交通一卡通移动票卡技术规范
第2部分：安全单元

1 范围

本文件规定了交通一卡通移动票卡安全单元类型及其基本要求、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、安全单元应用选择服务以及应用。

本文件适用于交通一卡通移动票卡系统涉及到的承载安全单元的载体的设计、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，仅该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。

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 集成电路卡 第4部分：用于交换的结构、安全和命令

GB/T 32918 （所有部分）信息安全技术 SM2椭圆曲线公钥密码算法

JT/T 978.2—2023 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 交通一卡通移动票卡技术规范 第1部分：总则

JT/T 1059.7 交通一卡通移动票卡技术规范 第7部分：终端

JT/T 1059.8 交通一卡通移动支付技术规范 第8部分：检测项目

JR/T 0025.15 中国金融集成电路（IC）卡规范 第15部分：电子现金双币支付应用规范

ISO/IEC 7816-4 识别卡 集成电路卡 第4部分：交换的组织、安全和命令（Identification cards—Integrated circuit cards—Part 4: Organization, security and commands for interchange）

ETSI TS 102 613 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 102 622 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 1059.1界定的以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讯功能的控制模块。

3.5

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。

4 缩略语

下列缩略语适用于本文件。

AAC：应用认证密文（Application Authorization Cryptogram）
AC：应用密文（Application Cryptogram）
ADF：应用专用文件（Application Definition File）
AFL：应用文件定位器（Application File Locator）
AID：应用标识符（Application Identifier）
AIP：应用交互特征（Application Interchange Profile）
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）
ARQC：授权请求密文（Authorization Request Cryptogram）
ATC：应用交易计数器（Application Default Action）
BER：基本编码规则（Basic Encoding Rules）
CA：电子商务认证授权机构（Certificate Authority）
CLA：命令报文的类别字节（Class Byte of the Command Message）
CLF：非接触前端（Contactless Front-end）
COS：片内操作系统（Chip Operating System）
CVR：卡片验证结果（Card Verification Results）
DAP：数据认证模式（Data Authentication Pattern）
DEK：数据加密密钥（Data Encryption Key）
DF：专用文件（Dedicated File）
DMSD：委托管理权限安全域（Security Domain with Delegated Management Privilege）
EF：基本文件（Elementary File）
eID:公民网络电子身份标识（electronic IDentity）
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）
FID：文件标识符（File Identifier）
GP：全球平台（GlobalPlatform）
HTTP：超文本传输协议（HyperText Transfer Protool）
ISD：主安全域（Issuer Security Domain）
INS：命令报文的指令字节（Instruction Byte of Command Message）
I2C：内部集成电路（Inter－Integrated Circuit）
Lc：命令报文数据域的长度（Length of the Command Data Field）
Le：响应报文数据域的最大期望长度（Maximum Length Expected of the Response Data Field）
MAC：报文鉴别码（Message Authentication Code）
MCU：微控制单元（Micro Controller Unit）
NFC：近场通信（Near Field Communication）
OPEN：全球平台环境（Global Platform Environment）

PAN：主账号（Primary Account Number）
PAMID：支付账户介质识别码（Payment Account Media Identifier）
PDOL：处理选项数据对象列表（Processing Options Data Object List）
PPSE：近距离支付系统环境（Proximity Payment Systems Environment）
P1：参数1（Parameter One）
P2：参数2（Parameter Two）
ROM：只读存储器（Read Only Memory）
SCP：安全通道协议（Secure Channel Protocol）
SD：安全域（Security Domain）
SE：安全单元（Secure Element）
SFI：短文件标识符（Short File Identifier）
SM2：SM2椭圆曲线公钥密码算法（PublicKey Cryptographic Algorithm SM2 Based on Elliptic Curves）
SPI：步串行外设接口（Serial Peripheral Interface）
SSD：辅助安全域（Supplementary Security Domain）
SWP：单线协议（Single Wire Protocol）
SW1：状态字1（Status Word One）
SW2：状态字2（Status Word Two）
S-ENC：安全通道命令和响应加密密钥（Secure Channel Encryption Key）
S-MAC：安全通道消息鉴别码会话密钥（Secure Channel Message Authentication Code Key）
TC：交易证书（Transaction Certificate）
TCSD：交通一卡通认证安全域（Transport Certification Security Domain）
TLV：表示标签、长度以及值的组合（Tag Length Value）
TSD：交通一卡通辅助安全域（Transport Security Domain）
TSM：可信服务管理（Trusted Service Management）
T-MTPS：交通一卡通公共服务（Transport-Mobile Trustable Public Service）
UART：通用异步收发器（Universal Asynchronous Receiver/Transmitter）
（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 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 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 102 613 V8.0 及以上版本的规定，其传输层协议应符合 ETSI TS 102 622 V8.0 及以上版本的规定。

5.1.4 SE逻辑结构

基于SWP接口的（U）SIM卡的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。基于SWP接口的（U）SIM卡SE逻辑结构应符合图1的规定。

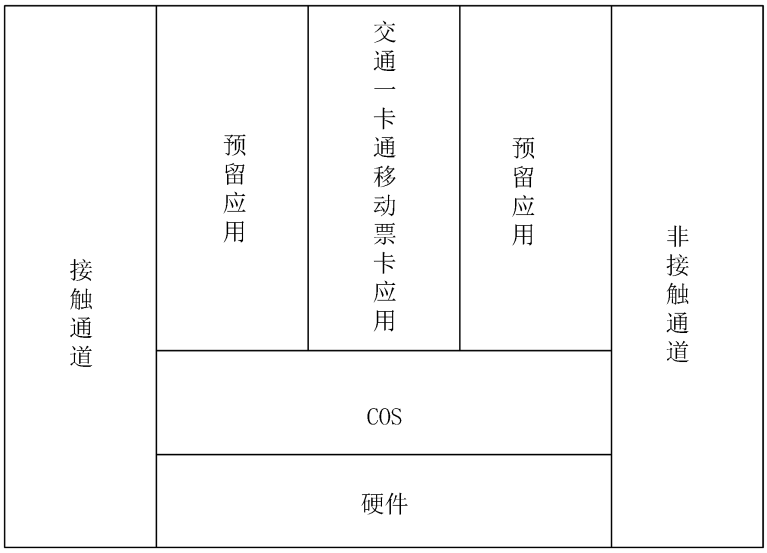


图 1　基于 SWP 接口的（U）SIM 卡 SE 逻辑结构

5.1.5　硬件方案结构

基于SWP接口（U）SIM卡移动票卡方案的核心硬件包括天线、CLF、（U）SIM等模块，可以在移动票卡终端上实现非接触IC卡卡片功能。基于SWP接口（U）SIM卡移动票卡硬件方案结构应符合图2的规定。

