中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

中国移动多应用开放平台
总体技术方案

版本号：1.0.0

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国移动通信有限公司　　发布

目　　录

前　　言

本标准是对多应用业务在开展业务过程中需要规范的内容提出全面要求，是多应用业务所需要遵从的纲领性技术文件。

本标准主要包括以下几方面内容业务特征、系统架构、组网结构、业务流程、接口要求。

本标准的附录　　为标准性附录，附录　　为资料性附录。

本标准由中移　　号文件印发。

本标准由中国移动通信有限公司技术部提出并归口。

本标准由标准归口部门负责解释。

本标准起草单位：中国移动通信研究院

本标准主要起草人：陆鸣、郭漫雪、朱本浩、李琳、黄更生

1. 范围

本方案规定了电子商务应用商店在业务开展中需要规范的内容，供中国移动内部和厂商共同适用；适用于电子商务应用商店业务开展、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网络环境。

本规范适用于具有CMS^{2}AC多应用功能的SE安全元件（以下简称SE）。

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)》	
[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
[5]	GSM 03.40	Digital cellular telecommunications system (Phase 2+)	（V7.4.0 :1999-12）
[6]	GSM 03.48	Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit	（V6.1.0 :1998-07）
[7]		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设备方案 中国移动多应用开放平台接口方案	

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：

3.1. 术语

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
CMS^{2}AC	中国移动SE多安全域多应用管理技术规范的英文简称
SE	Secure Element安全元件

3.2. 缩略语

表3-1

名词	解释
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。

CMS²AC应用	指遵循《中国移动SE多安全域多应用技术规范》，可被SE上CMS²AC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“CMS²AC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. 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. 业务功能

5.1. 安全域管理

多应用开放平台提供安全域管理，安全域的AID由多应用开放平台统一规划和分配。

5.1.1. 安全域类型

主安全域，作为运营商对SE上内容进行管理时的操作代理。运营商可以利用此授权程序加载、安装、删除运营商或其他应用提供方的应用。

辅助安全域，由中国移动进行创建，提供给中国移动或第三方进行应用下载及管理。辅助安全域按照业务模式分为代理第三方安全域、委托第三方安全域。

辅助安全域可由主安全域删除，可设置不可删除。

SE发行时，需预置主安全域。

5.1.2. 空间管理

安全域的空间管理包括签约空间管理和应用大小管理两种模式。安全域的空间管理由多应用开放平台完成。

签约空间管理是指为特定应用提供商提供独占SE中固定大小空间进行管理的方式。签约空间模式下需要指定安全域管理空间大小，且该空间为该安全域独占空间，在安全域空间未使用完的情况下，不属于该应用提供商安全域的应用不可使用该安全域可用空间；相反的，如果该安全域空间均已使用，即便SE上仍有其它物理空间也无法提供给该安全域使用。

应用大小管理是对应用提供商所需下载应用的自身大小进行管理的方式。SE上剩余的可用空间为所有签约应用大小管理方式的应用提供商共享的。应用大小管理模式不必指定安全管理空间大小，安全域大小本身没有限制，只受SE物理空间限制。

空间管理主要通过符合《中国移动SE多安全域多应用管理技术规范》要求的安全域管理实现。安全域是SE中划分的逻辑区域，拥有SE内容管理的权限，安全域中可以安装应用，安全域拥有应用安装、删除和管理的权限。安全域分配给某个应用提供商使用，可通过预置或由多应用开放平台动态创建，多应用开放平台拥有SE中安全域与安全域中安装应用的完整视图，可以实现上述两种模式的空间管理。

5.1.3. 安全域模式

安全域按照业务需求采用多种模式，以便于合作合作的开展。安全域模式是 SE 多应用管理的基础，一旦安全域创建后，安全域模式不能修改，多应用开放平台依据该模式进行相关的控制。安全域使用模式有以下几种：

模式一：主安全域，中国移动自有应用安装到 SE 上的主安全域（ISD）,ISD 密钥由中国移动控制。SE 上有且仅有一个主安全域；SE 发行前，主安全域需要预置在 SE 中。主安全域自身及其应用仅由主安全域进行管理和控制，其他辅助安全域不能对主安全域及其应用进行管理和控制。主安全域仅安装自有应用。

模式二：代理第三方安全域，该安全域满足第三方（应用提供商）的应用要求独立的安全域的要求。该安全域密钥可由中国移动或第三方应用提供商管理和控制。该安全域中应用的下载、管理等操作由中国移动主安全域控制。SE 上可有多个第三方安全域，该安全域通过多应用开放平台动态创建，中国移动或应用提供商提供安全域密钥，多应用开放平台进行密钥更新。

模式三：委托第三方安全域，应用提供商的应用要求独立的安全域，应用提供商自身控制管理安全域的密钥，且该安全域中应用的下载、管理等操作在中国移动授权的前提下由应用提供商安全域控制（Token 模式）。第三方应用由第三方自行管理。该安全域可通过多应用开放平台动态创建，由第三方进行密钥更新。

5.2. 应用管理

多应用开放平台将中国移动提供的应用发行相关能力进行封装，开放给自有或第三方业务平台，实现业务平台和SE间进行应用发行相关业务交互的能力。多应用开放平台提供的接口需满足以下要求：

（1） 采用开放的接口协议，将复杂的协议，例如CMS²AC指令、Mifare指令，以较为通用、易于理解的形式展现给自有或第三方业务平台。

（2） 采用灵活的架构，应用发行的业务能力的模式应是可以根据需求灵活扩充的。

5.2.1. 应用类型

应用包括SE上CMS²AC应用及Mifare应用以及NFC终端上的程序。

本规范重点定义SE上CMS²AC应用及Mifare应用下载，未特殊说明，应用特指CMS²AC应用。NFC终端上的应用程序可以通过其他下载渠道；手机钱包客户端应保证应用的完整性。

5.2.2. 生命周期管理

多应用开放平台对全网及本地应用的整个生命周期进行管理，对工作流进行控制。应用生命周期包括配置、上载、审核、测试、发布、更新和归档等。

应用配置，设置应用的属性，包括应用AID、Mifare应用为OID、所属应用提供商、所属安全域、全网或本省应用。

应用上载，上载应用的程序文件。CMS²AC应用的程序文件的后缀为.cap,Mifare应用的程序文件后缀为.mi。一个应用可包括一个或多个程序文件。

应用审核，具有审核权限的业务管理员根据应用提交的属性及应用文件进行审核。

应用测试，具有测试权限的业务管理员对应用进行在线测试。对应用进行测试时，应向所与（不同SE提供商的）SE进行兼容性测试，并记录应用在SE上的最大的使用空间，配置为该应用的大小。

应用发布，发布后应用可进行面向用户进行应用下载。应用发布时应指定应用适用的SE型号以及其他方式的用户限定。

应用更新，升级应用的版本，更新应用程序文件以及其他属性。

应用归档，结束应用生命周期，进行应用归档。

5.3. 用户管理

用户指使用 SE 设备的中国移动用户，由 SE 的 SE_ID 唯一标识。

5.3.1. 用户信息管理

多应用开放平台统一管理用户关联 SE 的标识（简称 SE_ID）；同时多应用开放平台也

管理平台的用户基本信息，包括用户身份、联系方式等个人信息。

多应用开放平台通过手机钱包客户端与 SE 交互时，在 NFC 终端的手机钱包客户端发现 IMSI 变更时，发送短信通知多应用开放平台，，多应用开放平台从短信中获取 NFC 终端的手机号码，并 SE_ID、MSISDN 绑定关系。

用户使用 SE 设备包括 NFC 终端、SIM 卡、贴片卡。其中使用 SIM 卡时，也需要终端协作，完成非接触功能。使用 NFC 终端、SIM 卡可使用空中、非接触两种管理渠道。使用贴片卡可使用非接触方式管理渠道。

5.3.2. 用户注册

用户注册指将用户的手机号码绑定到用户的 NFC 终端上。用户完成注册后才能够进行 SE 上应用下载及其他业务操作。一个手机号码可以绑定多个 NFC 终端，一个 NFC 终端仅能绑定到一个手机号码上。

