

CRM 租户自接支付通道接口

V1.3

2022-12-14

名词定义

名词	说明	提供方	示例
payKey	一个长度为 32 的字符串，用于签名与验签中的加密串	Haame	F5D43C246B3B4AB6BF000E07056610B2
支付 URL	租户自行开发实现的支付接口，提供给 CRM 系统调用，需要符合本文档的支付接口定义	租户	https://111.22.22.33/pay

签名生成算法（目前支持 MD5）

➤ 第一步：

设所有发送或者接收到的数据为集合 M，将集合 M 内**非空参数值**的参数按照参数名 ASCII 码从小到大排序（字典序），使用 URL 键值对的格式（即 key1=value1&key2=value2...）拼接成字符串 stringA。

➤ 第二步：

在 stringA 最后拼接上 payKey 得到 stringSignTemp 字符串，并对 stringSignTemp 进行 MD5 运算，得到 sign 值 signValue。

示例一（只有必填参数）：

```
// 假设传送的参数如下
{
    "callback_url": "http://crm.domain.com/user/order/callback/out",
    "amount": 236.06,
    "currency": "USD",
    "order_id": "2021072114545283922119",
    "sign_type": "md5",
    "account": "Live/123456"
}
// 第一步：对参数按照 key=value 的格式，并按照参数名 ASCII 字典序排序如：
stringA =
"account=Live/123456&amount=236.06&callback_url=http://crm.domain.com/user/order/callback/out&currency=USD&order_id=2021072114545283922119&sign_type=md5";
// 第二步：拼接 payKey：
signTemp = stringA + "&key=F5D43C246B3B4AB6BF000E07056610B2";
// MD5 运算
sign = md5(signTemp);
// 得到签名：ab5068d6ec6d9fce6ff9167cab81318
```

示例二（非必填参数为空时不参与验签）：

```

// 假设传送的参数如下
{
    "callback_url": "http://crm.domain.com/user/order/callback/out",
    "amount": 636.73,
    "user_name": "",
    "certiricate_type": "身份证",
    "currency": "CNY",
    "order_id": "2021121509335134515174",
    "sign_type": "md5",
    "certiricate_no": "530643199708121120",
    "account": "Live/21000001"
}
// 第一步：对参数按照 key-value 的格式，并按照参数名 ASCII 字典序排序如：
stringA =
"account=Live/21000001&amount=636.73&callback_url=http://crm.domain.com/
user/order/callback/out&certiricate_no=530643199708121120&certiricate_ty
pe=身份证&currency=CNY&order_id=2021121509335134515174&sign_type=md5";
// 第二步：拼接 payKey：
signTemp = stringA + "&key=F5D43C246B3B4AB6BF000E07056610B2";
// MD5 运算
sign = md5(signTemp);
// 得到签名: Fa7559eddc3d5ce1de0ead568d4de150

```

接口定义

1. 支付接口

支付 URL 由租户提供给 haame，租户的用户在线支付时，haame 会将订单信息发送到此 URL，此 URL 应该返回一个支付链接供用户支付；

haame 提交数据到支付 URL，提交方式为 POST，参数以 JSON 格式放于 body 中，请求参数如下：

参数名称	参数含义	数据类型	是否必填	参数说明
callback_url	服务器接受支付结果的回调地址	String	是	回调 haame 的地址，示例： http://crm.domain.com/use/r/order/callback/out
sign_type	签名类型	String	是	默认 md5
order_id	订单号	String	是	示例： 2021072114545283922119
amount	订单金额	String	是	示例：1.01
currency	货币类型	String	是	示例：CNY、USD
user_name	用户姓名	String	否	示例：张三

certificate_type	证件类型	String	否	示例: 身份证
certificate_no	证件号码	String	否	示例: 350203000000000000
account	客户账号	String	是	入金账号或用户钱包, 示例: BCRCO-Demo/ 77779、 F902K4/USD
email	客户邮箱	String	否	示例: 123456@qq.com
sign	签名	String	是	参考签名生成算法

注意: 租户收到数据后必须验签防止用户非法访问。

返回参数以 JSON 格式返回, 返回参数如下:

参数名称	参数含义	数据类型	是否必填	参数说明
code	接口调用结果代码	Integer	是	0 表示成功, -1 表示失败
data	结果数据	Object	是	
data>>url	支付链接	String	是	示例: http://xxx/xxx
data>>pay_order	第三方支付订单号	String	否	租户对接的第三方支付订单号
msg	结果信息	String	是	成功时为空, 失败时为失败原因

返回参数示例:

```
{
  "code": 0,
  "msg": "",
  "data": {
    "url": "http://xxx/xxx",
    "pay_order": "1234567890"
  }
}
```

2. 回调接口

用户支付成功后, 需要租户将成功后的信息回调给 haame 以便自动入金; 回调地址为上面的参数 `callback_url`; 回调提交方式为 `POST`, 参数以 JSON 格式放于 `body` 中, 回调参数如下:

参数名称	参数含义	数据类型	是否必填	参数说明
order_id	订单号	String	是	
pay_order	第三方支付订单号	String	是	租户对接的第三方支付订单号

receipt_amount	到款金额	String	否	用户实际支付的金额, 例如: 12.34, 如不填则以创建订单的金额入金
status	状态	Integer	是	0(表示成功), -1(表示失败)
sign_type	签名类型	String	是	默认 MD5
sign	签名	String	是	参考签名生成算法

租户回调 haame, haame 如果返回字符串 success 表示成功收到并处理, 如果没有返回 success 时租户应该有自动重复回调机制, 如每 5 分钟回调一次, 共回调 5 次。

请求参数示例:

```
{
  "pay_order": "392749779598",
  "sign": "eba738527db24568189b64e688db7509",
  "sign_type": "md5",
  "order_id": "2022010715071123555844",
  "status": 0,
  "receipt_amount": "12.34"
}
```

返回参数示例:

```
{
  "code": 0,
  "msg": "success"
}
```

常见问题

1. 验签时, 订单金额 amount 的小数位数会根据后台支付通道设置的小数位数四舍五入, 在接收参数验签时请注意末位的 0, 如后台支付通道设置的小数位数为 2, 订单金额实际为 12.00。
2. 有些参数是非必传的, 其值为空时不参与验签加密, 但不为空时需要参与加密的。