ICS 35.240.60
P 07

CJ

中华人民共和国城镇建设行业标准

CJ/T 243—2007

建设事业集成电路(IC)卡产品检测

Test methods for construction cause IC card

2007-04-18 发布　　2007-12-01 实施

中华人民共和国建设部　发布

目　次

前　言

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卡应用服务中心负责起草。

本标准参编单位：中外建设信息有限责任公司、国家金卡工程IC卡及机具产品检验中心、北京江南歌盟科技有限公司、黄石捷德万达金卡有限公司、北京融通高科科技发展有限公司、北京握奇数据系统有限公司、朝阳华龙电子仪表有限公司、成都前锋电子仪器厂、丹东思凯电子发展有限责任公司、杭州先锋电子技术有限公司、宁波东海集团有限公司、上海华虹集成电路有限责任公司、深圳市华旭科技开发有限公司、深圳市大明五洲城市一卡通科技有限公司、天津环球磁卡股份有限公司、武汉蓝焰自动化应用技术有限责任公司、武汉天喻信息产业股份有限公司、浙江威星仪表系统集成有限公司、重庆明光燃气设备有限公司、珠海东信和平智能卡股份有限公司、珠海亿达科技电子工业有限公司、汉中智能仪表工业有限公司、云南省宜威市荣祥智能水表厂、大连世达科技有限公司。

本标准主要起草人：马虹、申绯斐、王辉、杜昊、赵海波、周欣、王毅、（以下按姓氏笔画排序）丹明波、王天际、王辉（东信和平）、刘贤斌、孙立颖、朱洲、边红丽、汤天顺、闫延辉、张大群、张松林、杨德强、汪有余、周天宝、周承平、林立峰、欧阳由、钟键、钱维钧、高林洪、常波、黄铁军、谢文录、谢骏。

本标准为首次发布。

建设事业集成电路(IC)卡产品检测

1 范围

本标准规定了建设事业集成电路(IC)卡产品,包括接触式IC卡、非接触IC卡、双界面IC卡、IC卡终端的检测,以及逻辑加密卡表具类终端、CPU卡表具类终端、消费类及服务类IC卡终端的应用检测。

本标准适用于公共交通、出租车、轨道交通(地铁、轻轨)、轮渡、燃气、供水、供暖、数字社区、路桥收费、停车场、公园景点等应用领域的IC卡产品检测。

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 2099.1 家用和类似用途插头插座 第一部分:通用要求

GB/T 2423.1—2001 电工电子产品环境试验 第2部分:试验方法 试验A:低温

GB/T 2423.2—2001 电工电子产品环境试验 第2部分:试验方法 试验B:高温

GB/T 2423.3—2006 电工电子产品环境试验 第2部分:试验方法 试验Ca:恒定湿热

GB/T 2423.5—1995 电工电子产品环境试验 第2部分:试验方法 试验Ea和导则:冲击

GB/T 2423.6—1995 电工电子产品环境试验 第2部分:试验方法 试验Eb和导则:碰撞

GB/T 2423.10—1995 电工电子产品环境试验 第2部分:试验方法 试验Fc和导则:振动(正弦)

GB/T 4857.2—2005 包装运输包装件基本试验 第2部分:温湿度调节处理

GB/T 4857.5—1992 包装、运输包装件 跌落试验方法

GB 4943—2001 信息技术设备的安全

GB 9254—1998 信息技术设备的无线电骚扰限值和测量方法

GB/T 14916—2006 识别卡 物理特性

GB/T 16649.1—2006 识别卡 带触点的集成电路卡 第1部分:物理特性

GB/T 16649.2—2006 识别卡 带触点的集成电路卡 第2部分:触点的尺寸和位置

GB/T 16649.3—2006 识别卡 带触点的集成电路卡 第3部分:电信号和传输协议

GB/T 17554.1—2006 识别卡 测试方法 第1部分:一般特性测试

GB/T 17618—1998 信息技术设备抗扰度限值和测量方法

GB/T 17626.2—1998 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 17626.3—1998 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验

GB/T 17626.4—1998 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验

GB/T 17626.5—1998 电磁兼容 试验和测量技术 浪涌(冲击)抗扰度试验

GB/T 17626.6—1998 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度

GB/T 17626.8—1998 电磁兼容 试验和测量技术 工频磁场抗扰度试验

GB/T 17626.11—1999 电磁兼容 试验和测量技术 电压暂降、短时中断和电压变化的抗扰度试验

CJ/T 166—2006 建设事业集成电路(IC)卡应用技术

CJ/T 3087—1999 城市公共汽车、电车收费设备电子收费机应用技术条件

CJ 5024—1997 电子式出租汽车计价器

JR/T 0025—2005 中国金融集成电路(IC)卡规范

ISO 7637 道路车辆传导和耦合造成的电骚扰

ISO/IEC 10373-3:2001 识别卡 测试方法 第三部分:带触点的集成电路卡及其相关接口设备

ISO/IEC 10373-6:2001 识别卡 测试方法 第六部分:接近式卡

ISO/IEC 14443-1:2000 识别卡 无触点集成电路卡 接近式卡 第1部分:物理特性

ISO/IEC 14443-2 识别卡 无触点集成电路卡 接近式卡 第2部分:射频功率和信号接口

ISO/IEC 14443-3 识别卡 无触点集成电路卡 接近式卡 第3部分:初始化和防冲突

ISO/IEC 14443-4 识别卡 无触点集成电路卡 接近式卡 第4部分:传输协议

ISO/IEC 7810:2003 识别卡 物理特性

ISO/IEC 7816-1:1998 AMD.1:2003 识别卡 带触点的集成电路卡 第1部分:物理特性 修改件1 识别卡触点表面的最大高度

ISO/IEC 7816-3:1997 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 7816-3:1997 AMD.1:2002 识别卡 带触点的集成电路卡 第3部分:电信号和传输协议 修改件1 在5 V,3 V,1.8 V上工作的集成电路卡的电特性和等级表示

ISO/IEC 7816-4:2005 识别卡 带触点的集成电路卡 第3部分:交换用组织、安全和命令

3 术语和定义

下列术语和定义适用于本标准。

3.1

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。

3.2

非接触式IC卡 contactless IC card

无触点的集成电路卡。

3.3

接触式IC卡 contact IC card

带触点的集成电路卡。

3.4

CPU卡 central processing unit card

一种具有微处理器芯片的IC卡。

3.5

逻辑加密卡 logic encrypt card

采用密码控制逻辑单元的存储器卡。

3.6

消费安全认证模块 purchase secure access module

由IC卡发行主管部门或应用主管机构发行的可以用于对IC卡进行脱机消费交易认证的安全认证卡,安装在各类消费类IC卡终端中。

3.7

充值安全认证模块 input secure access module

由IC卡发行主管部门或应用主管机构发行的可以用于对IC卡进行充值安全认证的卡(模块),安装在充值类终端中。

3.8

嵌入式安全认证模块　embedded secure access module

由IC卡发行主管部门或应用主管机构发行的可以用于对IC卡进行脱机消费交易认证的嵌入式安全认证模块，安装在各类表具类IC卡终端中。

3.9

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安全数据进行非法攻击的硬件加密模块。

3.10

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。

3.11

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。

3.12

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。

3.13

密文　ciphertext

通过密码系统产生的不可理解的文字或信号。

3.14

密钥　key

控制加密转换操作的符号序列。

3.15

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。

3.16

访问控制字　access bit

逻辑加密卡中控制数据块读写权限的标志字。

3.17

口令　password

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

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。

3.19

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。

3.20

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。

3.21

电子存折　electronic deposit

一种为持卡人进行消费、取现等交易而设计的使用个人密码(PIN)保护的金融IC卡应用。它支持圈存、圈提、消费、取现、修改透支限额及查询余额交易。

3.22

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。

3.23

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。

3.24

黑名单　lawless list

由于结算、对账不符、非法交易、非法卡交易等产生的非法列表清单。

3.25

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。

3.26

IC卡读写器　reader

可与IC卡进行数据交换的终端设备。

3.27

充值终端　charge terminal

可以增加IC卡中服务计量值的终端设备。

3.28

消费类终端　purchase type terminal

支持在公共汽电车、出租汽车、地铁、城市轨道交通、轮渡、索道、公园、停车场等公共场所完成对IC卡消费交易的终端。

3.29

表具类终端　gauge type terminal

支持对预付费的水、燃气和热量给予正常供应的终端。

3.30

服务类终端　service type terminal

提供售卡、充值、验卡、圈存、管理等服务的终端。

3.31

物理安全性　physical security

设备的物理结构抵御攻击的能力。

3.32

安全加密设备　secure cryptographic device

能提供一系列安全加密服务,具有逻辑安全性和物理安全性的硬件设备。

3.33

攻击　attack

在未授权状况下,试图在设备上获取或修改敏感信息的一种行为。

3.34

T=0 协议

面向字符的异步半双工传输协议。

3.35

T=1 协议

面向块的异步半双工传输协议。

3.36

块 block

数据存储单元。

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)
An	字母数字型(Alphanumeric)
Ans	字母数字及特殊字符型(Alphanumeric Special)
APDU	应用协议数据单元(Application Protocol Data Unit)
B	二进制(Binary)
CLA	命令报文的类别字节(Class Byte of the Command Message)
Cn	压缩数字型(Compressed Numeric)
CPU	中央处理器(Central Processing Unit)
CSN	卡片惟一号(Card Single Number)
DDF	目录数据文件(Directory Definition File)
DF	专用文件(Dedicated File)
DIR	目录(Directory)
ED	电子存折(Electronic Deposit)
EF	基本文件(Elementary File)
EP	电子钱包(Electronic Purse)
ESAM	嵌入式安全认证模块(Embedded Secure Access Module)
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	充值安全认证模块(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 接近式耦合设备(Proximity Coupling Device)
PICC 接近式卡(Proximity Card)
PIN 个人密码(Personal Identification Number)
PSAM 消费安全认证模块(Purchase Secure Access Module)
SAM 安全存取模块(Secure Access Module)
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 IC 卡检测

5.1 接触式 IC 卡检测

接触式 IC 卡检测应符合表 1 的规定。

表 1 接触式 IC 卡检测

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	1	弯曲应力检测	① 确认样卡功能正常； ② 在试验机上设置弯曲次数：250 次，分别对样卡的长、短边四个测试方向各弯曲 250 次，并确认状态设置正确； ③ 按照试验机的操作规定，将样卡放在试验机的两个夹具之间，无误后启动设备； ④ 试验结束时对样卡进行功能测试，对测试结果进行判断、记录	应符合 GB/T 16649.1—2006 中 4.2.10 和 4.2.11 的要求	符合或不符合
2	2	扭曲应力检测	① 确认样卡功能正常； ② 在试验机上设置扭曲次数：1 000 次，并确认状态设置正确； ③ 按照试验机的操作规定，将样卡放在试验机的两个夹具之间，无误后启动设备； ④ 每 250 次扭曲之后，对样卡进行功能测试，对测试结果进行判断、记录		
3	3	抗紫外线检测	① 确认样卡功能正常； ② 检查试验设备状态，并确认状态设置正确； ③ 按照试验设备的操作规定，将样卡正确放入试验设备，无误后启动设备，对样卡的正面辐照，接受总能量为 15 Ws/cm^2 的光照； ④ 试验结束时对样卡进行功能测试，对测试结果进行判断、记录。同样方法，再对样卡的背面辐照	应符合 GB/T 17554.1—2006 中 5.12 条的要求	

