中国人民银行银川中心支行 宁夏回族自治区卫生和计划生育委员会关于发布《宁夏公共服务卡（居民健康卡）设计规范》的通知

宁银发〔2015〕172号

人民银行各市中心支行；各卫生计生委、局，自治区卫生计生委直属各单位；各国有商业银行宁夏分行，各股份制商业银行银川分行，中国邮政储蓄银行宁夏分行，宁夏银行，宁夏黄河农村商业银行，石嘴山银行；中国银联宁夏分公司：

为指导各参与银行按照统一规范对宁夏公共服务卡（居民健康卡）的卡片空间和卡面进行产品设计，确保宁夏公共服务卡（居民健康卡）卡面统一，并实现联网通用，人民银行银川中心支行、自治区卫生计生委在遵循PBOC 3.0标准和居民健康卡等相关行业应用规范的基础上，根据宁夏公共服务卡（居民健康卡）的设计目标及应用范围，制定了《宁夏公共服务卡（居民健康卡）设计规范V1.0》（简称《设计规范》），现予以发布，并就宁夏公共服务卡（居民健康卡）发行工作有关事宜通知如下。

一、《设计规范》对各参与银行以金融IC卡为载体，通过加载居民健康应用及公共服务领域其他行业应用，在全区范围内发行的宁夏公共服务卡（居民健康卡）行业应用加载、卡片空间

结构、卡面设计进行通用性规范约束。各市如要发行加载其他有特殊要求的行业应用（如市民一卡通）的宁夏公共服务卡（居民健康卡），可在遵循《设计规范》通用性要求、保持卡片空间基本结构和卡面固定元素不变的前提下，对卡面和卡片空间的可变元素及内容作个性化设计。设计方案应报送人民银行银川中心支行和宁夏卫生计生委批准后方可实施。

二、金融IC卡多应用银行间共享平台（简称“TSM平台”）是宁夏公共服务卡（居民健康卡）中居民健康应用个人化数据及其他后加载行业应用在参与银行间实现共享及动态分配的重要枢纽，同时也是《设计规范》所依托的基础技术环境，各参与银行应按照人民银行银川中心支行相关技术要求，规范开展行内发卡相关系统与TSM平台的对接工作，做好宁夏公共服务卡（居民健康卡）发行前的基础技术环境准备。

三、各参与银行发行宁夏公共服务卡（居民健康卡）前，应严格遵循《设计规范》开展宁夏公共服务卡（居民健康卡）的产品设计工作，制作测试样卡，并分别提交人民银行银川中心支行科技处、自治区卫生计生委信息中心作TSM系统、居民健康卡卡管及受理环境下的技术检测，检测合格后，须分别提交国家卫生计生委相关检测部门和银行卡检测中心作居民健康标准、PBOC3.0标准的技术检测，并报中国银联总公司备案。

四、各参与银行首次发行宁夏公共服务卡（居民健康卡），须提请人民银行银川中心支行、自治区卫生计生委分别根据各自

的业务管理范围进行技术标准符合性审核，审核通过后，方可面向社会公开发行。审核的内容主要包括发卡相关后台系统技术方案、卡面设计方案、卡空间设计方案、发行方案及相关单位对测试样卡的检测报告。

五、宁夏公共服务卡（居民健康卡）的卡片制造商、芯片制造商由各参与银行在国家卫生计生委公布的居民健康卡入围厂商名单中选择,经自治区卫生计生委信息中心审核备案后确认。

六、《设计规范》自发布之日起实施。

宁夏公共服务卡（居民健康卡）设计规范

版本:V1.0

2015-12-02 发布　　2015-12-02 实施

中国人民银行银川中心支行

宁夏回族自治区卫生和计划生育委员会　　发布

修改记录

日期	版本	章节	修改内容	修订人
2015.6	V1.0	全部	创建规范	
2015.11	V1.0	部分	修订规范	

目 录

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本规范参照 PBOC3.0 标准和居民健康卡相关行业应用规范起草。

本规范由中国人民银行银川中心支行和宁夏回族自治区卫生和计划生育委员会共同负责解释。

引　言

为规范宁夏公共服务卡（居民健康卡）卡面设计和卡片空间使用，确保各单位发行的宁夏公共服务卡（居民健康卡）遵循统一标准，并能联网通用，特制订本设计规范。

本设计规范定义了宁夏公共服务卡（居民健康卡）应用规范及卡片结构规范相关内容，包括普通IC卡的结构规范以及可视IC卡相关产品说明。

本设计规范对宁夏全区金融IC卡加载居民健康应用的卡片的应用规范及卡面设计进行约束，为全区通用版本，宁夏区内各城市如要发行加载其他行业应用（如市民一卡通应用）的宁夏公共服务卡（居民健康卡），须在遵循此规范基础上，对可变元素及内容进行设计，设计方案须报送人民银行银川中心支行和宁夏回族自治区卫生计生委批准后方可实施。

宁夏公共服务卡（居民健康卡）设计规范

1. 范围

本规范主要对宁夏公共服务卡（居民健康卡）应用卡片技术要求、文件结构进行了规定。适用于宁夏公共服务卡（居民健康卡）设计、生产、发行及使用过程中涉及的所有参与者，包括但不限于宁夏公共服务卡（居民健康卡）发卡机构、收单机构、卡片制造商、个性化服务提供商，以及授权使用宁夏公共服务卡（居民健康卡）标识并参与宁夏公共服务卡（居民健康卡）应用业务或提供相关服务的所有机构。

2. 卡片遵循标准

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本规范。

ISO/IEC 14443-1 识别卡 无触点集成电路卡 近程卡 第 1 部分：物理特性，2000-04-15

ISO/IEC 14443-2 第 2 部分：射频功率和信号接口， 2001-07-01

ISO/IEC 14443-3 第 3 部分：初始化和防冲突，2001-02-01

ISO/IEC 14443-4 第 4 部分：传输协议，2002-02-01

JR/T 0025.3 -2013 《中国金融集成电路（IC）卡规范》

《金融 IC 卡通用应用数据存储规范》

《居民健康卡技术规范》

GP2.1.1 规范

Java2.2.1 规范

3. 符号、缩略语和术语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

CPU 卡 Central Processing Unit Card

带有中央处理器（CPU）、存储单元以及芯片操作系统的集成电路卡。

3.1.2

芯片 Chip

本规范中特指卡中用于完成数据处理和存储功能的集成电路器件。

3.1.3

芯片操作系统 COS，Chip Operating System

CPU 卡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 CPU 卡芯片与外界信息交换为目的的嵌入式软件。

3.1.4

命令 Command

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.1.5

连接 Concatenation

两个元素的连接是指将第二个元素附加到第一个元素的末尾。每个元素的字节在结果串中的排列顺序与其从 IC 卡发送到终端的顺序相同，即：高位字节先送。每个字节位按照从最高位到最低位的顺序排列。一组元素或对象可以通过最先两个相连的方式连接成一个新元素，即第一个与第二个相连，再与第三个相连，…，依次类推。

3.1.6

触点 Contact

在集成电路卡和外部接口设备之间保持电流连续性的导电元件。

3.1.7

响应 Response

IC 卡处理完成收到的命令报文后，返回给终端的报文。

3.1.8

交易 Transaction

持卡者和业务、管理部门之间根据卡所支持的应用接受、提供服务的行为。

3.1.9

功能 Function

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.1.10

报文 Message

由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

3.1.11

报文鉴别代码 Message Authentication Code

对交易数据及其相关参数进行运算后产生的代码。主要用于验证报文的完整性。

3.1.12

明文 Plain text

没有加密的信息。

3.1.13

密文 Cipher text

通过密码系统产生的不可理解的文字或信号。

3.1.14

密钥 Key

控制加密转换操作的符号序列。

3.1.15

加密算法 Cryptographic Algorithm

为了隐藏或揭露信息内容而变换数据的算法。

3.1.16

对称加密技术 Symmetric Cryptographic Technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

