CJ

中华人民共和国城镇建设行业标准

CJ/T 166—2002

建设事业IC卡应用技术

Application technology for construction cause IC card

2002-06-03发布　　　　2002-10-01实施

中华人民共和国建设部　发布

目　　次

前　　言

随着我国社会、经济的发展和城镇建设规模的不断扩大，IC 卡技术及产品在城市建设事业中的应用越来越广泛。根据国办发[1997]22 号《国务院办公厅关于加强集成电路卡管理有关问题的通知》及建设部建计[1997]169 号《关于做好建设系统 IC 卡应用管理工作的通知》、建办[1998]131 号《关于开展建设事业 IC 卡应用试点工作的通知》、建办[1999]65 号《关于建设事业 IC 卡应用管理工作的通知》等文件精神和要求，为提高城市管理水平、促进应用行业社会效益、经济效益的增长，规范建设事业 IC 卡应用市场，贯彻落实国家对金卡工程提出的统一规划、统一标准、统一发卡、统一管理的原则，特制定本标准。

本标准的主要内容包括：

卡片技术要求：卡片的物理特性、逻辑接口、传输协议和命令集等内容。

终端技术要求：终端的物理特性、功能描述、数据安全要求、黑名单管理等内容。

应用技术要求：应用文件结构、交易流程和系统安全等内容。

密钥系统和安全认证技术要求：密钥机制和安全认证等内容。

本标准由建设部标准定额研究所提出并归口。

本标准由建设部 IC 卡应用管理领导小组办公室负责起草。

本标准参编单位：建设部 IC 卡应用服务中心、上海强生科技有限公司、上海华虹集团、北京握奇数据系统有限公司、中信技术公司、北京华民智能卡系统制造有限公司、北京公交华迅电子科技有限责任公司、北京同创恒远科技发展有限公司、北京捷德智能卡系统有限公司、航天金卡有限公司、天津环球磁卡有限公司、深圳华旭科技开发公司、深圳明华澳汉科技有限公司、丹东思凯电子发展有限责任公司、大连现代高技术发展有限公司、成都前锋电子仪器厂、南京同创交通信息技术有限公司、杭州先锋电子技术公司、中智建设技术工程有限责任公司、中外建设信息有限责任公司、重庆市智能水表有限责任公司。

本标准主要起草人：于成钢、孙一成、赵安民、(以下按姓氏笔划排列)丁敏、王毅、宋铁军、白雪晶、史健君、卢义明、孙敏、刘威、刘坚、何玉琼、严洪范、陈宇、陈志平、沈晓东、吴天文、吴健、张永华、邹驰、杨会平、杨明恕、金宽、金光辉、林立峰、欧勇强、徐明、谢晓光、曾维、魏庆华。

建设事业IC卡应用技术

1 范围

本标准规定了建设事业应用IC卡的卡片技术要求、终端技术要求、应用技术要求、密钥系统和安全认证技术要求和相应的定义、符号等。

本标准适用于由建设行业发行或接受的IC卡。其使用对象主要是与建设事业IC卡应用相关的卡片和终端设计、制造、管理、发行以及应用系统的研制、开发、集成和维护的部门(单位)。

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 2260—1999　中华人民共和国行政区划代码

GB/T 2828—1987　逐批检查计数抽样程序及抽样表(适用于连续批的检查)

GB/T 4754—1994　国民经济行业分类与代码

GB/T 7408—1994　数据元和交换格式　信息交换日期和时间表示方法

GB/T 14916—1994　识别卡　物理特性

GB/T 18239—2000　集成电路(IC)卡读写机通用规范

GB/T 18336.1—2001　信息技术　安全技术　信息技术安全性评估准则　第1部分:简介和一般模型

GB/T 18336.2—2001　信息技术　安全技术　信息技术安全性评估准则　第2部分:安全功能要求

GB/T 18336.3—2001　信息技术　安全技术　信息技术安全性评估准则　第3部分:安全保证要求

ISO/IEC 7811-1:1995　识别卡　记录技术　第1部分:凸印

ISO/IEC 7811-3:1995　识别卡　记录技术　第3部分:在ID-1卡上凸印字符定位

ISO/IEC 7812-1:2000　识别卡　发行者标识　第1部分:编号系统

ISO/IEC 7816-1:1998　信息技术　识别卡　带触点的集成电路卡　第1部分:物理特性

ISO/IEC 7816-2:1999　信息技术　识别卡　带触点的集成电路卡　第2部分:触点的尺寸和位置

ISO/IEC 7816-3:1997　信息技术　识别卡　带触点的集成电路卡　第3部分:电信号和传输协议

ISO/IEC 7816-4:1995　信息技术　识别卡　带触点的集成电路卡　第4部分:用于交换的行业间命令

ISO/IEC 7816-5:1994　识别卡　带触点的集成电路卡　第5部分:应用标识符的编号系统和登记规程

ISO/IEC 10373-1:1998　识别卡　测试方法　第1部分:通用性能测试

ISO/IEC 14443-1:2000　识别卡　无接触点集成电路卡　近程卡　第1部分:物理特性

ISO/IEC 14443-2:2001　识别卡　无触点集成电路卡　近程卡　第2部分:耦合区域的尺寸和位置

ISO/IEC 14443-3:2001 识别卡 无触点集成电路卡 近程卡 第3部分:电信号和复位规程
ISO/IEC 14443-4:2001 识别卡 无接触点集成电路卡 近程卡 第4部分:传输协议
《中国金融集成电路(IC)卡规范》

3 术语和定义

下列术语和定义适用于本标准

3.1

块 block

包含两个或三个域(头域、信息域、尾域)的字符组。

3.2

集成电路卡(IC卡) integrated circuit(s) card

内部封装一个或多个集成电路的ID-1型卡。

3.3

SAM模块 secure access module

一种能认证持卡人所持卡有效性的安全授权模块。

3.4

终端 terminal

为完成交易而在交易点安装的设备,用于同IC卡的连接。它包括接口设备,也可包括其他部件和接口,例如与主机通讯的接口。

3.5

命令 command

终端向IC卡发出的一条信息,该信息启动一个操作或一个应答。

3.6

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。

3.7

报文 message

由终端向卡或卡向终端发出的,不含传输控制字符的字节串。

3.8

密文 ciphertext

通过密码系统产生的不可理解的文字或信号。

3.9

密钥 key

控制加密转换操作的符号序列。

3.10

充值 charge

利用终端设备,在安全的条件下,根据一定的操作权限,增加IC卡中服务计量值的过程。

3.11

消费 pull

在指定应用的电子收费终端,对IC卡进行相应扣款写卡的过程。消费分专用消费和普通消费两种。

3.12

读写器 reader

可与IC卡进行数据交换的终端设备。

3.13

充值终端　charge terminal

可以增加IC卡中服务计量值的终端设备。

3.14

初始化　initialization

在卡发行前，由卡的发行机构对IC卡进行格式化，并在卡中写入卡的发行信息的过程。

3.15

应用文件　application file

按照一定的数据格式产生的具有不同功能的数据文件。IC卡的应用文件包括卡的文件标识、发行文件、钱包文件、月票钱包文件、交易记录文件和过程文件等。

3.16

电子钱包　electronic purse

一种为方便持卡人进行小额消费而设计的IC卡应用，它支持充值、消费等交易。

3.17

口令　passward

当一方能向另一方提交出预先约定的密码时，递交一方的合法性才得以承认。

3.18

非接触式IC卡　contactless IC card

使用时通过卡内的天线将卡内集成电路与外部接口设备进行连接的IC卡。

3.19

接触式IC卡　contact IC card

使用时通过有型的电极触点将卡内集成电路与外部接口设备进行连接的IC卡。

3.20

报文鉴别代码　message authentication code

对交易数据及其相关参数进行运算产生的代码。主要用于验证报文的完整性。

3.21

T=0

异步半双工字符传输协议。

3.22

T=1

异步半双工块传输协议。

3.23

黑名单　lawless list

由于结算、对帐不符、非法交易、非法卡交易等产生的非法列表清单。

3.24

CPU卡　central processing unit card

是一种具有微处理器芯片的IC卡。

3.25

逻辑加密卡　logic encrypt card

具有防止对卡中信息随意改写功能的存储IC卡。

3.26

消费类终端　purchase type terminal

该类终端包括车载机、IC卡计价器、通道闸机等机具。该类终端支持在公共汽车、出租汽车、地铁、

轻轨、轮渡、索道、公园、停车场等公共场所完成对 IC 卡的消费交易。

3.27

表具类终端　gauge type terminal

该类终端包括 IC 卡水表、IC 卡燃气表、IC 卡热力表等表具。该类表具支持对预付费的水、燃气和热力给予正常的供应。

3.28

服务类终端　service type terminal

该类终端包括充值机、自动售卡机、验卡机、自动圈存机等设备。该类终端支持在公共场所对公众完成售卡、充值、验卡、圈存等服务。

3.29

安全存取模块　secure access module

一种能够提供必要的安全机制以防止外界对终端所储存或处理的数据进行非法攻击的硬件加密模块。

3.30

控制位　access bit

逻辑加密卡中控制数据块读写权限的标志位。

4　缩略语和符号

ADF	应用数据文件(application definition file)
AEF	应用基本文件(application elementary file)
AID	应用标识符(application identifier)
APDU	应用协议数据单元(application protocol data unit)
BLOCK	块,非接触卡数据存贮单元
CLA	命令报文的类别字节(class byte of the command message)
CPU	中央处理器(central processing unit)
CSN	卡片唯一号(card single number)
DDF	目录数据文件(directory definition file)
DF	专用文件(dedicated file)
DIR	目录(directory)
EF	基本文件(elementary file)
FCI	文件控制信息(file control information)
IC	集成电路(integrated circuit)
IEC	国际电工委员会(international electrotechnical commission)
INS	命令报文的指令字节(instruction byte of command message)
IP	网络协议(internet protocol)
ISAM	充值安全存取模块(input secure access module)
ISO	国际标准化组织(international organization for standardization)
Lc	终端发出的命令数据的实际长度(exact length of data sent by the TAL in A case 3 or 4 command)
Le	响应数据的最大期望长度(maximum length of data expected by the TAL in response to a case 2 or 4 command)
Lr	响应数据域的长度(length of response data field)
MAC	报文鉴别代码(message authentication code)

