中国移动多应用开放平台
设备方案

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设备的具体要求。

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设备功能要求。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 123 040	《 Universal Mobile Telecommunications System (UMTS);Technical realization of the Short Message Service (SMS)》	
	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接口方案	

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
手机钱包客户端	移动商务应用管理器
UDHL	User Data Header Length
IEId	Information Element Identifier
IEL	Information Element Length
TK	Transport Key，传输密钥
KEK	Key Encryption Key，密钥加密密钥
DEK	Data Encryption Key，数据加密密钥
ENC	Encryption，加密
MAC	Message Authentication Code，消息鉴权码

带格式的：默认段落字体，字体：Times New Roman

带格式的：字体：非倾斜

带格式的：字体：Times New Roman，字体颜色：自动设置

带格式的：字体：Times New Roman，字体颜色：自动设置

3.2. 名词定义

名词	解释
OTA	通过移动通信网的空中接口对(U)SIM卡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SE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SE内容进行管理时的操作代理，CMS^{2}AC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。
个人化数据	个人化数据为个人化指令中的数据域
个人化指令	其格式为APDU，用于应用的个人化操作

4. 业务概述

中国移动多应用开放平台为用户提供移动电子商务应用发现、下载、删除以及管理功能的门户。同时为应用提供商提供安全空间租赁、应用生命周期管理、业务平台接入。

4.1. 业务对象

中国移动多应用开放平台面向中国移动所有用户，包括个人及集团客户。同时用户应具备如下特征之一：

1. 使用NFC终端（嵌入SE安全元件）的用户。
2. 使用贴片卡（嵌入SE安全元件）的用户。

中国移动多应用开放平台所管理应用的业务对象由具体业务定义。

4.2. 业务范围

应用程序特征为

1. 应用承载于NFC终端或贴片卡上
2. 应用可包括两部分，终端应用和CMS2AC应用。其中终端应用为客户端程序，实现用户操作逻辑；CMS2AC应用在SE上，实现安全存储及运算。

应用按业务划分包括

1. 消费类应用（例如电子钱包、便民卡）
2. 身份识别类应用（例如联机应用、门禁）
3. 社交娱乐类(例如名片交换)

4. 其他

按技术实现划分包括

1. 具有非接触功能
   a) 卡模拟模式（本期实现）
   b) 读卡器模式（本期实现）
   c) P2P模式（本期暂不实现）
2. 不具备非接触功能应用（例如远程支付）

应用按照是否收取功能费分为

1. 免费
2. 收取业务功能费，详见本规范附录B
   a) 通过话费账户收取
   b) 通过支付账户收取

多应用开放平台为使用嵌入SE安全元件的设备的中国移动用户提供的应用及安全域发行及管理。

用户使用多应用开发平台业务，有以下几种途径：

1. 空中方式。用户申请NFC终端，使用NFC终端上预置手机钱包客户端（GSM/GPRS/3G/WLAN）接入多应用开放平台。
2. 非接触方式。用户申请NFC终端，使用浏览器或PC（非接触读卡器）、营业厅专用终端远程接入多应用开放平台。
3. 非接触方式。用户申请贴片卡，使用浏览器或PC（非接触式读卡器）、营业厅专用终端远程接入多应用开放平台。

多应用开放平台受理中国移动自有业务及第三方业务的接入，对应用提供商进行注册及审核、安全域申请、应用上线、签约关系等管理。

多应用开放平台对应用提供商提供全网及本地应用生命周期管理，包括应用上线、测试、审核、发布、归档等。

5. 功能要求

5.1. 系统角色

系统角色包括：普通用户、系统操作人员、应用提供商；

1. 普通用户：可以进行渠道登陆、应用搜索/下载/删除等、业务投诉等等，该组基本上是面向广大用户的组，后期加入用户之间的互动，如：好友、论坛、群等，则可以动态分配一些对应的角色，如：论坛版主、群管理员等；
2. 系统操作人员：平台运营商操作人员，包括：
   a) 系统管理员：可以进行系统基础参数设置、权限管理、动态分配权限角色等，以及修改一些特殊的不能通过正常途径修改的内容等；
   b) 客服操作员：可以按照配置权限查看用户信息及SE信息，维护应用提供商、应用及安全域的基本信息，对用户的投诉进行管理等等；

c) 业务管理员：对所有需要审核的内容进行审核，如审核应用提供商的申请资料、安全域的创建、应用的发布等等，同时也具备客服操作员组的权限等等。

3. 应用提供商：可以进行其所提供应用的信息维护、应用上传及版本维护等操作，以及用户对该服务提供商实施的业务操作进行管理等

全网业务管理员权限包括安全域管理、应用管理、应用提供商管理，省级业务管理员具有应用提供商管理及应用管理权限。

客服操作人员可根据需要所属省、地市以及县的区域划分，可进行所属区域的用户及应用提供商管理的业务操作。

5.2. 设备功能

5.2.1. 体系结构图

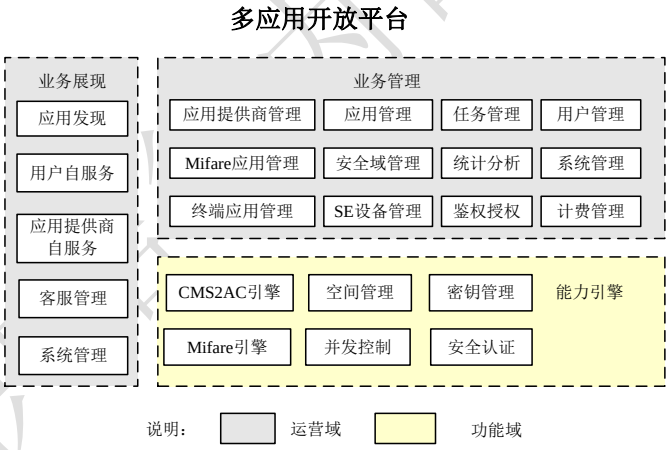


图5.1 多应用开放平台体系结构图

多应用开放平台由业务展现、业务管理、能力引擎三部分构成。

5.2.2. 功能描述

5.2.2.1. 业务展现

多应用开放平台能够实现全网及本地业务的展现。业务展现提供应用发现、用户自服务和应用提供商自服务功能，为用户或应用提供商提供发现、订购、下载、空间查询、应用下载情况查询和管理业务的直接途径。

5.2.2.2. 业务管理

多应用开放平台能够实现对全网及本地业务的管理。业务管理部分是指对自有应用、第三方应用的信息管理，其中包括对应用、第三方应用提供商、订购关系等数据进行管理，对CMS^{2}AC应用的生命周期进行控制、对应用、应用提供商的鉴权及对业务授权等。业务管理还具备基本的统计分析功能，例如对用户数与业务量的统计，从而实现对业务运营进行有效的支撑与管理。

本规范中应用具体指装到SE上应用，为符合CMS^{2}AC规范的可执行加载文件（Executable Load File），每个可执行加载文件中包含一个或多个可执行模块（Executable Load Module），可执行加载文件和可执行模块是静态程序，业务使用时需根据可执行模块及其可能的应用数据创建一个实例，一个可执行模块可以创建一个或多个实例。

多应用开放平台实现对全网及本地业务的接入及鉴权，实现自有或第三方业务平台的统一接入。

5.2.2.3. 能力引擎

多应用开放平台的按照业务管理的要求，为其提供相关的能力支持及安全信道管理、密钥管理和加解密操作。支持的能力包括：

- 应用下载、删除；
- 应用个人化、应用个人化更新
- 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
- Mifare应用下载、删除

5.3. 安全域管理

5.3.1. 属性

安全域至少应具备以下属性：

- 安全域AID，作为安全域的唯一标示，具体定义请参考《中国移动SE多安全域多应用管理技术规范》
- 安全域归属应用提供商的编号及名称
- 安全域空间管理类型及空间管理大小
- 安全域模式
- 安全域删除规则：当删除安全域中最后一个应用时，可根据设置决定同时删除安全域或通过单独的安全域删除指令删除安全域
- 密钥更新周期：安全域作为SE中安全管理的核心，从安全性考虑，安全域密钥是可以更新的，此属性可灵活定义密钥更新的周期
- 安全域安装参数，安全域的安装参数可根据安全域模式、管理空间大小等属性自动产生。具体定义请参考《中国移动SE多安全域多应用管理技术规范》

5.3.2. 安全域申请

多应用开放平台提供安全域申请功能。安全域申请需要由中国移动业务部门（自有业务）或应用提供商（第三方）提供书面申请及审批的材料。

业务管理员在安全域申请界面，输入申请所需资料信息，包括安全域归属者、安全域类型、安全域管理空间等，多应用开放平台为该安全域分配新的 AID。

5.3.3. 安全域审核

具有审核权限的业务管理员审核安全域。审核通过后，应用提供商可以查询安全域的信息，同时应用提供商可进行安全域下应用发行。

5.3.4. 安全域信息管理

多应用开放平台提供对已申请建立安全域的信息管理功能，具有权限业务管理员可以查阅、修改、删除的安全域信息。

已创建的安全域不能删除。

已创建的安全域仅能修改部分属性，包括删除规则、密钥更新周期。

5.4. 应用管理

5.4.1. 应用定义

应用指能够在NFC终端SE安装的程序和参数。SE上程序为符合CMS^{2}AC规范的可执行加载文件（Executable Load File），每个可执行加载文件中包含一个或多个可执行模块（Executable Load Module），可执行加载文件和可执行模块是静态程序，执行时需根据可执行模块及其可能的应用数据创建一个实例，一个可执行模块可以创建一个或多个实例，用不同的实例AID进行标示。对可执行加载文件中超过一个可执行模块的情况，需要定义其中一个可执行模块为主模块，该模块创建的实例的AID为整个应用定义的AID，完成与POS等外部设备的交互。