5.3.3. 用户注销

用户不再使用 NFC 终端，需要进行用户注销，解除手机号码与 NFC 终端的绑定关系。

5.3.4. 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。

5.3.5. 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。

5.3.6. 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。

5.3.7. 用户自服务

用户可通过手机终端（手机钱包客户端）以及多应用开放平台的门户进行自服务操作。用户自服务功能包括

- 应用发现，查询适配用户SE的可下载应用。
- 查询功能，查询已下载应用、使用空间、可用空间、SE设备信息；
- 业务操作，应用下载、删除、更新、锁定功能等。

5.4. 应用提供商管理

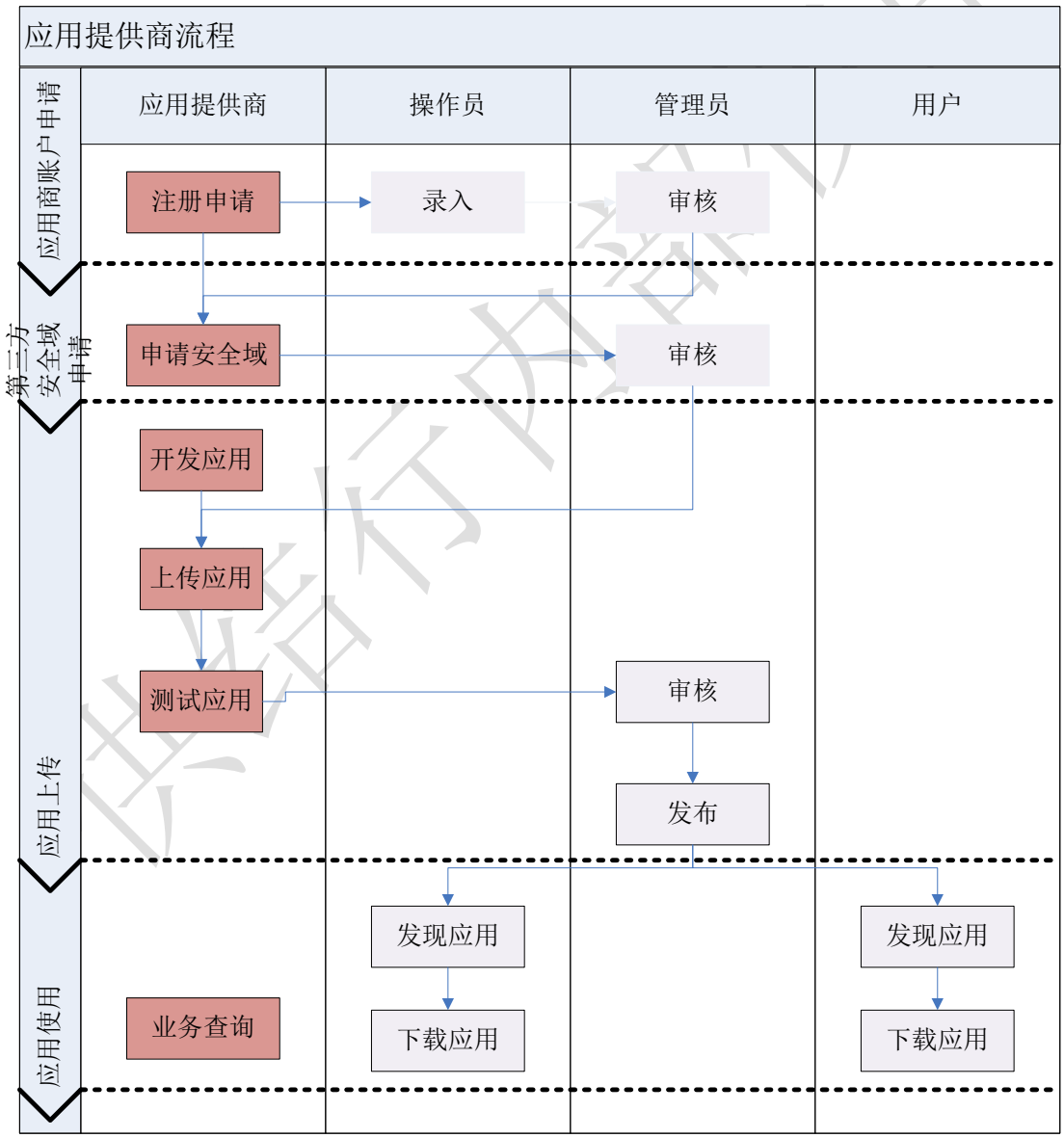

图 5-1　应用提供商相关流程

5.4.1. 基本信息管理

多应用开放平台提供应用提供商注册、审核功能，对应用提供商的信息资料进行管理。

5.4.2. 安全域申请

多应用开放平台为应用提供商提供安全域申请及审核的管理功能。

5.4.3. 应用申请

多应用开放平台为应用提供商提供应用生命周期管理功能。应用提供商可同时提供全网应用及本地应用。对全网应用，需要全网业务管理员进行审核；对本地应用仅需要本地业务管理员进行审核。

5.4.4. 签约关系管理

签约关系是应用提供商使用中国移动 SE 安全域进行应用发行业务的契约，中国移动据此对应用提供商收取相应费用。

5.4.5. 应用提供商自服务

应用提供商可通过多应用开放平台的门户进行自服务操作。

应用提供商自服务功能包括：

- 所属安全域信息查询、配置、申请。
- 所属应用信息查询、配置、申请、升级。
- 所属安全域、应用已下载的查询、统计。

5.5. 业务管理

5.5.1. 业务数据管理

多应用开放平台需要对各类业务数据进行配置管理，即对应用发行业务涉及到的对象的数据进行管理，如应用提供商、应用、安全域和签约关系等。

5.5.2. 业务类型

全网业务和本省业务。全网业务由全网业务管理进行管理审核。

5.5.3. 鉴权与授权

多应用开放平台对业务使用流程进行控制，在业务平台调用应用发行能力时，需要对应用提供商、业务平台、签约关系进行鉴权（Authentication）以及对调用的能力进行授权（Authorizaiton）。

5.5.4. 系统管理

系统管理员和业务管理员，同时为省公司分配相应的业务管理员角色，负责本省业务的开展。

5.6. SE 管理

5.6.1. SE 数据信息

SE 数据信息包括 SE 的 SE_ID、批次、密钥等静态信息以及已下载应用、可用空间等动态信息。

5.6.2. SE 管理渠道

目前提供非接触和空中两种渠道完成多应用开放平台与 SE 的业务操作。

非接触方式指使用 PC、手机钱包客户端（PC 客户端或浏览器控件）以及非接触读卡器，通过互联网或中国移动专网链接到多应用开放平台，完成业务操作。非接触方式可用于营业厅、自服务终端、用户自服务。

空中方式指使用 NFC 终端、手机钱包客户端（手机客户端），通过中国移动无线网络连接到多应用开放平台，完成业务操作。空中方式用于用户使用 NFC 终端自服务。

5.6.3. SE 安全域管理

5.6.3.1. 安全域创建

多应用开放平台可动态创建辅助安全域，包括第三方安全域和委托第三方安全域。

第三方安全域创建。首先多应用开放平台创建第三方安全域，然后第三方平台提供安全域密钥，最后多应用开放平台进行密钥更新并激活安全域。

委托第三方安全域创建。首先多应用开放平台创建委托第三方安全域，然后第三方平台进行初始密钥更新并激活安全域。

5.6.3.2. 安全域删除

多应用开放平台可删除创建辅助安全域，包括第三方安全域、委托第三方安全域。

5.6.3.3. 安全域密钥更新

多应用开放平台实现主安全域、第三方安全域以及委托第三方安全域的密钥更新，其中主安全域密钥由多应用开放平台提供，第三方安全域密钥由第三方平台提供。

委托第三方安全域密钥由第三方在中国移动控制下自行更新，由多应用开放平台为第三方平台提供 TOKEN 验证。

5.6.4. SE 应用管理

5.6.4.1. 应用发行

多应用开放平台提供基于SE上主安全域、第三方安全域下的应用的动态、安全下载功能。应用发行包括应用下载和应用个人化两个步骤，其中应用下载又可分为加载文件和创建实例两个过程。应用发行支持非接触、空中两种模式。平台具备的应用发行模式有：

（1）空卡模式（应用下载+应用个人化，应用下载由加载CAP文件和创建实例构成）

（2）实例创建模式（应用下载+应用个人化，应用下载仅需要创建实例）

（3）个人化模式（应用下载完成，仅需要进行个人化数据写入）

委托第三方安全域下的应用下载及个人化由第三方在中国移动的控制下进行，多应用开放平台为第三方平台的应用下载提供TOKEN验证。

多应用开放平台可查询委托第三方安全域信息及其已下载应用信息。

5.6.4.2. 应用删除

多应用开放平台提供应用删除功能，可通过非接触、空中方式，将已经安装在SE中主安全域、第三方安全域下应用删除的过程。与应用发行相对应，应用删除时也可以有删除整个应用程序和个人化数据两种模式，平台可针对不同应用、应用提供商需求灵活配置。

委托安全域下的应用删除由第三方在中国移动的控制下进行，多应用开放平台为第三方平台的应用删除提供TOKEN验证。

5.6.4.3. 应用锁定/解锁

多应用开放平台提供应用锁定/解锁功能，可以通过非接触、空中方式对运行于SE中主安全域、第三方安全域下的应用进行管理。一旦应用被锁定，则应用一切正常的业务操作被禁止（例如，手机支付应用的刷卡消费、充值等操作），可根据用户或业务系统风险控制的需要，对应用进行管理，减少由于各种风险带来的损失。应用解锁需要到营业厅办理或由客服人员办理。

委托第三方安全域下的应用锁定/解锁由第三方在中国移动的控制下进行，多应用开放平台为第三方平台的应用锁定/解锁提供TOKEN验证。

5.6.4.4. 应用升级

多应用开放平台提供应用升级功能，先删除旧版本应用，后下载新版本应用并进行应用个人化。

多应用开放平台删除旧版本应用前，应通知应用的业务平台，由业务平台获取应用在SE中个人化数据，并保存个人化在业务平台，完成新应用下载后由业务平台提供个人化数据，由多应用开放平台进行个人化数据更新。

