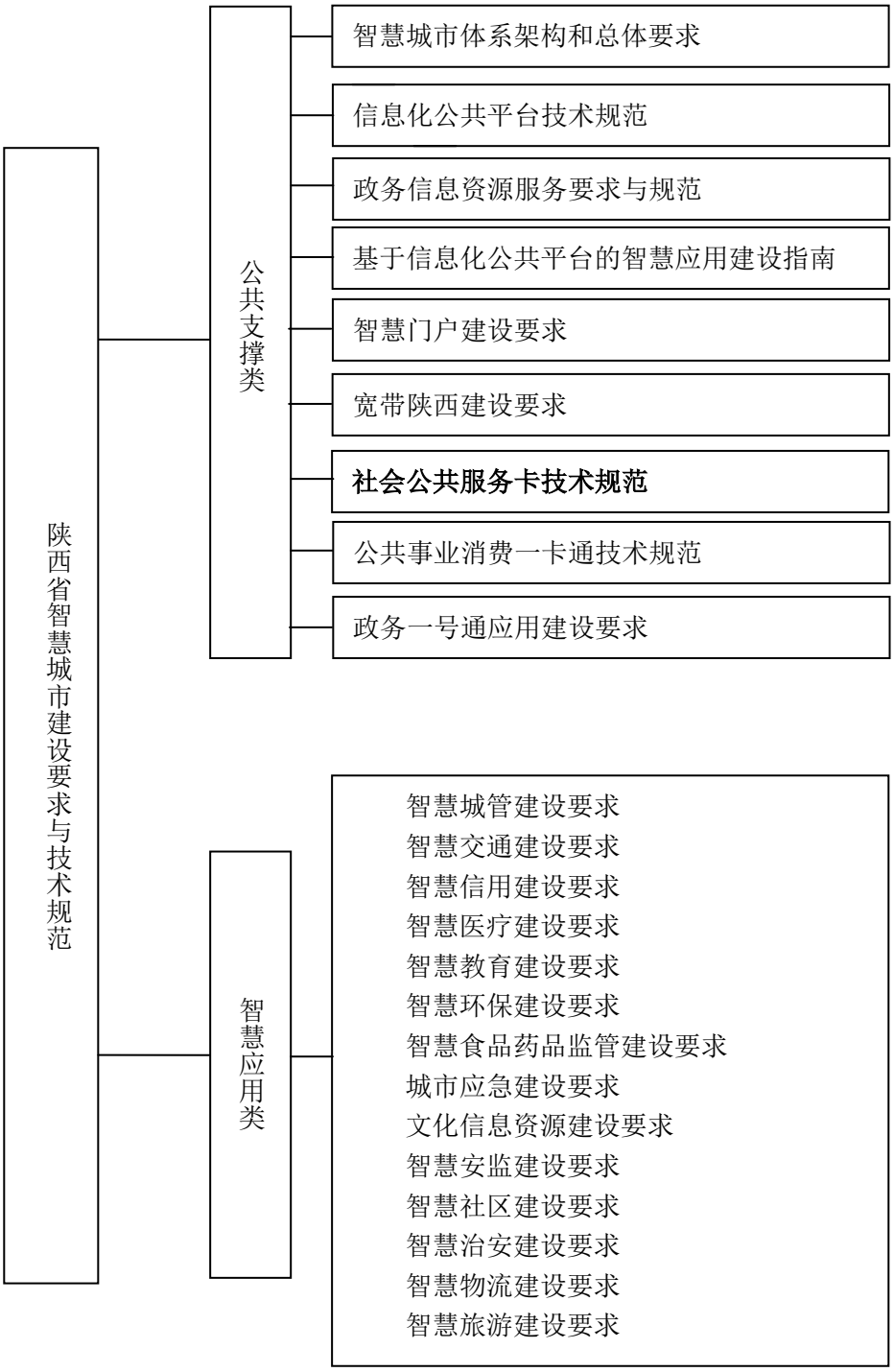
陕 西 省 智 慧 城 市 建 设 要 求 与 技 术 规 范

GF 61/T PT002—2014

社会公共服务卡技术规范

陕西省工业和信息化厅
陕西省卫生和计划生育委员会

陕西省智慧城市建设要求与技术规范体系图



前　言

本规范由陕西省信息化领导小组提出。

本规范由陕西省工业和信息化厅牵头。

本规范由陕西省信息化领导小组办公室归口。

本规范起草单位：陕西省信息化工程研究院、陕西省卫生和计划生育委员会、陕西省工业和信息化厅、西安邮电大学、陕西省人力资源和社会保障厅、陕西省财政厅、陕西省民政厅、宝鸡市工业和信息化局。

本规范由陕西省信息化工程研究院组织编制。

本规范按照GB/T 1.1-2009给出的规则起草。

本规范附录A、E、F为规范性附录，附录B、C、D为资料性附录。

引　言

智慧城市是新一轮信息技术变革和知识经济发展的产物，是信息化与工业化、城镇化的深度融合，并向更高阶段迈进的表现。为加快推进“数字陕西•智慧城市”建设，在国家和陕西省“十二五”信息化发展规划的框架下，制定和颁布了《“数字陕西•智慧城市”发展纲要（2013-2017年）》，用于指导“数字陕西•智慧城市”建设。

依据《“数字陕西•智慧城市”发展纲要（2013-2017年）》要求，陕西省信息化领导小组提出制定“数字陕西•智慧城市”系列规范，并由陕西省各业务主管部门牵头，陕西省信息化领导小组办公室归口，相关业务部门、企业和专家参与，陕西省信息化工程研究院负责组织编制。

本规范规定了陕西省社会公共服务卡的制作、发行、使用等活动，适用于陕西省社会公共服务卡所涉及的医疗卫生、社会保障、人口与计生等社会公共服务管理部门及银行、发卡机构等第三方机构和持卡人。

目　　次

1 范围

本规范规定了陕西省社会公共服务卡的制作、发行、使用等活动。

本规范适用于陕西省社会公共服务卡所涉及的医疗卫生、社会保障、人口与计生等社会公共服务管理部门及银行、发卡机构等第三方机构和持卡人。

陕西省社会公共服务卡是按纵向遵从、横向兼容原则规划设计，覆盖陕西省各类社会公共服务的身份识别卡。社会公共服务是指由各相关政府部门面向公众提供的各类社会保障性服务，主要包括城镇职工医疗保险、城镇居民医疗保险、新型农村合作医疗、养老保险、失业保险、工伤保险、区域卫生服务、人口与计生服务等。

陕西省社会公共服务卡在技术架构上满足国家相关部委社会保障类身份识别卡的技术要求和规范，兼顾省内各项社会公共服务，同时预留扩展空间，为今后增加和整合其它社会公共服务，如低保救助、伤残抚恤及第三方商业医疗保险等，提供技术支持，最终实现一卡多用和一卡通用。

注：除非特珠说明，以下各章节中的“社会公共服务卡”是指“陕西省社会公共服务卡”。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 11643-1999	公民身份证号码
GB 11714-1997	全国组织机构代码编制规则
GB/T 2260-2002	中华人民共和国行政区划代码
GB/T10114-2003	县以下行政区划代码编制规则
GB 2261.1-2003	人的性别代码
GB 3304-1991	中国各民族名称的罗马字母拼写法和代码
GB 4658-1984	文化程度代码
GB 2261.2-2003	婚姻状况代码
GB 2261.3-2003	健康状况代码
GA 324.6-2001	血型
GB 6864-2003	中华人民共和国学位代码
GB/T 7408-2005	数据元和交换格式、信息交换、日期和时间表示法
GB/T 15120-1994	识别卡 记录技术
GB 8561-2001	专业技术职务代码
GB/T 12402-2000	经济类型分类与代码
GB/T 16835-1997	高等学校本科、专科专业名称代码
ISO 7064:1983	效验码计算方法
GA342.1-2001	户口类别代码
GB/T16649.1-2006	识别卡 带触点的集成电路卡 第1部 物理特性
GB/T16649.2-2006	识别卡 带触点的集成电路卡 第2部分 触点的尺寸和位置
GB/T16649.3-2006	识别卡 带触点的集成电路卡 第3部分 电信号和传输协议
GB/T 16649.4-2010	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 16649.5-2002	识别卡 带触点的集成电路卡 第5部分
GB/T 16649.6-2002	识别卡 带触电的集成电路卡 第6部分 行业间数据元

GB/T 16649.8-2002	识别卡 带触点的集成电路卡 第8部分：与安全相关的行业间命令
ISO/IEC 14443-2008	识别卡 非接触式集成电路卡—接近式卡
ISO/IEC10536.1-1992	识别卡 无触点集成电路卡—第1部分：物理特性
ISO/IEC10536.2-1995	识别卡 无触点集成电路卡—第2部分：耦合区域的尺寸和位置
ISO/IEC 7810-2003	识别卡 物理特性
ISO 7498-2:1989	网络安全协议2
ISO/IEC 7811/2	卡识别记录技术2
JR/T0008-2000	银行卡发卡行标识代码及卡号
GB/T 6565-2009	职业分类与代码
GB/T 18347-2001	128条形码
LB002.1-2000	《 社会保障（个人）卡规范》-IC卡规范
LB002.2-2000	《 社会保障（个人）卡规范》-应用规范
LB002.3-2000	《 社会保障（个人）卡规范》-终端规范
GB/T 14504	银行卡
JR/T 00520-2010	银行卡片规范
WS XXXXX.1-2012	《居民健康卡技术规范》
WS XXXXX.2-2012	《居民健康卡技术规范》（修订版）
陕工信发【2011】21号	《城市一卡通技术规范（试行）》
Global Platform Specification	The Standard For Managing Applications On Secure Chip Technology
Java Card Platform Specification	Java Card technology is the leading open, interoperable platform for smart cards and secure tokens

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

智能卡 smart card

卡内的集成电路包括中央处理器（CPU）、可编程只读存储器（EEPROM）、闪速存储器、随机存储器（RAM）和固化在只读存储器（ROM）中的卡片操作系统（COS）。

3.1.2

多应用卡 multi-application card

遵从GB/T 16649标准、用于跨行业多应用领域的、计算机可识别的卡片。

3.1.3

双界面卡 dual interface card

是由聚氯乙烯（PVC）层合芯片线圈而成，基于接触式与非接触式双芯片为一体的双界面智能卡，可以通过接触方式的访问，也可以通过相隔一定距离，以射频方式来访问。接触式界面符合GB/T 16649；非接触式界面符合ISO/IEC 14443。

3.1.4

持卡人 card holder

持有社会公共服务卡的人。在卡中包含关于持卡人的信息和各个业务应用的数据。

3.1.5

芯片 chip

指用于完成数据处理和存储功能的集成电路器件。

3.1.6

卡片操作系统 card operation system

芯片中存储和可运行的，以保护应用数据和程序的机密性和完整性，控制卡与外界信息交换为目的的嵌入式软件。

3.1.7

卡应用系统 card application system

可以与社会公共服务卡通讯的应用系统。

3.1.8

行业应用 industrial application

卡上行业应用的程序和数据。

3.1.9

卡号 card number

系统自动编发的持卡人唯一编号，由本体码与校验码两部分组成。本体码表示编码对象的号码；校验码则是附加在本体码后边的，用来校验本体码在输入过程中准确性的号码。

3.1.10

条形码 bar codes

由一组规则排列的条、空以及对应的字符组成的标记，“条”指对光线反射率较低的部分，“空”指对光线反射率较高的部分，这些条和空组成的数据表达一定的信息，并能够用特定的设备识读，转换成与计算机兼容的二进制和十进制信息。

3.1.11

终端 terminal

为处理社会公共服务而在服务网点安装的设备，用于与卡进行连接通信。

3.1.12

电子钱包 electronic purse

一种为方便持卡人小额消费而设计的金融IC卡应用。支持圈存、消费等交易。除圈存交易外，使用电子钱包进行的其它交易不产生记录明细，且均无需用个人身份识别码（PIN）码验证。

3.1.13

加密算法 cryptographic algorithm

为了隐藏或显现数据信息内容的变换算法。

3.1.14

对称加密算法 symmetric cryptographic algorithm

加密密钥可以从解密密钥中推算出来，反过来也成立，在大多数算法中加/解密密钥是相同的。

3.1.15

非对称加密算法 asymmetric cryptographic algorithm

加密算法的加密密钥和解密密钥是不一样的，不能由一个密钥推导出另一个密钥。

3.1.16

密钥 key

控制加密转换操作的符号序列。

3.1.17

对称密钥 symmetric key

在对称加密算法中使用的密钥。

3.1.18

非对称密钥 asymmetric key

在非对称加密算法中使用的密钥，包括公钥和私钥。

3.1.19

公钥 public key

在一个实体使用的非对称密钥对中可以被公众使用的密钥。在数字签名方案中，公钥用于验证。

3.1.20

私钥 private key

在一个实体使用的非对称密钥对中仅被该实体使用的密钥。在数字签名方案中，私钥用于签名。

3.1.21

报文 message

由终端向卡或者卡向终端发出的，不含传输控制字符的字节串。

3.1.22

报文认证码 message authentication code

对交易数据及其相关参数运算后产生的代码。报文认证码主要用于验证报文的完整性。

3.1.23

命令 command

终端或者卡接受设备向卡发送的一条信息，启动一个操作或者请求一个响应。

3.1.24

响应 response

卡处理完成收到的命令报文后，返回给终端或者卡接受设备的报文。

3.1.25

记录 record

数据的集合。

3.1.26

数据信息 data information

数据信息包括共享数据、密钥和各个应用数据。

3.1.27

数据安全 security

指数据的机密性、完整性和有效性。

3.1.28

数据的完整性 data integrity

数据不能被以非授权的方式更改或破坏的属性。

3.1.29

机密性 confidentiality

信息不能被非授权个人、实体或流程得到或泄露。

3.1.30

数字签名 digital signature

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

3.1.31

应用协议数据单元 application protocol data unit

读卡器和智能卡之间的标准通信消息协议。

3.1.32

应用提供方 application provider

拥有应用并对应用的具体行为负责的实体。

3.1.33

卡片内容 card content

卡片内的代码和应用的信息(但不含应用的数据)，由OPEN负责管理，比如可执行加载文件，应用的实例等。

3.1.34

卡片管理器 card manager

负责对卡片进行管理的实体的统称，比如OPEN、发卡方安全域、持卡方验证方法服务提供方等。

3.1.35

委托管理 delegated management

由认证后的应用提供方来执行的、预先授权的对卡片内容进行改变的行动。

3.1.36

可执行加载文件 executable load file

实际存在于卡片上的包含一个或多个应用的可执行代码(可执行模块)的容器,它既可以驻留在只读内存中，也可以作为加载文件数据块的映像在可变内存中生成。

3.1.37

生命周期 life cycle

卡上卡片内容的存在以及不同阶段，也可以指卡片本身存在的各个阶段。

3.1.38

加载文件 load file

传送加载到卡片上的某种文件，包含了加载文件数据块以及一个或者多个数据鉴别块。

3.1.39

运行时环境 runtime environment

拥有全局平台注册表的卡片上的中心管理实体。

3.1.40

安全域 security domain

负责对某个卡外实体(例如发卡方、应用提供方、授权管理者)的管理、安全、通信需求进行支持的卡内实体。

3.1.41

令牌 token

发卡方出具的一个加密值，用来作为一个委托管理操作已经被授权进行的证据。

3.1.42

发卡方安全域 issuer security domain

负责对卡片管理者(通常是发卡方)的管理、安全、通信需求进行支持的卡上首要实体。

3.2 缩略语

下列缩略语适用于本文件。

ADF	应用专用文件（Application Definition File）
AID	应用标识（Application Identifier）
An	字母数字型（Alphanumeric）
ans	特殊字母数字型（Alphanumeric Special）
APDU	应用协议数据单元（Application Protocol Data Unit）
API	应用程序接口（Application Programming Interface）
ATR	复位应答（Answer To Reset）

b	二进制 （Binary）
BCD	二进制码的十进位数（Binary-Coded Decimal）
BER	基本编码规则（Basic Encoding Rules）
CAD	卡接受设备(Card Acceptance Device)
CBC	密码字组连接（Cipher Block Chaining）
CHVM	卡持有者确认方法（Card Holder Verification Method）
CIN	卡标识码（Card Identification Number）
CLA	命令报文的类字节（Class Byte of Command Message）
CLK	时钟信号输入（clock）
CMYK	印刷色彩模式（Cyan- Magenta-Yellow-blacK）
cn	压缩数字（Compressed Numeric）
COS	卡片操作系统（Card Operating System）
CPU	中央处理器（Central Processing Unit）
CRMI	基于 CPU 卡远程方法调用（CPU card Remote Method Invocation）
CVN	卡安全码（Card Verification Number）
DAP	数据鉴定模式（Data Authentication Procedure）
DDF	目录专用文件（Directory Definition File）
DEA	数据加密算法(Data Encryption Algorithm)
DEK	数据加密密钥（Data Encryption Key）
DES	数据加密标准（Data Encryption Standard）
DF	专有文件（Dedicated File）
DOS	磁盘操作系统（Disk Operating System）
ECB	电子码本（Electronic Code Book）
EEPROM	可编程只读存储器（Electrically Erasable Programmable Read-Only Memory）
EF	基本文件（Elementary File）
EMV	Europay，MasterCard 以及 Visa 的头三个字母；被用作支付系统的协议（Europay、MasterCard 和 Visa）
ENC	加密（Encoding）
Fc	射频工作场频率
FCI	文件控制信息（File Control Information）
FID	文件标识符（File Identifier）
GND	接地，基准电压
HEX	16 进制（Hexadecimal）
IAK	内部认证密钥（Internal Authentication key）
IC	集成电路（Integrated Circuit）
ICC	集成电路卡（Integrated Circuit Card）
ICCR	集成电路卡注册中心（Integrated Circuit Card Register）
ICV	初始连接向量（Initial Connection Vector）
ID	标识（Identifier）
IEC	国际电工委员会（International Electrotechnical Commission）
IIN	发行标识码（Issuance of Identification Number）
INS	报文指令字节（Instruction Byte of Command Message）
I/O	串行数据的输入/输出