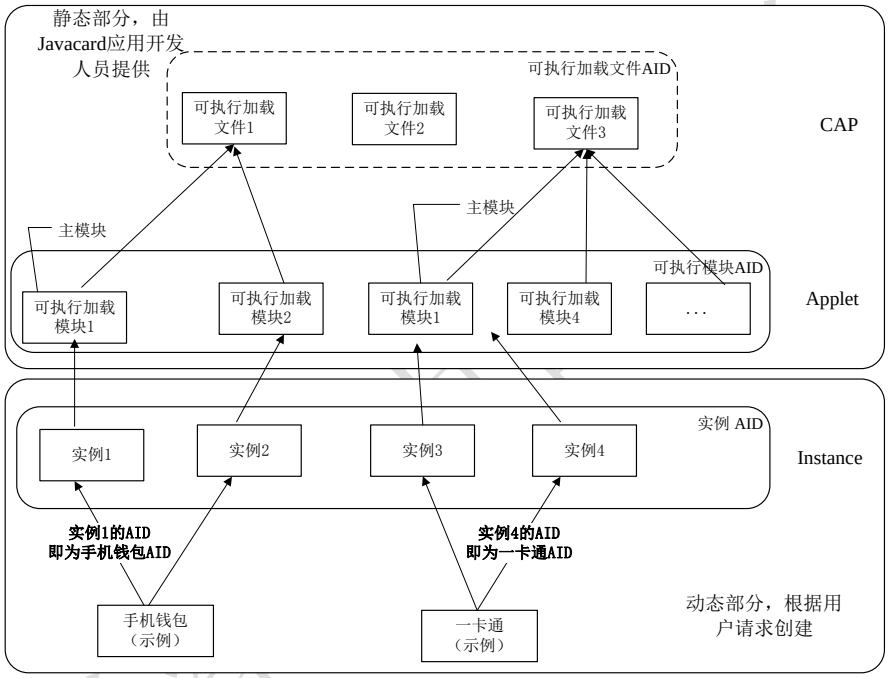


图 5-2 应用结构图

可执行加载文件中包含的可执行模块的组织关系由应用提供者决定，多应用开放平台支持可执行加载文件与可执行模块的两级管理，可执行加载文件、可执行模块与可执行模块的实例均需要用相关的AID唯一标示。

应用数据指安装程序实例化运行后所需的密钥、文件等参数信息，应用数据通常由业务平台提供，利用个人化操作装载至SE卡。

有关CMS^{2}AC程序详细描述请参考《中国移动SE多安全域多应用管理技术规范》

注：应用之间不共享可执行加载文件。若两个应用共享同一个可执行加载文件，需要安装分别安装可执行加载文件，并为其分配不同的AID。

5.4.2. 应用属性

应用至少应具备以下的属性：

- 应用AID：作为应用的唯一标示，具体定义请参考《中国移动SE多安全域多应用管理技术规范》，对应可执行主模块实例的AID
- 应用结构：可执行加载文件与对应的AID（Executable Load File AID）、可执行加载文件中包含的可执行模块与对应的AID（Executable Module AID）及可执行模块实例AID（Application AID），其中可执行主模块实例AID对应整个应用的AID。
- 应用归属安全域，即应用的实例关联的安全域
- 应用所属应用提供商
- 应用预置属性，包括是否预置，预置内存属性（ROM、Flash、EPROM）。如果预置在ROM中，该应用 删除。
- （CMS^{2}AC）应用是否有UI应用以及UI应用的URL。
- 应用文件及其Hash值：上传到多应用开放平台的应用应该是CAP文件类型，应用CAP文件Hash值，采用sha-1算法
- 应用的可执行加载文件关联的安全域
- 应用状态：标示应用处在生命周期的阶段，具有初始、已审核、已定义、已测试、发布和已归档等状态
- 应用基本信息：如应用大小、应用名称、应用版本、JAVA虚拟机版本信息、CMS^{2}AC版本号等
- 应用内存空间信息：应用文件空间（代码空间和数据空间）、应用实例非易失性空间(None Volatile Memory Space)、应用实例易失性空间(Volatile Memory Space)。
- SE批次信息：该应用所支持的SE批次信息
- SSD DAP签名：用于代理安全域三（DAP模式），由SSD所有者提供
- 应用类型，全网应用、省公司本地应用
- 依赖的应用扩展的列表。

5.4.3. 应用扩展

应用扩展是一种特殊的应用，用于提供其他应用所需要的扩展功能，只能进行加载，不能进行实例化，其属性如下：

- 应用AID：作为应用扩展的唯一标示，与其对应的可执行加载文件的AID相同
- 应用扩展结构：可执行加载文件对应的AID（Executable Load File AID），即为应用扩展的AID。
- 依赖的其他应用扩展的列表。
- 应用扩展所属应用提供商必为中国移动
- 文件及其Hash值：上传到多应用开放平台的应用应该是CAP文件类型，应用CAP文件Hash值，采用sha-1算法
- 应用扩展的可执行加载文件关联的安全域

- 生命周期状态：应用扩展的生命周期状态与包含其的应用生命周期相同，不对应用包含的各应用扩展进行单的生命周期管理。
- 内存空间信息：应用文件空间（代码空间和数据空间）。
- SE批次信息：该应用所支持的SE批次信息
- SSD DAP签名：用于代理安全域模式（DAP模式），由SSD所有者提供

5.4.4. 生命周期

根据应用在不同阶段的状态不同，应用生命周期分为初始、已审核、已测试、发布和已归档几个状态。其中，已测试和已发布属于产品管理阶段。

5.4.4.1. 应用配置及上传

应用提供商提交应用程序并提交该应用程序的结构，即将可执行加载文件及包含的可执行模块情况上报，对可执行加载文件中超过一个可执行模块的情况，另需指定一个可执行模块为主模块。多应用开放平台管理员向相关职能部门申请为该应用分配新的AID，该应用AID同时为主模块实例的AID，对可执行加载文件、其它可执行模块及可执行模块的实例也需分配相应的AID，并录入相关信息到系统，其中系统管理的应用程序版本号格式为：应用AID+软件版本号+日期，软件版本号由应用提供商提供，日期采用YYYYMMDD的格式。

5.4.4.2. 应用审核

具有审核权限管理员对提交的应用程序进行审核，给出审核结果（通过或者不通过）。

5.4.4.3. 应用测试

具有测试权限的测试人员对通过审核后的应用程序进行测试。若测试通过，记录该应用支持的SE卡的批次号、版本信息。管理员可以在多应用开放平台确认测试完成。

应用在测试阶段，仅可对系统设置的测试号进行测试。

5.4.4.4. 应用发布

具有应用发布权限的系统操作员可以对通过测试的应用进行发布操作，使得应用得以被应用发现Portal发现，并被用户所见。

应用发布时，可指定该应用适用的SE卡的批次号、版本信息。

应用发布时，可指定该应用适用的用户列表。

5.4.4.5. 应用归档

成功发布后的应用可以进行“注销”操作，当管理员确认注销某应用，应用程序进入归档状态且不再使用。应分为归档开始和归档结束两个状态

应用归档后应将用户已下载至NFC终端SE中的应用进行删除。应用删除方法分为系统主动删除和通知用户自行删除两种，可以根据不同业务类型由多应用接入管理平台决定，系统主动删除操作也需事先通过短信通知用户并且在用户同意的情况下进行，如果系统主动删除应用时失败，系统应具备相应的重试机制。

5.4.5. 应用发行模式

针对不同应用提供商和业务的需求，多应用开放平台提供多种应用发行模式，主要包括应用下载及个人化模式和个人化模式，对未预置应用的NFC终端选择执行应用下载及应用个人化操作，对预置应用的仅需执行应用个人化操作。

5.4.6. 应用删除模式

与应用发行相对，多应用开放平台提供多种应用删除模式。在应用需要被更新或者应用已经无效的情况下，多应用开放平台可以删除SE上的应用代码及所有相关的个人化信息。应用被删除后，应用空间将会被SE回收并用于新的应用的下载。多应用开放平台也可以仅删除SE上的应用实例及个人化信息，应用的代码被保留在SE中，需要重新使用应用时，仅需要创建应用的实例并下载应用个人化信息。

5.4.7. 终端应用管理

多应用开放平台管理 SE 上的 CMS^{2}AC 应用对应的终端应用，终端应用配合 CMS^{2}AC 应用，提供 UI 操作界面及远程操作功能。

多应用开放平台提供功能上载终端应用，提供门户便于用户下载终端应用。

5.4.8. Mifare 应用管理

多应用开放平台提供 Mifare 应用的管理。可上载、配置 Mifare 应用到多应用开放平台。可下载、删除、激活 Mifare 应用。

5.5. 用户管理

多应用开放平台的用户唯一标识由 NFC 终端 SE 的 SE_ID 唯一标识。

5.5.1. 用户信息管理

多应用开放平台统一管理用户 NFC 终端 SE 基本信息，SE 的 SE_ID、批次、密钥等信息以及动态信息。

用户 SE 的唯一标识为 SE_ID，用于用户身份识别及业务订购关系。

用户 SE 的批次信息详见 SE 设备管理。

用户 SE 的已下载安全域、已下载应用（包括可执行安装文件、可执行安装模块、已创建应用实例等）。

~~对实名制需求的业务，在实名业务时，需绑定 SE_ID。~~

用户 SE 上信息可通过 GET_DATA 进行同步获取。

5.5.2. 用户注册

使用嵌入 SE 安全元件的 NFC 终端的中国移动用户，使用 NFC 终端上预置手机钱包客户端时登录到多应用开放平台，多应用开放平台发现用户的 SE 未注册，即用户的手机号码 MSISDN 未绑定 SE，多应用开放平台绑定手机手机号码及 SE_ID，完成用户的自动注册。