应用升级是否由用户自服务完成，由业务决定。

应用删除及应用下载的参见本规范应用发行及应用删除的规定。

5.6.5. Mifare 应用管理

多应用开放平台提供Mifare应用下载功能，可通过通过非接触、空中方式将Mifare应用下载到SE上的Mifare Manager中。

多应用开放平台提供Mifare应用删除功能，可通过通过非接触、空中方式将Mifare Manager中的应用删除。

多应用开放平台提供Mifare应用激活功能，可通过通过非接触、空中方式激活Mifare Manager中的指定应用。

5.7. 业务门户

5.7.1. 专用客户端

用户通过手机钱包客户端访问多应用开放平台。客户端的功能包括用户管理（用户注册/注销、更换终端、挂失/解挂）及业务应用管理（应用下载/更新/恢复/删除、业务搜索、空间查询等）等。

客户端分为手机版和PC版(包括使用浏览器插件)，手机版是面向普通用户的应用管理软件，而PC版主要是为客服操作员提供使用访问多应用开放平台的能力。

5.7.2. 业务网站

用户可以通过网站查询应用的相关信息、自己的操作记录等，并通过浏览器插件进行应用管理。相对于手机版客户端，网站除了提供更为全面和细致的应用信息，还提供应用的使用说明、下载记录等。同时，网站还会提供论坛供用户交流。另外，网站还会开辟投诉专区，集中处理用户的投诉。

应用提供商可以通过网站提供的自服务功能，进行信息管理、应用管理、业务订购关系管理。

6. 系统架构

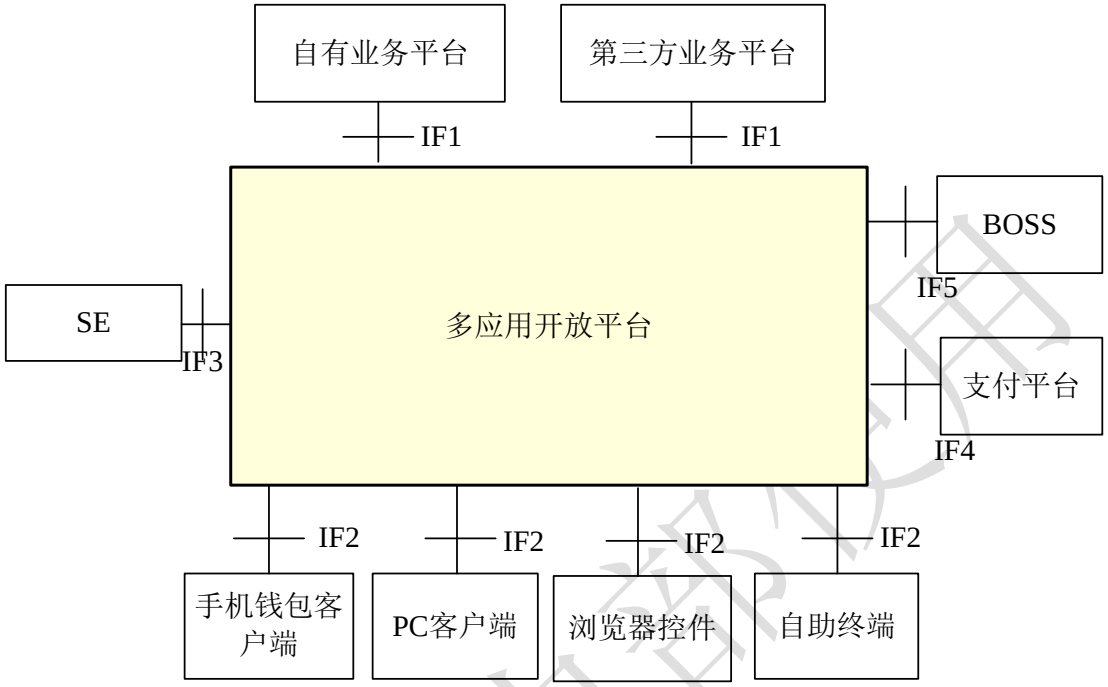

图 6-1　多应用开放平台系统架构

多应用开放平台统一接入业务平台，并向业务平台提供基于CMS^{2}AC SE的应用发行业务。

多应用平台对贴片卡本期暂不实现。

7. 组网要求

7.1. 组网原则

多应用开放平台建设统一平台，负责对全网应用及省本地应用，应用提供商进行管理，为全网及本省自有和第三方业务平台提供服务，并实现对全网及省业务平台的鉴权和授权；负责与SE建立安全通道，完成应用下载、管理的功能。

多应用开放平台可为省公司提供省级虚拟平台，由省级业务管理员对本省业务进行管理。

7.2. 组网结构

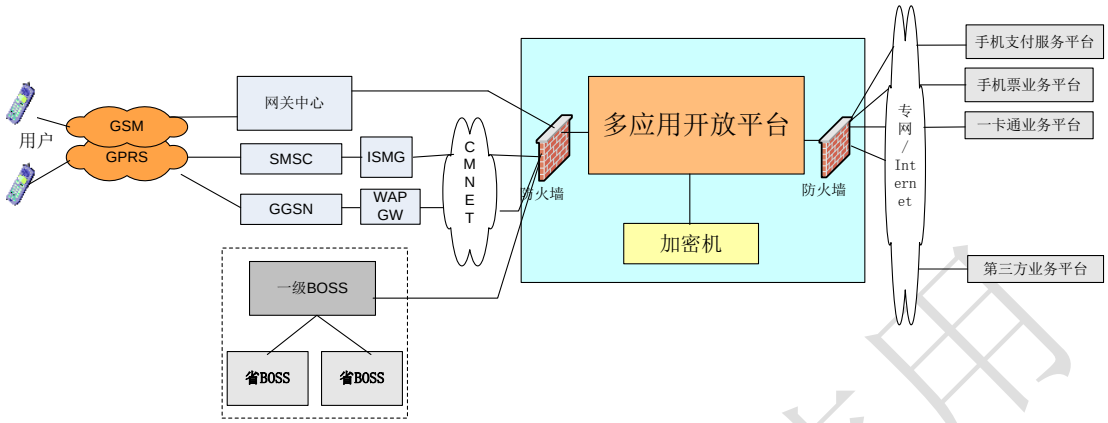

图7-1 多应用开放平台组网结构

8. 计费机制

8.1. 计费对象

多应用开发平台的计费对象为用户。

8.2. 用户计费原则

用户使用移动网络产生的通信费，按照中国移动既有资费标准收取和结算。
功能费现阶段暂不收取。

9. 应用提供商计费

多应用开发平台提供向应用提供商后向计费的能力，负责生成计费单。多应用开发平台的多应用开放平台提供的计费话单应与应用提供商的业务系统进行比对，以多应用开放平台为准。

向应用提供商收取的费用按照以下因素（分成比例待定）与省公司进行分成：

- NFC终端（省公司）
- 应用提供商拓展单位（省公司、基地）
- 技术支撑（基地）

可向应用提供商可收取功能费及空间使用费（现阶段暂不向应用提供商收取费用）。以下是详细的计费策略和原则。

9.1. 空间计费

应用提供商提供的应用将占用SE资源，需要对其进行空间收费。计费模式主要依据空间管理中签约空间和应用空间两种不同形式，结合用户数、计费周期综合形成。

计费模式一：按月收取，采用用户数和应用程序综合计费。应用程序单价可按照空间大小计算或指定应用程序单价进行计费。如采用按空间大小计费应考虑到应用在不同SE安装后所占空间的不精确性，中国移动需要事先对应用在所有类型SE的实际占用空间进行测试，得到平均值，然后找到平均值对应的收费档。收费档一般按空间范围划分，建议1K byte一档，粒度可调。单位粒度收费可以修改。

计费时机包括

1. 预置应用。计费公式：预置应用数*应用单价
2. 应用下载及个人化。计费公式：下载用户数*应用单价
3. 应用下载开通。计费公式：开通用户数*应用单价

计费模式二：按月收取，采用用户数和签约空间大小综合计费。收费档一般按空间范围划分，建议1K byte一档，粒度可调。单位粒度收费可以修改。计费公式：用户数×对应收费档资费。

计费时机包括

1. 预置固定空间安全域。计费公式：预置安全域数*空间大小*空间单价
2. 固定空间安全域创建。计费公式：创建安全域数*空间大小*空间单价

9.2. 功能计费

为应用提供商提供的动态的应用下载、删除、锁定以及解锁功能，按照用户使用次数对应用提供商进行后向计费。

计费模式一：按次收取，采用功能使用次数进行计费。

计费模式二：按月收取，采用按照使用业务的用户规模，使用阶梯价格进行包月计费。

需要进行计费的功能包括应用下载、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。

10. NFC 终端要求

多应用环境支持两类NFC终端，一类是嵌入SE安全元件的NFC终端、一类支持SWP协议支持嵌入SE的SIM卡的NFC终端。

NFC终端都需预置手机钱包客户端。

11. 码号要求

11.1. IP 地址

多应用开放平台需分配公网IP。

11.2. 短信接入码

多应用开放平台申请全网短信接入码。该短信接入码能够承载二进制数据短信。

11.2.1. 安全域 AID

主安全域AID为
辅助安全域AID由多应用开放平台统一分配。
安全域AID的格式参见《中国移动应用标识 (AID)编码规范》

11.2.2. 应用 AID

应用AID包括应用(实例)AID、可执行文件AID、可执行加载模块AID。
应用实例AID可由业务管理部门规定，多应用开放平台进行配置。
可执行文件AID、可执行加载模块AID可由多应用开放平台进行配置或自动产生。
多应用开放平台保证应用AID的唯一性。
应用AID的格式参见《中国移动应用标识 (AID)编码规范》

