CJZF-2016-2

北京畅捷通支付技术有限公司

2017-11-28

畅捷支付POS终端规范

V2.0

目 次

前 言 III

* 1. 消息域说明 5
  2. POS终端消息交换说明 53

附录A（规范性附录）个人标识码（PIN）的加密和解密方法 113

* 1. 用于PIN加、解密的主账号PAN取法 113
  2. PIN的长度 113
  3. PIN的字符集 113
  4. PIN格式 113

附录B（规范性附录）POS终端MAC的算法 115

附录C（规范性附录）磁道信息加密算法 116

* 1. 基本要求 116
  2. 数据源构成 116
  3. 加密方式 116
  4. 举例 116

附录D（规范性附录）对应答码的处理 117

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 日期 | 撰稿人 | 变更内容 |
| v1.6 | 2016/9/8 | 高峰 | 1.增加实名认证交易  2.增加二维码支付相关交易 |
| v1.7 | 2016/9/24 | 高峰 | 1.新增日结通知交易 |
| v1.8 | 2016/10/20 | 高峰 | 1.新增订单查询交易  2.增加订单类处理码，未新增交易，只在现有的消费，冲正，撤销报文中增加域 |
| v1.9 | 2016/11/21 | 高峰 | 1.普通消费增加订单号域(可选填)  2.预授权交易增加订单号域(可选填) |
| v1.9.1 | 2017/07/18 | 高峰 | 1. 入口添加银联21号文上送  2. 返回借贷记卡标识 |
| v2.0 | 2017/11/22 | 张书培 | 1.二维码主扫交易增加5域上送银联c2b码  2.二维码类交易44域增加 004:银联二维码交易  3.预授权类交易增加23域卡片序列号 |

前 言

本规范适用于所有接入畅捷通信息技术股份有限公司支付云事业部系统的POS终端设备。

文档中只涉及到和银联不同的部分(红色字体)，相同部分请参照银联《销售点终端(POS)应用规范》。

畅捷支付POS终端规范

* 1. POS终端安全要求
     1. POS终端联机交易密钥管理
        1. 三级密钥体系

POS终端密钥分为三级：

主密钥 Master Key 缩写：MK

终端主密钥 Terminal Master Key——缩写:TMK

工作密钥 Working Key——缩写:WK

* + - * 1. 主密钥(MK)

用于对终端主密钥(TMK)进行加密保护，多台终端拥有同一主密钥。

* + - * 1. 终端主密钥(TMK)

用于对工作密钥(WK)进行加密保护，每台POS终端与POS中心共享唯一的KEK。

KEK必须要有安全保护措施，只能写入并参与运算，不能被读取。

KEK至少应有三个，以便当KEK泄密时，POS中心与POS终端及时、方便地更换。POS中心与POS终端通过参数下载的方式约定使用哪个KEK。

* + - * 1. 工作密钥（WK）

分为用于对个人标识码(PIN)加密的PIK以及进行报文鉴别(MAC)的MAK。

由POS前置机的加密机产生，在POS终端每次签到时从POS中心利用KEK加密后下载，并由KEK加密存储。

POS终端工作密钥在下载时必须以密文传送，严禁明文传送。

* + - 1. POS终端MAC的算法

详细算法见附录B。

* + - 1. PIN加密

PIN加密采用ANSI X9.8 Format（带主账号信息）。

加密算法采用单倍长密钥算法或双倍长密钥算法。POS终端对以上两种加密算法都应支持。

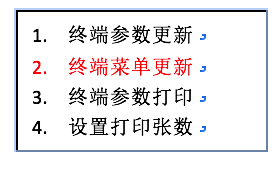
具体的方法见附录A。

* + - 1. 签退

离线签退

* + - 1. 批结算

终端采用离线结算方式。在结算前如果有未上送的冲正、脚本通知、脱机交易，需逐笔上送。如果再次上送失败，放弃上送。



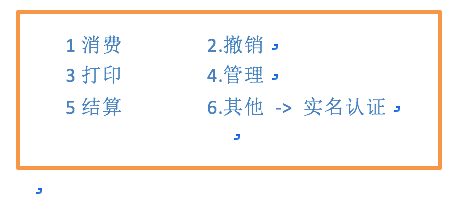
* 1. 主管界面
  2. POS终端交易功能
     1. 终端菜单更新

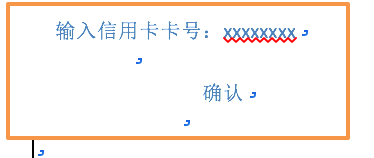
对应POS参数传递交易中网络管理码360交易

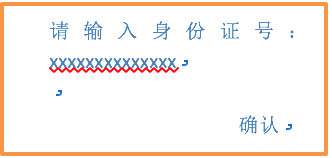
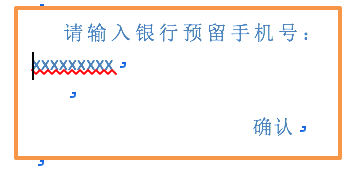
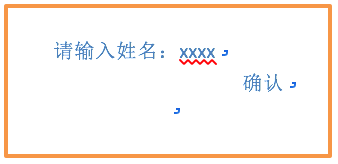
* + 1. 终端参数更新

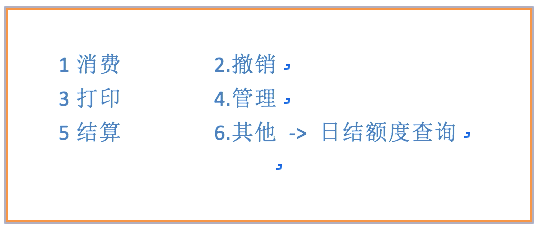
对应POS参数更新交易

* + 1. 实名认证菜单



* + - 1. 流程



* + 1. 日结额度交易
  1. 消息域说明
     1. 说明

POS终端与POS中心之间的消息(Message)是根据《ISO 8583:1987 Bank Card Originated Messages — Interchange Message Specifications — Content For Finalcial Transactions》定义的。

交易要素的描述分散在各个域描述中，以下给出确定交易类型的要素列表：

1. 交易要素

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 交易类型 | 消息类型 | 处理码  (3 域) | 服务点条件码  (25域) | 交易类型码  (60.1域) | 是否引发冲正 |
| 预授权 | 0100/0110 | 030000 | 06 | 10 | 有 |
| 预授权撤销 | 0100/0110 | 200000 | 06 | 11 | 有 |
| 磁条卡现金充值账户验证 | 0100/0110 | 330000 | 00 | 01 | 无 |
| MOTO（订购）预授权 | 0100/0110 | 030000 | 18 | 10 | 有 |
| MOTO（订购）预授权撤销 | 0100/0110 | 200000 | 18 | 11 | 有 |
| 查询 | 0200/0210 | 310000 | 00 | 01 | 无 |
| 联盟积分查询 | 0200/0210 | 310000 | 65 | 03 | 无 |
| 消费8 | 0200/0210 | 000000 | 00 | 22 | 有 |
| 消费撤销9 | 0200/0210 | 200000 | 00 | 23 | 有 |
| 预授权完成（请求） | 0200/0210 | 000000 | 06 | 20 | 有 |
| 预授权完成（请求）撤销 | 0200/0210 | 200000 | 06 | 21 | 有 |
| 订购预授权完成（请求） | 0200/0210 | 000000 | 18 | 20 | 有 |
| 订购预授权完成（请求）撤销 | 0200/0210 | 200000 | 18 | 21 | 有 |
| 电子现金脱机消费 | 0200/0210 | 000000 | 00 | 36 | 无 |
| 分期付款交易 | 0200/0210 | 000000 | 64 | 22 | 有 |
| 分期付款交易撤销 | 0200/0210 | 200000 | 64 | 23 | 有 |
| 积分消费 | 0200/0210 | 000000 | 65 | 22 | 有 |
| 积分消费撤销 | 0200/0210 | 200000 | 65 | 23 | 有 |
| MOTO（订购）消费 | 0200/0210 | 000000 | 08 | 22 | 有 |
| MOTO（订购）消费撤销 | 0200/0210 | 200000 | 08 | 23 | 有 |
| 基于PBOC电子钱包的IC卡指定账户圈存 | 0200/0210 | 600000 | 91 | 40 | 有 |
| 基于PBOC电子钱包的IC卡现金充值 | 0200/0210 | 630000 | 91 | 41 | 有 |
| 基于PBOC电子钱包的IC卡非指定账户转账圈存 | 0200/0210 | 620000 | 91 | 42 | 有 |
| 基于PBOC借/贷记应用的小额支付IC卡指定账户圈存 | 0200/0210 | 600000 | 91 | 45 | 有 |
| 基于PBOC借/贷记应用的小额支付IC卡现金充值 | 0200/0210 | 630000 | 91 | 46 | 有 |
| 基于PBOC借/贷记应用的小额支付IC卡非指定账户圈存 | 0200/0210 | 620000 | 91 | 47 | 有 |
| 磁条卡现金充值 | 0200/0210 | 630000 | 00 | 48 | 无 |
| 磁条卡账户充值 | 0200/0210 | 400000 | 66 | 49 | 无 |
| 预约消费 | 0200/0210 | 000000 | 67 | 54 | 有 |
| 预约消费撤销 | 0200/0210 | 200000 | 67 | 53 | 有 |
| 电子现金现金充值撤销 | 0200/0210 | 170000 | 91 | 51 | 有 |
| 退货（包含联盟积分的退货） | 0220/0230 | 200000 | 00 | 25 | 无 |

* + 1. 数据类型

POS终端与POS中心之间的交换消息中，各数据元类型如下所列：

* A 字母向左靠，右部多余部分填空格。
* 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。
* B 二进制bit位。
* DD 日。
* hh 时。
* LL 可变长域的长度值(二位数)。
* LLL 可变长域的长度值(三位数)。
* MM 月。
* mm 分。
* N 数值，右靠，首位有效数字前充零。若表示金额，则最右二位为角分。
* S 特殊符号。
* ss 秒。
* VAR 可变长域。
* X 借贷符号，在数值之前，D表示借，C表示贷。
* YY 年。
* Z 由ISO 7811和ISO 7813制定的磁条卡第二、三磁道的数据类型。
* CN BCD压缩编码数值。

对可变长数据元，以下例说明：

* 变量XYZ的数据类型为ANS...999(LLLVAR)，则表示：该变量中可含字母、数字和特殊符号，最长不超过999个字符，长度由三位数字确定。
* 变量XYZ的数据类型为N...999（LLLVAR），则在压缩时，其长度位用右靠的BCD码压缩，而其后紧随的数字内容用左靠的BCD码压缩。这是为了保证有效内容和其位数中间无缺省填充值。若不为偶数位，左靠的数字内容后补零。由于有长度位表征该域有效内容的长度，因此后补零不会改变该域的真实值。
* 本文档中声明的压缩变量属性是针对POS终端与POS中心之间的消息，POS中心与任何金融机构之间的消息将全部采用ASCII码且不压缩的格式。
  + 1. 数据元名称及其定义
       1. 消息类型

消息类型(Message Type Identifier)

* + - * 1. 变量属性

N4，4个字节的定长数字字符域。

压缩时用BCD码表示的2个字节的定长域。

* + - * 1. 域描述

消息类型。定义如下：

* 0100授权类请求消息：
* POS预授权请求。
* POS追加预授权请求。
* POS预授权撤销请求。
* 0110授权类应答消息：
* POS预授权应答。
* POS追加预授权应答。
* POS预授权撤销应答。
* 0200金融类请求消息：
* POS查询请求。
* POS消费请求。
* POS消费撤销请求。
* POS预授权完成（联机）请求。
* POS预授权完成撤销请求。
* 基于PBOC电子钱包的IC圈存
* 0210金融类应答消息:
* POS查询应答。
* POS消费应答。
* POS消费撤销应答。
* POS预授权完成（联机）应答。
* POS预授权完成撤销应答。
* 基于PBOC电子钱包的IC圈存
* 0220金融通知类消息：
* POS退货通知。
* POS结算通知。
* POS结算调整通知。
* POS预授权完成（离线）通知。
* 0230金融通知类应答消息:
* POS退货应答。
* POS结算应答。
* POS结算调整应答。
* POS预授权完成（离线）通知应答。
* 0320 批上送消息：
* POS终端批上送。
* 0330批上送应答消息：
* POS终端批上送应答。
* 0400冲正类消息：
* POS预授权冲正。
* POS预授权撤销冲正。
* POS消费冲正。
* POS消费撤销冲正。
* POS预授权完成（联机）冲正。
* POS预授权完成撤销冲正。
* 基于PBOC电子钱包的IC圈存
* 0410冲正类应答消息：
* POS预授权冲正应答。
* POS预授权撤销冲正应答。
* POS消费冲正应答。
* POS消费撤销冲正应答。
* POS预授权完成（联机）冲正应答。
* POS预授权完成撤销冲正应答。
* 基于PBOC电子钱包的IC圈存
* 0500对账类消息：
* POS终端批结算请求。
* 0510对账类应答消息：
* POS终端批结算应答。
* 0620基于PBOC借/贷记卡标准的IC卡脚本处理结果通知消息
* 基于PBOC借/贷记卡标准的IC卡脚本处理结果通知
* 0630基于PBOC借/贷记卡标准的IC卡脚本处理结果通知应答
* 基于PBOC借/贷记卡标准的IC卡脚本处理结果通知应答
* 0800网络业务管理类消息：
* POS终端签到请求。
* POS终端参数传递请求。
* 0810网络业务管理类应答消息：
* POS终端签到应答。
* POS终端参数传递应答。
* 0820网络业务管理类消息：
* POS终端签退请求。
* POS终端回响测试请求。
* POS终端状态上送。
* 0830网络业务管理类应答消息：
* POS终端签退应答。
* POS终端回响测试应答。
* POS终端状态上送应答。
  + - 1. 域2

主账号(Primary Account Number)

* + - * 1. 变量属性

N..19(LLVAR)，2个字节的长度值＋最大19个字节的主账号，

压缩时用BCD码表示的1个字节的长度值＋用左靠BCD码表示的最大10个字节的主账号。

* + - * 1. 域描述

用户主账号，即从磁条卡的第二磁道或第三磁道上获取的账号，或在交易时输入的主账户号，或读IC卡获得的卡号。该账号最多19个数字字符。长度值最大不能超过19。

主账号应符合下列标准之一：

a) 《中华人民共和国金融行业标准 JR/T 0008-2000 银行卡发卡行标识代码及卡号》的规定。

b) 银联认可的国际信用卡公司的规定。

c) 由中国人民银行认可的其他标准。

* + - * 1. 用法

若POS终端通过刷卡获取客户磁条卡的第二和第三磁道信息，则不置该域的值。客户的主账号将由POS中心从POS请求消息中的第二磁道或第三磁道信息上截取，填入此域，并转发给发卡方。POS终端可从应答消息中得到主账号信息。

若交易时操作员在POS终端手输卡号或者通过读IC卡得到卡号，POS终端无法获取客户磁条卡的第二和第三磁道信息，则需在请求消息中置入该域的值，POS中心将以此域为准，并在请求和应答消息中保持不变。

* + - 1. 域3

交易处理码(Processing Code)

* + - * 1. 变量属性

N6，6个字节的定长数字字符域，压缩时用BCD码表示的3个字节的定长域。

* + - * 1. 域描述

交易处理码(Processing Code)由六位数字组成。第1和第2位表示交易类别。

1. 交易处理码的第1和2位定义

| 第1、2位 | Description | 含义 |
| --- | --- | --- |
| **00-19** | **Debits** | **借记** |
| 00 | Goods And Service | 商品和服务 |
| 01 | Cash | 现金 |
| 02 | Adjustment | 调整 |
| 03 | Cheque Guarantee(Funds Guaranteed) | 支票担保(资金可担保) |
| 04 | Cheque Verification(Funds Available But Not Guaranteed) | 支票核实(资金可用但不担保) |
| 05 | Euro-cheque | 欧洲支票 |
| 06 | Traveller Cheque | 旅行支票 |
| 07 | letter Of Credit | 信用证 |
| 08 | Giro(Postal Banking) | 直接转账(邮政银行业务) |
| 09 | Goods And Service With Cash Disbursement Transfer | 现金支付的商品和服务 |
| 10-13 | Reserved For ISO Use | ISO保留使用 |
| 14-16 | Reserved For National Use | 国家保留使用 |
| 17-19 | Reserved For Private Use | 私有保留使用 |
| **20-29** | **Credits** | **贷记** |
| 20 | Returns | 退款 |
| 21 | Deposits | 存款 |
| 22 | Adjustment | 调整 |
| 23 | Cheque Deposit Guarantee | 支票存款担保 |
| 24 | Cheque Deposit | 支票存款 |
| 25-26 | Reserved For ISO Use | ISO保留使用 |
| 27 | Reserved For National Use | 国家保留使用 |
| 28-29 | Reserved For Private Use | 私有保留使用 |
| **30-39** | **Inquiry services** | **查询服务** |
| 30 | Available Funds Inquiry | 可用金额查询 |
| 31 | Balance Inquiry | 余额查询 |
| 32-35 | Reserved For ISO Use | ISO保留使用 |
| 36-37 | Reserved For National Use | 国家保留使用 |
| 38-39 | Reserved For Private Use | 私有保留使用 |
| **40-49** | **Transfer services** | **转账服务** |
| 40 | Cardholder Accounts Transfer | 持卡人账户转账 |
| 41-45 | Reserved For ISO Use | ISO保留使用 |
| 46-47 | Reserved For National Use | 国家保留使用 |
| 48-49 | Reserved For Private Use | 私有保留使用 |
| **50-99** | **Reserved** | 保留 |
| 60 |  | 圈存 |

第3和第4位表示受借记和查询，以及转出账户的账户类型。第5和第6位表示受贷记以及转入账户的账户类型。

1. 交易处理码第3和5位的定义

| **第3、5位** | **Description** | **含义** |
| --- | --- | --- |
| 0 | Default | 默认 |
| 1 | Saving Account | 储蓄账户 |
| 2 | Cheque Account | 支票账户 |
| 3 | Credit Facility | 信用透支账户 |
| 4 | Universal Account number | 通用账户 |
| 5 | Investment Account | 投资账户 |
| 6-7 | Reserved For ISO Use | ISO保留使用 |
| 8 | Reserved For national Use | 国家保留使用 |
| 9 | Reserved For Private Use | 私有保留使用 |

1. 交易处理码第4和6位的定义

| 第4、6位 | Description | 含义 |
| --- | --- | --- |
| 0 | Default | 默认 |
| 1-2 | Reserved For ISO Use | ISO保留使用 |
| 3-7 | Reserved For National Use | 国家保留使用 |
| 8-9 | Reserved For Private Use | 私有保留使用 |
| 4 | Universal Account number | 通用账户 |
| 5 | Investment Account | 投资账户 |

* + - * 1. 用法

1. 交易处理码用法

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 交易类型 | 未选卡种 | 储蓄卡账户 | 支票账户 | 信用卡账户 | 通用账户 |
| 余额查询 | 310000 | 311000 | 312000 | 313000 | 314000 |
| 预授权/冲正/追加预授权/冲正 | 030000 | 031000 | 032000 | 033000 | 034000 |
| 预授权撤销/冲正 | 200000 | 201000 | 202000 | 203000 | 204000 |
| 消费/冲正 | 000000 | 001000 | 002000 | 003000 | 004000 |
| 消费撤销/冲正 | 200000 | 201000 | 202000 | 203000 | 204000 |
| 预授权完成（联机）/冲正/预授权完成（离线）通知 | 000000 | 001000 | 002000 | 003000 | 004000 |
| 预授权完成撤销/冲正 | 200000 | 201000 | 202000 | 203000 | 204000 |
| 退货 | 200000 | 201000 | 202000 | 203000 | 204000 |
| 结算（离线） | 000000 | 001000 | 002000 | 003000 | 004000 |
| 结算调整（离线） | 000000 | 001000 | 002000 | 003000 | 004000 |
| 圈存/冲正 | 600000 | 601000 | 602000 | 603000 | 604000 |

* + - 1. 域4

交易金额(Amount Of Transactions)

* + - * 1. 变量属性

N12，12个字节的定长数字字符域，压缩时用BCD码表示的6个字节的定长域。

* + - * 1. 域描述

交易金额，交易金额不包括任何手续费。

* + - * 1. 用法

交易金额的币种由域49—交易币种(Currency Code Of Transaction)表示。若为人民币则交易金额的单位是人民币的分。

* ：POS消费金额为1000元，则交易金额应为000000100000。

当交易币种为外币时，如果该币种没有小数位，则该域的值代表实际交易金额；如果该币种有两个小数位，则表示方法同人民币；若有三个小数位，则最后一个小数位必须为零。用法举例如下表所示：

1. 交易金额用法

| 币种 | 小数位数 | 实际金额 | 本域值 |
| --- | --- | --- | --- |
| 人民币 | 两位小数 | 1000．02 | 000000100002 |
| 外币 | 没有小数位 | 1000 | 000000001000 |
| 两位小数 | 1000．02 | 000000100002 |
| 三位小数 | 1000．112 | 000001000110 |

在查询交易、管理类交易和脚本通知交易中，该域不出现。

* + - 1. 域11

受卡方系统跟踪号(System Trace Audit Number)

* + - * 1. 变量属性

N6，6个字节的定长数字字符域，压缩时用BCD码表示的3个字节的定长域。

* + - * 1. 域描述

受卡方(POS交易的POS终端)赋予交易的在某段时间内唯一确定该笔交易的流水号。对POS交易的受卡方来说，该跟踪号与41域(受卡方终端标识码)、42域(受卡方标识码)、60.2域(批次号)和消息类型的组合唯一标识该笔交易。

* + - * 1. 用法

对POS交易，POS终端对发起的每一笔正常交易赋予一个跟踪号。对于冲正交易该域与原始交易保持一致，而对于撤销消息，61.2域(原POS流水号)填原始交易的11域。

受卡方系统跟踪号是个关键的数据域。因此POS中心及发卡方在收到消息后保存该值，并在应答消息中原样返回给POS终端。POS终端应用该值和41域(受卡方终端标识码)、42域(受卡方标识码)、60.2域(批次号)、消息类型一起匹配原始请求消息。

* + - 1. 域12

受卡方所在地时间(Time Of Local Transaction)

* + - * 1. 变量属性

N6，6个字节的定长数字字符域，压缩时用BCD码表示的3个字节的定长域。

格式：hhmmss。

* + - * 1. 域描述

交易发生时，受卡方所在地时间。格式为hhmmss，其中hh为小时，mm为分，ss为秒。

* + - * 1. 用法

POS中心收到POS终端的请求消息时，POS中心赋予所在地时间。发卡方在收到请求消息后保存该值，并在应答消息中原样返回给POS中心。POS中心将把12域和13域一起返回给POS终端。

受卡方所在地时间的取值范围：

* hh： 00－23
* mm： 00－59
* ss： 00－59
  + - 1. 域13

受卡方所在地日期(Date Of Local Transaction)

