ICS 35.240.15
CCS L71

# 中华人民共和国国家标准

GB/T XXXXX.1—202X

# 中华人民共和国社会保障卡一卡通规范 第1部分：基础规范

Specifications for the social security card one-card-pass of the People's Republic of China - Part 1：Basic specifications

（征求意见稿）

（本草案完成时间：2023年11月04日）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

# 前　言

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

本文件是GB/T XXXXX《中华人民共和国社会保障卡一卡通规范》的第1部分。GB/T XXXXX已经发布了以下部分：

——第1部分：基础规范；

——第2部分：应用规范；

——第3部分：安全规范；

——第4部分：终端规范。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由人力资源和社会保障部提出并归口。

本文件起草单位：人力资源和社会保障部信息中心、XXX。

本文件主要起草人： XXX。

# 引　言

本文件通过规范社会保障卡一卡通应用实践，重点围绕社会保障卡一卡通业务需求，针对实体社会保障卡、电子社会保障卡及一卡通应用提出标准化解决方案，作为社会保障卡技术、质量管控、一卡通应用和管理要求的基础标准，对于实现社会保障卡“一卡多用、全国通用”、支撑政府公共服务一卡通、居民服务一卡通具有重要的基础指导作用并具有深远的战略意义。

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

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

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

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

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

# 中华人民共和国社会保障卡一卡通规范
# 第1部分：基础规范

## 1 范围

本文件规定了社会保障卡一卡通的体系架构、载体要求、服务渠道及基础支撑要求。

本文件适用于社会保障卡一卡通的设计、制造、发行、受理、使用及管理，以及社会保障卡一卡通相关系统的研发、集成、应用和维护等。

## 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 14916—2022，ISO/IEC 7810:2019，MOD）

GB 15093—2008 国徽

GB/T 15120.6 识别卡 记录技术 第6部分：磁条-高矫顽力（GB/T 15120.6—2012，ISO/IEC 7811-6:2008，MOD）

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

GB/T 16649.2 识别卡 带触点的集成电路卡 第2部分：触点的尺寸和位置（GB/T 16649.2－2006，ISO/IEC 7816-2:1999，IDT）

GB/T 16649.3 识别卡 带触点的集成电路卡 第3部分：电信号和传输协议（GB/T 16649.3－2006，ISO/IEC 7816-3:1997，IDT）

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

GB/T 17554.1 识别卡 测试方法 第1部分：一般特性测试（GB/T 17554.1－2006，ISO/IEC 10373-1:1998，MOD）

GB/T 25069 信息安全技术 术语

GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇（GB/T 29246－2017，ISO/IEC 27000:2016）

GB/T 41803.1 信息技术 社会保障卡生物特征识别应用系统 第1部分：通用要求

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

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

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

GA/T 461—2019 居民身份证制证用数字相片技术要求

LD/T 32—2015 社会保障卡规范

GB/T XXXXX.3—202X 中华人民共和国社会保障卡一卡通规范 第3部分 安全规范

GB/T XXXXX.4—202X 中华人民共和国社会保障卡一卡通规范 第4部分 终端规范

## 3 术语和定义

GB/T 16649.3、GB/T 16649.4、GB/T 25069、GB/T 29246、GB/T 41803.1、GB/T 42756.2、GB/T 42756.3、GB/T 42756.4界定的以及下列术语和定义适用于本文件。

3.1

**社会保障卡** social security card

中华人民共和国社会保障卡

由国务院人力资源和社会保障行政部门统一规划，各级人力资源和社会保障部门联合合作银行面向社会公众发行，是持卡人享受人力资源和社会保障权益及其他政府公共服务权益的服务载体。

注：社会保障卡包括实体社会保障卡和电子社会保障卡。两种形态的社会保障卡在业务经办中具有同等效力。实体社会保障卡是集成电路（IC）卡。

［来源：GB/T 41803.1—2022，3.1，有修改］

3.2

**电子社会保障卡** electronic social security card

电子社保卡

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，与实体社会保障卡一一对应、功能相通。

［来源：GB/T 41803.1—2022，3.2］

3.3

**社会保障卡一卡通** social security card one-card-pass

以社会保障卡为载体，推进跨业务、跨地区、跨层级、跨部门系统互通和服务融合，在政务服务、公共服务、社会治理等涉及居民服务的领域实现一卡多用、全国通用，打造共建共治共享的居民服务一卡通服务管理新模式。

3.4

**全国社会保障卡服务平台** national social security card service platform

全国社会保障卡线上身份认证与支付结算服务平台 national social security card online identity authentication and payment settlement service platform

国务院人力资源和社会保障行政部门统一建设、全国集中部署，实现全国电子社会保障卡的签发和应用，通过电子社会保障卡提供线上可信身份认证和支付服务，并依托部级持卡库实现电子社会保障卡与实体社会保障卡关联服务的平台。

［来源：GB/T 41803.1—2022，3.4，有修改］

3.5

**命令** command

终端向卡片发出的一条报文，该报文启动一个操作或请求一个应答。

3.6

**响应** response

卡片处理完成收到的命令报文后，返回给终端的报文。

3.7

**触点** contact

在集成电路卡（IC卡）和外部接口设备之间保持电流连续性的导电元件。

3.8

**报文** message

由终端向卡片或卡片向终端发出的，不含传输控制字符的字节串。

3.9

**数据元** data element

在接口处所看到的信息项，可以是名称、逻辑内容描述、格式和编码。

[来源：GB/T 16649.4—2010，3.12]

3.10

**应用** application

为满足特定功能所需的数据结构、数据元和程序模块。

[来源：GB/T 16649.4—2010，3.3]

3.11

**应用标识符** application identifier

标识应用的数据元（最多 16 字节）。

[来源：GB/T 16649.4—2010，3.5]

3.12

**应用模板** application template

与应用相关的数据对象的集合，其中的数据对象包括一个应用标识符数据对象。

[来源：GB/T 16649.4—2010，3.8]

3.13

**证书** certificate

由发行证书的认证中心使用其私钥对实体的公钥、身份信息以及其他相关信息进行签名，形成的不可伪造的数据。

[来源：GB/T 16649.4—2010，3.10]

3.14

**数字证书** 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。

[来源：GB/T 25069—2022，3.579]

3.15

**数据对象** data object

在接口处所看到的信息，由 tag 字段（必备）、长度字段（必备）和值字段（可选）串联组成。

[来源：GB/T 16649.4—2010，3.13]

3.16

**数字签名** digital signature

附加于数据串的数据，或对数据串的加密变换，它能够验证该数据串的原始性和完整性，保护数据串不被伪造。

[来源：GB/T 16649.4—2010，3.17]

3.17

**目录文件** directory file

可选的 EF，包含卡片支持的应用列表和可选相关数据元。

[来源：GB/T 16649.4—2010，3.18]

3.18

**基本文件** elementary file

共用同一文件标识符和同一安全属性的数据单元或记录或数据对象的集合。

[来源：GB/T 16649.4—2010，3.19]

3.19

**文件标识符** file identifier

用于文件访问的数据元（2 字节）。

[来源：GB/T 16649.4—2010，3.21]

3.20

**口令** password

应用可能需要的、用来鉴别卡的用户的数据。

[来源：GB/T 16649.4—2010，3.29]

3.21

**冷复位** cold reset

激活后的第一次复位。

[来源：GB/T 16649.3—2006，3.3.1]

3.22

**热复位** warm reset

非冷复位的所有其他复位。

[来源：GB/T 16649.3—2006，3.3.2]

## 4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

APP：应用程序（Application）

ACSE：非对称认证系统环境（Asymmetric Certification System Environment）

ADF：应用数据文件（Application Data File）

AEF：应用基本文件（Application Elementary File）

AID：应用标识符（Application Identifier）

APDU：应用协议数据单元（Application Protocol Data Unit）

ATR：复位应答（Answer To Reset）
an：字母数字型（alpha numeric）
BER：基本编码规则（Basic Encoding Rules）
B-TLV：符合基本编码规则的标签、长度、值（Basic encoding rules of Tag,Length,Value）
b：二进制（binary）
CIA：卡内医疗保险个人账户（Individual Account for Medical Treatment on Card）
CLA：命令报文的类别字节（Class Byte of the Command Message）
CLK：时钟（Clock）
$C_{IN}$：输入电容（Input Capacitance）
$C_{OUT}$：输出电容（Output Capacitance）
cn：压缩数字（compressed numeric）
DDF：目录定义文件（Directory Definition File）
DF：专用文件（Dedicated File）
EEPROM：电可擦可编程只读存储器（Electrically Erasable Programmable Read-Only Memory）
EF：基本文件（Elementary File）
FCI：文件控制信息（File Control Information）
HTML5：超文本标记语言 5.0（Hypertext Markup Language 5.0）
IC：集成电路（Integrated Circuit）
ICC：集成电路卡（Integrated Circuit（s）Card）
IFD：接口设备（Interface Device）
I/O：输入/输出（Input/Output）
$I_{IH}$：高电平输入电流（High Level Input Current）
$I_{IL}$：低电平输入电流（Low Level Input Current）
$I_{OH}$：高电平输出电流（High Level Output Current）
$I_{OL}$：低电平输出电流（Low Level Output Current）
INS：命令报文的指令字节（Instruction Byte of Command Message）
Lc：终端发出的命令数据的实际长度（exact Length of data sent by the TAL in a case 3 or 4 command）
Le：响应数据的最大期望长度（maximum Length of data expected by the TAL in response to a case 2 or 4 command）
M：必备型（Mandatory）
MAC：报文鉴别代码（Message Authentication Code）
O：可选型（Optional）
P1：参数 1（Parameter 1）
P2：参数 2（Parameter 2）
P3：参数 3（Parameter 3）
PICC：接近式卡 （Proximity ICC）
PIN：个人密码（Personal Identification Number）
PIX：专用应用标识符扩展码（Proprietary Application Identifier Extension）
PSAM：服务网点终端安全存取模块（Point of Service Secure Access Module）
PSE：支付系统环境（Payment System Environment）
PPSE：近距离支付系统环境（Proximity Payment Systems Environment）
PBOC：金融应用（People’s Bank of China Financial Application）
RFU：保留为将来使用（Reserved for Future Use）
RID：已注册的应用提供者标识符（Registered Application Provider Identifier）
RST：复位（Reset）

SFI：短文件标识符（Short File Identifier）
SPFP：统筹基金支付累计（Social-Pooling Fund Payment）
SPIP：个人自付累计（Accumulative Total of Individual Payment）
SSA：社会保障应用（Social Security Application）
SSC：社会保障卡（Social Security Card）
SSS：社会保障管理环境（Social Security System）
SSSE：社会保障系统环境（Social Security System Environment）
SW1：状态码 1（Status Word One）
SW2：状态码 2（Status Word Two）
TAC：交易验证码（Transaction Authorization Cryptogram）
TLV：标签、长度、值（Tag、Length、Value）
$t_F$：信号幅度从 90%下降到 10%的时间（Fall time between 90% and 10% of signal amplitude）
$t_R$：信号幅度从 10%上升到 90%的时间（Rise time between 10% and 90% of signal amplitude）
VCC：电源电压（Volt Current Condense）
VPP：编程电压（Programming Voltage）
$V_{IH}$：高电平输入电压（High Level Input Voltage）
$V_{IL}$：低电平输入电压（Low Level Input Voltage）
$V_{OH}$：高电平输出电压（High Level Output Voltage）
$V_{OL}$：低电平输出电压（Low Level Output Voltage）
‘0’-‘9’ ‘A’-‘F’：十六进制数字

## 5 社会保障卡一卡通体系架构

社会保障卡一卡通体系，是指围绕社会保障卡的制作发行、应用推广、服务管理、安全保障、运维支撑等环节而建设形成的生态系统。该体系具有开放、协同、安全等特点，以实体社会保障卡和电子社会保障卡为载体，以全国社会保障卡服务平台、社会保障卡管理信息系统、社会保障卡密钥管理系统、电子认证系统、社会保障卡持卡人员基础信息库作为支撑系统，构建全国及地方社会保障卡一卡通应用平台，对接全国一体化政务服务平台、有关部门政务服务平台及应用机构，整合各类数据资源，多渠道、全方位输出社会保障卡一卡通办事凭证、支付结算、待遇发放等应用能力和服务能力，实现政务服务、人社服务、就医购药、交通出行、旅游观光、文化体验、惠民惠农以及其他业务领域“一卡通用”。

社会保障卡一卡通体系的整体架构如图1所示。

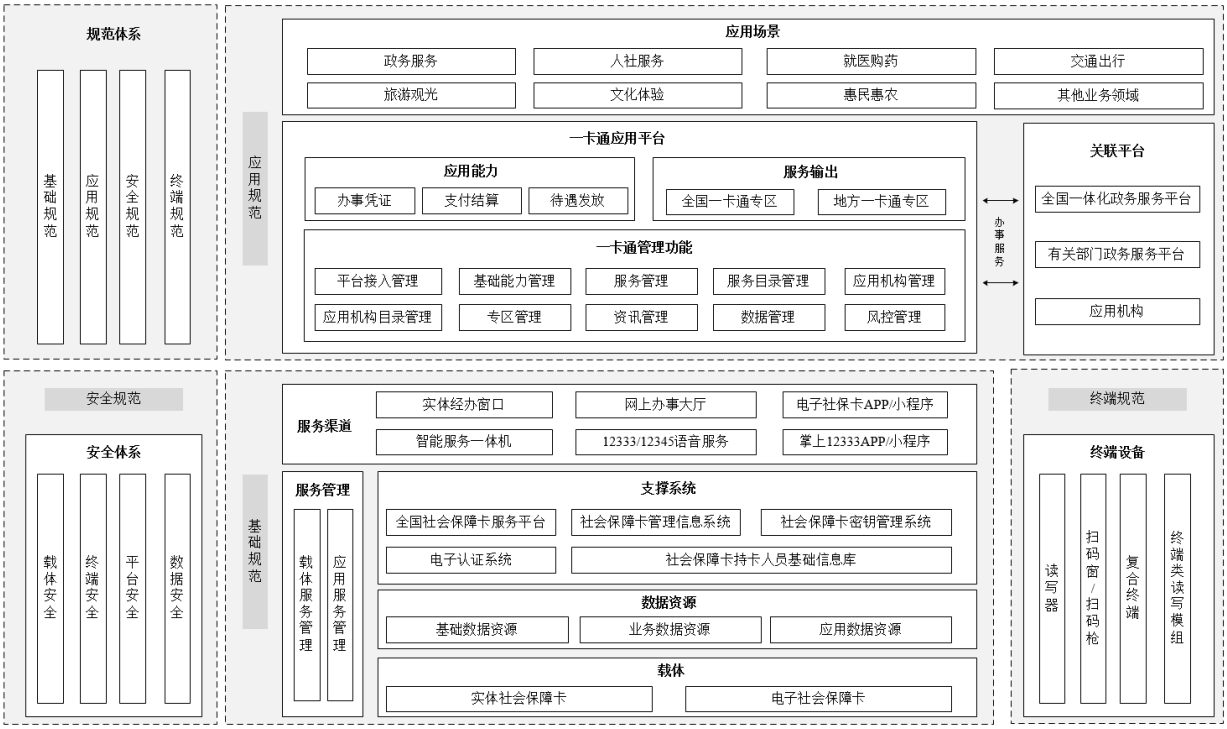



图1　社会保障卡一卡通体系架构

## 6　社会保障卡一卡通载体要求

### 6.1　社会保障卡一卡通载体形态

社会保障卡一卡通载体，包括实体社会保障卡和电子社会保障卡两种形态。

实体社会保障卡卡号规则和电子社会保障卡卡号规则应分别符合附录A和附录B的规定。

### 6.2　基本样式

#### 6.2.1　实体社会保障卡样式

##### 6.2.1.1　卡片外形和尺寸

实体社会保障卡的外形为圆角矩形，外形和尺寸分别见图2和表1。

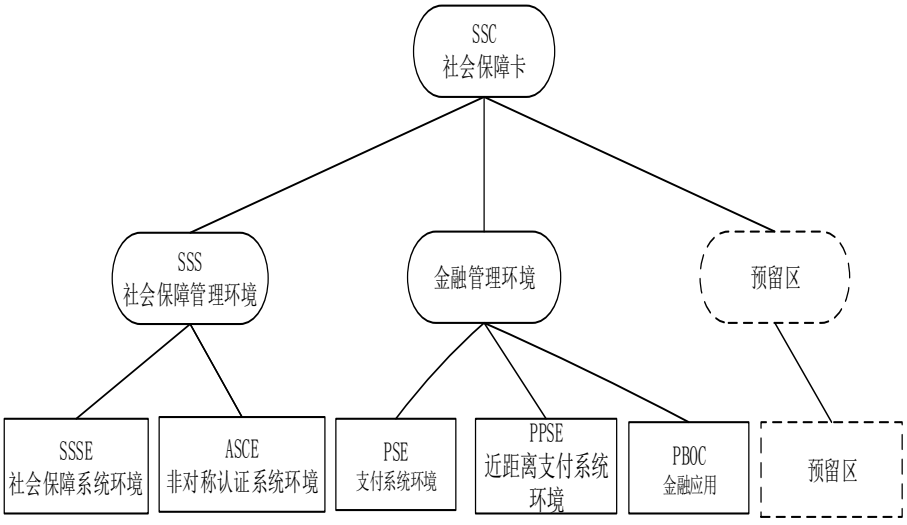


图2　卡片外形

表1　卡片尺寸

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

6.2.1.2　卡片正面

6.2.1.2.1　卡片正面布局及要素

实体社会保障卡的卡片正面应包括以下要素：国徽、卡名（中华人民共和国社会保障卡）、隐蔽磁条（可选）。卡片正面布局及要素分别见图 3 和表 2。

单位为毫米


图3　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<br>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 | ±0.25mm |
| 下边沿到卡片下边沿的距离 | 27.00mm | ±0.25mm |
| 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 | ±0.25mm |

| | | |
|---|---|---|
| 下边沿到卡片下边沿的距离 | 20.00mm | ±0.25mm |
| “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 | ±0.25mm |
| 下边沿到卡片下边沿的距离 | 10.00mm | ±0.25mm |
| 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 GB/T 15120.6 的相关规定 | |

#### 6.2.1.2.2 卡片正面色彩样图

卡片正面颜色色差允许公差见表 3，正面彩色样图如图 4 所示。

表3 卡片正面颜色

| 颜色区域 | 国徽专色红 | 卡面左上蓝 | 卡面左下蓝 | 字体黑 |
|---|---|---|---|---|
| 色差允许公差$\Delta E^*_{ab}$ | ≤5.00 | ≤4.00 | ≤4.00 | ≤4.00 |


图4 卡片正面彩色样图

#### 6.2.1.3 卡片背面

##### 6.2.1.3.1 卡片背面布局及要素

实体社会保障卡的卡片背面应包括以下要素：人社机构标识区、银行LOGO标识区、银行卡组织标识区、持卡人相片、持卡人个人信息、地方人力资源社会保障机构定义区、IC芯片、插卡方向箭头标识、人力资源社会保障机构印章、银行卡卡号、银行定义区、非接触标识区、ATM标识和箭头、服务电话、制卡厂商代码区、网纹、水印区。卡片背面布局及要素分别见图5和表4。卡片背面示例样图如图6所示。卡片背面底层网纹样图如图7所示。卡片背面水印图案可由地方人力资源社会保障机构自定义。持卡人相片应符合GA/T 461—2019的规定。

地方人力资源社会保障机构可根据应用拓展需要，在“地方人力资源社会保障机构定义区”、“银行定义区”增加其他要素，报人力资源和社会保障部审批。

单位为毫米

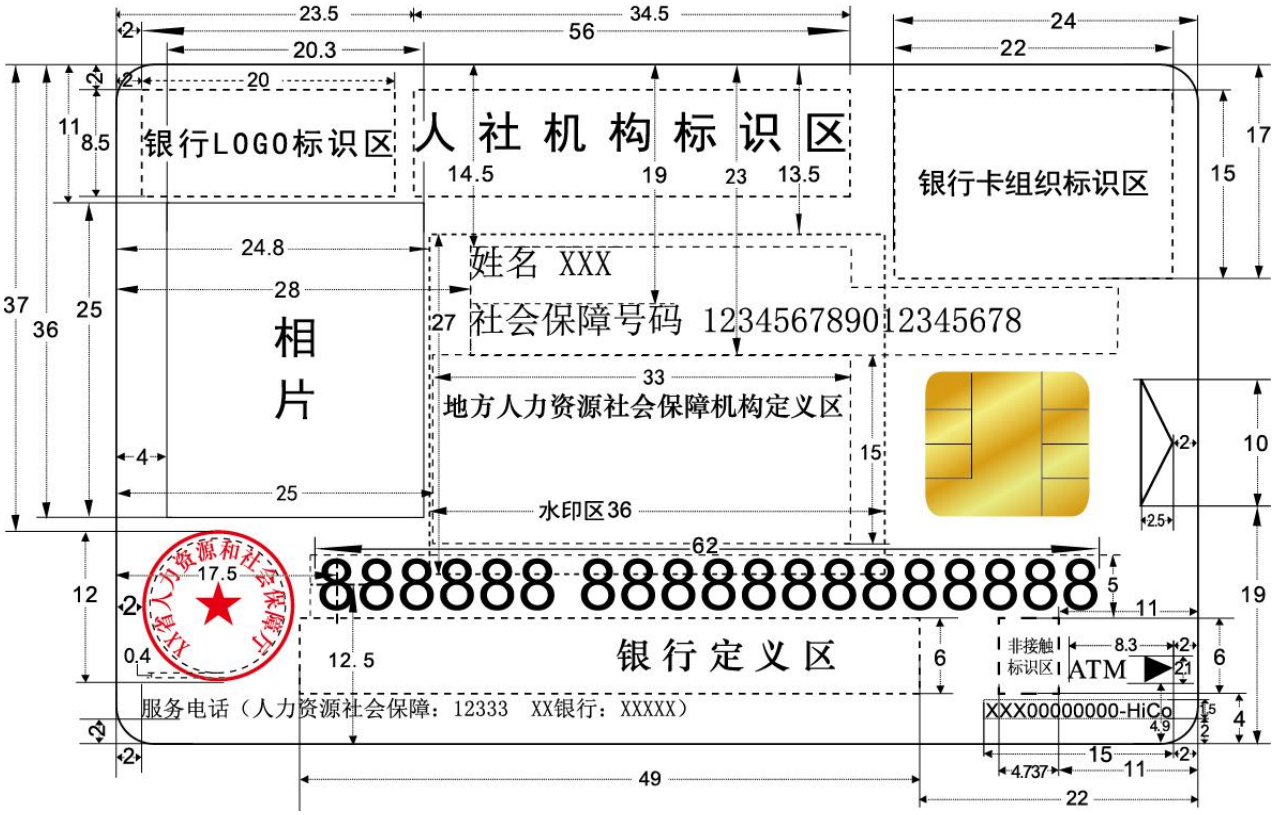



图5 卡片背面布局

表4 卡片背面要素

| 参数 | 规格及要求 | 公差 |
|---|---|---|
| 银行 LOGO 标识区 | | |
| 区域的宽度 | 20.00mm | ±0.10mm |
| 区域的高度 | 8.50mm | ±0.10mm |
| 区域左边沿到卡片左边沿的距离 | 2.00mm | ±0.30mm |
| 区域上边沿到卡片上边沿的距离 | 2.00mm | ±0.30mm |
| 人社机构标识区 | | |
| 区域的宽度 | 34.50mm | ±0.10mm |
| 区域的高度 | 8.50mm | ±0.10mm |
| 区域左边沿到卡片左边沿的距离 | 23.50mm | ±0.30mm |
| 区域上边沿到卡片上边沿的距离 | 2.00mm | ±0.30mm |
| 人社机构标识区字体大小（双语双行） | 汉语黑体 5.5 磅 | 少数民族语言无要求 |
| 人社机构标识区字体大小（非双语单、双行） | 黑体 7 磅 | — |
| 银行卡组织标识区 | | |
| 区域的宽度 | 22.00mm | ±0.10mm |
| 区域的高度 | 15.00mm | ±0.10mm |
| 区域左边沿到卡片右边沿的距离 | 24.00mm | ±0.30mm |
| 区域下边沿到卡片上边沿的距离 | 17.00mm | ±0.30mm |

| 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 | — |
| “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 |
| 人力资源社会保障机构印章 | | |
| 印章的直径 | 12.00mm | ±0.10mm |
| 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左边沿的距离 | 17.50mm | ±0.20mm |
| “卡号”左边首位的中心到卡片下边沿的距离 | 12.50mm | ±0.20mm |
| 银行定义区 | | |
| 区域的宽度 | 49.00mm | ±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 | 22.00mm | ±0.30mm |
| 区域下边沿到卡片下边沿的距离 | 4.00mm | ±0.30mm |
| 非接触标识区 | | |
| 区域的宽度 | 4.737mm | ±0.01mm |
| 区域的高度 | 6.00mm | ±0.01mm |
| 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 |
| “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 | |


