**电子健康卡API授权管理**

**系统设计方案**

**目录**

[电子健康卡API授权管理系统设计方案 3](#_Toc533515436)

[1 需求分析 3](#_Toc533515437)

[1.1 业务需求分析 3](#_Toc533515438)

[1.2 系统需求分析 3](#_Toc533515439)

[2 系统功能 3](#_Toc533515440)

[2.1 用户注册 3](#_Toc533515441)

[2.2 登录认证 4](#_Toc533515442)

[2.3 用户信息修改 4](#_Toc533515443)

[2.4 用户相关下载 4](#_Toc533515444)

[2.4.1 应用开发用户 4](#_Toc533515445)

[2.4.2 验证系统用户 4](#_Toc533515446)

[2.5 操作员应用审批与授权 4](#_Toc533515447)

[2.6 审计信息查询与审计 4](#_Toc533515448)

[2.7 管理员管理 4](#_Toc533515449)

[3 系统架构 5](#_Toc533515450)

[4 应用流程 7](#_Toc533515451)

[4.1 用户注册与审批 7](#_Toc533515452)

[4.2 应用开发商授权申请与授权码下载 8](#_Toc533515453)

[4.3 管理员管理 9](#_Toc533515454)

[4.4 审计员信息查询与审计 10](#_Toc533515455)

[5 页面设计 10](#_Toc533515456)

[5.1 普通用户 10](#_Toc533515457)

[5.2 超级管理员 11](#_Toc533515458)

[5.3 操作员 11](#_Toc533515459)

[5.4 审计员 11](#_Toc533515460)

[6 数据库设计 12](#_Toc533515461)

[6.1 管理员表（ADMIN） 12](#_Toc533515462)

[6.2 用户表（USER） 12](#_Toc533515463)

[6.3 API表（SDK） 13](#_Toc533515464)

[6.4 服务系统注册表（SDK\_KEY） 13](#_Toc533515465)

[6.5 API授权表（GRANTING） 13](#_Toc533515466)

[6.6 配置表（CONFIG） 14](#_Toc533515467)

[6.7 申请密钥表（GRANTING\_KEY） 14](#_Toc533515468)

[6.8 添加验证系统表（PUBLIC\_KEYID） 15](#_Toc533515469)

[6.9 管理日志表（AUDIT\_LOG） 15](#_Toc533515470)

[6.10 用户日志表（USER\_LOG） 15](#_Toc533515471)

电子健康卡API授权管理系统设计方案

# 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日志管理及备份恢复机制。

# 系统功能

## 用户注册

用户分为应用开发商和验证系统开发者，根据提示填写相应的信息。注册完成后，企业状态为“待审核”，管理员审核通过后，状态为“审核通过”，可以进行应用授权申请操作。

## 登录认证

用户通过用户名口令字方式认证登录。

管理员通过USBKEY方式登录。

## 用户信息修改

用户：允许修改自己的某些信息，密码，邮箱等等。

管理员：超级管理员授权操作员权限。

## 用户相关下载

### 应用开发用户

用户成功登录后，可申请对某个API的授权码，按照提示填写相关应用信息，提交申请。操作员审批通过后，可以查看和下载授权码。操作员审批未通过，可以修改应用授权申请信息，并重新提交。对于审批通过的应用，操作员拥有将其注销操作权限。

### 验证系统用户

登录成功后，可申请下载服务系统的密钥，提交申请后，操作员审批通过后，输入自定义pin码可下载改系统密钥。

## 操作员应用审批与授权

操作员审批待审批的应用授权申请，生成授权码。操作员数字签名，记录审计信息。为审批未通过的申请，填写未通过原因，待用户修改，可以继续提交申请。

## 审计信息查询与审计

审计员查询管理员管理、用户审批和应用授权审批等审计信息，验证签名通过，审计通过，否则为审计未通过。

## 管理员管理

超级管理员进行操作员的管理，可开启和禁用操作员。操作员负责审批用户信息和应用授权信息，添加API，电子健康卡服务系统等等的操作。审计员审计一些敏感的操作，用签名验签来保证信息的安全可靠性。

