ICS 35.240.40
A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0089.2—2012

中国金融移动支付　安全单元
第2部分：多应用管理规范

China financial mobile payment—Secure element—
Part 2: Management specification for multiple applications

2012－12－12 发布　　2012－12－12 实施

中国人民银行　　发 布

目　　次

前言..... II
引言..... III
1　范围..... 1
2　规范性引用文件..... 1
3　术语和定义..... 1
4　多应用管理概述..... 1
5　移动支付安全单元（SE）多应用架构..... 6
6　PAMID..... 9
7　金融安全域组件..... 9
8　金融目录管理应用..... 9
9　安全单元（SE）基本命令..... 11
10　安全单元（SE）密码算法要求..... 12
11　安全单元（SE）安全通信..... 12
12　安全单元（SE）可信服务..... 13
13　安全单元（SE）金融类辅助安全域管理与支付应用下载授权管理服务..... 13
14　应用个人化服务..... 13
15　安全单元（SE）应用选择服务..... 13

前　言

《移动支付—安全单元》由以下2部分构成：

——第1部分：通用技术要求；

——第2部分：多应用管理规范。

本部分为该标准的第2部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分负责起草单位：中国人民银行科技司、中国人民银行金融信息中心、中国金融电子化公司。

本部分参加起草单位：中移电子商务有限公司、中国银联股份有限公司、中国邮政储蓄银行、天翼电子商务有限公司、北京银联金卡科技有限公司（银行卡检测中心）、上海华虹集成电路有限责任公司、中钞信用卡产业发展有限公司、惠尔丰电子（北京）有限公司、宏达国际电子股份有限公司、握奇数据系统有限公司、北京同方微电子有限公司、大唐微电子技术有限公司、上海复旦微电子股份有限公司、恩智浦半导体有限公司、金雅拓智能卡公司、上海柯斯软件有限公司、福建联迪商用设备有限公司、武汉天喻信息产业股份有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、杜宁、李兴锋、韩建国、刘力慷、王妍娟、龚睿、乐祖晖、李一凡、江磊、田小雨、尚可、张柳成、张志茂、罗玲、吴星宇、陈敬宏、覃晖、邹重人、田燕军、范金钰、王晓华、任强、应根军、王文志、于海涛、胡瑞璟、姜达、赵亚平。

引　言

本部分描述了移动支付安全单元（SE）多应用管理所应遵循的技术规范。

中国金融移动支付 安全单元 第2部分：多应用管理规范

1 范围

本部分规定了移动支付安全单元（SE）多应用管理所应遵循的技术规范。首先，安全单元（SE）作为一种基本的多应用设备，其加载的多应用平台嵌入式软件需实现包括：安全域、全局服务应用、运行时环境等组件，这些组件可参考GPCS中的规格描述加以实现。除此之外，考虑移动支付联网通用目标，实现移动支付中安全单元（SE）的安全可信和开放共享，标准本部分还对安全单元（SE）作出有关：金融相关安全域配置、基本基础服务、加密及安全通道协议等方面的特定要求。

本部分适用于移动支付领域中移动终端、受理终端、安全单元（SE）生产厂商进行安全单元（SE）的设计、开发及选型参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0025.12 中国金融集成电路(IC)卡规范 第12部分:非接触式IC卡支付规范

JR/T 0097-2012 中国金融移动支付 可信服务管理技术规范

3 术语和定义

JR/T 0088.1-2012中界定的术语和定义适用于本文件。

4 多应用管理概述

4.1 概述

移动支付应用中，安全单元（SE）作为移动支付的安全载体，除负责对交易关键数据进行安全存储和运算，确保进行的敏感交易具有安全认证和不可抵赖性外，还需支持多应用动态管理及运行安全。具体地，移动支付安全单元（SE）多应用管理功能体现为：

——支持应用动态下载：支持在安全单元（SE）发行后，安全单元（SE）发行者或服务提供者根据业务扩充的需求，在安全单元（SE）上动态加载新的应用供用户使用；

——支持多应用共存：通过将安全单元（SE）上不同的应用关联至相应的安全域，可确保不同应用间互不影响，安全运行。有效解决诸如移动支付应用中的一卡多账户问题；

——支持动态空间管理：通过在安全单元（SE）上动态创建（删除）不同属性的安全域，可实现灵活、安全的空间管理，有效支撑建立基于安全单元（SE）的多种商业合作模式；

——支持与应用相匹配的安全策略：通过为不同的安全域实现其对应的安全通道，确保不同应用采用与之匹配的安全策略与安全单元（SE）外部实体之间进行鉴权及安全会话。

根据移动支付多应用需求，安全单元（SE）应实现多应用平台嵌入式软件，参考GPCS技术规范，安全单元（SE）多应用平台软件由安全域、全局服务应用、运行时环境、平台环境等一系列组件构成，为安全单元（SE）上的应用和卡外管理系统之间提供了一套独立于硬件和厂商的接口。

