# 测试接口

## 用户激活接口

### 请求

|  |  |
| --- | --- |
| **请求地址** | http(s)://{ip}:{port}/sso/v1/user/active |
| **请求方式** | POST |
| **请求头** | 安全验证：   |  |  |  | | --- | --- | --- | | **参数** | **参数说明** | **是否必选** | | once | 随机数(32位,可用UUID表示) | 必选 | | ts | 时间戳(13位) | 必选 | | appKey | 应用标识，由接口提供方提供 | 必选 | | signMethod | 签名方法(SHA-256算法) | 必选 | | signData | 签名结果 | 必选 |   其它：   |  |  | | --- | --- | | **参数** | **参数值** | | Content-Type | application/x-www-form-urlencoded;charset=UTF-8 | |
| **请求体** | mobile:15302132138123  password:12312312  isEncrypt:false |
| **参数说明** | mobile:手机号(唯一标识)  password:用户密码  isEncrypt:密码是否加密（可选，默认为false） |
| **备注** | 无 |

### 响应

|  |  |
| --- | --- |
| **响应行** | HTTP 200 OK |
| **响应头** | Content-Type:application/json;charset=UTF-8 |
| **响应体** | {     **"code"**:**200**,     **"message"**:**"成功"**,     **"data"**:**null** } |
| **备注** |  |

# 附录

## 接口安全校验签名规则

针对没有数字证书和签名服务器的现场环境，身份管理服务提供算法代码签名。身份管理服务会对每一个访问的请求进行身份验证，都需要请求中包含签名（signData）。服务器通过appKey、pwd验证的方法来验证请求的发送者身份，appKey、pwd由身份管理服务方发送给第三方对接应用，其中appKey用于标识访问者的身份；pwd是用于加密签名字符串和服务器端验证签名字符密钥，必须严格保密，只有统一授权方与对接应用知道。

### 签名步骤说明

* **1.header中参数键值对：**

once=aa03a5c692cf480b87887e0ff8cfe566

ts=1548414452442

appKey=320000000001

signMethod=SHA-256

* **2.对header中的所有参数进行ASCII排序，排序结果如下：**

appKey=320000000001

once=aa03a5c692cf480b87887e0ff8cfe566

signMethod=SHA-256

ts=1548414452442

* **3.利用密钥（pwd由身份管理服务统一签发）进行签名**

比如密钥为：abcdefg

**则需要签名的原文为：**

abcdefg:appKey=320000000001&once=aa03a5c692cf480b87887e0ff8cfe566&signMethod=S HA-256&ts=1548414452442:abcdefg

**签名算法采用SHA-256,则生成最终的签名结果为：**

b04ace6a85912e01d92d5ebd80e41bee0762d6121738d0c25fa4f43ecb8c2697

* **4.最终完成参数为：**

**header中参数键值对：**

once=aa03a5c692cf480b87887e0ff8cfe566

ts=1548414452442

appKey=320000000001

signMethod=SHA-256

signData=b04ace6a85912e01d92d5ebd80e41bee0762d6121738d0c25fa4f43ecb8c2697

### 签名实现示例



说明:调用HashUtil.getSignResult方法获取签名结果