(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 103179108 B
(45)授权公告日 2016.08.10

(21)申请号 201310020053.5

(22)申请日 2013.01.18

(30)优先权数据
13/354,324 2012.01.19 US

(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州

(72)发明人 V·艾德尔曼 B·克雷斯 M·莱布曼 M·努尔丁 L·余 H·罗

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 王英

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

(56)对比文件
CN 101610241 A,2009.12.23,
US 7520339 B2,2009.04.21,
US 2009/0287935 A1,2009.11.19,

审查员 谭梁镌

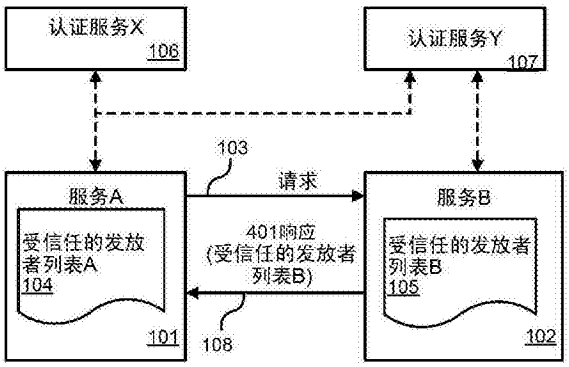
权利要求书1页 说明书9页 附图4页

(54)发明名称

应用认证方法及计算机系统

(57)摘要

本发明描述了将服务器应用与多个认证提供者集成。在线和场所内应用标识受信任的认证提供者。应用被配置有受信任的认证凭证发放者列表。当应用接收到要求认证的请求，应用返回包括受信任的发放者列表的401响应。提出请求的应用将来自401响应的受信任的发放者列表与它自己的认证提供者列表进行比较。如果在两个列表之间存在匹配，则提出请求的应用为认证提供者创建自发放令牌。认证提供者使用自发放令牌来为提出请求的应用生成认证令牌。提出请求的应用还可在没有认证提供者的情况下直接为目标伙伴应用创建令牌，如果在两个应用之间存在直接信任的话。



CN 103179108 B

1.一种应用认证方法,包括:

将请求从第一应用发送到第二应用(201);

接收对所述请求的响应,所述响应包括被所述第二应用信任的认证发放者列表(202);

将被所述第二应用信任的认证发放者列表与针对所述第一应用认可的认证发放者列表进行比较(203);以及

标识所述列表之间的认证发放者匹配(204);

使用来自经认可的认证发放者配置的承租人标识符来构造认证发放者的令牌;

获得来自匹配两个列表的认证发放者的认证凭证;

使用所述认证凭证来生成对所述第二应用的经修订的请求。

2.如权利要求1所述的方法,其特征在于,所述响应是指示未经认证的请求的401响应,并且其中被所述第二应用信任的认证发放者列表在所述401响应的WWW-Authenticate头部中传输。

3.如权利要求1所述的方法,其特征在于,还包括:

使用全局唯一标识符(GUID)来确定被所述第二应用信任的认证发放者是否匹配针对所述第一应用认可的认证发放者。

4.如权利要求3所述的方法,其特征在于,还包括:

生成一组输入参数;以及

使用来自所述输入参数的承租人标识符来构造认证发放者的令牌。

5.如权利要求1所述的方法,其特征在于,还包括:

使用匹配经认可的认证发放者配置的全局唯一标识符(GUID)和来自经认可的认证发放者配置的承租人标识符来创建所述认证发放者的自发放令牌。

6.如权利要求5所述的方法,其特征在于,还包括:

接收来自所述认证发放者的认证令牌,所述认证令牌由所述认证发放者使用所述自发放令牌来生成。

7.一种计算机系统,包括:

处理单元(408);

数据存储(402);

其上存储有计算机可执行指令的一个或多个计算机可读介质(404),所述指令在由所述处理单元(408)执行时使得所述处理单元(408)执行一种用于生成认证凭证的方法,所述处理单元(408)操作用于:

将请求从第一应用发送到第二应用(201);

接收对所述请求的响应,所述响应包括被所述第二应用信任的认证发放者列表(202);

将被所述第二应用信任的认证发放者列表与针对所述第一应用认可的认证发放者列表进行比较(203);以及

标识匹配两个列表的认证发放者(204);

使用来自经认可的认证发放者配置的承租人标识符来构造认证发放者的令牌;

获得来自匹配两个列表的认证发放者的认证凭证;

使用所述认证凭证来生成对所述第二应用的经修订的请求。

应用认证方法及计算机系统

技术领域

[0001] 本发明涉及将服务器应用与多个认证提供者集成。

背景技术

[0002] 跨多个场所内环境和在线环境而分布的服务器和服务的部署拓扑结构变得日益复杂。应用要求跨这些服务器和服务的安全访问，而不管它们的部署特性或位置如何。成功的安全访问通常由受到服务器和服务支持的认证方案来管理。通常，对另一服务器或服务作出请求的服务器或服务需要知道如何认证该请求以使得它将是成功的。

[0003] 诸如OAuth协议之类的标准认证协议可被服务器和服务用于成功认证。然而，这些标准协议并未充分地描述如何在服务器和服务之间为它们构建信任以使得其能够成功。另外，现有的认证协议未考虑跨越在线环境和场所内环境的复杂部署拓扑结构。

[0004] 例如，OAuth协议常常需要所有应用和服务都必须信赖并且依赖其来成功获取用于认证的凭证的单个认证服务器。然而，许多场景可能无法使用这一单个认证服务器概念。

[0005] 另外，尽管OAuth协议详细描述了协议流，但该协议将关于该协议的语义和内容的细节停留在认证服务器的具体实现。这意味着，与一个认证服务器集成的服务器或服务不一定能够成功地依赖于使用这一相同的认证服务器来对与一个不同的认证服务器集成的另一服务器或服务作出请求。在许多场景中，尤其在场所内场景中，服务器或服务根本无法与任何认证服务器集成。

[0006] 最终，在成功认证之后，服务器和服务通常实现授权机制来保护资源免受不必要的访问。通常，这些授权机制对于服务是专用的，但是是基于作为用于认证而查询的凭证的一部分来提供的身份的。在使用OAuth协议的情况下，客户机应用是经验证和受信任的身份。如果客户机应用的身份改变，则授权必须被重新配置，并且认证不可用直到用新的客户机应用身份进行验证。

