(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105007280 B
(45)授权公告日 2018.06.05

(21)申请号 201510473818.X
(22)申请日 2015.08.05
(65)同一申请的已公布的文献号
申请公布号 CN 105007280 A
(43)申请公布日 2015.10.28
(73)专利权人 郑州悉知信息科技股份有限公司
地址 450000 河南省郑州市高新区科学大道169号1幢1号楼
(72)发明人 王路 刘建辉
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王宝筠
(51)Int.Cl.
H04L 29/06(2006.01)

审查员 李俊华

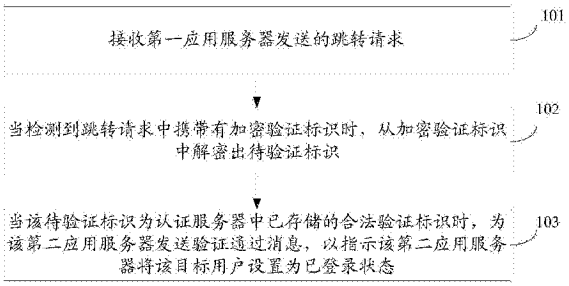
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种应用登录方法和装置

(57)摘要

本申请实施例提供了一种应用登录方法和装置，该方法包括：接收第一应用服务器发送的跳转请求；所述跳转请求用于请求登录至少一个第二应用服务器；当检测到跳转请求中携带有加密验证标识时，从加密验证标识中解密出待验证标识；当待验证标识为认证服务器中已存储的合法验证标识时，为第二应用服务器发送验证通过消息，以指示第二应用服务器将目标用户设置为已登录状态。该方法和装置可以降低单点登录中的数据配置量，降低单点登录的复杂度。



CN 105007280 B

1.一种应用登录方法,其特征在于,包括:

接收第一应用服务器发送的跳转请求,所述跳转请求为所述第一应用服务器中已登录的目标用户通过客户端的浏览器发送给所述第一应用服务器的,所述跳转请求用于请求登录至少一个第二应用服务器;

当检测到所述跳转请求中携带有加密验证标识时,从所述加密验证标识中解密出待验证标识,其中,所述待验证标识为所述浏览器存储的,与所述目标用户对应的标识信息;

当所述待验证标识为认证服务器中已存储的合法验证标识时,为所述第二应用服务器发送验证通过消息,以指示所述第二应用服务器将所述目标用户设置为已登录状态,所述合法验证标识为所述认证服务器对请求登录所述第一应用服务器的用户进行身份认证后,为身份验证通过的用户生成的唯一标识。

2.根据权利要求1所述的方法,其特征在于,在所述接收第一应用服务器发送的跳转请求之前,还包括:

接收所述第一应用服务器发送的登录请求,所述登录请求为所述目标用户通过所述客户端的浏览器发送给所述第一应用服务器的;

响应于所述登录请求,为所述浏览器返回登录页面;

当对所述登录页面中输入的用户名和密码验证通过时,生成身份验证标识,并将身份验证标识存储为合法验证标识;

为所述浏览器返回第一消息,所述第一消息携带有身份验证标识,且所述第一消息用于指示所述浏览器存储所述身份验证标识。

3.根据权利要求1所述的方法,其特征在于,所述合法验证标识包括:cookie数据和/或token令牌。

4.根据权利要求1或3所述的方法,其特征在于,在所述为所述第二应用服务器发送验证通过消息的同时,还包括:

重新生成用于更新的更新验证标识,并用所述更新验证标识替换存储的所述合法验证标识;

向所述浏览器发送第二消息,所述第二消息携带有所述更新验证标识,且所述第二消息用于指示所述浏览器用所述更新验证标识更新所述目标用户的标识信息。

5.根据权利要求1或2所述的方法,其特征在于,还包括:

当所述待验证标识不是所述认证服务器中已存储的合法验证标识时,通过所述第一应用服务器为所述浏览器返回登录页面;

当对所述登录页面中输入的用户名和密码验证通过时,生成身份验证标识并存储;

为所述浏览器返回第一消息,所述第一消息携带有身份验证标识,且所述第一消息用于指示所述浏览器存储所述身份验证标识。

6.一种应用登录装置,其特征在于,包括:

跳转接收单元,用于接收第一应用服务器发送的跳转请求,所述跳转请求为所述第一应用服务器中已登录的目标用户通过客户端的浏览器发送给所述第一应用服务器的;所述跳转请求用于请求登录至少一个第二应用服务器;

