XXXXXX

XXXXXXX

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS XXX—2018

# 电子健康卡技术规范 第 2 部分：管理系统

**Technical specification for electronic health card Part2：**

**Management system**

（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 ..... 3
2 规范性引用文件 ..... 3
3 术语和定义 ..... 4
3.1 电子健康卡 ..... 4
3.2 电子健康卡管理系统 ..... 4
3.3 主索引 ID ..... 4
3.4 电子健康卡 ID ..... 4
3.5 电子健康卡二维码 ..... 4
3.6 密码设备 ..... 4
3.7 接入机构 ..... 4
3.8 接入 APP ..... 4
3.9 电子健康卡 SDK 接口 ..... 5
3.10 电子健康卡 SDK 授权管理系统 ..... 5
3.11 识读终端 ..... 5
4 缩略语 ..... 5
5 技术要求 ..... 5
5.1 功能要求 ..... 5
5.1.1 用户管理 ..... 5
5.1.2 机构管理 ..... 7
5.1.3 APP 管理 ..... 7
5.1.4 识读终端管理 ..... 8
5.1.5 二维码使用 ..... 8
5.1.6 密码机管理 ..... 10
5.1.7 外部接口要求 ..... 10
5.2 性能要求 ..... 11
5.3 安全要求 ..... 11
5.3.1 基本要求 ..... 11
5.3.2 应用软件安全 ..... 11
5.4 SDK 接入要求 ..... 13
5.4.1 SDK 授权 ..... 13
5.4.2 SDK 验证 ..... 14
5.4.3 摘要值生成流程 ..... 15
6 检测要求 ..... 16
6.1 功能检测要求 ..... 16
6.2 性能检测要求 ..... 17
6.3 安全检测要求 ..... 17
6.4 SDK 接入要求 ..... 24
规范性附录： ..... 25
附录 A　二维码数据格式 ..... 25
附录 B　电子健康卡注册流程 ..... 25
附录 C　电子健康卡使用流程 ..... 26
附录 D　SDK 接口安全和数据格式 ..... 26

# 前　言

本标准由卫生部卫生信息标准专业委员会提出。

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2部分：管理系统

## 1 范围

本规范规定了电子健康卡管理系统标准化的内容及技术要求。

本规范适用于电子健康卡管理系统的建设、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

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 缩略语

XML Schema：可扩展标记语言结构模式（Extensible Markup Language Schema）
WSDL：网络服务描述语言（Web Services Description Language）
DNS：域名系统（Domain Name System）
IP:网络之间互联的协议（Internet Protocol）

## 5 技术要求

### 5.1 功能要求

本章节定义电子健康卡管理系统的必备功能。

#### 5.1.1 用户管理

##### 5.1.1.1 用户信息登记及管理

用户信息包括电子健康卡ID、主索引ID、用户身份信息、金融支付账户。
用户身份信息一般包括姓名、性别、民族、手机号、证件类型、证件号码等内容。
电子健康卡ID、主索引ID由密码机生成。

##### 5.1.1.2 用户注册

机构可通过如下接口进行注册。通过机构进行用户注册的主要字段包括：

表 1 APP 通过该接口注册电子健康卡

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | InstitutionID | 接入机构编号 | / |

| | | | |
|---|---|---|---|
| 2 | TerminalID | 申请终端编号 | / |
| 3 | Time | 申请时间 | 按照年月日时分秒格式上，如20180408123805。 |
| 4 | CertType | 证件类型 | / |
| 5 | CertID | 证件号码 | / |
| 6 | Name | 姓名 | / |
| 7 | / | 其他信息 | 选填 |
| 8 | MAC | 完整性校验信息 | / |

表 2 管理系统返回注册结果

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | Result | 申请结果 | 成功-0<br>失败-1 |
| 2 | | 其他信息 | 失败时应返回错误信息。 |
| 3 | MAC | 完整性校验信息 | / |

用户可通过APP进行注册。通过APP进行用户注册的主要字段包括：

表 3 APP 注册电子健康卡

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | AppPackageName | APP 包名 | / |
| 2 | AppVersion | APP 版本号 | / |
| 3 | AppUserID | APP 用户 ID | / |
| 4 | Time | 申请时间 | 按照年月日时分秒格式上，如20180408123805。 |
| 5 | CertType | 证件类型 | / |
| 6 | CertID | 证件号码 | / |
| 7 | Name | 姓名 | / |
| 8 | / | 其他信息 | 选填 |
| 9 | MAC | 完整性校验信息 | / |

表 4 管理系统返回注册结果

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | Result | 申请结果 | 成功-0<br>失败-1 |
| 2 | | 其他信息 | 失败时应返回错误信息。 |
| 3 | MAC | 完整性校验信息 | / |

#### 5.1.1.3 用户信息查询

实现用户端查询本人账户信息的功能。

实现管理端查询所有账户信息功能。

#### 5.1.1.4 用户信息变更

实现用户端自助变更个人信息的功能，不允许变更证件类型、证件号码、姓名等关键信息。
实现管理端变更所有用户信息的功能，变更关键信息时需要经过授权。

#### 5.1.1.5 用户注销

实现用户注销功能。

### 5.1.2 机构管理

#### 5.1.2.1 机构信息登记及管理

机构信息包括机构编号、机构名称、机构类型、接入IP地址等。

#### 5.1.2.2 机构接入申请

机构提交注册信息，提交接入申请。

#### 5.1.2.3 机构接入授权

对机构进行接入授权，只允许通过授权的机构进行二维码验证。

#### 5.1.2.4 机构信息查询

对机构信息进行查询。

#### 5.1.2.5 机构信息变更

对机构信息进行变更。

#### 5.1.2.6 机构退出

中止机构的合作关系。

### 5.1.3 APP 管理

#### 5.1.3.1 APP 信息登记及管理

APP信息包括APP显示名称、包名称、版本号等。

#### 5.1.3.2 APP 接入申请

提交APP注册信息，提交接入申请。

#### 5.1.3.3 APP 接入授权

对APP进行接入授权，只允许通过授权的APP进行二维码验证。

#### 5.1.3.4 APP 信息查询

对APP信息进行查询。

#### 5.1.3.5 APP 信息变更

对APP信息进行变更。

#### 5.1.3.6 APP 停用

中止APP的接入。

### 5.1.4 识读终端管理

#### 5.1.4.1 识读终端信息登记及管理

识读终端信息包括识读终端所属机构、识读终端编号、识读终端名称、识读终端状态等。

#### 5.1.4.2 识读终端接入申请

机构提交识读终端注册信息，提交接入申请。

#### 5.1.4.3 识读终端接入授权

进行识读终端接入授权，只允许通过授权识读终端进行二维码验证。

#### 5.1.4.4 识读终端信息查询

对识读终端信息进行查询。

#### 5.1.4.5 识读终端退出

中止识读终端的接入。

### 5.1.5 二维码使用

#### 5.1.5.1 二维码申请

二维码申请的流程应符合附录C.1的要求。
机构可通过如下接口进行申请。通过机构进行二维码申请的主要字段包括：

表 5 机构申请二维码

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | InstitutionID | 接入机构编号 | / |
| 2 | TerminalID | 申请终端编号 | / |
| 3 | Time | 申请时间 | 按照年月日时分秒格式上，如 20180408123805。 |
| 4 | CertType | 证件类型 | / |
| 5 | CertID | 证件号码 | / |
| 6 | / | 其他信息 | 选填 |
| 7 | MAC | 完整性校验信息 | / |