完成注册后，用户可通过手机钱包客户端进行应用发行、应用下载等业务操作。

若 SE 已注册，即 SE 与其他用户手机号码 MSISDN 有绑定关系，则多应用开放平台不能进行注册，用户不能进行多应用业务的操作。

用户手机号码 MSISDN 可绑定多个 SE，一个 SE 仅能绑定到唯一一个手机号码。

SE_ID 为 SE 安全元件的唯一的物理标识。

对使用嵌入 SE 安全元件的贴片卡的中国移动用户不提供注册功能。

用户使用 NFC 终端上手机钱包客户端登录多应用开放平台，多应用开放平台获取用户手机号码及 SE，如下处理流程。

1. 用户手机号码与 SE 已注册，手机钱包客户端登录完成，若业务系统有退订通知，多应用开放平台自动删除已退订未删除应用。
2. SE 都未绑定，则多应用开放平台自动完成用户注册，手机钱包客户端登录完成。如果 SE 与其他手机号码存在绑定关系，同时 SE 上有原手机号码订购应用，应提示用户完成原有手机号码上已下载应用（该应用的订购关系已解除，若已下载应用的订购关系未解除，SE 与原有用户手机号码的绑定关系不能解除）的删除。
3. SE 与其他用户手机号码已绑定。
   a) 如果原有手机号码在网，则提示用户，手机钱包客户端登录后仅能查询应用，不能进行应用下载或删除。
   b) 如果原有手机号码已销号，则多应用开放平台自动完成注册，SE 与手机号码绑定，用户不能下载 SE 上原有手机号码已订购应用。用户需通过客服或营业厅进行原有手机号码已订购应用的退订。

以上各流程之前，多应用开放平台应检查 SE 是否在挂失名单中，且 SE 与用户手机号码无绑定关系，多应用开放平台下发应用锁定指令。

用户注册过程中，多应用开放平台需要使用 STORE_DATA 指令向 SE 中写入 MSISDN、TOKEN 以及 IMSI 摘要。

其中 MSISDN 的标签值为 2F14，数据报文参见《中国移动 SE 多安全域多应用管理技术规范》

TOKEN 及 IMSI 摘要的标签值为 1047，数据报文格式如下：

表 5-1　Token 及 IMSI 格式

长度	描述	取值

2	卡唯一标识 Tag	1047
1	子 tag1（Token）	01
1	Token 长度	X
X	Token 数据	
1	子 tag2（IMSI 摘要）	02
1	IMSI 摘要长度	Y
Y	IMSI 摘要	

多应用开放平台通过 SEID、日期分散出 TOKEN，并加密存储。同时对动态 TOKEN 设置有效期，若 TOKEN 已失效，手机钱包客户端登录时，多应用开放平台需验证原 TOKEN 值，并生成新的 TOKEN 设置到 SE 中。

5.5.3. 用户注销

使用嵌入 SE 安全元件 NFC 终端的中国移动用户，可使用 NFC 终端上预置手机钱包客户端，请求用户注销，多应用开放平台接收到用户注销请求，检查用户手机号码与 SE_ID 有绑定关系，多应用开放平台解除用户手机号码与 MSISDN 的绑定关系。在注销前，用户需退订 SE 上所有业务，用户可使用 NFC 终端上手机钱包客户端请求注销时，可自动发起支持空中方式退订的应用删除流程，若已订购应用需要现场办理应用删除，手机钱包客户端可提示用户营业厅办理相关应用删除。

对使用嵌入 SE 安全元件的贴片卡的中国移动用户不提供注销功能。

5.5.4. 业务迁移

业务迁移指不改变应用订购关系情况下，将应用从一 NFC 终端上迁移到另一个终端上。上述终端需同时注册到用户的手机号码上，迁移后原终端删除应用。用户可通过 NFC 终端、多应用开放平台用户自服务、客服自服务、营业厅进行业务迁移。

如果用户有多个业务迁移，需执行多次业务迁移操作。

5.5.5. BOSS 换号

用户前往营业厅办理 BOSS 换号业务后，需使用营业厅专用 POS 进行 NFC 终端的 SE 上绑定的用户手机号码的更新。对于换号后，需要重新个人化的应用，进行应用的个人化。

5.5.6. 用户退网

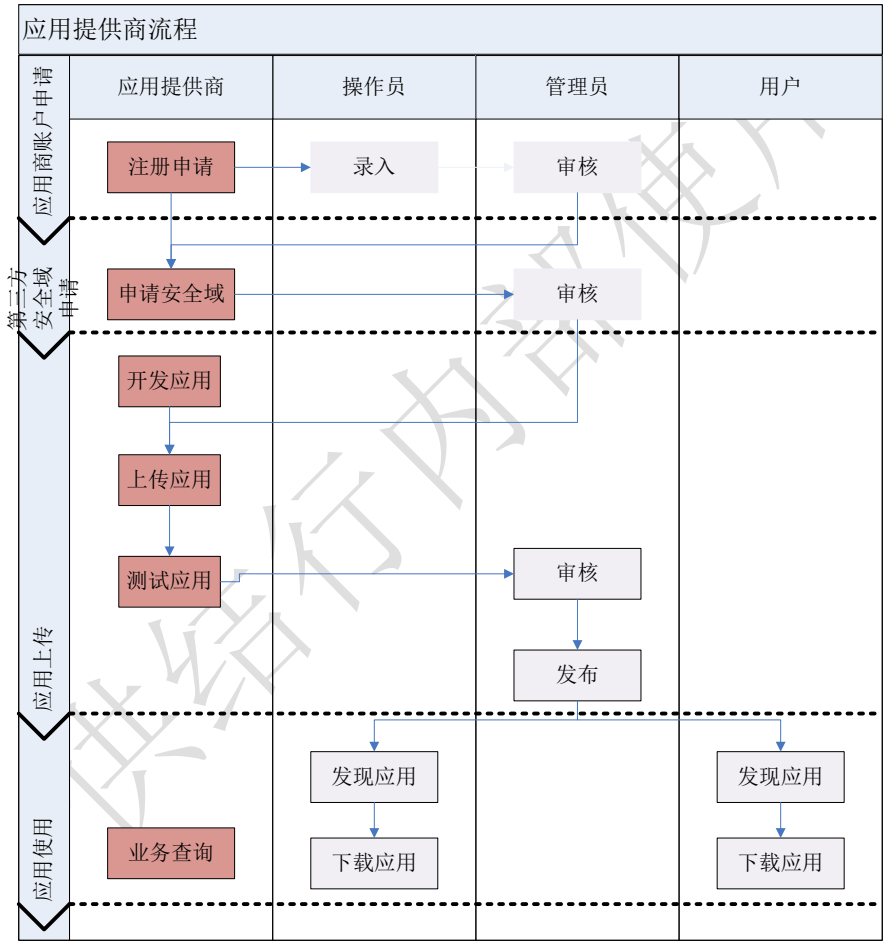
用户退网后，用户注册的 NFC 终端应用与用户的手机号码解除绑定关系。NFC 终端可以绑定到新的手机号码上，但原手机号码订购的应用处理：

1. 若获取业务系统的退订通知后，可进行删除。

2. 未获取退订通知的应用，不能删除。

5.6. 应用提供商管理

多应用开放平台管理业务的应用提供商，提供注册、查询、修改和注销等多种管理功能。



5.6.1. 属性

应用提供商的属性分为基本属性和扩展属性，应用提供商可以通过管理界面自行修改扩展属性，基本属性只能由系统管理员修改。基本属性主要包括：应用提供商编号、应用提供商名称、应用提供商类型、工商局注册编号、经营许可证编号、提供应用类型和合作类型等；

扩展属性包括：地址、邮编、电话、传真、联系人信息等内容。

5.6.2. 应用提供商注册

业务管理员负责应用提供商的注册，~~应用提供商需要提交书面材料，~~业务管理员将注册资料信息存储在多应用开放平台。在多应用平台注册后同时需要具有审批权限的业务管理员进行审批，审批通过后，将为应用提供商分配 SPID 及多应用开放平台登录账号和密码，并将账号和密码通知应用提供商。

5.6.3. 应用提供商信息查询

多应用开放平台系统提供对已经成功注册的应用提供商信息进行查询的功能，包括审核成功、在审和审核失败三种状态的提供商。

5.6.4. 应用提供商信息修改

多应用开放平台对应用提供商的注册资料、已提交的应用文件及参数配置进行存储管理。

应用提供商可以通过中国移动为其分配的应用提供商的登录账号登录多应用开放平台的应用提供商门户，修改其扩展材料。

应用提供商如需要对基本资料进行修改，需先向中国移动书面申请，获取审批后，由多应用开放平台操作员对其基本资料进行修改。

5.6.5. 应用提供商注销

应用提供商不再与中国移动合作时，多应用开放平台的管理员将从多应用开放平台注销应用提供商的账号及相关资料信息，并通知应用提供商。

应用提供商注销前，该应用提供商所提供的所有应用进行归档操作。

5.6.6. 应用提供商黑名单管理

多应用开放平台业务管理管理员可以对应用提供商黑名单进行管理，包括将应用提供商添加至黑名单，从黑名单移除应用提供商。同时提供查询黑名单操作。

应用提供商进入黑名单后，禁止该应用提供商登录多应用开放平台，同时该应用提供商的所有应用禁止下载及安装，但可对已下载的应用的用户进行删除、锁定等操作。

5.6.7. 应用提供商自服务

5.6.7.1. 业务展现密码更新

应用提供商可修改多应用开放平台的登录密码，多应用开放平台更新其新的密码信息并通知应用提供商密码更新成功。

5.6.7.2. 应用查询

应用提供商可按照应用状态、时间查询所属应用的信息。
应用提供商可按照日期、用户手机号、用户 SEID 等条件，查询应用下载信息。

5.6.7.3. SE 信息查询

应用提供商可查询 SE 信息，包括已注册 SE 数量、SE 的可用空间信息。

5.7. 业务管理

5.7.1. 业务鉴权授权

多应用开放平台具备对接入的业务平台的实时控制能力。在业务平台接入并调用相应能力时，多应用开放平台需要对该业务平台及该业务对应的应用提供商、用户订购关系进行鉴权（Authentication），同时需对业务平台请求调用的能力进行授权（Authorizaiton）。业务平台可调用的能力需要灵活配置，多应用开放平台提供的能力包括应用下载、删除、个人化/个人化更新、安全域创建/删除/密钥更新、应用锁定/解锁、应用指令等。

