中国移动通信
CHINA MOBILE

中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

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

Interface Specification for Mobile Payment Service between (U)SIM Cards and POS

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

本标准是对移动支付业务开展过程中POS终端与(U)SIM卡之间的接口提出全面要求，是使用该业务的依据。

本标准主要包括以下几方面内容：接口和传输协议、数据元、APDU命令、应用选择、安全机制、交易流程和现场脱机支付应用个人化指令流程。

本标准是手机支付业务系列标准之一。

序号	标准编号	标准名称
[1]		《中国移动手机支付业务规范-总册及远程支付部分》V1.0
[2]		《中国移动手机支付业务规范-现场支付部分》V1.0
[3]		《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》V1.0
[4]		《中国移动手机支付业务总体技术要求-现场支付部分》V1.0
[5]		《中国移动手机支付业务设备规范--手机支付服务平台设备部分（全国中心）》V1.0
[6]		《中国移动手机支付业务设备规范--手机支付服务平台设备部分（省）》V1.0
[7]		《中国移动手机支付业务设备规范-账户平台设备部分》V1.0
[8]		《中国移动手机支付业务设备规范-POS服务平台设备部分》V1.0
[9]		《NFC终端技术规范》V1.0
[10]		《中国移动手机支付业务现场脱机支付POS终端规范》V1.0
[11]		《中国移动手机支付SIM卡业务规范》V1.0（暂定）
[12]		《中国移动手机支付SIM卡设备规范》V1.0（暂定）
[13]		《中国移动手机支付业务PSAM卡规范》V1.0
[14]		《OTA支撑移动支付业务规范》V1.0（暂定）
[15]		《OTA支撑移动支付设备规范》V1.0（暂定）
[16]		《手机支付系统安全体系总体技术要求》V1.0
[17]		《手机支付系统安全技术规范 - 基础设施分册》V1.0
[18]		《手机支付系统安全技术规范 - 应用（业务）分册》V1.0
[19]		《手机支付系统密钥管理技术规范—现机支

付业务分册》V1.0

[20] 《手机支付系统密钥管理技术规范—POS服务系统分册》V1.0

[21] 《手机支付系统密钥管理技术规范—PSAM卡分册》V1.0

[22] 《手机支付系统密钥管理技术规范--OTA分册》V1.0

[23] 《手机支付系统密钥管理技术规范--用户卡分册》V1.0

[24] 《中国移动手机支付业务接口规范--POS终端与POS服务平台接口分册》V1.0

[25] 《中国移动手机支付业务接口规范--手机支付服务平台与POS服务平台接口分册》V1.0

[26] 《中国移动手机支付业务接口规范--手机支付服务平台与账户系统接口分册》V1.0（暂定）

[27] 《中国移动手机支付业务接口规范--手机支付服务平台与商户接口分册》V1.0（暂定）

[28] 《中国移动手机支付业务接口规范—中心平台与省平台接口分册》V1.0（暂定）

[29] 《中国移动手机支付业务接口规范--POS与（U）SIM卡接口规范》V1.0

[30] 《OTA支撑移动支付接口规范》V1.0（暂定） 本标准的附录B，附录C，附录D，附录E为标准性附录，附录A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：中国移动通信有限公司研究院 本标准主要起草人：李琳，乐祖晖，柏洪涛，陆鸣，刘斐，张雨廷，李征，朱本浩，郭漫雪

1. 范围

本标准规定了手机支付业务开展过程中POS终端与(U)SIM卡之间的接口，供中国移动内部和POS终端、(U)SIM卡厂商共同使用；适用于GSM/GPRS/3G网络环境。

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]	GSM 11.11	《 Digital cellular telecommunications system（Phase 2+）： Specification of the Subscriber Identity Module - Mobile Equipment （ SIM-ME ） interface （V8.3.0:2000）》	ETSI
[2]	GSM 11.14	《 Digital cellular telecommunications system（Phase 2+）：Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment （ SIM-ME ） interface （V8.3.0:2000）》	ETSI
[3]	TS 102.221	《 UICC-Terminal interface - Physical and logical characteristics（V7.5.0）》	ETSI 中国人
[4]		《中国金融集成电路（IC）卡电子钱包/电子存折规范第一部分：卡片规范》	民银行 中国
[5]		《中国金融集成电路（IC）卡电子钱包/电子存折规范第二部分：应用规范》	
[6]		《中国金融集成电路（IC）卡电子钱包扩展应用指南》	人民银行 中国人民银行
[7]	ISO/IEC 7816-3:1997	识别卡 带触点的集成电路卡 第3部分：电信号和传输协议	ISO
[8]	ISO/IEC	识别卡 带触点的集成电路卡 第4	ISO

	7816-4:1997	部分　行业间交易命令	
[9]	Q/CUP 007—2006	《中国银联POS终端规范》	中国银联股份有限公司
[10]	ISO/IEC 14443：1997	识别卡－非接触式集成电路卡－接近式卡	ISO
[11]		《中国移动SWP机卡接口规范》	中国移动通信有限公司
[12]		《中国移动手机支付业务现场脱机支付POS终端规范》	中国移动通信有限公司
[13]		《中国移动(U)SIM卡多应用管理技术规范》	中国移动通信有限公司
[14]		《手机支付系统密钥管理技术规范--用户卡分册》	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

词语	解释
AID	应用标识符（Application Identifier）
ATI	应用类型标识（Application Type Identifier）
an	字母数字型（Alphanumeric）
ans	字母数字及特殊字符型（Alphanumeric Special）
b	二进制（Binary）
CCPS	芯片卡支付服务（Chip Card Payment Service）
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）
L_c	终端发出的命令数据的实际长度（Exact Length of Data Sent）
L_e	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）
MF	主控文件（Master File）
n	数字型（Numeric）
P1	参数1（Parameter 1）
P2	参数2（Parameter 2）
PIN	个人密码（Personal Identification Number）

PIX	专用应用标识扩展码（Proprietary Application Identifier Extension）
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）
PSA	支付系统应用（Payment System Application）
PSE	支付系统环境（Payment System Environment）
PVV	PIN校验值（PIN Verification Value）
RFU	保留为将来使用（Reserved for Future Use）
RID	已注册的应用提供者标识（Registered Application Provider Identifier）
RSA	一种非对称加密算法（Rivest,Shamir,Adleman）
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 Crypogram）
TTI	交易类型标识（Transaction Type Identifier）
CCYYMMDD	年，月，日（Year, Month, Day）
3DEA	3倍DEA算法（Triple DES）
SWP	Single Wire Protocol
HCI	Host Control Interface
CAPP	复合应用（Complex Application）

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：

z 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。 z 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》。

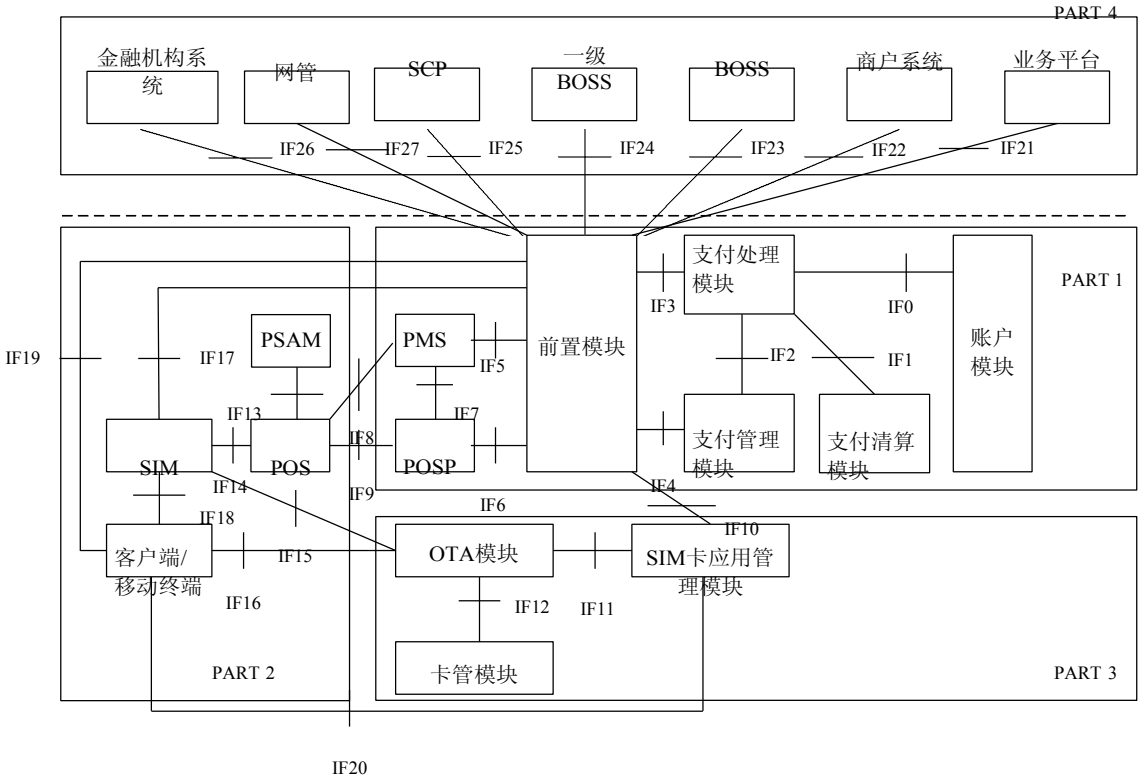


图4.1 手机支付系统结构图

5. 接口和传输协议

本标准描述的POS终端与(U)SIM卡之间的接口属于应用层接口，同具体的底层实现无关，不在本标准规范的范围内。

6. 数据元

(U)SIM卡中的每个应用都包括一系列信息项，在POS终端成功地完成应用选择后可以对这些信息进行访问（参见本标准第8章）。

一个信息项称为一个数据元，数据元是信息的最小单位，通过名称、逻辑内容说明、格式及代码来标识。

6.1 文件

数据文件中数据元以记录方式或二进制方式存储，文件结构及引用方式由文件的用途决定。除目录文件外，数据文件的结构和内容在应用规范中定义，也可由发卡方自行定义。

6.1.1 文件结构

本标准涉及的文件结构符合ISO/IEC 7816-4。 本标准描述了符合本标准的应用文件结构，这些应用被定义为支付系统应用（PSA）。

符合ISO/IEC 7816-4，但不符合本标准的其它应用也可以出现在(U)SIM卡上，并可以使用本标准中定义的命令进行操作。

(U)SIM卡中PSA的路径可以通过明确选择支付系统环境（PSE）来激活。如6.1.1.4节中描述的内容，成功选择PSE能够对目录结构进行访问。应用选择过程在本标准第7节中描述。

从POS角度来看，PSA相关的PSE文件呈一种可通过目录结构访问的树形结构。树的每一个分支是一个应用数据文件(ADF)。一个ADF是一个或多个应用基本文件(AEF)的入口点。一个ADF及其相关数据文件处于树的同一分支上。

6.1.1.1 应用数据文件（ADF）

ADF的树形结构：

—— 能够将数据文件与应用联系起来；

—— 确保应用之间的独立性；

—— 可以通过应用选择实现对其逻辑结构的访问。 从POS角度看，ADF是一个只包含其文件控制信息(FCI)中纯数据对象的文件。

6.1.1.2 应用基本文件（AEF）

一个AEF中包含有一个或多个原始基本编码规则——标签、长度、值(BER-TLV)数据对象。但在选择了某一应用后，AEF只能通过其短文件标识符(SFI)进行访问。

6.1.1.3 ISO/IEC 7816-4 文件结构中文件的映像

ISO/IEC 7816-4中使用下列映象表：

—— 包含一个FCI的专用文件(DF)(ISO/IEC 7816-4中定义)被映象为ADF，可以通过它来访问EF和DF。在卡中处于最高层的DF称为主控文件(MF)。

—— 包含一组记录中的基本文件(EF)(ISO/IEC 7816-4中定义)被映象为AEF，EF不能作为进入另一个不同DF文件的入口点。

在本标准中，DF中相连的EF的访问是透明的。

6.1.1.4 目录结构

SIM卡支持用于支付系统环境(PSE)应用列表的目录结构，PSE由发卡方通过目录选择。目录结构包括一个必备的支付系统目录文件(DIR文件)和一些可选的由目录数据文件(DDF)引用的附加目录。

目录结构采用以其应用标识符(AID)的方式进入一个应用,或以AID的前N个字节作为DDF名的方式进入一组应用。

在PSE选择的响应报文中对DIR文件进行编码(参见SELECT命令)。 DIR文件是一个AEF(换句话说，是一个记录结构的EF)，它包含ISO/IEC7816-5中定义的数据对象：

—— 本标准第6章中描述的一个或多个应用模板(标签为'61')；

—— 可能在目录自由模板中出现的其它数据对象(标签为'73')，此模板中包含的数据对象不在本标准中定义。

在SIM卡中支付系统外的其它目录是可选的，且不限制它们存在的数量。其中每个目录的位置由包括在每个DDF中的FCI的目录SFI数据对象指定。

6.1.1.5 (U)SIM 卡结构示例

图6.1给出了一个(U)SIM卡内部结构示例，该(U)SIM卡支持现场脱机支付应用、Easy entry以及两个没有定义的发卡方应用。图6.1仅仅是一个例子，可能有其它不限定应用数目的(U)SIM卡内部结构。

