

银联在线支付通行证

(UPOP OAuth2)

接入技术文档

版本号：v1.0

目录

一、	文档说明.....	3
	阅读对象.....	3
	Oauth2 解释.....	3
二、	功能描述.....	3
	登录相关.....	3
	支付相关.....	5
三、	授权流程.....	5
	简介.....	5
	获取 Authorization Code	6
	调用地址.....	6
	请求方式.....	6
	请求参数.....	6
	响应结果.....	7
	通过 Authorization Code 获取 Access Token.....	7
	调用地址.....	8
	请求方式.....	8
	请求参数.....	8
	响应结果.....	8
	通过 Refresh token 获取 Access Token	9
	调用地址.....	9
	请求方式.....	9
	请求参数.....	10
	响应结果.....	10
四、	资源获取接口.....	11
	用户信息获取接口.....	11
	调用地址.....	11
	请求方式.....	11
	请求参数.....	11
	响应结果.....	11
	地址信息获取接口.....	12
	地址信息前台选择.....	14
	地址信息后台获取.....	15
五、	错误码.....	16
	说明.....	16
	错误码参考.....	17
六、	示例代码说明.....	18

一、 文档说明

阅读对象

银联在线支付通行证接口技术文档是面向具有一定的网站开发能力，了解 ASP、PHP、JAVA、ASP.NET 等开发语言中的一种的网站开发、维护和管理人员。

Oauth2 解释

银联在线支付通行证产品采用的是 OAuth2.0 规范，OAuth 是一种国际通用的授权方式，官方技术说明可参看 <http://oauth.net/2/>

OAuth2.0 从逻辑上可以分为授权服务器和资源获取服务器。

授权服务器负责 Authorization Code 、 Access Token 、 Refresh Token 的颁发。其中 Authorization Code 是用户授权成功后的授权码，Access Token 是商户应用访问用户资源的令牌，Refresh Token 是用于刷新 Access Token 的令牌。资源获取服务器负责商户应用以获得的 Access Token 访问用户指定资源的回复。

