|  |  |
| --- | --- |
| 文档类型 | 标准规范 |
| 文档编号 |  |
| 保密等级 | **机密** |

**洪城一卡通**

**清算中心标准接入规范**

**TSM平台接入分册**

**Version 1.0**

**上海捷羿软件系统有限公司**

**二○一四年十月**

文档控制页

|  |  |  |
| --- | --- | --- |
| **文 档 历 史 记 录** | | |
| 版本号定义规则：   * 版本号由清算中心维护。 * 使用阿拉伯数字，并由小数点分割成三部分。   第一部分（一位有效数字）：清算中心整体升级或改造时使用。  第二部分（一位有效数字）：本文档重大修改时使用。通常需要修改当前生产使用的应用程序。  第三部分（位数不限）：本文档简单修改时使用。通常是增加说明、更加详细的描述，不影响当前生产使用的应用程序。 | | |
| 日 期 | 姓 名 | 版 本 更 新 记 录 |
| 2014年10月09日 | 胡向 | 初始版本 |
| 2014年10月15日 | 胡向 | 3.2.2.5章节交易类型说明错误，修改为1114； |
| 2014年10月15日 | 胡向 | 接口中APDU的数据类型说明修改； |
| 2014年10月15日 | 胡向 | 增加通讯应答码编码章节； |
| 2014年11月11日 | 胡向 | 根据银联的要求去掉卡认证交易；  修改应用秘钥更新交易的接口说明；  修改卡文件通用写卡文件的接口说明； |
| 2014年11月25日 | 胡向 | 根据多次的沟通对接口及业务流程进行了梳理，本次主要在附录中增加了银联TSM个性化的业务流程说明； |
| 2014年11月27日 | 胡向 | 对6.2章节的通讯应答码编码进行修正，并去掉了部分tsm平台无关的通讯应答码； |
| 2014年12月01日 | 胡向 | 6.3章节增加圈存类业务处理的中心应答码说明； |
| 2014年12月01日 | 胡向 | 卡号申请交易和公交开卡完成交易增加证件类型99-其它的说明； |
| 2014年12月24日 | 胡向 | 卡号申请交易中增加卡押金字段； |
| 2015年12月23日 | 胡向 | 调整3.3章节的空中圈存类交易接口；  调整7.2.3章节中的空中圈存类交易（一卡通侧）业务流程； |
|  |  |  |

目 录

[第1章 概述 5](#_Toc438628932)

[1.1 适用范围 5](#_Toc438628933)

[1.2 术语定义 5](#_Toc438628934)

[1.3 数据类型说明 5](#_Toc438628935)

[1.4 参考文档 6](#_Toc438628936)

[第2章 统一格式说明 6](#_Toc438628937)

[2.1 联机报文格式 6](#_Toc438628938)

[第3章 联机业务接口 6](#_Toc438628939)

[3.1 管理类交易接口 6](#_Toc438628940)

[3.1.1 功能及流程 6](#_Toc438628941)

[3.1.2 交易接口说明 7](#_Toc438628942)

[3.2 空中个人化类交易接口 10](#_Toc438628943)

[3.2.1 功能及流程 10](#_Toc438628944)

[3.2.2 交易接口说明 10](#_Toc438628945)

[3.3 空中圈存类交易接口 23](#_Toc438628946)

[3.3.1 功能及流程说明 23](#_Toc438628947)

[3.3.2 交易接口说明 23](#_Toc438628948)

[第4章 数据安全 34](#_Toc438628949)

[第5章 FTP交易对账接口 34](#_Toc438628950)

[5.1 对账原则 34](#_Toc438628951)

[5.2 Username 和Password 34](#_Toc438628952)

[5.3 对账文件的生成时间 34](#_Toc438628953)

[5.4 下载文件目录 34](#_Toc438628954)

[5.5 文件命名规则 34](#_Toc438628955)

[5.6 对账文件内容格式 35](#_Toc438628956)

[5.6.1 终端联机充值类对账明细文件（SD） 35](#_Toc438628957)

[第6章 编码规则 35](#_Toc438628958)

[6.1 交易类型定义 35](#_Toc438628959)

[6.2 通讯应答码编码 36](#_Toc438628960)

[6.3 交易处理结果编码 36](#_Toc438628961)

[6.4 异常流程处理说明 37](#_Toc438628962)

[第7章 附录 38](#_Toc438628963)

[7.1 附录一 PBOC-3DES-MAC算法说明 38](#_Toc438628964)

[7.2 附录二 TSM平台交互业务流程说明 39](#_Toc438628965)

[7.2.1 签到类交易业务流程 39](#_Toc438628966)

[7.2.2 空中发卡类交易业务流程 40](#_Toc438628967)

[7.2.3 空中圈存类交易（一卡通侧）业务流程 41](#_Toc438628968)

* 1. 概述

## 适用范围

本规范适用于所有与洪城一卡通清算中心系统相连的TSM平台，主要实现空中发卡和空中圈存业务。

## 术语定义

* **洪城一卡通清算中心系统：**负责“洪城一卡通”的发行，业务逻辑的处理；
* **TSM平台：**主要实现cap包及手机app的管理；

## 数据类型说明

为了方便维护和管理，所有都采用自定义的ASCII码报文结构。

默认情况下，数据类型描述遵守以下规定：

|  |  |
| --- | --- |
| **标示代码** | **说明** |
| A | 大写字母，左靠，右补空格 |
| a | 小写字母，左靠，右补空格 |
| N | 数值0-9；右靠，左补零；负号（－）使用“0X2D”，靠左，如：－00001表示“负一” |
| S | 特殊符号，需要专门说明 |
| AN | 字母和/或数字，左靠，右部多余部分填空格 |
| ANS | 字母、数字和/或特殊符号，左靠，右部多余部分填空格 |
| AS | 字母和/或特殊符号，左靠，右部多余部分填空格 |
| H | 十六进制数0-F； A-F为大写字母 |
| YY | 年 |
| MM | 月 |
| DD | 日 |
| hh | 时 |
| mm | 分 |
| ss | 秒 |
| VAR | 可变长说明，需要专门说明 |
|  | **未定义或未使用的域默认全部填写为：0** |

## 参考文档

* 1. 统一格式说明

## 联机报文格式

任何一次交互的消息报文均由消息包头、消息包体两部分组成。其中，消息包头又可划分为包长度、同步信息、压缩标志、加密算法、版本号、消息类型六个组成部分。消息报文结构如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段** | | **描述** | **类型** | **长度** |
| 消息包头 | 包长度 | 本消息报文的长度（不包括本字段本身长度） | N | 4 |
| 同步信息 | 清算终端号（由一卡通统一分配） | N | 12 |
| 压缩标志 | 报文内容压缩标志（默认填写0） | N | 1 |
| 加密算法 | 加密算法标志（默认填写0） | N | 1 |
| Version | 版本号（默认填写01） | N | 2 |
| Message type | 消息类型（默认填写5000） | AN | 4 |
| 消息包体 | | 报文内容 | AN | 变长 |