4.2 安全域

安全域负责提供各类安全服务，包括密钥管理、加密解密、针对其提供者(发行方、应用提供方、授权管理者)的应用进行数字签名的生成与验证。当发行方、应用提供方、授权管理者等卡外实体要将用到的安全服务进行隔离时，就可以通过安全域实现。

根据授权机构不同，安全单元（SE）安全域可以划分为三种主要类型：

发行方安全域：安全单元（SE）上首要的、强制性存在的安全域，是安全单元（SE）管理者(通常是发行方)在安全单元（SE）内的代表；

补充安全域：安全单元（SE）上次要的、可选择性存在的安全域，是应用提供方或发行方以及它们的代理方在安全单元（SE）内的代表；

授权管理者安全域：一种特殊类型的补充安全域，授权管理者负责将某种安全策略贯彻到所有加载到相应安全域的应用代码上，授权管理者安全域就是授权管理者在安全单元（SE）内的代表，安全单元（SE）上可能存在多个这样的安全域。

4.3 全局服务应用

安全单元（SE）上存在一个或者多个具有全局服务能力的应用，负责向其它应用提供者诸如安全单元（SE）持有者提供验证方法之类的服务。

4.4 运行时环境

安全单元（SE）多应用平台运行在一个安全的多应用运行时环境之上。该运行时环境负责向所有应用提供一套硬件中立应用编程接口，一种能确保各个应用的代码和数据能相互区隔的、安全的存储和执行空间分配机制，并提供服务来完成安全单元（SE）和安全单元（SE）外部实体之间的通信。

4.5 平台环境

安全单元（SE）平台环境的主要功能包括：向应用提供API、命令转发、应用选择、逻辑通道管理以及安全单元（SE）内容管理。当运行时环境没能实现或者没能以符合GP标准的方式实现这些功能时，则OPEN必须完成这些实现。

安全单元（SE）平台环境拥有一个内部的全局平台注册表，并利用它作为信息资源来进行安全单元（SE）内容管理。全局平台注册表包含了管理安全单元（SE）、可执行加载文件、应用、安全域关联以及权限所需要的信息。

安全单元（SE）平台环境的具体实现参照GPCS中对OPEN的规格定义。

4.6 平台 API

安全单元（SE）通过平台API向应用提供各种服务，比如持有方验证服务、个人化服务、安全服务等。此外还提供了安全单元（SE）内容管理服务，如安全单元（SE）锁定或应用生命周期状态更新服务。

4.7 安全单元（SE）内容

安全单元（SE）内容最初在安全单元（SE）里是以可执行装载文件的形式存在的。一个可执行装载文件可能存在于：

——安全单元（SE）内不可改变的存储区（ROM）中，在这种情况下，可执行装载文件在安全单元（SE）生产过程中就被装载到安全单元（SE）中，并且不可被改变（可以被禁止）；

——安全单元（SE）内可变存储区中：在这种情况下，可执行装载文件可以在发行前阶段或发行后阶段被装载或删除。

每一个可执行装载文件包含一个或多个可执行模块，也叫应用的代码。应用的安装会从一个可执行模块里创建一个实例连同该应用相关的数据一起放入安全单元（SE）的可变存储区中。任何应用的实例及其相关的数据都可以被移除。一个安全单元（SE）将支持多个可执行装载文件、多个可执行模块以及多个应用同时存在。

