ICS 03.220.20;35.240.15
R 85
备案号:

JT

中华人民共和国交通运输行业标准

JT/T 1059—2016

交通一卡通移动支付技术规范

Technical specification for mobile payment of transport card

2016-04-08发布　　2016-07-01　实施

中华人民共和国交通运输部　发布

总　目　次

R 85

备案号：

JT

中华人民共和国交通运输行业标准

JT/T 1059.6—2016

交通一卡通移动支付技术规范 第6部分：可信服务管理系统

Technical specification for mobile payment of transport card—Part 6:Trusted service management system

2016-04-08发布　　2016-07-01 实施

中华人民共和国交通运输部　发布

目　　次

80

前　言

JT/T 1059《交通一卡通移动支付技术规范》分为8个部分：

——第1部分：总则；

——第2部分：安全单元；

——第3部分：近场支付；

——第4部分：远程支付；

——第5部分：客户端软件；

——第6部分：可信服务管理系统；

——第7部分：终端设备；

——第8部分：检测项目。

本部分为JT/T 1059的第6部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由交通运输部运输服务司提出。

本部分由交通运输信息通信及导航标准化技术委员会归口。

本部分起草单位：北京中交金卡科技有限公司、江苏公共交通一卡通有限公司、北京市政交通一卡通有限公司、南京市市民卡有限公司、北京雷森科技发展有限公司、北京握奇数据系统有限公司、深圳市雪球科技有限公司、北京中交通联科技有限公司、武汉天喻信息产业股份有限公司、恒宝股份有限公司、北京恩安付通科技有限公司。

交通一卡通移动支付技术规范

第6部分：可信服务管理系统

1 范围

JT/T 1059的本部分规定了交通一卡通移动支付可信服务管理系统组成及基本要求、安全要求、业务流程管理要求、平台间接口、报文公共业务组件及接口报文定义。

本部分适用于交通一卡通移动支付可信服务管理系统及相关应用系统的研发、集成和维护，相关产品的设计、开发和制造。

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 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

JT/T 1059.1 交通一卡通移动支付技术规范第1部分：总则

JT/T 1059.2 交通一卡通移动支付技术规范第2部分：安全单元

3 术语和定义

JT/T 1059.1和JT/T 1059.2界定的以及下列术语和定义适用于本文件。

3.1

客户端 client

用于提供用户接口界面，和安全单元配合实现安全单元管理和应用管理功能的应用软件。

3.2

交通一卡通安全域 transport security domain

负责管理其下的身份认证应用、应用发行方辅助安全域和交通一卡通移动支付应用的安全域，由交通一卡通公共服务平台持有交通一卡通安全域的管理权限。

3.3

身份认证应用 traffic identity authentication application

用于存储、管理和验证安全单元及持有人实名身份信息的应用，由交通一卡通公共服务平台持有本应用的管理及使用权限。

3.4

安全单元开放共享部件　secure element share component

安全单元中由交通一卡通公共服务平台持有的、配合交通一卡通公共服务平台实现安全单元空间和能力开放共享的部件。该部件由交通一卡通辅助安全域、身份认证应用及其权限、配置的密钥等基础数据以及可提供的功能共同组成。

3.5

安全单元开放共享服务 secure element share service

交通一卡通公共服务平台通过其持有的安全单元开放共享部件，为移动支付的各应用提供方提供安全单元中空间和能力的共享，满足各应用提供方在安全单元中合理发放应用的需求。

3.6

安全单元载体管理 secure element equipment management

多应用管理 multi-application management

安全单元中负责安全单元生命周期管理、应用生命周期管理的智能卡操作系统、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等的总称。

3.7

支付账户介质识别码 payment account media identifier

唯一标识支付账户介质的代码。

4 缩略语

下列缩略语适用于本文件。

AID——应用程序标识符(Application Identifier)

APDU——应用协议数据单元(Application Protocol Data Unit)

C——国家代码(Country)

CA——数字证书认证中心(Certificate Authority)

COS—— 智能卡操作系统(Chip Operating System)

CN——交互性输入的名字与姓氏(Common Name)

DEK——数据加密密钥(Data Encryption Key)

DN——标识明(Distinguished Name)

L——城市或区域名称(Locality)

MAC——消息认证码(Message Authentication Code)

O——组织名称(Organization)

OU——组织单位名称(Organization Unit)

PAMID——支付账户介质识别码(Payment Account Media Identifier)

PIX——扩展的专用应用标识符(Proprietary Application Identifier Extension)

RA——用户注册中心(Registration Authority)

RCA——根证书认证机构(Root Certificate Authority)

SCP——安全通道协议(Secure Channel Protocol)

SE——安全单元(Security Element)

SEI-TSM——SE发行方可信服务管理(SE Issuer Trusted Service Management)

S-ENC——安全通道加密密钥(S-Encryption)

S-MAC——安全通道报文认证密钥(S-Message Authentication Code)

SP-TSM——服务提供方可信服务管理(Service Provider Trusted Service Management)

SSD——辅助安全域(Supplementary Security Domain)

ST——州或省份名称(State)

TIDAA——身份认证应用(Traffic Identity Authentication Application)

T-MTPS——交通一卡通公共服务(Transport-Mobile Trustable Public Service)

TOKEN——令牌化(Tokenization)

TSD——交通一卡通安全域(Transport Security Domain)