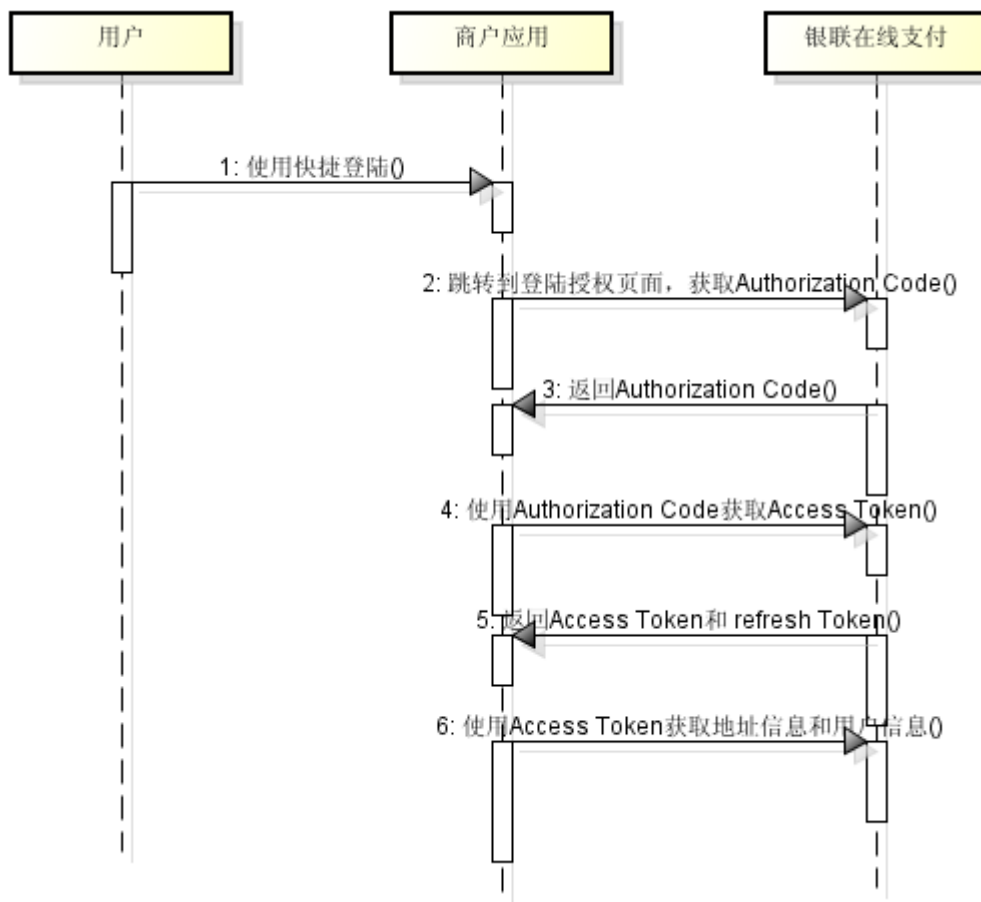
二、 功能描述

登录相关

银联在线支付通行证发起方式可以分为两类：

1) 被动请求方式：

用户通过商户网站主动请求跳转到银联在线支付通行证登录页面，输入银联在线支付用户名、密码授权后，以“已登录”状态返回到商户网站。流程图如下：



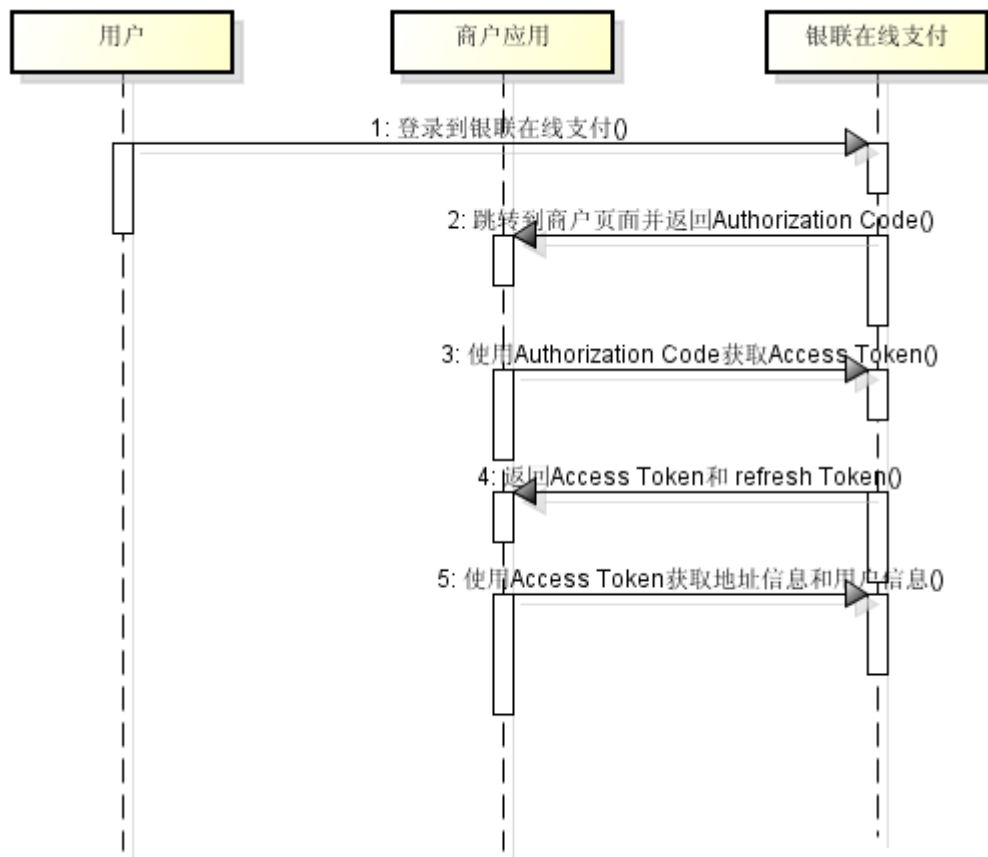
流程说明:

1. 用户在商户页面点击“使用银联在线支付通行证”链接
2. 商户页面跳转至通行证系统的登录页面，**获取 Authorization Code.**
3. 登录成功后，通行证系统返回 Authorization Code 至商户应用
4. 商户应用向通行证系统发送 **Authorization Code 获取 Access Token** 的请求
5. 通行证系统返回 Access Token 和 Refresh Token 至商户应用
6. 商户应用使用 Access Token **获取地址信息**和**获取用户信息**

