ICS 点击此处添加ICS号

点击此处添加中国标准文献分类号

|  |
| --- |
|  |

DB11

北京市地方标准

DB11/T 159.6—20xx

|  |
| --- |
|  |

市政交通一卡通技术规范第6部分：移动支付

Municipal administration & communication card technology specifications—Part 6:Mobile payment

|  |
| --- |
|  |
|  |

20XX - XX - XX发布

20XX - XX - XX实施

北京市市场监督管理局   发布

目  次

[前言 IV](#_Toc87124809)

[1 范围 1](#_Toc1870301256)

[2 规范性引用文件 1](#_Toc1435068453)

[3 术语和定义 1](#_Toc806650114)

[4 缩略语 3](#_Toc379969909)

[5 移动支付系统 4](#_Toc1685378032)

[5.1 系统组成 4](#_Toc839279894)

[5.2 系统功能 5](#_Toc1104584962)

[5.2.1 安全单元 5](#_Toc1910811666)

[5.2.2 可信服务管理系统 5](#_Toc1541213224)

[5.2.3 客户端软件 5](#_Toc222905654)

[6 安全单元 6](#_Toc1163846410)

[6.1 一般性要求 6](#_Toc1485555994)

[6.1.1 物理特性 6](#_Toc1094711136)

[6.1.2 接触通道 6](#_Toc1317658903)

[6.1.3 非接触通道 6](#_Toc1041814857)

[6.1.4 逻辑结构 6](#_Toc1348127608)

[6.1.5 硬件方案结构 6](#_Toc2028231806)

[6.1.6 供电要求 6](#_Toc1484034611)

[6.2 多应用管理 7](#_Toc1294630819)

[6.2.1 基本功能 7](#_Toc555863529)

[6.2.2 安全域 7](#_Toc844467453)

[6.2.3 全局服务应用 7](#_Toc245059548)

[6.2.4 运行时环境 7](#_Toc1989671937)

[6.2.5 平台环境 7](#_Toc1948377722)

[6.2.6 平台API 8](#_Toc1553724198)

[6.2.7 SE应用管理 8](#_Toc41448266)

[6.2.8 生命周期模型 8](#_Toc836305034)

[6.3 基本命令 8](#_Toc498236823)

[6.4 密钥要求 8](#_Toc827544508)

[6.5 安全通信 8](#_Toc1436447984)

[6.6 应用个人化服务 8](#_Toc370107514)

[6.6.1 基本功能 8](#_Toc1284346086)

[6.6.2 运行时消息流 9](#_Toc1646531405)

[6.6.3 安全域访问 9](#_Toc779048593)

[6.7 应用选择服务 9](#_Toc261906792)

[7 典型业务 9](#_Toc1673460441)

[7.1 业务分类 9](#_Toc256307128)

[7.2 开卡 9](#_Toc2049188061)

[7.2.1 交易模型 9](#_Toc1508494288)

[7.3 消费 10](#_Toc71561934)

[7.3.1 交易模型 10](#_Toc150582418)

[7.3.2 典型交易时间 10](#_Toc1102963160)

[7.4 充值 10](#_Toc422989216)

[7.4.1 交易模型 10](#_Toc1008881742)

[7.5 退卡 11](#_Toc1892044729)

[7.5.1 交易模型 11](#_Toc1805399174)

[7.6 迁卡 11](#_Toc1547468955)

[7.6.1 交易模型 11](#_Toc136277868)

[8 可信服务管理系统 12](#_Toc1204559774)

[8.1 系统功能 12](#_Toc707781349)

[8.2 接入机构管理 13](#_Toc769211910)

[8.3 应用配置管理 13](#_Toc293016430)

[8.3.1 基本要求 13](#_Toc547136439)

[8.3.2 AID分配原则 13](#_Toc197153819)

[8.3.3 应用注册管理 14](#_Toc2144452259)

[8.4 SE初始化 14](#_Toc591069412)

[8.4.1 基本要求 15](#_Toc1991740109)

[8.4.2 SE初始化 15](#_Toc200922527)

[8.5 移动支付管理 16](#_Toc1060618205)

[8.5.1 基本功能 16](#_Toc1695901335)

[8.5.2 应用下载 16](#_Toc1610774361)

[8.5.3 应用删除 17](#_Toc1105831245)

