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
--(U)SIM卡与门禁终端接口分册

Interface Specification for E-Card Pass Service between (U)SIM Cards and XX 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 II
1. 范围 4
2. 规范性引用文件 4
3. 术语、定义和缩略语 4
4. 一卡通业务概述 5
4.1 业务概述 5
4.2 系统结构图 5
5. 文件和命令 6
5.1 文件 6
5.2 APDU 命令 6
5.2.1 概述 6
5.2.2 GET SUB_APPLICATION DATA命令 6
6. 安全机制 8
7. 交易流程 8
7.1 交易预处理流程 8
7.2 门禁流程 8
8. 编制历史 9

前　言

本标准对一卡通业务开展过程中(U)SIM卡与门禁读写器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]		《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—一卡通平台部分》V1.0
[4]		《中国移动一卡通业务设备规范—(U)SIM卡应用部分》V1.0
[5]		《中国移动一卡通业务设备规范—SAM卡部分》V1.0
[6]		《中国移动一卡通业务终端设备规范—发卡终端部分》V1.0
[7]		《中国移动一卡通业务终端设备规范—门禁终端部分》V1.0
[8]		《中国移动一卡通业务终端设备规范—考勤终端部分》V1.0
[9]		《中国移动一卡通业务终端设备规范—消费终端部分》V1.0
[10]		《中国移动一卡通业务终端设备规范—充值终端部分》V1.0
[11]		《中国移动一卡通业务接口规范—(U)SIM卡与一卡通平台接口分册》V1.0
[12]		《中国移动一卡通业务接口规范—(U)SIM卡与发卡终端接口分册》V1.0
[13]		《中国移动一卡通业务接口规范—(U)SIM卡与门禁终端接口分册》V1.0
[14]		《中国移动一卡通业务接口规范-—(U)SIM卡与考勤终端接口分册》V1.0
[15]		《中国移动一卡通业务接口规范—(U)SIM卡与消费终端接口分册》V1.0
[16]		《中国移动一卡通业务接口规范—(U)SIM卡与充值终端接口分册》V1.0
[17]		《中国移动一卡通业务接口规范—发卡终端与一卡通系统接口分册》V1.0

[18] 《中国移动一卡通业务接口规范—考勤终端与一卡通系统接口分册》V1.0
[19] 《中国移动一卡通业务接口规范—门禁终端与一卡通系统接口分册》V1.0
[20] 《中国移动一卡通业务接口规范—消费终端与一卡通系统接口分册》V1.0
[21] 《中国移动一卡通业务接口规范—充值终端与一卡通系统接口分册》V1.0
[22] 《中国移动一卡通业务安全技术规范—总体要求》
[23] 《中国移动一卡通业务安全技术规范—密钥与算法要求》
[24] 《中国移动一卡通业务安全技术规范—密钥安全管理要求（一卡通服务系统）》
[25] 《中国移动一卡通业务安全技术规范—密钥安全管理要求（一卡通业务前置机）》
[26] 《中国移动一卡通业务安全技术规范—一卡通服务系统加密机设备要求》
[27] 《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　　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：

1. 范围

本标准规定了一卡通业务开展过程中(U)SIM卡与发卡终端之间的接口，供中国移动内部和门禁读写器、(U)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—(U)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—(U)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

下列术语、定义和缩略语适用于本标准：

词语	解释

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(U)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。