其中，流程 2 中的接口在授权流程中获取 [Authorization Code 章节](#)中有详细描述,流程 4 中的接口在授权流程中的[用 Authorization Code 获取 Access Token 的章节](#)中有详细描述。流程 6 中的接口在[资源获取相关接口](#)的章节中有详细描述

2) 主动请求方式:

用户在银联在线支付门户网站点击商户图标，跳转到银联在线支付通行证页面，输入银联在线支付用户名、密码授权后，以“已登录”状态主动跳转到商户网站。流程图如下:



流程说明：

1. 用户登录银联在线支付系统，登录成功后，在银联在线支付门户网站点击商户图标
2. 页面主动跳转到商户网站，并返回 Authorization Code
3. 商户应用向通行证系统发送用 **Authorization Code** 获取 **Access Token** 的请求
4. 通行证系统返回 Access Token 和 Refresh Token 至商户应用
5. 商户应用使用 Access Token 获取地址信息和获取用户信息

其中，流程 2 中的接口在授权流程中的[用 Authorization Code 获取 Access Token](#) 的章节中有详细描述。流程 5 中的接口在[资源获取相关接口](#)的章节中有详细描述

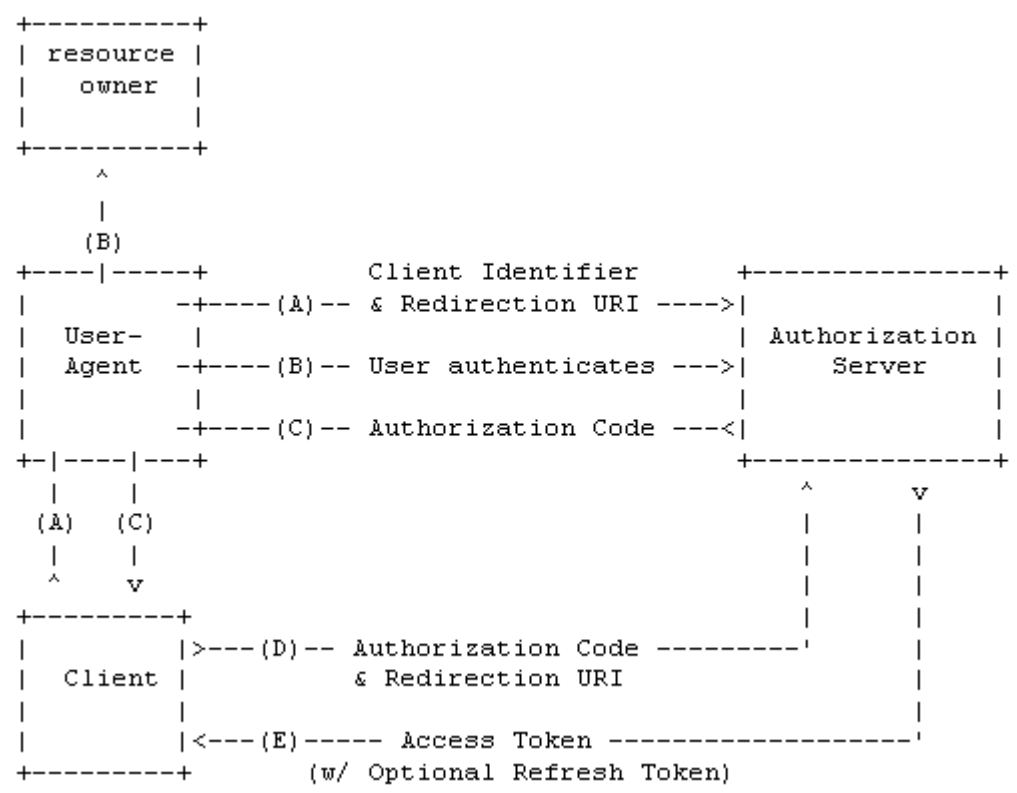
支付相关

由于通行证用户同时实现了在银联在线支付网关的登录，为让用户有更好的支付体验，对于银联在线支付通行证用户，在现有银联在线支付网关发布给商户的上送报文中，推荐设置域名 defaultPayType 为 ProPay（快捷支付）。支付接口信息请详见 《互联网商户及收单机构接入接口规范》

