中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

中国移动一卡通业务接口规范
--RFID-SIM卡与消费终端接口分册

Interface Specification for E-Card Pass Service between RFID-SIM Cards and Purchase Terminals

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

本标准对一卡通业务开展过程中RFID-SIM卡与消费终端之间的接口提出要求，是开展一卡通业务的依据。

本标准主要包括以下几方面内容：文件和命令、安全机制、交易流程。

本标准是一卡通业务系列标准之一，该系列标准的结构、名称或预计的名称如下：

序号	标准编号	标准名称
[1]	QB-D-111-2009	《中国移动一卡通业务规范》V1.0
[2]		《中国移动一卡通业务总体技术要求》V1.0
[3]		《中国移动一卡通业务设备规范--一卡通业务系统部分》V1.0
[4]		《中国移动一卡通业务设备规范--一卡通企业端管理系统部分》V1.0
[5]		《中国移动一卡通业务设备规范—RFID-SIM卡应用部分》V1.0
[6]		《中国移动一卡通业务设备规范--SAM卡部分》V1.0
[7]		《中国移动一卡通业务终端设备规范--发卡终端部分》V1.0
[8]		《中国移动一卡通业务终端设备规范--门禁终端部分》V1.0
[9]		《中国移动一卡通业务终端设备规范--考勤终端部分》V1.0
[10]		《中国移动一卡通业务终端设备规范--消费终端部分》V1.0
[11]		《中国移动一卡通业务终端设备规范--充值终端部分》V1.0
[12]		《中国移动一卡通业务接口规范—业务系统与企业端管理系统接口分册》V1.0
[13]		《中国移动一卡通业务接口规范—RFID-SIM卡与业务系统接口分册》V1.0
[14]		《中国移动一卡通业务接口规范-- RFID-SIM卡与发卡终端接口分册》V1.0
[15]		《中国移动一卡通业务接口规范-- RFID-SIM卡与门禁终端接口分册》V1.0
[16]		《中国移动一卡通业务接口规范-- RFID-SIM卡与考勤终端接口分册》V1.0
[17]		《中国移动一卡通业务接口规范-- RFID-SIM卡与消费终端接口分册》V1.0

[18] 《中国移动一卡通业务接口规范-- RFID-SIM卡与充值终端接口分册》V1.0
[19] 《中国移动一卡通业务安全技术规范-总体要求》
[20] 《中国移动一卡通业务安全技术规范-密钥与算法要求》
[21] 《中国移动一卡通业务安全技术规范-密钥安全管理要求（一卡通业务系统）》
[22] 《中国移动一卡通业务安全技术规范-密钥安全管理要求（一卡通企业端管理系统）》
[23] 《中国移动一卡通业务安全技术规范-一卡通业务系统加密机设备要求》
[24] 《中国移动一卡通业务安全技术规范-密钥母卡设备要求》

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：乐祖晖、罗烽、任晓明、郭漫雪、李亚强

1．范围

本标准规定了一卡通业务开展过程中RFID-SIM卡与发卡终端之间的接口，供中国移动内部和消费终端、RFID-SIM卡厂商共同使用；适用于GSM/GPRS/TD-SCDMA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]		《中国移动一卡通业务规范》V1.0	中国移动通信有限公司
[2]		《中国移动一卡通业务总体技术要求》V1.0	中国移动通信有限公司
[3]		《中国移动一卡通业务设备规范—RFID-SIM卡应用部分》V1.0	中国移动通信有限公司
[4]		《中国移动一卡通业务接口规范—RFID-SIM卡与发卡终端接口分册》V1.0	中国移动通信有限公司

3．术语、定义和缩略语

“必须”、“推荐”/“建议”、和“可选”等词语在本规范中的使用需遵循以下指导。

- “必选”/“必须”项是指业务、产品和设备所必须提供的功能或性能要求；对应于RFC2119 MUST，REQUIRED，SHALL。
- “推荐”/“建议”/“应”项是指在标准中未作强制要求，若业务、产品和设备提供的功能或性能要求被认为更佳；对应于RFC2119 RECOMMENDED，SHOULD。
- “可选”/“可”项指参考性要求，是业务、产品和设备在目前阶段可不提供的功能或性能要求；对应于RFC2119 MAY，OPTIONAL。
- 必不能，不能，不得：表示绝对的禁止；对应于RFC2119 MUST NOT，SHALL NOT。
- 不推荐，不建议：表示若业务、产品和设备按照所述内容制作，被认为略次；对应于RFC2119 SHOULD NOT，NOT RECOMMENDED。

