ICS 11.120
C 07

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS XXXXX.1—XXXX

居民健康卡技术规范
第 1 部分：用户卡技术规范

Residents’ health card technical specifications——

Part 1：Technical specification of the user card

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国国家卫生和计划生育委员会
发 布

前　言

WS XXXXX 《居民健康卡技术规范》现分为以下部分：

——第1部分：用户卡技术规范

——第2部分：用户卡应用规范

——第3部分：用户卡命令集

——第4部分：终端技术规范

——第5部分：用户卡及终端产品检测规范

……

本部分为 WS XXXXX 的第1部分。

本部分由国家卫生和计划生育委员会卫生信息标准专业委员会提出。

本部分主要起草单位：

本部分主要起草人：

居民健康卡技术规范

第 1 部分：用户卡技术规范

1 范围

本部分规定了全国统一的居民健康卡用户卡的主要技术要求，其中包括：卡号编码规则、卡介质、卡面、终端接口要求、卡数据标准、数据安全及应用。

本部分适用于所有制作、发行、使用居民健康卡的卫生行政管理部门、医疗卫生机构、第三方联合发卡机构、持卡人和生产企业。

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	公民身份号码
GB/T 14504	银行卡
GB/T 16649.4	识别卡　带触点的集成电路卡　第4部分
GB/T 16649.5	识别卡　带触点的集成电路卡　第5部分
GB/T 18347	128 条码
WS 363（所有部分）	卫生信息数据元目录
WS 364（所有部分）	卫生信息数据元值域代码
WS 365（所有部分）	城乡居民健康档案基本数据集
JR/T 00520	银行卡卡片规范
ISO/IEC 14443	识别卡　非接触式集成电路卡　接近式卡

3 术语和缩略语

3.1 术语

3.1.1

居民健康卡 residents’ health card

是中华人民共和国居民拥有的，在医疗卫生服务活动中用于身份识别，满足健康信息存储，实现跨地区和跨机构就医、数据交换和费用结算的基础载体，是计算机可识别的CPU卡。

3.1.2

CPU 卡 central processing unit card

带有中央处理器、存储单元以及卡片操作系统的集成电路卡。

3.1.3

芯片 chip

本部分中特指居民健康卡中用于完成数据处理和存储功能的集成电路器件。

3.1.4

卡片操作系统 COS，card 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

3.1.5

加密算法 cryptographic algorithm

为了隐藏或显现数据信息内容的变换算法。

3.1.6

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。

3.1.7

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。

3.1.8

密钥 key

加密转换中控制操作的符号序列。

3.1.9

对称密钥 symmetric key

在对称加密算法中使用的密钥。

3.1.10

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。

3.1.11

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。

3.1.12

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。

3.1.13

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。

3.1.14

生物标识 biomarker

人的某种特异性的生物学特征，具有遗传性和终身携带性，如血型。

3.1.15

医学警示 medical alert

患者在就医、急诊或抢救时需要特别提醒医生注意的信息，包括疾病史、体内装置、药物过敏史、对某些物质的不耐受史等。

3.2 缩略语

以下缩略语和符号表示适用于本部分。

缩略语和符号见表3-1。

表 3-1 缩略语和符号列表

缩略语	中文名	英文名
‘0’-‘9’ ‘A’-‘F’	十六进制数字	
AID	应用标识符	Application Identifier
an	字母数字型	Alphanumeric
ans	特殊字母数字型	Alphanumeric Special
b	二进制	Binary
CBC	密码块链接	Cipher Block Chaining
CLA	命令报文的类别字节	Class Byte of Command Message
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
CVN	卡安全码	Card Verification Number

DDF	目录定义文件	Directory Definition File
DF	专用文件	Dedicated File
EF	基本文件	Elementary File
FCI	文件控制信息	File Control Information
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
M	必选型	Mandatory
MAC	报文鉴别代码	Message Authentication Code
MF	主控文件	Master File
O	可选型	Optional
PIX	专用应用标识符扩展码	Proprietary Application Identifier Extension
SAM	安全存取模块	Secure Access Module
PVC	聚氯乙烯	Polyvinyl Chloride
RID	已注册的应用提供者标识	Registered Application Provider Identifier
RS232	串行通信接口	
USB	通用串行总线	Universal Serial BUS
xx	任意值	

4 卡号编码规则

居民健康卡的卡号采用公民身份号码（GB 11643—1999）。

5 卡介质

5.1 卡介质选择

居民健康卡为高安全型CPU卡，采用非接触式通信模式，符合ISO/IEC 14443通讯协议，可写数据存储器容量不少于32K字节，为加密非挥发存储器。

5.2 卡体材料

卡体材料使用普通PVC。

5.3 制卡要求

居民健康卡制造机构必须符合以下条件：

1) 居民健康卡芯片以及卡片制造机构应具有国家IC卡注册中心分配的注册标识号和注册证书。

2) 居民健康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。

3) 居民健康卡制造机构必须取得国家集成电路中心的ICCR注册证书和国家IC卡生产许可证。

4) 居民健康卡卡片操作系统（COS）要通过中国国家信息安全认证中心的EAL4+强制性安全认证。

5) 居民健康卡须经国家卫生和计划生育委员会指定的相关检测机构进行符合性检测，取得COS检测合格证书。

6) 居民健康卡增加金融应用的应符合中国人民银行相关要求。

6 卡面

6.1 卡片外形规格

居民健康卡卡片外形为圆角矩形，外形和尺寸分别见表6-1和图6-1。

表 6-1 卡片尺寸

参数	尺寸	公差
卡片宽度 L	85.60mm	85.47 mm -85.72 mm
卡片高度 W	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

注：倒角是在圆柱型工件的末端加工出一个具有角度的边。

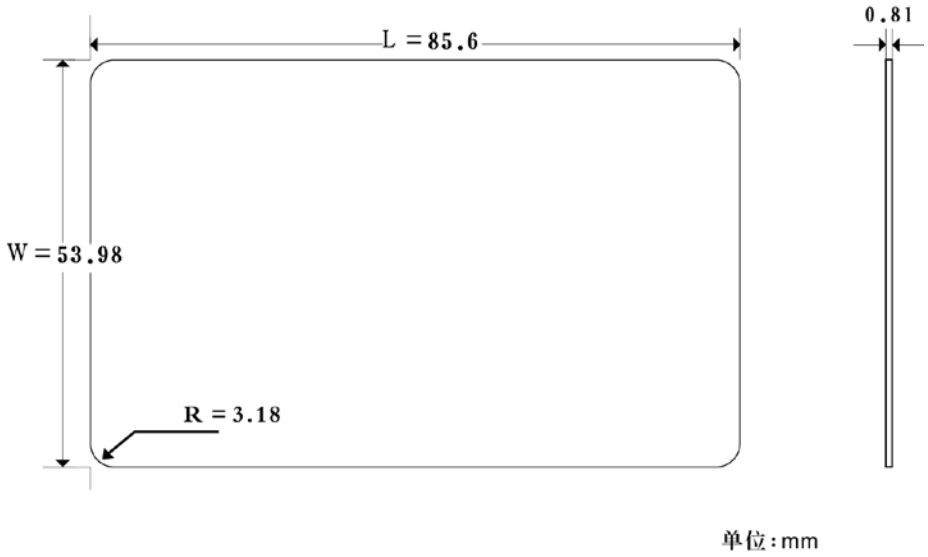


图 6-1 卡片尺寸

6.2 芯片位置

居民健康卡芯片放置位置不能影响卡片使用。

6.3 印刷要求

6.3.1 卡片背面样式

卡片背面应包括以下要素：持卡人照片、持卡人姓名、性别、民族、居民健康卡号码码、居民健康卡号条形码、发卡机构名称、发卡机构公章。

卡片背面参考布局及参数见6-2和表6-2。

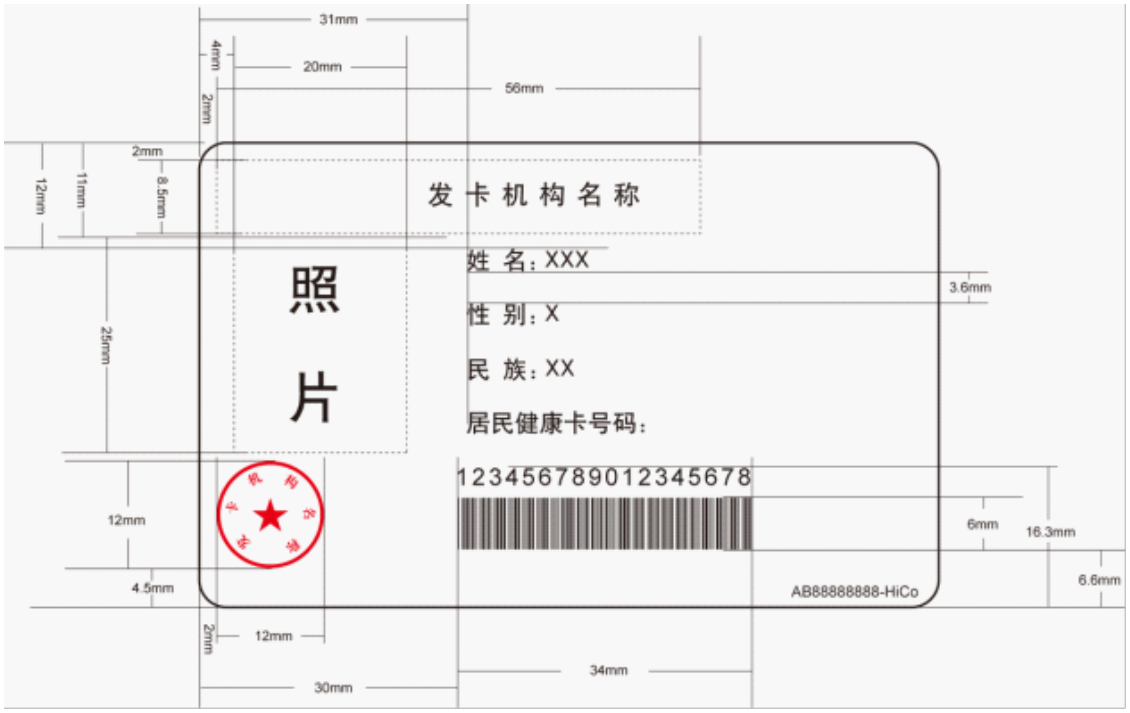


图 6-2 卡片背面布局

表 6-2 卡片背面布局参数

参数	规格及要求	公差
发卡机构标识区		
发卡机构公章直径	12.00mm	±0.30mm
发卡机构公章左边沿到卡的左边沿的距离	2.00mm	±0.30mm
发卡机构公章下边沿到卡的下边沿的距离	4.50mm	±0.30mm
发卡机构公章红色色值	C0、M100、Y100、K0	/
发卡机构公章边线	1.2pt	±0.30mm
发卡机构公章内五角星	4 mm x4mm	±0.30mm
发卡机构公章内文字	汉仪中宋 4.5PT	/
发卡机构公章内文字起始边界	五角星下方两个角的顶点延长线	/
“省级卫生厅局名称”字体	汉仪大黑简 8.6PT，加粗	/
“省级卫生厅局名称”区域左边沿到卡的左边沿的距离	31.00mm	±0.30mm
“省级卫生厅局名称”区域右边沿到卡的左边沿的距离	65.00mm	±0.30mm
“省级卫生厅局名称”区域上边沿到卡的上边沿的距离	2.00mm	±0.30mm
“省级卫生厅局名称”区域高度	8.50mm	±0.30mm
“省级卫生厅局名称”水平方向	水平方向上均匀充满区域	/
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
持卡人个人信息		
“姓名” 、“性别”、“民族”、“居民健康卡号码”字体	汉仪中黑 8.0PT	/
“姓名”、 “性别”、“民族”、 “居民健康卡号码”左边沿到卡的左边沿的距离	31.00mm	±0.30mm
“姓名”上边沿到卡的上边沿的距离	12.00mm	±0.30mm
“姓名”、“性别”、“民族”、 “居民健康卡号码” 的行间距	3.00mm	±0.30mm
可变信息部分		
“姓名、性别、民族、居民健康卡号码”填写值字体	汉仪中黑 8.0PT	/
“民族”填写值	不带”族”字，例如 ”汉”	/

