	文档编号	版本号	页数	密级
	CSC-6103	V3.1		

产品说明书

T5 一卡通系统

（仅供内部使用）

文档作者	GJM	日　　期	2016-11-05
审　　核		日　　期	
批　　准		日　　期	

赤松城（北京）科技有限公司

二〇一七年

文档修改履历

序号	日期	修改范围	新版本号	修改人
1	2016-11-05	初稿	V0.00	GJM
2	2016-11-7	增加了终端机与读卡器之间的通讯协议	V1.00	DZH
3	2016-11-11	增加了 ATS 命令和灰锁查询命令	V1.10	DZH
4	2016-11-24	完善了自定义协议，增加了使用举例	V1.20	DZH
5	2016-11--24	加入模块接口说明	V1.30	ZDP
6	2016-12-2	增加了灰锁处理指令，读写文件指令	V1.40	DZH
7	2016-12-5	增加了建议的操作流程	V1.50	DZH
8	2016-12-14	删减掉电子钱包功能，增加文件读写认证和交易前检测卡	V2.00	DZH
9	2016-12-19	汇总认证消费功能	V3.00	DZH
10	2016-12-19	修改产品名称，由“认证消费一卡通系统”改为“T5 一卡通系统”	V3.1	GJM

目 录

表目录

图目录

1 文档说明

本文档介绍了赤松城自主研发的一卡通系统平台的产品功能及使用范围，该平台集小额支付、身份识别、自助消费、快速通过等应用特点于一身，可为校园、企业量身订制员工卡（校园卡、学生卡）、密钥管理系统。

2 功能说明

赤松城一卡通系统主要分为以下几个部分。

1、 用户卡-兼容 7+1 CPU/M1 卡

2、 PSAM 卡—加密模块

3、 读卡器模块/整机-可选韦根接口，串口，USB 口

4、 用户卡/PSAM 卡发卡设备

5、 上位机发卡软件—可提供底层开发包，方便嵌入客户自行开发的应用环境

3 产品特性

- 高保密性 CPU 卡，内置多种加密算法， 需与 PSAM 安全模块配对使用才能读写数据；
- 用户资料管理：上位机支持 excel 文件管理，包括图片文件，可以方便的导入导出；
- 密钥管理：支持 excel 文件管理；
- 用户卡符合 ISO14443 Type A 标准；
- 80KFlash 空间，32KB 数据空间，兼容 M1 卡；
- 支持多应用，各应用之间相互独立，可建三级目录；
- 支持二进制文件、定长记录文件、不定长记录文件、循环文件、交易文件、安全文件；
- 支持 PBOC2.0 标准及建设部 IC 卡应用规范；
- Flash 满足 10 万次擦写指标；
- 数据有效期 10 年；
- 交易时间<350ms
- 卡工作温度 -25C ~ 70C
- 应用范围：门禁、食堂、超市、水电缴费、充电桩等

图 1 一卡通应用预览图

4 用户卡/PSAM 卡

4.1 国密一卡通用户卡

图 2 用户卡

个人用户的信息存储及密钥认证。

本系统的用户卡使用符合 ISO14443 协议的非接触 CPU 卡，内含国密 SM1 算法，M1 算法，由赤松城对其进行初始化，客户可以通过用户卡发卡设备配合发卡上位机对其进行个人化。用户自定义密钥，从上位机写入用户卡和 PSAM 卡，密钥一致的 PSAM 卡和用户卡配对使用。

4.2 国密一卡通 PSAM 卡

图 3 PSAM 卡

功能：密钥计算，与读卡设备配合使用

PSAM 卡插在内有读卡器的终端设备里面，用于认证过程的密钥计算，由赤松城对其进行初始化，客户可以通过 PSAM 卡发卡设备配合发卡上位机对其进行个人化。用户自定义密钥，从上位机写入用户卡和 PSAM 卡，密钥一致的 PSAM 卡和用户卡配对使用。

5 发卡设备

国密一卡通发卡器，用于赤松城国密一卡通系统用户卡和 PSAM 卡的发行。设备为 USB 接口的双界面读卡器，免驱动，支持 PCSC 规范。供电方式为 USB 供电，插入 PC 机，打开发卡上位机软件，进行信息输入即可写卡。