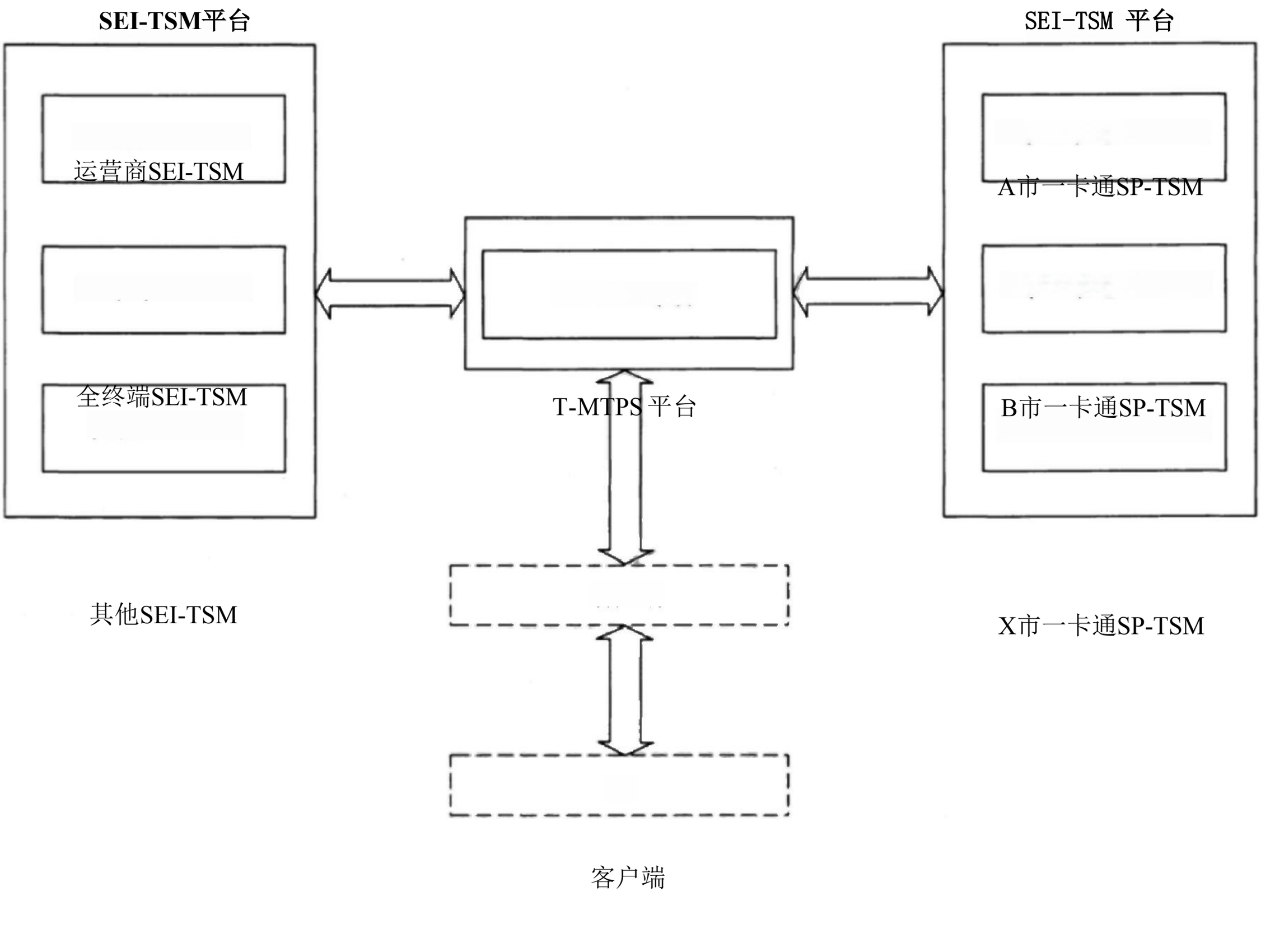
TSM____可信服务管理(Trusted Service Management)

3DES——三重数据加密算法(Triple Data Encryption Algorithm)

5 系统组成及基本要求

5.1 系统组成

交通一卡通移动支付可信服务管理系统由T-MTPS平台、SEI-TSM平台和SP-TSM平台三个平台共同组成，如图1所示。



SE

图 1　系统结构图

5.2　基本要求

5.2.1　T-MTPS 平台

5.2.1.1　概述

T-MTPS平台是交通一卡通移动支付参与各方认可的可信第三方平台。T-MTPS平台主要面向TSM 平台运营方、SE 发行方、应用提供方、服务提供方和用户，负责连接SEI-TSM 平 台 和SP-TSM 平 台 ，实现平台之间的资源共享。T-MTPS平台应提供跨系统交互路由、应用共享、SE 可信及开放共享四项服务，实现跨系统间的交易数据、用户数据、应用数据等信息数据的传递。

5.2.1.2　平台内实体间关系及其功能

5.2.1.2.1　平台内实体间关系

密钥管理系统和CA 系统作为T-MTPS 平台支持系统，应实现对T-MTPS平台业务功能的支持，

T-MTPS平台间关系如图2所示。

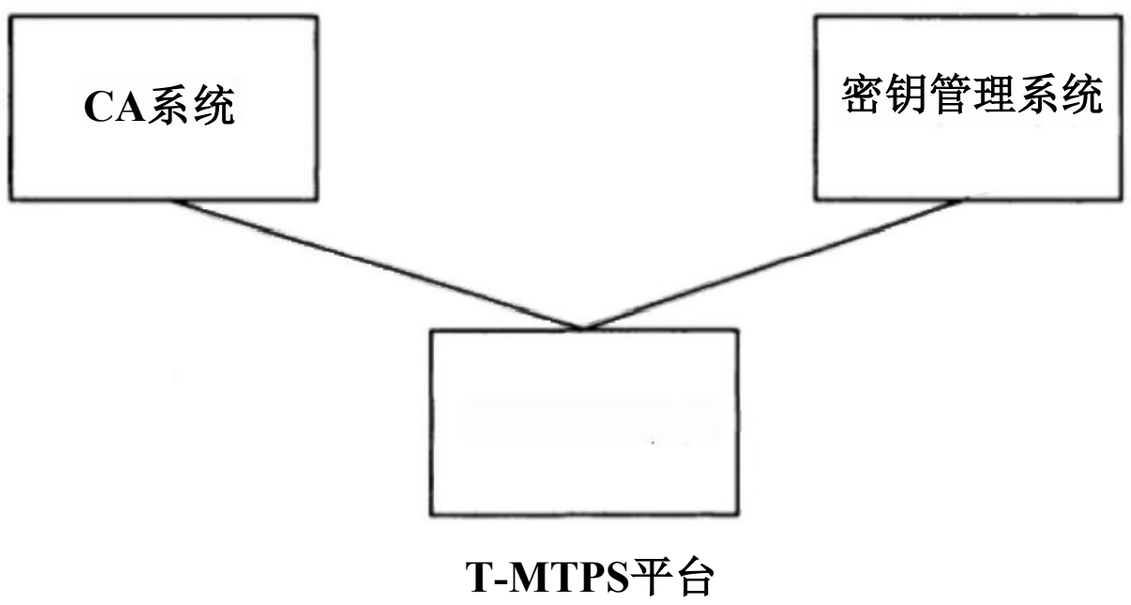


图2 T-MTPS 平台内实体间关系图

5.2.1.2.2 T-MTPS平台功能

T-MTPS 应具备如下功能：

a) 机构接入管理；

b) 应用信息配置管理；

c) 应用盘本信息配置管理；

d) SE 初始化；

e) 应用提供方SSD管理；

f) 交通一卡通移动支付应用管理。

5.2.1.2.3 CA 系统功能

CA系统应具备如下功能：

a) 证书申请；

b) 证书验证；

c) 证书更新。

5.2.1.2.4 密钥管理系统功能

密钥管理系统应具备如下功能：

a) 密钥申请；

b) SCPO2 会话密钥生成；

c) 密钥更新；

d) 数据转加密；

e) 3DES 加密、解密运算。

5.2.2 SEI-TSM 平台

SEI-TSM 应负责管理 SE 载体与多应用管理。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、应用管理授权和应用生命周期管理。本部分不对SEI-TSM平台的结构进行规定，但SEI-TSM与 T-MTPS 平台对接流程应符合本部分要求。

5.2.3 SP-TSM平台

SP-TSM 应负责提供对本机构自有应用进行管理的服务，确保自有应用能进行空中下载、圈存等功能需求。本部分不对SP-TSM的平台结构进行规定，但SP-TSM与 T-MTPS平台对接流程应符合本部分要求。

