## 1获取用户身份信息

公司会线下给客户提供一组oauth\_consumer\_key和oauth\_consumer\_secret。这是客户访问HDMS服务的凭证

## 2 调用获取token的接口

|  |  |
| --- | --- |
| http method | POST |
| url | <https://hdmap.navinfo.com/auth/v1/oauth2/token> |
| **header** |  |
| Content-Type | application/x-www-form-urlencoded |
| Authorization | OAuth  outh\_consumer\_key=”<user access key>”,  oauth\_nonce=”<random string>”,  oauth\_signature=”<signature>”  oauth\_signature\_method=”HMAC-SHA256”,  oauth\_timestamp=”<timestamp>”,  oauth\_version=”1.0” |
| **Request Parameters** |  |
| grant\_type | client\_credentials (总是为这个值) |
| expires\_in | <token expires in seconds> (该参数非必填) |

注意Authorization header中，OAuth后必须有一个空格。=两边不能有空格，=右边的值的两边需要有引号

Authorization header中的oauth\_signature需要按照oauth1.0的规范对请求的参数进行签名。下面我们来阐述如何生成这个签名

### 2.1 生成参数签名

#### 2.1.1生成源串(base\_string)

源串由三部分内容组成，每部分内容用&拼接

Base\_string = Uppercase(http Method) & urlencode(lowercase(url)) & urlencode(a=x&b=y&…).

从左往右看，第一个部分 http method必须为大写。第二个部分的url是接口的地址，全部是小写然后用urlencode编码。第三个部分是将请求中Authorization header中除oauth\_signature以外的参数和grant\_type请求参数，按照字典升序排列后&拼接。对拼接的结果做一次urlencode后的结果即为源串

#### 2.1.2生成签名

这里使用HMAC-SHA256算法。该算法需要两个参数，分别是base\_string和key。这里的key，这里的key的值oauth\_consumer\_secret后加一个&. 得出的结果，先做base64编码，再做一次urlencode，得到最终的签名。流程如下:

signature = HMAC-SHA256(base\_string, oauth\_consumer\_secret&)

signature = base64(signature)

signature = urlencode(signature)

#### 2.1.3 示例

假设第一步得到的key和secret分别是

Key: 0ae39b9a53460cb1d099027ef4cebfda364617e4c8651111322768215f9e3aaf

Secret: c78e5c8ecfaf06256f99e5c212368ffd7f1ec6b9038ff3c4e0db2728d014d6d3

POST <https://hdmap.navinfo.com/auth/v1/oauth2/token>

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

Authorization: OAuth oauth\_consumer\_key=” 0ae39b9a53460cb1d099027ef4cebfda364617e4c8651111322768215f9e3aaf”,

oauth\_nonce=”8346887”,

oauth\_signature=”<signature>”

oauth\_signature\_method=”HMAC-SHA256”,

oauth\_timestamp=” 1546937524”,

oauth\_version=”1.0”

表单参数:

grant\_type=client\_credentials

根据上面的参数，得到的base\_string 为:

POST&https%3A%2F%2Fhdmap.navinfo.com%2Fauth%2Fv1%2Foauth2%2Ftoken&grant\_type%3Dclient\_credentials%26oauth\_consumer\_key%3D0ae39b9a53460cb1d099027ef4cebfda364617e4c8651111322768215f9e3aaf%26oauth\_nonce%3D8346887%26oauth\_signature\_method%3DHMAC-SHA256%26oauth\_timestamp%3D1546937524%26oauth\_version%3D1.0

计算后的签名为

nvYQaHh6Y3A76sgL9N8PNjj1J5%2B5i243uejb6ve%2BMGw%3D

### 2.2 接口响应

Content-Type: application/json

|  |  |
| --- | --- |
| 参数 | 描述 |
| access\_token | 生成的token，可以用于发送请求 |
| token\_type | 固定值 "bearer" |
| expires\_in | 令牌到期前的秒数，令牌发布后有效期为24小时 |

{

“access\_token”: “VE5URXlJbjAuLmE4S0l4eVpQVE1zbHRwcnQyZ1BSVGcuS3RHT2V”,

“token\_type”: “bearer”,

“expire\_in”:86399

}