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

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 1059.2—2016

交通一卡通移动支付技术规范 第2部分：安全单元

Technical specification for mobile payment of transport card—Part2:Secure element

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2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：中国交通通信信息中心、北京中交金卡科技有限公司、北京市政交通一卡通有限公司、南京市市民卡有限公司、恩智浦(中国)管理有限公司、北京握奇数据系统有限公司、北京雷森科技发展有限公司、北京中广瑞波科技股份有限公司、深圳市雪球科技有限公司、北京中电华大电子设计有限责任公司、大唐微电子技术有限公司。

交通一卡通移动支付技术规范

第2部分：安全单元

1 范围

JT/T 1059的本部分规定了交通一卡通移动支付安全单元类型、多应用管理、多应用架构、支付账户介质识别码、交通一卡通身份认证应用、安全单元基本命令、密钥要求、安全通信、应用个人化服务以及安全单元应用选择服务。

本部分适用于交通一卡通移动支付系统涉及的承载安全单元载体的设计、生产以及相关应用系统的研发、集成和维护管理。

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 16649.1 识别卡带触点的集成电路卡第1部分：物理特性

GB/T 16649.3 识别卡带触点的集成电路卡第3部分：电信号和传输协议

GB/T 16649.4 识别卡带触点的集成电路卡第4部分：行业间交换用命令

JT/T 978 （所有部分） 城市公共交通IC 卡技术规范

JT/T 978.2 城市公共交通IC 卡技术规范第2部分：卡片

JT/T 978.5 城市公共交通IC卡技术规范第5部分：非接触接口通信

JT/T 978.6 城市公共交通IC 卡技术规范第6部分：安全

JT/T 1059.1 交通一卡通移动支付技术规范第1部分：总则

ETSI TS 102613 智能卡 UICC—非接触前端(CLF) 接口 第1部分：物理层和数据链路层特性[Smart Cards;UICC-Contactless Front-end(CLF)Interface;Part 1:Physical and data link layer characteristics]

ETSI TS 102622 智能卡 UICC—非接触前端(CLF) 接口 主机控制器接口(HCI)[Smart Cards;UICC-Contactless Front-end(CLF)Interface;Host Controller Interface(HCI)]

3 术语和定义

JT/T 978和 JT/T 1059.1界定的及下列术语和定义适用于本文件。

3.1

主安全域　issuer security domain

安全单元中负责对安全单元管理者(通常是安全单元发行方)的管理、安全、通信等功能需求进行支持的首要实体。

3.2

辅助安全域　supplementary security domain

除主安全域之外的其他安全域。

3.3

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。

3.4

非接触前端 contactless front-end

通过近场非接触接口实现通信功能的控制模块。

3.5

可穿戴设备 wearable device

可直接穿戴在身上，或可整合到服装或配件上的一种能通过软件实现数据交互功能的便携式设备。

3.6

可执行装载文件 executable load file

实际存在于卡片上的包含一个或多个应用的可执行代码(可执行模块)的容器，它既可以驻留在只读内存中，也可以作为加载文件数据块的映像在可变内存中生成。

3.7

可执行模块 executable module

可执行装载文件中包含的一个单独应用的可执行代码。

4 缩略语

下列缩略语适用于本文件。

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——应用编程接口(Application Programming Interface)

CLF——非接触前端(Contactless front-end)

COS——片内操作系统(Chip Operating System)

DAP——数据认证模式(Data Authentication Pattern)

DEK——数据加密密钥(Data Encryption Key)

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)

I2C——两线式总线接口(Inter -Integrated Circuit)

ISD——主安全域(Issuer Security Domain)

MCU——微控制单元(Micro Controller Unit)

OPEN——全球环境(Global Platform Environment)

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

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

ROM——只读存储器(Read Only Memory)

SCP——安全通道协议(Secure Channel Protocol)

S-ENC——安全通道加密密钥(Secure Channel Encryption Key)

S-MAC——安全通道消息认证码密钥(Secure Channel Message Authentication Code Key)

