

DBJT45

广西壮族自治区交通运输行业指南

DBJT 45/T 019—2020

交通一卡通移动支付技术指南

Technical guide for mobile payment of transport card

2020 - 12 - 05 发布

2021 - 01 - 01 实施

广西壮族自治区交通运输厅

发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 5

5 总则 5

6 安全单元 8

7 近场支付 9

8 远程支付 18

9 客户端软件 21

10 可信服务管理系统 28

11 终端设备 29

12 检测项目 30

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。

本文件由广西壮族自治区交通运输厅提出并宣贯。

本文件由广西交通运输标准化技术委员会归口。

本文件起草单位：广西交通一卡通有限公司。

本文件主要起草人：陈志、黄云川、覃山、蒲建勇、寿文斌、雷方韵、钟振、梁伟、罗凯、韦晶、谭亮、黄海杰、韦海峰。

交通一卡通移动支付技术指南

1 范围

本文件规定了广西交通一卡通移动的术语和定义、缩略语、总则、安全单元、近场支付、远程支付、客户端软件、可信服务管理系统、终端设备以及检测项目。

本文件适用于广西交通一卡通移动支付技术的相关系统、受理终端、智能终端客户端软件等的设计、研发和应用。

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。

- JT/T 978.2—2015 城市公共交通IC卡技术规范 第2部分：卡片
- JT/T 978.3 城市公共交通IC卡技术规范 第3部分：读写终端
- 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—2016 交通一卡通移动支付技术规范 第1部分：总则
- 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
- JT/T 1059.3—2016 交通一卡通移动支付技术规范 第3部分：近场支付
- 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 1059.5—2016 交通一卡通移动支付技术规范 第5部分：客户端软件
- 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
- JT/T 1059.7—2016 交通一卡通移动支付技术规范 第7部分：终端设备
- JT/T 1059.8—2016 交通一卡通移动支付技术规范 第8部分：检测项目

3 术语和定义

下列术语和定义适用于本文件。

3.1

广西交通一卡通卡 Guangxi urban public transport card
主要用于广西城市公共交通方式小额支付的集成电路卡。

3.2

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，主要分为近场支付和远程支付两种。

[来源：JT/T 1059.1—2016，3.2]

3.3

移动支付终端 mobile payment terminal

具有广西交通一卡通移动支付应用及移动通信能力的终端设备。

[来源: JT/T 1059.1—2016, 3.3]

3.4

近场支付 proximity payment

移动支付终端通过非接触式终端设备在本地或接入收单网络完成支付过程的支付方式。

[来源: JT/T 1059.1—2016, 3.4]

3.5

远程支付 remote payment

使用移动支付终端通过无线通信网络,与后台服务器之间进行交互,由服务器端完成交易处理的支付方式。

[来源: JT/T 1059.1—2016, 3.5]

3.6

终端设备 terminal

为广西交通一卡通移动支付业务提供受理环境的设备。

[来源: JT/T 1059.1—2016, 3.6]

3.7

收单网络 acquiring network

从事广西交通一卡通移动支付收单业务的市场主体提供线上和线下实现收单的网络渠道。

[来源: JT/T 1059.1—2016, 3.7]

3.8

支付内容平台 payment content platform

为用户提供订购商品或服务选择的平台。

[来源: JT/T 1059.1—2016, 3.8]

3.9

账户管理系统 account management system

实现广西交通一卡通用户账户体系整体管理功能的业务信息系统,包括账户开户、更改和销户及资金的管理等业务功能。

[来源: JT/T 1059.1—2016, 3.9]

3.10

后台账户 background account

用户在申请广西交通一卡通移动支付应用服务时在账户管理系统建立的对应记录,包括用户个人身份信息及资金信息。

[来源: JT/T 1059.1—2016, 3.10]

3.11

余额 balance

广西交通一卡通用户从后台账户圈存到电子钱包或电子现金中,可用于移动支付消费的金额。

3.12

安全单元 secure element

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]

3.13

安全载体 secure media

承载安全单元的介质。

[来源: JT/T 1059.1—2016, 3.13]

3.14

安全域 security domain

负责对某个安全单元外实体(如安全单元发行方、应用提供方、授权管理者)的管理、安全、通信需求进行支持的安全单元内实体。

[来源: JT/T 1059.1—2016, 3.14]

3.15

应用 application

在安全单元上安装后处于可选择状态的可执行模块的实例。

[来源: JT/T 1059.1—2016, 3.15]

3.16

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]

3.17

安全单元发行方 secure element issuer

为用户提供安全单元发行服务的主体。

[来源: JT/T 1059.1—2016, 3.17]

3.18

可信服务管理 trusted service management

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]

3.19

安全单元应用管理终端 secure element application manage terminal

与可信服务管理平台连接的专用于管理客户端中安全单元应用的终端。

[来源: JT/T 1059.1—2016, 3.19]

注: 安全单元应用管理终端在硬件上可以是销售终端、自助终端或其他类型设备形态, 一般布放在特定的场合, 提供用户对客户端中安全单元应用进行个性化、下载、查询及同步等功能。

3.20

安全单元发行方可信服务管理 secure element issuer trusted service management

为安全单元发行方提供的承载安全单元生命周期管理服务的可信服务管理。

[来源: JT/T 1059.1—2016, 3.21]

3.21

应用提供方可信服务管理 service provider trusted service management

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]

3.22

圈存 load

增加城市公共交通IC卡中电子现金和电子钱包共用余额的过程。

[来源: JT/T 1059.1—2016, 3.23]

3.23

圈提 `unload`

提取城市公共交通IC卡中电子现金和电子钱包共用余额的过程。

[来源: JT/T 1059.1—2016, 3.24]

3.24

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。

[来源: JT/T 1059.2—2016, 3.1]

3.25

辅助安全域 `supplementary security domain`

除主安全域之外的其他安全域。

[来源: JT/T 1059.2—2016, 3.2]

3.26

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。

[来源: JT/T 1059.2—2016, 3.3]

3.27

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文件。

[来源: JT/T 1059.2—2016, 3.7]

3.28

收单系统 `acquiring system`

为近场支付提供终端设备接入、交易信息及结算数据处理等功能的系统。

[来源: JT/T 1059.3—2016, 3.1]

3.29

清算系统 `clearing system`

对近场支付交易进行清算和结算的系统。

3.30

客户端 `client`

用于提供用户接口界面、与安全单元配合实现安全单元管理及应用管理功能的应用软件。

3.31

分体终端 `separated mobile payment terminal`

借助外部设备（如手机、POS）等完成移动支付交易的终端设备。

[来源: JT/T 1059.7—2016, 3.1]

3.32

移动终端 `mobile terminal`

具有移动通信能力的终端设备。

[来源: JT/T 1059.7—2016, 3.3]

3.33

蓝牙 `bluetooth`

用于移动电话、计算机等电子设备的短距离无线连接技术之一。

4 缩略语

下列缩略语适用于本文件。

AID: 应用标识符 (Application Identifier)
 APDU: 应用协议数据单元 (Application Protocol Data Unit)
 ATS: 选择应答 (Answer To Select)
 ECC: 椭圆曲线加密算法 (Elliptic Curves Cryptography)
 GPAT: 通用支付自动测试工具 (General Payment Automatic Testtool)
 IIN: 发卡机构识别码 (Issuer Identification Number)
 ISD: 主安全域 (Issuer Security Domain)
 OTA: 空中下载技术 (Over The Air Technology)
 POS: 销售终端 (Point Of Sale)
 PPSE: 近距离系统支付环境 (Proximity Payment Systems Environment)
 SE: 安全单元 (Secure Element)
 SEI-TSM: 安全单元发行方可信服务管理 (SE Issuer Trusted Service Management)
 STP: SIM卡开发工具包 (SIM Card Tool Kit)
 SP-TSM: 应用提供方可信服务管理 (Service Provider Trusted Service Management)
 SSD: 辅助安全域 (Supplementary Security Domain)
 SWP: 单线协议 (Single Wire Protocol)
 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)
 WIFI: 无线网 (Wireless Fidelity)

