中国移动多应用开放平台
接口方案

版本号 1.0.0

××××-××-××发布　　××××-××-××实施

中国移动通信有限公司　　发布

目　　录

前　言

本规范对多应用开放平台接口的具体要求。

本规范主要包括以下几方面内容：功能要求、接口要求、性能要求以及安全性要求等。

本标准由中移　　号文件印发。

本规范由中国移动通信有限公司技术部提出并归口。

本规范由规范归口部门负责解释。

本规范起草单位：中国移动通信研究院

本规范主要起草人：陆鸣、郭漫雪、朱本浩、李琳、黄更生

1. 范围

本规范定义了多应用开放平台接口要求。供中国移动内部和厂商共同适用；适用于多应用开放平台业务开展、招标选型，工程建设和运行维护为集团公司和省公司提供技术依据；适用于GSM、GPRS、3G、WLAN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。

表2-1

[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)》	
[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 TS 102 226	Smart Cards; Remote APDU structure for UICC based applications	
[3]	QB-D-	《中国移动通信SIM卡基础技术规范》	中国移动通信有限公司
[4]	QB-D-	《中国移动通信SIM卡应用技术规范》	中国移动通信有限公司
	GSM 03.40	Digital cellular telecommunications system (Phase 2+)	（V7.4.0 :1999-12）
	GSM 03.48	Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit	（V6.1.0 :1998-07）
		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	
		中国移动手机支付业务总体技术要求-现场支付部分	
		中国移动SE多安全域多应用管理技术规范	
		手机支付系统安全体系总体描述	
		手机支付系统安全技术规范 - 基础设施分册	
		手机支付系统安全技术规范 - 应用（业务）分册	
		中国移动SE多安全域多应用管理技术规范	
		中国移动多应用开放平台总体技术方案	
		中国移动多应用开放平台设备方案	

3. 缩略语及名词定义

3.1. 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
ME	Mobile Equipment
MO	Mobile Originating
MT	Mobile Terminating
MSISDN	Mobile Station International ISDN Number，移动台国际 ISDN 号码
IMSI	International Mobile Subscriber Identity，国际移动用户识别码
(U)SIM	(Universal) Subscriber Identity Module
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio System
SMS	Short Message Service，短消息业务
BIP	Bearer Independent Protocol，承载无关协议
OTA	Over The Air，空中下载
STK	SIM card Tool Kit，SIM卡开发工具包
BOSS	Business Operation Service System
HTTP	Hyper Text Transfer Protocol，超文本传输协议
SOAP	Simple Object Access Protocol，简单对象访问协议
COS	Chip Operating System，卡片操作系统
CMPP	China mobile

3.2. 名词定义

名词	解释
OTA	通过移动通信网的空中接口对SE上数据及应用进行远程管理的技术。
应用	本规范特指CMS^{2}AC应用
安全域	是一种具有特殊权限的应用。每个安全域负责管理自己的密钥，以确保来自于不同应用提供方的应用及数据可以在同一张卡片上共存，而不会破坏彼此的机密性及完整性。
主安全域	也称“发卡方安全域”，作为发卡方对卡片内容进行管理时的操作代理，CMS^{2}AC卡片必须实现此安全域应用。发卡方可以利用此授权程序加载、安装、删除发卡方或其他应用提供方的应用。发卡方安全域同卡上其它的安全域很相似。
辅助安全域	类似发卡方安全域，是某个应用提供方或控制机构在卡上的代表。
CMS^{2}AC应用	指遵循《中国移动SE多安全域多应用管理技术规范》，可被SE上CMS^{2}AC平台加载并受SE上安全域保护的可编译的应用程序。未做说明情况下，本规范中“应用”指“CMS^{2}AC应用”

终端应用	运行于手机终端的应用程序。终端应用依赖于手机终端的操作系统或虚拟机。例如J2ME上的MIDLet、Android上APK等。

4. 接口要求

4.1. 与短信网关接口要求

多应用开放平台与短信网关的接口主要实现对用户的报文的上下行，包括应用下载请求、应用下载、应用删除、远程文件更新等。

该接口遵循CMPP2.0协议与CMPP3.0协议，涉及到的网元，主要包括多应用开放平台和短信网关。

同时要求多应用开放平台与短信网关接口具备如下功能：

1）同时支持CMPP2.0与CMPP3.0协议，能根据不同的网关协议进行切换。

2）能支持多线程并发连接，线程和连接数目可以配置。

4.2. 与加密机接口要求

参见《中国移动手机支付OTA与加密机接口规范》

4.3. 与业务平台接口

业务平台包括但不限于手机支付服务平台、世博手机票业务平台、企业一卡通业务平台。

4.3.1. 数据域

数据域	数据类型	备注	最大长度 (byte)
simota:SynType	Dec	应用、安全域同步类型。0x01:增加; 0x02:修改; 0x03:删除.	1
simota:AppAID	HEX	应用 AID 及实例 AID	16
simota:SEID	HEX	SEID	10
simota:FileName	ASCII	如果是应用、安全域同步，FileName 为 AppAID	
simota:FileContent	HEX	个人化数据	64K
simota:DomainAID	HEX	安全域 AID	16
simota:AppName	ASCII 第一位 80UCS2	应用名称	100
simota:StatusCode	ASCII	状态码	4
simota:StatusDescription	ASCII	状态描述	60