4.8 生命周期模型

4.8.1 安全单元（SE）生命周期

本章对安全单元（SE）生命周期状态及其状态切换做简要说明，安全单元（SE）生命周期状态如图 1 所示：

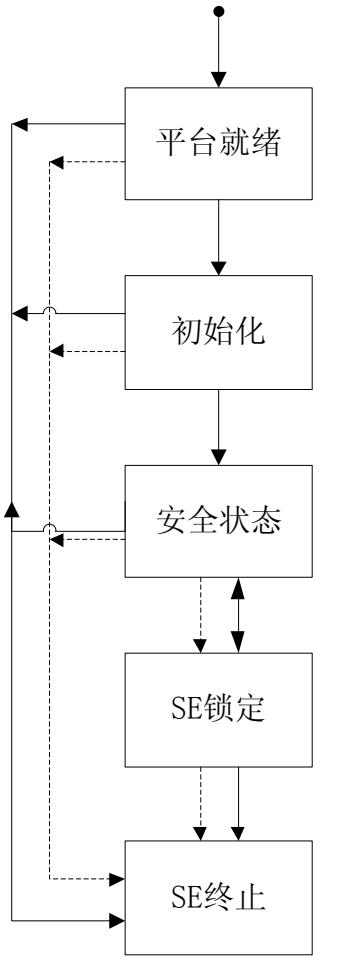

图1 生命周期状态迁移

状态说明：

——平台就绪：安全单元（SE）处于 OP_READY 状态时，发行方安全域应用选择就绪；命令处理模块做好接收、处理、响应 APDU 指令的准备；

——初始化：安全单元（SE）从生产机构切换至发行机构正式发行的中间产品管理状态，从平台就绪状态到初始化状态的切换为不可逆操作。初始化状态表明某些初始化信息(如发行方安全域的密钥及数据)已经驻留至安全单元（SE）；

——安全状态：标示安全单元（SE）生命周期处于正式发行后，产品已经发行到最终用户并正式启动、使用已装载业务。安全状态下，安全单元（SE）安全域和应用可以完全贯彻各自的安全策略。从初始化状态到安全状态的切换为不可逆操作；

——安全单元（SE）锁定：安全单元（SE）锁定状态下，禁止对载体上的安全域和应用进行选择。从安全状态到安全单元（SE）锁定状态的切换为可逆操作；

——安全单元（SE）终止：标志安全单元（SE）生命周期完结。安全单元（SE）终止状态意味着永久性禁止载体的任何功能以及任何内容管理和生命周期的改变。从任何其他状态都可直接切换到安全单元（SE）终止状态，且状态切换均为不可逆操作。

4.8.2 可执行加载文件/可执行模块生命周期管理

可执行装载文件生命周期只有一个状态。所有存放在安全单元（SE）内可变永久内存或不可变永久内存中的可执行装载文件处于 LOADED 状态。

可执行模块的生命周期取决于可执行装载文件的生命周期。

4.8.3 安全域/应用生命周期管理

安全域生命周期状态如图 2 所示：

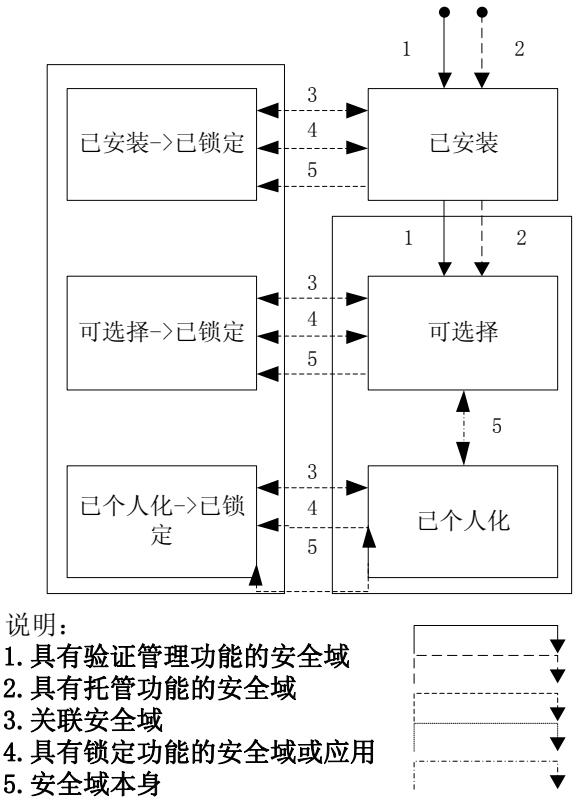

图2　生命周期状态迁移

注：授权管理安全域也符合上图安全域生命周期管理。

状态说明：

——已安装：状态标示安全域已完成注册表条目注册。该状态下，安全域服务不能被应用使用，安全域不可选定，不能与可执行装载文件或应用关联；

——可选择：状态标示安全域可被选择，可接收相关个人化指令。该状态下未装载应用密钥，不能和可执行装载文件或应用进行关联。从已安装状态到可选择状态的切换为不可逆操作；

——已个人化：状态标示安全域已完成运行所需个人化数据与密钥数据的装载。该状态下，安全域与应用已建立关联。从可选状态到已个人化状态的切换为不可逆操作；

——已锁定：OPEN 或经过发行者安全域认证后的卡外实体可以将安全域的生命周期状态设置为已锁定状态，以阻止该安全域进一步被选择。该状态下，安全域委托管理将不能成功执行。安全域锁定状态解锁仅发行者安全域或具有授权管理权限的安全域可完成。OPEN 保证该安全域生命周期在解锁后恢复至锁定前状态。

