

联动优势公共验证产品

商户接入规范

V1.0.2

|  |  |  |  |
| --- | --- | --- | --- |
| 文件编号： | | 生效日期： | |
| 版本号：V1.0.0 | 修改状态： | | 密级： |
| 编制：王方亮  日期：2015年4月11日 | 审核：  日期： | | 批准：  日期： |

版本控制信息

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 日期 | 描述 | 作者 |
| V0.0.1 | 2014-03-27 | 创建，待发布 | 李升、王杰、李志斌、王方亮 |
| V0.0.2 | 2015-4-29 |  | 王方亮 |
| V1.0.2 | 2015-5-06 | 修改目前支持产品为实名认证及身份认证 | 马祥城 |

目录

[V1.0.0 1](#_Toc417306050)

[目录 3](#_Toc417306051)

[1 引言 5](#_Toc417306052)

[1.1 概述 5](#_Toc417306053)

[1.2 适用范围 5](#_Toc417306054)

[1.3 名词解释 5](#_Toc417306055)

[2 开发规范 6](#_Toc417306056)

[2.1 数据接口规范 6](#_Toc417306057)

[2.1.1 请求 6](#_Toc417306058)

[2.1.2 响应 6](#_Toc417306059)

[2.1.3 消息报文示例 7](#_Toc417306060)

[3 通讯方式 10](#_Toc417306061)

[4 适用场景 10](#_Toc417306062)

[4.1 直接验证 10](#_Toc417306063)

[5 通信接口 11](#_Toc417306064)

[5.1 公共验证 11](#_Toc417306065)

[5.1.1 公共验证(商户🡪平台) 11](#_Toc417306066)

[6 附录 13](#_Toc417306067)

[6.1 签名机制 13](#_Toc417306068)

[6.1.1 需要参与签名的参数 13](#_Toc417306069)

[6.1.2 生成待签名字符串 13](#_Toc417306070)

[6.1.3 RSA签名 15](#_Toc417306071)

[6.1.4 证书颁发 15](#_Toc417306072)

[6.2 收费返回码说明 15](#_Toc417306073)

[6.3 返回信息说明 16](#_Toc417306074)

[6.4 计费状态说明 16](#_Toc417306075)

[6.5 证件类型 17](#_Toc417306076)

[6.6 支持银行列表 17](#_Toc417306077)

[6.6.1 借记卡四要素实名认证支持银行列表 17](#_Toc417306078)

[6.6.2 贷记卡四要素实名认证支持银行列表 17](#_Toc417306079)

[6.6.3 借记卡三要素实名认证支持银行 20](#_Toc417306080)

[6.6.4 借记卡两要素验证支持银行 21](#_Toc417306081)

# 引言

## 概述

联动优势公共验证产品商户接入规范定义了联动优势公共验证产品与调用业务线及商户系统之间的开放接口，主要是对商户接入、验证流程、开发规范、通信接口以及账务处理的定义。商户通过这一规范可以完成为验证、结算等用户信息验证相关事宜，同时可完成了解相关的处理。

## 适用范围

本文档的适用对象为接入资金账户托管平台的商户技术开发人员，日常维护人员以及日常结算人员。他们需要熟悉以下基本知识：

熟悉Mircosoft Windows 、UNIX和LINUX操作系统，熟悉这些操作系统上的网页制作以及基本的ASP和JSP的开发。了解一般的信息安全知识，比如HTTPS、非对称密钥机制、数字加密和数字签名等基本概念。熟悉验证流程，了解其基本原理。

