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 0025.2—201x
代替JR/T 0025.2—2010

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

China financial integrated circuit card specifications—
Part 2：Electronic purse/electronic deposit application specification

（送审稿）

201x-xx-xx 发布　　201x-xx-xx 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17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；

——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2部分。

本部分代替JR/T 0025.2—2005《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》。

本部分与JR/T 0025.2-2010相比主要变化如下：

——修订了标准的前言。

本部分与JR/T 0025.2—2005相比主要变化如下：

——重新起草标准的前言及引言；

——对“术语和定义”及“符号和缩略语”在正文中的出现的情况做了核对，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，并同步修改正文；

——对“规范性引用文件”在正文中的引用情况做了核对，对正文中引用到的文件根据标准编写要求进行重新编排和规范，将参考到的文件归集到参考文献，将没有引用也没有参考的文件予以剔除；

——根据当前先进技术的发展趋势及主流标准的应用情况，对本部分进行了补充完善；

——为保证标准的适用性，根据中国银行卡产业的实际需求，针对原标准在使用过程中发现的问题进行修订。

本部分的附录A、附录B和附录C为规范性附录。

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、上海浦东发展银行、中国银联股份有限公司、中国印钞造币总公司、中国金融电子化公司和

银行卡检测中心。

本部分主要起草人：。

本部分所代替标准的历次版本发布情况为：

——《中国金融集成电路（IC）卡规范》（V1.0）卡片规范；

——JR/T 0025.2—2005；

——JR/T 0025.2—2010。

引　言

本部分为JR/T 0025的第2部分，与JR/T 0025的第1部分一起构成电子钱包/电子存折规范。

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

1 范围

JR/T 0025的本部分主要规定了电子钱包/电子存折应用所涉及的文件、命令、安全需求及交易流程，也描述了磁条卡功能的相关需求，其中：

——电子存折/电子钱包应用。定义了用于电子存折和电子钱包的文件结构、命令集、交易流程和安全机制等内容。

——磁条卡功能（Easy Entry）。定义了一种利用金融IC卡实现磁条卡功能的简单应用，并对支持该应用的卡和终端数据文件、命令及应用选择等进行了详细描述。

本部分适用于由银行发行或接受的金融IC卡。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）。

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。

GB/T 14916 识别卡 物理特性（GB/T 14916—2006，ISO/IEC 7810:2003，IDT）

GB/T 15120（所有部分） 识别卡 记录技术[GB/T 15120（所有部分）—1994，ISO 7811:1985，IDT]

GB/T 15694.1 识别卡 发卡者标识 第1部分：编号体系（GB/T 15694.1—1995，ISO/IEC 7812-1:1993，IDT）

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（GB/T 16649.5—2002，ISO/IEC 7816-5:1994，NEQ）

GB/T 17552 识别卡 金融交易卡（GB/T 17552—1998，ISO/IEC 7813:1995，IDT）

GB/T 19584 银行卡磁条信息格式和使用规范

JR/T 0025.1 中国金融集成电路（IC）卡规范 第1部分：电子钱包/电子存折应用卡片规范

JR/T 0025.3 中国金融集成电路（IC）卡规范 第3部分：与应用无关的IC卡与终端接口规范

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

ISO 8731-1 银行业 批准的报文鉴别算法 第1部分：DEA

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

冷复位 cold reset

当提供给IC卡的电源电压和其他信号从静止状态中复苏且收到复位信号后，IC卡产生的复位。

3.2

热复位 warm reset

在时钟（CLK）和电源电压（VCC）处于激活状态的前提下，IC 卡收到复位信号时产生的复位。

3.3

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）。

3.4

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。

3.5

串联 concatenation

通过把第二个元素的字节添加到第一个元素的结尾将两个元素连接起来。每个元素中的字节在结果串中的顺序和原来从IC卡发到终端时的顺序相同，即高位字节在前。在每个字节中位按由高到低的顺序排列。

3.6

响应 response

IC卡处理完成收到的命令报文后，返回给终端的报文。

3.7

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。

3.8

集成电路 integrated circuit （IC）

具有处理和/或存储功能的电子器件。

3.9

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

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

3.10

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。

3.11

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。

3.12

半字节 nibble

一个字节的高四位或低四位。

3.13

明文 plaintext

未被加密的信息。

3.14

密钥 key

控制加密转换操作的符号序列。

3.15

加密算法 cryptographic algorithm

为了隐藏或显现数据信息内容的变换算法。

3.16

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。

3.17

电子存折 electronic deposit

一种为持卡人进行消费、取现等交易而设计的支持个人识别码（PIN）保护的金融IC卡应用。它支持圈存、圈提、消费和取现等交易。

3.18

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。

3.19

圈存 load

持卡人将其在银行相应账户上的资金划转到电子存折或电子钱包中。圈存交易必须在金融终端上联机进行[1]。

一般情况下，圈存到电子存折中的资金仍计付活期利息，圈存到电子钱包中的资金不计付利息。但具体作法由发卡方自行决定。

3.20

圈提 unload

持卡人将电子存折中的部分或全部资金划回到其在银行的相应账户上。圈提交易必须在金融终端上联机进行[2]。

4 符号和缩略语

下列符号和缩略语适用于 JR/T 0025 的本部分。

AID	应用标识符（Application Identifier）
an	字母数字型（Alphanumeric）
ans	字母数字及特殊字符型（Alphanumeric Special）
ATI	应用类型标识（Application Type Identifier）
b	二进制（Binary）
CLA	命令报文的类别字节（Class Byte of the Command Message）
cn	压缩数字型（Compressed Numeric）
DEA	数据加密算法（Data Encryption Algorithm）
DF	专用文件（Dedicated File）
ED	电子存折（Electronic Deposit）
EF	基本文件（Elementary File）
EP	电子钱包（Electronic Purse）
FCI	文件控制信息（File Control Information）
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）

[1]在发卡方之间联网的情况下，可以在其他发卡方终端联行进行。

[2]在发卡方之间联网的情况下，可以在其他发卡方终端联行进行。

Lc	终端发出的命令数据的实际长度（Exact Length of 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）
MF	主文件（Master File）
n	数字型（Numeric）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
PIN	个人识别码（Personal Identification Number）
POS	销售点终端（Point of Service）
PSAM	销售点终端安全存取模块（Purchase Secure Access Module）
PSE	支付系统环境（Payment System Environment）
PVN	PIN 校验值（PIN Verification Number）
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 Crypogram）
TTI	交易类型标识（Transaction Type Identifier）
YYYYMMDD	年、月、日（Year, Month, Day）

5 电子存折/电子钱包应用

电子存折/电子钱包应用是为持卡人进行金融交易而设计的一种应用。对于一张金融 IC 卡来说，它可以同时支持电子存折和电子钱包两种应用，也可以只支持其中的一种。卡片上两种应用的存在情况可以由应用类型标识（ATI）来指明。

5.1 文件

5.1.1 文件结构

电子存折/电子钱包应用的文件结构应符合ISO/IEC 7816-4及JR/T 0025.3的有关规定。

电子存折/电子钱包应用对应的专用文件（DF）与附录C中的基本文件构成一个树状结构的分支。该专用文件是其下属的基本文件的入口点。

5.1.2 专用文件

按照ISO 7816-4和JR/T 0025.3的规定，电子存折/电子钱包应用所对应的专用文件（DF）包含一个文件控制信息（FCI）。通过该文件可以对在附录C中描述的基本文件（EF）进行访问。该专用文件的上一层专用文件是主文件（MF）。

5.1.3 基本文件

按照ISO 7816-4和JR/T 0025.3的定义，基本文件（EF）包含了一组与应用相关的数据。

电子存折/电子钱包应用下的基本文件有两种类型：记录文件类型和二进制文件类型。

电子存折/电子钱包应用下的基本文件格式见附录C中的描述。

5.1.4 文件选择

电子存折/电子钱包应用的专用文件根据 JR/T 0025.3 的规定，采用应用标识符（AID）方式进行选择。

成功选择了电子存折/电子钱包应用的专用文件后，该专用文件被设置为当前文件，并允许使用该应用的特殊命令对其进行操作。

基本文件的选择是通过读取命令并采用SFI方式实现的。

5.2 命令

本条描述了电子存折/电子钱包应用（以下简称ED/EP应用）的命令和响应。

命令及其响应的代码约定和报文格式在JR/T 0025.1中描述。

附录A中详细定义了命令报文和响应报文的数据元。

在应用执行过程中，卡片总是处于以下状态之一，在一种状态下，只有某些命令能够被执行。卡片具有的状态如下：

——空闲状态；

——圈存状态；

——消费/取现状态；

——圈提状态；

——修改状态。

应用选择完成后，卡片首先进入空闲状态。当卡片从终端接收到一条命令时，它必须首先检查当前状态是否允许执行该命令。在命令执行成功后，卡片将如表1所示进入另一个状态（或同一个）。如果命令执行不成功，则卡片进入空闲状态。

表1说明了命令执行成功后的状态变化。第一行表示命令发出时卡片的当前状态，第一列表示发出的命令，整张表给出的是在当前状态下某个命令执行成功后的状态。

阴影部分表示在卡片处于相应状态时发出此命令是无效的。在这种情况下，卡片不执行该命令，并向终端回送“6901”状态字，同时卡片的状态变为空闲。

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	圈提	修改
CREDIT FOR LOAD	N/A	空闲	N/A	N/A	N/A
DEBIT FOR PURCHASE/CASH WITHDRAW	N/A	N/A	空闲	N/A	N/A
DEBIT FOR UNLOAD	N/A	N/A	N/A	空闲	N/A
GET BALANCE	空闲	圈存	消费/取现	圈提	修改
GET TRANSACTION PROVE	空闲	圈存	消费/取现	圈提	修改
INITIALIZE FOR LOAD	圈存	圈存	圈存	圈存	圈存
INITIALIZE FOR PURCHASE	消费/取现	消费/取现	消费/取现	消费/取现	消费/取现
INITIALIZE FOR WITHDRAW	消费/取现	消费/取现	消费/取现	消费/取现	消费/取现
INITIALIZE FOR UNLOAD	圈提	圈提	圈提	圈提	圈提
INITIALIZE FOR UPDATE	修改	修改	修改	修改	修改
UPDATE OVERDRAW LIMIT	N/A	N/A	N/A	N/A	空闲

表2定义了命令报文的类别字节和指令字节的编码以及ED/EP应用使用的参数P1和P2。

表2 命令的类别字节和指令字节

命令	CLA	INS	P1	P2
修改个人识别码（CHANGE PIN）	‘80’	‘5E’	‘01’	‘00’
圈存（CREDIT FOR LOAD）	‘80’	‘52’	‘00’	‘00’
消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）	‘80’	‘54’	‘01’	‘00’
圈提（DEBIT FOR UNLOAD）	‘80’	‘54’	‘03’	‘00’
读余额（GET BALANCE）	‘80’	‘5C’	‘00’	‘0X’
取交易认证（GET TRANSACTION PROVE）	‘80’	‘5A’	‘00’	‘XX’
取现初始化（INITIALIZE FOR CASH WITHDRAW）	‘80’	‘50’	‘02’	‘01’
圈存初始化（INITIALIZE FOR LOAD）	‘80	‘50’	‘00’	‘0X’

消费初始化（INITIALIZE FOR PURCHASE）	‘80’	‘50’	‘01’	‘0X’
圈提初始化（INITIALIZE FOR UNLOAD）	‘80’	‘50’	‘05’	‘01’
修改初始化（INITIALIZE FOR UPDATE）	‘80’	‘50’	‘04’	‘01’
重装个人识别码（RELOAD PIN）	‘80’	‘5E’	‘00’	‘00’
修改透支限额（UPDATE OVERDRAW LIMIT）	‘80’	‘58’	‘00’	‘00’

5.2.1 修改个人识别码（CHANGE PIN）命令

5.2.1.1 定义和范围

修改个人识别码（CHANGE PIN）允许持卡人将当前PIN修改为新的PIN。

当修改个人识别码（CHANGE PIN）命令成功完成后，卡片要进行以下操作：

——PIN 尝试计数器复位至 PIN 尝试次数的上限；

——将原个人识别码置为新的个人识别码。

此命令中的个人识别码（PIN）值以明文方式传送。命令数据中个人识别码（PIN）是以“cn”格式存放的，它不需要整字节的填充，只有最低有效字节的低半字节可能需要填充，且填以“F”。

5.2.1.2 命令报文

修改个人识别码（CHANGE PIN）命令报文见表3。

表3 修改个人识别码（CHANGE PIN）命令报文

代码	值
CLA	‘80’
INS	‘5E’
P1	‘01’
P2	‘00’
L_c	‘05’ - ‘0D’
Data	当前 PIN‖‘FF’‖新的 PIN
L_e	不用

5.2.1.3 响应报文数据域

响应报文的数据域不存在。

5.2.1.4 响应报文的状态字

此命令执行成功的状态字是“9000”。

表4描述了IC卡可能回送的错误状态。

表4 修改个人识别码（CHANGE PIN）错误状态

SW1	SW2	含义
‘63’	‘Cx’	验证失败，还剩下 X 次尝试机会
‘65’	‘81’	内存错误
‘69’	‘83’	验证方法锁定
‘69’	‘85’	使用条件不满足
‘6A’	‘80’	数据域参数不正确
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