12. 技术流程

12.1. 应用发行

应用发行对未预置应用的SE执行应用下载及应用个人化操作，对预置应用的SE仅需执行应用个人化操作。

12.1.1. 应用下载

适用于主安全域、代理第三方安全域下应用下载。

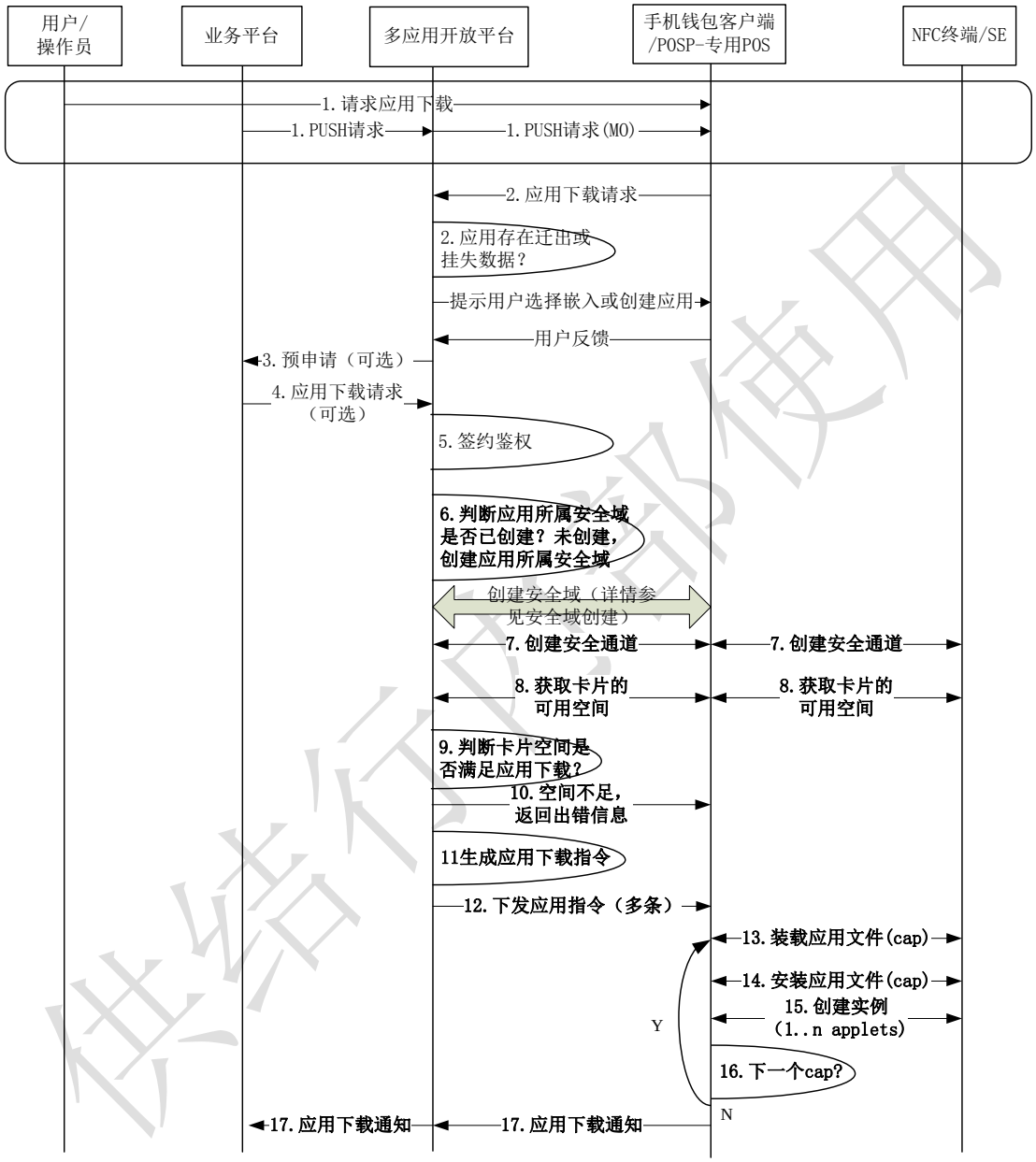

图 11- 1 应用下载

注：业务平台或多应用开放平台发起空中方式业务流程，通过MT短信激活NFC终端上手机钱包客户端应用，详见《中国移动多应用开放平台设备方案》远程PUSH一节。以下业务功能的空中方式同。

