中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

中国移动手机支付(U)SIM卡复合应用技术规范

版本号：1.0.0

XXXX-XX-XX发布　　XXXX-XX-XX实施

中国移动通信集团公司　　发布

目　　录

前　言

本标准对中国移动手机支付业务开展过程中(U)SIM卡上手机支付复合应用需要规范的内容提出全面要求，是使用该业务的依据。

本标准主要包括以下几方面内容：业务概述、文件和命令、安全、交易流程、交易处理性能。

本标准是手机支付业务系列标准之一。

本标准的附录B、D为标准性附录，附录A、C为资料性附录。

本标准由中移　　号文件印发。

本标准由中国移动通信集团市场经营部提出，集团公司技术部归口。

本标准起草单位：中国移动通信研究院

本标准主要起草人：乐祖晖、李琳、朱本浩

1．范围

本标准规定了中国移动手机支付复合应用的全面要求，供中国移动内部和(U)SIM卡、POS终端厂商共同使用；适用于GSM/GPRS/TD-SCDMA网络环境。

本标准定义的内容是《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》的补充和扩展，和《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》相同的内容本标准中直接引用，不再重复描述。

本标准主要包括以下内容：

———手机支付复合应用。定义了用于现场支付复合应用的数据元、文件、命令、交易流程、安全机制等内容。

———透支限额处理。定义了修改、使用透支限额的命令及交易流程。

———在《中国移动手机支付业务接口规范--POS 终端与(U)SIM 卡接口分册》定义基础上，修改了’21’文件中 29~30 字节的定义。

———异常处理流程。定义了异地异常处理流程。

2．规范性引用文件

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

序号	标准编号	标准名称	发布单位
1		《中国金融集成电路（IC）卡电子钱包扩展应用指南》	中国人民银行
2		《中国金融集成电路（IC）卡非接触式规范（V2.0）》	中国人民银行
3		《中国金融集成电路（IC）卡电子钱包/电子存折规范（V2.0）》	中国人民银行
4		《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》	中国移动通信有限公司
5		《中国移动手机支付业务PSAM卡规范》	中国移动通信有限公司

3．术语、定义和缩略语

下列术语、定义和缩略语适用于本标准：

表3-1 定义

词语	解释
终端	为完成金融交易而在交易点安装的设备，用于同(U)SIM卡进行交互。它包括接口设备，也可包括其它部件和接口，例如与主机通讯的接口。
命令	终端向(U)SIM卡发出的一条信息，该信息启动一个操作或请求一个应答。
响应	(U)SIM卡处理完收到的命令报文后，回送给终端的报文。
金融交易	手机用户、商户和收单行之间基于收、付款方式的商品或服务交换行为。
功能	由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。
报文	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。
报文鉴别代码	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。
明文	没有加密的信息。
密文	通过密码系统产生的不可理解的文字或信号。
密钥	控制加密转换操作的符号序列。
加密算法	为了隐藏或揭露信息内容而变换数据的算法。
数据完整性	数据不受未经许可的方法变更或破坏的属性。
复合应用	结合现场脱机支付应用和其它应用的应用模式。
终端随机数	终端通过PSAM卡产生的随机数

表3-2 缩略语

词语	解释
AID	应用标识符（Application Identifier）
CAPP	复合应用（Complex Application）
CLA	命令报文的类型字节（Class byte of the command message）
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	报文鉴别代码（Message Authentication Code）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
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）
RFU	保留为将来使用（Reserved for Future Use）
SAM	安全存取模块（Secure Access Module）
SFI	短文件标识符（Short File Identifier）
SW1	状态码 1（Status Word One）
SW2	状态码 2（Status Word Two）
TAC	交易验证码（Transaction Authorization Cryptogram）
TRAN	终端随机数（Terminal Random）

4．手机支付业务概述

4.1 业务概述

手机支付业务是指基于中国移动移动通信网络和互联网络技术，利用手机，通过短信息、STK、语音、WAP、RFID等方式，通过手机支付账户进行消费、充值、转账、查询等电子商务操作，并进行相关业务管理的业务。

通过手机支付业务提供的支付能力，用户可以进行实物商品、数字商品、服务的购买以及中国移动数据增值业务的付费。

手机支付业务的详细业务描述参见《中国移动手机支付业务规范》。

4.2 业务分类

依据用户进行交易时，用户支付方式的不同，可将手机支付分为：

1. 远程支付

在支付过程中，用户利用手机，基于移动通信网络，通过SMS、GPRS、WAP、STK等完成支付行为。例如：用户通过手机，在互联网上购买商品和服务。

2. 现场支付

在支付过程中，用户利用手机，通过近距离通信方式完成支付行为。例如：用户通过手机，在现实的商店（如便利店、快餐店）中，通过POS机“刷卡”方式购买商品与服务。

在现场支付中，根据POS是否需要联机进行支付处理，又可分为两类：

- 脱机支付

支付过程中，POS机不和后台系统交互，直接完成扣款操作。

- 联机支付

支付过程中，POS机通过网络连接到后台系统用联机交互的方式完成用户验证和扣款操作。

4.3 系统结构图

手机支付系统结构图如图4.1所示，各网元的功能描述详见《中国移动手机支付业务总体技术要求-总册及远程支付部分》。

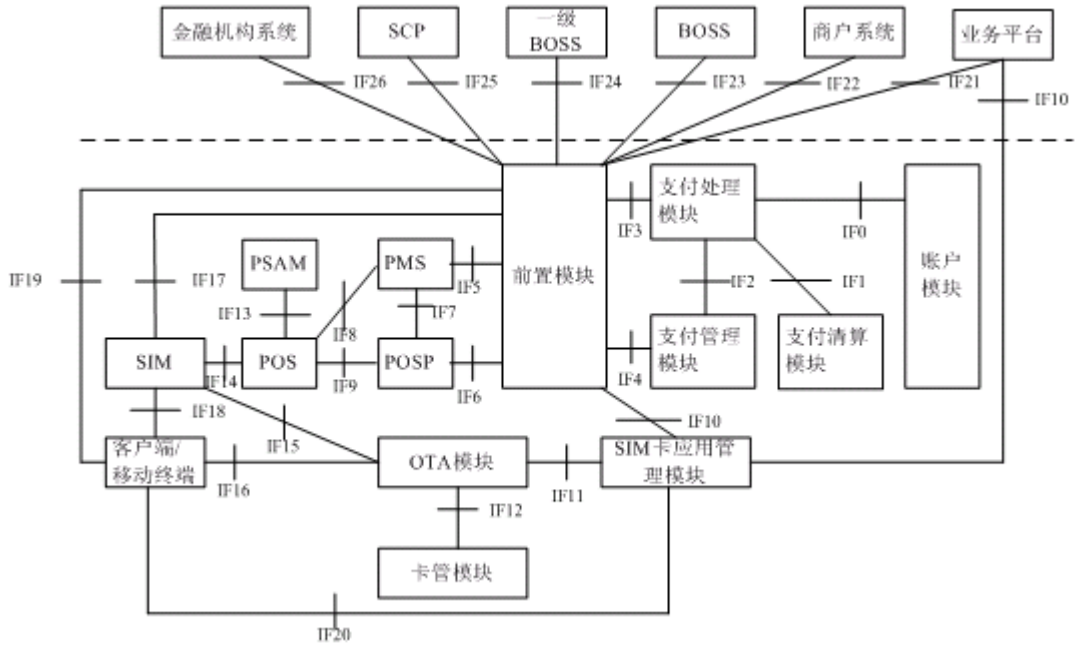

图4.1 手机支付系统结构图

5 文件和命令

本标准继承《中国移动手机支付业务接口规范--POS 终端与(U)SIM 卡接口分册》中有关现场支付应用的所有定义，并增加定义了一种现场支付应用模式：复合应用模式。