MF	主控文件(master file)
P1	参数 1(parameter 1)
P2	参数 2(parameter 2)
PCD	接近耦合设备(proximity coupling device)
PICC	接近式卡 (proximity card)
PIN	个人密码(personal identification number)
PSAM	消费安全存取模块(purchase secure access module)
SAM	安全存取模块(secure access module)
SECTOR	扇区,非接触式 IC 卡数据存贮单位。本标准规定的卡的数据存贮单位分 16 个扇区,每个扇区分 4 个块
SFI	短文件标识符(short file identifier)
SW1	状态字 1(status word one)
SW2	状态字 2(status word two)
TAC	交易验证码(transaction authorization cryptogram)
VLAN	虚拟局域网(virtual local area network)

5 卡片技术要求

5.1 接触式 IC 卡

接触式 IC 卡的物理特性、逻辑接口与传输协议应符合 ISO/IEC 7816 系列标准。

5.1.1 接触式 IC 卡物理特性

接触式 IC 卡应符合 ISO/IEC 7816-1 中有关物理特性的要求(如紫外线、X-射线、触点的表面断面、机械强度、电磁特性、抗静电特性等)。

5.1.2 接触式 IC 卡触点的尺寸和位置

接触式 IC 卡的每个触点的尺寸、数量和位置、分配以及表面接触电阻等应符合 ISO/IEC 7816-2 的要求。

5.1.3 接触式 IC 卡的电信号和传输协议

接触式 IC 卡触点的电特性、操作过程、复位应答、协议类型选择、T=0 异步半双工字符传输协议、T=1 异步半双工块传输协议应符合 ISO/IEC 7816-3 的要求。

5.2 非接触式 IC 卡

本标准所定义的非接触式 IC 卡的物理特性、初始化、防冲突及传输协议应符合 ISO/IEC 14443 系列标准。

5.2.1 非接触式 IC 卡物理特性

非接触式 IC 卡物理特性应符合 ISO/IEC 14443-1 中有关物理特性的要求(如一般特性、尺寸、紫外线、X-射线、动态弯曲应力、动态扭曲应力、交变磁场、交变电场、静电、静电磁场、工作温度等)。

5.2.2 非接触式 IC 卡射频功率和信号接口

非接触式 IC 卡的射频功率和信号接口应符合 ISO/IEC 14443-2 中的要求(如功率传送、从 PCD 到 PICC 的通信、从 PICC 到 PCD 的通信等)。

5.2.3 非接触式 IC 卡的初始化和防冲突

非接触式 IC 卡的初始化和防冲突应符合 ISO/IEC 14443-3 中有关初始化、防冲突等要求。

5.2.4 非接触式 IC 卡的传输协议

非接触式 IC 卡应符合 ISO/IEC 14443-4 中有关激活协议和半双工块传输协议等要求。

5.3 CPU 卡的数据元和文件结构

CPU 卡中的每一个应用都包括一系列信息项,在终端成功地完成应用选择后可以对这些信息进行

访问(参见本标准应用选择部分)。

一个信息项称为一个数据元。数据元是信息的最小单位,它用名称、逻辑内容说明、格式及代码来标识。

5.3.1 **CPU 卡文件结构**

CPU 卡的文件结构应符合 ISO/IEC 7816-4 中的要求。

从终端角度来看,各应用与根目录呈一种可通过目录结构访问的树形结构。树的每一分支是一个应用数据文件(ADF)。一个 ADF 是一个或多个应用基本文件(AEF)的入口点。一个 ADF 及其相关数据文件处于树的同一分支上。

5.3.2 **应用数据文件(ADF)**

ADF 的树形结构(见图 1):

a) 能够将数据文件与应用联系起来;

b) 确保应用之间的独立性;

c) 可以通过应用选择实现对其逻辑结构的访问。

从终端角度来看,ADF 是一个只包含其文件控制信息(FCI)中纯数据对象的文件。

5.3.3 **应用基本文件(AEF)**

一个 AEF 包含一个或多个原始基本编码规则——标签、长度、值(BER-TLV)数据对象。但在选择了某一个应用后,其查询方式见 5.3.6。

5.3.4 **ISO/IEC 7816-4 文件结构中文件的映象**

ISO/IEC 7816-4 中使用下列映象表:

a) 包含一个 FCI 的专用文件(DF)(ISO/IEC 7816-4 中定义)被映象为 ADF,可以通过它来访问 EF 和 DF。在卡中处于最高层的 DF 称为主控文件(MF)。

b) 包含一组记录中的基本文件(EF)(ISO/IEC 7816-4 中定义)被映象为 AEF,EF 不能作为进入另一个不同 DF 文件的入口点。

在本标准中,DF 中相连的 EF 的访问是透明的。

5.3.5 **目录结构**

IC 卡支持用于 MF 下各应用列表的目录结构。目录结构必备的文件是目录文件(DIR 文件)和一些可选的由目录数据文件(DDF)引用的附加目录。

目录结构采用以其应用标识符(AID)的方式进入一个应用,或以 AID 的前 N 个字节作为 DDF 名的方式进入一组应用。

DIR 文件是一个 AEF(一个记录结构的 EF),它包含 ISO/IEC 7816-5 中定义的数据对象:

a) 本标准中描述的一个或多个应用模板(标签为'61');

b) 可能在目录自由模板中出现的其他数据对象(标签为'73'),这些模板中包含的数据对象不在本标准中定义。

在 IC 卡中的应用目录都是可选的,且不限制它们存在的数量。其中每个目录的位置由包括在每个 DDF 中的 FCI 的目录 SFI 数据对象指定。

5.3.6 **文件查询**

依照其类型,文件可以通过文件名或 SFI 进行查询。

a) 卡中的任何 ADF 或 DDF 可通过其 DF 名查询,ADF 的 DF 名对应其 AID,每个 DF 名在给定的卡中应是唯一的。

b) SFI 用于选择 AEF。对给定应用中的任何 AEF,可以通过 SFI(5 位代码,取值范围从 1～30)查询。SFI 的编码在每个用到它的命令中描述。在一个给定的应用中应是唯一的。专用 SFI 的使用由应用决定。

5.3.7 **卡片结构示例**

本标准给出了一个卡片的内部结构见图 1，该卡片支持电子钱包以及一个没有定义的发卡方应用。

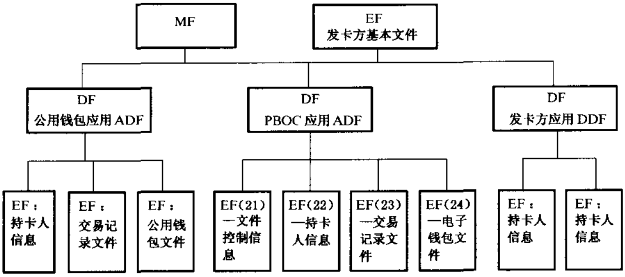

图 1　卡片内部结构

5.4 CPU 卡的命令

5.4.1 命令及其响应的 APDU 的内容及格式

命令的 APDU 的内容及格式见表 1，响应的 APDU 的内容及格式见表 2。

表 1　命令 APDU 的内容及格式

代码	描　　述	长度/byte
CLA	命令类别	1
INS	指令代码	1
P1	命令参数 1	1
P2	命令参数 2	1
Lc	命令数据域中存在的字节数	0 或 1
Data	命令发送的数据位串	=Lc
Le	响应数据域中期望的最大数据字节数	0 或 1

表 2　响应 APDU 的内容及格式

代码	描　　述	长度/byte
Data	响应中接受的数据位串	=Le
SW1	命令处理状态	1
SW2	命令处理限定	1

5.4.2 命令集

命令集见表 3。

表 3　命令集

编号	指令名称	CLA	INS	功能描述
1	APPEND RECORD	00/04	E2	增加记录
2	VERIFY	00/04	20	验证口令
3	EXTERNAL AUTHENTICATE	00	82	外部认证
4	GET CHALLENGE	00	84	取随机数
5	INTERNAL AUTHENTICATE	00	88	内部认证

表 3(续)

编号	指令名称	CLA	INS	功能描述
6	SELECT FILE	00	A4	选择文件
7	READ BINARY	00/04	B0	读二进制文件
8	READ RECORD	00/04	B2	读记录文件
9	GET RESPONSE	00	C0	取响应数据
10	UPDATE BINARY	00/04	D6/D0	写二进制文件
11	UPDATE RECORD	00/04	DC/D2	写记录文件
12	CARD BLOCK	84	16	卡片锁定
13	APPLICATION UNBLOCK	84	18	应用解锁
14	APPLICATION BLOCK	84	1E	应用锁定
15	PIN UNBLOCK	80/84	24	个人密码解锁
16	INITIALIZE	80	50	初始化交易
17	CREDIT FOR LOAD	80	52	圈存
18	DEBIT FOR PURCHASE/CASH WITHDRAW/UNLOAD	80	54	消费/取现/圈提
19	UPDATE OVERDRAW LIMIT	80	58	修改透支限额
20	GET TRANSCATION PROVE	80	5A	取交易认证
21	GET BALANCE	80	5C	读余额
22	RELOAD/CHANGE PIN	80	5E	重装/修改个人密码
23	PULL	80	30	专用消费
24	CHARGE	80	32	专用充值
25	INITIALIZE FOR CHARGE/PULL	80	50	专用充值/消费初始化
26	GET SPECIAL _ TRAN PROOF	80	5A	专用充值/消费取认证

说明:本表中第 1~11 条命令的解释参照 ISO/IEC 7816 系列标准;

本表中第 12~22 条命令的解释参照《中国金融集成电路(IC)卡规范》。

5.4.3 PULL 命令

5.4.3.1 范围 本命令用于专用消费。

5.4.3.2 命令报文 命令报文见表 4。

表 4 PULL 命令报文

代码	含义
CLA	'80'
INS	'30'
P1	'00'
P2	'00'
Lc	'0F'
Data	见表 5
Le	'08'

5.4.3.3 命令报文数据域　命令报文数据域见表 5。

表 5　命令报文数据域

说明	长度/byte
终端交易序号	4
交易日期	4
交易时间	3
MAC1	4

5.4.3.4 响应报文数据域　响应报文数据域见表 6。

表 6　响应报文数据域

说明	长度/byte
TAC	4
MAC2	4

5.4.3.5 响应报文状态　本命令执行成功的状态码是'9000'。

IC 卡可能回送的错误状态码见表 7。

表 7　PULL 命令错误状态

SW1	SW2	含义
65	81	内存失败
67	00	Lc 不正确
69	81	不是钱包文件
69	82	安全状态不满足
69	86	命令不允许
6A	80	数据域的参数不正确
6A	81	功能不支持
6A	86	参数 P1P2 不正确
93	02	MAC 错误
94	01	金额溢出或本次金额为 0

