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卡与发卡终端接口分册

Interface Specification for E-Card Pass Service between RFID-SIM Cards and Write Card 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卡与发卡终端之间的接口提出要求，是集团及省公司开展一卡通业务的依据之一。

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，供中国移动内部和发卡终端、RFID-SIM卡厂商共同使用；适用于GSM/GPRS/EDGE/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

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。

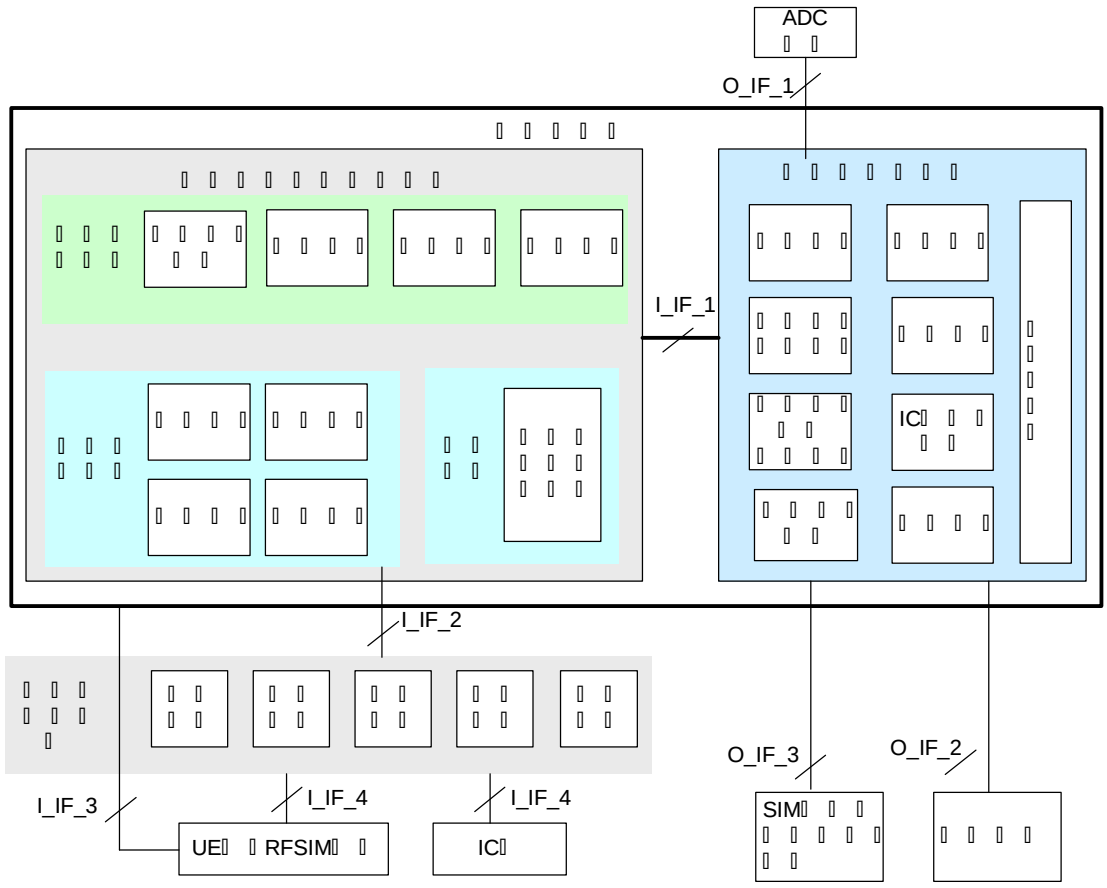

图4.1 一卡通业务系统结构图

5. 文件和命令

本章描述RFID-SIM卡与发卡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

若无特殊说明，在涉及MAC的命令执行前，需要先调用GET CHALLENGE命令获取4字节随机数以分散获得会话密钥。

MAC是用应用管理密钥（或企业主控密钥）的会话密钥对下数据进行MAC计算（按所列顺序）产生的：

——CLA
——INS
——P1
——P2
——Lc
——命令报文数据域

此命令计算MAC使用的会话密钥：
输入参数：
——应用管理密钥（或企业主控密钥）
——随机数（用Get Challenge获得的4字节随机数，后缀以0x80 0x00 0x00 0x00）
输出数据：
——应用管理密钥（或企业主控密钥）会话密钥

MAC的计算方法以及会话密钥的计算方法参见《中国移动一卡通业务安全技术规范-密钥与算法要求》。

5.2.2 GET CHALLENGE 命令

5.2.2.1 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。

该随机数只能用于下一条指令，无论下一条指令是否使用了该随机数，该随机数都将立即失效。

5.2.2.2 命令报文

GET CHALLENGE命令报文的编码见表5-1：

表5-1 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’

