(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 10 月 30 日 (30.10.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/173278 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2014/075883

(22) 国际申请日: 2014 年 4 月 22 日 (22.04.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310139856.2 2013 年 4 月 22 日 (22.04.2013) CN

(71) 申请人: **中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.)** [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: **柴洪峰 (CHAI, Hongfeng)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **吴承荣 (WU, Chengrong)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **何朔 (HE, Shuo)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **叶家炜 (YE, Jiawei)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **杨阳 (YANG, Yang)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **王国平 (WANG, Guoping)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: **中国专利代理（香港）有限公司 (CHINA PATENT AGENT (HK) LTD.)**; 中国香港特别行政区香港湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (CN)。

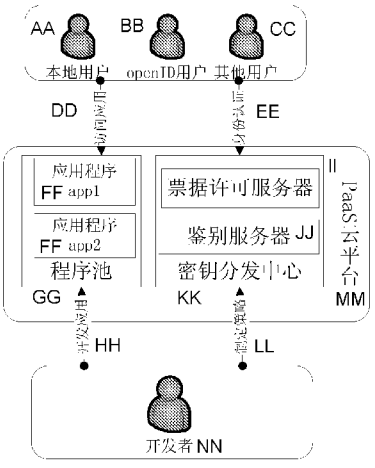
(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,

[见续页]

(54) Title: IDENTITY AUTHENTICATION METHOD AND IDENTITY AUTHENTICATION DEVICE BASED ON PAAS PLATFORM

(54) 发明名称 : 基于 PaaS 平台的身份认证方法以及身份认证设备



AA Local user
BB Open ID user
CC Another user
DD Application access
EE Identity authentication
FF Application program
GG Program pool
HH Application development
II Note permission server
JJ Authentication server
KK Key distribution center
LL Policy formulating
MM PaaS cloud platform
NN Developer

图 1 /Fig.1

(57) Abstract: Disclosed is an identity authentication device on a Platform-as-a-Service (PaaS) platform. The identity authentication device is used for performing identity authentication on a user that is prepared to access an application on the PaaS platform, and the identity authentication device comprises: a key distribution center, used for authenticating the user and distributing a note according to an access policy formulated by a developer of the application on the PaaS platform, and the key distribution center comprising an authentication server, the authentication server being configured to receive an authentication request from the user; determining a protocol that the identity of the user belongs to; and determining an authentication manner for the user according to the protocol, and sending a first permission note to the user after the authentication succeeds. Further disclosed is an identity authentication method based on a PaaS platform.

(57) 摘要:

[见续页]

WO 2014/173278 A1

BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种平台即服务（PaaS）平台上的身份认证设备，所述身份认证设备用于对准备访问所述 PaaS 平台上的应用的用户进行身份认证，所述身份认证设备包括：密钥分发中心，用于根据 PaaS 平台上的应用的开发者所制定的访问策略对用户进行认证并分发票据，其中所述密钥分发中心包括鉴别服务器，所述鉴别服务器配置成接收来自所述用户的验证请求；确定所述用户的身份所属的协议；根据所述协议来确定所述用户的验证方式以及在验证成功后向所述用户发送第一许可票据。本发明还公开了一种基于 PaaS 平台的身份认证方法。

基于 PaaS 平台的身份认证方法以及身份认证设备

技术领域

本发明涉及云计算安全领域，特别涉及一种基于 PaaS 平台的身份认证方法以及身份认证设备。

背景技术

PaaS 是 Platform-as-a-Service 的缩写，意思是平台即服务，把服务器平台作为一种服务提供的模式。通过网络进行程序提供的服务称之为 SaaS(Software as a Service)，而云计算时代相应的服务器平台或者开发环境作为服务进行提供就成为了 PaaS。

开发者在利用 PaaS 进行开发、部署其应用时，往往希望调用 PaaS 来提供接口，以便对用户进行身份认证，即提供类似 IPMaaS(Identity and Policy Management as a Service)服务。但是，PaaS 提供的认证服务的现状却不尽如人意。对于 PaaS 服务提供商而言，其提供的认证服务目前还不能同时兼容用户的多种身份，例如本地身份(即在 PaaS 平台上注册的身份)以及 OpenID 身份。除此之外，还存在着用户需多次进行认证，同一开发者的不同应用之间认证协同度不够的问题。

