ICS 35.240.40
A 11
备案号：

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0025.16—201x

中国金融集成电路（IC）卡规范
第16部分：IC卡互联网终端规范

China financial integrated circuit card specifications—
Part 16: IC card internet terminal specification

（送审稿）

201x-xx-xx 发布　　201x-xx-xx 实施

中国人民银行 发布

目　　次

前言 III
1 范围 4
2 规范性引用文件 4
3 术语和定义 4
4 符号和缩略语 7
5 终端硬件要求 8
5.1 终端安全要求 8
5.2 安全模块要求 8
5.3 硬件组成 8
5.4 电源 8
5.5 终端类型 8
6 一般终端要求 9
6.1 交易类型 9
6.2 支持卡片介质 9
6.3 下载管理 9
7 终端个人化 9
7.1 终端个人化数据 9
7.2 终端公私钥 9
7.3 终端个人化流程 9
7.4 证书申请和发放流程 10
8 安全体系 11
8.1 证书系统 11
8.2 安全通道 11
9 终端交易流程 13
9.1 开始交易 13
9.2 选择应用 13
9.3 应用初始化/读应用数据 13
9.4 脱机数据认证 13
9.5 处理限制 13
9.6 持卡人验证 13
9.7 终端风险管理 14
9.8 终端行为分析 14
9.9 卡片行为分析 14
9.10 联机处理 14
9.11 交易结束 14
9.12 发卡行脚本处理 14
10 终端接口协议 14
10.1 USB 接口协议 14

10.2 其他接口协议 14
附录 A （规范性附录） 终端命令集 15
A.1 终端命令集概述 15
A.2 管理命令 16
A.2.1 READ TERMINAL INFO 命令 16
A.2.2 MANAGE BUZZER 命令 18
A.2.3 MANAGE LED 命令 18
A.2.4 CONFIG DISPLAY FORMAT 命令 19
A.2.5 MULTIPLE INSTRUCTION 命令 20
A.3 安全通道命令 20
A.3.1 ADD CERTIFICATE 命令 20
A.3.2 UPDATE CERTIFICATE 命令 21
A.3.3 DELETE CERTIFICATE 命令 22
A.3.4 READ CERTIFICATE 命令 22
A.3.5 GET CERT RESPONSE 命令 23
A.3.6 GET CLIENT HELLO 命令 24
A.3.7 HASH SERVER CERTIFICATE 命令 24
A.3.8 VERIFY SERVER CERTIFICATE 命令 25
A.3.9 CLIENT SIGN 命令 26
A.3.10 EXPORT MASTERKEY 命令 26
A.3.11 HMAC 命令 27
A.3.12 TRANSMIT ENCRYPTED COMMAND 命令 27
A.3.13 CLOSE SECURE CHANNEL 命令 28
A.4 交易命令 29
A.4.1 CREDIT FOR LOAD 命令 29
A.4.2 DEBIT FOR PURCHASE 命令 31
A.4.3 GET ELECTRONIC CASH BALANCE 命令 33
A.4.4 GET PRIMARY BALANCE 命令 33
A.4.5 GET DOL VALUE 命令 35
A.4.6 GET REVERSAL INFO 命令 36
A.4.7 VERITY OFFLINE PIN 命令 37
A.5 终端命令响应状态码列表 38
附录 B（规范性附录） 报文鉴别码(MAC)计算方法 39
附录 C（资料性附录） 安全通道建立过程示例 41
附录 D（规范性附录） 终端支持双处理中心要求 42

前　言

JR/T 0025《中国金融集成电路（IC）卡规范》分为17部分：

——第1部分：电子钱包/电子存折应用卡片规范（废止）；

——第2部分：电子钱包/电子存折应用规范（废止）；

——第3部分：与应用无关的IC卡与终端接口规范；

——第4部分：借记/贷记应用规范；

——第5部分：借记/贷记应用卡片规范；

——第6部分：借记/贷记应用终端规范；

——第7部分：借记/贷记应用安全规范；

——第8部分：与应用无关的非接触式规范；

——第9部分：电子钱包扩展应用指南（废止）；

——第10部分：借记/贷记应用个人化指南；

——第11部分：非接触式IC卡通讯规范；

——第12部分：非接触式IC卡支付规范；

——第13部分：基于借记/贷记应用的小额支付规范；

——第14部分：非接触式IC卡小额支付扩展应用；

——第15部分：电子现金双币支付应用规范；

——第16部分：IC卡互联网终端规范；

——第17部分：借记/贷记应用安全增强规范。

本部分为JR/T 0025的第16部分。

本部分依据GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分主要起草单位：中国人民银行、中国工商银行、中国银行、中国建设银行、中国农业银行、交通银行、中国邮政储蓄银行、中国银联股份有限公司、银行卡检测中心、中钞信用卡产业发展有限公司、捷德(中国)信息科技有限公司、惠尔丰（中国）信息系统有限公司、福建联迪商用设备有限公司。

本部分主要起草人：

本部分为首次发布。

中国金融集成电路（IC）卡规范
第16部分：IC卡互联网终端规范

1 范围

本部分描述了IC卡互联网终端在硬件需求、接口协议、命令集、个人化以及安全体系方面的相关要求和规定。

本部分适用于受理符合JR/T 0025规范定义的金融IC卡的互联网终端设备。使用对象主要是与IC卡互联网终端应用相关的设计、制造、管理、受理以及应用系统的研制、开发、集成和维护等相关部门（单位）。

在本部分内所提到的终端若无特殊说明，均指IC卡互联网终端。

本部分描述了IC卡互联网终端在个人计算机上使用的规则，在其他应用环境（如智能手机、平板电脑等）的使用规则可参考本部分规定。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0001 银行卡销售点（POS）终端规范

JR/T 0025.3 中国金融集成电路（IC）卡规范 第3部分：与应用无关的IC卡与终端接口规范

JR/T 0025.6 中国金融集成电路（IC）卡规范 第6部分：借记/贷记应用终端规范

JR/T 0025.7 中国金融集成电路（IC）卡规范 第7部分：借记/贷记应用安全规范

JR/T 0025.8 中国金融集成电路（IC）卡规范 第8部分：与应用无关的非接触式规范

ISO/IEC 8859-1～ISO/IEC 8859-10 信息处理 八位单字节编码图形字符集

ISO/IEC 9797-1 信息技术 安全技术 报文鉴别码（MACs） 第1部分： 块密码机制

3 术语和定义

下列术语和定义适用于本文件。

3.1

应用 application

卡片和终端之间的应用协议和相关的数据集。

3.2

非对称加密技术 asymmetric cryptographic technique

采用两种相关变换的加密技术：公开变换（由公钥定义）和私有变换（由私钥定义）。这两种变换存在在获得公开变换的情况下是不能够通过计算得出私有变换的特性。

3.3

认证 authentication

确认一个实体所宣称的身份的措施。

3.4

证书 certificate

由发行证书的认证中心使用其私钥对实体的公钥、身份信息以及其它相关信息进行签名，形成的不可伪造的数据。

3.5

认证中心 certification authority

证明公钥和其它相关信息同其拥有者相关联的可信的第三方机构,本文中也简称为CA认证中心或CA中心。

3.6

认证中心根证书 certification authority root certificate

CA认证中心给自己颁发的未被签名的公钥证书或自签名的证书,是信任链的起始点。

3.7

命令 command

终端向IC卡发出的一条报文，该报文启动一个操作或请求一个响应。

3.8

密文 cryptogram

加密运算的结果。

3.9

加密算法 cryptographic algorithm

为了隐藏或显现数据信息内容的变换算法。

3.10

解密 decipherment

对应加密过程的逆操作。

3.11

数字签名 digital signature

对数据的一种非对称加密变换。该变换可以使数据接收方确认数据的来源和完整性，保护数据发送方发出和接收方收到的数据不被第三方篡改，也保护数据发送方发出的数据不被接收方篡改。

3.12

唯一甄别名 distinguished name

在数字证书的主体名称域中，用来唯一标识证书用户的名称，体现用户的唯一性。

3.13

加密 encipherment

基于某种加密算法对数据做可逆的变换从而生成密文的过程。

3.14

金融IC卡 financial integrated circuit(s) card

符合JR/T 0025要求，并由商业银行发行的集成电路（IC）卡。

3.15

握手协议 Handshake Protocol

用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

3.16

集成电路（IC） integrated circuit (IC)

具有处理和/或存储功能的电子器件。

3.17

集成电路卡（IC卡） integrated circuit(s) card (ICC)

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。

3.18

IC卡互联网终端 IC card internet terminal

通过互联网渠道、用于与IC卡配合共同完成IC卡交易的小型读卡设备，它应包括接口设备，也可包括其它的部件和接口（如与主机的通讯）。

3.19

接口设备 interface device

终端上插入IC卡的部分，包括其中的机械和电气部分。

3.20

管理命令 management command

终端用于执行获取终端参数信息、控制终端提示等操作的命令。

3.21

PIN 加密证书 PIN encryption certificate

由根CA中心签发的、用于加密联机PIN的数字证书。

3.22

私钥 private key

一个实体的非对称密钥对中含有的供实体自身使用的密钥。

3.23

处理中心 process centre

用于接收、处理或转发终端交易请求信息，并向终端回送交易结果信息的系统。

3.24

公钥 public key

在一个实体使用的非对称密钥对中可以公开的密钥。

3.25

公钥证书 public key certificate

由认证中心签名的不可伪造的某个实体的公钥信息。

3.26

圈存 load

增加卡中电子现金余额的过程。

3.27

记录协议 Record Protocol

建立在可靠的传输协议之上，为应用层协议提供数据封装、压缩、加密等基本功能的支持。

3.28

响应 response

IC卡处理完成收到的命令报文后，返回给终端的报文。

3.29

安全通道 secure channel

建立在IC卡互联网终端与处理中心之间的安全通信通道。

3.30

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。

3.31

安全通道命令 secure channel command

终端用于执行终端与处理中心之间建立安全通道和管理数字证书等操作的命令。

3.32

对称加密技术 symmetric cryptographic technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

3.33

终端证书 terminal certificate

用于标识终端设备身份的、符合X.509格式的唯一数字证书，每一个终端设备在预个人化时均会写入该证书。

3.34

交易命令 transaction command

终端用于执行借记/贷记应用流程的交易发起和联机处理等操作的命令。

3.35

渠道证书 trusted server certificate

用于标识处理中心系统服务器身份的、符合X.509格式的唯一数字证书，每一个处理中心服务器均配置唯一的渠道证书。

3.36

安全模块 trusted platform module

可信任平台模块，是一个可独立进行密钥生成、加解密的装置，内部拥有独立的处理器和存储单元，可存储密钥和特征数据，为设备提供加密和安全认证服务。用安全芯片进行加密，密钥被存储在硬件中，被窃的数据无法解密，从而保护商业隐私和数据安全。