[8.5.4 应用锁定/解锁 18](#_Toc1382253577)

[8.5.5 应用个人化 19](#_Toc57775393)

[8.6 平台安全要求 20](#_Toc368421707)

[9 客户端软件 20](#_Toc868275248)

[9.1 软件架构 20](#_Toc950711771)

[9.2 基本功能 21](#_Toc1334401517)

[9.2.1 注册 21](#_Toc1114570598)

[9.2.2 开卡 21](#_Toc88187805)

[9.2.3 消费 21](#_Toc408722205)

[9.2.4 充值 21](#_Toc1741396329)

[9.2.5 退卡 21](#_Toc1740960187)

[9.2.6 迁卡 21](#_Toc853172534)

[9.2.7 默认应用设置 21](#_Toc522467919)

[9.2.8 信息查询 21](#_Toc57682050)

[9.2.9 密码管理 22](#_Toc947089553)

[9.2.10 版本升级 22](#_Toc585325707)

[9.3 应用模型 22](#_Toc2094054289)

[9.4 安全要求 22](#_Toc1808428187)

[9.4.1 人机交互安全 22](#_Toc916482918)

[9.4.2 软件安全 22](#_Toc1575686542)

[9.4.3 数据安全 23](#_Toc1942860237)

[9.4.4 通信安全 23](#_Toc1163150624)

[9.5 管理要求 23](#_Toc528898927)

[9.5.1 设计要求 23](#_Toc769451156)

[9.5.2 开发要求 23](#_Toc19056658)

[9.5.3 发布要求 23](#_Toc310187603)

[9.5.4 维护要求 23](#_Toc1380232352)

前  言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是DB11/T 159《市政交通一卡通技术规范》的第6部分。DB11/T 159已经发布了以下部分：

——第1部分：总则；

——第2部分：卡片；

——第3部分：终端；

——第4部分：安全；

——第5部分：检测；

——第6部分：移动支付。

本文件由北京市交通委员会提出并归口。

本文件由北京市交通委员会组织实施。

本文件主要起草单位：北京市政交通一卡通有限公司、北京市智慧交通发展中心。

本文件主要起草人员：

本文件及其所代替文件的历次版本发布情况为：

——本次为首次发布。

市政交通一卡通技术规范

第6部分：移动支付

1. 范围

本文件规定了市政交通一卡通系统移动支付的组成、功能，及安全单元、可信服务管理系统、客户端软件技术和管理要求。

本文件适用于市政交通一卡通系统移动支付的规划、设计、研发、运营、管理和维护。

1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。 其中，注日期的引用文件，仅所注日期对应的版本适用于本文件；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。

JT/T 978 城市公共交通IC卡技术规范

JT/T 1059 交通一卡通移动支付技术规范

DB11/T 159.2 市政交通一卡通技术规范 第2部分：卡片

DB11/T 159.4 市政交通一卡通技术规范 第4部分：安全

1. 术语和定义

DB 11/T 159.1界定的以及下列术语和定义适用于本文件。



初始化 initialization

在卡发行前，由卡的发行机构对IC卡进行格式化，并在卡中写入卡的发行信息的过程。



安全单元 secure element （SE）

负责对具有安全认证的交易关键数据的安全存储和运算，且支持多应用管理及运行安全的移动支付安全载体。

[来源：JT/T 1059.1—2016,3.12]



个人化 personalization

SE发行者职责的最后流程，通过该流程配置SE、装载安全参数和设置密钥。个人化流程结束后，SE就可以完全操作并可发到最终用户手中。

[来源：JT/T 1059.8—2016,3.16]



移动支付 mobile payment

用户使用移动支付终端对所消费的服务进行账务支付的一种方式。

[来源：JT/T 1059.1—2016,3.2，有修改]



支付平台 payment platform

为用户提供货币支付及资金清算等服务的第三方平台。



密钥 key

对数据进行加密时使用的秘密参数，可利用密钥对密文解密，使原数据文件恢复。



终端设备 terminal

能完成一卡通卡应用的IC卡读写设备，从物理配置上分为A、B两类终端，两类终端都可以用来实现充值、消费或服务功能。



移动支付终端 mobile payment terminal

具有交通一卡通移动支付应用及移动通讯能力的终端设备。

[来源：JT/T 1059.1—2016,3.3]



