ICS

DB11

北　京　市　地　方　标　准

DB 11/T 1867.1—

"北京民生一卡通"技术规范 第 1 部分：卡片

Technical specification of "Beijing citizen livehood card"—

Part 1: Card

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

××××－××－××发布　　××××－××－××实施

北京市市场监督管理局　发布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第一部分：标准化文件的结构和起草规则》的规定起草。

本文件是DB11/T-1867《“北京民生一卡通”技术规范》的第1部分。DB11/T-1867已经发布以下部分：

——第 2 部分：二维码通用要求；

——第 3 部分：使用环境要求。

本文件由北京市人力资源和社会保障局提出并归口。

本文件由北京市人力资源和社会保障局组织实施。

本文件起草单位：

本文件主要起草人：

"北京民生一卡通"技术规范 第 1 部分： 卡片

1 范围

本文件规定了北京民生一卡通卡种类、卡介质、机电特性与通讯协议、应用构成、密钥管理、文件和数据规划、应用选择、应用流程和安全机制等方面的内容。

本文件适用于北京民生一卡通的设计、制造、管理、发行和应用。

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 14916 识别卡 物理特性

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 16649.3 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 16649.5 识别卡 带触点的集成电路卡 第5部分：应用标识符的编号系统和注册程序

GB/T 16649.6 识别卡 带触点的集成电路卡 第6部分：行业间数据元

GB/T 17554.1 识别卡 测试方法 第1部分：一般特性测试

GB/T 17554.3 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

JR/T 0025（所有部分） 中国金融集成电路（IC）卡规范

JT/T 978 城市公共交通IC卡技术规范

LD/T 32.6 社会保障卡规范 第6部分：应用数据结构

LD/T 32.7 社会保障卡规范 第7部分：应用流程

LD/T 33 社会保障卡读写终端规范

第三代中华人民共和国残疾人证技术规范

DB11/T 159 市政交通一卡通技术规范

DB11/T 1179 社会服务一卡通（北京通）卡片技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

CPU卡 central processing unit card

带有中央处理器（CPU）、存储单元以及芯片操作系统的集成电路卡。

3.2

北京民生一卡通 Beijing citizen livehood card

依托第三代社会保障卡，整合北京市社会保障、待遇发放、公共交通、医疗健康、养老优待、残疾人保障、优抚优待、金融服务、公园年票、教育管理等民生应用而形成的具有金融功能的实体卡和电子卡。

3.3

北京民生一卡通实体卡 physical Beijing citizen livehood card

北京民生一卡通线上应用的有效实体凭证，一种可识别其持卡人和发卡方的卡，卡上载有其预期应用和有关交易所要求输入的数据。

3.4

触点 contact

在集成电路卡和外部接口设备之间保持电流连续性的导电元件。

3.5

连接 concatenation

两个元素的连接是指将第二个元素附加到第一个元素的末尾。

3.6

受理终端 acceptance and dealing terminal

安装于受理点的用于与实体卡、二维码、人脸识别或其他方式配合共同完成身份认证、权益使用、支付等操作的设备。

3.7

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。

3.8

交易 transaction

持卡者和业务、管理部门之间根据卡所支持的应用接受、提供服务的行为。

3.9

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。

3.10

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、用于验证报文完整性的代码。

3.11

明文 plain text

没有加密的信息。

3.12

密文 cipher text

通过密码系统产生的不可理解的文字或信号。

3.13

密钥 key

控制加密转换操作的符号序列。

3.14

加密算法 cryptographic algorithm

为了隐藏或揭露信息内容而变换数据的算法。

3.15

对称加密技术 symmetric cryptographic technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术。

3.16

非对称加密技术 asymmetric cryptographic technique

采用两种相关变换进行加密的技术，一种是公开变换（由公共密钥定义），另一种是私有变换（由私有密钥定义）。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

3.17

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

[来源：GB/T 25056—2018，3.10]

3.18

公钥 public key

非对称密码算法中可公开的密钥。

[来源：GB/T 25056—2018，3.12]

3.19

保密密钥 secret key

对称加密技术中仅供指定实体所用的密钥。

3.20

数字签名 digital signature

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

3.21

数字证书（或证书） digital certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行数字签名的一个可信的数字化文件。数字证书包括公开密钥拥有者的信息、公开密钥、签名算法和CA的数字签名。

3.22

数据完整性 data integrity

数据不受未经许可的方法变更或破坏的属性。

3.23

T=0协议 T=0 protocol

面向字符的异步半双工传输协议。

3.24

冷复位 cold reset

当卡的电源电压和其他信号从静止状态中复苏且申请复位信号时，卡产生的复位。

3.25

热复位 warm reset

在时钟（CLK）和电源电压（VCC）处于激活状态的前提下，卡收到复位信号时产生的复位。

3.26

电子社会保障卡 electronic social security card

电子社会保障卡是社会保障卡的线上形态，是社会保障卡电子证照的具体表现形式，是持卡人线上享受人力资源和社会保障服务及其他民生服务的电子凭证和结算工具，与实体社会保障卡一一对应、唯一映射、状态相同、功能相通。

4 符号和缩略语

下列缩略语适用于本文件。

ATR 复位应答（answer to reset）

ATS 选择应答（answer to select）

CLK 时钟（clock）

COS 片内操作系统（chip operating system）

VCC 电源电压（supply voltage）

VCC VCC触点上测量到的电压（voltage measured on VCC contact）

VIH 高电平输入电压（high level input voltage）

VIL 低电平输入电压（low level input voltage）

VOH 高电平输出电压（high level output voltage）

VOL 低电平输出电压（low level output voltage）

VPP 编程电压（programming voltage）

VPP VPP触点上测量到的编程电压（programming voltage measured on VPP contact）

‘0’-‘9’ ‘A’-‘F’ 十六进制数字

5 北京民生一卡通基本要求

5.1 卡片样式

5.1.1 卡片外形和尺寸

北京民生一卡通外形为圆角矩形，尺寸见表1。

表1 卡片尺寸

参数	尺寸（mm）	范围（mm）
卡片长度	85.60	85.47～85.72
卡片宽度	53.98	53.92～54.03
卡片厚度	0.81	0.78～0.84
倒圆角半径	3.18	2.88～3.48

5.1.2 卡面布局和要素

5.1.2.1 卡片正面

5.1.2.1.1 卡片正面布局及要素

北京民生一卡通实体卡正面沿用第三代社会保障卡正面，包括以下要素：国徽、卡名（中华人民共和国社会保障卡）、隐蔽磁条，卡片正面布局及要素分别见图1和表2。

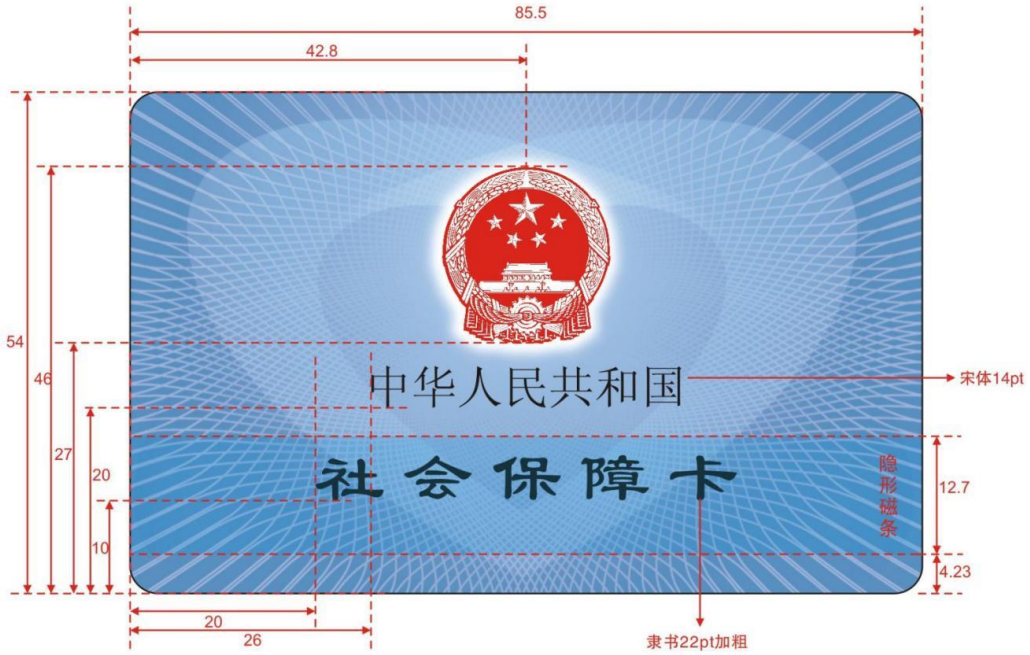


图1　卡片正面布局

表2　卡片正面要素

参数	规格及要求	公差
国徽		
图案	中华人民共和国国徽 应符合 GB 15093 的相关规定	—
中心到卡片左边沿的距离	42.80mm	±0.25mm
上边沿到卡片下边沿的距离	46.00mm	±0.25 mm
下边沿到卡片下边沿的距离	27.00mm	±0.25 mm
卡名		
“中华人民共和国”字样	宋体 14 磅	—
左边沿到卡片左边沿的距离	26.00mm	±0.25 mm
下边沿到卡片下边沿的距离	20.00mm	±0.25 mm
“社会保障卡”字样	隶书 22 磅加粗	—
左边沿到卡片左边沿的距离	20.00mm	±0.25 mm
下边沿到卡片下边沿的距离	10.00mm	±0.25 mm
隐蔽磁条		
磁条左边沿到卡片左边沿的距离	≤2.92mm	—
磁条右边沿到卡片左边沿的距离	≥82.55mm	—
磁条上边沿到卡片下边沿的距离	≥15.95mm	—
磁条下边沿到卡片下边沿的距离	≤5.54mm	—
磁条的物理特性	应符合 ISO/1EC 7811-6 的相关规定	

5.1.2.1.2　卡片正面颜色

卡片正面颜色色差允许公差见表3。

表3　卡片正面颜色

颜色区域	卡面左上蓝	卡面左下蓝	字体黑
色差允许公差	≤4. 00	≤4. 00	≤4. 00

5.1.2.2　卡片背面

5.1.2.2.1　卡片背面布局及要素

北京民生一卡通实体卡背面在第三代社保卡标准的基础上，按照北京民生一卡通要求进行设计，包括以下要素：北京民生一卡通名称、发卡机构印章、持卡人个人信息、持卡人照片、服务电话、特殊身份标识、盲文、银行卡组织标识区（银联标识）、数字人民币标识区（数币标识）、发卡机构标识区、IC芯片、银行卡卡号、ATM标识和箭头、插卡方向箭头标识、非接触标识区、制卡厂商代码区、网纹、水印。

卡片背面设计分标识版和普通版。根据持卡人特殊身份，在卡片背面指定位置标记残疾人标识，学生标识，优待人员标识。根据各发卡机构具体情况，在卡片背面指定位置标记数字人民币标识。普通版没有学生标识、残疾人标识、优待人员标识及数字人民币标识。卡片背面布局及要素分别见图2、图3、图4、图5及表4。

图2　标识版卡片背面

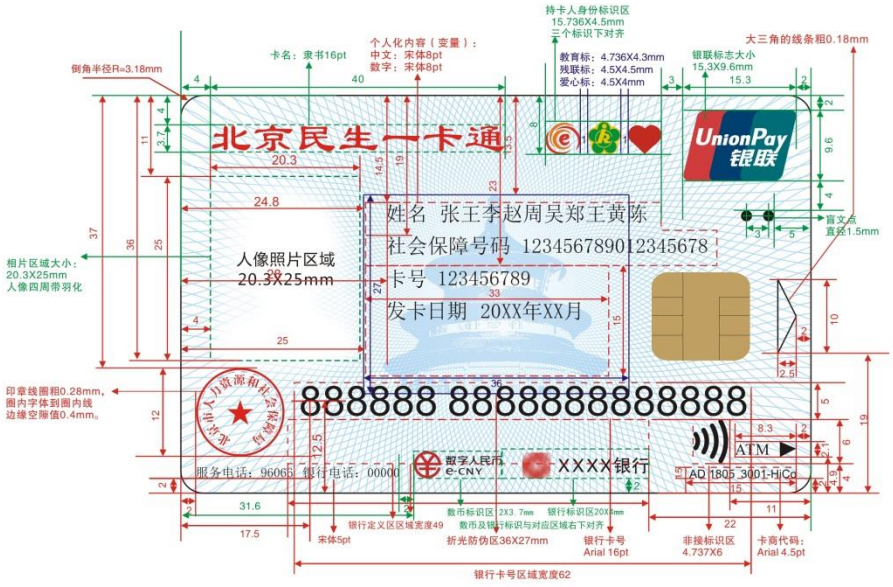


图3　标识版卡片背面布局

图4 普通版卡片背面

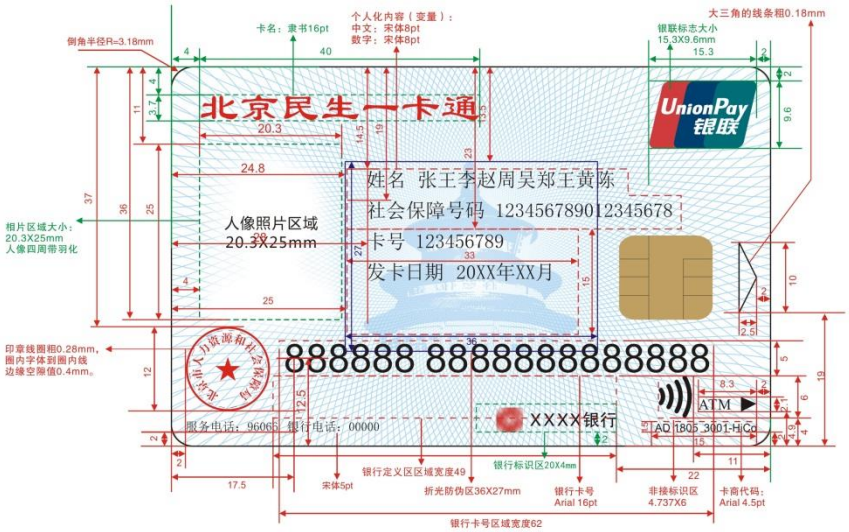


图5 普通版卡片背面布局

表4 卡片背面要素

参数	规格及要求	公差
发卡机构标识区		
区域的宽度	40.00mm	±0.10mm
区域的高度	3.7mm	±0.10mm
北京民生一卡通字号、字体及字距	隶书 16 磅 字距 16%	±0.10mm
北京民生一卡通文字色值（中国红）	C0 M100 Y100 K0	
区域左边沿到卡片左边沿的距离	4.00mm	±0.30mm

表 4（续）

区域上边沿到卡片上边沿的距离	4.00mm	±0.30mm
银行卡组织标识区(银联标识)		
区域的宽度	15.3mm	±0.10mm
区域的高度	9.60mm	±0.10mm
区域右边沿到卡片右边沿的距离	2mm	±0.10mm
区域上边沿到卡片上边沿的距离	2mm	±0.10mm
持卡人相片		
“相片”的宽度	20.30mm	±0.10mm
“相片”的高度	25.00mm	±0.10mm
“相片”左边沿到卡片左边沿的距离	4.00mm	±0.30mm
“相片”上边沿到卡片上边沿的距离	11.00mm	±0.30mm
持卡人个人信息		
“姓名”的字体和字号大小	宋体 8 磅	如果字符长度超过 10 个中文字符时，字号缩小到 5 号并折行处理
“姓名”左边沿到卡片左边沿的距离	28.00mm	±0.30mm
“姓名”上边沿到卡片上边沿的距离	14.50mm	±0.30mm
“社会保障号码”的字体和字号大小	宋体 8 磅	—
“社会保障号码”左边沿到卡片左边沿的距离	28.00mm	±0.30mm
“社会保障号码”上边沿到卡片上边沿的距离	19.00mm	±0.30mm
地方人力资源社会保障机构定义区		
区域的宽度	33.00mm	±0.10mm
区域的高度	15.00mm	±0.10mm
区域左边沿到卡片左边沿的距离	25.00mm	±0.30mm
区域上边沿到卡片上边沿的距离	23.00mm	±0.30mm
IC 芯片		
芯片的尺寸和位置	应符合 GB/T 16649.2 的相关规定	
插卡方向箭头标识		
标识的宽度	2.50mm	±0.10mm
标识的高度	10.00mm	±0.10mm
标识右端到卡片右边沿的距离	2.00mm	±0.30mm
标识下端到卡片下边沿的距离	19.00mm	±0.30mm
发卡机构印章		
印章的直径	12.00mm	±0.10mm

表 4（续）

印章外框线圈粗细	0.28mm	—
印章字体及字号	思源宋体加粗 5pt	—
印章的色值	C0 M100 Y100 K0	—
印章上边沿到卡片上边沿的距离	37.00mm	±0.30mm
印章左边沿到卡片左边沿的距离	2.00mm	±0.30mm
银行卡卡号		
“卡号”的字体和字号大小	Arial 16 磅	—
“卡号”区域的宽度	62.00mm	±0.10mm
“卡号”区域的高度	5.00mm	±0.10mm
“卡号”左边首位的中心到卡片下边沿的距离	12.50mm	±0.20mm
“卡号”左边首位的中心到卡片左边沿的距离	17.50mm	±0.20mm
银行定义区（银行标志）		
区域的宽度	20.00mm	±0.10mm
区域的高度	4.00mm	±0.10mm
区域右边沿到卡片右边沿的距离	22.00mm	0.10mm
区域下边沿到卡片下边沿的距离	2.00mm	0.10mm
数字人民币标识区（数字人民币标志）		
区域的宽度	12.00mm	±0.10mm
区域的高度	3.70mm	±0.10mm
区域右边沿到卡片左边沿的距离	31.60mm	0.10mm
区域下边沿到卡片下边沿的距离	2.00mm	0.10mm
非接触标识区		
区域的宽度	4.737mm	0.10mm
区域的高度	6.00mm	0.10mm
区域右边沿到卡片右边沿的距离	11.00mm	0.30mm
区域下边沿到卡片下边沿的距离	4.00mm	0.30mm
ATM 标识和箭头		
“标识”的宽度	8.30mm	±0.10mm
“标识”的高度	2.10mm	±0.10mm
“标识”右边沿到卡片右边沿的距离	2.00mm	±0.30mm
“标识”下边沿到卡片下边沿的距离	4.90mm	±0.30mm
服务电话		
“服务电话”的字体和字号大小	宋体 5 磅	—
“服务电话”左边沿到卡片左边沿的距离	2.00mm	± 0.30mm

表 4（续）

“服务电话”下边沿到卡片下边沿的距离	2.00mm	±0.30mm
制卡厂商代码区		
“制卡厂商代码”的字体和字号大小	Arial 4.5 磅	—
区域的宽度	15.00mm	±0.10mm
区域的高度	1.50mm	±0.10mm
区域右边沿到卡片右边沿的距离	2.00mm	±0.30mm
区域下边沿到卡片下边沿的距离	2.00mm	±0.30mm
水印区		
区域的宽度	36.00mm	±0.10mm
区域的高度	27.00mm	±0.10mm
区域左边沿到卡片左边沿的距离	24.80mm	±0.30mm
区域上边沿到卡片上边沿的距离	13.50mm	±0.30mm
水印的要求	折光防伪油墨，幻彩绿	—
特殊身份标识区		
区域的宽度	15.736mm	±0.10mm
区域的高度	4.5mm	±0.10mm
区域右边沿到卡片右边沿的距离	20.3mm	±0.30mm
区域下边沿到卡片上边沿的距离	8mm	±0.30mm
北京市教育委员会 LOGO 宽度	4.736mm	±0.30mm
北京市教育委员会 LOGO 高度	4.3mm	±0.30mm
残疾人标识宽度	4.5mm	±0.30mm
残疾人标识高度	4.5mm	±0.30mm
红色爱心宽度	4.5mm	±0.30mm
红色爱心高度	4mm	±0.30mm
各标识间间距	1mm	±0.30mm
盲文		
盲文直径	1.5mmX2	—
盲文右边沿距离卡片右边沿的距离	5mm	±0.80mm
盲文上边沿距离卡片上边沿的距离	15.6mm	±0.80mm
两个盲文圆点中心距离	3mm	±0.10mm
盲文高度	0.14mm	±0.02mm

5.1.2.2.2 卡片背面颜色

卡片背面底层网纹颜色色差允许公差见表5。

表5　卡片背面底层网纹颜色

颜色组成	蓝（C）	红（M）	黄（Y）	黑（K）
色值	27	0	0	6
色差允许公差	≤5.00			

5.1.3　彩色样图

预制卡卡片分盲文版预制卡和普通版预制卡，盲文版预制卡在标识版成品卡基础上去掉持卡人相片、持卡人信息以及特殊身份标识，其余具体参数、规格及要求与标识版成品卡一致；普通版预制卡在普通版成品卡基础上去掉持卡人相片以及持卡人信息，其余具体参数、规格及要求与普通版成品卡一致，预制卡卡片背面布局及要素分别见图6、图7、图8及图9。

图6　盲文版预制卡卡片背面

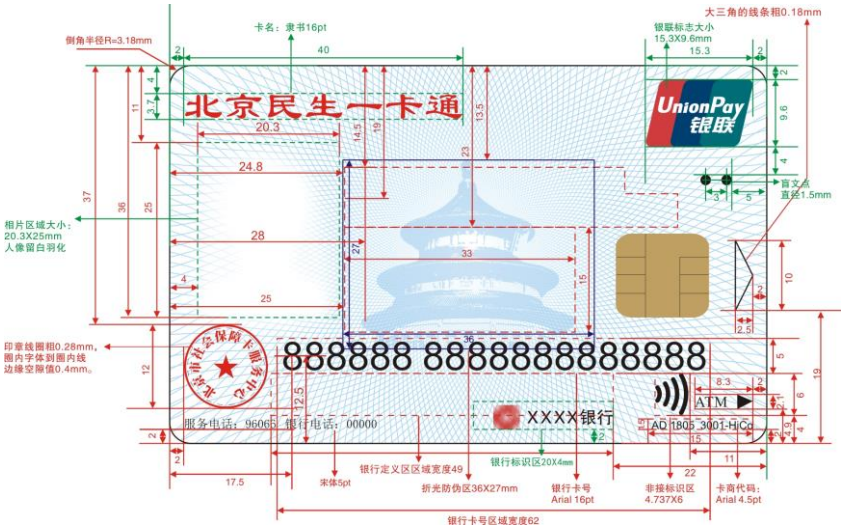


图7　盲文版预制卡卡片背面布局

图8　普通版预制卡卡片背面

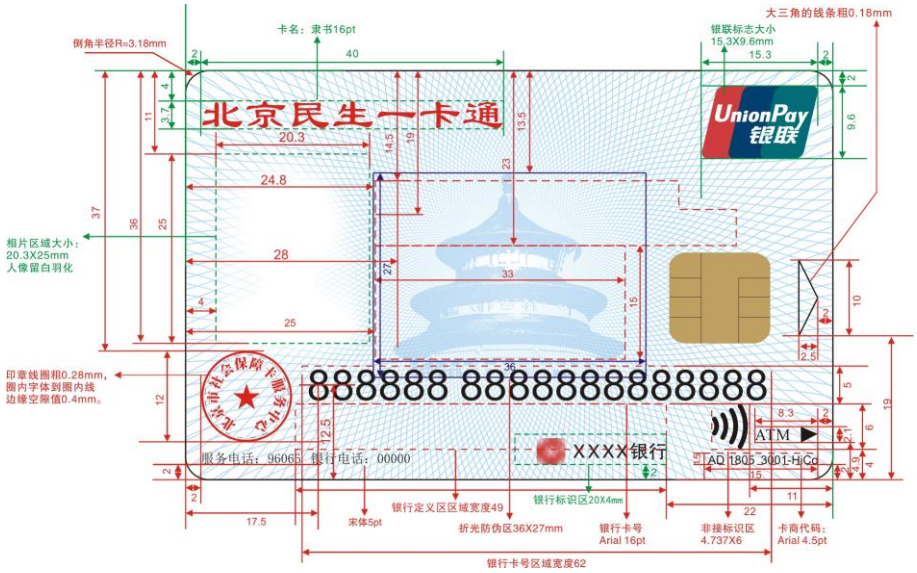


图9　普通版预制卡卡片背面布局

5.2　卡片机械特性

5.2.1　通则

除本条的特殊规定外，卡应符合GB/T 16649.1规定的有关物理特性，如紫外线、X射线、机械强度、电磁场的要求。

5.2.1.1　翘曲值

翘曲值≤1.50mm。

5.2.1.2　卡表层剥离强度

测量角度为90°，取样为10.00mm宽，取最低值，卡表层剥离强度值应≥4.5N/cm。

5.2.1.3　卡粘接特性

将卡5个一组叠在一起,放入40℃±3℃相对湿度设定为40%～60%的箱内,使卡背面朝下,其上加以2.5kPa的均匀压力。48h之后取出，应可以用手很容易地将单张卡分开。将卡拿到实验室环境温度下立刻观察,不能出现脱层、变色或色移、表面磨光变化、卡上有物质转移现象以及外观形变等变化。

5.2.1.4 动态弯扭曲

进行GB/T17554.1中描述的1000次弯曲循环测试后,卡应保持其功能并不应出现开裂；进行GB/T17554.1中描述的1000次扭曲循环测试后,卡应保持其功能并不应出现开裂。

5.2.1.5 外观质量

卡表面不得有油污、异物等杂物。距离30cm目测：卡表面上长度>0.3mm的尘点、墨点、气泡、杂质等异常斑点或异物不得超过6个；不得出现内容错误、图案错误、位置错误、漏印刷的问题；不得出现明显色斑、条纹、图案、字符有明重影、毛刺、缺损的问题。

5.2.1.6 触点尺寸和位置

触点尺寸：每个触点都应在不小于2mm*1.7mm的矩形表面区域内。

触点位置：触点之间应电隔离，触点位置范围值见表6。

表6 触点位置范围值

范围值 / 触点	距卡下边缘		距卡右边缘	
	最小值	最大值	最小值	最大值
C1	20.93 mm	19.23 mm	12.25 mm	10.25 mm
C2	23.47 mm	21.77 mm	12.25 mm	10.25 mm
C3	26.01 mm	24.31 mm	12.25 mm	10.25 mm
C4	28.55 mm	26.85 mm	12.25 mm	10.25 mm
C5	20.93 mm	19.23 mm	19.87 mm	17.87 mm
C6	23.47 mm	21.77 mm	19.87 mm	17.87 mm
C7	26.01 mm	24.31 mm	19.87 mm	17.87 mm
C8	28.55 mm	26.85 mm	19.87 mm	17.87 mm

