

# Q/CUP

## 中国银联股份有限公司企业标准

Q/CUP 008-2006

代替Q/CUP 008-2004

---

### 中国银联代理业务 ATM 终端技术规范

Technical Specification on Automatic Teller Machine(ATM)

for Agent Service

2007-01-10 发布

2007-01-10 实施

---

中国银联股份有限公司 发布



# 目 次

前 言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	2
4 ATM终端硬件要求 .....	7
4.1 适用标准 .....	7
4.2 硬件设计 .....	7
4.3 模块配置 .....	7
5 ATM终端软件要求 .....	7
5.1 软件设计 .....	7
5.2 软件配置 .....	7
5.3 ATM功能 .....	8
5.4 ATM状态 .....	8
5.5 其他要求 .....	9
6 ATM终端安全要求 .....	9
6.1 对称密钥管理 .....	9
6.2 加密处理说明 .....	10
6.3 PBOC借贷记卡交易相关公钥及管理 .....	10
7 ATM终端通信接口要求 .....	11
7.1 通信协议 .....	11
7.2 通信连接方式 .....	11
7.3 自检故障 .....	11
7.4 通信异常处理 .....	11
7.5 IP地址访问控制 .....	12
7.6 通讯中断或签到失败后的处理 .....	12
8 ATM终端交易功能 .....	12
8.1 取款 .....	12
8.2 余额查询 .....	12
8.3 明细查询 .....	12
8.4 转账 .....	12
8.5 修改密码 .....	12
8.6 代理业务 .....	13
9 ATM终端管理功能 .....	13
9.1 主动管理 .....	13
9.2 被动管理 .....	14
9.3 交易处理要求 .....	14
9.4 EMV相关终端参数管理 .....	15
10 用户界面 .....	17
11 ATM终端交易处理流程 .....	26

11.1 业务类交易 .....	26
11.2 主动管理类交易 .....	35
11.3 被动管理类交易 .....	38
12 报文的匹配 .....	41
12.1 关键信息域与报文的关联 .....	41
12.2 关键信息域的匹配 .....	41
12.3 交易对报文域的基本要求 .....	42
13 消息域说明 .....	47
13.1 说明 .....	47
13.2 数据元名称及其定义 .....	49
14 ATM终端消息交换说明 .....	74
14.1 报文结构说明 .....	74
14.2 说明 .....	76
14.3 业务类交易报文 .....	78
14.4 主动管理类交易报文 .....	94
14.5 被动管理类交易报文 .....	99
15 客户凭证要素及格式要求 .....	100
15.1 客户凭证要素 .....	100
15.2 格式要求 .....	100
15.3 客户凭证参考样式 .....	103
15.4 交易流水单中, EMV卡交易需要增加打印的要素 .....	105
附 录 A (规范性附录) 个人标识(PIN)的加密和解密方法 .....	106
附 录 B (规范性附录) ATM交易报文MAC的算法 .....	108
附 录 C (资料性附录) ATM终端显示规定 .....	111
附 录 D (资料性附录) ATM终端标识码编码规则 .....	114
附 录 E (资料性附录) 加钞交易成功后的打印凭条格式 .....	115

## 前 言

本规范以《银行磁条卡自动柜员机(ATM)应用规范》(JR/T0008-2001)为基础,根据《中国银联ATM前置系统业务需求》、《中国银联ATM前置系统技术规范》的相关规定,对磁条卡自动柜员机的应用要求作了规定,包括软硬件配置、通讯接口、交易画面、交易流程、报文格式和处理等内容。

自动柜员机(以下简称ATM)必须能够受理国内磁条卡(银行卡)交易,根据需要受理国外磁条卡(银行卡)交易、IC卡交易。

所有银行卡交易通过通讯网络直接送到ATM前置处理系统,ATM终端所能接受的银行卡卡种、交易种类都将由ATM前置处理系统进行判别,所有交易都通过ATM前置处理系统统一进行转接。

本标准的本次修订以《中国金融集成电路(IC)卡规范》(JR/T 0025-2005)为基础,主要增加了ATM关于IC卡交易的有关规定。

本次标准的修订版本代替Q/CUP 008-2004版本。

本标准由中国银联股份有限公司提出,中国银联股份有限公司技术管理部归口管理。本标准由中国银联股份有限公司技术管理部组织制定。

本标准主要起草单位:中国银联电子支付研究院、技术管理部、IC卡应用部、NCR、广电运通。

本标准主要起草人:刘钟、孙平、蒋海俭、林芑、黄发国、徐志忠、李蓓璇、朱经纬、柏建宁、徐静雯。



# 中国银联代理业务 ATM 终端技术规范

## 1 范围

本规范规定了中国银联代理业务ATM终端（磁条卡自动柜员机）的应用要求，包括银行卡自动柜员机的基本硬件要求、软件要求、安全要求、应用功能、用户界面、交易处理流程、终端报文格式等。本规范不涉及银行卡交易主机端的规定。

本规范适用于中国银联的开展代理业务的各种类型的自动柜员机设备，其受理范围包括中华人民共和国境内发行和使用的银行磁条卡、IC卡。

本规范提供的用户界面为基本功能界面，各使用机构可在此基础上进行个性化设计。

管理类功能只提供交易处理流程，不提供具体界面，各机构可根据自动柜员机设备不同的软硬件特性，自行定义用户操作界面、日志流水文件格式和内容等。

银行卡自动柜员机以下简称为ATM终端。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 2312-1980 信息交换用汉字编码字符集 基本集

GB/T 4943-1995 信息技术设备（包括电气事务设备）的安全

GB/T 6833.2~6833.6-1987 电子测量仪器的电磁兼容性试验规范

GB/T 9254-1988 信息技术设备的无线电干扰极限值和测量方法

GB/T 14916-1994 识别卡 物理特性

GB/T 15120.1-.5-1994 识别卡 记录技术

GB/T 15150-1994 产生报文的银行卡 交换报文规范 金融交易内容

GB/T 15694.1-1995 识别卡 发卡者标识 第1部分：编号体系

GB/T 17552-1998 识别卡 金融交易卡

GB/T 18789-2002 自动柜员机（ATM）通用规范

JR/T 0008-2000 银行卡发卡行标识代码及卡号

JR/T 0009-2000 银行卡磁条信息格式和使用规范

银行卡联网联合业务规范

银行卡联网联合技术规范

银行卡联网联合安全规范

《中国金融集成电路(IC)卡规范》第1部分：卡片规范（V2.0）

《中国金融集成电路(IC)卡规范》第2部分：应用规范（V2.0）

《中国金融集成电路(IC)卡规范》第3部分：终端规范（V2.0）

《中国金融集成电路(IC)卡借记/贷记规范》第1部分：卡片规范（V1.0）

《中国金融集成电路(IC)卡借记/贷记规范》第2部分：终端规范（V1.0）

《中国金融集成电路(IC)卡借记/贷记规范》第3部分：应用规范（V1.0）

《中国金融集成电路(IC)卡借记/贷记规范》第4部分：安全规范（V1.0）

《银联卡业务运作规章》第二卷《业务规则》

**银行卡联网联合技术规范V2.0**

ISO 7812-2: 2000 识别卡 发卡方的标识 第2部分: 申请和登记程序

ANSI X9.8 银行业——个人标识码的管理和安全

ISO 7812-2:1993 识别卡 发卡方的标识

ISO 8859 8位单字节编码图形字符集

EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0, Book 1, Application Independent ICC to Terminal Interface Requirements

EMV 2000 Integrated Circuit Card Specification for Payment Systems, Version 4.0, Book 2, Security and Key Management

EMV 2000 Integrated Circuit Card Specifications for Payment Systems, Version 4.0, Book 3, Application Specification

EMV 2000 Integrated Circuit Card Specifications for Payment Systems, Version 4.0, Book 4, Cardholder, Attendant and Acquirer Interface Requirements

### 3 术语和定义

下列术语和定义适用于本标准。

#### 3.1

**银行卡** bank card

商业银行等金融机构及邮政储汇机构向社会发行的, 具有消费信用、转账结算、存取现金等全部或部分功能的信用支付工具。

#### 3.2

**磁条卡** magnetic stripe card

物理特性符合GB/T 14916标准, 磁条记录符合GB/T 15120、GB/T 15694-1、ISO 7812-2、GB/T 17552和JR/T 0009-2000标准的卡片。

#### 3.3

**持卡人** card holder

卡的合法持有人, 即与卡对应的银行账户相联系的客户。

#### 3.4

**自动柜员机** automated teller machine; ATM

是一种组合了多种不同金融业务功能的自助服务设备, 持卡人可利用该设备所提供的功能完成存款、取款、信息查询、代理业务等金融服务。

#### 3.5

**卡处理模块** card accept module; CAM

ATM中对磁卡进行读写的卡接受部件单元。

#### 3.6

**凭条打印模块** receipt print module; RPM

ATM中为合法用户打印票据的打印部件单元。

#### 3.7

**日志打印模块** journal print module; JPM

ATM中记录ATM工作状态的打印部件单元。

#### 3.8

**出钞模块** cash dispense module; CDM

ATM中存放现金并为持卡人实现取款交易时提取现金的部件单元。



## 3.9

**终端控制模块** terminal control module; TCM  
ATM的主控处理机。

## 3.10

**数据安全模块** data security module; DSM  
采用加密算法, 实现ATM数据安全功能的软件和硬件部件单元。

## 3.11

**客户输入模块** customer input module; CIM  
ATM中用于实现输入客户交易数据和管理员(操作员)维护数据的输入部件单元。

## 3.12

**后台维护模块** operator's display module  
ATM中由银行管理员或维修人员使用的用于ATM系统维护、维修诊断等的部件单元。

## 3.13

**多媒体功能模块** multimedia function module; MFM  
ATM中实现语音、图像等多媒体功能的部件单元。

## 3.14

**发卡机构标识号码** issuer identification number; IIN  
标识主要行业和发卡机构的代码。

## 3.15

**个人账户标识** individual account identification  
为识别个人账户, 由发卡机构分配的号码。

## 3.16

**校验位** check digit  
位于持卡者标识之后的一位数字。它根据发卡机构标识号码和个人账户标识全部字符算出, 用以检验输入数据的正确性。

## 3.17

**主账号** primary account number; PAN  
标识发卡机构和持卡人信息的数字代码。它由发卡机构标识代码、个人账户标识和校验位组成, 是银行卡金融交易的主要账号, 在银行卡金融交易中等同于卡号。

## 3.18

**管理员** manager  
可以在ATM上进行一般维护与设置的合法使用者。管理员的所有操作都必须是为了保障ATM的正常运行。

## 3.19

**用户界面** user interface; UI  
持卡人在ATM上进行交易的操作界面。

## 3.20

**交易** transaction  
用于完成(如可能)原始信息发起者意图的相关信息的集合, 通常以一笔借记或贷记交易结束。随后进行的修正或撤消可视为一个独立的交易集合。

## 3.21

**报文** message  
是机构(或其代理)之间交换信息的数据元集合, 不包含或标识任何通信(头或尾、协议或字符码)等有关内容。

3.22

**数据包 datagram**

用于在机构(或其代理)之间交换信息的数据元集合。其与报文的区别是包含或标识了通信(头或尾、协议或字符码)或保密的有关内容。

3.23

**请求 request**

产生一系列交互报文的报文。

3.24

**冲正 reversal**

一种特殊的交易。由报文的发送方发起,用于通知接收方先前一笔授权类或金融类交易没有按预定流程完成,应该取消其处理结果。

3.25

**存储转发 store and forward**

发送方将报文存放在存储转发队列中,在一定次数内每隔一段时间重复发送。

3.26

**受理方 acquirer**

指受理交易的一方(即交易终端所在的一方)。受理方负责联机交易信息的产生和转接以及结算数据的收集、整理和提交等。

3.27

**发卡方 issuer**

指持卡人账户所在的一方(即批准授权的一方)。通常将发卡行及其联网的行内中心或区域中心统称为发卡方。

3.28

**代理业务 agent service**

受公用事业机构、商业机构、企事业单位等收付方委托办理的收费、发放现金等交易业务,如代收公用事业费(水、电、煤气)、代发工资、代交电话费、售票、缴税、证券交易等。

3.29

**电子日志 electronic log**

由计算机或其他电子设备在磁媒体、光媒体上存储的日志记录。

3.30

**TCP**

TCP(Transport Control Protocol),是一种可靠的传输控制协议。本规范中除了指传输控制协议外,还特指各系统中实现TCP协议的协议栈。

3.31

**长连接 persistent link**

指通信双方连接建立后不再关闭,在通信正常情况下一一直保持连通状态。

3.32

**短连接 transitory link**

指通信双方每次通信时建立连接,通信结束后关闭连接。

3.33

**ATM 前置处理系统 ATMP**

ATM前置处理系统是指进行联机交易处理时,与ATM终端建立通信连接的通信前置机或业务主机,能够接受、处理或转发ATM终端的交易请求信息,并向ATM终端回送交易结果信息。

3.34

**现金托管机构 cash manage agent**

具有现金管理资质的商业银行或其他机构，该机构需要有垫付现金和资金清算的能力。中国银联委托其管理银联代理业务ATM的现金。

**3.35****会计周期 account period**

现金托管机构对ATM进行加钞，由ATMP根据加钞记录给每一个会计周期分配一个新的批次号。两次加钞之间的时间定义为一个会计周期。

**3.36****个人标识代码 personal identification number; PIN**

即个人密码，是在联机交易中识别持卡人身份合法性的数据信息，在计算机和网络系统中任何环节都不允许PIN以明文的方式出现。

**3.37****报文鉴别码 message authentication code; MAC**

是消息来源正确性鉴别的数据。

**3.38****密钥加密密钥 key encryption key; KEK**

是ATM工作时，对工作密钥进行加密的密钥，由管理员统一设置并保存在系统硬件中，只能使用，不能读取，该密钥必须与加密算法放在同一加密芯片里。

**3.39****工作密钥 working key; WK**

也称为数据密钥，通常指PIN加密密钥和MAC计算的密钥。工作密钥必须经常更新。在联机更新的报文中对工作密钥必须用密钥加密密钥（KEK）加密，形成密文后进行传输。

**3.40****EMV Europay MasterCard VISA**

EMV是EUROPAY、MASTERCARD、VISA三个国际信用卡公司的首字母缩略词，这三个公司联合制定的IC卡借记/贷记应用标准，简称为EMV标准。

**3.41****EMV 卡**

本文中主要指具有借贷记功能的PBOC借贷记卡，也包括其它符合EMV规范的芯片卡。

**3.42****集成电路卡 integrated circuit card**

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

**3.43****支付系统环境 payment system environment; PSE**

当符合本标准的支付系统应用被选择，或者用于支付系统应用目的的目录定义文件（DDF）被选择后，IC卡中所确立的逻辑条件。

**3.44****应用标识 application identifier; AID**

由注册的应用提供商标识（RID）以及专用应用标识符扩展（PIX）组成。

**3.45****应用标签 application label**

根据ISO/IEC 7816-5标准，应用标签是与应用标识（AID）相关联的名称，用于应用选择。应用标签在应用数据文件（ADF）的文件控制信息（FCI）中可选（推荐要求），在ADF目录入口中必须存在。

3. 46

**应用首选名称** application preferred name

与应用标识(AID)相关联的应用名称。如果应用首选名称存在且终端支持发卡行代码表索引指示的语言,则应用选择过程中显示给持卡人的应用名称应采用应用首选名称,而不是应用标签。

3. 47

**应用选择指示符** application selection indicator; ASI

指示应用选择时终端上的应用标识(AID)与卡片中的应用标识(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应用标识(AID)仅有一个应用选择指示符。

3. 48

**脚本** script

发卡行向终端发送的命令或命令序列,目的是向IC卡连续输入命令。

3. 49

**应用认证密文** application authentication cryptogram; AAC

在EMV应用交易流程中,由IC卡生成的表示拒绝交易的应用密文。

3. 50

**授权响应密文** authorization response cryptogram; ARPC

由发卡行生成并在联机授权报文中返回给终端的应用密文,用于IC卡验证联机授权响应是否来自真正的发卡行。

3. 51

**授权请求密文** authorization request cryptogram; ARQC

IC卡为联机处理交易生成的应用密文,发卡行在联机卡片认证过程中通过验证ARQC来认证当前交易中卡片的有效性。

3. 52

**数据对象列表** data object list; DOL

在EMV应用交易流程中,终端能够根据卡片的要求建立可变的数据元列表,并通过相关命令发送给卡片。在EMV交易流程使用的DOL包括:通过取处理选项(GET PROCESS OPTIONS)命令使用的PDOL;通过生成应用密文(GENERATE AC)命令使用的CDOL1和CDOL2;用来产生TC哈希值的TDOL和通过内部认证(INTERNAL AUTHENTICATE)命令使用的DDOL。

3. 53

**降级使用** Fallback

在某些情况下,IC卡有可能无法在支持芯片卡的终端上使用,比如IC卡本身坏了,或终端上的读写器发生了故障。在这种情况下,支付系统允许使用卡上的磁条来进行交易。

3. 54

**终端行为代码** terminal action code; TAC

在EMV应用交易流程中,终端行为代码(缺省、拒绝、联机)反映了收单行根据TVR的内容选择的动作。

3. 55

**交易证书** transaction certificate; TC

在EMV应用交易流程中,由IC卡生成表示批准交易的交易证书。

3. 56

**终端校验结果** terminal verification results; TVR

在EMV应用交易流程中，用于标识终端执行脱机数据认证、处理限制、持卡人验证、终端风险管理、发卡行认证、发卡行脚本处理等各步骤的结果，终端和卡片将参考TVR的值对当前交易作出脱机拒绝、联机交易或脱机批准的决定。

### 3. 57

**交易验证码** transaction authorization cryptogram; TAC

用于验证交易的合法性。

### 3. 58

**EMV 简化流程**

指应用选择后，仅执行初始化应用和读应用数据，在得到足够交易的卡信息后，开始按处理磁条的流程进行交易，而不需要后序的EMV处理。

## 4 ATM 终端硬件要求

### 4. 1 适用标准

对于各种类型ATM终端的技术要求、试验方法、检验规则以及标志、包装、运输等首先都必须按照中华人民共和国国家标准GB/T 18789-2002《自动柜员机（ATM）通用规范》中规定执行。

### 4. 2 硬件设计

ATM终端的硬件设计应遵照安全、可靠、便于维修的原则。硬件系统和各模块的通用化逻辑设计应尽量采用统一的检验技术，并留有适当的逻辑余量，应具有一定自检功能。

ATM的结构设计应符合防火、防盗、防尘、防淋、防震等要求，配置的密封装置及门锁应耐久、安全、可靠。

ATM端应用软件应该能够支持TCP/IP通讯协议，支持专线和拨号通讯方式。

### 4. 3 模块配置

**必备模块：**电源模块、终端控制模块、显示模块、出钞模块、卡处理模块、平台打印模块、日志打印模块、客户输入模块、后台维护模块、数据安全模块、通讯模块。ATM也可以根据需要加装其他模块。

出钞模块应能辨识目前国内流通的10元以上币值的纸质人民币，根据中国人民银行2004年1月1日起开始执行的《不宜流通人民币挑剔标准》，对符合流通标准的纸币应能够正常出钞，对不符合流通标准的纸币（如残缺、破损、粘连、伪造变造币等）以及持卡人未取走的纸币，应能回收。出钞模块应至少配置2个钞箱（其中一个为回收箱）。

客户输入模块应包括屏幕选择和键盘输入两部分。其中屏幕选择共8个按键，平均分布在屏幕的左右两边。键盘应该包括0~9共10个数字键和『取消』（Cancel）、『确认/Confirm』（Enter）、『更正/Modify』（Clear）等三个功能键。

ATM终端必须配备PIN硬件加密模块。

ATM上其他模块的性能应确保ATM功能的实现。

## 5 ATM 终端软件要求

### 5. 1 软件设计

ATM终端的软件设计应与硬件系统的资源相适应。除应用软件外，还应配备完善的测试（诊断）软件。应用软件需保密的参数、文件以及数据传输过程中需保密的数据均应经过数据安全模块处理。软件技术规范以及字符集中字符的编码、字型等都应符合相应的国家标准。

### 5. 2 软件配置

软件配置要求如下：

——操作系统软件（必备）

- ATM 系统软件（必备）
  - ATM 控制软件（必备）
  - ATM 通信软件（必备）
  - ATM 故障诊断软件（必备）
- 二次开发平台（必备）
- ATM 辅助工具软件（可选）
- ATM 软件自动更新模块（可选）

### 5.3 ATM 功能

- 交易功能
  - 取款
  - 余额查询
  - 明细查询（可选）
  - 转账（可选）
  - 修改密码（可选）
  - 代理业务（可选）
- 数据安全功能
  - 数据加解密
  - 数据合法性检查
- 维护功能
  - 设备维护
  - 设置日期和时间
  - 设置终端代码
  - 设置密钥
  - 检查系统状态
  - 支持远程控制
  - 电子日志记录及转存（可选）
- 其他
  - 中/英文操作界面
  - 支持工作状态切换

### 5.4 ATM 状态

ATM状态可分为服务状态、管理状态和故障状态。ATM在任何情况下只能处于一种状态。ATM在不同状态间进行切换时，都需要通过管理类交易通知ATMP。

#### 5.4.1 服务状态

服务状态是指ATM终端签到后或者接收到ATMP的打开命令后所处的工作状态。在服务状态下，ATM可以支持规定的业务类交易功能。

#### 5.4.2 管理状态

当管理员对ATM终端进行管理类交易操作时，ATM进入管理状态。

在管理状态和其他状态之间进行切换时，需要通过管理员对ATM执行相关操作来实现。

在管理状态下，管理员可以执行规定的管理类交易功能。

#### 5.4.3 故障状态

当ATM自检发现故障，且故障会导致所有的ATM业务类交易都无法进行时，ATM应自动进入故障状态。ATM终端接收到ATMP的关闭命令后也进入故障状态。

当ATM故障被修复后，ATM自动从故障状态切换到服务状态。

如果ATM终端由于接收到关闭命令而进入故障状态，则在接收到打开命令后必须切换到服务状态。

## 5.5 其他要求

### 5.5.1 配置要求

ATM的硬件、软件功能及配置性能指标、数据安全等方面应符合GB/T 18789-2002的要求。

### 5.5.2 磁道要求

ATM应能正确地按顺序读取第二、三磁道并能根据JR/T00009-2000相关规定准确地识别主账号，跨行操作不能对银行卡磁道内容进行任何更改。

### 5.5.3 自检要求

当ATM接受银行卡后，先进行自检，当发现有关部件不能正常工作时，不应提供相应的操作选择或在操作界面上给予客户提示。

示例 1：当检测到钞箱无钞时，ATM 画面必须隐去『取款』的交易选项。

示例 2：当客户凭条无纸时，ATM 画面必须提示“无法打印客户凭条”。

### 5.5.4 时间同步要求

ATM终端时间与ATMP的系统时间通过联机交易报文的12域和13域进行同步，且只有在进行ATM签到和取款交易时才进行同步。当ATM发现与ATMP的时间误差大于1秒时，需要根据ATMP返回报文的12域和13域的值调整本机时间。

### 5.5.5 吞卡要求

如果交易处理失败，ATM应该根据交易返回码，按照“附录C：ATM终端显示规定”中的规定正确执行吞卡操作，同时打印客户凭条。

如果在交易进行过程中，持卡人在30秒内没有任何按键操作，则必须将银行卡退回至入卡口，同时屏幕提示持卡人取卡。如果在30秒内持卡人未将银行卡从入卡口取走，则必须执行吞卡操作，同时打印客户凭证。

### 5.5.6 交易结果显示要求

对于持卡人进行的交易，其交易结果的屏幕显示应该严格按照“附录C：ATM终端显示规定”中的规定执行。

### 5.5.7 流水纸打印

在流水纸上打印的一些交易信息需要添加交易终端号。根据目前的ATM交易种类，在客户进行取款、转账、代理业务（代缴费、充值）等三类与资金清算相关的交易以及加钞交易时，在流水纸上除打印现有信息外，还需要打印当前交易终端号，具体格式可根据实际打印情况设定。

## 6 ATM 终端安全要求

### 6.1 对称密钥管理

#### 6.1.1 二级密钥体系

ATM密钥分为二级：密钥加密密钥(KEK)和工作密钥(WK)。

#### 6.1.2 密钥加密密钥(KEK)

用于对工作密钥(WK)进行加密保护，每台ATM与ATMP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。当KEK泄密时，需要ATM与ATMP及时、方便地更换KEK。

#### 6.1.3 工作密钥(WK)

ATM采用两种工作密钥用于数据的加解密，即对个人密码(PIN)加解密的PIK和对消息鉴别码(MAC)进行加解密的MAK。

工作密钥由ATMP的硬件加密机产生，在ATM每次签到时从ATMP利用KEK加密后下载，并由KEK加密存储。

ATM工作密钥在下载时和传输时都必须以密文方式出现，严禁明文传送。

#### 6.1.4 密钥加密密钥(KEK)的输入

目前ATM密钥加密密钥由16个字符（‘0~9’和‘A~F’）组成，明文回显一次输入。需要改为支持两个人分两段输入8个字符（‘0~9’和‘A~F’）来解决，每人各输入两次（回显\*字符），程序需要对两次输入内容进行比较，如果出现不一致需要重新输入该段数据。

## 6.2 加密处理说明

### 6.2.1 算法

ATM的数据安全模块必须能够同时支持单倍长和双倍长密钥加密算法。

### 6.2.2 PIN 加密

PIN加密采用ANSI X9.8 Format(带主账号信息)，详见附录A:个人标识（PIN）的加密和解密方法。

PIN加解密应在PIN硬件加密模块中进行，并应采用双倍长密钥算法。应确保所有PIN在硬件加密模块之外传输和保存时是加密的。

### 6.2.3 MAC 的算法

从报文消息类型（MTI）到128域之间的全部数据域构成MAC ELEMENT BLOCK（MAB），采用ECB算法，加密结果为64位的MAC，详细算法见附录B:ATM交易报文MAC的算法。

## 6.3 PBOC 借贷记卡交易相关公钥及管理

### 6.3.1 认证中心公钥的导入

ATM终端应提供本地下载、远程下载等方式支持认证中心公钥的导入，同时应遵循以下原则：

- ATM 终端必须能够验证收到的认证中心公钥及相关数据的正确性。
- ATM 终端必须能够验证收到的认证中心公钥及相关数据的合法性。
- ATM 终端必须能向 ATM 中心或下载人员提供相应信息，确认新的认证中心公钥是否已经真正地、正确地导入终端。
- ATM 终端应能通过屏幕显示或打印的方式，提供系统管理员确认终端当前使用的认证中心公钥的相关信息，信息应包括认证中心公钥所属支付组织的名称或简称、认证中心公钥的索引号、认证中心公钥的有效期等。
- ATM 终端应能通过本地设置、远程下载等方式实现对特定认证中心公钥的有效期的更改，但必须先验证 ATM 操作人员或 ATM 中心的合法性。

### 6.3.2 认证中心公钥的存放

支持静态和/或动态数据认证的ATM终端必须对每个支付组织的借记/贷记应用提供6个认证中心公钥的支持。

每一个认证中心公钥由5个字节的标识支付系统的RID和1个字节的认证中心公钥索引号唯一标识，索引号是由支付系统分配给某个特定的认证中心公钥，且对于每个RID唯一。

表1详细说明了每一个认证中心公钥在终端中有用的数据元的最小集。

RID和认证中心公钥索引一起唯一标识了一个认证中心公钥，并将它和正确的支付系统联系起来。

认证中心公钥算法标识标识了和相应的认证中心公钥一起使用的数字签名算法。在目前来说，唯一被接受的值为16进制的‘01’，指明在EMV规范第二册附录A2.1和B2.1中指明的数字签名方案中使用RSA算法。哈希算法标识指定了在数字签名方案中用来生成哈希结果的哈希算法。在目前来说唯一被接受的值为16进制的‘01’，指明使用SHA-1算法。