6 安全要求

6.1 T-MTPS 平台安全要求

6.1.1 SE 应用下载

6.1.1.1 基本要求

在委托管理模式下应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，令牌主要包括用户应用的加载令牌(Load Token)、应用的安装令牌(Install Token)以及应用的迁移令牌(Extradition Token)。

用于进行Token 计算的密钥算法为SM2、SM3、RSA、SHA-256。

6.1.1.2 Token计算

6.1.1.2.1 Load Token计算

Load Token是向卡发行者提供将应用代码装载到特定安全域的证明，计算流程如图3所示。

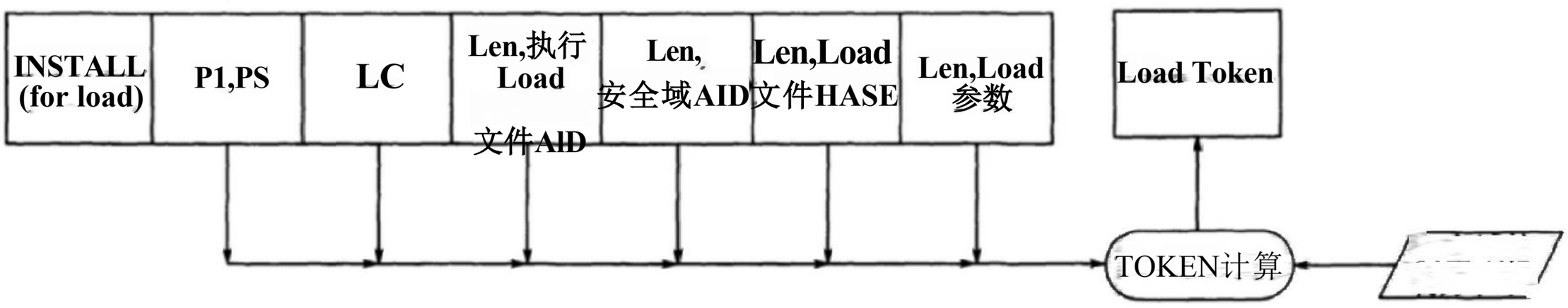


图3 Load Token计算输入结构

产生 Load Token应遵循以下要求：

a) 加载文件HASH应包含在签名当中；

b) Load包 AID、安全域AID应包含在签名当中；

c) Load Token应由具备“令牌验证权限”的安全域提供者发行。

Load Token输入字段见表1。

表 1 Load Token 输入字段

字 段	长 度	字 段	长 度
P1	1	安全域AID	5～16
P2	1	Load文件HASH值长度	1
LC	1	Load文件HASH值	20
Load包AID长度	1	Load参数域长度	1~2
Load包AID	5～16	Load参数域	0～n，其中TAG‘C9’前16字节表示为PAMID
安全域AID长度	1		

6.1.1.2.2 Install Token计算

Install Token是向卡发行者提供将应用代码安装到特定卡上的证明，计算流程如图4所示。

产生 Install Token应遵循以下要求：

a) 包 AID、类 AID、实例AID应包含在签名当中；

b) 只有能够通过 AID 被选择的实例，且该实例 AID 包含在签名数据当中，才能被使用；

c) 只有在签名中指定权限的应用才能安装；

d) Install Token 应由具备“令牌验证权限”的安全域提供者发行。

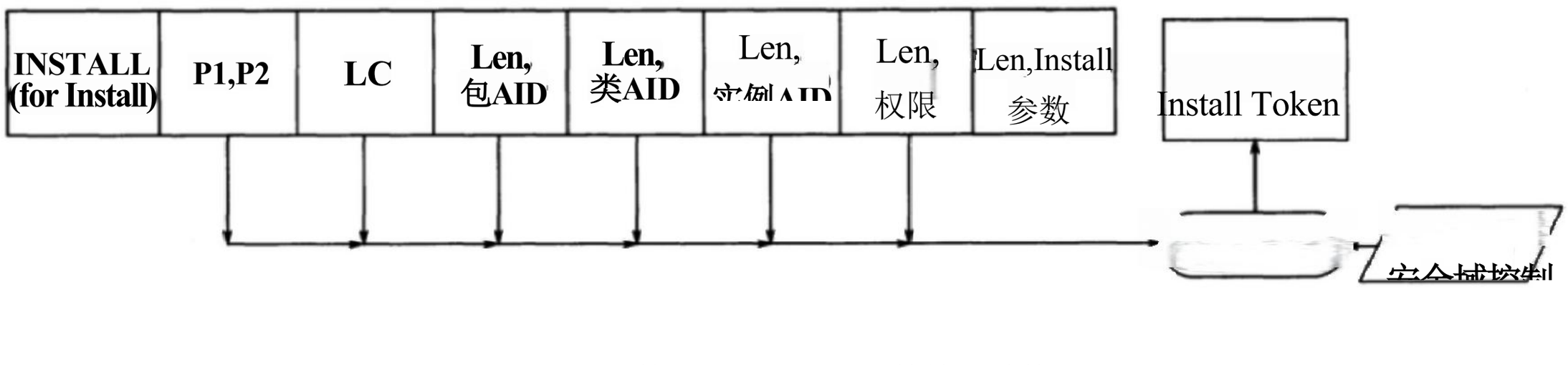


图 4 计算Install Token 计算输入结构

Install Token 输入字段见表2。

表 2 Install Token输入字段

字 段	长 度	字 段	长 度
P1	1	实例AID长度	1
P2	1	实例AID	5～16
LC	1	权限长度	1
包AID长度	1	权限(byte-1-byte2-byte3)	1或3
包AID	5～16	可选参数域长度	1
类AID长度	1	可选参数域	0～n,其中TAG’C9 前16字节表示为PAMID
类AID	5～16		