表 1(续)

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
4	4	特定温湿度下的卡片稳定性检测	① 确认样卡符合标准要求； ② 按照－40℃、50℃、5%、95%的顺序设置试验箱的温度、相对湿度，并确认状态设置正确； ③ 将样卡水平放入试验箱内，在每一种环境中经受 60 min 试验； ④ 每一种环境试验结束之后，将样卡从试验箱中取出，在 23℃±3℃、40%～60%条件下恢复 24 h 后，对样卡进行尺寸、翘曲测量，对测量结果进行判断、记录	在－40℃～50℃、相对湿度为 5%～95%的条件下卡片尺寸和翘曲应符合 GB/T 14916—2006 中 8.5 的要求	符合或不符合
5	5	剥离强度检测	① 先将样卡表面切成 4 条 10 mm 宽的切块； ② 再从卡基上切出一条约 10 mm 宽的涂覆层； ③ 将粘结带加在涂覆层背面，按照试验设备的操作规定，将样卡正确装入试验设备，试验设备无误后启动设备； ④ 试验结束后，对剥离强度测试值进行记录，并与标准值相比较。同样方法，对样卡的其余 3 条涂覆层进行检验	应符合 GB/T 14916—2006 中 8.8 的要求	
6	6	触点的表面轮廓检测	① 检查试验设备状态并确认状态设置正确； ② 将样卡放在刚性平台上，无误后启动设备进行测量； ③ 对测量结果进行判断、记录	应符合 GB/T 16649.1—2006 中 4.2.3 的要求	
7	7	机械强度检测	① 确认样卡功能正常； ② 在触点表面和触点区域(整个导电表面)施加 1.5 N 的工作压力。(芯片面积小于 4 平方毫米时)； ③ 将样卡正面朝上装入试验设备，在 ICC 上加一个 8 N 的力，无误后启动设备；将 ICC 触点在三个钢轮间往复移动； ④ 试验结束后对样卡进行功能测试，对测试结果进行判断、记录。同样方法，再对样卡的背面进行试验	应符合 GB/T 16649.1—2006 中 4.2.4	
8	8	触点电阻检测	① 检查试验设备状态并确认状态设置正确； ② 将样卡放在一个平整的硬表面上，将测试探针压在样卡的第一个触点上，无误后启动设备； ③ 对测试结果进行判断、记录； ④ 再移动测试探针，依次对样卡的各个触点进行测试	应符合 GB/T 16649.1—2006 中 4.2.5 的要求	

表 1(续)

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
9	9	电磁干扰检测(适用于带磁条的接触式IC卡)	① 确认样卡功能正常； ② 检查试验设备状态并确认状态设置正确； ③ 按照试验设备的操作规定，将样品正确装入试验设备，无误后启动设备进行测试； ④ 试验结束对样品进行功能测试，对测试结果进行判断、记录	应符合 GB/T 16649.1 2006 中 4.2.6 的要求	符合或不符合
10	10	电磁场检测	① 确认样卡功能正常； ② 检查试验设备状态并确认状态设置正确； ③ 将样卡放入静磁场中； ④ 试验结束对样卡进行功能测试，对测试结果进行判断、记录	应符合 GB/T 16649.1—2006 中 4.2.7 的要求	
11	11	抗静电检测	① 确认样卡功能正常； ② 设置试验电压 2 000 V，并确认状态设置正确； ③ 按照试验设备的操作规定，将样卡正确装入试验设备，将试验设备的接地插针与样卡的接地触点连接，无误后启动设备，对样卡的各触点进行正极性放电； ④ 试验结束后，对样卡进行功能测试，对测试结果进行判断、记录。同样方法，对样卡的各触点进行负极性放电	应符合 GB/T 16649.1 2006 中 4.2.8 的要求	
12	12	抗化学性检测	① 确认样卡功能正常； ② 将样卡分别浸入标准规定的各种溶液中 1 min(短期污染)或 24 h(长期污染)； ③ 从溶液中取出，立即在蒸馏水中清洗，擦干后，对样品进行功能测试、外观检验，对测试结果进行判断、记录	应符合 GB/T 17554.1—2006 中 5.4 的要求	
13	13	尺寸、触点位置和编号检测	① 检查测量设备状态并确认状态设置正确； ② 将样卡放在水平刚性平台上，压上 2.2 N±0.2 N 的负荷，无误后启动设备进行测量； ③ 对测量结果进行判断、记录	应符合 GB/T 14916 2006 中第 5 章；GB/T 16649.2—2006 中第 4 章和第 5 章的要求	
14	14	触点的尺寸检测	① 检查测量设备状态并确认状态设置正确； ② 将样卡放在水平刚性平台上，启动设备进行测量； ③ 对测量结果进行判断、记录	应符合 GB/T 16649.2 2006 中第 3 章的要求 触点的尺寸检测未通过，则终止检测	
15	15	电特性检测	① 检查试验设备状态并确认状态设置正确； ② 按照试验设备的操作规定，将样品正确装入试验设备，无误后启动设备进行测试； ③ 测试结束对测试结果进行判断、记录	应符合 GB/T 16649.3—2006 中第 4 章、ISO/IEC 7816-3:1997 中第 4 章、ISO/IEC 7816-3:1997 AMD.1:2002 的要求	

表 1(续)

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
16	16	复位应答检测	① 确认所分配的样品工作正常； ② 检查试验设备状态并确认状态设置正确； ③ 按照试验设备的操作规定，将样品正确装入试验设备，无误后启动设备进行测试； ④ 对测试结果进行判断、记录	应符合 GB/T 16649.3—2006 中第 5 章、ISO/IEC 7816-3:1997 中第 5 章、ISO/IEC 7816-3:1997 AMD.1:2002 的要求	符合或不符合
17	17	操作过程检测			
18	18	T=0 异步半双工字符传输协议检测		应符合 GB/T 16649.3—2006 中第 8 章、ISO/IEC 7816-3:1997 中第 8 章的要求	
19	19	行业间命令检测		应符合 CJ/T 166—2006 中 5.6 条、ISO/IEC 7816-4:2005 的要求	
20	20	功能检测		应能够正确完成 CJ/T 166 应用要求	
21	21	安全性能检测		应能保障 CJ/T 166 规定的应用安全执行	
22	22	命令参数检测		应支持 CJ/T 166 规定的命令参数	
23	23	防拔检测		在任何情况下应能保证非易失性存储器中数据的完整准确	

5.2 非接触式 IC 卡检测

非接触式 IC 卡检测应符合表 2 的规定。

表 2 非接触式 IC 卡检测

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	24	弯曲应力检测	参见接触式 IC 卡检测中项目编号 1 的检测方法步骤	应符合 ISO/IEC 14443-1:2000 中 4.3.3 的要求	符合或不符合
2	25	扭曲应力检测	参见接触式 IC 卡检测中项目编号 2 的检测方法步骤	应符合 ISO/IEC 14443-1:2000 中 4.3.4 的要求	
3	26	紫外线检测	参见接触式 IC 卡检测中项目编号 3 的检测方法步骤	应符合 GB/T 17554.1—2006 中 5.1.2 的要求	
4	27	特定温湿度下的卡片稳定性检测	参见接触式 IC 卡检测中项目编号 4 的测方法步骤	在－40℃～50℃、相对湿度为 5%～95%的条件下卡片尺寸和翘曲应能满足 GB/T 14916—2006 中 8.5 的要求	
5	28	剥离强度检测	参见接触式 IC 卡检测中项目编号 5 的检测方法步骤	应符合 GB/T 14916—2006 中 8.8 的要求	

表 2(续)

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
6	29	电磁干扰检测(适用于带磁条的非接触式IC卡)	参见接触式IC卡检测中项目编号9的检测方法步骤	应符合GB/T 16649.1—2006中4.2.6条的要求	符合或不符合
7	30	交变电场检测	参见接触式IC卡检测中项目编号16的检测方法步骤	应符合ISO/IEC 14443-1:2000中4.3.6的要求	
8	31	交变磁场检测		应符合ISO/IEC 14443-1:2000中4.3.5的要求	
9	32	抗静电检测	① 确认样卡功能正常; ② 设置试验电压6 000 V,并确认状态设置正确; ③ 按照试验设备的操作规定,将样卡正确装入试验设备,无误后启动设备,对样卡进行正极性放电; ④ 试验结束后,对样卡进行功能测试,对测试结果进行判断、记录。同样方法,对样卡进行负极性放电	应符合ISO/IEC 14443-1:2000中4.3.7的要求	
10	33	化学特性检测	参见接触式IC卡检测中项目编号12的检测方法步骤	应符合GB/T 17554.1—2006中5.4的要求	
11	34	卡片粘性检测	① 确认样卡符合标准要求; ② 设置试验箱的温度40℃、相对湿度40%~60%,并确认状态设置正确; ③ 将样卡5张一组堆积,均按同一个方向,卡的背面朝下,在最上层卡的表面,压上一个2.5 kPa的压块,放入试验设备,无误后启动设备; ④ 存放48 h后取出,对样卡进行外观检验,对检验结果进行判断、记录	应符合GB/T 14916—2006中8.9的要求	
12	35	射频功率和信号接口检测	参见接触式IC卡检测中项目编号16的检测方法步骤	应符合ISO/IEC 14443-2的要求	
13	36	读写距离检测	① 检查试验设备状态并确认状态设置正确; ② 按照试验设备的操作规定,将样卡放在正对天线的位置,无误后启动设备,移动卡或天线进行测量; ③ 对测量结果进行判断、记录	应符合非接触卡应用的实际要求	

表 2(续)

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
14	37	初始化和防冲突检测	参见接触式 IC 卡检测中项目编号 16 的检测方法步骤	应符合 ISO/IEC 14443-3 的要求	符合或不符合
15	38	非正常中断的恢复机制检测		应符合 CJ/T 166 的要求	
16	39	传输协议检测		应符合 ISO/IEC 14443-4 要求	
17	40	半双工块传输协议检测			
18	41	功能检测		应符合 CJ/T 166 的要求	
19	42	应用检测			
20	43	安全检测		应符合 CJ/T 166 应用数据安全的要求	

5.3 双界面 IC 卡检测

双界面 IC 卡检测应符合表 3 的规定。

表 3 双界面 IC 卡检测

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	44	物理特性检测	参见接触式 IC 卡检测中项目编号 16 的检测方法步骤	参照接触式 IC 卡检测和非接触式 IC 卡检测的相关要求	符合或不符合
2	45	电气特性检测			
3	46	传输协议检测			

6 IC 卡终端检测

6.1 结构、外观要求

IC 卡终端结构、外观检测应符合表 4 的规定。

表 4 IC 卡终端结构、外观要求

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	47	结构、外观检测	由检验人员目测或检测仪器检测	样品表面不应有明显的凹痕、划伤、裂缝、变形和污染等。表面镀层应均匀、不应起泡、龟裂、脱落和磨损。金属零部件不应有锈蚀及其他机械损伤。样品的零部件应紧固无松动,安装可替换部件的接插件应能可靠连接,键盘、开关按钮和其他控制部件的控制应灵活可靠,布局应方便使用。对于便携式产品而言,除特殊按键外,各按键应平整一致,其压力离散性不应大于 0.3 N,每个按键在规定的负荷条件下,通断寿命应大于 10^5 次。产品的标识、标注应符合国家有关规定的要求	符合或不符合