图6　卡片背面示例样图

图7　卡片背面底层网纹样图

### 6.2.2　电子社会保障卡样式

#### 6.2.2.1　卡面样式

##### 6.2.2.1.1　电子社会保障卡布局

电子社会保障卡的卡面通过电子设备展现，外形为圆角矩形，卡面背景颜色为浅蓝渐变纹理图，布局如图8所示。展现图片尺寸为682（宽）px× 370（高）px，实际应用尺寸以界面适配为准。


图8　电子社会保障卡布局

##### 6.2.2.1.2　电子社会保障卡要素

电子社会保障卡的社会保障卡服务渠道标识、“电子社保卡”、“姓名”、“社会保障号码”、“人力资源和社会保障部”等为静态元素，姓名、社会保障号码、持卡人相片、银行图标、银行名称、银行卡卡号、预留区、显示相片图标等为动态元素。具体要求见表5。

表5　电子社会保障卡要素

| 参数 | | 规格及要求 | 补充说明 |
|---|---|---|---|
| 卡面 | 宽度 | 682px | |
| | 高度 | 370px | |
| 社会保障卡服务渠道标识 | 图标的宽度 | 74px | |
| | 图标的高度 | 74px | |
| | 左侧边缘距离电子社会保障卡卡面左侧边缘 | 142px | |
| | 上侧边缘距离电子社会保障卡卡面上侧边缘 | 48px | |
| | 右侧边缘距离电子社保卡字样左侧边缘 | 36px | |
| 电子社会保障卡持卡人相片 | 相片的宽度 | 112px | |
| | 相片的高度 | 160px | |
| | 右侧边缘距离电子社会保障卡卡面右侧边缘 | 38px | |
| | 上侧边缘距离电子社会保障卡卡面上侧边缘 | 110px | |
| “电子社保卡”5 个字 | 字体的宽度 | 262px | |

| | | | |
|---|---|---|---|
| | 字体的高度 | 38px | |
| | 右侧边缘距离电子社会保障卡卡面右侧边缘 | 168px | |
| | 上侧边缘距离电子社会保障卡卡面上侧边缘 | 65px | |
| “人力资源和社会保障部”10个字 | 字体的宽度 | 262px | |
| | 字体的高度 | 40px | |
| | 右侧边缘距离电子社会保障卡卡面右侧边缘 | 0px | |
| | 下侧边缘距离电子社会保障卡卡面下侧边缘 | 28px | |
| 姓名 | 左侧边缘距离电子社会保障卡卡面左侧边缘 | 38px | |
| | 上侧边缘距离电子社会保障卡卡面上侧边缘 | 140px | |
| 社会保障号码 | 社会保障号码与“社会保障号码”的距离 | 10px | 社会保障号码与“社会保障号码”平齐 |
| | 左侧边缘距离电子社会保障卡卡面左侧边缘 | 38px | |
| 银行卡卡号 | 银行卡卡号与银行名称的距离 | 8px | 银行卡卡号与银行名称平齐 |
| 银行图标 | 图标的宽度 | 32px | |
| | 图标的高度 | 32px | |
| | 左侧边缘距离电子社会保障卡卡面左侧边缘 | 38px | |
| | 下侧边缘距离电子社会保障卡卡面下侧 | 92px | |
| | 以透明背景图片显示 | / | |
| 预留区（为可选项） | 区域的宽度 | / | 预留区域各省市卡面自定制命名，宽度自适应 |
| | 区域的高度 | 38px | |
| | 左侧边缘距离电子社会保障卡卡面左侧边缘 | 0px | |
| | 上侧边缘距离电子社会保障卡卡面上侧 | 0px | |
| 显示相片图标 | 图标的宽度 | 38px | |
| | 图标的高度 | 26px | |
| | 右侧边缘距离电子社会保障卡卡面右侧边缘 | 24px | |
| | 上侧边缘距离电子社会保障卡卡面上侧边缘 | 20px | |

#### 6.2.2.2 一维码样式

电子社会保障卡的一维码，用于办事凭证、支付结算等。样式如图9所示，采用code128编码方式，尺寸为544（宽）px×136（高）px。

图9　一维码样式

#### 6.2.2.3　二维码样式

电子社会保障卡的二维码，用于办事凭证、支付结算等。当用于支付结算时，应符合人民银行相关支付业务规范的要求。样式如图10所示，尺寸为280（宽）px×280（高）px。

图10　二维码样式

电子社会保障卡二维码的中心为社会保障卡服务渠道标识，样式如图 11 所示。尺寸为 80（宽）px×80（高）px。


图11　社会保障卡服务渠道标识样式

电子社会保障卡二维码要素。具体要求见表6。

表6　电子社会保障卡二维码样式要素

| 参数 | | 规格要求 | 补充说明 |
|---|---|---|---|
| 电子社会保障卡二维码 | 宽度 | 280px | |
| | 长度 | 280px | |
| 社会保障卡服务渠道标识 | 宽度 | 80px | |
| | 长度 | 80px | |

## 6.3　物理特性

### 6.3.1　总则

下列特性仅适用于实体社会保障卡。实体社会保障卡属于 ID-1 型卡，除符合本文件规定的物理特性要求外，还应符合 GB/T 14916 和 GB/T 16649 规定的其他物理特性要求，如触点尺寸、翘曲、抗热度、耐化学性、抗静电、阻光度、紫外线以及触点的机械强度等。

### 6.3.2　温、湿度条件下的卡尺寸稳定性和翘曲

社会保障卡在工作的温湿度条件下的卡尺寸稳定性和翘曲应符合 GB/T 14916 的规定。

### 6.3.3　剥离强度

测量剥离角度为 90°，取样宽 10.00mm，社会保障卡表层剥离强度的最低值应满足：

a)　相片区域表层剥离强度值≥3.5 N/cm；

b)　其余区域表层剥离强度值≥5N/cm。

### 6.3.4　耐湿性

在 40℃温度，相对湿度达到 95%的环境中放置 48h，卡片功能应正常，并符合 GB/T 14916 中规定的翘曲值要求。

### 6.3.5　模块与卡体粘合强度

IC 模块与卡体粘合力≥90N。针对 8 触点模块，曝露芯片背面部分，固定于点压装置上，芯片位置下部悬空，将探针对准芯片背面的曝露部分，以不大于 30mm/min 的速度下压芯片直至芯片完全脱落，下压过程中施加的压力≥90N。

### 6.3.6　外观质量

社会保障卡的表面不应有油污、异物等杂物。距离 30cm 目测：

a)　卡片表面上长度＞0.3mm 的尘点、墨点、气泡、杂质等异常斑点或异物不应超过 6 个；

b)　卡片表面不应出现内容错误、图案错误、位置错误、漏印刷问题；

c)　卡片表面不应出现明显色斑、条纹、图案、字符有明显重影、毛刺、缺损问题。

### 6.3.7　印刷牢度

用胶轮对社会保障卡的印刷表面进行 500 次磨损测试后，对卡片颜色、图案、字符进行目测，无明显掉色和模糊不清的现象。

### 6.3.8　插拔寿命

社会保障卡与终端间的插拔次数应不少于 10 万次，插拔后卡片功能正常。

## 6.4　电气特性及协议

### 6.4.1 总则

下列特性仅适用于实体社会保障卡。实体社会保障卡除符合本文件规定的电特性要求外，还应符合GB/T 16649 规定的其他电特性要求。

### 6.4.2 接触电特性及协议

#### 6.4.2.1 电特性

本节描述了实体社会保障卡的电特性要求。

a) 操作条件

本文件定义了两类操作条件，接口设备应通过触点 VCC 向卡片提供下列正常的电源电压：

——在 A 类条件下为 5V；

——在 B 类条件下为 3V。

卡片应至少同时支持 A 类和 B 类。

b) 电压和电流值

1) 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：

——高电平状态，如果卡片和接口设备都处于接收模式，或者由发送方强制此状态；

——低电平状态，由发送方强制此状态。

当线路的两端都处于接收模式时，该线路应处于高电平状态。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，但不应损坏卡片。操作过程中，接口设备和卡片不应同时处于传输模式。具体见表 7。

**表7 正常操作条件下 I/O 的电特性**

| 符号 | 条件 | 最小值 | 最大值 | 单位 |
|---|---|---|---|---|
| $V_{IH}$<br>$I_{IH}$ | <br>$V_{IH}$ | 0.7×VCC<br>-300 | VCC<br>+20 | V<br>μA |
| $V_{IL}$<br>$I_{IL}$ | <br>$V_{IL}$ | 0<br>-1000 | 0.15×VCC<br>+20 | V<br>μA |
| $V_{OH}$<br>$I_{OH}$ | VCC 接外部上拉电阻 20KΩ<br>$V_{OH}$ | 0.7×VCC | VCC<br>+20 | V<br>μA |
| $V_{OL}$ | $I_{OL}$ = 1mA [a] | 0 | 0.15×VCC | V |
| tR 和 tF | $C_{IN}$=30pF,$C_{OUT}$=30pF | - | 1.0 | μs |
| 注：I/O上的电压应维持在-0.3V~VCC+0.3V。 | | | | |
| a 接口设备的实现不应要求卡片的电流下降大于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。接口设备应向卡片提供一个阻抗，以便卡片能够保持所定义范围内的输出电压。

2) 时钟

该触点用来向卡片提供时钟信号。时钟信号频率的实际值表示为 *f*。

时钟信号的占空因数应处于其稳定运行周期的 40%~60%之间。本文件不使用频率切换。

当时钟频率处于 1MHz~5MHz（A 类）或 1MHz~4MHz（B 类）之间时，卡片应能正常工作。具体见表 8。

注：在卡片操作过程中，频率值将由终端维持在复位应答期间所用频率的±1%之内。

表8 正常操作条件下 CLK 的电特性

| 符号 | 条件 | 最小值 | 最大值 | 单位 |
|---|---|---|---|---|
| $V_{IH}$ | | 0.7×VCC | VCC | V |
| $I_{IH}$ | $V_{IH}$ | -20 | +150 | μA |
| $V_{IL}$ | | 0 | 0.5 | V |
| $I_{IL}$ | $V_{IL}$ | -200 | +20 | μA |
| tR 和 tF | $C_{IN}$=30pF | - | 9%的时钟周期 | |
| 注：CLK上的电压应维持在-0.3V至~VCC+0.3V之间。 | | | | |

3) 编程电压（VPP）

卡片不需要编程电压 VPP。

4) 触点电阻

在整个生命周期内，卡片触点的电阻（在清洁的卡片和清洁的标准接口设备触点间测量时）应小于 500mΩ。

注：一个标准接口设备触点可以看作是在 5.00μm 镍表面上的 1.25μm 的镀金触点。

### 6.4.2.2 操作过程

卡片的操作过程包括以下步骤：

——将卡片插入接口设备，使二者的触点相接并激活；

——卡片和接口设备之间信息交换总是由卡片对冷复位的应答来启动；

——进行交易处理操作；

——释放触点并从接口设备中取出卡片。

各步骤具体描述如下：

a) 激活

在卡片插入接口设备但触点还没有进行物理接触时，终端应确保其所有触点处于低电平状态（$V_{OL}$ 和 VCC 小于或等于 0.4V）。如果卡片在接口设备中位于插/拔方向正确位置的偏差在±0.5mm 范围内， 接口设备应能探测到卡片的存在。当所有触点进行物理接触后，触点才应被激活。终端应按下列顺序来激活触点：

1) 终端应在整个激活时序中保持 RST 为低电平状态；

2) 触点物理接触之后，应在 I/O 或 CLK 激活之前，根据接口设备选定的操作条件给 VCC 加电；

3) 终端在确认已稳定提供规定的电压和电流后，将 I/O 置于接收模式并提供终端技术要求中规定的合适、稳定的时钟。终端将其 I/O 置于接收模式可以在时钟启动之前，也可以在此之后，但最迟不得超过时钟启动后的 200 个时钟周期。

注：根据设计，终端可以给 VCC 一个足够的等待时间使之稳定，待稳定后再通过测量或其他方式检查它的状态。终端将其 I/O 置为接收模式后，其 I/O 状态取决于卡片上 I/O 的状态。

上述的触点激活过程完成后，卡片准备好后按规定的时序进行冷复位。

b) 信息交换

如果卡片支持操作条件类别，则卡片应应答任何复位请求。在任何复位应答完成后，接口设备可以启动一次卡片的热复位。对热复位的应答可以不同于前一次的应答，或者是冷复位的，或者是热复位的。卡片利用激活的低电平复位信号，采用异步方式进行复位应答。

c) 交易执行

实体社会保障卡中应用的选择以及执行一次交易操作所需的卡片与终端之间的信息交换，应

符合 LD/T 32.7—2015 的规定。

作为卡片操作的最后一步，根据交易的正常或异常结束（包括在卡片操作过程中将卡片从接口设备中拔出），终端将把接口设备触点置为静止状态，如图 12 所示。过程如下：

1) 终端将通过把 RST 置为低电平状态来启动释放时序；
2) 在置 RST 为低电平状态之后且 VCC 断电之前，终端将 CLK （除非 CLK 已停止在低电平状态） 和 I/O 设定为低电平状态；
3) 在置 RST、CLK 和 I/O 为低电平状态之后且卡片触点与接口设备触点物理分离之前，终端将切断 VCC 电源，此时的 VCC 应小于或等于 0.4V。

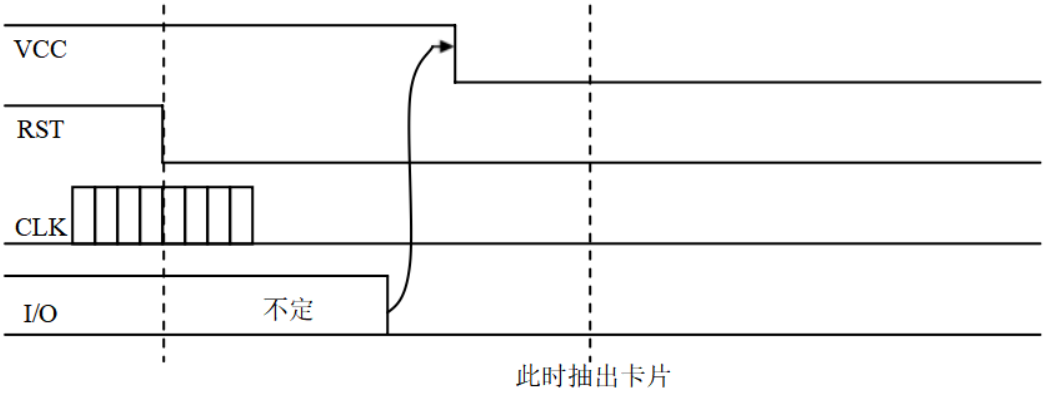



**图12　触点释放时序**

d) 交易过程的异常结束

在交易过程中，如果卡片以 1m/s 的速度过早地从终端中拔出，终端应能感觉到卡片相对于接口设备触点的移动，并在相对位移达到 1mm 之前，将接口设备的所有触点置为静止状态。在这种情况下，卡片的电气或机械特性应不受损坏。

注：对于滑触式结构的接口设备，终端有可能感觉到卡片触点与接口设备触点之间的相对位移。此处不对能否感知到相对运动作强制性要求，但在卡片和接口设备触点脱离之前应能够将其置为静止状态。

### 6.4.3　非接电特性及协议

#### 6.4.3.1　非接电特性

实体社会保障卡的非接电特性要求如下。

a) 交变磁场

在表 9 给出平均磁场强度的磁场内，在任意方向上暴露后，PICC 应能继续正常工作。平均时间为 6min，磁场的最大磁场强度值被限制在平均值的 33 倍以内。

**表9　磁场强度与频率**

| 频率范围（MHz） | 平均磁场强度（A/m） | 平均时间（min） |
|---|---|---|
| 0.3～3.0 | 1.63 | 6 |
| 3.0～30 | 4.89/*f* | 6 |
| 30～300 | 0.163 | 6 |
| 注：　*f* 为电场频率。 | | |

另外，在平均磁场强度值为 10A/m（rms）、13.56MHz 频率的磁场中持续暴露后，PICC 应能继续正常工作。平均时间为 30s，磁场的最大值被限制在 12A/m（rms）。

b) 交变电场

在表 10 给出平均电场强度的电场内，在任意方向上暴露后，PICC 应能继续正常工作。平均时间为 6min，电场的最大值被限制在平均值的 33 倍以内。

表10　电场强度与频率

| 频率范围（MHz） | 平均磁场强度（A/m） | 平均时间（min） |
|---|---|---|
| 0.3～3.0 | 614 | 6 |
| 3.0～30 | 1842/*f* | 6 |
| 30～300 | 61.4 | 6 |
| 注：　*f* 为电场频率。 | | |

c）　静电

按照 GB/T 17554.1 中描述的测试方法（其中测试电压为 6kV）测试后，PICC 应能继续正常工作。

d）　静态磁场

在 640kA/m 的静态磁场内暴露后，PICC 应能继续正常工作。

警告：磁条上的数据内容可能被这样的磁场擦去。

e）　工作温度

在 0℃~50℃的环境温度范围内，PICC 应能正常工作。

#### 6.4.3.2　射频功率和信号接口

实体社会保障卡的初始对话、功率传输、信号接口应符合 GB/T 42756.2 的规定，负载调试幅度应至少为 30/H1.2 mV（峰值）。

PICC 耦合天线可以为任何形状和位置，但应按照图 13 所示区域围绕，阴影部分是直径为 5.0mm 的区域。

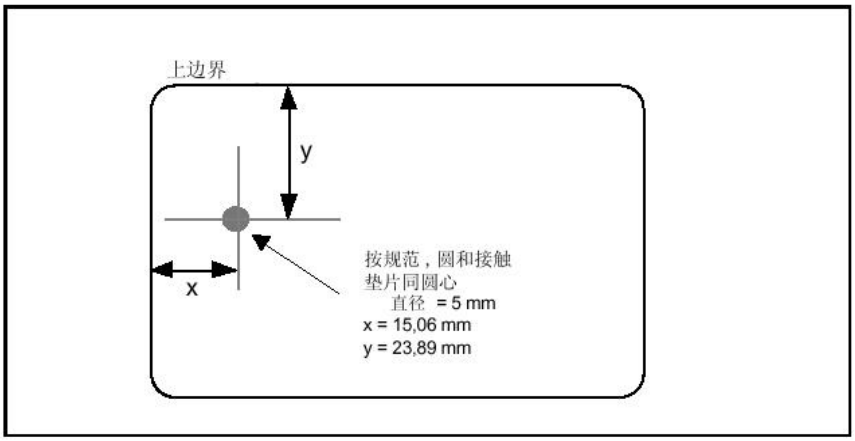



图13　PICC 最小耦合区

### 6.5　基本数据结构

#### 6.5.1　实体社会保障卡文件系统

##### 6.5.1.1　文件结构

###### 6.5.1.1.1　通则

应用相关的文件呈一种可通过目录访问的树形结构。树的根和每一分支都是一个ADF。一个ADF是一个或多个相关数据文件的入口点，一个ADF及其相关数据文件处于树的同一分支上。

#### 6.5.1.1.2 应用数据文件（ADF）

ADF是一个只包含其FCI中纯数据对象的文件，ADF的树形结构应能将数据文件与应用联系起来，应能确保应用之间的独立性，并可通过应用选择实现对其逻辑结构的访问。ADF文件控制信息见表11。

**表11 ADF 文件控制信息**

| 标志 | 值 | 存在方式 |
|---|---|---|
| ‘6F’ | FCI 模板 | M |
| ‘84’ | DF 名 | M |

#### 6.5.1.1.3 应用基本文件（AEF）

一个 AEF 包含有一个或多个原始 BER-TLV 数据对象（记录结构的 AEF），或一个非结构化的纯数据元（透明结构的 AEF）。在选择了某一应用后，AEF 既能通过其文件标识符进行查询，也可以通过其 SFI 进行查询。

记录结构的 AEF 具有如下属性：

——记录的长度是固定的或是可变的；

——记录的组织结构是线形结构或循环结构。

#### 6.5.1.1.4 文件结构中文件的映像

包含一个 FCI 的 DF 被映像为 ADF，可以通过它来访问 EF 和 DF。

包含一组应用数据元的 EF 被映像为 AEF。

#### 6.5.1.1.5 应用目录结构

应用的各个具体应用对应的 EF 和 DF 分别构成一个树状结构的各个分支。每个 DF 是其下属的 EF 的入口点。

为便于发卡方和应用提供者根据实际情况确定应用是否在卡片中存在，应用采用何种密码算法，以及是否允许在卡片中扩展其他应用，卡片可以选择支持用于 SSSE 和 ACSE 应用列表的目录结构，各应用由发卡方通过目录选择。

目录结构包括一个社会保障系统目录文件和一些由 DDF 引用的附加目录。

目录结构采用以其 AID 的方式进入一个应用，以 AID 的前 N 个字节作为 DF 名的方式进入一组应用。

在选择应用环境的响应报文中对目录文件进行编码。

目录文件是一个记录结构的 AEF，具体编码见 6.5.1.4.3。

#### 6.5.1.1.6 卡内结构示例

实体社会保障卡的文件结构如图 14 所示，其中，社会保障管理环境（SSS）、社会保障系统环境（SSSE）和非对称认证系统环境（ACSE）为社会保障应用专用，金融管理环境、支付系统环境（PSE）、近距离支付系统环境（PPSE）和金融应用（PBOC）为金融应用专用，其他为预留区，地方人力资源社会保障机构可根据应用拓展需要，按照相关行业或地方标准要求进行加载，并向人力资源和社会保障部报备。