验证单元,用于当检测到所述跳转请求中携带有加密验证标识时,从所述加密验证标识中解密出待验证标识,其中,所述待验证标识为所述浏览器存储的,与所述目标用户对应

的标识信息；

通知单元，用于当所述待验证标识为认证服务器中已存储的合法验证标识时，为所述第二应用服务器发送验证通过消息，以指示所述第二应用服务器将所述目标用户设置为已登录状态，所述合法验证标识为所述认证服务器对请求登录所述第一应用服务器的用户进行身份认证后，为身份验证通过的用户生成的唯一标识。

7.根据权利要求6所述的装置，其特征在于，还包括：

登录接收单元，用于在所述跳转接收单元接收到所述跳转请求之前，接收所述第一应用服务器发送的登录请求，所述登录请求为所述目标用户通过所述客户端的浏览器发送给所述第一应用服务器的；

页面返回单元，用于响应于所述登录请求，为所述浏览器返回登录页面；

标识生成单元，用于当对所述登录页面中输入的用户名和密码验证通过时，生成身份验证标识，并将身份验证标识存储为合法验证标识；

第一消息发送单元，用于为所述浏览器返回第一消息，所述第一消息携带有身份验证标识，且所述第一消息用于指示所述浏览器存储所述身份验证标识。

8.根据权利要求6所述的装置，其特征在于，所述合法验证标识包括：cookie数据和/或token令牌。

9.根据权利要求6或8所述的装置，其特征在于，还包括：

标识更新单元，用于在所述通知单元为所述第二应用服务器发送验证通过消息的同时，重新生成用于更新的更新验证标识，并用所述更新验证标识替换存储的所述合法验证标识；

第二消息发送单元，用于向所述浏览器发送第二消息，所述第二消息携带有所述更新验证标识，且所述第二消息用于指示所述浏览器用所述更新验证标识更新所述目标用户的标识信息。

10.根据权利要求6或7所述的装置，其特征在于，还包括：

登录触发单元，用于当所述待验证标识不是所述认证服务器中已存储的合法验证标识时，通过所述第一应用服务器为所述浏览器返回登录页面；

标识生成单元，用于当对所述登录页面中输入的用户名和密码验证通过时，生成身份验证标识并存储；

第一消息发送单元，用于为所述浏览器返回第一消息，所述第一消息携带有身份验证标识，且所述第一消息用于指示所述浏览器存储所述身份验证标识。

一种应用登录方法和装置

技术领域

[0001] 本申请涉及通信技术领域，更具体的说是涉及一种应用登录方法和装置。

背景技术

[0002] 随着网络技术的不断发展，用户能够访问的网站日益增多。而为了获取到不同网站的服务。用户需要通过浏览器登录到不同应用的登录界面进行注册，并通过注册获得的用户名和密码登录到相应应用网站。而随着用户注册行为的增多，用户需要记住大量用户名和密码，并在登录不同应用时输入该应用对应的用户名和密码，从而使得登录应用的过程复杂繁琐。为了提高用户登录应用的便捷性，减少用户需要记住的用户名和密码，现有技术提出了单点登录技术。

[0003] 所谓单点登录就是指通过一定的方式建立不同应用网站之间的关联，当用户在关联的多个网站中的任意一个网站进行登录后，如果用户再访问其他网站则不需要再次验证，就可以直接登录所需访问的该应用。然而现有应用单点登录技术的过程中，需要在关联的每个应用上均进行繁琐的配置，而每增加一个应用，都需要对所有应用均进行繁琐的配置和调试，从而造成了单点登录的复杂度。

发明内容

[0004] 有鉴于此，本申请提供了一种应用登录方法和装置，以降低单点登录的数据配置量，降低单点登录的复杂度。

[0005] 为实现上述目的，本申请提供如下技术方案：一种应用登录方法，包括：

[0006] 接收第一应用服务器发送的跳转请求，所述跳转请求为所述第一应用服务器中已登录的目标用户通过客户端的浏览器发送给所述第一应用服务器的；所述跳转请求用于请求登录至少一个第二应用服务器；

[0007] 当检测到所述跳转请求中携带有加密验证标识时，从所述加密验证标识中解密出待验证标识，其中，所述待验证标识为所述浏览器存储的，与所述目标用户对应的标识信息；