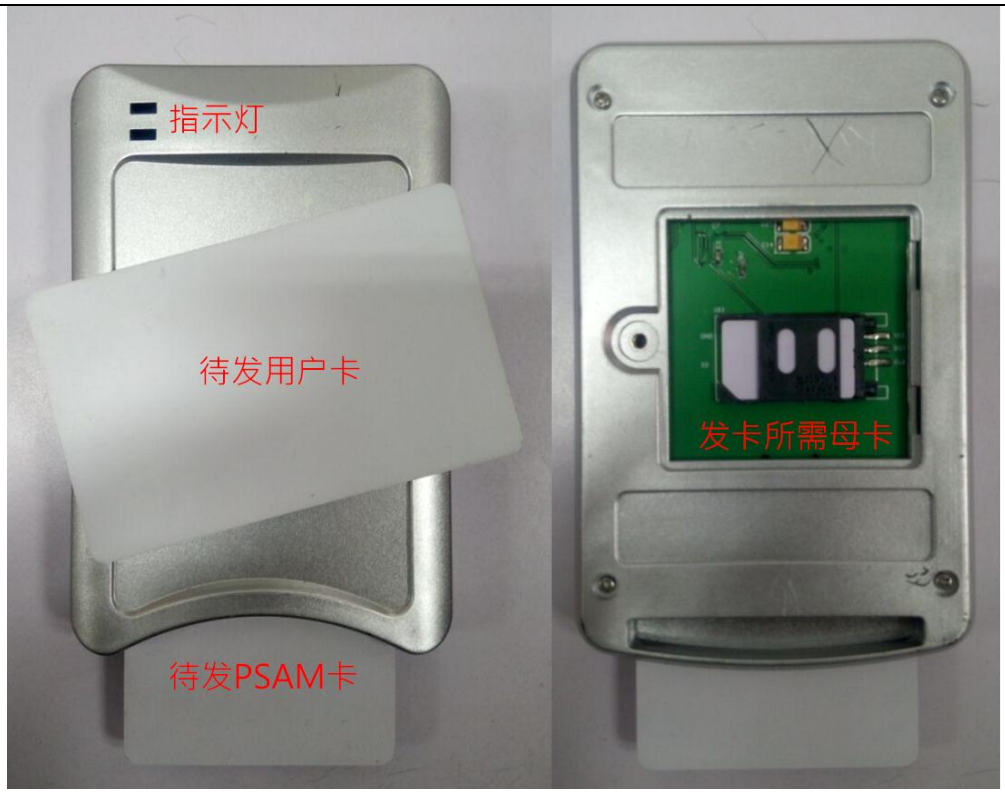

图 4 发卡设备

5.1 使用方法

背面放入发卡所需母卡，USB 线连接电脑，红色电源指示灯亮，等待发卡。

5.1.1 发用户卡

待发用户卡放入 RF 场内，绿色指示灯亮，操作发卡上位机软件进行发卡即可。

5.1.2 发 PSAM 卡

待发 PSAM 卡插入发卡器卡槽内（接触点朝下），绿色指示灯亮，操作发卡上位机软件进行发卡即可。

6 发卡软件

本公司可根据需要定制上位机界面，配合我司的发卡设备便可以对用户卡和 PSAM 卡进行个人化工作。以下介绍为门禁应用的一个上位机界面及使用。

6.1 特性

国密门禁卡发卡上位机软件配合国密门禁卡发卡器实现国密门禁用户卡和 PSAM 卡的发行。

- 符合 PCSC 规范，可以识别发卡设备，填写对应信息即可对用户卡和 PSAM 卡进行初始化。
- 区号：不大于 65535,，为韦根数据的前 2 个字节，PSAM 卡不需要写入此信息
- 卡号：不大于 65535，为韦根数据的后两个字节，PSAM 卡不需要写入此信息
- 密钥：国密密钥，16byte，128bit，用户卡和 PSAM 卡需要有相同的密钥，输入格式为 16 进制，长度必须为 32(两位代表一个字节，共 16 字节)。
- 持卡人信息：用户卡内存储的相关用户信息。可用 Load 进行导入，Save 进行保存。保存格式为 excel 文件。
- 支持自动写功能，卡拔出，插入下一张卡后可用自动将数据写入下一张卡。
- 支持卡号自动加一减一功能，每写完一张卡可进行对应操作。
- 支持 26bit/34bit 韦根数据，可切换正反向输出功能，即先输出卡号或先输出区号。