5.4.4 CHARGE 命令

5.4.4.1 范围　本命令用于向对应电子钱包中充值。

5.4.4.2 命令报文　命令报文见表 8。

表 8　CHARGE 命令报文

代码	含义
CLA	'80'
INS	'32'
P1	'00'
P2	'00'
Lc	0B

表 8(续)

代码	含义
Data	见表 9
Le	04

5.4.4.3 命令报文数据域 命令报文数据域见表 9。

表 9 命令报文数据域

说明	长度/byte
交易日期	4
交易时间	3
MAC2	4

5.4.4.4 响应报文数据域 响应报文数据域见表 10。

表 10 响应报文数据域

说明	长度/byte
TAC	4

5.4.4.5 响应报文状态 本命令执行成功的状态码是'9000'。

IC 卡可能回送的错误状态码见表 11。

表 11 CHARGE 命令错误状态

SW1	SW2	含义
65	81	内存失败
67	00	Lc 不正确
69	81	不是钱包文件
69	82	安全状态不满足
69	86	命令不允许
6A	80	数据域的参数不正确
6A	81	功能不支持
6A	86	参数 P1P2 不正确
93	02	MAC 错误
94	01	金额溢出或本次金额为 0

5.4.5 INITIALIZE FOR CHARGE/PULL 命令

5.4.5.1 范围 本命令用于电子钱包初始化充值/消费交易。

5.4.5.2 命令报文 命令报文见表 12 和表 13。

表 12 INITIALIZE FOR CHARGE 命令报文

代码	含义
CLA	'80'
INS	'50'
P1	'A1'=充值

表 12(续)

代码	含义
P2	'00'
Lc	'0B'
Data	见表 14
Le	'10'

表 13 INITIALIZE FOR PULL 命令报文

代码	含义
CLA	'80'
INS	'50'
P1	'A2'＝消费
P2	'00'
Lc	'0B'
Data	见表 14
Le	'0C'

5.4.5.3 命令报文数据域 命令报文数据域见表 14。

表 14 命令报文数据域

说明	长度/byte
密钥索引号	1
交易金额	4
终端机编号	6

5.4.5.4 响应报文数据域

P1＝A1 时,充值命令执行成功的响应报文数据域见表 15。

表 15 充值响应报文数据域

说明	长度/byte
余额	4
IC 卡充值交易序号	2
密钥版本	1
算法标识	1
伪随机数	4
MAC1	4

P1＝A2 时,消费命令执行成功的响应报文数据域见表 16。

表 16 消费响应报文数据域

说明	长度/byte
余额	4
IC 卡消费交易序号	2
密钥版本	1
算法标识	1
伪随机数	4

5.4.5.5 响应报文状态 本命令执行成功的状态码是'9000'。

IC 卡可能回送的错误状态码见表 17。

表 17 INITIALIZE FOR CHARGE/PULL 命令错误状态

SW1	SW2	含义
65	81	内存错误
67	00	Lc 不正确
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数不正确
94	03	密钥索引号不支持

5.4.6 GET SPECIAL _ TRAN PROOF 命令

5.4.6.1 范围

本命令提供了一种在充值/消费交易处理过程中拔出/离开并重新插入/进入感应区后卡片的恢复机制。

5.4.6.2 命令报文 命令报文见表 18。

表 18 GET SPECIAL _ TRAN PROOF 命令报文

代码	含义
CLA	'80'
INS	'5A'
P1	'A1'=充值,'A2'=消费
P2	'00'
Lc	'02'
Data	当前的充值/消费交易序号
Le	'08'

5.4.6.3 命令报文数据域 命令报文数据域为当前的充值/消费交易序号(加 1 前)。

5.4.6.4 响应报文数据域 4 字节 MAC2,4 字节 TAC。

5.4.6.5 响应报文状态 本命令执行成功的状态码是'9000'。

IC 卡可能回送的错误状态码见表 19。

表 19 GET SPECIAL _TRAN PROOF 命令错误状态

SW1	SW2	含义
65	81	内存错误
67	00	Lc 不正确
69	85	使用条件不满足
6A	81	功能不支持
94	06	所需 TAC/MAC2 不可用

6 终端技术要求

6.1 终端的基本性能要求

6.1.1 基本物理配置

对于任何类型的终端一般都应配置以下部件:显示器、读写部件、安全存取模块(SAM)、数据交换通道、电源、内存或其他存储设备。上述部件应符合国家或行业的相关产品标准。

6.1.2 终端交易时间要求

在脱机交易状态下:

——非接触 CPU 卡消费类终端的交易时间不大于 250 ms。

——非接触逻辑加密卡消费类终端的交易时间不大于 300 ms。

——接触式 CPU 卡消费类终端的交易时间不大于 850 ms(不包括发票打印时间)。

——接触式 CPU 卡表具类终端的交易时间不大于 1 050 ms(数据下载和上传的时间不计算在内)。

服务类终端的交易时间不作规定。

6.2 终端的一般要求

6.2.1 消费类终端和表具类终端的气候环境、机械环境、可靠性、安全性、电磁兼容性要求应符合产品的行业标准。没有行业标准的可以根据需要制定自己的产品标准,但关于产品的气候环境、机械环境、可靠性、安全性、电磁兼容性的要求至少应符合 GB/T 18239—2000 的相应条款。

6.2.2 终端的 IC 卡读写端口的物理特性、逻辑接口、通信协议

6.2.2.1 接触式终端的 IC 卡读写端口的物理特性应符合 ISO/IEC 7816-1 和 ISO/IEC 7816-2 的要求。

6.2.2.2 接触式终端的 IC 卡读写端口的逻辑接口、通讯协议应符合 ISO/IEC 7816-3 的要求。

6.2.2.3 非接触式终端的 IC 卡读写端口的逻辑接口和通信协议应符合 ISO/IEC 14443-3、ISO/IEC 14443-4 的要求。

6.3 终端的多应用要求

6.3.1 基本要求

多应用终端应给用户提供一个按优先级排序的列表以供选择。

6.3.2 终端多应用的管理

终端多应用的管理应达到以下目标:

a) 各个应用之间不能互相影响:各应用必须相互独立运行。

b) 共享数据必须保证:所有的应用可以共享终端中的通用数据,各应用的专用数据不能被其他应用得到。

6.4 终端的功能要求

本节从终端角度对充值、消费交易的一般功能、流程等方面提出了基本要求。终端的个性化功能设计、有关系统设计及后台处理等内容不属于本标准范围。

6.4.1 服务类终端

充值设备是服务类终端中安全技术要求最高的设备，本标准仅对充值设备提出要求。

6.4.1.1 充值设备一般要求

充值交易无论在充值设备联机或脱机进行交易时，充值设备应首先对IC卡的合法性予以验证，同时检查账户状况及其他交易数据。如果发卡方因某种原因不能接受交易，那么充值设备必须显示相应的告知信息。

6.4.1.2 安全要求

充值交易时，必须使用特定的充值安全存取模块(ISAM)。ISAM是由IC卡发行主管部门发行的可以用于对各种IC卡进行充值安全认证的卡(模块)，安装在各充值点的充值设备中。

充值设备在IC卡以及ISAM之间建立通信链路，充值设备的安全认证由IC卡和ISAM共同完成。充值设备只是在IC卡和ISAM之间传输安全信息，不参与进行密钥加密计算的过程。

充值设备在充值时与IC卡交易清算中心有联机方式、半脱机方式和脱机方式三种类型。该类设备在设计时应对交易清算中心授权的时间、次数和金额进行限制，防止该类设备在非法被使用时给系统造成重大损失(例如伪充值记录)。

充值设备在与交易清算中心的双向身份认证、密钥传送、授权、交易记录上传及黑名单下载等的通讯过程应采用密文加校验传送。

6.4.1.3 CPU卡充值设备的交易流程

本交易流程采用专用充值命令，CPU卡充值设备的充值交易流程见图2。

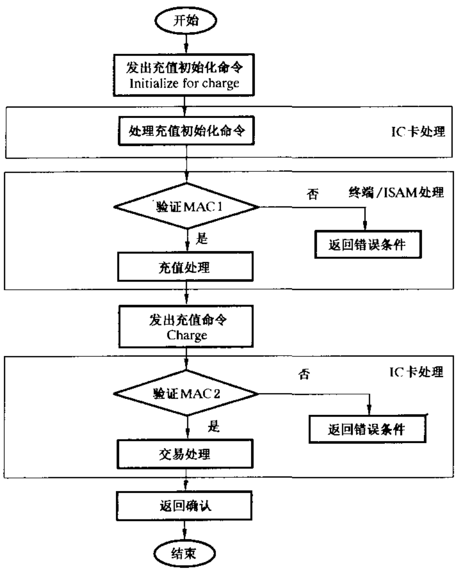

图2 CPU卡充值设备的交易流程

6.4.2 消费类/表具类终端

6.4.2.1 一般要求

消费类终端的消费交易允许持卡人使用电子钱包的余额获取服务。此交易在消费类终端中记录交易数据，由终端将交易记录数据上传到交易清算中心。

表具类终端允许持卡人使用计量文件中的预付值对终端充值以获取服务，并实现计量功能。此交易允许通过IC卡完成管理部门对终端的设置功能，同时通过IC卡将统计数据上传至管理部门。

6.4.2.2 **安全要求**

消费交易时，必须使用特定的消费安全存取模块(PSAM)。PSAM是由IC卡发行主管部门发行的可以用于对各种IC卡进行消费安全认证的卡(模块)，安装在各类消费机具/表具中。

消费机具/表具在IC卡以及PSAM之间建立通信链路，消费机具/表具的安全认证由IC卡和PSAM共同完成。

6.4.2.3 **交易流程**

消费类终端的消费交易分为单一票价消费、计程收费消费和月票消费等。单一票价消费和计程收费消费可以归纳为是在小钱包扣款，而月票消费也是在月票小钱包扣次。

表具类终端的消费交易一般为计量值的消费，计量值与金额的对应关系由管理部门规定。由表具的实际使用值去自动扣除表具的预付值，实现消费交易。

无论各种功能的消费类终端还是表具类终端在完成消费的基本交易流程都是在钱包内扣减数量，为了保证在一个大的系统内各类终端能在规定的技术规范下统一进行消费交易和非正常中断的数据恢复机制，本标准只规定消费有关的消费的基本交易流程。

