《电子健康卡建设指导方案》材料四

**电子健康卡API授权管理系统技术指引**

**（1.3版）**

**国家卫生计生委统计信息中心**

**2018年7月**

# 目录

[目录 1](#_Toc520731122)

[1 概述 2](#_Toc520731123)

[1.1 项目背景 2](#_Toc520731124)

[1.2 建设目标 2](#_Toc520731125)

[2 需求分析 2](#_Toc520731126)

[2.1 业务需求分析 2](#_Toc520731127)

[2.2 系统需求分析 3](#_Toc520731128)

[3 API授权管理系统详细设计 3](#_Toc520731129)

[3.1 系统架构 3](#_Toc520731130)

[3.2 省级API授权管理系统功能模块设计 5](#_Toc520731131)

[3.3 数据库设计 8](#_Toc520731132)

[4 系统设备与部署 12](#_Toc520731133)

[4.1 国家级API授权密钥管理系统设备与部署 12](#_Toc520731134)

[4.2 省级API授权管理系统设备与部署 13](#_Toc520731135)

[4.3 授权认证模块部署 13](#_Toc520731136)

[4.4 APP后台认证服务器部署 13](#_Toc520731137)

[5 系统安全性设计 13](#_Toc520731138)

[6 接口规则 14](#_Toc520731139)

[6.1 协议规则 14](#_Toc520731142)

[6.2 签名生成流程 14](#_Toc520731143)

[7 调用CLA签名认证服务器的方法请参考《CLA安全应用服务端（Java）接口发行包》。API 接口定义 16](#_Toc520731144)

[7.1 注册电子健康卡 16](#_Toc520731146)

[7.2 修改电子健康卡信息 18](#_Toc520731147)

[7.3 查询电子健康卡信息 19](#_Toc520731148)

[7.4 获取电子健康卡二维码 20](#_Toc520731149)

[7.5 验证电子健康卡二维码 22](#_Toc520731150)

[附录A（规范性附录）字典说明 24](#_Toc520731151)

[A.1 接口名称(method)字典 24](#_Toc520731152)

[A.2 证件类型(id\_type)字典 24](#_Toc520731153)

[A.3 用户性别(gender)字典 24](#_Toc520731154)

[附录B（规范性附录）加密规则 25](#_Toc520731155)

[B.1请求报文加密 25](#_Toc520731156)

[B.2返回报文解密 26](#_Toc520731157)

电子健康卡API授权管理系统技术指引

# 概述

## 项目背景

为了落实“十三五规划”和《健康中国2030规划纲要》，国家卫健委于2016年开始大力推动“三个一工程”的建设，特别是电子健康卡的推广与应用为实现公共医疗卫生服务的便民惠民利民提供了有效的手段。

目前，电子健康卡已在多个省市落地应用，国家卫健委已组织第三方机构对“电子健康卡管理系统”和相应的密码设备、密钥灌装进行了严格的安全检查与检测，以确保系统安全。但随着越来越多样化的接入手段的介入，也必须对接入设备、接入APP进行有效管控，只允许合法设备和APP的接入，以确保电子健康卡管理系统的可靠运行。

本指引旨在对接入方通过API接入电子健康卡管理系统的情况进行授权管理，只有被授权的接入方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。

## 建设目标

通过建设电子健康卡API授权管理系统，实现以下功能：

1、注册并发布合法的API接口；

2、对所有通过API接入电子健康卡的APP开发商进行注册和管理；

3、对已审批的开发商，授权其开发的APP使用API；

4、对APP开发商提供授权密钥和授权码文件下载。

# 需求分析

## 业务需求分析

电子健康卡管理系统应为所有接入该系统的APP提供相应的接口，该接口为APP提供用户注册、电子健康卡二维码申请、二维码验证、用户信息查询、用户注销等功能。

根据对目前APP应用开发技术的研究与分析对比，电子健康卡管理系统所提供的API应满足原生APP（本地调用）和H5或微信公众号（远程调用）两种方式。原生APP方式需要嵌入电子卡管系统提供的函数库（SDK）以及API授权管理系统提供的本地权限验证函数。H5或微信公众号方式智能终端（手机）通过页面方式调用APP后台，APP后台通过API接口访问电子健康卡管理系统。

电子健康卡API授权管理系统需要对上述两种调用方式进行授权，电子健康卡管理系统需要针对上述不同方式进行权限验证控制，以达到授权+访问控制的目的。

## 系统需求分析

电子健康卡API授权管理系统作为电子健康卡管理系统的组成部分应与电子健康卡管理系统一起部署，用于对该体系中的所有APP进行统一授权和访问控制。

1、需要对电子健康卡管理系统提供的API进行注册管理；

2、需要所有通过API接入电子健康卡管理系统的开发商进行注册管理；

3、系统管理员负责系统管理，企业用户自行注册并由系统管理员进行审核；

4、电子健康卡API授权管理系统应具备完善的日志管理及备份恢复机制。

# API授权管理系统详细设计

## 系统架构

API授权管理系统采取分布式部署，在国家级建设国家API授权密钥管理系统，各省建设省级API授权管理系统，各地电子健康卡管理中心部署授权认证模块，各地APP后台（包括H5、公众号）部署无证书认证服务器。总体结构图如下：



其中国家API授权密钥管理系统负责为省级API授权管理系统、APP后台的认证服务器发放基于SM2的无证书公私钥对，这些公私钥对使用省级授权系统和APP的标识生成，代表其身份执行授权签发以及身份认证过程中的签名。国家API授权密钥管理系统采用国密型号产品建设，包括《基于SM2的无证书密钥管理系统》和《基于SM2的无证书认证系统》。