5.2.2 机电特性

5.2.2.1 操作条件

5.2.2.1.1 操作条件的类别

本部分定义了三类操作条件，接口设备通过VCC触点向卡提供正常的电源电压分别如下：在A类条件下为5V，在B类条件下为3V，在C类条件下为1.8V。

因此，卡和接口设备应或者仅在A类环境中工作、或者仅在B类环境中工作、或者仅在C类环境中工作、或者可以在A类及B类环境中工作（下文中表示为AB类）、或者可以在A类、B类及C类环境中工作（下文中表示为ABC类）。

A类卡应使用A类、AB类和ABC类接口设备来进行操作。B类卡应使用B类、AB类和ABC类接口设备来进行操作，这类卡应按在A类操作条件下不会被损坏的一种方式来设计（根据定义，一张被损坏的卡不再按规定进行操作或包含被破坏的数据）。AB类卡应使用A类、B类、AB类和ABC类接口设备来进行操作。

5.2.2.1.2 操作条件的选择

接口设备在选择卡的操作条件类别的判断条件见图10。所给出的判断条件除出现“卡”字的之外，都是基于隐含在接口设备中的信息的。

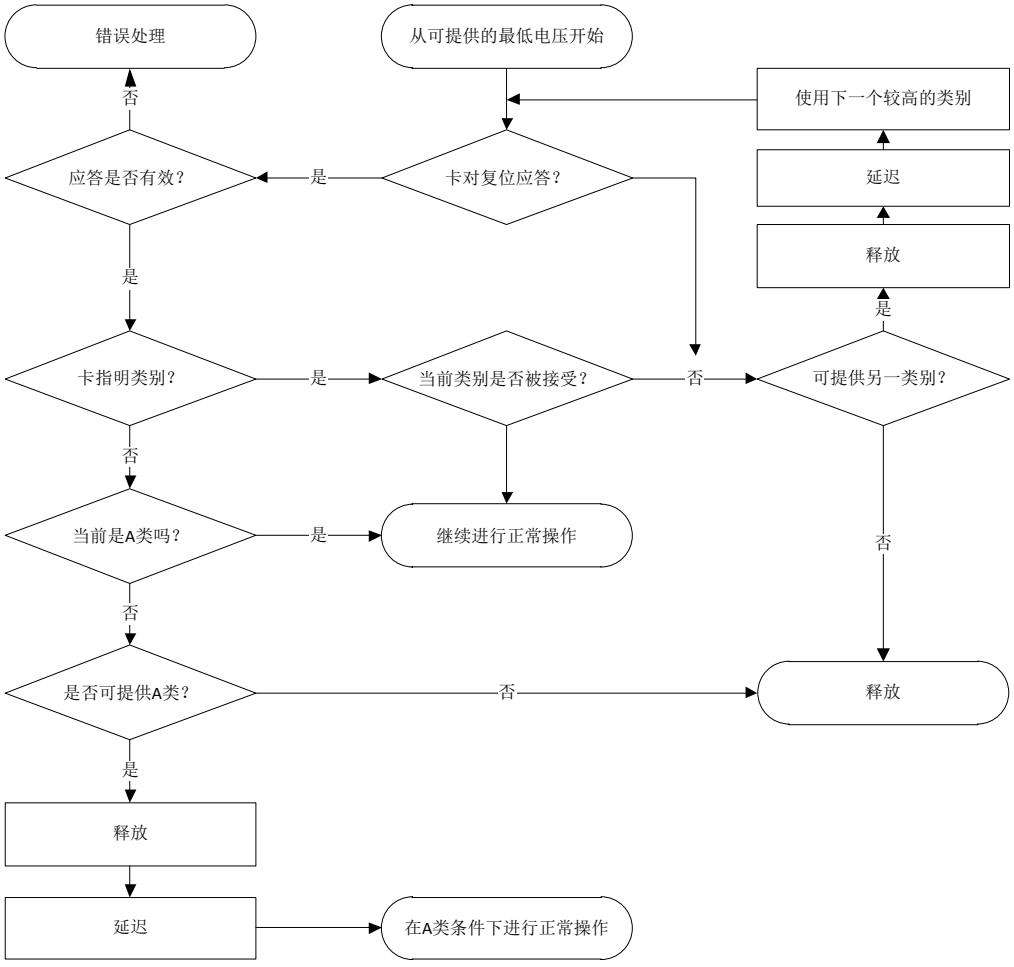


图10 接口设备对操作条件类别的选择

当在接口设备中可用时，用于卡的第一个操作条件应是B类条件。

在A类操作条件下，B类卡不提供ATR。

如果卡不提供ATR，则接口设备应释放该卡；在至少10ms的延迟后，接口设备应使用下一类可用的操作条件。

如果卡提供了没有类别指示符的ATR，则接口设备应使用或维持A类操作条件（如果可用的话）或释放该卡。

如果卡提供了带有类别指示符的ATR，并且接口设备正在使用卡所支持的操作条件类别，则正常的操作可以继续进行。

如果ATR未指示当前的操作条件类别，但接口设备也支持另一类操作条件，则接口设备应释放该卡，并在至少10ms的延迟后，使用该类操作条件。

一些符合GB/T 16649.3规定的卡在B类条件下操作时可能被损坏，这些卡应只在A类接口设备中使用。

5.2.2.2 电压和电流值

5.2.2.2.1 测量约定

所有测量应在卡和IFD之间的触点上进行，并以GND为参照。环境温度范围为0℃～50℃。

所有流入卡的电流均为正值。在流入接口设备的电流小于1mA，相对于触点GND的电压保持在0V～0.4V之间时，电路为不工作状态。

注：环境温度范围的限定是由聚氯乙烯（PVC）（大部分卡所用的材料）的特性决定，而不是由IC的特性决定。

5.2.2.2.2 电源电压（VCC）

该触点用来向卡提供电源电压。表7中的电流值是在1ms的时间内的平均值。为卡规定了最大电流值。接口设备应能在规定的电压范围内提供此电流值或者更大的电流值。

表7 正常操作条件下 VCC 的电特性

符号	条件	最小值	最大值
VCC	A 类	4.5V	5.5V
	B 类	2.7V	3.3V
	C 类	1.62V	1.98V
ICC	A 类，在允许的最大频率下	-	50 mA
	B 类，在允许的最大频率下		50 mA
	当时钟停止时		0.5 mA

即使在表8所规定的瞬间功耗条件下，电源电压仍应将电压值维持在规定的范围内。

表8 ICC 的尖峰值

类别	最大电荷量 a nA.s	最大持续时间 ns	ICC 的最大变动量 b mA
A	20	400	100
B	10	400	50
注：最大电荷量是最大持续时间和最大变动量的乘积的一半； 最大变动量在电源电流方面与平均值是不同的。			

5.2.2.2.3 输入/输出（I/O）

该触点作为输入端（接收模式）从终端接收数据或者作为输出端（传输模式）向终端传送数据。通过该触点交换的信息使用下列两种逻辑状态：

a）状态H，如果卡和接口设备都处于接收模式，或者由发送方强制此状态；

b）状态L，由发送方强制此状态。

当线路的两端都处于接收模式时，该线路应处于状态H。当两端处于不匹配的传输模式时，该线路的逻辑状态可以是不确定的，但不应损坏卡。操作过程中，卡和接口设备不应同时处于传输模式。正常操作条件下I/O的电特性见表9。

表9 正常操作条件下 I/O 的电特性

符号	条件	最小值	最大值

表 9（续）

IH IIH	VIH	0.7×Vcc V -300μA	Vcc V +20μA
VIL IIL	VIL	0V -1000μA	0.2×Vcc V +20μA
VOH IOH	Vcc 接外部上拉电阻 20kΩVOH	0.7×Vcc V	Vcc V +20μA
VOL	IOL=1mAa	0	0.08×Vcc V
tR 和 tF	CIN=30pF，COUT=30pF	-	1.0μs
注：I/O上的电压应维持在-0.3V～Vcc+0.3V。 接口设备的实现不应要求卡的电流下降大于500μA。			

当输入电压在允许范围内时，接口设备应能支持所定义范围内的输入电流。接口设备应向卡提供一个阻抗，以便卡能够保持所定义范围内的输出电压。

5.2.2.3 时钟（CLK）

该触点用来向卡提供时钟信号。时钟信号频率的实际值表示为 f。正常操作条件下 CLK 的电特性见表 10。

表10 正常操作条件下 CLK 的电特性

符号	条件	最小值	最大值
VIH IIH	VIH	0.7×Vcc V -20μA	Vcc V +150μA
VIL IIL	VIL	0V -200μA	0.2×Vcc V +20μA
tR 和 tF	CIN=30pF	-	9%的时钟周期
注：CLK上的电压应维持在-0.3V～Vcc+0.3V。			

时钟信号的占空因数应处于其稳定运行周期的 40%～60%之间。

当时钟频率处于 1MHz～5MHz（A 类）或 1MHz～4MHz（B 类）之间时，卡应能正常工作。

5.2.2.4 复位（RST）

该触点用来向卡提供复位信号。正常操作条件下 RST 的电特性见表 11。

表11 正常操作条件下 RST 的电特性

符号	条件	最小值	最大值
VIH IIH	VIH	0.7×Vcc V -20μA	Vcc V +150μA

表 11（续）

VIL IIL	VIL	0V -200μA	0.2×Vcc V +20μA
tR 和 tF	CIN=30pF	-	1μs
注：RST上的电压应维持在-0.3V～Vcc+0.3V。			

5.2.2.5 触点电阻

在整个生命周期内，卡触点的电阻（在清洁的卡和清洁的标准接口设备触点间测量时）应小于500mΩ（按GB/T 17554.3规定的测试方法）。

5.2.3 通讯协议

5.2.3.1 接触式

北京民生一卡通只使用字符传输协议（T=0）。以下将定义在ATR中提供的其他参数及与特定协议相关的参数。

协议根据以下层次模型定义：

——物理层，定义了位交换。

——数据链路层，包含以下定义：

a) 字符帧，定义了字符交换；

b) T=0，定义了 T=0 时的字符交换；

c) 对 T=0 的检错与纠错。

——传输层，定义了面向应用的报文传输。

——应用层，根据相同的应用协议，定义了报文交换的内容。

5.2.3.2 非接触式

描述了Type A PICC的协议激活、半双工传输协议和Type A PICC的协议停活。北京民生一卡通仅使用了信号接口Tpye A协议，信号接口Tpye B协议相关内容不在此描述。

5.2.3.3 复位应答

本条对ATR中可能回送的字符进行了详细描述。在符合基本ATR的情况下，一个字符是否存在，以及允许的取值范围（如果存在）由其“基本应答”信息指明。基本应答描述既不排斥其他字符值的使用，也不排斥发卡方增加或删减字符。例如，如果卡支持多个传输协议，它可以回送附加字符。但是，只有在卡返回一个基本ATR，或返回一个满足最低功能需求的终端所支持的ATR，才能保证字符的正确交换。

ATR中回送字符的最大个数（包括历史字符，但不包括TS）为32个。

6 卡结构组成

6.1 卡结构组成

北京民生一卡通卡结构由社保、金融、交通、北京通、残联、民政及数字人民币组成，卡结构见图11。

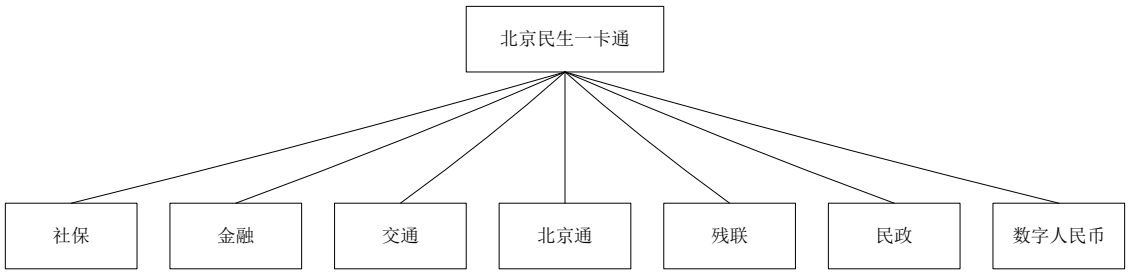


图11　卡结构

6.2　卡空间分配

根据各行业相关应用规范要求，各应用的应用标识符（AID）定义、空间分配、功能描述，见表12。

表12　空间分配

应用环境	应用名称	应用标识符（AID）	空间	功能说明
社保	社会保障应用	7378312E73682EC9E7BBE1B1A3D5CF	30K	社会保障应用数据结构
	非对称认证应用	504B492EC9E7BBE1B1A3D5CF	8K	标准的非对称认证应用
金融	金融应用	315041592E5359532E4444463031	16K	包含标准 PBOC3.0 相关数据内容（根据银行要求支持 UICS 相关内容）
		325041592E5359532E4444463031		
		A000000333010101		
交通	交通应用	325041592E5359532E4444463031	30K	交通部交通应用
		A000000632010105		
北京通	北京通应用	D15600001600	15K	包含各项公共服务功能
残联	中残联应用	D156000137	35K	程序区 20K+数据区 15K
民政	北京民政应用	F014181000000004	12.5K	民政应用
数字人民币	硬钱包	F044434550FF0101	124K	包含应用及个人化
	卡式软钱包	A000000044434550	4K	包含应用及个人化

6.3　社会保障应用数据结构

6.3.1　社会保障应用文件和数据规划

6.3.1.1　标识符和标签

社会保障系统环境的应用标识符见表13。

表13　社会保障系统环境的应用标识符

应用名称	应用标识符(AID)内容	应用标识符(AID)
SSSE	sx1.sh.社会保障	7378312E73682EC9E7BBE1B1A3D5CF

社会保障应用中各个具体应用的标识符（AID）应采用由国家IC卡注册中心颁发的RID，并通过RID选择该应用。对尚未获得RID的应用则采用规定的应用标签，并通过应用标签选择该应用。

社会保障应用的应用标识符、应用标签和应用标识符维护单位，见表14。

表14　社会保障应用的应用标识符和应用标签

应用名称	应用标识符	应用标签	应用标识符维护单位
公共应用	D15600000500	公共应用数据区	人力资源和社会保障部信息中心
就业与失业	D15600000501	就业与失业数据区	人力资源和社会保障部信息中心
社会保险 1	D15600000502	社会保险数据区 1	人力资源和社会保障部信息中心
社会保险 2	D15600000503	社会保险数据区 2	人力资源和社会保障部信息中心
人事与人才	D15600000504	人事与人才数据区	人力资源和社会保障部信息中心
生命与健康	D15600000505	生命与健康数据区	人力资源和社会保障部信息中心
社会救助	D15600000506	社会救助与优待抚恤数据区	人力资源和社会保障部信息中心
北京政务服务 1	D1560000050A	北京政务服务 1 信息区	人力资源和社会保障局
北京政务服务 2	D1560000050B	北京政务服务 2 信息区	人力资源和社会保障局
北京政务服务 3	D1560000050C	北京政务服务 3 信息区	人力资源和社会保障局
北京政务服务 4	D1560000050D	北京政务服务 4 信息区	人力资源和社会保障局
北京政务服务 5	D1560000050E	北京政务服务 5 信息区	人力资源和社会保障局

6.3.1.2　基本应用数据区

基本应用数据是指那些在社会保障应用的整个生命周期中不会改变的信息，该区内包括发卡机构数据文件（‘EF05’）、个人基本信息文件（‘EF06’）、指纹/指静脉数据文件（‘EF07’）和数字相片数据文件（‘EF08’）四个文件，它们被组织成基本文件存于SSSE的DDF下，见表15。

表15　基本应用数据区文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别
发卡机构数据文件	‘EF05’	‘05’	无	UKSSSE	记录	启用
个人基本信息文件	‘EF06’	‘06’	RKSSSE	UKSSSE	记录	启用
指纹/指静脉数据文件	‘EF07’	‘07’	RKSSSE	UKSSSE	透明	预设
数字相片数据文件	‘EF08’	‘08’	RKSSSE	UKSSSE	透明	预设

6.3.1.3　公共应用数据区

公共应用数据是指社会保障应用中由不同的应用提供方分别维护，但各种专业应用都需要使用的信息，包括持卡人的户籍信息文件（‘EF05’）、常住地信息文件（‘EF06’）、个人状况信息文件（‘EF07’）、婚姻状况信息文件（‘EF08’）、人员身份及就业单位信息文件（‘EF09’）、国家/地区及政治面貌信息文件（‘EF0A’）、学历信息文件（‘EF15’）及 5 个预留文件（‘EF16-1A’），它们被组织成基本文件存在于标识符为‘DF01’的 DF 下，见表 16。

表16　公共应用数据区文件特性

文件定义	文件 标识符	短文件 标识符	读控制	写控制	文件结构	类别
户籍信息文件	‘EF05’	‘05’	PIN 或 RK1DF01	UK1DF01	记录	启用
常住地信息文件	‘EF06’	‘06’	PIN 或 RK1DF01	UK4DF01	记录	启用
个人状况信息文件	‘EF07’	‘07’	PIN 或 RK1DF01	UK2DF01	记录	启用
婚姻状况信息文件	‘EF08’	‘08’	PIN 或 RK1DF01	UK3DF01	记录	启用
人员身份及就业单位信息文件	‘EF09’	‘09’	PIN 或 RK1DF01	UK2DF01	记录	启用
国家/地区及政治面貌信息文件	‘EF0A’	‘0A’	PIN 或 RK1DF01	UK5DF01	记录	启用
学历信息文件	‘EF15’	‘15’	PIN 或 RK1DF01	UK6DF01	记录	启用
预留信息文件 1	‘EF16’	‘16’	无	UK7DF01	透明	预留
预留信息文件 2	‘EF17’	‘17’	无	UK8DF01	透明	预留
预留信息文件 3	‘EF18’	‘18’	无	UK9DF01	透明	预留
预留信息文件 4	‘EF19’	‘19’	无	UKADF01	透明	预留
预留信息文件 5	‘EF1A’	‘1A’	无	UKBDF01	透明	预留

6.3.1.4　就业与失业数据区

就业与失业应用数据是指社会保障应用中由人力资源和社会保障部门维护，记录持卡人就业和失业等情况的信息，包括持卡人的职业和专业技能信息文件（‘EF05’）、就业状况信息文件（‘EF06’）、就业记录信息文件（‘EF07’）、就业创业证信息文件（‘EF09’）、就业援助对象认定信息文件（‘EF15’）、就业扶持政策享受信息文件（‘EF16’），它们被组织成基本文件存在于标志符为‘DF02’的 DF 下，见表17。

表17　就业与失业数据区文件特性

文件定义	文件 标志符	短文件 标志符	读控制	写控制	文件结构	类别
职业和专业技能信息文件	‘EF05’	‘05’	PIN 或 RK1DF02	UK1DF02	记录	预设
就业状况信息文件	‘EF06’	‘06’	PIN 或 RK1DF02	UK2DF02	记录	启用
就业记录信息文件	‘EF07’	‘07’	PIN 或 RK1DF02	UK3DF02	循环	启用
就业创业证信息文件	‘EF09’	‘09’	PIN 或 RK1DF02	UK4DF02	记录	启用
就业援助对象认定信息文件	‘EF15’	‘15’	PIN 或 RK1DF02	UK5DF02	记录	启用
就业扶持政策享受信息文件	‘EF16’	‘16’	PIN 或 RK1DF02	UK6DF02	循环	启用

6.3.1.5　社会保险数据区 1

本数据区中的应用数据是指社会保障应用中由人力资源社会保障部门维护，记录持卡人除医疗保险以外的各项社会保险的信息，包括失业保险信息文件（‘EF05’）、劳动能力鉴定信息文件（‘EF06’）、养老保险信息文件（‘EF07’）、工伤保险信息文件（‘EF15’）、生育保险信息文件（‘EF16’）、工伤认定信息文件（‘EF17’）、供养亲属信息文件（‘EF18’）、参保凭证信息文件（‘EF19’），它们被组织成基本文件存在于标识符为‘DF03’的DF下，见表18。

表18　社会保险数据区 1 文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别
失业保险信息文件	‘EF05’	‘05’	PIN 或 RK2DF03	UK1DF03	记录	启用
劳动能力鉴定信息文件	‘EF06’	‘06’	PIN 或 RK1DF03	UK2DF03	记录	启用
养老保险信息文件	‘EF07’	‘07’	PIN 或 RK1DF03	UK3DF03	记录	启用
工伤保险信息文件	‘EF15’	‘15’	PIN 或 RK1DF03	UK4DF03	记录	启用
生育保险信息文件	‘EF16’	‘16’	PIN 或 RK1DF03	UK5DF03	记录	启用
工伤认定信息文件	‘EF17’	‘17’	PIN 或 RK1DF03	UK6DF03	记录	启用
供养亲属信息文件	‘EF18’	‘18’	PIN 或 RK1DF03	UK7DF03	记录	启用
参保凭证信息文件	‘EF19’	‘19’	PIN 或 RK1DF03	UK8DF03	记录	启用

6.3.1.6　社会保险数据区 2

本数据区中的应用数据是指社会保障应用中由人力资源社会保障部门以及定点医疗机构、零售药店等医疗服务机构维护，记录持卡人医疗保险和医疗费用结算有关情况的信息。包括医疗、工伤、生育保险基本信息文件（‘EF 05’）、医疗保险临时脱网结算信息文件（‘EF06’）、医疗交易明细文件（‘EF 08’）、特殊医疗结算记录文件（‘EF15’）。它们被组织成基本文件存在于标识符为‘DF04’的DF下，见表19。

表19　社会保险数据区 2 文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别
医疗、工伤、生育保险基本信息文件	‘EF05’	‘05’	PIN 或 RK1DF04	UK1DF04	记录	启用
医疗保险临时脱网结算信息文件	‘EF06’	‘06’	PIN 与 RK1DF04	UK2DF04	记录	启用
医疗交易明细文件	‘EF08’	‘08’	PIN	不允许改写	循环	启用
特殊医疗结算记录文件	‘EF15’	‘15’	PIN 或 RK1DF04	UK2DF04	循环	启用

6.3.1.7　生命与健康应用数据区

生命与健康数据是指社会保障应用中由卫生部门维护，记录持卡人有关健康状况的信息，它们被组织成基本文件存在于标识符为‘DF05’的DF下,见表20。

表20　生命与健康应用数据区文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别

表 20（续）

生命与健康数据文件	‘EF05’	‘05’	自由	UK1DF05	记录	预设

6.3.1.8 社会救助与优待抚恤应用数据区

社会救助与优待抚恤应用数据是指社会保障应用中由民政部门维护，记录持卡人享受社会救助和优待抚恤情况的信息，包括社会救助信息和优待抚恤信息，它们被组织成基本文件存在于标识符为‘DF06’的DF下，见表21。

表21 社会救助与抚恤应用数据区文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别
社会救助信息文件	‘EF05’	‘05’	RK1DF06	UK1DF06	记录	预设
优待抚恤信息数据文件	‘EF06’	‘06’	RK1DF06	UK2DF06	记录	预设

6.3.1.9 人事与人才数据区

人事与人才数据是指社会保障应用中由人力资源社会保障部门以及相关人事管理单位分别维护，但各种专业应用都需要使用的人事人才信息，包括荣誉信息文件（‘EF05’）、专家信息文件（‘EF06’）、军队转业干部信息文件（‘EF07’），它们被组织成基本文件存在于标识符为‘DF07’的DF下，见表22。

表22 人事与人才数据区文件特性

文件定义	文件 标识符	短文件 标识符	读控制	写控制	文件结构	类别
荣誉信息文件	‘EF05’	‘05’	RK1DF07	UK1DF07	记录	预设
专家信息文件	‘EF06’	‘06’	RK2DF07	UK2DF07	记录	预设
军队转业干部信息文件	‘EF07’	‘07’	RK3DF07	UK3DF07	记录	预设

6.3.1.10 社会保障应用数据项格式

由于许多数据项的实际长度随持卡人的具体情况存在差异，当某一数据项的实际长度不足规范所定义的长度时，对格式为cn的数据项左靠齐并且右补十六进制‘F’，格式为an的数据项左靠齐并且右补十六进制‘0’，数据项的长度达到本规范所定义的长度，见表23。

表23 数据项格式及属性

标志	数据项	类型	长度	所属文件	备注
‘01’	卡识别码	cn	‘10’	SSSE ‘EF05’	—
‘02’	卡的类别	an	‘01’		
‘03’	规范版本	an	‘04’		
‘04’	初始化机构编号	cn	‘0C’		
‘05’	发卡日期	cn	‘04’		
‘06’	卡有效期	cn	‘04’		
‘07’	卡号	an	‘09’		

表 23（续）

‘08’	社会保障号码	an	‘12’	‘SSSE’ ‘EF06’	—
‘09’	姓名	an	‘1E’		
‘4E’	姓名扩展	an	‘14’		
‘0A’	性别	an	‘01’		
‘0B’	民族	cn	‘01’		
‘0C’	出生地	cn	‘03’		
‘0D’	出生日期	cn	‘04’		
—	指纹/指静脉	b	‘1000’	‘SSSE’ ‘EF07’	起始位置 0000
—	数字相片	b	‘2000’	‘SSSE’ ‘EF08’	起始位置 0000
‘20’	户口性质	an	‘02’	‘DF01’ ‘EF05’	—
‘21’	户口所在地地址	an	‘50’		
‘0E’	户口所在地行政区划代码	cn	‘03’		
‘23’	常住所在地地址	an	‘50’	‘DF01’ ‘EF06’	—
‘24’	常住所在地行政区划代码	cn	‘03’		
‘28’	联系电话	an	‘0F’		
‘2C’	联系人（监护人）姓名	an	‘32’		
‘2D’	联系人（监护人）联系电话	an	‘0F’		
‘29’	就业状态	an	‘01’	‘DF01’ ‘EF07’	—
‘2B’	婚姻状况	an	‘01’	‘DF01’ ‘EF08’	—
‘2E’	单位名称	an	‘46’	‘DF01’ ‘EF09’	—
‘30’	单位组织机构代码	an	‘09’		
‘32’	人员身份类别	an	‘02’		
‘37’	国家/地区代码	an	‘03’	‘DF01’ ‘EF0A’	—
‘38’	政治面貌	an	‘02’		
‘39’	参加党派日期	cn	‘04’		
‘2A’	学历	cn	‘01’	‘DF01’ ‘EF15’	—
‘40’	学位信息 1(见标志 ‘57’ - ‘59’)	B-TLV	‘34’		
‘40’	学位信息 2(见标志 ‘57’ - ‘59’)	B-TLV	‘34’		
‘40’	学位信息 3(见标志 ‘57’ - ‘59’)	B-TLV	‘34’		
‘57’	学位	an	‘03’		
‘58’	所学专业名称	cn	‘03’		
‘59’	毕业学校名称	an	‘28’		
—	预留信息文件 1	b	‘128’	‘DF01’‘EF16’	起始位置 0000
—	预留信息文件 2	b	‘128’	‘DF01’‘EF17’	起始位置 0000

