支付平台设计文档

编制：郝文超 日期：2015.10.08

*变更部分：只在对《设计说明书》做变更时填写，详见《变更控制工作规程》*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **历史修改变更记录** | | | | |
| 版本号 | 变更申请单序号 | 变更时间 | 变更内容（*可用链接方法说明）* | 撰写人 |
|  |  |  |  |  |
|  |  |  |  |  |

目 录

# 程序模块划分

## 程序模块结构图

## 模块说明

## 业务系统

业务系统：使用王府井支付平台进行交易支付的系统，例如王府井商城

## 王府井支付平台

## wfjpay(拆分为api和admin两个应用)

包括前端支付页面、订单查询，状态跟踪、业务数据管理以及与业务系统相关接口

前端：

后端：

## pp

负责与支付宝、易宝等第三方支付平台交互，记录系统交易流水、充值方式等

负责与wfjpay交互，返回交易数据等

负责发送通知消息到MQ

--非但应用,通道独立

## payTiming

定时任务模块

* 程序执行完业务处理后。如果业务系统没有反馈处理信息给支付平台，支付平台服

务器会不断重发通知，直到

超过24 小时 22 分钟。

一般情况下，25 小时以内完成8 次通知（通知的间隔频率一般是：

2m,10m,20m,1h,2h,6h,15h）

每隔一分钟定时轮询订单表，所有已支付的未完成的订单需要触发消息通知机制

* 负责过期订单处理，平台约定48小时内有效
* 发送产品运营统计报表邮件(也可单独统计模块或BI出)
* 程序每10秒查询系统中3分钟内未支付的交易，到各渠道进行单笔查询，如果支付成功更新状态并通知第三方
* 负责归档处理，将前3年数据定时归档

## 第三方支付平台

第三方支付平台包括：支付宝、易宝、财付通等成熟的支付平台，提供了各种银行以及业务支付接口供王府井支付平台使用。

# 名词定义

|  |  |
| --- | --- |
| **名称** | **描述** |
| **业务系统** | 如王府井网站等接入王府井支付平台的应用 |
| **王府井支付平台** | 具有支付功能的王府井核心支付业务平台 |
| **第三方支付平台** | 如支付宝、易宝、财付通等成熟的第三方支付平台 |
| **返回** | 页面跳转同步通知。王府井支付平台根据得到的数据处理完成后，当前页面从第三方支付平台的页面自动跳转回业务系统的网站，同时携带处理完成的结果信息反馈给业务系统。 |
| **请求** | 通过 HTTP、HTTPS 协议把需要传输的数据发送给接收方的过程。 |
| **通知** | 服务器异步通知。王府井支付平台根据得到的数据处理完成后，主动发起通知给业务系统，同时携带处理完成的结果信息反馈。 |
| **订单总金额** | 单次订单支付中的支付金额 |
| **支付账号** | 王府井的用户通行证账号 |
| **渠道** | 充值渠道。例如支付宝、易宝等第三方充值平台 |

# 角色定义

# 数据库说明

订单 日志 通知参数做分区表



# 功能介绍

## 5.1管理端功能

### 5.1.1业务平台签约

#### 5.1.1.1功能描述

业务系统（如网站）接入支付支付平台，需要首先在支付平台进行签约。管理员在管理后台输入业务平台的名称，描述、收款帐号（支付宝、财富通、银联帐号等）、系统自动为业务平台生成加密密钥。

#### 5.1.1.2流程图

无

#### 5.1.1.3主要界面

无

#### 5.1.1.4主要字段

|  |  |  |  |
| --- | --- | --- | --- |
| 中文名称 | 英文名称 | 类型 | 备注 |
| 自动编号 | ID | 数字 | 从1000000开始 |
| 业务平台名称 | BP\_NAME | 字符串 |  |
| 业务平台描述 | DESCRIPTION | 字符串 |  |
| 密匙 | BP\_KEY | 字符串 | 分配给业务平台的密匙（MD5加密小写字符串），用于请求校验 |
| 状态 | STATUS | 数字 | 0未启用（默认值） 1启用 |

