ICS35.240.15
CCS L71

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX.4—202X

中华人民共和国社会保障卡一卡通规范 第 4 部分：终端规范

Specifications for the social security card one-card-pass of the People's Republic of China - Part 4：Terminal specifications

（征求意见稿）

（本草案完成时间：2023 年 11 月 04 日）

XXXX-XX - XX 发布　　XXXX - XX -XX 实施

国 家 市 场 监 督 管 理 总 局
国 家 标 准 化 管 理 委 员 会　发 布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T XXXXX《中华人民共和国社会保障卡一卡通规范》的第4部分。GB/T XXXXX已经发布了以下部分：

——第1部分：基础规范；

——第2部分：应用规范；

——第3部分：安全规范；

——第4部分：终端规范。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由人力资源和社会保障部提出并归口。

本文件起草单位：人力资源和社会保障部信息中心、XXX。

本文件主要起草人： XXX。

引　言

本文件通过规范社会保障卡一卡通应用实践，重点围绕社会保障卡一卡通业务需求，针对实体社会保障卡、电子社会保障卡及一卡通应用提出标准化解决方案，作为社会保障卡技术、质量管控、一卡通应用和管理要求的基础标准，对于实现社会保障卡“一卡多用、全国通用”、支撑政府公共服务“一卡通”、居民服务“一卡通”具有重要的基础指导作用并具有深远的战略意义。

GB/T XXXXX《中华人民共和国社会保障卡一卡通规范》是规范全国社会保障卡一卡通工作的基础性和通用性的标准，目前由4个部分构成，具体如下：

——第1部分：基础规范。目的在于规定社会保障卡一卡通的基础要求，包括社会保障卡一卡通的体系架构、载体要求、服务渠道及基础支撑要求等内容。

——第2部分：应用规范。目的在于规定社会保障卡一卡通的应用要求，包括社会保障卡一卡通的应用平台、应用场景、应用流程、应用平台接入技术要求、应用平台接入工作流程、应用协作及推广要求等内容。

——第3部分：安全规范。目的在于规定社会保障卡一卡通的安全要求，包括社会保障卡一卡通的安全体系架构、载体安全要求、终端安全要求、应用平台安全要求、数据安全要求及密钥安全要求等内容。

——第4部分：终端规范。目的在于规定社会保障卡一卡通的终端要求，包括社会保障卡一卡通的终端形态、终端通用要求、终端技术要求等内容。

中华人民共和国社会保障卡一卡通规范
第4部分：终端规范

1 范围

本文件规定了社会保障卡一卡通终端形态、终端通用要求及终端技术要求。

本文件适用于社会保障卡一卡通终端的研发、制造、应用和维护。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 9254.1 信息技术设备、多媒体设备和接收机电磁兼容 第1部分：发射要求（GB/T 9254.1—2021，CISPR 32:2015，MOD）

GB/T 9254.2 信息技术设备、多媒体设备和接收机电磁兼容 第2部分：抗扰度要求（GB/T 9254.2—2021，CISPR 35:2016，MOD）

GB/T 16649.1 识别卡带触点的集成电路卡 第1部分：物理特性（GB/T 16649.1—2006，ISO/IEC 7816-1:1998，MOD）

GB/T 16649.2 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 16649.2—2006，ISO/IEC 7816-2:1999，IDT）

GB/T 16649.3 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 16649.3—2006，ISO/IEC 7816-3:1997，IDT）

GB/T 16649.4 识别卡带触点的集成电路卡 第4部分：用于交换的结构、安全和命令（GB/T 16649.4—2010，ISO/IEC 7816-4:2005，IDT）

GB/T 22351.1 识别卡无触点的集成电路卡邻近式卡 第1部分：物理特性（GB/T 22351.1-2008，ISO/IEC 15693-1:2000）

GB/T 22351.2 识别卡无触点的集成电路卡邻近式卡 第2部分：空中接口和初始化（GB/T 22351.2—2010，ISO/IEC 15693-2:2000）

GB/T 42756.2 卡及身份识别安全设备 无触点接近式对象 第2部分：射频功率和信号接口（GB/T 42756.2－2023，ISO/IEC 14443-2:2020，MOD）

GB/T 42756.3 卡及身份识别安全设备 无触点接近式对象 第3部分：初始化和防冲突（GB/T 42756.3－2023，ISO/IEC 14443-3:2018，IDT）

GB/T 42756.4 卡及身份识别安全设备 无触点接近式对象 第4部分：传输协议（GB/T 42756.4－2023，ISO/IEC 14443-4:2018，IDT）

LD/T 33—2015 社会保障卡读写终端规范

3 术语和定义

GB/T 9254.1、GB/T 16649.1、GB/T 16649.3、GB/T 42756.2、GB/T 42756.3、GB/T 42756.4、GB/T 41803.1界定的以及下列术语和定义适用于本文件。

3.1

功能 function

由一个或者多个命令实现的处理过程，其操作结果用于完成全部或者部分交易。

[来源：GB/T 9254.1-2021，3.1.16]

3.2

条码 barcode

由一组按一定编码规则排列的条、空符号，用以表示一定的字符、数字和符号组成的信息。包含一维码和二维码。

3.3

条码识读 barcode reading

通过扫描条码图获取其中所包含信息。

3.4

模块 module

由电子元器件组成的具有实现某一具体功能的电路。

3.5

模组 modules

通常指一组或多组模块。

3.6

交易 transaction

持卡者和业务、管理部门之间根据社会保障卡所支持的应用接受、提供服务的行为。

3.7

密钥 key

控制加密转换操作的符号序列。

[来源：GB/T 25069-2022，3.388]

3.8

人力资源和社会保障终端 human resource social security terminal

符合LD/T 33—2015行业标准的终端，适用于人力资源和社会保障相关业务办理场合，同时也符合本规范的要求。

3.9

接口设备 interface device

终端上插入卡片的部分，包括其中的机械、电气和逻辑控制部分。

[来源：GB/T 16649.3-2006，3.1.1]

3.10

触点 contact

在集成电路卡（IC卡）和外部接口设备之间保持电流连续性的导电元件。

[来源：GB/T 16649.1-2006，3.3]

3.11

集成电路（IC） integrated circuit

设计用于完成处理和/或存储功能的电子器件。

[来源：GB/T 16649.1-2006，3.1]

3.12

ID-1

标称尺寸为：宽度85.60mm，高度53.98mm，厚度0.76mm。

[来源：GB/T 14916-2022，3.5]

3.13

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

内部封装一个或者多个集成电路的ID-1型卡。

[来源：GB/T 16649.1—2006，3.2]

3.14

ICC **连接器** ICC connector

IFD与ICC电气连接的物理实现部分。在逻辑上，本文件规定用它来标识与它电气上稳定连接的ICC。

3.15

半字节 nibble

一个字节的高四位或者低四位。

3.16

T=0

面向字符的异步半双工传输协议。

3.17

T=15

不是传输协议，而是特指其后所传输字符的属性为全局接口字符。

3.18

静止状态 inactive

当卡上的电源电压（VCC）和其他信号相对于地的电压值小于或等于0.4V时，则称电源电压和这些信号处于静止状态。

3.19

命令 command

终端向卡片发出的一条信息，该信息启动一个操作或请求一个应答。

3.20

响应 response

卡片处理完成收到的命令报文后，返回给终端的报文。

3.21

邻近式 IC 卡（PICC） proximity integrated circuit（s）card

一种ID-1型卡，在它上面已装入集成电路和耦合电路，并且与集成电路的通信是通过与邻近式耦合设备的电感耦合完成的。

[来源：GB/T 22351.1—2008，3.4]

3.22

邻近式耦合设备（PCD） proximity coupling device

用电感耦合给PICC提供能量并控制与PICC交换数据的读/写设备。

[来源：GB/T 22351.1-2008，3.5]

3.23

调制系数 modulation index

定义为[a-b]/[a+b]，其中a，b分别是信号幅度的峰值和最小值。

注：该指数值可用百分率来表示。

[来源：GB/T 22351.2—2010，3.1]

3.24

副载波 subcarrier

频率为fs的信号，用来调制载波频率fc。

[来源：GB/T 22351.2—2010，3.2]

3.25

移幅键控 amplitude shift keying

以数字基带信号控制载波的幅度变化的数字调制方式，又称为数字调幅。

3.26

二进制启闭键控 on-off keying

载波的振幅随着数字基带信号（数字基带信号为二进制）而变化的数字调制方式，又称为二进制振幅键控（2ASK）。

3.27

二进制移相键控 binary phase shift keying

移相为180°的移相键控，从而导致两个可能的相位状态。

3.28

不归零电平 non-return to zero level

位编码的方式，位持续期间的逻辑状态。可借此通过通信媒介的两个已定义的物理状态之一来表示。

3.29

冲突 collision

在同一时间周期内，在同一PCD的工作场中，有两张或两张以上的PICC进行数据传输，使得PCD不能辨别数据是从哪一张PICC发出的。

3.30

景深 depth of field

条码图的垂直方向和法向，条码识读设备能够读取条码图的距离范围。

3.31

识读角度 reading angle

条码图沿轴线方向的偏转角，由X轴偏转角、Y轴偏转角及Z轴偏转角组成。

3.32

冷复位 cold reset

激活后的第一次复位。

[来源：GB/T 16649.3—2006，3.3.1]

3.33

热复位 warm reset

非冷复位的所有其他复位。

[来源：GB/T 16649.3—2006，3.3.2]

3.34

加密机 encryption machine

支撑各种密码算法，安全保存密钥的加密设备。

注：加密机和主机之间使用TCP/IP协议通信。

3.35

报文 message

由终端向卡片或卡片向终端发出的，不含传输控制字符的字节串。

3.36

报文鉴别代码 message authentication code

对交易数据及其相关参数进行运算后产生的代码。主要用于验证报文的完整性。

4 符号和缩略语

下列符号和缩略语适用于本文件。

ASK：移幅键控（Amplitude Shift Keying）
BPSK：二进制移相键控（Binary Phase Shift Keying）
CLK：时钟（Clock）
CIN：输入电容（Input Capacitance）
etu：基本时间单元（elementary time unit）
Fc：载波频率（frequency of operating field）
Fs：副载波调制频率（frequency of subcarrier）
GND：地（Ground）
IC：集成电路（Integrated Circuit）
ICC：集成电路卡（Integrated Circuit（s）Card）
IFD：接口设备（Interface Device）
I/O：输入/输出（Input/Output）
I_{IH}：高电平输入电流（High Level Input Current）
I_{IL}：低电平输入电流（Low Level Input Current）
I_{OH}：高电平输出电流（High Level Output Current）
I_{OL}：低电平输出电流（Low Level Output Current）
MAC：报文鉴别代码（Message Authentication Code）
Mil：长度单位
Lux：流明，光通量的单位
NRZ－L：不归零电平（Non-return to Zero）
OOK：二进制启闭键控（On/Off Keying）
PPS：协议和参数选择（Protocol and Parameters Selection）
PSE：金融支付系统环境（Payment System Environment）
REQA：对A型卡的请求（REQuest Command, Type A）
REQB：对B型卡的请求（REQuest Command, Type B）
RF：射频（Radio Frequency）
RFU：保留为将来使用（Reserved for Future Use）
RST：复位（Reset）
SW1：状态码1（Status Word One）
SW2：状态码2（Status Word Two）
t_F：信号幅度从90%下降到10%的时间（Fall Time Between 90% and 10% of Signal Amplitude）
t_R：信号幅度从10%上升到90%的时间（Rise Time Between 10% and 90% of Signal Amplitude）
VCC：电源电压（Supply Voltage）
VPP：编程电压（Programming Voltage）

VCC：触点上的测量电压（Voltage Measured On VCC Contact）
V_{IH}：高电平输入电压（High Level Input Voltage）
V_{IL}：低电平输入电压（Low Level Input Voltage）
V_{OH}：高电平输出电压（High Level Output Voltage）
V_{OL}：低电平输出电压（Low Level Output Voltage）
Xx：任意值
‘0’-‘9’‘A’-‘F’：十六进制数字

5 一卡通终端形态

5.1 通则

社会保障卡一卡通终端是指能够操作一卡通载体，与实体社会保障卡或者电子社会保障卡进行信息交互，用于各项一卡通应用场景业务办理并完成一定事务的设备。

社会保障卡一卡通终端的形态主要是根据其功能和使用场景及外观来区分，满足各使用场景下的功能和外观等需求，对不同使用场景下的选型和使用给予指导。

5.2 读写器

通常为桌面式，安装于平整桌面上使用，能受理实体社会保障卡的整机设备，有接触式卡槽、非接识读区域、指示灯、图形或文字标识等，其他部件按需配置。

5.3 扫码窗（枪）

具备条码识读功能，能受理电子社会保障卡的设备，带有指示灯、图形或者文字标识等。依据形态分类如下：

——手持式条码扫描设备（含具有扫描功能的手持终端设备）；

——固定式条码扫描设备。

5.4 复合终端

具备多种功能的终端，包含读写器、扫码窗（枪），同时支持社会保障应用和金融应用的社会保障金融联合终端。

5.5 终端类读写模组

终端类读写模组指用于嵌入其他设备中的一卡通读写模组，以嵌入式模块形式安装在各类设备上，包含接触式模块、非接触式模块、条码识读模块，各模块可集成一体，也可相互独立。内嵌读写模组的一卡通终端主要包括立式自助机、桌面式智能终端、壁挂式自助设备、手持式设备、便携式设备、闸机、门禁等。

6 一卡通终端通用要求

6.1 通则

为满足不同场景的使用需求及相关功能的具体实现，一卡通终端在其硬件、软件、设计和管理等方面需要满足一定的要求。

6.2 终端组成

一卡通终端应包含但不限于以下模块，具体见表1。

表1 终端功能部件配置要求

部件分类	部件名称	说明
一卡通读写模块	接触式模块	终端应至少包括其中一个模块
	非接触式模块	
	条码识读模块	
用户界面模块	显示模块	终端如支持用户界面功能应至少包括其中一个模块
	触控模块	
	键盘模块	
	音频模块	
安全存取模块	安全存取模块	按需配置
存储模块	非易失性存储器	按需配置
	硬盘	
打印模块	证卡打印模块	按需配置
	票据打印模块	
接口模块	串行通讯	终端如支持通讯功能应至少包括其中一个模块
	USB通讯	
	红外通讯	
	蓝牙通讯	
	以太网通讯	
	无线Wi-Fi通讯	
	移动通信网络通讯	
实时时钟模块	实时时钟模块	按需配置
电源模块	直流电源模块	按需配置
	交流电源模块	
生物特征识别模块	人脸识别模块	按需配置
	指纹识别模块	
	指静脉识别模块	
	虹膜识别模块	
	声纹识别模块	
	其他生物特征识别模块	

6.3 终端功能

6.3.1 一卡通读写模块

指可读写一卡通载体的模块，主要包括以下三种类型：

a) 接触式模块
以接触式方式读写实体社会保障卡。

b) 非接触式模块
以非接触式方式读写实体社会保障卡。

c) 条码识读模块
用于对电子社会保障卡识读，包括一维码和二维码。

6.3.2 用户界面模块

指用于设备和持卡人之间交互的模块，主要包括以下四种类型：

a) 显示模块
用于交易过程显示及错误指示。本文件要求显示器具有显示汉字、字母、数字和符号的能力。

b) 触控模块
用于人机交互操作的触摸屏或者触控按键，可替代鼠标和键盘。

c) 键盘模块
用于用户输入数据，至少配置数字键及确认功能键。

d) 音频模块
用于蜂鸣提示或者语音播报，提示持卡人当前操作状态及导引下一步操作。

6.3.3 安全存取模块

用于对实体社会保障卡进行权限鉴别，其主要功能包括存储权限控制密钥、计算鉴别数据等。

6.3.4 存储模块

用于存储对社会保障卡的操作记录或者扩展中文字符集等信息，主要包括非易失性存储器或者硬盘等。

6.3.5 打印模块

根据业务需要，终端可配备相应的打印模块，主要包括证卡打印模块、票据打印模块等。

6.3.6 接口模块

接口模块用于一卡通终端与主机之间的数据传输，可以是以下通讯方式的一组或多组。

a) 串行通讯
通过串行通讯接口进行数据传输，常见的接口类型包括RS-232、RS-485等。

b) USB通讯
通过USB接口进行数据传输，提供高速、可靠的连接方式。

c) 红外通讯
通过红外通讯接口进行数据传输，适用于近距离无线通信。

d) 蓝牙通讯
通过蓝牙通讯接口进行数据传输，适用于近距离无线通信。

e) 以太网通讯
通过以太网通讯接口进行数据传输，支持有线网络连接。

f) 无线Wi-Fi通讯
通过无线Wi-Fi通讯接口进行数据传输，提供无线网络连接。

g) 移动网络通讯

通过移动网络通讯接口进行数据传输，支持2G、3G、4G、5G或其他移动通信网络。

6.3.7 实时时钟模块

用于提供业务处理所需的终端时间，如交易时间。

6.3.8 电源模块

用于提供电源电压和电流的电子模块。一卡通终端可采用直流或者交流方式供电。

6.3.9 生物特征识别模块

利用人体生物特征进行身份认证的模块，主要包含人脸、指纹、指静脉、虹膜、声纹和其他生物特征识别模块。

6.4 终端接口

6.4.1 一卡通终端编程接口

一组用于特定目的的程序接口，主要包括基础接口和应用接口两部分。

a) 基础接口

一卡通终端提供的最底层的编程接口，用于社会保障卡与主机之间的指令交互和条码识读。具体见附录A。

b) 应用接口

基于基础接口，为全国一卡通应用平台或者其他部门一卡通应用系统提供的更高层次编程接口，实现某种特定社会保障卡业务。具体见附录B。

6.4.2 接口兼容性

指设备的各种软硬件接口的兼容，主要包括硬件通讯接口兼容和软件编程接口兼容。

a) 硬件通讯接口兼容主要是电气特性、通讯协议的兼容；

b) 软件编程接口兼容主要包括：

1) 接口兼容性：在各种操作系统、开发工具和编程语言环境下都能正常访问和调用；

2) 接口稳定性：接口的功能和参数应保持稳定，不受环境变化影响；

3) 参数一致性：输入参数和输出结果一致，包括参数类型、参数顺序和返回值类型。

6.5 终端管理

6.5.1 一卡通终端应用架构和要求

6.5.1.1 一卡通终端应用架构

一卡通终端应用包括一卡通基础支撑系统、一卡通应用平台、一卡通应用系统和一卡通终端等，其架构如图1所示。

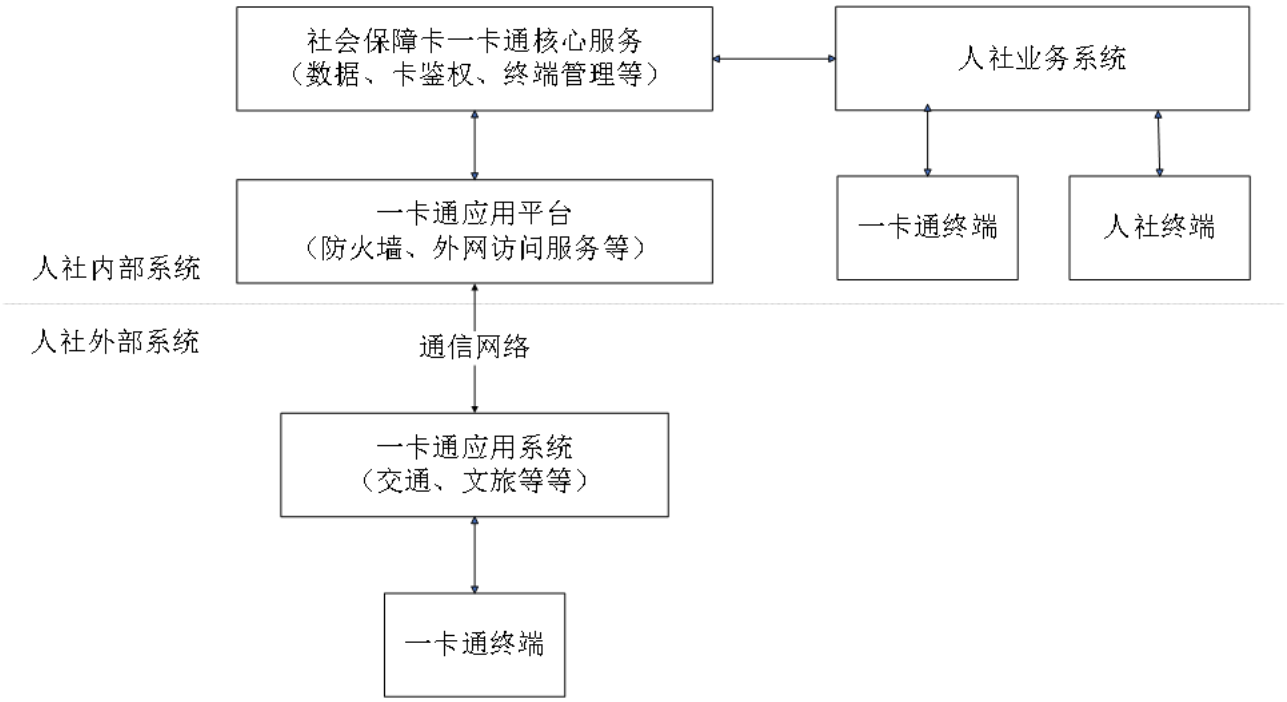


图1 一卡通终端应用架构

6.5.1.2 一卡通终端应用要求

一卡通终端应用要求具体如下：

a) 以人社业务系统服务为支撑，实现与各部门一卡通应用系统的对接，为一卡通终端提供接口服务；
b) 应用系统应与各部门的一卡通应用系统进行无缝对接，以支持跨部门数据共享和服务提供；
c) 针对接入应用系统，应实施必要的适配措施，确保与一卡通应用平台的兼容性；
d) 对已部署的人社终端进行必要的更新和配置调整，以满足一卡通应用的需求。