ISO	国际标准化组织（International Organization for Standardization）
Lc	在要求发送命令时，命令数据的确切长度
LD	填充字符
Le	在要求返回数据时，响应数据的期望最大长度
LV	长度值（Length of Value）
MAC	报文鉴定码（Message Authentication Code）
MACK	MAC 计算密钥（MAC Computing Key）
MF	主文件（Master File）
O	可选型 （Optional）
OID	对象标识符（Object Identifier）
Package	CPU 卡上一些相关的应用程序聚集在一起的实体
P1	引用控制参数 1
P2	引用控制参数 2
PROC	中国人民银行（Peoples Bank of China）
PIN	个人识别码（Personal Identification Number）
PIX	私有标识扩展（Proprietary Identifier Extension）
SAM	安全存取模块（Secure Access Module）
PSE	金融接触式支付环境（Payment System Environment）
PPSE	金融非接触式支付系统环境（Proximity Payment Systems Environment）
PVC	聚氯乙烯（Polyvinyl Chloride）
RAM	随机访问存储器（Random Access Memory）
RFU	保留以备将来使用
RID	资源标识（Resource Identifier）
ROM	只读存储器（Read-Only Memory）
RSA	非对称算法（Ron Rivest、Adi Shamirh 和 LenAdleman）
RS232	串行物理通信接口
RST	复位信号输入
SAM	安全存取模块（Secure Access Module）
SCP	安全信道协议（Secure Channel Protocol）
SW	状态字（Status Word）
TK	传输密钥（Transport Key）
TLV	标签长度值（Tag Length Value）
USB	通用串行总线通信接口（Universal Serial Bus）
VCC	电源电压输入
VPP	编程电压输入

4 卡号与业务号编码规则

社会公共服务卡的卡面号码采用一定的编码规则进行统一编码，编码共有 17 位，分配原则为 6 位陕西省县及县以上行政区划代码（也称行政代码）、2 位行业代码、8 位序列码和 1 位校验码，编码结构和陕西省县及县以上行政区划代码值参见附录 A。

社会公共服务卡卡内各业务号编码遵守各行业卡规范标准要求，无行业规范的业务号编码采用社会

公共服务卡的卡面号码，在卡内与居民身份证号码关联。

社会公共服务卡卡内业务应用ID号为2位行业代码，参见附录A。

5 卡规范

5.1 卡介质选择

社会公共服务卡采用双界面CPU卡，可写数据存储器可为EEPROM或FLASH，容量不小于64K字节。非接触式感应距离0～4cm属于正常刷卡的有效工作距离，4~10cm不做规定，超过10cm时刷卡失败，频率采用13.56MHz+7kHz，均要求符合ISO/IEC 14443和GB/IEC 7816标准。

双界面CPU卡是一种结合了接触及非接触两种通讯方式的智能卡，它们共用一个芯片，或各自独立使用芯片。

接触式：必须借助读卡终端进行插卡读写。

非接触式：信息通过电磁波进行传输。非接触式卡可以不与读卡终端接触而在一段距离内完成信息的传递。

注：如果社会公共服务卡需要加载银行金融业务，在卡片内部设两个独立的芯片，分别采用接触式和非接触式的通讯方式；并按JR/T 0052—2009银行卡卡片规范的规定增设磁道区域。双芯卡中，接触式芯片用于独立的银行金融业务，具体标准参考银行卡国家标准GB/T 14504；非接触式芯片用于社会公共服务相关的各类应用，其数据存储器采用闪速存储器，容量不小于64K字节,其中卫生行业应用32K字节，感应距离和频率如前所述。

5.2 卡体材料

卡体材料统一使用普通 PVC，有条件的地区推荐使用环保材料。

5.3 卡片要求

社会公共服务卡的制造、系统及应用机构必须符合以下条件：

a) 卡芯片以及卡片制造机构应具有国家集成电路(IC)卡注册中心分配的注册标识号和注册证书。

a) 卡芯片要通过中国国家信息安全认证中心的 EAL4+强制性安全认证。

b) 卡制造机构必须取得国家集成电路卡注册中心（ICCR）的集成电路卡注册证书和国家 IC 卡生产许可证。

c) 卡片操作系统（COS）要通过中国国家信息安全认证中心和相关机构的检查，取得 COS 检测合格证书。

d) 卡片虚拟机要符合虚拟机规范，并取得合格证书。

e) 卡片符合 Global Platform（GP）的平台环境要求和 Java Card 标准，支持主安全域和辅助安全域。

f) 卡片承载的应用必须符合各行业卡技术规范的要求，通过检测，并取得合格证书。

g) 对于没有卡技术规范的行业应用应符合陕西省社会公共服务卡技术规范的要求。

5.4 电器特性

由于本规范规定卡为双界面智能卡，所以电器特性分接触式和非接触式两部分。

a) 接触式

接触式智能卡有8个触点，即集成电路引脚，从C1到C8，如图1所示。GB/T 16649.1-2对接触式集成电路卡的触点尺寸和芯片位置以及功能作了具体的规定。

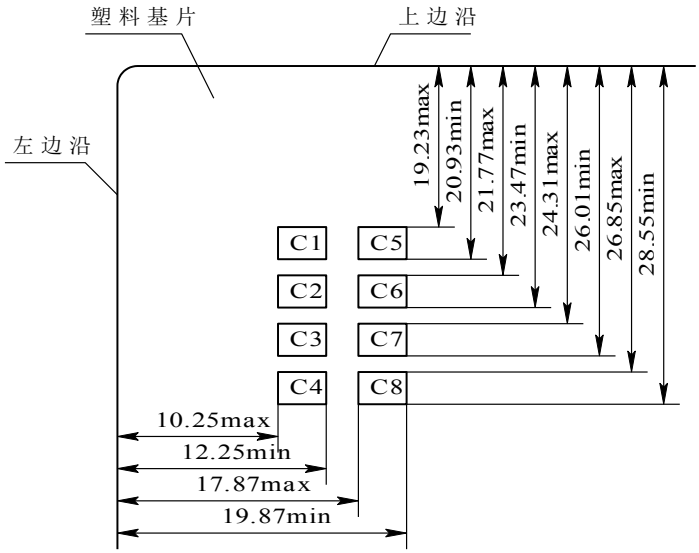


图1　接触式 IC 卡的触点尺寸及位置

智能卡的电极膜片(即8个触点)可安排在塑料基片的正面，也可安排在反面。触点之间的排列顺序必须按图1所示排列。各触点在卡基平面的几何尺寸、位置均以卡触点的接触面的左边沿和上边沿为基准边。其触点的尺寸及位置如图1所示，每个触点表面积的内切矩形面积不得小于2 mm×1.7 mm。

各触点之间应相互隔离。而相邻两个触点之间的最大距离为0.84 mm。8个触点所占最大面积不做规定，但最小面积不小于9.62 mm(长)×9.32 mm(宽)的矩形平面。

由 GB/T 16649.2规定，接触式电路触点如表1所示。

表1　触点的分配

触点号	分配	触点号	分配
C1	电源电压(VCC)	C5	地 (GND)
C2	复位(RST)	C6	编程电压 (VPP)
C3	时钟(CLK)	C7	输入/输出 (I/O)
C4	保留待未来使用	C8	保留待未来使用

其中：

——GND表示地，基准电压。

——VCC表示电源电压输入。

——I/O表示串行数据的输入/输出。

——CLK表示时钟信号输入。

——RST表示复位信号输入。

——VPP表示编程电压输入，由卡选用。

b)　非接触式

由ISO/IEC 14443规定，非接触式耦合区域和位置放置不能影响使用。

1）频率

射频工作场频率（fc）是13.56MHz+7kHz。

2）工作场

最小未调制工作场的值是1.5A/mrms，以Hmin表示。

最大未调制工作场的值是7.5A/mrms，以Hmax表示。

邻近卡应持续工作在Hmin和Hmax之间。

3）信道接口

ISO/IEC 14443规定了两种阅读器和近耦合IC卡之间的数据传输方式：A型和B型。一张IC卡只需选择两种方法之一。符合ISO/IEC 14443的阅读器必须同时支持这两种传输方式，以便支持所有的IC卡。

5.5 使用期限

卡片根据智能卡芯片刷卡频率，规定卡片的使用年限，推荐为10年。

卡片中应用程序使用年限，应遵守各行业规定，进行下载、更新、卸载。

6 卡面规范

6.1 总体要求

行业业务主管机构可以独立或者联合其它机构发行社会公共服务卡。

不论是独立发卡还是联合发卡，发卡单位必须经过陕西省社会公共服务卡管理机构审核和授权。

6.1.1 基本要素

本节主要对社会公共服务卡卡片上应印制、放置的要素内容及其规格、位置等进行规定。基本要素包括：卡号、持卡人姓名、性别、民族、社会公共服务卡标识字样、卡名、发卡机构名称标识等。

卡片正面指社会公共服务卡上印刷有“陕西省社会公共服务”标识信息的一面。卡正面除居民健康卡第一应用的标识外，不含有其它行业应用标识信息，具体见6.2.1。

卡片背面指社会公共服务卡上印刷有卡号、持卡人姓名、性别、民族、发卡机构名称、行业发卡标识等具体信息的一面，其中信息的规定和说明见6.2.2。

6.1.2 卡片外形规格

社会公共服务卡的标准卡片外形为矩形，如图2所示。

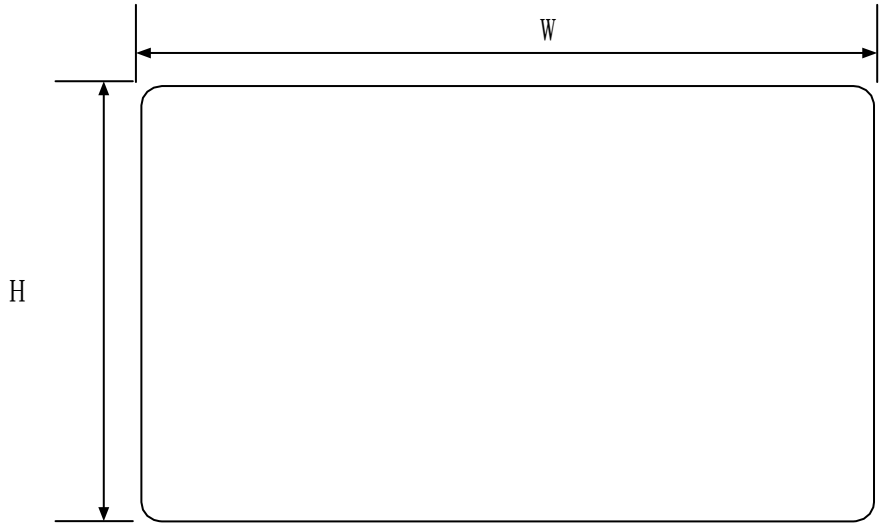


图2 陕西省社会公共服务卡外形规格示意图

社会公共服务卡片的标准尺寸如表2所示。

表2　卡片尺寸

参数	尺寸	公差
卡片宽度 W	85.60mm	85.47 mm -85.72 mm
卡片高度 H	53.98mm	53.92 mm -54.03 mm
卡片厚度 T	0.81mm	±0.03mm
倒角半径 R	3.18mm	±0.30mm

6.1.3　卡片基色

为保证社会公共服务卡的视觉完整性，便于提供相应的配套服务，社会公共服务卡管理机构对社会公共服务所采用的卡片基色进行专门管理。

卡面基色原则上禁止使用金属性金黄色和类似金属性金色的颜色，以及带金属性光泽或带珍珠光泽的银灰色、银色，或者其他可被理解为金色、白金色的颜色。卡面基色参考原卫生部发布的《居民健康卡技术规范》（修订版）要求。

6.1.4　介质布局

社会公共服务卡芯片的放置位置要求不影响使用，不影响卡片整体外观。

6.2　印刷要求

陕西省社会公共服务卡可以由某一具体社会公共服务单位（如卫生部门）独立发行，也可以采用联合其它机构（如联合银行等金融部门）的方式发行。鉴于这种多样化的卡片发行方式，此处给出卡面印刷的框架性要求：卡片正面应在醒目位置印刷“陕西省社会公共服务” 字样及标志图案等标识信息；卡片背面印刷卡号、持卡人姓名、性别、民族、发卡机构名称等具体信息。

以加载“居民健康卡”为第一应用的社会公共服务卡为例，6.2.1和6.2.2给出了卡片正、反面印刷样式设计参考。

6.2.1　卡片正面样式

参考原卫生部发布的《居民健康卡技术规范》（修订版）中的卡面设计，加载“居民健康”为第一应用的陕西省社会公共服务卡卡片正面设计如图3所示，增加“陕西省社会公共服务”字样。

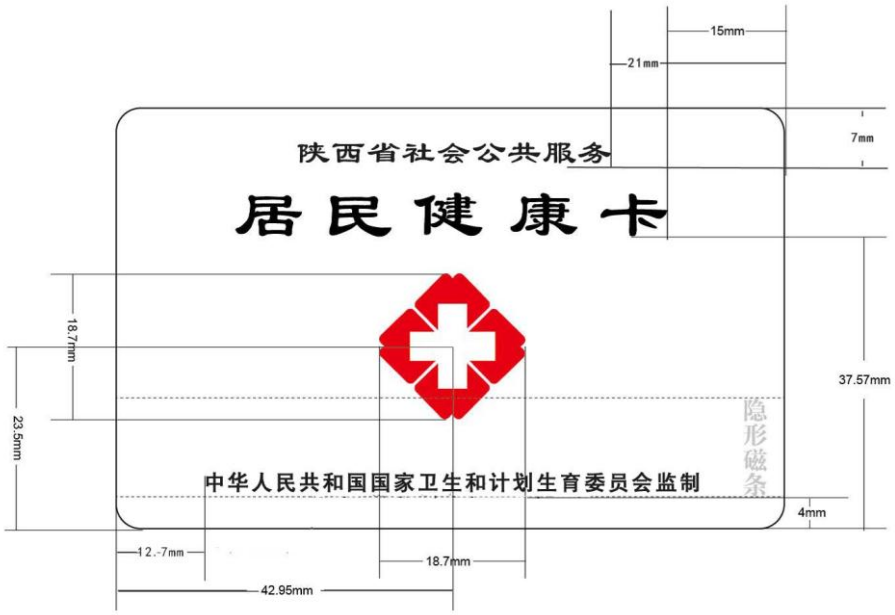


图3　陕西省社会公共服务卡正面印刷信息布局示意图

注：图3 中隐形磁条位置的虚线和文字是为了示意磁条区域，实际的卡片没有此效果。

卡片正面布局参数如表3所示。

表3　正面参数布局

参数	规格及要求	公差
“陕西省社会公共服务”		
“陕西省社会公共服务”字样	汉仪大隶书简体 10pt， 左右居中	/
右边沿到卡的右边沿的距离	21.00mm	±0.30 mm
下边沿到卡的上边沿的距离	7.00mm	±0.30 mm
“居民健康卡”		
“居民健康卡”字样	汉仪大隶书简体 28pt	/
右边沿到卡的右边沿的距离	15.00mm	±0.30 mm
下边沿到卡的下边沿的距离	37.57mm	±0.30 mm
居民健康卡标识图案		
居民健康卡标识图案	 ，左右居中	/

标识图案高度	18.70mm	±0.30mm
标识图案中心沿到卡的左边沿的距离	42.95mm	±0.30 mm
标识图案中心沿到卡的下边沿的距离	23.50mm	±0.30 mm
红色部分色号	C0、M100、Y100、K0	/
中华人民共和国国家卫生和计划生育委员会监制		
“中华人民共和国国家卫生和计划生育委员会监制”字样	汉仪中黑简体 9pt	/
左边沿到卡的左边沿的距离	12.7mm	±0.30 mm
下边沿到卡的下边沿的距离	4.00mm	±0.30 mm
磁条区		
磁条左边沿距离卡片左边沿	≤2.92mm	±0.30mm
磁条右边沿距离卡片左边沿	≥82.55mm	±0.30mm
磁条上边沿到卡的下边沿的距离	≥15.95mm	±0.30mm
磁条下边沿到卡的下边沿的距离	≤5.54mm	±0.30mm

注：1）社会公共服务卡的磁条应按JR/T 00520—2009的规定；第一磁道主账号数据为19位，其中前18位为中华人民共和国公民身份证号码，第19位为校验位，校验数算法见GB/T 14504 的规定。

2）卡片正反面未注明距离、高、宽公差的参数，公差为±0.30mm。

6.2.2 卡片背面样式

加载“居民健康卡”为第一应用的社会公共服务卡卡片的背面设计，以原卫生部发布的《居民健康卡技术规范》（修订版）为基础，增加“陕西省社会公共服务卡”字样，去掉“省级卫生厅局名称”和“地市卫生局名称”签章，如图 4所示。

