(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111431972 B
(45)授权公告日 2022.09.20

(21)申请号 202010147686.2

(22)申请日 2020.03.05

(65)同一申请的已公布的文献号
申请公布号 CN 111431972 A

(43)申请公布日 2020.07.17

(73)专利权人 北京龙归科技有限公司
地址 100085 北京市海淀区上地十街1号院6号楼2层209-266

(72)发明人 尹力炜 李新军 杨瀚

(74)专利代理机构 北京思创大成知识产权代理有限公司 11614
专利代理师 张立君

(51)Int.Cl.
H04L 67/51(2022.01)
H04L 67/56(2022.01)
H04L 9/40(2022.01)

(56)对比文件
CN 107786571 A,2018.03.09
CN 110035099 A,2019.07.19
CN 109472123 A,2019.03.15
CN 110740116 A,2020.01.31
CN 104994102 A,2015.10.21
CN 107147647 A,2017.09.08

审查员 李燕

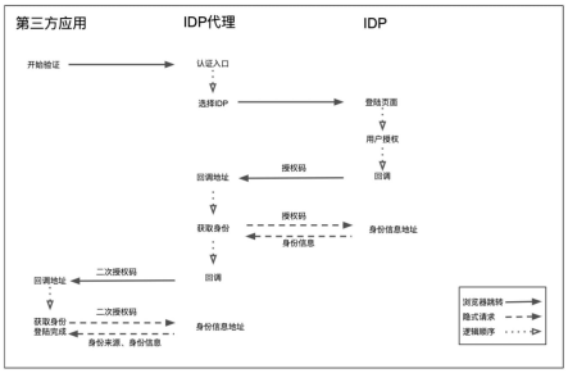
权利要求书2页 说明书5页 附图3页

(54)发明名称

基于IDP代理的应用授权方法、设备、存储介质及系统

(57)摘要

本发明公开了一种基于IDP代理的应用授权方法、设备、存储介质及系统。方法包括:提供IDP代理;将至少一个IDP服务和至少一个第三方应用在IDP代理中完成注册;将IDP代理的登录入口在第三方应用的登录页进行展示;IDP代理根据用户选择的IDP服务,跳转至所选IDP服务登录页面,申请获取所选IDP的授权,并将此授权转发给所述第三方应用,完成登录。能够让用户在使用多个第三方应用时可以通过统一的身份验证系统来登录,避免用户重复注册和登录操作。



CN 111431972 B

1.一种基于IDP代理的应用授权方法,其特征在于,包括:

提供IDP代理,所述IDP代理用于提供IDP服务的代理服务并与所述IDP服务和第三方应用通讯连接;

将至少一个IDP服务和至少一个第三方应用在所述IDP代理中完成注册,其中,所述IDP服务存储有用户信息,并能够提供登录页面,通过账号密码形式校验用户身份;所述IDP服务包括私有IDP和公有IDP,所述私有IDP在注册时,向所述IDP代理提供真实的网络地址,所述公有IDP在注册时,向所述IDP代理提供网络地址以及实际的IDP服务在所述公有IDP中的逻辑地址;

将所述IDP代理的登录入口在所述第三方应用的登录页进行展示,以供用户选择所述IDP代理中注册的IDP服务;

所述IDP代理根据用户选择的IDP服务,跳转至所选IDP服务的登录页面,申请获取所选IDP服务的授权,并将此授权转发给所述第三方应用,完成登录。

2.根据权利要求1所述的基于IDP代理的应用授权方法,其特征在于,将至少一个IDP服务和至少一个第三方应用在所述IDP代理中完成注册包括:

所述IDP代理记录所述IDP服务的网络地址并与所述IDP服务互换公钥;