按照文件结构定义，卡片应用数据空间应不小于 48KB。

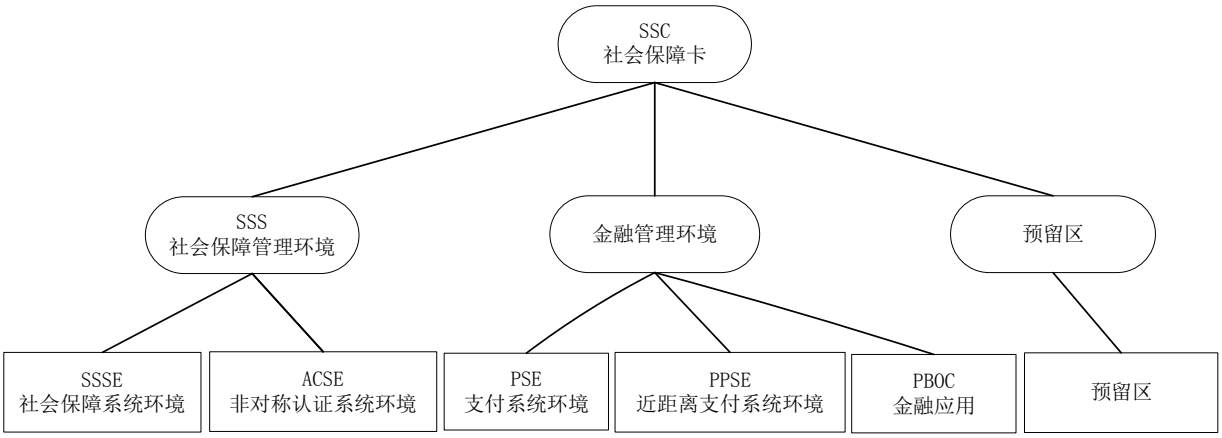



**图14　社会保障卡文件结构**

SSSE 的文件结构示意图如图 15 所示。

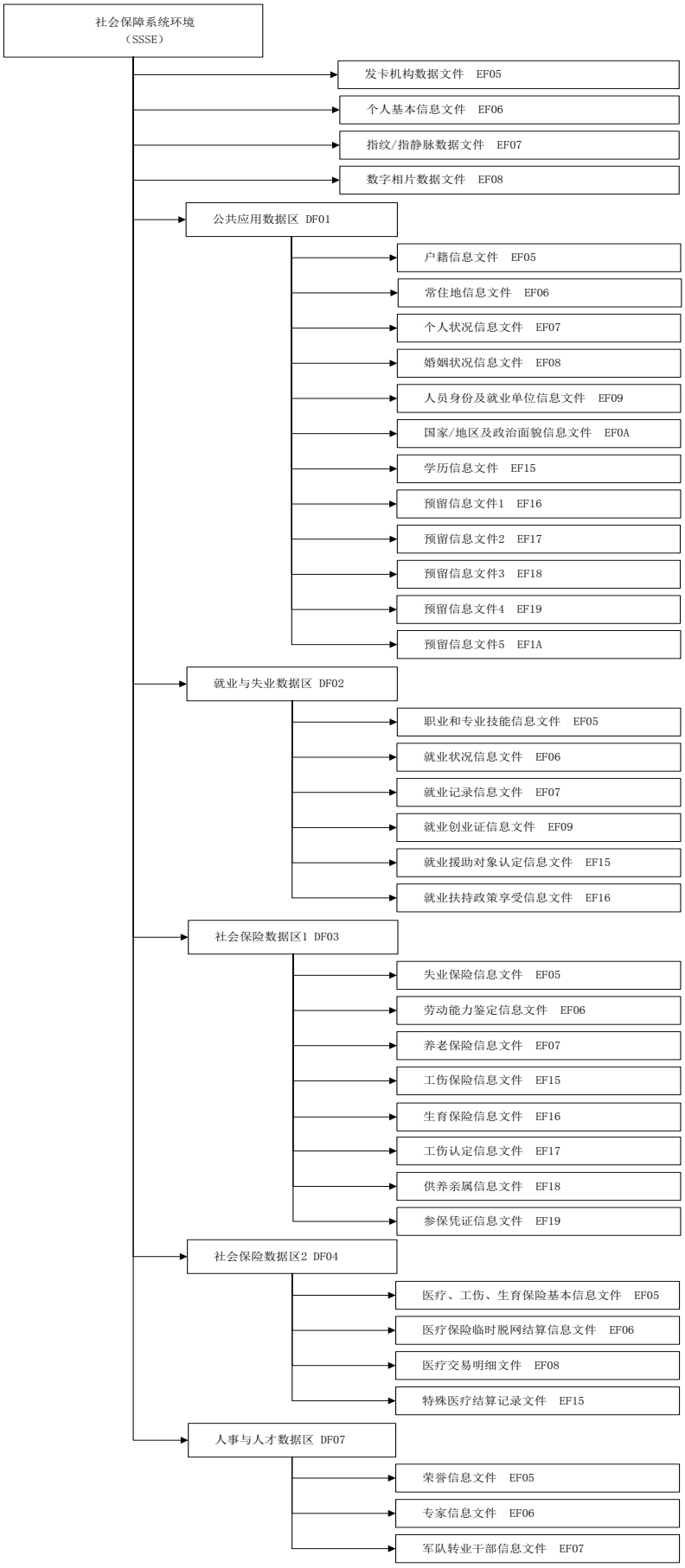



图15 SSSE 文件结构示意图

ACSE 的文件结构示意图如图 16 所示。

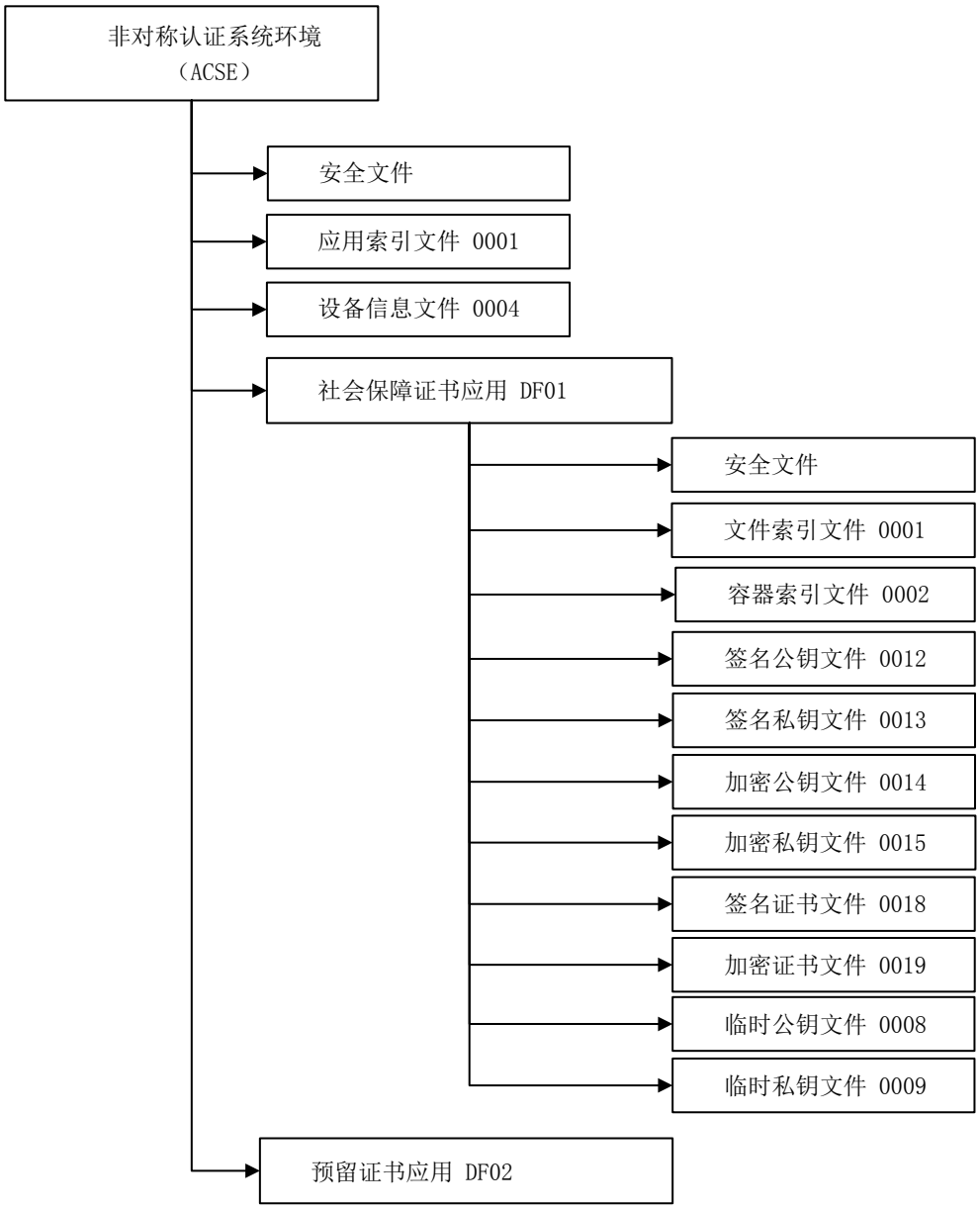



**图16　ACSE 文件结构示意图**

#### 6.5.1.1.7　应用数据项

数据项的标志、长度均以十六进制值表示。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定的长度时，对格式为cn的数据项左靠齐并且右补十六进制‘F’，对格式为an的数据项左靠齐并且右补十六进制‘0’，使数据项的长度达到规定的长度。具体数据项格式应附录D的规定。

### 6.5.1.2　文件引用

按照文件类型，文件可以通过文件名、文件标识符、短文件标识符进行引用：

a)　通过文件名

ADF 可通过其 DF 名查询，DF 名对应其 AID，每个 DF 名在给定的卡片中应唯一。社会保障应用各个具体的 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，应采用应用标识符维护单位所规定的应用标签，并通过应用标签选择该应用；

b) 通过文件标识符

ADF、AEF 可通过其文件标识符查询，每个 ADF 的文件标识符在所属环境中应唯一，每个 AEF 的文件标识符在所属的 ADF 中应唯一；

c) 通过短文件标识符

对给定应用中的 AEF，可以通过 SFI（5bits，取值范围为 1~30）查询。SFI 的编码在每个用到它的命令中描述。在一个给定的应用中 SFI 应唯一，专用 SFI 的使用由应用决定。

#### 6.5.1.3 记录引用

在每个记录结构的 EF 内，每个记录可以通过记录标识符和/或记录号来引用。记录标识符和记录号的值为 1~254 的整数，编码为‘01’~‘FE’。值‘00’被保留用于特殊用途，值‘FF’为 RFU，具体如下：

——通过记录标识符引用，每个记录标识符由应用来提供；

——通过记录号引用，在每个记录结构的 EF 内，记录号是唯一的和顺序的。

具体引用规则应符合 GB/T 16649.4 的规定。

#### 6.5.1.4 应用选择

##### 6.5.1.4.1 通则

从卡片和终端两个角度描述了应用选择的过程。从卡片的角度描述了该过程所需的卡数据和文件的逻辑结构，从终端的角度描述了适应这种卡逻辑结构的终端逻辑。

终端的应用选择过程，根据定义的协议使用卡数据来决定选择何种应用进行交易，其过程分两个步骤：

——建立卡片与终端两者共同支持的应用列表；

——在上述应用列表中选择一个将要运行的应用。

##### 6.5.1.4.2 应用标识符（AID）

所有应用都有唯一的 AID，AID 的结构包含两个部分：

a) RID（长度为 5 字节），它是应用提供者唯一标识；

b) 可选的 PIX 域，由应用提供者定义，最长 11 字节。

SSSE、ACSE 的相关 AID 分别见表 12 和表 13。

表12 SSSE 的相关应用标识符

| DDF | ADF | 应用标识符（AID）内容 | 应用标识符（AID） |
|---|---|---|---|
| SSSE | - | sx1.sh.社会保障 | 7378312E73682EC9E7BBE1B1A3D5CF |
| | 公共应用 | 公共应用数据区 | D15600000500 |
| | 就业与失业 | 就业与失业数据区 | D15600000501 |
| | 社会保险 1 | 社会保险数据区 1 | D15600000502 |
| | 社会保险 2 | 社会保险数据区 2 | D15600000503 |
| | 人事与人才 | 人事与人才数据区 | D15600000504 |

表13 ACSE 的相关应用标识符

| DDF | ADF | 应用标识符（AID）内容 | 应用标识符（AID） |
|---|---|---|---|

| | | | |
|---|---|---|---|
| ACSE | - | PKI.社会保障 | 504B492EC9E7BBE1B1A3D5CF |
| | 社会保障证书应用 | SS.CERT.ADF1 | 53532E434552542E41444631 |
| | 预留证书应用 | RFU.CERT.ADF2 | 5246552E434552542E41444632 |

#### 6.5.1.4.3 目录编码

目录文件是一个线性文件，用 5~15 的 SFI 标识。该目录文件附属于 DDF，目录文件的 SFI 包含在 DDF 文件控制信息中。目录文件可以按附录 C 中所定义的“READ RECORD”命令进行读取。目录文件中一个记录可以包含几个入口地址，但一个入口地址不能跨越多个记录存储。目录文件的每一个入口地址都是一个应用模板（标记‘61’），它应包含表 14 和表 15 所示信息。

**表14 DDF 目录入口地址格式**

| 标志 | 长度 | 值 | 存在状态 |
|---|---|---|---|
| ‘4F’ | 5~16 | DDF 名称 | M |

**表15 ADF 目录入口地址格式**

| 标志 | 长度 | 值 | 存在状态 |
|---|---|---|---|
| ‘4F’ | 5~16 | ADF 名称（AID） | M |
| ‘50’ | 1~16 | 应用标签 | M |

#### 6.5.1.4.4 选择方式及实现

终端应采用 SELECT 命令通过 AID 方式选择应用，其 AID 分别见表 11 和表 12。

终端将卡片返回的密码算法标识与终端支持的密码算法标识列表进行比较，如果卡片支持的密码算法标识不在终端所支持的密码算法标识列表中，则终端与卡片不匹配。

终端中应存放其所支持的应用及其对应的 AID 和密码算法标识列表。下面描述了两种应用选择过程：一个适用于支持较少数量应用的终端，另一个适用于支持较多数量应用的终端。

a) 直接选择应用

如果一个终端支持的应用较少，该终端可以简单地使用 SELECT 命令轮流选择每个应用。如果 SELECT 命令执行成功（回送 SW1-SW2=‘9000’），则该终端将它所支持的 AID 与被选择文件的 FCI 中的文件名进行比较，通过比较的结果来查证卡片是否支持此应用。如果二者相匹配，卡片支持该应用；如果返回的文件名比 AID 长而 AID 与返回文件名的起始部分相符，终端则重新发送 SELECT 命令并再次对长文件名的 AID 进行验证；如果卡片回送 SW1-SW2≠‘9000’，或者即使卡片回送 SW1-SW2= ‘9000’，而 AID 与文件名不相符且与文件名起始部分也不相符，则证明卡片不支持此应用。

一旦终端支持的应用都被选择出来，则卡片和终端都支持的应用列表就可以确定。然后终端可以选择指定的应用来运行。这一选择过程见“c)选择应用并执行操作”。

b) 目录的使用

如果终端支持较多的应用，可以通过使用 SSSE 或 ACSE 目录来确定卡片所支持的应用。应保证 SSSE 或 ACSE 目录的结构设计正确，以便终端可以按照本部分描述的过程正确地选择应用。终端正确使用目录文件的步骤如下：

1） 终端进入 SSSE 或 ACSE 后，如果目录文件不存在，转至步骤 5）；如果目录文件存在，则进入目录文件；

2） 终端从第一条记录开始，连续读目录文件中的所有记录，直到卡片回送 SW1-SW2=‘6A83’，表示所需记录序号已不存在。在执行 READ RECORD 命令查找第一条记录时，如果卡片回送 SW1-SW2=‘6A83’，则表示目录为空，转至下面步骤 5；

3） 如果目录中某个 ADF 名与终端支持的一个应用名相符，则将该应用列入最终应用选择的“候选名单”中；

4） 如果目录文件中出现一个指向 DDF 的入口地址，且该 DDF 的名称至少与一个终端所支持的 AID 的前几位匹配（例如：一个名为 D156123456 的 DDF 可与一个名为 D15612345678 的 AID 匹配），则终端选择该 DDF。使用所选 DDF 的 FCI 中的 SFI 读出目录并按步骤 3 处理，之后终端继续回到上一个目录处理；

5） 当终端处理完 SSSE 或 ACSE 目录的列表后，所有能够按此方式找到的 ADF 已经确定，查找完毕；

6） 终端也可采用其他方式寻找卡内其他专用应用（例如用 AID 找出本地特有的或非社会保障应用的专用选择方式）。

c) 选择应用并执行操作

当终端确定了卡片与终端相互支持的应用列表之后，下一步选取某个应用进行操作。可通过如下方法实现：

1） 如果没有互相支持的应用，则交易终止；

2） 如果只有一个相互支持的应用，终端应向持卡人提出确认请求，如持卡人同意，则终端选择该应用；否则终端终止该交易；

3） 建议显示应用列表请持卡人选择。显示应以终端的应用优先顺序为准；如果终端没有指定优先顺序，则按照应用在卡片中出现的顺序为准。

一旦终端或持卡人确定了待执行的应用，则该应用被选中，终端发出一个 SELECT 命令进行应用选择。如果命令回送的 SW1-SW2≠‘9000’，则将此应用从候选列表中删除，之后再将删除后的列表显示给持卡人，重新进行应用选择。

#### 6.5.1.5 应用命令

##### 6.5.1.5.1 命令格式

命令格式应符合 GB/T 16649.4 的规定。

命令通用状态返回码应符合 GB/T 16649.4 的规定，命令专有状态返回码见表 16。

**表16 命令专有状态返回码**

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘69’ | ‘01’ | 命令不接受（无效状态） |
| ‘93’ | ‘02’ | MAC 无效 |
| ‘93’ | ‘03’ | 应用被永久锁定 |
| ‘94’ | ‘01’ | 金额不足 |
| ‘94’ | ‘02’ | 交易计数器达到最大值 |
| ‘94’ | ‘03’ | 密钥索引不支持 |
| ‘94’ | ‘06’ | 所需 MAC 不可用 |

##### 6.5.1.5.2 命令定义

社会保障应用和非对称认证应用的命令集如下（具体的命令定义符合附录 C 的规定）：

a) 社会保障应用命令集

1） APPLICATION BLOCK（应用锁定）；
2） CARD BLOCK（卡片锁定）；
3） CHANGE PIN（修改个人密码）；
4） EXTERNAL AUTHENTICATION（外部鉴别）；
5） GET CHALLENGE（获取随机数）；
6） GET RESPONSE（获取响应）；
7） INTERNAL AUTHENTICATION（内部鉴别）；
8） PIN CHANGE/UNBLOCK（个人密码重置/解锁）；
9） READ BINARY（读取二进制数据）；
10）READ RECORD（读取记录内容）；
11）SELECT（选择文件）；
12）UPDATE BINARY（更新二进制数据）；
13）UPDATE RECORD（更新记录内容）；
14）VERIFY（校验个人密码）；
15）CREDIT FOR LOAD（账户划入）；
16）DEBIT FOR PURCHASE（医疗费用结算）；
17）GET BALANCE（读取卡内基本医疗保险个人账户余额/年度个人自付累计金额/年度统筹基金支付累计金额）；
18）GET TRANSACTION PROOF（读取交易认证码）；
19）INITIALIZE FOR LOAD（账户划入初始化）；
20）INITIALIZE FOR PURCHASE（医疗费用结算初始化）；
21）UPDATE STARTING DAY（修改年度起始日期）；
22）GET STARTING DAY （读取年度起始日期）。

b) 非对称认证应用命令集

1） CHANGE DEV KEY（修改设备密钥）；
2） CHANGE PIN/ RELOAD PIN（修改或重置）；
3） EXTERNAL AUTHENTICATE（外部鉴权）；
4） GET CHALLENGE（获取随机数）；
5） GET RESPONSE（获取响应）；
6） READ BINARY（读取二进制内容）；
7） READ RECORD（读取记录内容）；
8） SELECT FILE（选择文件）；
9） UPDATE BINARY（更新二进制内容）；
10）UPDATE RECORD（更新记录内容）；
11）VERIFY PIN（校验）；
12）GENERATE KEY PAIR（生成 SM2 密钥对）；
13）GET PUBLIC KEY（导出公钥）；

14）STORE PKI KEY（导入 SM2 密钥对）；

15）PUBLIC KEY OPERATION（加密/验签）；

16）PRIVATE KEY OPERATION（解密/签名）；

17）GENERATE ENVELOP（生成数字信封）；

18）OPEN ENVELOP（打开数字信封）；

19）CIPHER DATA（数据加解密）；

20）HASH OPERATION（哈希运算）。

### 6.5.2 电子社会保障卡二维码数据结构

#### 6.5.2.1 数据结构

电子社会保障卡二维码码值由以下三部分构成：渠道编号段（10 位）、随机因子段（10 位）、校验位段（2 位）。码值总长度 22 位，数据结构如图 17 所示。

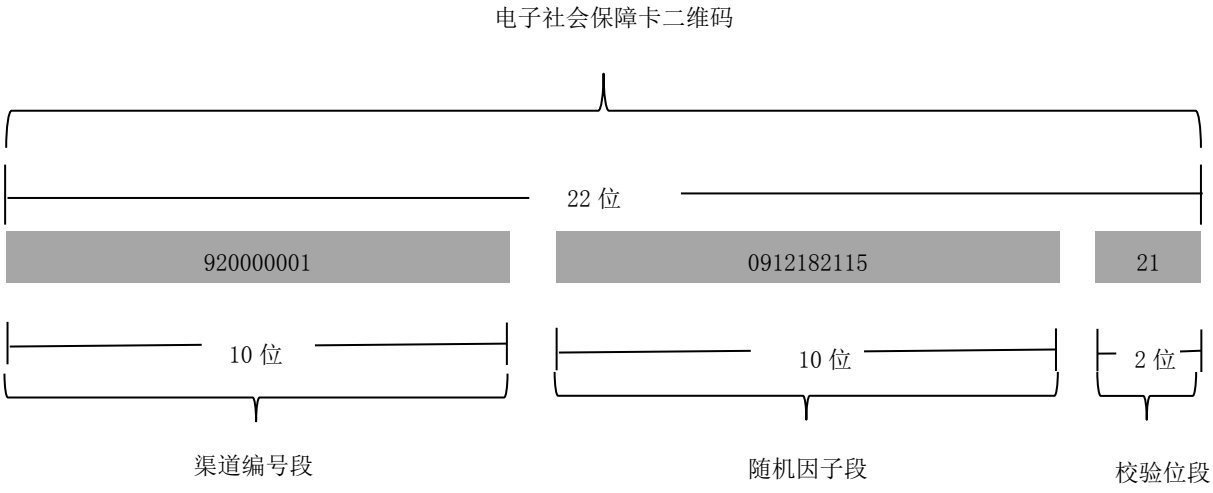



图17 电子社会保障卡二维码数据结构

#### 6.5.2.2 渠道编号段

渠道编号段用于区分电子社会保障卡签发渠道，由 10 位阿拉伯数字构成，编码规则如下：

a) 地方类渠道

1) 前 6 位为行政区划代码；
后 4 位为序号，顺序分配（0001—9999）。

b) 全国类渠道

1) 中央政府及政府各部门渠道
000001+4 位序号（0001—9999）；

2) 银行类渠道
91***+后 5 位，***为银行行别代码，具体如下：
——针对全国性商业银行，后 5 位为序号（00001—99999）；
——针对地方性商业银行，后 5 位中的前 2 位为行政区划代码的前 2 位（代表省份），后 3 位为序号（001—999）。

c) 第三方渠道（除地方类渠道、全国类渠道之外的合作运营渠道）
9200+6 位序号（000001—999999）（序号由人力资源和社会保障部统一赋码）。

#### 6.5.2.3 随机因子段

随机因子段用于确保电子社会保障卡二维码的唯一性，由 10 位阿拉伯数字构成，在 10min 内保证绝对唯一。

#### 6.5.2.4 校验位段

校验位段用于保证电子社会保障卡二维码的安全性，基于随机因子段和电子社会保障卡持卡人密码因子按照特定的离散函数和逻辑算法生成。

## 7 一卡通服务渠道

### 7.1 服务渠道类型

一卡通服务渠道是指接入一卡通应用平台，面向社会公众提供一卡通应用服务的实体。

一卡通服务渠道按照应用方式划分，可分为线上和线下两类渠道，见表17。

**表17 服务渠道类型**

| 渠道类型 | 渠道举例 |
| --- | --- |
| 线上 | 政务服务网上办事大厅、政务服务 APP、电子社保卡 APP/小程序、掌上 12333APP/小程序、12333/12345 语音服务、服务银行 APP、智慧城市 APP、各类公众号/小程序等 |
| 线下 | 政府部门、人社部门、银行及其他社会协作单位开办的服务窗口、综合柜员窗口、智能服务一体机终端以及各类应用场景下的受理终端等 |