SPI——串行外设接口(Serial Peripheral Interface)

SD——安全与权限(Security Domain)

SE——安全单元(Secure Element)

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

SWP——单线协议(Single Wire Protocol)

TCSD——交通一卡通认证安全域(Transport Certification Security Domain)

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

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

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

5 类型及其基本要求

5.1 基于 SWP 接口的(U)SIM 卡

5.1.1 物理特性

(U)SIM 卡的物理特性应符合GB/T 16649.1的规定。

5.1.2 接触通道

(U)SIM 卡的接触通道的接口电气特性和传输协议应符合GB/T 16649.3和 GB/T 16649.4的规定。

5.1.3 非接触通道

5.1.3.1 电气特性和传输协议

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

5.1.3.2 单线协议

CLF 和(U)SIM 卡之间应采用SWP 连接，SWP 接口的电气特性和链路层传输协议应符合 ETSI TS 102613 V8.0及以上版本的规定，其传输层协议应符合 ETSI TS 102622 V8.0及以上版本的规定。

5.1.4 SE逻辑结构

基于SWP 协议的(U)SIM 卡 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 逻辑结构如图1所示。

<table>
<tr><td>接触通道</td><td>预留应用</td><td>交通一卡通移动支付应用</td><td>预留应用</td><td>非接触通道</td></tr>
</table>

图 1　(U)SIM　卡 SE　逻辑结构

5.1.5 硬件方案结构

基于SWP接口(U)SIM 卡移动支付方案的核心硬件包括天线、CLF、(U)SIM等模块，可在移动支付终端上实现非接触IC 卡卡片功能。基于SWP接 口(U)SIM 卡移动支付方案结构如图2所示。