5 总则

5.1 系统组成和功能

5.1.1 系统组成

5.1.1.1 广西交通一卡通移动支付系统由 SE、TSM 系统、客户端软件组成，安全和检测作为支撑体系保障系统安全、正常运作。系统框架如图 1 所示。

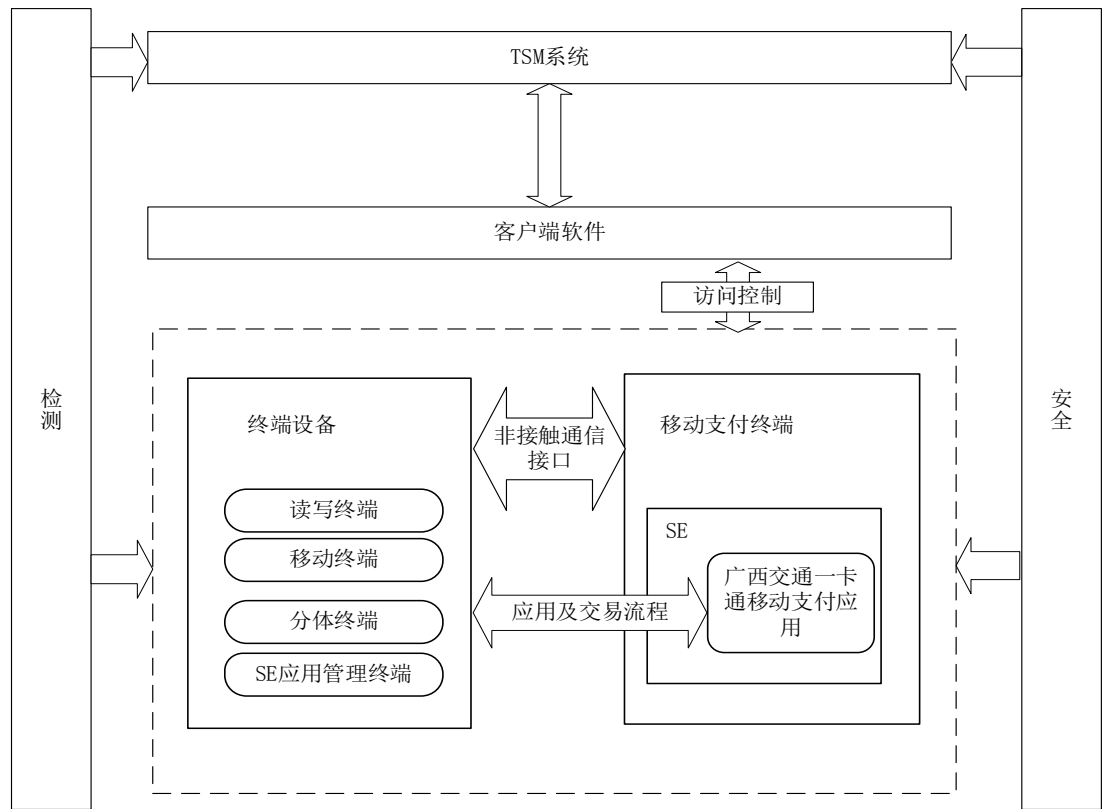


图1 系统框架

5.1.1.2 广西交通一卡通移动支付系统应以 SE 为载体，客户端软件为用户入口，依靠安全、可靠的网络，通过广西交通一卡通移动支付系统间统一的数据接口，实现空中发卡、空中圈存、消费、迁卡移资等功能。

5.1.1.3 广西交通一卡通移动支付应用场景包括近场支付和远程支付。

5.1.2 系统功能

5.1.2.1 SE

SE承载于全终端中，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信息及其持有人的实名身份信息，为应用提供方提供TSD管理、广西交通一卡通移动支付应用下载授权等功能，配合TSM系统实现相关服务。

5.1.2.2 TSM 系统

5.1.2.2.1 广西交通一卡通移动支付系统中的 TSM 系统可分为 SP-TSM 平台与 SEI-TSM 平台。

5.1.2.2.2 广西 SP-TSM 平台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、空中圈存等功能需求。

5.1.2.2.3 SEI-TSM 平台 SE 终端设备厂家自行建设后接入广西 SP-TSM 平台，也可使用广西省级中心建设的 SEI-TSM 平台，SEI-TSM 平台应提供 SE 载体管理与多应用管理，包括 SE 的生命周期管理、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。

5.1.2.3 客户端软件

客户端软件应连接手机终端与广西交通一卡通移动支付系统各参与方TSM的后台，以图文界面展示方式在为用户提供开卡、消费、圈存、账户余额查询、迁卡移资、删除卡片等功能。

5.1.2.4 终端设备

5.1.2.4.1 终端设备应提供广西交通一卡通移动支付业务的受理环境。

5.1.2.4.2 根据业务场景的不同，终端设备可包括以车载闸机为主的读写终端、具备移动通信能力的移动终端、配合移动终端完成支付功能的移动支付终端、配合移动终端使用的分体终端以及以自助式实现 SE 应用下载等功能的 SE 应用管理终端。

5.1.2.5 安全

系统中各种交易数据、数据传输及系统整体的安全性应通过密钥管理系统及数字证书认证中心(CA)系统保证。

5.1.2.6 检测

系统检测应具备依据统一的技术标准、质量要求和业务流程，对TSM平台、终端设备、客户端软件及SE嵌入式应用进行检测的功能，确保广西交通一卡通移动支付系统内各部分的规范性、稳定性和可靠性、以及入网各方技术环境的一致性和兼容性。

5.2 总体技术要求

5.2.1 SE

SE的架构、应用功能、基本命令、通信要求及密钥要求等，应符合JT/T 1059.2的规定。SE中承载的广西交通一卡通移动支付应用的实现方式应符合JT/T 978.2的规定。

5.2.2 TSM 系统

5.2.2.1 TSM 系统应兼顾移动支付在多种交通方式间的业务差异，实现用户对应用客户端下载、读写终端刷卡交易、近场支付及远程支付中各类交易流程的统一化和规范化。

5.2.2.2 TSM 系统应采用符合国际、国内通用标准的通信接口与信息接口，保障与相关系统的互联互通，以及相关交易信息的交换，为空中发卡、空中圈存等业务提供技术支持，为系统接入的应用发行方清分与结算提供有效数据支撑，保证系统的先进性、运行的稳定性及未来行业发展的可扩展性。

5.2.2.3 TSM 系统的技术要求应符合 JT/T 1059.6 的规定。

5.2.3 客户端软件

客户端软件作为连接手机等移动终端与广西交通一卡通移动支付系统各参与方TSM的后台服务软件，应满足TSM系统涉及的应用功能、安全要求及管理要求，并制定统一的技术要求。

5.2.4 终端设备

5.2.4.1 终端设备应按其应用场景划分类型。

5.2.4.2 终端设备与移动支付终端配合实现广西交通一卡通移动支付刷卡消费时采用的非接触通信接口应符合 JT/T 978.5 的规定，与移动支付终端间的交易流程应符合 JT/T 978.3 的规定。

5.2.5 安全

广西交通一卡通移动支付系统应采用对称密钥和非对称密钥相结合的方式,通过密钥的安全机制和加密算法,保证卡片金额、终端近场支付交易数据和远程支付交易数据的传输及系统整体的安全性。

5.2.6 检测

广西交通一卡通移动支付系统的检测项目应包含可信服务管理系统检测项目、客户端检测项目、终端设备检测项目、安全单元检测项目及GPAT测试。

6 安全单元

6.1 类型及其基本要求

应符合JT/T 1059.2—2016中第5章要求。

6.2 多应用管理

应符合JT/T 1059.2—2016中第6章要求。

6.3 多应用结构

符合JT/T 1059.2—2016中第7章要求。

6.4 支付账户介质识别码

应符合JT/T 1059.2—2016中第8章要求。

6.5 交通一卡通身份认证应用模型

应符合JT/T 1059.2—2016中第9章要求。

6.6 安全单元基本命令应用模型

应符合JT/T 1059.2—2016中第10章要求。

6.7 密钥要求

6.7.1 总则

应符合JT/T 1059.2—2016中第11章要求。

6.7.2 卡片密钥要求

针对卡片密钥,需严格按照全国交通一卡通互联互通平台下发的密钥值与分散规则发行到卡内,其余密钥可以由发卡机构自行定义,卡片密钥的组成规则需符合JT/T 978.6的要求,卡片密钥类型见表1。

表1 卡片密钥类型表

密钥用途	说明
全国消费密钥	一级分散后下发，用于入网机构所发行的用户卡电子钱包应用消费主密钥。
AC密钥	一级分散后下发，用于入网机构所发行的用户卡电子现金应用AC密钥。
TAC密钥	一级分散后下发，用于入网机构所发行的用户卡电子钱包应用TAC密钥。
用户卡应用维护密钥（应用锁定）	一级分散后下发，用于入网机构所发行的用户卡应用锁定。
互通记录保护密钥-电子现金	一级分散后下发，用于入网机构所发行的用户卡电子现金应用的行业扩展应用文件修改。
互通记录保护密钥-电子钱包	一级分散后下发，用于入网机构所发行的用户卡电子现金应用的复合交易文件修改。

6.8 安全通信

应符合JT/T 1059.2—2016中第12章要求。

6.9 应用个人化服务

应符合JT/T 1059.2—2016中第13章要求。

6.10 安全单元应用选择服务

应符合JT/T 1059.2—2016中第14章要求。

7 近场支付

7.1 应用模型

应符合JT/T 1059.3—2016中第5章要求。

7.2 交易分类与应用要求

根据移动支付终端与终端设备之间交互方式的不同，近场支付应用可分为电子现金应用和电子钱包应用。应用要求如下：

- a) 电子现金应用应符合 JT/T 978.2—2015 第 7 章要求，交互流程应符合 JT/T 978.3 的要求；
- b) 电子钱包应用应符合 JT/T 978.2—2015 第 8 章要求，交互流程应符合 JT/T 978.3 的要求。

7.3 交易模型

7.3.1 脱机交易模型

用户通过移动支付终端与终端设备交互进行支付，由终端设备直接进行承兑或拒绝，并在交易完成后通过收单系统和转接清算系统将交易通知或文件转发至账户管理系统进行清算处理。如图2所示。

