

Oauth2.0 协议

目录

1	Oauth2.0 接口定义	1
1.1	获取授权码	1
1.2	获取访问令牌（授权码模式）	2
1.3	获取访问令牌（客户端模式）	3
1.4	刷新访问令牌	4
2	附录	6
2.1	签发 access_token 包含参数	6
2.2	OAuth2.0 返回码	6

1 OAuth2.0 接口定义

1.1 获取授权码

一、接口描述

第三方 APP 附带身份认证参数访问登录页面，通过身份验证可打开登录页面。用户使用账号登录，登录成功后 TSP 调用第三方授权回调地址返回授权码。

请求方式：GET。

二、请求附带参数

序号	元素名称	数据类型/长度	说明	必填
1-1	response_type	string	授权类型，固定值 code	是
1-2	client_id	string	第三方平台 ID，oauth_clientid	是
1-3	scope	string	权限范围，示例：scp01001（用于扩展，作者程序中并未校验此参数）	否
1-4	state	string	客户端的当前状态，可以指定任意值，认证服务器返回客户端所指定的值	是
1-5	redirect_uri	string	账号登录授权回调地址	是

请求示例：

http://localhost:8010/oauth2/authorize?client_id=oauth_clientid&response_type=code&scope=scp01001&state=201&redirect_uri=http://www.baidu.com

三、回调附带参数

1. 成功响应附带参数

序号	元素名称	数据类型/长度	说明	必填
1-1	code	string	授权码，用于获取访问令牌，UUID，每个 code 仅可以使用一次，有效期为 5 分钟	是
1-2	state	string	客户端的当前状态，可以指定任意值，认证服务器返回客户端所指定的值	是

响应示例：

https://www.baidu.com/?state=201&code=37b3c978285bad5ac41001af70dc2b40

2. 失败响应附带参数

序号	元素名称	数据类型/长度	说明	必填
1-1	error_code	string	错误码，错误码定义参见附录 OAuth2.0 返回码	是
1-2	error_description	string	错误描述	是

2. 失败应答参数

序号	元素名称	数据类型/长度	说明	必填
1-1	error_code	string	错误码，错误码定义参见附录 OAuth2.0 返回码	是
1-2	error_description	string	错误描述	是

1.3 获取访问令牌（客户端模式）

一、接口描述

客户端请求获取用于访问资源服务的访问令牌。

请求方式：POST。

二、请求参数

序号	元素名称	数据类型/长度	说明	必填
1-1	grant_type	string	授权类型： client_credentials: 获取访问令牌（客户端模式）	是
1-2	client_id	string	第三方平台 ID, oauth_clientid	是
1-3	client_secret	string	第三方平台密码, oauth_clientsecret	是
1-4	scope	string	权限范围，示例：scp01001	是

请求示例:

Content-Type: application/x-www-form-urlencoded

```
grant_type=client_credentials&client_id=oauth_clientid&client_secret=oauth_clientsecret&scope=s
cp01001
```

三、应答参数

1. 成功应答参数

序号	元素名称	数据类型/长度	说明	必填
1-1	access_token	string	访问令牌，用于第三方访问资源服务，包含参数参见附录 签发 access token 包含参数	是
1-2	expires_in	int	过期时间，东八区 UTC 时间，默认签发时间+120min	是

```
{  
    "expires_in":7200,  
    "access_token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IlRTUDAxIn0.eyJzY3AiOiJzY3AwMTAwMSIsImV4cCI6IjE1NDE1NjQ4NTQiLCJzdWl0eSI6IjB0bnQiOiJPYXV0aF9DTiIsImF1dCI6IjE1NDE1NjQ4NTQiLCJwcm9udGVudCI6IjE1NDE1NjQ4NTQiLCJkaXI6IjE1NDE1NjQ4NTQiLCJmYW90IjoiIiwiaWF0IjoiMjAyMy0xMi0yNSAwOjowOjAwLjAifQ.INHMTzmzoM0ugj7jAs5LQ5qvY0shgk_TEWy4muUhci",  
}
```

2. 失败应答参数

序号	元素名称	数据类型/长度	说明	必填
1-1	error_code	string	错误码，错误码定义参见附录 OAuth2.0 返回码	是
1-2	error_description	string	错误描述	是

1.4 刷新访问令牌

一、接口描述

客户端通过授权码模式获取的访问令牌过期时请求刷新访问令牌。

请求方式：POST。

二、请求参数

序号	元素名称	数据类型/长度	说明	必填
1-1	grant_type	string	授权类型： refresh_token：刷新访问令牌	是
1-2	client_id	string	第三方平台 ID，oauth_clientid	是
1-4	client_secret	string	第三方账号密码，oauth_clientsecret	是
1-3	refresh_token	string	刷新码，刷新访问令牌必填	是

请求示例：

```
{
  "grant_type": "refresh_token",
  "client_id": "oauth_clientid",
  "client_secret": "oauth_clientsecret",
  "refresh_token": "075e162208578c4e266eef826635f0cc"
}
```

三、应答参数

1. 成功应答参数

序号	元素名称	数据类型/长度	说明	必填
1-1	access_token	string	访问令牌，用于第三方访问资源服务，包含参数参见附录 签发 access token 包含参数	是
1-2	refresh_token	string	刷新码，用于刷新访问令牌，UUID	是
1-3	expires_in	int	过期时间，东八区 UTC 时间，默认签发时间 +120min	是

```
{
  "expires_in": 7200
}
```

2. 失败应答参数

2 附录

2.1 签发 access_token 包含参数

序号	元素名称	数据类型/长度	说明	必填
1	Header	0		是
1-1	alg	string	加密算法, HS256	是
1-2	typ	string	签发类型, 默认 JWT	是
2	Payload	0		是
2-1	iss	string	签发方, 示例: TSP01	是
2-2	aud	string	接收方, 示例: baidu	
2-3	iat	string	签发时间, 东八区 UTC 时间	是
2-4	exp	string	过期时间, 东八区 UTC 时间, 默认签发时间+120min	是
2-5	scp	string	权限范围, 示例: scp01	是
2-6	sub	string	用户 ID (授权码模式必返回, 客户端模式为空)	

2.2 OAuth2.0 返回码

code	description
100201	服务器处理超时
100400	请求参数不符合协议规范
100500	服务器异常
100901	授权服务器不支持客户端所指定的 response_type
100902	scope 无效
100903	access_token 无效或已过期
100904	client_id 不存在
100905	client_id 和 client_secret 不匹配
100906	授权码无效或已过期
100907	refresh_token 无效或已过期