	第一位 80UCS2		
simota:SeqNum	ASCII	‘yyyyMMdd24hmmssxxxxxx’,xxxxxx 为 6 位流水号 SeqNum 与业务无关，应保证每个请求数据包中 SeqNum 的唯一性	20
simota:CommType	DEC	承载方式 1,SMS/BIP(后台客服人员 WEB 管理界面发起，终端用户短信、STK、WEB 或 WAP 发起);2，应用管理器,3，终端客户端	1
simota:Msisdn	ASCII	手机号码	20
simota:KeyVersion	HEX		1
simota:DomainKey	节点		
simota:LockFlag	DEC	锁定标志 0x00,解锁；0x01,锁定。	1
simota:ResultCode	ASCII	卡端操作结果通知的返回代码 0x00,成功；其他失败。	4
simota:ResultMsg	ASCII 第一位 80UCS2	SE 操作结果通知的返回信息。	60
simota:TimeStamp	ASCII	时间戳	14
simota:Imsi	ASCII		15
simota:Application	节点		
simota:SecurityDomain	节点		
simota:OriginalCommand	HEX	源发起请求的命令字	2
simota:OriginalSeqNum	Dec	源请求包流水号	20
simota:SessionID	ASCII	会话 ID,即业务平台生成的业务会话 ID，格式为‘ZZZZZZZZZyyyyMMdd24hmmssxxxxxx’,其中的 ZZZZZZZZZ 为 9 位的应用提供商编号，xxxxxx 为 6 位流水号 同一业务的数据包应使用相同的 SessionID	26
simota:SessionType	Dec	1、应用下载/业务订购，2、应用删除/业务退订，3、应用更新/业务更新，4、业务迁移，5、应用锁定，6 应用解锁，7、安全域创建，8 安全域删除，9 安全域密钥更新，10、个人化数据管理，11、BOSS 换号	
simota:TAR	HEX	应用或安全域的 TAR	3
simota:IsDeleteCAPFile	Dec	是否删除 CAP 文件 0x00 不删除；0x01 删除	1
simota:~~CmdType~~PersoType	Dec	0x00：其他，读写个人化数据，处	1

		理流程同方式一；~~个人化~~ 0x01：个人化方式一~~其他，~~0x02 个人化方式二，应用调用安全域个人化，0x03 个人化方式三，安全域调用应用个人化	
simota:Endflag	Dec	0x00：未完 0x01：结束	1
simota:APDUSum	hex	已执行 APDU 指令数	1
simota:LastAPDUSW	Hex	最后一条 APDU 执行结果 SW	2
simota:LastDate	Hex	最后一条指令的执行返回数据	256
simota:ModuleInfo	节点	Module信息	
simota:CardPOR	节点	卡片返回信息	
simota:ProvnCode	ASCII	省份代码	4
simota:IfContinueOpt	Dec	是否还有后续操作。0表示无，1表示有后续操作。	
simota:AppProviderCode	ASCII	应用提供商代码	6
simota:Token	Hex	完成签名的Token数据	
simota:HashValue	Hex	待签名的哈希数据	
simota:EventID	Dec	1、用户退网，2、业务退订，3、业务订购，4，SE挂失	

4.3.2. 预操作请求接口

多应用开放平台向业务平台应用下载请求。该接口用于多应用开放平台主动发起。应用下载请求接口、应用删除请求接口、创建安全域请求接口、安全域删除请求接口、安全域更新接口、应用锁定/解锁请求接口、个人化数据管理接口为业务平台主动发起。

发起方：多应用开放平台

被调方：业务平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义：

参数标识	PreOperationsReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">

	<SOAP-ENV:Body> <simota:PreOperationsReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话 ID</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:SEID>SEID</simota: SEID > <simota:IMEI> IMEI </simota: IMEI > <simota:AppAID>应用 AID</simota:AppAID> </simota:PreOperationsReq> <simota:OrgMsisdn>原手机号码</simota:OrgMsisdn> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

预操作请求 SessionType 可选值：应用下载、应用删除、应用更新、应用锁定、应用解锁、安全域创建、安全域删除、安全域密钥更新、BOSS 换号。

OrgMsisdn 在 BOSS 换号时设置。

返回数据格式：

参数标识	PreOperationsReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:PreOperationsReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota: ProviderSessionId> 业务平台调用操作时生成的 SessionID </simota:ProviderSessionId> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> <simota:DomainAID>安全域 AID</simota:DomainAID> <simota:SSDDapSign>辅安全域 DAP 签名</simota:SSDDapSign> <simota:KeyVersion>密钥版本号</simota:KeyVersion> <simota:DomainKey> <simota:KeyID>密钥 ID</simota:KeyID> <simota:KeyType>应用安装文 AID</simota:KeyType> <simota:KeyValue>密钥值</simota:KeyValue>

	<simota:KeyCheck>KeyCheck</simota:KeyCheck> </simota:DomainKey> ... <simota:DomainKey>...</simota:DomainKey> <simota:PersoType>个人化标识</simota:PersoType> <simota:Personalization> <simota:AppAID>需个人化 Applet 的 AID</simota:FileContent> <simota:FileContent>个人化数据</simota:FileContent> <simota:Personalization> …… <simota:Personalization> <simota:AppAID>需个人化 Applet 的 AID</simota:FileContent> <simota:FileContent>个人化数据</simota:FileContent> <simota:Personalization> <simota:Personalization> <simota:AppAID>需个人化 Applet 的 AID</simota:FileContent> <simota:FileContent>个人化数据</simota:FileContent> <simota:Personalization> </simota:PreOperationsReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