4 符号和缩略语

下列符号和缩略语适用于JR/T 0025的本部分。

an	字母数字型（Alphanumeric）
APDU	应用协议数据单元（Application Protocol Data Unit）
CA	认证中心（Certificate Authority）
CBC	密码块链接（Cipher Block Chaining）
CLA	命令报文的类别字节（Class Byte of the Command Message）
CCID	芯片智能卡接口设备标准（USB Chip/Smart Card Interface Devices-USB）
DES	数据加密标准（Data Encryption Standard）
DN	唯一甄别名（Distinguished Name）
DOL	数据对象列表(Data Object List)
FIPS	联邦信息处理标准（Federal Information Processing Standard）
HMAC	密钥相关的哈希运算消息认证码（Keyed-Hash Message Authentication Code）
INS	命令报文的指令字节（Instruction Byte of Command Message）
LED	发光二极管（Light Emitting Diode）
MAC	报文鉴别码（Message Authentication Code）
n	数字型（Numeric）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
PAN	主账号（Primary Account Number）
PIN	个人识别码（Personal Identification Number）
RSA	Rivest、Sharmir 和 Adleman 提出的一种非对称密钥算法
SHA-1	安全哈希算法（Secure Hash Algorithm）
USB	通用串行总线标准(Universal Serial BUS)
X.509	国际电信联盟远程通信标准化组织定义数字证书标准

5 终端硬件要求

5.1 终端安全要求

IC卡互联网终端应使用安全模块保证个人标识代码（PIN）等敏感信息的安全输入和加密处理，支持与处理中心之间建立安全通道，对与外部交互的数据进行加、解密运算及合法性、完整性验证。终端应能够安全地存储密钥，禁止外部对密钥的直接访问，并通过有效的安全机制防止密钥被非法注入、替换和使用。应保证终端的固件和软件不被非法注入或更新。

持卡人在终端上键入密码时，应只显示星号，不显示明文。

终端的安全存储空间应至少能够满足本部分所涉及交易所需的证书、密钥的安全存储要求。

5.2 安全模块要求

终端应采用具有密钥生成和数字签名运算能力的安全模块，保证敏感操作在安全模块内进行，不得泄露敏感信息或影响安全功能。

安全模块应有独立的不可读区域，存放终端私钥、终端密钥等代表终端唯一性的重要信息。不应存在输出明文私钥、明文密钥或者明文PIN的机制，或者使用本身可能已经泄露的密钥来加密密钥或PIN。

参与密钥运算的随机数应由安全模块生成，其随机性指标应符合国际通用硬件产生随机数标准要求。

5.3 硬件组成

5.3.1 IC 卡读卡模块

终端应具备IC卡读卡模块，可与IC卡进行命令数据通讯，支持接触式和非接触式IC卡。该模块应包括机械、电气和逻辑协议等部分，应符合JR/T 0025.3和JR/T 0025.11的规定。

终端应具备指示如何插入接触式IC卡和感应非接触式IC卡的标记。

5.3.2 显示屏

终端应配置有显示屏,以供监测交易过程、输入数据、设置选项或确认交易数据。终端应支持ISO 8859的基本字符集。显示屏应同时具备中文、英文和数字显示能力。

5.3.3 键盘

终端应带有用于输入交易金额、个人识别码（PIN）、选择命令和执行功能的按键键盘。数字键、字母键、命令键、功能键及其布局，应符合JR/T 0025.6的规定，如果采用了带颜色的命令键，推荐使用下面的颜色分配。

命令键颜色：确认－绿色；取消－红色；清除－黄色。

IC卡互联网终端键盘至少应具有10个数字键,若干功能键,功能键应必须包括清除和确认两种功能，至少包括余额查询键或功能键加上、下键的组合键。键盘输出密码至显示屏，不能显示明文，只能显示无意义字符号。

5.3.4 与主机通信模块

通讯端口应至少支持USB通信方式。

5.4 电源

终端应至少支持USB方式供电。参照现有USB供电要求，电源电压应为DC 5V±5%，工作电流小于500mA。

5.5 终端类型

对各种终端类型的硬件要求见表1。

表1 终端硬件要求

项目号	终端类型 / 硬件模块	接触式IC卡互联网终端	非接触式IC卡互联网终端	双界面IC卡互联网终端
1	键盘	必备	必备	必备

2	显示屏	必备	必备	必备
3	接触式IC卡读卡模块	必备	无	必备
4	非接触式IC读卡模块	无	必备	必备
5	主机通信模块	必备	必备	必备
6	安全模块	必备	必备	必备

6 一般终端要求

6.1 交易类型

IC卡互联网终端至少应支持电子现金圈存、电子现金余额查询、主账户联机消费和主账户联机余额查询交易。

6.2 支持卡片介质

终端应支持金融IC卡，不支持磁条卡。

6.3 下载管理

终端应提供证书、参数等数据的安全下载、更新和删除功能。

7 终端个人化

7.1 终端个人化数据

终端个人化数据应至少包括终端数据、终端证书、CA根证书和PIN加密证书。

7.1.1 终端数据

终端数据由以下信息组成：所属机构编码、所属机构自定义数据、终端标识码。终端数据应当在终端出厂前预置，出厂后不允许更改。

表2 终端数据

说明	长度（字节）	类型
所属机构编码	8	n
所属机构自定义数据	7	n
终端标识码	8	ans

7.1.2 终端证书

终端证书应由终端所属机构向CA中心申请，并由CA中心签发。该证书是用于标识终端合法身份的唯一公钥证书。

7.1.3 CA 根证书

CA根证书应由CA中心签发并管理，需要从CA中心服务器下载，主要用于在交易过程中验证终端证书、渠道证书、PIN加密证书合法性。

7.1.4 PIN 加密证书

PIN加密证书应由处理中心向CA中心申请并下载，主要用于联机PIN的加密。如终端中存在不止一个PIN加密证书，则终端根据渠道证书中的DN域选择对应的PIN加密证书对联机PIN进行加密。具体方法见附录D。

7.2 终端公私钥

终端公私钥在终端下载终端证书过程中由终端生产的。终端产生的公钥提交CA参与制作证书，终端私钥应保存终端的安全模块中，不允许导出。

7.3 终端个人化流程

终端个人化是在终端出厂前将终端个人化数据预先写入终端的过程，其中CA根证书、终端证书、PIN加密证书需要从CA中心服务器下载。

具体步骤如下：

——向终端写入终端数据信息；

——向终端设备中安装终端证书；

——向终端设备中安装 CA 根证书；

——向终端设备中安装 PIN 加密证书。

7.4 证书申请和发放流程

IC卡互联网终端涉及的证书包括渠道证书、终端证书、CA根证书和PIN加密证书。

7.4.1 CA 根证书

CA 根证书用于验证渠道证书、终端证书和 PIN 加密证书的真伪，以辨别合法身份，需要在个人化过程中写入 IC 卡互联网终端和处理中心的安全设备中。CA 根证书的下载由 CA 中心与终端所属机构协商而定。

7.4.2 终端证书

终端在从CA中心申请、制证和下载证书前，需要通过CA中心对证书申请渠道进行安全审核，审核通过后才能进行证书的申请和发放流程。CA中心审核通过后，其申请和发放流程见图1。

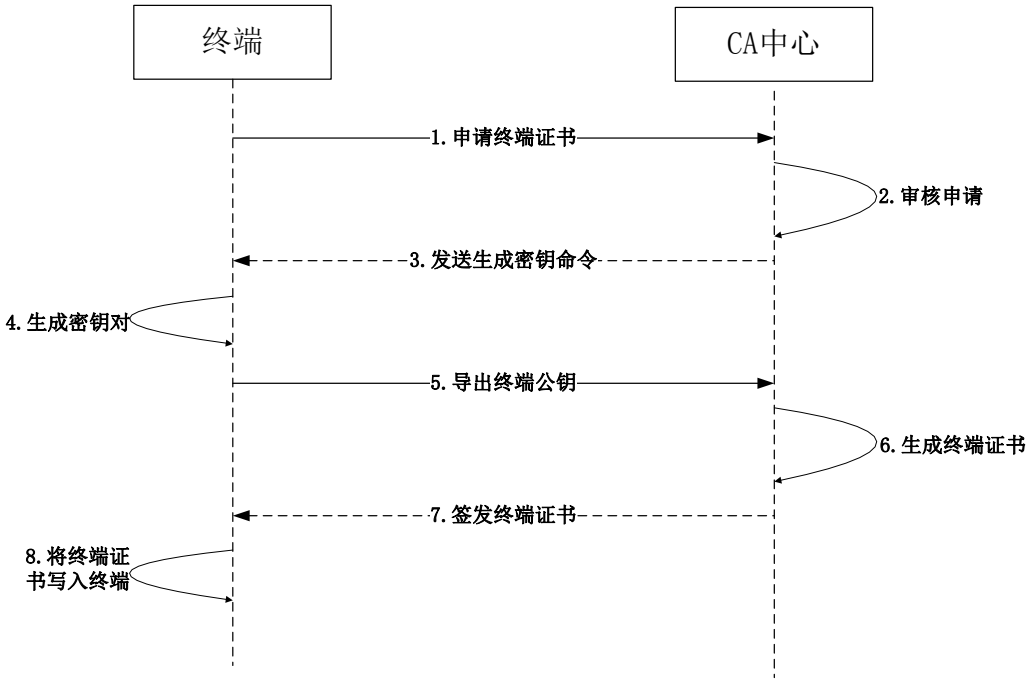


图1 终端证书发放流程

具体步骤如下：

1) 终端发送终端证书申请；
2) CA 中心审核终端证书申请；
3) CA 中心发送终端密钥对生成命令；
4) 终端生成密钥对；
5) 终端导出终端公钥；
6) CA 中心生成终端证书；
7) CA 中心签发终端证书；
8) 终端写入终端证书。

7.4.3 渠道证书

渠道证书可以用来验证处理中心服务器的真伪，防止服务器被假冒，并在与终端设备进行安全通讯时证明服务器的身份。渠道证书预置在处理中心的服务器中，其发放流程同终端证书。

