**喜马拉雅OAuth2.0-标准登录授权流程及接口说明**

[版本修改说明 1](#_Toc488074770)

[1、词汇说明 1](#_Toc488074771)

[2、概述 2](#_Toc488074772)

[3、响应数据包格式规范 3](#_Toc488074773)

[3.1、JSON格式输出 3](#_Toc488074774)

[3.2、错误响应输出格式 3](#_Toc488074775)

[3.3、错误码定义 3](#_Toc488074776)

[3.4、HTTP响应码 5](#_Toc488074777)

[4、oauth2授权流程和接口说明 5](#_Toc488074778)

[4.1、初始化状态下，引导用户到登录页面登录； 6](#_Toc488074779)

[4.1.1、https://m.ximalaya.com/login 6](#_Toc488074780)

[4.2、用户登录成功后，会自动跳转确认授权页面； 7](#_Toc488074781)

[4.3、用户同意授权后，重定向到合作方服务端的redirect\_uri网址上，并带上临时授权码code和state 7](#_Toc488074782)

[4.3.1 redirect\_uri?code=$CODE&state=$STATE&device\_id=$DIVICE\_ID 7](#_Toc488074783)

[4.4、合作方服务端通过code获取access\_token和refresh\_token. 8](#_Toc488074784)

[4.4.1、/oauth2/v2/access\_token 8](#_Toc488074785)

[4.5、合作方服务端刷新access\_token有效期 9](#_Toc488074786)

[4.5.1、/oauth2/refresh\_token 10](#_Toc488074787)

[4.6、access\_token异常过期情况下，合作方服务端可以通过4.6.1接口查询access\_token有效性 12](#_Toc488074788)

[4.6.1、/oauth2/get\_token\_info 12](#_Toc488074789)

[5、关于state参数的说明 13](#_Toc488074790)

# 版本修改说明

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 版本 | 修改记录 | 作者 |
| 2017-07-17 | V 1.0 | 初稿 | yatin@ximalaya.com |

# 1、词汇说明

|  |  |
| --- | --- |
| app\_key | 应用公钥，在创建开放平台应用时生成 |
| app\_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 |
| redirect\_uri | 授权回调地址，站外应用需与注册应用时设置的回调地址一致**（请使用urlencode对链接进行处理,最好提供https回调地址）** |
| state | 表示客户端的当前状态，见[5、state参数说明](#_5、关于state参数的说明) |
| display | 授权页面的终端类型 |
| scope | 申请权限所需参数 |
| code | 授权码，用于调用access\_token接口获取授权后的access token。 |
| access\_token | 访问令牌 |
| Authorization Server | 喜马拉雅认证服务器 |
| Resource Server | 喜马拉雅开放平台服务器 |
| Resource Owner | 喜马拉雅用户 |

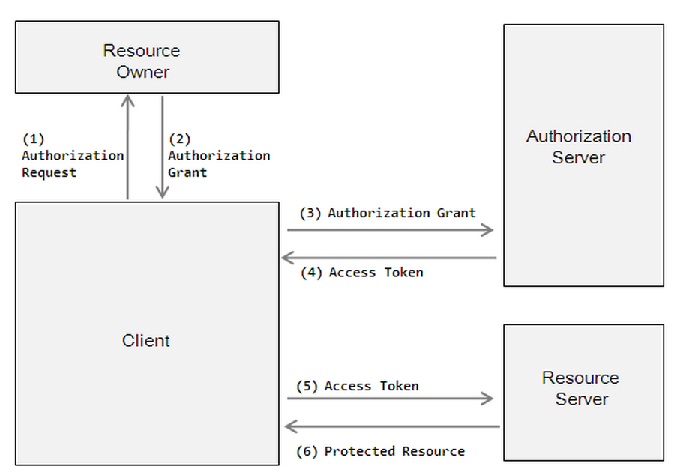
# 2、概述

**本文档主要描述喜马拉雅OAuth2标准授权协议整体实现流程以及接口说明。**

喜马拉雅开放平台标准授权登录流程采用OAuth2标准授权码（authorization code）模式。**授权码模式（authorization code）是功能最完整、流程最严密的授权模式。它的特点就是通过第三方客户端的后台服务器，与我们的oauth2认证服务器进行互动。**总体来说先进行用户登录，再进行用户授权。