发明内容

[0007] 提供本发明内容以便以简化形式介绍将在以下具体实施方式中进一步描述的一些概念。本发明内容并不旨在标识所要求保护主题的关键特征或必要特征，也不旨在用于限制所要求保护主题的范围。

[0008] 各实施例提供了一种用于使服务和服务器应用使用诸如OAuth2.0协议之类的标准认证协议成功进行认证的通用模型。服务器和服务可与实现不同协议语义的多个认证服务器集成。诸如其他服务器和服务之类的客户机可在没有认证服务器的情况下使用该标准协议来访问依赖方。向依赖方提供了允许客户机选择合适的凭证发放者来向依赖方进行认证的广告机制。

附图说明

[0009] 为了进一步阐明本发明的各实施例的以上和其他优点和特征，将参考附图来呈现

本发明的各实施例的更具体的描述。可以理解，这些附图只描绘本发明的典型实施例，因此将不被认为是对其范围的限制。本发明将通过使用附图用附加特征和细节来描述和解释，附图中：

[0010] 图1示出了彼此通信以标识可接受的认证源的两个服务；

[0011] 图2示出了一种用于标识受信任的认证凭证发放者的方法或过程；

[0012] 图3A和3B是示出一种用于为使用发放者匹配来选择出站令牌的发放者的应用构造出站令牌的方法或过程的流程图。

[0013] 图4显示了其上可以实现图1-3的示例的适当的计算和网络环境的示例。

具体实施方式

[0014] 图1示出了彼此通信以标识可接受的认证源的两个服务101和102。在某些实施例中，服务101和102可位于同一服务器上和/或位于同一场所内，并且可由同一管理员配置。在其他实施例中，服务101和102可彼此远离地位于分开的服务器上和/或位于分开的场所内，并且可由不同的管理员配置。在这种配置中，服务器101和102可经由诸如局域网(LAN)、广域网(WAN)、内联网或因特网之类的无线或有线网络来通信。这些配置在此处可被称为“场所内”配置。在服务101和102是云中的托管环境并且由单独的托管组织来管理的情况下，该配置在此处被称为“在线”配置。

[0015] 服务101和102可以是不同应用的单独实例，或者可以是同一应用的单独实例。在任一情况下，用户可能期望在服务101和102之间共享信息和数据。例如，用户可能想要在服务101上工作，并且想要对服务102执行动作或者与服务102交换数据。服务A101将请求103发送给服务B102以执行这种动作或交换数据。在服务B102对请求103进行操作之前，服务B102必须认证请求103。服务101被配置有标识经认可的认证凭证或令牌源的受信任的发放者列表104。类似地，服务102具有其自己的受信任的发放者列表105。受信任的发放者列表可例如标识一个或多个认证服务106、107。每一个服务101、102可具有其自己的可接受的认证服务的列表。例如，服务101可信任认证服务106和107，而服务102可仅信任认证服务107。

[0016] 在某些直接-信任实施例中，服务101和102能够自认证或创建它们自己的认证凭证或令牌。

[0017] 诸如OAuth协议之类的标准认证协议可用于向服务101和102彼此认证。然而，这些协议不总是成功的，因为服务101和102可能不共享同一认证服务106、107，或者可能具有不兼容的认证配置。

[0018] 当服务器102接收到请求103时，它返回401(未经授权的)响应108，该响应指示请求103要求认证。客户机可以用合适的授权头部字段来重复请求103。授权字段值由包含针对正被请求的资源的领域的应用的认证信息的凭证构成。

[0019] 在一个实施例中，401-未经授权的响应108包括来自响应服务102的受信任的发放者列表105。由此，响应108向服务101通知请求103必须被认证，并且提供服务101可从中获得必要的认证凭证或令牌的受信任的源的列表。服务101具有受信任的或经认可的认证服务的列表104。服务101将接收到的受信任的列表105与它自己的受信任的列表104进行比较，并且标识两个列表之间的任何匹配。例如，如果服务101信任认证服务106和107，而服务102信任认证服务107，则服务101可使用认证服务107来获得合适的凭证。

[0020] 服务101和102的受信任的发放者列表104、105可标识偏好的认证源的分层结构。例如，受信任的发放者列表104可对源排定优先级为或排名为(1)同一应用的其他部署的直接信任，(2)认证服务105，以及(3)认证服务106。在一个实施例中，服务101会将其列表104和接收到的列表105进行比较，并且将选择最 偏好的发放者。

[0021] 图2示出了一种用于标识受信任的认证凭证的发放者的方法或过程。在步骤201中，请求从第一服务被发送到第二服务。在步骤202中，第一服务接收到指示需要对请求进行认证的响应。该响应包括第二服务的受信任的认证发放者的列表。在步骤203中，第一服务将来自第二服务的受信任的发放者列表与其自己的受信任的发放者列表进行比较。在步骤204中，第一服务标识被第一和第二服务两者都信任的认证发放者。

[0022] 在步骤205中，第一服务获得来自被两个服务都信任的认证发放者的认证凭证。在步骤206中，第一服务生成包括认证凭证的新的请求。因为认证凭证来自被两个服务都信任的源，所以第二服务通常会接受该第二请求。

[0023] 配置

[0024] 为了参与受信任的发放者标识过程，每一个服务器或服务必须用合适的信息来配置。在一个实施例中，为每一个服务器或服务配置以下信息。

[0025] 应用发放者标识符。应用发放者标识符用于自发放的令牌的发放者字段。应用发放者标识符具有如下格式:PIDapp@realm。应用发放者标识符的所需字段如下被格式化。

[0026] PIDapp字段是应用的主要标识符。在一个实施例中，这是表示当前应用的全局唯一标识符(GUID)。在其他实施例中，确保跨这些标识符的唯一性的任何实现可被使用。Realm(领域)字段可以是用于场所内安装的默认域。在在线安装中，Realm值可以是承租人标识符。然而，承租人标识符只是Realm字段的一个可能值，Realm字段还可被设为某一其他值。

