ICS 35.240.40
A.11

JR

中华人民共和国金融行业标准

JR/T 0097—2012

中国金融移动支付
可信服务管理技术规范

China financial mobile payment—
Technical specification for trusted service management

2012-12-12 发布　　2012-12-12 实施

中国人民银行　　发布

目　　次

前　言

本规范按照GB/T 1.1-2009给出的规则起草。

本规范由中国人民银行提出。

本规范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：中国银联股份有限公司、中国工商银行、中国农业银行、交通银行、上海浦东发展银行、中国邮政储蓄银行、北京中电华大电子设计有限责任公司、天翼电子商务有限公司、联通支付有限公司、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、中国金融认证中心、金雅拓智能卡公司、握奇数据系统有限公司、捷德（中国）信息科技有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、姜云兵、杜宁、李兴锋、刘力慷、辛路、谭颖、袁捷、兰天、吴水炯、姜鹏、谢元呈、李晨光、李庆艳、李茁、纪洪明、宋铮、熊帅、陈震天、张健、孙战涛、马志全、燕宜军、温丽明。

引　言

随着移动支付新业务、新产品、新管理模式的不断涌现，以客户需求为主导的移动支付业务出现了不断交融和细化的趋势，不同机构、不同部门、不同业务之间的信息交换和信息共享变得越来越频繁。统一文件数据格式可以有效加强商业银行、支付机构、商户之间的互联互通及信息共享，降低交易成本，提高市场效率。

考虑到移动支付涉及面广、业务种类繁杂以及各商业银行、支付机构和公共服务平台建设方的业务系统现状，为便于标准的推广，本部分仅对目前移动支付领域中比较成熟的、通用的文件数据格式进行抽象和规范，同时对涉及公共服务平台的文件数据格式进行了扩充定义。对于仍存在不确定性的创新业务相关文件接口，在标准后续的修订过程中逐步纳入。

中国金融移动支付　可信服务管理技术规范

1　范围

本标准规定了移动支付可信服务管理系统组成、互联结构、SE安全可信和SE开放共享等服务模型，也规定了公共服务平台和TSM平台的主要功能、业务流程、应用接口以及系统安全性要求。

本部分适用于从事移动支付相关产品的设计、制造、管理、发行、受理以及相关应用系统的研制、开发、集成和维护的组织。

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。

GB/T 18238.3　信息技术 安全技术 散列函数

GB/T 20518　信息安全技术 公钥基础设施 数字证书格式

GM/T 0002　SM4分组密码算法

GM/T 0003　SM2椭圆曲线公钥密码算法

GM/T 0004　SM3密码杂凑算法

JR/T 0088.3　中国金融移动支付 应用基础 第3部分：支付应用标识符

JR/T 0089.2　中国金融移动支付 安全单元 第2部分：多应用管理规范

JR/T 0094.3　中国金融移动支付 中国金融移动支付 近场支付应用 第3部分：报文结构及要素

RFC 3280　Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

3　术语与定义

下列术语和定义适用于本文件。

3.1

金融认证安全域(FCSD)　Finance Certification Secure Domain (FCSD)

由公共服务平台持有，存储和验证SE及其持有人的实名身份信息的安全域。

3.2

金融管理安全域(FMSD) Finance Manage Secure Domain (FMSD)

由公共服务平台持有，具备授权管理者权限，提供辅助安全域管理功能、令牌验证功能、DAP验证功能的安全域。

3.3

管理客户端　Manage Client

用于提供用户接口界面，和SE配合实现SE管理和应用管理功能的终端。管理客户端包括专用的应用管理终端和移动终端上装载的客户端软件。

3.4

SE 可信服务 SE Trusted Service

指公共服务平台通过其持有的SE可信部件，为移动支付的各参与方提供独立第三方的SE及其持有人合法性验证与实名身份信息传递，满足参与各方获取SE及其持有人实名身份信息的需求。

3.5

SE 可信部件 SE Trusted Component

SE中由公共服务平台持有的、配合公共服务平台实现SE及其持有人合法性验证的部件。该部件由FCSD安全域及其权限、配置的密钥等基础数据以及可提供的功能共同组成。

3.6

SE 开放共享服务 SE Share Service

指公共服务平台通过其持有的SE开放共享部件，为移动支付的各应用提供方共享SE中空间和能力，满足各应用提供方在SE中合理发放应用的需求。

3.7

SE 开放共享部件 SE Share Component

SE中由公共服务平台持有的、配合公共服务平台实现SE空间和能力开放共享的部件。该部件由FMSD安全域及其权限、配置的密钥等基础数据以及可提供的功能共同组成。

3.8

SE 载体管理/多应用管理部件 SE Equitment Manage/MultApplication Manage Component

SE中负责SE生命周期管理、应用生命周期管理的COS、软件平台、运行环境，及其上的安全域、权限、配置的密钥等基础数据以及可提供的功能共同组成。

3.9

平台管理系统 Platform Manage System

用于提供用户接口界面，实现公共服务平台管理功能的信息系统。

4 移动支付可信服务管理系统架构

4.1 概述

移动支付可信服务管理系统是移动支付的可信基础设施，本部分描述了该可信服务管理系统的逻辑实体组成、基础服务模型，及其配置、功能和交互接口。这些结构和机制，构成了移动支付的安全可信、开放共享、多应用共存与互联互通的基础。

4.2 移动支付可信服务管理系统组成

4.2.1 系统组成

移动支付可信服务管理系统由公共服务平台、发行方TSM平台、应用提供方TSM平台和SE四个逻辑实体共同组成，每个逻辑实体都包括基本的配置、功能和交互接口。图1描述了移动支付可信服务管理系统的各逻辑实体和基本关系。

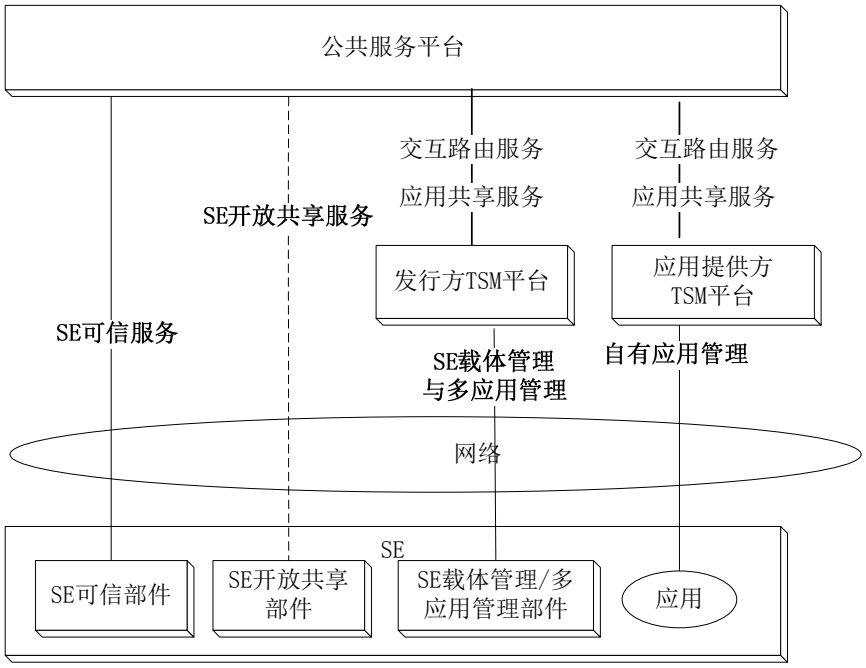

图1　移动支付可信服务管理系统结构

其中公共服务平台用于为跨机构的交互提供交互路由、应用共享、SE可信和SE开放共享等基础服务。

发行方TSM平台提供SE载体管理和多应用管理功能，应用提供方TSM平台提供对自有应用的管理功能。为方便描述，发行方TSM平台和应用提供方TSM平台统称为TSM平台。

SE作为可信服务管理系统的承载端，包括SE可信部件、SE开放共享部件和SE载体管理/多应用管理部件，其中SE可信部件和SE开放共享部件配合公共公共服务平台实现安全可信和开放共享服务，SE载体管理/多应用管理部件配合发行方TSM平台实现SE载体管理和多应用管理功能。为方便描述，在SE可信部件和SE开放共享部件同时存在时，也称为SE可信/开放共享部件。

图中虚线部分表示该服务及其所对应部件是可选的。

4.2.2　公共服务平台

公共服务平台是移动支付参与各方均认可的可信第三方实体，在跨机构的交互中，为 TSM 平台提供跨机构交互路由、应用共享、SE 可信、SE 开放共享四大服务。

其中跨机构交互路由服务包括 TSM 平台接入、跨机构交互的路由发现、消息分发和数据资源地址传递。

应用共享服务包括应用注册、应用发现、全网应用注册表维护。

SE 可信服务主要包括 SE 注册管理、SE 及其持有人身份获取和实名身份信息传递。

SE 开放共享服务主要包括金融类辅助安全域管理、初始密钥分发、应用授权管理。

公共服务平台基础服务组成如图2所示。

图2　公共服务平台基础服务

4.2.3　发行方 TSM 平台和应用提供方 TSM 平台

发行方 TSM 平台是承担 SE 载体管理与多应用管理的实体，主要提供 SE 载体管理与多应用管理两个服务。其中 SE 载体管理包括 SE 的生命周期管理，多应用管理包括应用提供方管理、辅助安全域的生命周期管理、应用存储与发布、应用管理授权、应用生命周期管理。

应用提供方 TSM 平台是承担应用管理的实体，主要提供对自有应用的管理服务，包括应用提供方管理、应用存储与发布、应用生命周期管理。

为方便描述，本标准中除非特别说明，发行方的 TSM 平台和应用提供方的 TSM 平台统称为 TSM 平台。

4.2.4　SE

SE 是移动支付可信服务管理系统功能的承载端，存储基础配置并提供基础功能，配合公共服务平台和 TSM 平台实现相关服务，本标准要求 SE 至少包括 SE 可信/开放共享部件和 SE 载体管理/多应用管理部件。

其中 SE 可信/开放共享部件配置必要的安全域，可存储密钥、证书等机密信息并提供密码计算等安全功能，具备相应的管理权限，配合公共服务平台，为移动支付各参与方提供 SE 及其持有人的实名身份信息，为应用提供方提供金融类辅助安全域管理、应用下载授权等功能。

SE载体管理/多应用管理部件提供基础运行环境，提供基本公共服务，配置必要的安全域和管理权限，配合TSM平台实现SE载体管理和多应用管理功能。

4.3　跨机构交互路由服务模型

公共服务平台提供跨机构交互的交互路由服务，该服务模型由多个连接到公共服务平台的TSM平台构成，包括跨机构交互的建立和跨机构数据资源下载两个环节。

在跨机构交互的建立环节，TSM平台分别接入到公共服务平台，由公共服务平台分配机构ID并登记各TSM平台的网络地址，形成全局路由表；当需要进行跨机构间的交互时，发起交互的TSM平台提供目标TSM平台的机构ID，由公共服务平台进行网络路由和消息分发，协调双方完成交互的建立。实体关系如图3所示。

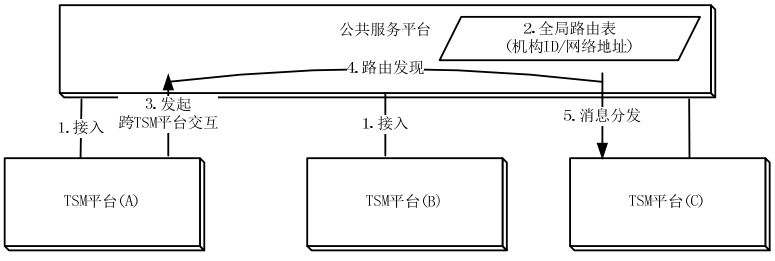

图3　跨机构交互路由—路由建立

实体关系描述如下：

步骤 1：TSM 平台接入到公共服务平台，公共服务平台分配机构 ID 并登记其网络地址；

步骤 2：公共服务平台维护全局路由表，分别建立并维护和各 TSM 平台的网络连接，用于跨机构交互的路由发现和消息分发；

步骤 3：对于跨机构的交互，发起方 TSM 平台提供目标 TSM 平台的机构 ID，发起跨机构的交互；

步骤 4：公共服务平台负责将目标 TSM 平台的 ID 解析为网络地址，实现路由发现；

步骤 5：由公共服务平台进行跨机构交互的消息分发，协调双方以完成交互的建立。

如果跨机构的交互中涉及到数据传输，双方经公共服务平台协调建立连接后，该服务进入跨机构数据资源下载环节。在该环节，由公共服务平台解析并返回数据资源地址到管理客户端/SE，并由管理客户端/SE 和目标 TSM 平台建立直接通道后下载数据。图 4 描述了跨机构数据资源下载的实体关系。

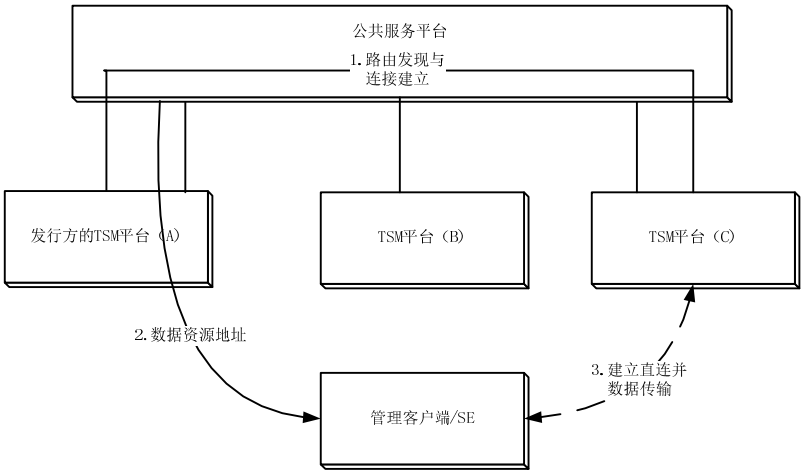

图4　跨机构交互路由—数据资源下载

实体关系描述如下：

步骤 1：涉及到数据传输的跨机构交互，由公共服务平台分发协调交互双方，建立连接；

步骤 2：公共服务平台返回数据资源地址到管理客户端/SE，该消息通过发行方的 TSM 平台透传；

步骤 3：管理客户端/SE 通过该数据资源地址建立和应用所在 TSM 平台的直连通道，下载应用。

4.4　跨机构应用共享模型

跨机构应用共享是指 SE 能够发现可信服务管理系统中所有可用的应用并下载安装。跨机构应用共享通过应用分发和应用下载两个环节实现。

在应用分发环节，参与实体包括发行方的 TSM 平台、公共服务平台、应用提供方的 TSM 平台。参与实体及其基本关系如图 5 所示。

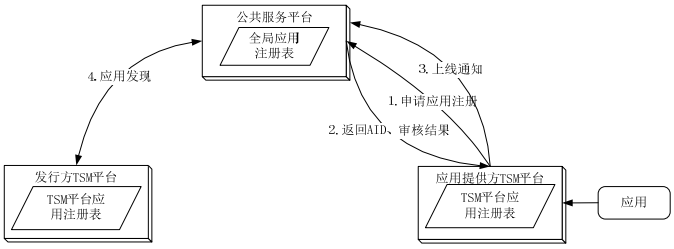

图5　跨机构应用共享—应用分发

实体关系描述如下：

步骤 1：应用提供方的 TSM 平台新增一个应用，该 TSM 平台向公共服务平台申请对该应用进行注册；

步骤 2：公共服务平台对该应用进行审查，通过后为其分配 PAID，登记到全局应用注册表中，并返回审查结果给应用提供方的 TSM 平台；

步骤 3：该应用在应用提供方 TSM 平台上线发布，应用提供方 TSM 平台向公共服务平台发出应用上线通知，公共服务平台修改全局应用注册表中该应用的状态。

步骤 4：管理客户端/SE 可以经由其相连的发行方 TSM 平台从公共服务平台获取所有可用的应用列

表，实现应用发现。

在应用下载环节，参与实体包括发行方的 TSM 平台、公共服务平台、应用提供方的 TSM 平台、管理客户端/SE 组成。参与实体及其基本关系如图 6 所示。

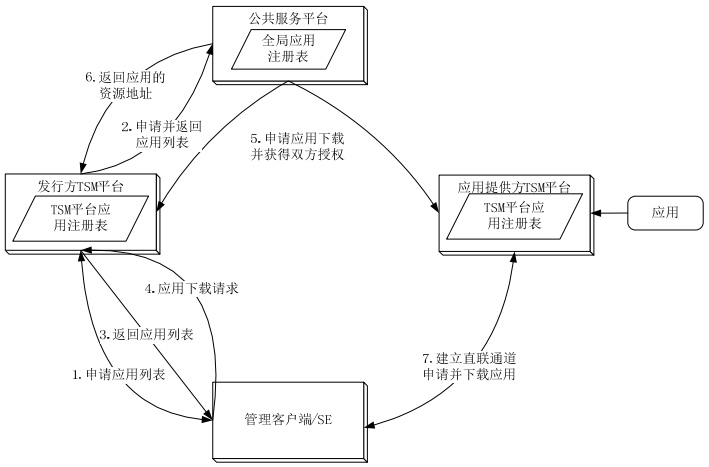

图6　跨机构应用共享—应用下载

实体关系描述如下：

步骤 1：管理客户端/SE 向其相连的发行方的 TSM 平台请求可用应用列表；

步骤 2：如果所请求的应用列表范围超过了发行方的 TSM 平台，发行方的 TSM 平台转发该请求到公共服务平台，公共服务平台从全网注册表中返回应用列表；

步骤 3：发行方的 TSM 平台返回应用列表给管理客户端/SE；

步骤 4：用户根据返回的应用列表，通过管理客户端/SE 选择应用下载，该请求发送到管理客户端连接的发行方 TSM 平台；发行方 TSM 平台转发该请求到公共服务平台；

步骤 5：公共服务平台协商应用提供方的 TSM 平台和发行方的 TSM 平台，获得双方的下载授权，这些操作均通过公共服务平台中转；

步骤 6：如果双方同意下载，公共服务平台向管理客户端/SE 返回应用的数据资源地址，该消息通过客户端/SE 相连的发行方 TSM 平台中转；

步骤 7：管理客户端/SE 根据数据资源定位地址，和应用提供方的 TSM 平台建立直连通道，发出下载请求并下载所选应用。

4.5　开放共享模型

4.5.1　概述

为了能够实现SE向移动支付各参与方的开放共享，本标准定义了移动支付的开放共享模型。不同的开放共享模型可以满足移动支付参与方的不同安全控制要求。根据业务的风险等级和合作模式，SE发行方可以自主选择其中一种开放共享模型。

4.5.2　以公共服务平台作为可信第三方的开放共享模型

该模型参与实体包括发行方的 TSM 平台、公共服务平台、应用提供方的 TSM 平台、SE。其中公共服务平台作为独立于发行方和应用提供方的可信第三方，作为授权管理者，执行 SE 及其持有人的实名身份获取、实名身份传递，金融类辅助安全域的创建、密钥分发、删除、锁定/解锁操作；对金融类辅助安全域中的应用下载、安装等操作进行授权。

图 7 描述了该开放共享模型下安全域的操作：

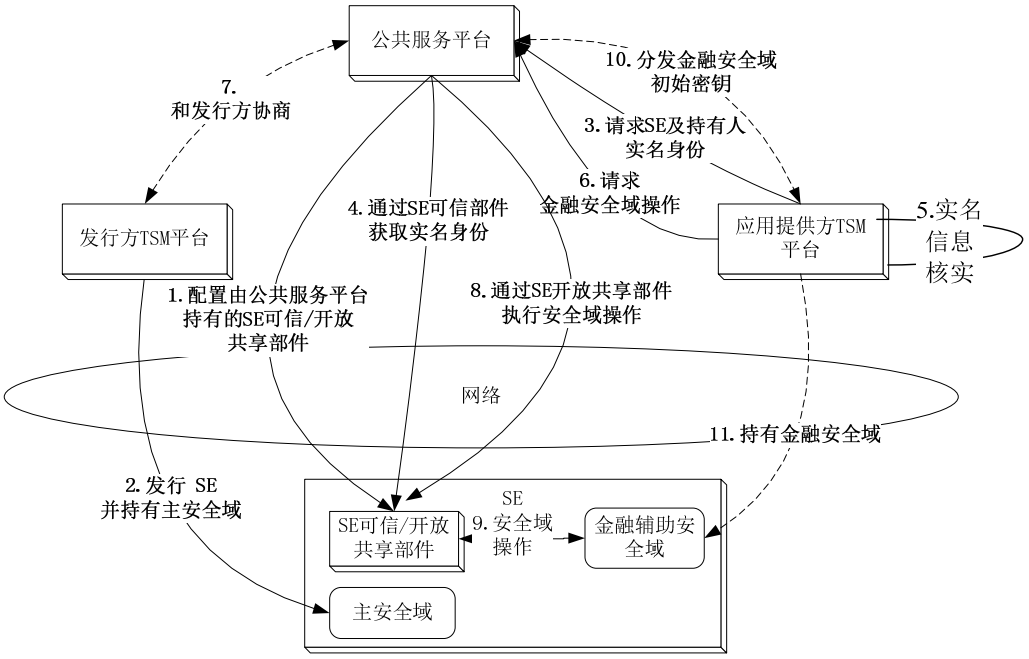

图7　公共服务平台作为可信第三方共享模型—安全域操作

安全域操作中，实体关系如下：

步骤 1：SE 在用户发放前，配置由公共服务平台持有的 SE 可信/开放共享部件，该部件体现为独立的授权管理者安全域及其权限和服务；

步骤 2：发行方的 TSM 平台向用户发 SE，并持有主安全域(ISD)；

步骤 3：应用提供方的 TSM 平台需要进行金融类辅助安全域操作前，需要请求公共服务平台通过 SE 可信部件验证并获取 SE 及其持有人身份；

步骤 4：公共服务平台通过 SE 可信部件验证并获取 SE 及其持有人身份信息，并传递给应用提供方的 TSM 平台；

步骤 5：应用提供方的 TSM 平台对所获得的实名身份根据业务安全等级要求进行核实，如临柜核实或电话核实等；

步骤 6：如果 SE 及其持有人身份合法，则向公共服务平台发出操作请求，操作类型包括金融类辅助安全域的创建、删除、锁定/解锁、个人化、状态查询；

步骤:7：如果需要和发行方的 TSM 平台进行操作的协商，公共服务平台和发行方的 TSM 平台交互并获得许可；

步骤 8：公共服务平台通过 SE 开放共享部件下发操作命令；

步骤 9：SE 开放共享部件执行金融类辅助安全域的相关操作；

步骤 10、步骤 11：如果需要进行金融类辅助安全域的个人化操作，公共服务平台分发初始化密钥给应用提供方的 TSM 平台；应用提供方的 TSM 平台更新密钥并持有安全域。

应用提供方的 TSM 平台持有金融类辅助安全域后，应用的操作由应用提供方的 TSM 平台实施，但需要由公共服务平台提供授权，图 8 描述了该开放共享模型下应用操作的实体关系。