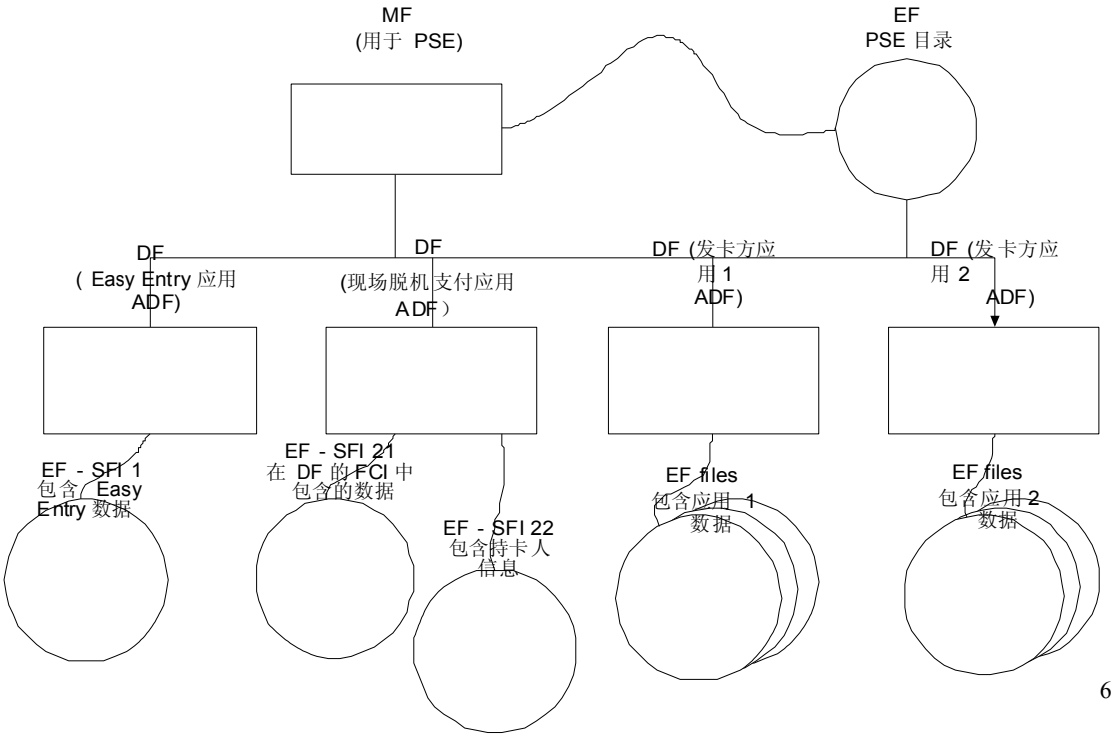


图6.1 (U)SIM卡内部结构示例

6.1.2 文件查询

6.1.2.1 通过文件名查询

(U)SIM卡中的任何ADF或DDF均可通过其文件名查询，ADF的DF名对应其AID，每个DF名在给定的(U)SIM卡中应是唯一的。

6.1.2.2 通过 SFI 查询

SFI用于选择AEF。对给定应用中的任何AEF，可以通过SFI(5位代码，取值范围从1～30)查询。SFI的编码在每个使用AEF的命令中描述。

在一个给定的应用中，SFI应是唯一的，专用SFI的使用由应用决定。

7. APDU 命令

7.1 概述

本节描述非接触交易POS终端与(U)SIM卡间基于现场脱机支付业务的命令和响应。 命令及其响应的报文格式在本规范本章节中逐一描述。 在应用执行过程中，(U)SIM卡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。(U)SIM卡具有的状态如下：

—— 空闲状态
—— 圈存状态
—— 消费状态
—— 修改状态 需要支持的命令包括：

- CHANGE PIN
- CREDIT FOR LOAD
- DEBIT FOR PURCHASE
- GET BALANCE
- GET CHALLENGE
- GET RESPONSE
- GET TRANSACTION PROVE
- INITIALIZE FOR LOAD
- INITIALIZE FOR PURCHASE
- READ BINARY
- READ RECORD
- RELOAD PIN
- SELECT

- UPDATE BINARY
- UPDATE RECORD
- VERIFY
- WRITE KEY POS需要支

持的命令包括：

GET CHALLENGE

- GET RESPONSE
- READ BINARY
- READ RECORD
- SELECT
- UPDATE BINARY
- UPDATE RECORD
- CREDIT FOR LOAD
- DEBIT FOR PURCHASE
- GET BALANCE
- GET TRANSACTION PROVE
- INITIALIZE FOR LOAD
- INITIALIZE FOR PURCHASE
- RELOAD PIN

WRITE KEY 完成应用选择后，(U)SIM卡首先进入空闲状态。当(U)SIM卡从POS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，(U)SIM卡将如表7-1所示进入另一个状态（或同一个）。如果命令执行不成功，则(U)SIM卡进入空闲状态。

表7-1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(U)SIM卡的当前状态，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。图7.1说明了SIM卡的状态，并描述每个命令执行后的状态转换关系。

阴影部分表示在(U)SIM卡处于相应状态时发出此命令是无效的。在这种情况下，(U)SIM卡不执行该命令，并向POS回送’6901’状态码，同时SIM卡的状态变为空闲。

表7-1 命令执行成功后SIM卡状态的变化

状态 命令	空闲	圈存	消费	修改
CREDIT FOR LOAD	N/A	空闲	N/A	N/A
DEBIT FOR PURCHASE	N/A	N/A	空闲	N/A
DEBIT FOR UNLOAD	N/A	N/A	N/A	N/A
GET BALANCE	空闲	圈存	消费	修改
GET TRANSACTION PROVE	空闲	圈存	消费	修改
INITIALIZE FOR LOAD	圈存	圈存	圈存	圈存
INITIALIZE FOR PURCHASE	消费	消费	消费	消费

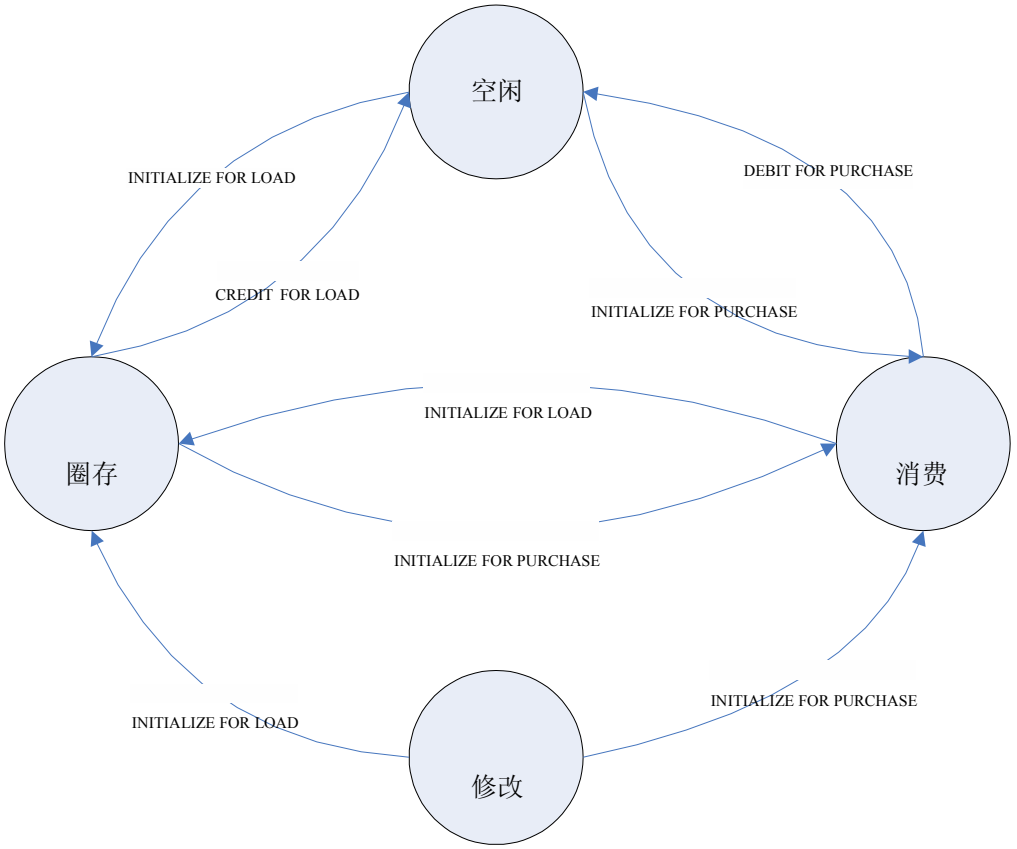


图7.1 SIM卡交易状态图

表7-2定义了命令报文的类别字节和指令字节的编码，以及现场脱机支付业务使用的参数P1和P2。

表7-2 命令的类别字节和指令字节

命　　令	CLA	INS	P1	P2
CHANGE PIN	‘80’	‘5E’	‘01’	‘00’
CREDIT FOR LOAD	‘80’	‘52’	‘00’	‘00’
DEBIT FOR PURCHASE	‘80’	‘54’	‘01’	‘00’
GET CHALLENGE	‘00’	‘84’	‘00’	‘00’
GET BALANCE	‘80’	‘5C’	‘00’	‘0X’
GET RESPONSE	‘00’	‘C0’	‘00’	‘00’
GET TRANSACTION PROVE	‘80’	‘5A’	‘00’	‘XX’
INITIALIZE FOR LOAD	‘80	‘50’	‘00’	‘0X’
INITIALIZE FOR PURCHASE	‘80’	‘50’	‘01’	‘0X’
RELOAD PIN	‘80’	‘5E’	‘00’	‘00’
READ BINARY	‘00’/ ‘04’	‘B0’	‘XX’	‘YY’
READ RECORD	‘00’/ ‘04’	‘B2’	‘XX’	‘YY’
SELECT	‘00’	‘A4’	‘XX’	‘YY’
UPDATE BINARY	‘00’/ ‘04’	‘D6’	‘XX’	‘YY’
UPDATE RECORD	‘00’/ ‘04’	‘DC’	‘XX’	‘YY’
VERIFY	‘00’	‘20’	‘00’	‘00’

命　　令	CLA	INS	P1	P2
WRITEKEY	‘84’	‘D4’	’XX’	‘00’

7.2 GET CHALLENGE 命令

7.2.1 定义和范围

GET CHALLENGE命令请求一个用于安全相关过程（例如：安全报文）的随机数。 该随机数用于后续指令，该随机数有效期一直到SIM卡接收到另外一条GET CHALLENGE命令。 在(U)SIM卡复位后，上次取的随机数失效。

7.2.2 命令报文

GET CHALLENGE命令报文编码见表7-3：

表7-3 GET CHALLENGE命令报文

代码	值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘04’或‘08’

7.2.3 命令报文数据域

命令报文数据域不存在。

7.2.4 响应报文数据域

响应报文数据域包括(U)SIM卡产生的随机数，长度为4字节或8字节。

7.2.5 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码如表7-4所示：

表7-4 GET CHALLENGE错误状态

SW1	SW2	含　　义
‘6A’	‘81’	不支持此功能

‘6A’	‘86’	参数P1 P2不正确
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误

7.3 GET RESPONSE 命令

7.3.1 定义和范围

本指令只用于T=0协议的(U)SIM卡。

当APDU不能用现有协议传输时，GET RESPONSE命令提供了一种从(U)SIM卡向接口设备传送APDU（或APDU的一部分）的传输方法。

7.3.2 命令报文

GET RESPONSE命令报文编码见表7-5：

表7-5 GET RESPONSE命令报文

代码	值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	响应的期望数据最大长度

7.3.3 命令报文数据域

命令报文数据域不存在。

7.3.4 响应报文数据域

响应报文数据域的长度由Le的值决定。 如果Le的值为零，在附加数据有效时，SIM卡必须回送状态码’6CXX’，否则回送状态码’6F00’。

7.3.5 响应报文状态码

此命令执行成功的状态码是’9000’。

表7-6列出正常处理情况：

表7-6 GET RESPONSE命令报文

SW1	SW2	含　　义

‘61’	‘XX’	正常处理
		‘XX’表示可以通过后续GET RESPONSE命令得到的额外数据长度

(U)SIM卡可能回送的警告状态码如表7-7所示：

表7-7 GET RESPONSE警告状态

SW1	SW2	含　义
‘62’	‘81’	回送的数据可能有错

(U)SIM卡可能回送的错误状态码如表7-8所示：

表7-8 GET RESPONSE错误状态

SW1	SW2	含　义
‘67’	‘00’	长度错误(Le 不正确)
‘6A’	‘86’	参数P1 P2不正确
‘6C’	‘XX’	长度错误(Le 不正确，’XX’表示实际长度)
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误
‘6F’	‘00’	数据无效

7.4 READ BINARY 命令

7.4.1 定义和范围

READ BINARY命令用于读取二进制文件的内容（或部分内容）。

7.4.2 命令报文

READ BINARY命令报文编码见表7-9：

表7-9 READ BINARY命令报文

代码	值
CLA	‘00’或’04’
INS	‘B0’
P1	见表7-10
P2	从文件中读取的第一个字节的偏移地址
Lc	不存在；(CLA=’04’时除外)
Data	不存在；(CLA=’04’时，应包括MAC)
Le	‘00’

表7-10定义了命令报文中的引用控制参数：

表7-10 READ BINARY命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　义
X 1								读取模式： -用SFI方式
	0	0						RFU(如果b8=1)

			X	X	X	X	X	SFI(取值范围21-30)

7.4.3 命令报文数据域

一般情况下,命令报文数据域不存在。当使用安全报文时,命令报文数据域中应包含MAC。MAC的计算方法和长度由应用决定。

7.4.4 响应报文数据域

当Le的值为零时，只要文件的最大长度在256(短长度)或65536(扩展长度)之内，则其全部字节将被读出。

7.4.5 响应报文状态码

此命令执行成功的状态码是'9000'。 (U)SIM卡可
能回送的警告状态码如表7-11所示：

表7-11 READ BINARY警告状态

SW1	SW2	含　　义
'62'	'81'	部分回送的数据可能有错
'62'	'82'	文件长度<Le

(U)SIM卡可能回送的错误状态码如表7-12所示：

表7-12 READ BINARY错误状态

SW1	SW2	含　　义
'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(非当前EF)
'6A'	'81'	不支持此功能
'6A'	'82'	未找到文件
'6A'	'86'	P1,P2不正确
'6B'	'00'	参数错误(偏移地址超出了EF)
'6C'	'XX'	长度错误(Le错误；'XX'为实际长度)
'6D'	'00'	INS不支持或错误
'6E'	'00'	CLA不支持或错误

7.5 READ RECORD 命令

7.5.1 定义和范围

READ RECORD命令用于读取记录文件的内容。
(U)SIM卡的响应由回送记录组成。

7.5.2 命令报文

READ RECORD命令报文编码见表7-13：

表7-13 READ RECORD命令报文

代码	值
CLA	‘00’或’04’
INS	‘B2’
P1	记录的个数
P2	引用控制参数(见表7-14)
Lc	不存在(CLA=’04’时除外)
Data	不存在(CLA=’04’时除外)
Le	‘00’