表 6 管理系统返回二维码

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | Result | 申请结果 | 成功-0<br>失败-1 |
| 2 | Data | 二维码数据 | / |
| 3 | / | 其他信息 | 失败时应返回错误信息。 |

| | | | |
|---|---|---|---|
| 4 | MAC | 完整性校验信息 | / |

APP可通过如下接口进行申请。通过APP进行二维码申请的主要字段包括：

表 7 APP 申请二维码

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | AppPackageName | APP 包名 | / |
| 2 | AppVersion | APP 版本号 | / |
| 3 | AppUserID | APP 用户 ID | / |
| 4 | Time | 申请时间 | 按照年月日时分秒格式上，如 20180408123805。 |
| 5 | / | 其他信息 | 选填 |
| 6 | MAC | 完整性校验信息 | / |

表 8 管理系统返回二维码

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | Result | 申请结果 | 成功-0<br>失败-1 |
| 2 | Data | 二维码数据 | / |
| 3 | / | 其他信息 | 失败时应返回错误信息。 |
| 4 | MAC | 完整性校验信息 | / |

#### 5.1.5.2 二维码验证

二维码验证的流程应符合附录C.2的要求。

机构通过此功能进行人员识别。二维码验证的主要字段包括：

表 9 机构申请二维码验证

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | InstitutionID | 接入机构编号 | / |
| 2 | TerminalID | 识读终端编号 | / |
| 3 | Time | 识读时间 | 按照年月日时分秒格式上，如 20180408123805。 |
| 4 | Data | 识读的二维码数据 | / |
| 5 | MAC | 完整性校验信息 | / |

表 10 管理系统返回验证结果

| 编号 | 数据域 | 数据域名称 | 说明 |
|---|---|---|---|
| 1 | Result | 验证结果 | 成功-0<br>失败-1 |
| 2 | Data | 身份信息 | 证件类型+证件号码 |
| 3 | / | 其他信息 | 失败时应返回错误信息。 |

| | | | |
|---|---|---|---|
| 4 | MAC | 完整性校验信息 | / |

#### 5.1.5.3 二维码使用记录

对二维码的生成和验证进行记录，记录内容包括日期、时间、事件类型、时间来源、处理结果等。对二维码使用记录进行查询和分析。

### 5.1.6 密码机管理

#### 5.1.6.1 密码机信息登记

对密码机的型号、唯一编号、IP地址进行登记。

#### 5.1.6.2 密码机接口

密码机接口参见《电子健康卡技术规范 第4部分：密码机》。

### 5.1.7 外部接口要求

#### 5.1.7.1 跨域主索引系统接口要求

为了配合国家卫生健康委员会居民健康信息主索引平台的搭建，整合电子健康卡等系统）居民个人健康信息，电子健康卡管理系统需与跨域主索引系统对接，主要分为以下几个部分：

——系统居民基本信息注册

——系统居民信息查询

——系统认证

接入层包含面向此接口的如下接口服务：

| 服务类型 | 说明 | 参数数据 | 返回数据 |
|---|---|---|---|
| 获取会话 token | 获取会话 token | appId、appSecret | token、校验结果 |
| 主索引人员注册 | 实现对居民主索引平台的注册功能 | 居民人员数据 | 注册结果 |
| 主索引批量注册 | 实现对居民主索引平台的批量注册功能 | 居民人员批量数据 | 注册结果 |
| 主索引域标识注册 | 实现在居民已完成主索引注册的前提下，将居民所使用的域标识绑定到主索引平台的功能 | 居民主索引 ID、注册域标识信息 | 注册结果 |
| 主索引域标识注销 | 注销居民使用域标识信息 | 主索引 ID、需注销域标识信息 | 注册结果 |
| 主索引人员识别 | 居民索引信息 | 人员姓名、域标识、发卡机构代码、标识域代码 | 有效性信息结果 |

#### 5.1.7.2 用卡监测系统接口要求

电子健康卡管理系统试运行之前应实现与国家居民健康卡用卡业务监测系统（以下简称用卡监测系统）互联互通要求，实现对居民用卡数据的监测功能。电子健康卡管理系统通过调用用卡监测系统提供SDK包，实现对电子健康卡用卡数据的上传国家用卡监测系统的功能。

用卡监测系统在本地部署数据交换服务，实现对本地服务器状态以及网络状态的监测功能，同时对数据稳定性提供保证。

注：用卡监测系统需要在电子健康卡管理系统所在地部署数据交换服务。电子健康卡管理系统提供用卡监测系统监测数据交换服务部署服务环境。

## 5.2 性能要求

应具备多用户同时在线并发的能力，应保障在高并发时，系统具有良好的性能，保障事务成功率，以及事务通过数、系统响应时间，保持系统稳定、高效运行。

## 5.3 安全要求

### 5.3.1 基本要求

电子健康卡管理系统必须与电子健康卡密码机同时使用。

### 5.3.2 应用软件安全

#### 5.3.2.1 身份鉴别

##### 5.3.2.1.1 系统与普通用户设置

1.业务系统、管理系统应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

2.应提供系统管理员和普通用户的设置功能。

##### 5.3.2.1.2 身份标识唯一性

1.应提供用户身份标识唯一性和鉴别信息复杂度检查功，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

2.应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

##### 5.3.2.1.3 登录访问安全策略

应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

##### 5.3.2.1.4 口令有效期限制

业务系统、管理系统应限制口令的有效期限，并进行提醒。

##### 5.3.2.1.5 非法访问警示和记录

1.业务系统、管理系统应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

2.业务系统、管理系统应对登录成功、失败进行日志记录。

##### 5.3.2.1.6 限制认证会话时间

业务系统、管理系统应对客户端认证会话时间进行限制。

##### 5.3.2.1.7 及时清除鉴别信息

业务系统、管理系统会话结束后应及时清除客户端鉴别信息。

#### 5.3.2.2 访问控制

##### 5.3.2.2.1 访问权限设置

1. 应提供访问控制功能；
2. 控制粒度应达到文件、数据库级；
3. 访问控制策略的授权主体；
4. 如设置默认用户，其权限有应被严格限制；
5. 各用户权限划分应依据最小权限原则，相互之间应存在制约关系。

