(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112738005 A
(43)申请公布日 2021.04.30

(21)申请号 201910974829.4

(22)申请日 2019.10.14

(71)申请人 中移(苏州)软件技术有限公司
地址 215163 江苏省苏州市高新区昆仑山路58号1幢
申请人 中国移动通信集团有限公司

(72)发明人 常润东 黄晓娟

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 李昂 张颖玲

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 29/08(2006.01)

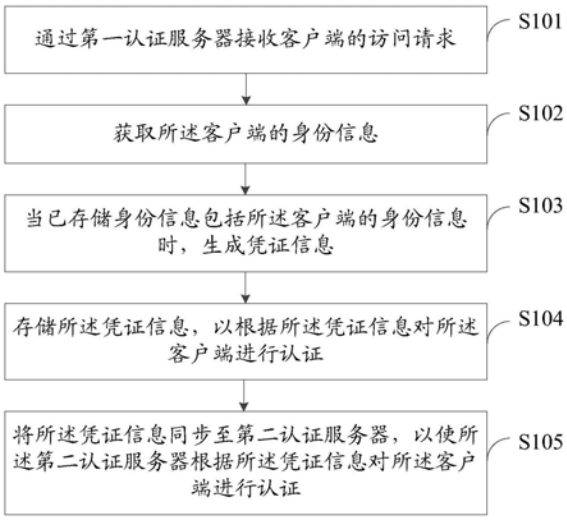
权利要求书2页 说明书12页 附图6页

(54)发明名称

访问处理方法、装置、系统、第一认证服务器及存储介质

(57)摘要

本发明提供了访问处理方法、装置、系统、第一认证服务器及计算机可读存储介质，其中所述访问处理方法包括：通过第一认证服务器接收客户端的访问请求；获取所述客户端的身份信息；当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。本发明提升了访问处理的兼容性和扩展性，适用于接入不同独立的应用系统服务器的公有云平台。



CN 112738005 A

1.一种访问处理方法,其特征在于,包括:

通过第一认证服务器接收客户端的访问请求;

获取所述客户端的身份信息;

当已存储身份信息包括所述客户端的身份信息时,生成凭证信息;

存储所述凭证信息,以根据所述凭证信息对所述客户端进行认证;

将所述凭证信息同步至第二认证服务器,以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

2.如权利要求1所述的访问处理方法,其特征在于,所述生成凭证信息,包括:

确定所述第一认证服务器存储的至少一个白名单地址,所述白名单地址对应所述第一认证服务器信任的第二认证服务器;

根据所述白名单地址生成凭证信息,所述凭证信息用于被同步至所述白名单地址对应的第二认证服务器。

3.如权利要求2所述的访问处理方法,其特征在于,还包括:

接收同步的凭证信息;

当所述凭证信息内的白名单地址与所述第一认证服务器的地址相同时,存储所述凭证信息;

当所述凭证信息内的白名单地址与所述第一认证服务器的地址不同时,丢弃所述凭证信息。

4.如权利要求2所述的访问处理方法,其特征在于,所述根据所述白名单地址生成凭证信息,包括:

对所述客户端的身份信息进行加密生成加密身份信息;

根据所述加密身份信息和所述白名单地址生成凭证信息。

5.如权利要求4所述的访问处理方法,其特征在于,所述对所述客户端的身份信息进行加密生成加密身份信息之后,还包括:

根据所述加密身份信息和所有所述白名单地址生成票据信息,将所述票据信息发送到所述客户端,以使所述客户端发起包括所述票据信息的访问请求进行认证。

6.如权利要求5所述的访问处理方法,其特征在于,还包括:

接收所述客户端的票据信息;

当所述票据信息与所述凭证信息中的加密身份信息相同,且所述票据信息包括所述凭证信息中的白名单地址时,确定所述客户端认证成功;

当所述票据信息与所述凭证信息中的加密身份信息不同,和/或所述票据信息未包括所述凭证信息中的白名单地址时,确定所述客户端认证失败。

7.如权利要求1至6任一项所述的访问处理方法,其特征在于,所述通过第一认证服务器接收客户端的访问请求,包括:

通过第一认证服务器接收重定向的访问请求,所述访问请求由所述第一认证服务器对应的应用系统服务器拦截并进行重定向。

8.如权利要求7所述的访问处理方法,其特征在于,还包括:

当所述已存储身份信息包括所述客户端的身份信息时,生成票据信息,将所述票据信息发送到所述客户端;

将所述票据信息添加至所述访问请求，并将所述访问请求重定向至所述应用系统服务器。

9.一种访问处理装置，其特征在于，包括：

接收单元，用于通过第一认证服务器接收客户端的访问请求；

获取单元，用于获取所述客户端的身份信息；

生成单元，用于当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；

存储单元，用于存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；

同步单元，用于将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

10.一种访问处理系统，包括客户端、第一认证服务器及第二认证服务器，所述第一认证服务器执行如权利要求1至8任一项所述访问处理方法。

11.一种第一认证服务器，其特征在于，所述第一认证服务器包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如权利要求1至8任一项所述访问处理方法。

12.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至8任一项所述访问处理方法。

访问处理方法、装置、系统、第一认证服务器及存储介质

技术领域

[0001] 本发明属于计算机技术领域，尤其涉及访问处理方法、装置、系统、第一认证服务器及计算机可读存储介质。

背景技术

[0002] 随着云计算技术的不断发展，云平台提供的服务越来越丰富。公有云平台除了自身的分布式架构，还要接入各种独立的外部应用系统服务器，如web系统服务器。由于不同的应用系统服务器之间相互独立，故通常要求客户端在使用每个应用系统服务器之前进行身份认证，在登录成功后才可使用应用系统服务器提供的服务，导致客户端的用户需要记住每一个应用系统服务器的认证方式，不便于使用，同时也加大了云平台进行用户管理的复杂度。

[0003] 针对该情况，目前提出了单点登录方式，即对各个应用系统服务器部署统一的认证服务器，由该认证服务器保存各应用系统服务器的身份信息，对客户端进行身份认证，并在认证成功后存储凭证信息，从而在客户端下次访问时根据凭证信息进行快速认证。但是，上述方式要求各个应用系统服务器的身份信息，如用户名和密码等，都必须符合统一标准和统一格式，在云平台接入认证方式不一致的应用系统服务器时，需要对身份认证服务以及对应的存储身份信息的数据库结构进行大量改造，兼容性和扩展性差。

发明内容

[0004] 本发明实施提供了一种访问处理方法、装置、系统、第一认证服务器及计算机可读存储介质，能够提升访问处理的兼容性和扩展性，适用于接入不同应用系统服务器的云平台。

[0005] 本发明实施例的技术方案是这样实现的：

[0006] 本发明实施例提供了一种访问处理方法，包括：

[0007] 通过第一认证服务器接收客户端的访问请求；

[0008] 获取所述客户端的身份信息；

[0009] 当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；

[0010] 存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；

[0011] 将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

[0012] 本发明实施例提供了一种访问处理装置，包括：

[0013] 接收单元，用于通过第一认证服务器接收客户端的访问请求；

[0014] 获取单元，用于获取所述客户端的身份信息；

[0015] 生成单元，用于当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；

[0016] 存储单元，用于存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；

[0017] 同步单元，用于将所述凭证信息同步至第二认证服务器，以使所述第二认证服务

器根据所述凭证信息对所述客户端进行认证。

[0018] 本发明实施例提供了一种第一认证服务器，所述第一认证服务器包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现：