表7-14定义了命令报文中的引用控制参数：

表7-14 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为记录的个数

7.5.3 命令报文数据域

如果未使用安全报文，命令报文数据域不存在。使用安全报文时，命令报文的数据域中应包含MAC。MAC的计算方法和长度由应用决定。

7.5.4 响应报文数据域

所有执行成功的READ RECORD命令的响应报文数据域由读取的记录组成。

7.5.5 响应报文状态码

此命令执行成功的状态码是’9000’。 (U)SIM卡可能回送的警告状态码如表7-15所示：

表7-15 READ RECORD警告状态

SW1	SW2	含　义
‘62’	‘81’	回送的数据可能有错

(U)SIM卡可能回送的错误状态码如表7-16所示：

表7-16 READ RECORD错误状态

SW1	SW2	含　义
‘64’	‘00’	标志状态位没变
‘67’	‘00’	长度错误(Lc域不存在)
‘69’	‘81’	命令与文件结构不相容
‘6A’	‘81’	不支持此功能

‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘86’	P1,P2不正确
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误

7.6 SELECT 命令

7.6.1 定义和范围

SELECT命令通过文件名或AID来选择(U)SIM卡中的PSE、DDF或ADF。应用选择在本标准的第8节中描述。

命令执行成功后，PSE、DDF或ADF的路径被设定。 应用到AEF的后续命令将采用SFI方式联系到所选定的PSE、DDF或ADF。 从(U)SIM卡的响应报文应由回送FCI组成。

7.6.2 命令报文

SELECT命令报文编码见表7-17：

表7-17 SELECT命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表7-18）
P2	‘00’第一个或仅有一个 ‘02’下一个
Lc	‘05’-’10’
Data	文件名
Le	‘00’

表7-18命令报文中的引用控制参数：

表7-18 SELECT命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含 义
0	0	0	0	0				
					1			通过文件名选择
						0	0	

7.6.3 命令报文数据域

命令报文数据域应包括所选择的PSE名、DF名或AID。

7.6.4 响应报文数据域

响应报文中的数据域应该包括所选择的PSE、DDF或ADF的FCI。表7-19到表7-21规定了此定义了所用的标志。本标准不规定FCI中回送的附加标志。

表7-19定义了成功选择PSE后回送的FCI：

表7-19 SELECT PSE的响应报文 （FCI）

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

表7-20定义了成功选择DDF后回送的FCI：

表7-20 SELECT DDF的响应报文(FCI)

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

表7-21定义了成功选择ADF后回送的FCI：

表7-21 SELECT ADF的响应报文(FCI)

标　志	值	存在方式
‘6F’	FCI模板	M
‘84’	DF名	M
‘A5’	FCI专用数据	M
‘9F0C’	发卡方自定数据的FCI	O

表7-22定义了ADF回送的‘A5’中包含的数据，其中必须包含标签为’9F08’的应用版本号，其数值由中国移动负责定义和维护。

表7-22 SELECT ADF的应答报文中的FCI数据专用模板

‘A5’	FCI数据专用模板		M
	‘50’	应用标签	O
	‘87’	应用优先指示符	O
	‘9F08’	应用版本号	M
	‘9F12’	应用优先名称	O

7.6.5 响应报文状态码

此命令执行成功的状态码是’9000’。 (U)SIM卡可

能回送的警告状态码如表7-23所示：

表7-23 SELECT警告状态

SW1	SW2	含　义
‘62’	‘83’	选择的文件无效
‘62’	‘84’	FCI格式与P2指定的不符

SIM卡可能回送的错误状态码如表7-24所示：

表7-24 SELECT错误状态

SW1	SW2	含　义
‘64’	‘00’	标志状态位没变
‘67’	‘00’	P1 P2与Lc不一致
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	参数P1 P2不正确
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误
‘93’	‘03’	应用永久锁定

注：SW1 SW2=’6A82’用于表示当SIM卡支持部分文件名选择时，没有与此部分文件名相匹配的文件。

7.7 UPDATE BINARY 命令

7.7.1 定义和范围

UPDATE BINARY命令报文使用命令APDU中给定的数据修改EF文件中已有的数据。

7.7.2 命令报文

UPDATE BINARY命令报文编码见表7-25：

表7-25 UPDATE BINARY命令报文

代码	值
CLA	‘00’或‘04’
INS	‘D6’
P1	见表7-26
P2	要修改的第一个字节的偏移地址
Lc	后续数据域的长度
Data	修改用的数据+报文鉴别代码(MAC)数据元(4字节)
Le	不存在

CLA = ‘00’ 不需要安全报文。

CLA = ‘04’ 需要安全报文。

表7-26定义了命令报文中的引用控制参数：

表7-26 UPDATE BINARY命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　义
X 1								读取模式： -用SFI方式
	0	0						RFU(如果b8=1)
			X	X	X	X	X	SFI(取值范围21-30)

7.7.3 命令报文数据域

命令报文数据域：包括更新原有数据的新数据。 报文鉴别代码(MAC)数据元：4字节 MAC以及过程密钥的计算的方法参见本标准第9节和附录B。

7.7.4 响应报文数据域

响应报文数据域不存在。

7.7.5 响应报文状态码

此命令执行成功的状态码是'9000'。 (U)SIM卡可能回送的警告状态码如表7-27所示：

表7-27 UPDATE BINARY警告状态

SW1	SW2	含 义
'63'	'CX'	使用内部重试程序更新成功 X='0'表示不提供计数器 X≠'0'表示重试次数

(U)SIM卡可能回送的错误状态码如表7-28所示：

表7-28 UPDATE BINARY错误状态

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'	'84'	引用数据无效
'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'	'86'	P1,P2参数错误
'6B'	'00'	参数错误(偏移地址超出了EF)
'6D'	'00'	INS不支持或错误
'6E'	'00'	CLA不支持或错误
'93'	'03'	应用永久锁定

7.8 UPDATE RECORD 命令

7.8.1 定义和范围

UPDATE RECORD 命令报文用命令APDU中给定的数据更改指定的记录。

在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

7.8.2 命令报文

UPDATE RECORD 命令报文编码见表7-29：

表7-29 UPDATE RECORD命令报文

代码	值
CLA	‘00’ 或‘04’
INS	‘DC’
P1	P1=‘00’表示当前记录 P1≠‘00’指定的记录号
P2	见表7-30
Lc	后续数据域的长度
Data	更新原有记录的新记录+报文鉴别代码(MAC)数据元(4字节)
Le	不存在

CLA = ‘00’ 不需要安全报文。

CLA = ‘04’ 需要安全报文。

表7-30定义了命令报文中的引用控制参数：

表7-30 UPDATE 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	第一个记录
					0	0	1	最后一个记录
					0	1	0	下一个记录
					0	1	1	上一个记录
					1	0	0	记录号在P1中给出
其余值								RFU

7.8.3 命令报文数据域

命令报文数据域由更新原有记录的新记录和报文鉴别代码(MAC)数据元(4字节)组成。MAC以及过程密钥的计算的方法参见本标准第9节和附录B。

7.8.4 响应报文数据域

响应报文数据域不存在。

7.8.5 响应报文状态码

此命令执行成功的状态码是’9000’。 (U)SIM卡可能回送的警告状态码如表7-31所示：

表7-31 UPDATE RECORD警告状态

SW1	SW2	含 义
‘63’	‘CX’	使用内部重试程序更新成功 X=’0’表示不提供计数器 X≠’0’表示重试次数

(U)SIM卡可能回送的错误状态码如表7-32所示：

表7-32 UPDATE RECORD错误状态

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
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误

7.9 CREDIT FOR LOAD 命令

7.9.1 定义和范围

CREDIT FOR LOAD命令用于圈存交易。

7.9.2 命令报文

CREDIT FOR LOAD命令报文见表7-33：

表7-33 CREDIT FOR LOAD命令报文

代码	值
CLA	‘80’
INS	‘52’
P1	‘00’
P2	‘00’
L_c	‘0B’
Data	见表7-34
L_e	‘04’

7.9.3 命令报文数据域

表7-34描述了命令报文数据域：

表7-34 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

7.9.4 响应报文数据域

CREDIT FOR LOAD响应报文数据域见表7-35。 如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表7-35 CREDIT FOR LOAD响应报文数据域

说明	长度（字节）
TAC	4

7.9.5 响应报文状态码

此命令执行成功的状态码是'9000'。

表7-36描述了(U)SIM卡可能回送的错误状态：

表7-36 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

7.10 DEBIT FOR PURCHASE 命令

7.10.1 定义和范围

DEBIT FOR PURCHASE命令用于消费交易。

7.10.2 命令报文

DEBIT FOR PURCHASE命令报文见表7-37。 执行INITIALIZE FOR PURCHASE后即选择了消费交易。

表7-37 DEBIT FOR PURCHASE命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
L_c	‘0F’
Data	见表7-38
L_e	‘08’

7.10.3 命令报文数据域

表7-38描述了命令报文数据域：

表7-38 DEBIT FOR PURCHASE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

7.10.4 响应报文数据域

此命令执行成功的响应报文数据域如表7-39所示。 如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表7-39 DEBIT FOR PURCHASE响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

7.10.5 响应报文状态码

此命令执行成功的状态码是’9000’。

表7-40描述了(U)SIM卡可能回送的错误状态：

表7-40 DEBIT FOR PURCHASE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

7.11 GET BALANCE 命令

7.11.1 定义和范围

GET BALANCE命令用于读取现场脱机支付应用余额，实现查询余额交易。

7.11.2 命令报文

GET BALANCE命令报文见表7-41：

表7-41 GET BALANCE命令报文

代码	值
CLA	‘80’
INS	‘5C’
P1	‘00’
P2	‘02’ 其它值保留
L_C	不存在
Data	不存在
L_e	‘04’

7.11.3 命令报文数据域

命令报文数据域不存在。

7.11.4 响应报文数据域

命令执行成功的响应报文数据域见表7-42。 如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表7-42 GET BALANCE响应报文数据域

说明	长度（字节）
现场脱机支付余额	4

7.11.5 响应报文状态码

此命令执行成功的状态码是’9000’。

表7-43描述了SIM卡可能回送的错误状态：

表7-43 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

7.12 GET TRANSACTION PROVE 命令

7.12.1 定义和范围

GET TRANSACTION PROVE命令提供了一种在交易处理过程中出现交易中断，(U)SIM卡的恢复机制。

7.12.2 命令报文

GET TRANSACTION PROVE命令报文见表7-44：

表7-44 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7-45
Le	‘08’

7.12.3 命令报文数据域

表7-45定义了命令报文数据域：

表7-45 GET TRANSACTION PROVE命令报文数据域

说明	长度（字节）
要取的MAC或/和TAC所对应的现场支付联机或脱机交易序号。	2

7.12.4 响应报文数据域

如果命令中指定的交易类型标识和现场支付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7-46：

表7-46 GET TRANSACTION PROVE响应报文数据域

说明	长度
MAC	4
TAC	4

7.12.5 响应报文状态码

此命令执行成功的状态码是'9000'。

表7-47描述了SIM卡可能回送的错误状态：

表7-47 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

7.13 INITIALIZE FOR LOAD 命令

7.13.1 定义和范围

INITIALIZE FOR LOAD命令用于初始化圈存交易。

7.13.2 命令报文

INITIALIZE FOR LOAD命令报文见表7-48：

表7-48 INITIALIZE FOR LOAD命令报文

代码	值
CLA	'80'
INS	'50'
P1	'00'
P2	'02' 其它值保留。
L_c	'0B'
Data	见表7-49
L_e	'10'

7.13.3 命令报文数据域

表7-49定义了命令报文数据域：

表7-49 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

7.13.4 响应报文数据域

此命令执行成功的响应报文数据域见表7-50。 如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表7-50 INITIALIZE FOR LOAD响应报文

说明	长度（字节）
现场支付余额	4
现场支付联机交易序号	2
密钥版本号（DLK）	1
算法标识（DLK）	1
伪随机数（(U)SIM卡）	4
MAC1	4

7.13.5 响应报文状态码

此命令执行成功的状态码是'9000'。

表7-51描述了(U)SIM卡可能回送的错误状态：

表7-51 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
'69'	'86'	圈存后余额超过上限值
'6A'	'81'	功能不支持
'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

7.14 INITIALIZE FOR PURCHASE 命令

7.14.1 定义和范围

INITIALIZE FOR PURCHASE命令用于初始化消费交易。

7.14.2 命令报文

INITIALIZE FOR PURCHASE命令报文见表7-52：

表7-52 INITIALIZE FOR PURCHASE命令报文

代码	值
CLA	'80'

INS	‘50’
P1	‘01’
P2	‘02’ 其它值保留
L_c	‘0B’
Data	见表7-53
L_e	‘0F’

7.14.3 命令报文数据域

表7-53定义了命令报文的数据域：

表7-53 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

7.14.4 响应报文数据域

此命令执行成功的响应报文数据域见表7-54。 如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表7-54 INITIALIZE FOR PURCHASE响应报文数据域

说明	长度（字节）
现场支付余额	4
现场支付脱机交易序号	2
透支限额	3
密钥版本号（DPK）	1
算法标识（DPK）	1
伪随机数（SIM卡）	4

7.14.5 响应报文状态码

此命令执行成功的状态码是’9000’。

表7-55描述了(U)SIM卡可能回送的错误状态。

表7-55 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

7.15 RELOAD PIN 命令

7.15.1 定义和范围

RELOAD PIN命令用于发卡方重新给用户产生一个新的PIN（可以与原PIN相同）。

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（例如发卡方营业厅终端）上执行。

在成功执行RELOAD PIN命令后，(U)SIM卡必须完成以下操作：

—— PIN错误尝试计数器复位。

—— (U)SIM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。

业务密码设置的规定：

—— 旧密码错误的提示：要有提示

—— 新密码长度错误的提示：要有提示，或根本不允许输入错误长度

—— 新密码输入非法字符的提示：要有提示，或者手机控制不允许输入

—— 新密码或旧密码或确认密码为空的提示：要有提示，或根本不允许输入

—— 新密码与确认密码不符的提示：要有提示

—— 新密码或旧密码不可以允许含有*#

—— 密码显示不能为明文

7.15.2 命令报文

RELOAD PIN命令报文见表7-56：

表7-56 RELOAD PIN命令报文

代码	值
CLA	‘80’
INS	‘5E’
P1	‘00’
P2	‘00’
L_c	‘06’ ～ ‘0A’
Data	见表7-57
L_e	不存在

7.15.3 命令报文数据域

表7-57 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。现场脱机支付业务密码的长度是2~6字节，即4～12个ACSII数字。参见附录A数据元的解释。