6.5.2 一卡通终端管理系统架构和要求

6.5.2.1 一卡通终端管理系统架构

一卡通终端管理系统应在一卡通基础支撑系统中提供，并通过一卡通应用平台与各接入的一卡通应用系统对接，其架构如图2所示。

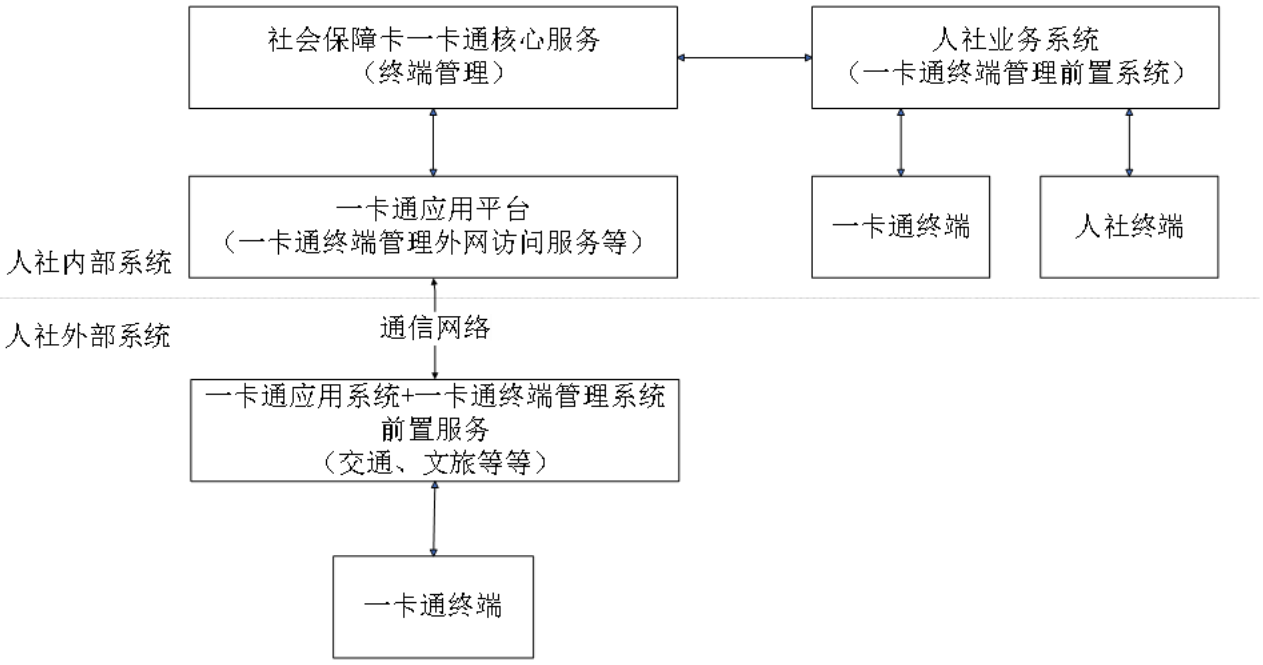


图2 一卡通终端管理系统架构

6.5.2.2 一卡通终端管理系统要求

具体应包括：

a) 一卡通终端应拥有统一的终端唯一识别码。

终端唯一识别码是一卡通终端的唯一标识，用于管理一卡通终端，应在出厂前被设置。

终端唯一识别码为一组 32 位定长 ASCII 编码字符，由终端设备号（20 位）和安全存取模块终端机编号（12 位）两部分顺序组成。其中终端设备号在终端出厂时写入，不应更改，由厂商代码（4 位）、产品型号（4 位，只能由字符或数字组成，厂商自定义）、生产年月（6 位，YYYYMM 格式）和生产流水号（6 位，取值范围：000000—999999）四部分顺序组成。安全存取模块制作完成后自动生成一个唯一的安全存取模块终端机编号。终端唯一识别码示例如图 3 所示。

注：如无终端设备号或者安全存取模块终端机编号其中之一的，则相应部分返回全 0 字符串即可。

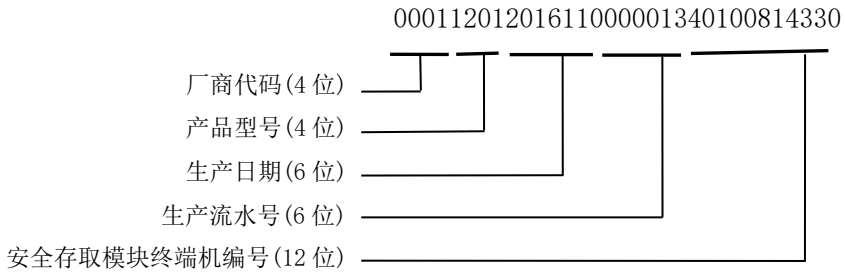


图3 终端唯一识别码示例

b) 一卡通终端应提供相应的途径与一卡通终端管理系统进行交互，可是动态库接口或者网络通信服务接口。动态库接口详见附录A和附录B。

c) 一卡通终端的身份信息除了自身的终端唯一识别码外，还包括终端分类和功能、使用和管理机构名称和编号、使用场景、软件和硬件版本及接入的一卡通应用系统名称和版本等信息。

d) 为保障终端使用过程中的安全可靠，一卡通终端管理系统需对不同应用场景下的一卡通终端进行有效管理，实现对一卡通终端的全流程管理。主要管理内容如下：

1) 终端注册：对一卡通终端的身份信息进行登记，主要包括生产厂商、产品型号、软件版本、终端类型、使用机构信息等。

2) 权限登记：对一卡通终端权限信息进行登记；
3) 终端鉴权：对一卡通终端身份信息等的有效性、合法性进行判定；
4) 状态监控：对一卡通终端的运行和使用状态进行监控；
5) 终端信息变更：对一卡通终端的身份信息、权限信息、终端状态等信息进行变更；
6) 终端注销：对作废的一卡通终端身份信息进行注销登记。

e) 一卡通终端管理系统前置服务。

前置服务对接一卡通终端和人社终端的动态库或应用软件，并与一卡通终端管理系统交互。前置服务兼容管理各类终端，并给一卡通终端管理系统和接入的一卡通应用系统提供统一的终端管理服务接口。

7 一卡通终端技术要求

7.1 通则

为保证一卡通终端的功能和性能，一卡通终端的功能参数和性能标准方面应满足特定的要求。

7.2 外观与结构要求

具体应包括：

a) 外形应美观大方，表面涂覆层应均匀，不应起泡、龟裂、脱落，不应有明显的破损、划痕、变形和污染等；
b) 零部件连接应紧固无松动，金属零部件不应有锈蚀及其他机械损伤；
c) 开关、按键应操作灵活可靠；
d) 商标、名称、型号和文字说明应清晰、端正。

7.3 环境适应性要求

7.3.1 气候环境适应性要求

7.3.1.1 温湿环境适应性要求

温湿环境适应性要求见表2。

表 2 温湿环境适应性要求

设备状态	温湿环境		大气压
	温度	相对湿度	
工作	-5℃～50℃	15%～90%，无冷凝	86～106kPa
贮存运输	-40℃～70℃	5%～93%，无冷凝	

7.3.1.2 盐雾试验适应性要求

一卡通终端在盐雾环境下放置48h后，应能正常工作。

7.3.2 机械环境适应性要求

7.3.2.1 振动适应性要求

振动适应性要求见表3。

表 3 振动适应性要求

项目	参数	取值范围
初始和最后振动响应	频率范围 Hz	10～55
	扫频速度 oct/min	≤1
	位移幅值 mm	0～15
定频耐久性	位移幅值 mm	0.75mm（10Hz～25Hz） 0.15mm（25Hz～55Hz）
	持续时间 min	30±1
扫频耐久性	频率范围 Hz	10～55～10
	位移幅值 mm	0.15mm
	扫频速度 oct/min	≤1
	循环次数	5

7.3.2.2 冲击适应性要求

冲击适应性要求见表4。

表 4 冲击适应性

峰值加速度（m/s^2）	脉冲持续时间（ms）	冲击波形
300	11	半正弦波

7.3.2.3 碰撞适应性要求

碰撞适应性要求见表5。

表 5 碰撞适应性

峰值加速度（m/s^2）	脉冲持续时间（ms）	碰撞次数	碰撞波形
100	16	1000	半正弦波

7.3.2.4 运输包装件跌落适应性要求

运输包装件跌落适应性要求见表6。

表 6 运输包装件跌落适应性

包装件质量m（kg）	跌落高度（mm）
m≤15	1000

15＜m≤30	800
30＜m≤40	600

7.3.3 电源适应性要求

一卡通终端可采用交流或者直流方式供电。

——采用交流电源供电时，在额定电压±10%范围内时，频率50～60Hz，终端应能正常工作；

——采用直流电源供电时，在额定电压±5%范围内，终端应能正常工作。

终端还应有掉电、过流、过压、短路、极性反接等保护措施。当电压恢复正常时，能自动恢复正常工作状态。

7.3.4 电磁兼容性要求

7.3.4.1 无线电骚扰

无线电骚扰限值应符合GB/T 9254.1的相关要求，并在终端标签或者说明书中指明A级或者B级。

7.3.4.2 抗扰度

抗扰度限值应符合GB/T 9254.2的相关要求。

7.3.5 可靠性要求

除特殊部件另有规定外，采用平均无故障工作时间衡量终端的可靠性水平，终端的平均无故障工作时间不小于15000h。

——卡座使用寿命应不低于1×10^5次；

——按键的使用寿命应不低于5×10^5次。

7.4 终端接触式技术要求

7.4.1 通则

本部分规定了终端接触部分的机电特性、逻辑接口及通信协议相关标准。所定义的IC卡特性遵从GB/T 16649.1、GB/T 16649.2、GB/T 16649.3、GB/T 16649.4，并根据实际需要及技术发展，做了一些必要调整。

终端接触部分的逻辑接口、通信协议应符合GB/T 16649.3的相关要求，且终端接触部分应支持T=0传输协议。

7.4.2 机械特性

7.4.2.1 接口设备

用于插入卡的接口设备应具备接收卡的能力，并具有以下特性：

——物理特性应符合 GB/T 16649.1 的规定；

——正面触点位置应符合 GB/T 16649.2 的规定。

定位的导轨和甲板（如果使用）不应损坏卡，特别是对印制在卡表面的相片、文字信息等区域。

接口设备上插入卡位置处，应配有一种机械设备，使得持卡人应在任何时候都能将卡插入或者拔出，如设备发生故障（如掉电）时取回卡。

7.4.2.2 触点压力

任何一个接口设备触点对相应的卡触点所施加的压力应在 0.2N～0.6N 之间。

7.4.2.3 触点分配

接口设备触点分配见表 7。

表 7 接口设备触点分配

触点	分配	触点	分配
C1	VCC	C5	GND
C2	RST	C6	不使用
C3	CLK	C7	I/O
注：C4 和 C8 不使用，在物理上可不存在。C6 是电隔离的。			

7.4.2.4 ICC 连接器的配置和要求

符合本文件的接口设备至少应配置两个 ICC 连接器。

a) 用于社会保障卡的应用ICC连接器；

b) 用于安全存取模块的安全ICC连接器。

7.4.3 电特性

7.4.3.1 测量约定

所有测量应在卡和接口设备之间的触点上进行，并以 GND 为参考。环境温度范围为 0℃～50℃。

所有流出终端的电流均为正值。

接口设备的工作电压为 5V 或者 3V，允差±5%。

7.4.3.2 输入/输出（I/O）

该触点作为输出端（传输模式）向卡传送数据，作为输入端（接收模式）从卡接收数据。在操作过程中，终端和卡不能同时处于传输模式，若万一发生此情况，I/O 触点的状态（电平）将处于不确定状态，但不应损坏终端。

当终端和卡都处于接收模式时，触点将处于高电平状态。为了达到这种状态，终端应在 VCC 上或者其他装置上连接一个上拉电阻。除非 VCC 加电并稳定在 8.4.2.6 中允许的范围内，终端不应将 I/O 置于高电平状态。

在任何情况下，均应将流入或者流出 I/O 触点的电流限定在±15mA 以内。具体模式如下：

a) 传输模式

在传输模式下，终端向卡传送数据，其 I/O 电特性见表 8。

表 8 传输模式下 I/O 电特征

符号	条件	最小值	最大值
V_{OH}	-20μA< I_{OH}< 20μA，VCC=最小值	0.8 ×VCC V	VCC V
V_{OL}	-1mA < I_{OL}<0 mA，VCC=最小值	0V	0.3V
t_R和 t_F	$C_{IN(ICC)}$ =30pF 最大	-	0.8μs

正负脉冲峰值	-	-0.25V	VCC + 0.25 V

b) 接收模式

除向卡传送数据时，终端应将其 I/O 信号驱动模式设置为接收模式。在接收模式下，当电源电压（VCC）在 7.4.3.6 中规定的范围内时，终端应能正确解释从卡发来的信号，其 I/O 电特性见表 9。

表 9 接收模式下 I/O 电特征

符号	最小值	最大值
V_{IH}	0.6×VCC V	VCC V
V_{IL}	0V	0.5V
t_R 和 t_F	-	1.2 μs

7.4.3.3 编程电压（VPP）

不要求终端产生 VPP。

7.4.3.4 时钟（CLK）

终端将产生一个 CLK 信号，其电特性见表 10。

表 10 CLK 电特征

符号	条件	最小值	最大值
V_{OH}	0 μA <I_{OH}<50 μA，VCC = 最小值	VCC - 0.5 V	VCC V
V_{OL}	-50 μA<I_{OL}< 0 μA，VCC = 最小值	0V	0.4V
t_R 和 t_F	$C_{IN\ (ICC)}$ = 30pF 最大	-	8%的时钟周期（μs）
正负脉冲峰值	-	-0.25 V	VCC + 0.25 V

频率范围在 1MHz～5MHz（对 A 类卡操作时）或 1MHz～4MHz（对 B 类卡操作时）之间，且在整个交易期间，其变化范围不应超过±1%。时钟占空因数应在其稳定运行周期的 45%～55%之间。

7.4.3.5 复位（RST）

终端产生一个 RST 信号，其电特性见表 11。

表 11 RST 电特征

符号	条件	最小值	最大值
V_{OH}	0 μA <I_{OH}<50 μA，VCC=最小值	VCC-0.5 V	VCC V
V_{OL}	-50 μA <I_{OL}<0 μA，VCC=最小值	0V	0.4V
t_R 和 t_F	$C_{IN\ (ICC)}$=30pF 最大	-	0.8 μs

正负脉冲峰值	-	-0.25V	VCC + 0.25 V

7.4.3.6 电源电压（VCC）

终端应带有保护电路以防止在误操作如对地或者V_{CC}短路时所造成的损坏。误操作既可能来源于内部，也可能来自外部接口如电源干扰、通讯链路故障等。

在卡的正常操作中，电流脉冲可在卡触点上引起 VCC 波动。电源应能中和小于 40nAs 且持续时间不超过 400ns 的电源波动，并在此时间内承受卡上 100mA 的电源消耗。

终端提供一个 VCC 信号，其电特性见表 12。

表 12 VCC 电特性

符号	条件	最小值	最大值
VCC	A类 B 类	4.6V 2.8V	5.4V 3.2V
ICC	A类，稳定输出 B 类，稳定输出	-	55mA 45mA
注：如果需要，终端应能够具有大于 55mA 的传输能力，但建议终端将稳定电流限制在 200mA 以内。			

7.4.3.7 触点电阻

在终端的整个设计寿命期间,触点电阻(在清洁的接口设备和清洁的标准卡触点间测量时)应小于500mΩ（参见GB/T 17554.3的测试方法）。

注：标准的卡触点可看作是在5.00μm的镍表面上的1.25μm镀金触点。

7.4.3.8 短路保护

当任何两个触点之间发生短路时，无论时间长短，终端都不应被损坏或者功能失常。如插入一块金属板或者带有金属性表面的卡。

接口设备所有的ICC连接器都应具有短路保护功能。

7.4.3.9 插入社会保障卡后，终端的加电和断电

插入社会保障卡后，当对终端进行加电或者断电时，触点的接口界面不应出现杂乱信号或者电源干扰，触点激活和释放的时序应分别符合GB/T 16649.3的规定。

7.4.4 接口设备在复位应答期间的操作

本条规定了接口设备在复位应答期间接收到卡回送字符后的相关操作。有关字符定义应符合GB/T 16649.3的规定。

7.4.4.1 TS-初始字符

终端应能够同时支持反向和正向逻辑约定，并接收卡回送的值为‘3B’或‘3F’的TS，但应拒绝接收其他TS值。

7.4.4.2 T0-格式字符

T0回送值正确且包含了所需的接口字符（TA1到TD1）和历史字符时，终端不应拒绝卡回送任何值。

7.4.4.3 接口字符 TA1 到 TC3

具体如下：

a) 接口字符TA1

终端不应拒绝卡回送 TA1=‘01’或‘11’（如果 T0 的 b5 位为‘1’），并在整个后续交易过程中继续使用缺省值 F=372 和 D=1；

注：如果回送 TA1，终端应能对其低半字节正确译码，并得出 D 的有效值 1、2、4 或 8。本文件以后的版本可能支持其他的 D 值，以提高 TTL 和卡之间的数据传送速率和选择其他协议类型。

b) 接口字符TB1

如果 T0 的 b6 位为‘1’，终端不应拒绝回送任何 TB1 的卡：如果 T0 的 b6 位为‘0’，则卡不回送 TB1，此时终端仍应继续卡片操作过程，且不提供 VPP，就像回送了 TB1=‘00’一样；