说明：

同步信息：12位终端号，该终端号由清算中心分配；

压缩标志： 0–不压缩、1–LZ77算法。当前填0，不支持压缩；

加密算法： 0–明文传输、1–RSA加密、2–DES加密。目前只需采用明文传输；

版本号：为描述方便，此字段在通讯数据接口每种消息包文中重复描述，在通讯交互中只作一次使用，目前统一为01；

消息类型：为描述方便，此字段在通讯数据接口每种消息包文中重复描述，在通讯交互中只作一次使用；

消息包体：由消息类型决定；

* 1. 联机业务接口

## 管理类交易接口

### 功能及流程

管理类交易主要包括主密钥下载交易和签到交易，用来保证通讯过程中报文的完整性和不可篡改性。

### 交易接口说明

#### 主密钥下载交易

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主密钥下载交易 | | | | |
| 数据元 | 数据类型 | 说明 | 请求和应答数据值 | |
| 客-服 | 服-客 |
| **Message header** |  |  |  |  |
| Version | N2 | 交易版本号 | M | M |
| Message type | N4 | 交易类型 | M | M |
| Message date time | YYYYMMDDhhmmss | 报文发送时间 | M | M |
| MAC | H8 | 通讯押码 | 全0 | 全0 |
| Response code | H2 | 通讯应答码 | 全0 | M |
| **Transaction header** |  |  |  |  |
| unitid | N8 | 营运单位代码 | M | M |
| ISAMID | N16 | ISAM卡号 | 全0 | M |
| Pos id | N12 | 设备号 | M | M |
| Termid | N12 | 终端编号 | M | M |
| KeySet | ANS32 | 终端主密钥 | 全0 | M |
| Reserved | ANS20 | 保留域 | 全0 | 全0 |
| Response Code | N5 | 交易应答码 | 全0 | M |

**业务说明：**

* 终端编号发生变化后，必须重新发送该报文，成功后，才可以进行业务。该报文在整个终端的有效使用周期中只需发送一次。在银联TSM对接过程中，该交易可省略。
* Version：版本号，默认填写10；
* Message type：交易类型，2055；

**域说明：**

* Unitid：营运单位代码，由一卡通统一提供给各接入TSM平台；
* ISAMID：ISAM卡号，此处默认填写全0；
* Pos id：设备号，由一卡通统一提供给各接入TSM平台；
* Termid：终端编号，此处与PosId保持一致（或者可以填写自有终端编号）；
* KeySet：终端主密钥，受初始密钥加密保护，3des算法，初始因子联调时由一卡通提供。初始密钥由总中心在设备初始化时，设置到终端中；
* Reserved：保留域，暂不使用，默认填写全0；
* Response Code：交易应答码，请求时默认全0，应答时由清算中心返回，TSM平台需要根据该应答码判断是否继续后续的业务处理；

#### 签到交易

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 签到交易 | | | | |
| 数据元 | 数据类型 | 说明 | 请求和应答数据值 | |
| 客-服 | 服-客 |
| **Message header** |  |  |  |  |
| Version | N2 | 交易版本号 | M | M |
| Message Type | N4 | 交易类型 | M | M |
| Message Date Time | YYYYMMDDhhmmss | 报文发送时间 | M | M |
| MAC | H8 | 通讯押码 | M | 全0 |
| Response code | H2 | 通讯应答码 | 全0 | M |
| **Transaction header** |  |  |  |  |
| Unitid | N8 | 营运单位代码 | M | M |
| TxnMode | N2 | 交易方式 | M | M |
| SAMID | N16 | SAM卡号 | 全0 | M |
| SAMAuthInfo | N16 | SAM卡授权信息 | 全0 | M |
| EDAuthInfo | N16 | ED卡授权信息 | 全0 | M |
| Posid | N12 | 清算设备代码 | M | M |
| Termid | N12 | 企业设备代码 | M | M |
| Operid | N16 | 操作员号 | M | M |
| EDCardId | N16 | 操作主卡卡号 | 全0 | M |
| SettDate | YYYYMMDD | 结算日期 | 全0 | M |
| BatchNo | N6 | 批次号 | 全0 | M |
| SysDatetime | YYYYMMDDhhmmss | 中心时间，可用于设备校正时间 | 全0 | M |
| Authcode | H24 | 授权认证码（M1） | 全0 | C |
| ParamBit | N32 | 参数更新标志位 | C | M |
| KeySet | ANS32 | 密钥(MAC密钥)(联机) | C | M |
| Reserved | ANS20 | 保留域 | C | C |
| Response Code | N5 | 交易应答码 | M | M |

**业务说明：**

* 要求系统每天定时进行一次签到，因为签到下发的工作密钥是以日期来进行分散的，另外接入机构需要保存中心下发的批次号和结算日期。
* Version：版本号，默认填写10；
* Message type：交易类型，2051；

**域说明：**

* Unitid：营运单位代码，由一卡通统一提供给各接入TSM平台；
* Txn Mode：交易方式，01表示联机，00表示脱机，默认使用01联机方式；
* Pos id：设备号，由一卡通统一提供给各接入TSM平台；
* Termid：终端编号，此处与PosId保持一致（或者可以填写自有终端编号）；
* Operid：操作员号，由一卡通统一提供给各接入TSM平台；
* SettDate：结算日期，请求时默认填写全0，应答时由一卡通中心返回；
* BatchNo：批次号，请求时默认填写全0，应答时由一卡通中心返回；
* SysDatetime：中心时间，一卡通系统时间，请求时默认填写全0，应答时由一卡通中心返回；
* ParamBit：32字节的0或1，0代表该参数不需要下载，1代表该参数需要下载。每一位表示一类参数，第1位：黑名单参数；第2位：通讯参数。在联机系统中暂时不需要下载参数（TSM平台签到可以不用管该标记）。
* KeySet：请求时默认填写全0，应答时由清算中心返回的mackey，受主密钥保护；
* Reserved：保留域，暂不使用，默认填写全0；
* Response Code：交易应答码，请求时默认全0，应答时由清算中心返回，TSM平台需要根据该应答码判断是否继续后续的业务处理；

## 空中个人化类交易接口

### 功能及流程

整个的空中个人化（空中发卡）是一个完整的流程，涉及多个接口，需要顺序执行。在接口中，涉及以下一组接口：

1. 公交卡号申请（卡号申请交易）
2. 公交应用密钥更新接口（应用密钥更新交易）
3. 公交15文件写卡接口，即售卡操作（卡状态启用，启用日期）
4. 公交开卡完成交易接口