表 23（续）

—	预留信息文件 3	b	‘128’	‘DF01’‘EF18’	起始位置 0000
—	预留信息文件 4	b	‘128’	‘DF01’‘EF19’	起始位置 0000
—	预留信息文件 5	b	‘128’	‘DF01’‘EF1A’	起始位置 0000
‘42’	专业技术职务代码	an	‘03’	‘DF02’ ‘EF05’	—
‘41’	专业技术职务级别	an	‘03’		
‘43’	职业资格(技能人员等级)信息 1 （见标志‘5A’-‘5E’）	B-TLV	‘6C’		
‘43’	职业资格(技能人员等级)信息 2 （见标志‘5A’-‘5E’）	B-TLV	‘6C’		
‘5A’	职业资格(技能人员等级)名称代码	an	‘07’		
‘5B’	职业资格(技能人员等级)等级	an	‘01’		
‘5C’	职业资格(技能人员等级)证书发证/年检机构名称	an	‘46’		
‘5D’	职业资格(技能人员等级)证书发证/年检日期	cn	‘04’		
‘5E’	职业资格(技能人员等级)证书编号	an	‘10’		
‘44’	职业资格（专业技术人员）信息 1 （见标志‘33’-‘36’）	B-TLV	‘65’		
‘44’	职业资格（专业技术人员）信息 2 （见标志‘33’-‘36’）	B-TLV	‘65’		
‘33’	职业资格（专业技术人员）名称代码	an	‘03’		
‘34’	职业资格（专业技术人员）注册登记/年检机构名称	an	‘46’		
‘35’	职业资格（专业技术人员）注册登记/年检日期	cn	‘04’		
‘36’	职业资格（专业技术人员）证书编号	an	‘10’		
‘4C’	最近一次办理就业登记日期	cn	‘04’	‘DF02’ ‘EF06’	—
‘4B’	就业登记类型及形式	an	‘05’		
‘4D’	就业登记地行政区划代码	cn	‘03’		
‘60’	最近一次办理失业登记日期	cn	‘04’		
‘4F’	失业登记类型、原因及注销原因	an	‘06’		
‘50’	失业登记地行政区划代码	cn	‘03’		
‘3A’	现从事职业（工种）	an	‘07’		
-	就业记录		‘55’	‘DF02’ ‘EF07’	循环文件,至少 4 条记录
-	从事职业（工种）	an	‘07’		

表 23（续）

-	就业起始日期	cn	‘04’	‘DF02’ ‘EF07’	循环文件，至少 4 条记录
-	就业终止日期	cn	‘04’		
-	就业工作单位名称	an	‘46’		
‘55’	就业创业证编号	an	‘10’	‘DF02’ ‘EF09’	—
‘56’	就业创业证发证机构	an	‘46’		
‘96’	就业创业证发证/年检日期	cn	‘04’		
‘97’	就业创业证发证地行政区划代码	cn	‘03’		
‘99’	就业援助对象认定信息 1（见标志‘10’到‘12’）	B-TLV	‘10’	‘DF02’ ‘EF15’	—
‘99’	就业援助对象认定信息 2（见标志‘10’到‘12’）	B-TLV	‘10’		
‘99’	就业援助对象认定信息 3（见标志‘10’到‘12’）	B-TLV	‘10’		
‘99’	就业援助对象认定信息 4（见标志‘10’到‘12’）	B-TLV	‘10’		
‘10’	认定为就业援助对象类型	an	‘03’		
‘11’	就业援助认定日期	cn	‘04’		
‘12’	就业援助认定地行政区划代码	cn	‘03’		
‘0F’	退出就业援助对象范围的认定日期	cn	‘04’		
‘1F’	退出就业援助对象范围的认定地行政区划代码	cn	‘03’		
—	就业扶持政策享受信息	—	‘12’	‘DF02’ ‘EF16’	循环文件，至少 4 条记录
—	享受就业扶持政策类型	an	‘03’		
—	享受就业扶持政策核准日期	cn	‘04’		
—	就业扶持政策享受开始日期	cn	‘04’		
—	就业扶持政策享受终止日期	cn	‘04’		
—	就业扶持政策享受地行政区划代码	cn	‘03’		
‘61’	失业保险参保地所属行政区划代码	cn	‘03’	‘DF03’ ‘EF05’	—
‘98’	最近一次失业保险金申领日期	cn	‘04’		
‘62’	失业保险金申领报到日期/信息更新日期	cn	‘04’		
‘63’	失业保险累计缴费月数	an	‘03’		
‘64’	失业保险有效缴费月数	an	‘03’		
‘65’	应领取失业保险金月数	an	‘03’		
‘66’	已领取失业保险金月数	an	‘03’		
‘45’	劳动能力鉴定编号	an	‘14’	‘DF03’ ‘EF06’	—

表 23（续）

‘46’	申请鉴定（确认）事项	an	‘02’	‘DF03’ ‘EF06’	—
‘47’	伤残等级	an	‘02’		
‘48’	生活自理障碍等级	an	‘01’		
‘49’	丧失劳动能力鉴定结论	an	‘01’		
‘67’	劳动能力鉴定日期	cn	‘04’		
‘6B’	劳动能力鉴定机构名称	an	‘3C’		
‘4A’	申请确认事项 1 （见标志‘13’—‘17’）	B-TLV	‘61’		
‘4A’	申请确认事项 2 （见标志‘13’—‘17’）	B-TLV	‘61’		
‘4A’	申请确认事项 3 （见标志‘13’—‘17’）	B-TLV	‘61’		
‘13’	申请确认事项	an	‘02’		
‘14’	确认事项结论	an	‘01’		
‘15’	配置辅助器具项目名称	an	‘14’		
‘16’	申请劳动能力确认日期	cn	‘04’		
‘17’	申请劳动能力确认机构名称	an	‘3C’		
‘70’	养老保险险种类型	an	‘03’	‘DF03’ ‘EF07’	—
‘71’	养老保险参保地所属行政区划代码	cn	‘03’		
‘6E’	基本养老保险个人账户建立日期	cn	‘04’		
‘6C’	离退休日期	cn	‘04’		
‘6F’	待遇享受开始日期	cn	‘04’		
‘73’	养老保险信息更新日期	cn	‘04’		
‘7A’	工伤保险参保地所属行政区划代码	cn	‘03’	‘DF03’ ‘EF15’	—
‘7B’	工伤定期待遇享受开始日期	cn	‘04’		
‘7C’	工伤保险信息更新日期	cn	‘04’		
‘51’	生育保险参保地所属行政区划代码	cn	‘03’	‘DF03’ ‘EF16’	—
‘5F’	职工未就业配偶标识	an	‘01’		
‘3B’	工伤认定编号	an	‘14’	‘DF03’ ‘EF17’	—
‘3C’	用人单位名称	an	‘46’		
‘3D’	工伤认定结论	an	‘01’		
‘3E’	工伤认定日期	cn	‘04’		
‘3F’	工伤认定部门名称	an	‘3C’		
‘74’	供养险种类型	an	‘03’	‘DF03’ ‘EF18’	—
‘75’	参保地所属行政区划代码	cn	‘03’		

表 23（续）

‘76’	供养关系	cn	‘01’	‘DF03’ ‘EF18’	—
‘77’	供养待遇享受开始日期	cn	‘04’		
‘78’	供养亲属信息更新日期	cn	‘04’		
‘79’	养老保险参保凭证信息 （见标志‘18’—‘1E’）	B-TLV	‘27’	‘DF03’ ‘EF19’	—
‘79’	医疗保险参保凭证信息 （见标志‘18’—‘1E’）	B-TLV	‘27’		
‘79’	失业保险参保凭证信息 （见标志‘18’—‘1E’）	B-TLV	‘27’		
‘79’	预留参保凭证信息 （见标志‘18’—‘1E’）	B-TLV	‘27’		
‘18’	险种类型	an	‘03’		
‘19’	参保地所属行政区划代码	cn	‘03’		
‘1A’	本地参保起始日期	cn	‘04’		
‘1B’	本地参保终止日期	cn	‘04’		
‘1C’	本地个人实际缴费金额	cn	‘04’		
‘1D’	本地实际缴费月数	an	‘03’		
‘1E’	凭证出具日期	cn	‘04’		
‘81’	医疗保险险种类型及标识	an	‘08’	‘DF04’ ‘EF05’	—
‘84’	医疗保险参保地所属行政区划代码	cn	‘03’		
‘87’	健康档案编号	an	‘11’		
‘8C’	医疗保险参保人员类别	cn	‘01’		
‘80’	基本医疗保险个人账户建立日期	cn	‘04’		
‘8B’	基本医疗保险个人账号	an	‘1D’		
‘8A’	医疗证号	an	‘0F’		
‘83’	定点医疗机构代码 1	an	‘09’		
‘86’	定点医疗机构代码 2	an	‘09’		
‘89’	定点医疗机构代码 3	an	‘09’		
‘7D’	工伤协议医疗机构代码 1	an	‘09’		
‘7E’	工伤协议医疗机构代码 2	an	‘09’		
‘7F’	工伤协议医疗机构代码 3	an	‘09’		
‘8D’	生育定点医疗机构代码 1	an	‘09’		
‘8E’	生育定点医疗机构代码 2	an	‘09’		
‘8F’	医疗保险用卡方式	an	‘01’		
‘90’	准许脱网医疗费用结算标识	an	‘01’	‘DF04’ ‘EF06’	—

表 23（续）

‘92’	脱网医疗费用结算累计金额	cn	‘04’	‘DF04’ ‘EF06’	—
‘93’	脱网医疗费用结算累计次数	an	‘02’		
-	医疗交易明细	-	‘1C’	‘DF04’ ‘EF08’	循环文件，至少 30 条记录
-	交易序号	b	‘02’		
-	交易类型	an	‘01’		
-	终端机编号	cn	‘06’		
-	交易时间	cn	‘07’		
-	个人账户交易金额	b	‘04’		
-	个人自付金额	b	‘04’		
-	统筹基金支付金额	b	‘04’		
-	特殊医疗结算记录	-	‘03’	‘DF04’ ‘EF15’	循环文件,至少 8 条
-	交易序号	b	‘02’		
-	结算类别	an	‘01’		
‘F0’	荣誉称号名称代码	an	‘02’	‘DF07’ ‘EF05’	—
‘F1’	荣誉称号级别	an	‘01’		
‘F2’	荣誉称号批准日期	cn	‘04’		
‘F3’	荣誉奖章名称代码	an	‘03’		
‘F4’	荣誉奖章批准日期	cn	‘04’		
‘F5’	专家类别	an	‘03’	‘DF07’ ‘EF06’	—
‘F6’	批准日期	cn	‘04’		
‘F7’	批准单位名称	an	‘46’		
‘F8’	批准转业日期	cn	‘04’	‘DF07’ ‘EF07’	—
‘F9’	安置方式	an	‘01’		
‘A0’	健康状况	an	‘01’	‘DF05’ ‘EF05’	—
‘A1’	残疾类别	an	‘01’		
‘B9’	残疾等级	an	‘01’		
‘A2’	ABO 血型代码	an	‘04’		
‘A9’	RH 血型代码	cn	‘01’		
‘A3’	禁忌药信息 1（见标志 ‘A5’ — ‘A6’）	B-TLV	‘18’		
‘A3’	禁忌药信息 2（见标志 ‘A5’ — ‘A6’）	B-TLV	‘18’		
‘A3’	禁忌药信息 3（见标志 ‘A5’ — ‘A6’）	B-TLV	‘18’		
‘A3’	禁忌药信息 4（见标志 ‘A5’ — ‘A6’）	B-TLV	‘18’		
‘A3’	禁忌药信息 5（见标志 ‘A5’ — ‘A6’）	B-TLV	‘18’		
‘A5’	禁忌药	an	‘10’		
‘A6’	禁忌药代码	an	‘04’		

表 23（续）

‘A4’	重大疾病信息 1（见标志‘A7’-‘A8’）	B-TLV	‘17’		
‘A4’	重大疾病信息 2（见标志‘A7’-‘A8’）	B-TLV	‘17’		
‘A4’	重大疾病信息 3（见标志‘A7’-‘A8’）	B-TLV	‘17’		
‘A4’	重大疾病信息 4（见标志‘A7’-‘A8’）	B-TLV	‘17’		
‘A4’	重大疾病信息 5（见标志‘A7’-‘A8’）	B-TLV	‘17’		
‘A7’	重大疾病	an	‘10’		
‘A8’	重大疾病代码	an	‘03’		
‘BA’	过敏物质名称	an	‘14’		
‘BB’	过敏反应	an	‘64’		
‘AA’	免疫接种名称	an	‘14’		
‘AB’	免疫接种时间	cn	‘04’		
‘AC’	哮喘标志	an	‘01’		
‘AD’	心脏病标志	an	‘01’	‘DF05’ ‘EF05’	—
‘AE’	心脑血管标志	an	‘01’		
‘AF’	癫痫病标志	an	‘01’		
‘B0’	凝血紊乱标志	an	‘01’		
‘B1’	糖尿病标志	an	‘01’		
‘B2’	青光眼标志	an	‘01’		
‘B3’	透析标志	an	‘01’		
‘B4’	器官移植标志	an	‘01’		
‘B5’	器官缺失标志	an	‘01’		
‘B6’	可装卸的义肢标志	an	‘01’		
‘B7’	心脏起搏器标志	an	‘01’		
‘BC’	精神病标志	an	‘01’		
‘B8’	其他医学警示名称	an	‘28’		
‘C0’	救助金发放机构名称	an	‘46’		
‘C2’	救助金发放机构代码	an	‘09’		
‘C3’	社会救助信息 1（见标志‘E3’-‘E7’）	B-TLV	‘1A’		
‘C4’	社会救助信息 2（见标志‘E3’-‘E7’）	B-TLV	‘1A’		
‘C5’	社会救助信息 3（见标志‘E3’-‘E7’）	B-TLV	‘1A’	‘DF06’ ‘EF05’	—
‘E3’	社会救助代码	cn	‘01’		
‘E4’	社会救助批准日期	cn	‘04’		
‘E5’	社会救助复核日期	cn	‘04’		
‘E6’	最近一次获得社会救助的金额	cn	‘04’		

表 23（续）

‘E7’	社会救助已发放月度	cn	‘03’	‘DF06’ ‘EF05’	—
‘C6’	优待抚恤金发放机构	an	‘46’	‘DF06’ ‘EF06’	—
‘C8’	优待抚恤金发放机构代码	an	‘09’		
‘C9’	优待抚恤代码 1	cn	‘01’		
‘CA’	优待抚恤批准日期 1	cn	‘04’		
‘CB’	优待抚恤截止日期 1	cn	‘04’		
‘CC’	当年义务兵优待金发放标准	cn	‘04’		
‘CD’	优待抚恤已发放年度 1	cn	‘02’		
‘CE’	优待抚恤代码 2	cn	‘01’		
‘CF’	优待抚恤批准日期 2	cn	‘04’		
‘D0’	优待抚恤截止日期 2	cn	‘04’		
‘D1’	当年定期抚恤金发放标准	cn	‘04’		
‘D2’	优待抚恤已发放月度 2	cn	‘03’		
‘D3’	优待抚恤代码 3	cn	‘01’		
‘D4’	优待抚恤批准日期 3	cn	‘04’		
‘D5’	优待抚恤截止日期 3	cn	‘04’		
‘D6’	当年定期补助发放标准	cn	‘04’		
‘D7’	优待抚恤已发放月度 3	cn	‘03’		
‘D8’	优待抚恤代码 4	cn	‘01’		
‘D9’	优待抚恤批准日期 4	cn	‘04’		
‘DA’	优待抚恤截止日期 4	cn	‘04’		
‘DB’	当年抚恤金标准（中央）	cn	‘04’		
‘DC’	当年抚恤金补助标准（地方）	cn	‘04’		
‘DD’	当年保健金标准（中央）	cn	‘04’		
‘DE’	当年保健金补助标准（地方）	cn	‘04’		
‘DF’	伤残抚恤金已发放月度	cn	‘03’		
‘E0’	伤残抚恤补助金已发放月度	cn	‘03’		
‘E1’	伤残保健金已发放年度	cn	‘02’		
‘E2’	伤残保健补助金已发放年度	cn	‘02’		

6.3.1.11 北京政务服务 1 数据区

本文档描述的是按照LD/T 32.6，应用扩充规则相关章节的要求，进行的应用扩充描述。北京政务服务1数据区，包括基本信息文件（‘EF05’）及预留空间,它们存在于标识符为‘DF0A’的DF下。

北京政务服务1数据区规划空间2K，见表24、表25。

表24　北京政务服务 1 文件特性

文件定义	文件 标识符	短文件 标识符	读控制	写控制	文件结构	类别
基本信息文件	‘EF05’	‘05’	PIN 或 RK1DF0A	UK1DF0A	透明	预设

表25　EF05 基本信息文件

文件 标识符	‘EF05’	SFI	‘05’	读控制	PIN 或 RK1DF0A	写控制	UK1DF0A	文件结 构	透明
数据空间	‘64’ [100 字节]								
标志	数据项							类型	长度
—	—							—	‘03’
—	默认值为 0x00							—	‘61’

6.3.1.12　北京政务服务 2 数据区

北京政务服务2数据区，包括基本信息文件(‘EF05’)及预留空间,它们存在于标识符为‘DF0B’的DF下。

北京政务服务2数据区规划空间1K，见表26、表27。

表26　北京政务服务 2 文件特性

文件定义	文件 标识符	短文件 标识符	读控制	写控制	文件结构	类别
基本信息文件	‘EF05’	‘05’	PIN 或 RK1DF0B	UK1DF0B	透明	预设

表27　EF05 基本信息文件

文件标识符	‘EF05’	SFI	‘05’	读控制	PIN 或 RK1DF0B	写控制	UK1DF0B	文件结构	透明
数据空间	‘64’ [100 字节]								
标志	数据项							类型	长度
—	—							—	‘03’
—	默认值为 0x00							—	‘61’

6.3.1.13　北京政务服务 3 数据区

北京政务服务3数据区，包括基本信息文件(‘EF05’)及预留空间,它们被组织成基本文件存在于标识符为‘DF0C’的DF下。

北京政务服务3数据区规划空间1K，见表28、表29。

表28　北京政务服务 3 文件特性

文件定义	文件 标识符	短文件 标识符	读控制	写控制	文件结构	类别

表 28（续）

基本信息文件	‘EF05’	‘05’	PIN 或 RK1DF0C	UK1DF0C	透明	预设

表29　EF05 基本信息文件

文件标识符	‘EF05’	SFI	‘05’	读控制	PIN 或 RK1DF0C	写控制	UK1DF0C	文件结构	透明
数据空间	‘64’ [100 字节]								
标志	数据项							类型	长度
—	—							—	‘03’
—	默认值为 0x00							—	‘61’

6.3.1.14　北京政务服务 4 数据区

北京政务服务4数据区,包括学生基本信息文件(‘EF05’)及预留空间,它们存在于标识符为‘DF0D’的DF下。

北京政务服务4数据区规划空间1K，见表30、表31。

表30　北京政务服务 4 文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别
基本信息文件	‘EF05’	‘05’	PIN 或 RK1DF0D	UK1DF0D	透明	预设

表31　EF05 基本信息文件

文件标识符	‘EF05’	SFI	‘05’	读控制	PIN 或 RK1DF0D	写控制	UK1DF0D	文件结构	透明
数据空间	‘64’ [100 字节]								
标志	数据项							类型	长度
—	—							—	‘03’
—	默认值为 0x00							—	‘61’

6.3.1.15　北京政务服务 5 数据区

北京政务服务5数据区包括基本信息文件(‘EF05’)及预留空间,它们存在于标识符为‘DF0E’的DF下。

北京政务服务5数据区规划空间1K，见表32、表33。

表32　北京政务服务5文件特性

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别
基本信息文件	‘EF05’	‘05’	PIN或RK1DF0E	UK1DF0E	透明	预设

表33　EF05 基本信息文件

文件标识符	‘EF05’	SFI	‘05’	读控制	PIN或RK1 DF0E	写控制	UK1DF0E	文件结构	透明
数据空间	‘64’ [100字节]								
标志	数据项							类型	长度
—	—							—	‘03’
—	默认值为0x00							—	‘61’

6.3.2　社会保障应用密钥管理

6.3.2.1　分散因子

一级分散因子是以省份标识号为基本元素构成的，构成方法如下：取用户卡中SSSE下的EF05文件中的“卡的识别码”记录的前三个字节“应用城市代码”（6位十进制数），将其展开为6个字节的ASCII码（如：110000展开为‘31 31 30 30 30 30’），取其中头两个字节，后补十六进制数‘30 30 30 30 73 68’，形成8个字节的一级分散因子。

二级分散因子是以地市标识号为基本元素构成的，构成方法如下：取用户卡中SSSE下的EF05文件中的“卡的识别码”记录的前三个字节“应用城市代码”（6位十进制数），将其展开为6个字节的ASCII码（如：110000展开为‘31 31 30 30 30 30’），后补十六进制数‘73 78’，形成8个字节的二级分散因子。

三级分散因子是由卡标识号构成的，构成数据为：用户卡复位应答历史字节的第6～13个字节。历史字节定义应按照LD/T 32.2的规定执行，其中T8-T9为发卡地区所在地的行政区划代码前四位，TA-TD由发卡地区自行编排并保持每张卡的唯一性。

终端机编号定义：前6位为发卡地区城市代码，第7-12位字符由PSAM卡或终端设备发放机构定义。

6.3.2.2　社会保障应用密钥列表

社会保障应用密钥列表，见表34。

表34　社会保障应用密钥列表

密钥	标识/索引	版本	限制	备注
IRK	‘00’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
PUK	‘06’	‘01’	‘03’	—
STKSSSE	‘02’	—	‘00’	—
BK	‘05’	‘01’	‘03’	—

表 34（续）

UKSSSE	‘04’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RKSSSE	‘0A’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
PIN	‘00’	—	‘06’	—
STKDF01	‘82’	—	‘00’	—
UK1DF01	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK2DF01	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK3DF01	‘85’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK4DF01	‘86’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK5DF01	‘87’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK6DF01	‘89’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK7DF01	‘8A’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK8DF01	‘8B’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK9DF01	‘8C’	‘01’	‘03’	—
		‘02’		—

表 34（续）

UK9DF01	‘8C’	‘03’	‘03’	—
UKADF01	‘8D’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UKBDF01	‘8E’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF01	‘88’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
STKDF02	‘82’	—	‘00’	—
UK1DF02	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK2DF02	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK3DF02	‘85’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK4DF02	‘86’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK5DF02	‘87’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK6DF02	‘89’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF02	‘88’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
STKDF03	‘82’	—	‘00’	—
LKDF03	‘83’	‘01’	‘03’	—

表 34（续）

UK1DF03	‘86’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK2DF03	‘87’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK3DF03	‘88’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK4DF03	‘89’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK5DF03	‘8A’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK6DF03	‘8B’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK7DF03	‘8C’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK8DF03	‘8D’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF03	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK2DF03	‘85’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
STKDF04	‘82’	—	‘00’	—
LKDF04	‘83’	‘01’	‘03’	—
UK1DF04	‘85’	‘01’	‘03’	—
		‘02’		—

表 34（续）

		‘03’		—
UK2DF04	‘86’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF04	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
		‘02’		—
		‘03’		—
STKDF07	‘82’	—	‘00’	—
UK1DF07	‘86’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK2DF07	‘87’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK3DF07	‘88’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF07	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK2DF07	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK3DF07	‘85’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
STKDF05	‘82’	—	‘00’	—
UK1DF05	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
STKDF06	‘82’	—	‘00’	—
LKDF06	‘87’	‘01’	‘03’	—

表 34（续）

UK1DF06	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK2DF06	‘85’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF06	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK1DF0A	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF0A	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK1DF0B	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF0B	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK1DF0C	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF0C	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK1DF0D	‘84’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
RK1DF0D	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—
UK1DF0E	‘84’	‘01’	‘03’	—

表 34（续）

UK1DF0E	‘84’	‘02’	‘03’	—
		‘03’		—
RK1DF0E	‘83’	‘01’	‘03’	—
		‘02’		—
		‘03’		—

6.3.3 非对称认证应用文件和数据规划

6.3.3.1 标识和标签

非对称认证系统环境的应用标识符见表35。

表35 非对称认证系统环境的应用标识符

应用名称	应用标识符内容	应用标识符
ACSE	PKI.社会保障	504B492EC9E7BBE1B1A3D5CF

非对称认证系统环境的文件结构以GM/T 0016中定义的应用逻辑结构为基础，示意图见图12，可根据实际情况进行扩展，如增加应用、容器或临时加解密公私钥等。

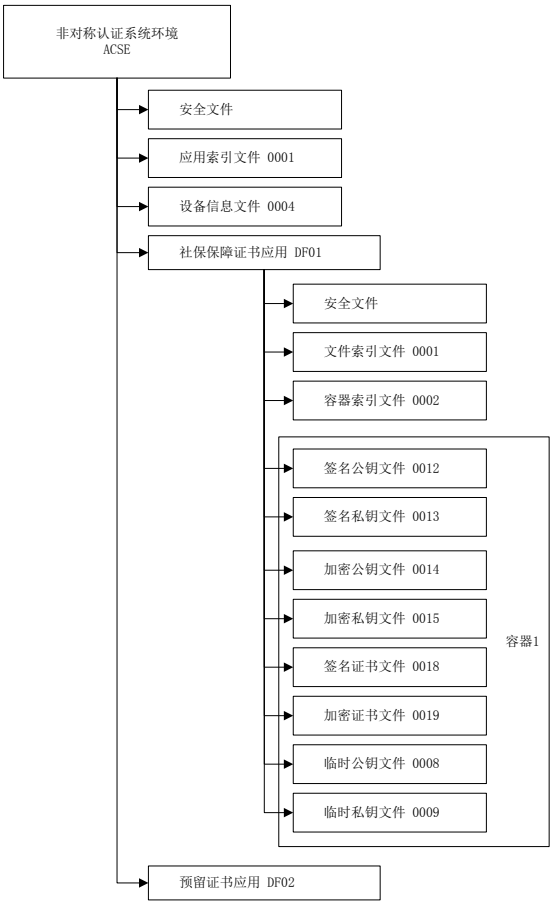


图12 非对称认证系统环境文件结构示意图

非对称认证应用的文件定义见表36。

表36　非对称认证应用的文件定义

数据区	文件标识	文件内容	文件结构	读控制	写控制	使用
非对称认证系统环境 ACSE	‘0001’	应用索引文件	定长记录	无	MKACSE	—
	‘0004’	设备信息文件	透明	无	MKACSE	—
社会保障证书应用 DF01	‘0001’	文件索引文件	定长记录	无	MKDF01	—
	‘0002’	容器索引文件	定长记录	无	MKDF01	—
容器 1	‘0012’	签名公钥文件	内部	无	PIN	无
	‘0013’	签名私钥文件	内部	不允许读	PIN	PIN
	‘0014’	加密公钥文件	内部	无	PIN	无
	‘0015’	加密私钥文件	内部	不允许读	PIN	PIN
	‘0018’	签名证书文件	透明	无	PIN	—
	‘0019’	加密证书文件	透明	无	PIN	—
	‘0008’	临时公钥文件	内部	无	PIN	无
	‘0009’	临时私钥文件	内部	不允许读	PIN	PIN
注：表中PIN为当前目录下的用户PIN，PIN标识符为01； ‘0018’和‘0019’文件大小分别为1K。						

