基于 OAuth2.0 的登录验证授权方式介绍

一、前言

如果您的应用和苏宁开放服务平台对接后，需要获取一些与用户紧密相关的信息（如订单、商品、促销等），为保证数据的安全性和隐私性，需要取得用户的同意，引导用户授权。苏宁开放服务平台采用国际通用的 OAuth2.0 标准协议，支持网站、桌面客户端、手机客户端。如果要了解更多关于 OAuth2.0 的技术说明，请参考官方网站 http://oauth.net/2/ 目前，苏宁开放服务平台的 OAuth2.0 支持以下方式获取 Access Token ， Token 有效时长为一年。

（1）Server-side flow 此流程要求 ISV 和商家应用有 Web Server，能够保持应用本身的密钥以及状态，可以通过 https 直接访问苏宁的授权服务器。

（2）Native Application 此流程适合 ISV 没有自己的 web 服务器，且应用为原生程序，即客户端应用（同时应用无法与浏览器交互，但是可以外调用浏览器）。

（3）Refreshing an Access Token 通过前两种流程，获取了 Access token 以及 Rrfresh token(刷新令牌，对于具有“获取 Refresh token 权限”的应用），Access token 都有一定的期限，当 Access token 过期时，用户可以用 Refresh token 获得一个 Access token。

二、名词解释

1. redirect_uri 和 callback 定义规则

redirect_uri 指的是应用发起请求时，所传的回调地址参数。
callback 指的是应用注册时填写的回调地址链接 或者网站接入时所验证的域名地址。

2. scope 定义规则

scope 指的是应用发起请求时，所请求的 API 调用权限范围。
scope 参数为以下可选值：
item,category, order
应用发起请求时，多个 scope 值要求用逗号分隔。
暂时不传

3. accessToken

Access Token 即用户授权后颁发的凭证。它代表了用户授予应用访问用户在苏宁上特定资源的权限。

4. AppKey 和 appSecret

AppKey 是创建应用时，开放平台分配给应用的的标识，用以鉴别应用的身份。
App Secret 是苏宁开放平台给应用分配的密钥，开发者需要妥善保存这个密钥，这个密钥用来保证应用来源的可靠性，防止被伪造。

三 Server-side flow

此流程要求应用有 Web Server，能够保持应用本身的密钥以及状态，可以通过 https 直接访问苏宁的授权服务器。
图 3.1 为 web server flow 授权流程图