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、复合应用删除及透支限额维护、使用。

关于复合应用的说明请见附录A。

5.1 复合应用专用文件

采用变长记录文件，记录格式采用简单TLV，该文件的定义见附录B。

5.2 APDU 命令

5.2.1 概述

5.2.1.1 卡状态

(U)SIM卡具有如下状态：

- 空闲状态
- 圈存状态
- 消费状态
- 复合应用消费状态1

- 复合应用消费状态2
- 修改状态

5.2.1.2 支持的命令

(U)SIM卡支持命令如下：

- INITIALIZE FOR LOAD（圈提初始化）
- CREDIT FOR LOAD（圈存）
- INITIALIZE FOR PURCHASE（消费初始化）
- DEBIT FOR PURCHASE（消费）
- GET BALANCE（读余额）
- GET TRANSACTION PROVE（取交易认证）

特别地，复合应用模式专用指令如下：

- 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）
- INITIALIZE FOR UPDATE（修改透支限额初始化）
- UPDATE OVERDRAW LIMIT（修改透支限额）

5.2.1.3 卡状态迁移表

(U)SIM卡状态迁移表如表5-1所示：

表5-1 命令执行成功后的状态变化

状态 命令	空闲	圈存	消费	CAPP1	CAPP2	修改
CREDIT FOR LOAD	N/A	空闲	N/A	N/A	N/A	N/A
DEBIT FOR PURCHASE	N/A	N/A	空闲	N/A	N/A	N/A
DEBIT FOR CAPP PURCHASE	N/A	N/A	N/A	N/A	空闲	N/A
GET BALANCE	空闲	圈存	消费	CAPP1	CAPP2	修改
GET TRANSACTION PROVE	空闲	圈存	消费	CAPP1	CAPP2	修改
INITIALIZE FOR LOAD	圈存	圈存	圈存	N/A	N/A	圈存
INITIALIZE FOR PURCHASE	消费	消费	消费	N/A	N/A	消费
INITIALIZE FOR CAPP PURCHASE	CAPP1	N/A	N/A	N/A	N/A	N/A
INITIALIZE FOR UPDATE	修改	修改	修改	N/A	N/A	修改
UPDATE CAPP DATA CACHE	N/A	N/A	N/A	CAPP2	CAPP2	N/A
UPDATE OVERDRAW LIMIT	N/A	N/A	N/A	N/A	N/A	空闲

5.2.1.4 命令类别字节及指令字节

命令的类别字节及指令字节如表5-2所示：

表5-2 命令的类别字节和指令字节

命　　令	CLA	INS	P1	P2
CREDIT FOR LOAD（圈存）	‘80’	‘52’	‘00’	‘00’
DEBIT FOR PURCHASE（消费）	‘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 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（复合消费初始化）	‘80’	‘50’	‘03’	‘02’
INITIALIZE FOR UPDATE（修改透支限额初始化）	‘80’	‘50’	‘07’	‘02’
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’	‘07’	‘02’

5.2.2 INITIALIZE FOR CAPP PURCHASE 命令

5.2.2.1 定义和范围

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

5.2.2.2 命令报文

INITIALIZE FOR CAPP PURCHASE命令报文见表5-3：

表5-3 INITIALIZE FOR CAPP PURCHASE命令报文格式

代码	值（16进制，下同）
CLA	‘80’
INS	‘50’
P1	‘03’
P2	‘02’
Lc	‘0B’
Data	见5.2.2.3
Le	‘0F’

5.2.2.3 命令报文数据域

此命令报文的数据域定义见表5-4：

表5-4 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

5.2.2.4 响应报文数据域

此命令执行成功的响应报文数据域见表5-5：

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

说明	长度（字节）
现场脱机支付余额	4
现场脱机支付脱机交易序号	2
透支限额	3
密钥算法版本号	1
密钥标识	1
伪随机数	4

现场脱机支付余额是真实余额与透支限额之和

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

5.2.2.5 响应报文状态码

此命令执行成功的状态码是’9000’。

(U)SIM卡可能回送的错误状态见表5-6：

表5-6 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

5.2.3 UPDATE CAPP DATA CACHE 命令

5.2.3.1 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。

考虑到今后的POS终端可能会发出大于卡上一条记录长度的CACHE数据，需要复合应用增加对多次接收UPDATE CAPP DATA CACHE命令的处理机制，要求支持至少2个UPDATE CAPP DATA CACHE命令的处理，同时要考虑CACHE大小。

5.2.3.2 命令报文

此命令报文见表5-7：

表5-7 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或记录号，根据P2取值来定
P2	见表5-8
Lc	后续数据域的长度
Data	见5.2.3.3节
Le	不存在

此命令报文中的引用控制参数P2定义见表5-8：

表5-8 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	P1为记录标识，第一个标识符出现的记录
					1	0	0	P1为记录号
—	—	—	—	—	X	X	X	RFU
其它值								RFU

5.2.3.3 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。

5.2.3.4 响应报文数据域

响应报文数据域不存在。

5.2.3.5 响应报文状态码

此命令执行成功的状态码是’9000’。

(U)SIM卡可能回送的错误状态码见表5-9：

表5-9 UPDATE CAPP DATA CACHE可能回送的错误状态码

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

5.2.4 DEBIT FOR CAPP PURCHASE 命令

5.2.4.1 定义和范围

DEBIT FOR CAPP PURCHASE命令用于复合应用消费交易。

5.2.4.2 命令报文

此命令报文见表5-10：

表5-10 DEBIT FOR CAPP PURCHASE命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
Lc	‘0F’
Data	见5.2.4.3节
Le	‘08’

5.2.4.3 命令报文数据域

此命令报文的数据域定义见表5-11：

表5-11 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

5.2.4.4 响应报文数据域

此命令执行成功的响应报文数据域见表5-12：

表5-12 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。

5.2.4.5 响应报文状态码

此命令执行成功的状态码是'9000'。

(U)SIM卡可能回送的错误状态见表5-13：

表5-13 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

5.2.5 INITIALIZE FOR UPDATE 命令

5.2.5.1 定义和范围

INITIALIZE FOR UPDATE命令用于初始化修改现场脱机支付透支限额交易。

5.2.5.2 命令报文

INITIALIZE FOR UPDATE命令报文见表5-14：

表5-14 INITIALIZE FOR UPDATE命令报文

代码	值
CLA	'80'
INS	'50'
P1	'07'
P2	'02'
L_c	'07'
Data	见表5-15
L_e	'13'