注：终端可保持 VPP 为静止状态。

c) 接口字符TC1

如果 T0 的 b7 位为‘0’，终端不应拒绝不回送 TC1 的卡，但如果终端接受了这样的卡，应能够继续卡片操作过程，就像回送了 TC1=‘00’一样；

注：应将 TC1 设置为卡可接受的最小值。TC1 取值过大将导致终端与卡之间的通讯缓慢，这样将延长交易时间。

d) 接口字符TD1

如果回送值正确且包含了所需的接口字符 TA2 到 TD2，终端不应拒绝这样的卡，即：其所回送 TD1 的高半字节为任意值且低半字节的值为‘0’或‘1’。终端应不拒绝回送其他 TD1 值的卡；

e) 接口字符TA2

如果终端在复位应答期间能够支持由卡通过 TA2 所指明的额外条件，它不应拒绝这样的卡，并应能立即使用这些条件；

f) 接口字符TB2

终端不应拒绝卡回送 TB2。但不论 TB2 是否回送、回送何值，终端均不应提供 VPP；

注：终端可保持 VPP 为静止状态。

g) 接口字符TC2

终端不应拒绝回送 TC2=‘10’的卡；

h) 接口字符TD2

如果回送值正确且包含了所需的接口字符 TA3 到 TD3，终端不应拒绝这样的卡，即其所回送 TD2 的高半字节为任意值且低半字节的值为‘1’、‘E’或‘F’。终端应拒绝卡回送其他的 TD2 值；

i) 接口字符TA3

如果此前 T=15 已存在，TD2 的 b5 位为‘0’，终端不应拒绝不回送 TA3 的卡。但如果终端接受了这样的卡，则应令 TA3=‘01’来继续卡片操作过程。终端应拒绝那些回送的 TA3 值不满足 GB/T 16649.3 相关要求的卡。

如果此前 T=15 不存在，终端不应拒绝正确回送接口字符 TA3 的卡；

j) 接口字符TB3和TC3

尽管 GB/T 16649.3 规定了社会保障卡只使用 T=0 的卡，但终端不应拒绝正确回送接口字符 TB3 和 TC3 的卡。

7.4.4.4 校验字符 TCK

在使用 T=0 协议且 T=15 不存在时，终端应拒绝回送了 TCK 的卡。如果卡回送了 TCK，终端应能对 TCK 进行计算。

GB/T 16649.3 对 TCK 的描述仅适用于那些支持 T=0 协议的卡。如果出于特殊原因，卡支持 T=14 协议，TCK 所遵循的条件应由该协议的规范确定。

7.4.5 接口设备在协商模式中的操作

在协商模式中，接口设备宜发起 PPS 请求，与卡协商后确定 F 和 D 的参数值。

7.4.6 终端与接口设备之间的数据交换

终端设备应能够接收卡一次返回 256 字节的数据及后续的状态码。

7.5 终端非接触式技术要求

7.5.1 通则

本部分规定了终端非接触式技术的相关要求，包括 PCD 和 PICC 之间的电气要求、传输协议、初始化和防冲突和性能要求。所定义的 IC 卡特性遵从 GB/T 42756.2、GB/T 42756.3、GB/T 42756.4，并根据实际需要及技术发展，做了一些必要的调整。

7.5.2 电气要求

7.5.2.1 射频功率和信号接口

具体如下：

a) 初始对话

PCD和PICC之间的初始对话通过下列连续操作进行：

——PCD的RF工作场激活PICC；

——PICC静待来自PCD的命令；

——PCD传输命令；

——PICC传输响应。

这些操作使用下列条款中规定的射频功率和信号接口。

b) 工作频率

RF工作频率（fc）：13.56MHz±7kHz。

c) 天线能量

1) 天线表面电磁场强度（Hmax）≤7.5A/m rms；

2) 天线表面发现方向在最大阅读距离处电磁场强度（Hmin）≥1.5A/m rms。

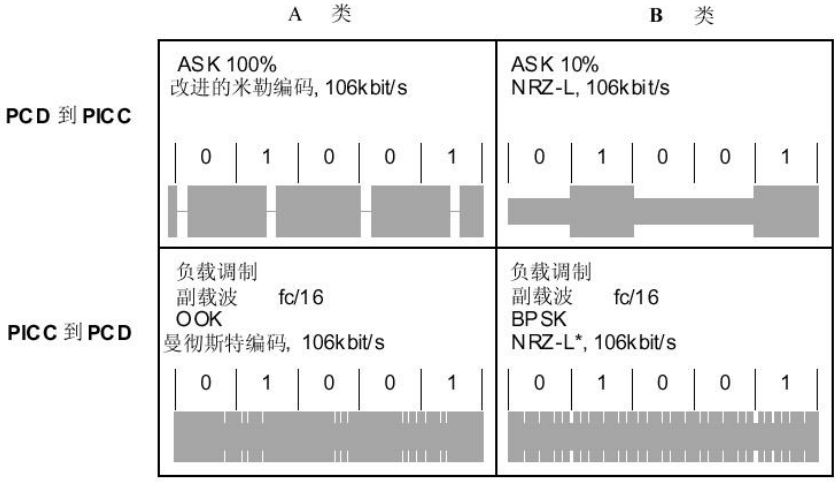
d) 信号接口

两种通信信号接口Type A和Type B在下列各条中予以描述。

在检测到Type A或Type B的PICC存在之前，PCD应选择两种调制方法之一。

在通信期间，直到PCD停止通信或PICC移走，只有一个通信信号接口可是有效的。后续序列可使用任一调制方法。

Type A、Type B接口的通信信号及以下几个部分描述概念示意如图4所示。



*也可能数据反相。

图 4 Type A、Type B 接口的通信信号举例

7.5.2.2 Type A 通信信号接口

具体如下：

a) PCD 到 PICC 调制输出

1) 比特率：fc/128（~106kbps）。

2) 调制方式：采用 ASK100%调制。

3) 调制系数：

PCD 场的包络线应单调递减到小于其初始值 HINITIAL 的 5%，并至少在 t2 时间内保持小于 5%。

如果 PCD 场的包络线不单调递减，则当前最大值和在当前最大值前通过相同值的时间之间的时间应不超过 0.5 μs。如果当前最大值大于 HINITIAL 的 5%，这种情况才适用。

上冲应保持在 HINITIAL 的 90%和 110%之内。

在 PCD 场超出 HINITIAL 的 5%之后和超出 HINITIAL 的 60%之前，PICC 应检测到“暂停（pause）结束”。

4) 位编码方式：改进的米勒编码；

5) 调制波形：应符合 GB/T 42756.2 的规定。

b) PICC 到 PCD 的通信采用副载波调制

1) 副载波频率：fc/16（~847kHz）；

2) 副载波调制方式：OOK 调制；

3) 位编码方式：曼彻斯特编码；

4) 副载波调制应符合 GB/T 42756.2 的规定。

7.5.2.3 Type B 通信信号接口

具体如下：

a) PCD 到 PICC 调制输出

1) 比特率：fc/128（~106kbps）；

2) 调制方式：采用 ASK10%调制；

3) 调制系数 8%-14%；

4) 编码方式：NRZ-L 编码；

5) 调制波形：应符合 GB/T 42756.2 的规定。

b) PICC 到 PCD 采用副载波调制。

1) 副载波频率： fc/16（~847KHz）；

2) 副载波调制方式：BPSK 调制；

3) 位编码方式：NRZ-L 编码；

4) 副载波调制应符合 GB/T 42756.2 的规定。

7.5.3 传输协议要求

传输协议应符合GB/T 42756.4的规定。

7.5.4 初始化和防冲突

7.5.4.1 轮询

为了检测到是否有PICC进入到PCD的有效作用区域，PCD重复的发出请求信号，并判断是否有响应。请求信号应是REQA和REQB，附加GB/T 42756.3其它部分描述的代码。A型卡和B型卡的命令和响应不能相互干扰。

7.5.4.2 Type A 的初始化和防冲突

当一个Type A PICC到达了非接识读区域的作用范围内，并且有足够的供应电能，卡就开始执行一些预置的程序后， PICC进入闲置状态。处于“闲置状态”的PICC不能响应PCD传输给其他PICC的数据。PICC在“闲置状态”接收到有效的REQA命令，则回送对请求的应答字ATQA。当PICC对REQA命令作了应答后，PICC处于READY状态。PCD识别出在作用范围内至少有一个PICC存在。通过发送SELECT命令启动“二进制检索树”防碰撞算法，选出一个PICC，对其进行操作。

7.5.4.3 Type B 的初始化和防冲突

当一个Type B PICC被置入PCD的作用范围内，PICC执行一些预置程序后进入“闲置状态”，等待接收有效的REQB命令。对于Type B PICC，通过发送REQB命令，可直接启动Slotted ALOHA防碰撞算法选出一张卡，对其进行操作。

7.5.5 性能要求

7.5.5.1 感应高度

终端应保证在外壳0~30mm高度内都可正常感应到卡片，没有盲区。

7.5.5.2 感应范围

终端应保证在外壳标注感应区域内，卡片以任意角度水平摆放，终端都可正常感应卡片。

7.5.5.3 卡片与外壳夹角

终端应保证卡片与外壳平面夹角小于10°时均能正常感应卡片。

7.6 终端条码识读技术要求

7.6.1 环境适应性要求

7.6.1.1 光照环境适应性

条码识读终端在不同光照环境下应满足以下要求：

——在户外阳光照射不高于86112 Lux的照度下应能正常工作；

——在室内不高于4842 Lux的照度下应能正常工作。

7.6.1.2 防尘防水适应性

户外使用场景的设备应能在雨雪等恶劣环境下正常使用，防护能力应满足IP54等级。

7.6.2 性能要求

7.6.2.1 解码能力

条码识读模块应能识读一维码和二维码。

7.6.2.2 精度

条码识读模块识读条码的精度应满足表13的要求。

表 13 精度

码制	设备形态	
	手持式条码扫描设备	固定式条码扫描设备
二维码	纸质码10mil/电子码15mil	
一维码		

7.6.2.3 景深

条码识读模块对条码图在Z轴方向上（即摄像头轴向）的最大识读距离和最小识读距离的差值应满足表14的要求。

表 14 景深

码制	设备形态	
	手持式条码扫描设备	固定式条码扫描设备
二维码	连续景深≫80mm	连续景深≫60mm
一维码		

7.6.2.4 识读速度

条码识读模块对条码图的识读速度应满足表15的要求。

表 15 识读速度

码制	设备形态	
	手持式条码扫描设备	固定式条码扫描设备
二维码	<1s	
一维码		

7.6.2.5 识读角度

条码识读模块对条码图的识读角度应满足表16的要求。

表 16 识读角度

码制	设备形态	
	手持式条码扫描设备	固定式条码扫描设备
二维码	偏转角：-30°～30° 旋转角：-180°～180°	
一维码	偏转角：-30°～30°	

7.6.2.6 识读出错率

条码识读模块对条码图的识读出错率应满足表17的要求。

表 17 识读出错率

码制	设备形态	
	手持式条码扫描设备	固定式条码扫描设备
二维码	<0.01%	
一维码		

7.6.2.7 纠错能力

条码识读模块识读低品质条码图的拒读率应不大于15%，同时不应误读。低品质类型主要包括打印间断、倾斜、磨损、畸变（胖瘦畸变、镜像码、污损码、渐变码）等。

7.6.2.8 移动识读能力

条码识读模块对条码图，分别沿X轴、Y轴方向进行移动识读，在准确识读的情况下，其移动识读速度应不低于表18的要求。

表 18 移动识读速度

码制	设备形态	
	手持式条码扫描设备	固定式条码扫描设备
二维码	10cm/s	
一维码		

附 录 A
（规范性）
一卡通终端基础接口

A.1 通则

本附录描述了一卡通终端的基础编程接口。

基础接口是提供给主机上的应用程序用来与社会保障卡进行交互操作的函数集。

基础接口的具体表现形式应包括：

a) 可以在 32 位或者 64 位 Windows 环境下（Windows XP 及以上各版本）运行的动态链接库（SSSE32.DLL）；

b) 可以在 Unix/Linux 环境下运行的动态链接库（SSSE32.SO）；

c) 可以在安卓环境下运行的动态链接库（SSSE32.SO）；

d) 可以在基于特定硬件平台上的动态链接库（SSSE32.SO 或者其他）。

上述所有基础接口应具有本文件所规定的统一动态链接库名称、函数名称、参数类型和顺序。

在以下的描述中，使用 C 语言格式来说明基础接口中的函数。

A.2 “打开设备“函数

函数：

long ICC_Reader_Open（char* dev_Name）

功能：

该函数通知主机操作系统打开与一卡通终端所对应的终端设备端口，以便两者建立通信的逻辑关系。

参数说明：

dev_Name：设备名称。取值范围“AUTO”、“COMn”、“USBn”，其中，“n”的取值范围为1~9。

返回值：

若正常，返回值为不小于0的设备句柄；反之返回值为状态码，其含义见A.12。

A.3 “关闭设备”函数

函数：

long ICC_Reader_Close（long ReaderHandle）

功能：

该函数通知操作系统关闭所指定的设备。

参数说明：

ReaderHandle：设备句柄。

返回值：

返回值含义见A.12。

A.4 “卡上电”或“热复位”函数

函数：

long ICC_Reader_PowerOn(long ReaderHandle, unsigned char ICC_Slot_No, unsigned char* Response）

功能：

该函数要求一卡通终端对 ICC 进行冷复位，若冷复位失败一卡通终端应启动一个热复位。

参数说明：

a) ReaderHandle：设备句柄；

b) ICC_Slot_No：ICC连接器号；用户卡（接触卡）连接器号 0x0n，用户卡（非接触卡）连接器号为0x3n，安全存取模块连接器号0x1n，其中“n”的取值范围为‘1’～‘F’；

c) Response：指向存放响应数据的存储区的指针。

返回值：

如果对 ICC 复位成功，则在 Response 的存储区中返回 ICC 的复位应答字节，返回值为存储区中的字节数；返回值小于 0 为状态码，其含义见 A.12。

A.5 “卡下电”函数

函数：

long ICC_Reader_PowerOff(long ReaderHandle，unsigned char ICC_Slot_No)

功能：

该函数要求一卡通终端撤销与 ICC 之间的电气连接。

参数说明：

a) ReaderHandle：设备句柄；

b) ICC_Slot_No：ICC连接器号。

返回值：

如果该函数成功执行，则返回值为 0；返回值小于 0 为状态码，其含义见 A.12。

A.6 “获取卡片状态”函数

函数：

long ICC_Reader_GetStatus(long ReaderHandle，unsigned char ICC_Slot_No)

功能：

查询有无卡以及卡片当前状态信息。

参数说明：

a) ReaderHandle：设备句柄；

b) ICC_Slot_No：ICC连接器号。

返回值：

返回 0 表示有卡且已上电；返回值小于 0 为状态码，其含义见 A.12。

A.7 “应用命令”函数

函数：

long ICC_Reader_Application（long ReaderHandle，unsigned char ICC_ Slot _No，
long Lenth_of_Command_APDU，unsigned char* Command_APDU，
unsigned char* Response_APDU）

功能：

该函数用于将符合 ANSI ISO/IEC 7816-4：1995 中所规定的基本和特殊功能的行业间交换用命令发送给指定的 ICC 连接器，并获取对应的响应。

参数说明：

a) ReaderHandle：设备句柄；

b) ICC_Slot_No：ICC连接器号；

c) Lenth_of_Command_APDU：其值为Command_APDU所指向缓冲区中的字节数；

d) Command_APDU：指向存放命令的缓冲区的指针；

e) Response_APDU：指向存放响应数据的存储区的指针（包括SW1 SW2）。

返回值：

如果函数执行成功，则在 Response_APDU 的存储区中返回响应数据，函数返回值为存储区中的字节数；返回值小于 0 为状态码，其含义见 A.12，Response_APDU 的存储区无任何数据。

A.8 “取信息”函数

函数：

long ICC_Reader_Libinfo（char* info）

功能：

该函数取得当前函数库的厂家信息。

参数说明：

info：指向存放厂家信息的存储区的指针。

厂家信息的存储格式见表 A.1。

表 A.1 厂家信息的存储格式

第 1～16 字符	第 17～30 字符	第 31～32 字符
厂家名称（不足补空格）	设备型号或系列号（不足补空格）	函数库版本号

A.9 “取终端设备号”函数

函数：

long ICC_Reader_GetDevID（long ReaderHandle, char *DevID）

功能：

该函数取得该终端的终端设备号。

参数说明：

a) ReaderHandle：设备句柄；

b) DevID：指向存放终端设备号的存储区的指针。

返回值的含义见 A.12。

A.10 “条码识读”函数

函数：

long ICC_Reader_GetQRCode (long ReaderHandle，int TimeOut，char *ScanCode)

功能：

通过一卡通终端上的扫码器，扫描获取条码信息。

参数说明：

a) ReaderHandle：设备句柄；

b) TimeOut：超时时间（最大25s）；

c) ScanCode：读出的数据。

返回值的含义见 A.12。

A.11 “获取密码键盘输入”函数

函数：

long ICC_Reader_GetPin(long ReaderHandle，int type，int TimeOut，unsignedchar *keys)

功能：

通过一卡通终端上的密码键盘（含内置或外置密码键盘），获取密码键盘输入密码。

参数说明：

a) ReaderHandle：设备句柄；

b) type：语音提示类别（1-请输入密码，2-请输入旧密码，3-请输入新密码，4-请再次输入密码）；

c) TimeOut：输入密码超时等待时间（最大30s）；

d) keys：从密码键盘输入的密码字符，ASCII码字符。

返回值的含义见 A.12。

A.12 函数返回值

高级编程接口 C 语言函数返回值见表 A.2。

表 A.2 高级编程接口 C 语言函数返回值

应用编程的标识符	返回值	含义
IFD_OK	0	执行成功

IFD_ICC_TypeError	-1	卡片类型不对
IFD_ICC_NoExist	-2	无卡
IFD_ICC_NoPower	-3	有卡未上电
IFD_ICC_NoResponse	-4	卡片无应答
IFD_ConnectError	-11	一卡通终端连接错
IFD_UnConnected	-12	未建立连接（没有执行打开设备函数）
IFD_BadCommand	-13	（动态库）不支持该命令
IFD_ParameterError	-14	（发给动态库的）命令参数错
IFD_CheckSumError	-15	信息校验和出错

