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 1059.5—2016

# 交通一卡通移动支付技术规范 第5部分：客户端软件

**Technical specification for mobile payment of transport card—Part 5:Client software**

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

# 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5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、武汉天喻信息产业股份有限公司、中钞信用卡产业发展有限公司、恒宝股份有限公司、江苏公共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、武汉城市一卡通有限公司。

# 交通一卡通移动支付技术规范

# 第5部分：客户端软件

## 1 范围

JT/T 1059的本部分规定了交通一卡通移动支付中客户端软件的系统架构及功能、应用模型和安全技术要求。

本部分适用于交通一卡通移动支付客户端软件及相关产品的设计、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。

JT/T 978(所有部分) 城市公共交通IC 卡技术规范

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 1059.4—2016 交通一卡通移动支付技术规范第4部分：远程支付

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

## 3 术语和定义

JT/T 978 和 JT/T 1059.1界定的术语和定义适用于本文件。

## 4 缩略语

下列缩略语适用于本文件。

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

APL____ 应用程序接口(Application Programming Interface)

ECC——椭圆曲线加密算法(Elliptic Curves Cryptography)

HTTP____ 超文本传输协议(HyperText Transfer Protocol)

IPSec——因特网安全协议(Internet Protocol Security)

MAC____ 报文鉴别码(Message Authentication Code)

OS——操作系统(Operating System)

SE——安全单元(Secure Element)

SM2——SM2椭圆曲线公钥密码算法(Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves)

SSL——安全套接字层(Secure Socket Layer)

SWP——单线传输协议(Single Wire 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)

(U)SIM——通用用户身份识别模块(Universal)(Subscriber Identity Module)

WAP——无线应用通信协议(Wireless Application Protocol)

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

# 5 系统架构及功能

## 5.1 系统架构

### 5.1.1 一般要求

客户端软件可分为基于SE 的客户端软件、无SE 的客户端软件和SE 内嵌的支付软件三种类型。三种客户端软件的系统架构各不相同。

### 5.1.2 基于SE 的客户端软件

5.1.2.1 基 于SE 的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，软件系统架构如图1所示。

| 客户端 | 支付应用软件层 |
| --- | --- |
| HTTP、WAP、SSL、TLS、WTLS等 | 网络协议层 |
| Android/IOS/Windows Phone/Symbian等 | 操作系统层 |
| SE | 物理设备层 |

**图 1 基于SE 的客户端软件系统架构**

5.1.2.2 基于SE 的客户端软件系统架构可划分为：

a) 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；

b) 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；

c) 操作系统层：为客户端软件运行提供基础平台，包括Android、IOS等移动支付终端操作系统；

d) 物理设备层：SE 内部安全域应存储密钥、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。

### 5.1.3 无 SE 的客户端软件

5.1.3.1 客户端软件运行在移动支付终端操作系统中，与远程支付系统建立通信连接，完成支付相关功能，其中交易敏感信息加密由客户端软件完成，软件系统架构如图2所示。

**5.1.3.2** 基于无SE 的客户端软件系统架构各层可划分为：

a) 支付应用软件：客户端软件直接面向用户，应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；

b) 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；

c） 操作系统层：为客户端软件运行提供基础平台，包括如Android、IOS 等移动支付终端操作系统。

| 客户端 | 支付应用软件层 |
| --- | --- |
| HTTP、WAP、SSL、TLS、WTLS等 | 网络协议层 |
| Android/IOS/Windows Phone/Symbian等 | 操作系统层 |