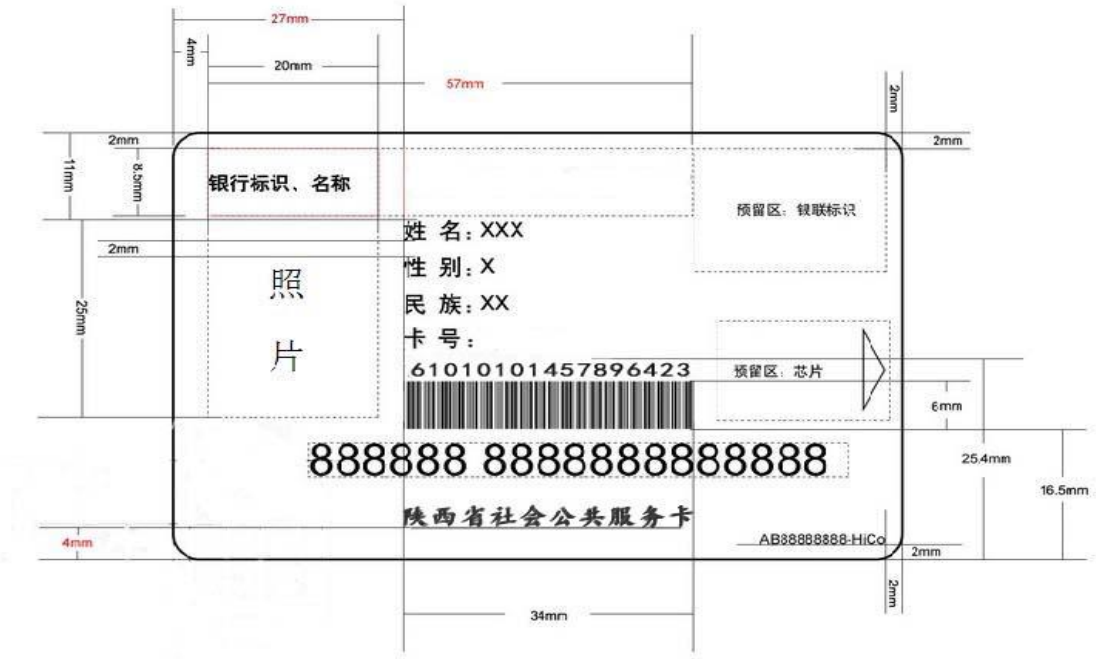


图4　陕西省社会公共服务卡背面印刷信息布局示意图

社会公共服务卡背面参数布局如表4所示。

表4　卡片背面参数布局

参数	规格及要求	公差
持卡人照片信息		
“照片”的宽度	20.00mm	±0.10mm
“照片”的高度	25.00mm	±0.10mm
“照片”左边沿到卡的左边沿的距离	4.00mm	±0.30mm
“照片”上边沿到卡的上边沿的距离	11.00mm	±0.30mm
若无照片，则此区域作为预留区使用		
持卡人个人信息		
“姓名” 、“性别”、“民族”、“卡号”字体	汉仪中黑 8.0PT	/
“姓名”、 “性别”、“民族”、“卡号”左边沿到卡的左边沿的距离	28.00mm	±0.30mm
“姓名”上边沿到卡的上边沿的距离	11.00mm	±0.30mm
“姓名”、“性别”、“民族”、 “卡号”四行的行间距	2.00mm	±0.30mm
社会公共服务卡号填写值上边沿距卡片下边沿距离	25.40mm	±0.30mm

可变信息部分		
“姓名、性别、民族”填写值字体	汉仪中黑 8.0PT	/
“姓名、性别、民族”字色值	K100	/
“卡号”填写值字体	汉仪中黑 8.0PT	/
“卡号”字色值	K100	/
条形码区		
条形码区域宽度	34.00mm	±0.30mm
条形码区域高度	6.00mm	±0.30mm
条形码左边沿到卡左边沿的距离	27.00mm	±0.30mm
条形码下边沿到卡的下边沿的距离	16.50mm	±0.30mm
陕西省社会公共服务卡		
“陕西省社会公共服务卡”字体	汉仪中黑 6pt	/
“陕西省社会公共服务卡”字间距	0	/
“陕西省社会公共服务卡”下边沿距卡的下边沿的距离	4mm	±0.30mm
“陕西省社会公共服务卡”水平方向	与条型码等长的区域内居中	±0.30mm
银联标准区		
银行卡号首位数字中心点到卡左边沿距离	17.50mm	±0.10mm
银行卡号首位数字中心点到卡下边沿距离	12.50mm	±0.10mm
银联标识上边沿到卡上边沿距离	2.00mm	±0.30mm
银联标识右边沿到卡右边沿距离	2.00mm	±0.30mm
银行标识、名称区		
“银行标识、名称”文字	在视觉上要小于“省级发卡机构名称”文字大小	/
“银行标识、名称”水平方向	区域内左对齐	/
“银行标识、名称” 垂直方向	区域内垂直居中	/
“银行标识、名称”区域左边沿到卡的左边沿的距离	4mm	±0.30mm
“银行标识、名称”区域右边沿到卡的左边沿的距离	24.00mm	±0.30mm

“银行标识、名称”区域上边沿到卡的上边沿的距离	2.00mm	±0.30mm
“银行标识、名称”区域高度	8.50mm	±0.30mm
卡商代码区		
“卡商代码”下边沿距卡的下边沿的距离	2mm	±0.30mm
“卡商代码”右边沿距卡的右边沿的距离	2mm	±0.30mm
“卡商代码”编码规则	卡商英文代码+年（yyyy）+月（mm）+日（dd）例如：HXGC20120818	

注1：1）使用照片基本要求，一寸近期正面免冠彩色头像，不着制式服装，常戴眼镜的居民应配戴眼镜，要求人像清晰、层次丰富，神态自然，无明显畸变，照片背景为白色，无边框。采集工作，可以采取两种方式：一是居民在照相馆照相，在办卡时提供符合标准的彩色照片，由办卡人员通过计算机扫描获得图像信息；二是居民到办卡网点通过数码相机照相，直接采集符合标准的图像信息。标准同二代身份证照片。符合 GB/T 15120 以及 ISO/IEC 7811-1/3 的规定。

2）条形码是对卡号进行编码的 128 条码，格式应按 GB/T 18347 行编码的神规定。

注2：关于原卫生部发布的《居民健康卡技术规范》（修订版）中联名卡的卡面设计，不再本规范中进行要求。

7 社会公共服务卡要求

7.1 卡的应用平台系统

陕西省社会公共服务卡应用平台系统由后端应用程序和系统、读取端主应用程序、读取端卡接受设备、卡运行时环境和卡上应用程序组成，陕西省社会公共服务卡中的所有应用必须在一个安全的运行时环境中实现，该运行时环境提供了一套硬件中立的应用编程接口以支持应用的可移植性、且起到了卡片中心管理者的作用，并定义一系列特殊的密钥和安全管理的应用被称作安全域，负责确保发卡方安全域和其他安全域提供者之间的密钥的完全隔离。卡的应用平台系统如图5所示。

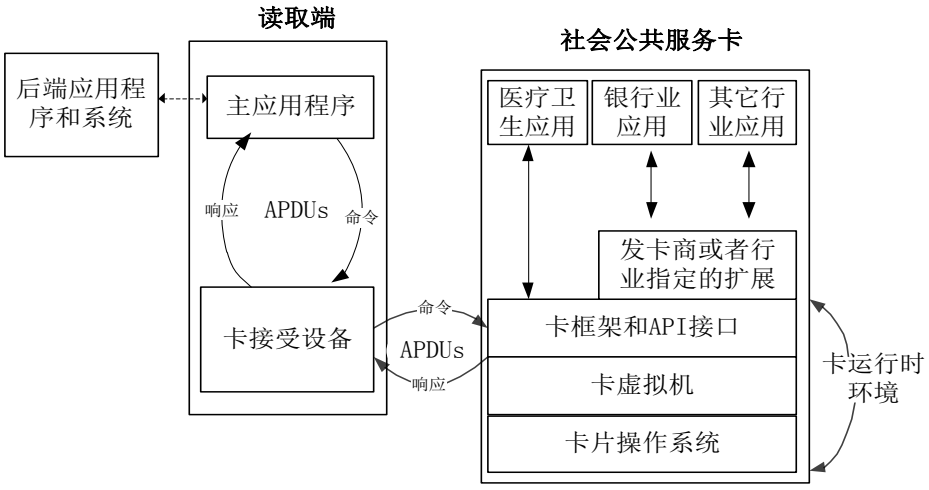


图5 卡的应用平台系统

7.1.1 后端应用程序和系统

不同行业提供支持卡上应用的服务端程序和系统，该服务端程序和系统独立运行。例如，不同行业的后端应用程序可以提供安全系统和卡上的证书连接，保证足够的安全性。

7.1.2 读取端主应用程序

存在于前台计算机或者终端、电子付款终端、手机或者一个安全子系统中。处理用户、社会公共服务卡上应用程序和后端应用程序之间的通信。

7.1.3 读取端卡接受设备

卡接受设备（CAD）是主应用程序和社会公共服务卡之间的接口设备。为卡片提供电力，以及与之进行电子或者射频通信。使用串行端口或者USB接口与计算机进行连接，或者可能被整合到终端内。接口设备从主应用程序转送应用程序协议数据单元（APDU）命令到卡片，并且从卡片向主应用程序转送响应。卡上行业应用环境的选择，由CAD上的行业SAM卡进行识别。

7.1.4 安全域

作为卡外授权方的卡片内代表的安全域，可以划分为三种主流类型：

a) 发卡方安全域，卡片上首要的、强制性存在的安全域，是卡片管理者(通常是发卡方)在卡片内的代表；
b) 补充安全域，卡片上次要的、可选择地存在的安全域，是应用提供方或发卡方以及它们的代理方在卡片内的代表；
c) 授权管理者安全域，一种特殊类型的补充安全域，授权管理者负责将某种安全策略贯彻到所有加载到卡片的应用代码上，授权管理者安全域就是授权管理者在卡片内的代表，卡片上可能存在多个这样的安全域。

以上三种安全域在本规范中，统称安全域。安全域负责提供各类安全服务，包括密钥管理、加密解密、针对其提供者(发卡方、应用提供方、授权管理者)的应用进行数字签名的生成与验证。当发卡方、应用提供方、授权管理者等卡外实体要将用到的密钥从其他实体区隔开来时，就可以通过新的安全域来代理它们实现这个需求。

7.1.5 卡运行时环境

为支持卡上应用程序的运行，卡运行时环境包括卡片操作系统（COS）、虚拟机、卡框架和API接口，如图5中所示的社会公共服务卡部分。

该运行时环境主要作用是负责向所有应用提供一套硬件中立应用编程接口，一种能确保各个应用的代码和数据能相互区隔的、安全的存储和执行空间分配机制，并提供服务来完成卡片和卡外实体之间的通信。

其主要功能包括：向应用提供API，命令转发，应用选择，逻辑通道管理以及卡片内容管理。运行时环境拥有一个内部的全局平台注册表，并利用它作为信息资源来进行卡片内容管理。全局平台注册表包含了管理卡片、可执行加载文件、应用、安全域关联以及权限所需要的信息。

7.1.5.1 卡片操作系统

卡片操作系统（COS）是驻留智能卡内的操作系统软件,是一个专用系统而不是通用系统，本质上更加接近于监控程序。 主要负责对外部的命令进行处理和响应。

7.1.5.2 卡虚拟机

卡虚拟机规范定义了程序设计语言的一个子集和一个用于智能卡的兼容虚拟机，包括二进制数据表示和文件格式，以及虚拟机指令集，是所有卡上应用程序运行的基础。

卡虚拟机分两个部分实现，一部分在卡外，一部分运行在卡本身。卡上的虚拟机解释字节码、管理类和对象等，卡外的部分用于把程序转换成适合在卡上运行的应用程序。

7.1.5.3 卡框架和应用程序接口（API）

卡框架是支撑服务的集合，为开发而统一规定的一种体系结构。

API为支持卡的应用编程接口，用于向应用提供各种服务，比如持卡方验证服务、个人化服务、安全服务等。此外还提供了卡片内容管理服务，如卡片锁定或应用生命周期状态更新服务。

7.1.6 卡上应用程序

社会公共服务卡应用程序主要是指ROM区中的应用可执行文件和EEPROM区中的应用可执行文件、应用实例和用户数据等。

社会公共服务卡上各个行业应用必须通过应用程序来实现。

卡上应用程序必须通过安全途径下载到卡中。

7.2 卡上应用程序的开发要求

社会公共服务卡上的应用程序开发，受硬件资源的限制，许多数据类型和语言特性不被支持，卡上应用程序的开发要求必须遵循卡虚拟机规范，便于实现社会公共服务卡上应用程序的移植。

7.3 卡中的 AID

本规范中每个卡上的应用程序和包都必须由一个应用标识符（AID）来唯一标识，AID的结构符合ISO/IEC 7816-5，AID格式是一个分为两部分的字节数组，第一部分是一个5字节值的资源标识（RID），第二部分是一个变长值的私有标识扩展（PIX），RID是ISO分配给包公司或应用程序服务商的ID ，PIX的长度是0到11个字节。AID可以是5到16个字节，其如图6所示。

RID	PIX
5 个字节	0-11 字节

图6 AID 的格式

包AID由公司的RID和包的PIX组成，AID和包名形成对应。卡上应用程序的AID由服务提供商的RID和应用的PIX组成。

卡上应用程序的AID不能和任何包的AID相同，包中的所有卡上应用程序的RID必须和包的RID相同。

编写卡上应用程序时，AID只需符合GB/T 16649的长度规定，而无须向ISO申请 RID 号。

7.4 卡上应用程序的安装与删除

在获得陕西省社会公共服务卡管理机构授权的情况下，如获得相应操作密钥，可以对社会公共服务卡上的应用程序进行安装和删除。

卡片应用的加载，实际是将卡片应用安装可执行文件加载至指定的安全域内。

卡片应用安装过程是将加载至指定安全域内的卡片应用安装可执行文件实例化的过程，它既可以与加载过程同步，也可以紧接在加载过程之后，或是在更晚到时候进行。

应用可选择化过程，启用卡片应用，进入到使用阶段。

在应用的使用过程中，可以通过二次个人化等操作实现应用的更新，以满足新的需求或者写入应用补丁；可以通过应用锁定与解锁来规避应用运行在不安全环境下的风险；在应用锁定期间可以通过[GET DATA]指令读取应用日志记录。

应用的删除过程，该过程通过对应用和/或可执行加载文件的删除，使得对卡片的空间进行灵活的回收。只有没被其他卡内应用引用的代码和数据可以被删除。

社会公共服务卡片的应用委托管理是指允许先前安装的应用或先前加载的应用程序安装文件关联到另一个不同的安全域。如果当前的安全域具备“委托管理权限”，那么委托管理使得应用提供方能够将属于它的某个应用迁移到另一个安全域。

7.5 卡的程序通信

卡上应用程序和卡终端主程序之间有两种通信方式，第一种是消息传送模型，第二种是基于CPU卡远程方法调用（CRMI），为兼容当前大多读卡设备，通信方式采用第一种。

消息传递模型的核心就是APDU，CPU卡框架接收CAD发送进来的 APDU 命令，并且传送到相应的应用程序中。卡上应用程序处理 APDU 命令，然后返回一个响应APDU。

读卡器和社会公共服务卡之间接触式的底层通信通基于T = 0或者 T = 1，T=0是异步半双工字符传输协议，T=1是异步半双工块传输协议，具体由GB/T 16649规定。非接触式基于Type A或者Type B，由ISO/IEC 14443规定。

7.6 卡的异常和错误

卡平台提供异常机制的完整支持。用户可以定义，抛出和捕获异常。卡平台中定义了一些异常和错误，CPU卡异常列表在开发的软件文档中提供。

8 终端要求

本规范要求设计的陕西省社会公共服务卡为多行业应用的智能卡，所以终端除了满足各行业的特殊需求外，还必须满足智能卡接触式或者非接触式通信等基本要求。

8.1 非接触式 IC 卡终端

8.1.1 基本要求

非接触式 IC 卡终端的逻辑接口、通信协议应符合相关规范要求。 非接触式IC 卡终端应该能够满足 ISO/IEC 14443的规定。

非接触式 IC 卡终端应该能够对应用中符合系统要求的卡片进行操作，自动识别处于磁场中的协议类型。

非接触式 IC 卡终端应该采用醒目的方式标示读卡区域，保证应用中能够方便的将卡片放置到操作区域。

非接触 IC 卡终端通过 USB 或者 RS232 口与计算机终端通信。

非接触 IC 卡终端应该能够支持至少一个 SAM 卡座，用以完成系统中的安全认证功能。

8.1.2 基本功能

非接触式 IC 卡终端与非接触式卡必须配合使用以保证交易安全、有效地运行，保证社会公共服务卡应用中规定的应用能够安全高效的完成。

非接触式 IC 卡终端应能提供对应用程序、密钥和参数等数据的下载、更新和删除，并提供对应用程序的选择和黑名单等功能。

8.2 接触式 IC 卡终端

8.2.1 基本要求

接触式 IC 卡终端的逻辑接口、通信协议应符合相关规范要求。 接触式 IC卡终端应该能够满足GB/T 16649的规定。

接触式 IC 卡终端应该能够对应用中符合系统要求的卡片进行操作。

接触式 IC 卡终端应该采用醒目的方式标示插卡正反面，保证应用中能够方便的将卡片插入到接触式 IC卡终端。

接触 IC 卡终端通过 USB 或者 RS232 口与计算机终端通信。

接触 IC 卡终端应该能够支持至少一个 SAM 卡座，用以完成系统中的安全认证功能。

8.2.2 基本功能

接触式 IC 卡终端与接触式 IC 卡必须配合使用以保证交易安全、有效地运行，保证社会公共服务卡应用中规定的应用能够安全高效的完成。接触式 IC 卡终端应能提供对应用程序、密钥和参数等数据的下载、更新和删除，并提供对应用程序的选择和黑名单等功能。

8.3 终端功能性部件

8.3.1 显示器

用于交易过程显示及错误提示，要求显示器有显示汉字、字母、数字和符号的能力。

8.3.2 键盘

用于输入交易数据、密码、业务信息，至少应配置数字字母键及确认功能键。

8.3.3 打印机

根据业务需求，终端可以配备打印机，打印凭条等数据。

8.3.4 存储设备

用于存储交易记录、黑名单、特殊的业务数据和扩展的字符集信息。应该根据用途配备存储设备的容量。

8.3.5 安全存取模块(SAM)