典型交易时间 currently transaction time

完成一次正常消费交易的卡片处理时间，这个时间是从终端寻卡成功，到终端接收到卡片返回的最后一条指令为止，包括卡片密钥计算、电子钱包消费、复合应用消费、读写卡片信息等与卡片交互的时间，不包括其他非卡片处理时间。



安全域 security domain

负责对某个SE外实体（例如SE发行方、应用提供方、授权管理者）的管理、安全、通信需求进行支持的SE内实体。

[来源：JT/T 1059.1—2016,3.14]



应用提供方 application provider

提供支付应用的主体。

[来源：JT/T 1059.1—2016,3.16]



SE发行方 SE issuer

为用户提供SE发行服务的主体。

[来源：JT/T 1059.1—2016,3.17]



可信服务管理 trusted service management （TSM）

由可信第三方提供的安全载体生命周期管理、应用生命周期管理和应用管理等服务。

[来源：JT/T 1059.1—2016,3.18]



SE发行方可信服务管理 SE issuer trusted service management （SE-TSM）

为SE发行方提供的承载SE生命周期管理服务的可信服务管理。

[来源：JT/T 1059.1—2016,3.21，有修改]



应用提供方可信服务管理 service provider trusted service management （SP-TSM）

为用户提供的承载应用生命周期管理服务的可信服务管理。

[来源：JT/T 1059.1—2016,3.22]



客户端 client

用于提供用户接口界面，与SE配合实现SE管理及应用管理功能的应用软件。

[来源：JT/T 1059.6—2016,3.1]

1. 缩略语

DB 11/T 159.1界定的以及下列缩略语适用于本文件

AID：应用标识符（Application Identifier）

AMSD：授权管理权限安全域（Security Domain with Authorized Management privilege）

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

API：应用程序接口（Application Programming Interface）

COS：卡片操作系统（Chip Operating System）

CPU：中央处理单元（Central Process Unit）

CSN ：芯片序列号（Chip Serial Number）

DES：数据加密标准（Data Encryption Standard）

DMSD：委托管理权限安全域（Security Domain with Delegated Management privilege）

FASD：最终应用权限安全域（Security Domain with Final Application privilege）

FCI：文件控制信息（File Control Information）

MAC：报文验证码（Message Authorization Code）

OPEN：全球环境（GlobalPlatform Environment）

OS：操作系统（Operating system）

PCD：接近耦合设备（Proximity Coupling Device）

PIN：个人识别码（Personal Identification Number）

PKI：公开密钥基础设施（Public Key Infrastructure）

PPSE：近距离支付系统环境（Proximity Payment Systems Environment）

ROM：只读存储器（Read Only Memory）

RSA：一种非对称加密算法（Rivest,Shamir,Adleman）

SE：安全单元 （Secure Element）

SE-TSM：SE发行方可信服务管理系统（SE Issuer Trusted Service Management）

SP-TSM：应用提供方可信服务管理平台（Service Provider Trusted Service Management）

SSL：安全套接字层(Secure Socket Layer)

TAC：交易验证码（Transaction Authorization Code）

TCP/IP：传输控制协议/网际协议(Transfer Control Protocol/ Internet Protocol)

TLS：传输层安全协议（Transport Layer Security）

TSD：交通一卡通辅助安全域（Transport Security Domain）

TSM：可信服务管理（Trusted Service Management）

UDP：用户数据报协议（User Dataprogram Protocol）

WTLS：无线传输层安全协议（Wireless Transport Layer Security）

1. 移动支付系统
   1. 系统组成

市政交通一卡通移动支付系统主要由安全单元（SE）、客户端软件、可信服务管理系统组成。以SE为载体，客户端软件为用户入口，依靠安全、可靠的网络，通过统一的数据接口，实现开卡、充值、消费等功能。

市政交通一卡通移动支付系统框架见图1。



1. 系统组成
   1. 系统功能
      1. 安全单元

安全单元（SE）主要分为SIM卡、全终端、外置式SE等类型。安全单元负责存储密钥、证书等机密信息，进行密码计算，为移动支付各参与方提供SE信息，为应用提供方提供辅助安全域管理、移动支付应用下载授权等功能。