认证中心公钥校验值采用SHA-1算法，用来保证接收到的认证中心公钥及其相关数据没有错误。终端可以用该数据元重新验证存放的认证中心公钥及其相关数据的完整性。

对存储的认证中心公钥的完整性的验证应该定期进行。

表1 存储在终端中的认证中心公钥相关数据元的最小集

名称	长度	描述	格式
注册的应用提供者标识（RID）	5	指定认证中心公钥和哪个支付系统相关	b
认证中心公钥索引	1	和 RID 一起指定认证中心公钥	b



认证中心公钥有效期	4	认证中心规定的有效期限	b
认证中心哈希算法标识	1	标识用来在数字签名方案中产生哈希结果的哈希算法	b
认证中心公钥算法标识	1	标识使用在认证中心公钥上的数字签名算法	b
认证中心公钥模	变长 最大为 248	认证中心公钥模部分的值	b
认证中心公钥指数	1 或 3	认证中心公钥指数部分的值，等于 3 或 $2^{16+1}$	b
认证中心公钥校验值	20	用 SHA-1 算法对认证中心公钥所有部分（RID，认证中心公钥索引，认证中心公钥模，认证中心公钥指数）的连接计算得到的校验值。	b

### 6.3.3 认证中心公钥的使用

交易中对认证中心公钥的使用必须遵循《中国集成电路（IC）卡借记/贷记规范》。

### 6.3.4 认证中心公钥的撤回

ATM终端应支持本地设置、远程参数下载等方式实现对认证中心公钥的撤回，同时应遵循以下原则：

- ATM终端必须能够验证对认证中心公钥的撤回操作或从ATM中心收到的撤回通告的正确性。
- ATM终端必须能够验证对认证中心公钥的撤回操作或从ATM中心收到的撤回通告的合法性。
- ATM终端必须能向ATM中心或操作人员提供相应信息，确认特定的认证中心公钥已经真正地、正确地终端撤回。
- ATM终端应确保已被撤回的认证中心公钥不会再被用作此后的任何交易。
- 建议ATM终端能够定期触发检查认证中心公钥是否已超出有效期，并实现对已到期公钥的自动撤回。

## 7 ATM 终端通信接口要求

### 7.1 通信协议

ATM终端应采用TCP/IP通信协议与ATMP进行通讯。在TCP/IP协议的基础上，必须使用套接字(socket)技术编写ATM终端通信程序。一个socket由IP地址和端口号唯一确定，一个socket连接由本地IP地址、端口号和远端IP地址、端口号唯一确定。

ATM的IP地址和端口号，都由负责ATM运行管理的机构统一分配。ATM和ATMP之间传送的所有数据均是八位的二进制数据，没有特殊含义字符和控制字符。

### 7.2 通信连接方式

ATM终端应支持长连接和短连接通信方式。ATM终端可根据实际物理通讯情况，采取其中一种方式与ATMP建立连接。

长连接是指通信双方连接建立后不再关闭，在通信正常情况下一一直保持连通状态，双方在收发数据时不再重新建立连接。

短连接是指通信双方每次通信时建立连接，通信结束后关闭连接。

### 7.3 自检故障

通信程序必须能够及时检测到通信异常的发生并做自动恢复的处理，而不需要人工干预经常性介入，从而最大限度保证ATM联机交易的正常进行。

### 7.4 通信异常处理

通信进程接收到消息包，即可对消息包进行解读，如果发现消息包异常则转入出错处理。

通信进程认为的通信异常包括以下若干情况：第一，收到零长度的消息包（注意，并非消息包的长度域为零），则认为对方关闭socket；第二，socket自动消失，则被看作是底层通讯出现问题。以上情况均被认为消息包出现异常。异常发生后，由于不希望人工干预的经常性介入，出错后的恢复机制就显得尤为重要。当某个socket发生异常时，通信进程应先将错误原因记录在错误日志文件中，然后关闭相应的socket，重新进行初始化操作。

### 7.5 IP 地址访问控制

为了便于管理和保障系统安全性，ATM终端必须使用统一分配的IP地址和端口号进行通讯处理。ATM和ATMP在建立TCP连接时，都必须对请求建立连接的对端IP地址做合法性检查，如果是规定的IP地址则允许建立连接，否则拒绝连接。

### 7.6 通讯中断或签到失败后的处理

ATM终端应能自动判断物理通讯与TCP连接状况并分开处理，应用不同的处理策略。

如果发生物理链路中断的情况，ATM应该不断的尝试进行TCP/IP的建链操作，直至建立连接。在两次尝试之间应有一定的时间间隔，时间间隔参数可以在config文件中自行设置，以秒为单位。程序应对该参数值进行控制，设置的间隔时间应该在“0秒”～“300秒”之间。如果该参数值超过300秒，程序应自动按最大值“300秒”进行运行。

在物理链路正常，TCP连接成功的基础上，如果首次签到失败后，应立即再次尝试进行签到。如果再次失败，则尝试第三次签到。如果第三次ATM签到依然失败，则采取以下处理策略。ATM不断向ATMP进行签到交易，在两次尝试之间应有一定的时间间隔，时间间隔参数可以在config文件中自行设置，以秒为单位。程序应对该参数值进行控制，设置的间隔时间应该在“60秒”～“3600秒”之间。如果该参数值超过3600秒，程序应自动按最大值“3600秒”进行运行。

## 8 ATM 终端交易功能

### 8.1 取款

持卡人在ATM终端上提取现金。

ATM终端确认吐钞成功后，必须发起吐钞成功确认报文，通知ATMP吐钞成功。

ATM终端确认吐钞失败后，必须自动发起取款冲正交易确保持卡人账户的完整性。

ATM终端可以提供指定取款金额的快速取款画面。

本规范允许从磁条发起取款交易。

本规范允许从芯片发起的完整的EMV流程的取款交易。

本规范允许降级到磁条进行取款交易。

### 8.2 余额查询

持卡人查询银行卡，在屏幕上显示银行卡账户余额、可用余额等信息。如果是多账户卡，则该操作针对默认账户进行，不需要进行账户选择。

本规范允许从磁条发起余额查询交易。

本规范允许从芯片发起的简化EMV流程的余额查询交易。

### 8.3 明细查询

完成银行卡账户中最近十笔交易明细查询，在屏幕上显示。如果是多账户卡，则该操作针对默认账户进行，不需要进行账户选择。

本规范允许从磁条发起明细查询交易。

### 8.4 转账

完成不同银行卡之间资金的转移。

本规范允许从磁条发起转账交易。

本规范允许从芯片发起的完整EMV流程的转账交易。

### 8.5 修改密码

为现金托管机构发行的银行卡提供修改密码功能，仅限于同城处理，不支持异地交易。

本规范仅允许从磁条发起修改密码交易。

## 8.6 代理业务

受公用事业机构、商业机构、企事业单位等收付方委托办理的收费、发放现金等业务。本规范以代缴费交易和充值交易为例说明代理业务在ATM终端上的实现，其中代缴费交易可以分为代缴费查询和实时缴费两个步骤实现。其他代理业务的交易流程、画面和报文可以参照代缴费交易或者充值交易进行。

本规范仅允许从磁条发起代理业务交易。

## 9 ATM终端管理功能

根据交易发起方不同，可以分为ATM终端发起的管理功能（以下简称主动管理）和ATMP发起的管理功能（以下简称被动管理）。

各受理方按照本规范制定交易流程进行管理类交易。本规范不对管理类交易规定统一界面，各受理方可以自行定义。管理类交易根据发起方不同，分为“由ATM发起的管理交易”和“由ATMP发起的管理交易”两大类。

由ATM发起的管理交易，不得与持卡人进行的业务类交易同时进行。当两类交易在时间上发生冲突时，ATM必须首先确保持卡人完成业务类交易后才能发起管理类交易。

由ATMP发起的管理交易采用短连接方式进行，和持卡人进行的业务类交易不共用一个通讯连接，因此不存在冲突的可能性。

### 9.1 主动管理

#### 9.1.1 设备签到

ATM开机后，或从管理状态切换到服务状态，或者在网络恢复正常后，自动发送签到请求，签到交易将把当前的ATM的软件版本号及参数版本号上送。ATM接收到的响应报文中应包含新的工作密钥等参数。对于业务类交易，如果ATM终端校验交易报文的MAC出错或收到校验MAC出错的应答报文，必须自动发起签到交易，重新申请工作密钥。

#### 9.1.2 加钞通知

管理员加钞后，通过ATM管理界面执行加钞交易，ATM应自动同时发起按当前批次号对账交易（无需人工干预），ATMP记录钞箱信息，并返回新的ATM交易批次号给ATM，ATM开始一个新的会计周期。

#### 9.1.3 定时状态报告

在规定时间内间隔内，ATM终端自动将其设备状态信息（包括钞箱、读卡器、流水打印机、凭证打印机、服务状态等）上送，ATMP收到报文后进行记录，同时更新ATM状态。

#### 9.1.4 状态切换报告

当ATM在服务状态、管理状态、故障状态之间切换时，自动上送状态切换通知交易，ATMP收到报文后进行记录。

#### 9.1.5 故障通知

在ATM设备出现故障的情况下，ATM自动上送故障通知交易，ATMP收到报文后进行记录。

#### 9.1.6 提醒通知

ATM监测钞票、打印机凭条等的使用情况，当到达设定的预警值时，主动上送通知交易给ATMP，ATMP收到报文后进行记录。

#### 9.1.7 吞卡通知

ATM终端吞卡后，必须自动发起吞卡通知交易，ATMP收到报文后进行记录。

#### 9.1.8 对账

由ATM操作人员在ATM上主动发起交易，将某一清算日（或某批次）交易统计信息发送到ATMP，ATMP收到后，进行核对并将对账结果返回ATM，ATM接到对账应答信息后在屏幕上显示对账结果，并在凭条上

打印。当ATM与ATMP对账不平时，应自动发起批上送交易明细，具体上送的交易数量应该根据ATMP返回的对账数据中与ATM本地记录不符的交易类型来决定，目前仅对涉及资金清算的交易记录进行核对。

ATMP和ATM的对账按ATM的加钞周期（两次加钞之间的交易周期为一个批次，每次加钞时，ATMP分配一个批次号）进行，要求现金托管机构在加钞时需要严格按照对账、加钞的顺序进行。

#### 9.1.9 EMV 卡交易公钥下载

操作员选择公钥下载，ATM发起下载公钥列表的请求，ATM检查下载的公钥列表，并根据需要下载终端没有的公钥，公钥的下载采用逐条请求和下载。ATM上送空的下载请求表示结束下载。

#### 9.1.10 EMV 卡交易参数下载

操作员选择EMV参数下载后，ATM发起下载AID列表的请求，并根据AID列表逐各AID下载该AID相关参数。ATM上送空的下载请求表示结束下载。

### 9.2 被动管理

ATM终端应支持由操作员在ATMP端发起的被动管理类交易。ATM终端接收到ATMP发出的被动管理类报文后，应对ATMP的IP地址进行校验，只有通过校验才能根据ATMP的远程控制命令进行相应的动作，并返回正确应答。

#### 9.2.1 打开 ATM 终端

ATMP通知ATM终端进入工作状态，ATM接收到允许其做交易的通知报文后，用户界面显示正常欢迎画面，ATM处于服务状态。

#### 9.2.2 关闭 ATM 终端

ATMP通知ATM终端进入关闭状态，ATM接收到停止做交易的通知报文后，用户界面显示暂停服务画面，进入故障状态。

#### 9.2.3 ATM 终端设备查询

ATMP向ATM终端发出查询设备状态的通知，ATM终端接收到该通知报文后，将当前自身的工作状态信息实时返回给ATMP，包括通讯状态（是否连通）、服务状态（正常、维护、管理）、设备状态（卡读写、出钞、凭条打印机、日志打印机等）等具体内容。

#### 9.2.4 参数下载

ATMP通知ATM终端进行参数下载，如超时参数、广告信息等。ATM终端应响应ATMP下载参数的通知，并对下载的参数进行相应的处理。

#### 9.2.5 通知上传交易明细

ATMP通知ATM终端上传交易明细。ATM终端接收到通知报文后，将指定清算日或批次号的交易明细记录按照交易时间排序后上传至ATMP，由ATMP进行接收和存储，以进行账务核对。目前上传的交易明细记录仅限于需要进行资金清算或者手续费结算的交易。

通知上传交易明细应支持断点续传功能，即能够在传输异常中断后，从中断处继续上传剩余交易明细，而不必全部重新传输。ATMP的通知上传交易明细报文中，可以指明ATM上传某个序号后的交易明细，若序号为0000则ATM上传该清算日或者批次号的所有交易记录，否则上传某个序号后的交易记录。当发生传输失败，ATMP再次通知上传时，则从上次传输失败前最后一次成功的记录序号开始请求。

#### 9.2.6 EMV 卡交易公钥下载

如果ATMP公钥有变化，ATMP在ATM联机交易时下载更新公钥的标志，ATM在接收到标志后发起下载公钥列表的请求，ATM检查下载的公钥列表，并根据需要下载终端没有的公钥，公钥的下载采用逐条请求和下载。ATM上送空的下载请求表示结束下载，ATMP取消下载标志。

#### 9.2.7 EMV 卡交易参数下载

如果ATMP修改了EMV参数，ATMP在ATM联机交易时下载EMV参数的标志，ATM在接收到标志后发起下载AID列表的请求，并根据AID列表逐各AID下载EMV参数。下载完AID列表后，ATM上送空的下载请求表示结束下载，ATMP取消EMV参数下载标志。

### 9.3 交易处理要求

### 9.3.1 吐钞要求

ATM接收到ATMP的要求吐钞的取款成功应答，从钞箱中点出正确数量的现金后应向ATMP发送取款确认报文，同时将现金送出钞口。

ATM点钞金额与交易金额不符的情况下，不允许出钞，已点出的现金应送入废钞箱。ATM不支持部分吐钞功能。

### 9.3.2 冲正通知说明

引发ATM终端产生冲正通知的交易只有取款交易。

当发生以下三种情况时，ATM必须向ATMP发起冲正通知交易，并且必须在接收到冲正交易已经成功发送的应答后才能继续为客户提供服务，否则ATM应暂停服务，持续尝试冲正直到冲正已经成功发送。

- a) 当 ATM 接收到要求吐钞的取款成功应答，校验 MAC 发现错误时，必须产生冲正通知。此时 ATM 应该先发起设备签到交易，更换 ATM 工作密钥后，然后再进行冲正处理。
- b) 当 ATM 接收到要求吐钞的取款成功应答，在吐钞过程中发生故障时，ATM 应在确认没有吐钞的情况下，产生冲正通知。
- a) 当 ATM 在限定时间内接收不到交易请求应答时，必须产生冲正通知。对于后面接收到的 ATMP 发送的取款成功迟到达应答，ATM 应直接丢弃。
- b) 当 EMV 卡发起的交易在联机批准后卡最终没能批准时，ATM 必须产生冲正通知。

## 9.4 EMV 相关终端参数管理

### 9.4.1 可修改参数

表2 可修改参数表

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
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期限	安装或调整时	交易应用
认证中心公钥哈希算法标识	b	1	DF06	标识用于在数字签名方案中产生哈希结果的哈希算法	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	20	DF03	验证认证中心公钥用	安装或调整时	交易应用
注：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。						

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

#### 9.4.2 参数修改规则

EMV参数分为公钥相关参数和AID相关参数，终端出厂时, EMV公钥、AID及AID相关参数为空，终端安装后必须下载公钥、AID及AID相关EMV参数，其中公钥参数依赖于RID和公钥索引，其他参数依赖于AID。

公钥下载时，先下载系统中的公钥列表，再根据公钥列表逐条下载公钥，终端应保证公钥列表中的全部公钥被正确下载。EMV AID相关参数下载时，先下载系统中的AID列表，再根据AID列表逐条下载该AID相关参数，终端应保证AID列表中的全部可下载参数被正确下载。

## 10 用户界面

### 10.1 初始画面

可根据中国银联或代理业务各相关合作方的意愿自行定义, 但是画面主体中必须包含明显的中国银联标志和文字说明。

### 10.2 等待交易画面

当持卡人出现在ATM前时，ATM将出现如图1所示等待交易画面。



图1 ATM 等待交易画面

### 10.3 语言选择画面

双语选择为可选，如果 ATM 支持双语同屏显示，此步骤可省。

持卡人插入银行卡后首先显示如图 2 所示语言选择画面。



图2 ATM 语言选择画面

### 10.4 个人密码输入画面

ATM个人密码输入画面如图3所示。密码的位数可为4~12位，当个人密码输入不足12位时，需要按【确认/Confirm】键继续下一步操作。当输入密码达到12位时，系统自动进入下一步操作，不需要按【确认/Confirm】键。



图3 ATM 个人密码输入画面

10.5 功能选择画面

输入个人密码后，显示图4所示画面。

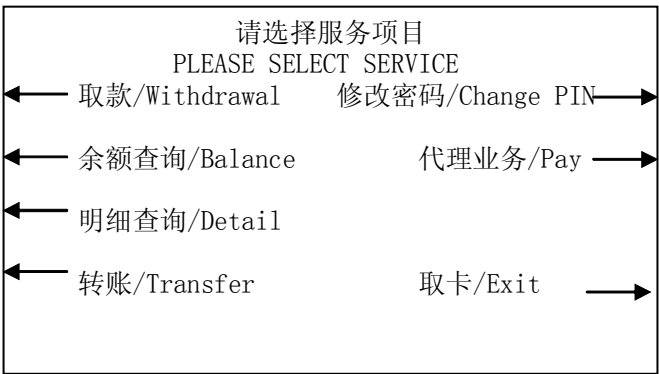


图4 ATM 功能选择画面

10.6 账户选择画面

此画面为可选画面，在持卡人输入密码后，可以显示图5所示画面，持卡人可以在此选择对应的银行卡种类。

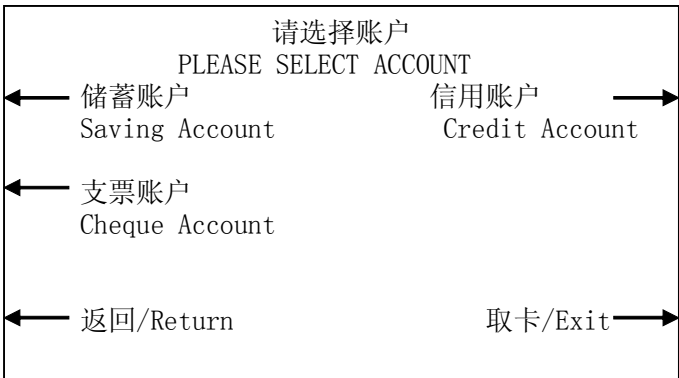


图5 ATM 账户选择画面

10.7 快速取款画面

功能选择画面中选择【取款/Withdrawal】功能后，显示图6所示画面。



请选择取款金额		
Express Withdrawal		
← 100		1000 →
← 200		1500 →
← 500	输入金额/Key in amount	→
← 800		取卡/Exit →

图6 ATM 快速取款画面

## 10.8 输入取款金额画面

在ATM快速取款画面选择【输入金额/Key in amount】功能后，显示图7所示画面。  
取款的最大限额可以在配置文件中通过参数进行设置，程序启动时必须读取该参数。

本次取款最大限额为	<input type="text"/>
(High Amount Limit)	
请输入取款金额	<input type="text"/>
(Please key in amount)	
本机此时能够提供以下面额纸币	→
人民币 XX 元 人民币 XX 元 人民币 XXX 元	
确认/Confirm	→
(RMB ¥XX ¥XX ¥XXX notes)	

图7 ATM 输入取款金额画面

## 10.9 余额查询输出画面

功能选择画面中选择【余额查询/Balance】功能后，接收到成功应答报文后显示图8所示画面。该画面显示两个余额，即账户余额和当日可用余额，如果选择【继续/Continue】，返回ATM功能选择画面。

账户余额：
(Amount Balance)
当日可用余额：
(Available Amount Balance)
继续/Continue →
取卡/Exit →

图8 ATM 余额查询输出画面

## 10.10 明细查询输出画面

功能选择画面中选择【**明细查询/Detail**】功能（及账户）后，显示图9所示画面，其中交易按照交易时间降序排列，最近发生的一笔成功交易显示在第一行，依次排列。日期采用8位显示YYYYMMDD，币种采用英文缩写表示，交易金额和余额精确到分。如果选择【**继续/Continue**】，返回ATM功能选择画面。

交易类型应该用中文表示，目前支持“取款”、“存款”、“消费”、“转账”、“预授权”、“代理业务”等交易。

图9 ATM 明细查询输出画面

10.11 提示信息画面

交易成功或出现任何异常情况时，显示图10所示画面，提示信息由交易的应答码（即报文的39号域的值）决定。如果个人密码错，返回图3重新输入个人密码继续按提示操作。如果选择【**继续/Continue**】，返回图4ATM功能选择画面。

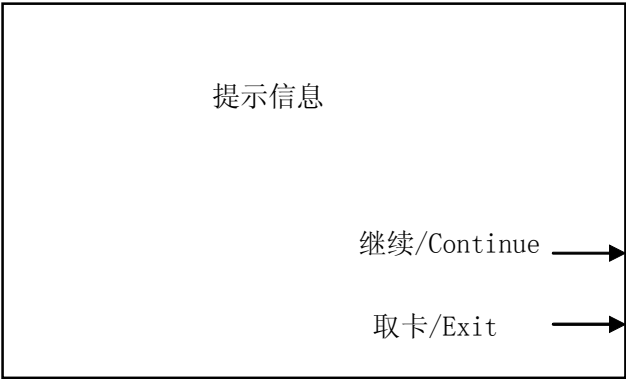


图10 ATM 提示信息画面

注： 无论何种交易，若ATMP返回需吞卡，屏幕需显示相应吞卡提示并打印含有完整卡号的ATM客户凭证，无须选择是否打印ATM客户凭证。

其它提示信息具体内容详见附录C：ATM终端显示规定。

10.12 取卡画面

除吞卡情况外，持卡人选【**取卡/Exit**】功能键时，ATM机需显示图11所示画面并吐出卡片。



图11 ATM 取卡画面

#### 10.13 操作等待画面

输入取款金额、输入转出金额、选择【余额查询/Balance】等功能选项后，在等待ATMP返回信息时，显示图12所示画面。



图12 操作等待画面

#### 10.14 等待客户取钞画面

取款交易成功，ATM终端点钞成功后，ATM吐钞并向ATMP发送取款确认报文，显示图13所示画面。



图13 ATM 等待客户取钞画面

#### 10.15 打印客户凭证画面

在进行需要打印凭证的交易成功时，显示图14所示画面，供客户选择是否打印凭证，如果选择【是/Yes】键后，ATM终端打印并吐出凭证，暂停五秒钟后返回图4：ATM功能选择画面。

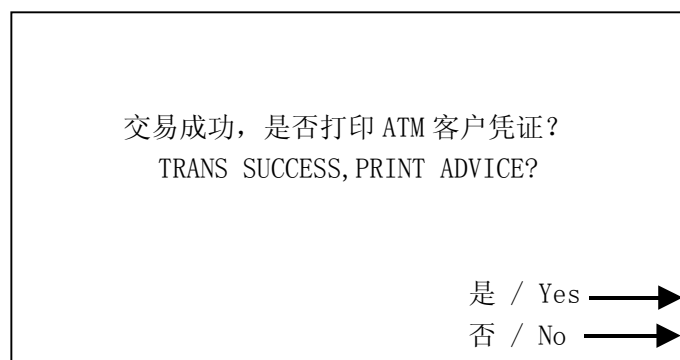


图14 ATM 打印客户凭证画面

#### 10.16 第一次输入新个人密码画面

选择【修改密码/Change PIN】功能键, 提示持卡人第一次输入新的个人密码, 显示图15所示画面。



图15 ATM 第一次输入新个人密码画面

#### 10.17 再次输入新个人密码画面

再次输入新个人密码, 显示图16所示画面。

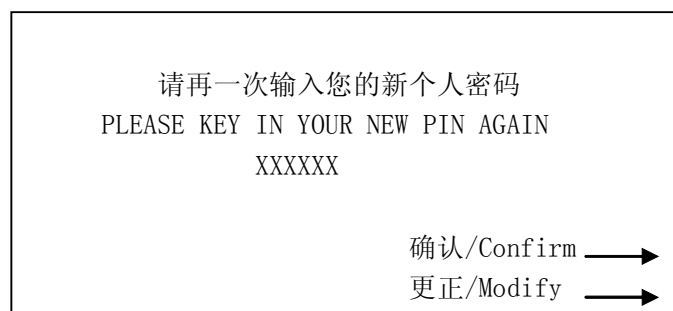


图16 ATM 再次输入新个人密码画面

#### 10.18 修改密码失败画面

如果两次输入的个人密码不正确, 显示图17所示画面。



图17 ATM 修改密码失败画面

#### 10.19 修改密码成功画面

如果修改密码成功，显示图18所示画面。



图18 ATM 修改密码成功画面

#### 10.20 第一次输入转入账号画面

选择『转账/Transfer』功能后，显示图19所示画面。



图19 ATM 第一次输入转入账号画面

#### 10.21 再次输入转入账号画面

再次输入转入账号画面如图20所示。



图20 ATM 再次输入转入账号画面

10.22 输入转出金额画面

如果两次输入的账号不一致，则提示重新输入。如果两次输入的账号一致，按【确认/Confirm】键后，显示图21所示画面，显示转入账号，持卡人输入转出金额。

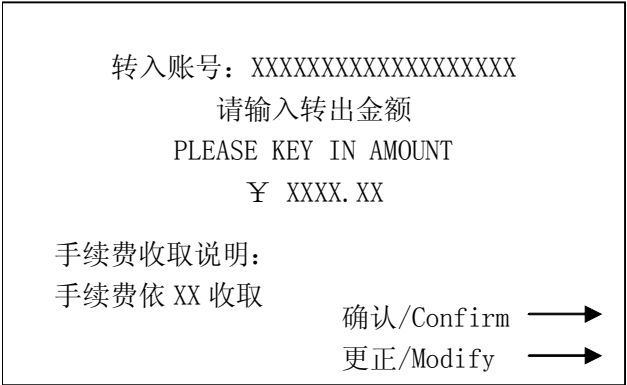


图21 ATM 输入转出金额画面

10.23 代理业务种类选择画面

功能选择画面中选择【代理业务/Pay】功能后，显示ATM上能够支持的代理业务种类，供持卡人选择，考虑到代理业务的多样性，种类较多，一个屏幕无法放置所有的交易选择，所以代理业务种类选择的画面由多个画面组合而成，下面以实现14个代理业务种类选择的ATM画面为例说明该画面的实现。