当 StatusCode 为 0000 时，表示业务平台通过审核，继续后续请求操作。返回其他状态时，操作终止。

其中：

当应用操作时，AppAID 为应用 AID，安全域操作时，AppAID 为安全域 AID。

请求应用下载时，可选项 DomainAID、SSDDapSign。

请求安全域密钥更新时，需设置一组或多组可选项 DomainKey。

请求应用个人化、BOSS 换号时，PersoType 设置个人化方式，需设置一组或多组 Personalization 数据。

4.3.3. 应用下载请求接口

业务平台向多应用开放平台应用下载请求。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定

义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义：

参数标识	DownloadApplicationReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:DownloadApplicationReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话类型</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:SEID>SEID</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> <simota:DomainAID>安全域 AID</simota:DomainAID> <simota:SSDDapSign>辅安全域 DAP 签名</simota:SSDDapSign> </simota:DownloadApplicationReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

返回数据格式：

参数标识	DownloadApplicationReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:DownloadApplicationReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> </simota:DownloadApplicationReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4.3.4. 应用删除请求接口

业务平台向多应用开放平台发起应用删除请求。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义：

参数标识	DeleteApplicationReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:DeleteApplicationReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话类型</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:SEID>SEID</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> </simota:DeleteApplicationReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

返回数据格式：

参数标识	DeleteApplicationReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:DeleteApplicationReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode>

	<simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> </simota:DeleteApplicationReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4.3.5. 创建安全域请求接口

业务平台向多应用开放平台发起安全域创建请求。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义：

参数标识	CreateSSDReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:CreateSSDReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话类型</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> <simota:SEID>SEID</simota:Msisdn> </simota:CreateSSDReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

返回数据格式：

参数标识	CreateSSDReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?>

	<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:CreateSSDReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> </simota:CreateSSDReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4.3.6. 安全域删除请求接口

业务平台向多应用开放平台发起安全域删除请求。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义：

参数标识	DeleteSSDReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:DeleteSSDReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话类型</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> <simota:SEID>SEID</simota:Msisdn>

	</simota:DeleteSSDReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

返回数据格式：

参数标识	DeleteSSDReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:DeleteSSDReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> </simota:DeleteSSDReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4.3.7. 安全域密钥更新接口

业务平台向多应用开放平台发起安全域密钥更新。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义

参数标识	UpdateDomainKeyReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:UpdateDomainKeyReq xmlns:simota ="http://www.chinamobile.com"> <simota:SeqNum>交易序号</simota:SeqNum>

	<simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话类型</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:SEID>SEID</simota:Msisdn> <simota:DomainAID>安全域 AID</simota:DomainAID> <simota:KeyVersion>密钥版本号</simota:KeyVersion> <simota:DomainKey> <simota:KeyID>密钥 ID</simota:KeyID> <simota:KeyType>应用安装文 AID</simota:KeyType> <simota:KeyValue>密钥值</simota:KeyValue> <simota:KeyCheck>KeyCheck</simota:KeyCheck> </simota:DomainKey> ... <simota:DomainKey>...</simota:DomainKey> </simota:UpdateDomainKeyReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

返回数据格式：

参数标识	UpdateDomainKeyReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:UpdateDomainKeyReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> </simota:UpdateDomainKeyReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4.3.8. 应用锁定/解锁请求接口

业务平台向多应用开放平台发起应用解锁/锁定请求。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义：

参数标识	LockApplicationReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:LockApplicationReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话类型</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:SessionType>会话类型</simota:SessionType> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:SEID>SEID</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> <simota:LockFlag>锁定标志</simota:LockFlag> </simota:LockApplicationReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

返回数据格式定义：

参数标识	LockApplicationReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:LockApplicationReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription>

	</simota:Status> </simota:LockApplicationReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4.3.9. 个人化管理接口

业务平台向多应用开放平台发起应用指令传递请求。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式：

参数标识	ApplicationAPDUReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:ApplicationAPDUReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话类型</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:~~CmdType~~PersoType>个人化标识</simota:~~CmdType~~PersoType> <simota:Endflag>结束标识</simota:Endflag> <simota:Msisdn>手机号码</simota:Msisdn> <simota:SEID>SEID</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> <simota:Personalization> <simota:AppAID>需个人化 Applet 的 AID</simota:FileContent> <simota:FileContent>个人化数据</simota:FileContent> <simota:Personalization> …… <simota:Personalization> <simota:AppAID>需个人化 Applet 的 AID</simota:FileContent>

	<simota:FileContent>个人化数据</simota:FileContent> <simota:Personalization> </simota:ApplicationAPDUReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

应用下载和应用个人化应视为同一业务，即【业务订购】，应用个人化请求数据包中的 SessionID 应与应用下载请求数据包中的 SessionID 保持一致。

一个应用可以有多个 Applet 组成，因此请求报文中可包含一组或多组个人化数据，分别对应不同的 Applet。

返回数据格式：

参数标识	ApplicationAPDUReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:ApplicationAPDUReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> </simota:ApplicationAPDUReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4.3.9.1. 方式一

使用个人化方式一时，请求报文中 ~~CmdType~~PersoType 设置为 0 时，Personalization 中的 AppAID 为空。

FileContent 包含一条或多条 APDU 指令，每条 APDU 采用 LV 格式：

L(2 字节):APDU 长度

V：APDU

FileContent 格式为“LVLV…LV”，举例参见附录 6.4.1。

APDU 指令包括应用个人化、更新应用密钥、更新应用文件等。

4.3.9.2. 方式二

使用个人化方式二时，~~CmdType~~PersoType 设置为 2。Personalization 中的 AppAID 为所需个人化的 Applet 的 AID ~~为空~~。

多应用开放平台获取的 FileContent 数据内容应为使用该业务平台设置的传输密钥(TK)加密后的密文。

使用传输密钥解密后的明文格式为：

```
TLVTLV……TLV[回车、换行]
TLVTLV……TLV [回车、换行]
.......
TLVTLV……TLV [回车、换行]
```