5.2.2.3 命令报文数据域

命令报文数据域不存在。

5.2.2.4 响应报文数据域

响应报文数据域包括RFID-SIM卡产生的随机数，长度为4字节或8字节。

5.2.2.5 响应报文状态码

此命令执行成功的状态码是’9000’。

RFID-SIM卡可能回送的错误状态码如表5-2所示：

表5-2 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

5.2.3 GET RESPONSE 命令

5.2.3.1 定义和范围

本指令只适用于T=0协议的RFID-SIM卡。

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

5.2.3.2 命令报文

GET RESPONSE命令报文编码见表5-3：

表5-3 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

5.2.3.3 命令报文数据域

命令报文数据域不存在。

5.2.3.4 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，RFID-SIM卡必须回送状态码’6CXX’，否则回送状态码’6F00’。

5.2.3.5 响应报文状态码

此命令执行成功的状态码是’9000’。

表5-4列出正常处理情况：

表5-4 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

RFID-SIM卡可能回送的警告状态码如表5-5所示：

表5-5 GET RESPONSE警告状态

SW1	SW2	含 义
‘62’	‘81’	回送的数据可能有错

RFID-SIM卡可能回送的错误状态码如表5-6所示：

表5-6 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

5.2.4 READ BINARY 命令

5.2.4.1 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）。

5.2.4.2 命令报文

READ BINARY命令报文编码见表5-7：

表5-7 READ BINARY命令报文

代码	值
CLA	‘00’或’04’
INS	‘B0’
P1	见表5-8
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5-8定义了命令报文中的引用控制参数：

表5-8 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）

5.2.4.3 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。

5.2.4.4 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。

5.2.4.5 响应报文状态码

此命令执行成功的状态码是’9000’。

RFID-SIM卡可能回送的警告状态码如表5-9所示：

表5-9 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

RFID-SIM卡可能回送的错误状态码如表5-10所示：

表5-10 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

5.2.5 READ RECORD 命令

5.2.5.1 定义和范围

READ RECORD命令用于读取记录文件的内容。

RFID-SIM卡的响应由回送记录组成。

5.2.5.2 命令报文

READ RECORD命令报文编码见表5-11：

表5-11 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5-12）
Lc	不存在（CLA=’04’时除外）
Data	不存在（CLA=’04’时除外）
Le	‘00’

表5-12定义了命令报文中的引用控制参数：

表5-12 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

5.2.5.3 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。

5.2.5.4 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。

5.2.5.5 响应报文状态码

此命令执行成功的状态码是'9000'。

RFID-SIM卡可能回送的警告状态码如表5-13所示：

表5-13 READ RECORD警告状态

SW1	SW2	含　义
'62'	'81'	回送的数据可能有错

RFID-SIM卡可能回送的错误状态码如表5-14所示：

表5-14 READ RECORD错误状态

SW1	SW2	含　义
'64'	'00'	标识状态位没变
'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

5.2.6 SELECT 命令

5.2.6.1 定义和范围

SELECT命令通过文件名或AID来选择RFID-SIM卡中的DDF或ADF，命令执行成功后，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DDF或ADF。

来自RFID-SIM卡的响应报文应由回送FCI组成。

5.2.6.2 **命令报文**

SELECT命令报文编码见表5-15：

表5-15 SELECT命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表5-16）
P2	‘00’第一个或仅有一个 ‘02’下一个
Lc	‘05’-’10’
Data	文件名
Le	‘00’

命令报文中的引用控制参数参见表5-16：

表5-16 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	

5.2.6.3 **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。

5.2.6.4 **响应报文数据域**

响应报文中的数据域应该包括所选择的DDF或ADF的FCI。表5-17到表5-19规定了此定义了所用的标识。本规范不规定FCI中回送的附加标识。

表5-18定义了成功选择DDF后回送的FCI：

表5-18 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5-19定义了成功选择ADF后回送的FCI：

表5-19 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’	发卡方自定义数据的FCI	O

表5-20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5-20 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

表5-21定义了ADF 回送的‘9F0C’中包含的数据，成功地选择了一卡通应用后，RFID-SIM卡回送应用必备的发卡方专用数据。发卡方自定义FCI数据是和SFI=21文件内信息一致（参见附录A.1）。