在所有的页面中最多只放置6个代理业务选择项，另在首页和尾页提供【返回/Return】按键，持卡人点击后返回图4。

10.23.1 代理业务种类选择画面—首页

如果代理业务种类选择不超过6个，则图22所示画面上不出现【下一页/Next】按键。

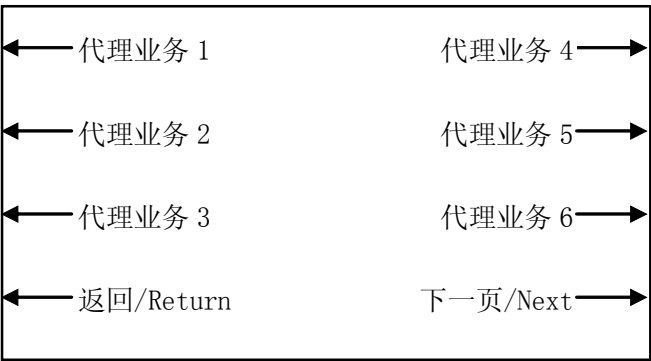


图22 代理业务种类选择画面—首页

### 10.23.2 代理业务种类选择画面—中间页

如果代理业务种类较多，可以出现多个中间页，页面布局一致，如图23所示。

← 代理业务 7	代理业务 10 →
← 代理业务 8	代理业务 11 →
← 代理业务 9	代理业务 12 →
← 上一页/Previous	下一页/Next →

图23 代理业务种类选择画面—中间页

### 10.23.3 代理业务种类选择画面—尾页

代理业务种类选择的尾页画面如图24所示。

← 代理业务 13	
← 代理业务 14	
← 上一页/Previous	返回/Return →

图24 代理业务种类选择画面—尾页

### 10.24 代缴费—输入客户号画面

选择代理业务种类后，如果是代缴费交易则显示图25所示画面，持卡人输入对应的客户号，按【确认/Confirm】后，提交查询。

代理业务种类: XXXXXX	
请输入客户号:	<input type="text"/>
	确认/Confirm →
	更正/Modify →

图25 代缴费—输入客户号画面

### 10.25 代缴费—查询金额输出画面

输入代缴费客户号后，如果代缴费信息查询成功则显示图26所示画面。持卡人按【缴费确认/Confirm】后，提交进行实时缴费交易。

代理业务种类: XXXXX  
客户号: XXXXXXXXXX  
应缴费: XXXX. XX

缴费确认/Confirm →  
取消/Cancel →

图26 代缴费—查询金额输出画面

10.26 充值—客户输入画面

对于充值类的代理业务交易，显示图27所示画面，供持卡人输入相应代理业务的客户号和充值金额后。持卡人在输入所要充值的客户号和金额后，按【确认/Confirm】后，提交进行充值交易。

代理业务种类: XXXXX  
客户号:   
充值金额:

确认/Confirm →  
取消/Cancel →

图27 充值—客户输入画面

10.27 缴费—客户输入画面

对于缴费类的代理业务交易，显示图28所示画面，供持卡人输入缴费金额。持卡人在输入缴费金额后，按【确认/Confirm】后，提交进行缴费交易。

种类:  客户号:   
应缴费:  金额  
请输入缴费金额 (至少大于应缴费金额)

确认/Confirm →  
取消/Cancel →

图28 缴费—客户输入画面

11 ATM 终端交易处理流程

11.1 业务类交易

11.1.1 卡介质的判断及处理流程

插卡、语言选择



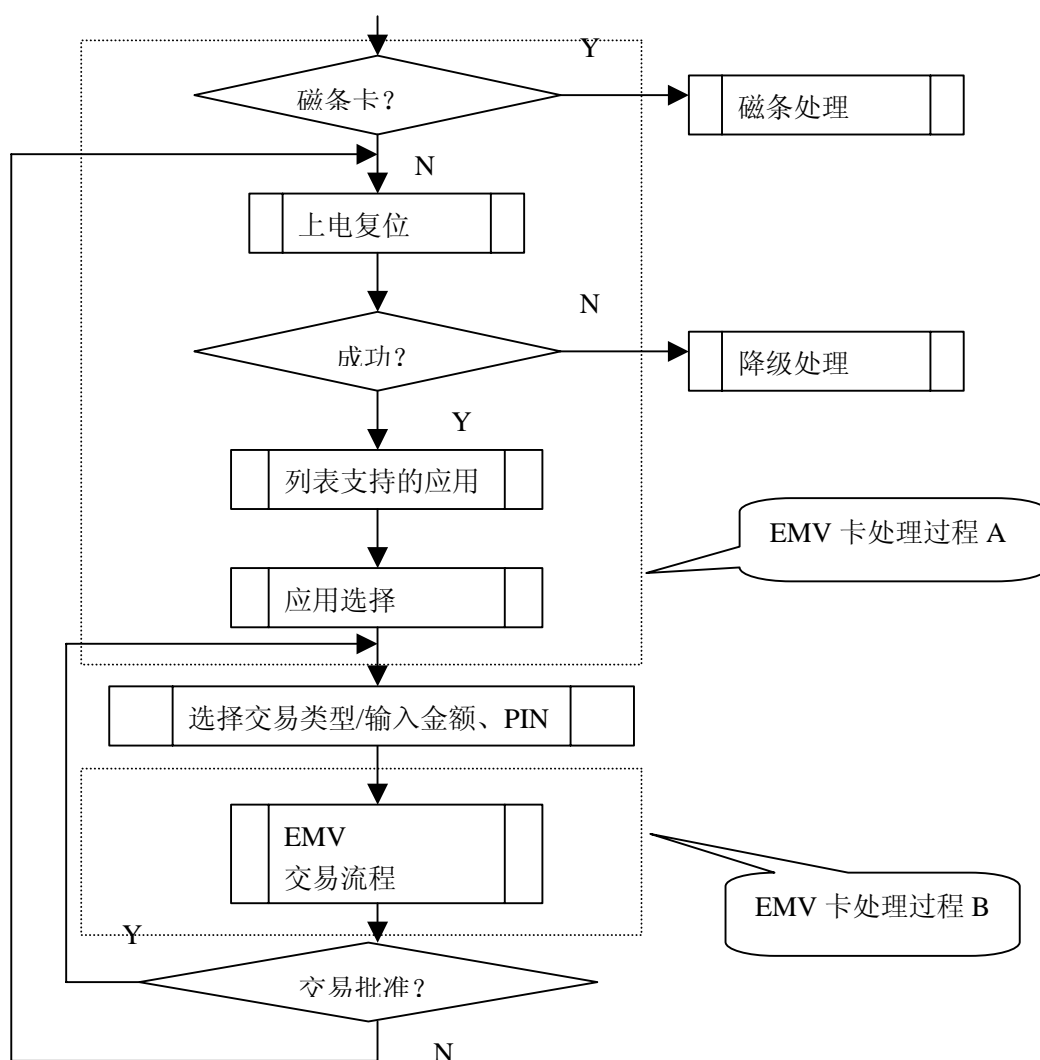


图29 卡介质判断及处理流程

#### 11.1.1.1 卡介质判断

由于 ATM 同时支持 EMV 卡交易，ATM 应该根据磁条的服务代码判断卡介质。用户插卡并进行语言选择后，ATM 先读磁条，根据磁条服务代码，ATM 判断卡片是 EMV 卡还是磁条卡，如果是磁条卡就按正常的磁条卡交易流程处理，否则转 11.1.1.2。

#### 11.1.1.2 EMV 卡处理过程 A

如果是 EMV 卡，ATM 应按 EMV2000 和 PBOC 有关规定要求开始读芯片卡并进行应用列表，其间如果发生非卡锁定或应用锁定的读卡错，应允许降级交易。降级交易处理过程同磁条卡交易，但应按规定填写报文。

如果没有进入降级交易，ATM 进入应用选择，终端应优先选择 PBOC 应用。如果没有共同支持的应用，终端将进入降级交易处理。应用选择过程严格按照 EMV2000 和 PBOC 有关规定。应用选择期间发生的非卡锁定、非应用锁定的读卡错或应用选择错应允许降级交易。降级交易处理过程同磁条卡交易，但应按规定填写报文。

在需要用户参与的应用选择或继续交易界面应同时允许退出交易，如下图所示：

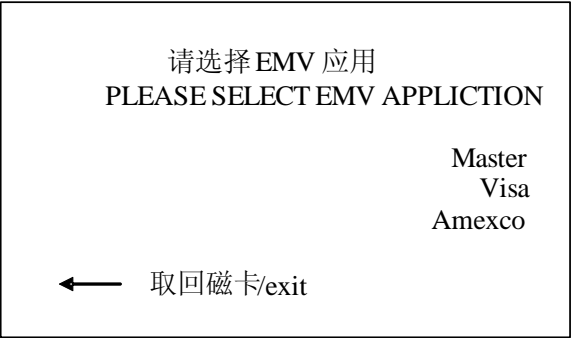


图30 应用选择界面

成功进行了应用选择后，转11.1.1.3，进入交易类型、交易金额及PIN的输入过程。

11.1.1.3 交易类型、交易金额及 PIN 的输入

用户进行交易类型、交易金额及PIN的输入，必须在客户选择EMV应用后，确定相应的Track2信息及账号信息后，方可进行密码的输入。该过程同磁条卡处理，之后根据交易类型转11.1.1.4，进入EMV卡处理过程B。

11.1.1.4 EMV 卡处理过程 B

在EMV卡处理过程中，根据交易类型，有两种EMV交易流程：完整的EMV交易流程和简化的EMV交易流程。

简化的EMV交易流程仅包括应用初始化和读应用数据，不包括后续步骤。简化的EMV流程如下图所示：

本规范规定查询交易采用简化的EMV流程。

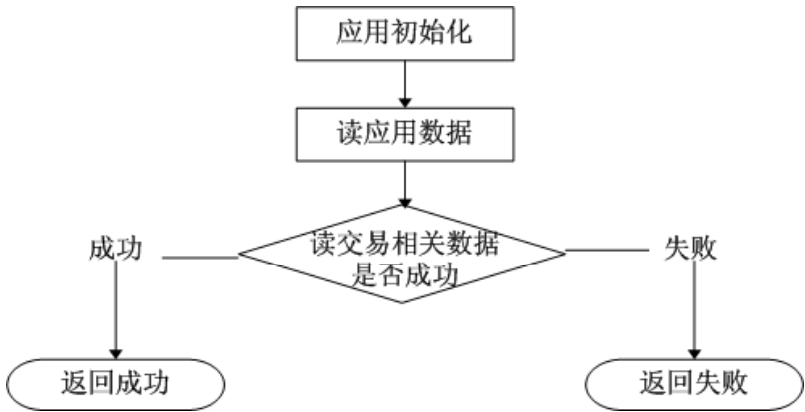


图31 简化的 EMV 流程

完整的EMV交易流程包括从应用初始化到最终的交易完成。如下图所示：  
本规范规定取款、转账交易采用完整的EMV流程。

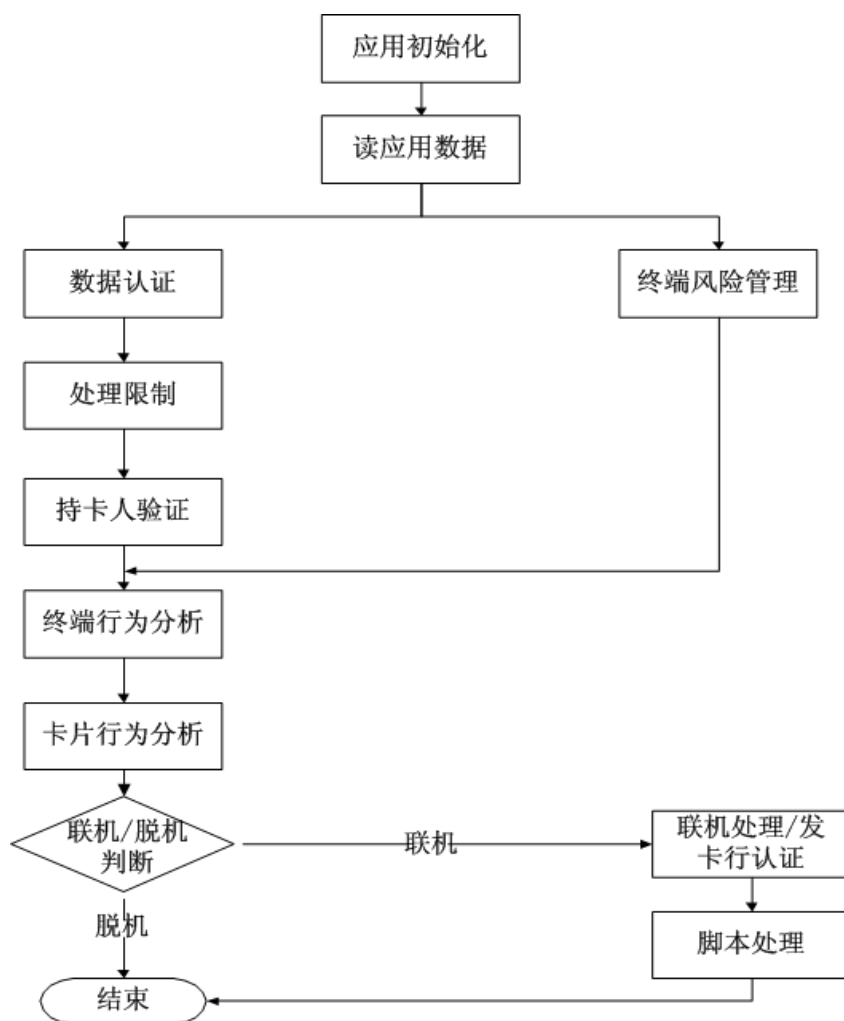


图32 完整的 EMV 流程

对于EMV卡转账交易，由于CUPS不支持转账交易的受理方冲正，故对CUPS应答批准的转账交易如果卡最终没有批准，终端应显示成功并上送AAC（同TC上送），同时业务上应不允许转账交易的AAC原因退单。

#### 11.1.1.5 EMV 交易流程结束后的处理

EMV交易正常结束后如果交易批准应安全保留PIN，并返回到成功应用选择之后的步骤，进行交易类型选择并进行新的交易，在流程需要验证PIN时自动使用保留的PIN。

EMV交易失败后应返回列表支持的应用开始处理。

对联机批准而卡最终拒绝的交易，ATM应该冲正。

#### 11.1.2 主要交易的处理流程

持卡人在ATM终端上进行的业务类交易的操作流程，其主要处理流程如图33所示：

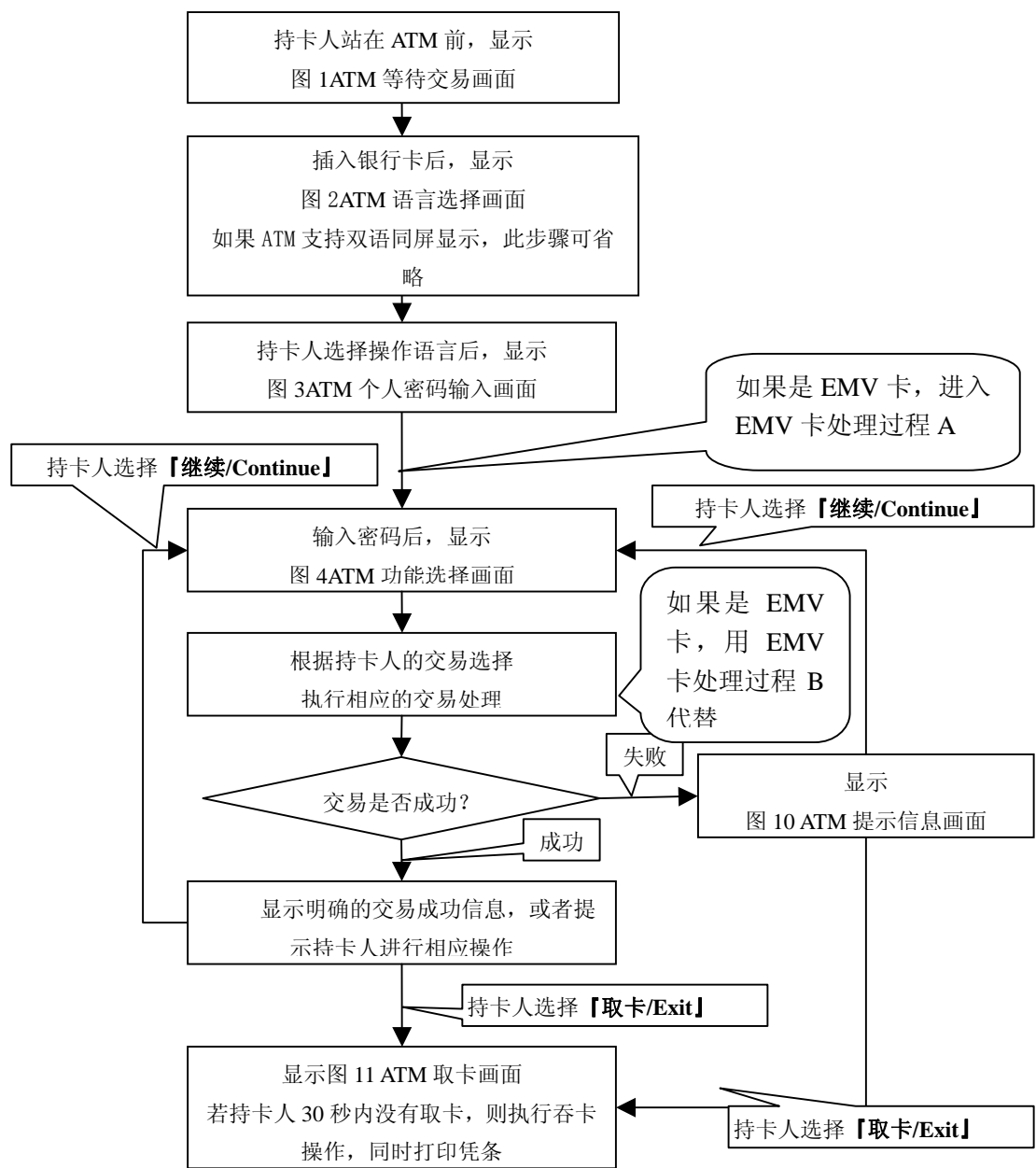


图33 ATM 业务类交易主要流程

其中，在持卡人选择语言后应进入EMV卡处理过程A，如果是EMV卡，在交易金额、交易类型及PIN输入后应进入EMV卡处理过程B。

#### 11.1.2.1 取款

[操作步骤] 见图34：取款交易。

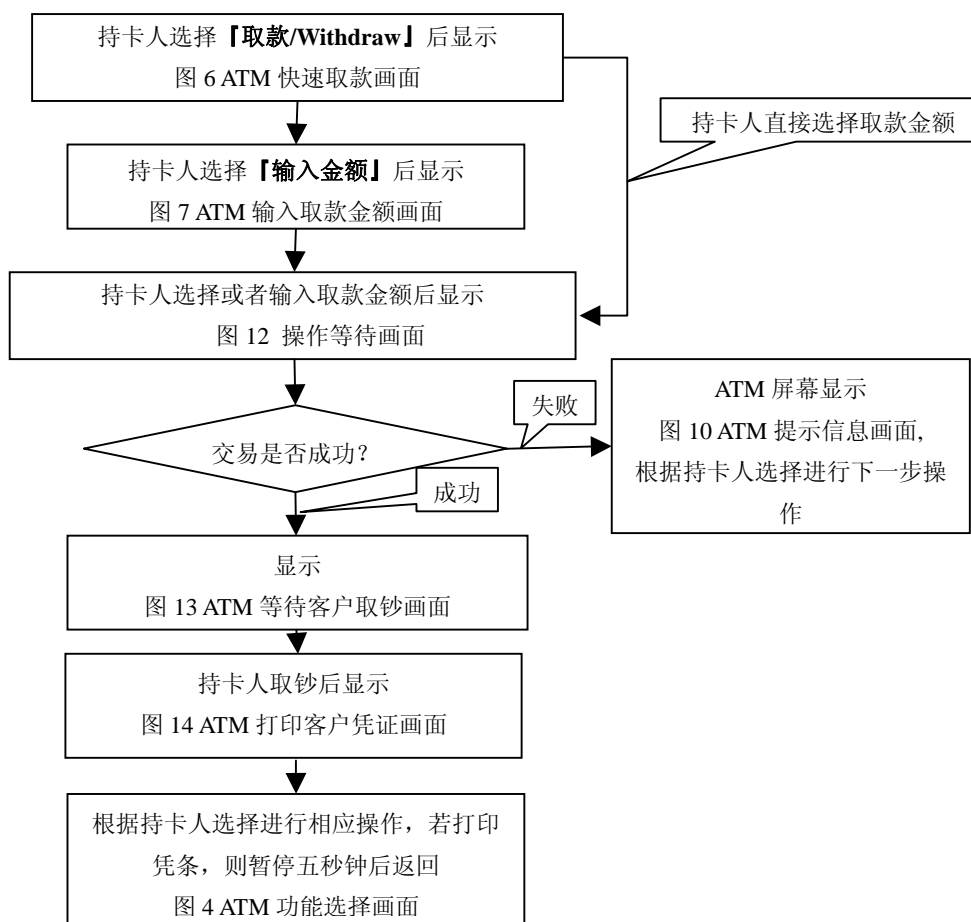


图34 取款交易

## 11.1.2.2 余额查询

[操作步骤] 见图35 余额查询交易。

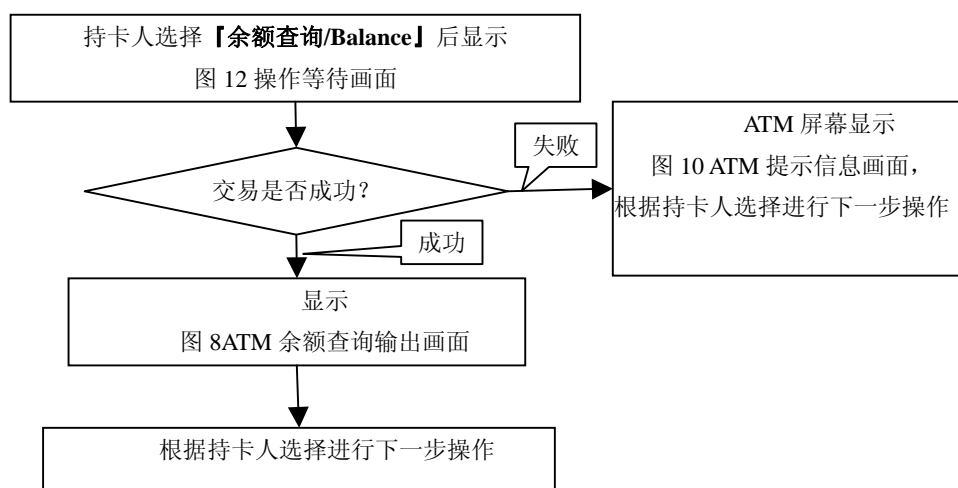


图35 余额查询交易

## 11.1.2.3 账户明细查询

[操作步骤] 与图35 余额查询交易一致。

## 11.1.2.4 修改密码

[操作步骤] 见图36 修改密码交易。

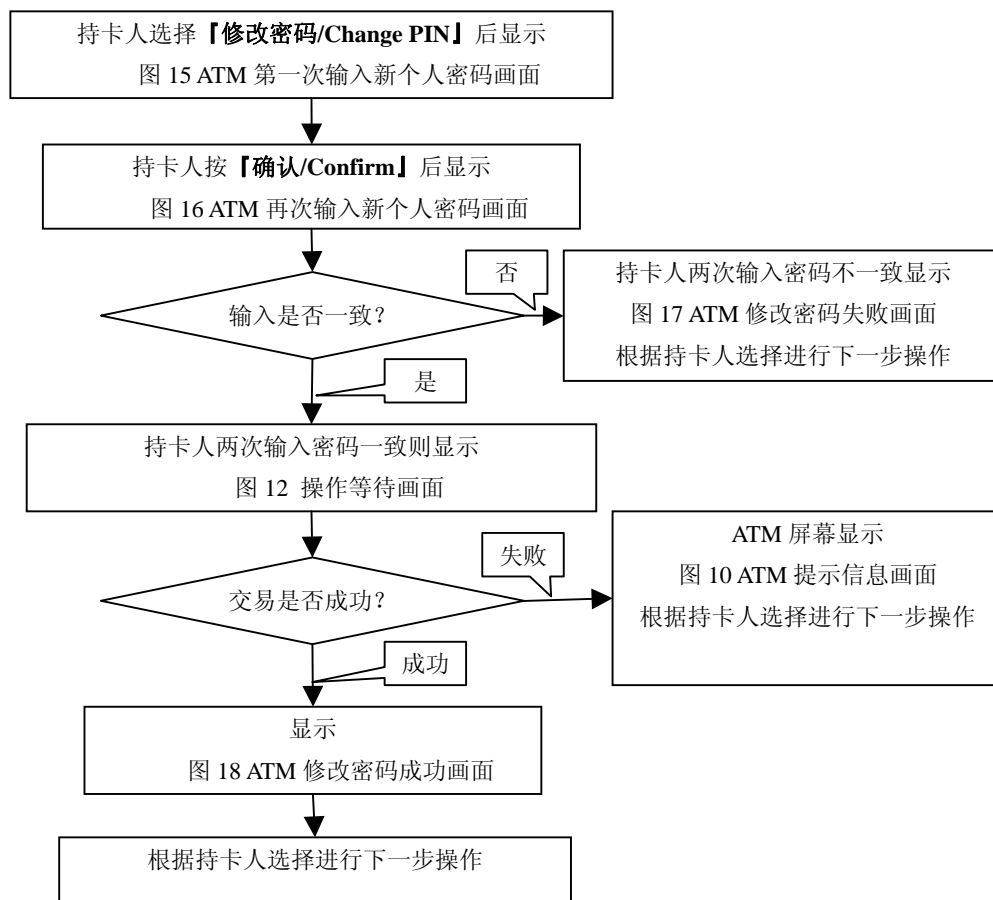


图36 修改密码交易

#### 11.1.2.5 转账

[操作步骤] 见图37 转账交易。

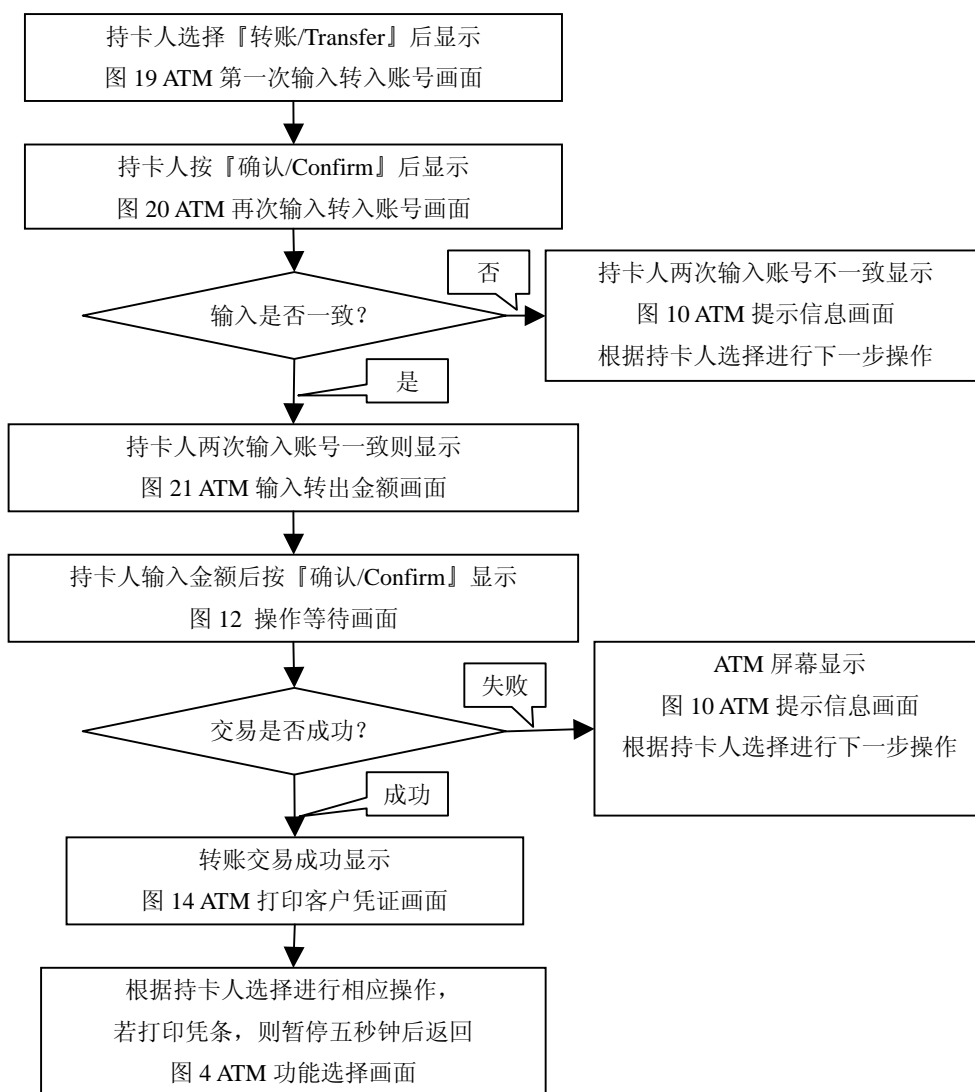


图37 转账交易

对EMV卡转账, 由于受理方不能对承兑的交易做冲正, 对ATMP应答的承兑转账交易, 如果卡最终没能批准, 终端应显示转账成功, 并上送TC (AAC), 发卡方不能以转账交易的AAC做为退单理由。