5.7.2. 计费管理

计费功能管理指定了业务运营过程中对应用提供商计费策略，并结合运营数据生成计费数据。多应用平台对应用提供商收取NFC终端SE空间使用费以及使用业务的功能费。

5.7.2.1. 计费规则管理

计费规则管理包括计费种类以及计费策略管理：

- 计费种类管理：包括对计费种类的增加、查询、修改、删除（非物理删除，指归档）。
  - 增加：增加应用提供商的收费类型，需有类型编号、类型解释、启用标志等
  - 查询：具备权限的业务管理员可以查看到所有计费类型，包括删除的计费类型
  - 修改：具备权限的业务管理员可以修改计费类型的解释，或者启用/禁用计费类型
  - 删除：对不再使用的计费类型，具备权限的业务管理员可以删除。
- 计费策略管理：对不同计费种类的实际计费实施进行策略配置。
  - 应用提供商计费策略：包括对计费周期（生成计费单的周期）、计费粒度（如按大小 K 字节等）、对不同计费种类的打包计费等参数配置，应用提供商的个性化交易佣金计算策略（如按交易量或交易时间段等配置不同费率）

5.7.2.2. 空间计费

对应用提供商进行空间计费时，按照以下规则生成计费单。

5.7.2.2.1. 计费生成

	应用提供商类型	计费条件				计费
		操作类型	安全域类型	应用所属安全域	大小	
1	中国移动	应用下载		不限	xx	不计费
2		安全域创建	不限		xx	不计费
3		预置自有应用		不限	xx	不计费
4		预置自有安全域	不限			不计费
5	第三方	应用下载		不固定空间安全域	xx	用户数*空间大小*单价
6				固定空间安全域	0	不计费
7		安全域创建	不固定空间		0	不计费
8			固定空间		xx	用户数*空间大小*单价
9		预置安全域	不固定空间		0	不计费
10			固定空间		xx	用户数*空间大小*单价
11		预置应用		不固定空间	xx	用户数*空

						间大小*单价
12				固定空间	0	不计费

5.7.2.2.2. 计费解除

	应用提供商类型	订购关系			
		操作类型	安全域类型	应用所属安全域	大小
1	中国移动	应用删除		不限	xx
2		安全域删除	不限		xx
5	第三方	应用删除		不限	xx
7		安全域删除	不限		0

注，删除应用的所有数据及文件时，多应用开放平台解除该用户的订购关系，如果仅删除应用实例，未删除应用文件，则多应用开放平台保留订购关系。

5.7.2.3. 功能计费

对应用下载、个人化、删除、锁定、解锁、个人化更新、安全域密钥更新、安全域创建、删除等业务操作按次或包月进行计费。

5.7.2.4. 计费单管理

1、计费单

多应用开放平台提供给BOSS系统计费使用的计费单文件，包括空间计费及功能计费；

2、计费单文件传输

计费单文件通过FTP协议传输，具备传输错误处理机制，保证计费单传输的完整、准确、及时。

3、计费单文件产生机制：按计费规则设定自动生成。

5.7.3. 系统管理

5.7.3.1. 角色管理

通过角色管理，可以对角色进行增加、删除和修改操作，同时可以为角色设置相应权限。

5.7.3.2. 权限管理

通过权限管理，对系统的权限进行增加、删除和修改操作。

5.7.3.3. 用户管理

通过用户管理，可以对系统的用户进行增加、删除、修改和查询等操作，也可以将用户分配角色。

5.7.3.4. 参数管理

参数管理部分包含业务管理系统参数配置信息的管理，包括增加、查询、修改和删除参数等功能。

5.8. SE 管理

5.8.1. SE 设备管理

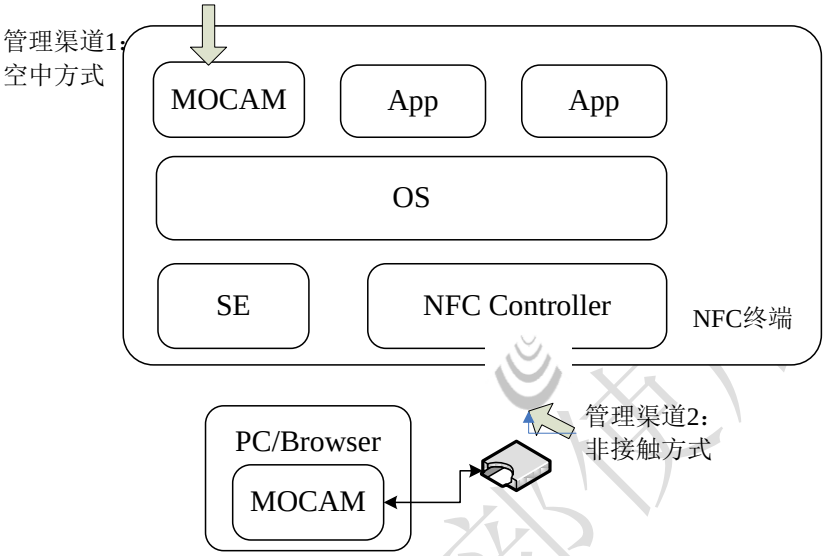
多应用开放平台根据 SE 的 SEID 号段为标识，进行 SE 设备管理，系统管理员对 SE 的批次信息进行配置及管理。

多应用开放平台根据 SE 的 SEID 号段，管理该批次 SE 主安全域的根密钥或动态密钥。主安全域密钥存储于加密机中。

多应用开放平台根据 SE 的 SEID 号段，管理该批次 SE 芯片类型、CMS2AC 版本、Java 版本信息。

多应用开放平台根据 SE 的 SEID 号段，管理该批次 SE 的初始可用空间、预置应用、预置内存类型（只读、可擦写）及状态、预置负责安全域、及状态。

5.8.2. 管理渠道



管理渠道是指在NFC终端SE与多应用开放平台之间进行数据传输的形式。可选择的承载方式：非接触方式、远程GPRS。两种承载方式都需要应用管理器（手机钱包客户端）作为NFC终端SE与多应用开放平台之间的中介完成应用下载、删除及应用管理等操作。

5.8.2.1. 应用管理器

通过应用管理器(手机钱包客户端) 及写卡设备（包括非接触读卡器等）可以实现CMS^{2}AC 应用及辅助安全域的下载、删除、更新等业务管理操作。

多应用接入管理平台中保存 CMS^{2}AC 应用程序的数据，控制 CMS^{2}AC 应用程序的应用管理器承载的应用下载、删除、锁定、解锁等操作。

应用管理器承载可在营业厅、手机终端、PC终端上进行。

应用管理器承载特点为：

1. 通道建立快，只需要实现对多应用开放平台的登录即可进行操作
2. 基于IP网络进行大数据量传输，传输速度高
3. 数据传输可靠性高
4. 使用非接触方式时，用户必须到营业厅进行操作。
5. 在应用管理器承载下，通过SCP02协议保证应用下载的安全性

应用管理器承载详见《中国移动客户端应用管理器技术规范》。

5.8.3. SE 安全域管理

5.8.3.1. 安全域创建

5.8.3.1.1. 功能描述

安全域创建提供了在 NFC 终端 SE 上划分安全域的功能。安全域创建需指定用户及待创建安全域的 AID，由多应用开放平台根据指定安全域的属性（详见参见 5.2.3 节）在 SE 上划分安全域。多应用开放平台提供辅助安全域的创建，包括 5.2.3.5 节中所述模式二、三、四三种辅助安全域。

中国移动自有辅助安全域创建后，由多应用开放平台自动触发安全域密钥更新流程修改安全域初始密钥，然后下发指令更改安全域个人化状态为已个人化。

第三方辅助安全域创建后，第三方业务平台需要调用多应用开放平台提供提供的安全域密钥更新流程，从第三方业务平台获取安全域密钥；密钥更新成功后，更改安全域个人化状态为“已个人化”。安全域个人化后才能正常使用。

完成安全域创建后，多应用开放平台更新用户 SE 的状态，对固定空间安全域，用户 SE 的可用空间应减少该安全域的固定空间。并生成应用提供商的安全域的订购关系。

5.8.3.1.2. 技术实现

应用管理器请求多应用开放平台进行安全域创建，首先多应用开放平台通过应用管理器，与 SE 的主安全域建立安全通道，多应用开放平台下发 GET_DATA 指令获取并更新该用户 SE 的可用空间，然后下发安全域创建指令、安全域密钥更新指令以及状态设置指令。完成安全域创建后多应用开放平台用户 SE 的状态并计算可用空间。

安全域创建的流程及指令应遵循《中国移动 SE 多安全域多应用管理技术规范》。

5.8.3.2. 安全域密钥更新

5.8.3.2.1. 功能描述

多应用开放平台提供安全域密钥更新，完成自有业务平台、第三方业务平台更新安全域密钥。更新时需要指定安全域 AID 和新的安全域密钥。对于由中国移动控制的安全域，新的安全域密钥由多应用开放平台提供。对于第三方安全域新的安全域密钥由第三方业务平台提供并加密传输。

SE 上安全域的密钥处于更新状态时，所有的业务操作必须在完成密钥更新业务操作之

后才能进行。

5.8.3.2.2. 技术实现

应用管理器请求多应用开放平台进行安全域密钥更新，首先多应用开放平台通过应用管理器，与 SE 的指定辅助安全域建立安全通道，多应用开放平台安全域密钥更新指令以及状态设置指令。

安全域密钥更新的流程及指令应遵循《中国移动 SE 多安全域多应用管理技术规范》。可以更新主安全域及辅助安全域密钥。

5.8.3.3. 安全域删除

5.8.3.3.1. 功能描述

多应用开放平台提供辅助安全域密钥删除功能，完成自有业务平台、第三方业务平台辅助安全域删除。删除时需要指定安全域 AID，删除后 SE 将释放该安全域管理的空间。如果指定删除的安全域包含应用，需事先手动删除该安全域所包含应用。安全域删除后应解除应用提供商该安全域的订购关系。

主安全域不可被删除。

5.8.3.3.2. 技术实现

应用管理器请求多应用开放平台进行安全域删除，首先多应用开放平台通过应用管理器，与 SE 的主安全域建立安全通道，多应用开放平台下发安全域删除。完成安全域删除后多应用开放平台下发 GET_DATA 指令获取并更新该用户 SE 的状态及可用空间。