表5-21 发卡方自定义数据的FCI

9F0C	发卡方自定数据的FCI		
	发卡方标识符	8字节	M
	发卡方应用版本号	1字节	M
	应用序列号	8字节	M
	应用启用日期	4字节	M
	应用有效日期	4字节	M
	发卡方自定义FCI数据 （取值 0x000001：RFID-SIM卡或普通IC卡； 0x000002：工作母卡 其他值保留 ）	3字节	M

5.2.6.5 响应报文状态码

此命令执行成功的状态码是’9000’。

RFID-SIM卡可能回送的警告状态码如表5-22所示：

表5-22 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

RFID-SIM卡可能回送的错误状态码如表5-23所示：

表5-23 SELECT错误状态

SW1	SW2	含　义
‘64’	‘00’	标识状态位没变
‘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RFID-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。

5.2.7 UPDATE BINARY 命令

5.2.7.1 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。

5.2.7.2 命令报文

UPDATE BINARY命令报文编码见表5-24：

表5-24 UPDATE BINARY命令报文

代码	值
CLA	‘04’
INS	‘D6’
P1	见表5-25
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 = ‘04’ 需要安全报文。

表5-25定义了命令报文中的引用控制参数：

表5-25 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）

5.2.7.3 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《中国移动一卡通业务安全技术规范-密钥与算法要求》，密钥采用应用管理密钥。

5.2.7.4 响应报文数据域

响应报文数据域不存在。

5.2.7.5 响应报文状态码

此命令执行成功的状态码是'9000'。

RFID-SIM卡可能回送的警告状态码如表5-26所示：

表5-26 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

RFID-SIM卡可能回送的错误状态码如表5-27所示：

表5-27 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

5.2.8 UPDATE RECORD 命令

5.2.8.1 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。

5.2.8.2 命令报文

UPDATE RECORD 命令报文编码见表5-28：

表5-28 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5-29
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5-29定义了命令报文中的引用控制参数：

表5-29 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

5.2.8.3 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《中国移动一卡通业务密钥管理规范》，密钥采用应用管理密钥。

5.2.8.4 响应报文数据域

响应报文数据域不存在。

5.2.8.5 响应报文状态码

此命令执行成功的状态码是’9000’。

RFID-SIM卡可能回送的警告状态码如表5-30所示：

表5-30 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

RFID-SIM卡可能回送的错误状态码如表5-31所示：

表5-31 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

5.2.9 CREATE SUB_APPLICATION 命令

5.2.9.1 定义和范围

CREATE SUB_APPLICATION命令用于在一卡通应用下创建一个子应用。

5.2.9.2 命令报文

CREATE SUB_APPLICATION命令报文见表5-32：

表5-32 CREATE SUB_APPLICATION命令报文

代码	值
CLA	‘84’
INS	‘50’
P1	‘00’
P2	‘00’
L_c	Data域的实际长度
Data	见表5-33
L_e	不存在

5.2.9.3 命令报文数据域

在调用CREATE SUB_APPLICATION命令前，需要先调用GET CHALLENGE命令获取4字节随机数以分散获得会话密钥。

CREATE SUB_APPLICATION命令报文数据域见表5-33，企业ID到MAC之前的数据为密文形式，采用应用管理密钥的会话密钥进行加密，MAC利用应用管理密钥的会话密钥计算得到。

表5-33 CREATE SUB_APPLICATION命令报文数据域

说明	长度（字节）
企业ID	6
员工ID	20
员工企业流水号	4
子应用索引号	1
子应用有效期	4
子应用类型	1
子应用锁定标识	1
子应用数据（参见表5-39~5-43）	X
MAC	4

注：子应用索引号为0x00的子应用对应该企业的主控子应用，此时子应用类型取值为0x00，对应的子应用数据见表5-34：

表5-34 主控子应用数据（子应用类型为0x00）

说明	长度（字节）
企业名称	16
企业主控密钥标识	1
企业主控密钥版本	1
企业主控密钥索引号	1
企业主控密钥算法标识	1
企业主控密钥	16
企业空中传输密钥标识	1
企业空中传输密钥版本	1
企业空中传输密钥索引号	1
企业空中传输密钥算法标识	1
企业空中传输密钥	16
企业空中报文MAC密钥标识	1
企业空中报文MAC密钥版本	1
企业空中报文MAC密钥索引号	1
企业空中报文MAC密钥算法标识	1
企业空中报文MAC密钥	16