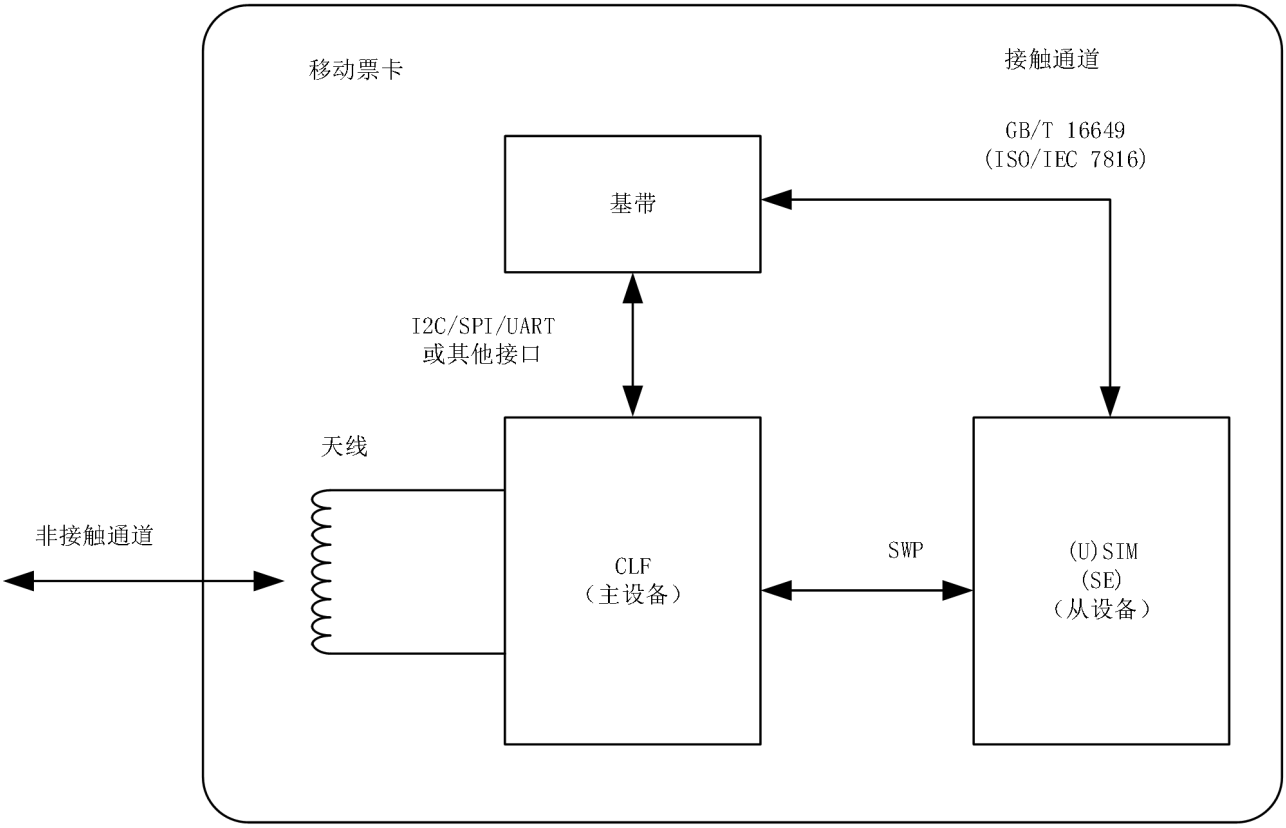


图 2　　基于 SWP 接口的（U）SIM 卡硬件方案结构

5.1.6　供电要求

5.1.6.1　当移动票卡终端处于开机状态，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 卡可使用移动票卡终端的电池作为电源能量；当移动票卡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 芯片从受理终端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票卡应用。

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。

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　移动票卡终端具备内置 SE 模块的情况下，CLF 和 SE 模块接口是内部接口。

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。全终端SE逻辑结构应符合图3的规定。

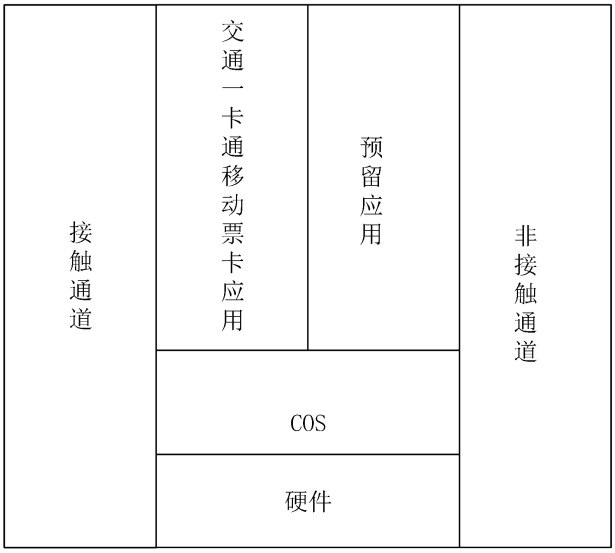


图 3　全终端 SE 逻辑结构

5.2.5　硬件方案结构

全终端移动票卡的核心硬件方案结构应至少包含内置SE模块、CLF和天线等，应符合图4的规定。

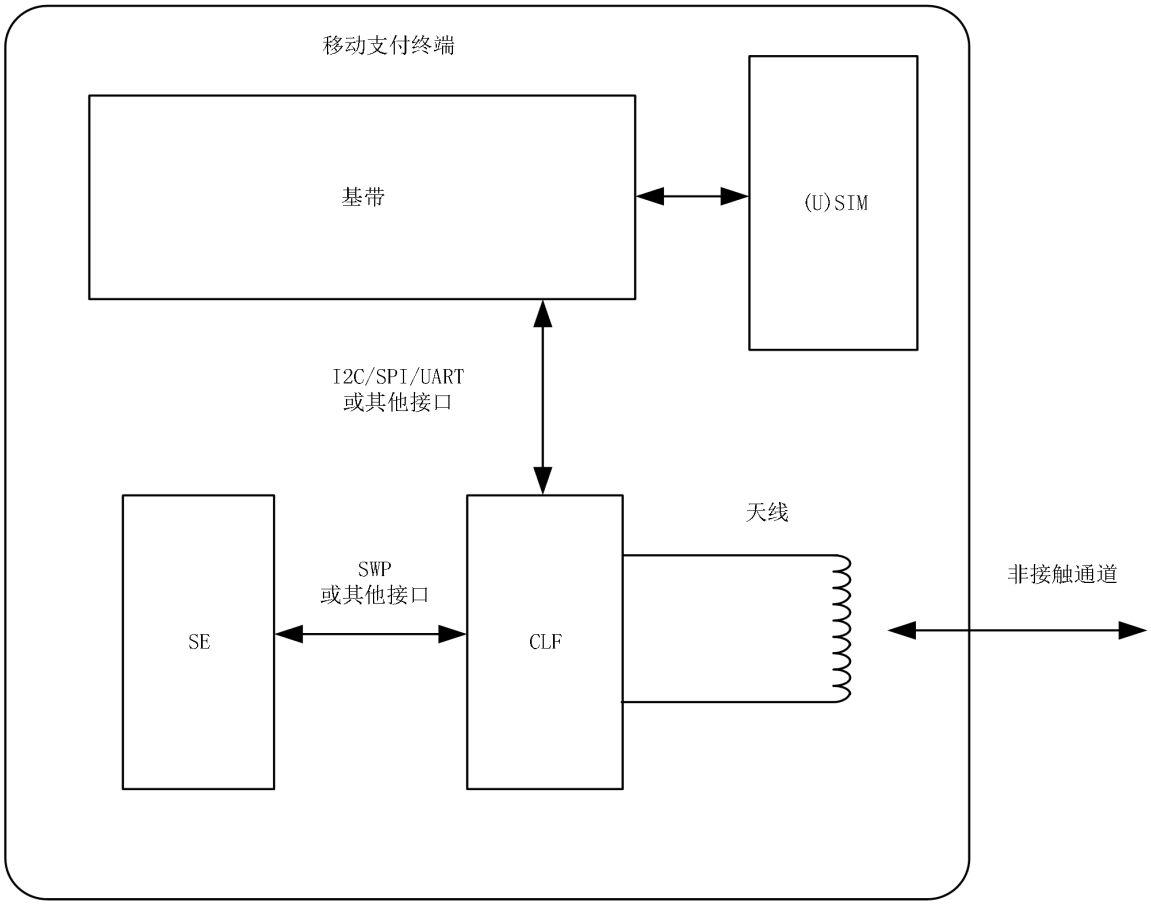


图 4　全终端硬件方案结构

5.2.6　供电要求

5.2.6.1　当移动票卡终端处于开机状态，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 模块可使用移动票卡终端的电池作为电源能量；当移动票卡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 芯片从受理终端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票卡应用。

5.3　外置式 SE

5.3.1　接触通道

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

5.3.1.2　MCU 与 SE 之间的接口应提供主处理器访问 SE 模块的通路。

5.3.2　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。

5.3.3　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逻辑结构应符合图5的规定。

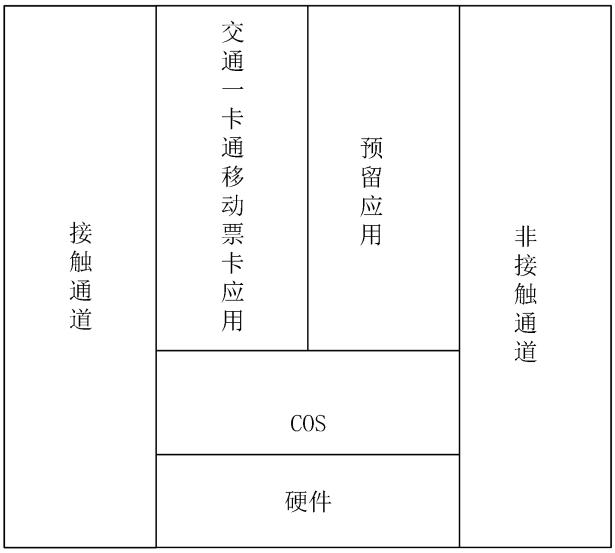


图 5　外置式 SE 逻辑结构

5.3.4　硬件方案结构

5.3.4.1　外置式 SE 是通过蓝牙等非接触通讯方式与移动票卡终端相连，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。

5.3.4.2　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，与移动票卡终端连接后，可实现交通一卡通移动票卡应用下载、个人化、远程支付、空中充值和余额查询等功能。