6.4.2.3.1 **CPU卡消费机具/表具的基本交易流程**

本交易流程采用专用消费命令，适用于CPU卡消费类终端和表具类终端的基本消费交易流程见图3。

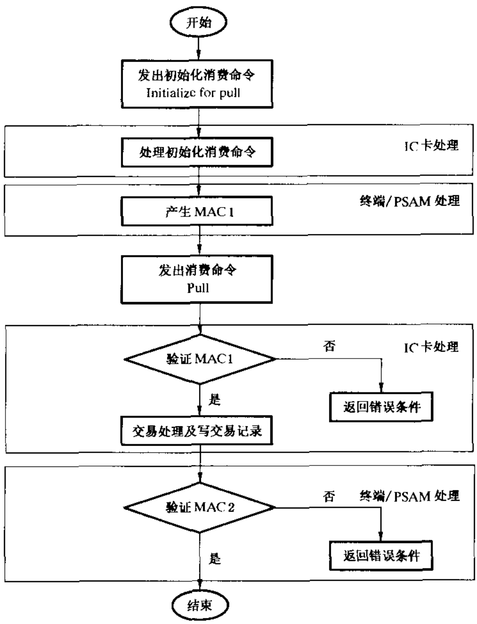

图3 CPU卡消费类/表具类终端基本交易流程

6.4.2.3.2 **非接触式逻辑加密卡消费类终端的基本交易流程**

非接触式逻辑加密卡消费类终端的基本交易流程见图 4。

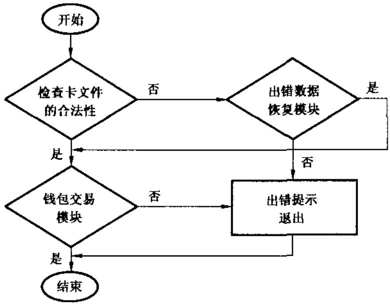

图 4 非接触式逻辑加密卡消费类终端的基本交易流程

非接触逻辑加密卡消费类终端的基本交易流程和非正常中断的数据恢复流程都由终端的程序来完成(细节见参考件)。

6.5 **终端的数据安全要求**

6.5.1 **一般要求**

各类终端一般存在两种类型的数据：

a) 通用数据:包括时间、终端识别号以及终端存储的交易记录等数据,外界可以对这些数据进行访问,但不允许进行无授权的修改;

b) 敏感数据:包括密钥、应用内部的参数(如 PSAM 标识号,密钥索引等),在未授权的情况下,外界不允许对这类数据进行访问和修改。

6.5.1.1 **通用数据安全要求**

通用数据一般存储在终端的存储器中。在更新参数和下装新的应用程序时,终端必须做到:

a) 只允许终端所有者或终端所有者授权的服务方验证身份并下载应用程序。

b) 校验下载数据的完整性。

对存储器要求必须做到:无论在什么情况下,终端中的数据都不会随意改变和丢失,并保证数据有效。

所有与交易相关的数据均以记录的形式存储在终端的存储器中,终端必须保证这些数据的完整性。

6.5.1.2 **敏感数据安全要求**

所有敏感数据都存储在安全存取模块中。对于安全模块的硬件形式在本标准中不作具体要求。

在正常的操作环境下,对安全存取模块必须要求:出入模块的、以及其内部存放和正在处理的数据不会由于模块自身或其接口造成任何泄露和改变。

安全存取模块的使用细节见参考件。

6.5.1.3 **交易上传数据**

终端需要上传的交易记录至少包括如下 40 字节数据,其格式见表 20。

6.5.2 **非正常中断数据恢复机制**

如果终端在处理 IC 卡交易时,卡被突然拔出、非接触 IC 卡离开感应区或由于终端方面的原因突然停止操作(如发生断电),终端应能监测到卡被拔出又重新插入、非接触卡重新进入感应区或检测到终端恢复供电后应对卡非正常交易的错误数据实施恢复处理。

在以上情况下,终端应进入这样一种状态:即持卡人应将原来的 IC 卡重新插入或进入感应区,并等

待最后一次交易完成。如果持卡人未插入IC卡或未进入感应区,则终端应提示持卡人重新插入或进入原来的IC卡。终端还应能够自动(插入超时)或以人工方式(如操作员按下取消键)退出这种待插卡状态。

在上述操作后,终端应执行以下操作之一:

a) 完成IC卡的最后一笔交易,向持卡人显示交易已完成(如果IC卡余额已被更新)

b) 取消最后一笔交易,向持卡人显示交易已被取消(如果IC卡余额没有被更新)

表 20 交易上传数据格式要求

序号	数据项(逻辑加密卡)	格式	长度/byte	数据项(CPU卡)	长度/byte	备注
1	唯一代码	HEX	4	卡号	16	
2	城市代码	BCD	2			
3	行业代码	BCD	2			
4	交易流水号	BCD	4			
5	卡认证码	HEX	4			
6	卡类	BCD	1	卡类	1	
7	钱包累计交易次数	HEX	2	消费交易计数器	2	
8	原额	HEX	4	原额	4	交易前余额
9	交易金额	HEX	3	交易金额	3	
10	交易日期	BCD	4	交易日期	4	YYYY/MM/DD
11	交易时间	BCD	3	交易时间	3	HH/MM/SS
12	交易类型	BCD	1	交易类型	1	
13	保留	HEX	2	充值交易计数器	2	保留时以FF填充
14	TAC	HEX	4	TAC	4	
合计			40		40	

6.6 黑名单管理

消费类终端和服务类终端应具有黑名单存储和检索功能,以实现IC卡脱机交易的安全处理。黑名单管理包括黑名单的收集、分发、存储、检索、更新等原则性的定义,黑名单的收集、黑名单的存储格式和内容的细节将不在本标准之内。

6.6.1 黑名单的记录类型

黑名单文件应该能够存储两种格式的黑名单记录:

a) 应用序列号;

b) 应用序列号的区间。

6.6.2 黑名单检查

黑名单检查操作在IC卡有效性检查过程中进行。卡片开始操作后,回送包括应用序列号在内的公共数据。终端根据序列号进行黑名单检查操作,检查该卡是否在终端存储的黑名单卡之列。

6.6.3 黑名单更新

黑名单文件更新包括增加、删除和重新下载等操作,需要在安全环境下进行。安全要求应包括:

a) 主机和终端间通信数据的安全性和完整性;

b) 终端对黑名单更新操作的安全认证;

c) 更新周期要满足应用要求。

6.6.4 黑名单库的容量要求

容量要满足应用的要求，最低不小于1000条。

7 应用技术要求

本节所涉及的技术要求是IC卡应用的基本要求，软件开发商和系统集成商在开发和实施建设事业IC卡应用系统项目时，应遵循本标准所规定的基本技术要求。

在具体实施过程中，终端交易流程是基本技术要求。对于卡片应用文件结构，根据目前国内的实际情况，本标准规定了用于消费类的非接触式逻辑加密卡的应用文件结构要求及用于表具类和消费类领域的接触式、非接触式CPU卡的应用文件结构要求。本标准从系统安全角度出发，规定了主机系统、网络系统、卡片介质和卡片终端的安全基本原则和要求。