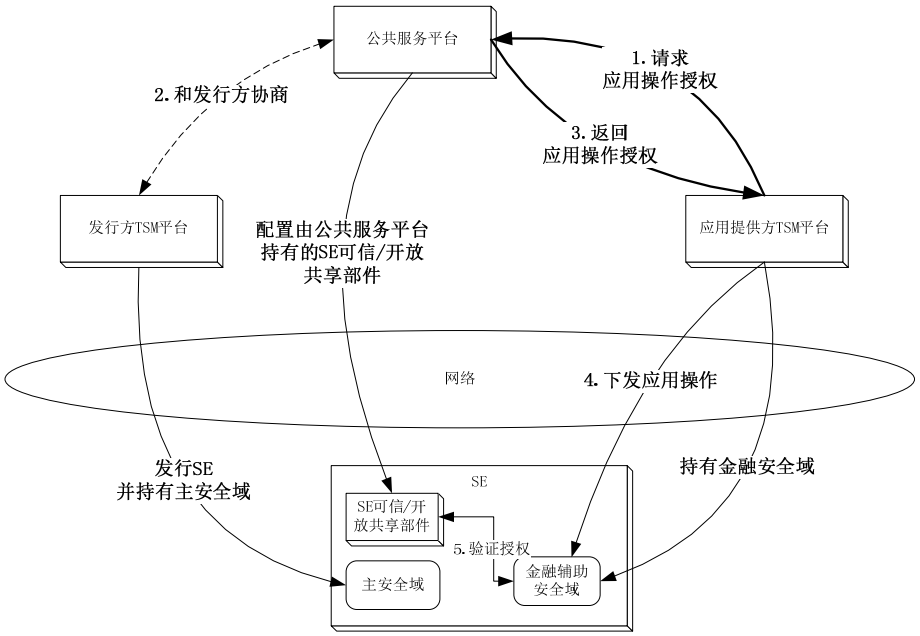

图8　公共服务平台作为可信第三方共享模型—应用操作

应用操作中实体关系如下：

步骤 1：应用提供方的 TSM 平台执行操作前，向公共服务平台请求应用操作的授权；

步骤 2：如果需要，公共服务平台和发行方的 TSM 平台协商，获得应用操作的许可；

步骤 3：公共服务平台对应用进行授权并返回给应用提供方的 TSM 平台，该授权具体体现为一个令牌；

步骤 4：应用提供方的 TSM 平台下发应用操作脚本到其持有的安全域；

步骤 5：SE 中由 SE 开放共享部件对操作的授权进行验证，如果通过，那么该操作执行；否则该操作失败。

4.5.3　以发行方作为可信管理者的开发共享模型

该模型参与实体包括发行方的 TSM 平台、公共服务平台、应用提供方的 TSM 平台、SE。其中发行方的 TSM 平台作为可信管理者，执行金融类辅助安全域的创建、删除、锁定/解锁、个人化操作；对金融类辅助安全域中的应用下载、删除、锁定/解锁操作进行授权；公共服务平台仅作为可信第三方提供 SE 及其持有人身份获取和实名身份信息传递。

图 9 描述了该开放共享模型下的安全域操作的实体关系。

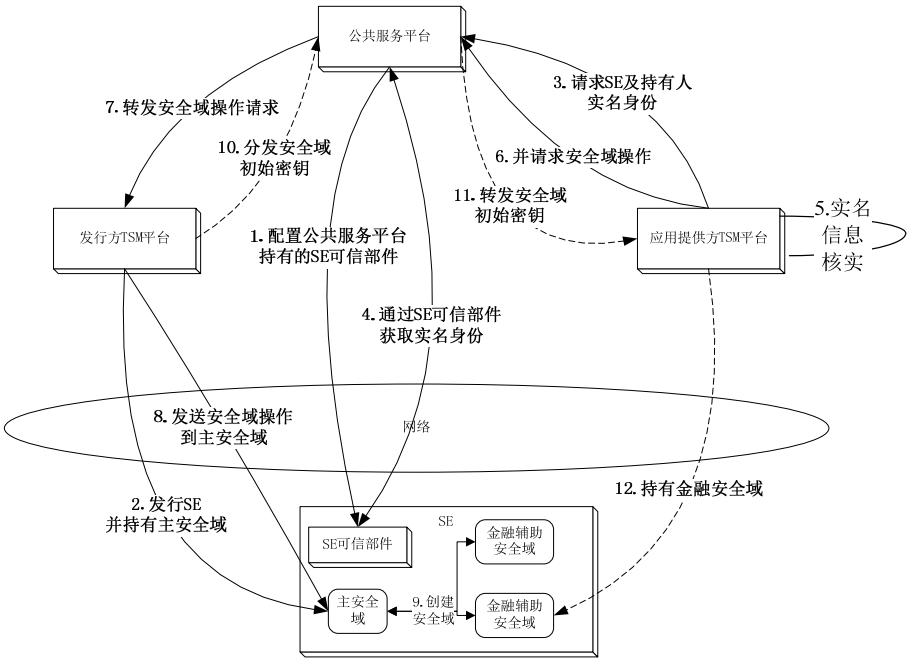

图9　发行方作为可信管理者开发共享模型—安全域操作

安全域操作中实体关系如下：

步骤 1：SE 在向用户发放前，配置由公共服务平台持有的 SE 可信部件，该部件体现为由其持有的一个安全域，仅提供实体验证服务；

步骤 2：发行方的 TSM 平台向用户发 SE，并持有主安全域(ISD)；

步骤 3：应用提供方的 TSM 平台执行安全域操作前，需要请求公共服务平台获取 SE 及持有人实名身份；

步骤 4：公共服务平台通过其持有的 SE 可信部件获取 SE 及其持有人的实名身份，并传递给应用提供方的 TSM 平台；

步骤 5：应用提供方对所获得的实名信息根据业务安全等级要求进行核实，如临柜核实或电话核实等；

步骤 6：如果身份合法，则向公共服务平台发出操作请求，操作类型包括金融类辅助安全域的创建、删除、锁定/解锁、个人化、状态查询；

步骤 7：公共服务平台转发安全域操作请求到发行方的 TSM 平台；

步骤 8：发行方的 TSM 平台分发金融类辅助安全域操作请求到主安全域；

步骤 9：主安全域执行金融类辅助安全域操作；

步骤 10：如果该操作是个人化，发行方的 TSM 平台分发初始化密钥到公共服务平台；

步骤 11：如果该操作是个人化，公共服务平台转发初始化密钥给应用提供方的 TSM 平台；

步骤 12：如果该操作是个人化，应用提供方的 TSM 平台更新密钥并持有该安全域。

应用提供方的 TSM 平台持有金融类辅助安全域后，在应用操作时，由发行方的 TSM 平台提供授权，图 10 描述了该开放共享模型下应用操作的实体关系。

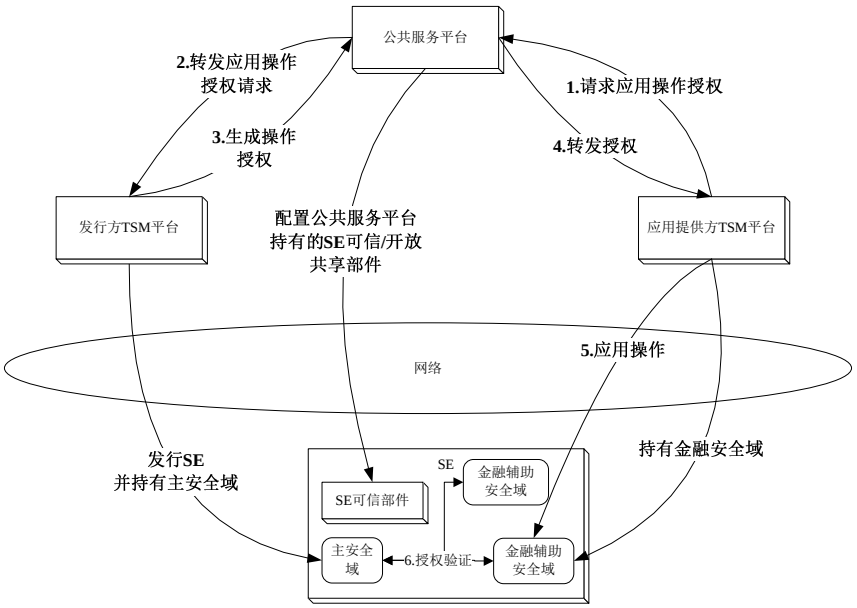

图10　发行方作为可信管理者开发共享模型—应用操作

应用操作中实体关系如下：

步骤 1：应用提供方的 TSM 平台执行应用操作前，向发行方的 TSM 平台请求应用授权，该请求通过公共服务平台转发；

步骤 2：公共服务平台转发该请求到发行方的 TSM 平台；

步骤 3：发行方的 TSM 平台生成并返回授权，具体体现为一个令牌，该授权通过公共服务平台转发；

步骤 4：公共服务平台转发该授权到应用提供方的 TSM 平台；

步骤 5：应用提供方的 TSM 平台发送应用操作到其持有的安全域；

步骤 6：SE 中由发行方的 TSM 平台持有的主安全域对操作授权进行验证，如果通过那么该操作执行；否则该操作失败。

4.6　SE 可信服务模型

SE可信服务是指公共服务平台通过其持有的SE可信部件，为移动支付的各参与方提供独立第三方的SE及其持有人身份获取、实名身份信息传递，满足参与各方获取SE及其持有人实名身份信息的需求。本标准定义了SE可信服务模型。该模型包括SE注册激活、SE实名身份获取两个环节。

在SE注册激活环节，参与实体包括检测机构、发行方、公共服务平台、具备金融账户开立资格的柜面和SE，其过程如图11所示。

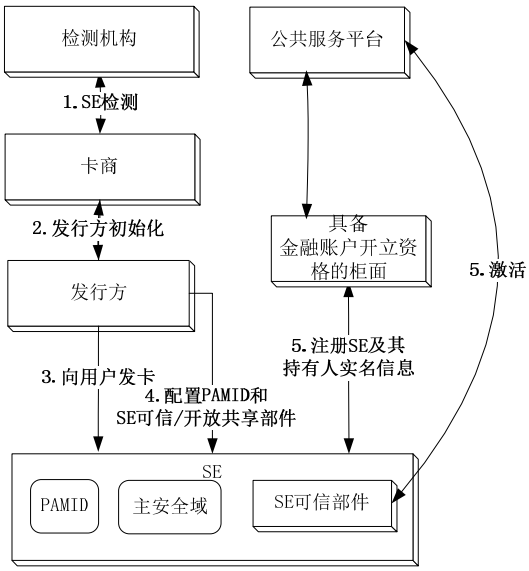

图11　可信服务模型—注册激活

SE注册激活环节实体关系如下：

步骤 1：发行方发行满足移动支付要求的 SE，接受委托的 SE 制造商向检测机构申请 SE 检测；

步骤 2：检测合规的 SE，SE 制造商根据发行方要求进行初始化，完成 SE 的制造；

步骤 3：发行方向用户发 SE；

步骤 4：SE 首次接入到金融网络中前，需要由发行方为 SE 配置 PAMID 和 SE 可信/开放共享部件。

步骤 5：配置完 PAMID 和 SE 可信/开放共享部件的 SE，由具备金融账户开立资格的柜面完成实名信息采集、审核和登记，实名信息采集和审核方式需满足根据金融业务管理规定。完成采集和审核后，注册 SE 和其持有人的实名身份，实现 SE 及其持有人的实名身份绑定；该实名身份绑定体现为在随后的激活环节，SE 可信部件中生成持有人的私钥，并存储由 CA 签发的持有人公钥证书和公共服务平台的公钥证书。如果发行方柜面同时具备金融账户开立资格，则发放 SE 和临柜面签两个步骤可以合二为一；

步骤 6：用户通过网络向公共服务平台激活该 SE。

在 SE 实名身份获取环节，参与实体包括发行方的 TSM 平台、公共服务平台、应用提供方的 TSM 平台和 SE。

图 12 描述了 SE 及其持有人实名身份获取的实体关系。

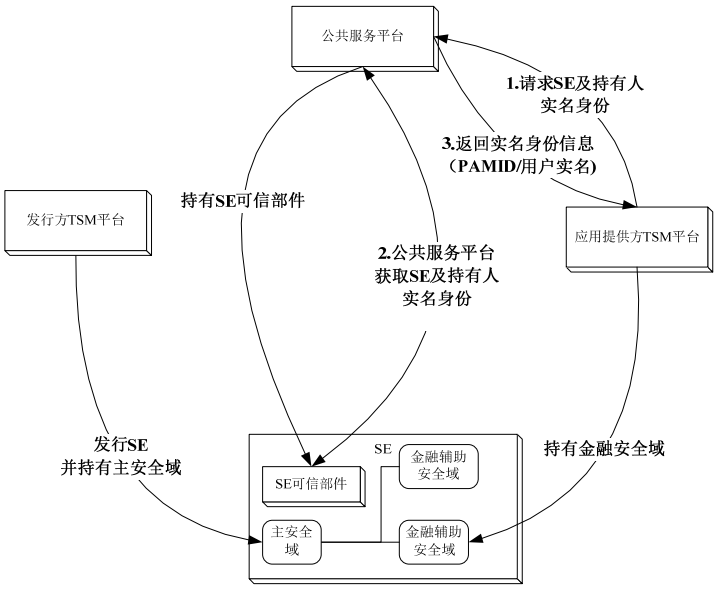

图12　可信服务模型—实名身份获取

上图描述的 SE 可信身份获取环节，实体关系如下：

步骤 1：应用提供方 TSM 平台请求 SE 及其持有人实名身份；

步骤 2：公共服务平台通过其持有的 SE 可信部件获取 SE 及持有人的实名身份，该获取过程基于 SE 可信部件和公共服务平台的公私钥加密和签名机制，所获得实名身份信息包括 SE 及其持有人的实名身份信息以及绑定关系；

步骤 3：公共服务平台返回实名身份信息，该信息包含获取结果、PAMID、以及其绑定的持有人的实名信息，应用提供方可以用该信息来核实 SE 及其持有人的合法性。

4.7　SE 可信/开放共享部件

4.7.1　概述

公共服务平台通过SE可信/开放共享部件实现SE可信和开放共享功能，SE的可信/开放共享部件由FCSD安全域、FMSD安全域，及其权限、配置的密钥等基础数据以及可提供的功能共同组成。这里的FCSD安全域、FMSD安全域都是逻辑描述，并不代表物理实现。

4.7.2　FCSD 安全域

SE可信部件由FCSD安全域提供，每个合法的SE在首次接入金融网络前，必须配置FCSD安全域。

类型：

该安全域是一个辅助安全域，但其安全域关联到自身，独立于主安全域，具备自己的安全策略。

持有方：

该安全域由公共服务平台持有。

生命周期：

该安全域的生命周期在SE首次接入到金融网络前创建，创建后将同发行方安全域一样，直接继承了卡片的生命周期，在卡片终止时终止。

权限配置：

该安全域具备安全域权限。该安全域只能由公共服务平台锁定。

配置数据：

该安全域激活时写入持有人私钥和公钥证书、公共服务平台公钥证书。

提供服务：

该安全域提供SE及其持有人实名身份存储和验证服务。

4.7.3 FMSD 安全域

SE开放共享部件由FMSD安全域提供。FMSD主要用于以公共服务平台作为可信第三方的开放共享模式中，该模式下，SE在首次接入到金融网络前，必须预先配置FMSD安全域。

类型：

该安全域是一个辅助安全域，但其安全域关联到自身，独立于主安全域，具备自己的安全策略。

持有方：

该安全域由公共服务平台持有。

生命周期：

该安全域的生命周期在SE首次接入金融网络前创建，创建后将同发行方安全域一样直接继承了卡片的生命周期，在卡片终止时终止。

权限配置：

该安全域具备安全域权限、授权管理权限、令牌验证权限、DAP权限。

配置数据：

无特别数据。

提供服务：

该安全域提供辅助安全域管理功能、令牌验证功能、DAP验证功能。

5 移动支付可信服务管理系统的实现与互联

5.1 概述

移动支付可信服务管理系统在实现方案中，根据互联方式形成了星型和网状两种不同的互联结构，其中网状互联结构可作为星型互联结构的过渡组网方案。

5.2 星型互联结构

该方案中，公共服务平台提供公共基础服务，各TSM平台接入到公共服务平台，使用公共服务平台的公共服务，形成星型互联结构。该实现方案及其互联结构图如图13所示：

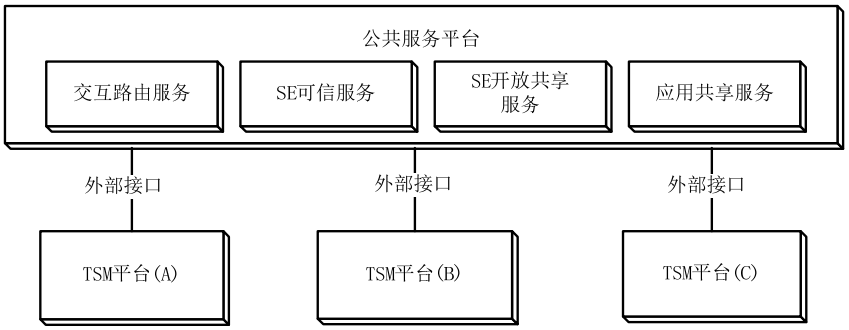

图13 星型互联结构

5.3 网状互联结构

该方案中， TSM平台可以同时与多个TSM平台互联，TSM平台之间互连形成网状，互联结构如图14所示。

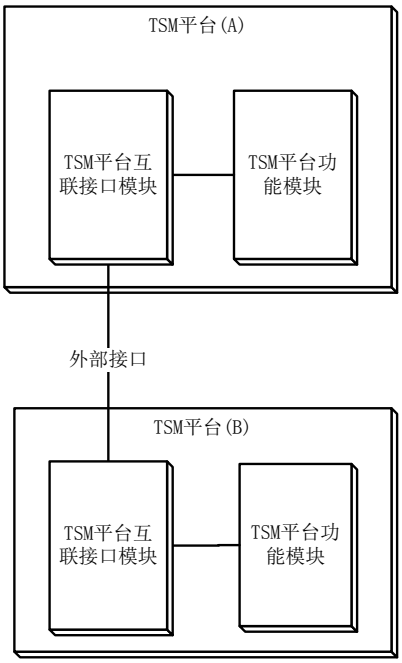

图14　网状互联结构

6　公共服务平台系统功能

6.1　公共服务平台功能概述

公共服务平台是移动支付参与各方认可的可信第三方实体，面向 TSM 平台运营方、SE 发行方、应用提供方、服务提供方和用户，提供机构注册接入、应用注册、跨机构交互路由、SE 可信、SE 开放共享功能、应用共享功能。

机构注册接入包括 TSM 平台运营方、应用提供方两类机构的注册接入。应用注册包括应用审查、PAID 分配、全局应用注册表维护。跨机构交互路由包括交互的建立、消息分发、应用资源地址分发。SE 可信管理包括 SE 的注册激活、SE 及其持有者实名身份获取和身份信息传递。SE 开放共享包括金融类辅助安全域的创建、删除、锁定解锁、个人化、终止、状态查询、安全域初始化密钥分发、应用操作授权、应用合法性验证。应用共享包括应用分发、应用发现、应用资源地址分发。

6.2　机构接入管理

机构注册接入包括TSM平台运营方、支付应用提供方两类机构的注册接入。公共服务平台根据TSM平台运营方和应用提供机构提交的注册申请信息为其分配机构 ID。注册完成后，公共服务平台允许 TSM 平台接入并提供服务，允许应用提供方提供支付应用。

TSM 平台运营机构在注册申请前，其 TSM 平台需经认可的第三方检测机构检测合格，并出具检测报告。TSM 平台运营机构的注册基本流程如图 15 所示，详细流程和管理办法另行规定。

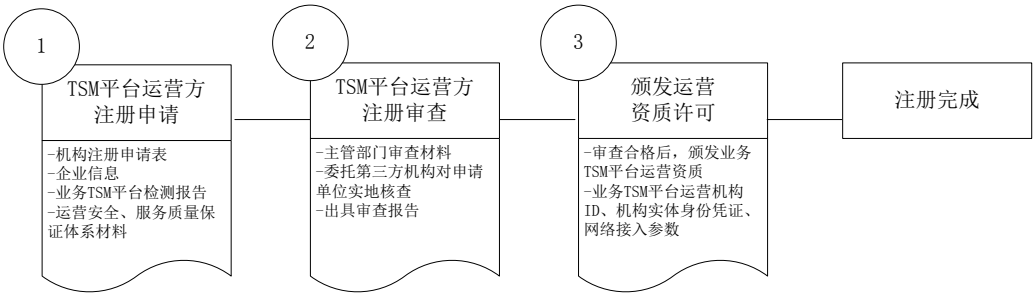

图15　TSM 平台运营机构注册流程

TSM 平台运营方的注册基本流程描述如下：

步骤 1：TSM 平台检测合格的运营方向主管机构提交运营机构注册申请，申请材料包括机构注册申请表，企业信息(如营业执照、税务登记证明)、TSM 平台检测报告、企业运营安全/服务质量保证体系材料；

步骤 2：主管部门审查材料，并委托第三方机构对申请单位实地核查，审查完成后出具审查报告；

步骤 3：对审查合格的机构，主管部门向 TSM 平台运营机构颁发运营许可证，发放机构 ID、机构实体身份凭证、网络接入参数。

应用提供方的注册基本流程如图 16 所示，详细流程和管理办法另行规定。

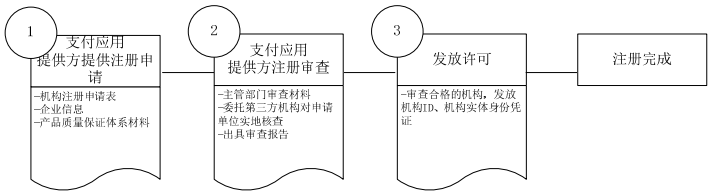

图16　支付应用发行机构注册流程

支付应用提供方的注册流程描述如下：

步骤 1：支付应用提供方向主管部门提交机构注册申请，申请材料包括机构注册申请表，企业信息(机构营业执照、税务登记证明)、产品质量保证体系材料；

步骤 2：主管部门审查材料，可委托第三方机构对申请单位实地核查，审查完成后出具审查报告；

步骤 3：对审查合格的机构，主管部门向支付应用发行机构发放机构 ID、机构实体身份凭证。

机构注册消息列表见表 1。

表1　机构注册消息列表

消息	命令功能描述	关键参数	后续操作	备注
机构注册申请	申请机构→主管部门 申请机构注册申请	注册申请表 企业信息	主管机构审核	线下流程
机构注册响应	主管部门→申请机构 返回审查结果	审查意见通知书 返回机构 ID、接入凭证、网络参数	--	线下流程

6.3　应用注册管理

6.3.1　概述

公共服务平台负责对支付应用统一分配PAID，以及应用的注册、上线发布和下架的管理，并维护所有支付应用的全局注册表。

6.3.2 PAID 分配

依据JR/T 0088.3-2012，PAID由应用提供者标识符(RID)、专有标识符、应用类型标识符、应用实现标识符、保留位构成。公共服务平台统一为各支付应用分配唯一的PAID。具备PAID的支付应用可以上线发布。

6.3.3 应用注册、上线发布

公共服务平台负责对所有支付应用进行注册、上线管理。支付应用注册前，须经认可的第三方检测机构检测合格，并出具检测报告。支付应用发行方将应用及其信息向公共服务平台提交注册申请，公共服务平台审核后，为应用分配 PAID，获得 PAID 的应用可以通过 TSM 平台上线发布。流程如图 17 所示。