* + - * 1. 变量属性

N4，4个字节的定长数字字符域，压缩时用BCD码表示的2个字节的定长域。

格式：MMDD。

* + - * 1. 域描述

交易发生时，受卡方所在地日期。

格式为MMDD，其中MM为月份，DD为日。

* + - * 1. 用法

POS中心收到POS终端的请求消息时，POS中心赋予POS中心所在地日期，其具体用途详见域12说明。

受卡方所在地日期的取值范围：

* MM： 01－12
* DD： 01－31
  + - 1. 域14

卡有效期(Date Of Expired)

* + - * 1. 变量属性

N4，4个字节的定长数字字符域，压缩时用BCD码表示的2个字节的定长域。

格式：YYMM。

* + - * 1. 域描述

银行卡的有效期。

格式为YYMM，其中YY为年份，MM为月份。

* + - * 1. 用法

在请求消息中，当手输卡号或主账号时，要求同时输入卡的有效期（如有），由POS机置入，否则不置。

在应答消息中，对于存在有效期的卡，由发卡方置入，否则不置。

* + - 1. 域15

清算日期(Date Of Settlement)

* + - * 1. 变量属性

N4，4个字节的定长数字字符域，压缩时用BCD码表示的2个字节的定长域。

格式：MMDD。

* + - * 1. 域描述

POS中心和发卡方之间的交易结算日期。

格式为MMDD，其中MM为月份，DD为日。

* + - * 1. 用法

POS中心对每个收到或发起的交易消息都赋予该交易的清算日期。表明该交易将于该清算日被POS中心清算。

POS终端可在应答消息中获知交易的清算日期。

对于冲正消息的清算日期应为原始交易的清算日期。不支持隔日冲正。

清算日期的取值范围：

* MM： 01－12
* DD： 01－31
  + - 1. 域22

服务点输入方式码(Point Of Service Entry Mode)

* + - * 1. 变量属性

N3，3个字节的定长数字字符域，压缩时用左靠BCD码表示的2个字节的定长域。

* + - * 1. 域描述

服务点输入方式码，即持卡人数据(如主账户和个人标识码)的输入方式。服务点(Point Of Service)是指交易的各种始发场合。

1. 服务点输入方式

| 第1、2位 | 含义 | 第3位 | 含义 |
| --- | --- | --- | --- |
| 00 | 未指明 | 0 | 未指明 |
| 01 | 手工 | 1 | PIN可输入 |
| 02 | 磁条 | 2 | PIN不可输入 |
| 03 | 条形码 | 3-5 | ISO保留使用 |
| 04 | 光学字符阅读 | 6-7 | 国家保留使用 |
| 05 | 集成电路卡 | 8-9 | 私有保留使用 |
| 06-60 | ISO保留使用 |  |  |
| 61-80 | 国家保留使用 |  |  |
| 81-99 | 私有保留使用 |  |  |
| 90 | 磁条读入信息可靠，第二磁道信息必须出现 |  |  |
| 95 | 集成电路卡，卡信息不可靠 |  |  |

* + - * 1. 用法

目前常用的服务点输入方式代码一般为：

* 021：刷卡，且PIN可输入；
* 022：刷卡，无PIN；
* 011或012：手工输入卡号或主账号；
* 050：IC卡读入，卡数据可靠；
* 950：是IC卡，但卡数据不可靠。

其他用法按照表12的说明。

* + - 1. 域23

卡序列号(Card Sequence Number)

* + - * 1. 变量属性

N3，3个字节的定长数字字符域，压缩时用右靠BCD码表示的2个字节的定长域。

* + - * 1. 域描述

IC卡的序列号

* + - * 1. 用法

用于区别具有相同PAN的不同卡。只在IC卡交易时使用。

* + - 1. 域25

服务点条件码(Point Of Service Condition Mode)

* + - * 1. 变量属性

N2，2个字节的定长数字字符域，压缩时用左靠BCD码表示的1个字节的定长域。

* + - * 1. 域描述

服务点条件码，用于和其他关键域来决定消息种类，描述如下：

1. 服务点条件码

| 代码 | 含义 | 与此相关的编辑 |
| --- | --- | --- |
| 00 | 正常提交 |  |
| 01 | 客户不提交 | 不允许PIN数据 |
| 02 | 非扩展终端 | 必须输入PIN |
| 03 | 可疑商户 |  |
| 05 | 客户提交但卡不提交 | 必须是01X0授权消息 |
| 06 | 预授权请求 | 要求预授权号 |
| 08 | 邮政或电话汇单 | 必须是01X0，00X0消息，但PIN不提交 |
| 10 | 确认的客户标识 |  |
| 11 | 作弊嫌疑 | 消息类型必须为0100或0200 |
| 12 | 安全原因 | 消息类型必须为0100或0200 |
| 51 | 电子商务交易的正常提交 |  |
| 52 | 电子商务交易的预授权请求 | 要求预授权号 |
| 60 | 追加预授权 |  |
| 91 | 基于PBOC电子钱包的IC卡圈存交易 |  |

* + - * 1. 用法

目前使用的服务点输入方式代码为：

* 00： 正常提交；
* 06： 预授权类交易。
  + - 1. 域26

服务点PIN获取码(Point Of Service PIN Capture Code)

* + - * 1. 变量属性

N2，2个字节的定长数字字符域，压缩时用BCD码表示的1个字节的定长域。

* + - * 1. 域描述

服务点设备所允许输入的个人密码明文的最大长度。

1. 服务点PIN获取码

|  |  |
| --- | --- |
| 代码 | 含义 |
| 0-3 | ISO保留使用 |
| 4-12 | 由服务点设备接受的PIN的最大字符数目 |
| 13-59 | ISO保留使用 |
| 60-73 | 国家保留使用 |
| 80-99 | 私有保留使用 |

* + - * 1. 用法

该域描述了服务点设备所允许输入的个人密码明文的最大长度。

* + - 1. 域27

借贷记标识(在小票上显示借贷记类型时，因pos不能识别卡类型，需后台返回卡类型)

* + - * 1. 变量属性

N1，1个字节的定长数字字符域，压缩时用左靠BCD码表示的1个字节的定长域。

* + - * 1. 域描述

| 代码 | 含义 |
| --- | --- |
| 0 | 借记卡 |
| 1 | 贷记卡 |

* + - 1. 域32

受理方标识码(Acquiring Institution Identification Code)

* + - * 1. 变量属性

N..11(LLVAR)，

2个字节的长度值＋最大11个字节的受理方标识码，

压缩时用BCD码表示的1个字节的长度值＋用左靠BCD码表示的最大6个字节的受理方标识码。

* + - * 1. 域描述

受理方标识码。POS交易中一般指POS中心。

* + - * 1. 用法

目前用八位数字来标识一个机构，故若此域的长度值不等于8则被认为消息格式出错，详细编码见《银行卡联网联合技术规范V2.0》中“第六部分 附录”。

* + - 1. 域35

2磁道数据(Track 2 Data)

* + - * 1. 变量属性

Z..37(LLVAR)，

2个字节的长度值＋最大37个字节的第二磁道数据(数字和分隔符)，

压缩时用BCD码表示的1个字节的长度值＋用左靠BCD码表示的最大19个字节的第二磁道数据。

* + - * 1. 域描述

用户磁条卡上的第二磁道数据。

* + - * 1. 用法

它从第二磁道开始符(；)后的第一个字符读起，包括域的分隔符，但不包括结束符和LRC符。

外卡只读二磁道。

* + - 1. 域36

3磁道数据(Track 3 Data)

* + - * 1. 变量属性

Z...104(LLLVAR)，

3个字节的长度值＋最大104个字节的第三磁道数据(数字和分隔符)，

压缩时用右靠BCD码表示的2个字节的长度值＋用左靠BCD码表示的最大52个字节的第三磁道数据。

* + - * 1. 域描述

用户磁条卡上的第三磁道数据。

* + - * 1. 用法

它从第三磁道开始符(；)后的第一个字符读起，包括域的分隔符，但不包括结束符和LRC符。

* + - 1. 域37

检索参考号(Retrieval Reference Number)

* + - * 1. 变量属性

AN12，12个字节的定长字符域。

* + - * 1. 域描述

POS中心赋予每笔从POS终端收到的预授权/金融/冲正交易的、在每个清算日内唯一的系统流水号。POS中心用该流水号与消息类型、12域(受卡方所在地时间)和13域(受卡方所在地日期)的组合唯一地标识该笔交易(重复发送的冲正交易将被认为是一笔交易)。

POS中心赋予POS终端发出的非在线交易类消息的流水号。

* + - * 1. 用法一

POS终端在收到交易应答消息时可获取POS中心的系统流水号，本域的值可作为日后交易查询的依据。

* + - * 1. 用法二

POS中心赋予POS终端发出的非在线交易类消息的流水号。

* + - 1. 域38

授权标识应答码(Authorization Identification Response)

* + - * 1. 变量属性

AN6，6个字节的定长字符域。

* + - * 1. 域描述

发卡方对交易的授权标识应答码，在一定时间段内保持唯一。

* + - * 1. 用法

在预授权交易中，发卡方将在成功的应答消息中返回一个有效的授权号，以供后续交易使用。

在预授权完成（联机）交易的请求消息中，POS终端将预授权交易或电话授权中得到的授权号放入本域，传给发卡方。由发卡方去匹配原始预授权交易；

对于冲正、撤销和退货交易，如原始交易的应答中有授权码，则本域的值应来自原始交易。

* + - 1. 域39

应答码(Response Code)

* + - * 1. 变量属性

AN2，2个字节的定长字符域。

* + - * 1. 域描述

发卡方或POS中心响应POS终端的应答码。

POS终端上送的冲正通知中表明冲正原因。

* + - * 1. 用法

交易应答码中仅"00"为交易成功，其它为交易不成功。

应答码表参见《银行卡联网联合技术规范V2.0》中第六部分附录中附录A.3应答码。

POS终端引发的冲正消息中，存放冲正原因码：

1. 冲正原因码

|  |  |
| --- | --- |
| 冲正原因码 | 说明 |
| 98 | POS终端在时限内未能收到POS中心的应答 |
| 96 | POS终端收到POS中心的批准应答消息，但由于POS机故障无法完成交易 |
| A0 | POS终端对收到POS中心的批准应答消息，验证MAC出错 |
| 06 | 其他情况引发的冲正 |

* + - 1. 域41

受卡机终端标识码(Card Acceptor Terminal Identification)

* + - * 1. 变量属性

ANS8，8个字节的定长域。

* + - * 1. 域描述

POS终端的标识码。该标识码在POS中心的网络中唯一标识一个终端，不能重复。

* + - * 1. 用法

受卡机终端标识码是个关键的数据域。POS中心及发卡方在收到消息后应保存该值，并在应答消息中原样返回给POS终端。

POS用该值和11域(受卡方系统跟踪号)、42域(受卡方标识码)、60.2域(批次号)一起匹配原始请求消息。

* + - 1. 域42

受卡方标识码(Card Acceptor Identification Code)

* + - * 1. 变量属性

ANS15，15个字节的定长域。

* + - * 1. 域描述

受卡方的标识码，即商户代码。

* + - * 1. 用法

目前根据中国银联规定的《银行卡特约商户统一编码及使用规则》执行。

* + - 1. 域44

附加响应数据(Additional Response Data)

* + - * 1. 变量属性

AN..25，2个字节长度+ 最大25个字节的数据。

压缩时用右靠BCD码表示的1个字节的长度值＋用ASCII码表示的最大25个字节的数据。

* + - * 1. 域描述

附加响应数据。发卡方的附加响应数据必须为有效字符。由发卡方在批准交易时载入应答消息。

* + - * 1. 用法

在交易响应消息中返回接收机构和收单机构的标识码。

格式如下：

* 数据元长度 N2
* 接收机构标识码 AN11 表示发卡行标识码（左靠，右部多余部分填空格）
* 收单机构标识码 AN11 表示商户结算行标识码（左靠，右部多余部分填空格）
  + - 1. 域48

附加数据 - 私有(Additional Data - Private)

* + - * 1. 变量属性

N...322(LLLVAR)，3个字节长度+ 最大322个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用左靠BCD码表示的最大161个字节的数据。

* + - * 1. 域描述

私有，用于存放POS批结算时的结算总额、批上送时的交易明细和交易明细总笔数。

* + - * 1. 用法一：结算总额

批结算时存放结算总额。

N...062(LLLVAR)，3个字节的长度值＋最大62个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用左靠BCD表示的最大31个字节的数据。

在POS批结算请求时，将本批次成功的交易的借记总金额、借记总笔数、贷记总金额、贷记总笔数上送POS中心。如果POS中心的处理结果是“对账不平”，则在POS批结算响应消息中，返回POS中心的结算总额，否则，原值返回。

如果内、外卡分开批结算，则需要内卡结算总额和外卡结算总额两部分，如果内外卡一起批结算，可以只用内卡结算总额部分存放合计总额。

格式定义如下：

* 数据元长度 N3
* 内卡结算总额，内容为：
* 借记总金额 N12
* 借记总笔数 N3
* 贷记总金额 N12
* 贷记总笔数 N3
* 对账应答代码 N1
* 外卡结算总额，内容为：
* 借记总金额 N12
* 借记总笔数 N3
* 贷记总金额 N12
* 贷记总笔数 N3
* 对账应答代码 N1

结算总额的统计算法如下：

a) 借记总金额：

∑（消费金额 + 预授权完成（联机）金额＋预授权完成（离线）金额+离线结算金额+结算调整金额＋基于PBOC电子钱包/存折标准的离线消费金额＋基于PBOC借/贷记标准的离线消费金额）

b) 借记总笔数：

∑（消费笔数 + 预授权完成（联机）笔数＋预授权完成（离线）笔数+离线结算笔数+结算调整笔数＋基于PBOC电子钱包/存折标准的离线消费笔数＋基于PBOC借/贷记标准的离线消费笔数）

c) 贷记总金额：

∑ ( 退货金额 + 消费撤销金额 + 预授权完成（联机）撤销金额＋基于PBOC借/贷记标准的消费撤销金额)

d) 贷记总笔数：

∑（退货笔数 + 消费撤销笔数 + 预授权完成（联机）撤销笔数＋基于PBOC借/贷记标准的消费撤销笔数）

* 1. 对账应答代码：

在请求消息中填“0”，在对账应答消息中表示接收方(POS中心)的处理结果。其中：

1. 对账应答码说明

| 对账应答码 | 对账应答码说明 |
| --- | --- |
| 0 | ISO保留 |
| 1 | 对账平 |
| 2 | 对账不平 |
| 3 | 出错 |
| 4-5 | ISO保留使用 |
| 6-7 | 国家保留使用 |
| 8-9 | 私有保留使用 |

* + - * 1. 用法二：磁条卡交易明细

批上送消息中存放磁条卡交易的明细信息，全部采用BCD码压缩标识，最大为161个字节。

其格式如下：

* 数据元长度 N3
* 交易笔数 N2 后面所跟的交易笔数，最大值为8。
* 交易明细1 N40 第一笔交易记录。
* 交易明细2 N40 第二笔交易记录。
* ……
* 交易明细8 N40 第八笔交易记录。

其中交易明细1—交易明细8为每笔交易的详细记录，其定义为：

* 卡类别 N2 00 内卡交易，01 外卡交易。
* 交易流水号 N6 POS流水号，原交易域11的值。
* 卡号 N20 卡号(右对齐，左补零)。
* 交易金额 N12 金额。
  + - * 1. 用法三：交易明细总笔数

批上送结束消息中本域用于存放本批所有批上送消息中包含的交易明细总笔数，采用BCD码压缩表示，共占2个字节：

* 数据元长度 N3
* 总笔数 N4 本批上送的交易总笔数。
  + - * 1. 用法四：小费金额

在离线结算和结算调整交易中存放小费的金额，采用BCD码压缩表示，共占6个字节。定义如下：

* 数据元长度 N3
* 金额 N12 小费金额。
  + - 1. 域49

交易货币代码(Currency Code Of Transaction)

* + - * 1. 变量属性

AN3，3个字节的定长字符域。

* + - * 1. 域描述

交易所用货币的代码。

* + - * 1. 用法

人民币的货币代码为156。

所有预授权/金融类交易消息中用本域标识交易币种。

现仅支持人民币作为交易币种。

* + - 1. 域52

个人标识码数据(PIN Data)

* + - * 1. 变量属性

B64，8个字节的定长二进制数域。

* + - * 1. 域描述

持卡人的个人密码的密文。

* + - * 1. 用法

如果域22指明有PIN输入，则本域必须出现。客户的个人标识码(PIN)必须加密后存放在此域中。PIN的格式在域53中标明。

本系统允许的PIN长度最大为12位数字。

* + - 1. 域53

安全控制信息(Security Related Control Information )

* + - * 1. 变量属性

n16，16个字节的定长数字字符域。

压缩时用BCD码表示的8个字节的定长域。

* + - * 1. 域描述

与安全相关的控制信息。

* + - * 1. 用法

在交易类消息中，该域用于标识PIN的类型。

该数据结构定义如下：

* PIN-FORMAT-USED n1 PIN格式
* ENCRYPTION-METHOD-USED n1 加密算法标志
* RESERVED n14 置为全“0”

1. 安全控制信息取值

|  |  |
| --- | --- |
| PIN-FORMAT-USED | PIN加密方法 1：ANSI X9.8 Format（不带主账号信息）  2：ANSI X9.8 Format（带主账号信息） |
| ENCRYPTION-METHOD-USED | 加密算法标志。 0：单倍长密钥算法  6：双倍长密钥算法  其他取值：其他加密算法(未用) |

* + - 1. 域54

附加金额(Balance Amount)

* + - * 1. 变量属性

AN...040(LLLVAR)，3个字节的长度值＋最大20个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大20个字节的数据。

* + - * 1. 域描述

表示附加金额数据。

* + - * 1. 用法一：账户可用余额

查询交易响应消息中表示持卡人的账户可用余额。

该域为自定义域，内容定义如下：

* LENGTH n3 数据元长度
* AVAILABLE-BALANCE-AMOUNT 账户上的可用余额，记录内容为：
* ACCOUNT-TYPE n2 账户类型
* AMOUNT-TYPE n2 数量类型
* CURRENCY-CODE an3 货币代码
* AMOUNT SIGN an1 余额符号
* AMOUNT n12 余额

上述各数据项取值为：

1. 域54用法一

|  |  |
| --- | --- |
| 数据项 | 取值 |
| Length | 020 |
| Amount Type | 可用余额：02 |
| Account Type | 储蓄账户：10  信用卡账户：30 |
| Currency Code | 156 |
| Amount Sign | 贷方金额：C为正值 |
| Amount | 余额的值 |

* + - * 1. 用法二：累计授权金额

用于追加预授权交易中，由发卡方填写，表示本笔追加预授权完成后的累计授权金额。

a) 用法标志－2字节，取值“TA”，含义为累计授权金额。

b) 剩余字节格式如下：

1. 域54用法二

|  |  |
| --- | --- |
| 内容 | 数据 |
| 累计授权金额 | N 12 |
| 保留使用 | Ans 6 |

若本笔追加预授权成功，则

累计授权金额＝本笔追加授权金额＋上期累计金额；

若本笔追加预授权失败，则

累计授权金额＝上期累计金额。

* + - * 1. 用法三：日结额度

查询交易响应消息中表示持卡人的账户可用余额。

该域为自定义域，内容定义如下：

* LENGTH n3 数据元长度
* AVAILABLE-BALANCE-AMOUNT 账户上的可用余额，记录内容为：
* ACCOUNT-TYPE n2 账户类型
* AMOUNT-TYPE n2 数量类型
* CURRENCY-CODE an3 货币代码
* AMOUNT SIGN an1 余额符号
* AMOUNT n12 余额

|  |  |
| --- | --- |
| 数据项 | 取值 |
| Length | 020 |
| Amount Type | 可用额度：02 |
| Account Type | 储蓄账户：10  信用卡账户：30 |
| Currency Code | 156 |
| Amount Sign | 贷方金额：C为正值 |
| Amount | 余额的值 |
| 数据项 | 取值 |
| Length | 020 |
| Amount Type | 总额度：03 |
| Account Type | 账户：10 |
| Currency Code | 156 |
| Amount Sign | 贷方金额：C为正值 |
| Amount | 余额的值 |

* + - 1. 域55

IC卡数据域(Intergrated Circuit Card System Related Data)

* + - * 1. 变量属性

该域是一个变长域（LLLVAR），最长可达255个字节，最开始是一个占3个字节的长度值信息。

压缩时采用右靠BCD码表示长度信息，长度信息占两个字节。

所支持的数据属性有：

* b 二进制（二进制数或者位组合）。
* cn BCD码。右对齐，左补‘0’。如，数字12345可以保存在n12的授权金额数据对象中，形如‘00 01 23 45’。
* An 每个字节包含一个字符字母数字型数据元（A-Z，a-z，0-9）。
* var. up to N 变长数据，最大长度可为N。
  + - * 1. 域描述

本域将根据不同的交易种类包含不同的子域。处理中心仅在受理方和发卡方之间传递这些适用于IC卡交易的特有数据，而不对它们进行任何修改和处理。为适应该子域需要不断变化的情况，本域采用TLV（tag-length-value）的表示方式，即每个子域由tag标签(T)，子域取值的长度(L)和子域取值(V)构成。

tag标签的属性为bit，由16进制表示，占1～2个字节长度。例如，“9F33”为一个占用两个字节的tag标签。而“95”为一个占用一个字节的tag标签。若tag标签的第一个字节（注：字节排序方向为从左往右数，第一个字节即为最左边的字节。bit排序规则同理。）的后四个bit为“1111”，则说明该tag占两个字节，例如“9F33”；否则占一个字节，例如“95”。

子域长度（即L本身）的属性也为bit，占1～3个字节长度。具体编码规则如下：

a) 当L字段最左边字节的最左bit位（即bit8）为0，表示该L字段占一个字节，它的后续7个bit位（即bit7～bit1）表示子域取值的长度，采用二进制数表示子域取值长度的十进制数。例如，某个域取值占3个字节，那么其子域取值长度表示为“00000011”。所以，若子域取值的长度在1～127字节之间，那么该L字段本身仅占一个字节。

b) 当L字段最左边字节的最左bit位（即bit8）为1，表示该L字段不止占一个字节，那么它到底占几个字节由该最左字节的后续7个bit位（即bit7～bit1）的十进制取值表示。例如，若最左字节为10000010，表示L字段除该字节外，后面还有两个字节。其后续字节的十进制取值表示子域取值的长度。例如，若L字段为“1000 0001 1111 1111”，表示该子域取值占255个字节。所以，若子域取值的长度在127～255字节之间，那么该L字段本身需占两个字节。

子域取值根据不同的子域含义分别取不同的数值。由于该域中所包含的子域都是IC卡卡片和IC卡终端所特有的信息，而非处理中心的特征信息，处理中心仅为一个数据传递的桥梁，所以具体取值需参见IC卡卡片及IC卡终端规范，并根据其标准的变化不断更新。对于境内交易需参见《中国金融集成电路（IC）卡借记贷记规范V2.0－卡片部分》和《中国金融集成电路（IC）卡借记贷记规范V2.0－终端部分》。对于外卡收单交易需根据不同国际信用卡公司组织（例如，Visa、万事达、JCB、大莱、运通）的发卡策略参见其相应的卡片和终端规范。但由于所有组织（包括银联）对卡片和终端的定义都是基于EMV2000标准的，因此不论这些信息的具体取值有何不同，它们的tag标签都是一致的。因此，在本标准中仅给出tag标签，入网机构即可根据标签取值查找到不同组织对该子域的具体取值。下面将列举每个子域的tag标签、和长度值及其属性。