5.3.4.3　外置式 SE 载体硬件方案结构应符合图 6 的规定。

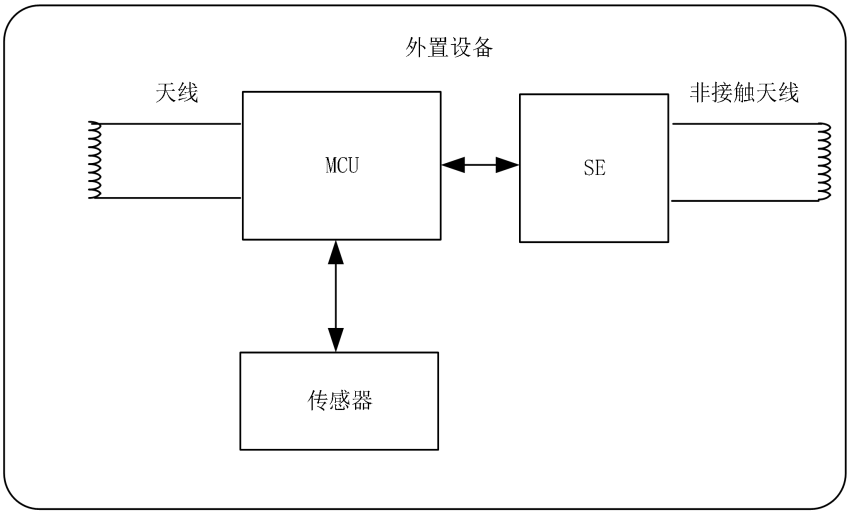


图 6　外置式 SE 载体硬件方案结构

5.3.5　供电要求

5.3.5.1　外置式 SE 可使用外置设备的电池作为电源能量。当外置设备的电池电量小于预设阀值时，应主动关机，预留部分电量供 SE 和非接触天线部件使用。外置设备关机时，电池应能通过电源管理系统正常提供电量给 SE，直至电量不能维持 SE 正常工作时，电源管理系统应切断 SE 的供电。

5.3.5.2　外置式 SE 也可选择使用非接触天线从受理终端的工作场中感应得到的电源能量。

5.3.5.3　在安全芯片 SE 可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票卡应用。

5.4　双界面（U）SIM 卡

5.4.1 物理特性

双界面（U）SIM卡的物理特性应符合GB/T 16649.1的规定。

5.4.2 接触通道

双界面（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。

5.4.3 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。

5.4.4 SE 逻辑结构

双界面（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。双界面（U）SIM卡SE逻辑结构应符合图7的规定。

图 7　双界面（U）SIM 卡 SE 逻辑结构

5.4.5 硬件方案结构

基于双界面（U）SIM卡实现近场支付功能的通讯受理终端的硬件方案结构应至少包含双界面（U）SIM、天线等模块，双界面（U）SIM卡硬件方案结构应符合图8的规定。

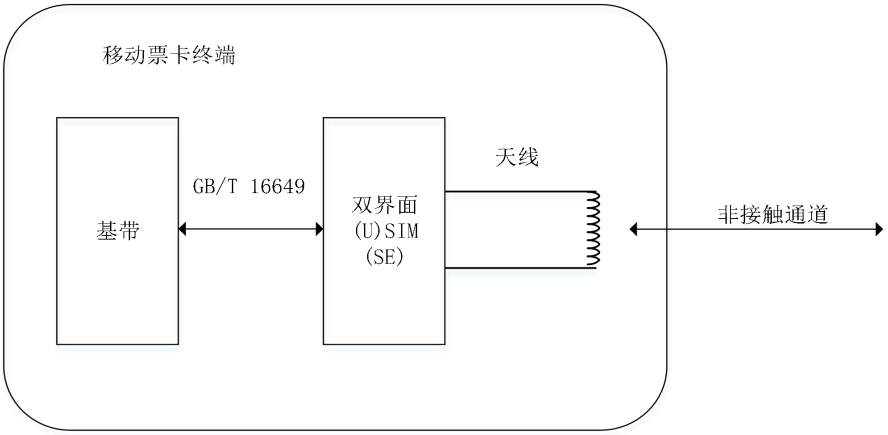


图 8　双界面（U）SIM 卡硬件方案结构

5.4.6 供电要求

5.4.6.1 当移动票卡终端处于开机状态，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，双界面（U）SIM 卡可使用移动票卡终端的电池作为电源能量；当移动票卡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，双界面（U）SIM 卡可选择使用其通过天线线圈从受理终端的工作场中感应得到的电源能量。

5.4.6.2 在双界面（U）SIM 卡可获得正常工作所需的电源能量的情况下，应能正常运行交通一卡通移动票卡应用。

5.5 基于云平台的 SE

5.5.1 物理特性

基于云平台的SE物理特性是利用远程服务器来完成SE的应用功能。

5.5.2 非接触通道

基于云平台SE的非接触通道应符合HTTP协议的规定。

5.5.3 硬件方案结构

基于云平台的SE硬件方案结构应至少包含主处理器、NFC控制器等模块，应符合图9的规定。

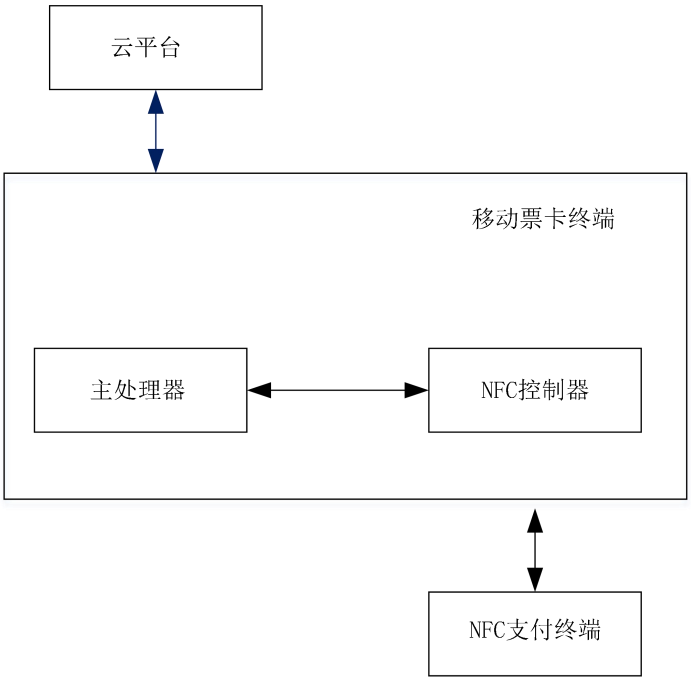


图 9 基于云平台的 SE 硬件方案结构

5.5.4 供电要求

云平台依赖服务器的运行，应采用不间断电源供电。

6 多应用管理

6.1 一般要求

6.1.1 交通一卡通移动票卡应用中，SE 作为移动票卡的安全载体，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，并保证其安全运行。移动票卡 SE 多应用管理应包括以下主要功能：

a) 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使用；

b) 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，确保不同应用间的独立安全运行，互不影响；
c) 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。

6.1.2 SE 应实现多应用的平台管理功能。SE 多应用平台由安全域、全局服务应用、运行时环境、平台环境等系列组件构成。SE 多应用平台应为 SE 上的应用和卡外 TSM 系统提供独立于硬件和厂商的接口。

6.2 安全域

6.2.1 安全域应提供各类安全服务，包括密钥管理、加密解密、针对其所有者（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等。当发卡机构、应用提供方、授权管理者等卡外实体要将用到的安全服务进行隔离时，应通过安全域实现。

6.2.2 根据授权机构不同，SE 安全域可划分为 ISD 和 SSD 两种主要类型。ISD 是 SE 上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；SSD 是 SE 上可选择存在的辅助安全域，是应用提供方或发行方以及它们的代理方在 SE 内的代表。

6.3 全局服务应用

SE上可存在一个或多个全局服务应用，负责向其他应用提供者（如SE持有者）提供验证方法等的服务。

6.4 运行时环境

SE多应用平台运行在一个安全的多应用运行时环境之上。运行时环境负责向所有应用提供硬件中立API，确保各个应用的代码和数据能相互区隔及安全存储，负责执行空间分配机制，并提供服务，用以完成SE和SE外部实体之间的通信。

6.5 平台环境

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、逻辑通道管理及SE内容管理。SE平台环境应拥有一个内部的全局平台注册表，用作信息资源进行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、安全域关联及权限所需信息。

6.6 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、个人化服务和安全服务等），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等）。

6.7 SE 应用管理

6.7.1 SE 负责管理其内部的安全域和各类应用，各类应用在通过平台指令下载至 SE 上后，应以可执行装载文件的形式定义并存在。可执行装载文件保存在下列位置中。

a) 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，且不可被改变（可以被禁止）。
b) 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。

6.7.2 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。应用的安装过程为：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，同时此应用生命周期状态转化为已安装状态。此后此应用的生命周期状态转换可参见 6.8.3 中应用生命周期管理。