注：图11-1包括两种受理渠道，用户使用手机钱包客户端空中方式。操作员使用专业POS是营业厅非接触方式。以下技术流程同理。

12.1.2. 应用个人化

应用个人化发起可以由业务平台，也可以由多应用开放平台发起，相关更新数据由多应用开放平台生成。

适用于主安全域、代理第三方安全域下应用个人化。需要个人化的应用在完成应用下载，接收到多应用开放平台的应用下载通知后，发起应用个人化请求。

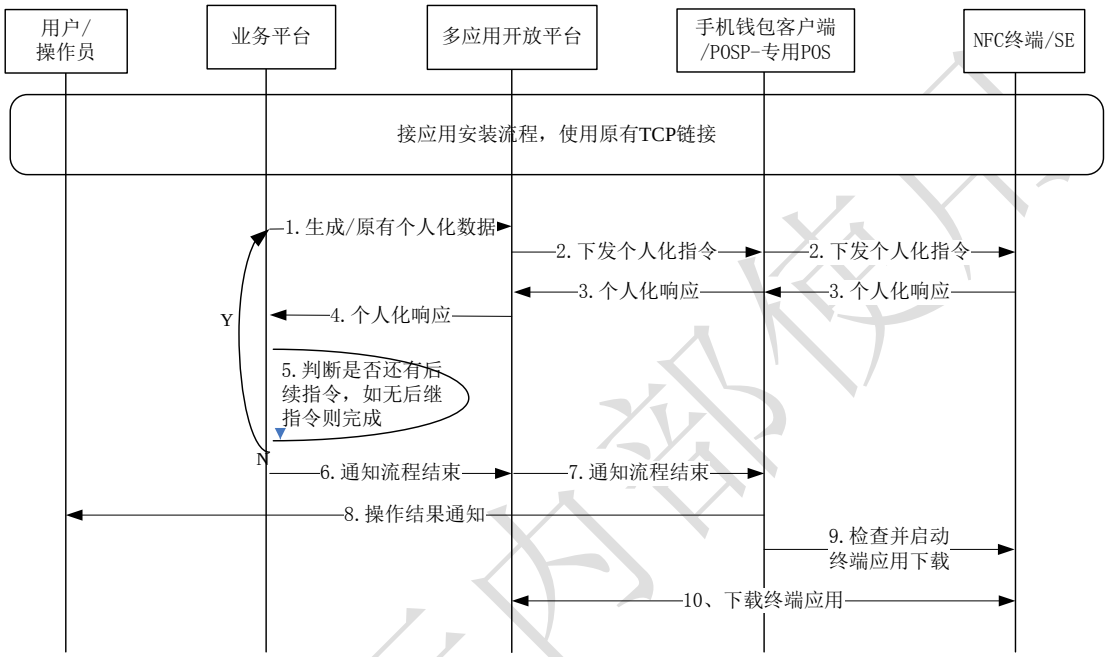

图11-2　应用个人化

12.2. 应用删除

适用于主安全域、代理第三方安全域下应用删除。

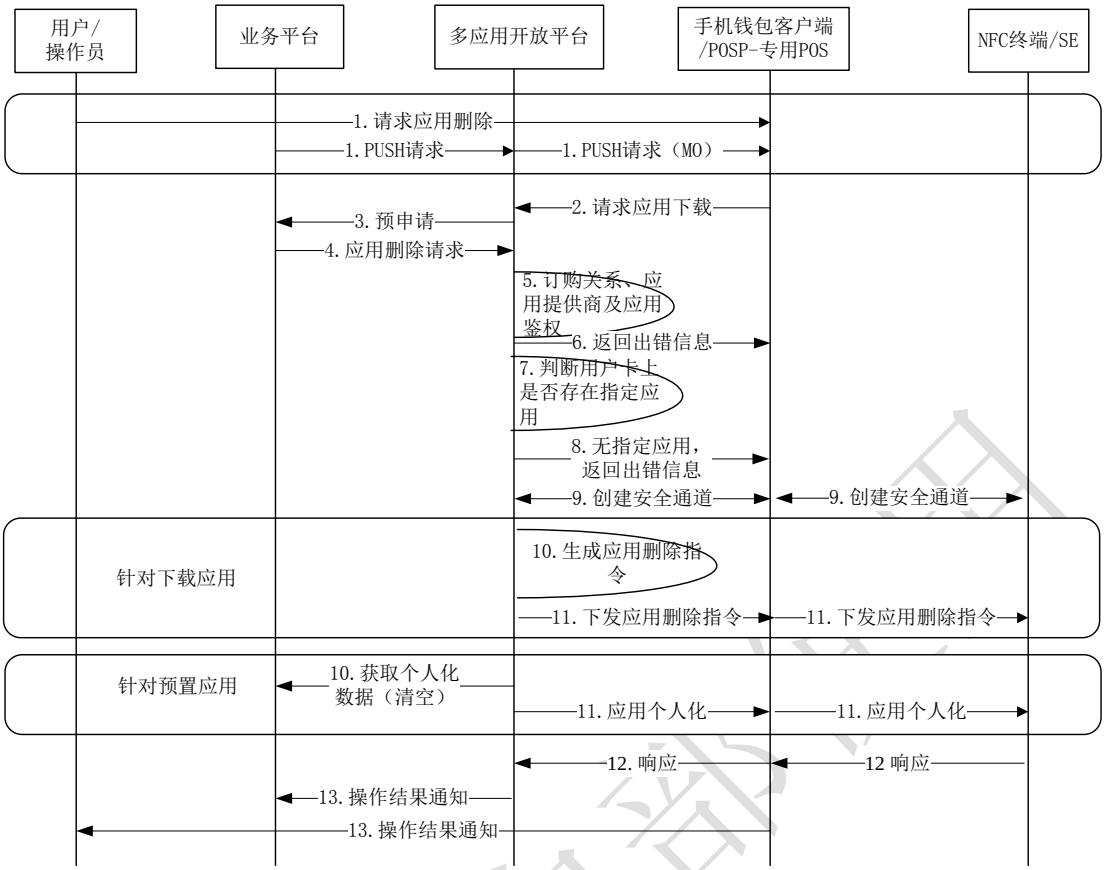

图 11- 3　应用删除

12.3. 应用更新

适用于主安全域、第三方安全域下应用更新。

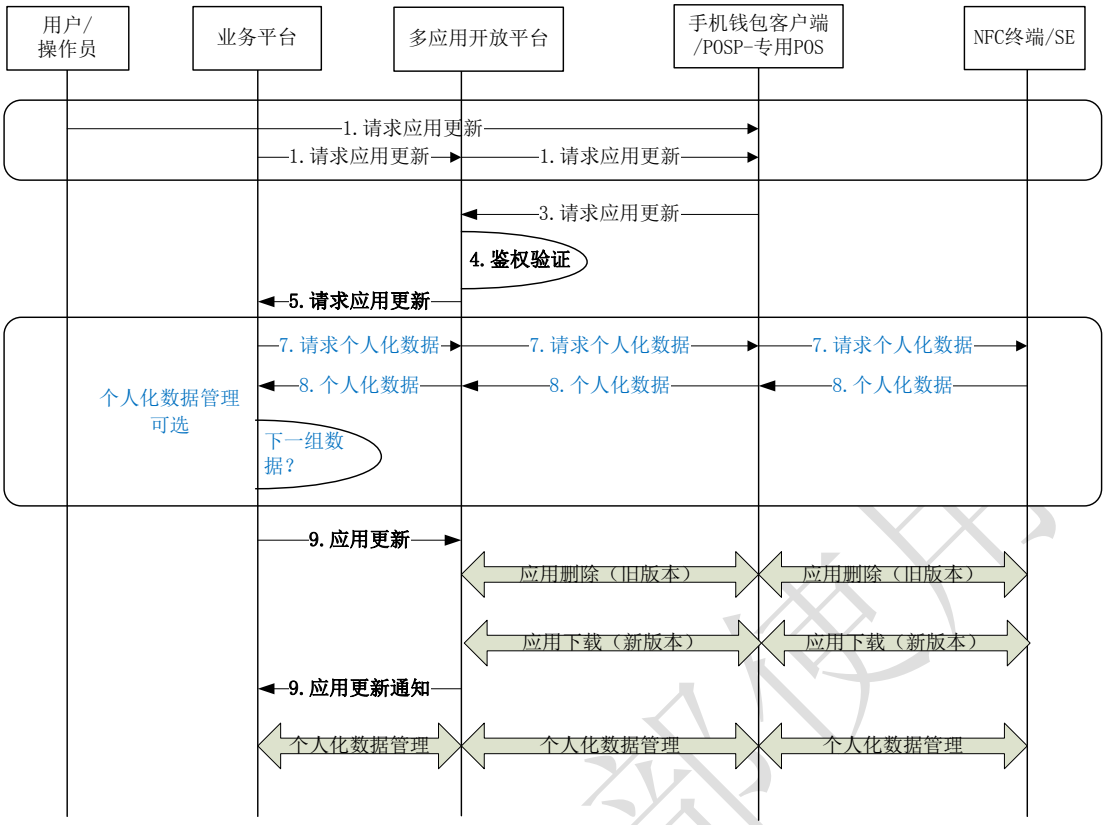

图 11- 4 应用更新

12.4. 安全域创建

适用于第三方安全域、委托第三方安全域。创建委托第三方安全域时，执行到安全域创建后流程结束，由第三方自行更新安全域密钥。

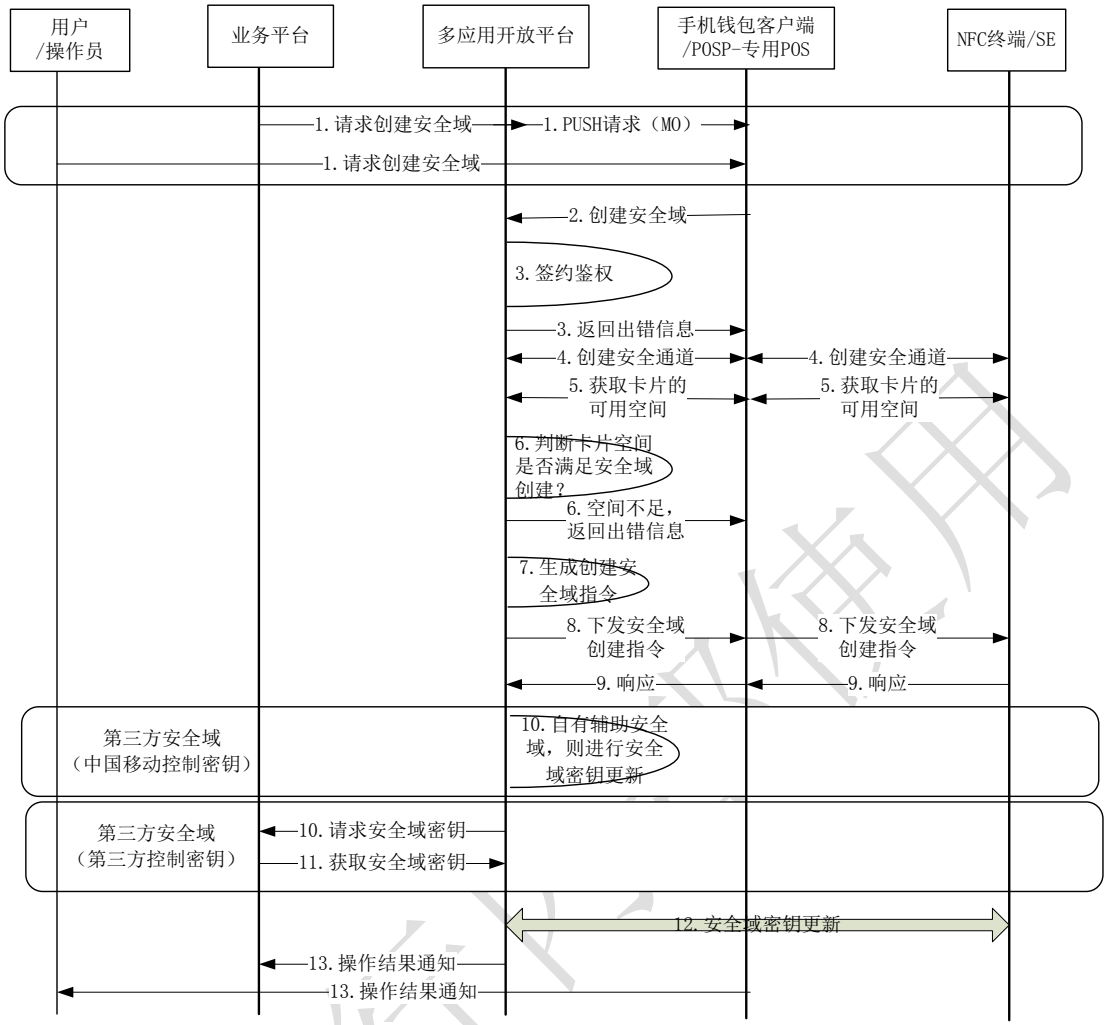

图11- 5　安全域创建

12.5. 安全域删除

如果安全域包含应用，则该安全域不可删除。适用于第三方安全域、委托第三方安全域。

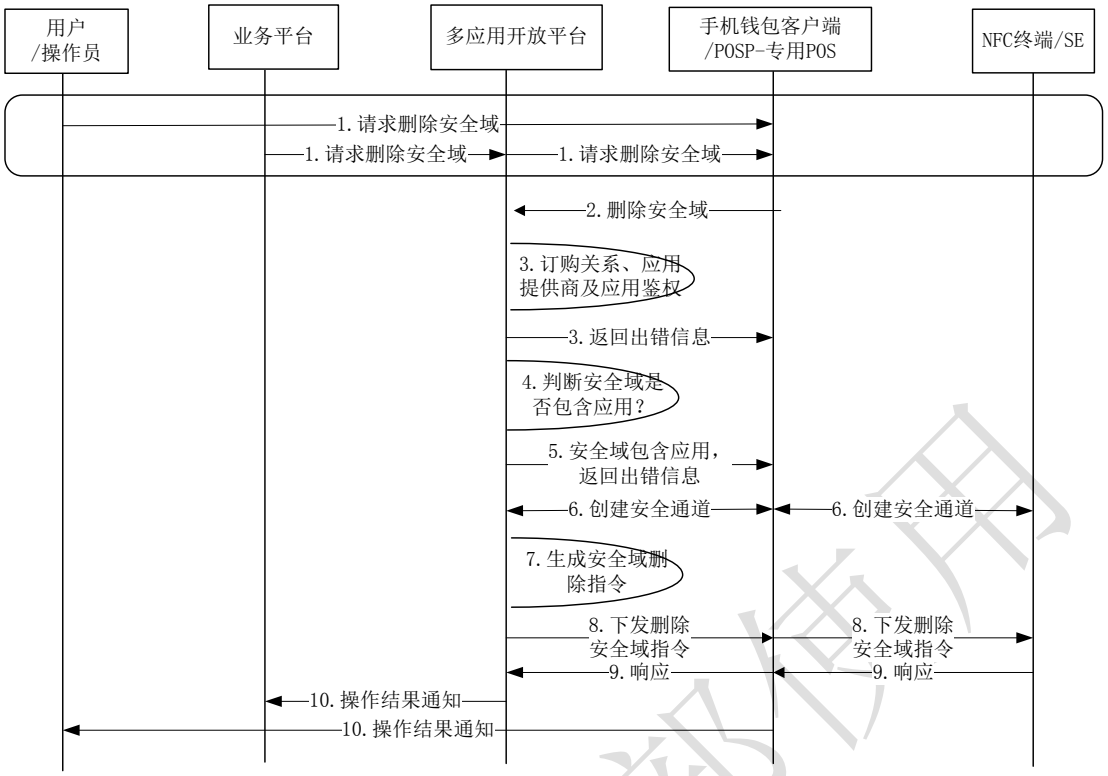

图11- 6　安全域删除

12.6. 安全域密钥更新

适用于主安全域、第三方安全域。

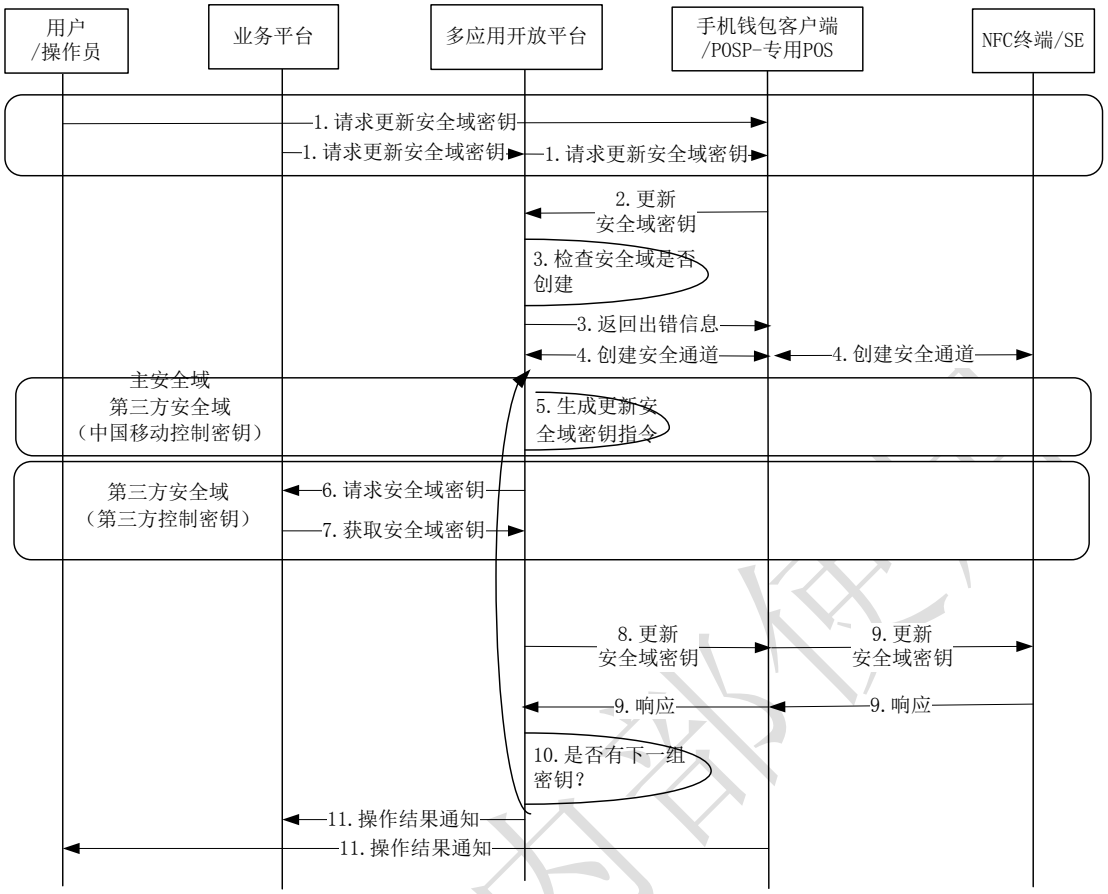

图11- 7 安全域密钥更新

12.7. 应用锁定

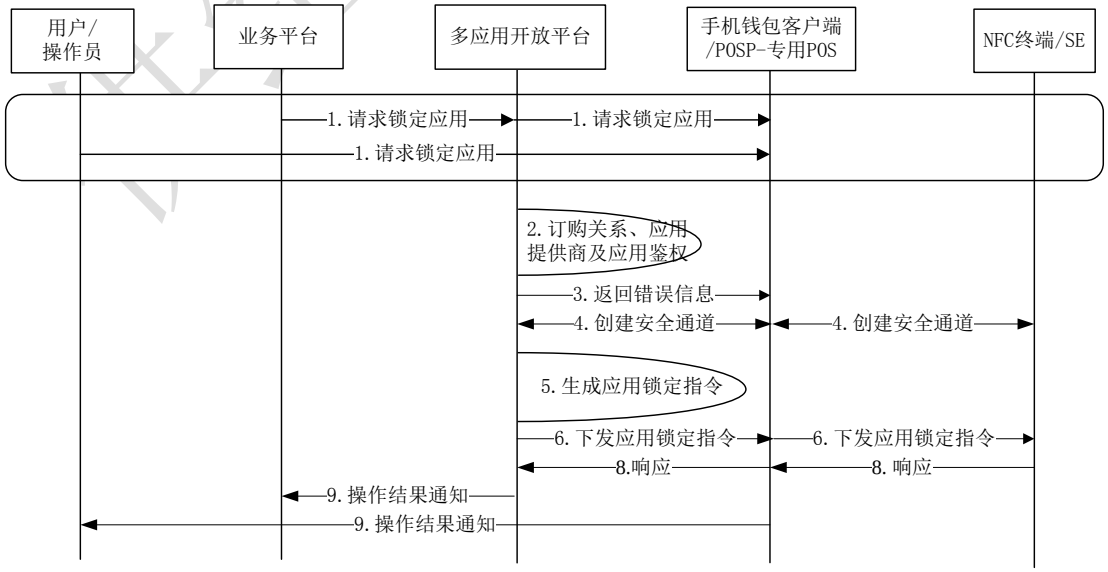

图11- 8 应用锁定

注：仅锁定SE上应用。终端应用不锁定。

12.8. 应用解锁

应用解锁只能通过营业厅完成。

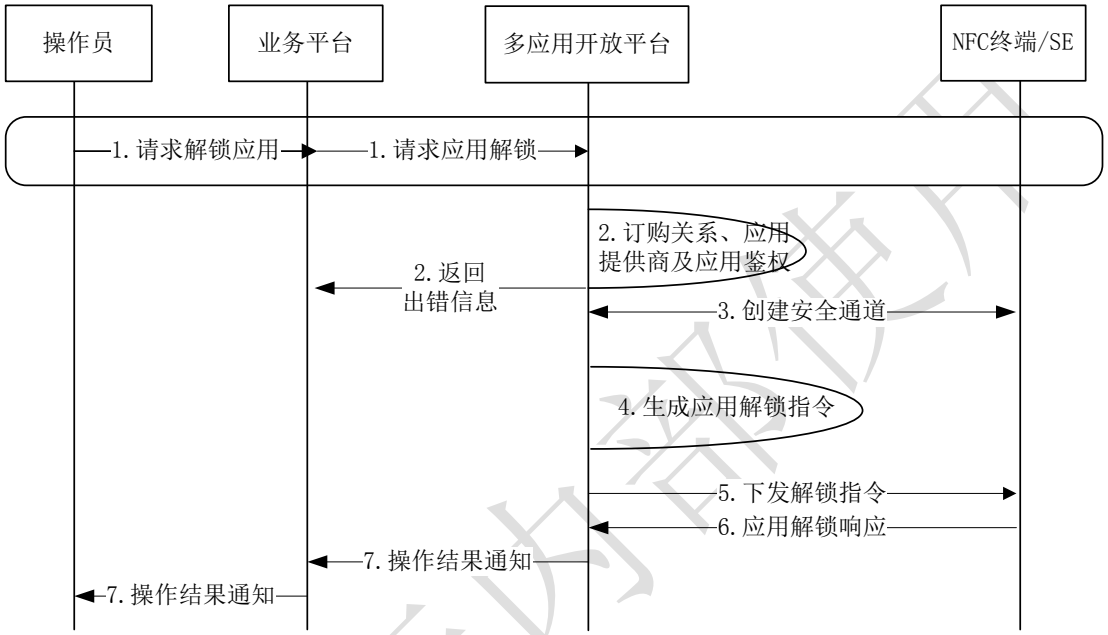

图11- 9　应用解锁

12.9. 个人化数据管理

应用的个人化数据，根据业务的变化需要进行更新/获取，由业务平台发起，相关更新数据由多应用开放平台生成。

应用个人化管理流程如下：

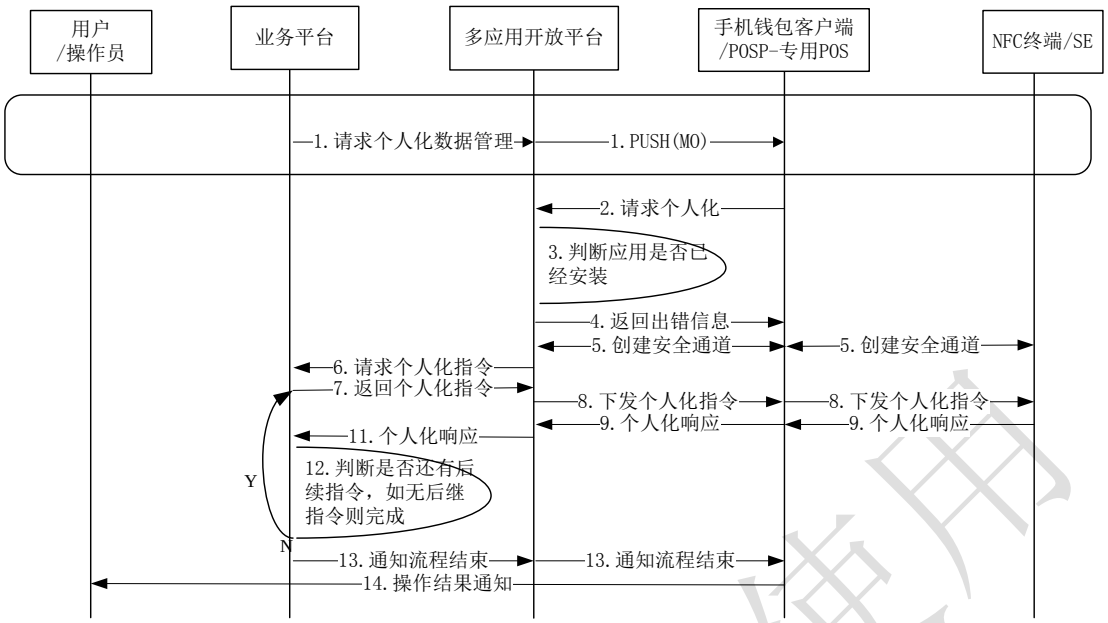

图11- 10 个人化数据管理

12.10. 业务迁移