省级API授权管理系统为API签发授权信息，并为本省卡管中心的授权信息及状态提供下载接口，包括卡管中心下载API生成密钥和授权认证模块下载API授权状态。API生成密钥可以派生各个API的具体密钥，API授权状态可以屏蔽已被注销的API访问卡管系统。

APP后台的认证服务器负责连接卡管系统的身份认证，没有签名的APP后台数据不能访问卡管系统。

省级API授权管理系统逻辑结构图如下：



系统模块包括：用户管理、管理员管理、API管理、APP授权、系统密钥管理、日志审计、备份恢复、签名认证服务器。

## 省级API授权管理系统功能模块设计

### 管理员管理

#### 管理员类型

超级管理员 -负责系统配置，操作员导入、操作员启用、禁用等功能。

审计管理员 -负责系统操作日志的审计。

操作员 -负责系统管理，如用户管理、APP管理、授权管理等功能。

#### 管理员生成方式

超级管理员与审计管理员在系统初始化时导入；

操作员由超级管理员导入。

#### 审计日志

管理员的操作若涉及数据变更，会生成审计日志，并自动使用管理员密钥对审计日志签名。

### 用户管理

#### 用户类型

系统管理员，企业用户（APP应用开发商）。

#### 用户注册

系统管理员在系统初始化时生成并导入。

企业用户可登陆电子健康卡API授权管理系统网站在线注册，需要企业提供工商注册相关信息、APP相关信息、API调用信息等，管理员审批通过后进行授权，根据调用方式，为APP生成app\_id、app\_secret或授权码文件。

一个企业可以注册申请多个APP授权。

### API密钥

无论是本地调用还是远程调用均需要系统管理员对API进行注册登记。

在注册登记API时，电子健康卡API授权管理系统将为API生成一个API密钥（api\_secret）,并秘密保存。

### APP授权

对已注册的APP，可用本模块实现APP授权。

#### 基本授权流程

无论是本地调用还是远程调用API均需要进行基本授权。

系统管理员根据企业注册APP信息以及调用API信息，为APP生成特定授权信息app\_id与app\_secret，并秘密保存。其中：

app\_id随机生成，长度不小于16字节；

app\_secret= SM3（app\_id + api\_secret）。

#### 增强授权流程

该授权只针对原生APP本地调用API方式。

系统管理员根据企业注册APP信息以及调用API信息，生成特定授权码文件。该授权码文件的主要内容是对APP信息和API信息等进行基于SM2的数字签名值:

sign=SM2（AppId，App名称，APP签名证书指纹，API名称）。

### API授权验证

#### 基本授权验证

无论是本地调用还是远程调用API均需要进行基本授权验证。

1）授权信息下载

电子健康卡管理系统需要从电子健康卡API授权管理系统秘密下载API密钥，并秘密保存，以供授权验证使用。

2）验证规则：

应用调用API连接电子健康卡管理系统服务接口时，以请求包中的主要参数及app\_secret为原文，调用签名认证服务器生成数字签名，数字签名生成流程请参考6.2；

应用将请求包及数字签名提交给电子健康卡管理系统；

电子健康卡管理系统收到请求包，将其转发给API授权认证子系统，验证该请求是否有效。

API授权认证接口请参考《API授权认证服务器-授权认证接口设计说明.docx》。

#### 增强验证流程

对原生APP调用API除完成上述基本验证流程外，还需要完成下述增强验证流程。

**APP嵌入授权验证函数库**

由电子健康卡API授权管理系统提供统一的API授权增强验证函数库，API开发方必须嵌入增强验证函数库，并在APP调用API的第一时间执行验证函数Veriry(“API注册名”)，以确保该SDK得到API有效保护。

**下载API及授权码文件**

APP应用开发商登录到电子健康卡API授权管理系统，申请APP授权并下载相应的API及配套的授权码文件，根据不同系统平台把授权码文件安装到相应的目录下，由验证函数自行读取授权码文件。

**验证规则**

当APP启动运行API时，由API调用增强验证函数Veriry(“API注册名”)，验证函数自行获取APP信息，再加上“API注册名”信息，组合出待签名文件，然后验证函数读取授权码文件取出与API对应的授权码（签名值sign），调用SM2算法验证该数字签名， 如果验签通过则继续，否则终止程序运行。

### 日志审计

管理员操作涉及数据变化，将自动记录审计日志，日志中包含管理员签名；

审计管理员可查询、统计、审计日志。

### 备份与恢复

系统根据安全备份策略定期对系统中的核心数据（包括企业注册信息、API密钥、APP授权信息等）进行全备份或增量备份，防止系统故障而导致的数据损失。

系统管理员可人工对已备份的数据进行恢复，以对历史数据进行查询或统计。

### 签名认证服务器

签名认证服务器提供符合国家标准的密码服务，如身份认证、数字签名验签、数据加解密等，本系统中用于对管理员进行强身份认证，并对API授权码进行数字签名等服务。

## 数据库设计

### 管理员表

|  |  |  |  |
| --- | --- | --- | --- |
| **表名：ADMIN** | | | |
| **列名** | **类型** | **约束** | **描述** |
| ID | INT | 主键 | 主键，由主键产生器产生 |
| ADMIN\_ID | VARCHAR(100) | 非空 | 管理员ID，唯一 |
| ADMIN\_NAME | VARCHAR(200) | 非空 | 管理员名称 |
| TYPE | INT | 非空 | 管理员权限：  100 - 超级管理员  30 - 操作员  20 - 审计员 |
| NOT\_BF | CHAR(6) | 非空 | 密钥生效日期 |
| NOT\_AF | CHAR(6) | 非空 | 密钥失效日期 |
| STATUS | INT | 非空 | 状态，用于逻辑删除  0 – 正常  1 – 删除 |
| DEVS\_CODE | VARCHAR(40) | 非空 | 设备号 |
| SPID | CHAR(16) | 非空 | 签名公钥短标识 |
| IDPID2 | VARCHAR(500) | 非空 | 签名公钥标识 |
| TIME | TIMESTAMP | 非空 | 操作时间 |