用于对终端操作的社会公共服务卡的权限鉴别，包括权限控制密钥的存储、鉴别数据的计算等功能。

8.3.6 通信接口

用于联机交易或终端与主机之间的数据传输，要求采用安全的网络线路。

8.4 终端检测

本规范规定的终端检测参考《中国金融集成电路（IC）卡非接触式应用终端检测规范》。

9 社会公共服务卡数据安全

社会公共服务卡除了必须满足金融、医疗、社保等行业规范的安全检测标准外，本章定义了卡内应用程序与卡外终端消息交换相关的安全服务。

9.1 基本安全要求

9.1.1 安全与共享

为了独立地管理一张卡上不同应用间的安全问题，每一个应用应该放在一个单独的DF中，即在应用之间应该设计一道“防火墙”以防止跨过应用进行非法访问，以及阻止对未授权的实例的属性和方法的访问。当需要调用其它包中应用的实例的属性和方法时，需要通过安全途径来访问，如图7所示。另外，每一个应用也不应该与个人化要求、卡中共存的其它应用的规则发生冲突。

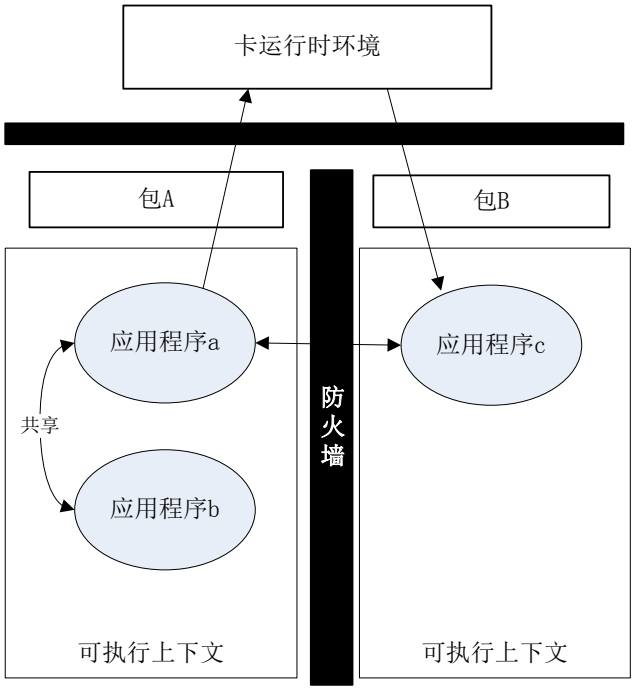


图7 社会公共服务卡应用程序隔离和对象共享

9.1.2 密钥的独立性

用于一种特定功能（如读取数据）的加（解）密密钥不能被任何其它功能所使用，包括保存在社会公共服务卡中的密钥以及用来产生、派生和传输这些密钥的密钥。

9.2 密钥和个人密码的存放

社会公共服务卡应该能够保证用于选定的加（解）密算法的非对称私有密钥或对称加密密钥在没有授权的情况下，不会被泄露出来。

如果使用个人密码，则应保证其在社会公共服务卡中的安全存放，且在任何情况下都不会被泄露。

9.3 安全报文传送

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。数据完整性和对发送方的认证通过使用报文鉴定码(MAC)来实现。数据的可靠性通过对数据域的加密来得到保证。

9.3.1 安全报文传送格式

本规范中定义的安全报文传送格式符合GB/T 16649的规定。当CLA字节的第二个半字节等于十六进制数字“4”时，表明对发送方命令数据要采用安全报文传送。卡中的FCI表明某个命令的数据域的数据是否需要加密传输，是否应该以加密的方式处理。安全报文传送的参数设置如表5所示。

表5　安全报文传送的参数设置

Bit4	Bit3	Bit2	Bit1	说明
0	0	X	X	不需要安全报文传送
0	1	X	X	需要安全报文传送

9.3.2　报文完整性和验证

MAC 是使用命令的所有元素（包括命令头）产生的。一条命令的完整性，包括命令数据域（如果存在的话）中的数据元，通过安全报文传送得以保证。

9.3.2.1　MAC 的位置

MAC 是命令数据域中最后一个数据元。

9.3.2.2　MAC 的长度

本规范中，MAC 的长度规定为 4 个字节。

9.3.2.3　MAC 格式

在GB/T 16649中定义了四种命令情况。本节简单讨论MAC格式对命令APDU的作用，APDU命令参考10.4节所述的基本格式。

情况一：命令没有数据送到卡中，也没有数据从卡中返回。

没有安全报文传送要求的命令情况如图8所示。

CLA	INS	P1	P2

图8　情况一没有安全报文传送要求的命令格式

有安全报文传送要求的命令情况如图9所示。

CLA	INS	P1	P2	Lc	MAC

图9　情况一有安全报文传送要求的命令格式

CLA为一个字节长度，它第二个半字节是‘4’，格式如二进制“xxxxx100”或者十进制“x4”，表明支持第一种情况的安全报文传送技术。Lc为MAC的长度。

情况二：命令没有数据送到卡中，但有数据从卡中返回。

没有安全报文传送要求的命令情况如图10所示。

CLA	INS	P1	P2	Le

图10　情况二没有安全报文传送要求的命令格式

有安全报文传送要求的命令情况如图11所示。

CLA	INS	P1	P2	Lc	MAC	Le

图11　情况二有安全报文传送要求的命令格式

CLA为一个字节长度，它第二个半字节是‘4’，格式如二进制“xxxxx100”或者十进制“x4”，表明支持第二种情况的安全报文传送技术。Lc为MAC的长度，Le为期望数据长度。

情况三：命令中有数据送到卡中，但没有数据从卡中返回。

没有安全报文传送要求的命令情况如图12所示。

CLA	INS	P1	P2	Lc	命令数据

图12　情况三没有安全报文传送要求的命令格式

有安全报文传送要求的命令情况如图13所示。

CLA	INS	P1	P2	Lc	命令数据	MAC

图13　情况三有安全报文传送要求的命令格式

CLA为一个字节长度，它第二个半字节是‘4’，格式如二进制“xxxxx100”或者十进制“x4”，表明支持第三种情况的安全报文传送技术。Lc为命令数据长度加上MAC的长度。

情况四：命令中有数据送到卡中，并有数据从卡中返回。

没有安全报文传送要求的命令情况如图14所示。

CLA	INS	P1	P2	Lc	命令数据	Le

图14　情况四没有安全报文传送要求的命令格式

有安全报文传送要求的命令情况如图15所示。

CLA	INS	P1	P2	Lc	命令数据	MAC	Le

图15　情况四有安全报文传送要求的命令格式

CLA为一个字节长度，它第二半字节是‘4’，格式如二进制“xxxxx100”或者十进制“x4”，表明支持第二种情况的安全报文传送技术。Lc为命令数据长度加上MAC的长度。

9.3.2.4 MAC 密钥的产生

在安全信息处理过程中用到的 MAC 过程密钥是按照附录B中描述的过程密钥的产生过程产生的。MAC数据加密算法（DEA）密钥的原始密钥用于产生MAC过程密钥。

9.3.3 数据可靠性

为保证命令中明文数据的保密性，系统对数据进行加密。

9.3.3.1 数据加密密钥的计算

在安全报文处理过程中用到的数据加密过程密钥按照附录B中描述的方式产生。数据加密过程密钥的产生过程是从卡中的数据加密DEA密钥开始的。

9.3.3.2 被加密数据的结构

当命令中要求的明文数据需要加密时，它先要被格式化为以下形式的数据块：

——明文数据的长度，不包括填充字符(Ld)；

——明文数据；

——填充字符，然后整个数据块使用数据加密算法进行加密。

9.3.3.3 加密算法

本规范为多行业应用标准，行业应用加密算法要求支持各行业规范要求的加密算法，并根据APDU命令中的算法标识，调用相应的算法，完成认证、签名、验签、加解密等功能。无行业规范的，要求采用陕西省社会公共服务卡管理机构确定的加密算法。本规范所采用的加密算法均应符合国家密码管理局对加密算法的要求。

国家密码管理局颁布的常用算法如下：

SM1 为对称加密算法。

SM2为非对称算法，可用于密钥或者证书的生成和验证、签名信息的生成和验证。

SM3为杂凑算法，用于对任意长度的报文生成一个32 字节的哈希值。

SM4为PBOC 3.0中规定使用的对称加密算法。

9.3.3.4 安全规划

卡上数据根据应用安全要求，分为只读数据区、只写数据区、可读写数据区，各使用机构权限的分配根据不同的应用要求配置 SAM 卡来进行数据的安全访问。

9.4 密钥机制

9.4.1 设计原则

在陕西省社会公共服务卡系统中，密钥的安全控制和管理是应用系统安全的关键。陕西省社会公共服务卡密钥管理系统的宗旨在于，通过全省统一的卡密钥管理体系，实现不同行业的全省跨地区刷卡服务，卡内行业的应用主密钥则由本行业的根密钥分散而来，实现行业全国跨省刷卡服务。

要完成以上目标，陕西省社会公共服务卡密钥管理系统要遵循以下几条设计原则：

1、卡密码算法统一：密码算法是智能卡安全体系中最基本的部分，在应用系统安全体系中，采用统一的密码算法，也是实现全省“社会公共服务”的基础。

2、密钥的共享和独立：在省社会公共服务卡密钥管理系统中，我们既要保证通用数据与安全的全省统一管理，同时又要保证各地区、各行业安全系统的独立性，即每个地区或行业的密钥不同。省社会公共服务卡管理机构实现卡片主控密钥和系列卡片维护密钥的安全性和共享性，而行业管理机构实现业务应用主控密钥和系列应用维护密钥的安全性和独立性。

3、在充分保证密钥安全性的基础上，支持密钥的生成、注入、导出、备份、恢复、更新、服务等功能，实现密钥的安全管理。

4、密钥受到严格的权限控制，不同机构或人员对不同密钥的读、写、更新、使用等操作具有不同的权限。

5、用户可根据实际使用的需要，选择密钥管理系统不同的配置和不同功能。

6、密钥服务一般以硬件密码机的形式提供，也可采用密钥卡的形式。

9.4.2 密钥的种类及功能

9.4.2.1 省级密钥的种类

陕西省社会公共服务卡采用CPU卡，根据CPU卡的规范，卡片出厂时含有厂家设置的传输密钥，以保证卡片传输的安全性。陕西省社会公共服务卡管理机构收到一批卡片后，使用陕西省社会公共服务卡管理机构生成的卡片主控密钥替换厂家设置的传输密钥，成为这批卡片的卡片主控密钥，然后在卡片主控密钥的控制下，加载以下几个省级密钥：

1、MAC认证密钥。

2、应用程序下载解密密钥：当应用程序是以密文的方式传输时，该密钥负责将应用程解密，并下载安装到卡内。

3、APDU解密密钥：CPU卡支持APDU以密文方式向卡内传输，该密钥负责解密APDU。

以上省级密钥为管理密钥，由陕西省社会公共服务卡管理机构维护。卡片主控密钥是CPU卡的基本密钥，它负责应用程的下载和其它卡密钥的加载与更新。

卡片主控密钥建立在MF下，它是卡片的控制密钥，所有的发卡过程都是在它的控制下进行。其功能有：

1、创建卡片MF区域的文件和应用目录。

2、装载卡片维护密钥、应用主控密钥。

3、更新卡片主控密钥、卡片维护密钥。

卡片主控密钥是控制发卡的密钥。所有在MF下建立的各行业的应用，首先都必须通过卡片主控密钥的认证。但它又不参与各应用业务层面的安全认证及业务管理。对于单一的发卡方来说，这个密钥由发卡方控制，对于陕西省社会公共服务卡来说，卡片主控密钥应该由省级密钥管理机构生成和管理。这种模式既保证了在同一卡片上可随时建立各种应用，又保证了各应用下的数据及业务的安全由各行业控制。

9.4.2.2 行业应用密钥的种类

本规范要求的密钥主要分为卡管理密钥和行业应用密钥。行业应用密钥的生成、管理、更新等由各个行业规范规定，本规范只进行引用，如居民健康应用中的密钥机制。

根据目前已经颁布的行业规范来看，行业应用密钥主要分为以下几种：

00　　应用主控密钥；

01　　应用维护密钥；

03　　PIN解锁密钥；

04　　PIN重装密钥；
10　　消费、取现密钥；
11　　圈存密钥；
12　　TAC 密钥；
13　　圈提密钥；
14　　修改透支限额密钥；
15~18　保留；
19　　内部认证密钥（加密）；
1A　　内部认证密钥（解密）；
1B　　个人密码；
1C　　内部认证密钥（MAC）；
1B~31　保留。

以上密钥在不同的行业规范中定义的ID号有所不同，但类型和功能基本一样。在上述密钥中，应用主控密钥决定发卡方是否具有在行业应用下对卡片进行预个人化和个人化的权力。

在目前的情况下，对于由国家部委进行行业管理的纵向应用来说，陕西省社会公共服务卡管理机构仅对行业应用的主控密钥进行统一初始化，这样发卡方只有得到陕西省社会公共服务卡管理机构的授权后方能发卡。其它业务密钥，由各行业的密钥管理系统生成，各行业在发卡时自行导入。

对于没有行业管理的应用来说，由省密钥管理机构统一生成以上所有的行业应用密钥，从而保证陕西省社会公共服务卡管理机构对卡应用的管理，实现陕西省社会公共服务卡的应用。

9.4.3　省密钥管理系统

陕西省全省社会公共服务卡系统中，首先要有密钥管理系统，它的功能就是支持密钥的生成、分散、注入、导出、备份、恢复、更新、服务等功能，实现密钥的安全管理，其基本架构如图16所示。

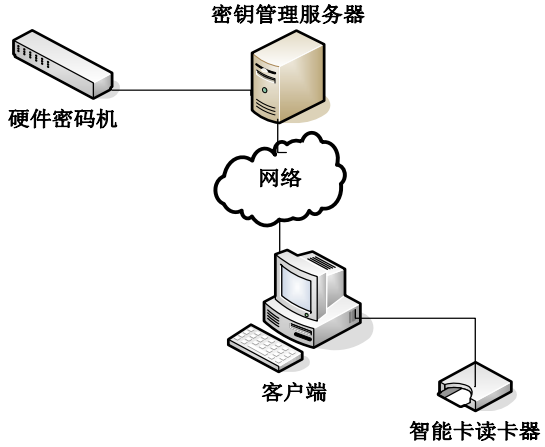


图16　省密钥系统架构

9.4.4　密钥的生成

在省级密钥管理系统中，密钥的生成包括三个部分，一是省级根密钥的生成，另一个是各地区二级密钥的生成，由于地区二级密钥没有用到，所以不进行说明；二是生成省级管理密钥；三是各行业应用的密钥。

9.4.4.1 省级根密钥的生成

省级根密钥是由一些种子密钥通过杂凑算法，再用省级分散因子通过加密算法分散而来的。种子密钥一般由多个省管理机构相关的主管随机输入，其过程如图17所示。

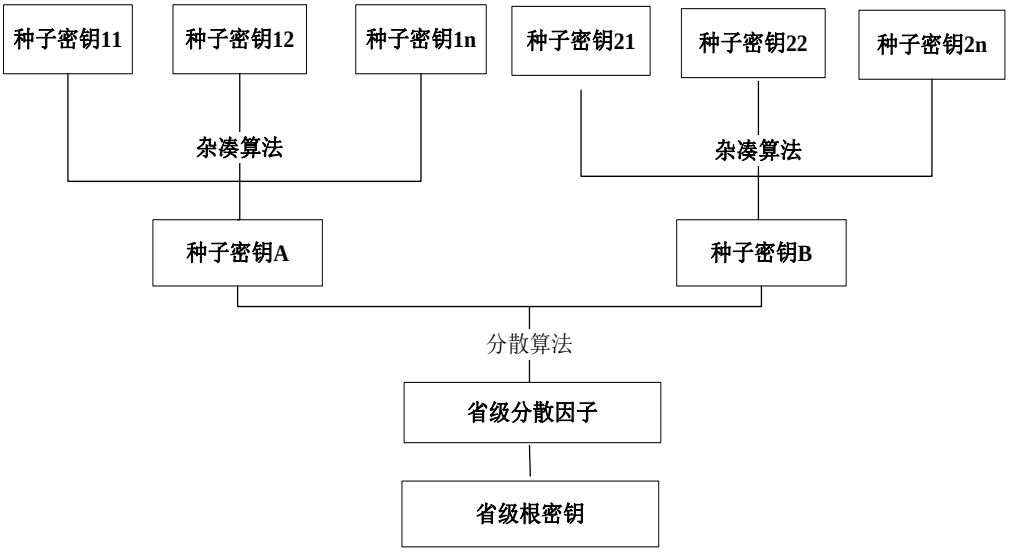


图17 省级根密钥生成

种子密钥A及种子密钥B一般以密文方式保存在系统数据库中，并打印密钥信封保存的密码箱中。生成的省级根密钥一般保存在硬件密码机中，并用母卡进行备份。

注：根据需要，省级根密钥可以是国家部委根据省分散因子分撒出来的二级密钥。

9.4.4.2 省级管理密钥的生成

省级管理密钥有四种：

1、卡片主控密钥；

2、MAC认证密钥；

3、应用程序下载解密密钥；

4、APDU解密密钥。

省级根密钥的分散过程如图18所示。

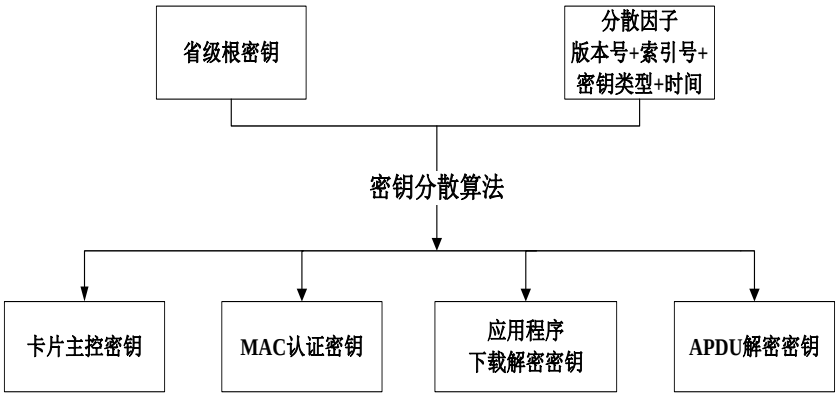


图18 省级根密钥的密钥分散

将图18中省级根密钥所分散出来的密钥装载到母卡中，生成省级洗卡母卡。省级洗卡母卡主要是对全省“陕西省社会公共服务卡”的用户卡进行应用程序下载以及应用密钥初始化。

注：省级分散因子由省社会公共服务卡密钥管理机构决定，例如陕西省社会公共服务卡密钥分散因子可定义为（SXSYKTMY）。

9.4.4.3 各行业应用主控密钥的生成

关于各行业应用主控密钥的生成，对于有行业管理或者行业规范的应用，省社会公共服务卡密钥管理机构不对行业根密钥进行分散，行业应用主控密钥和其它业务密钥都由该行业管理机构依据其行业规范自行生成，本规范和卡只进行引用和承载，发卡由该行业管理机构执行或第三方可信机构，省社会公共服务卡密钥管理机构只对其进行卡授权。行业根密钥的密钥分散如图19所示。

