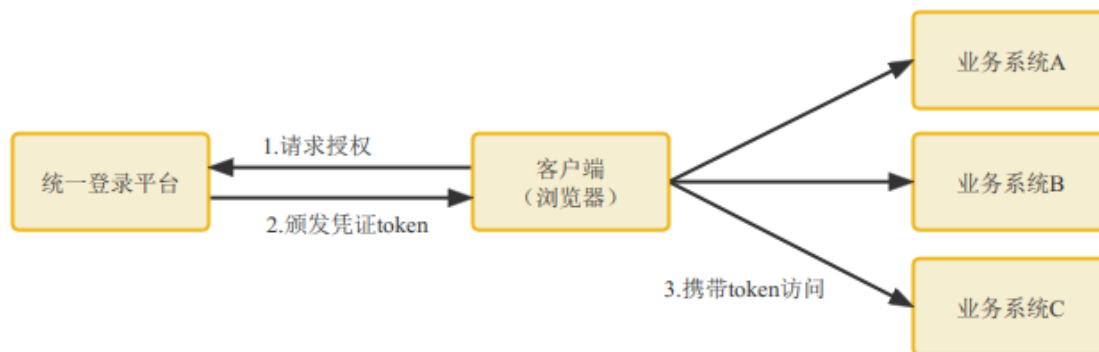


统一认证平台接入说明

简介

统一认证平台是一套基于统一身份治理概念实现的单点登录系统

系统基本架构为：



系统满足以下原则：

- 个人账户统一原则

个人邮箱账户一次认证，全平台业务系统可自动免密登录。

- 业务权限独立原则

统一登录平台只负责登录鉴权，不控制业务系统权限。每个业务系统的权限独立管理。

登录页 demo (链接待定) : <http://unipassport.chinastock.com.hk>

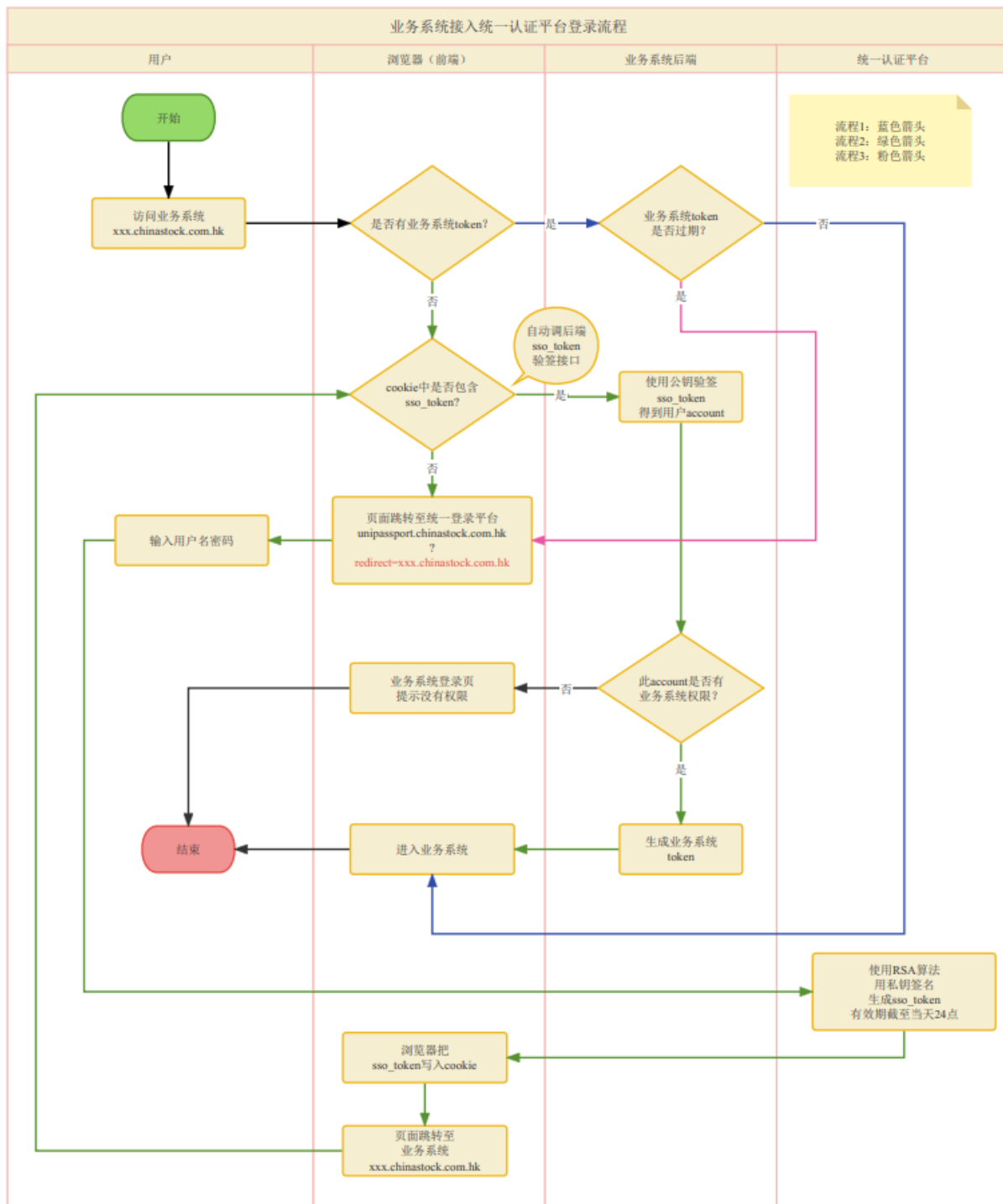


业务系统接入

基本认证流程

1. 用户在统一认证平台使用邮箱账号登录，会在浏览器的cookie写入一个sso_token，此sso_token是基于JWT标准、使用RSA算法私钥进行签名之后的字符串。此cookie所在域为chinastock.com.hk，有效期截至当天24点。
2. 当用户访问业务首页（或登录页）时，业务系统读取到sso_token，使用RSA公钥验签得到用户账号，验签成功即代表用户登录成功。