图11-20是在原NFC终端上业务的迁出流程，迁入流程参见应用下载。

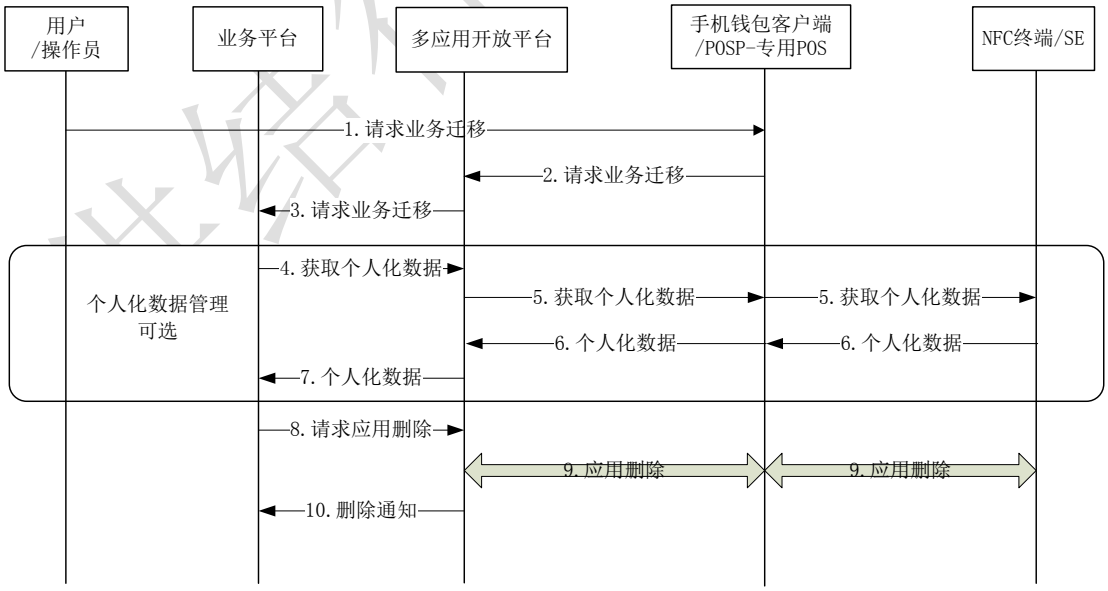

图11- 11业务迁移

12.11. 登录流程

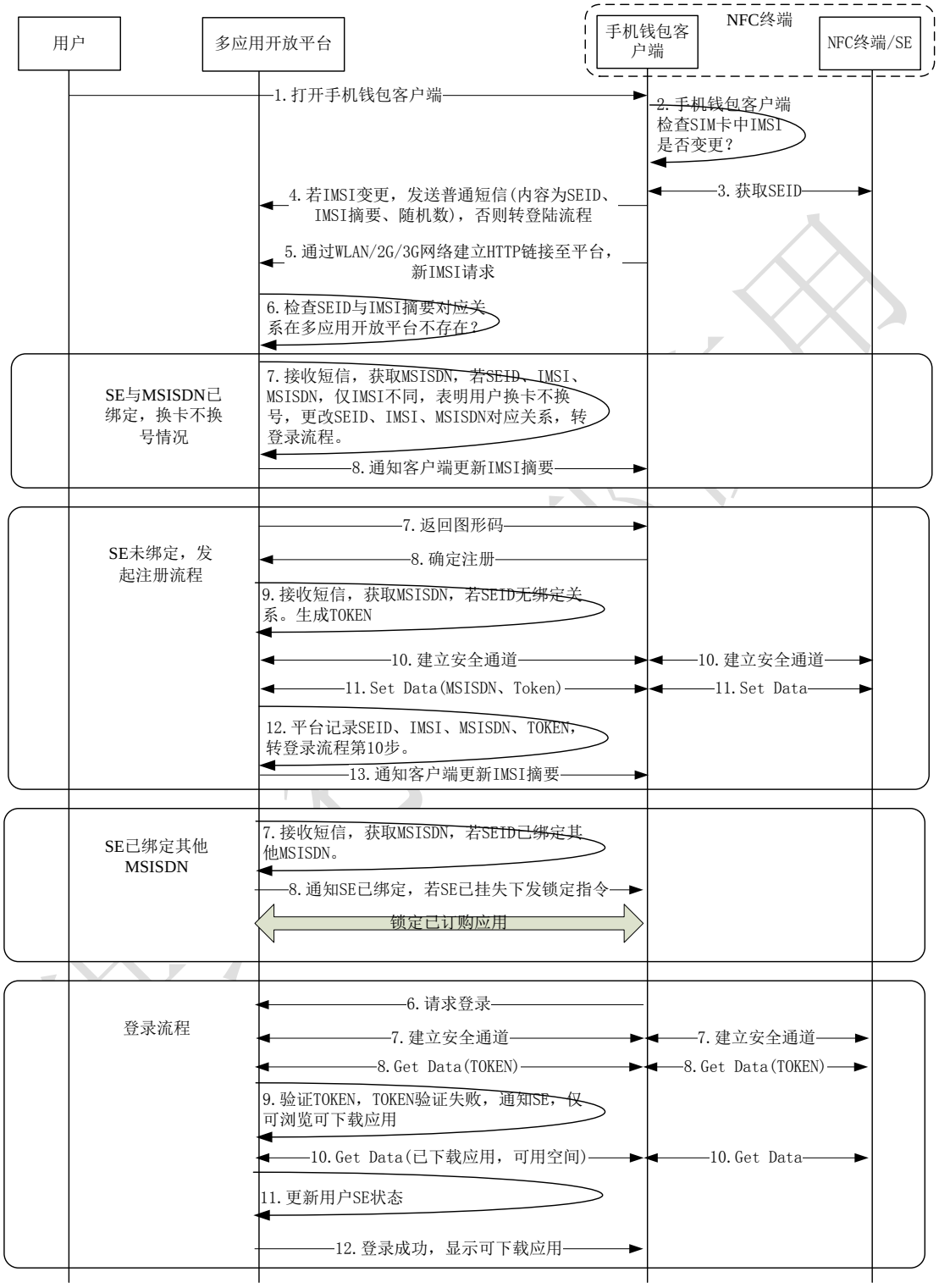

图11- 12 手机钱包客户端登录流程

12.12. 委托模式

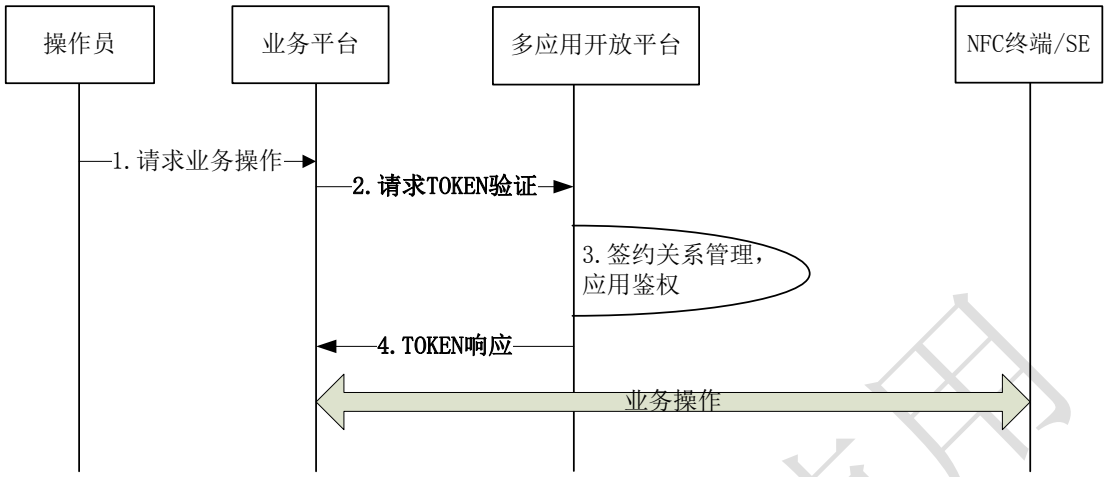

图11- 13 委托模式

适用委托第三方安全域下的SE操作，包括应用下载、删除、锁定、解锁、安全域密钥更新。

13. 接口要求

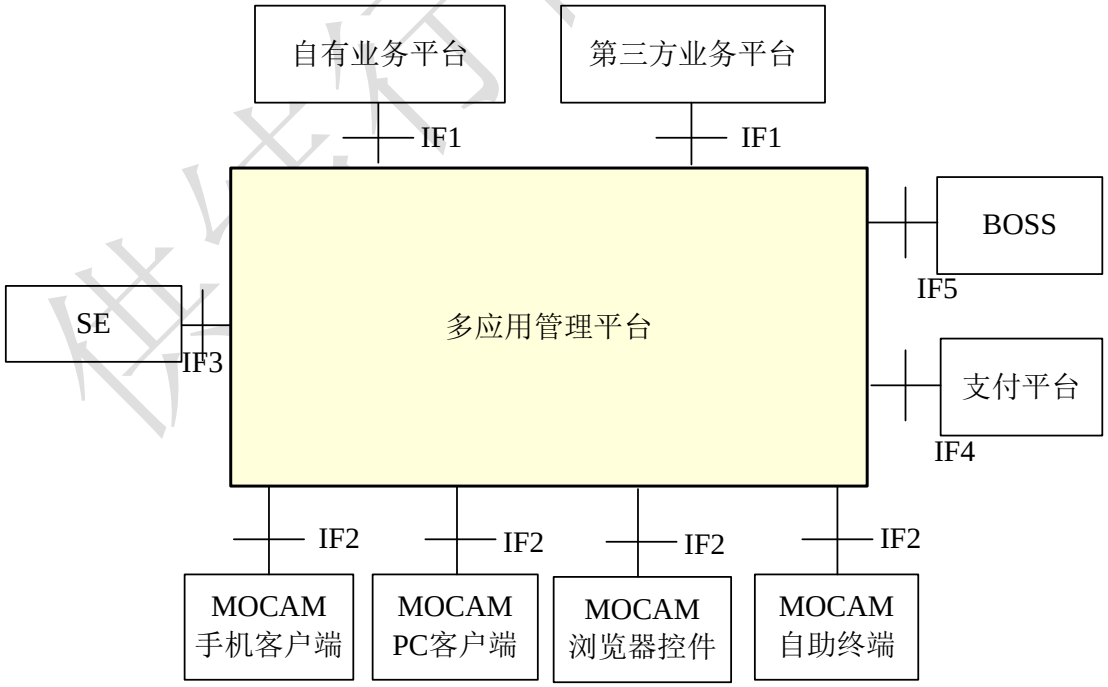

图 12- 1 多应用开放平台系统接口图

13.1. IF1（业务平台与多应用开放平台）

13.1.1. 安全域创建接口

- 请求方：业务平台
- 功能：业务平台向多应用开放平台转发安全域创建请求，由多应用开放平台完成安全域创建；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.2. 安全域删除接口

- 请求方：业务平台
- 功能：业务平台向多应用开放平台请求安全域删除，由多应用开放平台完成安全域删除；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.3. 安全域密钥更新接口

- 请求方：业务平台
- 功能：业务平台向多应用开放平台发起安全域密钥更新；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.4. 应用下载请求接口

- 请求方：业务平台
- 功能：业务平台向多应用开放平台转发应用下载请求，由多应用开放平台完成应用下载；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.5. 应用删除请求接口

- 请求方：业务平台
- 功能：业务平台向多应用开放平台发起应用删除请求，由多应用开放平台完成应用删除操作
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.6. 应用锁定/解锁请求接口

- 请求方：业务平台
- 功能：业务平台向多应用开放平台发起应用解锁/锁定请求，由多应用开放平台完成对用户卡片的锁定/解锁操作；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.7. 卡端操作结果通知接口