[0019] 通过第一认证服务器接收客户端的访问请求；

[0020] 获取所述客户端的身份信息；

[0021] 当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；

[0022] 存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；

[0023] 将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

[0024] 本发明实施例提供了一种访问处理系统，包括客户端、第一认证服务器及第二认证服务器，所述第一认证服务器执行：

[0025] 通过第一认证服务器接收客户端的访问请求；

[0026] 获取所述客户端的身份信息；

[0027] 当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；

[0028] 存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；

[0029] 将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

[0030] 本发明实施例提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现：

[0031] 通过第一认证服务器接收客户端的访问请求；

[0032] 获取所述客户端的身份信息；

[0033] 当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；

[0034] 存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；

[0035] 将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

[0036] 本发明实施例的有益效果是：

[0037] 本发明实施例通过第一认证服务器对客户端进行认证，在认证成功时生成并存储凭证信息，以根据凭证信息对客户端进行认证，除此之外，将凭证信息同步至第二认证服务器，以使第二认证服务器根据凭证信息对客户端进行认证，本发明实施例通过同步凭证信息，提升了访问处理的兼容性和扩展性，适用于接入不同独立的应用系统服务器的云平台。

附图说明

[0038] 图1是本发明实施例提供的访问处理方法的实现流程图；

[0039] 图2是本发明实施例提供的访问处理方法的一种架构图；

[0040] 图3是本发明实施例提供的访问处理方法的另一种架构图；

[0041] 图4是本发明实施例提供的生成凭证信息的实现流程图；

[0042] 图5是本发明实施例提供的对接收到的凭证信息进行处理的实现流程图；

[0043] 图6是本发明实施例提供的同步凭证信息的示意图；

[0044] 图7是本发明实施例提供的根据加密身份信息和白名单地址生成凭证信息的实现流程图；

[0045] 图8是本发明实施例提供的凭证信息的示意图；

[0046] 图9是本发明实施例提供的票据信息的示意图；

[0047] 图10是本发明实施例提供的根据票据信息及凭证信息确定认证结果的实现流程图；

[0048] 图11是本发明实施例提供的访问处理装置的结构框图；

[0049] 图12是本发明实施例提供的访问处理系统的示意图；

[0050] 图13是本发明实施例提供的第一认证服务器的示意图。

具体实施方式

[0051] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本发明实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本发明。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本发明的描述。

[0052] 为了说明本发明所述的技术方案，下面通过具体实施例来进行说明。

[0053] 图1示出了本发明实施例提供的访问处理方法的实现流程，详述如下：

[0054] 在S101中，通过第一认证服务器接收客户端的访问请求。

[0055] 公有云平台通常会接入独立的不同应用系统服务器，在传统的访问处理机制中，通常是构建一个统一的认证服务器，通过该认证服务器对客户端进行身份信息认证，认证成功后才允许客户端使用认证服务器对应的应用系统服务器提供的服务，如显示页面的服务。由于不同应用系统服务器的认证方式可能不同，如应用系统服务器A使用密码认证方式进行认证，应用系统服务器B使用短信验证码认证方式进行认证，故必须对各应用系统服务器的认证方式及身份信息进行标准化后，才能通过统一的认证服务器进行认证，而标准化往往会涉及到大量的数据迁移及数据关联操作，导致传统访问处理机制的兼容性和扩展性差。

[0056] 针对上述情况，在本发明实施例中，对不同的应用系统服务器单独建立对应的认证服务器，为了便于理解，以第一认证服务器和第二认证服务器进行区分，其中，“第一”和“第二”仅用于区分建立的不同认证服务器，并不指示顺序的先后。通过第一认证服务器接收客户端的访问请求，本发明实施例对客户端发起访问请求的方式不做限定，比如在第一认证服务器提供了登录页面的地址的前提下，客户端可直接通过浏览器访问该登录页面的地址，从而向第一认证服务器发起访问请求，其中，访问请求可为超文本传输协议(HyperText Transfer Protocol，HTTP)请求或应用其他协议的请求。

[0057] 在一种实现方式中，通过第一认证服务器接收重定向的访问请求，该访问请求由第一认证服务器对应的应用系统服务器拦截并进行重定向。如图2所示，在一些访问机制中，客户端可能直接向第一认证服务器对应的应用系统服务器发起访问请求，故在本发明实施例中，在应用系统服务器部署过滤(Filter)组件，通过该过滤组件拦截访问该应用系统服务器的访问请求，并将访问请求重定向至第一认证服务器进行验证。在此基础上，还可通过过滤组件判断客户端是否已认证过，根据判断结果执行不同的操作，如当客户端的访

问请求携带有认证后的信息，如票据信息时，不拦截该访问请求，其中，票据信息的具体内容在后文进行详细阐述；当客户端的访问请求未携带有认证后的信息时，确定客户端未登录过，则拦截该访问请求，并将该访问请求重定向至第一认证服务器。通过上述方法提升了处理访问请求的适用性。

[0058] 在S102中，获取所述客户端的身份信息。

[0059] 第一认证服务器接收到访问请求后，与客户端进行交互，获取客户端的身份信息，本发明实施例对身份信息的具体内容不做限定，如身份信息可包括用户名和密码。举例来说，第一认证服务器可提供登录页面至客户端的浏览器，客户端的用户在登录页面上输入身份信息，进行交互。

[0060] 在S103中，当已存储身份信息包括所述客户端的身份信息时，生成凭证信息。

[0061] 已存储身份信息是指具有使用服务权限的客户端的身份信息，当第一认证服务器的已存储身份信息包括客户端的身份信息时，证明该客户端具有使用服务权限，则生成与该客户端对应的凭证信息；当第一认证服务器的已存储身份信息未包括客户端的身份信息时，证明该客户端不具有使用服务权限，则确定该客户端认证失败，可向客户端输出认证失败的提示。

[0062] 在一种实现方式中，当已存储身份信息包括客户端的身份信息时，生成票据信息，将票据信息发送到客户端；将票据信息添加至访问请求，并将访问请求重定向至应用系统服务器。本发明实施例对根据凭证信息对客户端进行认证的方式不做限定，如除了生成凭证信息之外，还可生成票据信息，并将票据信息发送到客户端，客户端后续进行访问时，将票据信息添加至访问请求内，发往应用系统服务器，应用系统服务器将访问请求中的票据信息发送至第一认证服务器，第一认证服务器根据票据信息和凭证信息确定客户端认证成功或认证失败。另外，为了规范本次认证，将票据信息添加至访问请求，如在访问请求为HTTP请求的情况下，将票据信息添加在访问请求的统一资源定位符(Uniform Resource Locator，URL)中，并将访问请求重定向至应用系统服务器，从而应用系统服务器可将票据信息发送至第一认证服务器进行认证，由第一认证服务器确定客户端认证成功或认证失败。通过上述方法提升了访问处理的规范性。