### 交易接口说明

#### 卡号申请交易

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 卡号申请交易 | | | | |
| 数据元 | 数据类型 | 说明 | 请求和应答数据值 | |
| 客-服 | 服-客 |
| **Message header** |  |  |  |  |
| Version | N2 | 交易版本号 | M | M |
| Message type | N4 | 交易类型 | M | M |
| Message date time | YYYYMMDDhhmmss | 报文发送时间 | M | M |
| MAC | H8 | 通讯押码 | M | M |
| Response code | N2 | 通讯应答码 | 全0 | M |
| **Transaction header** |  |  |  |  |
| unitid | N8 | 营运单位代码（一卡通分配） | M | M |
| Pos id | N12 | 设备号（一卡通分配） | M | M |
| Pos sequence | N9 | 设备流水号 | M | M |
| Operid | N16 | 操作员号 | M | M |
| CItyCode | N4 | 城市代码 | M | M |
| CardId | N16 | 卡内号 | 全0 | M |
| CardMType | N2 | 主卡类型 | 全0 | M |
| CardSType | N2 | 子卡类型 | 全0 | M |
| CardModel | N1 | 卡型，3-M1卡 1-CPU卡（默认1） | M | M |
| DepositAmt | N8 | 卡押金 | 全0 | M |
| Seid | H40 | 手机卡物理序号 | M | M |
| Ats | H60 | 通过芯片上电复位指令获取，16进制 | M | M |
| Mobile | ANS20 | 手机号码 | M | M |
| regtype | ANS2 | 证件类型 | M | M |
| regNbr | ANS40 | 证件号 | M | M |
| custName | ANS60 | 客户姓名 | M | M |
| custAddlen | N3 | 客户附属信息长度(无则填写000) | M | M |
| custAddData | ANS…999 | 客户附属信息 | C | C |
| SettleDate | N8 | 中心结算日期：ic卡系统返回 | 全0 | M |
| WorkFlowSSN | N20 | TSM平台流水号，请求报文(8位TSM平台代码+12位扣款方唯一流水号) | M | M |
| Apdulen | N3 | Apdu长度 | M | M |
| Apdu | H999 | 请求报文中为指令头，中心需要自行组织完整的apdu，并计算mac。应答报文为完整的apdu指令。 | C  Apdulen〉0时存在 | C  成功交易必须存在 |
| Reserved | ANS20 | 保留域 | 全0 | 全0 |
| Response Code | N5 | 交易应答码 | 全0 | M |

**业务说明：**

* 卡号申请交易是一卡通清算中心系统根据TSM平台的请求中的Seid从中心获取到对应的卡号之后返回给对应TSM平台，同一Seid只能获取一个卡号。如果Seid已经申请过，则获取原卡号进行返回，否则分配一个新的一卡通卡号进行返回。
* Version：版本号，默认填写10；
* Message type：交易类型，1110；

**域说明：**

* Unitid：营运单位代码，由一卡通统一提供给各接入TSM平台；
* Pos id：设备号，由一卡通统一提供给各接入TSM平台；
* Pos sequence：设备流水号，由TSM平台生成的唯一序列号，生成规则由TSM平台确定，需要保证一段时间内唯一；
* Operid：操作员号，由一卡通统一提供给各接入TSM平台；
* CItyCode：城市代码，对于南昌一卡通，请求时可以默认填写3300，应答时由一卡通给出；
* CardId：卡内号，请求时默认填写全0，应答时由一卡通中心给出；
* CardMType：主卡类型，请求时默认填写全0，应答时由一卡通中心给出；
* CardSType：子卡类型，请求时默认填写全0，应答时由一卡通中心给出；
* CardModel：卡型，3-M1卡 1-CPU卡，请求时默认填写1，应答时由一卡通中心给出；
* DepositAmt：卡押金，卡号申请请求时填写全0，应答时由一卡通返回，单位为分；
* Seid：手机卡物理序号，由手机端获取并在请求时给出，该字段为必须字段；
* Ats：通过芯片上电复位指令获取，16进制，，由手机端获取并在请求时给出，该字段为必须字段。如26E2D9D6FE80A020；
* Mobile：用户手机号码，由手机端获取并在请求时给出；
* Regtype：证件类型，由手机端获取并在请求时给出。00 -居民身份证、01-中小学生证、02-护照、03-军官证、04-士兵证、05-武装警察身份证、06-港澳台通行证、07-台胞证、08-驾驶证、09-暂住证、99-其它；
* regNbr：证件号，根据证件类型来定，由手机端获取并在请求时给出；
* custName：客户姓名，由手机端获取并在请求时给出；
* custAddlen：客户信息附属长度，无则填写全0；
* custAddData：客户附属信息，根据客服信息附属长度而定；
* SettDate：结算日期，请求时默认填写全0（如允许请填写签到时一卡通返回的结算日期），应答时由一卡通中心返回；
* WorkFlowSSN：平台流水号，8位TSM平台代码+12位扣款方唯一流水号；
* Apdulen：Apdu长度，请求时填写对应apdu数据的长度；
* Apdu：请求报文中为指令头，中心需要自行组织完整的apdu，并计算mac。应答报文为完整的apdu指令；卡号申请交易该值默认为空；
* Reserved：保留域，暂不使用，默认填写全0；
* Response Code：交易应答码，请求时默认全0，应答时由清算中心返回，TSM平台需要根据该应答码判断是否继续后续的业务处理；

#### 应用密钥更新交易

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 应用密钥更新交易 | | | | |
| 数据元 | 数据类型 | 说明 | 请求和应答数据值 | |
| 客-服 | 服-客 |
| **Message header** |  |  |  |  |
| Version | N2 | 交易版本号 | M | M |
| Message type | N4 | 交易类型 | M | M |
| Message date time | YYYYMMDDhhmmss | 报文发送时间 | M | M |
| MAC | H8 | 通讯押码 | M | M |
| Response code | N2 | 通讯应答码 | 全0 | M |
| **Transaction header** |  |  |  |  |
| unitid | N8 | 营运单位代码（一卡通分配） | M | M |
| Pos id | N12 | 设备号（一卡通分配） | M | M |
| Pos sequence | N9 | 设备流水号 | M | M |
| CItyCode | N4 | 城市代码 | M | M |
| CardId | N16 | 卡内号 | M | M |
| CardMType | N2 | 主卡类型 | M | M |
| CardSType | N2 | 子卡类型 | M | M |
| CardModel | N1 | 卡型，3-M1卡 1-CPU卡（默认1） | M | M |
| Seid | H40 | 手机卡物理序号 | M | M |
| Ats | H60 | 通过芯片上电复位指令获取，16进制 | M | M |
| SettleDate | N8 | 中心结算日期：ic卡系统返回 | 全0 | M |
| WorkFlowSSN | N20 | TSM平台流水号，请求报文(8位TSM平台代码+12位扣款方唯一流水号) | M | M |
| keyTag | N2 | 密钥标识  0x00 应用主控子密钥  0x01 应用维护子密钥（4组）  0x02 应用PIN 解锁密钥  0x03 应用PIN 重装密钥  0x04 应用消费子密钥  0x05 应用圈存子密钥  0x06 TAC密钥  0x07 写卡密钥(保留)  0x08 应用PIN密钥（3组）  0x09 卡片PIN 解锁密钥  0x0A 卡片PIN 重装密钥  0x0B 复合消费维护密钥  0x0C 卡片主控子密钥（GP方式的由一卡通返回完整的Store Data指令（更新3F00的主控密钥））  0x0D 卡片维护子密钥  0x0E 卡片内部认证子密钥  0x0F 卡片PIN密钥  0x99 IK（SJL06 保护密钥保留）  0xFF（默认一次性下发所有秘钥）  十六进制 例:06/0B | M | M |
| keyIndex | N2 | 密钥分组  01 第一组密钥  02 第二组密钥  03 第三组秘钥  04 第四组秘钥  同keyTag组合使用  十六进制例:01、02 | M | M |
| CardRand | H8 | 卡片随机数  必须字段，参与发卡运算。这个是卡片给出的。  十六进制 | M | 0 |
| Apdulen | N3 | Apdu长度 | M | M |
| Apdu | H999 | 请求报文中为指令头，中心需要自行组织完整的apdu，并计算mac。应答报文为完整的apdu指令。  如果秘钥标志（keyTag）为0xFF表示一次性下发所有秘钥，本部分采用TLV规则（即tag：密钥标识+秘钥分组（单组即默认01，多组为对应组数）；Len：数据长度；value：秘钥内容），中心只负责组装返回对应的秘钥内容，不负责完整的apdu指令的下发；  Tag（4位）+Len（2位）+Value（Len长度） | M | M |
| keyHeadlen | H4 | 密钥头长度>=0，16进制 | M | M |
| Keyhead |  |  |  |  |
| keytaillen | H4 | 密钥尾长度>=0，16进制 | M | M |
| keytail |  |  |  |  |
| Reserved | ANS20 | 保留域 | 全0 | 全0 |
| Response Code | N5 | 交易应答码 | 全0 | M |