5.2.2 圈存（CREDIT FOR LOAD）命令

5.2.2.1 定义和范围

圈存（CREDIT FOR LOAD）命令用于圈存交易。

5.2.2.2 命令报文

圈存（CREDIT FOR LOAD）命令报文见表5。

表5 圈存（CREDIT FOR LOAD）命令报文

代码	值
CLA	‘80’
INS	‘52’
P1	‘00’
P2	‘00’
L_c	‘0B’
Data	见表 6
L_e	‘04’

5.2.2.3 命令报文数据域

表6描述了命令报文数据域。

表6 圈存（CREDIT FOR LOAD）命令报文数据域

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

5.2.2.4 响应报文数据域

圈存（CREDIT FOR LOAD）响应报文数据域见表7。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表7 圈存（CREDIT FOR LOAD）响应报文数据域

说明	长度（字节）
TAC	4

5.2.2.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表8描述了IC卡可能回送的错误状态。

表8 圈存（CREDIT FOR LOAD）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
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

5.2.3 消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令

5.2.3.1 定义和范围

消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令用于消费/取现交易。

5.2.3.2 命令报文

消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令报文见表9。

执行初始化消费/取现（INITIALIZE FOR PURCHASE或INITIALIZE FOR CASH WITHDRAW）后即选择了消费/取现交易。

表9 消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
L_c	‘0F’
Data	见表 10
L_e	‘08’

5.2.3.3 命令报文数据域

表10描述了命令报文数据域。

表10 消费/取现 DEBIT FOR PURCHASE/CASH WITHDRAW 命令报文数据域

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

5.2.3.4 响应报文数据域

此命令执行成功的响应报文数据域见表11。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表11 消费/取现 DEBIT FOR PURCHASE/CASH WITHDRAW 响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

5.2.3.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表12描述了IC卡可能回送的错误状态。

表12 消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）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
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

5.2.4 圈提（DEBIT FOR UNLOAD）命令

5.2.4.1 定义和范围

圈提（DEBIT FOR UNLOAD）命令用于圈提交易。

5.2.4.2 命令报文

圈提（DEBIT FOR UNLOAD）命令报文见表13。

表13 圈提（DEBIT FOR UNLOAD）命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘03’
P2	‘00’
L_c	‘0B’
Data	见表 14
L_e	‘04’

5.2.4.3 命令报文数据域

表14定义了命令报文数据域。

表14 圈提（DEBIT FOR UNLOAD 命）令报文数据域

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

5.2.4.4 响应报文数据域

此命令执行成功的响应报文数据域见表15。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表15 圈提（DEBIT FOR UNLOAD）响应报文数据域

说明	长度（字节）
MAC3	4

5.2.4.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表16描述了IC卡可能回送的错误状态。

表16 圈提（DEBIT FOR UNLOAD）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）
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

5.2.5 查询余额（GET BALANCE）命令

5.2.5.1 定义和范围

查询余额（GET BALANCE）命令用于读取电子存折或电子钱包余额，实现查询余额交易。

读取电子存折余额需验证个人识别码（PIN）。

5.2.5.2 命令报文

查询余额（GET BALANCE）命令报文见表17。

表17 查询余额（GET BALANCE）命令报文

代码	值
CLA	‘80’
INS	‘5C’
P1	‘00’
P2	‘01’或‘02’；‘01’用于ED，‘02’用于EP，其他值预留
L_c	不存在
Data	不存在
L_e	‘04’

5.2.5.3 响应报文数据域

命令执行成功的响应报文数据域见表18。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表18 查询余额（GET BALANCE）响应报文数据域

说明	长度（字节）
ED余额或EP余额	4

5.2.5.4 响应报文的状态字

此命令执行成功的状态字是“9000”。

表19描述了IC卡可能回送的错误状态。

表19 查询余额（GET BALANCE）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘69’	‘82’	安全条件不满足
‘6A’	‘86’	P1和P2参数不正确
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误

5.2.6 取交易认证（GET TRANSACTION PROVE）命令

5.2.6.1 定义和范围

取交易认证（GET TRANSACTION PROVE）命令提供了一种在交易处理过程中拔出并重插卡后卡片的恢复机制。该命令的用法在5.6中说明。

5.2.6.2 命令报文

取交易认证（GET TRANSACTION PROVE）命令报文见表20。

表20 取交易认证（GET TRANSACTION PROVE）命令报文

代码	值
CLA	‘80’
INS	‘5A’
P1	‘00’
P2	要取的MAC或/和TAC所对应的交易类型标识。
Lc	‘02’
Data	见表21
Le	‘08’

5.2.6.3 命令报文数据域

表21定义了命令报文数据域。

表21 取交易认证（GET TRANSACTION PROVE）命令报文数据域

说明	长度（字节）
要取的 MAC 或/和 TAC 所对应的 ED/EP 联机或脱机交易序号。	2

如果命令中指定的交易类型标识和ED/EP联机或脱机交易序号对应的MAC或TAC可用，则响应报文数据域见表22。

表22 取交易认证（GET TRANSACTION PROVE）响应报文数据域

说明	长度
MAC	4
TAC	4

5.2.6.4 响应报文的状态字

此命令执行成功的状态字是“9000”。

表23描述了IC卡可能回送的错误状态。

表23 取交易认证（GET TRANSACTION PROVE）错误状态

SW1	SW2	含义
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘06’	所需 MAC 不可用

5.2.7 初始化取现（INITIALIZE FOR CASH WITHDRAW）命令

5.2.7.1 定义和范围

初始化取现（INITIALIZE FOR CASH WITHDRAW）命令用于初始化取现交易。

5.2.7.2 命令报文

初始化取现（INITIALIZE FOR CASH WITHDRAW）命令报文见表24。

表24 初始化取现（INITIALIZE FOR CASH WITHDRAW）命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘02’
P2	‘01’用于 ED 取现交易，其他值预留。
L_c	‘0B’
Data	见表 25
L_e	‘0F’

5.2.7.3 命令报文数据域

表25定义了命令报文的数据域。

表25 初始化取现（INITIALIZE FOR CASH WITHDRAW）命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

5.2.7.4 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。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表26 初始化取现（INITIALIZE FOR CASH WITHDRAW）响应报文数据域

说明	长度（字节）
ED 余额	4
ED 脱机交易序号（IC 卡）	2
透支限额	3
密钥版本号（DPK）	1
算法标识（DPK）	1
伪随机数（IC 卡）	4

5.2.7.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表27描述了IC卡可能回送的错误状态。

表27 初始化取现（INITIALIZE FOR CASH WITHDRAW）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持

5.2.8 初始化圈存（INITIALIZE FOR LOAD）命令

5.2.8.1 定义和范围

初始化圈存（INITIALIZE FOR LOAD）命令用于初始化圈存交易。

5.2.8.2 命令报文

初始化圈存（INITIALIZE FOR LOAD）命令报文见表28。

表28 初始化圈存（INITIALIZE FOR LOAD）命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘00’
P2	‘01’或‘02’；‘01’用于ED，‘02’用于EP，其他值预留。
L_c	‘0B’
Data	见表 29
L_e	‘10’

5.2.8.3 命令报文数据域

表29定义了命令报文数据域。

表29 初始化圈存（INITIALIZE FOR LOAD）命令报文数据域

说明	长度（字节）
密钥索引号	1

交易金额	4
终端机编号	6

5.2.8.4 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。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表30 初始化圈存（INITIALIZE FOR LOAD）响应报文

说明	长度（字节）
ED 或 EP 余额	4
ED 或 EP 联机交易序号	2
密钥版本号（DLK）	1
算法标识（DLK）	1
伪随机数（IC 卡）	4
MAC1	4

5.2.8.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表31描述了IC卡可能回送的错误状态。

表31 初始化圈存（INITIALIZE FOR LOAD）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不支持
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘03’	密钥索引不支持

5.2.9 初始化消费（INITIALIZE FOR PURCHASE）命令

5.2.9.1 定义和范围

初始化消费（INITIALIZE FOR PURCHASE）命令用于初始化消费交易。

5.2.9.2 命令报文

初始化消费（INITIALIZE FOR PURCHASE）命令报文见表32。

表32 初始化消费（INITIALIZE FOR PURCHASE）命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘01’
P2	‘01’或‘02’：‘01’用于电子存折，‘02’用于电子钱包，其他值预留
L_c	‘0B’
Data	见表 33
L_e	‘0F’

5.2.9.3 命令报文数据域

表33定义了命令报文的数据域。

表33 初始化消费（INITIALIZE FOR PURCHASE）命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

5.2.9.4 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。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表34 初始化消费（INITIALIZE FOR PURCHASE）响应报文数据域

说明	长度（字节）
ED 或 EP 余额	4
ED 脱机交易序号或 EP 脱机交易序号	2
透支限额	3
密钥版本号（DPK）	1
算法标识（DPK）	1
伪随机数（IC 卡）	4

5.2.9.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表35描述了IC卡可能回送的错误状态。

表35 初始化消费（INITIALIZE FOR PURCHASE）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持

5.2.10 初始化圈提（INITIALIZE FOR UNLOAD）命令

5.2.10.1 定义和范围

初始化圈提（INITIALIZE FOR UNLOAD）命令用于初始化圈提交易。

5.2.10.2 命令报文

初始化圈提（INITIALIZE FOR UNLOAD）命令报文见表36。

表36 初始化圈提（INITIALIZE FOR UNLOAD）命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘05’
P2	‘01’用于电子存折圈提交易，其他值预留
L_c	‘0B’

Data	见表 37
L_e	‘10’

5.2.10.3 命令报文数据域

表37定义了命令报文的数据域。

表37 初始化圈提（INITIALIZE FOR UNLOAD）命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

5.2.10.4 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。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表38 初始化圈提（INITIALIZE FOR UNLOAD）响应报文数据域

说明	长度（字节）
ED 余额	4
ED 联机交易序号	2
密钥版本号（DULK）	1
算法标识（DULK）	1
伪随机数（IC 卡）	4
MAC1	4

5.2.10.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表39描述了IC卡可能回送的错误状态。

表39 初始化圈提（INITIALIZE FOR UNLOAD）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持

5.2.11 修改初始化（INITIALIZE FOR UPDATE）命令

5.2.11.1 定义和范围

INITIALIZE FOR UPDATE命令用于初始化修改透支限额交易。

5.2.11.2 命令报文

INITIALIZE FOR UPDATE命令报文见表40。

表40 修改初始化（INITIALIZE FOR UPDATE）命令报文

代码	值
CLA	‘80’

INS	‘50’
P1	‘04’
P2	‘01’
L_c	‘07’
Data	见表 41
L_e	‘13’

5.2.11.3 命令报文数据域

表41定义了命令报文的数据域。

表41 修改初始化（INITIALIZE FOR UPDATE）命令报文数据域

说明	长度（字节）
密钥索引号	1
终端机编号	6

5.2.11.4 响应报文数据域

命令执行成功的响应报文数据域见表42。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表42 修改初始化（INITIALIZE FOR UPDATE）响应报文数据域

说明	长度（字节）
ED 余额	4
ED 联机交易序号	2
原透支限额	3
密钥版本号（DUK）	1
算法标识（DUK）	1
伪随机数（IC 卡）	4
MAC1	4

5.2.11.5 响应报文的状态字

此命令执行成功的状态字是“9000”。

表43描述了IC卡可能回送的错误状态。

表43 修改初始化（INITIALIZE FOR UPDATE）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1 和 P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘03’	密钥索引不支持

5.2.12 重装个人识别码（RELOAD PIN）命令

5.2.12.1 定义和范围

重装个人识别码(RELOAD PIN)命令用于发卡方重新给持卡人产生一个新的PIN(可以与原PIN相同)。

重装个人识别码（RELOAD PIN）只能在拥有或能访问到重装PIN子密钥（DRPK）的发卡方终端（例如发卡方银行终端）上执行。

在成功执行重装个人识别码（RELOAD PIN）命令后，IC卡必须完成以下操作：

——PIN 尝试计数器复位。

——IC 卡的原 PIN 必须设置为新的 PIN 值。

命令中的PIN数据以明文传送。

RELOAD PIN命令连续执行三次失败后，应用将永久锁定。

5.2.12.2 命令报文

重装个人识别码（RELOAD PIN）命令报文见表 44。

表44 重装个人识别码（RELOAD PIN）命令报文

代码	值
CLA	‘80’
INS	‘5E’
P1	‘00’
P2	‘00’
L_c	‘06’～‘0A’
Data	见表 45
L_e	不存在

5.2.12.3 命令报文数据域

表45 重装个人识别码（RELOAD PIN）命令报文数据域

说明	长度（字节）
重装的 PIN 值	2-6
MAC	4

用DRPK左右8位字节进行异或运算后的结果按照附录B中描述的机制对新PIN值计算MAC。

5.2.12.4 响应报文数据域

响应报文的数据域不存在。

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”。

表46描述了IC卡可能回送的错误状态。

表46 重装个人识别码（RELOAD PIN）错误状态

SW1	SW2	含义
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘69’	‘88’	安全信息数据对象不正确
‘6A’	‘86’	P1 和 P2 参数不正确
‘6A’	‘88’	引用数据找不到
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用永久锁住