* + - * 1. 用法

1. 基本信息子域列表

| 子域中文名称 | 子域英文名称 | 子域缩写 | 子域tag标签值 | 子域所占长度  （单位：字节） | 子域属性 |
| --- | --- | --- | --- | --- | --- |
| 应用密文 | Application Cryptogram | AC | 9F26 | 8 | B |
| 密文信息数据 | Cryptogram Information Data | － | 9F27 | 1 | B |
| 发卡行应用数据 | Issuer Application Data | IAD | 9F10 | 最大到32 | B |
| 不可预知数 | Unpredictable Number | － | 9F37 | 4 | B |
| 应用交易计数器 | Application Transaction Counter | ATC | 9F36 | 2 | B |
| 终端验证结果 | Terminal Verificaion Result | TVR | 95 | 5 | B |
| 交易日期 | Transaction Date | － | 9A | 3 | CN（包含6位有效数字，格式YYMMDD） |
| 交易类型 | Transaction Type | － | 9C | 1 | CN（包含2位有效数字） |
| 授权金额 | Transaction Amount or Amount Authorized | － | 9F02 | 6 | CN（包含12位有效数字） |
| 交易货币代码 | Transaction Currency Code | － | 5F2A | 2 | CN（包含3位有效数字） |
| 应用交互特征 | Application Interchange Profile | － | 82 | 2 | B |
| 终端国家代码 | Terminal Country Code | － | 9F1A | 2 | CN（包含2位有效数字） |
| 其它金额 | Amount Other | － | 9F03 | 6 | CN（包含12位有效数字） |
| 终端性能 | Terminal Capabilities | － | 9F33 | 3 | B |

1. 可选信息子域列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 子域中文名称 | 子域英文名称 | 子域缩写 | 子域tag标签值 | 子域所占长度  （单位：字节） | 子域属性 |
| 持卡人验证方法结果 | Cardholder Verfication Method Results | CVM | 9F34 | 3 | B |
| 终端类型 | Terminal Type | － | 9F35 | 1 | CN（两位有效数字） |
| 接口设备序列号 | Interface Device Serial Number | IFD | 9F1E | 8 | AN |
| 专用文件名称 | Dedicated File Name | DF | 84 | 5～16 | B |
| 应用版本号 | Terminal Application Version Number | － | 9F09 | 2 | B |
| 交易序列计数器 | Transaction Sequence Counter | － | 9F41 | 2～4 | CN（包含4到8个有效数字） |
| 发卡行认证数据 | Issuer Authentication Data | － | 91 | 8～16 | B |
| 发卡行脚本1 | Issuer Script Template 1 | － | 71 | var. up to 128 | B |
| 发卡行脚本 2 | Issuer Script Template 2 | － | 72 | var. up to 128 | B |
| 发卡方脚本结果 | Issuer Script Results | － | DF31 | var. up to 21 | B |

1. 脱机交易专用子域列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 子域中文名称 | 子域英文名称 | 子域缩写 | 子域tag标签值 | 子域所占长度  （单位：字节） | 子域属性 |
| 授权响应码 | Authorization Response Code | － | 8A | 2 | an |

* + 1. 域57

自定义域(Reserved Private)

* + - 1. 变量属性

ANS...999(LLLVAR)，3个字节的长度值＋最大999个字节的数据域。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大999个字节的数据。

* + - 1. 域描述

POS 终端应用加密硬件序列号

a) 加密数据内容

加密数据内容为终端硬件序列号+加密随机因子.

b) 加密算法

加密算法采用国家密码算法SM4，密钥长度为16字节，加密算法详见附录A。

* + - 1. 用法

根据银联21号文规定，20170701号之后生产的pos需上送终端应用加密硬件序列号, 加密数据内容为终端硬件序列号+加密随机因子。

本域采用TLV（tag-length-value）的表示方式，即每个子域由tag标签(T)，子域取值的长度(L)和子域取值(V)构成。其中tag标签数据属性为an2，子域长度数据属性为n3，子域取值数据属性根据子域属性确定。

**57域内容**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 中文名称 | tag 标签值 | 取值所占长度（单位：字节） | 属性 | 备注 |
| SM 算法加密PIN 数据 |  | 16 字节 | B128 |  |
| 终端硬件序列号及密文数据 |  | 最长128 字节 | ANS…128 | A2 用法包含2  层TLV 定义 |
| 扫码付信息域 |  | 最长350 字节 | ANS…350 |  |
| 扫码付付款凭证码 |  | 最长20 字节 | AN…20 |  |
|  |  |  |  |  |

该域是一个变长域（LLLVAR），最长可达999字节，最开始是一个占3个字节的长度值信息。压缩

时采用右靠BCD码表示长度信息，长度信息占两个字节。

**用法A2 子域列表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 中文名称 | tag 标签值 | 取值所占长度（单位：字节） | 属性 | 备注 |
| 设备类型 | 04 | 2字节 | AN2 | 01：ATM  02：传统POS  03：MPOS  04：智能POS  05：II 型固定电  话POS |
| 终端硬件序列号 | 05 | 最长50 字节 | ANS…50 | 6 位厂商编号+2  位终端类型（同  设备类型）+42位自定义序列  号  详见《强化支付  终端规范管理  实施方案》 |
| 加密随机因子 | 06 | 最长10 字节 | AN…10 | 加密随机因子  取值说明：  银行卡交易采  用2 域卡号后6  位；  扫码付交易采  用C2B 码后6  位 |
| 硬件序列号密文数据 | 07 | 8 字节 | B64 |  |
| 应用程序版本号 | 08 | 8 字节 | ANS8 | 应用程序变更  应保证版本号  不重复，当长度  不足时，右补空  格 |

* + - 1. 域58

PBOC电子钱包标准的交易信息（PBOC\_ELECTRONIC\_DATA）

* + - * 1. 变量属性

ans...100(LLLVAR)，3个字节的长度值＋最大100个字节的字母、数字字符、特殊符号，压缩时采用右靠2个字节表示长度值。

* + - * 1. 域描述

本标准中只支持电子钱包的应用。

本域在IC卡圈存交易中存放用于计算MAC1、MAC2的数据。在脱机消费中存放用于计算TAC的数据。报文域中第一、二字节为ASCII码表示的用法标志, 用法以相应的英文缩写标识。

1. 域58域用法说明

|  |  |  |
| --- | --- | --- |
| 格式符 | 对应用法 | 说明 |
| RQ | 用法一 | load ReQuest IC卡的圈存请求 |
| RP | 用法二 | load ResPonse IC卡的圈存应答 |
| TA | 用法三 | 脱机消费请求 |

* + - * 1. 用法一： IC卡的圈存请求

用于IC卡的圈存请求报文中，指出该报文中的哪些域的值需要进行MAC1计算。

用法标志--2字节，取值“RQ”。

IC卡的圈存请求报文中需要进行MAC1计算的域包括：

1. 域58用法一

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 58域的子域 | 名称 | 说明 | 长度（字节） | 属性 |
| 58.1 | 发卡方标识 | 用来唯一标识发卡方的一个数字 | 8 | CN |
| 58.2 | 卡片应用序列号 | 发卡方分配的一个数字，符合国家标准GB/T14504-93 | 10 | CN |
| 58.3 | 伪随机数 | IC卡随机产生的一个数字 | 4 | B |
| 58.4 | 密钥索引号 | 为了唯一标识在一个密钥版本中的密钥索引号而分配的一个数字 | 1 | CN |
| 58.5 | 密钥版本号 | 圈存交易的密钥版本 | 1 | B |
| 58.6 | 钱包联机交易序号 | 每当交易发生时就增加 | 2 | B |
| 58.7 | 计算MAC1子域 |  |  |  |
| 58.7.1 | 钱包余额 | 电子钱包的当前余额 | 3 | B |
| 58.7.2 | 交易金额 | 当前交易的金额 | 4 | B |
| 58.7.3 | 交易类型标识，TTI | 02钱包圈存 | 1 | CN |
| 58.7.4 | 终端机编号 | 用来唯一标识商户终端的一个数字 | 6 | CN |
| 58.8 | MAC1 |  | 4 | B |
| * 如果某个子域报文中没有，则填二进制的0。 | | | | |

* + - * 1. 用法二： IC卡的圈存应答

用于IC卡的圈存应答报文中，指出该报文中的哪些域的值需要进行MAC2计算。

* 用法标志--2字节，取值“RP”。
* IC卡的圈存应答报文中需要进行MAC2计算的域包括：

1. 域58用法二

| 58域的子域 | 名称 | 说明 | 长度（字节） | 属性 |
| --- | --- | --- | --- | --- |
| 58.1 | 发卡方标识 | 用来唯一标识发卡方的一个数字 | 8 | CN |
| 58.2 | 卡片应用序列号 | 发卡方分配的一个数字，符合国家标准GB/T14504-93 | 10 | CN |
| 58.3 | 伪随机数 | IC卡随机产生的一个数字 | 4 | B |
| 58.4 | 密钥索引号 | 为了唯一标识在一个密钥版本中的密钥索引号而分配的一个数字 | 1 | CN |
| 58.5 | 密钥版本号 | 圈存交易的密钥版本 | 1 | B |
| 58.6 | 钱包联机交易序号 | 每当交易发生时就增加 | 2 | B |
| 58.7 | 计算MAC2子域 |  |  |  |
| 58.7.1 | 交易金额 | 当前交易的金额 | 4 | B |
| 58.7.2 | 交易类型标识，TTI | 02钱包圈存 | 1 | CN |
| 58.7.3 | 终端机编号 | 用来唯一标识商户终端的一个数字 | 6 | CN |
| 58.7.4 | 交易日期 | 主机时间（CCYYMMDD），其中“CC”表示：世纪。 | 4 | CN |
| 58.7.5 | 交易时间 | 主机时间（HHMMSS） | 3 | CN |
| 58.8 | MAC2 |  | 4 | B |
| * 如果某个子域报文中没有，则填二进制的0。 | | | | |

* + - * 1. 用法三：脱机消费请求

用于IC卡的脱机请求报文中，指出该报文中的哪些域的值需要进行MAC1计算。

用法标志--2字节，取值“TA”。

IC卡的脱机消费请求报文中需要进行TAC计算的域包括：

1. 域58用法三

| 58域的子域 | 名称 | 说明 | 长度（字节） | 属性 |
| --- | --- | --- | --- | --- |
| 58.1 | 发卡方标识 | 用来唯一标识发卡方的一个数字 | 8 | CN |
| 58.2 | 卡片应用序列号 | 发卡方分配的一个数字，符合国家标准GB/T14504-93 | 10 | CN |
| 58.3 | 伪随机数 | IC卡随机产生的一个数字 | 4 | B |
| 58.4 | 密钥索引号 | 为了唯一标识在一个密钥版本中的密钥索引号而分配的一个数字 | 1 | CN |
| 58.5 | 密钥版本号 | 脱机消费交易的密钥版本 | 1 | B |
| 58.6 | 钱包脱机交易序号 | 每当交易发生时就增加 | 2 | B |
| 58.7 | 计算TAC子域 |  |  |  |
| 58.7.1 | 交易金额 | 当前交易的金额 | 4 | B |
| 58.7.2 | 交易类型标识 | 06钱包脱机消费 |  |  |
| 58.7.3 | 终端机编号 | 用来唯一标识商户终端的一个数字 | 6 | CN |
| 58.7.4 | 终端交易计数器 | 终端里的一个计数器，每当交易发生就增加。 | 4 | B |
| 58.7.5 | 交易日期 | 终端日期（CCYYMMDD），其中“CC”表示：世纪。 | 4 | CN |
| 58.7.6 | 交易时间 | 终端时间（HHMMSS） | 3 | CN |
| 58.8 | TAC |  | 4 | B |
| * 如果某个子域报文中没有，则填二进制的0。 | | | | |

* + - 1. 域59

自定义域(Reserved Private)

* + - * 1. 变量属性

ANS...100(LLLVAR)，3个字节的长度值＋最大100个字节的数字字符域。

压缩时用右靠BCD码表示的2个字节的长度值＋用左靠BCD码表示的最大50个字节的数据。

* + - * 1. 域描述

本域为自定义域。

* + - * 1. 用法一：终端设备信息

所有的POS终端向收单处理平台发送的初始化请求交易消息中，均包含59.1域和59.2域。

* 数据元长度 N3
* 59.1 终端厂家标识 N20
* 59.2 终端序列号sn N30
* 59.3 基站信息 N10
* 59.4 pos程序版本号 N2
* 59.4域上送版本号定义，根据终端类型和通讯方式的不同，自定义如下：
* CDMA通讯：51 GPRS通讯：52 如有多种机型临时定义。
  + - * 1. 用法二：卡名称

在消费，消费撤销，预授权，预授权撤销，预授权完成和预授权完成撤销交易应答报文中，存放卡名称信息。

* 数据元长度 N3
* 59.1 卡标识 N4
* 59.2 卡名称 ANS20
  + - * 1. 用法三：基站信息

在消费，预授权，预授权完成交易请求报文中，存放无线pos的基站信息和sim卡id。

* 数据元长度 N3
* 59.1 基站信息 N10
* 59.2 Sim卡ID ANS50

参数编码表

| 含义 | 格式 | 取值 |
| --- | --- | --- |
| 基站信息 | N10 | 对于GPRS，内容包括LAC(5 bytes)+CELL\_ID(5 bytes)，不足5位左补0。  对于CDMA， 内容包括00000+BaseStationID（5 bytes），不足5位左补0。 |
| Sim卡ID | Ans50 | 读出来多少字节，就上送多少字节，不超过50字节 |

* + - 1. 域60

自定义域(Reserved Private)

* + - * 1. 变量属性

N...013(LLLVAR)，3个字节的长度值＋最大13个字节的数字字符域。

压缩时用右靠BCD码表示的2个字节的长度值＋用左靠BCD码表示的最大7个字节的数据。

* + - * 1. 域描述

本域为自定义域。

* 数据元长度 N3
* 60.1 消息类型码 N2
* 60.2 批次号 N6
* 60.3 网络管理信息码 N3
* 60.4 终端读取能力 N1
* 60.5 基于PBOC借/贷记标准的IC卡条件代码 N1
  + - * 1. 用法

所有的POS终端向POS中心发送的交易消息中，均包含60.1域和60.2域指明本交易的交易类型和清算批次。

POS的网络管理类报文中，网络管理信息码与消息类型码的组合标识不同的网络管理类消息。

其中：

1. 60.1 消息类型码

|  |  |  |
| --- | --- | --- |
| 消息类型编码 | 消息类型 | 说明 |
| 01 | 查询 | 第一位含义：  0——查询类交易  1——授权类交易  2——金融类交易  3——离线类交易  4——PBOC电子钱包交易  6——二维码交易  第二位含义：  偶数——借记  奇数——贷记 |
| 10 | 预授权/冲正/追加预授权/冲正 |
| 11 | 预授权撤销/冲正 |
| 20 | 预授权完成（联机）/冲正 |
| 21 | 预授权完成撤销/冲正 |
| 22 | 消费/冲正 |
| 23 | 消费撤销/冲正 |
| 24 | 预授权完成（离线） |
| 25 | 退货 |
| 30 | 离线结算 |
| 32 | 离线结算调整 |
| 34 | 离线结算调整(追加小费) |
| 36 | 离线消费 |
| 40 | 基于PBOC电子钱包的IC卡圈存/冲正 |  |
| 45 | 电子现金指定账户圈存/冲正 |  |
| 50 | 实名认证 |  |
| 60 | 下单交易 |  |

1. 60.3 网络管理信息码

| 消息类型 | 网络管理信息码 | 说明 |
| --- | --- | --- |
| 0800/0810 | 001 | POS终端签到 |
| 0820/0830 | 002 | POS终端签退 |
| 0800/0810 | 003 | POS终端签到（双倍长密钥算法) |
| 0500/0510 | 201 | POS终端批结算 |
| 0320/0330 | 201 | POS终端批上送 |
| 0320/0330 | 202 | 对账不平衡时，POS终端批上送结束 |
| 0320/0330 | 203 | 对账平衡时，POS终端上送成功的IC卡联机交易明细 |
| 0320/0330 | 204 | 对账平衡时，POS终端上送IC卡通知信息 |
| 0320/0330 | 205 | 对账不平衡时，POS终端上送成功的IC卡联机交易明细 |
| 0320/0330 | 206 | 对账不平衡时，POS终端上送IC卡通知信息 |
| 0320/0330 | 207 | 对账平衡时，POS终端批上送结束 |
| 0320/0330 | 208 | 对账平衡时，POS终端上送圈存交易圈存确认明细 |
| 0320/0330 | 209 | 对账不平衡时，POS终端上送圈存交易圈存确认明细 |
| 0820/0830 | 301 | 回响测试 |
| 0820/0830 | 362 | POS终端状态监控 |
| 0800/0810 | 360 | POS终端磁条卡参数下载 |
| 0800/0810 | 361 | POS终端磁条卡参数下载结束 |
| 0800/0810 | 370 | POS终端IC卡公钥下载 |
| 0800/0810 | 371 | POS终端IC卡公钥下载结束 |
| 0820/0830 | 372 | POS终端IC卡公钥信息查询 |
| 0800/0810 | 380 | POS终端IC卡参数下载 |
| 0800/0810 | 381 | POS终端IC卡参数下载结束 |
| 0820/0830 | 382 | POS终端IC卡参数信息查询 |
| 0620/0630 | 951 | 基于PBOC借/贷记标准IC卡脚本处理结果通知 |

1. 60.4 终端读取能力

|  |  |
| --- | --- |
| 取值 | 说明 |
| 0 | 终端读取能力不可知 |
| 2 | 可读取磁条卡 |
| 5 | 可读取IC卡。当22域取值05或95时，该域必须填5。 |

1. 60.5 基于PBOC借/贷记标准的IC卡条件代码

| 取值 | 说明 |
| --- | --- |
| 0 | 未使用或后续子域存在 |
| 1 | 上一笔交易不是IC卡交易或是一笔成功的IC卡交易 |
| 2 | 上一笔交易虽是IC卡交易但失败 |
| * 22域取值02或90且60.4取值5且60.5取值1或2表示Fall Back现象。   Fall Back现象可能出现在如下几种情况中：  a) 卡上的芯片出现问题或在芯片终端不工作的情况下，芯片卡只能通过读取卡上的磁条信息来进行交易。  b) 虽然卡片和芯片终端可以交互，但是终端却无法读取卡片上的应用，也只能通过读取卡上的磁条信息来进行交易。 | |

* + - 1. 域61

原始信息域(Original Message)

* + - * 1. 变量属性

N...029(LLLVAR)，3个字节的长度值＋最大29个字节的数字字符域，

压缩时用右靠BCD码表示的2个字节的长度值＋用左靠BCD码表示的最大15个字节的数据。

* + - * 1. 域描述

该域为自定义域，表示原始交易的信息。该域划分成五个子域，格式定义如下：

* 数据元长度 N3
* 61.1 原始交易批次号 N6
* 61.2 原始交易POS流水号 N6
* 61.3 原始交易日期 N4
* 61.4原交易授权方式 N2
* 61.5原交易授权机构代码 N11
  + - * 1. 用法

冲正、撤销和退货交易时填原始交易数据。

* 61.1 原始交易批次号：冲正、撤销、结算调整和基于PBOC借/贷记标准IC卡脚本处理结果通知交易时填原始请求交易的域60.2，其余情况置为六个零。
* 61.2 原始交易POS流水号：冲正、撤销、结算调整和基于PBOC借/贷记标准IC卡脚本处理结果通知交易时填原始请求交易的域11，其余情况置为六个零。
* 61.3 原始交易日期：冲正、撤销、预授权撤销、预授权完成（联机）、退货、离线结算和基于PBOC借/贷记标准IC卡脚本处理结果通知交易时填原始请求交易的域13，其余情况置为四个零。
* 61.4 原交易授权方式：离线结算/调整交易时填原始授权交易的授权方式。可以是如下几种情况：00—POS预授权，01—电话预授权，02—代授权。
* 61.5 原交易授权机构代码：离线结算交易时，如果原始授权交易为电话预授权，则填入授权机构的标识码。
  + - 1. 域62

自定义域(Reserved Private)

* + - * 1. 变量属性

ANS...512(LLLVAR)，3个字节的长度值＋最大512个字节的数据域。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大512个字节的数据。

* + - * 1. 用法一：终端密钥(POS Security Key)

变量属性

B...056(LLLVAR)，

3个字节的长度值＋最大56个字节的二进制域。

压缩时用右靠BCD码表示的2个字节的长度值＋最大56个字节的二进制域。

域描述

收单处理平台向POS终端约定的新工作密钥，若长度域不为75或100，将认为该域格式有误。

在POS终端签到的应答消息中，本域的长度应为75或100个字节，存放由收单处理平台产生的POS终端新工作密钥或新工作密钥和新TMK。

格式：密钥属性(1 位)+密钥密文(16 位)+校验值(8 位)

0x00:TMK

0x01:MAC\_KEY;

0x02:PIN\_KEY;

0x03：TDK(磁道信息加密密钥);

传送方式为二进制码，顺序为25位MAC\_KEY，25位PIN\_KEY，25位TDK，25位TMK。

校验值算法：用解出的16字节明文对8个数值0做双倍长密钥算法，比较checkvalue的值是否一致的。

* + - * 1. 用法二：终端状态信息(Terminal Status Information)

变量属性

ANS...160(LLLVAR)，3个字节的长度值＋最大160个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大160个字节的数据。

域描述

监控报文中存放终端状态信息。其格式为：编码+取值

1. 状态信息编码表

| 编码 | 含义 | 格式 | 取值 |
| --- | --- | --- | --- |
| 硬件状态 | | | |
| 01 | 键盘状态 | N1 | 1—正常，0—不正常 |
| 02 | 密码键盘状态 | N1 | 1—正常，0—不正常 |
| 03 | 读卡器状态 | N1 | 1—正常，0—不正常 |
| 04 | 打印机状态 | N1 | 1—正常，0—不正常 |
| 05 | 显示器状态 | N1 | 1—正常，0—不正常 |
| 下载的参数 | | | |
| 11 | POS终端应用类型 | N2 | 60 |
| 12 | 超时时间 | N2 | 2位数字表示的秒数 |
| 13 | 重试次数 | N1 | 1位数字 |
| 14 | 三个交易电话号码之一 | N14 | 14位数字 |
| 15 | 三个交易电话号码之二 | N14 | 14位数字 |
| 16 | 三个交易电话号码之三 | N14 | 14位数字 |
| 17 | 一个管理电话号码 | N14 | 14位数字 |
| 18 | 是否支持小费 | N1 | 1—支持，0—不支持 |
| 19 | 小费百分比 | N2 | 2位数字，00—99 |
| 20 | 是否支持手工输入卡号 | N1 | 1—支持，0—不支持 |
| 21 | 是否自动签退 | N1 | 1—自动，0—不自动 |
| 23 | 交易重发次数 | N1 | 1位数字 |
| 24 | 离线交易上送方式 | N1 | 1—随下笔联机交易上送一笔离线交易，  0—批结算之前一并上送 |
| 25 | 主密钥INDEX | N1 | 1位数字，指明当前使用主密钥序号 |
| 通讯统计 | | | |
| 51 | POS拨通率 | N12  (N4+N5+N3) | 从上次成功统计到本次统计的时间段(小时)+5位数字表示的总拨号次数+3位数字表示的拨通率(百分比) |