5.2.5.3 命令报文数据域

表5-15定义了命令报文的数据域：

表5-15 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

5.2.5.4 响应报文数据域

命令执行成功的响应报文数据域见表5-16。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表5-16 INITIALIZE FOR UPDATE响应报文数据域

说明	长度（字节）
现场脱机支付余额	4
现场脱机支付联机交易序号	2
旧透支限额	3
密钥版本号	1
算法标识	1
伪随机数（(U)SIM卡）	4
MAC1	4

5.2.5.5 响应报文状态码

此命令执行成功的状态码是’9000’。

表5-17描述了(U)SIM卡可能回送的错误状态。

表5-17 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、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

5.2.6 UPDATE OVERDRAW LIMIT 命令

5.2.6.1 定义和范围

UPDATE OVERDRAW LIMIT命令用于修改现场脱机支付透支限额交易。

在透支情况下不允许修改透支限额，卡应返回6985的错误状态码。

5.2.6.2 命令报文

UPDATE OVERDRAW LIMIT命令报文见表5-18：

表5-18 UPDATE OVERDRAW LIMIT命令报文

代码	值
CLA	‘**80**’

INS	‘**58**’
P1	‘**07**’
P2	‘**02**’
L_c	‘**0E**’
Data	见表**5-19**
L_e	‘**04**’

5.2.6.3 **命令报文数据域**

表**5-19**定义了命令报文的数据域：

表5-19 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**

5.2.6.4 **响应报文数据域**

此命令执行成功的响应报文数据域见表**5-20**。

如果命令执行不成功，则只在响应报文中回送**SW1**和**SW2**。

表5-20 UPDATE OVERDRAW LIMIT命响应报文数据域

说明	长度（字节）
TAC	**4**

5.2.6.5 **响应报文状态码**

此命令执行成功的状态码是’**9000**’。

表**5-21**描述了**(U)SIM**卡可能回送的错误状态：

表5-21 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

5.2.7 GET BALANCE 命令

5.2.7.1 定义和范围

GET BALANCE命令用于读取现场脱机支付余额，实现查询余额交易。

5.2.7.2 命令报文

GET BALANCE命令报文见表**5-22**：

表**5-22 GET BALANCE**命令报文

代码	值
CLA	'**80**'
INS	'**5C**'
P1	'**00**'
P2	'**02**'（参见《中国移动手机支付业务接口规范**--POS**终端与**(U)SIM**卡接口分册》） '**A0**'（同时读取现场脱机支付余额及透支限额）
L_c	不存在
Data	不存在
L_e	当**P2='02'**时，**Le='04'**； 当**P2='A0'**时，**Le='07'**。

5.2.7.3 响应报文数据域

命令执行成功的响应报文数据域见表**5-23**（**P2='02'**）和表**5-24**（**P2='A0'**）。
如果命令执行不成功，则只在响应报文中回送**SW1**和**SW2**。

表**5-23 GET BALANCE**响应报文数据域（**P2='02'**）

说明	长度（字节）
现场脱机支付真实余额（若真实余额小于0，返回0）	**4**

表**5-24 GET BALANCE**响应报文数据域（**P2='A0'**）

说明	长度（字节）
现场脱机支付余额	**4**
现场脱机支付透支限额	**3**

现场脱机支付余额是真实余额与透支限额之和。

5.2.7.4 响应报文状态码

此命令执行成功的状态码是'**9000**'。
表**5-25**描述了**(U)SIM**卡可能回送的错误状态：

表5-25 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、P2参数不正确
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误

6 安全

引用《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》第9章。

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密钥保护。

7 交易流程

本章描述现场脱机支付应用的交易流程，是(U)SIM卡被POS终端激活并选择而与POS终端相互作用后，所进行的交易处理过程。

消费交易要求POS终端必须具备交易安全存取模块（PSAM卡）。本标准假定POS终端与PSAM之间是以安全方式进行通信的，详见《中国移动手机支付业务PSAM卡规范》。

7.1 交易预处理流程

参见《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》第10.1节。

7.2 复合应用消费交易流程

复合应用消费交易允许用户使用现场脱机支付余额进行购物或获取服务。此交易可以在POS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密码（PIN）。