5.2.13 修改透支限额（UPDATE OVERDRAW LIMIT）命令

5.2.13.1 定义和范围

UPDATE OVERDRAW LIMIT命令用于修改透支限额交易。

5.2.13.2 命令报文

修改透支限额（UPDATE OVERDRAW LIMIT）命令报文见表47。

表47 修改透支限额（UPDATE OVERDRAW LIMIT）命令报文

代码	值
CLA	‘80’
INS	‘58’
P1	‘00’
P2	‘00’
L_c	‘0E’
Data	见表 48
L_e	‘04’

5.2.13.3 命令报文数据域

表48定义了命令报文的数据域。

表48 修改透支限额（UPDATE OVERDRAW LIMIT）命令报文数据域

说明	长度（字节）
新透支限额	3
交易日期（发卡方）	4
交易时间（发卡方）	3
MAC2	4

5.2.13.4 响应报文数据域

此命令执行成功的响应报文数据域见表49。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表49 修改透支限额（UPDATE OVERDRAW LIMIT）响应报文数据域

说明	长度（字节）
TAC	4

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”。

表50描述了IC卡可能回送的错误状态。

表50 修改透支限额（UPDATE OVERDRAW LIMIT）错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘00’	不能处理
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

5.3 安全

所有在JR/T 0025.1中描述的安全要求适用于ED/EP应用。

5.3.1 密钥管理概述

所有涉及到资金划转或修改IC卡中敏感数据的交易，必须使用加密密钥来保证应用的安全性。

金融IC卡的密钥管理采用部分集中管理方式（全部集中也可以），即发卡单位（指总行）将密钥分发给所辖发卡方。

ED/EP应用中IC卡和PSAM之间的密钥关系在附录B中进行了详细描述。

对于使用初始化命令的交易，密钥索引号包含在初始化命令报文中。IC卡收到初始化命令后，使用命令中所给的密钥索引号找到卡中的相应密钥进行运算。

过程密钥（Session keys）只用于交易的特定阶段。交易类型不同决定了产生过程密钥的输入数据和密钥也不同。附录B描述了ED/EP应用所用的过程密钥的产生方式。

5.3.2 密钥管理

IC卡上的密钥必须安全存储。

表51描述了存储在IC卡上共用于电子存折和电子钱包应用的密钥。只用于电子存折应用的密钥见表52。

表51 IC卡中存储的共用于电子存折和电子钱包应用的密钥

密钥	意义	用途
DPK	消费/取现密钥。发卡方基于ED/EP的应用序列号产生的一个双倍长密钥。	用来产生消费/取现交易中使用的过程密钥（SESPK）。
DLK	圈存密钥。发卡方基于EP/EP的应用序列号产生的一个双倍长密钥。	用来产生圈存交易中使用的过程密钥（SESLK）。
DTK	TAC密钥。发卡方基于ED/EP的应用序列号产生的一个双倍长密钥。	用来产生消费、取现和圈存交易中使用的TAC。
DPUK	PIN解锁密钥。发卡方基于ED/EP应用序列号产生的一个双字节密钥。	应用产生解锁PIN命令的MAC。
DRPK	重装PIN密钥。发卡方基于应用序列号产生的一个双字节密钥。	用于产生重装PIN命令的MAC。
DAMK	应用维护密钥。发卡方基于应用序列号产生的一个双字节密钥。	用于产生应用锁定、应用解锁、卡片锁定和更新二进制命令的MAC。

表52 IC卡中用于电子存折应用的密钥

密钥	意义	用途
DULK	圈提密钥。发卡方基于ED的应用序列号产生的一个双倍长密钥。	用来产生圈提交易中使用的过程密钥（SESULK）.
DUK	更新密钥。发卡基于ED的应用序列号产生的一个双倍长密钥。	用来产生修改透支限额交易中使用的过程密钥（SESUK）

5.4 终端

支持电子存折/电子钱包应用的终端必须符合JR/T 0025.1和JR/T 0025.3的规定。它应支持JR/T 0025.1和本部分所定义的电子存折/电子钱包应用的所有文件和命令。

支持电子存折/电子钱包应用的终端必须支持用于输入个人识别码PIN的密码键盘。

支持电子存折/电子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存折/电子钱包余额和/或交易明细的终端(如手持终端)。

5.5 交易流程

本条描述了电子存折/电子钱包应用的交易流程。该流程描述的是卡片插入终端并与终端相互作用后，所进行的交易处理过程。

消费或取现交易要求终端必须具有安全存取模块（PSAM）。本部分假定终端和PSAM之间是以安全方式进行通信的，因此不定义任何与PSAM通信相关的命令一响应对。

5.5.1 交易预处理

图1给出了对电子存折/电子钱包应用的所有交易类型共有的预处理流程。

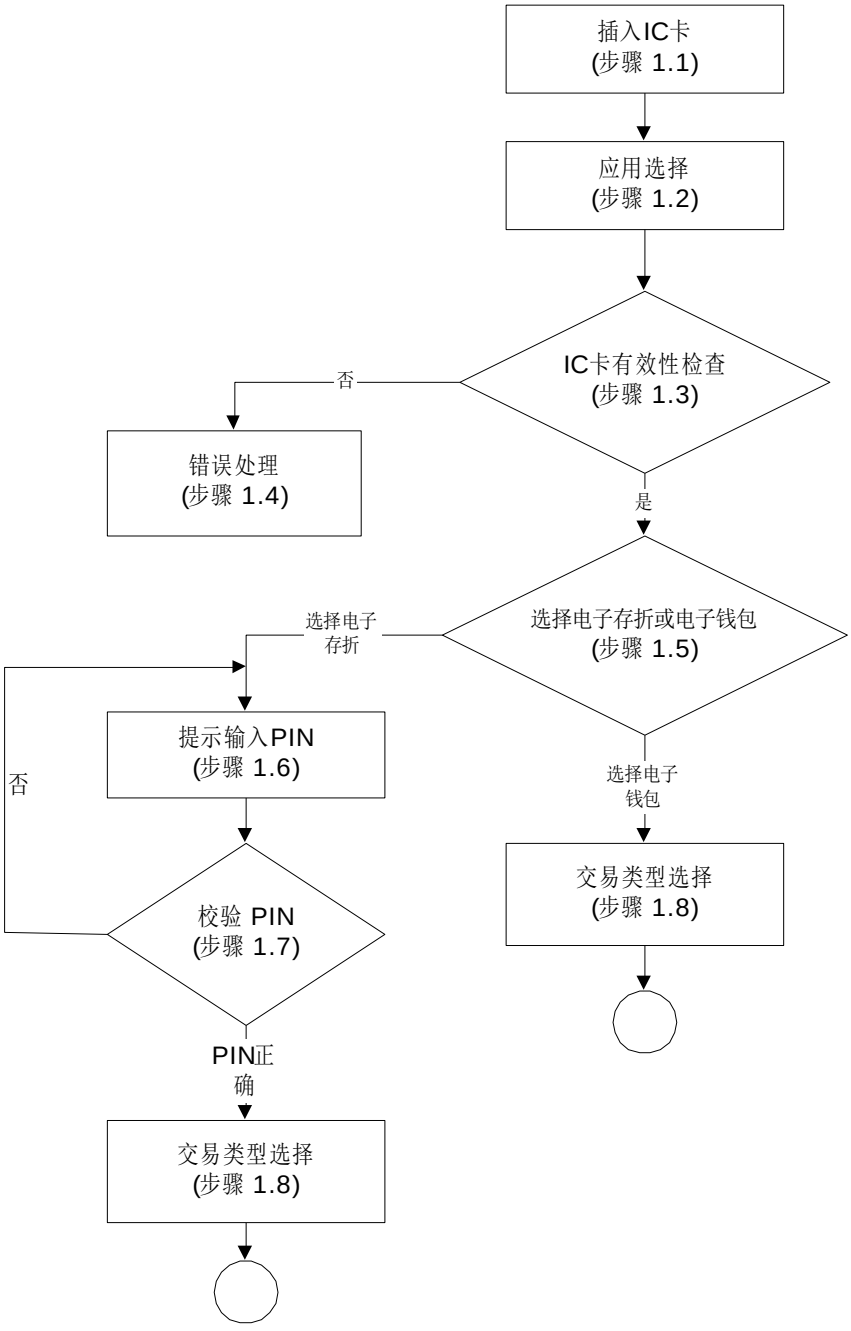


图1 交易预处理流程

5.5.1.1 插入 IC 卡（步骤 1.1）

终端应具有检测IC卡是否已经插入读卡器的功能。如果IC卡已经插入，终端将继续执行5.5.1.2的应用选择功能。

5.5.1.2 应用选择（步骤 1.2）

应用选择的执行过程见JR/T 0025.1的“应用选择”部分。电子存折/电子钱包应用的应用标识符（AID）将由全国金融标准化技术委员会负责分配和维护。

成功地选择了电子存折/电子钱包应用后，IC卡回送包含发卡方专用数据在内的文件控制信息。表53定义了此应用必备的发卡方专用数据。

表53 FCI 发卡方专用数据

数据字段的描述	长度（字节）
发卡方标识符	8
应用类型标识	1
发卡方应用版本号	1
应用序列号	10
应用启用日期	4
应用有效日期	4
发卡方自定义 FCI 数据	2

应用类型标识（ATI）在应用选择时由IC卡回送给终端。它标明电子存折和电子钱包应用在卡上的存在情况。

5.5.1.3 IC 卡有效性检查（步骤 1.3）

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[3]卡之列（使用发卡方标识和应用序列号）；

——终端是否支持该发卡方标识符；

——终端是否支持 IC 卡上的应用[使用应用类型标识（ATI）来检查]；

——终端是否支持从 IC 卡应用选择时返回的标签为‘9F08’的应用版本号所代表的应用版本，当前的版本号为 0x02；

——应用是否在有效期内。

如果以上任一条件不满足，交易将按5.5.1.4中的描述进行。

5.5.1.4 错误处理（步骤 1.4）

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。

5.5.1.5 选择电子存折或电子钱包（步骤 1.5）

终端根据应用选择时获得的应用类型标识判别IC卡支持ED、EP的情况。

如果IC卡和终端只同时支持ED或EP之一，则终端将自动地选择到ED或EP，继而进行5.5.1.6或5.5.1.8中所描述的步骤。

如果IC卡仅支持一种应用并且该应用不被终端支持，则该过程终止。

如果IC卡和终端彼此都支持ED和EP两种应用，终端应向持卡人提供选择ED或EP的过程，在这一过程中持卡人可以从中选择一种应用进行交易。

5.5.1.6 提示输入个人识别码（PIN）（步骤 1.6）

如果如5.5.1.5描述的选择了电子存折，终端将提示持卡人输入PIN。

5.5.1.7 校验 PIN（步骤 1.7）

持卡人输入PIN后，终端将使用VERIFY命令来校验持卡人输入的PIN是否正确。VERIFY命令在JR/T 0025.1的“文件和命令”部分定义。

当IC卡收到校验（VERIFY）命令后，它将进行以下操作：

——检查 PIN 尝试计数器。如果 PIN 尝试计数器为零，此时 PIN 已锁定，因此不执行该命令。这种情况下，IC 卡回送状态字“6983”（认证方式锁定）结束交易过程；

[3]黑名单的详细情况，包括维护、格式、内容不在本部分的范围之内。

——如果 PIN 没有被锁定，则将命令数据中的 PIN 和 IC 卡中存放的 PIN 进行比较；

——如果以上两个 PIN 相同，IC 卡将 PIN 尝试计数器置为允许 PIN 重试的最大次数并回送状态字“9000”。IC 卡必须记住 PIN 成功验证的结果，直到断电或选择了其他应用。交易处理按 5.5.1.8 中的描述继续进行；

——如果以上两个 PIN 不同，IC 卡将 PIN 尝试计数器减 1 并回送状态字“63Cx”，这里’x’是 PIN 尝试计数器的新值。在这种情况下，终端将检查 x 的值。如果 x 是零，将终止交易，且卡片自动锁定 PIN。否则，终端将提示重新输入 PIN 并重复以上过程。

如果持卡人输入的PIN正确，IC卡必须记住PIN成功验证的结果，直到断电、卡片复位、PIN再次验证错误或选择了其他应用。验证正确后，交易流程执行5.5.1.8中的步骤。

5.5.1.8 交易类型选择（步骤 1.8）

终端应该具备让持卡人选择交易类型的功能。每次交易最多只能选择一种交易类型。

对电子存折应用来说，持卡人应能选择如下交易类型：圈存、圈提、消费、取现、修改透支限额、查询余额、查询明细。

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。

5.5.2 圈存交易

通过圈存交易，持卡人可将其在银行相应账户上的资金划入电子存折或电子钱包中。这种交易必须在金融终端上联机进行并要求提交个人识别码（PIN）（无论电子存折还是电子钱包应用）。