6.3.3.2　非对称认证系统环境（ACSE）

6.3.3.2.1　0001 应用索引文件

应用索引文件的定义见表37。

表37　应用索引文件

文件标识符	‘0001’	SFI	‘01’	读控制	无	写控制	MKACSE	文件结构	定长记录
标志	数据项							类型	长度
01	应用名称 1							—	‘10’
01	应用名称 2							—	‘10’
注：表中的如下数据项使用固定值： “应用名称1”为社会保障证书应用名称 “SS.CERT.ADF1”； “应用名称2”为预留证书应用名称，命名规则按照“RFU.CERT.ADF2”。									

6.3.3.2.2　0004 设备信息文件

设备信息文件的定义见表38。

表38　设备信息文件

文件标识符	‘0004’	SFI	‘04’	读控制	无	写控制	MKACSE	文件结构	透明
起始位置	数据项							类型	长度
‘0000’	设备标签							an	‘20’
‘0020’	序列号							b	‘20’
‘0040’	分组密码算法标识							b	‘4’
‘0044’	非对称密码算法标识							b	‘4’
‘0048’	密码杂凑算法标识							b	‘4’
‘004C’	设备认证使用的分组密码算法标识							b	‘4’
‘0050’	预留数据							b	‘40’
注：表中的如下数据项使用固定值： “分组密码算法标识”为0x00000413； “非对称密码算法标识”为0x00020500； “密码杂凑算法标识”为0x00000001； “设备认证使用的分组密码算法标识”为0x00000401。									

6.3.3.2.3　社会保障证书应用（DF01）

文件索引文件的定义见表39。

表39　　文件索引文件

文件标识符	‘0001’	SFI	‘01’	读控制	无	写控制	MKDF01	文件结构	定长记录
标志	数据项							类型	长度
‘02’	文件1信息							—	‘2E’
‘A1’	文件FID							b	‘02’
‘A2’	文件名称							an	‘10’
‘A3’	空间大小							b	‘02’
‘A4’	读权限							b	‘01’
‘A5’	写权限							b	‘01’
‘A6’	使用权限							b	‘01’
‘A7’	预留							b	‘09’

表 39（续）

注：表中的如下数据项使用固定值：

第1条记录内容为：

-“文件FID”为‘00 12’

-“文件名称”为‘C7 A9 C3 FB B9 AB D4 BF CE C4 BC FE 00 00 00 00’ （签名公钥文件）

-其他数据项使用‘00’补全。

第2条记录内容为：

-“文件FID”为‘00 13’

-“文件名称”为‘C7 A9 C3 FB CB BD D4 BF CE C4 BC FE 00 00 0000’ （签名私钥文件）

-其他数据项使用‘00’补全。

第3条记录内容为：

-“文件FID”为‘00 14’

-“文件名称”为‘BCD3C3DCB9ABD4BFCEC4BCFE00000000’ （加密公钥文件）

-其他数据项使用‘00’补全。

第4条记录内容为：

-“文件FID”为‘00 15’

-“文件名称”为‘BCD3C3DCCBBDD4BFCEC4BCFE00000000’ （加密私钥文件）

-其他数据项使用‘00’补全。

第5条记录内容为：

-“文件FID”为‘00 18’

-“文件名称”为‘C7A9C3FBD6A4CAE9CEC4BCFE00000000’ （签名证书文件）

-其他数据项使用‘00’补全。

第6条记录内容为：

-“文件FID”为‘00 19’

-“文件名称”为‘BCD3C3DCD6A4CAE9CEC4BCFE00000000’ （加密证书文件）

-其他数据项使用‘00’补全。

第7条记录内容为：

-“文件FID”为‘00 08’

-“文件名称”为‘C1D9CAB1B9ABD4BFCEC4BCFE00000000’ （临时公钥文件）

-其他数据项使用‘00’补全。

第8条记录内容为：

-“文件FID”为‘00 09’

-“文件名称”为‘C1D9CAB1CBBDD4BFCEC4BCFE00000000’ （临时私钥文件）

-其他数据项使用‘00’补全。

容器索引文件的定义见表40。

表40 容器索引文件

文件标识符	‘0002’	SFI	‘02’	读控制	无	写控制	MKDF01	文件结构	定长记录
标志	数据项							类型	长度
‘03’	容器信息							—	‘45’
‘A8’	容器名称							an	‘40’

表 40（续）

‘A9’	容器类型	b	‘01’
注：表中的如下数据项使用固定值： “容器名称”为“SS.CERT.CONTAINER”； “容器类型”为“0x02”，标识SM2算法。			

6.4 金融应用数据结构

金融应用应按照JR/T 0025的规定执行。根据各发卡机构的数据结构要求，支持借贷记、小额支付和小额支付扩展应用等金融支付功能。

6.5 一卡通应用数据结构

6.5.1 文件和数据规划

一卡通应用在JT/T 978的基础上，扩展了本地应用，见图13。

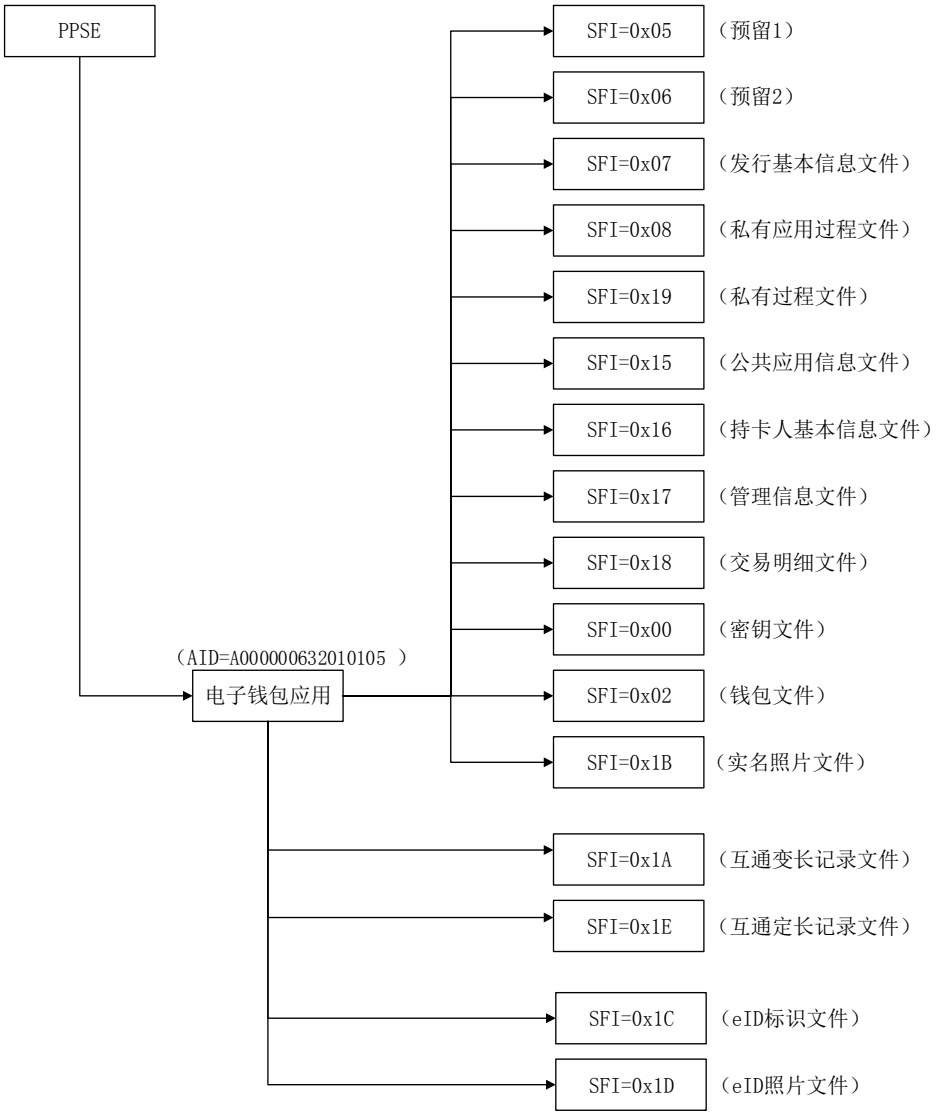


图13 一卡通应用结构

6.5.1.1 公共应用信息文件

公共应用信息文件的定义见表41。

表41 公共应用信息文件

文件标识（FID）		0x15
文件类型		二进制数据文件
文件大小（字节）		30
文件存取控制		读=自由
字节	数据元	长度（字节）
1～8	发卡机构标识	8
9	应用类型标识	1
10	应用启用标识	1
11～20	应用主账号	10
21～24	应用启用日期（YYYYMMDD）	4
25～28	应用有效日期（YYYYMMDD）	4
29～30	发卡机构自定义 FCI 数据	2

6.5.1.2 持卡人基本信息文件

持卡人基本信息文件的定义见表42。

表42 持卡人基本信息文件

文件标识（FID）		0x16
文件类型		二进制数据文件
文件大小（字节）		55
文件存取控制		读=自由
字节	数据元	长度（字节）
1	卡类型标识	1
2	本行职工标识	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

6.5.1.3 管理信息文件

管理信息文件的定义见表43。

表43　管理信息文件

文件标识（FID）		0x17
文件类型		二进制数据文件
文件大小（字节）		60
文件存取控制		读=自由
字节	数据元	长度（字节）
1～4	国际代码	4
5～6	省级代码	2
7～8	城市代码	2
9～10	互通卡种	2
11	卡种类型	1
12～15	认证机构编码	4
16～35	认证证书编号	20
36～60	预留	25

6.5.1.4　相片文件

相片文件的定义见表44。

表44　相片文件

文件标识（FID）		0x1B
文件类型		二进制数据文件
文件大小（字节）		6144
文件存取控制		读=自由，保护写
字节	数据元	长度（字节）
1～2	相片长度	2
3～（3+N）	JPG 相片二进制数	N
其余	预留	6144-2-N

6.5.1.5　交易明细文件

交易明细文件的定义见表45。

表45　交易明细文件

文件标识（FID）	0x18
文件类型	循环文件
文件大小（字节）	10×23
文件存取控制	读=自由

表 45（续）

字节	数据元	长度（字节）
1～2	EP 联机或脱机交易序号	2
3～5	透支限额	3
6～9	交易金额	4
10	交易类型标识	1
11～16	终端机编号	6
17～20	交易日期（终端）	4
21～23	交易时间（终端）	4

6.5.1.6 金额数据

卡内以安全方式存储，由卡片操作系统和应用自动进行维护，电子现金应用和电子钱包应用共用的一个余额数值。

6.5.1.7 公共交通过程信息变长记录文件

公共交通过程信息变长记录文件是变长记录结构，用于保存相应的换乘记录等信息。每条记录应有一定的预留字节，若发卡机构需要使用预留字节，则应按如下格式组织预留字节的内容：城市代码（2字节）、预留信息长度（1字节）和预留信息内容（N字节），公共交通过程信息变长记录文件见表46。

表46 公共交通过程信息变长记录文件

文件名称	公共交通过程信息变长记录文件——交易应用数据文件		
文件标识	SFI=0x1A	文件类型	变长记录文件
文件大小（字节）	2190		
文件权限	读取	自由	
	更新	保护	
记录号	记录描述		长度（字节）
1	城市轨道应用信息记录		128
2	公共汽电车应用信息记录		128
3	城市水上客运应用信息记录		128
4	出租汽车应用信息记录		128
5	租赁汽车应用信息记录		128
6	公共自行车应用信息记录		128
7	公共停车应用信息记录		112
8	长途客运应用信息记录		128
9	轮渡应用信息记录		128
10	城际铁路应用信息记录		128

表 46（续）

11	民航应用信息记录	128
12	高速公路应用信息记录	128
13	优惠信息记录	30
14	市郊铁路应用信息记录	128
15	公共充电桩应用信息记录	128
16	规范预留记录	128
17	规范预留记录	128
18	规范预留记录	128

6.5.1.8 公共交通过程信息循环记录文件

公共交通过程信息循环记录文件为循环记录结构，文件结构见表47。

具备换乘优惠的应用应将本次交易明细记录在公共交通过程信息循环记录文件中。在换乘优惠时，可读取循环记录文件中的内容作为换乘优惠的依据。

本部分也可用于行业的其他自定义应用。

表47 公共交通过程信息循环记录文件

文件名称	公共交通过程信息循环记录文件——交易信息记录文件		
文件类型	循环记录文件	文件标识	SFI=0x1E
文件大小（字节）	48*30		
文件权限	读取	自由	
	更新	保护	
字节	数据元	长度（字节）	数据格式
1	交易类型	1	BCD
2～9	终端编号	8	BCD
10	行业代码	1	HEX
11～12	线路	2	HEX
13～14	站点	2	HEX
15～16	运营代码	2	HEX
17	预留	1	HEX
18～21	交易金额	4	HEX(高字节在前)
22～25	交易后余额	4	HEX(高字节在前)
26～32	交易日期时间	7	YYYYMMDDhhmmss
33～34	受理方城市代码	2	BCD
35～42	受理方机构标识	8	BCD
43～48	本规范预留	6	初始为 00

6.5.1.9 发行基本信息文件

发行基本信息文件是变长记录结构，用于存储各本地应用的发行信息，文件结构见表48。

表48 发行基本信息文件

文件名称	发行基本信息文件		
文件标识	SFI=0x07	文件类型	变长记录文件
文件大小（字节）	1500		
文件权限	读取	自由	
	更新	保护	
记录号	记录描述		长度（字节）
1	应用卡类型标识区		20
2	预留		20
3	预留		20
4	预留（公园年票应用）		50
……	预留		……
34	预留		100

6.5.1.10 私有应用过程文件

私有应用过程文件是变长记录结构，用于存储各本地应用的使用过程信息，文件结构见表49。

表49 私有应用过程文件

文件名称	私有应用过程文件		
文件标识	SFI=0x08	文件类型	变长记录文件
文件大小（字节）	2250		
文件权限	读取	自由	
	更新	保护	
记录号	记录描述		长度（字节）
1	预留		50
2	预留（公园年票应用）		50
3	预留		50
4	预留		50
5	预留		50
……	预留		……
40	预留		100

6.5.1.11 预留文件 1

预留文件的初始值为全00，文件结构见表50。

表50　预留文件 1

文件标识（FID）		0x05
文件类型		二进制数据文件
文件大小（字节）		2048
文件存取控制		读=自由，保护写
字节	数据元	长度（字节）
1～2048	预留	2048

6.5.1.12　预留文件 2

预留文件的初始值为全00，文件结构见表51。

表51　预留文件 2

文件标识（FID）		0x06
文件类型		二进制数据文件
文件大小（字节）		2048
文件存取控制		读=自由，保护写
字节	数据元	长度（字节）
1～2048	预留	2048

6.5.1.13　私有过程文件

私有过程文件的初始值按下表进行初始化，每条记录的数据域默认为全00，文件结构见表52。

表52　私有过程文件

文件名称	私有过程文件		
文件标识	SFI=0x19	文件类型	变长记录文件
文件大小（字节）	500		
文件权限	读取	自由	
	更新	保护	
记录号	记录描述		长度（字节）
1	预留		50
2	预留		50
3	预留		50
4	预留		50
5	预留		50
……	预留		……
10	预留		50

6.5.1.14 eID 标识文件

eID标识文件的初始值为全00，文件结构见表53。

表53 eID 标识文件

文件标识（FID）		0x1C
文件类型		二进制数据文件
文件大小（字节）		250
文件存取控制		读=自由，保护写
字节	数据元	长度（字节）
1～2	标识文件的数据长度	2
3～250	标识文件的二进制数	n

6.5.1.15 eID 相片文件

eID相片文件的初始值为全00，文件结构见表54。

表54 eID 相片文件

文件标识（FID）		0x1D
文件类型		二进制数据文件
文件大小（字节）		2048
文件存取控制		读=自由，保护写
字节	数据元	长度（字节）
1～2	相片文件的数据长度	2
3～2048	相片文件的二进制数	n

6.5.1.16 交通 PPSE 应用

交通应用的PPSE与金融应用的PPSE，AID相同，格式也相同。当交通应用与金融应用共同存在于同一张卡中时，由厂商在制卡时将交通和金融的应用入口同时初始化到PPSE中。

6.5.2 密钥管理

——应用主控：在卡片预处理阶段完成对其他密钥的装载和修改，在交易阶段完成对卡片的外部认证；
——应用维护 1：用于修改 0015、0016、0017、001B、0007 等文件；
——应用维护 2：用于修改 0008、0019 文件；
——消费子密钥 1：电子钱包消费时使用；
——消费子密钥 2：电子钱包消费时使用；
——充值子密钥：电子钱包充值交易时使用；
——TAC 子密钥：电子钱包交易时验证交易合法性；
——应用锁定：用于对黑名单卡进行应用锁定；

——应用解锁：用于对临时锁定的应用进行应用解锁；
——修改透支限额：用于修改电子钱包的可透支限额；
——互通记录保护密钥：用于修改 001A、001E 文件；
——内部认证密钥：用于对终端的合法性验证。

6.6 北京通应用数据结构

6.6.1 文件和数据规划

6.6.1.1 北京通管理环境标识

北京通应用区管理环境的应用标识符，如表55所示。

表55 北京通应用区管理环境的应用标识符

管理环境	管理环境应用标识符
北京通	B1B1BEA9CDA8D3A6D3C3C7F8

6.6.1.2 北京通管理环境下应用划分

北京通应用包含基本数据应用、北京通应用2部分，见表56。
北京通应用使用SM4算法进行保护。在北京通管理环境下的应用，统一使用北京通密钥体系。

表56 北京通应用环境划分

环境	应用名称	应用标识符	空间	说明
北京通应用 53532EB1B1BEA9CDA8 （15K）	基本数据	D15600001601	10K	沿用北京通规范对基本数据的要求，相片调整为 8K
	北京通应用	D15600001600	5K	用于北京通支持行业的信息验证

6.6.1.3 北京通基本信息区

6.6.1.4 北京通基本信息应用结构规划

北京通基本信息应用结构规划，见图14。

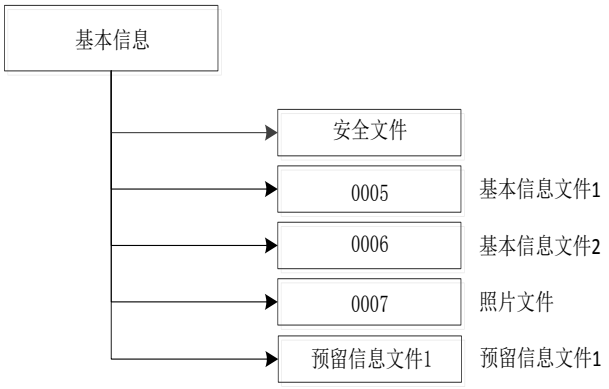


图14　基本信息应用结构

6.6.1.5　基本信息应用文件结构

基本信息应用是指由北京通维护的使用人相关信息，包括基本信息文件1（‘0005’）、基本信息文件2（‘0006’）、相片文件（‘0007’）以及预留信息文件1（‘0008’）它们被组织成基本文件存在于DF下，见表57。

表57　基本信息应用文件结构

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别
基本信息文件 1	‘0005’	‘05’	自由	UK1	变长记录	预设
基本信息文件 2	‘0006’	‘06’	RK1	UK1	变长记录	预设
相片文件	‘0007’	‘07’	RK1	UK1	二进制	预设
预留信息文件 1	‘0008’	‘08’	自由	UK1	变长记录	预设

6.6.1.6　基本信息文件 1(0005)

基本信息文件1结构见表58。

表58　基本信息文件 1

文件标识符	0005	SFI	05	读控制	无	写控制	UK1	文件结构	变长记录
标志	数据项							类型	长度
‘01’	姓名							an	‘32’
‘02’	性别							an	‘01’
‘03’	北京通号							an	‘0C’
‘04’	北京通卡的类别							cn	‘01’
‘05’	权益属性							an	‘20’
‘06’	发卡机构							an	‘20’
‘07’	制卡时间							cn	‘04’

a)　姓名：持卡人的姓名应使用全国通用文字，本规范规定卡内存储的姓名用汉字表达；

b) 性别：性别分为未知的性别、男性、女性和未说明的性别等四类。持卡人性别用一个字符的阿拉伯数字代码表示，其表示方法应符合 GB/T 2261.1 中的规定；
c) 北京通号：应符合北京通应用规范中的规定；
d) 北京通卡的类别：包括北京通社保卡‘01’、北京通基本卡‘02’、北京通临时卡‘03’；
e) 权益属性：证件名称是指此类卡片持有人的权益属性内容。可同时存储多个类型；
f) 发卡机构：发卡机构是指卡片的主发行机构名称；
g) 制卡时间：卡生成的年和月，按照年/月的格式。

6.6.1.7 基本信息文件 2(0006)

基本信息文件2结构见表59。

表59 基本信息文件 2

文件标识符	‘0006’	SFI	‘06’	读控制	RK1	写控制	UK1	文件结构	变长记录
标志	数据项							类型	长度
‘0A’	民族							cn	‘01’
‘0B’	出生日期							cn	‘04’
‘0C’	公民证件类别							cn	‘04’
‘0D’	证件号码							an	‘12’
‘0E’	固定电话/移动电话							an	‘0F’
‘0F’	居住地							an	‘50’
‘10’	户籍地址							an	‘50’

a) 民族：采用国家认定的民族名称来记录持卡人的民族信息。本规范规定民族名称用二个字符的阿拉伯数字代码表示，其表示方法应符合 GB/T 3304 的规定；
b) 出生日期：出生日期采用公历日期，其表示方法应符合 GB/T 7408 的规定；
c) 公民证件类别：身份证、护照、港澳台证等；
d) 证件号码：公民证件类别所对应的证件号码；
e) 固定电话/移动电话：能与持卡人保持联系的电话号码；
f) 居住地：持卡人现居住地址。居住地址可以是常住户口地址，也可以是常住户口以外的地址，表示方法应符合 GB/T 2260 的规定；
g) 户籍地址：常住户口所在地地址是指户口所在地的详细地址。常住户口所在地由中华人民共和国行政区划名称、街道（乡、镇）和街、路、巷、村等名称以及门牌号码及居室号码构成。行政区划名称应符合 GB/T 2260 的规定；

6.6.1.8 相片文件(0007)

相片文件结构见表60。

表60 相片文件

文件标识符	‘0007’	SFI	‘07’	读控制	RK1	写控制	UK1	文件结构	透明
标志	数据项							类型	长度
—	相片数据							B	‘2000’

6.6.1.9 预留文件(0008)

预留文件用于后续扩展持卡人就业情况，结构见表61。

表61 预留文件

文件标识符	‘0008’	SFI	‘08’	读控制	无	写控制	UK1	文件结构	变长记录
标志	数据项							类型	长度
—	预留							an/cn	‘200’

6.6.1.10 北京通应用

6.6.1.10.1 北京通应用结构规划

北京通应用区结构规划，见图15。

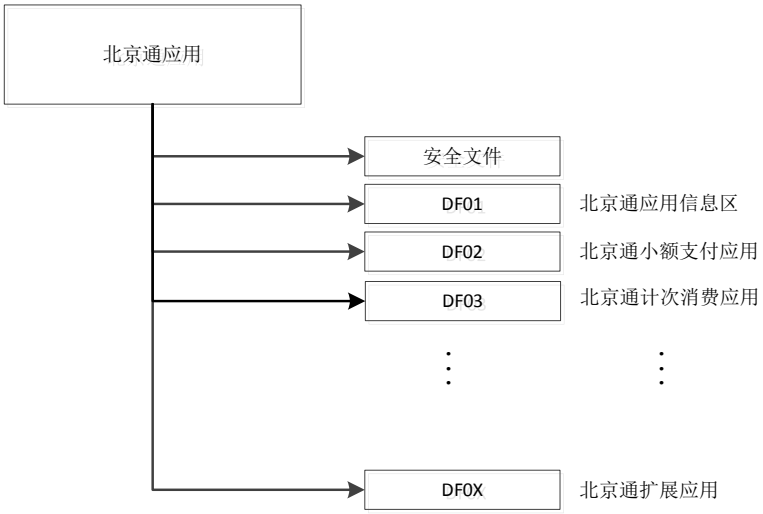


图15 北京通应用结构

6.6.1.10.2 北京通应用文件结构

北京通应用包含多个北京通相关行业应用数据信息文件并在此基础上预留7个扩展文件，结构见表62。

表62 北京通应用文件结构

应用	应用标识符
应用信息应用	D15600001611
小额消费应用	D15600001612
计次应用	D15600001613
扩展自主应用 1	D15600001614

6.6.1.10.3 北京通应用信息区文件规划

北京通应用信息区文件规划见表63。

表63　北京通应用信息区文件规划

文件定义	文件标识符	短文件标识符	读控制	写控制	文件结构	类别
北京通数据文件 1	‘0005’	‘05’	RK1DF01	UK1DF01	二进制	预设
北京通数据文件 2	‘0006’	‘06’	RK1DF01	UK1DF01	二进制	预设
北京通数据文件 3	‘0007’	‘07’	RK1DF01	UK1DF01	二进制	预设
北京通数据文件 4	‘0008’	‘08’	RK1DF01	UK1DF01	二进制	预设
预留扩展文件 1	‘0009’	‘09’	RK2DF01	UK2DF01	二进制	预设
预留扩展文件 2	‘000A’	‘0A’	RK2DF01	UK2DF01	二进制	预设
预留扩展文件 3	‘000B’	‘0B’	RK2DF01	UK2DF01	二进制	预设
预留扩展文件 4	‘000C’	‘0C’	RK3DF01	UK3DF01	二进制	预设
预留扩展文件 5	‘000D’	‘0D’	RK3DF01	UK3DF01	二进制	预设
预留扩展文件 6	‘000E’	‘0E’	RK4DF01	UK4DF01	二进制	预设
预留扩展文件 7	‘000F’	‘0F’	RK4DF01	UK4DF01	二进制	预设