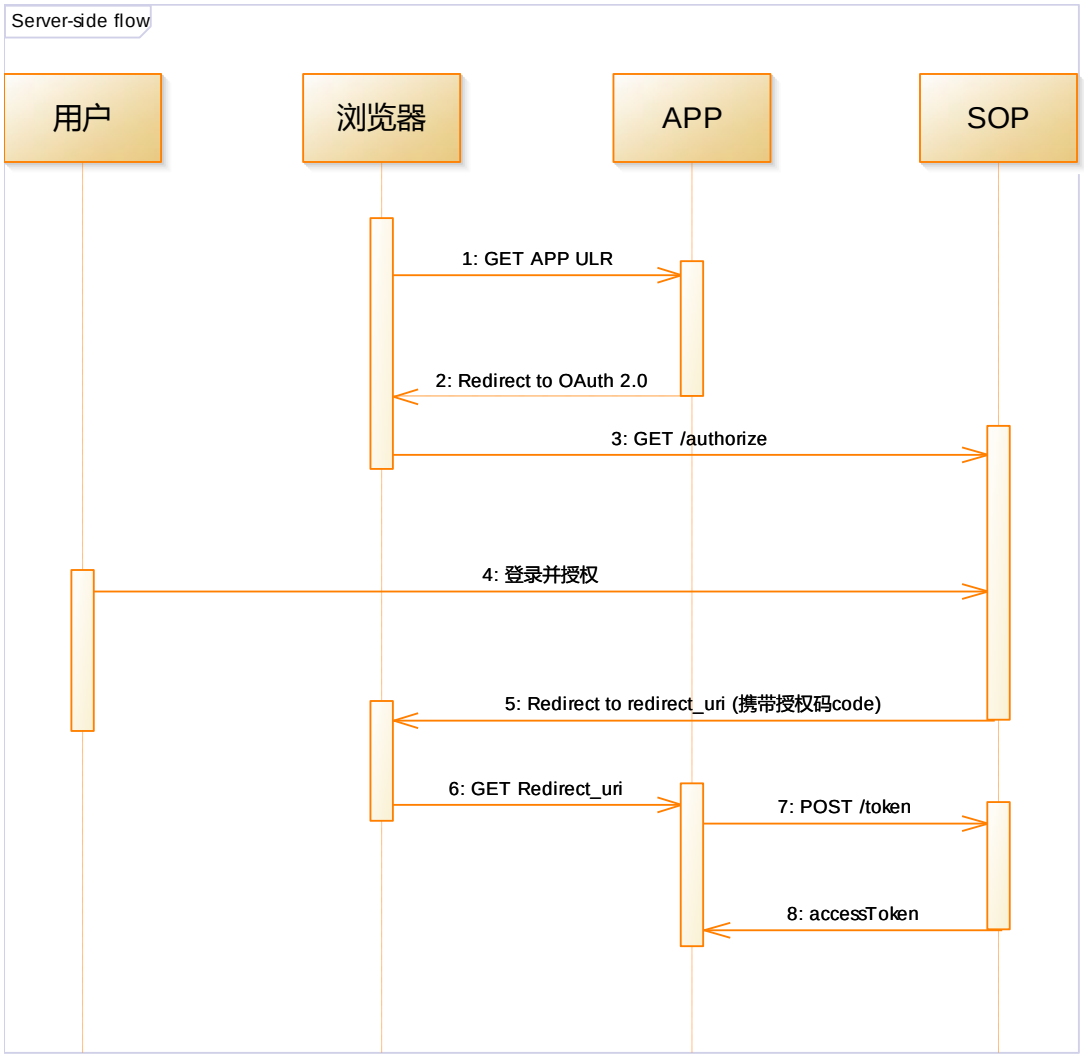


图 3-1 web server flow 授权流程图

授权过程分为两个步骤：

(1) 通过用户授权获取授权码 Code； （获取授权码:http://open.suning.com/api/oauth/authorize）

(2) 用上一步获取的 Code 和应用密钥（AppSecret）通过 Https Post 方式换取 Token。 （获取访问令牌：http://open.suning.com/api/oauth/token）

1. 参数说明

1.1 获取授权码参数

参数名字	参数选项	默认值	参数释义	用途描述	备注
client_id	必选		应用客户端标识	用来唯一标识应用	
response_type	必选	code	授权请求响	用来标识授权	请求访问令牌时参

			应类型	响应数据是访问令牌还是授权码信息	数值必须设为“token”，请求授权码时参数值必须设为“code”
redirect_uri	必选		授权响应重定向 URI	终端用户的授权步骤完成时授权服务器将要把 user-agent 重定向到的一个绝对 URI	应用注册时，需要预先注册它们的重定向 URI，再授权操作中，redirect_uri 必须和注册时的 URI 域名一致
scope	可选		授权范围	标识用户授予应用访问资源服务器上的资源范围	访问请求的作用域，以逗号隔开的字符串列表来表示 暂不使用
state	可选		状态码	维护请求和响应的状态，传入值与返回值保持一致	
View	可选	web		表示应用客户端类型，web 对应浏览器页面样式，wap 对应移动客户端样式。	

1.2 返回值说明

参数名字	参数选项	参数释义	用途描述
code	正常结果	授权码	授权码
error	异常时返回	错误码	错误码
error_description	异常时返回	错误码描述	错误码描述
state	可选	状态	维护请求和响应的状态

2.1 获取访问令牌参数

参数名字	参数选项	默认值	参数释义	用途描述	备注
client_id	必选		应用客户端	用来唯一标识	对应于应用注册时返

			标识	应用	回的 appKey
client_secret	必选		应用客户端密钥	用来进行应用鉴权	对应于应用注册时返回的 appSecret
code	必选		授权码	用户授权凭证	
grant_type	必选		授权许可类型	用于标识获取令牌的授权许可类型	Web-server 子态获取令牌流程，该字段为 authorization_code
redirect_uri	必选		授权响应重定向 URI	终端用户的授权步骤完成时授权服务器将要把 user-agent 重定向到的一个绝对 URI	应用注册时，需要预先注册它们的重定向 URI，再授权操作中，redirect_uri 必须和注册时的 URI 域名一致
scope	可选		授权范围	标识用户授予应用访问资源服务器上的资源范围	访问请求的作用域，以空格隔开的字符串列表来表示 暂不使用
state	可选		状态码	维护请求和响应的状态，传入值与返回值保持一致	