7.15.4 响应报文数据域

响应报文数据域不存在。

7.15.5 响应报文状态码

此命令执行成功的状态码是'9000'。

表7-68描述了(U)SIM卡可能回送的错误状态：

表7-68 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、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

7.16 CHANGE PIN 命令

7.16.1 定义和范围

CHANGE PIN命令允许用户将当前个人密码修改为新的密码。

当CHANGE PIN命令成功完成后，(U)SIM卡要进行以下操作：

—— 密码尝试计数器复位至密码尝试次数的上限；

—— 将原个人密码置为新的个人密码。 此命令中的个人密码（PIN）值以明文方式传送。命令数据中个人密码（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'。

7.16.2 命令报文

CHANGE PIN命令报文见表7-59：

表7-59 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

7.16.3 命令报文数据域

参见表7-59。

7.16.4 响应报文数据域

响应报文数据域不存在。

7.16.5 响应报文状态码

此命令执行成功的状态码是’9000’。

表7-60描述了(U)SIM卡可能回送的错误状态：

表7-60 RELOAD 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、P2参数不正确
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误

7.17 VERIFY 命令

7.17.1 定义和范围

VERIFY命令用于校验命令数据域中的个人密码的正确性。 如PIN文件位于某一应用下，当此应用被锁定时，禁止校验PIN；如PIN文件位于MF下，
当应用被锁定后可以执行校验PIN命令。

7.17.2 命令报文

VERIFY命令报文编码见表7-61：

表7-61 VERIFY命令报文

代码	值
CLA	‘00’

INS	‘20’
P1	‘00’
P2	‘00’
Lc	可变
Data	外部输入的个人密码
Le	不存在

P2=’00’表示无特殊限定符被使用。在(U)SIM卡上，VERIFY命令在处理过程中应明确知道如何去寻找个人密码。

7.17.3 命令报文数据域

命令报文数据域由用户输入的个人密码组成。

7.17.4 响应报文数据域

响应报文数据域不存在。

7.17.5 响应报文状态码

此命令执行成功的状态码是’9000’。 当前的应用选择中，命令数据域中外部输入的个人密码与卡中存放的个人密码校验失败
时，IC卡将回送SW2=’Cx’，’x’表示个人密码允许重试的次数；当卡回送’C0’时，表示不能重试个人密码。此时再使用VERIFY命令时，将回送失败状态码SW1 SW2=’6983’。

(U)SIM卡可能回送的警告状态码如表7-62所示：

表7-62 VERIFY警告状态

SW1	SW2	含　义
‘63’	‘Cx ‘	校验失败，’x’表示允许重试的次数

(U)SIM卡可能回送的错误状态码如表7-63所示：

表7-63 VERIFY错误状态

SW1	SW2	含　义
‘64’	‘00’	标志状态位没变
‘69’	‘83’	认证方法(个人密码)锁定
‘69’	‘84’	引用数据无效
‘6A’	‘86’	参数P1 P2不正确
‘6A’	‘88’	未找到引用数据
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误

8.1.1WRITE KEY 命令

矩阵式密钥是为了便于实现密钥更新提供的密钥管理机制。该机制中，由密钥管理中心生成密钥矩阵，在密钥灌装过程中，在用户卡和PSAM卡内分别写入矩阵的一行和一列（分别以版本和索引作为行列标识），交易过程中通过交换版本和索引号，来确定实际使用的密钥。在密钥更新时，只需要将用户卡或PSAM卡内的一组密钥更新为新的一组，即可完成密钥的更新。

需要说明的是：本方案中只要求脱机消费密钥采用矩阵式管理，其它密钥采用单密钥的管理方式。

8.1.2 （U）SIM卡密钥属性要求

SIM卡应用通过密钥标识、索引、版本三个属性唯一定位一个密钥。

详细内容参考《中国移动手机支付系统密钥管理及算法使用技术规范—手机支付业务分册》。

8.1.2.1 密钥标识

各密钥用途长度为1字节。密钥标识约定如下：

密钥标识

密钥标识								含义
b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	1	0x01—应用主控密钥
0	0	0	0	0	0	1	0	0x02—应用维护密钥
0	0	0	0	0	0	1	1	0x03—消费密钥
0	0	0	0	0	1	0	0	0x04—充值密钥
0	0	0	0	0	1	0	1	0x05—TAC 密钥
0	0	0	0	0	1	1	0	0x06—PIN 重装密钥
0	0	0	0	0	1	1	1	0x07—空中报文保护密钥(不用）
0	0	0	0	1	0	0	0	0x08—透支限额密钥
0	0	0	0	1	0	0	1	0x09—PIN 解锁密钥

8.1.2.2 密钥索引

密钥索引，长度为 1 字节，范围 0x01-0xFF。各密钥索引值如下，其中，消费密钥需支持 10 个索引值，即 SIM 卡中需存储 10 个索引的消费密钥。

密钥索引

密钥类型	密钥索引
应用主控密钥	0x01
应用维护密钥	0x01
消费密钥	0x01～0x0A
充值密钥	0x01
TAC 密钥	0x01
PIN 重装密钥	0x01
透支限额密钥	0x01
PIN 解锁密钥	0x01

8.1.2.3 算法标识

算法标识指定了密钥所支持的加密算法，长度为1字节。算法标识约定如下：

密钥算法标识

值	含义
‘00’-‘7F’	为私有定义预留
‘80’	DES
‘81’	预留（3DES）
‘82’	3DES-CBC
‘83’	DES-ECB
‘84’	DES-CBC
‘85’-‘87’	为其他对称算法预留
‘88’	AES
‘89’-‘8F’	为其他对称算法预留
‘90’	HMAC-SHA1

8.1.2.4 密钥版本

密钥版本指定某种类型密钥的标识，长度为1字节，范围0x01-0x7F。

8.1.3 PSAM卡密钥属性要求

PSAM卡内的密钥属性要求如下：

8.1.3.1 密钥标识

各密钥标识长度为1字节，低5位为密钥类型，高3位为密钥分散级数。密钥标识约定如下：

密钥标识

密钥分散级数			密钥类型					含义
b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	0	0--主控密钥
0	0	0	0	0	0	0	1	1--维护密钥
0	0	0	0	0	0	1	0	2--消费密钥
0	0	0	X	X	X	X	X	其它—保留

8.1.3.2 密钥索引

密钥索引，长度为 1 字节，范围 0x01-0xFF。

应用密钥的密钥索引用途说明如下：

在脱机消费交易过程中，PSAM 卡将卡内消费密钥的索引值传递给 SIM 卡，SIM 卡采用该索引值检索卡内存储的一个或多个索引的密钥。PSAM 卡内的该索引值不用做自身的密钥检索参数。密钥索引的设置应在 SIM 卡脱机密钥的范围内。

所有密钥的索引初始值为 0x01。

8.1.3.3 算法标识

算法标识指定了密钥所支持的加密算法，长度为1字节。算法标识约定如下：

密钥算法标识

值	含义
‘00’-‘7F’	为私有定义预留
‘80’	DES
‘81’	预留（3DES）
‘82’	3DES-CBC
‘83’	DES-ECB

‘84’	DES-CBC
‘85’ - ‘87’	为其他对称算法预留
‘88’	AES
‘89’ - ‘8F’	为其他对称算法预留
‘90’	HMAC-SHA1

8.1.3.4 密钥版本

密钥版本，长度为1字节，范围0x01-0xFF。

PSAM卡与SIM卡交互过程中获取密钥版本号，PSAM卡应用从卡内存储的一个或多个版本的密钥中检索到指定的密钥。同时PSAM卡也利用该参数构造子密钥的分散参数。

PSAM卡应支持10个版本的消费密钥，版本号序列设置为0x01~0x0A。

密钥版本

密钥类型	密钥版本
消费密钥	0x01~0x0A

其它密钥的密钥版本初始值均为 0x01。

8.2 WRITE KEY 命令

WriteKey指令的命令报文域增加密钥索引号属性，即密钥密文信息是用主控密钥的会话密钥对以下数据加密（按所列顺序）产生的：

——密钥标识
——密钥版本
——密钥索引号
——密钥算法标识
——密钥值

8. 应用选择

本章从(U)SIM卡和POS终端两个角度描述了应用选择的过程。一方面描述了该过程所需的(U)SIM卡数据和文件的逻辑结构，另一方面描述了适应这种(U)SIM卡逻辑结构的终端逻辑。

POS终端按本章所描述的应用选择过程，根据这里所定义的协议使用(U)SIM卡上的数据来决定选择哪种支付应用进行交易，其过程分两个步骤：

—— 建立卡与终端两者共同支持的应用列表。

—— 在上述步骤生成的应用列表中选择一个将要运行的应用。 本章描述了为完成正确的应用选择所需要(U)SIM卡上的必要的信息以及两个POS终端选择算法。其它能够实现同样结果的POS终端选择算法可用来代替本章描述的算法。

应用选择通常是最先执行的应用功能。

一种支付系统应用包括以下内容：

—— (U)SIM卡上一组已由发卡方进行过客户化处理的数据文件。

—— 一组由收单行或商户提供的终端中的数据。

—— 一套卡和终端共同遵守的应用协议。 所有应用都唯一的由一个应用标识符(AID)标识。 这里描述的支付系统所采用的技术在设计上应能满足下列主要目标：

—— 能够支持多功能(U)SIM卡。

—— 能够支持多功能终端。而这些终端能够支持符合本标准的(U)SIM卡。

—— 符合ISO标准。

—— (U)SIM卡支持多应用，但不要求所有的应用都是支付应用。

—— 尽可能保护现存应用，使其与本标准定义的应用在卡中共存。

—— 最小的存储开销和处理开销。

—— 具有允许发卡方优化选择过程的能力。 终端使用SELECT命令选择一个应用数据文件(ADF),ADF中定义了(U)SIM卡中所支持某种应用的一组数据。

8.1 应用标识符的编码

应用标识符(AID)的结构符合ISO/IEC 7816-5，它包含两个部分：

1.一个经过注册的应用提供者标识符(RID)(长度为5字节)，它唯一地标识应用提供者。

2.一个可选域，由应用提供者定义，最长11字节。这个域被称为“专用应用标识符扩展码(PIX)”，其长度为0到11字节，其值由应用提供者确定。该域的含义只对应于特定的RID，不同RID下的PIX不需要唯一。

(U)SIM卡上允许存在其它应用提供者的应用数据文件(ADF)，但是其RID的定义应避免与支付应用RID的范围发生重复。可遵照ISO/IEC 7816-5中相关规定，以确保其编码不发生冲突。

8.2 支付系统环境结构

在(U)SIM卡上，支付系统环境起始于一个名为1PAY.SYS.DDF01的目录数据文件(DDF)。该文件是必须存在的。这个DDF被映射到卡中的某个DF，这个DF可以是MF，也可以不是。与其它DDF类似，这个DDF包含了支付系统的目录。该DDF的文件控制信息(FCI)中至少要包含本标准第二部分定义的所有DDF的信息，另外，还可以包含语言选择(标记'5F2D')和发卡方代码表索引(标记'9F11')。

初始DDF所附属的目录包含了ADF的入口地址，这些入口地址是符合本标准格式的。而这些ADF定义的应用既可以符合也可以不符合本标准。该目录也可以包含其它DDF的入口地址，但这些入口地址的格式必须符合本标准。

不要求该目录包含(U)SIM卡上所有的DDF和ADF的入口地址，也不要求沿着DDF的链接一定能够找到(U)SIM卡支持的全部应用。当然，只有从初始目录开始，沿着DDF的链接能够找到的应用，才具备国际互通性。

(U)SIM卡的内部逻辑结构的举例，见附件A。

8.3 支付系统目录编码

支付系统目录(下文简称目录)是一个线件文件，用1到10的短文件标识符(SFI)标识。该目录附属于DDF，目录的SFI包含在DDF文件控制信息中。目录可以使用本标准第二部分定义的READ RECORD命令进行读取。目录中一个记录可以包含几个入口地址，但一个入口地址不能跨越多个记录存储。

支付系统目录的每一个入口地址都是一个应用模板(标记'61')它应包含表8-1、表8-2和表8-3所示信息。

表8-1 DDF目录入口地址格式

标志	长度	值						存在方式
70	var.	结构数据对象标签						M
		61	var.	应用模板				M
				9D	5-16	DDF名称		M
				52	var.	执行的命令（7.4节）		O
				73	var.	目录自定义模板		O
					XXXX	var.	1个或多个由应用提供商、发卡行或(U)SIM卡供应商提供的附加（私有）数据元	O

表8-2 ADF目录入口地址格式

标志	长度	值						存在方式
70	var.	结构数据对象标示						M
		61	var.	应用模板				M
				4F	5-16	ADF名称（AID）		M
				50	1-16	应用标签		M
				9F12	1-16	应用优先名称		O
				87	1	应用优先表明符（见表81）		O
				52	var.	执行的命令（7.4节）		O
				73	var.	目录自定义模板		O
					XXXX	var.	1个或多个由应用提供商、发卡行或(U)SIM卡供应商提供的附加（私有）数据元	O

表8-3 应用优先表明符

b8	b7-b5	b4-b1	定义
1			需要用户确认方可选择应用
0			不需用户确认即可选择应用
	XXX		保留
		0000	未指定优先权
		XXXX (0000 除外)	应用的排列或选择顺序,从1-15,其中最高优先权为1

