

随意付互联网支付开发参考文档

版本 v.1.4.3 beta

2018.5.9

第一章 文档描述

1、 文档说明

本说明文档用于指导注册商户实现与随意付支付接口的顺利对接。请相关技术人员详细阅读本文档。

2、 阅读对象

商户接口对接及平台开发人员。

2、系统概要介绍

术语定义

- 1、**商户**:指已独立拥有在线销售系统,并成为随意付在线支付即时到帐接口的系统。
- 2、**会员**, 且已使用或者将使用随意付在线支付即时到帐接口实现收付费或其他相关功能需求的企业或者个人。
- 3、**外部接入接口**:指随意付通过统一的方式接受外部请求的接口。
- 4、**商户系统**:指使用随意付在线支付即时到帐接口的计算机系统,一般指商户所拥有的在线销售系统。
- 5、**用户**:指在随意付认证商户系统内进行消费的企业或者个人。
- 6、**商户 ID**: 随意付为使用外部接入接口的商户统一分配的唯一标识。
- 7、**商户密钥 (KEY)**: 随意付认证商户在和在线即时到帐支付确定合作意想商户提供的 32 位字符串。该信息作为随意付认证商户系统和网关支付交互时身份确认的依据,需商户妥善保管。
- 8、**系统调用流程**

通常,一次支付最少包括 2 个交互过程。第一个过程是商户系统将支付信息提交到随意付接口的过程,这个过程称之为**下单**过程。第二个过程是在支付完成后,随意付服务器通过 http 协议将支付结果发给商户系统的过程,这个过程称之为**异步通知**过程。

如果商户希望用户在支付动作完成后,需要立即返回给商户页面,以方便用户继续完成操作,那么商户需要在下单过程中提交参数 **hrefbackurl**,那么用户在支付完成后会跳转到商户在下单提交过程中的 **hrefbackurl** 地址。**付款的**

结果通知请以异步通知为准!

9、查询流程

在商户系统将订单成功提交给随意付接口后的任意时间, 商户系统可发起请求查询订单的处理结果。该流程由商户系统发起, 由接口返回相应结果给商户。

10、 MD5 加密

随意付接口采用 MD5 加密方式对传输数据进行签名验证, 具体请参考相关接口定义。对 MD5 加密后的签名值, 请注意结果的大小写务必正确。

注意: 为了确保签名值不是因为 MD5 加密算法而导致结果不正确。请各商户在调用接口前对字符串 1234567890abcdefghijklmnopqrstuvwxyz 使用 MD5 加密算法进行加密, 若加密结果为 928f7bcdcd08869cc44c1bf24e7abec6 则表示 MD5 加密方法选用正确。(注意, 所有的字母均为小写)

11、 RSA 签名

随意付接口增加了 RSA 证书签名验签方式。目前为单向验签, 即随意付进行 RSA 签名, 商户进行 RSA 验签, 且只在异步通知、同步通知和补发通知时进行。

签名字符串拼接: 所有非空值字段 (包括 sign) 全部参与签名, 排序方式是按字段名首字母的 ASCII 顺序 (字典序) 从小到大排序。注意几点:

- 1) 所有参与签名的值均是原生值, 不能经过 UrlEncode;
- 2) 签名串使用 GB2312 编码;
- 3) 签名结果为 Base64 编码的字符串, 其中的 "+" 被替换为 "_";

3、支付接口定义

一、 下单过程接口定义（商户系统发起请求）

1、接入 URL：

https:// gateway.easyipay.com/interface/AutoBank/index.aspx

2、接入方式：POST 和 GET 方式

3、请求协议参数：

表 1 下单过程请求协议参数说明

参数名	参数	可空	说明
商户 ID	partner	否	商户 id，由随意付商户系统分配
银行类型	type	否	银行类型，具体请参考附录 1
金额	value	否	单位元（人民币），2 位小数，最小支付金额为 1.00,微信支付宝至少 2 元
商户订单号	orderid	否	商户系统订单号，该订单号将作为随意付接口的返回数据。该值需在商户系统内唯一
异步通知地址	callbackurl	否	异步通知过程的返回地址，需要以 http:// 开头且没有任何参数
同步通知地址	hrefbackurl	是	同步通知过程的返回地址(在支付完成后随意付接口将会跳转到的商户系统连接地址)。注：若提交值无该参数，或者该参数值为空，则在支付完成后，随意付接口将不会跳转到商户系统，用户将停留在随意付系统提示支付结果的页面。

备注消息	attach	是	备注信息，会原样返回。若该值包含中文，请注意编码
MD5 签名	sign	否	32 位小写 MD5 签名值，GB2312 编码

MD5 签名说明

待签名数据为表 1 中**红色加粗的部分**，签名顺序为表 1 中 parter 到

callbackurl 的顺序加商户密钥。具体 MD5 签名源串及格式如下：

parter={0}&type={1}&value={2}&orderid={3}&callbackurl={4}key。

其中，0 到 4 为对应的参数对应的数值，key 为商的 key。

接入实例：（假设商户 Id 为 99，商户密钥为 1234567890abcdef，使用工行网银直连）

GET 请求提交实例(建议 POST)：

https://

gateway.easypay.com/interface/AutoBank/index.aspx?parter=99&type=963&value=100.00&orderid=1234567890&callbackurl=http://www.baidu.com/backAction&hrefbackurl=http://www.baidu.com/notifyAction.1&sign=5d49ec003d46cd586a23dd689a99dd8a