“居民健康卡号码”填写值上边沿距卡片下边沿距离	20mm	±0.30mm
“姓名、性别、民族、居民健康卡号码”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	31.00mm	±0.30mm
条形码下边沿到卡的下边沿的距离	10.55mm	±0.30mm
联名卡名称区（该区内容根据需要可有可无）		
“联名卡名称”字体	汉仪中黑 6pt	/
“联名卡名称”字间距	0	/
“联名卡名称”下边沿距卡的下边沿的距离	4mm	±0.30mm
“联名卡名称”水平方向	与条型码等长的区域内居中	±0.30mm
银行标识、名称区（该区内容根据需要可有可无）		
“银行标识、名称”文字	在视觉上文字要小于“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	0.4mm	±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) 居民健康卡使用照片基本要求：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。

2) 居民健康卡的条形码是对居民健康卡卡号即公民身份号码进行编码的128条码，格式应按GB/T 18347—2001规定。

6.3.2 预留金融功能区的卡片背面样式

卡片背面应包括以下要素：持卡人照片、持卡人姓名、性别、民族、居民健康卡号码、居民健康卡号条形码、发卡机构名称、发卡机构公章。卡片背面布局及参数见图6-3和表6-3。

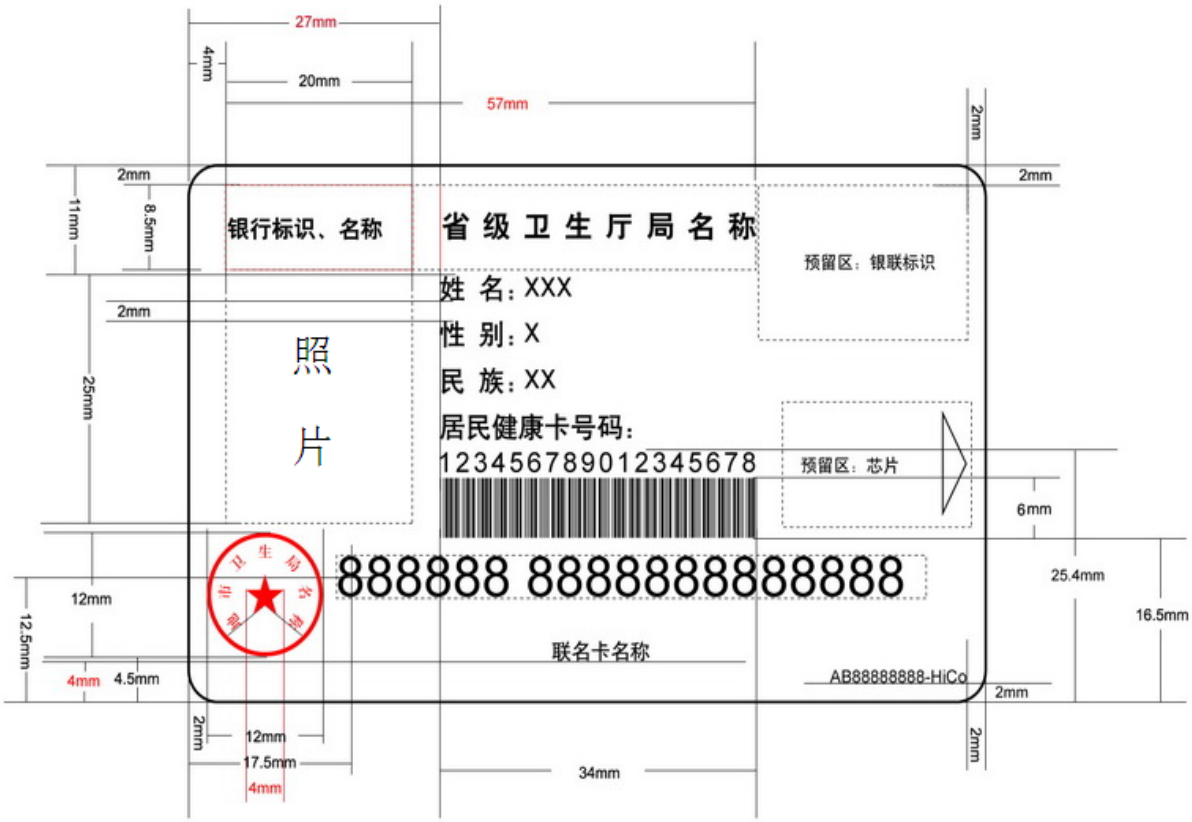


图 6-3 预留金融功能的居民健康卡背面布局

表 6-3 预留金融功能区的卡片背面布局参数

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
持卡人个人信息		
“姓名” 、“性别”、“民族”字体、“居民健康卡号码”字体	汉仪中黑 8.0PT	/
“姓名”、 “性别”、“民族”、 “居民健康卡号码”左边沿到卡的左边沿的距离	27.00mm	±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”、 “居民健康卡号码”四行的行间距	2.00mm	±0.30mm
可变信息部分		
“姓名、性别、民族、居民健康卡号码”填写值字体	汉仪中黑 8.0PT	/
“民族”填写值	不带”族”字， 例如 ”汉”	
“姓名、性别、民族、居民健康卡号码”字色值	K100	/
“居民健康卡号码”填写值上边沿距卡片下边沿距离	25.40mm	±0.30mm
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
发卡机构标识区		
“省级发卡机构名称”区域大小	宽 34MM 高 8.5MM	±0.30mm
“省级发卡机构名称”字体	汉仪大黑简 8.6PT，加粗	/
“省级发卡机构名称”区域左边沿到卡的左边沿的距离	27.00mm	±0.30mm
“省级发卡机构名称”区域右边沿到卡的左边沿的距离	61.00mm	±0.30mm
“省级发卡机构名称”区域上边沿到卡的上边沿的距离	2.00mm	±0.30mm
“省级发卡机构名称”区域高度	8.50mm	±0.30mm
“省级发卡机构名称”水平方向	水平方向上均匀充满区域	
发卡机构公章直径	12.00mm	±0.30mm
发卡机构公章左边沿到卡的左边沿的距离	2.00mm	±0.30mm
红色公章色值	C0 、 M100 、 Y100、K0	/
发卡机构公章下边沿到卡的下边沿的距离	4.50mm	±0.30mm
发卡机构公章边线	1.2pt	±0.30mm
发卡机构公章内五角星	4 mm x4mm	±0.30mm
发卡机构公章内文字	汉仪中宋 4.5PT	/
发卡机构公章内文字起始边界	五角星下方两个角	/

	内侧延长线	
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
联名卡名称区（该区内容根据需要可有可无）		
“联名卡名称”字体	汉仪中黑 6pt	/
“联名卡名称”字间距	0	/
“联名卡名称”下边沿距卡的下边沿的距离	4mm	±0.30mm
“联名卡名称”水平方向	与条型码等长的区域内居中	±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	

6.3.3 卡片正面样式

卡片正面应包括以下要素：居民健康卡标识图案、卡名（居民健康卡）和居民健康卡监制部门（中华人民共和国卫生部监制）卡片正面布局及参数见图6-4和表6-4。

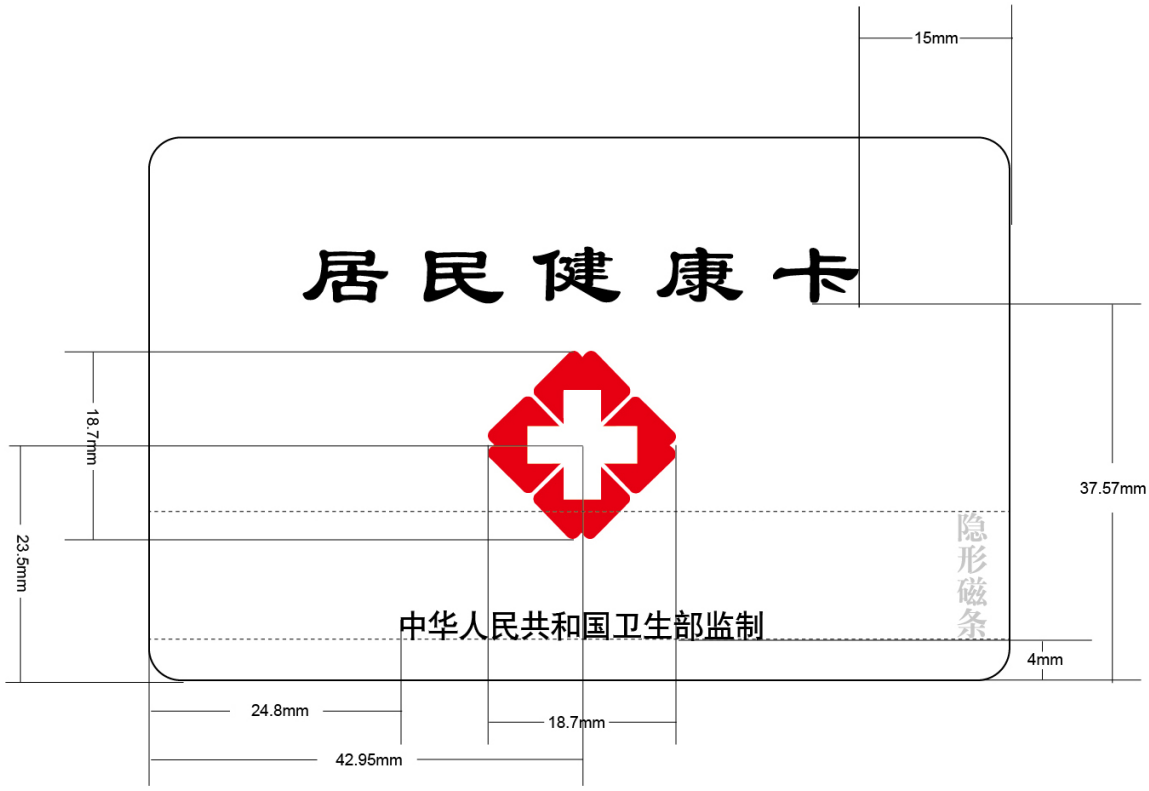


图 6-4 卡片正面布局

注：图6-4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。

表 6-4 卡片正面布局参数

参数	规格及要求	公差
居民健康卡标识图案		
居民健康卡标识图案		/
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	/
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
居民健康卡监制部门		
“中华人民共和国卫生部监制”字样	汉仪中黑简体 9pt	/
左边沿到卡的左边沿的距离	24.8mm	±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）居民健康卡使用照片基本要求：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。

2）居民健康卡的磁条应按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。

3) 卡片正反面未注明距离、高、宽公差的参数，公差为±0.30mm。

4) 居民康卡的条形码是对居民健康卡号码即公民身份号码进行编码的128条码，格式应按GB/T 18347—2001规定。

6.3.4 居民健康卡联名卡的卡片背面样式

卡片背面应包括以下要素和文字：底色与卡正面一致，无底纹、底图，带居民健康卡号条形码，有“本卡由**银行与**卫生厅局联合发行” 和“使用本卡遵循**银行及卫生部有关章程和规定”字样及持卡人姓名（拼音或汉字）。其中条形码遵循128标准，无特殊说明的卡面文字、位置及大小等根据各联合发卡金融机构（银行）需要，可按相应规范、标准进行调整，不做具体要求。卡片背面布局参考图6-5。

图 6-5 联名卡背面布局参考图

6.3.5 居民健康卡联名卡的卡片正面面样式

卡片正面底色、花纹、“居民健康卡及标识”以国家卫生和计划生育委员会提供的矢量文件为准，卡面应包括居民健康卡标识及卡名称（居民健康卡），卡片正面布局及参数见图6-6和表6-5。