三、 授权流程

简介

采用 Authorization Code 获取 Access Token 的授权验证流程又被称为 Web Server Flow，适用于所有有 Server 端的应用，如 Web/Wap 站点、有 Server 端的手机/桌面客户端应用等。其流程示意图如下：



对于应用而言，其流程由获取 Authorization Code 和通过 Authorization Code 获取 Access Token 这 2 步组成。

获取 Authorization Code

调用地址

<https://online.unionpay.com/oauth/authorize>

请求方式

http get/post

请求参数

参数名	必选	介绍
-----	----	----

client_id	true	申请的第三方商户 ID
response_type	true	此值固定为“code”
redirect_uri	true	授权后要回调的 URI，即接收 Authorization Code 的 URI。此时用户同意授权后，授权服务会将 Authorization Code 直接显示在响应页面的页面中及页面 title 中。
state	false	用于保持请求和回调的状态，授权服务器在回调时（重定向用户浏览器到“redirect_uri”时），会在 Query Parameter 中原样回传该参数

例如：“client_id”为“146027875337921”的应用要请求某个用户的默认权限，并在授权后需跳转到“http://www.example.com/oauth_redirect”，同时希望在弹出窗口中展现用户登录、授权界面，则应用需要重定向用户的浏览器到如下 URL：

```
https://online.unionpay.com/oauth/authorize?
response_type=code&
client_id=146027875337921&
redirect_uri=http%3A%2F%2Fwww.example.com%2Foauth_redirect&
```

响应结果

此时授权服务会根据应用传递参数的不同，为用户展现不同的授权页面。如果用户在此页面同意授权，授权服务则将重定向用户浏览器到应用所指定的“redirect_uri”，并附上表示授权服务所分配的 Authorization Code 的 code 参数，以及 state 参数（如果请求 authorization code 时带了这个参数）。

例如：继续上面的例子，假设授权服务在用户同意授权后生成的 Authorization Code 为“150d91267a8e45b0bbee720795dc4ac5”，则授权服务将会返回如下响应包以重定向用户浏览器到“http://www.example.com/oauth_redirect”地址上：

```
HTTP/1.1 200 OK

Location: http://www.example.com/oauth_redirect?code=ANXxSNjwQDug
OnqeikRMu2bKaXCdlLxn
```

注意：

- 1) 每一个 Authorization Code 的有效期为 15 分钟，并且只能使用一次，再次使用将无效。

通过 Authorization Code 获取 Access Token

调用地址

<https://online.unionpay.com/oauth/token>

请求方式

http post

请求参数

通过上面第一步获得 Authorization Code 后，便可以用其换取一个 Access Token。获取方式是，应用在其服务端程序中发送请求到银联在线支付通行证 OAuth 授权服务地址上，并带上以下 5 个必须参数：

参数名	必选	介绍
grant_type	true	此值固定为“authorization_code”
code	true	通过上面第一步所获得的 Authorization Code
client_id	true	申请的第三方商户 ID
client_secret	true	商户密钥
redirect_uri	true	该值必须与获取 Authorization Code 时传递的“redirect_uri”保持一致

例如：

```
https://online.uinonpay.com/oauth/token?  
  
grant_type=authorization_code&  
  
code=150d91267a8e45b0bbee720795dc4ac5&  
  
client_id=146027875337921&  
  
client_secret=5e521967f1bd4612b3e3fda32aaaacf3&  
  
redirect_uri=http%3A%2F%2Fwww.example.com%2Foauth_redirect
```

响应结果

若参数无误，服务器将返回一段 JSON 文本，包含以下参数：

参数名	介绍
access_token	要获取的 Access Token

expires_in	Access Token 的有效期，以秒为单位
refresh_token	用于刷新 Access Token 的 Refresh Token
scope	Access Token 最终的访问范围，访问范围现有 basic 和 logistics ,以空格分隔，logistics 指的是访问物流地址的权限
uid	已授权的用户在银联在线支付系统的用户号

例如：

```
HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-store

{

  "access_token": "6c64a42c69094a238e0d9ee4da6d0ed4",

  "expires_in": 2592000,

  "refresh_token": "f90ef6b607c94708b3e6451eac0c0ec3",

  "scope": "basic logistics",

  "uid": "1245691"

}
```