### 用户表

|  |  |  |  |
| --- | --- | --- | --- |
| **表名：USER** | | | |
| **列名** | **类型** | **约束** | **描述** |
| ID | INTEGER | 主键 | 主键，由主键产生器产生 |
| USER\_ID | VARCHAR(100) | 非空 | 用户ID |
| USER\_NAME | VARCHAR(100) | 非空 | 用户名称 |
| TYPE | INTEGER | 非空 | 用户类型：  0 - 企业  1 - 个人 |
| PASS | VARCHAR(200) | 非空 | 密码 |
| ADDR | VARCHAR(100) |  | 地址 |
| CONTACTS | VARCHAR(100) |  | 联系人 |
| TEL | VARCHAR(20) |  | 联系方式 |
| EMAIL | VARCHAR(50) |  | 邮件地址 |
| STATUS | INTEGER | 非空 | 审批状态：  0 - 未审批  1 - 审批通过  2 - 审批不通过  审批通过-后面项不为空 |
| TIME | TIMESTAMP | 非空 | 操作时间 |
| DESCRIPTION | VARCHAR(100) |  | 审批未通过的理由 |

### API表

|  |  |  |  |
| --- | --- | --- | --- |
| **表名：SDK** | | | |
| **列名** | **类型** | **约束** | **描述** |
| ID | INT | 主键 | 主键，由主键产生器产生 |
| NAME | Varchar(200) | 非空 | API名称 |
| TYPE | INTEGER | 非空 | API类型  1 - 本地调用类  2 - 连接服务类 |
| KEY\_ | VARCHAR(400) |  | API密钥（TYPE为2时有效）  用于生成CilentSecret  使用数字信封加密保护 |
| STATUS | INT | 非空 | 状态，用于逻辑删除  0 – 正常  1 – 删除 |
| TIME | TIMESTAMP | 非空 | 操作时间 |

### 授权表

|  |  |  |  |
| --- | --- | --- | --- |
| **表名：GRANTING** | | | |
| **列名** | **类型** | **约束** | **描述** |
| ID | INT | 主键 | 主键，由主键产生器产生 |
| USER\_ID | VARCHAR(50) | 非空 | 用户ID，外键，指向用户表 |
| API\_ID | INTEGER | 非空 | 授权的API的ID |
| API\_NAME | VARCHAR(100) | 非空 | 授权的API名称 |
| APP\_LABLE | VARCHAR(50) | 非空 | 应用名称 |
| APP\_ID | VARCHAR(30) |  | 应用ID，唯一 |
| APP\_ENV | VARCHAR(100) |  | 开发环境 |
| APP\_SHA1 | VARCHAR(100) |  | 发布版SHA1 |
| APP\_PACKAGE | VARCHAR(100) |  | 包名 |
| APP\_VERSION | VARCHAR(50) |  | 内置版本 |
| APP\_RANGE | VARCHAR(200) |  | 应用范围 |
| DEVELOPER | VARCHAR(20) |  | 开发者姓名 |
| STATUS | INTEGER | 非空 | 审批状态：  0 - 未审批  1 - 审批通过  2 - 审批不通过 |
| AUTH\_CODE | VARCHAR(100) |  | 授权码  （适用与本地调用类API） |
| CLIENT\_ID | VARCHAR(100) |  | 客户端ID  （适用于连接服务类API） |
| CLIENT\_SECRET | VARCHAR(100) |  | 客户端SECRET  （适用于连接服务类API） |
| ADMIN\_ID | VARCHAR(100) |  | 管理员ID，外键，指向管理员表 |
| SIGNATURE | VARCHAR(200) |  | 数字签名 |
| APPLY\_TIME | TIMESTAMP |  | 申请时间 |
| GRANT\_TIME | TIMESTAMP |  | 审核时间 |
| STATE | INTEGER |  | 逻辑删除  0 - 正常  1 - 删除 |
| DESCRIPTION | VARCHAR(100) |  | 描述（通常为审批未通过的原因） |

### 审计表

|  |  |  |  |
| --- | --- | --- | --- |
| **表名：AUDIT\_LOG** | | | |
| **列名** | **类型** | **约束** | **描述** |
| ID | INTEGER | 主键 | 主键，由主键产生器产生 |
| TIME | TIMESTAMP | 非空 | 操作时间 |
| TYPE | VARCHAR(100) | 非空 | 操作类型：  101 - 用户注册审批  102 - 用户删除  201 - 管理员添加  202 - 管理员删除  301 - API添加  302 - API删除  303 - API修改 |
| RESULT | VARCHAR(100) | 非空 | 操作结果  等于0 - 成功  大于0 - 失败 |
| PLAIN/SM4CRIPTION | VARCHAR(200) | 非空 | 操作结果描述 |
| ADMIN\_ID | VARCHAR(100) | 非空 | 管理员ID |
| ADMIN\_NAME | VARCHAR(100) | 非空 | 管理员名称 |
| ADMIN\_SPID | VARCHAR(100) | 非空 | 管理员公钥短标识 |
| OPERATE\_CONTENT | VARCHAR(200) | 非空 | 操作内容(可用ORIGINAL代替) |
| ORIGINAL | VARCHAR(500) | 非空 | 签名原文 |
| SIGNATURE | VARCHAR(500) | 非空 | 管理员签名 |
| AUDIT\_STATUS | INTEGER | 非空 | 审计状态 |
| AUDIT\_TIME | TIMESTAMP |  | 审计时间 |
| AUDITOR\_ID | INTEGER |  | 审计员id |
| AUDITOR\_NAME | VARCHAR(50) |  | 审计员名称 |