6.2 使用方法

PC 连接发卡器，运行发卡软件。

6.2.1 用户卡发卡

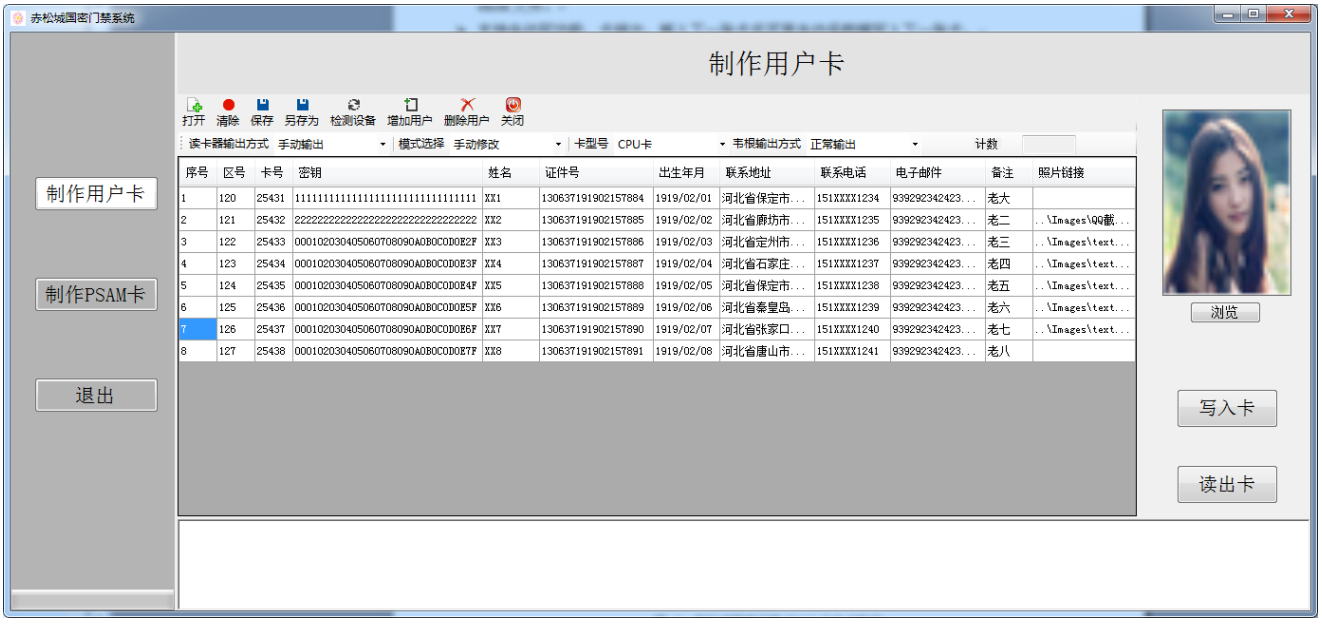

图 5 门禁用户卡发卡界面

菜单	
打开	打开已保存的用户信息表，格式.xls
清除	清除信息列表中的所有信息
保存	保存当前信息表，格式.xls
另存为	另存当前信息表，格式.xls
检测设备	检测发卡器设备，成功后才可进行发卡操作
增加用户	信息表中添加一行
删除用户	信息表中删除当前选择行
工具栏	
读卡器输出方式	手动：点击写入卡按钮写卡，自动：发卡器有卡进入时自动写卡
模式选择	手动：写卡完毕后当前选中行不变，加 1：写卡完毕后当前选中行下移一行，减 1：上移
卡型号	卡类型选择，目前仅 CPU 卡
韦根输出方式	正向：用户刷卡后，读卡器韦根接口输出顺序，区号(1A2B)-卡号(3C4D)，反向：卡号(4D3C)-区号(2B1A)
记数	发卡记数
用户信息表	
信息表	用户信息