复合应用消费交易流程如图7.1所示：

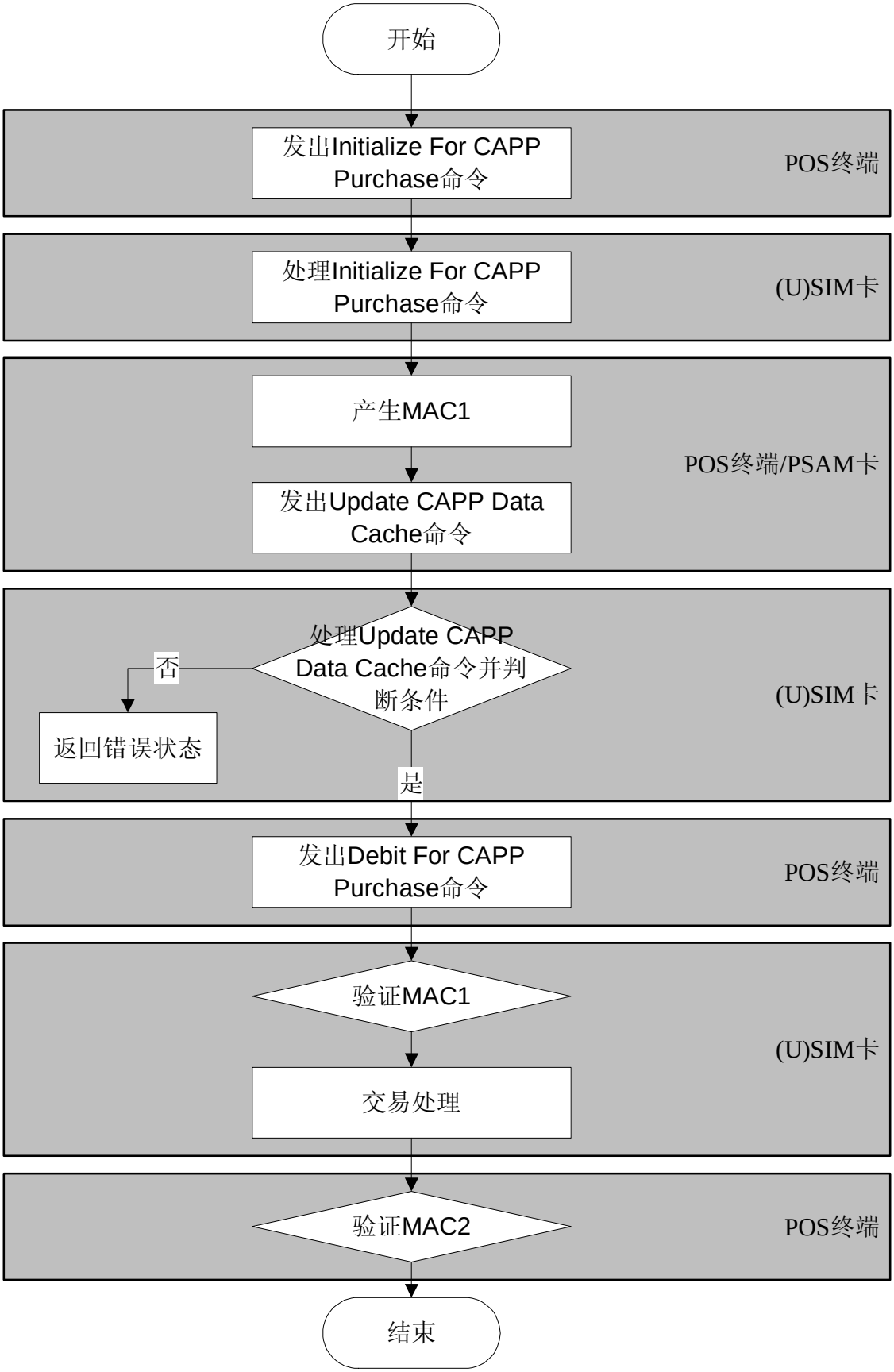

图7.1 复合消费交易流程

7.2.1 发出 INITIALIZE FOR CAPP PURCHASE 命令

POS 终端发出 INITIALIZE FOR CAPP PURCHASE 命令（参见 5.2.2 节）启动复合应用消费交易。

7.2.2 处理 INITIALIZE FOR CAPP PURCHASE 命令

(U)SIM 卡收到 INITIALIZE FOR CAPP PURCHASE 命令后，将进行下述操作：

检查是否支持命令中提供的密钥索引号，如果不支持，则回送状态码’9403’（密钥索引不支持），但不回送其它数据。

检查现场脱机支付余额是否大于或等于交易金额，如果小于交易金额，则回送状态码’9401’（金额不足），但不回送其它数据。POS 终端应采取的措施不在本标准的范围内。

在通过以上检查之后，(U)SIM 卡将产生一个伪随机数（(U)SIM 卡）和过程密钥。过程密钥是利用消费子密钥并按照《中国移动手机支付业务接口规范--POS 终端与(U)SIM 卡接口分册》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（(U)SIM 卡）|| 现场脱机支付脱机交易序号 || 终端交易序号的最右两个字节

7.2.3 产生 MAC1

使用伪随机数（(U)SIM 卡）和(U)SIM 卡回送的现场脱机支付交易序号，POS 终端的安全存取模块（PSAM 卡）将产生一个过程密钥（SESPK）和一个报文认证码（MAC1），供(U)SIM 卡来验证 PSAM 卡的合法性。

MAC1 的计算机制见《中国移动手机支付业务接口规范--POS 终端与(U)SIM 卡接口分册》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（POS 终端）
- 交易时间（POS 终端）

7.2.4 发出 UPDATE CAPP DATA CACHE 命令

POS 终端发出 UPDATE CAPP DATA CACHE 命令。

7.2.5 处理 UPDATE CAPP DATA CACHE 命令

(U)SIM 卡在收到 UPDATE CAPP DATA CACHE 命令后，将进行下述操作：

如果命令中存在 SFI 域，检查(U)SIM 卡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，回送状态码’6A82’（未找到文件），但不回送其它数据。POS 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，则回送状态码’6A83’（未找到记录），但不回送其它数据。POS 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。如果应用锁定标志被设置，则回送状态码’9407’（复合应用禁止），但不回送其它数据。POS 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，则回送状态码’6A84’（文件中存储空间不够），但不回送其它数据。POS 终端应终止此次复合应用消费交易。

在通过以上检查后，(U)SIM 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。

7.2.6 发出 DEBIT FOR CAPP PURCHASE 命令

POS 终端发出 DEBIT FOR CAPP PURCHASE 命令。

7.2.7 验证 MAC1

在收到 DEBIT FOR CAPP PURCHASE 命令后，(U)SIM 卡将验证 MAC1 的有效性。如果 MAC1 有效，交易处理将继续执行 7.2.8 中所描述的步骤。否则将向 POS 终端回送错误状态码’9302’（MAC 无效）。POS 终端对错误状态的处理不在本标准范围内。

7.2.8 交易处理

(U)SIM 卡从现场脱机支付余额中扣减消费的金额，现场脱机支付交易序号加 1，根据 7.2.5 中暂存的数据更新复合应用专用文件，更新现场脱机支付消费交易记录。(U)SIM 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 7.2.57.2.5 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，(U)SIM 卡应在数据后自动填充’00’至记录尾。

(U)SIM 卡产生一个报文签别码（MAC2）供 PSAM 卡对其进行合法性检查，并通过 DEBIT FOR CAPP PURCHASE 命令响应报文回送以下数据，作为 PSAM 卡产生 MAC2 的输入数据。MAC2 的计算机制见《中国移动手机支付业务接口规范--POS 终端与(U)SIM 卡接口分册》附录 B。用 SESPK 对以下数据进行加密产生 MAC2：

- 交易金额

(U)SIM 卡按照《中国移动手机支付业务接口规范--POS 终端与(U)SIM 卡接口分册》附录 B 中描述的机制直接用 TAC 密钥产生 TAC。TAC 将被写入终端交易明细，以便于后台进行交易验证。下面是用来生成 TAC 的数据，它们以明文形式通过 DEBIT FOR CAPP PURCHASE 命令的响应报文从(U)SIM 卡传送到 POS 终端：

- 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（POS 终端）
- 交易时间（POS 终端）

对于现场脱机支付消费交易，(U)SIM 卡将用以下数据组成的一个记录更新交易明细。

- 交易类型标识’09’
- 交易金额
- 卡交易序号
- 终端机编号
- 交易日期（POS 终端）
- 交易时间（POS 终端）

7.2.9 验证 MAC2

在收到(U)SIM卡（经过POS终端）传来的MAC2后，PSAM卡将验证MAC2的有效性。MAC2验证的结果被传送到POS终端以便采取必要的措施。POS终端的采取的措施不在本标准的范围之内。

7.3 应用维护功能

7.3.1 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，从而启用或重新启用相应的复合应用。

首先终端必须按照 7.1 进行交易预处理。

终端首先利用 SELECT FILE 命令，选择复合应用专用文件。如果文件不存在，则说明(U)SIM 卡不支持复合应用。终端应采取的措施不在本标准的范围内。

终端应提示用户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，终端应提示用户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(U)SIM 卡。回写成功后，终端应提示用户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，并提示用户复合应用已存在。

7.3.2 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(U)SIM卡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。

终端利用SELECT FILE命令，选择复合应用专用文件。如果文件不存在，则说明(U)SIM卡不支持复合应用。终端应采取的措施不在本标准的范围内。

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(U)SIM卡支持的所有复合应用，并提示用户选择。

用户选择后，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(U)SIM卡。回写成功后，终端应提示用户复合应用删除成功。