北京通数据文件格式见表64。

表64　北京通数据文件格式

文件标识（SFI）		0005、0006、0007、0008	
文件类型		二进制	
文件大小		1CH	
文件存取控制	读=RK1DF01	改写=UK1DF01	
字节	数据项	长度	默认值
0～0	应用大类	‘01’	—
1～1	应用行业特征码	‘01’	—
2～7	发行序列号	‘06’	—
8～11	应用启用日期	‘04’	YYYYMMDD
12～15	应用有效日期	‘04’	YYYYMMDD
16～27	行业动态数据	‘0C’	—

预留扩展文件1格式见表65。

表65　预留扩展文件格式 1

文件标识（SFI）		0009、000A、000B	
文件类型		二进制	
文件大小		38H	
文件存取控制	读=RK2DF01	改写=UK2DF01	
字节	数据项	长度	默认值

表 65（续）

0～56	预留数据项	‘38’	—

预留扩展文件2格式见表66。

表66　预留扩展文件格式 2

文件标识（SFI）		000C、000D	
文件类型		二进制	
文件大小		8CH	
文件存取控制	读=RK3DF01	改写=UK3DF01	
字节	数据项	长度	默认值
0～140	预留数据项	‘8C’	—

预留扩展文件3格式见表67。

表67　预留扩展文件格式 3

文件标识（SFI）		000E、000F	
文件类型		二进制	
文件大小		F0H	
文件存取控制	读=RK4DF01	改写=UK4DF01	
字节	数据项	长度	默认值
0～240	预留数据项	‘F0’	—

6.6.1.10.4　小额支付应用文件规划

小额消费基本信息文件格式见表68。

表68　小额费基本信息文件(0005)

文件标识（SFI）		0005	
文件类型		定长记录文件	
文件大小		26C	
文件存取控制	读=自由	改写=UK1DF02	
记录号	数据项	长度	默认值
1	第 1 记录内容	1F	—
2	第 2 记录内容	1F	—
3	第 3 记录内容	1F	—
4	第 4 记录内容	1F	—
5	第 5 记录内容	1F	—
……		1F	……
20	第 20 记录内容	1F	—

钱包专用文件格式见表69。

表69　钱包专用文件(0002)

文件标识（SFI）	0002	
文件类型	钱包专用	COS 管理

交易明细文件格式见表70。

表70　交易明细(0018)

文件标识（SFI）		0018	
文件类型		循环记录	
文件大小		E6	
文件存取控制	读=PIN	COS 改写	
字节	数据项类型	长度	—
1～2	ED/EP 联机或脱机交易序号	2	—
3～5	透支限额	3	—
6～9	交易金额	4	—
10	交易类型	1	消费、充值
11～16	终端机编号	6	—
17～20	交易日期	4	YYYYMMDD
21～23	交易时间	3	MMNNSS

6.6.1.10.5　计次服务应用结构规划

计次服务应用基本信息文件格式见表71。

表71　计次服务应用基本信息文件(0005)

文件标识（SFI）		0005	
文件类型		二进制	
文件大小		41H	
文件存取控制	读=自由	改写=UK1DF03	
字节	数据项	长度	默认值
0	应用启用标志	1	00：未启用 01：启用
1～4	启用日期	4	YYYYMMDD
5～9	有效日期	4	YYYYMMDD
10～11	计次基数	2	—
12～12	卡类型	1	—
13～41	应用信息	35	—

计次服务专用钱包文件格式见表72。

表72　计次服务专用钱包文件(0002)

文件标识（SFI）	0002	
文件类型	钱包专用	COS 管理

交易明细文件格式见表73。

表73　交易明细(0018)

文件标识（SFI）		0018	
文件类型		循环记录	
文件大小		E6	
文件存取控制	读=PIN	COS 改写	
字节	数据项	长度	—
1～2	ED/EP 联机或脱机交易序号	2	—
3～5	透支限额	3	—
6～9	交易金额	4	—
10	交易类型	1	消费、充值
11～16	终端机编号	6	—
17～20	交易日期	4	YYYYMMDD
21～23	交易时间	3	MMNNSS

6.6.1.10.6　扩展自主应用 1

扩展预留会员文件格式见表74。

表74　扩展预留会员应用(0019)

文件标识（SFI）			0019	
文件类型			定长记录文件	
文件大小			20*0CH=F0H	
文件存取控制	读=自由		改写= UK1DF04	
记录号	数据项		长度	默认值
1	第 1 记录内容，记录内字段	会员行业编码-会员类型-有效月数 行业编码(最多 32 个行业)会员类型(<16 种) 有效月数(<128 个月)	2	—
		会员号码	3	—
		启用年月(YYYYMMDD)	3	—
		发行 MAC	4	—

表 74（续）

2	第 2 记录内容	—	0C	—
3	第 3 记录内容	—	0C	—
4	第 4 记录内容	—	0C	—
5	第 5 记录内容	—	0C	—
……	……	—	……	—
20	第 20 记录内容	—	0C	—

6.6.1.11 密钥管理

北京通密钥分类表，见表75。

表75 北京通密钥分类表

密钥	备注
MK	应用主控密钥 1、北京通管理环境 2、基本信息区、北京通应用区
DAMK	应用维护密钥
UK	应用数据更新密钥，发卡方或应用提供方控制应用数据更新操作的密钥（密钥条数以实际应用要求为准）
RK	应用数据读取密钥，发卡方或应用提供方控制部分应用数据读取操作的密钥（密钥条数以实际应用要求为准）
IRK	鉴别发卡方的密钥（密钥条数以实际应用要求为准）
DLK	圈存密钥（密钥条数以实际应用要求为准）
DPK	消费密钥（密钥条数以实际应用要求为准）
DTK	TAC 密钥（密钥条数以实际应用要求为准）
DULK	应用解锁密钥（密钥条数以实际应用要求为准）
DUK	应用锁定密钥（密钥条数以实际应用要求为准）
DRPK	PIN 重装密钥（密钥条数以实际应用要求为准）
DPUK	PIN 解锁密钥（密钥条数以实际应用要求为准）
PIN	值：123456　次数：3 次

6.6.1.12 北京通应用密钥分散流程

北京通应用密钥分散应遵循如下流程。

a) 通过密码机产生随机种子密钥并存在种子卡（CPU 卡）中，随后自定义卡片 PIN 码。初始密钥卡由四张种子卡组成；

b) 通过硬件加密机的相应加密算法，生成出北京通根密钥；

c) 根据应用代码分散出各类一级应用密钥（包括应用鉴别密钥、应用数据更新密钥、应用数据读取密钥等等）。密钥分散完成后保存在加密机中，任何人都无法以明文的形式得到密钥内容，并同时导入密钥母卡中备份保存；
d) 通过配置文件中的北京市分散因子，生成出北京市二级区域密钥，并同时导入密钥母卡中备份保存；
e) 通过硬件加密机的密钥导出功能，把各类一级应用密钥导入到 SAM 卡中，以备终端使用；
f) 在个人化发卡中心，生产制卡过程中，使用卡级分散因子与二级区域密钥进行分散，分散出每张卡片的卡级应用密钥。

6.7 残疾人应用数据结构

6.7.1 残疾人应用文件和数据规划

残疾人应用结构，见图16。

图16　残疾人应用结构

残疾人应用的文件为树形结构。树的每一个分支是一个应用数据文件(ADF)或一个目录定义文件(DDF)。一个ADF是一个或者多个应用基本文件(AEF)的入口点。一个ADF及其相关的数据文件处于树的同一分支上。一个DDF是其他ADF或者DDF的入口点。DDF入口见表76。

表76 DDF 入口

目录	应用区名称	FID	AID
DDF1	残疾人证应用环境	DDF1	D156000137

残疾人应用结构见表77至表93的相关描述。

表77 发卡机构基本数据文件

文件标识（FID）			‘EF05’
文件类型			变长记录
文件存取控制		读=自由	改写不允许
标签	数据元	类型	长度
01	卡的类别	ans	01
02	规范版本	ans	04
03	发卡机构名称	ans	90
04	发卡机构代码	cn	11
05	发卡机构证书	b	158
06	发卡时间	cn	04
07	卡有效期	cn	04
08	卡号	ans	18
09	安全码	b	03
10	芯片序列号(UID)	b	10
11	应用城市代码	cn	03
12	卡片当前状态	cn	01
注：芯片序列号（UID）最长为10字节，残疾人证使用7字节。			

表78 持卡人基本数据文件

文件标识（FID）	‘EF06’

表 78（续）

文件类型			变长记录
文件存取控制		读=RK2DDF01	改写=AMK2DDF01&PIN
标签	数据元	类型	长度
13	姓名	ans	100
14	性别	b	01
15	民族代码	cn	01
16	出生日期	cn	04
17	公民身份号码	ans	18
18	户籍地编码	cn	06
19	户籍地地址	ans	240
20	所属街道名称	ans	240
21	固定电话	ans	20
22	移动电话	ans	20
23	残疾证号	ans	25
24	残疾证签发日期	cn	04

表79　持卡人扩展数据文件

文件标识（FID）			‘EF07’
文件类型			变长记录
文件存取控制		读=RK3DDF01	改写=AMK3DDF01&PIN
标签	数据元	类型	长度
25	文化程度代码	cn	01
26	婚姻状况代码	cn	01
27	政治面貌代码	cn	01
28	户口性质代码	cn	01

表80　联系人信息数据文件

文件标识（FID）			‘EF08’
文件类型			变长记录
文件存取控制		读=RK4DDF01	改写=AMK4DDF01&PIN
标签	数据元	类型	长度
29	联系人姓名	ans	100
30	联系人关系	cn	01
31	联系人电话	ans	100
32	居住地编码	cn	06
33	居住地地址	ans	240

表81　残疾信息数据文件

文件标识（FID）			‘EF09’
文件类型			变长记录
文件存取控制		读=RK5DDF01	改写=AMK5DDF01&PIN
标签	数据元	类型	长度
34	残疾人类别	cn	01
35	残疾人等级	cn	01
36	视力残疾等级	cn	01
37	听力残疾等级	cn	01
38	言语残疾等级	cn	01
39	肢体残疾等级	cn	01
40	智力残疾等级	cn	01
41	精神残疾等级	cn	01

表82　相片数据文件

文件标识（FID）			‘EF0A’
文件类型			二进制文件
文件存取控制		读=RK6DDF01	改写=AMK6DDF01&PIN
标签	数据元	类型	长度
42	相片	b	3074
注：相片文件存放方式为两字节相片数据长度+相片数据,例如相片数据为2066(0x0812)字节，则文件第一个字节为0x08，第二个字节为 0x12，从第三个字节开始为相片数据。			

表83　金融账户信息文件

文件标识（FID）			‘EF0B’
文件类型			变长记录文件
文件存取控制		读=RK7DDF01	改写=AMK7DDF01
标签	数据元	类型	长度
43	账号	cn	20
44	开户行标识	ans	100
45	开户时间	cn	4
46	开户人姓名	ans	100

表84　联机交易记录文件

文件标识（FID）			‘EF0C’
文件类型			循环记录（10 条）
文件存取控制		读=RK8DDF01	不可写，内部维护
标签	数据元	类型	长度
47	联机交易记录	cn	36

表85　联机交易记录格式

字段名	长度	数据来源
福利券信息	4	残联业务平台
联机交易认证码	4	
终端机编号	6	残联商户专用终端
终端交易序号	4	
终端交易日期	4	
终端交易时间	3	
密钥版本号	1	—
应用交易计数器	2	IC 卡
联机应用密文	8	IC 卡

表86　脱机认证信息文件

文件标识（FID）			‘EF0D’
文件类型			变长记录
文件存取控制		读=自由	改写=AMK9DDF01
标签	数据元	类型	长度
48	脱机认证算法类型	cn	01
49	CA 公钥索引	cn	01
注：脱机认证算法支持SM2算法，固定值为“04”。			

表87　发卡机构公钥证书文件

文件标识（FID）			‘EF0E’
文件类型			变长记录
文件存取控制		读=自由	改写不允许
标签	数据元	类型	长度
50	发卡机构公钥证书	cn	158

表88　IC卡公钥证书文件

文件标识（FID）			‘EF0F’
文件类型			变长记录
文件存取控制		读=自由	改写不允许
标签	数据元	类型	长度
51	IC卡公钥证书	cn	177

表89　IC卡私钥文件

文件标识（FID）			‘EF10’
文件类型			变长记录
文件存取控制		不可读	不可写
标签	数据元	类型	长度
52	IC卡私钥	cn	32

表90　数据签名文件

文件标识（FID）			‘EF11’
文件类型			变长记录
文件存取控制		读=自由	改写=AMK12DDF01
标签	数据元	类型	长度
53	姓名	ans	100
54	残疾人证号	ans	25
55	户籍地编码	cn	06
56	所属街道名称	ans	240
57	发卡机构基本数据文件HASH值	b	32
58	发卡机构基本数据签名	b	64

表 90（续）

59	IC 卡签名	b	64
注：发卡机构基本数据签名指的是用业务数据签名应用的私钥对标签57做签名。IC卡签名是将53||54||55||56||57||58进行SM3哈希运算，然后使用IC卡私钥进行签名得到签名结果。53-58其中的任一记录被更新，IC卡签名应同步更新。			

表91　中国残联业务预留文件

文件标识（FID）			‘EF12’
文件类型			变长记录
文件存取控制		读=RK13DDF01	改写=AMK13DDF01
标签	数据元	类型	长度
-	预留信息	N/A	1024

表92　地方业务预留文件 1

文件标识（FID）			‘EF13’
文件类型			变长记录
文件存取控制		读=RK14DDF01	改写=AMK14DDF01
标签	数据元	类型	长度
-	预留信息	N/A	1024

表93　地方业务预留文件 2

文件标识（FID）			‘EF14’
文件类型			变长记录
文件存取控制		读=RK15DDF01	改写=AMK15DDF01
标签	数据元	类型	长度
-	预留信息	N/A	1024

6.7.2 密钥管理

6.7.2.1 密钥种类

残疾人应用密钥类型，见表94。

表94 残疾人应用密钥类型表

密钥名称	用途	密钥形式	存在条件
卡片主控密钥	用于控制主文件的创建其他业务密钥的安装和更新	对称密钥	存在
应用主控密钥	用于控制当前应用下文件的创建其他业务密钥的安装和更新	对称密钥	存在
应用维护密钥	用于报文鉴别码（MAC）的产生和验证、数据加解密	对称密钥	存在
外部认证密钥	用于外部认证过程中验证外部认证数据	对称密钥	存在
联机交易密钥	用于联机交易时计算应用密文，应用密文用于后台对账	对称密钥	存在
口令密钥	用于验证个人识别码（PIN）	对称密钥	存在
口令重装密钥	用于个人识别码（PIN）的重装	对称密钥	存在
卡片公私密钥对	用于卡片关键数据签名及脱机数据认证	非对称密钥	存在

6.7.2.2 密钥属性说明

密钥属性表见表95。

表95 密钥属性表

密钥属性	索引	版本号	错误计数
卡片主控密钥（MKDDF01）	00	01	F
应用解锁锁定密钥（AMK8DDF01）	08	01	5
应用维护密钥 2（AMK2DDF01）	02	01	5
应用维护密钥 3（AMK3DDF01）	03	01	5
应用维护密钥 4（AMK4DDF01）	04	01	5
应用维护密钥 5（AMK5DDF01）	05	01	5
应用维护密钥 6（AMK6DDF01）	06	01	5
应用维护密钥 7（AMK7DDF01）	07	01	5
应用维护密钥 9（AMK9DDF01）	09	01	5
应用维护密钥 12（AMK12DDF01）	0C	01	5
应用维护密钥 13（AMK13DDF01）	0D	01	5
应用维护密钥 14（AMK14DDF01）	0E	01	5
应用维护密钥 15（AMK15DDF01）	0F	01	5
联机交易密钥 （OTK）	01	01	N/A
外部认证密钥 2（RK2DDF01）	02	01	6

表 95（续）

外部认证密钥 3（RK3DDF01）	03	01	6
外部认证密钥 4（RK4DDF01）	04	01	6
外部认证密钥 5（RK5DDF01）	05	01	6
外部认证密钥 6（RK6DDF01）	06	01	6
外部认证密钥 7（RK7DDF01）	07	01	6
外部认证密钥 8（RK8DDF01）	08	01	6
外部认证密钥 13（RK13DDF01）	0D	01	6
外部认证密钥 14（RK14DDF01）	0E	01	6
外部认证密钥 15（RK15DDF01）	0F	01	6
口令密钥(PIN)	00	00	6
口令重装密钥	01	01	5

6.8 民政应用数据结构

6.8.1 文件和数据规划

民政应用是指由民政维护的使用人相关信息，包括卡片基本信息文件1（‘0015’）、持卡人基本信息文件2（‘0016’）以及预留信息文件1（‘0008’），见表96、表97及表98。

表96 卡片基本信息文件

文件标识	0015			
文件类型	二进制	文件大小		00FFH
文件存取控制	读：自由	改写：密文+MAC，维护密钥 1		
创建指令	—			
字节	数据元	数据类型	长度	值
1	卡片类型	H	1	01-纯行业卡
2～9	合作机构代码	ans	8	用于唯一标识合作机构，一般由合作机构的缩写 asc 码构成，超过 8 字节取前面 8 字节，不够 8 个字符的补充 00。举例：ICBC0000 不够的后面补 00 ，卡片存储为“4943424330303030”
10～19	卡片编号	n	10	用于唯一标识发行的卡片，为 10 个数字编码，不够 10 位数字，左端补 0.举例：0001234567
20～23	卡片启用日期	n	4	格式：YYYYMMDD，制空白卡时值为 00000000
24～27	卡片失效日期	n	4	格式：YYYYMMDD，制空白卡时值为 00000000
28～31	批次编号	n	4	—

表 96（续）

32～81	发卡机构	H	50	制空白卡时值为空格
82～255	预留	H	174	—

表97　持卡人基本信息文件（0016）

文件标识		0016		
文件类型		二进制	文件大小	0400H
文件存取控制		读：认证读	改写：密文+MAC，维护密钥 3	
创建指令		—		
字节	数据元	数据类型	长度	值
1～40	民政号码	ans	40	多余字节在末尾填充空格
41	持卡人证件类型	H	1	编码规则待定，用户办理记名卡证件类型 例如： 0x01－身份证 0x02－军官证 0x03－护照 0x04～0x07（后续添加扩展）
42～81	持卡人证件号码	ans	40	例如："62272219880308123X"在卡中写入的编码格式为： “36323237323231393838303330383132335820202020202020202020202020202020202020202020”多余字节在末尾填充空白 0x20
82～131	持卡人姓名	ans	50	多余字节在末尾填充空格
132～181	持卡人姓名扩展	ans	50	多余字节在末尾填充空格
182～196	持卡人联系电话	ans	15	例如：“13925201876”在卡中写入的编码格式为：“31333932353230313837362020202020”多余数据在末尾填充空白 0x20
197	持卡人性别	H	1	例如： 0x01－男 0x02－女
198	持卡人民族	H	1	GB/T3304
199～204	持卡人出生地	H	6	多余字节在末尾填充空格
205～208	持卡人出生年月日	n	4	YYYYMMDD
209～210	持卡人户口性质	H	2	多余字节在末尾填充空格

表 97（续）

211～290	持卡人户口所在地址	ans	80	多余字节在末尾填充空格
291～370	持卡人住址	ans	80	多余字节在末尾填充空格
371～385	备用联系电话	ans	15	多余字节在末尾填充空格
386	监护人证件类型	H	1	编码规则待定，用户办理记名卡证件类型例如： 0x01－身份证 0x02－军官证 0x03－护照 0x04～0x07（后续添加扩展）
387～426	监护人证件号码	Ans	40	多余字节在末尾填充空格
427～476	监护人姓名	Ans	50	多余字节在末尾填充空格
476～526	监护人姓名扩展	Ans	50	多余字节在末尾填充空格
527～541	监护人联系电话	Ans	15	多余字节在末尾填充空格
541～1024	保留	H	483	—

表98　预留文件（0008）

文件标识	0008			
文件类型	二进制		文件大小	2000H
文件存取控制	读取：自由		改写：明文+MAC，维护密钥 2	
创建指令	—			
字节	数据元	数据类型	长度	值
1～8192	保留	H	8192	扩展备用

6.8.2　民政密钥管理

民政应用密钥相关信息，见表99、表100及表101。

表99　民政应用密钥列表

数据元	数据类型	长度	值
环境主控密钥	b	16	在卡片预处理阶段完成对安全通道的开启以及应用的安装（TK 加密）
应用主控密钥	b	16	在卡片预处理阶段完成对其他密钥的装载和修改，在交易阶段完成对卡片的外部认证（TK 加密）
卡片维护密钥 1	b	16	用于修改 0015 文件（TK 加密）
卡片维护密钥 2	b	16	用于修改 0008 文件（TK 加密）
卡片维护密钥 3	b	16	用于修改 0016 文件（TK 加密）

表100　民政密钥校验值

数据元	数据类型	长度	值
环境主控密钥校验值	B	3	—
应用主控密钥校验值	b	3	—
卡片维护密钥 1 校验值	b	3	—
卡片维护密钥 2 校验值	b	3	—
卡片维护密钥 3 校验值	b	3	—

表101　卡片密钥索引

数据元	数据类型	长度	值	索引	版本号	错误计数
环境主控密钥	b	16	在卡片预处理阶段完成对安全通道的开启以及应用的安装（TK 加密）	—	01	—
应用主控密钥	b	16	在卡片预处理阶段完成对其他密钥的装载和修改，在交易阶段完成对卡片的外部认证（TK 加密）	00	01	8
卡片维护密钥 1	b	16	用于修改 0015 文件（TK 加密）	01	01	8
卡片维护密钥 2	b	16	用于修改 0008 文件（TK 加密）	02	01	8
卡片维护密钥 3	b	16	用于修改 0016 文件（TK 加密）	03	01	8
注：环境主控密钥的算法为DES，GP认证分散因子为keydata后6个字节。						

6.9　数字人民币应用数据结构

遵照中国人民银行数字货币研究所制定的相关规范要求，制定统一的数字人民币应用标准和应用数据结构，支持数字人民币硬钱包和卡式软钱包余额查询、数字人民币交易等功能。

7　北京民生一卡通应用流程

7.1.1　社会保障应用流程

社会保障应用流程应按照LD/T 32.7中的规定执行。

7.1.2　金融应用流程

金融应用流程应按照JR/T 0025中的规定执行。

7.1.3　一卡通应用流程

一卡通应用流程应按照JT/T 978中的规定执行。

7.1.4　北京通应用流程

北京通应用流程应按照DB11/T 1179中的规定执行。

7.1.5 残疾人应用流程

残疾人应用流程应按照《中华人民共和国残疾人证技术规范》中的规定执行。

7.1.6 民政应用流程

发行民政应用主要是完成对文件结构的创建和密钥的注入，整体应用流程见图17。

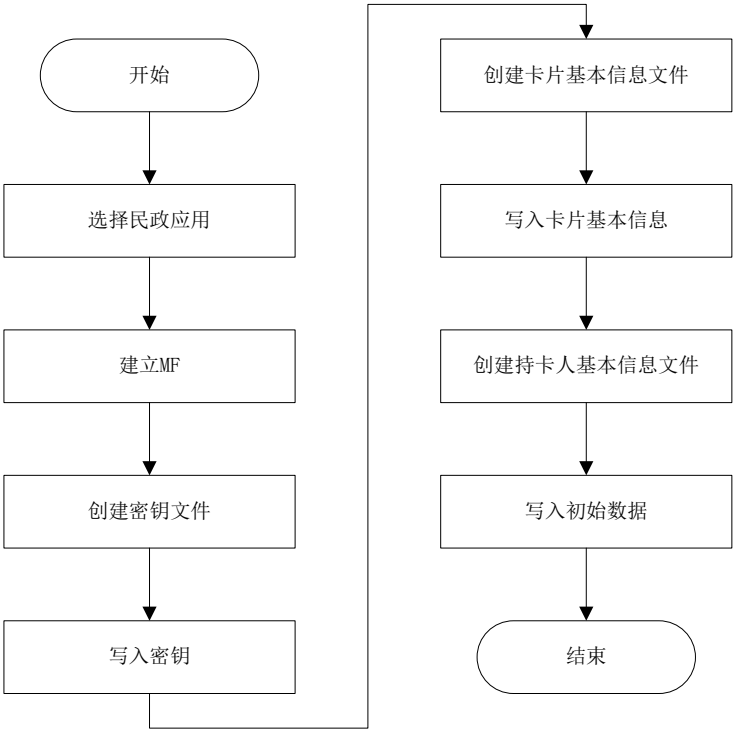


图17 民政应用流程图

7.1.6.1 民政应用处理流程

——写入应用信息；
——终端完成对卡片的外部认证操作；
——获取持卡人基本信息；
——写入持卡人基本信息。

7.1.6.1.1 读取应用信息

——终端完成卡片外部认证操作；
——终端读取卡片的持卡人基本信息文件。

7.1.7 数字人民币应用流程

数字人民币应用流程应按照中国人民银行数字货币研究所制定的相关规范中的规定执行。

8 安全机制

8.1 基本安全要求

8.1.1 共存应用

每一个应用间应设计“防火墙”以防止跨过应用进行非法访问。另外，每一个应用也不应与个性化要求、卡中共存的其他应用规则发生冲突。

8.1.2 安全计算的操作环境

与密钥有关的所有计算（包括产生、派生、传输、鉴别等）过程都应在保密、安全和可靠的环境中进行。这种环境可以由采取了相关措施的物理空间所提供，也可以由经国家密码管理机构认定的设备所提供。