注意：这种授权模式不会存储任何私钥在客户端（或浏览器端）。

这种授权模式的流程示意图如下：



# 3、响应数据包格式规范

## 3.1、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。

## 3.2、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。

## 3.3、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 |
| 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；

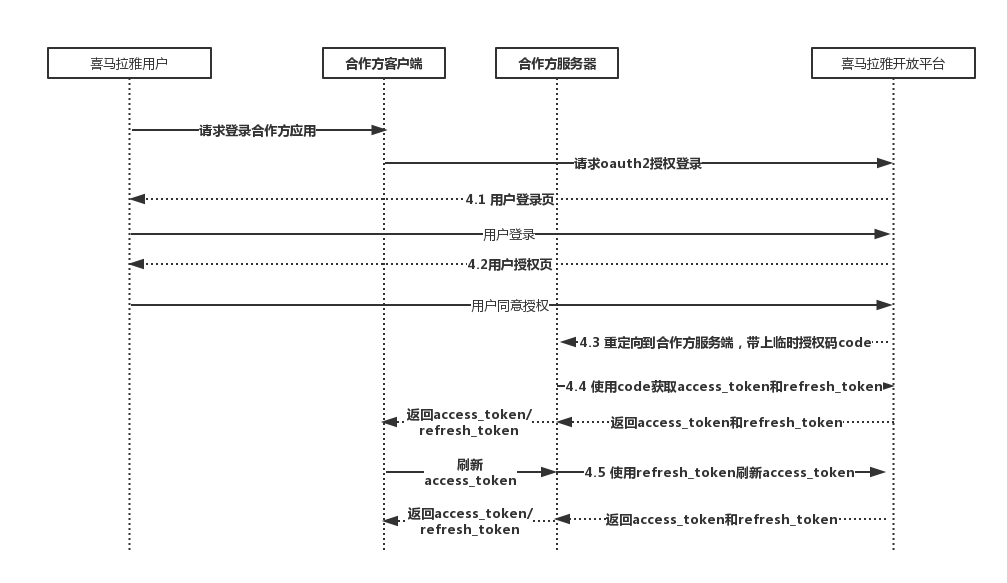
## 3.4、HTTP响应码

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 |

# 4、oauth2授权流程和接口说明

整体流程图示如下：



图中4.1、4.2、4.3、4.4、4.5具体说明如下.

## 4.1、初始化状态下，引导用户到登录页面登录；

1）若合作方客户端通过sdk方式对接，则sdk会自动引导跳到喜马拉雅登录页面，用户填写信息完成登录；

2）若合作方通过服务端方式接入，则需要自行控制跳转到我们的H5登录页面，用户填写信息完成登录。合作方服务端请求的喜马拉雅H5登录页面的网址如4.1.1所示；

### 4.1.1、https://m.ximalaya.com/login

**功能**

用于获取**喜马拉雅H5登录页面；**

**适用范围**

**第三方客户端或服务端**对接。

**HTTP Method**

GET

**请求参数**

|  |  |  |  |
| --- | --- | --- | --- |
| **参数** | **必选** | **类型** | **说明** |
| fromUri | 是 | string | https://api.ximalaya.com/oauth2/v2/authorize?client\_id=**[应用公钥]**&response\_type=code&redirect\_uri=**[oauth2回调地址]**&device\_id=**[设备唯一标识]**&**client\_os\_type=3**&state=**[表示合作方客户端的当前状态，可以指定任意值，认证服务器会原封不动地返回这个值]**  注意：fromUri参数需要进行urlencode；其中client\_id、redirect\_uri、device\_id、state需要填写合作方客户端相应的参数值； |

**注意：client\_os\_type一定要设为3（表示客户端为web方式接入）；**

**实例**

|  |  |
| --- | --- |
| URL | 线上环境：  https://m.ximalaya.com/login? fromUri=https%3A%2F%2Fapi.ximalaya.com%2Foauth2%2Fv2%2Fauthorize%3Fclient\_id%3D7721f10cb16aeb985303615f8e9f4aa5%26response\_type%3Dcode%26redirect\_uri%3Dhttps%3A%2F%2Fapi.ximalaya.com%2Fopenapi-collector-app%2Fget\_access\_token%26device\_id%3D869350024794165%26client\_os\_type%3D3%26state%3Ddaffsdfw23 |

## 4.2、用户登录成功后，会自动跳转确认授权页面；

在4.1步骤用户登录成功后，会自动跳转到喜马拉雅的确认授权页面，用户点击确认授权后，将继续4.3步骤；

## 4.3、用户同意授权后，重定向到合作方服务端的redirect\_uri网址上，并带上临时授权码code和state

在4.2步骤，用户点击同意授权后，将会重定向到合作方服务端的redirect\_uri的网址上，并且带上code和state参数，具体返回参数如下4.3.1所示；

