**OAuth2.0 –合作方使用第三方账号登录并授权的接口文档**

[版本修改说明 1](#_Toc485030841)

[1、词汇说明 1](#_Toc485030842)

[2、概述 1](#_Toc485030843)

[4、授权有效期 2](#_Toc485030844)

[5、响应数据包格式规范 3](#_Toc485030845)

[5.1、JSON格式输出 3](#_Toc485030846)

[5.2、错误响应输出格式 3](#_Toc485030847)

[5.3、错误码定义 3](#_Toc485030848)

[5.4、HTTP响应码 5](#_Toc485030849)

[6、oauth2接口说明 5](#_Toc485030850)

[6.1、/oauth2/exchange\_access\_token 5](#_Toc485030851)

[6.2、回调验证third\_token和third\_uid接口 7](#_Toc485030852)

[7、参考资料 8](#_Toc485030853)

# 版本修改说明

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 版本 | 修改记录 | 作者 |
| 2017-06-12 | V 1.0 | 第一版 | yatin@ximalaya.com |

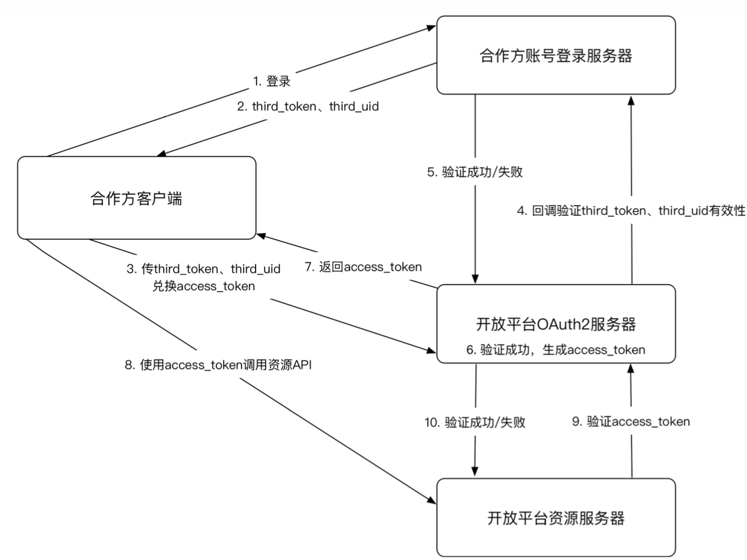
# 1、词汇说明

|  |  |
| --- | --- |
| app\_key或client\_id | 应用公钥，在创建开放平台应用时生成 |
| app\_secret或client\_secret | 应用私钥，在创建开放平台应用时生成 |
| response\_type | 表示授权类型，授权码模式时的值固定为"code" |
| grant\_type | 授权模式：authorization\_code表示授权码模式 |
| access\_token | 访问令牌 |

# 2、概述

本文档主要是关于合作方在他们的客户端使用合作方自己的账号登录并换取喜马拉雅oauth2授权access\_token的整体方案设计和接口说明。

**3、整体流程**



以下是以上流程图中各个环节的描述：

1. 【步骤1】合作方客户端调用合作方账号登录服务器完成登录，登录成功会通过【步骤2】返回标识第三方账号登录状态的third\_token和唯一标识第三方登录账号的third\_uid（第三方账号ID）；
2. 【步骤3】合作方调用喜马拉雅开放平台oauth2服务器[/oauth2/exchange\_access\_token接口](#_6.1、/oauth2/exchange_access_token)换取access\_token，需要把上一步骤的third\_uid和third\_token传过去；
3. 【步骤4】开放平台oauth2服务器回调合作方账号登录服务器验证third\_uid和third\_token的有效性，回调地址作为应用属性预先配置好，回调接口规范见[6.2节](#_6.2、回调验证third_token和third_uid接口)说明。验证结果会通过【步骤5】返回。
4. 【步骤6】如果验证通过，则会生成并返回access\_token.
5. 【步骤7】返回access\_token给合作方客户端，合作方之后可以使用access\_token去调用开放平台提供的各个服务API.

