速递易开放平台认证规范

姜润 `<jiangrun@sudiyi.net>`

曾浩 `<zenghao@isantai.cn>`

Table of Contents

1.#规范

速递易开放平台 API 采用标准的 HTTP Authorization 头域进行认证，该认证信息看起来具有如下形式：

Authorization: SDY SDYPartnerId:Signature

速递易会为每一位注册的开放平台合作伙伴发放唯一的标识符（SDYParnterId）和对应的密钥（SDYPartnerSecret）。合作伙伴需要用它们来对所有的 API 请求进行处理，以通过速递易平台的访问认证。

下面是计算以及拼装 Authorization 头域的伪代码：

Authorization = "SDY" + " " + SDYPartnerId + ":" + Signature;

Signature = Base64(HMAC-SHA1(SDYPartnerSecret, UTF-8-Encoding-Of(InfoToSign)));

其中，InfoToSign 是待签名的内容，采用如下方式拼装

InfoToSign = HTTP-Method + "\n"
Content-MD5 + "\n"
Content-Type + "\n"

Date + "\n"
HTTP-Request-Path;

注意：Content-Type中的charset必须使用大写，即 Content-Type:application/json; charset=UTF-8

字段名	说明	示例
HTTP-Method	请求的 HTTP 方法	GET / POST / PUT / DELETE
Content-MD5	请参考 [RFC-1864] (https://tools.ietf.org/html/rfc1864)	Base64(MD5(request-content))
Content-Type	请求的内容类型	application/json;charset=UTF-8
Date	请求的日期和时间	Fri, 18 Apr 2014 19:36:42 +0800
HTTP-Request-Path	请求的路径	/v3/devices/1001681

2. #示例

POST /v3/devices/1001681/resv_orders Content-Type: application/json;charset=UTF-8 Content-MD5: NmRkMTljYzI3MmU4Y2QxNg== Date: Fri, 18 Apr 2014 19:36:42 +0800 … …

{ "sender_mobile": "13882290198", "box_type": "grande", "auto_upgd" : true, "send_name": "张三", "consignee_mobile": "13518116720", "consignee_name":"李四", "notify_url": "http://foobar.com/notifyme?id=a1b2c3d4e5f6" }

InfoToSign 的拼接过程

InfoToSign = "POST" + "\n"
"NmRkMTljYzI3MmU4Y2QxNg==" + "\n"
"application/json;charset=UTF-8" + "\n"
"Fri, 18 Apr 2014 19:36:42 +0800" + "\n"
"/v3/devices/1001681/resv_orders";

3. #相关错误说明

HTTP 错误码	说明
412	未包含加密所需的头
401	请求未包含 Authorization 头域，认证无法进行

403	签名错误，或者没有访问系统的权限
420	超过API的访问频率限制
421	超过可以预约的箱格数量限制

4. #语言示例

下面使用多种语言来作一个说明，所有说明都以 `/v1/boxStatus` 为例。

4. 1. #Java

`Auth. java`

```java
import org.apache.http.client.methods.CloseableHttpResponse;
import org.apache.http.client.methods.HttpGet;
import org.apache.http.client.utils.URIBuilder;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.nio.charset.Charset;
import java.util.Base64;

public class Auth {
    protected static int ID = 0;               // 用户ID
    protected static final String SECRET = "";  // 分配的秘钥

    protected static final String HEADER_MD5
 = "ZDQxZDhjZDk4ZjAwYjIwNGU5ODAwOTk4ZWNmMODQyN2U=";
    protected static final String HEADER_CONTENT_TYPE = "application/json;
charset=UTF-8";
    protected static final String HEADER_DATE = "Thu, 07 Jul 2016 15:28:50 GMT";

    public static void main(String... args) throws Exception {
        try (CloseableHttpClient client = HttpClients.createDefault()) {    ❶
            URIBuilder builder = new URIBuilder("http://open.sudiyi.cn/v1/boxStatus");
            builder.addParameter("device", "1000018");
            HttpGet get = new HttpGet(builder.build());
```

```java
            StringBuilder infoToSignBuilder = new StringBuilder(200);
            infoToSignBuilder.append("GET").append("\n");
            infoToSignBuilder.append(HEADER_MD5).append("\n");
            infoToSignBuilder.append(HEADER_CONTENT_TYPE).append("\n");
            infoToSignBuilder.append(HEADER_DATE).append("\n");
            infoToSignBuilder.append("/v1/boxStatus");

            SecretKeySpec signingKey = new
    SecretKeySpec(SECRET.getBytes(Charset.forName("utf-8")), "HmacSHA1");
            Mac mac = Mac.getInstance("HmacSHA1");
            mac.init(signingKey);
            byte[] rowHmac = mac.doFinal(infoToSignBuilder.toString().getBytes("utf-8"));
            String signature = Base64.getEncoder().encodeToString(rowHmac);

            get.addHeader("Content-MD5", HEADER_MD5);
            get.addHeader("Content-Type", HEADER_CONTENT_TYPE);
            get.addHeader("Date", HEADER_DATE);
            get.addHeader("Authorization", "SDY " + ID + ":" + signature);

            try (CloseableHttpResponse resp = client.execute(get)) {
                BufferedReader reader = new BufferedReader(new
    InputStreamReader(resp.getEntity().getContent()));
                System.out.println("content is :");
                String line = reader.readLine();
                while (line != null) {
                    System.out.println(line);
                    line = reader.readLine();
                }
            }
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
}
```