* + 1. 可信服务管理系统

可信服务管理系统（TSM系统）由SE发行方可信服务管理平台（SE-TSM平台）和应用提供方可信服务管理平台（SP-TSM平台）组成，本规范中仅对可信服务管理系统功能、业务及流程进行规定。

1. SE-TSM平台负责管理SE载体与多应用管理。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。
2. SP-TSM平台负责对本机构自有应用进行管理，确保自有应用能进行空中下载、充值等。
   * 1. 客户端软件

客户端软件负责连接手机终端与市政交通一卡通移动支付系统各参与方的后台，以图文界面方式在支付应用中为用户提供开卡、消费、充值、退卡、迁卡等功能应用。

1. 安全单元
   1. 一般性要求
      1. 物理特性

通过手机内置SE模块模拟非接触式IC卡，其物理特性、非接触通道的电气特性和传输协议应符合JT/T 978.5的要求。

本文件对SE的外形尺寸和触点定义等物理特性不作规定。

* + 1. 接触通道

SE模块的接口应提供主处理器和外部读写器访问SE模块的通路。SE模块的接口，电气特性和传输协议不做规定。

* + 1. 非接触通道

非接触通道的电气特性和传输协议应符合JT/T 978.5的要求，保证SE与读写终端的兼容性。

* + 1. 逻辑结构

SE包括接触通道和非接触通道，接触通道和非接触通道应具有并发处理能力，且互不影响，SE的逻辑结构如图2所示。



1. 安全单元逻辑结构
   * 1. 硬件方案结构

应符合JT/T 1059.2中的相关规定。

* + 1. 供电要求

当移动支付终端处于开机状态，或处于关机状态但电池仍能通过电源管理系统正常提供电源能量时，内置SE模块可使用移动支付终端的电池作为电源能量；当移动支付终端的电池被取下，或电池无法通过电源管理系统正常提供电源能量时，内置SE模块可选择使用非接触芯片从终端设备的工作场中感应得到的电源能量。

在内置SE模块可获得正常工作所需的电源能量的情况下，应能正常执行市政交通一卡通移动支付应用。

* 1. 多应用管理
     1. 基本功能

移动支付应用中，SE作为移动支付的安全载体，除应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，还应支持多应用动态管理及运行安全。移动支付SE多应用管理主要功能包括：

1. 支持应用动态下载：支持在SE发行后，SE发行者或服务提供者根据业务扩充的需求，在SE上动态加载新的应用供用户下载使用；
2. 支持多应用共存：通过将SE上不同的应用关联至相应的安全域，可确保不同应用间安全运行，互不影响，有效解决一卡多账户问题；
3. 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，确保不同应用采取与之匹配的安全策略与SE外部实体进行鉴权及安全会话。

根据移动支付多应用需求，SE应实现多应用平台嵌入式软件，SE多应用平台软件由安全域、全局服务应用、运行时环境、平台环境等系列组件构成，为SE上的应用和卡外管理系统提供了独立于硬件和厂商的接口。

* + 1. 安全域

1. 安全域提供各类安全服务，包括密钥管理、加密解密、针对其提供者(发卡机构、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。当发卡机构、应用提供方、授权管理者等卡外实体需要将用到的安全服务进行隔离时，需通过安全域实现。
2. 根据授权机构不同，SE安全域可以划分为两种主要类型：
3. ISD：SE上首要的、强制性存在的安全域，是SE管理者(通常是发行方)在SE内的代表；
4. SSD：SE上次要的、可选择地存在的安全域，是应用提供方或发行方及其代理方在SE内的代表。
   * 1. 全局服务应用

全局服务应用是向其他应用提供者（如SE持有者）提供验证方法等的服务。安全单元上存在一个或者多个全局服务应用。

* + 1. 运行时环境

SE平台运行在一个安全的运行时环境之上。运行时环境向所有应用提供硬件中立应用编程接口，确保各个应用的代码和数据能相互区隔、安全存储，负责执行空间分配机制，提供服务，用以完成SE和SE外部实体之间的通信。

* + 1. 平台环境

1. 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SE内容管理。
2. SE平台环境应拥有一个内部的全局平台注册表，并将其作为信息资源进行SE的内容管理。全局平台注册表包含管理SE、可执行装载文件、应用、安全域关联以及权限所需信息。
   * 1. 平台API