# 4、授权有效期

OAuth2.0获得的access\_token有过期时间的，通常access\_token过期时间为**2小时**。

# 5、响应数据包格式规范

## 5.1、JSON格式输出

响应数据以JSON格式输出，HTTP响应头中的Content-Type为固定值application/json, charset=utf-8，字符编码格式为UTF-8。

## 5.2、错误响应输出格式

错误响应输出包括error\_no错误编号、error\_code错误码和error\_desc错误描述。其中error\_no按照1xx系列到5xx系列对错误情况进行分组，比如1xx系列全部表示通用错误、2xx系列全部表示OAuth 2相关错误、5xx系列表示服务器内部错误。

错误响应格式如下：

|  |
| --- |
| {  "error\_no": [错误编号],  "error\_code":[错误码],  "error\_desc": [错误描述],  "service": [出错的服务名]  } |

上述error\_no、error\_code和error\_desc一定会返回，而service可能返回，也可能不返回。

## 5.3、错误码定义

开放平台错误码定义如下表（后面可能会增加新的错误码或者对某些错误码做调整）：

|  |  |  |  |
| --- | --- | --- | --- |
| 100 | ximalaya.common.request\_param\_check\_failed | | 参数校验失败错误，包括参数缺失、参数格式错误等情况 |
| 101 | ximalaya.common.signature\_check\_failed | | 签名验证失败 |
| 102 | ximalaya.common.permission\_validate\_failed | | 权限验证失败 |
| 103 | | ximalaya.common.app\_validate\_failed | app\_key无效或者应用处于不可用状态或者应用的client\_os\_type、pack\_id等参数不匹配 |
| 104 | ximalaya.common.request\_out\_of\_limit | | 调用请求次数超出限额 |
| 105 | | ximalaya.common.http\_method\_invalid | HTTP谓词使用错误，比如有的API接口明确要求用POST，而你却用了GET |
| 200 | ximalaya.oauth2.redirect\_uri\_invalid | | 回调地址无效 |
| 201 | ximalaya.oauth2.response\_type\_invalid | | 授权类型无效 |
| 202 | ximalaya.oauth2.scope\_grant\_denied | | 授权范围无效或超出权限许可范围 |
| 203 | ximalaya.oauth2.authorization\_code\_invalid | | 授权临时票据code错误或失效 |
| 204 | ximalaya.oauth2.authorization\_grant\_denied | | 授权访问失败：用户或者授权服务器拒绝授予数据访问权限 |
| 205 | ximalaya.oauth2.grant\_type\_invalid | | 授权模式无效 |
| 206 | ximalaya.oauth2.access\_token\_invalid\_or\_expired | | 授权访问令牌access\_token无效或过期 |
| 207 | ximalaya.oauth2.user\_login\_failed | | 用户登录验证失败：用户名或密码错误；或者ssoCode失效 |
| 208 | ximalaya.authenticate.oauth2\_authenticate\_failed | | Oauth2签名验证失败 |
| 209 | ximalaya.authenticate.oauth2\_device\_id\_invalid | | device\_id无效 |
| 210 | ximalaya.common.app\_validate\_failed | | app\_key无效或者应用处于不可用状态 |
| 211 | ximalaya.common.uid\_is\_missing\_or\_invalid | | uid缺失或无效 |
| 212 | ximalaya.oauth2.refresh\_token\_invalid\_or\_expired | | 刷新令牌refresh\_token无效或过期 |
| 213 | ximalaya.oauth2.third\_uid\_invalid | | third\_uid无效 |
| 214 | ximalaya.oauth2.third\_token\_invalid | | third\_token无效 |
| 215 | ximalaya.oauth2.third\_token\_validate\_uri\_invalid | | 合作方的third\_token验证地址无效 |
| 216 | ximalaya.oauth2.third\_token\_validate\_failed | | third\_token无效或者过期，导致验证失败 |
| 500 | ximalaya.system.internal\_service\_error | | 调用开放平台内部服务发生错误 |
| 501 | ximalaya.system.thirdparty\_service\_error | | 调用第三方服务发生错误 |
| 502 | ximalaya.system.unknown\_server\_error | | 未知服务器错误 |

每个应用都有调用请求频率限制，如果超出限制就会返回104错误码。目前限制规则如下：

* 测试环境：每个应用每分钟限额200次，每个应用每小时限额3000次
* 线上环境：待定；

## 5.4、HTTP响应码

HTTP响应码说明如下：

|  |  |
| --- | --- |
| 响应码 | 描述 |
| 200 | 请求成功 |
| 201 | 创建成功 |
| 202 | 更新成功 |
| 301 | 请求永久重定向 |
| 302 | 请求临时重定向 |
| 304 | 未更改 |
| 400 | 请求地址不存在或者包含不支持的参数 |
| 401 | 未授权，因为未成功进行身份认证 |
| 403 | 被禁止访问，因为没有访问特定资源的权限 |
| 404 | 请求的资源不存在 |
| 422 | 服务器理解请求，但其中包含非法参数（如包含XSS攻击风险参数） |
| 429 | 调用请求频率超出限额 |
| 500 | 服务器内部错误 |