管理员使用Ukey登录，需要安装控件和驱动。

# 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。

# 应用流程

## 用户注册与审批



## 应用开发商授权申请与授权码下载



## 管理员管理

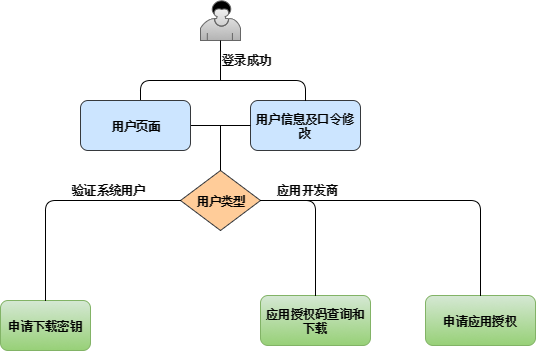


## 审计员信息查询与审计

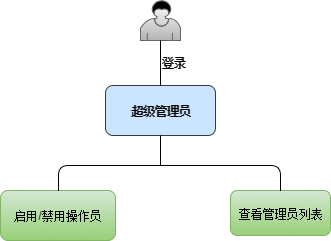


# 页面设计

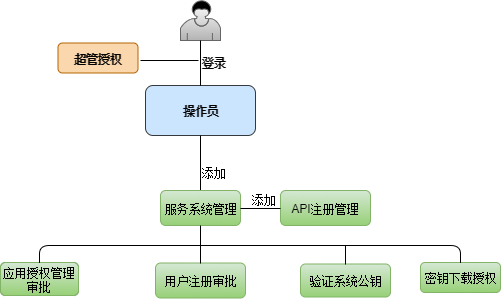
## 普通用户



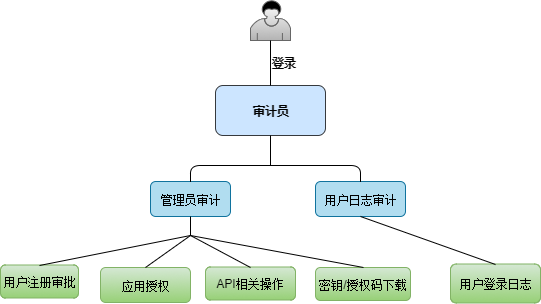
## 超级管理员



## 操作员



## 审计员



# 数据库设计

## 管理员表（ADMIN）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| ID | INT | 非空 | 主键 |
| ADMIN\_ID | VARCHAR(100) | 非空 | 管理员ID |
| ADMIN\_NAME | VARCHAR(200) | 非空 | 管理员名称 |
| TYPE | INT | 非空 | 管理员权限 |
| 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(默认为0) | 状态，用于逻辑删除 |
| 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(默认当前时间) | 操作时间 |

## 用户表（USER）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| ID | INTEGER | 非空 | 主键 |
| 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 |
| PASS | VARCHAR(200) | 非空 | 密码（加密存储） |
| ADDR | VARCHAR(100) | 是 | 地址 |
| CONTACTS | VARCHAR(100) | 是 | 联系人 |
| TEL | VARCHAR(20) | 是 | 联系方式 |
| EMAIL | VARCHAR(50) | 是 | 邮件地址 |
| STATUS | INTEGER | 非空 | 用户状态 |
| TIME | TIMESTAMP | 非空 | 操作时间 |
| DESCRIPTION | VARCHAR(100) | 是 | 未通过审批的理由 |
| CERT\_TYPE | VARCHAR(10) | 是 | 证件类型 |
| CERT\_NUM | VARCHAR(50) | 是 | 证件编号 |
| INDUSTRY\_SORT | VARCHAR(50) | 是 | 行业类别 |
| USER\_CASE | VARCHAR(50) | 是 | 使用场景 |
| REMARKS | VARCHAR(300) | 是 | 备注 |
| CERT\_PATH | VARCHAR(100) | 是 | 企业证件 |
| PERSON\_CARDZ | VARCHAR(100) | 是 | 身份证反面 |
| PERSON\_CARDF | VARCHAR(100) | 是 | 身份证正面 |
| ERRTIMES | INTEGER | 默认为0 | 错误登录次数 |
| LASTERRTIME | BIGINT | 默认为0 | 最后的错误登录时间 |