* + - * 1. 用法三：终端参数信息(Configation Table Message)

变量属性

ANS...160(LLLVAR)，3个字节的长度值＋最大160个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大160个字节的数据。

域描述

参数下载时存放参数信息。其格式为：编码+取值

参数编码表

| 编码 | 含义 | 格式 | 取值 | 默认值 |
| --- | --- | --- | --- | --- |
| 11 | 支持的交易类型 | N32 | 1010 0000 0000 0000 0000 0000 0000 0000 |  |
| 12 | 商户名称 | ANS40 |  |  |
| 13 | 广告语 | ANS120 |  |  |

1. 支持的交易类型说明

| 位数（BIT） | 表示的消息类型 | 取值说明 |
| --- | --- | --- |
| 1 | 查询 | 0——不支持该交易  1——支持该交易  24位之后取0 |
| 2 | 消费/冲正 |
| 3 | 消费撤销/冲正 |
| 4 | 退货 |
| 5 | 预授权/冲正 |
| 6 | 预授权撤销/冲正 |
| 7 | 预授权完成/冲正 |
| 8 | 预授权完成撤销/冲正 |
| 9－11 | 保留（原管理类交易） |
| 12 | 电子签名 |
| 13 | 电子现金消费（快速支付） |
| 14 | 电子现金消费（普通支付） |
| 15 | 电子现金明细查询离线消费 |
| 16 | 电子现金余额查询 |
| 17 | 脱机退货 |
| 18 | 指定账户圈存 |
| 19 | 非指定账户圈存 |
| 20 | 现金充值 |
| 21 | 现金充值撤销 |
| 22 | 插卡消费 |
| 23 | 闪付凭密消费 |
| 24 | 闪付凭密预授权 |
| 25 | 日结消费 |  |

* + - * 1. 用法四：PBOC借/贷记IC卡终端专用参数信息(PBOC IC Configation Table Message)

变量属性

ANS...512(LLLVAR)，3个字节的长度值＋最大512个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大512个字节的数据。

域描述

第一部分：认证中心公钥参数

PBOC借/贷记IC卡终端下载其专用参数时存放的参数信息。除基本应用参数外，它还有一套特殊的参数－认证中心公钥参数。下面首先描述认证中心公钥参数的下载参数信息和流程。

认证中心公钥参数共包含如下参数信息：RID、认证中心公钥索引、认证中心公钥有效期、认证中心公钥哈什算法标识、认证中心公钥算法标识、认证中心公钥模、认证中心公钥指数、认证中心公钥校验值。

每个信用卡组织都可能包含若干个公钥，因此，认证中心公钥参数会反复出现。

认证中心公钥类参数采用TLV（tag＋length＋value）格式表示，具体取值及含义为：

1. 认证中心公钥参数

| 参数名称 | 参数属性 | 参数长度（byte） | 参数tag值 | 参数含义 | 参数下载时间 | 参数适应场合 |
| --- | --- | --- | --- | --- | --- | --- |
| RID | b | 5 | 9F06 | 与认证中心公钥索引一起标识认证中心的公钥 | 安装或调整时 | 交易应用 |
| 认证中心公钥索引 | b | 1 | 9F22 | 与RID一起标识认证中心的公钥 | 安装或调整时 | 交易应用 |
| 认证中心公钥有效期 | n8 | 4 | DF05 | 认证中心规定的有效期限 | 安装或调整时 | 交易应用 |
| 认证中心公钥哈什算法标识 | b | 1 | DF06 | 标识用于在数字签名方案中产生哈什结果的哈什算法 | 安装或调整时 | 交易应用 |
| 认证中心公钥算法标识 | b | 1 | DF07 | 标识使用在认证中心公钥上的数字签名算法 | 安装或调整时 | 交易应用 |
| 认证中心公钥模 | b | 变长，最大为248 | DF02 | 公钥模值 | 安装或调整时 | 交易应用 |
| 认证中心公钥指数 | b | 1或3 | DF04 | 公钥指数 | 安装或调整时 | 交易应用 |
| 认证中心公钥校验值 | b | 变长 | DF03 | 验证认证中心公钥用 | 安装或调整时 | 交易应用 |
| * 认证中心公钥校验值的计算内容为RID+认证中心公钥索引＋认证中心公钥模+认证中心公钥指数；认证中心公钥校验值的计算方法为SHA-1。 | | | | | | |

下面描述认证中心公钥下载流程。

认证中心公钥下载可以区分为两个流程：一是POSP统一更新流程，一是POS主动更新流程。需要注意的是，不论是哪个流程，都应该遵守如下原则：每次只传输一个公钥，若传输过程中发生中断，则重新传输该公钥。

a) POSP统一更新流程：

第一步：从POSP控制台给所有需更新公钥信息的终端置更新公钥信息标志；

第二步：对于每台终端，不论其上送何种交易，只要POSP认为该终端需要更新认证中心公钥信息，即在POSP反馈给POS终端的应答报文头的“处理要求”字段中填入“4”，通知POS终端获取公钥信息；

第三步：POS终端接收到报文头“处理要求”字段填“4”的报文后，立即自动上送认证中心公钥信息查询报文，报文格式如12.4.9POS状态上送一节。网络管理码60.3域和62域用法四第一部分的具体取值请参见12.4.9节；

第四步：POSP收到POS终端上送查询认证中心公钥信息报文后，将POSP目前的公钥信息在应答报文中反馈给POS终端。网络管理码60.3域和62域用法四第一部分的具体取值请参见12.4.9节；

第五步：POS终端收到POSP公钥信息列表后，先进行删除公钥、更改有效期等操作，如果需要下载新的公钥，上送认证中心公钥下载请求报文，POSP收到请求报文后，将公钥内容在应答报文中传递给终端。网络管理码60.3域和62域用法四第一部分的具体取值请参见12.4.7节。

第六步：POS下载结束后，发送下载结束报文。具体报文格式请参见12.4.10节。网络管理码60.3域也请参见12.4.10节。该报文中不含62域。

b) POS主动更新流程：

POS也可以自行发起公钥下载交易，取1中描述的第三步、第四步、第五步和第六步。唯一不同的是，在第三步中，POS终端是自动发送认证中心公钥信息查询报文，而并不是等待POS中心通知其发送。

第二部分：其它参数

下面描述其它参数的下载流程。

IC卡除了需要用到公钥信息以外，还需要使用其它的参数信息。这些参数信息见下表：

1. IC卡其他参数

| 参数名称 | 参数属性 | 参数长度（byte） | 参数tag值 | 参数含义 | 参数下载时间 | 参数适用场合 |
| --- | --- | --- | --- | --- | --- | --- |
| AID | b | 5－16 | 9F06 | 终端支持的借贷记应用列表，如ISO/IEC 7816-5所述，指明应用 | 安装或调整时 | 交易应用 |
| 应用选择指示符（ASI） | b | 1 | DF01 | 指示应用选择时终端上的AID与卡片中的AID是完全匹配（长度和内容都必须一样），还是部分匹配（卡片AID的前面部分与终端AID相同，长度可以更长）。终端支持的应用列表中的每个AID仅有一个应用选择指示符。 | 安装或调整时 | 交易应用 |
| 应用版本号 | b | 2 | 9F08 | 支付系统给应用分配的版本号 | 安装或调整时 | 交易应用 |
| TAC－缺省 | b | 5 | DF11 | 标识如果交易可以联机完成但终端没有联机交易能力时，拒绝交易的收单行条件 | 安装或调整时 | 交易应用 |
| TAC－联机 | b | 5 | DF12 | 标识联机交易的收单行条件 | 安装或调整时 | 交易应用 |
| TAC－拒绝 | b | 5 | DF13 | 标识不作联机尝试即拒绝交易的收单行条件 | 安装或调整时 | 交易应用 |
| 终端最低限额 | b | 4 | 9F1B | IC卡消费时终端允许的最低脱机限额 | 安装或调整时 | 交易应用 |
| 偏置随机选择的阈值 | b | 4 | DF15 | 在终端风险管理中用于随机交易选择的值 | 安装或调整时 | 交易应用 |
| 偏置随机选择的最大目标百分数 | cn（包含两位有效数字） | 1 | DF16 | 用于偏置随机选择的最大目标百分数 | 安装或调整时 | 交易应用 |
| 随机选择的目标百分数 | cn（包含两位有效数字） | 1 | DF17 | 用于随机选择的目标百分数 | 安装或调整时 | 交易应用 |
| 缺省DDOL | b | 变长 | DF14 | 卡片中无DDOL时用于构造内部认证命令的DDOL | 安装或调整时 | 交易应用 |
| 终端联机PIN支持能力 | b | 1 | DF18 | 指示终端在每个AID的要求下是否支持联机PIN的输入。 | 安装或调整时 | 交易应用  当值为00000001时表示支持联机PIN。当值为00000000时表示不支持联机PIN。 |

下面描述参数下载流程。参数下载可以区分为两个流程：一是POSP统一更新流程，一是POS主动更新流程。

a) POSP统一更新流程：

第一步：从POSP控制台给所有需更新参数信息的终端置更新参数信息标志；

第二步：对于每台终端，不论其上送何种交易，只要POSP认为该终端需要更新参数信息，即在POSP反馈给POS终端的应答报文头的“处理要求”字段中填入“5”；

第三步：POS终端接收到报文头“处理要求”字段填“5”报文后，立即自动上送POS参数查询报文，报文格式如12.4.9POS状态上送。其中网络管理码和62域的具体取值请参见该报文格式中的说明。POSP收到终端的请求报文后，在应答报文中将该终端需要支持的AID应用列表发送给终端。

第四步：终端收到应用列表后，首先与自己存储的应用列表进行比较。如果是终端有而POSP反馈中没有的AID，终端需要在本机将其删除；如果是终端有且POSP反馈中也有，或者是终端没有而POSP反馈中有的，终端需要全部重新下载该类AID的参数信息。该功能通过POS参数传递报文实现。POS终端需要在请求报文62域中填写AID标识（直接填写AID取值即可），POSP在应答报文中将该AID的所有参数信息返回给终端。若POSP返回了多组AID参数，那么终端需要反复发送POS参数传递报文，直到所有AID参数都下载完成。需要注意的是，所有AID类参数可能无法全部储存在一个报文中，因此需要分次传送，那么所有参数都以组为单位，不能将一组内的参数分别放在两个报文中传递。报文格式如12.4.7POS参数传递一节。网络管理码60.3域和62域用法四第二部分的具体取值请参见12.4.7。

第四步：POS下载结束后，发送下载结束报文。具体报文格式请参见12.4.10节。网络管理码60.3域也请参见12.4.10节。该报文中不含62域。

b) POS主动更新流程：

POS也可以自行发起参数下载交易，取a中描述的第三步、第四步、第五步和第六步。唯一不同的是，在第三步中，POS终端是自动发送参数信息查询报文，而并不是等待POS中心通知其发送。

需要注意的是对于终端本身无任何AID参数信息的新装终端，修复后的终端等情况，在执行交易之前，必须首先强制该类终端发起主动更新AID参数的流程。

* + - * 1. 用法五：基于PBOC电子钱包标准的圈存确认明细

变量属性

ANS...53(LLLVAR)，3个字节的长度值＋最大53个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大53个字节的数据。

用法

批上送消息中存放基于PBOC电子钱包/存折标准的圈存交易的圈存确认明细。

* 数据元长度 N3
* 用法标识及交易笔数 N2
* 第一位取值5表示基于PBOC电子钱包/存折标准的圈存交易的圈存确认明细
* 第二位表示交易笔数，最大值为1
* 交易明细 ANS51

该离线交易的种类仅为消费和取现，其中交易明细的具体格式如下：

1. 基于PBOC电子钱包/存折标准的圈存交易的圈存确认交易明细格式

| 字节位置 | 长度(字节) | 格式 | 内容 | 说明 |
| --- | --- | --- | --- | --- |
| 0 | 8 | CN | 发卡方标识 |  |
| 8 | 10 | CN | 卡片应用序列号 |  |
| 18 | 4 | B | 伪随机数 |  |
| 22 | 1 | CN | 密钥索引号 |  |
| 23 | 1 | B | 密钥版本号 |  |
| 24 | 4 | B | TAC |  |
| 28 | 3 | B | 钱包余额 |  |
| 31 | 2 | B | 钱包联机交易序号 |  |
| 33 | 4 | B | 交易金额 |  |
| 37 | 1 | CN | 交易类型标识 |  |
| 38 | 6 | CN | 终端机编号 |  |
| 44 | 4 | CN | 主机交易日期 | 格式：CCYYMMDD |
| 48 | 3 | CN | 主机交易时间 | 格式：HHMMSS |

* + - * 1. 用法六：基于PBOC借/贷记标准的交易明细

变量属性

ANS...21(LLLVAR)，3个字节的长度值＋最大21个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大21个字节的数据。

批上送消息中存放基于PBOC借/贷记标准交易的明细信息。

* 数据元长度 N3
* 用法标识及交易笔数 N2
* 第一位取值6表示基于PBOC借/贷记标准的交易明细
* 第二位表示交易笔数，最大值为1
* 交易明细 ANS19

其中交易明细的具体格式如下：

1. 基于PBOC借/贷记标准的交易明细格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字节位置 | 长度（字节） | 格式 | 内容 | 说明 |
| 0 | 2 | n | 卡类别 | 数字域，取值如下：  00：内卡交易  01：外卡交易 |
| 2 | 2 | n | 交易响应码 | 数字域；  联机交易时填写，取值为：00； |
| 4 | 12 | n | 授权金额 | 数字域，由终端传送上来，若无法传送，该域以零填充；12位有效数字，具体小数位数由授权币种决定 |
| 16 | 3 | n | 授权币种 | 3位有效数字，指授权时所用的交易币种；若无法填写，该域以零填充 |

* + - * 1. 用法七：基于PBOC借/贷记标准的通知明细

变量属性

ANS...23(LLLVAR)，3个字节的长度值＋最大23个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大23个字节的数据。

用法

批上送消息中存放基于PBOC借/贷记标准交易的通知明细，该通知明细包含两类信息：

a) 离线交易失败时，用以通知发卡行该笔离线交易中的PBOC借/贷记特征信息；

b) IC卡卡片认证ARPC错但仍然同意该交易时，用于通知发卡行该笔脱机交易中的PBOC借/贷记特征信息。

* 数据元长度 N3
* 用法标识及交易笔数 N2
* 第一位取值7表示基于PBOC借/贷记标准的通知明细
* 第二位表示交易笔数，最大值为1
* 交易明细 ANS21

其中交易明细的具体格式如下：

1. 基于PBOC借/贷记标准的通知明细格式

| 字节位置 | 长度（byte） | 格式 | 内容 | 说明 |
| --- | --- | --- | --- | --- |
| 0 | 2 | n | 卡类别 | 数字域  取值如下：  00：内卡交易  01：外卡交易 |
| 2 | 2 | n | 交易响应码 | 当应用密文类型为1时，取值为：  11：脱机交易失败（对应联网联合技术规范V2.0版应答码的Z1）  13：不能联机，脱机交易失败（对应联网联合技术规范V2.0版应答码的Z3）  当应用密文类型为2时，取值为：  05：表示IC卡卡片认证ARPC错但仍然同意该交易的应答 |
| 4 | 12 | n | 授权金额 | 数字域，由终端传送上来，若无法传送，该域以零填充；12位有效数字，具体小数位数由授权币种决定 |
| 16 | 3 | n | 授权币种 | 3位有效数字，指授权时所用的交易币种；若无法填写，该域以零填充 |
| 19 | 1 | n | 应用密文类型 | 取值为：  1：AAC，表示脱机交易拒绝时产生的应用认证密文  2：ARPC，仅表示IC卡卡片认证ARPC错但仍然同意该交易的情况 |
| 20 | 1 | n | 卡片认证ARPC的结果 | 当应用密文类型为2时，取值为：  2：失败  当应用密文类型取值为1时（即脱机交易时），该域以零填充 |

* + - * 1. 用法二十一：非接参数

变量属性

ANS...512(LLLVAR)，3个字节的长度值＋最大160个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大160个字节的数据。

域描述

参数下载时存放参数信息。ascii：6位tag+3位长度+数据

例:FF805D0010FF803A003010FF803C003060FF8058012000000030000FF80540011FF80550011FF80560010FF80570011FF8059012000000030000FF805A0011

参数表

| tag | 含义 | 长度 | 取值 | 默认值 |
| --- | --- | --- | --- | --- |
| FF805D | 非接交易通道开关 | N1 | 0-非接联机优先，1-电子现金优先 | 0 |
| FF803A | 闪卡当笔处理时间 | N3 | 10s | 10s |
| FF803C | 闪卡全处理时间 | N3 | 60s | 60s |
| FF8054 | 非接小额免密开关 | N1 | 0-关闭,1 开启 | 1 |
| FF8058 | 非接小额免密限额 | N12 | 300元 | 300元 |
| FF8055 | bin 表 A | N1 | 0-关闭,1 开启 | 0 |
| FF8056 | bin 表 B | N1 | 0-关闭,1 开启 | 1 |
| FF8057 | CDCVM标识 | N1 | 0-关闭,1 开启 | 1 |
| FF805A | 小额免签开关 | N1 | 0-关闭,1 开启 | 1 |
| FF8059 | 免签限额 | N12 | 300元 | 300元 |

* + - * 1. 用法二十二：免密新增bin表

变量属性

ANS...512(LLLVAR)，3个字节的长度值＋最大160个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大160个字节的数据。

域描述

卡BIN下载请求格式

| 位置序号 | 含义 | 长度 |
| --- | --- | --- |
| 1 | 卡BIN起始号 | N3，必须出现，首次请求时填写000（申请第一条卡BIN），后续如需再请求时将上一次收到的“卡BIN结束号＋1”填入 |

卡BIN下载应答格式

| 位置序号 | 含义 | 长度 |
| --- | --- | --- |
| 1 | 标志位 | N1，只在应答时必须出现，0表示无卡BIN可更新，1表示无后续卡BIN下载，2表示有后续卡BIN下载 |
| 2 | 报文中卡BIN结束号 | N3，必须出现，填入最后一条卡BIN的编号； |
| 3 | 卡BIN1 | N12，12字节2位卡号长度+卡BIN信息(不足位补空格)  例:196230742 1962926033 196223091100 |
| 4 | 卡BIN2 | N12，12字节2位卡号长度+卡BIN信息(不足位补空格) |
| 5 | 卡BIN3 | N12，12字节2位卡号长度+卡BIN信息(不足位补空格) |
| 6 | …… | …… |

* + - * 1. 用法二十三：免密卡bin黑名单

变量属性

ANS...512(LLLVAR)，3个字节的长度值＋最大512个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大512个字节的数据。

卡BIN黑名单下载请求格式

| 位置序号 | 含义 | 长度 |
| --- | --- | --- |
| 1 | 卡BIN起始号 | N3，必须出现，首次请求时填写000（申请第一条卡BIN），后续如需再请求时将上一次收到的“卡BIN结束号＋1”填入 |

卡BIN黑名单下载应答格式

| 位置序号 | 含义 | 长度 |
| --- | --- | --- |
| 1 | 标志位 | N1，只在应答时必须出现，0表示无卡BIN黑名单可更新（即空表）；1表示无后续卡BIN黑名单下载，2表示有后续卡BIN黑名单下载 |
| 2 | 报文中卡BIN结束号 | N3，必须出现，填入最后一条卡BIN黑名单的编号（空表时该值填写位0） |
| 3 | 卡BIN1 | N12，12字节2位卡号长度+卡BIN信息(不足位补空格) |
| 4 | 卡BIN2 | N12，12字节2位卡号长度+卡BIN信息(不足位补空格) |
| 5 | 卡BIN3 | N12，12字节2位卡号长度+卡BIN信息(不足位补空格) |
| 6 | …… | …… |

* + - * 1. 用法二十四：持卡人身份认证信息

| 证件类别 | 证件编号 | 预留手机号 | 姓名 |
| --- | --- | --- | --- |
| n2 | an18 | n11 | ans30 |

其中证件类别取值如下：

01：身份证；

02：军官证；

03：护照；

04: 回乡证；

05: 台胞证；

06: 警官证；

07: 士兵证；

99: 其它证件

证件编号左对齐，不足18位后补空格。

* + - 1. 域63

自定义域(Reserved Private)

* + - * 1. 变量属性

ANS...163(LLLVAR)，3个字节的长度值＋最大123个字节的数据。

压缩时用右靠BCD码表示的2个字节的长度值＋用ASCII码表示的最大123个字节的数据。

* + - * 1. 域描述

该域为自定义域，划分成两个子域，格式定义如下：

* 数据元长度 N3
* 63.1 自定义域1 AN3
* 63.2 自定义域2 ANS…120（LLLVAR）
  + - * 1. 63.1自定义域1

用法一：国际信用卡公司代码

交易响应消息中POS中心返回国际信用卡公司代码；POS上送的通知消息和离线交易，需上送国际信用卡公司代码。国际信用卡公司代码为：

1. 63.1域用法一

| 国际信用卡公司中文 | 国际信用卡公司英文 | 3 位代码 |
| --- | --- | --- |
| 人民币卡 | China Union Pay | CUP |
| 威士卡 | VISA | VIS |
| 万事达卡 | Master Card | MCC |
| 万事达卡 | Maestro Card | MAE |
| JCB卡 | JCB | JCB |
| 大来卡 | Dinner Club | DCC |
| 运通卡 | American Express | AMX |

用法二：操作员代码

表示POS终端操作员代码，用作在POS签到和批结算交易中上送到POS中心，应答时原路返回。

* + - * 1. 63.2 自定义域2

该域为一变长域，长度值由右靠的BCD码表示，最大到120个字节。

该域由四个子域构成，具体描述如下：

* 63.2.1 发卡方保留域 ANS…20（LLVAR）
* 63.2.2 中国银联保留域 ANS…20（LLVAR）
* 63.2.3 受理机构保留域 ANS…20（LLVAR）
* 63.3.4 POS终端保留域 ANS…60（LLVAR）

上述四个子域顺序排列，若后续子域出现而前面子域没有取值，那么前面子域以空格填充。

63.2.1 发卡方保留域

用于交易的响应消息中。由发卡方填写，用于传送交易的一些特殊信息（可用于增值业务）。例如用于发卡方对承兑交易的中奖信息、持卡人的积分信息，商品信息，或发卡方需要告知持卡人的一些信息等。若该域不为空，需打印在签购单的备注栏中。

63.2.2 中国银联保留域

用于在交易响应消息中存放中国银联返回的一些特殊信息（例如处理中心的中奖信息，商品信息等），如不为空，需打印在签购单的备注栏中。

63.2.3 受理机构保留域

用于在交易响应消息中存放商户收单行（商户结算行）返回的信息，如不为空，需打印在签购单的备注栏中。

63.2.4 POS终端保留域

用于POS终端传送的一些特殊交易信息。

* + - 1. 域64

报文鉴别码(Message Authentication Code)