#### 11.1.2.6 代理业务一代缴费

[操作步骤] 见图38 代缴费交易。

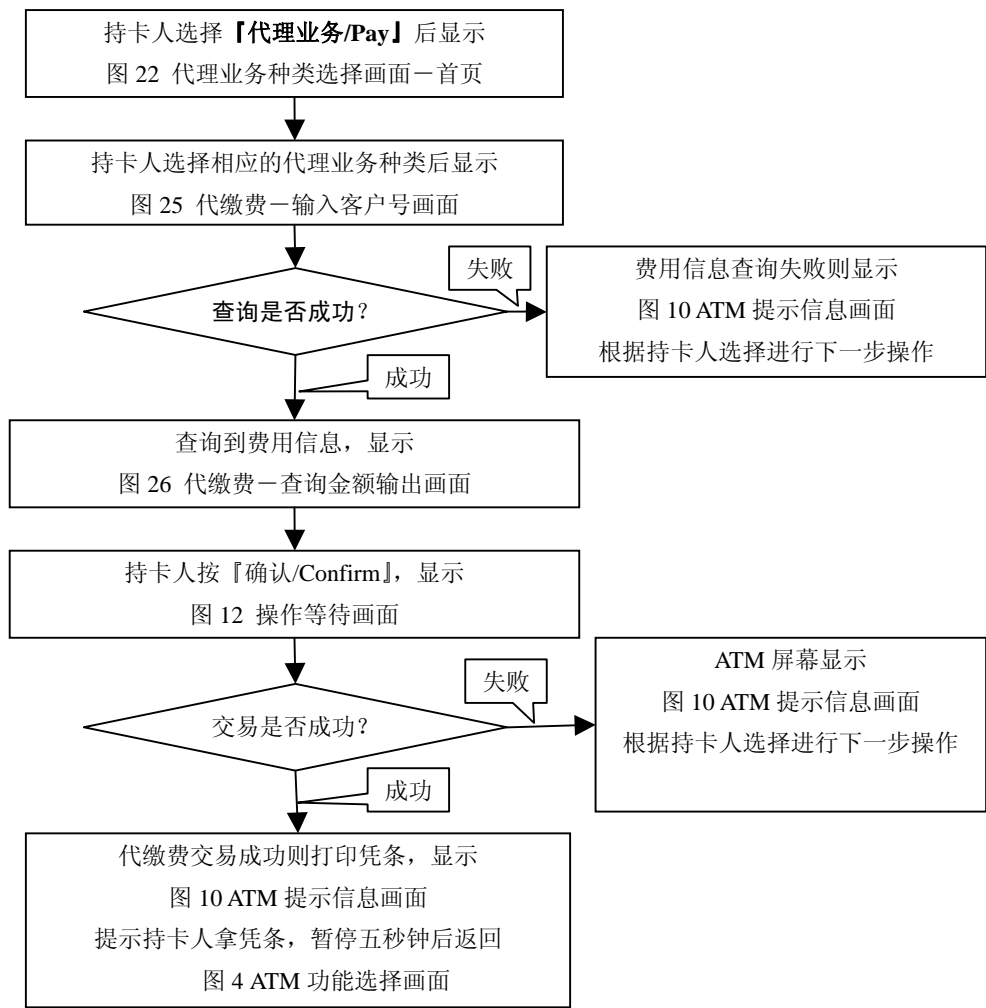


图38 代缴费交易

#### 11.1.2.7 代理业务—充值

[操作步骤] 见图39 充值交易。

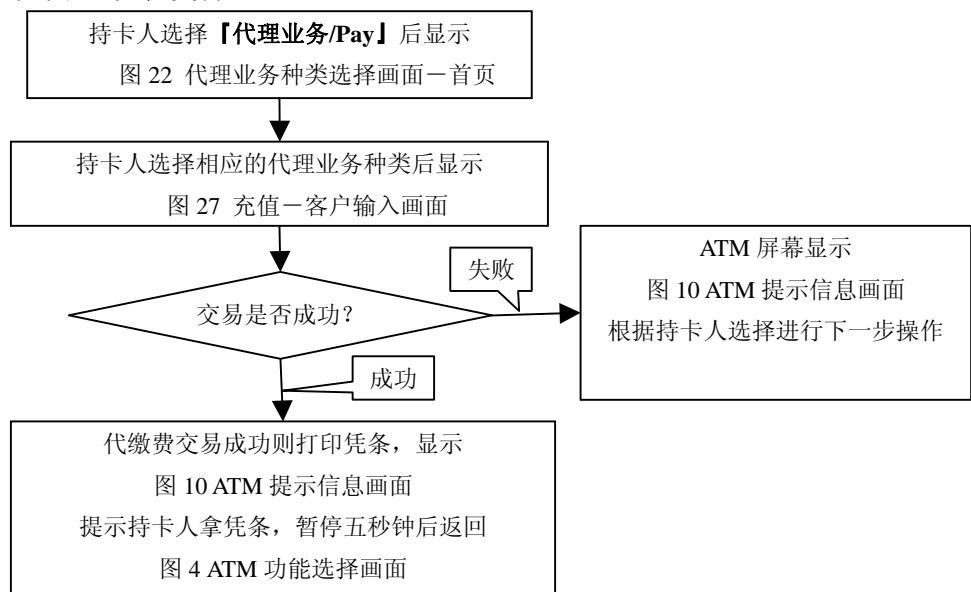


图39 充值交易



## 11.2 主动管理类交易

### 11.2.1 设备签到

ATM发送签到请求后，ATMP对签到报文的终端信息进行合法性检查，若是合法终端则允许该设备进行交易，否则签到失败。

[操作步骤] 见图40 设备签到流程。

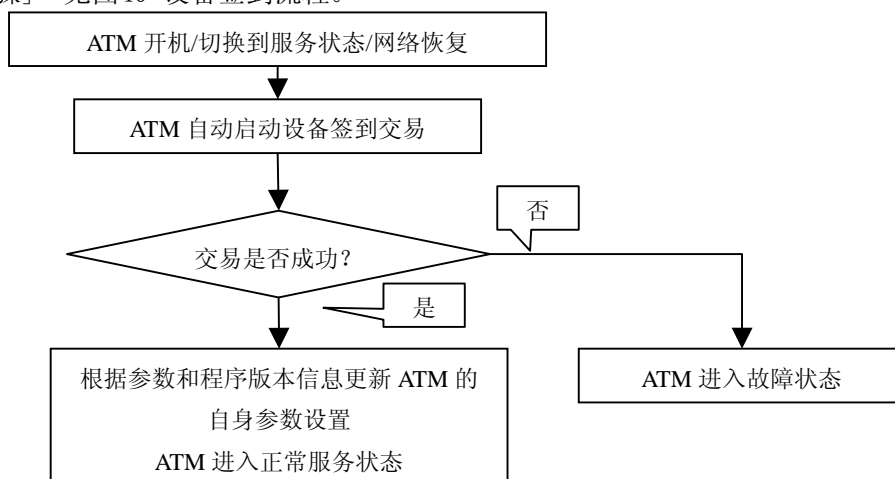


图40 设备签到流程

### 11.2.2 加钞通知

[操作步骤] 见图41 加钞通知。

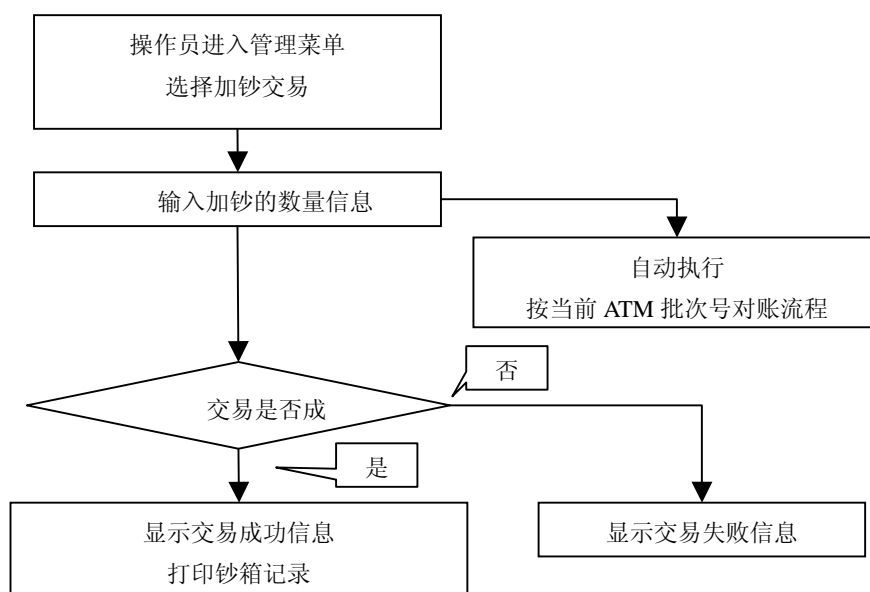


图41 加钞通知

### 11.2.3 定时状态报告

ATM能够根据事先设定的时间间隔，定时将自身状态上送ATMP。只有当ATM处于空闲状态时，系统才进行计时，定时发送状态报告。当有交易发生时，计时自动停止，待客户交易完毕后再重新计时。时间间隔可以根据ATMP下传的参数进行更新。

[操作步骤] 见图42 定时状态报告。

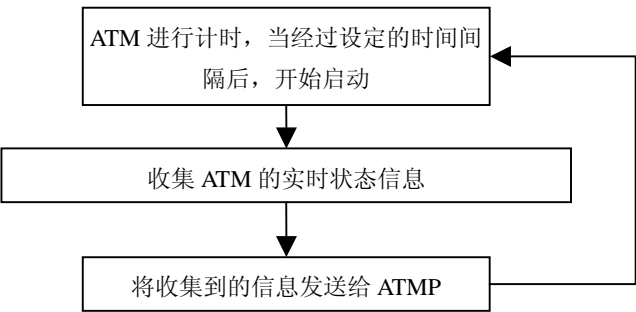


图42 定时状态报告

11.2.4 状态切换报告

[操作步骤] 如图43所示，ATM能够将自身的状态变化信息在状态切换完成后上送ATMP。

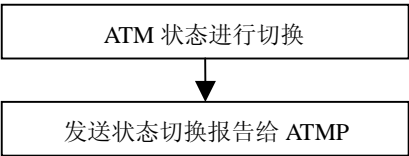


图43 状态切换报告

11.2.5 故障通知

ATM出现故障后，应自动向ATMP发送故障代码，无须人工操作。当以下ATM部件出现故障时需要发送故障通知。

- 硬件加密机
- 凭条打印模块
- 流水打印模块
- 磁卡读写器
- 出钞模块
- 机箱门

[操作步骤] 见图44 故障通知。

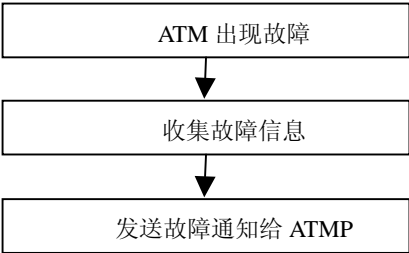


图44 故障通知

11.2.6 提醒通知

当ATM检测到自身钞箱现金、打印凭证数量等到达预警值后，应能自动发送提醒通知，无须人工操作。

[操作步骤] 见图45 提醒通知。

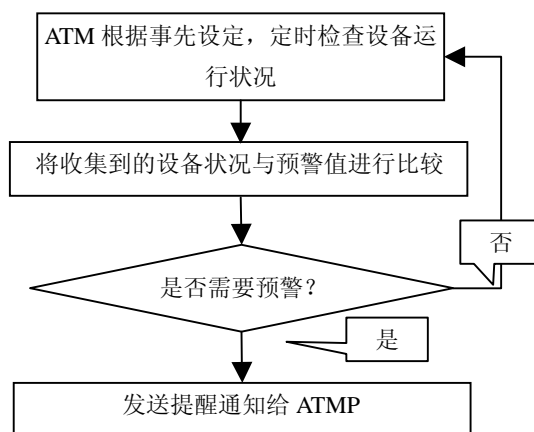


图45 提醒通知

### 11.2.7 吞卡通知

ATM出现吞卡情况后, 应能自动发送吞卡通知, 无须人工操作。无论何种交易, 若ATMP返回需吞卡, 或者用户操作超时, 屏幕需显示相应吞卡提示并打印含有完整卡号的ATM客户凭证, 无须选择是否打印ATM客户凭证。ATM吞卡后, 自动将卡号等信息发送给ATMP。

[操作步骤] 见图46 吞卡通知。

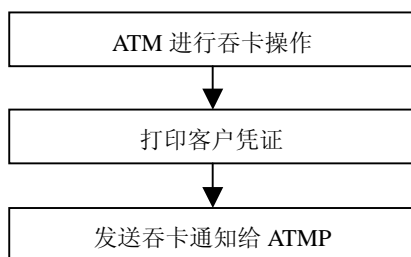


图46 吞卡通知

### 11.2.8 对账

[操作步骤] 见图47 对账。

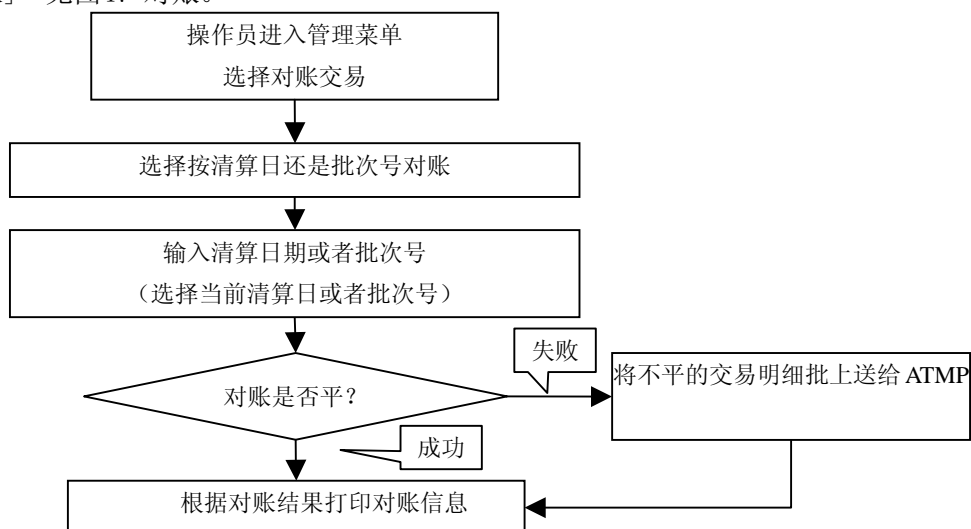
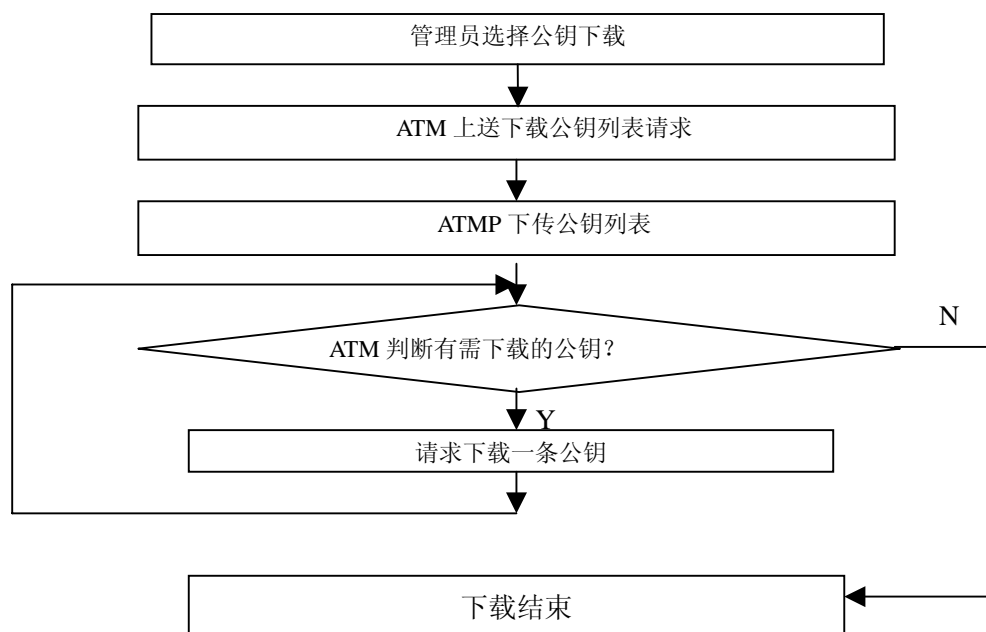
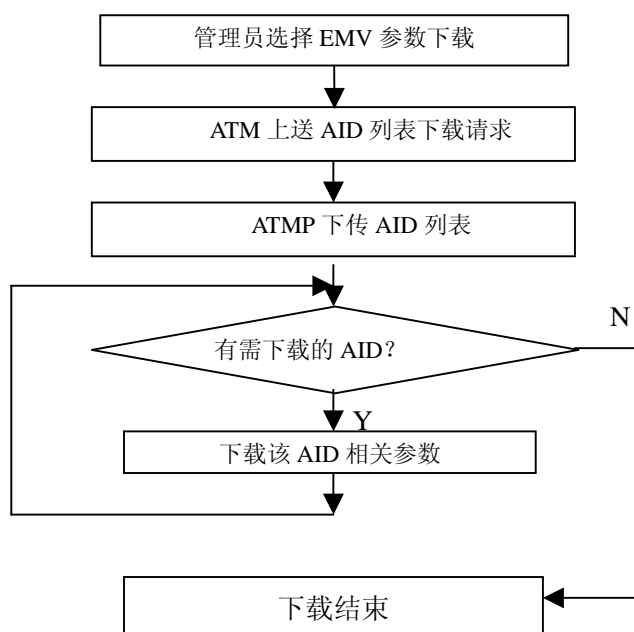


图47 对账

### 11.2.9 EMV 卡交易公钥下载



#### 11.2.10 EMV 卡交易参数下载



### 11.3 被动管理类交易

ATMP发起的管理交易都由ATM自动响应和操作，所以在管理菜单中不需设置相应菜单。以下交易都需在ATM设备签到成功后才能进行。

#### 11.3.1 打开 ATM 终端

[操作步骤] 见图48 打开ATM终端。

当ATM处于开机状态时，收到ATMP的开机指令，应返回操作成功的报文。

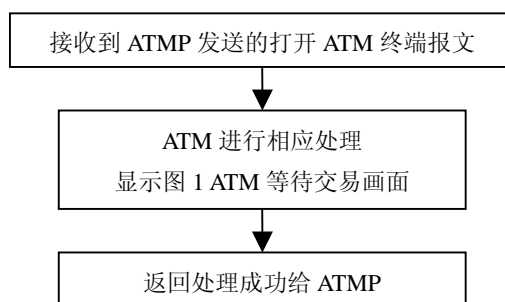


图48 打开 ATM 终端

### 11.3.2 关闭 ATM 终端

当ATM处于关闭状态时，收到ATMP的关闭指令，应返回操作成功的报文。

[操作步骤] 见图49 关闭 ATM终端。

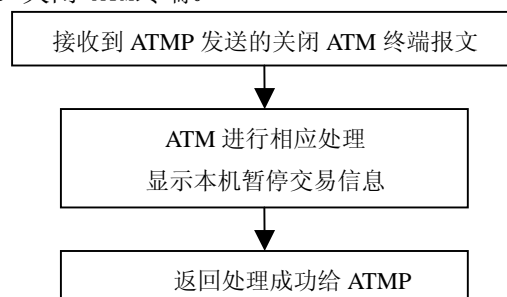


图49 关闭 ATM 终端

### 11.3.3 ATM 设备查询

[操作步骤] 见图50  
ATM设备查询。

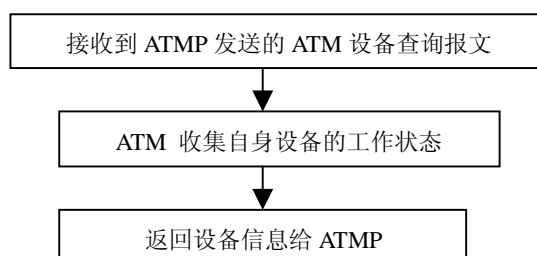


图50 ATM 设备查询

### 11.3.4 参数下载

[操作步骤] 见图51 参数下载。

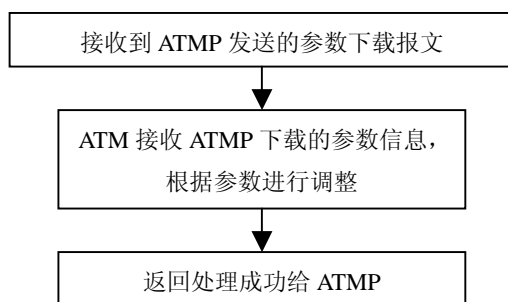


图51 参数下载

### 11.3.5 通知上传交易明细

[操作步骤] 见图52 通知上传交易明细。

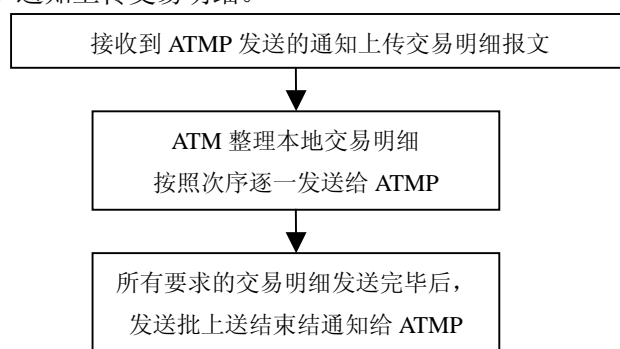
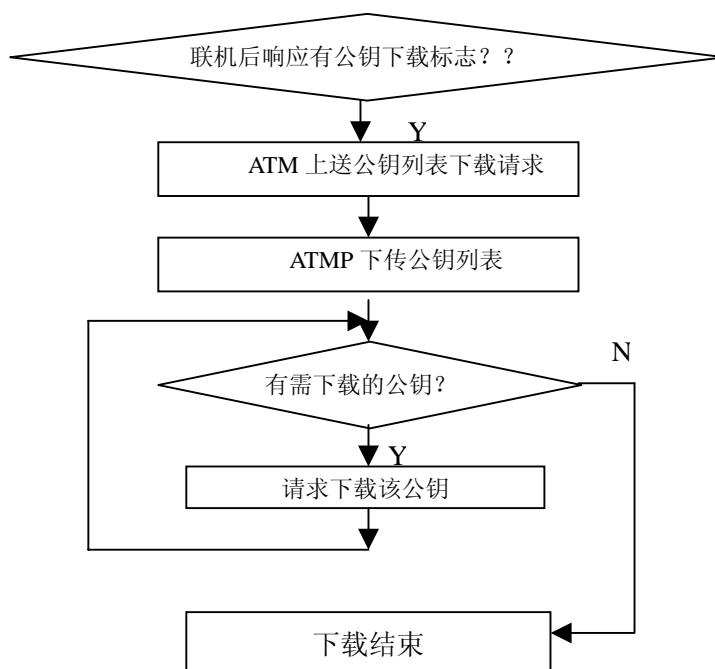
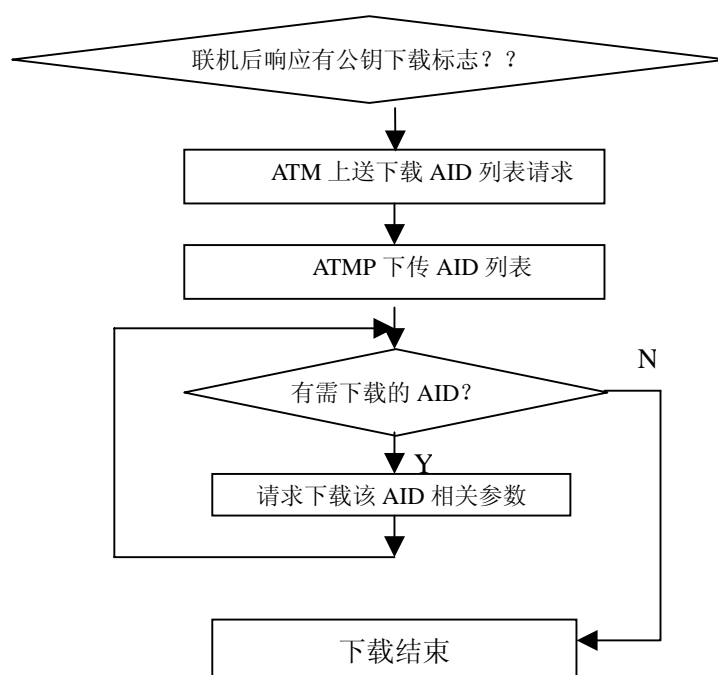