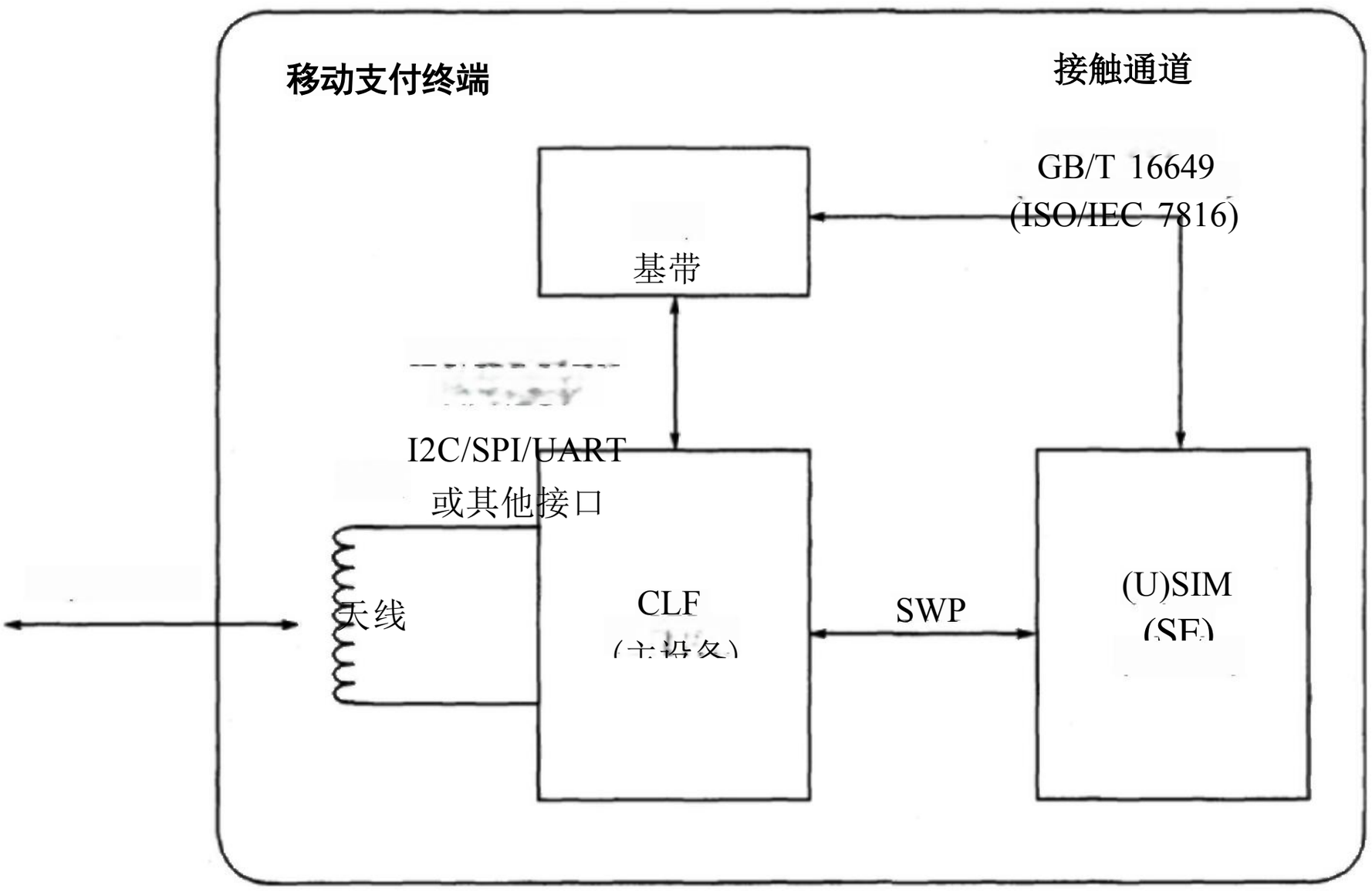

图 2 基于SWP 接口(U)SIM 卡硬件方案结构

5.1.6 供电要求

5.1.6.1 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，(U)SIM 卡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时，或电池无法通过电源管理系统正常提供电源能量时，(U)SIM 卡可选择使用CLF芯片从终端设备的工作场中感应得到的电源能量。