### 5.1.2交易查询

#### 5.1.2.1功能描述

业务方登陆支付平台管理端，通过检索条件[业务平台（权限筛选）、业务订单编号、交易流水号、支付渠道、时间范围]查询符合条件的交易记录。

业务方可以根据查询条件查询并导出excel表格。

#### 5.1.2.2流程图

#### 5.1.2.3主要界面

#### 5.1.2.4主要字段

### 5.1.3交易轨迹查询

#### 5.1.3.1功能描述

管理员或者业务方可以查询某笔交易的交易轨迹。

### 5.1.4网关配置

管理员可以为签约的业务平台配置支持的支付网关。

## 5.2服务介绍

交互时序：





### 5.2.1交易请求（PC端）

命令类型:directPay

请求参数：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **含义** | **类型** | **长度** | **必填** | **说明** |
| bpId | 业务平台ID | String | 16 | 是 | 分配给业务系统的标识 |
| sign | 签名 | String | 255 | 是 | 把相关参数结合在一起通过MD5加密得出的结果，具体加密方法参见本文档附录一中的[签名机制](#_签名机制) |
| bpOrderId | 业务平台订单编号 | Number | 100 | 是 | 业务系统的订单唯一标识 |
| goodsName | 商品名称 | String | 100 | 是 | 购买的商品名称（不能包含#、&、%、+等特殊字符，敏感词汇，且仅支持中英文） |
| totalFee | 订单总金额 | Number |  | 是 | 单位为RMB元，范围[0.01，99999999.99]，精确到小数点后两位 |
| content | 订单内容 | String | 100 | 是 | （不能包含#、&、%、+等特殊字符，敏感词汇，且仅支持中英文） |
| remark | 订单备注 | String | 128 | 否 | （不能包含#、&、%、+等特殊字符，敏感词汇，且仅支持中英文） |
| bpParams | 业务平台回传参数 | String | 200 | 否 | 如果用户请求时传递了该参数，则返回给业务平台时会回传该参数（不能包含#、&、%、+等特殊字符，敏感词汇，且仅支持中英文） |
| notifyUrl | 异步通知地址 | String | 100 | 否 | 用于支付完毕后支付平台回调应用平台处理业务 |
| returnUrl | 页面重定向通知地址 | String | 100 | 否 | 支付完毕用，支付平台进行重定向的地址 |
| showUrl | 商品展示的链接地址 | String | 100 | 否 |  |
| orderUrl | 订单详情页面地址 | String | 100 | 否 | 业务平台的订单详情页 |
| unid | 用户的unid | String | 32 | 是 |  |
| antiPhishingKey | 防钓鱼时间戳 | String | 200 | 是 | 通过时间戳查询接口获取的加密支付平台时间戳。 |

**返回值:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **含义** | **类型** | **长度** | **必填** | **说明** |
| isSuccess | 创建订单成功标识 | String | 20 | 是 | 成功:true  失败:false |
| errCode | 接口错误编码 | String | 255 | 否 |  |
| errMessage | 接口反馈消息 | String | 255 | 否 | 失败时的接口错误信息提示 |
| orderTradeNo | 支付平台订单唯一表示 | String | 255 | 否 | 支付平台生成的订单编号 |
| totalFee | 订单总金额 | String | 255 | 是 |  |
| content | 订单描述 | String | 2000 | 否 |  |
| account | 用户登录帐号 | String | 32 | 是 |  |

注意：

* 此接口只支持https请求
* 此接口只支持utf-8编码
* 此接口只支持POST方式提交
* 请按照“签名机制”中的签名方法对输入参数进行签名，该接口才能够被支付平台正确接收处理

### 5.2.2获取防钓鱼时间戳

通过防钓鱼时间戳查询接口获取的支付平台系统时间戳地址。

https://pay.wangfujing.com /api/generateAntiPhishingKey.do

### 5.2.3页面跳转同步返回数据

支付平台对业务系统的支付请求数据处理完成后，会将处理的结果数据通过系统程序控制客户端页面自动跳转的方式返回给业务系统。

业务系统仅需要在提交交易请求的时候传入returnUrl参数（如没有传入，使用业务平台签约时候的returnUrl）即可，如http://www.wangfujing.com/order/pay/returnUrl.do

**返回值:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 参数 | 含义 | 类型 | 长度 | 必填 | 说明 |
| tradeStatus | 交易状态 | String | 10 | 是 | 接口调用是否成功，success：成功；failure：失败；timeout:订单已超时 |
| notifyType | 通知方式 | String | 10 | 是 | 支付平台通知业务平台的类型；页面跳转的同步通知：rediectNotify，后台异步通知：asynNotify |
| sign | 签名 | String | 255 | 是 | 把相关参数结合在一起通过MD5加密得出的结果，具体加密方法参见本文档附录一中的签名机制 |
| bpOrderId | Bp平台的订单ID | String | 255 | 是 | 业务系统的订单唯一标识 |
| totalFee | 订单总金额 | Number |  | 是 | 单位RMB元，范围[0.01，100000000]，精确到小数点后两位 |
| orderTradeNo | 支付平台订单流水号 | String | 500 | 是 | 支付平台的订单标识 |
| payTime | 付款时间 | Long |  | 是 | 用户成功付款的完成时间 |
| notifyId | 通知校验ID | String | 200 | 是 |  |
| payType | 支付渠道 | String | 20 | 是 | 如通过支付宝支付:ALIPAY |
| unid | 用户登录帐号的unid | String | 128 | 是 | 对应请求时的帐号unid，原样返回 |
| bpParams | 回传参数 | String | 128 | 否 | 对应请求时的回传参数 |
| payBank | 支付银行简码 | String | 32 | 否 | 支付银行的简码 |