3.1.17

非对称加密技术 Asymmetric Cryptographic Technique

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

3.1.18

私有密钥 Private Key

一个实体的非对称密钥对中仅供实体自身使用的密钥，在数字签名模式中，私有密钥用于签名功能。

3.1.19

公共密钥 Public Key

一个实体的非对称密钥对中可以公开的密钥，在数字签名模式中，公共密钥用于验证功能。

3.1.20

保密密钥 Secret Key

对称加密技术中仅供指定实体所用的密钥。

3.1.21

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。

3.1.22

数字证书（或证书） digital certificate

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

3.1.23

数据完整性 Data Integrity

数据不受未经许可的方法变更或破坏的属性。

T=0

面向字符的异步半双工传输协议。

3.1.24

应用 Application

卡片和终端之间的应用协议和相关的数据集。

3.1.25

命令 Command

终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

3.1.26

密文 Cryptogram

加密运算的结果。

3.1.27

功能 Function

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

3.1.28

集成电路 Integrated Circuit(IC)

完成处理和/或存储功能的电子器件。

3.1.29

集成电路卡（IC）Integrated Circuit(s) Card

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

3.1.30

接口设备

终端上插入 IC 卡的部分，包括其中的机械和电气部分。

3.1.31

响应 Response

IC 卡处理完收到的命令报文后，返回给终端的报文。

3.1.32

脚本（Script）

发卡行向终端发送的命令或命令序列，目的是向 IC 卡连续输入命令。

3.1.33

终端 Terminal

为完成金融交易而在交易点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其它部件和接口，例如与主机通讯的接口。

3.2 符号、缩略语

表 1 所列的符号和缩略语适用于本规范。

表 1 缩略语和符号表示

AID	应用标识符 Application Identifier
APDU	应用协议数据单元 Application protocol Data Unit
An	字母数字型 Alphanumeric
Ans	特殊字母数字型 Alphanumeric Special
B	二进制 Binary
CLA	命令报文的类别字节 Class Byte of Command Message
Cn	压缩数字 Compressed Numeric
COS	芯片操作系统 Chip Operating System
CVN	卡安全码 Card Verification Number
DDF	目录定义文件 Directory Definition File
DEA	数据加密算法 Data Encryption Algorithm
DF	专用文件 Dedicated File
EF	基本文件 Elementary File
FCI	文件控制信息 File Control Information
HEX	十六进制数 Hexadecimal
FID	文件标识符 File Identifier
IC	集成电路 Integrated Circuit
IEC	国际电工委员会 International Electrotechnical Commission
INS	命令报文的指令字节 Instruction Byte of Command Message
ISO	国际标准化组织 International Organization for Standardization
MAC	报文鉴别代码 Message Authentication Code
MF	主控文件 Master File
SAM	安全存取模块 Secure Access Module
RID	已注册的应用提供者标识 Registered Application Provider Identifier
INS	命令报文的指令字节 Instruction Byte of Command Message
ISO	国际标准化组织 International Organization for Standardization
LC	终端发出的命令数据的实际长度 Exact Length of Data Sent
Le	响应数据中的最大期望长度 Maximum Length of Data Expected
n	数字型 Numeric
POS	销售点终端 Point of Service
PSAM	销售点终端安全存取模块
PSE	支付系统环境 Payment System Environment
RID	已注册的应用提供者标示 Registered Application Provider Identifier

4. 卡片应用基本要求

宁夏公共服务卡（居民健康卡）应用与标准 PBOC3.0 应用、居民健康卡应用和通用存储应用共存于同一张 IC 卡，各应用之间互相独立，互不干扰。在应用内部各自遵循自定义的应用流程和安全机制。

卡片用户空间还应预留用于其他行业应用软件包加载及个人化，包括交通、旅游、教育、民生服务等领域应用，供持卡人自由选择，实现“多卡合一、一卡多用、全区通用”。

综合目前现有的几大应用，对芯片容量做出如下要求：国产双界面 Java 芯片，不低于 80K 用户存储空间。

卡片的选择需要遵循分享的行业应用能被动态加载的原则，能够动态部署多应用技术的 IC 卡卡片。

为了实现这些基本要求，对卡片的选择需要遵循 GP（Global Platform）卡规范 V2.1.1 及以上版本。卡片的最终控制权是由发卡方掌握，通过 GP 规范的卡片架构，卡片的管理者和行业应用分享的合作伙伴能够以某种恰当的方式来管理自己运行在卡片上的应用。

为了实现对卡片的灵活管理，遵循 GP 规范的 Java 卡内架构了各类应用组件。卡片上运行了来自应用使用方和应用提供方的行业应用。所有这些应用必须在一个安全的运行环境中实现，该运行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。

卡片管理器作为 GP 架构中的首要组件起到了 GP 卡片中心管理者的作用，特定的密钥和安全管理应用被称作安全域。

在 Java 卡内存在各类应用组件，包括安全域、应用 PACKAGE 包、应用实例，其中安全域负责确保发卡方和其他安全域提供者之间密钥的完全隔离，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(应用使用方、应用提供方、应用提供者、授权管理者)的应用进行数字签名的生成与验证。

5. 宁夏公共服务卡（居民健康卡）说明及文件结构规范

宁夏公共服务卡（居民健康卡）发行，要求卡片生产商向发卡银行提供以下两种卡片的产品：

1．卡片在卡商出厂后，卡片已经写入各应用的相关正式密钥及数据。

此卡简称：预置卡

2．卡片在卡商出厂后，创建应用结构，按照行业机构要求写入初始密钥全 FF 或正式密钥，卡片不写入正式数据，后期进行数据写入。

此卡简称： 白卡

宁夏公共服务卡(居民健康卡)全区通用版卡片应用结构如图 1 所示。

宁夏区内如有城市需要发行加载其他行业应用（如市民一卡通应用）的宁夏公共服务卡（居民健康卡），可在此文件结构基础上，通过增加“市民一卡通应用”一级文件结构，或在“预留应用”目录增加下一级文件结构。