- 请求方：多应用开放平台
- 功能：多应用开放平台向业务平台发起卡端操作结果通知；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.8. 应用指令请求接口（用于个人化、获取随机数、密钥更新等指令）

- 请求方：业务平台
- 功能：业务平台向多应用开放平台发起应用指令传递请求；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.9. 预操作请求接口

- 请求方：多应用开放平台
- 功能： 多应用开放平台向业务平台发起操作请求；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.1.10. 用户销号/退订接口

- 请求方：业务平台
- 功能： 业务平台向多应用开放平台发起操作请求；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.2. IF2（多应用开放平台与手机钱包客户端）

详情参见《中国移动客户端应用管理器技术规范》。

13.2.1. 获取应用列表接口

- 请求方：手机钱包客户端
- 功能： 手机钱包客户端向多应用开放平台按指定条件获取应用列表；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.2.2. 上传数据接口

- 请求方：手机钱包客户端
- 功能： 手机钱包客户端向多应用开放平台上传数据，例如应用评论、业务推荐；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.2.3. 获取 APDU 命令序列接口

- 请求方：手机钱包客户端
- 功能： 手机钱包客户端向多应用开放平台 APDU 命令序列，APDU 命令对手机钱包客户端透明，由多应用开放平台根据业务场景和要求构建 APDU 命令序列；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.2.4. 下载终端软件接口

- 请求方：手机钱包客户端
- 功能： 手机钱包客户端向多应用开放平台请求获取终端软件 URL 地址；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.2.5. 用户签到接口

- 请求方：手机钱包客户端