安全域删除的流程及指令应遵循《中国移动 SE 多安全域多应用管理技术规范》。

5.8.4. SE 应用管理

5.8.4.1. 应用下载

5.8.4.1.1. 功能描述

多应用开放平台提供应用下载功能，应用下载时，需指定待下载应用的 AID_{16}，对于第三方应用提供商的应用下载，在下载前需要对用户的通信状态进行鉴权，下载成功后，需记录用户的状态。

首先前应检查应用的版本与 SE 批次及版本的有效性匹配，鉴权应用提供商的下载权限，以及应用的用户匹配性。

检查应用的所属安全域是否已在用户的 SE 上创建，若未创建首先进行安全域创建。

应用下载时，多应用开放平台检查应用的状态，依次下载应用包含的所有可执行加载文件及相关联的应用扩展文件、安装可执行模块、安装可执行加载模块的实例等操作。应根据应用执行状态的属性（参见 5.3.11.2 节定义），完成应用下载的操作；例如应用所关联的可执行加载文件及可执行加载模块已安装，多应用开放平台仅安装可执行加载模块的实例

应用所属的安全域和可执行加载文件所属的安全域不同时，应用先安装到文件关联的安全域，之后通过迁移操作关联到应用所属的安全域。

同一可执行加载文件可创建多个应用实例。

应用下载完成后多应用开放平台应更新该用户 SE 的状态及可用空间。

5.8.4.1.2. 技术实现

应用管理器请求多应用开放平台进行应用下载，首先多应用开放平台通过应用管理器，与 SE 上的主安全域或应用所属安全域（可由平台配置）建立安全通道，多应用开放平台下发 GET_DATA 指令获取并更新该用户 SE 的可用空间，并检查可用空间匹配性；多应用开放平台根据应用的状态，封装安装应用、加载应用、安装应用实例等指令，通过应用管理器逐条下发给 SE。完成应用下载后，多应用开放平台更新用户 SE 的状态及可用空间。

在执行过程中，若 SE 返回失败状态字，应用管理器应立即返回状态字给多应用开放平台，流程结束。

应用下载的流程及指令应遵循《中国移动 SE 多安全域多应用管理技术规范》。

5.8.4.2. 应用删除

5.8.4.2.1. 功能描述

多应用开放平台提供应用删除功能。应用删除需要指定待删除应用的 AID。

删除前，首先应鉴权应用提供商删除权限，并根据遵循应用的删除模式，若应用的可执行加载文件对应多个应用实例，忽略应用的删除模式，仅删除该应用实例，保留应用的可执行安装文件及可执行模块。应用删除完成后多应用开放平台应更新用户 SE 的状态及可用空间并解除订购关系。

应用的删除原则上由其关联的安全域进行，同时保留主安全域删除应用的权限。具体策略由平台设定。同一可执行加载文件生成的多个应用实例不应有依赖关系，应该能独立管理其生命周期。

5.8.4.2.2. 技术实现

应用管理器请求多应用开放平台进行应用删除，首先多应用开放平台通过应用管理器，与 SE 上的主安全域或应用所属安全域（可由平台配置）建立安全通道，多应用开放平台根据应用的状态及应用删除模式，封装应用删除等指令，通过应用管理器下发给 SE。完成应用下载后，多应用开放平台下发 GET_DATA 指令获取并更新该用户 SE 的状态及可用空间。

应用在不可擦写永久存储器，应用删除

应用删除的流程及指令应遵循《中国移动 SE 多安全域多应用管理技术规范》。

5.8.4.3. 应用解锁/锁定

5.8.4.3.1. 功能描述

应用锁定指对用户在SE上已开通的应用进行锁定，使其不能再使用。应用解锁指对SE上已被锁定的应用进行逆操作，使其恢复使用。

应用解锁仅能在营业厅进行操作。

应用锁定的业务场景可以用于（但不限于）当用户丢失 NFC 终端时，可以采用应用锁定来关闭应用程序，避免或减少用户损失。

对于临时需要禁用的应用，也可通过多应用开放平台对应用进行锁定操作。在应用被锁定后，用户将无法使用此应用，但该应用相关的个人数据不会被删除，应用锁定后不变更用户的订购关系；在应用被解锁后，用户可继续使用此应用。

应用锁定的其他业务场景可由具体需求确定。

5.8.4.3.2. 技术实现

应用管理器请求多应用开放平台进行应用锁定/解锁，首先多应用开放平台通过应用管理器，与SE上的主安全域或应用所属安全域（可由平台配置）建立安全通道，多应用开放平台，封装应用锁定/解锁指令，通过应用管理器下发给SE。完成应用锁定/解锁后，多应用开放平台更新该用户SE状态。

若应用包含多个 Applet 实例，需对每个实例进行锁定/解锁操作。

应用解锁/锁定的流程及指令符合《中国移动 SE 多安全域多应用管理技术规范》。

5.8.4.4. 个人化数据管理

5.8.4.4.1. 功能描述

多应用开放平台提供智能通道，完成业务平台及 SE 之间应用数据的交互。个人化数据管理包括应用个人化、个人化数据更新、获取个人化数据等功能。

5.8.4.4.2. 技术实现

业务平台可在应用下载后，利用应用下载应用管理器与多应用开放平台的链接进行应用的个人化数据管理，或业务平台可利用多应用开放平台的 SMS Push 功能，请求应用管理器建立链接，进行应用个人化或个人化更新。详见应用个人化。

5.8.4.5. 信息同步

多应用开放平台可通过 GET_DATA 获取 SE 上的静态及动态数据，包括批次、可用空间、已下载应用等。

5.8.4.6. 应用个人化

应用安装后，需要获得应用的个人化数据，包括自身的密钥和持卡人相关数据。根据个人化使用的安全通讯及密钥服务的类型，多应用开放平台~~完成~~提供以下三种应用个人化~~后，需要并建立应用提供商、应用及用户的订购关~~方式，~~系。~~

1、 使用应用自身密钥进行个人化数据的加密及安全传输。

2、 利用应用访问安全域服务的能力，使用安全域密钥进行个人化数据的加密及安全传输。

3、 利用安全域访问应用的能力，使用安全域密钥进行个人化数据的加密及安全传输。

SE 上应用个人化处理流程详见《中国移动 SE 多安全域多应用管理技术规范》。

5.8.4.6.1. 方式一

应用个人化可以通过方式一~~：应用指令实现，参见本规范应用指令小节。~~该方式的应用个人化，个人化指令由业务平台生成，多应用开放平台不对个人化指令进行处理，直接透传给 SE。

应用个人化指令的加密及 MAC 计算由业务平台负责。

~~多应用开放平台支持方式二：应用访问安全域密钥，进行个人化数据封装~~的方式以及方式三：安全域访问应用的个人化方式。如应用所属的安全域为主安全域或移动自有辅助安全域，即所属安全域的密钥由多应用开放平台管理，同时应用相关的密钥也同步多应用开放平

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： 1.38 厘米

带格式的： 字体：字体颜色：黑色，(国际) 宋体

带格式的： 字体颜色：黑色

带格式的： QB标题5，5 级，首行缩进： 0 字符，行距：多倍行距 1.73 字行，多级符号 + 级别：5 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0 厘米 + 制表符后于： 1.75 厘米 + 缩进位置： 1.75 厘米，制表位： 4.72 字符，左对齐

台的加密机中，到方式二、三的个人化指令可由多应用开放平台生成；如应用所属的安全域为第三方安全域，即所属安全域的密钥不由多应用开放平台管理，方式二、三的个人化流程同方式一。

多应用开放平台应可灵活配置个人化指令模式，例如可通过个人化指令模板。

5.8.4.6.2. 方式二

应用的个人化数据通过安全域密钥进行保护，由应用访问安全域密钥进行个人化数据的MAC 校验及解密。个人化指令由业务平台生成，多应用开放平台负责个人化指令加密及MAC 计算。业务平台和多应用开放平台传输的个人化指令通过传输密钥（TK）加密保护，其中敏感数据可使用密钥加密密钥（KEK）保护。

应用访问安全域密钥的个人化流程如下：

1. 业务平台请求多应用开放平台进行应用个人化~~操作~~，并提交个人化~~数据（非敏感数据，如应用序列号，发卡时间等数据~~指令。
2. ~~1.~~ 多应用开放平台对个人化指令进行解密（敏感数据任以 KEK 保护）；
3. ~~2.~~ 多应用开放平台与 SE 使用应用所属安全域密钥建立安全通道
4. ~~3.~~ 多应用开放平台加密~~生成~~个人化指令；~~填充业务平台提交的明文数据并调用加密机接口中获取密文包含的应用密钥。个人化指令格式由应用定义。多应用接入管理平台应配置应用密钥存储于加密机中的版本 Version 及索引号 Index。~~
   a) 多应用开放平台调用加密机，进行敏感数据转加密，即[敏感数据]$_{kek}$ 转为[敏感数据]$_{dek}$
   b) 根据安全通道~~的~~类型，加密~~下发~~个人化指令的数据域。
   c) 根据安全通道类型，计算个人化指令的 MAC 值。
5. ~~4.~~ 多应用开放平台下发个人化指令给 SE 上应用，由应用调用安全域的密钥进行个人化数据的 MAC 校验、解密以及敏感数据解密后，完成应用个人化。
6. ~~5.~~ 完成个人化操作，并向业务平台提交操作结果。

带格式的： 字体颜色：黑色

带格式的： QB标题5，5 级，行距：多倍行距 1.73 字行，多级符号 + 级别：5 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0 厘米 + 制表符后于： 1.75 厘米 + 缩进位置：1.75 厘米，制表位： 4.72 字符，左对齐

