百度钱包前置选择收银台银行接口V1.2

百度在线网络技术（北京）有限公司

(版权所有,翻版必究)

修改记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | 修改后  版本号 | 修改内容简介 | 修改日期 | 修改人 |
| 1 | V1.0 | 第一版 | 2014-06-19 | 李洋 |
| 2 | V1.1 | 取消对bankno和cardtype的签名 | 2014-06-19 | 李洋 |
| 3 | V1.2 | 补充参考文档<百度钱包企业版商户系统接入指南V5> | 2014-06-24 | 李洋 |

# 引言

## 文档概述

百度钱包提供了PC端前置选择收银台银行的接口，供第三方商户系统与百度钱包系统进行对接。本文档对接口规范进行描述，以指导商户系统开发人员顺利对接。

## 阅读对象

1. 接入百度钱包系统的商户系统开发人员
2. 百度钱包的对外接口相关技术人员，包括开发和技术支持

# 前置选择银行收银台简介

## 业务介绍

商户调用“查询可用银行列表”的接口，查询出该商户目前可以使用的快捷信用卡和快捷储蓄卡银行的列表。用户在商户收银台中选择了某一个快捷银行，跳转到百度钱包收银台后，会默认选中该银行，方便用户进行后续支付。

# 接口规范

## 名词解释

|  |  |
| --- | --- |
| **名称** | **解释** |
| **百度钱包商户号** | 百度钱包为接入百度钱包系统的每家商户分配一个独一无二的ID，作为商户身份的唯一标识，我们把这个ID称为百度钱包商户号。  百度钱包商户号在商户与百度钱包签约时分配。 |
| **百度钱包合作密钥** | 为了保证商户系统和百度钱包系统之间通信的真实性，百度钱包与商户签约时，为每个商户分配一个保密的、独一无二的key，我们把这个key称为百度钱包合作密钥。  百度钱包合作密钥将用于对通信数据的签名，必须确保只有商户和百度钱包知道，否则通信数据可能被篡改或伪造。 |

## 签名机制

由于商户和百度钱包之间的通信涉及到订单信息和支付信息，必须保证通信数据不被篡改和伪造。否则，将给商户和百度钱包造成资金损失。

百度钱包采用签名机制来保证通信安全。本文中的每个接口规范都包括两个参数：**sign\_method和sign**。sign\_method是摘要算法，sign是签名结果。商户或百度钱包向对方发送数据时，必须指定sign\_method并生成相应的sign；对方接收到数据后，必须使用相同的签名算法对sign的值进行验证。如果验证不通过，则说明通信数据已经被篡改或伪造。

百度钱包没有使用RSA、DSA等给予非对称密钥的签名算法，而是使用了MD5、SHA-1等摘要算法。这些摘要算法本身并不能用作签名，但是结合百度钱包合作密钥，也可以起到签名的作用，进而达到防篡改和伪造的目的。

商户与百度钱包签约时，百度钱包会分配一个百度钱包合作密钥。每个商户的密钥是唯一的，一定不能让第三方知道。如果密钥泄漏，必须及时通知百度钱包更换密钥。

签名机制包括拼接待签名数据和对待签名数据进行摘要两个步骤：

1. 待签名数据由除sign之外的所有请求参数和百度钱包合作密钥按以下规则拼接而成：
   1. 请求参数都按照名称字符升序排列（参数名称不允许相同 ）
   2. 某些请求参数的值是允许包含中文的，为了避免中文的编码问题，我们规定所有参数的值必须按照input\_charset进行编码（input\_charset的含义请参见即时到帐接口规范）
   3. 对于可选参数（接口规范中的非“必须”参数），如果没有使用，则无需参与拼接。这样可以增强接口参数的可扩展性。
   4. 将百度钱包合作密钥作为最后一个参数，参数名为key，参数值就是百度钱包合作密钥本身
   5. 将请求参数按上述顺序用&拼接起来