附 录 B
（规范性）
一卡通终端应用接口

B.1 通则

附录 B 描述的是在附录 A 的基础上，根据社会保障卡一卡通的要求，统一一卡通终端与一卡通应用系统及其客户端的高级编程接口。

适用于一卡通终端关联的相关一卡通应用系统接口的研发、集成及维护。

应用接口的具体表现形式应包括：

a) 可以在 32 位或 64 位 Windows 环境下（Windows XP 及以上各版本）运行的动态链接库（SSCardDriver.DLL），对应的 ActiveX 控件版本为：SSCARD，CLSID=D9532F10-603B-4BF7-87AE-F4130EF43553，对应的 Websocket 控件为：Websocket 服务；

b) 可以在 Unix/Linux 环境下运行的动态链接库（SSCardDriver.SO）；

c) 可以在安卓环境下运行的动态链接库（SSCardDriver.SO）；

d) 可以在基于特定硬件平台上的动态链接库（SSCardDriver.SO 或其他）。

上述所有基础接口应具有本文件所规定的统一动态链接库名称、函数名称、参数类型和顺序。

在以下的描述中，使用 C 语言格式来说明应用接口中的函数。

B.2 “读基本信息”函数

B.2.1 iReadCardBas“读基本信息”

具体如下：

a) 函数定义

读基本信息接口函数定义见表 B.1。在进行任何对社会保障卡操作前，应先调用此函数。

表 B.1 读基本信息接口函数定义

函数名称	读基本信息					
语法	long iReadCardBas(int iType, char* pOutInfo)					
功能描述	选择社会保障卡社会保障系统环境后，通过PSAM卡对社会保障卡进行内部认证，通过后将卡内的基本信息读出返回。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pOutInfo	OUT	字符串	1024	读出数据或返回错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

表示执行本函数时操作卡的类型，定义如下：1-接触式操作卡；2-非接触式操作卡；3-自动寻卡，接触式操作卡优先；4-自动寻卡，非接触式操作卡优先。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数 char* pOutInfo 为读出的卡内基本信息各数据项，依次为：发卡地区行政区划代码（卡识别码前 6 位）、社会保障号码、卡号、卡识别码、姓名、卡复位信息（仅取历史字节）、规范版本、发卡日期、卡有效期、终端机编号、终端设备号。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数 char* pOutInfo 为错误信息描述。

注：当没有终端设备号时，终端设备号返回空字符串。

B.2.2 iReadCardBas_HSM_Step1 “基于加密机的读基本信息（步骤一）”

具体如下：

a) 函数定义

基于加密机的读基本信息（步骤一）接口函数定义见表 B.2。

表 B.2 基于加密机的读基本信息（步骤一）接口函数定义

函数名称	基于加密机的读基本信息（步骤一）					
语法	longiReadCardBas_HSM_Step1(int iType, char* pOutInfo)					
功能描述	选择社会保障系统环境后，返回内部认证和外部认证所需信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pOutInfo	OUT	字符串	1024	返回认证信息或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数 char* pOutInfo 为读出的卡内内部认证和外部认证的计算数据，依次为：发卡地区行政区划代码（卡识别码前 6 位）、卡复位信息（仅取历史字节）、算法标识、卡识别码、内部认证过程因子、内部认证鉴别所需的原始信息、外部认证过程因子、外部认证鉴别所需的原始信息，其中外部认证相关数据项全部不为空或全部为空。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数 char* pOutInfo 为错误信息描述。

注：当外部认证相关数据项为空时，表示不做外部认证。

B.2.3 iReadCardBas_HSM_Step2 “基于加密机的读基本信息（步骤二）”

具体如下：

a) 函数定义

基于加密机的读基本信息（步骤二）接口函数定义见表 B.3。

表 B.3 基于加密机的读基本信息（步骤二）接口函数定义

函数名称	基于加密机的读基本信息（步骤二）					
语法	longiReadCardBas_HSM_Step2(char *pKey, char* pOutInfo)					
功能描述	根据加密机返回的内部认证和外部认证结果数据对社会保障卡进行内部认证和外部认证，通过后将卡内的基本信息读出返回。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pKey	IN	字符串	128	加密机返回的内部认证和外部认证结果数据

	2	pOutInfo	OUT	字符串	1024	读出数据或返回错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pKey

加密机返回的内部认证和外部认证结果数据，依次为：内部认证结果数据（即内部认证鉴别数据（16 位）和内部认证鉴别所需的原始信息（16 位）拼接组成）、外部认证结果数据（即外部认证鉴别数据（16 位）和外部认证鉴别所需的原始信息（16 位）拼接组成）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

注：如果不做外部认证，则后面一个参数都为空字符串。

2) 输出参数 pOutInfo

定义同 B.2.1 b）2）。

注：当没有 PSAM 卡时，终端机编号返回 12 个 0，即 6 个 0x00 对应的字符。

当没有终端设备号时，终端设备号返回空字符串。

B.3 “通用读卡”函数

B.3.1 iReadCard“通用读卡”

具体如下：

a) 函数定义

通用读卡接口函数定义见表 B.4。

表 B.4 通用读卡接口函数定义

函数名称	通用读卡					
语法	long iReadCard (int iType, int iAuthType, char* pCardInfo, char* pFileAddr, char* pOutInfo)					
功能描述	根据所需读取的信息进行认证后读出卡内指定文件的信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	iAuthType	IN	整数	4	认证方式
	3	pCardInfo	IN	字符串	128	卡基本信息
	4	pFileAddr	IN	字符串	1024	文件名及数据项
	5	pOutInfo	OUT	字符串	1024*20	读出数据或返回错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 iAuthType

当文件的读控制受 PIN 或 RK 密钥保护时，该参数用于指定读控制认证方式，定义如下：1-PIN 校验；2-RK 密钥认证。此参数只在文件的读控制权限为“PIN 或 RK”时有效。

3) 输入参数 pCardInfo

该参数用于传入卡的基本信息，依次为：卡识别码、卡号。各数据项之间以“|”分割，且最后一个

数据项以“|”结尾。

4) 输入参数 pFileAddr

该参数用于指定需要读出的文件和文件下的数据项。

文件名由 ADF 的文件标识符和 AEF 的文件标识符组成，如 SSSEEF05、DF01EF06。文件名及各数据项之间以“|”分隔，且最后一个数据项以“|”结尾。数据项以记录标识符表示，若同一数据项由多条记录组成，则在数据项后加“:”再加记录号表示。不同文件之间以“$”分隔，且最后应以“$”结束。

当所要读出的文件为循环文件时，如果只指定文件名，函数将读出该文件下的所有记录数据；如果同时给出指定文件名和记录号，函数将读出该文件下的记录号所对应的记录数据。每条记录之间以“|”分隔，每条记录里面的数据项之间以“^”分隔，最后一个数据项以“^”结尾，最后一条记录以“|”结尾。

当所要读出的文件为透明文件时，只需指定文件名，函数将读出该文件下的所有文件数据。

5) 输出参数 pOutInfo

当函数执行成功时，该输出参数为读出的由输入参数指定的各数据项，其格式与输入参数 pFileAddr 严格对应且分隔符完全一致。

当函数执行失败时，该输出参数为错误信息描述。

B.3.2 iReadCard_HSM_Step1 “基于加密机的通用读卡（步骤一）”

具体如下：

a) 函数定义

基于加密机的通用读卡（步骤一）接口函数定义见表 B.5。

表 B.5 基于加密机的通用读卡（步骤一）接口函数定义

函数名称	基于加密机的通用读卡（步骤一）					
语法	long iReadCard_HSM_Step1(int iType, char* pCardInfo, char* pFileAddr, char* pOutInfo)					
功能描述	根据所需读取的信息确定需要认证的密钥，并返回认证所需信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pFileAddr	IN	字符串	1024	文件名及数据项
	4	pOutInfo	OUT	字符串	1024	返回认证信息或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输入参数 pFileAddr

定义同 B.3.1 b）4）。

本函数只允许对一个文件进行操作。若传入多个文件则只对第一个文件进行操作，后续内容将被忽略。

4) 输出参数 pOutInfo

当函数执行成功时，该输出参数为需要计算的认证信息，依次为：算法标识、外部认证密钥地址、外部认证过程因子（从卡片获得的随机数）、外部认证鉴别所需的原始信息（从卡片获得的随机数）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数为错误信息描述。

B.3.3 iReadCard_HSM_Step2“基于加密机的通用读卡（步骤二）”

具体如下：

a) 函数定义

基于加密机的通用读卡（步骤二）接口函数定义见表 B.6。

表 B.6 基于加密机的通用读卡（步骤二）接口函数定义

函数名称	基于加密机的通用读卡（步骤二）					
语法	long iReadCard_HSM_Step2(char* pKey, char* pOutInfo)					
功能描述	根据加密机返回的结果数据对社会保障卡进行外部认证，通过后读出卡内指定文件的信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pKey	IN	字符串	32	加密机返回的结果数据
	2	pOutInfo	OUT	字符串	1024*20	读出数据或返回错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pKey

该参数用于传入由加密机返回的结果数据，由鉴别数据（过程因子分散后加密原始信息的密文）和鉴别所需的原始信息拼接组成，总长度为 32 位。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数为读出的由 iReadCard_HSM_Step1 函数输入参数 pFileAddr 指定的各数据项，其格式严格对应且分隔符完全一致。

当函数执行失败时，该输出参数为错误信息描述。

B.4 “通用写卡”函数

B.4.1 iWriteCard“通用写卡”

具体如下：

a) 函数定义

通用写卡接口函数定义见表 B.7。

表 B.7 通用写卡接口函数定义

函数名称	通用写卡					
语法	long iWriteCard (int iType, char* pCardInfo, char* pFileAddr, char* pWriteData, char* pOutInfo)					
功能描述	根据所需写入的信息进行外部认证后写入指定文件的信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型

	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pFileAddr	IN	字符串	1024	文件名及数据项
	4	pWriteData	IN	字符串	1024*20	写入数据项信息
	5	pOutInfo	OUT	字符串	1024	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输入参数 pFileAddr

该参数用于指定需写入的文件和文件下的数据项。

文件名由 ADF 的文件标识符和 AEF 的文件标识符组成，如 SSSEEF05、DF01EF06。文件名及各数据项之间以“|”分隔，且最后一个数据项以“|”结尾。数据项以记录标识符表示，若同一数据项由多条记录组成，则在数据项后加“:”再加记录号表示。不同文件之间以“$”分隔，且最后应以“$”结束。

当写入文件为循环文件时，只需指定文件名，函数将新增记录；当写入的文件为透明文件时，只需指定文件名，函数将更新全部文件数据。

4) 输入参数 pWriteData

该参数用于传入需写入的数据项信息时，其格式与输入参数 pFileAddr 严格对应且分隔符完全一致。

5) 输出参数 pOutInfo

当函数执行成功时，该输出参数为空字符串。

当函数执行失败时，该输出参数为错误信息描述。

B.4.2 iWriteCard_HSM_Step1“基于加密机的通用写卡（步骤一）”

具体如下：

a) 函数定义

基于加密机的通用写卡（步骤一）接口函数定义见表 B.8。

表 B.8 基于加密机的通用写卡（步骤一）接口函数定义

函数名称	基于加密机的通用写卡（步骤一）					
语法	long iWriteCard_HSM_Step1(int iType, char* pCardInfo, char* pFileAddr, char* pOutInfo)					
功能描述	根据所需写入的信息确定需要认证的密钥，并返回认证所需信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pFileAddr	IN	字符串	1024	文件名及数据项

	4	pOutInfo	OUT	字符串	1024	返回认证信息或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输入参数 pFileAddr

定义同 B.4.1 b）3）。

本函数只允许对一个文件进行操作。若传入多个文件则只对第一个文件进行操作，后续内容将被忽略。

4) 输出参数 pOutInfo

当函数执行成功时，该输出参数为需要计算的认证信息，依次为：算法标识、外部认证密钥地址、外部认证过程因子（从卡片获得的随机数）、外部认证鉴别所需的原始信息（从卡片获得的随机数）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数为错误信息描述。

B.4.3 iWriteCard_HSM_Step2 “基于加密机的通用写卡（步骤二）”

具体如下：

a) 函数定义

基于加密机的通用写卡（步骤二）接口函数定义见表 B.9。

表 B.9 基于加密机的通用写卡（步骤二）接口函数定义

函数名称	基于加密机的通用写卡（步骤二）					
语法	long iWriteCard_HSM_Step2(char* pKey, char* pWriteData, char* pOutInfo)					
功能描述	根据加密机返回的结果数据对社会保障卡进行外部认证，通过后写入卡内指定文件的信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pKey	IN	字符串	32	加密机返回的结果数据
	2	pWriteData	IN	字符串	1024*20	写入数据项信息
	3	pOutInfo	OUT	字符串	1024	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pKey

定义同 B.3.3 b）1）。

2) 输入参数 pWriteData

该参数用于传入要写入的数据项信息，其格式与 iWriteCard_HSM_Step1 函数输入参数 pFileAddr 严格对应且分隔符完全一致。

3) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.5 “PIN校验”函数

B.5.1 iVerifyPIN“PIN 校验”

具体如下：

a) 函数定义

PIN 校验接口函数定义见表 B.10。

表 B.10 PIN 校验接口函数定义

函数名称	PIN 校验					
语法	long iVerifyPIN(int iType, char* pOutInfo)					
功能描述	校验PIN。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.6 “PIN修改”函数

B.6.1 iChangePIN“PIN 修改”

具体如下：

a) 函数定义

PIN 修改接口函数定义见表 B.11。

表 B.11 PIN 修改接口函数定义

函数名称	PIN 修改					
语法	long iChangePIN(int iType, char* pOutInfo)					
功能描述	修改PIN。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.7 “PIN重置”函数

B.7.1 iReloadPIN“PIN 重置”

具体如下：

a) 函数定义

PIN 重置接口函数定义见表 B.12。

表 B.12 PIN 重置接口函数定义

函数名称	PIN 重置					
语法	long iReloadPIN(int iType, char* pCardInfo, char* pOutInfo)					
功能描述	重置PIN。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.7.2 iReloadPIN_HSM_Step1“基于加密机的 PIN 重置（步骤一）”

具体如下：

a) 函数定义

基于加密机的 PIN 重置（步骤一）接口函数定义见表 B.13。

表 B.13 基于加密机的 PIN 重置（步骤一）接口函数定义

函数名称	基于加密机的 PIN 重置（步骤一）					
语法	long iReloadPIN_HSM_Step1(int iType, char* pCardInfo, char* pOutInfo)					
功能描述	获取新PIN，返回所需的认证信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pOutInfo	OUT	字符串	512	返回认证信息或错误信息

返回值	0表示成功；非0表示失败。

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输出参数 pOutInfo

定义同 B.4.2 b）4）。

B.7.3 iReloadPIN_HSM_Step2 “基于加密机的 PIN 重置（步骤二）”

具体如下：

a) 函数定义

基于加密机的 PIN 重置（步骤二）接口函数定义见表 B.14。

表 B.14 基于加密机的 PIN 重置（步骤二）接口函数定义

函数名称	基于加密机的 PIN 重置（步骤二）					
语法	long iReloadPIN_HSM_Step2(char* pKey, char* pOutInfo)					
功能描述	进行认证，返回安全报文计算数据。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pKey	IN	字符串	32	加密机返回的结果数据
	2	pOutInfo	OUT	字符串	1024	返回安全报文计算数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pKey

定义同 B.3.3 b）1）。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数为需要由加密机计算的安全报文数据，依次为：算法标识、安全报文计算密钥地址、安全报文计算过程因子（从卡片获得的随机数）、APDU 命令头、APDU 命令明文数据（新 PIN）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数为错误信息描述。

B.7.4 iReloadPIN_HSM_Step3“基于加密机的 PIN 重置（步骤三）”

具体如下：

a) 函数定义

基于加密机的 PIN 重置（步骤三）接口函数定义见表 B.15。

表 B.15 基于加密机的 PIN 重置（步骤三）接口函数定义

函数名称	基于加密机的 PIN 重置（步骤三）
语法	long iReloadPIN_HSM_Step3(char* pKey, char* pOutInfo)

功能描述	完成PIN重置。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pKey	IN	字符串	50	安全报文数据
	2	pOutInfo	OUT	字符串	1024	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pKey

该参数用于传入由加密机计算的安全报文数据，由命令头、加密数据和 MAC 拼接组成，总长度为 34 位（DES 算法）或 50 位（SSF33/SM4 算法）。

2) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.8 “PIN解锁”函数

B.8.1 iUnblockPIN“PIN 解锁”

具体如下：

a) 函数定义

PIN 解锁接口函数定义见表 B.16。

表 B.16 PIN 解锁接口函数定义

函数名称	PIN 解锁					
语法	long iUnblockPIN(int iType, char* pCardInfo, char* pOutInfo)					
功能描述	解锁PIN。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.8.2 iUnblockPIN_HSM_Step1 “基于加密机的 PIN 解锁（步骤一）”

具体如下：

a) 函数定义

基于加密机的 PIN 解锁（步骤一）接口函数定义见表 B.17。

表 B.17 基于加密机的 PIN 解锁（步骤一）接口函数定义

函数名称	基于加密机的 PIN 解锁（步骤一）					
语法	longiUnblockPIN_HSM_Step1(int iType, char* pCardInfo, char* pOutInfo)					
功能描述	获得所需的认证信息。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pOutInfo	OUT	字符串	512	返回认证信息或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输出参数 pOutInfo

定义同 B.4.2 b）4）。

B.8.3 iUnblockPIN_HSM_Step2 “基于加密机的 PIN 解锁（步骤二）”

具体如下：

a) 函数定义

基于加密机的 PIN 解锁（步骤二）接口函数定义见表 B.18。

表 B.18 基于加密机的 PIN 解锁（步骤二）接口函数定义

函数名称	基于加密机的 PIN 解锁（步骤二）					
语法	long iUnblockPIN_HSM_Step2(char* pKey, char* pOutInfo)					
功能描述	进行认证，返回安全报文计算数据。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pKey	IN	字符串	32	加密机返回的结果数据
	2	pOutInfo	OUT	字符串	1024	返回安全报文计算数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pKey

定义同 B.3.3 b）1）。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数为需要由加密机计算的安全报文数据，依次为：算法标识、安全

报文计算密钥地址、安全报文计算过程因子（从卡片获得的随机数）、APDU 命令头、APDU 命令明文数据（空字符串）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数为错误信息描述。

B.8.4 iUnblockPIN_HSM_Step3 “基于加密机的 PIN 解锁（步骤三）”

具体如下：

a) 函数定义

基于加密机的 PIN 解锁（步骤三）接口函数定义见表 B.19。

表 B.19 基于加密机的 PIN 解锁（步骤三）接口函数定义

函数名称	基于加密机的 PIN 解锁（步骤三）					
语法	long iUnblockPIN_HSM_Step3(char* pKey, char* pOutInfo)					
功能描述	完成PIN解锁。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pKey	IN	字符串	18	安全报文数据
	2	pOutInfo	OUT	字符串	1024	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pKey

该参数用于传入由加密机计算的安全报文数据，由命令头和 MAC 拼接组成，总长度为 18 位。

2) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.9 “消费交易”函数

B.9.1 iDoDebit“消费交易”