6.2 气候环境要求

IC卡终端气候环境应符合表5的规定。

表5 IC卡终端气候环境要求

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	48	工作温度下限检测	参见接触式IC卡检测中项目编号16的检测方法步骤	按照GB/T 2423.1—2001中的“试验Ad”或“试验Ab”进行。城市公共汽车、电车收费设备应满足CJ/T 3087—1999规定的温度	符合或不符合
2	49	贮存温度下限检测		按照GB/T 2423.1—2001中的“试验Ab”进行。城市公共汽车、电车收费设备应满足CJ/T 3087—1999规定的温度	
3	50	工作温度上限检测		按照GB/T 2423.2—2001中的“试验Bd”或“试验Bb”进行。城市公共汽车、电车收费设备应满足CJ/T 3087—1999规定的温度	
4	51	贮存运输温度上限检测		按照GB/T 2423.2—2001中的“试验Bb”进行。城市公共汽车、电车收费设备应满足CJ/T 3087—1999规定的温度	
5	52	工作条件下的恒定湿热检测		参照GB/T 2423.3—2006中的“试验Ca”进行。城市公共汽车、电车收费设备应满足CJ/T 3087—1999的规定	
6	53	贮存运输条件下的恒定湿热检测			

6.3 机械环境要求

IC卡终端机械环境应符合表6的规定。

表6 IC卡终端机械环境要求

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	54	振动检测	参见接触式IC卡检测中项目编号16的检测方法步骤	按照GB/T 2423.10—1995中的“试验Fc”进行	符合或不符合
2	55	冲击检测		按照GB/T 2423.5—1995中的“试验Ea”进行	
3	56	碰撞检测		按照GB/T 2423.6—1995中的“试验Eb”进行	
4	57	运输包装件跌落检测		按照GB/T 4857.2—2005标准的规定、运输包装件按GB/T 4857.5—2005的要求、出租汽车计价器应符合CJ 5024—1997表4中倾斜跌落项要求	

6.4 电源适应性要求

IC卡终端电源适应性应符合表7的规定。

表 7 IC 卡终端电源适应性

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	58	对直流样品的电源适应性检测	参见接触式 IC 卡检测中项目编号 16 的检测方法步骤	城市公共汽车、电车收费设备应满足 CJ/T 3087—1999规定的电源要求。对于直流电源供电的整机产品，原则上当电压在标称值±5%范围内时，产品工作应正常	符合或不符合
2	59	对交流样品的电源适应性检测		对于交流电源供电的整机产品，一般应在 220 V±22 V，50 Hz±1 Hz 条件下正常工作。电源插头试验按照 GB 2099.1 的规定进行	
3	60	对车载样品的电源适应性检测		对于直流电源供电的车载产品，当电压在标称值±5%范围内时，产品工作应正常。采用蓄电池供电有特殊要求的产品，应对电池的一些关键指标提出明确要求	

6.5 电磁兼容性要求

IC 卡终端电磁兼容性应符合表 8 的规定。

表 8 IC 卡终端电磁兼容性要求

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	61	辐射骚扰检测	参见接触式 IC 卡检测中项目编号 16 的检测方法步骤	应符合 GB 9254—1998 中辐射骚扰限值的 A 级要求	符合或不符合
2	62	电源端子传导骚扰检测		应符合 GB 9254—1998 中电源端子骚扰电压限值的 A 级要求（220V 或电源适配器供电时适用）	
3	63	静电放电抗扰度检测		应符合 GB/T 17618—1998、GB/T 17626.2—1998 中的相关要求	
4	64	射频电磁场辐射抗扰度检测		应符合 GB/T 17618—1998、GB/T 17626.3—1998 中的相关要求	
5	65	电快速瞬变脉冲群抗扰度检测		应符合 GB/T 17618—1998、GB/T 17626.4—1998 中的相关要求（220V 或电源适配器供电时适用）	
6	66	浪涌（冲击）抗扰度检测		应符合 GB/T 17618—1998、GB/T 17626.5—1998 中的相关要求（220 V 或电源适配器供电时适用）	
7	67	射频场感应的传导骚扰抗扰度检测		应符合 GB/T 17618—1998、GB/T 17626.6—1998 中的相关要求（220V 或电源适配器供电时适用）	
8	68	工频磁场抗扰度检测		应符合 GB/T 17618—1998、GB/T 17626.8—1998 中的相关要求	
9	69	电压暂降、短时中断和电压变化扰度检测		应符合 GB/T 17618—1998 中、GB/T 17626.11—1999 中的相关要求（220 V 或电源适配器供电时适用）	

6.6 机具的电气安全要求

IC卡终端电气安全应符合表9的规定。

表9 IC卡终端的电气安全要求

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	70	对地泄漏电流检测	参见接触式IC卡检测中项目编号16的检测方法步骤	应符合GB 4943—2001中5.1的有关规定(220 V或电源适配器供电时适用)	符合或不符合
2	71	抗电强度检测		应符合GB 4943—2001中5.2的有关规定(220V或电源适配器供电时适用)	
3	72	保护接地措施检测		应符合GB 4943—2001中2.6.3.3的有关要求(220V或电源适配器供电时适用)	

6.7 非接触式IC卡机具的射频功率与信号接口要求

非接触IC卡机具的射频功率与信号接口应符合表10的规定。

表10 非接触IC卡机具的射频功率与信号接口

序号	项目编号	测试项目	测试方法步骤	测试要求	测试结论
1	73	射频功率与信号接口检测	参见接触式IC卡检测中项目编号16的检测方法步骤	应满足ISO/IEC 14443-2、ISO/IEC 10373-6:2001中第8章、ISO/IEC 10373-6:2001的要求	符合或不符合

6.8 接触式IC卡机具的电信号和传输协议要求

接触IC卡机具的电信号和传输协议应符合表11的规定。

表11 接触式IC卡机具的电信号和传输协议

序号	项目编号	检测项目	检测方法步骤	检测要求	检测结论
1	74	电信号和传输协议检测	参见接触式IC卡检测中项目编号16的检测方法步骤	应满足ISO/IEC 7816-3:1997、ISO/IEC 7816-3:1997 AMD. 1:2002、ISO/IEC 10373-6:2001中第8章,第9章的要求	符合或不符合

7 逻辑加密卡表具类终端应用检测

在水表、气表、热力表行业应配合使用ESAM安全模块与卡片,通过密钥的控制来进行数据交换。应主要检测逻辑加密卡表具的读写数据的交易流程。

7.1 检测卡种类

检测卡种类可分为:

a) 正式用充值卡,用正式密钥增加购买量的充值卡;

b) 检测用充值卡,用于检测实验阶段增加购买量;

c) 修改密钥卡,用于正式运行前下装正式密钥;

d) 恢复密钥卡,用于将密钥恢复成检测状态的公开密钥;

e) ESAM卡,用于表具的安全认证和存储数据。

7.2 文件结构

7.2.1 充值卡文件结构

逻辑加密卡是以数据块为基本的存储单元,可形成统一的数据格式。各种卡片中的数据应以密文的方式存放,读出数据并由ESAM内的解密密钥解开后,进行数据处理。

7.2.1.1 **数据结构定义(4442卡为例)**

逻辑加密卡表具类充值卡文件结构应符合表12的规定。

表12 逻辑加密卡表具类充值卡文件结构

分区名称		数据项名称	长度 Byte	单位	相对地址	数据格式
公共信息区		用户代码	8	无量纲	00H～07H	BCD
		地址代码	4	无量纲	08H～0BH	BCD
		卡类别码	1	无量纲	0CH	BCD
		应用索引	2	无量纲	0DH～0EH	HEX
		应用分区首址(A0)	2	无量纲	0FH～10H	HEX
		校验和	1	无量纲	11H	HEX
		保留	14		12H～1FH	HEX
应用分区1(首址A_0)	通用信息区	管理系统代码	4	无量纲	00H～03H	HEX
		管理系统版本号	4	无量纲	04H～07H	HEX
		营业网点编号	2	无量纲	08H～09H	HEX
		操作员编号	2	无量纲	0AH～0BH	HEX
		写卡时间	4	年、月、日、时	0CH～0FH	BCD
		卡有效日期	3	年、月、日	10H～12H	BCD
		校验和	1	无量纲	13H	HEX
		保留	4		14H～17H	HEX
	设置信息区	本次购买量	3	分(或m^3或kWh)	18H～1AH	HEX
		购买次数	2	无量纲	1BH～1CH	HEX
		参数版本号	1	无量纲	1DH	HEX
		允许囤积量	4	分(或m^3或kWh)	1EH～21H	HEX
		关阀报警量	2	分(或m^3或KWh)	22H～23H	HEX
		显示报警量	2	分(或m^3或kWh)	24H～25H	HEX
		允许透支量	2	分(或m^3或kWh)	26H～27H	HEX
		单价版本号	1	无量纲	28H	HEX
		阶梯限量1或结算周期	2	m^3(kWh)/m或m	29H～2AH	HEX
		阶梯限量2或交费时间	2	m^3(kWh)/m或d	2BH～2CH	HEX

表 12(续)

分区名称		数据项名称	长度 Byte	单位	相对地址	数据格式
应用分区 1（首址 A_0）	设置信息区	阶梯限量 3 或 m 起算时间	2	m^3(kWh)/m 或 d	2DH～2EH	HEX
		常规单价	3	分/m^3 或 kWh	2FH～31H	HEX
		第 1 阶单价	3	分/m^3 或 kWh	32H～34H	BCD
		第 2 阶单价	3	分/m^3 或 kWh	35H～37H	BCD
		第 3 阶单价	3	分/m^3 或 kWh	38H～3AH	BCD
		密钥版本号	1	无量纲	3BH	HEX
		密文密钥 1	24	无量纲	3CH～53H	HEX
		密文密钥 2	24	无量纲	54H～6BH	HEX
		密文密钥 3	24	无量纲	6CH～83H	HEX
		检验数据	4	无量纲	84H～87H	HEX
		校验和	1	无量纲	88H	HEX
		保留	4		89H～8CH	
	返回信息区	累计充值量	4	m^3 或 kWh	8DH～90H	HEX
		充值次数	1	无量纲	91H	HEX
		累计用量	4	m^3 或 kWh	92H～95H	HEX
		剩余量	3	分/m^3 或 kWh	96H～98H	HEX
		表具故障状态	1	无量纲	99H	HEX
		最近 12 个月用量	24	m^3 或 kWh/m	9AH～0B1H	HEX
		异常次数	1	无量纲	0B2H	HEX
		最后异常发生日期	4	年、月、日、时	0B3H～0B6H	BCD
		采集时间日期	5	年、月、日、时、分	0B7H～0BBH	BCD
		表具程序版本号	2	无量纲	0BCH～0BDH	BCD
		厂商代码	3	无量纲	OBEH～0C0H	HEX
		校验和	1	无量纲	0C1H	HEX
……	……	……	……		……	……

7.2.1.2 数据加密及解密

逻辑加密卡存放的密文，应由 ISAM 卡中的加密密钥对明文数据加密并由 ESAM 内的解密密钥对数据解密后，进行处理。

返写数据区存放的密文，应由 ESAM 加密密钥完成数据的加密。解密密钥应与 ISAM 卡中的解密密钥应对应。

7.2.2 修改/恢复密钥卡

7.2.2.1 文件结构定义

逻辑加密卡表具类修改/恢复密钥卡文件结构应符合表 13 的规定。

表 13 逻辑加密卡表具类修改/恢复密钥卡文件结构

	0H	1H	2H	3H	4H	5H	6H	7H	8H	9H	AH	BH	CH	DH	EH	FH
0H	保留															
1H	起始码	命令码	长度	用户号					密钥条数	逻辑加密卡解密						
2H	密钥密文									逻辑加密卡加密						
3H	密钥密文								校验和	结束码	保留区					
4H	保留区															
5H																
6H																
7H																
8H																
9H																
AH																
BH	返写数据区															
CH																
DH																
EH																
FH	保留															