图 6-6 联名卡正面布局

表 6-5 联名卡正面布局参数

参数	规格及要求	公差
居民健康卡及标识图案		
居民健康卡标识红色部分色号	C0、M100、Y100、K0	/
“居民健康卡及标识”区域	卡片右上区域	/
“居民健康卡及标识”下边沿距卡上边沿	12.20mm	±0.30mm
“居民健康卡”下边沿距卡上边沿	10.00mm	±0.30mm
“居民健康卡及标识”左边沿距卡右边沿	37.00mm	±0.30mm
“居民健康卡及标识”长度	32.00mm	±0.30mm
金融机构（银行）标识、名称区		
“银行标识、名称”区域	卡片左上区域	/
“银行标识、名称”	在视觉上不大于“居民健康卡及标识”	/
“银行标识、名称”区域右边沿到卡左边沿距离	37.00mm	±0.30mm
“银行标识、名称” 区域下边沿到卡上边沿距离	12.20mm	±0.30mm
“银行标识、名称”水平方向	区域内居中	/
“银行标识、名称”垂直方向	区域内靠下	/
其它区域（该区内容由合作发卡金融机构（银行）来定）		
有接触式芯片	金融功能由接触式芯片和磁条实现	/
无接触式芯片	金融功能由磁条实现	/

6.3.6 卡面颜色标准及图案

色度差、公差见表6-6。

表 6-6 卡片颜色标准

	居民健康卡标识图案红	公章红	字体颜色
允许公差△E*	<=5.00	<=5.00	<=5.00

注：△E*表示色差。

图案（矢量文件）及颜色由国家卫生和计划生育委员会统一提供。

7 终端接口要求

终端必须能够对居民健康卡进行操作。

终端应采用醒目的方式标示读卡区域，保证能方便地将卡放置到操作区域。

终端应带有至少一个安全存取模块（SAM）卡座，用以支持居民健康卡应用的安全认证功能。

终端须经国家卫生和计划生育委员会指定的相关检测机构进行符合性检测，取得终端产品备案证书。

终端具体要求遵循《WS XXX.3 居民健康卡技术规范 第4部分：终端技术规范》的有关规定。

8 卡数据标准

8.1 数据框架

居民健康卡数据分为身份识别数据、卡识别数据、基础健康数据、管理数据四大类，框架如图8-1所示。

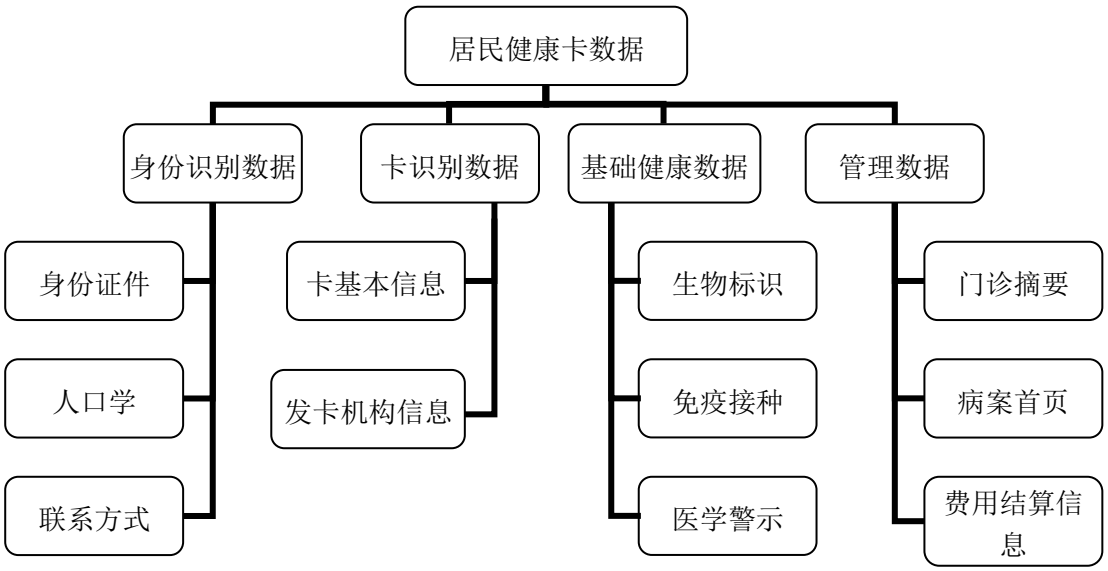


图 8-1 居民健康卡数据框架示意图

8.1.1 身份识别数据

身份识别数据指持卡人的唯一的身份标识，包括身份证件、人口学、联系方式等。

8.1.2 卡识别数据

卡识别数据指与居民健康卡基本数据及发卡机构有关数据，包括卡基本信息、发卡机构信息等。

8.1.3 基础健康数据

基础健康数据指与持卡人急诊、急救相关的静态数据，包括生物标识、免疫接种、医学警示等。

8.1.4 管理数据

管理数据指与持卡人基本诊疗活动有关的动态数据，包括门诊摘要、病案首页、费用结算信息等。

8.2 数据标准

居民健康卡数据标准应符合 WS 363、WS 364、WS 365，遵循《WS XXX 居民健康卡数据集》的有关要求。

8.3 数据格式

居民健康卡数据格式应符合WS 363、WS 364、WS 365，见表8-1，详细内容遵循《WS XXX 居民健康卡数据集》的有关要求。

表 8-1 居民健康卡数据格式列表

标志	数据项	类型	长度	字段属性	所属文件	备注
01	卡的类别	ans	01	禁止改写 自由读	MF\DDF1\EF05	
02	规范版本	ans	04			
03	发卡机构名称	ans	30			
04	发卡机构代码	cn	11			
05	发卡机构证书	b	180			
06	发卡时间	cn	04			
08	卡号	ans	18			
09	安全码	ans	03			
10	发卡序列号	ans	10			
57	应用城市代码	cn	03			
11	姓名	ans	30	禁止改写 读控制	MF\DDF1\EF06	
12	性别	b	01			
13	民族代码	cn	01			
14	出生日期	cn	04			

标志	数据项	类型	长度	字段属性	所属文件	备注
15	居民身份证号码	ans	18			
	照片	b	3074	读写控制	MF\DDF1\EF07	
07	卡有效期	cn	04	读写控制	MF\DDF1\EF08	
16	本人电话 1	ans	20			
17	本人电话 2	ans	20			
18	医疗费用支付方式	cn	01			
19	医疗费用支付方式	cn	01			
20	医疗费用支付方式	cn	01			
21	地址类别 1	cn	01	读写控制	MF\DDF1\DF01\ EF05	
22	地址 1	ans	100			
23	地址类别 2	cn	01			
24	地址 2	ans	100			
25	联系人姓名 1	ans	30	读写控制	MF\DDF1\DF01\EF06	
26	联系人关系 1	cn	01			
27	联系人电话 1	ans	20			
28	联系人姓名 2	ans	30			
29	联系人关系 2	cn	01			
30	联系人电话 2	ans	20			
31	联系人姓名 3	ans	30			
32	联系人关系 3	cn	01			
33	联系人电话 3	ans	20			
34	文化程度代码	cn	01	读写控制	MF\DDF1\DF01\EF07	
35	婚姻状况代码	cn	01			
36	职业代码	ans	03			

标志	数据项	类型	长度	字段属性	所属文件	备注
37	证件类别	cn	01	读写控制	MF\DDF1\DF01\EF08	
38	证件号码	ans	18			
39	健康档案编号	ans	17			
40	新农合证（卡）号	ans	18			
41	ABO 血型代码	b	01	读写控制	MF\DDF1\DF02\EF05	
42	RH 血型代码	cn	01			
43	哮喘标志	b	01			
44	心脏病标志	b	01			
45	心脑血管病标志	b	01			
46	癫痫病标志	b	01			
47	凝血紊乱标志	b	01			
48	糖尿病标志	b	01			
49	青光眼标志	b	01			
50	透析标志	b	01			
51	器官移植标志	b	01			
52	器官缺失标志	b	01			
53	可装卸的义肢标志	b	01			
54	心脏起搏器标志	b	01			
55	其他医学警示名称	ans	40			
56	精神病标志	b	01	读写控制	MF\DDF1\DF02\EF06	
	过敏物质名称	ans	20	读写控制	MF\DDF1\DF02\EF07	循环记录文件（3 条记录）
	过敏反应	ans	100			
	免疫接种名称	ans	20	读写控制	MF\DDF1\DF02\EF08	循环记录文件（10 条记录）
	免疫接种时间	cn	04			

标志	数据项	类型	长度	字段属性	所属文件	备注
	住院记录有效标志	b	01	读写控制	MF\DDF1\DF03\EF05	FF:记录无效 00:记录有效 定长记录文件 （3 条记录）
	门诊记录有效标志	b	01	读写控制	MF\DDF1\DF03\EF06	FF:记录无效 00:记录有效 定长记录文件 （5 条记录）
	住院机构名称	ans	70	读写控制	MF\DDF1\DF03\EE01 … MF\DDF1\DF03\EE03	
	住院机构组织机构代码	ans	10			
	入院日期	cn	04			
	住院患者住院次数	cn	02			
	病案号	ans	18			
	住院患者入院科室名称	ans	50			
	住院患者入院病情	cn	01			
	住院患者医院感染名称	ans	50			
	住院患者损伤和中毒外部原因	ans	07			
	住院患者血清学检查项目代码 1	cn	01			
	住院患者血清学检查结果代码 1	cn	01			
	疾病诊断名称 1	ans	50			
	疾病诊断代码 1	ans	07			
	确诊日期 1	cn	04			
	住院患者诊断符合情况-详细描述 1	ans	20			

标志	数据项	类型	长度	字段属性	所属文件	备注
	住院患者诊断符合情况-代码 1	cn	01			
	住院患者疾病诊断类型-详细描述 1	ans	20			
	住院患者疾病诊断类型-代码 1	cn	01			
	住院患者治疗结果代码 1	cn	01			
	手术/操作-名称 1	ans	80			
	手术/操作-代码 1	ans	5			
	手术/操作-日期 1	cn	04			
	麻醉-方法 1	ans	50			
	麻醉-方法代码 1	cn	01			
	手术切口愈合等级代码 1	cn	01			
	住院患者血清学检查项目代码 2	cn	01			
	住院患者血清学检查结果代码 2	cn	01			
	疾病诊断名称 2	ans	50			
	疾病诊断代码 2	ans	07			
	确诊日期 2	cn	04			
	住院患者诊断符合情况-详细描述 2	ans	20			
	住院患者诊断符合情况-代码 2	cn	01			
	住院患者疾病诊断类型-详细描述 2	ans	20			
	住院患者疾病诊断类型-代码 2	cn	01			
	住院患者治疗结果代码 2	cn	01			
	手术/操作-名称 2	ans	80			
	手术/操作-代码 2	ans	5			
	手术/操作-日期 2	cn	04			
	麻醉-方法 2	ans	50			

标志	数据项	类型	长度	字段属性	所属文件	备注
	麻醉-方法代码 2	cn	01			
	手术切口愈合等级代码 2	cn	01			
	住院患者血清学检查项目代码 3	cn	01			
	住院患者血清学检查结果代码 3	cn	01			
	疾病诊断名称 3	ans	50			
	疾病诊断代码 3	ans	07			
	确诊日期 3	cn	04			
	住院患者诊断符合情况-详细描述 3	ans	20			
	住院患者诊断符合情况-代码 3	cn	01			
	住院患者疾病诊断类型-详细描述 3	ans	20			
	住院患者疾病诊断类型-代码 3	cn	01			
	住院患者治疗结果代码 3	cn	01			
	手术/操作-名称 3	ans	80			
	手术/操作-代码 3	ans	5			
	手术/操作-日期 3	cn	04			
	麻醉-方法 3	ans	50			
	麻醉-方法代码 3	cn	01			
	手术切口愈合等级代码 3	cn	01			
	住院期间输血品种代码 1	cn	01			
	住院期间输血量 1	cn	02			
	住院患者输血量计量单位 1	ans	10			
	住院期间输血品种代码 2	cn	01			
	住院期间输血量 2	cn	02			
	住院患者输血量计量单位 2	ans	10			
	住院期间输血品种代码 3	cn	01			