SE可通过平台API向应用提供各种服务，如持卡方验证服务、个人化服务、安全服务等，也可通过平台API提供SE内容管理服务，如SE锁定或应用生命周期状态更新服务。

* + 1. SE应用管理

SE的主要任务是管理其内部的安全域和各类应用，而各类应用在通过平台指令下载至SE上后即以可执行装载文件的形式定义并存在，一个可执行装载文件可保存在：

1. 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SE生产过程中就被装载到SE中，并且不可被改变（可以被禁止）；
2. 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。

已下载并保存至SE的每一个可执行装载文件可包含一个或多个可执行模块，即应用代码。应用的安装过程即从一个可执行模块里创建一个应用实例并连同该应用相关的数据一起放入SE的可变存储区中，同时此应用将被转化为已安装状态。此后本应用的生命周期状态转换可参见4.2.8中应用生命周期管理。

任何应用的实例及其相关的数据都可以被移除。一个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。

* + 1. 生命周期模型

应符合JT/T 1059.2中的相关规定。

* 1. 基本命令

应符合JT/T 1059.2中的相关规定。

* 1. 密钥要求

应符合JT/T 1059.2中的相关规定。

* 1. 安全通信

SE安全通信采用SCP02安全通道机制或SCP03安全通道机制，在SECURED状态后，所需的APDU命令的最低安全级别要求见表1。

1. SCP02/SCP03 APDU命令的最低安全级别要求

|  |  |
| --- | --- |
| 指令 | 最低安全级别 |
| INITIALIZE UPDATE | 无 |
| EXTERNAL AUTHENTICATE | C-MAC （‘01’） |

* 1. 应用个人化服务
     1. 基本功能

应用安装后需要加载个人化数据，包括密钥、发卡机构应用数据。应用能够通过安全通信和其相关安全域提供的密钥解密服务来管理个人化数据的安全下载。

SE应支持以下两种方式实现个人化服务：

1. 使用运行时消息流；
2. 使用安全域访问。
   * 1. 运行时消息流

应符合JT/T 1059.2中的相关规定。

* + 1. 安全域访问

应符合JT/T 1059.2中的相关规定。

* 1. 应用选择服务

SE应用选择服务应包括以下两种：

1. 受理环境选择市政交通一卡通支付应用，非接触途径要求提供PPSE选择，按照JT/T 978.2中相关PPSE选择流程要求，通过FCI模板返回应用AID列表；
2. 移动终端上的应用管理客户端直接使用SELECT AID方式，选择市政交通一卡通支付应用。
3. 典型业务
   1. 业务分类

根据移动支付终端应用场景的不同，典型业务可分为六类：开卡、消费、充值、退卡和迁卡。其中，电子钱包的具体应用要求见JT/T 978.2，交互流程见JT/T 978.3。