表 1 门禁用户卡发卡界面说明

6.2.2 PSAM 卡发卡

图 6 门禁用户卡发卡界面

菜单	
检测设备	检测发卡器设备，成功后才可进行发卡操作
工具栏	
记数	发卡记数
PSAM 密钥	
PSAM 密钥	要写入的 PSAM 密钥

表 2 门禁用户卡发卡界面说明

7 读卡器/读头模块

模块共包含 3 组接口：1 个 2 脚电源接口 P1，1 个通信接口（串口）P2，1 个 6 脚 3FF 标准卡座。

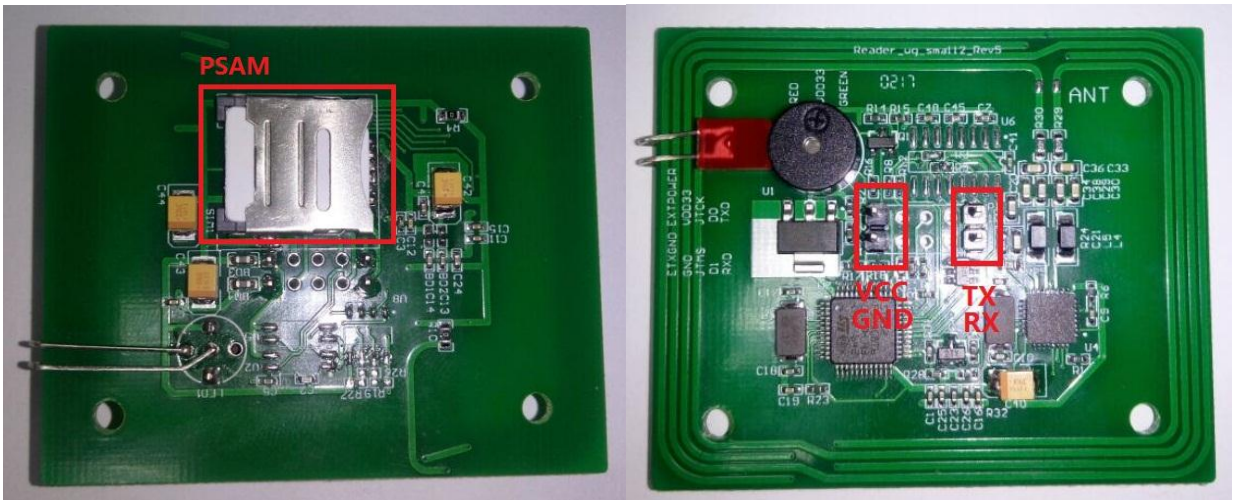

图 7 读卡器模块接口

P2	通信接口（串口，3.3V，兼容 5V）
TX	接终端数据发送端
RX	接终端数据接收端
P1	电源，5-9V
VCC	电源 正
GND	电源 负

表 3 读头接口定义

8 通讯协议

本部分主要介绍本公司开发的读卡器读头和外部控制设备之间的通讯协议，以供二次开发使用，下文中的终端机为通讯中的主设备，读卡器为通讯中的从设备。

8.1 通讯特性

- 驱动层采用串口通讯
- 协议层采用自定义规则，见下面描述
- 通讯模式包括透传模式和自定义模式，自定义模式下有认证系统和消费系统
- 传输波特率采用 38400bps

8.2 协议名词解释

- FID：认证应用或消费应用的文件标识符，每一个钱包对应一个 FID，长度 2byte
- PIN：圈存操作需要的 PIN 码，通常为 2 - 6 位，长度 6byte，长度不足通过 FF 填充。比如 PIN 为 123456，表示为 010203040506；PIN 为 1234，表示为 01020304FFFF
- 密钥索引：交易过程中的圈存密钥、消费密钥的标识，长度 1byte，默认定义为 0x01
- 交易金额：圈存、消费过程中的金额，长度 4byte
- 终端机编号：每一个终端机应有一个独一无二的编号，长度 6byte
- 终端机交易序号：每个终端机自己通过的交易序号，长度为 4byte
- 交易时间：终端机提供的交易时间，长度 7byte，格式为年月日时分秒，如 2007 年 12 月 10 日，18 点 23 分 56 秒，表示为 20071210182356(16 进制)
- 交易码：圈存或者消费的记录标识，通常交易成功会产生本次交易的交易码用于保存。长度 4byte

8.3 卡出厂状态

8.3.1 认证系统

用户卡和 PSAM 卡内均设置了认证密钥和权限密钥，认证密钥用于认证用户卡，防止伪卡，权限密钥用于获取用户卡文件读写权限，通过两个密钥实现双向认证的过程，防止其他读卡器随意更改用户卡文件。

用户卡内设置六个透明文件，每个文件的大小为 32 个字节。

用户卡出厂时处于未激活状态，首先应通过我们的发卡设备设置用户卡和 PSAM 卡的认证密钥和权限密钥，然后通过读头的激活指令进行激活，初始化的文件无数据(读指令无法返回数据)，必须对文件初始化写操作后，才可以读出数据。

8.3.2 消费系统

用户卡和 PSAM 卡内设置了消费密钥和圈存密钥，分别用于消费指令和圈存指令过程中的卡和设备相互认证。

用户卡出厂时处于未激活状态，首先应通过我们的发卡设备设置用户卡和 PSAM 卡的认证密钥和权限密钥，然后通过读头的激活指令进行激活，之后可以执行消费圈存等操作

8.4 自定义协议

读卡器与 PC 之间同通信由我们自己做出规定，根据我们常用的协议，类似的做出规范，规范中应包含数据包包头、数据包长度、数据包数据、数据包校验、数据包包尾等关键点，在读卡器与终端机的通信过过程中，应严格遵守此协议，对不符合协议的所有类型的异常应作出明确的异常处理。