#### 5.3.2.2.2 自主访问控制范围

访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。

#### 5.3.2.2.3 业务操作日志

应提供业务操作审计功能。

#### 5.3.2.2.4 关键数据操作控制

应严格控制用户对关键数据的操作。关键数据如：敏感数据、重要业务数据、系统管理数据等。

#### 5.3.2.2.5 异常中断维护

1. 应提供用户访问中断的保护措施；
2. 应保证数据不丢失。

### 5.3.2.3 安全审计

#### 5.3.2.3.1 对象操作审计

应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

#### 5.3.2.3.2 日志信息

1. 应具备安全审计功能；
2. 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

#### 5.3.2.3.3 日志权限和保护

1. 应保证无法单独中断审计进程；
2. 无法删除、修改或覆盖审计记录。

#### 5.3.2.3.4 系统信息查询和分析

应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

### 5.3.2.4 资源控制

#### 5.3.2.4.1 会话控制

1. 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
2. 应能够对单个账户的多重并发会话进行限制。

### 5.3.2.5 应用容错

#### 5.3.2.5.1 数据有效性校验

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

5.3.2.5.2 容错机制

应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

5.3.2.5.3 故障机制

发生故障后，系统应能够及时恢复。

5.3.2.5.4 回退机制

应具备回退机制，当故障发生时能够成功回退。

5.3.2.6 报文完整性

5.3.2.6.1 通信报文有效性

通信报文应采用密码技术保证通讯过程中交易数据的完整性。

5.3.2.7 报文保密性

5.3.2.7.1 报文或会话加密

在通讯时采用安全通道或对报文中敏感信息进行加密。

5.3.2.8 WEB 页面安全

5.3.2.8.1 登录防穷举

1.业务系统、管理系统应提供登录防穷举的措施，如图片验证码等；
2.登录失败后图形验证码应能自动更换；
3.图形验证码应该具备一定的复杂度，防止能够轻易地被自动化工具识别。

5.3.2.8.2 网站页面注入防范

业务系统、管理系统应无 SQL 注入、Path 注入和 LDAP 注入等漏洞。

5.3.2.8.3 网站页面跨站脚本攻击防范

业务系统、管理系统应无跨站脚本漏洞。

5.3.2.8.4 网站页面源代码暴露防范

业务系统、管理系统应无源代码暴露漏洞。

5.3.2.8.5 网站页面黑客挂马防范

应采取防范网站页面黑客挂马的机制和措施。

5.4 SDK 接入要求

5.4.1 SDK 授权

**1、基本授权流程**

通过电子健康卡 SDK 授权管理系统，为每一个 SDK 生成一个密钥，称之为 SDK 密钥；

对每一个申请使用 SDK 的 APP 应用，需要在 SDK 授权管理系统注册，SDK 授权管理系统管理员审核通过后，为 APP 应用生成 app_id 与 app_secret；

app_id 随机生成，长度不小于 16 字节；

app_secret=SM3(app_id+SDK 密钥)。

用户可登录 SDK 授权管理系统下载 app_id 与 app_secret，SDK 授权管理系统将对通信链路建立 ssl 通道，确保 app_secret 的安全。

**2、附加授权流程**

对于移动设备原生 APP，在完成上面的基本授权流程后，还需要将 APP 的特定信息（包括 appId、应用名称、SHA1、SDK 名称等）提交 SDK 授权管理系统，SDK 授权管理系统使用标识密钥对 APP 特定信息进行签名，为 APP 生成 SDK 授权码文件。

要求原生 SDK 内置授权码验证流程（参见“**附加授权的验证流程**”）。

原生 SDK 软件包连同 SDK 授权码文件可在线或离线方式下载给原生 APP 开发商。

### 5.4.2 SDK 验证

**1、基本授权的验证流程**

首先，电子健康卡管理平台从 SDK 授权管理系统下载并安全存储 SDK 密钥；

应用使用 SDK 连接电子健康卡管理平台时，以请求包中的主要参数及 app_secret 为原文，生成摘要值，生成过程参考“摘要值生成流程”；

应用将请求包提交给电子健康卡管理平台；

电子健康卡管理平台收到请求包，解析得到 app_id，计算 app_secret=SM3(app_id+SDK 密钥)；

使用“摘要值生成流程”描述的流程生成摘要值，和请求包中摘要值比对，相等则验证通过。

**2、附加授权的验证流程**

移动设备原生 APP 需要将 SDK 授权管理系统生成的授权码文件一起打包（android 系统 app 应将授权码文件存放于 assert 目录），原生 APP 调用 SDK 时，SDK 内部会读取 APP 的特定信息及授权码文件，通过内置验证流程利用标识公钥验证签名，验证通过则允许使用 SDK 的其他功能。

原生 SDK 内置授权码验证流程如下（以 Android 系统为例）：

- 首先，原生 SDK 需要集成 SDK 授权管理系统提供的验证授权码动态库；
- SDK 被调用时，SDK 内部先调用动态库中的授权码验证函数；

- 验证函数内部将获取 APP 特定信息（AppId，App 名称，APP 应用指纹，SDK 名称）及 assert 目录中的授权码文件；

使用内置标识公钥验证签名，验证通过则允许调用SDK的其他功能

### 5.4.3 摘要值生成流程

**1、筛选**

获取所有请求参数，不包括字节类型参数，如文件、字节流，剔除 digest 字段。

(app_id.、term_id、method、version、timestamp、digest_type、enc_type、biz_content)

**2、排序**

将筛选的参数按照第一个字符的键值 ASCII 码递增排序（字母升序排序），如果遇到相同字符则按照第二个字符的键值 ASCII 码递增排序，以此类推。

**3、生成摘要值原文**

将排序后的参数与其对应值，组合成“参数=参数值”的格式，并且把这些参数用&字符连接起来，最后拼接上 app_secret，格式如下：

“…&参数=参数值&app_secret=你的密钥”

例如下面的请求示例：

```
{
    "app_id": "<你的应用编号>",
    "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"
}
```