所述IDP代理记录所述第三方应用的回调地址并与所述第三方应用互换公钥。

3.根据权利要求1所述的基于IDP代理的应用授权方法,其特征在于,所述IDP服务的所述网络地址包括IP地址和/或域名。

4.根据权利要求1所述的基于IDP代理的应用授权方法,其特征在于,在所述IDP代理中完成注册的每个所述IDP服务具有唯一的编号,用户选择所述IDP代理中注册的IDP服务包括:

用户输入所述IDP服务的编号并确认后,若编号或相似编号真实存在,则显示多个所述IDP服务供用户选择需要的一个IDP服务。

5.一种电子设备,其特征在于,所述电子设备包括:

至少一个处理器;以及,

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行权利要求1-4任一所述的基于IDP代理的应用授权方法。

6.一种非暂态计算机可读存储介质,其特征在于,该非暂态计算机可读存储介质存储计算机指令,该计算机指令用于使计算机执行权利要求1-4任一所述的基于IDP代理的应用授权方法。

7.一种基于IDP代理的应用授权系统,其特征在于,包括IDP代理、至少一个IDP服务和至少一个第三方应用,所述IDP服务和所述第三方应用均在所述IDP代理中完成注册并分别与所述IDP代理通讯连接;所述IDP服务包括私有IDP和公有IDP,所述私有IDP在注册时,向所述IDP代理提供真实的网络地址,所述公有IDP在注册时,向所述IDP代理提供网络地址以及实际的IDP服务在所述公有IDP中的逻辑地址;

所述第三方应用的登录页能够展示所述IDP代理的登录入口,以供用户选择所述IDP代理中注册的IDP服务;

所述IDP服务用于存储用户信息,并能够提供登录页面,通过账号密码形式校验用户身份,以及能够将登录用户的授权信息返回给所述IDP代理;

所述IDP代理,根据用户选择的IDP服务,跳转至所选IDP服务的登录页面,申请获取所选IDP的授权,并将此授权转发给所述第三方应用,完成登录。

8.根据权利要求7所述的基于IDP代理的应用授权系统,其特征在于,所述IDP服务和所述第三方应用均在所述IDP代理中完成注册包括:

所述IDP代理记录所述IDP服务的网络地址并与所述IDP服务互换公钥;

所述IDP代理记录所述第三方应用的回调地址并与所述第三方应用互换公钥。

9.根据权利要求8所述的基于IDP代理的应用授权系统,其特征在于,所述IDP代理中完成注册的每个所述IDP服务具有唯一的编号。

基于IDP代理的应用授权方法、设备、存储介质及系统

技术领域

[0001] 本发明涉及网络通信技术领域，更具体地，涉及一种基于IDP代理的应用授权方法、设备、存储介质及系统。

背景技术

[0002] 随着云技术的发展，越来越多的SaaS(Software-as-a-Service，第三方应用)服务被推广使用。

[0003] IDP(Identity Provider)，意为身份提供商。由IDP提供的身份凭证(账号与口令)可在IDP接入的第三方应用处直接使用，即为单点登录(Single Sign-On)。

[0004] 目前，不同的SaaS服务在企业或者个人使用的时候，都需要单独注册与登录，需要大量的沟通和开发工作，同时导致用户在使用每个SaaS服务时都需要进行重复的注册和登录操作，严重影响用户体验。

[0005] 因此需要提出一种应用授权方法，能够避免这种重复的注册登录行为，让多个第三方应用可以通过统一的身份验证方式进行登录。

发明内容

[0006] 本发明的目的是提出一种基于IDP代理的应用授权方法、设备、存储介质及系统，实现让多个第三方应用可以通过统一的身份验证方式进行登录。

[0007] 为实现上述目的，本发明提出了一种基于IDP代理的应用授权方法，包括：

[0008] 提供IDP代理，所述IDP代理用于提供IDP服务的代理服务并与所述 IDP服务和第三方应用通讯连接；

[0009] 将至少一个IDP服务和至少一个第三方应用在所述IDP代理中完成注册，其中，所述IDP服务存储有用户信息，并能够提供登录页面，通过账号密码形式校验用户身份；