带格式的： 下标

带格式的： 非上标/ 下标

带格式的

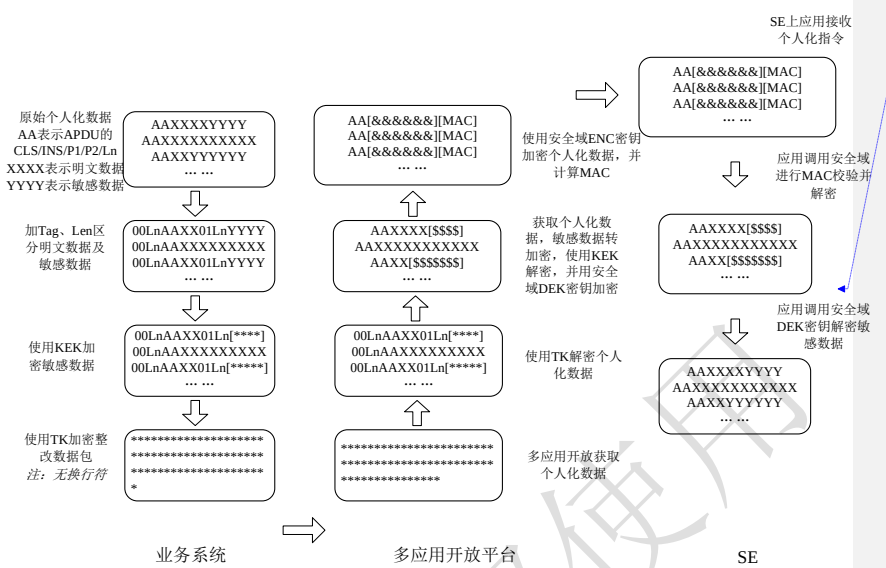


图 5-3　方式二个人化数据处理示意

5.8.4.6.3. 方式三

~~.~~应用的个人化数据通过安全域密钥进行保护，由安全域进行个人化数据的 MAC 校验及解密并转发给应用。个人化数据由业务平台生成，多应用开放平台负责个人化数据加密及 MAC 计算。业务平台和多应用开放平台传输的个人化数据通过传输密钥（TK）加密保护，其中敏感数据可使用密钥加密密钥（KEK）保护。安全域访问应用的个人化流程：

~~6.~~1. 业务平台请求多应用开放平台进行应用个人化~~操作~~，并提交个人化数据。~~（非敏感数据，如应用序列号，发卡时间等数据。~~

2. 多应用开放平台对个人化数据进行解密（敏感数据任以 KEK 保护）；

~~7.~~3. 多应用开放平台与 SE 使用应用所属安全域密钥建立安全通道。

4. 多应用开放平台生成 StoreData 个人化指令；~~应用的明文信息及密钥信息按照应用制定的格式作为 StoreData 指令的命令数据字段~~

a) 多应用开放平台调用加密机，进行敏感数据转加密；即$[敏感数据]_{kek}$转为$[敏感数据]_{dek}$。

b) 多应用开放平台生成并提交 Install for Personaliztion 指令给 SE 上安全域。

c) 多应用开放平台根据个人化数据，逐条生成 Store Data 指令给 SE 上安全域。

~~8.~~5. ~~。~~安全域获取 Store Data 指令，完成个人化数据的 MAC 校验和解密后，转发给应用进行个人化。

~~9. 根据安全通道的类型，下发个人化指令。~~

6. 完成个人化操作，并向业务平台提交操作结果。

安全域的个人化使用方式三。

带格式的：居中，与下段同页

带格式的：字体颜色：黑色

带格式的：QB标题5，5 级，行距：多倍行距 1.73 字行，多级符号 + 级别：5 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：1.75 厘米 + 缩进位置：1.75 厘米，制表位：4.72 字符，左对齐

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：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

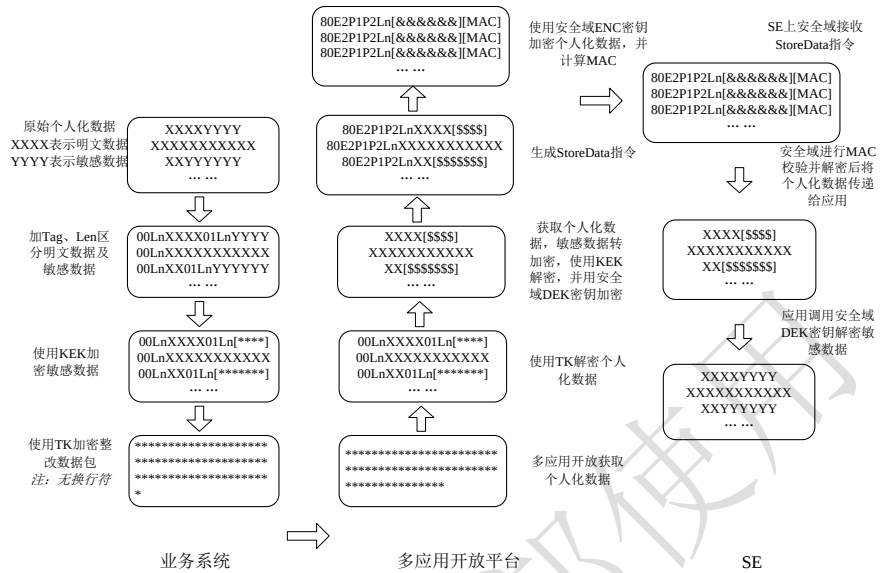


图 5-4 方式三个人化数据处理示意

5.8.5. 远程 PUSH

多应用开放平台提供 SMS Push 机制，使得业务平台及多应用开放平台具备业务推送能力。

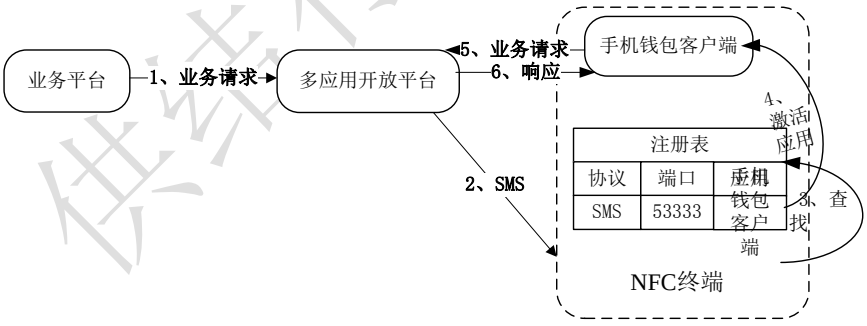


图 5-~~3~~ 5 PUSH 方式流程图

5.8.5.1. 先决条件

手机钱包客户端需事先向 NFC 终端注册 SMS 监听的端口号。
用户 SE 绑定 MSISDN。

5.8.5.2. PUSH 流程

业务平台或多应用开放平台可发起 PUSH 业务请求，多应用开放平台记录生成 Push 序列号以及任务操作及参数，并发送 SMS（SMS 数据中包含 Push 序列号）到 NFC 终端，NFC 终端收到 SMS 后，检查短信的端口号，并在注册表中发现注册短信端口的手机钱包客户端。若发现已注册应用 NFC 终端启动手机钱包客户端，并将 SMS 转发给手机钱包客户端。手机钱包客户端发起业务请求，参数为 Push 序列号，多应用开放平台接受到请求后，按照平台记录的 Push 序列号及业务类型，完成相应业务操作。

任务操作包括应用下载、应用删除、应用锁定、信息同步、安全域删除、安全域密钥更新、安全域创建以及自定义操作。

Push 序列号需保证唯一性，其格式由平台自行定义。

5.8.5.3. SMS 格式

图 5-1 PUSH 短信格式

带格式的：题注，居中，与下段同页

CMPP Header	CMPP body						
	UDH					SEID	Push serial
	UDHL	IEId	IEL	DA port	SRC port	……	
UDHI=1	06	05	04	XXXX	XXXX		

IEId详情参见《ETSI TS 123 040》9.2.3.24

注：NFC 终端上应用与多应用开放平台通过 HTTP 协议进行业务的交互，仅支持 Pull 业务模式。

5.8.6. 任务管理

多应用开放平台提供对任务的管理功能。任务是指根据用户请求，在指定的时间对指定的SE进行指定的操作。

多应用开放平台对任务的发起时间提供了定时、延时和即时3种方式，其中即时可以认为是参数时间为0的延时操作。

多应用开放平台对可以对单一的SE执行任务，也可以一次性对多个SE执行操作。

任务可以是应用下载、安全域创建等单独的操作，也可以是用户自定义的多个操作的组合。例如应用的升级操作就是先删除该应用然后再重新下载。

多应用开放平台对所有任务的操作结果进行管理，如果失败的任务，多应用开放平台应该对任务失败的原因进行统计，并分析解决方案。

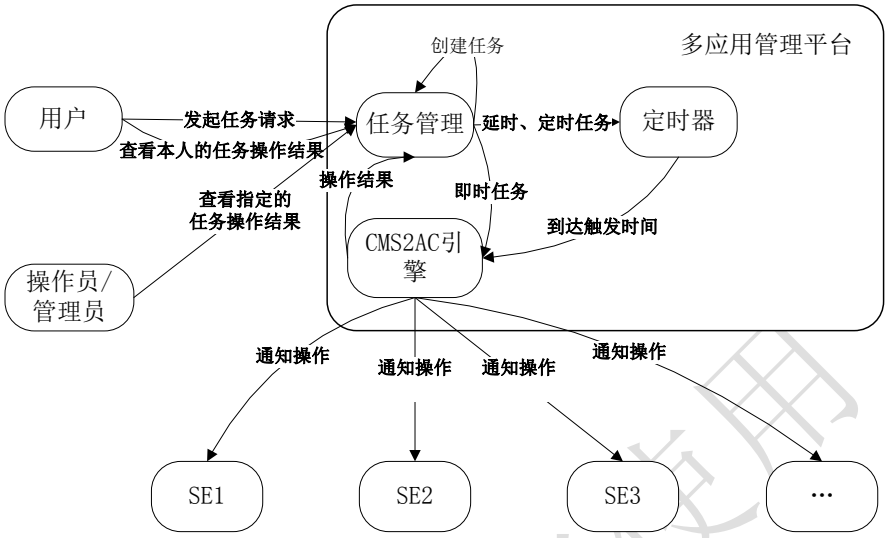


图 5-6　任务管理流程图

带格式的：与下段同页

带格式的：题注

5.8.7.　SE 及空间管理

5.8.7.1.　空间管理

具有 NFC 终端 SE 的可用空间分为不可变空间（包括不可变编码空间及不可变数据空间两部分）及可变数据空间。

下载安全域或 CMS^{2}AC 应用程序时，对于 CMS^{2}AC 应用程序所需代码空间， 多应用开放平台应通过 GET_DATA 指令获取 SE 内当前的可用空间（根据应用所属不固定空间或固定空间安全域类型，获取 SE 及安全域可用空间。），以便判断是否能够完成下载。同时多应用开放平台将计算并记录下载后的可用空间（下载前获取的可用空间-该应用程序的代码空间），