**图 2 无 SE 的客户端软件系统架构**

### 5.1.4 SE 内嵌的支付软件

**5.1.4.1** SE 内嵌支付软件运行在SE 操作系统中，SE 操作系统通过标准APDU指令实现SE 内嵌支付软件和 SE 之间的交互。软件系统架构如图3所示。

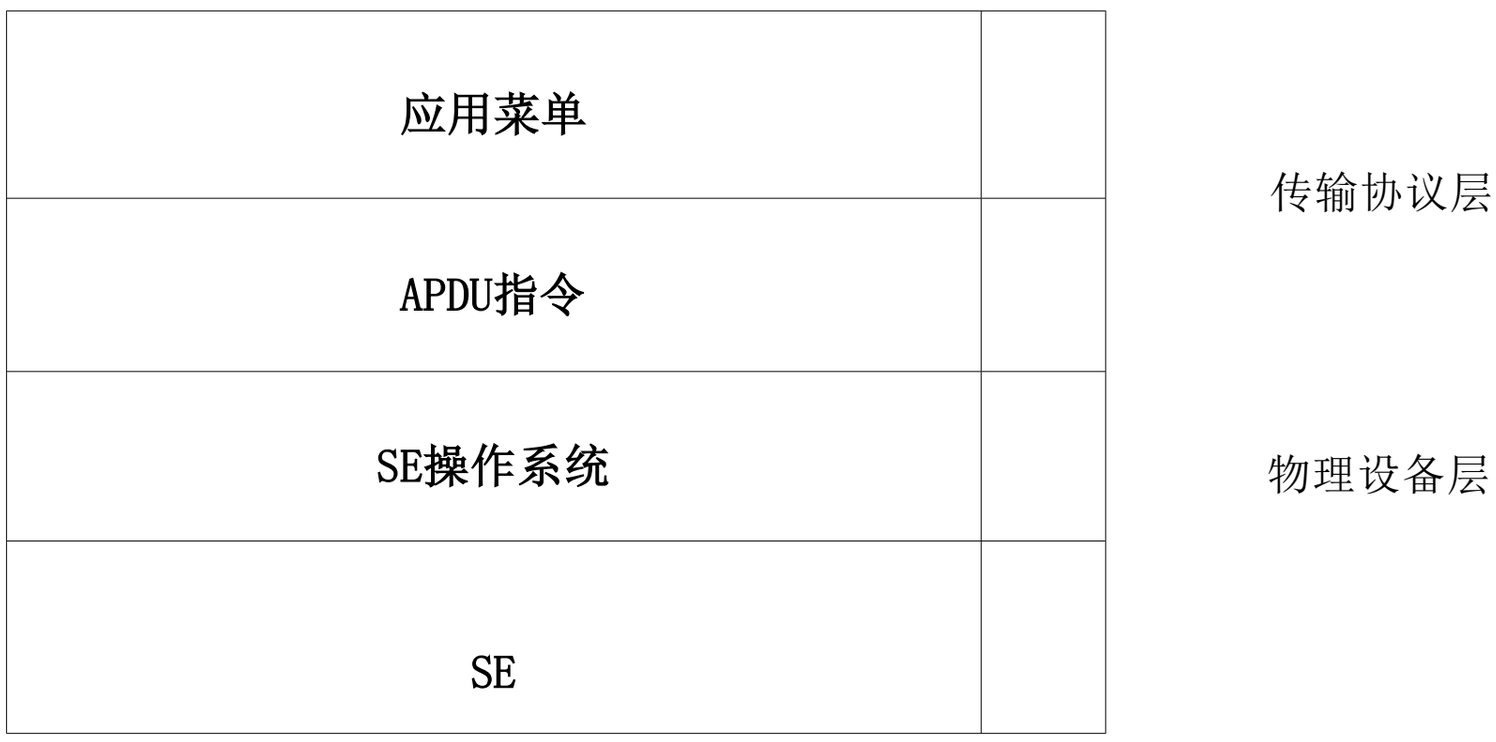


**图 3 SE 内嵌支付软件的软件系统架构**

**5.1.4.2** SE内嵌的支付软件架构各层划分为：

a) 应用界面层：应用界面层是与用户直接交互的功能层，基于客户端软件以菜单的模式为用户提供移动支付应用。根据用户需求，应用层应可以支持空中下载技术(OTA) 技术实现应用软件空中下载及升级服务。

b） 传输协议层：传输协议层作为应用界面层和操作系统层间的桥梁，应通过标准APDU 指令实现两者之间的交互。

c) 操作系统层：为SE 内嵌支付软件运行提供基础平台，负责解析所有应用指令并进行处理，提供基础的安全服务。

d) 物理设备层：为客户端软件安全服务的硬件基础，为上层应用提供基础的认证及加解密硬件资源。

## 5.2 基本功能与流程

### 5.2.1 用户注册

#### 5.2.1.1 功能定义

客户端通过用户界面收集用户信息，向远程支付平台发起用户注册请求。

#### 5.2.1.2 界面要求

应向用户显示注册结果界面。