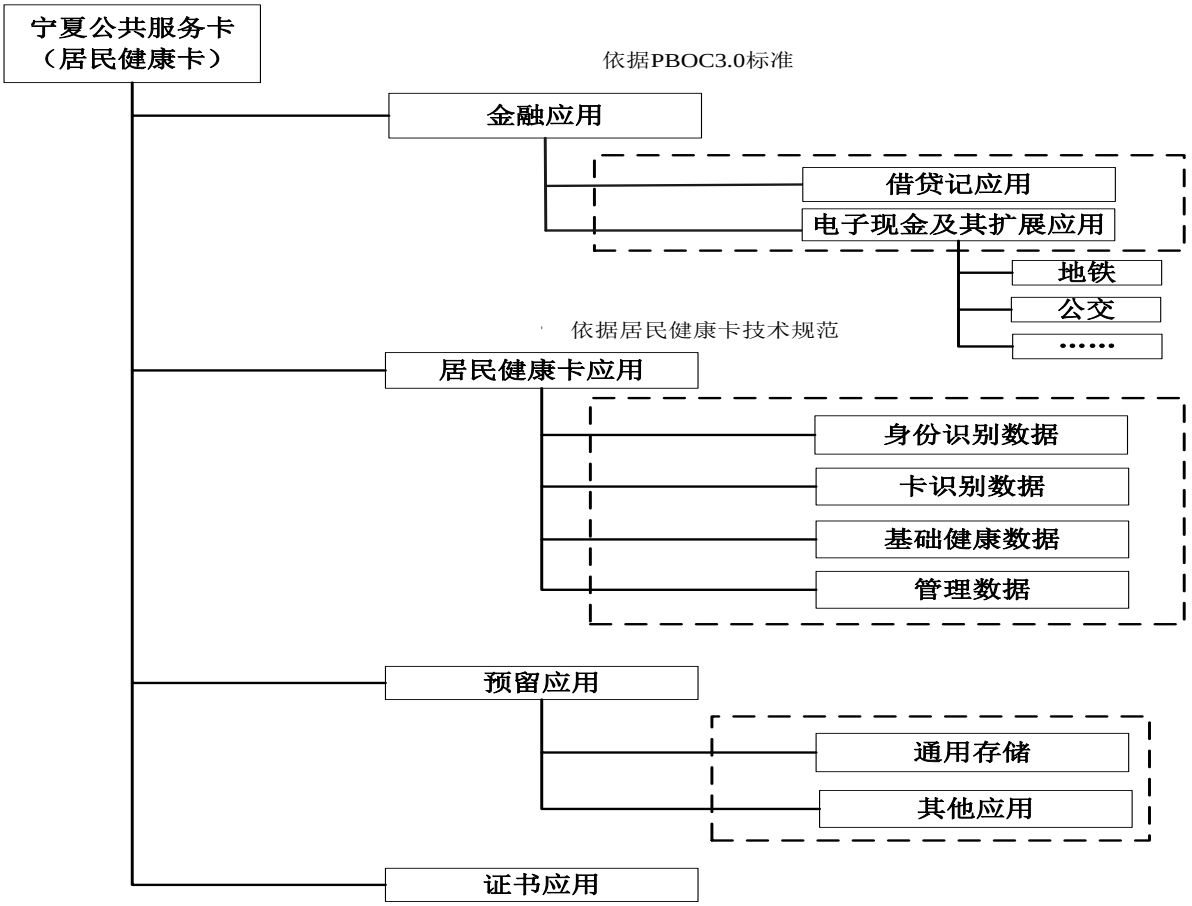


图 1 卡片应用结构

6. 宁夏公共服务卡（居民健康卡）卡面标识规范

本部分对宁夏公共服务卡（居民健康卡）卡面表示进行定义，卡面设计以中信银行为示例，各发卡银行需根据自身情况对发卡银行 Logo 作个性化设计。对于本节中未定义的卡面规范，参照《银联卡业务运作规章》第三卷：卡片 BIN 号及标识规则规定执行，本部分不做具体阐述。

6.1 卡片外形规格

宁夏公共服务卡（居民健康卡）的标准卡片外形为矩形，具体规格如下：

卡片宽度：W=85.60mm ±0.30mm；

卡片高度：H=53.98mm±0.30mm；

卡片厚度：T=0.76mm±0.08mm；

宁夏公共服务卡（居民健康卡）卡片的所有倒角半径为 3.18±0.30mm。

宁夏公共服务卡（居民健康卡）的标准卡规格图如图 2 所示（以中信银行为例）：

图 2　宁夏公共服务卡（居民健康卡）标准卡规格图

在宁夏公共服务卡（居民健康卡）全区通用版标准卡规格图中，芯片、银联标志、闪付（QuickPass）标识、银联全息防伪标识的放置规格参照本章 6.2 和 6.5 节相关规定。银行卡卡号、磁条及持卡人签名条、银行标识（Logo）、银行卡卡号等信息规格参照《银联卡业务运作规章》中相关要求。“服务电话”、“持卡人签名”字体下方备注文字为可变元素，各银行可根据实际情况进行更改。居民健康卡 Logo，宁夏通 Logo，为字体及图片大小、位置、颜色等要素不可变元素；宁夏回族自治区卫生和计划生育委员会 Logo，宁夏 12320 卫生热线二维码为内容、颜色不可变元素，图片及二维码大小及放置位置可变。卡片正面背景为可变元素，但卡片背景的选择应以美观，易于识别其他标识为基本原则。

6.2 芯片

宁夏公共服务卡（居民健康卡）卡片嵌入的芯片应满足：

1. 国产双界面高安全CPU卡芯片；
2. 存储空间不低于80K；
3. 遵循ISO/IEC 7816-1/2/3/4关于芯片的要求；
4. 遵循ISO/IEC 14443 TYPE A/B关于芯片的要求；
5. 符合JR/T 0025.4-2013关于芯片的要求；
6. 符合DB11T 159关于芯片的要求；
7. 符合LB002-2000关于芯片的要求；
8. 符合《居民健康卡技术规范》关于芯片的要求；
9. 符合Q/CPU 040-2011银联卡芯片安全规范；
10. 具有《银联卡芯片产品安全认证证书》。

芯片必须放置在卡片正面，芯片规格示意图如图 3 所示：

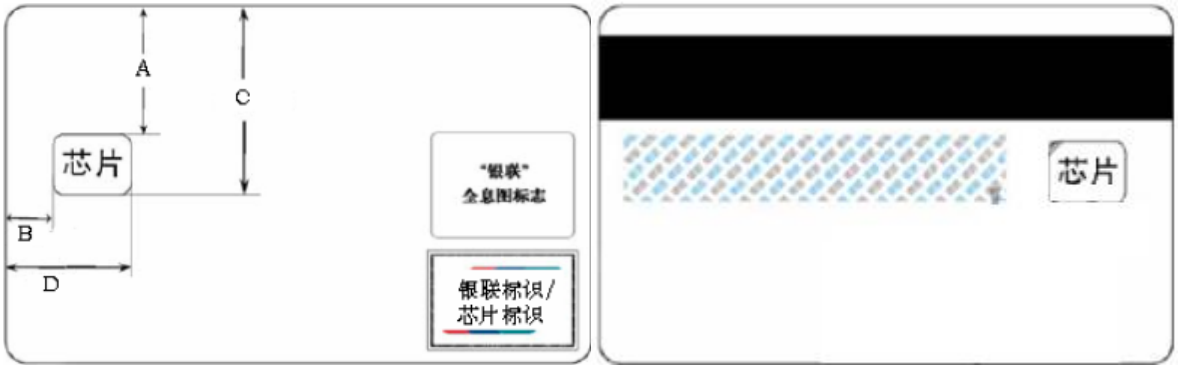


图 3 “银联”标识下置格式时的芯片规格示意图

芯片规格尺寸说明如表 2 所示：

表 2 芯片规格说明表

描述	位置及尺寸
接触式芯片	芯片位于卡片左侧卡号上方，具体触点应符合 ISO 7816 标准
芯片的高度	9.32mm
芯片的宽度	9.62mm
A 芯片的上边沿至卡片上边沿的距离	19.23mm
B 芯片的左边沿至卡片左边沿的距离	10.25mm
C 芯片的下边沿至卡片下边沿的距离	28.55mm
D 芯片的右边沿至卡片右边沿的距离	19.87mm

非接触式芯片规格应符合 ISO/IEC 7810 中规定的 ID-1 型卡的尺寸、物理特性要求，非接触式芯片可放置在卡片的四个角位置的任意一角，推荐放置在卡片正面的左下角，其他标准应符合 ISO/IEC 14443 的相关规定。

6.3 COS 要求

宁夏公共服务卡（居民健康卡）全区通用版本卡片 COS 应满足：

1. 符合JR/T 0025.4-2013关于COS的要求；
2. 符合DB11T 159关于COS的要求；合LB002-2000关于COS的要求；
3. 符合《居民健康卡技术规范》关于COS的要求；
4. 具有《银联卡嵌入式软件安全认证证书》；
5. 支持GP（Global Platform）卡规范V2.1.1及以上版本。
6. 为节省EEPROM空间，建议居民健康应用的CAP可以硬掩膜方式加载入卡片内。

6.4 制卡要求

宁夏公共服务卡（居民健康卡）卡片制卡推荐要求：

1. 芯片制造机构应具有中华人民共和国工业和信息化部颁发的《集成电路设计企业认定证书》。
2. 芯片制造机构应具有国家集成电路卡注册中心分配的注册标识号和注册证书。
3. 芯片制造机构应具有国家知识产权局颁发的《集成电路布图设计登记证书》。
4. 芯片制造机构应具有商用密码产品销售许可证、商用密码产品生产定点单位证书。
5. 卡片制造机构应具有国家集成电路卡注册中心注册证书和IC 卡生产许可证。
6. 卡片制造机构应具有全国工业产品生产许可证。
7. 卡片制造机构应具有银联标识产品企业资质认证证书。

8. 卡片制造机构应具有商用密码产品销售许可证。

6.5 银联标识

在仅具有小额支付功能的电子现金芯片卡上，应在卡片正面的银联标识区主标识位置贴放银联电子现金专用标识。

对同时具有借贷记功能和电子现金功能的芯片或磁条/芯片复合卡，在卡片正面的银联标识区主标识位置放置银联主标识，并在卡片背面磁条及签名条覆盖区域以下左侧空白区域，放置专用的银联电子现金专用标识。