6.1.1.2.3 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，计算流程如图5所示。

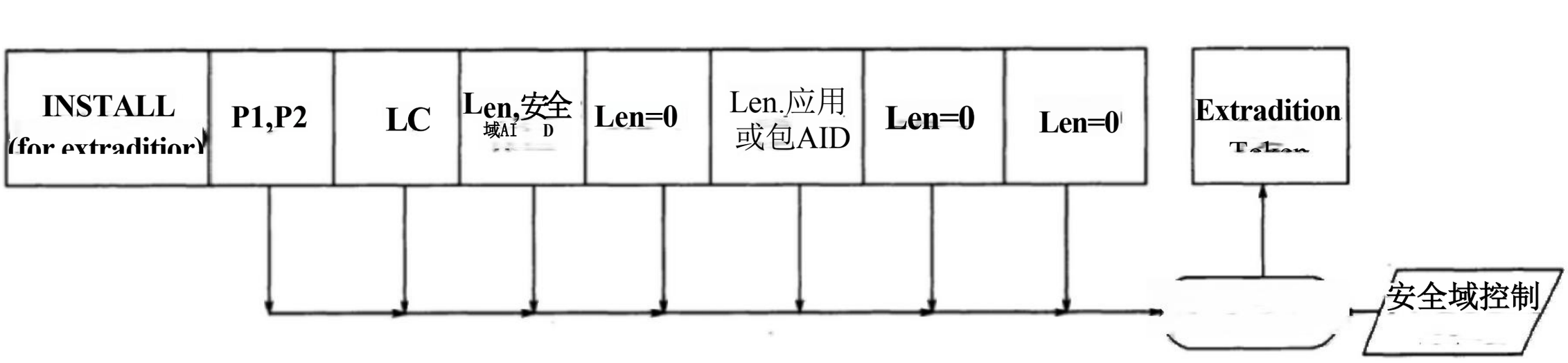


图5 Extradition Token计算输入结构

产生Extradition Token 应遵循以下要求：

a)　应用或者包AID 应包含在签名里面才可以被迁移；

b)　令牌只能由具备“令牌验证权限”的安全域提供者发行。

Extradition Token 输入字段见表3。

表3 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AID长度	1	强制
安全域AID	5～16	可选
Len=0	1	强制
包AID	5～16	强制
应用或包AID长度	1	强制
应用或包AID	5～16	强制
Len =0	1	强制
Len =0	1	强制

6.1.2 TSM 平台与应用提供方

6.1.2.1 传输安全

通信层传输安全要求如下：

a) 应使用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，互联网传输应采用数字证书进行双向证书验证；

b) 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；

c)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；

d) 定时重新协商会话密钥；

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

f) 如采用数字证书机制，数字证书应由T-MTPS平台端的CA 进行统一签发。

6.1.2.2 业务数据安全

业务数据处理安全要求如下：

a)TSM 平台与应用提供方应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，使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。

b) 通过互联网传输业务数据应采用数字证书保证数据的机密性和完整性。

c) 数字证书应由T-MTPS平台端的CA 系统进行统一签发。

6.1.3 T-MTPS平台与TSM 平台间安全技术要求

T-MTPS平台与TSM平台安全要求如下：

a) 应使用加密算法和安全协议保护T-MTPS平台与TSM平台之间的安全连接，通过互联网传输应进行双向数字证书验证，例如可使用SSL/TLS等协议；

b) 如使用SSL协议，应使用3.0及以上相对高版本的协议；

c)T-MTPS 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；

d) 定时重新协商会话密钥；

e) 对 于T-MTPS平台与TSM平台之间的敏感数据传输，应采用数字证书等方式确保内容的机密性和完整性；

f) 数字证书应由T-MTPS 平台端的CA系统进行统一签发。

SE的安全通道应支持SCPO2协议，模式参数i=‘15’,SCPO2 的密钥集定义见表4。

表 4 SE 安全通道密钥集定义

密 钥 标 识	密钥版本 ‘20	密钥版本 ‘21’	……	密 钥 版 本 ‘2F’
	Counter 1	Counter 2		Counter n
密钥标识1	S-ENC 1	S-ENC 2	…	S-ENC n
密钥标识2	S-MAC 1	S-MAC 2	…	S-MAC n
密钥标识3	DEK 1	DEK 2	…	DEK n
注：密钥版本取值范围为‘20’～‘2F’;密钥标识取值范围为‘01’～*03’。				

6.2 密钥体系与密码算法

6.2.1 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。对称密钥体系和非对称密钥体系均支持国产密码算法和国际密码算法。

6.2.2 密码算法

6.2.2.1 对称算法

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

SM4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 算法实现应按照GM/T 0002的要求。

3DES 加密是使用双长度(16 byte)密钥将8 byte明文数据块加密成密文数据块。

6.2.2.2 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，可用于认证中心、SE 的签名与认证。非对称算法中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。

SM2算法是一种椭圆曲线公钥密码算法，密钥位长为m(m=256)。SM2 算法实现应按照GM/T 0003的要求。

6.2.2.3 杂凑算法

杂凑算法支持国产的SM3算法和国际SHA-256算法。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算法应按照GM/T 0004的要求。

6.3 CA系统

6.3.1 系统架构

CA系统在密码服务系统的基础之上，通过建设CA系统，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通常采用RCA-CA-RA 三层构成：

a) RCA为根认证机构；
b) CA 为数字证书认证中心，提供数字证书签发、发布、管理、撤销等服务，CA机构签发的证书应由合法的第三方电子认证服务机构产生；
c) RA为用户证书申请注册中心，分为远程注册中心和本地注册中心。RA中心提供数字证书的申请注册、用户身份审核等服务。

6.3.2 CA 系统提供的服务

CA 系统主要提供如下服务：

a) 证书的签发和管理；
b) 证书撤销列表的签发和管理；
c) 证书/证书撤销列表的发布；
d) 系统自身的安全审计与安全管理；
e) 用户注册中心的设立、审核、维护及管理。

6.3.3 用户注册中心

RA的具体功能如下：

a) 用户数字证书申请的注册受理；
b) 用户真实身份的审核；
c) 用户数字证书的申请与下载；
d) 用户数字证书的撤销与更新的受理；
e) 证书受理核发点设立的审核及管理。

6.3.4 数字证书

6.3.4.1 功能

数字证书格式为X.509, 应符合GB/T 20518的要求。数字证书主要实现以下功能：

a)T-MTPS　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；

b)　对 T-MTPS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。

6.3.4.2　信息

6.3.4.2.1　数字证书中必要包含的信息包括：

a)　主体名称域中的 DN 信息；

b)　自定义扩展域中的身份信息以及SE 安全等级信息。

6.3.4.2.2 数字证书中信息设定规则如下：

a) 主体名称域中的DN信息：用于唯一标识用户的X.500 名称，通常需要设定CN、0U、0、C等组成部分：

1) CN部分：用于表示 PAMID;

2)0U 部分：用于表示证书申请机构，如OU=XX 机构；

3) 0部分：用于表示CA 系统的名称，如0=XXCA;

4)C 部分：用于表示用户所属国家或地区的英文简称，全部大写，如中国用户为C=CN。

b) 自定义扩展域中的身份信息以及SE 安全等级信息，通常需要设定证件类型、证件号码及SE安全等级：

1）证 件 类 型(IdentityCode): 按照表5的规定进行标识，如个人使用身份证申请证书时的编码为IdentityCode =0;

2）证 件 号 码(InsuranceNumber): 填写证件号码，在个人申请SE 数字证书时有此项扩展项，如 InsuranceNumber =110101190006162005;

3)SE 安全等级(SESecClassified): 在 SE 注册申请证书时应填写SE 属于某个级别的安全等级。

表 5 证 件 类 型

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

7 业务流程管理要求

7.1 T-MTPS 平台机构接入管理

T-MTPS平台根据TSM平台运营方、应用提供方和SE 发行方等机构提交的注册申请信息为其分配机构ID。注册完成后，T-MTPS平台允许相应机构接入并提供服务。

7.2 应用信息配置管理

7.2.1 基本要求

T-MTPS 平台负责管理应用提供方 SSD, 机构接入时提交的交通一卡通移动支付应用通过审查后，T-MTPS平台为该应用统一分配应用AID（包括包AID、类 AID 和实例AID), 并对应用的注册、测试、暂停、上线发布和下线进行管理。