[0027] 安全令牌服务(STS)。还为每一个服务器或服务配置一个或多个STS。每一个STS具有如下格式:PIDsts@[TID],metadataURL。

[0028] PIDsts字段是表示STS的GUID。

[0029] TID字段按照如下来配置：

[0030] 对于场所内安装，TID字段是承租人标识符(承租人ID)，它是GUID或确保唯一性以标识具体承租人的任何实现。

[0031] 对于大部分在线安装，TID字段为空(或*)，并且必须被合适的承租人ID替换。

[0032] 例如，对于在不同部署中表示同一公司的承租人之间的信任所需的具体承租人内的在线安装，TID字段是承租人ID。

[0033] metadataURL(元数据URL)字段包含用于检索用于与STS建立信任的证书的URL。

[0034] 某些应用不存储发放者标识符，而是改为仅存储密钥、密钥标识符(例如，证书拇指纹)和元数据URL。

[0035] 经配置的伙伴应用。经配置的伙伴应用具有以下格式:PIDapp@[realm],{UseSTS|metadataURL}。

[0036] PIDapp字段是表示诸如另一服务器或服务之类的伙伴应用(PA)的GUID。

[0037] Realm字段对于在线安装为空(或*)，并且必须被合适的承租人ID替换。Realm字段保持场所内安装的默认域。

[0038] UseSTS字段用于选择这一PA的传入令牌是否必须由经配置的STS之一来发放。

[0039] metadataURL字段是可用于检索用于对应用的直接信任的证书的URL。

[0040] 某些应用不存储发放者标识符，而是改为仅存储密钥、密钥标识符(例如，证书拇指纹)和元数据URL。

[0041] 有效域或领域列表。受信任的发放者列表被配置为用于在线和场所内配置。对于在线安装，受信任的发放者列表是由承租人映射的所有承租人域后缀的列表。对于场所内安装，受信任的发放者列表是所有有效域后缀的列表。

[0042] 一般地，空的领域被解释为意味着与“*”领域相同。“*”条目用于支持全局配置模板，其中单个经配置的条目可支持数以百万计的承租人以简化配置和存储要求。

[0043] 领域是安全边界的标识符，并且PID(主要ID)是由领域来鉴定(即对于领域是唯一的)。TID(承租人ID)是领域的可能的值串。TID是数据中心中领域的主要名称。DNS域名是对于场所内配置中所使用的领域的另一可能的值串。DNS域名可作为在听众/资源中的领域被发送给STS，但域名在STS发放的令牌中被TID替换。

[0044] 发放者信息的发布。

[0045] 发放者列表在401响应中被返回给认证失败的、在Authorization(授权)头部 中使用Bearer(承载)方案的任何请求。

[0046] 每一个应用主机构造它将接受来自其的令牌的受信任的发放者列表。在一个实施例中，这一列表包括来自上述配置的所有STS以及不取决于STS的信任的所有伙伴应用(即，将使用直接信任的所有伙伴应用)。在某些实施例中，不在配置数据中存储发放者标识符但改为仅存储密钥及它们的标识符的应用可能无法构造发放者列表。

[0047] 在一个实施例中，如果发放者列表无法由应用构造，则在这种情况下应用返回其标识符(例如，client_id)和领域。Realm值可以是承租人标识符。如果构造了发放者列表，或者在领域可以从产生401响应的应用的端点URL中明白地确定的情况下，则领域是可任选的，并且通常在应用之间采用直接信任(即非STS)的纯场所内部署中提供。

[0048] 例如，请求可被格式化为

[0049] POST/resource HTTP/1.1

[0050] Authorization:Bearer

[0051] 401响应在“WWW-Authenticate”头部中的“Bearer”认证方案的“trusted_issuers”参数中携带如下的用逗号分隔的发放者列表：

[0052] HTTP/1.1401Unauthorized(未经授权的)

[0053] WWW-Authenticate:Bearer trusted_issuers="PIDsts@*,PIDapp@realm",realm="realm",client_id="PID"

[0054] 场所内安装可在元数据文档中发布PID、领域、和证书以便于在没有STS的场所内安装之间建立直接信任。对于在线安装，发布是不需要的。

[0055] 出站令牌的构造

[0056] 图3A和3B是示出一种用于为使用发放者匹配来选择出站令牌的发放者的应用构造出站令牌的方法或过程300的流程图。过程300具有以下输入参数：

[0057] 具有user@user-domain格式的用户或其他URI；

[0058] 伙伴应用标识符(PIDpa)；

[0059] 目的地主机(pahost);

[0060] 仅用于在线配置的承租人ID(tid);以及

[0061] 出站STS列表,其包括全局STS以及具体承租人的条目(仅在线)。

[0062] 在步骤301中,应用确定trusted_issuers参数是否被包括在对失败请求的答复中接收到的401响应中,其中该请求具有"Bearer"方案。在步骤302中,应用从401响应消息中的WWW-Authenticate头部的trusted_issuers参数获得发放者列表(即,传入发放者列表)。如果trusted_issuers参数未出现在401响应消息中的WWW-Authenticate头部中,则该过程移动至312。

[0063] 在步骤303中,应用确定传入发放者列表中的发放者之一是否匹配本地应用发放者标识符(PIDapp@realm)。在一个实施例中,所有的PID和领域组件必须在传入列表上的发放者和本地应用发放者标识符之间准确匹配。

[0064] 如果PID和领域组件在步骤303中匹配,则该过程移动至步骤304以创建自发放令牌。自发放令牌包括以下元素:

[0065] iss:PIDapp@realm;

[0066] nameid:PIDapp@realm;以及

[0067] aud:PIDpa@target-realm/pahost@user-domain.

[0068] iss(发放者)和nameid(名称标识符)元素对应于本地应用发放者标识符。aud(听众)元素基于伙伴应用的ID(PIDpa)、目的地主机(pahost)、和用户域(user-domain)来构造。target-realm字段是应用中服务试图呼叫的领域。

[0069] 如果在步骤303中没有与本地应用发放者标识符的匹配,则该过程移动至步骤305。在步骤305中,应用确定传入发放者列表中的发放者之一是否匹配仅使用PIDsts的经配置的STS之一,即GUID表示STS。应用对于这一匹配忽略领域参数。如果在步骤305中存在匹配,则在步骤306中,应用确定经匹配的STS配置条目是否具有空TID。

[0070] 在步骤307中,如果经匹配的STS配置条目包含非空TID,则应用在构造STS的令牌时将来自匹配STS条目的TID用作领域参数。或者,在步骤308中,如果匹配STS配置条目具有空TID,则应用在构造STS的令牌时将来自上述输入参数的承租人ID用作领域参数。

[0071] 在步骤309中,应用为STS创建自发放令牌。STS的自发放令牌包括以下参数:

[0072] iss:PIDapp@tid;

[0073] nameid:PIDapp@tid;

[0074] aud:PIDsts@tid/pahost@user-domain;以及

[0075] resource:PIDpa@target-realm/pahost@user-domain.