仅银联信用卡方可贴印银联全息防伪标识。

银联主标识如图 4 所示：

银联主标识

图 4 银联主标识示意图

6.6 卫生标识

宁夏公共服务卡（居民健康卡）卫生标识如图 5 所示：

图 5 宁夏公共服务卡（居民健康卡）卫生标识示意图

6.7 附加信息

宁夏公共服务卡（居民健康卡）卡片上应印制、放置的要素内容及其规格、位置，除遵循现有银联卡卡片规范外，还应包括宁夏公共服务卡（居民健康卡）标识和卡片功能说明等要素，且必须采用银联标识下置格式的规格标准。

卡片功能说明：

宁夏公共服务卡（居民健康卡）卡片功能说明：本卡符合宁夏公共服务卡（居民健康卡）行业应

用规范，可用于宁夏区内通过金融标准认证的公共交通公用事业终端，包括：交通、旅游、教育、民生服务等领域应用，供持卡人自由选择，实现“多卡合一、一卡多用、全区通用”。

7. 机电特性与通讯协议

7.1 机电特性

本节描述的机电特性包括 IC 卡的物理特性和电气特性。

宁夏公共服务卡（居民健康卡）卡的机电特性应遵从 GB/T 16649 标准、ISO/IEC 7816 系列标准、GB/T 14916-2006 标准、ISO/IEC 14443 TYPE-A/B 系列标准的相关要求。

7.2 通讯协议和复位应答

7.2.1 接触接口

通讯协议

符合 ISO/IEC 7816-3 T=0 通讯协议。

复位应答（ATR）

在终端发出复位信号后，IC 卡以一串字节作为应答（即复位应答）。这些传输到终端的字节规定了卡和终端之间即将建立的通信的特征。

宁夏公共服务卡（居民健康卡）卡片的复位应答（ATR）信息如下：

3B	6x（'0'~'F'）	00	00	历史字节（0~15 字节）

其中历史字节定义：

2 字节	3 字节	2 字节	6 字节
芯片商注册标识号	COS 名称和版本	卡制造商注册标识号	唯一序列号

7.2.2 非接触接口

通讯协议

符合 ISO/IEC 14443-3 TYPE A/B 通讯协议。

复位应答（ATS）

IC 卡上电检测到处于非接触通讯方式后，等待接收 REQA 或 WUPA 命令，如果接收到 REQA 或 WUPA 命令，则 IC 卡返回 ATQA。

接收到 ATQA 后，读卡器发出防冲突和选卡指令，当 IC 卡被选中时，IC 卡返回 SAK；读卡器接

收到 SAK 后，如果 IC 卡支持 ISO/IEC 14443-4，则读卡器发送 RATS 命令给 IC 卡，IC 卡接收到 RATS 命令后，返回一个 ATS。

宁夏公共服务卡（居民健康卡）卡片的复位应答（ATS）信息如下：

XX(‘05’~‘14’)	‘78’	TA1	TB1	‘02’	历史字节（0~15 字节）

其中历史字节定义：

2 字节	2 字节	4 字节
芯片商注册标识号	卡片制造商注册标识	唯一序列号

8. 安全域管理

8.1 密钥管理应用构成

宁夏公共服务卡（居民健康卡）全区通用版密钥管理应用构成如表 3 所示：

表 3 密钥管理应用构成

应用区	安全域	密钥管理系统
金融应用	主安全域	银行卡密钥管理系统
居民健康卡应用	辅助安全域	居民健康卡密钥管理系统
预留应用	辅助安全域	行业应用机构

8.2 宁夏公共服务卡（居民健康卡）安全域管理

宁夏公共服务卡（居民健康卡）卡片内部的安全域有两种类型，即：

1. 发卡方安全域（ISD）：即主安全域。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。

2. 辅助安全域（SSD）：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。

安装到卡片上的每类行业应用都有相应的安全域来管理。为了实现金融 IC 卡持卡人可在发卡银行柜面或自助服务终端上动态加载本行或其他银行拓展的多个行业应用，需要为这些动态加载的行业应用统一建立辅助安全域。

辅助安全域实现的功能有密钥管理、加密解密、针对其提供者的应用进行数字签名的生成与验证，以管理它下面的应用实例。辅助安全域的创建采用预制和动态创建两种方式。

白卡与预置卡均要求预制两个铺助安全域：宁夏卫生计生委辅助安全域、预留辅助安全域。同时，要求卡片在发卡后，支持发卡行动态创建通用辅助安全域。

行业应用由宁夏金融 IC 卡多应用银行间共享平台统一发布、统一管理。卡片的管理由发卡方负

责。行业应用的 CAP 包装载的 DAP 验证密钥由人民银行管理，这样人民银行可以对加载到金融 IC 卡多应用银行间共享平台上的 CAP 包进行 DAP 签名处理，有利于共享行业应用的统一发布和管理（包括应用的申请、审批、上传、上线发布、下线等）。

卡片数据空间要求大于等于 80K 字节。卡片结构如图 6 所示：

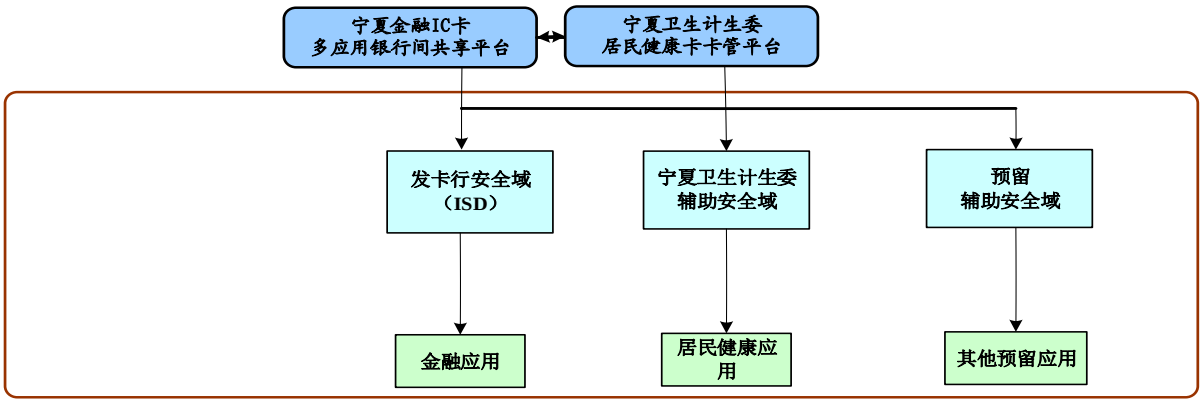


图 6　宁夏公共服务卡（居民健康卡）卡片结构图

8.3　主安全域

宁夏公共服务卡（居民健康卡）主安全域代表发卡方，预制在 IC 卡中，具有唯一性和强制性。主安全域不可被删除和创建。主安全域可以创建和删除辅助安全域。发卡方的应用，即金融应用，安装在主安全域下。

主安全域 AID 由发卡行自定义。

主安全域密钥至少支持 SCP 02 i=15 密钥体系。

8.4　辅助安全域

宁夏公共服务卡（居民健康卡）全区通用版辅助安全域包括宁夏卫生计生委辅助安全域和预留辅助安全域两个辅助安全域，宁夏全区如有城市需要发行加载其他行业应用（如市民一卡通应用）的宁夏公共服务卡（居民健康卡），可通过创建并预留专有的行业应用安全域或在“预留安全域”下创建新的行业应用安全域来实现。

若采用预留专有的行业应用辅助安全域，则整个卡片辅助安全域包括宁夏卫生计生委辅助安全域、该行业应用安全域、预留辅助安全域，此种情况下该预留专有辅助安全域采用预置方式，具有 DAP Verification 权限，禁止应用的迁入和迁出操作，且不支持在该辅助安全域下创建新的辅助安全域。该辅助安全域仅用于安装该行业应用，应用采用后下载方式安装在 IC 卡中。该辅助安全域密钥至少支持 SCP 02 i=15 密钥体系，密钥由行业应用卡管平台生成和管理，支持安全域密钥的增加、更新和