[0063] 在S104中，存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证。

[0064] 将得到的凭证信息进行存储，具体可将凭证信息存储于第一认证服务器的缓存和数据库中，以在下次认证时，根据凭证信息对该客户端进行认证。

[0065] 在S105中，将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

[0066] 第一认证服务器将凭证信息同步至第二认证服务器，以使第二认证服务器存储凭证信息后，根据凭证信息对该客户端进行认证。如此，就算第一认证服务器和第二认证服务器原本应用的是不同的认证方式，在同步了凭证信息后，第二认证服务器便可根据凭证信息对对应的客户端进行快速认证。

[0067] 为了便于理解本发明实施例的内容，提供了如图3所示的访问处理方法的另一种架构图，在图3中，应用系统服务器1对应第一认证服务器，应用系统服务器2对应第二认证服务器，第一认证服务器与第二认证服务器之间可互通凭证信息。当客户端向应用系统服务器1发送访问请求，应用系统服务器1将访问请求重定向至第一认证服务器进行验证，第

一认证服务器对客户端进行身份认证，在身份认证成功，即第一认证服务器的已存储身份信息包括客户端的身份信息时，第一认证服务器生成并存储凭证信息，并将凭证信息同步至第二认证服务器。如此，第二认证服务器在存储同步的凭证信息后，便可根据凭证信息对相同的客户端进行快速认证。

[0068] 通过发明实施例中对于图1的上述示例性实施可知，通过第一认证服务器对客户端进行认证，当认证成功时，生成并存储凭证信息，并将该凭证信息同步至第二认证服务器，以使第二认证服务器根据凭证信息对客户端进行认证，本发明实施例通过建立第一认证服务器和第二认证服务器并同步凭证信息，避免对不同的认证方式及不同格式的身份信息进行标准化，提升了访问处理的兼容性和扩展性，适用于接入不同应用系统服务器的公有云平台。

[0069] 图4所示，是本发明实施例提供的生成凭证信息的实现流程图，如图4所示，可以包括以下步骤：

[0070] 在S401中，确定所述第一认证服务器存储的至少一个白名单地址，所述白名单地址对应所述第一认证服务器信任的第二认证服务器。

[0071] 在本发明实施例中，应用白名单的机制对凭证信息的流向进行控制，具体地，确定第一认证服务器存储的至少一个白名单地址，该白名单地址为第一认证服务器信任的第二认证服务器的地址，可根据实际应用场景进行设置。值得说明的是，第一认证服务器信任某个第二认证服务器，是指该第一认证服务器和该第二认证服务器可共用相同的凭证信息进行认证。

[0072] 在S402中，根据所述白名单地址生成凭证信息，所述凭证信息用于被同步至所述白名单地址对应的第二认证服务器。

[0073] 根据确定出的白名单地址单独生成凭证信息，该凭证信息用于被同步至其内的白名单地址对应的第二认证服务器，即生成的凭证信息仅包括单个白名单地址。举例来说，第一认证服务器存储的白名单地址包括$Address_A$和$Address_B$，则生成包括$Address_A$的凭证信息，该凭证信息用于被同步至$Address_A$对应的第二认证服务器；生成包括$Address_B$的凭证信息，该凭证信息用于被同步至$Address_B$对应的第二认证服务器。

[0074] 通过发明实施例中对于图4的上述示例性实施可知，确定第一认证服务器存储的至少一个白名单地址，根据白名单地址生成凭证信息，该凭证信息用于被同步至白名单地址对应的第二认证服务器，本发明实施例通过控制凭证信息的流向，提升了同步凭证信息的有序性。

[0075] 图5所示，是本发明实施例提供的对接收到的凭证信息进行处理的实现流程图，如图5所示，可以包括以下步骤：

[0076] 在S501中，接收同步的凭证信息。

[0077] 在第一认证服务器接收到同步的凭证信息时，确定该凭证信息中的白名单地址。

[0078] 在S502中，当所述凭证信息内的白名单地址与所述第一认证服务器的地址相同时，存储所述凭证信息。

[0079] 在生成凭证信息后，凭证信息可能会被不知情地同步，如图6所示，认证服务器1内的白名单地址包括认证服务器2的地址、认证服务器3的地址及认证服务器4的地址，认证服务器2内的白名单地址包括认证服务器1的地址及认证服务器3的地址，认证服务器3内的白

名单地址包括认证服务器1的地址及认证服务器4的地址。在此基础上，若认证服务器2生成了凭证信息，那么凭证信息会被同步至认证服务器1及认证服务器3，然后认证服务器3会根据自身存储的白名单地址进行继续同步，将凭证信息同步至认证服务器4，但认证服务器4的地址并不是生成凭证信息的认证服务器2的白名单地址，即：将凭证信息同步至认证服务器4的过程是在认证服务器2不知情的情况下进行的。故在本发明实施例中，当凭证信息内的白名单地址与第一认证服务器自身的地址相同时，证明第一认证服务器是该凭证信息原本被期望同步的认证服务器，则存储该凭证信息。

[0080] 在S503中，当所述凭证信息内的白名单地址与所述第一认证服务器的地址不同时，丢弃所述凭证信息。

[0081] 当凭证信息内的白名单地址与第一认证服务器的地址不同时，证明该凭证信息被错误地同步至第一认证服务器，则丢弃该凭证信息，防止非法扩散。举例来说，假设第一认证服务器的地址为$Address_1$，第一认证服务器接收到的凭证信息内的白名单地址为$Address_2$，则凭证信息内的白名单地址与第一认证服务器的地址不同，第一认证服务器丢弃该凭证信息。值得说明的是，S501～S503同样适用于第二认证服务器。

[0082] 通过发明实施例中对于图5的上述示例性实施可知，接收同步的凭证信息，当该凭证信息内的白名单地址与第一认证服务器的地址相同时，存储该凭证信息；当该凭证信息内的白名单地址与第一认证服务器的地址不同时，丢弃该凭证信息，本发明实施例通过验证凭证信息内的白名单地址，提升了同步凭证信息的安全性，有效地避免了凭证信息非法扩散。

[0083] 图7所示，是本发明实施例提供的根据加密身份信息和白名单地址生成凭证信息的实现流程图，如图7所示，可以包括以下步骤：

[0084] 在S701中，对所述客户端的身份信息进行加密生成加密身份信息。

[0085] 为了保证不同客户端对应的凭证信息是不同的，在本发明实施例中，对客户端的身份信息进行加密生成加密身份信息，具体可对客户端的身份信息的部分内容或全部内容进行加密，除此之外，还可添加其他信息，如随机字符串或系统当前时间等进行加密。本发明实施例对加密所采用的加密算法并不做限定，如可采用消息摘要算法进行加密。

