**商户端API（Web Payment）接口说明**

**[MustangPay平台]**

版本记录

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **日期** | **编写** | **备注** |
| 1.O | 2024/09/26 | Hyssop | 1、1.1系统对外商户升级版本 |

目录

[1. 接入说明 2](#_Toc1269315037)

[1.1 通讯方式 2](#_Toc275277561)

[1.2 字符编码 2](#_Toc910192089)

[1.3 同步接口 2](#_Toc1072422242)

[1.4 异步接口 2](#_Toc370372023)

[1.5 通知接口 2](#_Toc1434981555)

[1.6 IP白名单 3](#_Toc1493639075)

[1.7 请求(响应)报文格式说明(JSON) 3](#_Toc1655583742)

[1.7.1. 报文字段类型说明 3](#_Toc450337615)

[1.7.2. 报文所有参数（JSON） 3](#_Toc1091923277)

[1.7.3. 请求报文头head格式（JSON） 4](#_Toc1706752924)

[1.8 签名机制 4](#_Toc1457320689)

[1.8.1. AES加解密 4](#_Toc1137825988)

[1.8.2. RSA签名 4](#_Toc99503781)

[1.8.3. 加密签名顺序(请求方) 4](#_Toc1617769901)

[1.8.4. 验签解密顺序(接收方) 5](#_Toc568271440)

[2. 接口说明（报文体body） 5](#_Toc1078313871)

[2.1. 预下单接口（同步接口） 6](#_Toc606732864)

[2.2. 商户订单查询接口 （同步接口） 7](#_Toc1106889292)

[2.3. 商户异步通知接口（异步接口） 9](#_Toc1984980330)

[3. 附录 9](#_Toc405950165)

[3.1. 接口返回码列表 9](#_Toc248876636)

[3.2. payMethod类目 11](#_Toc1718960543)

[3.3. orderStatus订单状态 11](#_Toc472343110)

[3.4. currency币种 11](#_Toc1571090458)

[3.5. Country国家 11](#_Toc2005887741)

[4. 注意事项 12](#_Toc1756972381)

[4.1. 联调注意事项 12](#_Toc1534661217)

[4.2. 上线注意事项 12](#_Toc1772473649)

[5. POSTMAN 12](#_Toc71467559)

[6. 接入代码（java） 12](#_Toc711905440)

[6.1. jar包 12](#_Toc1363332643)

[6.2、测试环境公私钥 13](#_Toc2028701058)

[6.2.1、mustangPay的公私钥 13](#_Toc780818387)

[6.2.2、商户公私钥 13](#_Toc2089547139)

[6.2.3、线上公私钥交换 14](#_Toc1218685782)

[7、 环境信息 14](#_Toc1900396635)

# 接入说明

## 通讯方式

所有报文域以Json字符串的形式，通过HTTPS POST请求方式发送；

本平台接口采用同步接口、异步接口（同步请求受理、异步通知最终结果方式）2种受理机制。

## 字符编码

API接口中传输、加密等所有需要编码都采用UTF-8字符集。

## 同步接口

商户通过API接口请求到MustangPay平台（以下简称‘平台’），平台会同步响应接口定义的响应参数数据，不再有后续流程，一次性完成。

## 异步接口

商户通过API接口请求到平台，平台会同步响应请求的接收状态，最终订单结果通过商户提供的通知地址通知到商户或商户主动调用平台提供的对应查询接口获取订单最终结果。

## 通知接口

商户接到异步通知返回字符串SUCCESS表示接收通知成功，需要商户主动来调用查询接口查询或者通过人工方式核实 。

## IP白名单

双方都要提交接口请求的IP白名单配置到各自系统中，接口发送的时候都要做IP白名单判断，对于是合法的IP白名单才能允许放行，否则直接返回IP限制错误。

IP绑定只能通过人工方式绑定，需要联系Mustangpay工作人员申请。

## 请求(响应)报文格式说明(JSON)



### 报文字段类型说明

|  |  |
| --- | --- |
| 字段 | 说明 |
| country | 只支持（ZAF） |
| currency | 只支持（ZAR） |
| amount | Amount类型  Long value;  String currency;//ZAR |