[0008] 当所述待验证标识为认证服务器中已存储的合法验证标识时，为所述第二应用服务器发送验证通过消息，以指示所述第二应用服务器将所述目标用户设置为已登录状态，所述合法验证标识为所述认证服务器对请求登录所述第一应用服务器的用户进行身份认证后，为身份验证通过的用户生成的唯一标识。

[0009] 优选的，在所述接收第一应用服务器发送的跳转请求之前，还包括：

[0010] 接收所述第一应用服务器发送的登录请求，所述登录请求为所述目标用户通过所述客户端的浏览器发送给所述第一应用服务器的；

[0011] 响应于所述登录请求，为所述浏览器返回登录页面；

[0012] 当对所述登录页面中输入的用户名和密码验证通过时，生成身份验证标识，并将身份验证标识存储为合法验证标识；

[0013] 为所述浏览器返回第一消息，所述第一消息携带有身份验证标识，且所述第一消息用于指示所述浏览器存储所述身份验证标识。

[0014] 优选的，所述合法验证标识包括：cookie数据和/或token令牌。

[0015] 优选的，在所述为所述第二应用服务器发送验证通过消息的同时，还包括：

[0016] 重新生成用于更新的更新验证标识，并用所述更新验证标识替换存储的所述合法验证标识；

[0017] 向所述浏览器发送第二消息，所述第二消息携带有所述更新验证标识，且所述第二消息用于指示所述浏览器用所述更新验证标识更新所述目标用户的标识信息。

[0018] 优选的，还包括：

[0019] 当所述待验证标识不是所述认证服务器中已存储的合法验证标识时，通过所述第一应用服务器为所述浏览器返回登录页面；

[0020] 当对所述登录页面中输入的用户名和密码验证通过时，生成身份验证标识并存储；

[0021] 为所述浏览器返回第一消息，所述第一消息携带有身份验证标识，且所述第一消息用于指示所述浏览器存储所述身份验证标识。

[0022] 另一方面，本申请还提供了一种应用登录装置，包括：

[0023] 跳转接收单元，用于接收第一应用服务器发送的跳转请求，所述跳转请求为所述第一应用服务器中已登录的目标用户通过客户端的浏览器发送给所述第一应用服务器的；所述跳转请求用于请求登录至少一个第二应用服务器；

[0024] 验证单元，用于当检测到所述跳转请求中携带有加密验证标识时，从所述加密验证标识中解密出待验证标识，其中，所述待验证标识为所述浏览器存储的，与所述目标用户对应的标识信息；

[0025] 通知单元，用于当所述待验证标识为认证服务器中已存储的合法验证标识时，为所述第二应用服务器发送验证通过消息，以指示所述第二应用服务器将所述目标用户设置为已登录状态，所述合法验证标识为所述认证服务器对请求登录所述第一应用服务器的用户进行身份认证后，为身份验证通过的用户生成的唯一标识。

[0026] 优选的，还包括：

[0027] 登录接收单元，用于在所述跳转接收单元接收到所述跳转请求之前，接收所述第一应用服务器发送的登录请求，所述登录请求为所述目标用户通过所述客户端的浏览器发送给所述第一应用服务器的；

[0028] 页面返回单元，用于响应于所述登录请求，为所述浏览器返回登录页面；

[0029] 标识生成单元，用于当对所述登录页面中输入的用户名和密码验证通过时，生成身份验证标识，并将身份验证标识存储为合法验证标识；

[0030] 第一消息发送单元，用于为所述浏览器返回第一消息，所述第一消息携带有身份验证标识，且所述第一消息用于指示所述浏览器存储所述身份验证标识。

[0031] 优选的，所述合法验证标识包括：cookie数据和/或token令牌。

[0032] 优选的，还包括：

[0033] 标识更新单元，用于在所述通知单元为所述第二应用服务器发送验证通过消息的同时，重新生成用于更新的更新验证标识，并用所述更新验证标识替换存储的所述合法验

证标识；

[0034] 第二消息发送单元，用于向所述浏览器发送第二消息，所述第二消息携带有所述更新验证标识，且所述第二消息用于指示所述浏览器用所述更新验证标识更新所述目标用户的标识信息。