7.1 交易流程

7.1.1 卡片发行流程

卡片发行是指对生产商提供的空白的IC卡进行初始化，创建文件结构，写入初始化数据和发行商信息的过程。卡片发行必须在具有安全保障和严格控制的专用场所统一进行。

卡片发行流程示意见图5。

7.1.2 消费类IC卡交易流程

非接触式逻辑加密卡单一票制消费交易流程见图6(典型的公交消费终端交易流程图)。

CPU卡消费交易流程见图7。

7.1.3 表具类IC卡交易流程

表具类CPU卡消费交易流程见图8。

7.2 卡片应用文件结构

7.2.1 非接触式逻辑加密卡应用文件结构

本节规定了非接触逻辑加密IC卡的文件数据结构。

卡片应用分区必须设置目录区、应用发行区、电子钱包区、交易记录区、公共信息区。也可根据需要设置其他应用分区。

7.2.1.1 应用文件结构

应用文件结构见表21。

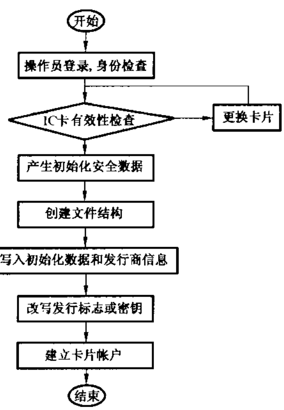

图5 卡片发行流程

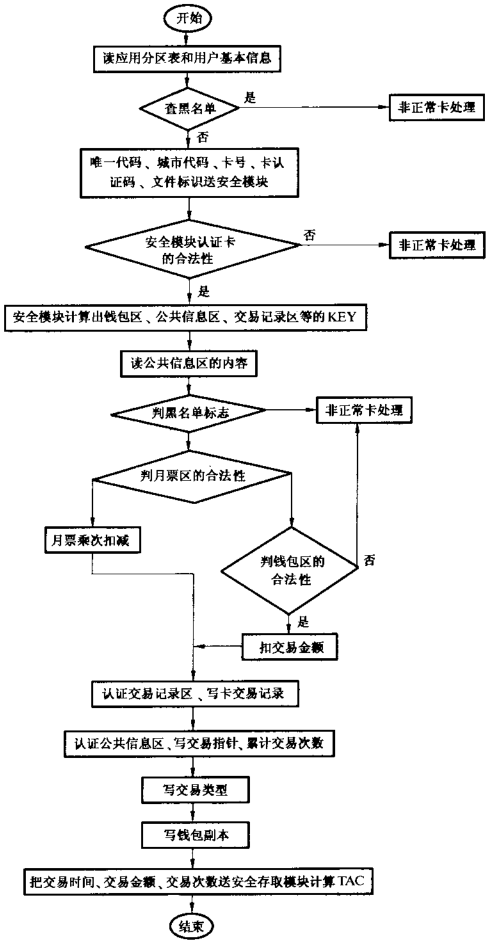

图6 非接触式逻辑加密卡消费交易流程

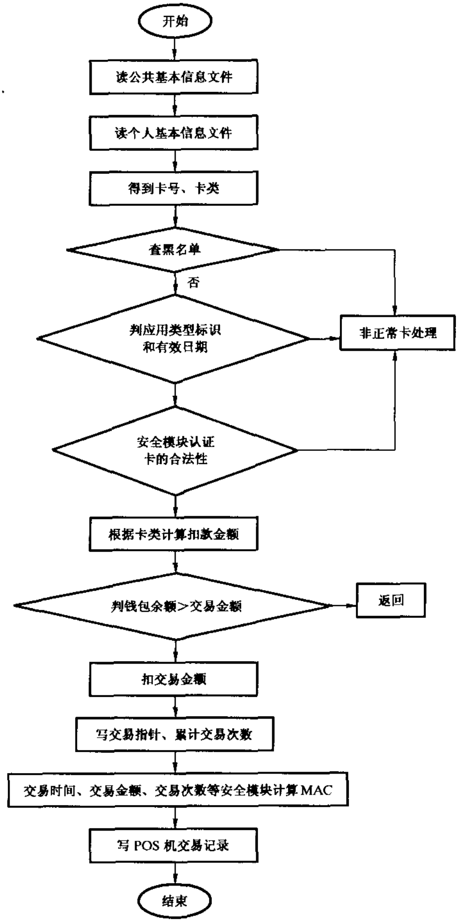

图7　消费类CPU卡消费交易流程

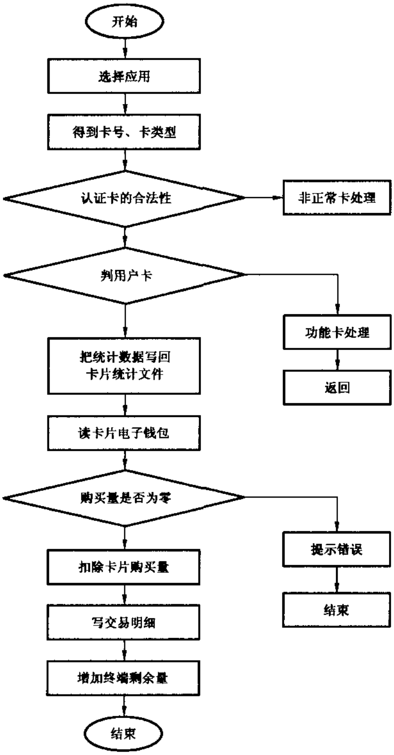

图 8　表具类 CPU 卡消费交易流程

表 21　应用文件结构

Sector	Block		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0 应用标识目录区	0	0	唯一代码(CSN)															
	1	1	00	01	10	03	03	03	06	FF	FF	FF	FF	FF	FF	FF	FF	FF
	2	2																
	3	3	KeyA0(读)						Access				KeyB0(写)					
1 发行区	0	4	城市代码		行业代码		发行流水号				卡认证码				启用标识	卡类	押金	校验
	1	5	发行日期				有效日期				启用日期				保留			校验
	2	6	充值时间年月日时					原额 1				本次加款值		操作员号				校验
	3	7	KeyA1(读)						Access Bit				KeyB1(写)					

表 21(续)

Sector	Block		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2 公共钱包区	0	8	累计加款值				余额				充值设备号				保留			校验
	1	9	钱包				钱包				钱包				校验			
	2	10	钱包备份				钱包备份				钱包备份				校验			
	3	11	KeyA2(读/减)						Access Bit				KeyB2(加/写)					
3 钱包交易记录区 A	0	12	交易时间 日/时/分/秒 交易记录 1				原额				交易金额			交易类型	终端号			
	1	13	交易记录 2				原额				交易金额			交易类型	终端号			
	2	14	交易记录 3				原额				交易金额			交易类型	终端号			
	3	15	KeyA3(读/写)						Access Bit				KeyB3(读/写)					
4 钱包交易记录区 B	0	16	交易时间 日/时/分/秒 交易记录 4				原额				交易金额			交易类型	终端号			
	1	17	交易记录 5				原额				交易金额			交易类型	终端号			
	2	18	交易记录 6				原额				交易金额			交易类型	终端号			
	3	19	KeyA4(读/写)						Access Bit				KeyB4(读/写)					
5 钱包交易记录区 C	0	20	交易时间 日/时/分/秒 交易记录 7				原额				交易金额			交易类型	终端号			
	1	21	交易记录 8				原额				交易金额			交易类型	终端号			
	2	22	交易记录 9				原额				交易金额			交易类型	终端号			
	3	23	KeyA5(读/写)						Access Bit				KeyB5(读/写)					
6 公共信息区	0	24	卡交易指针	钱包累计交易次数		交易进程标志	月票累计交易次数		黑名单标志	文件标识	FF	FF	FF	FF	FF	FF	FF	校验
	1	25	**卡交易指针**	**钱包累计交易次数**		**交易进程标志**	**月票累计交易次数**		**黑名单标志**	**文件标识**	FF	FF	FF	FF	FF	FF	FF	**校验**
	2	26	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
	3	27	KeyA6(读/写)						Access Bit				KeyB6(读/写)					
说明：图中阴影部分为原文取反。																		

7.2.1.2 分区说明

7.2.1.2.1 目录区

由于各个城市的应用各不相同，为了使终端能识别在 IC 卡上存在哪些应用，设立目录区，以便对应用的文件进行编码，见表 22。

表 22 分区编码

应用文件	文件标识(HEX)
目录区	00
发行区	01
交易记录区	03
公共信息区	06
公共钱包区	10
未使用扇区	FF

目录区建立在目录扇区的1块，其每个字节代表相应的文件所在的区。

例题：

应用标志目录区所有的内容代表：

目录区　　0扇区

发行区　　1扇区

公用钱包　　2扇区

交易记录区　　3、4、5扇区

公共信息区　　6扇区

目录区文件结构见表23。

表 23 目录区结构

<table>
<tr><td>Sector</td><td>Block</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td></tr>
<tr><td rowspan="4">0
应用标识目录区</td><td>0</td><td colspan="4">唯一代码(CSN)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>00</td><td>01</td><td>10</td><td>03</td><td>03</td><td>03</td><td>06</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td></tr>
<tr><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td colspan="6">KeyA0(读)</td><td colspan="4">Access Bit</td><td colspan="6">Key B0(写)</td></tr>
</table>

交易记录区的扇区要连续使用。

访问条件：

目录区固定在扇区0，目录区的Key A为“A0A1A2A3A4A5”。

认证目录区文件的KeyA可以对目录区实现读操作。

认证目录区文件的KeyB可以对目录区实现写操作。

目录区文件的KeyB由安全模块计算。

7.2.1.2.2 发行区文件

卡的发行信息包括卡的卡号、卡的发行日期、有效日期、启用日期、启用标志、卡类和卡押金。同时又包含卡的充值信息：充值时间(年/月/日/时)、原额、本次充值额、充值设备编号和操作员工号。

只有发行机构的初始化系统和充值系统具有读、写发行区的功能，其他系统只具有读的功能。发行区文件结构见表24。

表 24 发行区结构

<table>
<tr><td rowspan="4">1
发行区</td><td>0-4</td><td colspan="2">城市代码</td><td colspan="2">行业代码</td><td colspan="4">发行流水号</td><td colspan="4">卡认证码</td><td>启用标志</td><td>卡类</td><td>押金</td><td>校验</td></tr>
<tr><td>1-5</td><td colspan="4">发行日期</td><td colspan="4">有效日期</td><td colspan="4">启用日期</td><td colspan="3">保留</td><td>校验</td></tr>
<tr><td>2-6</td><td colspan="4">充值时间
年月日时</td><td colspan="4">原额1</td><td colspan="4">本次充值金额</td><td colspan="3">操作员号</td><td>校验</td></tr>
<tr><td>3-7</td><td colspan="6">Key A1(读)</td><td colspan="4">Access Bit</td><td colspan="6">Key B0(写)</td></tr>
</table>

a）卡号

卡号由城市代码、行业代码、发行流水号和卡的认证码构成。

卡的认证码由卡的唯一代码(CSN)、城市代码和发行流水号与内部的Key，经过加密运算得到，用以认证IC卡的合法性。

b）卡的类别

根据持卡人的不同，可分为普通卡、优惠卡等。

卡的类别的编码表见表25。

表25 卡类别的编码表

类别	代码
普通卡	00
其他	不规定

c）发行日期、有效日期和启用日期

卡的发行日期/有效日期和启用日期的年、月、日表示方法应符合GB/T 7408规定。

卡的发行数据定义见表26。

表26 卡的发行数据定义

	名称	长度	内容	数据格式
1	城市代号	2	邮政城市代码前4位	BCD
2	行业代码	2	按本标准规定	BCD
3	发行流水号	4	发卡机构在发行时生成的发行序号	BCD
4	卡认证码	4	用以认证用户卡的合法性	HEX
5	启用标志	1	卡的发行机构初始化后的标志位	HEX
6	卡类	1	卡类代码	HEX/BCD
7	押金	1	用户购卡时付的卡的价值的押金	HEX
8	校验	1	用于校验发行数据区数据的正确性	HEX
9	发行日期	4	年、月、日	BCD
10	有效日期	4	年、月、日	BCD
11	发行流水号	4	年、月、日	BCD

城市代码　　应用城市代码按邮政的城市代码的前4位确定。

行业代码　　按建设部的规定，记录行业代码。行业代码见表27。

发行流水号　　发卡机构在对卡进行初始化时给出的流水号。

卡的认证码　　由卡的唯一代码(CSN)、用户卡的城市代码和发行流水号与内部的Key，经过加密运算得到，用以认证用户卡的合法性。

表27 行业代码表

序号	行业	代码
1	城市通用	00
2	公交	01
3	出租汽车	02
4	地铁	03

表 27(续)

序号	行业	代码
5	轻轨	04
6	轮渡	05
7	园林	06
8	道路	07
9	旅游大巴	08
10	停车场	09
21	预付费表具	20
22	自来水	21
23	煤气	22
24	热能	23

d) 启用标志

表示卡初始化后的使用标志,其定义见表 28。

表 28 启用标志

编码	意义
01	未启用
02	启用
03	停用
04	黑名单卡

e) 充值记录

充值记录包括充值日期、充值前钱包原额、本次充值金额、充值后钱包余额、充值设备编号、操作员工号。

充值日期记录当前充值的日期,其年、月、日,表示方法应符合 GB/T 7408 规定。

原额记录本次充值前卡内钱包的剩余金额。

本次充值额记录当次充值数额。

余额记录本次充值后卡内钱包的金额。

充值设备编号记录完成当次充值的终端设备编号。

操作员工号记录完成当次充值的操作员工号。

充值记录的数据结构见表 29。

表 29 充值记录数据结构

名称	长度/byte	内容	数据格式
充值日期	4	年、月、日	BCD
原额 1	4	RMB 元、角、分	HEX
本次充值金额	2	RMB 元	BCD

表 29(续)