具体如下：

a) 函数定义

消费交易接口函数定义见表 B.20。

表 B.20 消费交易接口函数定义

函数名称	消费交易					
语法	long iDoDebit(int iType, char* pCardInfo, char* pPayInfo, char* pOutInfo)					
功能描述	执行社会保障卡消费交易并写入消费记录。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pPayInfo	IN	字符串	512	消费信息
	4	pOutInfo	OUT	字符串	512	返回交易验证数据或错误信息

返回值	0表示成功；非0表示失败。

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输入参数 pPayInfo

该参数用于传入消费相关信息，依次为：本次消费总金额(小于 42949672.95 的小数，小数点后保留两位)、个人账户交易金额和统筹基金支付金额相加的总金额（小于 42949672.95 的小数，小数点后保留两位）、交易时间（格式为 YYYYMMDDHHMMSS）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

4) 输出参数 pOutInfo

当函数执行成功时，该输出参数为交易验证码及相关信息，依次为：算法标识、密钥地址、交易金额（转换成十六进制向卡片发送命令时的后两个金额拼接组成）、交易类型、终端机编号、终端交易序号、交易时间（格式为 YYYYMMDDHHMMSS）、交易验证码（TAC）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数为错误信息描述。

B.9.2 iDoDebit_HSM _Step1“基于加密机的消费交易（步骤一）”

具体如下：

a) 函数定义

基于加密机的消费交易（步骤一）接口函数定义见表 B.21。

表 B.21 基于加密机的消费交易（步骤一）接口函数定义

函数名称	基于加密机的消费交易（步骤一）					
语法	long iDoDebit_HSM_Step1(int iType, char* pCardInfo, char* pPayInfo, char* pOutInfo)					
功能描述	执行社会保障卡消费交易初始化命令并返回交易认证相关数据					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pCardInfo	IN	字符串	128	卡基本信息
	3	pPayInfo	IN	字符串	512	消费信息
	4	pOutInfo	OUT	字符串	512	返回交易认证数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输入参数 pCardInfo

定义同 B.3.1 b）3）。

3) 输入参数 pPayInfo

定义同 B.9.1 b）3）。

4) 输出参数 pOutInfo

当函数执行成功时，该输出参数为用于计算 MAC1 的相关交易认证数据，依次为：算法标识、密钥地址、伪随机数、医疗消费交易序号、交易金额（转换成十六进制向卡片发送命令时的后两个金额拼接组成）、交易类型、终端机编号、交易时间（格式为 YYYYMMDDHHMMSS）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数为错误信息描述。

注：当没有 PSAM 卡时，终端机编号返回 12 个 0，即 6 个 0x00 对应的字符。

B.9.3 iDoDebit_HSM _Step2“基于加密机的消费交易（步骤二）”

具体如下：

a) 函数定义

基于加密机的消费交易（步骤二）接口函数定义见表 B.22。

表 B.22 基于加密机的消费交易（步骤二）接口函数定义

函数名称	基于加密机的消费交易（步骤二）					
语法	long iDoDebit_HSM_Step2 (char* pKey, char* pOutInfo)					
功能描述	完成消费交易写入消费记录					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pKey	IN	字符串	128	交易认证数据
	2	pOutInfo	OUT	字符串	1024	返回交易验证数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pKey

该参数用于传入由加密机计算的交易认证数据，依次为：终端交易序号、交易时间、MAC1。各数据项之间以 “|”分割，且最后一个数据项以“|”结尾。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数为交易验证码及相关信息，依次为：MAC2、算法标识、密钥地址、交易金额（转换成十六进制向卡片发送命令时的后两个金额拼接组成）、交易类型、终端机编号、终端交易序号、交易时间（格式为 YYYYMMDDHHMMSS）、交易验证码（TAC）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

当函数执行失败时，该输出参数为错误信息描述。

B.10 “读消费交易记录”函数

B.10.1 iReadDebitRecord“读消费交易记录”

具体如下：

a) 函数定义

读消费交易记录接口函数定义见表 B.23。

表 B.23 读取消费交易记录接口函数定义

函数名称	读消费交易记录

语法	long iReadDebitRecord(int iType, char* pOutInfo)					
功能描述	读取消费交易记录。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
	2	pOutInfo	OUT	字符串	2048	返回交易记录或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

定义同 B.2.1 b）1）。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数为读出的交易记录，每条记录由交易序号、终端机编号、交易时间（格式为 YYYYMMDDHHMMSS）、本次消费总金额、个人账户交易金额和统筹基金支付金额相加的总金额组成。每条记录之间以“|”分隔，每条记录里面的数据项之间以“^”分隔，最后一个数据项以“^”结尾，最后一条记录以“|”结尾。

当函数执行失败时，该输出参数为错误信息描述。

B.11 证书应用函数

B.11.1 PKI_SignData“签名”

具体如下：

a) 函数定义

签名接口函数定义见表 B.24。

表 B.24 签名接口函数定义

函数名称	签名					
语法	long PKI_SignData(int iFile, char* pInData, char* pOutInfo)					
功能描述	对输入的数据进行数字签名					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iFile	IN	整数	4	证书类型
	2	pInData	IN	字符串	6*1024	待签名原文数据
	3	pOutInfo	OUT	字符串	4*1024	返回签名数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iFile

表示签名时使用的证书类型，定义如下：12-社保签名证书，22-地方签名证书。

2) 输入参数 pInData

待签名的原文数据。

3) 输出参数 pOutInfo

当函数执行成功时，该输出参数为经 Base64 编码后的签名数据。

当函数执行失败时，该输出参数为错误信息描述。

B.11.2 PKI_VerifySign“验签”

具体如下：

a) 函数定义

验签接口函数定义见表 B.25。

表 B.25 验签接口函数定义

函数名称	验签					
语法	long PKI_VerifySign(char* pCert, char* pInData, char* pSignature, char* pOutInfo)					
功能描述	对输入的数据进行数字签名					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pCert	IN	字符串	3*1024	验签所用的证书
	2	pInData	IN	字符串	6*1024	签名原文数据
	3	pSignature	IN	字符串	4*1024	待验证的签名数据
	4	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pCert

验签所使用的经 Base64 编码后的签名证书。

2) 输入参数 pInData

签名的原文数据。

3) 输入参数 pSignature

经 Base64 编码后的待验签的签名数据。

4) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.11.3 PKI_DataEncryption“数据加密”

具体如下：

a) 函数定义

数据加密接口函数定义见表 B.26。

表 B.26 数据加密接口函数定义

函数名称	数据加密					
语法	long PKI_DataEncryption(char* pCert, char* pInData, char* pOutInfo)					
功能描述	使用SM2算法对输入的数据进行加密					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pCert	IN	字符串	3*1024	加密所用的数字证书

	2	pInData	IN	字符串	160*2	原文数据
	3	pOutInfo	OUT	字符串	256*2	返回密文数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pCert

加密所使用的经 Base64 编码后的数字证书。

2) 输入参数 pInData

需要加密的原文数据。

3) 输出参数 pOutInfo

当函数执行成功时，该输出参数为经 Base64 编码后的已加密的密文数据。

当函数执行失败时，该输出参数为错误信息描述。

B.11.4 PKI_DataDecryption“数据解密”

具体如下：

a) 函数定义

数据加密接口函数定义见表 B.27。

表 B.27 数据解密接口函数定义

函数名称	数据解密					
语法	long PKI_DataDecryption (int iFile, char* pInData, char* pOutInfo)					
功能描述	使用SM2算法对输入的密文数据进行解密					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iFile	IN	整数	4	证书类型
	2	pInData	IN	字符串	247*2	密文数据
	3	pOutInfo	OUT	字符串	151*2	返回原文数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iFile

表示解密时使用的证书类型，定义如下：11-社保加密证书，21-地方加密证书。

2) 输入参数 pInData

需要解密的经 Base64 编码后的密文数据。

3) 输出参数 pOutInfo

当函数执行成功时，该输出参数为解密后的原文数据。

当函数执行失败时，该输出参数为错误信息描述。

B.11.5 PKI_HashData“哈希运算”

具体如下：

a) 函数定义

哈希运算接口函数定义见表 B.28。

表 B.28 哈希运算接口函数定义

函数名称	哈希运算					
语法	long PKI_HashData (char* pInData, char* pOutInfo)					
功能描述	对输入数据进行SM3哈希运算					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pInData	IN	字符串	6*1024	原文数据
	2	pOutInfo	OUT	字符串	512	返回Hash值或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pInData

需要进行运算的原文数据。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数为经 Base64 编码后的 HASH 值。

当函数执行失败时，该输出参数为错误信息描述。

B.11.6 PKI_ GetCert“证书读取”

具体如下：

a) 函数定义

证书读取接口函数定义见表 B.29。

表 B.29 证书读取接口函数定义

函数名称	证书读取					
语法	long PKI_ GetCert(int iFile, char* pOutInfo)					
功能描述	从卡内读出相应的证书					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iFile	IN	整数	4	证书类型
	2	pOutInfo	OUT	字符串	3*1024	返回证书数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iFile

表示需要读出的证书类型，定义如下：11-社保加密证书，12-社保签名证书，21-地方加密证书 22-地方签名证书。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数为经 Base64 编码后的证书数据。

当函数执行失败时，该输出参数为错误信息描述。

B.11.7 PKI_ ChangePIN“证书 PIN 修改”

具体如下：

a) 函数定义

证书 PIN 修改接口函数定义见表 B.30。

表 B.30 证书 PIN 修改接口函数定义

函数名称	证书 PIN 修改					
语法	long PKI_ ChangePIN(int iType, char* pOutInfo)					
功能描述	修改卡内非对称应用下的用户PIN					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	证书应用类型
	2	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

表示证书应用类型，定义如下：1-人社证书应用，2-地方证书应用。

2) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.11.8 PKI_ ReloadPIN“证书 PIN 重置”

具体如下：

a) 函数定义

证书 PIN 重置接口函数定义见表 B.31。

表 B.31 证书 PIN 重置接口函数定义

函数名称	证书 PIN 重置					
语法	long PKI_ReloadPIN(int iType,char* pAdminPIN,char* pOutInfo)					
功能描述	重置卡内非对称应用下的用户PIN					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	证书应用类型
	2	pAdminPIN	IN	字符串	32	管理员PIN
	3	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

表示证书应用类型，定义如下：1-人社证书应用，2-地方证书应用。

2) 输入参数 pAdminPIN

申请证书时生成的证书管理员 PIN，可由省级 RA 系统查询获得。

3) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.11.9 PKI_ VerifyPIN“证书 PIN 校验”

具体如下：

a) 函数定义

证书 PIN 校验接口函数定义见表 B.32。

表 B.32 证书 PIN 校验接口函数定义

函数名称	证书 PIN 校验					
语法	long PKI_VerifyPIN (int iType,char* pOutInfo)					
功能描述	重置卡内非对称应用下的用户PIN					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	证书应用类型
	2	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iType

表示证书应用类型，定义如下：1-人社证书应用，2-地方证书应用。

2) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.12 证书制卡函数

B.12.1 iWriteCA_HSM_Step1“制卡证书写入（步骤一）”

具体如下：

a) 函数定义

制卡证书写入（步骤一）接口函数定义见表 B.33。

表 B.33 制卡证书写入（步骤一）接口函数定义

函数名称	制卡证书写入（步骤一）					
语法	long iWriteCA_HSM_Step1(char* pAdminPin, char* pUserPin, char* pOutInfo)					
功能描述	在卡内产生签名公私钥对，并输出编码后的公钥数据					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pAdminPin	IN	字符串	32	旧的管理员PIN
	2	pUserPin	IN	字符串	32	新的用户PIN
	3	pOutInfo	OUT	字符串	512	返回签名公钥数据或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 pAdminPin

建立人社证书应用文件时设置的管理员 PIN。

2) 输入参数 pUserPin

各地规定的初始证书 PIN 值。

3) 输出参数 pOutInfo

当函数执行成功时，该输出参数为经 Base64 编码后的签名公钥数据。

当函数执行失败时，该输出参数为错误信息描述。

B.12.2 iWriteCA_HSM_Step2“制卡证书写入（步骤二）”

具体如下：

a) 函数定义

制卡证书写入（步骤二）接口函数定义见表 B.34。

表 B.34 制卡证书写入（步骤二）接口函数定义

函数名称	制卡证书写入（步骤二）					
语法	long iWriteCA_HSM_Step2(char* QMZS, char* JMZS, char* JMMY, char* ZKMY, char* GLYPIN, char* oldZKMY, char* pOutInfo)					
功能描述	在卡内产生签名公私钥对，并输出编码后的公钥数据					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	QMZS	IN	字符串	3*1024	签名证书
	2	JMZS	IN	字符串	3*1024	加密证书
	3	JMMY	IN	字符串	1024	加密密钥
	4	ZKMY	IN	字符串	64	新主控密钥
	5	GLYPIN	IN	字符串	32	新管理员PIN
	6	oldZKMY	IN	字符串	64	旧主控密钥
	7	pOutInfo	OUT	字符串	512	返回空字符串或错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 QMZS

申请证书时省级 RA 系统返回的经 Base64 编码的签名证书数据。

2) 输入参数 JMZS

申请证书时省级 RA 系统返回的经 Base64 编码的加密证书数据。

3) 输入参数 JMMY

申请证书时省级 RA 系统返回的经 Base64 编码的加密密钥数据。

4) 输入参数 ZKMY

申请证书时省级 RA 系统返回的新主控密钥值。

5) 输入参数 GLYPIN

申请证书时省级 RA 系统返回的新管理员 PIN 值。

6) 输入参数 oldZKMY

建立非对称认证应用环境和人社证书应用文件时设置的主控密钥值。

7) 输出参数 pOutInfo

定义同 B.4.1 b）5）。

B.13 “条码识读”函数

B.13.1 GetQRCode“条码识读”

具体如下：

a) 函数定义

条码识读接口函数定义见表 B.35。

表 B.35 条码识读接口函数定义

函数名称	条码识读					
语法	long iGetQRCode(int iTimeOut, char* pOutInfo)					
功能描述	通过一卡通终端上的条码识读模块，扫描获取条码信息					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iTimeOut	IN	整数	4	条码识读等待的超时时间
	2	pOutInfo	OUT	字符串	1024	识读数据或返回错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输入参数 iTimeOut

表示执行本函数时等待电子社会保障卡接近扫码区域进行获取数据操作的超时时间。

2) 输出参数 pOutInfo

当函数执行成功时，该输出参数为获取到的电子社会保障卡数据，且数据项以“|”结尾。

如：9200000012345678901234|，当函数执行失败时，该输出参数为错误信息描述。

B.14 “读社会保障卡银行账户”函数

B.14.1 GetICcardNum“读社会保障卡银行账户”

具体如下：

a) 函数定义

读社会保障卡银行账户接口函数定义见表 B.36。

表 B.36 读社会保障卡银行账户接口函数定义

函数名称	读社会保障卡银行账户					
语法	long GetICcardNum(char *pOutInfo)					
功能描述	读取社会保障卡银行账户信息					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	pOutInfo	OUT	整数	19	账户数据或返回错误信息
返回值	0表示成功；非0表示失败。					

b) 参数说明

1) 输出参数 pOutInfo

当函数执行成功时，该输出参数为获取到的读社会保障卡银行账户数据，且数据项以“|”结尾。

如：6217214402023168739|。

当函数执行失败时，该输出参数为错误信息描述。

B.15 ActiveX控件出参说明

在此附录的标准动态库基础上，原标准动态库的函数的输出参数 pOutInfo 在 ActiveX 控件中调整成以属性形式返回。举例“读基本信息”控件接口函数定义见表 37。

表 B.37 读基本信息控件接口函数定义

函数名称	读基本信息					
语法	long iReadCardBas(int iType)					
功能描述	选择社会保障卡社会保障系统环境后，通过PSAM卡对社会保障卡进行内部认证，通过后将卡内的基本信息读出返回。					
参数说明	序号	参数	输入/输出	类型	长度（十进制）	含义
	1	iType	IN	整数	4	操作卡的类型
返回值	0表示成功；非0表示失败。					
属性说明	pOutInfo：读出数据或返回错误信息					

B.16 Websocket服务出参说明

在此附录的标准动态库基础上，原标准动态库的函数的输出参数 pOutInfo 在 Websocket 中调整成以属性形式返回。举例“读基本信息”websocket 服务接口函数定义见表 38。

表 B.38 读基本信息 Websocket 服务接口函数定义

序号	指标编码	指标名称	参数类型	代码标识	是否必填	说明
1	function	调用函数	C	N	Y	调用函数，和入参一致
2	result	处理结果标志	C	Y	Y	0：成功 1：失败
3	reinfo	处理结果信息	C	N	N	返回处理失败的信息
4	pOutInfo	请求发送时间	C	N	Y	返回读卡结果字符串

输出参数报文示例：

{
"function":"iReadCardBas",
"result":"0",
"reinfo":"处理成功",
"pOutInfo":"100000|444444198404044449|A00001014|100000D15600000520002186E5CEEA96|李建|0081544C968684100020002186|3.00|20200115|20300115|100001900026|0002MT20220105000002|"
}

