1. **专利名称**：一种单点登录方式的实现
2. **设计人**：路以恒 门合建

**联系电话及email**：15948740896 1321968067@qq.com

**说明书摘要**：

本发明实现一种通过第三方应用的接入来实现单点登录的方法。通过应用服务端向sso平台请求票据，实现新型单点登录方式。具体包括：

对于提交应用信息的第三方，系统平台为其提供appcode及签名证书。平台应用端请求平台服务端获取临时code传给应用客户端。应用客户端利用临时code和应用标识进行数字签名，向sso平台获取ticket票据。检查ticket状态是否需要刷新。应用利用ticket获取用户基本信息和认证信息。

1. **说明书：**
   1. **技术领域**

本发明涉及计算机应用技术领域，特别利用第三方应用接入实现单点登录的实现方法。

* 1. **背景技术**

企业发展之初，每个企业使用到的系统很少，两个或者更少，每个系统独立运行，分别拥有自己独自的登录模块。久而久之，随着企业使用的系统增多，系统之间相互独立费事费时的弊端便逐渐显露出来，sso（Single Sign On,单点登录系统）便应运而生，联通各个系统，一处登录即可浏览全部相关系统，无需再重复登录。

然而即使有了sso单点登录系统，我们若想实现一处登录多点免登的需求，仍需要拥有一个账号作为登录通行证才可以浏览其他系统的相关网页。而对于时间比较紧张的用户，为了体验单点登录的快捷从而再去注册一个新的账号，无形中造成了不必要的时间浪费，和方便快捷的初衷也南辕北辙；并且重新申请账号无异于增大了信息泄露的风险，使得一些对个人隐私保护较为苛刻的用户望而却步。

因此，推出一种通过第三方介入实现单点登录的方式，既能实现一处登录其他互通的设计理念，也能在其基础进行改进和创新，让用户无需承担信息泄露的风险无需忍受注册流程的繁琐，实现一种新型单点登录方式。

* 1. **发明内容**
     1. **发明目的（所要解决的技术问题）**

本发明旨在提供一种利用第三方应用接入来实现单点登录的技术方法，实现业务的互通。

* + 1. **技术方案**

该方法基于单点登录实现原理，通过对系统平台及第三方应用的登录检测、登录授权、传递身份信息来完成利用第三方完成单点登录。流程图如图1所示。

* + - 1. **申请接入平台**

第三方应用提供相应信息，系统平台根据第三方提供的内容会颁发一个签名证书及认证标识

应用若接入平台需要提供如图2所需内容。

* + - 1. **应用端获取ticket**

第三方应用服务端使用系统平台服务端临时code及自身应用标识获取基础信息票据、刷新票据、认证信息票据：

|  |  |
| --- | --- |
| accessTicket | 可用来换取用户信息，有效期2小时。 |
| refreshTicket | 可用来刷新accessTicket的有效期用来保持用户登录状态。 |
| realAuthTicket | 可用来换取用户实名认证信息，有效期2小时（如果不需要认证信息，则realAuthTicket为空） |

返回结果为returnCode（返回状态标识）、description（信息描述）、result（返回结果）。

* + - 1. **检查ticket是否过期并刷新（refreshTicket）**

如果accessTicket票据过期，则调用如下接口进行刷新，获取最新的登录票据。返回值包括description（结果描述）、result（最新的ticket）、returnCode（返回状态标识）

* + - 1. **获取用户基础信息（证书签名认证）**

应用服务端使用accessTicket、appcode、sign，获取用户基础信息，其中sign是根据签名证书和appCode标识生成，其中涉及到签名认证工具类。应用服务端使用签名认证工具类RsaUtils.java进行签名。例：String sign = RsaUtil.sign(loginTicket +appCode);（loginTicket：需要进行签名的内容，appCode: 每个应用的应用编码，对应一个签名证书文件\*.P8）

* + - 1. **换取用户认证信息（realAuthTicket加密约束）**

第三方应用使用realAuthTicket获取用户实名认证信息

1. 加密：首先对字符段进行base64加密，然后在加密后获得的字符串之前加一段特定的字符。例如：

李明进行base64加密，得到“5p2O5piO”，在首部加“ch”，最后得到“ch5p2O5piO”

1. 解密：将前面的特定字符去除，然后利用base64算法对去除字符后的字符串进行解密。例如：

将串“ch5p2O5piO”去掉前2位，然后base64算法解密，得到正常值。

* + 1. **说明有益效果**

1. 该方法省略繁杂的注册流程，只需登录第三方应用并授权，即可实现账号信息共享并访问所需资源。
2. 该方法在向sso获取用户基本信息及认证信息为加密传输，极大程度保证了用户信息的安全。
3. 该方法通过第三方应用同系统平台的交互与传输数据，利用第三方的信息即可浏览系统平台下所有的内容。
   1. **附图说明（可选）**