规范中除了明确指明为 “推荐”/“建议”、“可选”外，均为必须要求。

4．一卡通业务概述

4.1 业务概述

中国移动一卡通业务是以RFID-SIM卡为核心，以RFID非接触技术为基础，为中国移动的企业客户提供的包含门禁、考勤、内部消费、增值信息服务（如考勤账单通信、消费帐单通知等）等功能在内的企业信息化解决方案。

详细的业务描述定义参见《中国移动一卡通业务规范》V1.0.0。

4.2 系统结构图

一卡通业务系统结构图如图4.1所示，各网元的功能描述详见《中国移动一卡通业务总体技术要求》V1.0.0。

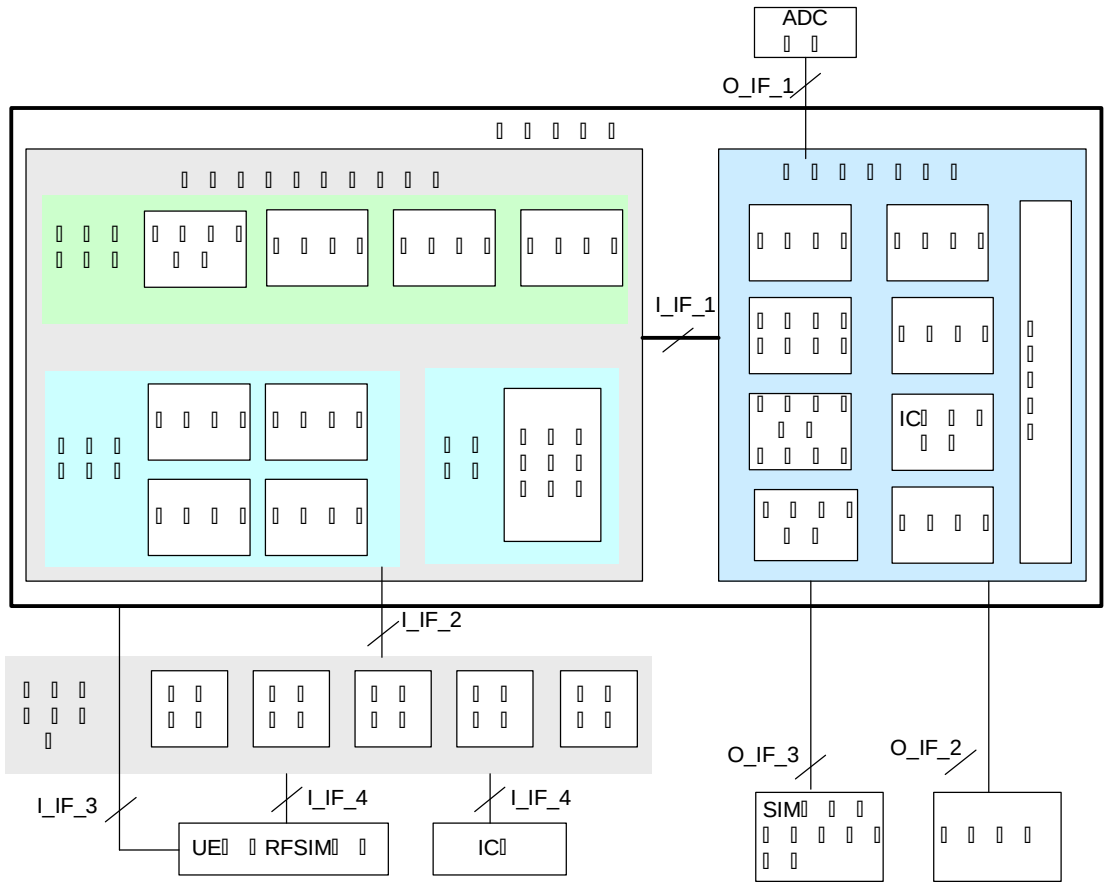

图4.1 一卡通业务系统结构图

5．文件和命令

本章描述RFID-SIM卡与消费终端间基于一卡通业务的命令和响应。

命令及其响应的代码约定和报文格式符合ISO/IEC 7816-4规范。

5.1 文件

5.2 APDU 命令

5.2.1 概述

常用APDU命令参见《中国移动一卡通业务接口规范--RFID-SIM卡与发卡终端接口分册》。

GET TRANSACTION PROVE命令参见《中国移动一卡通业务接口规范--RFID-SIM卡与充值终端接口分册》。

本规范只定义消费终端专用APDU指令。

5.2.2 INITIALIZE FOR PURCHASE 命令

5.2.2.1 定义和范围

INITIALIZE FOR PURCHASE命令用于初始化消费交易。

5.2.2.2 命令报文

INITIALIZE FOR PURCHASE命令报文见表5-1：

表5-1 INITIALIZE FOR PURCHASE命令报文

代码	值
CLA	‘80’
INS	‘7C’
P1	‘01’
P2	‘02’
L_c	‘12’
Data	见表5-2
L_e	‘2B’

5.2.2.3 命令报文数据域

表5-2定义了命令报文的数据域：

表5-2 INITIALIZE FOR PURCHASE命令报文数据域

说明	长度（字节）	取值
企业ID	6	
子应用索引号	1	

密钥索引号	1	’00’
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5-3。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表5-3 INITIALIZE FOR PURCHASE响应报文数据域

说明	长度（字节）
员工ID	20
员工企业流水号	4
钱包余额（或剩余使用次数）	4
钱包余额（或剩余使用次数）有效期	4
钱包脱机交易序号	2
透支限额	3
密钥版本号	1
算法标识	1
伪随机数（RFID-SIM卡）	4

5.2.2.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

表5-4描述了RFID-SIM卡可能回送的错误状态。

表5-4 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
‘93’	‘16’	企业ID错误
‘93’	‘17’	子应用索引号错误

5.2.3 DEBIT FOR PURCHASE 命令

5.2.3.1 定义和范围

DEBIT FOR PURCHASE命令用于消费交易。

5.2.3.2 **命令报文**

DEBIT FOR PURCHASE命令报文见表5-5。