### 4.3.1 redirect\_uri?code=$CODE&state=$STATE&device\_id=$DIVICE\_ID

redirect\_uri包含以下参数：

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **必选** | **类型** | **说明** |
| code | 是 | string | 临时访问授权码，用于调用access\_token接口获取授权后的access token和refresh\_token。 |
| state | 是 | string | 表示客户端的当前状态，可以指定任意值，认证服务器会原封不动地返回这个值。 |
| device\_id | 是 | string | 设备唯一标识 |

**实例**

|  |  |
| --- | --- |
| 响应内容 | 重定向url：  https://weibo.com/?state=sdkjlj3232&code=e24f730946d5f955e1e18fc84b2bf3db&device\_id= dasffasddafs |

## 4.4、合作方服务端通过code获取access\_token和refresh\_token.

在4.3步骤中合作方服务端获取临时访问授权码code后，使用code请求4.4.1接口获取访问令牌access\_token和refresh\_token.

### 4.4.1、/oauth2/v2/access\_token

**功能**

授权码模式下，获取授权后的access\_token和refresh\_token。**注意：此接口需要由合作方服务端调用。**

**适用范围**

第三方服务端对接。

**HTTP Method**

POST

**注意：**

**Content-Type请求头必须设为**

**application/x-www-form-urlencoded；**

**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 |
| client\_secret | 是 | string | 申请应用时分配的AppSecret |
| device\_id | 是 | string | 设备唯一标识 | |
| grant\_type | 是 | string | 表示使用授权模式，填写authorization\_code |
| code | 是 | string | 临时访问授权码code |
| redirect\_uri | 是 | string | 回调地址，需需与注册应用里的回调地址一致。（请使用urlencode对链接进行处理,最好提供https回调地址） |

**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 |
| refresh\_token | 是 | string | 用于刷新access\_token |
| uid | 是 | Int | 喜马拉雅用户id |
| device\_id | 是 | string | 设备唯一标识 |
| scope | 否 | string | 获得的授权范围, 使用逗号（,）分隔 |

**实例**

|  |  |
| --- | --- |
| URL | **线上环境地址**  **https://api.ximalaya.com/oauth2/v2/access\_token（POST方式）**  测试环境地址  **http://192.168.3.54:8206/oauth2-auth-app/v2/access\_token?**  Body:  grant\_type=authorization\_code&redirect\_uri=http://api.test.ximalaya.com:8137/openapi-collector-app/get\_access\_token&client\_secret=c1c9c9cc4b2d3e2982ce09513dad8ac8&client\_id=7721f10cb16aeb985303615f8e9f4aa5&device\_id=869350024794165&code=e24f730946d5f955e1e18fc84b2bf3db |
| 响应内容 | {      "access\_token": " 87b32b4972d3bc1233772f6dca2e4987",      "expires\_in": 604800, // 单位为秒      "refresh\_token": " b034ea4ed29d2eb676b926690caf5ac7",  "uid":12345,  "device\_id":"869350024794165",    "scope": "basic"  } |

## 4.5、合作方服务端刷新access\_token有效期

access\_token是调用开放平台资源接口的凭证，由于access\_token有效期（目前为2个小时）较短，当access\_token超时后，可以使用refresh\_token进行刷新，access\_token刷新结果有两种：

* **1）**. 若access\_token已超时，那么进行refresh\_token会获取一个新的
* access\_token，新的2小时超时时间；

**2）**. 若access\_token未超时，那么进行refresh\_token不会改变access\_token，但超时时间会刷新，相当于续期access\_token。

每次刷新access\_token时，refresh\_token的有效期也会被刷新为新的30天；当refresh\_token失效的后，需要用户重新授权。刷新access\_token的接口如下**4.5.1**所示；

### 4.5.1、/oauth2/refresh\_token

**功能**

OAuth2的refresh\_token接口。用于在refresh\_token有效且access\_token无效时刷新产生新的access\_token，若refresh\_token失效则需要用户重新授权。**注意：此接口需要由合作方服务端调用。**

**适用范围**

**第三方服务端**对接。

**HTTP Method**

POST

**注意：**

**Content-Type请求头必须设为**

**application/x-www-form-urlencoded；**

**请求参数**

包括下列参数：（不需要传递公共参数！）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **参数** | **必选** | | | **类型** | | | **说明** |
| grant\_type | 是 | | | string | 表示使用授权模式，填写refresh\_token | | |
| refresh\_token | 是 | | | string | | 用于刷新access\_token的refresh\_token参数 | |
| client\_id | 是 | | | string | | 申请应用时分配的公钥appKey | |
| client\_secret | 是 | | | string | | 申请应用时分配的私钥appSecret | |
| device\_id | 是 | | | string | | 设备唯一标识 | |
| redirect\_uri | | 是 | string | | | 授权回调地址，站外应用需与设置的回调地址一致**（请使用urlencode对链接进行处理,最好提供https回调地址）** | | |