5.1.6.2 在(U)SIM 卡获得正常工作所需的电源能量时，应能正常运行交通一卡通移动支付应用。

5.2 全终端

5.2.1 物理特性

全终端通过内置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。

本部分对全终端内置SE 的外形尺寸和触电定义等物理特性不作规定。

5.2.2 接触通道

5.2.2.1 CLF与内置SE 模块之间的接口应提供主处理器和外部读写器设备访问SE 模块的通路。

5.2.2.2　移动支付终端具备内置SE 模块的情况下，CLF 和 SE 模块接口是内部接口，本部分对其电气特性和传输协议不作规定。

5.2.3　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的规定，并应保证SE 与读写终端的兼容性。

5.2.4 SE 逻辑结构

全终端所用的 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 逻辑结构如图3所示。

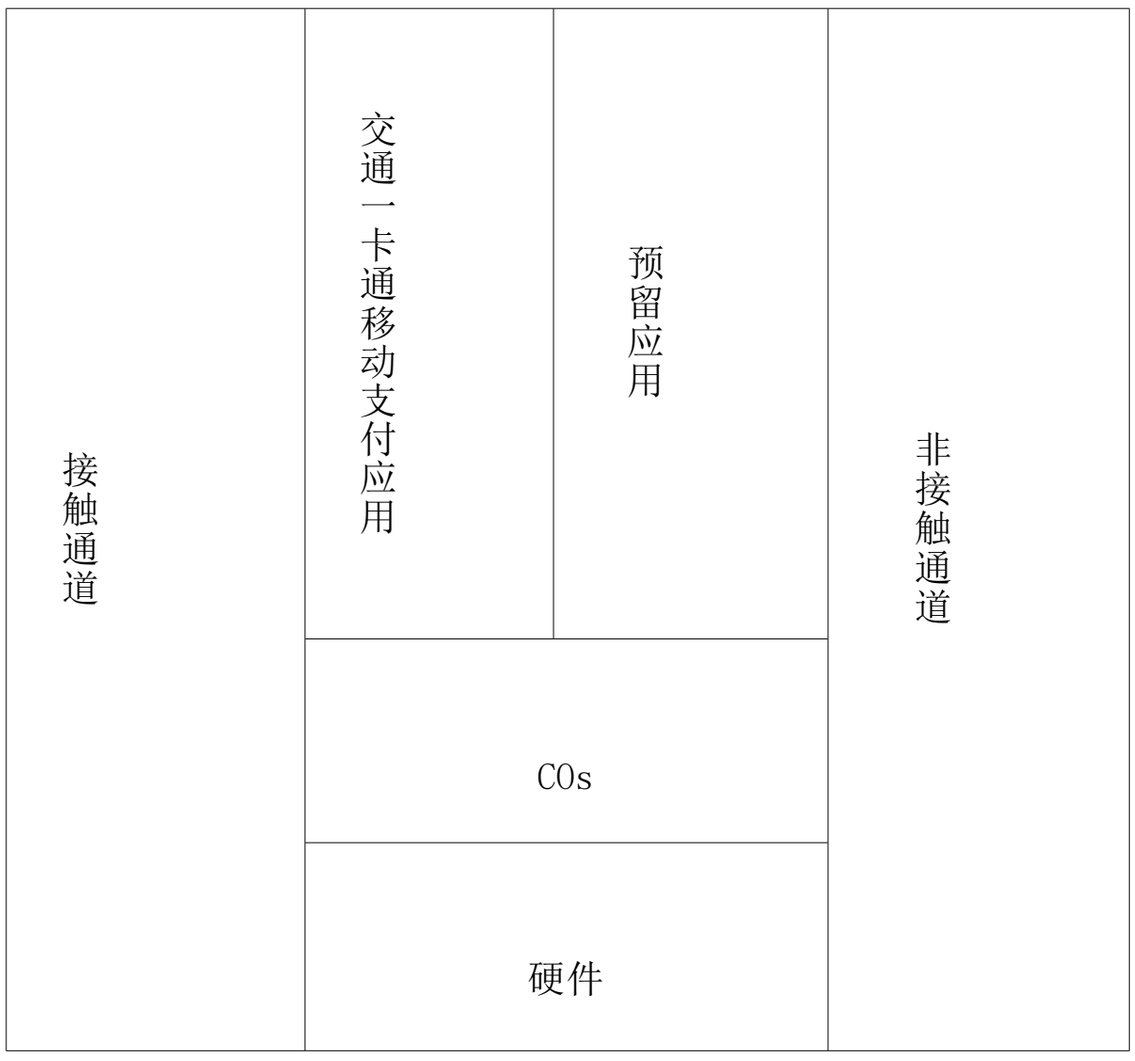

图 3 全终端SE 逻辑结构

5.2.5 硬件方案结构

全终端移动支付的核心硬件方案结构至少应包含内置SE 模块、CLF和天线等，如图4所示。