发明内容

为解决上述问题，根据本发明的一个方面，提供了一种基于 PaaS 平台的身份认证方法，包括：接收来自使用所述 PaaS 平台的用户的验证请求；确定所述用户的身份所属的协议；以及根据所述协议来确定所述用户的验证方式。

上述身份认证方法还可包括：在验证成功后向所述用户发送第一许可票据。

上述身份认证方法还可包括：从所述用户接收针对 PaaS 平台中的第一应用的票据请求，所述票据请求中包含所述第一许可票据；向所述用户发送针对所述第一应用的第二许可票据，使得所述用户凭借此第二许可票据可获得所述第一应用的服务；从所述用户接收针对 PaaS 平台中的第二应用的票据请求，

所述票据请求中包含所述第一许可票据；以及向所述用户发送针对所述第二应用的第三许可票据，使得所述用户凭借此第三许可票据可获得所述第二应用的服务。

在上述身份认证方法中，所述第一许可票据为票据许可票据 TGT，所述第二许可票据和所述第三许可票据为服务许可票据。

在上述身份认证方法中，所述用户的身份所属的协议可以是 Kerberos 协议或 OpenID 协议。

在上述身份认证方法中，当确定所述用户的身份所属的协议是 OpenID 协议时，PaaS 平台中的鉴别服务器、OpenID 提供商以及所述用户三方依据 OpenID 的协议标准进行认证。

在上述身份认证方法中，所述用户和所述鉴别服务器利用 Diffie-Hellman 算法来计算共享的密钥。

根据本发明的另一个方面，提供了一种 PaaS 平台上的身份认证设备，所述身份认证设备用于对准备访问所述 PaaS 平台上的应用的用户进行身份认证，所述身份认证设备包括：密钥分发中心，用于根据 PaaS 平台上的应用的开发者所制定的访问策略对用户进行认证并分发票据，其中，所述密钥分发中心包括鉴别服务器，所述鉴别服务器配置成接收来自所述用户的验证请求；确定所述用户的身份所属的协议；根据所述协议来确定所述用户的验证方式以及在验证成功后向所述用户发送第一许可票据。

在上述身份认证设备中，所述密钥分发中心还包括：票据许可服务器，所述票据许可服务器配置成从所述用户接收针对 PaaS 平台中的第一应用的票据请求，所述票据请求中包含所述第一许可票据；向所述用户发送针对所述第一应用的第二许可票据，使得所述用户凭借此第二许可票据可获得所述第一应用的服务。所述票据许可服务器可进一步配置成从所述用户接收针对 PaaS 平台中的第二应用的票据请求，所述票据请求中包含所述第一许可票据；以及向所述用户发送针对所述第二应用的第三许可票据，使得所述用户凭借此第三许可票据可获得所述第二应用的服务。

在上述身份认证设备中，所述第一许可票据为票据许可票据 TGT，所述第二许可票据和所述第三许可票据为服务许可票据。

在上述身份认证设备中，所述用户的身份所属的协议可以是 Kerberos 协议或 OpenID 协议。

在上述身份认证设备中，当所述鉴别服务器确定所述用户的身份所属的协议是 OpenID 协议时，所述鉴别服务器、OpenID 提供商以及所述用户三方依据 OpenID 的协议标准进行认证。

在上述身份认证设备中，所述用户和所述鉴别服务器利用 Diffie-Hellman 算法来计算共享的密钥。

上述基于PaaS平台的身份认证方法和身份认证设备使PaaS服务提供商为其上的应用程序提供高效灵活的身份认证服务。该身份认证方法和设备能低代价地满足同一开发者开发多个相对独立的、但却又相同/相近身份认证的需求。并且，该身份认证方法和设备可兼容本地身份以及代表联合身份认证趋势的 OpenID 身份，并有很好的扩展性以兼容更多类别的身份。整个认证过程可达到 Kerberos 协议相似的低认证次数效果。

附图说明

在参照附图阅读了本发明的具体实施方式以后，本领域技术人员将会更清楚地了解本发明的各个方面。本领域技术人员应当理解的是：这些附图仅仅用于配合具体实施方式说明本发明的技术方案，而并非意在对本发明的保护范围构成限制。