本协议共支持两种模式：

自定义模式：

1、 针对认证系统定义了交易前检测卡、寻卡(认证)、读写文件、激活卡、查询激活状态六个命令

2、 针对消费系统定义了圈存、普通消费、灰锁消费、查询余额、查询明细五种命令

透传模式：可以直接透过读卡器发送 APDU 到卡片

具体协议如下：

请参考以下图表：

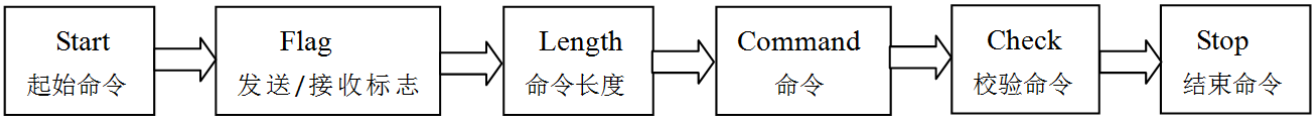

图 8 通讯协议数据传输格式

8.4.1 终端机发送

	Start	Flag	Length	MODE	Command	Check	Stop
终端机发送	0x6A	0x00 发送模式 终端机发送到读卡器	Command 的长度	0x00 消费模式	具体定义见下表	除 Stop 命令外，所有字节按位的异或值	0xFF
				0x80 透传模式	发送到用户卡的 APDU		

表 4 终端机发送的包格式

8.4.2 终端机接收

	Start	Flag	Length	MODE	Return	Check	Stop
终端机接收	0x6A	0x01 接收模式 读卡器发送到终端机	Command 的长度	0x80 透传模式	发送到用户卡的 APDU	除 Stop 命令外，所有字节按位的异或值	0xFF
				0x00 消费模式	具体定义见下表		

表 5 终端机接收的包格式

8.4.3 通用指令

8.4.3.1 发送指令

指令	Command	说明
寻卡操作	0x04	卡上电，获取 UID 和 ATS
交易前检测卡	0x06	正常情况监测是否存在卡
交易后检测卡	0x07	交易完成后监测卡是否离场
激活卡指令	0x20	激活某个应用
查询激活状态指令	0x21	查询某个应用的激活状态
选择应用	0x22	一般寻卡后应执行选择应用操作

表 6 终端机通用指令发送

8.4.3.2 接收指令

指令	Command	说明
寻卡操作	0x04 + UIDLEN + UID + ATSLEN +ATS + 9000	
交易前检测卡	0x06 + 卡状态 +0x 9000	卡状态为 0x00 表示无卡，0x01 表示有卡
交易后检测卡	0x07 + 卡状态 + 0x 9000	卡状态为 0x00 表示无卡，0x01 表示有卡
激活卡指令	0x20 + 激活状态 + 0x9000	激活状态为 0x00 表示未激活，0x01 表示已激活
查询激活状态指令	0x21 + 激活状态 + 0x9000	激活状态为 0x00 表示未激活，0x01 表示已激活
选择应用	0x22 + 0x9000	

表 7 终端机通用指令接收

8.4.4 认证系统指令

8.4.4.1 发送指令

指令	Command	说明
认证并获取权限	0x0F	认证卡片为内部卡，并且获取当前应用读写权限
读取文件	0x0D + 文件编号(1 - 6) + 预期读取长度	
写文件	0x0E + 文件编号(1 - 6)+ 写入长度(1byte) + 数据	

表 8 终端机认证指令发送

8.4.4.2 接收指令

指令	Command	说明
认证并获取权限	0x0F+ 认证状态+获取权限状态+ 0x 9000	认证状态为 0x00 表示认证失败，0x01 表示认证成功 权限状态为 0x00 表示获取读写权限失败，0x01 表示获取读写权限成功
读取文件	0x0D + 数据+ 0x 9000	
写文件	0x0E + 0x 9000	

表 9 终端机认证指令接收

8.4.5 消费系统指令

8.4.5.1 发送指令

指令	Command	说明
圈存	0x00 + PIN + 密钥索引 + 交易金额 + 终端机编号 + 交易时间	存钱操作
灰锁消费	0x01 + 密钥索引 + 交易金额 + 终端机编号 + 终端机交易序号 + 交易时间	将灰锁初始化以及灰锁继续交易两个指令统一为一条指令
查询余额	0x02	
读取交易明细	0x03 + 明细序号(1 - 10)	读取交易明细，最多读取 10 个最近的交易
查询灰锁状态	0x05	状态包括未灰锁，已灰锁未执行交易、已灰锁交易未解除灰锁
灰锁继续交易	0x08 +交易金额	已灰锁，但交易未执行，继续执行上次交易
灰锁解除交易	0x09	已灰锁，但交易未执行，停止执行上次交易
灰锁初始化	0x0A	初始化灰锁消费操作，之后需要灰锁继续交易或者灰锁解除交易指令进行解除灰锁
解除灰锁标志	0x0B	1、 正常消费下，对已灰锁交易完成但未解除灰锁的情况进行解锁处理 2、 联合消费下，对第二个钱包扣款完成后，对第一个钱包执行此操作，表示完成联合消费
普通消费	0x0C + 密钥索引 + 交易金额 + 终端机编号+ 终端机交易序号 + 交易时间	快速消费，不执行灰锁过程