子应用类型为0x01的子应用对应该企业的门禁子应用，对应的子应用数据见表5-35：

表5-35 门禁子应用数据（子应用类型为0x01）

说明	长度（字节）
门禁名称	16
门禁密钥标识	1
门禁密钥版本	1
门禁密钥索引号	1
门禁密钥算法标识	1
门禁密钥	16

子应用类型为0x02的子应用对应该企业的考勤子应用，对应的子应用数据见表5-36：

表5-36 考勤子应用数据（子应用类型为0x02）

说明	长度（字节）
考勤名称	16
考勤密钥标识	1
考勤密钥版本	1
考勤密钥索引号	1
考勤密钥算法标识	1
考勤密钥	16

子应用类型为0x03的子应用对应该企业的电子钱包子应用，对应的子应用数据见表5-37：

表5-37 电子钱包子应用数据（子应用类型为0x03）

说明	长度（字节）
电子钱包名称	16
钱包类型	1
钱包余额有效期启用标识	1
钱包余额类型	1
钱包透支限额	3
电子钱包消费密钥标识	1
电子钱包消费密钥版本	1
电子钱包消费密钥索引号	1
电子钱包消费密钥算法标识	1
电子钱包消费密钥	16
电子钱包充值密钥标识	1
电子钱包充值密钥版本	1
电子钱包充值密钥索引号	1
电子钱包充值密钥算法标识	1
电子钱包充值密钥	16
电子钱包TAC密钥标识	1
电子钱包TAC密钥版本	1
电子钱包TAC密钥索引号	1
电子钱包TAC密钥算法标识	1
电子钱包TAC密钥	16

子应用类型为0x04的子应用对应该企业的联机消费子应用，对应的子应用数据见表5-38：

表5-38 联机消费子应用数据（子应用类型为0x04）

说明	长度（字节）
联机消费名称	16
消费金额类型	1
联机交易鉴权密钥标识	1
联机交易鉴权密钥版本	1
联机交易鉴权密钥索引号	1

联机交易鉴权密钥算法标识	1
联机交易鉴权密钥	16
联机交易TAC密钥标识	1
联机交易TAC密钥版本	1
联机交易TAC密钥索引号	1
联机交易TAC密钥算法标识	1
联机交易TAC密钥	16

子应用类型为0x10~0x1F的子应用对应该企业的自定义子应用，对应的子应用数据见表5-39：

表5-39 企业自定义子应用数据（子应用类型为0x10~0x1F）

说明	长度（字节）
自定义数据	64

5.2.9.4 响应报文数据域

响应报文数据域不存在。

5.2.9.5 响应报文状态码

此命令执行成功的状态码是'9000'。

RFID-SIM卡可能回送的错误状态码如表5-40所示：

表5-40 CREATE SUB_APPLICATION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'	应用永久锁定
'93'	'11'	MAC错误
'93'	'12'	企业主控子应用不存在（必须先创建企业主控子应用才可以创建其它子应用）
'93'	'13'	指定的子应用索引号已存在
'93'	'14'	子应用类型错误
'93'	'15'	子应用数据长度错误
'93'	'1B'	子应用数目达到上限。

5.2.10 GET SUB_APPLICATION STATUS 命令

5.2.10.1 定义和范围

GET SUB_APPLICATION STATUS命令用于判断一卡通应用下指定子应用是否存在。

5.2.10.2 命令报文

GET SUB_APPLICATION STATUS命令报文见表5-41：

表5-41 GET SUB_APPLICATION STATUS命令报文

代码	值
CLA	‘80’
INS	‘52’
P1	‘00’
P2	‘00’
L_c	0x07
Data	见表5-42
L_e	不存在

5.2.10.3 命令报文数据域

命令报文数据域见表5-42：

表5-42 GET SUB_APPLICATION STATUS命令报文数据域

说明	长度（字节）
企业ID	6
子应用索引号	1

5.2.10.4 响应报文数据域

响应报文数据域不存在。

5.2.10.5 响应报文状态码

此命令执行成功的状态码是’9000’。

RFID-SIM卡可能回送的错误状态码如表5-43所示：

表5-43 GET SUB_APPLICATION STATUS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’	应用永久锁定
‘93’	‘16’	企业ID错误
‘93’	‘17’	子应用索引号错误

5.2.11 UPDATE SUB_APPLICATION DATA 命令

5.2.11.1 定义和范围

UPDATE SUB_APPLICATION DATA命令用于在一卡通应用下更新一个指定的子应用（通过命令报文数据域中包含的企业ID和子应用索引号唯一标识）。

5.2.11.2 命令报文

UPDATE SUB_APPLICATION DATA命令报文见表5-44：

表5-44 UPDATE SUB_APPLICATION DATA命令报文

代码	值
CLA	‘84’
INS	‘54’
P1	‘00’：不更新员工ID、员工企业流水号 ‘01’：更新员工ID、员工企业流水号
P2	‘00’
L_c	Data域的实际长度
Data	见表5-45
L_e	不存在