## 名词解释

1、为了文中描述的方便、表达的一致性，特进行以下的约定和说明，下文中凡提到的与下面表格中相同的词汇，如无特殊说明，皆遵循以下表格中的解释和定义。

|  |  |  |
| --- | --- | --- |
| 序号 | 术语或缩略语 | 说明性定义 |
|  | 实名认证 | 支持对姓名及身份证号码的真实性验证 |
|  | 四要素借记卡实名认证 | 业务线或商户发起验证，对用户借记卡信息，包括卡（账）号+户名+证件类型+证件号+银行预留手机号的信息进行实名认证。 |
|  | 四要素贷记卡卡实名认证 | 业务线或商户发起验证，对用户贷记卡信息，包括卡（账）号+户名+证件类型+证件号+银行预留手机号+CVV2+有效期的信息进行实名认证。 |
|  | 三要素借记卡实名认证 | 业务线或商户发起验证，对用户借记卡信息，包括卡（账）号+户名+证件类型+证件号的信息进行实名认证。 |
|  | 两要素验证 | 业务线或商户发起验证，对用户借记卡信息，包括卡（账）号+户名的信息进行实名认证。 |
|  | 身份验证 | 业务线或商户发起验证，对用户姓名+身份证号码进行验证 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 开发规范

## 数据接口规范

### 请求

1、商户提交给平台的请求可以以POST和GET的方式提交，当以GET方式请求时各参数的参数值需做URL编码，编码字符集UTF-8，当以POST方式请求时各参数的参数值不需要做URL编码。

2、签名的数据根据接口的定义，参见附录签名机制。

3、各请求参数的参数值的前后不允许出现空白符，否则将影响签名的正确性。

### 响应

响应的内容写在HTTP响应<META>标签的CONTENT属性中，该内容中各数据项以字符“&”隔开。CONTENT必须大写，并且其内容中不能出现“<”和“>”的字符，每个数据项内不允许出现“&”符号。因为在HTML中可能有多个<META>标签存在，此标签通过其NAME属性判断，其属性值为MobilePayPlatform，其格式如下：<META NAME=” MobilePayPlatform” CONTENT=“key1=value1&key2=value2&key3=value3&….&sign=签名”/>

签名的数据根据接口的定义，将需要签名的数据项以“key1=value1&key2=value2&key3=value3….”的格式做为签名对象进行签名，签名对象要求严格按照接口规范里的参数从字母a-z的升序顺序组装并且在签名对象末尾不能包含“&”符号。

各响应参数的参数值的前后不允许出现空白符，否则将影响签名的正确性。

### 消息报文示例

#### 请求（商户->平台）

http://pay.soopay.net/spay/pay/payservice.do?account\_name=dz2QaCHhjFJJMOcxLKOhLCHiA7P5F3FReAzcklLtPnaf3K8UL9aT4jugWhKaEYccKZ3B7H5CEtAR0WKPXbmVetIhsGeprwzksFCDDOAprR4MToW39HqElteiRAH8P4Hw3r9+fFJVyEeXgzJxBDAZSzlDo0N4zlcR8ChJCGe9d38=&amount=&auth\_mode=0&mer\_Order\_id=T00000001&auth\_type=1&bank\_Account=UyJuf0wQJbtT4dbDXu5OPPYlcILbEnkHWO8PeNc4xKkqv8bYFiKDfWqusbGiWdo34g2IZGQ1J+JvcVtDTxDlrhSaSC66QrCHqglmkah45f7/DHnz8BZuEqJGMdLbRjOdjA4HVWx7koMhjyqSBp9QhxwADjSVi6+IP8evz1sgMWM=&charset=UTF-8&cvv2=&endDate=&identity\_code=Tbg6cGW/bc0eUbi4bJNUFha/Nb+XmQBeVBkMkLxnqmgThXVlb0pFeeTBiHfyCf1jZECpdkSMvAMVsmYbMlKh7T0TVvt3qEKRHSpPvDU+7wYU8tsUYMXgp7wb1SFFjgGYFX1+ACL7lNEh2yQqXN77wT2DjWGIC9d+CNGB7IS71xk=&identity\_type=1&mer\_id=25019&mobile\_id=13800138000&res\_format=HTML&service=comm\_auth&version=1.0