图 1 是根据本发明的一个实施例的身份认证服务模型的示意图；

图 2 是根据本发明的一个实施例、基于 PaaS 平台的身份认证方法的示意图。

具体实施方式

下面介绍的是本发明的多个可能实施例中的一些，旨在提供对本发明的基本了解，并不旨在确认本发明的关键或决定性的要素或限定所要保护的范围。容易理解，根据本发明的技术方案，在不变更本发明的实质精神下，本领域的一般技术人员可以提出可相互替换的其它实现方式。因此，以下具体实施方式以及附图仅是对本发明的技术方案的示例性说明，而不应当视为本发明的全部

或者视为对本发明技术方案的限定或限制。

对于 PaaS 而言，只支持本地身份的 PaaS 会在其业务拓展上遇到瓶颈。让用户省去注册的步骤并直接兼容用户已有身份是未来互联网发展的趋势，其中最有代表性的联合身份认证协议便是 OpenID。例如，登录一个支持 OpenID 的网站非常简单，只需要输入预先注册的 OpenID 用户名，然后登录的网站会跳转到 OpenID 服务网站。在 OpenID 服务网站内输入密码(或者其他需要填写的信息)验证通过后，跳转回登录的网站并且这时已经成功登录。OpenID 可应用于所有需要身份验证的地方，既可以应用于单点登录系统，也可以用于共享敏感数据时的身份认证。因而兼容本地身份以及 OpenID 身份(或其他身份)的 PaaS 是所希望的。

对于应用程序(Application, App)开发者而言，其在 PaaS 云平台上开发了自己应用程序，例如 App1 和 App2。应用程序在功能上相对独立，并且使用不同的语言开发，但通常其身份认证需求是相近的。随着身份种类的增多，身份认证问题变得越发复杂。开发者往往希望 PaaS 平台能够提供身份认证服务，以使得开发者只需简单调用 API 便能够对用户进行身份认证。作为举例，开发者可配置其应用程序的访问策略，例如：对于 App1，开发者希望只有本地身份才可以访问；对于 App2，开发者希望本地身份以及 OpenID 身份都可以访问。

对于使用开发者应用程序的用户而言，不管其拥有的身份如何，总希望在访问应用时减少认证次数。认证次数的减少意味着密钥使用频率的下降，这一点除了能够提高系统效率，还能够显著提高安全性。

为了兼容多种身份、满足 PaaS 上应用程序对身份认证的需求以及减少认证次数，本文提供了 PaaS 平台上的身份认证设备以及基于 PaaS 平台的身份认证方法。提供 PaaS 服务的云计算服务商可以使用这种身份认证设备和方法来为其上的应用提供高效、灵活、易扩展的身份认证服务。

图 1 示出了基于 PaaS 环境下的身份认证模型的示意图。该身份认证模型包括了三大部分：用户、开发者以及 PaaS 平台。以下依次对其进行简单的介绍。

如图 1 所示，用户(custom, C)包括本地用户、OpenID 用户以及其他用户。其中，本地用户指在 PaaS 平台注册的用户，OpenID 用户指根据 OpenID 协议

在某个 OpenID 提供商处注册的身份，而其他用户则是指扩展的其他多种身份的用户。

开发者是借助云平台开发应用 App 服务的人员，其可向 PaaS 平台制定其开发的应用程序的访问策略。

PaaS 云平台一方面对开发者提供 PaaS 服务以部署应用程序，另一方面对访问平台上的应用程序的用户进行身份验证。如图 1 所示，PaaS 云平台可包括程序池和密钥分发中心。

图 1 中的程序池仅示出有两个应用程序：第一应用程序(app1)和第二应用程序(app2)，但本领域技术人员应当理解，程序池中可包含更多或更少的程序，而不单单限于两个。

在一个具体的实施例中，本文所述的身份认证设备可通过 PaaS 平台上的密钥分发中心来实现。该密钥分发中心用于根据开发者的访问策略对用户进行认证并分发票据。

如图 1 所示，密钥分发中心可包括用于负责认证用户身份，并分发票据许可票据(Ticket Granting Ticket，TGT)的鉴别服务器(Authentication Server，AS)。在一个具体的实施例中，鉴别服务器可配置成接收来自用户的验证请求，确定用户的身份所属的协议，根据协议来确定用户的验证方式以及在验证成功后向用户发送票据许可票据。有必要指出的是，用户的身份所属的协议可以是 Kerberos 协议、OpenID 协议或其他扩展的协议。