如锁定标志已被设置，则终端终止处理，并提示用户复合应用已删除。

7.4 修改透支限额功能

“透支功能”是本标准从技术上支持的一种基于复合应用的有限信用功能。当现场脱机支付中的实际金额不足时，它为用户提供了一种在中国移动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营业厅终端上联机或通过空中的方式进行。

是否使用“透支功能”以及允许透支的额度由中国移动决定。修改透支限额交易的具体业务作法和要求不在本标准的范围之内。

如果透支限额存在，现场脱机支付余额是真实余额与透支限额之和。现场脱机支付应用不允许透支，复合应用对透支的次数没有限制，但要求子账户的余额不能小于0。

修改透支限额交易流程如图7.2所示：

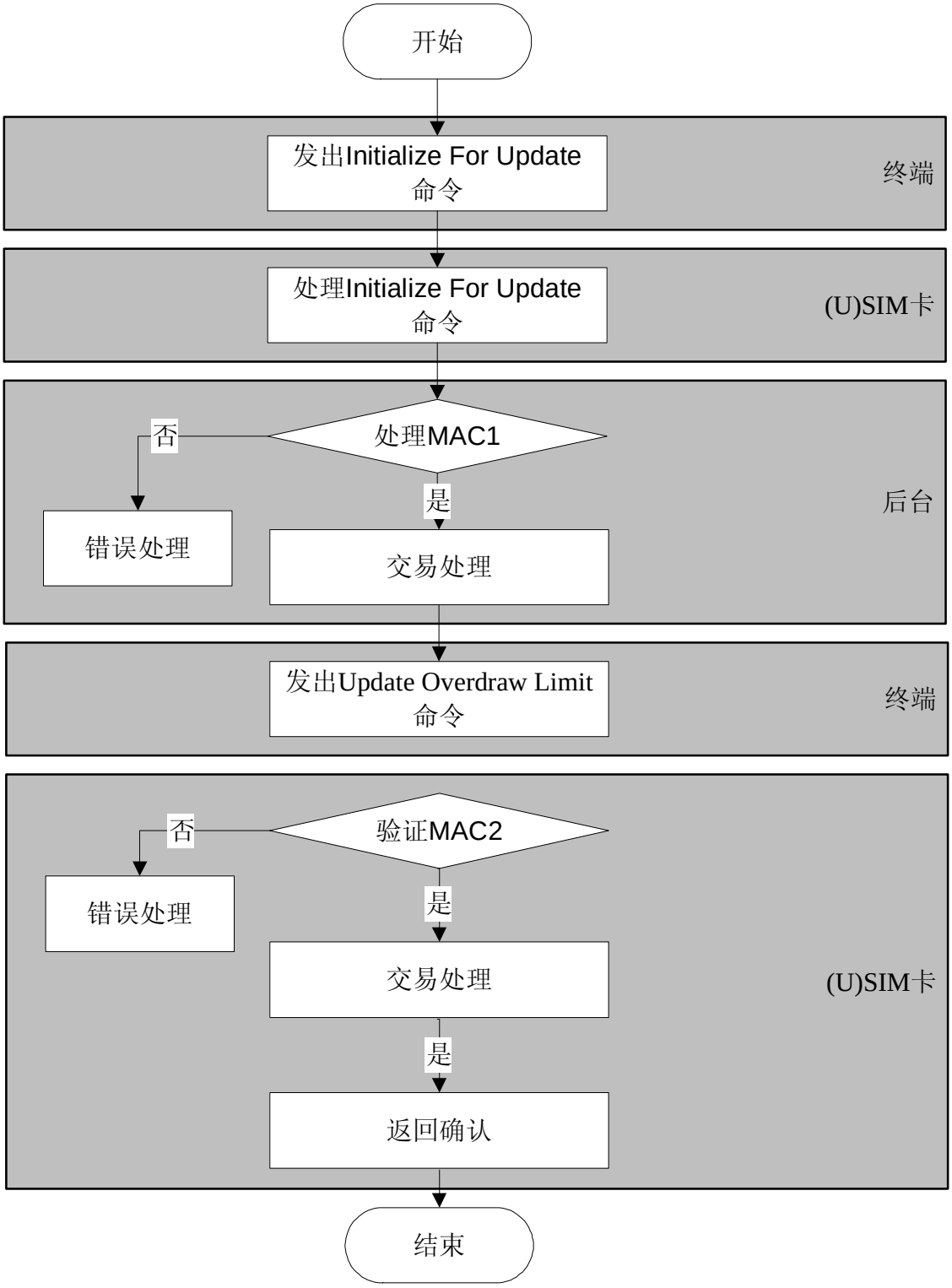

图7.2 修改透支限额流程

7.4.1 发出 INITIALIZE FOR UPDATE 命令

终端发出INITIALIZE FOR UPDATE命令启动修改透支限额交易。

7.4.2 处理 INITIALIZE FOR UPDATE 命令

收到INITIALIZE FOR UPDATE命令后，(U)SIM卡将执行以下操作：

- 检查是否支持命令中提供的密钥索引号。如果不支持，则回送状态码‘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标准的范围以内。

在通过了以上检查之后，(U)SIM卡将产生一个伪随机数、一个过程密钥SESUK和一个报文签别码（MAC1）。该过程密钥是利用修改透支限额密钥（DUK）并按照《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》附录B所描述的机制产生。用于产生过程密钥的输入数据如下：

SESUK：伪随机数||现场脱机支付联机交易序号||‘8000’

MAC1的计算机制见《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》附录B。用SESUK对以下数据加密产生MAC1（按所列顺序）：

- 现场脱机支付余额（交易前）
- 现场脱机支付透支限额（交易前）
- 交易类型标识
- 终端机编号

7.4.3 处理 INITIALIZE FOR UPDATE 命令响应

在收到INITIALIZE FOR UPDATE命令执行成功的响应报文后，终端应向后台传送表5-16定义的数据以及其它后台需要的数据以便于验证MAC1。

7.4.4 验证 MAC1

利用步骤7.4.3中终端传来的报文，后台将产生与(U)SIM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7.4.5中所描述的步骤。否则，后台应向终端回送错误状态码。终端针对错误状态所做的处理不在本标准范围以内。

7.4.5 后台处理

假定后台已经知道(U)SIM卡的透支限额。

基于MAC1（或者其他由后台决定的验证标准）验证的结果，后台将决定是否允许修改透支限额。。

如果后台拒绝交易，则应向终端发送一个拒绝报文，结束交易处理。

如果后台允许交易，则应生成一个报文签别码（MAC2），以供(U)SIM卡对后台合法性进行检查。

MAC2的计算机制见《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》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（后台）
- 交易时间（后台）

后台将现场脱机支付联机交易序号加1。

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

7.4.6 发出 UPDATE OVERDRAWLIMIT 命令

如果后台同意交易，终端将发出UPDATE OVERDRAWLIMIT命令。

7.4.7 验证 MAC2

(U)SIM卡将验证MAC2的有效性。如果MAC2有效, 交易处理将执行7.4.8中的步骤。否则(U)SIM卡回送错误状态码’9302’（MAC无效）。终端对此错误状态所做的处理不在本标准范围之内。