表5-5 DEBIT FOR PURCHASE命令报文

代码	值
CLA	‘84’
INS	‘7E’
P1	‘01’
P2	‘00’
L_c	‘16’
Data	见表5-6
L_e	‘08’

5.2.3.3 **命令报文数据域**

表5-5描述了命令报文数据域（用于产生计算MAC1所需会话密钥的输入数据如下：伪随机数（RFID-SIM卡）||电子钱包脱机交易序号||终端交易序号的最右两个字节；计算MAC1的数据如下：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））：

表5-6 DEBIT FOR PURCHASE命令报文数据域

说明	长度（字节）
企业ID	6
子应用索引号	1
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如表5-7所示（计算TAC的密钥参见《中国移动一卡通业务安全技术规范-密钥与算法要求》；计算TAC的数据如下：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)。用于产生计算MAC2所需会话密钥同5.2.3.3节；计算MAC2的数据如下：交易金额。）。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表5-7 DEBIT FOR PURCHASE响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

5.2.3.5 响应报文的状态码

此命令执行成功的状态码是'9000'。

表5-8描述了RFID-SIM卡可能回送的错误状态：

表5-8 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
'93'	'16'	企业ID错误
'93'	'17'	子应用索引号错误

5.2.4 INITIALIZE FOR CANCEL 命令

5.2.4.1 定义和范围

INITIALIZE FOR CANCEL命令用于初始化脱机消费撤销交易。

5.2.4.2 命令报文

INITIALIZE FOR CANCEL命令报文见表5-9：

表5-9 INITIALIZE FOR CANCEL命令报文格式

代码	值
CLA	'80'
INS	'80'
P1	'00'
P2	'07'
L_c	'14'
Data	见表5-10
L_e	'2C'

5.2.4.3 命令报文数据域

表5-10定义了命令报文数据域：

表5-10 INITIALIZE FOR CANCEL命令报文数据域

说明	长度（字节）	取值
企业ID	6	

子应用索引号	1	
钱包脱机交易序号	2	
密钥索引号	1	‘00’
交易金额	4	
终端机编号	6	

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5-11(用于产生计算MAC1所需会话密钥的输入数据如下：伪随机数（RFID-SIM卡）||电子钱包脱机交易序号||’8000’；计算MAC1的数据如下：电子钱包余额（交易前）、交易金额、交易类型标识、终端机编号）。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表5-11 INITIALIZE FOR CANCEL响应报文数据域