5.5.2.1 发出初始化圈存（INITIALIZE FOR LOAD）命令（步骤 2.1）

终端应按5.2.8中的描述发出初始化圈存（INITIALIZE FOR LOAD命）令启动圈存交易。

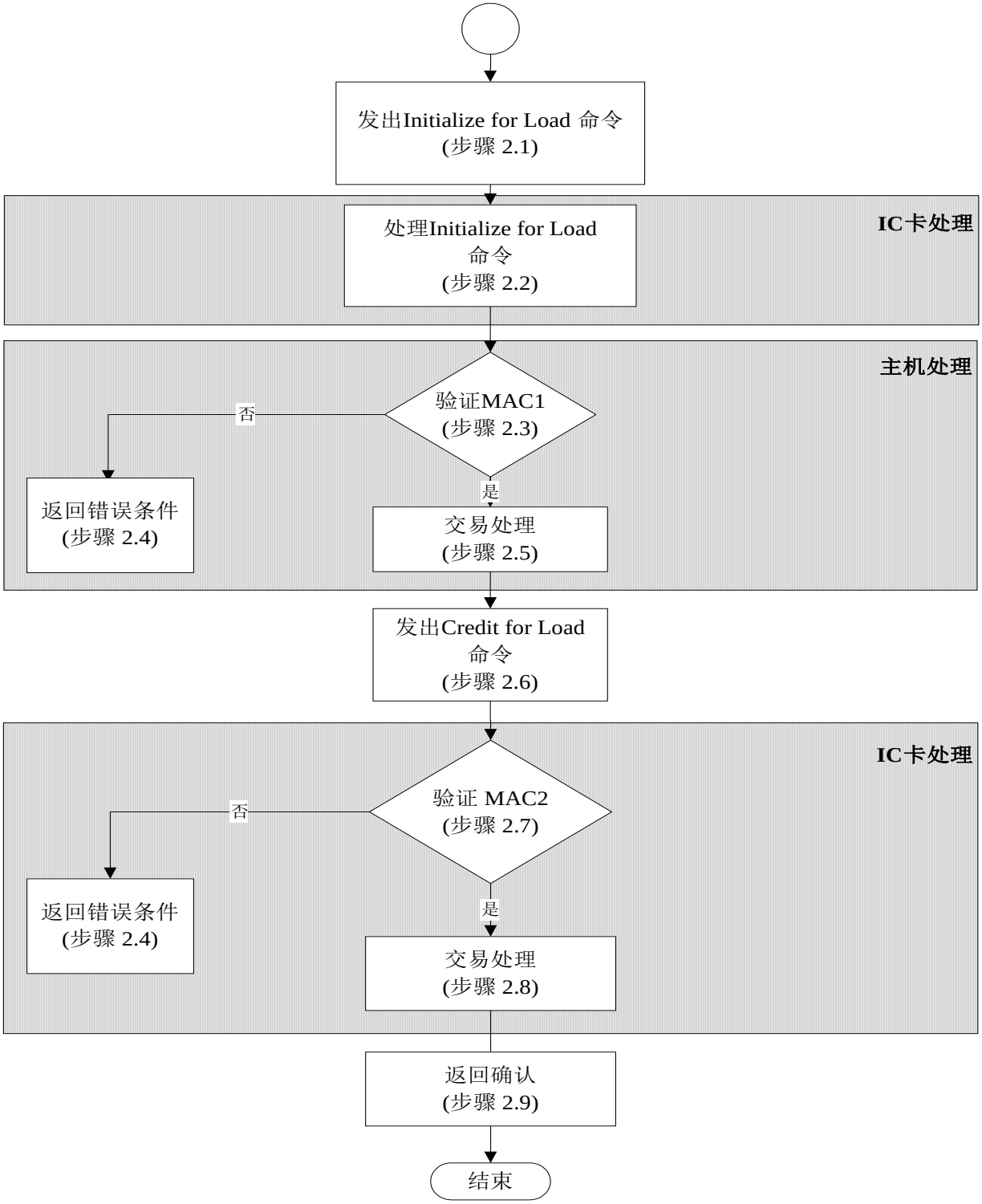


图2 圈存交易处理流程

5.5.2.2 处理初始化圈存（INITIALIZE FOR LOAD）命令（步骤 2.2）

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 SESLK 和一个报文签别码（MAC1），用以供主机验证圈存交易及 IC 卡的合法性。

SESLK是用于电子存折或电子钱包圈存交易的过程密钥。该过程密钥是用DLK密钥按照附录B描述的机制产生的。用来产生过程密钥SESLK的输入数据如下：

SESLK：伪随机数（ICC）‖电子存折联机交易序号或电子钱包联机交易序号‖“8000”

MAC1的计算机制见附录B。用SESLK对以下数据加密产生MAC1（按所列顺序）：

——电子存折余额（交易前）或者电子钱包余额（交易前）；

——交易金额；

——交易类型标识；

——终端机编号。

IC卡将把5.2.8.4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。

5.5.2.3 验证 MAC1（步骤 2.3）

收到初始化圈存（INITIALIZE FOR LOAD）命令响应报文后，终端把表30[4]定义的数据传给发卡方主机。主机将生成SESLK并确认MAC1是否有效。如果MAC1有效，交易处理将按5.5.2.5中描述的步骤继续执行。否则，交易处理将执行5.5.2.4中所描述的步骤。

5.5.2.4 回送错误状态（步骤 2.4）

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。

5.5.2.5 交易处理（步骤 2.5）

在确认能够进行圈存交易后，主机从持卡人在银行的相应账户中扣减圈存金额。

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。附录B中描述了主机用来生成MAC2的机制。用SESLK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，主机将电子存折联机交易序号或电子钱包联机交易序号加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）。

5.5.2.6 发出圈存（CREDIT FOR LOAD）命令（步骤 2.6）

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）命令更新卡上电子存折或电子钱包余额。圈存（CREDIT FOR LOAD）命令见5.2.2中的描述。

5.5.2.7 验证 MAC2（步骤 2.7）

收到圈存（CREDIT FOR LOAD）命令后，IC卡必须确认MAC2的有效性。如果MAC2有效，交易处理将执行5.5.2.8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。

5.5.2.8 交易处理（步骤 2.8）

IC卡将电子存折联机交易序号或电子钱包联机交易序号加1，并且把交易金额加在电子存折或电子钱包的余额上。IC卡必须成功地完成以上所有操作或者一个也不完成。

在电子存折圈存交易或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：

——电子存折联机交易序号或电子钱包联机交易序号；

——交易金额；

——交易类型标识；

[4]包含在圈存认证请求报文中的其他信息不在本部分的范围内。

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

TAC的计算机制见附录B。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）：

——电子存折余额（交易后）或电子钱包余额（交易后）；

——电子存折联机交易序号（加 1 前）或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）。

5.5.2.9 返回确认（步骤 2.9）

在成功完成步骤2.8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。

5.5.3 圈提交易

通过圈提交易，持卡人可以把电子存折中的部分或全部资金划回到其在银行的相应账户上。这种交易必须在金融终端上联机进行并要求提交个人识别码（PIN）。只有电子存折应用支持圈提交易。

5.5.3.1 发出初始化圈提（INITIALIZE FOR UNLOAD）命令（步骤 3.1）

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

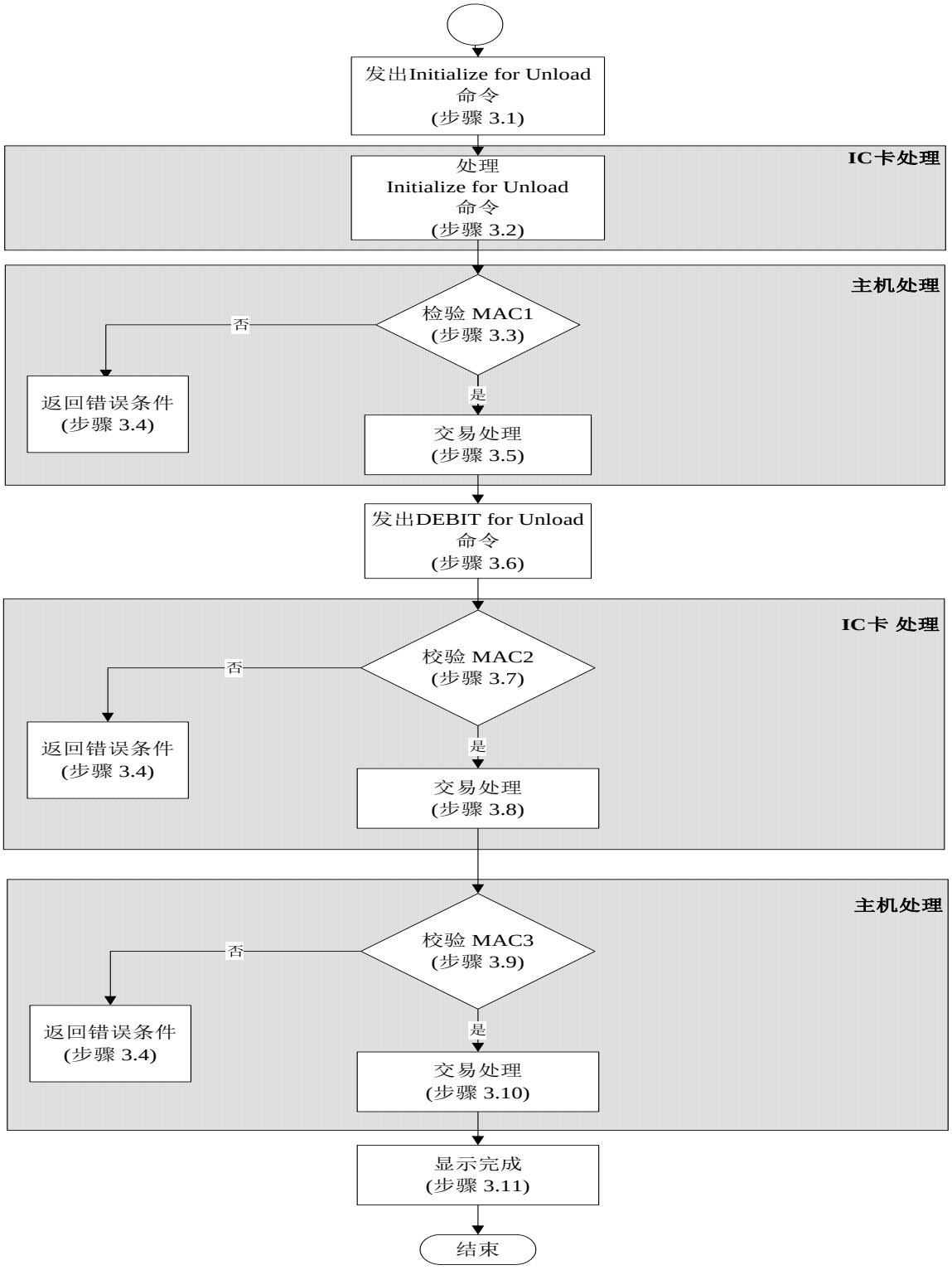


图3 圈提交易处理流程

5.5.3.2 处理初始化圈提（INITIALIZE FOR UNLOAD）命令（步骤 3.2）

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存折余额。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和一个报文签别码（MAC1），供主机验证圈提交易及IC卡的合法性。

SESULK是用于电子存折圈提交易的过程密钥。该过程密钥是利用DULK并按照附录B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）‖电子存折联机交易序号‖“8000”

MAC1的计算机制见附录B。用SESULK对以下数据加密产生MAC1（按所列顺序）：

——电子存折余额（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5.2.10.4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，终端将一个包含表38数据的圈提许可请求报文MAC1送往发卡方主机。

5.5.3.3 验证 MAC1（步骤 3.3）

主机将产生SESULK并验证MAC1是否有效。如果MAC1有效，将执行5.5.3.5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5.5.3.4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。

5.5.3.4 回送错误状态（步骤 3.4）

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。

5.5.3.5 主机处理（步骤 3.5）

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的计算机制见附录B。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。

5.5.3.6 发出圈提（DEBIT FOR UNLOAD）命令（步骤 3.6）

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存折余额。圈提（DEBIT FOR UNLOAD）命令见5.2.4。

5.5.3.7 验证 MAC2（步骤 3.7）

IC卡必须确认MAC2是有效的。如果MAC2有效，交易处理将执行5.5.3.8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。

5.5.3.8 交易处理（步骤 3.8）

IC卡将电子存折联机交易序号加1，并从卡上的电子存折余额中扣减交易金额。IC卡必须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）：

——电子存折余额（交易后）；

——电子存折联机交易序号（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）。

IC卡用以下数据组成的一个记录更新交易明细：

——电子存折联机交易序号；

——交易金额；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

5.5.3.9 验证 MAC3（步骤 3.9）

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5.5.3.10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。

5.5.3.10 交易处理（步骤 3.10）

发卡方主机将交易金额加在持卡人的相应银行账户上，并将主机的电子存折联机交易序号加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。

5.5.3.11 显示完成（步骤 3.11）

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。

5.5.4 消费交易

消费交易[5]允许持卡人使用电子存折或电子钱包的余额进行购物或获取服务。此交易可以在销售点终端（POS）上脱机进行。使用电子存折进行的消费交易必须提交个人识别码（PIN），使用电子钱包则不需要。