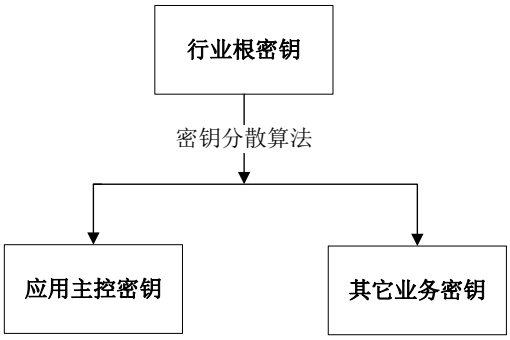


图19 行业根密钥的密钥分散

对于没有明确行业规范的省级各项社会公共服务业务，由省社会公共服务卡密钥管理机构生成包括应用主控密钥在内的全套行业应用密钥。各行业应用主控密钥在省社会公共服务卡密钥管理机构的硬件密码机中存储和备份。

9.4.4.4 用户卡和认证卡

对于目前已由各部委统一管理的发卡行业，陕西省社会公共服务卡管理机构向发卡单位或第三方可信委托机构发放认证卡，以取得卡片访问的权限。

认证卡和用户卡的认证关系如图20所示。

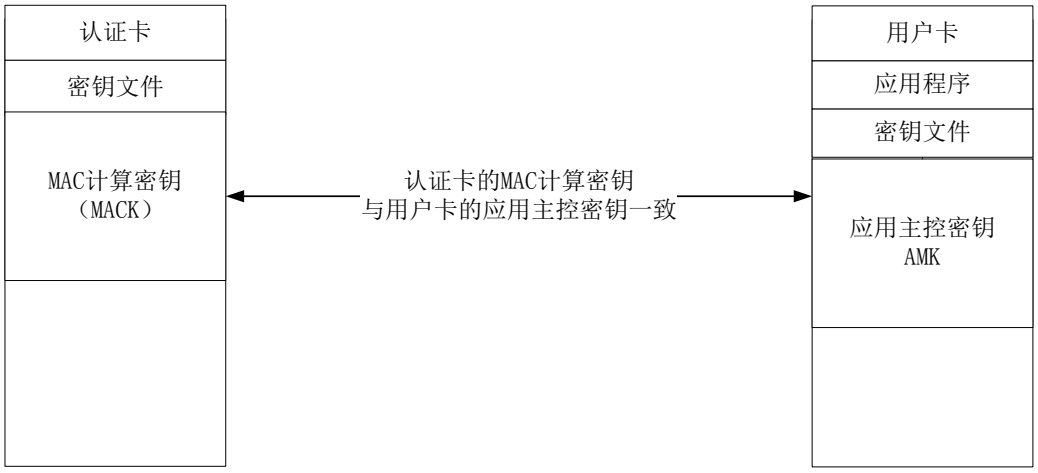


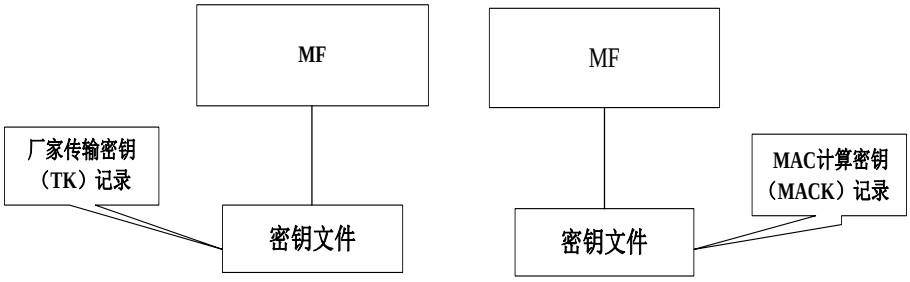
图20 认证卡和用户卡的认证关系

9.4.5 密钥的发行

由省社会公共服务卡密钥管理机构生成的省级管理密钥和初始行业应用主控密钥向各发卡中心发行。

9.4.5.1 空白卡

智能卡从厂家出厂时为只有MF的空白卡片。卡片中设置一个初始的传输密钥，将这个传输密钥存放在传输密钥卡中，通过两个不同的渠道将空白卡和传输密钥卡交给社会公共服务卡密钥管理机构。空白卡和传输密钥卡如图21所示。



注：TK的值与MACK的值相同

图21 空白卡和传输密钥卡

9.4.5.2 省社会公共服务卡密钥管理机构洗卡

空白卡片内有厂家设置的厂家传输密钥，省社会公共服务卡密钥管理机构需要将厂家传输密钥更换掉。因此，用省级主控密钥（即省级根密钥分散出来的卡片主控密钥）替换厂家传输密钥，即洗卡，具体流程如图22所示。

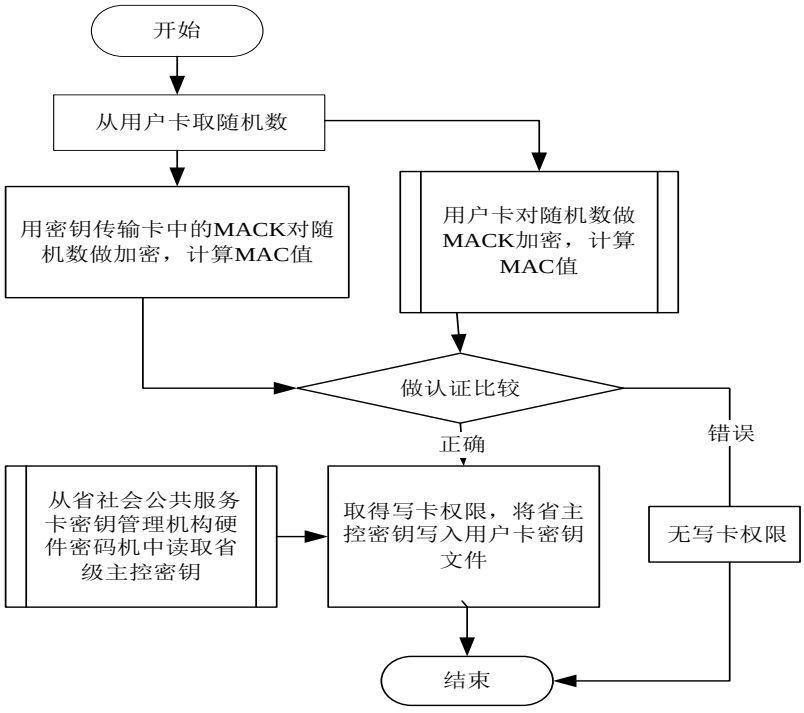


图22　省社会公共服务卡密钥管理机构的洗卡流程

9.4.5.3　省社会公共服务卡密钥管理机构密钥加载

经过图22所示的洗卡流程后，省社会公共服务卡管钥管理机构在卡片主控密钥的控制下加载省级其他管理密钥，包括MAC认证密钥、应用程序下载解密密钥和APDU解密密钥等。此外，省社会公共服务卡密钥管理机构还需要在卡片主控密钥的控制下加载多个初始应用主控密钥，它们将对应于各个行业应用，并生成这些初始应用主控密钥相应的认证卡。为了实现省社会公共服务卡密钥管理机构对各个行业应用的卡片进行授权，这些初始应用主控密钥是利用卡片主控密钥和各个行业分散因子进行分散而来的。

9.4.5.4　发卡方密钥的认证

用户卡经过陕西省社会公共服务卡管理机构的洗卡后，变成由陕西省社会公共服务卡管理机构认可的全省适用卡片。任何发卡方在这种卡片上加载全省社会公共服务，需通过陕西省社会公共服务卡管理机构的授权，在陕西省社会公共服务卡管理机构授权的卡片上建立自己的地区及行业的应用，而不受其它已发卡行业的限制。

洗卡后的用户卡结构如图23所示。

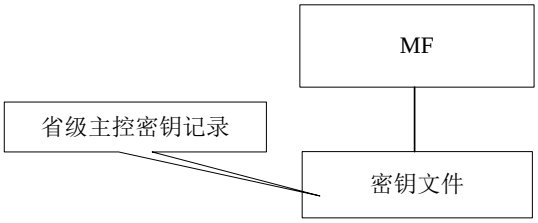


图23　洗卡后的用户卡

作为发卡方，要想在图23所示的用户卡卡片上建立自己的应用，就必须通过省级主控密钥的认证及应用授权，即获得省级主控密钥分散出来的授权密钥（即初始应用主控密钥），才能进行发卡。

类似于卡片出厂的方式，由省社会公共服务卡管理机构向审核过的发卡方发行“认证卡”。发卡方可通过该卡片与用户卡的认证，获得发卡权限，从而在卡片上建立自己的文件系统和密钥。认证卡如图24所示。

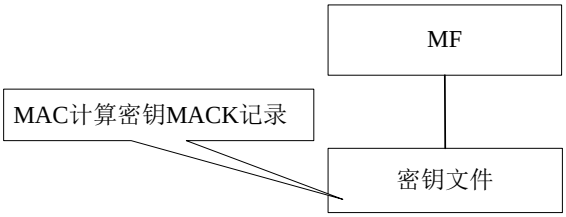


图24　认证卡

9.4.6　各行业发卡流程

行业发卡分为两种形式，一种是由专门机构对各个行业业务进行代理（如发卡、维护、更新等），一种是把用户白卡发售各个行业部门，由各个业务机构进行业务加载、维护，更新等操作。第一种方式，便于卡和所有业务统一管理，不具操作性，实现困难；第二种，陕西省社会公共服务卡管理机构只管理

卡和业务应用加载授权，不对具体业务进行管理，实现简单。无论那种方式，发卡加载业务必须获得卡和业务上级部门的授权。

用户卡中存有的省级主控密钥，根据业务需求，发卡部门从不同渠道安全获得授权的认证卡和行业业务加密机，根据图25所示流程，进行业务加载。

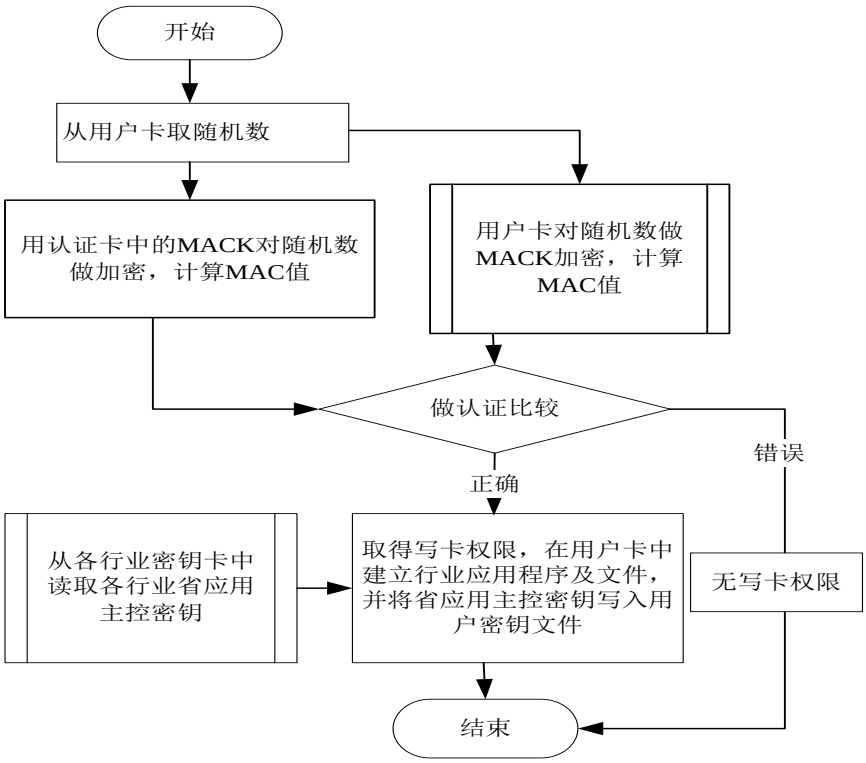


图25　各行业的发卡流程

各行业卡中心与省卡管理中心省卡管理中心通过安全通道连接，在行业前台进行发卡或者信息更新时，行业卡中心数据和省卡管理中心数据必须实时同步或者定期同步更新，以便每个行业在发卡或者加载应用时，首先查询申请人或者持卡人的数据记录，依据记录状态的合理性，审核进行发卡或者加载应用，当发卡或者加载完毕后，应实时更新相关的数据记录，以确保各行业对社会公共服务卡发卡的唯一性，锁定、解锁、挂失、解挂、补办的准确性和实时性。

9.4.6.1　医疗业务发卡流程

医疗卫生机构从上级部门获得本地业务加密机，并从省社会公共服务卡管理机构获得认证卡权限。居民到医疗卫生发卡网点，填写卡和初始业务（即医疗卫生服务）的申请表，网点根据卫生行业数据库记录情况，若判定为合格且为初始申请，则发卡，并根据图26所示流程，加载医疗卫生应用程序及密钥资源,发卡完毕后及时向行业卡中心和省卡管理中心更新相关数据记录。如果发卡业务已委托形式进行，则其流程不在此赘述。

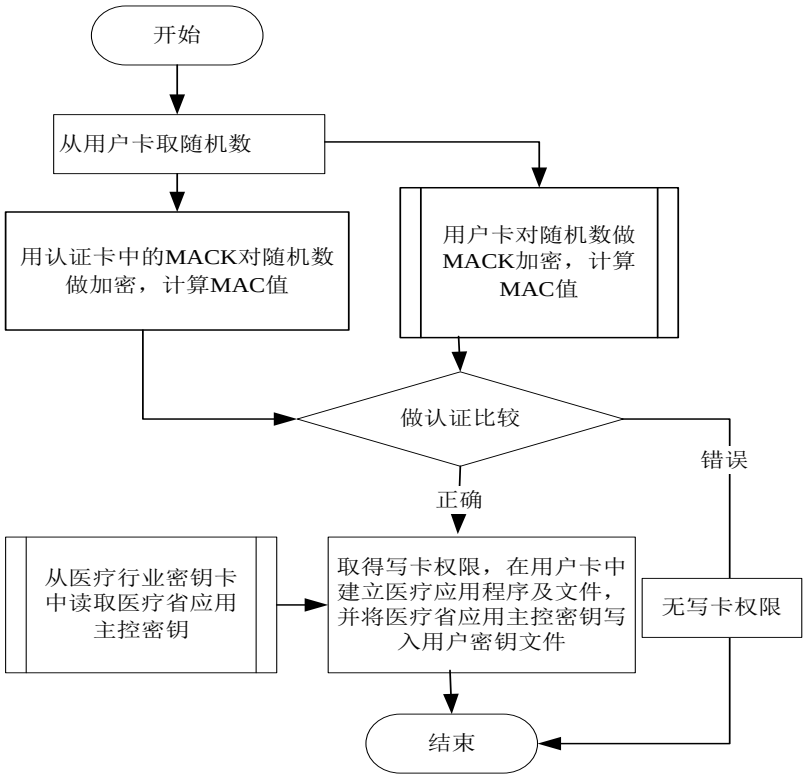


图26　医疗业务发卡流程

9.4.6.2　后续新增业务发卡

对于新增业务卡中心从上级部门获得本地业务密码机，或者主控应用密钥及其配套密钥，并从省社会公共服务卡密钥管理机构获得对应业务的认证卡，此时用户可以持有先前载有初始业务的用户卡，到该行业服务网点，进行申请，行业服务网点依据申请数据，查询申请人和卡片数据，依据数据状态，审核是否加载新增业务。如果审核通过，则根据如图27所示进行验证，加载业务应用程序及密钥，与医疗卫生发卡流程保持一致。此业务加载并不覆盖其它加载的业务应用程序，资源密钥文件被分配在自己的DF中，运行限制在自己启动的上下文中，有防火墙隔离。加载完毕后与行业卡中心和省卡管理中心省卡管理中心进行数据同步更新。