4.2 系统结构图

一卡通系统结构图如图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。

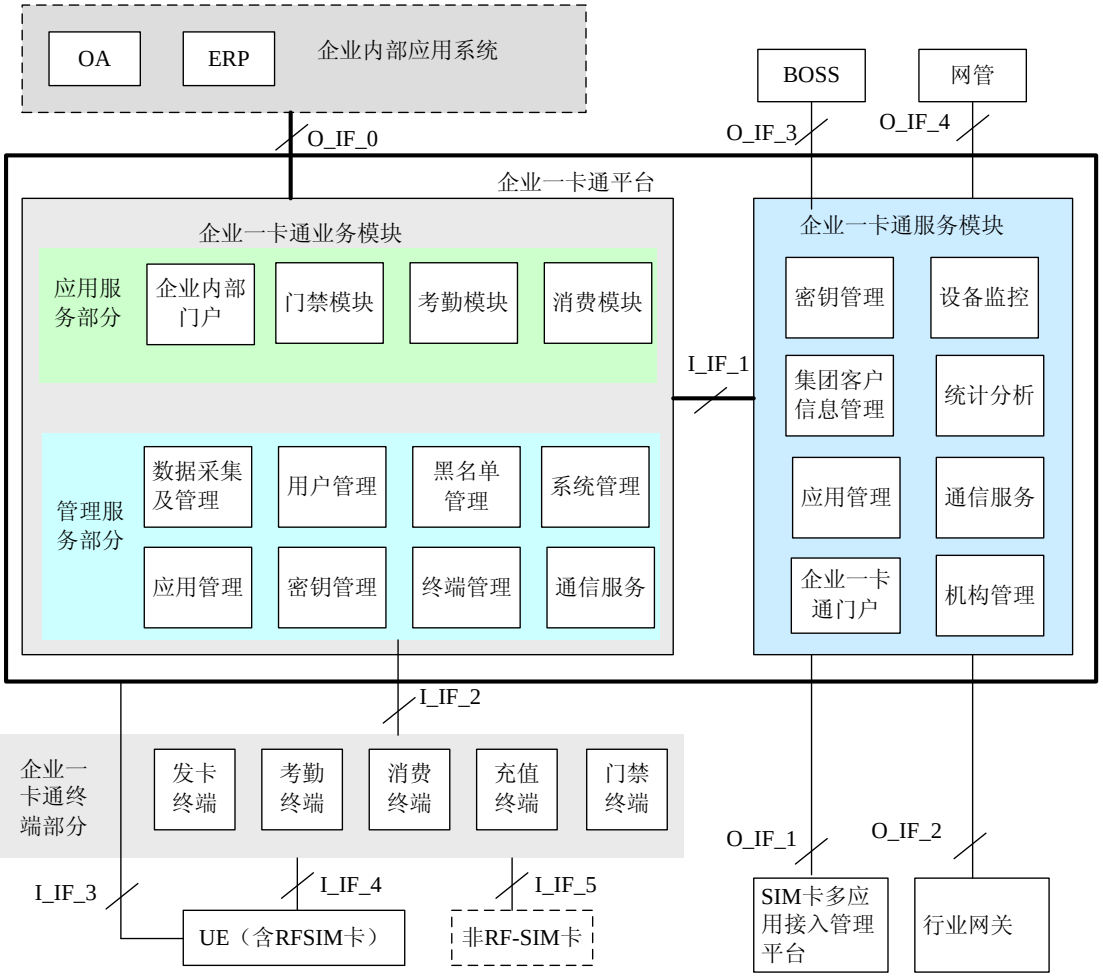

图4.1 一卡通系统结构图

5. 文件和命令

本章描述(U)SIM卡与门禁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--(U)SIM卡与发卡终端接口分册》。
本规范只定义门禁控制器专用APDU指令。

5.2.2 GET SUB_APPLICATION DATA 命令

5.2.2.1 定义和范围

GET SUB_APPLICATION DATA命令用于获取一卡通应用的指定子应用数据。

5.2.2.2 命令报文

GET SUB_APPLICATION DATA命令报文见表5-1：

表5-1 GET SUB_APPLICATION DATA命令报文格式

代码	值（16进制，下同）
CLA	‘80’或‘84’
INS	‘5C’
P1	‘00’
P2	‘00’
Lc	‘0A’或’07’
Data	参见表5-2、表5-3
Le	视Data域而定

5.2.2.3 命令报文数据域

在调用GET SUB_APPLICATION DATA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。

GET SUB_APPLICATION DATA命令报文数据域见表5-2、表5-3：

表5-2 GET SUB_APPLICATION DATA命令报文数据域（CLA=’84’）

说明	长度（字节）
企业ID	6
子应用索引号	1
RAND2	4
MAC1	4

表5-3 GET SUB_APPLICATION DATA命令报文数据域（CLA=’80’）

说明	长度（字节）
企业ID	6
子应用索引号	1

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表5-4、表5-5（参与MAC2计算的数据为企业ID、员工ID、员工企业流水号、子应用索引号、子应用有效期、子应用类型、子应用锁定标识、RAND2）：

表5-4 GET SUB_APPLICATION DATA命令执行成功的响应报文数据域（CLA=’84’）

说明	长度（字节）	备注
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	
MAC2	4	

表5-5 GET SUB_APPLICATION DATA命令执行成功的响应报文数据域（CLA=’80’）

说明	长度（字节）	备注
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	
自定义数据	64	

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 GET SUB_APPLICATION DATA命令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’	‘85’	使用条件不满足
‘69’	‘82’	安全条件不满足
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	P1、P2参数不正确
‘6B’	‘00’	参数错误（Data域参数错误）
‘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
‘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（CLA=’84’时，子应用类型必须是0x01或0x02；CLA=’80’时，子应用类型必须是0x10~0x1F范围内的值；如果不满足上述条件，返回’9314’）
‘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