**业务说明：**

* 对卡片密钥进行更新，一卡通中心系统在收到应用密钥更新请求交易所时，会产生相应的卡密钥，并将其返回给第三方，有卡片主控密钥、维护子密钥、充值子密钥、消费子密钥等；
* Version：版本号，默认填写10；
* Message type：交易类型，1112；

**域说明：**

* Unitid：营运单位代码，由一卡通统一提供给各接入TSM平台；
* Pos id：设备号，由一卡通统一提供给各接入TSM平台；
* Pos sequence：设备流水号，由TSM平台生成的唯一序列号；
* CItyCode：城市代码，请求时填写卡号申请交易时一卡通中心返回的城市代码；
* CardId：卡内号，请求时填写卡号申请交易时一卡通中心返回的城市代码卡内号；
* CardMType：主卡类型，请求时填写卡号申请交易时一卡通中心返回的主卡类型；
* CardSType：子卡类型，请求时填写卡号申请交易时一卡通中心返回的子卡类型；
* CardModel：卡型，3-M1卡 1-CPU卡，请求时填写卡号申请交易时一卡通中心返回的卡型；
* Seid：手机卡物理序号，由手机端获取并在请求时给出，该字段为必须字段；
* Ats：通过芯片上电复位指令获取，16进制，，由手机端获取并在请求时给出，该字段为必须字段。如26E2D9D6FE80A020；
* SettDate：结算日期，请求时默认填写全0（如允许请填写签到时一卡通返回的结算日期），应答时由一卡通中心返回；
* WorkFlowSSN：平台流水号，8位TSM平台代码+12位扣款方唯一流水号；
* keyTag：应用标志；
* keyIndex：密钥分组标志；
* CardRand：卡片随机数，必须字段，参与发卡运算。这个是卡片给出的，十六进制；
* Apdulen：Apdu长度，请求时填写对应apdu数据的长度；
* Apdu：请求报文中为指令头，中心需要自行组织完整的apdu，并计算mac。应答报文为完整的apdu指令；对于银联tsm请求时该字段为空，应答时由一卡通中心以TLV格式返回对应秘钥数据。
* keyHeadlen：密钥头长度，十六进制，无密钥头则填写0；
* Keyhead：密钥头，如果密钥头长度大于0 则存在该域；
* Keytaillen：密钥尾长度，（针对特殊COS，默认为0）十六进制；
* Keytail：密钥尾，如果密钥尾长度大于0 则存在该域；
* Reserved：保留域，暂不使用，默认填写全0；
* Response Code：交易应答码，请求时默认全0，应答时由清算中心返回，TSM平台需要根据该应答码判断是否继续后续的业务处理；

#### 卡文件通用写卡交易

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 卡文件通用写卡交易 | | | | |
| 数据元 | 数据类型 | 说明 | 请求和应答数据值 | |
| 客-服 | 服-客 |
| **Message header** |  |  |  |  |
| Version | N2 | 交易版本号 | M | M |
| Message type | N4 | 交易类型 | M | M |
| Message date time | YYYYMMDDhhmmss | 报文发送时间 | M | M |
| MAC | H8 | 通讯押码 | M | M |
| Response code | N2 | 通讯应答码 | 全0 | M |
| **Transaction header** |  |  |  |  |
| unitid | N8 | 营运单位代码（一卡通分配） | M | M |
| Pos id | N12 | 设备号（一卡通分配） | M | M |
| Pos sequence | N9 | 设备流水号 | M | M |
| CItyCode | N4 | 城市代码 | M | M |
| CardId | N16 | 卡内号 | M | M |
| CardMType | N2 | 主卡类型 | M | M |
| CardSType | N2 | 子卡类型 | M | M |
| CardModel | N1 | 卡型，3-M1卡 1-CPU卡（默认1） | M | M |
| Seid | H40 | 手机卡物理序号 | M | M |
| Ats | H60 | 通过芯片上电复位指令获取，16进制 | M | M |
| SettleDate | N8 | 中心结算日期：ic卡系统返回 | 全0 | M |
| WorkFlowSSN | N20 | TSM平台流水号，请求报文(8位TSM平台代码+12位扣款方唯一流水号) | M | M |
| Fileid | H4 | 文件标识：  0005文件  0015文件  0016文件  00FF所有文件 | M | M |
| KeyVer | H2 | 卡片密钥版本 | M | 0 |
| AlgInd | H2 | 卡片算法标识 | M | 0 |
| KeyIndex | H2 | 密钥分组号 | M | M |
| CardRand | H8 | 卡片随机数 | M | M |
| Opertype | N2 | 0文件初始化  1启动卡片启用标  2关闭卡片启用标识  3 延长有效期 | M | M |
| Validate | N8 | 有效期 | 0 | M |
| Apdulen | N3 | Apdu长度 | M | M |
| Apdu | H999 | 请求报文中为指令头，中心需要自行组织完整的apdu，并计算mac。应答报文为完整的apdu指令。  如果文件标志（Fileid）为FFFF表示一次性下发所有需要写入的文件内容，本部分采用TLV规则（即tag：文件标志；Len：数据长度；value：文件内容），中心只负责组装返回对应的文件内容，不负责完整的apdu指令的下发；Tag（4位）+Len（2位）+Value（Len长度） | M | M |
| Reserved | ANS20 | 保留域 | 全0 | 全0 |
| Response Code | N5 | 交易应答码 | 全0 | M |