#### 响应（平台->商户）

<html>

<head>

<META NAME="MobilePayPlatform" CONTENT="isCharge=0&mer\_id=25019&ret\_code=0000&ret\_msg=鉴权成功!&sign\_type=RSA&version=1.0&sign=Oc2JRsee9sZra3PdBzKqkyfvy6cTP/jiSRzODfTRBoGdbuc+dnZhqDdAY2ZLh4jWMthlHO8m8f6ihf4J+VVvn0fVTeKwiWCUPJJ8mN7D3VTyKK30FIgh6/yS/Bigkm4UZQII29TkUq58DMvREW7oBJ7V6gnYgnVV1oz1Mx6IW50=">

</head>

<body>

</body>

</html>

# 通讯方式

双方采用HTTP/HTTPS协议进行通信，双方互为服务器。如下图所示：



# 适用场景

## 直接验证

商户收集验证信息，请求公共验证进行验证操作。



**流程说明：**

要素信息验证主要分成以下步骤，分别为：

1. 用户在商户端提供验证要素信息；
2. 商户收集并组织验证信息，调用公共验证接口；
3. 公共验证进行验证处理，并返回验证结果；
4. 商户结果通知用户；

**主要接口：**

1. 付款通道；
2. 扣款通道；
3. 直连银行及银联通道借记卡、贷记卡实名认证验证接口；
4. 身份信息验证接口；

# 通信接口

**接口地址：**<http://pay.soopay.net/spay/pay/payservice.do>

## 公共验证(商户→平台)

### 验证模式

参数验证表单

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 认证类型 | 验证模式  auth\_mode | 银行卡号 bank\_account | 账户姓名 account\_name | 证件类型 identity\_type | 证件号码 identity\_code | 手机号码 mobile\_id | 金额 amount | 信用卡CVV2 cvv2 | 信用卡有效期 endDate |
| [借记卡实名认证](#_借记卡实名认证) （四要素） | 0 | √ | √ | √ | √ | √ |  |  |  |
| [借记卡实名认证](#_借记卡实名认证)（三要素） | 0 | √ | √ | √ | √ |  |  |  |  |
| [身份认证](#_身份认证) | 3 |  | √ |  | √ |  |  |  |  |

### 接口地址

<http://pay.soopay.net/spay/pay/payservice.do>

### 请求数据列表

注：银行卡号bank\_account；账户姓名account\_name；证件号码identity\_code；信用卡CVV2cvv2；信用卡有效期endDate这几个参数都需要做加密处理，联动提供的接口方法已包含相应的加密处理功能，无需商户自行操作。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | **字段** | **名称** | **长度** | **说明** | **必填** |
| **协议参数** | | | | | |
| 1 | service | 接口名称 | 变长 32 | 定值： comm\_auth | Y |
| 2 | charset | 参数字符编码集 | 变长 16 | 商户网站使用的编码格式，支持  UTF-8、GBK、GB2312、GB18030 | Y |
| 3 | mer\_id | 商户编号 | 变长8 | 由平台统一分配合作商户唯一标识 | Y |
| 4 | sign\_type | 签名方式 | 定长 8 | 暂只支持RSA必须大写 | Y |
| 5 | sign | 签名 | 变长256 | 参见[签名机制](#_签名机制) | Y |
| 6 | version | 版本号 | 定长3 | 定值 1.0 | Y |
| **业务参数** | | | | | |
| 1 | auth\_type | 验证类型 | 定长1 | 1-直接验证 | Y |
| 2 | auth\_mode | 验证模式 | 定长1 | 0：银行卡实名认证；  3：身份认证；  **如传递该值，需要根据[5.1.1验证模式](#_验证模式)表单内不同验证模式传递不同的参数，如传递参数不符，则无法通过。**  **如传入验证模式为空，将根据传入要素进行模式判断。** | N |
| 3 | order\_id | 商户订单号 | 变长32 | 商户订单号 | Y |