应用的生命周期管理，按照JR/T 0097-2012相关内容及GP应用生命周期状态配置说明，安全单元（SE）应用生命周期状态如图3所示。

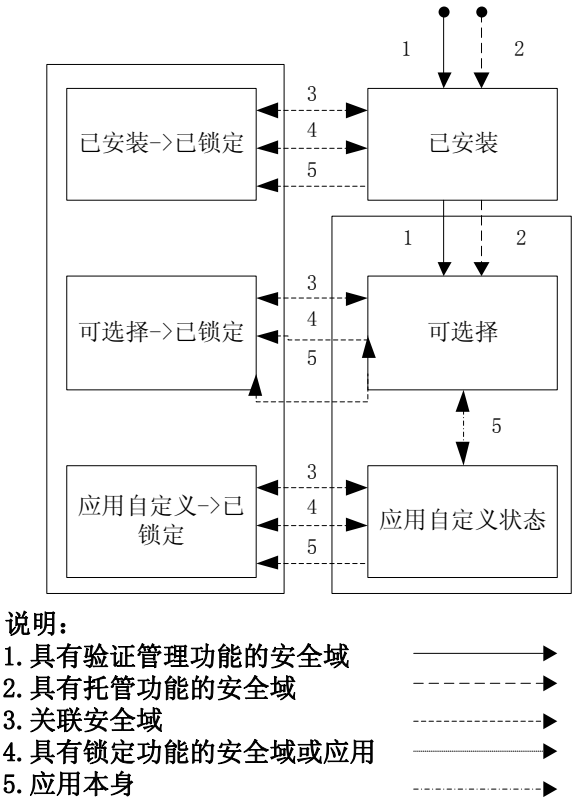

图3　生命周期状态迁移

状态说明：

——已安装：状态标示应用已完成安全单元（SE）注册表条目注册。该状态下，该应用为不可选；

——可选择：状态标示应用可被成功选择，可接收相关指令。从已安装状态到可选择状态的切换为不可逆操作；

——已锁定：OPEN 或经过发行者安全域认证后的安全单元（SE）外实体可以将应用的生命周期状

态设置为已锁定状态，以阻止该应用被成功选择或执行。应用锁定状态解锁仅对应用有管理权限的安全域可完成。OPEN 保证该应用生命周期在解锁后恢复至锁定前状态；

——应用自定义：此为应用本身自定义状态，标准本部分不做说明。

5 移动支付安全单元（SE）多应用架构

5.1 安全单元（SE）多应用组件

支持移动支付的安全单元（SE）多应用架构由一系列组件构成，包括PAMID、金融安全域组件、金融目录管理应用组件和支付应用组件。

其中PAMID是安全单元（SE）在金融网络的唯一身份标识符，由发行方写入安全单元（SE）硬件中，PAMID写入后不能够被更改。

金融安全域组件是用于支持移动支付的一系列特定安全域，以实现移动支付的安全单元（SE）安全可信和开放共享服务。

