(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111783067 B
(45)授权公告日 2023.09.08

(21)申请号 202010548020.8

(22)申请日 2016.05.09

(65)同一申请的已公布的文献号
申请公布号 CN 111783067 A

(43)申请公布日 2020.10.16

(62)分案原申请数据
201610302819.2 2016.05.09

(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心

(72)发明人 龚磊

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 周嗣勇

(51)Int.Cl.
G06F 21/41(2013.01)
G06F 21/46(2013.01)

(56)对比文件
CN 105472052 A,2016.04.06
CN 103428179 A,2013.12.04
CN 105430102 A,2016.03.23
US 2015381618 A1,2015.12.31
US 9203829 B1,2015.12.01
CN 104348777 A,2015.02.11
US 2010211796 A1,2010.08.19
CN 104580074 A,2015.04.29
CN 101771534 A,2010.07.07
CN 104378376 A,2015.02.25
US 9325696 B1,2016.04.26
CN 104038503 A,2014.09.10
CN 104348612 A,2015.02.11
CN 104869127 A,2015.08.26
US 2014245411 A1,2014.08.28
WO 0239237 A2,2002.05.16
CN 103457738 A,2013.12.18

审查员 王琪

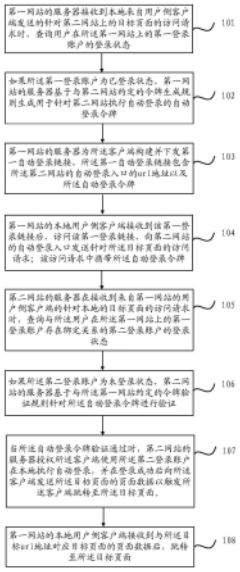
权利要求书3页 说明书16页 附图4页

(54)发明名称

多网站间的自动登录方法及装置

(57)摘要

本申请提供一种多网站间的自动登录方法及装置，包括：第一网站的服务器接收到来自客户端的针对第二网站上的目标页面的访问请求时，查询用户在第一网站上的第一登录账户的登录状态；如果第一登录账户为已登录状态，基于与第二网站约定的令牌生成规则生成自动登录令牌；为客户端构建并下发包含第二网站的自动登录入口url地址以及自动登录令牌的自动登录链接，客户端访问自动登录链接向第二网站的自动登录入口发送携带自动登陆令牌的针对目标页面的访问请求，第二网站的服务器验证自动登录令牌通过后，授权客户端使用与第一登录账户存在绑定关系的第二登录账户在第二网站执行自动登录并跳转至目标页面。本申请可以优化用户体验。



CN 111783067 B

1.一种多网站间的自动登录方法,应用于第一网站的服务器,该方法包括:

响应于用户通过客户端发起的针对第二网站上的目标页面的访问请求,查询所述用户在所述第一网站上的第一登录账户的登录状态;

如果所述第一登录账户为已登录状态,生成自动登录令牌;其中,所述自动登录令牌用于向所述第二网站共享用户在所述第一网站登录成功的鉴权结果;

向所述客户端下发第一自动登录链接,所述第一自动登录链接包含所述第二网站的自动登录入口的url地址和所述自动登录令牌,以使所述客户端访问所述第一自动登录链接,基于与所述第一登录账户存在绑定关系的、用户在所述第二网站上的第二登录账户在所述第二网站执行自动登录,并跳转至所述目标页面。

2.根据权利要求1所述的方法,所述生成自动登录令牌,包括:

基于与第二网站约定的令牌生成规则生成自动登录令牌。

3.根据权利要求1所述的方法,所述方法还包括:

响应于所述客户端发起的针对第二网站的资源访问请求,向所述客户端下发第二自动登录链接,所述第二自动登录链接包含本地自动登录入口的url地址以及所述客户端请求的资源所在的第二网站上的目标页面的url地址,以使所述客户端访问所述第二自动登录链接,向本地自动登录入口发送所述针对所述目标页面的访问请求。

4.根据权利要求1所述的方法,所述方法还包括:

如果所述第一登录账户为未登录状态,向所述客户端下发本地主动登录入口的url地址,以触发所述客户端访问所述url地址,跳转至与所述url地址对应的登录页面,使用所述第一登录账户完成主动登录。

5.根据权利要求2所述的方法,所述与第二网站约定的令牌生成规则包括存储在第二网站的登陆域配置信息中的预设加密算法以及密钥;

所述基于与第二网站约定的令牌生成规则生成自动登录令牌包括:

从第二网站的登陆域配置信息中读取预设加密算法以及密钥;

基于读取到的所述预设加密算法以及密钥针对与第二网站约定的令牌生成参数进行计算,生成作为所述自动登录令牌的随机字符串;

其中,所述令牌生成参数包括以下内容中的一个或者多个的组合:

所述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间。

6.一种多网站间的自动登录方法,应用于第二网站的服务器,其特征在于,该方法包括:

响应于用户通过第一网站的客户端发起的针对第二网站的目标页面的访问请求,查询与所述用户在所述第一网站上的第一登录账户存在绑定关系的、用户在所述第二网站的第二登录账户的登录状态;其中,所述访问请求携带自动登录令牌;所述自动登录令牌用于向所述第二网站共享用户在所述第一网站登录成功的鉴权结果;

如果所述第二登录账户为未登录状态,基于所述第二登录账户在所述第二网站执行自动登录,并跳转至所述目标页面。

7.根据权利要求6所述的方法,所述基于所述第二登录账户在所述第二网站执行自动登录,包括:

基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证;

当所述自动登录令牌验证通过时，授权所述客户端使用所述第二登录账户在所述第二网站执行自动登录。

8.根据权利要求6所述的方法，所述方法还包括：

如果所述第二登录账户为已登录状态，向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

9.根据权利要求7所述的方法，所述方法还包括：

当所述自动登录令牌验证失败时，向所述客户端下发本地主动登录入口的url地址，以触发所述客户端跳转至与所述本地主动登录入口的url地址对应的登录页面，使用所述第二登录账户完成主动登录。

10.根据权利要求7所述的方法，所述与所述第一网站约定的令牌验证规则为存储在本地登陆域配置信息中的预设解密算法以及密钥；

所述基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证，包括：

从本地的登陆域配置信息中读取预设解密算法以及密钥；

基于读取到的预设解密算法以及密钥针对所述自动登录令牌进行解密，并验证解密后生成的参数是否为与所述第一网站约定的令牌生成参数；如果是，则所述自动登录令牌验证通过；

其中，所述令牌生成参数包括以下内容中的一个或者多个的组合：

所述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间。

11.一种多网站间的自动登录装置，应用于第一网站的服务器，该装置包括：

第一查询模块，用于响应于用户通过客户端发起的针对第二网站上的目标页面的访问请求，查询所述用户在所述第一网站上的第一登录账户的登录状态；

生成模块，用于在所述第一登录账户为已登录状态，生成自动登录令牌；其中，所述自动登录令牌用于向所述第二网站共享用户在所述第一网站登录成功的鉴权结果；

下发模块，用于向所述客户端下发第一自动登录链接，所述第一自动登录链接包含所述第二网站的自动登录入口的url地址和所述自动登录令牌，以使所述客户端访问所述第一自动登录链接，基于与所述第一登录账户存在绑定关系的、用户在所述第二网站上的第二登录账户在所述第二网站执行自动登录，并跳转至所述目标页面。

12.根据权利要求11所述的装置，所述生成模块进一步用于：

基于与第二网站约定的令牌生成规则生成自动登录令牌。

13.根据权利要求11所述的装置，所述下发模块进一步用于：

响应于所述客户端发起的针对第二网站的资源访问请求，向所述客户端下发第二自动登录链接，所述第二自动登录链接包含本地自动登录入口的url地址以及所述客户端请求的资源所在的第二网站上的目标页面的url地址，以使所述客户端访问所述第二自动登录链接，向本地自动登录入口发送所述针对所述目标页面的访问请求。

14.根据权利要求11所述的装置，所述下发模块进一步用于：

如果所述第一登录账户为未登录状态，向所述客户端下发本地主动登录入口的url地址，以触发所述客户端访问所述url地址，跳转至与所述url地址对应的登录页面，使用所述第一登录账户完成主动登录。

15.根据权利要求12所述的装置，所述与第二网站约定的令牌生成规则包括存储在第二网站的登陆域配置信息中的预设加密算法以及密钥；

所述生成模块具体用于：

从第二网站的登陆域配置信息中读取预设加密算法以及密钥；

基于读取到的所述预设加密算法以及密钥针对与第二网站约定的令牌生成参数进行计算，生成作为所述自动登录令牌的随机字符串；

其中，所述令牌生成参数包括以下内容中的一个或者多个的组合：

所述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间。

16.一种多网站间的自动登录装置，应用于第二网站的服务器，该装置包括：

第二查询模块，用于响应于用户通过第一网站的客户端发起的针对第二网站的目标页面的访问请求，查询与所述用户在所述第一网站上的第一登录账户存在绑定关系的、用户在所述第二网站的第二登录账户的登录状态；其中，所述访问请求携带自动登录令牌；所述自动登录令牌用于向所述第二网站共享用户在所述第一网站登录成功的鉴权结果；