图52 通知上传交易明细

### 11.3.6 EMV 卡交易公钥下载



### 11.3.7 EMV 卡交易参数下载



## 12 报文的匹配

### 12.1 关键信息域与报文的关联

关键信息域(Key Field)被用来识别和匹配交易。ATM必须使用这些关键域匹配交易的请求和应答、原始交易和关联交易。

当ATM发现一笔取款交易处理或传输出错时，可以产生一个用于更正的报文，如出钞设备出故障，ATM产生一笔取款冲正。

在ATM中关联交易主要是指取款交易和取款冲正交易。

### 12.2 关键信息域的匹配

#### 12.2.1 授权类交易

响应消息0110必须与请求消息0100匹配的关键信息域：

- 交易日期时间（域 7）
- 系统跟踪号（域 11）
- 终端标识符（域 41）

#### 12.2.2 查询交易

响应消息0210必须与请求消息0200匹配的关键信息域：

- 交易日期时间（域 7）
- 系统跟踪号（域 11）
- 终端标识符（域 41）

#### 12.2.3 金融交易

响应消息0210必须与请求消息0200匹配的关键信息域：

- 交易日期时间（域 7）
- 系统跟踪号（域 11）
- 终端标识符（域 41）

## 12.2.4 冲正通知

通知请求消息0420必须与原交易消息匹配的关键信息域：

——终端标识符（域 41）

——原始数据元（域 90）：从原始交易中提取组成

响应消息0430必须与请求消息0420匹配的关键信息域：

——交易日期时间（域 7）

——系统跟踪号（域 11）

——终端标识符（域 41）

## 12.2.5 对账交易

响应消息0520必须与请求消息0530匹配的关键信息域：

——交易日期时间（域 7）

——系统跟踪号（域 11）

——终端标识符（域 41）

## 12.2.6 网络管理通知交易

响应消息0830必须与请求消息0820匹配的关键信息域：

——交易日期时间（域 7）

——系统跟踪号（域 11）

——终端标识符（域 41）

## 12.3 交易对报文域的基本要求

## 12.3.1 业务类交易

## 12.3.1.1 ATM 余额查询

ATM余额查询的关键域要求见表3。

表3 ATM 余额查询的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0200/0210
处理码必须指明为余额查询	域 3：30x000
请求中金额不出现	域 4 不出现
刷卡交易	域 35、36 必须提供
需要 PIN	域 52、53 必须出现
成功应答中需返回余额	在成功应答报文中域 54 出现

## 12.3.1.2 ATM 明细查询

ATM明细查询的关键域要求见表4。

表4 ATM 明细查询的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0200/0210
处理码必须指明为明细查询	域 3：39x000
请求中金额不出现	域 4 不出现
刷卡交易	域 35、36 必须提供
需要 PIN	域 52、53 必须出现
请求中指明明细查询类型和成功应答中返回明细响应数据	域 59 必须出现

## 12.3.1.3 ATM 取款（含取款确认）

ATM取款（含取款确认）的关键域要求见表5。

表5 ATM 取款（含取款确认）的关键域要求



关键域的要求	关键域的取值
报文类型必须指明	0200/0210
处理代码必须指明是取款交易	域 3: 01x000
请求中指明金额	域 4 必须出现
刷卡交易	域 35、36 必须提供
需要 PIN	域 52、53 必须出现

#### 12.3.1.4 ATM 转账

ATM转账的关键域要求见表6。

表6 ATM 转账的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0200/0210
处理码必须指明是转账交易	域 3: 40x000
请求中指明转账金额	域 4 必须出现
刷卡交易	域 35、36 必须提供
需要 PIN	域 52、53 必须出现
说明转入和转出账户	域 102、103 必须出现

#### 12.3.1.5 修改密码

修改密码的关键域要求见表7。

表7 修改密码的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0100/0110
处理代码指明是修改密码交易	域 3: 70x000
刷卡交易	域 35、36 必须提供
需要 PIN	域 48、52、53 必须出现
交易金额域必须不存在	域 4 必须不存在

#### 12.3.1.6 ATM 代缴费查询

ATM代缴费查询的关键域要求见表8。

表8 ATM 代缴费查询的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0200/0210
处理代码必须指明是代缴费查询	域 3: 31x000
刷卡交易	域 35、36 必须提供
代缴费信息	域 48, 用法一

#### 12.3.1.7 ATM 实时缴费和充值

ATM实时缴费和充值的关键域要求见表9。

表9 ATM 实时缴费和充值的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0200/0210
处理代码必须指明是代缴费	域 3: 19x000
刷卡交易	域 35、36 必须提供
需要 PIN	域 52、53 必须出现
代缴费信息	域 48, 用法一

## 12.3.2 主动管理类

## 12.3.2.1 签到

签到的关键域要求见表10。

表10 签到的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
必须提供软件和参数版本号	域 48，用法五、用法六
网络管理码域必须指明	域 70：001、003

## 12.3.2.2 加钞通知

加钞通知的关键域要求见表11。

表11 加钞通知的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
说明加钞数量，并返回批次号	域 48，用法二
网络管理码域必须指明	域 70：261

## 12.3.2.3 批上送交易明细

批上送交易明细的关键域要求见表12。

表12 批上送交易明细的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
交易明细数据	域 48，用法八
网络管理码域必须指明	域 70：271

## 12.3.2.4 批上送结束

批上送结束的关键域要求见表13。

表13 批上送结束的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
批上送统计信息	域 48，用法九
网络管理码域必须指明	域 70：272

## 12.3.2.5 定时状态报告

定时状态报告的关键域要求见表14。

表14 定时状态报告的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
设备状态信息	域 48，用法三
网络管理码域必须指明	域 70：361

## 12.3.2.6 状态切换报告

状态切换报告的关键域要求见表15。

表15 状态切换报告的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
设备状态信息	域 48，用法三
网络管理码域必须指明	域 70：362

## 12.3.2.7 提醒信息报告

提醒信息报告的关键域要求见表16。

表16 提醒信息报告的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
设备状态信息	域 48，用法三
网络管理码域必须指明	域 70：363

## 12.3.2.8 故障信息报告

故障信息报告的关键域要求见表17。

表17 故障信息报告的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
设备状态信息	域 48，用法三
网络管理码域必须指明	域 70：364

## 12.3.2.9 吞卡信息报告

吞卡信息报告的关键域要求见表18。

表18 吞卡信息报告的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
说明被吞卡的卡号	域 2
网络管理码域必须指明	域 70：365

## 12.3.2.10 对账

对账的关键域要求见表19。

表19 对账的关键域要求

关键域的要求	关键域的取值
报文类型必须指明为对账	0520/0530
交易统计数据	域 48：用法七

## 12.3.2.11 EMV 交易 TC 上送

TC上送的关键域要求见表20。

表20 TC 上送的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
参数信息	域 48，用法十五
网络管理码域必须指明	域 70：095

## 12.3.2.12 EMV 脚本通知

EMV脚本通知的关键域要求见表21。

表21 EMV 脚本通知的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
参数信息	域 48, 用法十六
网络管理码域必须指明	域 70: 097

### 12.3.2.13 EMV 公钥列表下载

EMV公钥列表下载的关键域要求见表21。

表22 EMV 公钥列表下载的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
参数信息	域 48, 用法十一
网络管理码域必须指明	域 70: 091

### 12.3.2.14 单个 EMV 公钥数据下载

EMV公钥数据下载的关键域要求见表21。

表23 EMV 公钥数据下载的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
参数信息	域 48, 用法十三
网络管理码域必须指明	域 70: 091

### 12.3.2.15 EMV AID 列表下载

EMV AID列表下载的关键域要求见表21。

表24 EMV AID 列表下载的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
参数信息	域 48, 用法十二
网络管理码域必须指明	域 70: 093

### 12.3.2.16 单个 AID 相关参数修改

单个AID相关参数修改的关键域要求见表21。

表25 单个 AID 相关参数修改的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
参数信息	域 48, 用法十四
网络管理码域必须指明	域 70: 093

## 12.3.3 被动管理类

### 12.3.3.1 打开 ATM 终端

打开ATM终端的关键域要求见表26。

表26 打开 ATM 终端的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
网络管理码域必须指明	域 70: 081

### 12.3.3.2 关闭 ATM 终端

关闭ATM终端的关键域要求见表27。

表27 关闭 ATM 终端的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
网络管理码域必须指明	域 70: 082

## 12.3.3.3 设备状态查询

设备状态查询的关键域要求见表28。

表28 设备状态查询的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
设备状态信息	域 48, 用法三
网络管理码域必须指明	域 70: 381

## 12.3.3.4 参数下载

参数下载的关键域要求见表29。

表29 参数下载的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
参数信息	域 48, 用法四
网络管理码域必须指明	域 70: 090

## 12.3.3.5 通知上传交易明细

通知上传交易明细的关键域要求见表30。

表30 通知上传交易明细的关键域要求

关键域的要求	关键域的取值
报文类型必须指明	0820/0830
网络管理码域必须指明	域 70: 290

## 12.3.3.6 EMV 公钥列表下载

同主动管理。

## 12.3.3.7 单个 EMV 公钥数据下载

同主动管理。

## 12.3.3.8 EMV AID 列表下载

同主动管理。

## 12.3.3.9 单个 AID 相关参数修改

同主动管理。

## 13 消息域说明

## 13.1 说明

## 13.1.1 符号说明

表31给出本规范的消息域符号说明。

表31 消息域符号说明

符号	描述
a	字母字符, A 至 Z, a 至 z, 向左靠, 右边多余位填充格
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
n	数值, 0 至 9, 右靠, 首位有效数字前填零。若表示人民币金额, 则最右二位为角、分

符号	描述
p	打印字符，空格
s	特殊符号
an	字母和数字字符，左靠，右边多余位填充空格
as	字母和特殊字符，左靠，右边多余位填充空格
cn	压缩数字码，即 BCD 码
ns	数字和特殊字符，左靠，右边多余位填充空格
ans	字母、数字和特殊字符，左靠，右边多余位填充空格
MM	月份，01 至 12
DD	日期，01 至 31
YY	年份，00 至 99
hh	时，00 至 23
mm	分，00 至 59
ss	秒，00 至 59
LL	后面跟随数据元的可变长度值，01 至 99
LLL	后面跟随数据元的可变长度值，001 至 999
VAR	可变长度数据元
3	3 字符的固定长度
..17	最大 17 个字符的可变长度。所有可变长度字段在数据元的前面应另外包含 2 个或 3 个位置，以表示后面到数据元结束时的位置数。
X	借贷符号，贷记为“C”，借记为“D”，并且总是与一个数字型金额数据元相连，例如，X+n16 含义为前缀“C”或“D”和 16 位数字。
Z	ISO 4909 和 ISO 7813 中定义的磁卡第二、三磁道的代码集
注 1：对任何最大长度小于 100 个字符的可变长度数据元，两个附加位位于该数据元之前，标明其后所跟数据元的长度。其格式表示为 LLVAR。 注 2：对任何最大长度小于 1000 个字符的可变长度数据元，三个附加位位于该数据元之前，标明其后所跟数据元的长度。其格式表示为 LLLVAR。	

### 13.1.2 注释

本规范所使用的域按 ISO8583 中所给的域的序号，从小至大排序说明的。本规范还使用了 ISO8583 中的保留域，并定义了特殊用法。

本规范所采用的编码方式为 ASCII 码。数字字符也不采用压缩的 BCD 码方式，而是采用 ASCII 码表示。本章中的所有错误码请参见《银行卡联网联合技术规范》中错误代码描述。

### 13.1.3 域的长度

域的长度应符合以下要求：

- ISO 标准中规定的可变长度域最长可以达到 999 个字节。本规范中的域描述给出了每个可变长度域的最大长度字节数，这个长度限制适应于整个域，该域中所有子域的长度和应小于等于整个域的长度。
- 所有的长度值不包括长度子域本身的长度。
- 报文域的长度占位含义依赖于域的属性，可以是字母、数字或二进制位。
- 所有的二进制位域，如位图和 PIN，它们的位串必须被正确地构造。

### 13.1.4 对未使用位置的填充

对于固定长度的报文域有以下填充规则：

- 如果是数字域，右靠齐，左边多余位填零。

——如果不是数字域，左靠齐，右边多余位填充空格。

### 13.1.5 带有可选择子域的报文域

如果一个域带有子域，并且不是全部子域都要求出现在报文中，那么该域的任何一个子域出现在报文中，该域的在位图中对应的位就要设为1。

## 13.2 数据元名称及其定义

### 13.2.1 报文类型标识符

报文类型标识符(Message Type ID)

#### 13.2.1.1 变量属性：

n4，4位定长数字字符。

#### 13.2.1.2 域描述：

用于确定报文的类型。根据代理业务ATM终端所支持的交易类型定义如下：

——0100/0110 授权类消息

- 修改密码请求/应答

——0200/0210 查询类消息

- 余额查询请求/应答
- 明细查询请求/应答

——0200/0210 金融类消息

- 取款请求/应答
- 转账请求/应答
- 代缴费查询请求/应答
- 代缴费请求/应答

——0420/0430 冲正通知类消息

- ATM取款冲正通知/应答

——0520/0530 对账类消息

- ATM对账通知请求/应答

——0820/0830 网络管理通知类消息

- ATM签到通知/应答
- 打开终端设备通知/应答
- 关闭终端设备通知/应答
- 参数下载通知/应答
- 加钞信息通知/应答
- 批上送交易明细
- 批上送结束
- 上传交易明细通知/应答
- 定时状态报告通知/应答
- 状态切换报告通知/应答
- 提醒信息报告通知/应答
- 故障信息报告通知/应答
- 吞卡信息报告通知/应答
- 设备状态查询通知/应答

### 13.2.2 域2

主账号(Primary Account Number, PAN)

#### 13.2.2.1 变量属性：

n..19(LLVAR) 2个字节的长度值+最大19个字节（数字字符）的主账号。

13.2.2.2 域描述:

用户主账号,即从磁卡的第二磁道上获取的账号。从第二磁道的起始符开始(不包含)至字段分隔符止(不包含)。针对内卡,该账号长度为13-19个数字字符;针对外卡,该账号长度为11-19个数字字符。

主账号应符合下列标准之一:

- 《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,即由表 32 所示三部分组成:

表32 主账号组成

XXXXXX	X ... .. X	X
发卡行标识代码	6-12 自定义位	校验位

- VISA 国际组织的规定。
- MASTERCARD 国际组织的规定。
- 由中国人民银行认可的其他标准。
- 其他银行卡组织(公司)的规定。

13.2.2.3 用法:

该域在所有的金融请求、应答和通知中都要求存在。该域用来确定发卡机构,确定交易报文的路由。如果交易的原始请求报文中存在该域,则该交易的随后相关报文中也必须有该域存在。如果该域在请求或通知报文中出现,则该域必须在应答报文中原值返回。

转账交易报文中本域为转出账户的卡号。

缴费交易报文中本域为扣费账户的卡号。

13.2.3 域 3

交易处理码(Processing Code)

13.2.3.1 变量属性:

n6, 6位定长数字字符。

13.2.3.2 域描述:

交易处理码(Processing-Code)由六位数字组成,如表33所示。

表33 交易处理码的组成

1-2 位	3-4 位	5-6 位
交易类型	转出账户类型	转入账户类型

交易处理码的第1-2位定义如表34所示:

表34 交易处理码第 1-2 位定义

值	含义
01	取款
19	代缴费
30	余额查询
31	代缴费查询
39	明细查询
40	转账
70	修改密码

交易处理码的第3位和第5位定义如表35所示:

表35 交易处理码第 3 位和第 5 位定义

值	含义
0	默认
1	储蓄账户



2	支票账户
3	信用透支账户
4	通用账户
5	投资账户

交易处理码的第4位和第6位定义如表36所示：

表36 交易处理码第4位和第6位定义

值	含义
0	默认

**13.2.3.3 用法:**

在交易应答中该域必须与交易请求一致。

在冲正交易中该域必须与原始交易一致。

**13.2.4 域4**

交易金额(Amount, Transactions)

**13.2.4.1 变量属性: :**

n12, 12位定长数字字符。

**13.2.4.2 域描述:**

交易金额。交易金额不包括任何服务费; 本域中不带小数点。小数位根据交易币种来决定。

**13.2.4.3 用法:**

交易金额的币种由域49交易币种(Currency-Code-of-Transaction)表示, 若表示人民币则单位为分。例如: ATM取款金额为1000元, 则交易金额=“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。

在查询请求中本域不出现。在代理业务的实时缴费报文中, 该域的值是代缴费的交易金额。

**13.2.5 域7**

交易传输时间(Transmission Date/Time)

**13.2.5.1 变量属性:**

n10, 10位定长数字字符。

格式: MMDDhhmmss

**13.2.5.2 域描述:**

ATM系统的工作日日期和时间(都为北京时间)。

**13.2.5.3 用法:**

当ATM发起交易请求报文时, 即赋予该交易ATM的系统工作日日期和时间。

ATMP在收到报文时应保存该值, 并在应答报文中原样返回。

该域为关键信息域, ATMP在接收到交易应答时, 将用该值匹配原始请求报文的该域值。

当发送冲正报文时, 冲正产生方将给冲正报文一个新的交易时间。重复发送冲正报文时, 将不改变原先已赋予冲正交易的时间。

交易传输时间的取值范围如表37所示:

表37 交易传输时间取值范围

	MM	DD	hh	mm	ss
取值范围	01—12	01—31	00—23	00—59	00—59

**13.2.6 域11**

系统跟踪号(System Trace Audit Number)

**13.2.6.1 变量属性:**

n6, 6位定长数字字符。

**13.2.6.2 域描述:**

ATM赋予交易的一组数字, 用于唯一标识一笔交易的编号, 该编号ATM将循环重复使用(从000000~999999)。

**13.2.6.3 用法:**

ATM对发出的每一条请求报文，必须赋予一个系统跟踪号。对于重发的冲正报文，该系统跟踪号的值与原冲正交易一致。在整个交易周期中该值保持不变。

该域为关键信息域，其值在一个清算日内不能重复。ATMP在接收到交易应答时，将用该值匹配原始请求报文。

### 13.2.7 域 12

受卡方所在地时间(Time, Local Transaction)

#### 13.2.7.1 变量属性:

n6, 6位定长数字字符。

格式: hhmmss

#### 13.2.7.2 域描述:

交易发生时，ATM终端的时间。格式为hhmmss，其中hh=小时，mm=分，ss=秒。

#### 13.2.7.3 用法:

在0200的请求报文中，ATM应赋予交易发生时的终端时间。冲正报文中的本地交易时间，必须与原取款交易报文的本地交易时间保持一致。

表38 受卡方所在地时间取值范围

	hh	mm	ss
取值范围	00—23	00—59	00—59

### 13.2.8 域 13

受卡方所在地日期(Date, Local Transaction)

#### 13.2.8.1 变量属性:

n4, 4位定长数字字符。

格式: MMDD

#### 13.2.8.2 域描述:

交易发生时，ATM终端的日期。格式为MMDD，其中MM=月份，DD=日。

#### 13.2.8.3 用法:

在0200的请求报文中，ATM应赋予交易发生时的终端日期。冲正报文中的本地交易日期，必须与原始报文的本地交易日期保持一致。

表39 受卡方所在地日期取值范围

	MM	DD
取值范围	01—12	01—31

### 13.2.9 域 14

卡有效期(Date, Expiration)

#### 13.2.9.1 变量属性:

n4, 4位定长数字字符。

格式为: YYMM

#### 13.2.9.2 域描述:

银行卡的有效期，域值是银行卡过期的年月。卡磁条信息中包含有卡有效期信息。其中YY=年份，MM=月份。

#### 13.2.9.3 用法:

由发卡行根据实际情况填入卡片的有效期限。无有效期的卡填充“0”。

### 13.2.10 域 15

清算日期(Date, Settlement)

#### 13.2.10.1 变量属性:

n4, 4位定长数字字符。

格式: MMDD

### 13.2.10.2 域描述:

交易的结算日期。日期为MMDD格式, 其中MM=月份, DD=日。

### 13.2.10.3 用法:

应答报文中应将清算日期原样返回。对于重发报文的清算日期应为原报文的清算日期。

表40 清算日期取值范围

	MM	DD
取值范围	01—12	01—31

### 13.2.11 域 22

服务点输入方式码(Point Of Service Entry Mode Code)

#### 13.2.11.1 变量属性:

n3, 3位定长数字字符。

#### 13.2.11.2 域描述:

服务点输入方式码, 即持卡人数据 (如PAN和PIN) 的输入方式。服务点 (point of service) 是指各种交易始发场合。

#### 13.2.11.3 用法:

本域第1、2位的取值与终端输入能力相关。目前使用的服务点输入方式代码为:

021: 磁条读入, 且带PIN;

022: 磁条读入, 且不带PIN;

051: 芯片读入, 且带PIN;

052: 芯片读入, 且不带PIN;

### 13.2.12 域 23

卡序列号(Card Sequence Number)

#### 13.2.12.1 变量属性

n3, 3位定长数字字符。

#### 13.2.12.2 域描述

IC卡的序列号

#### 13.2.12.3 用法

13.2.13 用于区别具有相同 PAN 的不同的卡, 只有在 IC 卡交易而且卡上有该数据元时才使用。域 26

服务点 PIN 获取码(Point of Service Pin Capture Code)

#### 13.2.13.1 变量属性:

n2, 2位定长数字字符。

#### 13.2.13.2 域描述:

服务点设备PIN获取码。

#### 13.2.13.3 用法:

该域描述了服务点设备接受PIN的最大长度。

### 13.2.14 域 32

代理机构标识码(Acquiring Institution Identification Code)

#### 13.2.14.1 变量属性:

n..11(LLVAR), 2个字节的长度值+最大11个字节的代理机构标识码。

#### 13.2.14.2 域描述:

传统业务处理中表示代理机构的标识码。该代理机构应是已被批准入网, 为ATM提供现金管理服务的成员机构。

代理业务处理中表示接入渠道商的机构标识码。

**13.2.14.3 用法:**

传统业务处理中该域用来标识现金托管机构标识码。

代理业务处理中该域用来标识接入渠道商的机构标识码。

**13.2.15 域 33**

**发送机构标识码(Forwarding Institution Identification Code)**

**13.2.15.1 变量属性:**

n..11(LLVAR), 2个字节的长度值+最大11个字节的发送机构标识码。

**13.2.15.2 域描述:**

传统业务处理中表示发送机构标识码。该发送机构应是已被批准入网, 发送一个交易请求或通知报文的机构。

**13.2.15.3 用法:**

传统业务处理中该域用来标识一个入网机构。

**13.2.16 域 35**

**第二磁道数据(Track 2 Data)**

**13.2.16.1 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(字符)。

**13.2.16.2 域描述:**

银行卡上第二磁道的数据。

**13.2.16.3 用法:**

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

**13.2.17 域 36**

**第三磁道数据(Track 3 Data)**

**13.2.17.1 变量属性:**

z...104(LLVAR), 3个字节的长度值+最大104个字节的第三磁道数据(字符)。

**13.2.17.2 域描述:**

银行卡上第三磁道的数据。

**13.2.17.3 用法:**

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

**13.2.18 域 37**

**检索参考号(Retrieval Reference Number)**

**13.2.18.1 变量属性:**

an12, 12位定长的字母和数字字符。

**13.2.18.2 域描述:**

ATMP给予交易的系统检索参考号。

**13.2.18.3 用法:**

本域是由ATMP分配的用于定位持卡人原始交易的一个系统参考号。本域在整个交易周期内保持不变。

ATMP对每一个取现、代缴费、查询、转账等业务类交易请求赋给一个新值。在冲正交易中本域使用原始交易的值。

**13.2.19 域 39**

**应答码(Response Code)**

**13.2.19.1 变量属性:**

an2, 2位定长的字母和数字字符。

**13.2.19.2 域描述:**

交易的应答码，在回应报文中必须存在该域。

13.2.19.3 用法：

对每个收到的请求报文，都应将本系统处理的结果在本域中返回给ATM。  
具体应答码请参考《银行卡联网联合技术规范》中相关规定。

13.2.20 域 41

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

13.2.20.1 变量属性：

ans8，8位定长的字母、数字和特殊字符。

13.2.20.2 域描述：

ATM的终端标识码。该标识码在同一ATMP网络中必须唯一标识一台ATM。

13.2.20.3 用法：

如果终端标识码少于八位，则按左靠，右边补空格。  
所有卡交易请求中必须带上终端标识码，且在整个交易周期中保持不变。

13.2.21 域 42

受卡方标识码（Card Acceptor Identification Code）

13.2.21.1 变量属性：

ans15，15位定长的字母、数字和特殊字符。

13.2.21.2 域描述：

用于代理业务交易报文，受卡方的标识码，即服务提供商代码。

13.2.21.3 用法：

在代理业务交易中出现，受卡方标识码（服务提供商代码）必须为有效数字字符。由公共服务平台分发。对所有代理业务交易的请求报文，该域必须出现，且在整个交易周期中保持不变。

13.2.22 域 43

受卡方名称地址（Card Acceptor Name/Location）

13.2.22.1 变量属性：

ans40，40位定长的字母、数字和特殊字符。

13.2.22.2 域描述：

ATM的名称和放置位置。

13.2.22.3 用法：

在信息中必须包括ATM所在地点和所在城市、省的名称，格式如表41所示：

表41 受卡方名称地址格式

位置	长度	用法	值
0	3	国家代码	总是为 CHN
3	2	所在省代码（字母码）	《中华人民共和国行政区划代码》(GB/T2260-1999)中省、自治区、直辖市、特别行政区及分省代码表中编码。
5	3	地区代码（字母码）	
8	32	所在地点	如果少于 32 个字母，则后补空格。

13.2.23 域 48

附加数据—私有(Additional Data-Private)

13.2.23.1 变量属性：

ans...512(LLLVAR)，3个字节的长度值+最大512个字节的数据(字母、数字和特殊字符)。

13.2.23.2 域描述：

ISO将此字段定义为私有数据。本规范将此字段用作多种用途，每种用途有一特定格式。在所有情况下，将用如下总体格式：

<长度><格式符><数据>

——〈长度〉

说明该字段的总长度(包含〈格式符〉)，长度为3个字节。

——〈格式符〉

说明后随数据的类型，长度为2个字节，如表42所示。

表42 域 48 格式符说明

格式符	对应用法	说明
AA 或 PA	用法一	代理业务系统数据
BS	用法二	钞箱信息数据
DS	用法三	设备状态数据
DP	用法四	设备参数下载
SU	用法五	签到上送数据
SD	用法六	签到下送数据
RC	用法七	对账数据
TD	用法八	交易明细包数据
BT	用法九	批上送统计数据
NP	用法十	新密码数据
PL	用法十一	公钥列表
AL	用法十二	AID 列表
PK	用法十三	特定的公钥数据
AP	用法十四	特定的 AID 相关参数
TC	用法十五	TC 实时上送
SC	用法十六	脚本通知

——〈数据〉

具体数据，其格式取决于〈格式符〉字符，长度最长不超过510个字节。

### 13.2.23.3 用法：

#### 13.2.23.3.1 用法一（代理业务系统数据）

分成三个部分，用法标志—2字节，代理业务交易类型定义—2字节，自由文字格式—最大508字节，如表43所示。

表43 域 48—代理业务系统数据定义

ID	数据元名称	类型	说明
	长度	n3	不超过 512
0	标识符	ans2	AA 表示代缴费查询 PA 表示实时缴费和充值
1	请求/应答标志	n1	‘0’ 表示请求，‘1’ 表示应答
2	代理业务交易类型定义	n2	01：代缴费查询 03：实时缴费 04：充值
3	代理业务种类	an2	两位数字，表示代理业务的种类
4	代理业务信息	ans503	可变长度

其中第4子域的定义根据代理业务交易类型不同而有不同的定义，说明如下：

——01：代缴费查询

- 请求报文如表 44 所示：

表44 域 48—代缴费查询请求报文

ID	数据元名称	类型	说明
AA.1	服务提供商方用户代码	an32	比如手机号码、电话号码等，左对齐，右补空格
AA.2	查询起始年月	n4	暂不用，填空格
AA.3	查询终止年月	n4	暂不用，填空格
AA.4	服务提供商方用户密码	b64	如果服务商要求查询输入密码，则此字段出现。 本字段为加密后的密文，加密方式同 PIN 加密