[0010] 将所述IDP代理的登录入口在所述第三方应用的登录页进行展示，以供用户选择所述IDP代理中注册的IDP服务；

[0011] 所述IDP代理根据用户选择的IDP服务，跳转至所选IDP服务的登录页面，申请获取所选IDP服务的授权，并将此授权转发给所述第三方应用，完成登录。

[0012] 可选地，将至少一个IDP服务和至少一个第三方应用在所述IDP代理中完成注册包括：

[0013] 所述IDP代理记录所述IDP服务的网络地址并与所述IDP服务互换公钥；

[0014] 所述IDP代理记录所述第三方应用的回调地址并与所述第三方应用互换公钥。

[0015] 可选地，所述IDP服务包括私有IDP服务和公有IDP服务。

[0016] 可选地，所述IDP服务的所述网络地址包括IP地址和/或域名；

[0017] 可选地，在所述IDP代理中完成注册的每个所述IDP具有唯一的编号，用户选择所述IDP代理中注册的IDP服务包括：

[0018] 用户输入所述IDP的编号并确认后，若编号或相似编号真实存在，则显示多个所述

IDP服务供用户选择需要的一个IDP服务。

[0019] 本发明还提出一种电子设备,所述电子设备包括:

[0020] 至少一个处理器;以及,

[0021] 与所述至少一个处理器通信连接的存储器;其中,

[0022] 所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行上述的基于 IDP代理的应用授权方法。

[0023] 本发明还提出一种非暂态计算机可读存储介质,该非暂态计算机可读存储介质存储计算机指令,该计算机指令用于使计算机执行上述的基于IDP 代理的应用授权方法。

[0024] 本发明还提出一种基于IDP代理的应用授权系统,包括IDP代理、至少一个IDP服务和至少一个第三方应用,所述IDP服务和所述第三方应用均在所述IDP代理中完成注册并分别与所述IDP代理通讯连接;

[0025] 所述第三方应用的登录页能够展示所述IDP代理的登录入口,以供用户选择所述IDP代理中注册的IDP服务;

[0026] 所述IDP服务用于存储用户信息,并能够提供登录页面,通过账号密码形式校验用户身份,以及能够将登陆用户的授权返回给所述IDP代理;

[0027] 所述IDP代理,用于根据用户选择的IDP服务,跳转至所选IDP服务的登录页面,申请获取所选IDP的授权,并将此授权转发给所述第三方应用,完成登录。

[0028] 可选地,所述IDP服务和所述第三方应用均在所述IDP代理中完成注册包括:所述IDP代理记录所述IDP服务的网络地址并与所述IDP服务互换公钥;所述IDP代理记录所述第三方应用的回调地址并与所述第三方应用互换公钥。

[0029] 可选地,所述IDP服务包括私有IDP服务和公有IDP服务,且在所述 IDP代理中完成注册的每个所述IDP服务具有唯一的编号。

[0030] 本发明的有益效果在于:

[0031] 通过IDP代理的方式,IDP服务和第三方应用均能够在IDP代理处完成注册并分别与IDP代理建立通讯连接,使IDP服务可以迅速被已经接入 IDP代理的三方应用所使用,让用户在使用多个第三方应用时可以通过统一的身份验证系统来登录,避免了用户重复注册和登录操作,让企业或者个人在使用SaaS服务时看起来如同使用私有应用一样,大大减少了沟通、开发工作和用户的使用成本。

[0032] 本发明的装置具有其它的特性和优点,这些特性和优点从并入本文中的附图和随后的具体实施方式中将是显而易见的,或者将在并入本文中的附图和随后的具体实施方式中进行详细陈述,这些附图和具体实施方式共同用于解释本发明的特定原理。

附图说明

[0033] 通过结合附图对本发明示例性实施例进行更详细的描述,本发明的上述以及其它目的、特征和优势将变得更加明显,在本发明示例性实施例中,相同的参考标号通常代表相同部件。