授权模块，用于如果所述第二登录账户为未登录状态，基于所述第二登录账户在所述第二网站执行自动登录，并跳转至所述目标页面。

17.根据权利要求16所述的装置，该装置还包括验证模块，所述验证模块进一步用于：

基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证；

当所述自动登录令牌验证通过时，授权所述客户端使用所述第二登录账户在所述第二网站执行自动登录。

18.根据权利要求16所述的装置，所述授权模块进一步用于包括：

如果所述第二登录账户为已登录状态，向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

19.根据权利要求17所述的装置，所述验证模块进一步用于：

当所述自动登录令牌验证失败时，向所述客户端下发本地主动登录入口的url地址，以触发所述客户端跳转至与所述本地主动登录入口的url地址对应的登录页面，使用所述第二登录账户完成主动登录。

20.根据权利要求17所述的装置，所述与所述第一网站约定的令牌验证规则为存储在本地登陆域配置信息中的预设解密算法以及密钥；

所述验证模块具体用于：

从本地的登陆域配置信息中读取预设解密算法以及密钥；

基于读取到的预设解密算法以及密钥针对所述自动登录令牌进行解密，并验证解密后生成的参数是否为与所述第一网站约定的令牌生成参数；如果是，则所述自动登录令牌验证通过；

其中，所述令牌生成参数包括以下内容中的一个或者多个的组合：

所述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间。

多网站间的自动登录方法及装置

技术领域

[0001] 本申请涉及通信领域，尤其涉及一种多网站间的自动登录方法及装置。

背景技术

[0002] 在相关技术中，对于存在合作关系的不同网站之间，用户通常可以使用第一网站的本地客户端来直接访问第二网站上的目标页面；例如，可以在第一网站的本地客户端中添加第二网站上的目标页面的访问链接，用户可以通过点击该访问链接跳转至对应的目标页面进行访问。

[0003] 然后，用户在使用第一网站的本地客户端访问第二网站上的目标页面时，第二网站通常会要求用户使用在第二网站上的登录账户和密码登录第二网站后，才能能获得该目标页面的访问权限跳转至该目标页面，因此操作非常不方便。

发明内容

[0004] 本申请提出一种多网站间的自动登录方法，该方法包括：

[0005] 当接收到来自用户侧客户端的针对第二网站上的目标页面的访问请求时，查询用户在所述第一网站上的第一登录账户的登录状态；

[0006] 如果所述第一登录账户为已登录状态，基于与第二网站约定的令牌生成规则生成自动登录令牌；

[0007] 为所述客户端构建并下发第一自动登录链接，所述第一自动登录链接包含所述第二网站的自动登录入口的url地址以及所述自动登录令牌，以使所述客户端访问该第一自动登录链接向第二网站的自动登录入口发送携带所述自动登陆令牌的针对所述目标页面的访问请求，并在所述第二网站的服务器针对所述自动登录令牌验证通过后，授权所述客户端使用与所述第一登录账户存在绑定关系的第二登录账户在第二网站执行自动登录并跳转至所述目标页面。

[0008] 在本例中，所述方法还包括：

[0009] 在接收到来自所述用户侧客户端的针对第二网站的资源访问请求时，为所述客户端构建并下发第二自动登录链接，所述第二自动登录链接包含本地自动登录入口的url地址以及所述客户端请求的资源所在的第二网站上的目标页面的url地址，以使所述客户端访问该第二自动登录链接向本地自动登录入口发送所述针对所述目标页面的访问请求。

[0010] 在本例中，所述方法还包括：

[0011] 如果所述第一登录账户为未登录状态，向所述客户端下发本地主动登录入口的url地址，以触发所述客户端跳转至与所述本地主动登录入口的url地址对应的登录页面，使用所述第一登录账户完成主动登录。

[0012] 在本例中，所述与第二网站约定的令牌生成规则包括存储在第二网站的登陆域配置信息中的预设加密算法以及密钥；

[0013] 所述基于与第二网站约定的令牌生成规则生成自动登录令牌包括：

[0014] 从第二网站的登陆域配置信息中读取预设加密算法以及密钥；

[0015] 基于读取到的所述预设加密算法以及密钥针对与第二网站约定的令牌生成参数进行计算生成作为所述自动登录令牌的随机字符串；

[0016] 其中，所述令牌生成参数包括以下内容中的一个或者多个的组合：

[0017] 所述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间。

[0018] 本申请还提出一种多网站间的自动登录方法，应用于第二网站的服务器，该方法包括：

[0019] 当接收到来自第一网站的用户侧客户端的针对本地的目标页面的访问请求时，查询与所述用户在所述第一网站上的第一登录账户存在绑定关系的第二登录账户的登录状态；其中，所述访问请求携带所述第一网站的服务器基于约定的令牌生成规则生成的自动登录令牌；

[0020] 如果所述第二登录账户为未登录状态，基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证；

[0021] 当所述自动登录令牌验证通过时，授权所述客户端使用所述第二登录账户在本地执行自动登录，并在登录成功后向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

[0022] 在本例中，所述方法还包括：

[0023] 如果所述第二登录账户为已登录状态，向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

[0024] 在本例中，所述方法还包括：

[0025] 当所述自动登录令牌验证失败时，向所述客户端下发本地主动登录入口的url地址，以触发所述客户端跳转至与所述本地主动登录入口的url地址对应的登录页面，使用所述第二登录账户完成主动登录。

[0026] 在本例中，所述与第一网站约定的令牌验证规则为存储在本地登陆域配置信息中的预设解密算法以及密钥；

[0027] 所述基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证包括：

[0028] 从本地的登陆域配置信息中读取预设解密算法以及密钥；

[0029] 基于读取到的预设解密算法以及密钥针对所述自动登录令牌进行解密，并验证解密后生成的参数是否为与所述第一网站约定的令牌生成参数；如果是，则所述自动登录令牌验证通过；

[0030] 其中，所述令牌生成参数包括以下内容中的一个或者多个的组合：

[0031] 所述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间。

[0032] 本申请还提出一种多网站间的自动登录装置，应用于第一网站的服务器，该装置包括：

[0033] 第一查询模块，用于当接收到来自用户侧客户端的针对第二网站上的目标页面的访问请求时，查询用户在所述第一网站上的第一登录账户的登录状态；

[0034] 生成模块，用于在所述第一登录账户为已登录状态，基于与第二网站约定的令牌生成规则生成自动登录令牌；

[0035] 下发模块，用于为所述客户端构建并下发第一自动登录链接，所述第一自动登录链接包含所述第二网站的自动登录入口的url地址以及所述自动登录令牌，以使所述客户端访问该第一自动登录链接向第二网站的自动登录入口发送携带所述自动登陆令牌的针对所述目标页面的访问请求，并在所述第二网站的服务器针对所述自动登录令牌验证通过后，授权所述客户端使用与所述第一登录账户存在绑定关系的第二登录账户在第二网站执行自动登录并跳转至所述目标页面。

[0036] 在本例中，所述下发模块进一步用于：

[0037] 在接收到来自所述用户侧客户端的针对第二网站的资源访问请求时，为所述客户端构建并下发第二自动登录链接，所述第二自动登录链接包含本地自动登录入口的url地址以及所述客户端请求的资源所在的第二网站上的目标页面的url地址，以使所述客户端访问该第二自动登录链接向本地自动登录入口发送所述针对所述目标页面的访问请求。

[0038] 在本例中，所述下发模块进一步用于：

[0039] 如果所述第一登录账户为未登录状态，向所述客户端下发本地主动登录入口的url地址，以触发所述客户端跳转至与所述本地主动登录入口的url地址对应的登录页面，使用所述第一登录账户完成主动登录。

[0040] 在本例中，所述与第二网站约定的令牌生成规则包括存储在第二网站的登陆域配置信息中的预设加密算法以及密钥；

[0041] 所述生成模块具体用于：

[0042] 从第二网站的登陆域配置信息中读取预设加密算法以及密钥；

[0043] 基于读取到的所述预设加密算法以及密钥针对与第二网站约定的令牌生成参数进行计算生成作为所述自动登录令牌的随机字符串；

[0044] 其中，所述令牌生成参数包括以下内容中的一个或者多个的组合：

[0045] 所述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间。

[0046] 本申请还提出一种多网站间的自动登录装置，应用于第二网站的服务器，该装置包括：

[0047] 第二查询模块，用于当接收到来自第一网站的用户侧客户端的针对本地的目标页面的访问请求时，查询与所述用户在所述第一网站上的第一登录账户存在绑定关系的第二登录账户的登录状态；其中，所述访问请求携带所述第一网站的服务器基于约定的令牌生成规则生成的自动登录令牌；

[0048] 验证模块，用于如果所述第二登录账户为未登录状态，基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证；

[0049] 授权模块，用于当所述自动登录令牌验证通过时，授权所述客户端使用所述第二登录账户在本地执行自动登录，并在登录成功后向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

[0050] 在本例中，所述授权模块进一步用于包括：

[0051] 如果所述第二登录账户为已登录状态，向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

[0052] 在本例中，所述验证模块进一步用于：

[0053] 当所述自动登录令牌验证失败时，向所述客户端下发本地主动登录入口的url地

址,以触发所述客户端跳转至与所述本地主动登录入口的url地址对应的登录页面,使用所述第二登录账户完成主动登录。

[0054] 在本例中,所述与第一网站约定的令牌验证规则为存储在本地登陆域配置信息中的预设解密算法以及密钥;

[0055] 所述验证模块具体用于:

[0056] 从本地的登陆域配置信息中读取预设解密算法以及密钥;