8.4 目录入口中“执行的命令”的使用

一个目录入口地址总是与卡中的一个数据文件(DF)相对应。如果在目录入口地址中没有指定一个“执行的命令”，则需执行SELECT命令(本标准第6章描述)来选择入口地址中指定的DF，并使用目录中ADF名或DDF名作为文件名。有些(U)SIM卡对SELECT命令的解释具有二义性，比如对于支持DF部分名的(U)SIM卡就有可能将其入口地址中指定的文件名当成另一DF文件的部分名而造成选择应用错误。

“执行的命令”作为一种机制提供给(U)SIM卡，使得(U)SIM卡可以利用这个机制准确地选择正确的DF，即选择与目录入口地址对应的DF。“执行的命令”可以是SELECT命令的变形，即不一定是“按名称选择”的形式(例如按路径或文件标识选择)；也可以是其它命令，通过这些命令也能实现正确选择DF的结果并返回FCI。当“执行的命令”数据项存在时，终端会利用它代替“按名称选择”命令来选择相关的DF。“执行的命令”数据项中采用的具体命令本标准不作规定。

8.5 其它目录的编码

除了初始目录之外，其它目录在支付系统环境下都是可选的，对此类目录的存在数目没有明确限制。每一个目录由一个目录SFI定位，SFI存放在每个DDF的FCI中。目录SFI包括执行READ RECORD命令读目录时所用的SFI。当包含该目录的DDF为当前选定的文件时，SFI可用来读此目录。

目录SFI数据应出现在一个DDF(FCI专用模板)的FCI专用数据区域内。一个DDF最多包含一个目录，因此目录SFI数据只在FCI中出现一次。

除了初始目录之外，所有目录入口均为ADF文件,或以包含目录DDF名称开始的DDF。所有目录(包括初始目录)的格式相同，详细描述请见7.3节。

8.6 终端的应用选择

终端中应存放终端所支持的应用及其对应的应用标识符(AID)列表。本章描述两种应用选择过程：一个适用于支持较少数量应用的终端；另一个适用于支持较多数量应用的终端。

8.6.1 直接选择应用

如果一个终端支持的应用不多，该终端可以简单地使用SELECT命令轮流选择每个应用。如果SELECT命令执行成功(回送SW1SW2='9000')，则该终端将它所支持的AID与被选择文件的FCI中的文件名进行比较，通过比较的结果来查证(U)SIM卡是否支持此应用。如果二者相匹配，(U)SIM卡支持该应用；如果返回的文件名比AID长而AID与返回文件名的起始部分相符，终端则重新发送SELECT命令并再次对选择进行验证；如果(U)SIM卡回送SW1SW2不等于'9000'，或者即使(U)SIM卡回送SW1SW2等于'9000'，而AID与文件名不相符且与文件名起始部分也不相符，证明卡不支持此应用。

一但终端支持的应用都被选择出来，则(U)SIM卡和终端都支持的应用列表就可以确定。然后终端可以选择指定的应用来运行。这一选择过程见7.6.3节。

直接选择适用于那些仅支持较少应用的终端，并且不能支持用户潜在的应用。这种方式不支持终端访问应用标签或应用优先名称，这些名称仅存在于目录中。

8.6.2 支付系统目录的使用

如果终端支持大量的应用,可以通过使用(U)SIM卡的目录(或多个目录)来确定(U)SIM卡所支持的应用。必须保证(U)SIM卡目录的结构设计正确，以便终端可以按照本标准描述的过程正确地选择应用。终端正确使用目录的步骤如下：

1.终端首先在支付系统环境下用本标准第7节中描述的“SELECT”命令对文件'1PAY.SYS.DDF01'直接选择。由此建立支付系统环境并进入初始目录。

2.终端从第一条记录开始，连续读目录中的所有记录，直到卡回送SW1SW2＝'6A83'，表示所需记录序号已不存在。在执行READ RECORD命令查找第一个记录时，如果卡回送SW1SW2＝'6A83'，则表示目录为空，转至下面步骤6。

3.如果目录中某个ADF名与终端支持的一个应用名相符，则将该应用列入最终应用选择的“候选名单”中。

4.如果目录中出现一个指向DDF的入口地址，且该DDF的名称至少与一个终端所支持的AID的前几位匹配(例如：一个名为1234的DDF可与一个名为12345678的AID匹配)，则终端选择该DDF。如果该入口包含一个“执行的命令”，则执行该命令完成选择；如果不存在“执行的命令”，终端发出带DDF名的SELECT命令。使用所选DDF的文件控制信息(FCI)中的目录短文件标识符(SFI)，读出目录并按规则3处理，之后终端继续回到上一个目录处理。

5.当终端处理完第一个目录的列表后，所有能够按此方式找到的ADF就确定了，查找完毕。

6.终端也可以采用其它方式寻找卡内其它的专用应用(例如:用AID找出本地的或非支付应用的专用选择方式)，但不在本标准范围之内。

8.6.3 选择应用并执行操作

当终端确定了卡与终端相互支持的应用列表之后，下一步即要选取某个应用进行操作。可通过如下方法实现：

1.如果没有互相支持的应用，交易终止。

2.如果只有一个相互支持的应用，终端核查应用优先表明符的b8位。如果b8等于‘0’，终端选择该应用。如果b8等于‘1’并且终端规定要有用户的确认，在这种情况下，终端需要向用户提出确认请求，如用户同意，即选择该应用。如果终端没有规定要有用户的确认，或者终端请求确认被拒绝，终端终止该交易。

3.建议显示应用列表请用户选择。将采用级别优先方式为用户提供应用列表目录，高优先级别的应用在先。如果卡中没有指定优先顺序，则以终端的应用优先顺序为准；如果终端也没有指定优先顺序，则按照应用在卡中出现的顺序为准。如果出现多个应用重复指定优先顺序，或个别入口地址缺少应用优先表明符的情况，也可采用类似的方法，也就是说，在这种情况下终端可使用自己的优先顺序,也可以按卡上顺序将有重复优先符或无优先符的应用显示出来。

4.终端可在没有用户协助的情况下选择应用。在这种情况下，终端应从相互支持的应用列表中选择优先级别最高的应用,如果终端不能对选择的应用提供确认,则应用选择禁止(应用优先表明符的b8等于‘1’)。

一旦终端或用户确定了待执行的应用，则该应用被选中。如果与应用相关的目录入口地址指定了一个“执行的命令”，终端执行该命令进行应用的选择。如果不存在“执行的命令”，终端发出一个“SELECT”命令(根据本标准第7节)进行应用的选择。无论使用哪种命令，如果命令回送的SW1SW2值≠‘9000’，则此应用将从候选列表中删除，之后再将删除后的列表显示给用户，或者选择下一个优先级高的应用，重新进行应用选择。在合适的情况下，终端要给用户以提示。

9. 安全机制

9.1 安全报文传送

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。数据完整性和对发送方的认证通过使用MAC来实现。数据的可靠性通过对数据域的加密来得到保证。

9.1.1 安全报文传送格式

本标准中定义的安全报文传送格式符合ISO 7816-4的规定。当CLA字节的第二个半字节等于十六进制数字'4'时，表明对发送方命令数据要采用安全报文传送。卡中的FCI表明某个命令的数据域的数据是否需要加密传输，是否应该以加密的方式处理。

表9-1 CLA字节第二个半字节编码

b4	b3	b2	b1	说　明
0	0	x	x	不需要安全报文
0	1	x	x	需要安全报文

9.1.2 报文完整性和验证

MAC是使用命令的所有元素(包括命令头)产生的。一条命令的完整性,包括命令数据域(如果存在的话)中的数据元,通过安全报文传送得以保证。

9.1.2.1 MAC 的位置

MAC是命令数据域中最后一个数据元。

9.1.2.2 MAC 的长度

本标准中，MAC的长度规定为4个字节。

9.1.2.3 MAC 的计算

参见附录B中解释。

9.1.3 数据可靠性

为保证命令中明文数据的保密性，可以将数据加密。所使用的数据加密技术，应被命令发送方和当前卡中被选择的应用所了解。

9.1.3.1 数据加密密钥的计算

在安全报文处理过程中用到的数据，加密过程密钥按照附录B中描述的方式产生。数据加密过程密钥的产生过程是从卡中的数据加密DEA密钥开始的。

9.1.3.2 被加密数据的结构

当命令中要求的明文数据需要加密时，它先要被格式化为以下形式的数据块：

—— 明文数据的长度，不包括填充字符(LD)

—— 明文数据
—— 填充字符(根据9.1.3.3的要求) 然后整个数据块使用
9.1.3.3中描述的数据加密技术进行加密。

9.1.3.3 数据加密计算

数据加密技术如下所述： 第一步：用LD表示明文数据的长度，在明文数据前加上LD产生新的数据块。 第二步：将第一步中生成的数据块分解成8字节数据块，标号为D1，D2，D3，D4等等。
最后一个数据块长度有可能不足8位。 第三步：如果最后(或唯一)的数据块长度等于8字节，转入第四步；如果不足8字节，在
右边添加16进制数字'80'。如果长度已达8字节，转入第四步；否则，在其右边添加1字节16进制数字'0'直到长度达到8字节。
第四步：每一个数据块使用9.1.3.3中描述的数据加密方式加密。 如果采用单长度数据加密DEA密钥，数据块的加密如图9.1所示(使用数据加密过程密钥
A进行加密)。

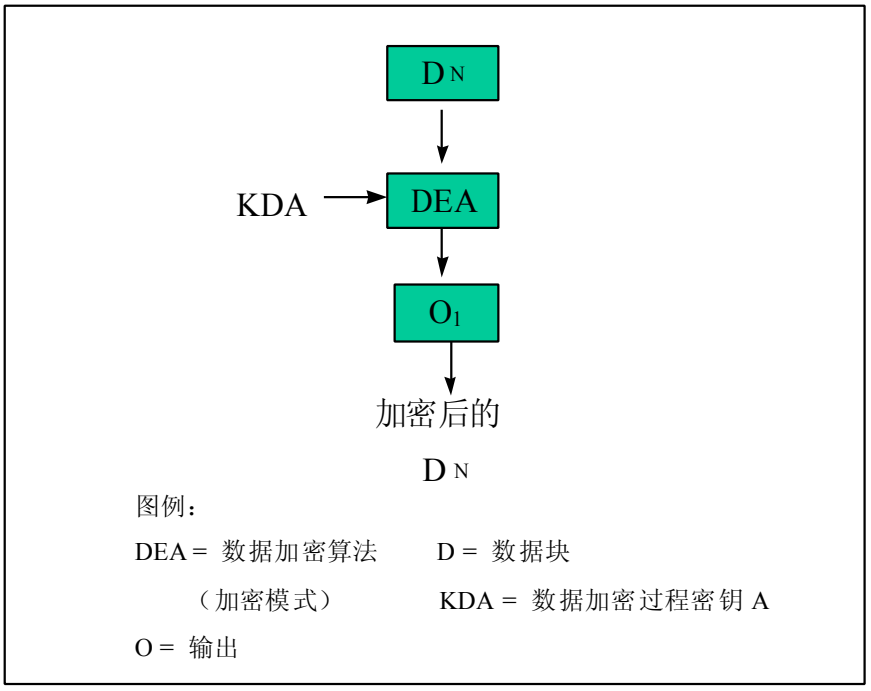


图9.1 单长度DEA密钥的数据加密

如果采用双长度数据加密DEA密钥，则数据块的加密如图9.2所示(使用数据加密过程密钥A和B来进行加密)。

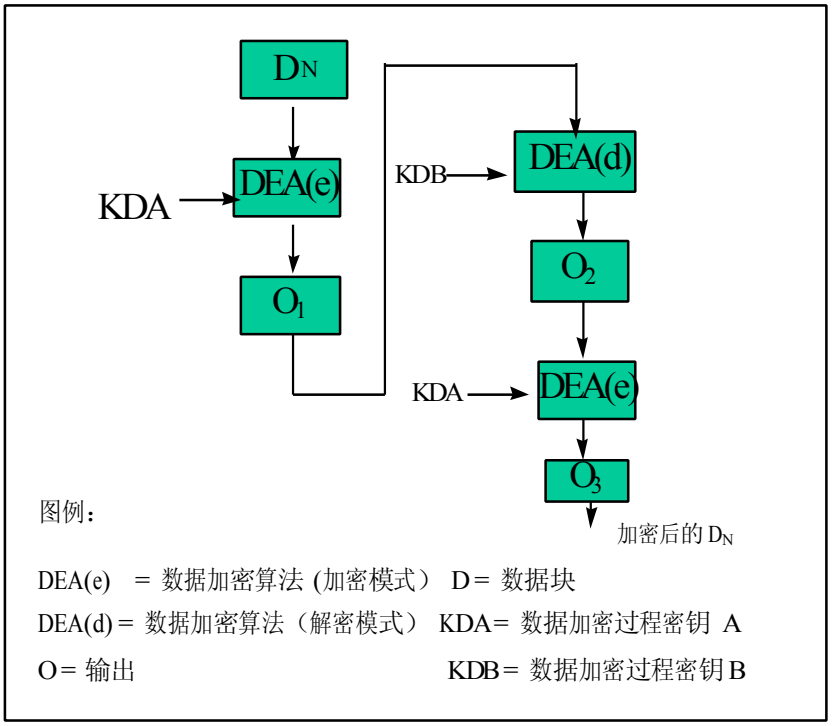


图9.2 使用双长度DEA密钥的数据加密

第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起(加密后的D1，加密后的D2，等等)。并将结果数据块插入到命令数据域中。

9.1.3.4 数据解密计算

(U)SIM卡接收到命令之后，需要将包含在命令中的加密数据进行解密。数据解密的技术如下：

第一步：将命令数据域中的数据块分解成8字节长的数据块，标号为D1，D2，D3，D4等等。每个数据块使用如9.1.3.3所描述的方法产生的数据加密过程密钥进行解密。