B.17 一卡通应用系统调用一卡通终端应用接口流程

本章给出一卡通应用系统调用一卡通终端应用接口的基本流程，有几点说明如下：

a) 所有操作的第一步均应调用“读基本信息”函数进行读基本信息操作，应用系统如果判断到五种情况的错误代码（详见B.21），则继续调用“基于加密机的读基本信息（步骤一）”函数进行读基本信息操作；

b) 一卡通应用系统应缓存读取的基本信息留作后用；

c) 在通用读卡和通用写卡接口函数中，应用系统应根据不同“规范版本”的文件结构确定读写卡调用的函数和输入参数。

B.17.1 读基本信息

读基本信息流程如图 B.1 所示。

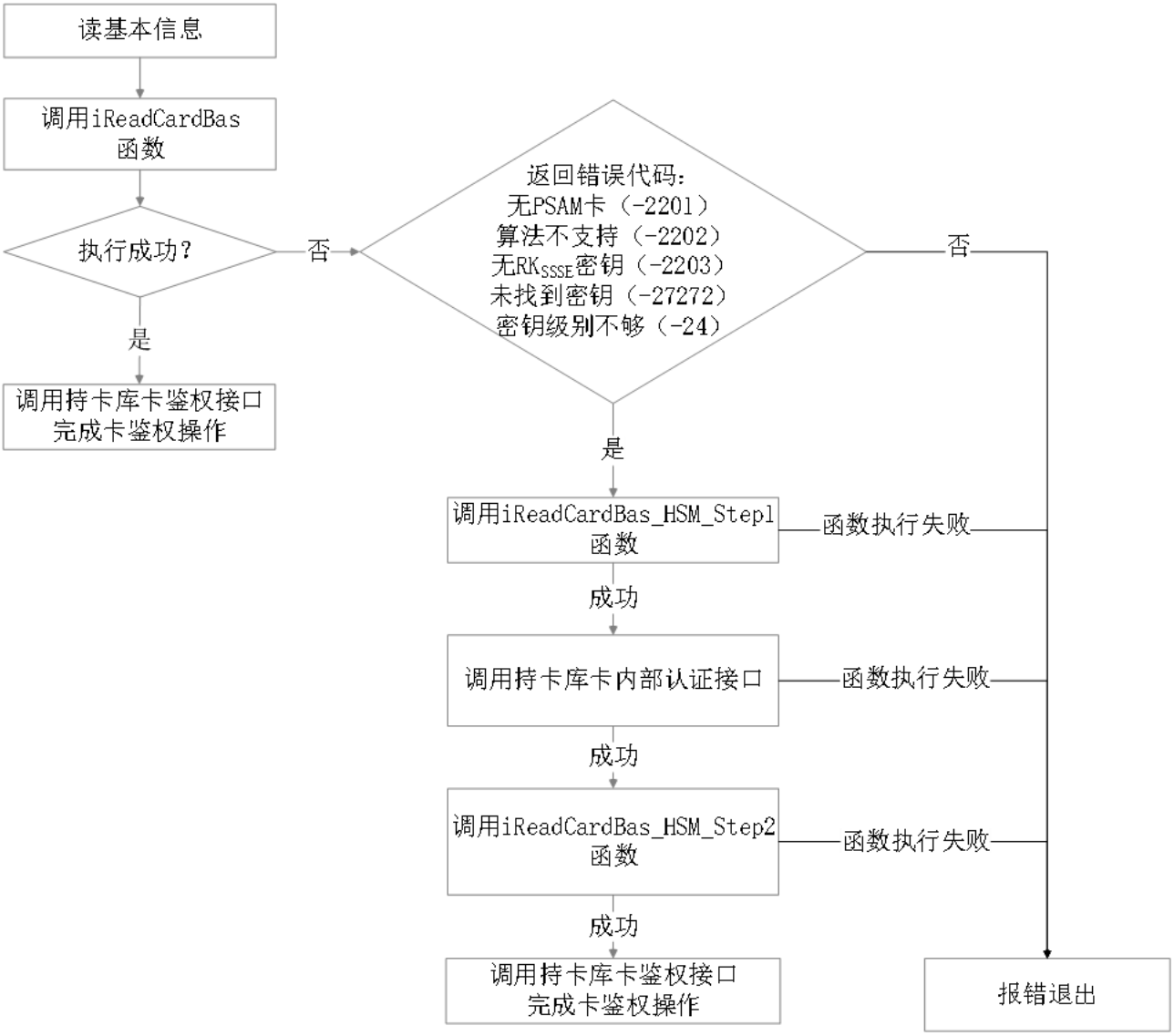


图 B.1 读基本信息流程

具体流程如下：

a) 调用iReadCardBas函数，判断函数执行结果，若执行成功，则返回基本信息，调用持卡库的卡鉴权服务接口，完成卡鉴权操作；若执行失败，返回错误代码并进行判断，当判断到五种情况的错误代码（详见B.21）后，则调用基于加密机的iReadCardBas_HSM_Step1函数，否则报错退出；

b) 若iReadCardBas_HSM_Step1函数执行成功，则分析返回数据内容，组织持卡库报文，调用持卡库的卡内部认证服务接口，否则报错退出；

c) 若卡内部认证服务接口调用成功，则调用基于加密机的iReadCardBas_HSM_Step2函数，否则报错退出；

d) 若iReadCardBas_HSM_Step2函数执行成功，则返回基本信息，调用持卡库的卡鉴权服务接口，完成卡鉴权操作，否则报错退出。

B.17.2 通用读卡

通用读卡流程如图 B.2 所示。

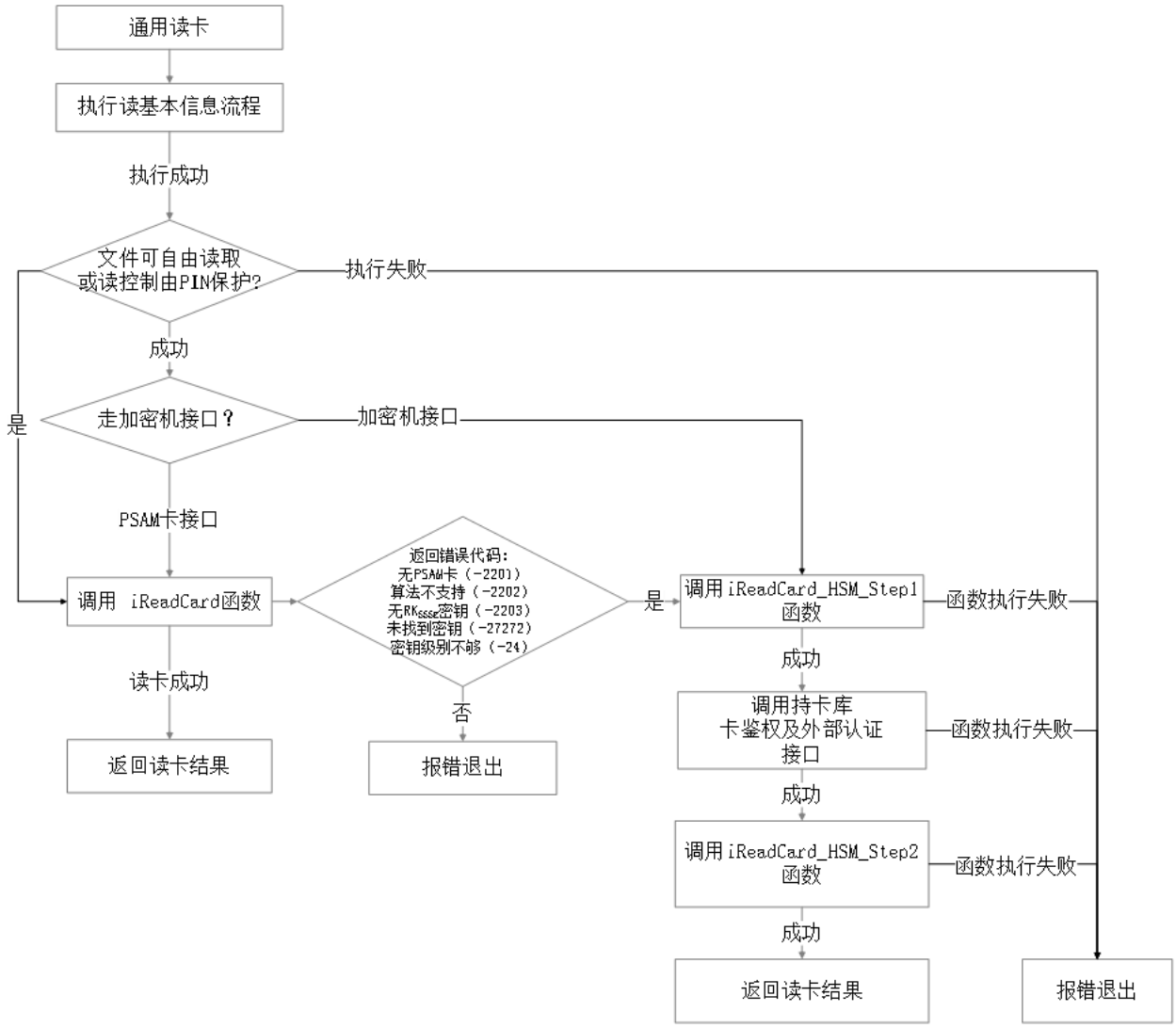


图 B.2 通用读卡流程

具体流程如下：

a) 执行读基本信息流程，若执行失败，则报错退出；若执行成功，则判断文件读控制权限；
b) 若文件可自由读取或读控制由PIN保护，则走PSAM卡接口；若不是，判断是否走加密机接口；
c) 若走PSAM卡接口，则调用iReadCard函数，判断函数执行结果；若执行成功，则读出所需数据，返回读卡结果；若执行失败，返回错误代码并进行判断，当判断到五种情况的错误代码（详见B.21）后，则调用基于加密机的iReadCard_HSM_Step1函数，否则其他错误代码时，则报错退出；
d) 若iReadCard_HSM_Step1函数执行成功，则分析返回数据内容，组织持卡库报文，调用持卡库的卡鉴权及外部认证服务接口；否则报错退出，若此函数返回错误代码“-2204”（具体参见B.13）且所读文件可自由读取或读控制仅受PIN保护，则业务系统继续调用iReadCard函数进行通用读卡操作；
e) 若卡鉴权及外部认证服务接口调用成功，则调用基于加密机的iReadCard_HSM_Step2函数，否则报错退出；
f) 若iReadCard_HSM_Step2函数执行成功，则读出所需数据，返回读卡结果，否则报错退出。

B.17.3 通用写卡

通用写卡流程如图 B.3 所示。

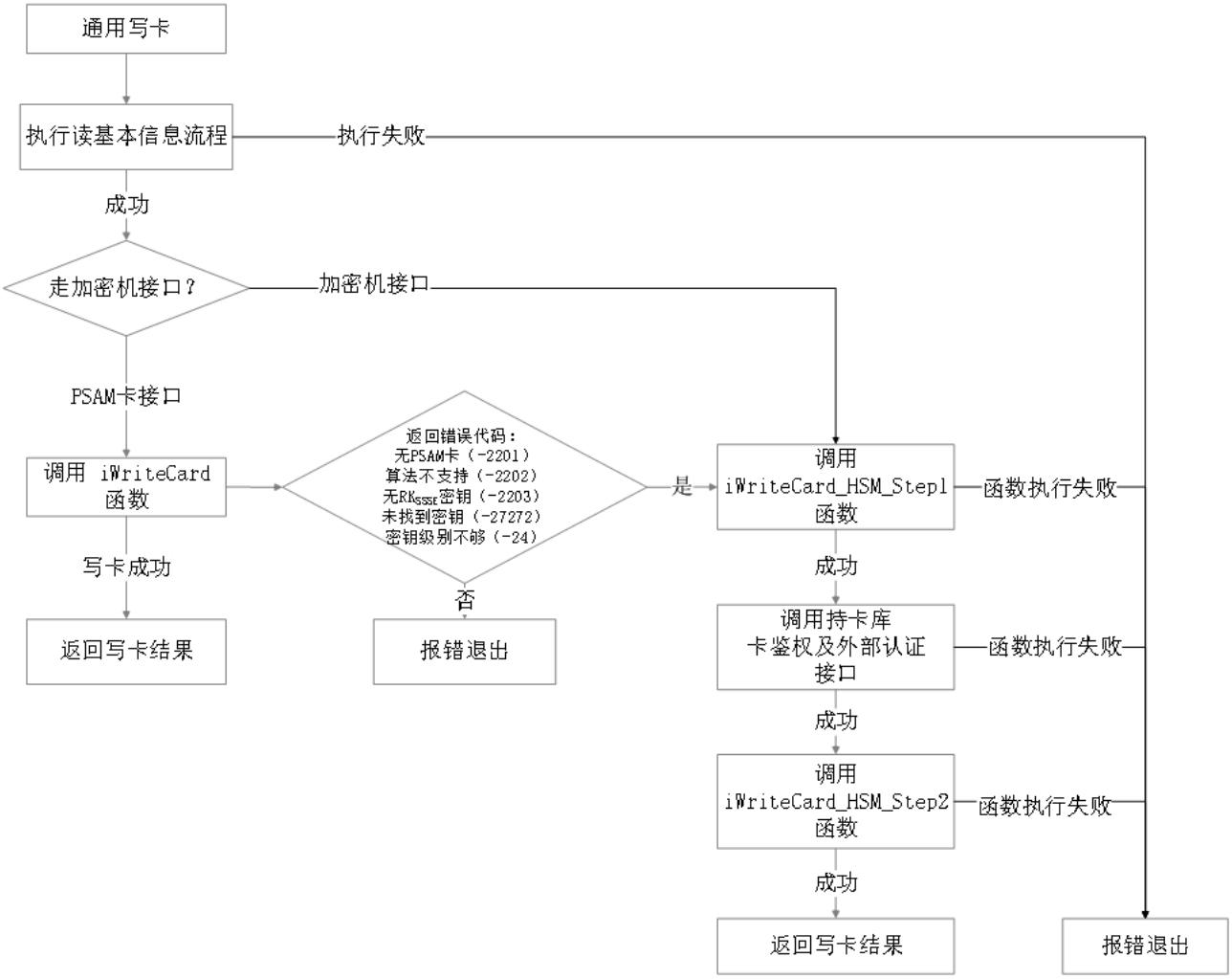


图 B.3 通用写卡流程

具体流程如下：

a) 执行读基本信息流程，若执行失败，则报错退出；若执行成功，则判断是否走加密机接口；

b) 若走PSAM卡接口，则调用iWriteCard函数，判断函数执行结果；若执行成功，则写入数据，返回写卡结果；若执行失败，返回错误代码并进行判断，当判断到五种情况的错误代码（详见B.21）后，则调用基于加密机的iWriteCard_HSM_Step1函数，否则其他错误代码时，则报错退出；

c) 若iWriteCard_HSM_Step1函数执行成功，则分析返回数据内容，组织持卡库报文，调用持卡库的卡鉴权及外部认证服务接口，否则报错退出；

d) 若卡鉴权及外部认证服务接口调用成功，则调用基于加密机的iWriteCard_HSM_Step2函数，否则报错退出；

e) 若iWriteCard_HSM_Step2函数执行成功，则写入数据，返回写卡结果，否则报错退出。

B.17.4 PIN 重置

PIN 重置流程如图 B.4 所示。

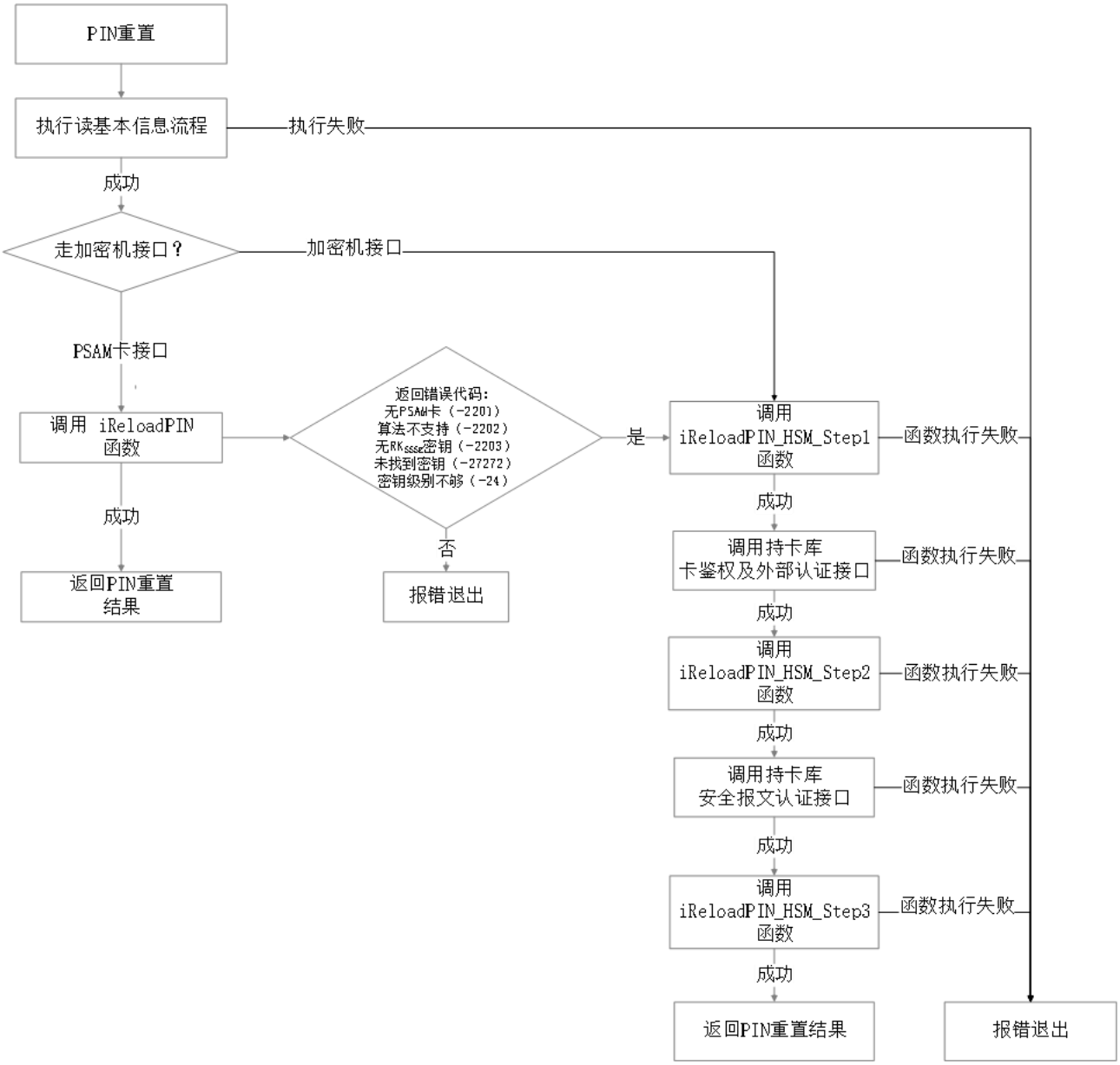


图 B.4　PIN 重置流程

具体流程如下：

a) 执行读基本信息流程，若执行失败，则报错退出；若执行成功，则判断是否走加密机接口；

b) 若走PSAM卡接口，则调用iReloadPIN函数，判断函数执行结果；若执行成功，则进行PIN重置；若执行失败，返回错误代码并进行判断，当判断到五种情况的错误代码（详见B.21）后，则调用基于加密机的iReloadPIN_HSM_Step1函数，否则其他错误代码时，则报错退出；