[0057] 基于读取到的预设解密算法以及密钥针对所述自动登录令牌进行解密,并验证解密后生成的参数是否为与所述第一网站约定的令牌生成参数;如果是,则所述自动登录令牌验证通过;

[0058] 其中,所述令牌生成参数包括以下内容中的一个或者多个的组合:

[0059] 所述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间。

[0060] 本申请中,第一网站的服务器在接收到来自用户客户端的针对第二网站的目标页面的访问请求时,如果查询到该用户在第一网站上的第一登录账户为已登录状态,可以基于与第二网站约定的令牌生成规则生成自动登录令牌,并为客户端构建并下发包含第二网站的自动登录入口的url地址以及所述自动登录令牌的登录链接;客户端在收到该登录链接后,可以访问该登录链接,向第二网站的自动登录入口发送携带所述自动登录令牌的针对所述目标url地址的访问请求,第二网站的服务器在接收到该访问请求后,如果查询到与所述第一登录账户存在绑定关系的第二登录账户为未登录状态时,则对该访问请求中的自动登录令牌进行验证,并在验证通过后,授权所述客户端使用该第二登录账户在本地执行自动登录,以及在登录成功后向所述客户端发送与所述目标url地址对应的页面数据,来触发该客户端跳转至与该目标url对应的目标页面;本申请实现了用户在使用第一网站的客户端访问第二网站上的目标页面时,可以直接跳转至第二网站上的目标页面,而不需要用户手动输入在第二网站上的第二登录账户和密码来执行手动登录,从而可以降低操作复杂度,极大的优化用户体验。

附图说明

[0061] 图1是本申请一实施例提供的一种多网站间的自动登录方法的流程图;

[0062] 图2是本申请一实施例提供的一种核心组件架构图;

[0063] 图3是本申请一实施例提供的一种多网站间的自动登录装置的逻辑框图;

[0064] 图4是本申请一实施例提供的承载所述一种多网站间的自动登录装置的第一网站的服务器的硬件结构图;

[0065] 图5是本申请一实施例提供的另一种多网站间的自动登录装置的逻辑框图;

[0066] 图6是本申请一实施例提供的承载所述另一种多网站间的自动登录装置的第二网站的服务器的硬件结构图。

具体实施方式

[0067] 在相关技术中,用户在使用第一网站的用户侧客户端访问第二网站上的目标页面时,通常需要输入用户在第二网站上的登录账户和密码登录第二网站,并在登陆成功后才能获得该目标页面的访问权限并跳转至该目标页面,因此操作非常不方便。

[0068] 为了解决上述问题，本申请提出一种多网站间的自动登录方法，第一网站的服务器在接收到来自用户客户端的针对第二网站的目标页面的访问请求时，如果查询到该用户在第一网站上的第一登录账户为已登录状态，可以基于与第二网站约定的令牌生成规则生成自动登录令牌，并为客户端构建并下发包含第二网站的自动登录入口的url地址以及所述自动登录令牌的登录链接；客户端在收到该登录链接后，可以访问该登录链接，向第二网站的自动登录入口发送携带所述自动登录令牌的针对所述目标url地址的访问请求，第二网站的服务器在接收到该访问请求后，如果查询到与所述第一登录账户存在绑定关系的第二登录账户为未登录状态时，则对该访问请求中的自动登录令牌进行验证，并在验证通过后，授权所述客户端使用该第二登录账户在本地执行自动登录，以及在登录成功后向所述客户端发送与所述目标url地址对应的页面数据，来触发该客户端跳转至与该目标url对应的目标页面；

[0069] 本申请实现了用户在使用第一网站的客户端访问第二网站上的目标页面时，可以直接跳转至第二网站上的目标页面，而不需要用户手动输入在第二网站上的第二登录账户和密码来执行手动登录，从而可以降低操作复杂度，极大的优化用户体验。

[0070] 下面通过具体实施例并结合具体的应用场景对本申请进行描述。

[0071] 请参考图1，图1是本申请一实施例提供的一种多网站间的自动登录方法，所述方法执行以下步骤：

[0072] 步骤101，第一网站的服务器接收到来自用户侧客户端的针对第二网站上的目标页面的访问请求时，查询用户在所述第一网站上的第一登录账户的登录状态；

[0073] 在本例中，上述用户客户端可以包括第一网站的web客户端(比如浏览器)。在上述客户端的用户界面中，可以预先添加指向第一网站的自动登录入口的用于访问第二网站上的资源的访问链接；

[0074] 其中，上述访问链接可以包括第一网站的自动登录入口的url地址以及上述客户端在访问第二网站上的资源时，需要向第一网站的自动登录入口传递的查询参数；

[0075] 当用户需要使用第一网站的用户侧客户端来请求访问第二网站上的资源时，可以通过点击上述访问链接，来触发该客户端向第一网站的服务器发送针对第二网站的资源访问请求。

[0076] 当用户“点击”该上述访问链接后，上述客户端可以基于该访问链接中的查询参数以及用户在第一网站上的第一登录账户，来构建资源访问请求，然后访问第一网站的自动登录入口的url地址，将构建完成的该资源访问请求发往第一网站的服务器上的自动登录入口。

[0077] 其中，在用户通过在第一网站的用户侧客户端中，查询第二网站上的业务资源的应用场景中，上述用于访问第二网站上的资源的访问链接可以是一业务查询链接；上述查询参数可以包括与用户需要查询的业务资源对应的业务标识等信息；而上述客户端构建的上述资源访问请求则可以是一业务查询请求。

[0078] 例如，以第一网站为支付宝(alipay)，第二网站为淘宝(taobao)为例，用户需要在支付宝客户端中查询一笔由支付宝完成支付的淘宝交易的详情信息，此时上述资源访问请求可以是针对该笔交易的业务查询请求，上述查询参数则可以是该笔淘宝交易的交易号。

[0079] 假设该笔淘宝交易的交易号为“20150411252031”，支付宝的自动登录入口url地

址为“http://www.alipay.com/auto_login.htm”,此时上述业务查询链接可以是如下链接:

[0080] “http://www.alipay.com/auto_login.htm?tradeNo=20150411252031”

[0081] 在上述链接中,“?”为上述业务查询链接中的参数传递标识符,该参数传递标识符后面的内容即为支付宝客户端在查询交易号为20150411252031的淘宝交易的详情信息时,需要向支付宝的自动登录入口传递的业务查询参数。

[0082] 支付宝客户端可以在用户界面中与该笔交易的对应位置上添加一个“查看交易详情”的标记,并将该标记指向上述业务查询链接。当用户在支付宝客户端中点击“查询交易详情”的标记时,此时客户端可以读取上述业务查询链接中的tradeNo(即交易号),构建一个携带该交易号以及用户的支付宝账号的业务查询请求,然后可以访问支付宝的自动登录入口的url地址,将业务查询请求该发往支付宝服务器的自动登录入口。以下以用户通过第一网站的用户侧客户端查询第二网站上的业务资源的应用场景为例进行说明。

[0083] 在本例中,当第一网站的服务器通过自动登录入口接收到用户侧客户端发送的业务查询请求后,可以读取该业务查询请求中的业务查询参数,在本地业务数据库中进行相应的业务资源查询。

[0084] 如果第一网站的服务器在本地业务数据库中查询到了对应的业务详情信息,表明与该业务查询请求对应的业务资源为第一网站的本地业务资源,此时第一网站的服务器可以检查该业务查询请求中携带的第一登录账户的登录状态;如果该第一登录账户为已登录状态,此时表明用户已使用第一登录账户登录了第一网站,第一网站的服务器可以直接向该本地客户端返回对应的业务资源即可。

[0085] 如果在本地业务数据库中未查询到对应的业务资源,表明与该业务查询请求对应的业务资源为属于第三方网站的非本地业务资源。

[0086] 对于属于第三方网站的非本地业务资源,在第一网站的服务器上通常会预存储该业务资源与该业务资源所在的第三方网站上的目标页面的目标url地址之间的映射关系;其中该目标url地址,即为第一网站的用户侧客户端在查询第二网站上的非本地业务资源时,需要访问的第二网站上的目标页面的url地址。

[0087] 如果第一网站的服务器在本地业务数据库中未查询到与上述业务查询请求对应的业务资源,则可以基于上述映射关系来确定出与需要查询的该业务资源对应的第二网站的目标页面的url地址,然后为该客户端构建并下发一个用于在第一网站的登陆域中执行自动登录的自动登录链接(即第二登录链接)。

[0088] 在本例中,上述登陆域是指用户希望登录的目标系统。在第一网站的服务器上,可以维护多个登录域。在实际应用中,第一网站的服务器可以和其它网站(比如与第一网站存在合作关系的其它网站)的服务器进行交互,将各自登录域的配置信息周期性的互相同步至其它网站的服务器。

[0089] 例如,假设第一网站为支付宝,支付宝为淘宝、当当等电商平台提供第三方支付解决方案,那么支付宝的服务器可以与淘宝、当当的服务器分别进行交互,将各自登陆域的配置信息同步给对方,从而使得支付宝的服务器上可以同时维护淘宝、当当等多个电商平台所属登陆域的配置信息。

