

XXXXXX  
XXXX

WS

中华人民共和国卫生行业标准

WS XXX—201X

## 电子健康卡技术规范 第1部分：总则

Technical specification for electronic health card Part 1:

General

(征求意见稿)

201X-XX-XX 发布

201X-XX-XX 实施

国家卫生健康委员会 发布



## 目 次

1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	2
3.1 电子健康卡 .....	2
3.2 电子健康卡管理系统 .....	2
3.3 主索引 ID .....	3
3.4 电子健康卡 ID .....	3
3.5 电子健康卡二维码 .....	3
3.6 密码设备 .....	3
3.7 接入机构 .....	3
3.8 接入 APP .....	3
3.9 电子健康卡 SDK 接口 .....	3
3.10 电子健康卡 SDK 授权管理系统 .....	3
3.11 识读终端 .....	4
4 前言 .....	4
5 系统框架 .....	5
6 技术要求 .....	7
7 检测要求 .....	8

## 前 言

本标准由卫生部卫生信息标准专业委员会提出。

WS XXX 《电子健康卡技术规范》分为6个部分：

- 第1部分：总则；
- 第2部分：管理系统；
- 第3部分：识读终端；
- 第4部分：密码机；
- 第5部分：客户端应用软件接入检测；
- 第6部分：联网检测；

本部分为WS XXX的第1部分。

本标准主要起草单位：国家卫生健康委员会

本标准主要起草人：

# 电子健康卡技术规范 第 1 部分：总则

## 1 范围

本规范规定了电子健康卡应用相关系统及设备标准化的内容及技术要求。

本规范适用于电子健康卡应用相关系统及设备的建设、应用、检测和运营维护，适用于所有建设、发行、使用电子健康卡的医疗卫生机构、第三方联合发卡机构、持卡人、相关系统及设备的生产企业等。

## 2 规范性引用文件

下列文件对于本规范的应用是必不可少的。凡是注日期的引用文件，其随后所有的修改单(不包括刊物的内容)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(包括所有的修改单)适用于本规范。

中华人民共和国主席令第 18 号. 中华人民共和国电子签名法. 2004 年 8 月 28 日

中华人民共和国国务院令第 273 号. 商用密码管理条例. 1999 年 10 月 7 日

GB/T 17172-1997 四一七二维码

GB/T 18284-2000 快速响应矩阵码 (QR)

GB/T 21049-2007 汉信码

GB/T 27766-2011 网格矩阵码 (GM)

GB/T 27767-2011 紧密矩阵码 (CM)

GB/T 31770-2015 D9ing 矩阵图码防伪技术条件

GB/T 31868-2015 D9ing 矩阵图码生成器防伪技术条件

GB/T 31869-2015 D9ing 矩阵图码识别仪防伪技术条件

GM/T 0003-2012 SM2 椭圆曲线公钥密码算法

GM/T 0004-2012 SM3 杂凑密码算法

GM/T 0009-2012 SM2 密码算法使用规范

GM/T 0002-2012 sm4 分组密码算法

WS XXX—201X

GM/T 0018-2012 密码设备应用接口规范  
GM/T 0030-2014 服务器密码机技术规范  
GM/T 0022-2014 IPSec VPN 技术规范  
GM/T 0023-2014 IPSec VPN 网关产品规范  
GM/T 0024-2014 SSL VPN 技术规范  
GM/T 0025-2014 SSL VPN 网关产品规范  
WS/T 543.2-2017 居民健康卡技术规范 第2部分：用户卡技术规范  
WS/T 543.3-2017 居民健康卡技术规范 第3部分：用户卡应用规范  
WS/T 543.5-2017 居民健康卡技术规范 第5部分：终端技术规范  
JR/T 0149-2016 中国金融移动支付 支付标记化技术规范  
PCAC/T 0001-2016 个人信息保护技术指引  
Q/CUP 073—2015 中国银联云端支付安全规范  
Q/CUP 053—2016 中国银联电子支付二维码应用规范  
Q/CUP 067—2016 中国银联电子支付二维码安全规范  
卫办综发〔2012〕26号《居民健康卡密钥管理办法》  
卫办综发〔2012〕26号《居民健康卡密钥管理系统技术方案》  
卫办综发〔2012〕26号《居民健康卡生产单位及产品备案管理办法》