标志	数据项	类型	长度	字段属性	所属文件	备注
	住院期间输血量 3	cn	02			
	住院患者输血量计量单位 3	ans	10			
	住院期间输血品种代码 4	cn	01			
	住院期间输血量 4	cn	02			
	住院患者输血量计量单位 4	ans	10			
	住院患者抢救次数	cn	02			
	住院患者抢救成功次数	cn	02			
	出院日期	cn	04			
	住院患者出院科室名称	ans	50			
	住院患者住院天数	cn	03			
	住院患者尸检标志	b	01			
	住院患者随诊标志	b	01			
	住院费用-医疗付款方式代码	cn	01			
	住院费用-分类 1	ans	20			
	住院费用-分类代码 1	ans	01			
	住院费用-金额 1	cn	05			
	住院费用-分类 2	ans	20			
	住院费用-分类代码 2	ans	01			
	住院费用-金额 2	cn	05			
	住院费用-分类 3	ans	20			
	住院费用-分类代码 3	ans	01			
	住院费用-金额 3	cn	05			
	住院费用-分类 4	ans	20			
	住院费用-分类代码 4	ans	01			
	住院费用-金额 4	cn	05			
	住院费用-分类 5	ans	20			
	住院费用-分类代码 5	ans	01			
	住院费用-金额 5	cn	05			

标志	数据项	类型	长度	字段属性	所属文件	备注
	住院费用-分类 6	ans	20			
	住院费用-分类代码 6	ans	01			
	住院费用-金额 6	cn	05			
	住院费用-分类 7	ans	20			
	住院费用-分类代码 7	ans	01			
	住院费用-金额 7	cn	05			
	住院费用-分类 8	ans	20			
	住院费用-分类代码 8	ans	01			
	住院费用-金额 8	cn	05			
	住院费用-分类 9	ans	20			
	住院费用-分类代码 9	ans	01			
	住院费用-金额 9	cn	05			
	住院费用-分类 10	ans	20			
	住院费用-分类代码 10	ans	01			
	住院费用-金额 10	cn	05			
	住院费用-分类 11	ans	20			
	住院费用-分类代码 11	ans	01			
	住院费用-金额 11	cn	05			
	住院费用-分类 12	ans	20			
	住院费用-分类代码 12	ans	01			
	住院费用-金额 12	cn	05			
	住院费用-分类 13	ans	20			
	住院费用-分类代码 13	ans	01			
	住院费用-金额 13	cn	05			
	住院费用-分类 14	ans	20			
	住院费用-分类代码 14	ans	01			
	住院费用-金额 14	cn	05			
	住院费用-分类 15	ans	20			
	住院费用-分类代码 15	ans	01			

标志	数据项	类型	长度	字段属性	所属文件	备注
	住院费用-金额 15	cn	05			
	住院费用-分类 16	ans	20			
	住院费用-分类代码 16	ans	01			
	住院费用-金额 16	cn	05			
	住院费用-分类 17	ans	20			
	住院费用-分类代码 17	ans	01			
	住院费用-金额 17	cn	05			
	住院费用-分类 18	ans	20			
	住院费用-分类代码 18	ans	01			
	住院费用-金额 18	cn	05			
	住院费用-分类 19	ans	20			
	住院费用-分类代码 19	ans	01			
	住院费用-金额 19	cn	05			
	住院费用-分类 20	ans	20			
	住院费用-分类代码 20	ans	01			
	住院费用-金额 20	cn	05			
	住院总费用	cn	05			
	床位费	cn	05			
	住院护理费	cn	05			
	住院西药费	cn	05			
	住院中药费	cn	05			
	住院化验费	cn	05			
	住院诊疗费	cn	05			
	住院手术费	cn	05			
	住院检查费	cn	05			
	其他住院费用	cn	05			
	交易信息签名	b	64			
	SAM 卡证书	b	190			

标志	数据项	类型	长度	字段属性	所属文件	备注
	就诊机构名称	ans	70	读写控制	MF\DDF1\DF03\ED01 … MF\DDF1\DF01\ED05	
	就诊机构组织机构代码	ans	10			
	就诊日期时间	cn	07			
	门诊号	ans	18			
	就医科室名称	ans	50			
	医疗付款方式	cn	01			
	症状名称 1	ans	50			
	症状代码 1	ans	05			
	诊断日期 1	cn	04			
	门诊诊断名称 1	ans	50			
	门诊诊断代码 1	ans	07			
	发病日期时间 1	cn	07			
	症状持续时间 1	cn	02			
	症状名称 2	ans	50			
	症状代码 2	ans	05			
	诊断日期 2	cn	04			
	门诊诊断名称 2	ans	50			
	门诊诊断代码 2	ans	07			
	发病日期时间 2	cn	07			
	症状持续时间 2	cn	02			
	症状名称 3	ans	50			
	症状代码 3	ans	05			
	诊断日期 3	cn	04			
	门诊诊断名称 3	ans	50			
	门诊诊断代码 3	ans	07			

标志	数据项	类型	长度	字段属性	所属文件	备注
	发病日期时间 3	cn	07			
	症状持续时间 3	cn	02			
	症状名称 4	ans	50			
	症状代码 4	ans	05			
	诊断日期 4	cn	04			
	门诊诊断名称 4	ans	50			
	门诊诊断代码 4	ans	07			
	发病日期时间 4	cn	07			
	症状持续时间 4	cn	02			
	症状名称 5	ans	50			
	症状代码 5	ans	05			
	诊断日期 5	cn	04			
	门诊诊断名称 5	ans	50			
	门诊诊断代码 5	ans	07			
	发病日期时间 5	cn	07			
	症状持续时间 5	cn	02			
	检查/检验项目名称 1	ans	80			
	检查/检验结果代码 1	cn	01			
	检查/检验定量结果 1	cn	05			
	检查/检验计量单位 1	ans	20			
	检查/检验项目代码 1	ans	20			
	检查/检验项目名称 2	ans	80			
	检查/检验结果代码 2	cn	01			
	检查/检验定量结果 2	cn	05			
	检查/检验计量单位 2	ans	20			
	检查/检验项目代码 2	ans	20			
	检查/检验项目名称 3	ans	80			
	检查/检验结果代码 3	cn	01			

标志	数据项	类型	长度	字段属性	所属文件	备注
	检查/检验定量结果 3	cn	05			
	检查/检验计量单位 3	ans	20			
	检查/检验项目代码 3	ans	20			
	检查/检验项目名称 4	ans	80			
	检查/检验结果代码 4	cn	01			
	检查/检验定量结果 4	cn	05			
	检查/检验计量单位 4	ans	20			
	检查/检验项目代码 4	ans	20			
	检查/检验项目名称 5	ans	80			
	检查/检验结果代码 5	cn	01			
	检查/检验定量结果 5	cn	05			
	检查/检验计量单位 5	ans	20			
	检查/检验项目代码 5	ans	20			
	检查/检验项目名称 6	ans	80			
	检查/检验结果代码 6	cn	01			
	检查/检验定量结果 6	cn	05			
	检查/检验计量单位 6	ans	20			
	检查/检验项目代码 6	ans	20			
	检查/检验项目名称 7	ans	80			
	检查/检验结果代码 7	cn	01			
	检查/检验定量结果 7	cn	05			
	检查/检验计量单位 7	ans	20			
	检查/检验项目代码 7	ans	20			
	检查/检验项目名称 8	ans	80			
	检查/检验结果代码 8	cn	01			
	检查/检验定量结果 8	cn	05			
	检查/检验计量单位 8	ans	20			
	检查/检验项目代码 8	ans	20			
	检查/检验项目名称 9	ans	80			

标志	数据项	类型	长度	字段属性	所属文件	备注
	检查/检验结果代码 9	cn	01			
	检查/检验定量结果 9	cn	05			
	检查/检验计量单位 9	ans	20			
	检查/检验项目代码 9	ans	20			
	检查/检验项目名称 10	ans	80			
	检查/检验结果代码 10	cn	01			
	检查/检验定量结果 10	cn	05			
	检查/检验计量单位 10	ans	20			
	检查/检验项目代码 10	ans	20			
	药物名称 1	ans	50			
	药物剂型代码 1	cn	01			
	用药天数 1	cn	03			
	药物使用频率 1	ans	20			
	药物使用剂量单位 1	ans	06			
	药物使用次剂量 1	cn	03			
	药物使用总剂量 1	cn	06			
	药物使用途径代码 1	cn	02			
	药物名称 2	ans	50			
	药物剂型代码 2	cn	01			
	用药天数 2	cn	03			
	药物使用频率 2	ans	20			
	药物使用剂量单位 2	ans	06			
	药物使用次剂量 2	cn	03			
	药物使用总剂量 2	cn	06			
	药物使用途径代码 2	cn	02			
	药物名称 3	ans	50			
	药物剂型代码 3	cn	01			
	用药天数 3	cn	03			

标志	数据项	类型	长度	字段属性	所属文件	备注
	药物使用频率 3	ans	20			
	药物使用剂量单位 3	ans	06			
	药物使用次剂量 3	cn	03			
	药物使用总剂量 3	cn	06			
	药物使用途径代码 3	cn	02			
	药物名称 4	ans	50			
	药物剂型代码 4	cn	01			
	用药天数 4	cn	03			
	药物使用频率 4	ans	20			
	药物使用剂量单位 4	ans	06			
	药物使用次剂量 4	cn	03			
	药物使用总剂量 4	cn	06			
	药物使用途径代码 4	cn	02			
	药物名称 5	ans	50			
	药物剂型代码 5	cn	01			
	用药天数 5	cn	03			
	药物使用频率 5	ans	20			
	药物使用剂量单位 5	ans	06			
	药物使用次剂量 5	cn	03			
	药物使用总剂量 5	cn	06			
	药物使用途径代码 5	cn	02			
	手术/操作名称 1	ans	80			
	手术/操作代码 1	ans	5			
	手术/操作日期 1	cn	04			
	手术/操作名称 2	ans	80			
	手术/操作代码 2	ans	5			
	手术/操作日期 2	cn	04			
	手术/操作名称 3	ans	80			
	手术/操作代码 3	ans	5			

标志	数据项	类型	长度	字段属性	所属文件	备注
	手术/操作日期 3	cn	04			
	门诊费用分类名称 1	ans	20			
	门诊费用分类代码 1	cn	01			
	门诊费用金额 1	cn	04			
	门诊费用分类名称 2	ans	20			
	门诊费用分类代码 2	cn	01			
	门诊费用金额 2	cn	04			
	门诊费用分类名称 3	ans	20			
	门诊费用分类代码 3	cn	01			
	门诊费用金额 3	cn	04			
	门诊费用分类名称 4	ans	20			
	门诊费用分类代码 4	cn	01			
	门诊费用金额 4	cn	04			
	门诊费用分类名称 5	ans	20			
	门诊费用分类代码 5	cn	01			
	门诊费用金额 5	cn	04			
	门诊费用分类名称 6	ans	20			
	门诊费用分类代码 6	cn	01			
	门诊费用金额 6	cn	04			
	门诊费用分类名称 7	ans	20			
	门诊费用分类代码 7	cn	01			
	门诊费用金额 7	cn	04			
	门诊费用分类名称 8	ans	20			
	门诊费用分类代码 8	cn	01			
	门诊费用金额 8	cn	04			
	门诊费用分类名称 9	ans	20			
	门诊费用分类代码 9	cn	01			
	门诊费用金额 9	cn	04			

标志	数据项	类型	长度	字段属性	所属文件	备注
	门诊费用分类名称 10	ans	20			
	门诊费用分类代码 10	cn	01			
	门诊费用金额 10	cn	04			
	交易信息签名	b	64			
	SAM 卡证书	b	190			

注：“类型”项是指一种数据表示类型，其中“b”表示二进制数(Binary)，“cn”表示压缩数字(Compressed Numeric)，“ans”表示特殊字母数字型(Alphanumeric Special)。“长度”项采用的是十进制表示。