### 5.2.4服务器异步通知数据

支付平台对业务系统的请求数据处理完成后，会将处理的结果数据通过服务器主动通知的方式通知给业务系统。

业务系统仅需要在提交交易请求的时候传入notifyUrl参数（如没有传入，使用业务平台签约时候的notifyUrl）即可，如http://www.wangfujing.com/order/pay/notifyUrl.do

**返回值:同5.2.3**

### 5.2.5校验是否是支付平台通知

验证此次通知信息是否是支付平台服务器发来的信息，以帮助校验反馈回来的数据的

真假性。

* 工作原理

获取支付平台返回数据之一的通知校验ID（notifyId），按照支付平台要求的格式拼接成要请求的链接，其中orderTradeNo为支付平台返回给业务平台的支付平台订单流水号，notifyId为支付平台对于的返回参数。如：

https://pay.wangfujing.com /api/verifyNotifyId.do? orderTradeNo=20130424101004104528164&notifyId=e037c198f9ca4f9a87962f8eae776825

返回的信息即为验证是否成功，返回true表示成功，返回false表示失败

通过访问这个请求链接，利用编程方法来模拟https请求与支付平台服务器进行交 互，获得支付平台服务器上处理的结果。如果获得的信息是true，则校验成功；如果获 得的信息是其他，则校验失败。

### 5.2.6单笔交易查询

命令类型:singleTradeQuery

请求参数：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **含义** | **类型** | **长度** | **必填** | **说明** |
| bpId | 业务平台ID | String | 16 | 是 | 分配给业务系统的标识 |
| bpOrderId | 业务平台订单编号 | Number | 100 | 是 | 业务系统的订单唯一标识 |

返回值：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参数** | **含义** | **类型** | **长度** | **必填** | **说明** |
| isSuccess | 创建订单成功标识 | String | 20 | 是 | 成功:true  失败:false |
| errCode | 接口错误编码 | String | 255 | 否 | 失败时的接口错误信息编码 |
| errMessage | 接口反馈消息 | String | 255 | 否 | 失败时的接口错误信息提示 |
| bpId | 业务平台ID | String | 16 | 是 | 分配给业务系统的标识 |
| bpOrderId | 业务平台订单编号 | Number | 100 | 是 | 业务系统的订单唯一标识 |
| orderTradeNo | 支付平台订单唯一表示 | String | 255 | 否 | 支付平台生成的订单编号 |
| totalFee | 订单总金额 | String | 255 | 是 |  |
| status | 状态 | String |  |  | 1 等待付款  2 已付款  3 已取消  4 失败  5 已删除 |
| payDateFormat | 支付时间 | String | 32 |  | 支付时间时间戳，如1372316309811，需要new Date（1372316309811L）格式化 |
| payType | 支付渠道 | String | 20 |  | 如通过支付宝支付:ALIPAY |
| payBank | 支付银行 | String | 32 |  |  |
| bpParams | 透传参数 | String | 200 |  |  |
| payUnid | 完成支付的用户unid | String | 32 |  |  |

### 5.2.7获取网关列表

暂无，依赖于业务线网关配置

# 6签名机制

## 6.1生成签名参数说明

### 6.1.1.需要参与签名的参数

在请求参数列表中，除去sign、sign\_type(MD5，默认MD5一期不考虑其他加密方式，所以不使用sign\_type参数)四个参数外，其他需要使用到的参数皆是要签名的参数。（空值参数不要参与签名，个别接口中参数sign\_type也需要参与签名。）

在通知返回参数列表中，除去sign、sign\_type两个参数外，凡是通知返回回来的

参数皆是要签名的参数。

### 6.1.2.业务平台密钥参数说明

业务平台密钥，下面简称密钥（常用代码变量名为bpKey）。支付平台会给每个业务系统分配一个（需向支付平台申请，业务平台ID即bpId也需要申请），在生成签名时，需要密钥参与签名。密钥是以英文字母和数字组成的 32位字符串。

## 6.2.生成签名规则

### 6.2.1.生成待签名字符串

对于如下的参数数组：

string[] parameters={

"service=create\_direct\_pay\_by\_user",

"partner=2088101568338364",

"returnUrl= http://www.test.com/alipay/returnUrl.asp",

"out\_trade\_no=6741334835157966",

"subject=贝尔金护腕式",

"payment\_type=1 ",

"seller\_email=alipay-test01@alipay.com",

"total\_fee=100"

};