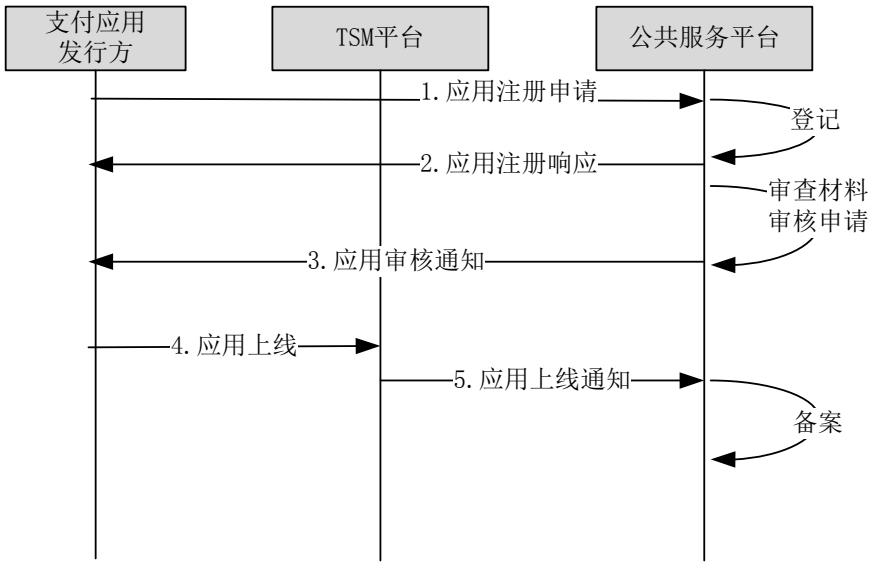

图17 应用注册、上线发布流程

应用注册、上线发布流程如下：

步骤 1：支付应用提供方向公共服务平台提交支付应用注册申请，提交的材料包括应用注册申请表，应用检测报告等；

步骤 2：公共服务平台登记申请材料，返回收到确认；

步骤 3：公共服务平台审查材料，生成正式的意见通知书，审查合格的应用分配 PAID，并登记备案；具备 PAID 的支付应用可以上线发布；

步骤 4，5：应用提供方将获得 PAID 的应用提供给 TSM 平台，由具备接入资质的 TSM 平台上线发布，TSM 平台需要通知公共服务平台应用上线。

应用注册、上线消息列表见表 2。

表2 应用注册、上线消息列表

消息	命令功能描述	关键参数	备注
应用注册申请	支付应用提供方→公共服	应用名、应用类型、应用版本、	公共服务平台管理功能

消息	命令功能描述	关键参数	备注
	务平台 申请应用注册	应用功能说明、应用提供方机构 ID、注册时间(自动生成)、应用检测报告、期望发布范围、期望有效期	参见 8.7.2
应用注册响应	公共服务平台→支付应用提供方返回收到确认	应用编号(自动生成)，收到确认	公共服务平台管理功能 参见 8.7.2
应用注册通知	公共服务平台→支付应用提供方 向支付应用提供方返回审查通知	审查意见通知书、应用编号、应用名、应用 PAID、应用安全等级、应用发布范围、应用有效期、应用生命周期状态	公共服务平台管理功能 参见 8.7.3
应用上线通知	TSM 平台→公共服务平台 应用上线通知	应用 PAID、TSM 平台机构 ID，上线时间	参见 8.8.2

6.3.4 应用的下架

对已经上线的应用，应用提供方、TSM 平台或公共服务平台可以申请下架，下架操作由 TSM 平台执行，并通知公共服务平台，公共服务平台进行备案。下架后，支付应用不能再被用户查询和下载。

应用的下架流程如图 18 所示：

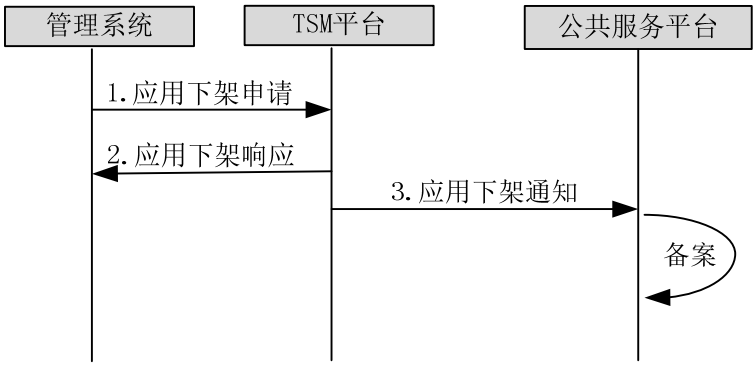

图18 应用下架流程

应用下架流程描述如下：

步骤 1：TSM 平台收到应用下架申请，该申请包括下架原因说明；

步骤 2：TSM 平台审核应用下架申请后执行下架动作，返回操作响应；

步骤 3：TSM 平台向公共服务平台发出应用下架通知，公共服务平台对应用下架进行备案。

应用下架消息列表见表 3。

表3 应用下架消息列表

消息	命令功能描述	关键参数	后续操作	备注
应用下架申请	申请机构→TSM 平台 申请应用下架	应用 PAID，申请机构 ID，下架原因说明，下架申请时间(自动生成)	执行下架操作，更新应用生命周期状态，返回下架响应	TSM 平台自行定义
应用下架响应	TSM 平台→申请机构	应用 PAID，是否下架，下架时间	生成下架通知，提交给	TSM 平台

消息	命令功能描述	关键参数	后续操作	备注
	下架操作结果	(自动生成)	公共服务平台	自行定义
应用下架通知	TSM 平台→公共服务平台通知公共服务平台应用已下架	应用 PAID，申请机构 ID，下架时间(自动生成)	标注已下架	参见 8.8.2

6.3.5 应用注册表

公共服务平台维护一张全局应用注册表，该注册表登记了上线的所有应用的基本信息。

应用注册表信息须包括如下内容：应用 PAID、应用类型、应用版本、应用功能说明、应用占有空间、应用权限、应用提供机构代码、负责应用发行的 TSM 平台机构代码、应用的安全等级、应用发布范围、应用有效期、应用生命周期状态。

应用的注册信息在TSM平台向公共服务平台进行上线备案时登记到应用注册表中。

6.4 SE 可信服务

6.4.1 概述

SE可信服务是指公共服务平台通过其持有的SE可信部件，为移动支付的各参与方提供独立第三方的SE及其持有人身份获取、实名身份传递，满足参与各方获取SE及其持有人实名身份的需求。SE可信服务包括SE在金融网络的注册与激活、SE实名身份获取与传递两个环节。

6.4.2 SE 的注册与激活

SE制卡、用户发放、金融网络的注册激活完整流程如下：

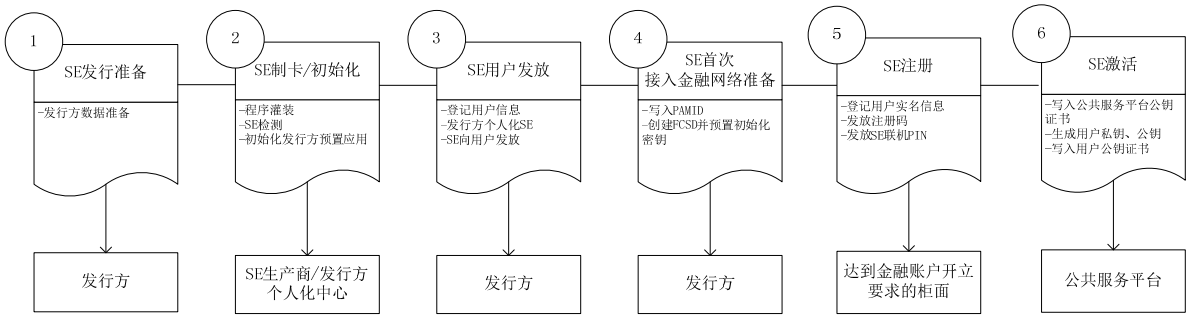

图19 SE 注册激活基本流程

步骤1：SE发行准备，发行方准备数据，并委托卡生产商制卡；

步骤2：SE制卡/初始化，接受委托的SE制造商完成SE程序灌装，然后提交认可的检测机构进行检测，检测通过的SE初始化发行方预置应用，完成制卡；

步骤3：SE用户发放，发行方登记用户信息，完成SE个人化，发放给用户；

步骤4：SE首次接入金融网络准备，SE在金融网络注册激活前必须由发行方配置PAMID和FCSD辅助安全域。PAMID是SE具有的金融网络中的唯一标识，FCSD辅助安全域用于用于保证SE和其持有人的实名身份绑定关系。

步骤5：SE注册，SE与其持有人实名身份在金融网络中的注册操作必须在满足金融账户面签要求的柜面实施，并由公共服务平台完成。包括登记SE及其持有人身份登记、验证码发放和SE联机PIN码发放。

步骤6：SE激活，SE与其持有人实名身份在金融网络中的激活由用户主动完成，激活后SE将生成用户私钥，并写入用户公钥证书和公共服务平台公钥证书。

SE在接入金融网络前应由发行方写入PAMID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。流程如图20所示：

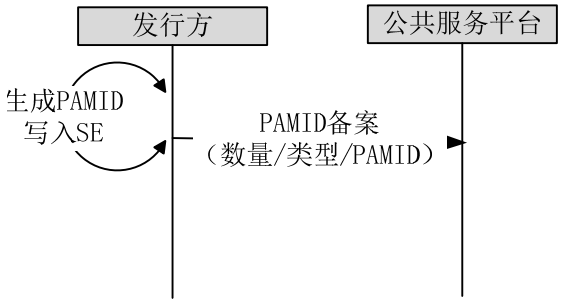

图20　PAMID 备案流程

FCSD辅助安全域存储SE持有人的私钥、公钥证书和公共服务平台公钥证书，用于保证SE和其持有人的实名信息之间的绑定关系。该安全域在SE在首次接入金融网络前由发行方创建并写入初始化密钥。配置了FCSD安全域的SE由具备金融账户开立资格的柜面进行实名信息采集、审核和注册，并由用户激活，激活后FCSD安全域不允许被主安全域锁定和删除。FCSD安全域的初始化密钥采用两级分散体系，如图21所示，密钥分散算法和分散因子参见第9章。

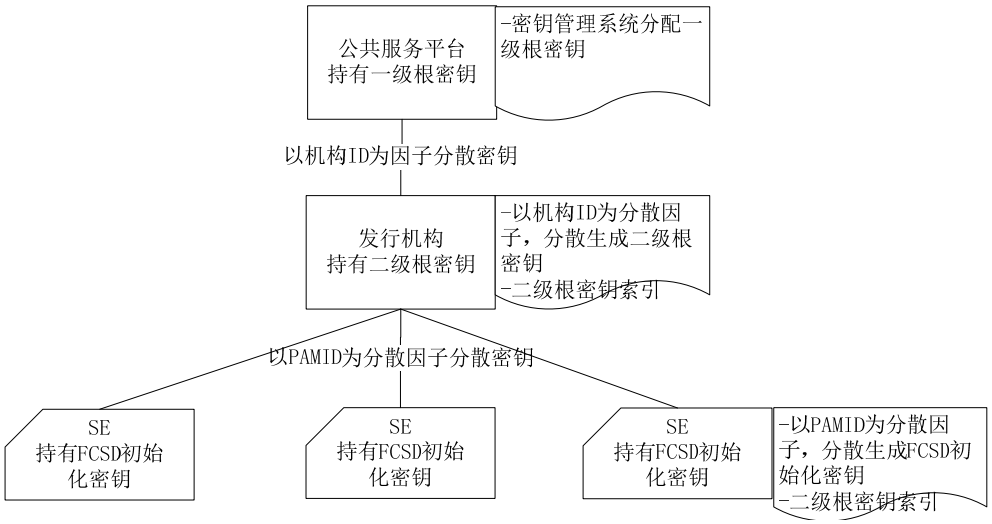

图21　FCSD 安全域初始化密钥分散体系

配置了PAMID和FCSD安全域的SE，由满足金融账户开立资格的柜面采集、审核并登记持有人的实名信息和PAMID，同时发放用户验证码。用户使用验证码，向公共服务平台申请SE激活，该过程利用SE中FCSD安全域的初始化密钥打开该安全域，在FCSD安全域中生成用户的公私钥对，使用公钥和用户实名信息构造公钥证书，并下发到FCSD安全域中。

SE注册激活流程如图22所示，在注册与激活前，需要在FCSD中配置初始化密钥以及对应的二级根密钥索引。

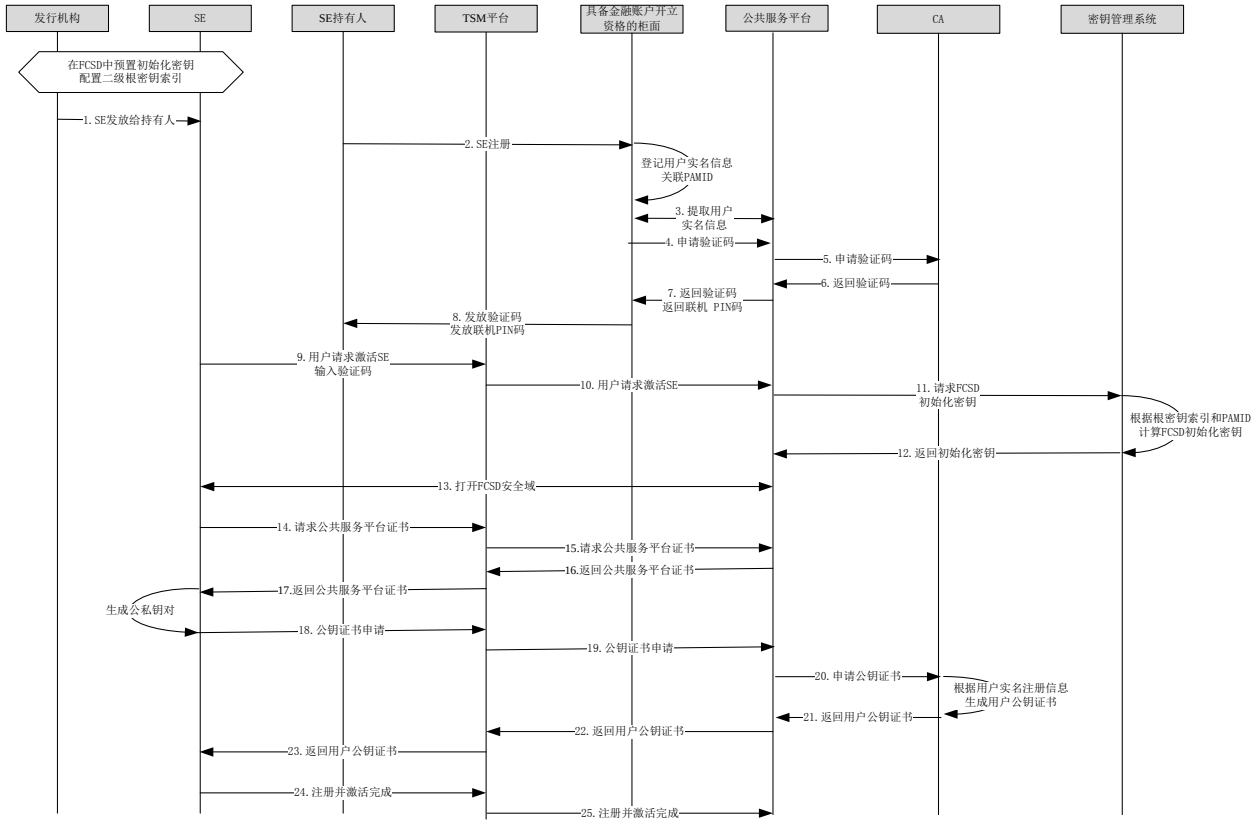

图22　SE 注册激活流程

SE注册激活的流程描述如下：

步骤1：发行方将SE发放给持有人，该过程是一个线下过程；

步骤2：SE持有人首次办理金融应用时，持有人由具备金融账号开立资格的个人化柜面采集、审核并登记实名信息，完成SE注册流程；该个人化柜面所登记信息和PAMID关联；

步骤3：个人化柜面操作人员将步骤2中登记的实名信息提取到柜面上的公共服务平台注册网关中；

步骤4、步骤5：个人化柜面操作人员使用柜面上的公共服务平台注册网关，向公共服务平台发起验证码申请，该申请中带有SE持有人的实名信息；公共服务平台转发该申请请求到CA系统；

步骤6：CA返回验证码到公共服务平台；

步骤7：公共服务平台生成联机PIN，将验证码、联机PIN一起返回给个人化柜面；

步骤8：个人化柜面操作人员离线发放验证码和联机PIN码；

步骤9、步骤10：用户发起SE激活请求，该请求包括用户输入的验证码，PAMID、SE存储的二级根密钥索引；该请求由SE相连的TSM平台中转到公共服务平台；

步骤11：公共服务平台向密钥管理系统发起FCSD初始化密钥申请，密钥管理系统根据PAMID和二级根密钥索引，计算出FCSD安全域的初始化密钥；

步骤12：密钥管理系统返回SE中FCSD的初始化密钥到公共服务平台；

步骤13：公共服务平台使用得到的SE中的FCSD初始化密钥，与SE的FCSD安全域建立安全通道，打开FCSD安全域；该步骤包括一系列消息交互，均通过SE相连的TSM平台中转。

步骤14、步骤15：SE请求公共服务平台公钥证书，该请求通过SE相连的TSM平台中转；

步骤16、步骤17：公共服务平台返回公共服务平台公钥证书，该消息通过SE相连的TSM平台中转到SE，并写入到SE的FCSD安全域中；

步骤18、步骤19：SE生成公私钥对，向公共服务平台发起持有人公钥证书申请，申请中包含SE生成的公钥，该申请通过SE相连的TSM平台中转；

步骤20：公共服务平台收到持有人公钥证书申请后，向CA系统请求公钥证书；

步骤21：CA系统收到请求后，根据持有人的实名信息、公钥、SE安全等级等信息，构造SE和持有人公钥证书，返回用户公钥证书到公共服务平台；

步骤22、步骤23：公共服务平台返回SE及持有人公钥证书，写入到SE的FCSD安全域中，该消息通过SE相连的TSM平台中转；

步骤24、步骤25：SE向公共服务平台返回注册并激活完成消息，该消息通过SE相连的TSM平台中转。

SE注册激活的消息列表见表4。

表4　SE 注册激活消息列表

消息	命令功能描述	关键参数	后续操作	备注
SE 分发	发行方→SE 持有人	--		线下流程
SE 注册	SE 持有人→满足移动支付安全要求的面签柜面	PAMID	登记用户实名信息、关联 PAMID	线下流程
用户实名信息申请	公共服务平台→面签柜面所属发行方	PAMID、面签柜面所属发行方机构 ID		参见 8.8.14
用户实名信息响应	面签柜面所属发行方→公共服务平台	PAMID、面签柜面所属发行方机构 ID、用户实名、身份证号、		参见 8.8.14
验证码申请请求	公共服务平台→CA 系统	PAMID、面签柜面所属发行方机构 ID、用户实名、身份证号	CA 构造唯一验证码	参见 8.5.1.1
验证码申请响应	CA 系统→公共服务平台	PAMID、验证码、联机 PIN 码	将验证码发送给公共服务平台	参见 8.5.1.1
发放验证码	公共服务平台→SE 持有人	验证码、联机 PIN 码	用户激活	线下流程
激活 SE 请求	SE→TSM 平台	PAMID、验证码、根密钥索引		参见 8.9.1
激活 SE 请求	TSM 平台→公共服务平台	PAMID、验证码、根密钥索引		参见 8.8.17
FCSD 初始化密钥请求	公共服务平台→密钥管理系统	PAMID、根密钥索引		参见 8.6
FCSD 初始化密钥响应	密钥管理系统→公共服务平台	PAMID、FCSD 初始化密钥	将 FCSD 初始化密钥透传给公共服务平台	参见 8.6
FCSD 鉴权	公共服务平台←→TSM 平台	PAMID、FCSD 初始化密钥		参见 8.8.17
FCSD 鉴权	TSM 平台←→SE	PAMID、FCSD 初始化密钥	建立 FCSD 安全通道	参见 8.9.1
请求公共服务平台公钥证书	SE→TSM 平台	PAMID		参见 8.9.1
请求公共服务平台公钥证书	TSM 平台→公共服务平台	PAMID		参见 8.8.17
写入公共服务平台公钥证书	公共服务平台→TSM 平台	公共服务平台公钥证书		参见 8.8.17
写入公共服务平台公钥证书	TSM 平台→SE	公共服务平台公钥证书	SE 内部生成公私钥对	参见 7.9.1

消息	命令功能描述	关键参数	后续操作	备注
公钥证书申请请求	SE→TSM 平台	PAMID、验证码、PKCS#10 请求		参见 8.9.1
公钥证书申请请求	TSM 平台→公共服务平台	PAMID、验证码、PKCS#10 请求		参见 8.8.17
申请公钥证书	公共服务平台→CA 系统	PAMID、验证码、SE 安全等级、PKCS#10 请求	CA 系统产生公钥证书	参见 8.5.1.2
返回公钥证书	CA 系统→公共服务平台	持有人公钥证书	准备写入公钥证书	参见 8.5.1.2
写入公钥证书	公共服务平台→TSM 平台	持有人公钥证书		参见 8.8.17
写入公钥证书	TSM 平台→SE	持有人公钥证书	SE 激活完成	参见 8.9.1
用户激活完成通知	SE→TSM 平台	PAMID		参见 8.9.1
用户激活完成通知	TSM 平台→公共服务平台	PAMID	更新 SE 状态为激活	参见 8.8.17

6.4.3 SE 及持有人的实名身份获取与传递

在需要获得SE及其持有人的实名身份时，应用提供方可以请求公共服务平台对SE进行实名身份获取，实名身份获取验证包括基于非对称密钥体系的实体验证、会话密钥协商和实名身份传递三个过程，具体如图23所示：