每一行个人化数据为一条 APDU 指令，其中 T[ag]、L[ength]各占一个字节。

Tag 标签	描述
00	明文数据
01	敏感数据，表示数据使用该业务平台与多应用开放平台协商的 KEK 密钥加密的敏感数据。

多应用开放平台处理 FileContent 数据~~每条指令~~的~~逻辑~~流程：

1. 初始化输出内容，为空 HEX 字符串。
2. 读取第一个 Tag，
   a) 若 Tag 为 00，读取后续 Length 字节定义的相应长度的数据并追加到输出内容中。
   b) 若 Tag 为 01，读取后续 Length 字节定义的相应长度的数据，调用加密机接口进行转加密，即在加密机中使用 KEK 密钥进行解密，并使用安全域的 DEK 密钥进行加密，输出加密数据追加到输出内容中
3. 读取下一个 Tag，重复步骤 2，直至行结束符。
4. 每一条输出应为一条完整的个人化指令。
5. 重复以上步骤，按顺序获取 FileContent 中包含的所有个人化指令。
6. ~~最后，多应用开放平台使用安全域创建的安全域通道的 ENC、MAC 密钥对该条指令的数据域进行加密及 MAC 计算，生成最终的指令提交给 SE。~~

多应用开放平台处理每组 Personalization 数据的流程：

1. 生成 Select 指令，选择 Personalization 中 AppAID。
2. 使用应用的 Applet 所在安全域，创建安全通道。
3. 最后，多应用开放平台使用安全域创建的安全域通道的 ENC、MAC 密钥对 FileContent 中各个人化指令的数据域进行加密及 MAC 计算，生成最终的指令提交给 SE。

带格式的： 首行缩进： 0 字符，编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0.74 厘米 + 缩进位置： 1.48 厘米

4.3.9.3. 方式三

使用个人化方式三时，~~CmdType~~PersoType 设置为 3。Personalization 中的 AppAID 为所需个人化的 Applet 的 AID。使用个人化方式三时，报文中包含一或多组 Personalization 数据。

多应用开放平台获取的 FileContent 数据内容应为使用该业务平台设置的传输密钥(TK)加密后的密文。

使用传输密钥解密后的明文格式为：

```
TLVTLV……TLV[回车、换行]
TLVTLV……TLV [回车、换行]
.......
TLVTLV……TLV [回车、换行]
```

每一行个人化数据为一条 APDU 指令，其中 T[ag]、L[ength]各占一个字节。

Tag 标签	描述
00	明文数据
01	敏感数据，表示数据使用该业务平台与多应用开放平台协商的 KEK 密钥加密的敏感数据。

多应用开放平台处理~~每条指令~~ FileContent 数据的的流程~~逻辑~~：

1. 初始化输出内容，为空 HEX 字符串。
2. 读取第一个 Tag，
   a) 若 Tag 为 00，读取后续 Length 字节定义的相应长度的数据并追加到输出内容中。
   b) 若 Tag 为 01，读取后续 Length 字节定义的相应长度的数据，调用加密机接口

进行转加密，即在加密机中使用 KEK 密钥进行解密，并使用安全域的 DEK 密钥进行加密，输出加密数据追加到输出内容中

3. 读取下一个 Tag，重复步骤 2，直至行结束符。

4. 每一条输出应为一条完整的个人化数据。

~~4.~~5. 重复以上步骤，按顺序获取所有的个人化数据。

~~5.~~6. ~~使用 StoreData 指令并设置以上个人化数据，形成一条完成的个人化指令。~~

多应用开放平台处理每组 Personalization 数据的流程：

1. 使用应用的 Applet 所在安全域，创建安全通道。

2. 生成 Install for Personalization 指令，选择需要个人化的 Applet 的 AppAID。

3. 生成 StoreData 指令，按照顺序生成 FileContent 中个人化数据，每条个人化数据生成一条 StoreData 指令。

注：步骤 2，3 按照创建安全通道类型进行加密及 MAC 计算。

~~最后，多应用开放平台使用安全域创建的安全域通道的 ENC、MAC 密钥对该条指令的数据域进行加密及 MAC 计算，生成最终的指令提交给 SE。~~

带格式的： 编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0.74 厘米 + 缩进位置： 1.48 厘米

带格式的： 首行缩进： 0 字符，编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0.74 厘米 + 缩进位置： 1.48 厘米

带格式的： 字体：倾斜

带格式的： 字体：倾斜

4.3.10. 业务事件通知接口

业务平台向多应用开放平台发送业务通知接口，包括用户退网通知、业务退订通知。多应用开放平台接收到通知后，仅在多应用开放平台中保留相应的用户状态。当手机钱包客户端等应用管理终端接入多应用开放平台后，进行相应处理。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式：

参数标识	EventNotifyReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">

	<SOAP-ENV:Body> <simota:ApplicationAPDUReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> <simota:SEID>SEID</simota:Msisdn> <simota:EventID>EventID</simota:EventID> </simota:ApplicationAPDUReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

返回数据格式：

参数标识	EventNotifyReqResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:ApplicationAPDUReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> </simota:ApplicationAPDUReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

多应用开放平台接收到业务事件通知后，仅保持用户状态。等待手机钱包客户端接入，平台根据相应的事件通知进行处理。

1. 用户退网事件，多应用开放平台通知手机钱包客户端应锁定 SE 上已下载应用，并允许 SE 注册到其他用户手机号码上。
2. 业务退订事件，多应用开放平台通知手机钱包客户端删除 SE 上已退订未删除应用。
3. 业务订购事件，多应用开放平台更改应用的状态。
4. 业务挂失事件，多应用开放平台将 SE 加入挂失列表。