7.2.2　AID 分配原则

AID由应用提供者标识符(RID)、专有标识符、应用类型标识符、机构代码、应用编码、保留位和扩展编码构成。T-MTPS 平台统一为交通行业移动支付应用或安全域分配唯一的AID。

参照ISO/IEC　7816-4的要求，T-MTPS平台对交通行业支付应用和安全域分配的AID 编码要求见表6。

表6 AID 编 码 规 则

AID						
RID″	PIX					
	业务/应用编码				保留	扩展编码
	专有标识符	应用类型	机构代码	应用编码		
B1～B5	B6	B7～B8	B9～B13	B14	B15	B16
5字节	1字节	2字节	5字节	1字节	1字节	1字节
“取五个字节常数值(十六进制表示):A000000632(RID)。 B6固定为01。 000-保留；0105-电子钱包；0106-电子现金。 d由T-MTPS平台分配给应用所属机构。 • 采用正整数编码：0x00表示辅助安全域；0x01表示应用。 保留为将来扩展。 “标识AID的扩展信息，按位(b8 b7 b6 b5 b4 b3 b2 b1)编码，其中，b8 b7取值：00-包AID;01-类AID;10-实例AID;11-保留。						

7.2.3 应用注册管理

7.2.3.1 T-MTPS平台负责对所有交通一卡通移动支付应用进行注册管理。应用发行方将应用及其信息向T-MTPS平台提交注册申请，T-MTPS平台审核后，为应用分配相关的AID资源信息，流程如图6所示。

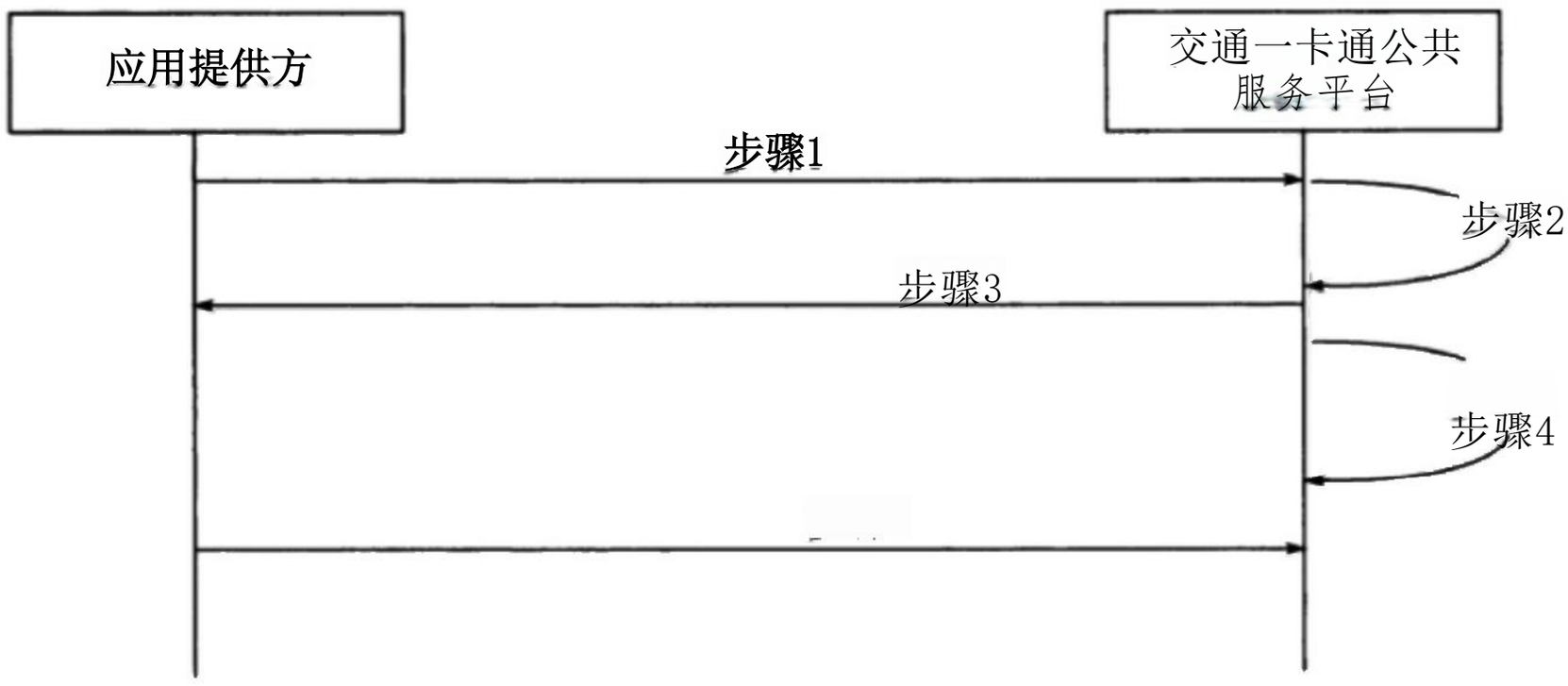


图 6 应用注册管理流程图

7.2.3.2 图6中的步骤说明如下：

a) 步骤1:交通一卡通应用提供方登录T-MTPS平台填写应用注册申请信息和提交相关材料。

b) 步骤2:T-MTPS平台将交通一卡通应用提供方填写的应用注册信息和相关材料信息登记入库。

c) 步骤3 :T-MTPS平台记录填写的信息及申请材料，并向应用提供方提示操作状态。

d) 步骤4:由人工对交通一卡通公共服务平台中的应用注册信息和相关材料信息进行审核。

e) 步骤5:T-MTPS平台业务管理员进行信息审核及材料审查，并为审查合格的应用分配AID,应

用提供方上传应用，登记备案。信息审核通过后业务管理员将应用状态更新为审批通过；审批通过的交通一卡通移动支付应用可以进行调测、上线发布。

7.2.4 应用状态管理

T-MTPS平台的应用状态包括：待审批、调测、上线、暂停下载、下线和注销。各状态说明见表7。

表 7 应用状态说明表

应 用 状 态	说　　明
待审批	应用初始状态：该状态下，应用提供方提交的应用申请等待业务管理员审批
调测	该状态下，应用提供方可对申请应用进行版本配置和版本测试，应用只对测试用户可见
上线	应用的正常状态：该状态下，应用对用户可见。合作伙伴可进行新版本的配置及测试
暂停下载	应用的管理状态：该状态下，应用只对已下载用户可见(仅限删除)。应用提供方可进行新应用版本的配置及测试
下线	应用的管理状态：该状态时，应用只对已下载用户可见(仅限删除)。应用提供方不能进行新应用版本的配置及测试
注销	应用的最终状态：该状态时，应用只对已下载用户可见(仅限删除),且应用不可重新上线