7.4.4 PIN 加密证书

用于IC卡互联网终端在交易过程中保护金融交易PIN。IC卡互联网终端发放前需要预置PIN加密证书，其申请与发放流程同终端证书。

8 安全体系

8.1 证书系统

8.1.1 CA 系统结构

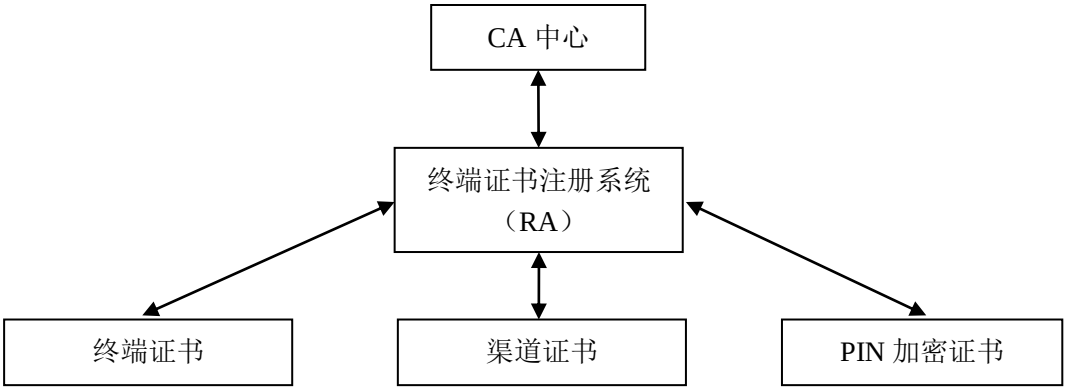


图2 终端 CA 系统结构

如图2所示，终端证书注册系统（RA）主要用于审核终端厂商和处理中心的证书申请，并在审核通过后，向终端和处理中心发放证书。

8.1.2 密钥算法

采用JR/T 0025.7中认可的对称、非对称及哈希算法。

8.2 安全通道

IC卡互联网终端通过与其连接的主机等联网设备接入到处理中心，并通过联网设备采用下节描述的握手工作原理与处理中心建立端到端的逻辑安全通道。其总体架构见图3。

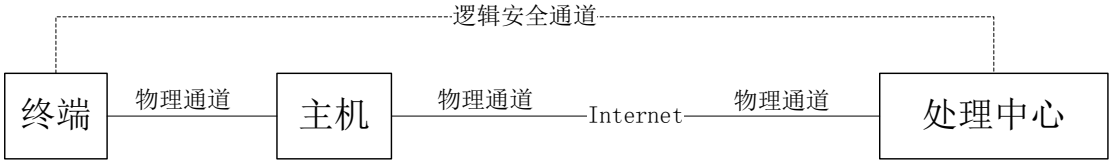


图3 安全通道示意图

安全通道的建立协议由握手协议和记录协议两部分组成。其中握手协议用于完成终端与处理中心的双向身份认证和会话密钥的交换过程。记录协议用于完成应用数据的加密传输。

安全通道的建立示例参见附录C。

8.2.1 握手协议工作原理

握手协议用于完成终端和处理中心之间的双向身份认证和会话密钥的交换过程。

握手协议基本流程

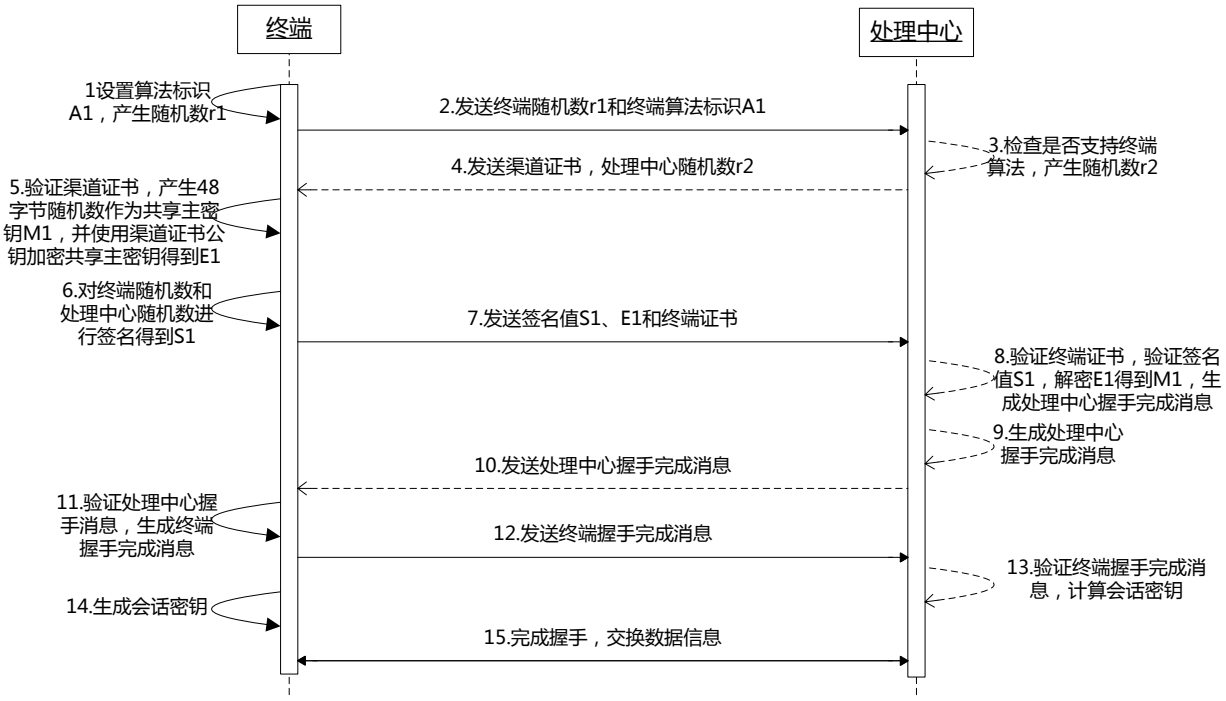


图4　握手协议消息序列图

握手协议工作步骤

1） 终端获取算法标识 A1,并产生随机数 r1，r1 和 A1 连接后得到 R1（R1=r1||A1），根据终端的算法支持设置在以下步骤中需要用到的对称算法和非对称算法；

2） 终端将随机数和算法信息发送到处理中心，启动握手协议；

3） 处理中心选择算法标识 A2，产生随机数 r2，r2 和 A2 连接后得到 R2。根据从终端发来的算法信息，检查处理中心是否支持，如果处理中心支持此算法，则设置处理中心对应的加解密算法；不支持则返回错误信息，断开连接；

4） 处理中心发送随机数和处理中心的渠道证书；

5） 终端使用终端中预制的 CA 根证书验证收到的处理中心的渠道证书，如果验证不通过，则发送出错消息，结束链接；否则，终端产生 48 字节随机数作为共享主密钥 M1，并且使用处理中心的渠道证书中的公钥采用之前设置的非对称算法对 M1 加密得到 E1；

6） R1 和 R2 连接后得到 R3，终端先对 R3 进行摘要算法得到 H1，然后使用终端私钥对 H1 进行签名运算得到 S1；

7） 终端将 S1、E1 和终端证书发送到处理中心；

8） 处理中心使用 CA 根证书验证终端证书合法性，若终端证书验证不通过，则发送错误消息，结束链接；如果终端证书验证通过，则使用终端证书验证 S1。若 S1 验证不通过，则发送错误消息，结束链接。否则，从 E1 中解密得到共享主密钥 M1；

9） 处理中心对渠道证书进行摘要运算得到 H2，对终端证书进行摘要运算得到 H3。将 R1、R2、H2、H3、S1、E1 连接后得到 T1（T1=R1||R2||H2||H3||S1||E1）；然后对 T1 进行摘要运算得到 H4；将 ASCII 码“SERVER”和 H4 连接后得到 D1；使用 M1 前 16 个字节对 D1 进行 HMAC 运算得到 F1（HMAC 计算方法见 B.2）；

10） 处理中心发送握手验证完成消息 F1 到终端；

11） 终端验证接收到的处理中心发来的 F1，若验证不成功，则发送错误消息，结束链接；否则，发送终端握手验证消息F2到处理中心;F2运算与F1运算方法一样,只需要将F1运算时的ASCII

码“SERVER”改为ASCII码“CLIENT”；

12）终端发送握手验证完成消息F2到处理中心；

13）处理中心使用同样的计算方法验证接收到的F2消息。验证失败，则发送错误消息，结束链接；

14）上述握手过程成功后，双方使用如下方法计算会话密钥：

X = HMAC(M1, key_label||r1||r2)　　（M1取其前16个字节）

其中key_label为3字节ASCII码“KEY”，HMAC算法见附录B.2。令X1X2…X20分别为X的第1个至第20字节，则加密密钥SKey为：SKey = X1X2…X16，MAC密钥MKey为：MKey = X5X6…X20；

15）握手过程结束。

8.2.2 记录协议工作原理

握手成功之后，双方可在建立的安全通道上进行数据传输。

记录协议的数据加密方法

在传输的数据Data前添加数据块长度Length(2字节)，构成数据块D = （Length||Data）。使用加密密钥SKey按照终端与处理中心约定的加密算法对D进行加密。即：

EData = E_{SKey} (D)；

记录协议的数据完整性保护方法

在记录协议的传输过程中，为双端每个发送和接收记录指定记录序列号，其初始值Seq0按以下方法生成：

取终端随机数的前8个字节Random1，取处理中心前8个字节Random2，则Seq0 = Random1 || Random2。

每发送或接收一帧记录信息后，记录序列号加1，即$Seq_i = Seq_{i-1} + 1$。注意双端要保持发送接收序列号的同步。

双方交互的应用数据的完整性使用消息认证码MAC进行保护，MAC按以下方法生成：

DataMAC = MAC(MKey, Seq_i || EData)　　（MKey取其前16个字节）

其中EData是所传输的加密应用数据，Seq_i是当前的记录序列号。MAC的计算方法见附录B.1。终端或处理中心接收到数据后，首先验证MAC的正确性，如果正确则进行处理；否则，发送错误消息，并结束当前链接。

9 终端交易流程

本章条描述IC卡互联网终端联机交易流程，是在互联网终端与处理中心进行相互认证建立安全通道后，所进行的交易处理流程。

9.1 开始交易

当终端与处理中心建立安全通道后，终端根据从处理中心接收到的交易命令进行分析处理，处理无误后开始借记/贷记交易处理流程。交易命令见附录A。

对于圈存交易终端应自动查询电子现金余额上限，并提示持卡人可圈存最大金额。

9.2 选择应用

符合JR/T 0025.6的规定。

9.3 应用初始化/读应用数据

符合JR/T 0025.6的规定。

9.4 脱机数据认证

IC卡互联网终端，仅支持联机交易，终端可不支持脱机数据认证。

9.5 处理限制

符合JR/T 0025.6的规定。

9.6 持卡人验证

IC卡互联网终端进行联机交易流程时，应强制进行联机PIN验证。终端应显示交易金额，并提示持卡人在终端上输入PIN。

9.7 终端风险管理

终端在终端风险管理中设置为本次交易为强制联机，其他处理应符合JR/T 0025.6的规定。

9.8 终端行为分析

符合JR/T 0025.6的规定。

9.9 卡片行为分析

符合JR/T 0025.6的规定。

9.10 联机处理

符合JR/T 0025.6的规定。

9.11 交易结束

除符合JR/T 0025.6的规定外，在交易结束时，终端应以声光电等方式提示持卡人交易结束。

9.12 发卡行脚本处理

对于发卡行联机成功的交易，如果在授权响应报文中包含了脚本，则终端将脚本解析成脚本命令，并发送给IC卡执行。

对于圈存交易，若IC卡执行脚本响应超时，则不发起冲正。

10 终端接口协议

10.1 USB 接口协议

终端采用USB接口，使用CCID协议。主机发送到终端的命令格式见表3。

表3 主机发送到终端的命令格式

信息域	标识	字节长度	含义
通信数据头	Type	1	CCID 指令
	Length	4	Abdata 的长度
	Slot	1	卡槽号
	Bseq	1	结果号
	bBwi	1	块等待时间
	Level Param	2	选择通讯方式
指令	Abdata		发送给终端的数据

