**业务系统集成统一认证平台说明-CS**

# 1. 系统要求

业务系统为CS结构，即分客户端和服务端，客户端和服务端的认证授权基于Token进行，服务端采用dubbox框架开发。

# 2. 集成步骤

## 2.1 配置统一认证平台提供的Token校验服务的引用

<dubbo:reference id="tokenService" interface="com.hisign.sso.api.service.sys.TokenService" timeout="20000" retries="0"/>

## 2.2 在拦截器调用Token校验服务

接口类：com.hisign.sso.api.service.sys.TokenService

方法：checkToken

参数：

String token, 从客户端请求中取到的Token，未取到传""。

String sysCode, 业务系统的系统编码，如"XCKY"，对应统一认证平台表uaop\_service\_resource的SYSTEM\_ID字段。

String serviceCode 服务编码，用于权限控制，对应统一认证平台表uaop\_service\_resource的RESOURCE\_ID字段。

返回JSON字符串：

TOKEN有效返回：

{

"rspCode": "0000"

}

TOKEN无效返回：

{

"rspCode": "1001",

"loginRestUrl": "http://127.0.0.1:8811/ssorest/sys/login.json"

}

rspCode含义：

1001：TOKEN不存在

1002：TOKEN过期

2000：其他错误

业务系统服务端在收到TOKEN有效的返回后继续做业务，收到无效和错误返回则中止业务，返回客户端统一登录的REST接口地址，由客户端调用统一认证平台进行登录，并由客户端保存统一认证平台返回的TOKEN，再次发起对业务系统服务端的请求时带上此TOKEN。

## 2.3 统一认证登录的REST接口协议

采用HTTP POST方法。

URL:

http://ip:端口/ssorest/sys/login.json

HTTP请求头：

Content-Type: application/json

请求：

{

"reqHead": {

"reqSn": "10001",

"reqTime": "20151223173601",

"apiCode": "sys.login",

"sysCode": "xcky",

"secretKey": "密钥字符串"

},

"reqBody": "密文字符串"

}

reqBody明文:

{

"account": "用户账号字符串",

"pass": "密码明文"

}

响应：

{

"rspHead": {

"reqSn": "同请求中的reqSn",

"rspTime": "20151223173601",

"secretKey": "同请求中的密钥字符串"

},

"rspBody": "密文字符串"

}

rspBody明文:

{

"token": "字符串",

"invalidTime": "令牌失效时间(长整型)"

}

reqBody和rspBody采用相同的密钥进行AES对称加密算法，对称密钥存在请求reqHead中的"secretKey"，secretKey由客户端随机生成，secretKey采用RSA非对称加密，RSA的公钥存在REST请求的客户端，RSA的私钥只存在REST请求的服务端。