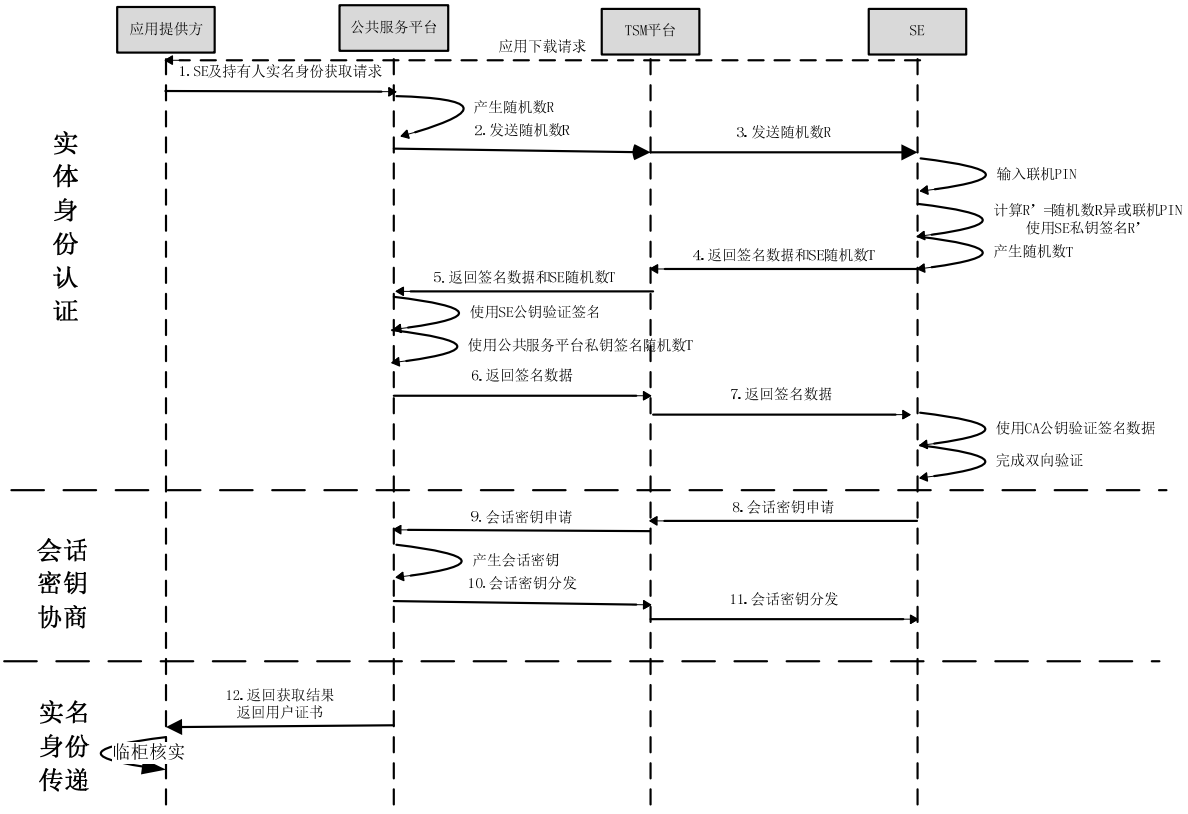

图23　可信身份验证流程

实名身份获取的流程如下：

步骤1：应用提供方发出SE及持有人实名身份获取请求；

步骤2、步骤3：公共服务平台产生随机数R，并发送该随机数给SE，该消息通过SE相连的TSM平台转发；

步骤4、步骤5：请求用户输入联机PIN码，计算R'=R异或联机PIN码，然后使用SE私钥签名随机数R'，同时产生随机数T，然后将签名数据和随机数T返回，该消息通过SE相连的TSM平台转发；

步骤6、步骤7：公共服务平台用SE公钥验证签名，然后使用公共服务平台私钥签名随机数T，向SE发送签名，该请求通过SE相连的TSM平台转发；SE使用配置的公共服务平台公钥验证签名，如果通过，完成了双向实体验证；

步骤8、步骤9：SE发起会话密钥申请消息，该消息通过SE相连的TSM平台转发；

步骤10、步骤11：公共服务平台下发会话密钥到SE；

步骤12：公共服务平台返回实体验证结果和用户公钥证书给应用提供方，这两项标明了用户的实名身份，应用提供方可根据业务需求，对获得的信息进行核实，如临柜核实、电话核实等。

安全SE可信身份验证通过启动SCP10安全通道会话来实现，设置SCP10方式的安全通道所支持的密钥和签名类型参数"i"为'02'，即采用传送密钥(transport key)和无需恢复加密数据的证书(signature without recovery)方式。会话密钥由公共服务平台生成16字节的密钥，通过Perform Security Operation[decipher]命令将密钥传送至FCSD安全域。流程如图24所示：

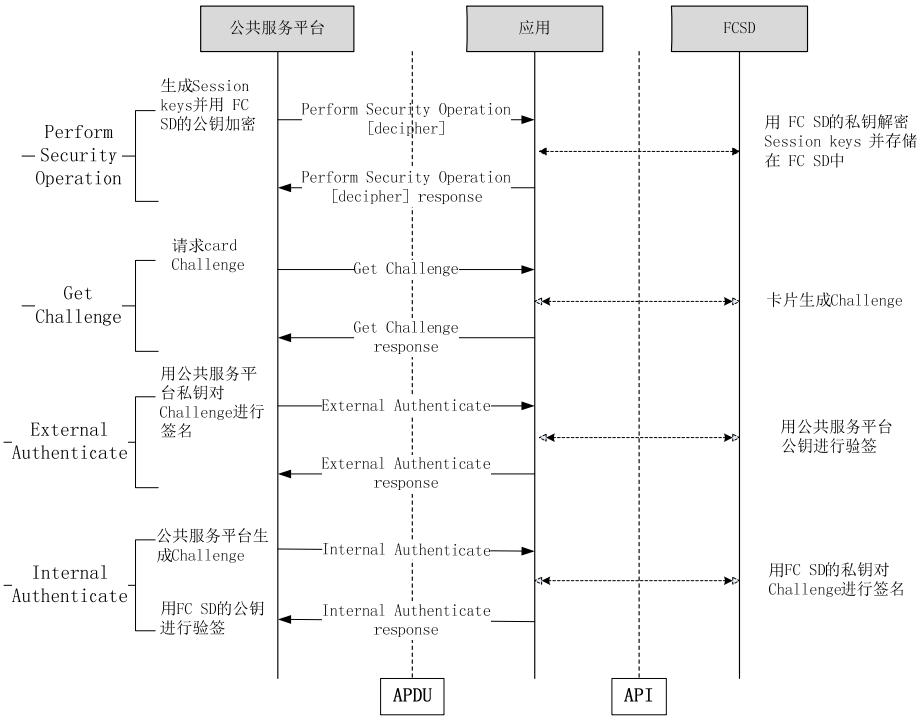

图24　使用 SCP10 安全通道会话流程实现可信身份验证

SE可信身份验证消息列表见表5。

表5　SE 可信身份验证消息列表

消息	命令功能描述	关键参数	后续操作	备注

消息	命令功能描述	关键参数	后续操作	备注
应用下载请求	SE→TSM 平台	PAMID、PAID		参见 8.9.4
SE/持有人实名身份获取请求	TSM 平台→公共服务平台	PAMID、TSM 平台机构 ID		参见 8.8.16
SE/持有人实名身份获取请求	公共服务平台→TSM 平台	PAMID、随机数 R		参见 8.8.16
SE/持有人实名身份获取请求	TSM 平台→SE	PAMID、随机数 R	计算 R'=R 异或联机 PIN 码，使用 SE 私钥对 R'签名；生成随机数 T； 构造 SE 认证响应	参见 8.9.4
SE 认证响应	SE →TSM 平台	PAMID、R'的私钥签名、SE 公钥证书，随机数 T		参见 8.9.4
SE 认证响应	TSM 平台→公共服务平台	PAMID、R'的私钥签名、SE 公钥证书，随机数 T	验证 SE 公钥证书 用 SE 公钥验证 R'的签名 用公共服务平台私钥对 T 签名	参见 8.8.16
SE 认证确认	公共服务平台→TSM 平台	PAMID、随机数 T 私钥签名		参见 8.8.16
SE 认证确认	TSM 平台→ SE	PAMID、随机数 T 私钥签名	用公共服务平台公钥验证随机数 T 的签名	参见 8.9.4
会话密钥请求	SE → TSM 平台	PAMID		参见 8.9.4
会话密钥请求	TSM 平台→公共服务平台	PAMID		参见 8.8.16
会话密钥响应	公共服务平台→ TSM 平台	PAMID、会话密钥		参见 8.8.16
会话密钥响应	TSM 平台→SE	PAMID、会话密钥	用私钥解密得到会话密钥	参见 8.9.4
公钥证书通告	公共服务平台→TSM 平台	PAMID、公钥证书		参见 8.8.5

6.5 金融类辅助安全域管理

6.5.1 概述

以公共服务平台作为可信第三方的开放共享模式下，要求 SE 中配置 FMSD 安全域。公共服务平台通过 FMSD 安全域为支付应用提供方进行金融类辅助安全域的生命周期管理，包括辅助安全域的创建、删除、个人化、锁定/解锁。创建的金融类辅助安全域采用委托管理模式。

6.5.2 安全域创建

在以公共服务平台作为可信第三方的开发共享模式下，金融类辅助安全域的创建由FMSD安全域负责。初始密钥由公共服务平台或应用提供方产生和分配，TSM平台可以通过空中方式更新其初始密钥。

安全域创建流程如图25所示，在安全域创建前，需要通过SE可信服务流程获取SE及持有人实名身份，并根据业务安全要求进行再次核实，如临柜核实或电话核实等：

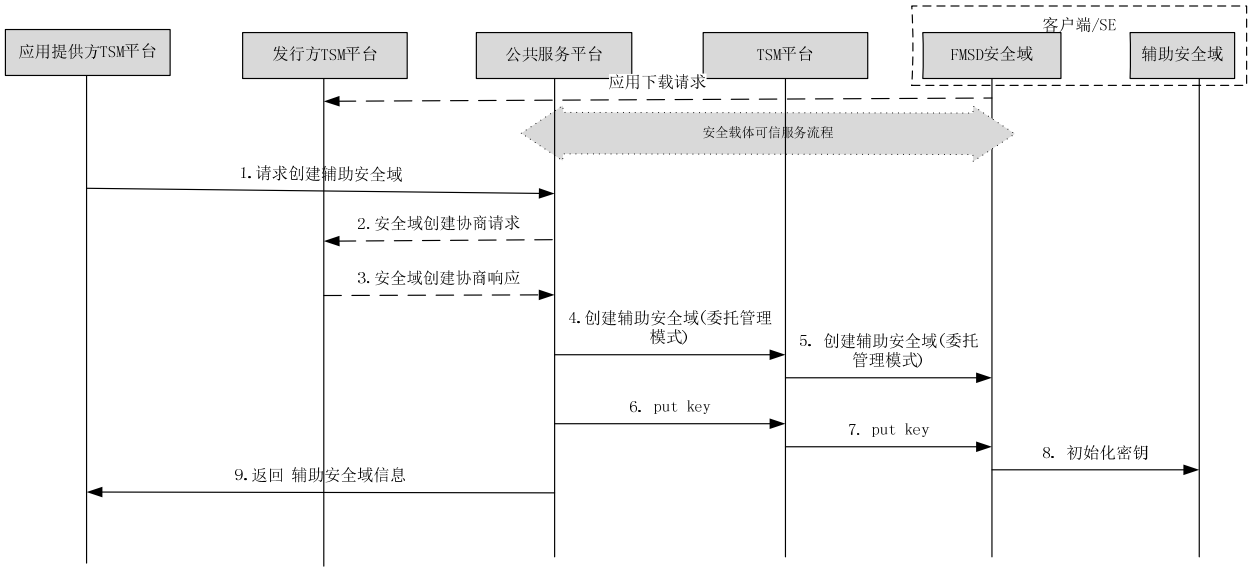

图25　金融类辅助安全域创建

以公共服务平台作为可信第三方的开放共享模式下，金融类辅助安全域创建流程如下：

步骤 1：应用提供方的 TSM 平台向公共服务平台请求创建辅助安全域；

步骤 2：该步骤可选，公共服务平台向发行方的 TSM 平台发起创建辅助安全域的协商请求；

步骤 3：该步骤可选，发行方的 TSM 平台返回创建协商响应；

步骤 4、步骤 5：公共服务平台通过其持有的 FMSD 安全域创建辅助安全域，采用委托管理模式，该命令通过 SE 相连的 TSM 平台中转；

步骤 6、步骤 7：创建成功后，公共服务平台向 FMSD 安全域发起初始化密钥命令，该命令通过 SE 相连的 TSM 平台中转；

步骤 8：FMSD 安全域将初始密钥推送到创建的辅助安全域中；

步骤 9：公共服务平台向应用提供方的 TSM 平台返回所创建安全域的信息，包括安全域 PAID、初始化密钥。

金融类辅助安全域创建的消息列表见表 6。

表6　金融类辅助安全域创建消息列表

消息	命令功能描述	关键参数	后续操作	备注
应用下载请求	SE→TSM 平台	PAMID、PAID		参见 8.9.4
请求创建辅助安全域	应用提供方的 TSM 平台→公共服务平台	PAMID、申请机构 ID	创建申请备案	参见 8.8.10
安全域创建协商请求	公共服务平台→发行方的 TSM 平台	PAMID、申请空间	发行方备案， 查看空间使用情况	参见 8.8.11
安全域创建协商响应	发行方的 TSM 平台→公共服务平台	协商结果		参见 8.8.11
创建辅助安全域请求	公共服务平台→TSM 平台			参见 8.8.10
创建辅助安全域请求	TSM 平台→SE(FMSD 安全域)	PAMID、辅助安全域 PAID、创建脚本		参见 8.9.4

消息	命令功能描述	关键参数	后续操作	备注
设置初始密钥	公共服务平台→TSM 平台	PAMID、辅助安全域 PAID、初始密钥		参见 8.8.10
设置初始密钥	TMS 平台→ SE(FMSD 安全域)	PAMID、辅助安全域 PAID、初始密钥		参见 8.9.4
设置初始密钥	FMSD 安全域→ 辅助安全域	辅助安全域 PAID、初始密钥	为新创建的辅助安全域设置初始密钥	卡内部接口
提供辅助安全域信息	公共服务平台→应用提供方的 TSM 平台	辅助安全域 PAID、初始化密钥		参见 8.8.6

6.5.3 安全域删除

在金融类辅助安全域的删除前，如果该安全域中有相关联的应用，则应与关联应用的应用提供方进行协商。没有相关联的应用的安全域才可被删除。

在以公共服务平台作为可信第三方的开放共享模式下，金融类辅助安全域删除由FMSD安全域负责。流程如图26所示：

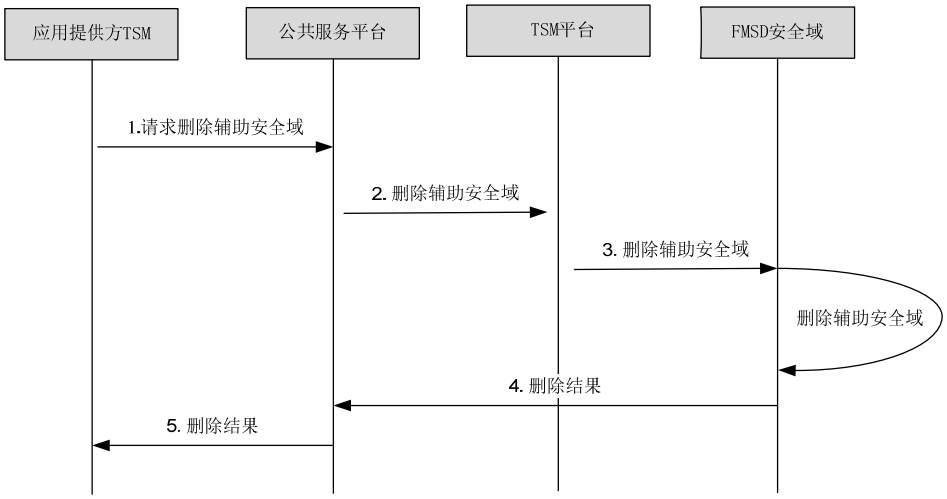

图26 金融类辅助安全域删除

在以公共服务平台作为可信第三方的开放共享模式下，安全域删除流程如下：

步骤 1：安全域持有者通过平台管理系统向公共服务平台发起删除辅助安全域请求；

步骤 2、步骤 3：公共服务平台向其持有的 FMSD 安全域发出删除操作命令，该命令通过 SE 相连的 TSM 平台中转；FMSD 安全域删除所请求的辅助安全域；

步骤 4：返回删除结果给安全域持有者。

金融类辅助安全域删除的消息列表见表 7。

表7 金融类辅助安全域删除消息列表

消息	命令功能描述	关键参数	后续操作	备注
删除辅助安全域请求	应用提供方的 TSM 平台→公共服务平台	PAMID、辅助安全域 PAID		参见 8.8.12
删除辅助安全域请求	公共服务平台→TSM 平台	PAMID、辅助安全域 PAID、删除脚本		参见 8.8.12

消息	命令功能描述	关键参数	后续操作	备注
删除辅助安全域请求	TSM 平台→SE(FMSD 安全域)	PAMID、辅助安全域 PAID、删除脚本	删除 FMSD 安全域下的辅助安全域	参见 8.9.6
通知应用提供方的 TSM 平台	公共服务平台→应用提供方的 TSM 平台	辅助安全域 PAID、删除结果		参见 8.8.13

6.5.4 安全域的锁定/解锁

如果发现卡片存在威胁且与特定的安全域相关，则可将该安全域状态设置为锁定状态。处于锁定状态的安全域，其相关安全域和应用将无法被操作。安全域锁定的需求来源主要是因为商业或安全的原因，决定将卡片上的特定安全域进行锁定。安全域锁定后其相关联的应用则不可用。

安全域锁定后只可由 FMSD 安全域对其进行解锁，恢复到锁定前的状态。

在以公共服务平台作为可信第三方的开发共享模式下安全域锁定/解锁由FMSD安全域负责。流程如图27所示：

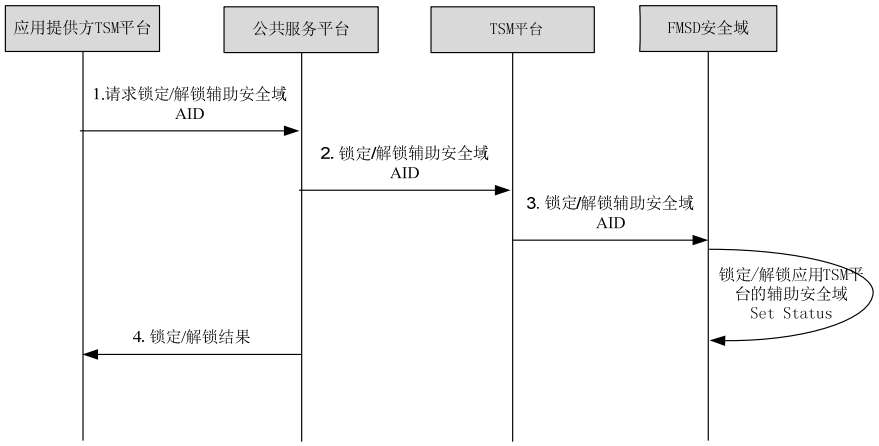

图27 辅助安全域的锁定/解锁

在以公共服务平台作为可信第三方的开放共享模式下，安全域锁定/解锁流程如下：

步骤 1：安全域持有方通过平台管理系统向公共服务平台发起锁定/解锁辅助安全域的请求；

步骤 2、步骤 3：公共服务平台向其持有的 FMSD 安全域发出锁定/解锁操作命令，该命令通过 SE 相连的 TSM 平台中转；FMSD 安全域执行锁定/解锁操作；

步骤 4：公共服务平台向请求 TSM 平台返回结果。

辅助安全域锁定/解锁消息列表见表 8。

表8 辅助安全域锁定/解锁消息列表

消息	命令功能描述	关键参数	后续操作	备注
请求锁定、解锁辅助安全域	应用提供方的 TSM 平台→公共服务平台	PAMID、辅助安全域 PAID		参见 8.8.12
锁定、解锁辅助安全域请求	公共服务平台→TSM 平台	PAMID、辅助安全域 PAID、操作脚本		参见 8.8.12
锁定、解锁辅助安全域请求	TSM 平台→FMSD 安全域	PAMID、辅助安全域 PAID、操作脚本	锁定、解锁 FMSD 安全域下的辅助安全域	参见 8.9.6

消息	命令功能描述	关键参数	后续操作	备注
通知应用提供方的 TSM 平台	公共服务平台→应用提供方的 TSM 平台	辅助安全域 PAID、操作结果		参见 8.8.13

6.6 金融类辅助安全域中应用授权

金融类辅助安全域采用委托管理模式，对其所属应用进行操作时需要 FMSD 安全域签发的委托令牌，并在卡片端对委托令牌进行验证，验证通过后才可进行后续操作。

委托管理模式支持的应用操作有：

——应用加载

——应用安装

——应用迁移

委托令牌签发验证流程如图28所示：

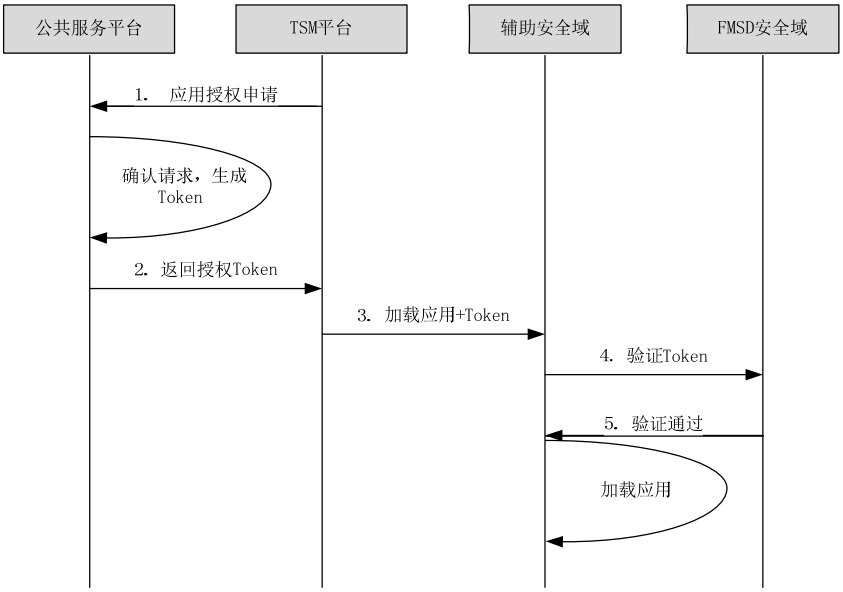

图28 应用授权流程

在以公共服务平台作为可信第三方的开放共享模式下委托 Token 签发、验证流程如下：

步骤 1：TSM 平台向公共服务平台发送下载应用的授权请求，同时附带应用的 Hash；公共服务平台确认请求后，生成授权 Token；

步骤 2：公共服务平台返回授权 Token 给 TSM 平台；

步骤 3：TSM 平台将应用和 Token 加载到其辅助安全域中；

步骤 4：采用委托管理模式的辅助安全域将加载 Token 发送到 FMSD 安全域请求 Token 验证；

步骤 5：FMSD 安全域对加载 Token 进行验证，通过后发送通知给辅助安全域；Token 验证通过后，进行应用加载操作。

应用授权消息列表见表 9。

表9 应用授权消息列表

消息	命令功能描述	关键参数	后续操作	备注
应用授权申请	应用提供方的 TSM 平台→	PAMID、PAID、机构 ID、Install For	公共服务平台生成	参见 8.8.7

消息	命令功能描述	关键参数	后续操作	备注
	公共服务平台 申请应用的授权	Load Hash 值、Install For Install hash 值	Token	
返回授权响应	公共服务平台→应用提供方的 TSM 平台	PAMID、PAID、Install For Load Token、Install For Install Token		参见 8.8.7

6.7 应用跨机构联网分发的安全审计

应用跨机构联网分发，是指非发行方的TSM平台上的应用，通过跨机构流程下载到SE上的过程。在该流程中，公共服务平台需要进行安全审计。规则要求如下：

——公共服务平台需要审查交互的TSM平台双方是否是已注册的合法机构。

——公共服务平台需要审查待下载应用和SE的安全等级的匹配性，不允许高安全等级的应用下载到低安全等级的SE上，同时需要根据SE安全等级和当期业务风险控制安装应用的数量。

——安全域作为一种特殊的应用，在安全域的创建时，需要审查请求创建安全域的应用提供方与SE安全等级的匹配性，同时需要根据SE安全等级和当期业务风险控制安全域数量。

6.8 和转接清算系统数据同步

公共服务平台需要和转接清算平台进行数据同步，同步内容包括注册机构ID信息。数据同步使用文件同步机制。

7 TSM 平台功能

7.1 TSM 平台功能概述

TSM 平台面向 SE 发行方、服务提供方，通过使用公共服务平台提供的基础服务，实现 SE 的注册发行，安全域的创建，业务应用的下载、个人化等流程。

SE 的发行商通过 TSM 平台，对发行的 SE 提供完整的生命周期管理。TSM 平台根据需要在 SE 上创建辅助安全域，通过建立安全通道，将应用提供方提供的业务应用安全的下载到预先创建好的辅助安全域中。