[0034] 图1示出了现有的一种IDP服务对第三方应用完成授权的示意图。

[0035] 图2示出了根据本发明的一种基于IDP代理的应用授权方法的步骤图。

[0036] 图3示出了根据本发明的一个实施例的一种基于IDP代理的应用授权方法的授权

流程图。

[0037] 图4示出了根据本发明的一个实施例的一种基于IDP代理的应用授权系统的示意图。

具体实施方式

[0038] 参考图1,现有技术中,通过OAuth2.0协议实现IDP服务与三方应用分离的效果,例如微信就提供给其它第三方网站通过微信直接登录的方式,这里可以将微信看成是一个私有IDP服务,微信保存了用户的账号密码等信息,通过OAuth2.0协议,完成对第三方应用的授权。这里,微信是作为 IDP服务,第三方应用直接在微信的IDP上完成注册和对接。

[0039] 但是私有IDP服务本身可能往往并不稳定,当地址更换或者出现其它情况,该用户身份可能就会消失。

[0040] 因此本发明的方案通过IDP代理的方式,私有IDP服务可以迅速被已经接入IDP代理的第三方应用所使用,能够大大减少沟通和开发工作。

[0041] 下面将参照附图更详细地描述本发明。虽然附图中显示了本发明的优选实施例,然而应该理解,可以以各种形式实现本发明而不应被这里阐述的实施例所限制。相反,提供这些实施例是为了使本发明更加透彻和完整,并且能够将本发明的范围完整地传达给本领域的技术人员。

[0042] 图2示出了根据本发明的一种基于IDP代理的应用授权方法的步骤图。

[0043] 根据本发明的一种基于IDP代理的应用授权方法,包括:

[0044] 提供IDP代理,IDP代理用于提供IDP服务的代理服务并与IDP服务和第三方应用通讯连接;

[0045] 将至少一个IDP服务和至少一个第三方应用在IDP代理中完成注册,其中,IDP服务存储有用户信息,并能够提供登录页面,通过账号密码形式校验用户身份;

[0046] 将IDP代理的登录入口在第三方应用的登录页进行展示,以供用户选择IDP代理中注册的IDP服务;

[0047] IDP代理根据用户选择的IDP服务,跳转至所选IDP服务的登录页面,申请获取所选IDP服务的授权,并将此授权转发给所述第三方应用,完成登录。

[0048] 具体地,通过IDP代理的方式,IDP服务和第三方应用均能够在IDP 代理处完成注册并分别与IDP代理建立通讯连接,使IDP服务可以迅速被已经接入IDP代理的三方应用所使用,让用户在使用多个第三方应用时可以通过统一的身份验证系统来登录,避免了用户重复注册和登录操作。

[0049] 进一步地,通过IDP代理的方式,可以虚拟化IDP服务。时间跨度上,一个的IDP背后,可以对应多个实际的IDP服务。当IDP服务发生地址迁移等变化,也可以通过更换地址等信息来保证IDP服务的稳定,起到类似域名的作用。

[0050] 在一个示例中,将至少一个IDP服务和至少一个第三方应用在IDP代理中完成注册包括:

[0051] IDP代理记录IDP服务的网络地址并与IDP服务互换公钥;

[0052] IDP代理记录第三方应用的回调地址并与第三方应用互换公钥。

[0053] 在一个示例中,IDP服务包括私有IDP服务和公有IDP服务;

[0054] IDP服务的网络地址包括IP地址和/或逻辑地址。

[0055] 具体地，私有IDP可以理解为一个组织(个人或者企业)，拥有的自己在公有云服务或者自有机房或自有设备中安装并运行的IDP服务；公有IDP 提供多个组织来使用的SaaS版的IDP服务；无论是共有IDP还是私有IDP 都可以在IDP代理中注册，不同点在于私有IDP是提供的是真实的网络地址，如IP地址；而公有IDP除了要提供网络地址以外，还要提供实际的IDP 服务在公有IDP中的逻辑地址。

