

居民健康卡技术规范  
第 1 部分：总则

Residents' health card technical specifications——

Part 1: General specification

2017 - 07 - 25 发布

2017 - 12 - 01 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

本标准按照GB/T1.1—2009给出的规则起草。

WS/T 543 《居民健康卡技术规范》分为6个部分：

- 第1部分：总则；
- 第2部分：用户卡技术规范；
- 第3部分：用户卡应用规范；
- 第4部分：用户卡命令集；
- 第5部分：终端技术规范；
- 第6部分：用户卡及终端产品检测规范；

本部分为WS/T 543的第1部分。

本部分起草单位：国家卫生计生委统计信息中心、辽宁省卫生计生委信息中心、河南省卫生计生委统计信息中心、佛山市卫生和计划生育局、内蒙古自治区卫生计生委信息中心、中国人民解放军第四军医大学。

本部分主要起草人：孟群、胡建平、郝惠英、杨佐森、王永峰、杨博、王成亮、徐勇勇、边红丽、李岳峰。

# 居民健康卡技术规范 第1部分：总则

## 1 范围

WS/T543的本部分规定了全国统一的居民健康卡、终端、安全机制、产品检测的基本概念及要求。

本部分适用于制作、发行、使用居民健康卡的卫生计生行政管理部门、医疗卫生机构、第三方联合发卡机构和生产企业。

## 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

GM/T 0003 SM2椭圆曲线公钥密码算法

GM/T 0004 SM3密码杂凑算法

WS/T 543.6 居民健康卡技术规范 第6部分：用户卡及终端产品检测规范

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**居民健康卡** residents' health card

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，实现跨地区和跨机构就医、数据交换和费用结算的信息介质，满足健康信息存储的基础载体，计算机可识别的CPU卡。

### 3.2

**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。

### 3.3

**芯片** chip

用于完成数据处理和存储功能的集成电路器件。

### 3.4

**芯片操作系统** chip operating system; COS

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。

### 3.5

**加密算法** cryptographic algorithm

为了隐藏或显现数据信息内容的变换算法。

3.6

**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，反之也成立。即在大多数算法中加/解密密钥是相同的。

3.7

**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。

3.8

**密钥** key

加密转换中控制操作的符号序列。

3.9

**终端** terminal

用于对居民健康卡进行读写操作的设备。

## 4 居民健康卡概述

居民健康卡包含身份识别、基础健康信息存储、跨机构跨地区诊疗、费用结算等应用。

## 5 用户卡

在WS/T 543的各部分中用户卡即为居民健康卡，卡号采用居民身份证号码（见GB 11643）。

## 6 安全机制

居民健康卡安全机制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。通过加载国密算法的安全存取模块（SAM）卡，实现用户卡使用过程中的安全认证。

居民健康卡采用全国统一、两级管理的三级密钥体系，实现居民健康卡跨地区使用。

## 7 产品检测

居民健康卡芯片、芯片操作系统（COS）、成卡及终端等产品应通过权威检测机构的检测。产品检测技术要求见 WS/T 543.6。