中交易金额为0。

终端根据其自身情况，在UPDATE CAPP DATA CACHE中更新此特定复合应用专用数据，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。

交易成功后，终端应允许持卡人进收费区。

E.2.2.2 文件改写方式

持卡人使用非接触式金融IC卡在此特定应用环境中进行进收费区交易时，终端将作如下处理：

——终端首先选择和激活卡片，判断卡片为非接触式金融 IC 卡，并通过 AID 选择进入电子钱包应用目录；

——终端发出 READ RECORD 命令查询复合应用，判断卡片是否支持复合应用，是否支持此特定复合应用。

如支持，终端应读取此特定复合应用专用数据，并根据数据进行处理，如判断上次是否未出收费区等等。如处理结果为不允许进行进收费区交易，终端应提示持卡人。

如处理结果允许进行进收费区交易，则终端向卡片发出GET CHALLENGE命令获取卡片随机数，并利用随机数和消费密钥DPK生成更改后的此特定复合应用专用数据MAC。终端向卡片发出包含更改后的此特定复合应用专用数据及MAC的UPDATE RECORD命令，更新复合应用专用文件记录。

更新成功即表示进收费区交易成功，终端应允许持卡人进收费区。

E.2.3 出收费区交易

持卡人使用非接触式金融IC卡在此特定应用环境中进行出收费区交易时，终端将作如下处理：

——终端首先选择和激活卡片，判断卡片为非接触式金融 IC 卡，并通过 AID 选择进入电子钱包应用目录；

——终端发出 READ RECORD 命令查询复合应用，判断卡片是否支持复合应用，是否支持此特定复合应用。

如支持，终端应读取此特定复合应用专用数据，并根据数据进行处理，如判断上次是否未进收费区等等，并计算需消费金额。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，终端根据7.4条进行复合应用消费交易，其中交易金额为计算所得的消费金额。

终端根据其自身情况，在UPDATE CAPP DATA CACHE中更新此特定复合应用专用数据，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。

交易成果后，终端应允许持卡人出收费区。

附 录 F
（规范性附录）
补充卡片指令

F.1 增加记录命令（APPEND RECORD）

F.1.1 定义和范围

APPEND RECORD命令用于对变长记录文件追加新记录。

F.1.2 命令报文

增加记录命名报文编码在表F.1中。

表 F.1 APPEND RECORD 命令报文编码

代码	值
CLA	‘04’或‘00’
INS	‘E2’
P1	‘00’
P2	见表 F.2
Lc	后续数据域的长度
Data	追加的新记录+报文鉴别码（MAC）数据元（4 字节）
Le	不存在

表F.2定义了命令报文中的引用控制参数。

表 F.2 APPEND RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
x	x	x	x	x				SFI
					0	0	0	追加新记录

F.1.3 命令报文数据域

命令报文数据域由追加的新记录和报文鉴别码（MAC）组成。

F.1.4 响应报文数据域

响应报文数据域不存在。

F.1.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的错误状态字如表F.3所示。

表 F.3 APPEND RECORD 错误状态

SW1	SW2	含义
65	81	内存失败
67	00	长度错误
69	81	命令与文件结构不相容
69	82	不满足安全状态
6A	81	不支持此功能
6A	82	未找到文件
6A	84	文件中存储空间不够

F.2 读记录命令（READ RECORD）

READ RECORD命令在JR/T 0025.1的6.2.12中定义。为满足在扩展应用中的使用情况，增加以下定义：P1表示记录号或记录标识。

P1表示记录号或记录标识。

READ RECORD命令报文中的引用控制参数在表F.4中定义。

表 F.4 READ RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
x	x	x	x	x				SFI
					1	0	0	P1 为记录号
					0	0	0	P1 为记录标识