- 应答报文如表 45 所示：

表45 域 48—代缴费查询应答报文

ID	数据元名称	类型	说明
AA.1	服务提供商方用户代码	an32	比如手机号码、电话号码等，左对齐，右补空格
AA.2	查询起始年月	n4	暂不用，填空格
AA.3	查询终止年月	n4	暂不用，填空格
AA.4	缴费金额	n12	以分为单位，左补 0
AA.5	其他行业特定信息	ans150	左对齐，右补空格

——03：实时缴费

——04：充值

- 请求报文如表 46 所示：

表46 域 48—充值请求报文

ID	数据元名称	类型	说明
PA.1	服务提供商方用户代码	an32	比如手机号码、电话号码等，左对齐，右补空格
PA.2	缴费年月	n4	暂不用，填空格
PA.3	服务提供商方用户密码	b64	左对齐，右补空格（可选）

- 应答报文如表 47 所示：

表47 域 48—充值应答报文

ID	数据元名称	类型	说明
PA.1	服务提供商方用户代码	an32	比如手机号码、电话号码等，左对齐，右补空格
PA.2	缴费年月	n4	暂不用，填空格
PA.3	其他行业特定信息	ans150	左对齐，右补空格

### 13.2.23.3.2 用法二（钞箱信息数据）

在加钞报文中，本域表示钞箱中实际加入的钞票数目。

本域定义如表48所示：

表48 域 48—钞箱信息数据定义

ID	数据元名称	类型	说明
	长度	n3	不超过 512
BS.0	标识符	ans2	BS 表示钞箱信息数据
BS.1	批次号	n14	采用年月日时分秒编码格式
BS.2	操作员号	an8	
BS.3	第一钞箱信息数据	n11	
BS.3	第二钞箱信息数据	n11	
BS.3	第三钞箱信息数据	n11	
BS.3	第四钞箱信息数据	n11	

其中，BS.3钞箱信息数据的定义如表49所示：

表49 域 48—BS.3 钞箱信息数据定义



ID	数据元名称	类型	说明
BS.3.1	币种	n3	参见 ISO 4217 标准
BS.3.2	面值	n4	
BS.3.3	张数	n4	

其中, BS.1批次号在除加钞交易的响应报文外, 该字段的值应为当前ATM的交易批次号。在加钞的响应交易报文中, 由ATMP负责将分配好的批次号放在该字段中返回。

### 13.2.23.3.3 用法三（设备状态数据）

在设备状态报文中, 本域定义如表50所示:

表50 域 48—设备状态数据定义

ID	数据元名称	类型	说明
	长度	n3	不超过 512
DS.1	标识符	ans2	DS 表示设备状态数据
DS.2	ATM 状态	an1	0: 服务状态(正常) 1: 业务管理状态 2: 系统管理状态 9: 故障状态
DS.3	事件代码	n6	保留使用
DS.4	流水打印机状态	an1	0: 正常 1: 纸少 2: 缺纸 3: 卡纸 9: 故障
DS.5	凭条打印机状态	an1	0: 正常 1: 纸少 2: 缺纸 3: 卡纸 9: 故障
DS.6	磁卡读卡器状态	an1	0: 正常 9: 故障
DS.7	出钞模块状态	an1	0: 正常 9: 故障
DS.8	保险门状态	an1	0: 正常（关） 1: 正常（开） 9: 异常
DS.9	机箱门状态	an1	0: 正常（关） 1: 正常（开） 9: 异常
DS.10	硬件加密器状态	an1	0: 正常 9: 异常
DS.11	废钞箱状态	an1	0: 正常 9: 异常
DS.12	废钞箱张数	n3	
DS.13	吞卡张数	n2	

ID	数据元名称	类型	说明
DS.14	第一钞箱状态	an1	0: 正常 1: 钞少 2: 缺钞 3: 无钞箱 9: 故障
DS.14	第二钞箱状态	an1	
DS.14	第三钞箱状态	an1	
DS.14	第四钞箱状态	an1	
DS.15	第一钞箱信息数据	n11	
DS.15	第二钞箱信息数据	n11	
DS.15	第三钞箱信息数据	n11	
DS.15	第四钞箱信息数据	n11	

其中, DS. 15钞箱信息数据的定义如表51所示:

表51 域 48—DS. 15 钞箱信息数据定义

ID	数据元名称	类型	说明
DS.15.1	币种	n3	参见 ISO 4217 标准
DS.15.2	面值	n4	
DS.15.3	张数	n4	

#### 13. 2. 23. 3. 4 用法四 (设备参数数据)

在参数数据报文中, 本域定义如表52所示:

表52 域 48—设备参数数据定义

ID	数据元名称	类型	说明
	长度	n3	不超过 512
DP.1	标识符	ans2	DP 表示设备参数数据
DP.2	参数数据	ans...512 (LLVAR)	保留使用, 根据不同的 ATMC 另行定义

参考实例:

ID	数据元名称	类型	说明
DP.2.1	间隔发送状态包时长	n6	以秒为单位, 不足前补 0
DP.2.2	一次最大取款金额	n12	以分为单位, 右对齐, 不足前补 0
DP.2.3	一次最小取款金额	n12	以分为单位, 右对齐, 不足前补 0
DP.2.4	一次最大转账金额	n12	以分为单位, 右对齐, 不足前补 0
DP.2.5	IC 卡一次最大圈存额	n12	以分为单位, 右对齐, 不足前补 0
DP.2.6	IC 卡一次最小圈存额	n12	以分为单位, 右对齐, 不足前补 0
DP.2.7	IC 卡一次最大圈取额	n12	以分为单位, 右对齐, 不足前补 0
DP.2.8	一次最大存款金额	n12	以分为单位, 右对齐, 不足前补 0
DP.2.9	保留字段	n16	全置 0

#### 13. 2. 23. 3. 5 用法五 (签到上送数据)

在签到请求报文中, 本域定义如表53所示:

表53 域 48—签到上送数据定义

ID	数据元名称	类型	说明
	长度	an3	不超过 512
SU.1	标识符	ans2	SU 表示签到上送数据
SU.2	软件版本号	n14	采用年月日时分秒编码格式
SU.3	参数版本号	n14	采用年月日时分秒编码格式

#### 13. 2. 23. 3. 6 用法六 (签到下送数据)

在签到应答报文中, 本域定义如表54所示:

表54 域 48—签到下送数据定义

ID	数据元名称	类型	说明
	长度	an3	不超过 512
SD.1	标识符	ans2	SD 表示签到下送数据
SD.2	加密的 PIN 密钥	b128	如果密钥长度为 64bit, 则使用前 64bit 存放数据
SD.3	PIN 密钥的验证码	ans16	
SD.4	加密的 MAC 密钥	b128	如果密钥长度为 64bit, 则使用前 64bit 存放数据
SD.5	MAC 密钥的验证码	ans16	
SD.6	软件版本号	n14	采用年月日时分秒编码格式
SD.7	参数版本号	n14	采用年月日时分秒编码格式
SD.8	当前批次号	n14	采用年月日时分秒编码格式
SD.9	交易信息	n8	每个字节表示一个交易是否开通, ‘0’ 表示未开通, ‘1’ 表示开通。交易信息根据功能选择画面定义, 按照取款、余额查询、明细查询、转账、修改密码、代缴费、备用 1、备用 2 的顺序排列
SD.10	代理业务种类	n32	每一字节取值表示某项代理业务是否开通和开通类型, ‘0’ 表示未开通, ‘1’ 表示开通代缴费交易, ‘2’ 表示开通充值交易
SD.11	代理业务信息	ans320	可变长度, 采用固定 10 个字节根据代理业务种类的内容按顺序写入已经开通的所有代理业务的名称, 代理业务名称不足 10 个字节的, 左对齐, 右补空格

如果签到上送报文中的SU. 2和SU. 3与ATMP中保存的对应终端的软件版本号、参数版本号一致, 则响应报文的SD. 6和SD. 7域内容与签到报文的SU. 2与SU. 3一致, 且响应报文中不包括SD. 8、SD. 9、SD. 10、SD. 11子域。如果不一致, 则SD. 6与SD. 7赋ATMP中保存的对应终端的软件版本号、参数版本号, 且在响应报文中包括SD. 8、SD. 9、SD. 10、SD. 11子域。

### 13. 2. 23. 3. 7 用法七（对账数据）

在对账报文中, 本域定义如表55所示。

表55 域 48—对账数据定义

ID	数据元名称	类型	说明
	长度	n3	不超过 512
RC.0	标识符	ans2	RC 表示设备状态数据
RC.1	对账周期信息	n14	表明对账周期的数据, 即清算日期或者批次号
RC.2	借方交易笔数	n4	成功交易
RC.3	借方交易金额	n12	成功交易
RC.4	贷方交易笔数	n4	成功交易
RC.5	贷方交易金额	n12	成功交易
RC.6	贷记冲正交易笔数	n4	成功交易
RC.7	贷记冲正交易金额	n12	成功交易
RC.8	转账交易笔数	n4	成功交易
RC.9	转账交易金额	n12	成功交易
RC.10	代缴费/充值交易笔数	n4	成功交易
RC.11	代缴费/充值交易金额	n12	成功交易

ID	数据元名称	类型	说明
RC.12	余额查询交易笔数	n6	成功交易
RC.13	明细查询交易笔数	n4	成功交易
RC.14	修改密码交易笔数	n4	成功交易
注：RC.1中数据内容、请求与响应报文应该一致。如果按照清算日对账，则该域的内容为8位日期格式“YYYYMMDD”再加6个空格组成。如果按照批次号对账，则应该完整的填入需要对账的批次号。			

### 13.2.23.3.8 用法八（交易明细包数据）

13.2.23.3.8.1 在ATMP通知上传交易明细请求报文格式中，本域定义如表56所示：

表56 域48—上传交易明细请求报文格式

ID	数据元名称	类型	说明
	长度	n3	不超过512
TD.0	标识符	ans2	TD表示交易明细包数据
TD.1	对账周期	n14	表明对账周期的数据，即清算日期或者批次号
TD.2	起始序号	n4	表示需要上传的交易明细起始序号

13.2.23.3.8.2 ATM向ATMP发送批上送交易明细数据报文中，本域定义如表57所示：

表57 域48—上传交易明细请求报文格式

ID	数据元名称	类型	说明
	长度	n3	不超过512
TD.0	标识符	ans2	TD表示交易明细包数据
TD.1	对账周期	n14	表明对账周期的数据，即清算日期或者批次号
TD.2	起始序号	n4	表示本记录中交易明细起始序号
TD.3	交易明细一	ans42	每次允许最多10条明细记录
TD.3	交易明细二	ans42	
	...		
TD.3	交易明细n	n42	

其中，TD.3交易明细的定义如表58所示：

表58 域48—TD.3交易明细定义

ID	数据元名称	类型	说明
TD.3.1	卡号	n19	域2
TD.3.2	交易类型	n2	域3的第1、2位
TD.3.3	交易金额	n12	域4
TD.3.4	系统跟踪号	n6	域11
TD.3.5	币种	an3	域49

### 13.2.23.3.9 用法九(批上送统计数据)

在批上送统计数据报文中，本域定义如表59所示：

表59 域48—批上送统计数据定义

ID	数据元名称	类型	说明
	长度	n3	不超过512
BT.0	标识符	ans2	BT表示批上送统计数据

BT.1	对账周期	n14	表明对账周期的数据，即清算日期或者批次号
BT.2	批上送交易明细总数	n5	

### 13.2.23.3.10 用法十(新密码数据)

在修改密码数据报文中，本域定义如表60所示：

表60 域 48—新密码数据定义

ID	数据元名称	类型	说明
	长度	n3	不超过 512
PS.1	标识符	ans2	PS 表示新密码数据
PS.2	新密码	b64	64bit 的二进制数据，加密存放新密码，格式与 52 域相同

### 13.2.23.3.11 用法十一（公钥列表）

在下载公钥列表报文中，本域定义如下：

ID	数据元名称	类型	说明
	长度	n3	不超过 512
PL.1	标识符	ans2	PL 表示公钥列表下载
PL.2	公钥列表	b	请求报文时不存在， 响应报文时为多个{RID (TLV)+索引 (TLV) +有效期 (TLV) }

### 13.2.23.3.12 用法十二（AID 列表）

在下载AID列表报文中，本域定义如下：

ID	数据元名称	类型	说明
	长度	n3	不超过 512
AL.1	标识符	ans2	AL 表示 AID 列表下载
AL.2	AID 列表	b	请求报文时不存在， 响应报文时为多个 AID (TLV 编码)

### 13.2.23.3.13 用法十三（RID 相关的 CA 公钥数据）

特定公钥列表报文中，本域定义如下：

ID	数据元名称	类型	说明
	长度	n3	不超过 512
PK.1	标识符	ans2	PK 表示特定公钥下载
PK.2	公钥数据	b	请求报文时为 RID 标识（定长 5 字节），下载结束时填全 ‘0’ 的 RID。， 响应报文时为{公钥最小数据元(TLV 格式)}格式。每次仅下载一个公钥。

### 13.2.23.3.14 用法十四（AID 相关的 EMV 参数）

在下载特定AID相关EMV参数中，本域定义如下：

ID	数据元名称	类型	说明
	长度	n3	不超过 512
AP.1	标识符	ans2	AP 表示公钥列表下载

ID	数据元名称	类型	说明
AP.2	EMV 参数	b	请求报文时为某个 AID (TLV 编码), 每次仅请求下载一个 AID 的全部相关参数, 下载结束时不存在。, 响应报文时为请求的 AID (TLV 编码) + 多个{参数 (TLV 编码)}格式。每次仅下载一个 AID 的全部相关参数。

### 13.2.23.3.15 用法十五 (EMV 卡批准交易的 TC 实时上送)

EMV卡交易批准后立即上送TC相关信息。

在上送TC中, 本域定义如下:

ID	数据元名称	类型	说明
	长度	n3	不超过 512
TC.1	标识符	ans2	TC 表示 TC 上送

### 13.2.23.3.16 用法十六 (脚本执行通知)

脚本执行后立即发送脚本通知。

在脚本通知中, 本域定义如下:

ID	数据元名称	类型	说明
	长度	n3	不超过 512
SC.1	标识符	ans2	SC 表示脚本通知

### 13.2.24 域 49

交易货币代码(Currency Code, Transaction)

#### 13.2.24.1 变量属性:

an3, 3位定长的字母和数字字符。

#### 13.2.24.2 域描述:

指域4所用货币的种类。

#### 13.2.24.3 用法:

参见ISO 4217标准, 人民币代码为156。

### 13.2.25 域 52

个人标识码数据(Pin Data)

#### 13.2.25.1 变量属性:

64bit的二进制数。

#### 13.2.25.2 域描述:

个人标识码PIN的密文。

#### 13.2.25.3 用法:

对于ATM交易本域必须出现。客户的个人标识码(PIN)必须加密后存放在此域中。PIN的格式采用ANSI X9.8带主账号参与异或运算的格式。

本系统允许的PIN最大长度为12位数字。

### 13.2.26 域 53

安全控制信息(Security Related Control Information)

#### 13.2.26.1 变量属性:

n16, 16位定长数字字符。

### 13.2.26.2 域描述:

与安全相关的控制信息。

在交易类报文中, 该域用于标识PIN的类型, 如表61所示。

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”

表61 安全控制信息格式

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 2-9: 其他加密算法(未用)
注 1: PIN加密方法 ANSI X9.8 Format, 参见附录A: 个人标识(PIN)的加密和解密方法说明。 注 2: PIN加解密应采用双倍长密钥算法	

### 13.2.27 域 54

实际余额(Additional Amounts)

#### 13.2.27.1 变量属性:

an...040 (LLVAR), 3个字节的长度值+最大40个字节的数据(字母、数字字符)。

#### 13.2.27.2 域描述:

交易后账户上的实际余额。该域分为两部分余额, 即账面余额和当日可用余额。账面余额为客户账户内余留的金额; 当日可用余额为当天可参与交易的金额。

当日可用余额 = 账面余额 + 信用度 - 授权金额。

#### 13.2.27.3 用法:

这个数据元的名称是自定义的, 实际采用可变长的标准数据元, 取长度为40。即, 20个字节为一个记录, 共二个记录, 内容定义如表62所示:

表62 实际余额格式

ID	数据元名称	类型	说明	取值
	LENGTH	n3	本域长度	040
54.1	ACCOUNT-TYPE	n2	账户类型	见域 3 的定义
54.2	AMOUNT-TYPE	n2	数量类型	01 表示账面余额
54.3	CURRENCY-CODE	an3	货币代码	见域 49 定义
54.4	AMOUNT SIGN	an1	余额符号	借方为 D, 贷方为 C
54.5	AMOUNT	n12	余额	交易不成功置为零
54.6	ACCOUNT-TYPE	n2	账户类型	见域 3 的定义
54.7	AMOUNT-TYPE	n2	数量类型	02 表示可用余额
54.8	CURRENCY-CODE	an3	货币代码	见域 49 定义
54.9	AMOUNT SIGN	an1	余额符号	借方为 D, 贷方为 C
54.10	AMOUNT	n12	余额	交易不成功置为零
注 1: 54.1到54.5域为账户上的账面余额(LEDGER-BALANCE-AMOUNT)。 注 2: 54.6到54.10域为账户上的可用余额(AVAILABLE-BALANCE-AMOUNT)。				

### 13.2.28 域 55

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

13.2.28.1 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。

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。

13.2.28.2 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：

- 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。
- 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。

13.2.28.3 用法

表63 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	—	9F27	1	B



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
	Data				
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

表64 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 Verification 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

表65 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

## 13.2.29 域 59

明细查询数据(Details-Inquiry-Data)

## 13.2.29.1 变量属性:

ans...600 (LLLVAR), 3个字节的长度值+最大600个字节的数据(字母、数字和特殊字符)。

## 13.2.29.2 域描述:

在明细查询报文中存放请求和响应数据。一笔响应记录最多存放十笔交易明细。

在所有情况下, 将用如下总体格式:

<长度><格式符><数据>

——<长度>

说明该字段的总长度(包含<格式符>)

——<格式符>

说明后随数据的类型, 如表66所示。

表66 明细查询数据格式

格式符	用法	说明
QL	用法一	Query Latest 查询最新明细请求报文
QD	用法二	Query Date 按日期查询明细
QR	用法三	Query Result 查询明细响应数据

——<数据>

具体数据, 其格式取决于<格式符>字符。

## 13.2.29.3 用法:

## 13.2.29.3.1 用法一(查询最新明细请求报文)

在查询最新明细请求报文中, 本域定义如表67所示:

表67 域 59—查询最新明细请求报文定义

ID	数据元名称	类型	说明
	长度	n3	不超过 600
QL.1	标识符	ans2	QL 表示查询最新发生的十笔明细
CURRENT-SEQUENCE-NU MBER	当前明细顺序号	n3	

## 13.2.29.3.2 用法二(按日期查询明细请求报文)

在按日期查询明细请求报文中, 本域定义如表68所示:

表68 域 59—按日期查询明细请求报文定义

ID	数据元名称	类型	说明
	长度	n3	不超过 600
QD.1	标识符	ans2	QD 表示按日期查询明细
QD.2	当前明细顺序号	n3	当前明细顺序号按下列原则填写: 如果共

ID	数据元名称	类型	说明
			计有 35 条记录,那么在第一次发出请求时,当前明细顺序号应填 001;第二次发出请求时,当前明细顺序号应填 011;第三次发出请求时,当前明细顺序号应填 021,以此类推。
QD.2	明细起始日期	n8(YYYYMMDD)	
QD.3	明细中止日期	n8(YYYYMMDD)	

### 13.2.29.3.3 用法三（查询明细响应数据）

在明细查询响应报文中,本域定义如表69所示:

表69 域 59—明细查询响应报文定义

ID	数据元名称	类型	说明
	长度	n3	不超过 600
QR.1	标识符	ans2	QR 表示明细查询响应
QR.2	卡账户货币代码	an3	
QR.3	明细总个数	n3	所有满足查询条件的记录数
QR.4	账户明细数据一	ans50	明细记录按交易发生时间降序(时间递减)排列。
QR.4	账户明细数据二	ans50	
	...		
QR.n	账户明细数据 n	ans50	

其中QR.4明细数据的定义如表70所示:

表70 QR.4 明细数据定义

ID	数据元名称	类型	说明
QR.4.1	明细顺序号	n3	
QR.4.2	交易日期	n8	
QR.4.3	交易货币代码	an3	
QR.4.4	交易金额	x+n12	
QR.4.5	余额	x+n12	
QR.4.6	交易类型	Ans4	
QR.4.7	备注代码	Ans6	

### 13.2.30 域 60

自定义域 (Reserved)

#### 13.2.30.1 变量属性:

ans..030 (LLLVAR), 3个字节的长度值+最大30个字节(字母、数字和特殊字符)的数据。

#### 13.2.30.2 域描述:

本域为自定义域,由表71所示子域组成:

表71 域 60 的组成

位置	1-4 字节	5-14 字节	15-28 字节	29 字节	30 字节
子域	60.1	60.2	60.3	60.4	60.5

#### 13.2.30.3 子域描述

##### 13.2.30.3.1 60.1 域: 报文原因码 (Message Reason Code)

n4, 长度为4个字节的数字字符,在取款冲正报文中引用,用于描述引发冲正报文的原因。在正常交易报文中填写固定值“0000”。

根据《银行卡联网联合技术规范》2.0版中附录中关于报文原因码的定义进行填写，如表72所示：

表72 报文原因码

冲正理由			
4003	Format error, no action taken	格式错误，不采取行动	冲正报文
4004	Completed partially	部分完成	冲正报文
4005	Original amount incorrect	原始金额不正确	冲正报文
4006	Response received too late	收到应答太迟	冲正报文
4007	Card acceptor device unable to complete transaction	受卡设备不能完成交易	冲正报文
4008	Deposit out of balance	存款不平	冲正报文
4010	Payment out of balance	付款不平	冲正报文
4011	Deposit out of balance/applied contents	存款不平/与应用内容不符	冲正报文
4012	Payment out of balance/applied contents	付款不平/与应用内容不符	冲正报文
4013	Unable to deliver message to terminal	不能传送报文至终端	冲正报文
4014	Suspected malfunction/card retained	怀疑故障/卡被扣	冲正报文
4015	Suspected malfunction/card returned	怀疑故障/卡退回	冲正报文
4016	Suspected malfunction/track 3 not updated	怀疑故障/第三磁道未更新	冲正报文
4017	Suspected malfunction/no cash dispensed	怀疑故障/未吐钞	冲正报文
4018	Timed-out at taking money/no cash dispensed	取款超时/未吐钞	冲正报文
4019	Timed-out at taking card/card retained and no cash dispensed	取卡超时/扣卡，未吐钞	冲正报文
4020	Invalid response, no action taken	无效应答，不采取行动	冲正报文
4021	Timeout waiting for response	应答超时	冲正报文
(4351—4499) ISO 保留给民间使用			
4351	Terminal-generated reversal (full amount)	终端引发冲正（全额）	冲正报文
4352	Terminal-generated reversal (partial amount)	终端引发冲正（部分）	冲正报文
4353	Acquirer received late response from CUPS	受理方收到 CUPS 迟到的应答	冲正报文
4354	Acquirer detected time-out	受理方检测到超时	冲正报文
4355	Acquirer detected incorrect MAC from response message	受理方检测到应答报文的 MAC 不对	冲正报文
4356	Acquirer not able to send operating command to terminal	受理方不能向终端发操作命令	冲正报文
4360	CUPS received late response from card issuer	CUPS 收到发卡方迟到的应答	冲正报文
4361	CUPS waiting for issuer's response until time-out	CUPS 等发卡方应答超时	冲正报文
4362	CUPS detected incorrect MAC from issuer's response message	CUPS 检测到发卡方应答报文的 MAC 不对	冲正报文
4363	CUPS unable to forward issuer's	CUPS 不能向受理方转发发卡方应答报文	冲正报文

冲正理由			
	response message to acquirer		
4364	CUPS unable to forward request to transfer-in party	CUPS 不能向转入方转发交易请求	冲正报文
4365	dispenser out of notes	终端正常, 钞箱无钞票	冲正报文

### 13.2.30.3.2 60.2 域: 服务点附加信息 (Additional Point Of Service Information)

ans10, 10位定长字母、数字、特殊符号, 填入固定值“0000010000”, 表明是从ATM上发起的交易。

### 13.2.30.3.3 60.3 域: 批次号

n14, 14位定长数字, 采用年月日时分秒编码格式“YYYYMMDDhhmmss”, 表明ATM的当前批次号。

### 13.2.30.3.4 60.4 域: 终端读取能力

n1, 1位定长数字。

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。当终端能读取 EMV 卡时, 该域必须填 5。

### 13.2.30.3.5 60.5 域: 芯片条件码

n1, 1位定长数字。

取值	说明
0	默认
1	终端原因引起降级
2	卡原因引起降级

注: 22域取值02X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。

### 13.2.31 域 66

清算代码(Settlement-Code)

#### 13.2.31.1 变量属性:

n1, 1位定长数字字符。

#### 13.2.31.2 域描述:

对账应答代码。

#### 13.2.31.3 用法:

在对账应答报文中表示ATMP上对特定ATM的对账结果。含义见表73。

表73 对账应答代码

代码	含 义
1	对账平
2	对账不平
3	错误

### 13.2.32 域 70

网络管理信息码(Network Management Information Code)

#### 13.2.32.1 变量属性:

n3, 3位定长数字字符。

### 13.2.32.2 域描述:

网络管理功能码。

### 13.2.32.3 用法:

内容如表74所示:

表74 网络管理功能码

功能码	含义
001	支持单倍长密钥算法终端签到
003	支持双倍长密钥算法终端签到
301	线路测试
261	加钞信息报告
262	减钞信息报告
263	钞箱清空报告
361	定时状态报告
362	状态切换报告
363	提醒信息报告
364	故障信息报告
365	吞卡信息报告
081	打开 ATM 终端
082	关闭 ATM 终端
090	参数下载
091	EMV 公钥下载
093	EMV 参数下载
095	EMV 交易 TC 上送
097	EMV 脚本通知
381	设备状态查询
271	批上送交易明细
272	批上送结束通知
273	通知上传交易明细

### 13.2.33 域 90

原始数据元(Original Data Elements)

#### 13.2.33.1 变量属性:

n42, 42位定长数字字符。

#### 13.2.33.2 域描述:

冲正通知交易所用的原始数据记录 (Original-Data-Elements)。

在ATM故障通知交易中用于表示设备发生故障时或之前的交易记录。

#### 13.2.33.3 用法:

内容如表75所示:

表75 原始数据元定义

ID	数据元名称	类型	说明
90.1	原始报文类型	n4	原始交易报文类型
90.2	原始系统跟踪号	n6	原始交易域 11
90.3	原始系统日期时间	n10	原始交易域 7

ID	数据元名称	类型	说明
90.4	原始受理机构标识码	n11	原始交易域 32
90.5	原始发送机构标识码	n11	原始交易域 33
注： 如果没有收到0210的返回报文，90.4和90.5的值填全零。			

### 13.2.34 域 100

接收机构标识码 (Receiving Institution Identification Code)

#### 13.2.34.1 变量属性:

n..11(LLVAR)，2个字节的长度值+最大11个字节（数字字符）的接收方标识码。

#### 13.2.34.2 域描述:

在报文中表示报文接收方机构的标识。

#### 13.2.34.3 用法:

该域在传送途中的值不变。

### 13.2.35 域 102

账户标识 1(Account Identification 1)