[0035] 优选的，还包括：

[0036] 登录触发单元，用于当所述待验证标识不是所述认证服务器中已存储的合法验证标识时，通过所述第一应用服务器为所述浏览器返回登录页面；

[0037] 标识生成单元，用于当对所述登录页面中输入的用户名和密码验证通过时，生成身份验证标识并存储；

[0038] 第一消息发送单元，用于为所述浏览器返回第一消息，所述第一消息携带有身份验证标识，且所述第一消息用于指示所述浏览器存储所述身份验证标识。

[0039] 经由上述的技术方案可知，在本实施例中浏览器发出的跳转请求由认证服务器来处理，且认证服务器中会存储验证用户身份的验证标识，从而实现了在认证服务器侧配置一套验证系统就可以完整对所有跳转请求的身份验证，避免了在应用的服务器或者客户端上进行复杂的配置，提高了单点登录的便捷性。

附图说明

[0040] 为了更清楚地说明本申请实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0041] 图1示出了本申请一种应用登录方法一个实施例的流程示意图；

[0042] 图2示出了本申请一种应用登录方法另一个实施例的流程示意图；

[0043] 图3示出了本申请一种应用登录装置一个实施例的结构示意图。

具体实施方式

[0044] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0045] 首先对本申请的一种应用登录方法进行介绍。

[0046] 参见图1，其示出了本申请一种应用登录方法一个实施例的流程示意图，本实施例的方法应用于单点登录系统的认证服务器。本实施例的方法可以包括：

[0047] 101，接收第一应用服务器发送的跳转请求。

[0048] 其中，该跳转请求为第一应用服务器中已登录的目标用户通过客户端的浏览器发送给该第一应用服务器的；该跳转请求用于请求登录至少一个第二应用服务器。

[0049] 在本申请实施例中，已登录该第一应用服务器的目标用户如果希望登录与该第一应用服务器对应的第一应用相关联的第二应用时，则该目标用户通过浏览器发出跳转请求后，该第一应用服务器并不会处理该跳转请求，而是将该跳转请求转发给认证服务器，以便

由认证服务器来统一处理所有关联的应用接收到的跳转请求。

[0050] 102，当检测到跳转请求中携带有加密验证标识时，从加密验证标识中解密出待验证标识。

[0051] 其中，该待验证标识为浏览器存储的，与该目标用户对应的标识信息。

[0052] 103，当该待验证标识为认证服务器中已存储的合法验证标识时，为该第二应用服务器发送验证通过消息，以指示该第二应用服务器将该目标用户设置为已登录状态。

[0053] 其中，合法验证标识为该认证服务器对请求登录该第一应用服务器的用户进行身份认证后，为身份验证通过的用户生成的唯一标识。

[0054] 在本申请实施例中，该认证服务器负责对用户登录应用，已登录用户请求跳转到其他应用的所有请求进行处理。

[0055] 其中，用户通过浏览器向应用服务器发出登录请求后，应用服务器会将登录请求自动发送到该认证服务器，并由认证服务器为该浏览器返回登录页面，同时，认证服务器对登录页面输入的用户名和密码验证通过后，可以为该用户生成唯一的合法验证标识并转发给浏览器，后续该用户通过浏览器请求跳转到其他应用时，浏览器会携带该认证服务器为该用户分配的合法验证标识，以便认证服务器验证该用户是否为已登录的合法用户。因此，如果该目标用户已登录该认证服务器，则该浏览器中会存储有该目标用户对应的验证标识，且该验证标识应是该认证服务器中存储的合法验证标识。

[0056] 如果浏览器发送的跳转请求中所携带的待验证标识为该认证服务器中存储的合法验证标识，则对该已登录的目标用户的身份验证通过，从而向该跳转请求所请求登录的第二应用服务器发送验证通过消息，从而使得第二应用服务器将该目标用户设置为已登录用户，实现该目标用户直接登录该第二应用服务器的目的。

[0057] 在本申请实施例中已登录第一应用服务器的目标用户通过浏览器发送跳转请求后，第一应用服务器会将该跳转请求自动转发到认证服务器。认证服务器会在验证该跳转请求中携带有验证标识，且该验证标识为该认证服务器生成的验证标识后，确定该目标用户为具备合法访问权限的用户，并通知该跳转请求所请求的第二应用服务器设置该目标用户为已登录用户。可见，在本实施例中浏览器发出的跳转请求由认证服务器来处理，且认证服务器中会存储验证用户身份的验证标识，从而实现了在认证服务器侧配置一套验证系统就可以完整对所有跳转请求的身份验证，避免了在应用的服务器或者客户端上进行复杂的配置，提高了单点登录的便捷性。

[0058] 需要说明的是，在本申请实施例中该认证服务器可以为现有的任意形式的认证服务器，如该可以为CAS(Central Authentication Service)中央验证服务器。