* + - * 1. 变量属性

B64，8个字节的定长域。

* + - * 1. 域描述

报文来源正确性鉴别码。

* + - * 1. 用法

报文来源正确性鉴别码是对消息中的某些敏感域的数据计算MAC值。当交易消息被发送者发出之前，应由发送者产生MAC；接收者收到消息后，将重新计算MAC值，以鉴别消息在传送途中是否被篡改。

计算MAC的算法参见“数据安全传输接口”。

* 1. POS终端消息交换说明
     1. 消息格式说明
        1. 消息格式

POS终端上送POS中心的消息报文结构包括TPDU、报文头和应用数据三部分：

1. 报文结构

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TPDU | | | 报文头 | | | | | 应用数据 |
| ISO8583 Msg |
| ID | 目的  地址 | 源地址 | 应用类别定义 | 软件  版本号 | 终端  状态 | 处理  要求 | 保留  使用 | 交易数据 |
| 60H | NN NN | NN NN | N2 | N2 | N1 | N1 | **N6** | 不定长度 |

* TPDU说明：长度为5个字节。
* 报文头说明：总长度为12字节，压缩时用BCD码表示为6个字节长度的数值。

在POS上送的请求/通知报文中，该数值由POS终端应用程序在打包上送时根据POS终端参数和当前状态填入应用类别、软件版本号和终端状态，用于POS中心根据数值进行相应的处理。

在POS中心返回的响应报文中，由POS中心填入处理要求，其他域保持原值返回，POS将根据收到报文头中的处理要求进行相应处理。

报文头取值如下：

* 应用类别定义：

目前只定义

磁条卡金融支付类应用为：60

IC卡金融支付类应用为： 61

磁条卡增值业务类支付为：62

IC卡增值业务类支付为： 63

* 软件版本号：

1. 软件版本号

| 软件版本号 | 说 明 |
| --- | --- |
| 10 | 畅捷支付POS终端规范2014 |
| 20 | 畅捷支付POS终端规范2016 |

* 终端状态：

1. 终端状态

|  |  |
| --- | --- |
| 终端状态 | 含义 |
| 0 | 正常交易状态 |
| 1 | 测试交易状态 |

* 处理要求：所有管理类交易必须判断是否有处理要求

1. 处理要求

|  |  |
| --- | --- |
| 处理要求编码 | 处理要求说明 |
| 0 | 无处理要求 |
| 1 | 下传终端磁条卡参数 |
| 2 | 上传终端磁条卡状态信息 |
| 3 | 重新签到 |
| 4 | 通知终端发起更新公钥信息操作 |
| 5 | 下载终端IC卡参数 |
| 6 | TMS参数下载 |
| 7 | 卡BIN黑名单下载 |
| 8 | 币种汇率下载（仅在境外使用）/助弄取款手续费比率下载（仅在境内使用） |
| 9 | 非接业务参数下载 |
| b | 免密新增bin表更新下载 |
| c | 免密卡bin黑名单更新下载 |

* 保留使用：暂时不用，填全“0”

应用数据说明：符合ISO 8583金融交换信息格式的交易数据，本文档将定义各种交易的报文格式。

* + - 1. 符号定义
* M 强制域(Mandatory)，此域在该消息中必须出现否则将被认为消息格式出错。
* C 条件域(Conditional)，此域在一定条件下出现在该消息中，具体的条件请参考备注说明。
* O 选用域(Optional)，此域在该消息中由发送方自选。。
* Space 此域在该种消息中不出现。
* A 字母a－z
* n 数字0－9
* s 特殊字符
* an 字母和数字字符
* ans 字母、数字和特殊字符
* MM 月
* DD 日
* YY 年
* hh 小时
* mm 分
* ss 秒
* LL 允许的最大长度为99
* LLL 允许的最大长度为999
* VAR 可变长度域
* b 数据的二进制表示，后跟数字表示位（bit）的个数
* B 用于表示变长的二进制数，后跟数字表示二进制数据所占字节（Byte）的个数
* z 按GB/T 15120和GB/T 17552的2、3磁道编码
* cn BCD压缩编码数值
  + 1. 交易类
       1. 余额查询

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 当22域指明非磁条输入且可判卡号，手机芯片交易该域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 310000 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | POS终端交易流水号 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C1 | C2 | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  |  |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 00 |
| 26 | 服务点PIN获取码 | n2 |  | BCD | C |  | 当22域指明PIN可输入且持卡人输入了PIN |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 35 | 2磁道数据 | z..37 | LLVAR | BCD | C |  | 22域磁条输入且存在二磁道信息 |
| 36 | 3磁道数据 | z…104 | LLLVAR | BCD | C |  | 22域磁条输入且存在三磁道信息 |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | 收单系统流水号 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | POS终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | ans..25 | LLVAR | ASCII |  | M | 接收/收单机构 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 52 | 个人标识码数据 | b64 |  | BINARY | C |  | 交易有PIN时必选； |
| 53 | 安全控制信息 | n16 |  | BCD | C | C | 有安全要求时必选 |
| 54 | 附加金额 | an…020 | LLLVAR | ASCII |  | C | 39域为“00”时必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 以下子域中的M仅当该交易为IC卡交易时有效，M2仅当交易为手机芯片交易时有效 |
| 9F26（tag） | 应用密文 | b64 |  | BINARY | M |  |  |
| 9F27（tag） | 应用信息数据 | b8 |  | BINARY | M |  |  |
| 9F10（tag） | 发卡行应用数据 | b…256 | VAR | BINARY | M |  |  |
| 9F37（tag） | 不可预知数 | b32 |  | BINARY | M |  |  |
| 9F36（tag） | 应用交易计数器 | b16 |  | BINARY | M | C | C：若处理中心返回应答，则在响应中出现，并与请求中的内容一致 |
| 95（tag） | 终端验证结果 | b40 |  | BINARY | M |  |  |
| 9A（tag） | 交易日期 | n6 |  | BCD | M |  |  |
| 9C（tag） | 交易类型 | n2 |  | BCD | M |  |  |
| 9F02（tag） | 授权金额 | n12 |  | BCD | M |  |  |
| 5F2A（tag） | 交易货币代码 | n3 |  | BCD | M |  |  |
| 82（tag） | 应用交互特征 | b16 |  | BINARY | M |  |  |
| 9F1A（tag） | 终端国家代码 | n3 |  | BCD | M |  |  |
| 9F03（tag） | 其他金额 | n12 |  | BCD | M |  |  |
| 9F33（tag） | 终端性能 | b24 |  | BINARY | M |  |  |
| 9F34（tag） | 持卡人验证结果 | b24 |  | BINARY | O |  |  |
| 9F35（tag） | 终端类型 | n2 |  | BCD | O |  |  |
| 9F1E（tag） | 接口设备序列号 | an8 |  | ASCII | C |  | 如果终端标识不能隐含确定接口设备序列号，则出现 |
| 84（tag） | 专用文件名称 | b…128 | VAR | BINARY | O |  |  |
| 9F09（tag） | 应用版本号 | b16 |  | BINARY | O |  |  |
| 9F41（tag） | 交易序列计数器 | n…4 | VAR | BCD | O |  |  |
| 9F63 | 卡产品标识 | b128 |  | BINARY | C |  | 当终端能够获取卡标识信息时，本域出现；否则，本域不出现 |
| 91（tag） | 发卡行认证数据 | b…128 | VAR | BINARY |  | C | 若处理中心返回应答，则在响应中出现 |
| 71（tag） | 发卡行脚本1 | b…1024 | VAR | BINARY |  | C | 若处理中心返回应答，则在响应中出现 |
| 72（tag） | 发卡行脚本2 | b…1024 | VAR | BINARY |  | C | 若处理中心返回应答，则在响应中出现 |
| DF32（tag） | 芯片序列号 | B8…32s |  | BINARY | M2 |  |  |
| DF33（tag） | 过程密钥数据 | B8…32 |  | BINARY | M2 |  |  |
| DF34（tag） | 终端读取时间 | N14 |  | BCD | M2 |  |  |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M |  |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 62 | 自定义域 | ans…22 | LLLVAR | ASC | C |  | 当需要携带持卡人身份认证信息时该域出现并选用用法四。 |
| 63 | 自定义域 | ans…003 | LLLVAR | ASCII | M | M |  |
| 63.1 | 国际信用卡公司代码 | an3 |  | ASCII |  | M | 应答时填写国际信用卡公司代码； |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | B64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + - 1. 订单查询

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 311000 |
| 6 | 订单号 | Ans..30 | LLVAR | ASCII | C | C | 订单消费必送 |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 37 | 检索参考号 | An12 |  | ASCII |  | M | 收单处理平台系统流水号 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | Ans..25 | LLVAR | ASCII |  | M | 接收/收单机构 |
| 54 | 附加金额 | An…20 | LLLVAR | ASCII |  | C | 成功应答，用法一 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 1 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 63 | 自定义域 | ans…123 | LLLVAR | ASCII | M | M |  |
| 63.1 | 操作员号 | an3 |  | ASCII | M | M | 请求时填写操作员号； |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”或“10”时必选 |

* + - 1. 消费/日结消费/订单消费

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 当22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 普通:000000  日结:280000  订单:100000 |
| 4 | 交易金额 | N12 |  | BCD | M | M |  |
| 6 | 商户订单号 | Ans..30 | LLVAR | ASCII | C | C | 订单消费必送 普通消费/日结消费交易选送 |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | N4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | N4 | YYMM | BCD | C1 | C2 | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | N3 |  | BCD | M |  |  |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C：当POS能够获得该值时存在； |
| 25 | 服务点条件码 | N2 |  | BCD | M | M | 普通消费交易填写00； |
| 26 | 服务点PIN获取码 | n2 |  | BCD | C |  | 22域指明PIN可输入且持卡人输入了PIN |
| 27 | 借贷记标识 | N1 |  | BCD |  | M | 27域指明交易卡类型（0：借记卡，1：贷记卡） |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 35 | 2磁道数据 | z..37 | LLVAR | BCD | C |  | 22域磁条输入且存在二磁道信息 |
| 36 | 3磁道数据 | z…104 | LLLVAR | BCD | C |  | 22域磁条输入且存在三磁道信息 |
| 37 | 检索参考号 | An12 |  | ASCII |  | M | 收单处理平台系统流水号 |
| 38 | 授权码 | an6 |  | ASCII |  | C | 交易承兑时由发卡行自定 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | Ans..25 | LLVAR | ASCII |  | M | 接收/收单机构 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 52 | 个人标识码数据 | B64 |  | BINARY | C |  | 对于交易有PIN输入时必选； |
| 53 | 安全控制信息 | N16 |  | BCD | C | C | 有安全要求必选 |
| 54 | 附加金额 | An…20 | LLLVAR | ASCII |  | C | 成功应答，用法一 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 以下子域中的M1仅当该交易为IC卡交易时有效，M2仅当交易为手机芯片交易时有效 |
| 9F26（tag） | 应用密文 | b64 |  | BINARY | M1 |  |  |
| 9F27（tag） | 应用信息数据 | b8 |  | BINARY | M1 |  |  |
| 9F10（tag） | 发卡行应用数据 | b…256 | VAR | BINARY | M1 |  |  |
| 9F37（tag） | 不可预知数 | b32 |  | BINARY | M1 |  |  |
| 9F36（tag） | 应用交易计数器 | b16 |  | BINARY | M1 | C1 | C：若处理中心返回应答，则在响应中出现，并与请求中的内容一致 |
| 95（tag） | 终端验证结果 | b40 |  | BINARY | M1 |  |  |
| 9A（tag） | 交易日期 | n6 |  | BCD | M1 |  |  |
| 9C（tag） | 交易类型 | n2 |  | BCD | M1 |  |  |
| 9F02（tag） | 授权金额 | n12 |  | BCD | M1 |  |  |
| 5F2A（tag） | 交易货币代码 | n3 |  | BCD | M1 |  |  |
| 82（tag） | 应用交互特征 | b16 |  | BINARY | M1 |  |  |
| 9F1A（tag） | 终端国家代码 | n3 |  | BCD | M1 |  |  |
| 9F03（tag） | 其他金额 | n12 |  | BCD | M1 |  |  |
| 9F33（tag） | 终端性能 | b24 |  | BINARY | M1 |  |  |
| 9F34（tag） | 持卡人验证结果 | b24 |  | BINARY | O1 |  |  |
| 9F35（tag） | 终端类型 | n2 |  | BCD | O1 |  |  |
| 9F1E（tag） | 接口设备序列号 | an8 |  | ASCII | C1 |  | 如果终端标识不能隐含确定接口设备序列号，则出现 |
| 84（tag） | 专用文件名称 | b…128 | VAR | BINARY | O1 |  |  |
| 9F09（tag） | 应用版本号 | b16 |  | BINARY | O1 |  |  |
| 9F41（tag） | 交易序列计数器 | n…4 | VAR | BCD | O1 |  |  |
| 9F63 | 卡产品标识 | b128 |  | BINARY | C |  | 当终端能够获取卡标识信息时，本域出现；否则，本域不出现 |
| 91（tag） | 发卡行认证数据 | b…128 | VAR | BINARY |  | C | 若处理中心返回应答，则在响应中出现 |
| 71（tag） | 发卡行脚本1 | b…1024 | VAR | BINARY |  | C | 若处理中心返回应答，则在响应中出现 |
| 72（tag） | 发卡行脚本2 | b…1024 | VAR | BINARY |  | C | 若处理中心返回应答，则在响应中出现 |
| DF32（tag） | 芯片序列号 | B8…32s |  | BINARY | M2 |  |  |
| DF33（tag） | 过程密钥数据 | B8…32 |  | BINARY | M2 |  |  |
| DF34（tag） | 终端读取时间 | N14 |  | BCD | M2 |  |  |
| 57 | 终端应用加密硬件序列号 | ans…999 | LLLVAR | ASCII | C |  | 根据银联21号文规定，20170701号之后生产的pos需上送终端应用加密硬件序列号,用法见57域说明 |
| 59 | 自定义域 | ans…100 | LLLVAR | ASCII | C | M | 请求：11-基站信息 12-sim卡id  应答：卡名称，用法二 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 22 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 62 | 自定义域 | ans…512 | LLLVAR | ASCII | C |  | 如果需要携带持卡人身份认证信息则该域出现并选用用法三。 |
| 63 | 自定义域 | ans…003 | LLLVAR | ASCII | M | M |  |
| 63.1 | 国际信用卡公司代码 | an3 |  | ASCII | M | M | 请求时填写操作员号； |
| 应答时填写国际信用卡公司代码； |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”或“10”时必选 |

* + - 1. 日结确认

在消费成功并且打印出平条后，发送此交易

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0620 | 0630 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 同原交易 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 280000 |
| 4 | 交易金额 | n12 |  | BCD | M | M | 同原消费交易应答报文 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | POS终端交易流水号 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII | M | M | 请求时为原消费交易参考号 |
| 38 | 授权标识应答码 | an6 |  | ASCII | C1 | C2 | C1：如果原始交易的应答中有授权码，则须填入原交易授权码 |
| C2：交易承兑时由发卡行自定 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 同原交易 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原交易 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 同原交易 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 原消费交易的批次号 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 原消费交易的流水号 |
| 63 | 自定义域 | ans…003 | LLLVAR | ASCII | M | M |  |
| 63.1 | 国际信用卡公司代码 | an3 |  | ASCII | M |  | 请求时填写操作员号； |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00” 或“10”时必选 |

* + - 1. 消费冲正

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0400 | 0410 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 同原交易 |
| 4 | 交易金额 | n12 |  | BCD | M | M | 同原交易请求 |
| 6 | 商户订单号 | Ans..30 | LLVAR | ASCII | C | C | 同原交易请求 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | 同原交易 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C | C | 同原请求交易 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C：当POS能够获得该值时存在；同原始交易 |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  | 同原交易 |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 同原交易 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | 收单处理平台系统流水号 |
| 38 | 授权标识应答码 | an6 |  | ASCII | C |  | C：如果原始交易的应答中有授权码，则须填入原交易授权码 |
| 39 | 应答码 | an2 |  | ASCII | M | M | 请求时为冲正原因 |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 同原交易 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原交易 |
| 44 | 附加响应数据 | ans..25 | LLVAR | ASCII |  | M | 接收/收单机构 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M | 同原交易 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 以下子域中的M仅当该交易为IC卡交易时有效，M2仅当交易为手机芯片交易时有效 |
| 95（tag） | 终端验证结果 | b40 |  | BINARY | C |  | 该交易仅由终端发起，且该交易虽然被发卡方批准但被卡片拒绝，则本域出现 |
| 9F1E(tag) | 接口设备序列号 | an8 |  | ASCII | C |  | 如果终端标识不能隐含确定接口设备序列号，则出现；同原交易 |
| 9F10(tag) | 发卡行应用数据 | b…256 | VAR | BINARY | C |  | 该交易仅由终端发起，且该交易虽然被发卡方批准但被卡片拒绝，则本域出现 |
| 9F36(tag) | 应用交易计数器 | b16 |  | BINARY | M | O | C：若处理中心返回应答，则在响应中出现，并与请求中的内容一致 |
| DF31(tag) | 发卡行脚本结果 | b…168 | VAR | BINARY | C |  | 当原始交易的应答报文中出现发卡行脚本时，本域出现 |
| DF32(tag) | 芯片序列号 | B8…32s |  | BINARY | M2 |  |  |
| DF33(tag) | 过程密钥数据 | B8…32 |  | BINARY | M2 |  |  |
| DF34(tag) | 终端读取时间 | N14 |  | BCD | M2 |  |  |
| 60 | 自定义域 | an…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 同原交易 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 62 | 自定义域 | ans…22 | LLLVAR | ASC | C |  | 如果需要携带持卡人身份认证信息则该域出现并选用用法三。 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00” 或“10”时必选 |
| * 由下列情形引发冲正：   a) POS终端在时限内未能收到收单处理平台的应答消息而引发，冲正原因码填“98”。  b) POS终端在时限内收到收单处理平台的批准应答消息，但由于POS机故障无法完成交易而引发，冲正原因码填“96”。  c) POS终端对收到收单处理平台的应答消息，验证MAC出错，冲正原因码填“A0”。  d) 其他情况，冲正原因码填“06”。 | | | | | | | |

* + - 1. 消费撤销

| **位** | **域名定义** | | | **属性** | **格式** | | | **类型** | | **请求** | | **响应** | | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | | | n4 |  | | | BCD | | 0200 | | 0210 | | MSG-TYPE-ID |
|  | 位元表 | | | b64 |  | | | BINARY | | M | | M | | BIT MAP |
| 2 | 主账号 | | | n..19 | LLVAR | | | BCD | | C | | M | | 22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | | | n6 |  | | | BCD | | M | | M | | 消费:200000  订单:210000 |
| 4 | 交易金额 | | | n12 |  | | | BCD | | M | | M | | 同原消费交易应答报文 |
| 6 | 商户订单号 | | | Ans..30 | LLVAR | | | ASCII | | C | | C | | 同原交易请求 |
| 11 | 受卡方系统跟踪号 | | | n6 |  | | | BCD | | M | | M | | POS终端交易流水号 |
| 12 | 受卡方所在地时间 | | | n6 | hhmmss | | | BCD | |  | | M | |  |
| 13 | 受卡方所在地日期 | | | n4 | MMDD | | | BCD | |  | | M | |  |
| 14 | 卡有效期 | | | n4 | YYMM | | | BCD | | C1 | | C2 | | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 15 | 清算日期 | | | n4 | MMDD | | | BCD | |  | | M | |  |
| 22 | 服务点输入方式码 | | | n3 |  | | | BCD | | M | |  | |  |
| 23 | 卡片序列号 | | | n3 |  | | | BCD | | C | | C | | C：当POS能够获得该值时存在；同原始交易 |
| 25 | 服务点条件码 | | | n2 |  | | | BCD | | M | | M | | 撤销交易填写00； |
| 26 | 服务点PIN获取码 | | | n2 |  | | | BCD | | C | |  | | 22域指明PIN可输入且持卡人输入了PIN |
| 27 | | 借贷记标识 | N1 | | |  | BCD | |  | | M | | 27域指明交易卡类型（0：借记卡，1：贷记卡） | | |
| 32 | 受理方标识码 | | | n..11 | LLVAR | | | BCD | |  | | M | |  |
| 35 | 2磁道数据 | | | z..37 | LLVAR | | | BCD | | C | |  | | 22域磁条输入且存在二磁道信息 |
| 36 | 3磁道数据 | | | z…104 | LLLVAR | | | BCD | | C | |  | | 22域磁条输入且存在三磁道信息 |
| 37 | 检索参考号 | | | an12 |  | | | ASCII | | M | | M | | 请求时为原消费交易参考号 |
| 38 | 授权标识应答码 | | | an6 |  | | | ASCII | | C1 | | C2 | | C1：如果原始交易的应答中有授权码，则须填入原交易授权码 |
| C2：交易承兑时由发卡行自定 |
| 39 | 应答码 | | | an2 |  | | | ASCII | |  | | M | |  |
| 41 | 受卡机终端标识码 | | | ans8 |  | | | ASCII | | M | | M | | 同原交易 |
| 42 | 受卡方标识码 | | | ans15 |  | | | ASCII | | M | | M | | 同原交易 |
| 44 | 附加响应数据 | | | ans..25 | LLVAR | | | ASCII | |  | | M | | 接收/收单机构 |
| 49 | 交易货币代码 | | | an3 |  | | | ASCII | | M | | M | |  |
| 52 | 个人标识码数据 | | | b64 |  | | | BINARY | | C | |  | | 对于交易有PIN输入时必选； |
| 53 | 安全控制信息 | | | n16 |  | | | BCD | | C | | C | | 有安全要求必选 |
| 55 | IC卡数据域 | | | 最大255字节数据 | LLLVAR | | | 包含多个子域 | |  | |  | | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | | | B8…32s |  | | | BINARY | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | | | B8…32 |  | | | BINARY | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | | | N14 |  | | | BCD | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| 59 | 自定义域 | | | ans…50 | LLLVAR | | | ASCII | |  | | M | | 卡名称，用法二 |
| 60 | 自定义域 | | | n…011 | LLLVAR | | | BCD | | M | | M | |  |
| 60.1 | 交易类型码 | | | n2 |  | | | BCD | | M | | M | | 23 |
| 60.2 | 批次号 | | | n6 |  | | | BCD | | M | | M | |  |
| 60.3 | 网络管理码 | | | n3 |  | | | BCD | | M | | M | | 非网络管理类交易，填充缺省值000 |
| 61 | 原始信息域 | | | n…029 | LLLVAR | | | BCD | | M | |  | |  |
| 61.1 | 原批号 | | | n6 |  | | | BCD | | M | |  | | 原消费交易的批次号 |
| 61.2 | 原POS流水号 | | | n6 |  | | | BCD | | M | |  | | 原消费交易的流水号 |
| 63 | 自定义域 | | | ans…003 | LLLVAR | | | ASCII | | M | | M | |  |
| 63.1 | 国际信用卡公司代码 | | | an3 |  | | | ASCII | | M | | M | | 请求时填写操作员号； |
| 应答时填写国际信用卡公司代码； |
| 63.2 | 自定义域 | | | ans120 |  | | | ASCII | |  | | M | | 应答描述 |
| 64 | MAC | | | b64 |  | | | BINARY | | M | | C | | 响应消息中39域为“00” 或“10”时必选 |