对数组里的每一个值从 a 到 z 的顺序排序，若遇到相同首字母，则看第二个字母，

以此类推。

排序完成之后，再把所有数组值以“&”字符连接起来，如：

out\_trade\_no=6741334835157966&partner=2088101568338364

&payment\_type=1&returnUrl=http://www.test.com/alipay/returnUrl.asp&sell

er\_email=alipay-test01@alipay.com&service=create\_direct\_pay\_by\_user&subje

ct=贝尔金护腕式&total\_fee=100

这串字符串便是待签名字符串。

注意：

1. 根据HTTP 协议要求，传递参数的值中如果存在特殊字符（如：&、@等），

那么该值需要做URL Encoding，这样请求接收方才能接收到正确的参数值。这

种情况下，待签名数据应该是原生值而不是encoding 之后的值。例如：调用某

接口需要对请求参数email 进行数字签名，那么待签名数据应该是

email=test@msn.com，而不是email=test%40msn.com。

### 6.2.2.MD5 签名

*  请求时签名

当拿到请求时的待签名字符串后，需要把私钥直接拼接到待签名字符串后面，形成

新的字符串，利用MD5 的签名函数对这个新的字符串进行签名运算，从而得到32

位签名结果字符串（该字符串赋值于参数sign）。

* 通知返回时验证签名

当获得到通知返回时的待签名字符串后，同理，需要把私钥直接拼接到待签名字符

串后面，形成新的字符串，利用MD5的签名函数对这个新的字符串进行签名运算，

从而得到 32 位签名结果字符串。此时这个新的字符串需要与支付平台通知返回参数

中的参数 sign 的值进行验证是否相等，来判断签名是否验证通过。

## 6.3实例

**伪代码：**

Begin

输入：参数数组

string[] parameters=

{

'unid=12046121',  
'antiPhishingKey=1234567891011',  
'bpId=10068',  
'content=实例',  
'goodsName=伪代码',  
'totalFee=1000000',

……(其他参数)

};

parameters=字典表排序(parameters)

while(parameter<parameters){

prestr+=parameter+'&'

}

prestr=删除末尾'&'字符(prestr);

prestr=prestr+([业务平台密钥](#_6.1.2.业务平台密钥参数说明))

sign = md5加密（sign）

End

### 6.3.1 Java实例（仅供参考）

或者可以引入项目OrderEncrypt，参考OrderEncryptUtilTest类中的测试方法.

/\*\*

\* 生成签名

\*

\* **@param**sArray

\* 要签名的数组

\* **@param** key

\* 为支付平台分配给业务平台的密钥

\* **@return**签名结果字符串

\*/

**publicstatic** String buildMysign(Map<String, String>sArray, String bpKey) {

List<String> keys = **new**ArrayList<String>(sArray.keySet());

// 按字典表顺序排序

Collections.sort(keys);

// 待签名字符串

String prestr = **null**;

// 拼接参数

**for** (String key : keys) {

String value = sArray.get(key);

prestr = prestr + key + "=" + value + "&";

}

prestr.substring(0, prestr.length() - 1);

// 把拼接后的字符串再与业务平台密钥直接连接起来

prestr = prestr + bpKey;

//进行md5加密（该例子中用Alipay提供的md5加密方式）

String sign = AlipayMd5Encrypt.*md5*(prestr);

**return** sign;

}

### 6.3.2 PHP实例（仅供参考）

//设置参数  
$paramsArr= array(  
'antiPhishingKey'=>$timestamp,  
'bpId' =>'10000',  
'bpOrderId' =>$insertId,  
'content' =>self::ACT\_NAME,  
'goodsName' =>self::ACT\_NAME,  
'notifyUrl' =>'http://xxx.wangfujing.com/order/returnUrl.do',  
'returnUrl' =>' http://xxx.wangfujing.com/api/notifyUrl.do ',  
'totalFee' =>$price,  
'unid' =>$\_SESSION[self::QIANZHUI.'\_userid'],  
);  
//参数排序  
ksort($paramsArr);  
$sign = '';  
//拼接参数  
foreach($paramsArras$k=>$v){  
$sign .= $k . '=' . $v .'&' ;  
}  
$sign = trim($sign,'&');  
//尾部拼接业务平台密钥，并进行md5码加密  
$paramsArr['sign'] = md5($sign.'密钥');

# 7注意事项

当支付平台处理完成后，支付平台会把处理结果以当前页面跳转同步通知和支付平台服务器主动通知业务系统两种形式，反馈给业务系统。业务系统可以从页面跳转同步通知页面或者从服务器异步通知页面中获得这些信息，并且在验证通过的判断中增加的业务逻辑处理程序。当业务有传递参数notifyUrl（服务器异步通知页面路径）或returnUrl（页面跳转同步通知页面路径）时，业务系统必须判断商户网站中是否已经对该次的通知结果数据做过同样处理。**如果不判断，存在潜在的风险，业务系统自行承担因此而产生的所有损失**。