[0076] iss/nameid PID元素(PIDapp)来自应用发放者标识符。领域元素(tid)从步骤307/308中选择,并且或基于经配置的STS TID或基于来自上述的输入参数的承租人ID。aud PID元素(PIDsts)来自STS配置条目。resource元素基于伙伴应用的ID(PIDpa)和user-domain(用户-域)来构造。

[0077] 自发放令牌随后被提供给STS,STS在步骤310中使用以下参数来生成令牌:

[0078] iss:PIDsts@tid;

[0079] nameid:PIDapp@tid;以及

[0080] aud:PIDpa@tid/desthost@tid

[0081] STS为iss元素使用它自己的发放者@tenant ID(承租人ID)。nameid元素被确认有效并且从自发放令牌被复制。aud元素被确认有效并且从请求参数的令牌的资源元素被复制。如果领域作为DNS域来提供,则用实际的承租人ID来替换它。如果领域作为承租人id来提供,则不需要替换。

[0082] 如果在步骤303和305中不存在匹配,则令牌无法被创建并且该过程在步骤311中结束。

[0083] 如果在步骤301中在401响应中不存在trusted_isssuers参数,则该过程移动至步骤312。

[0084] 在步骤312,应用确定在401响应的WWW-Authenticate头部中是否存在领域参数。在步骤313中,应用确定401响应中的用“@”和领域值串接的伙伴应用标识符(例如,PIDpa@realm)是否准确匹配经配置的伙伴应用之一。如果在步骤313中PIDpa@realm准确匹配经配置的伙伴应用之一并且直接信任被配置,则在步骤314中应用创建自发放令牌。自发放令牌使用以下参数来格式化:

[0085] iss:PIDapp@realm;

[0086] nameid:PIDapp@realm;以及

[0087] aud:PIDpa@realm/pahost@realm.

[0088] iss和nameid元素(PIDapp@realm)对应于本地应用发放者标识符。aud元素基于伙伴应用的ID(PIDpa)和401响应中返回的领域值来构造。

[0089] 如果在步骤313中在PIDpa@realm和经配置的伙伴应用之一之间不存在匹 配,则该过程移动至步骤315。在步骤315中,应用确定401响应中返回的领域值是否准确匹配任何经配置的STS的领域。

[0090] 如果在步骤315中不存在准确匹配,则在步骤316中应用选择具有空领域的STS配置。

[0091] 如果在步骤315或316中存在匹配,则在步骤317中,应用确定经匹配的STS配置条目是否包含空TID。如果经匹配的STS配置条目包含非空TID,则在步骤318中,应用将来自经匹配的STS配置的TID用作领域来构造STS的自发放令牌。如果经匹配的STS配置条目具有空/“*”领域,则在步骤319中,应用使用来自上述的输入参数的领域[TID]来构造STS的自发放令牌。自发放令牌具有以下参数:

[0092] iss:PIDapp@tid;

[0093] nameid:PIDapp@tid;

[0094] aud:PIDsts@tid/stshost@tid;以及

[0095] resource:PIDpa@target-realm/pahost@user-domain.

[0096] iss和nameid元素PID(PIDapp)来自应用发放者标识符。aud元素PID(PIDsts)来自STS配置条目。iss、nameid和aud元素的领域(tid)基于经配置的STS TID或来自输入参数的承租人ID来选择。stshost元素来自STS元数据文档中的发放者端点,resource元素基于伙伴应用的ID(PIDpa)和user-domain来构造。

[0097] 来自步骤318或319的自发放令牌随后被提供给STS,STS在步骤320中使用以下参数来生成令牌:

[0098] iss:PIDsts@tid;

[0099] nameid:PIDapp@tid;以及

[0100] aud:PIDpa@tid/desthost@tid.

[0101] STS为iss元素使用它自己的发放者@tenant ID(承租人ID)。nameid元素被确认有效并且从自发放令牌被复制。aud元素被确认有效并且从自发放令牌的资源元素被复制。如果DNS域被提供,则DNS领域用实际的承租人ID(tid)来替换。否则,如果承租人id被提供,则不需要替换。

[0102] 如果图3A和3B的步骤未得到任何匹配,则该过程停止并且令牌无法被创建。

[0103] 对于使用单个出站发放者的应用,则应用应该仅使用该发放者来使用步骤317-320来产生令牌。

[0104] 入站令牌的确认

[0105] 如果应用实现基于发放者标识符的令牌确认,则应用获得发放者标识符并且定位令牌签名确认的证书。应用对照其STS列表来匹配发放者,该STS列表是应用的全局配置的一部分。发放者中的PID应该准确匹配STS配置。领域应该仅在它在STS配置条目中被指定时(即,不为空)匹配。如果STS配置条目具有空领域或“*”,则发放者标识符中的领域值必须是有效的承租人ID。

[0106] 令牌可对照具有直接信任的伙伴应用的列表来匹配。具有直接信任的应用列表来自应用的全局配置。在某些实施例中,直接信任可包括来自承租人配置的应用。承租人基于令牌的听众(aud:)字段中的领域来查找。在一个实施例中,所有字段(PID@realm)必须准确匹配以用于直接信任并且不允许通配符匹配。令牌中的名称标识符的PID和领域必须与发放者的PID和领域相同。

[0107] 如果不存在匹配,则应用拒绝该令牌。否则,应用可检索证书。证书可以从与STS或伙伴应用相关联的元数据文档获得。或者,也允许证书的直接配置。

[0108] 如果应用实现基于密钥标识符的令牌确认,则应用获得诸如来自令牌的证书拇指纹之类的密钥标识符,并且对照配置中的所有有效密钥标识符来匹配它。如果不存在匹配,则应用拒绝该令牌。否则,应用可从与密钥相关联的元数据文档中检索证书,或者可配置证书本身。

[0109] 应用使用检索到的证书来确认令牌签名。

[0110] 在一个实施例中,应用获得名称标识符并且将其对照伙伴应用列表来匹配。PID应该准确匹配。领域应该仅在它在伙伴应用配置条目中被指定时(即,不为空)匹配。如果伙伴应用配置条目具有空领域,则名称标识符的领域必须与发放者的领域相同。