如果采用单长度数据加密的DEA密钥，数据块解密如图9.3所示(使用数据加密过程密钥A进行解密)。

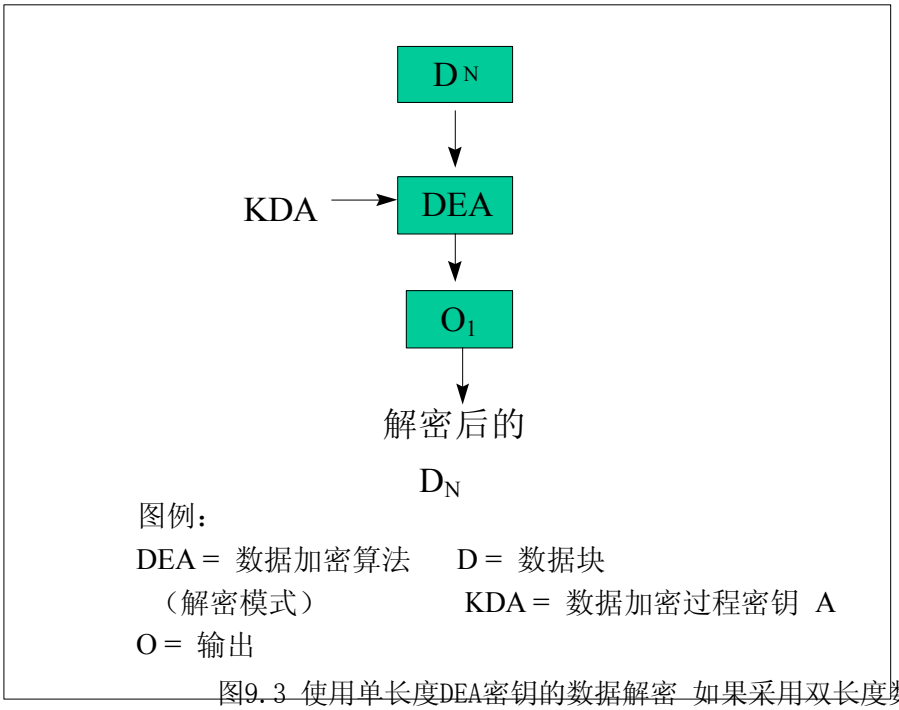


图9.3 使用单长度DEA密钥的数据解密 如果采用双长度数据加密的DEA密钥，则数据块的解密如图9.4所示(使用数据加密过程密钥 A和B来进行解密)。

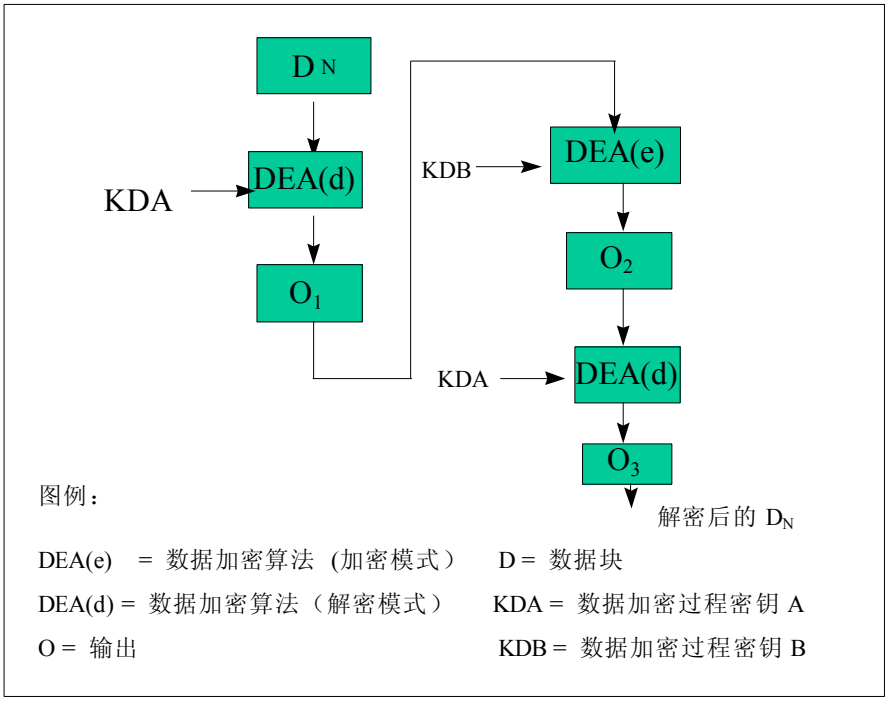


图9.4 使用双长度DEA密钥的数据解密

第二步：计算结束后，所有解密后的数据块依照顺序(解密后的D1，解密后的D2，等等)链接在一起。数据块由LD、明文数据、填充字符(如果在9.1.3.3描述的加密过程中增加的话)组成。

第三步：因为LD表示明文数据的长度，因此，它被用来恢复明文数据。

9.1.4 安全报文传送的命令情况

在ISO/IEC 7816-4中定义了四种命令情况。本节简单的讨论这些情况对命令APDU的作用。

情况一：这种情况时，没有数据送到ICC(Lc)中，也没有数据从卡中返回(Le)。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC

CLA的第二个半字节是'4'表明支持第二种情况的安全报文传送技术。Lc为MAC的长度。

情况二：这种情况时，命令中没有数据送到卡中，但有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC	Le

CLA的第二个半字节是'4'表明支持第二种情况的安全报文传送技术。Lc为MAC的长度。

情况三：这种情况时，命令中有数据传送到卡中，但没有数据从卡中返回。没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC

CLA的第二个半字节是'4'表明支持第二种情况的安全报文传送技术。Lc为命令数据加上MAC的长度。 情况四：这种情况时，在命令中有数据送到卡中，也有数据从卡中返回。没有安全报文

传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	Le

有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC	Le

CLA的第二个半字节是'4'表明支持第二种情况的安全报文传送技术。Lc为命令数据加上MAC的长度。

9.2 认可的加密算法

9.2.1 对称算法(DES)

安全报文允许使用64位块加密算法，该算法在ISO 8731-1、ISO 8732、ISO/IEC 10116中定义。以下定义的单DES加密和3-DES加密版本都可以用在第9.1节中描述的加密运算和MAC机制中。

3-DES加密是指使用双长度(16字节)密钥$K=(K_L||K_R)$将8字节明文数据块加密成密文数据块，如下所示：

$$Y = DES(K_L)[DES^{-1}(K_R)[DES(K_L)[X]]]$$

解密的方式如下：

$$X = DES^{-1}(K_L)[DES(K_R)[DES^{-1}(K_L)[Y]]]$$

9.3 现场支付应用涉及到的安全报文传送

当用于应用维护密钥（DAMK）时：

—— 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(U)SIM卡获得一个随机数。终端向(U)SIM卡发出一个GET CHALLENGE 命令）。从(U)SIM卡回送的随机数被送往主机以用于安全报文处理。

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

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

9.4 密钥管理概述

所有涉及到资金划转或修改(U)SIM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。

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

现场支付应用中(U)SIM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。(U)SIM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描述了现场支付应用所用的过程密钥的产生方式。

9.5 密钥管理

(U)SIM卡上的密钥必须安全存储。

表9-2描述了存储在(U)SIM卡上用于现场支付应用的密钥。

表9-2 (U)SIM卡中存储的用于现场支付应用的密钥

密钥	意义	用途
DPK	消费密钥。发卡方基于现场支付的应用序列号产生的一个双倍长密钥。	用来产生消费交易中使用的过程密钥(SESPK)。
DLK	圈存密钥。发卡方基于现场支付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。发卡方基于现场支付的应用序列号产生的一个双倍长密钥。	用来产生消费和圈存交易中使用的TAC。
DPUK	PIN解锁密钥。发卡方基于现场支付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、(U)SIM卡锁定和更新二进制命令的MAC。
应用主控子密钥	用于应用密钥保护的密钥。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。	用于应用密钥保护的密钥。
空中传输命令报文MAC子密钥	用于应用在空中传输指令MAC的密钥。发卡方基于应用序列号产生的一个双字节密钥。	用于应用在空中传输指令MAC的密钥。
空中传输命令报文子密钥	用于应用在空中传输指令中敏感数据加密的密钥。发卡方基于应用序列号产生的一个双字节密钥。	用于应用在空中传输指令中敏感数据加密的密钥。

10. 交易流程

本节描述了现场支付应用的交易流程，描述(U)SIM卡靠近POS终端并与终端相互作用后，所进行的交易处理过程。

消费交易要求终端必须具有安全存取模块（PSAM）。本规范假定终端和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－响应对。

10.1 交易预处理

图10.1给出了对现场支付应用的所有交易类型共有的预处理流程。

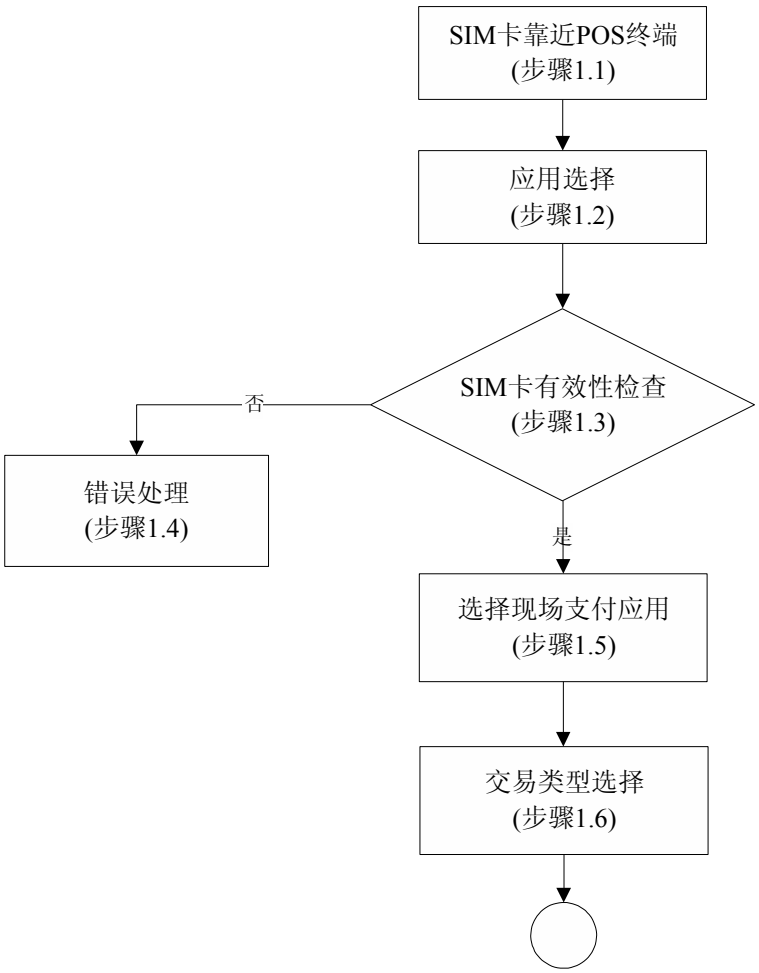


图10.1 交易预处理流程

10.1.1 (U)SIM 卡靠近 POS 终端（步骤 1.1）

终端应具有非接功能，能够检测(U)SIM卡是否已经进入有效工作区的功能。如果(U)SIM卡已经进入有效工作区，终端将继续执行10.1.2的应用选择功能。

10.1.2 应用选择（步骤 1.2）

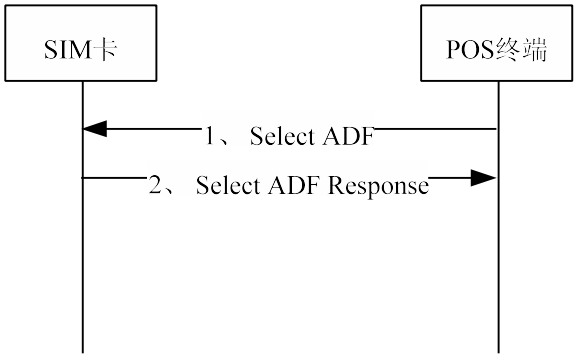


图10.2 应用选择处理流程

应用选择的执行过程请参见本标准第8节。现场支付应用的应用标识符（AID）将由中国移动负责分配和维护。 成功地选择了现场支付应用后，(U)SIM卡回送包含发卡方专用数据在内的文件控制信息。表10-1定义了此应用必备的发卡方专用数据

表10-1 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(U)SIM卡回送给终端。它标明现场支付应用在卡上的存在情况。

10.1.3 (U)SIM 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[1)] 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(U)SIM卡上的应用(使用应用类型标识（ATI）来检查)；

—— 终端是否支持从(U)SIM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；

—— 应用是否在有效期内。 如果以上任一条件不满足，交易将按10.1.4中的描述进行。

10.1.4 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规范的范围。

10.1.5 选择现场支付应用（步骤 1.5）

终端根据应用选择时获得的应用类型标识判别(U)SIM卡支持现场支付应用的情况。 如果(U)SIM卡和终端同时支持现场支付应用，则终端将自动地选择到现场支付应用，继而进行10.1.6中所描述的步骤。