2.2 返回值说明

参数名字	参数选项	默认值	参数释义	用途描述	备注
access_token	必选		访问令牌	用于访问资源服务上用户的资源凭证	
token_type	必选		令牌类型	类型目前只支持 Bearer	
refresh_token	可选		刷新令牌	用户访问令牌的刷新或者生成新的访问令牌	
expires_in	必选		访问令牌过期时间	用于访问令牌的时效性控制	单位秒
re_expires_in	可选		刷新令牌过期时间	用于刷新令牌的时效性控制	单位秒
scope	可选		授权范围	标识用户授予应用访问资源服务器上的资源范围	

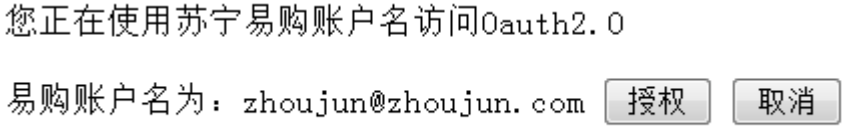
suning_user_name	可选		苏宁用户名	考虑到应用可能需要苏宁用户名和访问令牌进行绑定操作	

2. 应用示例

2.1 应用引导用户登录

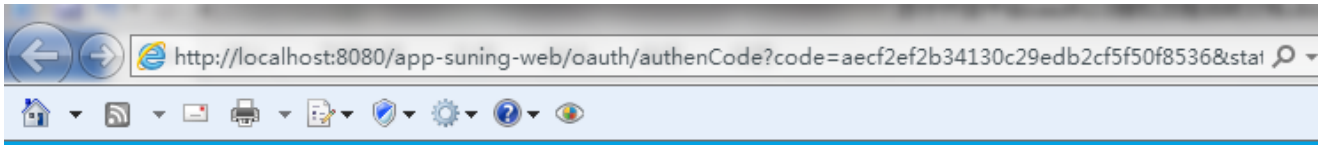
http://open.suning.com/api/oauth/authorize?response_type=code&client_id=d6202c483162e62b0345334868fc7e36&redirect_uri=http://oauth.net/2/&scope=item,price,catagory,order&state=1231414

2.2 请求授权用户授权（用户登录后）



2.3 获取授权码 code

出现授权页面后，用户可以选择"授权" 或 "取消"。
若用户同意授权，页面跳转至应用的回调地址，同时返回授权码 code 以及 state 参数。



用户取消授权，则页面跳转至应用的回调地址，同时返回如下错误信息：
error=access_denied

2.4 获取访问令牌 access_token

用上一步获取的 code 和注册应用时分配的 AppSecret，通过 Http Post 方式换取 Token（访问令牌，即 Sessionkey），苏宁开放服务平台会以 json 文本的形式返回响应的值

对于程序，可以参考如下代码获取 AccessToken

```
String uri = “https://oauth.suning.com/oauth/token”;
OutputStream dos = null;
InputStream dis = null;
URL url = new URL(uri);
HttpsURLConnection connection = (HttpsURLConnection) url
.openConnection();
connection.setRequestMethod("POST");
connection.setDoOutput(true);
connection.setDoInput(true);
connection.setAllowUserInteraction(true);
connection.setRequestProperty("Content-Length",
    String.valueOf(params.getBytes().length));
Set<Entry<String, Object>> entrySet = headers.entrySet();
for (Map.Entry<String, Object> entry : entrySet) {
    String key = (String) entry.getKey();
    Object obj = entry.getValue();
    connection.setRequestProperty(key, (String) obj);
}
dos = connection.getOutputStream();
dos.write(params.getBytes("utf-8"));
dos.flush();
int code = connection.getResponseCode();
dis = connection.getInputStream();
ByteArrayOutputStream out = new ByteArrayOutputStream();
String data2 = new String(out.toByteArray());
```