❶ 使用Apache HttpClient作为网络客户端

4.2. #C#

```csharp
using System;
using System.Text;
using RestSharp;
using System.Security.Cryptography;


namespace SudiyiOpen
```

```
{
    public class Auth
    {
        private const int _thirdpartyId = 0;   // 用户ID
        private const string _encrypt = "";     // 分配的秘钥

        private const String HEADER_MD5 = "ZDQxZDhjZDk4ZjAwYjIwNGU5ODAwOTk4ZWNmODQyN2U=";
        private const String HEADER_CONTENT_TYPE = "application/json; charset=UTF-8";

        public static void Main(String[] args)
        {
            RestClient client = new RestClient("http://open.sudiyi.cn");        ❶
            RestRequest request = new RestRequest("/v1/boxStatus", Method.GET);
            request.AddParameter("device", "1000018");
            request.AddHeader("Content-MD5", HEADER_MD5);
            request.AddHeader("Content-Type", HEADER_CONTENT_TYPE);
            string date = DateTime.Now.ToString("r");        ❷
            request.AddHeader("Date", date);


            StringBuilder sb = new StringBuilder(200);
            sb.Append(Method.GET.ToString()).Append("\n");
            sb.Append(HEADER_MD5).Append("\n");
            sb.Append(HEADER_CONTENT_TYPE).Append("\n");
            sb.Append(date).Append("\n");
            sb.Append("/v1/boxStatus");

            Encoding encoding = Encoding.UTF8;

            byte[] byteKey = encoding.GetBytes(_encrypt);
            HMACSHA1 hmac = new HMACSHA1();
            hmac.Key = byteKey;
            byte[] Signature_HMACSHA =
 hmac.ComputeHash(encoding.GetBytes(sb.ToString()));
            string auth = Convert.ToBase64String(Signature_HMACSHA);

            request.AddHeader("Authorization", "SDY " + _thirdpartyId + ":" + auth);

            IRestResponse resp = client.Execute(request);
            Console.Write(resp.Content);
            Console.ReadKey();
        }
    }
}
```

❶   使用 RestSharp 作为网络客户端

❷ 必须使用 `ToString("r")`，其它格式的日期字符串会被.Net底层重写

4. 3. #python

auth.py

```python
from requests import get    ❶
import hmac
import hashlib
import base64

thirdparty_id = 0    # your id
thirdparty_secret =  '' #  your secret

def gen_authorization(headers, method, path, secret):
    tosign = method + '\n'
    tosign = tosign + headers['Content-MD5'] + '\n'
    tosign = tosign + headers['Content-Type'] + '\n'
    tosign = tosign + headers['Date'] + '\n'
    tosign = tosign + path
    tosign = tosign.encode('utf-8')

    hash1 = hmac.new(secret, tosign, hashlib.sha1).digest()
    ret = base64.encodestring(hash1)
    if ret[-1] == "\n":
        return ret[:-1]
    else:
        return ret


headers = {
    'Content-Type': 'application/json;charset=UTF-8',
    'Content-MD5': 'ZDQxZDhjZDk4ZjAwYjIwNGU5ODAwOTk4ZWNmODQyN2U=',
    'Date': 'Thu, 07 Jul 2016 15:28:50 GMT',
    'Accept': 'application/json'
}

headers['Authorization'] = "SDY " + str(thirdparty_id) + ':' + \
                        gen_authorization(headers, 'GET', '/v1/boxStatus',
 thirdparty_secret)

print('GET /v1/boxStatus/ ...')
resp = get('http://open.sudiyi.cn/v1/boxStatus', params={"device": 1000018},
 headers=headers)
print('response status code: %d' % resp.status_code)
```

```
print('response content: ' + resp.content)
```

❶ 使用 requests 来发送http请求

4. 4. #php

auth. php

```php
<?php

$partner_id = 0;
$partner_key = '';
$now = date('D,d M Y H:i:s',time()).' GMT';
$n = "\n";
$content_type = 'application/json;charset=UTF-8';
$content_md5 = base64_encode(md5(''));
$info2sign = 'GET' . $n . $content_md5 . $n . $content_type . $n . $now . $n . '/v1/
boxStatus';
$authorization = "SDY ".$partner_id.":".base64_encode(hash_hmac("sha1", $info2sign,
 $partner_key, true));

$header = array(
    'Content-Type:' . $content_type,
    'Date:'.$now,
    'Content-MD5:' . $content_md5,
    'Authorization:' . $authorization,
);

$ch = curl_init();
curl_setopt($ch, CURLOPT_TIMEOUT, 5);
curl_setopt($ch, CURLOPT_HTTPHEADER, $header);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 0);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_URL, 'http://open.sudiyi.cn/v1/boxStatus?device=1000018');
curl_setopt($ch, CURLOPT_HTTPGET, 1);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);
$response = curl_exec($ch);

if ($response) {
    curl_close($ch);
    var_dump($response);
} else {
    $info = curl_getinfo($ch);
    curl_close($ch);
```

```
    }
```