7.4.8 交易处理

(U)SIM卡将按照《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》附录B中描述的机制，直接用密钥TAC密钥左右8字节异或后的结果对以下数据加密产生一个TAC：

- 现场脱机支付余额（交易后）
- 现场脱机支付联机交易序号（加 1 前）
- 现场脱机支付透支限额（交易后）
- 交易类型标识
- 终端机编号
- 交易日期（后台）
- 交易时间（后台）

将当前现场脱机支付余额置为新的现场脱机支付余额，更新透支限额并使现场脱机支付联机交易序号加1。这三个修改必须全部完成，或一个也不完成。

(U)SIM卡通过响应报文将TAC和状态码’9000’传送给终端。

(U)SIM卡用以下数据组成的一个记录更新交易明细：

- 现场脱机支付联机交易序号
- 透支限额
- 交易类型标识
- 终端机编号
- 交易日期（后台）
- 交易时间（后台）

7.4.9 回送确认

(U)SIM卡在UPDATE OVERDRAW LIMIT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。

8 交易处理性能

交易处理性能要求针对非接触式(U)SIM 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(U)SIM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300ms。

9 STK 菜单

支持复合应用功能的手机支付 STK 菜单参见附录 E。

10．中国移动手机支付服务平台与(U)SIM 卡接口

本标准继承《中国移动手机支付业务接口规范--手机支付服务平台与(U)SIM 卡接口规范》中有关接口的所有定义，并增加定义了支持用户补登刷卡记录的上下行指令。

10.1 上行报文

新增上行报文：

表10-1 上行报文

序号(十六进制)	命令类型
0x1E	上传异地未完成交易
0x1F	修改透支限额初始化响应
0x20	修改透支限额响应

10.1.1 上传异地未完成交易

手机支付服务平台需要对本指令进行加密传输，因为本指令包含敏感数据。加密密钥、加密算法和输入数据的定义如下：

表10-2中的命令格式为明文格式和MAC，实际应用中本指令必须采用加密方式传输。加密的输入数据为命令参数的部分内容：即从“应用序列号”到“随机数”之前的字节。加密后输出数据替代从“应用序列号”到随机数之前的字节。“命令长度”为加密后的密文数据长度加上随机数的长度（4字节）和MAC长度（4字节）。

数据加密采用与MAC计算相同的密钥（空中报文保护密钥子密钥）和算法，即用手机支付空中报文保护密钥子密钥的会话密钥，ICV=0。

上传异地未完成交易，应该先判断钱包真实余额是否满足“异地完成交易”的交易金额的扣款需求，如果钱包余额小于该交易金额，应不允许卡片发起该交易，直至用户补足相应的金额。在此情况，卡片应提示用户“钱包余额不足，请先进行充值”。钱包真实余额是现场脱机支付余额减去透支限额。

表**10-2** 上传异地未完成交易命令

项目	名称	长度（字节）	类型	说明
命令类型	上传异地未完成交易命令	**1**	**B**	取值**0x1E**
命令版本	命令版本	**1**	**B**	参见《中国移动手机支付业务接口规范**--**手机支付服务平台与**(U)SIM**卡接口规范》
命令长度	命令长度	**2**	**B**	密文命令参数长度
	应用序列号	**10**	**Cn**	
	现场脱机支付余额	**4**	**B**	
	现场脱机支付联机交易序号	**2**	**B**	从**0x0000**开始；每次交易成功后自动加**1**；达到**0xFFFF**，再次成功交易成功后循环至**0x0000**。
	透支限额	**3**	**B**	
	刷卡记录	**64**	**B**	附录**B**记录**01**中包含的信息，从第**1**字节到第**64**字节
	报文流水号	**4**	**B**	参见《中国移动手机支付业务接口规范**--**手机支付服务平台与**(U)SIM**卡接口规范》
	随机数	**4**	**B**	
	MAC	**4**	**B**	

10.1.2 修改透支限额初始化响应

修改透支限额初始化响应如表**10-3**所示：

表**10-3** 修改透支限额初始化响应

项目	名称	长度（字节）	类型	说明
命令类型	修改透支限额初始化响应	**1**	**b**	取值**0x1F**
命令版本	命令版本	**1**	**b**	参见**10.1.1**节
命令长度	命令长度	**2**	**b**	命令参数长度
命令参数	应用序列号	**10**	**cn**	
	响应状态码	**2**		参见**5.2.5**节
	现场脱机支付余额	4		当且仅当响应状态码为“**0x9000**”时存在这些字段，参见**5.2.5**节。
	现场脱机支付联机交易序号	2		
	旧透支限额	3		
	密钥版本号	1		
	算法标识	1		
	伪随机数（(U)SIM卡）	4		
	MAC1	4		

	报文流水号	4	b	参见《中国移动手机支付业务接口规范--手机支付服务平台与(U)SIM卡接口规范》
	随机数	4	b	
	MAC	4	b	

10.1.3 修改透支限额响应

修改透支限额响应如表10-4所示：

表10-4 修改透支限额响应

项目	名称	长度（字节）	类型	说明
命令类型	修改透支限额响应	1	b	取值0x20
命令版本	命令版本	1	b	参见10.1.1节
命令长度	命令长度	2	b	命令参数长度
命令参数	应用序列号	10	cn	
	响应状态码	2		参见5.2.6节
	TAC	4		当且仅当响应状态码为“0x9000”时存在这些字段，参见5.2.6节。
	报文流水号	4	b	参见《中国移动手机支付业务接口规范--手机支付服务平台与(U)SIM卡接口规范》
	随机数	4	b	
	MAC	4	b	

10.2 下行报文

新增下行报文：

表10-5 下行报文

序号（十六进制）	命令类型
0x18	补登异地刷卡记录响应
0x19	修改透支限额初始化请求
0x1A	修改透支限额请求

10.2.1 上传异地未完成交易响应

上传异地未完成交易响应如表10-6所示：

表10-6 上传异地未完成交易响应

项目	名称	长度（字节）	类型	说明
命令类型	上传异地未完成交易响应	1	b	取值0x18

命令长度	命令长度	**2**	**b**	命令参数长度
命令参数	处理结果	**1**	**b**	**0x00**：成功； **0x01**：失败。
	现场脱机支付余额	**4**	**b**	
	现场脱机支付联机交易序号	**2**	**b**	
	透支限额	**3**	**b**	
	报文流水号	**4**	**b**	参见《中国移动手机支付业务接口规范--手机支付服务平台与(U)SIM卡接口规范》
	随机数	**4**	**b**	
	MAC	**4**	**b**	