5.2.11.3 命令报文数据域

UPDATE SUB_APPLICATION DATA命令报文数据域见表5-45，企业ID、子应用索引号和子应用类型不可更新，员工ID到MAC之前的数据为密文形式，采用企业主控密钥的会话密钥进行加密，MAC利用企业主控密钥的会话密钥计算得到：

表5-45 UPDATE SUB_APPLICATION DATA命令报文数据域

说明	长度（字节）
企业ID	6
员工ID	20
员工企业流水号	4

子应用索引号	1
子应用有效期	4
子应用类型	1
子应用锁定标识	1
子应用数据（参见表5-46~5-47）	X
MAC	4

子应用数据参见表5-46~5-47：

表5-46 主控子应用数据（子应用类型为0x00）

说明	长度（字节）
企业名称	16

子应用类型为0x01的子应用对应该企业的门禁子应用，对应的子应用数据见表5-47：

表5-47 门禁子应用数据（子应用类型为0x01）

说明	长度（字节）
门禁名称	16

子应用类型为0x02的子应用对应该企业的考勤子应用，对应的子应用数据见表5-48：

表5-48 考勤子应用数据（子应用类型为0x02）

说明	长度（字节）
考勤名称	16

子应用类型为0x03的子应用对应该企业的电子钱包子应用，对应的子应用数据见表5-49：

表5-49 电子钱包子应用数据（子应用类型为0x03）

说明	长度（字节）
电子钱包名称	16
钱包类型	1
钱包余额有效期启用标识	1
钱包余额类型	1
钱包透支限额	3

子应用类型为0x04的子应用对应该企业的联机消费子应用，对应的子应用数据见表5-50：

表5-50 联机消费子应用数据（子应用类型为0x04）

说明	长度（字节）
联机消费名称	16
消费金额类型	1

子应用类型为0x10~0x1F的子应用对应该企业的自定义子应用，对应的子应用数据见表5-51：

表5-51 企业自定义子应用数据（子应用类型为0x10~0x1F）

说明	长度（字节）

自定义数据	64

5.2.11.4 响应报文数据域

响应报文数据域不存在。

5.2.11.5 响应报文状态码

此命令执行成功的状态码是'9000'。

RFID-SIM卡可能回送的错误状态码如表5-52所示：

表5-52 CREATE SUB_APPLICATION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
'93'	'11'	MAC错误
'93'	'12'	企业主控子应用不存在（必须先创建企业主控子应用才可以更新其它子应用）
'93'	'14'	子应用类型错误
'93'	'15'	子应用数据长度错误
'93'	'16'	企业ID错误
'93'	'17'	子应用索引号错误

5.2.12 UPDATE SUB_APPLICATION KEYS 命令

5.2.12.1 定义和范围

UPDATE SUB_APPLICATION KEYS命令用于在一卡通应用下更新一个子应用的密钥。

5.2.12.2 命令报文

UPDATE SUB_APPLICATION KEYS命令报文见表5-53。

命令报文数据域包括要装载的密钥密文信息和MAC。

密钥密文信息是用应用管理密钥（或企业主控密钥）的会话密钥对以下数据加密（按所列顺序）产生的：

——密钥标识（参见下文，长度为1字节）

——密钥版本（参见下文，长度为1字节）

——密钥算法标识（参见下文，长度为1字节）

——密钥值（长度为16字节）

密钥标识、密钥算法标识参见《中国移动一卡通业务安全技术规范-密钥与算法要求》。

表5-53 UPDATE SUB_APPLICATION KEYS命令报文

代码	值
CLA	‘84’
INS	‘56’
P1	‘00’
P2	‘00’
L_c	Data域的实际长度
Data	见表5-48
L_e	不存在

5.2.12.3 命令报文数据域

UPDATE SUB_APPLICATION KEYS命令报文数据域见表5-54，子应用索引号到MAC之前的数据为密文形式，采用企业主控密钥子密钥的会话密钥进行加密，MAC利用企业主控密钥子密钥的会话密钥计算得到。

表5-54 UPDATE SUB_APPLICATION KEYS命令报文数据域

说明	长度（字节）
企业ID	6
子应用索引号	1
子应用密钥数据（参见表5-55、5-56）	X
MAC	4

子应用索引号为0x00的子应用对应该企业的主控子应用，对应的子应用数据见表5-55：

表5-55 主控子应用密钥数据（子应用类型为0x00）

说明	长度（字节）
企业主控密钥标识	1
企业主控密钥版本	1
企业主控密钥索引号	1
企业主控密钥算法标识	1
企业主控密钥	16
企业空中传输密钥标识	1
企业空中传输密钥版本	1
企业空中传输密钥索引号	1