组成的摘要值原文为：

```
app_id=1BQA48ETK000A718A8C000001FFAA482&biz_content={"ehealth_code":"F404379A
66B50640EF1367CCE000F6463BA5F0AC09AB1FFA3D10F8C6ED2D204F:2:15855D11D6068A3C53
60374B741DFCD7","out_verify_no":"V17093010293789","out_verify_time":"20171211
135852"}&enc_type=SM4&method=ehc.ehealthcode.verify&digest_type=SM3&term_id=3
5020010001&timestamp=1512971932368&version=X.M.0.1&app_secret=<你的密钥>
```

**4、生成摘要**

使用各自语言对应的摘要函数，对上面得到的原文做摘要，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：C96986F508F51555BC7B22E45792D4C382709620B589723BA422AF787EAF7219。

## 6 检测要求

### 6.1 功能检测要求

| 编号 | 检测项 | | 检测说明 |
|---|---|---|---|
| 1 | 电子健康卡管理 | 1.1 账户信息管理 | 必测项 |
| | | 1.2 注册 | 必测项 |
| | | 1.3 查询 | 必测项 |
| | | 1.4 变更 | 必测项 |
| | | 1.5 注销 | 必测项 |
| | | 1.6 账户变更记录 | 必测项 |
| 2 | 机构管理 | 2.1 机构信息登记及管理 | 必测项 |
| | | 2.2 机构接入申请 | 必测项 |
| | | 2.3 机构接入授权 | 必测项 |
| | | 2.4 机构信息查询 | 必测项 |
| | | 2.5 机构信息变更 | 必测项 |
| | | 2.6 机构退出 | 必测项 |
| 3 | APP 管理 | 3.1 APP 信息登记及管理 | 必测项 |
| | | 3.2 APP 接入申请 | 必测项 |
| | | 3.3 APP 接入授权（**基本授权的验证**） | 必测项 |
| | | 3.4 APP 信息查询 | 必测项 |
| | | 3.5 APP 信息变更 | 必测项 |
| | | 3.6 APP 退出 | 必测项 |
| 4 | 识读终端管理 | 4.1 识读终端信息登记及管理 | 识读终端直接接入管理系统时必测 |
| | | 4.2 识读终端接入授权 | 识读终端直接接入管 |

| 编号 | 检测项 | | 检测说明 |
|---|---|---|---|
| | | | 理系统时必测 |
| | | 4.3 识读终端信息查询 | 识读终端直接接入管理系统时必测 |
| | | 4.4 识读终端移除 | 识读终端直接接入管理系统时必测 |
| 5 | 二维码管理 | 5.1 二维码生成 | 必测项 |
| | | 5.2 二维码验证 | 必测项 |
| | | 5.3 二维码使用记录 | 必测项 |
| 6 | 密码及管理 | 6.1 密码机信息登记 | 必测项 |
| | | 6.2 密码机接口 | 必测项 |

## 6.2 性能检测要求

在多用户并发的情况下，系统事务成功率不低于95%，响应时间不高于5秒，低于100个并发用户注册的情况下，响应时间不高于3秒。

| 编号 | 检测项 | 检测说明 |
|---|---|---|
| 1 | 1.1 注册 | 必测项 |
| | 1.2 申请二维码 | 必测项 |
| | 1.3 二维码验证 | 必测项 |

## 6.3 安全检测要求

| 序号 | 检测项 | 检测点 | 检测要求细化 | 检测方法及步骤 | 预期结果及判定 |
|---|---|---|---|---|---|
| 1 | 身份鉴别 | 1.1 系统与普通用户设置 | 1.业务系统、管理系统应提供专用的登录控制模块对登录用户进行身份标识和鉴别；<br>2.应提供系统管理员和普通用户的设置功能。 | 1.查看系统是否提供专用模块对用户进行身份标识和鉴别,如登录模块；<br>2.验证身份鉴别模块是否有效，身份鉴别是否正确。 | 1.系统提供登录模块对用户进行身份标识和鉴别；<br>2.系统身份鉴别模块有效，且身份鉴别结果正确。 |
| | | 1.2 身份标识唯一性 | 1.应提供用户身份标识唯一性和鉴别信息复杂度检查功，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；<br>2.应启用身份鉴别、用户身份标识唯一性检查、用户身份 | 1.检查系统是否提供用户身份标识唯一性检查功能，如通过新建用户等方式验证；<br>2.检查系统是否提供鉴别信息复杂度检查功能，如创建用户时，口令至少为 8 位，至少包括数字、字母及特殊字符；<br>3.检查系统是否启用了身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复 | 1.提供了用户身份标识唯一性和鉴别信息复杂度检查功能；<br>2.启用了身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。 |

| 序号 | 检测项 | 检测点 | 检测要求细化 | 检测方法及步骤 | 预期结果及判定 |
|---|---|---|---|---|---|
| | | | 鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。 | 杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。 | |
| | | 1.3 登录访问安全策略 | 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。 | 查看系统是否采用多种身份鉴别技术。 | 系统采用两种身份鉴别技术（用户/口令、数字证书、动态令牌等）。 |
| | | 1.4 口令有效期限制 | 业务系统、管理系统应限制口令的有效期限，并进行提醒。 | 查看系统是否有定期口令更改提示功能，对一段时间内未修改口令的账户进行提醒。 | 系统提供定期口令更改提示功能，对到期未修改口令的账户进行提醒。 |
| | | 1.5 非法访问警示和记录 | 1.业务系统、管理系统应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；<br>2.业务系统、管理系统应对登录成功、失败进行日志记录。 | 1.检查系统是否提供多次登录失败处理功能，如账户锁定、关闭浏览器、结束会话等；<br>2.检查登录错误提示是否过于详细（错误明确提示用户名错误、密码错误）；<br>3.是否对登录成功、失败进行日志记录，用户登录后系统是否提示上次登录情况（如登录时间、IP、登录成功/失败情况等）。 | 1.系统提供多次登录失败处理功能，口令多次错误后账户锁定/关闭浏览器/结束会话；<br>2.系统用户名/口令错误时，系统提示；<br>3.系统对用户登录成功、失败进行日志记录，用户登录后系统提示上次登录情况，提示内容包括上次登录时间、IP、登录成功/失败情况等。 |
| | | 1.6 限制认证会话时间 | 业务系统、管理系统应对客户端认证会话时间进行限制。 | 查看系统是否具有空闲会话超时功能，如对于 Web 应用系统，可检查是否对中间件相关配置进行了设置。 | 系统具有空闲会话超时功能，空闲会话超时时间合理。 |
| | | 1.7 及时清除鉴别信息 | 业务系统、管理系统会话结束后应及时清除客户端鉴别信息。 | 1.如该系统为 B/S 模式，可通过下列步骤进行测试：a、登录系统，并复制某功能模块 URL；b、正常退出后，通过浏览器访问该 URL，查看是否可以访问并继续进行操作；c、直接关闭浏览器，模拟非正常退出，再打开浏览器，通过浏览器访问该 URL，查看是否可以访问并继续进行操作；<br>2.如该系统为 C/S 模式，模拟正常/非正常退出系统，检 | 1.系统为 B/S 模式，模拟正常/非正常退出系统，均无法通过访问 URL 的方式继续进行操作，会话结束后，系统及时清除了客户端鉴别信息；<br>2.系统为 C/S 模式，模拟正常/非正常退出系统，均未发现安装目录中存在鉴别信息。 |