[0111] 应用获得听众并且匹配其字段。PID应该准确匹配本地应用PID以及应用通过它被访问的主机名。对于STS-发放的令牌,领域应该匹配发放者(承租人ID)的领域。对于应用-发放的令牌,领域应该匹配本地配置的全局或承租人域之一。对于在线或多承租人环境,领域应该是有效承租人ID或解析到有效承租人的域。

[0112] 将理解,如此处所述的令牌的构造和确认可由两个或更多参与者来使用,所述参与者可包括应用、服务器、服务、设备、产品等。参与者可被配置成标识经配置的STS、伙伴应用和受信任的发放者。参与者随后如上所述地创建、交换和确认 令牌。

[0113] 可以理解,图2中所示的过程的步骤201-206和图3中所示的过程的步骤301-320可被同时和/或顺序执行。还可以理解,每个步骤可以按任何顺序执行,且可被执行一次或重

复执行。

[0114] 图4显示了在其上面可以实现图1-3的示例的适当的计算和网络环境400的示例。认证服务、此处描述的用于获得认证凭证的服务和应用可被实现在计算机系统400上。计算系统环境400只是合适计算环境的一个示例，而非意在暗示对本发明使用范围或功能有任何限制。本发明可用各种其他通用或专用计算系统环境或配置来操作。适用于本发明的公知计算系统、环境、和/或配置的示例包括但不限于：个人计算机、服务器计算机、手持式或膝上型设备、平板设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络PC、微型计算机、大型计算机、包括任何以上系统或设备的分布式计算环境等等。

[0115] 本发明可在诸如程序模块等由计算机执行的计算机可执行指令的通用上下文中描述。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。本发明也可以在其中任务由通过通信网络链接的远程处理设备执行的分布式计算环境中实现。在分布式计算环境中，程序模块可以位于包括存储器存储设备在内的本地和/或远程计算机存储介质中。

[0116] 参看图4，用于实现本发明的各个方面的示例性系统可以包括计算机400形式的通用计算设备。组件可以包括，但不限于，处理单元408、诸如系统存储器等数据存储402、以及将包括数据存储402的各种系统组件耦合到处理单元408的系统总线403。系统总线403可以是若干类型的总线结构中的任一种，包括使用各种总线体系结构中的任一种的存储器总线或存储器控制器、外围总线、以及局部总线。作为示例而非限制，这样的架构包括工业标准架构(ISA)总线、微通道架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线、以及也称为夹层(Mezzanine)总线的外围组件互连(PCI)总线。

[0117] 计算机400通常包括各种计算机可读介质404。计算机可读介质404可以是能由计算机400访问的任何可用介质，并同时包含易失性和非易失性介质以及可移动、不可移动介质，但不包括传播信号。作为示例而非限制，计算机可读介质404可包括计算机存储介质和通信介质。计算机存储介质包括以存储诸如计算机可读的 指令、数据结构、程序模块或其他数据之类的信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括，但不仅限于，RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁带盒、磁带、磁盘存储或其他磁存储设备，或可以用来存储所需信息并可以被计算机400访问的任何其他介质。通信介质通常以诸如载波或其他传输机制之类的已调制数据信号来体现计算机可读指令、数据结构、程序模块或其他数据，并且包括任何信息传送介质。术语“已调制数据信号”是指使得以在信号中编码信息的方式来设定或改变其一个或多个特征的信号。作为示例而非限制，通信介质包括诸如有线网络或直接线连接之类的有线介质，以及诸如声学、RF、红外及其他无线介质之类的无线介质。上面各项中的任何项的组合也包括在计算机可读介质的范围内。计算机可读介质可被实现为计算机程序产品，诸如存储在计算机存储介质上的软件。

[0118] 数据存储或系统存储器402包括诸如只读存储器(ROM)和/或随机存取存储器(RAM)之类的易失性和/或非易失性存储器形式的计算机存储介质。基本输入/输出系统(BIOS)包含有助于诸如启动时在计算机400中元件之间传递信息的基本例程，它通常被存储在ROM中。RAM通常包含处理单元408可立即访问和/或当前正在操作的数据和/或程序模块。作为示例而非限制性，存储器402保存操作系统、应用程序、其他程序模块、和程序数据。

[0119] 数据存储402还可以包括其它可移动/不可移动、易失性/非易失性计算机存储介质。仅作为示例，数据存储402可以是对不可移动、非易失性磁介质进行读写的硬盘驱动器，对可移动、非易失性磁盘进行读写的磁盘驱动器，以及对诸如CD ROM或其它光学介质等可移动、非易失性光盘进行读写的光盘驱动器。可在示例性操作环境中使用的其他可移动/不可移动、易失性/非易失性计算机存储介质包括但不限于，磁带盒、闪存卡、数字多功能盘、数字录像带、固态RAM、固态ROM等。上文所描述的并且在图4中所显示的驱动器以及它们的关联的计算机存储介质，为计算机400提供对计算机可读取的指令、数据结构、程序模块及其他数据的存储。

[0120] 用户可通过用户接口405或诸如平板、电子数字化仪、话筒、键盘和/或定点设备(通常指的是鼠标、跟踪球或触摸垫)等其它输入设备输入命令和信息。其他 输入设备可以包括操纵杆、游戏垫、圆盘式卫星天线、扫描仪等等。另外，可使用语音输入或自然用户界面(NUI)。这些及其他输入设备常常通过耦合到系统总线403的用户输入接口405连接到处理单元408，但是，也可以通过其他接口和总线结构，如并行端口、游戏端口或通用串行总线(USB)，来进行连接。监视器406或其他类型的显示设备也通过诸如视频接口之类的接口连接至系统总线403。监视器406也可以与触摸屏面板等集成。注意到监视器和/或触摸屏面板可以在物理上耦合至其中包括计算设备400的外壳，诸如在平板型个人计算机中。此外，诸如计算设备400等计算机还可以包括其他外围输出设备，诸如扬声器和打印机，它们可以通过输出外围接口等连接。

[0121] 计算机400可使用至一个或多个远程计算机(如远程计算机)的逻辑连接407在网络化环境中操作。例如，认证服务、服务和应用可经由网络连接通信以获得认证凭证。远程计算机可以是个人计算机、服务器、路由器、网络PC、对等设备或其它常见的网络节点，并且一般包括上面相对于计算机400所述的许多或全部元件。图4中所描述的逻辑连接包括一个或多个局域网(LAN)和一个或多个广域网(WAN)，但是，也可以包括其他网络。此类联网环境在办公室、企业范围的计算机网络、内联网和因特网中是常见的。