继续参考图 1，密钥分发中心还可包括用于验证票据许可票据(TGT)并负责分发访问 App 的服务许可票据的票据许可服务器(Ticket Granting Server，TGS)。在一个具体的实施例中，票据许可服务器可配置成从用户接收针对 PaaS 平台中的第一应用程序(app1)的票据请求，该票据请求中包含票据许可票据；向用户发送针对第一应用程序的服务许可票据，使得用户凭借此服务许可票据可获得第一应用程序的服务。票据许可服务器可进一步配置成从用户接收针对 PaaS 平台中的第二应用程序(app2)的票据请求，该票据请求中同样包含票据许可票据；以及向用户发送针对第二应用程序的服务许可票据，使得用户凭借此服务许可票据可获得第二应用程序的服务。

表 1 示出了身份认证模型中的重要交互。

表 1

	PaaS 平台	
	程序池	密钥分发中心
开发者	开发者开发程序，程序部署在 PaaS 平台程序池中。	开发者根据需求制定用户访问其应用的策略，并把策略存至密钥分发中心。
用户	用户用持有的 TGT 访问程序。	认证用户，并根据开发者制定的策略分发票据 TGT。

用户认证是身份认证模型的核心部分。根据本发明的一个具体实施例，用户访问应用程序主要经过三大步骤。

第一步，鉴别访问交换：用户访问密钥分发中心的鉴别服务器以验证身份并获得票据许可票据，验证的方式根据其身份所属的协议不同而有所差异。第二步，票据许可服务交换：用户访问密钥分发中心的票据许可服务器，用票据许可票据换取服务许可票据。第三步，客户/服务器鉴别交换：用服务许可票据访问应用的服务。

在第一步鉴别访问交换中，用户既可以用本地身份登陆也可以使用 OpenID 身份登陆，随着系统的扩展还可以使用更多的其他身份登陆。如果使用本地身份，那么用户类似传统方式在 PaaS 服务商注册，此后用户和 AS 根据注册时创建的共享口令按照 Kerberos V5 的鉴别访问交换协议进行认证。如果使用 OpenID 身份，则用户和云平台的身份认证工作需要由 OpenID 提供商协助完成。Kerberos V5 协议的鉴别访问交换的前提是用户和鉴别服务器已共享密钥，而在 OpenID 协议中却是另一种场景。用户在 OpenID 提供商处注册 OpenID 身份，使得只有 OpenID 提供商拥有对用户进行认证的能力。此时用户访问作为 RP(Relying Party，依赖方)的 PaaS 服务商，RP 并没有和用户共享密钥。RP 对用户的身份认证必须依照 OpenID 协议引入 OpenID 提供商方的协助。基于上述考虑需要对 Kerberos 的鉴别访问交换进行修改，具体认证流程如下：

(1)用户利用 Diffie-Hellman 协议计算公私钥对；

(2)用户向鉴别服务器发送请求，请求中包括用户 ID 标识、票据许可服务

器标识、用户端时钟和用户方公钥；

(3)鉴别服务器、OpenID 提供商以及用户三方依据 OpenID 的协议标准进行认证，成功认证后鉴别服务器信任用户符合其声称的身份；

(4)鉴别服务器利用 Diffie-Hellman 协议计算公私钥对以及其与用户之间共享的密钥；

(5)鉴别服务器向用户发送票据许可票据，其中包含鉴别服务器方公钥，以及用鉴别服务器与用户之间共享的密钥加密的内容，该内容包括用户与票据许可服务器共享的密钥、票据许可服务器标识、服务许可票据的签发时间、服务许可票据的有效期、以及用户用来访问票据许可服务器的票据。其中，用户用来访问票据许可服务器的票据可进一步包括用票据许可服务器与鉴别服务器之间共享的永久密钥加密的第二内容。第二内容包括用户与票据许可服务器临时生成的共享密钥、用户 ID 标识、票据许可服务器标识、该票据的签发时间以及该票据的有效期。

在现有技术中，Kerberos 是一种多应用身份认证解决方案，但是其局限性在于 Kerberos 认证前假设每个用户的口令都已储存在认证服务器端，双方的认证是基于预共享口令，这点限制了 Kerberos 的应用。有必要指出的是，在本发明的实施例中，用户与鉴别服务器之间临时生成的共享密钥能有效弥补用户与鉴别服务器在传递请求之前没有共享密钥的问题，实现了保密性。