[0056] 在一个示例中，在所述IDP代理中完成注册的每个IDP服务具有唯一的编号，用户选择IDP代理中注册的IDP服务包括：

[0057] 用户输入所述IDP的编号并确认后，若编号或相似编号真实存在，则显示多个所述IDP服务供用户选择需要的一个IDP服务。

[0058] 一种具体实施方式如下：

[0059] 1、准备工作：

[0060] (1)IDP服务(可以是公有IDP，也可以是私有IDP)用来存储用户信息，IDP服务向IDP代理注册，告知IDP代理其具体位置并完成公钥互换，IDP代理与IDP服务在通讯过程中的信息都做加密处理。其中每个IDP 服务都被赋予一个唯一的编号；

[0061] (2)三方应用在IDP代理处完成注册和公钥互换，再使用IDP代理提供的SDK或者API服务，将IDP代理的登陆入口展示在三方应用的登录页。

[0062] 2、授权流程，参考图3：

[0063] (1)用户点击IDP代理登陆入口开始授权流程；

[0064] (2)IDP代理会返回IDP服务的选择页面，要求输入IDP服务的编号；

[0065] (3)用户输入IDP服务编号并确认。若编号或相似编号真实存在，则显示多个IDP服务供用户选择需要的一个IDP服务。

[0066] (4)IDP代理明确被选中的IDP服务。根据IDP服务在IDP代理中的注册信息跳转至IDP服务；

[0067] (5)IDP服务会返回一个登录页面给用户；

[0068] (6)用户输入账号密码；

[0069] (7)IDP服务完成验证，生成授权码返回并跳转至IDP代理；

[0070] (8)IDP代理将授权按第三方应用注册时提供的回调地址，转发给第三方应用，完成登录。

[0071] 关于上述实施方式的具体开发流程本领域人员容易实现，此处不再赘述。

[0072] 本发明实施例还提出一种电子设备，电子设备包括：

[0073] 至少一个处理器；以及，

[0074] 与至少一个处理器通信连接的存储器；其中，

[0075] 存储器存储有可被至少一个处理器执行的指令，指令被至少一个处理器执行，以使至少一个处理器能够执行上述的基于IDP代理的应用授权方法。

[0076] 本发明实施例还提出一种非暂态计算机可读存储介质，该非暂态计算机可读存储介质存储计算机指令，该计算机指令用于使计算机执行上述的基于IDP代理的应用授权方法。

[0077] 参考图4，本发明实施例还提出一种基于IDP代理的应用授权系统，包括IDP代理、

至少一个IDP服务和至少一个第三方应用，IDP服务和第三方应用均在IDP代理中完成注册并分别与IDP代理通讯连接；

[0078] 第三方应用的登录页能够展示IDP代理的登录入口，以供用户选择IDP 代理中注册的IDP服务；

[0079] IDP服务用于存储用户信息，并能够提供登录页面，通过账号密码等形式校验用户身份，以及能够将登陆用户的授权返回给IDP代理；

[0080] IDP代理根据用户选择的IDP服务，跳转至所选IDP服务的登录页面，申请获取所选IDP的授权，并将此授权转发给第三方应用，完成登录。

[0081] 在一个示例中，IDP服务和第三方应用均在IDP代理中完成注册包括：IDP代理记录IDP服务的网络地址并与IDP服务互换公钥；IDP代理记录第三方应用的回调地址并与第三方应用互换公钥。IDP服务包括私有IDP 服务和公有IDP服务，且在IDP代理中完成注册的每个IDP服务具有唯一的编号。

[0082] 本发明的基于IDP代理的应用授权方法和系统通过IDP代理的方式，时间跨度上，一个IDP背后，可以对应多个实际的IDP服务，当IDP服务发生地址迁移等变化，也可以通过更换地址等信息来保证IDP服务的稳定，能够使IDP服务可以迅速被已经接入IDP代理的三方应用所使用，让用户在使用多个第三方应用时可以通过统一的身份验证系统来登录，避免了用户重复注册和登录操作，让企业或者个人在使用SaaS服务时看起来如同使用私有应用一样，大大减少了沟通、开发工作和用户的使用成本。