* + - 1. 消费撤销冲正

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0400 | 0410 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 同原交易 |
| 4 | 交易金额 | n12 |  | BCD | M | M | 同原交易请求消息 |
| 6 | 商户订单号 | Ans..30 | LLVAR | ASCII | C | C | 同原交易请求 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | 同原交易 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C | C | 同原请求交易 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  | 原输入方式 |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C：当POS能够获得该值时存在；同原始交易 |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 同原交易 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | 收单处理平台系统流水号 |
| 38 | 授权标识应答码 | an6 |  | ASCII | C |  | 如果原始交易的应答中有授权码，则须填入原交易授权码 |
| 39 | 应答码 | an2 |  | ASCII | M | M | 请求时为冲正原因 |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 同原交易 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原交易 |
| 44 | 附加响应数据 | ans..25 | LLVAR | ASCII |  | M | 接收/收单机构 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 53 | 安全控制信息 | n16 |  | BCD | C | C | 有安全要求必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | B8…32s |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | B8…32 |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | N14 |  | BCD | C |  | 当二磁道数据或三磁道数据出现时存在 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 同原交易 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 原交易的批次号 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 原交易的流水号 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00” 或“10”时必选 |

* + - 1. 退货

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0220 | 0230 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | C | 当22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 200000 |
| 4 | 交易金额 | n12 |  | BCD | M | M |  |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C | C | C：POS能判断时存在 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  | 当该域前两位为“01”，表示“手工输入”时，受理方应拒绝此类交易 |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 00 |
| 26 | 服务点PIN获取码 | n2 |  | BCD | C |  | 22域指明PIN可输入且持卡人输入了PIN |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 35 | 2磁道数据 | z..37 | LLVAR | BCD | C |  | 22域磁条输入且存在二磁道信息 |
| 36 | 3磁道数据 | z…104 | LLLVAR | BCD | C |  | 22域磁条输入且存在三磁道信息 |
| 37 | 检索参考号 | an12 |  | ASCII | M | M | 请求时同原始交易 |
| 38 | 授权标识应答码 | an6 |  | ASCII | C1 |  | 原交易存在授权码时 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M |  |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原交易 |
| 44 | 附加响应数据 | ans..25 | LLVAR | ASCII |  | M | 接收/收单机构 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 52 | 个人标识码数据 | b64 |  | BINARY | C |  | 22域指明PIN可输入且持卡人输入了PIN时必选 |
| 53 | 安全控制信息 | n16 |  | BCD | C | C | 有安全要求必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | B8…32s |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | B8…32 |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | N14 |  | BCD | C |  | 当二磁道数据或三磁道数据出现时存在 |
| 59 | 自定义域 | ans…50 | LLLVAR | ASCII |  | M | 卡名称，用法二 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 25 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 若有，同原交易的批次号；否则填全0 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 若有，同原交易的流水号；否则填全0 |
| 61.3 | 原交易日期 | n4 |  | BCD | M |  | 原交易日期 |
| 63 | 自定义域 | ans…063 | LLLVAR | ASCII | M | M |  |
| 63.1 | 国际信用卡公司代码 | an3 |  | ASCII | M | M | 请求时填写操作员号； |
| 应答时填写国际信用卡公司代码如无，填全零； |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + - 1. 预授权

| **位** | | **域名定义** | | **属性** | | **格式** | | **类型** | | **请求** | | **响应** | | **备 注** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | 消息类型 | | n4 | |  | | BCD | | 0100 | | 0110 | | MSG-TYPE-ID | |
|  | | 位元表 | | b64 | |  | | BINARY | | M | | M | | BIT MAP | |
| 2 | | 主账号 | | n..19 | | LLVAR | | BCD | | C | | M | | 当22域指明非磁条输入且可判卡号该域必须出现 | |
| 3 | | 交易处理码 | | n6 | |  | | BCD | | M | | M | | 030000 | |
| 4 | | 交易金额 | | n12 | |  | | BCD | | M | | M | |  | |
| 6 | | 商户订单号 | | Ans..30 | | LLVAR | | ASCII | | O | | O | | 可选 | |
| 11 | | 受卡方系统跟踪号 | | n6 | |  | | BCD | | M | | M | |  | |
| 12 | | 受卡方所在地时间 | | n6 | | hhmmss | | BCD | |  | | M | |  | |
| 13 | | 受卡方所在地日期 | | n4 | | MMDD | | BCD | |  | | M | |  | |
| 14 | | 卡有效期 | | n4 | | YYMM | | BCD | | C1 | | C2 | | C1：POS能判断时存在 | |
| C2：具有有效期的卡存在 | |
| 15 | | 清算日期 | | n4 | | MMDD | | BCD | |  | | M | |  | |
| 22 | | 服务点输入方式码 | | n3 | |  | | BCD | | M | |  | |  | |
| 23 | | 卡片序列号 | | n3 | |  | | BCD | | C | | C | | C:当pos能够获得该值时存在 | |
| 25 | | 服务点条件码 | | n2 | |  | | BCD | | M | | M | | 06 | |
| 26 | | 服务点PIN获取码 | | n2 | |  | | BCD | | C | |  | | 22域指明PIN可输入且持卡人输入了PIN | |
| 27 | 借贷记标识 | | N1 | |  | | BCD | |  | | M | | 27域指明交易卡类型（0：借记卡，1：贷记卡） | |
| 32 | | 受理方标识码 | | n..11 | | LLVAR | | BCD | |  | | M | |  | |
| 35 | | 2磁道数据 | | z..37 | | LLVAR | | BCD | | C | |  | | 22域磁条输入且存在二磁道信息 | |
| 36 | | 3磁道数据 | | z…104 | | LLLVAR | | BCD | | C | |  | | 22域磁条输入且存在三磁道信息 | |
| 37 | | 检索参考号 | | an12 | |  | | ASCII | |  | | M | | 收单处理平台系统流水号 | |
| 38 | | 授权标识应答码 | | an6 | |  | | ASCII | |  | | C | | 39域为“00”时必选 | |
| 39 | | 应答码 | | an2 | |  | | ASCII | |  | | M | |  | |
| 41 | | 受卡机终端标识码 | | ans8 | |  | | ASCII | | M | | M | | 终端代码 | |
| 42 | | 受卡方标识码 | | ans15 | |  | | ASCII | | M | | M | | 商户代码 | |
| 44 | | 附加响应数据 | | ans..25 | | LLVAR | | ASCII | |  | | M | | 接收/收单机构 | |
| 49 | | 交易货币代码 | | an3 | |  | | ASCII | | M | | M | |  | |
| 52 | | 个人标识码数据 | | b64 | |  | | BINARY | | C | |  | | 对于交易有PIN输入时必选； | |
| 53 | | 安全控制信息 | | n16 | |  | | BCD | | C | | C | | 有安全要求必选 | |
| 54 | | 附加金额 | | An…20 | | LLLVAR | | ASCII | |  | | C | | 成功应答，返回余额 | |
| 55 | | IC卡数据域 | | 最大255字节数据 | | LLLVAR | | 包含多个子域 | |  | |  | | 以下子域中的M仅当该交易为IC卡交易时有效，M2仅当交易为手机芯片交易时有效 | |
| 9F26（tag） | | 应用密文 | | b64 | |  | | BINARY | | M | |  | |  | |
| 9F27（tag） | | 应用信息数据 | | b8 | |  | | BINARY | | M | |  | |  | |
| 9F10（tag） | | 发卡行应用数据 | | b…256 | | VAR | | BINARY | | M | |  | |  | |
| 9F37（tag） | | 不可预知数 | | b32 | |  | | BINARY | | M | |  | |  | |
| 9F36（tag） | | 应用交易计数器 | | b16 | |  | | BINARY | | M | | C | | C：若处理中心返回应答，则在响应中出现，并与请求中的内容一致 | |
| 95（tag） | | 终端验证结果 | | b40 | |  | | BINARY | | M | |  | |  | |
| 9A（tag） | | 交易日期 | | n6 | |  | | BCD | | M | |  | |  | |
| 9C（tag） | | 交易类型 | | n2 | |  | | BCD | | M | |  | |  | |
| 9F02（tag） | | 授权金额 | | n12 | |  | | BCD | | M | |  | |  | |
| 5F2A（tag） | | 交易货币代码 | | n3 | |  | | BCD | | M | |  | |  | |
| 82（tag） | | 应用交互特征 | | b16 | |  | | BINARY | | M | |  | |  | |
| 9F1A（tag） | | 终端国家代码 | | n3 | |  | | BCD | | M | |  | |  | |
| 9F03（tag） | | 其他金额 | | n12 | |  | | BCD | | M | |  | |  | |
| 9F33（tag） | | 终端性能 | | b24 | |  | | BINARY | | M | |  | |  | |
| 9F34（tag） | | 持卡人验证结果 | | b24 | |  | | BINARY | | O | |  | |  | |
| 9F35（tag） | | 终端类型 | | n2 | |  | | BCD | | O | |  | |  | |
| 9F1E（tag） | | 接口设备序列号 | | an8 | |  | | ASCII | | C | |  | | 如果终端标识不能隐含确定接口设备序列号，则出现 | |
| 84（tag） | | 专用文件名称 | | b…128 | | VAR | | BINARY | | O | |  | |  | |
| 9F09（tag） | | 应用版本号 | | b16 | |  | | BINARY | | O | |  | |  | |
| 9F41（tag） | | 交易序列计数器 | | n…4 | | VAR | | BCD | | O | |  | |  | |
| 9F63 | | 卡产品标识 | | b128 | |  | | BINARY | | C | |  | | 当终端能够获取卡标识信息时，本域出现；否则，本域不出现 | |
| 91（tag） | | 发卡行认证数据 | | b…128 | | VAR | | BINARY | |  | | C | | 若处理中心返回应答，则在响应中出现 | |
| 71（tag） | | 发卡行脚本1 | | b…1024 | | VAR | | BINARY | |  | | C | | 若处理中心返回应答，则在响应中出现 | |
| 72（tag） | | 发卡行脚本2 | | b…1024 | | VAR | | BINARY | |  | | C | | 若处理中心返回应答，则在响应中出现 | |
| DF32（tag） | | 芯片序列号 | | B8…32s | |  | | BINARY | | M2 | |  | |  | |
| DF33（tag） | | 过程密钥数据 | | B8…32 | |  | | BINARY | | M2 | |  | |  | |
| DF34（tag） | | 终端读取时间 | | N14 | |  | | BCD | | M2 | |  | |  | |
| 57 | | 终端应用加密硬件序列号 | | ans…999 | | LLLVAR | | ASCII | | C | |  | | 根据银联21号文规定，20170701号之后生产的pos需上送终端应用加密硬件序列号,用法见57域说明 | |
| 59 | | 自定义域 | | ans…100 | | LLLVAR | | ASCII | | C | | M | | 请求：11-基站信息 12-sim卡id  应答：卡名称，用法二 | |
| 60 | | 自定义域 | | n…011 | | LLLVAR | | BCD | | M | | M | |  | |
| 60.1 | | 交易类型码 | | n2 | |  | | BCD | | M | | M | | 10 | |
| 60.2 | | 批次号 | | n6 | |  | | BCD | | M | | M | |  | |
| 60.3 | | 网络管理码 | | n3 | |  | | BCD | | M | | M | | 非网络管理类交易，此处以缺省值000填充 | |
| 63 | | 自定义域 | | ans…003 | | LLLVAR | | ASCII | | M | | M | |  | |
| 63.1 | | 国际信用卡公司代码 | | an3 | |  | | ASCII | | M | | M | | 请求时填写操作员号； | |
| 应答时填写国际信用卡公司代码 | |
| 63.2 | | 自定义域 | | ans120 | |  | | ASCII | |  | | M | | 应答描述 | |
| 64 | | MAC | | b64 | |  | | BINARY | | M | | C | | 响应消息中39域为“00” 或“10”时必选 | |

* + - 1. 预授权冲正

| 位 | 域名定义 | 属性 | 格式 | 类型 | 请求 | 响应 | 备 注 |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0400 | 0410 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 22域指明非磁条输入且可判卡号域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 同原交易 |
| 4 | 交易金额 | n12 |  | BCD | M | M | 同原预授权交易 |
| 6 | 商户订单号 | Ans..30 | LLVAR | ASCII | O | O | 同原交易 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | 原流水号 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C | C | 同原请求交易 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  | 原输入方式 |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C:当pos能够获得该值时存在  同原始交易 |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 06 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | POS中心流水号 |
| 38 | 授权标识应答码 | an6 |  | ASCII | C |  | 如果有原始交易应答，则填入原交易授权码 |
| 39 | 应答码 | an2 |  | ASCII | M | M | 请求时为冲正原因 |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 同原交易 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原交易 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 53 | 安全控制信息 | n16 |  | BCD | C | C | 有安全要求必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 以下子域中的M仅当该交易为IC卡交易时有效，M2仅当交易为手机芯片交易时有效 |
| 95（tag） | 终端验证结果 | b40 |  | BINARY | C |  | 该交易仅由终端发起，且该交易虽然被发卡方批准但被卡片拒绝，则本域出现 |
| 9F1E(tag) | 接口设备序列号 | an8 |  | ASCII | C |  | 如果终端标识不能隐含确定接口设备序列号，则出现；同原交易 |
| 9F10(tag) | 发卡行应用数据 | b…256 | VAR | BINARY | C |  | 该交易仅由终端发起，且该交易虽然被发卡方批准但被卡片拒绝，则本域出现 |
| 9F36(tag) | 应用交易计数器 | b16 |  | BINARY | M | C | C：若处理中心返回应答，则在响应中出现，并与请求中的内容一致 |
| DF31(tag) | 发卡行脚本结果 | b…168 | VAR | BINARY | C |  | 当原始交易的应答报文中出现发卡行脚本时，本域出现 |
| DF32(tag) | 芯片序列号 | B8…32s |  | BINARY | M2 |  |  |
| DF33(tag) | 过程密钥数据 | B8…32 |  | BINARY | M2 |  |  |
| DF34(tag) | 终端读取时间 | N14 |  | BCD | M2 |  |  |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 同原交易 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 此处以缺省值000填充 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + - 1. 预授权撤销

| **位** | **域名定义** | | **属性** | **格式** | | | **类型** | | **请求** | | **响应** | | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | | n4 |  | | | BCD | | 0100 | | 0110 | | MSG-TYPE-ID |
|  | 位元表 | | b64 |  | | | BINARY | | M | | M | | BIT MAP |
| 2 | 主账号 | | n..19 | LLVAR | | | BCD | | C | | M | | 22域指明非磁条输入且可判卡号  该域必须出现 |
| 3 | 交易处理码 | | n6 |  | | | BCD | | M | | M | | 200000 |
| 4 | 交易金额 | | n12 |  | | | BCD | | M | | M | | 同原预授权交易应答报文 |
| 11 | 受卡方系统跟踪号 | | n6 |  | | | BCD | | M | | M | | POS终端交易流水号 |
| 12 | 受卡方所在地时间 | | n6 | hhmmss | | | BCD | |  | | M | |  |
| 13 | 受卡方所在地日期 | | n4 | MMDD | | | BCD | |  | | M | |  |
| 14 | 卡有效期 | | n4 | YYMM | | | BCD | | C1 | | C2 | | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 15 | 清算日期 | | n4 | MMDD | | | BCD | |  | | M | |  |
| 22 | 服务点输入方式码 | | n3 |  | | | BCD | | M | |  | |  |
| 23 | 卡片序列号 | | n3 |  | | | BCD | | C | | C | | C:当pos能够获得该值时存在  同原始交易 |
| 25 | 服务点条件码 | | n2 |  | | | BCD | | M | | M | | 06 |
| 26 | 服务点PIN获取码 | | n2 |  | | | BCD | | C | |  | | 22域指明PIN可输入且持卡人输入了PIN |
| 27 | | | 借贷记标识 | N1 | |  | BCD | |  | | M | | 27域指明交易卡类型（0：借记卡，1：贷记卡） | | |
| 32 | 受理方标识码 | | n..11 | LLVAR | | | BCD | |  | | M | |  |
| 35 | 2磁道数据 | | z..37 | LLVAR | | | BCD | | C | |  | | 22域磁条输入且存在二磁道信息 |
| 36 | 3磁道数据 | | z…104 | LLLVAR | | | BCD | | C | |  | | 22域磁条输入且存在二磁道信息 |
| 37 | 检索参考号 | | an12 |  | | | ASCII | |  | | M | | 收单处理平台流水号 |
| 38 | 授权标识应答码 | | an6 |  | | | ASCII | | M | | C | | 请求时，同原预授权（追加预授权）交易 |
| 39 | 应答码 | | an2 |  | | | ASCII | |  | | M | |  |
| 41 | 受卡机终端标识码 | | ans8 |  | | | ASCII | | M | | M | |  |
| 42 | 受卡方标识码 | | ans15 |  | | | ASCII | | M | | M | | 同原交易 |
| 44 | 附加响应数据 | | ans..25 | LLVAR | | | ASCII | |  | | M | | 接收/收单机构 |
| 49 | 交易货币代码 | | an3 |  | | | ASCII | | M | | M | |  |
| 52 | 个人标识码数据 | | b64 |  | | | BINARY | | C | |  | | 对于交易有PIN输入时必选； |
| 53 | 安全控制信息 | | n16 |  | | | BCD | | C | | C | | 有安全要求必选 |
| 55 | IC卡数据域 | | 最大255字节数据 | LLLVAR | | | 包含多个子域 | |  | |  | | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | | B8…32s |  | | | BINARY | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | | B8…32 |  | | | BINARY | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | | N14 |  | | | BCD | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| 59 | 自定义域 | | ans…50 | LLLVAR | | | ASCII | |  | | M | | 卡名称，用法二 |
| 60 | 自定义域 | | an…011 | LLLVAR | | | BCD | | M | | M | |  |
| 60.1 | 交易类型码 | | n2 |  | | | BCD | | M | | M | | 11 |
| 60.2 | 批次号 | | n6 |  | | | BCD | | M | | M | |  |
| 60.3 | 网络管理码 | | n3 |  | | | BCD | | M | | M | | 非网络管理类交易，此处以缺省值000填充 |
| 61 | 原始信息域 | | n…029 | LLLVAR | | | BCD | | M | |  | |  |
| 61.1 | 原批号 | | n6 |  | | | BCD | | M | |  | | 若有，同原交易的批次号；否则填全0 |
| 61.2 | 原POS流水号 | | n6 |  | | | BCD | | M | |  | | 若有，同原交易的流水号；否则填全0 |
| 61.3 | 原交易日期 | | n4 |  | | | BCD | | M | |  | | 原预授权交易日期，如无，填全零 |
| 63 | 自定义域 | | ans…003 | LLLVAR | | | ASCII | | M | | M | |  |
| 63.1 | 国际信用卡公司代码 | | an3 |  | | | ASCII | | M | | M | | 请求时填写操作员号； |
| 应答时填写国际信用卡公司代 |
| 63.2 | 自定义域 | | ans120 |  | | | ASCII | |  | | M | | 应答描述 |
| 64 | MAC | | b64 |  | | | BINARY | | M | | C | | 响应消息中39域为“00” 或“10”时必选 |

* + - 1. 预授权撤销冲正

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0400 | 0410 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 同原交易 |
| 4 | 交易金额 | n12 |  | BCD | M | M | 同原始交易金额4域 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | 同原交易 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C | C | 同原请求交易 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  | 原输入方式 |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C:当pos能够获得该值时存在  同原始交易 |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 06 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | 收单处理平台系统流水号 |
| 38 | 授权标识应答码 | an6 |  | ASCII | M |  | 同原交易请求； |
| 39 | 应答码 | an2 |  | ASCII | M | M | 请求时为冲正原因 |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 同原交易 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原交易 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 53 | 安全控制信息 | n16 |  | BCD | C | C | 有安全要求必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | B8…32s |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | B8…32 |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | N14 |  | BCD | C |  | 当二磁道数据或三磁道数据出现时存在 |
| 60 | 自定义域 | an…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 同原交易 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 同原交易 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 同原交易 |
| 61.3 | 原交易日期 | n4 |  | BCD | M |  | 同原交易 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00” 或“10”时必选 |

* + - 1. 预授权完成

| **位** | **域名定义** | | **属性** | | **格式** | | | **类型** | | **请求** | | **响应** | | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | | n4 | |  | | | BCD | | 0200 | | 0210 | | MSG-TYPE-ID |
|  | 位元表 | | b64 | |  | | | BINARY | | M | | M | | BIT MAP |
| 2 | 主账号 | | n..19 | | LLVAR | | | BCD | | C | | M | | 22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | | n6 | |  | | | BCD | | M | | M | | 000000 |
| 4 | 交易金额 | | n12 | |  | | | BCD | | M | | M | |  |
| 11 | 受卡方系统跟踪号 | | n6 | |  | | | BCD | | M | | M | | POS终端交易流水 |
| 12 | 受卡方所在地时间 | | n6 | | hhmmss | | | BCD | |  | | M | |  |
| 13 | 受卡方所在地日期 | | n4 | | MMDD | | | BCD | |  | | M | |  |
| 14 | 卡有效期 | | n4 | | YYMM | | | BCD | | C1 | | C2 | | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 15 | 清算日期 | | n4 | | MMDD | | | BCD | |  | | M | |  |
| 22 | 服务点输入方式码 | | n3 | |  | | | BCD | | M | |  | |  |
| 23 | 卡片序列号 | | n3 | |  | | | BCD | | C | | C | | C:当pos能够获得该值时存在 |
| 25 | 服务点条件码 | | n2 | |  | | | BCD | | M | | M | | 06 |
| 26 | 服务点PIN获取码 | | n2 | |  | | | BCD | | C | |  | | 22域指明PIN可输入且持卡人输入了PIN |
| 27 | | 借贷记标识 | | N1 | |  | BCD | |  | | M | | 27域指明交易卡类型（0：借记卡，1：贷记卡） | | |
| 32 | 受理方标识码 | | n..11 | | LLVAR | | | BCD | |  | | M | |  |
| 35 | 2磁道数据 | | z..37 | | LLVAR | | | BCD | | C | |  | | 22域磁条输入且存在二磁道信息 |
| 36 | 3磁道数据 | | z…104 | | LLLVAR | | | BCD | | C | |  | | 22域磁条输入且存在三磁道信息 |
| 37 | 检索参考号 | | an12 | |  | | | ASCII | |  | | M | | 收单处理平台流水号 |
| 38 | 授权标识应答码 | | an6 | |  | | | ASCII | | M | | C | | 请求时同原预授权交易 |
| C：发卡方有返回时填写 |
| 39 | 应答码 | | an2 | |  | | | ASCII | |  | | M | |  |
| 41 | 受卡机终端标识码 | | ans8 | |  | | | ASCII | | M | | M | | 终端代码 |
| 42 | 受卡方标识码 | | ans15 | |  | | | ASCII | | M | | M | | 商户代码 |
| 44 | 附加响应数据 | | ans..25 | | LLVAR | | | ASCII | |  | | M | | 接收/收单机构 |
| 49 | 交易货币代码 | | an3 | |  | | | ASCII | | M | | M | |  |
| 52 | 个人标识码数据 | | b64 | |  | | | BINARY | | C | |  | | 22域指明PIN可输入且持卡人输入了PIN |
| 53 | 安全控制信息 | | n16 | |  | | | BCD | | C | | C | | 有安全要求必选 |
| 54 | 附加金额 | | An…20 | | LLLVAR | | | ASCII | |  | | C | | 63.2.4.1取值为1时，且是预付费卡的成功应答 |
| 55 | IC卡数据域 | | 最大255字节数据 | | LLLVAR | | | 包含多个子域 | |  | |  | | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | | B8…32s | |  | | | BINARY | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | | B8…32 | |  | | | BINARY | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | | N14 | |  | | | BCD | | C | |  | | 当二磁道数据或三磁道数据出现时存在 |
| 59 | 自定义域 | | ans…100 | | LLLVAR | | | ASCII | | C | | M | | 请求：11-基站信息 12-sim卡id  应答：卡名称，用法二 |
| 60 | 自定义域 | | n…011 | | LLLVAR | | | BCD | | M | | M | |  |
| 60.1 | 交易类型码 | | n2 | |  | | | BCD | | M | | M | |  |
| 60.2 | 批次号 | | n6 | |  | | | BCD | | M | | M | |  |
| 60.3 | 网络管理码 | | n3 | |  | | | BCD | | M | | M | | 非网络管理类交易，此处以缺省值000填充 |
| 61 | 原始信息域 | | n…029 | | LLLVAR | | | BCD | | M | |  | |  |
| 61.1 | 原批号 | | n6 | |  | | | BCD | | M | |  | | 若有，同原交易的批次号；否则填全0 |
| 61.2 | 原POS流水号 | | n6 | |  | | | BCD | | M | |  | | 若有，同原交易的流水号；否则填全0 |
| 61.3 | 原交易日期 | | n4 | |  | | | BCD | | M | |  | | 原授权交易日期，如无，填全零 |
| 63 | 自定义域 | | ans…003 | | LLLVAR | | | ASCII | | M | | M | |  |
| 63.1 | 国际信用卡公司代码 | | an3 | |  | | | ASCII | | M | | M | | 请求时填写操作员号； |
| 应答时填写国际信用卡公司代 |
| 63.2 | 自定义域 | | ans120 | |  | | | ASCII | |  | | M | | 应答描述 |
| 64 | MAC | | b64 | |  | | | BINARY | | M | | C | | 响应消息中39域为“00”时必选 |

