**手机软证书服务器**

**设计文档**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 文件编号： | | 生效日期： | | 受控编号： | |
| 密级：秘密 | | 版次：Ver | | 修改状态： | |
| 总页数 |  | 正文 |  | 附录 |  |
| 编制： | | 审核： | | 批准： | |

广东省电子商务认证有限公司

（版权所有，翻版必究）

目录

[1 引言 3](#_Toc531850967)

[1.1 编写目的 3](#_Toc531850968)

[1.2 参考资料 3](#_Toc531850969)

[1.3 系统约束 3](#_Toc531850970)

[2 数据库设计 3](#_Toc531850971)

[3 接口设计 6](#_Toc531850972)

[3.1 注册公钥 6](#_Toc531850973)

[3.2 产生密钥对 6](#_Toc531850974)

[3.3 签名 7](#_Toc531850975)

[3.4 私钥解密 7](#_Toc531850976)

## 引言

### 编写目的

本说明书的编写目的是为了说明 手机软证书服务器 的体系架构，提供系统的数据库设计、接口设计等方面的规范和说明，为系统详细设计人员提供输入参考文档。

### 参考资料

1 《手机软证书设计文档》

### 系统约束

本系统开发过程受以下限制和约束：

|  |  |
| --- | --- |
| 操作系统 | Linux 64位 |
| 开发语言 | JAVA 8以上 64位 |
| 数据库 | MySQL 5.7以上 |
| 网证通中间件 | 5.7以上 |

## 数据库设计

手机软证书服务器的整数据库设计如下所示

* 1. device\_register\_publickey（设备注册公钥表）

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| device\_register\_kid | varchar(64) | 服务器分配的公钥唯一ID |  |
| kty | char(20) | EC |  |
| crv | char(20) | SM2 |  |
| x | varchar(255) | 公钥的x坐标 |  |
| y | varchar(255) | 公钥的y坐标 |  |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

* 1. app\_publickey（公钥表）：保存公钥信息

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| device\_register\_kid | varchar(64) | 服务器分配的公钥唯一ID |  |
| app\_kid | varchar(64) | 公钥的标识 |  |
| kty | char(20) | EC |  |
| crv | char(20) | SM2 |  |
| x | varchar(255) | 公钥的x坐标 |  |
| y | varchar(255) | 公钥的y坐标 |  |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

* 1. app\_privkey（私钥表）：保存服务器私钥

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| app\_kid | varchar(64) | 公钥的标识 |  |
| d2 | blob | 服务器的私钥 |  |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

* 1. enc\_sub\_privkey（加密子私钥表）

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| device\_register\_kid | varchar(64) | 服务器分配的公钥唯一ID |  |
| enc\_sub\_kid | varchar(64) | 加密的子私钥的ID |  |
| sub\_privkey | text | 加密的子私钥 |  |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

* 1. mobile\_code（验证码）

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| req\_no | varchar(64) | 业务编号 |  |
| phone\_no | char(20) | 手机号码 |  |
| validity\_code | char(6) | 验证码 |  |
| validity\_period | int(11) | 验证码有效期 |  |
| hmac\_algo | varchar(10) | Hash算法 |  |
| device\_register\_publickey\_hash | varchar(255) | 注册公钥的Hash值 |  |
| publickey\_hash\_algo | char(10) | 公钥Hash算法 |  |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

* 1. device\_operate\_recode

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

* 1. app\_use\_recode

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

* 1. interface\_log（应用服务接口日志表）

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| name | varchar(32) | 接口名称 |  |
| ip | varchar(64) | 请求ip |  |
| request\_signature | text |  |  |
| request\_payLoad | text | 请求信息 |  |
| response\_msg | text | 响应信息 |  |
| response\_code | int(11) | 响应码 |  |
| http\_code | int(11) | http响应状态码 |  |
| memo | text | 备注，失败时包含异常信息 |  |
| start\_time | datetime | 接口开始时间 |  |
| end\_time | datetime | 接口结束时间 |  |

* 1. system\_config（系统配置）

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | bigint(20) | 编号 | 主键 |
| type | tinyint(2) | 1为签名相关配置项 |  |
| name | varchar(64) | 配置项名称 |  |
| key | varchar (64) | 配置项key |  |
| value | text | 配置项值 |  |
| description | varchar(255) | 描述 |  |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

* 1. sms\_log

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 数据类型 | 注释 | 类型 |
| id | int(10) | 编号 | 主键 |
| sms\_mode | tinyint(3) |  |  |
| sms\_uri | varchar(512) |  |  |
| type | int(10) |  |  |
| status | tinyint(2) |  |  |
| phone | varchar(64) |  |  |
| content | text |  |  |
| resp\_msg | text |  |  |
| memo | text |  |  |
| gmt\_create | datetime | 当前记录创建时间 |  |
| gmt\_modified | datetime | 当前记录最后修改时间 |  |

## 接口设计

### 注册公钥

注册公钥是手机端产生一对密钥对（每个应用一对），把其中的公钥发送给服务器保存。

服务器端注册公钥实现步骤：

1. 验证和解析JWS，获取获取请求内容
2. 解析请求内容，生产服务器端公钥对象模型（DeviceRegisterPublickey）
3. 根据公钥的x坐标和y坐标以及服务器配置的hash算法（public\_key\_hash\_algo）生成公钥hash值（public\_key\_hash\_value）
4. 如果服务器配置了手机短信验证码，验证手机验证码
5. 分配公钥唯一ID（kid），并保存在服务器端公钥对象模型（DeviceRegisterPublickey）
6. 保存注册公钥信息，即持久化服务器端公钥对象模型（DeviceRegisterPublickey）到数据库device\_register\_publickey表
7. 返回kid、public\_key\_hash\_value、public\_key\_hash\_algo给客户端

### 产生密钥对

服务器端产生密钥对实现步骤：

1. 验证和解析JWS，获取获取请求内容
2. 解析请求内容，获取客户端计算点P1
3. 使用中间件内存设备（PseudoDevice）产生随机数d2（服务器端私钥）
4. 通过P1和d2计算真正使用的SM2的公钥p
5. 根据公钥p生成公钥的x坐标和y坐标
6. 生成公钥标识（kid）
7. 封装公钥对象AppPublickey（包括kid、x坐标、y坐标、crv、kty），并持久化到数据库app\_publickey表
8. 封装服务器私钥对象AppPrivkey（包括kid、d2），并持久化到数据库app\_privkey表
9. 返回公钥对象AppPublickey（包含公钥标识kid）给客户端

### 签名

服务器端签名实现步骤：

1. 验证和解析JWS，获取获取请求内容
2. 解析请求内容，获取客户端计算点Q1、整数e’、 签名公钥的标识kid
3. 产生随机数k2，并计算服务器计算点Q2
4. 根据签名公钥的标识kid去数据库app\_privkey表查询服务器私钥对象AppPrivkey，获取服务端私钥d2
5. 产生随机数k3，使用服务器私钥d2、k3生成s2
6. 使用k3、q2生成r
7. 使用r、k2、d2生成s3
8. 返回r、s2、s3给客户端

### 私钥解密

服务器端签名实现步骤：

1. 验证和解析JWS，获取获取请求内容
2. 解析请求内容，获取客户端计算点T1和 签名公钥的标识kid
3. 根据签名公钥的标识kid去数据库app\_privkey表查询服务器私钥对象AppPrivkey，获取服务端私钥d2
4. 使用T1和d2计算服务器计算点T2
5. 将T2转化为x坐标和y坐标返回给客户端