1. **接入单点登录准备工作**
2. 联系单点登录开发者（罗延文），提供网站部署的地址，以获取分配到的apikey和secret
3. 保存key和secret到site项目中，以供下面登录流程使用
4. 基本变量

API\_KEY = "咨询SSOServer开发者获得"

API\_SECRET = "咨询SSOServer开发者获得"

SSO\_SERVER = "http://106.12.27.16:9000/ " *现提供开发地址，以后会换成实际地址*

AUTH\_TOKEN\_URL = SSO\_SERVER + "/sso/authtoken"

SSO\_LOGIN\_URL = SSO\_SERVER + "/sso/login"

SSO\_LOGOUT\_URL = SSO\_SERVER + "/sso/logout"

SSO\_SIGNUP\_URL = SSO\_SERVER + "/sso/signup"

SSO\_CHANGE\_PWD\_URL = SSO\_SERVER + "/sso/changepwd"

1. **接口说明**

**【按调用顺序】**

1. **显示登录页面（site to SSOServer）**

*接口说明：*

在site中使用表单方式，携带apikey等信息提交到SSO的登录页面

*接口地址：*

SSO\_LOGIN\_URL

*请求方式：*

POST

*请求参数：*

apikey API\_KEY

callback 登录成功后回调地址（通常为site自己的主页）

*返回值：*

*无*

*示例：*

<http://106.12.27.16:9000/sso/login/> （表单参数apikey= 0e920c6d ；callback= <http://xxx.xx.com/home/>）

1. **SSOServer登录成功后跳转至site（SSOServer to site）**

*接口说明：*

在SSOServer中验证登录成功后，使用表单方式，携带authtoken跳转到site的callback页面

*接口地址：*

1中的callback参数 【注】这里意味着在各site需要有相应的callback实际值对应的处理页面

*请求方式：*

POST

*请求参数：*

auth\_token SSOServer授权当前登录用户的令牌，需site保存（建议存到session或cache）

*返回值：*

*无*

*示例：*

1. **验证auth\_token有效性，并获取用户信息（site to SSOServer）**

*接口说明：*

在site中使用2中ssoserver分配的auth\_token获取用户信息（目前只提供用户名）；如果auth\_token过期（20分钟）或者错误，则无法获得用户信息

*接口地址：*

AUTH\_TOKEN\_URL

*请求方式：*

GET

*请求参数：*

auth\_token 第2接口中由ssoserver分配的令牌

timestamp 1970以来到现在的秒数，UNIX time

apikey API\_KEY

signature &signature之前的内容（/sso/authtoken/?auth\_token=xx& timestamp=23230434& apikey=sdfsdfsdg）使用API\_SECRET进行hmacsha256加密，然后把结果转成base64

*返回值：*

*{"username":”luoyanwen”} 成功*

*{“error”:”token invalid”} 失败*

*示例：*

http://106.12.27.16:9000/sso/authtoken/? timestamp=1508121931.94&auth\_token=afea15354aefe633da7770457876d1cc4c169ffca1e0552d3f07e524b6317819&apikey=0e920c6d&signature=gWmiXCzlG5kpA2FSIeAD4uah7xr8xR3QUL+1pPnedvA=

1. **登出（site to SSOServer）**

*接口说明：*

在site中登出

*接口地址：*

SSO\_LOGOUT\_URL

*请求方式：*

GET

*请求参数：*

auth\_token 第2接口中由ssoserver分配的令牌

client\_ip site中当前请求登出的用户的ip地址

timestamp 1970以来到现在的秒数，UNIX time

signature &signature之前的内容（/sso/logout? auth\_token=xx& timestamp=23230434）使用API\_SECRET进行hmacsha256加密，然后把结果转成base64

*返回值：*

*{" error":”” } 成功*

*{“error”:”token invalid”} 失败*

*示例：*

http://106.12.27.16:9000/sso/logout/? timestamp=1508121931.94&auth\_token=afea15354aefe633da7770457876d1cc4c169ffca1e0552d3f07e524b6317819&signature=gWmiXCzlG5kpA2FSIeAD4uah7xr8xR3QUL+1pPnedvA=

1. **另一个site登出成功后，由SSOServer向其他site群发logout请求（SSOServer to sites）**

*接口说明：*

其中一个已登录site中登出成功后，SSOServer会向所有已经登录的各个site发起登出回调请求，携带authtoken发送到各个site的logoutcallback接口

*接口地址：*

各个site的/sso/logoutcallback【注】这里意味着在各site需要有相应的callback实际值对应的处理接口

*请求方式：*

GET

*请求参数：*

auth\_token SSOServer授权当前登录用户的令牌

*返回值：*

*示例：*

1. **显示注册页面（site to SSOServer）**

*接口说明：*

在site中使用表单方式，携带apikey等信息提交到SSO的注册页面

*接口地址：*

SSO\_SIGNUP\_URL

*请求方式：*

POST

*请求参数：*

apikey API\_KEY

callback 注册成功后回调地址（通常为site自己完善用户信息的界面，或者不需要完善的话就进入登录界面）

*返回值：*

*无*

*示例：*

1. **SSOServer注册成功后跳转至site（SSOServer to site）**

*接口说明：*

在SSOServer中验证注册成功后，使用表单方式，携带authtoken跳转到site的callback页面

*接口地址：*

1中的callback参数 【注】这里意味着在各site需要有相应的callback实际值对应的处理页面

*请求方式：*

POST

*请求参数：*

auth\_token SSOServer授权当前注册用户的令牌，需site保存（建议存到session或cache）

*返回值：*

*无*

*示例：*

1. **显示修改密码页面（site to SSOServer）**

*接口说明：*

在site中使用表单方式，携带apikey等信息提交到SSO的注册页面

*接口地址：*

SSO\_CHANGE\_PWD\_URL

*请求方式：*

POST

*请求参数：*

apikey API\_KEY

callback 修改成功后回调地址

*返回值：*

*无*

*示例：*

1. **SSOServer修改密码成功后跳转至site（SSOServer to site）**

*接口说明：*

在SSOServer中验证修改密码成功后，使用表单方式，携带authtoken跳转到site的callback页面

*接口地址：*

1中的callback参数 【注】这里意味着在各site需要有相应的callback实际值对应的处理页面

*请求方式：*

POST

*请求参数：*

auth\_token SSOServer授权当前用户的令牌，需site保存（建议存到session或cache）

*返回值：*

*无*

*示例：*