实际进行 MD5 加密的串是

parter=99&type=963&value=100.00&orderid=1234567890&callbackurl=http://www.baidu.com/backAction1234567890abcdef, 该串 MD5 加密结果为(注意不要有换行符)

5d49ec003d46cd586a23dd689a99dd8a

6、特别说明：

- ① 在接口使用中，商户系统内发起请求时应使用页面跳转的方式跳转到接口地址。如在 Asp 中，使用 `response.sendRedirect(接口地址及参数)`，在.net 中，使用 `Response.Redirect(接口地址及参数)`。
- ② 若 `hrefbackurl` 有效，则在跳转返回通知过程中，随意付接口将使用相同方法跳转回商户系统，跳转地址是 `hrefbackurl`。
- ③ 根据 HTTP 协议要求，提交参数的值中若存在特殊字符（如：空格、@等）时，为使随意付接口能接收到正确的参数，这些特殊字符需要做 URL Encoding。需特别注意的是，此时待签名数据应该是原生值而不是 encoding 之后的值。

关于直接获取二维码方式

随意付本身提供直接返回二维码的方式，例如微信直接返回 `weixin://`开头的 `uuid` 码，但因渠道经常变动，会有一些渠道强制跳转收银台扫码的方式，因此这种方式不稳定，**如需要请向运营咨询**，如没有特殊必要，**请使用随意付的扫码收银台即可**

关于网银收银台选择银行付款方式(非直连，选银行跳转，减少对接时间)

随意付提供网银收银台和快捷支付收银台，如需要，请向运营咨询

二、异步通知过程接口定义（随意付接口发起请求）（回调接口）

1、接入 URL： 下单过程中请求参数 callbackurl 值

2、接入方式： GET 方式

3、请求协议参数：

表 2 过程请求协议参数说明		
参数名	参数	说明
商户订单号	orderid	下单过程中商户系统传入的 orderid
订单结果	opstate	0：支付成功
订单金额	ovalue	订单实际支付金额，单位元
通知时间戳	systime	第一次通知时的时间戳，年/月/日 时：分：秒，如 2010/04/05 21:50:58
MD5 签名	sign	32 位小写 MD5 签名值，GB2312 编码
订单号	sysorderid	此次订单过程中随意付接口系统内的订单 Id
订单时间	completiontime	此次订单过程中随意付接口系统内的订单结束时间。格式为年/月/日 时：分：秒，如 2010/04/05 21:50:58
银行类型	type	银行类型，具体请参考附录 1
备注信息	attach	备注信息，下单中 attach 原样返回

订单结果说明	msg	订单结果说明
RSA 签名	RSA_sign	Base64+GB2312 编码，“+”被换成“_”

4、MD5 签名说明：

待签名数据为表 2 中中**红色加粗的部分**以及商户密钥，签名顺序为表 2 中 orderid 到 ovalue 的顺序加商户密钥。具体 MD5 签名源串及格式如下：

orderid={}&opstate={}&ovalue={}&key

其中，key 为商户密钥。

5、返回协议参数：

表 3 异步通知返回协议参数

参数名	参数	说明
是否收到	opstate	0：处理成功

说明：

① 异步通知过程在整个支付流程中一定存在。商户系统在收到通知过程后，需向随意付接口返回 **opstate=0 的结果**。随意付接口根据该返回值判断商户系统是否已经收到结果。若返回结果不是 opstate=0，随意付接口会根据商家和随意付接口的约定，再次反复向 callbackurl 发送结果，直到商户返回 opstate=0 或者达到和商户约定的重复发送次数。

② 当随意付接口在异步通知过程中返回在线支付结果时，商户系统在收到数据后，应该通过 **sign 值**判断是否是有效的返回数据，防止数据在网络传输过程中被恶意篡改。

a) 注意事项:

- ① 在收到随意付接口订单异步通知结果时，**商户系统需首先验证订单通知的合法性，如果不合法，则不要更新商户系统上的订单状态。**
- ② 商户系统内订单状态和订单实际金额务必以此次随意付接口订单异步通知的结果为准。
- ③ 商户系统在成功提交订单后，在未没有收到随意付接口异步通知结果时，请不要更新商户系统上的订单状态。

④ 商户系统收到异步通知结果后，处理流程可表示为

if(返回参数同表 2 相同并且签名正确)

```
{
```

```
    if (opstate==0)  //这个为随意付发给商户的 opstate
```

```
    {
```

```
        按照成功处理商户系统内订单，订单实际金额为 ovalue
```

```
    }
```

```
    else
```

```
    {
```

```
        按照失败处理商户系统内订单
```

```
    }
```

```
        同步返回 opstate=0//这个是成功回执，类似 PHP 的 echo "opstate=0"
```

```
}
```