[0122] 当在LAN网络环境中使用时，计算机400通过网络接口或适配器407连接至LAN。当在WAN联网环境中使用时，计算机400通常包括调制解调器或用于通过诸如因特网等的WAN建立通信的其它装置。调制解调器可以是内置或外置的，它经由网络接口407或其它适当的机制连接至系统总线403。诸如包括接口和天线的无线联网组件可通过诸如接入点或对等计算机等合适的设备耦合到WAN或LAN。在联网环境中，相对于计算机400所示的程序模块或其部分可被存储在远程存储器存储设备中。可以理解，所示的网络连接是示例性的，也可以使用在计算机之间建立通信链路的其他手段。

[0123] 尽管用结构特征和/或方法动作专用的语言描述了本主题，但可以理解，所附权利要求书中定义的主题不必限于上述具体特征或动作。更确切而言，上述具体特征和动作是作为实现权利要求的示例形式公开的。

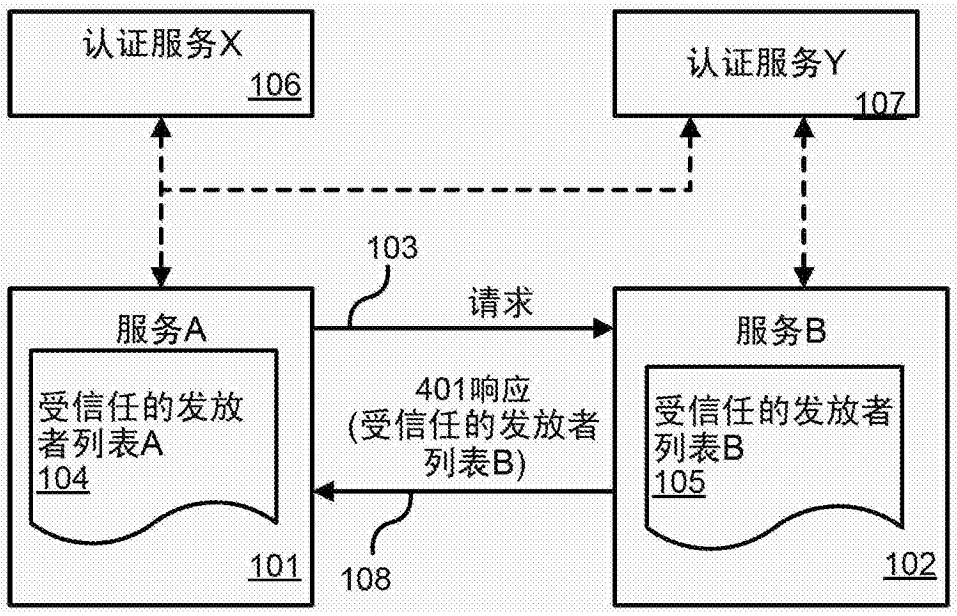

认证服务X
106
认证服务Y
107
103
请求
服务A
服务B
受信任的发放者列表A
104
401响应
(受信任的发放者列表B)
受信任的发放者列表B
105
101
108
102

图1

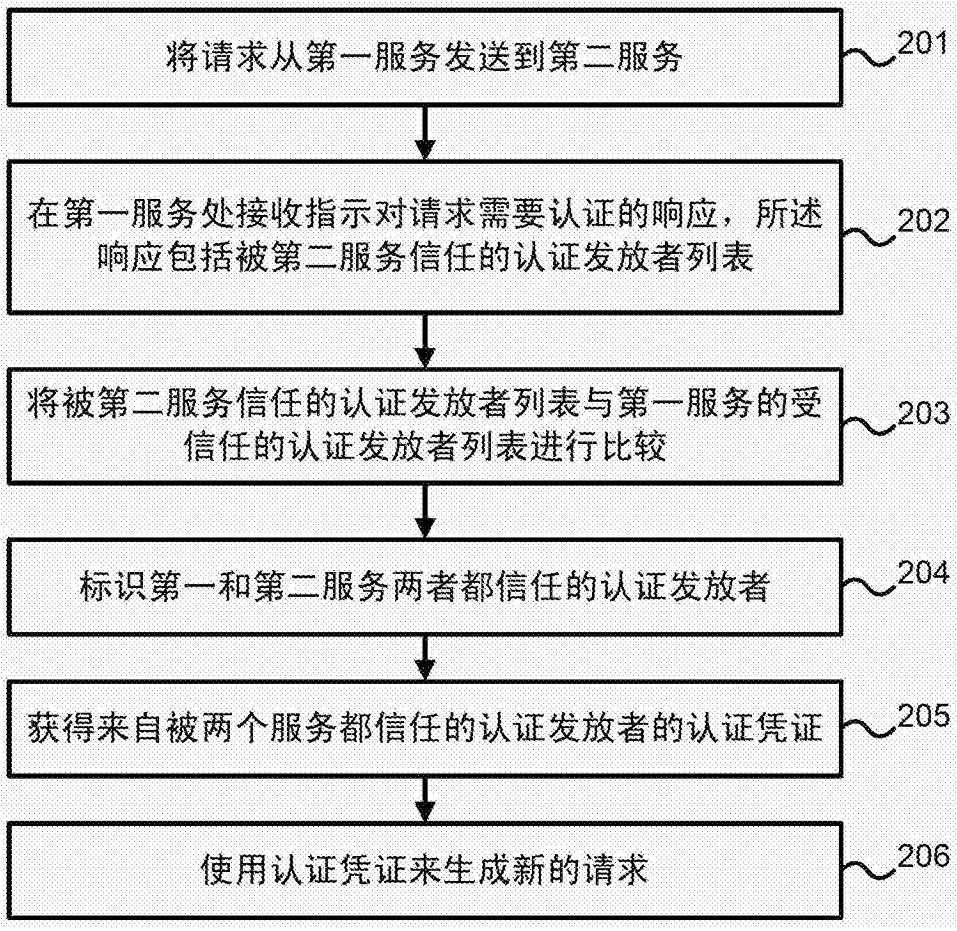

将请求从第一服务发送到第二服务
201
在第一服务处接收指示对请求需要认证的响应，所述响应包括被第二服务信任的认证发放者列表
202
将被第二服务信任的认证发放者列表与第一服务的受信任的认证发放者列表进行比较
203
标识第一和第二服务两者都信任的认证发放者
204
获得来自被两个服务都信任的认证发放者的认证凭证
205
使用认证凭证来生成新的请求
206