7.3 应用版本信息配置管理

7.3.1 CAP 文件配置

T-MTPS 平台应具备应用下载的功能。应用发行方可将自有CAP 文件及信息提交至T-MTPS平台进行配置管理或采用通用交通一卡通移动支付应用。

CAP 文件的集合称为“CAP 包”。平台以“包”为单位对CAP 文件进行管理和控制，即同一包AID可以对应多个版本，每个版本对应一个CAP包文件，同一SE 上不应存在同一个AID的多个CAP 包文件，如图7所示。

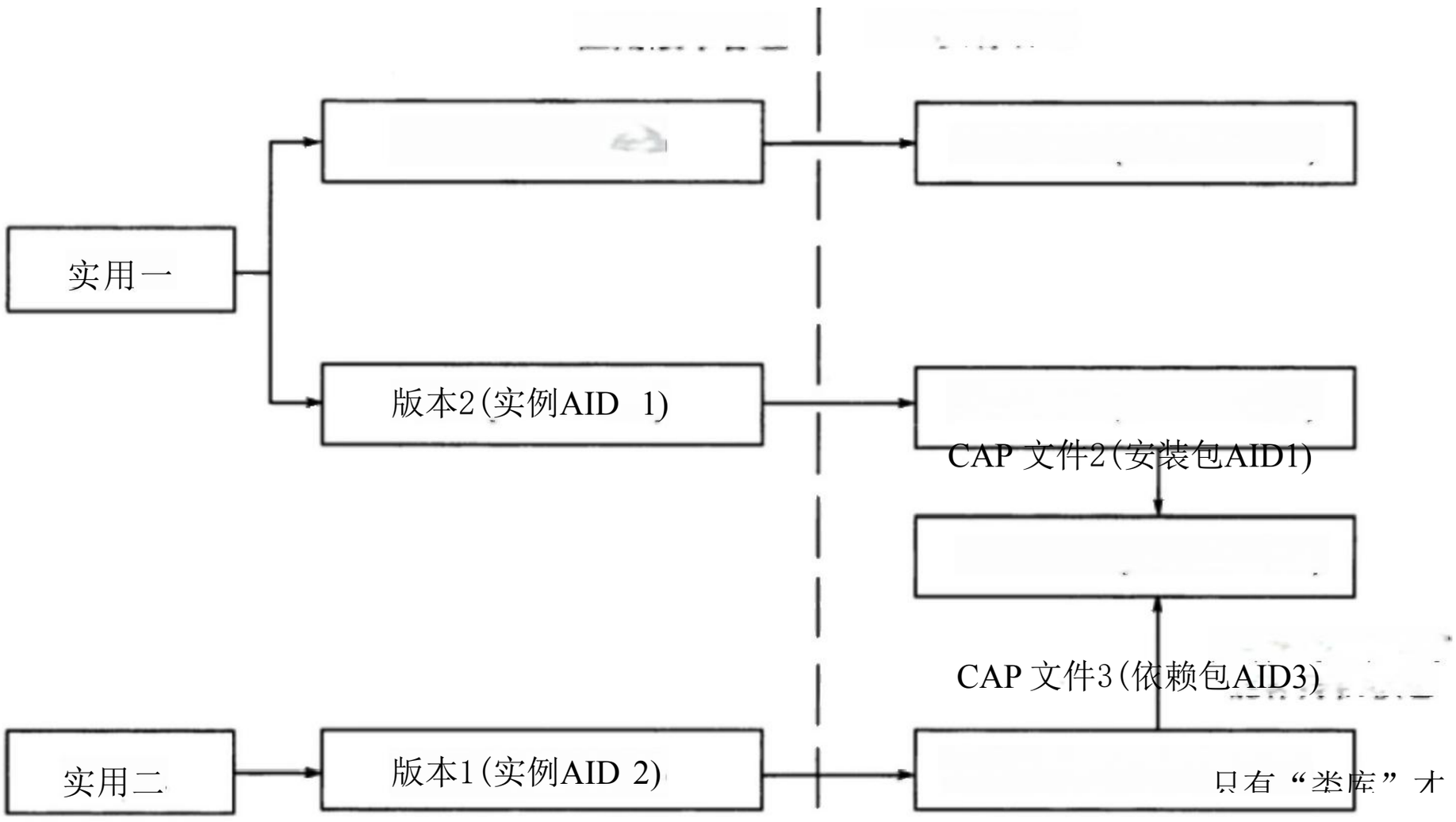


图 7　应用版本与CAP 文件的对应关系图

交通一卡通应用发行方应提供如下配置信息：

a) 包名称；
b) 包 AID;
c) 类 AID;
d) 包版本；
e) 包描述；
f) 加载参数等。

CAP包文件导入时，应对哈希值(HASH) 进行验证，不通过验证，不允许导入。

7.3.2 应用版本信息管理

7.3.2.1 基本要求

应用版本信息管理应符合如下要求：

a) 一个应用对应多个应用版本；
b) 不同的应用版本之间互斥，即同一个应用在用户卡片上只存在一个版本；
c) 高版本的应用兼容低版本的应用。

7.3.2.2 应用版本信息

交通一卡通移动支付应用发行方在进行应用版本配置时，应提供的属性参数见表8。

表 8 应用版本信息表

属 性 名 称	说 明
版本号	系统以此作为新旧版本的判断依据
实例AID	一个版本应用对应一个Applet实例AID,允许不同版本应用的实例AID相同
应用安装参数	应用安装时所需的参数信息
应用安装权限	应用所具有的权限，参见GPCS V2.2.1规范要求
版本简述	简要描述此版本的功能，用以在门户展现应用时使用
版本状态	用以控制应用版本发布流程管理
应用所占RAM空间大小	应用所占的RAM空间大小
应用所占NVM空间大小	应用所占的非挥发存储器大小

7.3.2.3 应用版本状态

应用版本状态包括待测试、测试、发布、暂停及下线。各状态说明见表9。

表 9 应用版本状态

状 态 名 称	说 明
待测试	应用提供方和业务管理员对应用版本进行安装参数配置。配置完成后，合作伙伴向业务管理员提交应用版本测试申请
测试	测试人员对所测试的应用版本进行功能测试

发布	应用版本通过测试，经验收合格后。业务管理员将该应用版本状态置为“发布”
暂停	应用版本的管理状态。 此状态下，应用版本的配置和测试暂停。对于已发布的应用版本，不参与应用下载的用户适配环节
下线	应用版本不可用