删除操作。该辅助安全域 AID 由需要加载其他行业应用的城市根据相关规则选定，但在正式启用之前必须向中国人民银行银川中心支行申请报备。

8.4.1 宁夏卫生计生委辅助安全域

宁夏公共服务卡（居民健康卡）中的宁夏卫生计生委辅助安全域采用预制方式，具有 DAP Verification 权限，禁止应用的迁入和迁出操作。不支持在该辅助安全域下创建新的辅助安全域。

该安全域 AID 定义为 D156000001 00200000000000100000000，只安装卫生计生委居民健康应用，并且应用预置在卡内。

安全域密钥至少支持 SCP 02 i=15 密钥体系，密钥由卫生计生委卡管平台生成和管理，支持安全域密钥的增加、更新和删除操作。

8.4.2 预留辅助安全域

预留辅助安全域由卡商创建完成，该安全域的 AID 为 D156000001 00200000000000300000000。预留辅助安全域用于安装其他行业相关应用，应用采用后下载方式安装在 IC 卡中。预留辅助安全域由宁夏金融 IC 卡多应用银行间共享平台（TSM 平台）管理，且此安全域必须要有授权（AM）权限以实现 TSM 对卡片的管理。（注：如果安全域是 DM 权限，TSM 每次在安装辅助安全域或应用、删除安全域或应用时必须经过发卡方的授权，这种情况下，各参与银行需要建设相应的卡片授权系统与 TSM 平台进行对接，且对现行 TSM 技术实施方案影响较大，不利于实施。）

TSM 平台对该辅助安全域具有完全的管理权限，即，可在预留辅助安全域下载创建新的辅助安全域、删除辅助安全域以及锁定辅助安全域，并能安装、删除、锁定解锁应用等。TSM 平台可替换辅助安全域密钥。

TSM 平台在该预留辅助安全域下创建的辅助安全域 AID 由 TSM 平台自行管理。

9. 文件和数据规划

宁夏公共服务卡（居民健康卡）卡片文件包括宁夏卫生计生委居民健康应用和预留行业应用文件结构，宁夏区内如有城市需要发行加载其他行业应用（如市民一卡通应用）的宁夏公共服务卡（居民健康卡），可采用单独创建预留该行业应用辅助安全域并加载应用文件或在预留辅助安全域下创建新的子辅助安全域并安装应用。

如采用单独预留该行业应用辅助安全域方式，需要定义该行业应用文件及数据结构，并在卡片从卡商出厂时，建立该行业应用的应用结构。对于白卡，需卡商同时写入正式密钥，并根据相应卡面设

计印刷相应个性化信息；对于预制卡，需要卡商获取该行业密钥的正式密钥及数据，并将密钥及数据写入相应的文件结构内。此种情况下，若白卡，则在出厂后，可通过宁夏金融 IC 卡多应用银行间共享平台（简称“共享平台”）进行该行业应用信息写入（前提是该行业应用提供方已将该应用上传至共享平台），写入流程如下：

1. 共享平台选择该行业应用，做安全认证；
2. 共享平台发送个人化写入指令，写入个人化数据。

9.1 宁夏卫生计生委居民健康应用

白卡：卡商在出厂时，需建立健康卡应用结构，按照宁夏卫生计生委要求写入初始密钥全 FF 或是正式密钥。卡面只印刷相关银行信息字段，包括卡片银行卡号、有效期等，卫生信息不做印刷。

预置卡：卡商在出厂时，需建立健康卡应用结构，同时从宁夏卫生计生委密管系统获取正式密钥，从卡管机构获取个人正式数据，将密钥及数据均写入相应的文件结构内。

对于白卡出厂后，可通过宁夏金融 IC 卡多应用银行间共享平台（简称“共享平台”）进行宁夏公共服务卡（居民健康卡）中健康信息写入，流程如下：

1. 共享平台选择健康卡应用，做安全认证。
2. 共享平台发送个人化指令写入个人化数据。

9.1.1 文件结构

卫计委居民健康应用的文件结构应符合 GB/T 16649.4 及本部分中相关的规定。

文件结构示意图如图 7 所示。其中，DDF1 是居民健康卡应用环境，DDF2 是其他预留应用环境。居民健康卡应用的各个具体应用项对应的专用文件（DF），与相关的基本数据文件（EF）分别构成一个树状结构的各个分支。每个专用文件（DF）是其下面基本数据文件（EF）的入口点。

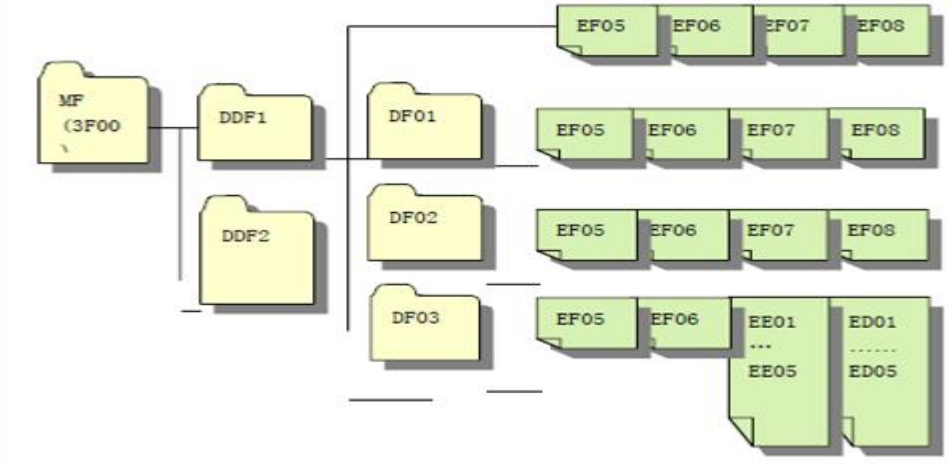


图 7　居民健康应用文件结构图

居民健康应用系统环境是居民健康应用的入口，进入居民健康卡应用系统环境后的应用应符合居民健康卡相关规范要求。具体规范可详见《居民健康卡应用规范 V1.1》。

9.2 预留行业应用

预留行业应用为了后期做其他行业应用做预留使用。

应用的安装包采用后下载方式存储在卡中。

对于其他行业应用，无论白卡和预置卡均采用宁夏金融 IC 卡多应用银行间共享平台（简称“共享平台”）进行后下载方式，可参考具体流程如下：

1. 共享平台管理预留辅助安全域。
2. 共享平台在预留辅助安全域在每个行业应用创建专有的辅助安全域。
3. 共享平台做卡片的安全认证。
4. 共享平台向应用专用的辅助安全域下载应用安装包。
5. 共享平台向卡片发送应用安装指令完成应用安装。

后下载应用的个人化过程：

1. 共享平台选择行业应用，做安全认证。
2. 共享平台发送个人化指令建立文件结构。
3. 共享平台发送密钥写入指令，写入应用正式密钥及个人化数据。

10. 证书应用

数字证书包括加密证书和签名证书两张证书，用于为持卡人提供身份验证功能和数字签名功能，该两张证书应当安全存储在 IC 卡证书应用区内。

数字证书采用 X.509v3 格式，采用 SM2、SM3 等国产算法，并由具有资质的可信第三方 CA 认证机构进行签发并提供数字证书生命周期的管理。

证书应用的逻辑如图 8 所示。

图 8 中容器中存放加密密钥对、签名密钥对和会话密钥。其中加密密钥对用于保护会话密钥，签名密钥对用于数字签名和验证，会话密钥用于数据加解密和 MAC 运算。其中，签名密钥对由内部产生，加密密钥对由外部产生并安全导入，会话密钥可由内部产生或者由外部产生并安全导入。