[5]本部分仅提供脱机交易流程。

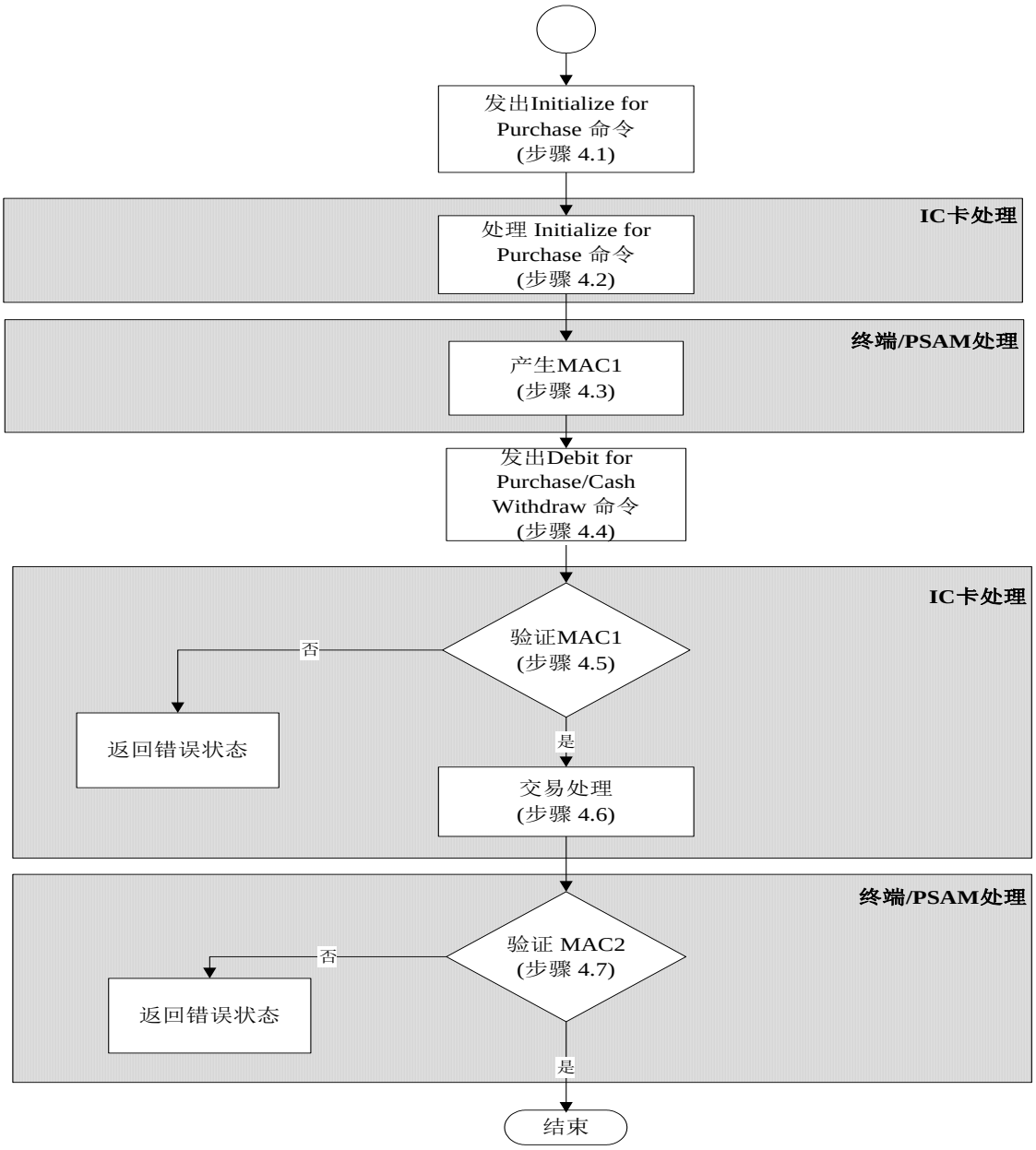


图4 消费交易处理流程

5.5.4.1 发出初始化消费（INITIALIZE FOR PURCHASE）命令（步骤 4.1）

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

5.5.4.2 处理初始化消费（INITIALIZE FOR PURCHASE）命令（步骤 4.2）

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；

——检查电子存折余额或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5.5.4.5中生成过程密钥并验证MAC1。过程密钥是利用DPK并按照附录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）‖电子存折脱机交易序号或电子钱包脱机交易序号‖终端交易序号的最右两个字节

5.5.4.3 产生 MAC1（步骤 4.3）

使用伪随机数（ICC）和IC卡回送的电子存折脱机交易序号或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的计算机制见附录B。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）。

5.5.4.4 发出消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令（步骤 4.4）

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

5.5.4.5 验证 MAC1（步骤 4.5）

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5.5.4.6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。

5.5.4.6 交易处理（步骤 4.6）

IC卡从电子存折余额或电子钱包余额中扣减消费的金额，并将电子存折或电子钱包脱机交易序号加1。IC卡必须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PSAM对其进行合法性检查，并通过DEBIT FOR PURCHASE/CASH WITHDRAW命令的响应报文回送终端。MAC2的计算机制见附录B。用SESPK对以下数据进行加密产生MAC2：

——交易金额。

IC卡按照附录B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/CASH WITHDRAW）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）。

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

——电子存折脱机交易序号或电子钱包脱机交易序号；

——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）。

5.5.4.7 验证 MAC2（步骤 4.7）

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。终端应采取的相应措施不在本部分的范围之内。

5.5.5 取现交易

取现交易[6]允许持卡人从电子存折中提取现金。此交易必须在金融终端上进行，但可以脱机处理。只有电子存折应用支持此交易，且必须提交个人识别码PIN。

5.5.5.1 发出初始化取现（INITIALIZE FOR CASH WITHDRAW）命令（步骤 5.1）

终端发出初始化取现（INITIALIZE FOR CASH WITHDRAW）命令启动取现交易。

5.5.5.2 处理初始化取现（INITIALIZE FOR CASH WITHDRAW）（步骤 5.2）

收到初始化取现（INITIALIZE FOR CASH WITHDRAW）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），但不回送其他数据。

——检查 ED 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），但不回送其它数据。终端采取的措施不在本部分范围内。

对以上错误状态终端的处理不在本部分的范围内。

通过以上检查之后，IC卡将产生一个伪随机数并在5.5.5.5中生成过程密钥并验证MAC1。过程密钥是利用DPK并按照附录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）||电子存折脱机交易序号||终端交易序号的最右边两个字节

5.5.5.3 验证 MAC1（步骤 5.3）

验证了交易金额有效之后，终端使用伪随机数（ICC）和IC卡回送的电子存折脱机交易序号产生相同的过程密钥（SESPK）和报文鉴别码（MAC1），供IC卡验证PSAM的合法性。

MAC1的计算机制见附录B。用SESPK对以下数据加密产生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）。

[6]本部分仅提供脱机交易流程。

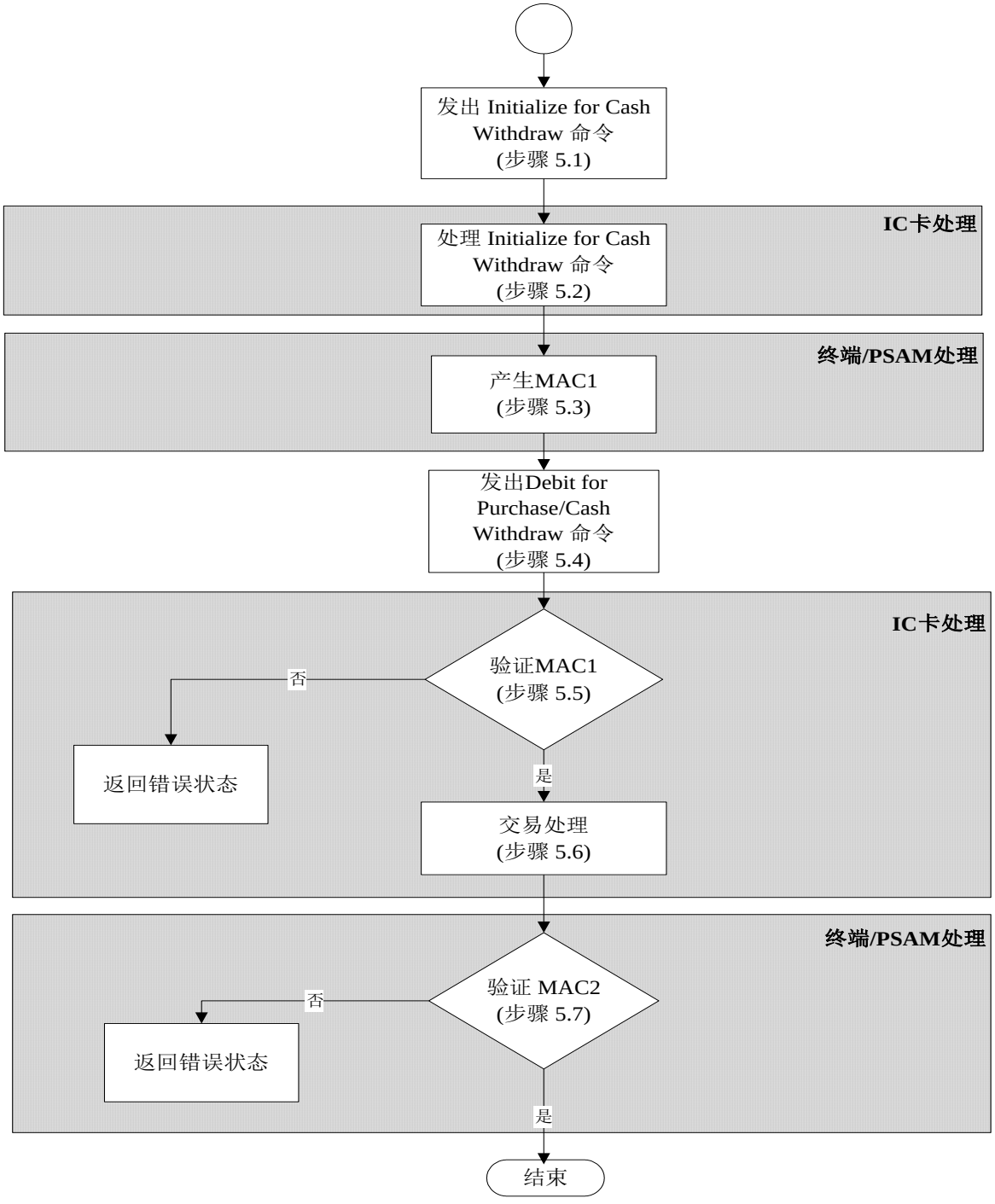


图5 取现交易处理流程

5.5.5.4 发出消费/取现（DEBIT FOR PURCHASE/CASH WITHDRAW）命令（步骤 5.4）

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

5.5.5.5 验证 MAC1（步骤 5.5）

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，交易处理会继续执行5.5.5.6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以内。

5.5.5.6 交易处理（步骤 5.6）

IC卡从卡上的电子存折余额中扣减取现交易金额，并将电子存折脱机交易序号加1。IC卡必须成功地完成以上所有步骤或者一个也不完成，如果余额或序号的更新没有成功，交易明细也不应被更新。

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

—— 交易金额。

IC卡按照附录B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/CASH WITHDRAW）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）。

IC卡将用以下数据组成的一个记录更新IC卡交易明细。

——电子存折脱机交易序号；

——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）。

5.5.5.7 验证 MAC2（步骤 5.7）

在收到IC卡（经过终端）传来的MAC2后，PSAM将验证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。

5.5.6 修改透支限额交易

“透支功能”是本部分从技术上支持的一种基于电子存折应用的有限信用功能。当电子存折中的实际金额不足时，它为持卡人提供了一种在发卡方所允许的透支额度内继续进行交易的方便性。修改透支限额交易必须在金融终端上联机进行，且必须提交个人识别码（PIN）。