### 3 术语和定义

下列术语和定义适用于本规范。

#### 3.1 电子健康卡

通过用户身份标识建立的电子健康卡虚拟化账户，电子健康卡虚拟化账户使用时，可通过二维码形式展现为电子健康卡，功能与实体居民健康卡相同。

#### 3.2 电子健康卡管理系统

在电子健康卡注册用卡过程中，负责电子健康卡发卡数据的生产、使用和管理，采用电子账户对信息进行存储，并支持线下交互的技术应用。

### 3.3 主索引 ID

是标识居民健康卡用户唯一性的信息，通过主索引 ID 关联用户的实体居民健康卡、电子健康卡、医院就诊卡等不同类型账户。

### 3.4 电子健康卡 ID

电子健康卡管理系统用于标识电子健康卡账户唯一性的信息，电子健康卡 ID 由用户的证件类型和证件号码的密文组成。

### 3.5 电子健康卡二维码

电子健康卡通过二维码的形式予以展示，通过“面对面”方式进行交互使用。电子健康卡二维码包括静态二维码和动态二维码：静态二维码可通过移动APP呈现，也可印刷或粘贴于就诊卡等介质上，适用于挂号、问诊等非核心应用场景；动态二维码由APP呈现，在每次使用前生成，其生命周期根据应用安全的要求限定时间范围，适用于病历查询、结算交易等核心应用场景。

### 3.6 密码设备

密码设备是具有某种密码功能或能完成某种密码工作任务的设备的统称。

### 3.7 接入机构

接入使用居民健康卡虚拟化平台，与平台提供接口存在交互逻辑的相关机构事业单位，包括但不限于医疗卫生机构、医保机构等。

### 3.8 接入 APP

接入居民健康卡虚拟化应用平台，与平台接口存在交互逻辑的互联网移动应用。

### 3.9 电子健康卡 SDK 接口

是泛指远程连接到电子健康卡管理系统的API接口软件包，主要完成电子健康卡的注册、二维码申请、二维码验证等功能，接入APP通过SDK接口连接电子健康卡管理系统。

### 3.10 电子健康卡 SDK 授权管理系统

在电子健康卡通过APP进行应用前，需要对该APP通过SDK接口接入电子健康卡管理系统的情况进行授权管理，只有被授权的APP才能接入电子健康卡管理系统，为用户提供注册、电子健康卡申请、电子健康卡验证等服务。

### 3.11 识读终端

识读二维码并与后台应用系统进行交互的终端，一般包括二维码的识读设备和终端机上的应用软件。

## 4 前言

居民健康卡是国家卫生健康委员会统一规划实施的统一标准的“就诊卡”，可实现居民全程健康管理，提升居民健康的统一服务水平。当前智能卡应用正处在从“线下实体”向“线上虚拟”加速转型过程中，推进安全、可信的居民健康卡虚拟化应用建设，实现线上线下一体化的身份认证服务，对于促进服务流程优化，保障线上应用安全，降低发卡用卡成本，实现居民健康卡应用广泛覆盖等具有十分重要的意义。

随着移动技术的发展，移动终端应用软件及虚拟账户的应用已得到普及。通过将实体卡虚拟化的转变方式，可提升居民健康卡在使用过程中的用户体验和应用效率，并可降低发行实体卡的成本。同时，二维码技术在金融支付等领域已得到广泛应用。国家卫生健康委员会联合国家密码管理局、中国支付清算协会、中国银联等共同对二维码技术在居民健康卡体系中的应用进行了研究论证，利用二维码技术高效、低成本等特点，结合标记化技术，有助于推动居民健康卡虚拟化应用的健康、快速发展。

本指引针对居民健康卡虚拟化应用的建设，以目前比较成熟的二维码技术为基础制定，基于其他技术的虚拟化应用将另行制定技术指导方案。本指引适用于各试点单位在实施居民健康卡虚拟化应用时作为依据参考。