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ans的数据元左对齐，右补0。

9 数据安全

9.1 算法

居民健康卡采用国家密码管理局颁布的对称算法SM1算法，非对称算法SM2算法和杂凑算法SM3算法。

9.1.1 算法

SM1算法的分组长度为128比特，密钥长度为128比特。

9.1.2 SM2 算法

本规范中SM2算法用于证书的生成和验证、签名数据的生成和验证。

本规范使用基于256位Fp（素数域）上的椭圆曲线参数。涉及到的参数包括：

— 一个256位长的大素数p；

— 大整数a和b，定义曲线方程y2＝x3+ax+b mod p；

— 椭圆曲线的阶n，表示满足方程y2＝x3+ax+b mod p的点的数量，要求n为素数；

— 一个椭圆曲线上的点G＝（Gx，Gy），满足方程Gy2＝Gx3+aGx+b mod p，G被称为基点，通过基点可以生成椭圆曲线上的所有点。

SM2密钥对包括私钥SK和公钥PK ：

— SK是一个小于n-1的正整数，使用随机数产生；

— PK＝（x，y）是椭圆曲线上的点，即满足方程y2＝x3+ax+b mod p，由于p的长度为32字节，因此PK的长度为64字节。

SM2包含下面三种算法：

— 依赖于私钥SK的签名函数Sign(SK)[M]，该函数输出两个32字节长度的数字r和s。

— 依赖于公钥PK的验证函数Verify(PK)[M，Sign(SK)[M]]，该函数输出True或False，表示验证正确或失败。

— 使用SM3哈希算法H[ ]，将任意长度的报文映射为一个32字节的哈希值。

9.1.3 SM3 算法

SM3算法对于任意长度的报文输入，产生一个32字节的哈希值。

9.2 基本安全要求

9.2.1 共存应用

居民健康卡上每一个应用应该放在一个单独的DF中，亦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。

9.2.2 密钥的独立性

用于一种特定功能（如读取数据）的加密/解密密钥不能被任何其他功能所使用，包括保存在居民健康卡中的密钥和用来产生、派生和传输这些密钥的密钥。

9.3 密钥和个人密码的存放

居民健康卡应该能够保证用于选定的加（解）密算法的非对称私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，则应保证其在居民健康卡中的安全存放，且在任何情况下都不会被泄露。

9.4 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。

9.4.1 安全报文传送格式

本部分中定义的安全报文传送格式须符合GB/T 16649.4的规定。当CLA字节的第二个半字节等于十六进制数字‘4’时，表明对发送方命令数据要采用安全报文传送。

9.4.2 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。

9.4.2.1MAC 的位置

MAC是命令数据域中最后一个数据元。

9.4.2.2MAC 的长度

本部分中，MAC的长度规定为4个字节。

9.4.2.3 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 9.6 章节描述的过程密钥的产生过程产生的。

应用维护密钥用于产生 MAC 过程密钥。

9.4.2.4MAC 的计算

使用SM1算法 CBC分组加密方式产生MAC，步骤如下：

1) 取16字节的十六进制数‘00’作为初始变量。

2) 按照顺序将以下数据连接在一起形成数据块：

——（CLA，INS，P1，P2，Lc）

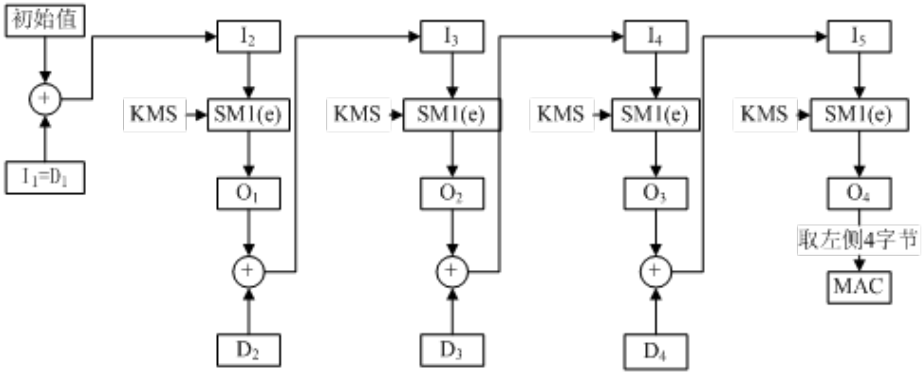
——在命令的数据域中（如果存在）包含明文或加密的数据。（例：如果要更改个人密码，加密后的个人密码数据块放在命令数据域中传输）

3) 将该数据块分成16字节为单位的数据块，标号为D1，D2，D3，D4等。最后的数据块可能是1-16个字节。

4) 如果最后的数据块长度是16字节的话，则在其后加上十六进制数‘80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’，转到步骤5）；如果最后的数据块长度不足16字节，则在其后加上十六进制数‘80’，如果达到16字节长度，则转入步骤5）；否则在其后加入十六进制数‘00’直到长度达到16字节。

5) 按图9- 1所述方法计算MAC，过程密钥按照9.6 章节描述的方式产生。

6) 最终得到的是从计算结果左侧取得4字节长度的MAC。



I = 输入　　D = 数据块

SM1(e) = 数据加密算法（加密模式）　　KMS = MAC过程密钥

+ = 异或运算　　O = 输出

图 9-1 MAC 计算

9.4.3 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。

9.4.3.1 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9.6 章节描述的方式产生。应用维护密钥用于产生数据加密过程密钥。

9.4.3.2 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技术进行加密。

9.4.3.3 数据加密计算

数据加密计算，如图9-2，步骤如下：

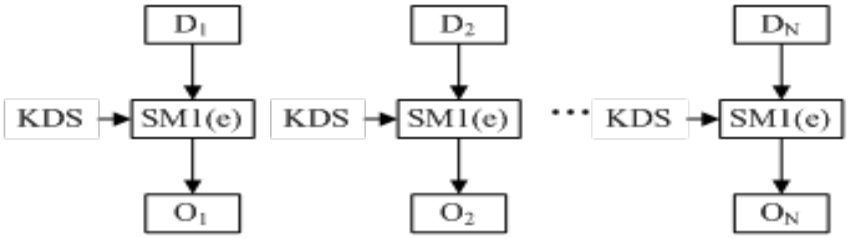
1) 用LD表示明文数据的长度，在明文数据前加上LD产生新的数据块。

2) 将步骤1）中生成的数据块分解成16字节数据块，标号为D1，D2，D3，D4等等。最后一个数据块长度有可能不足16字节。

3) 如果最后（或唯一）的数据块长度等于16字节，转入步骤4）；如果不足16字节，在右边添加十六进制数‘80’。如果长度已达16字节，转入步骤4）；否则，在其右边添加十六进制数‘00’，直到长度达到16字节。

4) 每一个数据块使用9.6 章节描述的数据加密过程密钥加密。

5) 计算结束后，所有加密后的数据块依照原顺序连接在一起（O1，O2，等等）。



SM1(e) = 数据加密算法（加密模式） D = 数据块

SM1(d) = 数据加密算法（解密模式） KDS = 数据加密过程密钥

O = 输出

图 9-2 数据加密

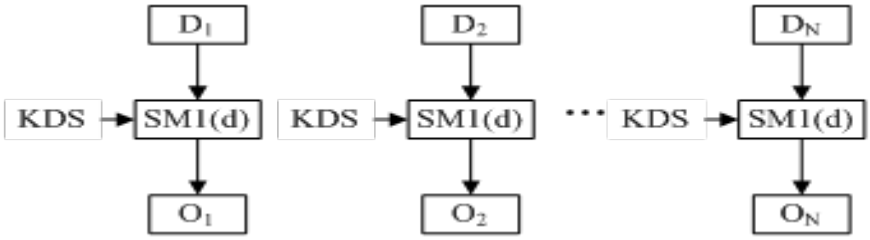
9.4.3.4 数据解密计算

数据解密计算，如图9-3，步骤如下：

1) 将命令数据域中的数据块分解成16字节长的数据块，标号为D1，D2，D3，D4等等。每个数据块使用如9.6 章节所描述的方法产生的数据加密过程密钥进行解密。

2) 计算结束后，所有解密后的数据块依照顺序（O1， O2，等等)链接在一起。数据块由LD、明文数据、填充字符组成。

3) LD表示明文数据的长度，用来恢复明文数据。



SM1(e) = 数据加密算法（加密模式） D = 数据块

SM1(d) = 数据加密算法（解密模式） KDS = 数据加密过程密钥 O = 输出

图9-3数据解密

9.5 子密钥分散

如图9-4，子密钥的分散因子为8字节。用指定的分散因子拼接分散因子求反值作为输入数据，做加密计算，产生的16字节的结果作为子密钥。

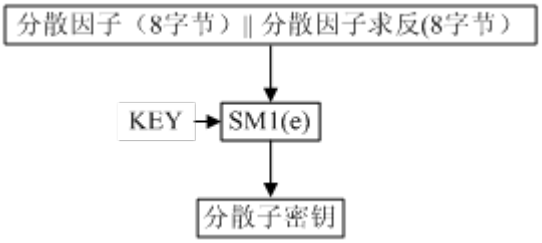


图 9- 4 子密钥计算方法

9.6 过程密钥的产生

如图9-5，MAC和数据加密的过程密钥是用可变数据产生的密钥。

过程密钥产生后只能在某过程中使用一次。

输入数据是8字节随机数拼接8字节全‘00’。

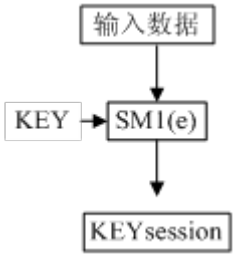


图 9-5 过程密钥的产生

9.7 操作权限鉴别

操作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。

9.7.1 鉴别数据的长度

本部分中，鉴别数据的长度规定为8个字节。

9.7.2 操作权限鉴别过程密钥的产生

在操作权限鉴别过程中用到的操作权限鉴别过程密钥是在鉴别过程中用可变数据产生的密钥，按照9.6 章节中描述的方法产生。

操作权限鉴别加密算法密钥的鉴别密钥用于产生操作权限鉴别过程密钥。

过程密钥产生后只能在鉴别过程中使用一次。

输入数据是鉴别命令引用的可变数据（如随机数）。

9.7.3 鉴别数据的计算

如图9-6，使用9.6 章节描述的操作权限鉴别过程密钥对原始数据进行加密，加密结果左右8字节异或得到鉴别数据。

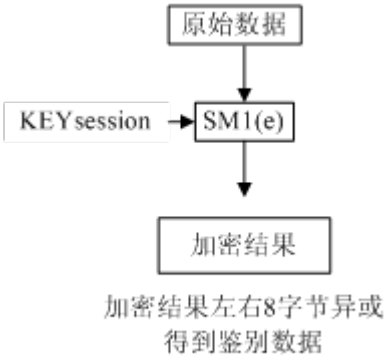


图 9-6 鉴别数据计算

9.8 数字签名产生与验证

数字签名产生，对任意长数据组成的报文MSG签名的步骤如下：

1) 计算报文MSG的32字节的HASH值 h:= H[MSG]；

2) 计算Sign(SK)[h]，得到两个32字节长度的数字r和s；

3) 数字签名S被定义为64字节长度的数字S:=r||s，即数字签名S由数字r和s串联而成。

数字签名验证，对任意长数据组成的报文MSG验证签名S的步骤如下：

1) 计算报文MSG的32字节的HASH值 h:= H[MSG]；

2) 计算Verify(PK)[h, S]，若函数输出True表示验证正确，若输出False，表示验证失败。

9.9 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。

SAM卡内嵌于居民健康卡终端设备中，为系统提供高级别的安全保护。SAM卡与终端可以视为一体。SAM卡中存放多组不同版本不同索引的主密钥。所有的主密钥通常必须在终端投入使用之前，被下载到SAM卡中。如果在终端使用过程中，主密钥需要修改，必须使用安全报文。该操作的实现必须在特殊的授权情况下完成。为避免伪操作，存放在SAM卡中的不同类型的主密钥必须与不同特定的应用操作相结合使用。在终端上进行居民健康卡应用操作时需要使用SAM卡进行安全保护。不同机构配发的SAM卡中装载的密钥类型依据该机构的所支持的应用类型决定。