图2

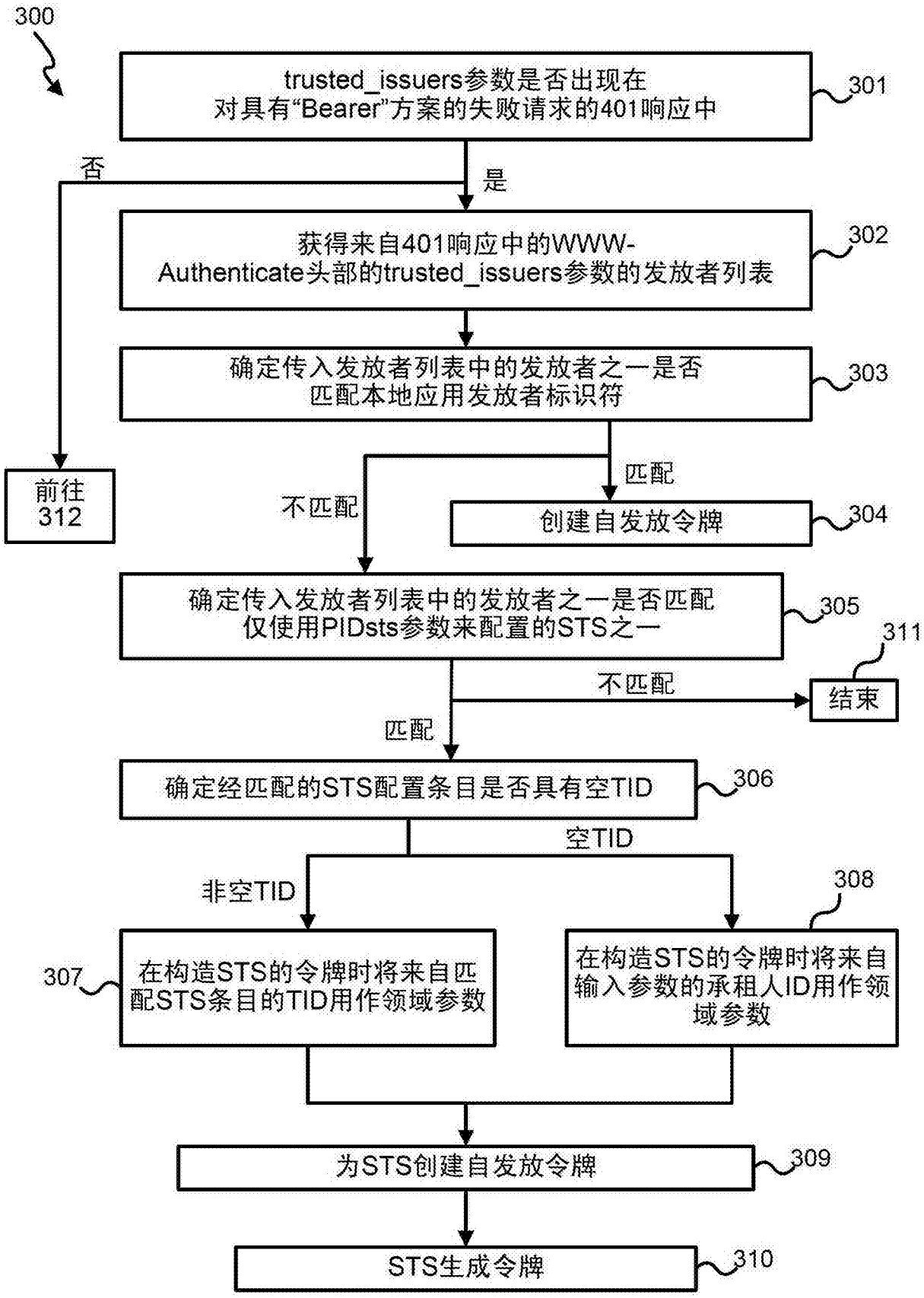

300
trusted_issuers参数是否出现在
对具有“Bearer”方案的失败请求的401响应中
301
否
是
获得来自401响应中的WWW-
Authenticate头部的trusted_issuers参数的发放者列表
302
确定传入发放者列表中的发放者之一是否
匹配本地应用发放者标识符
303
前往
312
不匹配
匹配
创建自发放令牌
304
确定传入发放者列表中的发放者之一是否匹配
仅使用PIDsts参数来配置的STS之一
305
311
不匹配
结束
匹配
确定经匹配的STS配置条目是否具有空TID
306
空TID
非空TID
308
307
在构造STS的令牌时将来自匹
配STS条目的TID用作领域参数
在构造STS的令牌时将来自
输入参数的承租人ID用作领
域参数
为STS创建自发放令牌
309
STS生成令牌
310