说明	长度（字节）
员工ID	20
员工企业流水号	4
钱包余额（或剩余使用次数）	4
钱包余额（或剩余使用次数）有效期	4
钱包脱机交易序号	2
密钥版本号	1
算法标识	1
伪随机数（RFID-SIM卡）	4
MAC1	4

5.2.4.5 响应报文状态码

此命令执行成功的状态码是’9000’。

表5-12描述了RFID-SIM卡可能回送的错误状态：

表5-12 INITIALIZE FOR CANCEL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、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
‘93’	‘1A’	交易不存在或已失效
‘93’	‘16’	企业ID错误
‘93’	‘17’	子应用索引号错误

5.2.5 CREDIT FOR CANCEL 命令

5.2.5.1 定义和范围

CREDIT FOR CANCEL命令用于脱机消费撤销交易。

5.2.5.2 命令报文

CREDIT FOR CANCEL命令报文见表5-13：

表5-13 CREDIT FOR CANCEL命令报文格式

代码	值
CLA	‘84’
INS	‘82’
P1	‘00’
P2	‘01’
L_c	‘16’
Data	见表5-12
L_e	‘04’

5.2.5.3 命令报文数据域

表5-14描述了命令报文数据域(用于产生计算MAC2所需会话密钥同5.2.4.4节;计算MAC2的数据如下：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))：

表5-14 CREDIT FOR CANCEL响应报文格式

说明	长度（字节）
企业ID	6
子应用索引号	1
交易日期（终端）	4
交易时间（终端）	3
终端交易序号	4
MAC2	4

5.2.5.4 响应报文数据域

CREDIT FOR CANCEL响应报文数据域见表5-15（计算TAC的密钥参见《中国移动一卡通业务安全技术规范-密钥与算法要求》；计算TAC的数据如下：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)。）。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表5-15 CREDIT FOR CANCEL响应报文数据域

说明	长度（字节）
TAC	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5-16描述了RFID-SIM卡可能回送的错误状态：

表5-16 CREDIT FOR CANCEL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'	'11'	MAC错误
'93'	'16'	企业ID错误
'93'	'17'	子应用索引号错误

5.2.6 ONLINE PURCHASE 命令

5.2.6.1 定义和范围

ONLINE PURCHASE命令用于联机消费交易。

5.2.2.2 命令报文

ONLINE PURCHASE命令报文见表5-17：

表5-17 ONLINE PURCHASE命令报文

代码	值
CLA	'84'
INS	'86'
P1	'00'
P2	'07'
L_c	'24'
Data	见表5-18
L_e	'8'

5.2.2.3 命令报文数据域

表5-18定义了命令报文的数据域（用于产生计算MAC1所需会话密钥的输入数据如下：随机数（卡）||随机数（平台）；计算MAC1的数据如下：交易金额、交易类型标识、终端机编号、交易日期（平台）、交易时间（平台））：

表5-18 ONLINE PURCHASE命令报文数据域

说明	长度（字节）	取值
企业ID	6	
子应用索引号	1	
交易日期（平台）	4	
交易时间（平台）	3	
密钥索引号	1	’00’
交易金额	4	
终端机编号	6	
终端机交易流水号	3	
随机数（平台）	4	
MAC1	4	

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5-19（计算TAC的密钥参见《中国移动一卡通业务安全技术规范-密钥与算法要求》；计算TAC的数据如下：交易金额、交易类型标识、终端机编号、交易日期（平台）、交易时间（平台）。用于产生计算MAC2所需会话密钥同5.2.2.3节；计算MAC2的数据如下：交易金额。）。

如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表5-19 ONLINE PURCHASE响应报文数据域

说明	长度（字节）
MAC2	4
TAC	4

5.2.2.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

表5-20描述了RFID-SIM卡可能回送的错误状态。

表5-20 ONLINE 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
‘93’	‘02’	MAC无效
‘94’	‘03’	密钥索引不支持
‘93’	‘16’	企业ID错误
‘93’	‘17’	子应用索引号错误