| 序号 | 检测项 | 检测点 | 检测要求细化 | 检测方法及步骤 | 预期结果及判定 |
|---|---|---|---|---|---|
| | | | | 查客户端程序的安装目录中的文件，是否有未删除的临时文件，临时文件中是否含有用户鉴别信息。 | |
| 2 | 访问控制 | 2.1 访问权限设置 | 1.应提供访问控制功能；<br>2.控制粒度应达到文件、数据库级；<br>3.访问控制策略的授权主体；<br>4.如设置默认用户，其权限有应被严格限制；<br>5.各用户权限划分应依据最小权限原则，相互之间应存在制约关系。 | 1.应访谈应用系统管理员，询问应用系统是否提供访问控制措施，以及具体措施和访问控制策略有哪些，访问控制的粒度如何；<br>2.应检查应用系统，查看访问控制的粒度是否达到主体为用户级，客体为文件、数据库表级；查看其是否有由授权用户设置其它用户访问系统功能和用户数据的权限的功能，是否限制默认用户的访问权限；<br>3.应检查应用系统，查看系统是否授予不同账户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约；<br>4.应测试应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效；<br>5.应测试应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认账户的访问权限；<br>6.在不登录的情况下，或通过低权限用户登录后通过 URL 直接跳转到高权限用户的功能 | 1.系统提供了访问控制功能，控制粒度主体为用户级，客体为文件、数据库表级；<br>2.访问控制措施由授权主体设置，并限制了默认用户的访问权限；<br>3.各用户按照最小权限原则进行权限划分，并在相互之间形成制约关系。 |
| | | 2.2 自主访问控制范围 | 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。 | 应检查应用系统，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作，如对客体的增、删、改、查 | 访问控制的覆盖范围包括了与资源访问相关的主体、客体及它们之间的操作。 |

| 序号 | 检测项 | 检测点 | 检测要求细化 | 检测方法及步骤 | 预期结果及判定 |
|---|---|---|---|---|---|
| | | | | 等操作。 | |
| | | 2.3 业务操作日志 | 应提供业务操作审计功能。 | 1.应访谈安全审计员，系统是否具备对所有业务操作的审计功能；<br>2.应检查应用系统，查看系统是否记录了所有业务操作日志；<br>3.应测试应用系统，可通过业务操作产生相关审计日志，并查看是否能够正确记录。 | 系统具有对所有业务操作进行日志记录的功能。 |
| | | 2.4 关键数据操作控制 | 应严格控制用户对关键数据的操作。关键数据如：敏感数据、重要业务数据、系统管理数据等。 | 1.访谈系统管理员，系统内关键数据有哪些，是否配置了针对关键数据的访问控制策略；<br>2.应渗透测试应用系统，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。 | 严格控制了用户对关键数据的操作，无法绕过访问控制对其进行操作。 |
| | | 2.5 异常中断维护 | 1.应提供用户访问中断的保护措施；<br>2.应保证数据不丢失。 | 1.应访谈系统管理员，用户访问异常中断的防护手段有哪些；<br>2.应测试应用系统，在用户访问异常中断后，查看用户数据是否丢失。 | 用户访问异常中断后，能够保证用户数据不丢失。 |
| 3 | 安全审计 | 3.1 对象操作审计 | 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。 | 1.检查应用系统，查看其当前审计范围是否覆盖到每个用户；<br>2.检查应用系统，查看其审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等；<br>3.测试应用系统，在应用系统上试图产生一些重要的安全相关事件（如用户登录、修改用户权限等），查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户。 | 1.审计范围覆盖到每个用户；<br>2.审计策略覆盖系统内的重要安全事件，包括用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等。 |
| | | 3.2 日志信息 | 1.应具备安全审计 | 1.应访谈安全审计员，询问应 | 1.系统具备安全审计功 |

| 序号 | 检测项 | 检测点 | 检测要求细化 | 检测方法及步骤 | 预期结果及判定 |
|---|---|---|---|---|---|
| | | | 功能；<br>2.审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。 | 用系统是否有安全审计功能；<br>2.应检查应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容；<br>3.应测试应用系统，在应用系统上试图产生一些重要的安全相关事件（如用户登录、修改用户权限等），查看应用系统是否对其进行了审计；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等。 | 能；<br>2.审计要素包括了事件的日期、时间、发起者信息、类型、描述和结果等。 |
| | | 3.3 日志权限和保护 | 1.应保证无法单独中断审计进程；<br>2.无法删除、修改或覆盖审计记录。 | 1.应访谈安全审计员，对审计日志的保护措施有哪些； 2.应测试应用系统，可通过非审计员的其他账户试图中断审计进程，验证审计进程是否受到保护；<br>3.应测试应用系统，试图非授权删除、修改或覆盖审计记录，验证安全审计的保护情况是否无法非授权删除、修改或覆盖审计记录。 | 1.无法单独中断审计进程；<br>2.提供了审计记录保护措施，无法删除、修改或覆盖审计记录；<br>3.审计数据进行了备份。 |
| | | 3.4 系统信息查询和分析 | 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。 | 检查应用系统，查看其是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表。 | 系统提供了审计记录数据进行统计、查询、分析及生成审计报表的功能。 |
| 4 | 资源控制 | 4.1 会话控制 | 1.当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；<br>2.应能够对单个账户的多重并发会话 | 1.检查应用系统，查看是否限制单个账户的多重并发会话；<br>2.测试应用系统，可通过对系统进行超过规定的单个账户的多重并发会话数进行连接，验证系统是否能够正确地限制单个账户的多重并发 | 1.会话超时会自动结束会话；<br>2.限制了单个用户的多重并发会话。 |