6.7.3 任何应用的实例及其相关的数据都可以被移除。一个 SE 应支持多个可执行装载文件、多个可执行模块及多个应用同时存在。

6.8 生命周期模型

6.8.1 SE 生命周期管理

SE生命周期包含平台就绪、初始化、安全状态、SE锁定和SE终止五个状态，图10中各状态符合下列要求。

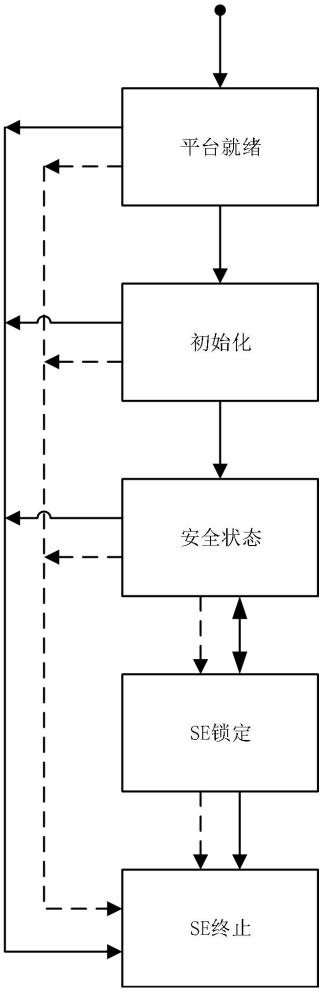
a) 平台就绪：SE 处于 OP_READY 状态时，发行方安全域应用选择就绪；命令处理模块应做好接收、处理、响应 APDU 指令的准备。

b) 初始化：SE 从生产机构切换至发行机构正式发行的中间产品管理状态，从平台就绪状态到初始化状态的切换应为不可逆操作。初始化状态应使某些初始化信息（如发行方安全域的密钥及数据）已经驻留至 SE。

c) 安全状态：标示 SE 生命周期处于正式发行后，产品已经发行到最终用户并正式启动、使用已装载业务。安全状态下，SE 安全域和应用可完全贯彻各自的安全策略。从初始化状态到安全状态的切换应为不可逆操作。

d) SE 锁定：SE 锁定状态下，应禁止对载体上的安全域和应用进行选择。从安全状态到 SE 锁定状态的切换应为可逆操作。

e) SE 终止：标示 SE 生命周期完结。SE 终止状态应永久性禁止载体的任何功能以及任何内容管理和生命周期的改变。从任何其他状态都可直接切换到 SE 终止状态，且状态切换应均为不可逆操作。



注：此图中实线箭头表示SE安全域策略，虚线箭头表示SE应用策略。

图 10　SE 生命周期状态

6.8.2　可执行装载文件和可执行模块生命周期管理

6.8.2.1　可执行装载文件生命周期应只有一个状态。所有存放在 SE 内的可执行装载文件应处于 LOADED 状态。

6.8.2.2　可执行模块生命周期应与可执行装载文件的生命周期相匹配。

6.8.3 安全域和应用生命周期管理

6.8.3.1 安全域生命周期包含已安装、可选择、已个人化及已锁定四个状态，图 11 中各状态符合以下要求。

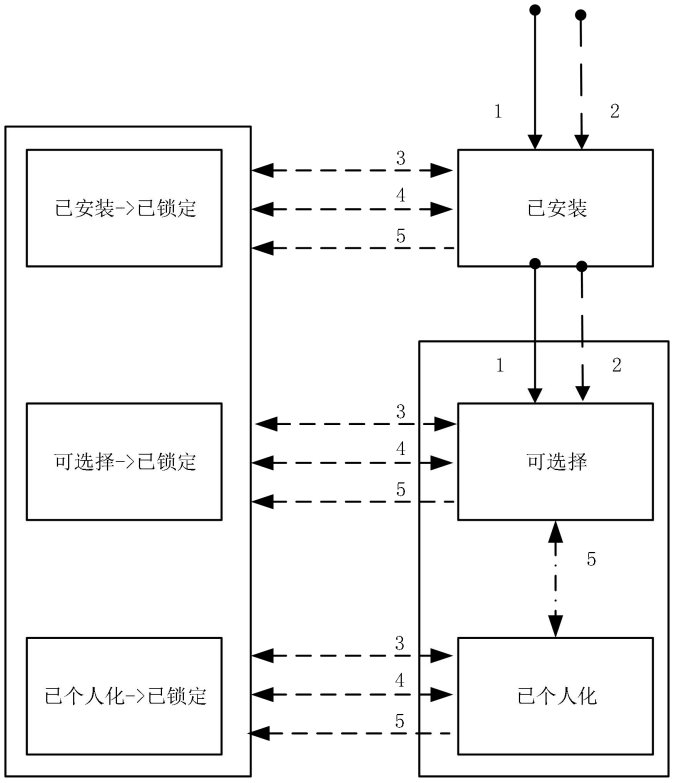
a) 已安装状态：标示安全域已完成注册表条目注册。该状态下，安全域服务不应被应用使用，安全域不可选定，不应与可执行装载文件或应用关联。

b) 可选择状态：标示安全域可被选择，可接收相关个人化指令。该状态下未装载应用密钥，不应和可执行装载文件或应用进行关联。从已安装状态到可选择状态的切换应为不可逆操作。

c) 已个人化状态：标示安全域已完成运行所需个人化数据与密钥数据的装载。该状态下，安全域与应用已建立关联。从可选状态到已个人化状态的切换应为不可逆操作。

d) 已锁定状态：OPEN 或经过发行者安全域认证后的卡外实体应能将安全域的生命周期状态设置为已锁定状态，并能阻止该安全域进一步被选择。处于锁定状态的安全域应被禁止用于委托管理操作。应仅发行方可对安全域锁定状态进行解锁。OPEN 保证该安全域生命周期在解锁后恢复至锁定前状态。

注：授权管理安全域也符合图中安全域生命周期管理。



标引序号说明：

1——具有验证管理功能的安全域；

2——具有托管功能的安全域；

3——关联安全域；

4——具有锁定功能的安全域或应用；

5——安全域本身。

图 11 安全域生命周期状态

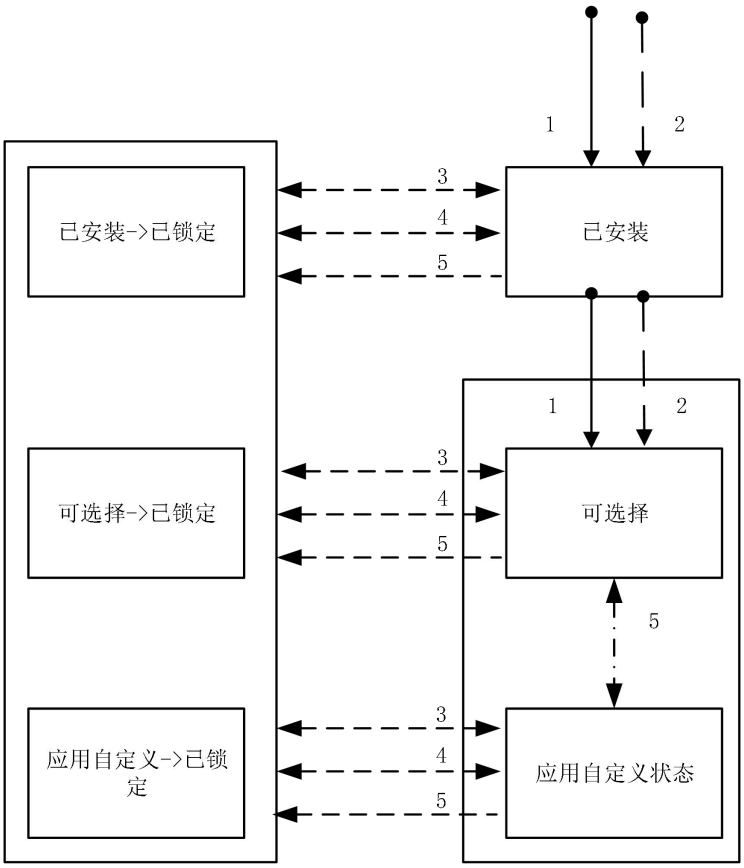
6.8.3.2 SE 应用生命周期包含已安装、可选择、已锁定及应用自定义四个状态，图 12 中各状态应符合下列规定。

a) 已安装状态：标示应用已完成 SE 注册表条目注册。该状态下，该应用应为不可选。

b) 可选择状态：标示应用可被成功选择，可接收相关指令。从已安装状态到可选择状态的切换应为不可逆操作。

c) 已锁定状态：标示 OPEN 或经过发行者安全域认证后的 SE 外实体应将应用的生命周期状态设置为已锁定状态，以阻止该应用被成功选择或执行。应仅发行方可对应用锁定状态进行解锁。OPEN 确保该应用生命周期在解锁后应恢复至锁定前状态。

d) 应用自定义状态：可为应用本身自定义状态。



标引序号说明：

1——具有验证管理功能的安全域；

2——具有托管功能的安全域；

3——关联安全域；

4——具有锁定功能的安全域或应用；

5——安全域本身。

图 12　SE 应用生命周期状态

7　多应用架构

7.1　一般要求

SE多应用架构包括多应用架构A和多应用架构B两种形式，每种应用架构由一系列的SE多应用组件构成。移动票卡SE多应用组件应符合图13的规定，组件应满足以下要求：

a) PAMID 应是 SE 的唯一身份标识符，满足第 8 章的要求；

b) 交通安全域组件用于支持移动票卡的一系列特定安全域，以实现移动票卡的 SE 安全可信和开放共享服务；
c) PPSE 用于管理非接触应用列表；
d) 交通一卡通移动票卡应用是在 SE 上安全地提供支付功能的系列应用。

