|  |  |
| --- | --- |
| 文档编号 | V1.0 |
| 文档负责人 |  |
| 文档名称 | 短信验证码模块概要设计 |

短信验证码模块概要设计

目录

[目录 2](#_Toc417848221)

[第1章 文档记录 3](#_Toc417848222)

[第2章 引言 4](#_Toc417848223)

[2.1 目的 4](#_Toc417848224)

[2.2 目标读者 4](#_Toc417848225)

[2.3 名词解释 4](#_Toc417848226)

[2.4 文档约定 4](#_Toc417848227)

[第3章 业务流程 5](#_Toc417848228)

[3.1 下发短信验证码 5](#_Toc417848229)

[3.2 验证短信验证码 6](#_Toc417848230)

[第4章 数据库设计 7](#_Toc417848231)

[4.1 短信验证码表 7](#_Toc417848232)

[4.2 短信验证码流水表 8](#_Toc417848233)

[第5章 接口设计 11](#_Toc417848234)

[5.1 账户交易（mvcode\_service） 11](#_Toc417848235)

[5.1.1 下发短信验证码 11](#_Toc417848236)

[5.1.2 验证短信验证码 12](#_Toc417848237)

[第6章 安全设计 13](#_Toc417848238)

# 文档记录

# 引言

## 目的

## 目标读者

## 名词解释

## 文档约定

是否必填项说明

|  |  |  |
| --- | --- | --- |
| 选项 | 全称 | 说明 |
| R | Required | 必需 |
| C | Conditional | 有条件必填 |
| O | Optional | 可选项 |

# 业务流程

## 下发短信验证码



## 验证短信验证码



# 数据库设计

## 短信验证码表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **表名** | 短信验证码信息表 | | **描述** | 记录下发的短信验证码和验证的短信验证码信息 |
|  | sms\_db\_xx.t\_mvcode\_info\_y | |  | 按手机号手三位分库分表 |
| **主键** | | Fmobile\_no+ Ftmpl\_id | | |
| **索引** | |  | | |
| **字段名** | | **类型** | | **说明** |
| Fmobile\_no | | Varchar(32) | | 手机号码 |
| Ftmpl\_id | | bigint | | 短信模板ID |
| Fverify\_code | | Varchar(16) | | 验证码 |
| Frela\_key | | Varchar(128) | | 关联key |
| Frela\_info | | Varchar(1024) | | 关联存储的信息 |
| Fchk\_suc\_times | | Int | | 校验成功的次数 |
| Fchk\_err\_times | | int | | 校验失败的次数 |
| Fclient\_ip | | Varchar(32) | | 用户IP |
| Fsend\_time | | datetime | | 下发时间 |
| Fcheck\_time | | datetime | | 最后一次验证时间 |
| Fexpired\_time | | datetime | | 验证码过期时间 |
|  | |  | |  |
|  | |  | |  |
| Fstandby1 | | bigint | | 预留字段 |
| Fstandby2 | | varchar(255) | | 预留字段 |
|  | |  | |  |

## 短信验证码流水表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **表名** | 短信验证码流水表 | | **描述** | 记录短信验证码流水信息，流水用表来记录下发的所有记录，对于短信网关平台会按条收费，以备查用 |
|  | sms\_db.t\_mvcode\_log\_yyyymm | |  | 按月分表 |
| **主键** | | Fpkid | | |
| **索引** | | Fmobile\_no | | |
| **字段名** | | **类型** | | **说明** |
| Fpkid | | bigint(auto\_increment) | | 流水编号（自增主键） |
| Fmobile\_no | | Varchar(32) | | 手机号码 |
| Ftmpl\_id | | bigint | | 短信模板ID |
| Fverify\_code | | Varchar(16) | | 验证码 |
| Frela\_key | | Varchar(128) | | 关联key |
| Frela\_info | | Varchar(1024) | | 关联存储的信息 |
| Fchk\_suc\_times | | Int | | 校验成功的次数 |
| Fchk\_err\_times | | int | | 校验失败的次数 |
| Fclient\_ip | | Varchar(32) | | 用户IP |
| Fsend\_time | | datetime | | 下发时间 |
| Fcheck\_time | | datetime | | 最后一次验证时间 |
| Fexpired\_time | | datetime | | 验证码过期时间 |
| Fstandby1 | | bigint | | 预留字段 |
| Fstandby2 | | varchar(255) | | 预留字段 |

## 手机号频率受限记录表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **表名** | 手机号频率受限记录表 | | **描述** | 记录手机号下发频率超过限制的信息，需要定期将该表的无效过期记录清除 |
|  | mv\_db.t\_mobile\_limit | |  |  |
| **主键** | | Fpkid | | |
| **索引** | | 唯一索引Fmobile\_no | | |
| **字段名** | | **类型** | | **说明** |
| Fpkid | | bigint(auto\_increment) | | 流水编号（自增主键） |
| Fmobile\_no | | Varchar(32) | | 手机号码 |
| Ftmpl\_id | | bigint | | 短信模板ID，触发受限的短信模板ID |
| Fblock\_stime | | datetime | | 受限制的开始时间 |
| Fblock\_timespan | | int | | 受限制的时长，秒为单位，只有当前时间大于Fblock\_stime+ Fblock\_timespan才解除限制 |

## IP频率受限记录表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **表名** | IP频率受限记录表 | | **描述** | 记录手机号下发的IP频率超过限制的信息，需要定期将该表的无效过期记录清除 |
|  | mv\_db.t\_ip\_limit | |  |  |
| **主键** | | Fpkid | | |
| **索引** | | 唯一索引Fclient\_ip | | |
| **字段名** | | **类型** | | **说明** |
| Fpkid | | bigint(auto\_increment) | | 流水编号（自增主键） |
| Fclient\_ip | | Varchar(32) | | 用户IP |
| Ftmpl\_id | | bigint | | 短信模板ID，触发受限的短信模板ID |
| Fblock\_stime | | datetime | | 受限制的开始时间 |
| Fblock\_timespan | | int | | 受限制的时长，秒为单位，只有当前时间大于Fblock\_stime+ Fblock\_timespan才解除限制 |