是否使用“透支功能”以及允许透支的额度由发卡方决定。修改透支限额交易的具体业务作法和要求不在本部分的范围之内。

如果透支限额存在，电子存折的余额是实际圈存余额与透支限额之和。

5.5.6.1 发出初始化修改透支现额（INITIALIZE FOR UPDATE）命令（步骤 6.1）

终端发出初始化修改透支现额（INITIALIZE FOR UPDATE）命令启动修改透支限额交易。

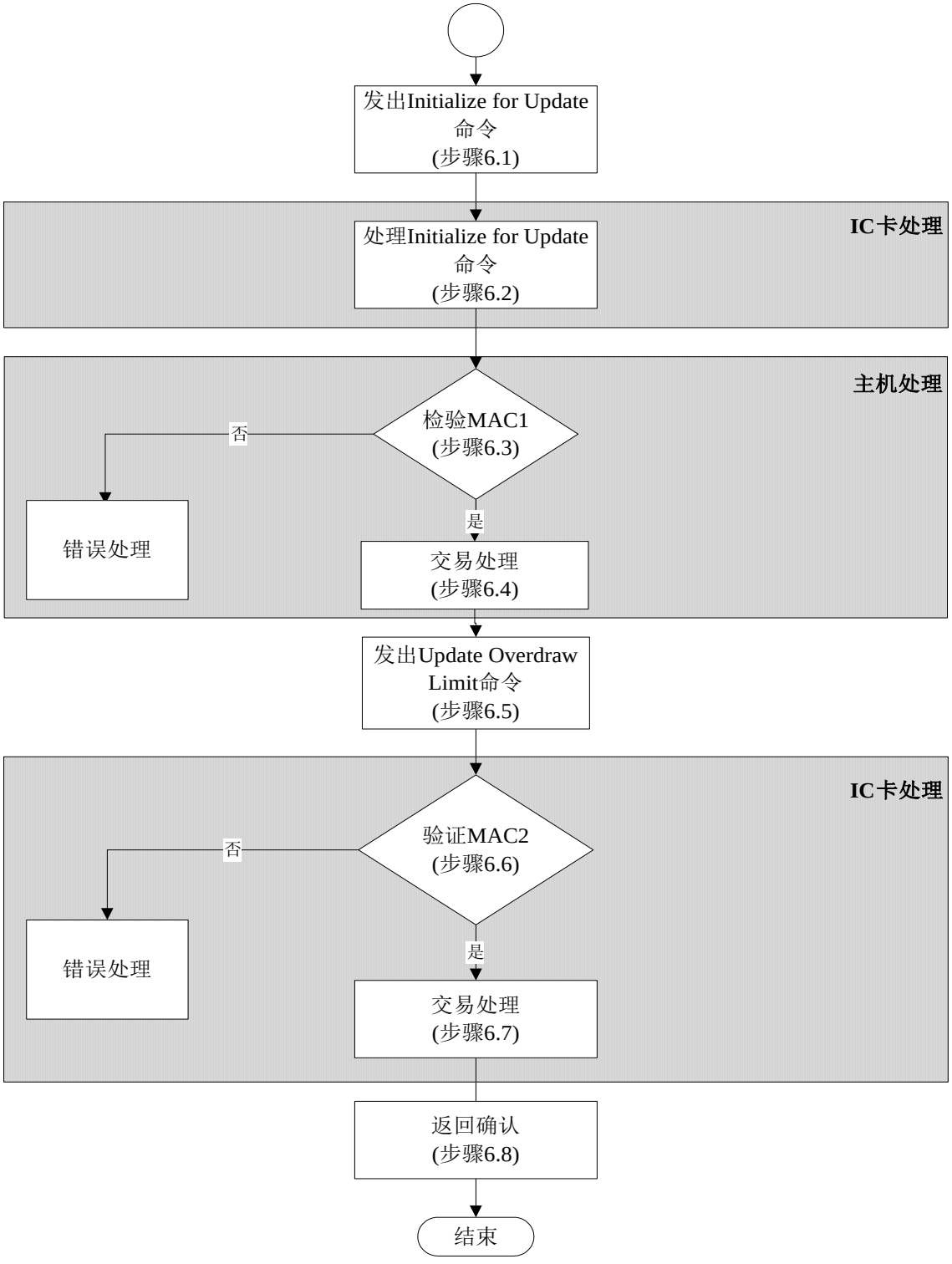


图6 修改透支限额交易

5.5.6.2 处理初始化修改透支现额（INITIALIZE FOR UPDATE）命令（步骤 6.2）

收到初始化修改透支现额（INITIALIZE FOR UPDATE）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）但不回送其他数据。

终端对以上错误所做的处理不在本部分的范围以内。

在通过了以上检查之后，IC卡将产生一个伪随机数（ICC）、一个过程密钥SESUK和一个报文鉴别码（MAC1）。该过程密钥是利用DUK并按附录B描述的机制产生的。用于产生过程密钥的输入数据如下：

SESUK：伪随机数（ICC）‖电子存折联机交易序号‖“8000”

MAC1按照附录B描述的机制产生。用SESUK对以下数据加密产生MAC1（按所列顺序）：

——电子存折余额（交易前）；

——透支限额（交易前）；

——交易类型标识；

——终端机编号。

5.5.6.3 处理初始化修改透支现额（INITIALIZE FOR UPDATE）命令（步骤 6.3）

在收到初始化修改透支现额（INITIALIZE FOR UPDATE）命令执行成功的响应报文后，终端应向主机传送表42定义的数据以及其它主机需要的数据以便于验证MAC1。

5.5.6.4 验证 MAC1（步骤 6.4）

利用步骤6.3中终端传来的报文，主机将产生与IC卡相同的过程密钥（SESUK）来验证MAC1。

如果MAC1有效，交易处理将执行5.5.6.5中所描述的步骤。否则，主机应通过终端回送错误状态字。终端针对错误状态所做的处理不在本部分范围以内。

5.5.6.5 主机处理（步骤 6.5）

假定主机已经知道IC卡的透支限额。

基于MAC1（或者其他由主机决定的验证标准）验证的结果，主机将决定是否允许修改透支限额。。

如果主机拒绝交易，则应向终端发送一个拒绝报文，结束交易处理。

如果主机允许交易，则应生成一个报文签别码（MAC2），以供IC卡对主机合法性进行检查。

MAC2的计算机制见附录B。用SESUK对以下数据加密产生MAC2（按所列顺序）：

——透支限额（交易后）；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

主机将电子存折联机交易序号加1。

主机应向终端发送一个至少包括新透支限额、交易日期（主机）、交易时间（主机）和MAC2的许可信息。

5.5.6.6 发出修改透支现额（UPDATE OVERDRAWLIMIT）命令（步骤 6.6）

如果主机同意交易，终端将发出修改透支现额（UPDATE OVERDRAWLIMIT）命令。

5.5.6.7 验证 MAC2（步骤 6.7）

IC卡将验证MAC2的有效性。如果MAC2有效，交易处理将执行5.5.6.8中的步骤。否则向终端回送错误状态字“9302”（MAC无效）。终端对此错误状态所做的处理不在本部分范围之内。

5.5.6.8 交易处理（步骤 6.8）

IC卡将按照附录B中描述的机制，直接用密钥DTK左右8字节异或后的结果对以下数据加密产生一个TAC：

——电子存折余额（交易后）；

——电子存折联机交易序号（加 1 前）；

——电子存折透支限额（交易后）；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

将当前电子存折余额置为新的电子存折余额，更新透支限额并使电子存折联机交易序号加1。这三个修改必须全部完成，或一个也不完成。

IC卡通过响应报文将TAC和状态字“9000”传送给终端。

IC卡用以下数据组成的一个记录更新交易明细：

——电子存折联机交易序号；

——透支限额；

——交易类型标识；

——终端机编号；

——交易日期（主机）；

——交易时间（主机）。

5.5.6.9 回送确认（步骤5.9）

IC卡在修改透支现额（UPDATE OVERDRAWLIMIT）命令的响应报文中回送TAC和一个完成码，表明透支限额已经被成功更新。

5.5.7 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存折中的余额。此交易一般脱机进行。在电子存折应用中进行此交易必须提交个人识别码（PIN）。电子钱包则不需要。

终端利用查询余额（GET BALANCE）命令实现查询余额交易。

5.5.8 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。交易时需提交个人识别码（PIN）。

终端发出一个READ RECORD命令（符合JR/T 0025.1中“文件和命令”部分的规定）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、电子存折圈存交易、电子存折圈提交易、电子存折消费交易、电子钱包消费交易（可选）、电子存折取现交易、电子存折修改透支限额交易。

5.5.9 应用维护功能

以下交易必须在拥有相应密钥的设备上执行。

5.5.9.1 安全报文

电子存折/电子钱包应用涉及到的安全机制，应按照JR/T 0025.1第8章“安全机制”部分的规定进行，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JR/T 0025.1第6章“文件和命令”）。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，用以代替JR/T 0025.1中定义的初始化值。

——不采用过程密钥。除去PIN UNBLOCK命令外，均使用导出的应用维护密钥（DAMK）来计算MAC。PIN UNBLOCK命令采用导出的PIN解锁密钥来产生MAC。

——全部采用双字节密钥的3DEA算法。

5.5.9.2 卡片锁定

终端发出卡片锁定（CARD BLOCK）命令来锁定卡片。

此命令参照JR/T 0025.1第6章“文件和命令”部分。其安全机制在5.5.9.1中描述。命令的成功执行使得IC卡中的所有应用无效。在这种情况下，进行应用选择将会回送状态字“6A81”（功能不被支持）。

5.5.9.3 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JR/T 0025.1的“文件和命令”部分。其安全机制在5.5.9.1中描述。在本部分所述的应用中，命令的成功执行导致IC卡中的电子存折/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）：

a） 当用 SELECT 命令选择此应用或其他应用时；

b） 产生随机数（GET CHALLANGE）命令；

c） 应用锁定（APPLICATION BLOCK）命令；

d） 卡片锁定 （CARD BOLCK）命令；

e） 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存折联机交易序号和电子钱包联机交易序号的值。

5.5.9.4 应用解锁

终端发出应用解锁（APPLICATION UNBLOCK）命令来对应用解锁，详细定义见JR/T 0025.1，安全机制见5.5.9.1。

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存折联机交易序号和电子钱包联机交易序号的值。

5.5.9.5 PIN 解锁

终端发出PIN解锁（PIN UNBLOCK）命令对PIN解锁见JR/T 0025.1，安全报文见5.5.9.1。

在命令报文中，P2取‘00’值。使用DPUK对PIN数据加密（见JR/T 0025.1第8章“安全机制”）。

如果PIN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）。

5.5.9.6 二进制形式修改

终端按照JR/T 0025.1和5.5.9.1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）。

5.5.9.7 更改 PIN

更改PIN功能不需要MAC，它可以在任意支持该命令的终端上执行。

当IC卡接到此命令时，将进行以下操作：

——检查 PIN 尝试计数器。如果为 0，表明 PIN 已锁定，此命令不能执行。在这种情况下，IC 卡回送状态字“6983”（认证方式锁定）。

——如果 PIN 没有锁定，则命令中的“当前 PIN”会和 IC 卡上存放的 PIN 比较。

如果二者相同，IC卡将进行以下操作：

a） 将 IC 卡上的 PIN 改为命令中的新 PIN；

b） 将 PIN 尝试计数器置为 PIN 重试的最大次数。

——如果卡上的 PIN 和命令中的“当前 PIN”并不相同，IC 卡将进行以下操作：

a） 将 PIN 尝试计数器减 1；

b） 回送状态字“63Cx”，这里 x 是 PIN 尝试计数器的新值。如达到零，则卡片自动锁定 PIN。

5.5.9.8 重装 PIN

终端按照5.2.12条中的描述发出重装个人识别码（RELOAD PIN）命令来重装PIN。

按照附录B中描述的机制用密钥DRPK来产生一个MAC。

当此命令失败三次之后，应用被永久锁定。

5.6 防拔

卡片必须能够在交易处理中的任何情况下，甚至是在更新EEPROM过程中掉电的情况下，保持数据的完整性。这就需要在每次更新数据前对数据进行备份，并且在重新加电后自动地触发恢复机制。

在终端发给IC卡一个命令以更新电子存折余额或电子钱包余额时，卡片总会回送一个MAC或/和TAC，以证明更新已经发生。这样的情况有圈存（TAC），圈提（MAC3）、消费/取现（TAC）和修改透支限额（TAC）。

IC卡必须在更新余额前计算MAC或/和TAC，一旦余额更新成功，必须保证可以通过GET TRANSCTION PROVE命令获得此MAC或/和TAC。如果防拔恢复已使余额恢复到更新前的数值，那么有关的加密数据不必再保留。接到更改ED或EP余额的命令，如Debit、Credit命令时，这些加密数据可能被丢弃。

如果在命令已执行结束，而终端还未收到响应之前，卡片突然拔出，终端将会处于不知卡片是否更新的不定状态。这种情况下，终端应负责用GET TRANSACTION PROVE命令进行恢复。

如果卡片正在处理时被突然拔出，终端应提醒持卡人重新插入卡片。之后终端将检查发卡方标识和应用序列号以确认插入的卡片和前面拔出的卡片是否同一张卡。如果是同一张卡，终端发出取交易认证（GET TRANSACTION PROVE）命令。假如MAC或/和TAC返回，终端即完成交易处理；如果MAC或/和TAC无法回送，则说明IC卡中的余额没有被修改。交易可以用适当的初始化命令重新开始。

6 磁条卡功能

6.1 卡片和终端要求

卡片和终端磁条卡功能（Easy Entry）的主要技术特点如下：

——符合 JR/T 0025.3 中的电气物理特性、传输协议和复位应答要求；

——符合 JR/T 0025.3 中的应用选择要求；

——卡中存在一个由一条记录组成的卡片文件，该文件包括第二磁道数据；

——符合 JR/T 0025.3 中的数据编码定义；

——交易处理使用的报文格式与现行的磁条交易所使用的数据相同。

6.1.1 卡片要求

6.1.1.1 电气机械特性、传输协议

卡片应符合JR/T 0025.3中的电气机械要求，并支持T=0或T=1协议，也可以同时支持两种协议。

6.1.1.2 复位应答

卡片至少应该支持JR/T 0025.3定义的热复位。它还应支持JR/T 0025.3中定义的冷复位并可以支持特定的冷复位规范。对于特定应用的选择，卡片可以支持复位后的隐含选择，但这种隐含选择不适用于磁条卡功能（Easy Entry）。