**业务说明：**

* 对卡片文件进行对应的写操作，包括0x05、0x15、0x16文件及其它文件的更新；对于银联tsm的接入，该部分仅针对0x15文件进行更新，即通常所说的售卡交易；
* 该接口可以用于修改各类文件的内容，但apdu指令中的data必须正确上送，中心只计算指令mac；
* 中心根据Fileid 和Opertype 组装apdu的data，并计算指令mac。
* 卡端只需要上送apdu头和正确的卡信息；
* Version：版本号，默认填写10；
* Message type：交易类型，1113；

**域说明：**

* Unitid：营运单位代码，由一卡通统一提供给各接入TSM平台；
* Pos id：设备号，由一卡通统一提供给各接入TSM平台；
* Pos sequence：设备流水号，由TSM平台生成的唯一序列号；
* CItyCode：城市代码，卡内读取；
* CardId：卡内号，卡内读取；
* CardMType：主卡类型，卡内读取；
* CardSType：子卡类型，卡内读取；
* CardModel：卡型，3-M1卡 1-CPU卡，卡内读取；
* Seid：手机卡物理序号，由手机端获取并在请求时给出，该字段为必须字段；
* Ats：通过芯片上电复位指令获取，16进制，，由手机端获取并在请求时给出，该字段为必须字段。如26E2D9D6FE80A020；
* SettDate：结算日期，请求时默认填写全0（如允许请填写签到时一卡通返回的结算日期），应答时由一卡通中心返回；
* WorkFlowSSN：平台流水号，8位TSM平台代码+12位扣款方唯一流水号；
* Fileid：文件标志， 0x05、0x15、0x16、0x9999(0x9999代表擦除卡片的请求)、0xA0 (更新主控密钥前的INSTALL（for personalization)、0xFFFF表示下发所有文件信息；
* KeyVer：卡片密钥版本，请求时默认填写01；
* AlgInd：卡片算法标志，请求时默认填写00；
* KeyIndex：密钥分组号，请求时默认填写01；
* CardRand：卡片随机数，必须字段，参与发卡运算。这个是卡片给出的，十六进制；
* Opertype：操作类型，该域仅对0x15文件有效，15文件的写文件操作会执行两次，第一次写文件，第二次写文件中的一个标志位。因此增加一个字段，区分执行不同的工作；
* Validate：有效期，延期填写新有效期，其他同请求报文；
* Apdulen：Apdu长度；请求时填写对应apdu数据的长度；
* Apdu：请求报文中为指令头，中心需要自行组织完整的apdu，并计算mac。应答报文为完整的apdu指令；
* Reserved：保留域，暂不使用；
* Response Code：交易应答码，请求时默认全0，应答时由清算中心返回，TSM平台需要根据该应答码判断是否继续后续的业务处理；

#### 公交开卡完成交易

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 公交开卡完成交易 | | | | |
| 数据元 | 数据类型 | 说明 | 请求和应答数据值 | |
| 客-服 | 服-客 |
| **Message header** |  |  |  |  |
| Version | N2 | 交易版本号 | M | M |
| Message type | N4 | 交易类型 | M | M |
| Message date time | YYYYMMDDhhmmss | 报文发送时间 | M | M |
| MAC | H8 | 通讯押码 | M | M |
| Response code | N2 | 通讯应答码 | 全0 | M |
| **Transaction header** |  |  |  |  |
| unitid | N8 | 营运单位代码（一卡通分配） | M | M |
| Pos id | N12 | 设备号（一卡通分配） | M | M |
| Pos sequence | N9 | 设备流水号 | M | M |
| CItyCode | N4 | 城市代码 | M | M |
| CardId | N16 | 卡内号 | M | M |
| CardMType | N2 | 主卡类型 | M | M |
| CardSType | N2 | 子卡类型 | M | M |
| CardModel | N1 | 卡型，3-M1卡 1-CPU卡（默认1） | M | M |
| Seid | H40 | 手机卡物理序号 | M | M |
| SettleDate | N8 | 中心结算日期：ic卡系统返回 | 全0 | M |
| WorkFlowSSN | N20 | TSM平台流水号，请求报文(8位TSM平台代码+12位扣款方唯一流水号) | M | M |
| Mobile | ANS20 | 手机号码 | M | M |
| regtype | ANS2 | 证件类型 | M | M |
| regNbr | ANS40 | 证件号 | M | M |
| custName | ANS60 | 客户姓名 | M | M |
| operation | N1 | 0：开户成功  1：其他开户失败 | M | M |
| Reserved | ANS20 | 保留域 | 全0 | 全0 |
| Response Code | N5 | 交易应答码 | 全0 | M |

**业务说明：**

* 对卡片文件进行对应的写操作，包括0x05、0x15、0x16文件及其它文件的更新；
* 该接口可以用于修改各类文件的内容，但apdu指令中的data必须正确上送，中心只计算指令mac；
* 15文件的写文件操作会执行两次，第一次写文件，第二次写文件中的一个标志位。因此增加一个字段，区分执行不同的工作；对于15文件，apdu指令中的DATA信息由中心组装，卡端只需要上送apdu头和正确的卡信息；
* Version：版本号，默认填写10；
* Message type：交易类型，1114；

**域说明：**

* Unitid：营运单位代码，由一卡通统一提供给各接入TSM平台；
* Pos id：设备号，由一卡通统一提供给各接入TSM平台；
* Pos sequence：设备流水号，由TSM平台生成的唯一序列号；
* CItyCode：城市代码，卡内读取；
* CardId：卡内号，卡内读取；
* CardMType：主卡类型，卡内读取；
* CardSType：子卡类型，卡内读取；
* CardModel：卡型，3-M1卡 1-CPU卡，卡内读取；
* Seid：手机卡物理序号，由手机端获取并在请求时给出，该字段为必须字段；
* Ats：通过芯片上电复位指令获取，16进制，，由手机端获取并在请求时给出，该字段为必须字段。如26E2D9D6FE80A020；
* SettDate：结算日期，请求时默认填写全0（如允许请填写签到时一卡通返回的结算日期），应答时由一卡通中心返回；
* WorkFlowSSN：平台流水号，8位TSM平台代码+12位扣款方唯一流水号；
* Regtype：证件类型，00 -居民身份证、01-中小学生证、02-护照、03-军官证、04-士兵证、05-武装警察身份证、06-港澳台通行证、07-台胞证、08-驾驶证、09-暂住证、99-其它；
* Mobile：用户手机号码，由手机端获取并在请求时给出；
* Regtype：证件类型，由手机端获取并在请求时给出。00 -居民身份证、01-中小学生证、02-护照、03-军官证、04-士兵证、05-武装警察身份证、06-港澳台通行证、07-台胞证、08-驾驶证、09-暂住证；
* regNbr：证件号，根据证件类型来定，由手机端获取并在请求时给出；
* custName：客户姓名，由手机端获取并在请求时给出；
* operation：开通状态，0：开户成功1：其他开户失败；填写卡片实际操作的标志，一卡通中心将根据该标志来修改卡片状态。
* Reserved：保留域，暂不使用，默认填写全0；
* Response Code：交易应答码，请求时默认全0，应答时由清算中心返回，TSM平台需要根据该应答码判断是否继续后续的业务处理；