7.2.2.2 密钥修改及恢复

逻辑加密卡存放修改密钥的密文，应由 ESAM 主控密钥加密。从起始码到结束码存放的是由加密密钥加密的数据密文，应由 ESAM 解密密钥解开后并将密钥密文传给 ESAM，进行密钥更新。

返写数据区存放的密文，应由 ESAM 加密密钥完成数据的加密。解密密钥应与 ISAM 卡中的解密密钥应对应。

7.2.3 ESAM 模块文件结构

逻辑加密卡表具 ESAM 模块文件结构应符合表 14 的规定。

表 14 逻辑加密卡表具 ESAM 模块文件结构

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
EF1	参数信息二进制文件	0001
EF2	表具运行参数信息文件	0002
EF3	购量钱包文件	0003

7.2.3.1 密钥体系(MKF)

逻辑加密卡表具类 ESAM 模块密钥体系应符合表 15 的规定。

表 15 逻辑加密卡表具类 ESAM 模块密钥体系

标识	名称
00	主控密钥
01	钱包交易计算密钥
02	购量文件计算密钥
03	返写文件计算密钥
04	相互内部认证密钥
05	ESAM 外部认证密钥
06	用户卡外部认证
07	逻辑加密卡解密密钥
08	逻辑加密卡加密密钥

注 1：主控密钥为该系统中的密钥线路保护密钥。

注 2：钱包交易计算密钥用于对购量钱包文件进行增款操作，与用户卡配对使用。

注 3：返写文件计算密钥用于对用户卡返写二进制文件进行控制，认证通过后可以将表内信息返写到用户卡中，与用户卡配对使用。

注 4：相互内部认证主密钥用于比较各种卡与 ESAM 是否为同一系统发行的。

7.2.3.2 参数信息二进制文件

逻辑加密卡表具 ESAM 模块参数信息二进制文件应符合表 16 的规定。

表 16 逻辑加密卡表具 ESAM 模块参数信息二进制文件

偏移量	数据项	长度	说明
00H	起始码	1	68H
01H	命令码	1	00H
02H	长度	1	HEX
03H～04H	系统序列号	2	HEX
05H～09H	户号	5	HEX
0AH～0EH	表号	5	HEX
0FH	卡序号	1	HEX
10H～13H	阶梯一费率	4	HEX
14H～17H	阶梯二费率	4	HEX
18H～1BH	阶梯三费率	4	HEX
1CH～1FH	阶梯四费率	4	HEX
20H～23H	报警量 1(金额)	4	HEX
24H～27H	报警量 2(金额)	4	HEX
28H～2BH	囤积量(金额)	4	HEX
2CH～2EH	预留	3	HEX
2FH	预留	1	HEX
30H	预留	1	HEX
31H	预留	1	HEX
32H	预留	1	HEX
33H～36H	预留	4	HEX
37H	校验和	1	HEX
38H	结束码	1	HEX

7.2.3.3 表具运行信息二进制文件

逻辑加密卡表具ESAM模块运行信息二进制文件应符合表17的规定。

表17 逻辑加密卡表具ESAM模块运行信息二进制文件

偏移量	数据项	长度	说明
00H	起始码	1	68H
01H	命令码	1	00H
02H	长度	1	HEX
03H～06H	剩余量(金额)	4	HEX
07H～AH	累计购量(金额)	4	HEX
BH～EH	本次购量(金额)	4	HEX
FH～10H	购买次数	2	HEX
11H～14H	累计用量	4	HEX
15H～18H	阶梯用量一	4	HEX
19H～1CH	阶梯用量二	4	HEX
1DH～20H	阶梯用量三	4	HEX
21H～24H	阶梯用量四	4	HEX
25H～28H	过零量(金额)	4	HEX
29H～2CH	上月末冻结总量	4	HEX
2DH～30H	报警量1(金额)	4	HEX
31H～34H	报警量2(金额)	4	HEX
35H～38H	囤积量(金额)	4	HEX
39H～3BH	预留	3	HEX
3CH	预留	1	HEX
3DH	预留	1	HEX
3EH	非法插卡次数	1	HEX
3FH	校验和	1	HEX
40H	结束码	1	HEX