通过 Refresh token 获取 Access Token

无论通过 OAuth2.0 哪种方式获取 Access Token，都会拿到一个有效期为 5 小时的 Access Token 和有效期为 1 天的 Refresh Token。对于这些应用，只要用户在 1 天内登录，应用就可以使用 Refresh Token 刷新以获得新的 Access Token（新的 Refresh Token 也会同时下发），因此用户只要在 1 天内登录过你的应用，就不需要重新登录。

调用地址

<https://online.unionpay.com/oauth/token>

请求方式

http post

请求参数

参数名	必选	介绍
grant_type	true	固定为“refresh_token”
refresh_token	true	用于刷新 Access Token 用的 Refresh Token
client_id	true	申请的第三方商户 ID
client_secret	true	商户密钥

例如:

```
https://online.uinonpay.com/oauth/token?  
  
grant_type=refresh_token&  
  
refresh_token=f90ef6b607c94708b3e6451eac0c0ec3&  
  
client_id=769868076312474&  
  
client_secret=5e521967f1bd4612b3e3fda32aaaacf3&
```

响应结果

若参数无误，服务器将返回一段 JSON 文本，包含以下参数：

参数名	介绍
access_token	要获取的 Access Token
expires_in	Access Token 的有效期，以秒为单位
refresh_token	用于刷新 Access Token 的 Refresh Token
scope	Access Token 最终的访问范围，访问范围现有 basic 和 logistics ,以空格分隔，logistics 指的是访问物流地址的权限

```
HTTP/1.1 200 OK  
  
Content-Type: application/json  
  
Cache-Control: no-store  
  
{  
  
  "access_token": "6c64a42c69094a238e0d9ee4da6d0ed4",
```

```
"expires_in": 2592000,

"refresh_token": "f90ef6b607c94708b3e6451eac0c0ec3",

"scope": " basic logistics"

}
```