如果希望支持 PaaS 平台支持更多的身份以访问应用，只需根据身份所参照的协议修改鉴别访问交换阶段即可，这体现了本模型对于更多身份类别的可扩展性。

鉴别访问交换阶段结束后，用户得到了票据许可票据。

对于第二步票据许可服务交换，其实现的流程可如下所示：

(1)客户向票据许可服务器发送请求用于访问某个程序 V，该请求中包括应用程序 V 的标识、用户用来访问票据许可服务器的票据(该票据例如可从鉴别访问交换的第 5 步中获得)、由用户生成标识自身的内容，该内容包含用用户与票据许可服务器临时生成的共享密钥来对用户标识和用户申请服务许可票据的时间两者进行加密的内容；

(2)票据许可服务器向用户返回用以访问程序 V 的票据，该票据包括用用

户与票据许可服务器临时生成的共享密钥来对用户与应用程序之间的共享密钥、程序 V 的标识、该票据签发的时间以及用户用以访问应用程序 V 的票据进行加密的内容。用户用以访问应用程序 V 的票据可进一步包括用应用程序 V 的密钥对用户与应用程序 V 之间的共享密钥、用户标识、应用程序 V 标识以及该票据的签发时间进行加密的内容。

票据许可服务交换独立于鉴别服务器的鉴别过程。应用程序的开发者事先定义了访问的策略，并由票据许可服务器存储授权该策略。在票据许可服务交换阶段，票据许可服务器依据开发者定义的授权信息来分发具体应用的服务许可票据。

对于第三步用户/服务器鉴别交换，用户使用服务许可票据来访问应用程序 V。具体来说，用户向应用程序发送访问请求，其中包括服务许可票据以及用用户与应用程序之间的共享密钥对用户标识进行加密的内容。

图 2 中示出的基于 PaaS 平台的身份认证方法很好地展示了上述三大步骤。图 2 中示出的请求 TGT、身份认证、返回 TGT 步骤示意示出之前所述的鉴别访问阶段，图 2 中示出的请求 ticket、返回 ticket 步骤则示意示出了票据许可服务交换阶段。最后，图 2 中示出的访问应用步骤则属于用户/服务器鉴别交换阶段。

综上，采用本发明所述的基于 PaaS 平台的身份认证方法和身份认证设备可取得如下优点：

1)传统身份认证方式访问每个应用都需要独立的身份验证。本发明中 AS 和 TGS 的设计使得用户多次访问同一位开发者的不同 App 应用时无需反复进行身份认证。用户只需通过一次身份认证以获得 TGT，随后针对不同的 App 用 TGT 换取应用程序对应的 ticket，减少了用户口令的使用频度。

2)与现有的一些跨应用身份认证方式相比，兼容了本地身份以及 OpenID，并对其他的身份兼容也有很好的扩展性和灵活性。当系统需要支持更多的身份类别时，只需要在鉴别访问交换阶段增加认证方式。

3)本发明设计的 PaaS 的身份认证服务使得应用程序开发者从越发复杂的身份认证问题中解脱出来，能够专注于应用的开发。

4)最小化认证开销，减小了用户口令的使用频度，用户体验更加友好。

上文中，参照附图描述了本发明的具体实施方式。但是，本领域中的普通技术人员能够理解，在不偏离本发明的精神和范围的情况下，还可以对本发明的具体实施方式作各种变更和替换。这些变更和替换都落在本发明权利要求书所限定的范围内。