- 功能： 手机钱包客户端向多应用开放平台请求用户注册/注消/登录/重置密码操作；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.2.6. 联机请求接口

- 请求方：手机钱包客户端
- 功能： 手机钱包客户端启动后通知手机钱包客户端联机，可获取默认应用列表；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

13.3. IF3（多应用开放平台与 SE）

详情参见《中国移动SE多安全域多应用管理技术规范》。

13.3.1. 应用删除接口

- 请求方：多应用开放平台
- 功能： 多应用开放平台向 SE 发起应用删除请求；
- 报文协议：APDU ， Delete 指令

13.3.2. 应用加载接口

- 请求方：多应用开放平台
- 功能： 多应用开放平台向 SE 发起应用加载请求；
- 报文协议：APDU，Load 指令

13.3.3. 应用安装接口

- 请求方：多应用开放平台
- 功能： 多应用开放平台向 SE 发起应用安装请求；
- 报文协议：APDU，Install 指令

13.3.4. 获取数据接口

- 请求方：多应用开放平台
- 功能： 多应用开放平台向 SE 发起获取数据请求；
- 报文协议：APDU，GET_DATA 指令

13.3.5. 存储数据接口

- 请求方：多应用开放平台
- 功能： 多应用开放平台向 SE 发起存储数据请求；
- 报文协议：APDU，STORE_DATA 指令

13.3.6. 获取状态接口

- 请求方：多应用开放平台
- 功能： 多应用开放平台向 SE 发起获取状态请求；
- 报文协议：APDU，GET_STATUS 指令

13.3.7. 设置状态接口

- 请求方：多应用开放平台
- 功能： 多应用开放平台向 SE 发起设置状态请求；
- 报文协议：APDU，SET_STATUS 指令

13.4. IF4（多应用开放平台与支付平台）

13.4.1. 用户应用订购关系通知

- 请求方：支付平台
- 功能： 支付平台向多应用开放平台发送订购关系通知
- 属性：用户手机号码、应用名、订购关系建立、时间
- 报文协议：Web Service/SOAP

13.4.2. 用户销号/退订接口

- 请求方：业务平台

- 功能： 业务平台向多应用开放平台发起操作请求；
- 通讯协议：TCP/IP
- 报文协议：SOAP/Web Service

14. 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