### 7.2 服务渠道要求

各服务渠道应遵循以下要求：

a) 服务窗口：

——服务窗口应设置社会保障卡业务专属柜台，配置读写终端设备，投放即时制卡终端等设备，负责设备日常维护；

——服务窗口应投入人员配备，组建专业服务团队，能够提供社会保障卡日常服务；

——服务窗口应具备健全的业务经办和处理规范、完整的服务质量追溯机制及应急预案，持续优化业务流程、改善服务质量，对持卡人及相关单位提出的服务意见和建议做到专人负责、快速响应、快速解决。

b) 终端设备：

——终端设备包括读卡终端、即时制卡终端、自助服务终端、扫码终端等；

——终端设备应符合 GB/T XXXXX.4—202X 的要求，且通过检测机构的检测；

——终端设备的品牌、型号、使用地点、使用模式、有效性、配置时间、配置数量等信息应做好登记。

c) APP/小程序及网页服务：

——各类 APP/小程序及网页服务应遵循安全性、完整性和公益性的要求；

——电子社保卡 APP/小程序的接入、签发应用等管理应按照全国社会保障卡服务平台统一标准要求开展；

——应建立规范安全的服务通道，提供保障签发和应用的基础服务能力，确保对外提供电子社会保障卡标准服务，并根据自身服务场景，拓展服务能力。

d) 语音服务：

——各类语音服务为社会保障卡持卡人提供咨询服务

——12333/12345 语音服务内容应包括社会保障卡业务知识库，涵盖社会保障卡发行应用服务，同时提供人社业务咨询服务。

### 7.3 服务渠道标识

支持受理社会保障卡的各类一卡通服务网点，应使用统一的服务渠道标识，如图 11 所示。

## 8 社会保障卡一卡通基础支撑要求

### 8.1 通用要求

社会保障卡一卡通应用体系的基础支撑主要功能如下：

a) 卡唯一性控制。通过卡数据入库校验控制，确保全国范围一人一卡；

b) 卡有效性鉴权。在社会保障卡使用过程中，对卡片的有效性进行鉴别，对卡片的归属地等进行判断，面向各类业务提供用卡鉴权服务；

c) 基础信息共享。为各级各类社会保障卡一卡通应用系统提供人员、卡基础信息校验，实现基础信息的共享，支持基础信息的比对，保证基础信息的一致性；

d) 基础信息交换。通过联动机制实现与各社会保障卡一卡通应用系统的数据联动，实现信息在各社会保障卡一卡通应用系统之间的交换，促进业务协同。

### 8.2 系统功能

#### 8.2.1 通则

社会保障卡一卡通应用体系的基础支撑系统主要包含全国社会保障卡服务平台、社会保障卡管理信息系统、社会保障卡密钥管理系统、电子认证系统、社会保障卡持卡人员基础信息库。

a) 全国社会保障卡服务平台，统一对外提供线上服务和应用，能够支撑实现电子社会保障卡签发服务和服务渠道管理、社会保障卡一卡通应用管理等功能；

b) 社会保障卡管理信息系统，负责支撑社会保障卡的申领、制作、发放、挂失、补换、注销等服务；

c) 社会保障卡密钥管理系统，为实现发卡及跨业务、跨地区、跨部门用卡提供密钥支持和认证服务；

d) 电子认证系统，为人力资源社会保障各类业务系统提供身份认证、授权管理和责任认定等安全服务；

e) 社会保障卡持卡人员基础信息库，负责支撑卡唯一性控制、卡有效性鉴权、人员基础信息共享、人员基本业务状态信息交换服务。

#### 8.2.2 全国社会保障卡服务平台

全国社会保障卡服务平台，是面向电子社会保障卡全口径业务服务、高度复用的能力平台，为所有服务渠道客户端提供面向互联网的业务服务。

全国社会保障卡服务平台统一对电子社会保障卡签发和服务渠道进行管理，基本功能如下：

a) 统一管理电子社会保障卡的各服务渠道（各服务银行小程序、APP 等）；

b) 统一管理电子社会保障卡签发、二维码展码和验码、“扫一扫”认证、密码认证、人脸认证、密码修改和重置、解除关联等能力；

c) 统一管理全国服务、本地服务、社会保障卡一卡通服务专区等应用服务；

d) 统一管理数据统计、业务办理、文档共享等日常运维服务。

#### 8.2.3 社会保障卡管理信息系统

社会保障卡管理信息系统应具备如下功能：

a) 基本信息管理：实现社会保障卡申领人员信息采集、服务网点机构信息管理、系统操作人员管理、PSAM 卡管理；
b) 申领管理：负责社会保障卡的申领受理和信息核验；
c) 生产发放管理：实现社会保障卡的下单、卡片制作、物流配送、卡片领取管理等；
d) 安全管理：实现持卡人员信息的修改，卡片的挂失和解挂、密码修改和重置以及卡片注销等；
e) 补换卡管理：实现社会保障卡的补卡和换卡。

### 8.2.4 社会保障卡密钥管理系统

社会保障卡密钥管理系统，是依托部、省两级社会保障卡密钥体系构建的社会保障卡密钥支持和认证服务系统，为实现发卡及跨业务、跨地区、跨部门用卡提供技术支撑。

社会保障卡密钥管理系统应具备以下功能：

a) 终端管理：实现社会保障卡终端信息采集、登记、黑白名单管理；
b) 密钥权限管理：对已采集的终端，通过其所属机构和使用场景分配密钥使用权限；
c) 密钥支持接口：为制卡和即时发卡提供密钥安全接口；
d) 认证接口：为社会保障卡一卡通业务场景提供安全认证接口。

### 8.2.5 电子认证系统

电子认证系统，是基于密码技术实现证书生命周期管理，以及安全认证、加密保护、签名验证等证书应用功能的安全系统，支撑各类业务系统实现以身份认证、授权管理和责任认定为主要内容的各类安全应用。

电子认证系统主要包括证书认证设施和密钥管理设施，以及相配套的基础安全防护设施，如图18所示。其中：

a) 证书认证设施，包括证书签发管理系统、证书注册管理系统和证书查验服务系统；
   1) 证书签发管理系统是对生命周期内的数字证书进行全过程管理的安全系统，采用双证书（签名证书和加密证书）机制，使用 SM2 算法签发各类数字证书；
   2) 证书注册管理系统负责持卡人的证书申请、身份审核和证书下载；
   3) 证书查验服务系统主要负责为持卡人和应用系统提供证书状态查询服务。
b) 密钥管理设施，主要指密钥管理系统。密钥管理系统基于公开密钥密码技术，负责为证书认证设施提供 SM2 加密证书密钥对等密钥服务，并对生命周期内的 SM2 加密证书密钥对进行全过程管理；
c) 基础安全防护设施，主要包括防病毒系统、防火墙、漏洞扫描、入侵检测等安全防护设备，是保证电子认证系统安全可靠运行的必要条件。

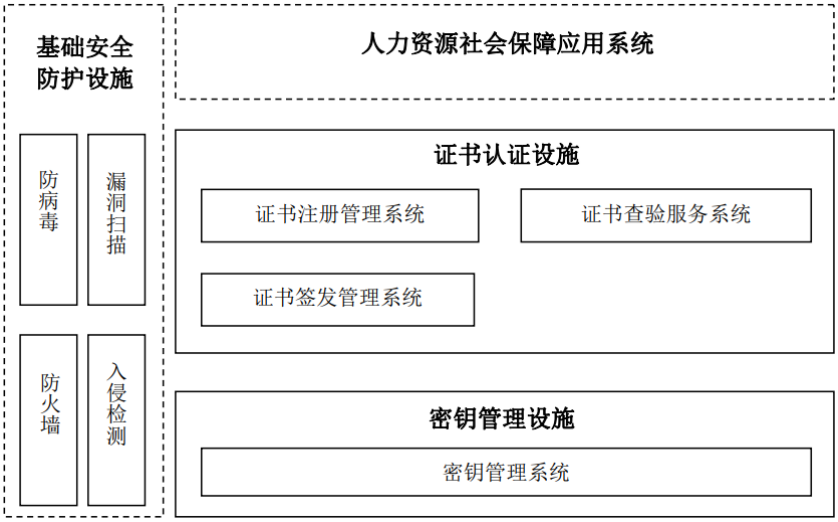



图18　电子认证系统

### 8.2.6　社会保障卡持卡人员基础信息库

社会保障卡持卡人员基础信息库，通过与各业务系统衔接，支持卡唯一性控制、卡有效性鉴权、人员基础信息共享、人员基本业务状态信息交换等应用，实现跨业务、跨地区、跨部门用卡。

社会保障卡持卡人员基础信息库包括部、省两级系统，分别实现对全国及省内持卡人员基础信息的集中管理和动态更新。部、省两级系统通过交易机制保持数据的一致性，接口开放，支持业务信息共享。

社会保障卡持卡人员基础信息库，应具备以下功能：

a)　信息生成与变更：为社会保障卡管理信息系统和各业务系统提供接口，实现相关信息的新增、变更和删除等操作；

b)　部省信息同步：省级系统与部级系统同步，保证部、省两级信息一致；

c)　信息查询校核：依据管辖权限和业务需求，各业务系统从部、省两级系统中读取、校核相关信息；

d)　辅助功能：包括日志下载、报表统计等。

## 8.3　服务管理功能

### 8.3.1　载体服务管理

社会保障卡一卡通的载体服务管理，包括实体社会保障卡和电子社会保障卡两部分：

a)　实体社会保障卡的载体服务管理，按照人力资源和社会保障部全流程监管要求实现，包含制发、启用、应用状态查询、密码修改与重置、挂失与解挂，补领、换领、换发、注销、应用锁定与解锁、信息变更，以及卡片样式变更审批等；

b)　电子社会保障卡的载体服务管理，包括领取、密码修改和重置、解除关联、查看领取渠道、应用授权等。

### 8.3.2　应用服务管理

社会保障卡一卡通的应用服务管理，包括服务支撑和服务输出两部分：

a)　服务支撑

包括平台接入管理、基础能力管理、应用管理、应用目录管理、机构目录管理、服务专区管理、服务资讯管理、数据管理、风控管理等功能，支撑各级社会保障卡一卡通管理机构进行应用拓展、丰富应用场景。

b)　服务输出

包括基础能力、地方专区、应用机构、服务资讯、使用记录等，用于构建场景化应用服务专区，为同级政务服务平台等渠道输出应用服务。

## 8.4 应用能力

### 8.4.1 办事凭证

#### 8.4.1.1 实卡认证

持卡人使用实体社会保障卡在终端设备上刷卡时，终端设备获取证件号码（社会保障号码）、证件类型、姓名等信息，社会保障卡一卡通应用系统经过各平台通道或者直接调用省级社会保障卡一卡通应用平台进行卡鉴权。对于跨省用卡，省级社会保障卡一卡通应用平台调用部级社会保障卡持卡人员基础信息库进行卡鉴权，逐级反馈卡鉴权结果，并将业务数据逐级上报至全国社会保障卡一卡通应用平台。

#### 8.4.1.2 扫码认证

持卡人使用电子社会保障卡服务渠道展示电子社会保障卡二维码，终端设备扫码后获取电子社会保障卡码值，经过各平台通道，通过省级社会保障卡一卡通应用平台到全国社会保障卡一卡通应用平台进行解码，全国社会保障卡一卡通应用平台逐级反馈证件号码（社会保障号码）、证件类型、姓名等身份信息，业务系统按照持卡人选择的业务继续完成业务办理，同时将业务数据逐级上报至全国社会保障卡一卡通应用平台。

一卡通应用系统支持如下两类基础能力：

a) 二维码生码 API。业务系统通过省级社会保障卡一卡通应用平台向全国社会保障卡一卡通应用平台获取电子社会保障卡码值，并生成动态二维码展示；
b) 二维码解码 API。业务系统通过省级社会保障卡一卡通应用平台到全国社会保障卡一卡通应用平台进行解码。

#### 8.4.1.3 实人认证

持卡人在相关应用场景中，使用电子社会保障卡扫码等方式关联人脸识别，社会保障卡一卡通应用系统采集获取人脸图像，随后将持卡人身份信息、人脸图像等经各平台通道，发送给全国一卡通应用平台进行人脸识别认证，全国社会保障卡一卡通应用平台逐级反馈认证结果，业务系统继续完成业务办理，同时将业务数据逐级上报全国社会保障卡一卡通应用平台。

社会保障卡一卡通应用系统支持如下两类人脸识别能力：

a) 人脸比对 API。社会保障卡一卡通应用系统通过终端设备采集获取人脸图像，调用人脸比对 API；
b) 人脸识别 HTML5。社会保障卡一卡通应用系统调用全国社会保障卡一卡通应用平台人脸识别 HTML5 服务。

#### 8.4.1.4 登录认证

持卡人在相关平台点击使用电子社会保障卡登录，身份信息经各平台通道上送至全国社会保障卡一卡通应用平台，全国社会保障卡卡通应用平台进行身份校验并将结果逐级反馈，相关平台获取持卡人身份信息后，提示持卡人登录成功。

社会保障卡一卡通应用系统支持如下三类登录能力：

a) 授权登录 HTML5。社会保障卡一卡通应用系统调用全国社会保障卡一卡通应用平台授权登录页面，持卡人输入社会保障号码、电子社会保障卡密码等身份信息；
b) 扫码登录 API。社会保障卡一卡通应用系统通过省级社会保障卡一卡通应用平台向全国一卡通应用平台获取电子社会保障卡码值，并生成动态二维码展示，持卡人使用电子社会保障卡“扫一扫”功能进行扫码；

c） 扫码登录 HTML5。社会保障卡一卡通应用系统调用全国社会保障卡一卡通应用平台的电子社会保障卡登录二维码页面，持卡人使用电子社会保障卡“扫一扫”功能进行扫码。

#### 8.4.2 支付结算

##### 8.4.2.1 就医结算

就医结算指个人持社会保障卡在定点医疗机构、定点零售药店就诊购药以及工伤保险协议机构办理业务时，使用社会保障卡记录的身份信息完成与医疗费用结算、工伤康复和辅助器具配置费用结算等，费用报销资金统一发放到社会保障卡银行账户。支付方式如下：

a） 对于实体社会保障卡，持卡人在医疗机构、零售药店以及工伤保险协议机构的终端设备上用卡时，医保信息系统调用卡鉴权接口，通过社会保障卡一卡通应用平台的卡鉴权接口进行实卡认证，在接收到反馈的卡鉴权结果后，根据用卡地区社会保障卡医保结算交易模式执行相应的卡处理流程，并按照持卡人的选择继续完成就医购药等业务办理。同时将业务数据逐级上报至全国社会保障卡一卡通应用平台；

b） 对于电子社会保障卡，持卡人使用电子社会保障卡服务渠道展示电子社会保障卡二维码，医疗机构、零售药店以及工伤保险协议机构的终端设备扫码后获取码值，医保信息系统通过社会保障卡一卡通应用平台调用全国社会保障卡一卡通应用平台解码接口进行解码验证，在获取到身份信息结果后，按照持卡人的选择继续完成就医购药等业务办理。同时将业务数据逐级上报至全国社会保障卡一卡通应用平台。

##### 8.4.2.2 金融支付

金融支付指持卡人使用社会保障卡银行账户进行线上或线下支付结算。支付方式如下：

a） 对于实体社会保障卡，持卡人在金融支付终端或支付平台上完成支付结算，应用流程应符合金融行业相关标准及要求；

b） 对于电子社会保障卡，持卡人通过电子社会保障卡服务渠道发起支付，业务系统将请求经各平台发送给全国社会保障卡卡通应用平台进行解析，获取持卡人身份信息后支付下单。支付下单请求经各平台发送给全国社会保障卡一卡通应用平台，前台页面调用电子社会保障卡收银台进行支付，并将结果反馈各平台及业务系统，并同步前台页面通知持卡人。

系统应支持如下三类支付能力：

a） 线上支付。持卡人通过电子社会保障卡服务渠道发起支付，向业务系统发起身份解析请求；

b） 被扫支付。持卡人使用电子社会保障卡服务渠道展示电子社会保障卡二维码，终端设备扫码后获取电子社会保障卡码值，向业务系统发起解码请求；

c） 主扫支付。收款方经各平台向全国社会保障卡一卡通应用平台发起生成主扫商户码的请求，展示商户码，持卡人通过电子社会保障卡的“扫一扫”功能扫描商户码，前台页面调用电子社会保障卡收银台进行支付。

#### 8.4.3 待遇发放

待遇发放指持卡人的相关待遇补贴等资金统一通过社会保障卡银行账户进行资金发放。持卡人使用社会保障卡银行账户进行待遇领取。

待遇补贴发放系统通过社会保障卡一卡通应用平台进行发放人员的身份认证，认证通过后将待遇发放数据传递给银行系统（支付平台）进行发放，随后将银行系统反馈的发放完成信息传递给社会保障卡一卡通应用平台，并通过电子社会保障卡服务渠道通知持卡人。

### 8.5 数据资源

社会保障卡一卡通应用体系的数据资源主要包括基础数据资源、业务数据资源和应用数据资源三类：

a) 基础数据资源，包括持卡人姓名、社会保障号码、相片、手机号码，电子社会保障卡的签发渠道、签发人员、服务功能以及签发人员的权限和使用记录等关键信息；
b) 业务数据资源，指在各类社会保障卡一卡通业务办理的过程中，相关业务部门的身份资格、业务状态、个人权益等数据资源；
c) 应用数据资源，指在各类社会保障卡一卡通业务办理过程中归集、整理的应用数据，包括办事凭证、支付结算、待遇发放、用户授权、应用机构五类数据。

# 附 录 A
（规范性）
实体社会保障卡卡号编制规则

## A.1 通则

本附录规定了实体社会保障卡卡号的编码方法，使每张社会保障卡在某一发卡地区均获得一个唯一的、始终不变的代码。

## A.2 卡号的结构和表示形式

### A.2.1 卡号的结构

社会保障卡卡号由 8 位数字（或大写拉丁字母）本体代码和 1 位数字（或大写拉丁字母）校验码组成。

本体代码采用系列（即分区段）顺序编码方法。

$$C_9 = 11 - MOD(\sum_{i=1}^{8} C_i \times W_i, 11) \quad \text{(A.1)}$$

校验码按公式（A.1）计算：

式中：MOD——表示求余函数；

$i$——表示代码字符从左至右位置序号；

$C_i$——表示第 $i$ 位置上的代码字符的值；

$C_9$——表示校验码；

$W_i$——表示第 $i$ 位置上的加权因子，其数值见表 A.1。

表 A.1 第 i 位置上的加权因子

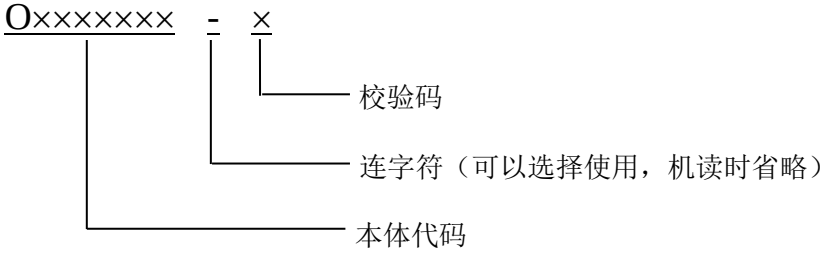
| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $W_i$ | 3 | 7 | 9 | 10 | 5 | 8 | 4 | 2 |

当 MOD 函数值为 1（即 $C_9$=10）时，校验码应用大写拉丁字母 X 表示；当 MOD 函数值为 0（即 $C_9$=11）时，校验码仍用 0 表示。

### A.2.2 卡号的表示形式

为便于人工识别，可以选择使用一个连字符“-”分隔本体代码与校验码。机读时，连字符省略。表示形式为：

本体代码中首位字符 O 为大写拉丁字母，代表发卡地区所辖各个地市/区县；本体代码中的其他 7 位字符为顺序码，由各个发卡地区自行定义。



## A.3 校验码数值的计算方法实例

实体社会保障卡卡号校验码数值的计算过程见表 A.2。

**表 A.2 校验码数值计算过程**

| 计算步骤 | 计算方法 | |
|---|---|---|
| | 说明 | 举例 |
| 1 | 取社会保障卡卡号的八位本体代码为基数 | D 2 1 4 3 5 6 9 |
| 2 | 取 $W_i$ 加权因子数值 | 3 7 9 10 5 8 4 2 |
| 3 | 本体代码与加权因子对应各位相乘 | 13×3 2×7 1×9 4×10 3×5 5×8 6×4 9×2 |
| 4 | 乘积相加求和数 | 39 + 14 + 9 + 40 + 15 + 40 + 24 + 18 = 199 |
| 5 | 取模数 11 除和数，求余数 | 199 ÷ 11 = 18 余 1 |
| 6 | 以模数 11 减余数，求校验码数值，当余数为 1，校验码数值为 10 时，校验码用大写拉丁字母“X”表示；当余数为 0，校验码数值为 11 时，校验码用“0”表示 | 11 – 1 = 10<br>校验码为 X |
| 7 | 将所得校验码置于八位本体代码之后即成为完整的社会保障卡卡号 | D 2 1 4 3 5 6 9 – X<br>校验码<br>连字符（机读时省略）<br>本体代码 |