5.2.7 ONLINE CANCEL 命令

5.2.7.1 定义和范围

ONLINE CANCEL命令用于联机撤销交易。

5.2.7.2 命令报文

ONLINE CANCEL命令报文见表5-21：

表5-21 ONLINE CANCEL命令报文

代码	值
CLA	‘84’
INS	‘88’
P1	‘00’
P2	‘08’
L_c	‘24’
Data	见表5-22
L_e	‘8’

5.2.7.3 命令报文数据域

表5-22定义了命令报文的数据域（用于产生计算MAC1所需会话密钥的输入数据如下：随机数（卡）||随机数（平台）；计算MAC1的数据如下：交易金额、交易类型标识、终端机编号、交易日期（平台）、交易时间（平台））：

表5-22 ONLINE CANCEL命令报文数据域

说明	长度（字节）	取值
企业ID	6	
子应用索引号	1	
交易日期（平台）	4	
交易时间（平台）	3	
密钥索引号	1	’00’
交易金额	4	
终端机编号	6	
终端机交易流水号	3	
随机数（平台）	4	
MAC1	4	

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5-23（计算TAC的密钥参见《中国移动一卡通业务安全技术规范-密钥与算法要求》；计算TAC的数据如下：交易金额、交易类型标识、终端

机编号、交易日期（平台)、交易时间（平台)。用于产生计算MAC2所需会话密钥同5.2.2.3节；计算MAC2的数据如下：交易金额。）。

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 ONLINE CANCEL响应报文数据域

说明	长度（字节）
MAC2	4
TAC	4

5.2.7.5 响应报文的状态码

此命令执行成功的状态码是'9000'。

表5-24描述了RFID-SIM卡可能回送的错误状态。

表5-24 ONLINE CANCEL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
'93'	'02'	MAC无效
'94'	'03'	密钥索引不支持
'93'	'16'	企业ID错误
'93'	'17'	子应用索引号错误