[0083] 以上已经描述了本发明的各实施例，上述说明是示例性的，并非穷尽性的，并且也不限于所披露的各实施例。在不偏离所说明的各实施例的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。

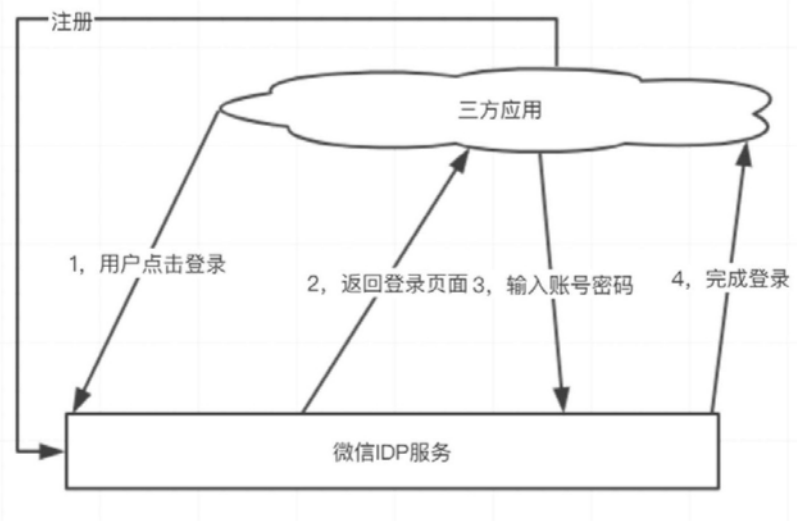

注册
三方应用
1，用户点击登录
2，返回登录页面
3，输入账号密码
4，完成登录
微信IDP服务

图1

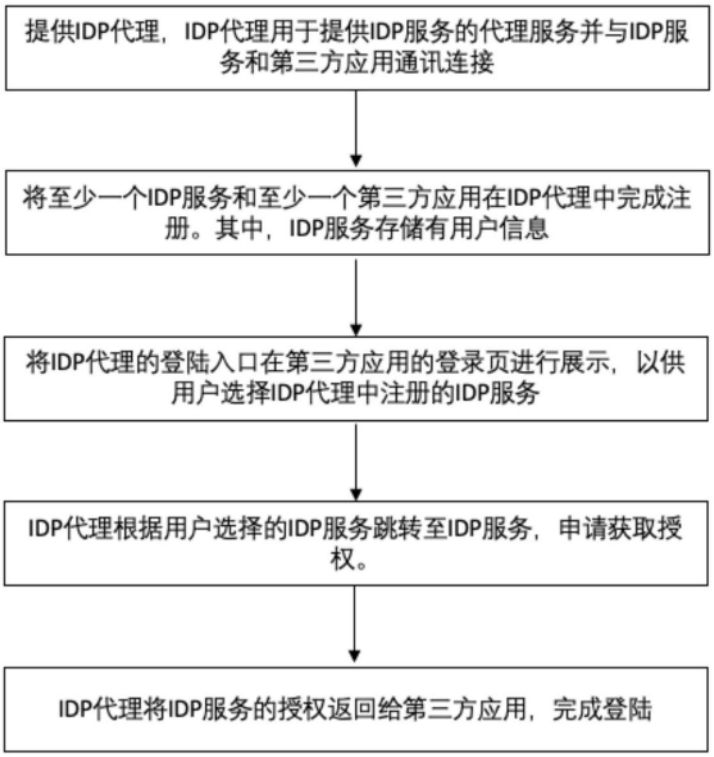

提供IDP代理，IDP代理用于提供IDP服务的代理服务并与IDP服务和第三方应用通讯连接
将至少一个IDP服务和至少一个第三方应用在IDP代理中完成注册。其中，IDP服务存储有用户信息
将IDP代理的登陆入口在第三方应用的登录页进行展示，以供用户选择IDP代理中注册的IDP服务
IDP代理根据用户选择的IDP服务跳转至IDP服务，申请获取授权。
IDP代理将IDP服务的授权返回给第三方应用，完成登陆