表 10 终端机消费指令发送

8.4.5.2 接收指令

指令	Command	说明
圈存	0x00 + 交易码 + 0x9000	
灰锁消费	0x01 + 交易码 + 0x 9000	
查询余额	0x02 + 余额 + 0x 9000	
读取交易明细	0x03 + 交易明细 + 0x 9000	
查询灰锁状态	0x05 + 灰锁状态 + 0x 9000	
灰锁继续交易	0x08+ 交易码 + 0x 9000	
灰锁解除交易	0x09+ 交易码 + 0x 9000	
解除灰锁标志	0x0B + 9000	
普通消费	0x0C+ 交易码 + 0x 9000	

表 11 终端机消费指令接收

交易明细包括以下内容：

卡交易序号(2byte)、交易金额(7byte)、交易类型(1byte)、终端机编号(6byte)、交易时间(7byte)

交易类型为 0x93 代表灰锁消费、0x02 代表圈存交易

灰锁状态分为以下三种情况

1、 正常状态：

状态字(00)、上次解扣交易类型(93)、交易电子钱包(01)、上次解扣交易余额(4byte)、上次解扣卡交易序号(2byte)、上次解扣终端机编号(6byte)、上次解扣交易时间(7byte)、上次解扣交易金额(4byte)、上次解扣交易码(4byte)

2、 灰锁状态(执行中断，未扣取金额)

状态字(01)、灰锁的交易类型(91)、交易电子钱包(01)、灰锁的交易余额(4byte)、灰锁的卡交易序号(2byte)、灰锁的终端机编号(6byte)、灰锁的交易时间、灰锁的交易金额(4byte)、灰锁的 MAC2、灰锁的 GTAC

3、交易完成未解除灰锁状态(执行中断，已扣取金额)

状态字(10)、上次解扣交易类型(93)、交易电子钱包(01)、上次解扣交易余额(4byte)、上次解扣卡交易序号(2byte)、上次解扣终端机编号(6byte)、上次解扣交易时间(7byte)、解扣交易金额(4byte)、上次解扣交易码(4byte)

8.4.6 交易出错返回

指令	Command
圈存	0x00 + 错误码
灰锁消费	0x01 +错误码
查询余额	0x02 +错误码
读取交易明细	0x03 +错误码
寻卡操作	0x04 +错误码
查询灰锁状态	0x05 +错误码
交易前检测卡	0x06 +错误码
交易后检测卡	0x07 +错误码
灰锁继续交易	0x08+错误码
灰锁解除交易	0x09+错误码
灰锁初始化	0x0A +错误码
解除灰锁标志	0x0B +错误码
普通消费	0x0C+错误码
读取文件	0x0D+错误码
写文件	0x0E+错误码
认证并获取权限	0x0F+错误码
激活卡指令	0x20+错误码
查询激活状态指令	0x21+错误码
选择应用	0x22+错误码

表 12 交易出错指令返回格式

错误码高 8 位	错误码低 8 位	含义
90	00	命令执行成功
CC	01	命令头错误
CC	02	命令标志位错误
CC	03	命令模式位错误

CC	04	Command 指令头出错
CC	05	Command 长度出错
CC	06	Command 校验位出错
CC	07	Command 结束位出错
C0	01	PSAM 卡文件读取出错
C0	02	用户卡文件读取出错
C0	03	初始化圈存出错
C0	04	圈存 MAC1 校验出错
C0	05	圈存 MAC2 校验出错
C0	06	圈存 PIN 校验出错
C1	03	初始化消费出错
C1	04	消费 MAC1 校验出错
C1	05	消费 MAC2 校验出错
C1	06	消费 LOCK 状态错误
C1	07	消费 LOCK 出错
C1	08	消费 UNLOCK 出错
C1	09	PSAM 中间密钥生成出错
C1	0A	消费 GMAC 校验出错
C1	0B	消费清除锁定出错
C1	0C	处理普通消费出错
CC	0A	寻卡出错
CC	0B	校验 MAC 出错
CD	01	卡激活状态出错
CD	02	未获取权限