[0086] 在S702中，根据所述加密身份信息和所述白名单地址生成凭证信息。

[0087] 根据加密身份信息和白名单地址生成凭证信息，如图8所示，生成的凭证信息包括加密身份信息和白名单地址。

[0088] 在一种实现方式中，根据加密身份信息和所有白名单地址生成票据信息，将票据信息发送到客户端，以使客户端发起包括票据信息的访问请求进行认证。除了生成凭证信息之外，在本发明实施例中，还可生成票据信息，具体根据加密身份信息和第一认证服务器存储的所有白名单地址生成票据信息，并将票据信息发送到客户端，客户端存储票据信息后，下次便可发起包括票据信息的访问请求进行认证。如图9所示，假设第一认证服务器存储的白名单地址包括N个，N为大于2的整数，则生成的票据信息包括加密身份信息和N个白名单地址。通过上述方法保证了票据信息的唯一性。

[0089] 通过发明实施例中对于图7的上述示例性实施可知，对客户端的身份信息进行加密生成加密身份信息，根据加密身份信息和白名单地址生成凭证信息，本发明实施例保证了凭证信息的唯一性，避免因不同的客户端对应同一个凭证信息导致认证混乱。

[0090] 图10所示，是本发明实施例提供的根据票据信息及凭证信息确定认证结果的实现流程图，如图10所示，可以包括以下步骤：

[0091] 在S1001中，接收所述客户端的票据信息。

[0092] 在生成的凭证信息包括加密身份信息和白名单地址，且生成的票据信息包括加密身份信息和第一认证服务器存储的所有白名单地址的前提下，当第一认证服务器接收到客户端的票据信息时，根据票据信息内的加密身份信息及所有白名单地址确定认证结果。值得说明的是，票据信息可能由客户端直接发送至第一认证服务器，也可能由客户端发送至应用系统服务器，应用系统服务器再将票据信息发送至第一认证服务器。

[0093] 在S1002中，当所述票据信息与所述凭证信息中的加密身份信息相同，且所述票据信息包括所述凭证信息中的白名单地址时，确定所述客户端认证成功。

[0094] 当票据信息与凭证信息中的加密身份信息相同，且票据信息包括凭证信息中的白名单地址时，确定客户端认证成功，可输出认证成功的信息至第一认证服务器对应的应用系统服务器，使得应用系统服务器为客户端提供服务。除此之外，还可能存在另一种情况，即票据信息与凭证信息中的加密身份信息相同，但凭证信息中的白名单地址为空，该情况证明该凭证信息并不是从第二认证服务器同步的，则确定第一认证服务器是生成凭证信息的认证服务器，由第一认证服务器确定客户端认证成功。

[0095] 在S1003中，当所述票据信息与所述凭证信息中的加密身份信息不同，和/或所述票据信息未包括所述凭证信息中的白名单地址时，确定所述客户端认证失败。

[0096] 在同步凭证信息的过程中，可能通过修改凭证信息中的白名单地址，使得凭证信息非法地存储于第一认证服务器中，比如第一认证服务器在接收到的凭证信息内的白名单地址不为该第一认证服务器的地址的情况下，可能非法地将凭证信息内的地址修改为该第一认证服务器的地址，从而存储该凭证信息。故在本发明实施例中，当票据信息与凭证信息中的加密身份信息不同，和/或票据信息未包括凭证信息中的白名单地址时，确定客户端认证失败，从而避免非法存储凭证信息的第一认证服务器根据该凭证信息确定客户端认证成功。

[0097] 通过发明实施例中对于图10的上述示例性实施可知，接收客户端的票据信息，当票据信息与凭证信息中的加密身份信息相同，且票据信息包括凭证信息中的白名单地址时，确定客户端认证成功；当票据信息与凭证信息中的加密身份信息不同，和/或票据信息未包括凭证信息中的白名单地址时，确定客户端认证失败。本发明实施例提升了对客户端进行认证的安全性，避免非法存储凭证信息的第一认证服务器对客户端认证成功。

[0098] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0099] 对应于上文实施例所述的访问处理方法，图11示出了本发明实施例提供的访问处理装置的结构框图，参照图11，该访问处理装置包括：

[0100] 接收单元111，用于通过第一认证服务器接收客户端的访问请求；

[0101] 获取单元112，用于获取所述客户端的身份信息；

[0102] 生成单元113，用于当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；

[0103] 存储单元114，用于存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；

[0104] 同步单元115，用于将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

[0105] 在一种实现方式中，生成单元113包括：

[0106] 确定所述第一认证服务器存储的至少一个白名单地址，所述白名单地址对应所述第一认证服务器信任的第二认证服务器；

[0107] 根据所述白名单地址生成凭证信息，所述凭证信息用于被同步至所述白名单地址对应的第二认证服务器。

[0108] 在一种实现方式中，访问处理装置还包括：

[0109] 凭证接收单元，用于接收同步的凭证信息；

[0110] 凭证存储单元，当所述凭证信息内的白名单地址与所述第一认证服务器的地址相同时，存储所述凭证信息；

[0111] 凭证丢弃单元，当所述凭证信息内的白名单地址与所述第一认证服务器的地址不同时，丢弃所述凭证信息。

[0112] 在一种实现方式中，根据所述白名单地址生成凭证信息，包括：

[0113] 对所述客户端的身份信息进行加密生成加密身份信息；

[0114] 根据所述加密身份信息和所述白名单地址生成凭证信息。

[0115] 在一种实现方式中，对所述客户端的身份信息进行加密生成加密身份信息之后，还包括：

[0116] 根据所述加密身份信息和所有所述白名单地址生成票据信息，将所述票据信息发送到所述客户端，以使所述客户端发起包括所述票据信息的访问请求进行认证。

[0117] 在一种实现方式中，访问处理装置还包括：

[0118] 票据接收单元，用于接收所述客户端的票据信息；

[0119] 第一认证单元，用于当所述票据信息与所述凭证信息中的加密身份信息相同，且所述票据信息包括所述凭证信息中的白名单地址时，确定所述客户端认证成功；

[0120] 第二认证单元，用于当所述票据信息与所述凭证信息中的加密身份信息不同，和/或所述票据信息未包括所述凭证信息中的白名单地址时，确定所述客户端认证失败。

[0121] 在一种实现方式中，接收单元111包括：

[0122] 通过第一认证服务器接收重定向的访问请求，所述访问请求由所述第一认证服务器对应的应用系统服务器拦截并进行重定向。

[0123] 在一种实现方式中，访问处理装置还包括：

[0124] 票据生成单元，用于当所述已存储身份信息包括所述客户端的身份信息时，生成票据信息，将所述票据信息发送到所述客户端；

[0125] 重定向单元，用于将所述票据信息添加至所述访问请求，并将所述访问请求重定向至所述应用系统服务器。

[0126] 因此，本发明实施例提供的访问处理装置通过第一认证服务器对客户端进行认证，并在认证成功后将生成的凭证信息同步至第二认证服务器，提升了访问处理的兼容性和扩展性，适用于接入不同应用系统服务器的公有云平台。

[0127] 图12示出了本发明实施例提供的访问处理系统的示意图，在图12中，访问处理系统12包括客户端121、第一认证服务器122及第二认证服务器123，本发明实施例对第二认证服务器123的数量不做限定，在图12中以第二认证服务器123的数量为两个作为示例。其中，第一认证服务器122执行：