## API表（SDK）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段** | **类型** | | **是否可以为空** | **备注** |
| ID | INT | 主键 | | 主键 |
| NAME | VARCHAR(200) | 否 | | API名称 |
| TYPE | INTEGER | 否 | | API类型 |
| CATEGROY | INTEGER | 是 | | 外键-关联SDK\_KEY表 |
| STATUS | INTERGER | 默认为0 | | 状态-用于逻辑删除 |
| TIME | TIMESTAMP | 默认当前时间 | | 操作时间 |

## 服务系统注册表（SDK\_KEY）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| SDK\_CATEGORY | INT | 主键 | 主键 |
| KEY\_ | VARCHAR(1000) | 非空 | 服务系统密钥 |
| KEY\_NAME | VARCHAR(100) | 非空 | 服务系统名称 |
| DESCRIPTION | VARCHAR(100) | 非空 | 描述 |

## API授权表（GRANTING）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| ID | INT | 主键 | 主键 |
| USER\_ID | VARCHAR(200) | 否 | 关联USER表的ID |
| SDK\_ID | INTEGER | 否 | 关联SDK表的ID |
| SDK\_NAME | INTEGER | 否 | 关联SDK表的名称 |
| APP\_LABLE | INTERGER | 否 | App的应用名称 |
| APP\_ID | TIMESTAMP | 是 | / |
| APP\_ENV | VARCHAR(100) | 是 | App开发环境 |
| APP\_SHA1 | VARCHAR(100) | 是 | SHA1值 |
| APP\_PACKAGE | VARCHAR(100) | 是 | App包名 |
| APP\_VERSION | VARCHAR(50) | 是 | App版本 |
| APP\_RANGE | VARCHAR(200) | 是 | App应用范围 |
| DEVELOPER | VARCHAR(20) | 是 | 开发者名称 |
| STATUS | INTEGER | 默认为0 | 状态-是否审批通过 |
| AUTH\_CODE | VARCHAR(500) | 是 | 本地调用类的授权码 |
| CLIENT\_ID | VARCHAR(100) | 是 | 远程连接类的APPID |
| CLIENT\_SECRET | VARCHAR(100) | 是 | 远程连接类的APPSECR |
| IDPID | VARCHAR(500) | 是 | 签名公钥标识 |
| VERSION | BIGINT | 默认为0 | 版本-推送授权信息用 |
| ADMIN\_ID | VARCHAR(100) | 是 | 管理员ID |
| SIGNATURE | VARCHAR(200) | 是 | 签名值（审计用） |
| APPLY\_TIME | TIMESTAMP | 是 | 申请时间 |
| GRANT\_TIME | TIMESTAMP | 是 | 授权时间 |
| STATE | INTEGER | 默认0 | 用于逻辑删除 |
| DESCRIPTION | VARCHAR(100) | 是 | 审批时的描述 |
| EX\_TIME | VARCHAR(10) | 是 | 有效期 |
| DEV\_CERT\_TYPE | VARCHAR(50) | 是 | 证件类型 |
| DEV\_CERT\_NO | VARCHAR(60) | 是 | 证件编号 |
| DEV\_ADDR | VARCHAR(200) | 是 | 地址 |
| DEV\_TEL | VARCHAR(100) | 是 | 电话 |
| DEV\_EMAIL | VARCHAR(100) | 是 | 邮箱 |
| REMARKS | VARCHAR(300) | 是 | 备注 |
| DEVELOPER\_CARDZ | VARCHAR(100) | 是 | 用户身份证正面 |
| DEVELOPER\_CARDF | VARCHAR(100) | 是 | 用户身份证反面 |