4.3.11. SE 操作反馈接口

多应用开放平台向发起 SE 操作结果反馈通知。

发起方：多应用开放平台

被调方：业务平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义：

参数标识	OperationResultNotify
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:OperationResultNotify xmlns:simota ="http://www.chinamobile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:SessionType>会话类型</simota:SessionType> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:OriginalSeqNum>源请求包交易序号</simota:OriginalSeqNum> <simota:Msisdn>手机号码</simota:Msisdn> <simota:SEID>SEID</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> <simota:ResultCode>卡端操作结果通知的返回代码</simota:ResultCode> <simota:ResultMsg>卡端操作结果通知的返回信息</simota:ResultMsg> <simota:Imsi>Imsi</simota:Imsi> <simota:CardPOR> <simota:APDUSum>已执行 APDU 指令数</simota:APDUSum> <simota:LastAPDUSW> 最 后 一 条 APDU 执 行 结 果 SW</simota:LastAPDUSW> <simota:LastData>最后一条指令的执行返回数据</simota:LastData> </simota:CardPOR> </simota:OperationResultNotify> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

*注 1：AppAID 存在条件。当 OriginalCommand 为 DownloadApplication、UpdateDomainKey、CreateSSD 、 DeleteSSD 、 ApplicationAPDU 、 DeleteApplication 、 LockApplication 、 ExtraditeApplication ，AppAID 应存在。

Imsi 存在条件。当 OriginalCommand 为 DownloadApplication 和 CreateSSD、ApplicationAPDU 时， Imsi 应存在。

*注 2：SeqNum 由多应用开放平台生成，格式由多应用开放平台自定义

*注 3：对 ResultCode 的说明。当服务器端接收到卡片上发最后一条 APDU 的响应为成功时，则认为业务成功结束，此时 ResultCode 应取值为“0000”。如果卡片上发 APDU 执行失败的状态字，ResultCode 取值应为此状态字。服务器出现内部错误时，ResultCode 取值参见附录《服务器错误代码定义》。

*注 4：SessionID 应与对应业务管理平台请求数据包中的 SessionID 相同。

返回数据格式定义：

参数标识	OperationResultNotifyResponse
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:OperationResultNotifyResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> <simota:IfContinueOpt>是否还有后续操作</simota:IfContinueOpt> <simota:PersoType>个人化标识</simota:PersoType> <simota:Personalization> <simota:AppAID>需个人化 Applet 的 AID</simota:FileContent> <simota:FileContent>个人化数据</simota:FileContent> <simota:Personalization> <~~simota:FileContent>文件内容</simota:FileContent>~~> <simota:KeyVersion>密钥版本号</simota:KeyVersion> <simota:DomainKey> <simota:KeyID>密钥 ID</simota:KeyID> <simota:KeyType>应用安装文 AID</simota:KeyType> <simota:KeyValue>密钥值</simota:KeyValue> <simota:KeyCheck>KeyCheck</simota:KeyCheck> </simota:DomainKey> ... </simota:OperationResultNotifyResponse> </SOAP-ENV:Body>

	</SOAP-ENV:Envelope>

当完成应用下载后通知业务平台，若应用需个人化时，业务平台可返回 ~~FileContent~~ 一或多组 Personalization 个人化数据，通知多应用开发平台进行个人化操作，在应用下载流程中，应用下载及个人化使用同一 SessionID 及 SessionType。

当创建委托方式辅助安全域后通知业务平台，业务平台可返回一组或多组安全域密钥，通知多应用开发平台进行密钥更新。

4.3.12. 获取 Token

业务平台向多应用开放平台请求获取 Token。

发起方：业务平台

被调方：多应用开放平台

接口协议：SOAP/Web Service

调用流程：发起方调用接口，传入参数。被调方检查参数格式是否满足请求数据格式定义。如果不满足定义，返回失败信息。如果满足定义，则进行相应的业务操作。

请求数据格式定义：

参数标识	DownloadApplicationReq
消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:AcquireTokenReq xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:SessionID>会话 ID</simota:SessionID> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:CommType>承载方式</simota:CommType> <simota:Msisdn>手机号码</simota:Msisdn> <simota:AppAID>应用 AID</simota:AppAID> <simota:SEID>SEID</simota:Msisdn> <simota:DomainAID>安全域 AID</simota:DomainAID> <simota:HashValue>待签名 Token 数据</simota:HashValue > </simota:AcquireTokenReq> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

返回数据格式：

参数标识	AcquireTokenReqResponse

消息格式	<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body> <simota:AcquireTokenReqResponse xmlns:simota ="http://www.chinamboile.com"> <simota:SeqNum>交易序号</simota:SeqNum> <simota:TimeStamp>时间戳</simota:TimeStamp> <simota:Token>Token</simota:Token> <simota:Status> <simota:StatusCode>返回状态</simota:StatusCode> <simota:StatusDescription>状态描述</simota:StatusDescription> </simota:Status> </simota:AcquireTokenReqResponse> </SOAP-ENV:Body> </SOAP-ENV:Envelope>

4.4. 与手机钱包客户端接口

详见参见《中国移动客户端应用管理器技术规范》。

4.5. CMS²AC 程序管理指令

详见《中国移动 SE 多安全域多应用技术规范》。

4.6. 命令数据

4.6.1. CMS²AC 应用程序的 AID 管理

按照ISO-7816规范的定义，AID用来唯一标识卡上的应用。CMS²AC应用程序的AID由两部分组成：RID（resource identifier）和PIX（proprietary identifier extension）。其中RID为5个字节，由ISO组织分配，PIX可以由0到11个字节组成。对于ToolkitApplet，如果应用的AID为16个字节，其中第13、14、15字节为该ToolkitApplet对应的TAR值。如果应用的AID为非16个字节时（9~15字节），应用的AID可以动态配置，可以通过安装参数给应用配置一个或多个TAR值，详情参见ETSI TS 102 226规范。