[0128] 通过第一认证服务器122接收客户端121的访问请求；

[0129] 获取所述客户端121的身份信息；

[0130] 当已存储身份信息包括所述客户端121的身份信息时，生成凭证信息；

[0131] 存储所述凭证信息，以根据所述凭证信息对所述客户端121进行认证；

[0132] 将所述凭证信息同步至第二认证服务器123，以使所述第二认证服务器123根据所述凭证信息对所述客户端121进行认证。

[0133] 在一种实现方式中，生成凭证信息，包括：

[0134] 确定所述第一认证服务器122存储的至少一个白名单地址，所述白名单地址对应所述第一认证服务器122信任的第二认证服务器123；

[0135] 根据所述白名单地址生成凭证信息，所述凭证信息用于被同步至所述白名单地址对应的第二认证服务器123。

[0136] 在一种实现方式中，第一认证服务器122还执行：

[0137] 接收同步的凭证信息；

[0138] 当所述凭证信息内的白名单地址与所述第一认证服务器122的地址相同时，存储所述凭证信息；

[0139] 当所述凭证信息内的白名单地址与所述第一认证服务器122的地址不同时，丢弃所述凭证信息。

[0140] 在一种实现方式中，根据所述白名单地址生成凭证信息，包括：

[0141] 对所述客户端121的身份信息进行加密生成加密身份信息；

[0142] 根据所述加密身份信息和所述白名单地址生成凭证信息。

[0143] 在一种实现方式中，对所述客户端121的身份信息进行加密生成加密身份信息之后，还包括：

[0144] 根据所述加密身份信息和所有所述白名单地址生成票据信息，将所述票据信息发送到所述客户端121，以使所述客户端121发起包括所述票据信息的访问请求进行认证。

[0145] 在一种实现方式中，第一认证服务器122还执行：

[0146] 接收所述客户端121的票据信息；

[0147] 当所述票据信息与所述凭证信息中的加密身份信息相同，且所述票据信息包括所述凭证信息中的白名单地址时，确定所述客户端121认证成功；

[0148] 当所述票据信息与所述凭证信息中的加密身份信息不同，和/或所述票据信息未包括所述凭证信息中的白名单地址时，确定所述客户端121认证失败。

[0149] 在一种实现方式中，通过第一认证服务器122接收客户端121的访问请求，包括：

[0150] 通过第一认证服务器122接收重定向的访问请求，所述访问请求由所述第一认证服务器122对应的应用系统服务器拦截并进行重定向。

[0151] 在一种实现方式中，第一认证服务器122还执行：

[0152] 当所述已存储身份信息包括所述客户端121的身份信息时，生成票据信息，将所述

票据信息发送到所述客户端121；

[0153] 将所述票据信息添加至所述访问请求，并将所述访问请求重定向至所述应用系统服务器。

[0154] 因此，本发明实施例提供的访问处理系统12通过同步生成的凭证信息，提升了访问处理的兼容性和扩展性，适用于接入不同应用系统服务器的公有云平台。

[0155] 图13是本发明实施例提供的第一认证服务器的示意图。如图13所示，该实施例的第一认证服务器13包括：处理器130、存储器131以及存储在所述存储器131中并可在所述处理器130上运行的计算机程序132，例如访问处理程序。所述处理器130执行所述计算机程序132时实现上述各个访问处理方法实施例，例如图1所示的步骤S101至S105。或者，所述处理器130执行所述计算机程序132时实现上述各访问处理装置实施例中各单元的功能，例如图11所示单元111至115的功能。

[0156] 示例性的，所述计算机程序132可以被分割成一个或多个单元，所述一个或者多个单元被存储在所述存储器131中，并由所述处理器130执行，以完成本发明。所述一个或多个单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序132在所述第一认证服务器13中的执行过程。例如，所述计算机程序132可以被分割成接收单元、获取单元、生成单元、存储单元及同步单元，各单元具体功能如下：

[0157] 接收单元，用于通过第一认证服务器接收客户端的访问请求；

[0158] 获取单元，用于获取所述客户端的身份信息；

[0159] 生成单元，用于当已存储身份信息包括所述客户端的身份信息时，生成凭证信息；

[0160] 存储单元，用于存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证；

[0161] 同步单元，用于将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证。

[0162] 所述第一认证服务器13可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述第一认证服务器可包括，但不仅限于，处理器130、存储器131。本领域技术人员可以理解，图13仅仅是第一认证服务器13的示例，并不构成对第一认证服务器13的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述第一认证服务器还可以包括输入输出设备、网络接入设备、总线等。

[0163] 所称处理器130可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0164] 所述存储器131可以是所述第一认证服务器13的内部存储单元，例如第一认证服务器13的硬盘或内存。所述存储器131也可以是所述第一认证服务器13的外部存储设备，例如所述第一认证服务器13上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。进一步地，所述存储器131还可以既包括所述第一认证服务器13的内部存储单元也包括外部存储设备。所述存储器131用于存储所述计算机程序以及所述第一认证服务器所需的其他程序和数据。所述存储器131还

可以用于暂时地存储已经输出或者将要输出的数据。

[0165] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元完成，即将所述第一认证服务器的内部结构划分成不同的功能单元，以完成以上描述的全部或者部分功能。实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0166] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0167] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0168] 在本发明所提供的实施例中，应该理解到，所揭露的第一认证服务器和方法，可以通过其它的方式实现。例如，以上所描述的第一认证服务器实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口，装置或单元的间接耦合或通讯连接，可以是电性，机械或其它的形式。

[0169] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0170] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0171] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读存储介质中。基于这样的理解，本发明实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读存储介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读存储介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如

在某些司法管辖区，根据立法和专利实践，计算机可读存储介质不包括电载波信号和电信信号。

[0172] 以上所述实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围，均应包含在本发明的保护范围之内。