[0090] 在本例中,第一网站的服务器为上述客户端构建并下发的上述用于在第一网站的

登录域中执行自动登录的自动登录链接，可以包括第一网站的自动登录入口的url地址，用户需要访问的业务资源所在的第二网站的目标页面的url地址，以及上述客户端在访问第二网站上的目标页面的url地址时，需要向第一网站的自动登录入口的传递的业务查询参数。

[0091] 其中，在示出的一种实施方式中，上述客户端在访问第二网站上的目标页面时，需要向第一网站的自动登录入口的传递的业务查询参数中，可以包括该业务请求来源的登陆域名称，第二网站的目标页面的url地址，第二网站的登陆域名称，用户在第一网站登录时所使用的第一登录账户等信息。

[0092] 上述客户端在接收到第一网站的服务器下发的上述自动登录链接后，可以基于上述自动登录链接中包含的业务查询参数，构建一个针对第二网站的目标页面的url地址的访问请求，然后访问第一网站的自动登录入口的url地址，将构建完成的针对第二网站的目标页面的url地址的访问请求发送至第一网站的自动登录入口；其中，构建完成的该访问请求中携带的参数，将与上述自动登录链接中包含的业务查询参数保持一致。

[0093] 例如，仍然以第一网站为支付宝，第二网站为淘宝，以及用户需要在支付宝客户端中查询一笔由支付宝完成支付的淘宝交易的详情信息为例，假设支付宝的自动登录入口url地址为“http://www.alipay.com/auto_login.htm”，用户要访问的淘宝的目标页面的url地址为“www.taobao.com/trade/list.htm”，支付宝的服务器为支付宝客户端构建并下发的用于在支付宝的登陆域中执行自动登录的自动登录链接可以为如下链接：

[0094] http://www.alipay.com/auto_login.htm?loginRequestFrom＝Alipay&target＝http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm&domain＝taobao&loginAccount＝test_123@alipay.com；

[0095] 在以上自动登录链接中，“?”为上述自动登录链接中的参数传递标识符，该参数传递标识符后面的内容即为支付宝客户端在访问淘宝上的上述目标url地址时，需要向支付宝的自动登录入口传递的业务查询参数。

[0096] 其中，“loginRequestFrom＝Alipay”表示支付宝客户端基于该参数构建的访问请求来源于支付宝的登陆域；“loginAccount＝test_123@alipay.com”表示用户登录支付系统所使用的支付宝账户的名称为test_123@alipay.com；“target＝http%3A%2F%2Fae.com%2Ftrade%2Flist.htm”即为编码处理后的支付宝客户端访问的淘宝中的目标页面的url地址；“domain＝taobao”表示与支付宝系统对接的对端登陆域名称为taobao。

[0097] 支付宝客户端在接收到支付宝的服务器下发的上述自动登录链接后，可以基于上述自动登录链接中包含的业务查询参数，来构建一个针对第二网站的目标url地址的访问请求，然后访问支付宝的自动登录入口的url地址，将该访问请求发送至支付宝的服务器。

[0098] 在本例中，当第一网站的服务器通过本地的自动登录入口，接收到本地客户端发送的针对第二网站的目标页面的url地址的访问请求时，由于该访问请求的目的端为本地的自动登录入口，因此表明该本地客户端需要使用上述第一登录账户登录第一网站的登陆域后，才能够取得具有针对第二网站的目标url地址的访问权限。

[0099] 在这种情况下，第一网站的服务器在接收到客户端发送的针对第二网站的目标页面的url地址的访问请求后，可以从该访问请求中读取上述第一登录账号，然后在本地查询该第一登录账户的登录状态；

[0100] 例如,在实现时,第一网站的服务器可以将该第一登录账户作为查询索引,查询本地是否存储了与该第一登录账户对应的登录成功的鉴权结果,如果本地未存储该第一登录账户的登录成功的鉴权结果,则可以确认第一登录账户为未登录状态;反之,如果查询到了与该第一登录账户对应的登录成功的鉴权结果,则可以确认第一登录账户为未登录状态。

[0101] 步骤102,如果所述第一登录账户为已登录状态,第一网站的服务器基于与第二网站约定的令牌生成规则生成用于针对第二网站执行自动登录的自动登录令牌。

[0102] 在本例中,如果第一网站的服务器查询到第一登录账户为已登录状态,表明用户已经使用第一登录账户在第一网站的系统中执行了登录,此时第一网站的服务器可以基于与第二网站约定的令牌生成规则生成自动登录令牌(Token)。

[0103] 其中,该自动登录令牌用于在不同网站的登录域之间共享登录成功的鉴权结果;第一网站的服务器可以通过将生成的自动登录令牌传递至第二网站的服务器,将第一登录账户在第一网站的登陆域中登录成功的鉴权结果共享至第二网站。

[0104] 在示出的一种实施方式中,第一网站与第二网站约定的令牌生成规则,可以作为登陆域配置信息,预先存储在第一网站的服务器在本地维护的第二网站的登录域配置信息中。

[0105] 上述登陆域配置信息通常包括该登陆域的主动登录入口的url以及自动登录入口的url,而上述令牌生成规则具体可以包括约定的加密算法和密钥。因此,如果将网站之间约定的令牌生成规则也存储在登陆域配置信息中,那么该登录域配置信息中除了该登陆域的主动登录入口的url以及自动登录入口的url等信息以外,则还可以包含网站之间约定的加密算法以及密钥或者密钥的获取方式等信息。

[0106] 其中,需要说明的是,第一网站和第二网站约定的用于生成自动登录令牌的加密算法,在本例中不进行特别限定;例如,上述预设的加密算法可以包括DSA算法、RSA算法、MD5算法或者其它类型的对称加密算法。

[0107] 第一网站的服务器在基于与第二网站约定的令牌生成规则生成自动登录令牌时,可以从第二网站的登陆域配置信息中读取加密算法和密钥,并基于读取到的该加密算法和密钥针对与第二网站约定的令牌生成参数进行计算,以生成一个随机字符串,然后将生成的该随机字符串作为自动登录令牌进行存储。

[0108] 其中,在示出的一种实施方式中,上述令牌生成参数可以包括:第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间等信息中的一个或者多个的组合。即在本例中,在生成上述自动登录令牌时,上述令牌生成参数可以是与用户在第二网站上的第二登录账户完全无关的信息。

[0109] 当然,在实际应用中,上述令牌生成参数除了以上示出的第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间等信息以外,也可以包括其它类型的信息,在本例中不再一一列举。

[0110] 在本例中,如果第一网站的服务器查询到第一登录账户为未登录状态,表明用户尚未使用第一登录账户在第一网站的系统中执行登录,在这种情况下,第一网站的服务器可以将本地的主动登录入口的url地址下发给本地客户端。

[0111] 当该客户端接收到该主动登录入口的url地址时,可以访问该url地址,然后跳转至与该url地址对应的登录页面,然后由用户在该登录页面中手动输入上述第一登录账户,

以及对应的登录密码来执行主动登录。

[0112] 步骤103,第一网站的服务器为所述客户端构建并下发第一自动登录链接,所述第一自动登录链接包含所述第二网站的自动登录入口的url地址以及所述自动登录令牌。

[0113] 步骤104,第一网站的用户侧客户端接收到该第一登录链接后,访问该第一登录链接,向第二网站的自动登录入口发送针对所述目标页面的访问请求;该访问请求中携带所述自动登录令牌;

[0114] 在本例中,当第一网站的服务器在确定上述第一登录账户为已登录状态,并且生成了上述自动登录令牌后,可以为用户侧客户端构建并下发一个用于在第二网站的登陆域中执行自动登录的自动登录链接(即第一登录链接),以将该本地客户端针对第二网站的目标页面的访问请求,重定向至第二网站的自动登录入口。

[0115] 第一网站的服务器为用户侧客户端构建并下发的上述用于在第二网站的登录域执行自动登录的自动登录链接,可以包括第二网站的自动登录入口的url地址,生成的上述自动登录令牌,以及上述客户端在访问第二网站的目标页面的url地址时,需要向第二网站的自动登录入口的传递的业务查询参数。

[0116] 其中,在示出的一种实施方式中,上述客户端在访问第二网站的目标页面时,需要向第二网站的自动登录入口的传递的业务查询参数中,可以包括该业务请求来源的登陆域名称,第二网站的目标页面的url地址,第二网站的登陆域名称,用户在第一网站登录时所使用的第一登录账户,以及第一网站的服务器生成的上述自动登录令牌和该自动登录令牌的生成时间(用于第二网站的服务器验证自动登录令牌)。

[0117] 上述客户端在接收到第一网站的服务器下发的上述自动登录链接后,可以基于上述自动登录链接中包含的业务查询参数,构建一个针对第二网站的目标url地址的访问请求,然后访问第二网站的自动登录入口的url地址,将构建完成的针对第二网站的目标页面的url地址的访问请求重定向至第二网站的自动登录入口。其中,构建完成的该访问请求中携带的参数,与上述自动登录链接中包含的业务查询参数保持一致。

[0118] 例如,仍然以第一网站为支付宝,第二网站为淘宝,以及用户需要在支付宝客户端中查询一笔由支付宝完成支付的淘宝交易的详情信息为例,假设淘宝的自动登录入口url地址为“http://www.taobao.com/auto_login.htm”,用户要访问的淘宝的目标页面的url地址为“www.taobao.com/trade/list.htm”,支付宝的服务器为支付宝客户端构建并下发的,用于在淘宝的登陆域中执行自动登录的自动登录链接可以为如下链接:

[0119] http://www.taobao.com/auto_login.htm?loginRequestFrom=Alipay&target=http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm&domain=taobao&loginAccount=test_123@alipay.com&token=432085320498320841fjkdsljfdsj&tokentime=201504111104;

[0120] 其中,“loginRequestFrom=Alipay”表示支付宝客户端基于该参数构建的访问请求来源于支付宝的登陆域;“loginAccount=test_123@alipay.com”表示用户登录支付系统所使用的支付宝账户的名称为test_123@alipay.com;“target=http%3A%2F%2Fae.com%2Ftrade%2Flist.htm”即为编码处理后的支付宝客户端访问的淘宝中的目标页面的url地址;“domain=alipay”表示与淘宝系统对接的对端登陆域名称为alipay;“token=432085320498320841fjkdsljfdsj”表示支付宝的服务器生成的上述自动登录令

牌;“tokentime＝201504111104”表示上述自动登录令牌的生成时间。

[0121] 支付宝客户端在接收到支付宝的服务器下发的上述自动登录链接后,可以基于上述自动登录链接中包含的业务查询参数,来构建一个针对淘宝上的目标页面的url地址的访问请求,然后支付宝客户端可以访问淘宝的自动登录入口的url地址,将该访问请求发送至淘宝的服务器。

[0122] 步骤105,第二网站的服务器在接收到来自第一网站的用户侧客户端的针对本地的目标页面的访问请求时,查询与所述用户在所述第一网站上的第一登录账户存在绑定关系的第二登录账户的登录状态;

[0123] 在本例中,用户登录第一网站的上述第一登录账户,与用户登录第二网站的第二登录账户之间可以预先进行账户绑定,该绑定关系可以预先分别存储在第一网站和第二网站的服务器上;

[0124] 例如,以第一网站为支付宝,第二网站为淘宝为例,假设第一登录账户为用户登录支付宝系统的支付宝账户test_123@alipay.com,第二登录账户为用户登录淘宝系统的淘宝账户为test_123@taobao.com,则支付宝和淘宝的服务器上可以分别保存账户test_123@alipay.com和test_123@taobao.com的绑定关系。

[0125] 当第二网站的服务器在接收到第一网站的本地客户端发送的针对本地的目标页面的url地址的访问请求时,可以读取该访问请求中的上述第一登录账户,基于建立的上述绑定关系,查询与该第一登录账户绑定的第二登录账户。当查询到与第一登录账户绑定的第二登录账户时,第二网站的服务器可以在本地查询第二登录账户的登录状态。

[0126] 步骤106,如果所述第二登录账户为未登录状态,第二网站的服务器基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证;

[0127] 在本例中,如果第二网站的服务器查询到上述第二登录账户为未登录状态,则可以读取上述访问请求中携带的自动登录令牌,并基于与第一网站约定的令牌验证规则对该自动登录令牌进行验证。

[0128] 其中,第二网站与第一网站约定的令牌验证规则与第一网站生成自动登录令牌时采用的令牌生成规则互相对应。

[0129] 在本例中,上述令牌验证规则仍然可以作为登陆域配置信息,预先存储在第二网站的登录域配置信息中,上述令牌验证规则可以包括约定的加密算法和密钥,其中作为令牌验证规则的加密算法和密钥需要与第一网站的服务器在生成自动登录令牌时采用的加密算法和密钥保持一致。

[0130] 第二网站的服务器在针对上述自动登录令牌进行验证时,可以从本地的登陆域配置信息中读取加密算法和密钥,并基于读取到的该加密算法和密钥针对该自动登录令牌进行反向解密计算,得到若干参数,然后第二网站的服务器可以验证解密计算得到的该些参数,与第一网站约定的用于生成上述自动登录令牌的令牌生成参数是否一致;

[0131] 例如,假设第一网站的服务器在生成上述自动登录令牌时,使用的令牌生成参数为上述第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间等信息(令牌生成参数可以携带在上述客户端发送的访问请求中),第二网站的服务器在针对该自动登录令牌进行验证时,可以基于相同的算法和密钥对该自动登录令牌进行反向解密得到若干参数,然后第二网站的服务器可以将反向解密计算得到的该些参数,与第一网站的服务器生

成上述自动登录令牌时使用的令牌生成参数一一进行比对，当第一登录账户、第一网站的登录域名称、自动登录令牌的生成时间等信息全部匹配时，则确定该自动登录令牌验证通过。反之，以上参数中的任一参数不匹配时，则可以确定该自动登录令牌验证失败。

[0132] 步骤107，当所述自动登录令牌验证通过时，第二网站的服务器授权所述客户端使用所述第二登录账户在本地执行自动登录，并在登录成功后向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

[0133] 在本例中，如果第二网站的服务器针对上述自动登录令牌验证通过，此时第二网站的服务器可以在本地的登录域中，直接认可上述第一登录账户在第一网站的登陆域中登录成功的鉴权结果。即第二网站的服务器可以通过验证自动登录令牌，来确定是否可以直接将用户在第一网站的登录结果直接在第二网站的登录域中进行共享。

[0134] 在这种情况下，第二网站的服务器可以针对该第二登录账户在第二网站的登陆域中执行登录授权，授权上述客户端使用与上述第一登录账户存在绑定关系的该第二登录账户在第二网站的登陆域中执行自动登录。在整个过程中，第二网站的服务器不需要针对上述第二登录账户执行任何形式的登录验证。

[0135] 当自动登录成功后，此时上述客户端已经取得针对第二网站上的上述目标url地址的访问权限，第二网站的服务器可以向该客户端发送与上述目标url地址对应的页面数据，以触发所述客户端跳转至对应的目标页面

[0136] 当然，如果上述自动登录令牌验证失败，此时第二网站的服务器可以将本地的主动登录入口的url地址下发给上述本地客户端。当该客户端接收到该主动登录入口的url地址时，可以访问该url地址，然后跳转至与该url地址对应的登录页面，然后由用户在该登录页面中手动输入上述第二登录账户，以及对应的登录密码来执行主动登录。

[0137] 步骤108，第一网站的用户侧客户端接收到与所述目标页面的页面数据后，跳转至所述目标页面。

[0138] 在本例中，当第一网站的用户侧客户端接收到由第二网站的服务器发送的与上述目标url地址对应的页面数据后，可以在浏览器中加载接收到的页面数据，然后跳转至与上述目标url地址对应的目标页面。

[0139] 至此，用户通过第一网站的用户侧客户端针对第二网站上的目标页面的访问完成。在整个过程中，当第一网站的用户侧客户端在访问第二网站的目标页面时，只需要验证用户是否使用第一登录账户成功登录了第一网站；如果用户已使用第一登录账户登录了第一网站，则可以通过生成自动登录令牌将用户在第一网站登录成功的鉴权结果共享至第二网站，由第二网站对自动登录令牌验证通过后，使用与第一登录账户绑定的第二登录账户执行自动登录即可，整个登录流程中，不需要对第二登录账户执行任何形式的验证。

[0140] 通过以上实施例可见，当用户通过第一网站的用户客户端，跨网站访问第二网站上的目标页面时，如果用户在第一网站上的第一登录账户在第一网站的登陆域中已完成登录，第一网站的服务器可以基于与第二网站的服务器约定的令牌生成规则生成一个自动登录令牌，并通过将该自动登录令牌发送至第二网站的服务器，将第一登录账户在第一网站的登陆域中登录成功的鉴权结果共享至第二网站。

[0141] 第二网站的服务器可以对该自动登录令牌进行验证，如果验证通过，可以直接授权上述客户端使用与上述第一登录账户存在绑定关系的第二登录账户自动登录第二网站

的登陆域，使得用户通过上述客户端可以直接跳转至与上述目标页面进行访问，而不需要在登录界面中重复输入上述第二登录账户和登录密码重复登录第二网站，由于在整个跳转登录的过程中，不需要针对第二登录账户执行任何形式的验证，因此可以降低操作复杂度，极大的优化用户体验。

[0142] 另外，需要说明的是，以上实施例中描述了用户通过第一网站的用户侧客户端，来跨网站访问第二网站的目标页面的详细过程，在实际应用中，用户也可以通过第二网站的用户侧客户端，来跨网站访问第一网站上的目标页面，其具体的实施过程本申请中不再赘述，本领域技术人员在付诸实现时，可以参考以上实施例中的描述。

[0143] 以下以上述第一网站为支付宝(Alipay)、第二网站为淘宝(Taobao)为例，并结合用户通过支付宝客户端查看淘宝的交易详情信息的应用场景对以上实施例中的技术方案进行详细描述。

[0144] 在本例中示出的场景中，包括承载支付宝客户端的浏览器(以下简称浏览器)、支付宝服务器以及淘宝服务器。

[0145] 在本例中，支付宝可以作为一个第三方支付公司，为淘宝提供在线的支付解决方案。在支付宝的消费记录中，用户通常能查看到所有与支付相关的第三方的交易信息，而支付宝中的交易信息通常只包含交易的摘要信息，比如可能仅包括交易的名称等，因此如果用户需要查看交易的详情信息，则需要跳转到淘宝的网站中进行查询。

[0146] 在相关技术中，用户在通过浏览器跳转到淘宝的网站查询交易的详情信息时，淘宝的系统通常会要求用户输入用户在淘宝中已注册的登录账号和密码执行登录，并在登录成功后才有查看交易详情信息的权限，因此操作非常不方便。