图2

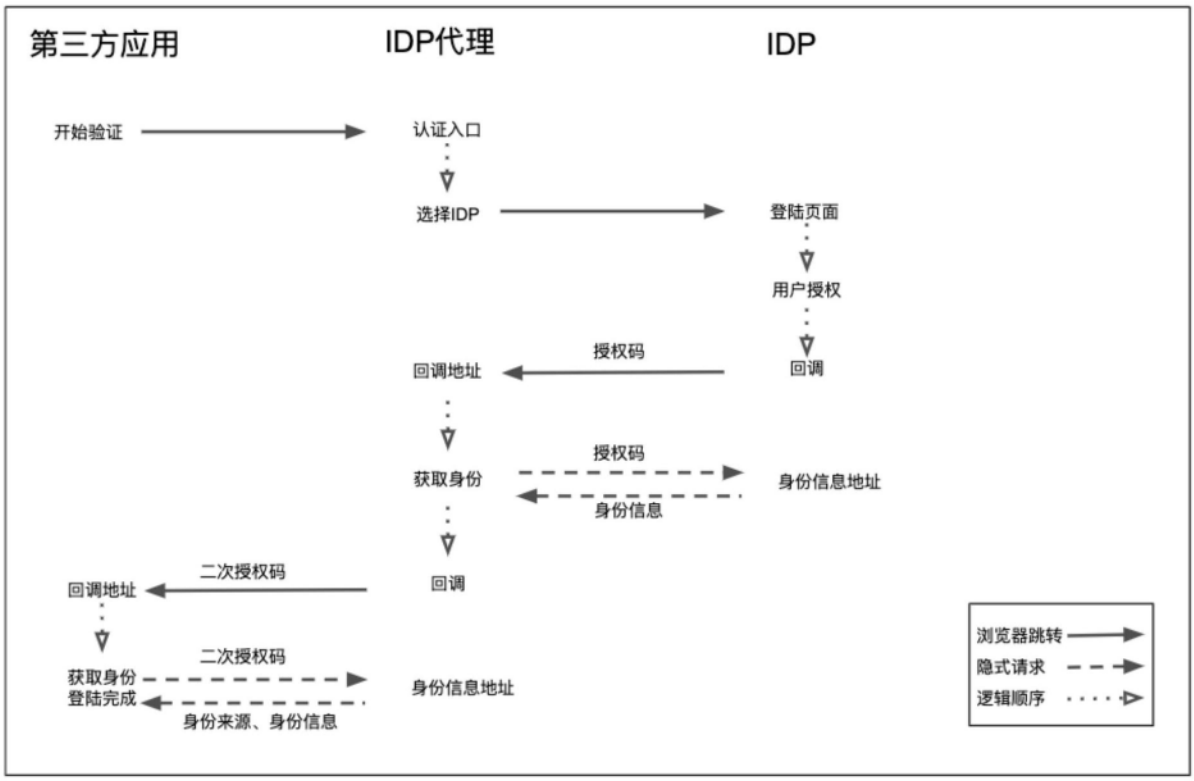

第三方应用
IDP代理
IDP
开始验证
认证入口
选择IDP
登陆页面
用户授权
回调
授权码
回调地址
获取身份
授权码
身份信息地址
身份信息
回调
二次授权码
回调地址
获取身份
登陆完成
二次授权码
身份信息地址
身份来源、身份信息
浏览器跳转
隐式请求
逻辑顺序