证书应用中，卡片需配合 SM2 算法密码应用接口规范，实现设备管理、应用管理、文件管理、容器管理、访问控制、密码服务等各项应用功能。

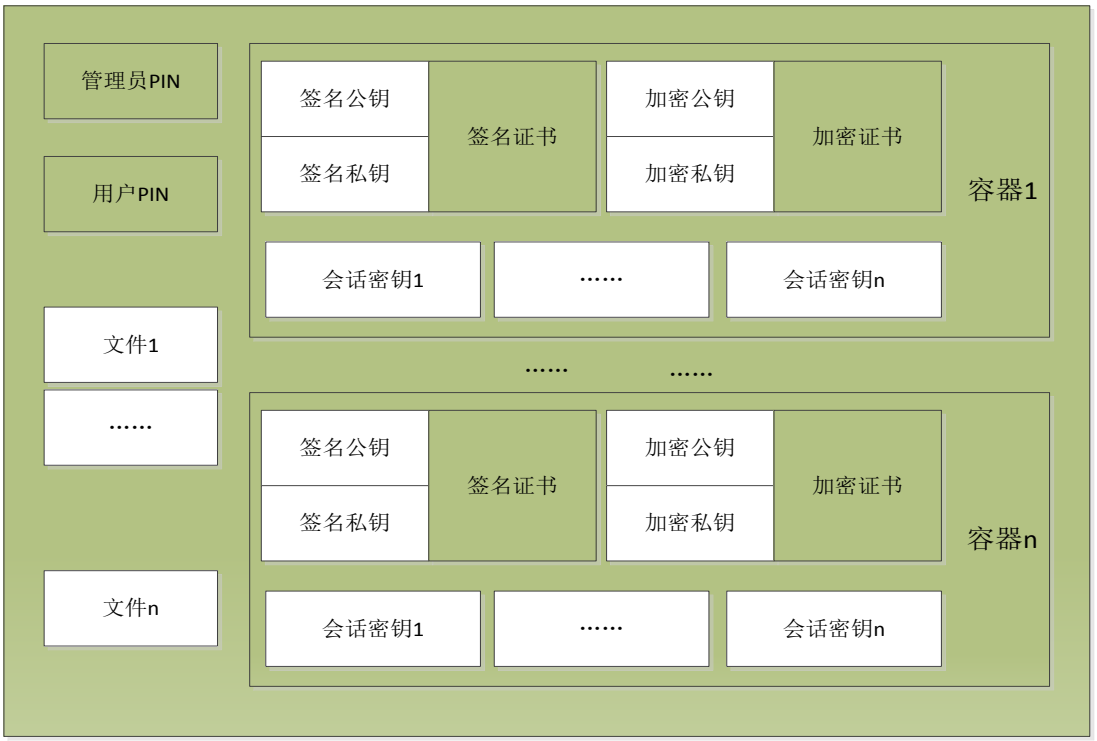


图 8　证书应用逻辑结构图

11. 宁夏公共服务卡(居民健康卡)可视 IC 产品说明书

11.1 引 言

本部分产品说明书主要描述了宁夏公共服务卡（居民健康卡）可视 IC 卡全区通用版本的运行和使用流程。该产品集成了银行卡功能、居民健康卡的应用功能。卡片支持多种工作方式，分别为银行电子现金余额、健康国密 SM3 算法的动态口令、健康信息（包含出生日期、紧急联系人电话、血型、卡号等持卡人信息）、银行电子现金交易记录查询。同时作为金融 IC 卡使用时，本产品支持双界面通信模式，既支持接触式（ISO7816）通信方式，又支持非接触式（ISO14443）通信方式，可以与目前市场上标准的金融读卡器具无缝对接。

该卡支持以下几种工作方式：

1. 支持电子现金账户的余额查询；
2. 支持电子现金账户的交易记录查询；
3. 支持居民健康卡相关信息查询；
4. 支持基于时间型模式的动态口令。

11.2 卡面效果

宁夏公共服务卡（居民健康卡）全区通用版可视 IC 产品卡面效果如图 9-a, 图 9-b 所示（以中信银行为例）：

图 9-a 卡片效果图（正面）

图 9-b 卡片效果图（反面）

在宁夏公共服务卡（居民健康卡）全区通用版可视 IC 卡产品中，除 6.1 节规定的可变和不可变部分外，需要遵循：

1. 银行卡卡号位置如图 9-a 所示；

2.卡片正面 6、7、8、9 号按键在全区通用版为自定义，各市可根据本地实际需要在发卡时自行定义按键功能。

11.3 卡片遵循标准

宁夏公共服务卡（居民健康卡）全区通用版可视 IC 产品须符合以下标准：

ISO/IEC 14443-1 识别卡 无触点集成电路卡 近程卡 第 1 部分：物理特性，2000-04-15

ISO/IEC 14443-2 第 2 部分：射频功率和信号接口， 2001-07-01

ISO/IEC 14443-3 第 3 部分：初始化和防冲突，2001-02-01

ISO/IEC 14443-4 第 4 部分：传输协议，2002-02-01

JR/T 0025.3 -2013 《中国金融集成电路（IC）卡规范》

《金融 IC 卡通用应用数据存储规范》

《居民健康卡技术规范》

GP2.1.1 规范

Java2.2.1 规范

11.4 产品信息

宁夏公共服务卡（居民健康卡）全区通用版可视 IC 产品卡片产品信息如表 34 所示：

表 34 卡片产品信息

产品规格	相关标准
产品尺寸	85.6±0.12×53.98±0.05×0.76±0.08mm
SE 型号	卡商提供
键盘形式	12 键锅仔按键
动态口令密钥下载方式	支持 RF 下载方式
动态口令时钟校准方式	支持 RF 校准方式
卡片静置自动关闭时间	60s 无操作自动关机
自检顺序	1) 所有数字全显 2) 固件版本号 3) 编程日期 4) 复位次数 5) 序列号高 8 位 6) 序列号低 8 位
使用寿命	5 年
卡面	哑光
卡号印刷方式	激光
有效期印刷方式	激光

11.5 按键定义

宁夏公共服务卡（居民健康卡）全区通用版 IC 可视卡共有 12 个锅仔按键，分别为控制键“确认”，“删除”以及数字键“0”-“9”。

1. “确认”键，功能见表 35。

表 35 “确认”键功能表

状态	功能
关机状态	开机
关机状态长按 3 秒	版本查询
功能选择状态	关机
余额显示状态	关机
锁定码显示状态	关机
交易记录显示状态	关机
健康信息查询显示状态	关机
输入激活码/设置 PIN 码状态	确认

2. “返回”键，功能见表 36。

表 36 “返回”键功能表

状态	功能
时间型动态口令显示状态	返回功能选择状态
显示余额、显示交易记录状态	返回功能选择状态
健康信息显示状态	返回功能选择状态
锁定码状态	无响应
输入激活码/设置 PIN 码状态	删除前一个数字，当无任何输入时，则返回功能选择状态

3. “0”-“9”键，这 10 个键可作为数字键输入，部分同时又可作为功能选择键，详情见表 37。

表 37 数字键复用功能表

数字键	复用功能
0	修改开机 PIN 码设置
5	上翻按键，用于信息查询时的“上翻”功能，可滚动翻屏
1	银行电子现金余额查询
2	健康卡时间型动态口令认证
3	持卡人健康信息查询
4	银行电子现金交易记录查询
6-9	自定义