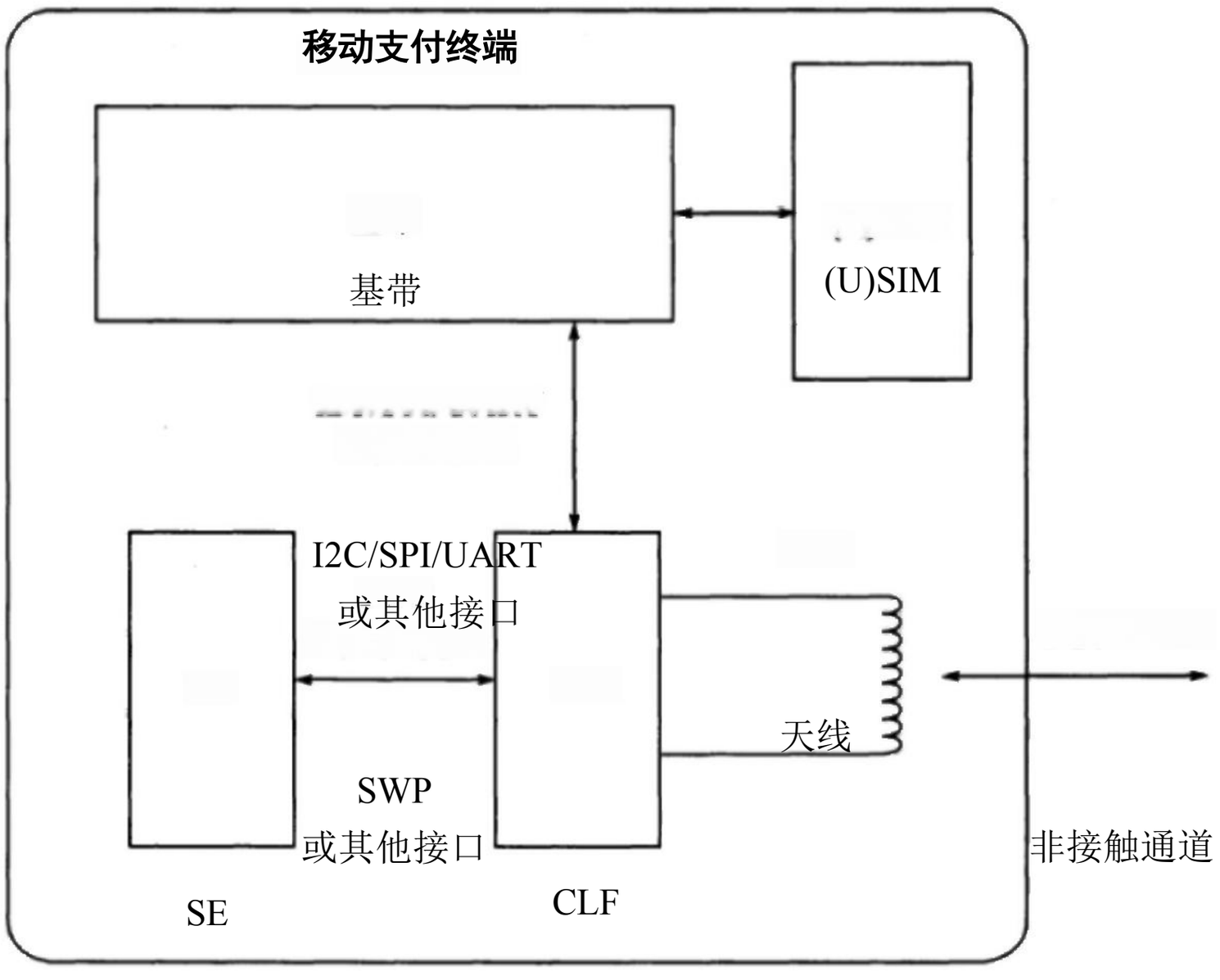

图 4　全终端硬件方案结构

5.2.6　供电要求

5.2.6.1　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时，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CLF芯片从终端设备的工作场中感应得到的电源能量。

5.2.6.2 在内置SE 模块获得正常工作所需的电源能量时，应能正常运行交通一卡通移动支付应用。

5.3 外置式 SE

5.3.1 物理特性

本部分对外置式SE 的外形尺寸和触点等物理特性不作规定。

5.3.2 接触通道

5.3.2.1 MCU与 SE 之间的接口应提供主处理器和外部读写终端访问SE 模块的通路。

5.3.2.2 MCU与 SE 接口是内部接口，宜采用GB/T 16649.3、SPI及其他内部接口协议。

5.3.3 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的规定。

5.3.4 SE 逻辑结构

外置式SE 模块所用的 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。外置式SE 逻辑结构如图5所示。