9.10 密钥机制

9.10.1 对称密钥

对系统使用的对称密钥，用特定的分散因子作为输入数据，做加密计算，产生的结果作为子密钥。系统中密钥的生成机制如图9-1所示。

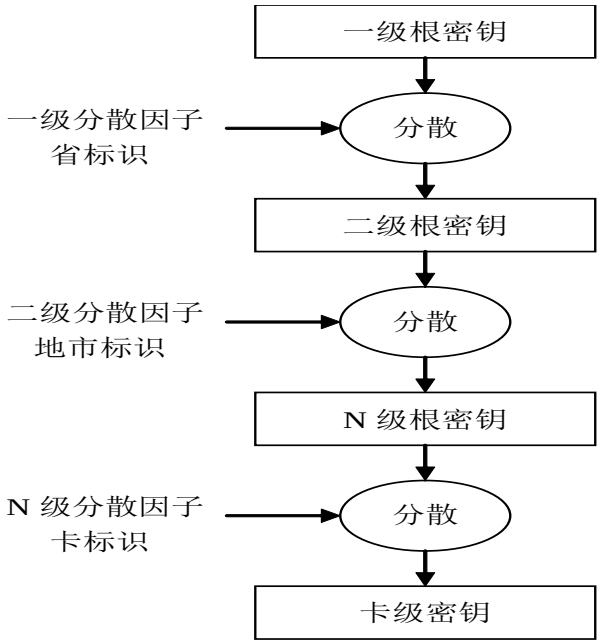


图 9-7 密钥生成机制

9.10.2 非对称密钥

9.10.2.1 居民健康卡二级非对称密钥体系

居民健康卡的非对称密钥体系采用二级架构，如图9-2所示。

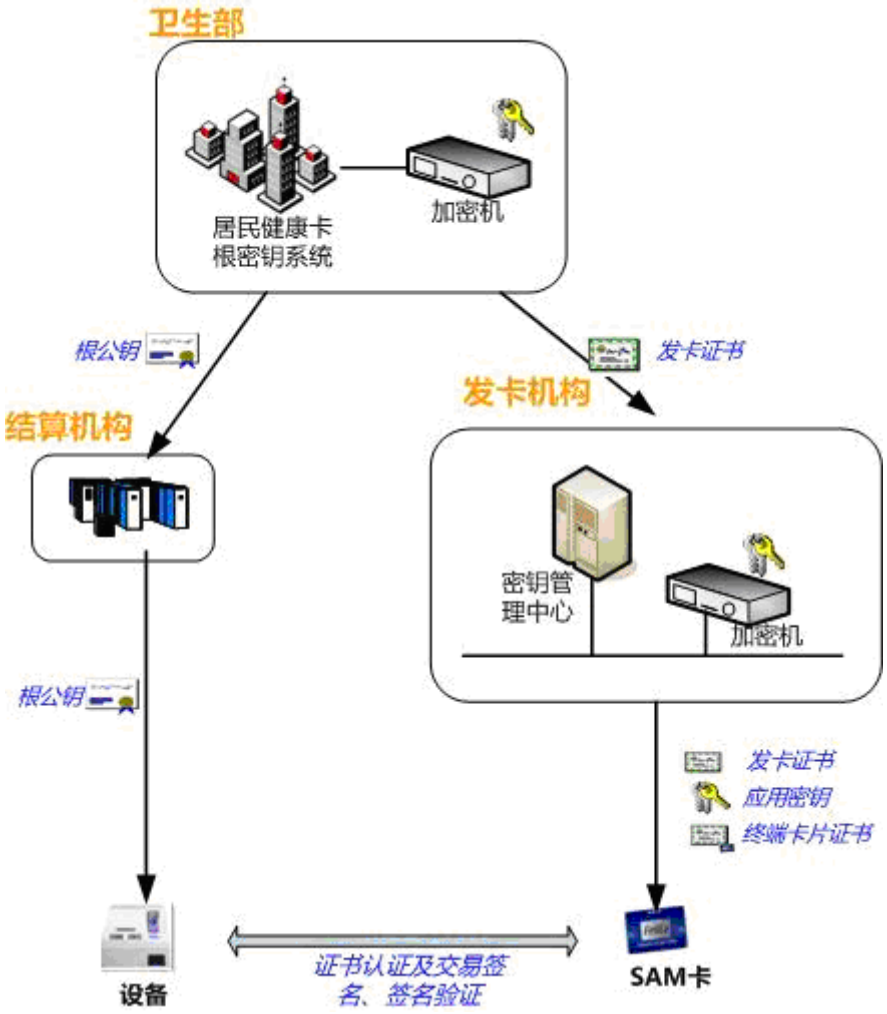


图 9-8 非对称密钥体系

居民健康卡根密钥管理机构负责签发发卡机构的公钥证书。根密钥管理机构私钥由根密钥管理机构保管并保证其私密性和安全性。

发卡机构负责签发终端SAM的公钥证书，发卡机构私钥由发卡机构保管并保证其私密性和安全性。发卡机构的发卡证书，使用居民健康卡根密钥管理机构的根私钥签名生成。

终端SAM卡的证书，由发卡机构使用私钥对终端公钥及证书信息进行签名生成。

9.10.2.2 证书密钥使用

证书密钥使用如图9-3，结算机构终端通过根公钥索引定位根公钥，并用根公钥验证发卡机构的发卡证书并得到发卡机构的公钥值，再使用发卡机构的公钥验证终端SAM卡的证书并得到SAM卡的公钥，结算机构终端得到SAM卡的公钥后，就可以使用该公钥验证卡片中的签名数据。

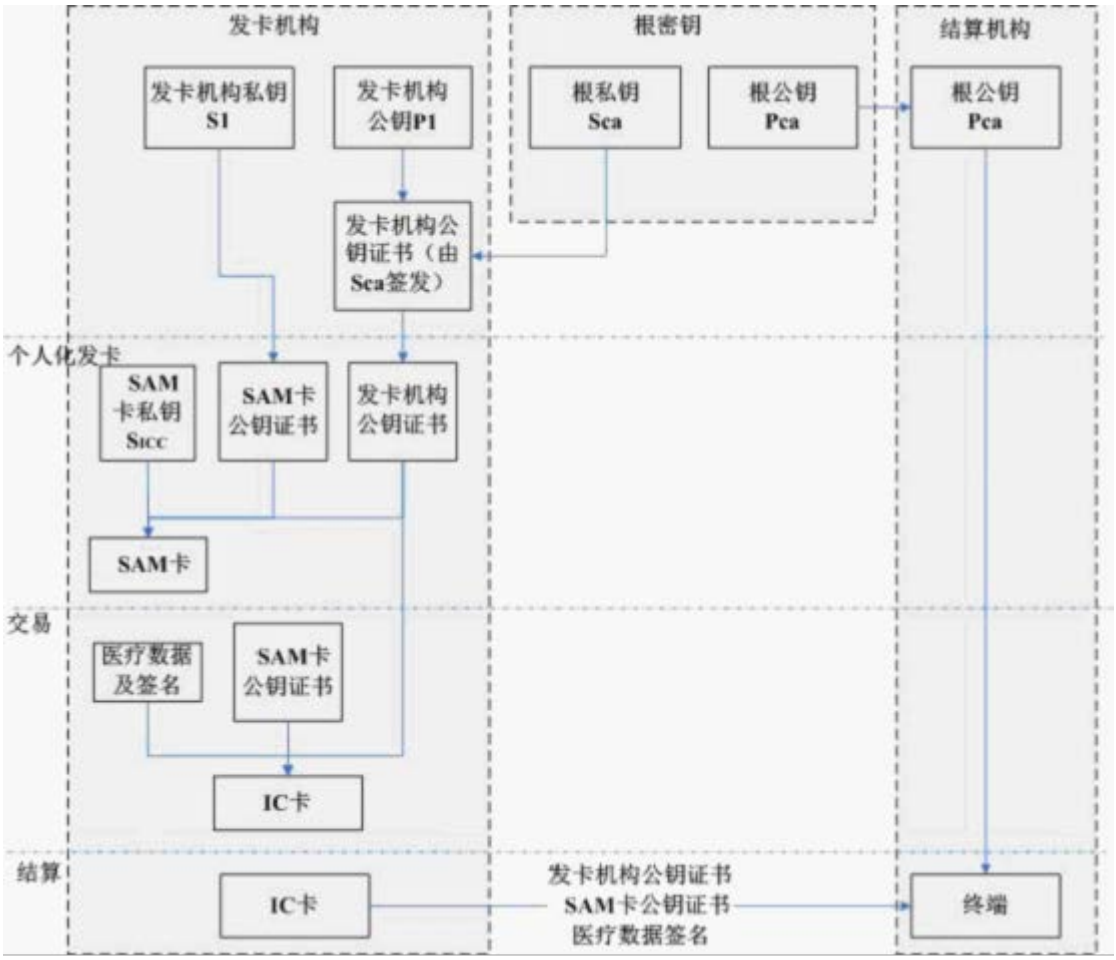


图 9-9 证书密钥使用

9.10.2.3 居民健康卡使用的公钥种类

在居民健康卡公钥认证体系中使用了三种公私钥对：根公私钥对、发卡机构公私钥对和终端SAM卡公私钥对，其作用如表9-1。

表 9-1 非对称密钥种类

密钥名称	用途
根公私钥对	用于对发卡机构签发公钥证书
发卡机构公私钥对	用于对 SAM 卡签发公钥证书
SAM 卡公私钥对	用于交易签名和验证

9.10.2.4 根证书文件

1） 根证书的文件命名

根证书文件的命名格式为：00000001.RAA，其中：

— 00000001为居民健康卡的应用标识号

— R为根证书的类型标识

— AA为根公钥的索引，以0xAA格式标识

2） 根证书的内容格式

根证书是二进制数据，其格式和内容如表9-2所示。

表 9-2 根证书格式

字段名	长度（字节）	描述
未签名根公钥输出扩展	47+64	详细见表 9-3
自签名的根公钥数据	64	

3） 未签名根公钥输出扩展

未签名根公钥输出扩展是根公钥文件的第一部分，其格式和内容如表9-3所示。

表 9-3 未签名根公钥输出扩展格式

字段名	长度（字节）	描述	格式
记录头	1	十六进制’20’	b
应用标识号	4	标识一个应用，居民健康卡应用标识为十六进制’00000001’	b
根公钥长度	2	根证书的公钥长度以十六进制表示，当前为’0040’	b
根公钥算法标识	1	十六进制’02’-SM2	b
哈希算法标识	1	十六进制’03’-SM3	b
应用供应商标识	5	标识国家卫生和计划生育委员会	b
根公钥索引	1	唯一标识根公钥	b
根公钥 1	32	根公钥 1	b
根公钥 2	32	根公钥 2	b
哈希值	32	本表从第 1 到 9 项的连接数据的 SM3 哈希值	b

4） 自签名的根公钥数据

使用根私钥对未签名根公钥输出扩展中的“哈希值”数据进行私钥加密的结果就是自签名的根公钥数据。

9.10.2.5 发卡机构公钥输入文件

发卡机构为获得发卡机构生产型公钥证书或测试型公钥证书，需向根密钥管理机构提交发卡机构公钥证书申请，申请时需要提交发卡机构公钥输入文件。

1) 发卡机构公钥输入文件命名

发卡机构公钥输入文件的命名格式为：WSTTTTTT.INP，其中：

— WS为国家卫生和计划生育委员会的标识

— TTTTTT为记录号，唯一标识一个发卡机构的一次申请，由根密钥管理机构统一管理和分发

— INP为文件类型标识

2) 发卡机构公钥输入文件的内容格式

发卡机构公钥输入文件是二进制数据，其格式和内容如表9-4所示。

表 9-4 发卡机构公钥输入文件格式

字段名	长度（字节）	描述
未签名发卡机构公钥输入扩展	51+64	详细见表 9-5
自签名的发卡机构公钥数据	64	

3) 未签名发卡机构公钥输入扩展

未签名发卡机构公钥输入扩展是文件的第一部分，其格式和内容如表9-5所示。

表 9-5 未签名发卡机构公钥输入扩展格式

字段名	长度（字节）	描述	格式
记录头	1	十六进制’21’	b
应用标识号	4	标识一个应用，居民健康卡应用标识为十六进制’00000001’	b
证书格式	1	十六进制’01’	b
发卡机构标识	4	发卡机构的编号	cn8
证书失效日期	2	月和年（MMYY），在该月最后一天之后证书失效	n4
记录号	3	发卡机构公钥证书申请记录号	n6