**返回值：**

1. **若刷新成功，返回结果如下：**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |
| refresh\_token | 是 | string | 用户刷新access\_token |
| device\_id | 是 | string | 设备唯一标识 |

1. **若刷新失败，返回如下提示表示refresh\_token已过期，此时需要让用户重新登录授权；**

**{**

**"error\_no": 212,**

**"error\_code": "ximalaya.oauth2.refresh\_token\_invalid\_or\_expired",**

**"error\_desc": "refresh\_token is invalid or expired"**

**}**

**实例**

|  |  |
| --- | --- |
| URL | POST方式：  **线上环境地址**  **https://api.ximalaya.com/oauth2/refresh\_token?**  测试环境地址  **http://192.168.3.54:8206/oauth2-auth-app/refresh\_token?**  BODY:  grant\_type=refresh\_token&client\_id=7721f10cb16aeb985303615f8e9f4aa5&client\_secret=c1c9c9cc4b2d3e2982ce09513dad8ac8&device\_id=869350024794165&redirect\_uri=http://api.test.ximalaya.com:8137/openapi-collector-app/get\_access\_token&refresh\_token=b034ea4ed29d2eb676b926690caf5ac7 |
| 响应内容 | **返回值如下：**  {      "access\_token": "SlAV32hkKGsdUUTjh",      "expires\_in": 7200, // 单位为秒      "refresh\_token": " b034ea4ed29d2eb676b926690caf5ac7",  "device\_id":"869350024794165"  } |

## 4.6、access\_token异常过期情况下，合作方服务端可以通过4.6.1接口查询access\_token有效性

### 4.6.1、/oauth2/get\_token\_info

**功能**

OAuth2的查询access\_token信息接口。用于查询access\_token是否有效。

**（注意：正常流程不需要请求此接口来验证access\_token有效期的！）**

**适用范围**

第三方客户端或服务端对接。

**HTTP Method**

GET

**请求参数**

包括下列参数：（不需要传递公共参数！）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **参数** | **必选** | **类型** | | **说明** |
| access\_token | 是 | string | 授权得到的access\_token令牌 | |
| client\_id | 是 | string | 申请应用时分配的公钥appKey | |
| client\_secret | 是 | string | 申请应用时分配的私钥appSecret | |
| device\_id | 是 | string | 设备唯一标识 | |
| uid | 否 | Long | 喜马拉雅用户id | |

**返回值：**

**返回结果如下：**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |
| created\_at | 是 | Int | access\_token生成时间，单位秒 |
| uid | 是 | Long | 喜马拉雅用户id |

**实例**

|  |  |
| --- | --- |
| URL | GET方式：  线上环境：https://api.ximalaya.com/oauth2/get\_token\_info?  client\_id=7721f10cb16aeb985303615f8e9f4aa5&client\_secret=c1c9c9cc4b2d3e2982ce09513dad8ac8&access\_token=b034ea4ed29d2eb676b926690caf5ac7&deivce\_id=sdfsd1235&uid=12345 |
| 响应内容 | **access\_token有效时，返回值如下：**  {      "access\_token": " b034ea4ed29d2eb676b926690caf5ac7",      "expires\_in": 7200, // 单位为秒      "uid": "12345",  "created\_at":1491386657 //Unix时间戳，单位为秒  }  **access\_token失效时，返回值如下：**  {  "error\_no": 206,  "error\_code": "ximalaya.oauth2.access\_token\_invalid\_or\_expired",  "error\_desc": "access\_token is invalid or expired"  } |

# 5、关于state参数的说明

Oauth 2.0引入了state参数，用于保持请求和回调的状态，在回调时，会在Query Parameter中回传该参数。开发者可以用这个参数验证请求有效性，也可以记录用户请求授权页前的位置。这个参数可用于防止跨站请求伪造（CSRF）攻击。

**我们强烈建议，第三方每次发起授权都带上这个state参数。**

**state参数的生成原则**：既不可预测，又必须可以充分证明client和当前第三方网站的登录认证状态存在关联（如果存在过期时间更好）。

**state参数建议的生成方式：**随机算一个字符串，然后拼接上第三方用户uid或设备号等可识别客户端唯一标识信息，作为state参数然后保存在session，回调时检查state参数和session里面的值，就满足要求了。