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

7.2 门禁流程

门禁流程如图7.1所示：

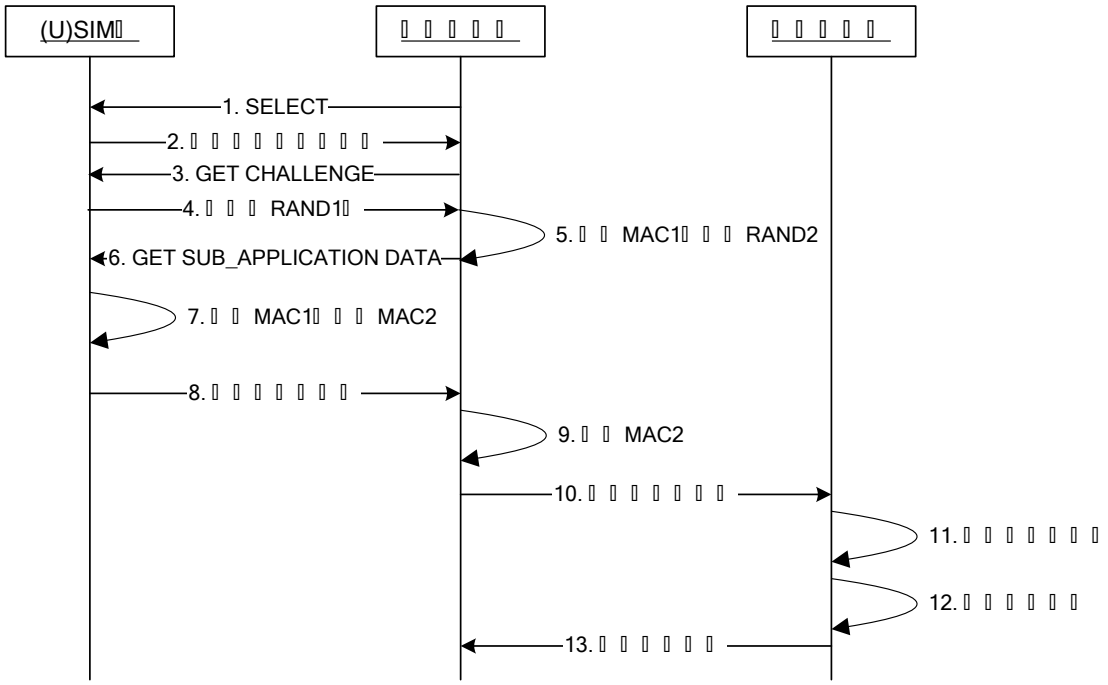

图7.1 门禁流程

1. 门禁读写器向(U)SIM卡发送SELECT命令选择一卡通应用；
2. (U)SIM卡向门禁读写器返回一卡通应用序列号等信息；
3. 门禁读写器向(U)SIM卡发送GET CHALLENGE命令获取随机数；
4. (U)SIM卡向门禁读写器返回随机数RAND1；
5. 门禁读写器根据(U)SIM卡返回的一卡通应用序列号分散得到门禁密钥子密钥，同时生成RAND2，根据RAND1、RAND2生成门禁密钥会话密钥，门禁读写器利用该会话密钥对GET SUB_APPLICATION DATA命令从CLA字段到子应用索引号字段的数据进行计算得到MAC1；
6. 门禁读写器向(U)SIM卡发送GET SUB_APPLICATION DATA命令；
7. (U)SIM卡校验GET SUB_APPLICATION DATA命令中MAC1的有效性，若MAC1错误则结束流程，若MAC1正确则同时生成MAC2；
8. (U)SIM卡返回企业ID、员工ID、企业流水号、MAC2等信息；
9. 门禁读写器收到响应后校验MAC2的有效性，若MAC2错误则提示(U)SIM卡无效，并结束流程；
10. 门禁读写器向门禁控制器上送子应用信息；
11. 门禁控制器收到子应用信息后，处理该用户的个人信息，若用户信息无效则提示告警；
12. 门禁控制器根据子应用信息的有效性执行相应的门控操作；
13. 门禁控制器向门禁读写器返回处理结果，若用户个人信息无效，则提示告警。

8. 编制历史

版本号	更新时间	主要内容或重大修改
1.0.0	2009-7-5	1.0.0版本
	2009-8-13	1. 修改GET SUB_APPLICATION

DATA指令；

2. 修改门禁流程。