| 序号 | 检测项 | 检测点 | 检测要求细化 | 检测方法及步骤 | 预期结果及判定 |
|---|---|---|---|---|---|
| | | | 进行限制。 | 会话数；<br>3.测试重要应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。 | |
| 5 | 应用容错 | 5.1 数据有效性校验 | 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。 | 1.应访谈应用系统管理员，询问应用系统是否具有保证软件容错能力的措施，具体措施有哪些；<br>2.应检查应用系统，查看应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验，是否存在 SQL 注入、XSS 跨站脚本漏洞、框架注入钓鱼和远程命令执行等；<br>3.应测试应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确。 | 对通过人机接口输入或通过通信接口输入的数据格式或长度进行了严格限制。 |
| | | 5.2 容错机制 | 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。 | 检查应用系统是否具备冗余机制，如双机热备、集群等。 | 具备冗余机制，如双机热备、集群等。 |
| | | 5.3 故障机制 | 发生故障后，系统应能够及时恢复。 | 1.访谈管理员，了解业务系统故障恢复机制和时间要求；<br>2.查看故障恢复日志或记录；<br>3.检查保障系统及时恢复的措施。 | 1.系统故障恢复功能正常，恢复时间符合要求；<br>2.提供恢复日志或记录；<br>3.系统具有发生故障后及时恢复的措施。 |
| | | 5.4 回退机制 | 应具备回退机制，当故障发生时能够成功回退。 | 1.应访谈系统管理员，系统是否具备回退功能；<br>2.查看历史回退记录。 | 1.提供了回退功能；<br>2.能够及时回退到故障发生前的状态。 |
| 6 | 报文完整性 | 6.1 通信报文有效性 | 通信报文应采用密码技术保证通讯过程中交易数据的完整性。 | 1.应访谈相关人员，询问应用系统是否具有在数据传输过程中保护其完整性的措施，具体措施是什么；<br>2.应检查设计或验收文档，查看其是否有关于保护通信完整性的说明，如果有则查看 | 采用了密码技术保证通信过程中数据的完整性。 |

| 序号 | 检测项 | 检测点 | 检测要求细化 | 检测方法及步骤 | 预期结果及判定 |
|---|---|---|---|---|---|
| | | | | 其是否有用密码技术来保证通信过程中数据的完整性的描述；<br>3.应测试应用系统，可通过获取通信双方的数据包，查看通信报文是否含有加密的验证码。 | |
| 7 | 报文保密性 | 7.1 报文或会话加密 | 在通讯时采用安全通道或对报文中敏感信息进行加密。 | 1.应访谈相关人员，询问应用系统数据在通信过程中是否采取保密措施，具体措施有哪些；<br>2.应测试应用系统，通过查看通信双方数据包的内容，查看系统在通信过程中，安全通道或对报文敏感字段进行加密的功能是否有效。 | 在通讯时采用了安全通道或对报文中敏感信息进行加密。 |
| 8 | WEB 页面安全 | 8.1 登录防穷举 | 1.业务系统、管理系统应提供登录防穷举的措施，如图片验证码等；<br>2.登录失败后图形验证码应能自动更换；<br>3.图形验证码应该具备一定的复杂度，防止能够轻易地被自动化工具识别。 | 1.检查是否提供图形验证码机制防范对用户名、口令穷举攻击；<br>2.输入错误的口令、错误的验证码后查看图形验证码是否会及时更新；<br>3.检查图形验证码是否采用了字体变形、黏连、背景干扰信息等技术防止被自动化工具识别。 | 1.系统使用图形验证码技术防范登录穷举；<br>2.图形验证码在登录失败后自动更换；<br>3.系统使用的图形验证码采用了字体变形、黏连、背景干扰信息等技术防止被自动化工具识别。 |
| | | 8.2 网站页面注入防范 | 业务系统、管理系统应无 SQL 注入、Path 注入和 LDAP 注入等漏洞。 | 通过 Web 扫描软件及手工测试，查看系统是否存在 SQL 注入、Path 注入和 LDAP 注入等漏洞。 | 通过 Web 扫描软件及手工测试，未发现系统存在 SQL 注入、Path 注入和 LDAP 等漏洞。 |
| | | 8.3 网站页面跨站脚本攻击防范 | 业务系统、管理系统应无跨站脚本漏洞。 | 通过 Web 扫描软件及手工测试，查看系统是否存在跨站脚本漏洞。 | 通过 Web 扫描软件及手工测试，未发现系统存在跨站脚本漏洞。 |
| | | 8.4 网站页面源代码暴露防范 | 业务系统、管理系统应无源代码暴露漏洞。 | 通过 Web 扫描软件及手工测试，查看系统是否存在源代码暴露漏洞。 | 通过 Web 扫描软件及手工测试，未发现系统存在源代码暴露漏洞。 |
| | | 8.5 网站页面黑客挂马防范 | 应采取防范网站页面黑客挂马的机制和措施。 | 1.检查网站是否存在黑客挂马情况；<br>2.根据 Web 扫描软件及手工测试，是否发现网站有被黑 | 1.通过检测，未发现系统存在黑客挂马情况；<br>2.通过检测，未发现网站存在被黑客挂马的风 |

| 序号 | 检测项 | 检测点 | 检测要求细化 | 检测方法及步骤 | 预期结果及判定 |
|---|---|---|---|---|---|
| | | | | 客挂马的风险；<br>3.查看系统是否使用了网页防篡改系统。 | 险；<br>3.系统使用了网页防篡改系统防止黑客挂马。 |

6.4 SDK 接入要求

| 编号 | 检测项 | | 检测说明 |
|---|---|---|---|
| 1 | 接口功能 | 注册电子健康卡 | 必测项 |
| 2 | | 修改电子健康卡信息 | 必测项 |
| 3 | | 注销电子健康卡 | 必测项 |
| 4 | | 查询电子健康卡信息 | 必测项 |
| 5 | | 获取电子健康卡二维码 | 必测项 |
| 6 | | 验证电子健康卡二维码 | 必测项 |
| 7 | 数据一致 | 接口名称 | 必测项 |
| 8 | | 证件类型 | 必测项 |
| 9 | | 用户性别 | 必测项 |
| 10 | 报名加密 | 组装请求报文 | 必测项 |
| 11 | | 待加密串 | 必测项 |
| 12 | | 报文加密密钥 | 必测项 |
| 13 | | 获取密文 | 必测项 |
| 14 | | 设置密文 | 必测项 |
| 15 | 报文解密 | 获取响应报文 | 必测项 |
| 16 | | 获取加密密文数据 | 必测项 |
| 17 | | 报文解密密钥 | 必测项 |
| 18 | | 获取明文 | 必测项 |
| 19 | | 设置明文 | 必测项 |
| 20 | 授权验证 | 基本**授权的验证**<br>**原生 SDK 附加授权的验证** | 必测项<br>必测项 |