TSM 平台的主要功能有：提供 SE 的生命周期管理，包括 SE 的个人化（注册），SE 的锁定解锁与废止，以及 SE 的状态查询等功能；提供 SE 上辅助安全域的生命周期管理，提供辅助安全域的创建，辅助安全域的锁定解锁，辅助安全域的删除和辅助安全域的密钥更新等功能；提供业务应用的数据准备，应用下载，应用的锁定解锁，应用的删除等功能。

TSM 平台需要支持不同形态的安全载体：包括 SIM 卡， SD 卡，嵌入式安全单元等。

7.2 SE 的生命周期管理

7.2.1 SE 的个人化与注册

SE的个人化与注册包括发行方实施的个人化操作，以及由具备金融账户开立资格的柜面实施的个人化。

本标准规定，SE与其持有人实名身份绑定的个人化操作必须由具备金融账户开立资格柜面实施，个人化方式需满足金融业务管理规定。该操作应基于FCSD安全域，配合公共服务平台、CA系统一同实现，相关流程参见6.4.2。发行方实施的个人化操作由发行方定义，本标准不做强制约束。在实现层面，如果发行方同时也是满足金融账户开立面签要求的柜面机构，则两个个人化可以一并完成。

7.2.2 SE 的合法性检查

在SE创建承载联网通用支付应用的辅助安全域之前，本标准规定必须通过公共服务平台对SE进行合法性检查，流程参见6.4.3。

7.2.3 SE 的终止

发行方或公共服务平台都可以发起 SE 的终止请求，该请求由发行方 TSM 平台实施。SE 的终止包括两种：整卡终止和金融 SE 的终止。SE 整卡终止将禁止 SE 上的所有应用，金融 SE 的终止将只禁止金融类辅助安全域和支付应用。这两种 SE 的终止均由发行方 TSM 平台实施。

在SE处于任何状态，发行方TSM平台都可以执行终止操作。发行方TSM平台要保证在SE终止前，所有SE上的应用正常终止。发行方TSM平台终止SE后，必须通知公共服务平台进行备案，公共服务平台注销该SE，随后将SE终止状态通知给SE上所有安全域各自所属的TSM平台，流程如图29所示。

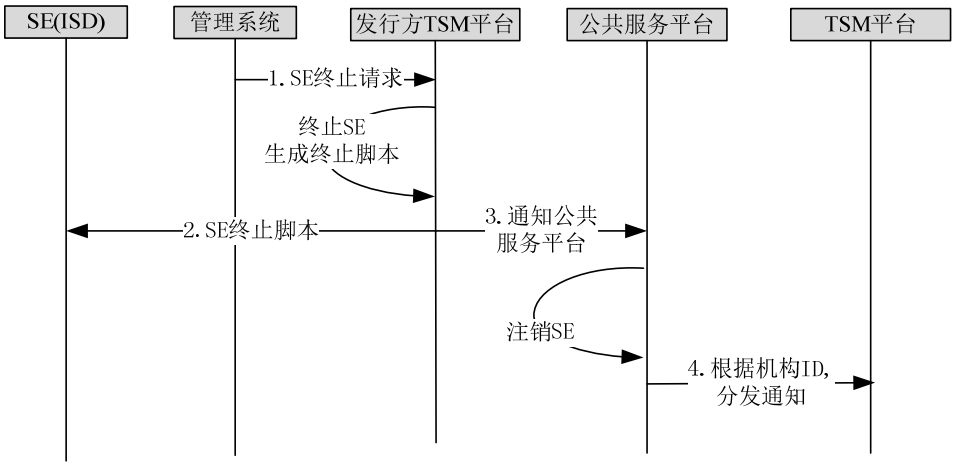

图29 SE 的终止

SE 的终止流程如下：

步骤 1：SE 发行方 TSM 平台收到 SE 终止请求后，系统侧执行终止操作，生成终止脚本；

步骤 2：向 SE 发送终止脚本；

步骤 3：SE 发行方 TSM 平台将 SE 终止信息通知给公共服务平台，信息包括 PAMID、TSM 平台的机构 ID；

步骤4：公共服务平台注销SE，并根据机构ID，将SE终止消息发给各应用提供方TSM平台。

SE终止的消息列表见表10。

表10 SE 终止消息列表

消息	命令功能描述	关键参数	后续操作	备注
SE 终止请求	→SE 发行方 TSM 平台	PAMID	后台系统终止 SE 生成终止脚本	参见 8.9.7
终止脚本下发	SE 发行方 TSM 平台→SE	PAMID、终止脚本		参见 8.9.7
通知公共服务平台	SE 发行方 TSM 平台→公共服务平台	PAMID、SE 应用相关 TSM 平台机构 ID	更改 SE 生命周期，根据机构 ID 生成消息	参见 8.9.13

消息	命令功能描述	关键参数	后续操作	备注
分发 SE 终止通知	公共服务平台→应用提供方的 TSM 平台	PAMID、SE 应用相关 TSM 平台机构 ID		参见 8.9.13

7.2.4 SE 的挂起与解挂

发行方或公共服务平台都可以发起SE的挂起和解挂请求，SE的挂起和解挂包括两种：整卡挂起/解挂和金融SE的挂起/解挂。整卡挂起/解挂将禁止/恢复SE上的所有应用，金融SE的挂起/解挂将只禁止/恢复金融类辅助安全域和支付应用。这两种挂起/解挂操作均由发行方TSM平台实施。

挂起解挂请求由发行方 TSM 平台实施。发行方 TSM 平台挂起或解挂 SE 后，由公共服务平台将 SE 状态通知给 SE 上所有支付应用各自所属的 TSM 平台，流程如图 30 所示。

挂起操作前，发行方TSM平台应首先获取SE的状态，要进行挂起状态的SE必须处于安全（Secure）状态，满足状态转换条件的继续该操作流程。解挂操作前，TSM平台应先获取SE的状态，要进行解挂状态的SE必须处于挂起状态，满足状态转换条件的继续该操作流程。

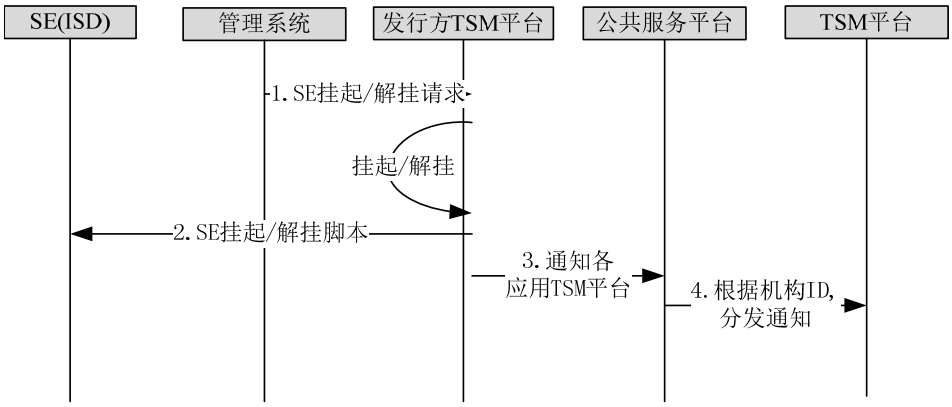

图30 SE 的挂起与解挂

SE 的挂起/解挂的流程如下：

步骤 1：SE 发行方 TSM 平台收到 SE 挂失/解挂请求后，系统侧执行 SE 挂失/解挂，生成相应脚本；

步骤 2：向 SE 下发挂起/解挂脚本；

步骤 3：SE 发行方 TSM 平台将 SE 挂起/解挂信息通知给公共服务平台，信息包括 PAMID 和 TSM 平台机构 ID；

步骤 4：公共服务平台根据机构 ID，将 SE 挂起/解挂信息分发给各支付应用提供方 TSM 平台。

SE 挂起/解挂的消息列表见表 11。

表11 SE 挂起/解挂消息列表

消息	命令功能描述	关键参数	后续操作	备注
SE 挂起/解挂请求	平台管理系统→SE 发行方 TSM 平台	PAMID	挂起/解挂	参见 8.9.7
挂起/解挂脚本下发	SE 发行方 TSM 平台→SE	PAMID、挂起/解挂脚本		参见 8.9.7
通知公共服务平台	SE 发行方 TSM 平台→公共服务平台	PAMID、SE 应用相关 TSM 平台机构 ID	更改 SE 生命周期，根据机构 ID 生成消息	参见 8.8.13
分发通知	公共服务平台→应用提供	PAMID、SE 应用相关 TSM 平台		参见 8.8.13

消息	命令功能描述	关键参数	后续操作	备注
	方的 TSM 平台	机构 ID		

7.2.5 SE 的锁定与解锁

发行方或公共服务平台都可以发起SE的锁定/解锁请求，SE的锁定/解锁包括两种：整卡锁定/解锁和金融SE的锁定/解锁。整卡锁定/解锁将禁止/恢复SE上的所有应用，金融SE的锁定/解锁将只禁止/恢复金融类辅助安全域和支付应用。这两种锁定/解锁均由发行方TSM平台实施。

锁定和解锁请求由发行方 TSM 平台实施。发行方 TSM 平台锁定或解锁 SE 后，通知公共服务平台更新所存储的 SE 状态，公共服务平台随后将 SE 状态通知给 SE 上所有支付应用各自所属的 TSM 平台，流程如图 31 所示。

锁定操作前，发行方TSM平台应首先获取SE的状态，要进行锁定状态的SE必须处于安全（Secure）状态，满足状态转换条件的继续该操作流程。解锁操作前，TSM平台应先获取SE的状态，要进行解锁状态的SE必须处于锁定状态，满足状态转换条件的继续该操作流程。

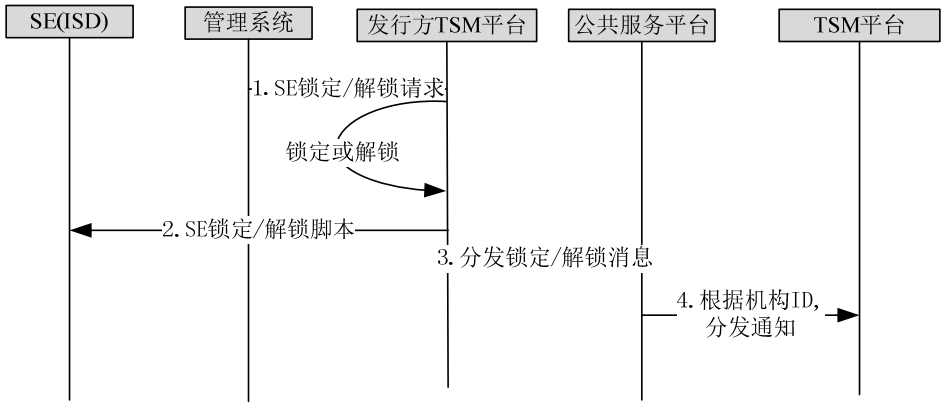

图31 SE 的锁定与解锁

SE 的锁定/解锁流程如下：

步骤 1：SE 发行方 TSM 平台收到 SE 锁定/解锁请求后，系统侧执行锁定/解锁操作，生成相应脚本；

步骤 2：向 SE 下发操作脚本；

步骤 3：SE 发行方 TSM 平台将 SE 锁定/解锁信息通知给公共服务平台，信息包括 PAMID 和机构 ID；

步骤4：公共服务平台根据机构ID，将SE锁定/解锁信息分发给各支付应用提供方TSM平台。

SE的锁定/解锁消息列表见表12。

表12 SE 锁定/解锁消息列表

消息	命令功能描述	关键参数	后续操作	备注
SE 锁定/解锁请求	→SE 发行方 TSM 平台	PAMID	锁定/解锁 SE	参见 8.9.7
锁定/解锁脚本下发	SE 发行方 TSM 平台→SE	PAMID、锁定/解锁脚本		参见 8.9.7
通知公共服务平台	SE 发行方 TSM 平台→公共服务平台	PAMID、SE 应用相关 TSM 机构 ID	更改 SE 生命周期，根据机构 ID 生成消息	参见 8.8.13
分发通知	公共服务平台→应用提供	PAMID、SE 应用相关 TSM 机构		参见 8.8.13

消息	命令功能描述	关键参数	后续操作	备注
	方的 TSM 平台	ID		

7.2.6 SE 状态查询

发行方TSM平台应维护SE的生命周期状态，TSM平台可以向公共服务平台发出SE状态查询请求来获得SE的状态，或者通过请求获取SE及持有人实名身份的合法性时，公共服务平台向发行方TSM平台查询到SE的状态，并返回给申请查询的TSM。

SE的生命周期状态由发行方维护，发行方任何导致SE生命周期状态的操作都需要由公共服务平台转发给该SE上所有支付应用所属的TSM平台。

SE安全状态查询流程如图32所示。

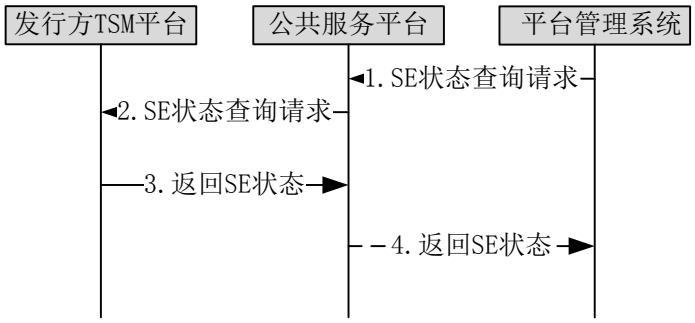

图32 SE 状态查询

SE状态查询流程如下：

步骤 1：该步骤可选，公共服务平台收到查询 SE 状态的请求；

步骤 2：公共服务平台将 SE 状态查询请求发给 SE 发行方 TSM 平台，查询中包括查询类型；

步骤 3：SE 发行方 TSM 平台将 SE 的状态返回给公共服务平台；

步骤4：该步骤可选，公共服务平台返回SE状态查询结果。

SE状态查询消息列表见表13。

表13 SE 状态查询消息列表

消息	命令功能描述	关键参数	后续操作	备注
SE 状态查询请求	管理系统→公共服务平台	PAMID		参见 8.7.4
SE 状态查询请求	公共服务平台→SE 发行方 TSM 平台	PAMID		参见 8.8.14
返回 SE 状态	SE 发行方 TSM 平台 →公共服务平台	PAMID、生命周期状态		参见 8.8.14
返回 SE 状态	公共服务平台→管理系统	PAMID、生命周期状态		参见 8.7.4

7.2.7 SE 应用信息查询

在以发行方作为可信管理者的开发共享模式下，发行方TSM平台应维护SE上所有应用信息，在以公共服务平台为可信第三方的开放共享模式下，SE的支付应用信息由公共服务平台维护。

公共服务平台接收请求后，通过SE注册表找到该SE的发行方，并向该发行方发出查询申请，以获得SE的应用信息。

在以公共服务平台为可信第三方的开放共享模式下，SE的支付应用信息由公共服务平台维护；否则都由发行方维护。公共服务平台可以查询SE上金融相关辅助安全域的信息及支付应用列表，并可将该查询结果转发给信息查询申请机构。SE的应用信息查询流程见图33。

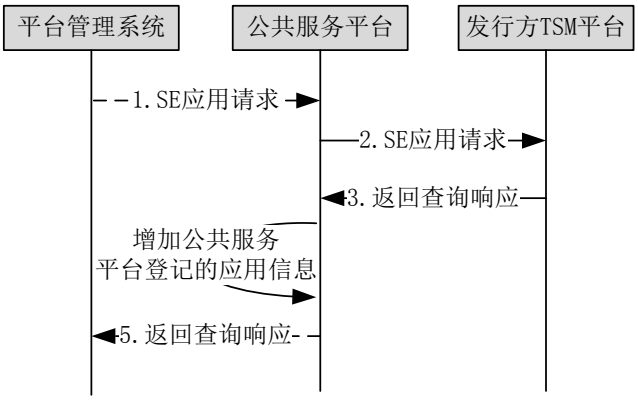

图33　SE 的应用信息查询

SE 的应用信息查询流程如下：

步骤 1：该步骤可选，公共服务平台收到查询 SE 所安装应用的请求；

步骤 2：公共服务平台将 SE 应用查询请求转发给 SE 发行方 TSM 平台；

步骤 3：SE 发行方将 SE 安装的应用信息返回给公共服务平台；

步骤4：公共服务平台将发行方返回的应用信息，加上所管理的支付应用信息，构造返回数据；

步骤5：该步骤可选，公共服务平台返回查询响应。

SE应用信息查询消息列表见表14。

表14　SE 应用信息查询消息列表

消息	命令功能描述	关键参数	后续操作	备注
SE 应用请求查询	管理系统→公共服务平台	PAMID、查询机构 ID		参见 8.7.5
SE 应用请求查询	公共服务平台→SE 发行方 TSM 平台	PAMID、查询机构 ID		参见 8.8.15
返回应用信息	SE 发行方 TSM 平台 →公共服务平台	PAMID、返回值、安全域 ID、安全域持有人、安全域属性、应用 ID、所属安全域、持有人	增加公共服务平台登记的应用信息	参见 8.8.15
返回应用信息	公共服务平台→管理系统	PAMID、返回值、安全域 ID、安全域持有人、安全域属性、应用 ID、所属安全域、持有人		参见 8.7.5

7.2.8　SE 状态同步

由于手机关机、网络连接故障等问题，可能会造成SE状态与TSM平台维护状态信息不一致。当SE联网时，首先需要与发行方的TSM平台进行SE状态信息的同步。发行方的TSM平台向管理客户端应用下发状态同步脚本，如锁定SE等。

SE状态同步流程见图34。

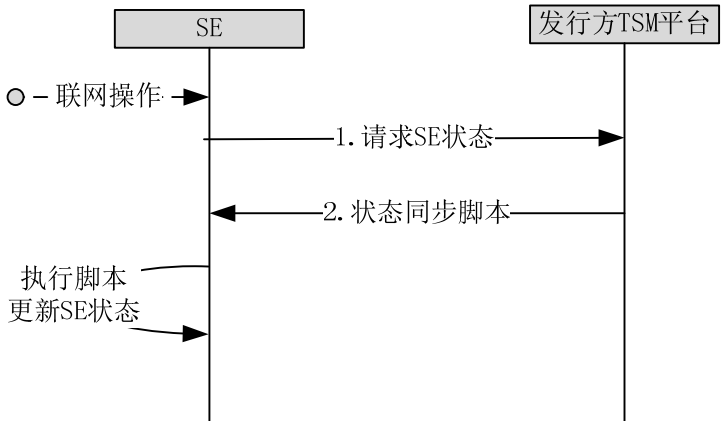

图34　SE 状态同步

7.3　辅助安全域生命周期管理

7.3.1　概述

在以发行方作为可信管理者的开发共享模式下，金融类辅助安全域的生命周期管理由发行方负责。发行方通过其持有的主安全域，为应用提供方进行金融类辅助安全域的生命周期管理，包括辅助安全域的创建、删除、个人化、锁定/解锁。创建的辅助安全域采用委托管理或采用授权管理模式不做规定。

在以发行方作为可信管理者的开放共享模式下，SE中可创建的金融类辅助安全域的数量，需要根据SE的安全等级和业务风险进行控制。

7.3.2　辅助安全域的创建

发行方的TSM平台通过其持有的主安全域为应用提供方创建金融类辅助安全域，初始密钥由TSM平台系统或应用提供方产生和分配。如果创建涉及到联网通用金融业务的辅助安全域，规定应用提供方必须通过公共服务平台完成对SE的可信身份验证，验证通过后才允许发起安全域创建请求。

安全域创建流程如图35所示，在安全域创建前，需要通过SE可信服务流程获取SE及其持有人的实名身份，并根据业务安全要求进行核实，如临柜核实或电话核实等：

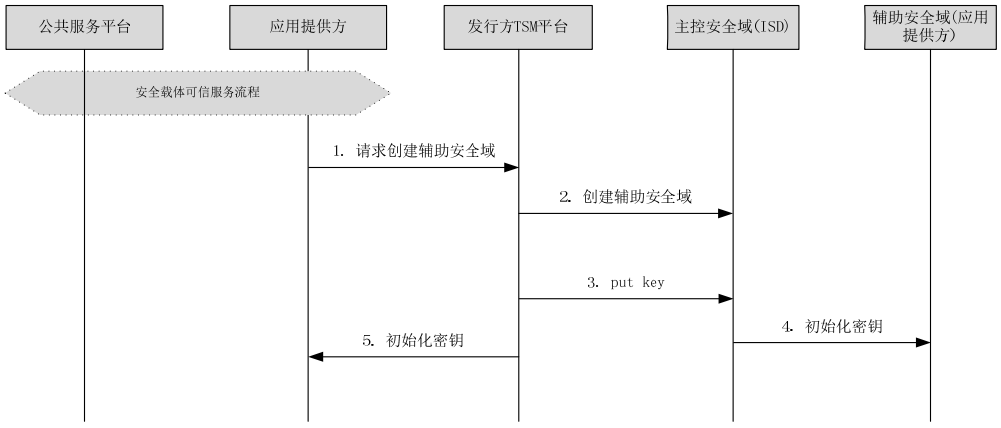

图35　辅助安全域的创建

辅助安全域创建流程如下：

步骤 1：由应用提供方请求发行方的 TSM 平台创建其需要的辅助安全域；
步骤 2：发行方的 TSM 平台通过主控安全域创建应用提供方的辅助安全域；
步骤 3：创建成功后发行方的 TSM 平台向主控安全域发起初始化密钥命令；
步骤 4：将初始密钥推送到应用提供方的辅助安全域中；
步骤5：向应用提供方返还初始化密钥。

7.3.3 辅助安全域的删除

在以发行方作为可信管理者的开发共享模式下，安全域删除由主控安全域负责。流程如图36所示：

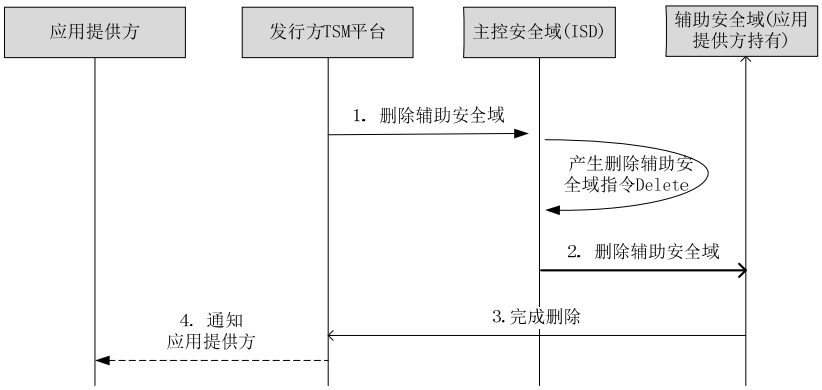

图36 辅助安全域的删除

在以发行方作为可信管理者的开发共享模式下辅助安全域删除流程如下：
步骤 1：发行方的 TSM 平台与主控安全域创建安全通道，主控安全域删除所请求的辅助安全域；
步骤 2： 如果有需要，通知应用提供方。