**注：**首位字符O在计算时取值为：A为10，B为11，…G为16，…，以此类推。

# 附 录 B
（规范性）
# 电子社会保障卡卡号生成规则

电子社会保障卡卡号由发卡地行政区划和社会保障卡卡号按照一定的规则算法生成，具体生成规则如图B.1所示。

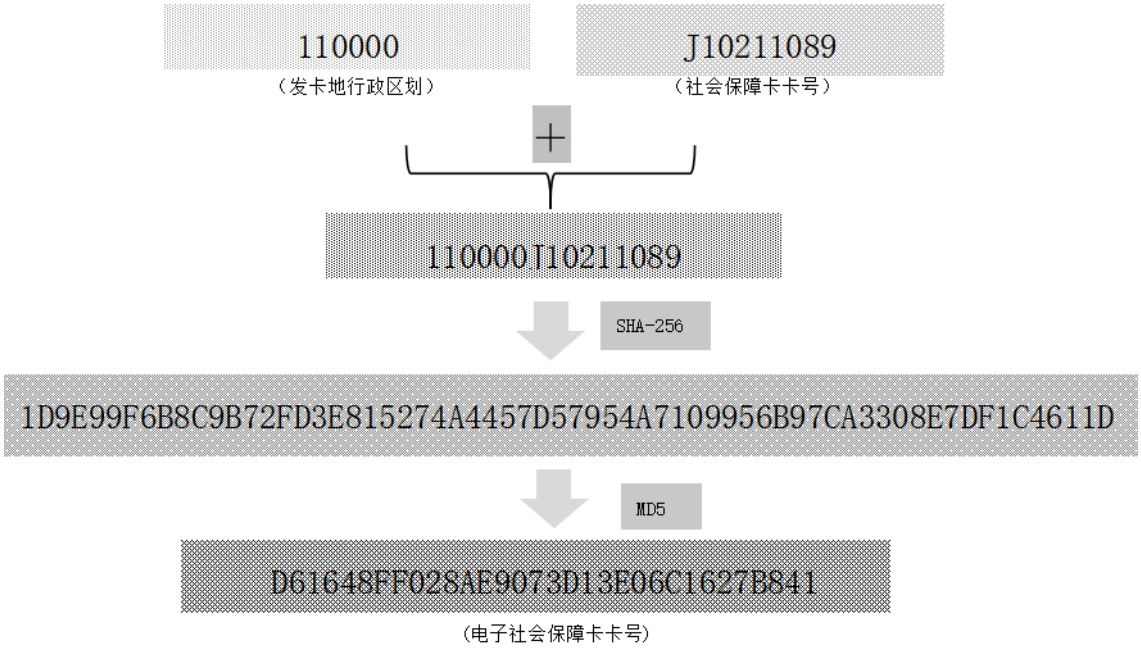



图 B.1 电子社会保障卡卡号生成规则

# 附 录 C
（规范性）
实体社会保障卡命令

## C.1 社会保障应用基本命令

### C.1.1 APPLICATION BLOCK（应用锁定）

#### C.1.1.1 定义和范围

APPLICATION BLOCK 命令使当前选择的应用失效。

当 APPLICATION BLOCK 命令执行成功后，用 SELECT 命令选择已失效的应用，回送状态码‘9303’（应用被永久锁定）。对其他命令的影响根据不同应用而定。

此命令执行成功后将永久锁定应用。

#### C.1.1.2 命令报文

APPLICATION BLOCK 命令报文编码见表 C.1。

表 C.1 APPLICATION BLOCK 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘84’ |
| INS | ‘1E’ |
| P1 | ‘00’ |
| P2 | ‘01’ |
| Lc | ‘04’ |
| Data | 见 C.1.1.3 |
| Le | 不存在 |

#### C.1.1.3 命令报文数据域

命令报文数据域为 MAC 数据元，MAC 的计算规则应符合 GB/T XXXXX.3—202X 中附录 A 的规定。

#### C.1.1.4 响应报文数据域

响应报文数据域不存在。

#### C.1.1.5 响应报文状态码

无论应用是否已经失效，此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.2。

表 C.2 APPLICATION BLOCK 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |

| | | |
|---|---|---|
| ‘67’ | ‘00’ | LC 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘69’ | ‘88’ | MAC 不正确 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘88’ | 未找到引用数据 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.2 CARD BLOCK（卡片锁定）

#### C.1.2.1 定义和范围

CARD BLOCK 命令使社会保障系统环境中所有应用永久失效。

当 CARD BLOCK 命令执行成功后，所有后续的命令都将回送状态码‘6A81’（功能不被支持），且不执行任何其他操作。

#### C.1.2.2 命令报文

CARD BLOCK 命令报文编码见表 C.3

C.3 CARD BLOCK 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘84’ |
| INS | ‘16’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | ‘04’ |
| Data | 见 C.1.2.3. |
| Le | 不存在 |

#### C.1.2.3 命令报文数据域

命令报文数据域为 MAC 数据元，MAC 的计算规则应符合 GB/T XXXXX.3—202X 中附录 A 的规定。

#### C.1.2.4 响应报文数据域

响应报文数据域不存在。

#### C.1.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.4。

表 C.4 CARD BLOCK 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |

| | | |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘69’ | ‘88’ | MAC 不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6A’ | ‘88’ | 未找到引用数据 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.1.3 CHANGE PIN（修改个人密码）

#### C.1.3.1 定义和范围

CHANGE PIN 命令允许持卡人将当前 PIN 修改为新 PIN。

当 CHANGE PIN 命令成功完成后，卡片要进行以下操作：

——密码尝试计数器复位至密码尝试次数的上限。

——将当前 PIN 置为新 PIN。

此命令中的 PIN 以明文方式传送。命令数据中的 PIN 是以 cn 格式存放的，它不需要整字节的填充，只有最低有效字节的低半字节可能需要填充，且填以‘F’。有效的 PIN 为 4-16 位阿拉伯数字。

#### C.1.3.2 命令报文

CHANGE PIN 命令报文编码见表 C.5。

表 C.5 CHANGE PIN 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘5E’ |
| P1 | ‘01’ |
| P2 | ‘00’ |
| Lc | ‘03’~‘11’ |
| Data | 当前 PIN ‖ ‘FF’ ‖ 新 PIN |
| Le | 不存在 |

#### C.1.3.3 命令报文数据域

命令报文数据域包括当前 PIN ‖ ‘FF’ ‖ 新 PIN,如果当前未使用 PIN 或更改后不再使用 PIN，则命令数据域中的‘当前 PIN’或‘新 PIN’可以不存在。

#### C.1.3.4 响应报文数据域

响应报文数据域不存在。

#### C.1.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的警告状态码见表 C.6。

表 C.6 CHANGE PIN 警告状态码

| SW1 | SW2 | 含义 |
|---|---|---|
| ‘63’ | ‘Cx’ | 鉴别失败，‘x’表示允许继续尝试的次数（‘0’-‘F’） |

卡片可能回送的错误状态码见表 C.7。

表 C.7 CHANGE PIN 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘83’ | 验证方法锁定 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.1.4 EXTERNAL AUTHENTICATION（外部鉴别）

#### C.1.4.1 定义和范围

EXTERNAL AUTHENTICATION 命令要求卡片中的应用验证 IFD 中保密模块的有效性，以使 IFD 获得某种授权。卡片的响应包括命令处理状态的回送。

#### C.1.4.2 命令报文

EXTERNAL AUTHENTICATION 命令报文编码见表 C.8。

表 C.8 EXTERNAL AUTHENTICATION 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘82’ |
| P1 | ‘00’ |
| P2 | 密钥标识符（见表 C.9） |
| Lc | ‘10’~‘11’ |
| Data | 见 C.1.4.3 |
| Le | 不存在 |

命令报文中的密钥标识符的结构见表 C.9。

表 C.9 密钥标识符的结构

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含　义 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 保留密钥 |
| 0 | | | | | | | | 全局参考数据 |
| 1 | | | | | | | | 专用参考数据 |
| | | | | x | x | x | x | 密钥号 |

#### C.1.4.3 命令报文数据域

命令报文数据域中包含 16-17 个字节的数据：

——第 1 至第 8 个字节为鉴别数据；

——第 9 至第 16 个字节是鉴别所需的原始信息；

——第 17 个字节是可选的，表示密钥版本。

其中，鉴别数据根据 GB/T XXXXX.3—202X 中的规定进行编码。

#### C.1.4.4 响应报文数据域

响应报文数据域不存在。

#### C.1.4.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的警告状态码见表 C.10。

表 C.10 EXTERNAL AUTHENTICATION 警告状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘63’ | ‘Cx’ | 鉴别失败，‘x’表示允许继续尝试的次数（‘0’-‘F’） |

卡片可能回送的错误状态码见表 C.11。

表 C.11 EXTERNAL AUTHENTICATION 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘83’ | 鉴别方法锁定 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6A’ | ‘88’ | 密钥未找到 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.5 GET CHALLENGE（获取随机数）

#### C.1.5.1 定义和范围

GET CHALLENGE 命令请求一个用于安全相关过程（如：安全报文、安全鉴别）的随机数。此随机数只能在当前应用下使用且只能使用一次。

#### C.1.5.2 命令报文

GET CHALLENGE 命令报文编码见表 C.12。

表 C.12 GET CHALLENGE 命令报文编码

| 代码 | 值 |
|---|---|

| | |
|---|---|
| CLA | ‘00’ |
| INS | ‘84’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | 不存在 |
| Data | 不存在 |
| Le | ‘04’或‘08’或‘10’ |

#### C.1.5.3 命令报文数据域

命令报文数据域不存在。

#### C.1.5.4 响应报文数据域

响应报文数据域包括随机数，长度为 4、8 或 16 字节。

#### C.1.5.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.13。

表 C.13 GET CHALLENGE 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Le 不正确 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.6 GET RESPONSE（获取响应）

#### C.1.6.1 定义和范围

在 T=0 协议下，当 APDU 不能使用现有协议传输时，GET RESPONSE 命令提供了一种从卡片向 IFD 传送 APDU（或 APDU 的一部分）的传输方法。

#### C.1.6.2 命令报文

GET RESPONSE 命令报文编码见表 C.14。

表 C.14 GET RESPONSE 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘C0’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | 不存在 |
| Data | 不存在 |
| Le | 响应的期望数据最大长度 |

#### C.1.6.3 命令报文数据域

命令报文数据域不存在。

#### C.1.6.4 响应报文数据域

响应报文数据域的长度由 Le 的值决定。

如果 Le 的值为 0，在附加数据有效时，卡片应回送状态码‘6Cxx’，否则回送状态码‘6F00’。

#### C.1.6.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的警告状态码见表 C.15。

表 C.15 GET RESPONSE 警告状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘61’ | ‘xx’ | 正常处理，‘xx’表示可以通过后续的 GET RESPONSE 命令得到的额外数据长度 |

卡片可能回送的错误状态码见表 C.16。

表 C.16 GET RESPONSE 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Le 不正确 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6C’ | ‘xx’ | Le 不正确；‘xx’表示实际长度 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘6F’ | ‘00’ | 数据无效 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.7 INTERNAL AUTHENTICATION（内部鉴别）

#### C.1.7.1 定义和范围

INTERNAL AUTHENTICATION 命令提供了利用 IFD 发来的随机数和自身存储的相关密钥进行数据鉴别的功能。

当有关密钥位于 SSSE 目录下时，该命令可以用来鉴别 SSSE 的合法性；当有关密钥位于 DF 目录下时，该命令可以用来鉴别特定应用的合法性。

#### C.1.7.2 命令报文

INTERNAL AUTHENTICATION 命令报文编码见表 C.17。

表 C.17 INTERNAL AUTHENTICATION 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘88’ |
| P1 | ‘00’ |

| | |
|---|---|
| P2 | ‘00’ |
| Lc | ‘10’~ 11’ |
| Data | 见 C.1.7.3 |
| Le | ‘08’ |

#### C.1.7.3 命令报文数据域

命令报文数据域的内容是卡片或应用专用的鉴别数据，包含 16-17 个字节的数据：

——第 1 至第 8 个字节是过程密钥计算使用的数据；

——第 9 至第 16 个字节是鉴别所需的原始信息；

——第 17 个字节是可选的，表示密钥版本。

#### C.1.7.4 响应报文数据域

响应报文数据域内容是相关的鉴别数据，其值根据 GB/T XXXXX.3—202X 中的规定进行编码。

#### C.1.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.18。

表 C.18 INTERNAL AUTHENTICATION 错误状态码

| SW1 | SW2 | 含义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6A’ | ‘88’ | 密钥未找到 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.8 PIN CHANGE/UNBLOCK（个人密码重置/解锁）

#### C.1.8.1 定义和范围

该命令用于重置 PIN 或解锁 PIN（即重置 PIN 尝试计数器的值为应用设定的最大尝试次数）。

此命令中 PIN 的传递采用加密方式。

#### C.1.8.2 命令报文

PIN CHANGE/UNBLOCK 命令报文编码见表 C.19。

表 C.19 PIN CHANGE/UNBLOCK 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘84’ |
| INS | ‘24’ |
| P1 | ‘00’ |
| P2 | 引用控制参数（见表 C.20） |
| Lc | 数据域长度 |

| | |
|---|---|
| Data | 见 C.1.8.3 |
| Le | 不存在 |

命令报文中的控制参数见表 C.20。

表 C.20 PIN CHANGE/UNBLOCK 命令引用控制参数

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含义 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 重置 PIN。重置尝试计数器，并以新 PIN 取代当前 PIN。 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 解锁 PIN。仅重置尝试计数器，并不更改当前 PIN。 |

### C.1.8.3 命令报文数据域

Lc 值与数据域内容的对应关系见表 C.21。

表 C.21 Lc 值与数据域内容的对应关系

| 操作 | Lc 值 | 数据域内容 |
|---|---|---|
| 解锁 PIN | ‘04’ | Lc 应包括 MAC 数据元的长度。 |
| 更改 PIN | ‘0C’或‘14’ | Lc 应同时包括被加密的 PIN 数据元和 MAC 数据元的长度。 |

PIN 数据元和 MAC 数据元根据 GB/T XXXXX.3—202X 中的规定进行编码。

当被加密的 PIN 数据元长度为零时，应将卡片中已存在的有效的 PIN 置为空的 PIN。

### C.1.8.4 响应报文数据域

响应报文数据域不存在。

### C.1.8.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.22。

表 C.22 PIN CHANGE/UNBLOCK 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘69’ | ‘85’ | 不满足使用条件 |
| ‘69’ | ‘88’ | MAC 不正确 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 不支持此功能 |
| ‘6A’ | ‘86’ | P1、 P2 不正确 |
| ‘6A’ | ‘88’ | 未找到引用数据 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

## C.1.9 READ BINARY（读取二进制数据）

### C.1.9.1 定义和范围

READ BINARY 命令用于读取透明文件的内容（或部分内容）。

### C.1.9.2 命令报文

READ BINARY 命令报文编码见表 C.23 。

表 C.23 READ BINARY 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘B0’ |
| P1 | 引用控制参数（见表 C.24） |
| P2 | |
| Lc | 不存在 |
| Data | 不存在 |
| Le | ‘00’或要读出数据的长度 |

命令报文中的控制参数见表 C.24

表 C.24 READ BINARY 命令引用控制参数

| P1 | | | | | | | | P2 | | | | | | | | 含　义 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | |
| 1 | 0 | 0 | x | x | x | x | x | y | y | y | y | y | y | y | y | xxxxx 表示 SFI，yyyyyyyy 为要读的首字节距离文件首字节的偏移量。 |
| 0 | x | x | x | x | x | x | x | y | y | y | y | y | y | y | y | P1×256+P2 为要读的首字节距离文件首字节的偏移量。 |

### C.1.9.3 命令报文数据域

命令报文数据域不存在。

### C.1.9.4 响应报文数据域

当 Le 的值为 0 时，读出自要读的首字节起的 256 字节；如果在读出 256 字节前已到达文件最后一个字节，则自要读的首字节起的全部字节将被读出。

### C.1.9.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.25。

表 C.25　READ BINARY 的错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘69’ | ‘81’ | 命令与文件结构不相容 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘86’ | 不满足命令执行的条件（无当前基本文件） |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘86’ | P1、 P2 不正确 |
| ‘6B’ | ‘00’ | 参数不正确（偏移地址超出了 EF） |
| ‘6C’ | ‘xx’ | Le 不正确；‘xx’为实际长度 |
| ‘6E’ | ‘00’ | CLA 不正确 |

| | | |
|---|---|---|
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.10 READ RECORD（读取记录内容）

#### C.1.10.1 定义和范围

READ RECORD 命令读取记录结构的基本文件中一些指定的记录或一个记录起始部分的数据。卡片的响应由回送记录组成。

#### C.1.10.2 命令报文

READ RECORD 命令报文编码见表 C.26。

表 C.26 READ RECORD 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘B2’ |
| P1 | 记录号或记录标识符，记录号的取值范围为‘01’－‘FE’，‘00’表示当前记录 |
| P2 | 引用控制参数（见表 C.27） |
| Lc | 不存在 |
| Data | 不存在 |
| Le | ‘00’或要读出数据的长度 |

命令报文中的控制参数见表 C.27。

表 C.27 READ RECORD 命令引用控制参数

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含　义 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | - | - | - | 对当前文件进行操作 |
| x | x | x | x | x | - | - | - | SFI |
| - | - | - | - | - | 1 | 0 | 0 | 读 P1 指定的记录 |
| - | - | - | - | - | 1 | 0 | 1 | 从 P1 指定的记录开始读到最后一个记录 |
| - | - | - | - | - | 1 | 1 | 0 | 从最后一个记录开始读到 P1 指定的记录 |
| - | - | - | - | - | 0 | 0 | 0 | 读具有 P1 指定的记录标识符的第一个实例 |
| - | - | - | - | - | 0 | 0 | 1 | 读具有 P1 指定的记录标识符的最后一个实例 |
| - | - | - | - | - | 0 | 1 | 0 | 读具有 P1 指定的记录标识符的下一个实例 |
| - | - | - | - | - | 0 | 1 | 1 | 读具有 P1 指定的记录标识符的上一个实例 |

#### C.1.10.3 命令报文数据域

命令报文数据域不存在。

#### C.1.10.4 响应报文数据域

所有执行成功的 READ RECORD 命令的响应报文数据域由读取的记录组成。

当 Le=00 时，应以‘6Cxx’返回可读的实际长度。当可读的实际数据长度大于 256 字节时，按报错处理，返回‘6700’。

#### C.1.10.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.28。

表 C.28 READ RECORD 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘81’ | 命令与文件结构不相容 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘86’ | 命令不允许使用（无当前基本文件） |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘83’ | 未找到记录 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6C’ | ‘xx’ | Le 不正确；‘xx’为实际长度 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.11　SELECT（选择文件）

#### C.1.11.1　定义和范围

SELECT 命令通过文件名或 AID 来选择卡片中的 SSSE，通过文件名或 AID、文件标识符来选择 ADF，通过文件标识符来选择 ADF 中的 AEF。

命令执行成功后，SSSE、DDF 或 ADF、AEF 的路径被设定。

除选择 AEF 外，卡片的响应报文应由回送的 FCI 组成。

在当前 ADF 未被 SELECT 命令改变或重新设定时，该 ADF 下的所有安全状态应被保持。

#### C.1.11.2　命令报文

SELECT 命令报文编码见表 C.29。

表 C.29 SELECT 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘A4’ |
| P1 | 引用控制参数（见表 C.30） |
| P2 | ‘00’第一个或唯一一个文件实例<br>‘02’下一个文件实例 |
| Lc | ‘05’-‘10’（使用文件名或 AID 时）或‘02’（使用文件标识符时）或‘00’ |
| Data | 见 C.1.11.3 |
| Le | ‘00’或 FCI 的长度 |

命令报文中的控制参数见表 C.30。

表 C.30 SELECT 命令引用控制参数

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含　义 |
|---|---|---|---|---|---|---|---|---|

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 用文件标识符选择 DF（数据域=文件标识符或空） |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 用文件标识符在当前 DF 下选择 EF（数据域=EF 的文件标识符） |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 通过文件名选择 DF（数据域=DF 的文件名） |

如果 P1='00'并且数据域为空或等于'3F00'，该命令将退出 SSSE。

#### C.1.11.3 命令报文数据域

命令报文数据域可能是文件名、AID、文件标识符或不存在。

#### C.1.11.4 响应报文数据域

除选择 AEF 外，响应报文中数据域应包括所选择的 SSSE、DDF 或 ADF 的 FCI。表 C.31 到表 C.33 规定了所用的标志。

SELECT SSSE 成功后回送的 FCI 见表 C.31。

表 C.31 SELECT SSSE 的响应报文（FCI）

| 标志 | | | 值 | 存在方式 |
|---|---|---|---|---|
| '6F' | | | FCI 模板 | M |
| | '84' | | DF 名 | M |
| | 'A5' | | FCI 专用模板 | M |
| | | '88' | 目录基本文件的 SFI | O |
| | | '9F0C' | 算法标识信息：'86 01 算法类型'（DES 算法类型：'01'；SSF33 算法类型：'02'；SM4 算法类型：'03'） | O |

SELECT DDF 成功后回送的 FCI 见表 C.32。

表 C.32 SELECT DDF 的响应报文（FCI）

| 标志 | | | 值 | 存在方式 |
|---|---|---|---|---|
| '6F' | | | FCI 模板 | M |
| | '84' | | DF 名 | M |
| | 'A5' | | FCI 专用模板 | M |
| | | '88' | 目录基本文件的 SFI | O |

SELECT ADF 成功后回送的 FCI 见表 C.33。

表 C.33 SELECT ADF 的响应报文（FCI）

| 标志 | | 值 | 存在方式 |
|---|---|---|---|
| '6F' | | FCI 模板 | M |
| | '84' | DF 名 | M |

#### C.1.11.5 响应报文状态码

此命令执行成功的状态码是'9000'。卡片可能回送的错误状态码见表 C.34。

表 C.34 SELECT 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|

| | | |
|---|---|---|
| ‘67’ | ‘00’ | P1、P2 与 Lc 不一致 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.12 UPDATE BINARY（更新二进制数据）

#### C.1.12.1 定义和范围

UPDATE BINARY 命令报文使用命令 APDU 中给定的数据写入或修改透明结构的基本文件的全部或部分数据。

#### C.1.12.2 命令报文

UPDATE BINARY 命令报文编码见表 C.35。

表 C.35 UPDATE BINARY 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’或‘04’ |
| INS | ‘D6’ |
| P1 | 引用控制参数（见表 C.36） |
| P2 | |
| Lc | Data 域数据长度 |
| Data | 见 C.1.12.3 |
| Le | 不存在 |

命令报文中的引用控制参数见表 C.36。

表 C.36 UPDATE BINARY 命令引用控制参数

| P1 | | | | | | | | P2 | | | | | | | | 含　义 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | |
| 1 | 0 | 0 | x | x | x | x | x | y | y | y | y | y | y | y | y | xxxxx 表示 SFI，yyyyyyyy 为要写入或修改的首字节距离文件首字节的偏移量。 |
| 0 | x | x | x | x | x | x | x | y | y | y | y | y | y | y | y | P1×256+P2 为要写入或修改的首字节距离文件首字节的偏移量。 |

#### C.1.12.3 命令报文数据域

命令报文数据域包括用来写入或修改用的数据。

#### C.1.12.4 响应报文数据域

响应报文数据域不存在。

#### C.1.12.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.37。

表 C.37 UPDATE BINARY 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘81’ | 命令与文件结构不相容 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘69’ | ‘86’ | 不满足命令执行的条件（无当前基本文件） |
| ‘69’ | ‘88’ | MAC 不正确 |
| ‘6A’ | ‘81’ | 不支持此功能 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘86’ | P1、 P2 不正确 |
| ‘6B’ | ‘00’ | 参数不正确（偏移地址超出了 EF） |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.13　UPDATE RECORD（更新记录内容）

#### C.1.13.1　定义和范围

UPDATE RECORD 命令报文用命令 APDU 中给定的数据添加新的记录或修改指定记录。

对线性结构文件来说，当指定的记录号不存在时，可按记录号顺序添加新的记录。按记录标识符访问的记录不存在时，也应视为添加新的记录。

对循环结构文件来说，当使用“P1 指定标识的上一个实例”命令选项时应视为添加新的记录。

在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

#### C.1.13.2　命令报文

UPDATE RECORD 命令报文编码见表 C.38。

表 C.38 UPDATE RECORD 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’或‘04’ |
| INS | ‘DC’ |
| P1 | 记录号或记录标识符（‘00’，表示当前记录） |
| P2 | 引用控制参数（见表 C.39） |
| Lc | Data 域数据长度 |
| Data | 见 C.1.13.3 |
| Le | 不存在 |