图3A

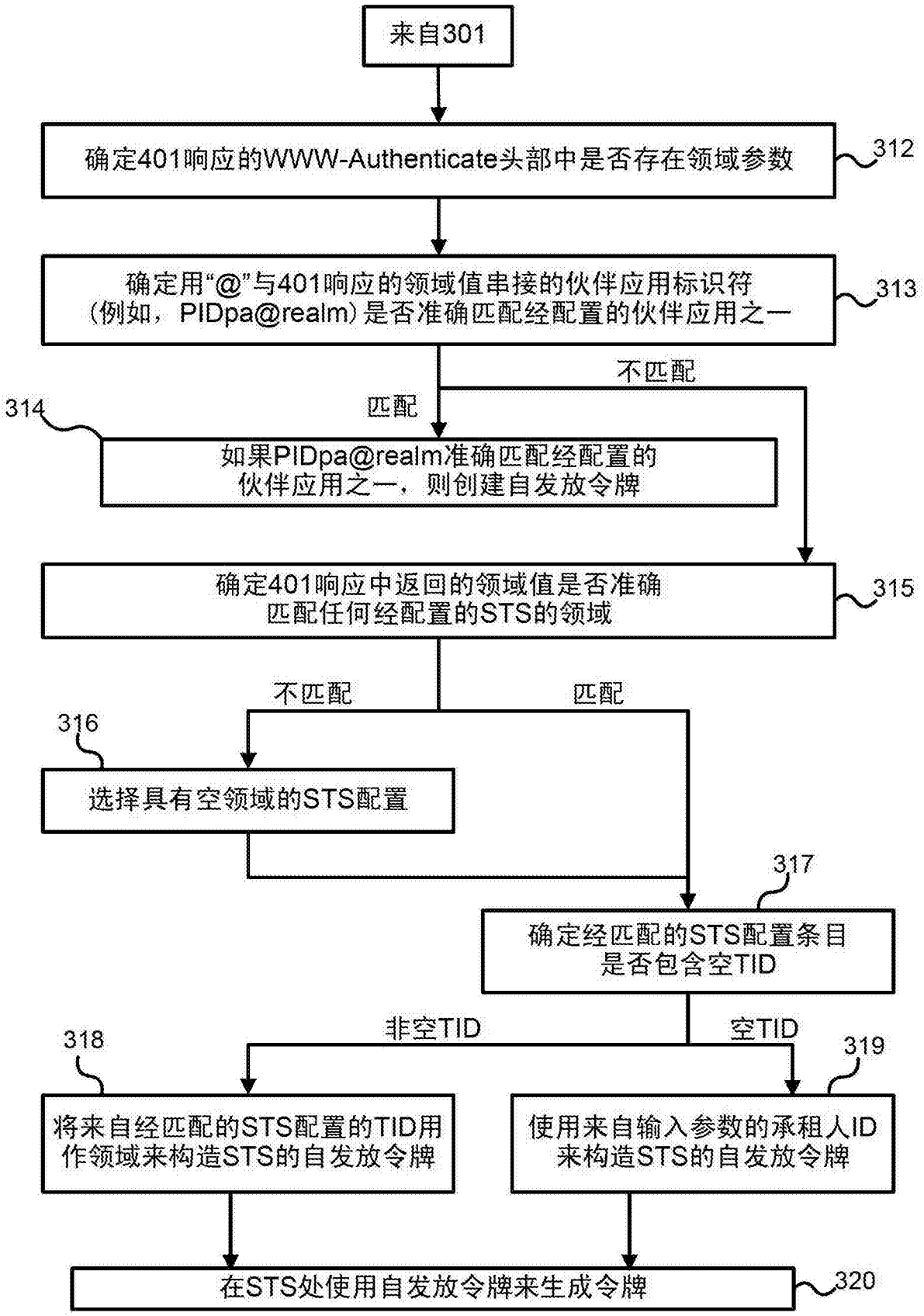

来自301
确定401响应的WWW-Authenticate头部中是否存在领域参数
312
确定用“@”与401响应的领域值串接的伙伴应用标识符（例如，PIDpa@realm）是否准确匹配经配置的伙伴应用之一
313
不匹配
匹配
314
如果PIDpa@realm准确匹配经配置的伙伴应用之一，则创建自发放令牌
确定401响应中返回的领域值是否准确匹配任何经配置的STS的领域
315
不匹配
匹配
316
选择具有空领域的STS配置
317
确定经匹配的STS配置条目是否包含空TID
非空TID
空TID
318
319
将来自经匹配的STS配置的TID用作领域来构造STS的自发放令牌
使用来自输入参数的承租人ID来构造STS的自发放令牌
在STS处使用自发放令牌来生成令牌
320

图3B

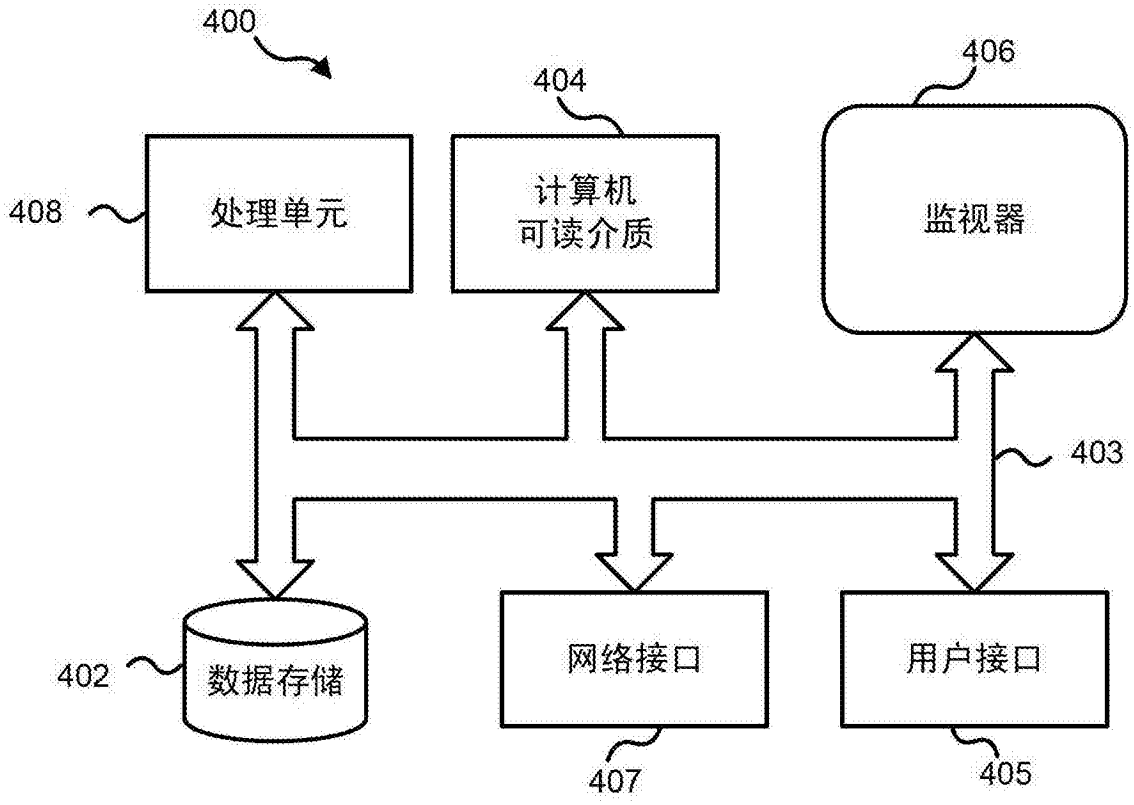

400
404
406
408
处理单元
计算机
可读介质
监视器
403
402
数据存储
网络接口
用户接口
407
405

图4