金融 IC 卡读取随机数命令举例：

```
6F    05000000    00    F1    00    0000    0084000008
↓        ↓        ↓     ↓     ↓     ↓        ↓
Type  Length     Slot  Bseq  bBwi  Level   Abdata
```

10.2 其他接口协议

其他接口协议本部分规范不具体定义。

附 录 A
（规范性附录）
终端命令集

A.1 终端命令集概述

终端命令APDU格式和响应APDU格式符合JR/T 0025.3的规定。

终端命令集包括两部分：专用命令集和普通命令集。

——专用命令集：指在本部分中所有命令报文的命令类别（CLA）为 7E 或 7F 的类 APDU 命令。其中，7E 表示明文传输数据；7F 表示加密传输数据，密钥包括会话（数据加密）密钥和 MAC 密钥，密钥通过安全通道双方协商生产。终端专用命令根据功能划分为五类，分别为管理类命令、安全通道类命令、交易类命令、发卡行保留命令和本规范保留命令。终端专用命令定义具体见表A.1。

——普通命令集：指除本部分规定的终端专用命令以外的其它 APDU 命令。

注：

1）管理类命令：定义了获取终端参数信息、控制终端提示等管理类命令。

2）安全通道类命令：定义了终端与处理中心之间建立安全通道和管理数字证书等安全类命令。

3）交易类命令：定义部分借记/贷记应用流程的交易发起和联机处理等交易类命令。

4）发卡行保留命令：由发卡行定义使用。

5）本规范保留命令：由本规范保留使用。

表A.1 终端专用命令定义

CLA 命令类别	INS 指令代码	用途
7E/7F	10-1F	管理类命令
7E/7F	20-2F	安全通道类命令
7E/7F	40-4F	交易类命令
7E/7F	50-6F	发卡行保留
7E/7F	其他	本规范保留

本部分所涉及专用命令集数据类型未经特殊说明的，数据类型均按照JR/T 0025定义。本部分定义的终端专用命令见表A.2。

表A.2 终端专用命令集

编号	命令名称	CLA	INS	功能描述	必选（M）/可选(O)
管理类指令	READ TERMINAL INFO	7E	10	用于获取终端数据、交易 IC 卡卡号、固件版本号、设备状态等信息。	M
	MANAGE BUZZER	7E	11	用于控制蜂鸣器的状态。	O
	MANAGE LED	7E	12	用于控制 LED 的状态。	O
	CONFIG DISPLAY FORMAT	7E	13	用于控制显示屏上提示信息的显示格式。	O
	ADD CERTIFICATE	7E	20	用于向终端中安装证书。	M

通道类命令	UPDATE CERTIFICATE	7E	21	用于更新终端中已经存在的证书。	M
	DELETE CERTIFICATE	7E	22	用于回收（删除）终端中的证书。	M
	READ CERTIFICATE	7E	23	用于读取终端中的证书。	M
	GET CERT RESPONSE	7E	24	用于读取 READ CERTIFICATE 命令返回的响应数据。	M
	GET CLIENT HELLO	7E	25	用于获取建立安全通道所必须的终端算法标识及终端随机数。	M
	HASH SERVER CERTIFICATE	7E	26	用于对渠道证书信息进行哈希运算操作。	M
	VERIFY SERVER CERTIFICATE	7E	27	用于验证渠道证书的合法性。	M
	CLIENT SIGN	7E	28	用于使用终端私钥对输入数据进行签名操作。	M
	EXPORT MASTERKEY	7E	29	用于以密文方式导出共享主密钥。	M
	HMAC	7E	2A	用于生成终端 HMAC，验证处理中心 HMAC 以及分散过程密钥。	M
	TRANSMIT ENCRYPTED COMMAND	7F	2B	用于传输加密后的 APDU 命令。	M
	CLOSE SECURE CHANNEL	7E	2C	用于关闭安全通道。	M
交易类命令	CREDIT FOR LOAD	7E	40	用于实现金融 IC 卡圈存交易的联机处理。	M
	DEBIT FOR PURCHASE	7E	41	用于实现金融 IC 卡消费交易的联机处理。	M
	GET ELECTRONIC CASH BALANCE	7E	42	用于实现金融 IC 卡电子现金余额查询。	O
	GET PRIMARY BALANCE	7E	43	用于实现金融 IC 卡主账户余额联机查询。	M
	GET PBOC TAG VALUE	7E	45	用于按照输入的数据对象列表获取数据对象内容	M
	GET REVERSE INFO	7E	46	用于获取冲正信息或者脚本执行结果通知信息。	M

A.2 管理命令

A.2.1 READ TERMINAL INFO命令

A.2.1.1 定义和范围

READ TERMINAL INFO 命令用于获取终端生产厂商信息，包括固件版本号、终端状态等。

A.2.1.2 命令报文

READ TERMINAL INFO命令报文编码见表A.3。

表A.3 READ TERMINAL INFO 命令报文

代码	值
CLA	7E
INS	10
P1	00
P2	00：读取终端设备状态/01：读取终端设备信息

Lc	不存在
Data	不存在
Le	见说明

A.2.1.3 命令报文数据域

命令报文数据域不存在。

A.2.1.4 响应报文数据域

P2=0x00：

表示获取终端状态，返回1字节状态信息，Le=0x01。状态字节bit位定义见表A.4。

表A.4 终端状态字节定义

B7	B6	B5	B4	B3	B2	B1	B0	备注
							1	已设置终端数据
							0	未设置终端数据
						1		已安装 CA 根证书
						0		未安装 CA 根证书
					X			保留
				1				已安装 PIN 加密证书
				0				未安装 PIN 加密证书
			1					已安装终端证书
			0					未安装终端证书
	0	0						终端状态：上电
	1	0						终端状态：交易允许
	X	X						其他值保留
X								保留

P2=0x01：

表示获取终端数据、固件版本号和金融 IC 卡卡号等。

输出数据采用 TLV 格式，响应数据定义见表 A.5。

表A.5 READ TERMINAL INFO 读取终端信息响应报文数据域

说明	长度（字节）	备注
终端数据标签	1	标签值：01
终端数据长度	1	
终端数据	23	
终端固件版本号数据标签	1	标签值：02
终端固件版本号数据长度	1	
终端固件版本号	1-16	
公钥版本号数据标签	1	标签值：03
公钥版本号数据长度	1	
公钥版本号	2	00-99
IC 卡卡号数据标签	1	标签值：04
IC 卡卡号数据长度	1	
IC 卡卡号	14-19	
冲正标识位数据标签	1	标签值：05
冲正标识位数据长度	1	

冲正标识位	1	0x30：无冲正信息，0x31：有冲正信息
终端型号数据标签	1	标签值：06
终端型号数据长度	1	
终端型号	1-16	

A.2.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.2.2 MANAGE BUZZER命令

A.2.2.1 定义和范围

MANAGE BUZZER 命令用于控制蜂鸣器的状态，该命令为可选命令。

A.2.2.2 命令报文

MANAGE BUZZER 命令报文编码见表 A.6。

表A.6 MANAGE BUZZER 命令报文

代码	值
CLA	7E
INS	11
P1	00
P2	00
Lc	01
Data	蜂鸣器状态码
Le	不存在

A.2.2.3 命令报文数据域

命令报文数据域编码见表 A.7。

表A.7 MANAGE BUZZER 数据域编码

值	含义
00	关闭
01	蜂鸣一声
02	持续蜂鸣
03	持续间歇蜂鸣
其他	保留

A.2.2.4 响应报文数据域

响应报文数据域不存在。

A.2.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录 A.5。

A.2.3 MANAGE LED命令

A.2.3.1 定义和范围

MANAGE LED 命令用于设置 LED 的状态，通过对 LED 状态的设置，以简单、明确的方式通知持卡人交易状态。

A.2.3.2 命令报文

MANAGE LED命令报文编码见表A.8.

表A.8 MANAGE LED 命令报文

代码	值
CLA	7E
INS	12
P1	00
P2	00
Lc	01
Data	LED状态设置信息
Le	不存在

A.2.3.3 命令报文数据域

命令报文数据域编码见表A.9。

表A.9 MANAGE LED 数据域编码

值	含义
00	LED关闭
01	LED亮一次
02	LED长亮
03	LED闪烁
其他	保留

A.2.3.4 响应报文数据域

响应报文数据域不存在。

A.2.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录 A.5。

A.2.4 CONFIG DISPLAY FORMAT命令

A.2.4.1 定义和范围

CONFIG DISPLAY FORMAT 用于控制终端屏幕显示。本命令为可选命令。

A.2.4.2 命令报文

CONFIG DISPLAY FORMAT 命令报文编码见表 A.10.