7.2.3.4 剩余量钱包

逻辑加密卡表具ESAM模块剩余量钱包文件应符合表18的规定。

表18 逻辑加密卡表具ESAM模块剩余量钱包文件

偏移量	数据项	长度	说明
00H～03H	剩余量(金额)	4	HEX
04H～05H	购买次数	2	HEX

7.3 安全认证测试

7.3.1 使用修改密钥卡

7.3.1.1 测试流程

修改密钥卡测试流程见图1。

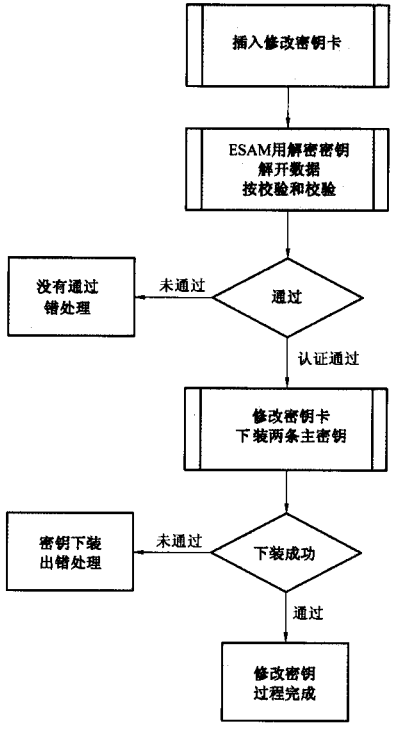

图 1　修改密钥卡测试流程图

a) 在表具终端中装入正确的 ESAM；

b) 用错误密文数据的修改密钥卡进行修改密钥操作，该表具终端应报错；

c) 用缺少主密钥的修改密钥卡进行修改密钥操作，该表具终端应报错；

d) 用正确的修改密钥卡进行修改密钥操作，该表具终端应报成功。

7.3.1.2　ESAM 验证修改密钥卡

a) 读取卡中的密文数据，由解密密钥解开密文数据；

b) 验证数据的有效性，表具终端计算校验码与卡给出的校验码进行比较，相同则数据的有效性通过，不相同则数据的有效性不通过。

7.3.1.3　修改密钥卡下装主密钥

正式主密钥在 ESAM 主控密钥的保护下，以密文的方式写到 ESAM 卡中：

a) 读出要更新的正式密钥密文；

b) 向 ESAM 发更新密钥指令：命令头＋正式密钥密文；

c) ESAM 用 ESAM 主控密钥解密，将正式密钥明文写到密钥文件中。

7.3.2 使用恢复密钥卡

7.3.2.1 测试流程

恢复密钥卡测试流程见图 2。

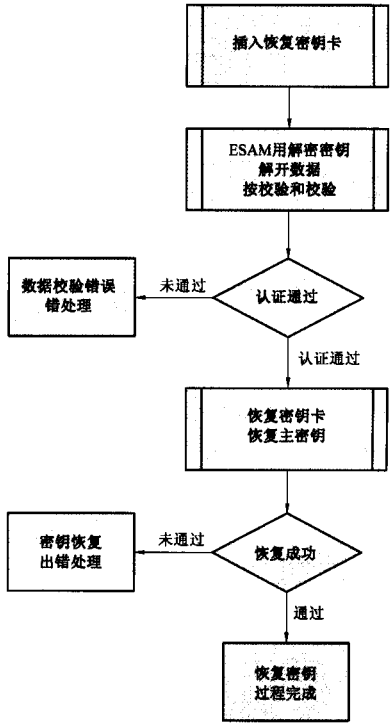

图 2 恢复密钥卡测试流程图

a) 在表具终端中装入正确的 ESAM；

b) 读出并记录充值前数据；

c) 用密文数据错误的充值卡进行充值操作，该表具终端应报错；

d) 用正确的充值卡进行充值操作，该表具终端应报成功；

e) 读取充值后数据，检查表具显示是否正常。

7.3.2.2 ESAM 验证恢复密钥卡

ESAM 验证恢复密钥卡：

a) 读取卡中的密文数据，由解密密钥解开密文数据；

b) 验证数据的有效性，终端计算校验码与卡给出的校验码进行比较。相同则数据的有效性通过，不相同则数据的有效性不通过。

7.3.2.3 恢复密钥卡下装主密钥

初始的主密钥在 ESAM 主控密钥的保护下，以密文的方式写到 ESAM 卡中；

a) 读出要更新的初始密钥密文；

b) 向 ESAM 发更新密钥指令：命令头＋初始密钥密文；

c) ESAM 用 ESAM 主控密钥解密，将初始密钥明文写到密钥文件中。

7.4 交易过程测试

充值密钥卡测试流程见图 3。

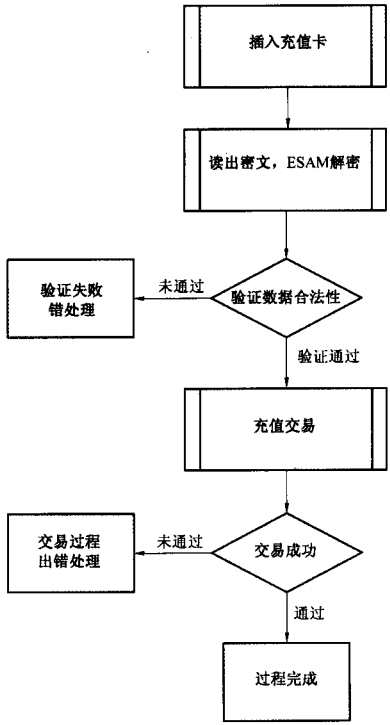

图 3 充值密钥卡测试流程图

a) 在表具终端中装入正确的 ESAM；

b) 表具终端读入充值卡数据，ESAM 对数据进行解密；

c) ESAM 对解密的数据验证其合法性；

d) 验证数据合法后充值，否则表具终端应报错；

e) 终端应显示充值交易过程完成。

7.5 表具测试流程

7.5.1 测试流程

逻辑加密卡表具测试流程见图 4。

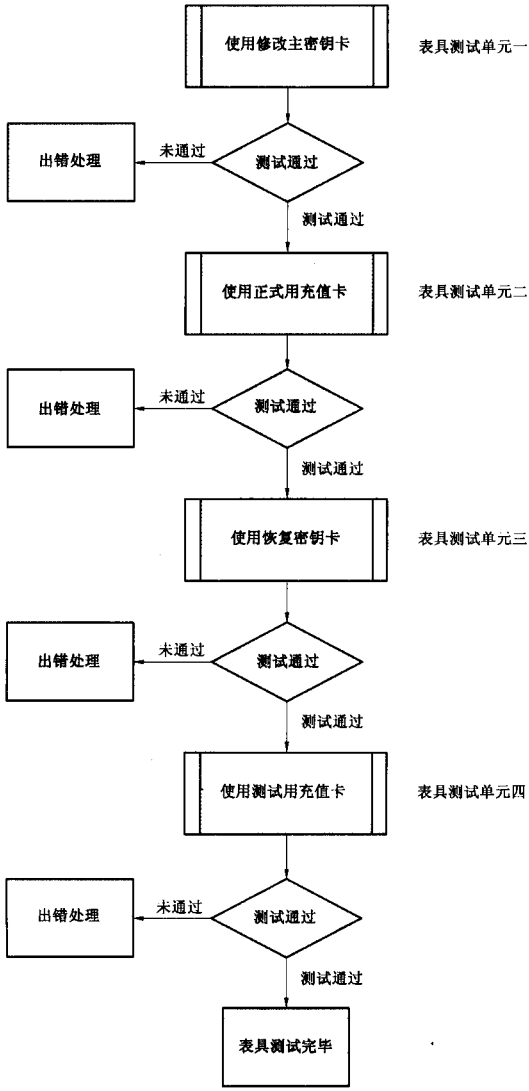

图 4　逻辑加密卡表具测试流程图

a）　表具测试单元二使用的充值卡是正式充值卡；

b）　表具测试单元四使用的充值卡是测试充值卡。

8 CPU卡表具类终端应用检测

为了提高建设事业领域三表应用系统的安全性和规范性的要求，需要在三表行业应用推广使用ESAM安全模块，主要检测IC卡表具的安全认证流程和交易流程。

8.1 检测卡种类

检测卡种类可分为：

a) 正式用充值卡，用正式密钥增加购买量的充值卡；

b) 检测用充值卡，用于检测实验阶段增加购买量；

c) 修改密钥卡，用于正式运行前下装正式密钥；

d) 恢复密钥卡，用于将密钥恢复成检测状态的公开密钥；

e) ESAM卡，用于表具的安全认证和存储数据。

8.2 文件结构

8.2.1 充值卡文件结构

CPU卡表具充值卡文件结构应符合表19的规定。

表19 CPU卡表具充值卡文件结构

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
DF01	表具应用目录文件	3F01
DKF	表具应用密钥文件	0000
EF1	维护卡指令信息文件	0001

8.2.1.1 密钥体系

CPU卡表具充值卡密钥体系应符合表20的规定。

表20 CPU卡表具充值卡密钥体系

标识	名称
00	主控密钥
01	购买文件计算密钥
02	返写文件计算密钥
03	表具内部认证密钥
04	ESAM外部认证密钥
05	用户卡外部认证

8.2.1.2 充值卡信息文件

CPU卡表具充值卡信息文件应符合表21的规定。

表21 CPU卡表具充值卡信息文件

偏移量	数据项	长度	说明
00H	起始码	1	68H
01H	命令码	1	12H
02H	长度	1	HEX
03H～07H	户号	5	HEX

表 21(续)

偏移量	数据项	长度	说明
08H～BH	增加量(金额)	4	HEX
CH～DH	购买次数	2	HEX
EH	校验和	1	HEX
FH	结束码	1	16H

8.2.2 修改/恢复密钥卡

CPU 卡表具修改/恢复密钥卡文件结构应符合表 22 的规定。

表 22 CPU 卡表具修改/恢复密钥卡文件结构

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
DF01	表具应用目录文件	3F01
DKF	表具应用密钥文件	0000
EF1	主密钥信息文件	0001

8.2.2.1 修改/恢复密钥卡密钥

CPU 卡表具修改/恢复密钥卡密钥应符合表 23 的规定。

表 23 CPU 卡表具修改/恢复密钥卡密钥

标识	名称	说明
01	相互内部认证主密钥	密钥修改的认证密钥用来对 ESAM 上密钥的更改权进行控制,与 ESAM 配对使用

8.2.2.2 主密钥信息文件

CPU 卡表具修改/恢复密钥卡主密钥信息文件应符合表 24 规定。

表 24 CPU 卡表具修改/恢复密钥卡主密钥信息文件

偏移量	数据项	长度	说明
00H	起始码	1	68H
01H	命令码	1	10H
02H	长度	1	AEH
03H～07H	户号	5	06H
08H	密钥条数	1	HEX
09H～20H	新购买文件计算密钥密文	12	HEX
21H～38H	新内部认证密钥密文	18	HEX
39H～50H	新返写文件计算密钥密文	12	HEX
51H～68H	新钱包交易认证密钥密文	18	HEX
69H～80H	新用户卡外部认证密钥密文	12	HEX
81H～98H	新 ESAM 外部认证密钥密文	18	HEX
99H	校验和	1	HEX
9Ah	结束码	1	16H

8.2.3 ESAM 模块文件结构

CPU 卡表具 ESAM 模块文件结构应符合表 25 的规定。

表 25 CPU 卡表具 ESAM 模块文件结构

文件	内容说明	标识
MF	主文件	3F00
MKF	主密钥文件	0000
EF1	参数信息二进制文件	0001
EF2	表具运行参数信息文件	0002
EF3	购量钱包文件	0003

8.2.3.1 ESAM 模块密钥体系(MKF)

CPU 卡表具 ESAM 模块密钥体系应符合表 26 的规定。

表 26 CPU 卡表具 ESAM 模块密钥体系

标识	名称
00	主控密钥
01	钱包交易计算密钥
02	购量文件计算密钥
03	返写文件计算密钥
04	相互内部认证密钥
05	ESAM 外部认证密钥
06	用户卡外部认证

注 1：主控密钥为该系统中的密钥线路保护密钥。

注 2：钱包交易计算密钥用于对购量钱包文件进行增款操作，与用户卡配对使用。

注 3：返写文件计算密钥用于对用户卡返写二进制文件进行控制，认证通过后可以将表内信息返写到用户卡中，与用户卡配对使用。

注 4：相互内部认证主密钥用于比较各种卡与 ESAM 是否为同一系统发行的。

8.2.3.2 参数信息二进制文件

CPU 卡表具 ESAM 模块参数信息二进制文件应符合表 27 的规定。

表 27 CPU 卡表具 ESAM 模块参数信息二进制文件

偏移量	数据项	长度	说明
00H	起始码	1	68H
01H	命令码	1	00H
02H	长度	1	HEX
03H～04H	系统序列号	2	HEX
05H～09H	户号	5	HEX
0AH～0EH	表号	5	HEX
0FH	卡序号	1	HEX
10H～13H	阶梯二费率	4	HEX
14H～17H	阶梯二费率	4	HEX

表 27(续)

偏移量	数据项	长度	说明
18H～1BH	阶梯三费率	4	HEX
1CH～1FH	阶梯四费率	4	HEX
20H～23H	报警量 1(金额)	4	HEX
24H～27H	报警量 2(金额)	4	HEX
28H～2BH	囤积量(金额)	4	HEX
2CH～2EH	预留	3	HEX
2FH	预留	1	HEX
30H	预留	1	HEX
31H	预留	1	HEX
32H	预留	1	HEX
33H～36H	预留	4	HEX
37H	校验和	1	HEX
38H	结束码	1	HEX

8.2.3.3 表具运行信息二进制文件

CPU 卡表具 ESAM 模块表具运行信息二进制文件应符合表 28 的规定。

表 28 CPU 卡表具 ESAM 模块表具运行信息二进制文件

偏移量	数据项	长度	说明
00H	起始码	1	68H
01H	命令码	1	00H
02H	长度	1	HEX
03H～06H	剩余量(金额)	4	HEX
07H～AH	累计购量(金额)	4	HEX
BH～EH	本次购量(金额)	4	HEX
FH～10H	购买次数	2	HEX
11H～14H	累计用量	4	HEX
15H～18H	阶梯用量一	4	HEX
19H～1CH	阶梯用量二	4	HEX
1DH～20H	阶梯用量三	4	HEX
21H～24H	阶梯用量四	4	HEX
25H～28H	过零量(金额)	4	HEX
29H～2CH	上月末冻结总量	4	HEX
2DH～30H	报警量 1(金额)	4	HEX
31H～34H	报警量 2(金额)	4	HEX
35H～38H	囤积量(金额)	4	HEX
39H～3BH	预留	3	HEX
3CH	预留	1	HEX
3DH	预留	1	HEX

表 28(续)

偏移量	数据项	长度	说明
3EH	非法插卡次数	1	HEX
3FH	校验和	1	HEX
40H	结束码	1	HEX

8.2.3.4 剩余量钱包文件

CPU 卡表具 ESAM 模块剩余量钱包文件应符合表 29 的规定。

表 29 CPU 卡表具 ESAM 模块剩余量钱包文件

偏移量	数据项	长度	说明
00H～03H	剩余量(金额)	4	HEX
04H～05H	购买次数	2	HEX

8.3 安全认证测试

8.3.1 使用修改密钥卡

8.3.1.1 测试流程

修改密钥卡测试流程图(CPU 卡)见图 5。

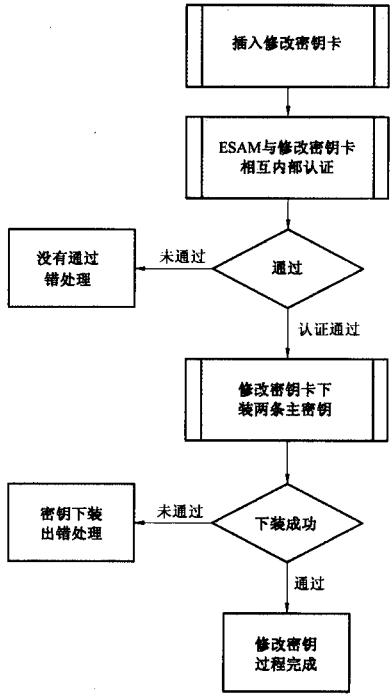

图 5 修改密钥卡测试流程图(CPU 卡)

a) 在表具终端中装入正确的 ESAM；

b) ESAM 与修改密钥卡相互内部认证，如果认证出错该表具终端应报错；

c) 正式主密钥在 ESAM 主控密钥的保护下，以密文的方式写到 ESAM 卡，如果出错该表具终端应报错；

d) 修改密钥卡进行修改密钥操作完成后，该表具终端应报成功。

8.3.1.2 ESAM 与修改密钥卡相互内部认证

ESAM 与修改密钥卡相互内部认证：

a) 取修改密钥卡随机数，返回 8 字节随机数；

b) 修改密钥卡内部认证，返回 8 字节密文；

c) ESAM 卡内部认证，返回 8 字节密文；

d) 判断两个密文是否相同，相同则内部认证通过，不相同则内部认证不通过。

8.3.1.3 修改密钥卡下装主密钥

正式主密钥在 ESAM 主控密钥的保护下，以密文的方式写到 ESAM 卡中：

a) 读出要更新的正式密钥密文；

b) 向 ESAM 发更新密钥指令：命令头＋正式密钥密文；

c) 用 ESAM 主控密钥解密，将正式密钥明文写到密钥文件中。

8.3.2 使用恢复密钥卡

8.3.2.1 测试流程

恢复密钥卡测试流程见图 6。

a) 在表具终端中装入正确的 ESAM；

b) ESAM 与恢复密钥卡相互内部认证，如果认证出错该表具终端应报错；

c) 初始的主密钥在 ESAM 主控密钥的保护下，以密文的方式写到 ESAM 卡中，如果出错该表具终端应报错；

d) 恢复密钥卡进行修改密钥操作完成后，该表具终端应报成功。

8.3.2.2 ESAM 与恢复密钥卡相互内部认证

ESAM 与恢复密钥卡相互内部认证：

a) 取恢复密钥卡随机数，返回 8 字节随机数；

b) 恢复密钥卡内部认证，返回 8 字节密文；

c) ESAM 卡内部认证，返回 8 字节密文；

d) 判断两个密文是否相同，相同则内部认证通过，不相同则内部认证不通过。

8.3.2.3 恢复密钥卡下装主密钥

初始的主密钥在 ESAM 主控密钥的保护下，以密文的方式写到 ESAM 卡中：

a) 读出要更新的初始密钥密文；

b) 向 ESAM 发更新密钥指令：命令头＋初始密钥密文；

c) 用 ESAM 主控密钥解密，将初始密钥明文写到密钥文件中。

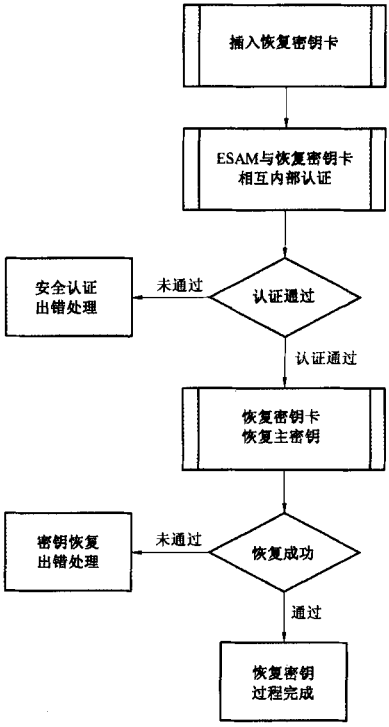

图 6 恢复密钥卡测试流程图(CPU 卡)