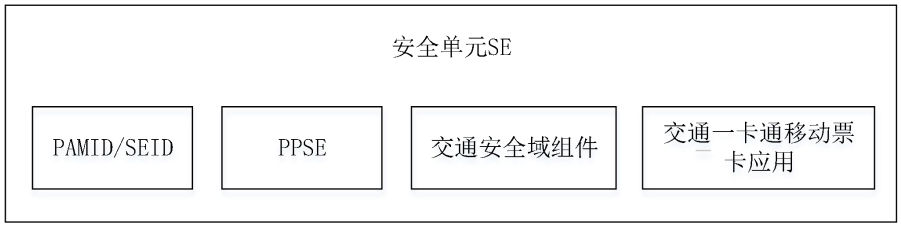


图 13　移动票卡 SE 多应用组件

7.2　SE 多应用架构 A

7.2.1　一般要求

7.2.1.1　SE 多应用架构 A 包括 ISD、TSD、应用提供方 SSD、交通一卡通支付应用和身份认证应用，应符合图 14 的规定。

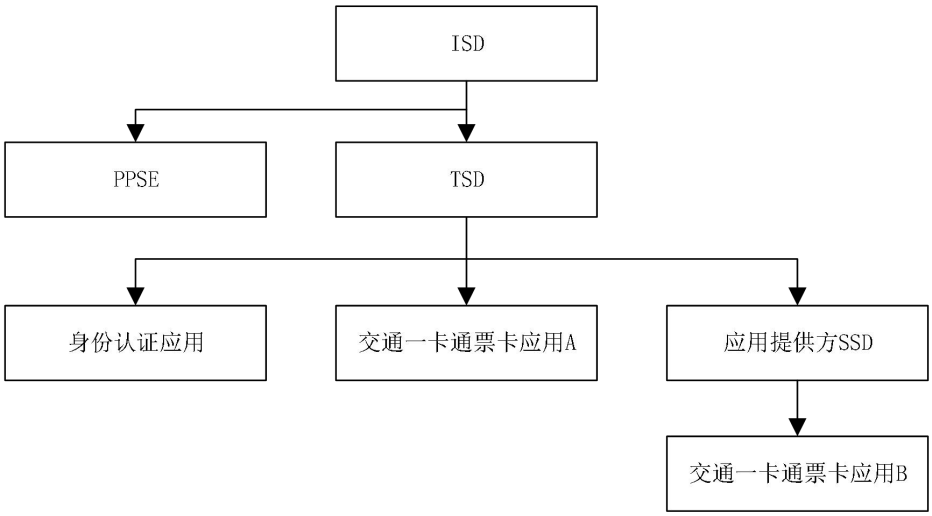


图 14　SE 多应用架构 A

7.2.1.2　在架构 A 中，ISD 由 SE 发行方持有，提供 TSD 的生命周期管理和应用管理授权，TSD 采用委托管理模式。交通一卡通移动票卡应用关联到应用提供方 SSD 或 TSD，并由 ISD 管理授权。
7.2.1.3　应用提供方不具备交通一卡通移动票卡应用的个人化能力时，可委托 T-MTPS 平台进行应用个人化操作。如图 14 所示，将交通一卡通移动票卡应用 A 安装在 TSD 下，由 T-MTPS 平台负责完成应用个人化。
7.2.1.4　应用提供方具备交通一卡通移动票卡应用个人化能力时，由应用提供方自行完成应用个人化操作。如图 14 所示，交通一卡通支付应用 A 下载、安装到 TSD 后，被迁移到应用提供方 SSD 下，由应用提供方负责应用个人化。

7.2.2　辅助安全域安全要求

7.2.2.1　TSD及TSD下辅助安全域负责存储其所有方的通讯密钥和DAP验证密钥(DAP验证密钥为可选)。交通一卡通移动票卡应用个人化时,应可借助其关联安全域的安全通讯功能,保护个人化数据的安全性。

7.2.2.2　安全域在创建时，其安全通道协议要求应设置为SCP02并采用i=15或i=55实现方式，并至少注入一组初始密钥。

7.2.2.3　SCP02每组密钥应包含S-ENC、S-MAC和DEK三种密钥，应符合表1的规定。

表1　SCP02密钥信息

类型	标识	用法	长度（Byte）	是否必选
S-ENC	0x01	安全通道的鉴权和数据加密	16	是
S-MAC	0x02	安全通道的MAC验证和生成	16	是
DEK	0x03	敏感数据加/解密	16	是

7.2.3　辅助安全域权限要求

7.2.3.1　TSD应至少具备的权限应符合表2的规定。

表2　TSD权限

序号	权限	描述
1	安全域权限（Security Domain）	拥有此权限的应用是一个安全域
2	委托管理权限（Delegated Management）	拥有此权限的应用应能够对卡片内容进行委托管理
3	可信路径权限（Trusted Path）	拥有此权限的应用是应用间通信的一条可信路径

7.2.3.2　应用提供方SSD应至少具备的权限应符合表3的规定。

表3　应用提供方SSD权限

序号	权限	描述
1	安全域权限（Security Domain）	拥有此权限的应用是一个安全域
2	可信路径权限（Trusted Path）	拥有此权限的应用是应用间通信的一条可信路径

7.2.4　辅助安全域功能要求

辅助安全域应具备应用迁移、应用个人化和应用服务的能力。在安装辅助安全域时，安装标签C9支持的参数应符合表4的规定，其中82和87标签编码规则应符合表5的规定。

表4　安装标签C9支持的参数

标签	长度（hex）	描述
81	0x02	用于设置安全通道的id和i（15或55）
82	0x01或0x02	用于设置应用或安装包是否可迁入本辅助安全域
84	0x00	如果未出现该项标签，则在个人化结束后默认设置为个人化状态；如果出现该项标签，则在个人化结束后通过set status对设置成个人化状态
87	0x01或 0x02	用于设置应用或安装包是否可从本辅助安全域迁出

表5　82和87标签编码规则

b8	b7	b6	b5	b4	b3	b2	b1	描述
0	0	0	0	0	–	–	–	SSD不接受迁入、迁出。如果安装参数不带82、87标签，此为默认设置
1	0	–	0	–	–	–	–	SSD接受从上一级具有授权管理权限的SSD迁入、迁出
1	1	–	0	–	–	–	–	SSD接受从同一层次体系的任何具有授权管理权限的SSD迁入、迁出
–	–	1	0	–	–	–	–	接受从ISD迁入、迁出
–	–	–	–	1	–	–	–	接受从具有委托管理权限的SSD迁入、迁出
1	1	1	1	–	–	–	–	接受从SE上任何具备授权管理权限的SSD迁入、迁出
–	–	–	–	–	x	x	x	保留

7.3　SE多应用架构B

7.3.1 一般要求

7.3.1.1 SE 多应用架构 B 包括 ISD、TSD、TCSD、应用提供方 SSD 和交通一卡通移动票卡应用，应符合图 15 的规定。

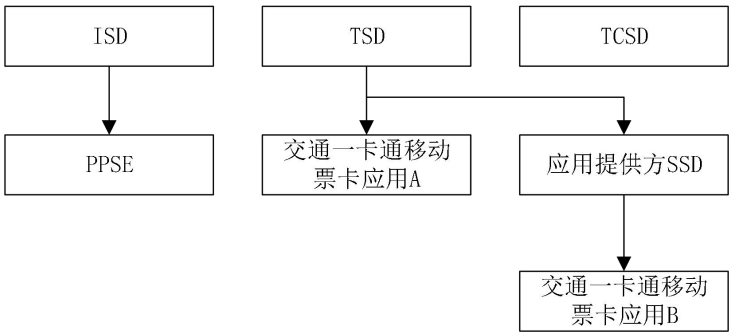


图 15 SE 多应用架构 B

7.3.1.2 TCSD 主要功能是进行 SE 及其持有人实名身份的验证和获取，应满足以下要求：

a) 是 T-MTPS 平台在 SE 内的代表，由 T-MTPS 平台持有；
b) 具备安全域权限；
c) 提供 SCP02 安全通道；
d) 存储的数据包括 SE 持有人的私钥和公钥证书、交通一卡通移动票卡平台公钥证书及其他私有数据。除 SE 持有人私钥以外的数据可以通过 GET DATA 命令获得。

7.3.2 辅助安全域安全要求

SE多应用架构B的辅助安全域安全要求应符合7.2.2的规定。

7.3.3 辅助安全域权限要求

7.3.3.1 TSD 和 TCSD 的权限

TSD和TCSD支持的权限应至少包括表6中的内容。

表 6 TSD 和 TCSD 支持的权限

序号	权限	描述
1	安全域权限（Security Domain）	拥有此权限的应用是一个安全域。
2	授权管理权限（Authorized Management）	拥有此权限的应用应能管理卡片内容。
3	可信路径权限（Trusted Path）	拥有此权限的应用是应用间通信的一条可信路径。