表A.10 CONFIG DISPLAY FORMAT 命令报文

代码	值
CLA	7E
INS	13
P1	信息显示的行号
P2	信息显示的偏移位置
Lc	显示信息长度
Data	显示信息
Le	不存在

命令报文数据域

命令报文数据域表示在显示屏内显示的字符内容。

A.2.4.3 响应报文数据域

响应报文数据域不存在。

A.2.4.4 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录 A.5。

A.2.5 MULTIPLE INSTRUCTION命令

A.2.5.1 定义和范围

多指令处理命令，用于打包多条卡片执行指令，由终端解析每条逐一执行卡片指令，直到所有指令执行完成或指令执行错误，并将最后一条指令的执行结果或错误响应返回。

A.2.5.2 命令报文

MULTIPLE INSTRUCTION 命令报文编码见表 A.11。

表A.11 MULTIPLE INSTRUCTION 命令报文

代码	值
CLA	7E
INS	16
P1	00
P2	00
Lc	Data域字节长度
Data	多指令内容
Le	‘00’

A.2.5.3 命令报文数据域

命令报文数据域包含了多条终端规范的指令或者卡片指令，每条指令以‘,’（逗号 0x2C）为分隔符。指令执行过程中，若指令执行不成功，则终止执行后续指令并返回最后执行指令的指令序列号和响应码。

实例：7E160000 18 00A4040007A0000003330101 2C 0084000004 2C 0084000008

A.2.5.4 响应报文数据域

响应报文数据域为多指令中最后一条指令的响应数据,若执行失败则返回指令序列号和卡片错误响应码。

A.2.5.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录 A.5。

A.3 安全通道命令

A.3.1 ADD CERTIFICATE命令

A.3.1.1 定义和范围

ADD CERTIFICATE 命令用于为终端安装新证书。

A.3.1.2 命令报文

ADD CERTIFICATE 命令报文编码见表 A.12。

表A.12 ADD CERTIFICATE 命令报文

代码	值
CLA	7E
INS	20
P1	高4bit为证书类别，低4bit为偏移值
P2	偏移值（低8bit）
Lc	证书分包长度
Data	证书分包数据
Le	不存在

P1高4位信息定义增加证书的证书类别，具体定义见表A.13。

表A.13 证书类别标识定义

B7	B6	B5	B4	说明
0	0	0	1	一级CA根证书
0	0	1	0	二级CA根证书
0	1	0	0	PIN加密证书
1	0	0	0	保留

P1低4位与P2字节组成12bit偏移值，偏移范围从0~4095字节。

A.3.1.3 命令报文数据域

命令报文数据域的内容包括证书数据包。

受通信协议包大小限制，证书数据需要分包传输，即需要执行多次 ADD CERTIFICATE 命令。

A.3.1.4 响应报文数据域

响应报文数据域不存在。

A.3.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.3.2 UPDATE CERTIFICATE命令

A.3.2.1 定义和范围

UPDATE CERTIFICATE 命令用于更新终端内已有证书。

A.3.2.2 命令报文

UPDATE CERTIFICATE 命令报文编码见表 A.14。

表A.14 UPDATE CERTIFICATE 命令报文

代码	值
CLA	7E
INS	21
P1	高4bit为证书类别，低4bit为偏移值
P2	偏移值（低8bit）
Lc	证书分包长度
Data	证书分包数据
Le	不存在

P1高4bit信息定义增加证书的证书类别，具体定义见表A.15。

表A.15 证书类别标识定义

B7	B6	B5	B4	说明
0	0	0	1	一级CA根证书
0	0	1	0	二级CA根证书
0	1	0	0	PIN加密证书
1	0	0	0	保留

P1低4bit与P2字节组成12位偏移字节，偏移范围从0~4095字节。

A.3.2.3 命令报文数据域

命令报文数据域的内容包括新的证书数据。

受通信协议包大小限制，证书数据需要分包传输，需要执行多次 UPDATE CERTIFICATE 命令。

A.3.2.4 响应报文数据域

响应报文数据域不存在。

A.3.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录 A.5。

A.3.3 DELETE CERTIFICATE命令

A.3.3.1 定义和范围

DELETE CERTIFICATE 命令用于删除终端内已有公钥证书。

A.3.3.2 命令报文

DELETE CERTIFICATE 命令报文编码见表 A.16。

表A.16 DELETE CERTIFICATE 命令报文

代码	值
CLA	7E
INS	22
P1	证书类别标识（见表A.17说明）
P2	00
Lc	Data域数据长度
Data	终端信息
Le	不存在

P1高4bit信息定义增加证书的证书类别，具体定义见表A.17。

表A.17 证书类别标识定义

B7	B6	B5	B4	说明
0	0	0	1	一级CA根证书
0	0	1	0	二级CA根证书
0	1	0	0	PIN加密证书
1	0	0	0	保留

A.3.3.3 命令报文数据域

终端对处理中心下发的终端信息进行验证，如果验证结果一致，则终端执行删除指定的证书类别；否则，该命令执行失败。

表A.18 DELETE CERTIFICATE 命令数据域

数据	长度（字节）	备注
终端号	23	
固件版本号	1-16	

A.3.3.4 响应报文数据域

响应报文数据域不存在。

A.3.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.3.4 READ CERTIFICATE命令

A.3.4.1 定义和范围

READ CERTIFICATE 命令用于读取终端内已有证书。

A.3.4.2 命令报文

READ CERTIFICATE 命令报文编码见表 A.19。

表A.19 READ CERTIFICATE 命令报文

代码	值
CLA	7E
INS	23
P1	00：读取证书；01：读证书的hash值
P2	控制参数见说明
Lc	不存在
Data	不存在
Le	见说明

表A.20 控制参数取值说明

P2	所读取内容	备注
0x00	终端证书	
0x01	一级 CA 根证书	
0x02	二级 CA 根证书	
0x03	PIN 加密证书	

A.3.4.3 命令报文数据域

命令报文数据域不存在。

A.3.4.4 响应报文数据域

响应报文数据域不存在。

A.3.4.5 响应报文状态码

此命令执行成功的状态码是‘61FF’，表明需要调用 GET CERT RESPONSE 读取响应数据。

命令可能返回的错误信息见附录A.5。

A.3.5 GET CERT RESPONSE命令

A.3.5.1 定义和范围

GET CERT RESPONSE 命令用于读取 READ CERTIFICATE 命令返回的响应数据。

A.3.5.2 命令报文

GET CERT RESPONSE 命令报文编码见表 A.21。

表A.21 GET CERT RESPONSE 命令报文

代码	值
CLA	7E
INS	24
P1	00
P2	00
Lc	不存在
Data	不存在
Le	期望读取的证书数据包长度

A.3.5.3 命令报文数据域

命令报文数据域不存在。

A.3.5.4 响应报文数据域

按指定长度返回的证书数据。

A.3.5.5 响应报文状态码

此命令执行成功的状态码是‘9000’；当状态码是‘61XX’，表示后续还有XX个数据可以读出。

命令可能返回的错误信息见附录A.5。

A.3.6 GET CLIENT HELLO命令

A.3.6.1 定义和范围

GET CLIENT HELLO用于获取终端支持的算法标识和随机数。

A.3.6.2 命令报文

GET CLIENT HELLO命令报文编码见表A.22。

表A.22 GET CLIENT HELLO命令报文

代码	值
CLA	7E
INS	25
P1	00
P2	00
Lc	不存在
Data	不存在
Le	0x21

A.3.6.3 命令报文数据域

命令报文数据域不存在。

A.3.6.4 响应报文数据域

响应数据包含0x01个字节的算法标识和0x20个字节的随机数。算法描述见表A.23。

表A.23 算法描述符字节定义

B7	B6	B5	B4	B3	B2	B1	B0	算法
*	*	*	*	*	*	*	1	RSA
*	*	*	*	*	*	1	*	ECC
*	*	*	1	*	*	*	*	3DES
*	*	1	*	*	*	*	*	保留

A.3.6.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.3.7 HASH SERVER CERTIFICATE命令

A.3.7.1 定义和范围

HASH SERVER CERTIFICATE命令用于对渠道证书进行摘要操作,此摘要结果用于VERIFY CERTIFICATE命令进行解密结果的比对。

A.3.7.2 命令报文

HASH SERVER CERTIFICATE命令报文编码见表A.24。

表A.24 HASH SERVER CERTIFICATE命令报文

代码	值
CLA	7E
INS	26
P1	00
P2	00：SHA-1算法；其他：保留
Lc	输入数据长度
Data	输入数据

Le	不存在

A.3.7.3 命令报文数据域

命令数据的结构为：1 字节标志位+1 字节提取信息偏移值+渠道证书分包数据。

1 字节标志位定义见表 A.25。

表A.25 标志位字节各 bit 表示的含义

B7	分段证书信息起始包标志位
B6	分段证书信息终止包标志位
B5	本次数据需提取 OU 字段标志位
B4	本次数据需提取公钥字段标志位
B3	保留
B2	保留
B1	保留
B0	保留

1 字节提取信息偏移字节：若需在分包数据中提取 OU 字段或公钥字段，表示其在分包数据中的距离首字节的偏移长度，以便终端固件快速提取该信息。

A.3.7.4 响应报文数据域

响应报文数据不存在。

A.3.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.3.8 VERIFY SERVER CERTIFICATE命令

A.3.8.1 定义和范围

VERIFY SERVER CERTIFICATE 命令用于对渠道证书签名值进行解密，解密结果与 HASH SERVER CERTIFICATE 的摘要值在终端内部进行比对，比对一致则验证渠道证书通过。

A.3.8.2 命令报文

VERIFY SERVER CERTIFICATE 命令报文编码见表 A.26。

表A.26 VERIFY SERVER CERTIFICATE 命令报文

代码	值
CLA	7E
INS	27
P1	00
P2	00：RSA算法；其他：保留
Lc	输入数据长度
Data	输入数据
Le	不存在

A.3.8.3 命令报文数据域

输入命令数据的结构格式为：1 字节标志位字节+1 字节偏移值+签名值分包数据

1 字节标志位字节定义见表 A.27。

表A.27 标志位字节各 bit 表示的含义

B7	签名值起始包标志位
B6	签名值终止包标志位
B5	保留
B4	保留

B3	保留
B2	保留
B1	保留
B0	保留

由于传入的证书签名值为 TLV 编码格式，偏移值表示 Value 距分包首地址的偏移长度。

A.3.8.4 响应报文数据域

响应报文数据不存在。

A.3.8.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.3.9 CLIENT SIGN命令

A.3.9.1 定义和范围

CLIENT SIGN 命令使用终端私钥对指定数据进行签名，并且返回签名值。

A.3.9.2 命令报文

CLIENT SIGN 命令报文编码见表 A.28。

表A.28 CLIENT SIGN 命令报文

代码	值
CLA	7E
INS	28
P1	00
P2	00
Lc	输入数据长度
Data	输入数据
Le	00

A.3.9.3 命令报文数据域

签名源数据。此处源数据见本部分 8.3.1 条。

A.3.9.4 响应报文数据域

签名值。

A.3.9.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.3.10 EXPORT MASTERKEY命令

A.3.10.1 定义和范围

EXPORT MASTERKEY 命令用于获取终端产生的共享主密钥，并使用渠道证书的公钥进行加密。

A.3.10.2 命令报文

EXPORT MASTERKEY 命令报文编码见表 A.29。

表A.29 EXPORT MASTERKEY 命令报文

代码	值
CLA	7E
INS	29
P1	00
P2	00
Lc	不存在

Data	不存在
Le	00

A.3.10.3 命令报文数据域

命令报文数据不存在。

A.3.10.4 响应报文数据域

渠道证书公钥加密的共享主密钥密文信息。

A.3.10.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录 A.5。

A.3.11 HMAC命令

A.3.11.1 定义和范围

HMAC 命令用于：

1）取出协议过程中终端握手完成产生的 HMAC 值，发给处理中心进行验证。

2）输入协议过程中处理中心握手完成产生的 HMAC 值，发给终端进行验证。

3）终端通过 HMAC 算法内部产生会话密钥。

以上内容见本部分 8.2.1 和 8.2.2 条的定义。

A.3.11.2 命令报文

HMAC 命令报文编码见表 A.30。

表A.30 HMAC 命令报文

代码	值
CLA	7E
INS	2A
P1	00
P2	控制参数（见说明）
Lc	根据P2取值，见下面说明
Data	根据P2取值，见下面说明
Le	根据P2取值，见下面说明