6.1.1.3 应用选择

卡片必须支持JR/T 0025.1中定义的支付系统环境（PSE）选择和直接选择。

PSE目录必须至少包含一条磁条卡功能（Easy Entry）的记录，PSE目录包含应用标识符（AID）和应用标签。应用标签由发卡方定义，并应该明确标识出是否PBOC应用。对于PBOC应用，必须将AID和应用标签放在卡片目录中，对非PBOC应用建议将以上信息放在卡片目录中。

6.1.1.4 命令支持

即使IC卡仅仅支持磁条卡功能（Easy Entry）以及可能具有与JR/T 0025兼容但不符合的应用，IC卡也应当支持SELECT和READ RECORD命令。在SELECT命令的响应报文中，卡片回送的FCI所包含的应用优先级标识值为‘00’。

6.1.1.5 强制记录

如表54所示，磁条卡功能（Easy Entry）至少包含一个应用基本文件（AEF），这个应用基本文件至少包含一个记录，文件中与AEF相关的SFI应该是1。SFI的第一个记录（记录1）应该包含表54中所列的数据。发卡方可以增加更多的记录、数据和文件，但是这些数据不能存储在该文件记录1中。附加数据可以存储在SFI为1的AEF的后续记录中。

表 54 强制文件（记录 1，SFI1）

数据	状态	长度
2 磁道数据	M	可变长 19 字节
持卡人姓名	M	2-26 字节
3 磁道数据	O	可变长 52 字节

如果发卡方支持持卡人个人识别码（PIN），则发卡方必须能够修改磁条的PIN校验值（PVN），因此也应能修改磁道2等同数据的PVN。如果磁道2等同数据可能因为这个原因被修改，发卡方也必须确保SFI为1的AEF的记录1数据也能被修改，并且发卡方必须提供足够的安全措施以保证修改是在其控制和授权下进行的。非发卡方不能修改该记录。实际的处理过程是由发卡方自行决定的。这样的安全修改过程可能包含了使用卡中存放的密钥做校验的过程（由校验命令完成）。（卡片密钥的产生按照JR/T 0025.1描述的产生DEA密钥的方法进行）。

如果发卡方永远不允许修改PVN，那么SFI是1的AEF中的记录1必须通过存储权限来控制以确保其数据永不被修改。

磁道2等同数据必须包括以下磁道2数据（磁道2数据的定义符合GB/T 15120和GB/T 19584的要求）：

——主账号（PAN）、字段分隔符、有效期、服务码、卡片校验值（CVN）、PVN（如果目前磁条卡中存在）；

——发卡方自定义数据（如果目前磁条卡中存在）；

包含在磁道2等同数据域中的数据除如开始标识、结束标识和纵向冗余校验（LRC）外，其它数据应该与磁条的磁道2数据相同；

——如果 IC 卡是用整个持卡人姓名来加密的，那么持卡人姓名应与磁道 2 中持卡人姓名相同。否则，持卡人姓名必须包含一个空格，空格后面跟一个字符“\”。

6.1.2 终端需求

终端支持磁条卡功能（Easy Entry）的要求如下所述。

6.1.2.1 电气机械特性、传输协议

终端应符合JR/T 0025.3中规定的电气和机械要求，并支持T=0和T=1两种协议。

6.1.2.2 复位应答

终端应支持JR/T 0025.3所定义的热复位，并且能够接受一个不兼容的冷复位。对非PBOC应用，终端可以在复位后为支持一个隐含的选择。

IC卡插入终端后，终端应该执行一个按照JR/T 0025.3规定的冷复位，并按以下规定处理复位应答：

——如果这个冷复位应答不符合 JR/T 0025.3，但能够被终端识别，终端即可以选择一个不符合 JR/T 0025.1[7]的应用。例如一个隐含选择出来的不符合 JR/T 0025 的储值应用；

——如果终端不能识别不符合 JR/T 0025.3 的冷复位应答，终端必须按照 JR/T 0025.3 的规定对 IC 卡进行热复位；

——如果冷复位应答符合 JR/T 0025.3，终端可直接选择 PBOC 应用[7]；

——如果热复位应答不符合 JR/T 0025.3，则终端应终止交易并显示错误信息（例如“卡片错误”）[8]；

——如果热复位符合 JR/T 0025.3，终端可以直接选择 PBOC 应用。

如上定义中，不符合 JR/T 0025.1 的应用可以与符合 JR/T 0025 的应用共存。

6.1.2.3 应用选择

终端必须有一个它所支持的所有PBOC应用的应用列表。该列表应包含这些应用的AID。

终端必须能支持JR/T 0025.1规定的直接应用选择。也可以支持目录方式的应用选择。

直接选择PBOC应用时，终端必须按以下之一执行：

——读卡片目录（用 READ RECORD 命令），卡片的 AID 与终端的应用列表通过比较找出一个相匹配的 AID，然后用此 AID 向 IC 卡发 SELECT 命令；

——直接向 IC 卡发出 SELECT 命令，每次使用不同的 AID 直到 IC 卡回送正确的响应（SW1 SW2=“9000”）。

选择了一个PBOC应用后，终端通过READ RECORD命令读出短文件标识SFI为1的文件中第一条记录里的磁条卡功能（Easy Entry）应用数据。终端不校验LRC，也不检查磁道2和磁道3（如果出现）数据的起始位和终止位。

6.1.2.4 卡的读取和处理

终端必须支持IC读卡器，并符合JR/T 0025.3中有关电气和机械特性的规定。

终端必须支持磁条读写器，并能够读符合GB/T 14916、GB/T 15120、GB/T 15694.1和GB/T 17552的磁条卡。

用IC读写器读卡时，不管服务码是什么值，终端对这笔交易的处理应与处理磁条卡交易的方式相同。

6.1.3 相互受理和共存

磁条卡功能（Easy Entry）应用作为PBOC应用的一个子集并隐含包括在PBOC芯片应用中。任何支持磁条卡功能（Easy Entry）的终端都能接受PBOC芯片应用，而任何支持PBOC芯片的终端也能够接受磁条卡功能（Easy Entry）应用。因此，两种应用的相互受理在所有情况下都是可以的。

——如果 IC 卡和终端都能支持 PBOC 芯片应用，产生的交易就是 PBOC 芯片交易而不能默认为磁条卡功能（Easy Entry）交易。

——如果 IC 卡支持 PBOC 芯片应用，而终端仅支持磁条卡功能（Easy Entry）应用，那么终端默认为磁条卡功能（Easy Entry）交易。

——如果 IC 卡支持磁条卡功能（Easy Entry）应用，并且终端支持磁条卡功能（Easy Entry）应用，终端按磁条卡功能（Easy Entry）交易方式处理交易。

——如果 IC 卡支持磁条卡功能（Easy Entry）应用，而终端支持 PBOC 芯片应用，那么 IC 卡拒绝交易。表 55 列出了相互受理的各种情况。

表 55 相互受理需求

	终端支持 PBOC 芯片应用	终端支持磁条卡功能
卡片支持 PBOC 芯片应用	PBOC 芯片应用	磁条卡功能（Easy Entry）
卡片支持磁条卡功能	拒绝	磁条卡功能（Easy Entry）

6.2 关于授权报文和清算报文

[7]根据特定说明终端也可以识别不符合 JR/T 0025 的应用（例如通过使用复位应答中历史字符来标识）。

[8]根据特定说明终端也可进行其它类型的复位（例如一次性存储卡）。

对于支持磁条卡功能（Easy Entry）的终端交易来讲，授权报文和清算报文的差别很小。除了销售点终端（POS）的“进入方式代码”（Entry Mode Code）外，对于只带磁条的卡所做的交易和磁条卡功能（Easy Entry）应用的交易，其报文的内容是一致的。终端向收单行传送的报文中，如果销售点终端的“进入方式代码”（Entry Mode Code）的值为‘05’，表示数据是从IC卡读出的。

附 录 A
（规范性附录）
数据元解释

表A.1定义本部分所使用的数据元。

表A.1 数据元表

数据域	说明	来源	格式	长度(字节)	值
算法标识（DLK）	用来标识圈存交易的加密算法。	IC卡终端	b	1	
算法标识（DPK）	用来标识消费和取现交易的加密算法。	IC卡终端	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。	IC卡终端	b	1	
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。	IC卡终端	b	1	
算法标识(DULK)	用来标识在圈提交易中使用的加密算法。	IC卡终端	b	1	
应用有效日期	该日期后卡应用终止。	IC卡	cn CCYYMMDD	4	
应用标识符	用于标识一个应用，并符合GB/T 16649.5	IC卡终端	b	5-16	
应用序列号	发卡方分配的一个数字。	IC卡	cn	10	
应用启用日期	指示应用生效日期。	IC卡	cn CCYYMMDD	4	
应用类型标识	IC 卡支持的表示卡存在的应用类型（ED 或 EP）的标识。	IC卡	cn	1	值： 01：只有 ED 02：只有 EP 03：ED 和 EP 都存在 所有其他值预留。
应用版本号	表示 IC 卡当前使用的应用版本的一个数字。	IC卡	b	1	
发卡方应用版本号	表示发卡方当前使用的应用版本的一个数字。	IC卡	b	1	
本行职工标识	用来表示持卡人是否银行职员的一个标识。该标识可用来获得某种优惠。	IC卡	n	1	
卡类型标识		IC卡	cn	1	值： 00：个人卡 10：单位卡 所有其他值预留
持卡人证件号码	用来标识持卡人。	IC卡	an	32	

数据域	说明	来源	格式	长度(字节)	值
持卡人证件类型	用于区分持卡人证件类型而分配的值。	IC 卡	cn	1	值： 00：身份证 01：军官证 02：护照 03：入境证（仅限香港/台湾居民使用） 04：临时身份证 05：其他
持卡人姓名	根据 GB/T 17552 格式，标识持卡人姓名。	IC 卡	an	20	
ED 余额	IC 卡中 ED 的当前余额。这个 ED 余额是卡上实际余额和透支限额之和。	IC 卡	b	4	
ED 脱机交易计数器	IC 卡中的一个计数器，每发生一次 ED 消费/取款交易时就增加。	IC 卡	b	2	
ED 联机交易计数器	IC 卡中的一个计数器，每发生一次 ED 圈存、圈提或修改透支限额交易时就增加。该计数器和主机同步，并且可以在过程密钥的产生中使用。	IC 卡	b	2	
EP 余额	IC 卡中 EP 的当前余额。	IC 卡	b	3	
EP 脱机交易计数器	IC 卡中的一个计数器，每当 EP 消费交易发生就增加。	IC 卡	b	2	
EP 联机交易计数器	IC 卡中的一个计数器，每次发生 EP 圈存交易时就增加。该计数器和主机同步，并且可以在过程密钥的产生中使用。	IC 卡、主机	b	2	
发卡方标识	用来唯一标识发卡方的一个数字	IC 卡	cn	8	
发卡方自定义 FCI 数据	发卡方在其自己终端上用于特殊处理的自定义数据	IC 卡	b	2	
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。	IC 卡终端	cn	1	
密钥版本号（DLK）	用来唯一标识圈存交易的密钥版本。	IC 卡	b	1	
密钥版本号（DPK）	用来唯一标识一个消费或取现交易的密钥版本。	IC 卡	b	1	
密钥版本号（DTK）	用来唯一标识计算 TAC 所用的密钥版本。	IC 卡	b	1	

数据域	说明	来源	格式	长度(字节)	值
密钥版本号（DUK）	用来唯一标识一个修改透支限额交易的密钥版本。	IC卡	b	1	
密钥版本号（DULK）	用来唯一标识一个圈提交易的密钥版本。	IC卡	b	1	
透支限额	发卡方给持卡人指定的最大透支额度。	IC卡	b	3	
PIN尝试计数器	用来记录剩余的PIN尝试次数。	IC卡	b	1	
PIN尝试上限	发卡方给定的一个应用中允许PIN连续错误的最大次数。	IC卡	b	1	该数据元必须初始一个值
PSAM标识符	用来唯一标识安装在终端中的PSAM的一个数字。	PSAM	b	4	
伪随机数(IC卡)	IC卡随机产生的一个数字。	IC卡	b	4	
PIN参考值	IC卡中存放的用来与持卡人输入的个人识别码的值进行比较的值。	IC卡	cn	2-6	
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	
交易金额	当前交易的金额。	终端	B	4	
交易日期（发卡方）	交易发生日期。	发卡方	cn CCYYMMDD	4	
交易日期(终端)	交易发生日期。	终端	cn CCYYMMDD	4	
交易时间	交易发生时间。	终端	cn	3	
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、IC卡	cn	1	值： 01：ED圈存 02：EP圈存 03：圈提 04：ED取款 05：ED消费 06：EP消费 07：ED修改透支限额 08：信用消费