### 配置表

|  |  |  |  |
| --- | --- | --- | --- |
| **表名：CONFIG** | | | |
| **列名** | **类型** | **约束** | **描述** |
| NAME | VARCHAR(100) | 非空 | 配置名称 |
| VALUE | VARCHAR(1000) | 非空 | 配置值 |
| SORT | INTEGER | 非空 | 排序值 |
| EDITABLE | INTEGER | 非空 | 是否可编辑  0 - 不可编辑  1 - 可编辑 |
| VISIABLE | INTEGER | 非空 | 是否可见  0 - 不可见  1 - 可见 |
| DESCRIPTION | VARCHAR(200) | 非空 | 描述 |

# 系统设备与部署

## 国家级API授权密钥管理系统设备与部署

国家级API授权密钥管理系统包括KGS、KSS、KRS、KDS模块，拟用一台PC服务器、一台密码机、一台PC机来支撑。密码机和服务器可部署在有防护设备的机房内，PC机部署在办公室内。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | **设备名称** | **用途及性能指标** | **数量** |
| 1 | PC服务器 | 安装国家级API授权密钥管理系统、数据库系统，Intel Xeon E5系列 CPU\*2 ，内存32G ，硬盘SAS 300GB \*5 支持raid0、1、5，电源冗余双电源,双千兆网卡\*2、光驱、带Linux操作系统， | 1 |
| 2 | 密码机 | 生成密钥、支持PKCS#1/#7格式数字签名、验证签名、PKCS#7格式数字信封加解密等 | 1 |
| 3 | PC机 | 带USB接口通用PC机，用于系统操作、管理 | 1 |

## 省级API授权管理系统设备与部署

省级API授权管理系统主要设备包括授权管理服务器、签名认证服务器、PC管理终端、交换机等，系统部署在省电子健康卡管理系统安全区域内，可利用原有系统防护设备。省级API授权管理系统设备列表如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | **设备名称** | **用途及性能指标** | **数量** |
| 1 | 授权管理系统 | 用户注册、API密钥生成、API授权等核心管理功能 | 1 |
| 2 | 签名认证服务器 | 生成密钥、授权文件签名，支持PKCS#1/#7格式数字签名、验证签名、PKCS#7格式数字信封加解密等 | 2 |
| 3 | PC服务器 | 安装API授权管理系统、数据库系统，Intel Xeon E5系列 CPU\*2 ，内存32G ，硬盘SAS 300GB \*5 支持raid0、1、5，电源冗余双电源,双千兆网卡\*2、光驱、带Linux操作系统， | 1 |
| 4 | 交换机 | 内部连接设备，千兆以太网交换机， | 1 |
| 5 | 管理控制台 | API授权管理系统管理终端，主流配置PC机 | 1 |

## 授权认证模块部署

授权认证模块可以安装在各个卡管系统中，为卡管系统提供认证服务。

## APP后台认证服务器部署

APP后台独立部署认证服务器，过网络接口方式为APP后台提供服务，与APP后台部署在同地。

# 系统安全性设计

电子健康卡API授权管理系统的安全性涉及密码算法安全、通信协议安全，密码应用安全，密钥管理安全，网络安全，主机系统安全，系统可靠性，身份认证技术，访问控制技术，安全审计，系统安全以及安全管理等方面。

系统中的密码算法皆为国密算法。

通过采取国密型号的硬件密码设备、密钥管理安全协议、密钥存取访问控制、密钥管理操作审计等多种安全措施，保障电子健康卡API授权管理系统中所使用的密钥，在其整个生命周期中的安全。

通过部署在电子健康卡管理系统安全区域内，保障网络、主机系统、应用系统及数据库运行的安全。

通过磁盘镜像与存储备份对重要数据进行备份，保证电子健康卡API授权管理系统的关键业务数据和签名认证服务器密钥在发生灾难性破坏时，系统能够及时和尽可能完整的恢复被破坏的数据。

在管理方面，设置多层管理人员，完善的管理制度，分权制衡管理机制和有效的应急响应系统。

综上所述，电子健康卡API授权管理系统的安全性设计具有设置完整、技术先进、措施有效、管理严密、遵循规范等特性。通过这些安全防护技术能够保障整个电子健康卡API授权管理系统安全、稳定、高效地运行。

# 接口规则



## 协议规则

|  |  |
| --- | --- |
| **调用方式** | HTTPS |
| **提交方式** | POST |
| **数据格式** | 提交和返回数据均为JSON格式 |
| **字符编码** | 统一采用UTF-8字符编码 |
| **判断逻辑** | 先判断协议字段返回，再判断业务返回，最后判断交易状态 |
| **签名算法** | SM2 |

## 签名生成流程

#### 生成签名原文

签名原文的生成规则为：

data+app\_secret

其中data是请求包，app\_secret是授权管理系统为应用生成的密钥，“+”为字符串直接拼接。

示例：

|  |
| --- |
| **data={**  **"app\_id"**: "<你的应用编号>"**,**  **"biz\_content"**: "F404379A66B50640EF1367CCE000F6463BA1D6068A3C5360374B741DFCD7…"**,**  **"enc\_type"**: "SM4"**,**  **"method"**: "ehc.ehealthcode.verify"**,**  **"term\_id"**: "35020010001"**,**  **"timestamp"**: "1512971932368"**,**  **"version"**: "X.M.0.1"  **}**  **app\_secret=**0F6463BA5F0AC09AB1FFA3D10F8C620D |