* + - 1. 预授权完成冲正

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0400 | 0410 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 同原交易 |
| 4 | 交易金额 | n12 |  | BCD | M | M | 同原交易请求消息中4域 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | 同原交易 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C1 | C2 | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  | 原输入方式 |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C:当pos能够获得该值时存在 |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 同原交易 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | 收单处理平台流水号 |
| 38 | 授权标识应答码 | an6 |  | ASCII | M |  | 同原交易请求 |
| 39 | 应答码 | an2 |  | ASCII | M | M | 请求时为冲正原因 |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 同原交易 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原交易 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 53 | 安全控制信息 | n16 |  | BCD | C | C | 有安全要求必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | B8…32s |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | B8…32 |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | N14 |  | BCD | C |  | 当二磁道数据或三磁道数据出现时存在 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 同原交易 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 原交易的批次号 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 原交易的流水号 |
| 61.3 | 原交易日期 | n4 |  | BCD | M |  | 原交易日期 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + - 1. 预授权完成撤销

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 200000 |
| 4 | 交易金额 | n12 |  | BCD | M | M | 同原始预授权完成（请求）交易的4域 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C1 | C2 | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  | 刷卡时填022，不刷卡时填012 |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C:当pos能够获得该值时存在 |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 06 |
| 26 | 服务点PIN获取码 | n2 |  | BCD | C |  | 22域指明PIN可输入且持卡人输入了PIN |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 35 | 2磁道数据 | z..37 | LLVAR | BCD | C |  | 22域磁条输入且存在二磁道信息 |
| 36 | 3磁道数据 | z…104 | LLLVAR | BCD | C |  | 22域磁条输入且存在二磁道信息 |
| 37 | 检索参考号 | an12 |  | ASCII | M | M | 请求时同原始预授权完成（请求）交易 |
| 38 | 授权标识应答码 | an6 |  | ASCII | C1 | C2 | C1：同原交易请求  C2：交易成功由发卡行给出 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 同原交易 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原交易 |
| 44 | 附加响应数据 | ans..25 | LLVAR | ASCII |  | M | 接收/收单机构 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 52 | 个人标识码数据 | b64 |  | BINARY | C |  | 22域指明PIN可输入且持卡人输入了PIN |
| 53 | 安全控制信息 | n16 |  | BCD | C | C | 有安全要求必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | B8…32s |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | B8…32 |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | N14 |  | BCD | C |  | 当二磁道数据或三磁道数据出现时存在 |
| 59 | 自定义域 | ans…50 | LLLVAR | ASCII |  | M | 卡名称，用法二 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M |  |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 原交易的批次号 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 原交易的流水号 |
| 61.3 | 原交易日期 | n4 |  | BCD | M |  | 原交易日期 |
| 63 | 自定义域 | ans…003 | LLLVAR | ASCII | M | M |  |
| 63.1 | 国际信用卡公司代码 | an3 |  | ASCII | M | M | 请求时填写操作员号； |
| 应答时填写国际信用卡公司代 |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + - 1. 预授权完成撤销冲正

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0400 | 0410 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 22域指明非磁条输入且可判卡号，该域必须出现 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 同原始交易 |
| 4 | 交易金额 | n12 |  | BCD | M | M | 同原始交易 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | 同原始交易 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | C1 | C2 | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | n3 |  | BCD | M |  | 原输入方式 |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C:当pos能够获得该值时存在 |
| 25 | 服务点条件码 | n2 |  | BCD | M | M | 同原始交易 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | 收单处理平台系统流水号 |
| 38 | 授权标识应答码 | an6 |  | ASCII | C |  | C：同原交易请求 |
| 39 | 应答码 | an2 |  | ASCII | M | M | 请求时为冲正原因 |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 同原始交易 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 同原始交易 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 53 | 安全控制信息 | n16 |  | BCD | C | C | 有安全要求必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 仅当交易为手机芯片交易时有效，不需上送该域 |
| DF32(tag) | 芯片序列号 | B8…32s |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF33(tag) | 过程密钥数据 | B8…32 |  | BINARY | C |  | 当二磁道数据或三磁道数据出现时存在 |
| DF34(tag) | 终端读取时间 | N14 |  | BCD | C |  | 当二磁道数据或三磁道数据出现时存在 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 同原始交易 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 原交易的批次号 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 原交易的流水号 |
| 61.3 | 原交易日期 | n4 |  | BCD | M |  | 原始交易日期 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + - 1. 基于 PBOC 借/贷记标准 IC 卡脚本处理结果通知(含小额支付应用)

当一笔交易(仅指余额查询、取现、消费、预授权、现金充值(撤销)、指定账户圈存、非指定账

户圈存)包含发卡行脚本时,受理方需要将卡片执行的脚本结果通知到发卡方。该交易随同下一笔交易 (签到除外)一并发送。若在发送下一笔交易时还存在冲正交易,那么脚本通知交易先于冲正交易发送。

表 基于 PBOC 借/贷记标准 IC 卡脚本处理结果通知报文

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0620 | 0630 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 当22域指明非磁条输入且可判卡号 |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 同执行该脚本通知交易的原始信息 |
| 4 | 交易金额 | N12 |  | BCD | C |  | 执行该脚本通知交易的原始中包 含该域信息,本域出现,对于部分 承兑消费,以应答金额为准,其余 交易,以请求金额为准;否则不出 现 |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | N4 | MMDD | BCD |  | M |  |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | N3 |  | BCD | M |  | 同原交易请求 |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C:当POS能够获得该值时存在；  同执行该脚本通知交易的原始信息 |
| 25 | 服务点条件码 | N2 |  | BCD | M | M | 同原交易请求 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M | 同执行该脚本通知交易的原始信息 |
| 37 | 检索参考号 | An12 |  | ASCII |  | M | 同包含该脚本信息的原始交易 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 以下子域中的M仅当该交易为IC卡交易时有效 |
| 9F33（tag） | 终端性能 | b24 |  | BINARY | C |  | C:在上一个关联的原始交易中出 现时,则本域出现。同原始交易 |
| 95（tag） | 终端验证结果 | b40 |  | BINARY | M |  |  |
| 9F37（tag） | 不可预知数 | b32 |  | BINARY | C |  | C:在上一个关联的原始交易中出 现时,则本域出现。同原始交易 |
| 9F1E（tag） | 接口设备序列号 | an8 |  | ASCII | C |  | C:在上一个关联的原始交易中出 现时,则本域出现。同原始交易 |
| 9F10（tag） | 发卡行应用数据 | b…256 | VAR | BINARY | M |  |  |
| 9F26（tag） | 应用密文 | b64 |  | BINARY | M |  |  |
| 9F36（tag） | 应用交易计数器 | b16 |  | BINARY | M | C | M：同原始交易  C：若处理中心返回应答，则在响应中出现，并与请求中的内容一致 |
| 82（tag） | 应用交互特征 | b16 |  | BINARY | M |  | 同原始交易 |
| DF31（tag） | 发卡行脚本结果 | b…168 | VAR | BINARY | M |  |  |
| 9F1A（tag） | 终端国家代码 | n3 |  | BCD | M |  | 同原始交易 |
| 9A（tag） | 交易日期 | n6 |  | BCD | M |  | 同原始交易 |
| 60 | 自定义域 | n…017 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 填写00 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | C | C | 951 |
| 60.4 | 终端读取能力 | n1 |  | BCD | M | M | 同原始交易 |
| 60.5 | 基于PBOC借/贷记标准的IC卡条件代码 | n1 |  | BCD | M | M | 同原始交易 |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 原交易的批次号 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 原交易的流水号 |
| 61.3 | 原交易日期 | n4 |  | BCD | M |  | 原始交易日期 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + 1. 二维码类
       1. 被扫支付

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 700000 |
| 4 | 交易金额 | N12 |  | BCD | M | M |  |
| 5 | url | ans…100 | LLLVAR | ASCII |  | M |  |
| 6 | 二维码订单号 | Ans..30 | LLVAR | ASCII |  | M |  |
| 7 | 商户订单号 | Ans..30 | LLVAR | ASCII | O | O | 可选 |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | N4 | MMDD | BCD |  | M |  |
| 14 | 订单有效期 | N4 |  | BCD | C | M | 单位分钟 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M | 平台分配标识 |
| 37 | 检索参考号 | An12 |  | ASCII |  | M |  |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | Ans..25 | LLVAR | ASCII | M | M | 002:微信  003:支付宝  004:银联 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 58 | 订单标题 | ans…256 | LLLVAR | ASCII | C |  |  |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 60 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 62 | 订单描述 | ans…512 | LLLVAR | ASCII | O |  |  |
| 63 | 自定义域 | ans…120 | LLLVAR | ASCII | M | M |  |
| 63.1 | 操作员号 | an3 |  | ASCII | M | M |  |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”或“10”时必选 |

* + - 1. 主扫支付

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 710000 |
| 4 | 交易金额 | N12 |  | BCD | M | M |  |
| 5 | url | ans…100 | LLLVAR | ASCII | O |  | 银联支付时上送C2B码 |
| 6 | 二维码订单号 | Ans..30 | LLVAR | ASCII |  | M |  |
| 7 | 商户订单号 | Ans..30 | LLVAR | ASCII | O | O | 可选 |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | N4 | MMDD | BCD |  | M |  |
| 14 | 订单有效期 | N4 |  | BCD | C | M | 单位分钟 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M | 平台分配标识 |
| 37 | 检索参考号 | An12 |  | ASCII |  | M |  |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | Ans..25 | LLVAR | ASCII | M | M | 002:微信  003:支付宝  004:银联 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 58 | 订单标题 | ans…256 | LLLVAR | ASCII | O |  |  |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 60 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 62 | 订单描述 | ans…512 | LLLVAR | ASCII | O |  |  |
| 63 | 自定义域 | ans…120 | LLLVAR | ASCII | M | M |  |
| 63.1 | 操作员号 | an3 |  | ASCII | M | M |  |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”或“10”时必选 |

* + - 1. 二维码消费查询(查询支付是否成功)

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 730000 |
| 4 | 交易金额 | N12 |  | BCD |  | M | 成功金额 |
| 6 | 二维码订单号 | Ans..30 | LLVAR | ASCII | M | M |  |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | N4 | MMDD | BCD |  | M |  |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M | 平台分配标识 |
| 37 | 检索参考号 | An12 |  | ASCII |  | M |  |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | Ans..25 | LLVAR | ASCII | M | M | 002:微信  003:支付宝  004:银联 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 60 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 63 | 自定义域 | ans…120 | LLLVAR | ASCII | M | M |  |
| 63.1 | 操作员号 | an3 |  | ASCII | M | M |  |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”或“10”时必选 |

* + - 1. 二维码支付撤销

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 720000 |
| 4 | 交易金额 | N12 |  | BCD | M | M |  |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | N4 | MMDD | BCD |  | M |  |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M | 平台分配标识 |
| 37 | 检索参考号 | An12 |  | ASCII | M | M | 请求时同原交易 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | Ans..25 | LLVAR | ASCII | M | M | 002:微信  003:支付宝  004:银联 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 原消费交易的批次号 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 原消费交易的流水号 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 60 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 63 | 自定义域 | ans…120 | LLLVAR | ASCII | M | M |  |
| 63.1 | 操作员号 | an3 |  | ASCII | M | M |  |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”或“10”时必选 |

* + - 1. 二维码支付退货

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 740000 |
| 4 | 交易金额 | N12 |  | BCD | M | M |  |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | N4 | MMDD | BCD |  | M |  |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M | 平台分配标识 |
| 37 | 检索参考号 | An12 |  | ASCII | M | M | 请求时同原交易 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | Ans..25 | LLVAR | ASCII |  | M | 002:微信  003:支付宝  004:银联 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 61 | 原始信息域 | n…029 | LLLVAR | BCD | M |  |  |
| 61.1 | 原批号 | n6 |  | BCD | M |  | 若有，同原交易的批次号；否则填全0 |
| 61.2 | 原POS流水号 | n6 |  | BCD | M |  | 若有，同原交易的流水号；否则填全0 |
| 61.3 | 原交易日期 | n4 |  | BCD | M |  | 原交易日期 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 60 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，填充缺省值000 |
| 63 | 自定义域 | ans…120 | LLLVAR | ASCII | M | M |  |
| 63.1 | 操作员号 | an3 |  | ASCII | M | M |  |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”或“10”时必选 |

* + 1. 离线类
       1. 基于PBOC借/贷记标准的IC卡离线交易（含小额支付应用）

基于PBOC借/贷记标准的IC卡离线交易（含小额支付应用）仅包含消费。对于小额支付应用的IC卡离线交易报文且可以获取时，55域的tag“9F74”必须出现，35、36域不必上送。报文格式如下：

表 基于PBOC借/贷记标准的IC卡离线消费报文（含小额支付应用）

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 当22域指明非磁条输入且可判卡号 |
| 3 | 交易处理码 | N6 |  | BCD | M | M | 000000 |
| 4 | 交易金额 | N12 |  | BCD | M | M |  |
| 7 | 商户订单号 | Ans..30 | LLVAR | ASCII | O | O | 可选 |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | N6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | N4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | N4 | YYMM | BCD | C1 | C2 | C1：POS能判断时存在 |
| C2：具有有效期的卡存在 |
| 15 | 清算日期 | n4 | MMDD | BCD |  | M |  |
| 22 | 服务点输入方式码 | N3 |  | BCD | M |  |  |
| 23 | 卡片序列号 | n3 |  | BCD | C | C | C:当POS能够获得该值时存在； |
| 25 | 服务点条件码 | N2 |  | BCD | M | M | 00 |
| 26 | 服务点PIN获取码 | n2 |  | BCD | C |  | 22域指明PIN可输入且持卡人输入了PIN |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 35 | 2磁道数据 | z..37 | LLVAR | BCD | C |  | 22域 磁条输入且存在二磁道数据 |
| 36 | 3磁道数据 | z..104 | LLLVAR | BCD | C |  | 22域 磁条输入且存在三磁道数据 |
| 37 | 检索参考号 | An12 |  | ASCII |  | M | POS中心系统流水号 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 44 | 附加响应数据 | Ans..25 | LLVAR | ASCII |  | M | 接收/收单机构 |
| 49 | 交易货币代码 | an3 |  | ASCII | M | M |  |
| 52 | 个人标识码数据 | B64 |  | BINARY | C |  | 对于磁条卡交易有PIN输入时必选；对于基于PBOC借/贷记标准的IC卡交易，当使用脱机密码验证时，该域不出现；当使用联机密码验证时，该域出现 |
| 53 | 安全控制信息 | N16 |  | BCD | C | C | 有安全要求或磁条信息出现时必选 |
| 55 | IC卡数据域 | 最大255字节数据 | LLLVAR | 包含多个子域 |  |  | 以下子域中的M仅当该交易为IC卡交易时有效 |
| 9F26（tag） | 应用密文 | b64 |  | BINARY | M |  | 存放TC结果 |
| 9F27（tag） | 应用信息数据 | b8 |  | BINARY | M |  | 存放TC结果 |
| 9F10（tag） | 发卡行应用数据 | b…256 | VAR | BINARY | M |  |  |
| 9F37（tag） | 不可预知数 | b32 |  | BINARY | M |  |  |
| 9F36（tag） | 应用交易计数器 | b16 |  | BINARY | M | C | C：若处理中心返回应答，则在响应中出现，并与请求中的内容一致 |
| 95（tag） | 终端验证结果 | b40 |  | BINARY | M |  |  |
| 9A（tag） | 交易日期 | n6 |  | BCD | M |  |  |
| 9C（tag） | 交易类型 | n2 |  | BCD | M |  |  |
| 9F02（tag） | 交易金额 | n12 |  | BCD | M |  |  |
| 5F2A（tag） | 交易货币代码 | n3 |  | BCD | M |  |  |
| 82（tag） | 应用交互特征 | b16 |  | BINARY | M |  |  |
| 9F1A（tag） | 终端国家代码 | n3 |  | BCD | M |  |  |
| 9F03（tag） | 其它金额 | n12 |  | BCD | M |  | 注1 |
| 9F33（tag） | 终端性能 | b24 |  | BINARY | M |  |  |
| 9F1E（tag） | 接口设备序列号 | an8 |  | ASCII | C |  | 如果终端标识不能隐含确定接口设备序列号，则出现 |
| 84（tag） | 专用文件名称 | b…128 | VAR | BINARY | O |  |  |
| 9F09（tag） | 应用版本号 | b16 |  | BINARY | O |  |  |
| 9F41（tag） | 交易序列计数器 | n…4 | VAR | BCD | O |  |  |
| 9F34（tag） | 持卡人验证结果 | b24 |  | BINARY | O |  |  |
| 9F35（tag） | 终端类型 | n2 |  | BCD | O |  |  |
| 9F63 | 卡产品标识 | b128 |  | BINARY | C |  | 当终端能够获取卡标识信息时，本域出现；否则，本域不出现 |
| 9F74  （tag） | 电子现金发卡行授权码 | a6 |  | ASCII | C |  | 小额支付应用且能获取时，必须上送该tag |
| 8A  （tag） | 授权响应码 | an2 |  | ASCII | M |  | 取值如下：  Y1：脱机接受  Y3：不能联机（脱机接受） |
| 60 | 自定义域 | n…017 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 取36 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | C | C | 有后续子域存在时，本域才出现。非网络管理类交易，此处以缺省值000填充 |
| 60.4 | 终端读取能力 | n1 |  | BCD | C | C | 仅在IC卡交易和Fall Back情况下出现 |
| 60.5 | 基于PBOC借/贷记标准的IC卡条件代码 | n1 |  | BCD | C | C | 仅在IC卡交易和Fall Back情况下出现 |
| 63 | 自定义域 | ans...063 | LLLVAR | ASCII | M | M |  |
| 63.1 | 国际信用卡公司代码 | an3 |  | ASCII | M | M |  |
| 63.2 | 自定义域2 | ans…120 | LLVAR | ASCII |  | C | 当POS终端、中国银联、发卡行、商户结算行等需要传送特殊信息时出现 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |
| * 1：若无其它金额，该域填零。 | | | | | | | |

* + 1. 管理类
       1. 签到

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备注** |
|  | 消息类型 | n4 |  | BCD | 0800 | 0810 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BITMAP |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M |  |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 填“00” |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理信息码 | n3 |  | BCD | M | M | 双倍长密钥算法终端用 003 |
| 62 | 终端密钥 | b…056 | LLLVAR | BINARY |  | C | 当39域为“00”时必选，为50字节的PIK 和MAK或75字节的PIK、MAK和TMK,用法一 |
| 63 | 自定义域 | ans…003 | LLLVAR | ASCII | M |  |  |
| 63.1 | 操作员代码 | an3 |  | ASCII | M |  |  |

* + - 1. POS参数更新

根据终端的序列号下发商户号和终端号。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备注** |
|  | 消息类型 | n4 |  | BCD | 0800 | 0810 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BITMAP |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M |  |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII |  | M |  |
| 42 | 受卡方标识码 | ans15 |  | ASCII |  | M |  |
| 59 | 终端信息 | ans…100 | LLLVAR | ASCII | M |  | 请求：用法一  应答：用法三 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 填“00” |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理信息码 | n3 |  | BCD | M | M | 101 |

* + - 1. POS 电子签名上送

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | N4 |  | BCD | 0820 | 0830 | MSG-TYPE-ID |
|  | 位元表 | B64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C |  | 签购单要素。当原交易应答报文返回主账号时，该域必须出现， |
| 4 | 交易金额 | N12 |  | BCD | M |  | 签购单要素。同原交易应答报文 |
| 11 | 受卡方系统跟踪号 | N6 |  | BCD | M | M | 签购单要素。请求同原交易应答报文 |
| 15 | 清算日期 | n4 | MMDD | BCD | M |  | 请求同原交易应答报文 |
| 37 | 检索参考号 | An12 |  | ASCII | C | C | 签购单要素，原交易应答出现时出现。请求同原交易应答报文，应答同请求。 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 签购单要素。请求同原交易终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 签购单要素。请求同原交易商户代码 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 请求填写07，应答同请求。 |
| 60.2 | 批次号 | n6 |  | BCD | M | M | 请签购单要素。求同原交易的批次号 |
| 60.3 | 网络管理信息码 | n3 |  | BCD | M | M | 301 |
| 62 | 电子签字域 | b…999 | LLLVAR | BINARY | M |  | 签购单要素，用法四 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + - 1. POS参数传递