中国移动自管应用RID统一采用XX XX XX XX XX。

对于ToolkitApplet，TAR分配按照如下原则：

1、 禁止采用下列现网已用的TAR值：

序号	TAR 值	说明
1	B00010	OTA 应用管理（含 CMS^{2}AC 应用程序管理）
2	B0001F	远程文件管理
3	B0001A	补丁下载
4	000000	RAM, 卡片锁定、解锁、应用下载、删除、锁定、安全域创建、安全域删除等
5	B0001E	保留。以备支持 GSM 03.48 报文格式的其他管理指令：如公钥上传，公钥请求指令

2、 卡商自用tar值区间

C00000-CFFFFF。

3、 移动保留的tar值区间

B00000-BFFFFF。

4、 第三方可分配的tar值区间

D00000-DFFFFF。

5. 附录　　编制历史

版本号	更新时间	主要内容或重大修改
1.0.0	2011.8.1	报批稿

6. 附录 B　错误代码

6.1. 卡片返回状态字定义

6.1.1. 卡片正确状态字

代码	说明
9000	正确
91XX	正确，有长度为 XX 的响应数据可取
9EXX	正确，有长度为 XX 的响应数据可取
9FXX	正确，有长度为 XX 的响应数据可取
61XX	正确，有长度为 XX 的响应数据可取

6.1.2. 卡片通用错误代码

错误代码	说明
6400	无明确诊断
6700	错误的 Lc 长度
6881	逻辑通道不支持或未激活
6982	安全状态不满足

6985	使用条件不满足
6A86	不正确的 P1、P2
6D00	不正确的 instruction
6E00	不正确的 class

6.1.3. 删除应用错误代码

错误代码	说明
6581	内存失败
6A88	引用数据不存在
6A82	应用不存在
6A80	命令数据中有不正确的值

6.1.4. 应用下载错误代码

错误代码	说明
6310	需要更多的数据
6581	内存失败
6A80	数据域中存在不正确参数
6A84	内存空间不足
6A88	引用数据不存在

6.1.5. 应用密钥更新错误代码

错误代码	说明
6581	内存失败
6A84	内存空间不足
6A88	引用数据不存在
9484	算法不支持
9485	不正确的 key 检验值

6.1.6. 应用选择错误代码

错误代码	说明
6882	安全消息不支持
6A81	功能不支持，例如卡片生命周期为 CARD_LOCKED

6A82	选择的应用或文件不存在
6283	状态的 CARD_LOCKED

6.1.7. 应用个人化错误代码

错误代码	说明
6581	内存失败
6700	长度错误
6981	命令与文件结构不相容，当前文件非所需文件
6982	操作条件不满足
6984	随机数无效
6985	使用条件不满足（应用被锁定）
6986	不满足命令执行条件，当前文件不是 EF
6987	MAC 丢失
6988	MAC 不正确
6A81	应用锁定/不支持此功能
6A82	未找到文件
6A84	文件空间不够
6A86	P1 或 P2 不正确
6B00	参数错误(偏移地址超出了 EF)
6D00	INS 不正确
6E00	CLA 不正确
9303	应用被永久锁定
9403	未找到相应的密钥

6.2. 服务器错误代码定义

6.2.1. 服务器通用错误代码

错误代码	说明
1000	业务处理时间超时
1001	数据库操作失败
1002	短消息网关通讯失败
1003	读卡器控件通讯失败
1004	BIP 通讯失败
1005	加密机模块处理失败
1006	CMSAC 安全通道创建失败
1007	生成 APDU 失败
1008	短消息组包失败

1009	读卡器控件接口组包失败
1010	用户未注册
1011	用户 BIP 通道忙
1012	目录已创建
1013	应用无 STK 菜单

6.2.2. 应用相关错误代码

错误代码	说明
1100	用户卡片无可用空间
1101	用户安全域无可用空间
1102	应用已下载至卡片
1200	应用已被锁定
1201	应用已解锁
1300	应用不存在，用户未下载过该应用

6.3. 厂商自定义错误代码

错误代码	说明
2XXX	厂商自定义错误代码

6.4. 个人化举例

个人化数据由应用定义，个人化数据的更新由业务平台与多应用接入管理平台协作完成。个人化数据内容通过应用指令接口中的FileContent传递；FileContent定义说明见4.5.9节。其内容定义举例如下。

6.4.1. 方式一个人化举例

采用方式一得电子钱包个人化数据，其FileContent内容为：

002184D400001CBD16140AC50B5B803F522ABF56BEDA39642AEEC2863858584F19DF1D002184D400001CD40997F971B6569769D6CED1975C2BF7067F1A25CA64D1841D7F17A6002184D400001C731971009DCC9C205DEBA4D953E0D5960BAF2CB9CE4714CCD963C854002184D400001CAA314F490DAE90FB76B3020895516 56FB28544F46D5F024D6610B807002184D400001C5E722EA3CD3F02DB66D8633C3D7C9C732B8742EAB06F623DB47DB99C002184D400