企业空中传输密钥算法标识	1
企业空中传输密钥	16
企业空中报文MAC密钥标识	1
企业空中报文MAC密钥版本	1
企业空中报文MAC密钥索引号	1
企业空中报文MAC密钥算法标识	1
企业空中报文MAC密钥	16

子应用类型为0x01的子应用对应该企业的门禁子应用，对应的子应用数据见表5-56：

表5-56 门禁子应用密钥数据（子应用类型为0x01）

说明	长度（字节）
门禁密钥标识	1
门禁密钥版本	1
门禁密钥索引号	1
门禁密钥算法标识	1
门禁密钥	16

子应用类型为0x02的子应用对应该企业的考勤子应用，对应的子应用数据见表5-57：

表5-57 考勤子应用密钥数据（子应用类型为0x02）

说明	长度（字节）
考勤密钥标识	1
考勤密钥版本	1
考勤密钥索引号	1
考勤密钥算法标识	1
考勤密钥	16

子应用类型为0x03的子应用对应该企业的电子钱包子应用，对应的子应用数据见表5-58：

表5-58 电子钱包子应用密钥数据（子应用类型为0x03）

说明	长度（字节）
电子钱包消费密钥标识	1
电子钱包消费密钥版本	1
电子钱包消费密钥索引号	1
电子钱包消费密钥算法标识	1
电子钱包消费密钥	16
电子钱包充值密钥标识	1
电子钱包充值密钥版本	1
电子钱包充值密钥索引号	1
电子钱包充值密钥算法标识	1
电子钱包充值密钥	16
电子钱包TAC密钥标识	1
电子钱包TAC密钥版本	1
电子钱包TAC密钥索引号	1

电子钱包TAC密钥算法标识	1
电子钱包TAC密钥	16

子应用类型为0x04的子应用对应该企业的联机消费子应用，对应的子应用数据见表5-59：

表5-59 联机消费子应用数据（子应用类型为0x04）

说明	长度（字节）
联机交易鉴权密钥标识	1
联机交易鉴权密钥版本	1
联机交易鉴权密钥索引号	1
联机交易鉴权密钥算法标识	1
联机交易鉴权密钥	16
联机交易TAC密钥标识	1
联机交易TAC密钥版本	1
联机交易TAC密钥索引号	1
联机交易TAC密钥算法标识	1
联机交易TAC密钥	16

5.2.12.4 响应报文数据域

响应报文数据域不存在。

5.2.12.5 响应报文状态码

此命令执行成功的状态码是’9000’。

RFID-SIM卡可能回送的错误状态码如表5-60所示：

表5-60 CREATE SUB_APPLICATION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’	应用永久锁定
‘93’	‘11’	MAC错误
‘93’	‘12’	企业主控子应用不存在
‘93’	‘14’	子应用类型错误
‘93’	‘15’	子应用数据长度错误
‘93’	‘16’	企业ID错误

‘93’	‘17’	子应用索引号错误

5.2.13 RELOAD KEY(S)命令

5.2.13.1 定义和范围

RELOAD KEY(S)命令用于恢复一卡通应用下指定企业主控子应用的密钥。

RELOAD KEY(S)只能在拥有或能访问到应用管理密钥的终端上执行。

在成功执行RELOAD KEY(S)命令后，RFID-SIM卡必须完成以下操作：

- 指定企业主控子应用密钥的错误尝试计数器复位
- 所有KEY设置为命令中指定的值

RELOAD KEY(S)命令连续执行三次失败（如：MAC错误）后，一卡通应用将被锁定。

5.2.13.2 命令报文

RELOAD KEY(S)命令报文见表5-61，企业ID到MAC之前的数据为密文形式，采用应用管理密钥的会话密钥进行加密，MAC利用应用管理密钥的会话密钥计算得到。

表5-61 RELOAD KEY(S)命令报文

代码	值
CLA	‘84’
INS	‘58’
P1	‘00’：指定企业主控子应用
P2	‘00’
L_c	Data域的实际长度
Data	见表5-62
L_e	0x00

5.2.13.3 命令报文数据域

命令报文数据域见表5-63：

表5-63 RELOAD KEY(S)命令报文数据域

说明	长度（字节）
企业ID	6
子应用索引号	1（取值：0x00）
企业主控密钥标识	1
企业主控密钥版本	1
企业主控密钥索引号	1
企业主控密钥算法标识	1
企业主控密钥	16
企业空中传输密钥标识	1