7.3.4 辅助安全域的锁定/解锁

在以发行方作为可信管理者的开发共享模式下，辅助安全域的锁定/解锁由主控安全域负责，流程如图 37 所示：

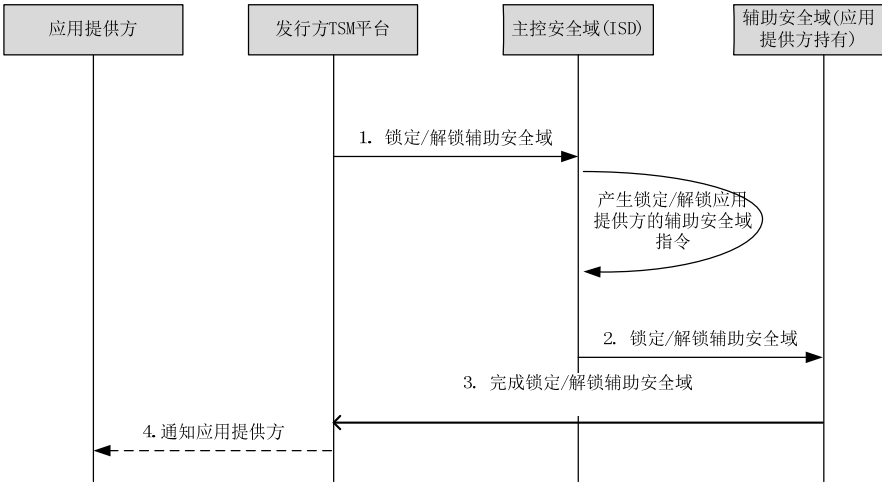

图37 辅助安全域的锁定与解锁

在以发行方作为可信管理者的开发共享模式下辅助安全域锁定/解锁流程如下：

步骤 1：发行方的 TSM 平台与主控安全域创建安全通道，主控安全域锁定/解锁所请求的辅助安全域；

步骤 2：如果需要则通知应用提供方。

7.3.5 辅助安全域密钥更新

辅助安全域在创建完成后会配置初始化密钥，即金融类辅助安全域具有初始的密钥。为了保证安全需要，需对初始密钥进行个人化，即辅助安全域密钥的更新。流程如图38所示：

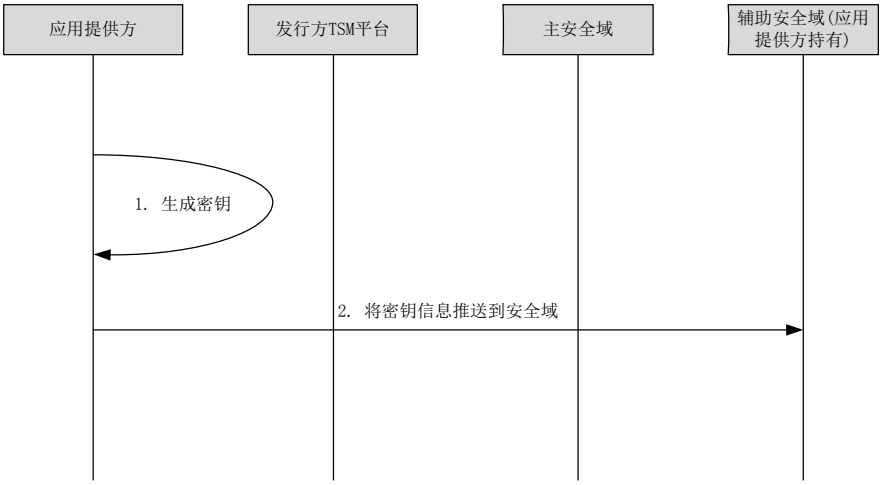

图38 辅助安全域的密钥更新

在以发行方作为可信管理者的开发共享模式下辅助安全域个人化流程如下：

步骤 1：应用提供方生成新密钥信息；

步骤2：应用提供方与其辅助安全域通过初始密钥建安全通道后，将新密钥信息推送到辅助安全域中。

7.4 应用生命周期管理

SE配合相应的管理客户端实现应用的生命周期管理，包括：应用的查询、应用的下载、应用的个人化、应用的锁定/解锁、应用的删除。

7.4.1 应用查询

应用查询包括系统侧应用的查询发现和SE上已安装应用的查询发现。本标准定义的应用查询是指应用管理客户端/SE通过其所连接的TSM平台，发现系统侧可下载的应用列表；SE上已安装应用列表及状态的查询不在本标准定义范围内。

7.4.2 应用下载与授权

应用下载是指将应用文件安全可靠地下载到SE上，并安装应用。

应用安装是生成应用实例的过程，每个应用可以经过安装生成多个应用实例。TSM要为SE上的每个应用实例分配唯一一个PAID，该PAID分配规则如下：同一个SE下，同一个应用的每个实例的PAID，其应用提供者标识符(RID)、专有标志位、应用类型、应用实现字段应和应用PAID相同，保留位从1开始顺序递增。

应用下载需要判断SE的状态，如果SE挂起、锁定，则终止应用下载。

应用下载需要判断应用所属安全域状态；若安全域不存在，则需要进行安全域的创建、安全域个人化；若安全域处于锁定状态，则终止应用下载操作，否则进行应用下载操作。

应用下载前，需要获取安全域剩余空间信息，若剩余空间不足，则终止应用下载操作。

在以公共服务平台为可信第三方的开放共享模式下，用户应用下载流程如图39所示：

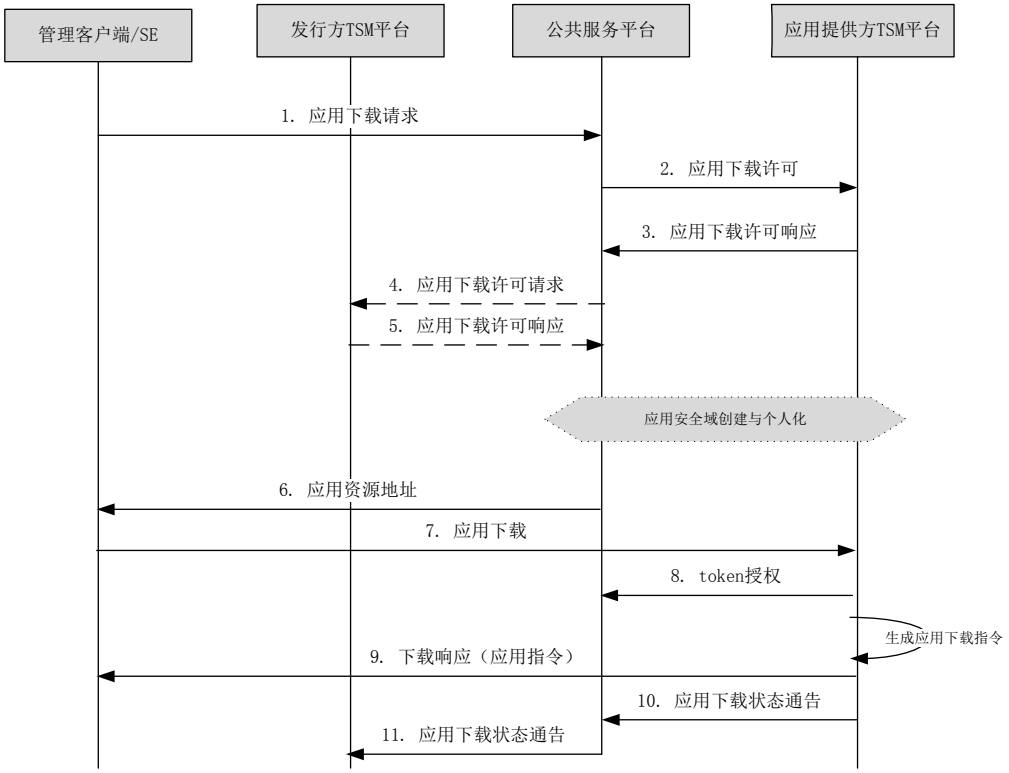

图39　公共服务平台作为可信第三方模式下的应用下载

应用下载流程如下：

步骤 1：管理客户端/SE 向公共服务平台发送应用下载请求；

步骤 2：公共服务平台向应用提供方的 TSM 平台请求下载许可；

步骤 3：应用提供方的 TSM 平台返回下载许可；

步骤 4：如果应用提供方的 TSM 平台允许下载，公共服务平台向发行方的 TSM 平台请求下载许可请求；

步骤 5：发行方的 TSM 平台收到下载许可请求，向公共服务平台返回下载许可响应；

步骤 6：如果发行方的 TSM 平台允许下载，判断应用安全域是否存在，如果不存在，进行安全域创建及个人化；然后向管理客户端/SE 返回应用的数据资源地址；

步骤 7：管理客户端/SE 根据得到的应用的数据资源地址，建立和应用所在 TSM 平台的直接连接，申请应用下载；

步骤 8：应用提供方的 TSM 平台向公共服务平台获取 Token 授权，并生成下载指令；

步骤 9：应用提供方的 TSM 平台返回应用下载指令给管理客户端/SE；

步骤 10，步骤 11：应用提供方的 TSM 完成下载操作后，应该向公共服务平台通告下载操作状态；公共服务平台向发行方的 TSM 转发给通告。

公共服务平台作为可信第三方模式下的应用下载消息列表见表 15。

表15　公共服务平台作为可信第三方模式的应用下载消息列表

消息	命令功能描述	命令与关键参数	后续操作	备注
应用下载请求	管理客户端→TSM 平台	PAMID、应用 PAID		参见 8.9.4
应用下载许可	TSM 平台→公共服务平台	PAMID、应用 PAID		参见 8.8.3
应用提供方的 TSM 平台下载许可	公共服务平台→应用提供方的 TSM 平台	PAMID、应用 PAID	判断 SE 的合法性，给予下载许可	参见 8.8.4
发行方应用下载协商	公共服务平台→发行方的 TSM 平台	PAMID、应用 PAID，应用所占用空间	给予 SE 空间许可	参见 8.8.11
应用下载终止通知	公共服务平台→应用提供方的 TSM 平台	PAMID、应用 PAID，终止代码		参见 8.8.13
应用下载请求	管理客户端→应用提供方的 TSM 平台	PAMID、应用 PAID，应用下载指令	应用下载指令生成	参见 8.9.4
Token 授权	应用提供方的 TSM 平台 →发行方的 TSM 平台	PAMID、应用 PAID，指令 hash 值	授权，生成 Token	参见 8.8.7
应用下载通告	应用提供方的 TSM→公共服务平台	PAMID、应用 PAID、下载状态		参见 8.8.13
应用下载通告	公共服务平台→发行方的 TSM	PAMID、应用 PAID、下载状态		参见 8.8.13

在以发行方作为可信管理者的开发共享模式下，如果应用是发行方的应用，流程如图40所示：

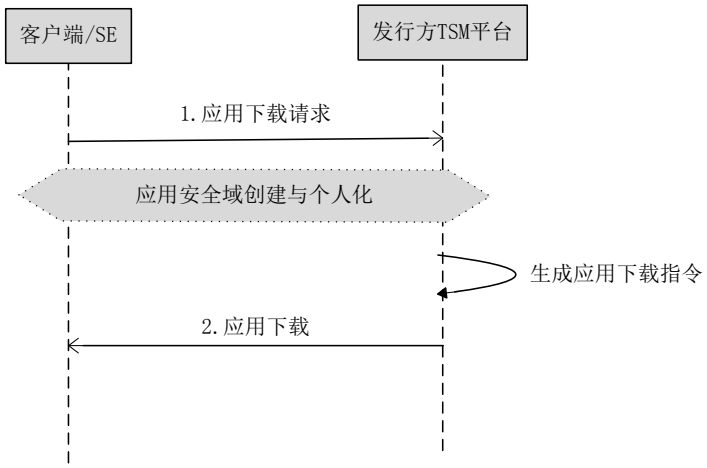

图40　发行方作为可信管理者自有应用下载

应用下载流程如下：

步骤 1：管理客户端向发行方的 TSM 平台发送应用下载请求；判断应用安全域是否存在，如果不存在，进行安全域创建及个人化；

步骤 2：发行方的 TSM 平台生成应用下载指令，并返回给管理客户端。

以发行方作为可信管理者模式下自有应用下载消息列表见表 16。

表16　发行方作为可信管理者模式下自有应用下载消息列表

消息	命令功能描述	命令与关键参数	后续操作	备注
应用下载请求	管理客户端→发行方的TSM平台	PAMID、应用PAID，	应用下载指令生成	参见8.9.4
应用下载响应	发行方的TSM平台→管理客户端	PAMID、应用PAID，应用下载指令		参见8.9.4

在以发行方作为可信管理者的开发共享模式下，如果应用是非发行方的应用，流程如图41所示：

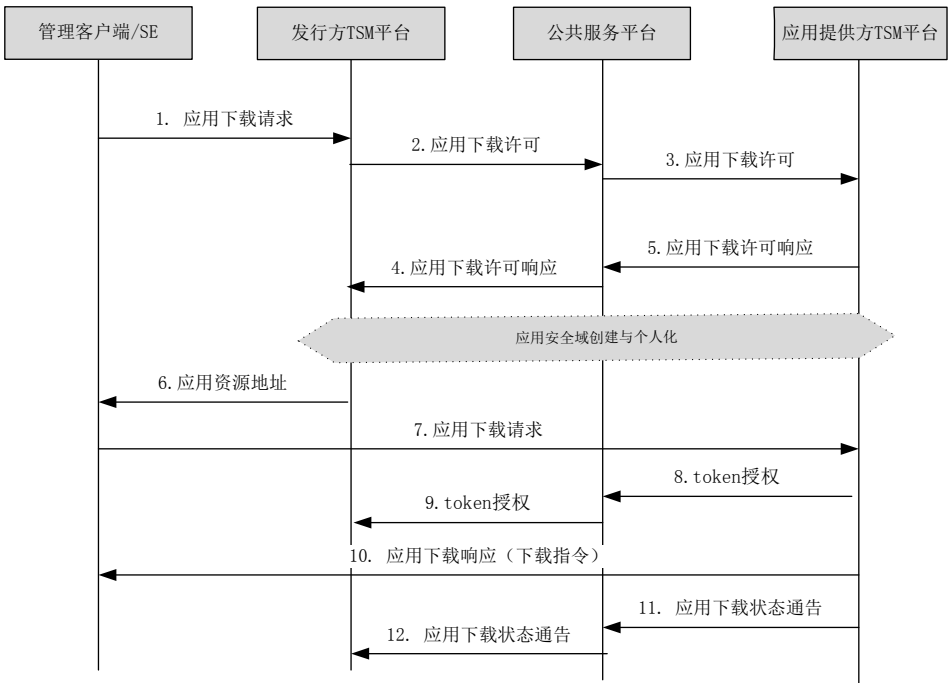

图41　发行方作为可信管理者的跨机构应用下载流程

应用下载流程如下：

步骤1：管理客户端/SE向发卡行的TSM平台发送应用下载请求；

步骤2、步骤3：发行方的TSM平台向应用提供方的TSM平台请求下载许可，该请求通过公共服务平台中转；

步骤4、步骤5：应用提供方的TSM平台向发行方的TSM平台返回下载许可响应，该响应通过公共服务平台中转；

步骤6：如果应用提供方允许下载，发行方的TSM平台向管理客户端/SE发送应用资源地址；

步骤7：管理客户端/SE根据得到的应用资源地址，建立到应用所在的TSM平台的直接连接，申请应用下载；

步骤8、步骤9：应用提供方的TSM平台向发行方的TSM平台申请Token授权，该消息通过公共服务平台中转；

步骤10：应用提供方的TSM平台构造下载指令，返回应用下载指令给管理客户端/SE。

步骤11，步骤12：应用提供方完成下载后，应该向公共服务平台通告下载操作状态；公共服务平台向发行方的TSM转发给通告。

以发行方作为可信管理者模式下跨机构应用下载消息列表见表17。

表17　发行方作为可信管理者模式下跨机构应用下载消息列表

消息	命令功能描述	命令与关键参数	后续操作	备注
应用下载请求	管理客户端→发行方的TSM 平台	PAMID、应用 PAID		参见 8.9.4
应用提供方的 TSM 平台下载许可	发行方的 TSM 平台→公共服务平台	PAMID、应用 PAID		参见 8.8.3
应用提供方的 TSM 平台下载许可	公共服务平台→应用提供方的 TSM 平台	PAMID、应用 PAID	判断 SE 的合法性，给予下载许可	参见 8.8.4
应用下载终止通知	公共服务平台→应用提供方的 TSM 平台	PAMID、应用 PAID，终止代码		参见 8.8.13
应用下载请求	管理客户端→应用提供方的 TSM 平台	PAMID、应用 PAID，应用下载指令	应用下载指令生成	参见 8.9.4
Token 授权	应用提供方的 TSM 平台→发行方的 TSM 平台	PAMID、应用 PAID，指令 hash 值	授权，生成 Token	参见 8.8.7
应用下载通告	应用提供方的 TSM→公共服务平台	PAMID、应用 PAID、下载状态		参见 8.8.13
应用下载通告	公共服务平台→发行方的 TSM	PAMID、应用 PAID、下载状态		参见 8.8.13

如果发行方的安全域要求验证 Token 时，则应用下载时应用提供方需要向发行方的 TSM 平台请求 Token，应用提供方的 TSM 平台需要通过公共服务平台，向发行方的 TSM 平台申请 Token（需提交下载内容的 hash 值），发行方的 TSM 平台生成 Token，返回给应用提供方的 TSM 平台。

应用下载安装之后，可以进行应用个人化过程，此过程为可选项。

7.4.3 应用个人化

应用个人化是SE应用实例加载个人数据的过程，应用TSM平台从应用提供方获取个人化数据，并将个人化数据下载到SE上。

应用TSM平台应验证应用提供方的合法性，与应用提供方建立端到端加密的安全通讯连接，从应用提供方获取相关应用的个人化数据，个人化数据包括：应用数据、密钥、指令等。应用提供方的TSM平台组织个人化指令，并通过空中方式发送到SE上。

7.4.4 应用锁定/解锁

应用可以设置锁定/解锁权限，TSM平台拥有应用的锁定/解锁权限。

锁定/解锁应用操作，由应用提供方向应用提供方的TSM平台发送锁定/解锁应用申请，此过程为可选项，可以根据应用属性灵活配置；应用提供方的TSM平台组织相应的锁定/解锁指令，并通过空中方式发送到SE上。锁定/解锁应用前，需要验证SE上应用状态，只有锁定的应用才可以进行解锁操作。

应用锁定/解锁需要支持，用户通过电话或者网站方式申请，此时TSM平台向应用提供方发送锁定/解锁应用申请，并记录锁定/解锁方式，并通知发行方的TSM平台。待用户登录终端时，需要进行远程管理指令同步。

7.4.5 应用删除

应用可以设置删除权限，TSM平台拥有应用的删除权限，才可以进行相关操作。

应用删除前，判断SE上应用是否存在，若存在则进行应用删除流程；应用删除后，需释放安全域空间。

应用删除操作，TSM平台向应用提供方发送删除应用通知，此过程为可选项，可以根据应用属性灵活配置。

7.4.6 远程管理指令同步

远程管理指令同步是将通过 TSM 平台操作的应用管理指令，同步到 SE 上。指令包括：SE 锁定/解锁指令、安全域锁定/解锁指令、应用锁定/解锁指令等。

7.4.7 SE 应用同步

由于手机突然关机、网络连接故障等问题，可能会造成 SE 上应用及其状态与 TSM 平台维护的状态信息不一致。应用同步操作，可以将 SE 上应用及相关状态上报给 TSM 平台，TSM 平台根据实际情况修改状态信息。

7.5 合作 TSM 平台管理

每个 TSM 平台均需要维护与其它合作应用提供方的 TSM 平台的关系列表。应用提供方的 TSM 平台可以录入或者同步与其合作的 TSM 平台相关信息，信息可以包括：合作方 TSM 平台的编号、通信地址、合作方式等；同时可以更新相关信息，变更合作状态。

7.6 应用提供方管理

7.6.1 注册

应用提供方向 TSM 平台提交基本信息，例如机构名称、机构代码、机构联系人、联系方式、机构通信地址、个人化中心地址（应用需要个人化时提供）等，申请接入 TSM 平台管理。

7.6.2 审核

应用提供方的 TSM 平台管理员需要审核应用提供方的信息，审核通过后，管理员设置对应用提供方的管理期限，应用提供方可以在管理期限范围内接入 TSM 平台。

7.6.3 更新

应用提供方更新相关信息，更新后的信息需提交给应用提供方的 TSM 平台管理员进行审核。

7.6.4 状态变更

应用提供方的 TSM 平台管理员可以设置应用提供方的状态，如注销某一应用提供方，暂停对其提供业务服务。应用提供方注销后，其发布的应用即可停止管理。

7.7 应用管理

7.7.1 PAID 申请

应用提供方在上传应用前，需要向公共服务平台申请应用 PAID，需要输入应用的相关信息，例如：应用名称、应用类型、应用描述等，公共服务平台平台审核通过后，统一分配 PAID。

7.7.2 上传

应用提供方可上传应用，设置应用的相关参数，如应用名称、应用 PAID、package PAID，模块 PAID，应用类型、应用版本号、应用权限、安装参数、占用空间等，并设置应用提供方的 TSM 平台对应用的管理权限。

7.7.3 测试、审核

在应用审核前，需要应用提供方的 TSM 平台管理员测试应用。测试通过的应用，才可以进行审核操作。

7.7.4 发布

审核通过的应用，可以进行应用发布，发布后的应用，才可以进行应用生命周期的管理。发布支付应用时，需要通知公共服务平台。

7.7.5 下架

支付应用需要终止时，需要进行应用下架操作。支付应用下架时，需要通知公共服务平台。

8 移动支付可信服务管理系统间接口

8.1 可信服务管理系统间接口概述

本章后续各节所述实体间关系和接口，不限定于 TSM 平台和公共服务平台构成的星型组网机构，或 TSM 平台直接互联形成的网状互联结构。但在 TSM 平台直接互联形成的网络互联结构中， TSM 平台可以使用本标准定义的接口，也可根据互联关系中所提供的功能和服务情况制定相应系统间接口。

本章节接口报文只定义了报文的核心数据元，实现的接口报文包括但不限于这些数据元。

8.2 可信服务管理系统各实体关系图

可信服务管理系统各实体间关系见图42所示。

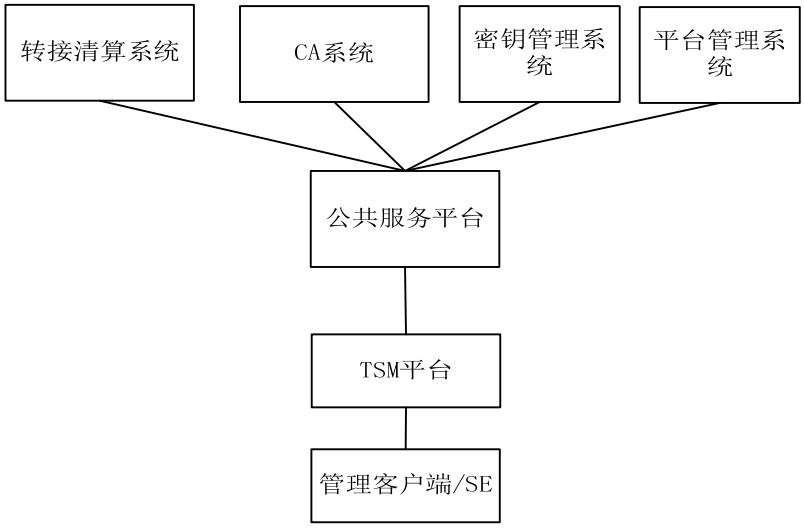

图42 可信服务系统各实体关系

公共服务平台和转接清算系统、CA系统、密钥管理系统、平台管理系统、TSM平台相连，其中平台管理系统是公共服务平台的管理客户端。

TSM平台和公共服务平台、管理客户端/SE相连，其中管理客户端/SE 表示SE及其配套的管理客户端。

8.3 符号定义

接口中的符号定义见表18。

表18 符号定义

符号	说明
M	强制域(Mandatory)，此域在该消息中必须出现否则将被认为消息格式出错
C	条件域(Conditional)，此域在一定条件下出现在该消息中，具体的条件请参考备注说明
C1	条件域(Conditional)，该域出现在需要TSM平台和终端经过多次交互才能完成的交易当中，该域只需要在第一次请求时上送，在后续请求交互中无须出现
O	选用域(Optional)，此域在该消息中由发送方自选
Space	此域在该种消息中不出现
A	字母a－z
N	数字0－9
S	特殊字符
An	字母和数字字符
Ans	字母、数字和特殊字符
MM	月
DD	日
YY	年
Hh	小时
Mm	分
Ss	秒
LL	允许的最大长度为99
LLL	允许的最大长度为999
Var	可变长度域
B	数据的二进制表示，后跟数字表示位（bit）的个数
B	数据的二进制表示，后跟数字表示二进制数据所占字节（Byte）的个数
Z	按GB/T 15120和GB/T 17552的2、3磁道编码
Cn	BCD压缩编码数值