**无**

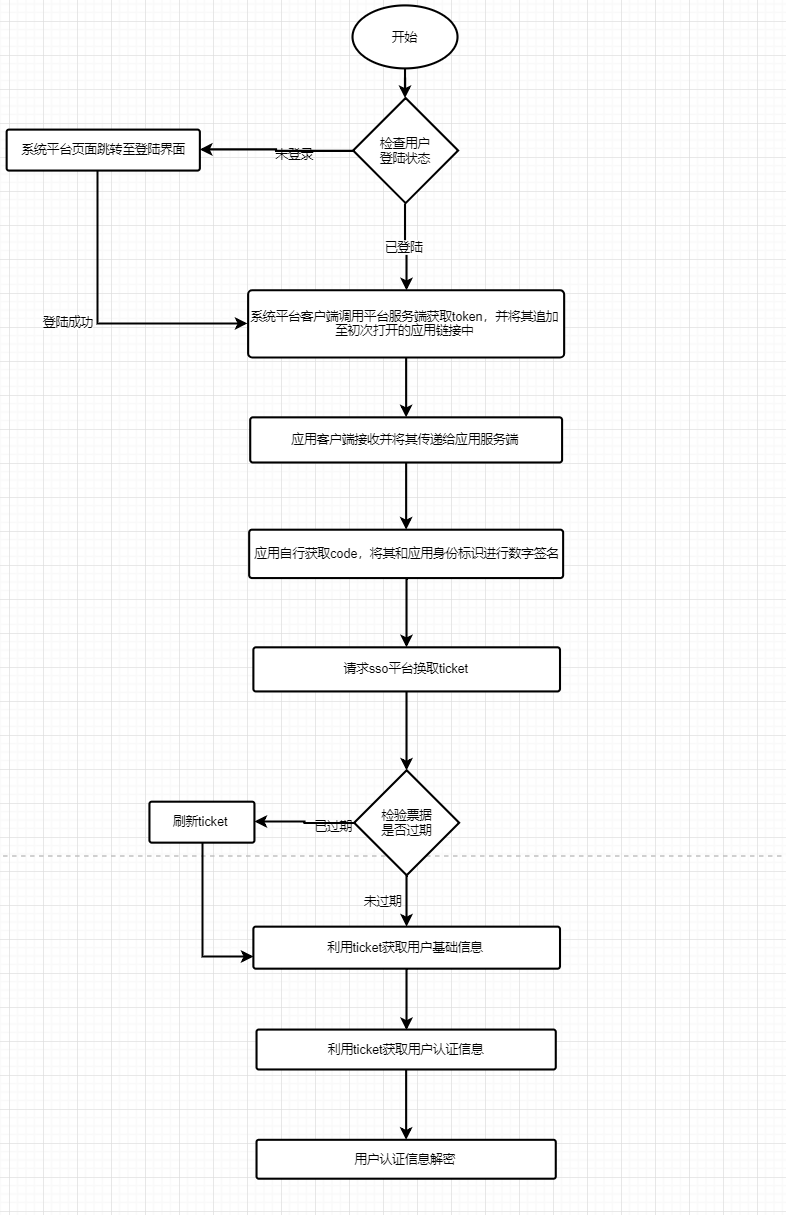
1. **说明书附图及附图说明**

图1 方法流程图

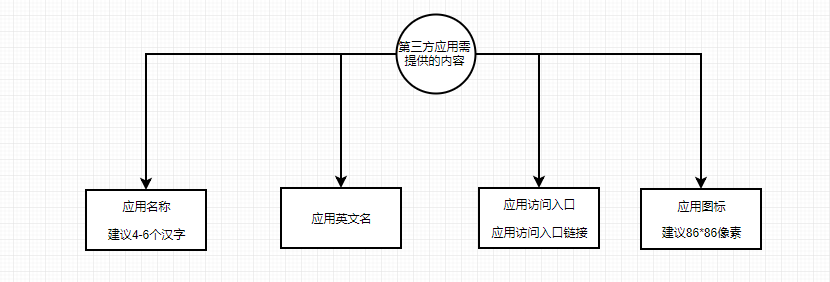


图2 第三方所需提供信息

1. **摘要附图及附图说明（可选，有则附上）**

**无**

1. **权利要求书**
   * 1. 本发明涉及计算机应用技术领域，特别利用第三方应用接入实现单点登录的实现方法。
     2. 如权利要求1所述的一种单点登录的实现方法，其特征是对于提交应用信息的第三方，系统平台为其提供appcode及签名证书，用于应用获取用户信息时进行签名认证。
     3. 如权利要求1所述的一种单点登录的实现方法，其特征是应用客户端获取ticket票据时，利用临时code和应用标识进行数字签名，并ticket状态是否需要刷新。
     4. 如权利要求1所述的一种单点登录的实现方法，其特征是应用获取用户基本信息和认证信息为加密状态，要进行解密，保障安全性。