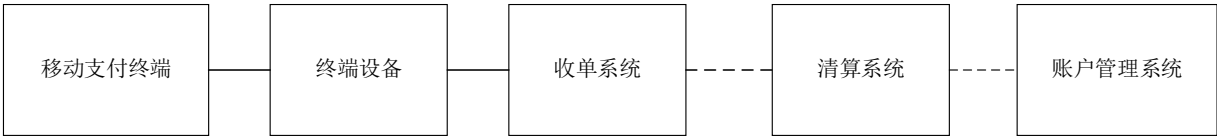


图2 脱机交易模型

7.3.2 联机交易模型

应符合JT/T 1059.3—2016中7.2的要求。

7.3.3 移动支付终端内部交易模型

移动支付终端内部交易模型是SE与客户端(含STK)之间进行的交互。如图3所示。

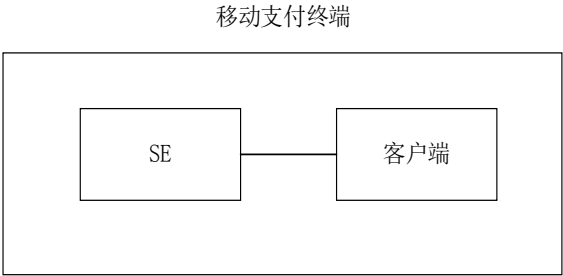


图3 移动支付终端内部交易模型

7.3.4 外置式 SE 交易模型

应符合JT/T 1059.3—2016中7.4的要求。

7.3.5 云端支付交易模型

应符合JT/T 1059.3—2016中7.5的要求。

7.3.6 应用管理交易模型

应符合JT/T 1059.3—2016中7.6的要求。

7.4 交易流程

7.4.1 电子钱包脱机交易流程

7.4.1.1 应用支持判断

通过选择PPSE获得卡片返回的信息，判断卡片是否支持终端应用所需支持的钱包应用模式。如图4所示。

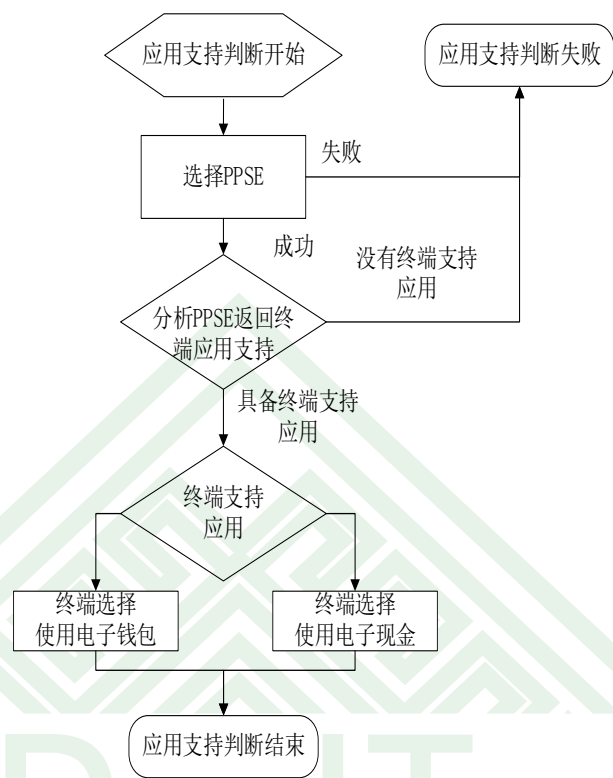


图4 应用支持判断

7.4.1.2 用户卡识别

通过用户卡识别，分析卡的业务可执行性，并确定后续该执行单步消费处理还是多步消费处理。如图5所示。

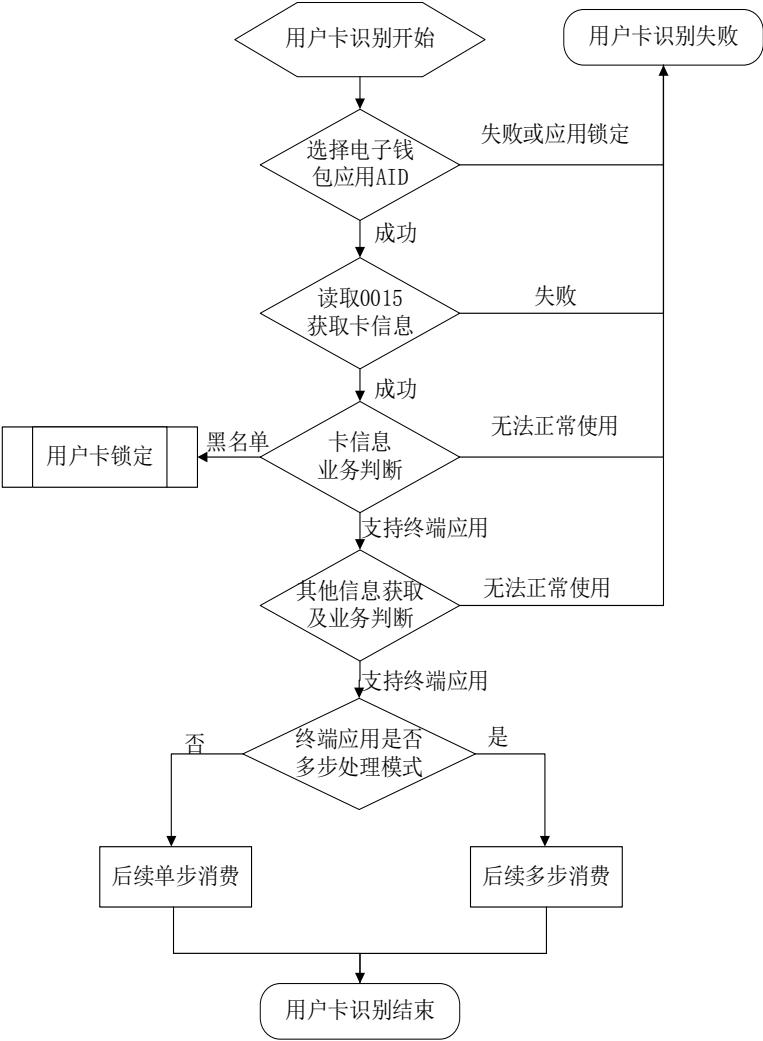


图5 用户卡识别

7.4.1.3 单步消费

通过单步消费，完成单步消费应用业务。如图6所示。

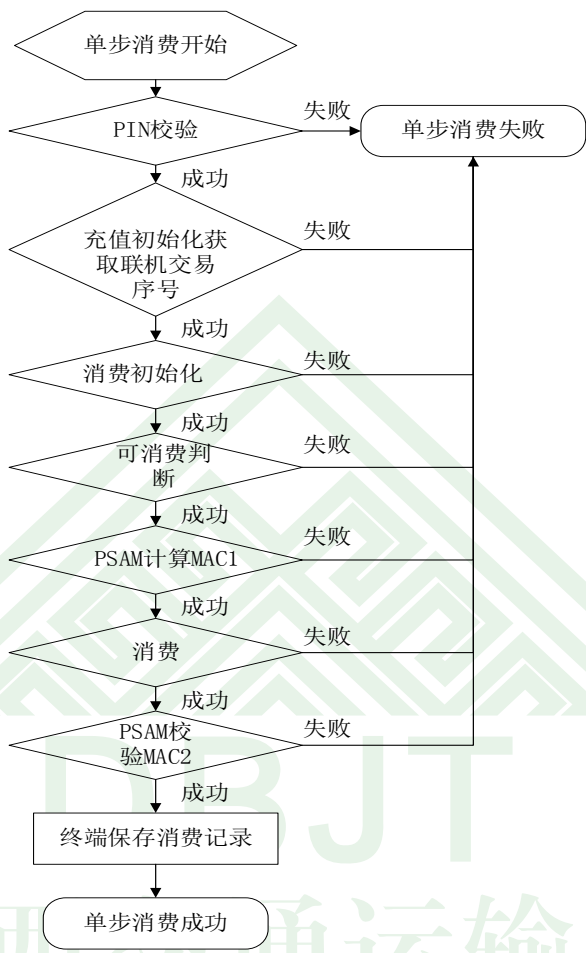


图6 单步消费

7.4.1.4 多步消费初步

通过多步消费初步，完成多步消费应用业务末步交易判断所需的关键信息写入。如图7所示。

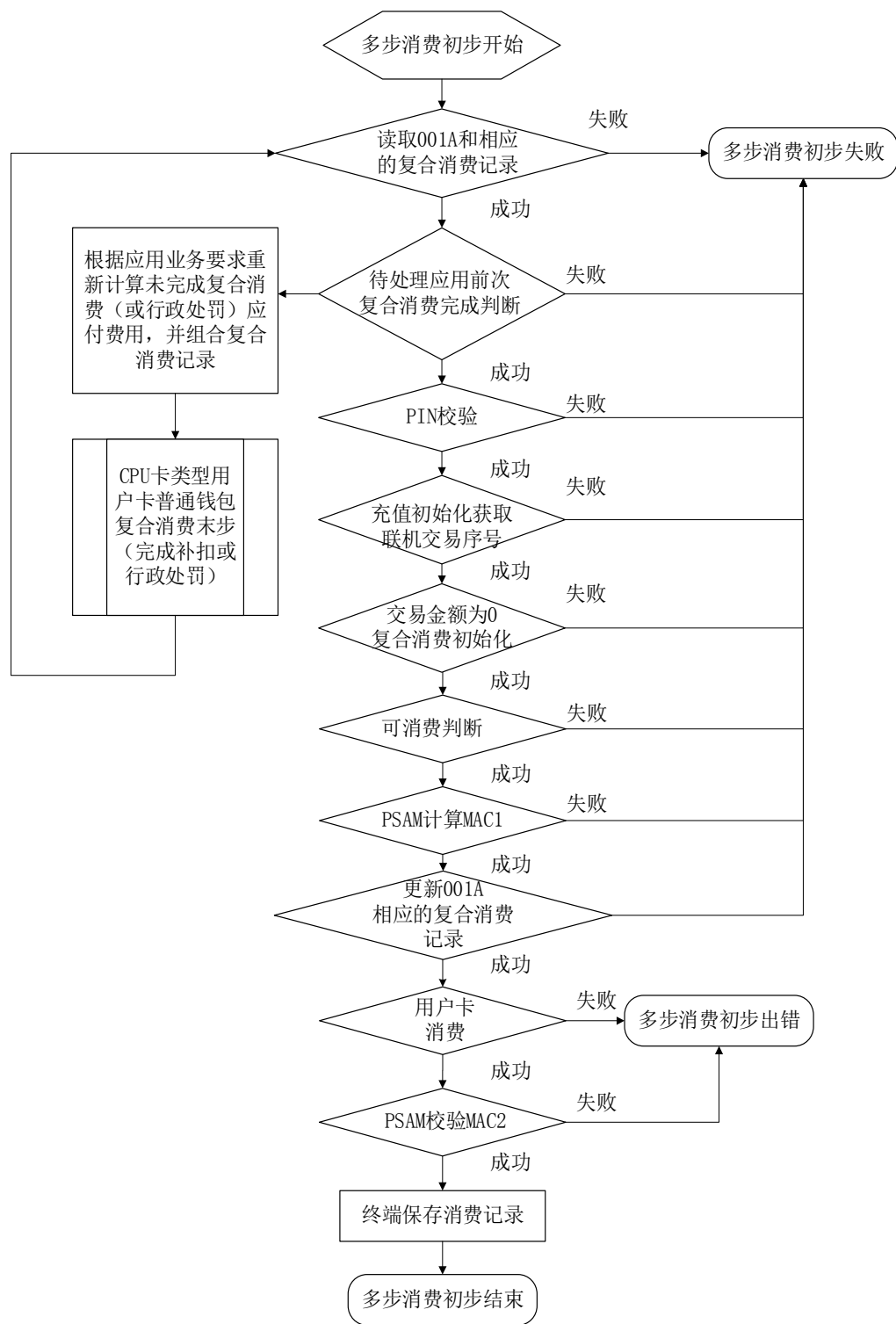


图7 多步消费初步

7.4.2 电子现金交易流程

7.4.2.1 电子现金联机交易流程实例如图 8 所示。

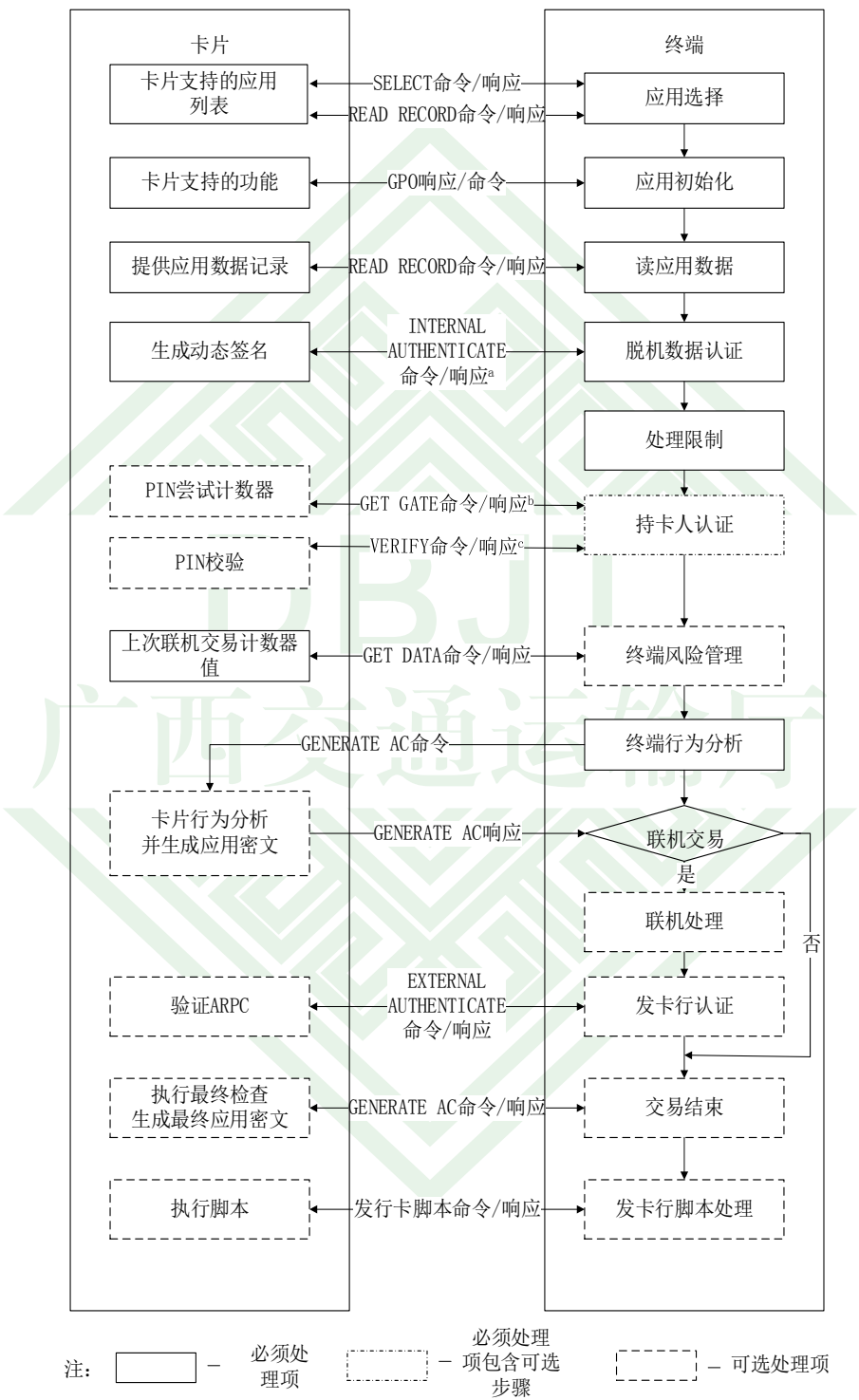


图8 电子现金联机交易流程实例

7.4.2.2 电子现金联机交易流程如下：

- a) 应用选择。此为必备项。当卡片连接终端时，终端决定哪些应用由卡片和终端共同支持，终端选择应用的方法包括：
 - 1) 终端检测终端和卡片都支持的应用并进行显示，供用户选择；
 - 2) 终端根据发卡机构预定义的优先级别自动选择卡片上优先级最高的应用；
 - 3) 终端发送选择命令(SELECT)选择应用，卡片返回文件控制信息(FCI)，其中应包括PDOL。
- c) 应用初始化。此为必备项。在终端选择应用之后，应读取卡片中的应用数据，以获取卡片具备的功能以及需要提供给卡片的支持等信息。终端读取卡片指示的数据，并使用支持的功能列表，来决定要执行的处理流程；