图3

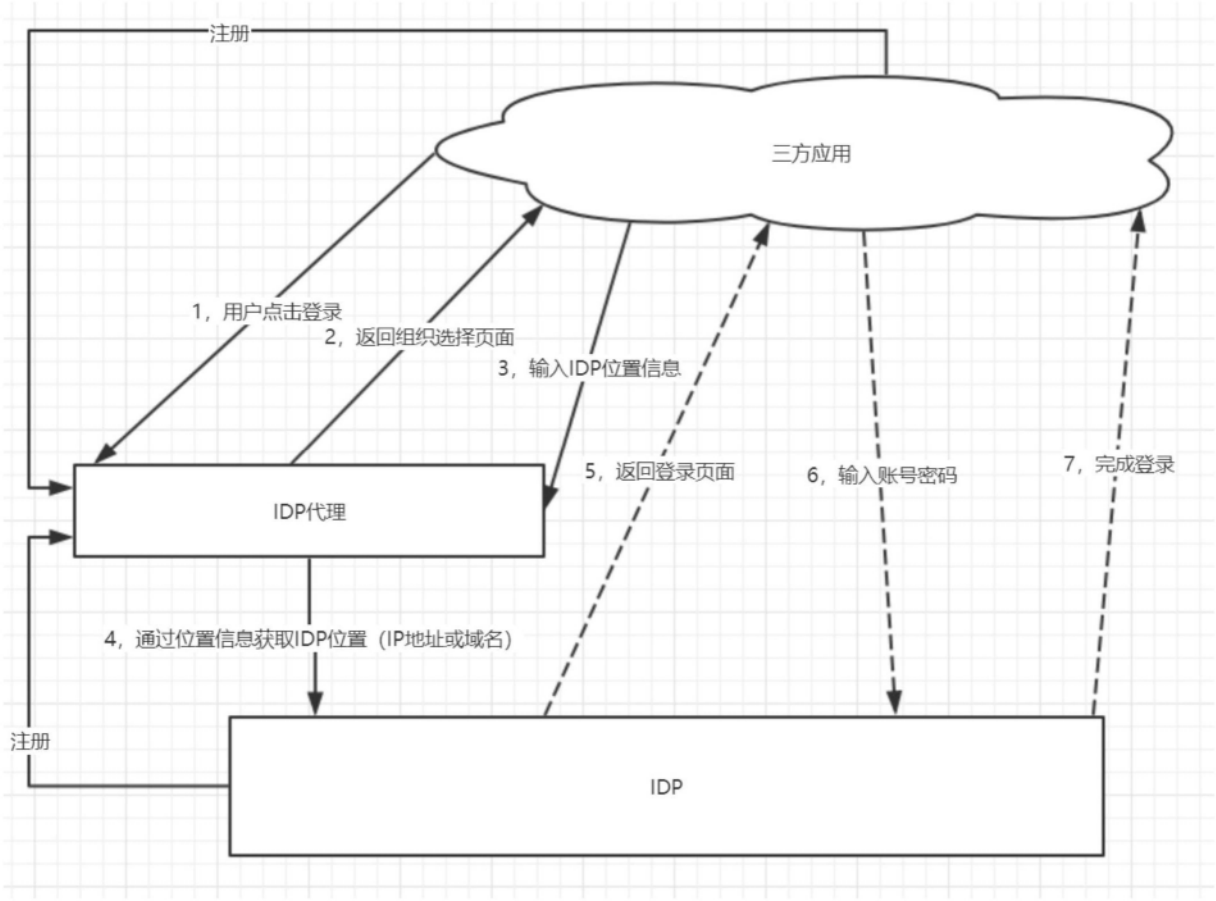

注册
三方应用
1，用户点击登录
2，返回组织选择页面
3，输入IDP位置信息
5，返回登录页面
6，输入账号密码
7，完成登录
IDP代理
4，通过位置信息获取IDP位置（IP地址或域名）
注册
IDP

图4