c) 若iReloadPIN_HSM_Step1函数执行成功，则分析返回数据内容，组织持卡库报文，调用持卡库的卡鉴权及外部认证服务接口，否则报错退出；

d) 若卡鉴权及外部认证服务接口调用成功，则调用基于加密机的iReloadPIN_HSM_Step2函数，否则报错退出；

e) 若iReloadPIN_HSM_Step2函数执行成功，则分析返回数据内容，组织持卡库报文，调用持卡库的安全报文认证服务接口，否则报错退出；

f) 若安全报文认证服务接口调用成功，则调用基于加密机的iReloadPIN_HSM_Step3函数，否则报退出；

g) 若iReloadPIN_HSM_Step3函数执行成功，则进行PIN重置，否则报错退出。

B.17.5 PIN 解锁

PIN 解锁流程如图 B.5 所示。

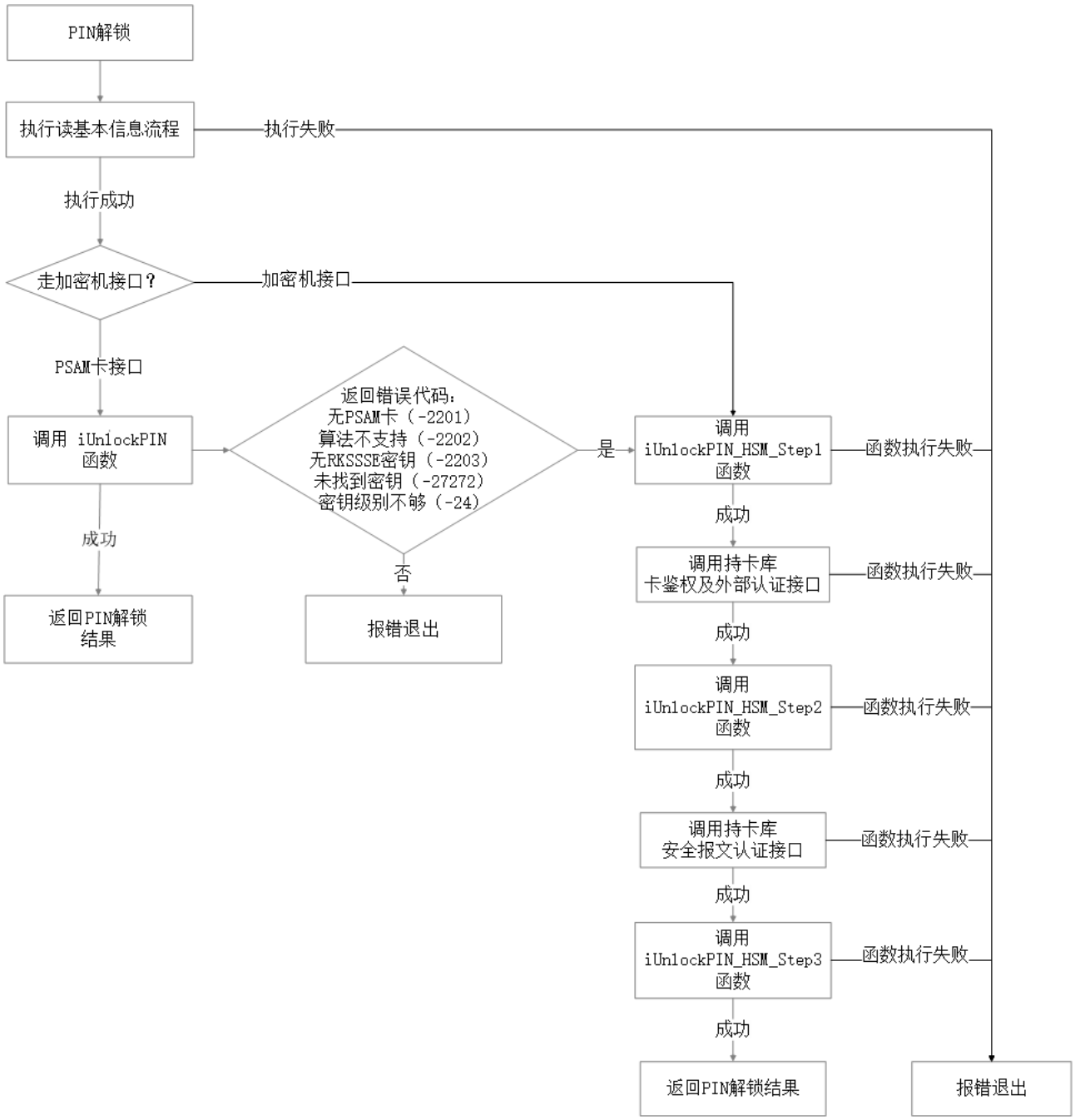


图 B.5 PIN 解锁流程

具体流程如下：

a) 执行读基本信息流程，若执行失败，则报错退出；若执行成功，则判断是否走加密机接口；

b) 若走PSAM卡接口，则调用iUnlockPIN函数，判断函数执行结果；若执行成功，则进行PIN解锁；若执行失败，返回错误代码并进行判断，当判断到五种情况的错误代码（详见B.21）后，则调用基于加密机的iUnlockPIN_HSM_Step1函数，否则其他错误代码时，则报错退出；

c) 若iUnlockPIN_HSM_Step1函数执行成功，则分析返回数据内容，组织持卡库报文，调用持卡库的卡鉴权及外部认证服务接口，否则报错退出；
d) 若卡鉴权及外部认证服务接口调用成功，则调用基于加密机的iUnlockPIN_HSM_Step2函数，否则报错退出；
e) 若iUnlockPIN_HSM_Step2函数执行成功，则分析返回数据内容，组织持卡库报文，调用持卡库的安全报文认证服务接口，否则报错退出；
f) 若安全报文认证服务接口调用成功，则调用基于加密机的iUnlockPIN_HSM_Step3函数，否则报错退出；
g) 若iUnlockPIN_HSM_Step3函数执行成功，则进行PIN解锁，否则报错退出。

B.17.6 消费交易

消费交易流程如图 B.6 所示。

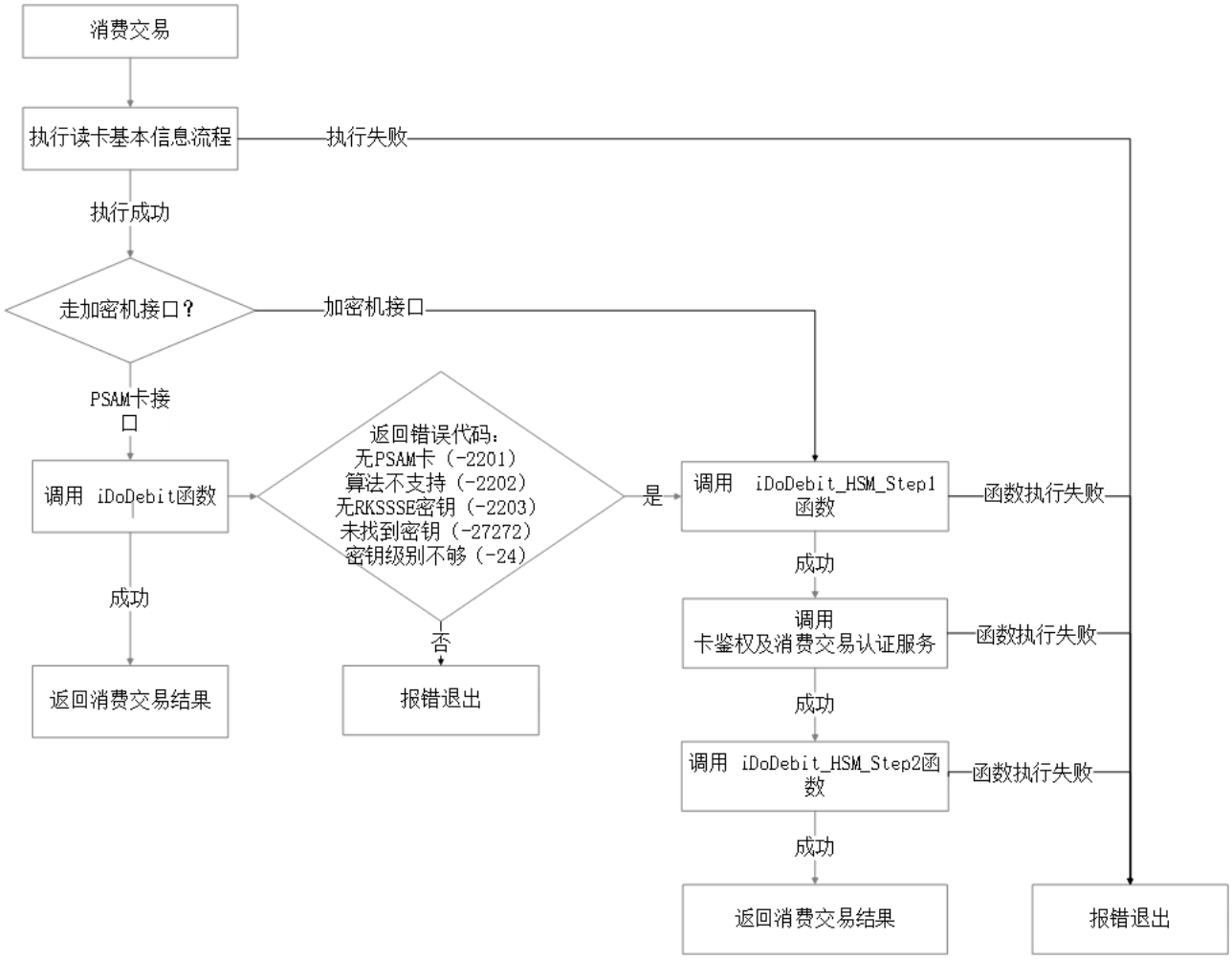


图 B.6 消费交易流程

具体流程如下：

a) 执行读基本信息流程，若执行失败，则报错退出；若执行成功，则判断是否走加密机接口；
b) 若走PSAM卡接口，则调用iDoDebit函数，判断函数执行结果；若执行成功，则进行消费交易，返回消费交易结果；若执行失败，返回错误代码并进行判断，当判断到五种情况的错误代码（详见B.21）后，则调用基于加密机的iDoDebit_HSM_Step1函数，否则其他错误代码时，则报错退出；
c) 若iDoDebit_HSM_Step1函数执行成功，则分析返回数据内容，组织持卡库报文，调用持卡库的卡鉴权及消费交易认证服务接口，否则报错退出；

d) 若卡鉴权及消费交易认证服务接口调用成功，则调用基于加密机的iDoDebit_HSM_Step2函数，否则报错退出；

e) 若iDoDebit_HSM_Step2函数执行成功，则进行消费交易，返回消费交易结果，否则报错退出。

B.17.7 消费交易结算验证

消费交易结算验证流程如图 B.7 所示。

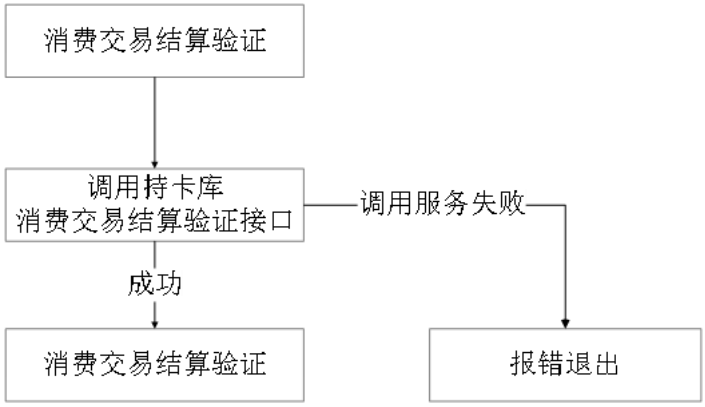


图 B.7 消费交易结算验证流程

具体流程如下：

根据保存的交易记录，组织持卡库报文，调用持卡库的消费交易结算验证服务接口，若调用成功，则取得返回结果，并根据返回结果判定是否交易验证成功，否则报错退出。

B.18 证书应用系统接口流程

B.18.1 数据签名

数据签名流程如图 B.8 所示。

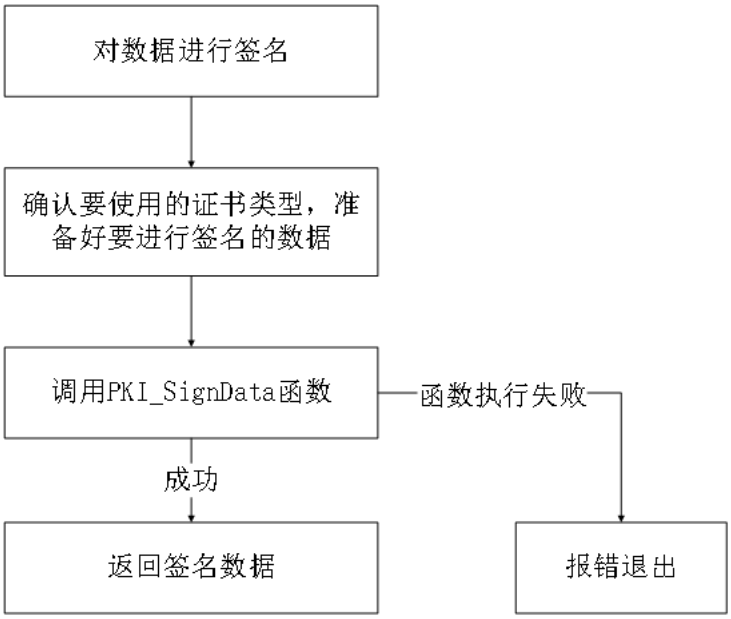


图 B.8 数据签名流程

具体流程如下：

准备好要进行签名的数据，并确认签名要使用的证书类型，然后调用证书应用签名接口 PKI_SignData，若调用成功，则返回签名好的签名数据，否则报错退出。

B.18.2 签名数据验签

签名数据验签流程如图 B.9 所示。

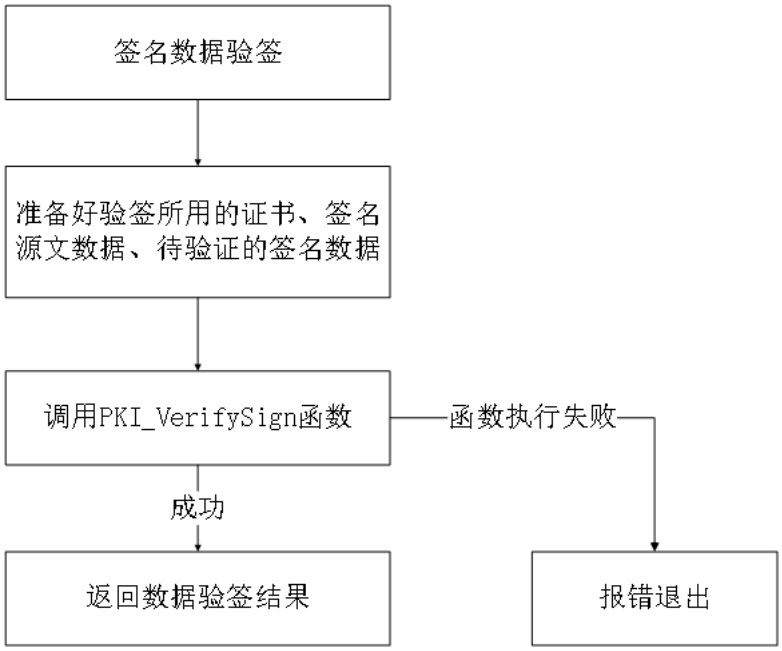


图 B.9 签名数据验签流程

具体流程如下：

准备好验签所用的证书、签名原文数据、待验证的签名数据，然后调用证书应用验签接口 PKI_VerifySign，若调用成功，则返回数据验签结果，否则报错退出。

B.18.3 数据加密

数据加密流程如图 B.10 所示。

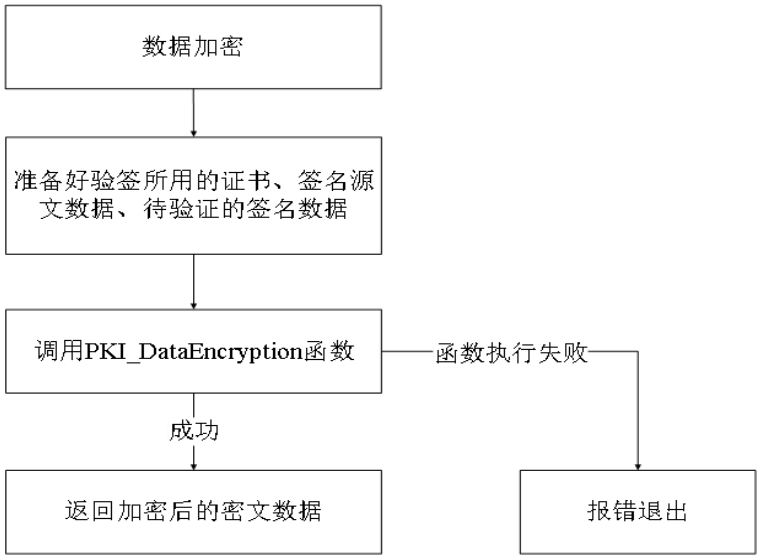


图 B.10 数据加密流程

具体流程如下：

准备好加密所用数字证书、待加密原文数据，然后调用证书应用数据加密接口 PKI_DataEncryption，若调用成功，则返回密文数据，返回值为 0，否则报错退出，返回值为非 0。

B.18.4 数据解密

数据解密流程如图 B.11 所示。

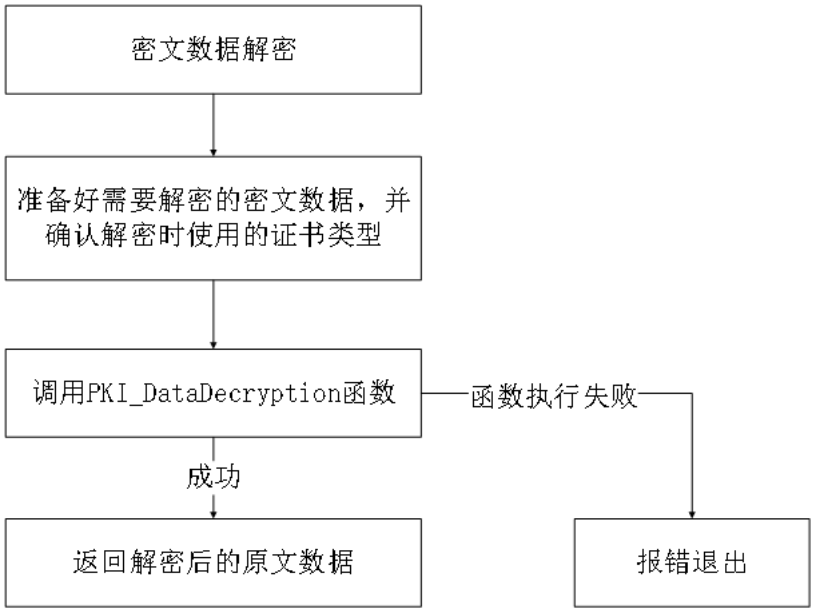


图 B.11 数据解密流程

具体流程如下：

准备好需要解密的密文数据并确认解密时使用的证书类型，然后调用证书应用数据解密接口 PKI_DataDecryption，若调用成功，返回解密后的原文数据，否则报错退出。