- d) 读应用数据。此为必备项。终端使用读记录命令(READ RECORD)读出交易处理中使用的卡片数据，卡片在应用初始化的响应中提供AFL，标记了这些数据所在的文件与记录号，终端应存储读出的所有可识别的数据对象；
- e) 脱机数据认证。此为可选项。终端根据卡片和终端对脱机数据认证功能的支持情况，决定是否使用动态数据认证来脱机认证卡片。如果终端支持脱机数据认证功能，并且检测到卡片支持动态数据认证(DDA)，则终端需进行脱机数据认证；
- f) 处理限制。此为必备项。终端执行交易处理限制来判断交易是否允许进行。终端应对卡片是否达到生效日期、卡片是否超过失效日期、卡片和终端的应用版本是否匹配、应用用途控制(AUC)限制是否生效进行检查。发卡机构可使用AUC限制卡片的应用，包括国内、国外、现金、商品、服务或返现；
- g) 持卡人验证。此为必备项。持卡人验证可用来确保持卡人合法并且卡片没有遗失或被盗。终端使用卡片中的持卡人验证方法(CVM)列表数据决定验证的执行方法。CVM列表建立了持卡人验证方法优先级别，根据终端能力和交易特性提示用户采用特定的持卡人验证方法。如果持卡人验证方法是脱机PIN，终端提示持卡人输入PIN并传送持卡人输入的PIN到卡片中，卡片比较输入的PIN和卡片中的PIN值；

注：CVM也可能指定联机PIN、签名或不需要持卡人验证。

- h) 终端风险管理。此为必备项。终端应具备风险管理功能。终端风险管理检查包括：交易是否超过最低限额、账号是否在终端异常文件中、连续脱机交易次数是否超过限制次数、是否新卡、商户是否强制进行联机；

注：终端风险管理也包括可选的频度检查。终端使用卡片中的数据进行检查。在终端行为分析过程中要考虑终端频度检查的结果。

- i) 终端行为分析。此为必备项。终端应具备终端行为分析功能。终端行为分析根据脱机数据认证、处理限制、持卡人验证、终端风险管理的结果以及终端和卡片中设置的风险管理参数，决定如何继续交易(脱机批准、脱机拒绝和联机授权)。由卡片返回给终端的发卡机构行为代码(IAC)设立卡片规则，在终端行为代码设立终端规则。决定交易处理之后，终端向卡片请求应用密文。不同的应用密文对应不同的交易处理：以交易证书(TC)为批准，授权请求密文(ARQC)为联机请求，应用认证密文(AAC)为拒绝。如下：
 - 1) 同意脱机完成(TC)；
 - 2) 联机授权(ARQC)；
 - 3) 拒绝交易(AAC)。
- j) 卡片行为分析。此为必备项。卡片应可执行发卡机构定义的风险管理算法以防止发卡机构被欺诈。当卡片收到终端的应用密文请求时，卡片就执行风险管理检查，来决定是否要改变终端设定的交易处理，检查包括：先前未完成的联机交易、上一笔交易发卡机构认证或脱机数据认证