各试点单位参照本指引结合自身情况必须编制建设实施方案，并通过专家论证、报国家卫生健康委员会统计信息中心备案。

各试点单位在实施过程对本指引的意见或建议，可向国家卫生健康委员会统计信息中心基层信息化与健康卡管理处提出。

## 5 系统框架

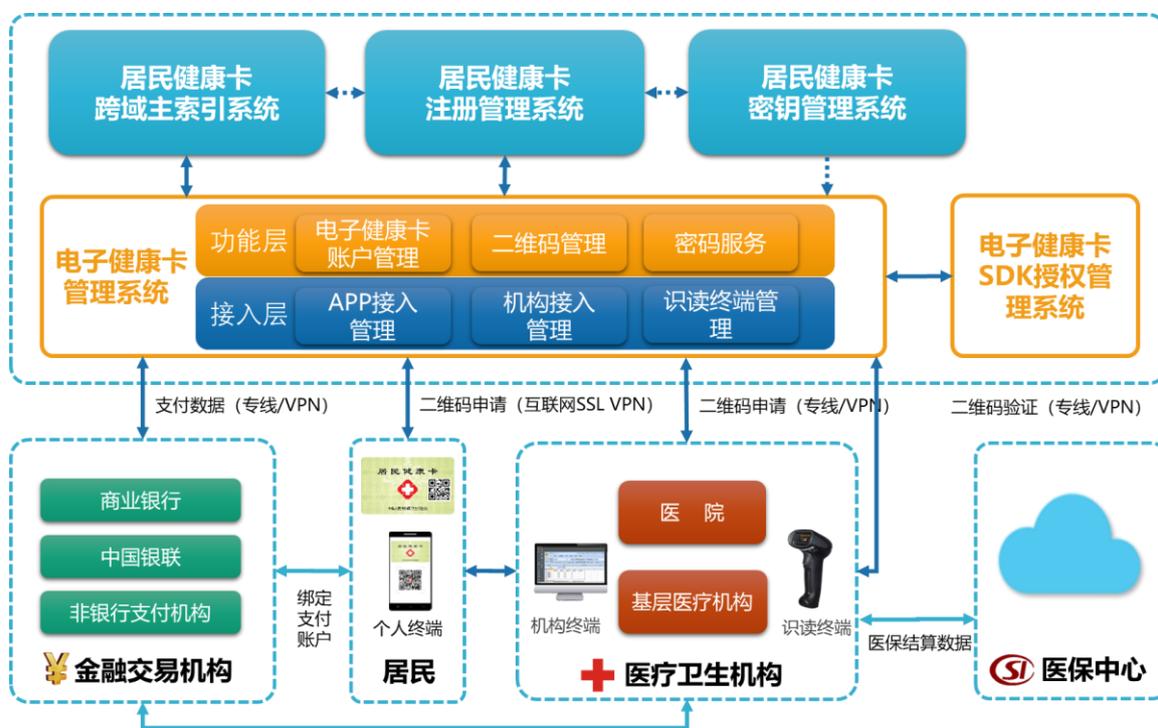


图 5.1 居民健康卡虚拟化系统架构图

注：此图仅表述各系统间的关系，不代表实际的部署架构。

### 5.1 居民健康卡跨域主索引系统

居民健康卡跨域主索引系统是实现全国、省域或市级区域范围内居民信息统一识别的独立的信息管理系统。基于该系统可实现对所辖各区域居民标识域，以及身份证、社保卡、军官证、归国华侨证、就诊卡等标识证的统一注册管理，通过主索引 ID 进行唯一性标识。

### 5.2 居民健康卡注册管理系统

注册管理系统是实体居民健康卡制作和应用过程中，负责居民健康卡制卡数据的生产和管理、提供查验等支持功能的系统，也称居民健康卡卡片管理系统。

在居民健康卡虚拟化建设前期，可将注册管理系统的数据库批量导入虚拟化应用管理系统中，为已有实体居民健康卡用户生成电子健康卡。电子健康卡应具有明确的标识，以便与实体卡区分。

### 5.3 居民健康卡密钥管理系统

居民健康卡密钥管理系统主要功能是对实体居民健康卡密钥生命周期进行管理，包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥恢复、密钥归档。

在居民健康卡虚拟化应用中，为充分利用各省已建成的居民健康卡密钥管理系统，满足密钥使用的统一性，选用应用数据读取密钥和内部认证密钥支撑电子健康卡的应用：应用数据读取密钥作为安全密钥，用于生成电子健康卡 ID，对用户的定位和身份验证；内部认证密钥作为保护密钥，用于对有效时间等信息的加密。

密钥下载需要符合原居民健康卡密钥管理系统的安全规定和管理流程。

#### 5.4 电子健康卡 SDK 授权管理系统

随着居民健康卡虚拟化应用的深入，需要对接入设备、接入 APP 进行有效管控，只允许合法设备和 APP 的接入，以确保电子健康卡虚拟化管理系统的可靠运行。

因此，在建设电子健康卡应用管理系统的同时，需要同步建设电子健康卡 SDK 授权管理系统。通过该系统注册并发布合法的 SDK；对所有通过 SDK 接入电子健康卡虚拟化应用管理系统的 APP 进行注册；对所有注册的 APP 针对相应的 SDK 进行授权；并为电子健康卡管理系统和 APP 开发商提供授权密钥和授权码文件下载。该系统也可对其它采用 SDK 方式进行接入的应用系统提供授权支持。