名称	长度/byte	内容	数据格式
累计加款值	4	RMB 元、角、分	HEX
余额	4	RMB 元、角、分	HEX
充值设备编号	4		BCD
操作员工号	2		BCD

f) 访问条件

发行区的 Key A＝前 6 字节(CSN＋CSN)。

认证发行区文件的 KeyA 可以对发行区实现读操作。

发行区文件的 KeyB 由安全模块计算。

认证发行区文件的 KeyB 可以对发行区实现写的操作。

7.2.1.2.3 钱包文件

钱包文件包括电子钱包、钱包备份、钱包校验码和累计充值额等信息。

a) 电子钱包

电子钱包文件占一个扇区，其扇区位置由发卡机构定义，数据文件标识符在卡的初始化时，由发卡机构写入扇区 0 的指定应用目录块内。

电子钱包应包括钱包、钱包备份和钱包校验码，并分别存贮在同一扇区的 1 块和 2 块内。卡在每次充值或交易时，备份数据应与钱包数据作比较，如两者数据不一致，应将正确数据拷贝到不正确的数据块。

b) 累计充值额

记录钱包的累计充值总值，每次充值操作时改写。

c) 钱包文件数据结构

钱包文件数据结构见表 30。

表 30　钱包文件数据结构

<table>
<tr><td rowspan="4">N
公共钱
包区</td><td>N-0</td><td colspan="2">累计加款值</td><td colspan="2">余额</td><td colspan="2">充值设备编号</td><td>保留</td><td>校验</td></tr>
<tr><td>N-1</td><td colspan="2">钱包</td><td colspan="2">钱包</td><td colspan="2">钱包</td><td colspan="2">校验</td></tr>
<tr><td>N-2</td><td colspan="2">钱包备份</td><td colspan="2">钱包备份</td><td colspan="2">钱包备份</td><td colspan="2">校验</td></tr>
<tr><td>N-3</td><td colspan="3">Key A2(读/减)</td><td colspan="2">Access Bit</td><td colspan="3">Key B2(加/写)</td></tr>
<tr><td colspan="10">说明：图中阴影部分为原文取反。</td></tr>
</table>

d) 访问条件

认证钱包文件的 KeyA 可以对钱包实现读和减的操作，钱包和钱包备份之间可以传输和恢复。

认证钱包文件的 KeyB 可以对钱包实现加和写的操作，钱包和钱包备份之间可以传输和恢复。

块 0 存放累计加款值，0 块与钱包之间不可以传输和恢复。

7.2.1.2.4 交易记录文件

交易记录文件占连续的三个扇区，每个扇区记录 3 条信息，交易记录的扇区位置由发卡中心定义，交易记录文件的标识符在卡的初始化时，由发卡中心写入扇区 0 的指定目录块内。

卡在每次交易后，应将交易信息存放在卡内。卡内存放交易记录 9 条，为定长循环结构。交易记录的内容包括：交易时间(日/时/分/秒)、原额、交易金额、交易类型、机具编号。

a) 交易记录的数据结构

交易记录的数据结构见表 31。

表 31 交易记录数据结构

N 钱包交易记录区 A	N—0	交易时间 日/时/分/秒	原额	交易金额	交易类型	终端号
	—1					
	—2					
	—3	Key A3(读/写)	Access Bit		Key B3(读/写)	
N+1 钱包交易记录区 B	(N+1) —0	交易时间 日/时/分/秒	原额	交易金额	交易类型	终端号
	—1					
	—2					
	—3	Key A3(读/写)	Access Bit		Key B3(读/写)	
N+2 钱包交易记录区 C	(N+2) —0	交易时间 日/时/分/秒	原额	交易金额	交易类型	终端号
	—1					
	—2					
	—3	Key A3(读/写)	Access Bit		Key B3(读/写)	

b）交易时间

交易时间记录当次交易的日、时、分、秒，表示方法应符合 GB/T 7408 规定。

c）原额

原额记录当次交易前的钱包金额。

d）交易金额

交易金额记录当次交易的金额。

e）交易类型

交易类型记录当次交易的交易类型。其表示方法见表 32。

表 32 交易类型编码

交易类型	编码
公交消费	01
出租汽车消费	02
地铁	03
轻轨	04
轮渡	05
园林	06
道路收费	07
旅游大巴	08
停车场	09
公交月票	10
公园月票	11
充值	88
提现	89
退卡	8A
圈存到公交月票	8B
锁卡交易	99

交易记录区数据定义见表 33。

表 33　交易记录区数据定义

	名称	长度	内　　容	数据格式
01	交易时间	4	记录当次交易的日、时、时、分、秒，表示方法应符合 GB/T 7408 规定	BCD
02	原额	4	记录当次交易前的钱包金额	HEX
03	交易金额	3	记录当次交易的扣款金额	BCD
04	交易类型	1	记录当次交易的交易类型	BCD
05	终端号	4	记录执行当次交易的终端编号	BCD

f）机具编号

记录执行当次交易的机具编号。

g）访问条件

认证交易记录文件的 KeyA 和 KeyB 都可以对交易记录文件实现读和写的操作。

7.2.1.2.5　公共信息区

公共信息是指地铁、公共电汽车、轮渡、出租汽车等建设事业的各种应用共用的交易记录信息区，公共交易信息包含交易记录指针、公共钱包累计交易次数、交易类型、黑名单标志等。占用 1 个扇区，0 块为公共信息区，1 块为公共信息区备份。

a）公共信息区的数据结构

公共信息区的数据结构见表 34。

表 34　公共信息区数据结构

<table>
<tr><td>N
公共信息区</td><td>N-0</td><td>交易记录指针</td><td colspan="2">钱包累计交易次数</td><td>交易过程标志</td><td colspan="2">月票累计交易次数</td><td>黑名单标志</td><td>文件标识</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>校验</td></tr>
<tr><td rowspan="3">公共信息区副本</td><td>N-1</td><td>交易记录指针</td><td colspan="2">钱包累计交易次数</td><td>交易过程标志</td><td colspan="2">月票累计交易次数</td><td>黑名单标志</td><td>文件标识</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>校验</td></tr>
<tr><td>-2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>-3</td><td colspan="6">Key A6(读/写)</td><td colspan="4">Access Bit</td><td colspan="6">Key B6(读/写)</td></tr>
<tr><td colspan="18">说明：图中阴影部分为原文取反。</td></tr>
</table>

b）交易记录指针

指向交易记录区的最后一条记录。合法数据为 1-9。

c）钱包累计交易次数

记录公共钱包的累计交易次数，包含与公共钱包有关的消费交易、充值交易等交易的累计次数。

d）交易过程标志

用于记录当次交易的过程。其定义见表 35。

表 35　交易过程标志编码表

编号	类型
01	单一票价开始
02	单一票价完成
03	计程收费开始
04	计程收费完成
05-	保留

e) 黑名单标志

用于在某次交易时发现该卡为黑名单卡时做的标记，交易时只要在公共信息区发现黑名单标志，不需要查黑名单即可判定该卡为黑名单卡。HEX 码，1 字节。其表示为：04 为黑名单卡，其他为正常卡。

f) 文件标识

文件标识是指当次交易对应的钱包文件的标识。

公共信息区的数据定义见表 36。

表 36　公共信息区数据定义

	名称	长度	内容	数据格式
01	交易记录指针	1	合法数据 01-09H	HEX
02	钱包累计交易次数	2	通用钱包消费与充值交易次数的累计次数	HEX
03	交易过程标志	1	标记交易的进程，用于出错数据恢复	BCD
04	月票累计交易次数	2	月票消费与充值交易次数的累计次数	HEX
05	黑名单标志	1	黑名单＝04H	HEX
06	文件标识	1	见 7.2.1.2.1 定义	HEX
07	保留	7	用 FF 填充	HEX
08	校验	1	用于校验公共信息区数据的正确性	HEX

g) 访问条件

认证公共信息区文件的 KeyA 和 KeyB 可以对公共信息区实现读和写的操作。

7.2.2　接触式、非接触式 CPU 卡应用文件结构

CPU 卡的应用文件结构见图 9。

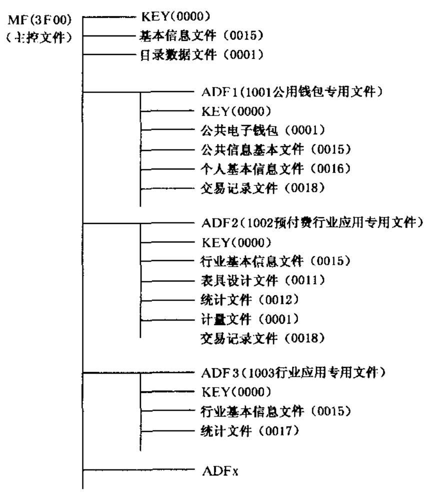

图 9　接触式、非接触式 CPU 卡应用文件结构

7.2.2.1　应用文件内容说明

7.2.2.1.1　用户卡文件详细信息

用户卡文件详细信息见表 37。

表 37 用户卡文件详细信息

文件名称	文件类型	文件标识符	读权	写权
MF 主控文件	目录文件	3F00	满足一定条件建立	
KEY	密钥文件	0000		
基本信息文件	二进制文件	0015	自由	需认证
目录数据文件	变长记录文件	0001	自由	需认证
ADF1 公用钱包专用文件	目录文件	1001	满足一定条件建立	
KEY	密钥文件	0000		
公用基本信息文件	二进制文件	0015	自由	需认证
个人基本信息文件	二进制文件	0016	自由	需认证
公共电子钱包	专用钱包文件	0001	自由	需认证
交易记录文件	循环文件	0018	自由	需认证
ADF2 预付费行业应用专用文件	目录文件	1002	满足一定条件建立	
KEY	密钥文件	0000		
行业基本信息文件	二进制文件	0015	自由	需认证
表具设置文件	二进制文件	0011	需认证	需认证
统计文件	二进制文件	0012	自由	需认证
计量文件	专用钱包文件	0001	自由	需认证
交易记录文件	循环文件	0018	自由	需认证
ADF3～ADF×	目录文件	1003～10××	满足一定条件建立	
KEY	密钥文件	0000		
行业基本信息文件	二进制文件	0015	自由	需认证
计量文件	二进制文件	0017	自由	需认证
说明：短文件标识符取为文件标识符的低字节的后 5 位(bit)				