注：检测项用到的技术参数和规则见附录D SDK接口安全和数据格式。

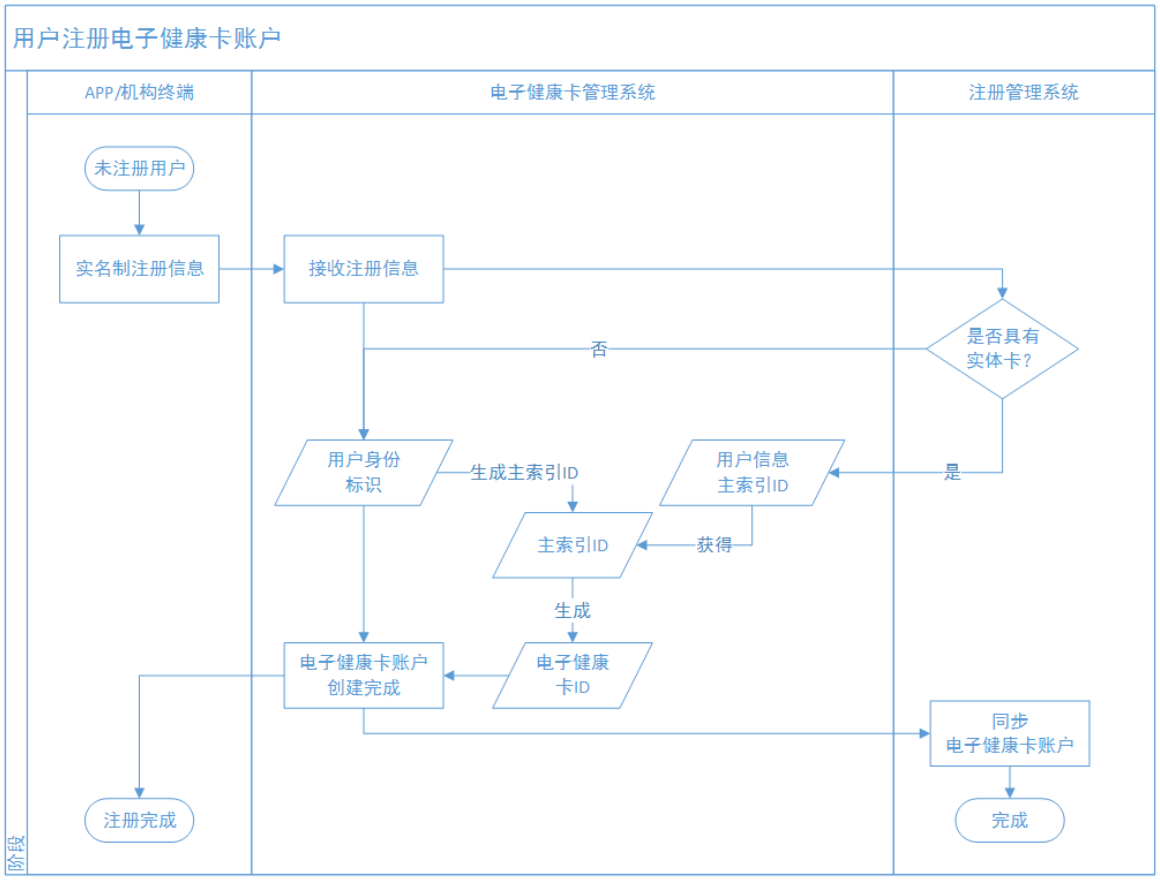
**规范性附录：**

附录 A　二维码数据格式

本节定义电子健康卡二维码数据格式。

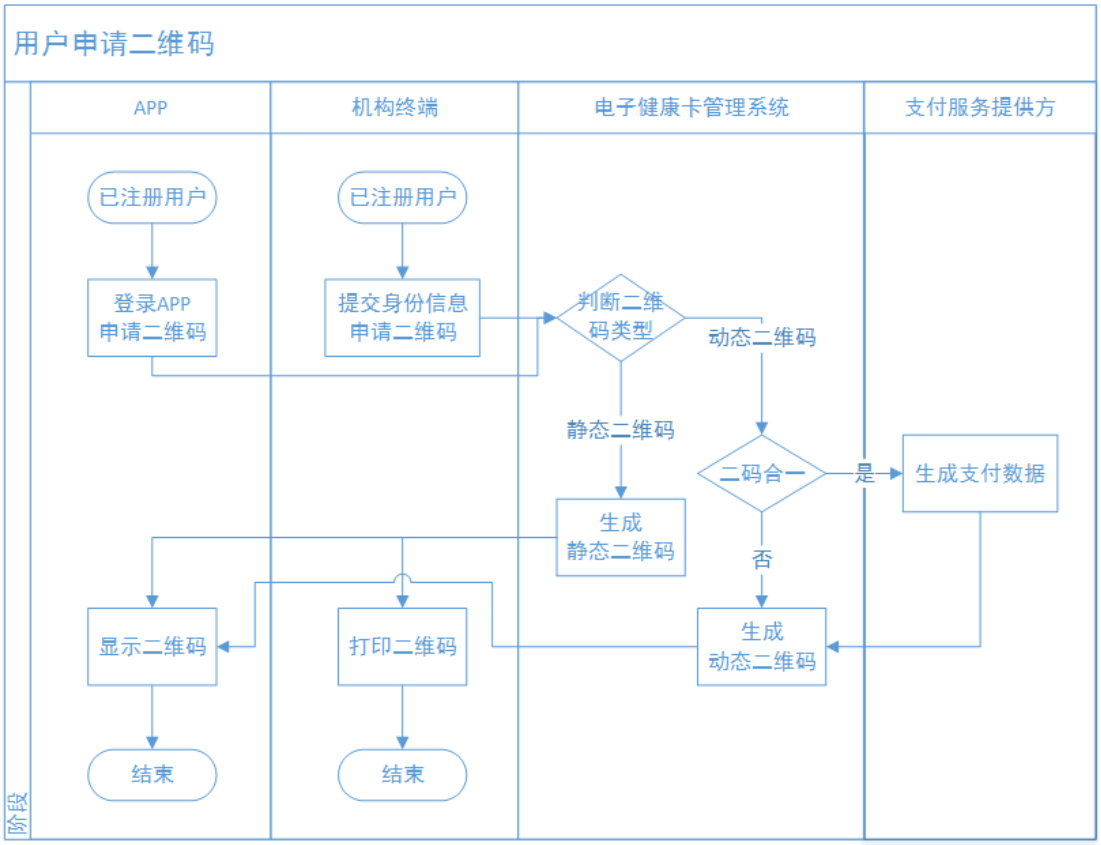
| 序号 | 字段内容 | 代码 | 备注 |
|---|---|---|---|
| 1 | 电子健康卡 ID | VUID | 用 VUID 表示。 |
| 2 | 二维码类型标识符 | | 0 为动态二维码标识符，1 为静态二维码标识符 |
| 3 | 二维码有效性信息 | VALID | 由密码服务模块对有效时间加密产生。 |
| 4 | 支付数据 | TOKEN | 支付服务提供方支付数据，二码合一支付使用。 |
| 二维码不同字段使用英文半角冒号作为分隔符。<br>二维码示例如下：<br>静态二维码　VUID:1<br>动态二维码　VUID:0:VALID<br>二码合一　　VUID:0:VALID:TOKEN | | | |