可以从 http 返回结果中，得到 AccessToken 和 Refresh_token

```
{
    "suning_user_name": "zhoujun@zhoujun.com",
    "scope": "catagory price order item",
    "re_expires_in": "5616000",
    "token_type": "Bearer",
    "expires_in": 1800,
    "refresh_token": "1baf781cab593edea40e73ae781f62a8",
    "access_token": "502b297f0e173aa18e2ffe33bb05cc8f"
}
```

四 Native Application

此流程适合 ISV 没有自己的 web 服务器，且应用为原生程序，即客户端应用（同时应用无法与浏览器交互，但是可以外调用浏览器）。
请求的流程有：
获取授权码:http://open.suning.com/api/oauth/authorize
获取访问令牌：http://open.suning.com/api/oauth/token

1．参数说明

1.1 获取授权码输入参数

参数名字	参数选项	默认值	参数释义	用途描述	备注
client_id	必选		应用客户端标识	用来唯一标识应用	
response_type	必选	code	授权请求响应类型	用来标识授权响应数据是访问令牌还是授权码信息	请求访问令牌时参数值必须设为“token”，请求授权码时参数值必须设为“code”
redirect_uri	必选	urn:ietf:wg:oauth:2.0:oob	授权响应重定向 URI	终端用户的授权步骤完成时授权服务器将要把 user-agent 重定向到的一个绝对 URI	应用注册时，需要预先注册它们的重定向 URI，再授权操作中，redirect_uri 必须和注册时的 URI 域名一致
scope	可选		授权范围	标识用户授予应用访问资源服务器上的资源范围	访问请求的作用域，以逗号隔开的字符串列表来表示
state	可选		状态码	维护请求和响应的状态，传入值与返回值保持一致	

1.2 获取访问令牌参数

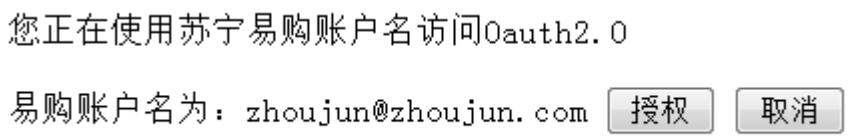
参数名字	参数选项	默认值	参数释义	用途描述	备注
client_id	必选		应用客户端标识	用来唯一标识应用	对应于应用注册时返回的 appKey
client_secret	必选		应用客户端密钥	用来进行应用鉴权	对应于应用注册时返回的 appSecret
code	必选		授权码	用户授权凭证	
grant_type	必选		授权许可类型	用于标识获取令牌的授权许可类型	Web-server 子态获取令牌流程，该字段为 authorization_code
redirect_uri	必选	urn:ietf:wg:oauth:2.0:oob	授权响应重定向 URI	终端用户的授权步骤完成时授权服务器将要把 user-agent 重定向到的一个绝对 URI	应用注册时，需要预先注册它们的重定向 URI，再授权操作中，redirect_uri 必须和注册时的 URI 域名一致
scope	可选		授权范围	标识用户授予应用访问资源服务器上的资源范围	访问请求的作用域，以空格隔开的字符串列表来表示
state	可选		状态码	维护请求和响应的状态，传入值与返回值保持一致	

2. 应用示例

2.1 应用引导用户登录

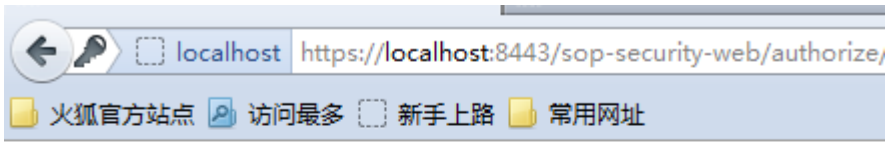
http://open.suning.com/api/oauth/authorize?response_type=code&client_id=d6202c483162e62b0345334868fc7e36&redirect_uri=urn:ietf:wg:oauth:2.0:oob&scope=item,price,catagory,order&state=1231414