表A.31 控制参数取值表

P2	Lc	Data	Le	备注
0x00	不存在	不存在	0x14	终端握手完成产生的 HMAC 值
0x01	0x14	处理中心 HMAC 值	0x00	终端验证处理中心握手完成产生的 HMAC 值
0x02	不存在	不存在	0x00	HMAC 算法内部产生会话密钥

A.3.11.3 命令报文数据域

见控制参数取值表说明。

A.3.11.4 响应报文数据域

P2=00 时，响应报文数据域为终端计算的 HMAC 值。终端计算 HMAC 的数据元见本部分 8.2.1 条。

P2=01 和 P2=02 时，无响应报文数据域。

A.3.11.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.3.12 TRANSMIT ENCRYPTED COMMAND命令

A.3.12.1 定义和范围

TRANSMIT ENCRYPTED COMMAND 命令用于处理中心与终端之间的加密传输。

A.3.12.2 命令报文

TRANSMIT ENCRYPTED COMMAND 命令报文编码见表 A.32。

表A.32 TRANSMIT ENCRYPTED COMMAND 命令报文

代码	值
CLA	7F
INS	2B
P1	00
P2	00:无级联方式；01：级联方式
Lc	输入数据长度
Data	输入数据
Le	00

P2 = 0x00 时，安全通道的消息报文以无级联方式传送，或消息报文已达到级联数据最后一帧。

P2 = 0x01 时，安全通道的消息报文以级联方式传送，后续还有数据。

A.3.12.3 命令报文数据域

处理中心下发的由 SKey 加密的命令数据和 MKey 计算的 MAC。

A.3.12.4 响应报文数据域

加密后的命令响应数据和 MAC。

A.3.12.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

备注：

（1）交易命令只能通过此加密命令传输给终端设备，即只有在安全通道建立之后，终端才能进行交易。

（2）通过此命令传输的终端命令，在解密后执行，执行结果和返回码需要加密返回给处理中心，而且返回码也同时以明文的形式紧接在返回密文后。

例：以下‘【】’（括号）表示 APDU 指令的 Data 域，该域包含了对括号内明文数据进行加密的数据密文和密文数据的 MAC 两部分，该域内容计算方法具体描述见本部分 8.2.2 条。

处理中心发送命令 ：7F 2B 00 00 10 【00 05 7E 2C 00 00 00】

终端返回 数据:【90 00】90 00 90 00

A.3.13 CLOSE SECURE CHANNEL命令

A.3.13.1 定义和范围

CLOSE SECURE CHANNEL 命令用于关闭安全通道，销毁安全通道协商的所有密钥。

A.3.13.2 命令报文

CLOSE SECURE CHANNEL 命令报文编码见表 A.33。

表A.33 CLOSE SECURE CHANNEL 命令报文

代码	值
CLA	7E
INS	2C
P1	00
P2	00
Lc	不存在
Data	不存在
Le	00

A.3.13.3 命令报文数据域

命令报文数据域不存在。

A.3.13.4 响应报文数据域

响应报文数据域不存在。

A.3.13.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.4 交易命令

A.4.1 CREDIT FOR LOAD命令

A.4.1.1 定义和范围

CREDIT FOR LOAD 命令用于支持金融 IC 卡的联机圈存交易，允许将金融 IC 卡主账户资金划入电子现金账户，并完成 IC 卡电子现金余额更新的操作。圈存金额在终端输入。交易过程中，终端应自动查询圈存上限，并提示持卡人可圈存最大金额。

A.4.1.2 命令报文

CREDIT FOR LOAD 令报文编码见表 A.34。

表A.34 CREDIT FOR LOAD 命令报文

代码	值
CLA	7E
INS	40
P1	00/01
P2	当P1=00，P2=00时：开始交易，读取表A.36中定义的数据； 当P1=00，P2=01时：读取表A.37定义的数据； 当P1=01，P2=00时：联机返回数据
Lc	Data域数据长度
Data	见命令报文数据域说明
Le	00

A.4.1.3 命令报文数据域

P1=00，P2=00 时：

开始圈存交易，命令报文数据域见表 A.35。

表A.35 开始圈存交易命令报文数据域

数据	长度（字节）	备注
交易金额	6	固定为 0
交易日期 YYMMDD	3	处理中心当前日期
交易时间 HHMMSS	3	处理中心当前时间
其他交易数据	可变（VAR）	见表下方注

注：其他交易数据为处理中心的数据，需要在异常（冲正、脚本通知）交易报文中回送前置处理系统。终端不需要对此数据解析。其他交易处理方法相同。

P1=00，P2=01 时：

命令报文中没有数据域。

P1=01 时：

联机返回数据，命令报文数据域见表 A.36。

表A.36 圈存联机数据命令报文数据域

数据	长度（字节）	备注

联机结果	1	00：正常联机；01：无法联机
发卡行授权数据（标签 91）	10-18	TLV 格式
授权响应码（标签 8A）	4	TLV 格式
71 脚本数据（标签 71）	可变	TLV 格式
72 脚本数据（标签 72）	可变	TLV 格式

A.4.1.4 响应报文数据域

P1=00，P2=00 时：

开始圈存交易，命令响应数据域见表 A.37。

表A.37 开始圈存交易响应报文数据域

数据	长度（字节）	备注
圈存金额	6	实际圈存金额
交易结果	1	01：交易拒绝；02：请求联机
终端验证结果 TVR（标签 95）	7	TLV 格式
交易日期（标签 9A）	5	TLV 格式
随机数（标签 9F37）	7	TLV 格式
应用交互特征（AIP）（标签 82）	4	TLV 格式
应用交易序号（ATC）（标签 9F36）	5	TLV 格式
密文信息类型（CID）（标签 9F27）	4	TLV 格式
应用密文（AC）（标签 9F26）	11	TLV 格式
发卡行应用数据（标签 9F10）	最大 35	TLV 格式
持卡人验证方法（CVM）结果（标签 9F34）	6	TLV 格式
交易序列计数器（标签 9F41）	5-7	TLV 格式
专用文件名称（标签 84）	7-18	TLV 格式
应用版本号（标签 9F09）	5	TLV 格式
授权金额（标签 9F02）	9	实际圈存金额

P1=00，P2=01 时：

读取 PAN、PAN 序列号等信息，命令响应数据域见表 A.38。

表A.38 响应报文数据域

数据	长度（字节）	备注
PAN（标签 5A）	最大 12	应用主账号，TLV 格式
PAN 序列号（标签 5F34）	4	应用主账号序列号，TLV 格式
二磁道等效数据（标签 57）	最大 21	磁条 2 等效数据，TLV 格式
联机 PIN 密文（标签 99）	130	使用 PIN 加密公钥加密的联机 PIN 密文

P1=01 时：

终端向处理中心返回联机数据，响应报文数据域见表 A.39。

表A.39 圈存联机响应报文数据域

数据	长度（字节）	备注
交易结果	1	00：交易批准；01：交易拒绝
脚本执行结果(标签 DF31)	8	TLV 格式
终端验证结果（TVR）(标签 95)	7	TLV 格式
应用交易序号（ATC）(标签 9F36)	5	TLV 格式

密文信息类型（CID）(标签 9F27)	4	TLV 格式
应用密文（AC）(标签 9F26)	11	TLV 格式
发卡行应用数据(标签 9F10)	最大 35	TLV 格式

A.4.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.4.2 DEBIT FOR PURCHASE命令

A.4.2.1 定义和范围

DEBIT FOR PURCHASE 命令用于支持金融 IC 卡的联机消费交易，允许持卡人使用金融 IC 卡完成互联网购物和获取相关服务。

A.4.2.2 命令报文

DEBIT FOR PURCHASE 命令报文编码见表 A.40。

表A.40 DEBIT FOR PURCHASE 命令报文

代码	值
CLA	7E
INS	41
P1	00/01
P2	当P1=00，P2=00时：开始交易，读取表A.42中定义的数据； 当P1=00，P2=01时：读取表A.43定义的数据； 当P1=01，P2=00时：联机返回数据
Lc	Data域数据长度
Data	见命令报文数据域说明
Le	00

A.4.2.3 命令报文数据域

P1=00，P2=00 时：

开始联机消费交易，命令报文数据域见表 A.41。

表A.41 命令报文数据域

数据	长度（字节）	备注
交易金额	6	消费金额
交易日期 YYMMDD	3	处理中心当前日期
交易时间 HHMMSS	3	处理中心当前时间
其他交易数据	可变（VAR）	见表下方注

注：其他交易数据为处理中心的数据，需要在异常（冲正、脚本通知）交易报文中回送处理中心。终端不需要对此数据解析。

P1=00，P2=01 时：

命令报文中没有数据域。

P1=01 时：

联机返回数据，命令报文数据域见表 A.42。

表A.42 命令报文数据域

数据	长度（字节）	备注
联机结果	1	00：正常联机；01：无法联机
发卡行授权数据（标签 91）	10-18	TLV 格式

授权响应码（标签 8A）	4	TLV 格式
71 脚本数据（标签 71）	可变	TLV 格式
72 脚本数据（标签 72）	可变	TLV 格式

A.4.2.4 响应报文数据域

P1=00，P2=00 时：

开始联机消费交易，命令响应数据域见表 A.43。

表A.43 响应报文数据域

数据	长度（字节）	备注
交易结果	1	01：交易拒绝；02：请求联机
终端验证结果 TVR（标签 95）	7	TLV 格式
交易日期（标签 9A）	5	TLV 格式
随机数（标签 9F37）	7	TLV 格式
应用交互特征（AIP）（标签 82）	4	TLV 格式
应用交易序号（ATC）（标签 9F36）	5	TLV 格式
密文信息类型（CID）（标签 9F27）	4	TLV 格式
应用密文（AC）（标签 9F26）	11	TLV 格式
发卡行应用数据（标签 9F10）	最大 35	TLV 格式
持卡人验证方法（CVM）结果（标签 9F34）	6	TLV 格式
交易序列计数器（标签 9F41）	5-7	TLV 格式
专用文件名称（标签 84）	7-18	TLV 格式
应用版本号（标签 9F09）	5	TLV 格式

P1=00，P2=01 时：

读取 PAN、PAN 序列号等信息，命令响应数据域见表 A.44。

表A.44 响应报文数据域

数据	长度（字节）	备注
PAN（标签 5A）	最大 12	应用主账号，TLV 格式
PAN 序列号（标签 5F34）	4	应用主账号序列号，TLV 格式
二磁道等效数据（标签 57）	最大 21	磁条 2 等效数据，TLV 格式
联机 PIN 密文（标签 99）	130	使用 PIN 加密公钥加密的联机 PIN 密文