[0147] 在本例中，为了实现用户在支付宝的消费记录查看淘宝交易的详情信息时，浏览器自动跳转至查看交易详情信息的目标页面的功能，在支付宝和淘宝的网站架构中可以集成相同的核心组件。

[0148] 请参见图2，图2为本例示出的一种核心组件架构图。

[0149] 在图2示出的核心组件架构中，包括自动登录流程控制器、Token(自动登录令牌)生成组件、Token验证组件、登录组件以及登陆域的配置信息。

[0150] 其中，上述自动登录流程控制器(Auto Login Service，以下简称ALS)，为自动登陆的总入口，用于负责总控一次自动登陆的所有流程，用户可以通过浏览器访问自动登录入口的url地址，访问自动登录流程控制器，向自动登录流程控制器传递参数，来实现自动登录。

[0151] 上述Token生成组件(Token Generate Service，以下简称TGS组件)，运行于已登录系统一侧，用于基于与对端登录系统约定的Token生成规则生成Token；其中生成token的主要参数可以包括已登陆的账号、对端登陆域名称以及生成token的时间。Token生成规则由网站之间相互约定，可以包括DSA、RSA或者MD5等对称加密算法和密钥。

[0152] 上述Token验证组件(Token Validate Service，以下简称TVS组件)：运行于待登录系统一侧，用于基于约定的Token验证规则验证已登陆系统传递过来的Token，其中验证的方式与Token生成组件生成Token时的生成规则相对应。

[0153] 上述登陆组件(Login Service，以下简称LS组件)：用于检查当前需要登陆的账号是否已经在本系统中完成登陆，以及为需要登陆的账号执行一次自动登陆。

[0154] 上述登陆域的配置信息:负责管理各登陆域的配置信息,包括各登陆域主动登陆入口的url地址、自动登陆入口的url地址、加密算法以及密钥或者密钥的获取方式等信息。

[0155] 在本例中,假设用户登录支付宝的第一登录账户为test_123@alipay.com,用户登录淘宝的第二登录账户为test_123@taobao.com;在淘宝的服务器上可以预先保存登录账户test_123@alipay.com与test_123@taobao.com的绑定关系。

[0156] 在支付宝的消费记录中,包含一笔淘宝的交易的摘要信息,在该摘要信息的预设位置,预先添加了一个“查看交易详情”的标记,该标记指向支付宝的自动登录入口的url地址http://www.alipay.com/auto_login.htm。

[0157] 当用户点击该“查看交易详情”的标记希望跳转至淘宝的交易界面,查询该笔淘宝交易的详情信息时,浏览器会向支付宝的服务器发送一个针对该笔交易详情信息的查询请求。支付宝的服务器收到该查询请求后,基于映射关系,查找到淘宝的交易界面的url地址为www.taobao.com/trade/list.htm后,可以向浏览器下发第一自动登录链接:

[0158] http://www.alipay.com/auto_login.htm?loginRequestFrom=Alipay&target=http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm&domain=taobao&loginAccount=test_123@alipay.com;

[0159] 浏览器接收到该第一自动登录链接后,构建针对淘宝的交易界面的url地址的访问请求,并访问支付宝的自动登录入口的url地址,将该访问请求发送至支付宝服务器的自动登录入口。

[0160] 此时该访问请求中携带的信息包括:该访问请求来源于Alipay、淘宝的交易页面的url地址、淘宝的登陆域名称以及用户需要登录的支付宝账户test_123@alipay.com。

[0161] 支付宝服务器上的ALS组件处理该访问请求,首先发现该访问请求来源于本地的登陆域,此时会触发Token生成,ALS组件调用LS组件查询登录账户test_123@alipay.com的登录状态,如果登录账户test_123@alipay.com为已登录状态,则继续调用TGS组件生成Token。

[0162] 当生成Token后,ALS组件读取淘宝的登陆域的配置信息,为支付宝客户端构建并下发第二自动登录链接,以对支付宝客户端针对淘宝的交易页面的url的访问请求重定向至淘宝的自动登录入口;

[0163] 此时第二自动登录链接为:

[0164] http://www.taobao.com/auto_login.htm?loginRequestFrom=Alipay&target=http%3A%2F%2Ftaobao.com%2Ftrade%2Flist.htm&domain=taobao&loginAccount=test_123@alipay.com&token=432085320498320841fjkdsljfdsj&tokentime=201504111104;

[0165] 浏览器接收到该第二自动登录链接后,重新构建针对淘宝的交易界面的url地址的访问请求,并访问淘宝的自动登录入口的url地址,将重新构建的该访问请求重定向至淘宝的自动登录入口。

[0166] 此时该访问请求中携带的信息包括:该访问请求来源于Alipay、淘宝的交易页面的url地址、支付宝的登陆域名称(重定向后对端登陆域发生了变化)、用户需要登录的支付宝账户test_123@alipay.com、生成的Token以及Token的生成时间。

[0167] 淘宝服务器上的ALS组件处理该访问请求,首先发现该访问请求来源于支付宝的

登陆域，此时会触发Token验证，ALS组件调用LS组件查询与test_123@alipay.com存在绑定关系的登录账户test_123@taobao.com的登录状态，如果登录账户test_123@taobao.com为已登录状态，则继续调用TVS组件验证该Token。

[0168] 当该Token验证通过后，表明淘宝的系统认可用户使用test_123@alipay.com在支付宝的登陆域中登录成功的鉴权结果，此时ALS组件可以调用LS组件为登录账户test_123@taobao.com授权一次自动登录。

[0169] 当登录账户test_123@taobao.com自动登录淘宝的登陆域后，淘宝的服务器可以将与www.taobao.com/trade/list.htm对应的交易页面的页面数据下发至支付宝客户端所在的浏览器。浏览器收到淘宝的服务器下发的页面数据后，可以加载该页面数据，然后自动跳转至淘宝的交易页面，向用户显示该笔淘宝交易的详情信息。

[0170] 至此，用户在支付宝的消费记录中查看该笔淘宝交易的详情信息的操作完成时，在整个过程中，用户不需要在界面中输入淘宝的登陆账户test_123@taobao.com以及登录密码登录淘宝的登陆域，浏览器将自动跳转至淘宝的交易界面向用户输出交易的详情信息。

[0171] 与上述方法实施例相对应，本申请还提供了装置的实施例。

[0172] 请参见图3，本申请提出一种多网站间的自动登录装置30，应用于第一网站的服务器；其中，请参见图4，作为承载所述多网站间的自动登录装置30的服务器所涉及的硬件架构中，通常包括CPU、内存、非易失性存储器、网络接口以及内部总线等；以软件实现为例，所述多网站间的自动登录装置30通常可以理解为加载在内存中的计算机程序，通过CPU运行之后形成的软硬件相结合的逻辑装置，所述装置30包括：

[0173] 第一查询模块301，用于当接收到来自用户侧客户端的针对第二网站上的目标页面的访问请求时，查询用户在所述第一网站上的第一登录账户的登录状态；

[0174] 生成模块302，用于在所述第一登录账户为已登录状态，基于与第二网站约定的令牌生成规则生成自动登录令牌；

[0175] 下发模块303，用于为所述客户端构建并下发第一自动登录链接，所述第一自动登录链接包含所述第二网站的自动登录入口的url地址以及所述自动登录令牌，以使所述客户端访问该第一自动登录链接向第二网站的自动登录入口发送携带所述自动登陆令牌的针对所述目标页面的访问请求，并在所述第二网站的服务器针对所述自动登录令牌验证通过后，授权所述客户端使用与所述第一登录账户存在绑定关系的第二登录账户在第二网站执行自动登录并跳转至所述目标页面。

[0176] 在本例中，所述下发模块303进一步用于：

[0177] 在接收到来自所述用户侧客户端的针对第二网站的资源访问请求时，为所述客户端构建并下发第二自动登录链接，所述第二自动登录链接包含本地自动登录入口的url地址以及所述客户端请求的资源所在的第二网站上的目标页面的url地址，以使所述客户端访问该第二自动登录链接向本地自动登录入口发送所述针对所述目标页面的访问请求。

[0178] 在本例中，所述下发模块303进一步用于：

[0179] 如果所述第一登录账户为未登录状态，向所述客户端下发本地主动登录入口的url地址，以触发所述客户端跳转至与所述本地主动登录入口的url地址对应的登录页面，使用所述第一登录账户完成主动登录。

[0180] 在本例中，所述与第二网站约定的令牌生成规则包括存储在第二网站的登陆域配置信息中的预设加密算法以及密钥；

[0181] 所述生成模块302具体用于：

[0182] 从第二网站的登陆域配置信息中读取预设加密算法以及密钥；

[0183] 基于读取到的所述预设加密算法以及密钥针对与第二网站约定的令牌生成参数进行计算生成作为所述自动登录令牌的随机字符串；

[0184] 其中，所述令牌生成参数包括以下内容中的一个或者多个的组合：

[0185] 所述第一登录账户、第二网站的登录域名称、自动登录令牌的生成时间。

[0186] 请参见图5，本申请提出另一种多网站间的自动登录装置50，应用于第二网站的服务器；其中，请参见图6，作为承载所述多网站间的自动登录装置50的服务器所涉及的硬件架构中，通常包括CPU、内存、非易失性存储器、网络接口以及内部总线等；以软件实现为例，所述多网站间的自动登录装置50通常可以理解为加载在内存中的计算机程序，通过CPU运行之后形成的软硬件相结合的逻辑装置，所述装置50包括：