[0059] 而认证服务器存储该合法验证标识可以是存储到服务器任意固定存储单元中，也可以是存储于数据库中，可选的，该认证服务器可以将合法验证标识存储于redis数据库中。

[0060] 可以理解的是，在该认证服务器中还可以存储不同应用之间的关联关系，这样，当确定该待验证标识为认证服务器中已存储的合法验证标识后，该认证服务器还可以查询该跳转请求所请求登录的第二应用服务器与该第一应用服务器之间是否建立有预设的关联关系，如果建立有该关联关系，则为该第二应用服务器发送验证通过消息，以指示第二应用服务器将该目标用户设置为已登录状态。

[0061] 参见图2，其示出了本申请一种应用登录方法另一个实施例的流程示意图，本实施例的方法可以包括：

[0062] 201，接收第一应用服务器发送的登录请求。

[0063] 其中，该登录请求为该目标用户通过所述客户端的浏览器发送给该第一应用服务器的。

[0064] 当第一应用服务器检测到用户通过客户端的浏览器发出登录请求时，会链接认证服务器，以便认证服务器向该浏览器返回登录页面。

[0065] 202，响应于该登录请求，为该浏览器返回登录页面。

[0066] 203，当对该登录页面中输入的用户名和密码验证通过时，生成身份验证标识并存储。

[0067] 当该目标用户向认证服务器返回的登录页面中输入用户名和密码后，认证服务器会对用户名和密码进行验证，并在验证通过后，为该目标用户生成一身份验证标识。其中，认证服务器中可以存储不同应用所涉及到的用户的用户名和密码，并通过验证该用户名和密码是否匹配，来验证该用户是否具备登录该应用的权限。

[0068] 其中，认证服务器为该目标用户生成身份验证标识后，可以将该身份验证标识作为合法验证标识进行存储。

[0069] 可以理解的是，当登录页面中输入的用户名和密码验证通过后，实际上该认证服务器会通知该第一应用服务器，以便第一应用服务器将该用户设置为登录状态。同时，对用户名和密码验证通过后，该认证服务器存储该身份验证标识，则认为该目标用户已登录该认证服务器。

[0070] 204，为该浏览器返回第一消息。

[0071] 其中，该第一消息携带有身份验证标识，且该第一消息用于指示该浏览器存储所述身份验证标识。

[0072] 浏览器接收到该身份验证标识后，会在客户端本地存储该身份验证标识，以便后续需要链接其他应用时，将该身份验证标识发送给认证服务器进行认证。

[0073] 在本申请实施例中。对用户来说，整个身份验证是透明的，除了看到登录请求调到中央验证服务器，无任何变化，用户体验好。

[0074] 205，接收第一应用服务器发送的跳转请求。

[0075] 其中，该跳转请求为第一应用服务器中已登录的目标用户通过客户端的浏览器发送给该第一应用服务器的；该跳转请求用于请求登录至少一个第二应用服务器。

[0076] 在该目标用户登录了认证服务器之后，如果该目标用户需要跳转到第二应用，则可以通过浏览器向第一应用服务器发送跳转请求，并携带登录认证服务器时由该认证服务器返回的身份验证标识。

[0077] 需要说明的是，在实际应用中用户发送的跳转请求可以是一个统一资源定位符(URL，Uniform Resoure Locator)请求。在该URL请求中可以携带身份验证标识。

[0078] 206，当检测到跳转请求中携带有加密验证标识时，从加密验证标识中解密出待验证标识。

[0079] 其中，该待验证标识为浏览器存储的，与该目标用户对应的标识信息；

[0080] 207，当该待验证标识为认证服务器中已存储的合法验证标识时，为该第二应用服

务器发送验证通过消息，以指示该第二应用服务器将该目标用户设置为已登录状态。

[0081] 需要说明的是，该步骤205至步骤207为该目标用户通过认证服务器的验证，登录该第一应用服务器和该认证服务器之后，在该目标用户希望访问该第一应用服务器之外的其他应用的情况下，用户通过浏览器发出跳转请求后，该认证服务器侧的操作。由于该步骤205至步骤207的操作与前面实施例的相关内容相似，所以相似之处可以参见前面实施例的相关介绍。