失败、达到了交易笔数或金额的限制等。卡片可将终端请求的脱机接受改成联机授权或脱机拒绝。卡片不能推翻终端做出的拒绝交易的决定。卡片可决定以下方式继续交易：

- 1) 同意脱机完成 (TC)；
- 2) 联机授权 (ARQC)；
- 3) 拒绝交易 (AAC)。

注：完成检查后，卡片使用应用数据及一个存储在卡片上的应用密文过程密钥生成应用密文，再将这个密文返回到终端。对于脱机批准的交易，TC以及生成TC的数据通过清算消息传送给发卡机构，以备未来发生持卡人争议或退单时使用。当持卡人对交易有争议时，TC可作为交易的证据还可验证商户或收单机构是否未改动交易数据。

k) 联机处理：

- 1) 此为可选项。如果卡片或终端决定交易需要进行联机授权，同时终端具备联机能力，终端将卡片产生的 ARQC 报文送至发卡机构进行联机授权。此报文包括 ARQC 密文，用来生成 ARQC 的数据以及表示脱机处理结果的指示器。在联机处理中，发卡机构在联机卡片认证方法 (CAM) 过程中验证 ARQC 来认证卡片。发卡机构可在它的授权决定中查看 CAM 结果和脱机处理结果；
- 2) 传送回终端的授权响应信息可包括发卡机构生成的授权响应密文 (ARPC) (由 ARQC、授权响应码和卡片应用密文过程密钥产生)。此响应也可包括发卡机构脚本，对卡片进行发卡后更新；
- 3) 如果授权响应包含 ARPC 而且卡片支持发卡机构认证，卡片通过确认 ARPC 而执行发卡机构认证，来校验响应数据是否来自真实的发卡机构 (或其代理)。在成功得到发卡机构认证数据后，才能在卡片里重新设置某些相关的安全参数。这阻止了通过模拟联机处理来剽窃卡片的安全特性，以及通过欺诈性地批准交易来重设卡片的计数器和指示器。如果发卡机构认证失败，随后的卡片交易将发送联机授权，直到发卡机构认证成功，发卡机构有权设置卡片拒绝交易。

l) 交易结束：

- 1) 此为必备项。若交易未在前几个步骤因处理异常被终止，则终端应执行此功能用来结束交易；
- 2) 卡片和终端执行最后处理来完成交易。经发卡机构认可的交易可能根据卡片中的发卡机构认证结果和发卡机构写入的参数而被拒绝。卡片使用交易处理、发卡机构校验结果，以及发卡机构写入的规则来决定是否重设基于芯片卡片计数器和指示器。卡片生成 TC 来认可交易，生成 AAC 来拒绝交易；
- 3) 如果终端在授权消息之后传送清算信息，则 TC 应包括在该清算信息里。对于发卡机构批准而卡片拒绝的交易，终端应发起冲正；
- 4) 当卡片做出接受交易的结论 (卡片返回 TC) 后，卡片会记录交易日志。

- m) 发卡机构脚本处理。此为可选项。如果发卡机构在授权响应报文中包含了脚本，终端将这些脚本命令发送给卡片。在使用这些更新之前，卡片执行安全检查以确保脚本来自有效的发卡机构，且在传输中未有变动。这些命令对当前交易并不产生影响，主要会影响卡片的后续功能，如卡片应用解锁、卡片锁定、修改 PIN 等。

7.4.3 联机交易流程

应符合 JT/T 1059.3—2016 中 8.2 的要求。

7.4.4 应用管理交易流程

应符合 JT/T 1059.3—2016 中 8.3 的要求。

8 远程支付

8.1 应用模型

应符合JT/T 1059.4—2016中第4章的要求。

8.2 业务处理

8.2.1 用户注册

应符合JT/T 1059.4—2016中5.1的要求。

8.2.2 账户查询

应符合JT/T 1059.4—2016中5.2的要求。

8.2.3 消费

应符合JT/T 1059.4—2016中5.3的要求。

8.2.4 转账

应符合JT/T 1059.4—2016中5.4的要求。

8.2.5 空中圈存

应符合JT/T 1059.4—2016中5.5的要求。

8.2.6 冲正

应符合JT/T 1059.4—2016中5.6的要求。

8.2.7 异常处理

应符合JT/T 1059.4—2016中5.6的要求。

8.2.8 开卡

8.2.8.1 用户使用移动支付终端客户端，通过远程支付系统向广西交通一卡通 TSM 系统申请开通广西交通一卡通应用并加载个人化数据。开卡的交易模型步骤如下：

- a) 步骤 1：移动支付终端向 SEI-TSM 申请安装广西交通一卡通应用；
- b) 步骤 2：SEI-TSM 向移动支付终端下发安装广西交通一卡通应用；
- c) 步骤 3：移动支付终端向广西 SP-TSM 平台发送开卡请求；
- d) 步骤 4：广西 SP-TSM 下发返回个人化脚本；
- e) 步骤 5：移动支付终端执行脚本并将结果告知广西 SP-TSM 平台；
- f) 步骤 6：广西 SP-TSM 平台调用广西交通一卡通业务系统的接口进行售卡操作；
- g) 步骤 7：广西交通一卡通业务系统返回售卡结果；
- h) 步骤 8：广西 SP-TSM 平台返回开卡结果。

8.2.8.2 开卡的交易模型如图 9 所示。

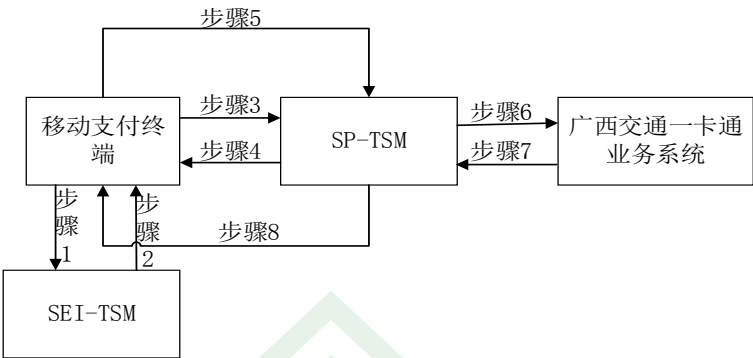


图9 开卡交易模型

8.2.9 迁出

8.2.9.1 用户使用客户端，通过广西交通一卡通 TSM 系统将移动支付终端内的广西交通一卡通应用中的个人化数据上传至广西 SP-TSM 平台。迁出的交易模型步骤如下：

- a) 步骤 1：移动支付终端向广西 SP-TSM 申请 0 元充值指令；
- b) 步骤 2：广西 SP-TSM 向移动支付终端下发 0 元充值指令；
- c) 步骤 3：移动支付终端执行 0 元充值指令；
- d) 步骤 4：移动支付终端将执行结果告知广西 SP-TSM；
- e) 步骤 5：广西 SP-TSM 记录卡片卡号、余额等信息；
- f) 步骤 6：广西 SP-TSM 向移动支付终端下发卡片删除指令。

8.2.9.2 迁出的交易模型如图 10 所示。

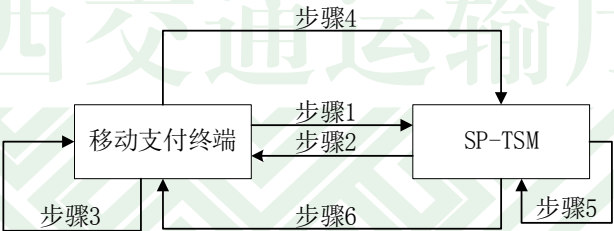


图10 迁出交易模型

8.2.10 迁入

8.2.10.1 用户使用客户端，通过广西交通一卡通 TSM 系统将广西 SP-TSM 平台内的广西交通一卡通应用个人化数据重新下载至移动支付终端内。

8.2.10.2 迁入流程包含了开卡和充值流程。充值时的金额，根据凭证号，查找上一次迁出时记录的余额信息。

8.2.10.3 迁入的交易模型步骤如下：

- a) 步骤 1：移动支付终端向 SEI-TSM 申请安装广西交通一卡通应用；
- b) 步骤 2：SEI-TSM 向移动支付终端下发安装广西交通一卡通应用；
- c) 步骤 3：移动支付终端向广西 SP-TSM 平台发送开卡请求；
- d) 步骤 4：广西 SP-TSM 下发返回个人化脚本；
- e) 步骤 5：移动支付终端执行脚本并将结果告知广西 SP-TSM 平台；
- f) 步骤 6：广西 SP-TSM 平台调用广西交通一卡通业务系统的接口进行售卡操作；

- g) 步骤 7: 广西交通一卡通业务系统返回售卡结果;
- h) 步骤 8: 广西 SP-TSM 平台返回开卡结果;
- i) 步骤 9: 移动支付终端向广西 SP-TSM 平台申请迁入充值指令;
- j) 步骤 10: 广西 SP-TSM 平台向移动支付终端下发余额充值指令;
- k) 步骤 11: 移动支付终端执行余额充值指令;
- l) 步骤 12: 移动支付终端将执行结果告知广西 SP-TSM 平台。