7.4 SE 初始化

7.4.1 基本要求

TSD和 TIDAA在第一次下载交通一卡通应用时应进行初始化和激活。

TSD负责其下交通一卡通应用和安全域的管理操作。TSD 安全域的初始化密钥采用两级分散体系，如图8所示。

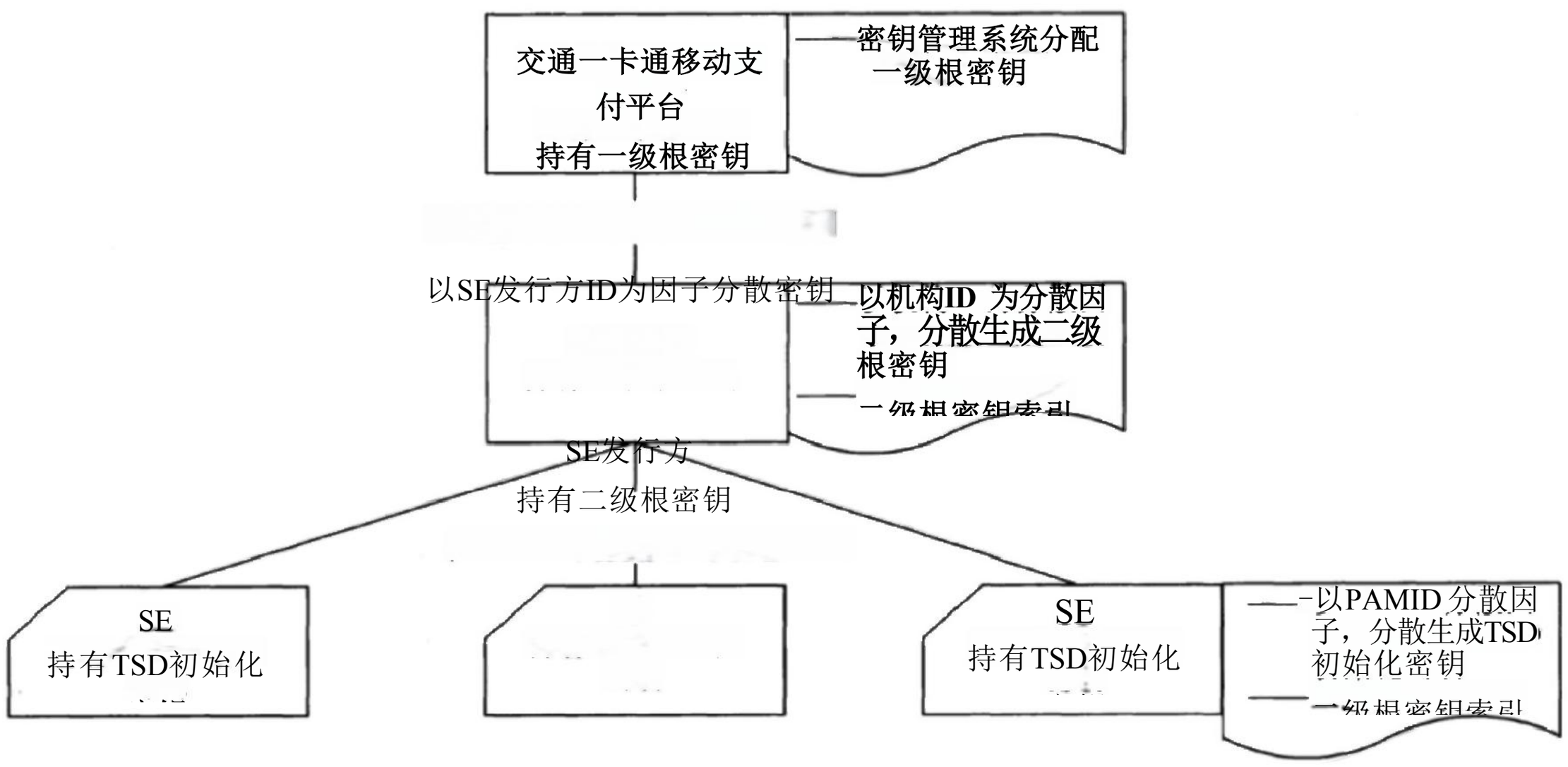


图8 TSD 安全域初始化密钥分散体系

7.4.2 预置模式下 SE 初始化

预置模式下SE 初始化流程如图9所示，预置模式下SE 初始化步骤如下：

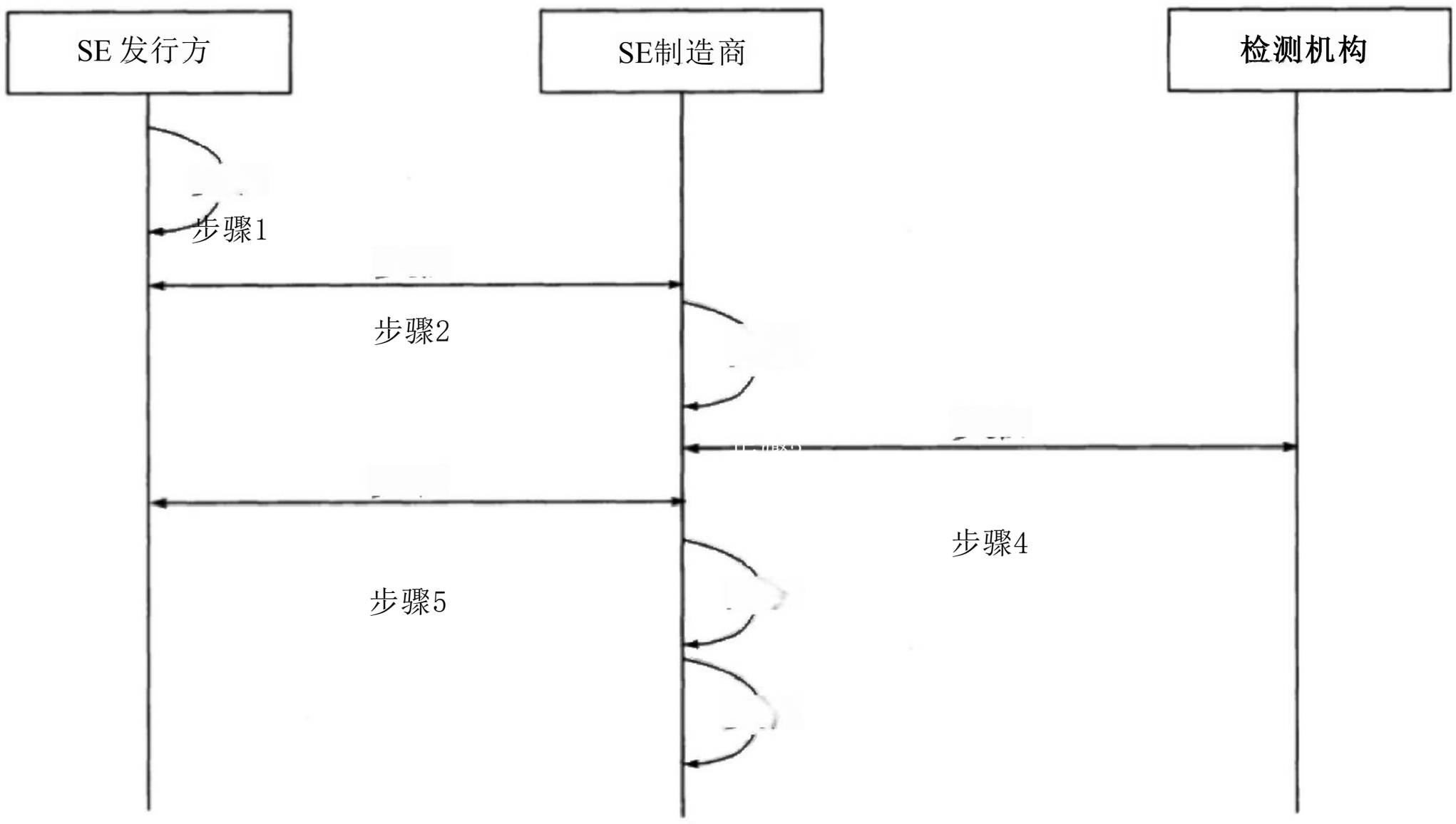


图 9　预置模式 SE 注册流程

a) 步骤1:SE 发行准备，发行方准备数据；

b) 步骤2:SE 发行方委托 SE 制造商生产；

c) 步骤3:接受委托的SE 制造商完成COS灌装；

d) 步骤4:SE 制造商将SE 提交检测机构进行检测；

e) 步骤5:检测通过的SE 向发行方获取对应分配的 PAMID(PAMID一旦写入则不可进行更改操作)；

f) 步骤6:SE 制造商完成应用预置；

g) 步骤7:SE 制造商将PAMID写入TSD进行存储，完成SE 初始化。

7.4.3 空发模式下 SE 初始化

空发模式下SE 初始化流程如图10所示，空发模式下SE 初始化步骤如下：