- ⑤在异步通知过程中商户系统返回结果值 opstate 回随意付接口时，opstate 的值并不是将随意付接口在异步通知的结果原样返回。商户系统返回值 opstate=0 时表示商户系统已经成功接收到了结果（不论结果是什么，总之是收

到了) , 而其他值表示因为某些原因商户系统并不认为随意付接口的返回是有效的。随意付接口在收到商户系统的返回后, 如果返回的值为 opstate=0, 随意付接口将不再次发送结果, 否则随意付接口会根据随意付接口同商户的约定再次发送结果

三、同步通知过程接口定义（随意付接口发起请求）

具体的到账情况请以第二章的异步通知为准！

1、接入 URL： **下单过程**中请求参数 hrefbackurl 值

2、接入方式： GET 方式

3、请求协议参数：

随意付建议同步通知的地址作为一个客户的成功付款页面，或者是商城的首页，或者是任何成功付款后，客户跳转到的地址，同步通知会采用直接跳转的方式并附带参数，**请勿采集跳转过去的任何数据，所有的到账情况请以异步通知为准！**，同步通知的结果不作为到账的标准！

同步过程请求协议参数说明		
参数名	参数	说明
商户订单号	orderid	下单过程中商户系统传入的 orderid
订单结果	opstate	0：支付成功
订单金额	ovalue	订单实际支付金额，单位元
通知时间戳	sysstime	此次通知时的时间戳，年/月/日 时：分：秒，如 2010/04/05 21:50:58

MD5 签名	sign	32 位小写 MD5 签名值, GB2312 编码
订单号	sysorderid	此次订单过程中随意付接口系统内的订单 Id
订单时间	completiontime	此次订单过程中随意付接口系统内的订单结束时间。格式为年/月/日 时:分:秒, 如 2010/04/05 21:50:58
银行类型	type	银行类型, 具体请参考附录 1
备注信息	attach	备注信息, 下单中 attach 原样返回
订单结果说明	msg	订单结果说明
RSA 签名	RSA_sign	Base64+GB2312 编码, "+" 被换成 " " -

四、查询流程接口定义

1、接入 URL: [https:// gateway.easyipay.com/interface/search.aspx](https://gateway.easyipay.com/interface/search.aspx)

2、接入方式: GET 方式

3、请求协议参数:

表 4 查询流程请求协议参数

参数名	参数	加入签名	说明
商户订单号	orderid	Y	需查询的商户系统订单号
商户 ID	partner	Y	商户 id, 由网银支付分配。
MD5 签名	sign	-	32 位小写 MD5 签名值, GB2312 编码

4、返回协议参数

表 5 查询流程返回协议参数

参数名	参数	加入签名	说明
商户订单号	orderid	Y	请求的商户订单号
订单结果	opstate	Y	3: 请求参数无效 2: 签名错误 1: 商户订单号无效 0: 支付成功 -1: 用户还未完成支付或者支付失败
订单金额	ovalue	Y	订单实际金额, 单位元

MD5 签名	sign	-	32 位小写 MD5 签名值, GB2312 编码
--------	------	---	---------------------------

5、MD5 签名说明:

① 查询请求签名:

待签名数据为表 4 中加入签名列值为 Y 的参数以及商户密钥, 签名顺序为表 4

中orderid到parter的顺序加商户密钥。具体 MD5 签名源串及格式如下:

orderid={}&parter={}key

其中, key 为商户签名。

例如商户号为 123, 订单号为 000, KEY 为 13579

如

https://

gateway.easypay.com/interface/search.aspx?orderid=000&parter=123

&sign=XXX

Sign=MD5 加密(orderid=000&parter=12313579)

② 查询返回签名:

待签名数据为表 5 中加入签名列值为 Y 的参数以及商户密钥, 签名顺序为表 5

中orderid到ovalue的顺序加商户密钥。具体 MD5 签名源串及格式如下:

orderid={}&opstate={}&ovalue={}key

其中, key 为商户密钥。

附录 1：支付接口类型说明

随意付接口类型说明(银行仅支持借记卡)

编号	类型
1004	PC 微信 扫码
1007	适配手机界面的微信 扫码
1006	适配手机界面的支付宝 扫码
1001	银联扫码
1002	京东扫码
1003	百度钱包
1005	手机网银（自带收银台跳转）
1008	银联快捷
1009	银联一码付
1010	微信条码
1011	QQ 条码
1012	京东 H5
1100	H5 微信
1101	H5 支付宝
1102	H5QQ
992	PC 支付宝 扫码

993	qq 扫码
962	中信银行
963	中国银行
964	中国农业银行
965	中国建设银行
967	中国工商银行
970	招商银行
971	中国邮政储蓄银行
972	兴业银行
977	浦东发展银行
978	平安银行
980	民生银行
981	交通银行
982	华夏银行
985	广东发展银行
986	光大银行
1962	网银快捷