#### 借记卡实名认证

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **0-银行卡实名认证（借记卡）**  **支持四要素&三要素验证，区别为手机号是否传递验证。** | | | | | |
| 4 | bank\_account | 银行卡号 | 变长256 | 用联动的公钥进行RSA加密该字段 | Y |
| 5 | account\_name | 账户姓名 | 变长256 | BASE64(GBK编码)加密该字段，然后用公钥进行RSA加密。 | Y |
| 6 | identity\_type | 证件类型 | 定长1 | 1:身份证 | Y |
| 7 | identity\_code | 证件号码 | 变长256 | 用联动的公钥进行RSA加密该字段 | Y |
| 8 | mobile\_id | 手机号 | 定长11 | 银行端预留手机号  如传递该值则会验证手机号，验证模式为四要素验证。如不传递该值，则不验证手机号，验证模式为三要素验证。 | N |

#### 身份认证

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **3-身份认证（借记卡）**  **验证要素：姓名+身份证号。** | | | | | |
| 4 | account\_name | 账户姓名 | 变长256 | BASE64(GBK编码)加密该字段，然后用公钥进行RSA加密。 | Y |
| 5 | identity\_code | 证件号码 | 变长256 | 用联动的公钥进行RSA加密该字段 | Y |

### 响应数据列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | **字段** | **名称** | **长度** | **说明** | **必填** |
| **协议参数** | | | | | |
| 1 | sign\_type | 签名方式 | 定长 8 | 暂只支持RSA必须大写 | Y |
| 2 | sign | 签名 | 变长256 | 参见[签名机制](#_签名机制) | Y |
| 3 | mer\_id | 商户编号 | 变长8 | 由平台统一分配合作商户唯一标识 | Y |
| 4 | version | 版本号 | 定长3 | 定值 1.0 | Y |
| **业务参数** | | | | | |
| 1 | ret\_code | 返回码 | 变长8 | 0000鉴权通过 | Y |
| 2 | ret\_msg | 返回信息 | 变长128 |  | N |
| 3 | isCharge | 是否计费 | 定长 1 | 0-计费；其他-不计费 | Y |

# 附录

## 签名机制

### 需要参与签名的参数

在请求参数列表中，除去sign、sign\_type 两个参数外，其他需要使用到的参数皆是要签名的参数。

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。

### 生成待签名字符串

对于如下的参数数组：

string[] parameters={

"service= mer\_cancel ",

" charset =GBK",

" mer\_id =9996",

"version =1.0",

"res\_[format](app:ds:format" \t "_self)=HTML",

"order\_id =123456789 ",

"mer\_date =20110101",

" amount =500"

};

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：

amount=500&charset=GBK&mer\_date=20110101&mer\_id=9996&order\_id=123456789&res\_format=HTML&service=mer\_cancel&version=1.0

这串字符串便是待签名字符串。

**注意：**

* 没有值的参数无需传递，也无需包含到待签名数据中；
* 签名时将字符转化成字节流时指定的字符集与\_input\_charset保持一致；
* 如果传递了input\_charset或charset参数，这个参数也应该包含在待签名数据中；
* 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media\_Id进行数字签名，那么待签名数据应该是media\_Id =test@msn.com，而不是media\_Id =test%40msn.com。

### RSA签名

在签名时，需要私钥和公钥一起参与签名。私钥与公钥皆是客户通过 OPENSSL 来生成得出的。客户把生成出的公钥与联动优势技术人员配置好的平台公钥做交换。因此，在签名时，客户要用到的是客户的私钥及平台的公钥。

**请求时签名**

当拿到请求时的待签名字符串后，把待签名字符串与客户的私钥一同放入RSA的签名函数中进行签名运算，从而得到签名结果字符串。

**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，把待签名字符串、平台提供的公钥、平台通知返回参数中的参数 sign 的值三者一同放入RSA 的签名函数中进行非对称的签名运算，来判断签名是否验证通过。