* 1. 开卡
     1. 交易模型

用户通过移动支付终端发起开卡请求，完成SE应用创建的过程。开卡交易模型如下图3：



标引序号说明：

1——移动支付终端请求SE-TSM平台进行SE安全域初始化，并下载应用、安装应用。

2——移动支付终端请求SP-TSM平台生成应用个人化数据，完成开卡。

3­——SP-TSM平台同步开卡信息到总中心计算机处理系统，完成卡片账户创建。

1. 开卡交易模型
   1. 消费
      1. 交易模型

用户通过移动支付终端与终端设备或支付平台交互进行支付，并在交易完成后将交易通知或文件转发至总中心计算机处理系统进行处理。消费交易模型如下图4：



1. 消费交易模型
   * 1. 典型交易时间

典型交易时间要求应符合 DB11/T 159.2中的相关规定。

* 1. 充值
     1. 交易模型

用户通过移动支付终端请求TSM完成SE应用充值的过程，充值的交易模型如下图5：



标引序号说明：

1——用户通过移动支付终端向支付平台发起银行账户或第三方账户资金的支付。

2­——移动支付终端向SP-TSM平台发起充值请求。SP-TSM平台向支付平台确认支付结果，下发充值脚本更新移动支付终端中SE应用的余额。

3­——SP-TSM平台收到充值结果，并上送充值交易到总中心计算机处理系统。

1. 充值交易模型
   1. 退卡
      1. 交易模型

用户通过移动支付终端请求TSM平台删除SE应用并退还余额的过程。退卡交易模型如下图6：



标引序号说明：

1——用户通过移动支付终端发起退卡请求到SP-TSM，SP-TSM平台下发退卡脚本。

2——SP-TSM平台收到退卡脚本执行结果后，同步退卡信息到总中心计算机处理系统。

3­——SE-TSM平台通知移动支付终端删除SE应用。

1. 退卡交易模型
   1. 迁卡
      1. 交易模型

用户将移动支付终端上的一个SE应用迁移到另一台移动支付终端上的过程，迁移前后SE应用数据完全一致。迁卡交易分为迁出、迁入两个步骤，迁出交易模型如下图7：



标引序号说明：

1——用户通过移动支付终端发起迁出SE应用请求到SP-TSM，SP-TSM下发迁出指令脚本。

2——SP-TSM确认迁出结果，发送迁出信息到总中心计算机处理系统。

3——SE-TSM确认迁出结果，发送删除SE中已迁出应用指令。

1. 迁出交易模型

­迁入交易模型如图8：



标引序号说明：

1——用户通过移动支付终端发起SE应用迁入请求到SP-TSM。

2——SP-TSM从总中心计算机处理系统获取迁入SE应用数据。

3——SE-TSM初始化移动支付终端中SE，并下载、安装应用。

4——SP-TSM下发SE应用个人化脚本，迁入SE应用。

5­——SP-TSM收到迁入结果后，同步迁入信息给总中心计算机处理系统。

1. 迁入交易模型
2. 可信服务管理系统
   1. 系统功能

可信服务管理系统由SE-TSM和SP-TSM组成，可信服务管理系统提供的功能如下：

1. 机构接入：应用提供方机构的接入；
2. 应用注册：包括应用审查、应用AID（包括包AID、类AID和实例AID）分配；
3. SE可信管理：包括SE的注册；
4. SE开放共享：包括应用提供方SSD的创建、删除、锁定解锁、个人化、终止、状态查询、应用操作授权等功能；
5. SE载体管理：包括SE的生命周期管理；
6. 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；
7. 应用管理：包括应用空中下载、充值等；
   1. 接入机构管理

SE-TSM根据SP-TSM平台运营方和应用提供方提交的注册申请信息为其分配机构ID。注册完成后，SE-TSM允许SP-TSM平台运营方接入并提供服务。

* 1. 应用配置管理
     1. 基本要求

可信服务管理系统负责管理应用提供方SSD，为市政交通一卡通移动支付应用统一分配应用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。

* + 1. 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、保留位和序号编码构成。可信服务管理系统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ISO7816-4的要求，可信服务管理系统对交通行业支付应用和安全域分配的AID编码要求见表2、表3。

1. 应用AID编码规则

|  |  |  |  |
| --- | --- | --- | --- |
| AID | | | |
| RID | PIX | | |
| 业务/应用编码 | 保留 | 序号编码 |
| B1～B5 | B6-B14 | B15 | B16 |
| 5字节 | 9字节 | 1字节 | 1字节 |
| 注1：RID：取五个字节常数值（十六进制表示）。  注2：业务/应用编码：9字节。  注3：保留：保留为将来扩展。  注4：序号：0-F。 | | | |

1. 辅助安全域AID编码规则

|  |  |  |  |
| --- | --- | --- | --- |
| AID | | | |
| RID | PIX | | |
| 业务/应用编码 | 保留 | 序号编码 |
| B1～B5 | B6-B14 | B15 | B16 |
| 5字节 | 9字节 | 1字节 | 1字节 |
| 注1：RID：取五个字节常数值（十六进制表示）。  注2：业务/应用编码：9字节。  注3：保留：保留为将来扩展。  注4：序号：0-F。 | | | |

* + 1. 应用注册管理

可信服务管理系统负责对所有市政交通一卡通移动支付应用进行注册管理。应用提供方将应用及其信息向SE-TSM提交注册申请，SE-TSM审核后，为应用分配相关的AID资源信息，流程如图9所示。



标引序号说明：

1——应用提供方向SE-TSM提供应用注册申请信息和相关材料。

2——SE-TSM将市政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。

3——SE-TSM向应用提供方提示操作状态。

4——由人工对应用注册信息和相关材料信息进行审核，并为审查合格的应用分配AID。

5­——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；审批通过的市政交通一卡通应用可以进行调测、上线发布。