[0082] 需要说明的是，在本申请实施例中该认证服务器侧存储的验证标识可以是根据该目标用户的用户名和密码生成。而验证标识也可以有多种形式，如，验证标识可以为cookie数据，或者是token令牌，其中，该token令牌的使用周期仅有一次。当然，该验证标识也可以同时包括该cookie数据和token令牌。

[0083] 浏览器接收到该cookie数据或者是token令牌等标识信息后，可以将这些标识信息存储在该客户端本地的cookies文件夹中。当然，浏览器发送的跳转请求中除了包含这些标识信息外，还可以包括HTTP的header头信息。

[0084] 为了提高身份标识信息的安全性，认证服务器可以对该目标用户的身份验证信息进行更新，可选的，可以设置该身份验证标识的单次有效性，则每次该目标用户通过浏览器向该认证服务器发送跳转请求后，则更新该目标用户的身份验证标识。

[0085] 具体的，在验证了该待验证身份标识为该认证服务器存储的合法身份验证标识后，可以重新生成用于更新的更新验证标识，并用该更新验证标识替换存储的合法验证标识。然后，向浏览器发送第二消息，改第二消息携带有所述更新验证标识，且第二消息用于指示该浏览器利用该更新验证标识更新该目标用户的标识信息。

[0086] 可以理解的是，在以上任意一个实施例中，当该待验证标识不是所述认证服务器中已存储的合法验证标识时，则说明该目标用户尚未登录该认证服务器，则可以通过所述第一应用服务器为所述浏览器返回登录页面；同时，当对登录页面中输入的用户名和密码验证通过时，生成身份验证标识并存储；为该浏览器返回第一消息。其中，该第一消息携带有身份验证标识，且第一消息用于指示该浏览器存储该身份验证标识。

[0087] 对应本申请的一种应用登录方法，本申请实施例还提供了一种应用登录装置。

[0088] 参见图3，其示出了本申请一种应用登录装置一个实施例的结构示意图，本实施例的装置可以应用于单点登录系统中的认证服务器，本实施例的装置可以包括：

[0089] 跳转接收单元301，用于接收第一应用服务器发送的跳转请求，所述跳转请求为所述第一应用服务器中已登录的目标用户通过客户端的浏览器发送给所述第一应用服务器的；所述跳转请求用于请求登录至少一个第二应用服务器；

[0090] 验证单元302，用于当检测到所述跳转请求中携带有加密验证标识时，从所述加密验证标识中解密出待验证标识，其中，所述待验证标识为所述浏览器存储的，与所述目标用户对应的标识信息；

[0091] 通知单元303，用于当所述待验证标识为认证服务器中已存储的合法验证标识时，为所述第二应用服务器发送验证通过消息，以指示所述第二应用服务器将所述目标用户设置为已登录状态，所述合法验证标识为所述认证服务器对请求登录所述第一应用服务器的用户进行身份认证后，为身份验证通过的用户生成的唯一标识。

[0092] 在本申请实施例中已登录第一应用服务器的目标用户通过浏览器发送跳转请求

后，第一应用服务器会将该跳转请求自动转发到认证服务器。认证服务器会在验证该跳转请求中携带有验证标识，且该验证标识为该认证服务器生成的验证标识后，确定该目标用户为具备合法访问权限的用户，并通知该跳转请求所请求的第二应用服务器设置该目标用户为已登录用户。可见，在本实施例中浏览器发出的跳转请求由认证服务器来处理，且认证服务器中会存储验证用户身份的验证标识，从而实现了在认证服务器侧配置一套验证系统就可以完整对所有跳转请求的身份验证，避免了在应用的服务器或者客户端上进行复杂的配置，提高了单点登录的便捷性。

[0093] 可选的，该装置还包括：

[0094] 登录接收单元，用于在所述跳转接收单元接收到所述跳转请求之前，接收所述第一应用服务器发送的登录请求，所述登录请求为所述目标用户通过所述客户端的浏览器发送给所述第一应用服务器的；

[0095] 页面返回单元，用于响应于所述登录请求，为所述浏览器返回登录页面；

[0096] 标识生成单元，用于当对所述登录页面中输入的用户名和密码验证通过时，生成身份验证标识，并将身份验证标识存储为合法验证标识；

[0097] 第一消息发送单元，用于为所述浏览器返回第一消息，所述第一消息携带有身份验证标识，且所述第一消息用于指示所述浏览器存储所述身份验证标识。

[0098] 可选的，在以上任意一个装置的实施例中，合法验证标识包括：cookie数据和/或token令牌。

[0099] 可选的，在以上任意一个装置的实施例中，该装置还可以包括：

[0100] 标识更新单元，用于在所述通知单元为所述第二应用服务器发送验证通过消息的同时，重新生成用于更新的更新验证标识，并用所述更新验证标识替换存储的所述合法验证标识；