### 报文所有参数（JSON）

*所有接口的请求和响应都是JSON格式，都包含以下字段,参考：*

{

"merchantId": "240717251000200170",

"encryptData": "",

"encryptKey": "gtHWDQdKvgPGEheZWaZzfoAiYp40jqtkisDHFhvD0jee1gdJUZN0TS7Cl4WRncVocpA6PU3wkdvoBaq\_IsM1VukiV2MnEkmzNFgfWGTVg0EP9x2XRCCisdLzfNxBs6DaXlCASBj-BvQA4uaMfxoRbw22MNsy-88WSPI5BxoPSaI"

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 说明 | 类型 | 是否必输 | 备注 |
| merchantId | 商户订单号 | String | Y | 商户入网，mustangPay给到商户的唯一商户号。 |
| head | 报文头 | Text | Y | JSON,参考《请求/响应报文头head格式》 |
| encryptData | 密文 | FixStrin（1024） | Y | 参考 签名机制 |
| encryptKey | 密文 | Text | Y | 参考 签名机制 |

### 请求报文头head格式（JSON）

{"version":"1.0","reqTime":"2020-07-24T11:32:40+08:00"}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 说明 | 类型 | 是否必输 | 备注 |
| version | 接口版本号 | FixString（3） | Y | 1.0 |
| reqTime | 时间戳 | Datetime | Y | 发送报文的时间戳  yyyy-MM-dd'T'HH:mm:ssXXX |

## 签名机制

为保证数据传输过程中的数据真实性，完整性和不可抵赖，我们需要对数据进行数字签名，在接收签名数据之后进行签名校验。签名算法为RSA。签名是为了防止从商户系统提交的请求以及通知数据被非法篡改。



### AES加解密

AES加密，算法为AES算法的GCM模式进行加密，数据采用PKCS#7填充。

### RSA签名

商户与平台各自生成一对RSA公钥文件(public.key)和私钥钥文件(private.key)，位数1024格式为PKCS#8，并双方交换公钥文件(public.key)；

签名方式使用算法：Sha256WithRSA。



### 加密签名顺序(请求方)

*适合接口请求方组织请求数据的签名 和 接口接收方响应数据的签名*

1. 按照各接口要求，生成原始JSON格式的报文头head：srcHead和报文体body：srcBody；
2. 将srcBody包装成JSON字符串。
3. 将JSON字符串按照SerializerFeature.MapSortField排序

使用商户的私钥和RSA工具包签名，签名的值放置到步骤1的JSON对象当中（字段名称：sign）

1. 再一次按照json的排序方法SerializerFeature.MapSortField进行排序。
2. 生成一个随机的aesKey
3. 用随机的aesKey加密步骤4的json字符串的报文。
4. 使用mustangpay的公钥加密aesKey
5. 将其包装成包括以下三个字段的json对象传给mustangPay.
6. 被加密的aesKey的值放置到encryptKey.
7. 将加密报文放置到encryptData字段当中.
8. 商户号用merchantId字段传。

### 验签解密顺序(接收方)

*适合接口接收方数据验证签名 和 接口请求接收到响应数据的验证签名。*

1. 获取到mustangPay的报文之后。encryptData为加密报文。encryptKey为加密密钥.
2. 要使用mustangPay给到商户的公钥为数据进行验签。
3. 获取encryptKey和encryptData内容