流程图



1. 流程1（蓝色线）：此流程表示 当浏览器中有有效的业务系统token时，用户可直接进入业务系统。此流程一般业务系统已具备，不需要改动。

2. 流程2（粉色线）：此流程表示 当浏览器中的业务系统token过期时，前端应跳转至统一认证平台（此前为跳转到业务系统登录页），跳转时应携带redirect参数为业务系统访问路径。

备注：业务系统后端拦截到token过期时，也可以直接读取cookie中的sso_token完成验签，然后对业务系统token进行自动续期，这样用户就不用再次登录了。

3. 流程3（绿色线）：此流程表示 当用户直接访问业务系统首页（或登录页）：

业务系统读取到 sso_token：验签此sso_token完成自动登录

业务系统未能读取到 sso_token：前端应跳转至统一认证平台，跳转时应携带redirect参数为业务系统访问路径。用户在统一认证平台登录完成后，前端会自动跳转回redirect路径，此时业务系统能读取到 sso_token，然后完成自动登录。

验签

提供两种验签方式，可**自行选择一种方式**：

1. 业务系统使用公钥验签（推荐）

使用RSA公钥验签，示例代码（JAVA）：

```
private static final String PUB_KEY =
"MIIBIjANBgqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlkLO24YqosKAZcI3G7k09mLq5KfADArBi89hrk
Em9Izquda//Lu4UouvfomqbqsZHIWjm3g5C2TuUt6pOVfudCVVPmpFQxmaAyB1m79jQZNssCu2sb+nAvHsa
pjGbaIYGXiieEbau5GKBCXnOVM0ToX6+KHpdYTIhL/C1IkaFoEE/9cpawOz4tY8n9d1JKmHg4jo3i7V4a9tm
CvKcLPj/ou6DzEQPcIrIagDJ9Wu1HpYvPFcBsZvwFZ5ZvmDOgrY//MvHW82/G8aPKprq/AvUN5LnSI0iVPJK
4dbpkaicP8/4qa8BGxQs5EX0wPkNWq/LKKi+pZeFEWNQNRd3adQIDAQAB";

/**
 * get user account from sso_token
 *
 * @param token sso_token in cookie
 * @return return a lowercase account without an email domain suffix
 */
public static String getAccount(String token) {
    PublicKey publicKey = null;
    try {
        publicKey = getPublicKey();
    } catch (Exception e) {
        // failed to get public key
        return null;
    }

    try {
        Jws<Claims> claimsJws =
Jwts.parser().setSigningKey(publicKey).parseClaimsJws(token);
        Claims claims = claimsJws.getBody();
        // get user account from sso_token
        return claims.get("account").toString();
    } catch (Exception e) {
        // sso_token has expired or invalid
        return null;
    }
}

/**
 * get public key
 *
 * @return PublicKey
 */
public static PublicKey getPublicKey() throws Exception {
```

```
byte[] bytes = PUB_KEY.getBytes();
bytes = Base64.getDecoder().decode(bytes);
X509EncodedKeySpec spec = new X509EncodedKeySpec(bytes);
KeyFactory factory = KeyFactory.getInstance("RSA");
return factory.generatePublic(spec);
}
```

2. 调用统一认证平台接口验签

接口路径、请求响应参数如下图：

The screenshot shows a REST client interface with a POST request to `http://unipassport.chinastock.com.hk/unipassport/sso/verify/v1`. The request body is raw and contains the following text:

```
{
  "ssoToken": "eyJhbGciOiJIUzI1NiJ9.eyJhY2NvdW50Ijoid19mYW56aGVuZ3l1bmciLCJqdGkiOiI2YTl1mWwRbH93NjkwLTQwMDAtODVmMy1hNDIzNmQ2YjYyMzU1LCJleHAiOjE2ODE4MzM1OTI9.KR1_FYJaSzp0xgoFqvC7gLSOP6mHXpJVqc0tkaBKVDjxapMaESj66Rw3JJv_53gqRkS-fkXZ9-KDHECFZP1n45L18HV9jw_Dv_Y5zwYBZ1aJeicsISAtdrBeBjizr4733-VsieVRBphVHK98wvsS2AUMPSwjAJrR3aoSvRlwcXdzZTthIuGeBrjze-_tpH9Jm4eMo71LwDQ8r21m8G6d0eBWHsH_w921zZiah41rlxQm9UqdQe70tLHq1HWITe450k3LTX-KB_hYhAuYP-00tqRpXhwL0ZNhTqpRIWjzWR4UiA4heBp7hHELaPBdSmwTwchvpdBsv9_8iLWv8b-Q"
```

The response body is JSON and contains the following data:

```
{
  "code": 0,
  "msg": "success",
  "data": {
    "account": "v_fanzhengyong"
  }
}
```

注意事项

1. 业务系统的域名必须是 chinastock.com.hk 结尾，才能读取到 sso_token
2. 请只接入生产环境