11.6 可视 IC 产品使用说明

11.6.1 可视 IC 产品运行逻辑图

宁夏公共服务卡（居民健康卡）全区通用版可视 IC 卡产品运行逻辑图如图 10 所示：

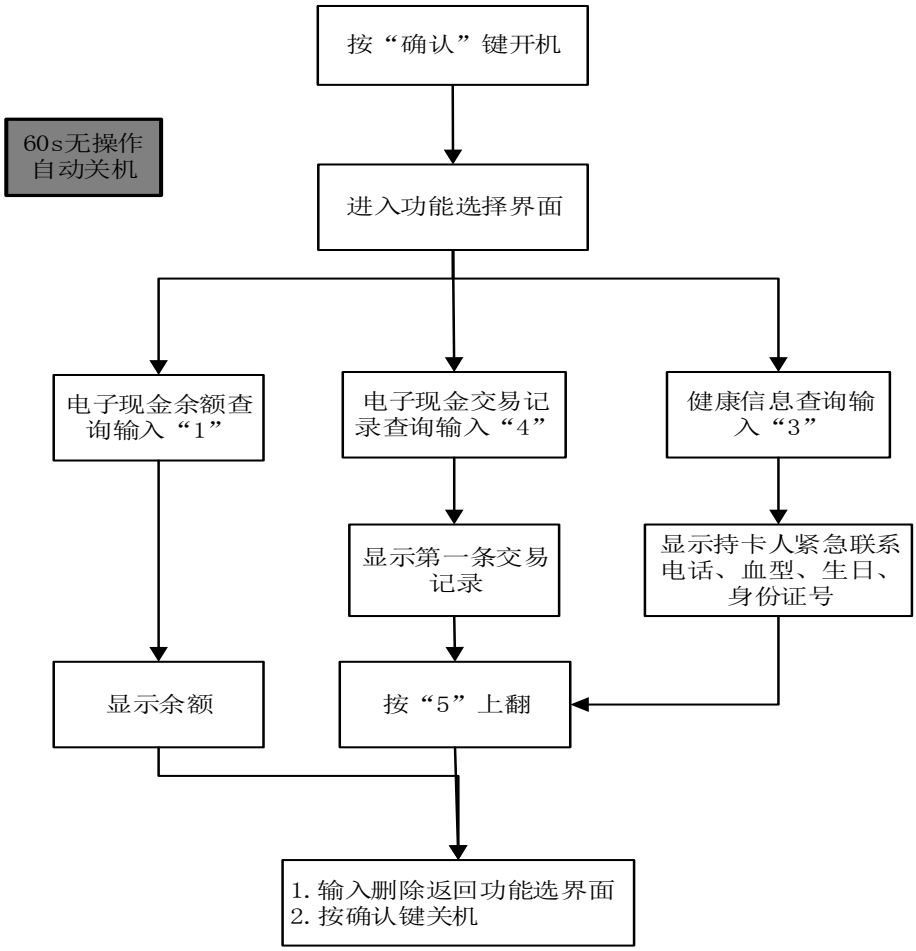


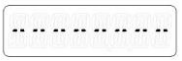
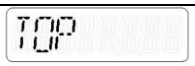
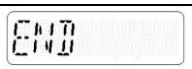
图 10 产品运行逻辑图

11.6.2 功能显示说明

宁夏公共服务卡（居民健康卡）全区通用版可视 IC 卡产品功能显示说明如表 38 所示：

表 38 功能显示说明

电子现金余额查询界面	
	在“SELECT--”界面下，按数字键“1”，进入电子现金余额查询模式
	显示“E-CASH”, 进入显示电子现金余额模式，屏幕提示保持 0.5 秒
	屏幕显示当前卡内电子现金余额（小数点后支持 2 位）

电子现金交易记录查询界面	
	在“SELECT--”界面下，按数字键“4”，进入交易记录查询模式。
	进入查询交易明细模式，屏幕提示将保持 0.5 秒
	屏幕显示交易明细记录中的交易金额信息
	按“0”键，屏幕显示交易明细记录中的交易日期
	按“0”键，屏幕显示交易明细记录中的交易时间
	时间信息缺省状态下，显示“—”
	按“0”键，可下翻下一条记录，按“5”键，可上翻上一条记录。 若无交易明细记录或者无有效的记录，则屏幕显示“EMPTY”
	向上翻页到顶，显示“TOP”。
	向下翻页到底，显示“END”。
健康信息查询界面	
	在“SELECT--”界面下，按数字键“3”，进入健康信息查询模式。
	进入健康信息查询模式，屏幕提示将保持 0.5 秒。
	“ICE”代表紧急联系人，“In Case of Emergency”的缩写。可以按上翻键来切换显示功能。
	按“确认”键显示联系方式。
	屏幕显示 8 位数字，当多于 8 位会自动滚屏显示。
	“BLOOD”代表血型。可以按上翻键来切换显示功能。
	按“确认”键显示持卡人的血型。
	“BIRTHDAY”代表出生日期。可以按上翻键来切换显示功能。
	“ID CARD”代表身份证号。可以按上翻键来切换显示功能。
	按“确认”键显示身份证号。
	自动滚动来显示完整身份证号码。
	身份证号码最后两位（3X）。

11.7 可视 IC 卡中健康信息加解密方式

11.7.1 目的

目前健康卡信息规范要求卫生部信息只能用于非接方式读取，没有打开 ISO7816 接口。而可视 IC 卡要读到 SE 芯片内容，必须使用 ISO7816 接口方式，为解决安全和可用问题，制定以下算法。

11.7.2 算法说明

1）符号定义

K：密钥，32 字节。

K1-Kn：扩展后的密钥。

T：明文。

T1-Tn：扩展后的明文。

TL： 明文长度。

C：密文。

C1-Cn： 分组后的密文。

CL： 密文长度。

R：随机数，8 字节。

2） 用 SM3 算法加密

1. 对明文进行扩展分组，每 32 字节为一组，不足 32 字节补 0x00，即将 T 扩展为 T1，T2，T3…Tn。

2. 加密端生成 8 字节随机数 R。

3. 对密钥进行扩展分组，扩展至与明文一样的长度，即将 K 扩展为 K1，K2，K3…Kn，扩展算法为 K1=SM3（K，R），K2=SM3（K1，R），K3=SM3（K2，R）…，Kn=SM3（Kn-1，R）。

4. 将扩展后的密钥 K1，K2，K3…Kn 与扩展后的明文 T1，T2，T3…Tn 进行异或运算得到密文 C，即 C=（K1｜K2｜K3…Kn）XOR （T1｜T2｜T3…｜Tn）。

5. 传输过程，加密端将随机数 R+C 进行传输。

3）用 SM3 算法解密

1. 解密端接收 R+C。

2. 对密钥进行扩展分组，扩展至与密文一样的长度，即将 K 扩展为 K1，K2，K3…Kn，扩展算法为 K1=SM3（K，R），K2=SM3（K1，R），K3=SM3（K2，R）…，Kn=SM3（Kn-1，R）。

3. 将密文 C 每 32 字节进行分组得到 C1，C2，C3…Cn。

4. 将扩展后的密钥 K1，K2，K3…Kn 与分组后的密文 C1，C2，C3…Cn 进行异或运算得到明文 T，即 T=（K1｜K2｜K3…Kn）XOR（C1｜C2｜C3…｜Cn）。

4）加密端解密端 K 的初始化

1. 本文档的加密端指安全芯片 SE，解密端指微处理器 MCU。
2. SE 与 MCU 通过 7816 接口进行数据传输。
3. MCU 用 SM3 算法对 MCU 计数器的随机值进行离散生成密钥 K。
4. MCU 调用 APDU 指令将 K 写入 SE。
5. 对 SE 写 KEY 的接口只允许调用一次。
6. 写 K 的过程在出厂前完成。
7. 对于未对 SE 写密钥 K 的产品会提示错误代码，保证出厂前产品均初始化了密钥 K，以及方便出厂后产品的抽检是否已初始密钥 K。
8. K 由 MCU 内部计数器通过离散算法生成，初始化 K 后，只有 SE 及 MCU 知道 K，第三方无法获取到 K。

5）加密例子

密钥 K（32 字节）：30313233343536373839303132333435363738393031323334353637383930313233343536373839303132。

明文 T（43 字节）：

303132333435363738393031323334353637383930313233343536373839303132333435363738393031323334353637383930313233343536373839303132。

1. 将 43 字节明文补 0x00 进行扩展得到 64 字节明文 T1T2：

303132333435363738393031323334353637383930313233343536373839
303132333435363738393031323334353637383930313233343536373839
303132000000000000000000000000000000000000000000000000000000

2. SE 生成 8 字节随机数 R=3132333435363738。
3. SE 运算 K1=SM3（K丨R），

即：K1=42d0b6cb4dd0a66196b01db315a726859e241ce245cda2958254c7127d047f2d。

K2=SM3（K1丨R），

即：K2=4cbc3a1fafb621988b201ad22b627eba5983c96be1e91c07426785d09a7d14e2。

K1K2=K1丨K2，

即：

K1K2=42d0b6cb4dd0a66196b01db315a726859e241ce245cda2958254c7127d047f2d4cbc3a1fafb621988b201ad22b627eba5983c96be1e91c07426785d09a7d14e2