金融目录管理应用组件用于管理安全单元（SE）上已安装支付应用的目录列表，提供安全单元（SE）上支付应用的选择服务。

支付应用组件是在安全单元（SE）上安全的提供支付功能的系列应用。

安全单元（SE）多应用组件如图4所示：

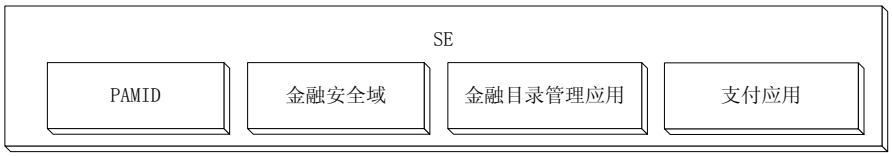

图4 移动支付 SE 多应用组件

根据开放共享模型的不同，由如上组件可构成两种多应用框架：

——以发行方作为可信管理者的安全单元（SE）多应用框架；

——以公共服务平台作为可信管理者的安全单元（SE）多应用框架。

5.2 以发行方作为可信管理者的安全单元（SE）多应用框架

该框架中包括主控安全域、金融认证安全域（FCSD）、金融目录管理应用和支付应用，详见图5。

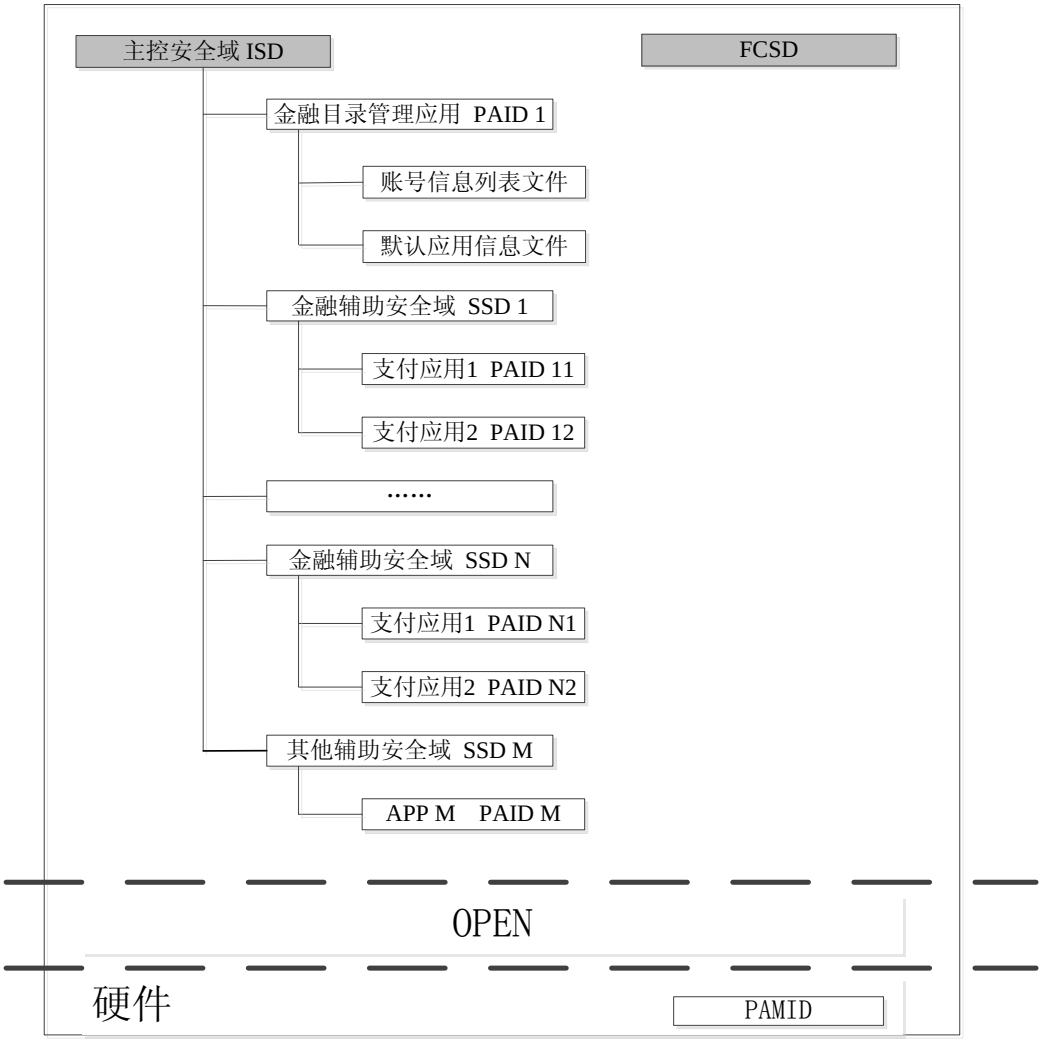

图5 以发行方作为可信管理者的安全单元（SE）多应用框架

本框架中，主安全域由发行方持有，提供金融类辅助安全域的生命周期管理和应用管理授权，金融类辅助安全域采用委托或授权管理模式不做要求。支付应用关联到金融类辅助安全域，并可由主安全域管理授权。金融目录管理应用关联到主安全域，提供支付应用目录管理和选择服务。金融认证安全域由公共服务平台持有，在安全单元（SE）首次接入到金融网络前配置，提供安全单元（SE）可信服务。

