|  |
| --- |
|  |

|  |
| --- |
|  |
| 接口说明-集成认证 |
| 版本 V1.0 |

**会签**

陕西 西安

2021．02

|  |  |  |  |
| --- | --- | --- | --- |
| 作者 | ZhengWei(HY) | 日期 | 2021-02-02 |
| 审核 |  | 日期 |  |
| 批准 |  | 日期 |  |

**版本**

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 日期 | 更新 | 签字 |
| 1.0 | 2021-02-02 | 创建 | ZhengWei(HY) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[1. 接口格式 5](#_Toc63161200)

[1.1 创建应用生成密钥对 5](#_Toc63161201)

[1.2 获取访问Token 6](#_Toc63161202)

# 接口格式

所有的 API 都是基于 HTTP 1.1 [RFC2616]， 采用 REST 风格定义。每一个请求都包含  
HTTP 的 POST、 GET 等请求方法，对应于请求的每一个响应都含有标准的 HTTP 状态  
码(status code)。大部分请求响应还包含了 JSON 格式的消息正文。

### 1.1 生成应用密钥对

此接口对于一个应用只调用一次就好，须将返回信息汇总管理员，并添加到ms.xsso.appKey.Config.xml配置文件中才能生效（请重启服务）。

#### 1.1.1 接口请求参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **名称** | 创建应用生成密钥对 | | | | |
| **说明** | 创建应用生成密钥对 | | | | |
| **地址** | <http://127.0.0.1:80/>服务名称/xsso/createApp | | | | |
| **方式** | Get请求 | | | | |
| **接口请求参数** | | | | | |
| **序号** | **参数名称** | **参数说明** | **参数类型** | **是否必须** | **备注** |
| 01 | 无 | 无 | 无 | 无 |  |

#### 1.1.2 接口响应参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **接口返回参数** | | | | | |
| **序号** | **参数名称** | **参数说明** | **参数类型** | **是否必须** | **备注** |
| 01 | appKey | 应用编码 | String | 是 | 注册应用方妥善保存 |
| 02 | privateKey | 私钥加密验证 | String | 是 | 注册应用方妥善保存 |
| 03 | publicKey | 公钥加密验证 | String | 否 | 本服务妥善保存在：ms.xsso.appKey.Config.xml配置文件中。 |

#### 1.1.3 接口举例-请求报文

无

#### 1.1.4 接口举例-响应报文

{

    "code": "200",

    "message": "成功",

    "data": {

        "data": {

            "appKey": "70A78B5680FD4C7C9A9D9522F41F5E5E",

            "privateKey": "",

            "publicKey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD0ry8BiVBTOg7APlYAwlmYpiqQAOYkje2BpDbtebfUow2LWxX1Gv8kSKO/u0A7CgD2NnI3JyKITUy2m+o/vXJ6qQ7aP1geOPz2FQV9uNvIFUcf1dCO1axASEMeJgWLhOhDikeymCevf7sv/2PMzd80xvFFnpQdv9xTmX4wdSu1sQIDAQAB"

        }

    }

}

### 1.2 获取访问Token

应用创建成功后，会生成应用的 appKey 和 appSecret 的值，租户管理员可将这个两个值交给开发者，开发者可用 appKey 和 appSecret 获取 token 进行接口的调用。

#### 1.2.1 接口请求参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **名称** | 获取访问Token | | | | |
| **说明** | 调用接口令牌 access\_token 是应用调用开放平台业务接口的凭证，有效期为2小时,过期后需要重新获取。 | | | | |
| **地址** | <http://127.0.0.1:80/>服务名称/xsso/createApp | | | | |
| **方式** | Get请求 | | | | |
| **接口请求参数** | | | | | |
| **序号** | **参数名称** | **参数说明** | **参数类型** | **是否必须** | **备注** |
| 01 | appKey | 应用 appKey | String | 是 |  |
| 02 | timestamp | 毫秒时间戳 | Long | 是 |  |
| 03 | signature | 校验签名 | String | 是 |  |

**signature校验签名的生成方式**

其中，签名字段signature计算使用RAS算法，具体计算方式如下：

URLEncode( Base64EnCode( RAS( parameters) ) )

其中，parameters 按照参数名称排序，参数名称与参数值依次拼接(signature字段除外)，形成待计算签名的字符串。

示例 ：若发送请求参数appKey为0904202FB2EA4AC3A899B423928A0F8E,时间戳timestamp为1609221942639，则待加密字符串的值为 appKey0904202FB2EA4AC3A899B423928A0F8E timestamp1609221942639

之后对 parameters使用 RAS 计算签名，RAS 的 key 为自建应用的 appSecret 。计算出的二进制签名先进行 Base64，之后进行 URLEncode，即得到 signatrue 字段的值。

#### 1.2.2 接口响应参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **接口返回参数** | | | | | |
| **序号** | **参数名称** | **参数说明** | **参数类型** | **是否必须** | **备注** |
| 01 | code | 是否成功标识 | String | 是 | 200为成功 |
| 02 | message | 消息说明 | String | 是 |  |
| 03 | access\_token | 访问令牌 | String | 否 | 成功时，返回 |
| 04 | expire | 过期时长 | String | 否 | 成功时，返回。  单位：秒  默认为：7200 |

#### 1.2.3 接口举例-请求报文

<http://127.0.0.1/>msXSSO/**getAccessToken**?**appKey**=0904202FB2EA4AC3A899B423928A0F8E&**timestamp**=1609221942639&**signature**=fPAHpZghqNLpssMr%2FeMlbTizQSpCX91hRMRKdrKs0djDCyH4Hb0ozv7yfFSgjGBTGLhd6K%2FAqxE3UQQMmk33OCiuHztNbyRaxSGgrQ75HIVmvriQFYtPTUGOtYR4vmKzGOcxghv4s%2FTdWsGGRWwcK8y%2Bg9ZULRHVUtu8EMErud4%3D

#### 1.2.4 接口举例-响应报文

{

    "code": "200",

    "message": "成功",

    "data": {

        "data": {

            "accessToken": "E4BB5E15665E4ABC8FC3376D13447730",

            "expire": 7200

        }

    }

}