#### 13.2.35.1 变量属性:

ans..28(LLVAR)，2个字节的长度值+最大28个字节的数据（字母、数字和特殊字符）。

#### 13.2.35.2 域描述:

转账交易中为转出账户的账（卡）号标识。

#### 13.2.35.3 用法:

本域用于转账交易时，填写转出账（卡）号。

### 13.2.36 域 103

账户标识 2(Account Identification 2)

#### 13.2.36.1 变量属性:

ans..28(LLVAR)，2个字节的长度值+最大28个字节的数据（字母、数字和特殊字符）。

#### 13.2.36.2 域描述:

转账交易中为转入账户的账（卡）号标识。

#### 13.2.36.3 用法:

本域用于转账交易时，填写转入账（卡）号。

### 13.2.37 域 128

报文鉴别码(Message Authentication Code)

#### 13.2.37.1 变量属性:

64bit二进制数。

#### 13.2.37.2 域描述:

报文来源正确性鉴别码。

#### 13.2.37.3 用法:

报文来源正确性鉴别码是对报文中的某些敏感域的数据用指定的算法计算出MAC值。产生和验证MAC应由加密机完成。

当交易报文被发送者发出之前，应由发送者产生MAC；接收者收到报文后，将重新计算MAC值，以鉴别报文在传送途中是否被篡改。

## 14 ATM 终端消息交换说明

### 14.1 报文结构说明



以下描述了中国银联代理业务ATM终端与ATMP之间使用的报文格式、报文域的定义以及编码形式，供ATM终端开发接口程序时使用。ISO8583是国际标准化组织推荐用于交换中心和银行系统通讯的报文格式，本文档是中国银联在代理业务ATM上对ISO8583标准的解释和实现。

ATM终端联机报文包含四个组成部分：报文头、报文类型标识符、位图和报文域。其结构如图53所示：

报文头	报文类型标识	位图	报文域
-----	--------	----	-----

图53 报文组成

报文头是报文的第一个数据元素。报文头与报文类型标识、位图和报文域一块组成了一个完整的报文。

报文类型标识是报文的第二个数据元素，是最高级别报文类型定义，定义了报文一般性分类，比如是金融类报文还是管理类报文。报文类型标识符长度是四个字节。每个报文都要求有报文类型标识符。

位图定义了哪些报文域会出现在报文中。位图区包含两个位图。位图一定义域2到域64，位图二定义域65到域128。

报文域构成了报文的主体，参照ISO 8583定义进行了裁剪，其中部分域的格式和内容银联进行了重新定义。

#### 14.1.1 报文头

##### 14.1.1.1 报文头组成

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

在ATM终端和ATMP处理响应报文时，报文头保持原值返回。表65是报文头的具体组成，共占12个字节。

表76 报文头组成

应用类别	规范版本号	终端状态	保留使用
n2	n2	n1	n7

##### 14.1.1.2 应用类别

应用类别是报文头的第一个元素，表示后跟的报文类型，长度是2 个字节，接入模块根据该域决定路由。具体值定义如表77所示：

表77 报文头—应用类别定义

值	含义	包含交易说明
65	ATM 交易类	包括余额查询、明细查询、取款（及关联交易）、转账、修改密码等交易
75	ATM 代理业务类	现有的 ATM 代理业务类交易（及关联交易）
85	ATM 主动管理类	所有由 ATM 发起的管理类交易
99	ATM 被动管理类	所有 ATM 能够处理的被动管理类交易

##### 14.1.1.3 规范版本号

规范版本号是报文头的第二个元素，表示该报文采用何种规范，长度为2个字节。具体值定义如表78所示：

表78 报文头—规范版本号定义

值	含义
01	2003 年中国银联 ATM 应用规范版本

##### 14.1.1.4 终端状态

终端状态是报文头的第三个元素，表示该报文表示的交易状态，长度为1个字节。具体值定义如表79所示：

表79 报文头—终端状态定义

值	含义
0	正常交易状态
1	测试交易状态

14.1.1.5 保留使用

保留使用是报文头的第四个元素，暂不使用，默认填为“0”，长度为7个字节。

‘0000000’：为默认。

‘0000001’：为公钥下载标志。

‘0000002’：为EMV参数下载标志。

14.1.2 位图说明

在网络中传输报文的长度是变化的，报文中带有位图来标识报文中有哪些域而没有哪些域。一个报文中可以有有一个或两个位图，根据交易类型确定位图数量。

14.1.2.1 第一个位图

每一个报文都有第一个位图，即主位图。它是由64个二进制位(8个字节)构成，位于报文类型标识符之后。除了第一位，每一位和一个域相对应，即和域2到域64相对应。每位的值指示该域是否出现在报文中：

——如果一个位为 0，与之相关的域不出现在报文中。

——如果一个位为 1，与之相关的域出现在报文中。

域号是1的域即是第二个位图，因此基本位图的第一位用来指明在主位图后是否还有第二个位图。

14.1.2.2 第二个位图

主位图的第一位指明了主位图后是否有第二个位图—位图二。和主位图相同，位图二也由64个二进制位(八字节)构成。可以认为位图二是主位图的扩展，和域65到128相关。

只有当报文中包含有域65到域128中的域，位图二才会使用到。位图二紧接着主位图，并在报文域之前。每一位和一个域相对应，即和域65到域128相对应。每位的值指示该域是否出现在报文中：

——如果一个位为 0，与之相关的域不出现在报文中。

——如果一个位为 1，与之相关的域出现在报文中。

14.2 说明

14.2.1 符号约定

消息交换中用到的符号约定如表80所示：

表80 符号约定

符号	含义
M	必须填写的域
C	某条件成立时必须填写的域
C+	某条件成立时增加的域
C-	某条件成立时删除的域
M+	必须增加的域
O	受理方和发卡方自选填写的域
→	转发域
	必须与先前报文中对应域的值相同的域
00	自定义数据元中须填充 0 的域
	必须去除的域

### 14.2.2 报文域条件数据元说明

报文域条件数据元说明如下：

- C1：当域 22 (POS ENTRY MODE CODE) 指明为磁条卡输入，且磁卡上存在第二磁道信息时本域出现。
- C2：当域 22 (POS ENTRY MODE CODE) 指明为磁条卡输入，且磁卡上存在第三磁道信息时，本域出现。
- C3：当域 52 (PIN DATA) 出现时，本域出现。
- C4：签到交易时，本域必须出现。
- C5：发送吞卡通知时，2 号域必须出现。
- C6：发送故障通知时，90 号域必须出现。

### 14.2.3 各栏含义

后续表中各栏含义说明见表81：

表81 各栏含义

栏名	含义
位	表示字段在位图中的位置
数据元	字段名称
类型	字段类型
请求	ATM 与 ATMP 之间的请求报文
响应	ATM 与 ATMP 之间的响应报文

## 14.3 业务类交易报文

## 14.3.1 取款

取款交易用于向发卡方请求对持卡人取现行为及金额的确认，本交易可引发冲正通知，ATM只有在确切未吐钞的情况下才发送冲正通知。取款交易报文见表82。

表82 取款交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	01X000	M	
4	交易金额	n12	M	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡方终端标识	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
60	消息原因	ans30	M		
100	接收机构标识码	n..11(LLVAR)		M	
128	MAC	b64	M	M	

## 14.3.2 取款冲正

当ATM在限定的时间内收不到取款请求报文的应答，或收到的取款成功应答，但校验MAC发现错误，或收到取款成功应答，但在吐钞过程中发生故障而未吐钞，ATM应引发取款冲正交易。交易报文见表83。

当ATM作为冲正发送方未能收到冲正应答时，则必须不断引发冲正交易，直至收到冲正成功的正确应答报文。

冲正交易必须与原交易发生在同一个结算日内进行。

表83 取款冲正交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0420	0430	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	M	M	
4	交易金额	n12	M	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
15	清算日期	n4		M+	
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
37	检索参考号	an12	M	M	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
60	消息原因	ans30	M		
90	原始数据元	n42	M		
100	接收机构标识码	n..11(LLVAR)		M	
128	MAC	b64	M	M	

#### 14.3.3 吐钞确认

ATM在收到取款成功的应该报文后，执行吐钞动作成功，应向ATMP发送吐钞确认交易报文，如表84所示。ATMP对于本请求报文不发送响应报文。

表84 吐钞确认交易报文

位	数据元	类型	原交易	确认	备注
-	报文类型	n4	0200	0200	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	01X000	02X000	
4	交易金额	n12	M	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
32	受理机构标识码	n..11(LLVAR)		M	

位	数据元	类型	原交易	确认	备注
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
43	受卡方名称地址	ans40	M	M	
49	交易货币代码	an3	M	M	
100	接收机构标识码	n..11(LLVAR)		M	
128	MAC	b64	M	M	

#### 14.3.4 余额查询

余额查询交易用于查询银行卡账面余额或可用余额。本交易不引发冲正。交易报文见表85。

当ATM接收不到ATMP的应答时，将直接拒绝该交易。

表85 余额查询交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	30X000	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
54	附加金额	An...40(LLVAR)		M	余额
60	消息原因	ans30	M		
100	接收机构标识码	n..11(LLVAR)		M	

位	数据元	类型	请求	响应	备注
128	MAC	b64	M	M	

#### 14.3.5 明细查询

明细查询交易用于查询银行卡账户最近的交易记录情况。本交易不引发冲正。交易报文见表86。  
当ATM接收不到ATMP的应答时，将直接拒绝该交易。

表86 明细查询交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	39X000	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
59	明细数据	ans...600(LLVAR)	M	M	
60	消息原因	ans30	M		
100	接收机构标识码	n..11(LLVAR)		M	
128	MAC	b64	M	M	

#### 14.3.6 转账

ATM仅作为转账交易的发起方参与交易。本交易不引发冲正。交易报文见表87。

表87 转账交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	40X000	M	

位	数据元	类型	请求	响应	备注
4	交易金额	n12	M	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4	O	M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
60	消息原因	ans30	M		
100	接收机构标识码	n..11(LLVAR)		M	
102	转出账号	ans..28(LLVAR)	M	M	
103	转入账号	ans..28(LLVAR)	M	M	
128	MAC	b64	M	M	

#### 14.3.7 修改密码

ATM发送交易给ATMP，ATMP完成相关处理后给ATM应答，ATM根据应答码进行操作。本交易不引发冲突。交易报文见表88。

当ATM接收不到ATMP的应答时，将直接拒绝该交易。

表88 修改密码交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0100	0110	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	70X000	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		



位	数据元	类型	请求	响应	备注
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
43	受卡方名称地址	ans40	M		
48	新密码数据	ans...512(LLVAR)	M	M	用法十
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
60	消息原因	ans30	M		
100	接收机构标识码	n..11(LLVAR)		M	
128	MAC	b64	M	M	

#### 14.3.8 代缴费查询

代缴费查询交易用于查询用户要缴的代缴费，如水电费等。本交易不引发冲正。交易报文见表89。  
当ATM接收不到ATMP的应答时，将直接拒绝该交易。

表89 代缴费查询交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	31X000	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
42	受卡方标识码	ans15	M	M	
43	受卡方名称地址	ans40	M		
48	代理业务系统数据	ans...512(LLVAR)	M	M	用法一
49	交易货币代码	an3	M	M	
60	消息原因	ans30	M		

位	数据元	类型	请求	响应	备注
128	MAC	b64	M	M	

#### 14.3.9 实时缴费

实时缴费交易用于持卡人确认缴费查询后向发卡方发送请求完成银行卡扣款,是代缴费交易的第二个流程。本交易不引发冲正。交易报文见表90。

表90 实时缴费交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	19X000	M	
4	交易金额	n12	M	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12	M	M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
42	受卡方标识码	ans15	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
48	代理业务系统数据	ans...512(LLVAR)	M	M	用法一
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
60	消息原因	ans30	M		
100	接收机构标识码	n..11(LLVAR)		M	
128	MAC	b64	M	M	

#### 14.3.10 充值

充值交易的报文与实时缴费报文格式一致,在48号域的具体用法上存在区别,详见域48中用法一的定义说明。

#### 14.3.11 EMV 卡发起的取款

取款交易用于向发卡方请求对持卡人取现行为及金额的确认,本交易可引发冲正通知,ATM只有在确切未吐钞或发卡方批准而卡最终拒绝交易时的情况下才发送冲正通知。

表91 EMV 卡取款交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	01X000	M	
4	交易金额	n12	M	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
23	卡片序列号	N3	C	C	如果卡上有
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
38	授权码	An6		C	
39	响应码	an2		M+	
41	受卡方终端标识	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
55	IC 卡数据域	最大 255 字节数据	M	M	
9F26 (tag)	应用密文	b64	M		
9F27 (tag)	应用信息数据	b8	M		
9F10 (tag)	发卡行应用数据	b...256	M		
9F37 (tag)	不可预知数	b32	M		
9F36 (tag)	应用交易计数器	b16	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	M		
9A (tag)	交易日期	n6	M		
9C (tag)	交易类型	n2	M		
9F02	授权金额 <sup>a</sup>	n12	M		

位	数据元	类型	请求	响应	备注
(tag)					
5F2A (tag)	交易货币代码 <sup>b</sup>	n3	M		
82 (tag)	应用交互特征	b16	M		
9F1A (tag)	终端国家代码	n3	M		
9F03 (tag)	其它金额 <sup>c</sup>	n12	M		
9F33 (tag)	终端性能	b24	M		
9F34 (tag)	持卡人验证结果	b24	O		
9F35 (tag)	终端类型	n2	O		
9F1E (tag)	接口设备序列号	an8	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	O		
9F09 (tag)	应用版本号	b16	O		
9F41 (tag)	交易序列计数器	n...4	O		
91 (tag)	发卡行认证数据	b...128		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		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		C	若处理中心返回应答, 则在响应中出现
60	消息原因	ans30	M		
60.1	交易类型码	n4	M		
60.2	服务点附加信息	ans10	M		
60.3	批次号网络管理码	n14	M		
60.4	终端读取能力	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。上述各类情况中该域都填 5。
60.5	基于 PBOC 借/贷记标准的 IC 卡条件代码	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。IC 卡交易、Fall Back 交易根据实际情况填写。纯磁条卡交易发生在 IC 卡终端上填 0。
100	接收机构标识码	n..11(LLVAR)		M	

位	数据元	类型	请求	响应	备注
128	MAC	b64	M	M	

#### 14.3.12 EMV 卡发起的余额查询

余额查询交易用于查询银行卡账面余额或可用余额。本交易不引发冲正。

当ATM接收不到ATMP的应答时，将直接拒绝该交易。

表92 EMV 卡余额查询交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	30X0 00	M	
7	传输日期和时间	n10(MMDDhhmmss )	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
23	卡片序列号	N3	C	C	如果卡上有
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
42	受卡方标识码		M	M	
43	受卡方名称地址	ans40	M		
44	附加响应数据	ans..25		M	
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
54	附加金额	An...40(LLVAR)		M	余额

位	数据元	类型	请求	响应	备注
60	消息原因	ans30	M		
60.1	报文原因码	N4	M		
60.2	服务点附加信息	ans10	M		
60.3	批次号	N14	M		
60.4	终端读取能力	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。上述各类情况中该域都填 5。
60.5	基于 PBOC 借/贷记标准的 IC 卡条件代码	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。IC 卡交易、Fall Back 交易根据实际情况填写。纯磁条卡交易发生在 IC 卡终端上填 0。
100	接收机构标识码	n..11(LLVAR)		M	
128	MAC	b64	M	M	

#### 14.3.13 EMV 卡发起的明细查询

明细查询交易用于查询银行卡账户最近的交易记录情况。本交易不引发冲正。

当ATM接收不到ATMP的应答时，将直接拒绝该交易。

表93 EMV 卡明细查询交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	39X000	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
23	卡片序列号	N3	C	C	
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		

位	数据元	类型	请求	响应	备注
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
39	响应码	an2		M+	
41	受卡机终端标识码	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
59	明细数据	ans...600(LLVAR)	M	M	
60	消息原因	ans30	M		
100	接收机构标识码	n..11(LLVAR)		M	
60	消息原因		M		
60.1	报文原因码	N4	M		
60.2	服务点附加信息	ans10	M		
60.3	批次号	N14	M		
60.4	终端读取能力	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。上述各类情况中该域都填 5。
60.5	基于 PBOC 借/贷记标准的 IC 卡条件代码	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。IC 卡交易、Fall Back 交易根据实际情况填写。纯磁条卡交易发生在 IC 卡终端上填 0。
128	MAC	b64	M	M	

## 14.3.14 EMV 卡发起的转账，转出卡为 EMV 卡

表94 EMV 卡转账交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0200	0210	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	04X000	M	
4	交易金额	n12	M	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	

位	数据元	类型	请求	响应	备注
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
23	卡片序列号	N3	C	C	
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
35	第二磁道数据	Z..37(LLVAR)	C1		
36	第三磁道数据	Z...104(LLVAR)	C2		
37	检索参考号	an12		M+	
38	授权码	An6		C	
39	响应码	an2		M+	
41	受卡方终端标识	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
55	IC 卡数据域	最大 255 字节数据			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	M		
9F27 (tag)	应用信息数据	b8	M		
9F10 (tag)	发卡行应用数据	b...256	M		
9F37 (tag)	不可预知数	b32	M		
9F36 (tag)	应用交易计数器	b16	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	M		
9A (tag)	交易日期	n6	M		
9C (tag)	交易类型	n2	M		
9F02 (tag)	授权金额 <sup>a</sup>	n12	M		
5F2A (tag)	交易货币代码 <sup>b</sup>	n3	M		
82 (tag)	应用交互特征	b16	M		
9F1A (tag)	终端国家代码	n3	M		
9F03 (tag)	其它金额 <sup>c</sup>	n12	M		
9F33 (tag)	终端性能	b24	M		
9F34 (tag)	持卡人验证结果	b24	O		
9F35 (tag)	终端类型	n2	O		
9F1E (tag)	接口设备序列号	an8	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	O		
9F09 (tag)	应用版本号	b16	O		
9F41 (tag)	交易序列计数器	n...4	O		
91 (tag)	发卡行认证数据	b...128		C	若处理中心返回应答, 则在响应中出现



位	数据元	类型	请求	响应	备注
71 (tag)	发卡行脚本 1	b...1024		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		C	若处理中心返回应答, 则在响应中出现
60	消息原因	ans30	M		
60.1	报文原因码	N4	M		
60.2	服务点附加信息	Ans10	M		
60.3	批次号	N14	M		
60.4	终端读取能力	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。上述各类情况中该域都填 5。
60.5	基于 PBOC 借/贷记标准的 IC 卡条件代码	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。IC 卡交易、Fall Back 交易根据实际情况填写。纯磁条卡交易发生在 IC 卡终端上填 0。
100	接收机构标识码	n..11(LLVAR)		M	
102	转出账号	ans..28(LLVAR)	M	M	
103	转入账号	ans..28(LLVAR)	M	M	
128	MAC	b64	M	M	

其中23域、55域信息为转出卡信息。

#### 14.3.15 EMV 卡取款交易冲正

当ATM在限定的时间内收不到取款请求报文的应答, 或收到的取款成功应答, 但校验MAC发现错误, 或收到取款成功应答, 但在吐钞过程中发生故障而未吐钞, ATM应引发取款冲正交易。交易报文见表96。

当ATM作为冲正发送方未能收到冲正应答时, 则必须不断引发冲正交易, 直至收到冲正成功的正确应答报文。

冲正交易必须与原交易发生在同一个清算日内进行。

表95 取款冲正交易报文

表96

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0400	0410	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	
3	处理码	n6	01X000	M	
4	交易金额	n12	M	M	
7	传输日期和时间	n10(MMDDhhmmss)	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	

位	数据元	类型	请求	响应	备注
13	本地交易日期	n4(MMDD)	M	M	
14	卡片有效日期	n4		M	
15	清算日期	n4		M+	
22	服务点输入方式码	n3	M		
23	卡片序列号	N3	C	C	如果原交易有
26	服务点 PIN 采集代码	n2	M		
32	受理机构标识码	n..11(LLVAR)		M	
33	发送机构标识码	n..11(LLVAR)		M	
37	检索参考号	an12		M+	
38	授权码	An6		C	
39	响应码	an2		M+	
41	受卡方终端标识	ans8	M	M	
43	受卡方名称地址	ans40	M		
49	交易货币代码	an3	M	M	
52	个人密码	b64	M		
53	安全控制信息	n16	C3		
55	IC 卡数据域	最大 255 字节数据			
9F26 (tag)	应用密文	b64			
9F27 (tag)	应用信息数据	b8			
9F10 (tag)	发卡行应用数据	b...256			
9F37 (tag)	不可预知数	b32			
9F36 (tag)	应用交易计数器	b16	M	C	M: 同原交易 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
95 (tag)	终端验证结果	b40	C		C: 如果是卡没有批准的冲正, TAG95 为新值
9A (tag)	交易日期	n6			
9C (tag)	交易类型	n2			
9F02 (tag)	授权金额 <sup>a</sup>	n12			
5F2A (tag)	交易货币代码 <sup>b</sup>	n3			
82 (tag)	应用交互特征	b16			
9F1A (tag)	终端国家代码	n3			
9F03 (tag)	其它金额 <sup>c</sup>	n12			
9F33 (tag)	终端性能	b24			
9F34 (tag)	持卡人验证结果	b24			
9F35 (tag)	终端类型	n2			
9F1E (tag)	接口设备序列号	an8			

位	数据元	类型	请求	响应	备注
84 (tag)	专用文件名称	b...128			
9F09 (tag)	应用版本号	b16			
9F41 (tag)	交易序列计数器	n...4			
91 (tag)	发卡行认证数据	b...128			
71 (tag)	发卡行脚本 1	b...1024			
72 (tag)	发卡行脚本 2	b...1024			
DF31(tag)	发卡行脚本结果	b...168		C	C: 如果执行脚本
60	消息原因	ans30	M	M	
60.1	报文原因码	N4	M		
60.2	服务点附加信息	ans10	M		
60.3	批次号	N14	C		
60.4	终端读取能力	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。上述各类情况中该域都填 5。
60.5	基于 PBOC 借/贷记标准的 IC 卡条件代码	N1	C		仅在 IC 卡交易、Fall Back、纯磁条卡交易发生在 IC 卡终端等情况下出现。IC 卡交易、Fall Back 交易根据实际情况填写。纯磁条卡交易发生在 IC 卡终端上填 0。
100	接收机构标识码	n..11(LLVAR)		M	
128	MAC	b64	M	M	

注： 由下列情形引发冲正：

- ATM在时限内未能收到ATMP的应答消息而引发，冲正原因码填“98”。
- ATM在时限内收到ATMP的批准应答消息，但由于ATM故障无法完成交易而引发，冲正原因码填“96”。
- ATM对收到ATMP的应答消息，验证MAC出错，冲正原因码填“A0”。
- 其他情况，冲正原因码填“06”。

#### 14.3.16 EMV 卡交易转账冲正交易

由于银联交换系统不支持受理方对转账交易的冲正，故终端不支持转账冲正交易。

#### 14.3.17 降级交易

报文格式同相应的磁条交易报文，但60.4、60.5编码为51或52。

#### 14.3.18 降级交易冲正

报文格式同相应的磁条交易冲正报文，但60.4、60.5编码为51或52。

## 14.4 主动管理类交易报文

## 14.4.1 签到

ATM签到时，把当前的ATM的软件版本号及参数版本号上送。ATM接收到的响应报文中应包含新的工作密钥等参数。交易报文见表97。

表97 签到报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	An2		M	
41	受卡机终端标识码	ans8	M	M	
48	签到交换数据	ans...512(LLLVAR)	C4	C4	用法五 用法六
70	网络管理信息码	n3	M	M	

## 14.4.2 事件通知

事件通知包括定时状态报告、状态切换报告、故障通知、提醒通知、吞卡通知等管理类交易。事件通知交易主要用于ATM的监控管理。交易报文见表98。

表98 事件通知报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	C5	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备状态数据	ans...512(LLLVAR)	M	M	用法三
70	网络管理信息码	n3	M	M	
90	原始数据元	n42	C6		

## 14.4.3 钞箱管理交易

钞箱管理交易包括加钞通知等管理类交易。

加钞通知交易用于现金管理人员通知ATM的实际加钞情况。交易报文见表99。

表99 钞箱管理交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	

位	数据元	类型	请求	响应	备注
39	响应码	An2		M	
41	受卡机终端标识码	ans8	M	M	
48	钞箱信息数据	ans...512(LLVAR)	M	M	用法二
70	网络管理信息码	n3	M	M	

#### 14.4.4 批上送交易明细

接收到ATMP端要求上传交易明细的通知后，ATM将指定清算日或者批次号的所有成功交易的明细信息上传给ATMP。交易报文见表100。

当ATM与ATMP对账不平时，应自动发起批上送交易明细，具体上送的交易数量应该根据ATMP返回的对账数据中与ATM本地记录不符的交易类型来决定，目前仅对涉及资金清算的交易记录进行核对。

表100 批上送交易明细报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	交易明细包数据	ans...512(LLVAR)	M		用法八
70	网络管理信息码	n3	M	M	

#### 14.4.5 批上送结束通知

当ATM将指定清算日的交易明细上送结束后，发送该报文，通知ATMP交易明细批上送结束。交易报文见表101。

表101 批上送结束通知报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	Ans8	M	M	
48	批上送统计数据	Ans...512(LLVAR)	M	M	用法九
70	网络管理信息码	n3	M	M	

#### 14.4.6 对账交易

对账用于核对某一清算日或者当前会计周期的钞箱变化情况。接收到请求后的ATMP应根据交易情况的统计信息以及加钞通知，给予相应的回答。交易报文见表102。

ATM在接收到对账不平的回应报文后，应自动发起批上送交易明细交易，发送成功之后再发送批上送结束通知完成整个对账过程。

表102 对账交易报文

位	数据元	类型	请求	响应	备注
---	-----	----	----	----	----

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0520	0530	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
41	受卡机终端标识码	ans8	M	M	
48	对账数据	ans...512(LLLVAR)	M	M	用法七
66	结算响应码	n1		M	

## 14.4.7 EMV 卡交易公钥列表下载

表103 公钥列下载交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备参数数据	ans...512(LLLVAR)	M	M	用法十一
70	网络管理信息码	n3	M	M	

## 14.4.8 EMV 卡交易单个公钥下载

表104 列单个公钥下载交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备参数数据	ans...512(LLLVAR)	M	M	用法十三
70	网络管理信息码	n3	M	M	

## 14.4.9 EMV 卡 AID 列表下载

表105 AID 列表下载交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	

位	数据元	类型	请求	响应	备注
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备参数数据	ans...512(LLVAR)	M	M	用法十二
70	网络管理信息码	n3	M	M	

## 14.4.10 EMV 卡单个 AID 相关的参数下载

表106 单个 AID 参数下载交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备参数数据	ans...512(LLVAR)	M	M	用法十四
70	网络管理信息码	n3	M	M	

## 14.4.11 TC 上送通知

当一笔EMV卡取款交易卡最终批准后，ATM应实时上送交易TC。

表107 基于 EMV 卡交易 TC 上送通知报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	同原交易
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
23	卡片序列号	n3	C	C	C:如果卡有
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备状态数据	ans...512(LLVAR)	M	M	用法十五
55	IC 卡数据域	最大为 255 字节			
9F33(tag)	终端性能	b24	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	C		C: 如果参与 TC 运算的值
9F37(tag)	不可预知数	b32	C		C: 如果参与 TC 运算的值
9F1E(tag)	接口设备序列号	an8	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	M		新值
9F26(tag)	应用密文	b64	M		
9F36(tag)	应用交易计数器	b16	M	C	M: 参与 TC 运算的值 C: 如果应答
82(tag)	应用交互特征	b16	C		同原交易
9F1A(tag)	交易国家代码	n3	C		同原交易
9A(tag)	交易日期	n6	C		同原交易
70	网络管理信息码	n3	M	M	
90	原始数据元	n42	C6		