## 空中圈存类交易接口

### 功能及流程说明

空中圈存主要实现卡片的空中充值功能。

### 交易接口说明

#### 联机卡操作请求交易

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 联机卡操作请求交易 | | | | |
| 数据元 | 数据类型 | 说明 | 请求和应答数据值 | |
| 客-服 | 服-客 |
| **Message header** | | | | |
| Version | N2 | 交易版本号 | M | M |
| Message Type | N4 | 交易类型 | M | M |
| Message Date Time | YYYYMMDDhhmmss | 报文发送时间 | M | M |
| MAC | H8 | 通讯押码 | M | 全0 |
| Response Code | H2 | 通讯应答码 | 全0 | M |
| **Transaction header** | | | | |
| Unitid | N8 | 营运单位代码 | M | M |
| NetId | N12 | 网点号 | C | C |
| Posid | N12 | 清算设备代码 | M | M |
| PosSequence | N9 | POS机流水号 | M | M |
| Termid | N12 | 企业设备代码 | M | M |
| Operid | N16 | 操作员号 | M | M |
| EDCardId | N16 | 操作主卡卡号 | C | C |
| CardOprType | N4 | 卡操作交易类型 | M | M |
| CItyCode | N4 | 城市代码 | M | M |
| CardId | N16 | 卡内号 | M | M |
| CardMType | N2 | 主卡类型 | M | M |
| CardSType | N2 | 子卡类型 | M | M |
| CardModel | N1 | 卡型，3-M1卡 1-CPU卡 | M | M |
| TransType | N2 | 业务类型 | M | M |
| CardCSN | H16 | 卡物理标示编号 | C | C |
| SysDatetime | YYYYMMDDhhmmss | 中心时间，可用于设备校正时间 | 全0 | M |
| Deposit | N8 | 押金 | M | M |
| OrigAmt | N8 | 应收金额 | M | M |
| ReloadBal | N8 | 交易金额(仅在钱包操作有效) | C | C |
| UnloadBal | N8 | 需要圈提的金额 | C | C |
| CardValDate | N8 | 卡有效期 | M | M |
| MAC2 | H8 | 钱包加值需要的MAC2（CPU） | C | C |
| SrcBal | N8 | 卡片原额（CPU） | M | M |
| CardSeq | N6 | 卡片交易流水（CPU） | M | M |
| KeyVer | N2 | 卡片密钥版本（CPU） | M | M |
| AlgInd | N2 | 卡片算法标识（CPU） | M | M |
| CardRand | H8 | 卡片随机数（CPU） | M | M |
| MAC1 | H8 | 充资返回信息MAC1（CPU） | M | M |
| DicMAC | H16 | 指令MAC（CPU） | C | C |
| DivData | H18 | 分散因子（CPU） | M | M |
| SettDate | YYYYMMDD | 结算日期 | C | M |
| Txndate | N8 | 交易日期 | M | M |
| Txntime | N6 | 交易时间 | M | M |
| BatchNo | N6 | 批次号 | M | M |
| AuthSeq | N10 | 密钥授权流水号 | C | M |
| Reserved | ANS20 | 保留域 | C | C |
| CommandLen | N3 | APDU指令长度（CPU） | C | C |
| Command | CommandLen | APDU指令（CPU） | C | C |
| Response Code | N5 | 交易应答码 | 全0 | M |

**业务说明：**

* 交易类型为5101，写卡及混合消费查询授权请求；
* 所有联机卡操作业务，都必须先发送5101的联机卡操作请求以联机获取写卡操作秘钥；

**域说明：**

* Version：版本号，POS终端联机交易接入报文版本号均为10；
* MessageType：交易类型，请参照编码规则章节中的外部交易类型说明；
* Message Date Time：报文发送时间，填写终端的当前报文发送时间；
* MAC：通讯押码，计算规则请参考附录中的PBOC-3DES-MAC算法说明；
* Response code：通讯应答码，终端接收到一卡通清算中心应答之后，需要优先判断该通讯应答码是否成功，如果不成功则直接认为该交易失败，不需要对该交易进行后续操作；
* Unitid：营运单位代码，由一卡通统一分配，对于代缴终端要求支持手工维护；
* NetId：网点号，由一卡通统一分配，对于代缴终端要求支持手工维护；
* Posid：清算设备代码，由一卡通统一分配，对于代缴终端要求支持手工维护；
* PosSequence：设备流水号，填写代缴终端交易流水，要求在一定时间内保持唯一；
* TremId：企业设备代码，默认与Posid（清算设备代码）保持一致；
* Operid：操作员号，对于POS终端设备该字段默认由12位清算设备代码（posid）+4位终端操作员号组成；对于客服平台或接入机构该部分由一卡通统一分配；
* ED Card Id：操作主卡卡号，每张操作主卡中的卡内号；
* CardOprType：卡操作交易类型，填写卡操作完成时通知类交易的交易类型（Message Type）；
* CityCode：城市代码，CPU卡内读取；
* CardId：卡号，CPU卡内读取；注意卡号编码规则为城市代码（2BCD）+主卡类型（1BCD）+子卡+类型（1BCD）+卡序列号（4HEX）；
* CardMType：主卡类型 从用户卡中获取；
* CardSType：子卡类型 从用户卡中获取；
* CardModel：对于CPU卡交易，该字段为卡型，3-M1卡 1-CPU卡；
* TransType：01：联机充值请求； 04：充值授权额度冲正；
* CardCSN：卡物理标示编号，在做CPU卡非钱包区操作时需带上CPU卡的ATR后8字节（HEX，报文中需转成16位ASC码，右补零），M1卡操作时为M1卡的CSN（HEX，报文中需转成ASC码，右补零）；
* SysDatetime：清算中心时间，由清算中心应答报文带回，可作为终端时间调整参数；
* ReloadBal：交易金额，只在对电子钱包操作时带入；
* UnloadBal：混合消费时，如判断需要做圈提则中心返回圈提金额；预授权完成申请查询,如果审核通过则返回预授权完成时需充值的金额
* MAC1：充资时CPU卡返回MAC1信息，CPU卡钱包操作时，必须带入；
* MAC2：CPU卡钱包操作时，有清算中心应答报文带回；
* SrcBal：卡片原额，必须带入；
* CardSeq：卡片交易流水，CPU卡钱包操作时，必须带入；
* KeyVer：卡片密钥版本，CPU卡钱包操作时，必须带入；
* AlgInd：卡片算法标识，CPU卡钱包操作时，必须带入；
* CardRand：卡片随机数，CPU卡钱包操作时，必须带入；
* CommandLen：APDU指令长度，CPU卡钱包操作时可不带，非钱包操作的卡写操作时必须带入；
* Command：APDU指令，CPU卡钱包操作时可不带，非钱包操作的卡写操作时必须带入；
* DicMAC：指令MAC，CPU卡钱包操作时可不带，非钱包操作的卡写操作时必须带入；
* BatchNo：签到时获取到的批次号信息；
* AuthSeq：密钥授权流水号，清算中心返回的交易流水号；注：充值授权冲正时，和settdate一起保留
* DivData：CPU卡内住建部安全认证码；
* CardValDate：卡有效期；
* Reserved：如无特殊说明，请求时填写全0；
* CommandLen：APDU指令长度，该字段内容根据实际Command内容进行填写；
* Command：APDU指令内容，填写实际长度的apdu指令数据；
* Response Code：交易应答码，请求时默认全0，应答时由清算中心返回，各接入机构需要根据该应答码判断是否继续后续的业务处理；