[0187] 第二查询模块501，用于当接收到来自第一网站的用户侧客户端的针对本地的目标页面的访问请求时，查询与所述用户在所述第一网站上的第一登录账户存在绑定关系的第二登录账户的登录状态；其中，所述访问请求携带所述第一网站的服务器基于约定的令牌生成规则生成的自动登录令牌；

[0188] 验证模块502，用于如果所述第二登录账户为未登录状态，基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证；

[0189] 授权模块503，用于当所述自动登录令牌验证通过时，授权所述客户端使用所述第二登录账户在本地执行自动登录，并在登录成功后向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

[0190] 在本例中，所述授权模块503进一步用于包括：

[0191] 如果所述第二登录账户为已登录状态，向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。

[0192] 在本例中，所述验证模块502进一步用于：

[0193] 当所述自动登录令牌验证失败时，向所述客户端下发本地主动登录入口的url地址，以触发所述客户端跳转至与所述本地主动登录入口的url地址对应的登录页面，使用所述第二登录账户完成主动登录。

[0194] 在本例中，所述与第一网站约定的令牌验证规则为存储在本地登陆域配置信息中的预设解密算法以及密钥；

[0195] 所述验证模块502具体用于：

[0196] 从本地的登陆域配置信息中读取预设解密算法以及密钥；

[0197] 基于读取到的预设解密算法以及密钥针对所述自动登录令牌进行解密，并验证解密后生成的参数是否为与所述第一网站约定的令牌生成参数；如果是，则所述自动登录令牌验证通过；

[0198] 其中，所述令牌生成参数包括以下内容中的一个或者多个的组合：

[0199] 所述第一登录账户、本地登录域名称、自动登录令牌的生成时间。

[0200] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其

它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

[0201] 应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

[0202] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

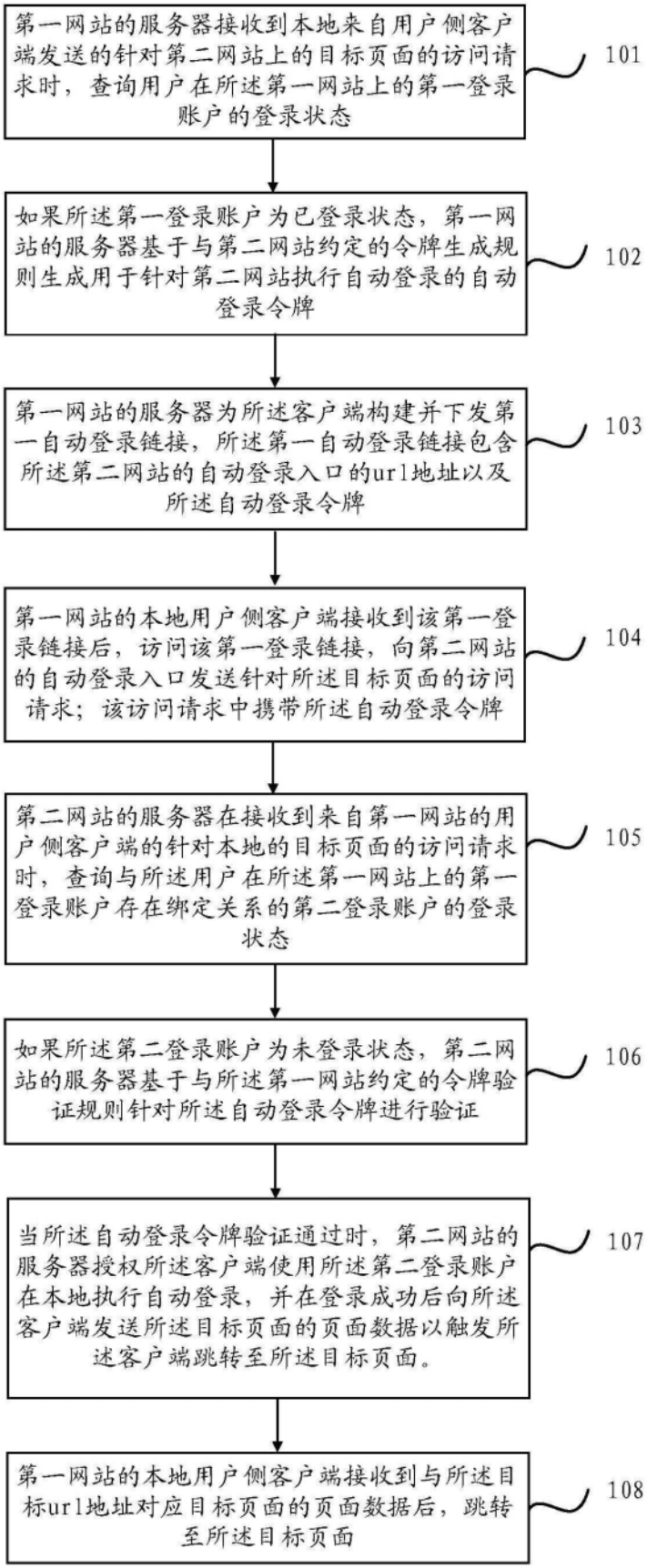

第一网站的服务器接收到本地来自用户侧客户端发送的针对第二网站上的目标页面的访问请求时，查询用户在所述第一网站上的第一登录账户的登录状态
101
如果所述第一登录账户为已登录状态，第一网站的服务器基于与第二网站约定的令牌生成规则生成用于针对第二网站执行自动登录的自动登录令牌
102
第一网站的服务器为所述客户端构建并下发第一自动登录链接，所述第一自动登录链接包含所述第二网站的自动登录入口的url地址以及所述自动登录令牌
103
第一网站的本地用户侧客户端接收到该第一登录链接后，访问该第一登录链接，向第二网站的自动登录入口发送针对所述目标页面的访问请求；该访问请求中携带所述自动登录令牌
104
第二网站的服务器在接收到来自第一网站的用户侧客户端的针对本地的目标页面的访问请求时，查询与所述用户在所述第一网站上的第一登录账户存在绑定关系的第二登录账户的登录状态
105
如果所述第二登录账户为未登录状态，第二网站的服务器基于与所述第一网站约定的令牌验证规则针对所述自动登录令牌进行验证
106
当所述自动登录令牌验证通过时，第二网站的服务器授权所述客户端使用所述第二登录账户在本地执行自动登录，并在登录成功后向所述客户端发送所述目标页面的页面数据以触发所述客户端跳转至所述目标页面。
107
第一网站的本地用户侧客户端接收到与所述目标url地址对应目标页面的页面数据后，跳转至所述目标页面
108