表 13 终端机错误码定义

8.5 建议的交易流程

8.5.1 认证系统

读写文件条件：

1、 寻卡成功，并且认证和获取读写权限成功

2、 卡处于激活状态

NOTE：

1、 读写文件前会判断激活状态，未激活的卡是不允许读写的，返回 CD01 错误

2、 若寻卡失败或者未寻卡，执行读写文件指令，读头无法判断激活状态，会返回 CD01 错误

3、 只有认证和获取读写权限成功，才可以查询激活状态，否则会返回错误

4、 当卡在读头场范围时，未执行交易前检测指令，也可以执行寻卡指令

5、 若进入了读写流程，不可以执行交易前检测卡指令，若执行了，必须要再次寻卡获取权限才可以继续进行读写操作

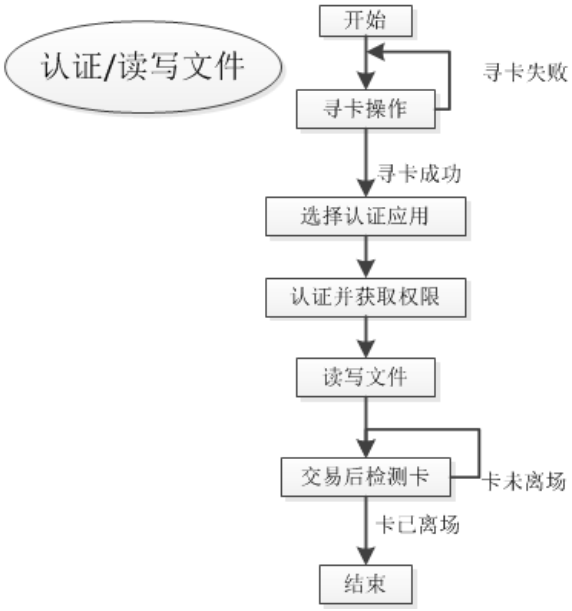

图 9 认证流程

8.5.2 消费系统

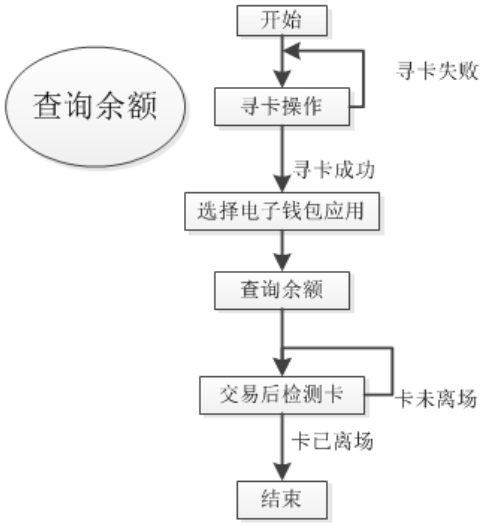

图 10 查询余额流程

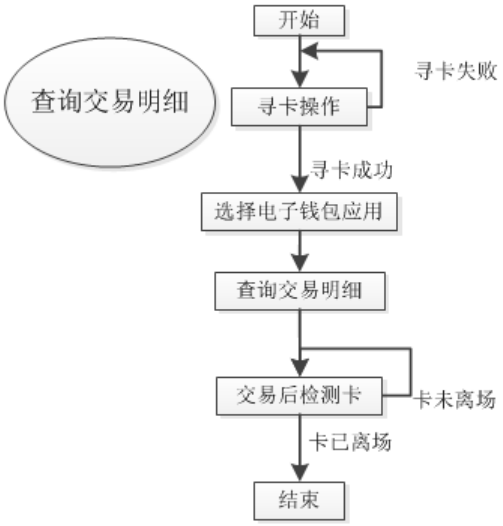

图 11 查询交易明细流程

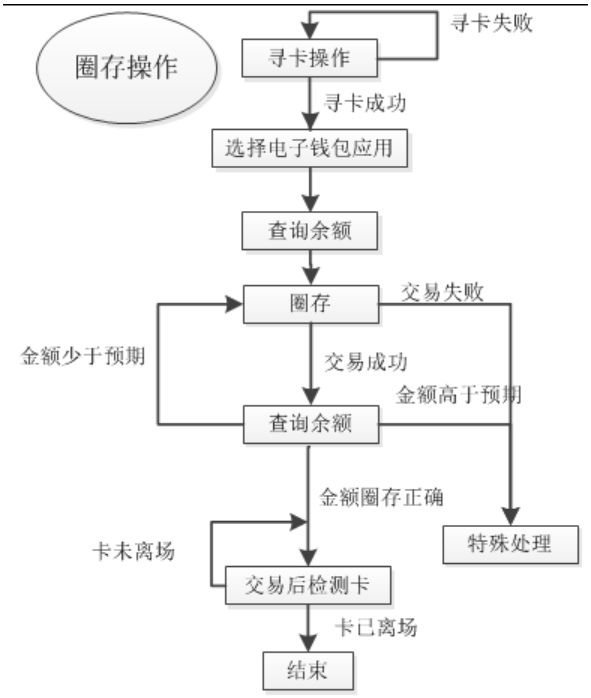

图 12 圈存操作流程

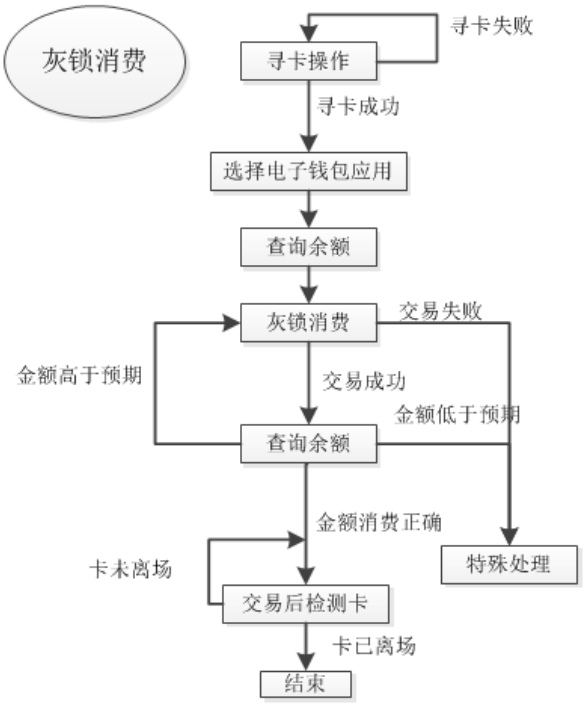

图 13 灰锁消费流程

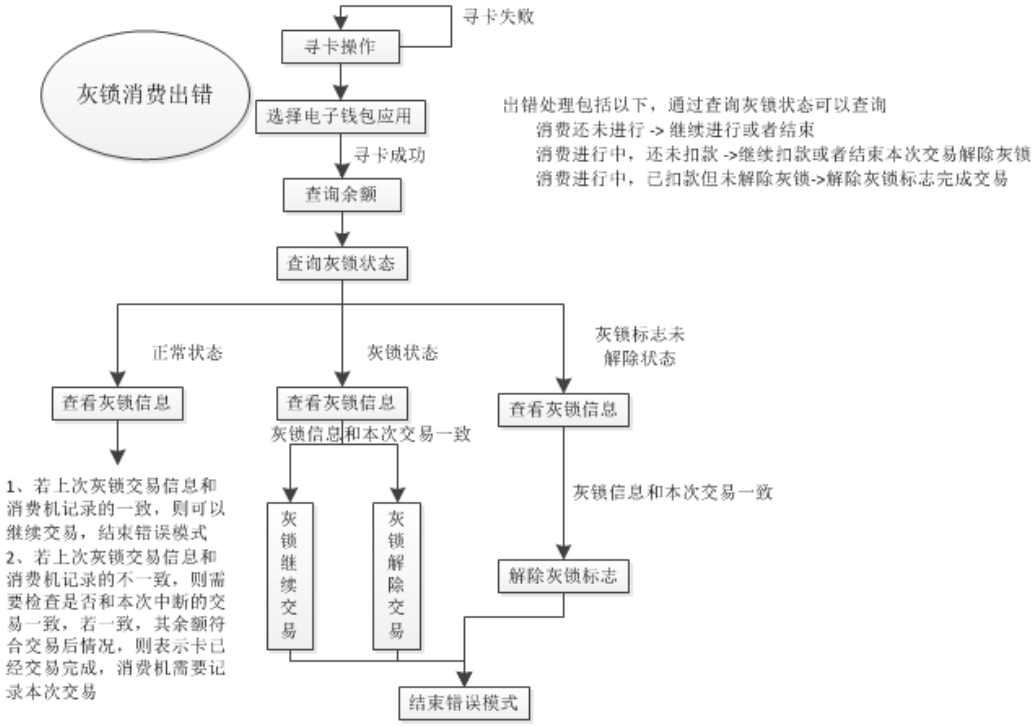

图 14 灰锁消费出错处理流程