6. 安全机制

参见《中国移动一卡通业务安全技术规范-密钥与算法要求》。

7. 交易流程

7.1 交易预处理

交易预处理流程《中国移动一卡通业务接口规范--RFID-SIM卡与发卡终端接口分册》第7.1节。

7.2 脱机消费交易

脱机消费交易流程如图7.1所示：

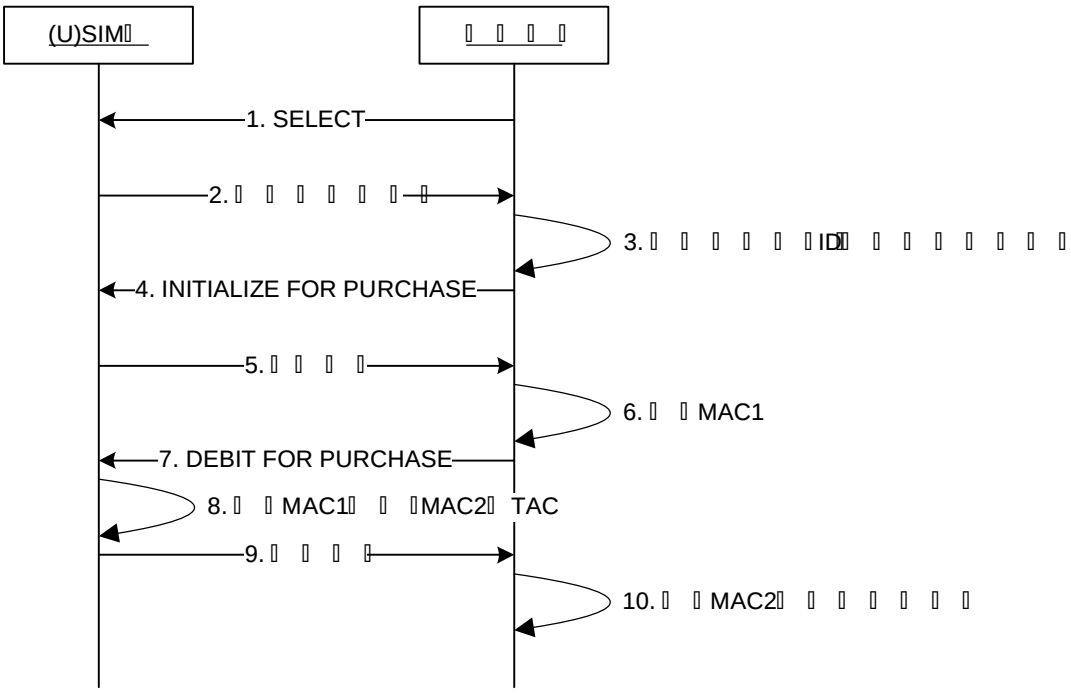

图7.1 脱机消费交易流程

1. 消费终端向RFID-SIM卡发送SELECT命令；
2. RFID-SIM卡向消费终端返回应用序列号；
3. 消费终端选择指定钱包；
4. 消费终端向RFID-SIM卡发送INITIALIZE FOR PURCHASE命令；
5. RFID-SIM卡向消费终端返回响应信息；
6. 消费终端生成MAC1；
7. 消费终端向RFID-SIM卡发送DEBIT FOR PURCHASE命令；
8. RFID-SIM卡校验MAC1是否有效，若无效流程结束，否则生成MAC2、TAC；
9. RFID-SIM卡向消费终端返回响应信息，包含MAC2、TAC；
10. 消费终端判断MAC2是否有效，同时保存交易记录，若MAC2无效给与报警。