每次下载安全域或 CMS^{2}AC 应用程序之前，多应用开放平台先下发获取状态命令（GET_STATUS）获取 SE 内应用状态信息，据此判断是否需要删除上次未成功下载的残留数据。

在删除安全域或 CMS^{2}AC 应用之后，多应用开放平台下发 GET_DATA 指令获取删除后的可用空间（不可变空间及可变数据空间）。

注 1：CMS^{2}AC 应用文件占用不可变编码空间、应用实例占用不可变数据空间，应用运行占用可变数据空间。

注 2：安全域是一个应用，占用不可变编码空间、不可变数据空间、可变数据空间。以及安全域管理的空间。

注 3：在有第三方 TSM 下载应用后，多应用开放平台上记录的可用空间会出现偏差。因此空间数据仅作为参考数据。

注 3,：由于 SE 厂商实现差异，同一应用安装到不同的 SE 中所占空间会有细微差别，因此多应用开放平台管理应用所记录的占用空间为安装到各批次各厂商 SE 实际测试值的最大值。因此多应用开放平台计算的 SE 剩余空间（可用空间-登记的应用空间）应小于等于 SE 的实际空间。若多应用开放平台获取 SE 的剩余空间小于计算空间，则以 SE 实际空间为准，差异的空间标识为第三方应用。多应用开放平台的用户页面应显示记录应用空间及计算出的剩余空间，以保证用户体验的一致性。

5.8.7.2. 应用状态管理

应用的状态包括 Ready（初始即未下载）、Loaded（已下载）、Instantiated（已创建实例、未个人化状态）、Personalized（已个人化、未订购）、Locked 锁定、Usable（已订购）。

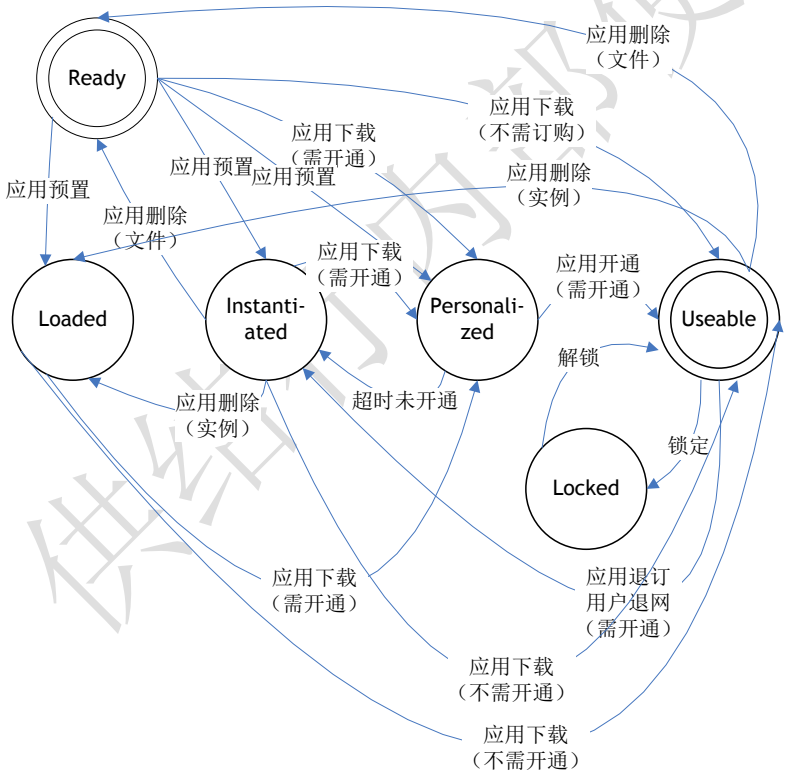


图 5-7 应用的状态图

Ready 状态，为起始状态，可通过应用预置转换到 Loaded、Instantiated、Personalized 状态。对于需要开通的应用，完成应用下载后从 Ready 转换到 Personalized 状态，对于不需开通的应用，完成应用下载后从 Ready 转换到 Usable 状态。在应用下载的过程中，多应用开放平台自动完成应用从 Ready、Loaded、Instantiated、Personalized、Useable 状态的转换。

带格式的：与下段同页

带格式的：题注，居中

若应用下载出现异常中断时，应用的状态可停留在 Loaded、Instantiated 等中间状态，再次进行应用下载时，多应用开放平台应从中间状态恢复应用下载。应用在 Instantiated、Useable 状态时，完成应用文件删除，转换为 Ready 状态；为 Ready 状态。对于不需个人化的应用，创建实例后，直接转换为 Personalized 状态，对于不需开通的应用，完成个人化后直接转换为 Useable 状态，对于即不需个人化也不需开通的应用，创建实例后直接转换为 Useable 状态。

Loaded 状态，在应用下载的过程，应用状态应经过 Loaded 状态。达到 Loaded 状态的条件是应用及其所属应用扩展完成安装。可通过应用下载转换到 Personalized 或 Useable 状态。应用在 Instantiated、Useable 状态时，完成应用实例删除，转换为 Loaded 状态。

Instantiated 状态，在应用下载的过程，应用状态应经过 Instantiated 状态。达到 Instantiated 状态的条件是应用及其所属应用扩展完成实例创建。可通过应用下载转换到 Personalized 或 Useable 状态。应用在 Useable 状态时，获取业务平台的退订通知、用户退网通知，转换为 Instantiated 状态；从 Useable 转换到 Instantiated 状态，无需进行 SE 操作，仅由多应用开放平台更改应用状态即可。

Personalized 状态，对于需要开通的应用，多应用开放平台完成应用下载后，转换为 Personalized 状态。多应用开放平台获取业务平台的开通通知后，将应用状态转换为 Usable 状态。在系统设定的周期内，未收到业务平台的开通通知，多应用开放平台自动将应用状态转换为 Instantiated 状态。

Useable 状态，对于需要开通的应用，多应用开放平台获取开通通知后，由 Personalized 转换为 Useable 状态。对于不需开通的应用，完成应用下载后，可由 Ready、Loaded、Instantiated 等状态转换为 Useable 状态。

Locked 状态，对 Useable 状态的应用可进行锁定操作，进入 Locked 状态。Locked 状态解锁后重新转换为 Useable 状态。应用在其他状态不提供锁定功能。

应用处于 Ready、Loaded、Instantiated 状态时，应显示在手机钱包客户端的应用下载列表中。应用处于 Instantiated 状态时，应显示在手机钱包客户端的应用删除列表中；对于不需开通的应用，应用处于 Useable 状态时，应显示在手机钱包客户端的应用删除列表中。应用处于 Useable 状态时，应显示在手机钱包客户端的应用锁定列表中。应用处于 Locked 状态时，应显示在手机钱包客户端的应用解锁列表中。

对于无需个人化但需开通的应用，完成应用下载后，从 Ready 状态转换为 Personalized，若超时未收到业务平台的开通通知，应用状态应用从 Personalized 转换为 Instantiated 状态。用户可选择进行应用删除。若用户选择应用下载，多应用开放平台仅将应用状态转换为 Personalized 即可，无需进行个人化操作。

应用扩展无独立的状态，与所属应用的状态相同。

5.8.7.3. 逻辑通道

SE 应支持多个逻辑通道，用于支持手机钱包客户端及客户端等终端应用对 SE 的访问。

5.8.8. 并发控制

多应用开放平台与每一用户 SE 仅建立唯一的数据链接，其他任务进入队列等待执行。如果应用管理器在用户 SE 等待多应用开放平台下载数据期间用户发起另一次下载、删除或列表更新申请，则应用管理器需要提示用户是否取消上次的下载申请，并根据用户选择结果

只保留一个操作。

在多应用开放平台下发应用下载操作之前，应先发送 GET_STATUS 指令给用户卡，查看用户卡上是否存在没有下载完成的应用。如果有，则多应用开放平台应首先发送删除应用操作以便删除不完整的应用，再下发新的应用下载操作。

如果 SE 在等待多应用开放平台反馈操作命令的反馈数据时，多应用开放平台发起了新的操作命令，则 SE 应优先处理多应用开放平台下发的新的操作命令，放弃等待中的原来申请指令。

多应用开放平台应提供功能，查询用户 SE 正执行任务及队列中排队的所有待处理任务操作，并可终止正执行任务操作。

5.8.9. 数据下载的安全认证

5.8.9.1. 数据的安全认证

多应用开放平台平台与 SE 进行的业务数据传输需启用计数器、MAC 校验、数据加密等机制，以避免数据重传、数据篡改、数据窃取带来的安全性问题。

SE 对于 CMS^{2}AC 应用程序应提供如下三个级别的安全：

- 双向认证：卡和卡外实体能相互认知对方；
- 完整性和数据源认证：SE 应保证其收到的数据确实是来自于已认证过的卡外实体并按照正确的顺序发过来的，并且保证数据未被修改过；
- 机密性：数据从卡外实体传向卡的过程中不应被未经认证的实体看到。

5.8.9.2. 安全信道

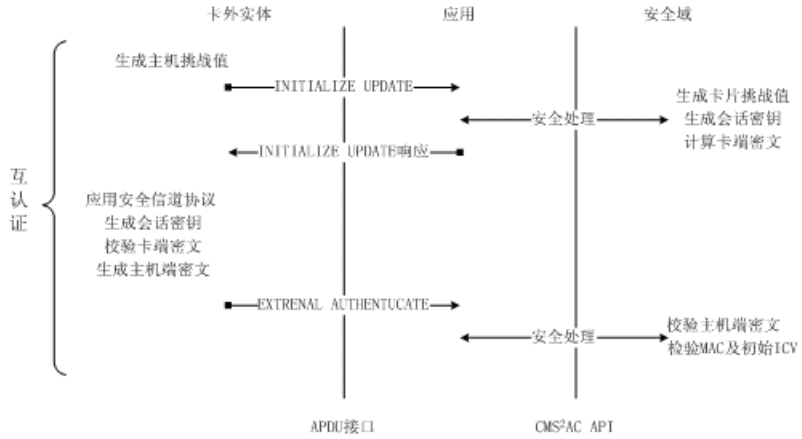
多应用开放平台与 SE 之间使用主安全域密钥建立安全信道的能力。应用下载、删除、安全域创建、删除时，其 APDU 命令需要在建立安全信道之后传输。