8.1.3 密码算法的安全要求

密码算法用于实现密钥派生（分散）、内部认证、外部认证、数据加密、数据解密及MAC计算等六种类型的安全功能。

卡中所存储的实现密码算法的代码模块，在卡的整个生命周期中不能被修改，也不能被读取、泄露至卡外部。

8.2 密钥的安全要求

8.2.1 密钥的独立性

用于一种特定功能（例如读取数据）的加（解）密密钥，包括保存在卡中的密钥和用于产生、派生、传输这些密钥的密钥，不能被任何其他功能所使用。

如果应用要求进行权限验证，其对终端、发卡方、PSAM或加密机的安全要求请见LD/T 33中的有关规定。

8.2.2 密钥的生成和派生

在密钥的生成和派生过程中，应有物理的随机数发生器所产生的随机数参与计算，同时这种计算不会导致密码算法所规定密钥空间的缩小。

8.2.3 密钥的存放和访问

卡应能够保证密钥在没有授权的情况下，不被泄露；同时卡也应保证密钥除在卡操作系统的控制下用于芯片内部的安全计算外，不能被外界直接访问。

8.2.4 密钥的终止

卡应具有对其所存储密钥的生命周期管理功能，以阻止已失效或过期密钥的使用。

如果应用被永久锁定，与该应用相关的密钥就全部失效。

密钥生成和派生过程中可能产生或使用的临时密钥，只能存放在密码机或卡的挥发性电存储介质中，以确保在密钥生成和派生过程结束后，随着电源的消失而被销毁。

8.2.5 密钥的管理

所有涉及到读取或修改北京民生一卡通中敏感数据的交易，应使用加密密钥来保证应用的安全性。

北京民生一卡通的密钥管理采用按类分级管理方式，即：

——对于由人力资源和社会保障部信息中心负责维护其 AID 的应用，由人力资源和社会保障部信息中心将密钥分发给人力资源和社会保障局。

——对于其他应用（包括发卡方扩充的应用），由发卡方进行密钥管理。

对于使用多版本密钥控制的交易，密钥版本号包含在相关的命令报文中。北京民生一卡通收到这种命令后，使用命令中所给的密钥版本号找到卡中的相应密钥进行运算。

在交易过程中，涉及密钥控制的所有阶段都应使用过程密钥。

存储在北京民生一卡通中用于社会保障应用的密钥见表102。

表102　北京民生一卡通中用于社会保障应用的密钥

分类	密钥	用途	适用的应用范围	管理方式
-	IRK	鉴别发卡方的密钥	应用提供者	部
-	PUK	PIN 解锁密钥	发卡方	省
应用维护密钥	STKSSSE	发卡方或应用提供者用于产生应用锁定、卡片锁定和读取或更新二进制或记录命令的 MAC	发卡方	部
	STKDF01		公共应用	部
	STKDF02		就业与失业应用	部
	STKDF03		社会保险 1 应用	部
	STKDF04		社会保险 2 应用	部
	STKDF07		人事与人才应用	部
卡片或应用锁定控制密钥	BK	发卡方或应用提供者控制锁定卡片或应用操作的密钥	发卡方	省
	LKDF03		社会保险 1 应用	省
	LKDF04		社会保险 2 应用	省
应用数据更新密钥	UKSSSE	发卡方或应用提供者控制应用数据更新操作的密钥	发卡方和个人基本信息	省
	UK1DF01		户籍信息	省
	UK2DF01		个人状况信息	省
	UK3DF01		婚姻状况信息	部
	UK4DF01		通讯信息	部
	UK5DF01		国家/地区及政治面貌信息	省
	UK6DF01		学历信息	部
	UK7DF01		预留信息 1	部
	UK8DF01		预留信息 2	部
	UK9DF01		预留信息 3	部
	UKADF01		预留信息 4	部
	UKBDF01		预留信息 5	部
	UK1DF02		职业和专业技能信息	部
	UK2DF02		就业状况信息	省
	UK3DF02		就业记录	省
	UK4DF02		就业创业证信息	部
	UK5DF02		就业援助对象认定信息	部
	UK6DF02		就业扶持政策享受信息	部

表 102（续）

应用数据更新密钥	UK1DF03	发卡方或应用提供者控制应用数据更新操作的密钥	失业保险信息	省
	UK2DF03		劳动能力鉴定信息	部
	UK3DF03		养老保险信息	省
	UK4DF03		工伤保险信息	部
	UK5DF03		生育保险信息	部
	UK6DF03		工伤认定信息	部
	UK7DF03		供养亲属信息	部
	UK8DF03		参保凭证信息	部
	UK1DF04		医疗、工伤、生育保险基本信息	省
	UK2DF04		医疗保险临时脱网结算信息	部
	UK1DF07		荣誉信息	部
	UK2DF07		专家信息	部
	UK3DF07		军队转业干部信息	部
医疗保险交易密钥	DLK	用于产生账户划入交易中使用的过程密钥 SESLK，在账户划入交易中计算 MAC	医疗保险账户划入交易	省
	DPK	用于产生医疗费用结算中使用的过程密钥 SESPK，在医疗费用结算交易中计算 MAC	医疗保险医疗费用结算交易	部
	DSK	用于更新年度起始日期的密钥	更新年度起始日期	省
	DTK	用于产生账户支付、个人自付和统筹基金支付交易中使用的 TAC	医疗保险交易	省
应用数据读取密钥	RKSSSE	发卡方或应用提供者控制部分应用数据读取操作的密钥	指纹和相片信息	部
	RK1DF01		公共应用信息	部
	RK1DF02		就业与失业信息	部
	RK1DF03		养老、工伤、生育保险信息	部
	RK2DF03		失业保险信息	部
	RK1DF04		医疗保险和医疗费用结算信息	部
	RK1DF07		荣誉信息	部
	RK2DF07		专家信息	部
	RK3DF07		军队转业干部信息	部

8.3 报文传输方式

8.3.1 安全报文传送目的

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。数据的可靠性通过对数据域的加密来得以保证。数据的完整性和对发送方的认证通过使用MAC来实现。

8.3.2 安全报文传送格式

安全报文传送格式应符合GB/T 16649.4的规定。当CLA字节的第二个半字节等于十六进制数字‘4’时，表明对发送方命令数据要采用安全报文传送。根据应用的要求，应事先确定某个命令的数据域的数据是否需要加密传输、是否应以加密的方式处理等。

9 北京民生一卡通终端

9.1 社会保障用卡终端

9.1.1 终端类型、功能及升级

9.1.1.1 类型与功能

9.1.1.1.1 基础型

功能：支持接触、非接操作北京民生一卡通。通过接触、非接界面读取北京民生一卡通实体卡信息。主要用于医院、药店和其他需要跨部门读北京民生一卡通基本信息的场所，如民政部门的身份识别。

9.1.1.1.2 增强型

功能：支持接触、非接操作北京民生一卡通，支持二维码识读。在支持北京民生一卡通实体卡的基础上，增加对北京民生一卡通虚拟卡/电子卡的支持。主要应用于医院、药店和其他需要同时对北京民生一卡通实体卡和虚拟卡做身份识别的场所。

9.1.1.1.3 多功能型

功能：支持接触、非接操作北京民生一卡通，支持二维码识读，支持身份证读取。主要应用于一些对北京民生一卡通和身份证同时有需求的场景。如北京民生一卡通业务经办场所、医院和药店的某些应用、旅游景点检票（人工或闸机）、博物馆的闸机、图书馆的读者证办理或阅览室门禁等。

9.1.1.1.4 全功能型

功能：支持接触、非接操作北京民生一卡通，支持二维码识读，支持身份证读取，支持3D结构光人脸识别。主要应用于需要更高安全要求的人证比对场景，如医院药店防骗保、北京民生一卡通经办场所的人证合一比对等。

9.1.1.2 终端升级要求

用卡机构若需保留现有终端设备，则应满足下列要求：

a) 终端设备厂商应符合行业主管部门对读写终端接口的相关要求以及附录 A 中要求对底层驱动进行改造；
b) 应通过通用操作套件测试及认证。

9.1.2 终端资质要求

北京民生一卡通终端设备应具备以下资质：社会保障卡读卡器检测报告，社会保障卡读写终端接口检测报告，银行卡检测中心支付终端相关检测报告。

如产品支持身份证阅读功能则应具备中国安全技术防范认证中心颁发的中国公共安全产品认证证书，公安部安全与警用电子产品质量检测中心出具的社会公共安全产品认证并提供检测报告。

9.1.3 终端机电特性及传输协议

北京民生一卡通终端设备机电特性及传输协议应符合行业主管部门对社会保障卡读写终端的相关要求。

9.1.4 终端唯一识别码的设计和使用

终端唯一识别码为一组32位定长ASCII码字符串，由终端设备号（20位）与PSAM卡终端机编号（12位）两部分顺序组成。其中终端设备号由厂商代码（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，在终端设备出厂时写入（无法更改），见图18。

PSAM卡终端机编号则是在PSAM卡制作完成后自动生成的一个唯一的PSAM卡终端机编号；

如读卡时发生无终端设备号或PSAM卡终端机编号中任一情况，则缺少部分返回全为0的字符串即可。

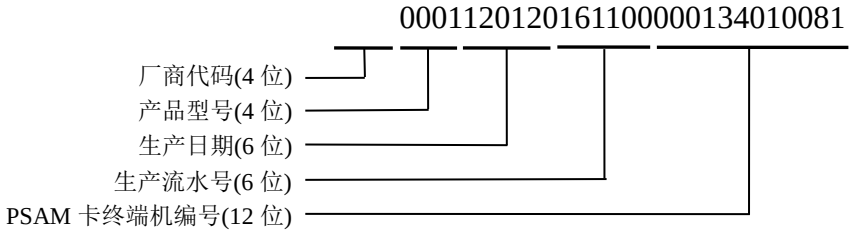


图18 终端唯一识别码示例

终端设备应符合行业主管部门对社会保障卡读写终端的相关要求，若用卡机构现有设备终端设备号或终端设备号命名标准不符合该要求，可对终端设备进行更换或升级。

9.1.5 通用操作套件对接标准

北京民生一卡通通用操作套件基于SSSE32社保环境标准，依据行业主管部门对机具通用技术相关要求进行研发，以满足对终端读写设备控制、社保卡实体卡、电子卡安全认证以及卡内信息的通用读写功能；

用卡机构对接接口应符合附录A中各项要求。

9.1.5.1 通用操作套件接入要求

9.1.5.1.1 接入要求

a) 用卡机构应通过通用操作套件中安全终端注册接口对终端信息进行注册。

b) 用卡机构终端应与北京民生一卡通通用操作套件对接。通用操作套件提供了终端直连认证与中心服务端认证模式以确保用卡环境安全，同时为满足不同客户端系统环境下的集成与使用，通用操作套件支持 C、Java 等版本。

1) 中心服务端认证模式

用卡过程中通用操作套件提供了客户端本地对北京民生一卡通、终端及PSAM认证数据、交易及用卡轨迹数据的安全防护接口，见表103。

表103　套件具体功能

功能范围	具体功能	具体描述
通用功能	机具控制	对终端读写机具的通用性控制，包括： 1、机具设备的打开/关闭 2、判断卡片是否上电 3、获取 32 位唯一识别码 4、一二三代卡识别 5、本地、异地卡识别
	社保区域信息的通用读取	对三代社保卡社保基础应用区域数据进行获取，获取内容包括： 1、基本数据文件信息读取 2、公共应用数据读取 3、就业与失业数据读取 4、社会保险数据读取 5、医疗保险数据读取 6、生命与健康应用数据读取 7、社会救助与抚恤应用数据读取 8、人事与人才应用数据读取
		对三代社保卡社保扩展区域数据进行读取，读取内容包括： 1、北京政务服务 1 应用数据读取 2、北京政务服务 2 应用数据读取 3、北京政务服务 3 应用数据读取 4、北京政务服务 4 应用数据读取 5、北京政务服务 5 应用数据读取
		对一二代社保卡社保基础应用区域、扩展区域数据进行获取
	社保区域信息的通用写入	对三代社保卡社保基础应用区域、扩展区域数据进行通用写入，具体写入内容见“社保区域信息的通用读取”内容
	电子社会保障卡认证	对电子社会保障卡二维码信息读取及认证
安全功能	终端认证数据安全防护	终端认证过程中对终端认证数据及安全服务端认证结果的安全防护
	PSAM 卡认证数据安全防护	PSAM 卡有效性认证过程中对认证数据及安全服务端认证结果的安全防护
	无 PSAM 卡认证数据安全防护	无 PSAM 卡认证过程中对客户端认证数据及安全服务端结果的安全防护

表 103（续）

	卡交易、用卡轨迹数据签名	通过卡内私钥对北京民生一卡通在终端用卡过程中产生的交易、用卡轨迹数据进行本地签名，包括在签名过程中对数字证书 PIN 码进行安全验证
安全功能	PIN 码操作	1、PIN 码验证 2、PIN 码修改 3、PIN 码重置 4、PIN 码解锁

用卡机构应用系统服务端可通过通用操作套件与后台安全服务进行通讯。为满足不同服务端系统环境下的集成和使用，通用操作套件支持C、Java等版本，见表104。

表104　通用套件功能

功能	备注
终端认证	通过中心服务端集中收集终端认证请求并调用后台安全认证服务实现终端有效性安全认证
PSAM 卡认证	通过中心服务端集中收集 PSAM 卡认证请求并调用后台安全认证服务实现 PSAM 卡有效性安全认证
无 PSAM 卡认证	通过中心服务端集中收集无 PSAM 卡认证请求并调用后台安全认证服务实现北京民生一卡通联机认证
数据签名认证	通过中心服务端集中收集数据签名认证请求并调用后台安全认证服务实现北京民生一卡通数据签名认证

2)　终端直连认证模式

终端直连认证模式是指用卡机构终端直接与安全认证服务端进行通讯，从而实现北京民生一卡通、终端设备的有效性认证。若使用该认证模式，用卡机构终端应与后台安全认证服务在相同网络环境中。

9.1.5.1.2　读写规则及终端功能要求

读写规则应符合行业主管部门对安全读写终端全生命周期管理和认证的相关要求，安全读写终端设备应支持终端唯一识别码读取功能。

终端功能结合北京市第一、二代社会保障卡用卡环境现状，北京民生一卡通用卡环境中终端设备应符合表105中的要求。

表105　终端设备对比

机具版本	机具唯一识别码是否 20 位	是否可以 PSAM 卡认证	是否可以后台联机认证
新机具	是	是	是
旧机具	否	是	否

9.1.5.2　通用操作套件接口调用流程

通用操作套件接口调用方式及流程见图19。

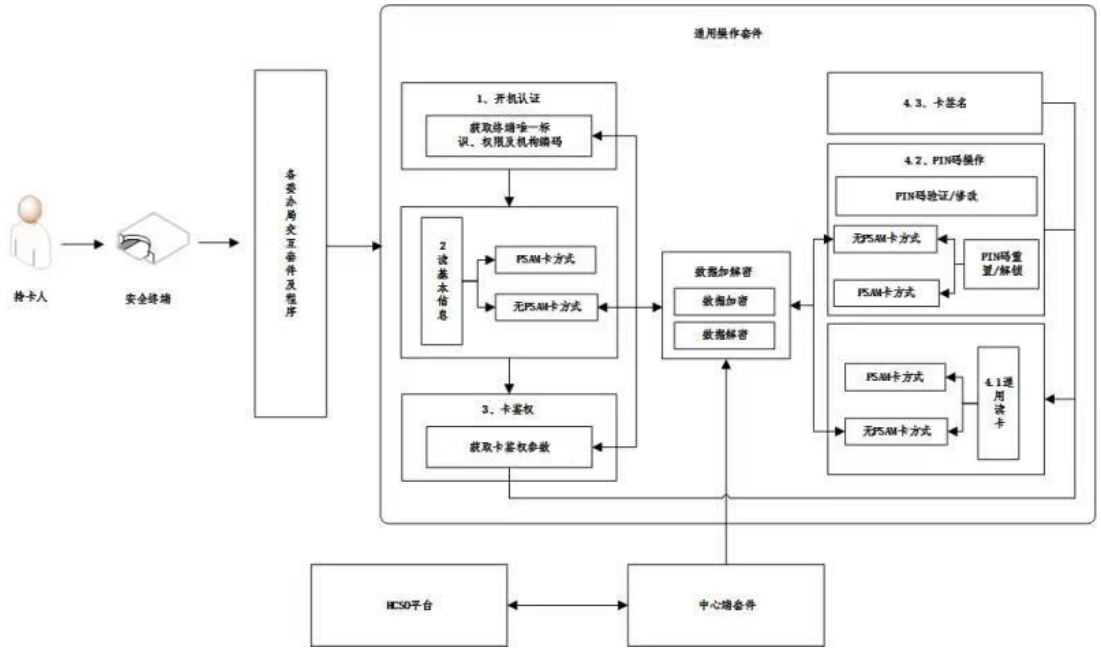


图19　通用操作套件接口调用方式及流程图

9.1.5.2.1.1　开机认证

开机认证流程如下：

a)　终端设备开机后通过调用接口获取终端唯一识别标识、权限及机构编码；

b)　调用“数据加密/解密”接口将获取到的终端唯一识别标识、权限及机构编码进行加密并发送至中心端套件（密文）；

c)　中心端套件与 HCSO 平台交互对该终端进行认证；

d)　认证成功后通过调用“数据加密/解密”接口将返回的终端认证信息进行解密。

9.1.5.2.1.2　读基本信息

a)　有 PSAM 卡读基本信息流程如下：

通过调用接口直接对PSAM卡中基本信息进行读取。

b)　无 PSAM 卡读基本信息流程如下：

1)　通过调用“数据加密/解密”接口将 PSAM 卡信息加密并发送至中心端套件（密文）；

2)　中心端套件与 HCSO 平台交互对 PSAM 卡进行认证；

3)　认证成功后通过调用“数据加密/解密”接口将返回的卡基本信息进行解密。

9.1.5.2.1.3　卡鉴权

卡鉴权流程如下

a)　通过调用接口获取卡鉴权参数；

b)　调用“数据加密/解密”接口将获取到的卡鉴权参数加密并发送至中心端套件（密文）；

c)　中心端套件与 HCSO 平台交互进行卡鉴权；

d)　认证成功后通过调用“数据加密/解密”接口将返回的卡鉴权信息进行解密；

e)　通用读卡、PIN 码操作及卡签名；

f) 用卡机构交互套件及程序可通过调用“通用读卡”、“PIN码操作”、“卡签名”接口对卡数据进行相应的处理。

9.1.5.3 终端驱动改造要求

a) 终端设备应符合行业主管部门对读写终端接口的相关要求；
b) 终端设备应符合附录A中各项接口要求；
c) SSCardDriver.dll中应添加专有接口，并指定PSAM卡槽1为社保使用；
d) 接口调用方式为__stdcall方式。

9.1.5.3.1 扩展区域通用读写规范

用卡操作套件（BJRSCard）在支持第一、二、三代社会保障卡基本信息区域的通用读写外，还应满足对北京市扩展区域信息的通用读写功能。

即：北京市第一、二代社会保障卡的DF0A区，北京民生一卡通的北京政务服务1区至政务服务5区。

终端设备厂商应符合行业主管部门对读写终端接口相关要求的基础上，对所提供的SSCardDriver动态库中“通用读卡”函数和“通用写卡”函数进行改造。

改造要求：原则无需改变SSCardDriver动态库中“通用读卡”函数和“通用写卡”函数的函数结构（包括函数名称、出参、入参、数据结构），仅应在具体函数的代码逻辑以及业务实现的基础上进行内部调整。

9.1.5.3.2 终端设备接口要求

9.1.5.3.2.1 获取终端唯一识别码接口

终端设备厂商在提供的SSCardDriver动态链接库中增加统一的终端唯一标识获取函数,用于对读写设备32位标识码的获取操作。32位终端唯一标识由20位终端设备号和12位PSAM卡号组成。如果终端设备中无PSAM卡，则后12位编码以0补齐。

a) 接口功能

获取终端唯一识别码。

终端唯一识别码为一组 32 位定长 ASCII 码字符串，由终端设备号（20 位）和 PSAM 卡终端机编号（12 位）两部分顺序组成。

b) 接口定义

long iGetDevUID(char *pOutInfo)。

c) 参数说明

参数说明应符合表106的规定。

表106 接口说明

参数	输入/输出	类型	长度	含义
pOutInfo	OUT	字符串	512	返回终端唯一识别码或错误信息

1) 输出参数pOutInfo

当函数执行成功时，输出参数为终端唯一识别码。

当函数执行失败时，输出参数为错误信息描述。

d) 返回值

操作成功时返回0，其他返回值为错误代码。

9.1.5.3.2.2 电子社会保障卡读取接口

利用终端设备中扫码窗口，扫描电子社会保障卡二维码。

终端设备厂商需在SSCardDriver动态链接库中统一增加电子社会保障卡二维码信息读取接口。

a) 接口功能

对于支持扫码窗口的终端设备，通过此接口读取电子社会保障卡二维码信息。

b) 接口定义

long iReadSCode(int iTimeout, char *pOutInfo)。

c) 参数说明

参数说明应符合表107的规定。

表107 参数说明

参数	输入/输出	类型	长度	含义
iTimeout	IN	整型	4	扫描二维码的超时时间
pOutInfo	OUT	字符串	512	返回数据或错误信息

1) 入出参数 iTimeout

超时时间。

2) 输出参数 pOutInfo

当函数执行成功时，输出参数为电子社会保障卡信息；

当函数执行失败时，输出参数为错误信息描述。

d) 返回值

操作成功时返回0，其他返回值为错误代码。

9.1.5.3.2.3 医保信息读取

a) 接口功能

获取医保信息。

b) 接口定义

long iReadYBInfo(int iType, char* pCardInfo, char* pOutInfo)。

c) 参数说明

参数说明应符合表108的规定。

表108 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整型	4	扫描二维码的超时时间
pCardInfo	IN	字符串	512	卡片信息
pOutInfo	OUT	字符串	512	返回数据或错误信息

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输入。

2) 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。

3) 输出参数 pOutInfo

当函数执行成功时，该输出参数为读出的DF0AEF0C文件相关信息。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。

d) 返回值

操作成功时返回0，其他返回值为错误代码。

9.1.5.3.2.4 北京民生一卡通数据签名接口

a) 接口功能

使用北京民生一卡通中的非对称区密钥，对输入数据签名，输出签名值和签名证书。北京民生一卡通非对称区用户PIN码默认为123456。

b) 接口定义

long iSignData(int iType,

char *pCardInfo,

char *pSrcData,

char *pOutInfo)。

c) 参数说明

参数说明应符合表109的规定。

表109 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡类型
pCardInfo	IN	字符串	512	卡片信息
pSrcData	IN	字符串	1024*10	需要签名的数据(Hex)
pOutInfo	OUT	字符串	512	返回签名数据或错误信息

1) 输入参数 iType

操作卡类型应符合《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号的规定。

2) 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。

3) 输入参数 pSrcData

签名的原始数据(HEX格式数据)。

4) 输出参数 pOutInfo

当函数执行成功时，该输出参数为签名信息，依次为：签名值、签名证书ID。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，输出参数为错误信息描述。

d) 返回值

操作成功时返回0，其他返回值为错误代码。

9.1.5.3.2.5 身份证信息读取

a) 接口功能

获取证件信息。

b) 接口定义

long iReadCertInfo(int iType, char *pPhotoPath,char *pPhotoData, char *pOutInfo)。

c) 参数说明

参数说明应符合表110的规定。

表110 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	相片处理方式
pPhotoPath	IN	字符串	1024	相片保存路径(保留)
pPhotoData	OUT	字符串	10240	相片 base64 数据流(保留)
pOutInfo	OUT	字符串	1024	返回数据或错误信息

1) 输入参数 iType

相片处理方式

0-不生成相片，不输出相片base64数据流

其他值-保留相片。

2) 输入参数 pPhotoPath

相片保存路径(保留参数)。

3) 输出参数 pPhotoData

相片base64数据流(保留参数)。

4) 输出参数 pOutInfo

当函数执行成功时，该输出参数为读出的证件上除相片外的其他信息。

返回值为0时，返回身份证信息，数据格式为：姓名、性别、民族、出生日期、地址、身份证号码、发行机关、有效开始日期、有效截止日期、相片文件存放路径。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

返回值为1时，返回外国人居住证信息，数据格式为：英文名、中文名、性别、国籍或所在区域代码、出生日期、永久居住证号码、有效开始日期、有效截止日期、当次申请受理机关代码、证件版本号、相片文件存放路径。各数据项之间以“|”分割，且最后一个数据项以“|”结尾(该功能暂不开放)。