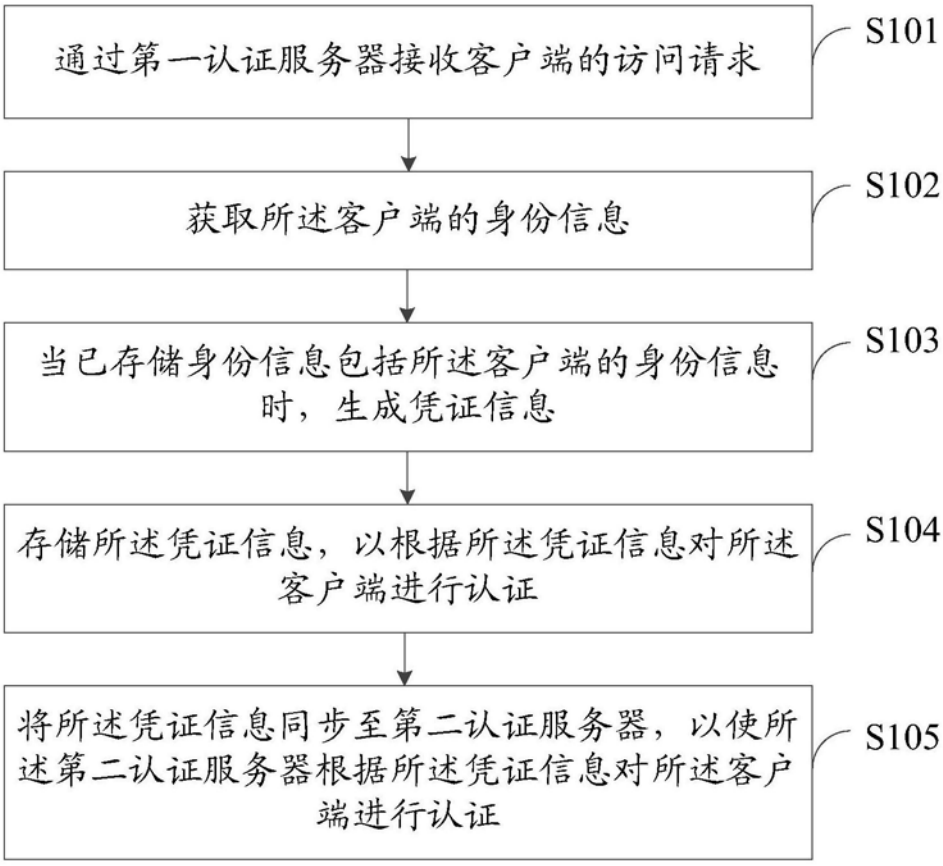

通过第一认证服务器接收客户端的访问请求
S101
获取所述客户端的身份信息
S102
当已存储身份信息包括所述客户端的身份信息时，生成凭证信息
S103
存储所述凭证信息，以根据所述凭证信息对所述客户端进行认证
S104
将所述凭证信息同步至第二认证服务器，以使所述第二认证服务器根据所述凭证信息对所述客户端进行认证
S105

图1

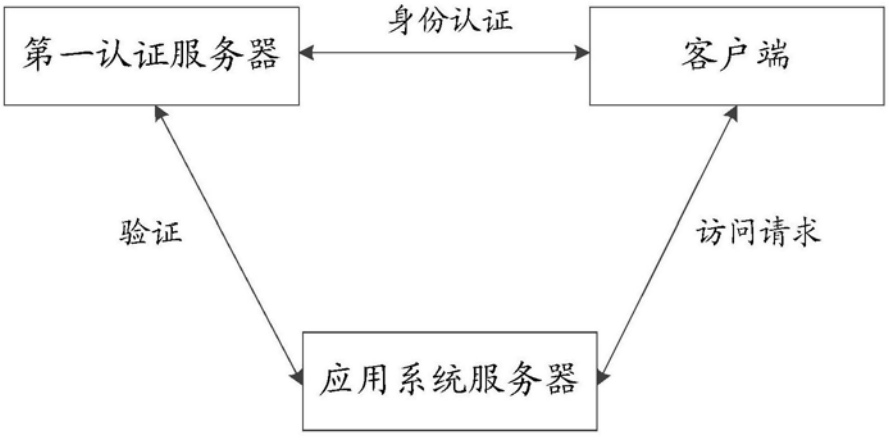

第一认证服务器
身份认证
客户端
验证
访问请求
应用系统服务器

图2

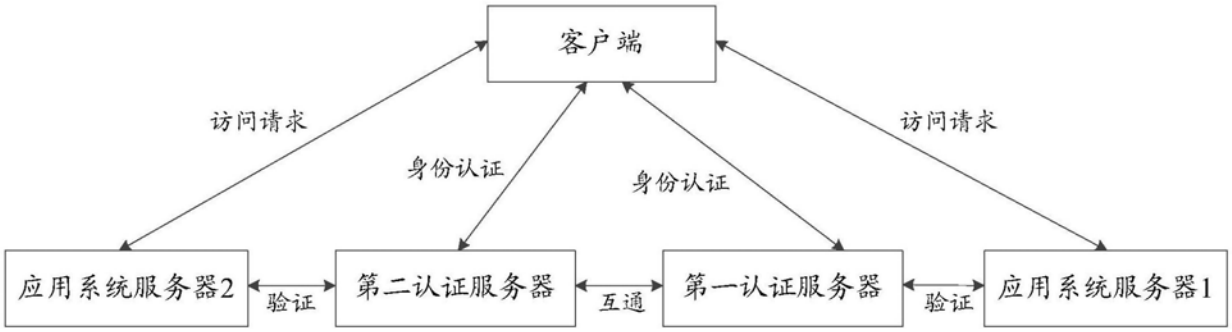

客户端
访问请求
身份认证
身份认证
访问请求
应用系统服务器2
验证
第二认证服务器
互通
第一认证服务器
验证
应用系统服务器1

图3

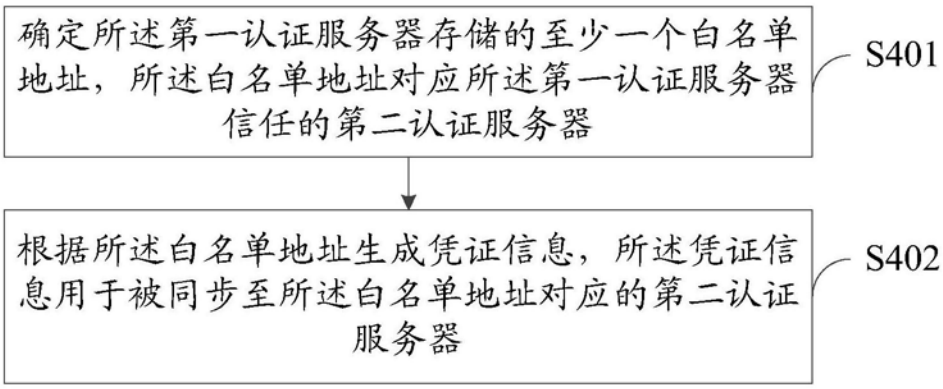

确定所述第一认证服务器存储的至少一个白名单地址，所述白名单地址对应所述第一认证服务器信任的第二认证服务器
S401
根据所述白名单地址生成凭证信息，所述凭证信息用于被同步至所述白名单地址对应的第二认证服务器
S402