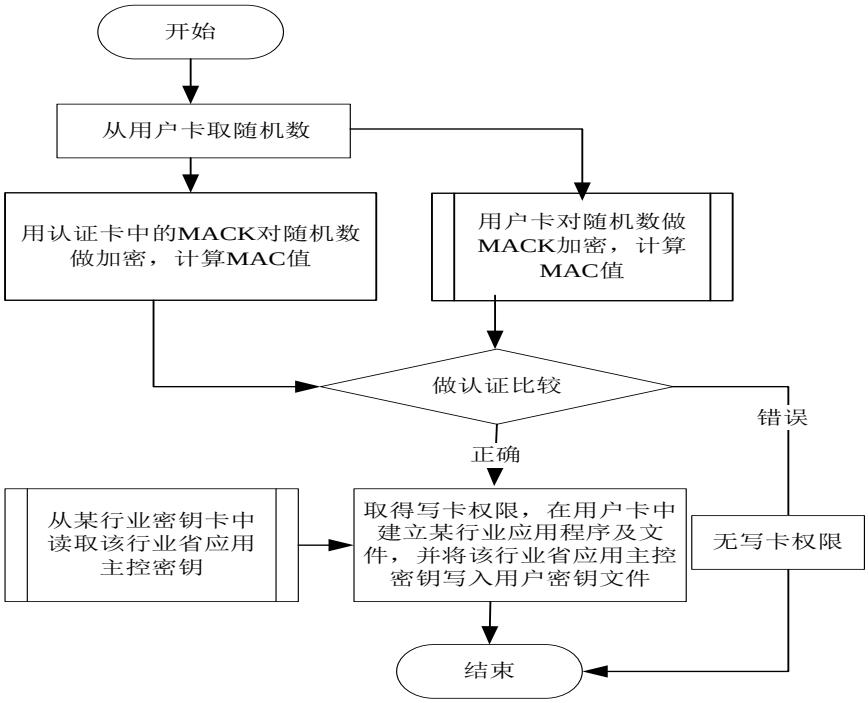


图27　其它业务发卡流程

9.5　密钥管理

9.5.1　卡密钥

陕西省社会公共服务卡的密钥管理采用省级统管、各行业应用分管的模式。对于卡的发行、维护、统计、业务加载授权等密钥都由省级部门统管。密钥机制产生见9.4。

9.5.2　业务密钥

对于业务根密钥的生成、维护、更新导入、导出等由相关业务主管部门进行密钥管理，具体遵守各应用规范和标准。

9.5.3　密钥说明

陕西省社会公共服务卡的卡密钥说明参见附录C。

9.6　权限鉴别

权限鉴别的目的是验证终端对卡中数据进行读写操作的合法性。

9.6.1　鉴别数据的长度

本规范规定鉴别数据的长度为8字节。

9.6.2　业务鉴别密钥的产生

对业务使用的密钥，用特定的分散因子作为输入数据，做加密计算，采用各行业规范中规定的算法，产生的结果作为子密钥。所有机构 SAM 卡安装内部认证密钥，可以用来进行社会公共服务卡业务的鉴别，如对医疗、社保、新农合等业务进行鉴别。

9.6.3 鉴别数据的计算

使用9.5.2中描述的操作权限鉴别密钥对原始数据进行加密，如图28所示。

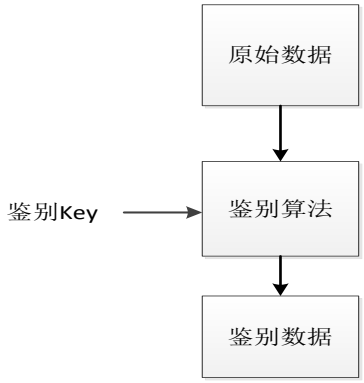


图28 鉴别数据的计算

9.7 锁定与解锁

9.7.1 应用的锁定与解锁

行业卡业务机构 SAM 卡上安装卡应用解锁密钥用于锁定卡业务和解锁；在只需要进行卡业务上读取的管理机构安装相关业务读控密钥，并在只需要进行卡上业务写的管理机构安装业务写控密钥。用于限定持卡人应用业务的锁定与解锁。

9.7.2 卡片的锁定与解锁

省卡管理中心SAM 卡上安装卡解锁密钥用于锁定卡和解锁;在只需要进行卡上读取的省卡管理中心安装卡读控密钥，并在只需要进行卡上业务写的管理机构安装卡写控密钥。用于限定行业应用业务和持卡人业务的锁定和解锁。

9.8 卡片的挂失与终止

9.8.1 卡片的挂失

卡片的挂失锁定权限在省卡管理中心，或者由省卡中心授权委托第三方机构完成。

持卡人可以用以下两种方式进行卡片挂失登记。

挂失登记方式1：持卡人到任意一个行业或者社会公共服务卡发卡网点，持本人有效身份证明，进行卡片挂失登记。发卡网点将挂失登记信息在12小时内通过联网数据传递至省卡管理中心；省卡管理中心更新挂失数据库，并在24小时内将更新的挂失数据库共享至所有发卡机构。

挂失登记方式2：持卡人通过服务热线或网站登录方式，直接向省卡管理中心进行卡片挂失登记；挂失登记需提供个人验证信息：包括身份证号码、姓名、联系方式、卡片密码，或发卡机构、或发卡时间、或卡片最近三次使用/消费记录。

挂失登记成功后，卡片即挂失锁定。挂失锁定后允许一周内申请取消挂失，一周后挂失正式起效，被挂失卡片永久失效。

申请取消挂失可以向发卡网点或卡管中心进行取消挂失登记，方式与挂失登记方式相同。

申请取消挂失方式1：持卡人到任意一个社会公共服务卡发卡网点，持本人有效身份证明，申请取消卡片挂失。

发卡网点将申请挂失取消信息在12小时内通过联网数据传递至省卡管理中心;省卡管理中心更新挂失数据库，取消卡片挂失，并在24小时内将更新的挂失数据库共享至所有发卡机构，卡片应用即恢复正常状态。

申请取消挂失方式2：持卡人通过服务热线或网站登录方式，直接向省卡管理中心申请取消卡片挂失；申请人需提供个人验证信息：包括身份证号码、姓名、联系方式、卡片密码，或发卡机构、或发卡时间、或卡片最近三次使用/消费记录。

省卡管理中心即时更新挂失数据库，取消卡片挂失，并在24小时内将更新的挂失数据库共享至所有发卡机构，卡片应用即恢复正常状态。

9.8.2 卡片的终止

卡片终止的适用条件：自然人死亡或迁移（如出国定居），则卡片服务终止。

卡片的终止锁定权限在省卡管理中心。

卡片终止服务方式一：省卡管理中心数据库与公安数据库定时进行数据交互，每周更新自然人生存数据信息，自动终止锁定符合卡片终止条件的持卡人的社会公共服务卡；更新卡片终止数据库，并在24小时内将更新的卡片终止数据库共享至所有发卡机构。被自动终止锁定的卡片，暂时无法正常使用。如无数据库信息异动，被自动终止锁定的卡片一个月后永久锁定，卡片永久失效。

卡片终止服务方式二：符合卡片终止条件的持卡人亲属或持卡人，至任意一个社会公共服务卡发卡网点，持本人有效身份证明，及符合卡片锁定的相关证明材料（如自然人死亡证明、国籍变更证明）进行卡片终止登记。

发卡网点将终止登记信息在12小时内通过联网数据传递至省卡管理中心;省卡管理中心更新卡片终止数据库，并在24小时内将更新的卡片终止数据库共享至所有发卡机构。申请终止锁定的卡片，暂时无法正常使用。

省卡管理中心数据库与公安数据库定时进行数据交互时，再次核对申请终止卡片的持卡人信息；如无数据库信息异动，申请终止锁定的卡片一个月后永久锁定，卡片永久失效。

10 社会公共服务卡应用

10.1 卡文件结构

本节定义了社会公共服务卡的各项应用环境，既可以支持全部定义的应用，也可以只支持其中的某几项，目录可以根据应用需求，动态添加和删除。当前主要以医疗卫生、银行、社保为主要应用主体，示例如图29所示,该示例中的应用目录只表示多应用目录的支撑，并不对实际目录文件格式进行定义，其中各应用环境下的规范由行业卡技术规范规定。如医疗卫生需遵循原卫生部发布的《居民健康卡技术规范》要求。

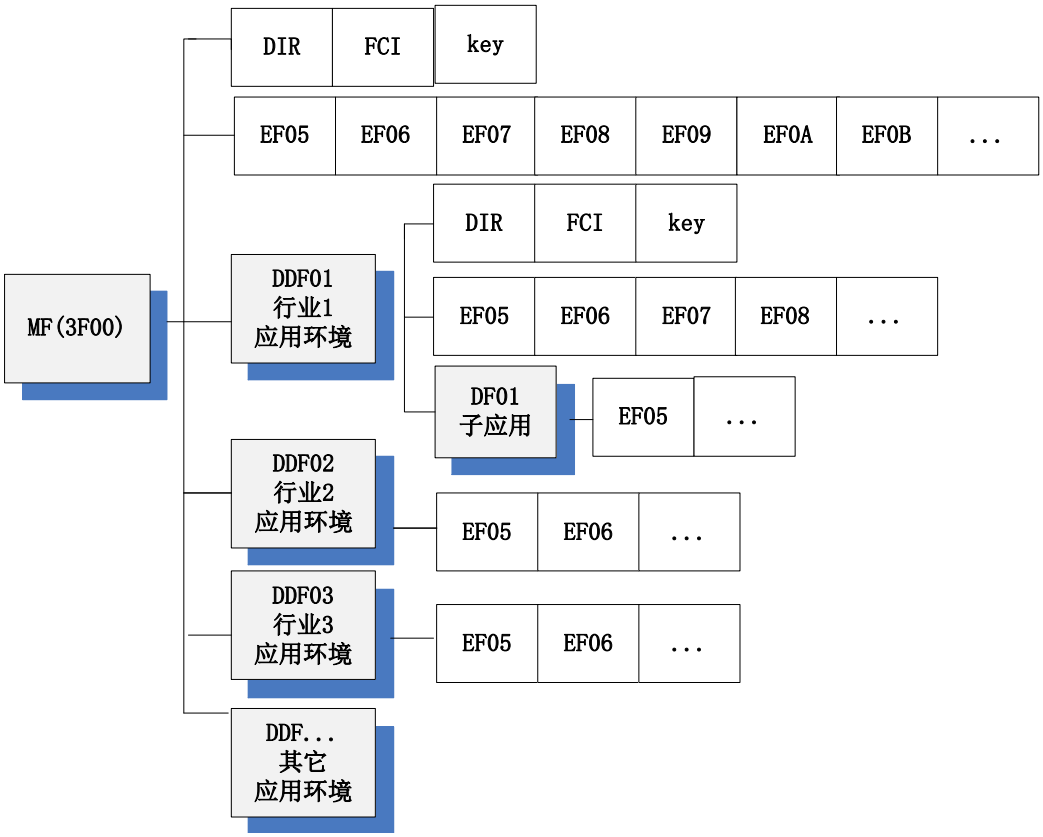


图29　社会公共服务卡文件结构示例

10.1.1　文件结构

社会公共服务卡的文件系统由GB/T 16649及规范中应用相关的规定，由主文件（MF）、专用文件（DF）和基本文件（EF）组成。

10.1.2　主文件(MF)

MF是社会公共服务卡文件系统的根，相当于磁盘操作系统（DOS）的根目录，每张卡要求有且只有一个MF，存储公共信息并为各种应用服务。

10.1.3　专有文件(DF)

DF是MF下针对不同应用(如社保、医疗应用等)建立的文件，相当于DOS的子目录。按照GB/T 16649的规定，每一个应用所对应的专用文件（DF）应包含一个文件控制信息（FCI）。通过该文件可以对其下的基本数据文件（EF）进行访问。专用文件的上一层专用文件是对应社会公共服务卡环境的专用文件（DF或MF）。每个专用文件是其下面基本数据文件的入口点。

10.1.4　目录专用文件（DDF）

在一个DF下包含子DF的话，则称该DF为目录专用文件（DDF），DDF是一组应用DF的集合，在公共服务卡中作为行业应用环境的入口。在每一个DDF下可以包含一个DIR系统文件，用以记录所有子DF的入口。

注：DDF01行业1应用环境可以映射为医疗卫生应用环境，即《居民健康卡技术规范》规定的MF入口；

DDF02行业3应用环境可以映射为金融银行应用环境，即《中国金融集成电路（IC）卡规范》规定的MF入口；
DDF03行业2应用环境可以映射为社保应用环境，即《社会保障卡标准规范》规定的MF入口；
其它类似。

10.1.5 应用专用文件（ADF）

如果一个DF下不包含其它子DF，只包含了文件控制信息FCI和数据文件，则该DF称为应用专用文件（ADF），是单个应用在卡内的逻辑映射，因为没有其它DF文件，所以就不存在DIR文件。

10.1.6 基本文件（EF）

基本数据文件(EF)用于存储各种应用的数据信息，其存在于MF和DF下。 每一个应用下的基本数据文件（EF）有两种类型： 记录文件类型和二进制文件类型。EF从存储内容上分为基本安全文件和基本工作文件。

10.1.7 数据元

社会公共服务卡个人基础信息使用省人口资源库，如附录D提供的基础数据进行筛选，形成社会服务基本元数据，如附录E所示。

10.1.8 数据结构

社会公共服务卡的卡的数据结构请遵守附录F。

10.1.9 文件选择

各个应用的专用文件，可以用应用标识符（AID）、文件标识符（FID） 两种方式来进行选择。

成功选择了应用的专用文件后，该专用文件被设置成当前专用文件，允许使用相关的命令对其进行操作。

基本数据文件的选择可以采用下面的两种方式来实现：

隐式选择：使用READ 或UPDATE命令通过 SFI 来选择文件；显式选择：使用 SELECT 命令通过文件标识符来选择文件。

10.2 应用标识符

社会公共服务卡中的包和应用程序通过AID进行选择。

各个应用的标识符（AID），必须采用由国家 IC 卡注册中心颁发的标准，格式遵守本规范7.3节要求。

10.3 应用选择流程

本节以医疗应用流程为例。描述持卡人刷卡、卡片与终端相互作用后，所进行的应用处理流程。所有应用都要求终端必须具有安全存取模块（SAM）。本部分假定终端与医疗应用 SAM 之间是以安全方式进行通信的，因此不定义任何与SAM通信相关的命令－响应对。

10.3.1 应用预处理流程

图30给出了社会公共服务卡中的医疗应用对应的预处理流程，其它应用的预处理流程类似。

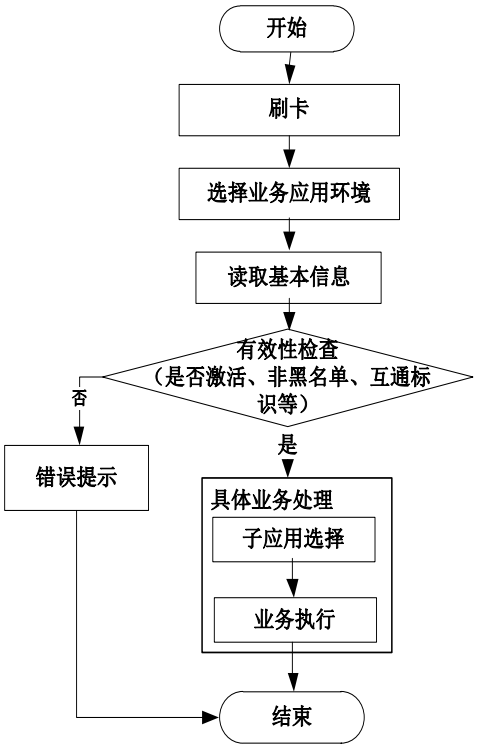


图30　社会公共服务卡医疗应用的预处理流程

10.3.1.1　刷卡

接触式按照正确的卡面和方向插卡，非接触式要求在规定的距离之内刷卡。

10.3.1.2　选择应用环境

终端发送带有医疗标识的“端发送带有医疗命令，对社会公共服务卡中医疗应用环境进行选择。

10.3.1.3　有效性检查及持卡人身份认证

首先使用内部认证密钥(IRK)对 IC 卡中该行业应用的有效性进行验证，步骤如下：

1、终端产生8字节的随机数，该随机数作为“INTERNAL AUTHENTICATION机命令的数据域；

2、终端发送“INTERNAL AUTHENTICATION机命令，卡将计算鉴别数据 并回送；

3、终端在收到鉴别数据后，进行比较验证。如果验证不通过，则按10.3.1.4 描述进行；如果验证通过，则用“READ BINARY述命令读取业务应用发行机构数据，终端将对这些数据进行以下检查：

a）该卡是否在医疗终端存储的黑名单之列；

b）终端是否支持发卡机构编号；

c）终端是否支持从卡回送的“卡的类别”所代表的卡类型；

d）终端是否支持从卡回送的应用版本；

e）卡中的应用是否在有效期内。

10.3.1.4　错误处理

终端对交易预处理出错的处理方法不属于本规范的范围,业务错误码的规定遵守各个行业卡应用规范。

10.3.1.5 具体应用选择

成功地选择了某个具体的应用后，IC 卡回送文件控制信息。 通过应用选择，终端可以建立 IC 卡所支持的业务列表。

10.3.2 卡读数据

通过读应用信息,业务管理部门的操作员可以从社会公共服务卡中获得持卡人办理具体事务时产生需要读取的相关信息。

对某一具体的应用信息的读操作仅受终端中的 SAM 卡的控制。具体操作流程分为以下步骤。

第一步:判断读信息是否受控。终端或者应该明确知道对某一具体的应用信息的读取操作是否受控。如果信息读取操作是不受控的，则转入第三步；否则， 继续按下述步骤执行。

第二步：读操作权限的鉴别。

第三步：发出读命令，根据应用数据的存储格式，终端应按读命令来读取所需的应用信息。

第四步：返回确认，在成功读取数据后，IC 卡应向终端回送状态码来确认数 据读取操作的完成。

第五步：判断是否还需继续读取数据，终端在成功读取一条信息后，应根据 交易的要求，判断是否还要读取更多的数据。如果需要继续读取数据，则转入第三步继续进行，否则继续后续操作。