P1=01 时：

终端向处理中心返回联机数据，响应报文数据域见表 A.45。

表A.45 响应报文数据域

数据	长度（字节）	备注
交易结果	1	00：交易批准；01：交易拒绝
脚本执行结果(标签 DF31)	8	TLV 格式
终端验证结果（TVR）(标签 95)	7	TLV 格式
应用交易序号（ATC）(标签 9F36)	5	TLV 格式
密文信息类型（CID）(标签 9F27)	4	TLV 格式
应用密文（AC）(标签 9F26)	11	TLV 格式
发卡行应用数据(标签 9F10)	最大 35	TLV 格式

A.4.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录 A.5。

A.4.3 GET ELECTRONIC CASH BALANCE命令

A.4.3.1 定义和范围

GET ELECTRONIC CASH BALANCE 命令用于通过终端查询 IC 卡电子现金余额，本交易脱机进行。

A.4.3.2 命令报文

GET ELECTRONIC CASH BALANCE 命令报文编码见表 A.46。

表A.46 GET ELECTRONIC CASH BALANCE 命令报文

代码	值
CLA	7E
INS	42
P1	00：显示电子现金余额
P2	00
Lc	不存在
Data	不存在
Le	00

A.4.3.3 命令报文数据域

命令报文数据域不存在。

A.4.3.4 响应报文数据域

金融IC卡电子现金余额，响应报文数据域见表A.47。

表A.47 GET ELECTRONIC CASH BALANCE 响应报文数据域

说明	长度（字节）	备注
电子现金余额	6	BCD码

A.4.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.4.4 GET PRIMARY BALANCE命令

A.4.4.1 定义和范围

GET PRIMARY BALANCE 命令用于联机查询借记/贷记应用主账户余额。

A.4.4.2 命令报文

GET PRIMARY BALANCE 命令报文编码见表 A.48。

表A.48 GET PRIMARY BALANCE 命令报文

代码	值
CLA	7E
INS	43
P1	00/01
P2	当P1=00，P2=00时：开始交易，读取表A.50中定义的数据； 当P1=00，P2=01时：读取表A.51定义的数据； 当P1=01，P2=00时：联机返回数据
Lc	Data域数据长度
Data	见命令报文数据域说明
Le	00

A.4.4.3 命令报文数据域

P1=00，P2=00 时：

开始借记/贷记主账户余额查询交易，命令报文数据域见表 A.49。

表A.49　命令报文数据域

数据	长度（字节）	备注
交易金额	6	金额固定为 0
交易日期 YYMMDD	3	处理中心当前日期
交易时间 HHMMSS	3	处理中心当前时间
其他交易数据	可变（VAR）	见表下方注

注：其他交易数据为处理中心的数据，需要在异常（冲正、脚本通知）交易报文中回送前置处理系统。终端不需要对此数据解析。

P1=00，P2=01 时：

命令报文中没有数据域。

P1=01 时：

联机返回数据，命令报文数据域见表 A.50。

表A.50　命令报文数据域

数据	长度（字节）	备注
联机结果	1	00：正常联机；01：无法联机
主账号金额	6	BCD
发卡行授权数据（标签 91）	10-18	TLV 格式
授权响应码（标签 8A）	4	TLV 格式
71 脚本数据（标签 71）	可变	TLV 格式
72 脚本数据（标签 72）	可变	TLV 格式

A.4.4.4　响应报文数据域

P1=00，P2=00 时：

开始借记/贷记主账户余额查询交易，命令响应数据域见表 A.51。

表A.51　响应报文数据域

数据	长度（字节）	备注
交易结果	1	01：交易拒绝；02：请求联机
终端验证结果 TVR（标签 95）	7	TLV 格式
交易日期（标签 9A）	5	TLV 格式
随机数（标签 9F37）	7	TLV 格式
应用交互特征（AIP）（标签 82）	4	TLV 格式
应用交易序号（ATC）（标签 9F36）	5	TLV 格式
密文信息类型（CID）（标签 9F27）	4	TLV 格式
应用密文（AC）（标签 9F26）	11	TLV 格式
发卡行应用数据（标签 9F10）	最大 35	TLV 格式
持卡人验证方法（CVM）结果（标签 9F34）	6	TLV 格式
交易序列计数器（标签 9F41）	5-7	TLV 格式
专用文件名称（标签 84）	7-18	TLV 格式
应用版本号（标签 9F09）	5	TLV 格式

P1=00，P2=01 时：

读取 PAN、PAN 序列号等信息，命令响应数据域见表 A.52。

表A.52　响应报文数据域

数据	长度（字节）	备注
PAN（标签 5A）	最大 12	应用主账号
PAN 序列号（标签 5F34）	4	应用主账号序列号
二磁道等效数据（标签 57）	最大 21	磁条 2 等效数据
联机 PIN 密文（标签 99）	130	使用 PIN 加密公钥加密的联机 PIN 密文

P1=01 时：

终端向处理中心返回联机数据，响应报文数据域见表 A.53。

表A.53　响应报文数据域

数据	长度（字节）	备注
交易结果	1	00：交易批准；01：交易拒绝
脚本执行结果(标签 DF31)	8	TLV 格式
终端验证结果（TVR）(标签 95)	7	TLV 格式
应用交易序号（ATC）(标签 9F36)	5	TLV 格式
密文信息类型（CID）(标签 9F27)	4	TLV 格式
应用密文（AC）(标签 9F26)	11	TLV 格式
发卡行应用数据(标签 9F10)	最大 35	TLV 格式

A.4.4.5　响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.4.5　GET DOL VALUE命令

A.4.5.1　定义和范围

GET DOL TAG VALUE 命令用于按照输入的数据对象列表获取数据对象内容。

A.4.5.2　命令报文

GET DOL VALUE 命令报文编码见表 A.54。

表A.54　GET DOL VALUE 命令报文

代码	值
CLA	7E
INS	45
P1	00
P2	00
Lc	Data域数据长度
Data	见命令报文数据域说明
Le	00

A.4.5.3　命令报文数据域

输入数据对象列表格式见表 A.55。

表A.55　GET DOL VALUE 命令报文数据域格式

标签 1	长度 1	标签 2	长度 2	……	标签 n	长度 n

注：长度表示需要获取的标签值的长度。

A.4.5.4　响应报文数据域

响应报文的数据域是BER-TLV编码的数据对象。这个数据对象需要按照下列格式编码：

表A.56 GET DOL VALUE 响应报文数据域格式

标签 1	长度 1	值 1	标签 2	长度 2	值 2	……	标签 3	长度 3	值 3

A.4.5.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.4.6 GET REVERSAL INFO命令

A.4.6.1 定义和范围

GET REVERSAL INFO 命令用于获取金融 IC 卡在联机交易异常时保存冲正信息或者脚本执行结果通知信息。

A.4.6.2 命令报文

GET REVERSAL INFO 令报文编码见表 A.57。

表A.57 GET REVERSAL INFO 命令报文

代码	值
CLA	7E
INS	46
P1	00：读取信息；01：清信息
P2	00：冲正信息；01：脚本通知
Lc	不存在
Data	不存在
Le	00

A.4.6.3 命令报文数据域

命令报文数据域不存在。

A.4.6.4 响应报文数据域

P1=00、P2=00 时：

读取交易冲正信息，命令响应数据域见表 A.58。

表A.58 读冲正信息命令响应数据域格式

数据	长度（字节）	备注
交易结果	1	00：交易批准；01：交易拒绝； 02：请求联机
交易金额	6	原交易金额
交易日期 YYMMDD	3	原交易日期
交易时间 HHMMSS	3	原交易时间
其他交易数据	可变（VAR）	交易时保存的数据
PAN（标签 5A）	最大 12	应用主账号，TLV 格式
PAN 序列号（标签 5F34）	4	应用主账号序列号，TLV 格式
二磁道等效数据（标签 57）	最大 21	磁条 2 等效数据，TLV 格式
脚本执行结果(标签 DF31)	8	TLV 格式
终端验证结果（TVR）(标签 95)	7	TLV 格式
应用交易序号（ATC）(标签 9F36)	5	TLV 格式
密文信息类型（CID）(标签 9F27)	4	TLV 格式
应用密文（AC）(标签 9F26)	11	TLV 格式
发卡行应用数据(标签 9F10)	最大 35	TLV 格式

P1=00、P2=01 时：

命令响应数据域不存在。

P1=01、P2=00 时：

读取脚本执行结果通知信息，命令响应数据域见表 A.59。

表A.59　读脚本执行结果通知命令响应数据域格式

数据	长度（字节）	备注
交易结果	1	00：交易批准；01：交易拒绝； 02：请求联机
交易金额	6	原交易金额
交易日期 YYMMDD	3	原交易日期
交易时间 HHMMSS	3	原交易时间
其他交易数据	可变（VAR）	交易时保存的数据
PAN（标签 5A）	最大 12	应用主账号，TLV 格式
PAN 序列号（标签 5F34）	4	应用主账号序列号，TLV 格式
二磁道等效数据（标签 57）	最大 21	磁条 2 等效数据，TLV 格式
脚本执行结果(标签 DF31)	8	TLV 格式
终端验证结果（TVR）(标签 95)	7	TLV 格式
应用交易序号（ATC）(标签 9F36)	5	TLV 格式
密文信息类型（CID）(标签 9F27)	4	TLV 格式
应用密文（AC）(标签 9F26)	11	TLV 格式
发卡行应用数据(标签 9F10)	最大 35	TLV 格式

P1=01、P2=01 时：

命令响应数据域不存在。

A.4.6.5　响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.4.7　VERITY OFFLINE PIN命令

A.4.7.1　定义和范围

VERITY OFFLINE PIN命令用于终端发起卡片验证脱机卡片PIN。验证命令引发IC卡将命令报文数据域内的交易PIN数据和与该应用相关的参考PIN数据进行比较验证。验证方式由IC卡中的应用自行决定。

A.4.7.2　命令报文

VERITY OFFLINE PIN 命令报文编码见表 A.60。

表A.60　VERITY OFFLINE PIN 命令报文

代码	值
CLA	7E
INS	4A
P1	00
P2	00
Lc	不存在
Data	不存在
Le	00

A.4.7.3　命令报文数据域

命令报文数据域不存在。

A.4.7.4　响应报文数据域

响应报文数据域不存在。

A.4.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

命令可能返回的错误信息见附录A.5。

A.5 终端命令响应状态码列表

表A.61 终端命令响应状态码列表

SW1	SW2	含义
‘90’	‘00’	正常处理
‘61’	‘XX’	正常处理，‘XX’表示可以通过后续命令得到的额外数据长度
‘6C’	‘XX’	长度错误（Le 不正确，’XX’表示实际长度）
‘65’	‘81’	终端设备错误
‘69’	‘82’	安全状态不满足
‘69’	‘85’	使用条件不满足
‘69’	‘86’	命令不允许
‘69’	‘88’	安全报文数据对象不正确
‘67’	‘00’	数据长度错误
‘6A’	‘80’	数据对象不存在
‘6A’	‘84’	终端存储空间不足
‘6A’	‘86’	P1、P2参数不正确
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00 ‘	CLA不支持或错误