5.3 以公共服务平台作为可信第三方管理者的安全单元（SE）多应用框架

本框架中，包括主控安全域、金融认证安全域(FCSD)、金融管理安全域（FMSD）、金融目录管理应用和支付应用，详见图6。

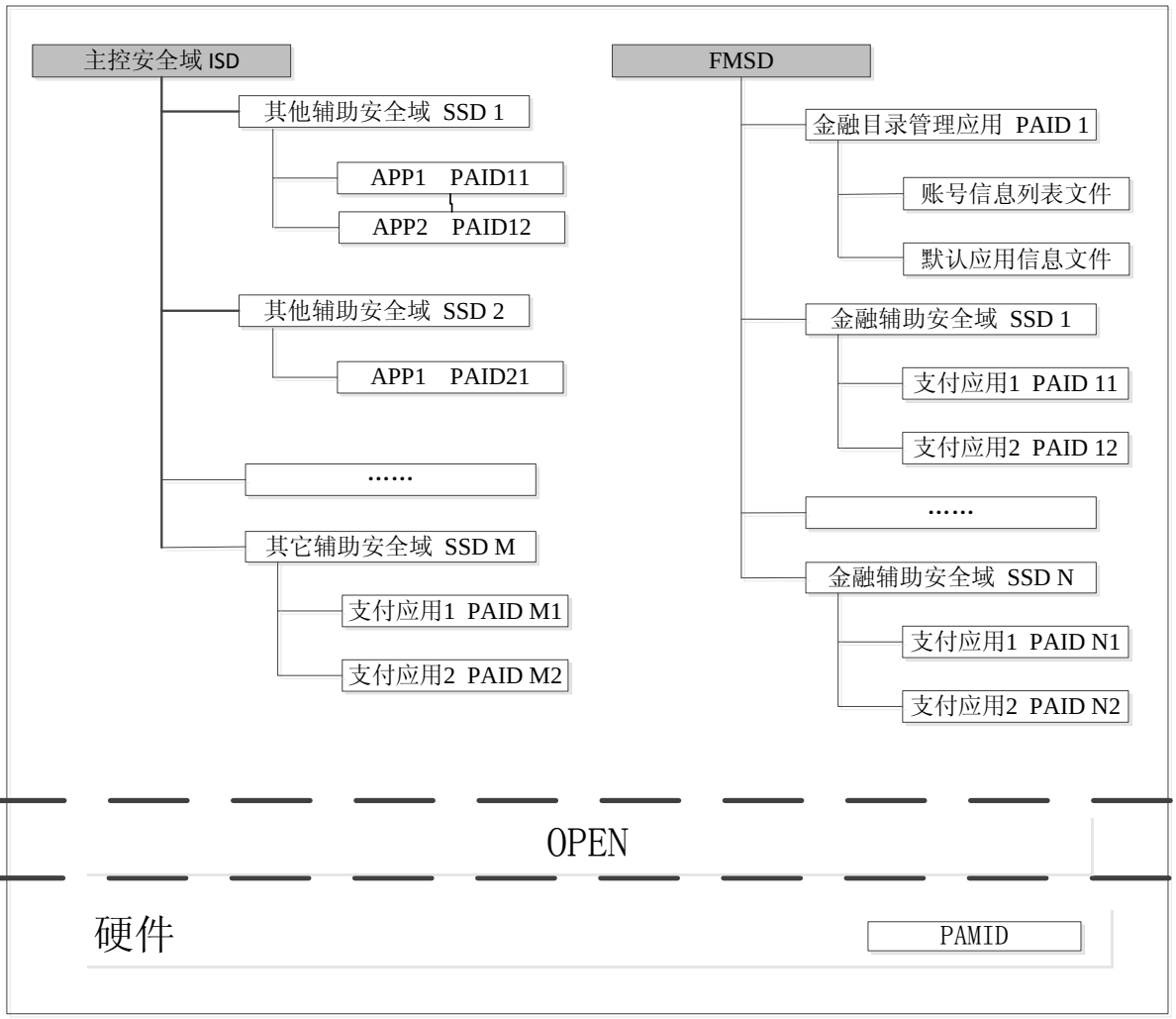

图6 以公共服务平台作为可信管理者的安全单元（SE）多应用框架

本框架中，主安全域由发行方持有，提供非金融类辅助安全域的生命周期管理和应用管理授权。金融管理安全域由公共服务平台持有，在安全单元（SE）首次接入到金融网络前配置，具备授权管理者权限，提供金融类辅助安全域的生命周期管理和支付应用授权管理。支付应用关联到金融类辅助安全域，并由金融管理安全域授权。金融目录管理应用关联到金融认证安全域，提供支付应用目录管理和选择服务。