用商户自己的私钥解密encryptKey，获取到加密报文的aesKey

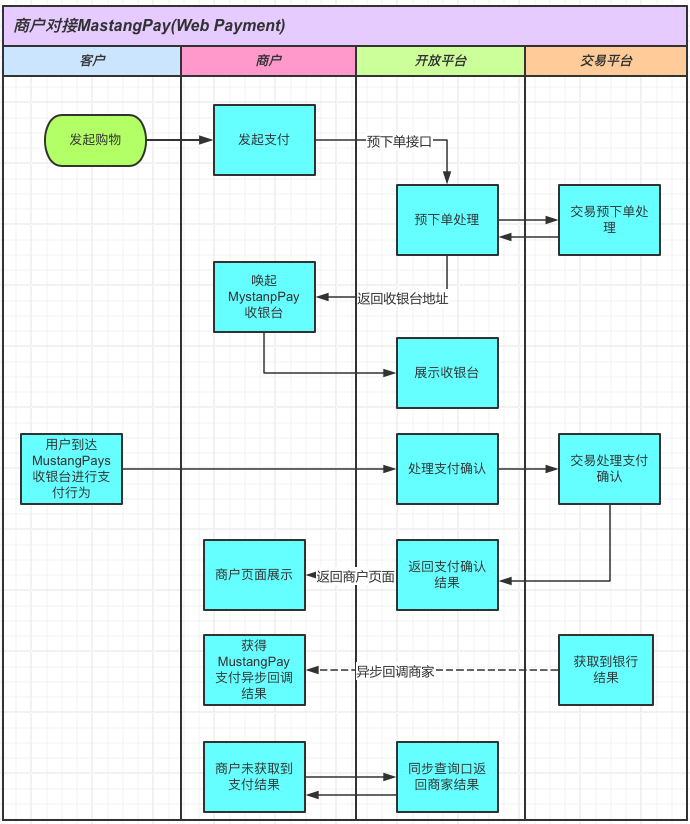
用AES算法，用解析出来的aesKey解密encryptData获得originalData。

originalData包装成fastJson对象originalDataObj

originalDataObj中取出来sign字段，并将sign排除originalDataObj对象当中

有了sign字段，有了mustangPay的公钥和originalDataObj，使用rsa算法就可以验证签名是否通过。

# 接口说明（报文体body）



处理流程图

## 预下单接口（同步接口）

请求url: /openApi/merchant\_direct/cashier/preorder（域名见7）

请求方式：POST

请求body包含字段：

{

"merchantId": "240717251000200170",

"merchantName": "",

"reference": "merchantOrderNo\_14dd90e38590", //商户订单号

"amount": 1000,

"currency": "ZAR",

"country": "ZA",

"businessType": "MerchantAcquiring",

"remark": "remark\_83c200fa64ff",

"callbackUrl": "https://mustangpay-test-demo-dev.mstpay-inc.com/callback",

"returnUrl": "https://mustangpay-test-demo-dev.mstpay-inc.com",

"cancelUrl": "",

"ip": "127.0.0.1",

"product": {

"name": "productname",

"shortName": "short",

"description": "productDesc",

"mobile": "18518245678"

},

"expireAt": 30,

"vat": 10,

"vatNumber": "1234"

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **是否必填** | **长度限制** | **参考值** |
| merchantId | String | 必填 | 32 | 240717251000200170 |
| reference | String | 必填（商户单号） | 64 | merchantOrderNo\_14dd90e38590 |
| amount | Amount | 必填（金额） private Long value; private String currency; |  | {"value": 10, "currency": "ZAR"} |
| currency | String | 必填ZAR |  | ZAR |
| country | String | 必填ZAF |  | ZAF |
| businessType | String | 非必填 默认MerchantAcquiring | 64 | MerchantAcquiring |
| remark | String | 非必填，标注 | 255 | remark\_83c200fa64ff |
| callbackUrl | String | 商户回调地址（必填） | 255 | callbackUrl |
| returnUrl | String | 商户返回地址（必填） | 255 | returnUrl |
| cancelUrl | String | 用户取消订单返回商户地址（非必填） | 255 | (空值) |

*响应body包含字段：*

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **描述** | **参考值** |
| code | String | 六个0表示成功，非六个0表示报错 | 000000 |
| message | String |  | ok |
| data | Object |  | { ... } |
| - reference | String | 商户单号 | merchantOrderNo\_14dd90e38590 |
| - orderNo | String | 订单号 | 240719101001007914 |
| - orderStatus | String | 订单状态 | Initial |
| - amount | Amount | 订单金额 | {"value":100000,"currency":"ZAR"} |
| - vat | Amount |  | {"value":100000,"currency":"ZAR"} |
| - errorCode | String | 错误码 | (null) |