[0101] 第二消息发送单元，用于向所述浏览器发送第二消息，所述第二消息携带有所述更新验证标识，且所述第二消息用于指示所述浏览器用所述更新验证标识更新所述目标用户的标识信息。

[0102] 可选的，在以上任意一个装置的实施例中，该装置还可以包括：

[0103] 登录触发单元，用于当所述待验证标识不是所述认证服务器中已存储的合法验证标识时，通过所述第一应用服务器为所述浏览器返回登录页面；

[0104] 标识生成单元，用于当对所述登录页面中输入的用户名和密码验证通过时，生成身份验证标识并存储；

[0105] 第一消息发送单元，用于为所述浏览器返回第一消息，所述第一消息携带有身份验证标识，且所述第一消息用于指示所述浏览器存储所述身份验证标识。

[0106] 本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的装置而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。

[0107] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请

将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

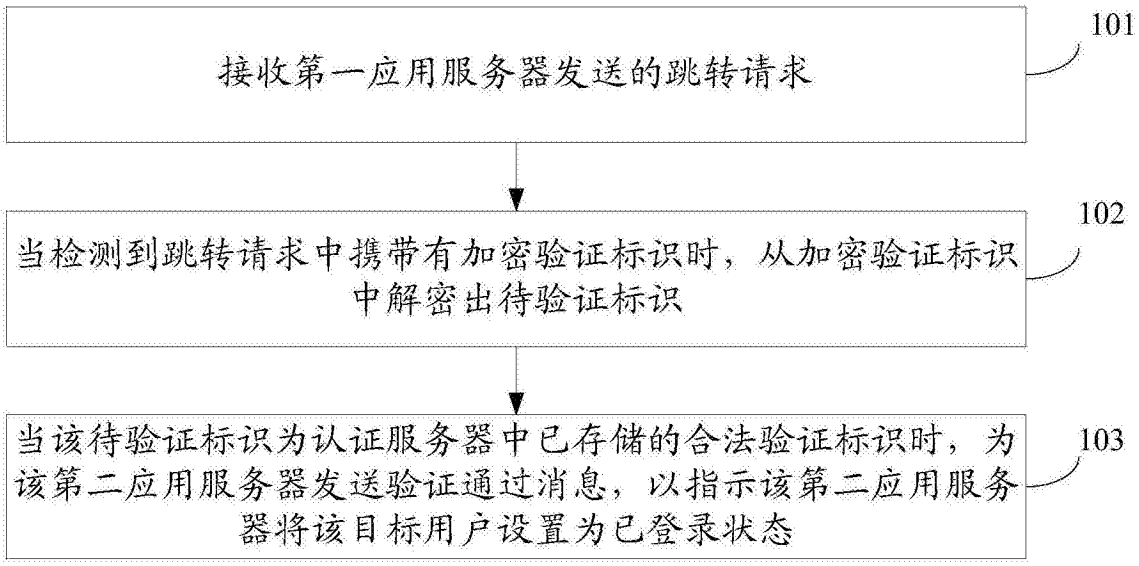

接收第一应用服务器发送的跳转请求
101
当检测到跳转请求中携带有加密验证标识时，从加密验证标识中解密出待验证标识
102
当该待验证标识为认证服务器中已存储的合法验证标识时，为该第二应用服务器发送验证通过消息，以指示该第二应用服务器将该目标用户设置为已登录状态
103

