认证流程

郑心 <xinzheng1@chinaums.com> – Version 20181023, 郑心, 2018-10-23 | 初始版本

目录

1. 关键字

1. AppId: 产品ID，由银联商务方提供
2. AppKey: 产品密钥，由银联商务方提供

2. 流程说明

开放平台提供两种认证方式，分别如下：

1. OPEN-ACCESS-TOKEN方式

    该认证方式下，接入方需要**预先**进行AccessToken的获取，获取后将AccessToken放入认证报文中，AccessToken获取方式见后续章节。
    认证内容为：

    ```
    OPEN-ACCESS-TOKEN AccessToken="AccessToken"
    ```

    在该模式下，请注意以下几点：

    - 在相同时间，相同**AppId**下，**AccessToken**的最大有效个数为**10**个；
    - AccessToken有效期为1小时；
    - 使用AppId和AppKey来获得AccessToken；
    - 注意：请勿频繁获取**AccessToken**，尤其是不要每次接口调用都先获取**AccessToken**。

2. OPEN-BODY-SIG方式

该认证方式下，接入方须进行报文体内容以及其它参数的签名，并将相关内容放入认证报文中。认证内容为：

```
OPEN-BODY-SIG AppId="AppId", Timestamp="时间戳", Nonce="随机数", Signature="签名"
```

其中，参数格式为：

参数名称	参数说明	参数类型	长度	是否必须	备注
AppId	AppId	字符串	⇐32	是	
Timestamp	时间戳	字符串	14	是	yyyyMMddHHmmss
Nonce	随机数	字符串	⇐128	是	
Signature	签名	字符串		是	Base64_Encode(HmacSHA256(AppId + timestamp + nonce + SHA256(报文体), AppKey))

签名算法：

1. 取报文体，即正文全部内容获得字节数组A，进行SHA256算法取16进制小写字符串获得B，算法公式为B=SHA256_WITH_LOWER_HEXSTR(A)。

   例如：

   ```
   A=[(byte)65]，得
   B="559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd"
   ```

2. 取AppId、Timestamp、Nonce、B进行字符串拼接，以UTF-8进行编码获得待签名串C，取AppKey作为签名密钥D。

   例如：

   ```
   AppId="1234567890123456789012345678901 2"，Timestamp="20170101120000"，
   Nonce="09876543210987654321098765432109"，得
   C="123456789012345678901234567890122017010112000009876543210987654321098765432109
   559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd"，
   D="6789012345678901234567890123456 7"
   ```

3. 以C和D进行HMAC-SHA256算法获得签名字节数组E，算法公式为：
   E=HmacSHA256(signingBytes: C, keyBytes: D)。

   例如：

```
E=
[0x18,0x83,0x6c,0x09,0x3c,0x8d,0x29,0x3a,0x44,0x23,0xd2,0x97,0x3b,0x5e,0x8a,0xa9,
0x92,0x7a,0xe1,0xf3,0xb2,0x03,0x2b,0x44,0x2a,0x5f,0x1a,0x69,0x1f,0xc3,0xcb,0x4f]
```

4. 对E进行Base64编码获得F，F即为签名内容，算法公式为F=Base64_Encode(E)。

   例如：

```
F="GINsCTyNKTpEI9KXO16KqZJ64fOyAytEKl8aaR/Dy08="
```

示例：

```
OPEN-BODY-SIG
AppId="10037ca75e6125aa015e9e12a89b001b",Timestamp="20170606135700",Nonce="99930a14
7f5353dd8a8f29a5329f37e9",Signature="IPmdGHYCcfN+mtoO/02ZkwoUf1NT3YqPKaUyKMaec1I"
```

3. AccessToken获取

3.1. 报文协议

HTTP(S) + JSON

3.2. 接口地址

测试地址：http://58.247.0.18:29015/v1/token/access
生产地址：https://api-mop.chinaums.com/v1/token/access

3.3. 报文格式

1. 请求

   URL参数：无
   POST参数：

格式：**JSON**					
参数名称	参数说明	参数类型	长度	是否必须	备注

appId	产品ID	字符串	⇐32	是	
timestamp	时间戳	字符串	14	是	yyyyMMddHHmmss
nonce	随机数	字符串	⇐128	是	
signMethod	签名方法	字符串		是	SHA256
signature	签名	字符串		是	SHA256_hex(appId+timestamp+nonce+appKey)

2. 响应

格式：**JSON**					
参数名称	参数说明	参数类型	长度	是否必须	备注
errCode	错误代码	字符串	4	是	0000为成功
errInfo	错误说明	字符串		是	
accessToken	授权令牌	字符串	32	是	
expiresIn	失效时间	数字型		是	单位为秒

3.4. 建议

为了保密appKey，建议需要一个accessToken获取和刷新的中控服务器，而其他业务逻辑所使用的accessToken均来自于该中控服务器。