8.4 交易过程测试

充值密钥卡(CPU 卡)测试流程见图 7。

a) 在表具终端中装入正确的 ESAM;

b) ESAM 与充值卡相互内部认证,如果认证出错该表具终端应报错;

c) ESAM 与充值卡外部认证,如果认证出错该表具终端应报错;

d) 外部认证成功后,进行充值交易处理,该表具终端提示充值卡交易过程完。

8.4.1 ESAM 与充值卡相互内部认证

ESAM 与充值卡相互内部认证:

a) 取修改密钥卡随机数,返回 8 字节随机数;

b) 修改密钥卡内部认证,返回 8 字节密文;

c) ESAM 卡内部认证,返回 8 字节密文;

d) 判断两个密文是否相同,相同则内部认证通过,不相同则内部认证不通过。

8.4.2 ESAM 外部认证

ESAM 外部认证:

a) 取 ESAM 随机数,返回 8 字节随机数;

b) 充值卡内部认证，返回 8 字节密文；

c) ESAM 验证 8 字节密文。

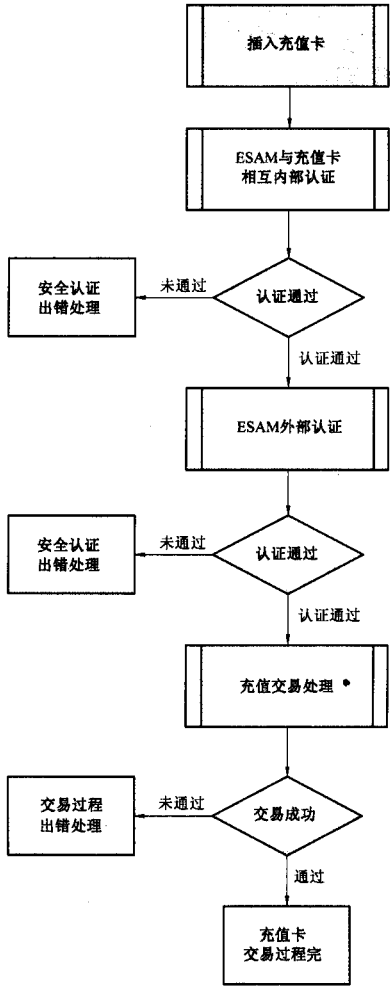

图 7 充值密钥卡测试流程图(CPU 卡)

8.5 表具测试流程

表具测试流程图(CPU 卡)见图 8。

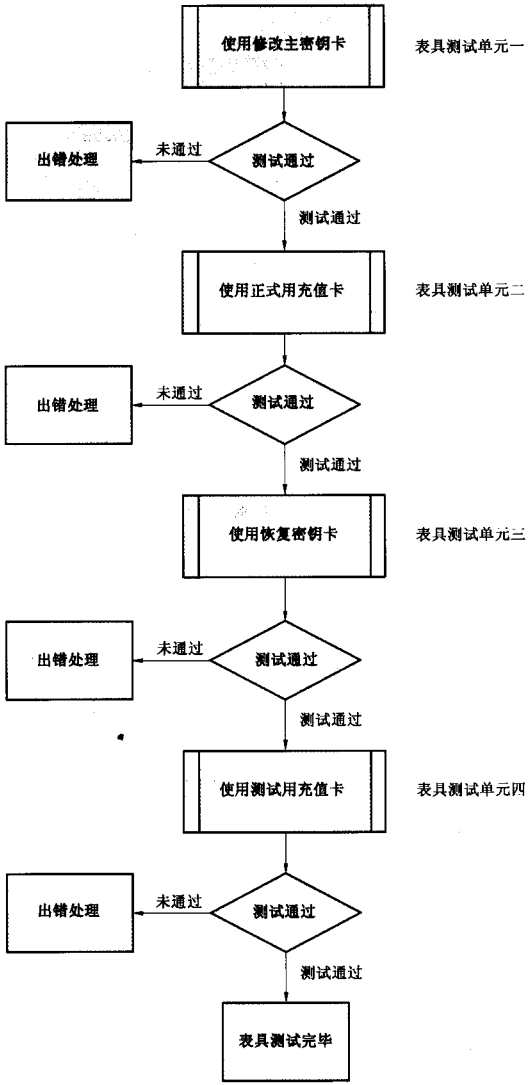

图 8　表具测试流程图(CPU 卡)

a)　表具测试单元二使用的充值卡是正式充值卡；

b)　表具测试单元四使用的充值卡是测试充值卡。

9 消费类及服务类 IC 卡终端应用检测

检测 IC 卡机具安全认证流程及交易流程的检测方法。

9.1 检测卡种类

检测卡按照卡功能类型分为用户卡、PSAM 卡和 ISAM 卡三种，ISAM 卡和 PSAM 卡在本次检测中均认为是可信的数据来源，根据卡中数据不同分为以下三种进行检测：

a) 数据正确，密钥正确，用于消费类及服务类 IC 卡终端检测正常认证和交易。该终端可以完成安全认证检测和所有交易流程检测；

b) 数据错误，密钥正确，用于消费类及服务类 IC 卡终端检测交易的限制条件判断。该终端可以完成部分安全认证检测，交易流程检测可以完成；

c) 数据正确，密钥错误，用于检测机具对密钥错误卡(非法卡)的处理。密钥错误还可以分为交易密钥错误其他密钥正确、所有密钥错误两种，检测机具交易过程中的错误处理。

9.2 用户卡的文件结构

用户卡文件结构见图 9。

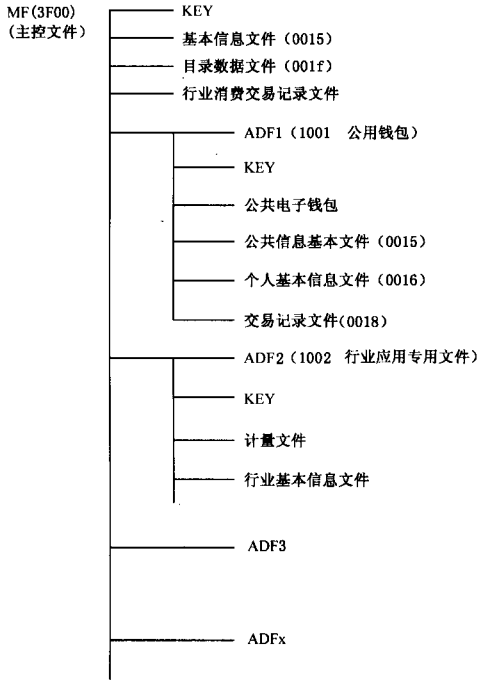

图 9 用户卡文件结构图

9.2.1 用户卡文件详细信息

消费类 CPU 用户卡文件详细信息应符合表 30 的规定。

表 30 消费类 CPU 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			
基本信息文件	二进制文件	0015	自由	安全信息
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			
公用基本信息文件	二进制文件	0015	自由	安全信息
个人基本信息文件	二进制文件	0016	自由	安全信息
公共电子钱包	专用钱包文件	专用指令		
交易记录文件	循环文件	0018	自由	

9.2.2 MF 主控文件内容

9.2.2.1 Key

消费类 CPU 卡用户卡 MF 主控文件的 KEY 应符合表 31 的规定。

表 31 消费类 CPU 卡用户卡 MF 主控文件的 KEY

密钥名称
主控密钥 DRTK
维护密钥
充值密钥组 1
充值密钥组 2
……
充值密钥组 5

9.2.2.2 基本信息文件

消费类 CPU 卡用户卡 MF 主控文件的基本信息文件应符合表 32 的规定。

表 32 消费类 CPU 卡用户卡 MF 主控文件的基本信息文件

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
1～6	发行点代码	6
7～14	发行点操作员代码	8
15～18	押金金额	4
19～20	自定义	2

9.2.2.3 目录数据文件

ADF1～ADFx：目录名或短文件标识符。

9.2.2.4 行业消费交易记录文件

消费类 CPU 用户卡 MF 主控文件的行业消费交易记录文件应符合表 33 的规定。

表 33 消费类 CPU 卡用户卡 MF 主控文件的行业消费交易记录文件

字段名	长度 Byte	备注
终端机编号	4	xx(行业代码)xxxxxx(序号)
交易日期时间	7	xxxx(年)xx(月)xx(日)xx(时)xx(分)xx(秒)
交易金额	3	xx(元)xx(角)xx(分)
现有余额	4	xx(元)xx(角)xx(分)
交易次数	2	HEX 码
交易计数器	2	HEX 码

9.2.3 ADF1 公用钱包专用文件内容

9.2.3.1 KEY

消费类 CPU 用户卡 ADF1 公用钱包专用文件的 KEY 文件应符合表 34 的规定。

表 34 消费类 CPU 用户卡 ADF1 公用钱包专用文件的 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 2
……
消费子密钥组 5
充值子密钥组 1
充值子密钥组 2
……
充值子密钥组 5
TAC 子密钥

9.2.3.2 公共基本信息文件

消费类 CPU 用户卡 ADF1 公用钱包专用文件的公共基本信息文件应符合表 35 的规定。

表 35 消费类 CPU 用户卡 ADF1 公用钱包专用文件的公共基本信息文件

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)
1～8	发卡方标识	8
9	启用标志	1
10	卡类别标识	1
11～20	应用序列号	10
21～24	启动日期	4
25～28	有效日期	4
29～30	发卡方自定义文件控制信息数据	2
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)＋应用代码(2 字节)＋卡发行流水号(4 字节)。		

卡类型标识是卡片类别(持卡人类别)信息,数据结构应符合表36的规定。

表36 消费类CPU用户卡卡类型标识数据结构

名称	长度/Byte	内容	数据格式
卡型	1	卡片类别号码	HEX

卡型编码应符合表37的规定。

表37 消费类CPU卡用户卡卡型编码表

卡型	代码(HEX)
管理卡	01
操作员卡	02
系统检测卡	63
成人卡	03～0A
纪念卡	0A～27
优惠卡	27～3B
员工卡	3C～45
记名卡	46～4F
其他	50～62