需要注意的是：在签名时，如果参数的值包括&、@等特殊字符或中文，这些字符需要保持原样，不要做URL编码。发送HTTP请求时，是需要进行URL编码的。

1. 用指定的摘要算法对待签名数据进行摘要，生成签名数据（不区分大小写），作为附加的请求参数sign的值。

下面是一个使用MD5算法进行签名的示例：

|  |
| --- |
| sign =  MD5(currency=1&extra=&goods\_desc=使用百度钱包支付的订单&goods\_url=  &goods\_category=1&input\_charset=1&order\_create\_time=20080808080808&order\_no=20080808123456123456&pay\_type=1&return\_url=http://127.0.0.1/return\_url&service\_code=1&sign\_method=1&sp\_no=1234567890&total\_amount=2500&transport\_amount=500&unit\_amount=1000&unit\_count=2&key=XXXXXXXXXXXXXXXX)  =  39375042FD5F801C2B0A128B145589C3  其中，goods\_desc的值（红字部分）应该是按照input\_charset编码后的结果。 |

下面解释一下为什么签名之前，需要对中文进行特定的编码。

相同的字符串(包括中文)，如果内部编码格式不同，那么对应的字节流可能也不相同。MD5等摘要算法是对字节流进行操作的。因此，相同字符串的摘要结果未必相同，取决于内部编码。

商户和百度钱包必须协商好中文的编码，才能成功验签。如果商户的请求参数中可能包含中文，那么必须指定input\_charset参数，并按照input\_charset进行编码后，才能签名。百度钱包收到请求数据后，使用相同的编码进行验签。

# 接口

### 可用银行列表的查询接口

* 请求URL：https://www.baifubao.com/\_u/api/banklist
* 请求方式：POST
* 请求参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 参数名 | 参数类型 | 参数含义 | 说明 | 是否必须 |
| sp\_no | int | 商户号 | 10位数字 | 是 |
| source\_flag | int | 终端 | 目前可选值：  0 表示pc  1 表示h5  2 表示iframe  3 表示android | 是 |
| sign\_method | int | 签名方法 | 目前固定为1。表示用md5方式签名。 | 是 |
| sign | string | 签名 | 见接口签名说明 | 是 |

* 返回json格式：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 参数含义 | 说明 | 是否必须 |
| result | 状态码 | 为0时表示成功。否则表示错误码，[附错误码列表](#_错误码列表)。 | 是 |
| result\_string | 错误描述 | 错误描述字符串。中文字符是以unicode编码 | 是 |
| bank | 网银可用银行列表 | 前端银行编码 | 否 |
| easypay\_credit | 信用卡快捷可用银行 | 前端银行编码 | 否 |
| easypay\_deposit | 储蓄卡快捷可用银行 | 前端银行编码 | 否 |

示例：

{"result":"0", "result\_string":"OK", "bank":["1001","2001"], "easypay\_credit":["3001" , "4001"] ,"easypay\_deposit":["5001" , "6001"]}

或者：

{"result": "111", "result\_string": "xxxxxx"}

* 注意事项：

在百度钱包上线新银行或者下线银行后，该接口也会实时返回该商户最新的可用银行列表。

对于新增的银行，可能需要商户收银台进行调整，确保能正确显示。

### 前置银行选择接口

目前支持在商户收银台界面上前置选择**快捷信用卡**和**快捷储蓄卡**。

如果用户在商户收银台界面中选择了快捷银行，在跳转PC端钱包的url接口中需要增加两个参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 参数名 | 参数类型 | 参数含义 | 说明 | 是否必须 |
| bankno | int | 前端银行编码 | 数字。来自“可用银行列表的查询接口”的结果。 | 否。  这两个参数不加入签名。 |
| cardtype | int | 卡类型 | 目前可选值：  1：信用卡快捷  2：储蓄卡快捷 |

* 注意事项：

商户接入PC收银台的详细方式请参考文档《百度钱包企业版商户系统接入指南V5》的5.1部分。 

# 附录

## 错误码列表

|  |  |
| --- | --- |
| 错误码 | 含义 |
| 113 | 获取渠道决策失败 |
| 5808 | IP无权限访问 |
| 114 | 商户无权限访问 |
| 5801 | 缺少参数 |
| 5802 | 无效参数 |
| 5803 | 无效的签名方法 |
| 5804 | 验签失败 |