接入说明

http请求如何通过易百小E系统完成对接。本文档主要面向的读者为各有需求接入易百小E的，有一定开发能力的技术人员。

配置密钥

对接方对接时，需跟业务同事沟通后把公钥发送到指定邮箱。易百小E系统会分配app_id, version, 易百小E系统公钥等信息

开发者调用接口前需自行生成RSA密钥, RSA密钥包含:

- 应用私钥(APP_PRIVATE_KEY)
- 应用公钥(APP_PUBLIC_KEY)

RSA私钥与公钥生成方法

1.运行 openssl

```
CMD> openssl
```

2.生成明文RSA私钥

```
OpenSSL> genrsa -out rsa_private_key.pem 2048
```

- [rsa_private_key.pem] [2048] 为密钥长度
- 默认情况下, openssl 输出的密钥格式为 PKCS#1-PEM

3.生成明文RSA公钥

```
OpenSSL> rsa -in rsa_private_key.pem -pubout -out rsa_public_key.pem
```

- [rsa_private_key.pem] [rsa_public_key.pem] 为公钥保存的文件名

4.如果是Java语言，私钥需要转成PKCS8格式

```
OpenSSL> pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -out rsa_private_key.pkcs8 -nocrypt
```

- [rsa_private_key.pem] [rsa_private_key.pkcs8] 为私钥PKCS8格式保存的文件名

第三步：搭建和配置开发环境

1.调用方法

内容	说明
通讯方式	采用 HTTPS 方式访问
提交方法	POST (application/json)
交互数据格式	JSON
字符编码	UTF-8
签名算法	SHA256WithRSA
签名验证	提交和返回数据都需要验证签名

2.报文结构

请求报文和返回报文都采用如下的报文结构

序号	参数	类型	参考数据	参数说明	备注
1	action	String	queryPmsProjectProduct	对接方法	具体接口有详细说明
2	app_id	String	2014072300007148	应用ID	开放平台分配给开发者的应用ID
3	biz_content	String	BASE64	报文内容BASE64	具体接口中有详细说明，本域需要采用BA
4	timestamp	String	1483372334	Unix时间戳	单位：秒
5	version	String	20171212	版本号	用于兼容不同的报文协议对应后台不同的处
6	sign	String	7E65B60DCFA42B04	数据签名	详见：签名算法

注意事项

- 其中biz_content字段是对请求参数或返回参数进行BASE64编码后得到的，例如：

JSON

```
{
  "xiaoeActivityProductId": "XZXMCG2024005377"
}
```

- BASE64编码后得到：

ewogICAgICAgICAidHJhY2VObyI6ICI5OTAwMDAwOTEwMDAxMDEwMTczMjEyMyIsCiAgICAgICAgICJvcmlnaW5hbFRyYWNlTm8iOiAiOTkwMDAwMDkxMDAwMTAxMDE3MzIxMjQiCiAgICAgfQ==

- 赋值给biz_content字段。
- 如果请求报文无法解析，或传过来的app_id无效，则异常提示返回的报文中sign字段为空。

报文举例

JSON


```
{
    "action" : "queryPmsProjectProduct",
    "app_id" : "2014072300007148",
    "biz_content" :
"ewogICAgICAgICAidHJhY2VObyI6ICI5OTAwMDAwOTEwMDAxMDEwMTczMjEyMyIsCiAgICAgICAgICJvcmlnaW5hbFRrYWNlTm8iOiAiOTkwMDAwMDkxMDAwMTAxMDE3MzIxMjQiCiAgICAgfQ==",
    "timestamp" : "1483372334",
    "version" : "20171212",
    "sign" : "7E65B60DCFA42B04"
 }
```


3.签名算法

a.筛选并排序

获取所有请求参数，不包括字节类型参数，如文件、字节流，剔除sign字段，剔除值为空的参数，并按照第一个字符的键值ASCII码递增排序（字母升序排序），如果遇到相同字符则按照第二个字符的键值ASCII[

- 注意: biz_content字段需要先Base64编码，再进行拼接

b.拼接

将排序后的参数与其对应值，组合成“参数=参数值”的格式，并且把这些参数用&字符连接起来，此时生成的字符串为待签名字符串。

c.签名值计算

使用各自语言对应的SHA256WithRSA签名函数利用应用私钥（APP_PRIVATE_KEY）对待签名字符串进行签名，并进行Base64编码。

示例报文

```
{
    "action" : "queryPmsProjectProduct",
    "app_id" : "102410000",
    "biz_content" :
"ewogICAgICAgICAidHJhY2VObyI6ICI5OTAwMDAwOTEwMDAxMDEwMTczMjEyMyIsCiAgICAgICAgICJvcmlnaW5hbFRyYWNlTm8iOiAiOTkwMDAwMDkxMDAwMTAxMDE3MzIxMjQiCiAgICAgfQ==",
    "timestamp" : "1483372334",
    "version" : "20171212",
    "sign" : "7E65B60DCFA42B04"
}
```