权利要求

1. 一种基于 PaaS 平台的身份认证方法，包括：

接收来自使用所述 PaaS 平台的用户的验证请求；

确定所述用户的身份所属的协议；以及

根据所述协议来确定所述用户的验证方式。

2. 如权利要求1所述的身份认证方法，还包括：

在验证成功后向所述用户发送第一许可票据。

3. 如权利要求2所述的身份认证方法，还包括：

从所述用户接收针对 PaaS 平台中的第一应用的票据请求，所述票据请求中包含所述第一许可票据；以及

向所述用户发送针对所述第一应用的第二许可票据，使得所述用户凭借此第二许可票据可获得所述第一应用的服务。

4. 如权利要求3所述的身份认证方法，进一步包括：

从所述用户接收针对 PaaS 平台中的第二应用的票据请求，所述票据请求中包含所述第一许可票据；以及

向所述用户发送针对所述第二应用的第三许可票据，使得所述用户凭借此第三许可票据可获得所述第二应用的服务。

5. 如权利要求2至4中任一项所述的身份认证方法，其中，所述第一许可票据为票据许可票据 TGT。

6. 如权利要求3所述的身份认证方法，其中，所述第二许可票据为服务许可票据。

7. 如权利要求4所述的身份认证方法，其中，所述第三许可票据为服务许可票据。

8. 如权利要求1所述的身份认证方法，其中，所述用户的身份所属的协议可以是 Kerberos 协议或 OpenID 协议。

9. 如权利要求8所述的身份认证方法，其中，当确定所述用户的身份所属的协议是 OpenID 协议时，PaaS 平台中的鉴别服务器、OpenID 提供商以及所述用户三方依据 OpenID 的协议标准进行认证。

10. 如权利要求9所述的身份认证方法，其中，所述用户和所述鉴别服务器利用 Diffie-Hellman 算法来计算共享的密钥。

11. 一种 PaaS 平台上的身份认证设备，所述身份认证设备用于对准备访问所述 PaaS 平台上的应用的用户进行身份认证，所述身份认证设备包括：

密钥分发中心，用于根据 PaaS 平台上的应用的开发者所制定的访问策略对用户进行认证并分发票据，其中，所述密钥分发中心包括鉴别服务器，所述鉴别服务器配置成接收来自所述用户的验证请求；确定所述用户的身份所属的协议；根据所述协议来确定所述用户的验证方式以及在验证成功后向所述用户发送第一许可票据。

12. 如权利要求11所述的身份认证设备，其中，所述密钥分发中心还包括：票据许可服务器，所述票据许可服务器配置成从所述用户接收针对 PaaS 平台中的第一应用的票据请求，所述票据请求中包含所述第一许可票据；向所述用户发送针对所述第一应用的第二许可票据，使得所述用户凭借此第二许可票据可获得所述第一应用的服务。

13. 如权利要求12所述的身份认证设备，其中，所述票据许可服务器还配置成从所述用户接收针对 PaaS 平台中的第二应用的票据请求，所述票据请求中包含所述第一许可票据；以及向所述用户发送针对所述第二应用的第三许可票据，使得所述用户凭借此第三许可票据可获得所述第二应用的服务。

14. 如权利要求11至13中的任一项所述的身份认证设备，其中，所述第一许可票据为票据许可票据 TGT。

15. 如权利要求12所述的身份认证设备，其中所述第二许可票据为服务许可票据。

16. 如权利要求13所述的身份认证设备，其中所述第三许可票据为服务许可票据。

17. 如权利要求11所述的身份认证设备，其中，所述用户的身份所属的协议可以是 Kerberos 协议或 OpenID 协议。

18. 如权利要求17所述的身份认证设备，其中，当所述鉴别服务器确定所述用户的身份所属的协议是 OpenID 协议时，所述鉴别服务器、OpenID 提供商以及所述用户三方依据 OpenID 的协议标准进行认证。

19. 如权利要求18所述的身份认证设备，其中，所述用户和所述鉴别服务器利用 Diffie-Hellman 算法来计算共享的密钥。

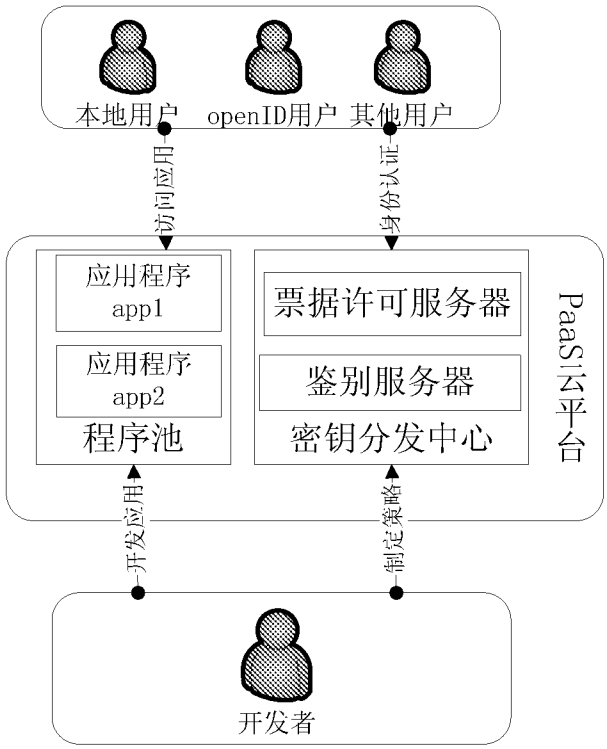

本地用户
openID用户
其他用户
访问应用
身份认证
应用程序
app1
应用程序
app2
程序池
票据许可服务器
鉴别服务器
密钥分发中心
PaaS云平台
开发应用
制定策略
开发者