001C8936A8EBAEBD3D3078E6828BC074BA5605DA54EAD08B19190768751E

002184D400001C33F28933D19DF1160F6C917946DCA7E9AD264640CD12C7

99F74E585C002504D695002262640022333300010201000000100000000000

00492001010120101231556647 23F90B

说明：文件内容包括多条APDU指令，每条APDU指令为LV结构。

6.4.2. 方式二个人化举例

采用方式二得电子钱包个人化数据，其FileContent内容为：

6.4.3. 方式三个人化举例

7. 附录 C Mifare 程序管理指令

7.1. INITIALIZE UPDATE 命令

7.1.1. 定义和范围

这个命令是用来传送卡和安全通道之间的会话数据。这个命令启动一个安全通道的消息机制。跟 GP 一样

7.1.2. 前提条件

Mifare Card Manager 已经个人化。

7.1.3. 命令内容

代码	值	含义
CLA	80	
INS	50	初始化更新
P1	xx	密钥版本号
P2	xx	参考控制参数
LC	08	主安全密钥的长度
Data	xxxx…	主安全密钥

Le	00	

7.1.3.1. P2 代码定义

这取决于实施安全通道协议

1. 使用 SCP01, P2 = 密钥 ID;
2. 使用 SCP02, P2 = ‘00’.

7.1.4. 返回消息

Data 领域返回的响应消息：

名称	长度（字节）
密钥的变化数据	10
密钥信息	2
卡的安全密钥	8
卡的密码	8

卡的安全密钥取决于实施安全通道协议

返回信息包括的处理状态：

‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	SW2	含义
6A	88	引用的数据找不到

7.2. EXTERNAL AUTHENTICATE 命令

7.2.1. 定义和范围

该命令为所有随后的命令确定所需的卡认证安全级别，跟 GP 一样

7.2.2. 前提条件

Mifare Card Manager 已经个人化。

INITIALIZE-UPDATE 命令已经执行

7.2.3. 命令内容

代码	值	含义
CLA	84	
INS	82	EXTERNAL AUTHENTICATE
P1	xx	安全等级，参考控制参数
P2	00	
LC	10	数据范围的长度
Data	xxxx…	主安全密钥和 MAC
Le	00	

7.2.3.1. P1 代码定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0b	0b	0b	0b	0b	0b	1b	1b	C-DECRYPTION and C-MAC
0b	0b	0b	0b	0b	0b	0b	1b	C-MAC
0b	0b	0b	0b	0b	0b	0b	1b	没有预期的安全消息

7.2.4. 返回消息

返回信息包括的处理状态：
‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	SW2	含义
63	00	验证主安全密钥失败

7.3. DELETE 命令

7.3.1. 定义和范围

这个命令是用来撤销一项已经安装的 Mifare 应用。

7.3.2. 前提条件

Mifare Card Manager 已经个人化。
安全通道已经建立。

7.3.3. 命令内容

代码	值	含义
CLA	84	
INS	E4	DELETE
P1	00	安全等级，参考控制参数
P2	04	
LC	xx	数据范围的长度
Data	xxxx…	TLV 代码对象（和存在的 MAC）
Le	00	

7.3.4. DATA 代码定义

标签	长度	含义	状态
4F	8 bytes	SOID	强制的

7.3.5. 返回消息

Data 领域返回的响应消息：

名称	长度（字节）	值	状态
密钥的变化数据	1	00	强制的

返回信息包括的处理状态：

‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	SW2	含义
65	81	存储器故障
6A	88	引用的数据找不到
6A	82	应用找不到
6A	80	错误的数据

7.4. INSTALL 命令：

7.4.1. 定义和范围

这个命令是用来创建和完成安装一个 Mifare 应用对象

INSTALL for [load]

INSTALL for [install]

7.4.2. 前提条件

Mifare Card Manager 已经个人化。
安全通道已经初始化。

7.4.3. 命令内容：

代码	值	含义
CLA	84	
INS	E6	INSTALL
P1	xx	参考控制参数
P2	04	
LC	xx	数据范围的长度
Data	xxxx…	安装的数据（和存在的 MAC）
Le	00	

7.4.3.1. P1 代码定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0b								最后或者仅有的命令
1b								更多的命令
	0b	0b	0b	0b	1b	0b	0b	For install
	0b	0b	0b	0b	0b	1b	0b	For load
	0b	0b	0b	0b	0b	0b	1b	For reload

7.4.3.2. LOAD 参数

标签	长度（字节）	名称	状态
EF	8	系统特定的参数	强制的
C6	2	MIFARE 应用最小存储要求	强制的
C9	2	元数据最小存储要求	强制的

7.4.3.3. DATA 在 INSTALL[for install]的定义

名称	长度（字节）	值	状态
无定义	1	00	强制的
无定义	1	00	强制的
SOID 的长度	1	08	强制的
SOID	8	xxx…	强制的
特权的长度	1	01	强制的
特权	1	00	强制的
安装参数范围的长度	1	xx	强制的
安装参数范围	2-n	xxx…	强制的
无定义	1	00	强制的

7.4.3.4. Install 参数

标签	长度（字节）	名称	状态
C9	1-n	应用特定的参数	强制的
EF	1	系统特定的参数(长度是‘00’)	条件的

7.4.4. 返回消息

Data 领域返回的响应消息：

名称	长度(字节)	值	状态
安装确认的长度	1	00	强制的

返回信息包括的处理状态：

‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	SW2	含义
65	81	存储器故障
6A	88	引用的数据找不到
6A	84	没有足够的存储空间
6A	80	错误的数据

7.5. LOAD 命令

7.5.1. 定义和范围

这个命令是用来装载一个 Mifare 应用。一个应用会执行多个 LOAD APDU 命令向 Mifare Card Manager 安装一 Mifare 个应用。