## 商户订单查询接口 （同步接口）

*请求url: [openApi/merchant\_direct/cashier/getOrderStatusByMerchantOrderNo](http://110.238.76.97:8777/openApi/merchant_direct/cashier/getOrderStatusByMerchantOrderNo)(域名见7)*

*请求方式：POST*

*请求body包含字段：*

*{*

*"merchantId": "240717251000200170",*

*"reference": "merchantOrderNo\_14dd90e38590"*

*}*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 说明 | 长度 | 是否必输 | 备注 |
| merchantId | 商户id | 32 | Y | MustangPay分配 |
| reference | 商户订单号 | 64 | Y | 商户侧下单号 |

*响应body包含字段（如果code非000000则返回的body中的errorCode和errorMessage是错误信息）：*

{

"merchantId": "123456789",

"merchantOrderNo": "240909011103192628533242",

"orderNo": "IN20230101",

"orderStatus": "Success",

"merchantName": "Example Merchant",

"vatNumber": "VAT123456",

"errorCode": "0",

"errorMessage": "No error",

"amount": {

"value": 100.00,

"currency": "ZAR"

}

}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段** | **说明** | **长度** | **是否必输** | **备注** |
| merchantId | 商户ID | 32 | 是 | 唯一标识商户的ID |
| merchantOrderNo | 商户订单号 | 64 | 是 | 商户生成的订单号 |
| orderNo | 订单号 | 32 | 是 | 系统生成的唯一订单号 |
| orderStatus | 订单状态 | 8 | 是 | 订单的当前状态 |
| merchantName | 商户名称 | 32 | 否 | 商户的名称 |
| vatNumber | 增值税号码 |  | 否 | 商户的增值税号码 |
| errorCode | 错误代码 | 4 | 否 | 错误时返回的状态码 |
| errorMessage | 错误信息 | 16 | 否 | 错误描述信息 |
| amount | 订单金额信息（对象） | Amount | 是 | 包含订单金额的详细信息 |

## 商户异步通知接口（异步接口）



*请求body包含字段：*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 说明 | 长度 | 是否必输 | 备注 |
| orderNo | String | 32 | 是 | 订单号 |
| merchantId | String | 32 | 是 | 商户id |
| merchantOrderNo | String | 64 | 是 | 商户订单号 |
| orderStatus | String | 32 | 是 | 订单状态，见附录3.3 |
| errorCode | String | 32 | 否 | 错误码 |
| errorMessage | String | 255 | 否 | 错误信息 |
| amount | Amount |  | 是 | 金额 |
| -value | long |  | 是 | 金额-Cents |
| -currency | String | 8 | 是 | 币种-ZAR |

# 附录

## 接口返回码列表

***对应返回码列表中没有定义的返回码，请不要处理，将交易暂停，联系平台技术协助查询原因。***

|  |  |  |
| --- | --- | --- |
| **返回码** | **描述** | **处理意见** |
| **000000** | **请求成功** | **明确请求接受成功。**  **对于异步接口，只表示接受状态，不代表实际处理状态，最终处理状态还需要通过被动接受回调通知接口或主动请求查询接口判断实际处理结果。** |
| 100022 | payMethod传错等 | 系统异常。 |
| 100018 | 传递的payMethod，该商户不支持 | 请求失败，请技术查明问题。 |
| 100002 | 系统异常 | 请求失败，请技术查明问题。 |
| 030380 | 系统异常 | 请求失败，请技术查明问题。 |
| 03015 | IP没有访问权限 | 请求失败，请技术查明问题。 |
| 06001 | Transaction is being processed | Pending |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## payMethod类目

|  |  |  |
| --- | --- | --- |
| **编码** | **描述** | **备注** |
| CardPayment | 卡支付 |  |
| InstantEFT | eft支付 |  |