7.3 联机消费交易

联机消费交易流程如图7.2所示：

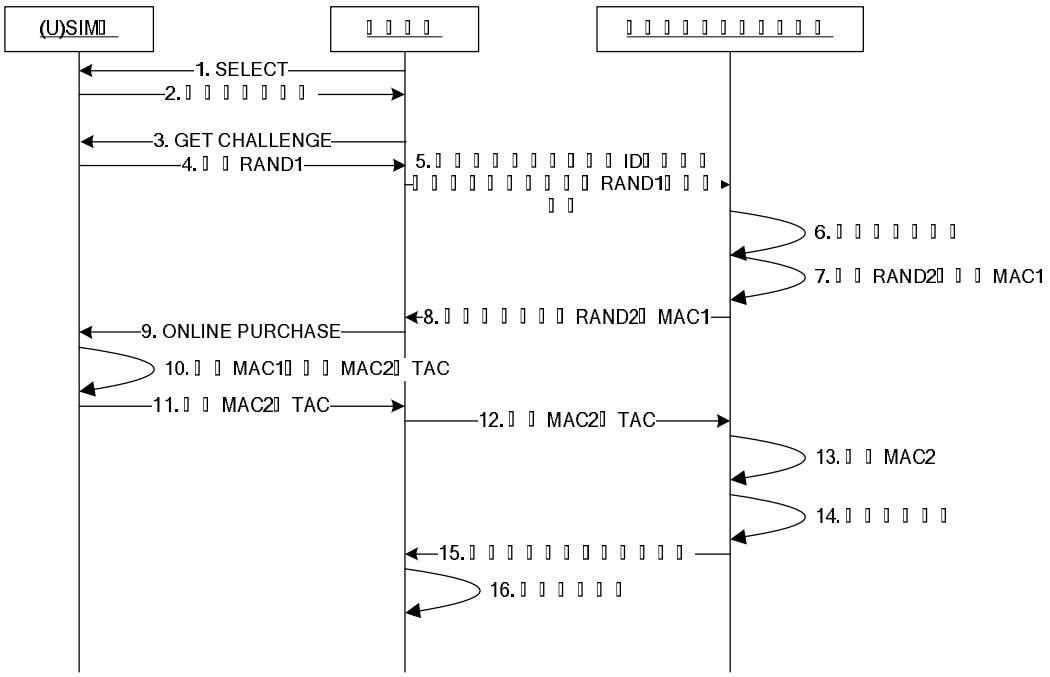

图7.2 联机消费交易流程

1. 消费终端向RFID-SIM卡发送SELECT命令；
2. RFID-SIM卡向消费终端返回应用序列号；
3. 消费终端向RFID-SIM卡发送GET CHALLENGE命令；
4. RFID-SIM卡向消费终端返回随机数RAND1；
5. 消费终端向一卡通平台业务模块提交应用序列号、企业ID、子应用索引号、终端机编号、扣款金额信息；
6. 一卡通平台业务模块检查用户账户状态是否有效，若无效返回用户账户无效结果给消费终端，否则生成MAC1；
7. 一卡通平台业务模块向消费终端返回验证结果；
8. 若用户账户无效，消费终端给与相应提示，否则向RFID-SIM卡发送ONLINE PURCHASE命令；
9. RFID-SIM卡验证MAC1的有效性，若有效，计算MAC2、TAC；
10. 若MAC1无效，RFID-SIM卡返回错误状态码，否则返回MAC2、TAC；
11. 消费终端将MAC2、TAC信息提交给一卡通平台业务模块；
12. 一卡通平台业务模块验证MAC2的有效性；
13. 若MAC2有效，一卡通平台业务模块处理用户账户，如扣款；
14. 若MAC2无效，一卡通平台业务模块返回错误状态码，否则返回消费成功结果；
15. 消费终端显示消费结果。

7.4 脱机消费撤销交易

脱机消费撤销交易流程如图7.3所示：

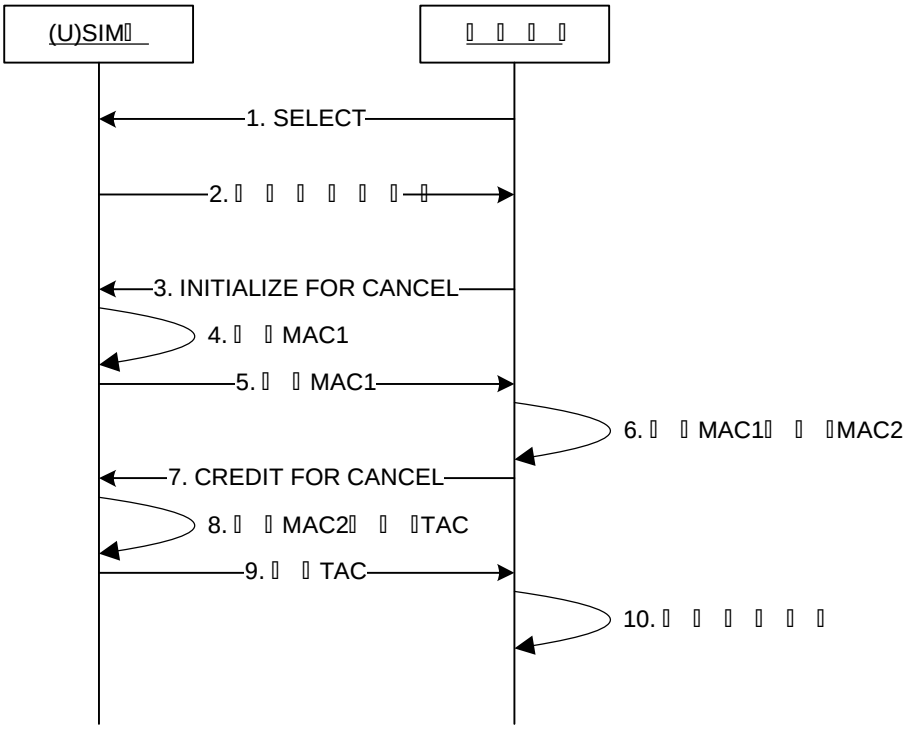

图7.3 脱机消费撤销交易流程

1. 消费终端向RFID-SIM卡发送SELECT命令；
2. RFID-SIM卡向消费终端返回应用序列号；
3. 消费终端向RFID-SIM卡发送INITIALIZE FOR CANCEL命令；
4. RFID-SIM卡判断指定的消费记录是否存在或是否已经过期，若不存在或已过期则返回错误并提示，否则生成MAC1；
5. 若指定消费记录有效则RFID-SIM卡向消费终端返回MAC1，否则返回错误状态码；
6. 消费终端若收到错误状态码，给与相应提示并终止流程，否则校验MAC1的有效性，若MAC1有效则生成MAC2，否则给与相应提示并终止流程；
7. 消费终端向RFID-SIM卡发送CREDIT FOR CANCEL命令；
8. RFID-SIM卡校验MAC2的有效性，若无效返回错误状态码，否则生成TAC；
9. 若MAC2有效则RFID-SIM卡向消费终端返回TAC，否则返回错误状态码；
10. 消费终端若收到错误状态码，给与相应提示并终止流程，否则保存交易信息。