第六步：提示已读取完毕，终端在确认应用要求的所有数据都已读取完成后， 将通过适当的设备向业务管理部门的操作员提示交易完成。

10.3.3 卡写数据

通过写应用信息,业务管理部门的操作员可以在社会公共服务卡中记录持卡人办理具体事务时产生写入的相关信息。

对某一具体的应用信息的更新操作仅受终端中的SAM卡的控制。具体操作 流程分为以下步骤。

第一步：判断更新信息是否受控。终端或者应该明确知道对某一具体的应用 信息的更新操作是否受控。如果信息更新操作是不受控的，则转入第三步；否则， 继续按下述步骤执行。

第二步：更新操作权限的鉴别。

第三步：发出更新命令，根据应用数据的存储格式，终端应按规范中的描述发出更新命令来更新所需的应用信息。

第四步：返回确认，在成功更新数据后，智能卡应向终端回送状态码来确认数据更新操作的完成。

第五步：判断是否还需继续更新数据，终端在成功更新一条信息后，应根据 交易的要求，判断是否还要更新更多的数据。如果需要继续更新数据，则转入第 三步继续进行，否则继续后续操作。

第六步：提示已更新完毕，终端在确认应用要求的所有数据都已更新完成后， 将通过适当的设备向业务管理部门的操作员提示交易完成。

10.4 基本命令

符合GB/T 16649中基本命令，分为C-APDU和R-APDU两大类。

10.4.1 C-APDU 格式

C-APDU由4字节长的必备头后跟一个可变长的条件体组成，如图31所示。

CLA	INS	P1	P2	Lc	Data	Le
必备头				条件体		

图31　C-APDU 格式

C-APDU中发送的数据字节数用Lc（命令数据域的长度）表示。

R-APDU中期望返回的数据字节数用Le（期望数据长度）表示。当Le存在且值为0时，表示需要最大字节数（256字节）。在命令报文需要时，Le可始终被设为“00”。

C-APDU报文的内容见表6。

表6　C-APDU 的内容

代码	描述	长度
CLA	命令类别	1
INS	指令字节	1
P1	指令参数 1	1
P2	指令参数 2	1
Lc	命令数据域中存在的字节数	0 或 1
Data	命令发送的数据位串（=Lc）	可变
Le	响应数据域中期望的最大数据字节数	0 或 1

10.4.2　R-APDU 格式

R-APDU格式由一个变长的条件体和后随两字节长的必备尾组成，如图32所示。

Data	SW1	SW2
条件体	必备尾	

图32　R-APDU 格式

R-APDU报文的内容见表7。

表7　R-APDU 的内容

代码	描述	长度
Data	响应中接受的数据位串（=Lr）	变长
SW1	命令处理状态	1
SW2	命令处理限定	1

当使用T=1协议时，对于所有Le=“00”的命令，状态字SW1、SW2=“90 00”或“61 La”均表示命令的成功执行。但由于可读性的需要，这两种应答码只用了“90 00”作为参考。

本条描述了以下的C-APDU/R-APDU：

——APPLICATION BLOCK（应用锁定）；

——APPLICATION UNBLOCK（应用解锁）；
——CARD BLOCK（卡片锁定）；
——EXTERNAL AUTHENTICATION（外部认证）；
——GET RESPONSE（取响应）；
——GET CHALLENGE（产生随机数）；
——INTERNAL AUTHENTICATION（内部认证）；
——PIN CHANGE/UNBLOCK（个人识别码修改/解锁）；
——READ BINARY（读二进制）；
——READ RECORD（读记录）；
——SELECT（选择）；
——UPDATE BINARY（修改二进制）；
——UPDATE RECORD（修改记录）；
——VERIFY（校验）。

10.4.3 应用命令

社会公共服务卡除了支持以上描述的基本文件、命令外，还应支持应用所需的各个行业的卡应用命令。

11 社会公共服务卡业务功能

社会公共服务卡作为所有社会服务的电子凭证，所涵盖的业务主要有城镇职工医疗保险、城镇居民医疗保险、新型农村合作医疗、区域卫生、工伤保险、人口计划生育公共服务及社会救助等，社会公共服务卡是社会服务信息系统中极为重要的组成部分,其主要功能如下：

1、身份认证
2、权限认证
3、信息共享与交互
4、电子证明
5、个人资料存贮
6、信息查询
7、与银行卡关联
8、电子钱包
9、条形码应用
10、扩展应用

11.1 身份识别

通过读取社会公共服务卡中的持卡人基本信息数据来识别个人信息,通过连接社会公共服务卡系统验证社会公共服务卡及其信息的有效性，或在终端机上做专用SAM身份有效性验证。

11.2 权限认证

根据指令状态安全属性认证鉴别用户的操作、文件读写的访问权限等。

11.3 信息共享与交换

应用单位根据业务需要，定时或不定时从社会公共服务卡注册中心数据交换区读取社会公共服务卡变更信息，如：卡挂失、解挂、冻结以及个人基本信息变更等，注册中心根据需要实时更新交换区数据。社会公共服务卡的数据信息数据库可以共享给相关的应用系统，支撑健康档案基础数据的建立。

11.4 电子证明

能识别持卡者在社会服务业务中的合法身份，并作为享受社会服务及办理就医结算等业务的电子凭证。

11.5 个人资料存储

卡中存有持卡人的身份、住址、联系方式等各种个人资料。

11.6 信息查询

支持卡和应用各种信息的终端脱机、联网、热线查询。如卡中应用的数目、激活状态、个人信息等。

11.7 银行卡关联

当社会公共服务卡需要支持银行卡应用时，可以在卡片增加银行应用的工作环境，卡内的金融工作环境由《居民健康卡技术规范》（修改版）的金融接触式支付环境（PSE）和金融非接触式支付系统环境（PPSE）决定，其中PSE为可选。银行应用由应用程序来实现，该应用程序密钥管理、卡内信息以及交易流程应符合合作银行的应用规范。与银行关联交易流程如图33所示。

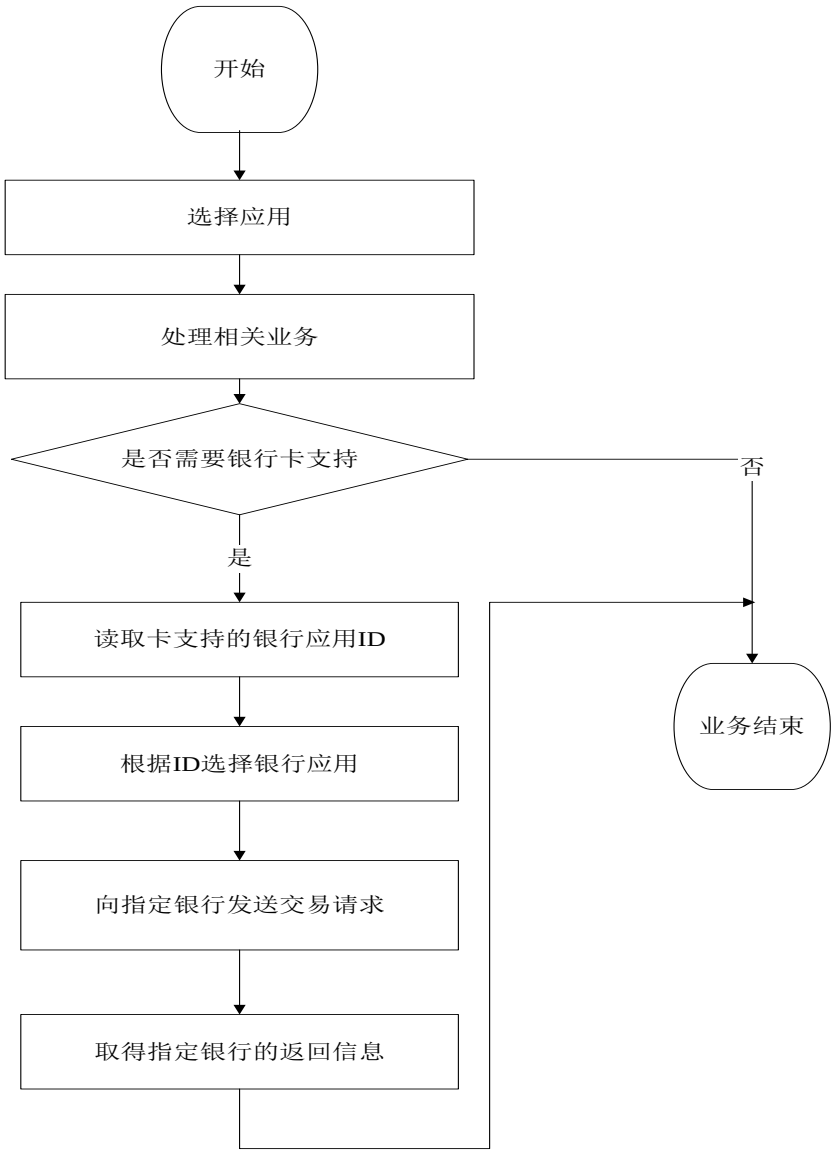


图33　与银行关联交易流程

下面以医疗卫生消费交易流程为例进行说明，如图34所示。

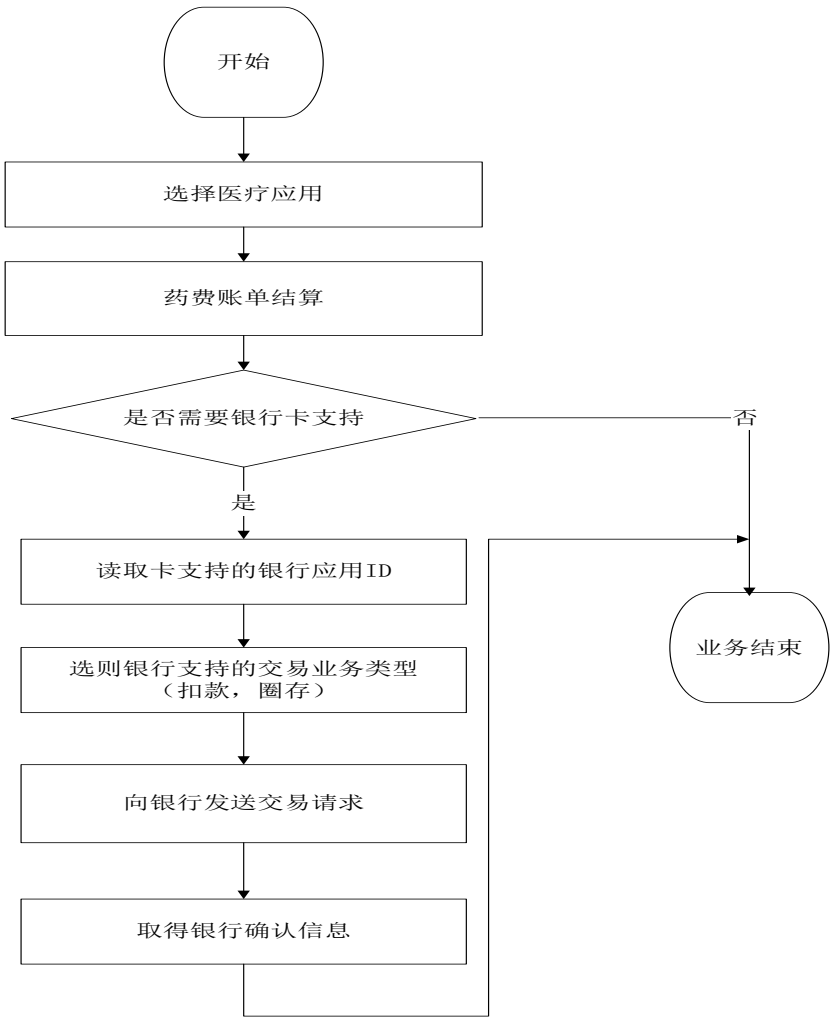


图34　医药消费交易流程

不同的业务和不同银行决定不同的交易方式，本规范不进行限制，以实际情况为准。

11.8　电子钱包

电子钱包采用接触方式。为满足持卡人进行小额消费而设计的金融应用类型，它支持圈存、消费等快速无需提交个人PIN码的交易，除圈存交易外，使用电子钱包的其它交易都不产生交易明细。

本规范中的电子钱包的技术规范和APDU命令由中国金融集成电路（IC）卡规范第 1 部分—电子钱包/电子存折应用卡片规范和第九部分—电子钱包扩展应用指南规定，电子钱包的具体业务数据元、业务密钥等生成和算法由陕西省工业和信息化厅下发的《城市一卡通技术规范（试行）》规范规定。

电子钱包的预处理流程如10.3.1的图30所示。小额消费交易流程和充值流程分别如图35和图36所示。

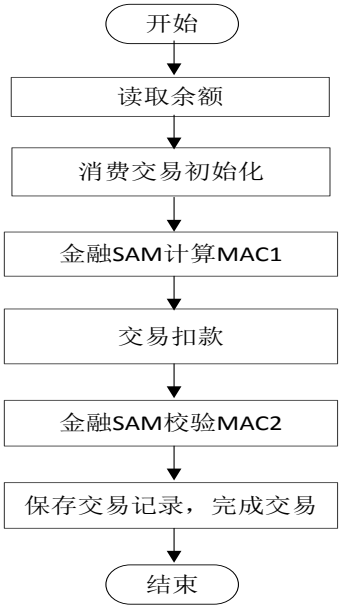


图35　小额消费交易流程

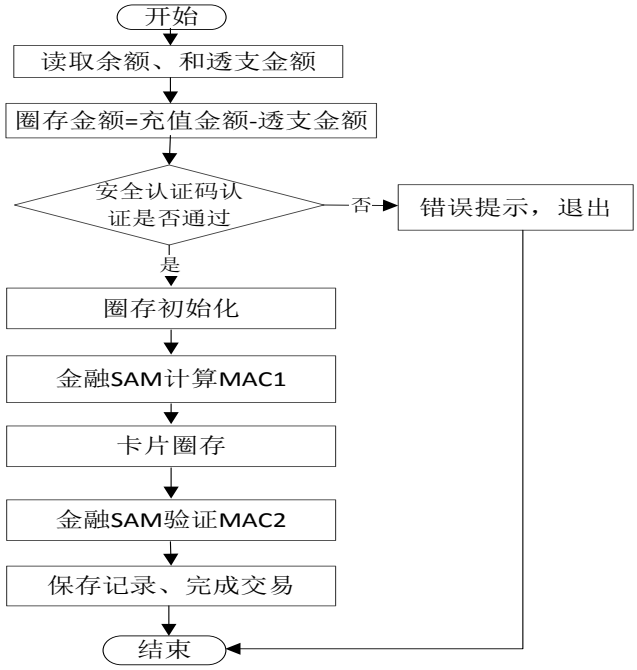


图36　充值流程

11.9　条形码应用

按照条形码的规范规定，对卡和个人进行关联标识，以便进行人卡识别。

11.10　应用扩展

在需要进行扩展应用的地方，借助社会公共服务卡通过应用程序的形式扩展需要的应用业务（如民政、计生、交通、电、燃气等）。

社会公共服务卡的各类信息应严格遵循统一的数据标准和交换格式，并在数据交换操作后，保留操作日志。

附 录 A
（规范性附录）
社会公共服务卡的卡面号码编码

A.1 编码结构

社会公共服务卡的卡面号码由17位数字连续排列组成，结构如下：
AABBCCXXYYYYYYYYZ
其中：
——AABBCC表示陕西省县及县以上行政区划代码（也称行政代码），长度为6位，其值定义见A.2。
——XX表示行业代码，长度为2位，其值定义如下：
01 居民健康卡业务；
其他值保留。
——YYYYYYYY表示序列码，长度为8位，其值为发卡时产生的顺序数。
——Z表示校验码，校验数算法见GB/T 14504 的规定。

注：中华人民共和国县及县以上行政区划代码从左至右的含义是：
第一、二位表示省（自治区、直辖市、特别行政区）；
第三、四位表示市（地区、自治州、盟及国家直辖市所属市辖区和县的汇总码），其中01-20、51-70表示省直辖市，21-50表示地区（自治州、盟）；
第五、六位表示县（市辖区、县级市、旗），其中01-18表示市辖区或地区（自治州、盟）辖县级市，21-80表示县（旗），81-99表示省直辖县级市。

A.2 陕西省县及县以上行政区划代码值

陕西省县及县以上行政区划代码值定义如表A.1所示。

表A.1 陕西省县及县以上行政区划代码值

行政区划代码	地区	行政区划代码	地区
610000	陕西省	610600	延安市
610100	西安市	610602	宝塔区
610102	新城区	610621	延长县
610103	碑林区	610622	延川县
610104	莲湖区	610623	子长县
610111	灞桥区	610624	安塞县
610112	未央区	610625	志丹县
610113	雁塔区	610626	吴起县
610114	阎良区	610627	甘泉县
610115	临潼区	610628	富县
610116	长安区	610629	洛川县
610122	蓝田县	610630	宜川县

610124	周至县	610631	黄龙县
610125	户县	610632	黄陵县
610126	高陵县	610700	汉中市
610200	铜川市	610702	汉台区
610202	王益区	610721	南郑县
610203	印台区	610722	城固县
610204	耀州区	610723	洋县
610222	宜君县	610724	西乡县
610300	宝鸡市	610725	勉县
610302	渭滨区	610726	宁强县
610303	金台区	610727	略阳县
610304	陈仓区	610728	镇巴县
610322	凤翔县	610729	留坝县
610323	岐山县	610730	佛坪县
610324	扶风县	610800	榆林市
610326	眉县	610802	榆阳区
610327	陇县	610821	神木县
610328	千阳县	610822	府谷县
610329	麟游县	610823	横山县
610330	凤县	610824	靖边县
610331	太白县	610825	定边县
610400	咸阳市	610826	绥德县
610402	秦都区	610827	米脂县
610404	渭城区	610828	佳县
610422	三原县	610829	吴堡县
610423	泾阳县	610830	清涧县
610424	乾县	610831	子洲县
610425	礼泉县	610900	安康市
610426	永寿县	610902	汉滨区
610427	彬县	610921	汉阴县
610428	长武县	610922	石泉县
610429	旬邑县	610923	宁陕县
610430	淳化县	610924	紫阳县
610431	武功县	610925	岚皋县
610481	兴平市	610926	平利县
610500	渭南市	610927	镇坪县
610502	临渭区	610928	旬阳县
610521	华县	610929	白河县
610522	潼关县	611000	商洛市
610523	大荔县	611002	商州区
610524	合阳县	611021	洛南县