B.18.5 哈希运算

对数据进行哈希运算流程如图 B.12 所示。

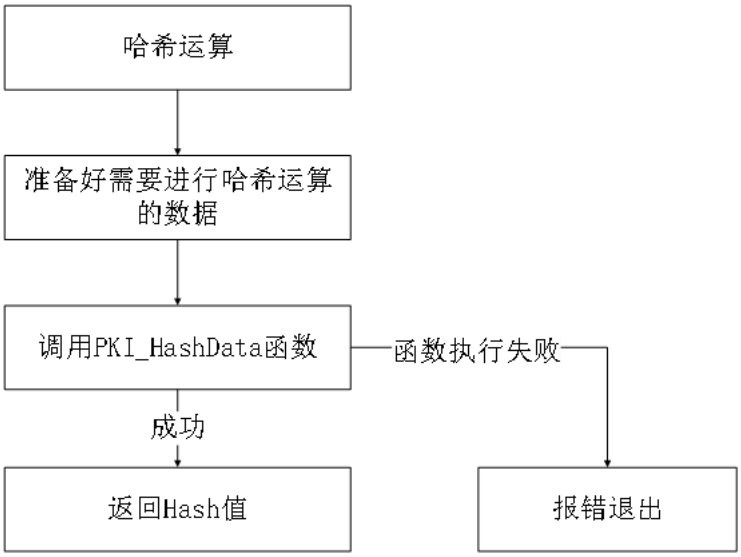


图 B.12 哈希运算流程

具体流程如下：

准备好需要进行哈希运算的数据，然后调用证书应用哈希运算接口 PKI_HashData，若调用成功，则返回 Hash 值，否则报错退出。

B.18.6 证书读取

证书读取流程如图 B.13 所示。

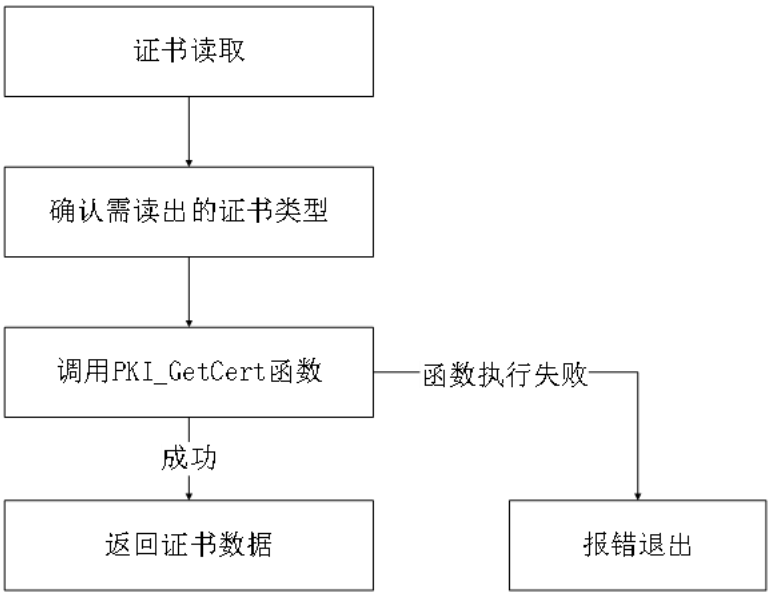


图 B.13 证书读取流程

具体流程如下：

确认需要读出的证书类型，然后调用证书应用证书读取接口 PKI_ GetCert，若调用成功，则返回证书数据，否则报错退出。

B.18.7 证书 PIN 修改

证书 PIN 修改流程如图 B.14 所示。

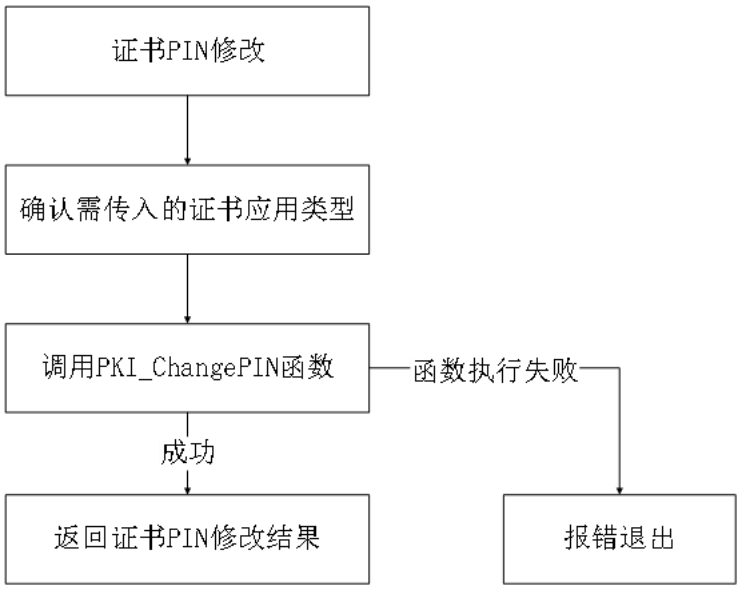


图 B.14 证书 PIN 修改流程

具体流程如下：

确认需传入的证书应用类型，然后调用证书应用证书 PIN 修改接口 PKI_ ChangePIN，若调用成功，则返回证书 PIN 修改结果，否则报错退出。

B.18.8 证书 PIN 重置

证书 PIN 重置流程如图 B.15 所示。

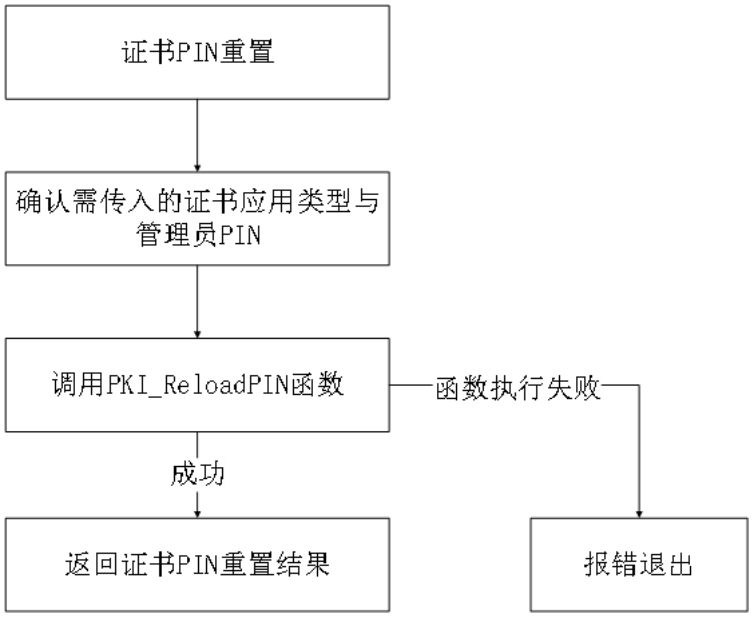


图 B.15 证书 PIN 重置流程

具体流程如下：

确认需传入的证书应用类型与管理员 PIN，然后调用证书应用证书 PIN 重置接口 PKI_ReloadPIN，若调用成功，则返回证书 PIN 重置结果，否则报错退出。

B.18.9 证书 PIN 校验

证书 PIN 校验流程如图 B.16 所示。

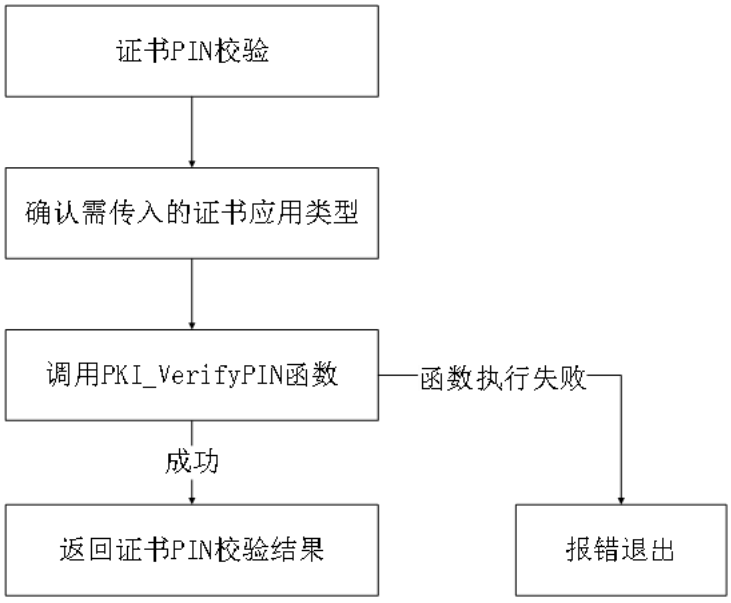


图 B.16 证书 PIN 校验流程

具体流程如下：

确认需传入的证书应用类型，然后调用证书应用证书 PIN 校验接口 PKI_ VerifyPIN，若调用成功，则返回证书 PIN 校验结果，否则报错退出。

B.18.10 证书制卡

证书制卡流程如图 B.21 所示。

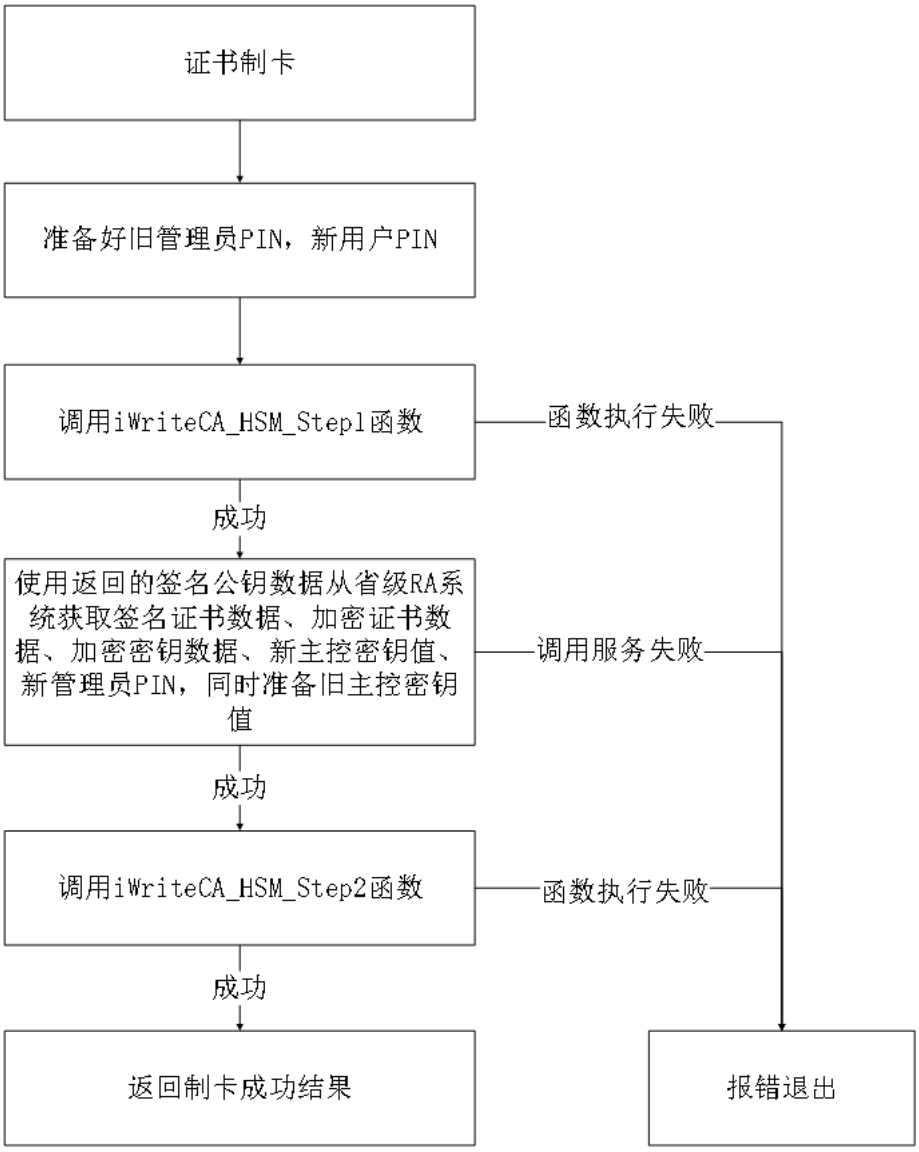


图 B.17 证书制卡流程

具体流程如下：

a) 准备好旧管理员 PIN，新用户 PIN，然后调用证书应用制卡证书写入（步骤一）接口 iWriteCA_HSM_Step1，若调用成功，则返回签名公钥数据，否则报错退出；

b) 第 a）步成功后，使用返回的签名公钥数据从省级 RA 系统获取签名证书数据、加密证书数据、加密密钥数据、新主控密钥值、新管理员 PIN，同时准备旧主控密钥值，然后调用证书应用制卡证书写入（步骤二）接口 iWriteCA_HSM_Step2，若调用成功，则返回制卡成功结果，否则报错退出。

B.19 条码识读

条码识读流程如图 B.18 所示。

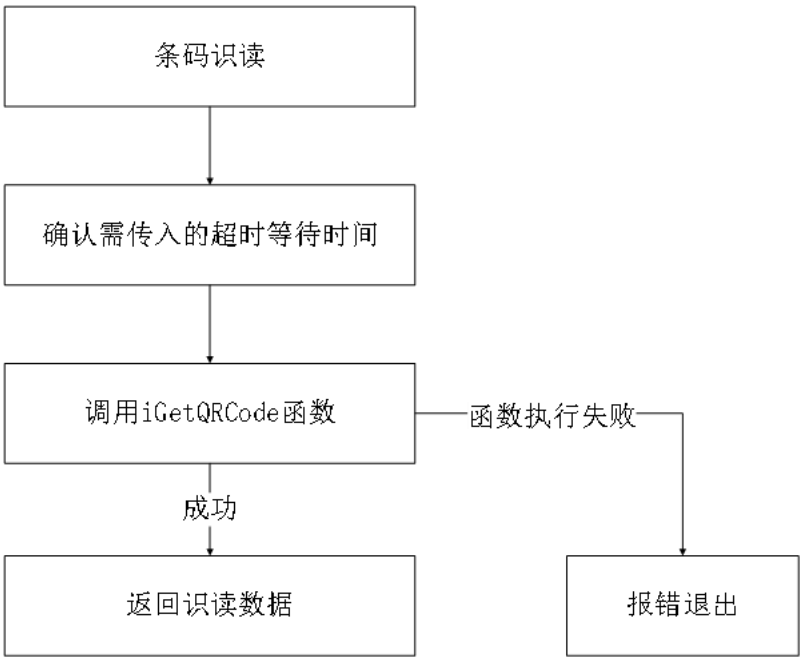


图 B.18 条码识读流程

具体流程如下：

确认需传入的超时等待时间，然后调用条码识读接口 iGetQRCode，若调用成功，则返回识读数据，否则报错退出。

B.20 社会保障卡银行账户读取

社会保障卡银行账户读取流程如图 B.19 所示。

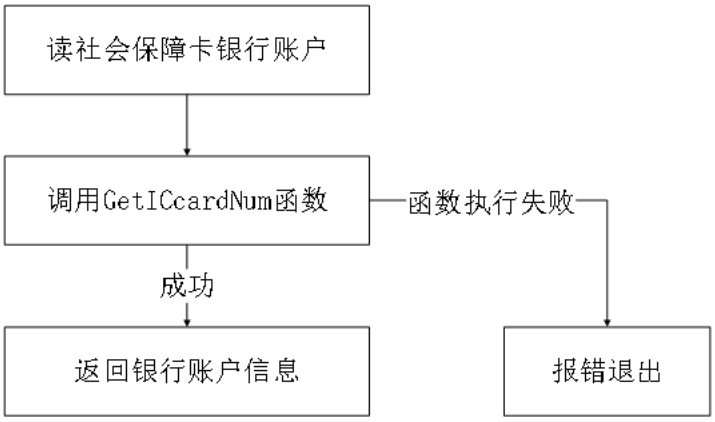


图 B.19 社会保障卡银行账户读取流程

具体流程如下：

一卡通终端在满足 SSSE 社会保障系统环境和 PSE 金融支付系统环境安全要求后，调用读社会保障卡银行账户接口 GetICcardNum，若调用成功，则返回银行账户信息，否则报错退出。

B.21 常见错误信息

常见错误信息见表 B.39。

表B.39 常见错误信息

返回值	错误信息描述
-1	卡片类型不对
-2	无卡
-3	有卡未上电
-4	卡片无应答
-5	加载动态库错
-11	一卡通终端连接错
-12	未建立连接
-13	（动态库）不支持该命令
-14	（发给动态库的）命令参数错
-15	信息校验和出错
-20	卡识别码格式错
-21	内部认证失败（用户卡不合法）
-22	传入数据与卡内不符
-23	传入数据不合法
-24	PSAM卡密钥级别不够
-31	用户取消密码输入
-32	密码输入操作超时
-33	输入密码长度错
-34	两次输入密码不一致
-35（预留）	初始密码不能交易
-36（预留）	不能改为初始密码
-41	运算数据含非法字符
-42	运算数据长度错
-51	PIN校验失败，剩余次数N次（根据卡返回信息）
-52	PIN锁定
-2201	无PSAM卡
-2202	PSAM卡算法不支持（即PSAM卡内没有SSF33算法或SM4算法）
-2203	PSAM卡内没有RK_{SSSE}密钥（3.0卡读个人基本信息需要RK_{SSSE}密钥外部认证）
-2204	不需要加密机认证
-25536、-25537、-25538	外部认证失败，剩余可尝试次数2、1、0次
-26368	Lc/Le不正确
-26881	命令不接受（无效状态）

-27009	命令与文件结构不相符、当前文件非所需文件
-27010	不满足安全条件
-27011	密钥锁定（算法锁定）鉴别方法锁定
-27012	引用数据无效、随机数无效
-27013	不满足使用条件、应用被锁定、应用未选择、余额上溢
-27016	安全报文数据项不正确、MAC不正确
-27264	数据域参数不正确
-27265	不支持该功能、卡中无MF、卡被锁定、应用锁定
-27266	未找到文件、文件标识相重、SFI不正确
-27267	未找到记录
-27272	未找到引用数据、未找到密钥
-37634	MAC无效
-37635	应用已被永久锁定、卡片锁定
-37891	PSAM卡不支持消费交易
-37894	所需MAC（或/和TAC）有误
其他	未知错误

参考文献

[1]GB/T 1988—1998 信息处理交换用七位编码字符集
[2]GB/T 14916—2006 识别卡物理特性
[3]GB/T 15120—2012 识别卡记录技术
[4]GB/T 15273 信息处理八位单字节编码图形字符集
[5]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
[6]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
[7]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
[8]GB/T 16649.4—2010 识别卡集成电路卡第4部分：用于交换的结构、安全和命令
[9]GB/T 17554.3—2006 识别卡测试方法第3部分：带触点的集成电路卡及其相关接口设备
[10]GB 18030—2022 信息技术 中文编码字符集
[11]GB/T 22351.1—2008 识别卡无触点的集成电路卡邻近式卡第1部分：物理特性
[12]GB/T 22351.2—2010 识别卡无触点的集成电路卡邻近式卡第2部分：空中接口和初始化
[13]GB/T 22351.3—2008 识别卡无触点的集成电路卡邻近式卡第3部分：防冲突和传输协议
[14]ISO/IEC 7816.4 信息技术识别卡带触点的集成电路卡第4部分：INCITS采纳的交换用工业间指令
[15]ISO/IEC 14443.2 卡及身份识别安全设备无触点的接近式对象（ISO/IEC 14443-2 Cards and security devices for personal identification - Contactless proximity objects）
[16]ISO/IEC 14443.4 卡及身份识别安全设备无触点的接近式对象 第4部分：传输协议（ISO/IEC 14443-4 Cards and security devices for personal identification - Contactless proximity objects - Part 4: Transmission protocol）
[17]JR/T 0025—2018 中国金融集成电路（IC）卡规范
[18]JR/T 0052—2009 银行卡卡片规范
[19]JR/T 0055—2009 银行卡联网联合技术规范
[20]LD/T 02—2022 人力资源社会保障电子认证体系规范
[21]《人力资源社会保障部关于开展社会保障卡持卡人员基础信息库建设的通知》（人社部发〔2014〕36号）
[22]《关于印发社会保障卡读写终端接口规范的通知》（人社信息函〔2016〕38号）
[23]《关于印发社会保障卡读写终端接口规范补充说明的通知》（人社信息函〔2016〕59号）
[24]《关于印发第三代社会保障卡相关技术规范（试行）的通知》（人社信息函〔2017〕27号）
[25]《社会保障卡规范第8部分：与接触无关的非接触式技术要求》（人社信息函〔2018〕1号）附件
[26]《社会保障卡规范第9部分：非对称认证应用技术要求》（人社信息函〔2018〕1号）附件