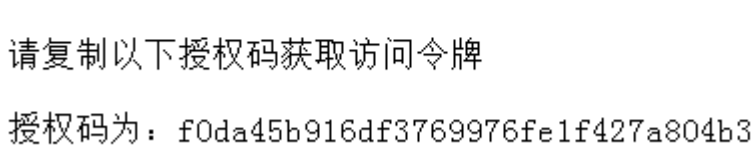
2.2 请求授权用户授权（用户登录后）



2.3 获取授权码

回调到授权默认页面，同时将授权码显示在页面上





2.4 获取访问令牌 access_token

用上一步获取的 code 和注册应用时分配的 AppSecret，通过 Http Post 方式换取 Token（访问令牌，即 Sessionkey），苏宁开放服务平台会以 json 文本的形式返回响应的值

对于程序，可以参考如下代码获取 AccessToken

```
String uri = “https://oauth.suning.com/oauth/token”;
OutputStream dos = null;
InputStream dis = null;
URL url = new URL(uri);
HttpsURLConnection connection = (HttpsURLConnection) url
.openConnection();
connection.setRequestMethod("POST");
connection.setDoOutput(true);
connection.setDoInput(true);
connection.setAllowUserInteraction(true);
connection.setRequestProperty("Content-Length",
    String.valueOf(params.getBytes().length));
Set<Entry<String, Object>> entrySet = headers.entrySet();
for (Map.Entry<String, Object> entry : entrySet) {
    String key = (String) entry.getKey();
    Object obj = entry.getValue();
    connection.setRequestProperty(key, (String) obj);
}
dos = connection.getOutputStream();
dos.write(params.getBytes("utf-8"));
dos.flush();
int code = connection.getResponseCode();
dis = connection.getInputStream();
ByteArrayOutputStream out = new ByteArrayOutputStream();
String data2 = new String(out.toByteArray());
```

可以从 http 返回结果中，得到 AccessToken 和 Refresh_token

```
{
	"suning_user_name": "zhoujun@zhoujun.com",
	"scope": "catagory price order item",
	"re_expires_in": "5616000",
	"token_type": "Bearer",
	"expires_in": 1800,
	"refresh_token": "1baf781cab593edea40e73ae781f62a8",
	"access_token": "502b297f0e173aa18e2ffe33bb05cc8f"
}
```


五 Refreshing an Access Token

1. 参数说明

通过前两种种流程，获取了 Access token 以及 Refresh token（对于具有“获取 Refresh token 权限”的应用）,但是一般来讲，access token 都有一定的有效期，在刷新有效时长内必须通过 Refresh token 来延迟 Access token 的时长。

请求的流程有：

http://open.suning.com/api/oauth/token

通过 http post 请求发送刷新。

参数名字	参数选项	默认值	参数释义	用途描述	备注
client_id	必选		应用客户点标识	用来唯一标识应用	对应于应用注册时返回的 appKey
client_secret	必选		应用客户端密钥	用来进行应用鉴权	对应于应用注册时返回的 appSecret
refresh_token	必选		授权请求响应类型	用来标识授权响应数据是访问令牌还是授权码信息	请求访问令牌时参数值必须设为“token”，请求授权码时参数值必须设为“code”
grant_type	必选		授权许可类型	用于标识获取令牌的授权许可类型	刷新令牌流程，该字段为 refresh_token
scope	可选		授权范围	标识用户授予应用访问资源服务器上的资源范围	访问请求的作用域，以空格隔开的字符串列表来表示
state	可选		状态码	维护请求和响应的状态，传入	

				值与返回值保持一致	

2. 应用示例

http://open.suning.com/api/oauth/token

grant_type=refresh_token&client_id=d6202c483162e62b0345334868fc7e36&client_secret=4bfca4ad2be8b59bd00e144d1945bb43&state=12314&refresh_token=1baf781cab593edea40e73ae781f62a8

返回结果内容示例：

```
{
	"suning_user_name": "zhoujun@zhoujun.com",
	"scope": "catagory price order item",
	"token_type": "Bearer",
	"expires_in": 1800,
	"refresh_token": "1baf781cab593edea40e73ae781f62a8",
	"access_token": "502b297f0e173aa18e2ffe33bb05cc8f"
}
```

access_token 会获取到新的，refresh_token 则不返回，当刷新令牌和访问令牌都过期后需要用户重新授权。

六 测试环境

1.测试环境调用地址

获取授权码:http://apipre.cnsuning.com/api/oauth/authorize
获取访问令牌：http://apipre.cnsuning.com/api/oauth/token