安全信道的建立流程采用显式安全信道初始化流程，安全信道以 CMS2AC SCP02 为基础，具体要求如下：

RMAC	隐式信道	显示信道	Session key Algorithm	C-MAC	R-MAC	ENCR
不需求	不要求	必选	SCP02	SCP02	不要求	必选

建立安全信道的认证流程图如下：

当服务器向 SE 发送 APDU 时，首先需要产生出 host challenge 下发到 SE，SE 产生 session key，card challenge 并计算出 card cryptogram 返回到服务器。服务器在对 card cryptogram 验证正确后，产生 session key 并计算出 host cryptogram 下发到 SE。SE 验证 host cryptogram 和 MAC 后，建立安全信道完成。



多应用开放平台建立安全通道，应支持安全级别 01、02、03 三种安全选项，并可进行动态配置。详见《中国移动 SE 多安全域多应用管理技术规范》。

5.8.9.3. 密钥管理

多应用开放平台与 SE 交互时，应使用到主安全域及辅助安全域的密钥。各安全域的密钥包括：安全信道加密密钥（S-ENC）、安全信道报文鉴权码密钥（S-MAC）、数据加密密钥（DEK）、DAP 密钥（可选）、Token 密钥（可选）以及密钥 KIc、KID。

使用 SCP02 信道时，应使用对应安全域的 S-ENC、S-MAC、DEK 密钥进行加密及 MAC 校验。使用 SCP80 信道时，应使用对应安全域的 KIc、KID 密钥。

多应用开放平台的交易加密机应从密管中心同步主安全域密钥及移动自有辅助安全域密钥。第三方辅助安全域的密钥应由第三方平台管理。对 DAP 模式的第三方辅助安全域的相关操作，多应用开放平台仅提供数据传输通道，数据的生成、加密以及 MAC 校验由第三方平台完成，对 Token 模式的辅助安全域，多应用开放平台提供接口给第三方平台完成 Token 验证。

由于对批量用户的安全域密钥更新需要一个过程，因此多应用开放平台在支持同一安全域在 SE 上使用不同的密钥版本进行 SE 相关操作。

参见《中国移动 SE 多安全域多应用管理技术规范》及《中国移动手机支付密钥管理-OTA 密钥管理分册》

5.8.9.4. 密钥产生

参见《中国移动手机支付密钥管理-OTA 密钥管理分册》

5.8.9.5. 密钥存储

参见《中国移动手机支付密钥管理-OTA 密钥管理分册》

5.8.9.6. 计数器

多应用开放平台维护两个计数器，分别为 SCP80 密钥及 SCP02 密钥计数器，详情参见《中国移动 SE 多安全域多应用管理技术规范》。

5.8.10. Mifare 引擎

5.8.10.1. Mifare Card Manager

多应用开放平台与运行在安全元件 SE 中的 Mifare Card Manager 进行交换，完成 SE 中所有的 Mifare 应用程序的生命周期管理，同时多应用开放平台负责读写 SE 中嵌入的 Mifare Emulator 的内存区。Mifare Card Manager 的 AID 为 A0 00 00 03 96 4D 66 34 4D 00 02。

5.8.10.2. Mifare 应用下载

应用管理器请求多应用开放平台 Mifare 应用下载，多应用开放平台与 SE 创建安全通道，并下载 Mifare 应用。详细指令参见《中国移动多应用开放平台接口方案》

5.8.10.3. Mifare 应用删除

应用管理器请求多应用开放平台 Mifare 应用删除，多应用开放平台与 SE 创建安全通道，并删除指定的 Mifare 应用。详细指令参见《中国移动多应用开放平台接口方案》

5.8.10.4. Mifare 信息同步

应用管理器请求多应用开放平台获取 Mifare 安装信息。详细指令参见《中国移动多应用开放平台接口方案》

5.9. 业务展现

多应用开放平台业务展现模块是包含全网应用与应用相关信息的展现平台，实现了对应用、安全域及应用提供商的管理。

5.9.1. 应用发现 PORTAL

多应用开放平台业务展现部分含有“帮助用户统一发现应用”的职责。应用范围包括本省及全网业务。需要展现给用户不同的应用发行方法。

- 使用文本介绍（如：发送某短信指令到某短信子号开通业务）
- 使用超链接导航至相关业务平台的 Portal 订购页面

- 展现给用户所有非接触业务的手机客户端程序画面，由用户选择下载相应的客户端软件，并安装在手机终端，自行发起应用发行的操作。

5.9.2. 用户自服务

用户可在用户自服务门户进行自助注册和注销，注册时需要输入用户的语言信息/用户Email 信箱/用户地址/用户邮编/家庭电话/公司电话等用户基本信息，该信息是可以查询并可由用户灵活修改的。注册后产生登录密码，并以短信方式发送给用户。

成功注册的用户可以通过输入手机号码和登录密码登录到用户自服务界面，无论用户是在中央还是归属省的门户注册，在归属省和中央任何一个门户均可登陆。

用户自服务支持用户查询已下载的安全域及应用、以及应用关联的可执行加载文件及可执行加载模块，SE 上已使用空间和可用空间，从而使用户有方便的渠道了解 SE 空间管理及利用情况。查询的已下载应用及空间信息包括本地应用和全网应用。

5.9.3. 应用提供商自服务

应用提供商必须在多应用开放平台注册，由多应用开放平台具有审批权限的管理员进行审批，审批通过后，将为应用提供商分配其编号及业务应用平台登录账号和密码，并将账号和密码通知应用提供商。操作员将注册资料信息存储在多应用开放平台。

对已注册的应用提供商，可输入账号和密码登录自服务门户，通过自服务门户可实现基本信息查询、已提交的应用状态查询等自助操作。

5.9.4. 客服自服务

客服人员可通过多应用开放平台客服服务功能帮助用户完成应用下载、删除、锁定/解锁、业务迁移操作。查询用户及SE信息。

客服人员需设定地区，客服人员仅能够设定地区内用户的客服功能。

6. 性能要求

6.1. 吞吐量

多应用开放平台应根据部署省用户数、活跃度制定吞吐量要求。多应用开放平台应具备动态扩容能力，以满足用户规模、活跃度变化的需要。

多应用开放平台的吞吐量既要满足应用下载及管理日常业务需求，又要满足新的业务升级海量更新（在一定时间要求内，对所有用户进行更新）的需求。多应用开放平台的吞吐量主要应考虑短信、TCP 的系统处理能力。

短信的处理能力（以 1000 万用户计算）：

日常业务能力：每天 1%的活跃用户短信业务，每次上行短信的数量为 1MO 短信。每天应能处理的短信。

海量更新能力：全部用户在 20 天内完成，每个用户完成更新的上下行短信的数量为 6MO、15MT 短信。

按照每天 8 小时有效工作时间进行日常业务，每天 16 小时闲事进行海量更新，并以两倍的峰值，短信能力应达到 10MO/秒、25MT/秒。

TCP 处理能力（以 1000 万用户计算）：
日常业务能力：每天 0.5%的活跃用户进行应用管理器承载、BIP 业务，每次交互的数据量为 1000K，

每天 Web 访问的次数 0.5%，每次访问的页面数据量为 10M。

按照每天 8 小时有效工作时间计算，并以两倍的峰值，TCP 的能力达到 3.75M/s

6.2. 存储能力

多应用开放平台应能够支持千万级用户。

6.3. 其它要求

参见《电信级设备指标标准设备要求分册》。

7. 安全性要求

多应用开放平台在安全方面遵循如下规范:《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》。

简要描述如下：

7.1. 访问控制

为确保对多应用开放平台访问的安全性、正确性和有效性，需要采用如下访问控制措施：

- **角色管理与权限划分：**对访问多应用开放平台的所有角色进行划分和管理，并按照角色分配相应的权限。其原则是每个角色只能访问其业务相关的信息，而无关信息则禁止访问。
- **身份认证：**根据应用和业务的安全级别分别采用相应级别的身份认证方式。

7.2. 通信安全

为了保证多应用开放平台与 SE 及其它业务平台之间通信信息的机密性和完整性，需要采取如下安全措施：

- **安全通信协议**：根据具体的通信要求选择相应的安全通信协议。
- **密码体制**：需要根据通信协议选择对称、非对称密码体制以及加解密/完整性算法，密钥长度等。
- **密钥管理**：为了保证密钥的安全性，需要充分保证密钥的生成、传输、更新和销毁

整个密钥生命周期过程的安全性。

7.3. 可用性

多应用开放平台采取必要的可用性措施提供保障，包括：

- **数据可用性**：对于多应用开放平台的数据库以及重要的文件系统数据均需进行定时备份，从而最大限度的保证数据的可用性。
- **操作系统可用性**：通过系统热备等措施实现多应用开放平台的高可用性。

7.4. 安全审计

多应用开放平台至少需要对如下操作进行审计：

- **对业务流程中的关键操作的审计**：包括业务流程中的各种关键环节的操作，需要做必要的记录，从而为后续的统计、异常分析等操作提供依据。
- **系统管理员、应用管理员的关键操作的审计**：包括管理员的登陆、退出操作，和管理员对用户的增加、修改、删除等操作。

7.5. 数据存储安全

多应用开放平台对重要业务数据（包括应用、用户信息）的存储需要满足如下要求：

- **机密性**：关键敏感数据需要采用安全存储，避免泄露。
- **完整性**：对各类应用数据采取进行完整性措施，防止非法的篡改
- **访问控制**：对各类应用数据需要采取访问控制措施，避免非法用户的访问

7.6. 防攻击/防病毒

多应用开放平台需要在应用自身、系统及网络层分别提供防攻击/防病毒的措施。

附录 A 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