□□□□APP_PRIVATE_KEY□

```
-----BEGIN RSA PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCdR0+PdnzkvvaNbSEp5Q8RpaelnrHu4msHAPiw1/
DJXFPucoEPqPmDAq4IoaW02/mbvHQGr8d/g/g+cbCqUVctl8ygigTvlOAsoWJWrd76gk9lK+SsQBx3BN1pMbPADAljtF
S3oJw10MjCg/wIgmwWaqdCRB1QGwJzw3HnripbHr59BKMv/VYPvgDJx+ohQrfLd9fysbJRcsQKqCs72jxD8U9KHO87u
pvpZtJT2QYdVrntsWL1UUxfyEIKmZy2Lf3UZvqKC4sahgH6pQhCMIhwBWm06FyktRji1ewNfF6zIpkCla/HvJzfqXaqhou
XJm2qgRjJ/crfTjONdd/9iuNlAgMBAAECggEAS4GbwY0p4ouHRFha7okIVfmIZautUrkilscxnXzeHV2U8cnJCiKePvY/ZOd
t7UkaKVks/rTO+vn5aMkd/nZ0evAAjiYUvoxjnymPU3u/q9Z5lWGgM83HnKAaR9FTsWRV8ab2cP3LYM6uQywoCFHM
4GotiFO5GucMo1T2Tzq/HOUAjMzQASQ0ywaANZvNoZDw6ScMPUgGnYnHWbs34l7F2abyKyDiNo7sPtMtRpFYi+go+
S7dygMX0G1IFoCIr4X2HNu/4e3XIFvJjzoUhCF/byDcM992LvcWVgM3Ke/F1oBm+bCFit67hN6mxoi2SEARdQGnBysv
Vo1FLPHKZ60FVQKBgQDidFk8hq8YKEvcjqPSJSd8Oo30zeyWf0R/QNLQOAIqYKCJAcAiHDcYMx5clQQxjFTYXriY+B1J3
he6w3+5NStZqL1o1lcy5w7dhcVFXT1yn2KwUiO6YSJ25KeJHvXtDH66WGIQJMmbg90J2u4HRJxYNODmeVdS1seK5q
aL0uxs6wKBgQCxzHbdbkoiJgFd/c7BdTKnZh2h6x7SsX44IcbTqKsx7zA61ogoegHaKB4yq3xaR8Gm9uazo5SCtbjS0b
O5iQLrv8oLUDaNm5Ckm2ENk/M+TB0Hq24eFytiwUAS6FmdCncjq4xb2x8mqOQQiGvlyD91Na4HRBwxP16Wqwhz3
Nac7wKBgAY1lIDRXJm3+SSKELnhZOzGGkBdKSCTSsiGeYFWF9Ebpys6jg8hYO1b8XguadgF9gmcx0kCfKMa4OGxHJ
5yc8bYlqD6R5fQuBqg4WDehqHO9wDIr8wbf7ts158t5yZh0lO/uqigqZqHCheMFjzCx9qvUH9hUmCmHQCVBHoPBYa
TAoGBAJcixAPURaYjglQAdOlUE3vivNuvvqLBCBb090tifCvVM71AMbuegsaMBadyyCECECY6iL85FPvLN1HVuh3DzrzR
ahEV3VmgXGLgRa7CDintj1u+qLthXJr0xN+NrOdmRwIGSCio6iD1vfAj1vwbrX2X5Nf+WKywPlp7BpNerPv3AoGALv4i
JpOJVAW3Pmuvmc1a3cAsAvv0DGjiGOXn+IyBdX9tJtKppVPEwElibNAltvvgWX++5ctYD2SXNQLV56rkZCmauXP2gT
PG3tCutH4jNiNIBUCfDXlt9DDyQAe0KfRFemzIa5rTWA7wRNsVTCm3n4ZqPlKfMC4HmOGU2hgN3LY=
-----END RSA PRIVATE KEY-----
```

□□□□□

String
List

action=queryPmsProjectProduct&app_id=2014072300007148&biz_content=ewogICAgICAgICAidHJhY2VObyI6ICI5OTAwMDAwOTEwMDAxMDEwMTczMjEyMyIsCiAgICAgICAgICJvcmlnaW5hbFRyYWNlTm8iOiAiOTkwMDAwMDkxMDAwMTAxMDE3MzIxMjQiCiAgICAgICAgfQ==&timestamp=1483372334&version=20171212

□□□□

gUTdEB0lAS/ECkP98weSHf6k31Fmd4hcw0zPG8ewbMTfDFSubKlel/1C16upb2AHzN873HMwUlkcTg7ZuN92KDlkfsblNd2IwVY2tWMvKt5O8gqC2a8XbS25ZObUlLK5zZmU7mQ/DLbyY+EAhkYdGnwskloJkydi2zmLv99xT5G01yXBLSNiTrPBTsc2OhBkA44kknnok0x+hS4HfcgQwGPMG4y+V5aT1bhPDypwdbfAg+EN/5XoSECsIcsvBirdk+BGPjBIuwHHF+Hir/3E3i20ImtlowBc6jwh5qFOVqGN/w2UEPfg6xJxHyW04FBipt6mw7huD4PA4pA4qZRnsg==

Revision #2
Created 17 June 2024 13:55:39 by zhangshuai
Updated 17 June 2024 14:22:56 by zhangshuai