权限微服务接入手册

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 内容 | 时间 | 备注 |
| 1.0 | 第三方应用使用权限微服务的流程 | 2016-7-14 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 背景

大部分微服务都使用鉴权微服务作为鉴权依据，因此第三方应用调用微服务前应先获得访问码才可以进行请求。本文主要介绍这一流程。

# 鉴权原理

微服务采用统一的鉴权服务提供权限认证服务，每一项微服务下可定义一组服务接口，并有分别唯一的服务编号和接口编号。鉴权服务为每个接口配置访问的权限。

需注意的是权限微服务采用的是客户端鉴权方式，即权限微服务只负责验证请求Token的有效性，并返回其对应的权限列表，而具体是否提供服务由被访问系统自行决定。详细鉴权流程如下：



图表 1

1. 请求方申请访问令牌Token

请求参数由Appkey、timestamp、sign组成，其中

sign=md5（Appkey+timestamp+appsecret）

1. 账号检测

鉴权服务判断Appkey/Secret是否匹配合法，是则生成一个32位的标识符作为访问令牌Token。一个Appkey允许同时拥有多个Token，且每个Token最大有效时间为120分钟，过期则失效。

请求方收到Token后应在本地缓存，并在每次使用前检查Token是否有效，如果临近失效（1分钟内）则应重新请求Token。

由于服务提供方要求IP鉴权，因此要求每台服务器都应适用独立的Token。

1. 请求服务
2. 鉴权

服务提供方收到请求后，检查本地Token在本地是否有缓存并有效，否则向鉴权服务请求鉴权。

1. 返回权限

鉴权服务返回指定Token对应的Token信息、访问权限集合。服务提供方收到权限集合后应在本地缓存。

1. 返回请求结果

服务提供方对照被请求地址是否在访问权限集合中，是则通过并返回结果，否则提示鉴权失败。

## 服务提供方鉴权流程



图表 2

# 接入流程

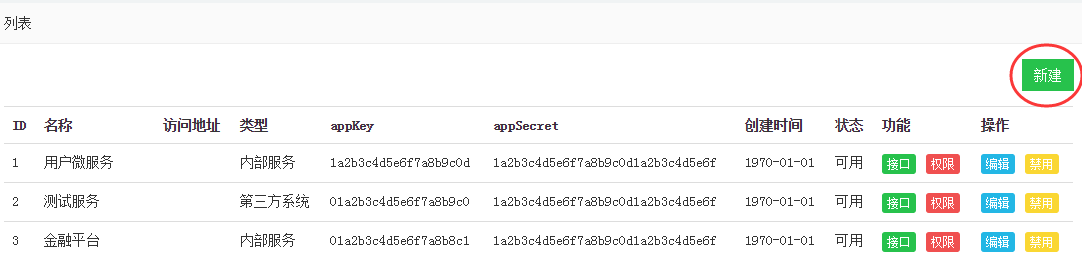
权限微服务接入分为两部分：账号分配、程序接入。

## 账号分配

账号分配由系统管理员登陆微服务管理后台完成，并将账号信息提供给接入方。

微服务管理后台地址：http://micro.colourlife.com/backend/login.html

新增接入点击下图红圈“新建”按钮，进入新增接入应用页面。



图表 3



图表 4

新增接入需按要求填写以下信息：

* 类型

必填项，应用类型主要为了区分不同的接入应用进行分类，并为将来权限扩展需要提供扩展空间。目前分为：微服务，彩之云系统，第三方系统。

微服务：彩生活集团内部IT系统及其附属的微服务。

彩之云系统：专指彩之云APP及其周边系统。

第三方系统：指除上述系统外的外部合作伙伴、专业公司的各类系统。

* 应用名称

必填项，命名接入应用的名称。

* 访问地址url

选填项，与实际请求地址无关，只备注接入应用的部署网址。

* ip白名单

选填项，保留字段，目前默认天255.255.255.255。

* 备注

选填项，接入应用说明。

**接入应用新增成功后，系统将自动生成20位的appkey和32位的appsercet**。

如接入方提供服务则需要配置接口，如接入方使用服务则需配置权限，具体操作见以下小节。

### 接口配置

接口是指应用对外提供的服务接口，是权限微服务鉴权的基本单位。申请接入时，提供服务的接入应用应提供完整的接口列表。

接口定义字段包括：

* 接口名称

必填项

* 访问地址url

必填项，接口访问的相对地址。如接口的完整请求地址是http://www.abc.com:1000/welcome/sayhello，则这里应填写welcome/sayhello