7.5 联机消费撤销交易

联机消费撤销交易流程如图7.4所示：

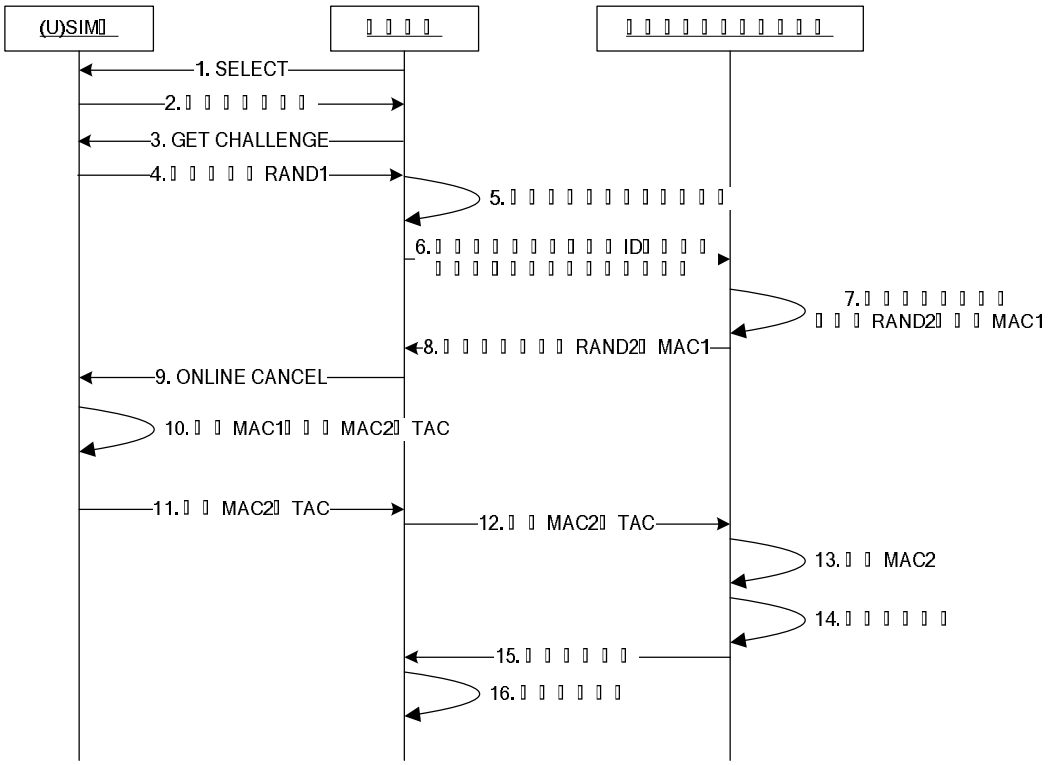

图7.4 联机消费撤销交易流程

1. 消费终端向RFID-SIM卡发送SELECT命令；
2. RFID-SIM卡向消费终端返回应用序列号；
3. 消费终端向RFID-SIM卡发送GET CHALLENGE命令；
4. RFID-SIM卡向消费终端返回随机数RAND1；
5. 操作人员在消费终端上输入交易流水号和交易金额；
6. 消费终端向一卡通平台业务模块提交用户应用序列号、企业ID、子应用索引号、终端机编号、交易流水号和交易金额信息；
7. 一卡通平台业务模块检查用户账户状态是否有效，若无效返回用户账户无效结果给消费终端，否则生成MAC1；
8. 一卡通平台业务模块向消费终端返回验证结果；
9. 若用户账户无效，消费终端给与相应提示，否则向RFID-SIM卡发送ONLINE CANCEL命令；
10. RFID-SIM卡验证MAC1的有效性，若有效，计算MAC2、TAC；
11. 若MAC1无效，RFID-SIM卡返回错误状态码，否则返回MAC2、TAC；
12. 消费终端将MAC2、TAC信息提交给一卡通平台业务模块；
13. 一卡通平台业务模块验证MAC2的有效性；
14. 若MAC2有效，一卡通平台业务模块处理用户账户，如消费撤销；
15. 若MAC2无效，一卡通平台业务模块返回错误状态码，否则返回撤销成功结果；
16. 消费终端显示撤销结果。

8．编制历史

版本号	更新时间	主要内容或重大修改

1.0.0	2010-1-15	1.0.0版本