# 短信模板

## 短信模板





|  |  |
| --- | --- |
| **字段名** | **说明** |
| timespan | 频率控制的周期，以秒为单位 |
| mob\_no\_limit | 手机号频率值，以条为单位 |
| ip\_limit | ip频率值，以条为单位 |
| blocktime | 超过频率后被限制的时间，以秒为单位 |
| mob\_no\_whitelist | 不受频率限制的手机号白名单，以分号分隔 |
| ip\_whitelist | 不受频率限制的IP白名单，以分号分隔 |
| send\_notify\_sms\_ips | 内部下发通知消息的IP白名单，以分号分隔 |
| id | 短信模板ID，不能重复，在使用时需要人工分配再配置 |
| err\_chk\_times | 验证错误的次数，超过次数则此验证码不再有效 |
| succ\_chk\_times | 验证成功能的次数，用来控制是否可以多次验证，默认取1，即验证成功后不允行再次验证。 |
| expire\_time | 验证码过期时间，过期后验证码失效 |
| use\_relakey | 是否使用关联key进行验证 |
| auth\_code\_len | 验证码长度 |
| tmpl\_text | 模板内容，以$变量名$，$auth\_code$固定为验证码参数，在申请模板时可以定义参数，则验证码下发接口传入参数进行替换 |
|  |  |

# 频率限制

## 频率限制方式

使用缓存来进行频率限制，可以考虑使用memcached来实现。

1. 需要根据sms\_conf.xml中strategy的timespan来设置过期时间
2. 记录发送数量时使用CAS方式计数
3. Strategy中每一个item一个key，手机号的频率限制格式为：sms\_手机号\_timespan值；IP频率限制的格式为：sms\_IP值\_timespan值

# 接口设计

## 短信服务（sms\_service）

### 下发短信验证码

接口说明

xxxx/ smsFacade.hessian的sendMCode方法

功能说明

发送短信验证码

输入参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必填 | 说明 |
| mobile | string | R | 手机号 |
| tmpl\_id | bigint | R | 短信模板ID |
| client\_ip | string | R | 用户IP |
| relation\_key | string | O | 关联的参数，下发时传入，验证时必须传入 |
| relation\_info | string | O | 关联的信息，在验证成功后会将该信息返回 |
| use\_bak\_port | Int | O | 是否使用备用渠道发送 |
| tmpl\_value | map | O | 短信模板的参数值，以key-value的形式传递给验证码模块 |
|  |  |  |  |

输出参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必填 | 说明 |
|  |  |  |  |

内部逻辑

1. 检查输入参数，手机号格式是否正确，模板是否配置
2. 按手机号和IP检查是否超过频率限制（可以考虑使用memcached、mysql内存表、单机缓存等方式来保存频率）
3. 生成验证码
4. 保存验证码，将历史的验证码信息记录流水表中
5. 根据模板和输入参数，生成短信内容
6. 调短信网关下发短信
7. 返回下发结果

### 验证短信验证码

接口说明

xxxx/ smsFacade.hessian的verifyMCode方法

输入参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必填 | 说明 |
| mobile | string | R | 手机号 |
| tmpl\_id | bigint | R | 短信模板ID |
| verify\_code | string | R | 验证码 |
| relation\_key | string | O | 关联的参数，下发时传入，验证时必须传入 |
| client\_ip | string | R | 用户IP |

输出参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必填 | 说明 |
| relation\_info | string | C | 关联的信息，在验证成功后会将该信息返回  验证失败会抛出异常和对应错误码 |
|  |  |  |  |
|  |  |  |  |

内部逻辑

1. 检查输入参数，手机号格式是否正确，模板是否配置
2. 查询当前手机号和模板ID对应的最新验码信息
3. 校验是否超过有效期；校验是否超过验证次数
4. 校验输入的验证码与下发的验证码是否相同，并更新验证相应的结果信息
5. 返回验证结果和关联信息

### 发送通知短信

接口说明

xxxx/ smsFacade.hessian的sendSM方法

功能说明

用于下发通知类短信消息，不同于验证码的下发。比如用于在给用户付款到账后发短信通知已到账。

输入参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必填 | 说明 |
| mobile | string | R | 手机号 |
| tmpl\_id | bigint | R | 短信模板ID |
| client\_ip | string | R | 用户IP |
| use\_bak\_port | Int | O | 是否使用备用渠道发送 |
| tmpl\_value | map | O | 短信模板的参数值，以key=value的形式传递 |
| op\_code | string | R | 内部操码 |

输出参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必填 | 说明 |
|  |  |  |  |

内部逻辑

1. 检查op\_code是否正确
2. 检查输入参数，手机号格式是否正确，模板是否配置
3. 验证IP是否为内部授权IP（下发通知类的消息只有内部白名单的机器可以调用），不再进行频率限制控制。
4. 保存短信消息（将tmpl\_value的值保存到Frela\_info字段中），将历史的短信发送信息记录流水表中
5. 根据模板和输入参数，生成短信内容
6. 调短信网关下发短信
7. 返回下发结果

# 安全设计

1. 需要考虑发送时随意填写手机号乱发送验证码

在下发验证码时对手机号和来源IP做频率限制，按1分钟 、1小时、4小时、1天来限制

1. 防验证码暴力破解

验证码增加有效时长；对验证的次数进行限制，超过次数则不能再进行验证