#### 联机卡充值交易

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **联机卡充值交易** | | | | |
| 数据元 | 数据类型 | 说明 | 请求和应答数据值 | |
| 客-服 | 服-客 |
| **Message header** | | | | |
| Version | N2 | 交易版本号 | M | M |
| Message Type | N4 | 交易类型 | M | M |
| MessageDateTime | YYYYMMDDhhmmss | 报文发送时间 | M | M |
| MAC | H8 | 通讯押码 | M | 全0 |
| Response Code | H2 | 通讯应答码 | 全0 | M |
| **Transaction header** | | | | |
| Unitid | N8 | 营运单位代码 | M | M |
| LocalSequence | N10 | 发送方报文流水号 | M | M |
| TransType | N2 | 业务类型 | M | M |
| PosId | N12 | 清算设备代码 | M | M |
| SamId | N16 | Sam卡卡号 | C | C |
| PosSequence | N9 | POS机流水号 | M | M |
| Termid | N12 | 企业设备代码 | C | C |
| OperId | N16 | 操作员号 | M | M |
| EDCardId | N16 | 操作主卡卡号 | C | C |
| CardId | N16 | 卡号 | M | M |
| CardAuthCode | H8 | 卡认证码 | C | M |
| CardCnt | N6 | 卡计数器 | M | M |
| CardMKnd | N2 | 卡主类型 | M | M |
| CardSKind | N2 | 卡子类型 | M | M |
| CardModel | N1 | 卡型，3-M11-CPU卡 | M | M |
| ReloadCnt | N4 | 实充次数 | C | C |
| BefBalance | N8 | 交易前钱包剩余额度 | M | M |
| OrigAmt | N8 | 应收金额 | M | M |
| TxnAmt | N8 | 实充额度 | M | M |
| HandingCharge | N8 | 手续费 | M | M |
| Deposit | N8 | 押金 | M | M |
| CardValDate | N8 | 卡有效期 | M | M |
| TradeBeginDate | N8 | 行业钱包起始日期 | C | C |
| TradeEndDate | N8 | 行业钱包终止日期 | C | C |
| TxnDate | YYYYMMDD | 交易日期 | M | M |
| TxnTime | Hhmmss | 交易时间 | M | M |
| CityCode | N4 | 城市代码 | M | M |
| CardVerNo | N2 | 卡内版本号 | M | M |
| SettDate | YYYYMMDD | 结算日期 | 全0 | M |
| BatchNo | N6 | 批次号 | M | M |
| AuthSeq | N18 | 工作密钥授权流水号 | M | M |
| LimitedAuthSeql | N10 | 额度授权流水号 | M | M |
| LastTxnType | N4 | 上笔交易类型 | C | M |
| LastPosId | N12 | 上笔交易终端号 | C | M |
| LastTxnAmt | N8 | 上笔交易金额 | C | M |
| LastCrdCnt | N6 | 上笔交易卡计数器 | C | M |
| LastTxnTime | N14 | 上笔交易时间 | C | M |
| Lastaftamt | N8 | 上笔交易交易前金额 | C | M |
| Lasttac | H8 | 上笔交易TAC | C | M |
| Reserved | ANS20 | 保留域 | 全0 | 全0 |
| TAC | H8 | 交易押码 | M | M |
| TxnResponse | N5 | 交易应答码 | 全0 | M |

**业务说明：**

* 进行卡电子钱包、卡行业钱包的卡片充值操作后，生成充值交易，实时上传至清算中心，完成帐户更新；
* 未实时上传，或上传后无应答的充值交易，需以报文形式进行补传；
* Message Type：交易类型 （2069-联机公用电子钱包充值）；

**域说明：**

* Unitid：营运单位代码，由一卡通统一分配，对于POS终端要求支持手工维护；
* LocalSequence：本地交易流水号，填写代缴终端交易流水，要求在一定时间内保持唯一（如为终端直连默认与设备流水号保持一致）；
* TransType：业务类型，默认填写02；
* Posid：清算设备代码，由一卡通统一分配，对于POS终端要求支持手工维护；；
* SamId：sam卡号，默认填写全0；
* PosSequence：设备流水号，无SAM卡时为设备自行维护的交易连续性编号（等同LocalSequence），有SAM卡时为SAM卡交易流水号；
* Termid：企业设备编号，此处与PosId保持一致（或者可以填写自有终端编号）；
* OperId：操作员号，对于POS终端设备该字段默认由12位清算设备代码（posid）+4位终端操作员号组成；对于客服平台或接入机构该部分由一卡通统一分配；
* EDCardId：操作主卡卡号，如无操作员主卡卡号，该字段默认填写操作员号；
* CardID：用户卡卡内号，从用户卡中获取；
* CardAuthCode：用于MF1卡的反充交易，对于CPU卡该字段默认填写全0；
* CardCnt：卡计数器，对于CPU卡交易卡操作返回；
* CardMType：主卡类型，从用户卡中获取；
* CardSType：子卡类型，从用户卡中获取；
* CardModel：卡物理类型，3-M1、1-CPU卡，默认填写1（CPU卡）；
* ReloadCnt：实充次数，2069电子钱包充值时，直接=1；
* BefBalance：2069-充值时，公用电子钱包中冲之前金额；
* OrigAmt：实际充值时，收取的现金；
* TxnAmt：2069-充值时，实际往卡电子钱包写入的金额（如存在充值优惠时，该域值可能会比OrigAmt大）；
* HandingCharge：充值时，收取的手续费（根据业务规则计算）；
* Deposit：押金，从用户卡中获取；
* CardValDate：卡片有效期，CPU卡卡内读取；
* TradeBeginDate：行业钱包起始日期，默认填写全0；
* TradeEndDate：行业钱包终止日期，默认填写全0；
* TxnDate：交易日期，填写终端交易的日期；
* TxnTime：交易时间，填写终端交易的时间；
* CityCode：用户卡卡内城市编号，CPU卡内读取，默认为卡号的前4位；
* CardVerNo：卡内版本号，从用户卡中获取；
* SettDate：一卡通中心结算日期，请求时填写签到一卡通中心下发的结算日期；
* BatchNo：签到时获取到的批次号信息；
* AuthSeq：5101联机卡操作请求报文中返回的8位结算日期+10密钥授权流水号；
* LimitedAuthSeql：5101联机卡操作请求报文中返回的LimitedAuthSeql值；
* LastTxnType：上笔交易类型，卡内保存的上笔交易信息；
* LastPosId：上笔交易终端号，卡内保存的上笔交易信息；
* LastTxnAmt：上笔交易金额，卡内保存的上笔交易信息；
* LastCrdCnt：上笔交易卡计数器，卡内保存的上笔交易信息；
* LastTxnTime：上笔交易时间，卡内保存的上笔交易信息；
* Lastaftamt:上笔交易交易前金额，卡内保存的上笔交易信息；
* Lasttac:上笔交易TAC，卡内保存的上笔交易信息；
* Reserved：保留域，暂不使用；
* TAC：CPU卡写卡完成之后卡内返回；
* Response Code：交易应答码，请求时默认全0，应答时由清算中心返回，各接入机构需要根据该应答码判断是否继续后续的业务处理；
  1. 数据安全