在实现中，当同时存在金融认证安全域和金融管理安全域时，金融管理安全域的功能应集成到金融认证安全域内。图7描述了该模型下安全单元（SE）的一个实现结构：

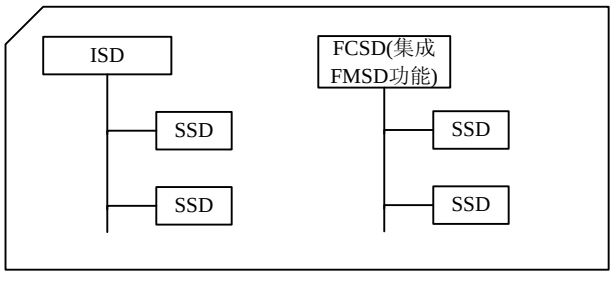

图7　以公共服务平台作为可信管理者

6　PAMID

PAMID是安全单元（SE）在金融网络中的唯一身份标识符，

PAMID由公共服务平台负责统一分配，由安全单元（SE）发行方写入并向公共服务平台备案。PAMID包含发行方代码、SE类型代码（SIM、SD、全终端等）及唯一序列号，其中发行方代码及SE类型代码由公共服务平台统一分配，唯一序列号由发行方根据编码规则自行管理。PAMID写入SE后，发行方向公共服务平台备案，PAMID写入后不允许更改。分配和备案管理流程见JR/T 0097-2012。

芯片生产商应在芯片中为PAMID提供一段物理存储区，该存储区可保证PAMID写入后不可被更改。芯片生产商应提供写入接口给安全单元（SE）发行方，由发行方将PAMID写入安全单元（SE）中。

OPEN应该提供接口用于安全域和支付应用读取PAMID。

7　金融安全域组件

7.1　金融认证安全域

金融认证安全域(FCSD)是一种特殊的辅助安全域，其主要功能是进行安全单元（SE）及其持有人实名身份的验证和获取：

——是公共服务平台在安全单元（SE）内的代表，由公共服务平台持有；

——具备安全域权限；

——其安全域关联到自身；

——安全单元（SE）接入金融网络前配置，配置完成后继承了卡片生命周期状态；

——不允许被主安全域锁定、删除；

——提供 SCP02 和 SCP10 安全通道，SCP02 安全通道用于初始化金融认证安全域，初始化完成后应只能够使用 SCP10 安全通道。

金融认证安全域应能存储下述数据：SE 及持有人的私钥和公钥证书，公共服务平台公钥证书，其它私有数据。这些数据可以使用 GET DATA 命令获得。

7.2　金融管理安全域

金融管理安全域(FMSD)是一种特殊的辅助安全域，安全域关联到自身，其主要功能是进行金融类辅助安全域的生命周期管理和应用授权。

——是公共服务平台在安全单元（SE）内的代表，由公共服务平台持有；

——具备安全域权限，授权管理者权限，令牌校验权限，DAP 权限；

——其安全域关联到自身；

——安全单元（SE）接入金融网络前配置，配置完成后继承了卡片生命周期状态；

——不允许被主安全域锁定、删除；

——提供 SCP02 和 SCP10 安全通道，SCP02 安全通道用于初始化金融管理安全域，初始化完成后应只能够使用 SCP10 安全通道。

——实现中不允许单独存在金融管理安全域，在金融认证安全域和金融管理安全域同时存在的情况下，要求金融管理安全域功能集成到金融认证安全域内。

8　金融目录管理应用

金融目录管理应用用于管理安全单元（SE）上已安装支付应用的目录列表，提供安全单元（SE）上支付应用的选择服务。金融目录管理应用可通过账户信息列表文件和默认账户信息列表文件的方式来实现，一个实现如图8所示。

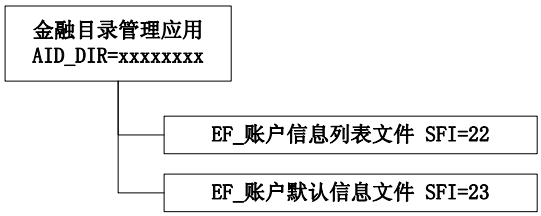

图8　金融目录管理应用

在移动支付SE中，每个安装的应用实例都在账户信息列表文件中注册一条记录，当应用实例删除时同时删除列表文件中的对应记录。

在移动支付SE中，当同一类型的应用(PAID的应用类型字段相同)存在多个应用实例，可以设置其中的一个应用实例为默认应用实例。设置为默认的应用实例会在账户默认信息文件中注册一条记录。当同一类型的有且只有一个应用实例时，该应用实例缺省作为默认的应用实例。

账户信息列表文件定义如表1：

表1　账户信息列表文件

文件标识(SFI)		22
文件类型		循环记录文件
文件大小		26*50
记录长度		26
记录个数		20
读权限		CVM
写权限		安全通道建立
字节	数据元	长度
1-50	账户编号	50
51-66	应用标识符（PAID）	16