返回值为2时，返回港澳台居住证信息，数据格式为：姓名、性别、出生日期、地址、身份证号码、发行机关、有效开始日期、有效截止日期、通行证号码、签发次数、相片文件存放路径。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。

d) 返回值

0-身份证；

1-外国人居住证；

2-港澳台居住证。

小于 0 则为错误代码：

-2-无卡；

-13-（动态库）不支持该命令。

9.1.5.3.2.6 设备信息读取

a) 接口功能

获取终端设备厂商，设备类型，库版本信息。

b) 接口定义

long iDeviceGetInfo(char *pOutInfo)。

c) 参数说明

参数说明应符合表111的规定。

表111 参数说明

参数	输入/输出	类型	长度	含义
pOutInfo	OUT	字符串	1024	返回厂商信息或错误信息

1) 输出参数 pOutInfo

当函数执行成功时，输出参数为终端设备厂家信息。

终端设备厂商信息的存储格式见表112。

表112 终端设备厂商信息的存储格式

第 1～16 字符	第 17～30 字符	第 31～32 字符
厂商名称（不足空格补齐）	设备型号或系列号（不足空格补齐）	函数库版本号

当函数执行失败时，输出参数为错误信息描述。

d) 返回值

操作成功时返回0，其他返回值为错误代码。

9.2 金融用卡终端

金融用卡终端应符合行业主管部门对金融行业应用终端的相关要求。

9.3 一卡通用卡终端

对于支持交通行业应用卡片读写功能的读写器，有以下基本要求：

a) 通信要求

终端通信要求应符合《城市公共交通IC卡技术规范第5部分：非接触接口通讯》的规定，并应同时支持 Type A卡片和Type B卡片。

b) SAM 卡读卡器及卡槽

支持北京市政交通一卡通的交通应用标准的SAM卡接口的SAM卡读写器及卡槽。SAM卡默认采用9600bps的通讯速率，最高可协调至115200bps的通讯速率。

c) 基本性能要求

射频兼容标准：应同时支持 Type A和Type B的非接触芯片，在兼容其它通讯协议时不得影响此协议；

射频工作频率：13.56MHz±7KHz；

射频通信速率：106kbit/s；

非接触标识：读卡器位置应有明显刷卡标识；

非接触卡片放置保护：非手持刷卡的终端，卡片置于刷卡区后，应有边缘保护，不能被轻易碰掉，从而使通信中断。

d) 通用要求

读卡器本身可以通过二次程序开发实现部分或全部非接触式IC卡业务逻辑。

e) 终端应用选择要求

终端可分为仅支持交通卡刷卡终端和支持多种支付方式刷卡/刷码的终端，终端中应存储有可支持的应用（或应用AID）列表，终端应用选择是指从具有多个非接触应用的列表中进行选择的行为。交通行业终端，在终端支持的应用列表中，应优先选择交通部电子钱包应用，并且采用直接选择AID的方式选中（AID = A0000006320101O5）。

f) 终端提示信息

终端应能根据业务处理要求，对北京民生一卡通卡片的刷卡交易有声音或信息显示等变化做相应调整。

9.4 北京通用卡终端

北京通用卡终端应符合行业主管部门对社会保障卡读写终端的相关要求。

9.5 民政用卡终端

民政领域暂无用卡场景，目前未涉及相关终端技术规范要求。

9.6 残联用卡终端

残联用卡终端应符合行业主管部门对接触式、非接触式IC卡读卡终端的相关要求。

9.7 数字人民币用卡终端

数字人民币应用卡终端应符合中国人民银行数字货币研究所制定的规范中的相关要求。

10 北京民生一卡通电子卡

北京民生一卡通电子卡应符合相关行业主管部门对电子社会保障卡的相关要求。

附 录 A
（规范性）
通用操作套件接口方案

A.1 北京民生一卡通社会保障应用接口

系统支持：

Win7 SP1及以上系统，x86/X64处理器；

接口为win32动态库，支持win32程序调用。

接口约定：

接口函数的调用约定为__stdcall方式。

接口函数的名称前缀为BJRS_。

接口说明：

接口按使用的设备，可以分为三类：

a) 中心端方式适用于需要连接后台方式，但无法直接连接，需要通过其他途径中转数据；

b) 非中心端方式适用于两种情况：只使用本地 PSAM 卡操作或套件可以直连后台；

c) 通用接口不需要 PSAM 或加密机参与。

三类接口可混合调用。

A.1.1 中心端方式接口

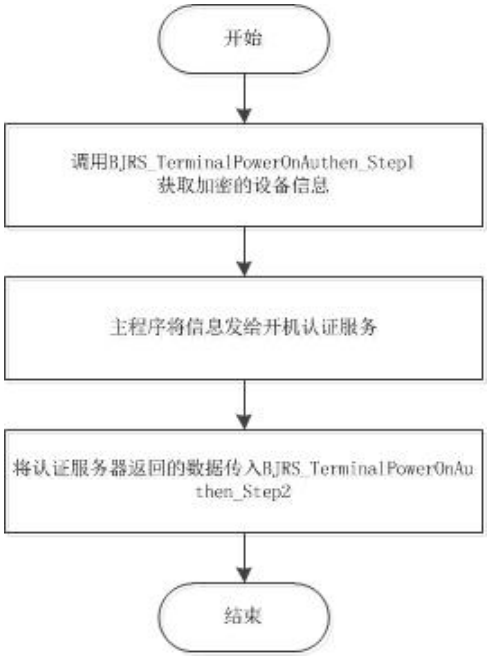
A.1.1.1 开机认证接口（步骤一）

A.1.1.1.1 接口功能

验证终端的有效性，见图A.1。

终端设备接入电脑后，需要先开机认证，有效的设备才可进行后续操作。

对于未联网终端，在调用第一步成功后，可以使用本地PSAM卡进行操作，此方式为离线操作。如要使用后台相关功能，需要调用开机认证第二步。



图A.1 中心端方式的调用流程

本接口内部执行流程：

a) 先检测当前连接的读写机具；

b) 读取机具终端唯一识别码，将输入的信息和唯一识别码加密输出。

A.1.1.1.2 接口定义

long BJRS_TerminalPowerOnAuthen_Step1 (const char *pSysId,const char * pDeptId, int iDeviceAuth,char* pOutInfo)。

A.1.1.1.3 参数说明

参数说明见表A.1。

表A.1 参数说明

参数	输入/输出	类型	长度	含义
pSysId	IN	字符串	64	应用系统类型
pDeptId	IN	字符串	64	终端所属机构
iDeviceAuth	IN	整数	4	终端权限类型
pOutInfo	OUT	字符串	1024	输出密文或返回错误信息

输入参数pSysId,应用系统代码，医保系统固定为 YBXT001 。

输入参数pDeptId,终端所属的机构代码，由后台系统分配。

输入参数iDeviceAuth,终端权限类型，后台系统进行注册时的终端权限。1-人社局权限；2-医保局权限；3-医院权限；4-卡服务网点权限；5-基本应用权限。

输出参数pOutInfo,当函数执行成功时，输出密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.1.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.2 开机认证接口（步骤二）

A.1.1.2.1 接口功能

中心端方式开机认证第二步。

本接口内部执行流程：

a) 解密认证服务器返回的数据；

b) 验证终端的有效性，返回验证结果。

A.1.1.2.2 定义

long BJRS_TerminalPowerOnAuthen_Step2 (const char *pKey, char* pOutInfo)。

A.1.1.2.3 参数说明

参数说明见表A.2。

表A.2 参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	认证服务器返回的密文
pOutInfo	OUT	字符串	1024	输出为终端信息或返回错误信息

输入参数pKey,认证服务器返回的密文。

输出参数pOutInfo,当函数执行成功时，输出终端唯一识别码、套件版本号，以“|”分割。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.2.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

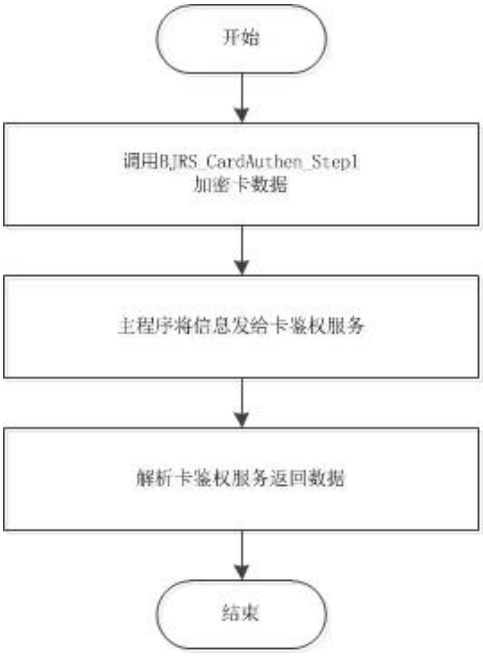
A.1.1.3 卡鉴权接口

A.1.1.3.1 接口功能

调用后台持卡库，验证卡的有效性。

在读取到卡的基本信息后，应卡鉴权，然后再对有效卡进行其他操作。

卡鉴权接口的调用流程见图A.2。



图A.2 卡鉴权接口的调用流程图

本接口内部执行流程：

a) 对输入数据进行加密；

b) 输出密文。

A.1.1.3.2 接口定义

long BJRS_CardAuthen_Step1 (const char * pMessage, char* pOutInfo)。

A.1.1.3.3 参数说明

参数说明见表A.3。

表A.3 参数说明

参数	输入/输出	类型	长度	含义
pMessage	IN	字符串	1024	卡信息
pOutInfo	OUT	字符串	1024	输出密文或返回错误信息

输入参数pMessage,该参数用于传入卡的信息，依次为：卡规范版本号、发卡地行政区划代码、社会保障号码、社会保障卡卡号、识别码、姓名。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

输出参数pOutInfo,当函数执行成功时，输出密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.3.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

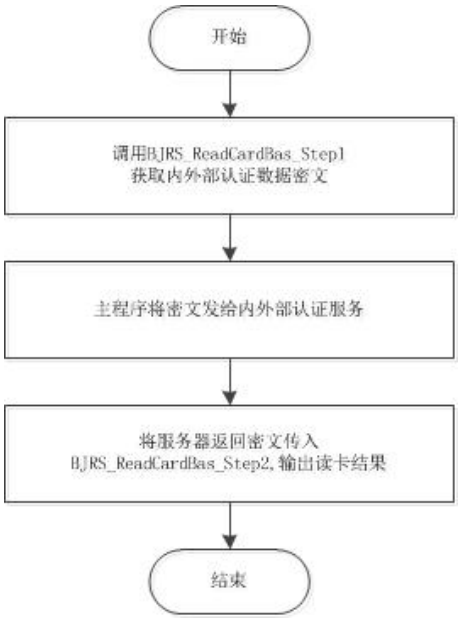
A.1.1.4 读北京民生一卡通社会保障应用基本信息接口（中心端 步骤一）

A.1.1.4.1 接口功能

读取北京民生一卡通社会保障应用的基本信息(卡片信息和个人信息)。

在中心端方式进行任何北京民生一卡通操作前，应先调用此函数。

中心端方式读社保卡基本信息分为2个步骤。接口调用流程见图A.3。



图A.3 接口调用流程

接口的内部执行流程为：

a) 读取卡内的发卡信息文件和内外部认证数据；

b) 将数据进行加密并输出。

A.1.1.4.2 接口定义

long BJRS_ReadCardBas_Step1(int iType, char* pOutInfo)。

A.1.1.4.3 参数说明

参数说明见表A.4。

表A.4 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pOutInfo	OUT	字符串	1024	内部认证数据密文或返回错误信息

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。

输出参数pOutInfo,当函数执行成功时，该输出参数为内外部认证数据密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.4.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.5 读北京民生一卡通社会保障应用基本信息接口（中心端 步骤二）

A.1.1.5.1 接口功能

读取北京民生一卡通社会保障应用的基本信息第三步，输出读卡的结果。

接口的内部执行流程为：

a) 将内外部认证服务返回密文，获取内部认证,外部认证鉴别数据；

b) 对卡进行认证，输出读卡结果。

A.1.1.5.2 接口定义

long BJRS_ReadCardBas_Step2(const char *pKey, char* pOutInfo)。

A.1.1.5.3 参数说明

参数说明见表A.5。

表A.5 参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	内外部认证服务返回密文
pOutInfo	OUT	字符串	1024	读出数据或返回错误信息

输入参数pKey，内外部认证服务返回密文。

输出参数pOutInfo，当函数执行成功时，该输出参数为读出的北京民生一卡通社会保障应用基本信息各数据项。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，该输出参数为错误信息描述。

示例：639900|111111198101011110|X00000019|639900D15600000500BF7C7A48FB4966|xxxx|00814E43238697159900BF7C7A|1.00|20101001|20201001|410100813475|终端设备号|。

A.1.1.5.4 返回值

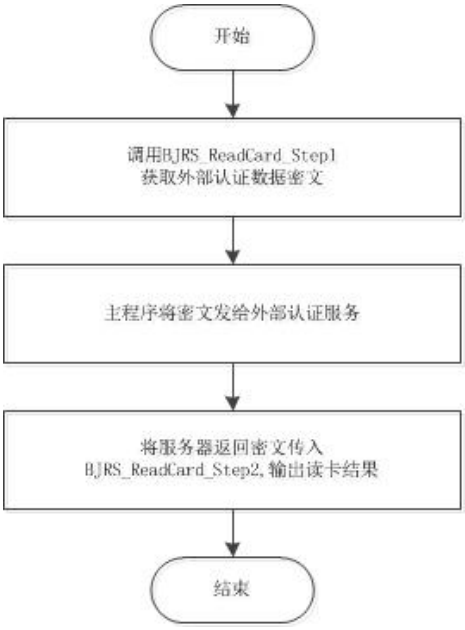
操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.6 通用读卡接口（步骤一）

A.1.1.6.1 接口功能

读取卡内社保区的指定文件的内容，每次调用只能读同一个文件中信息。

中心端方式通用读卡分2个步骤。接口调用流程见图A.4。



图A.4　接口调用流程

接口的内部执行流程为：

a)　根据需要读取的文件，生成外部认证信息；

b)　对外部认证信息加密，输出密文。

A.1.1.6.2　接口定义

long BJRS_ReadCard_Step1(int iType,const char* pCardInfo, const char* pFileAddr, char* pOutInfo)。

A.1.1.6.3　参数说明

参数说明见表A.6。

表A.6　参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pCardInfo	IN	字符串	128	卡基本信息
pFileAddr	IN	字符串	1024	文件名及数据项
pOutInfo	OUT	字符串	1024*20	密文或返回错误信息

输入参数iType，定义同上。

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。

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。例

如读出2.0卡的学位信息2表示为：DF01EF15|40:2|$；读出国家/地区代码、学历、学位信息2表示为：DF01EF0A|37|$DF01EF15|2A|40:2|$。

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。

输出参数pOutInfo

当函数执行成功时，该输出参数为外部认证密文；

当函数执行失败时，该输出参数为错误信息描述。

A.1.1.6.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.7 通用读卡接口（步骤二）

A.1.1.7.1 接口功能

通用读卡功能第二步。

接口内部执行流程为：

a) 解密外部认证服务返回的密文，提取鉴别数据；

b) 对卡外部认证，读取卡信息，输出结果。

A.1.1.7.2 接口定义

long BJRS_ReadCard_Step2(const char* pKey, char* pOutInfo)。

A.1.1.7.3 参数说明

参数说明见表A.7。

表A.7 参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	外部认证服务返回密文
pOutInfo	OUT	字符串	1024*20	读出数据或返回错误信息

输入参数pKey，调用外部认证服务返回的密文。

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。例如读出国家/地区代码的输出参数表示为：DF01EF0A|CHN|$。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.7.4 返回值

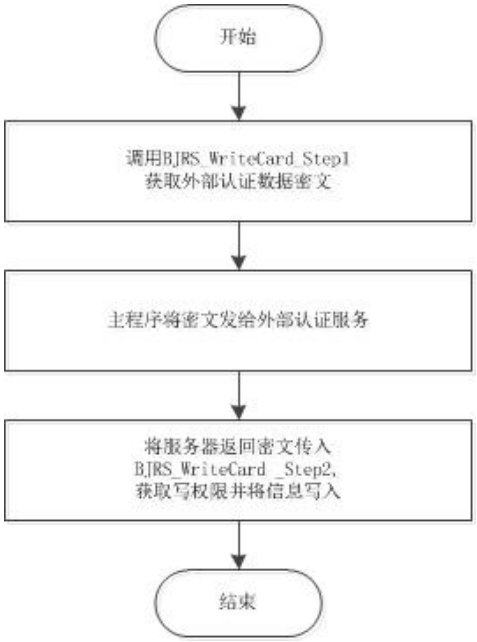
操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.8 通用写卡接口（步骤一）

A.1.1.8.1 接口功能

更新社保区内指定文件的内容，每次只写同一个文件，可以写同一文件多个字段。

中心端方式的通用写卡流程如A.5。



图A.5　通用写卡流程

本接口执行流程为：

a)　根据要写入的文件，生成外部认证数据；

b)　对数据加密，输出密文。

A.1.1.8.2　接口定义

long BJRS_WriteCard_Step1(int iType, const char* pCardInfo, const char* pFileAddr, char* pOutInfo)。

A.1.1.8.3　参数说明

参数说明见表A.8。

表A.8　参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pCardInfo	IN	字符串	128	卡基本信息
pFileAddr	IN	字符串	1024	文件名及数据项
pOutInfo	OUT	字符串	1024	密文或错误信息

输入参数iType，定义同上。

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。

输入参数pFileAddr，该参数用于指定拟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。例如写入2.0卡就业状态，表示为：DF01EF07|29|$；写入国家/地区代码，表示为： DF01EF0A|37|$。

当拟写入的文件为循环文件时，只需指定文件名，函数将新增记录；当拟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。

输出参数pOutInfo，当函数执行成功时，该输出参数为外部认证数据密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.8.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.9 通用写卡接口（步骤二）

A.1.1.9.1 接口功能

通用写卡功能第二步。

接口内部执行流程为：

a) 解密外部认证服务返回的密文，获取鉴别数据；

b) 对卡进行外部认证并写入信息，返回处理结果。

A.1.1.9.2 接口定义

long BJRS_WriteCard_Step2(const char* pKey,const char* pWriteData, char* pOutInfo)。

A.1.1.9.3 参数说明

参数说明见表A.9。

表A.9 参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	外部认证服务返回密文
pWriteData	IN	字符串	1024*20	写入数据项信息
pOutInfo	OUT	字符串	1024	返回空字符串或错误信息

输入参数pKey，外部认证返回的密文信息。

输入参数pWriteData，该参数用于传入拟写入的数据项信息。其格式与输入参数pFileAddr严格对应且分隔符完全一致。例如写入2.0卡就业状态为1，表示为：DF01EF07|1|$；写入国家/地区代码为CHN，表示为：DF01EF0A|CHN|$。

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。

A.1.1.9.4 返回值

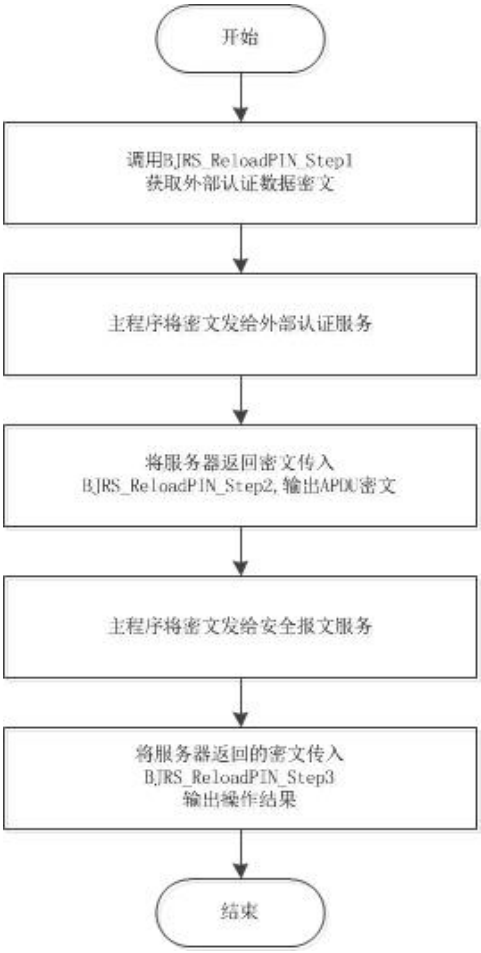
操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.10 PIN重置接口（步骤一）

A.1.1.10.1 接口功能

重置社会保障应用的PIN码。

中心端方式的PIN重置接口分为3个步骤，调用流程见图A.6。



图A.6　调用流程

本接口的内部执行流程为：

a)　从卡片获取外部认证数据；

b)　将外部认证数据加密，输出密文。

A.1.1.10.2　接口定义

long BJRS_ReloadPIN_Step1(int iType,const char* pCardInfo, char* pOutInfo)。

A.1.1.10.3　参数说明

参数说明见表A.10。

表A.10　参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pCardInfo	IN	字符串	128	卡基本信息
pOutInfo	OUT	字符串	1024	密文或错误信息

输入参数iType,定义同上。

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。

输出参数pOutInfo,当函数执行成功时，该输出参数为外部认证密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.10.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.11 PIN重置接口（步骤二）

A.1.1.11.1 接口功能

重置社保区的PIN码第二步。

本接口的内部执行流程为：

a) 解密外部认证服务返回的密文，获取鉴别数据；

b) 对卡进行外部认证，输出安全报文密文数据。

A.1.1.11.2 接口定义

long BJRS_ReloadPIN_Step2(const char* pKey, char* pOutInfo)。

A.1.1.11.3 参数说明

参数说明见表A.11。

表A.11 参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	外部认证服务返回的密文
pOutInfo	OUT	字符串	1024	密文或错误信息

输入参数pKey，外部认证服务返回的密文。

输出参数pOutInfo，当函数执行成功时，该输出参数为安全报文数据密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.11.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.12 PIN重置接口（步骤三）

A.1.1.12.1 接口功能

重置社保区的PIN码第三步。

本接口的内部执行流程为：

a) 解密安全报文认证服务返回的密文，获取 APDU 指令；

b) 执行指令并输出操作结果。

A.1.1.12.2 接口定义

long BJRS_ReloadPIN_Step3(const char* pKey, char* pOutInfo)。

A.1.1.12.3 参数说明

参数说明见表A.12。

表A.12 参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	安全报文认证服务返回的密文
pOutInfo	OUT	字符串	1024	密文或错误信息

输入参数pKey，外部认证服务返回的密文。

输出参数pOutInfo，当函数执行成功时，该输出参数为安全报文数据密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.12.4 返回值

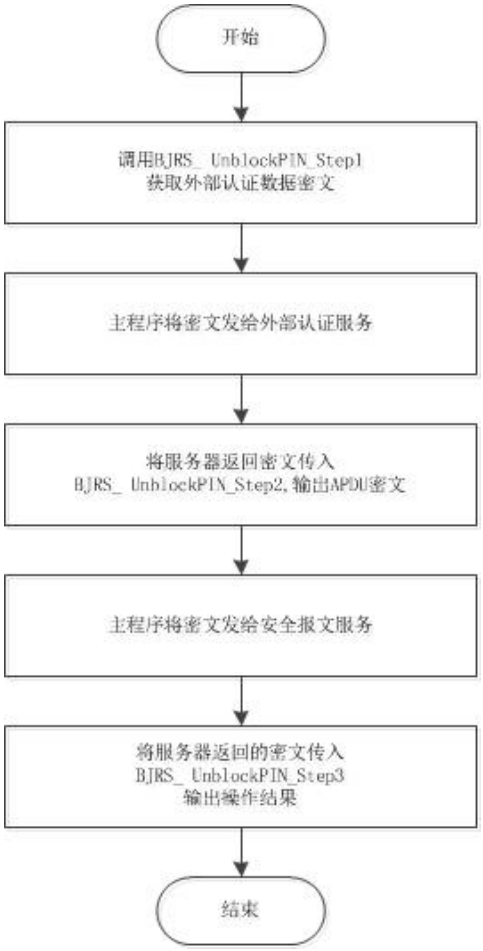
操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.13 PIN解锁接口（步骤一）

A.1.1.13.1 接口功能

社会保障应用PIN解锁。

中心端方式的PIN解锁分为3个步骤，调用流程见图A.7。



图A.7 调用流程

本接口内部执行流程为：

a) 从卡内获取外部认证数据；

b) 对数据进行加密，输出密文。

A.1.1.13.2 接口定义

long BJRS_UnblockPIN_Step1(int iType, const char* pCardInfo, char* pOutInfo)。

A.1.1.13.3 参数说明

参数说明见表A.13。

表A.13　参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pCardInfo	IN	字符串	128	卡基本信息
pOutInfo	OUT	字符串	512	返回空字符串或错误信息

输入参数iType，定义同上。

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。

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。

A.1.1.13.4　返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.14　PIN解锁接口（步骤二）

A.1.1.14.1　接口功能

社会保障应用PIN解锁步骤二。

本接口内部执行流程为：

a)　对外部认证服务返回密文解密，获取鉴别数据；

b)　对卡进行外部认证，生成安全报文请求并加密，输出密文。

A.1.1.14.2　接口定义

long BJRS_UnblockPIN_Step2(const char* pKey, char* pOutInfo)。

A.1.1.14.3　参数说明

参数说明见表A.14。

表A.14　参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	外部认证服务返回的密文
pOutInfo	OUT	字符串	1024	返回密文或错误信息

输入参数pKey，外部认证服务返回的密文。

输出参数pOutInfo，当函数执行成功时，该输出参数为安全报文密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.14.4　返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.15　PIN解锁接口（步骤三）

A.1.1.15.1　接口功能

社会保障应用PIN解锁步骤三。

本接口内部执行流程为：

a)　对安全报文认证服务返回密文解密，获取卡指令；

b)　执行卡指令，并输出操作结果。

A.1.1.15.2　接口定义

long BJRS_UnblockPIN_Step3(const char* pKey, char* pOutInfo)。

A.1.1.15.3 参数说明

参数说明见表A.15。

表A.15 参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	外部认证服务返回的密文
pOutInfo	OUT	字符串	1024	返回空字符串或错误信息

输入参数pKey，安全报文认证服务返回的密文。

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。

A.1.1.15.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.16 终端注册接口

A.1.1.16.1 接口功能

将终端注册到后台系统。由于后台系统返回无数据，不需要进一步处理。

本接口内部执行流程为：

a) 查找终端设备，找到后读取终端唯一识别码；

b) 构造请求数据，加密并返回结果。

A.1.1.16.2 接口定义

long BJRS_TerminalRegisterAuthen _Step1(const char *pSysId, const char *pDeptId, int iDeviceAuth, char *pOutInfo)。

A.1.1.16.3 参数说明

参数说明见表A.16。

表A.16 参数说明

参数	输入/输出	类型	长度	含义
pSysId	IN	字符串	64	应用系统类型
pDeptId	IN	字符串	64	终端所属机构
iDeviceAuth	IN	整数	4	终端权限类型
pOutInfo	OUT	字符串	1024	输出密文或返回错误信息

输入参数pSysId，应用系统代码，由后台系统分配。

输入参数pDeptId，终端所属的机构代码，由后台系统分配。

输入参数iDeviceAuth，终端权限类型，后台系统进行注册时的终端权限。1-人保局权限；2-医保局权限；3-医院权限；4-卡服务网点权限；5-基本应用权限。

输出参数pOutInfo，当函数执行成功时，输出密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.16.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.17 终端注销接口

A.1.1.17.1 接口功能

注销终端设备和PSAM卡。注销后的设备不可再使用。

本接口内部执行流程为：

a) 查找终端设备并读取设置的唯一识别码；

b) 构造请求并进行加密，返回结果。

A.1.1.17.2 接口定义

long BJRS_TerminalCancelAuthen_Step1(const char *pSysId, const char *pDeptId, int iDeviceAuth, int iCancelType, char *pOutInfo)。

A.1.1.17.3 参数说明

参数说明见表A.17。

表A.17 参数说明

参数	输入/输出	类型	长度	含义
pSysId	IN	字符串	64	应用系统类型
pDeptId	IN	字符串	64	终端所属机构
iDeviceAuth	IN	整数	4	终端权限类型
iCancelType	IN	整数	4	注销原因
pOutInfo	OUT	字符串	1024	输出密文或返回错误信息

输入参数pSysId，应用系统代码，由后台系统分配。

输入参数pDeptId，终端所属的机构代码，由后台系统分配。

输入参数iDeviceAuth，终端权限类型，后台系统进行注册时的终端权限。1-人保局权限；2-医保局权限；3-医院权限；4-卡服务网点权限；5-基本应用权限。

输入参数iCancelType，注销终端的原因，0-终端PSAM卡丢失/损坏；1-终端丢失/损坏； 2-PSAM卡丢失/损坏。

输出参数pOutInfo，当函数执行成功时，输出密文。当函数执行失败时，该输出参数为错误信息描述。

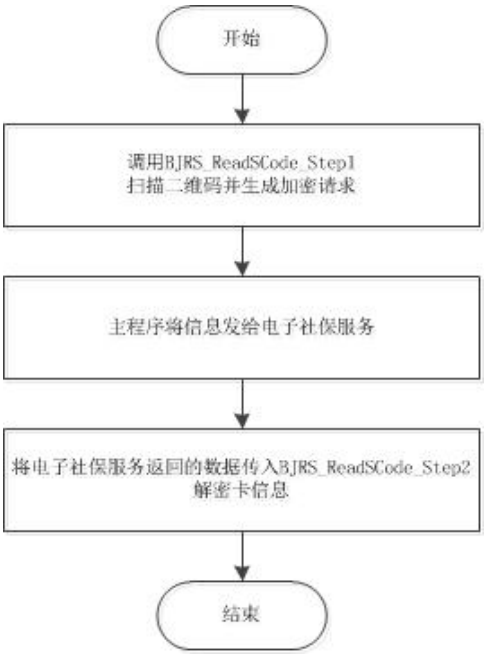
A.1.1.17.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.18 读电子社会保障卡接口（步骤一）