4. SE 用密钥 K1K2 与明文 T 进行异或得到密文 C，即 C=K1K2 XOR T1T2。
5. SE 将随机数 R+密文 C 返回给 MCU。

11.8 动态口令认证

11.8.1 功能说明

卡片包含激活码、开机密码、健康国密 SM3 算法的动态口令,分别用于卡片密钥更新、卡片本身保护、完成用户的身份认证，实现线上支付等功能。

11.8.2 功能信息

卡片动态口令认证功能信息如表 39 所示：

表 39 功能信息表

动态口令功能	相关标准
动态口令工作模式	时间型模式
动态口令安全算法类型	SM3
动态口令同步方式	时间同步
显示动态口令密码位数	6 位
动态口令密码有效时间	60s
激活码	12 位十进制数字
种子文件格式	XML 形式
时钟补偿算法	符合国密算法的时钟补偿机制
种子下载协议	符合国密算法的种子下载协议
动态口令激活	支持

11.8.3 功能流程

宁夏公共服务卡（居民健康卡）全区通用版可视 IC 产品功能流程如图 11 所示：

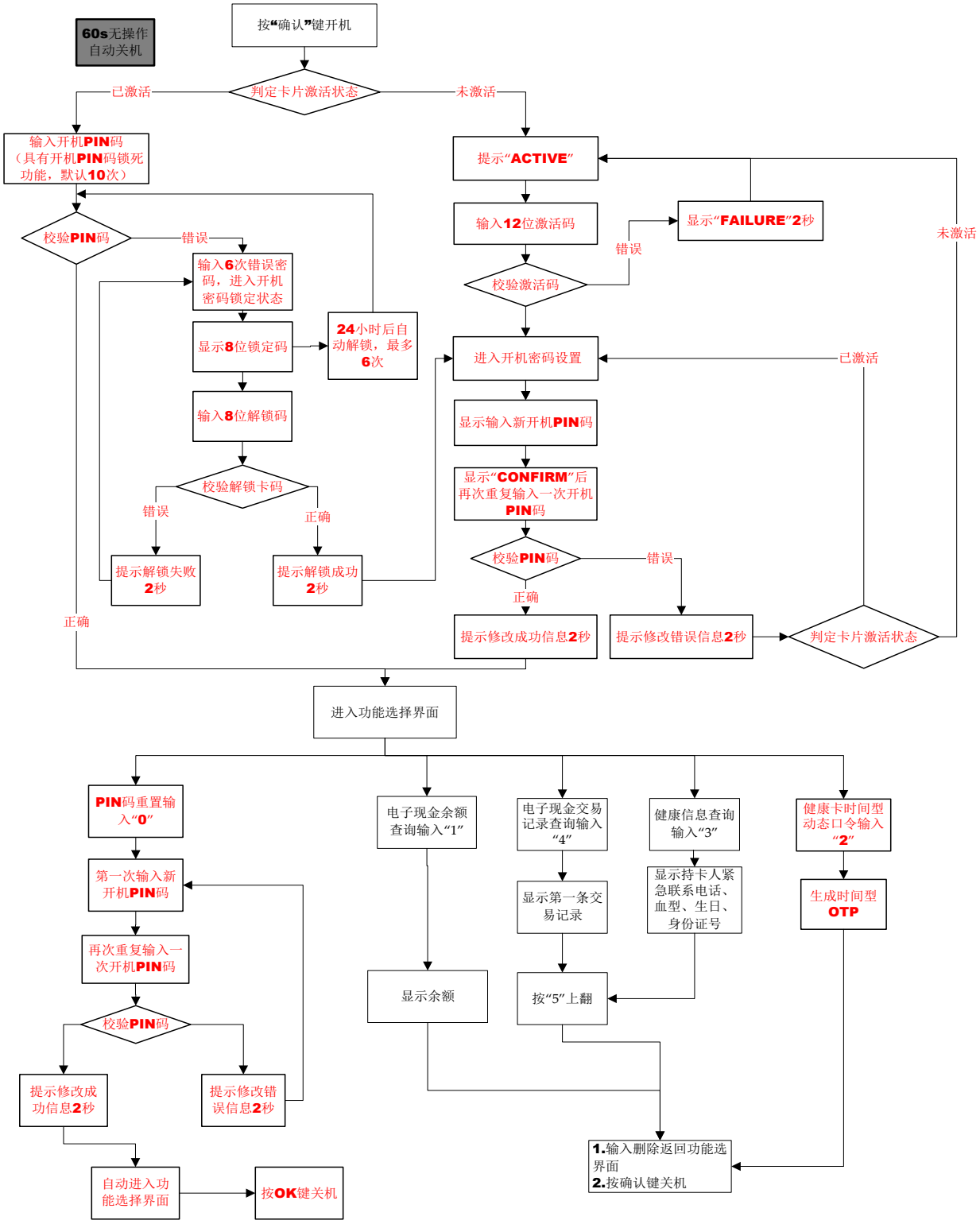


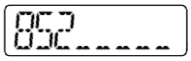
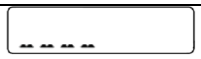
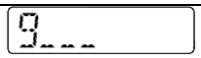
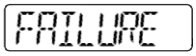
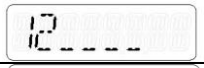
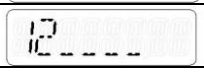
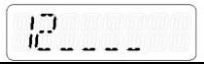
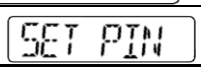
图 11 功能流程图

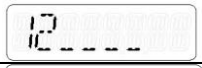
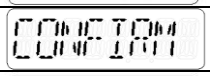
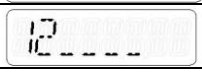
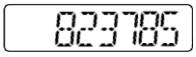
注：图 11 中红色部分、加粗方框部分为增加动态口令认证功能。

11.8.4 功能显示说明

宁夏公共服务卡（居民健康卡）可视 IC 卡显示功能说明如表 40 所示：

表 40 功能显示说明

开机激活界面	
显示状态	说明
	按“确认”键开机，屏幕显示“ ACTIVE ”字样，定义为健康卡系统激活。
	采用 0 至 9 数字键盘输入激活码，屏幕会显示 8 个下划线，并在已输入的位置显示实际输入的数字。
	当输入满 8 位数字时，屏幕显示 0.5 秒，自动进入后 4 位数字输入等待界面。
	再继续输入后 4 位数字，输入过程中每按一次“返回”键将删除最后一位数字。
	如果激活码输入正确，则屏幕提示成功字样，2 秒后进入设置开机密码界面。
	如果激活码输入错误，则屏幕提示失败字样，2 秒后回到激活”ACTIVE 1”界面。
设置开机密码界面	
	激活码验证成功后，必须设置开机密码。 屏幕提示用户输入 6 位数字的新开机密码。
	输入新开机密码.
	输入 6 位数字完成后，按“确认”键提交，屏幕提示用户再次重复输入一次。
	再次重复输入新开机密码后按<确认>键确认
	两次输入的开机密码一致，屏幕提示成功字样，持续显示约 2 秒，自动进入功能选择状态。
	两次输入的开机密码不一致，屏幕显示失败字样。
重置密码界面	
	按“确认”键开机，屏幕提示输入当前开机密码。
	采用 0-9 数字键盘输入当前开机密码，按确认键确认完成输入。
	若开机密码验证未通过，则屏幕提示失败，显示持续 2 秒后提示重新输入“PIN”。
	若开机密码验证通过，屏幕显示“SELECT--”界面，按数字键“0”（持续显示 0.5 秒）。
	进入重置密码功能，等待按数字键。

	屏幕提示用户输入 6 位数字的新开机密码。
	输入新开机密码
	输入 6 位数字完成后，按“确认”键提交，屏幕提示用户再次重复输入一次。
	再次重复输入新开机密码后按“确认”键确认
	两次输入的开机密码一致，屏幕提示成功字样。
	两次输入的开机密码不一致，屏幕显示失败字样。
健康时间型动态口令界面	
	在“SELECT--”界面下，按数字键“2”。
	进入时间型动态口令模式，屏幕提示保持 0.5 秒。
	得到 6 位时间型动态口令，按“C”键，返回功能选择界面，若持续 60 秒无任何操作，则自动关机。