## orderStatus订单状态

|  |  |  |
| --- | --- | --- |
| **编码** | **描述** | **备注** |
| Initial | 预下单 |  |
| Pending | 处理中 |  |
| Success | 成功 |  |
| Fail | 失败 |  |
| Return | 退票 |  |
| Close | 超时关单 |  |

## currency币种

|  |  |  |
| --- | --- | --- |
| **编码** | **描述** | **备注** |
| ZAR | 南非兰特 | 币种 |
|  |  |  |

## Country国家

|  |  |  |
| --- | --- | --- |
| **编码** | **描述** | **备注** |
| ZAF | 南非 |  |

# 注意事项

## 联调注意事项

1. 联调出款接口前需要先联调用户签约接口，否则出款会失败。
2. 由于联调环境和测试是同一套环境，因此联调环境不是真实打款。
3. 商户支持的支付方式（payMethod）是签约时候商定好，由研发人员维护进测试数据的。

## 上线注意事项

使用MustangPay api提供的方法生成公私钥。公钥发送给工作人员邮箱：[hyssop.zhang@mustangcash.com](mailto:hyssop.zhang@mustangcash.com)

私钥妥善保管，不要泄露。

# POSTMAN



# 接入代码（java）

## jar包

Mustangpay有demo代码，会在商户对接的过程当中提供代码。

## 6.2、测试环境公私钥

### 6.2.1、mustangPay的公私钥

|  |  |
| --- | --- |
| **公钥** | MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkip3xt6L5hJiLpXH6hpQ1u3ecFdAMoOvhFlAZ/BGzBurI1SnhLIEA7NGd7TgwBTm3AekqHxy6/li3NkOWuQX4ddkYxqWCMjsV/V/TSdTkgeC5h2V1dt7s2jTjuH21NzWG2Muor3FIM4Cof1bEDT8j8+Vi0wxUoYwT3Au9yMqWmyyMphKs6rD6K44Dkuk4Q0eDHybKBjjLSTCtgLPkC1I7B+/P4lfSmMBbsOZUc6ujajOl3VxwzB5EN20LVuUTdLPE9JHI/jpdjsbxDtxbtGRqEs/cw9CTbznFP36jg0wEmha1tBIAqvBthEmcRI7xBPdlIjMZqo+ZjagGnKGhcy3bQIDAQAB |

### 6.2.2、商户公私钥

|  |  |
| --- | --- |
| 公钥 | MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkip3xt6L5hJiLpXH6hpQ1u3ecFdAMoOvhFlAZ/BGzBurI1SnhLIEA7NGd7TgwBTm3AekqHxy6/li3NkOWuQX4ddkYxqWCMjsV/V/TSdTkgeC5h2V1dt7s2jTjuH21NzWG2Muor3FIM4Cof1bEDT8j8+Vi0wxUoYwT3Au9yMqWmyyMphKs6rD6K44Dkuk4Q0eDHybKBjjLSTCtgLPkC1I7B+/P4lfSmMBbsOZUc6ujajOl3VxwzB5EN20LVuUTdLPE9JHI/jpdjsbxDtxbtGRqEs/cw9CTbznFP36jg0wEmha1tBIAqvBthEmcRI7xBPdlIjMZqo+ZjagGnKGhcy3bQIDAQAB |
| 私钥 |  |

### 6.2.3、线上公私钥交换

使用demo代码当中的MerchantRsaKeyCreateTest生成公私钥，私钥用于商户自己解密mustangpay返回的加密数据：验签和解密 !!! [发送公钥到邮箱hyssop.zhang@mustangcash.com。](mailto:发送公钥到邮箱hyssop.zhang@mustangcash.com。)

# 环境信息

|  |  |
| --- | --- |
| 测试环境地址 | https://openapi-dev.mstpay-inc.com |
| 线上调试地址 | https://openapi.mustangpay.co.za |
|  |  |