8.4 公共服务平台与转接清算管理系统的接口

发起方：公共服务平台，关键数据元见表 19。

表19 公共服务平台与转接清算管理系统的接口

	字段定义	属性	备　　注
1	CommandType	n2	命令类型
2	TrandeNo	n20	交易序列号

	字段定义	属性	备　　注
3	TradeTime	n14	交易时间
4	OrgID	an32	机构 ID
5	OrgName	anMAX(100)	机构名称
6	OrgStatus	an2	机构状态
7	OrgSummary	anMAX(500)	机构简介

8.5　公共服务平台与 CA 系统的接口

8.5.1　FCSD 证书申请

8.5.1.1　验证码申请

发起方：公共服务平台，关键数据元见表 20。

表20　证书申请注册

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	PAMID	n32	M	M	PAMID
5	IdentityCode	an36	M		证件号
6	IdentityType	n2	M		证件类型
7	UserName	ansMAX (80)	M		申请人
8	Dn	ansMAX (1024)	M		DN 信息
9	StartTime	n14	M		证书开始时间
10	EndTime	n14	M		证书截止时间
11	Pkcs10	var	M		PKCS#10
12	RepCode	an4		M	成功标志： 0000 证书申请成功 FFFF 申请失败
13	Cert	var		M	证书信息： 只有 REPCODE 为 0 时才附带证书信息。为 X509 证书格式的数字证书，其格式参见《信息安全技术 公钥基础设施 数字证书格式》
14	RefNumber	an64		M	参考号
15	AuthCode	an64		M	授权码
16	UserPIN	An6		M	用户联机 PIN

8.5.1.2　证书申请

发起方：公共服务平台，关键数据元见表 21。

表21　证书下载

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	RefNumber	an64	M		参考号
3	AuthCode	an64	M		授权码
4	Pkcs10Len	n2	M		PKCS10 请求长度
5	Pkcs10Request	var	M		PKCS#10 请求
6	CertLen	n2		M	证书长度
7	SeCert	var		M	SE 的 X509 证书

8.5.2　FCSD 证书验证

发起方：公共服务平台，关键数据元见表 22。

表22　FCSD 证书验证

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	Certificateserial_No	n40	M		证书编号
5	RepStatue	an4		M	返回状态： 0000 成功 FFFF 失败

证书的验证可以采用 CRL 方式进行验证，CRL 方式详细信息参考 RFC 3280《Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile》, CRL 方式需要公共服务平台将 CA 的 CRL 列表下载至本地进行验证。

8.5.3　FCSD 证书更新

证书更新将重新产生密钥并生成证书,其过程和申请证书一致,参考接口参考证书申请。

8.6　公共服务平台与密钥管理系统的接口

发起方：公共服务平台，关键数据元见表 23。

表23　密钥申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型：密钥申请
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	SE 发行方 TSM 平台机构 ID

	字段定义	属性	请求	响应	备　　注
5	PAMID	n32	M	M	
6	SSDPAID	an32	M	M	安全域 PAID
7	KeyIndex	n2	M		根密钥索引
8	ResponseCode	n6		M	交易结果，000000 表示成功
9	SSDKeyEnc	an32		M	Enc 密钥（敏感数据）
10	SSDKeyMac	an32		M	Mac 密钥（敏感数据）
11	SSDKeyDek	an32		M	DEK 密钥（敏感数据）

8.7　公共服务平台与平台管理系统接口

8.7.1　验证码申请

发送方：平台管理系统，关键数据元见表 24。

表24　验证码申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型：验证码申请
2	PAMID	n32	M	M	载体 ID
3	IdentityCode	ansMAX(32)	M		证件号
4	IdentityType	an2	M		证件类型
5	UserName	ansMAX(20)	M		申请人
6	StartTime	n14	M		证书开始时间
7	EndTime	n14	M		证书截止时间
8	ResponseCode	n6		M	交易结果，000000 表示成功
9	AuthenticationCode	n32		M	验证码

8.7.2　应用注册申请

发送方：平台管理系统，关键数据元见表 25。

表25　应用注册申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	AppName	ansMAX(20)	M	M	应用名称
5	AppType	n8	M	M	应用类型
6	OrgID	An32	M	M	应用提供方机构 ID
7	AppDesc	ansMAX (300)	O		应用描述

	字段定义	属性	请求	响应	备　　注
8	AppTestReport	ansMAX (500)	O		应用检测报告
9	ValidePeroid	n14	O		有效期
10	ResponseCode	n6		M	交易结果，000000 表示成功

8.7.3　应用注册通知

发送方：公共服务平台，关键数据元见表 26。

表26　应用通知

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	PAID	an32	M	M	应用 PAID
5	AppName	ansMAX(50)	M	M	应用名称
6	AppType	n8	M		应用类型
7	OrgID	An32	M		应用提供方机构 ID
8	ResponseCode	n6		M	交易结果，000000 表示成功

8.7.4　SE 信息查询

发起方：平台管理系统，关键数据元见表 27。

表27　SE 信息查询

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	PAMID	n32	M	M	
5	IssureCode	an32		M	发行方代码
6	UserIdNo	ans18		O	最多 18 个字节，不足 18 个字节的右填空格补齐
7	UserIdType	ans2		O	01-身份证，以 16 进制形式表示
8	UserName	ansMAX(20)		O	用户名称
9	State	an2		M	SE 状态：01 锁定 02 解锁 03 终止
10	ResponseCode	n6		M	交易结果，000000 表示成功

8.7.5　SE 应用列表查询

发起方：平台管理系统，关键数据元见表 28。

表28　SE 应用列表查询

		字段定义	属性	请求	响应	备　　注
1		CommandType	n2	M	M	命令类型
2		TrandeNo	n20	M	M	交易序列号
3		TradeTime	n14	M	M	交易时间
4		PAMID	n32	M	M	
5		ResponseCode	n6		M	交易结果，000000 表示成功
列表	6	PAID	an32		M	当 responseCode 为 000000 时出现
	7	AppName	ansMAX(50)		M	
	8	AppVersion	an4		M	
	9	AppState	n2		M	
	10	AppType	n2		M	
	11	AppDescription	ansMAX(300)		O	

8.8　公共服务平台与 TSM 平台的接口

8.8.1　PAID 申请

发起方：TSM 平台，关键数据元见表 29。

表29　PAID 申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	接收方 TSM 平台机构 ID
6	AppName	ansMAX(50)	M	M	应用名称
7	AppType	n8	M	M	应用类型
8	OrgID	An32	M	M	应用提供方机构 ID
9	AppDesc	ansMAX(300)	O		应用描述
10	ResponseCode	n6		M	交易结果，000000 表示成功
11	PAID	an32		M	应用 PAID

8.8.2　应用列表同步

发起方：TSM 平台，关键数据元见表 30。

表30　应用列表同步

		字段定义	属性	请求	响应	备　　注
1		CommandType	n2	M	M	命令类型
2		TrandeNo	n20	M	M	交易序列号
3		TradeTime	n14	M	M	交易时间
4		SrcTsmId	an32	M		发起方 TSM 平台机构 ID
5		DesTsmId	an32	M		接收方 TSM 平台机构 ID
6		ResponseCode	n6		M	交易结果，000000 表示成功
列表	7	PAID	an32		M	当 RESPONSE_CODE 为 000000 时出现，应用状态 00 表示上线，FF 表示下架
	8	AppName	ansMAX (50)		M	
	9	AppVersion	an4		M	
	10	AppState	n2		M	
	11	AppType	n8		M	
	12	AppDescription	ansMAX (300)		O	

8.8.3　应用列表查询

发起方：TSM 平台，关键数据元见表 31。

表31　应用列表查询

		字段定义	属性	请求	响应	备　　注
1		CommandType	n2	M	M	命令类型
2		TrandeNo	n20	M	M	交易序列号
3		TradeTime	n14	M	M	交易时间
4		SrcTsmId	an32	M		发起方 TSM 平台机构 ID
5		DesTsmId	an32	M		接收方 TSM 平台机构 ID
6		ResponseCode	n6		M	交易结果，000000 表示成功
列表	7	PAID	an32		M	当 RESPONSE_CODE 为 000000 时出现，应用状态 00 表示上线
	8	AppName	ansMAX (50)		M	
	9	AppVersion	an4		M	
	10	AppState	n2		M	
	11	AppType	n8		M	
	12	AppDescription	ansMAX (300)		O	

8.8.4 应用下载许可

发起方：TSM 平台，关键数据元见表 32。

表32 应用下载许可

	字段定义	属性	请求	响应	备 注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	接收方 TSM 平台机构 ID
6	PAMID	n32	M	M	
7	PAID	an32	M		应用 PAID
8	AppVersion	an4	O	O	应用版本号
9	ResponseCode	n6		M	交易结果:000000 表示成功
10	AuthenticateRes	an4		M	0000 下载许可，0001：需要公共服务平台获取 SE 及持有人实名身份,FFFF 禁止下载
11	CoTsmUrl	ansMAX (1024)		C	当获取到下载许可时，返回应用提供方的 TSM 平台的网络地址
12	ResponseApdu	ansMAX (1024)		C	当需要公共服务平台获取 SE 及持有人实名身份时，生成验证 SE 的指令
13	SeResponse	ansMAX (2048)	O		响应数据,返回 SE 执行验证指令后的结果

8.8.5 应用下载许可

发起方：公共服务平台，关键数据元见表 33。

表33 应用下载许可

	字段定义	属性	请求	响应	备 注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID
6	PAMID	n32	M	M	
7	PAID	an32	M		应用 PAID
8	AppVersion	an4	O	O	应用版本号

	字段定义	属性	请求	响应	备　　注
9	ResponseCode	n6		M	交易结果，000000 表示成功
10	AuthenticateRes	an4		M	0000 下载许可，0001：需要公共服务平台获取 SE 及持有人实名身份,FFFF 禁止下载
12	CoTsmUrl	ansMAX (1024)		C	TSM 平台的网络地址,当获取到下载许可时出现

8.8.6　验证结果通知

发起方：公共服务平台，关键数据元见表34。

表34　验证结果通知

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID
6	PAMID	n32	M	M	
7	PAID	an32	M		应用 PAID
8	AppVersion	an4	O	O	应用版本号
9	ValidationCode	an4	M		验证结果，0000 通过验证，FFFF 验证失败
10	SeCert	var	C		SE 的 X509 证书
11	ResponseCode	n6		M	交易结果，000000 表示成功
12	AuthenticateRes	an4		M	0000 下载许可
13	CoTsmUrl	ansMAX (1024)		M	TSM 平台的网络地址

8.8.7　安全域密钥交换

发起方：公共服务平台或者 TSM 平台，关键数据元见表 35。

表35　安全域密钥交换

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID

	字段定义	属性	请求	响应	备　　注
5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID
6	PAMID	n32	M	M	
7	SSDPAID	an32	M		安全域 PAID
8	SSDPrevilage	an2	M		安全与权限
9	PAID	an32	O		应用 PAID
10	AppVersion	an4	O	O	应用版本号
11	SSDKeyEnc	an32	M		Enc 密钥（敏感数据）
12	SSDKeyMac	an32	M		Mac 密钥（敏感数据）
13	SSDKeyDek	an32	M		DEK 密钥（敏感数据）
14	ResponseCode	n6		M	交易结果，000000 表示成功

8.8.8　Token 申请

发起方：TSM 平台，关键数据元见表 36。

表36　Token 申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID
6	PAMID	n32	M	M	
7	PAID	an32	M	M	应用 PAID
8	AppVersion	an4	O	O	应用版本号
9	LoadHash	ansMAX(256)	M		Load 指令的 hash 值
10	InstallHash	ansMAX(256)	M		install 指令的 hash 值
11	ResponseCode	n6		M	交易结果，000000 表示成功
12	LoadToken	ansMAX(256)		M	Load 指令的 Token
13	InstallToken	ansMAX(256)		M	Install 指令的 Token

8.8.9　发行方创建安全域申请

发起方：TSM 平台，关键数据元见表 37。

表37　发行方创建安全域申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID
6	PAID	an32	M		应用 PAID
7	ResponseCode	n6		M	交易结果，000000 表示成功
8	SSDPAID	an32		M	安全域 PAID
9	CoTsmUrl	ansMAX (1024)		M	发行方 TSM 平台的网络地址

8.8.10　发行方安全域删除/锁定/解锁申请

发起方：TSM 平台，关键数据元见表 38。

表38　发行方安全域删除/锁定/解锁申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID
6	SSDPAID	an32	M	M	安全域 PAID
7	ResponseCode	n6		M	交易结果，000000 表示成功
9	CoTsmUrl	ansMAX (1024)		M	TSM 平台的网络地址

8.8.11　公共服务平台创建安全域申请

发起方：TSM 平台，关键数据元见表 39。

表39　公共服务平台创建安全域申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号

	字段定义	属性	请求	响应	备　　注
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	公共服务平台机构 ID
6	PAID	an32	M		应用 PAID
7	ResponseCode	n6		M	交易结果，000000 表示成功
8	SSDPAID	an32		M	安全域 PAID
9	ResponseApdu	ansMAX(1024)		M	指令
10	SeResponse	ansMAX (1024)	C		响应数据,返回 SE 执行指令后的结果

8.8.12　公共服务平台应用操作许可

发起方：TSM 平台，关键数据元见表 40。

表40　应用操作许可

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	公共服务平台机构 ID
5	DesTsmId	an32	M	M	发卡行 TSM 平台机构 ID
6	SSDPAID	an32	O	O	安全域 PAID
7	PAID	an32	O	O	应用 PAID
7	ResponseCode	n6		M	交易结果，000000 表示成功
9	AuthenticateRes	an4		M	验证许可：0000：允许创建，FFFF 禁止创建

8.8.13　公共服务平台安全域删除/锁定/解锁申请

发起方：TSM 平台，关键数据元见表 41。

表41　公共服务平台安全域删除/锁定/解锁申请

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	公共服务平台机构 ID

	字段定义	属性	请求	响应	备　　注
6	SSDPAID	an32	M	M	安全域 PAID
7	ResponseCode	n6		M	交易结果，000000 表示成功
9	ResponseApdu	ansMAX (1024)		M	指令
10	SeResponse	ansMAX (1024)	C		响应数据,返回 SE 执行指令后的结果

8.8.14　操作结果通知

发起方：TSM 平台或者公共服务平台，关键数据元见表 42。

表42　操作结果通知

		字段定义	属性	请求	响应	备　　注
1		CommandType	n2	M	M	命令类型
2		TrandeNo	n20	M	M	交易序列号
3		TradeTime	n14	M	M	交易时间
4		SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
列表	5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID
6		OpType	n2	M	M	操作类型
7		OpResult	n6	M		操作结果
8		PAMID	n32	M	M	
9		SSDPAID	an32	O	O	安全域 PAID
10		PAID	an32	O	O	应用 PAID
11		AppVersion	an4	O	O	应用版本号
12		ResponseCode	n6		M	交易结果:000000 表示成功

8.8.15　SE 信息查询

发起方：公共服务平台或者 TSM 平台，关键数据元见表 43。

表43　SE 状态信息查询

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID

	字段定义	属性	请求	响应	备　　注
6	PAMID	n32	M	M	
7	IssureCode	an32		M	发行方代码
8	UserIdNo	ans18		O	最多 18 个字节，不足 18 个字节的右填空格补齐
9	UserIdType	ans2		O	01-身份证，以 16 进制形式表示
10	UserName	ansMAX(20)		O	用户名称
11	State	an2		M	SE 状态：01 锁定 02 解锁 03 终止
12	ResponseCode	n6		M	交易结果，000000 表示成功

8.8.16 SE 应用列表查询

发起方：公共服务平台或者 TSM 平台，关键数据元见表 44。

表44 SE 应用列表查询

		字段定义	属性	请求	响应	备　　注
1		CommandType	n2	M	M	命令类型
2		TrandeNo	n20	M	M	交易序列号
3		TradeTime	n14	M	M	交易时间
4		SrcTsmId	an32	M		发起方 TSM 平台机构 ID
5		DesTsmId	an32	M		合作方 TSM 平台机构 ID
6		PAMID	n32	M	M	
7		ResponseCode	n6		M	交易结果，000000 表示成功
列表	8	PAID	an32		M	当 responseCode 为 000000 时出现
	9	AppName	ansMAX (20)		M	
	10	AppVersion	an4		M	
	11	AppState	n2		M	
	12	AppType	n2		M	
	13	AppDescription	ansMAX (300)		O	

8.8.17 SE 身份验证

发起方：TSM 平台，关键数据元见表 45。

表45 SE 身份验证

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TrandeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间

	字段定义	属性	请求	响应	备　　注
4	SrcTsmId	an32	M	M	发起方 TSM 平台机构 ID
5	DesTsmId	an32	M	M	合作方 TSM 平台机构 ID
6	PAMID	n32	M	M	
7	UserPIN	An6	M		用户联机 PIN
8	ResponseCode	n6		M	交易结果:000000 表示成功
9	ValidationResult	an4		M	验证结果：0000 验证通过 0001 验证中，FFFF 验证失败；
10	ResponseApdu	ansMAX (1024)		M	当需要公共服务平台获取 SE 及持有人实名身份时，生成验证 SE 的指令
11	SeResponse	ansMAX (1024)	C		响应数据

8.8.18　SE 激活

发起方：TSM 平台，关键数据元见表 46。

表46　SE 激活

	字段定义	属性	请求	响应	备　　注
1	CommandType	n2	M	M	命令类型
2	TradeNo	n20	M	M	交易序列号
3	TradeTime	n14	M	M	交易时间
5	PAMID	n32	M	M	
6	Imei	n15	O		
7	Imsi	n15	O		
8	VerifyCode	nMAX(32)	M		验证码
8	UserName	Ans(20)	O		用户名
9	UserIdNo	ans18	O		最多 18 个字节，不足 18 个字节的右填空格补齐
10	UserIdType	ans2	O		01-身份证，以 16 进制形式表示
11	Msisdn	ans16	O		最多 16 个字节，不足 16 个字节的右填空格补齐
12	ResultCode	n6		M	响应码：000000 表示成功
13	RegisterResult	an4		M	激活结果:0000 激活成功，0001 激活中，FFFF 激活失败
列表 15	ResponseApdu	ansMAX(1024)		C	服务响应数据（APDU），当需要给载体下发 APDU 指令时出现
16	SeResponse	ansMAX (1024)	C		响应数据,返回 SE 执行指令后的结果

8.9　TSM 平台与管理客户端接口

8.9.1 SE 激活

如果发起方是应用管理终端，见 JR/T 0094.3-2012 的 7.3.11 节。
如果发起方是移动终端客户端，见 JR/T 0094.3-2012 的 8.3.9 节。

8.9.2 应用查询

如果发起方是应用管理终端，见 JR/T 0094.3-2012 的 7.3.1 节，7.3.2 节，7.3.3 节。
如果发起方是移动终端客户端，见 JR/T 0094.3-2012 的 8.3.1 节，8.3.2 节，8.3.3 节。

8.9.3 应用同步

如果发起方是应用管理终端，见 JR/T 0094.3-2012 的 7.3.9 节。
如果发起方是移动终端客户端，见JR/T 0094.3-2012的8.3.9节。

8.9.4 应用下载/删除/锁定/解锁

如果发起方是应用管理终端，应用下载见JR/T 0094.3-2012的7.3.4节，应用删除见JR/T 0094.3-2012的7.3.8节，应用锁定见JR/T 0094.3-2012的7.3.6节，应用解锁见JR/T 0094.3-2012的7.3.7节。

如果发起方是移动终端客户端，应用下载见JR/T 0094.3-2012的8.3.4节，应用删除见JR/T 0094.3-2012的8.3.6节。

8.9.5 应用个人化

如果发起方是应用管理终端，见 JR/T 0094.3-2012 的 7.3.5 节。
如果发起方是移动终端客户端，见JR/T 0094.3-2012的8.3.5节。

8.9.6 应用远程管理同步

如果发起方是应用管理终端，见 JR/T 0094.3-2012 的 7.3.10 节。
如果发起方是移动终端客户端，见JR/T 0094.3-2012的8.3.8节。

8.9.7 SE 的锁定/解锁/终止

如果发起方是应用管理终端，SE 锁定见 JR/T 0094.3-2012 的 7.3.12 节，SE 解锁见 JR/T 0094.3-2012 的 7.3.13 节，SE 终止见 JR/T 0094.3-2012 的 7.3.14 节。

8.9.8 安全域的锁定/解锁/终止

如果发起方是应用管理终端，安全域锁定见 JR/T 0094.3-2012 的 7.3.15 节，安全域解锁见 JR/T 0094.3-2012 的 7.3.16 节，安全域终止见 JR/T 0094.3-2012 的 7.3.17 节。

9 SE 要求

9.1 PAMID

每个 SE 都具有金融网络唯一的身份标识 PAMID，PAMID 由公共服务平台负责统一分配和备案管理，由发行方写入 SE 中，PAMID 写入后不能够被更改。PAMID 包含发行方代码、SE 类型代码（SIM、SD、全终端等）及唯一序列号等。

9.2 基本安全域配置

SE 中的安全域分为如下几类：

——主安全域：主安全域即发行方安全域，由发行方持有，主安全域没有安全域生命周期状态，他直接继承了卡片生命周期状态。

——辅助安全域：主安全域以外的其他安全域称为辅助安全域。

——FCSD 安全域：FCSD 安全域是一种特殊的辅助安全域，安全域关联到自身，在 SE 首次接入到金融网络前创建，创建后将同发行方安全域一样，直接继承了卡片的生命周期，在卡片终止时终止。FCSD 安全域由公共服务平台持有，不能被主安全域锁定、删除。其主要功能是进行 SE 及其持有人实名身份的验证和获取。

——FMSD 安全域：FMSD 安全域是一种特殊的辅助安全域，安全域关联到自身，在 SE 首次接入到金融网络前创建，创建后将同发行方安全域一样，直接继承了卡片的生命周期，在卡片终止时终止。FMSD 安全域具有授权管理者权限，由公共服务平台持有，不能被主安全域锁定、删除。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。