命令报文中的引用控制参数见表 C.39。

表 C.39 UPDATE RECORD 命令引用控制参数

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含　义 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | - | - | - | 当前的 EF 文件 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| X | x | x | x | x | - | - | - | SFI |
| - | - | - | - | - | 1 | x | x | 使用 P1 中的记录号 |
| - | - | - | - | - | 1 | 0 | 0 | P1 指定记录号 |
| - | - | - | - | - | 0 | x | x | 使用 P1 中的记录标识符 |
| - | - | - | - | - | 0 | 0 | 0 | P1 指定标识的第一个实例 |
| - | - | - | - | - | 0 | 0 | 1 | P1 指定标识的最后一个实例 |
| - | - | - | - | - | 0 | 1 | 0 | P1 指定标识的下一个实例 |
| - | - | - | - | - | 0 | 1 | 1 | P1 指定标识的上一个实例 |
| 其余值 | | | | | | | | RFU |

#### C.1.13.3 命令报文数据域

命令报文数据域由添加或修改原有记录的新记录组成。

#### C.1.13.4 响应报文数据域

响应报文数据域不存在。

#### C.1.13.5 响应报文状态码

命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.40。

表 C.40 UPDATE RECORD 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | 长度不正确（Lc 域为空） |
| ‘69’ | ‘81’ | 命令与文件结构不相容 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘69’ | ‘86’ | 不满足命令执行的条件（不是当前的 EF） |
| ‘69’ | ‘88’ | MAC 不正确 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘83’ | 未找到记录 |
| ‘6A’ | ‘84’ | 文件中存储空间不够 |
| ‘6A’ | ‘85’ | Lc 与 TLV 结构不符 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.14 VERIFY（校验个人密码）

#### C.1.14.1 定义和范围

VERIFY 命令用于校验命令数据域中的 PIN 的正确性。VERIFY 命令在处理过程中应明确知道如何去寻找 PIN。

#### C.1.14.2 命令报文

VERIFY 命令报文编码见表 C.41。

表 C.41 VERIFY 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘20’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | ‘00’或‘02’~‘08’ |
| Data | 见 C.1.14.3 |
| Le | 不存在 |

#### C.1.14.3 命令报文数据域

命令报文数据域不为空时由外部输入的 PIN 组成。

#### C.1.14.4 响应报文数据域

响应报文数据域不存在。

#### C.1.14.5 响应报文状态码

当命令报文数据域不为空时，此命令执行成功的状态码是‘9000’。命令数据域中外部输入的 PIN 与卡片中存放的 PIN 校验失败时（包括卡片中存放的 PIN 为空的情况），卡片将回送 SW1SW2=‘63Cx’，‘x’表示 PIN 允许重试的次数；当卡片回送‘63C0’时，表示不能重试 PIN。此时再使用 VERIFY 命令时，将回送错误状态码 SW1SW2=‘6983’。

当命令报文数据域为空时，如果卡片中存放的 PIN 不为空，则卡片将回送 SW1SW2=‘63Cx’，‘x’表示 PIN 允许重试的次数；如果卡片中存放的 PIN 为空，卡片将回送状态码‘9000’。

卡片可能回送的警告状态码见表 C.42。

表 C.42 VERIFY 警告状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘63’ | ‘Cx’ | 鉴别失败，‘x’表示允许继续尝试的次数 |

卡片可能回送的错误状态码见表 C.43。

表 C.43 VERIFY 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘83’ | PIN 锁定 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6A’ | ‘88’ | 未找到引用数据 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.15 CREDIT FOR LOAD（账户划入）

#### C.1.15.1 定义和范围

CREDIT FOR LOAD 命令用于账户划入。在执行 CREDIT FOR LOAD 命令之前，应成功执行 INITIALIZE FOR LOAD 命令。

#### C.1.15.2 命令报文

CREDIT FOR LOAD 命令报文编码见表 C.44。

表 C.44 CREDIT FOR LOAD 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘B0’ |
| INS | ‘2A’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | ‘0B’ |
| Data | 见 C.1.15.3 |
| Le | ‘04’ |

#### C.1.15.3 命令报文数据域

CREDIT FOR LOAD 命令报文数据域见表 C.45。

表 C.45 CREDIT FOR LOAD 命令报文数据域

| 说明 | 长度（字节） |
|---|---|
| 交易时间（主机） | ‘07’ |
| MAC2 | ‘04’ |

#### C.1.15.4 响应报文数据域

CREDIT FOR LOAD 响应报文数据域见表 C.46。

表 C.46 CREDIT FOR LOAD 响应报文数据域

| 说明 | 长度（字节） |
|---|---|
| TAC | ‘04’ |

#### C.1.15.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.47。

表 C.47 CREDIT FOR LOAD 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | EEPROM 损坏，导致卡片锁定 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘01’ | 命令不接受（无效状态） |
| ‘69’ | ‘85’ | 使用条件不满足 |

| | | |
|---|---|---|
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | 命令类型不正确 |
| ‘93’ | ‘02’ | MAC 无效 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.16 DEBIT FOR PURCHASE（医疗费用结算）

#### C.1.16.1 定义和范围

DEBIT FOR PURCHASE 命令用于医疗费用结算。在执行 DEBIT FOR PURCHASE 命令之前，应成功执行 INITIALIZE FOR PURCHASE 命令。

#### C.1.16.2 命令报文

DEBIT FOR PURCHASE 命令报文编码见表 C.48。

表 C.48 DEBIT FOR PURCHASE 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘B0’ |
| INS | ‘2C’ |
| P1 | ‘01’ |
| P2 | ‘00’ |
| Lc | ‘0F’ |
| Data | 见 C.1.16.3 |
| Le | ‘08’ |

#### C.1.16.3 命令报文数据域

DEBIT FOR PURCHASE 命令报文数据域见表 C.49。

表 C.49 DEBIT FOR PURCHASE 命令报文数据域

| 说明 | 长度（字节） |
|---|---|
| 终端交易序号 | ‘04’ |
| 交易时间 | ‘07’ |
| MAC1 | ‘04’ |

#### C.1.16.4 响应报文数据域

DEBIT FOR PURCHASE 响应报文数据域见表 C.50。

表 C.50 DEBIT FOR PURCHASE 命令报文数据域

| 说明 | 长度（字节） |
|---|---|
| TAC | ‘04’ |
| MAC2 | ‘04’ |

#### C.1.16.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.51。

表 C.51 DEBIT FOR PURCHASE 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | EEPROM 损坏，导致卡片锁定 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘01’ | 命令不接受（无效状态） |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | 命令类型不正确 |
| ‘93’ | ‘02’ | MAC 无效 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.17　GET BALANCE（读取卡片内基本医疗保险个人账户余额/年度个人自付累计金额/年度统筹基金支付累计金额）

#### C.1.17.1　定义和范围

GET BALANCE 命令用于读取 CIA 余额/年度 SPIP 金额/年度 SPFP 金额。该命令应验证 PIN。

#### C.1.17.2　命令报文

GET BALANCE 命令报文编码见表 C.52。

表 C.52 GET BALANCE 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘B0’ |
| INS | ‘26’ |
| P1 | ‘00’ |
| P2 | ‘01’：用于 CIA；<br>‘02’：用于 SPIP；<br>‘03’：用于 SPFP；<br>其他值保留。 |
| Lc | 不存在 |
| Data | 不存在 |
| Le | ‘04’（P2=‘01’时）；<br>‘06’（P2=‘02’或‘03’时）。 |

#### C.1.17.3　命令报文数据域

命令报文数据域不存在。

#### C.1.17.4　响应报文数据域

此命令执行成功的响应报文数据域见表 C.53。

表 C.53 GET BALANCE 响应报文数据域

| 说明 | 长度（字节） |
|---|---|
| CIA 余额/SPIP 金额/SPFP 金额 | ‘04’ |
| 支付年度（当 P2=‘02’或‘03’时存在） | ‘02’ |

### C.1.17.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.54。

表 C.54 GET BALANCE 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Le 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | 命令类型不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.18 GET TRANSACTION PROOF（读取交易认证码）

### C.1.18.1 定义和范围

GET TRANSACTION PROOF 命令用于取 TAC 和 MAC。它提供了一种在交易处理过程中异常掉电后的恢复机制。

### C.1.18.2 命令报文

GET TRANSACTION PROOF 命令报文编码见表 C.55。

表 C.55 GET TRANSACTION PROOF 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘B0’ |
| INS | ‘2E’ |
| P1 | ‘00’ |
| P2 | 要取的 MAC 和 TAC 所对应的交易类型标识 |
| Lc | ‘02’ |
| Data | 见 C.1.18.3 |
| Le | ‘08’ |

### C.1.18.3 命令报文数据域

GET TRANSACTION PROOF 命令报文数据域见表 C.56。

表 C.56 GET TRANSACTION PROOF 命令报文数据域

| 说明 | 长度（字节） |
|---|---|
| 要取的 MAC 和 TAC 所对应的 CIA 划入或医疗费用结算交易序号 | ‘02’ |

#### C.1.18.4 响应报文数据域

如果命令中指定的交易类型标识和CIA划入或医疗费用结算交易序号对应的MAC 或TAC可用，则响应报文数据域见表C.57。

表C.57 GET TRANSACTION PROOF 响应报文数据域

| 说明 | 长度（字节） |
|---|---|
| MAC | ‘04’ |
| TAC | ‘04’ |

#### C.1.18.5 响应报文状态码

此命令执行成功的状态码是‘9000’。 卡片可能回送的错误状态码见表C.58。

表C.58 GET TRANSACTION PROOF 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Le不正确 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2不正确 |
| ‘6E’ | ‘00’ | 命令类型不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |
| ‘94’ | ‘06’ | 所需MAC不可用 |

### C.1.19 INITIALIZE FOR LOAD（账户划入初始化）

#### C.1.19.1 定义和范围

INITIALIZE FOR LOAD命令用于账户划入的初始化。执行该命令后即选择了账户划入交易，下一条应执行CREDIT FOR LOAD命令。INITIALIZE FOR LOAD命令仅对下一条命令有效。

#### C.1.19.2 命令报文

INITIALIZE FOR LOAD命令报文编码见表C.59。

表C.59 INITIALIZE FOR LOAD 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘B0’ |
| INS | ‘28’ |
| P1 | ‘00’ |
| P2 | ‘01’；<br>其他值保留。 |
| Lc | ‘0B’ |
| Data | 见C.1.19.3 |
| Le | ‘10’ |

#### C.1.19.3 命令报文数据域

INITIALIZE FOR LOAD 命令报文数据域见表 C.60。

表 C.60 INITIALIZE FOR LOAD 命令报文数据域

| 说明 | 长度（字节） |
|---|---|
| 密钥索引号 | ‘01’ |
| 交易金额 | ‘04’ |
| 终端机编号 | ‘06’ |

### C.1.19.4 响应报文数据域

此命令执行成功的响应报文数据域见表 C.61。

表 C.61 INITIALIZE FOR LOAD 响应报文数据域

| 说明 | 长度（字节） |
|---|---|
| CIA 余额 | ‘04’ |
| CIA 划入交易序号 | ‘02’ |
| 密钥版本号 | ‘01’ |
| 算法标识 | ‘01’ |
| 伪随机数 | ‘04’ |
| MAC1 | ‘04’ |

### C.1.19.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.62。

表 C.62 INITIALIZE FOR LOAD 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | EEPROM 损坏，导致卡片锁定 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | 命令类型不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |
| ‘94’ | ‘02’ | 交易计数器达到最大值 |
| ‘94’ | ‘03’ | 密钥索引不支持 |

## C.1.20 INITIALIZE FOR PURCHASE（医疗费用结算初始化）

### C.1.20.1 定义和范围

INITIALIZE FOR PURCHASE 命令用于医疗费用结算的初始化。执行该命令后即选择了医疗费用结算交易，下一条应执行 DEBIT FOR PURCHASE 命令。INITIALIZE FOR PURCHASE 命令仅对下一条命令有效。

### C.1.20.2 命令报文

INITIALIZE FOR PURCHASE 命令报文编码见表 C.63。

表 C.63 INITIALIZE FOR PURCHASE 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘B0’ |
| INS | ‘28’ |
| P1 | ‘01’ |
| P2 | ‘01’；其他值保留。 |
| Lc | ‘13’ |
| Data | 见 C.1.20.3 |
| Le | ‘16’ |

### C.1.20.3 命令报文数据域

INITIALIZE FOR PURCHASE 命令报文数据域见表 C.64。

表 C.64 INITIALIZE FOR PURCHASE 命令报文数据域

| 说明 | 长度（字节） |
|---|---|
| 密钥索引号 | ‘01’ |
| 个人账户支付金额 | ‘04’ |
| 个人自付金额 | ‘04’ |
| 统筹基金支付金额 | ‘04’ |
| 终端机编号 | ‘06’ |

### C.1.20.4 响应报文数据域

此命令执行成功的响应报文数据域见表 C.65。

表 C.65 INITIALIZE FOR PURCHASE 响应报文数据域

| 说明 | 长度（字节） |
|---|---|
| CIA 余额 | ‘04’ |
| SPIP 金额 | ‘04’ |
| SPFP 金额 | ‘04’ |
| 支付年度 | ‘02’ |
| 医疗费用结算交易序号 | ‘02’ |
| 密钥版本号 | ‘01’ |
| 算法标识 | ‘01’ |
| 伪随机数 | ‘04’ |

### C.1.20.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.66。

表 C.66 INITIALIZE FOR PURCHASE 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | EEPROM 损坏，导致卡片锁定 |

| | | |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | 命令类型不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |
| ‘94’ | ‘01’ | 金额不足 |
| ‘94’ | ‘02’ | 交易计数器达到最大值 |
| ‘94’ | ‘03’ | 密钥索引不支持 |

### C.1.21 UPDATE STARTING DAY（修改年度起始日期）

#### C.1.21.1 定义和范围

UPDATE STARTING DAY 命令用于修改医疗保险账户中的“年度起始日期”数据元。修改权限与在该应用下建立文件的权限相同。

使用该命令前应经过 DSK 密钥认证（DSK 密钥是专用于控制和更新年度起始日期的密钥）。

#### C.1.21.2 命令报文

UPDATE STARTING DAY 命令报文编码见表 C.67。

表 C.67 UPDATE STARTING DAY 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘B0’ |
| INS | ‘56’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | ‘02’ |
| Data | 见 C.1.21.3 |
| Le | 不存在 |

#### C.1.21.3 命令报文数据域

UPDATE STARTING DAY 命令报文数据域见表 C.68。

表 C.68 UPDATE STARTING DAY 命令报文数据域

| 说明 | 长度（字节） |
|---|---|
| 年度起始日期（格式：mmdd） | ‘02’ |

#### C.1.21.4 响应报文数据域

响应报文数据域不存在。

#### C.1.21.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.69。

表 C.69 UPDATE STARTING DAY 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | 命令类型不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

### C.1.22　GET STARTING DAY （读取年度起始日期）

#### C.1.22.1　定义和范围

GET STARTING DAY 命令用于读取医疗保险账户中的“年度起始日期”数据元。

#### C.1.22.2　命令报文

GET STARTING DAY 命令报文编码见表 C.70。

表 C.70 GET STARTING DAY 命令报文编码

| 代码 | 值 |
|---|---|
| CLA | ‘B0’ |
| INS | ‘56’ |
| P1 | ‘01’ |
| P2 | ‘00’ |
| Lc | 不存在 |
| Data | 不存在 |
| Le | ‘02’ |

#### C.1.22.3　命令报文数据域

命令报文数据域不存在。

#### C.1.22.4　响应报文数据域

GET STARTING DAY 响应报文数据域见表 C.71。

表 C.71 GET STARTING DAY 响应报文数据域

| 说明 | 长度（字节） |
|---|---|
| 年度起始日期（格式：mmdd） | ‘02’ |

#### C.1.22.5　响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.72。

表 C.72 GET STARTING DAY 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘69’ | ‘82’ | 不满足安全状态 |

| | | |
|---|---|---|
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘81’ | 功能不被支持 |
| ‘6A’ | ‘86’ | P1、P2 不正确 |
| ‘6E’ | ‘00’ | 命令类型不正确 |
| ‘93’ | ‘03’ | 应用被永久锁定 |

## C.2 非对称认证应用基本命令

### C.2.1 CHANGE DEV KEY（修改设备密钥）

#### C.2.1.1 定义和范围

CHANGE DEV KEY 命令用于修改设备密钥，即 DF 的主控密钥。CHANGE DEV KEY 命令执行时，应使用密文和安全报文方式进行更新。

#### C.2.1.2 命令报文

CHANGE DEV KEY 命令报文见表 C.73。

表 C.73 CHANGE DEV KEY 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘84’ |
| INS | ‘D4’ |
| P1 | ‘01’ |
| P2 | ‘00’ |
| Lc | ‘24’ |
| Data | 加密的密钥信息+4 字节 MAC 数据元 |
| Le | 不存在 |

#### C.2.1.3 命令报文数据域

“密钥信息”是指：用途（‘00’）＋标识（‘00’）＋版本（‘00’）＋密钥值本身。

数据加密及安全报文的计算密钥使用当前目录的主控密钥。

#### C.2.1.4 响应报文数据域

响应报文数据域不存在。

#### C.2.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.74。

表 C.74 CHANGE DEV KEY 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘83’ | 认证密钥锁定 |
| ‘69’ | ‘84’ | 引用数据无效（未申请随机数） |

| | | |
|---|---|---|
| ‘69’ | ‘88’ | 安全信息（MAC 和密文）不正确 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘88’ | 未找到密钥数据 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.2 CHANGE PIN/ RELOAD PIN（修改或重置）

#### C.2.2.1 定义和范围

CHANGE PIN/ RELOAD PIN 命令允许用户修改 PIN 或重置 PIN。

CHANGE PIN 校验成功将更新原 PIN，并将尝试计数器恢复到最大值，同时应用安全状态切换到用户态（相当于 PIN 校验成功）；RELOAD PIN 成功后，则重置 PIN，并将尝试计数器恢复到最大值。

命令数据中的 PIN 是以 cn 格式存放，有效的 PIN 为 4-16 位。

用户 PIN 的可尝试次数为 6 次。CHANGE PIN/ RELOAD PIN 命令需满足 PIN 的修改权限。

#### C.2.2.2 命令报文

CHANGE PIN/ RELOAD PIN 命令报文见表 C.75。

表 C.75 CHANGE PIN/ RELOAD PIN 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘84’ |
| INS | ‘5E’ |
| P1 | ‘01’ 修改 PIN<br>‘02’ 重置 PIN |
| P2 | 见表 C.76 |
| Lc | ‘14’ |
| Data | 见 C.2.2.3 |
| Le | 不存在 |

命令报文中的控制参数见表 C.76。

表 C.76 P2 参数说明

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 说　明 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | - | - | - | - | - | 修改或重置用户 PIN |
| - | - | - | x | x | x | x | x | 用户 PIN 标识符 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 修改管理员 PIN |

#### C.2.2.3 命令报文数据域

当修改 PIN 时，使用 SM3 算法对旧 PIN 计算哈希值并取前 16 字节作为子密钥。

当重置 PIN 时，使用 SM3 算法对管理员 PIN 计算哈希值并取前 16 字节作为子密钥。

利用子密钥对新 PIN 进行数据加密计算，再使用子密钥对命令报文计算 MAC，命令数据域包括

新 PIN 密文和 MAC。加密和 MAC 计算算法类型由主控密钥决定。命令数据域见表 C.77。

表 C.77 命令数据域

| 名称 | 长度 |
|---|---|
| 新 PIN 密文 | ‘10’ |
| MAC | ‘04’ |

如果 MAC 校验失败，PIN 的剩余次数减 1，并返回当前剩余次数（SW=‘63Cx’）。

#### C.2.2.4 响应报文数据域

响应报文数据域不存在。

#### C.2.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.78。

表 C.78 CHANGE PIN/ RELOAD PIN 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘63’ | ‘Cx’ | 验证失败，‘x’表示重试次数 |
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 长度不正确 |
| ‘69’ | ‘83’ | 验证 PIN 锁定 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘88’ | 未找到 PIN 数据 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.3 EXTERNAL AUTHENTICATE（外部鉴权）

#### C.2.3.1 定义和范围

EXTERNAL AUTHENTICATE 命令要求卡片中的应用验证 IFD 的有效性，以使 IFD 获得某种授权。EXTERNAL AUTHENTICATE 命令所使用的密钥（由 P2 参数指定）应满足可使用条件。验证失败，错误计数器减 1，并清除 KEY 对应的安全状态。连续失败达到错误计数器设定的最大值，所用密钥将被锁定。

#### C.2.3.2 命令报文

EXTERNAL AUTHENTICATE 命令报文见表 C.79。

表 C.79 EXTERNAL AUTHENTICATE 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘82’ |

| P1 | ‘00’ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| P2 | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 说　明 |
| | - | - | - | x | x | x | x | x | 密钥标识 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 当前 DF 下的 MK |
| Lc | ‘10’，采用 SM4 算法 | | | | | | | | |
| | ‘00’，返回当前剩余次数 | | | | | | | | |
| Data | 认证数据 | | | | | | | | |
| Le | 不存在 | | | | | | | | |

#### C.2.3.3　命令报文数据域

认证数据。

#### C.2.3.4　响应报文数据域

响应报文数据域不存在。

#### C.2.3.5　响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.80。

表 C.80 EXTERNAL AUTHENTICATE 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘63’ | ‘Cx’ | 认证失败，还可认证‘x’次 |
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘83’ | 认证密钥锁定 |
| ‘69’ | ‘84’ | 引用数据无效（未申请随机数） |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘88’ | 未找到密钥数据 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.4　GET CHALLENGE（获取随机数）

#### C.2.4.1　定义和范围

GET CHALLENGE 命令从卡片中读取与安全相关的随机数，用于其后的安全相关过程。GET CHALLENGE 命令不受安全条件限制，可以自由使用，但是其后的安全相关命令应紧接着执行，否则该随机数没有意义。

#### C.2.4.2　命令报文

GET CHALLENGE 命令报文见表 C.81。

表 C.81 GET CHALLENGE 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘84’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | 不存在 |
| Data | 不存在 |
| Le | ‘08’ 或‘10’ |

#### C.2.4.3 命令报文数据域

命令报文数据域不存在。

#### C.2.4.4 响应报文数据域

响应报文数据域中的数据说明见表 C.82。

表 C.82 响应报文数据域中的数据说明

| 说 明 | 长度（字节） |
|---|---|
| 随机数 | 8、16 |

#### C.2.4.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.83。

表 C.83 GET CHALLENGE 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Le 不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.5 GET RESPONSE（获取响应）

#### C.2.5.1 定义和范围

在 T=0 协议下，GET RESPONSE 命令提供了一种从卡片向 IFD 传送 APDU（或 APDU 的一部分）的传输方法。

#### C.2.5.2 命令报文

GET RESPONSE 命令报文见表 C.84。

表 C.84 GET RESPONSE 命令报文

| 代码 | 值 |
|---|---|

| | |
|---|---|
| CLA | ‘00’ |
| INS | ‘C0’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | 不存在 |
| Data | 不存在 |
| Le | 响应的最大数据长度 |