#### 14.4.12 脚本通知

当一笔交易（仅指余额查询、取现、消费、预授权）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。该交易随同下一步交易一并发送。若在发送下一步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108 基于 PBOC 借/贷记标准 IC 卡脚本处理结果通知报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
2	主账号	n..19(LLVAR)	M	M	同原交易
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
23	卡片序列号	n3	C	C	C:如果卡有
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备状态数据	ans...512(LLVAR)	M	M	用法十六
55	IC 卡数据域	最大为 255 字节			
9F33(tag)	终端性能	b24			
95(tag)	终端验证结果	b40	C		C: 如果参与 TC 运算的值
9F37(tag)	不可预知数	b32			
9F1E(tag)	接口设备序列号	an8			
9F10(tag)	发卡行应用数据	b...256			
9F26(tag)	应用密文	b64			
9F36(tag)	应用交易计数器	b16	M	C	C: 如果应答
82(tag)	应用交互特征	b16			
9F1A(tag)	交易国家代码	n3			
9A(tag)	交易日期	n6			
DF31(tag)	发卡行脚本结果	b...168		M	
70	网络管理信息码	n3	M	M	
90	原始数据元	n42	C6		



## 14.5 被动管理类交易报文

### 14.5.1 ATM 管理

ATM管理交易包括打开ATM终端、关闭ATM终端。ATM管理交易是ATM与ATMP之间的网络管理操作信息，用于改变ATM工作状态以及网络应用层联通测试等。交易报文见表209。

表109 ATM 管理交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
70	网络管理信息码	n3	M	M	

### 14.5.2 设备状态查询

设备状态查询用于ATM的监控管理。交易报文见表110。

表110 设备状态查询交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备状态数据	ans...512(LLLVAR)		M	用法三
70	网络管理信息码	n3	M	M	

### 14.5.3 参数下载

ATMP在更新后ATM的参数后，可以执行该操作将参数直接更新到相应的ATM上。交易报文见表111。

表111 参数下载交易报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	设备参数数据	ans...512(LLLVAR)	M	M	用法四
70	网络管理信息码	n3	M	M	

### 14.5.4 通知上传交易明细

通知上传交易明细用于通知ATM将某清算日或者某批次号的成功交易明细按照交易时间排序上传ATMP，以便于交易勾对、差错信息查询确认等。目前只限于把涉及资金清算的交易记录上传给ATMP。交易报文见表112。

表112 通知上传交易明细报文

位	数据元	类型	请求	响应	备注
-	报文类型	n4	0820	0830	
-	位元表	b128	M	M	
11	系统跟踪号	n6	M	M	
12	本地交易时间	n6(hhmmss)	M	M	
13	本地交易日期	n4(MMDD)	M	M	
39	响应码	an2		M	
41	受卡机终端标识码	ans8	M	M	
48	交易明细包数据	ans...512(LLLVAR)	M	M	用法八
70	网络管理信息码	n3	M	M	

#### 14.5.5 EMV 卡交易公钥列表下载

当联机交易的响应报文头保留域编码为‘0000001’时，为公钥下载标志。此时终端在处理完当前交易后应发起下载公钥列表请求，并根据得到的公钥列表全刷新下载公钥。

同主动管理报文。

#### 14.5.6 EMV 卡交易单个公钥下载

同主动管理报文。

#### 14.5.7 EMV 卡单 ID 列表下载

当联机交易的响应报文头保留域编码为‘0000002’时，为EMV AID相关参数下载标志。此时终端在处理完当前交易后应发起下载AID列表请求，并根据得到的AID列表全刷新下载AID参数。

同主动管理报文。

#### 14.5.8 EMV 卡单个 AID 相关的参数下载

同主动管理报文。

### 15 客户凭证要素及格式要求

#### 15.1 客户凭证要素

客户凭证要素主要包括：账号、受理行标识、交易类型、交易金额、结果、转入账号、服务提供商代码、用户代码、检索参考号、系统跟踪号、终端编号、交易日期、交易时间、发卡行标识、备注。

交易凭证打印的卡号，除被吞卡和转账交易的转入卡外，应根据当地业务监管机构要求隐去但不限于卡号校验位前4位数字。

#### 15.2 格式要求

##### 15.2.1 总体要求

除吞卡以外的交易，由客户决定是否打印凭证，吞卡时必须按照要求打印客户凭证。

吞卡前需要确认凭证打印模块是否正常，当凭证打印模块发生故障时不得进行吞卡操作。

打印客户凭证应该根据客户对界面的选择而自动的打印相应的中文或者英文格式，如果ATM支持双语显示，则客户凭证同时打印中英文。

##### 15.2.2 账号

中文标题：账号

英文标题：Account Number

内容：银行卡的主账号PAN

要求：必选

说明： 最长19位数字  
 样例： 5359 1800 120\* \*\*\*1  
 对应域： 2号域

### 15.2.3 受理行标识

中文标题：受理行标识  
 英文标题：Acquirer ID  
 内容： 受理行号  
 要求： 必选  
 说明： 最大长度11位数字  
 样例： 00000900011  
 对应域： 32号域

### 15.2.4 交易类型

中文标题：交易类型  
 英文标题：Trans Type  
 内容： 交易类型的英文或中/英文名称  
 要求： 必选  
 说明： 中文名称（取款、转账、代理业务、修改密码）  
 英文名称(Withdrawal、Transfer、Payment、Chg PIN)  
 对应域： 消息类型+3号域

### 15.2.5 交易金额

中文标题：交易金额  
 英文标题：Transaction Amount  
 内容： 交易金额  
 要求： 必选  
 说明： 精确到分，元与角之间用“.”隔开。打印时金额数值前应印出表示货币种类的前缀，前缀与金额数值之间不得有空格。  
 样例： ¥1200.00 或 RMB 1200.00  
 对应域： 4号域

### 15.2.6 结果

中文标题：结果  
 英文标题：Result  
 内容： ATMP响应的应答代码，用于备查  
 要求： 必选  
 说明： 一般情况下，当操作时没有硬件模块故障发生时，根据ATMP返回报文的39号域取值，根据39号域取值时，如果是“00”，则显示“成功”（SUCCESS），否则根据39号域值进行填写，2位定长的字母和数字字符；如果39号域为“00”，但是ATM在收到报文后继续吐钞等交易动作时发生硬件故障而导致交易失败，则显示“失败”。  
 样例： 61  
 对应域： 39号域

### 15.2.7 转入账号

中文标题：转入账号  
 英文标题：In Card No.  
 内容： 转账交易的转入账号  
 要求： 转账交易必选

说明： 最长19位数字  
样例： 5359180012000001  
对应域： 39号域

#### 15.2.8 服务提供商代码

中文标题：服务提供商代码  
英文标题：Service Code  
内容： 存放代理业务的服务提供商的代码  
要求： 可选  
说明： 最大长度15位数字  
样例： 00000900011  
对应交易报文域： 42号域

#### 15.2.9 用户代码

中文标题：用户代码  
英文标题：User Code  
内容： 存放代理业务中持卡人输入的用户代码  
要求： 可选  
说明： 最大长度32位数字  
样例： 12345678901234567890123456789012  
对应域： 48号域的子域

#### 15.2.10 检索参考号

中文标题：检索参考号  
英文标题：RETRIEVAL REFERENCE NUMBER  
内容： ATMP分配的用于定位持卡人原始交易的一个系统参考号  
要求： 必选  
说明： 12位定长的字母和数字字符  
样例： 123456789012  
对应域： 37号域

#### 15.2.11 系统跟踪号

中文标题：系统跟踪号  
英文标题：SYS\_TRACE\_AUDIT\_NUM  
内容： ATM终端的交易流水号，用于备查。  
要求： 必选  
说明： 6位定长数字字符  
样例： 012345  
对应域： 11号域

#### 15.2.12 终端编号

中文标题：终端编号  
英文标题：ATM ID  
内容： ATMP为该ATM分配的编号。  
要求： 必选  
说明： 8位定长的字母、数字和特殊字符  
样例： 00456002  
对应域： 41号域

#### 15.2.13 交易日期

中文标题：日期  
 英文标题：DATE  
 内容：ATM本地的交易日期  
 要求：必选  
 说明：YYYY/MM/DD  
 样例：2001/04/20  
 对应域：MM/DD对应13号域，YYYY自拼上去。

#### 15.2.14 交易时间

中文标题：时间  
 英文标题：TIME  
 内容：ATM本次的交易时间  
 要求：必选  
 说明：HH: MM: SS  
 样例：12: 34: 56  
 对应域：12号域。

#### 15.2.15 发卡行标识

中文标题：发卡行标识  
 英文标题：Issuer ID  
 内容：如果ATM吞卡，该域填写银行卡的发卡机构代码，否则为空白  
 要求：可选  
 说明：最大长度11位数字  
 样例：12345678901  
 对应域：100号域

#### 15.2.16 备注

中文标题：备注  
 英文标题：Remark  
 内容：用于存放交易的附加信息  
 要求：可选  
 说明：最大长度40位英文字符（20个中文字符）  
 样例：1234567890123456789012345678901234567890  
 对应域：代理业务用于显示第48号域的“行业特定信息”

#### 15.2.17 EMV 卡交易凭证

由于可以受理EMV卡，凭证打印应区分EMV交易、磁条交易、降级交易，加打应用首选名称/应用标签。

### 15.3 客户凭证参考样式

#### 15.3.1 中文样式

XX现金托管机构

客户通知书

账号 12345678901234***9		受理行号 12345678901
交易类型 取款	交易金额 RMB 1500.00	结果 成功
转入账号 1234567890123456789		
代理业务信息 1234567890123456789012 123344536546457567657567		
检索参考号 123456789012	系统跟踪号 123456	终端编号 12345678
日期 2004/01/08	时间 18:06:38	发卡行标识 12345678901
备注 123456789012345678901234567890123456789		

1、如果有疑问或银行卡被自动柜员机保留，  
请凭此凭条与银行联系。

2、转账请自行通知收款人，本行不另行通知。

图54 客户凭证中文参考样式

## 15.3.2 英文样式

**XX CASH TRUSTEE CUSTOMER ADVICE**

Account Number 12345678901234***9		Acquirer ID 12345678901	
Trans Type Withdrawal	Trans Amount RMB 1500.00		Result SUCCESS
In Card No 1234567890123456789			
Agent Info 12345678901234567890123456789012 35346456457657687			
Reference No 123456789012	Trace No 123456	ATM ID 12345678	
Date 2004/01/08	Time 18:06:38	Issuer ID 12345678901	
Remark 1234567890123456789012345678901234567890123456789			

- 1、If you have any question or your card retained by ATM, please contact the bank with this Customer Advice
- 2、Please advise the beneficiary of transfers since the Bank will not do so.

图55 客户凭证英文参考样式

## 15.4 EMV卡交易需要增加打印的交易流水单要素

名称	中文标题	英文标题	要求	格式	来源
IC 卡交易证书	IC 卡交易证书	TXN CERT.	可选 (EMV 借/贷记卡必选)		EMV 借/贷记卡
TVR	终端验证结果	TVR	可选 (EMV 借/贷记卡必选)		EMV 借/贷记卡
TSI	交易状态信息	TSI	可选 (EMV 借/贷记卡必选)		EMV 借/贷记卡
AID	应用标识	AID	可选 (EMV 借/贷记卡必选)		EMV 借/贷记卡
ATC	应用交易计数器	ATC	可选 (EMV 借/贷记卡必选)		EMV 借/贷记卡
应用标签	应用标签	Appl Label	可选 (EMV 借/贷记卡必选)		EMV 借/贷记卡
应用首选名称	应用标签	Appl Name	可选 (EMV 借/贷记卡必选)		EMV 借/贷记卡

附 录 A  
(规范性附录)  
个人标识 (PIN) 的加密和解密方法

#### A.1 用于PIN加、解密的主账号PAN取法

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。

#### A.2 PIN的长度

PIN的长度一般为6位 (可扩展到12位)。

#### A.3 PIN的字符集

PIN用数字字符表示, 表A.1给出了它的二进制对照表:

表 A.1 PIN 字符与二进制对照表

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

#### A.4 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格式见表A.2:

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格式见表A.3:

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 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

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（SECURITY-RELATED—CONTROL—INFORMATION）中标明。

附 录 B  
(规范性附录)  
ATM 交易报文 MAC 的算法

报文来源正确性鉴别(MAC-Message Authentication Code)是一种判别报文来源是否正确, 以及报文在发送途中是否被篡改的计算方法。

MAC算法取自于《ISO8731-1992 Approved Algorithms for Authentication》。

**B.1 MAC报文域的选择**

MAC域的选择采用系统约定的方式, MAC算法采用密文块链接(CBC)的模式。

参与MAC计算的数据元集, 一般包括以下数据域:

- 具有唯一性的数据域(流水号、日期、时间等);
- 表征报文特征的数据域(报文类型、交易种类等);
- 交易相关数据域(卡号、金额、应答码等)。

**B.2 消息类型为 01xx、02xx、04xx、05xx类交易的报文域选择**

以下域出现或条件成立时, 就应该包含在MAC计算中。

消息类型为01xx、02xx、04xx、05xx类交易的报文域选择见表B.1。

**表 B.1 消息类型为 01xx、02xx、04xx、05xx 类交易的报文域选择**

序号	域	域名	属性	说明
1	0	Message-type-identifier	n4	报文类型 <sup>a</sup>
2	2	Primary-account-number	n...19(LLVAR)	主账号 <sup>b</sup>
3	3	Processing-code	n6	交易处理码
4	4	Amount-of-Transactions	n12	交易金额
5	7	Transmission-date-and-time	n10	交易传输时间
6	11	System-trace-audit-number	n6	系统跟踪号
7	18	Merchants-type	n4	商户类型
8	25	Point-of-service-condition-code	n2	服务点条件码
9	28	Amount_transaction_fee	x+n 8	交易手续费
10	32	Acquiring-institution-identification-code	n..11(LLVAR)	受理机构标识码 <sup>c</sup>
11	33	Forwarding-institution-identification-code	n..11(LLVAR)	发送机构标识码 <sup>d</sup>
12	38	Authorization-identification-response	an6	授权标识应答码
13	39	Response-code	an2	应答码
14	41	Card-acceptor-terminal-identification	ans8	受卡方终端标识码
15	42	Card-acceptor-identification-code	ans15	受卡方标识码
16	90	Original-data-elements	n42	原始数据元 <sup>e</sup>
<sup>a</sup> Message-type-identifier: 报文类型 (0100/0110、0200/0210、0220/0230、0420/0430、0422/0432)				
<sup>b</sup> Primary-account-number: 主账号, 内容为两位的PAN长度+PAN				
<sup>c</sup> Acquiring-institution-identification-code: 受理机构标识码, 内容为两位的长度 (n) +最长 11 位机构标识				
<sup>d</sup> Forwarding-institution-identification-code: 发送机构标识码, 内容为两位的长度 (n) +最长 11 位机构标识				

序号	域	域名	属性	说明
<sup>e</sup> Original-data-elements: 只取前 20 位数值, 内容为: org-message-type                      n4              原始报文类型 org-system-trace-number              n6              原始报文跟踪号 org-transmission-date-time              n10              原始报文的交易传输时间				

### B.3 转账类交易的报文域选择

转账类交易包括转账、转出转账、转入转账、转出冲正、转入确认等。对于转账类交易, 只要以下域出现, 就应该包含在MAC计算中:

转账类交易的报文域选择见表B. 2。

表 B.2 转账类交易的报文域选择

序号	域	域名	属性	说明
1	0	Message-type	n4	报文类型 <sup>a</sup>
2	2	Primary-account-number	n..19(LLVAR)	主账号
3	3	Processing-code	n6	交易处理码
4	4	Amount-of-Transaction	n12	交易金额
5	7	Transmission-date-and-time	n10	交易传输日期时间
6	11	System-trace-audit-number	n6	系统跟踪号
7	18	Merchants-type	n4	商户类型
8	25	Point-of-service-condition-code	n2	服务点条件码
9	28	Amount Transaction Fee	x+n8	交易费
10	32	Acquiring-institution-identification-code	n..11(LLVAR)	受理方机构代码
11	33	Forwarding- institution-identification-code	n..11(LLVAR)	转发机构代码
12	38	Authorization-identification-response	n6	授权标识应答码
13	39	Response-code	n2	应答码
14	41	Card-acceptor-terminal-identification	an8	受卡机终端标识码
15	42	Card-acceptor-identification-code	an15	受卡方标识码
16	90	Original-data-elements	n42	原始数据元 <sup>b</sup>
<sup>a</sup> Message-type-identifier: 报文类型 (0200/0210、0420/0430) <sup>b</sup> Original-data-elements: 只取前 20 位数值, 内容为: org-message-type                      n4              原始报文类型 org-system-trace-number              n6              原始报文跟踪号 org-transmission-date-time              n10              原始报文的交易传输时间				

### B.4 对账类交易的报文域选择

对于对账类交易, 只要以下域出现, 就应该包含在 MAC 计算中:

对账类交易的报文域选择见表 B.3。

表 B.3 对账类交易的报文域选择

序号	域	域名	属性	说明
1	0	Message-type-identifier	n4	报文类型 <sup>a</sup>
2	7	Transmission-date-and-time	n10	交易传输时间
3	11	system-trace-audit-number	n6	系统跟踪号
4	66	Settlement-code	n1	清算代码

序号	域	域名	属性	说明
5	82	Processing-fee-amount-of-credits	n12	贷记服务费金额
6	84	Processing-fee-amount-of-debits	n12	借记服务费金额
7	86	Amount-of-credits	n16	贷记交易金额
8	87	Reversal-amount-of-credits	n16	冲正贷记金额
9	88	Amount-of-debits	n16	借记交易金额
10	89	Reversal-amount-of-debits	n16	冲正借记金额
11	97	Amount-of-net-settlement	X+n16	净清算额 <sup>b</sup>
<sup>a</sup> Message-type-identifier: 报文类型 (0520/0530、0522/0532)				
<sup>b</sup> Amount-of-net-settlement: 净清算额, 内容为 1 位符号位 (C—贷记/D—借记) +16 位数字的净清算额				

## B.5 MAC域的构成规则

### B.5.1 MAC字符选择:

对所选择的MAC报文域, 应进一步作字符处理。除去一些冗余信息, 以提高MAC的质量。处理方法如下:

- 带长度值的域在计算 MAC 时应包含其长度值信息;
- 在域和域之间插入一个空格;
- 所有的小写字母转换成大写字母;
- 除了字母(A-Z), 数字(0-9), 空格, 逗号(,)和点号(.)以外的字符都删去;
- 删去所有域的起始空格和结尾空格;
- 多于一个的连续空格, 由一个空格代替。

### B.5.2 MAC块(MAB)的构成:

数据从报文中选择出来后, 经MAC字符选择处理, 然后构成MAB(Message Authentication Block)。构成MAB的方法是:

将MAC字符选择处理后的数据按64bit划分成64bit的块, 一直划分到数据的最后一块, 它的位数小于或等于64bit, 不满64bit时补二进制0。

## B.6 通过MAB计算MAC的方法(单倍长密钥算法)

将MAB中的每8个字节分为一组(最后一组如不足8个字节, 则右补0X00), 用MAK作为单倍长密钥密钥依次对除最后一组外的每一组进行如下操作:

- 进行单倍长密钥运算
- 将运算结果与后一组的 8 个字节异或, 结果取代后一组, 继续进行操作。对最后一组进行单倍长密钥运算, 得出 8 个字节的加密值。

附 录 C  
(资料性附录)  
ATM 终端显示规定

为规范银行卡跨行交易应答码在ATM终端的显示内容，根据银联函[2003]61号文件“关于印发《银行卡跨行交易应答码终端显示规定（试行）》的通知”中与ATM终端相关的规定为依据进行编写，本规范中描述为银联函[2003]61号文件中关于ATM终端部分的全部引述，未做修改。

银行卡自动柜员机（ATM）显示内容面向持卡人，用于引导持卡人正确操作，正确地完成银行卡自助业务。根据现有跨行业务种类及交易应答码（消息报文的39号域）的不同，银行卡自动柜员机（ATM）显示内容分别设为20类，具体提示内容参见表C.1。

表 C.1 ATM 终端显示规定

序号	ATM 终端显示内容	Code	Response Description	Action	含 义
1	交易成功 Transaction successful	00	Approved or completed successfully	Approve	承兑或交易成功
2	交易失败，请联系发卡行 Transaction failed, please contact the issuer	01	Refer to card issuer	Decline	查发卡行
		02	Refer to card issuer's special condition	--	查发卡行的特殊条件
		05	Do not honor	Decline	不予承兑
		06	Error	--	出错
		12	Invalid transaction	--	无效交易
		14	Invalid card number (no such number)	Decline	无效卡号
		20	Invalid response	--	无效应答
		21	No action taken	--	不作任何处理
		23	Unacceptable transaction fee	Decline	不可接受的交易费
		25	Unable to locate record on file	--	未能找到文件上记录
		30	Format error	--	格式错误
		39	No credit account	Decline	无此信用卡账户
		40	Requested function not supported	Decline	请求的功能尚不支持
		42	No universal account	Decline	无此账户
		44	No investment account	Decline	无此投资账户
		52	No chequing account	Decline	无此支票账户
		53	No saving account	Decline	无此储蓄卡账户
		56	No card record	--	无此卡记录
		57	Transaction not permitted to cardholder	Decline	不允许持卡人进行的交易
		58	Transaction not permitted to terminal	Decline	不允许终端进行的交易
		59	Suspected fraud	Decline	有作弊嫌疑

序号	ATM 终端显示内容	Code	Response Description	Action	含 义
		62	Restricted card	Decline	受限制的卡
		63	Security violation	--	违反安全保密规定
		64	Original amount incorrect	Decline	原始金额不正确
		93	Transaction cannot be completed. Violation of law	Decline	交易违法、不能完成
3	卡片没收, 请联系发卡行 Card retained, please contact issuer	04	Pick-up	Pick-up	没收卡(仅限于受理外卡)
		07	Pick-up card, special condition	Pick-up	特殊条件下没收卡
		34	Suspected fraud	Pick-up	有作弊嫌疑
		41	Lost card	Pick-up	丢失卡
		43	Stolen card, pick-up	Pick-up	被窃卡
		67	Hard capture (requires that card be picked up at ATM)	Pick-up	捕捉
4	金额有误, 请重试 Invalid amount, please retry	13	Invalid amount	--	无效金额
5	此卡不能受理 Card not accepted	15	No such issuer	Decline	无此发卡行
		31	Bank not supported by switch centre	Decline	银联不支持的银行
6	交易失败, 请重试 Transaction failed, please try again	19	Re-enter transaction	Decline	重新送入交易
7	操作有误, 请重试 Wrong operation, please try again	22	Suspected malfunction	--	怀疑操作有误
8	卡片过期, 请联系发卡行 Card expired, please contact the issuer	33	Expired card	Decline	过期的卡
		54	Expired card	Decline	过期的卡
9	此卡有误, 请联系发卡行 Card restricted, please contact issuer	36	Restricted card	--	受限制的卡
10	密码错误次数超限 Wrong pin, tries exceeded	38	Allowable PIN tries exceeded	Decline	超过允许的 PIN 试输入
		75	Allowable number of PIN tries exceeded	Decline	允许的输入 PIN 次数超限
11	余额不足, 请查询 Balance Insufficient, please inquire	51	Not sufficient funds	Decline	无足够的存款
12	密码错, 请重试 Incorrect pin, please try again	55	Incorrect personal identification number	Decline	不正确的 PIN
13	取款金额超限或未达最低取款金额 Exceeds withdrawal amount limit	61	Exceeds withdrawal amount limit	Decline	超出取款金额限制

序号	ATM 终端显示内容	Code	Response Description	Action	含 义
14	超过取款次数限制 Exceeds withdrawal frequency limit	65	Exceeds withdrawal frequency limit	Decline	超出取款次数限制
15	交易超时,请稍后重试 Time out, please retry later	68	Response received too late	--	收到的回答太迟
		98	SW couldn't get reply from IS	--	银联收不到发卡行应答
16	交易失败, 请稍后重试 Transaction failed, please retry later	09	Request in progress	--	请求正在处理中
		90	Cutoff is in process	--	日期切换正在处理
		91	Issuer or switch is inoperative	Decline	发卡行或银联不能操作
		92	Financial institution or intermediate network facility cannot be found for routing	Decline	金融机构或中间网络设施找不到或无法达到
		94	Duplicate transaction	--	重复交易
		95	Reconcile error	--	调节控制错
		96	System malfunction	--	系统异常、失效
		99	PIN Block Error	--	PIN 格式错
		A0	MAC failed	--	MAC 鉴别失败
17	无效终端, 请联系银联 Invalid terminal, please contact switch centre	97	Invalid ATM IDs	--	ATM 终端号找不到
18	转账货币不一致, 交易无法完成 Different currencies, can't transfer	A1		--	转账货币不一致
19	交易超时, 请查询转入账户 Time out, please inquiry the destination account	A2		--	转入行超时
20	无此转入账户 No destination account	A3		--	转入行无此账户

附 录 D  
(资料性附录)  
ATM 终端标识码编码规则

ATM终端标识码在ATM网络中必须唯一标识一个ATM终端，用于报文的第41域。为了更好的对代理业务ATM终端进行管理，特制订本编码规则用于规范该域的使用。

根据第41域的定义，终端标识码应为8位定长的字母、数字和特殊字符。

编码规则如下：

- 1-4 位：地区代码（参照《中华人民共和国国家标准 GB13497/92-全国清算中心代码》）；
- 5-8 位：顺序号，采用 4 位数字，从 0000～9999，同一地区内编号不得重复。

XXXX	XXXX
地区代码	自定义位

示例 1：上海本地的代理业务 ATM 终端编码范围，应为 29000000～29009999。

示例 2：江苏南京的代理业务 ATM 终端编码范围，应为 30100000～30109999。



## 附 录 E (资料性附录)

### 加钞交易成功后的打印凭条格式

为了方便现金托管机构的账务处理，需在ATM上加钞成功后提供凭条打印服务，打印内容是前一批次的交易对账信息和本批次的加钞信息。凭条格式如图E. 1所示：

#### XX现金托管机构 交易统计

日期 2004/01/08	时间 18:06:38	终端编号 12345678
系统跟踪号 123456	批次号 20040601131415	对账 平
统计类别	总笔数	总金额
借方交易	10	50000.00
贷方交易	0	0
贷记冲正交易	0	0
转账交易	0	0
代缴费/充值	0	0
余额查询	0	0
明细查询	0	0
修改密码	0	0

#### XX现金托管机构 加钞信息

日期 2004/01/08	时间 18:06:38	终端编号 12345678
50元张数 100	100元张数 200	加钞总金额 25000
系统跟踪号 123456	批次号 20040601131415	

**图 E. 1 现金托管机构加钞凭条**

交易统计凭条中内容，根据ATM终端的对账交易请求与响应的相关域值进行填写。总金额以“元”为单位，有两位小数。

加钞信息凭条中内容，根据ATM终端的加钞交易请求与响应的相关域值进行填写。总金额以“元”为单位。