四、 资源获取接口

注意：所有的资源获取接口默认返回的都是用 URL 编码后的字符（字符集为 UTF-8）

用户信息获取接口

调用地址

<https://online.unionpay.com/oauth/user>

请求方式

http get/post

请求参数

参数名	必选	介绍
access_token	true	访问令牌,如:6c64a42c69094a238e0d9ee4da6d0ed4

响应结果

若参数无误，服务器将返回一段 JSON 文本，包含以下参数：

参数名	介绍
uid	用户号

name	用户姓名，若无则返回空的文本信息
email	邮箱，若无则返回空的文本信息

注意：1、如果商户没有申请此接口的访问权限(basic)，则返回错误报文；2、返回报文后续可能会增加参数，需要客户端进行兼容支持。

```
HTTP/1.1 200 OK

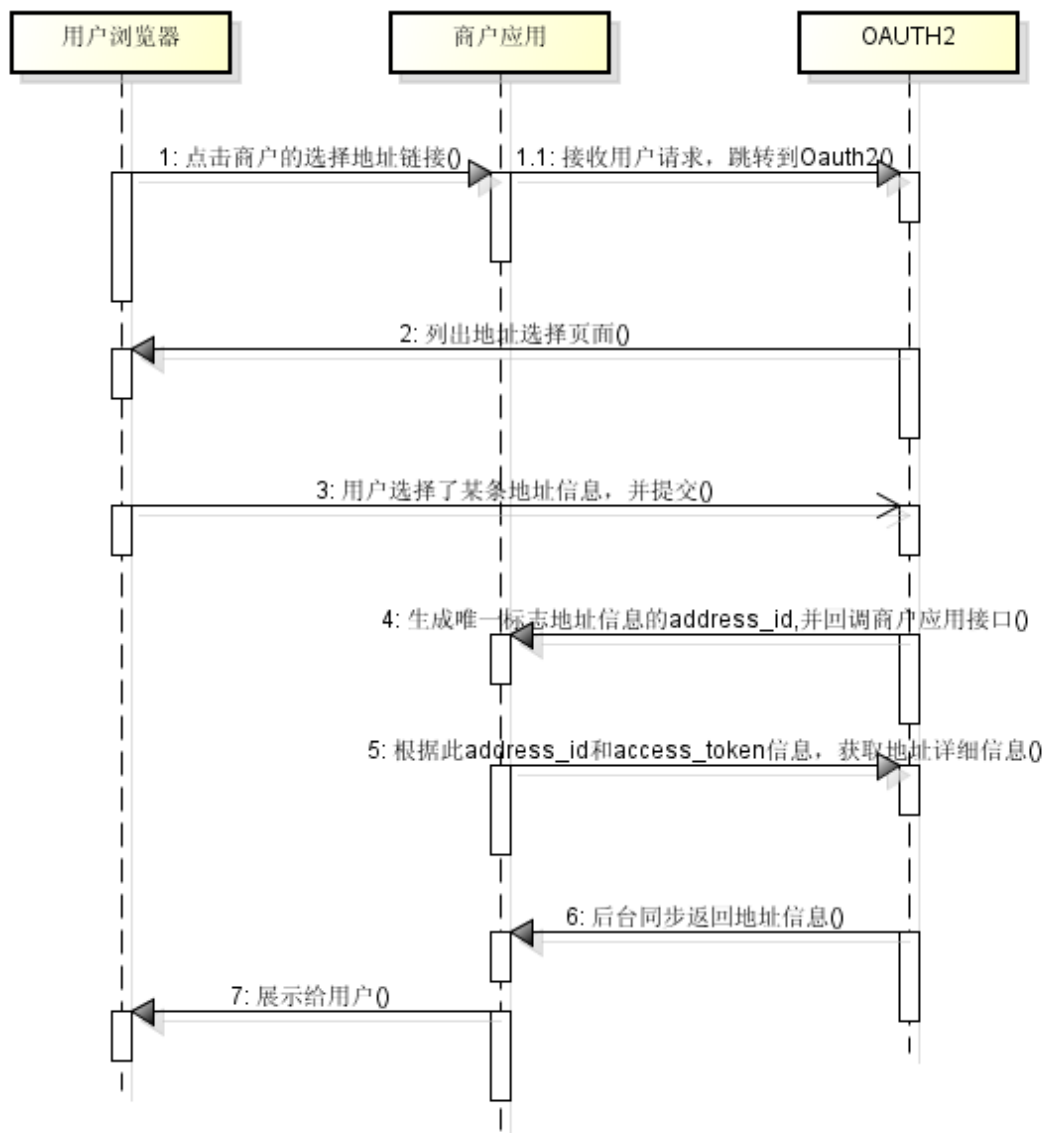
Content-Type: application/json

Cache-Control: no-store

{
    "uid": "12932845",
    "name": "\u5434\u4e09",
    "email": "123@abc.com"
}
```

地址信息获取接口

地址信息获取的流程如下图所示：



大致流程说明:

1. 用户在已登录的情况下, 在商户页面上有链接指向银联 `oauth` 的地址选择页面
2. 浏览器新弹出页面, 列出用户已保存的地址列表供用户选择
3. 选择好地址后, 提交, `oauth` 将新生成与地址信息关联的 `address_id` 重定向到商户的接收 URL。
4. 商终端应用接收到结果后, 用获取的 `address_id` 调用地址获取接口来获取用户在页面上选择的地址信息

地址信息前台选择

调用地址

<https://online.unionpay.com/oauth/addressChoose.do>

请求方式

http get/post

请求参数

参数名	必选	介绍
uid	true	用户号
client_id	true	分配给商户的 id
redirect_uri	true	返回给商户的 url, 如: http://www.example.com/address/callback.do
state	false	用于保持请求和回调的状态, 授权服务器在回调时 (重定向用户浏览器到“redirect_uri”时), 会在 Query Parameter 中原样回传该参数

响应结果

若参数无误, 服务器将提交表单至商户的接收地址, 包含以下参数:

参数名	介绍
address_id	用户选择的物流地址号
state	用于保持请求和回调的状态, 授权服务器在回调时 (重定向用户浏览器到“redirect_uri”时), 会在 Query Parameter 中原样回传该参数

```
<form action=http://www.example.com/address/callback.do
method="post" name="autoPostForm" id="autoPostForm" >

    <input type="hidden" name="address_id" value="35564" />

</form>
```

地址信息后台获取

调用地址

<https://online.unionpay.com/oauth/address>

请求方式

http get/post

请求参数

参数名	必选	介绍
access_token	true	访问令牌,如:6c64a42c69094a238e0d9ee4da6d0ed4
address_id	true	地址 ID,浏览器返回