附录 B　电子健康卡注册流程

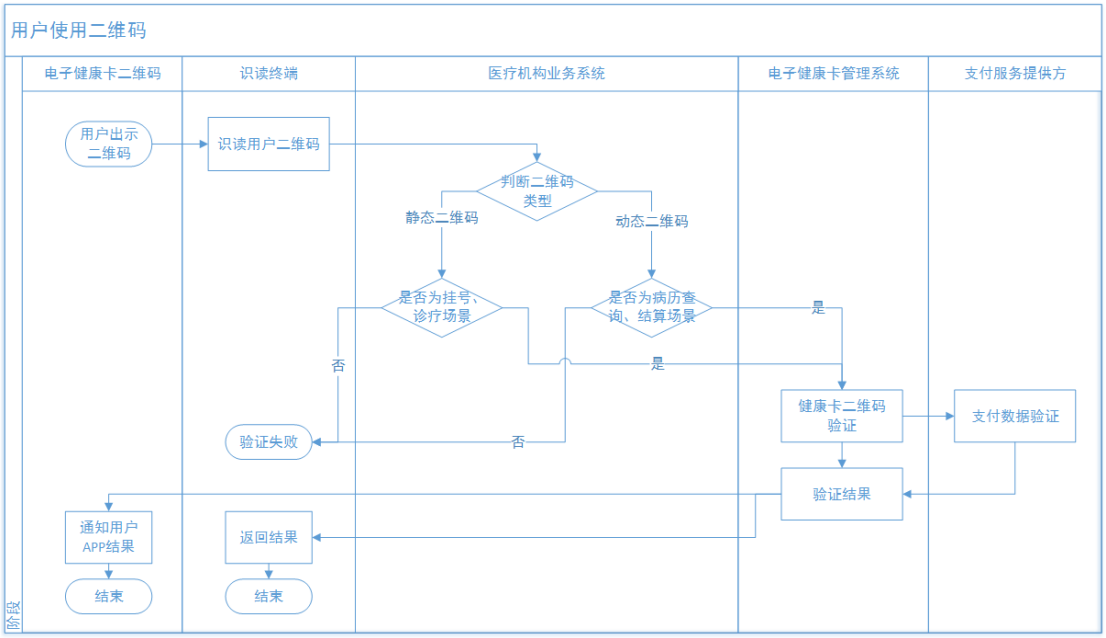


附录 C　电子健康卡使用流程

C.1 电子健康卡二维码申请流程




C.2 电子健康卡二维码验证流程




附录 D　SDK 接口安全和数据格式

## 1. 字典说明

**1）接口名称(method)字典**

| 接口名称 | 接口说明 |
|---|---|
| ehc.ehealthcode.verify | 电子健康卡二维码验证 |
| ehc.ehealthcard.regquery | 查询（注册）电子健康卡信息 |

**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 |

**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 |

## 2. 加密规则-请求报文加密

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。

**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"
}
```

**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\"}

**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。

**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

**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":
"1EBA275881C8E1BBB31E72BB800C625C05F7F6D7A99DD44741E1CEC73828F844D954E1302A382F7A427403FB3638
051A78605C57AD7490F7E3E4B87CA9D5925C630561AB3E6C5D68757B774E7B19C9727202628D2EC4532CA8F1B3F4C
CC2DA481CEAC13E3B91120F6BE0DE2D6337B30265A1DB126510D657D04458D0083E3955AE57AD4B9ED4B177187BF1
B099EB9015C235240E6D2C19CF3D4C0273F3C81154619697CB27CBB4E80859709891ADF368",
    "enc_type": "SM4",
    "method": "ehc.ehealthcode.verify",
    "digest": "9F9A7E008EF3E19AF4202FEC45FB5FEC",
    "digest_type": "SM3",
    "term_id": "35020010001",
    "timestamp": "1512971932368",
    "version": "X.M.0.1"
}
```


## 3. 加密规则-返回报文解密

**1）获取响应报文**


```
{
    "app_id": "1BQA48ETK000A718A8C000001FFAA482",
    "biz_content":
"9E10E1E5A27826900BF234112A7991FD7AFE06AADCF53DE67E653F243754E02C06AF821C9A1590459A3B22E2F599
CA9468AED550D62C8646484F3A67DFE05CFD56F99F328DA5CC14912375BE5DD14354FD923B90E5DB8C0EF3202FA50
E69042EA1D645E0B82CA0807653D67723370BFEF8DC0CE6F8C88C05830283CD97D3808CFF23C56BCC6D743B376705
0E109A2E8455133DCC59E0E26AA92EC3E44449D322DAE8B4ECEDD07462D1859F81BB0E0E46CA088B77C216D1F267E
F22F6B6B391B0729732E847FABBBAA08AB261D64420433FFC6750C608075A2F5482AA2462ED842E51CDA746B862CD
C30F0D75EAEF4ED65E2A0BF8A43306B7D6BE761AA276E2F1C4FAB29B5A32BE1FF536FF1ECEBB94C7",
    "enc_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"
}
```


**2）获取加密密文数据 encryptData**

9E10E1E5A27826900BF234112A7991FD7AFE06AADCF53DE67E653F243754E02C06AF821C9A1590459A3B22E2F599CA9468AED550D62C8646484F3A67DFE05CFD56F99F328DA5CC14912375BE5DD14354FD923B90E5DB8C0EF3202FA50E69042EA1D645E0B82CA0807653D67723370BFEF8DC0CE6F8C88C05830283CD97D3808CFF23C56BCC6D743B3767050E109A2E8455133DCC59E0E26AA92EC3E44449D322DAE8B4ECEDD07462D1859F81BB0E0E46CA088B77C216D1F267EF22F6B6B391B0729732E847FABBBAA08AB261D64420433FFC6750C608075A2F5482AA2462ED842E51CDA746B862CDC30F0D75EAEF4ED65E2A0BF8A43306B7D6BE761AA276E2F1C4FAB29B5A32BE1FF536FF1ECEBB94C7

**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；

**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\"}

**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。