7.3.3.2 应用提供方 SSD 的权限

应用提供方SSD具备的权限应符合7.2.3中的表3规定。

7.3.4 辅助安全域功能要求

SE多应用架构B的辅助安全域功能要求应符合7.2.4的规定。

8 PAMID

8.1 PAMID 应在 TSD 创建过程中作为其属性写入 SE 中，且 PAMID 应一次写入，之后只能读取不能更改。

8.2 存储 PAMID 的标识符（Tag）设置为 0x74，用 STORE DATA 指令写入，用 GET DATA 指令读取。
8.3 PAMID 应由 T-MTPS 统一管理，其编码格式应符合表 7 的规定。

表 7 PAMID 编码格式

发行方机构代码	介质类型	发行方SE内部编码
5 Byte	1 Byte	10 Byte
注：介质类型参数00-SWP（U）SIM卡、01-全终端、02-双界面（U）SIM卡、03-外置设备		

9 交通一卡通身份认证应用

9.1 交通一卡通身份认证应用应能提供 SE 及其持有人实名身份的验证和获取服务，应用内容包括存储经加密的卡片持有人实名身份信息（或信息的索引）。无特殊权限，应安装在 TSD 或 SSD 下，通过 TSD 或 SSD 的安全服务进行个人化，提供私有指令方式验证（或获取）卡片持有人实名身份信息或私有数据的服务。
9.2 身份认证应用包括人脸识别和身份信息的识别。其中人脸识别应符合附录 A 的规定。身份信息的识别可以将身份信息存储在 eID 文件中。

10 安全单元基本命令

SE基本命令应符合表8的规定。

表 8 SE 基本命令

命令	OP_READY			INITIALIZED			SECURED			CARD_LOCKED		TERMINATED	
	AMSD	DMSD	SD	AMSD	DMSD	SD	AMSD	DMSD	SD	FASD	SD	FASD	SD
DELETE 可执行装载文件	□	□	■	□	□	■	□	□	■	■	■	■	■
DELETE 可执行装载文件和相关应用	□	□	■	□	□	■	□	□	■	■	■	■	■
DELETE 应用	√	√	■	√	√	■	√	√	■	■	■	■	■
DELETE 密钥	□	□	□	□	□	□	□	□	□	■	■	■	■
GET DATA	√	√	√	√	√	√	√	√	√	√	■	√	■
GET STATUS	√	□	□	√	□	□	√	□	□	√	■	■	■
INSTALL[加载]	□	□	■	□	□	■	□	□	■	■	■	■	■
INSTALL[安装]	□	□	■	□	□	■	□	□	■	■	■	■	■
INSTALL[加载、安装和设为可选]	□	□	■	□	□	■	□	□	■	■	■	■	■
INSTALL [安装和设为可选]	√	√	■	√	√	■	√	√	■	■	■	■	■
INSTALL[设为可选]	□	□	■	□	□	■	□	□	■	■	■	■	■
	AMSD	DMSD	SD	AMSD	DMSD	SD	AMSD	DMSD	SD	FASD	SD	FASD	SD
INSTALL[迁移]	□	□	■	□	□	■	□	□	■	■	■	■	■
INSTALL[更新注册表]	□	□	■	□	□	■	□	□	■	■	■	■	■
INSTALL[个人化]	□	□	□	□	□	□	□	□	□	■	■	■	■
LOAD	□	□	■	□	□	■	□	□	■	■	■	■	■
PUT KEY	√	□	□	√	□	□	√	√[a]	√[a]	■	■	■	■
SELECT	√	√	√	√	√	√	√	√	√	√	■	■	■
SET STATUS	√	□	□	√	□	□	√	√[b]	√[b]	√	■	■	■

表8　SE基本命令（续）

命令	OP_READY			INITIALIZED			SECURED			CARD_LOCKED		TERMINATED	
	AMSD	DMSD	SD	AMSD	DMSD	SD	AMSD	DMSD	SD	FASD	SD	FASD	SD
STORE DATA	√	□	□	√	□	□	√	□	□	■	■	■	■
注1：√——必备，□——可选，■——禁止； 注2：TCSD及TSD在SE多应用架构B中属于AMSD； 注3：TSD在SE多应用架构A中属于DMSD。													
[a] 支持 DMSD/SD PUT Key 操作。 [b] 支持 DMSD/SD 锁定、解锁相关应用。													

11　密钥要求

11.1　密钥种类

11.1.1　令牌和收条密钥

若SE支持委托管理，则应具有令牌验证权限和生成收条权限的安全域，该安全域应当具有表9所示的密钥，并满足表9的规定。表中RSA密钥的长度应大于等于上述最短长度，且是32位的倍数。

表 9　令牌和收条密钥

密钥	用途	最短长度	说明
令牌	令牌验证（RSA 公钥）	1024 bit	仅委托管理
收条	生成收条（DES 密钥），可选	16 Byte	仅委托管理
收条	生成收条（RSA 私钥），可选	1024 bit	仅委托管理

11.1.2　DAP 验证密钥

若安全域支持DAP验证，则安全域应当有一个RSA公钥或一个DES密钥来验证加载文件数据块签名，并应满足表10的规定。表中RSA密钥的长度应大于等于上述最短长度，且是32位的倍数。

表 10　DAP 验证密钥

密钥	用途	最短长度	说明
DAP 验证	加载文件数据块签名验证（RSA 公钥）	1024 bit	仅 DAP 验证
DAP 验证	加载文件数据块签名验证（DES 密钥）	16 Byte	仅 DAP 验证

11.2　密钥算法

交通一卡通移动票卡业务使用的密钥算法应符合JT/T 978.6的规定。

12　安全通信

SE安全通信采用SCP02安全通道协议，在SECURED状态后，所需的APDU命令的最低安全级别要求应符合表11的规定。

表 11　　所需的 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）

13　应用个人化服务

13.1　一般要求

13.1.1　应用安装后，应加载其个人化数据，包括密钥、发卡机构应用数据和持卡人数据。该应用通过

安全通信及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。

13.1.2 SE 应支持以下两种方式实现个人化服务：

a) 使用运行时消息流；

b) 使用安全域访问。

13.2 运行时的消息流

安全域可以为其直接关联的应用提供运行时支持。应用可以通过关联的安全域服务实现安全通道的建立和数据的安全传递，以实现应用的个人化。运行时消息流实现应用个人化流程应符合图16的规定。

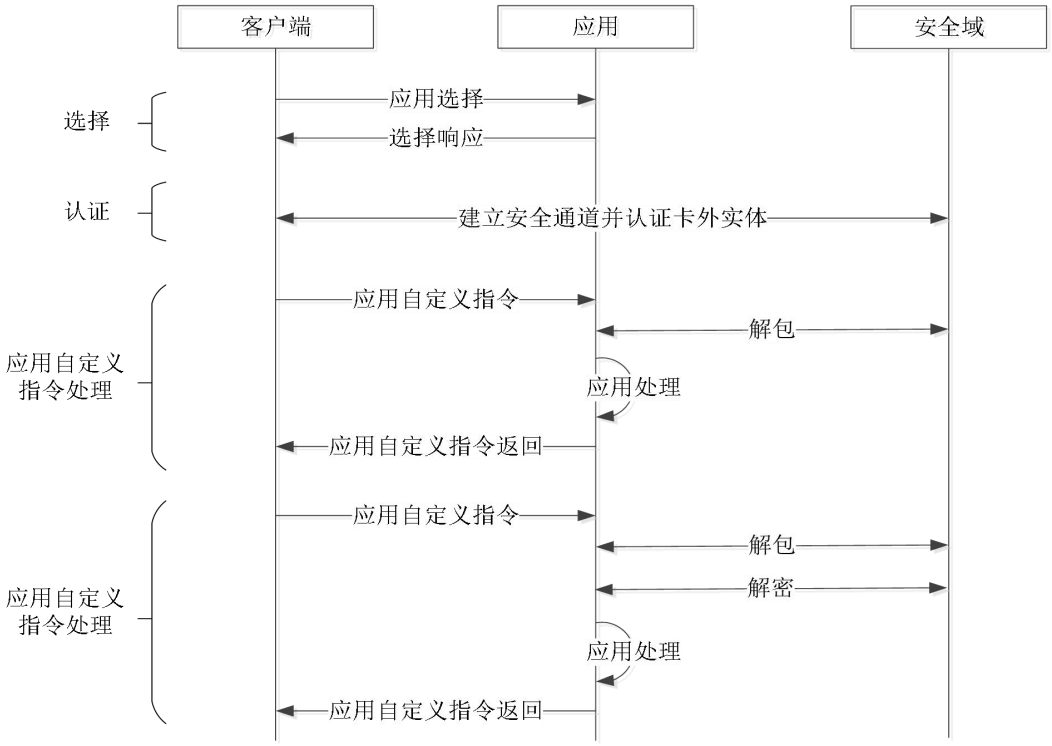


图 16 运行时消息流实现应用个人化流程

13.3 安全域访问

安全域应有能力接收一个STORE DATA指令并发送给与其相关联的应用。安全域将指令转发给应用之前，应能根据安全通道的级别对指令进行验证并解包。解包后的指令结构应保持跟封包之前的格式一致安全域访问实现应用个人化流程应符合图17的规定。