610525	澄城县	611022	丹凤县
610526	蒲城县	611023	商南县
610527	白水县	611024	山阳县
610528	富平县	611025	镇安县
610581	韩城市	611026	柞水县
610582	华阴市	611100	杨凌农业示范区(虚拟)

注：后续新增的陕西省县及县以上行政区划代码见中华人民共和国国家统计局发布的最新数据。

附 录 B
（资料性附录）
过程密钥的产生

MAC过程密钥和数据加密钥过程密钥（统称为“过程密钥A”和“过程密钥B”）的产生如下所述。

B.1 基于单长度DEA密钥的过程密钥

第一步：卡片/发卡方决定是使用MAC DEA密钥A还是数据加密DEA密钥A（统称为“Key A”）来进行所选择的算法处理。

第二步：用Key A与预先决定的变量（如当前的交易序号）做异或运行产生过程密钥A。在做异或运算前，数据（例如：交易序号）如果少于8个字节，则在其右边用十六进制数字“0”填满。

B.2 基于双长度DEA密钥的过程密钥

第一步：卡片/发卡方决定是使用MAC DEA密钥A和B还是数据加密DEA密钥A和B（统称为“Key A”和“Key B”）来进行所选择的算法处理。

第二步：用Key A与预先决定的变量（如当前的交易序号）做异或运行产生过程密钥A。在做异或运算前，数据（例如：交易序号）如果少于8个字节，则在其右边用十六进制数字“0”填满

用Key B与第二步中产生的过程密钥A所用数据的非做异或运算得到过程密钥B。非运算是以位为单位的，把值为“1”的位转换为“0”，将值为“0”的位转换为“1”。在做异或运算前，数据如果少于8个字节，则在其右边用十六进制数字“0”填满。

附 录 C
（资料性附录）
社会公共服务卡密钥说明

分类	密钥	用途	适用范围
—	IRK	鉴别发卡方的密钥	应用提供者
—	PUK	个人密码解锁密钥	发卡方
应用维护密钥	STK MF	发卡方或应用提供方用于产生应用锁定、卡片锁定和更新二进制或记录命令的 MAC	发卡方
	STK DDF01		医疗卫生应用
	STK DDF02		银行业应用
	STK DDF03		社会保险应用
	STK DDF...		其它应用
卡片或应用锁定或者解锁密钥	BK MF	发卡方或应用提供方控制锁定卡片或应用操作的密钥	发卡方
	LK DDF01		医疗卫生应用
	LK DDF02		银行业应用
	LK DDF03		社会保险应用
	LK DDF…		其它应用
卡片或者应用数据更新密钥	UK MF	发卡方或应用提供方 控制应用数据更新操作的密钥	发卡方和持卡人基本信息
	UK1 DDF01		医疗卫生应用
	UK2 DDF02		银行业应用
	UK3 DDF03		社会保险应用
	UK… DDF…		其它应用
交易密钥	DLK	用来产生帐户划入交易中使用的过程密钥（SESLK），在帐户划入交易中计算 MAC	帐户划入交易
	DPK	用来产生消费交易中使用的过程密钥（SESPK），在各个应用消费交易中计算 MAC。	医疗卫生、社会保险、生育保险医疗、银联消费交易（脱网）等
	DTK	用来产生帐户支付、个人自付和统筹基金等支付交易中使用的 TAC	医疗保险、社会保险交易、银行交易等
	DSK	控制和更新年度起始日期	医疗保险、社会保险、银行等
应用数据读取密钥	RK1 DDF01		医疗卫生应用
	RK2 DDF02		银行业应用
	RK3 DDF03		社会保险应用
	RK… DDF…		其它行业应用

附 录 D
（资料性附录）
省人口库共享数据目录

序号	数据项名称	类型	长度	采用标准或说明	来源
001	姓名	C	20	小于等于 20 位	公安
002	性别	C	1	GB/T 2261.1	卫生
003	出生日期	D	8	GB/T 7408	卫生
004	民族	C	2	GB/T 3304	公安
005	公民身份证号码	C	18	GB 11643 15 到 18 位	公安
006	最近婚姻状况	C	2	GB/T 2261.2	民政
007	初婚日期	D	8	GB/T 7408	民政
008	最近婚姻变动日期	D	8	GB/T 7408	民政
009	户口类型	C	1	GA 324.1-2001	公安
010	照片	Blob			公安
011	现居住地地址	C	200	省+地+县+乡+村	人口计生或公安
012	户籍地地址	C	200	省+地+县+乡+村	公安
013	流动状况	N	2		人口计生或公安
014	居住状况	C	1		人口计生
015	户口性质	C	1	GB/T 17538	公安
016	出生地	C	200	省+地+县+乡+村	卫生
017	血型	C	30	GA 324.6-2001	卫生
018	身份证签发信息	C		参考公安标准	公安
019	身份证有效期	D	8	GB/T 7408	公安
020	个人身份	C	1	GB/T 14946-2002	公安
021	户号	C	9	GA 214-1999	公安
022	家庭关系	C	2	GB/T 4761-2008	公安
023	户口注销类别	C	2	参照 GA 324.2-2001 指定地方标准	公安
024	户口注销时间	D	8	GB/T 7408	公安
025	健康状况	C	2	GB/T 4767-1984	卫生
026	死亡日期	D	8	GB/T 7408	民政或卫生或公安
027	死亡原因	C	2	参照 GA 324.2-2001 地方标准	卫生
028	学历	C	2	GB/T 4658	教育
029	专业	C	6	GB/T 16835-1997	教育

序号	数据项名称	类型	长度	采用标准或说明	来源
030	毕业学校	C	100		教育
031	毕业时间	D	8	GB/T 7408	教育
032	就业状态	C	3	LB 101-2000	人社
033	工作单位	C	100		人社
034	参加工作时间	D	8	GB/T 7408	人社
035	行业类别	C	6	GB/T 4754-1994	人社
036	职业类别	C	3	GB/T 6565-1999	人社
037	累计参加养老保险时间	N	3		人社
038	最近参加养老保险日期	D	8	GB/T 7408	人社
039	累计参加医疗保险时间	N	3		人社
040	最近参加医疗保险日期	D	8	GB/T 7408	人社
041	累计参加失业保险时间	N	3		人社
042	最近参加失业保险日期	D	8	GB/T 7408	人社
043	低保金发放金额	N	10.2		民政
044	低保金发放日期	D	8	GB/T 7408	民政
045	人员低保对象身份标志	Boolean			民政
046	税务信息	C			税务
047	法人信息	C			工商
048	住房信息	C			住房和公积金
049	公积金贷款信息	C			住房和公积金
050	独生子女父母光荣证时间	D	8	GB/T 7408	人口计生
051	备注	C	100		

注：姓名、性别、出生日期、出生地、民族、公民身份证号码为国家基本项；为社会公共服务卡必选数据项；黑体部分为社会公共服务卡选取的其它基础数据项；若需要数据，可在其中为扩展，省人口数据库中的其它信息正在采集中。

附 录 E
（规范性附录）
社会公共服务卡数据的元数据

社会公共服务卡个人基础数据来自于省人口数据共享目标，所列元数据的表格如下：

<table>
<tr><td rowspan="8">个人身份识别数据</td><td>姓 名</td><td colspan="2"></td><td rowspan="3">照片</td></tr>
<tr><td>性别</td><td colspan="2">1男□ 2女□</td></tr>
<tr><td>出生日期</td><td colspan="2">□□□□年□□月□□日</td></tr>
<tr><td>身份标识</td><td colspan="3">居民身份证 居民身份证件号码：□□□□□□□□□□□□□□□□□□ 其他证件证件号码： □□□□□□□□□□□□□□□□□□</td></tr>
<tr><td>民族</td><td>1 汉 2 少数民族_____□</td><td>本人电话</td><td></td></tr>
<tr><td>婚姻状况</td><td colspan="3">1已婚 2未婚 3离婚 4丧偶 5未说明的婚姻状况 □</td></tr>
<tr><td>血型</td><td colspan="3">血型： 1 A型 2 B型 3 AB型 4 O型 /RH阴性：1否 2 是 □/□</td></tr>
<tr><td></td><td>健康状况</td><td colspan="3"></td></tr>
<tr><td></td><td>职业</td><td colspan="3">1 国家机关、党群组织、企业、事业单位负责人2 专业技术人员3商业、服务业人员 4办事人员 5农、林、牧、渔、水利业生产人员 6生产、运输设备操作人员 7军人8 其他 □</td></tr>
<tr><td></td><td>工作单位</td><td colspan="3"></td></tr>
<tr><td></td><td>学历</td><td colspan="3">1 文盲及半文盲 2 小学 3 初中 4 高中/技校/中专 5 大学专科及以上 6 不详 □</td></tr>
<tr><td></td><td>联系人</td><td colspan="3">1. 姓名_____与持卡人的关系_____电话_____；
2. 姓名_____与持卡人的关系_____电话_____；
3. 姓名_____与持卡人的关系_____电话_____；</td></tr>
<tr><td></td><td>户籍地址</td><td colspan="3">_____省_____市_____县（区）_____乡(镇、街道)
_____(村)居委会</td></tr>
</table>

	现居住地址	_____省_____市_____县（区）____ ___乡(镇、街道) _____(村)居委会 (当现居住地址与户籍地址不符合时填写)
备注：		

1、性别：如果两性畸形，选择显性的那个性别。

2、出生日期：根据居民身份证的出生日期填写。按照年（4 位）、月（2 位）、 日（2 位）顺序填写，如 19490101。

3、身份证号：需如实、完整填写。如果不是居民身份证，需填写证件名称及 证件号码。

4、照片：根据标准要求采集。

5、民族：少数民族应填写全称，如彝族、回族等。

6、联系人电话：填写确实能够及时、有效取得联系的电话号码。

7、婚姻：

——已婚：指在婚者，包括曾离婚或丧偶现已再婚的人。

——未婚：指建档之前从未结过婚的人。

——离婚：指建档时已与配偶解除婚姻关系，且未再婚的人。

——丧偶：指配偶去世未再婚的人。

8、血型:在前一个 “□”内填写与 ABO 血型对应编号的数字;在后一个“□” 内填写是否为“RH 阴性”。

9、职业：

“国家机关、党群组织、企业、事业单位负责人”指在中国共产党中央委员 会和地方各级党组织、各级人民代表大会常务委员会、人民政协、人民法院、人 民检察院、国家行政机关、各民主党派、工会、共青团、妇联等人民团体，群众 自治组织和其他社团组织及其工作机构、企业、事业单位中担任领导职务并具有 决策、管理权的人员。

“专业技术人员”指专门从事各种科学研究和专业技术工作的人员。“商业、服务业人员”指从事商业、餐饮、旅游、娱乐、运输、医疗辅助服务及社会和居民生活等服务工作的人员。 “办事人员”指在国家机关、党群组织、企业、事业单位中从事行政业务、行政事务工作的人员和从事安全保卫、消防、邮电等业务人员。

“农、林、牧、渔、水利生产人员”指从事农业、林业、畜牧业及水里生产、 管理、产品初加工的人员。

“生产、运输设备操作人员”指从事矿产勘查、开采，产品的生产制造、工 程施工和运输设备操作的人员及有关人员。

10、联系人：指紧急情况联系人。需至少填写一位联系人的姓名、与持卡人 的关系、联系电话。这里要求填写与建卡对象关系紧密的亲友姓名，该联系人应

为当遇特殊情况或紧急情况无法与建档对象直接沟通而急需建卡对象亲友提供 帮助时，确实可以取得联系并能提供帮助的人。

11、户籍地址：需如实填写户籍所在地，准确到村（居委会）。

12、现居住地：当居住地与户籍地址不符时填写，该地址应为建卡人常住或 近期居住地址。

附 录 F
（规范性附录）
社会公共服务卡数据结构说明

F.1 基本数据区（MF）

F.1.1 发卡机构数据文件

文件标识	EF05	短文件标识	05	文件类型	变长记录文件
文件存取控制		读：无		写：UKMF	文件大小：32

序号	标志	数据项	类型	长度(16 进制)
01	01	卡的识别码[必选项目]	Cn	10
02	02	卡的类别[必选项目]	An	01
03	03	规范版本[必选项目]	An	04
04	04	初始化机构编号[必选项目]	Cn	0C
05	05	发卡日期[必选项目]	Cn	04
06	06	卡有效期[必选项目]	Cn	04
07	07	卡号[必选项目]	An	09

F.1.2 持卡人基本信息数据文件

文件标识	EF06	短文件标识	06	文件类型	变长记录文件
文件存取控制		读：无		写：UKMF	文件大小：39

序号	标志	数据项	类型	长度(16 进制)
01	08	公民身份证号码[必选项目]	An	12
02	09	姓名[必选项目]	An	1E
03	0A	性别[必选项目]	An	01
04	0B	民族[必选项目]	Cn	01
05	0C	出生地[必选项目]	Cn	03
06	0D	出生日期[必选项目]	Cn	04

F.1.3 指纹数据文件

文件标识	EF07	短文件标识	07	文件类型	二进制文件
文件存取控制		读：无		写：UKMF	文件大小：300

序号	标志	数据项	类型	长度(16 进制)
01	1A	指纹[必选项目]	B	300

F.1.4 户籍信息文件

文件标识	EF08	短文件标识	08	文件类型	变长记录文件

文件存取控制		读：PIN	写：UK MF	文件大小：51
序号	标志	数据项	类型	长度(16 进制)
01	20	户口类别[必选项目]	An	01
02	21	常住户口所在地地址[必选项目]	An	3E
03	22	常住户口所在地地址扩展[可选项目]	An	12

F.1.5 通讯信息文件

文件标识	EF09	短文件标识	09	文件类型	变长记录文件
文件存取控制		读：PIN	写：UK MF	文件大小：62	
序号	标志	数据项	类型	长度(16 进制)	
01	25	通讯地址[必选项目]	An	3E	
02	26	通讯地址扩展[可选项目]	An	12	
03	27	通讯地址邮政编码[必选项目]	Cn	03	
04	28	联系电话[必选项目]	An	0F	

F.1.6 个人状况信息文件

文件标识	EF0A	短文件标识	0A	文件类型	定长记录文件
文件存取控制		读：PIN 或 UK MF	写：UK MF	文件大小：4E	
序号	标志	数据项	类型	长度	
01	29	个人就业或离退休状态[必选项目]	An	01	
02	2A	文化程度[必选项目]	Cn	01	
03	A0	个人 ID 号，[必选项目]	An	0A	
04	A1	人员类别，[必选项目]	An	03	
05	A2	人员身份，[必选项目]	Cn	01	

F.1.7 婚姻状况信息文件

文件标识	EF0B	短文件标识	0B	文件类型	变长记录文件
文件存取控制		读：PIN	写：UK MF	文件大小：1	
序号	标志	数据项	类型	长度	
01	2B	婚姻状况[必选项目]	An	01	

F.1.8 就业单位信息文件

文件标识	EF0C	短文件标识	0C	文件类型	变长记录文件
文件存取控制		读：PIN 或 UK	写：UK MF	文件大小：105	
序号	标志	数据项	类型	长度	
01	2E	单位名称[必选项目]	An	3E	
02	2F	单位名称扩展[可选项目]	An	08	
03	30	单位类型[必选项目]	An	01	
04	31	单位参保险种[必选项目]	An	0A	
05	32	单位隶属关系[必选项目]	An	01	
06	32	单位编码(ID) [必选项目]	An	08	

07	33	单位通讯地址[可选项目]	An	64
08	34	单位邮政编码[可选项目]	An	06
09	35	单位联系电话[可选项目]	An	0D

F.1.9 卡内应用数据文件

文件标识	DIR	短文件标识	01	文件类型	变长记录文件
文件存取控制		读：UK MF		写：UK MF	文件大小：120

序号	标志	数据项	类型	长度(16 进制)
01	40	卡中的应用数目[必选项目]	An	2
02	41	应用 1 的名称[必选项目]	cn	2E
03	42	版本号[必选项目]	cn	06
04	43	激活状态[必选项目]	An	01
05	44	应用 2 的名称[必选项目]	Cn	2E
06	45	版本号[必选项目]	Cn	06
07	46	激活状态[必选项目]	An	01
08	47	应用 3 的名称[必选项目]	cn	2E
09	48	版本号[必选项目]	cn	06
10	49	激活状态[必选项目]	An	01
11	50	应用 4 的名称[必选项目]	Cn	2E
12	51	版本号[必选项目]	cn	06
13	52	激活状态[必选项目]	An	01

注：“类型”项是指一种数据表示类型，其中“cn”表示压缩数字(Compressed Numeric)，“an”表示字母数字型(Alphanumeric)。“长度”项采用的是十六进制表示。当为数据定义的长度超过数据实际长度，而位数没有占满时，补位规则如下：

——格式 cn 的数据元左对齐，右补 F；

——格式 an 的数据元左对齐，右补 0。

F.2 行业应用数据区(DDF)

社会保险、医疗卫生、银行等应用中的业务数据结构和密钥由各自卡片规范规定。

参 考 文 献

[1] 陕西省信息化领导小组《数字陕西·智慧城市”发展纲要（2013-2017）》。