8.2.10.4 迁入的交易模型如图 11 所示。

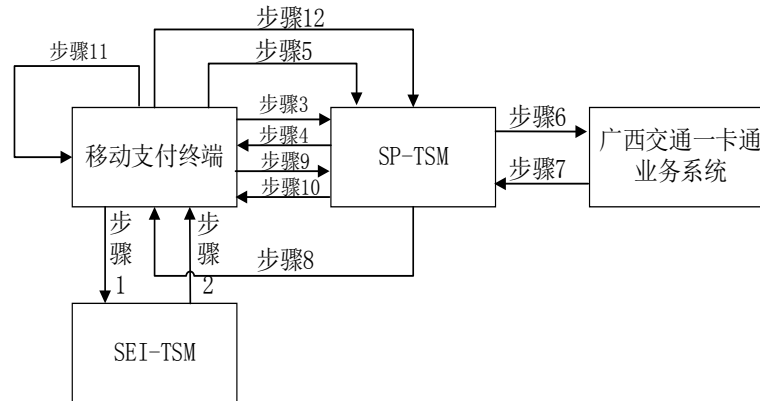


图11 迁入交易模型

8.2.11 坏卡退卡

8.2.11.1 用户使用客户端退卡时,通过访问广西交通一卡通 TSM 系统对广西交通一卡通应用进行退卡操作。坏卡退卡的交易模型交易步骤如下:

- a) 步骤 1: 移动支付终端通过读取终端设备号向广西 SP-TSM 平台申请坏卡退卡;
- b) 步骤 2: 广西 SP-TSM 平台向移动支付终端发送卡号及坏卡退卡结果。

8.2.11.2 坏卡退卡的交易模型如图 12 所示。

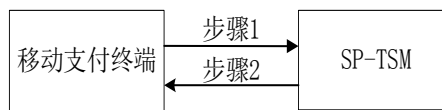


图12 坏卡退卡交易模型

8.2.12 查询退卡余额

8.2.12.1 坏卡退卡处理完毕 7 日后,需要查询退卡余额,进行退资处理。查询退卡余额的交易模型交易步骤如下:

- a) 步骤 1: 移动支付终端通过卡号向广西 SP-TSM 平台查询卡片余额;
- b) 步骤 2: 广西 SP-TSM 平台返回卡片余额。

8.2.12.2 查询退卡余额的交易模型如图 13 所示。

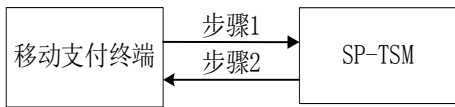


图13 查询退卡余额交易模型

8.2.13 查询状态

8.2.13.1 用户使用客户端查询终端设备内的广西交通一卡通应用的卡片状态。查询卡片状态交易模型步骤如下：

- a) 步骤 1：移动支付终端通过卡号向广西 SP-TSM 平台查询卡片状态；
- b) 步骤 2：广西 SP-TSM 平台返回卡片状态。

8.2.13.2 查询卡片状态交易模型如图 14 所示。

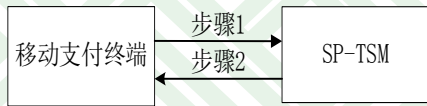


图14 查询卡状态交易模型

9 客户端软件

9.1 系统架构及功能

9.1.1 系统架构

9.1.1.1 一般要求

本章节仅对系统结构为SE内嵌的支付软件的客户端进行定义，对基于SE的客户端软件、无SE的客户端软件的客户端定义请参考JT/T 1059.5—2016 中5.1.2和5.1.3的规定。

9.1.1.2 SE 内嵌的支付软件

9.1.1.2.1 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)，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：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：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源。

9.1.1.2.2 基于 SE 的客户端软件与 TSM 平台等相关系统的模型如图 15 所示。

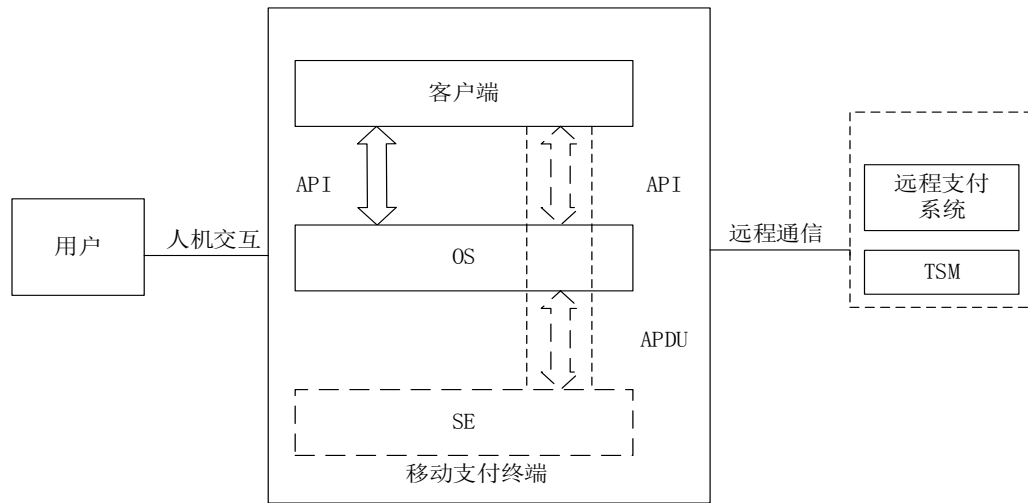


图15 客户端与相关系统模型架构

9.1.2 基本功能与流程

9.1.2.1 SE 初始化

请参考JT/T 1059.5—2016中5.2.2的规定。

9.1.2.2 应用查询

请参考JT/T 1059.5—2016中5.2.3的规定。

9.1.2.3 应用下载

请参考JT/T 1059.5—2016中5.2.4的规定。

9.1.2.4 应用删除

请参考JT/T 1059.5—2016中5.2.5的规定。

9.1.2.5 默认应用设置

请参考JT/T 1059.5—2016中5.2.6的规定。

9.1.2.6 空中圈存

9.1.2.6.1 功能定义

用户使用客户端，通过远程支付系统给交通应用充值。

9.1.2.6.2 界面要求

圈存前，宜向用户显示核心交易信息，如账户号、交易金额等，供用户确认。圈存完成后，应向用户显示圈存结果。

9.1.2.7 开卡

9.1.2.7.1 功能定义

用户使用客户端，通过远程支付系统开通广西交通一卡通应用。

9.1.2.7.2 界面要求

开卡前，应向用户显示核心信息，如开卡所属区域、开卡费用、圈存费用等，供用户确认。开卡完成后，应向用户显示开卡结果。

9.1.2.8 迁出

9.1.2.8.1 功能定义

用户使用客户端，通过远程支付系统将广西交通一卡通应用中的个人化数据上传至平台。

9.1.2.8.2 界面要求

迁出前，应向用户显示个人化数据信息及注意事项，如卡号、卡内余额等供用户确认。迁出完成后，应向用户显示迁出结果。

9.1.2.9 迁入

9.1.2.9.1 功能定义

用户使用客户端，通过远程支付系统将平台中的广西交通一卡通应用中的个人化数据下载至设备当中。

9.1.2.9.2 界面要求

迁入前，应向用户显示个人化数据信息及注意事项，如卡号、卡内余额等供用户确认。迁入完成后，应向用户显示迁入结果。

9.1.2.10 坏卡退卡

9.1.2.10.1 功能定义

用户使用客户端退卡时，通过远程支付系统对广西交通一卡通应用进行退卡操作。

9.1.2.10.2 界面要求

坏卡退卡前，应向用户显示个人化数据信息及注意事项，如卡号、卡内余额等供用户确认。退卡完成后，应向用户显示退卡结果。

9.1.2.11 查询退卡余额

9.1.2.11.1 功能定义

用户进行坏卡退卡后，使用客户端访问广西交通一卡通系统接口获取实际退卡的余额。

9.1.2.11.2 界面要求

客户进行查询退卡余额，应向用户显示个人化数据信息及注意事项，如卡号，余额等供用户确认。

9.1.2.12 查询状态

9.1.2.12.1 功能定义

用户使用客户端查询设备内的广西交通一卡通卡的状态。

9.1.2.12.2 界面要求

客户进行状态查询操作，应向用户显示个性化数据信息及注意事项，如卡号，余额，卡片状态，交易记录等供用户确认。

9.2 安全技术要求

9.2.1 人机交互安全

9.2.1.1 密码管理

9.2.1.1.1 登录密码管理

登录密码安全管理要求如下：

- a) 如需在移动支付终端本地保存，应采用密文方式；
- b) 用户输入登录密码时，应提供即时加密功能；
- c) 认证操作结束后应立即清除缓存，防止信息泄漏。

9.2.1.1.2 支付密码管理

支付密码安全管理要求如下：

- a) 不应保存在移动支付终端本地；
- b) 用户输入时，应提供即时加密功能，如密码键盘和动态口令等；
- c) 认证操作结束后，为防止信息泄漏，应立即清除缓存。

9.2.1.2 认证方式

对于大额支付和重要信息修改等关键业务，除密码认证以外，客户端还应采用其他安全认证方式，如动态口令和短信认证等。

9.2.1.3 登录失败处理

客户端对用户登录应采取限定连续登录失败的次数，如连续登录失败多次后，则账号锁定。

9.2.1.4 移动支付终端交易异常处理

当客户端检测到移动支付终端交易出现异常时，应向用户提示出错信息。

9.2.2 软件安全

9.2.2.1 数据有效性校验

客户端应提供数据有效性校验功能，保证数据格式或长度等信息通过人机接口或通信接口输入时符合系统设定的要求，如输入的资金金额和账户等信息应不含特殊字符。

9.2.2.2 页面回退清除敏感信息机制

客户端应支持页面回退清除敏感信息的机制。

9.2.2.3 反编译

客户端应采用反逆向工程保护措施，如采取代码混淆等技术手段，防范攻击者对客户端的反编译分析。

9.2.2.4 防篡改

客户端启动和更新时，应进行真实性和完整性校验，防范客户端被篡改。

9.2.3 数据安全

9.2.3.1 敏感数据录入

录入敏感数据时，客户端软件要求如下：

- a) 应采取安全显示方式，对于密码等敏感数据不应以明文显示；
- b) 应采取防截获安全措施，保证敏感数据不被移动支付终端连接的其他设备或程序非授权获取；
- c) 应采取防篡改机制，保证数据不被移动支付终端的其他设备或程序篡改。