1. 应用注册管理流程图
   1. SE初始化
      1. 基本要求

SSD和Applet在第一次下载市政交通一卡通应用时应进行初始化和激活。

SSD负责其下市政交通一卡通应用和安全域的管理操作。SSD安全域的初始化密钥采用两级分散体系，如图10所示。



1. SSD安全域初始化密钥分散体系
   * 1. SE初始化

SE初始化流程如图11所示。



标引序号说明：

1——客户端向SE-TSM请求获取应用列表。

2——SE-TSM响应应用查询结果。

3——客户端首先进行判断SSD是否创建。

4——如果客户端判断SSD没有创建，则向SE-TSM发起TSM创建请求。

5——SE-TSM判断SSD是否创建。

6——若未创建与客户端交互完成SSD创建操作(预制SSD初始密钥)。

7——客户端与SE-TSM交互完成Applet下载、安装操作。

1. SE初始化流程
   1. 移动支付管理
      1. 基本功能

可信服务管理系统可以通过SSD对应用提供方SSD下的应用进行生命周期管理，包括市政交通一卡通移动支付应用的下载、删除、个人化、锁定/解锁。

* + 1. 应用下载

市政交通一卡通移动支付应用下载流程如图12所示。



标引序号说明：

1——客户端向SE-TSM发起应用下载的认证申请操作。

2——SE-TSM将结果响应至客户端。

3——客户端向SE-TSM发起应用下载请求。

4——­SE-TSM向SP-TSM发起应用下载申请。

5——SP-TSM检查是否具备下载应用条件。

6——SP-TSM将是否允许下载结果反馈至SE-TSM。

7——SE-TSM平台组装应用下载响应指令。

8——SE-TSM响应客户端下载请求。

9——客户端向SE-TSM发送应用下载结果通知。

10——SE-TSM将应用下载结果同步SP-TSM平台。

1. 应用下载流程图
   * 1. 应用删除

应用删除流程如图13所示。



标引序号说明：

1——客户端向SE-TSM发起应用删除认证申请操作。

2——SE-TSM处理后，将处理结果响应至客户端。

3——客户端向SE-TSM发起应用删除请求操作。

4——SE-TSM向SP-TSM发起应用删除申请操作。

5——SP-TSM进行应用是否符合删除条件检查。

6——SP-TSM将是否具备删除条件的结果响应至SE-TSM。

7——SE-TSM进行删除指令脚本准备。

8——SE-TSM进行应用删除指令下发。

9——客户端将应用删除操作结果通知给SE-TSM。

10——SE-TSM将应用删除操作结果通知给SP-TSM。

1. 应用删除流程图
   * 1. 应用锁定/解锁

应用锁定/解锁流程如图14所示。



标引序号说明：

1——客户端向SP-TSM发起应用锁定/解锁请求操作。

2——SP-TSM组织应用锁定/解锁脚本。

3­——SP-TSM下发应用锁定/解锁脚本。

4——客户端将应用锁定/解锁结果通知SP-TSM平台。

5——SP-TSM将应用锁定/解锁结果通知SE-TSM平台。

1. 应用锁定/解锁流程图
   * 1. 应用个人化

应用个人化流程如图15所示。



标引序号说明：

1——客户端向SP-TSM发起申请个人化操作。

2——SP-TSM组织个人化脚本。

3——SP-TSM将脚本发往SE执行。

4——客户端将执行结果通知SP-TSM。

5——SP-TSM将应用个人化状态通知SE-TSM平台。

1. 应用个人化流程图
   1. 平台安全要求

应符合 DB11/T159.4中的相关规定。

1. 客户端软件
   1. 软件架构

客户端软件运行在移动支付终端操作系统中，通过SE对交易敏感信息等加密,并与远程支付系统建立通信连接，完成支付相关功能。软件架构见图16。

|  |  |
| --- | --- |
| 客户端 | 支付应用软件层 |
| HTTP、WAP、SSL、TLS等 | 网络协议层 |
| ANDROID、IOS、鸿蒙等 | 操作系统层 |
| SE | 物理设备层 |