组成的签名原文为：

|  |
| --- |
| **{**  **"app\_id"**: "<你的应用编号>"**,**  **"biz\_content"**: "F404379A66B50640EF1367CCE000F6463BA1D6068A3C5360374B741DFCD7…"**,**  **"enc\_type"**: "SM4"**,**  **"method"**: "ehc.ehealthcode.verify"**,**  **"term\_id"**: "35020010001"**,**  **"timestamp"**: "1512971932368"**,**  **"version"**: "X.M.0.1"  **}**  0F6463BA5F0AC09AB1FFA3D10F8C620D |

#### 生成签名

可调用CLA签名认证服务器，对上面得到的原文制作签名，再将字节码转换成16进制字符串，并对转换后的字符串转换成大写。

如：C96986F508F51555BC7B22E45792D4C382709620B589723BA422AF787EAF72。

# 调用CLA签名认证服务器的方法请参考《CLA安全应用服务端（Java）接口发行包》。API 接口定义



## 注册电子健康卡



### 接口功能

用户通过线下刷身份证、社保卡，通过实名认证后在电子健康卡管理平台开户。

### 请求参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | **参数说明** | **样例** |
| 公共请求参数 | | | | | |
| method | 接口名称 | String(50) | N |  | ehc.ehealthcard.register |
| app\_id | 应用编号 | String(32) | N |  |  |
| term\_id | 终端编号 | String(32) | N |  |  |
| version | 接口版本号 | String(10) | N |  |  |
| timestamp | 请求时间戳 | String(20) | N |  |  |
| digest\_type | 摘要类型 | String(10) | N |  | SM3 |
| digest | 摘要值 | String(256) | N |  |  |
| enc\_type | 加密类型 | String(10) | N |  | PLAIN/SM4 |
| biz\_content | 请求参数集合 | String(-) | N | 请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>> |  |
| <<接口请求参数>> | | | | | |
| register\_no | 外部注册流水号 | String(32) | N |  |  |
| register\_time | 外部注册时间 | String(32) | N |  |  |
| apply\_type | 申请方式 | String(1) |  |  |  |
| id\_type | 证件类型 | String(2) | N | 见字典 |  |
| id\_no | 证件号 | String(32) | N |  |  |
| name | 用户姓名 | String(50) | N |  |  |
| gender | 用户性别 | String(1) | N |  |  |
| birthday | 出生日期 | String(10) | Y |  | yyyyMMdd |
| cellphone | 手机号码 | String(32) | Y |  |  |
| telephone | 联系电话 | String(32) | Y |  |  |
| address | 居住地址 | String(200) | Y |  |  |
| unit | 工作单位 | String(100) | Y |  |  |

### 响应参数

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | | **参数说明** | **样例** |
| 公共响应参数 | | | | | | |
| code | 返回结果码 | String(10) | N | |  | 0000 |
| message | 返回结果说明 | String(200) | N | |  | 操作成功 |
| method | 接口名称 | String(50) | N | | 与请求报文一致 |  |
| app\_id | 应用编号 | String(20) | N | | 与请求报文一致 |  |
| version | 接口版本号 | String(10) | N | | 与请求报文一致 |  |
| timestamp | 响应报文时间戳 | String(20) | N | |  |  |
| digest\_type | 摘要类型 | String(10) | N | |  | SM3 |
| digest | 摘要值 | String(256) | N | |  |  |
| enc\_type | 加密类型 | String(10) | | Y |  | PLAIN/SM4 |
| biz\_content | 响应参数集合 | String(-) | | Y | 响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>> |  |
| <<接口响应参数>> | | | | | | |
| ehealth\_card\_id | 电子健康卡ID | String(128) | N | |  |  |
| mindex\_id | 居民健康卡主索引ID | String(128) | N | |  |  |
| health\_card\_no | 居民健康卡卡号 | String(32) | N | |  |  |
| xman\_id | 市民健康系统ID | String(32) | Y | |  |  |
| id\_type | 证件类型 | String(2) | N | |  |  |
| id\_no | 证件号 | String(32) | N | |  |  |
| name | 用户姓名 | String(50) | N | |  |  |
| card\_type | 卡类型 | String(2) | Y | | 默认关联卡类型  01社保卡  02市民健康正式卡  03市民健康临时卡  04市民卡（经信局）  05居民健康卡 |  |
| card\_no | 就诊卡号 | String(32) | Y | | 默认关联卡号 |  |
| card\_list | 绑定卡列表 | JSON | | Y |  | [  {  “card\_type”:”01”,  “card\_no”:”D635128”  },  {  “card\_type”:”02”,  “card\_no”:”D635128”  }  ] |

## 修改电子健康卡信息



### 接口功能

修改电子健康卡用户个人信息。

### 请求参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | **参数说明** | **样例** |
| 公共请求参数 | | | | | |
| method | 接口名称 | String(50) | N |  | ehc.ehealthcard.alterinfo |
| app\_id | 应用编号 | String(32) | N |  |  |
| term\_id | 终端编号 | String(32) | N |  |  |
| version | 接口版本号 | String(10) | N |  |  |
| timestamp | 请求时间戳 | String(20) | N |  |  |
| digest\_type | 摘要类型 | String(10) | N |  | SM3 |
| digest | 摘要值 | String(256) | N |  |  |
| enc\_type | 加密类型 | String(10) | N |  | PLAIN/SM4 |
| biz\_content | 请求参数集合 | String(-) | N | 请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>> |  |
| <<接口请求参数>> | | | | | |
| ehealth\_card\_id | 电子健康卡ID | String(128) | N |  |  |
| gender | 变更性别 | String(32) | Y |  |  |
| birthday | 出生日期 | String(10) | Y |  |  |
| cellphone | 变更手机号 | String(20) | Y |  |  |
| telephone | 联系电话 | String(32) | Y |  |  |
| address | 居住地址 | String(200) | Y |  |  |
| unit | 工作单位 | String(100) | Y |  |  |
| alter\_no | 外部变更流水号 | String(32) | N |  |  |
| alter\_time | 外部变更时间 | String(32) | N |  |  |