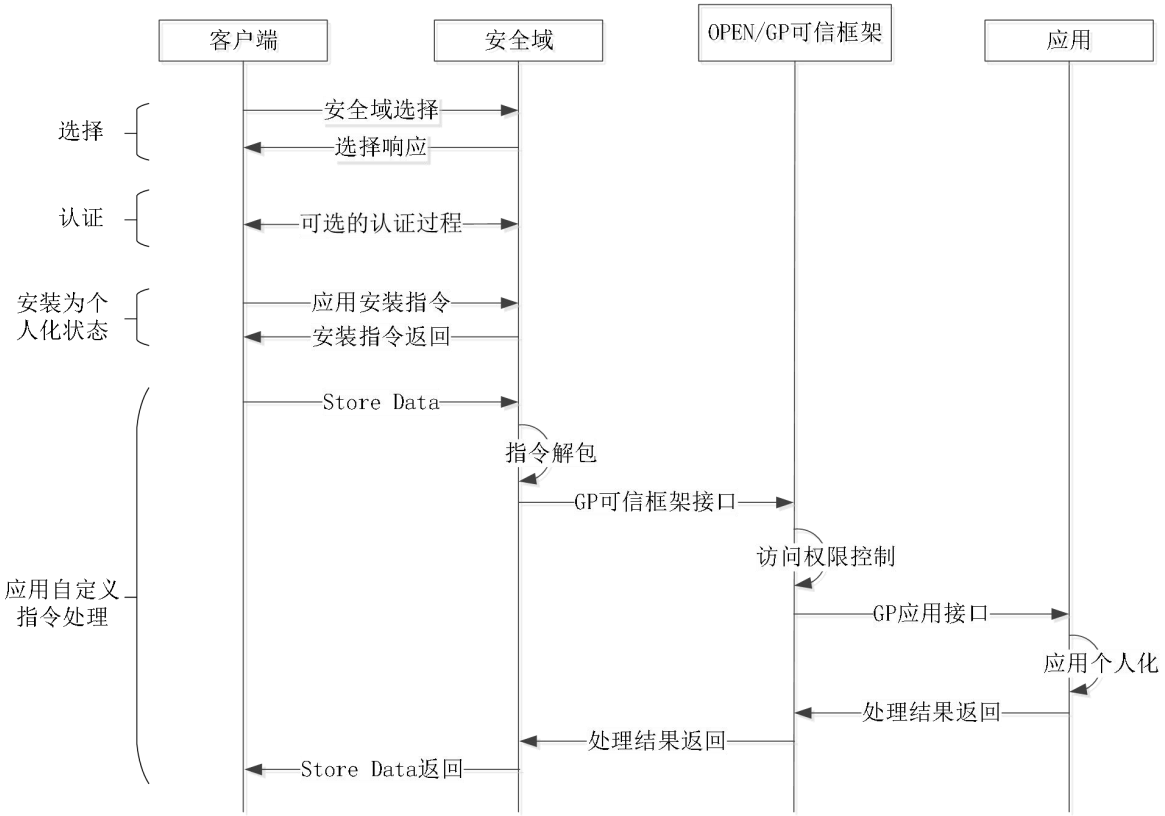


图 17　安全域访问实现应用个人化流程

14　SE 应用选择服务

SE应用选择服务应包括以下两种：

a)　受理环境选择交通一卡通移动票卡应用，非接触途径要求仅提供 PPSE 选择，符合 JT/T 978.2 中相关 PPSE 选择流程的要求，通过 FCI 模板返回应用 AID 列表；

b)　移动票卡终端上的应用管理客户端直接使用 SELECT AID 方式，选择交通一卡通移动票卡应用。

15　交通一卡通移动票卡应用

15.1　电子钱包

15.1.1　文件结构

电子钱包的文件结构应符合图18的规定。

图 18　电子钱包的文件结构

15.1.1.1　二进制文件

公共应用信息文件、持卡人基本信息文件、管理信息文件、交易明细文件、eID 标识文件、照片密文信息文件，应符合 JT/T 978.2—2023 中 B.2.2 的规定。公共应用信息文件中的“应用启用标识”在卡片侧不做判断，由终端侧进行判断。

15.1.1.2　记录文件

15.1.1.2.1　公共交通过程信息变长记录文件

公共交通过程变长记录文件应符合 JT/T 978.2—2023 中 B.2.4 的规定，每个记录文件中的“应用锁定标志”在卡片侧不做判断，由终端侧进行判断。

15.1.1.2.2　公共交通过程信息循环记录文件

公共交通过程信息循环记录文件应符合 JT/T 978.2—2023 中 B.2.5 的规定。

15.1.1.3　照片信息文件

照片信息文件（SFI=0X1B）应符合附录 A 的规定。

15.1.1.4　余额说明

15.1.1.4.1　第一票种余额

卡片应具备电子钱包脱机实际余额计数器1和电子钱包脱机已透支金额计数器2，计数器上限为3个字节FF。第一票种余额由9F51识别，包括：可用余额、透支限额、已透支金额、实际余额、实际余额上限。

15.1.1.4.2　第二票种余额

卡片应具备电子钱包脱机实际余额计数器3和电子钱包脱机已透支金额计数器4，计数器上限为3个字节FF。第二票种余额由DF71识别，包括：可用余额、透支限额、已透支金额、实际余额、实际余额上限。

15.1.2 指令

15.1.2.1 选择 PPSE 命令

选择PPSE（SELECT PPSE）命令应符合JT/T 978.2—2023中C.1.1的规定。

15.1.2.2 选择 ADF 命令

15.1.2.2.1 概述

选择ADF（SELECT ADF）命令属于ISO/IEC 7816-4规定的指令模式4，通过选择AID来选择卡片中ADF。成功执行该命令设定ADF的路径。从卡片返回的响应报文包含回送FCI。

15.1.2.2.2 命令报文编码

SELECT ADF命令报文编码应符合表12的规定。

表 12 SELECT ADF 命令报文编码

编码	值（十六进制）
CLA	00
INS	A4
P1	04
P2	00
Lc	08～10
Data	15.1.3 要求的 AID
Le	00

15.1.2.2.3 命令报文数据域

命令报文数据域应包括DF名、AID。

15.1.2.2.4 响应报文数据域

SELECT ADF命令响应报文数据应符合表13的规定，发卡机构自定义数据应符合表14的规定。

表 13 SELECT ADF 命令响应报文数据

标签	值（十六进制）			条件
6F	FCI 模板			M
	84	DF 名		M
	A5	FCI 数据专用模板		M
		9F51	第 1 票种货币代码	M
		DF71	第 2 票种货币代码	M
		9F08	应用版本号	O
		9F12	应用优先名称	O
		DF00	SM 算法具备指示器	M
		DF0A	eID 信息标识	M
		9F0C	发卡机构自定义数据见表 14	M

表 13 SELECT ADF 响应报文数据（续）

注1：9F51为两个字节，DF71为两个字节。 **注2**：9F08的值为02；9F08为可选项，如果无此Tag，则应用版本默认为01。 **注3**：无DF00标识仅支持国际算法。 **注4**：DF00用于指示当前卡片支持的算法为一字节（00：国际算法，01：国密算法，02：双算法）。 **注5**：DF0A为两字节，第一字节bit0为1时表示支持eID标识，其他bit及第二字节为预留。

表 14　发卡机构自定义数据

数据字段名称	长度（Byte）
发卡机构代码	8
应用类型标识	1
应用启用标识	1
应用序列号	10
应用启用日期	4
应用有效日期	4
发卡机构自定义 FCI 数据	2

15.1.2.2.5　响应报文状态字

SELECT ADF命令响应报文状态字应符合表15的规定。

表 15　SELECT ADF 命令响应报文状态字

SW1	SW2	状态
6A	82	未找到文件
62	83	选择文件无效，应用已临时锁定
62	84	选择文件无效，应用已永久锁定
状态字由SW1和SW2组成。		

15.1.2.3　国际/国密算法操作命令

应符合JT/T 978.2—2023的C.3.22的规定。

15.1.2.4　应用锁定命令

15.1.2.4.1　概述

应用锁定（APPLICATION BLOCK）命令属于ISO/IEC 7816-4规定的指令模式3，使当前选择的应用失效，该指令只能在特殊终端上使用。当APPLICATION BLOCK命令成功完成应用临时锁定后，用SELECT命令选择已临时锁定的应用（电子钱包、电子现金应用），将回送状态字“选择文件无效”（SW1 SW2=6283），同时回送FCI。当APPLICATION BLOCK命令成功完成应用永久锁定后，电子钱包、电子现金应用执行所有命令，卡片将回送状态字“应用永久锁定”（SW1 SW2=9303）。对其他命令的影响根据不同应用而定。

15.1.2.4.2　命令报文编码

APPLICATION BLOCK命令报文编码应符合表16的规定。

表 16　APPLICATION BLOCK 命令报文编码

编码	值（十六进制）
CLA	84
INS	1E
P1	00：使用国际算法 01：使用国密算法
P2	00 或 01
Lc	数据字节数

表16　APPLICATION BLOCK命令报文编码（续）

编码	值（十六进制）
Data	MAC 数据元
Le	不存在
注1：P2-00，此命令执行成功后可锁定应用，但该应用可用APPLICATION UNBLOCK命令解锁。 注2：P2-01，此命令执行成功后将永久锁定应用。	