# 6、oauth2接口说明

## 6.1、/oauth2/exchange\_access\_token

**功能**

exchange模式下，第三方使用third\_uid和third\_token换取授权后的access\_token。

**适用范围**

SDK对接。

**HTTP Method**

POST

**注意：**

**Content-Type请求头必须设为**

**application/x-www-form-urlencode；**

**参数**

包括下列参数：

|  |  |  |  |
| --- | --- | --- | --- |
| **参数** | **必选** | **类型** | **说明** |
| client\_id | 是 | string | 申请应用时分配的appKey |
| device\_id | 是 | string | 设备唯一标识 |
| grant\_type | 是 | string | 表示使用授权模式，填写token\_exchange |
| nonce | 是 | string | 随机字符串，长度建议8-32位，每次请求都要重新生成，用于防重放攻击 |
| timestamp | 是 | Long | Unix毫秒数时间戳，每次请求都要重新生成，用于防重放攻击 |
| third\_uid | 是 | string | 第三方登录唯一账号（oauth2服务器会调用合作方提供的6.2接口验证third\_uid有效性） |
| third\_token | 是 | string | 第三方标识账号登录状态的token（oauth2服务器会调用合作方提供的6.2接口验证third\_token有效性） |
| sig | 是 | string | 参数签名，对除sig外所有参数进行签名 |

**返回数据：**

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **必选** | **类型** | **说明** |
| access\_token | 是 | string | 获取授权后的access token。 |
| expires\_in | 是 | Int | access\_token的生命周期，单位是秒数 |

**实例**

|  |  |
| --- | --- |
| URL | **https://api.ximalaya.com/oauth2/exchange\_access\_token**（**POST方式**）  Body:  [grant\_type=token\_exchange&nonce=aafdfsasd&timestamp=1453089576872&client\_id=](http://192.168.3.54:8206/oauth2-auth-app/exchange_access_token?grant_type=token_exchange&nonce=aafdfsasd&timestamp=1453089576872&client_id=7721f10cb16aeb985303615f8e9f4aa5&device_id=dasffasddafs&third_uid=baidui123&third_token=afdsfasdweew22&sig=1cca8b158629673e347739f803a9df8c)b617866c20482d133d5de66fceb37da3[&device\_id=123dasffasddafs&third\_uid=alibaba123&third\_token=afdsfasdweew22&sig=](http://192.168.3.54:8206/oauth2-auth-app/exchange_access_token?grant_type=token_exchange&nonce=aafdfsasd&timestamp=1453089576872&client_id=7721f10cb16aeb985303615f8e9f4aa5&device_id=dasffasddafs&third_uid=baidui123&third_token=afdsfasdweew22&sig=1cca8b158629673e347739f803a9df8c)0ccfacd263b2224f7442dcfd35e1875c |
| 响应内容 | {      "access\_token": "SlAV32hkKGsdUUTjh",      "expires\_in": 7200, // 单位为秒  } |

## 6.2、回调验证third\_token和third\_uid接口

**功能**

该接口由合作方实现并提供给开放平台使用。合作方需要按照如下接口规范实现，并提供接口地址给喜马拉雅开放平台工程师配置（配置为开放平台应用属性）；

**接口规范说明：**

**接口名**

**/ximalaya/validate\_third\_token**

Http Method

**POST**

**入参：**

包括下列参数

|  |  |  |  |
| --- | --- | --- | --- |
| **参数** | **必选** | **类型** | **说明** |
| app\_key | 是 | string | 申请应用时分配的appKey |
| nonce | 是 | string | 随机字符串，长度建议8-32位，每次请求都重新生成，用于防重放攻击 |
| timestamp | 是 | Long | Unix毫秒数时间戳，每次请求都重新生成，用于防重放攻击 |
| third\_uid | 是 | string | 第三方登录唯一账号 |
| third\_token | 是 | string | 第三方标识账号登录状态的token |
| sig | 是 | string | 参数签名，对除sig外所有参数进行签名。  **签名参数生成算法**如下（贵方需对此签名参数进行检查）：  **A、将其他所有请求参数的原始值按照参数名的字典序排序；**  **B、将排序后的参数键值对用&拼接，即拼接成key1=val1&key2=val2这样的形式；**  **C、在B步骤得到的字符串后拼上app\_secret，比如app\_secret为abc，那么现在就得到key1=val1&key2=val2&app\_secret=abc；**  **D、对C步骤得到的字符串进行MD5运算得到32位小写字符串，即为sig** |

# 7、参考资料

1). http://open.weibo.com/wiki

2) https://mp.weixin.qq.com/wiki

3) http://drops.wooyun.org/papers/598