在以发行方为可信管理者的开发共享模式下，在 SE 首次接入到金融网络前，SE 中需配置的安全域为：

——主安全域

——FCSD安全域

图43描述了该模型下SE的一个实现结构：

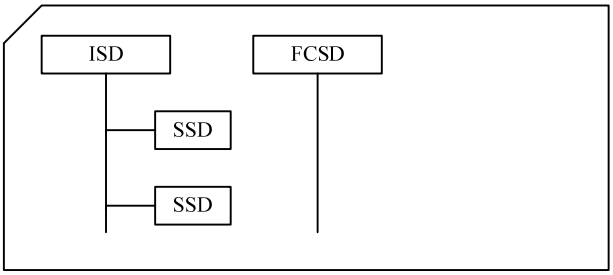

图43　发行方作为可信管理者的开发共享模型下的 SE 实现

在以公共服务平台作为可信第三方的开放共享模式下，在 SE 首次接入到金融网络前，SE 中需配置的功能安全域如下：

——主安全域

——FCSD 安全域

——FMSD安全域

实现中要求将FMSD安全域功能集成到FCSD安全域中，图44描述了该模型下SE的一个实现结构：

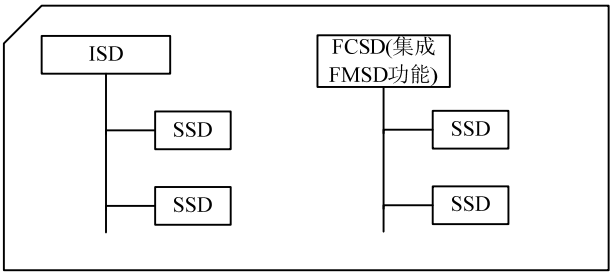

图44　以公共服务平台作为可信第三方开放共享模型下的 SE 实现

9.3　基本基础服务

9.3.1 概述

基本基础服务是指SE必须具备的服务，这些服务能够为卡上的应用操作提供基础。

9.3.2 应用选择服务

应用选择服务通过金融目录管理应用实现。金融目录管理应用在 SE 上作为必选应用装载。在以发行方作为可信管理者的开发共享模式下，该应用关联到主安全域，在以公共服务平台作为可信第三方的开放共享模式下，该应用关联到 FMSD 安全域。

金融目录管理应用参见 JR/T 0089.2-2012。

9.3.3 SE 可信服务

SE 可信服务是由公共服务平台调用的局部服务，用于提供 SE 及其持有者实名身份获取和传递。

SE 可信服务由 FCSD 安全域提供，FCSD 安全域中存有 SE 持有者的非对称密钥、公钥证书和公共服务平台的公钥证书。

9.3.4 SE 的脱机 PIN 校验

SE 的脱机 PIN 校验服务是一个全局服务，用于当管理客户端访问 SE 时进行 PIN 校验。

SE 的脱机 PIN 校验由 OPEN 提供，OPEN 具备 CVM 管理权限，当管理客户端试图访问 SE 内支付应用时，发送 VERIFY PIN 指令，OPEN 调用 GP API 进行脱机 PIN 校验。

9.4 基本权限配置

对于主安全域的权限，至少要有安全域权限，卡片锁定权限，卡片终止权限，令牌校验权限。

对于 FCSD 安全域的权限，至少要具备安全域权限。

对于 FMSD 的权限，至少要具备安全域权限，授权管理权限，令牌校验权限，DAP 权限。

对于 OPEN，至少要具备 CVM 权限。

9.5 APDU 命令

SE 支持的 APDU 命令包括：

——DELETE
——GET DATA
——GET STATUS
——INSTALL
——LOAD
——MANAGE CHANNEL
——PUT KEY
——SELECT
——SET STATUS
——STORE DATA
——PERFORM SECURITY OPERATION
——GET CHALLENGE
——EXTERNAL AUTHENTICATION
——INTERNAL AUTHENTICATION
——MANAGE SECURITY ENVIRONMNET

——VERIFY PIN

9.6 安全通道

FCSD 安全域的安全通道采用 SCP10 方式的安全通道。

辅助安全域的安全通道类型由应用提供方与辅助安全域的创建者协商确定，本标准不做定义。

10 移动支付可信服务管理系统安全要求

10.1 密钥体系与密码算法

10.1.1 密钥体系

密钥体系包含对称密钥体系和非对称密钥体系。

对称密钥体系实现对用户交易过程中敏感数据的加密和校验，非对称密钥体系实现对数字证书的应用，实现各实体间在互联网上进行传输数据的加密及签名校验。本标准中对称密钥体系和非对称密钥体系对国产密码算法和国际密码算法均进行支持。

10.1.2 认可的加密算法

——对称算法

对称算法支持国产 SM4 对称算法和国际 3DES 对称算法，对称算法可以用于加密运算和 MAC 机制中。

国产对称算法为 SM4，该算法是一个分组算法，该算法的分组长度为 128 比特，密钥长度为 128 比特。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

SM4 算法实现详见 GM/T 0002。

3-DES 加密是指使用双长度（16 字节）密钥将 8 字节明文数据块加密成密文数据块。

对称算法可用于借贷记密钥体系 PIN 加密和报文计算 MAC 进行完整性保证等领域,推荐加解密采用 CBC 模式进行计算，MAC 计算采用 ECB 模式进行计算。

——非对称算法

非对称算法支持国产的 SM2 算法和国际的 RSA 算法，非对称密码算法用于认证中心、SE 的签名与认证。私钥用于对信息的加密和签名，公钥用于加密数据的恢复与验证。

国产非对称算法为 SM2，其密钥位长为 m（m=256）。该算法是一种椭圆曲线公钥密码算法。

SM2 算法实现详见　GM/T 0003。

——杂凑算法

杂凑算法支持国产的 SM3 算法和国际算法 SHA-1。杂凑算法算出的哈希值用于校验签名的交易数据的完整性。

SM3算法对于给定的长度为k(k<264)的消息， SM3杂凑算法经过填充和迭代压缩，生成杂凑值，杂凑值长度为256比特。

SM3 算法详见 GM/T 0004。

SHA-1 中输入任意长度的信息，产生一个 20 字节的哈希值。SHA-1 算法见 GB/T 18238.3。

10.2 CA 体系

10.2.1 概述

电子认证服务 CA 系统是公共服务平台的基础系统，该系统在密码服务系统的基础之上，通过建设证书认证机构 CA，用户注册中心 RA 提供数字证书的生产服务，实现 SE 与可信服务管理系统之间以及各系统之间的实体认证和通信安全保障。完整的证书认证体系一般采用 RCA-CA-RA3 层结构构成,RCA 和 CA 建设在公共服务平台一端。

RCA 为根认证机构。

CA 为证书认证服务系统的主体机构，CA 提供数字证书签发、发布、管理、撤销等服务，CA 签发的证书应由合法的第三方电子认证服务机构产生。

RA 为用户证书申请注册机构，分为远程注册机构和本地注册机构。RA 中心提供数字证书的申请注册、用户身份审核等服务。

10.2.2 CA 系统

CA 是电子认证服务系统的核心业务节点，主要提供下列服务：

——证书的签发和管理；

——证书撤销列表的签发和管理；

——证书/证书撤销列表的发布；

——系统自身的安全审计与安全管理；

——用户注册中心的设立、审核、维护及管理。

10.2.3 注册机构 RA

注册机构 RA 是 CA 体系的重要节点，是证书认证服务系统的用户申请证书的注册与审核机构，由 CA 中心授权运作，提供如下服务功能：

——用户数字证书申请的注册受理；

——用户真实身份的审核；

——用户数字证书的申请与下载；

——用户数字证书的撤销与更新的受理；

——证书受理核发点设立的审核及管理。

10.2.4 数字证书

数字证书在本标准中主要实现以下功能：

——实现公共服务平台对 SE 实体的身份鉴别及 TSM 平台与 SE 之间数据安全的保障；

——实现对公共服务平台、业务 TSM 平台、应用提供方、终端间数据机密性和完整性的安全保障；

——数字证书格式为 X509 详细参考标准 GB/T 20518。

数字证书中必要包含的信息为主体名称中的 DN 信息和自定义扩展域中的身份信息及 SE 安全等级，其设定规则如下：

1、数字证书中 DN 信息规则：

DN 在数字证书的主体名称域中，用于唯一标识用户的 X.500 名称，通常包括 CN、OU、O、C 等组成部分。

下面给出具体的 DN 规则。

——CN 部分（用于表示 PAMID）；

——OU 部分（用于表示证书申请机构）；

如 OU=xx 支付机构；

——O 部分；

在证书中用于表示 CA 系统的名称，如：

O=XXCA；

——C 部分

用于表示订户所属国家或地区的英文简称，全部大写，如中国订户为：C=CN。

2、自定义扩展域：

证件类型、证件号码及 SE 安全等级体现在自定义扩展域中，包括：

——身份标识码（IdentityCode）：按照下表中定义的证件类型编号进行标识，如个人使用身份证申请证书时的编码为：IdentityCode=0。

——个人证件号码（InsuranceNumber）：填写个人证件号码，在个人申请 SE 数字证书时有此项扩展项。

如 InsuranceNumber=110101190006162005

附：允许使用的证件类型及编码

数字证书的重要作用之一是用于标识订户的身份信息。为确保订户身份信息的唯一性及权威性，要求了可用于申请 SE 数字证书的证件类型。个人申请 SE 数字证书时，适用以下证件类型，且相应的编码为：

表47　证件类型

证件类型	编码
身份证	0
护照	1
军人身份证件	2
武装警察身份证件	A
港澳居民往来内地通行证	B
台湾居民来往大陆通行证	C
户口簿	E
其他	Z

——SE 安全等级(SESecClassified)：

表示了 SE 属于哪个级别的安全等级，在 SE 注册申请证书时需要填入该项。

10.3　SE 注册与激活安全要求

10.3.1　基本要求

SE 初始化需要在安全的环境下进行，初始化的完成要进行端到端的加密。

10.3.2　密钥安全要求

初始密钥要求三级密钥体系生成，一级密钥为公共服务平台的对称主密钥，二级密钥为发行方 TSM 平台向公共服务平台申请的，并由公共服务平台主密钥分散产生的次主密钥，SE 的初始密钥由发行方 TSM 平台的次主密钥分散产生。

一级密钥的产生由公共服务平台采用随机数的方式产生。

二级密钥由公共服务平台主密钥，按照分散规则产生，并由发行方采用安全的方式（IC 卡方式，或其他安全方式）加载到 TSM 平台中。

SE 的对称密钥由发行方通过二级密钥分散产生，分散因子为 PAMID 和根密钥索引 ID。

根密钥索引ID为机构注册ID+机构ID组成，机构注册ID为4位数字组成，由公共服务平台注册时系统产生。

10.3.3 证书安全要求

证书申请过程：

——机构数字证书

机构数字证书用于保证机构与机构之间,机构与公共服务平台之间的通信安全保障，该证书由机构向公共服务平台的 CA 进行申请，证书须存放在 USBKey 等硬件加密设备中进行使用。

——用于实体鉴别的数字证书

用于 SE 实体鉴别的数字证书由用户在柜面面签时，由发行方向公共服务平台 CA 申请产生，并获得由发行方提供的下载凭证，用户获得证书下载凭证，凭证须采用密码信封等安全方式交予用户。

SE 在进行注册时完成证书的下载，证书的公私钥对在 SE 内部产生，SE 将 PAMID 和公钥信息采用 PKCS#10 请求方式发送到公共服务平台，并向 CA 完成申请数字证书。

10.3.4 证书的申请过程

证书的申请，由申请人通过柜面向发行方提出申请，同时发行方通过 RA 系统向公共服务平台 CA 提交申请信息，获得下载凭证，并将下载凭证使用密码信封等安全方式交由申请人，申请人凭借下载凭证在注册时下载证书。

10.4 SE 可信身份验证安全要求

公共服务平台须采用基于PKI技术的电子认证服务体系实现对SE身份验证，保证SE与其所有人的身份一一对应。

SE使用过程中要求使用PIN码验证，防止SE被非法授权使用。

PIN码仅能由SE所有人掌握并使用。

10.5 SE 应用下载安全

10.5.1 基本要求

在委托管理模式进行应用操作需要采用令牌机制进行应用下载审核，根据不同的应用下载方式，令牌主要有用户应用加载的 Load Token，用于应用安装的 Install Token 以及用于应用迁移的 Extradition Token。

用于进行 Token 计算的密钥算法为 SM2、SM3、RSA、SHA-1。

10.5.2 Token 计算

10.5.2.1 Load Token 计算

Load Token 是允许应用程序加载到 SE 的令牌，用以验证 Load 请求的合法性。

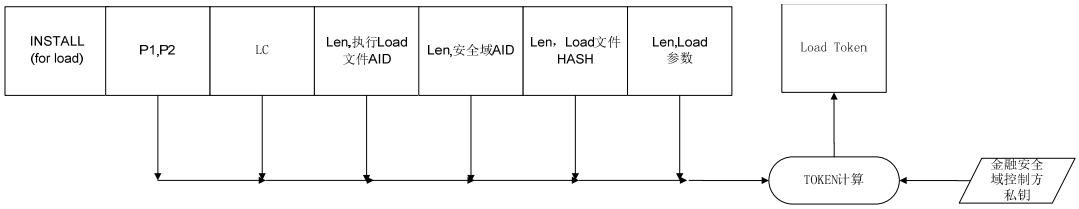

图45 Load Token 计算输入结构

产生 Load Token 的须遵循以下要求：

——只有应用代码包含在签名当中才可以被加载到 SE 中；

——Load 文件的 PAID 必须包含在签名当中；
——与安全域有关的执行 Load 文件和所有执行模块必须包含在签名当中；
——Load Token 必须由具备“令牌验证权限”的安全域提供者发行。

表48　Load Token 输入字段

字段	长度
P1	1
P2	1
LC	1
Load 文件 PAID 长度	1
Load 文件 PAID	5-16
安全域 PAID 长度	1
安全域 PAID	5-16
Load 文件 HASH 值长度	1
Load 文件 HASH 值	20
Load 参数域长度	1-2
Load 参数域	0-n,其中 TAG’C9’前 16 字节表示为 PAMID

10.5.2.2　Install Token 计算：

Install Token 是一个包含 Load 文件的签名应用，用于验证安装到 SE 中的应用是否被合法授权。

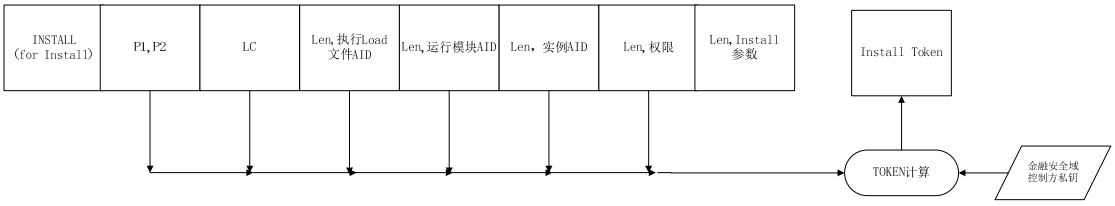

图46　计算 Install Token 计算输入结构

产生 Install Token 必须遵循以下步骤：
——只有包含在签名中的应用和可执行的 Load 文件可以安装到 SE；
——只有能够通过 PAID 被选择的实例，且该实例 PAID 包含在签名数据当中，才能被使用；
——只有在签名中指定权限的应用才能安装；
——Install Token 必须由具备“令牌验证权限”的安全域提供者发行。

表49　Install Token 输入字段

字段	长度
P1	1
P2	1
LC	1
执行 Load 文件 PAID 长度	1
执行 Load 文件 PAID	5-16
执行模块 PAID 长度	1
执行 Load 文件内部 PAID	5-16

字段	长度
实例 PAID 长度	1
实例 PAID	5-16
权限长度	1
权限（byte-1-byte2-byte3）	1 或 3
可选参数域长度	1
可选参数域	0-n,其中 TAG’C9’前 16 字节表示为 PAMID

10.5.2.3 Extradition Token 计算

Extradition Token 是授权应用从一个安全域迁移到另一个安全域的令牌。

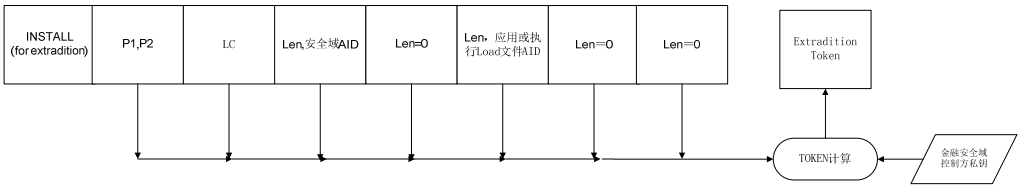

图47 Extradition Token 计算输入结构

一个 Extradition Token 应保证按照以下要求产生：

——应用或者执行文件必须包含在签名里面才可以被迁移；

——令牌只能由具备“令牌验证权限”的安全域提供者发行。

表50 Extradition Token 输入字段

字段	长度	说明
P1	1	强制
P2	1	强制
LC	1	强制
安全域 PAID 长度	1	强制
安全域 PAID	5-16	可选
Len=0	1	强制
执行 Load 文件内部 PAID	5-16	强制
应用或执行 Load File PAID 长度	1	强制
应用或执行 Load File PAID	5-16	强制
Len=0	1	强制
Extradition 参数域长度	1	强制
Extradition 参数域	0-n	可选

10.6 管理客户端与 TSM 平台

10.6.1 传输安全

对于管理客户端，应满足以下安全要求：

——应使用足够强度的加密算法和安全协议保护管理客户端与TSM平台之间的连接，通过互联网传输必须采用数字证书机制以保证数据的机密性、完整性和不可抵赖性；

——应使用足够强度的加密算法和安全协议保护管理客户端与服务器之间的连接，例如使用SSL/TLS和IPSEC等协议；

——如使用SSL协议，应使用3.0及以上相对高版本的协议，取消对低版本协议的支持；

——管理客户端到服务器的SSL加密密钥长度应不低于128位，用于签名的SM2密钥不低于256位，RSA密钥长度应不低于1024位；

——管理客户端通过专线连接TSM平台传输数据时，须定时重新协商会话密钥；

——对于数据短信传输模式，包括上行短信和下行短信，关键数据域必须经通讯层加密及MAC校验码计算；

——如采用数字证书机制，数字证书的签发须由公共服务平台端的CA进行统一签发。

10.6.2 业务数据安全

数据处理应满足以下安全要求：

——管理客户端与TSM平台必须对发送的报文关键要素计算MAC或进行签名加密，以供接收方校验报文的真实性及保证关键要素数据的机密性。关键要素包括但不限于应用数据下载安装指令、响应数据等。报文的接收方，用与发送方相同的方法计算MAC或进行验签，并验证报文MAC或签名的正确性；

——客户手机号、密码、证件号码等敏感信息按要求进行加密传输、保存和使用，显示时应进行屏蔽处理；

——通过互联网传输数据必须采用数字证书保证数据的机密性和完整性；

——数字证书的签发须由公共服务平台端的CA进行统一签发。

10.6.3 会话密钥

会话包括报文加密会话密钥、报文MAC会话密钥。

在加密管理客户端和可信服务管理系统之间传送的报文数据时，报文加密会话密钥由报文加密主密钥加上会话特征数据分散生成；

在计算管理客户端和可信服务管理系统之间传送的报文数据的MAC时，报文MAC会话密钥由报文MAC主密钥加上会话的特征数据分散生成；

其中特征数据中包含的随机数由硬件设备随机数发生器产生。

10.7 TSM 平台与应用提供方

10.7.1 传输安全

通讯层传输安全应满足以下安全要求：

——应使用足够强度的加密算法和安全协议保护TSM平台与应用提供方之间的连接，通过互联网传输必须采用数字证书进行双向证书验证；

——如使用SSL协议，应使用3.0及以上相对高版本的协议，取消对低版本协议的支持；

——TSM平台到应用提供方的SSL加密密钥长度应不低于128位，用于签名的RSA密钥长度应不低于1024位，用于签名的SM2密钥长度应不低于256位；

——定时重新协商会话密钥；

——对于应用方下发的个人化数据以及应用下载数据，须通过数字证书等方式确保内容不被篡改；

——如采用数字证书机制，数字证书的签发须由公共服务平台端的CA进行统一签发。

10.7.2 业务数据安全

业务数据处理应满足以下安全要求：

——TSM平台与应用提供方必须对发送的报文关键要素进行签名加密，以供接收方校验报文的真实性及保证关键要素数据的机密性。关键要素包括但不限于应用数据下载安装指令、响应数据等。报文的接收方，用与发送方相同的方法计算MAC或进行验签，并验证报文MAC或签名的正确性；

——通过互联网传输业务数据必须采用数字证书保证数据的机密性和完整性；

——数字证书的签发须由公共服务平台端的CA进行统一签发。

10.8 公共服务平台与 TSM 平台安全技术要求

公共服务平台与 TSM 平台安全技术应满足以下安全要求：

——应使用足够强度的加密算法和安全协议保护公共服务平台与 TSM 平台之间的安全连接，通过互联网传输必须进行双向数字证书验证，例如可使用 SSL/TLS 等协议；

——如使用 SSL 协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持；

——公共服务平台与 TSM 平台的 SSL 加密密钥长度应不低于 128 位，用于签名的 RSA 密钥长度不低于 1024 位，用于签名的 SM2 密钥长度应不低于 256 位；

——定时重新协商会话密钥；

——对于公共服务平台与 TSM 平台之间的敏感数据传输，须采用数字证书等方式确保内容的机密性和完整性；

——数字证书的签发须由公共服务平台端的CA进行统一签发。

10.9 TSM 平台与 TSM 平台互联安全技术要求

在 TSM 平台互联方案下， TSM 平台与 TSM 平台安全技术应满足以下安全要求：

——应使用足够强度的加密算法和安全协议保护 TSM 平台与 TSM 平台之间的安全连接，通过互联网传输必须进行双向数字证书验证，例如可使用 SSL/TLS 等协议；

——如使用 SSL 协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持；

——TMS 平台与 TSM 平台的 SSL 加密密钥长度应不低于 128 位，用于签名的 RSA 密钥长度不低于 1024 位，用于签名的 SM2 密钥长度应不低于 256 位；

——定时重新协商会话密钥；

——对于 TSM 平台与 TSM 平台之间的敏感数据传输，须采用数字证书等方式确保内容的机密性和完整性；

——数字证书的签发须由公共服务平台端的CA进行统一签发。

参 考 文 献

[1] ETSI TS 102.221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics，Release 7

[2] ETSI TS 102.223 Card Application Toolkit (CAT), Release 7

[3] ETSI TS 102.226 Remote APDU structure for UICC based applications V7.2.0

[4] ETSI TS 102.127 Transport Protocol for CAT applications

[5] 3GPP TS 23.048 Security mechanisms for the (U)SIM application toolkit

[6] GlobalPlatform Card Specification v2.1.1

[7] GlobalPlatform Card Specification v2.2.1

[8] GB/T 16649.4-2004 识别卡 带触点的集成电路卡 第4部分：用于交换的行业间命令

[9] GB/T 16649.6-2001 识别卡 带触点的集成电路卡 第6部分：行业间数据元

[10] GB/T 17964 信息安全技术 分组密码算法的工作模式

[11] GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

[12] GB/T 25064 信息安全技术 公钥基础设施 电子签名格式规范

[13] JR/T 0025.7 中国金融集成电路（IC）卡规范 第7部分：借记/贷记应用安全规范