图4

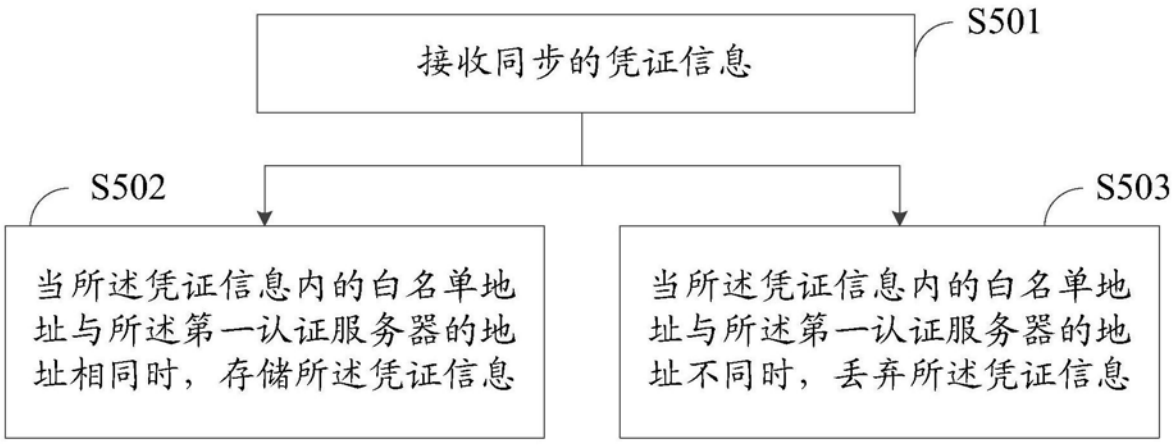

接收同步的凭证信息
S501
S502
当所述凭证信息内的白名单地址与所述第一认证服务器的地址相同时，存储所述凭证信息
S503
当所述凭证信息内的白名单地址与所述第一认证服务器的地址不同时，丢弃所述凭证信息

图5

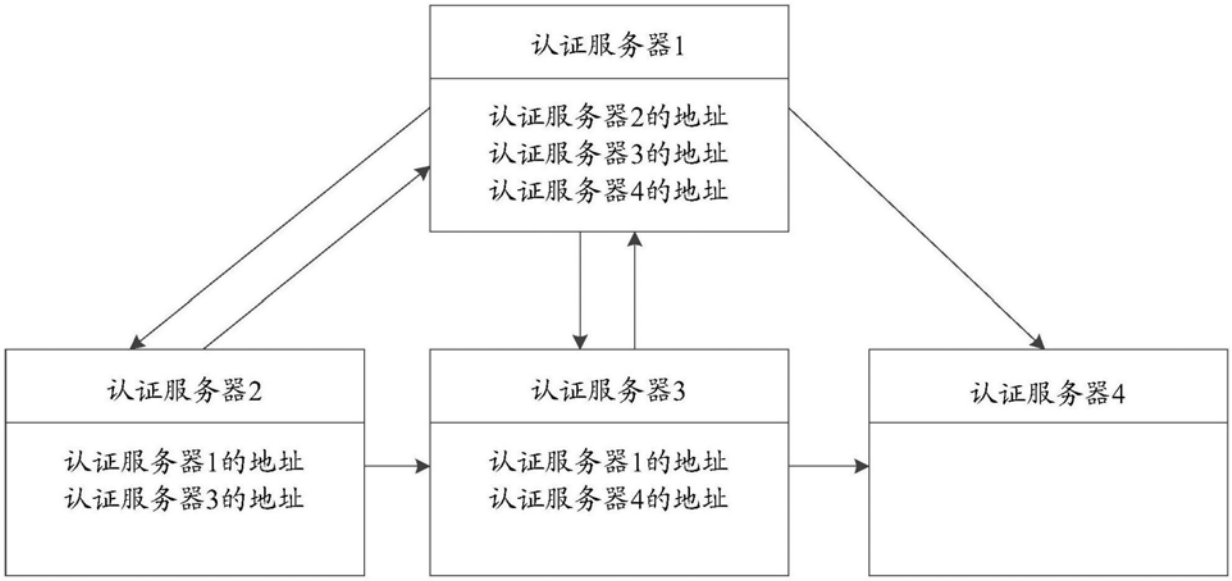

认证服务器1
认证服务器2的地址
认证服务器3的地址
认证服务器4的地址
认证服务器2
认证服务器1的地址
认证服务器3的地址
认证服务器3
认证服务器1的地址
认证服务器4的地址
认证服务器4