A.1.1.18.1 接口功能

使用读写机具上的扫码窗口,扫描电子社会保障卡二维码,然后将读到的信息发送到电子社保服务，获取社保信息。中心端方式的调用流程，见图A.8。



图A.8　中心端方式调用流程

本接口内部执行流程：

a)　启动扫码功能，扫描用户的二维码；

b)　读取机具终端唯一识别码，将输入的信息和唯一识别码加密输出。

A.1.1.18.2　接口定义

long BJRS_ReadSCode_Step1(int iTimeout, char* pOutInfo)。

A.1.1.18.3　参数说明

参数说明见表A.18。

表A.18　参数说明

参数	输入/输出	类型	长度	含义
iTimeout	IN	整数	4	扫码超时时间
pOutInfo	OUT	字符串	1024	输出密文或返回错误信息

输入参数iTimeout，扫码超时时间，以秒为单位。

输出参数pOutInfo，当函数执行成功时，输出密文。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.18.4　返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.1.19　读电子社会保障卡接口（步骤二）

A.1.1.19.1　接口功能

中心端方式读电子社会保障卡的第二步。

本接口内部执行流程：

a)　解密电子社保服务返回的数据；

b)　输出解密结果。

A.1.1.19.2　接口定义

long BJRS_ReadSCode_Step2 (const char *pKey, char* pOutInfo)。

A.1.1.19.3 参数说明

参数说明见表A.19。

表A.19 参数说明

参数	输入/输出	类型	长度	含义
pKey	IN	字符串	1024	服务器返回的密文
pOutInfo	OUT	字符串	1024	输出为电子社会保障卡或返回错误信息

输入参数pKey，服务器返回的密文。

输出参数pOutInfo，当函数执行成功时，输出电子社会保障卡信息。当函数执行失败时，该输出参数为错误信息描述。

A.1.1.19.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2 非中心端方式(直连)接口

本部分接口功能受开机认证操作的影响：

使用分步操作开机认证初始化后，所有的接口都不连接后台加密机，只使用PSAM卡操作；

使用下面的开机认证时，如果指定bUseHsm为1，才会直连加密机；如果bUseHsm为0，卡操作函数也不会连接后台加密机，只使用PSAM卡操作。

A.1.2.1 开机认证

A.1.2.1.1 接口功能

验证终端的有效性。

终端设备接入电脑后，应先开机认证，有效的设备才可进行后续操作。

本接口内部执行流程：

a) 先检测当前连接的读写机具；

b) 读取机具终端唯一识别码；

c) 将终端唯一识别码和注册信息发给开机认证服务，验证终端有效性。

A.1.2.1.2 接口定义

long BJRS_TerminalPowerOnAuthen(const char *pSysId,const char * pDeptId, int iDeviceAuth, int bUseHsm,char* pOutInfo)。

A.1.2.1.3 参数说明

参数说明见表A.20。

表A.20 参数说明

参数	输入/输出	类型	长度	含义
pSysId	IN	字符串	64	应用系统
pDeptId	IN	字符串	64	终端所属机构
bUseHsm	IN	整数	4	是否使用加密机
iDeviceAuth	IN	整数	4	终端权限类型
pOutInfo	OUT	字符串	1024	输出密文或返回错误信息

输入参数pSysId，应用系统代码，医保系统固定为 YBXT001 ；

输入参数pDeptId，终端所属的机构代码，由后台系统分配；

输入参数iDeviceAuth，终端权限类型，后台系统进行注册时的终端权限；

输入参数bUseHsm，在使用PSAM卡方式无法完成操作时，是否使用加密机：0-不使用加密机；1-使用加密机；

输出参数pOutInfo，当函数执行成功时，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。

A.1.2.1.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.2 卡鉴权接口

A.1.2.2.1 接口功能

调用后台持卡库，验证卡的有效性。

在读取到卡的基本信息后，应卡鉴权，然后再对有效卡进行其他操作。

本接口内部执行流程：

1) 对输入数据进行加密；
2) 将数据发送到卡鉴权服务器，并取回结果。

A.1.2.2.2 接口定义

long BJRS_CardAuthen(const char * pMessage, char* pOutInfo)。

A.1.2.2.3 参数说明

参数说明见表A.21。

表A.21 参数说明

参数	输入/输出	类型	长度	含义
pMessage	IN	字符串	1024	卡信息
pOutInfo	OUT	字符串	1024	输出卡鉴权结果或返回错误信息

输入参数pMessage，该参数用于传入卡的信息，依次为：卡规范版本号、发卡地行政区划代码、社会保障号码、社会保障卡卡号、识别码、姓名。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

输出参数pOutInfo，当函数执行成功时，该输出参数为鉴权数据：社保卡鉴权结果、反馈提示信息，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。

A.1.2.2.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.3 读北京民生一卡通社会保障应用基本信息（非中心端）

A.1.2.3.1 接口功能

读取北京民生一卡通社会保障应用基本信息(卡片信息和个人信息)。

在非中心端方式进行任何社保卡操作前，应先调用此函数。

接口内部执行流程为：

a) 尝试使用 PSAM 卡方式读卡基本信息，成功后返回结果；

b) 使用 PSAM 不成功时，如果开机认证时启用加密机，则继续使用加密机操作,返回处理结果。

A.1.2.3.2 接口定义

long BJRS_ReadCardBas(int iType, char* pOutInfo)。

A.1.2.3.3 参数说明

参数说明见表A.22。

表A.22 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pOutInfo	OUT	字符串	1024	读出数据或返回错误信息

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。

输出参数pOutInfo，当函数执行成功时，该输出参数为读出的社保应用基本信息各数据项，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。

示例：639900|111111198101011110|X00000019|639900D15600000500BF7C7A48FB4966|xxxx|00814E4323869715990 0BF7C7A|1.00|20101001|20201001|410100813475|终端设备号|。

当函数执行失败时，该输出参数为错误信息描述。

A.1.2.3.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.4 通用读卡接口

A.1.2.4.1 接口功能

读取卡内社保区的指定文件的内容。

接口内部执行流程为：

a) 尝试用 PSAM 卡的方式读取社保应用信息，成功时直接返回；

b) 如果开机认证时指定指定使用加密机，则继续使用加密机方式读取社保应用信息，并返回处理结果。

A.1.2.4.2 接口定义

long BJRS_ReadCard(int iType,int iAuthType, const char* pCardInfo, const char* pFileAddr, char* pOutInfo)。

A.1.2.4.3 参数说明.

参数说明见表A.23。

表A.23 参数说明

参数	输入/输出	类型	长度（十进制）	含义
iType	IN	整数	4	操作卡的类型
iAuthType	IN	整数	4	认证方式
pCardInfo	IN	字符串	128	卡基本信息
pFileAddr	IN	字符串	1024	文件名及数据项
pOutInfo	OUT	字符串	1024*20	读出数据或返回错误信息

输入参数iType，定义同上。

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。

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。

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。不同规范版本的卡内数据文件结构应符合行业主管部门对社会保障卡读写终端的相关要求。

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。例如读出2.0卡的学位信息2表示为：DF01EF15|40:2|$；读出国家/地区代码、学历、学位信息2表示为：DF01EF0A|37|$DF01EF15|2A|40:2|$。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。

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。例如读出国家/地区代码的输出参数表示为：DF01EF0A|CHN|$。当函数执行失败时，该输出参数为错误信息描述。

A.1.2.4.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.5 通用写卡接口

A.1.2.5.1 接口功能

更新社保区内指定文件的内容。

内部执行流程为：

a) 尝试使用 PSAM 卡认证方式写入信息，成功后直接返回结果；

b) 如果开机认证指定使用加密机，则继续使用加密机认证方式写入信息，返回处理结果。

A.1.2.5.2 接口定义

long BJRS_WriteCard(int iType, const char* pCardInfo,const char* pFileAddr, const char* pWriteData,char* pOutInfo)。

A.1.2.5.3 参数说明

参数说明见表A.24。

表A.24 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pCardInfo	IN	字符串	128	卡基本信息
pFileAddr	IN	字符串	1024	文件名及数据项
pWriteData	IN	字符串	1024*20	写入数据项信息
pOutInfo	OUT	字符串	1024	返回空字符串或错误信息

输入参数iType，定义同上。

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。

输入参数pFileAddr，该参数用于指定拟写入的文件和文件下的数据项。不同规范版本的卡内数据文件结构应符合行业主管部门对社会保障卡读写终端的相关要求。

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。例如写入2.0卡就业状态，表示为：DF01EF07|29|$；写入国家/地区代码，表示为： DF01EF0A|37|$。

当拟写入的文件为循环文件时，只需指定文件名，函数将新增记录；当拟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。

输入参数pWriteData，该参数用于传入拟写入的数据项信息。其格式与输入参数pFileAddr严格对应且分隔符完全一致。例如写入2.0卡就业状态为1，表示为：DF01EF07|1|$；写入国家/地区代码为CHN，表示为：DF01EF0A|CHN|$。

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。

A.1.2.5.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.6 PIN重置接口

A.1.2.6.1 接口功能

重置社保区的PIN码。

内部执行流程为：

a) 尝试使用 PSAM 认证重置，成功后直接返回结果；

b) 如果开机认证指定使用加密机，则继续使用加密机认证重置，返回处理结果。

A.1.2.6.2 接口定义

long BJRS_ReloadPIN(int iType, const char* pCardInfo, char* pOutInfo)。

A.1.2.6.3 参数说明

参数说明见表A.25。

表A.25 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pCardInfo	IN	字符串	128	卡基本信息
pOutInfo	OUT	字符串	512	返回空字符串或错误信息

输入参数iType，定义同上。

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。

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。

A.1.2.6.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.7 解锁接口

A.1.2.7.1 接口功能

社会保障应用PIN解锁。

内部执行流程为：

a) 尝试使用 PSAM 认证解锁 PIN 码，操作成功后直接结果；

b) 如果开机认证指定使用加密机，则继续使用加密机认证解锁 PIN 码，返回处理结果。

A.1.2.7.2 接口定义

long BJRS_UnblockPIN(int iType, const char* pCardInfo, char* pOutInfo)。

A.1.2.7.3 参数说明

参数说明见表A.26。

表A.26 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pCardInfo	IN	字符串	128	卡基本信息
pOutInfo	OUT	字符串	512	返回空字符串或错误信息

输入参数iType，定义同上。

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。

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。

A.1.2.7.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.8 消费交易接口

A.1.2.8.1 接口功能

执行社保卡消费交易并写入消费记录。

本接口只支持PSAM卡方式。

A.1.2.8.2 接口定义

long BJRS_DoDebit(int iType, const char* pCardInfo, const char* pPayInfo,char* pOutInfo)。

A.1.2.8.3 参数说明

参数说明见表A.27。

表A.27 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pCardInfo	IN	字符串	128	卡基本信息
pPayInfo	IN	字符串	512	消费信息
pOutInfo	OUT	字符串	512	返回交易验证数据或错误信息

输入参数iType，定义同上。

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。

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。

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。

A.1.2.8.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.9 终端注册接口

A.1.2.9.1 接口功能

将终端注册到后台系统。由于后台系统返回无数据，不需要进一步处理。

本接口内部执行流程为：

a) 查找终端设备，找到后读取终端唯一识别码；

b) 构造请求数据，加密并返回结果。

A.1.2.9.2 接口定义

long BJRS_TerminalRegisterAuthen(const char *pSysId, const char *pDeptId, int iDeviceAuth, char *pOutInfo)。

A.1.2.9.3 参数说明

参数说明见表A.28。

表A.28 参数说明

参数	输入/输出	类型	长度	含义
pSysId	IN	字符串	64	应用系统类型
pDeptId	IN	字符串	64	终端所属机构
iDeviceAuth	IN	整数	4	终端权限类型
pOutInfo	OUT	字符串	1024	输出结果信息或是错误信息

输入参数pSysId，应用系统代码，由后台系统分配。

输入参数pDeptId，终端所属的机构代码，由后台系统分配。

输入参数iDeviceAuth，终端权限类型，后台系统进行注册时的终端权限。

输出参数pOutInfo，当函数执行成功时，输出服务器返回信息。当函数执行失败时，该输出参数为错误信息描述。

A.1.2.9.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.10 终端注销接口

A.1.2.10.1 接口功能

注销终端设备和PSAM卡。注销后的设备不可再使用。

本接口内部执行流程为：

a) 查找终端设备并读取设置的唯一识别码；

b) 构造请求并进行加密，返回结果。

A.1.2.10.2 接口定义

long BJRS_TerminalCancelAuthen(const char *pSysId, const char *pDeptId,int iDeviceAuth,int iCancelType,char *pOutInfo)。

A.1.2.10.3 参数说明

参数说明见表A.29。

表A.29 参数说明

参数	输入/输出	类型	长度	含义
pSysId	IN	字符串	64	应用系统类型
pDeptId	IN	字符串	64	终端所属机构
iDeviceAuth	IN	整数	4	终端权限类型
iCancelType	IN	整数	4	注销原因
pOutInfo	OUT	字符串	1024	输出成功信息或错误信息

输入参数pSysId，应用系统代码，由后台系统分配。

输入参数pDeptId，终端所属的机构代码，由后台系统分配。

输入参数iDeviceAuth，终端权限类型，后台系统进行注册时的终端权限。

输入参数iCancelType，注销终端的原因，如PSAM丢失，代码由后台系统给出。

输出参数pOutInfo，当函数执行成功时，输出成功信息。当函数执行失败时，该输出参数为错误信息描述。

A.1.2.10.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.2.11 读电子社会保障卡接口

A.1.2.11.1 接口功能

对于带扫码功能的机具，可以使用此接口读读取电子社会保障卡。

本接口内部执行流程为：

a) 启动扫码功能，扫描用户的电子社会保障卡二维码；

b) 向电子社保服务请求卡信息，返回结果。

A.1.2.11.2 接口定义

long BJRS_ReadSCode(int iTimeout, char* pOutInfo)。

A.1.2.11.3 参数说明

参数说明见表A.30。

表A.30 参数说明

参数	输入/输出	类型	长度	含义
iTimeout	IN	整数	4	读电子社会保障卡超时时间
pOutInfo	OUT	字符串	1024	输出成功信息或错误信息

输入参数iTimeout，读电子社会保障卡超时时间。

输出参数pOutInfo，当函数执行成功时，输出电子社会保障卡信息。当函数执行失败时，该输出参数为错误信息描述。

A.1.2.11.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.3 通用接口（不区分中心端和非中心端）

A.1.3.1 读消费交易记录接口

A.1.3.1.1 接口功能

读取消费交易记录。本接口无需PSAM卡或是加密机参与。

A.1.3.1.2 接口定义

long BJRS_ReadDebitRecord(int iType, char* pOutInfo)。

A.1.3.1.3 参数说明

参数说明见表A.31。

表A.31 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pOutInfo	OUT	字符串	2048	返回交易记录或错误信息

输入参数iType，定义同上。

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。

A.1.3.1.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.3.2 PIN校验接口

A.1.3.2.1 接口功能

验证社会保障应用的PIN码。

该接口只使用社保卡，无需PSAM或加密机参与。

A.1.3.2.2 接口定义

long BJRS_VerifyPIN(int iType, char* pOutInfo)。

A.1.3.2.3 参数说明

参数说明见表A.32。

表A.32 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pOutInfo	OUT	字符串	512	返回空字符串或错误信息

输入参数iType，定义同上。

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。

A.1.3.2.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.3.3 PIN修改接口

A.1.3.3.1 接口功能

修改社会保障应用的PIN码。

该接口，只使用社保卡，无需PSAM或加密机参与。

A.1.3.3.2 接口定义

long BJRS_ChangePIN(int iType,char* pOutInfo)。

A.1.3.3.3 参数说明

参数说明见表A.33。

表A.33 参数说明

参数	输入/输出	类型	长度	含义
iType	IN	整数	4	操作卡的类型
pOutInfo	OUT	字符串	512	返回空字符串或错误信息

输入参数iType，定义同上。

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。

A.1.3.3.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.3.4 获取终端唯一识别码接口

A.1.3.4.1 接口功能

获取终端唯一识别码。本接口非社保卡应用，可直接调用。

终端唯一识别码为一组 32 位定长 ASCII 码字符串，由终端设备号（20 位）和 PSAM 卡终端机编号（12 位）两部分顺序组成。

A.1.3.4.2 接口定义

long BJRS_GetReaderUID(char *pOutInfo)。

A.1.3.4.3 参数说明

参数说明见表 A.34。

表A.34 参数说明

参数	输入/输出	类型	长度	含义
pOutInfo	OUT	字符串	512	返回终端唯一识别码或错误信息

输出参数pOutInfo，当函数执行成功时，该输出参数为终端唯一识别码。当函数执行失败时，该输出参数为错误信息描述。

A.1.3.4.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.3.5 卡签名接口

A.1.3.5.1 接口功能

终端对社保交易信息计算签名值。调用此接前需要先打开读写器，北京民生一卡通上电；此函数操作完成后，可以将卡下电，关闭读写器。

A.1.3.5.2 接口定义

```
int BjCardSign(
CardApdu CardApdu, void *userData,
unsigned char* MedicareData, int MedicareDataLen,
unsigned char* SignInfo, int* SignInfoLen,
```

unsigned char* CertId, unsigned char* ErrorInfo)。

A.1.3.5.3 输入参数

参数说明见表A.35。

表A.35 参数说明

参数	输入/输出	类型	长度	含义
CardApdu	IN	回调函数	-	回调函数
userData	IN	void*	-	用户自字义数据（传给回调函数）
MedicareData	IN	BYTE *	-	交易数据
MedicareDataLen	IN	int	4	交易数据长度
SignInfo	OUT	BYTE *	-	签名数据
SignInfoLen	IN/OUT	Int*	-	签名数据长度
CertId	OUT	BYTE *	-	证书 ID
ErrorInfo	OUT	BYTE *	-	返回信息

输入参数CardApdu，读卡器操作函数，签名函数通过调用此函数向社保卡发送指令，完成签名过程。此函数由调用方实现。int(*CardApdu)(void *userData, unsigned char *command, int commandLen, unsigned char *response, int *responseLen)。 *response, int *responseLen)。

a) userData:用户自定义数据；
b) command:卡指令数据；
c) commandLen:指令长度；
d) response:卡响应数据；
e) responseLen:卡响应数据长度。

返回： 函数返回卡指令的状态字，0x9000表示成功，其他为错误值，请参考卡指令手册。

输入参数userData，用户自定义数据，传给cardApdu函数的第一个参数。

输入参数MedicareData，待签名数据。

输入参数MedicareDataLen，待签名数据长度。

输出参数SignInfo，签名数据。

输出参数SignInfoLen，签名数据长度。

输出参数CertId，签名证书ID号。

输出参数ErrorInfo，操作成功时，输出为空字符串。操作失败时，输出错误信息。

A.1.3.5.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.3.6 获取DF0AEF0C医保信息

A.1.3.6.1 接口功能

读取社会保障应用本地扩展部分的DF0AEF0C文件中的医保信息。

A.1.3.6.2 接口定义

long BJRS_ReadYBInfo(int iType, const char* pCardInfo, char* pOutInfo)。

A.1.3.6.3 参数说明

参数说明见表A.36。

表A.36 参数说明

参数	输入/输出	类型	长度	含义
pOutInfo	OUT	字符串	512	返回终端唯一识别码或错误信息
pOutInfo	OUT	字符串	512	返回终端唯一识别码或错误信息

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。

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。

输出参数pOutInfo，当函数执行成功时，该输出参数为读出的DF0AEF0C文件相关信息。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。

A.1.3.6.4 返回值

操作成功时返回0，其他返回值为错误代码，见错误代码表A.37。

A.1.4 套件配置文件

用卡环境套件配置文件：

用卡环境的配置文件为BJRSCard.dat,文件的格式为windows配置文件ini的格式,以加密密文保存，解密后文件的内容如下：

[Global]

x-hw-id=bde9fda4-d09b-4165-824e-00f883acb22a

x-hw-appKey=7b751229f0f61ef8bf97112212d82ee78eafddda7d89ee926f81ca88fd8cf87a

default_host=http://172.26.59.45:80

[EquipmentCertification]

openAuth_Addr=http://172.26.59.45:80

deviceCancel_Addr=http://172.26.59.45:80

deviceRegister_Addr=http://172.26.59.45:80

[SymmetricKey]

in_Auth_Addr=http://172.26.59.45:80

ex_Auth_Addr=http://172.26.59.45:80

safe_msg_Addr=https://172.26.59.45:80

card_Auth_Addr=http://172.26.59.45:80。

A.1.4.1 Global结点

本结点下保存全局参数。

x-hw-id和x-hw-appKey: 为华为云的应用ID号。

default_host: 默认的服务主机，当没有在配置项中找到配置时使用此IP。

A.1.4.2 EquipmentCertification 结点

本结点保存终端认证配置和其它配置项。

openAuth_Addr： 开机认证地址配置项。

deviceRegister_Addr：设备注册配置项。

deviceCancel_Addr: 设备注销配置项。

A.1.4.3 SymmetricKey 结点

本结点保存加密机类配置项。

in_Auth_Addr： 内部认证配置项。

ex_Auth_Addr：外部认证配置项。

safe_msg_Addr：安全报文认证配置项。

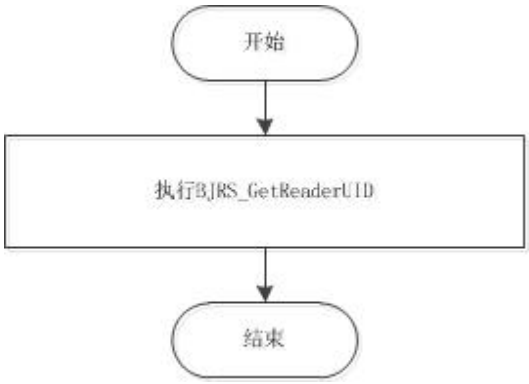
card_Auth_Addr：卡鉴权配置项。

A.1.5 通用操作套件部署

通用操作套件为BJRSCARD.dll。在相同的目录下，为各个终端设备厂商建立目录，SSCARDDRIVER_XX为各个终端设备厂商的SDK目录。

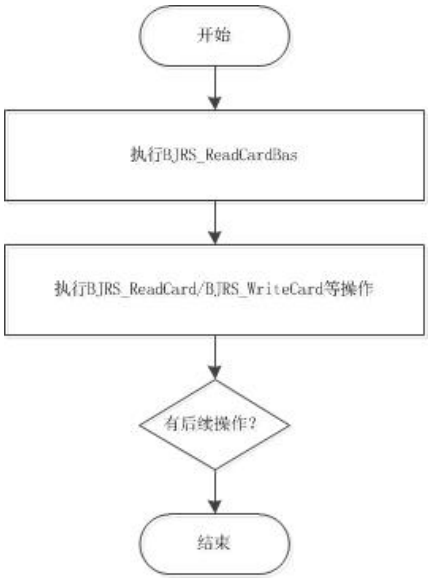
A.2 应用流程说明

读取设备终端号流程，见图A.9。



图A.9 读取设备终端号流程

北京民生一卡通操作流程，见图A.10。



图A.10 北京民生一卡通操作流程

A.3 错误代码表

通用错误信息应符合行业主管部门对社会保障卡读写终端的相关要求。

扩展错误信息详细内容见表A.37。

表A.37　错误代码表

错误值	说明
-101	设备未进行开机认证
-102	没有发现 SSCardDriver 库
-104	加密机内部认证失败
-105	加密机外部认证失败
-106	数据字段数量错误
-107	卡鉴权失败
-108	SSCardDriver 库没有加载
-109	安全报文认证失败
-110	设备的唯一识别码无效
-111	程序执行中出现异常
-112	开机认证失败
-113	注册认证失败
-114	注销认证失败

参 考 文 献

[1] GB 15093—2008 国徽
[2] GB/T 11643—1999 公民身份号码
[3] GB/T 11714—1997 全国组织机构代码编制规则
[4] 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
[5] GB/T 16649.5—2002 识别卡带触点的集成电路卡第 5 部分：应用标识符的国家编号体系和注册规程
[6] GB/T 2260—2007 中华人民共和国行政区划代码
[7] GB/T 2261.1—2003 人的性别代码
[8] GB/T 2261.2—2003 婚姻状况代码
[9] GB/T 26341-2010 残疾人残疾分类和分级标准
[10]GB/T 31022-2014 名片二维码通用技术规范
[11]GB/T 3304—1991 全国各民族名称的罗马字母拼写法和代码
[12]GB/T 4658—1984 文化程度代码
[13]GB/T 6565—2009 职业分类与代码
[14]GA 342.1—2001 户口类别代码
[15]GA 461—2004 居民身份证制证用数字相片技术要求
[16]GM/T 0003 SM2 椭圆曲线公钥密码算法
[17]GM/T 0004 SM3 密码杂凑算法
[18]GM/T 0016 智能密码钥匙密码应用接口规范
[19]GM/T AAAA SM2 密码算法使用规范
[20]ISO/IEC 14443 识别卡非接触式集成电路卡接近式卡
[21]ISO/IEC 7810—2003 识别卡物理特性
[22]ISO/IEC 7811-2—2001 卡识别记录技术第 2 部分
[23]ISO/1EC 7811-6 识别卡记录技术第 6 部分
[24]Q/T CDPF 0001—2012 中国残疾人联合会信息技术标准
[25]Q CUP 005-2019 银联卡卡片规范
[26]JT/T 978-2015 城市公共交通 IC 卡技术规范
[27]LD／T 33-2015 社会保障卡读写终端规范
[28]城市公共交通 IC 卡技术规范第 5 部分：非接触接口通讯
[29]DB11/T 159-2015 市政交通一卡通技术规范
[30]RFC 2279—1998 信息交换用汉字编码字符集基本集
[31]《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
[32]全国一体化在线政务服务平台电子证照-社会保障卡
[33]社会保障卡读写器名单