9.2.3.2 数据访问

根据业务需要，敏感数据应仅供授权用户或授权应用组件访问。

9.2.3.3 数据存储

对数据存储的要求如下：

- a) 关键数据存储：客户端应保留最少的用户敏感数据(如登录密码、软件证书和账户信息等)，并限制数据存储量和保留时间；
- b) 用户信息存储安全：客户端不应保存用户支付信息(如支付密码等)及其密文；
- c) 敏感信息显示：客户端显示敏感信息时，应屏蔽部分内容(如身份证号等)；
- d) 残余信息保护：客户端在使用过身份认证和交易等敏感信息后，应及时清除敏感数据。

9.2.3.4 数据传输

对数据传输的要求如下：

- a) 远程数据传输保密性：支付密码等敏感数据通过公共网络传输时应采取加密措施，保证敏感数据传输的保密性；
- b) 本地数据传输保密性：支付密码等敏感数据在本地软件其他进程间传输时应采取加密措施，保证敏感数据传输的保密性；
- c) 数据传输完整性：交易数据在传输时，客户端应采取安全措施(如 MAC 等)以确保交易数据的完整性。

9.2.4 通信安全

9.2.4.1 网络通信协议

应符合JT/T 1059.5—2016中7.4.1的要求。

9.2.4.2 安全认证

客户端的网络协议层应对远程支付系统进行身份认证。

9.2.4.3 抗抵赖

通过客户端发送的报文的关键要素应进行数字签名，以确保支付内容的真实性和不可抵赖性。

9.3 卡片

9.3.1 卡面要求

客户端内的广西交通一卡通卡片正面应包括“交通联合”标识、卡号及桂民卡标识，卡号符合JT/T 978.2的应用主账号（PAN）。交通联合标识位于卡片正面右侧，可分为下置格式和上置格式两种设计方案，下置格式见图16、上置格式见图17、桂民卡标识见图18。

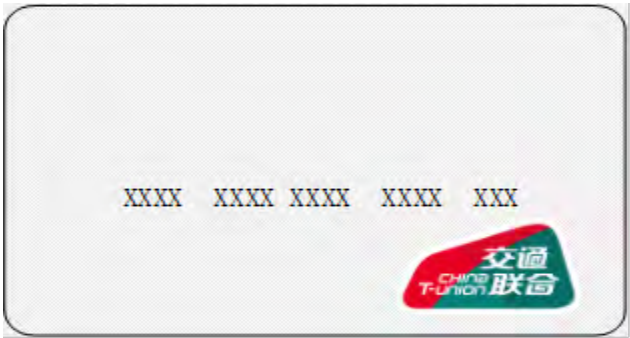


图16 交通联合标识下置格式



图17 交通联合标识上置格式



图18 桂民卡标识

9.3.2 卡号规则

卡号长度及结构应符合规定，卡号长度为19位，全部由0~9的阿拉伯数字组成，扩展后发卡机构识别码为8位，由全国交通一卡通互联互通平台统一分配，卡片末尾一位为校验位，校验位生成规则是前18位卡号求和取个位值。各发卡机构可个性化配置其余的卡号位编码规则。卡号组成规则见表2。

表2 卡号组成规则

3AAAAA	BB	CCCC CCCC CC	D
发卡机构识别码 (即 IIN 码)	发卡机构识别码的扩展码	发卡机构自定义 10 位	发卡机构自定义校验位
注：扩展后的发卡机构识别码共8位，如3AAA AABB，由全国交通一卡通互联互通平台统一分配			

9.3.3 卡片文件要求

- 9.3.3.1 规定卡片中的数据信息项的存储方式，规定不同用途的数据信息项和存储方式的选用要求。
- 9.3.3.2 互联互通的交易终端应将以下数据元作为判断是否为互联互通卡的依据，异地消费判断为不互通标识时应拒绝交易：
- a) 电子钱包 0x17 文件互通卡种数据元；
 - b) 电子现金标签 DF11 互通卡种数据元，若终端判断电子现金应用存在 0x08 文件，应判断 0x08 文件下的互通卡种标记。
- 9.3.3.3 按照技术规范发行的除普通卡外，电子钱包及电子现金应用定义的学生卡、老人卡、测试卡、军人卡等卡种类型作为互联互通卡种的预留，为未来全国统一特种卡的优惠政策后使用；对于目前各地可挂失的实名制卡片，以及学生卡、老人卡等特种卡，由于各地卡片使用管理要求的差异，故这类卡片仅在入网机构系统内使用，暂不参与互联互通。
- 9.3.3.4 发卡机构可采用本标准发行本地卡片。发卡机构发行本地卡，可使用技术规范定义的应用标识码（AID），互联互通标识（“交通联合” logo）不适用于本地卡卡面的标识印制。特种卡片的使用章程以各地发卡机构公布的为准。

9.3.4 交易时间

- 9.3.4.1 电子钱包脱机交易时间是指从终端寻获卡片并上电成功，到终端接收到卡片返回的最后一个字节为止的时间。电子钱包脱机消费交易时间应不超过 300 ms。
- 9.3.4.2 电子现金单次脱机交易时间是指从终端寻获卡片并上电成功，到终端接收到卡片返回的最后一个字节为止的时间，不包括终端脱机数据认证中验证静态或动态签名所需的时间。
- 9.3.4.3 电子现金单次脱机交易时间要求：采用 1024 位 RSA 算法时，标准快速支付交易时间应不超过 400 ms，更新一条过程记录的分时分段扣费交易时间应不超过 500 ms。

9.3.5 文件结构

卡片中应同时存在电子现金和电子钱包两个应用，两个应用拥有独立的文件结构，两个应用的文件结构应符合JT/T 978.3交易流程及JT/T 978.6安全体系，两个应用均可访问共用余额文件、公共交通过程信息变长记录文件（0x1A）和公共交通过程信息循环记录文件（0x1E），本规范未定义的应用不允许访问。电子现金应用和电子钱包应用共享以下数据信息：实际余额、透支限额、已透支金额、余额上限。卡片文件结构见图19。