图 1

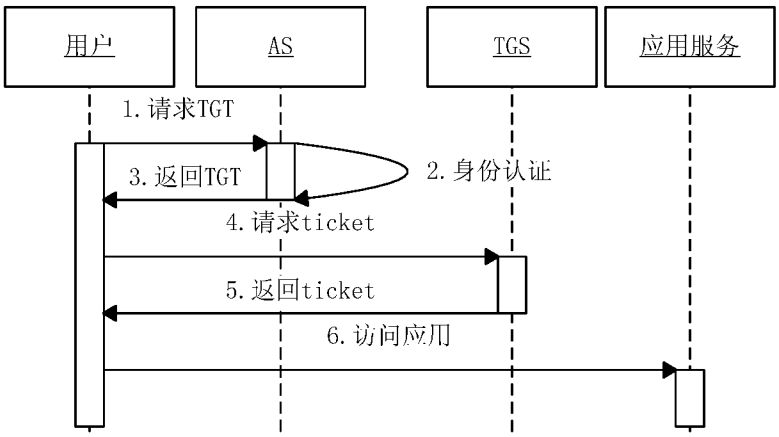

用户
AS
TGS
应用服务
1.请求TGT
3.返回TGT
2.身份认证
4.请求ticket
5.返回ticket
6.访问应用

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/075883

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04Q; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT; CNABS; VEN; CNKI: pass, ticket granting ticket, openID, kerberos, TGT, serv+, authenticat+, platform, log in, password, applicat+, request???, program, identity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102457376 A (ZTE CORPORATION) 16 May 2012 (16.05.2012) description, paragraphs [0059]-[0070] and figures 1-3	1-19
X	CN 102571948 A (G-CLOUD TECHNOLOGY CO., LTD.) 11 July 2012 (11.07.2012) description, paragraphs [0091]-[0103] and figure 3	1-19
A	US 2013007845 A1 (INT BUSINESS MACHINES CORP.) 03 January 2013 (03.01.2013) the whole document	1-19

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 July 2014	25 July 2014
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer ZHANG, Yaoyao Telephone No. (86-10) 62411326

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/075883

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102457376 A	16 May 2012	None	
CN 102571948 A	11 July 2012	None	
US 2013007845 A1	03 January 2013	WO 2013000080 A1	03 January 2013
		GB 2506564 A	02 April 2014
		DE 112012002741 T5	13 March 2014
		GB 201401348 D0	12 March 2014
		CN 103563294 A	05 February 2014

国际检索报告

国际申请号
PCT/CN2014/075883

A. 主题的分类

H04L 9/32 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04Q; H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNTXT;CNABS; VEN; CNKI:平台，服务，票据，认证，验证，密码，请求，应用，程序，身份，登录，登陆，pass，ticket granting ticket，openID，kerberos，TGT，serv+，authenticat+，platform，log in，password，applicat+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 102457376A (中兴通讯股份有限公司) 2012年 5月 16日 (2012-05-16) 说明书第[0059]-[0070]段，图1-3	1-19
X	CN 102571948A (国云科技股份有限公司) 2012年 7月 11日 (2012-07-11) 说明书第[0091]-[0103]段，图3	1-19
A	US 2013007845A1 (INT BUSINESS MACHINES CORP) 2013年 1月 03日 (2013-01-03) 全文	1-19

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2014年 7月 04日	2014年 7月 25日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国	张瑶瑶
传真号 (86-10)62019451	电话号码 (86-10)62411326

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/075883

检索报告引用的专利文件	公布日（年/月/日）	同族专利	公布日（年/月/日）
CN 102457376A	2012年 5月 16日	无	
CN 102571948A	2012年 7月 11日	无	
US 2013007845A1	2013年 1月 03日	WO 2013000080A1	2013年 1月 03日
		GB 2506564A	2014年 4月 02日
		DE 112012002741T5	2014年 3月 13日
		GB 201401348D0	2014年 3月 12日
		CN 103563294A	2014年 2月 05日