a) 步骤1:客户端向T-MTPS平台请求获取全网应用列表；

b) 步骤2:T-MTPS平台响应全网应用查询结果；

c) 步骤3:客户端首先进行判断TSD是否创建；

d) 步骤4:如果客户端判断TSD没有创建，则向SEI-TSM平台发起TSM 创建请求；

e) 步骤5:SEI-TSM平台判断TSD是否创建；

f) 步骤6:若未创建，与客户端交互完成TSD创建操作(平台生成PAMID写 入TSD,PAMID一 旦写入则不可进行更改操作)；

g) 步骤7:SEI-TSM平台在TSD创建成功后通知T-MTPS平台；

h) 步骤8:客户端与T-MTPS平台交互完成TIDAA下载及个人化操作；

i) 步骤9:T-MTPS平台校验卡片返回结果，若执行成功则将应用的状态同步至SEI-TSM。

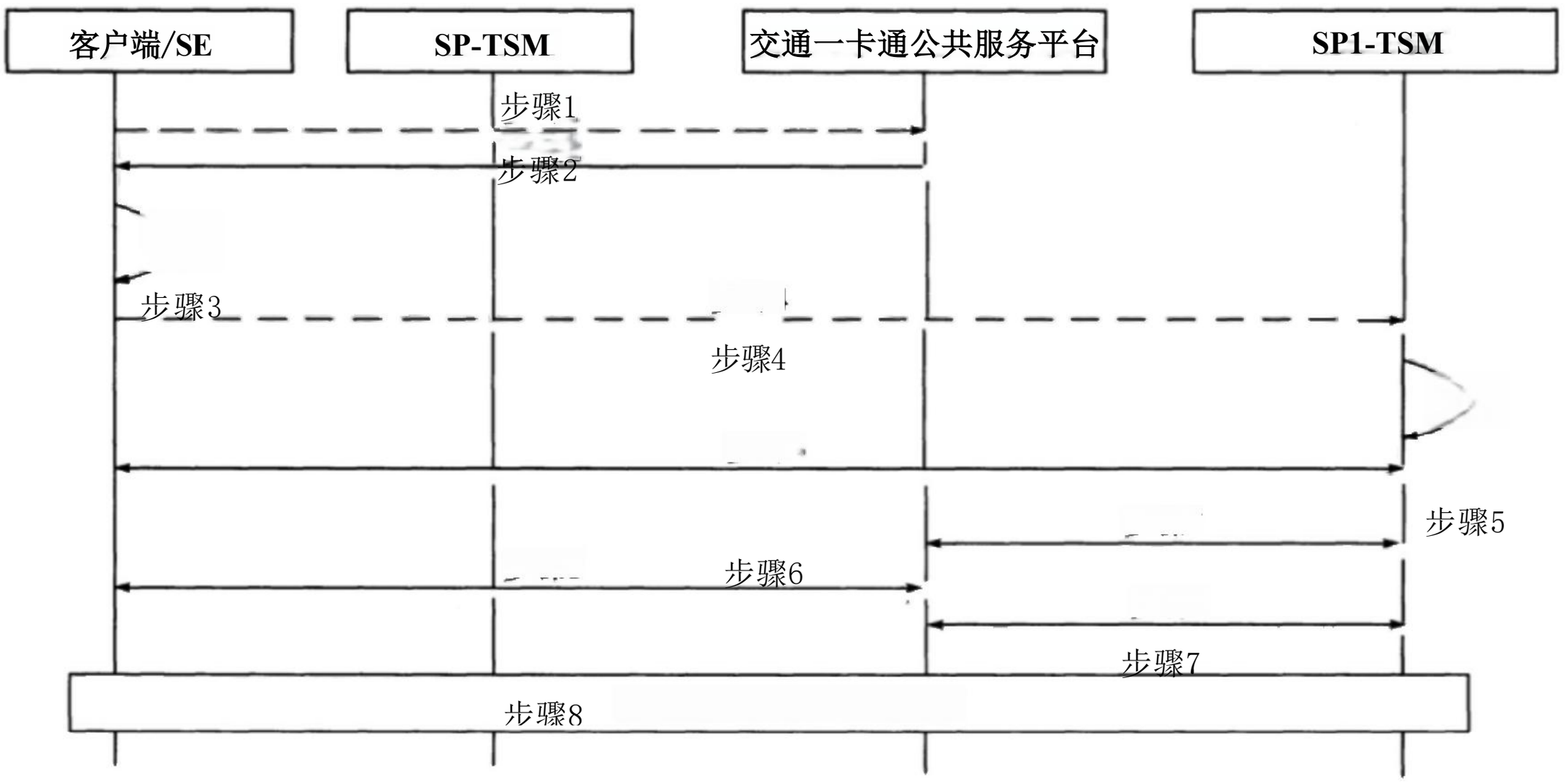


图10 空发模式SE 注册流程

7.5 应用提供方SSD 管理

7.5.1　基本要求

以 T-MTPS平台作为可信第三方的开放共享模式中，要求SE 中配置TSD 。T-MTPS平台可以通过TSD安全域为交通一卡通移动支付应用提供方进行 SSD 的生命周期管理，包括辅助安全域的创建、删除、个人化、锁定和解锁。应用提供方 SSD创建采用委托管理模式。