图6

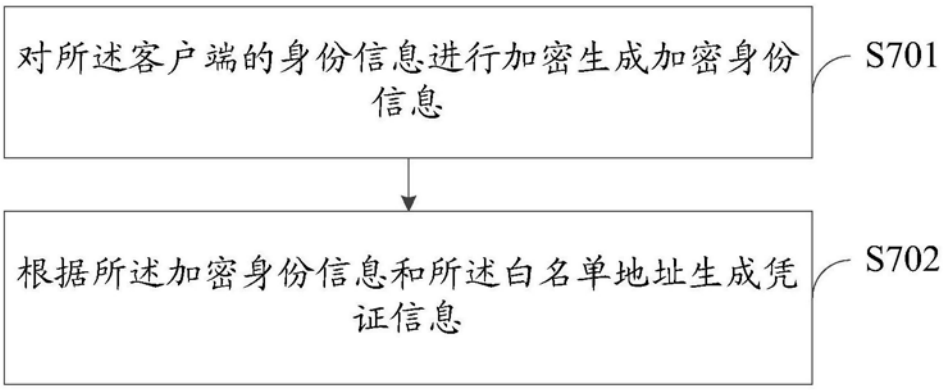

对所述客户端的身份信息进行加密生成加密身份信息
S701
根据所述加密身份信息和所述白名单地址生成凭证信息
S702

图7

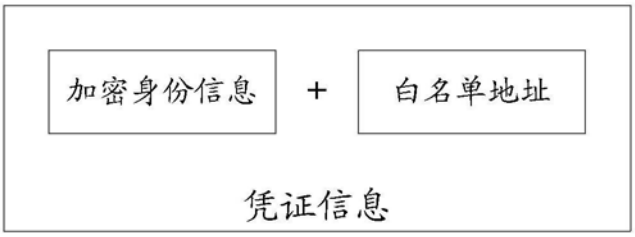

加密身份信息
+
白名单地址
凭证信息

图8

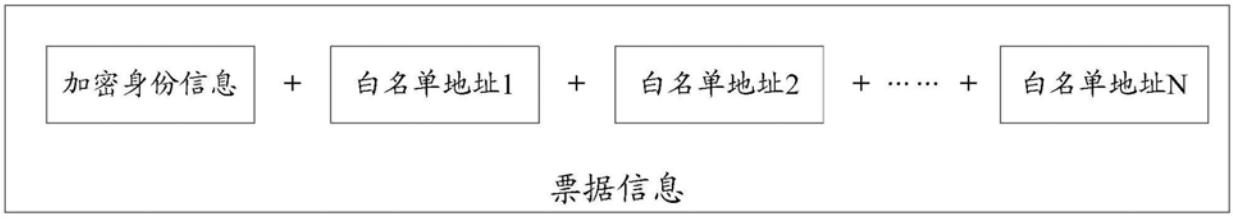

加密身份信息
+
白名单地址1
+
白名单地址2
+ …… +
白名单地址N
票据信息

图9

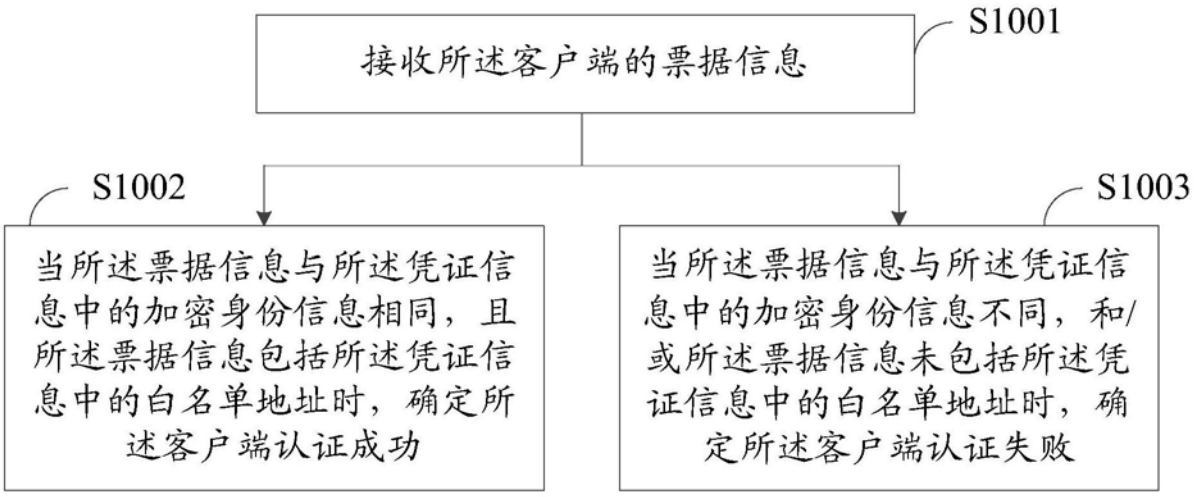

接收所述客户端的票据信息
S1001
S1002
当所述票据信息与所述凭证信息中的加密身份信息相同，且所述票据信息包括所述凭证信息中的白名单地址时，确定所述客户端认证成功
S1003
当所述票据信息与所述凭证信息中的加密身份信息不同，和/或所述票据信息未包括所述凭证信息中的白名单地址时，确定所述客户端认证失败

图10

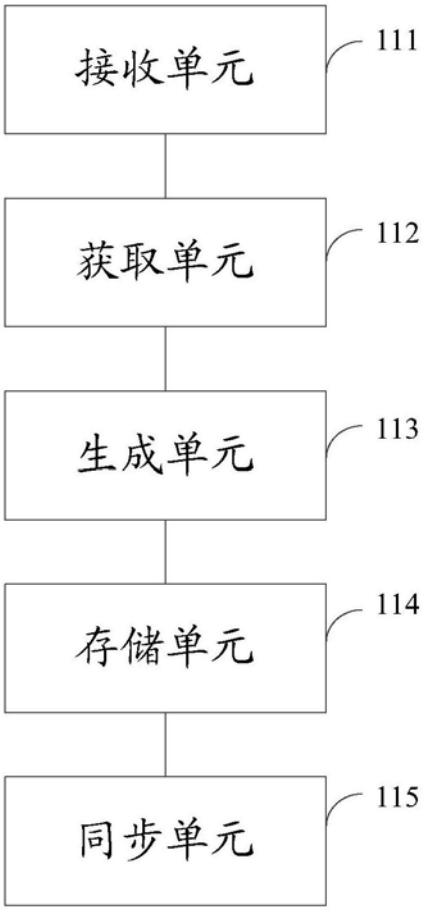

接收单元
111
获取单元
112
生成单元
113
存储单元
114
同步单元
115

图11

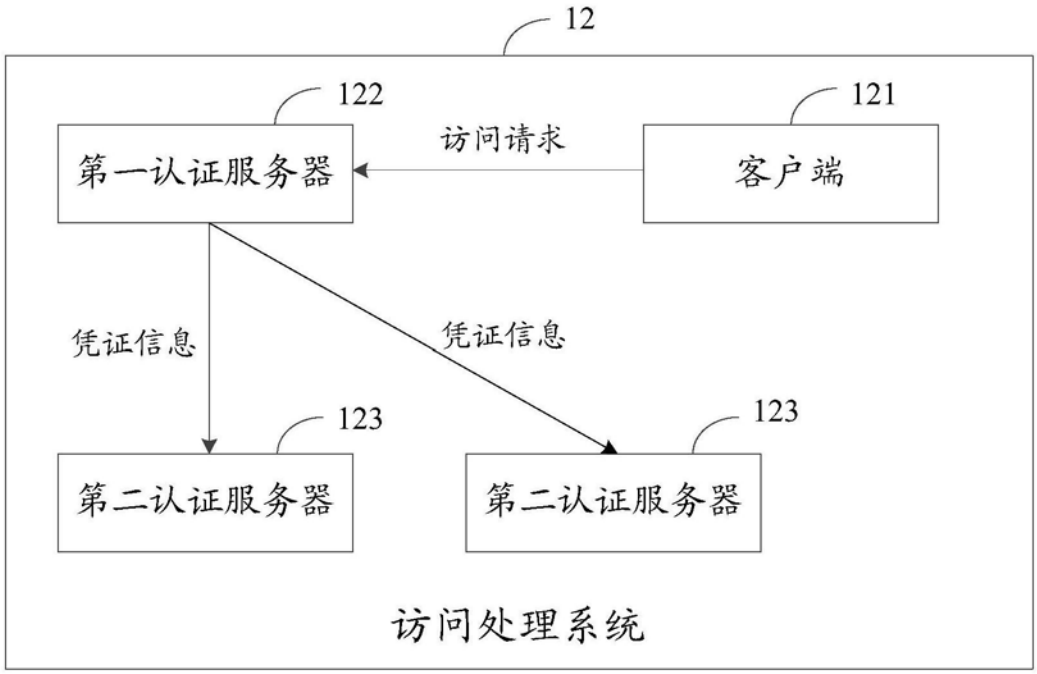

12
122
第一认证服务器
访问请求
121
客户端
凭证信息
凭证信息
123
第二认证服务器
123
第二认证服务器
访问处理系统

图12

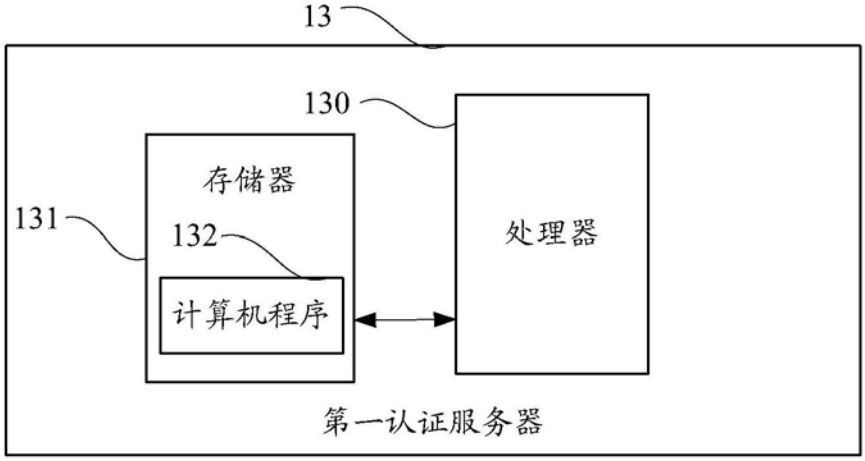


图13