公钥算法标识	1	十六进制’02’-SM2	b
哈希算法标识	1	十六进制’03’-SM3	b
发卡机构公钥长度	2	公钥长度以十六进制表示，当前为’0040’	b
发卡机构公钥 1	32	发卡机构公钥 1	b
发卡机构公钥 2	32	发卡机构公钥 2	b
哈希值	32	本表从第 1 到 11 项的连接数据的 SM3 哈希值	b

4) 自签名的发卡机构公钥数据

使用发卡机构私钥对未签名发卡机构公钥输入扩展中的“哈希值”数据进行私钥加密的结果就是签名的发卡机构公钥数据。

9.10.2.6 发卡机构公钥输出文件

发卡机构的公钥证书文件。

1) 发卡机构公钥输出文件命名

发卡机构公钥输出文件的命名格式为：AAAAAA.INN，其中：

— AAAAAA为记录号，唯一标识一个发卡机构的发卡证书，由根密钥管理机构统一管理和分发，与发卡机构公钥输入文件的记录号一致。

— I为文件类型标识，表示发卡证书

— NN为根公钥索引

2) 发卡机构公钥输出文件的内容格式

发卡机构公钥输出文件是二进制数据，其格式和内容如表9-6所示。

表 9-6 发卡机构公钥输出文件格式

字段名	长度（字节）	描述
未签名发卡机构公钥输出扩展	52+64	详细见表 9-7
签名的发卡机构公钥数据	64	

3) 未签名发卡机构公钥输出扩展

未签名发卡机构公钥输出扩展是文件的第一部分，其格式和内容如表9-7所示。

表 9-7 未签名发卡机构公钥输出扩展格式

字段名	长度（字节）	描述	格式
记录头	1	十六进制’23’	b
应用标识号	4	标识一个应用，居民健康卡应用标识为十六进制’00000001’	b
证书格式	1	十六进制’02’	b
发卡机构标识	4	发卡机构的编号	cn8
证书失效日期	2	月和年（MMYY），在该月最后一天之后证书失效	n4
记录号	3	发卡机构公钥证书申请记录号	n6
公钥算法标识	1	十六进制’02’-SM2	b
哈希算法标识	1	十六进制’03’-SM3	b
发卡机构公钥长度	2	公钥长度以十六进制表示，当前为’0040’	b
发卡机构公钥 1	32	发卡机构公钥 1	b
发卡机构公钥 2	32	发卡机构公钥 2	b
根公钥索引	1	根密钥系统用来签发发卡机构公钥证书的公钥索引	b
哈希值	32	本表从第 1 到 12 项的连接数据的 SM3 哈希值	b

4) 签名的发卡机构公钥数据

使用根私钥对未签名发卡机构公钥输出扩展中的“哈希值”数据进行私钥加密的结果

9.10.2.7 终端 SAM 卡证书

终端SAM卡的公钥证书格式，该证书不单独形成文件，而是整合在卡片个人化文件中一起下发给个人化系统，由个人化系统写入SAM卡。

1) SAM卡证书格式

SAM卡证书是二进制数据，其格式和内容如表9-8所示。

表 9-8 SAM 卡证书格式

字段名	长度（字节）	描述
未签名的 SAM 卡公钥输出扩展	62+64	详细见表 9-9
签名的 SAM 卡公钥数据	64	

2) 未签名的SAM卡公钥输出扩展

未签名的SAM卡公钥输出扩展，其格式和内容如表9-9所示。

表 9-9 未签名的 SAM 卡公钥输出扩展

字段名	长度（字节）	描述	格式
证书格式	1	十六进制’04’	b
卡号	10	SAM 卡的卡号	cn
证书序列号	3	由发卡机构分配给这张证书的唯一的二进制数	b
证书失效日期	2	月和年（MMYY），在该月最后一天之后证书失效	n4
所属机构代码	10	本终端 SAM 卡所属的医疗机构组织机构代码，不足 10 字节后补十六进制’00’	ans
公钥算法标识	1	十六进制’02’-SM2	b
哈希算法标识	1	十六进制’03’-SM3	b
SAM 卡公钥长度	2	SAM 卡证书公钥长度以十六进制表示，当前为’00 40’	b
SAM 卡公钥 1	32	SAM 卡公钥 1	b
SAM 卡公钥 2	32	SAM 卡公钥 2	b
哈希值	32	本表从第 1 到 10 项的连接数据的 SM3 哈希值	b

3) SAM卡公钥数据

使用发卡机构私钥对未签名的SAM卡公钥输出扩展中的“哈希值”数据进行私钥加密的结果就是签名的SAM卡公钥数据。

10 应用

10.1 文件

本部分定义了居民健康卡在医疗领域的各项专有应用，如图10-1所示，DDF1是居民健康卡应用环境，DDF2是其他预留应用环境。

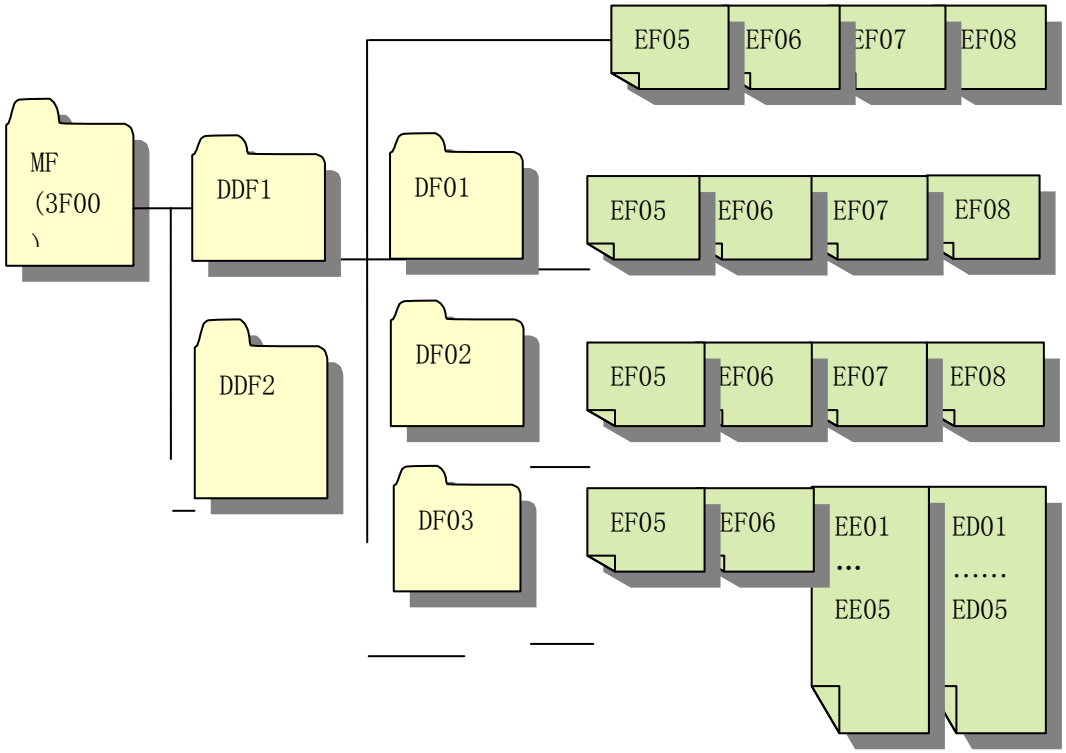


图 10-1 居民健康卡文件结构示意图

10.1.1 文件结构

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

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。

10.1.2 专用文件

居民健康卡目录定义文件（DDF1）的下一层是各具体应用所对应的专用文件（DF），各DF下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。

10.1.3 数据文件

基本数据文件（EF）包含了一组与应用相关的数据。

居民健康卡应用的基本数据文件（EF）有两种类型：记录文件类型和二进制文件类型。

10.1.4 文件选择

居民健康卡应用的各个专用文件，可以用应用标识符（AID）、文件标识符（FID）两种方式来进行选择。

成功选择了居民健康卡应用的专用文件后，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。

10.2 应用标识符

应用标识符（AID）的结构符合GB/T 16649.5的规定，它包含两个部分：

1) 一个经过注册的应用提供者标识符（长度为5字节），它唯一地标识应用提供者。

2) 一个可选的“专用应用标识符扩展码（PIX）域，由应用提供者定义，最长11字节。

居民健康卡应用的各个具体应用的标识符（AID），必须采用由国家IC卡注册中心颁发的RID，并通过RID选择该应用。

10.3 应用密钥

10.3.1 密钥配置

所有 SAM 卡安装内部认证密钥，用来进行居民康卡的鉴别。在需要读取居民康卡内数据的终端 SAM 卡上安装数据读控密钥，在需要更新居民康卡内数据的终端 SAM 卡上安装数据写控密钥。居民康卡密钥配置文件说明见表10-1。

表 10-1 密钥配置文件列表

数据区	文件标识符	文件类型	读控制	写控制
MF\DDF1	EF05	变长记录	无	禁止改写
	EF06	变长记录	读控密钥	禁止改写
	EF07	变长记录	读控密钥	写控密钥
	EF08	变长记录	读控密钥	写控密钥
MF\DDF1\DF01（身份识别数据区）	EF05	变长记录	读控密钥	写控密钥
	EF06	变长记录	读控密钥	写控密钥
	EF07	变长记录	读控密钥	写控密钥
	EF08	变长记录	读控密钥	写控密钥
MF\DDF1\DF02（基础健康信息）	EF05	变长记录	读控密钥	写控密钥
	EF06	变长记录	读控密钥	写控密钥
	EF07	循环记录	读控密钥	写控密钥
	EF08	循环记录	读控密钥	写控密钥
MF\DDF1\DF03（管理数据）	EF05	定长记录	读控密钥	写控密钥
	EF06	定长记录	读控密钥	写控密钥
	EE01…EE03	二进制	读控密钥	写控密钥
	ED01…ED03	二进制	读控密钥	写控密钥
预留				

注： 1)其中，MF\DDF1\DF01区域下的EF05、EF06、EF07、EF08文件，MF\DDF1\DF02区域下的EF05、EF06、EF07、EF08文件，在进行更新时需要采用密文加MAC的安全报文传送格式；MF\DDF1\DF03区域下的EF05、EF06文件，在进行更新时需要采用MAC的安全报文传送格式。

2)读控密钥、写控密钥是用于文件读写控制的鉴别密钥。

10.3.2 密钥用途

居民建康卡上的密钥必须安全存储。存储在居民健康卡上的密钥用途见表10-2。

表 10- 2 密钥用途列表

分类	密钥	用途	密钥对应文件	适用的应用范围
内部认证密钥	IRK_{DDF1}	鉴别发卡方的密钥	-	应用提供者
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_{DDF1}		-	卡识别应用
	STK_{DF01}		-	身份识别应用
	STK_{DF02}		-	基础健康应用
	STK_{DF03}		-	管理数据应用
卡片或应用锁定控制密钥	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_{DF01}		-	身份识别应用
	LK_{DF02}		-	基础健康应用
	LK_{DF03}		-	管理数据应用
应用数据更新密钥	$UK1_{DDF1}$	发卡方或应用提供方控制应用数据更新操作的鉴别密钥	EF07、EF08	发卡方和持卡人基本信息
	$UK1_{DF01}$		EF05 、 EF06 、 EF07、EF08	身份识别数据信息
	$UK1_{DF02}$		EF05	医学警示数据信息
	$UK2_{DF02}$		EF06	特殊信息数据信息
	$UK3_{DF02}$		EF07、EF08	过敏、免疫基本数据信息
	$UK1_{DF03}$		EF05、EF06、EE01…EE05 ED01…ED05	管理数据信息
应用数据擦除密钥	$UK2_{DF03}$	发卡方或应用提供方	EF05、EF06	管理数据信息