企业空中传输密钥版本	1
企业空中传输密钥索引号	1
企业空中传输密钥算法标识	1
企业空中传输密钥	16
企业空中报文MAC密钥标识	1
企业空中报文MAC密钥版本	1
企业空中报文MAC密钥索引号	1
企业空中报文MAC密钥算法标识	1
企业空中报文MAC密钥	16
MAC	4

5.2.13.4 响应报文数据域

响应报文数据域不存在。

5.2.13.5 响应报文状态码

此命令执行成功的状态码是'9000'。

RFID-SIM卡可能回送的错误状态码如表5-64所示：

表5-64 RELOAD KEY(S)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
'93'	'11'	MAC错误
'93'	'12'	企业主控子应用不存在
'93'	'16'	企业ID错误
'93'	'17'	子应用索引号错误

5.2.14 SET SUB_APPLICATION STATUS 命令

5.2.14.1 定义和范围

SET SUB_APPLICATION STATUS命令用于暂停/恢复、激活/去激活一卡通应用，暂停/恢复指定企业所有子应用、或指定企业下指定子应用。

5.2.14.2 命令报文

SET SUB_APPLICATION STATUS命令报文见表5-65。

表5-65 SET SUB_APPLICATION STATUS命令报文

代码	值
CLA	‘84’
INS	‘5A’
P1	‘00’：一卡通应用 ‘01’：指定企业所有子应用 ‘02’：指定企业指定子应用
P2	‘00’：激活/去激活 ‘01’：暂停/恢复
L_c	‘0C’
Data	见表5-66
L_e	不存在

5.2.14.3 命令报文数据域

命令报文数据域见表5-66，企业ID到MAC之前的数据为密文形式，采用应用管理密钥的会话密钥进行加密，MAC利用应用管理密钥的会话密钥计算得到：

表5-66 SET SUB_APPLICATION STATUS命令报文数据域

说明	长度（字节）
企业ID	6
子应用索引号	1
状态值	1
MAC	4

5.2.14.4 响应报文数据域

响应报文数据域不存在。

5.2.14.5 响应报文状态码

此命令执行成功的状态码是’9000’。

RFID-SIM卡可能回送的错误状态码如表5-67所示：

表5-67 SET SUB_APPLICATION STATUS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
‘93’	‘11’	MAC错误
‘93’	‘12’	企业主控子应用不存在
‘93’	‘16’	企业ID错误
‘93’	‘17’	子应用索引号错误
‘93’	‘18’	状态值错误

5.2.15 DELETE SUB_APPLICATION 命令

5.2.15.1 定义和范围

DELETE SUB_APPLICATION命令用于删除一卡通应用下所有企业、指定企业、指定企业下的指定子应用。

5.2.15.2 命令报文

DELETE SUB_APPLICATION命令报文见表5-68：

表5-68 DELETE SUB_APPLICATION命令报文

代码	值
CLA	‘84’
INS	‘8A’
P1	‘00’：一卡通应用下所有企业的子应用 ‘01’：指定企业所有子应用 ‘02’：指定企业指定子应用
P2	‘00’
L_c	‘0B’
Data	见表5-69
L_e	不存在

5.2.15.3 命令报文数据域

命令报文数据域见表5-69，企业ID到MAC之前的数据为密文形式，采用应用管理密钥的会话密钥进行加密，MAC利用应用管理密钥的会话密钥计算得到：

表5-69 DELETE SUB_APPLICATION命令报文数据域

说明	长度（字节）
企业ID	6
子应用索引号	1

MAC	4

5.2.15.4 响应报文数据域

响应报文数据域不存在。

5.2.15.5 响应报文状态码

此命令执行成功的状态码是'9000'。

RFID-SIM卡可能回送的错误状态码如表5-70所示：

表5-70 DELETE SUB_APPLICATION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
'93'	'11'	MAC错误
'93'	'12'	企业主控子应用不存在
'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 交易预处理流程