账户默认信息文件定义如表2：

表2　账户默认信息文件

文件标识（SFI）	23
文件类型	记录文件
文件大小	16*20
记录长度	16
记录个数	10
读权限	CVM

文件标识（SFI）		23
写权限		CVM
字节	数据元	长度
1～16	默认应用标识符PAID	16

9 安全单元（SE）基本命令

安全单元（SE）基本命令参见表 3：

表3 安全单元（SE）基本命令

命令	OP_READY			INITIALIZED			SECURED			CARD_LOCKED		TERMINATED	
	AMSD	DMSD	SD	AMSD	DMSD	SD	AMSD	DMSD	SD	FCSD FMSD	SD	FCSD FMSD	SD
DELETE 可执行加载文件													
DELETE 可执行加载文件和相关应用													
DELETE 应用	√	√		√	√		√	√					
DELETE 密钥													
GET DATA	√	√	√	√	√	√	√	√	√	√		√	
GET STATUS	√			√			√			√			
INSTALL [加载]													
INSTALL [安装]													
INSTALL [加载、安装和设为可选]													
INSTALL [安装和设为可选]	√	√		√	√		√	√					
INSTALL [设为可选]													
INSTALL [引渡]													
INSTALL [更新注册表]													

命令	OP_READY			INITIALIZED			SECURED			CARD_LOCKED		TERMINATED	
	AM SD	DM SD	SD	AM SD	DM SD	SD	AM SD	DM SD	SD	FCSD FMSD	SD	FCSD FMSD	SD
INSTALL [个人化]													
LOAD													
PUT KEY	√			√			√						
SELECT	√	√	√	√	√	√	√	√	√	√			
SET STATUS	√			√			√			√			
STORE DATA	√			√			√						

10 安全单元（SE）密码算法要求

移动支付业务处理过程中，使用到的密码算法主要包括对称加密算法、非对称加密算法、摘要算法三种：

——对称加密算法，包括但不限于：SM4、DES、3DES；

——非对称加密算法，包括但不仅限于：SM2、RSA；

——摘要算法，包括但不仅限于：SM3、SHA-1。

算法选择应符合国家行业主管部门要求。

11 安全单元（SE）安全通信

11.1 SCP02 安全通道机制

SCP02 安全通道机制所需 APDU 命令，详见表 4。

表4 SCP02 APDU 命令

指令	最低安全级别
INITIALIZE UPDATE	无
EXTERNAL AUTHENTICATE	C-MAC

11.2 SCP10 安全通道机制

SCP10 安全通道机制所需 APDU 命令，详见表 5。

表5 SCP10 APDU 命令

指令	安全通道初始化	
	不带安全信息（message recovery）签名	带安全信息（message recovery）签名
EXTERNAL AUTHENTICATE	√	√
GET CHALLENGE	√	√
GET DATA[certificate]	√	√

指令	安全通道初始化	
	不带安全信息（message recovery）签名	带安全信息（message recovery）签名
INTERNAL AUTHENTICATE	√	√
MANAGE SECURITY ENVIRONMENT	√	√
PERFORM SECURITY OPERATION[decipher]	√	
PERFORM SECURITY OPERATION[verify certificate]	√	√

12 安全单元（SE）可信服务

配置有金融认证安全域的安全单元（SE）提供安全单元（SE）可信服务，安全单元（SE）可信服务流程见 JR/T 0097-2012。

13 安全单元（SE）金融类辅助安全域管理与支付应用下载授权管理服务

配置有金融管理安全域的安全单元(SE)提供金融类辅助安全域管理和支付应用下载授权管理服务，相关流程见 JR/T 0097-2012。

14 应用个人化服务

应用安装后，应用可能需要加载其个人化数据，包括它自己的密钥和针对持卡人的数据。应用能够使用安全通信和其相关安全域提供的密钥解密服务来管理定制数据的安全下载。

安全单元（SE）应支持如下两种方式实现个人化：

——使用运行时消息支持；

——使用安全域访问应用的能力。

15 安全单元（SE）应用选择服务

安全单元（SE）应用选择服务由金融目录管理应用提供，包括如下两种：

——受理环境选择金融应用，非接触途径要求仅提供 PPSE（Proximity Payment Systems Environment 近距离支付系统环境）选择，按照 JR/T0025.12 中相关 PPSE 选择流程描述，通过 FCI（File Control Information 文件控制信息）模板返回应用 AID 列表。

——移动终端上的应用管理客户端选择金融应用，应用管理客户端直接使用 SELECT AID 方式，选择金融应用。通过 READ RECORD 指令（指令参数 SFI 为 22 或 23，即账户信息文件和默认账户信息文件）读取记录文件，实现应用选择。