### 响应参数

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | | **参数说明** | **样例** |
| 公共响应参数 | | | | | | |
| code | 返回结果码 | String(10) | N | |  | 0000 |
| message | 返回结果说明 | String(200) | N | |  | 操作成功 |
| app\_id | 应用编号 | String(20) | N | | 与请求报文一致 |  |
| method | 接口名称 | String(50) | N | | 与请求报文一致 |  |
| version | 接口版本号 | String(10) | N | | 与请求报文一致 |  |
| timestamp | 响应报文时间戳 | String(20) | N | |  |  |
| digest\_type | 摘要类型 | String(10) | N | |  | SM3 |
| digest | 摘要值 | String(256) | N | |  |  |
| enc\_type | 加密类型 | String(10) | | Y |  | PLAIN/SM4 |
| biz\_content | 响应参数集合 | String(-) | | Y | 响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>> |  |
| <<接口响应参数>> | | | | | | |
| ehealth\_card\_id | 电子健康卡ID | String(128) | N | |  |  |
| mindex\_id | 居民健康卡主索引ID | String(128) | N | |  |  |
| out\_alter\_no | 外部变更流水号 | String(32) | N | |  |  |
| alter\_no | 平台变更流水号 | String(32) | N | |  |  |

## 查询电子健康卡信息



### 接口功能

根据电子健康卡ID等信息查询电子健康卡信息。

### 请求参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | **参数说明** | **样例** |
| 公共请求参数 | | | | | |
| method | 接口名称 | String(50) | N |  | ehc.ehealthcode.verify |
| app\_id | 应用编号 | String(32) | N |  |  |
| term\_id | 终端编号 | String(32) | N |  |  |
| version | 接口版本号 | String(10) | N |  |  |
| timestamp | 请求时间戳 | String(20) | N |  |  |
| digest\_type | 摘要类型 | String(10) | N |  | SM3 |
| digest | 摘要值 | String(256) | N |  |  |
| enc\_type | 加密类型 | String(10) | N |  | PLAIN/SM4 |
| biz\_content | 请求参数集合 | String(-) | N | 请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>> |  |
| <<接口请求参数>> | | | | | |
| ehealth\_card\_id | 电子健康卡ID | String(128) | N | 可根据电子健康卡ID或证件信息组合查询 |  |
| id\_type | 证件类型 | String(2) | N  N |  |
| id\_no | 证件号 | String(32) |  |

### 响应参数

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | | **参数说明** | **样例** |
| 公共响应参数 | | | | | | |
| code | 返回结果码 | String(10) | N | |  | 0000 |
| message | 返回结果说明 | String(200) | N | |  | 操作成功 |
| method | 接口名称 | String(50) | N | | 与请求报文一致 |  |
| app\_id | 应用编号 | String(20) | N | | 与请求报文一致 |  |
| version | 接口版本号 | String(10) | N | | 与请求报文一致 |  |
| timestamp | 响应报文时间戳 | String(20) | N | |  |  |
| digest\_type | 摘要类型 | String(10) | N | |  | SM3 |
| digest | 摘要值 | String(256) | N | |  |  |
| enc\_type | 加密类型 | String(10) | | Y |  | PLAIN/SM4 |
| biz\_content | 响应参数集合 | String(-) | | Y | 响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>> |  |
| <<接口响应参数>> | | | | | | |
| ehealth\_card\_id | 电子健康卡ID | String(128) | N | |  |  |
| mindex\_id | 居民健康卡  主索引ID | String(128) | N | |  |  |
| id\_type | 证件类型 | String(2) | N | | 见字典 |  |
| id\_no | 证件号 | String(32) | N | |  |  |
| name | 用户姓名 | String(50) | N | |  |  |
| gender | 用户性别 | String(1) | N | |  |  |
| birthday | 出生日期 | String(10) | Y | |  |  |
| cellphone | 手机号码 | String(32) | N | |  |  |
| telephone | 联系电话 | String(32) | Y | |  |  |
| address | 居住地址 | String(200) | Y | |  |  |
| unit | 工作单位 | String(100) | Y | |  |  |

## 获取电子健康卡二维码



### 接口功能

根据电子健康卡ID申请电子健康卡二维码。

### 请求参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | **参数说明** | **样例** |
| 公共请求参数 | | | | | |
| method | 接口名称 | String(50) | N |  | ehc.ehealthcode.generate |
| app\_id | 应用编号 | String(32) | N |  |  |
| term\_id | 终端编号 | String(32) | N |  |  |
| version | 接口版本号 | String(10) | N |  |  |
| timestamp | 请求时间戳 | String(20) | N |  |  |
| digest\_type | 摘要类型 | String(10) | N |  | SM3 |
| digest | 摘要值 | String(256) | N |  |  |
| enc\_type | 加密类型 | String(10) | N |  | PLAIN/SM4 |
| biz\_content | 请求参数集合 | String(-) | N | 请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>> |  |
| <<接口请求参数>> | | | | | |
| ehealth\_card\_id | 电子健康卡ID | String(128) | N |  |  |
| generate\_no | 外部生成流水 | String(32) | N |  |  |
| generate\_time | 外部生成时间 | String(32) | N |  |  |

### 响应参数

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | | **参数说明** | **样例** |
| 公共响应参数 | | | | | | |
| code | 返回结果码 | String(10) | N | |  | 0000 |
| message | 返回结果说明 | String(200) | N | |  | 操作成功 |
| method | 接口名称 | String(50) | N | | 与请求报文一致 |  |
| app\_id | 应用编号 | String(20) | N | | 与请求报文一致 |  |
| version | 接口版本号 | String(10) | N | | 与请求报文一致 |  |
| timestamp | 响应报文时间戳 | String(20) | N | |  |  |
| digest\_type | 摘要类型 | String(10) | N | |  | SM3 |
| digest | 摘要值 | String(256) | N | |  |  |
| enc\_type | 加密类型 | String(10) | | Y |  | PLAIN/SM4 |
| biz\_content | 响应参数集合 | String(-) | | Y | 响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>> |  |
| <<接口响应参数>> | | | | | | |
| ehealth\_code | 电子健康卡二维码 | String(2) | N | |  |  |