为了保证一卡通清算中心与TSM平台间密钥更新过程中的数据安全，要求对一卡通系统提供的所有的apdu指令均进行加密，保证传输过程中的数据安全。

APDU指令数据加密统一采用PBOC-3DES-MAC加密标准算法，详见附录一的算法说明；加密秘钥由双方进行约定。

* 1. FTP交易对账接口

由于公交应用的交易流水文件可能非常庞大，不适用与常规数据接口形式来传输，因此需要提供一个FTP服务，以便于行业应用系统进行上传。

## 对账原则

本次系统所涉及的对账交易为开户、充值等交易的记录数据。

## Username 和Password

待定；

## 对账文件的生成时间

待定；

## 下载文件目录

待定；

## 文件命名规则

|  |  |  |
| --- | --- | --- |
| **其它文件名格式** | | |
| 数据元 | 数据类型 | 说明 |
| 文件标示 | A2 | 区分文件类型 |
| 日期 | YYMMDD | 年（用后2位） |
| 营运单位代码 | N8 | 给营运公司的文件用N8，给采集点的文件用N11 |
| 序列号 | N5 | 00000~99999循环 |
| 文件标志 | AN1 | H-手工帐，A-自动帐 |

例如：FD1503197300000100001A

## 对账文件内容格式

### 终端联机充值类对账明细文件（SD）

|  |  |  |  |
| --- | --- | --- | --- |
| **终端联机充值类对账明细文件** | | | |
| 数据元 | 数据类型 | 说明 | 备注 |
| **File Description Area** |  |  |  |
| Version | N2 | 版本号 | 当前版本是10 |
| RtnSign | S2 | 回车符 | 0x0d，0x0a |
| **Transaction Header** |  |  |  |
| settledate | N8 | 结算日期 |  |
| CorpId | N8 | 营运单位代码 |  |
| RecNum | N10 | 记录总数 |  |
| RtnSign | S2 | 回车符 | 0x0d，0x0a |
| **Transaction data（N）** |  |  |  |
| TxnType | N4 | 交易类型 |  |
| TransType | N2 | 业务类型 |  |
| Censeq | N10 | 中心流水号 |  |
| PosId | N12 | 清算设备编号 |  |
| PosSeq | N10 | 终端流水号 |  |
| CardId | N16 | 卡号 |  |
| CityCode | N4 | 城市代码 |  |
| TxnDate | N8 | 交易日期（YYYYMMDD） |  |
| TxnTime | N6 | 交易时间（HHMMSS） |  |
| TxnAmt | N8 | 交易金额（分） |  |
| ErrorCode | N5 | 错误代码 |  |
| RtnSign | S2 | 回车符 | 0x0d，0x0a |

* 1. 编码规则

## 交易类型定义

|  |  |
| --- | --- |
| **交易类型** | **描述** |
| 2055 | 主密钥下载 |
| 2051 | 联机充值签到 |
| 2061 | 联机卡操作请求 |
| 2062 | 联机公用电子钱包充值 |
| 2661 | 联机卡操作冲正 |
| 1110 | 卡号申请交易 |
| 1111 | 卡认证交易 |
| 1112 | 应用密钥更新交易 |
| 1113 | 卡文件通用写卡交易 |
| 1114 | 公交开卡完成交易 |
|  |  |

## 通讯应答码编码

|  |  |  |
| --- | --- | --- |
| **应答编码** | **描述** | **备注** |
| 00 | 成功 |  |
| 01 | 无效的加密压缩算法 |  |
| 02 | 无效的消息类型码 |  |
| 03 | 无效的消息版本 |  |
| 04 | 报文长度无效 |  |
| 05 | 通讯MAC错 |  |
| 06 | 通讯超时 |  |
| 07 | 通讯目标节点不可到达 |  |
| 08 | 报文格式错误 |  |
| 23 | 其它未定义的错误 |  |
| 25 | 无效的交易类型码 |  |
| 50 | 系统错误 |  |
|  |  |  |

## 交易处理结果编码

|  |  |  |
| --- | --- | --- |
| **应答编码** | **描述** | **备注** |
| 00000 | 成功 |  |
| **交易级错误代码** | | |
| 90001 | 该卡已经发行过 | 适应于空中发卡业务 |
| 90002 | 该卡未登记 | 适应于空中发卡业务 |
| 90003 | 其他错误 | 适应于空中发卡业务 |
| 91000 | 通讯mac 错误 | 适应于空中发卡业务 |
| 98888 | 获取卡号失败 | 适应于空中发卡业务 |
| 99998 | 交易数据域错 | 适应于空中发卡业务 |
| 99999 | 表示其他或系统错误 | 适应于空中发卡业务 |
|  | | |
| 00001 | 系统错误 |  |
| 20001 | 无效交易类型 |  |
| 21013 | 卡号不存在 |  |
| 21014 | 卡状态错误 |  |
| 21015 | 卡超过有效期 |  |
| 21022 | 黑名单卡交易 |  |
| 21028 | 卡需要先解挂 |  |
| 24001 | 授权状态未审核 |  |
| 24002 | 授权状态审核失败 |  |
| 24003 | 授权有效截止时间 |  |
| 24004 | 授权金额超过限额 |  |
| 24005 | 授权信息未找到 |  |
| 25003 | 终端设备未签到 |  |
| 25018 | 设备编号不存在 |  |
| 25033 | 该设备已禁用 |  |
| 26040 | 验证充值MAC1失败 |  |
| 26041 | 计算充值MAC2失败 |  |
|  |  |  |

## 异常流程处理说明

|  |  |
| --- | --- |
| **异常情况** | **处理说明** |
| 发卡失败 | 用户删除应用后，重新下载应用进行发卡操作 |
| 扣款成功，TSM平台获取写卡指令失败 | TSM平台判断获取写卡指令失败后，发起冲正请求。 |
| 扣款成功，客户端写卡失败，上送状态成功 | TSM平台获取写卡失败状态后，发起冲正请求。 |
| 扣款成功，客户端写卡失败，上送状态失败 | TSM平台不做处理，在对账流程处理。 |
| 扣款成功，客户端写卡失败，上送状态失败 | TSM平台不做处理，在对账流程处理。 |
|  |  |

* 1. 附录

## 附录一 PBOC-3DES-MAC算法说明



## 附录二 TSM平台交互业务流程说明

### 签到类交易业务流程



### 空中发卡类交易业务流程



### 空中圈存类交易（一卡通侧）业务流程