10.1.6 交易类型选择（步骤 1.6）

终端应该具备让用户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。

注；[1)] 黑名单的详细情况，包括维护、格式、内容不在本规范范围之内。

对现场支付应用来说，用户应能选择如下交易类型：圈存、 消费、余额查询。

10.2 POS 圈存交易

通过圈存交易，用户可将其在手机支付主账户上的资金划入现场支付账户中。这种交易必须在营业厅终端上联机进行，但在POS圈存操作中不要求提交个人密码（PIN）。

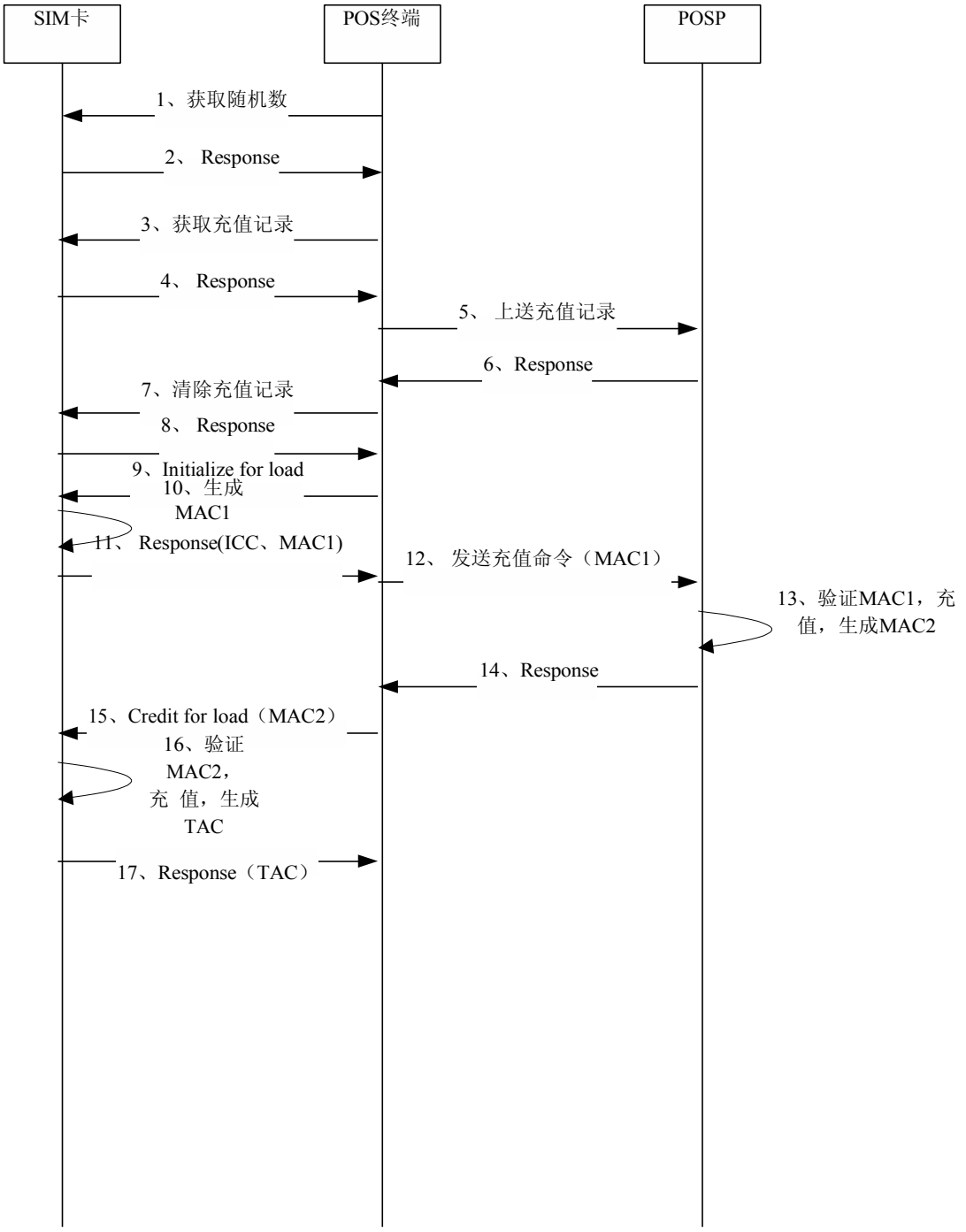


图10.3 POS圈存交易完整处理流程

10.2.1 POS 从(U)SIM 卡获取随机数

POS终端发送GET CHALLENGE命令获取随机数。命令描述遵照7.2节中的相应指令定义。

10.2.2 POS 从(U)SIM 卡获取充值记录

POS终端发送READ BINARY命令获取充值记录。命令描述遵照7.4节中的相应指令定义。读取附录C中的“未确认交易信息文件”。此时不需要MAC。 建议每次都读取整个文件内容，共70字节。

10.2.3 POS 上送充值记录

POS终端向POSP上送刚获取的充值记录（即未确认信息文件的内容）和随机数。

10.2.4 POS 接收清除充值记录指令

POS终端接收从POSP返回的清除(U)SIM卡充值记录命令（包括MAC）。

10.2.5 POS 清除(U)SIM 卡充值记录

POS终端发送UPDATE BINARY命令清除充值记录。命令描述遵照7.7节中的相应指令定义。

更新附录C中的“未确认交易信息文件”。此时需要MAC。 每次清除此文件内容，由POS机决定更新部分字节或所有70字节。当文件清空的时候使用全0格式。

10.2.6 发出 INITIALIZE FOR LOAD 命令（步骤 2.1）

终端应按本规范7.13节中定义的指令发出INITIALIZE FOR LOAD命令启动圈存交易。

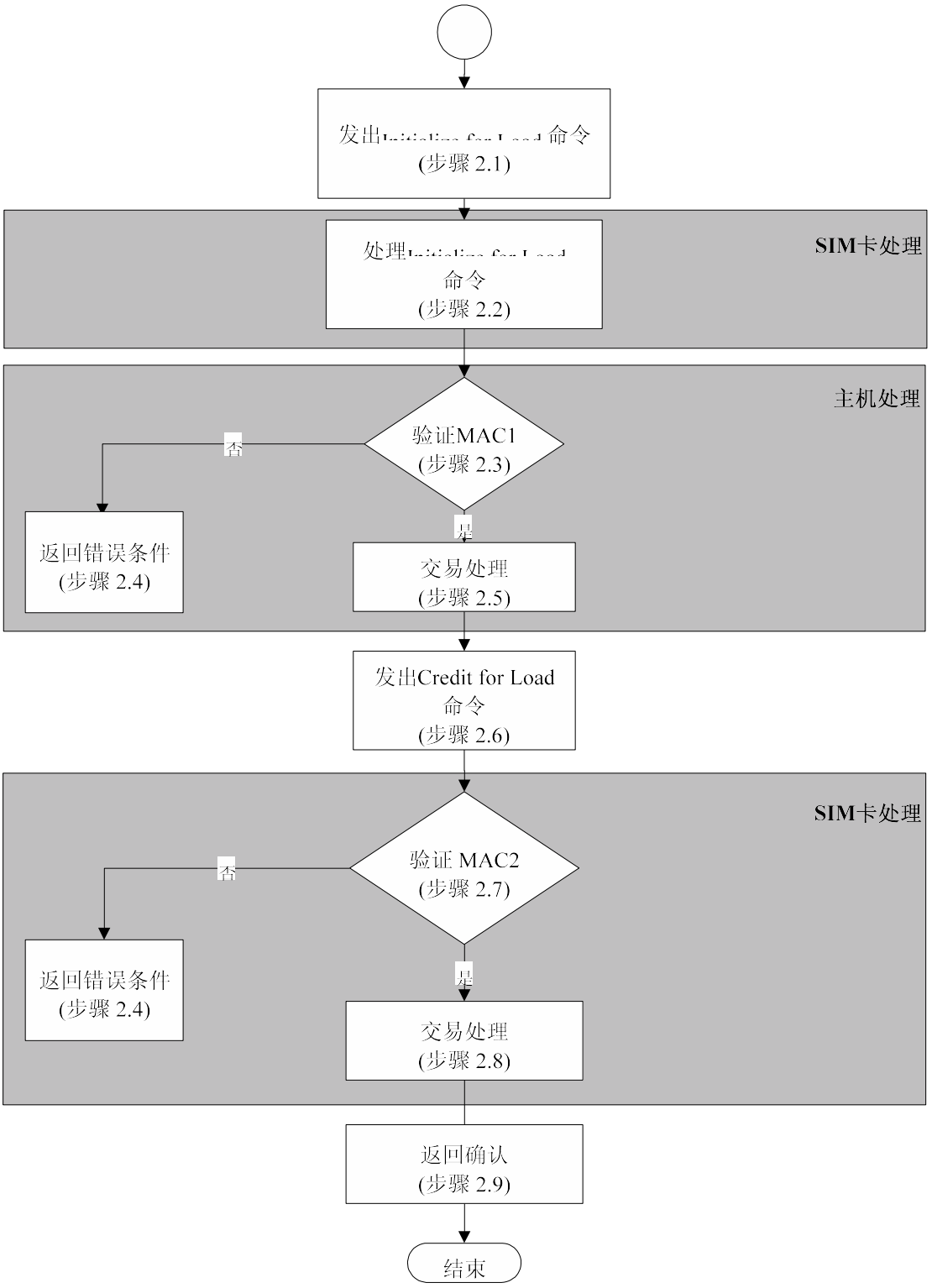


图10.4 圈存交易处理流程

10.2.7 处理 INITIALIZE FOR LOAD 命令（步骤 2.2）

收到INITIALIZE FOR LOAD命令后，(U)SIM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，则回送状态码‘9403’（不支持的密钥索引），但不回送任何其它数据，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(U)SIM卡的合法性。 SESLK是用于现场支付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）||现场支付联机交易序号||‘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):

—— 现场支付余额（交易前）

—— 交易金额

—— 交易类型标识

—— 终端机编号

(U)SIM卡将把本规范第7节中的相应指令定义中定义的INITIALIZE FOR LOAD响应报文回送给终端处理。如果(U)SIM卡回送的状态码不是‘9000’，则交易终止。

10.2.8 验证 MAC1（步骤 2.3）

收到INITIALIZE FOR LOAD命令响应报文后，终端把表7-50[1)] 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，交易处理将按本规范7.13中的相应指令定义中描述的步骤继续执行。否则，交易处理将执行图10.4所描述的步骤。

10.2.9 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规范范围内。

10.2.10 交易处理（步骤 2.5）

在确认能够进行圈存交易后，主机从用户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(U)SIM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，主机将现场支付联机交易序号加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）。

注：[1)] 包含在圈存认证请求报文中的其他信息不在本规范范围内。

10.2.11 发出 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CREDIT FOR LOAD命令更新卡上现场支付应用余额。CREDIT FOR LOAD命令见本规范7.9节中的相应指令定义中的描述。

10.2.12 验证 MAC2（步骤 2.7）

收到CREDIT FOR LOAD命令后，(U)SIM卡必须确认MAC2的有效性。如果MAC2有效,交易处理将执行上图中描述的步骤。否则将向终端回送状态码‘9302’（MAC无效）。终端对错误所应采取的相应措施不在本规范范围内。

10.2.13 交易处理（步骤 2.8）

(U)SIM卡将现场支付联机交易序号加1，并且把交易金额加在现场支付应用的余额上。(U)SIM卡必须成功地完成以上所有操作或者一个也不完成。

在现场支付圈存交易中，(U)SIM卡用以下数据组成的一个记录更新交易明细：

—— 现场支付联机交易序号
—— 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）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)：

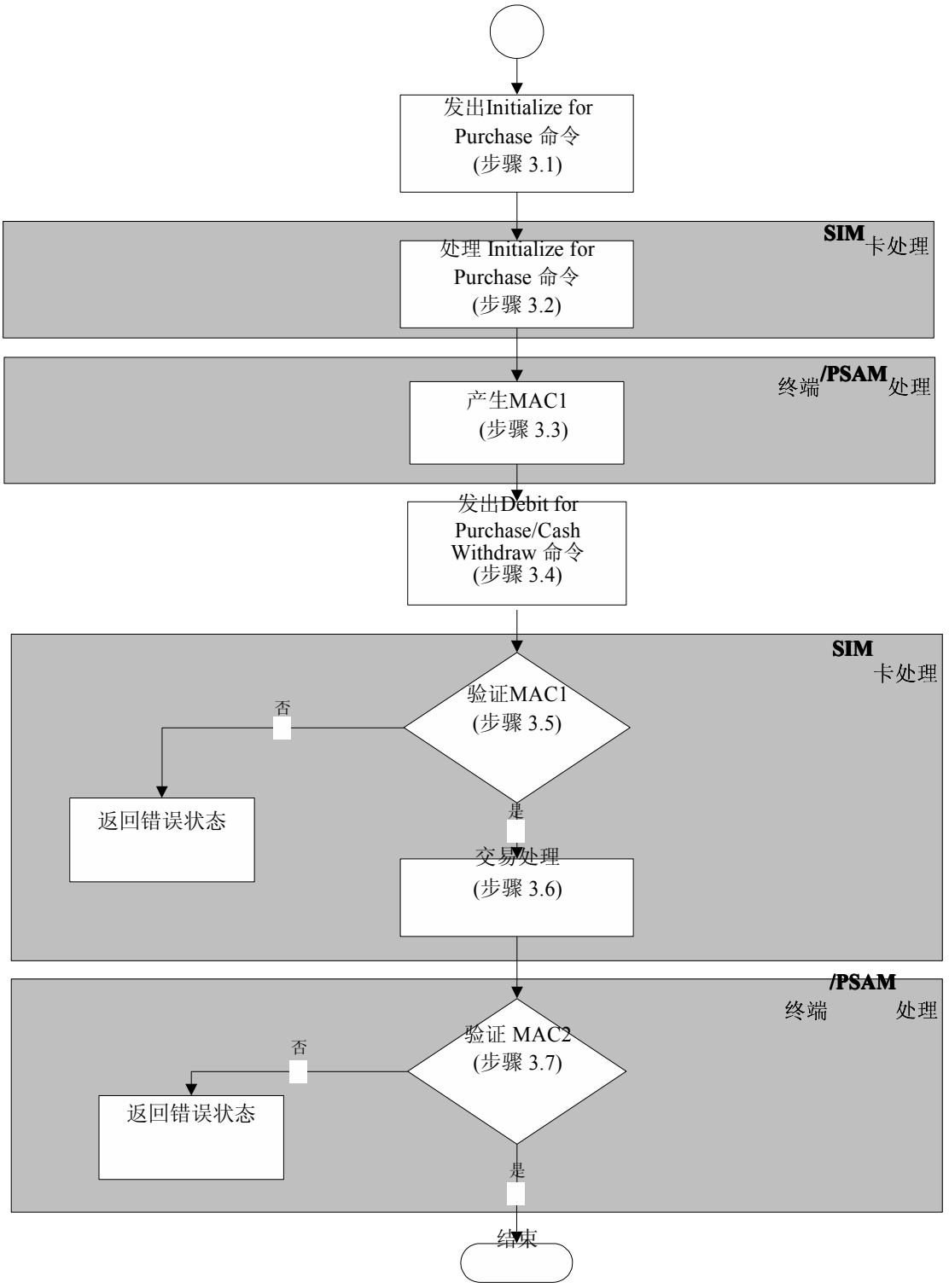
—— 现场支付余额（交易后）
—— 现场支付联机交易序号（加1前）
—— 交易金额
—— 交易类型标识
—— 终端机编号
—— 交易日期（主机）
—— 交易时间（主机）