当为数据定义的长度超过实际数据长度，而位数没有占满时，补位规则如下：

——格式n的数据元右靠齐并且左补十六进制“0”；

——格式cn的数据元左靠齐并且右补十六进制“F”；

——格式an的数据元左靠齐并且右补十六进制“0”；

——格式ans的数据元左靠齐并且右补十六进制“0”。

当数据从一个实体移动到另一个时（如卡到终端），不管其内部如何存放，都是按照由高到低的顺序传送。数据的串联也同样符合这个原则。

附 录 B
（规范性附录）
ED/EP 应用的密钥关系

本附录描述了与ED/EP应用相关的设备实体之间的密钥关系，此处还描述了IC卡密钥的推导方法和过程密钥的产生方法；本部分之外的密钥用法（如：个人化过程的密钥）不在本部分范围之内。

以下描述的所有密钥均为双倍长DEA密钥（128比特长）。为确保密钥的安全，密钥的产生和存放都应由一个专用的安全模块来处理。表B.1和表B.2概述了支持ED和EP应用的主机与IC卡、POS设备之间的密钥关系。

B.1 密钥关系表

表B.1 IC 卡中存储的共用于电子存折和电子钱包应用的密钥

密钥	发卡方	IC 卡	POS（PSAM）
用于消费/取现交易的密钥	消费主密钥（MPK）	消费子密钥（DPK），由 MPK 用应用序列号推导获得。	消费主密钥（MPK）
用于圈存交易的密钥	圈存主密钥（MLK）	圈存子密钥（DLK），由 MLK 用应用序列号推导获得。	N/A
消费/取现交易中用于产生 TAC 的密钥	TAC 主密钥（MTK）	TAC 子密钥（DTK），由 MTK 用应用序列号推导获得。	N/A
用于解锁 PIN 的密钥	PIN 解锁主密钥（MPUK）	PIN 解锁子密钥（DPUK），由 MPUK 用应用序列号推导获得。	由发卡方考虑决定
用于重装 PIN 的密钥	PIN 重装主密钥（MRPK）	PIN 重装子密钥（DRPK），由 MRPK 用应用序列号推导获得。	N/A
用于应用维护功能的密钥	应用主控密钥（MAMK）	应用主控子密钥（DAMK），由 MAMK 用应用序列号推导获得。	N/A

表B.2 IC 卡中用于电子存折应用的密钥

密钥	发卡方	IC 卡	POS（PSAM）
用于圈提交易的密钥	圈提主密钥（MULK）	圈提子密钥（DULK），由 MULK 用应用序列号推导获得。	N/A
用于修改透支限额交易的密钥	修改主密钥（MUK）	子修改（透支限额）密钥（DUK），由 MUK 用应用序列号推导获得。	N/A

B.2 子密钥推导方法

本条描述了IC卡中密钥的推导方法。图B.1和图B.2描述了DPK推导的过程。

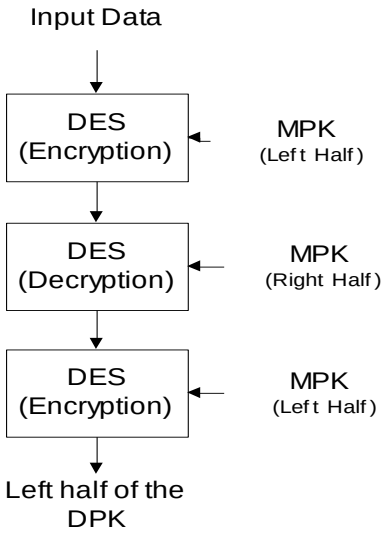
B.2.1 DPK左半部分的推导方法

推导双倍长DPK左半部分的方法：

——将应用序列号的最右 16 个数字作为输入数据；

——将 MPK 作为加密密钥；

——用 MPK 对输入数据进行 3DEA 运算。



图B.1 推导 DPK 左半部分

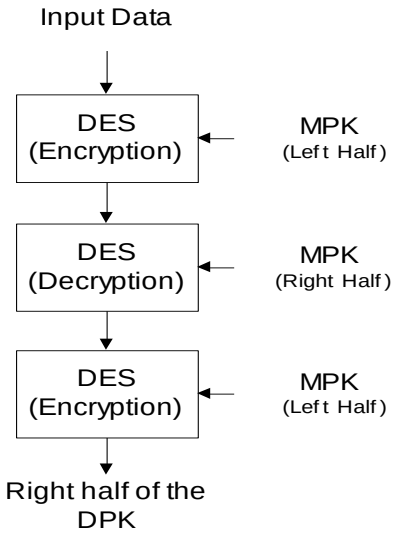
B.2.2 DPK右半部分的推导方法

推导双倍长DPK右半部分的方法：

——将应用序列号的最右 16 个数字的求反作为输入数据；

——将 MPK 作为加密密钥；

——用 MPK 对输入数据进行 3DEA 运算。



图B.2 推导 DPK 右半部分

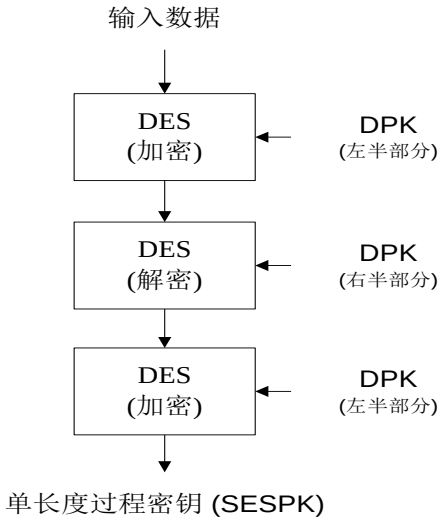
图B.1和图B.2描述的方法同样适用于ED的消费/取现、圈存和圈提、修改等子密钥的推导，及EP的消费和圈存子密钥的推导。

B.3 过程密钥的产生

过程密钥是在交易过程中用可变数据产生的单倍长密钥。

过程密钥产生后只能在某过程/交易中使用一次。

图B.3描述了EP进行消费交易时产生过程密钥的机制。这方法也用于不同交易类型的过程密钥的产生，但输入的数据取决于不同的交易类型。



图B.3 过程密钥的产生

B.4 MAC/TAC的计算

MAC/TAC的产生使用以下单倍长DEA算法：

第一步：将一个8个字节长的初始值（Initial Vector）设定为16进制的“0x 00 00 00 00 00 00 00 00”。

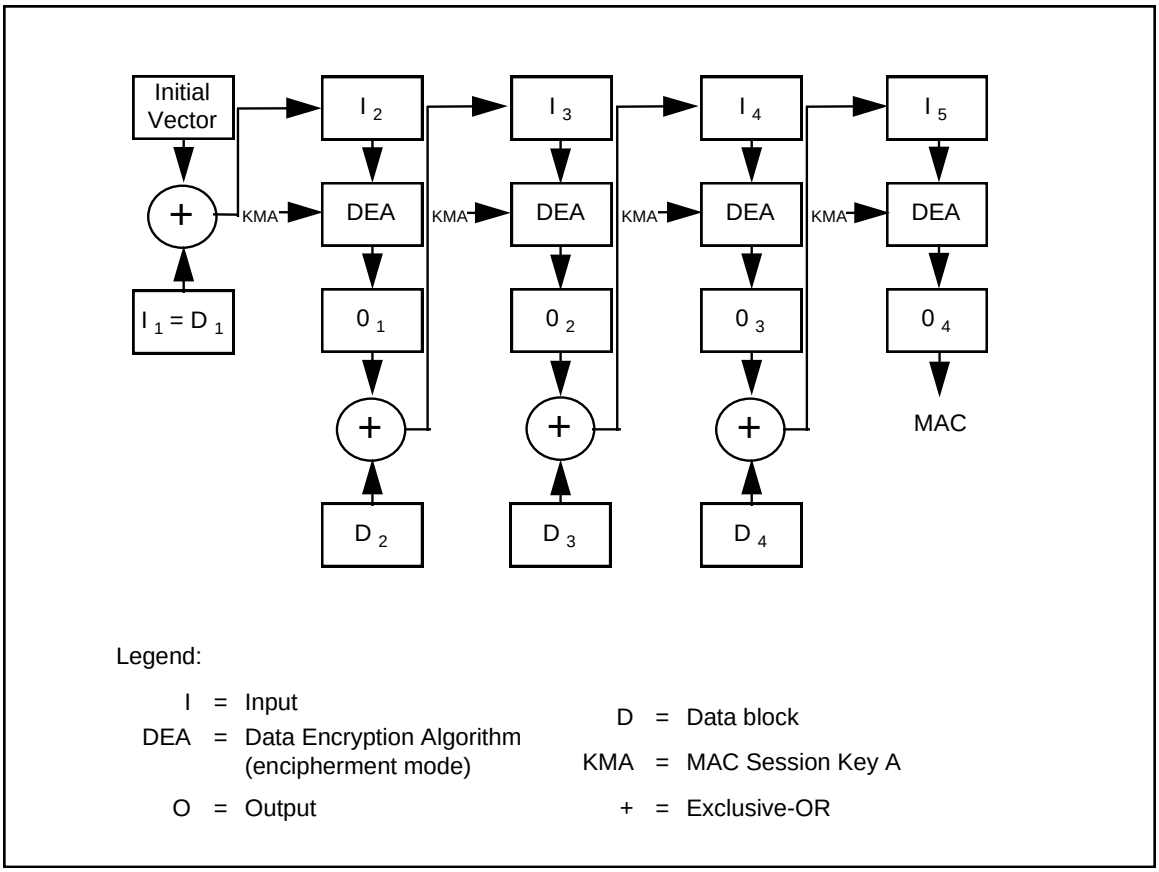
第二步：将所有的输入数据按指定顺序串联成一个数据块。

第三步：将串联成的数据块分割为8字节长的数据块组，标识为D1、D2、D3与D4等。分割到最后，余下的字节组成一个长度小于等于8字节的最后一块数据块。

第四步：如果最后一个数据块长度为8字节，则在此数据块后附加一个8字节长的数据块，附加的数据块为16进制的“0x 80 00 00 00 00 00 00 00”。如果最后一个数据块长度小于8字节，则该数据块的最后填补一个值为16进制“0x80”的字节。如果填补之后的数据块长度等于8字节，则跳至第五步。如果填补之后的数据块长度仍小于8字节，则在数据块后填补16进制“0x0”的字节至数据块长度为8字节。

第五步：MAC的产生是通过上述方法产生的数据块组，由过程密钥进行加密运算，过程密钥的产生方法见图B.3。TAC的产生是通过上述方法产生的数据块组，由DTK密钥左右8位字节进行异或运算的结果进行加密运算。MAC或TAC的算法见图B.4描述。

第六步：最终值的左4字节为MAC或TAC。



图B.4 MAC 和 TAC 的单倍长 DEA 密钥算法

附 录 C
（规范性附录）
ED/EP 应用的基本文件

C.1 ED和EP应用的基本文件

表C.1 ED 和 EP 应用的公共应用基本文件

文件标识（SFI）		‘21’（十进制）
文件类型		透明
文件大小		30
文件存取控制		读=自由 改写=需要安全信息
字节	数据元	长度
1-8	发卡方标识	8
9	应用类型标识	1
10	发卡方应用版本	1
11-20	应用序列号	10
21-24	应用启用日期	4
25-28	应用有效日期	4
29-30	发卡方自定义 FCI 数据	2

表C.2 ED 和 EP 应用的持卡人基本文件

文件标识（SFI）		‘22’（十进制）
文件类型		透明
文件大小		55
文件存取控制		读=自由 改写=需要安全信息
字节	数据元	长度
1	卡类型标识	1
2	本行职工标识	1
3-22	持卡人姓名	20
23-54	持卡人证件号码	32
55	持卡人证件类型	1

表C.3 内部数据元

数据元	长度
ED 余额	4
ED 脱机交易序号	2
ED 联机交易序号	2
透支限额	3
EP 余额	3
EP 脱机交易序号	2
EP 联机交易序号	2

密钥版本号（DPK）	1
密钥版本号（DTK）	1
密钥版本号（DLK）	1
密钥版本号（DULK）	1
密钥版本号（DUK）	1
算法标识（DPK）	1
算法标识（DTK）	1
算法标识（DLK）	1
算法标识（DULK）	1
算法标识（DUK）	1

C.2 IC卡交易明细

这个文件必须能够容纳至少十条消费、取款、圈存、圈提交易记录。

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 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.4 IC卡交易明细文件

文件标识（SFI）		‘24’（十进制）
文件类型		循环
文件存取控制		读=PIN保护 改写=不允许[9]
记录大小		23
字节	数据元	长度
1-2	ED或EP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

[9]交易明细由IC卡维护。不允许外部对其修改。

参考文献

[1] prEN 1546-1：1994 识别卡系统 电子钱包 第1部分 定义、概念和结构（委员会草案）
[2] PrEN 1546-2：1996 识别卡系统 电子钱包 第2部分 安全机制（委员会草案）
[3] PrEN 1546-3：1996 识别卡系统 电子钱包 第3部分 数据元及交换
[4] PrEN 1546-4：1996 识别卡系统 电子钱包 第4部分 设备（委员会草案）
[5] EMV支付系统集成电路卡规范：2004，第1册～第4册
[6] VIS：1996 VISA集成电路卡规范（版本1.3）