7.2.2.1.2 **MF 主控文件内容**

a）KEY 文件内容见表 38。

表 38 KEY 文件内容

密钥文件
主控密钥
维护密钥
充值密钥组 1
……
充值密钥组 5

b）基本信息文件见表 39。

表 39 基本信息文件

文件标识(SFI)			15H
文件类型			二进制
文件大小			14H
文件存取控制		读=自由	写=需要安全信息
字节	数据元		长度/byte
1～6	发行点代码		6
7～14	发行点操作员代码		8
15～18	押金额		4
19～20	自定义		2

发行点操作员代码:操作员代码即操作员工号。

c) 目录数据文件

ADF1～ADFx: 目录名或短文件标识符。

7.2.2.1.3 **ADF1 公用钱包专用文件内容**

a) KEY 文件内容见表 40。

表 40 KEY 文件内容

密钥名称
应用主控
应用维护
消费子密钥组 1
……
消费子密钥组 5
充值子密钥组 1
……
充值子密钥组 5
TAC 子密钥

b) 公共基本信息文件见表 41。

表 41 公共基本信息文件

文件标识(SFI)			15H	
文件类型			二进制	
文件大小			1EH	
文件存取控制		读=自由	写=需要安全信息	
字节	数据元		长度/byte	格式
1～8	发卡方标识		8	BCD
9	启用标识		1	BCD
10	卡类型标识		1	BCD

表 41(续)

文件标识(SFI)		15H	
11～20	应用序列号	10	BCD
21～24	启用日期	4	BCD
25～28	有效日期	4	BCD
29～30	发卡方自定义文件控制信息数据	2	BCD
说明：应用序列号按下列顺序排列：国家标识(1 字节)+建设部标识(1 字节)+城市代码(2 字节)+行业代码(2 字节)+卡发行流水号(4 字节)。			

卡类型编码如见表 42。

表 42　卡类型编码

卡型	代码
普通卡	00
其他	自定义

启用标识的定义见表 29。

启动日期是指用户的购卡日期，年、月、日表示方法应符合 GB/T 7408 规定。

有效日期是卡的有效期限，4 字节，表示方法同上。

c) 个人基本信息文件见表 43。

表 43　个人基本信息文件

文件标识(SFI)		16H
文件类型		二进制
文件大小		27H
文件存取控制	读＝自由	写＝需要安全信息
字节	数据元	长度/byte
1	应用版本	1
2	本单位职工标识	1
3～22	持卡人姓名	20
23～38	持卡人证件号码	16
39	持卡人证件类型	1

d) 公用电子钱包文件见表 44。

表 44　公用电子钱包文件

字段名	长度/byte
余额	4
消费交易序号(次数)	2
充值交易序号(次数)	2

e) 交易记录文件见表 45。

交易记录文件中的记录数不少于 10 条。

表 45 交易记录文件

文件标识(SFI)		18H
文件类型		循环记录
文件大小		18H
文件存取控制	读=自由	写=需要安全信息
字节	数据元	长度/byte
1～6	终端机编号	6 备注:行业代码(2)+序号(4)
7～13	交易日期时间	7
14～17	交易金额	4
18	交易类型	1 备注:02=消费
19～22	现有余额	4
23～24	交易序号	2

7.2.2.1.3 **ADF2～ADF×行业应用专用文件内容**

a) KEY 文件内容见表 46。

表 46 KEY 文件

密钥名称
应用主控
应用维护
消费子密钥组 1
……
消费子密钥组 5
TAC 子密钥

各行业的专用钱包,对某些行业可以是计量文件。例如:月票计次、燃气和水的计量资料。

b) ADF2 预付费类行业应用专用文件内容

——行业的基本数据文件见表 47。

表 47 行业的基本数据文件

文件标识(SFI)		15H	
文件类型		二进制	
文件大小		1EH	
文件存取控制	读=自由	写=需要安全信息	
字节	数据元	长度/byte	格式
1	卡类型	1	BCD
2～9	卡号	8	BCD
10	保留	1	BCD
11～20	应用序列号	10	BCD
21～30	保留	10	BCD
说明:应用序列号的顺序排列见表 41 的说明			

——卡类型编码表见表 48。

表 48 卡类型编码表

卡型	代码
用户卡	01
其他	自定义

——表具设置文件见表 49。

表 49 表具设置文件

<table>
<tr><td colspan="3">文件标识(SFI)</td><td>11H</td></tr>
<tr><td colspan="3">文件类型</td><td>二进制</td></tr>
<tr><td colspan="3">文件大小</td><td>01H</td></tr>
<tr><td colspan="2">文件存取控制</td><td>读=需要安全信息</td><td>写=需要安全信息</td></tr>
<tr><td>字节</td><td colspan="2">数据元</td><td>长度/byte</td></tr>
<tr><td>1</td><td colspan="2">报警线</td><td>1</td></tr>
<tr><td>2</td><td colspan="2">关阀线</td><td>1</td></tr>
<tr><td>3～14</td><td colspan="2">发卡方自定义的信息资料</td><td>12</td></tr>
</table>

发卡机构通过 IC 卡中表具设置文件对预付费终端的参数进行设置，本标准仅规定了表具设置文件的基本内容，发卡机构可根据需要自定义其他信息内容。

——统计文件见表 50。

表 50 统计文件

<table>
<tr><td colspan="3">文件标识(SFI)</td><td>12H</td></tr>
<tr><td colspan="3">文件类型</td><td>定长记录</td></tr>
<tr><td>记录大小</td><td>6</td><td>记录数</td><td>≥12</td></tr>
<tr><td colspan="2">文件存取控制</td><td>读=自由</td><td>写=需要安全信息</td></tr>
<tr><td>字节</td><td colspan="2">数据元</td><td>长度/byte</td></tr>
<tr><td>1</td><td colspan="2">年</td><td>1</td></tr>
<tr><td>2</td><td colspan="2">月</td><td>1</td></tr>
<tr><td>3～6</td><td colspan="2">月用量</td><td>4</td></tr>
</table>

表具类终端每次对用户 IC 卡操作时，把各月的统计数据写回统计文件，发卡方通过统计文件中的内容对用户的使用情况进行查询和统计，统计文件至少应能存储 12 个月的使用量。

——计量文件见表 51。

表 51 计量文件

字段名	长度/byte
购买量	4
消费交易序号(次数)	2
充值交易序号(次数)	2

计量文件中存储的购买量是指用户购买的预付值。发卡方对 IC 卡进行充值操作时应根据价格对用户收取相应的资金。用户在预付费终端消费时，计量文件中的购买量一次性或分次被扣除，同时终端存储的剩余量相应增加。

——行业应用交易记录文件见表 52。

表 52 行业应用交易记录文件

文件标识(SFI)		18H
文件类型		循环记录
文件大小		18H
文件存取控制	读=自由	写=需要安全信息
字节	数据元	长度/byte
1～6	终端机编号	6 备注:行业代码(2)+序号(4)
7～13	交易日期时间	7
14～17	交易金额	4
18	交易类型	1 备注:02=消费
19～22	现有余额	4
23～24	交易序号	2