10.2.14 返回确认（步骤 2.9）

在成功完成步骤2.8后,(U)SIM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。

10.3 消费交易

消费交易[1)] 允许用户使用现场支付应用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。使用现场支付不需要提交个人密码（PIN）。



注：[1)] 本规范仅提供脱机交易流程。

图10.5 消费交易处理流程

10.3.1 发出 INITIALIZE FOR PURCHASE 命令（步骤 3.1）

终端发出INITIALIZE FOR PURCHASE命令启动消费交易。

10.3.2 处理 INITIALIZE FOR PURCHASE 命令（步骤 3.2）

(U)SIM卡收到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，则回送状态码‘9403’（不支持的密钥索引），但不回送其它数据。

—— 检查现场支付应用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’（资金不足），但不回送其它数据。终端应采取的措施不在本规范的范围内。

在通过以上检查之后，(U)SIM卡将在10.3.5中产生一个伪随机数（ICC)和过程密钥用于验证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）||现场支付脱机交易序号||终端交易序号的最右两个字节

10.3.3 产生 MAC1（步骤 3.3）

使用伪随机数（ICC）和(U)SIM卡回送的现场支付脱机交易序号，终端的安全存取模块（PSAM）将产生一个过程密钥（SESPK）和一个报文认证码（MAC1），供(U)SIM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）

10.3.4 发出 DEBIT FOR PURCHASE 命令（步骤 3.4）

终端发出DEBIT FOR PURCHASE命令。

10.3.5 验证 MAC1（步骤 3.5）

在收到DEBIT FOR 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10.3.7中所描述的步骤。否则将向终端回送错误状态码‘9302’（MAC无效）。终端对错误状态的处理不在本规范范围内。

10.3.6 交易处理（步骤 3.6）

(U)SIM卡从现场支付应用余额中扣减消费的金额，并将现场支付脱机交易序号加1。(U)SIM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。

(U)SIM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 PURCHASE命令响应报文回送以下数据，作为PASM产生MAC2的输入数据。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 (U)SIM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。下面是用来生成TAC的数据，它们以明文形式通过CREDTE FOR PURCHASE命令的响应报文从(U)SIM卡传送到终端：

—— 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 (终端)
—— 交易时间 (终端) 对于现场支付消费交易（可选），(U)SIM卡将用以下数据组成的一个记录更新交易明细。
—— 现场支付脱机交易序号
—— 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)

10.3.7 验证 MAC2（步骤 3.7）

在收到(U)SIM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本规范的范围之内。

10.4 查询余额交易

用户可以通过终端或其它读卡设备读取现场支付应用中的余额，用户不需要提交个人密码（PIN）。

终端利用GET BALANCE命令实现查询余额交易。

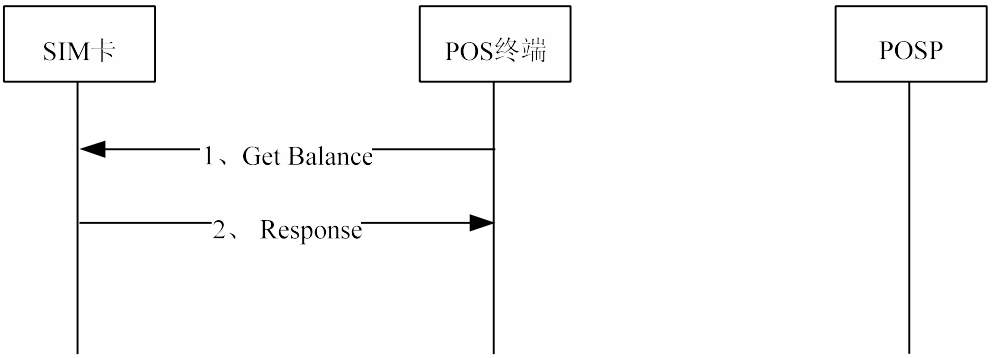


图10.6 POS查询余额处理流程

10.5 查询明细交易

用户可以通过终端或其它读卡设备读取(U)SIM卡中的交易明细记录。此交易一般采用脱机方式处理。交易时无需提交个人密码（PIN）。

终端发出一个READ RECORD命令（符合《中国金融集成电路(IC)卡规范》第1部分：卡片规范中“数据元和命令”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《中国金融集成电路(IC)卡规范》的要求，(U)SIM卡应支持在以下交易中记录明细：现场支付圈存交易、现场支付消费交易。

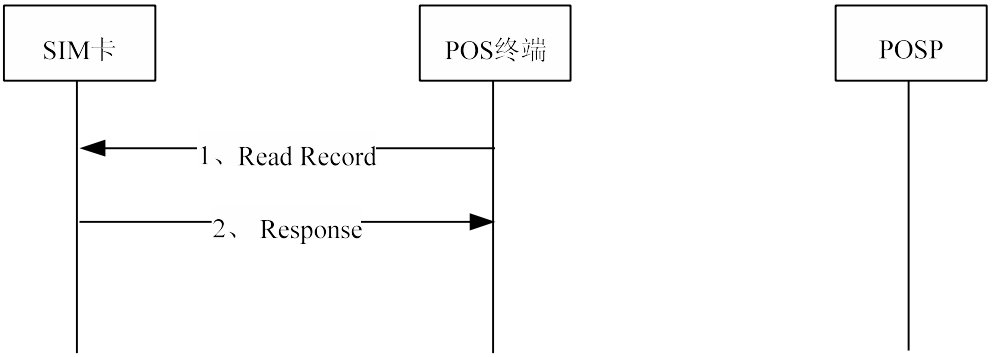


图10.7 POS查询明细处理流程

10.6 撤销交易

用户提供原交易客户凭条，操作员确认交易是本批次发生，操作员选择消费撤消交易并按照提示把手机放在读卡区。用户可以通过终端或其它读卡设备读取(U)SIM卡中的卡号信息。此交易一般采用联机方式处理。交易时无需提交个人密码（PIN）。

终端发出一个READ BINARY命令（符合《中国金融集成电路(IC)卡规范》第1部分：卡片规范中“数据元和命令”部分的规定）来获得卡号信息。这个命令会回送给POS终端现场支付的卡号相关信息,参见附录C中文件。

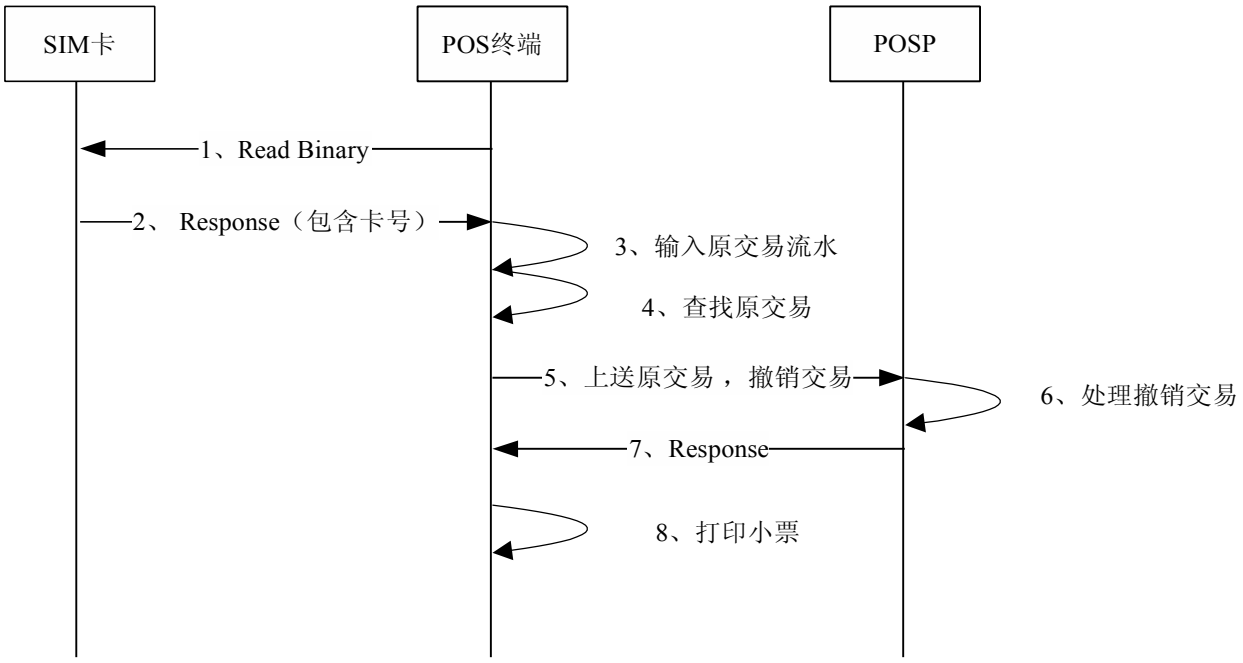


图10.8 撤销交易处理流程

10.7 退货交易

用户提供原交易客户凭条，操作原确认交易非本批次发生，需要退货处理。操作员选择退货交易并按照提示把手机放在读卡区。用户可以通过终端或其它读卡设备读取(U)SIM卡中的卡号信息。此交易一般采用联机方式处理。交易时无需提交个人密码（PIN）。

终端发出一个READ BINARY命令（符合《中国金融集成电路(IC)卡规范》第1部分：卡片规范中“数据元和命令”部分的规定）来获得卡号信息。这个命令会回送给POS终端现场支付的卡号相关信息,参见附录C中文件。

备注：退货不用在原POS上进行

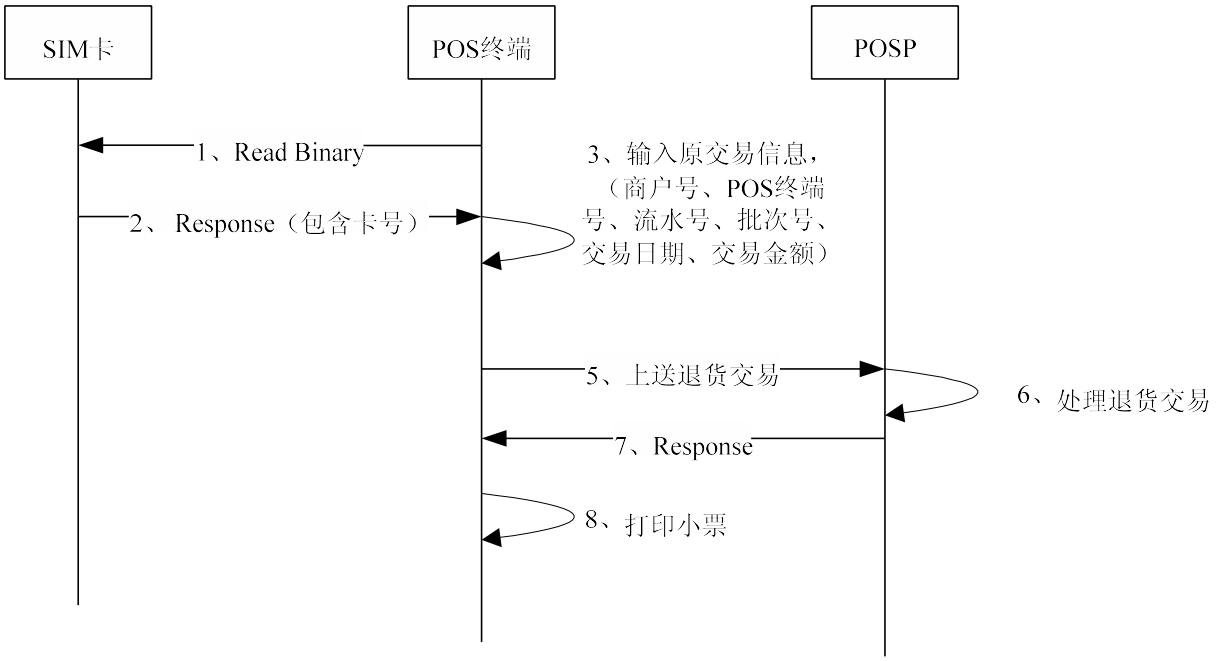


图10.9 退货交易处理流程

10.8 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。

10.8.1 卡片锁定

(U)SIM卡的锁定遵循《中国移动(U)SIM卡多应用管理技术规范》中卡片锁定状态的规定。

命令的成功执行使得(U)SIM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码“6A81”（功能不被支持）。

10.8.2 应用锁定

应用的锁定遵循《中国移动(U)SIM卡多应用管理技术规范》中应用锁定状态的规定。

此操作并不改变现场支付联机交易序号的值。

10.8.3 应用解锁

应用的解锁遵循《中国移动(U)SIM卡多应用管理技术规范》中应用锁定状态的规定。

此操作并不改变现场支付联机交易序号的值。

10.8.4 PIN 解锁

终端发出UNBLOCK PIN命令对PIN解锁，详细描述参见《中国金融集成电路(IC)卡规范》第1部分：卡片规范，有关安全要求见第2部分应用规范5.5.9.1。

在命令报文中，P2取‘01’值。使用DPUK对PIN数据加密（《中国金融集成电路(IC)卡规范》第1部分：卡片规范“安全机制”部分）。

如果PIN连续三次解锁失败，则(U)SIM卡将永久锁定此应用并回送状态码‘9303’（应用永久锁定）。

10.8.5 二进制形式修改

终端发出UPDATE BINARY指令。如果三次执行此命令均告失败，则(U)SIM卡将永久锁定此应用并回送状态码‘9303’（应用永久锁定）。

10.8.6 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(U)SIM卡接到此命令时，它将进行以下操作：

—— 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，(U)SIM卡回送状态码‘6983’（认证方式锁定）。

—— 如果PIN没有锁定，则命令中的‘当前PIN’会和(U)SIM卡上存放的PIN比较。如果二者相同，(U)SIM卡将进行以下操作：

a) 将(U)SIM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，(U)SIM卡将进行以下操作：

a) 将PIN尝试计数器减1；

b) 回送状态码‘63Cx’，这里x是PIN尝试计数器的新值。如达到零， 则(U)SIM卡自动锁定PIN。

10.8.7 重装 PIN

终端按照7.15节中的描述发出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。

版本号	更新时间	主要内容或重大修改
1.0.0	2009-01-23	