#### 5.5 电子健康卡管理系统

电子健康卡应用管理系统是居民健康卡虚拟化的核心系统，具有虚拟化账户管理、二维码管理、密码服务等功能，并对外部接入的机构和终端进行管理。虚拟化应用管理系统中按照主索引生成方案生成主索引 ID。虚拟化应用管理系统与注册管理系统连接，保证电子健康卡数据与实体卡数据同步；没有市级或省级注册管理系统的，虚拟化应用管理系统应与国家注册管理系统连接。

#### 5.6 医疗卫生机构

##### 5.6.1 机构终端

医疗卫生机构部署机构终端用于申请二维码。机构终端可包括自助终端、挂号窗口终端等多种形式。

##### 5.6.2 识读终端

医疗卫生机构可通过识读终端识读用户提供二维码，并将二维码信息传输至居民健康卡虚拟化应用管理系统，用于识别用户身份。

### 5.6.3 个人终端

个人终端（如手机等移动设备）运行的电子健康卡 APP 接入居民健康卡虚拟化应用管理系统。电子健康卡 APP 可注册电子健康卡账户，申请电子健康卡二维码，并可管理与居民健康卡绑定的各医院就诊卡账户，查询居民在各医院的就诊信息。

## 5.7 金融交易机构

金融交易机构可接入应用管理系统，通过支付数据与电子健康卡二维码数据结合，实现二码合一。二码合一方案需要电子健康卡用户绑定支付服务方的账户（如银行卡账户），虚拟化应用管理系统根据用户绑定的账户向支付服务提供方申请支付数据。金融交易机构也可直接与医疗卫生机构建立支付结算通道。

## 5.8 医保中心

医保中心与医疗卫生机构连接，可以进行信息共享并提供医保结算服务。

# 6 技术要求

电子健康卡管理系统、电子健康卡SDK授权管理系统、电子健康卡识读终端、电子健康卡密码机是电子健康卡推广应用中的通用型产品。电子健康卡技术规范规定了电子健康卡相关产品的技术实现要求，为电子健康卡的系统开发和集成做出相应的指导，电子健康卡相关产品应满足技术要求，以便实现电子健康卡的产品通用性。

《电子健康卡技术规范 第2部分：管理系统》提出了电子健康卡管理系统功能、性能、安全性各方面要求。系统功能要求是支撑电子健康卡从用户注册到身份识别全生命周期的基础；性能要求是适应电子健康卡大规模应用的必备条件；安全性要求是电子健康卡稳定运行的重要保障。

《电子健康卡技术规范 第3部分：识读终端》提出了电子健康卡识读终端外观和结构、识读性能、电源适应能力、环境适应性各方面的技术要求。识读性能是识读终端的核心指标，良好的识读性能对提升电子健康卡的用户体验有重要意义。

《电子健康卡技术规范 第4部分：密码机》提出了电子健康卡密码机外观和结构、功能、接口、通讯方式、电源适应性、气候环境条件等方面的要求。接口要求是电子健康卡密码机的核心指标，规定了电子健康卡应用过程中主索引ID、电子健康卡ID、有效性信息等关键要素的生成方式，是实现电子健康卡密码服务标准化的基础。

## 7 检测要求

电子健康卡检测规范制定了电子健康卡管理系统、电子健康卡SDK授权管理系统、识读终端、密码机以及接入到电子健康卡管理系统的APP、电子健康卡管理系统联网部署环境相应的检测方法，用于对电子健康卡建设过程中的产品和设施进行检测。

为保证电子健康卡技术的应用能够满足功能和安全需求，电子健康卡管理系统、电子健康卡SDK授权管理系统、识读终端、密码机应在上线前通过第三方检测机构检测；并在发生较大版本变更时通过第三方检测机构检测。电子健康卡APP应在接入电子健康卡管理系统前通过第三方检测机构检测。

第三方检测机构应当获得中国合格评定国家认可委员会（CNAS）的认可，具有信息安全风险评估服务资质和信息安全等级保护测评资质，并具备电子健康卡技术相关要求的安全检测能力。第三方检测机构应根据居民健康卡技术安全检测的程序、标准提供安全检测服务。

电子健康卡管理系统、电子健康卡SDK授权管理系统、识读终端、密码机、电子健康卡APP未按照技术标准和安全要求进行技术安全检测，或技术安全检测的程序、方法存在重大缺陷的，应重新进行检测。