以上数据格式中未经特殊指出的均为 BCD 码。

7.3 应用系统安全要求

7.3.1 安全保密的基本原则

根据目前我国建设部所辖行业的实际情况，建设事业 IC 卡应用安全保密的基本原则是：

a）安全服从于国家利益:任何部门或机构在实施安全管理时应遵循国家有关法律、法规，并接受国家相关部门的指导、监督和检查。

b）独立自主:在建设事业 IC 卡应用中，凡涉及安全保密的重要环节，所用技术与产品应遵守国家有关管理部门的规定。

c）选用成熟技术:建设事业 IC 卡应用系统应尽量采用成熟的技术和产品。

7.3.2 主机系统安全要求

7.3.2.1 主机系统安全要求要点

为保证主机系统的安全，应采取以下措施：

a）关键数据不以明码的形式出现在系统与网络上的任何地方；

b）发现受到攻击时，能够马上进行封闭；

c）任何操作和数据存取在系统中留下记录；

d）禁止使用者接触与之无关的数据和进行无权进行的操作，防止无意的误操作。

7.3.2.2 主机系统安全措施要点

a）主机用户管理

主机操作系统提供了用户登录注册、口令和权限等控制措施；系统管理员在进入应用系统控制平台维护系统时须再次通过新的登录和密码检验，从而保证系统的安全。

b）主机文档管理

主机操作系统提供完善的文档及周边设备的使用权限管理，系统管理和维护人员可以分别针对每个人或工作组设定不同的文档读写及执行权限。

c）安全规范

主机系统安全管理符合 GB/T 18336 所规定的等级安全规范要求。

d）系统审计

在主机系统中通过设置审计功能，可以对主机系统中关键数据文件和代码存取进行记录，以文件形式保留备查。

7.3.3 网络系统安全要求

a）采用可按端口级和MAC地址级划分VLAN的以太交换机，具有MAC地址过滤功能，保证局域网络的安全；

b）利用路由器IP地址过滤功能，防止非法IP节点的侵入；

c）利用网管工作站实时网络自动发现功能，一旦在网络拓扑图中出现新的IP节点，自动产生报警或执行自动操作进行断链；

d）对于分组交换网，建议采用闭合用户群的方式加强网络的安全；

e）尽可能选用本系统专用网；

f）对于拨号方式，利用路由器的Chat协议进行身份认证；

g）双机备份、交易日志、非正常中断的恢复功能、信息传输过程的加密和MAC校验、定时对帐、通信中断后的身份认证程序等。

7.3.4 终端安全要求

终端能够识别操作IC卡，终端的安全是IC卡应用系统安全的重要条件。

终端的管理要遵循以下原则：

7.3.4.1 终端程序的下载

建设事业IC卡使用的终端必须统一编号，统一管理：

a）开发终端程序的软件包必须严格控制；

b）终端对程序的下载必须有口令控制，以防止非法下载；

c）终端程序的下载由专人执行，并做记录。

7.3.4.2 终端的加密

安全存取模块（ISAM、PSAM）具备以下功能：

a）保护所有敏感数据不会泄漏；

b）受到非法攻击和篡改会自动删除内部的所有敏感数据；

c）批准交易时可进行黑名单查找；

d）完成安全报文传送和密钥算法。

7.3.4.3 终端内部应用的安全

如果终端上有多个应用，在应用程序上做到：公用数据可以共享，各应用的内部数据要相互独立。

8 密钥系统和安全认证技术要求

本节规定了建设事业IC卡应用项目中密钥系统和服务中的互操作性建立的需求和指南。

阐明了各类密钥的生成、发行、更新和使用办法，各类安全存取模块的数据结构，用户卡和各类消费终端的安全认证流程，各类数据安全报文的传送方式等安全方面的要求。

本节规定了密钥系统的最低要求，一个城市的密钥系统，无论是在一台计算机或一台终端上实现，不能以比本标准规定的安全、保护或控制要求还要低的方式来实现或控制。

8.1 密钥系统

密钥系统分为部级密钥系统和城市级密钥系统两级。

8.2 城市密钥系统

城市密钥系统的作用是生成城市的充值根密钥和产生城市各行业的充值主密钥以及发行ISAM和用户卡。

8.2.1 密钥的种类

公共充值密钥、行业充值密钥、PIN解锁主密钥、PIN重装主密钥、ISAM维护密钥。

8.2.2 密钥的生成和发行

8.2.2.1 **密钥生成的基本安全要求**

为保证密钥的安全和防止密钥的泄露，在密钥生成时，应采取以下措施：

a）密钥生成采用多人生成或硬件加密的方式；

b）密钥生成的环境应保证绝对安全；

c）参加密钥生成的特殊人员的安全管理规定；

d）密钥生成过程必须按照严格的操作规程进行。

8.2.2.2 **密钥生成方式**

密钥一般采用集中方式生成，即由项目最高管理机构生成相应的各种主密钥组，其他密钥由该组密钥分散生成。密钥生成的两种基本方法：

a）不重复的密钥生成：随机过程，生成不可恢复的密钥，每次的数值不相同；

b）可重复的密钥生成：密钥变换、密钥衍生；而且密钥的生成是可以重复的，在需要的情况下能够重新得到与原来相同的密钥值。

8.2.2.3 **密钥生成的安全技术**

不需重复生成的密钥采用随机产生的办法生成，由系统随机产生这些密钥，写入安全存取模块中保存，可重复生成的密钥采用密钥交换或密钥衍生的办法生成，确保密钥变换或密钥衍生的过程绝对安全。

8.2.2.4 **密钥发行方式**

密钥的发行采用梯级生成、下发方式。即由上一级生成下一级所需的各种子密钥，并以卡片的形式传递给下一级。

8.2.2.5 **密钥发行的安全技术**

使用传输密钥控制业务主密钥的加密装载、直接加密导出、分散加密导出。

8.2.3 **密钥的更新**

8.2.3.1 **密钥更新的基本安全要求**

当密钥的生命周期结束或系统密钥泄露后，需要进行密钥更新。密钥更新的基本原则是保护持卡人的利益不受损害，不影响持卡人的正常交易；密钥更新的全过程必须保证系统的安全性能不受影响。

8.2.3.2 **正常密钥更新**

正常密钥更新的两种方法：

a）密钥替换；

b）更换密钥组。

8.2.3.3 **紧急密钥更新**

一旦密钥泄露，必须立即进行紧急密钥更新。

紧急密钥更新的主要方法有：

a）安装多组紧急密钥备份组；

b）停止现有密钥的使用，重新生成密钥。

8.3 **安全存取模块**

8.3.1 **安全存取模块的物理安全要求**

安全存取模块的硬件设计必须能够保证在物理上限制对其内部存储的敏感数据的认证与窃取，以及对安全存取模块的非授权使用和修改。一旦安全存取模块受到非法的篡改及攻击，其自身必须能够立即完成对内部敏感数据的有效保护，要实现这些目标，安全存取模块应具有防窃等相应机制。

对安全存取模块的构造必须满足下列要求：

a）即使通过特别的工具或专用严重破坏的方法，也不能对模块的硬件或软件进行增加、替换或修改；

b）任何对敏感数据的访问或修改，只有通过对模块的授权才能达到；

c）安全存取模块的任何部分的损坏或失效都不会导致敏感数据的泄露；

d）如果安全存取模块是由多个分离的部分组合而成，而处理的数据又必须在这些部件之间传递，那么各部件须保持相同的安全级别。

8.3.2 安全存取模块的逻辑安全要求

一个安全存取模块的逻辑设计应保证，调用任何单一功能或组合功能，都不会导致敏感数据的泄露。对于某些敏感数据操作，必须有一定的权限限制。

安全存取模块中可以存放多组不同版本不同索引的主密钥。所有的主密钥通常必须在终端机使用之前被下装到安全存取模块中。如果在使用过程中，主密钥需要修改，则必须使用安全报文。而要实现这一过程通常必须在特殊的授权情况下完成。对外部不能存在任何取得密钥的机会。

为避免伪操作，存放在安全存取模块中的不同类型的主密钥必须与不同特定的应用操作相结合。

所有脱机交易相关的主密钥和敏感数据必须存储在安全存取模块中。

安全存取模块必须可以实现对称密钥算法。

8.3.3 PSAM 数据结构

PSAM 数据结构见图 10。

- MF（3F00）
  - 密钥数据元文件
  - 0015（公共信息文件）
  - 0016（终端信息文件）
  - ADF1(1001) （目录名:MMCC）
    - 密钥数据元文件
    - 0017（ADF1应用公共信息文件）
  - ADF2 （1002）（目录名：CITY）
    - 密钥数据元文件
    - 0017（ADF2应用公共信息文件）
  - ADF3 （1003）（目录名：MIFARE）
    - 密钥数据元文件
    - 0017（ADF3应用公共信息文件）
  - ADF4 （1004）（目录名：其他）
    - 密钥数据元文件

图 10 PSAM 结构拓扑图

PSAM 文件详细信息见表 53。

表 53 PSAM 文件详细信息

文件名称	文件类型	文件标识符	文件长度(HEX)	操作权限	
MF		3F00		满足一定条件可建立文件	
密钥数据元文件					
DIR 文件	记录文件	0001		读＝自由	写＝需要安全信息
公共信息文件	二进制文件	0015	0EH		
终端信息文件	二进制文件	0016	06H		
ADF1		1001			
密钥数据元文件					
应用公共信息文件	二进制文件	0017	19H	读＝自由	写＝需要安全信息
ADF2		1002			
密钥数据元文件	二进制文件				
应用公共信息文件		0017	19H	读＝自由	写＝需要安全信息
ADF3		1003			

表 53(续)

文件名称	文件类型	文件标识符	文件长度(HEX)	操作权限	
密钥数据元文件					
应用公共信息		0017	19H	读＝自由	写＝需要安全信息
ADF4		1004			
密钥数据元文件					
说明:短文件标识符为文件标识符的低字节的后 5 位(bit)					

8.3.4 ISAM 数据结构

ISAM 数据结构见图 11。

ISAM 文件详细信息见表 54。

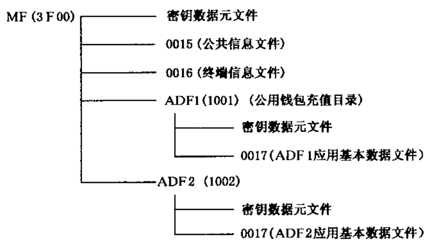

图 11　ISAM 结构拓扑图

表 54　ISAM 文件详细信息

文件名称	文件类型	文件表示符	文件长度(HEX)	操作权限	
MF		3F00			
密钥数据元文件					
公共信息文件	二进制文件	0015	000E	读＝自由	写＝需要安全信息
终端信息文件	二进制文件	0016	0006		
ADF1		1001			
密钥数据元文件					
应用公共信息文件	二进制文件	0017	0029	读＝自由	写＝需要安全信息
ADF2		1002			
密钥数据元文件					
应用公共信息文件	二进制文件	0017	0019	读＝自由	写＝需要安全信息

8.4 安全认证流程

8.4.1 消费交易安全认证流程

消费交易安全认证流程见图 12。

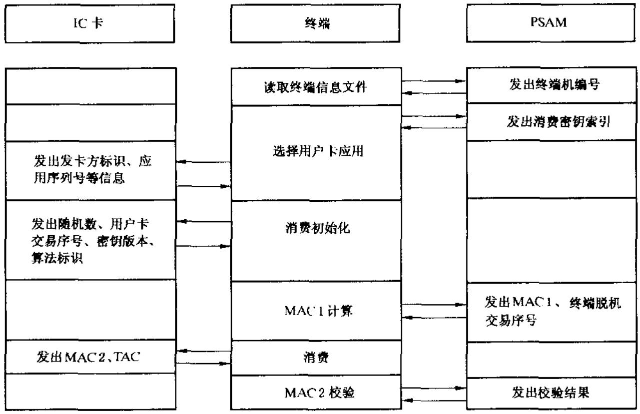

图 12　消费交易安全认证流程

8.4.2　充值交易安全认证流程

充值交易安全认证流程见图 13。

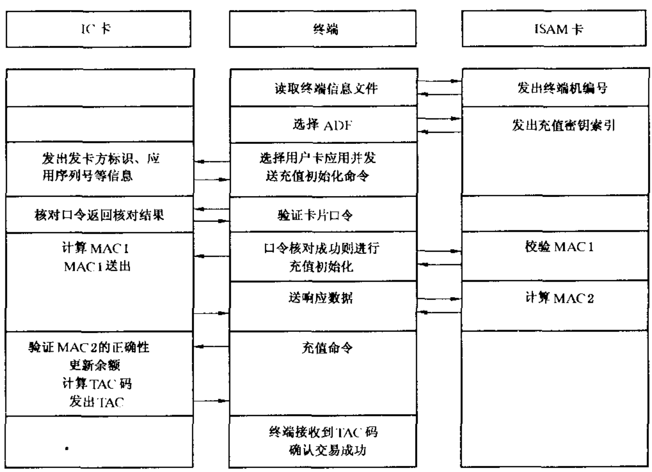

图 13　充值交易安全认证流程