若处理结果为**00**，**(U)SIM**卡扣除相应金额，删除异地刷卡记录，否则保留该记录。

10.2.2 修改透支限额初始化请求

修改透支限额初始化请求如表**10-8**所示：

表**10-8** 修改透支限额初始化请求

项目	名称	长度（字节）	类型	说明
命令类型	修改透支限额初始化请求	**1**	**b**	取值**0x19**
命令长度	命令长度	**2**	**b**	命令参数长度
命令参数	密钥索引号	1	**b**	
	终端机编号	6	**b**	全**0**
	报文流水号	**4**	**b**	参见《中国移动手机支付业务接口规范--手机支付服务平台与(U)SIM卡接口规范》
	随机数	**4**	**b**	
	MAC	**4**	**b**	

10.2.3 修改透支限额请求

修改透支限额请求如表**10-9**所示：

表**10-9** 修改透支限额请求

项目	名称	长度（字节）	类型	说明
命令类型	修改透支限额请求	**1**	**b**	取值**0x1A**
命令长度	命令长度	**2**	**b**	命令参数长度
命令参数	新透支限额	**3**	**b**	
	交易日期（发卡方）	**4**	**cn**	
	交易时间（发卡方）	**3**	**cn**	
	MAC2	**4**	**b**	
	报文流水号	**4**	**b**	参见《中国移动手机支付

	随机数	4	b	业务接口规范--手机支付服务平台与(U)SIM卡接口规范》
	MAC	4	b	

11 编制历史

版本号	更新时间	主要内容或重大修改
0.9.0	2009-7-1	0.9.0版本
	2009-7-11	新增透支限额功能 修改STK菜单 新增空中接口
	2009-7-13	修改手机支付应用的公共应用基本数据文件
	2009-7-15	新增异地异常处理流程 新增处理异地未完成交易响应 新增INITIALIZE FOR PURCHASE命令的补充说明
	2009-7-26	新增修改透支限额空中接口
	2009-8-1	修改下行报文命令类型取值
1.0.0	2009-8-5	1.0.0版本
	2009-08-11	附录中增加密钥版本号，交易类型标识。 补充说明透支情况下不允许修改透支限额，返回6985。 5.2.3，增加对多次接收UPDATE CAPP DATA CACHE命令的处理机制，要求支持至少2个UPDATE CAPP DATA CACHE命令的处理。
	2009-08-17	更新5.2.3 UPDATE CAPP DATA CACHE命令，扩展P1的取值来支持通过记录号来操作。
	2009-08-19	更新7.2.3，调整MAC1计算中参数交易金额、交易类型标识的位置，和电子钱包其他MAC1计算一致。
	2009-08-19	增加附录J 省编码 更新附录F,增加缺省的设置值
	2009-08-28	更新附录J，增加卡类型定义
	2009-9-15	10.1.1，上传异地未完成交易，应该先判断钱包真实余额是否满足“异地完成交易”的交易金额的扣款需求，如果钱包余额小于该交易

	金额，应不允许卡片发起该交易，直至用户补足相应的金额。在此情况，卡片应提示用户“钱包余额不足，请先进行钱包充值”。钱包真实余额是现场脱机支付余额减去透支限额。
2009-9-21	附录**A**， 增加运营企业代码，复合消费记录版本号缺省数值。
2009-9-28	更新修改历史信息，删除重复的附录**K**。

附录 A 复合应用说明

复合应用是本标准在《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》中的现场支付应用基础上，根据部分行业应用的特点而引入的一种新应用模式。

复合应用消费与现场脱机支付消费的主要差别在于前者增加了在消费交易中卡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。

本标准应保证复合应用数据在卡中存储的完整性和存取的安全性。

本标准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标准的范围内。

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 B 复合应用专用文件

表B-1：复合应用专用文件

文件标识（SFI）	0x19			
文件类型	变长记录文件			
文件大小				
文件存取控制	读=自由		改写=复合消费中	
记录号	字节	数据元	长度	格式
01	1	复合消费标志	1	BCD
	2	记录长度	1	HEX
	3	应用锁定标志位	1	HEX
	4	复合消费记录版本号	1	HEX
	5	交易类型	1	HEX
	6-11	终端机编号	6	BCD
	12-15	交易金额	4	HEX
	16-19	交易日期	4	YYYYMMDD
	20-22	交易时间	3	HHMMSS
	23-24	城市代码（终端机所属城市）（参见附录I）	2	BCD
	25	异地异常交易数据上传标志	1	HEX
	26-28	运营企业代码	3	BCD
	29-64	自定义数据	39	VAR
02	1	复合消费标志	1	BCD
	2	记录长度	1	HEX
	3	应用锁定标志位	1	HEX
	4-64	应用自定义数据	61	VAR

03~10	1-64	自定义数据	64	

- 复合应用专用文件的大小建议至少为1K。
- 复合消费记录01是全国公共交通行业应用记录，如果(U)SIM卡不属于本地卡片，则终端应使用本记录作为复合消费记录。记录中“复合消费标志”建议取值0x09。
- 复合消费记录02为地方公共交通行业应用记录。如果(U)SIM卡为本地卡片，则终端使用本记录作为复合消费记录。
- 消费记录03-10保留。
- 记录01中的交易类型字段取值：0x00-已完成交易（已出站），0x01-未完成交易（未出站）。
- 运营企业代码采用**BCD**编码，对于复合消费记录01中缺省设置为000001.
- 复合消费记录01中的复合消费记录版本号缺省设置为0x10，即1.0版本。

附录 C 复合应用消费交易举例

本节以手机支付现场脱机支付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。用户在进入收费区时，终端将在(U)SIM卡中写入特定信息；当用户离开收费区时，终端根据特定信息计算所需支付费用，并从现场脱机支付中扣除等额金额。

C.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C-1：

表C-1 复合应用记录格式

字段名	长度	字节
城市代码	2	1-2
运营企业代码	6	3-8
记录格式版本号	1	9
交易标志	1	10
进收费区交易时间	4	11-14
进收费区交易线路代码	1	15
进收费区交易站点代码	1	16
进收费区交易闸机代码	1	17
进收费区交易序号	4	18-21
出收费区交易时间	4	22-25
出收费区交易线路代码	1	26
出收费区交易站点代码	1	27
出收费区交易闸机代码	1	28
出收费区交易金额	3	29-32
出收费区交易序号	4	33-36
专用TAC	4	39-42

C.2 交易流程

C.2.1 增加复合应用类型

用户如需在特定应用环境中进行交易，需先在(U)SIM 卡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本标准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(U)SIM 卡后，由用户选择进入增加复合应用增加操作界面，终端向用户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。

当用户选择增加此特定复合应用后，终端使用 READ RECORD 命令查询(U)SIM 卡是否支持复合应用，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(U)SIM 卡已支持此特定复合应用，终端应提示用户。

如(U)SIM 卡支持复合应用，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 7.3.1 节在(U)SIM 卡中增加此特定复合应用，即创建以'13'为记录号的长度为 41 字节的记录，并将记录内所有字节初始化为 0。

C.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。

C.2.2.1 交易方式

用户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(U)SIM 卡，并通过 AID 选择进入手机支付应用目录。

终端发出 READ RECORD 命令查询复合应用，判断(U)SIM 卡是否支持复合应用，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，终端应提示用户。