## 验证电子健康卡二维码



### 接口功能

根据电子健康卡二维码数据标准对识读终端上送的二维码进行验证，并返回验证结果。

### 请求参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | **参数说明** | **样例** |
| 公共请求参数 | | | | | |
| method | 接口名称 | String(50) | N |  | ehc.ehealthcode.verify |
| app\_id | 应用编号 | String(32) | N |  |  |
| term\_id | 终端编号 | String(32) | N |  |  |
| version | 接口版本号 | String(10) | N |  |  |
| timestamp | 请求时间戳 | String(20) | N |  |  |
| digest\_type | 摘要类型 | String(10) | N |  | SM3 |
| digest | 摘要值 | String(256) | N |  |  |
| enc\_type | 加密类型 | String(10) | N |  | PLAIN/SM4 |
| biz\_content | 请求参数集合 | String(-) | N | 请求参数的集合，最大长度不限，除公共请求参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口请求参数>> |  |
| <<接口请求参数>> | | | | | |
| ehealth\_code | 二维码数据内容 | String(128) | N |  |  |

### 响应参数

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **参数** | **参数名称** | **类型** | **可空** | | **参数说明** | **样例** |
| 公共响应参数 | | | | | | |
| code | 返回结果码 | String(10) | N | |  | 0000 |
| message | 返回结果说明 | String(200) | N | |  | 操作成功 |
| method | 接口名称 | String(50) | N | | 与请求报文一致 |  |
| app\_id | 应用编号 | String(20) | N | | 与请求报文一致 |  |
| version | 接口版本号 | String(10) | N | | 与请求报文一致 |  |
| timestamp | 响应报文时间戳 | String(20) | N | |  |  |
| digest\_type | 摘要类型 | String(10) | N | |  | SM3 |
| digest | 摘要值 | String(256) | N | |  |  |
| enc\_type | 加密类型 | String(10) | | Y |  | PLAIN/SM4 |
| biz\_content | 响应参数集合 | String(-) | | Y | 响应参数的集合，最大长度不限，除公共响应参数外所有请求参数都必须放在这个参数中传递，具体参照各接口<<接口响应参数>> |  |
| <<接口响应参数>> | | | | | | |
| ehealth\_card\_id | 电子健康卡ID | String(128) | N | |  |  |
| mindex\_id | 居民健康卡  主索引ID | String(128) | N | |  |  |
| id\_type | 证件类型 | String(2) | N | | 见字典 |  |
| id\_no | 证件号 | String(32) | N | |  |  |
| name | 用户姓名 | String(50) | N | |  |  |
| gender | 用户性别 | String(1) | N | |  |  |
| birthday | 出生日期 | String(10) | Y | |  |  |
| cellphone | 手机号码 | String(32) | N | |  |  |
| telephone | 联系电话 | String(32) | Y | |  |  |
| address | 居住地址 | String(200) | Y | |  |  |
| unit | 工作单位 | String(100) | Y | |  |  |

# 附录A（规范性附录）字典说明

## A.1 接口名称(method)字典

|  |  |
| --- | --- |
| **接口名称** | **接口说明** |
| ehc.ehealthcard.register | 注册电子健康卡 |
| ehc.ehealthcard.modify | 修改电子健康卡用户信息 |
| ehc.ehealthcard.query | 查询电子健康卡用户信息 |
| ehc.ehealthcode.apply | 获取电子健康卡二维码 |
| ehc.ehealthcode.verify | 验证电子健康卡二维码 |

## A.2 证件类型(id\_type)字典

|  |  |
| --- | --- |
| **证件代码** | **证件说明** |
| 01 | 居民身份证 |
| 02 | 居民户口簿 |
| 03 | 护照 |
| 04 | 军官证 |
| 05 | 驾驶证 |
| 06 | 港澳居民来往内地通行证 |
| 07 | 台湾居民来往内地通行证 |
| 99 | 其他法定有效证件 |

## A.3 用户性别(gender)字典

|  |  |
| --- | --- |
| **性别代码** | **性别说明** |
| 0 | 未知性别 |
| 1 | 男 |
| 2 | 女 |
| 9 | 未说明性别 |

# 附录B（规范性附录）加密规则

应用接入时如需加密，可参考以下步骤，对请求报文及响应报文加密处理。

## B.1请求报文加密

### B.1.1 组装请求报文

根据API列表定义参数，整理请求报文

|  |
| --- |
| **{**  **"app\_id"**: "1BQA48ETK000A718A8C000001FFAA482"**,**  **"biz\_content"**: "{\"ehealth\_code\":\"F404379A66B50640EF1367CCE000F6463BA5F0AC09AB1FFA3D10F8C6ED2D204F:2:15855D11D6068A3C5360374B741DFCD7\",\"out\_verify\_no\":\"V17093010293789\",\"out\_verify\_time\":\"20171211135852\"}"**,**  **"enc\_type"**: "SM4"**,**  **"method"**: "ehc.ehealthcode.verify"**,**  **"digest"**: "9F9A7E008EF3E19AF4202FEC45FB5FEC"**,**  **"digest\_type"**: "SM3"**,**  **"term\_id"**: "35020010001"**,**  **"timestamp"**: "1512971932368"**,**  **"version"**: "X.M.0.1"  **}** |