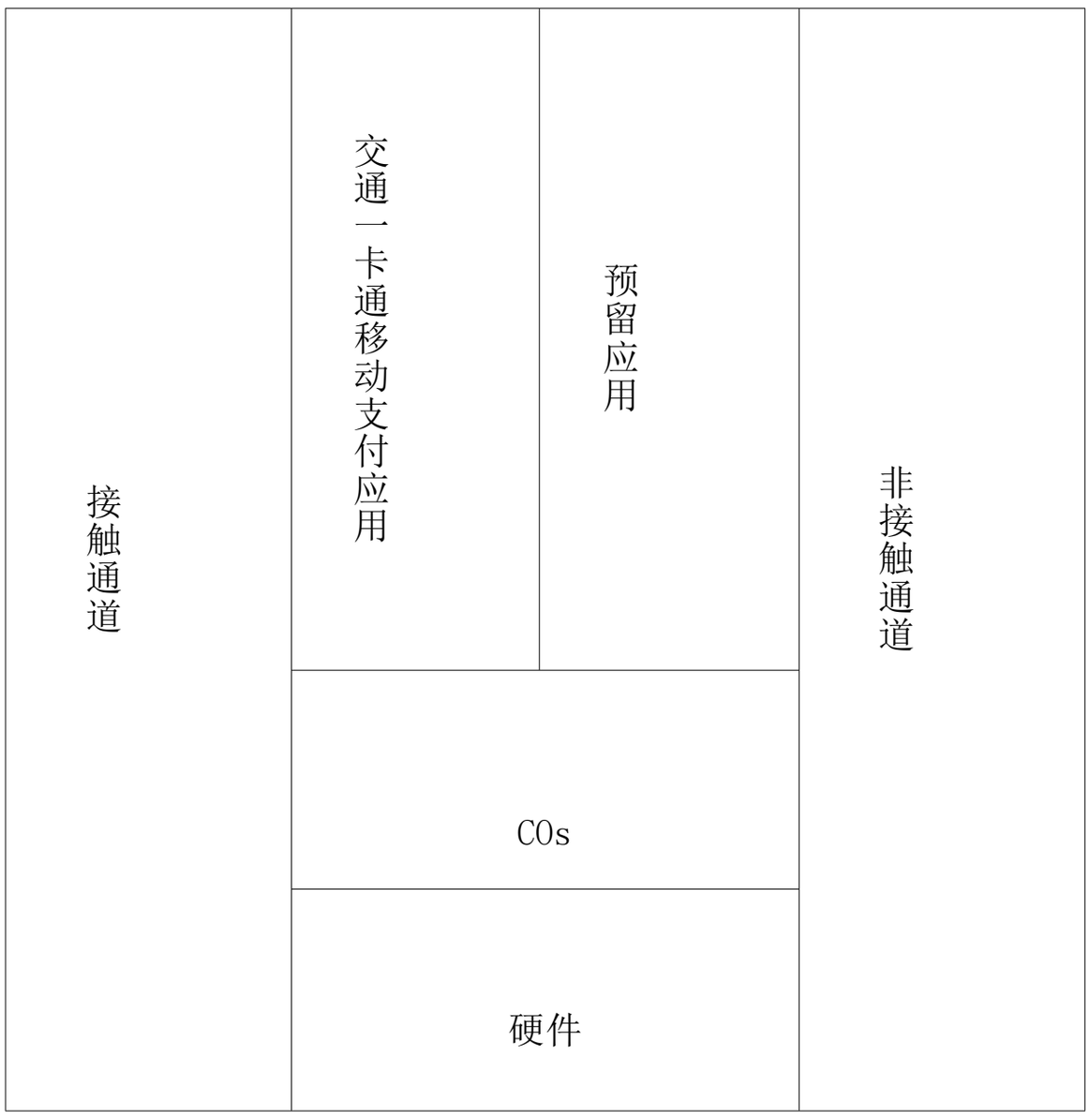

图 5 外置式 SE 逻辑结构

5.3.5 硬件方案结构

5.3.5.1　外置式 SE 是通过蓝牙等非接触通信方式与移动支付终端相连外部设备中的SE 模块，能模拟非接触式IC 卡，其非接触通信功能应符合JT/T 978.5的规定。

5.3.5.2　外置式 SE 载体(包括可穿戴设备、异型卡等)的内部安装SE 芯片和非接触天线，与移动支付终端连接后，可实现应用下载、个人化、远程支付、空中充值和余额查询等功能。