		控制应用数据擦除操作的鉴别密钥		
应用数据读取密钥	$RK1_{DDF1}$	发卡方或应用提供方控制部分应用数据读取操作的鉴别密钥	EF06 、 EF07 、 EF08	基本信息
	$RK1_{DF01}$		EF05、EF06、EF07、EF08	证件记录信息
	$RK1_{DF02}$		EF05、EF06、EF07、EF08	特殊信息数据信息
	$RK1_{DF03}$		EF05、EF06、EE01…EE03 ED01…ED05	管理数据信息

10.4 应用流程

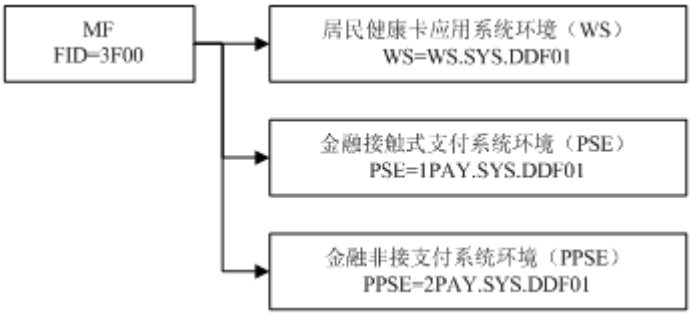
所有应用都要求终端必须安装居民健康卡SAM卡，终端与SAM卡之间以安全方式进行通信。应用流程遵循WS XXXXX.2-2013 居民健康卡技术规范 第2部分：用户卡应用规范。

附 录 A
（规范性附录）
加载金融应用居民健康卡及终端技术要求

A.1 多应用选择

A.1.1 多应用卡片文件结构

多应用居民健康IC卡的卡片总体结构应符合图A.1要求。



图A.1 卡片总体结构

MF是多应用居民健康IC卡的根，其下有：

□□健康卡应用系统环境WS；

□□金融接触式支付环境PSE（可选）；

□□金融非接支付系统环境PPSE。

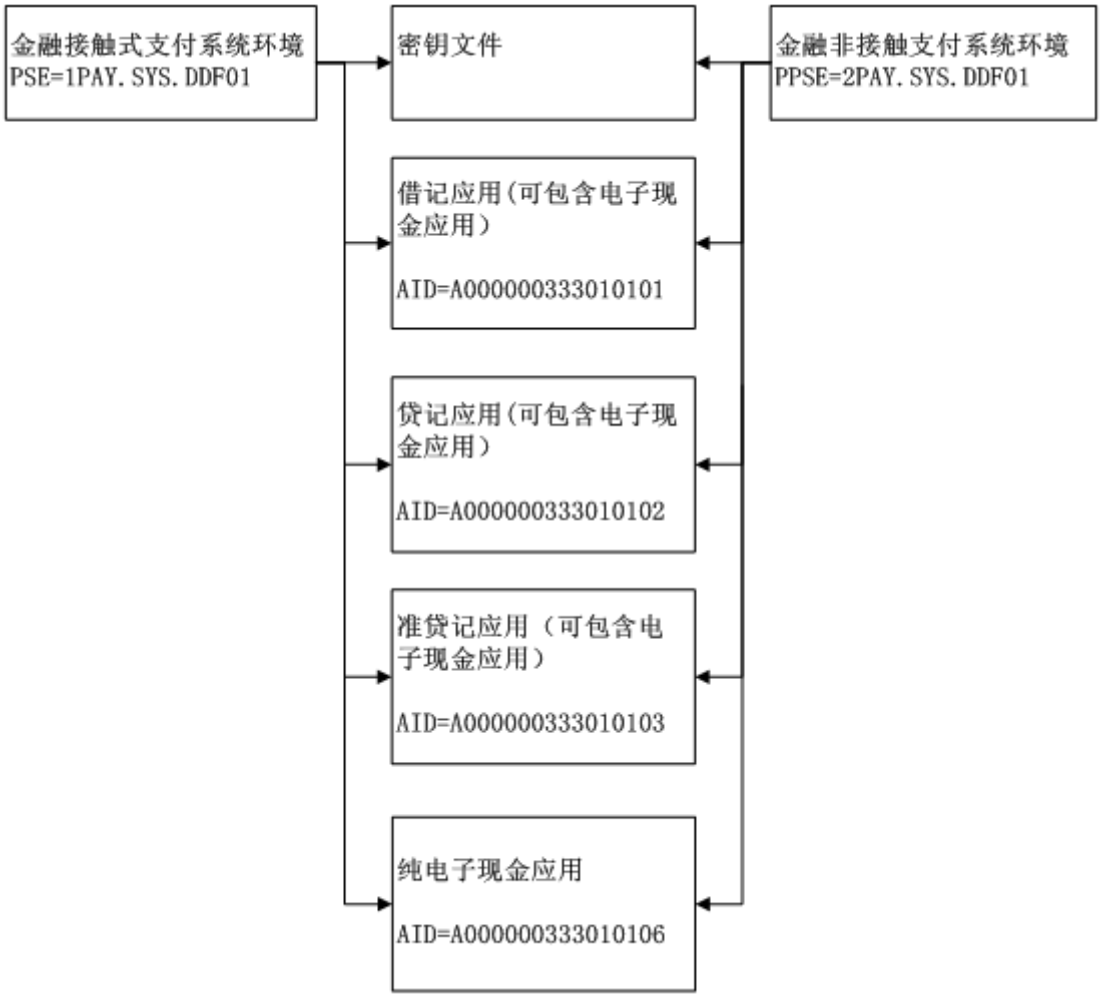
进入到各系统环境后，相关指令、交易流程、安全机制遵循当前应用环境卡片技术规范要求（健康卡应用系统环境-居民健康卡相关规范，金融环境-JR/T0025）。卡片和终端在完成复位应答后，卡片当前目录应位于MF下。

A.1.1.1 金融支付系统环境

金融支付系统环境是中国金融集成电路IC卡应用的入口。

金融支付系统环境具有2种入口形式分别是：接触式支付环境入口和非接触支付环境入口，其中接触式支付环境为可选环境。

内部结构如图A.2所示：



图A.2　金融支付系统环境结构

金融支付系统环境分为PSE入口和PPSE入口，其中PSE对应标准接触式金融支付交易入口，PPSE对应非接触式金融支付系统环境入口。

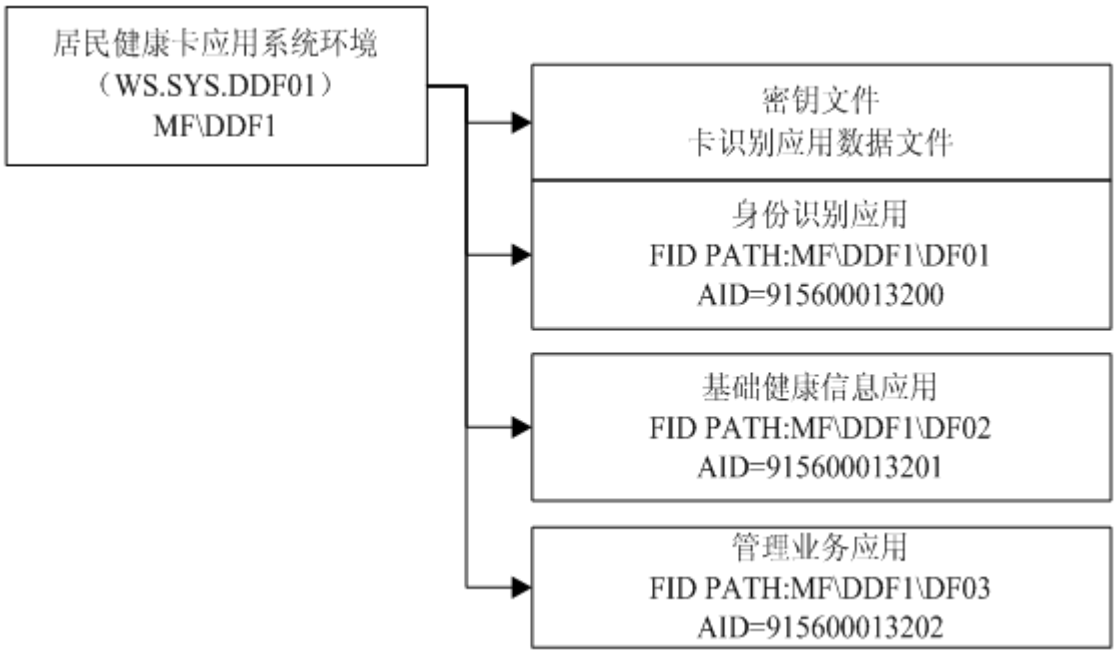
由PSE进入的应用应符合JR/T0025.3-7，

具有小额支付功能的还应符合JR/T0025.13，

由PPSE进入的应用应符合JR/T0025.12。

A.1.1.2　居民健康卡应用系统环境

居民健康卡应用系统环境是居民健康卡应用的入口，其内容接口如图A.3所示。



图A.3　居民健康卡应用卡片结构

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。

A.1.2　多应用选择流程

A.1.2.1　终端复位

终端与卡片完成复位应答后，卡片当前目录应位于MF下，终端通过选择不同的应用环境进入不同的应用场景。

应用环境名称列表如下：

环境	AID
WS	‘WS.SYS.DDF01’
PSE	‘1PAY.SYS.DDF01’
PPSE	‘2PAY.SYS.DDF01’

A.1.2.2　选择金融应用环境

1)　终端通过发送SELECT PSE进入接触式金融支付应用，其指令、应用流程和安全机制均符合JR/T0025的要求。

2)　终端通过发送SELECT PPSE进入非接触金融支付应用，其指令、应用流程和安全机制均符合JR/T0025.12的要求。

3)　进入金融支付应用后，终端应通过应用选择的方式确定一个应用（借记应用或贷记应用或准贷记应用或纯电子现金应用）进行支付。

A.1.2.3　选择健康卡应用环境

1)　终端通过发送SELECT　WS.SYS.DDF01进入居民健康卡应用，其指令、应用流程和安全机制均符合居民健康卡相关规范。

2) 进入居民健康卡应用后，终端应通过文件、应用选择的方式进行卫生医疗文件信息读写操作。

A.2 居民健康卡及终端技术要求:

加载金融应用的居民健康卡及终端应满足以下要求:

1) 居民健康卡用户卡——电气特性部分（fc+fs时调制信号幅度和fc-fs时调制信号幅度等）参照金融规范《中国金融集成电路（IC）卡规范》第11部分：非接触式IC 卡通讯规范。

测试依据参照《中国金融集成电路（IC）卡非接触式 IC卡检测规范》。

2) 居民健康卡用户卡——通讯协议部分（基本交换及时间和块协议中的命令处理等）参照金融规范《中国金融集成电路（IC）卡规范》第11部分：非接触式IC 卡通讯规范。

测试依据参照《中国金融集成电路（IC）卡非接触式 IC卡检测规范》。

3) 居民健康卡终端——非接触模拟部分（PCD场强、PCD灵敏度响应和PCD位编码和异步响应等）参照金融规范《中国金融集成电路（IC）卡规范》第11部分：非接触式IC 卡通讯规范。

测试依据参照《中国金融集成电路（IC）卡 非接触式应用终端检测规范》。

4) 居民健康卡终端——非接触数字部分（轮询的执行及时间、同步时间前响应和链接I块响应等）参照金融规范《中国金融集成电路（IC）卡规范》第11部分：非接触式IC 卡通讯规范。

测试依据参照《中国金融集成电路（IC）卡 非接触式应用终端检测规范》。