### B.1.2 待加密串

取出**biz\_content**明文字段，得到待加密串明文串jStr：{\"ehealth\_code\":\"F404379A66B50640EF1367CCE000F6463BA5F0AC09AB1FFA3D10F8C6ED2D204F:2:15855D11D6068A3C5360374B741DFCD7\",\"out\_verify\_no\":\"V17093010293789\",\"out\_verify\_time\":\"20171211135852\"}

### B.1.3 报文加密密钥

根据**enc\_type**声明加密算法SM4*(SM4算法加密参数见末尾备注)*，使用*app\_secret转16进制，截取前面32位*作为报文加密密钥。

### B.1.4 获取密文

根据**enc\_type**声明加密算法SM4，使用3获得的报文加密密钥，加密jStr十六进制字符串，并将加密结果转16进制，再将16进制串转换为大写，获得加密密文**enc\_data**:

1EBA275881C8E1BBB31E72BB800C625C05F7F6D7A99DD44741E1CEC73828F844D954E1302A382F7A427403FB3638051A78605C57AD7490F7E3E4B87CA9D5925C630561AB3E6C5D68757B774E7B19C9727202628D2EC4532CA8F1B3F4CCC2DA481CEAC13E3B91120F6BE0DE2D6337B30265A1DB126510D657D04458D0083E3955AE57AD4B9ED4B177187BF1B099EB9015C235240E6D2C19CF3D4C0273F3C81154619697CB27CBB4E80859709891ADF368

### B.1.5 设置密文

将加密结果**enc\_data**，赋值替换**biz\_content**明文成密文，将新获取报文发送服务器

*如：String encryptData = SM4Util.encrypt(jStr, newPassword);*

*// 待加密内容 data*

*// 加密密钥 newPassword.substring(0, 16)*

|  |
| --- |
| **{**  **"app\_id"**: "1BQA48ETK000A718A8C000001FFAA482"**,**  **"biz\_content"**: "1EBA275881C8E1BBB31E72BB800C625C05F7F6D7A99DD44741E1CEC73828F844D954E1302A382F7A427403FB3638051A78605C57AD7490F7E3E4B87CA9D5925C630561AB3E6C5D68757B774E7B19C9727202628D2EC4532CA8F1B3F4CCC2DA481CEAC13E3B91120F6BE0DE2D6337B30265A1DB126510D657D04458D0083E3955AE57AD4B9ED4B177187BF1B099EB9015C235240E6D2C19CF3D4C0273F3C81154619697CB27CBB4E80859709891ADF368"**,**  **"enc\_type"**: "SM4"**,**  **"method"**: "ehc.ehealthcode.verify"**,**  **"digest"**: "9F9A7E008EF3E19AF4202FEC45FB5FEC"**,**  **"digest\_type"**: "SM3"**,**  **"term\_id"**: "35020010001"**,**  **"timestamp"**: "1512971932368"**,**  **"version"**: "X.M.0.1"  **}** |

## B.2返回报文解密



### B.2.1 获取响应报文

|  |
| --- |
| **{**  **"app\_id"**: "1BQA48ETK000A718A8C000001FFAA482"**,**  **"biz\_contentenc\_type"**: "SM4"**,**  **"method"**: "ehc.ehealthcode.verify"**,**  **"code"**: "0000"**,**  **"message"**: "交易成功"**,**  **"digest"**: "DE73D039B83F7E8000FA5C9B44453C33"**,**  **"ditest\_type"**: "SM3"**,**  **"timestamp"**: "20171211135848"**,**  **"version"**: "X.M.0.1"  **}** |

### B.2.2 获取加密密文数据encryptData



### B.2.3 报文解密密钥

根据enc\_type声明加密算法，截取app\_secret转16进制，截取32位，即获得报文解密密钥；

### B.2.4 获取明文

根据enc\_type声明加密算法，报文解密密钥，解密enc\_data获取JSON字符串明文jStr：

{\"card\_list\":\"[{\\\"card\_no\\\":\\\"1D00000066\\\",\\\"card\_type\\\":\\\"05\\\"}]\",\"card\_no\":\"1D00000066\",\"card\_type\":\"05\",\"ehealth\_card\_id\":\"F404379A66B50640EF1367CCE000F646BCFF1112239AE539\",\"id\_no\":\"350582199211163057\",\"id\_type\":\"01\",\"mindex\_id\":\"a59d5f25ce9c6e47367cbdd62427204a\",\"cellphone\":\"18959177477\",\"name\":\"许顺义\"}

### B.2.5 设置明文

将jStr转换为JSON赋值param，获取解密后返回报文

|  |
| --- |
| **{**  **"app\_id"**: "1BQA48ETK000A718A8C000001FFAA482"**,**  **"biz\_content"**: "{\"card\_list\":\"[{\\\"card\_no\\\":\\\"1D00000066\\\",\\\"card\_type\\\":\\\"05\\\"}]\",\"card\_no\":\"1D00000066\",\"card\_type\":\"05\",\"ehealth\_card\_id\":\"F404379A66B50640EF1367CCE000F646BCFF1112239AE539\",\"id\_no\":\"350582199211163057\",\"id\_type\":\"01\",\"mindex\_id\":\"a59d5f25ce9c6e47367cbdd62427204a\",\"mobile\_phone\":\"18959177477\",\"user\_name\":\"许顺义\"}"**,**  **"enc\_type"**: "SM4"**,**  **"method"**: "ehc.ehealthcode.verify"**,**  **"code"**: "0000"**,**  **"message"**: "交易成功"**,**  **"digest"**: "DE73D039B83F7E8000FA5C9B44453C33"**,**  **"digest\_type"**: "SM3"**,**  **"timestamp"**: "20171211135848"**,**  **"version"**: "X.M.0.1"  **}** |

备注：SM4 加密使用ECB模式。