图1

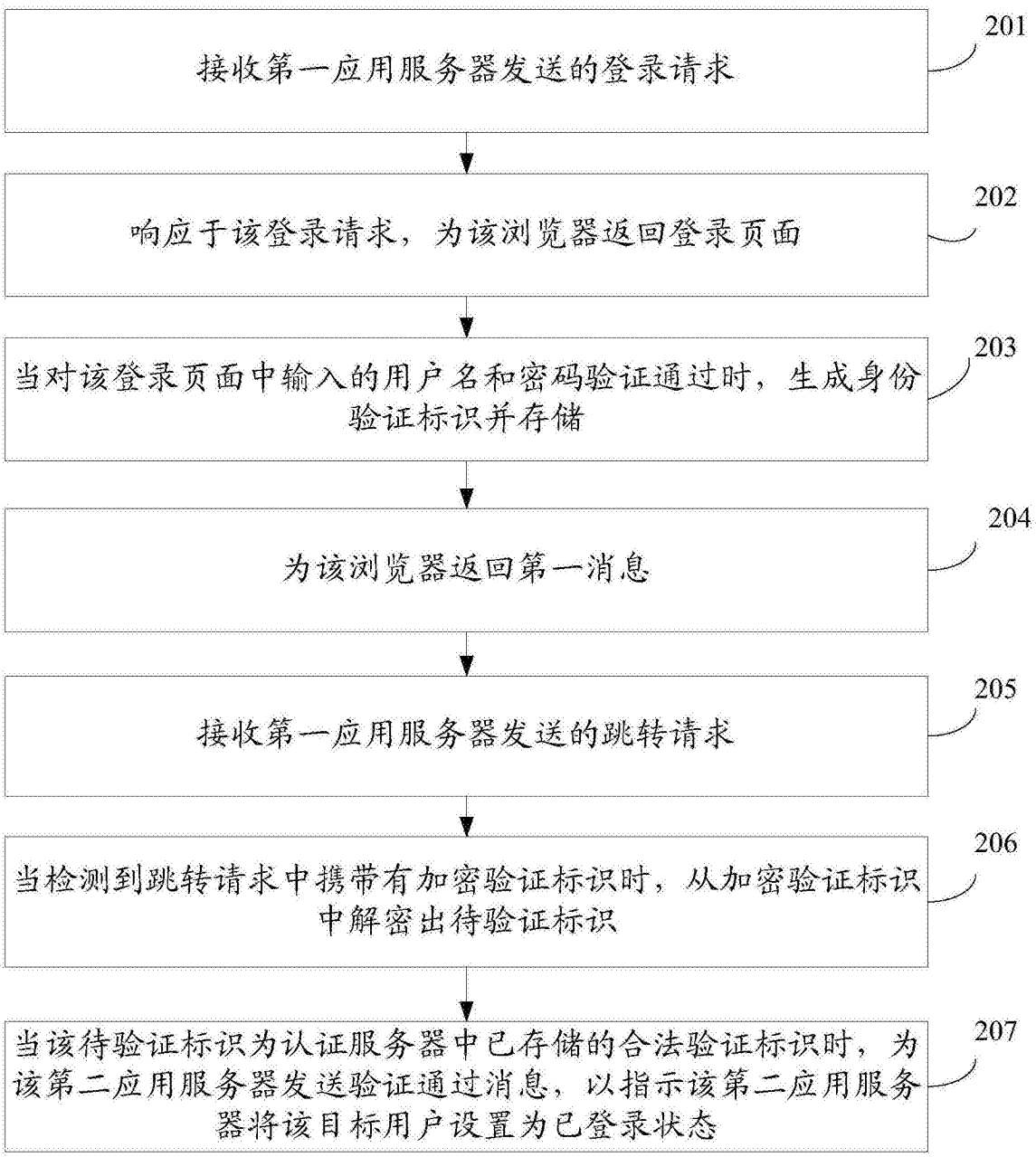

接收第一应用服务器发送的登录请求
201
响应于该登录请求，为该浏览器返回登录页面
202
当对该登录页面中输入的用户名和密码验证通过时，生成身份验证标识并存储
203
为该浏览器返回第一消息
204
接收第一应用服务器发送的跳转请求
205
当检测到跳转请求中携带有加密验证标识时，从加密验证标识中解密出待验证标识
206
当该待验证标识为认证服务器中已存储的合法验证标识时，为该第二应用服务器发送验证通过消息，以指示该第二应用服务器将该目标用户设置为已登录状态
207

图2

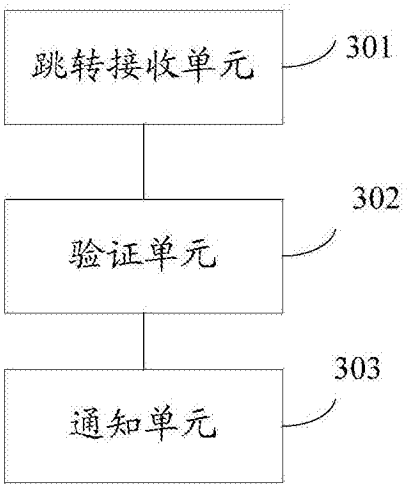


图3