* 备注

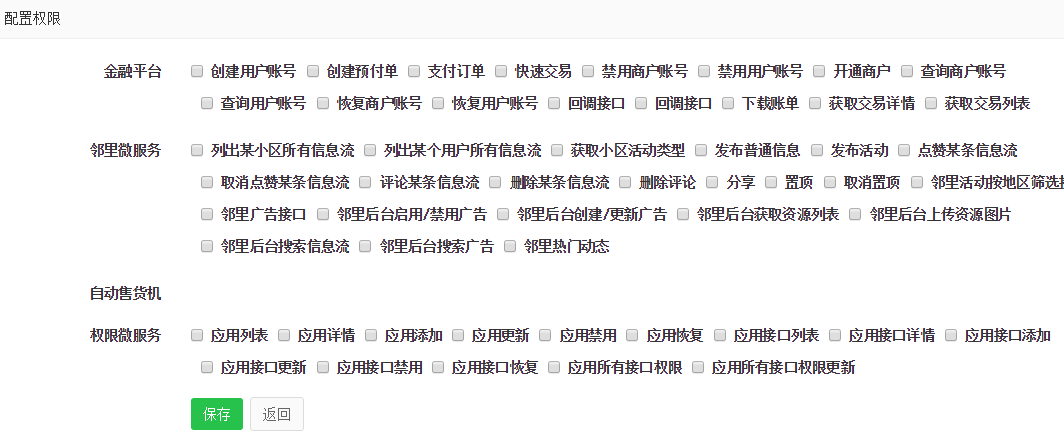
选填项，接口详细介绍。



图表 5

### 权限配置

权限是指接入应用可访问的接口集合。点击接入应用列表中的“权限”按钮进入权限配置页面。选中接口前方的复选框并保存即可获得访问权限。



图表 6

## 程序接入

### 接口规范

#### 请求

所有接口都以RESTFUL API的方式提供外部应用调用，外部应用调用统一采用POST的方式调用接口，返回标准的JSON格式数据。

#### 结果

所有接口返回结果格式统一为：

|  |  |  |
| --- | --- | --- |
| 字段 | 类型 | 说明 |
| code | 整形 | 结果码，0表示成功，其它失败 |
| message | 字符串 | 结果说明 |
| contentEncrypt | 字符串 | 加密结果，保留字段 |
| content | 字符串 | 非加密结果，下面接口中的“返回结果”默认表示content中的元素 |

例子：

*{*

*"code": 0,*

*"message": "",*

*"contentEncrypt": "",*

*"content":{*

*"expire": 1468931684,*

*"access\_token": "b8ced4c70c16b202664d6c5ef9de30e1"*

*}*

*}*

### 获取访问码

接口生成的access\_token，有效期为2小时。

|  |  |  |
| --- | --- | --- |
| **请求地址** | /app/auth | |
| **请求方式** | post | |
| **参数** | | **备注** |
| appkey | 应用编号 |  |
| timestamp | 时间戳 |  |
| signature | 签名，算法  md5(appKey + timestamp + appscret); |  |
| **返回结果** | | **备注** |
| expire | 过期时间，时间戳 |  |
| access\_token | 访问码 |  |
| **异常** | | |
| 2001 | 缺少key | |
| 2002 | 缺少时间戳 | |
| 2003 | 无效的时间戳，时间戳与当前时间误差超过20分钟 | |
| 2004 | 缺少签名 | |
| 2005 | 验证失败 | |
| 2006 | 应用不存在 | |

### 获取访问码权限

|  |  |  |
| --- | --- | --- |
| **请求地址** | /privilege/listprivilege | |
| **请求方式** | post | |
| **参数** | | **备注** |
| access\_token | 需获取权限的访问码（第三方应用的访问码） |  |
| token | 自身的访问码 |  |
| **返回结果** | | **备注** |
| appId | access\_token对应的应用id |  |
| app\_name | access\_token对应的应用名称 |  |
| privileges | access\_token对应的应用中本系统中的权限列表 | 数组，元素是访问接口的相对地址，如：  ['app/auth', 'privilege/list'] |
| **异常** | | |
| 100 | 缺少access\_token | |
| 101 | 无效的access\_token | |
| 3003 | 无效的Token | |
| 3004 | 应用不存在 | |