附 录 B
（规范性附录）
报文鉴别码(MAC)计算方法

B.1 基于分组算法的MAC

MAC 算法依照 ISO/IEC 9797-1 规范，使用密钥长度为 128 位的对称加密算法采用 CBC 模式对任意长度的报文计算 8 字节 MAC 值。

表B.1 MAC 算法参数说明

M	明文消息
C	密文消息
M_{AC}	消息认证码
K	MAC 密钥
IV	初始向量
$E_K(M)$	使用密钥 K 对 M 进行加密
$D_K(C)$	使用密钥 K 对 C 进行解密

填充分组:

在明文 M 后附加 0x80，然后在右端填充最少的 0x00，使得填充后消息 M = (M||80||00||00||…||00)的长度为 8 的整数倍。将 M 分为 16 字节的块 $M_1, M_2,\ldots,M_n$。

计算 MAC

使用 3DES 算法,采用 CBC 模式使用密钥 K 的左半部分 8 字节 KL 加密分组 $M_1, M_2,\ldots,M_n$。其中初始向量 IV = (00 ‖ 00 ‖ 00 ‖ 00 ‖ 00 ‖ 00 ‖ 00 ‖ 00)。

CBC 模式加密过程如下:

$$C_0 = IV$$

$$C_i = E_{KL}(M_i \oplus C_{i-1}), \quad i = 1, 2, \ldots, n$$

使用最后一块数据计算消息认证码的方法为：

$M_{AC} = E_{KL}(D_{KR}(C_n))$

B.2 基于HASH算法的HMAC

HMAC 算法依照 FIPS 规范，使用摘要算法生成 HMAC。

表B.2 HMAC 算法参数说明

ipad	填充字节串，内容为：8 位字节 0x36 重复 64 次
opad	填充字节串，内容为：8 位字节 0x5c 重复 64 次
text	所输入的需要计算 MAC 的数据，不包括填充字节串
K	MAC 密钥
t	所得 MAC 的字节长度
Hash 安全哈希算法	使用密钥 K 对 M 进行加密
$D_K(C)$	见 FIPS 180-3

使用如下公式计算输入数据 text 的 MAC 值：

$$MAC(text)_t = HMAC(K, text)_t = Hash((K_0 \oplus opad) \| Hash((K_0 \oplus ipad) \| text))$$

具体描述如下：

1. 若 K = 64，令 K_0 = K。跳转到步骤 4；
2. 若 K > 64，令 K_0 = Hash (K)。跳转到步骤 4；
3. 若 K < 64，则在 K 末尾补字节 0x00 产生 64 字节 K_0；
4. K_0 与 ipad 异或产生 64 字节字符串：$K_0 \oplus$ ipad；
5. 将 text 追加到步骤 4 得到的字符串 $K_0 \oplus$ ipad 末尾：($K_0 \oplus$ ipad)||text；
6. 对步骤 5 得到的字符串进行哈希得到：Hash (($K_0 \oplus$ ipad)||text)；
7. K_0 与 opad 异或：$K_0 \oplus$ opad；
8. 将步骤 6 产生的结果追加到步骤 7 的结果末尾：

   (K_0 ⊕ opad) || Hash ((K_0 ⊕ ipad) || text)
9. 对步骤 8 的结果做哈希得到：

   Hash (($K_0 \oplus$ opad) || Hash ((K_0 ⊕ ipad) || text))。
10. 步骤 9 得到的哈希值作为 MAC 值。

附 录 C
（资料性附录）
安全通道建立过程示例

主机向终端发送GET CLIENT HELLO命令，终端返回1字节的算法标识和32字节随机数；

主机从1字节的算法标识中获得终端支持的对称和非对称算法列表，此标识将被发送到处理中心，处理中心会根据算法列表，检查算法列表中是否包含处理中心渠道证书所用的签名算法和对称算法；

随机数在此后的验证和生成认证信息时用到。

处理中心发送渠道证书、算法标识和32字节的随机数到终端。

此时终端应该先检查渠道证书的合法性，即HASH SERVER CERTIFICATE命令和VERIFY SERVER CERTIFICATE命令；

HASH SERVER CERTIFICATE命令用来对渠道证书主体进行哈希运算，并且将哈希运算结果保存在终端内部；

VERIFY SERVER CERTIFICATE命令则使用终端内的CA根证书对渠道证书的签名值进行解密，并且与HASH SERVER CERTIFICATE的哈希结果进行对比，从而检查渠道证书的合法性；

完成对渠道证书的合法性检测后，终端将产生48字节的随机数作为共享主密钥，并且使用渠道证书对此共享主密钥进行公钥加密，EXPORT MASTERKEY命令即完成渠道证书对共享主密钥的加密并且返回128字节的密文；

通过READ CERTIFICATE命令和GET CERT RESPONSE命令读出终端证书，因为考虑到证书大小比CCID单条命令最大传输字节数还要大，所以无法通过一条命令来读出终端证书，GET CERT RESPONSE命令可以多次调用，直到完全读出终端证书，命令详细解释见附录A.3；

处理中心认证终端时，需要通过校验终端私钥签名来完成。终端通过CLIENT SIGN命令对传入的处理中心随机数和终端本身随机数的连接值进行哈希和签名操作，返回128字节的签名数据；

终端将128字节共享主密钥的密文、终端证书和128字节的签名值发送到处理中心。

处理中心使用根证书检验终端证书的合法性，如果终端证书合法，则使用终端公钥验证签名值，从而确定终端的合法性；完成对终端的认证后，则使用渠道证书的私钥对共享主密钥的密文进行解密得到48字节的共享主密钥；此处需要发送一个处理中心认证完成的消息，为了防止此消息被伪造，此消息通过计算HMAC的方式来完成，其密钥为48字节共享主密钥的前16个字节，数据为ASCII“SERVER”、终端随机数、处理中心随机数、渠道证书哈希值、终端证书哈希值、终端发到处理中心的签名值、和共享主密钥的密文信息；

处理中心将握手完成消息，即处理中心计算出来的HMAC值发送到终端。

终端收到HMAC后，使用HMAC（P2=0x01）命令终端验证处理中心握手完成产生的HMAC值。然后，使用HMAC（P2=0x00）命令返回终端握手完成产生的HMAC值，此命令的计算HMAC值的过程与处理中心产生HMAC值的方法一样，只需要将ASCII“SERVER”改为“CLIENT”；

终端将握手完成消息，即终端计算出来的HMAC值发送到处理中心；

终端通过HMAC（P2=0x02）命令产生会话密钥，此会话密钥只保存在终端内，不能导出，并且断电需要重新生成。

处理中心验证终端握手完成消息后，产生会话密钥。

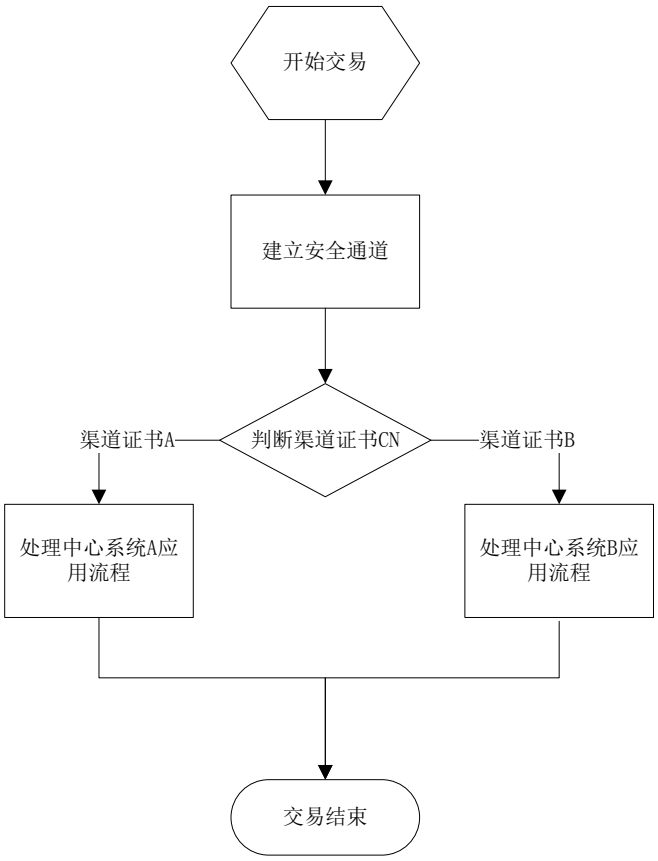
最终，终端和处理中心都共同拥有48字节的共享主密钥和20字节的会话密钥，其中20字节的会话密钥的前16个字节作为加密密钥，后面取16个字节作为计算MAC的密钥。

附 录 D
（规范性附录）
终端支持双处理中心要求

终端应具备可在2个不同处理中心系统进行交易的能力。终端根据处理中心的渠道证书的唯一甄别名（DN），辨别处理中心身份，区别不同的处理中心。

D.1 终端程序处理流程

当终端连接处理中心进行联机交易时，终端必须判断所连的处理中心身份，并执行相应处理中心的终端功能、终端交易应用（业务）流程和选用相应渠道的PIN加密证书加密PIN数据。



图D.1 终端程序处理流程

1) 持卡人开始联机交易；
2) 处理中心与终端建立安全通道；
3) 终端根据建立安全通道中获取的渠道证书 DN 域中的通用名内容，判断终端所连接的处理中心身份。若渠道证书为处理中心系统 A 的渠道证书，则进入处理中心 A 的终端应用（业务）流程；若渠道证书为处理中心系统 B 的渠道证书，则进入处理中心 B 的终端应用（业务）流程；
4) 根据步骤 3）判断执行处理中心终端应用（业务）流程（包括使用对应处理中心的 PIN 加密证书进行 PIN 加密、冲正机制、显示信息提示等）；
5) 交易流程执行完毕，交易结束。

D.2 终端个人化区别

支持双处理中心的终端的终端数据、证书体系与仅单处理中心终端相同，但终端个人化的证书数量有所不同。个人化证书数量区别详见表D.2。

表D.1　个人化证书数量

终端能力 证书类型	单处理中心终端	双处理中心的终端
终端证书	1	1
CA 根证书	1	1
PIN 加密证书	1	2
渠道证书	无须个人化	无须个人化

注：渠道证书在安全通道建立过程中，由处理中心发送给终端验证。