### 证书颁发

目前商户的公私钥、联动的公私钥都由联动生成。

## 收费返回码说明

|  |  |  |
| --- | --- | --- |
| 序号 | 返回码 | 返回码描述 |
| 1. | 0000 | 成功 |
| 2. | 00290501 | 库中无此号 |
| 3. | 00290502 | 不一致 |
| 4. | 00080554 | 输入的卡号无效，请确认后输入 |
| 5. | 00210024 | 卡状态不正确 |
| 6. | 00090020 | 输入卡信息有误，交易失败 |
| 7. | 00210028 | 持卡人身份信息或手机号输入不正确，验证失败 |
| 8. | 00131070 | 账户属性和账号不符 |
| 9. | 00180005 | 持卡人身份证号码检验不通过 |
| 10. | 00180016 | 输入手机号与注册手机号不一致 |
| 11. | 00060620 | 注册此手机号的用户不存在 |
| 12. | 00060720 | 用户手机号错误 |
| 13. | 00060721 | 用户未开通该银行 |
| 14. | 00080530 | 信用卡有效期错误或卡已过期 |
| 15. | 00080531 | 银行卡手机号或CVN2码错误 |
| 16. | 00080532 | 银行卡绑定的手机号错误 |
| 17. | 00080533 | 银行卡的CVN2码错误 |
| 18. | 00080534 | 银行卡号与证件号码不符 |
| 19. | 00080535 | 发卡银行不支持 |
| 20. | 00080547 | 证件类型不支持 |
| 21. | 00080554 | 银行卡号有误 |
| 22. | 00210037 | 用户信息有误或未开通银联在线服务 |

## 返回信息说明

返回信息主要通过接口中的ret\_msg字段来体现，目前联动优势采用信息模版的方式对返回信息进行监管，具体使用方式为：

1. 不同的模版用半角“&”来区分，模版按照“&”分隔的顺序表示。
2. 同一模版中不同的内容用半角“=”来分隔。

## 计费状态说明

|  |  |  |
| --- | --- | --- |
| 编号 | 名称 | 描述 |
| 1 | 计费 | 验证成功及提供明确验证结果的验证订单进行计费。 |
| 2 | 不计费 | 系统、通讯及未获取明确验证结果等情况不计费。 |

## 证件类型

|  |  |  |
| --- | --- | --- |
| 编号 | 名称 | 备注 |
| 1 | 身份证号 |  |

## 支持银行列表

### 借记卡四要素实名认证支持银行列表

卡（账）号+户名+证件类型+证件号+银行预留手机号的信息进行实名认证。

|  |  |  |
| --- | --- | --- |
| 序号 | 银行名称 | 备注 |
|  | 农业银行 |  |
|  | 交通银行 |  |
|  | 中国银行 |  |
|  | 建设银行 |  |
|  | 光大银行 |  |
|  | 兴业银行 |  |
|  | 中信银行 | 需开通银联无卡支付 |
|  | 广东发展银行 |  |
|  | 工商银行 |  |
|  | 兰州银行 |  |
|  | 平安银行 |  |
|  | 中国邮政 |  |

### 借记卡三要素实名认证支持银行

包括卡（账）号+户名+证件类型+证件号的信息进行实名认证。

|  |  |  |
| --- | --- | --- |
| 序号 | 银行简码 | 备注 |
|  | 农业银行 | 实名认证 |
|  | 交通银行 | 实名认证 |
|  | 中国银行 | 实名认证 |
|  | 华夏银行 | 实名认证 |
|  | 光大银行 | 实名认证 |
|  | 兴业银行 | 实名认证 |
|  | 中信银行 | 实名认证 |
|  | 广东发展银行 | 实名认证 |
|  | 工商银行 | 实名认证 |
|  | 兰州银行 | 实名认证 |
|  | 平安银行 | 实名认证 |
|  | 中国邮政 | 实名认证 |
|  | 中国建设银行 | 实名认证 |