注1：支付应用软件层：客户端软件直接面向用户，通过各种形式的图形化操作界面，为用户提供方便快捷的支付服务。

注2：网络协议层：为客户端提供基础的网络协议服务，包括各种安全通信协议SSL、TLS、WTLS等，也可根据客户端需求提供定制化的专用网络协议。

注3：操作系统层：操作系统层是客户端软件运行的基础平台。目前主流的智能移动支付终端操作系统包括Android、IOS、鸿蒙等。

注4：物理设备层：SE内部安全域存储密钥、数字证书等机密信息，并为客户端提供交易敏感信息加密处理等安全功能。

1. SE客户端软件架构
   1. 基本功能
      1. 注册

用户通过客户端软件向总中心计算机处理系统进行用户注册。

* + 1. 开卡

用户通过客户端软件向可信应用管理系统发起请求，并实现在移动支付终端SE中创建市政交通一卡通应用的过程。

* + 1. 消费

用户通过客户端软件在终端设备或支付平台进行支付交易的过程。

* + 1. 充值

用户通过客户端软件向可信服务管理系统发起充值交易的过程。

* + 1. 退卡

用户通过客户端软件请求可信服务管理系统删除SE应用并退还余额的过程。

* + 1. 迁卡

用户通过客户端软件向可信服务管理系统发起迁卡请求，并完成卡片应用在移动支付终端SE间转移的过程。

* + 1. 默认应用设置

用户通过客户端软件对移动支付终端的SE中的默认应用（支付交易时的默认应用）进行修改设置的过程。

* + 1. 信息查询

用户通过客户端软件对余额、交易明细等信息进行查询的过程。

* + 1. 密码管理

密码管理是指用户通过客户端软件对登录密码进行管理。密码管理包括密码修改和密码找回两项功能。

* + 1. 版本升级

客户端软件具备版本在线检测和升级功能。

* 1. 应用模型

客户端软件应能向用户提供支付和TSM应用管理等功能。以图文界面方式在支付应用中为用户提供注册、开卡、消费、充值、退卡、迁卡、查询等功能。应用模型见图17。



标引序号说明：

1——用户打开手机客户端软件进行业务操作。

2——客户端软件通过OS将指令写入SE中获取卡片信息。

3——客户端将卡片信息传输到支付内容平台。

4——TSM平台通过加密机生成新的指令发送到客户端软件。

5——客户端软件将TSM系统下发的指令通过OS写入到SE。

6——SE将指令执行后反馈结果到客户端软件。

7——客户端软件向用户展示结果。

1. 客户端应用模型
   1. 安全要求
      1. 人机交互安全

应符合 DB11/T159.4中的相关规定。

* + 1. 软件安全

应符合 DB11/T159.4中的相关规定。

* + 1. 数据安全

应符合 DB11/T159.4中的相关规定。

* + 1. 通信安全

应符合 DB11/T159.4中的相关规定。

* 1. 管理要求
     1. 设计要求

设计应遵循安全、可靠、易用、可维护和可扩展等原则。

* + 1. 开发要求

开发过程中应遵循严格的开发流程和编码安全规范，并进行完整的测试，避免存在漏洞。

开发过程中应建立并维护开发文档，包括需求说明、需求分析、概要设计、详细设计、数据模型设计、源码归档、测试用例及配置管理等。

开发完成后，应进行功能性、安全性和兼容性等方面测试，并同步完成产品手册和用户手册等相关文档。

* + 1. 发布要求

应有严格、规范的上线发布流程，并应提供安全可靠的客户端软件下载、发布和升级渠道。

安装前应有明确的风险提示。安装过程中，应拥有独立的安装目录，唯一的应用标识符，明确的版本序号，不得篡改、覆盖、删除系统文件和其他软件。安装完成后应明确告知用户成功或失败。

卸载时应严格依据登记注册的卸载项，应删除运行时产生的所有缓存文件、日志文件等，不得篡改、覆盖、删除系统文件和其他软件，确保卸载后系统环境正常运行。

* + 1. 维护要求

应有科学、合理的管理策略和执行条例，指导工作协同、项目管理、质量管控、安全检测等，规范日常运维流程。

建立并维护工程实施、项目管理、测试报告、变更控制、系统运维管理、监控与应急管理、安全管理、安全审计等文档。