9.2.3.3 个人基本信息文件

消费类CPU用户卡ADF1公用钱包专用文件的个人基本信息文件应符合表38的规定。

表38 消费类CPU用户卡ADF1公用钱包专用文件的个人基本信息文件

文件标识(SFI)		16H
文件类型		二进制
文件大小		37H
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
23～54	持卡人证件号码	32
55	持卡人证件类型	1

9.2.3.4 消费类CPU用户卡卡类型标识数据结构金融电子钱包

消费类CPU用户卡ADF1公用钱包专用文件的金融电子钱包文件应符合表39的规定。

表39 消费类CPU用户卡ADF1公用钱包专用文件的金融电子钱包文件

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

9.2.3.5 交易记录文件

消费类CPU用户卡ADF1公用钱包专用文件的交易记录文件应符合表40的规定。

表 40 消费类 CPU 用户卡 ADF1 公用钱包专用文件的交易记录文件

文件标识(SFI)		18H
文件类型		循环记录
记录大小		18H×n(n≥5)
文件存取控制	读=自由	写=禁止
数据元	长度(字节)	备注
终端机编号	6	
交易日期时间	7	
交易金额	4	
交易类型	1	
现有余额	4	
交易序号	2	
说明:交易时间记录当次交易的时、分、秒,表示方法应符合 GB/T 7408 规定。		

交易类型:记录当次交易的交易类型,其表示方法应符合表 41 的规定。

表 41 消费类 CPU 卡用户卡交易类型表

编码	交易类型
01	月票
02	消费
03	提现
04	充值
05	圈存到公交月票
06	圈存到公园月票
07	圈存到轮渡月票
08	其他

9.2.4 ADF2～ADFx 行业应用专用文件内容

消费类 CPU 用户卡 ADF2～ADFx 行业应用专用文件内容应符合表 42 的规定。

表 42 消费类 CPU 用户卡 ADF2～ADFx 行业应用专用文件内容

密钥名称
应用主控
应用维护 DRTK
消费密钥组 1
消费密钥组 2
……
消费密钥组 5

9.3 ISAM 卡的文件结构

ISAM 卡文件结构见图 10。

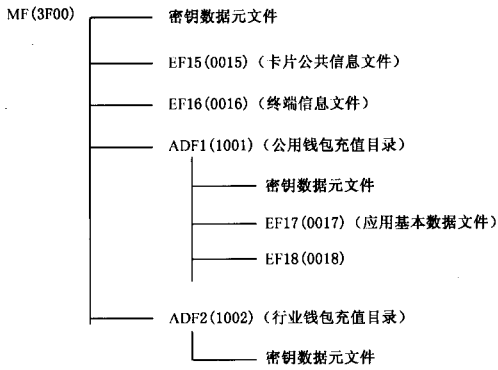

图 10　ISAM 卡文件结构图

9.3.1　ISAM 卡文件详细信息

消费类 ISAM 卡文件详细信息应符合表 43 的规定。

表 43　消费类 ISAM 卡文件详细信息

文件名称	文件类型	文件标识符	文件长度（HEX）	操作权限	
MF		3F00			
密钥数据元文件					
卡片公共信息	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	二进制文件	0017	0019	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	二进制文件	0017	0019	读＝自由	写＝需要安全信息

9.3.2　MF 下密钥数据元文件内容

ISAM 卡 MF 下密钥数据元文件内容应符合表 44 的规定。

表 44　ISAM 卡 MF 下密钥数据元文件内容

密钥名称
卡片主控密钥

9.3.3　ADF1 下密钥数据元文件内容

ISAM 卡 ADF1 下密钥数据元文件内容应符合表 45 的规定。

表 45 ISAM 卡 ADF1 下密钥数据元文件内容

密钥名称
应用主控密钥
公共钱包充值主密钥
PIN 解锁主密钥
重装 PIN 主密钥
TAC 主密钥

9.3.4 ADF2 下密钥数据元文件内容

ISAM 卡 ADF2 下密钥数据元文件内容应符合表 46 的规定。

表 46 ISAM 卡 ADF2 下密钥数据元文件内容

密钥名称
应用主控密钥
行业钱包充值主密钥
TAC 主密钥

9.4 PSAM 卡的文件结构

PSAM 卡文件结构见图 11。

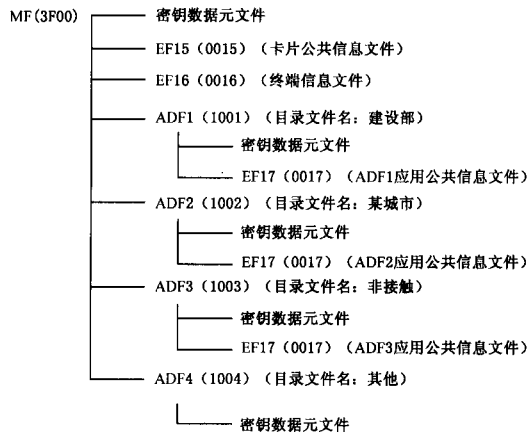

图 11 PSAM 卡文件结构图

9.4.1 PSAM 卡文件详细信息

PSAM 卡文件详细信息应符合表 47 的规定。

表 47 PSAM 卡文件详细信息

文件名称	文件类型	文件标识符	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
卡片公共信息文件	二进制文件	0015		
终端信息文件	二进制文件	0016		
ADF1		1001		
密钥数据元文件	二进制文件			
应用公共信息	二进制文件	0017	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	二进制文件	0017	读＝自由	写＝需要安全信息
ADF3		1003		
密钥数据元文件	二进制文件			
应用公共信息	二进制文件	0017	读＝自由	写＝需要安全信息
ADF4		1004		
密钥数据元文件	二进制文件			

9.4.2 MF 下密钥数据元文件内容

PSAM 卡 MF 下密钥数据元文件内容应符合表 48 的规定。

表 48 PSAM 卡 MF 下密钥数据元文件内容

卡片主控密钥
卡片维护密钥

9.4.3 ADF1 下密钥数据元文件内容

PSAM 卡 ADF1 下密钥数据元文件内容应符合表 49 的规定。

表 49 PSAM 卡 ADF1 下密钥数据元文件内容

密钥名称
应用主控密钥
应用维护密钥
公用钱包消费主密钥
用户卡应用维护主密钥
TAC 主密钥

9.4.4 ADF2 下密钥数据元文件内容

PSAM 卡 ADF2 下密钥数据元文件内容应符合表 50 的规定。

表 50 PSAM 卡 ADF2 下密钥数据元文件内容

密钥名称
应用主控密钥
应用维护密钥
行业消费主密钥
用户卡应用维护主密钥
TAC 主密钥

9.4.5 ADF3 下密钥数据元文件内容

PSAM 卡 ADF3 下密钥数据元文件内容应符合表 51 的规定。

表 51 PSAM 卡 ADF3 下密钥数据元文件内容

密钥名称
应用主控密钥
应用维护密钥
逻辑加密卡消费主密钥
用户卡应用维护主密钥
TAC 主密钥

9.4.6 ADF4 下密钥数据元文件内容

PSAM 卡 ADF4 下密钥数据元文件内容应符合表 52 的规定。

表 52 PSAM 卡 ADF4 下密钥数据元文件内容

密钥名称
应用主控密钥

9.5 安全认证测试

安全认证测试流程见图 12。

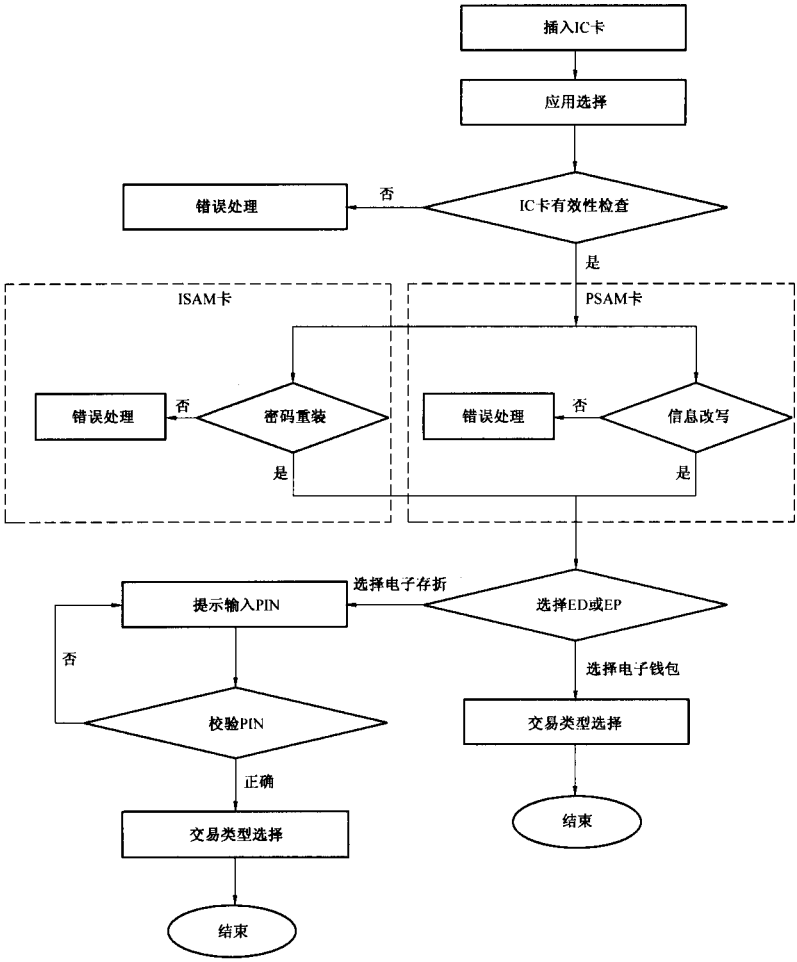

图 12　安全认证测试流程图

9.5.1 **插卡判断**

终端判断是否插入 ISAM 卡和用户卡并进行提示。

9.5.2 **应用选择**

判断卡片为异地卡还是本地卡，异地卡选择全国通用电子钱包应用目录，本地卡选择相应的行业应用目录；卡中数据错误则进行相应提示退出认证测试。

9.5.3 **防拔处理**

终端在处理 IC 卡交易时，卡被突然拔出或由于终端方面的原因突然停止操作（如发生断电），则终端应能根据 JR/T 0025—2005 第 2 部分：应用规范中的规定，当终端检测到卡被拔出又重新被插入或检测到终端恢复供电后应对卡实施防拔处理。

在以上情况下，终端应进入这样一种状态：即持卡人应重新插入原来的 IC 卡，并确认最后一次交易已经完成。如果持卡人未插入 IC 卡，则终端应提示持卡人重新插入原来的 IC 卡。如果插入的卡不是原来的卡，则终端应提示持卡人重新插入原来的卡。终端还应能够自动或人工方式恢复到安全认证测试流程中。