15.1.2.4.3　命令报文数据域

MAC数据元是根据JT/T 978.6，由应用锁定密钥计算。

15.1.2.4.4　响应报文数据域

响应报文数据域不存在。

15.1.2.4.5　响应报文状态字

此命令执行成功的状态字是9000;如果卡片为表17中的状态,则应按表17的规定返回相应的状态字。

表 17　APPLICATION BLOCK 命令响应报文状态字

SW1	SW2	状态
62	00	无信息提供
62	81	回送数据可能出错
62	83	选择文件无效
6A	81	不具备此功能
93	03	应用永久锁定
64	00	状态标志位未变
65	81	内存失败
69	82	不满足安全状态
69	84	未取随机数
69	87	安全报文数据项丢失
69	88	安全报文数据项不正确
6A	88	未找到引用数据

15.1.2.5　应用解锁命令

15.1.2.5.1　概述

应用解锁（APPLICATION UNBLOCK）命令属于ISO/IEC 7816-4规定的指令模式3，用于恢复卡片应用，该指令只能在解锁终端上使用。当APPLICATION UNBLOCK命令成功完成后,自动取消由APPLICATION BLOCK命令产生的对卡片命令响应的限制，并将消费、圈存、圈提、复合消费和修改透支限额命令中的MAC错误计数器清零。

15.1.2.5.2　命令报文编码

APPLICATION UNBLOCK命令报文编码应符合表18的规定。

表 18　APPLICATION UNBLOCK 命令报文编码

编码	值（十六进制）
CLA	84
INS	18
P1	00：使用国际算法 01：使用国密算法
P2	00
Lc	数据字节数
Data	MAC 数据元
Le	不存在

15.1.2.5.3 命令报文数据域

MAC数据元由应用解锁密钥计算。

15.1.2.5.4 响应报文数据域

响应报文数据域不存在。

15.1.2.5.5 响应报文状态字

当应用被临时锁定时，此命令执行成功的状态字是9000。当应用未被临时锁定，此命令执行返回的状态字是使用条件不满足（SW1 SW2=6985）。如果卡片为表19中的状态，则应按表19的规定返回相应的状态字。

表 19 APPLICATION UNBLOCK 响应报文状态字

SW1	SW2	状态
64	00	标志状态位未变
65	81	内存失败
69	01	命令不接受（无效状态机）
69	82	不满足安全状态
69	84	未取随机数
69	85	使用条件不满足
69	87	安全报文数据项丢失
69	88	安全报文数据项不正确
93	03	应用已被永久锁定

15.1.2.6 外部认证命令

应符合JT/T 978.2—2023的C.3.3的规定。

15.1.2.7 取随机数命令

应符合JT/T 978.2—2023的C.3.4的规定。

15.1.2.8 读二进制文件命令

应符合JT/T 978.2—2023的C.3.6的规定，如果卡片为表20中的状态，则应按表20的规定返回相应的状态字。

表 20 READ BINARY 响应报文状态字

SW1	SW2	状态
62	81	部分回送的数据可能有错
62	82	文件长度<Le
69	81	命令与文件结构不相容
69	82	不满足安全状态
69	86	不满足命令执行的条件（非当前 EF）
6A	81	不具备此功能
6A	82	未找到文件
6B	00	参数错误（偏移地址超出了 EF）
62	83	临时锁定
93	03	永久锁定
6C	XX	长度错误（Le 错误；XX 为实际长度）

15.1.2.9 更新二进制文件命令

应符合JT/T 978.2-2023的C.3.7的规定。

15.1.2.10 初始化圈存命令

15.1.2.10.1 概述

初始化圈存（INITIALIZE FOR LOAD）命令属于ISO/IEC 7816-4规定的指令模式4，用于初始化圈存交易。

15.1.2.10.2 命令报文编码

INITIALIZE FOR LOAD命令报文编码应符合表21的规定。

表 21 INITIALIZE FOR LOAD 命令报文编码

编码	值（十六进制）
CLA	80
INS	50
P1	00：交易第 1 票种 10：交易第 2 票种
P2	02
Lc	0B
Data	按表 22
Le	10

15.1.2.10.3 命令报文数据域

INITIALIZE FOR LOAD命令报文数据域应符合表22的规定。

表 22 INITIALIZE FOR LOAD 命令报文数据域

元素	长度（Byte）
密钥索引号	1
交易金额	4
终端机编号	6

15.1.2.10.4 响应报文数据域

此命令执行成功的响应报文数据域应符合表23的规定；如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表 23 INITIALIZE FOR LOAD 响应报文数据域

元素	长度（Byte）
电子钱包余额（实际余额+透支限额-已透支金额）	4
联机交易序号	2
密钥索引（DLK）	1
算法标识（DLK）	1
伪随机数（卡片）	4
MAC1	4

15.1.2.10.5 响应报文状态字

此命令执行成功的状态字是9000;如果卡片为表24中的状态,则应按表24的规定返回相应的状态字。

表 24 INITIALIZE FOR LOAD 响应报文状态字

SW1	SW2	状态
65	81	内存错误
69	85	使用条件（状态机）不满足
93	03	应用永久锁定
6A	81	功能不具备
94	01	交易金额超限
94	03	密钥索引不具备
94	02	交易计数器达到最大值

15.1.2.11 圈存命令

15.1.2.11.1 概述

圈存（CREDIT FOR LOAD）命令属于ISO/IEC 7816-4规定的指令模式4，用于圈存交易。

15.1.2.11.2 命令报文编码

CREDIT FOR LOAD命令报文编码应符合表25的规定。

表 25 CREDIT FOR LOAD 命令报文编码

编码	值（十六进制）
CLA	80
INS	52
P1	00：交易第 1 票种 10：交易第 2 票种
P2	00
Lc	0B
Data	按表 26
Le	04

15.1.2.11.3 命令报文数据域

CREDIT FOR LOAD命令报文数据域应符合表26的规定。

表 26 CREDIT FOR LOAD 命令报文数据域

元素	长度（Byte）
交易日期（主机）	4
交易时间（主机）	3
MAC2	4

15.1.2.11.4 响应报文数据域

CREDIT FOR LOAD响应报文数据域应符合表27的规定；如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表 27 CREDIT FOR LOAD 响应报文数据域

元素	长度（Byte）
TAC	4

15.1.2.11.5 响应报文状态字

此命令执行成功的状态字是9000;如果卡片为表28中的状态,则应按表28的规定返回相应的状态字。

表 28 CREDIT FOR LOAD 响应报文状态字

SW1	SW2	状态
65	81	内存错误
69	01	命令不接受（无效状态机）
69	85	使用条件不满足
93	02	MAC 无效
62	83	连续累计圈存 MAC 错误超限后临时锁定应用
93	03	应用永久锁定

15.1.2.12 初始化消费命令

15.1.2.12.1 概述

初始化消费（INITIALIZE FOR PURCHASE）命令属于ISO/IEC 7816-4规定的指令模式4，用于初始化消费交易。

15.1.2.12.2 命令报文编码

INITIALIZE FOR PURCHASE命令报文编码见表29。

表 29　INITIALIZE FOR PURCHASE 命令报文编码

编码	值（十六进制）
CLA	80
INS	50
P1	01：交易第 1 票种 11：交易第 2 票种
P2	02
Lc	0B
Data	按表 30
Le	0F

15.1.2.12.3　命令报文数据域

INITIALIZE FOR PURCHASE命令报文数据域应符合表30的规定。

表 30　INITIALIZE FOR PURCHASE 命令报文数据域

元素	长度（Byte）
密钥索引号	1
交易金额	4
终端机编号	6

15.1.2.12.4　响应报文数据域

此命令执行成功的响应报文数据域应符合表31的规定；如果命令执行不成功，则只在响应报文中回送SW1和SW2。

表 31　INITIALIZE FOR PURCHASE 响应报文数据域

元素	长度（Byte）
电子钱包余额（实际余额+透支限额-已透支金额）	4
脱机交易序号	2
透支限额	3
密钥索引	1
算法标识	1
伪随机数（卡片）	4

15.1.2.12.5　响应报文状态字

此命令执行成功的状态字是9000;如果卡片为表32中的状态,则应按表32的规定返回相应的状态字。

表 32　INITIALIZE FOR PURCHASE 响应报文状态字

SW1	SW2	状态
65	81	内存错误
69	85	使用条件（状态机）不满足
93	03	应用永久锁定
94	01	交易金额超限
94	03	密钥索引不具备
94	02	交易计数器达到最大值

15.1.2.13　消费命令

15.1.2.13.1　概述

消费（DEBIT FOR PURCHASE）命令属于ISO/IEC 7816-4规定的指令模式4，用于消费交易。

15.1.2.13.2　命令报文编码

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/798115011124006067