7.5.2. 前提条件

Mifare Card Manager 已经个人化。
安全通道已经初始化。

7.5.3. 命令内容

代码	值	含义
CLA	84	
INS	E8	LOAD
P1	xx	参考控制参数
P2	xx	数量编号
LC	xx	数据范围的长度
Data	xxxx…	装载的数据（和存在的 MAC）
Le	00	

7.5.3.1. P1 代码定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
0b								最后或者仅有的命令
1b								更多的命令
							0b	数据
							1b	元数据（公共的和私有的）
	Xb	Xb	Xb	Xb	Xb	Xb		RFC

7.5.3.2. DATA 定义

数据是包含 MIFARE 应用和元数据的一个 Mifare 应用对象

7.5.4. 返回消息

Data 领域返回的响应消息：

名称	长度（字节）	值	状态
装载确认的长度	1	00	强制的

返回信息包括的处理状态：

‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	SW2	含义
65	81	存储器故障
6A	84	没有足够的存储空间

7.6. GET DATA 命令：

7.6.1. 定义和范围：

这个命令是用来查询 Mifare Card Manager 数据。此外,存储管理特定的信息可能被收回

7.6.2. 命令内容：

代码	值	含义
CLA	80	
INS	CA	GET DATA
P1	00	参考控制参数
P2	xx	低阶标签的值
LC	00 或者 08	数据范围的长度
Data	xxxx…	存在的 MAC
Le	00	

7.6.2.1. P2 代码定义：

- 00：返回 Mifare Card Manager 厂商信息
- 01：返回 MIFARE 数据值
- 02 到 7F：RFU
- 80 到 FE：空闲的存储管理

7.6.3. **返回消息：**

Data 领域返回的响应消息：

名称	**长度（字节）**	**值**	**状态**
数据	n	xxx…	强制的

返回信息包括的处理状态：

‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	**SW2**	**含义**
65	81	存储器故障
6A	88	引用的数据找不到
6A	84	没有足够的存储空间
6A	80	错误的数据

7.7. VERIFY PIN **命令：**

7.7.1. **定义和范围：**

这个命令是用于鉴定 Mifare Card Manager 的 PIN 。

7.7.2. **前提条件：**

7.7.3. **命令内容：**

代码	**值**	**含义**
CLA	80	
INS	20	VERIFY PIN
P1	00	参考控制参数
P2	00	
LC	03	密码的长度
Data	xxxx…	密码（HEX）
Le	00	

7.7.4. **返回消息：**

返回信息包括的处理状态：
‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	**SW2**	**含义**
6A	80	错误的密码

7.8. CHANGE PIN **命令：**

7.8.1. **定义和范围：**

这个命令是用来改变 Mifare Card Manager 的 PIN 密码。

7.8.2. **前提条件：**

MIFARE4Mobile 服务管理器已经个人化。

7.8.3. **命令内容：**

代码	**值**	**含义**
CLA	80	
INS	24	STORE DATA
P1	00	参考控制参数
P2	00	
LC	07	数据范围的长度
Data	xxxx…	旧的密码+‘FF’+新的密码
Le	00	

7.8.3.1. DATA **定义：**

长度（字节）	**值**	**含义**
3	xxx	旧的密码
1	FF	分割标示
3	xxx	新的密码

7.8.4. 返回消息

返回信息包括的处理状态：
‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	SW2	含义
6A	80	错误的旧的密码或者错误的数据范围长度

7.9. UNBLOCK PIN 命令

7.9.1. 定义和范围：

这个命令是用于改变并解锁 Mifare Card Manager 当前 PIN 密码。

7.9.2. 前提条件：

服务管理器已经个人化。
安全通道已经建立

7.9.3. 命令内容：

代码	值	含义
CLA	84	
INS	2C	UNBLOCK PIN
P1	00	参考控制参数
P2	00	
LC	00 或者 03	密码的长度
Data	xxxx…	空或者新密码（HEX）
Le	00	

7.9.4. 返回消息

返回信息包括的处理状态：
‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	SW2	含义
6A	80	错误的密码长度

7.10. ACTIVATE 命令

7.10.1. 定义和范围：

这个命令是用来激活已经安装成功Mifare应用对象。

7.10.2. 前提条件：

服务管理器已经个人化。
密码验证通过

7.10.3. 命令内容：

代码	值	含义
CLA	80	
INS	51	STORE DATA
P1	xx	参考控制参数
P2	00	
LC	08	SOID 的长度
Data	xxxx…	SOID
Le	00	

7.10.3.1. P1 定义：

- 00：反激活应用
- 01：激活应用

7.10.4. 返回消息：

返回信息包括的处理状态：
‘90 00’表明这是一条成功的命令被执行，以下则是失败的命令返回。

SW1	SW2	含义
6A	82	找不到应用

7.11. RETRIEVE DATA 命令：

7.11.1. 定义和范围：

这个命令是用来返回Mifare应用元数据和应用的数据。

7.11.2. 前提条件：

服务管理器已经个人化。
密码验证通过

7.11.3. 命令内容：

代码	值	含义
CLA	80	
INS	CF	RETRIEVE DATA
P1	xx	参考控制参数
P2	xx	
LC	xx	数据的长度
Data	xxxx…	数据
Le	00	

7.11.3.1. P1-P2 定义：

- 01 6A：返回公共的元数据

7.11.3.2. DATA 定义：

- 01 6A：没有数据

返回消息：

- P1-P2定义为01 6A：返回的数据范围是公共的元数据的TLV编码格式。如果返回的数据没有结束，该状态字节为‘9F xx’（‘xx’为还剩下没有返回的字节数，通过相同的RETRIEVE DATA命令来获取），‘90 00’表示返回结束。