9.5.4 **有效性检查**

根据应用选择返回的数据，依次进行以下判断：

a) 终端应判断该卡是否在的黑名单卡之列，若卡中数据错误则进行相应操作提示退出认证测试；

b) 终端应判断发卡方标识，若卡中数据错误则进行相应提示退出认证测试；

c) 终端应判断卡片应用是否在有效期内，判断起止日期，若卡中数据错误则进行相应提示退出认证测试。

9.5.5 **密钥验证**

9.5.5.1 **重装口令（ISAM 专用）**

通过 ISAM 卡中的重装 PIN 主密钥，计算得到用户卡 ADF1 中重装所需密文，向用户卡发送重装口令，重装成功证明密钥无误，若卡中返回错误则进行相应提示，并退出认证测试。

9.5.5.2 **个人信息文件更新（PSAM 专用）**

读取用户卡 ADF1 中个人信息文件，将读取的第一字节信息以线路保护方式写入卡中，测试用户卡应用维护密钥是否正确。通过 PSAM 卡中的应用维护主密钥，计算得到 MAC 值，向用户卡发送更新二进制文件指令，重装成功证明密钥无误，若卡中返回错误则进行相应提示，并退出认证测试。

装口令成功后，继续采用 ISAM 卡进行圈存交易测试。

个人信息文件更新成功后，继续采用 PSAM 卡进行消费交易测试。

9.6 **交易流程测试**

9.6.1 **充值（ISAM 卡专用）**

充值交易流程见图 13。

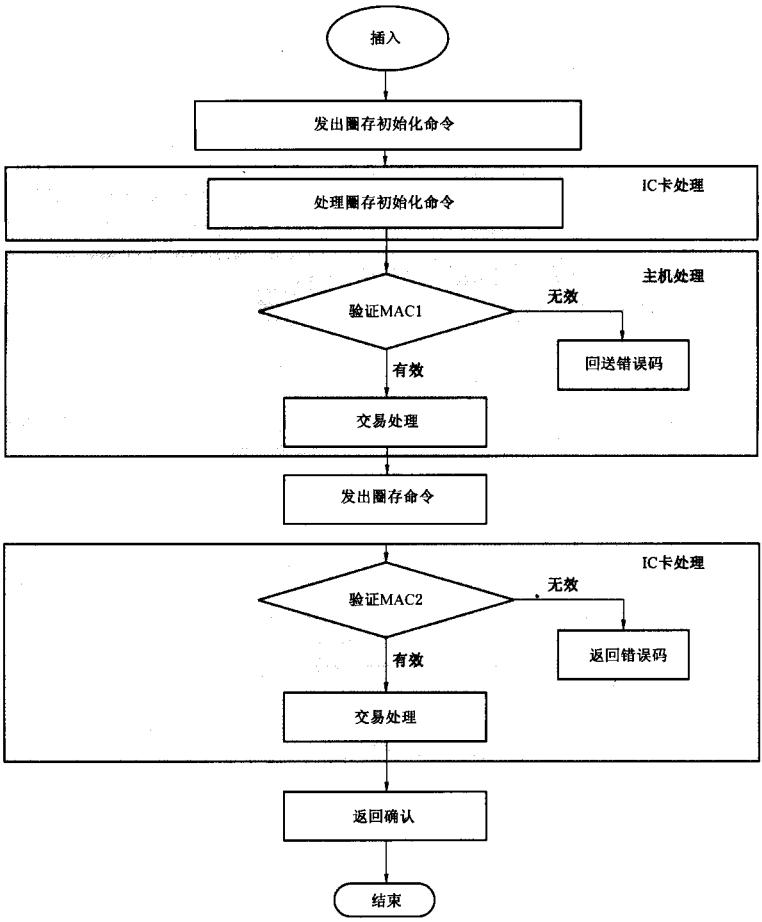

图 13　充值交易流程图

通过圈存交易，持卡人可将相应账户上的资金划入 ED/EP 中。这种交易必须在发卡方授权的终端上进行，并要求验证个人密码(PIN)。

9.6.1.1　发出圈存初始化命令

终端应发出圈存初始化命令启动圈存交易。

9.6.1.2　处理圈存初始化命令

收到圈存初始化命令后，IC 卡将进行以下操作：

检查是否支持命令中包含的密钥索引号。如果不支持，则回送状态码'9403'(不支持的密钥索引号)，但不回送任何其他数据，同时终止命令的处理过程。

产生一个伪随机数(ICC),过程密钥和一个报文鉴别码(MAC1),用以供 ISAM 验证圈存交易及 IC 卡的合法性。

过程密钥是用于 ED/EP 圈存交易的过程密钥。用来产生过程密钥的输入数据:伪随机数(ICC)||ED/EP 联机交易序号||'8000'。

用过程密钥对以下数据加密产生 MAC1(按所列顺序):

a) ED/EP 余额;

b) 交易金额;

c) 交易类型标识;

d) 终端机编号。

9.6.1.3 **验证 MAC1**

收到圈存初始化命令响应报文后,终端把相应报文的数据传给 ISAM 卡,ISAM 卡生成过程密钥并通过过程密钥计算 MAC1,比较结果是否与用户卡返回的 MAC1 一致。如果 MAC1 相同,交易处理将继续执行。否则,交易处理将回送错误状态并停止交易。

9.6.1.4 **回送错误状态**

如果不接受圈存交易,则终端应进行提示。

9.6.1.5 **交易处理**

在确认能够进行圈存交易后,终端记录从持卡人相应账户中扣减圈存金额。

由 ISAM 卡计算产生一个报文鉴别码(MAC2),用于 IC 卡对 ISAM 卡进行合法性检查。用过程密钥对以下数据加密产生 MAC2(按所列顺序):

a) 交易金额;

b) 交易类型标识;

c) 终端机编号;

d) 交易日期(主机);

e) 交易时间(主机)。

9.6.1.6 **发出圈存命令**

终端通过 ISAM 卡计算得到 MAC2 报文后,向用户卡发出圈存命令更新卡上 ED/EP 余额。

9.6.1.7 **验证 MAC2**

收到圈存命令后,用户卡必须确认 MAC2 的有效性。否则将向终端回送状态码'9302'(MAC 无效)。

9.6.1.8 **交易处理**

IC 卡将 ED/EP 联机交易序号加 1,并且把交易金额加在 ED/EP 的余额上。IC 卡必须成功地完成以上所有操作或者一个也不完成。

在 ED/EP 圈存交易中,IC 卡用以下数据组成的一个记录更新标准交易明细:

a) ED/EP 联机交易序号;

b) 交易金额;

c) 交易类型标识;

d) 终端机编号;

e) 交易日期(主机);

f) 交易时间(主机)。

TAC 的计算不采用过程密钥方式,它用 DTK 左右 8 位字节异或运算的结果对以下数据进行加密运算来产生(按所列顺序):

a) ED/EP 余额;

b) ED/EP 联机交易序号(加 1 前);

c) 交易金额；

d) 交易类型标识；

e) 终端机编号；

f) 交易日期(主机)；

g) 交易时间(主机)。

9.6.1.9 返回确认

IC卡通过圈存命令的响应报文将TAC回送给终端。终端通过ISAM卡中的TAC主密钥计算当前交易的TAC值，进行TAC验证。如果TAC正确，终端应提示圈存交易测试完成。

9.6.2 消费(PSAM卡专用)

9.6.2.1 脱机消费交易过程

脱机消费交易过程见图14。

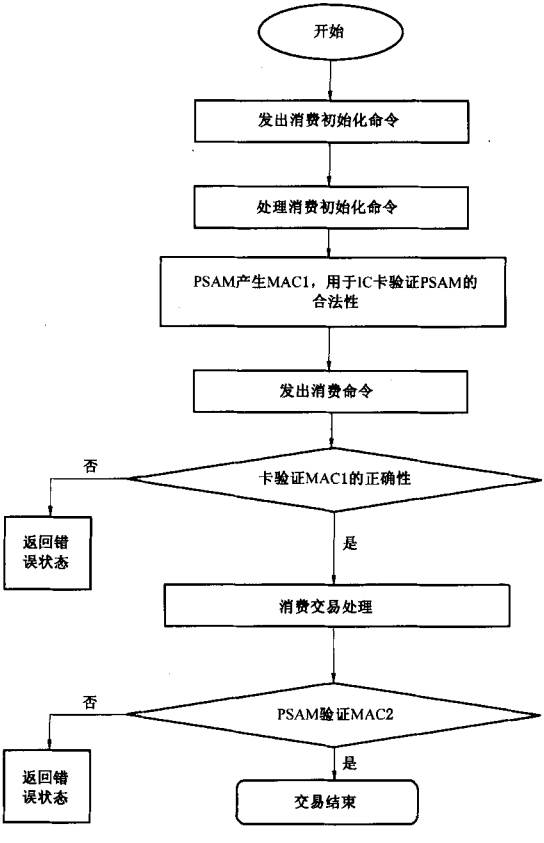

图 14 脱机消费交易过程图

9.6.2.2 IC卡处理消费初始化命令

IC卡处理消费初始化命令过程如下：

a) 检查是否支持命令中提供的密钥索引号，如果不支持则送回状态码'9403'；

b) 检查电子钱包/电子存折的余额是否大于或等于交易金额，如果小于交易金额，则送回状态码'9401'(金额不足)；

c) 通过以上的检查之后，IC卡将产生一个伪随机数和过程密钥来验证MAC1。

9.6.2.3 产生MAC1

PSAM卡依据选择该应用时回送的卡号分散出消费子密钥(即该张卡内的消费密钥)对卡回送的数据(4字节随机数+2字节脱机交易序号+终端交易序号的最右2字节)加密产生过程密钥，过程密钥对如下数据加密生成MAC1：

a) 交易金额；

b) 交易类型；

c) 终端交易序号；

d) 交易日期(终端)；

e) 交易时间(终端)。

9.6.2.4 消费/取现命令

终端发出消费/取现命令。

9.6.2.5 验证MAC1

卡片收到消费/取现命令后，IC卡用上述MAC1的产生过程相同的方法产生MAC1，IC卡将验证MAC1的有效性。如果MAC1无效，将向终端回送错误状态码'9302'(MAC无效)。MAC1有效，交易处理将执行9.6.2.6中所描述的步骤。

9.6.2.6 交易处理

IC卡从电子存折余额或电子钱包余额中扣减消费的金额，并将电子存折或电子钱包脱机交易序号加1。IC卡必须成功地完成以上所有步骤或者一个也不完成。只有余额和序号的更新均成功后，交易明细才可更新。

IC卡产生一个报文签别码(MAC2)供PSAM对其进行合法性检查，并通过消费/取现命令响应报文回送以下数据，作为PSAM产生MAC2的输入数据，用过程密钥对交易金额进行加密产生MAC2。

TAC的计算用DTK左右8位字节异或运算的结果对以下数据进行加密运算来产生(按所列顺序)。TAC将被写入终端交易明细，以便于主机进行交易验证。以明文形式通过消费/取现命令的响应报文从IC卡传送到终端：

a) 交易金额；

b) 交易类型标识；

c) 终端机编号；

d) 终端交易序号；

e) 交易日期(终端)；

f) 交易时间(终端)。

对于电子存折消费交易，IC卡将用以下数据组成的一个记录更新交易明细：

a) 交易金额；

b) 交易类型标识；

c) 终端机编号；

d) 终端交易序号；

e) 交易日期(终端)；

f) 交易时间(终端)。

9.6.2.7 **验证 MAC2**

PSAM 卡用相同的方法生成 MAC2，并与 IC 卡回送的 MAC2 相比较若不相同，PSAM 应给出一错误状态，终端应提示交易异常终止。若相同，终端应提示交易正常结束。