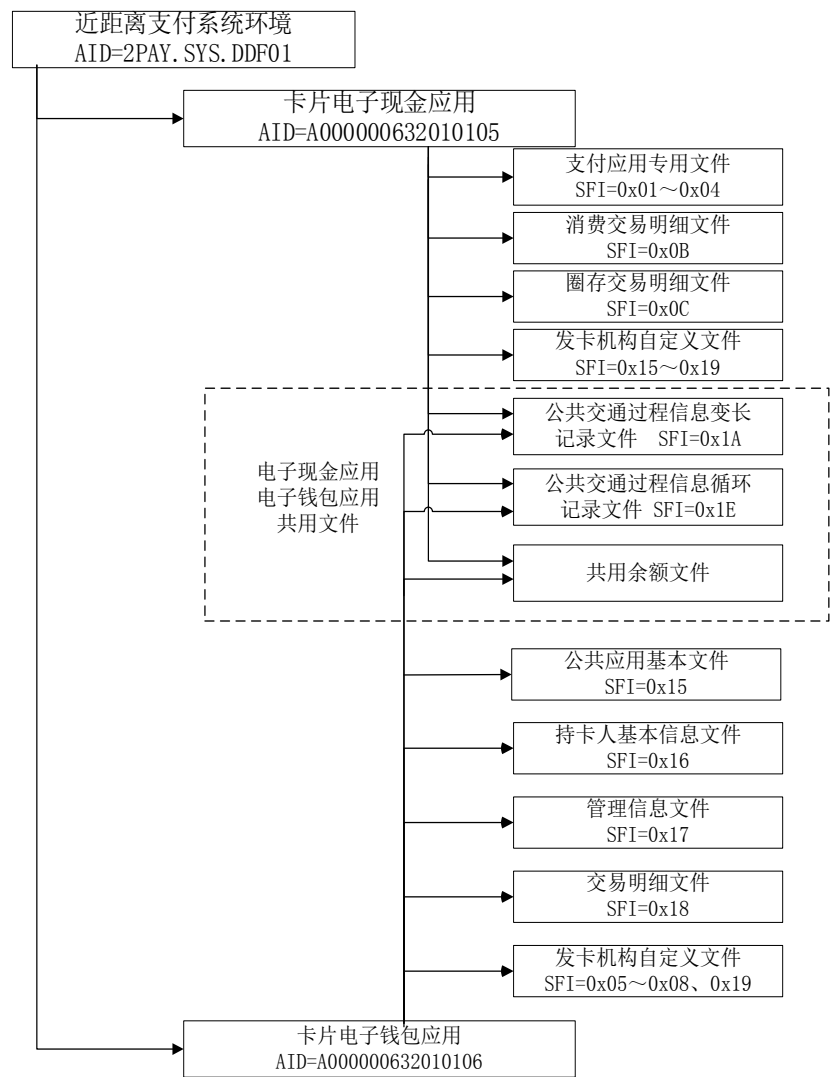


图19 广西交通一卡通移动支付互联互通卡片结构

10 可信服务管理系统

10.1 系统组成及基本要求

应符合JT/T 1059.6—2016中第5章要求。

10.2 安全要求

应符合JT/T 1059.6—2016中第6章要求。

10.3 业务流程管理要求

应符合JT/T 1059.6—2016中第7章要求。

10.4 平台间接口

应符合JT/T 1059.6—2016中第8章要求。

10.5 报文公共业务组件

应符合JT/T 1059.6—2016中第9章要求。

10.6 接口报文定义

应符合JT/T 1059.6—2016中第10章要求。

11 终端设备

11.1 总体分类

11.1.1 分类

按照广西交通一卡通移动支付终端设备的应用场景可将终端设备分为读写终端、移动终端、分体终端和SE应用管理终端，其中：

- a) 读写终端适用于公共汽电车、城市轨道交通和出租车等场景，并应满足 JT/T 978.3 的规定；
- b) 移动终端适用于个人用户受理城市公共交通 IC 卡或移动支付终端，并应满足 JT/T 1059.7—2016 中 5.1 的规定；
- c) 分体终端应用场景与移动终端类似，区别主要是出于安全考虑在物理形态和整体架构上对终端进行了分离，此类终端会将非接触通信部分、密码输入部分以及关键的逻辑加密等风险等级较高的部分分离出来并集中放置于分体终端一侧，而主控端、常规逻辑和与后台的通信模块则放置于手机或其他通用的移动设备端，两者通过蓝牙、WIFI 及有线等方式进行通信和信息交换，共同完成交易处理或 SE 管理功能；
- d) SE 应用管理终端适用于营业网点或布放的对 SE 状态及应用管理等进行操作和管理的终端类型，包括 POS 和自助终端两种。

11.1.2 通用要求

11.1.2.1 规定终端的非接触式电气特性和通信协议的要求、应用和基本业务流程要求、基本安全要求和对输入设备或模块的要求。

11.1.2.2 终端的非接触式电气特性和通信协议应符合 JT/T 978.5 的要求。

11.1.2.3 终端的应用和基本业务流程应符合 JT/T 978.3 的要求。

11.1.2.4 终端的基本安全应符合 JT/T 978.6 的要求。

11.1.2.5 若终端配备 PIN 输入设备或模块(如密码键盘)，则要求如下：

- a) PIN 输入设备应具备一定的物理和逻辑安全机制，如应具备入侵检测机制，防止 PIN 输入过程被监听，可安全地存储敏感信息，具备完整的密钥体系等；
- b) 在 PIN 输入设备和非接触式读卡器间传输 PIN 相关信息时，应有效地保护所传输的数据。

11.2 读写终端

应符合JT/T 1059.7—2016中第6章要求。

11.3 移动终端

应符合JT/T 1059.7—2016中第7章要求。

11.4 分体终端

应符合JT/T 1059.7—2016中第8章要求。

11.5 SE 应用管理终端

应符合JT/T 1059.7—2016中第9章要求。

12 检测项目

12.1 可信服务管理系统

应符合JT/T 1059.8—2016中第5章要求。

12.2 客户端

应符合JT/T 1059.8—2016中第6章要求。

12.3 终端设备

应符合JT/T 1059.8—2016中第7章要求。

12.4 安全单元

应符合JT/T 1059.8—2016中第8章要求。

12.5 GPAT 模板检测

12.5.1 ATS 模板案例

ATS模板案例如下表3。

表3 ATS 模板案例

序号	检测项	测试步骤	检测要求	检测结论
1	ATS 模板案例编号 2	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

12.5.2 PPSE 模板案例

PPSE模板案例如下表4。

表4 PPSE 模板案例

序号	检测项	测试步骤	检测要求	检测结论
1	PPSE 选择返回 FCI 模板案例编号 1924	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

12.5.3 AID 轮寻测试模板案例

AID轮寻测试模板案例如下表5。

表5 AID 轮寻测试模板案例

序号	检测项	测试步骤	检测要求	检测结论
1	AID 轮寻测试	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

12.5.4 余额查询模板案例

余额查询模板案例如下表6。

表6 余额查询模板案例

序号	检测项	测试步骤	检测要求	检测结论
1	个人化结束后电子现金应用和电子钱包应用余额相等案例 2302	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

12.5.5 检查 1A 和 1E 文件的初始值模板案例

检查1A和1E文件的初始值模板案例如下表7。

表7 检查 1A 和 1E 文件的初始值模板案例

序号	检测项	测试步骤	检测要求	检测结论
1	个人化结束后电子现金应用和电子钱包应用余额相等案例 591	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
2	1E 个人化增加 30 条记录检查 1E 文件的初始值案例编号 591	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
3	检查 1A 文件的初始值城市轨道交通应用信息记录 2701 案例编号 451	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
4	检查 1A 文件的初始值公共汽车应用信息记录 2702 案例编号 1998	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
5	检查 1A 文件的初始值城市水上客运应用信息记录 2703 案例编号 2079	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
6	检查 1A 文件的初始值出租汽车应用信息记录 2704 案例编号 2080	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

表 7 检查 1A 和 1E 文件的初始值模板案例（续）

序号	检测项	测试步骤	检测要求	检测结论
7	检查 1A 文件的初始值租赁汽车应用信息记录 2705 案例编号 2081	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
8	检查 1A 文件的初始值公共自行车应用信息记录 2706 案例编号 2082	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
9	检查 1A 文件的初始值停车收费应用信息记录 2707 案例编号 2083	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
10	检查 1A 文件的初始值长途客运应用信息记录 2708 案例编号 2084	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
11	检查 1A 文件的初始值轮渡应用信息记录 2709 案例编号 2085	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
12	检查 1A 文件的初始值高铁应用信息记录 270a 案例编号 2086	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
13	检查 1A 文件的初始值民航应用信息记录 270b 案例编号 2087	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
14	检查 1A 文件的初始值高速公路收费应用信息记录 270c 案例编号 2088	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
15	检查 1A 文件的初始值优惠信息记录 270d 案例编号 1999	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
16	检查 1A 文件的初始值城际慢速铁路应用信息记录 270e 案例编号 2078	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
17	检查 1A 文件的初始值本规范预留记录 270f 案例编号 2089	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
18	检查 1A 文件的初始值本规范预留记录 2710 案例编号 2090	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
19	检查 1A 文件的初始值本规范预留记录 2711 案例编号 2091	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

表7 检查 1A 和 1E 文件的初始值模板案例（续）

序号	检测项	测试步骤	检测要求	检测结论
20	检查 1A 文件的初始值本规范预留记录 2712 案例编号 2092	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
21	EP AID 选择返回 FCI 模板 案例编号 552	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
22	电子钱包 15 文件读取与字段判别 案例编号 1522	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
23	电子钱包 16 文件读取与字段判别 案例编号 1523	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
24	电子钱包 17 文件读取与字段判别 案例编号 1890	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
25	电子现金钱包应用的生效日期和失效日期分别同步 案例编号 5476	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

12.5.6 EP 扩展文件模板案例

EP 扩展文件模板案例如下表 8。

表8 EP 扩展文件模板案例

序号	检测项	测试步骤	检测要求	检测结论
1	EPCAPP0x1E 操作 案例编号 591	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
2	EPCAPP0x1A 记录 2701 操作 案例编号 451	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
3	EPCAPP0x1A 记录 2702 操作 案例编号 1998	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
4	EPCAPP0x1A 记录 2703 操作 案例编号 2079	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
5	EPCAPP0x1A 记录 2704 操作 案例编号 2080	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
6	EPCAPP0x1A 记录 2705 操作 案例编号 2081	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
7	EPCAPP0x1A 记录 2706 操作 案例编号 2082	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
8	EPCAPP0x1A 记录 2707 操作 案例编号 2083	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
9	EPCAPP0x1A 记录 2708 操作 案例编号 2084	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

表 8 EP 扩展文件模板案例（续）

序号	检测项	测试步骤	检测要求	检测结论
10	EPCAPP0x1A 记录 2709 操作 案例编号 2085	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
11	EPCAPP0x1A 记录 270a 操作 案例编号 2086	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
12	EPCAPP0x1A 记录 270b 操作 案例编号 2087	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
13	EPCAPP0x1A 记录 270c 操作 案例编号 2088	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
14	EPCAPP0x1A 记录 270d 操作 案例编号 1999	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
15	EPCAPP0x1A 记录 270e 操作 案例编号 2078	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
16	EPCAPP0x1A 记录 270f 操作 案例编号 2089	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
17	EPCAPP0x1A 记录 2710 操作 案例编号 2090	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
18	EPCAPP0x1A 记录 2711 操作 案例编号 2091	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
19	EPCAPP0x1A 记录 2712 操作 案例编号 2092	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
20	读取 COS 维护的 10 条交易记录案例编号 1524	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

12.5.7 EP 应用余额清 0 模板案例

EP应用余额清0模板案例如下表9。

表9 EP 应用余额清 0 模板案例

序号	检测项	测试步骤	检测要求	检测结论
1	EP 应用余额清 0	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过

12.5.8 EP 应用锁定密钥测试模板案例

EP应用锁定密钥测试模板案例如下表10。

表10 EP 应用锁定密钥测试模板案例

序号	检测项	测试步骤	检测要求	检测结论
1	EP 应用余额清 0	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过
2	使用 xml 文件中配置的 解锁密钥解锁 EP 应用案例 编号	使用交通运输部 GPAT 对应案例	应符合 JT/T 978.3 的要求	通过/不通过



中华人民共和国广西交通运输行业指南

交通一卡通移动支付技术指南

DBJT 45/T 019—2020

广西壮族自治区交通运输厅统一印刷

版权专有 侵权必究