如处理结果允许进行进收费区交易，终端根据 7.2 节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，终端应允许用户进收费区。

C.2.2.2 文件改写方式

用户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(U)SIM 卡，并通过 AID 选择进入手机支付应用目录。

终端发出 READ RECORD 命令查询复合应用，判断(U)SIM 卡是否支持复合应用，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，终端应提示用户。

如处理结果允许进行进收费区交易，则终端向(U)SIM 卡发出 GET CHALLENGE 命令获取(U)SIM 卡随机数，并利用随机数和消费密钥生成更改后的此特定复合应用专用数据 MAC。终端向(U)SIM 卡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，终端应允许用户进收费区。

C.2.3 出收费区交易

用户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(U)SIM 卡，并通过 AID 选择进入手机支付应用目录。

终端发出 READ RECORD 命令查询复合应用，判断(U)SIM 卡是否支持复合应用，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，终端应提示用户。

如处理结果允许进行出收费区交易，终端根据 7.2 节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，终端应允许用户出收费区。

附录 D 补充 APDU 指令

D.1 APPEND RECORD 命令

D.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。

D.1.2 命令报文

增加记录命令报文编码见表D-1：

表D-1 APPEND RECORD命令报文编码：

代码	值
CLA	‘04’
INS	‘E2’
P1	‘00’
P2	见表D-2
Lc	后续数据域的长度
Data	追加的新记录
Le	不存在

表D-2定义了命令报文中的引用控制参数P2：

表D-2 APPEND RECORD命令引用控制参数P2

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

D.1.3 命令报文数据域

命令报文数据域由追加的新记录组成。

D.1.4 响应报文数据域

响应报文数据域不存在。

D.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

(U)SIM卡可能回送的错误状态码如表D-3所示：

表D-3 APPEND RECORD命令可能回送的错误状态

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

D.2 READ RECORD 命令

READ RECORD命令在《中国移动手机支付业务接口规范--POS终端与(U)SIM卡接口分册》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。

READ RECORD命令报文中的引用控制参数在表D-4中定义：

表D-4 READ RECORD命令引用控制参数P2

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

附录 E 支持复合应用的手机支付 STK 菜单

参见《中国移动手机支付(U)SIM卡业务规范》附录A。

附录 F 手机支付应用的公共应用基本数据文件

表**F-1** 手机支付应用的公共应用基本数据文件

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	卡类型（**BCD**编码）	**1**
30	省编码（**BCD**编码）	**1**

其中，

发卡方标识：与**AID**中的**RID**部分数值相同，建议值为**D156000101**，**000000**，；

应用类型标识：与**AID**中行业编码数值相同，建议值为**0x38**

发卡方应用版本：发卡方应用版本设置为手机支付规范版本，且与手机支付规范版本保持同步，建议值为0x01；

应用序列号：由移动电子商务基地根据应用序列号编码规则分配；

卡类型： 0x00 — 个人用户卡；

0x01 — 行业用户卡；

0x02~0xFF — 其余为将来预留；

省编码：详见附件J。

附录 G 异地异常处理流程

用户因为某种原因在异地1未完成出站刷卡交易，即复合应用专用文件（SFI=0x19）的01记录中只保存有用户在异地1的进站刷卡交易。出现这种情况时，当用户前往异地2，进站时异地2的POS终端将01记录中的“异地异常交易数据上传标志”（第25字节）修改为“0x01”（正常情况下该标志位被设置为“0x00”），同时拒绝用户在异地2进站。相应的处理流程不在本标准的范围内定义。

当01记录中的“异常交易数据上传标志”（第25字节）为“0x01”时，用户可以通过STK查看到该笔异常交易，并可以选择处理该笔异常交易。当用户处理完成该笔异常交易，即若

处理异地未完成交易响应的处理结果为“**0x00**”，(U)SIM卡扣除相应金额，更新异地刷卡记录（将该标志位被设置为“0x00”），同时将交易类型（第5字节）设置为“0x00”。同时，手机支付服务平台向用户发送短信通知“该异常交易已完成”。

附录 H 现场脱机支付余额及透支处理流程

(U)SIM卡对透支功能的处理如下：

- (U)SIM卡在处理GET BALANCE命令时，当P2=’02’时（Le=’04’）(U)SIM卡返回真实余额（若真实余额小于0，返回0），当P2=’A0’时（Le=’07’）(U)SIM卡返回现场脱机支付余额和透支限额；
- (U)SIM卡在处理INITIALIZE FOR PURCHASE命令时，当命令数据中包含的消费金额大于(U)SIM卡内现场脱机支付真实余额时，(U)SIM卡返回’9401’（金额不足），否则(U)SIM卡在响应报文数据域中的现场脱机支付余额是真实余额与透支限额之和，透支限额为实际设定的透支限额；
- (U)SIM卡在处理INITIALIZE FOR LOAD命令时，(U)SIM卡在响应报文数据域中的现场脱机支付余额是真实余额与透支限额之和；
- (U)SIM卡在处理INITIALIZE FOR CAPP PURCHASE命令时，当命令数据中包含的消费金额大于(U)SIM卡内现场脱机支付余额时，(U)SIM卡返回’9401’（金额不足），否则(U)SIM卡在响应报文数据域中的现场脱机支付余额是真实余额与透支限额之和，透支限额为实际设定的透支限额；
- (U)SIM卡在计算MAC和TAC时，所有提及的现场脱机支付余额均指真实余额与透支限额之和。

附录 I 城市代码

《中国移动手机支付业务总体技术要求-总册及远程支付部分》中7.3.4.2.节描述了“现场脱机支付子账户”，该账户的N7-N9：地区标识，3位数字（地区区号去掉首位0；如只有两位，后补零，例：北京为“100”）。

本规范介绍的城市代码在上述**3**位数字前补**0**附录**J** 密钥版本号

密钥版本号缺省是0x01。

取值范围等其他要求参照《机支付业务接口规范--POS终端与(U)SIM卡接口分册(报批稿)》

附录 J 省编码

省区市	代码		省区市	代码	
	十进制	十六进制		十进制	十六进制

北京	01	0x01	河南	16	0x10
天津	02	0x02	湖北	17	0x11
河北	03	0x03	湖南	18	0x12
山西	04	0x 04	广东	19	0x 13
内蒙古	05	0x 05	广西	20	0x 14
辽宁	06	0x 06	海南	21	0x 15
吉林	07	0x 07	四川	22	0x 16
黑龙江	08	0x 08	贵州	23	0x 17
上海	09	0x 09	云南	24	0x 18
江苏	10	0x 0A	西藏	25	0x 19
浙江	11	0x 0B	陕西	26	0x 1A
安徽	12	0x 0C	甘肃	27	0x 1B
福建	13	0x 0D	青海	28	0x 1C
江西	14	0x 0E	宁夏	29	0x 1D
山东	15	0x 0F	新疆	30	0x 1E
			重庆	31	0x 1F

附录 K 密钥版本号

缺省值都是0x01

附录 L 交易类型标识

修改透支限额的交易类型标识取值为0x11。