图1

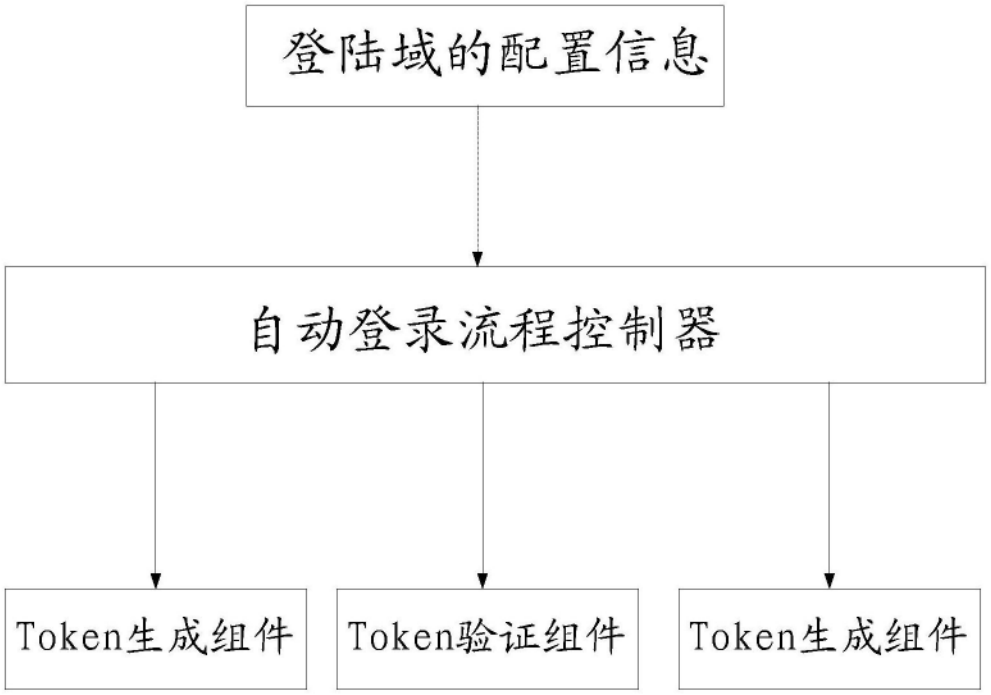

登陆域的配置信息
自动登录流程控制器
Token生成组件
Token验证组件
Token生成组件

图2

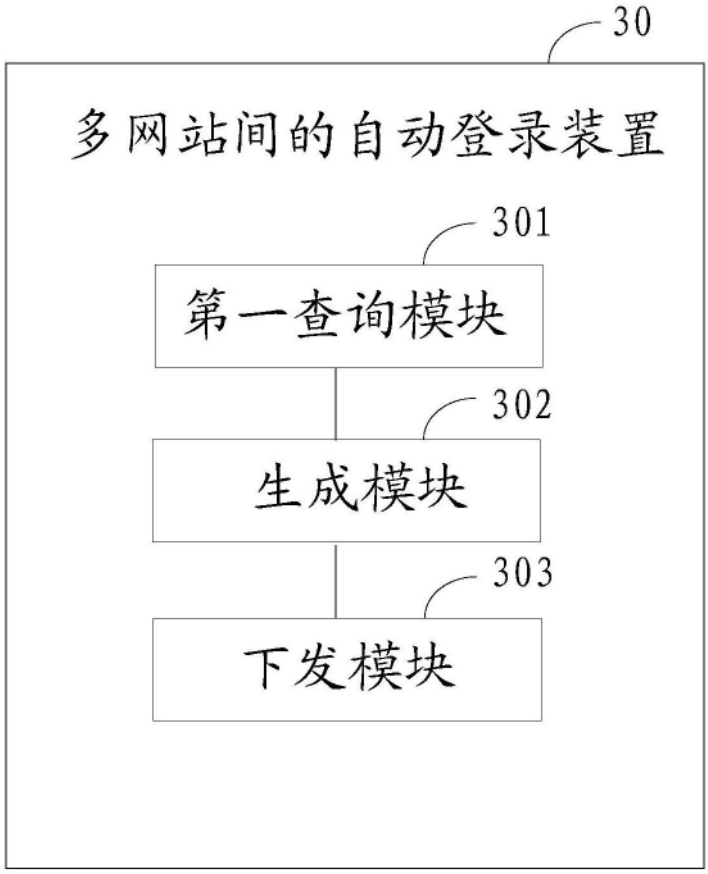

30
多网站间的自动登录装置
301
第一查询模块
302
生成模块
303
下发模块

图3

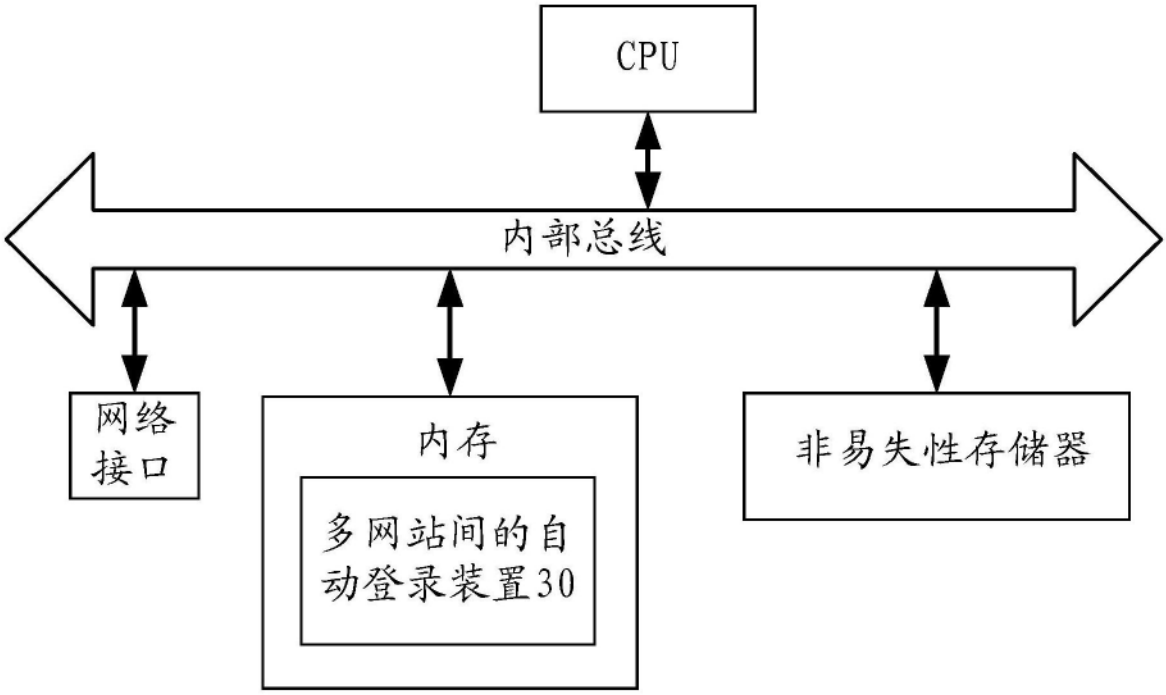

CPU
内部总线
网络接口
内存
多网站间的自动登录装置30
非易失性存储器

图4

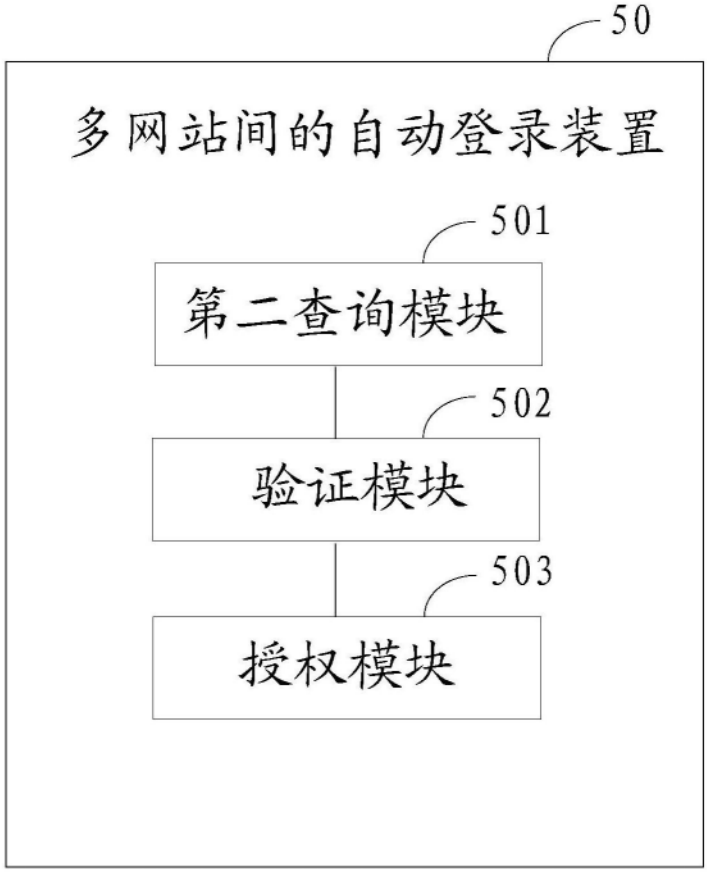

50
多网站间的自动登录装置
501
第二查询模块
502
验证模块
503
授权模块

图5

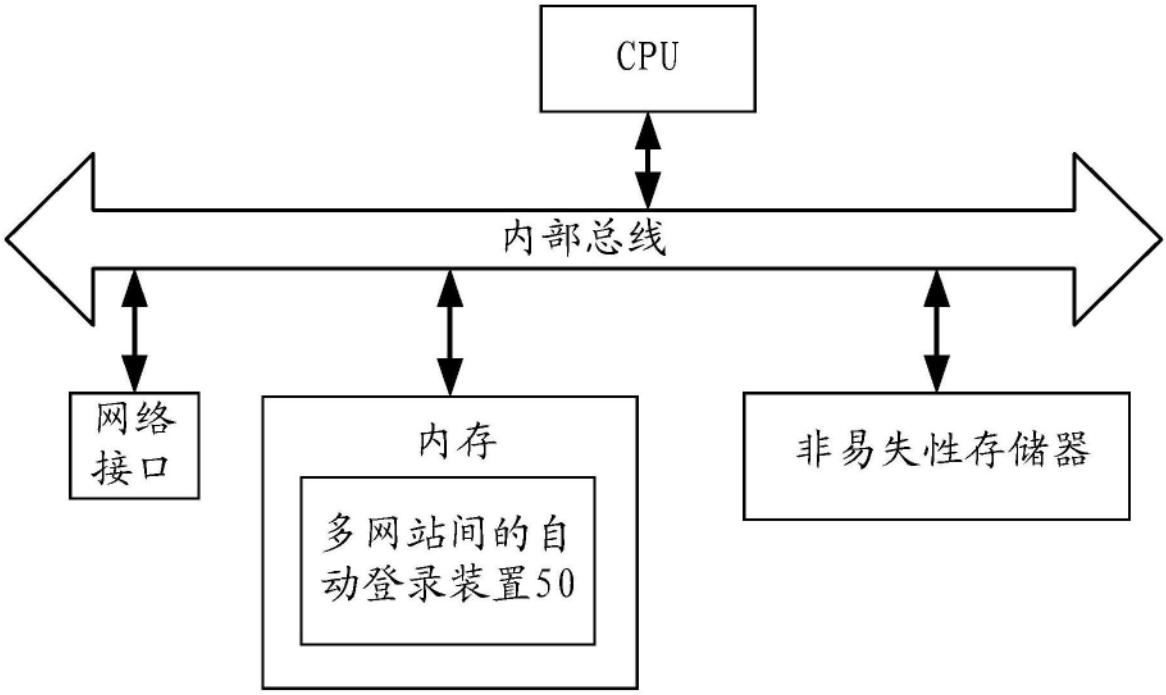


图6