图7.1给出了RFID-SIM卡同各类一卡通终端之间进行现场交易共有的预处理流程：

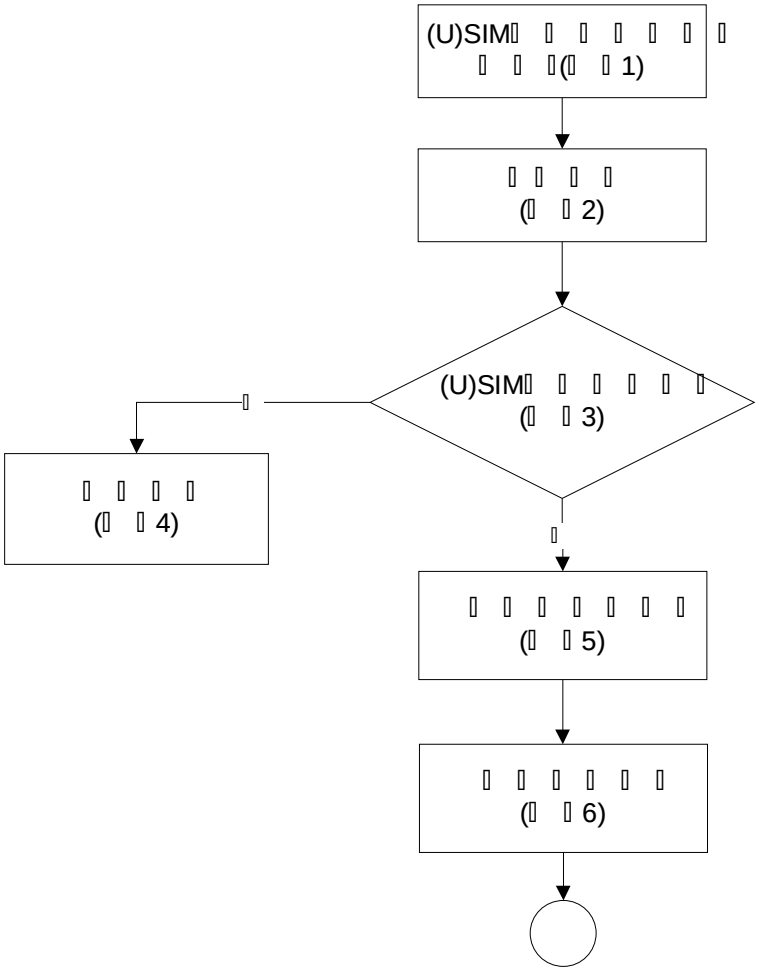

图7.1 交易预处理流程

7.1.1 RFID-SIM 卡靠近—卡通终端（步骤 1）

一卡通终端应具备非接触通信功能，能够检测RFID-SIM卡是否已经进入一卡通终端的有效工作区。如果RFID-SIM卡已经进入有效工作区，终端将继续执行7.1.2的应用选择功能。

7.1.2 应用选择（步骤 2）

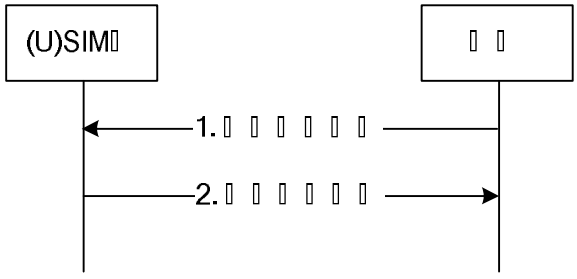

图7.2 应用选择流程

应用选择的执行过程参见第5章。

7.1.3 RFID-SIM 卡有效性检查（步骤 3）

对于应用选择命令回送的数据，一卡通终端将对这些数据进行以下检查：
—— 该RFID-SIM卡是否在一卡通终端存储的黑名单之列；
—— 该一卡通终端是否支持该发卡方标识符；
—— 该一卡通终端是否支持RFID-SIM卡上的一卡通应用(使用应用类型标识来检查)；
—— 该一卡通终端是否支持RFID-SIM卡上应用的版本；
—— RFID-SIM卡上的一卡通应用是否在有效期内。
如果以上任一条件不满足，交易将按7.1.4中的描述进行。

7.1.4 错误处理（步骤 4）

7.1.3中描述的任一条件不满足时，一卡通终端所做的处理不属于本规范的范围。

7.1.5 选择一卡通应用（步骤 5）

一卡通终端根据应用选择时获得的应用类型标识判别RFID-SIM卡支持一卡通应用的情况。
如果RFID-SIM卡和一卡通终端同时支持一卡通应用，则一卡通终端将自动选择一卡通应用，继而执行7.1.6中描述的流程。

7.1.6 交易类型选择（步骤 6）

一卡通终端应具备让操作人员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。

7.2 发卡流程

详细发卡流程参见《中国移动一卡通业务总体技术要求》。

8. 编制历史

版本号	更新时间	主要内容或重大修改
1.0.0	2010-1-13	1.0.0版本