表 POS参数传递报文

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备注** |
|  | 消息类型 | n4 |  | BCD | 0800 | 0810 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BITMAP |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M |  |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 填“00” |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理信息码 | n3 |  | BCD | M | M | 菜单更新采用 360/361  IC 卡公钥下载交易采用 370/371 IC 卡参数下载交易采用 380/381 TMS 参数下载采用 364/365  卡 BIN 黑名单下载采用 390/391 IC 卡公钥下载(含 SM2 公钥)373  非接参数下载采用394/395  免密新增卡bin更新下载采用396/397  免密卡bin黑名单采用398/399 |
| 62 | 终端参数信息 | Ans…512 |  | ASCII | C(此处c的含 义为当 传递 IC 卡公钥 信息交 易或 IC 卡参数 信息时 或卡 BIN 黑 名单下 载,该域 出现 | C | 成功应答时必填  一.磁条卡交易该域中存放下传的 POS 参数(用法二);  二、IC 卡公钥下载交易中采用如下 方式构造该域内容:  1、 请求报文中填写需要下载的  公钥 RID 和索引,采用 TLV 格式,每次只能请求一组公钥 信息。若需要请求多组公钥, 必须反复发送该报文  2、应答报文中该域的第一个字节 为 0 表示 POS 中心没有该公钥,为 1 表示后续有公钥信息。公钥信息 的格式为: RID+索引+有效期+哈什算法标 识+公钥算法标识+公钥模+公 钥指数+公钥校验值。每个元素都 采用 TLV 的格式,每次只能返回一 组公钥信息。  SM2 算法:RID+索引+有效期+ 公钥签名算法标识+公钥值+椭圆 曲线参数标识+公钥校验值。  三、参数下载交易中采用如下方式构造该域内容:  1、 请求报文中填写需要下载参  数的 AID,采用 TLV 格式,每 次只能请求一组参数信息。若 需要请求多组参数,必须反复 发送该报文  2、应答报文中该域的第一个字节 为 0 表示 POS 中心没有该参数,为 1 表示后续参数信息。公钥信息的 格式为: AID+应用选择指示符(ASI)+ TAC-缺省+TAC-联机+偏置随 机选择的阈值+TAC-拒绝+终端 最低限额+偏置随机选择的最大 目标百分数+随机选择的目标百 分数+缺省 DDOL+终端联机 PIN 支持能力。  六、非接业务参数下载参见用法二十一；  七、新增免密bin表更新下载参见用法二十二  八、免密卡bin黑名单更新下载参见用法二十三 |

* + - 1. POS状态上送

表 POS状态上送报文

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备注** |
|  | 消息类型 | n4 |  | BCD | 0800 | 0810 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BITMAP |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M |  |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 填“00” |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理信息码 | n3 |  | BCD | M | M | 菜单更新采用 362;  IC 卡公钥下载交易采用 372;  IC 卡公钥下栽(含 SM2 公钥)交易采 用 373；  IC 卡参数下载交易采用 382； |
| 62 | 终端状态信息 | Ans…512 |  | ASCII | M | C(此处c的含 义为当 传递 IC 卡公钥 信息交 易或 IC 卡参数 信息时 或卡 BIN 黑 名单下 载,该域 出现 | 中存放 POS 终端状态 信息,用法二  二、IC 卡公钥下载交易中采用如下方 式构造该域内容:  1、 请求报文中该域占三个字节,第 一个字节为数字 1,表示是认证中 心公钥信息查询报文;后面两个 字节联合起来表示 POS 收到的所 有公钥信息个数,所以首先上送 该请求交易时,整个域取值应为 100。  2、 应答报文中该域的第一个字节为 数字 0 表示 POS 中心没有公钥信 息,为数字 1 表示后续有公钥信 息,且一个报文就可以存放下所 有的公钥信息。后续公钥信息的 格式如下:  RID1,索引 1,有效期 1;RID2,索 引 2,有效期 2,...,RIDn,索引 n,有效 期 n。同样采用 TLV 的格式  3、 应答报文中该域的第一个字节为  数字 2 表示一个报文无法存放所 有的公钥信息,需要 POS 终端再 上送请求报文,在与该请求报文 对应的应答报文中存放后续的公 钥信息,公钥信息格式如 2 中所 示。需要注意的是,公钥信息都中存放 POS 终端状态 信息,用法二  二、IC 卡公钥下载交易中采用如下方 式构造该域内容:  1、 请求报文中该域占三个字节,第 一个字节为数字 1,表示是认证中 心公钥信息查询报文;后面两个 字节联合起来表示 POS 收到的所 有公钥信息个数,所以首先上送 该请求交易时,整个域取值应为 100。  2、 应答报文中该域的第一个字节为 数字 0 表示 POS 中心没有公钥信 息,为数字 1 表示后续有公钥信 息,且一个报文就可以存放下所 有的公钥信息。后续公钥信息的 格式如下:  RID1,索引 1,有效期 1;RID2,索 引 2,有效期 2,...,RIDn,索引 n,有效 期 n。同样采用 TLV 的格式  3、 应答报文中该域的第一个字节为  数字 2 表示一个报文无法存放所 有的公钥信息,需要 POS 终端再 上送请求报文,在与该请求报文 对应的应答报文中存放后续的公 钥信息,公钥信息格式如 2 中所 示。需要注意的是,公钥信息都 |

* + - 1. 卡公钥/参数/TMS参数/卡BIN黑名单下载结束

表 IC卡公钥/参数/TMS参数/卡BIN黑名单下载结束报文

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备注** |
|  | 消息类型 | n4 |  | BCD | 0800 | 0810 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BITMAP |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 37 | 检索参考号 | an12 |  | ASCII |  | M |  |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 填“00” |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理信息码 | n3 |  | BCD | M | M | IC 卡公钥下载交易采用 371;  IC 卡参数下载交易采用 381;  TMS 参数下载结束采用 365;  卡 BIN 黑名单下载结束采用 391；  非接业务参数下载结束395  免密新增bin表更新下载结束397  免密卡bin黑名单下载结束399 |

* + - 1. 实名认证

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 2 | 主账号 | n..19 | LLVAR | BCD | C | M | 信用卡卡号 |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 330000 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 14 | 卡有效期 | n4 | YYMM | BCD | M | C | 信用卡有效期 |
| 23 | 卡安全码 | n3 | MMDD | BCD | M | C | CVV2信用卡安全码 |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M | 平台分配标识 |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | 收单处理平台流水号 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 50 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 62 | 身份认证信息 | ans..512 |  | ASCII | M |  | 持卡人身份认证信息选用  用法二十四 |
| 63 | 自定义域 | ans…003 | LLLVAR | ASCII | M |  |  |
| 63.1 | 国际信用卡公司代码 | an3 |  | ASCII | M | M | 请求时填写操作员号； |
| 应答时填写国际信用卡公司代 |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

* + - 1. 日结额度查询

| **位** | **域名定义** | **属性** | **格式** | **类型** | **请求** | **响应** | **备 注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 消息类型 | n4 |  | BCD | 0200 | 0210 | MSG-TYPE-ID |
|  | 位元表 | b64 |  | BINARY | M | M | BIT MAP |
| 3 | 交易处理码 | n6 |  | BCD | M | M | 340000 |
| 11 | 受卡方系统跟踪号 | n6 |  | BCD | M | M | POS终端交易流水 |
| 12 | 受卡方所在地时间 | n6 | hhmmss | BCD |  | M |  |
| 13 | 受卡方所在地日期 | n4 | MMDD | BCD |  | M |  |
| 32 | 受理方标识码 | n..11 | LLVAR | BCD | M | M | 平台分配标识 |
| 37 | 检索参考号 | an12 |  | ASCII |  | M | 收单处理平台流水号 |
| 39 | 应答码 | an2 |  | ASCII |  | M |  |
| 41 | 受卡机终端标识码 | ans8 |  | ASCII | M | M | 终端代码 |
| 42 | 受卡方标识码 | ans15 |  | ASCII | M | M | 商户代码 |
| 54 | 日结额度 | an…040 | LLLVAR | ASCII |  | C | 用法三:日结额度  39域为“00”时必选 |
| 60 | 自定义域 | n…011 | LLLVAR | BCD | M | M |  |
| 60.1 | 交易类型码 | n2 |  | BCD | M | M | 50 |
| 60.2 | 批次号 | n6 |  | BCD | M | M |  |
| 60.3 | 网络管理码 | n3 |  | BCD | M | M | 非网络管理类交易，此处以缺省值000填充 |
| 63 | 自定义域 | ans…003 | LLLVAR | ASCII | M |  |  |
| 63.1 | 国际信用卡公司代码 | an3 |  | ASCII | M | M | 请求时填写操作员号； |
| 应答时填写国际信用卡公司代 |
| 63.2 | 自定义域 | ans120 |  | ASCII |  | M | 应答描述 |
| 64 | MAC | b64 |  | BINARY | M | C | 响应消息中39域为“00”时必选 |

附录A（规范性附录）个人标识码（PIN）的加密和解密方法

* 1. 用于PIN加、解密的主账号PAN取法
     1. 手输卡号

如为手输卡号，从所输卡号（2域）右边数第二位开始，向左取12位，作为参与PIN加、解密的PAN。

* + 1. 刷卡方式

如为刷卡方式，从磁道2（35域）分隔符‘＝’左边第二位开始，向左取12个字符，作为参与PIN加密的PAN；如只有磁道3（36域），则从磁道3分隔符‘＝’左边第二位开始，向左取12个字符，作为参与PIN加、解密的PAN。

* 1. PIN的长度

PIN的长度为6位（可扩展到12位）。

* 1. PIN的字符集

PIN用数字字符表示，下表给出了它的二进制对照表：

表A.1 PIN字符二进制表示

|  |  |
| --- | --- |
| PIN字符 | 二进制表示 |
| 0 | 0000 |
| 1 | 0001 |
| 2 | 0010 |
| 3 | 0011 |
| 4 | 0100 |
| 5 | 0101 |
| 6 | 0110 |
| 7 | 0111 |
| 8 | 1000 |
| 9 | 1001 |

* 1. PIN格式

PIN的格式应符合ANSI X9.8 Format（带主账号信息）

PIN BLOCK格式等于PIN按位异或主账号(PAN):

PIN格式：

表A.2 PIN格式

|  |  |  |
| --- | --- | --- |
| 位置 | 长度 | 说明 |
| 1 | 1 BYTE | PIN长度 |
| 2 | 7 BYTE | 6-12位PIN(每个字符占4个BIT，不足右补F) |

PAN格式：

表A.3 PAN格式

|  |  |  |
| --- | --- | --- |
| 位置 | 长度 | 说明 |
| 1 | 2 BYTE | ％H0000 |
| 3 | 6 BYTE | 取主账号的右12位（参见A.1） |

* 1

例如：明文PIN为： 123456，

假设： 磁卡上的PAN：1234 5678 9012 3456 78

截取下的PAN：6789 0123 4567

则用于PIN加密的PAN为：0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

PIN BLOCK为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

异或：0x00 0x00 0x67 0x89 0x01 0x23 0x45 0x67

结果为：0x06 0x12 0x53 0xDF 0xFE 0xDC 0xBA 0x98

* 2

假设：磁卡上PAN：1234 5678 9012 3456

截取下的PAN：4567 8901 2345

则用于PIN加密的主账号为：0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

PIN BLOCK为：0x06 0x12 0x34 0x56 0xFF 0xFF 0xFF 0xFF

异或：0x00 0x00 0x45 0x67 0x89 0x01 0x23 0x45

结果为：0x06 0x12 0x71 0x31 0x76 0xFE 0xDC 0xBA

PIN的类型（类型2）必须在消息报文的域53（SECURITY­RELATED－CONTROL－INFORMATION）中标明。

附录B（规范性附录）POS终端MAC的算法

终端除管理类交易(电子签名上送除外)外其它交易上行包均用校验验证码（MAC）的方法来保证每一个传送

信息的完整性。计算方法采用国际标准算法，算出的 MAC 直接附在交易报文的后面，随报文一起传送，下面具体描述产生和校验 MAC 的方法。

1. MAC 的产生：

终端与前置机之间的交易报文格式为：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 报文长度 | TPDU | 报文头 | MSGID | bitmap | 交易数据 | MAC |
| 2Bytes | 5Bytes | 12Bytes | 2Bytes | 8Bytes | 变长 | 8Bytes |

计算 MAC：

1. 将要加密的数据（MSGID+BITMAP+交易数据）进行分组，8 字节为一组，不足 8字节后补 0x00；
2. 进行分组异或，最终得到 8 字节数据；
3. 使用 MAC Key 对 8 字节数据进行 3DES 加密，得到 MAC；
4. MAC 的校验：

MAC 的校验采用了跟 MAC 的产生相同的算法，它通过在正文后面附加 64 位的

MAC，作为正文确认用；信息传送到对方后，接受方通过与发送方相同的密钥和算法

对信息进行加密后，比较计算出来的 MAC 与收到的 MAC 是否一致来判断信息本身是

否完整和准确。

附录C（规范性附录）磁道信息加密算法

* 1. 基本要求

PIN输入设备需对下列磁道信息中敏感信息进行加密: 发卡方信息(包括卡片验证码CVN等信息)。 加密采用双倍长密钥算法,磁道信息加密密钥TDK通过POS签到交易获得,存储在PIN输入设备中。

* 1. 数据源构成
     1. 二磁道数据源

二磁道数据(35域)从结束标志“?”向左第2个字节开始,再向左取8个字节作为参与加密的二磁 道中发卡方信息,记为TDB2。

* + 1. 三磁道数据源

类似二磁道数据源构造方法,三磁道数据(36域,如果存在)磁道信息块构造方法如下:

三磁道数据(36域)从结束标志“?”向左第2个字节开始,再向左取8个字节作为参与加密的三磁 道中发卡方信息(若不足右补足F),记为TDB3。

* + 1. 异常处理

对于二磁道或三磁道缺失的情况,终端应上送8字节全F。

* 1. 加密方式

采用双倍长密钥TDK分别对TDB2,TDB3进行加密,将密文输出后按照对应位置替换原先的明文 数据。

* 1. 举例

二磁道数据(37):

1234567890123456789=0508201781999168302

表示为:

0x12 0x34 0x56 0x78 0x90 0x12 0x34 0x56 0x78 0x9D 0x05 0x08 0x20 0x17 0x81 0x99 0x91 0x68

0x30 0x20

三磁道数据(104): 991234567890123456789=156000000000000000000378199921600000508000000000000000000000=0

00000000003=0000000000 表示为:

0x99 0x12 0x34 0x56 0x78 0x90 0x12 0x34 0x56 0x78 0x9D 0x15 0x60 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x03 0x78 0x19 0x99 0x21 0x60 0x00 0x00 0x50 0x80 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0xD0 0x00 0x00 0x00 0x00 0x00 0x3D 0x00 0x00 0x00 0x00 0x00

则TDB2表示为:0x08 0x20 0x17 0x81 0x99 0x91 0x68 0x30 则TDB3表示为:0x00 0x00 0x00 0x3D 0x00 0x00 0x00 0x00 采用TDK对TDB2、TDB3分别进行TDES加密,加密后的磁道信息为: ENC BLOCK1 = eTDK(0x08 0x20 0x17 0x81 0x99 0x91 0x68 0x30)

ENC BLOCK2 = eTDK(0x00 0x00 0x00 0x3D 0x00 0x00 0x00 0x00)

附录D（规范性附录）对应答码的处理

交易返回POS终端时都有39 域，POS终端和终端操作员根据应答码要采取相应的操作，可以把操作分为以下几类：

A：交易成功

B：交易失败，可重试

C：交易失败，不需要重试

D：交易失败, 终端操作员处理

E：交易失败,系统故障，不需要重试

* 1：如果 39 域的内容不能在下表中找到，就显示“交易失败”
* 2：如果POS交易的批次号和网络中心批次号不一致时应答码会填 “77”，此时POS机应当提示操作员重新签到，再作交易。
* C.1 应答码表

| 代码 | 意义 | 类别 | 原因/采取的措施 | POS显示的内容 |
| --- | --- | --- | --- | --- |
| 00 | 承兑或交易成功 | A | 承兑或交易成功 | 交易成功 |
| 01 | 查发卡行 | C | 查发卡行 | 交易失败，请联系发卡行 |
| 02 | 查发卡行的特殊条件 | C | 可电话向发卡行查询 | 交易失败，请联系发卡行 |
| 03 | 无效商户 | C | 商户需要在银行或中心登记 | 商户未登记 |
| 04 | 没收卡 | D | 操作员没收卡 | 没收卡，请联系收单行 |
| 05 | 不予承兑 | C | 发卡不予承兑 | 交易失败，请联系发卡行 |
| 06 | 出错 | E | 发卡行故障 | 交易失败，请联系发卡行 |
| 07 | 特殊条件下没收卡 | D | 特殊条件下没收卡 | 没收卡，请联系收单行 |
| 09 | 请求正在处理中 | B | 重新提交交易请求 | 交易失败，请重试 |
| 12 | 无效交易 | C | 发卡行不支持的交易 | 交易失败，请重试 |
| 13 | 无效金额 | B | 金额为0 或太大 | 交易金额超限，请重试 |
| 14 | 无效卡号 | B | 卡种未在中心登记或读卡号有误 | 无效卡号，请联系发卡行 |
| 15 | 无此发卡行 | C | 此发卡行未与中心开通业务 | 此卡不能受理 |
| 19 | 重新送入交易 | C | 刷卡读取数据有误，可重新刷卡 | 交易失败，请联系发卡行 |
| 20 | 无效应答 | C | 无效应答 | 交易失败，请联系发卡行 |
| 21 | 不做任何处理 | C | 不做任何处理 | 交易失败，请联系发卡行 |
| 22 | 怀疑操作有误 | C | POS状态与中心不符，可重新签到 | 操作有误，请重试 |
| 23 | 不可接受的交易费 | C | 不可接受的交易费 | 交易失败，请联系发卡行 |
| 25 | 未能找到文件上记录 | C | 发卡行未能找到有关记录 | 交易失败，请联系发卡行 |
| 30 | 格式错误 | C | 格式错误 | 交易失败，请重试 |
| 31 | 银联不支持的银行 | C | 此发卡方未与中心开通业务 | 此卡不能受理 |
| 33 | 过期的卡 | D | 过期的卡，操作员可以没收 | 过期卡，请联系发卡行 |
| 34 | 有作弊嫌疑 | D | 有作弊嫌疑的卡，操作员可以没收 | 没收卡，请联系收单行 |
| 35 | 受卡方与安全保密部门联系 | D | 有作弊嫌疑的卡，操作员可以没收 | 没收卡，请联系收单行 |
| 36 | 受限制的卡 | D | 有作弊嫌疑的卡，操作员可以没收 | 此卡有误，请换卡重试 |
| 37 | 受卡方呼受理方安全保密部门(没收卡) | D | 有作弊嫌疑的卡，操作员可以没收 | 没收卡，请联系收单行 |
| 38 | 超过允许的PIN试输入 | D | 密码错次数超限，操作员可以没收 | 密码错误次数超限 |
| 39 | 无此信用卡账户 | C | 可能刷卡操作有误 | 交易失败，请联系发卡行 |
| 40 | 请求的功能尚不支持 | C | 发卡行不支持的交易类型 | 交易失败，请联系发卡行 |
| 41 | 丢失卡 | D | 挂失的卡， 操作员可以没收 | 没收卡，请联系收单行 |
| 42 | 无此账户 | B | 发卡行找不到此账户 | 交易失败，请联系发卡方 |
| 43 | 被窃卡 | D | 被窃卡， 操作员可以没收 | 没收卡，请联系收单行 |
| 44 | 无此投资账户 | C | 可能刷卡操作有误 | 交易失败，请联系发卡行 |
| 51 | 无足够的存款 | C | 账户内余额不足 | 余额不足，请查询 |
| 52 | 无此支票账户 | C | 无此支票账户 | 交易失败，请联系发卡行 |
| 53 | 无此储蓄卡账户 | C | 无此储蓄卡账户 | 交易失败，请联系发卡行 |
| 54 | 过期的卡 | C | 过期的卡 | 过期卡，请联系发卡行 |
| 55 | 不正确的PIN | C | 密码输错 | 密码错，请重试 |
| 56 | 无此卡记录 | C | 发卡行找不到此账户 | 交易失败，请联系发卡行 |
| 57 | 不允许持卡人进行的交易 | C | 不允许持卡人进行的交易 | 交易失败，请联系发卡行 |
| 58 | 不允许终端进行的交易 | C | 该商户不允许进行的交易 | 终端无效，请联系收单行或银联 |
| 59 | 有作弊嫌疑 | C |  | 交易失败，请联系发卡行 |
| 60 | 受卡方与安全保密部门联系 | C |  | 交易失败，请联系发卡行 |
| 61 | 超出取款金额限制 | C | 一次交易的金额太大 | 金额太大 |
| 62 | 受限制的卡 | C |  | 交易失败，请联系发卡行 |
| 63 | 违反安全保密规定 | C | 违反安全保密规定 | 交易失败，请联系发卡行 |
| 64 | 原始金额不正确 | C | 原始金额不正确 | 交易失败，请联系发卡行 |
| 65 | 超出取款次数限制 | C | 超出取款次数限制 | 超出取款次数限制 |
| 66 | 受卡方呼受理方安全保密部门 | C | 受卡方呼受理方安全保密部门 | 交易失败，请联系收单行或银联 |
| 67 | 捕捉（没收卡） | C | 捕捉（没收卡） | 没收卡 |
| 68 | 收到的回答太迟 | C | 发卡行规定时间内没有回答 | 交易超时，请重试 |
| 75 | 允许的输入PIN次数超限 | C | 允许的输入PIN次数超限 | 密码错误次数超限 |
| 77 | 需要向网络中心签到 | D | POS批次与网络中心不一致 | 请向网络中心签到 |
| 79 | 脱机交易对账不平 | C | POS终端上传的脱机数据对账不平 | POS终端重传脱机数据 |
| 90 | 日期切换正在处理 | C | 日期切换正在处理 | 交易失败，请稍后重试 |
| 91 | 发卡行或银联不能操作 | C | 电话查询发卡方或银联，可重作 | 交易失败，请稍后重试 |
| 92 | 金融机构或中间网络设施找不到或无法达到 | C | 电话查询发卡方或网络中心，可重作 | 交易失败，请稍后重试 |
| 93 | 交易违法、不能完成 | C | 交易违法、不能完成 | 交易失败，请联系发卡行 |
| 94 | 重复交易 | C | 查询网络中心，可重新签到作交易 | 交易失败，请稍后重试 |
| 95 | 调节控制错 | C | 调节控制错 | 交易失败，请稍后重试 |
| 96 | 系统异常、失效 | C | 发卡方或网络中心出现故障 | 交易失败，请稍后重试 |
| 97 | POS终端号找不到 | D | 终端未在中心或银行登记 | 终端未登记，请联系收单行或银联 |
| 98 | 银联收不到发卡行应答 | E | 银联收不到发卡行应答 | 交易超时，请重试 |
| 99 | PIN格式错 | B | 可重新签到作交易 | 校验错，请重新签到 |
| A0 | MAC校验错 | B | 可重新签到作交易 | 校验错，请重新签到 |
| D5 | 提现超额 | C | 提现超额 | 提现超额 |
| D6 | 未开通，请联系服务商 | C | 未开通，请联系服务商 | 未开通，请联系服务商 |
| D7 | 交易时间不在T0结算时间内 | C | 交易时间不在T0结算时间内 | 交易时间不在T0结算时间内 |