#### C.2.5.3 命令报文数据域

命令报文数据域不存在。

#### C.2.5.4 响应报文数据域

实际可用数据。

#### C.2.5.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.85。

表 C.85 GET RESPONSE 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Le 不正确 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6C’ | ‘xx’ | Le 不正确，‘xx’表示实际长度 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |
| ‘6F’ | ‘00’ | 数据无效 |

### C.2.6 READ BINARY（读取二进制内容）

#### C.2.6.1 定义和范围

READ BINARY 命令用于读出透明文件的内容。READ BINARY 命令的执行应满足相应文件的读条件和读属性。

#### C.2.6.2 命令报文

READ BINARY 命令报文见表 C.86。

表 C.86 READ BINARY 命令报文

| 代码 | 值 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CLA | ‘00’ | | | | | | | | |
| INS | ‘B0’ | | | | | | | | |
| P1 | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 说 明 |
| | 0 | x | x | x | x | x | x | x | 当前 EF 文件偏移地址高字节 |
| | 1 | 0 | 0 | x | x | x | x | x | 通过 SFI 方式访问 |
| P2 | 若 P1 的 b8=0，偏移地址低字节<br>若 P1 的 b8=1，偏移地址 | | | | | | | | |

| | |
|---|---|
| Lc | 不存在 |
| Data | 不存在 |
| Le | 期望返回的数据长度 |

#### C.2.6.3 命令报文数据域

命令报文数据域不存在。

#### C.2.6.4 响应报文数据域

响应报文数据域中的数据为明文数据。

#### C.2.6.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.87。

表 C.87 READ BINARY 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘69’ | ‘81’ | 当前文件不是透明文件 |
| ‘69’ | ‘82’ | 安全状态不满足 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘69’ | ‘86’ | 没有选择当前文件 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6B’ | ‘00’ | 起始地址超出范围 |
| ‘6C’ | ‘xx’ | Le 不正确。‘xx’表示实际长度 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.7 READ RECORD（读取记录内容）

#### C.2.7.1 定义和范围

READ RECORD 命令读记录文件中指定的记录。READ RECORD 命令的执行应满足相应文件的读条件和读属性。

#### C.2.7.2 命令报文

READ RECORD 命令报文见表 C.88。

表 C.88 READ RECORD 命令报文

| 代码 | 值 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CLA | ‘00’ | | | | | | | | |
| INS | ‘B2’ | | | | | | | | |
| P1 | 记录号或记录标识符，记录号的取值范围为‘01’~‘FE’，‘00’表示当前记录 | | | | | | | | |
| P2 | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 说 明 |
| | 0 | 0 | 0 | 0 | 0 | - | - | - | 当前的 EF 文件 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | x | x | x | x | x | - | - | - | 用 SFI 方式 |
| | - | - | - | - | - | 1 | 0 | 0 | 读 P1 指定的记录 |
| | - | - | - | - | - | 1 | 0 | 1 | 从 P1 指定的记录开始读到最后一个记录 |
| | - | - | - | - | - | 1 | 1 | 0 | 从最后一个记录开始读到 P1 指定的记录 |
| | - | - | - | - | - | 0 | 0 | 0 | 读具有 P1 指定的记录标识符的第一个实例 |
| | - | - | - | - | - | 0 | 0 | 1 | 读具有 P1 指定的记录标识符的最后一个实例 |
| | - | - | - | - | - | 0 | 1 | 0 | 读具有 P1 指定的记录标识符的下一个实例 |
| | - | - | - | - | - | 0 | 1 | 1 | 读具有 P1 指定的记录标识符的上一个实例 |
| | 任何其他值 | | | | | | | | 保留 |
| Lc | 不存在 | | | | | | | | |
| Data | 不存在 | | | | | | | | |
| Le | 期望返回的明文字节数 | | | | | | | | |

### C.2.7.3 命令报文数据域

命令报文数据域不存在。

### C.2.7.4 响应报文数据域

响应报文数据域中的数据说明见表 C.89。

**表 C.89 响应报文数据域中的数据说明**

| 说　明 | 长度（字节） |
|---|---|
| 明文数据 | ‘xx’ |

### C.2.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.90。

**表 C.90 READ RECORD 错误状态码**

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘81’ | 当前文件不是记录文件 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘69’ | ‘86’ | 没有选择当前文件 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘83’ | 未找到记录 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |

| | | |
|---|---|---|
| ‘6C’ | ‘xx’ | Le 不正确，‘xx’表示实际长度 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.8 SELECT FILE（选择文件）

#### C.2.8.1 定义和范围

SELECT FILE 命令通过 FID 或 AID 来选择卡片中的 DF 或 EF 文件。

#### C.2.8.2 命令报文

SELECT FILE 命令报文见表 C.91。

表 C.91 SELECT FILE 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘A4’ |
| P1 | ‘00’通过 FID 选择 DF、EF<br>‘04’通过 AID 选择应用 |
| P2 | ‘00’ |
| Lc | 若 P1=‘00’，‘02’<br>若 P1=‘04’，‘05’—‘10’Data 域的数据长度 |
| Data | 若 P1=‘00’，FID（2 字节）<br>若 P1=‘04’，AID |
| Le | FCI 文件中信息的长度（选择 DF 时） |

#### C.2.8.3 命令报文数据域

命令报文数据域不存在。

#### C.2.8.4 响应报文数据域

响应报文数据域的结构见表 C.92 和表 C.93。

表 C.92 SELECT ACSE 的响应报文

| 标签 | | | | 存在方式 |
|---|---|---|---|---|
| ‘6F’ | FCI 模板 | | | M |
| | ‘84’ | DF 名 | | M |
| | ‘73’ | – FCI 数据专用模板 | | M |
| | | ‘92’ | 应用规范版本，2 字节 | M |
| **注：**表中的应用规范版本使用固定值‘33 30’。 | | | | |

表 C.93 SELECT ADF（证书应用）的响应报文

| 标志 | | 值 | 存在方式 |
|---|---|---|---|
| ‘6F’ | | FCI 模板 | M |

| | | | |
|---|---|---|---|
| | ‘84’ | DF 名 | M |

C.2.8.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.94。

表 C.94 SELECT FILE 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6E’ | ‘00’ | CLA 不正确 |

C.2.9 UPDATE BINARY（更新二进制内容）

C.2.9.1 定义和范围

UPDATE BINARY 命令用命令中给定的数据代替透明文件中已有的数据。UPDATE BINARY 命令的执行应满足相应文件的改写条件和改写属性。

C.2.9.2 命令报文

UPDATE BINARY 命令报文见表 C.95。

表 C.95 UPDATE BINARY 命令报文

| 代码 | 值 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CLA | ‘00’ | | | | | | | | |
| INS | ‘D6’ | | | | | | | | |
| P1 | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 说 明 |
| | 0 | x | x | x | x | x | x | x | 当前 EF 文件偏移地址高字节 |
| | 1 | 0 | 0 | x | x | x | x | x | 通过 SFI 方式访问 |
| P2 | 若 P1 的 b8=0，偏移地址低字节<br>若 P1 的 b8=1，偏移地址 | | | | | | | | |
| Lc | Data 域数据长度 | | | | | | | | |
| Data | 用来写入或修改用的数据 | | | | | | | | |
| Le | 不存在 | | | | | | | | |

C.2.9.3 命令报文数据域

命令报文数据域包括用来写入或修改用的数据。

C.2.9.4 响应报文数据域

响应报文数据域不存在。

C.2.9.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.96。

表 C.96 UPDATE BINARY 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘81’ | 当前文件不是透明文件 |
| ‘69’ | ‘82’ | 安全状态不满足 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘69’ | ‘86’ | 未选择文件 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6B’ | ‘00’ | 起始地址超出范围 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.10　UPDATE RECORD（更新记录内容）

#### C.2.10.1　定义和范围

UPDATE RECORD 命令用给定的数据代替记录文件中指定的记录。对循环定长记录文件，可以通过修改上一条记录的方式实现添加记录。UPDATE RECORD 命令的执行应满足相应文件的改写条件和改写属性。

#### C.2.10.2　命令报文

UPDATE RECORD 命令报文见表 C.97。

表 C.97 UPDATE RECORD 命令报文

| 代码 | 值 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CLA | ‘00’ | | | | | | | | |
| INS | ‘DC’ | | | | | | | | |
| P1 | 记录号或记录标识符，（‘00’，表示当前记录） | | | | | | | | |
| P2 | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 说　明 |
| | 0 | 0 | 0 | 0 | 0 | - | - | - | 当前的 EF 文件 |
| | x | x | x | x | x | - | - | - | 用 SFI 方式 |
| | - | - | - | - | - | 1 | x | x | 使用 P1 中的记录号 |
| | - | - | - | - | - | 1 | 0 | 0 | P1 指定记录号 |
| | - | - | - | - | - | 0 | x | x | 使用 P1 中的记录标识符 |
| | - | - | - | - | - | 0 | 0 | 0 | P1 指定标识的第一个实例 |
| | - | - | - | - | - | 0 | 0 | 1 | P1 指定标识的最后一个实例 |
| | - | - | - | - | - | 0 | 1 | 0 | P1 指定标识的下一个实例 |
| | - | - | - | - | - | 0 | 1 | 1 | P1 指定标识符的上一个实例 |
| | 任何其他值 | | | | | | | | 保留 |
| Lc | Data 域数据长度 | | | | | | | | |

| | |
|---|---|
| Data | 添加或修改原有记录的新记录 |
| Le | 不存在 |

#### C.2.10.3 命令报文数据域

添加或修改原有记录的新记录。

#### C.2.10.4 响应报文数据域

响应报文数据域不存在。

#### C.2.10.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.98。

表 C.98 UPDATE RECORD 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘65’ | ‘81’ | 内存错误 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘81’ | 当前文件不是记录文件 |
| ‘69’ | ‘82’ | 安全状态不满足 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘69’ | ‘86’ | 未选择文件 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 未找到文件 |
| ‘6A’ | ‘83’ | 未找到记录 |
| ‘6A’ | ‘85’ | Lc 与 TLV 结构不匹配 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.11 VERIFY PIN（校验）

#### C.2.11.1 定义和范围

VERIFY PIN 命令要求卡片对终端提供的 PIN 与卡片中存放的参考 PIN 做比较验证。执行 VERIFY PIN 命令前，应满足 PIN 的可使用条件。验证失败，错误计数器减 1，并清除 PIN 对应的安全状态。连续失败达到错误计数器设定的最大值时，PIN 将被锁定。

#### C.2.11.2 命令报文

VERIFY PIN 命令报文见表 C.99。

表 C.99 VERIFY PIN 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘00’ |
| INS | ‘20’ |
| P1 | ‘01’ |

| P2 | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 说　明 |
|---|---|---|---|---|---|---|---|---|---|
| | 1 | 0 | 0 | | | | | | 用户 PIN |
| | - | - | - | x | x | x | x | x | 口令标识 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 管理员 PIN |
| Lc | ‘00’/‘10’ | | | | | | | | |
| Data | 见 C.2.11.3 | | | | | | | | |
| Le | 不存在 | | | | | | | | |

### C.2.11.3　命令报文数据域

卡片应先发送 GET CHALLENGE 命令取随机数，若取 8 字节随机数，则后补‘00’至 16 字节；若取 16 字节随机数，则直接使用。

对 PIN 明文做 SM3 哈希计算，取哈希计算结果的前 16 字节作为加密密钥对卡片随机数进行加密，加密算法为 SM4 ECB，加密结果作为命令报文数据域。

Lc=‘00’时，命令报文数据域不存在。

### C.2.11.4　响应报文数据域

响应报文数据域不存在。

### C.2.11.5　响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.100。

表 C.100 VERIFY PIN 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘63’ | ‘Cx’ | 当前剩余次数。‘x’表示重试次数 |
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘83’ | 认证 PIN 锁定 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘88’ | 未找到 PIN 数据 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

## C.2.12　GENERATE KEY PAIR（生成SM2密钥对）

### C.2.12.1　定义和范围

GENERATE KEY PAIR 用于产生 SM2 密钥对，同时将私钥和公钥分别存放在指定文件中。满足公私钥文件的更新权限。

### C.2.12.2　命令报文

GENERATE KEY PAIR 命令报文见表 C.101。

表 C.101 GENERATE KEY PAIR 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘40’ |
| P1 | ‘00’ |
| P2 | ‘00’ |
| Lc | ‘08’ |
| Data | 指定存放公私钥的文件 FID 数据元 |
| Le | 不存在 |

#### C.2.12.3 命令报文数据域

公钥文件 FID 数据元和私钥文件 FID 数据元，其格式分别见表 C.102 和表 C.103。

表 C.102 公钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C0’ | ‘02’ | 公钥文件 FID |

表 C.103 私钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C2’ | ‘02’ | 私钥文件 FID |

#### C.2.12.4 响应报文数据域

响应报文数据域不存在。

#### C.2.12.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.104。

表 C.104 GENERATE KEY PAIR 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 文件未找到 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘89’ | 文件类型（密钥长度）与当前操作不匹配 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.13 GET PUBLIC KEY（导出公钥）

#### C.2.13.1 定义和范围

GET PUBLIC KEY 用于导出指定公钥，应使用指定私钥对该公钥进行保护。满足公钥文件的读

权限和指定私钥文件的使用权限。

### C.2.13.2 命令报文

GET PUBLIC KEY 命令报文见表 C.105。

表 C.105 GET PUBLIC KEY 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘C9’ |
| P1 | 见表 C.106 |
| P2 | 见表 C.107 |
| Lc | 数据长度 |
| Data | 见 C.2.13.3 |
| Le | ‘00’：按实际计算结果长度返回 |

命令报文中的控制参数见表 C.106 和表 C.107。

表 C.106 P1 参数说明

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含 义 |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | RFU |
| 1 | - | - | - | - | - | - | - | 导出 SM2 公钥 |
| | 0 | 0 | - | - | - | - | - | 对公钥签名导出 |
| | x | x | - | - | - | - | - | RFU |
| | | | x | x | x | - | - | RFU |
| | | | | | | 1 | 0 | SM2 |
| | | | | | | x | x | RFU |

表 C.107 P2 参数说明

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含 义 |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | 第一次命令，有命令数据域，响应数据为数字签名数据 |
| 1 | - | - | - | - | - | - | - | 第二次命令，无命令数据域，响应数据为公钥参数数据 |
| | x | x | x | x | x | x | x | RFU |

### C.2.13.3 命令报文数据域

公钥文件 FID 数据元和私钥文件 FID 数据元，其格式分别见表 C.108 和表 C.109。

表 C.108 公钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C0’ | ‘02’ | 公钥文件 FID |

表 C.109 私钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C2’ | ‘02’ | 签名私钥文件 FID |

C.2.13.4 响应报文数据域

响应报文数据域中的数据：包括公钥数据元和数字签名数据元，其格式分别见表C.110和表C.111。

表 C.110 SM2 公钥参数数据元格式

| T | L | V |
|---|---|---|
| ‘C3’ | ‘40’ | SM2 公钥值（高字节在前，低字节在后） |

表 C.111 数字签名数据元格式

| T | L | V |
|---|---|---|
| ‘C1’ | ‘40’ | SM2 数字签名 |

C.2.13.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.112。

表 C.112 GET PUBLIC KEY 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘01’ | 块链接错误 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 文件未找到 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘89’ | 文件类型（密钥长度）与当前操作不匹配 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

C.2.14 STORE PKI KEY（导入SM2密钥对）

C.2.14.1 定义和范围

STORE PKI KEY 用于导入 SM2 公私钥到指定文件中，应支持使用卡片内对称会话密钥加密导入公私钥。如选择密文导入，则执行指令前应先生成或导入对称会话密钥。应满足文件的更新权限。

C.2.14.2 命令报文

STORE PKI KEY 命令报文见表 C.113。

表 C.113 STORE PKI KEY 命令报文

| 代码 | 值 |
|---|---|

| | |
|---|---|
| CLA | ‘80’ |
| INS | ‘C2’ |
| P1 | 见表 C.114 |
| P2 | ‘00’：导入公钥；<br>‘01’：导入私钥；<br>其他值：RFU。 |
| Lc | 数据长度 |
| Data | 见 C.2.14.3 |
| Le | 无 |

命令报文中的控制参数见表 C.114。

表 C.114 P1 参数说明

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含　义 |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | 明文导入 |
| 1 | - | - | - | - | - | - | - | 密文导入 |
| | 0 | - | - | - | - | - | - | 小端格式 |
| | 1 | - | - | - | - | - | - | 大端格式 |
| | | x | x | x | x | - | - | 会话密钥索引 0～4 |
| | | | | | | x | x | RFU |

**注：**大小端格式指的是公私钥明文或加密前的数据格式，如果是密文导入，输入的密文是高字节在前、低字节在后。

### C.2.14.3　命令报文数据域

包含公钥或私钥文件 FID 以及公私钥参数。若 P1.b8=0，则公私钥参数是明文；若 P1.b8=1，则公私钥参数值由事先生成或导入的对称会话密钥加密导入，但 Tag 和 Length 字段是明文。公钥和私钥文件 FID 数据元分别见表 C.115 和表 C.116。公私钥参数明文和密文数据元格式分别见表 C.117 和表 C.118。

表 C.115 公钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C0’ | ‘02’ | 公钥文件 FID |

表 C.116 私钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C2’ | ‘02’ | 私钥文件 FID |

表 C.117 公私钥参数明文数据元格式

| T | L | V |
|---|---|---|
| ‘CA’ | ‘40’ | 公钥 |
| ‘CB’ | ‘20’ | 私钥 |

表 C.118 公私钥参数密文数据元格式

| T | L | V |
|---|---|---|
| ‘CA’ | ‘40’ | 公钥密文（高字节在前，低字节在后） |
| ‘CB’ | ‘20’ | 私钥密文（高字节在前，低字节在后） |

#### C.2.14.4 响应报文数据域

响应报文数据域不存在。

#### C.2.14.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.119。

表 C.119 STORE PKI KEY 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘84’ | 引用数据无效 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 文件未找到 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘88’ | 未找到密钥数据 |
| ‘6A’ | ‘89’ | 文件类型（密钥长度）与当前操作不匹配 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.15 PUBLIC KEY OPERATION（加密/验签）

#### C.2.15.1 定义和范围

PUBLIC KEY OPERATION 用于使用 SM2 公钥进行加密/验签计算。需要满足公钥的使用权限。

#### C.2.15.2 命令报文

PUBLIC KEY OPERATION 命令报文见表 C.120。

表 C.120 PUBLIC KEY OPERATION 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘4C’ |
| P1 | ‘00’ |
| P2 | ‘00’：SM2 公钥验签；<br>‘01’：SM2 公钥加密；<br>其他值：RFU。 |
| Lc | SM2 验签操作：<br>Lc=‘06’+公钥文件 FID 长度+Hash 值长度+签名长度。 |

| | |
|---|---|
| | SM2 加密操作：<br>Lc=‘06’+公钥文件 FID 长度+待加密数据长度。 |
| Data | 待计算数据 |
| Le | ‘00’：按实际计算结果长度返回或无 |

#### C.2.15.3 命令报文数据域

指定公钥文件 FID 和计算数据块，采用 TLV 格式。公钥文件 FID 数据元格式见表 C.121。SM2 验签和加密计算输入数据块数据元格式分别见表 C.122 和表 C.123。

表 C.121 公钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C0’ | ‘02’ | 公钥文件 FID |

表 C.122 SM2 验签计算输入数据块数据元格式

| T | L | V |
|---|---|---|
| ‘C1’ | ‘820060’ | Hash 值+数字签名 |

表 C.123 SM2 加密计算输入数据块数据元格式

| T | L | V |
|---|---|---|
| ‘C1’ | ‘82xxxx’ | 待加密数据，‘xxxx’表示数据字节长度，1-160 字节。 |

#### C.2.15.4 响应报文数据域

响应报文数据域中的数据：加密操作时，返回加密结果；验签操作时，无响应数据。

#### C.2.15.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.124。

表 C.124 PUBLIC KEY OPERATION 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 文件未找到 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘89’ | 文件类型（密钥长度）与当前操作不匹配 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.16 PRIVATE KEY OPERATION（解密/签名）

#### C.2.16.1 定义和范围

PRIVATE KEY OPERATION 用于使用 SM2 私钥进行解密/签名计算。需要满足私钥使用权限。

### C.2.16.2 命令报文

PRIVATE KEY OPERATION 命令报文见表 C.125。

表 C.125 PRIVATE KEY OPERATION 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘4E’ |
| P1 | ‘00’ |
| P2 | ‘00’：SM2 私钥签名；<br>‘01’：SM2 私钥解密；<br>其他值：RFU。 |
| Lc | SM2 签名操作：<br>Lc=‘06’+私钥文件 FID 长度+待签名数据长度。<br>SM2 解密操作：<br>Lc=‘06’+私钥文件 FID 长度+待解密数据长度。 |
| Data | 见 C.2.16.3 |
| Le | ‘00’：按实际计算结果长度返回 |

### C.2.16.3 命令报文数据域

指定私钥文件 FID 和计算数据块，采用 TLV 格式。私钥文件 FID 数据元格式见表 C.126。SM2 签名和解密计算输入数据块数据元格式分别见表 C.127 和表 C.128。

表 C.126 私钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C2’ | ‘02’ | 私钥文件 FID |

表 C.127 SM2 签名计算输入数据块数据元格式

| T | L | V |
|---|---|---|
| ‘C1’ | ‘820020’ | Hash 值 |

表 C.128 SM2 解密计算输入数据块数据元格式

| T | L | V |
|---|---|---|
| ‘C1’ | ‘82xxxx’ | 待解密数据，‘xxxx’表示数据字节长度，97-247 字节。 |

### C.2.16.4 响应报文数据域

响应报文数据域中的数据：签名结果或解密结果。

### C.2.16.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.129。

表 C.129 PRIVATE KEY OPERATION 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘80’ | 数据域参数不正确（数据大于模数 N） |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 文件未找到 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘89’ | 文件类型（密钥长度）与当前操作不匹配 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E ‘ | ‘00 ‘ | CLA 不正确 |

### C.2.17　GENERATE ENVELOP（生成数字信封）

#### C.2.17.1　定义和范围

GENERATE ENVELOP 用于内部生成对称会话密钥保存到 RAM 中并导出。

如果指定索引位置密钥不存在，则产生一个随机密钥导出并将该密钥保存在 RAM 中。

——RAM 中应有足够空间保存会话密钥；

——应满足加密公钥的使用权限。

#### C.2.17.2　命令报文

GENERATE ENVELOP 命令报文见表 C.130。

表 C.130 GENERATE ENVELOP 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘D8’ |
| P1 | ‘02’：SM4；<br>其他值：RFU。 |
| P2 | 见表 C.131 |
| Lc | ‘04’/无 |
| Data | 加密导出：公钥文件 FID 数据元<br>明文导出：无 |
| Le | 会话密钥明文或密文长度 |

命令报文中的控制参数见表 C.131。

表 C.131 P2 参数说明

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含　义 |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | 明文 |
| 1 | - | - | - | - | - | - | - | 密文 |
|  | 0 | 1 | - | - | - | - | - | SM2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | x | x | - | - | - | - | - | RFU |
| | | | x | x | - | - | - | RFU |
| | | | | | x | x | x | 索引号（0~4） |