## 配置表（CONFIG）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| 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 |
| VISIABLE | INTEGER | 非空 | 是否可见 |
| DESCRIPTION | VARCHAR(200) | 非空 | 描述 |

## 申请密钥表（GRANTING\_KEY）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| ID | INTEGER | 非空 | 主键 |
| USER\_ID | VARCHAR(100) | 非空 | 验证系统用户ID |
| USER\_NAME | VARCHAR(100) | 非空 | 验证系统用户名称 |
| SDK\_CATEGORY | INTEGER | 非空 | 服务系统ID |
| KEY\_NAME | VARCHAR(100) | 非空 | 服务系统名称 |
| ADMIN\_ID | VARCHAR(100) | 是 | 管理员ID |
| STATUS | INTEGER | 非空(默认为0) | 状态 |
| STATE | INTEGER | 非空（默认为0） | 用于逻辑删除 |
| TIME | TIMESTAMP | 是 | 操作时间 |
| GRANT\_TIME | TIMESTAMP | 是 | 授权时间 |

## 添加验证系统表（PUBLIC\_KEYID）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| ID | INTEGER | 主键 | 主键 |
| SPID | VARCHAR(30) | 否 | 用户ID(UID) |
| IDPID | VARCHAR(500) | 否 | 验证系统公钥标识 |
| NAME | VARCHAR(50) | 否 | 验证系统名称 |
| DESCRIPTION | VARCHAR(100) | 是 | 描述 |
| TIME | TIMESTAMP | 默认当前时间 | 操作时间 |

## 管理日志表（AUDIT\_LOG）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| ID | INTEGER | 非空 | 主键 |
| TIME | TIMESTAMP | 是 | 操作时间 |
| TYPE | VARCHAR(100) | 否 | 操作类型 |
| RESULT | VARCHAR(100) | 否 | 操作结果 |
| DESCRIPTION | VARCHAR(200) | 否 | 描述 |
| ADMIN\_ID | VARCHAR(100) | 否 | 管理员ID |
| ADMIN\_NAME | VARCHAR(100) | 否 | 管理员名称 |
| ADMIN\_SPID | VARCHAR(100) | 否 | 管理员SPID |
| OPERATE\_CONTENT | VARCHAR(200) | 是 | 操作内容 |
| ORIGINAL | VARCHAR(1500) | 否 | JSON串 |
| SIGNATURE | VARCHAR(500) | 否 | 签名值 |
| AUDIT\_STATUS | INTEGER | 默认为0 | 审计状态 |
| AUDIT\_TIME | TIMESTAMP | 是 | 审计时间 |
| AUDITOR\_ID | INTEGER | 是 | 审计员ID |
| AUDITOR\_NAME | VARCHAR(50) | 是 | 审计员名称 |

## 用户日志表（USER\_LOG）

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **类型** | **是否可以为空** | **备注** |
| ID | INTEGER | 非空 | 主键 |
| TIME | TIMESTAMP | 是 | 操作时间 |
| TYPE | VARCHAR(100) | 否 | 操作类型 |
| RESULT | VARCHAR(100) | 否 | 操作结果 |
| DESCRIPTION | VARCHAR(200) | 否 | 描述 |
| USER\_ID | VARCHAR(100) | 否 | 用户ID |
| USER\_NAME | VARCHAR(100) | 否 | 用户名称 |
| OPERATE\_CONTENT | VARCHAR(200) | 是 | 操作内容 |
| AUDIT\_STATUS | INTEGER | 默认为0 | 审计状态 |
| AUDIT\_TIME | TIMESTAMP | 是 | 审计时间 |
| AUDITOR\_ID | INTEGER | 是 | 审计员ID |
| AUDITOR\_NAME | VARCHAR(50) | 是 | 审计员名称 |