响应结果

若参数无误，服务器将返回一段 JSON 文本，包含以下参数：

参数名	介绍
uid	用户号
recipient	收件人
post_code	邮政编码
address	地址详细信息
mobile	手机号
telephone	固定电话号码
province_code	省地区国标代码
city_code	市地区国标代码
district_code	区县地区国标代码

注意：

如果商户没有申请此接口的访问权限(logistics)，则返回错误报文。

地区代码请参考国家统计局官方网站发布的信息

HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-store

```
{
  "uid":12932845,
  "recipient": "%E8%B7%AF%E5",
  "post_code": "201103",
  "address": "%E4%B8%8A%E6%B5%B7%E5%B8%82%E9%BB%",
  " province_code ": "130000",
  " city_code ": "130100",
  " district_code ": "130102"
}
```

五、 错误码

说明

银联在线支付 OAuth2.0 实现中，服务器在接收到请求时，会按照 OAuth2.0 协议对本请求内容进行检验，若请求不合法或业务发生异常时，服务器会返回相应的错误信息，包含以下几个参数：

参数名	介绍
error	错误英文码
error_code	错误编号
error_description	错误描述

错误信息的返回方式为 JSON 文本：

例如：

```
{
  "error": "invalid_token ",
  "error_code": "30001 ",
  "error_description": " invalid token ,can not find access_token in authz server! "
}
```

错误码参考

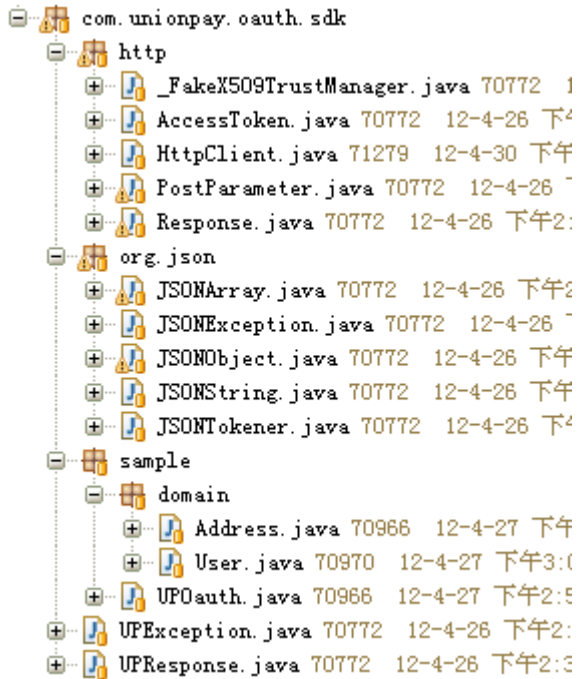
OAuth2.0 错误响应中的错误码定义如下表所示：

错误码(error)	错误编号(error_code)	错误说明
server_error	10001	系统内部异常
temporarily_unavailable	10002	当前服务暂不可用
invalid_request_method	10003	请求的 HTTP METHOD 不支持
invalid_client	10004	client_id、client_secret 参数无效
redirect_uri_mismatch	10005	redirect_uri 所在根域与注册应用时所填写根域名不匹配，或者与获取 authorization_code 时的值不一致
invalid_request	20001	请求缺少参数或者参数不合法要求
unauthorized_client	20004	应用没有被授权，无法使用所指定的 grant_type
access_denied	20101	请求被拒绝
unsupported_response_type	20102	请求的 response_type 参数缺失或无效
invalid_grant	20201	提供的 Access Grant 是无效的、过期的或已撤销的
unsupported_grant_type	20202	请求的 grant_type 参数缺失或无效
invalid_token	30001	请求的 access_token 参数缺失或无效、已过期
insufficient_scope	30002	请求的资源访问没有权限，或商户没有开通此接口
invalid_user	30003	请求的 uid 参数无效

invalid_address	30201	请求的 address_id 参数无效
-----------------	-------	---------------------

六、 示例代码说明

示例代码的包结构如下：



注释：

1. http 目录下的类负责与银联 oauth 服务器的交互。
2. org.json 目录下的类负责 json 数据的解析。
3. sample 目录下的类则是用于指导开发的示例代码。详细可参考 UPOauth.java。