C.2.17.3 命令报文数据域

密文导出时，命令数据域包括用于加密的公钥文件 FID 数据元，说明见表 C.132。

表 C.132 命令数据域说明

| T | L | V |
|---|---|---|
| ‘C0’ | ‘02’ | 公钥文件 FID |

C.2.17.4 响应报文数据域

响应报文数据域中的数据：密钥值明文或密文，数据格式为高字节在前，低字节在后，说明见表 C.133。

表 C.133 响应数据说明

| T | L | V |
|---|---|---|
| ‘C1’ | ‘xx’ | 密钥值密文 |

C.2.17.5 响应报文状态码

此命令执行成功的状态码是‘9000’。响应报文数据域中可能的状态码见表 C.134。

表 C.134 GENERATE ENVELOP 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 文件未找到 |
| ‘6A’ | ‘84’ | 空间不足 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘89’ | 文件类型（密钥长度）与当前操作不匹配 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

C.2.18 OPEN ENVELOP（打开数字信封）

C.2.18.1 定义和范围

OPEN ENVELOP 用于使用明文或加密方式导入对称会话密钥，该会话密钥保存在卡片内易失性存储器中（卡片内最多同时保存 5 条会话密钥），卡片掉电后自动失效。密钥在应用目录重新选择后继续有效，也可以删除指定会话密钥。

——加密导入时，应满足解密用私钥的使用权限；

——删除指定会话密钥时，如该索引号对应的密钥不存在，返回‘9000’。

### C.2.18.2 命令报文

OPEN ENVELOP 命令报文见表 C.135。

表 C.135 OPEN ENVELOP 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘4A’ |
| P1 | ‘02’：SM4；<br>‘FF’：删除指定的会话密钥；<br>其他值：RFU。 |
| P2 | 见表 C.136 |
| Lc | 会话密钥明文或密文长度 |
| Data | P1=‘FF’：无<br>P1=其他值：会话密钥明文或密文 |
| Le | P1=‘FF’：无<br>P1=其他值：‘01’ |

命令报文中的控制参数见表 C.136。

表 C.136 P2 参数说明

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含　义 |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | 明文 |
| 1 | - | - | - | - | - | - | - | 密文 |
| | 0 | 1 | - | - | - | - | - | SM2 |
| | x | x | - | - | - | - | - | RFU |
| | | | 0 | - | - | - | - | 会话密钥明文为小端模式 |
| | | | 1 | - | - | - | - | 会话密钥明文为大端模式 |
| | | | | x | x | x | x | 索引号（00：增加新密钥；1~5：指定密钥索引号+1） |

### C.2.18.3 命令报文数据域

如果是密文导入会话密钥，数据域为指定私钥文件 FID 和待解密数据块，否则数据域为会话密钥明文数据元。格式采用 TLV 格式。私钥文件 FID 数据元格式见表 C.137。会话密钥明文数据元格式见表 C.138。SM2 算法计算的会话密钥密文数据元格式见表 C.139。

表 C.137 私钥文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C2’ | ‘02’ | 私钥文件 FID |

表 C.138 会话密钥值明文数据元格式

| T | L | V |
|---|---|---|

| | | |
|---|---|---|
| ‘C1’ | ‘xx’ | 会话密钥值明文 |

表 C.139 SM2 算法计算的会话密钥密文数据元格式

| T | L | V |
|---|---|---|
| ‘C1’ | ‘82xxxx’ | 会话密钥密文，‘xxxx’为密文长度 |

注：输入的会话密钥数据是高字节在前，低字节在后。

#### C.2.18.4 响应报文数据域

响应报文数据域中的数据：如果是导入会话密钥成功，返回会话密钥索引号（0-4）。

#### C.2.18.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.140。

表 C.140 OPEN ENVELOP 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘69’ | ‘85’ | 使用条件不满足 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 文件未找到 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘89’ | 文件类型（密钥长度）与当前操作不匹配 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.19 CIPHER DATA（数据加解密）

#### C.2.19.1 定义和范围

CIPHER DATA 用于使用对称会话密钥对数据（满足分组长度的整数倍，卡片内不做填充处理）进行加解密。

#### C.2.19.2 命令报文

CIPHER DATA 命令报文见表 C.141。

表 C.141 CIPHER DATA 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘FA’ |
| P1 | ‘00’ 唯一数据块<br>‘01’ 第一个数据块<br>‘02’ 中间数据块<br>‘03’ 末尾数据块 |

| | |
|---|---|
| | 其他：RFU |
| P2 | P1=‘00’/‘01’：P2 见表 C.142；<br>P1=‘02’/‘03’：P2=‘00’； |
| Lc | 输入数据长度 |
| Data | 见 C.2.19.3 |
| Le | ‘00’：按实际计算结果长度返回 |

命令报文中的控制参数见表 C.142。

表 C.142 P2 参数说明

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含　义 |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | 加密操作 |
| 1 | - | - | - | - | - | - | - | 解密操作 |
| | 1 | 0 | - | - | - | - | - | 使用已导入的会话密钥 |
| | x | x | - | - | - | - | - | RFU |
| | | | x | - | - | - | - | RFU |
| | | | | 0 | 0 | 0 | - | 算法由密钥记录中的算法标识指定 |
| | | | | | | | 0 | ECB 模式 |
| | | | | | | | 1 | CBC 模式 |

### C.2.19.3　命令报文数据域

——ECB 模式：

1) 唯一块/首块的数据：4 字节密钥 ID+待计算数据；

2) 中间块/末尾块的数据：待计算数据。

——CBC 模式：

1) 唯一块/首块的数据：4 字节密钥 ID+IV+待计算数据；

2) 中间块/末尾块的数据：待计算数据。

### C.2.19.4　响应报文数据域

响应报文数据域中的数据：加解密计算结果。

### C.2.19.5　响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.143。

表 C.143 CIPHER DATA 错误状态码

| SW1 | SW2 | 含　义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘01’ | 块链接错误 |
| ‘6A’ | ‘80’ | 数据域参数不正确 |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘88’ | 未找到密钥数据 |

| | | |
|---|---|---|
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

### C.2.20 HASH OPERATION（哈希运算）

#### C.2.20.1 定义和范围

HASH OPERATION 用安全散列算法 SM3 将数据压缩为固定长度字节。有卡内数据参与计算时，对于一次计算过程只允许出现一次，可在任意的分块指令中指定卡内文件。

#### C.2.20.2 命令报文

HASH OPERATION 命令报文见表 C.144。

表 C.144 HASH OPERATION 命令报文

| 代码 | 值 |
|---|---|
| CLA | ‘80’ |
| INS | ‘C4’ |
| P1 | 见表 C.145 |
| P2 | ‘03’：SM3<br>其他值：RFU。 |
| Lc | 待计算数据长度 |
| Data | 待计算数据 |
| Le | ‘00’：按压缩算法输出长度返回结果或无 |

命令报文中的控制参数见表 C.145。

表 C.145 P1 参数说明

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | 含 义 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | - | - | - | - | - | - | 数据来自卡外 |
| 0 | 1 | - | - | - | - | - | - | 数据来自卡内指定文件 |
| 1 | 0 | - | - | - | - | - | - | 数据来自卡外和卡内指定文件 |
| 1 | 1 | - | - | - | - | - | - | 保留 |
| | | x | x | x | x | - | - | RFU |
| | | | | | | 0 | 0 | 首块 |
| | | | | | | 0 | 1 | 仅此一块 |
| | | | | | | 1 | 0 | 中间块 |
| | | | | | | 1 | 1 | 最后一块 |

#### C.2.20.3 命令报文数据域

当用于 Hash 计算数据有来自卡内的数据时，命令数据域中应包括卡内数据文件的 FID。

有卡外输入数据和卡内文件数据时，按卡外输入数据在前，卡内数据在后组织所有的数据计算 Hash 值。

对于卡内数据文件，其类型应为透明文件（二进制文件）。

若命令数据域中包含卡外输入数据，不管是“第一块”、“唯一块”、“中间块”、“结尾块”，

“卡外输入数据块数据元”的 T 和 L 总是存在。

卡内数据文件 FID 数据元格式见表 C.146。Hash 计算输入数据块数据元格式见表 C.147。

表 C.146 卡内数据文件 FID 数据元格式

| T | L | V |
|---|---|---|
| ‘C0’ | ‘02’ | 数据文件 FID |

表 C.147 Hash 计算输入数据块数据元格式

| T | L | V |
|---|---|---|
| ‘C1’ | ‘xx’ | 输入数据块，高字节在前，低字节在后 |

### C.2.20.4 响应报文数据域

响应报文数据域中的数据：如果 P1 的最低位是 1，返回数据压缩的结果（非 TLV 结构，高字节在前，低字节在后），否则无响应报文数据域数据。

### C.2.20.5 响应报文状态码

此命令执行成功的状态码是‘9000’。卡片可能回送的错误状态码见表 C.148。

表 C.148 HASH OPERATION 错误状态码

| SW1 | SW2 | 含 义 |
|---|---|---|
| ‘67’ | ‘00’ | Lc 不正确 |
| ‘69’ | ‘01’ | 块链接错误 |
| ‘69’ | ‘82’ | 不满足安全状态 |
| ‘6A’ | ‘80’ | 数据域参数不正确（出现多个卡内文件） |
| ‘6A’ | ‘81’ | 功能不支持 |
| ‘6A’ | ‘82’ | 文件未找到 |
| ‘6A’ | ‘86’ | P1、P2 参数不正确 |
| ‘6A’ | ‘89’ | 文件类型（密钥长度）与当前操作不匹配 |
| ‘6D’ | ‘00’ | 命令不存在 |
| ‘6E’ | ‘00’ | CLA 不正确 |

# 附 录 D
（规范性）
实体社会保障卡应用数据项

## D.1 社会保障卡应用数据项

### D.1.1 基本应用数据区

基本应用数据是指在社会保障卡的整个生命周期中不会改变的信息，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’），它们被组织成基本文件存于 SSSE 的 DDF 下,详见表 D.1。

表 D.1 基本应用数据区

| 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 | $UK_{SSSE}$ | 变长记录 | 启用 |
| 个人基本信息文件 | ‘EF06’ | ‘06’ | $RK_{SSSE}$ | $UK_{SSSE}$ | 变长记录 | 启用 |
| 指纹/指静脉数据文件 | ‘EF07’ | ‘07’ | $RK_{SSSE}$ | $UK_{SSSE}$ | 透明 | 预设 |
| 数字相片数据文件 | ‘EF08’ | ‘08’ | $RK_{SSSE}$ | $UK_{SSSE}$ | 透明 | 预设 |

### D.1.2 公共应用数据区

公共应用数据是指社会保障卡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～EF1A’），它们被组织成基本文件存在于标识符为‘DF01’的 DF 下，详见表 D.2。

表 D.2 公共应用数据区

| 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 $RK1_{DF01}$ | $UK1_{DF01}$ | 变长记录 | 启用 |
| 常住地信息文件 | ‘EF06’ | ‘06’ | PIN 或 $RK1_{DF01}$ | $UK4_{DF01}$ | 变长记录 | 启用 |
| 个人状况信息文件 | ‘EF07’ | ‘07’ | PIN 或 $RK1_{DF01}$ | $UK2_{DF01}$ | 变长记录 | 启用 |
| 婚姻状况信息文件 | ‘EF08’ | ‘08’ | PIN 或 $RK1_{DF01}$ | $UK3_{DF01}$ | 变长记录 | 启用 |
| 人员身份及就业单位信息文件 | ‘EF09’ | ‘09’ | PIN 或 $RK1_{DF01}$ | $UK2_{DF01}$ | 变长记录 | 启用 |
| 国家/地区及政治面貌信息文件 | ‘EF0A’ | ‘0A’ | PIN 或 $RK1_{DF01}$ | $UK5_{DF01}$ | 变长记录 | 启用 |
| 学历信息文件 | ‘EF15’ | ‘15’ | PIN 或 $RK1_{DF01}$ | $UK6_{DF01}$ | 变长记录 | 启用 |
| 预留信息文件 1 | ‘EF16’ | ‘16’ | 无 | $UK7_{DF01}$ | 透明 | 预留 |
| 预留信息文件 2 | ‘EF17’ | ‘17’ | 无 | $UK8_{DF01}$ | 透明 | 预留 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 预留信息文件 3 | ‘EF18’ | ‘18’ | 无 | $UK9_{DF01}$ | 透明 | 预留 |
| 预留信息文件 4 | ‘EF19 | ‘19’ | 无 | $UKA_{DF01}$ | 透明 | 预留 |
| 预留信息文件 5 | ‘EF1A’ | ‘1A’ | 无 | $UKB_{DF01}$ | 透明 | 预留 |

### D.1.3 就业与失业数据区

就业与失业应用数据是指社会保障卡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，详见表 D.3。

表 D.3 就业与失业数据区

| 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 $RK1_{DF02}$ | $UK1_{DF02}$ | 变长记录 | 预设 |
| 就业状况信息文件 | ‘EF06’ | ‘06’ | PIN 或 $RK1_{DF02}$ | $UK2_{DF02}$ | 变长记录 | 启用 |
| 就业记录信息文件 | ‘EF07’ | ‘07’ | PIN 或 $RK1_{DF02}$ | $UK3_{DF02}$ | 循环 | 启用 |
| 就业创业证信息文件 | ‘EF09’ | ‘09’ | PIN 或 $RK1_{DF02}$ | $UK4_{DF02}$ | 变长记录 | 启用 |
| 就业援助对象认定信息文件 | ‘EF15’ | ‘15’ | PIN 或 $RK1_{DF02}$ | $UK5_{DF02}$ | 变长记录 | 启用 |
| 就业扶持政策享受信息文件 | ‘EF16’ | ‘16’ | PIN 或 $RK1_{DF02}$ | $UK6_{DF02}$ | 循环 | 启用 |

### D.1.4 社会保险数据区1

本数据区中的应用数据是指社会保障卡中由人力资源和社会保障部门维护，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，详见表 D.4。

表 D.4 社会保险数据区 1

| 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 $RK2_{DF03}$ | $UK1_{DF03}$ | 变长记录 | 启用 |
| 劳动能力鉴定信息文件 | ‘EF06’ | ‘06’ | PIN 或 $RK1_{DF03}$ | $UK2_{DF03}$ | 变长记录 | 启用 |
| 养老保险信息文件 | ‘EF07’ | ‘07’ | PIN 或 $RK1_{DF03}$ | $UK3_{DF03}$ | 变长记录 | 启用 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 工伤保险信息文件 | ‘EF15’ | ‘15’ | PIN 或 $RK1_{DF03}$ | $UK4_{DF03}$ | 变长记录 | 启用 |
| 生育保险信息文件 | ‘EF16’ | ‘16’ | PIN 或 $RK1_{DF03}$ | $UK5_{DF03}$ | 变长记录 | 启用 |
| 工伤认定信息文件 | ‘EF17’ | ‘17’ | PIN 或 $RK1_{DF03}$ | $UK6_{DF03}$ | 变长记录 | 启用 |
| 供养亲属信息文件 | ‘EF18’ | ‘18’ | PIN 或 $RK1_{DF03}$ | $UK7_{DF03}$ | 变长记录 | 启用 |
| 参保凭证信息文件 | ‘EF19’ | ‘19’ | PIN 或 $RK1_{DF03}$ | $UK8_{DF03}$ | 定长记录 | 启用 |

### D.1.5 社会保险数据区2

本数据区中的应用数据是指社会保障卡中由人力资源和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（‘EF05’）、医疗保险临时脱网结算信息文件（‘EF06’）、医疗交易明细文件（‘EF08’）、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，详见表 D.5。

表 D.5 社会保险数据区 2

| 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 $RK1_{DF04}$ | $UK1_{DF04}$ | 变长记录 | 启用 |
| 医疗保险临时脱网结算信息文件 | ‘EF06’ | ‘06’ | PIN&$RK1_{DF04}$ | $UK2_{DF04}$ | 变长记录 | 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 $RK1_{DF04}$ | $UK2_{DF04}$ | 循环 | 启用 |

### D.1.6 人事与人才数据区

人事与人才数据是指社会保障卡中由人力资源和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，详见表 D.6。

表 D.6 人事与人才数据区

| 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’ | $RK1_{DF07}$ | $UK1_{DF07}$ | 变长记录 | 预设 |
| 专家信息文件 | ‘EF06’ | ‘06’ | $RK2_{DF07}$ | $UK2_{DF07}$ | 变长记录 | 预设 |
| 军队转业干部信息文件 | ‘EF07’ | ‘07’ | $RK3_{DF07}$ | $UK3_{DF07}$ | 变长记录 | 预设 |

## D.2 社会保障卡应用数据格式（建议最终统一删除）

社会保障应用数据格式详见表 D.7。

表 D.7 社会保障应用数据格式

| 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’ | | |
| ‘08’ | 社会保障号码 | an | ‘12’ | SSSE EF06 | 当数据的长度超过数据项‘09’的最大长度时，可以使用数据项‘4E’继续存储 |
| ‘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。固定存储 2 枚指纹，长度为“800”，指静脉或预留长度为“800” |
| — | 数字相片 | b | ‘2000’ | SSSE EF08 | 起始位置 0000。固定存储 1 张数字相片 |
| ‘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’ | | |

| 标志 | 数据项 | 类型 | 长度 | 所属文件 | 备注 |
|---|---|---|---|---|---|
| ‘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 |
| — | 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（职业技能等级）信息 1（见标志‘5A’-‘5E’） | B-TLV | ‘6C’ | | |
| ‘43’ | 职业资格（职业技能等级）信息 2（见标志‘5A’-‘5E’） | B-TLV | ‘6C’ | | |
| ‘5A’ | 职业资格（职业技能等级）名称代码 | an | ‘07’ | | |
| ‘5B’ | 职业资格（职业技能等级）等级 | an | ‘01’ | | |

| 标志 | 数据项 | 类型 | 长度 | 所属文件 | 备注 |
|---|---|---|---|---|---|
| ‘5C’ | 职业资格（职业技能等级）证书发证/年检机构名称 | an | ‘46’ | | |
| ‘5D’ | 职业资格（职业技能等级）证书发证/年检日期 | cn | ‘04’ | | |
| ‘5E’ | 职业资格（职业技能等级）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’ | | |
| - | 就业起始日期 | cn | ‘04’ | | |
| - | 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 | |

| 标志 | 数据项 | 类型 | 长度 | 所属文件 | 备注 |
|---|---|---|---|---|---|
| ‘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 | |
| ‘46’ | 申请鉴定（确认）事项 | an | ‘02’ | | |
| ‘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’ | | |

| 标志 | 数据项 | 类型 | 长度 | 所属文件 | 备注 |
|---|---|---|---|---|---|
| ‘4A’ | 申请确认事项 1<br>（见标志‘13‘—‘17‘） | B-TLV | ‘61’ | | |
| ‘4A’ | 申请确认事项 2<br>（见标志‘13‘—‘17‘） | B-TLV | ‘61’ | | |
| ‘4A’ | 申请确认事项 3<br>（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’ | | |
| ‘76’ | 供养关系 | cn | ‘01’ | | |
| ‘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<br>（见标志‘18‘—‘1E‘） | B-TLV | ‘27’ | DF03 EF19 | |

| 标志 | 数据项 | 类型 | 长度 | 所属文件 | 备注 |
|---|---|---|---|---|---|
| ‘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 | |
| ‘92’ | 脱网医疗费用结算累计金额 | cn | ‘04’ | | |
| ‘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’ | | |

| 标志 | 数据项 | 类型 | 长度 | 所属文件 | 备注 |
|---|---|---|---|---|---|
| - | 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’ | | |

## D.3 非对称认证应用数据及格式

非对称认证系统环境的文件结构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,详见表 D.8、表 D.9、表 D.10、表 D.11、表 D.12。

**表 D.8 非对称认证应用文件结构**

| 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 | $MK_{ACSE}$ | - |
| | ‘0004’ | 设备信息文件 | 透明 | 无 | $MK_{ACSE}$ | - |
| 社会保障证书应用 DF01 | ‘0001’ | 文件索引文件 | 定长记录 | 无 | $MK_{DF01}$ | - |
| | ‘0002’ | 容器索引文件 | 定长记录 | 无 | $MK_{DF01}$ | - |
| 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 |

表 D.9 应用索引文件

| 文件标识符 | ‘0001’ | SFI | ‘01’ | 读控制 | 无 | 写控制 | $MK_{ACSE}$ | 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：<br>“应用名称 1”为社会保障证书应用名称 “SS.CERT.ADF1”；<br>“应用名称 2”为预留证书应用名称，命名规则按照“RFU.CERT.ADF2”。 | | | | | | | | | |

表 D.10 设备信息文件

| 文件标识符 | ‘0004’ | SFI | ‘04’ | 读控制 | 无 | 写控制 | $MK_{ACSE}$ | 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：<br>“分组密码算法标识”为 0x00000413；<br>“非对称密码算法标识”为 0x00020500；<br>“密码杂凑算法标识”为 0x00000001；<br>“设备认证使用的分组密码算法标识”为 0x00000401。 | | | | | | | | | |

表 D.11 文件索引文件

| 文件标识符 | ‘0001’ | SFI | ‘01’ | 读控制 | 无 | 写控制 | $MK_{DF01}$ | 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’ |

**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‘C7A9C3FBB9ABD4BFCEC4BCFE00000000’（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‘C7A9C3FBCBBDD4BFCEC4BCFE00000000’（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。

表 D.12 容器索引文件

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 文件标识符 | ‘0002’ | SFI | ‘02’ | 读控制 | 无 | 写控制 | $MK_{DF01}$ | 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’ |
| ‘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。

# 参考文献

[1]GB/T 29263—2012 信息技术 面向服务的体系结构（SOA）应用的总体技术要求
[2]JR/T 0025—2018 中国金融集成电路（IC）卡规范
[3]LD/T 30—2009 人力资源社会保障电子认证体系规范
[4]《中国人民银行办公厅关于印发人民币银行结算账户管理系统银行机构代码信息管理规定的通知》（银办发〔2007〕75号）
[5]《中国人民银行 人力资源社会保障部关于社会保障卡银行业务应用有关事宜的通知》（银发〔2010〕348号）
[6]《人力资源社会保障部、中国人民银行关于社会保障卡加载金融功能的通知》（人社部发〔2011〕83号）
[7]《人力资源社会保障部关于开展社会保障卡持卡人员基础信息库建设的通知》（人社部发〔2014〕36号）
[8]《人力资源社会保障部关于加快推进社会保障卡应用的意见》（人社部发〔2014〕52号）
[9]《人力资源社会保障部办公厅关于印发人力资源社会保障数据中心应用系统安全管理规范的通知》（人社厅发〔2014〕47号）
[10]《人力资源社会保障部办公厅关于印发人力资源社会保障数据中心数据库安全管理规范的通知》（人社厅发〔2014〕48号）
[11]《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）
[12]《中国人民银行办公厅 人力资源社会保障部办公厅关于印发具有金融功能的第三代社会保障卡技术规范的通知》（银办发〔2017〕170号）
[13]《关于印发第三代社会保障卡相关技术规范的通知》（人社网信函〔2018〕1号）
[14]《人力资源社会保障部办公厅关于全面开展电子社会保障卡应用工作的通知》（人社厅发〔2019〕45号）
[15]《关于新增和完善社会保障卡持卡人员基础信息库服务功能的通知》（人社网信函〔2019〕23号）
[16]《关于印发<电子社会保障卡服务渠道管理办法（试行）>和<电子社会保障卡服务渠道接入安全技术规范（1.0版）>的通知》 （人社网信函〔2020〕22号）
[17]《人力资源社会保障部办公厅 中国人民银行办公厅关于推广应用具有金融功能的第三代社会保障卡的通知》（人社厅发〔2020〕101号）
[18]《关于规范第三代社会保障卡建设有关工作的通知》（人社网信函〔2021〕1号）