(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116015824 A
(43)申请公布日 2023.04.25

(21)申请号 202211636332.X

(22)申请日 2022.12.20

(71)申请人 上海浦东发展银行股份有限公司
地址 200002 上海市黄浦区中山东一路12号

(72)发明人 铁锦程 孙兵兵 姜丽丽

(74)专利代理机构 上海科盛知识产权代理有限公司 31225
专利代理师 翁惠瑜

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

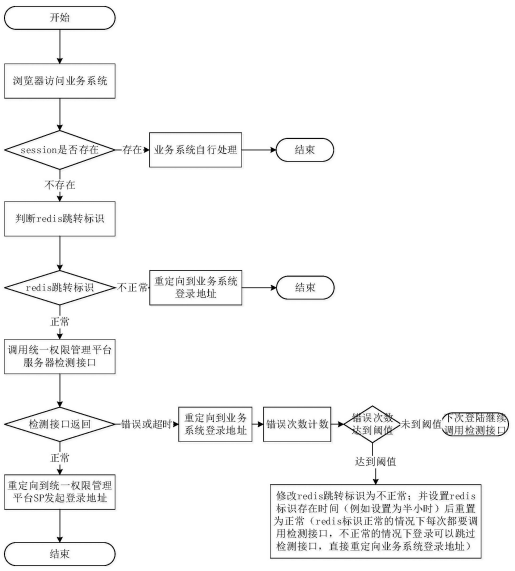
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种平台统一认证方法、设备、介质

(57)摘要

本发明涉及一种平台统一认证方法、设备、介质，所述方法应用于服务端的认证平台，用于针对多个业务系统实现登录认证及角色权限管理，认证方法包括如下步骤：获取包括目标URL地址的用户请求信息，判断用户是否已经登录，若否，经过降级检测后跳转至预设的登陆发起页面，若是，转至与目标URL地址匹配的页面；在登陆发起页面中，获取登录账户及口令信息，并与通过预设的接口获取的和/或预置在内的包括多个业务系统的角色权限信息进行匹配，判断身份认证是否通过，若是，生成令牌信息，业务系统在校验令牌信息后，跳转至与目标URL地址匹配的页面，完成登录。与现有技术相比，本发明具有灵活性高、权限数据的管理方便等优点。



CN 116015824 A

1.一种平台统一认证方法,其特征在于,应用于服务端的认证平台,用于针对多个业务系统实现登录认证及角色权限管理,所述认证方法包括如下步骤:

获取包括目标URL地址的用户请求信息,判断用户是否已经登录,若否,经过降级检测后跳转至预设的登陆发起页面,若是,转至与所述目标URL地址匹配的页面;

在所述登陆发起页面中,获取登录账户及口令信息,并与通过预设的接口获取的和/或预置在内的包括多个业务系统的角色权限信息进行匹配,判断身份认证是否通过,若是,生成令牌信息,业务系统在校验所述令牌信息后,跳转至与所述目标URL地址匹配的页面,并创建session会话完成登录,若否,发送认证失败的提示信息。

2.根据权利要求1所述的一种平台统一认证方法,其特征在于,判断用户是否已经登录具体为:

根据是否存在session信息判断用户是否已经登录。

3.根据权利要求1所述的一种平台统一认证方法,其特征在于,所述的业务系统通过SDK或源码解析实现对所述令牌信息的校验。

4.根据权利要求1所述的一种平台统一认证方法,其特征在于,所述的降级检测具体为:

判断redis跳转标识是否正常,若否,跳转至预设的业务系统登录页面,若是,对预设的登录认证接口进行检测,判断接口返回是否正常,若是,降级检测通过,若否,跳转至预设的业务系统登录页面,对错误进行记录,满足预设规则后将redis跳转标识设置为不正常状态。

5.根据权利要求4所述的一种平台统一认证方法,其特征在于,满足预设规则后将redis跳转标识设置为不正常状态具体为:

当错误次数达到预设的阈值后,修改redis跳转标识设置为不正常状态。

6.根据权利要求4所述的一种平台统一认证方法,其特征在于,若redis跳转标识设置为不正常状态,经过预设时间后重置为正常状态。

7.根据权利要求4所述的一种平台统一认证方法,其特征在于,跳转至预设的业务系统登录页面之后,还包括:

获取登录账户及口令信息,通过统预设的认证接口进行认证。

8.根据权利要求1所述的一种平台统一认证方法,其特征在于,还包括:

定期通过预设接口和/或数据的同步方式获取并更新所述角色权限信息。

9.一种电子设备,其特征在于,包括:一个或多个处理器以及存储器,所述存储器内储存有一个或多个程序,所述一个或多个程序包括用于执行如权利要求1-8任一所述平台统一认证方法的指令。

10.一种计算机可读存储介质,其特征在于,包括供电子设备的一个或多个处理器执行的一个或多个程序,所述一个或多个程序包括用于执行如权利要求1-8任一所述平台统一认证方法的指令。

一种平台统一认证方法、设备、介质

技术领域

[0001] 本发明涉及网络安全领域，尤其是涉及一种平台统一认证方法、设备、介质。

背景技术

[0002] 现有多平台账户权限统一管理方法灵活性较差，且对权限数据的管理效率较低。现有的管理系统大多使用微服务框架搭建，为每个对接系统分配一个公钥，当用户登录时记录用户登录信息，并返回一个token，业务系统根据token获取用户的角色、权限等信息。

[0003] 中国专利申请号CN201710283872.7公开了一种面向系统集成的跨域单点登录系统及方法。该系统包括终端、访问代理服务器、单点登录服务器，访问代理服务器部署在子系统前，并与子系统处于同一顶级域下，用于全权处理和转发一切发往子系统的请求；单点登录服务器，包括统一登录接口、授权码生成模块、授权码管理模块、模拟登录模块。在不侵入系统代码、不更改系统设置的情况下，实现跨域、跨开发平台的单点登录，适用于高并发场景、支持免登陆。当用户访问子系统时，访问代理服务器将请求重定向到统一登录界面，用户成功登录后，生成唯一授权码。通过使用模拟登录的方式，将授权码及登录信息发送到子系统。用户使用授权码直接访问本系统或其他系统，无需再次登录。但是，该申请并未解决对权限数据的管理效率较低的问题。

[0004] 综上，角色与权限的管理，目前各业务系统自行维护权限信息，统一管理成本较高，且对本系统依赖较大。当前缺少一种平台统一认证方法，以解决或部分解决对权限数据的管理效率较低的问题。

发明内容

[0005] 本发明的目的就是为了克服上述现有技术存在的缺陷而提供一种平台统一认证方法、设备、介质，以解决或部分解决现有的权限管理平台灵活性较差，且对权限数据的管理效率较低的问题。

[0006] 本发明的目的可以通过以下技术方案来实现：

[0007] 本发明的一个方面，提供了一种平台统一认证方法，应用于服务端的认证平台，用于针对多个业务系统实现登录认证及角色权限管理，所述认证方法包括如下步骤：

[0008] 获取包括目标URL地址的用户请求信息，判断用户是否已经登录，若否，经过降级检测后跳转至预设的登陆发起页面，若是，转至与所述目标URL地址匹配的页面；

[0009] 在所述登陆发起页面中，获取登录账户及口令信息，并与通过预设的接口获取的和/或预置在内的包括多个业务系统的角色权限信息进行匹配，判断身份认证是否通过，若是，生成令牌信息，业务系统在校验所述令牌信息后，跳转至与所述目标URL地址匹配的页面，并创建session会话完成登录，若否，发送认证失败的提示信息。

[0010] 作为优选的技术方案，判断用户是否已经登录具体为：

[0011] 根据是否存在session信息判断用户是否已经登录。

[0012] 作为优选的技术方案，所述的业务系统通过SDK或源码解析实现对所述令牌信息

的校验。

[0013] 作为优选的技术方案,所述的降级检测具体为:

[0014] 判断redis跳转标识是否正常,若否,跳转至预设的业务系统登录页面,若是,对预设的登录认证接口进行检测,判断接口返回是否正常,若是,降级检测通过,若否,跳转至预设的业务系统登录页面,对错误进行记录,满足预设规则后将redis跳转标识设置为不正常状态。

[0015] 作为优选的技术方案,满足预设规则后将redis跳转标识设置为不正常状态具体为:

[0016] 当错误次数达到预设的阈值后,修改redis跳转标识设置为不正常状态。

[0017] 作为优选的技术方案,若redis跳转标识设置为不正常状态,经过预设时间后重置为正常状态。

[0018] 作为优选的技术方案,跳转至预设的业务系统登录页面之后,还包括:

[0019] 获取登录账户及口令信息,通过统预设的认证接口进行认证。

[0020] 作为优选的技术方案,还包括:

[0021] 定期通过预设接口和/或数据的同步方式获取并更新所述角色权限信息。

[0022] 本发明的另一个方面,提供了一种电子设备,包括:一个或多个处理器以及存储器,所述存储器内储存有一个或多个程序,所述一个或多个程序包括用于执行上述平台统一认证方法的指令。

[0023] 本发明的另一个方面,提供了一种计算机可读存储介质,包括供电子设备的一个或多个处理器执行的一个或多个程序,所述一个或多个程序包括用于执行上述平台统一认证方法的指令。

[0024] 与现有技术相比,本发明具有以下优点:

[0025] (1)相较于传统的方法需要为每个业务系统分配公钥,自行维护权限信息的方法,本方法通过使权限管理认证平台与各个业务系统对接,将登录认证及权限管理的功能集中,各业务系统接到请求信息后判断用户是否登录,若未登录由认证平台根据获取的角色权限信息进行认证,由此能够实现业务系统用户与角色的统一管理以及登录认证,减小权限管理成本,提高权限管理效率,并提高认证平台的灵活度。

[0026] (2)在跳转至预设的登陆发起页面前进行降级检测,能够在认证平台的登陆页面因故无法访问时,跳转至业务系统自带的认证页面,通过平台预设的认证接口完成登录,有较强的鲁棒性。

附图说明

[0027] 图1为实施例1中平台统一认证方法的流程图;

[0028] 图2为实施例1中平台统一认证过程的示意图。

具体实施方式

[0029] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明的一部分实施例,而不是全部实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实

施例，都应属于本发明保护的范围。

[0030] 实施例1

[0031] 如图1-2所述，本实施例提供了一种平台统一认证方法。本方法通过在服务端设置统一权限管理平台实现登录认证、用户数据同步和权限角色管控。其中登录认证又根据业务系统自身特点不同，分为单点登录和接口后置两种模式。

[0032] 统一权限管理平台的功能如表1所述。

[0033] 表1 统一权限管理平台的功能

[0034]

对接内容	对接模式	说明
登录认证	接口后置	业务系统使用自己的登录界面引导用户登录，用户输入用户名密码后，业务系统通过调用统一权限管理平台的密码验证接口进行校验。 同时由统一权限管理平台记录登录日志供审计使用。
	单点登录	业务系统使用统一权限管理平台的登录界面引导用户登录，统一权限平台完成用户校验后，通过传递 id_token 给业务系统，业务系统仅需校验 id_token 的有效性而无须再验证用户的密码信息。 同时由统一权限管理平台记录登录日志供审计使用。
角色权限		统一权限平台接管业务系统的人员角色管理功能，通过登录接口和数据同步方式提供业务系统人员角色权限信息
数据同步		统一权限管理平台定时生成：组织机构数据文件、用户数据文件、用户权限信息文件，文件格式为 excel，同步文件最终通过文件中转平台，传递到业务系统提供的服务器，业务系统从自己的服务器再进行文件的解析和处理。

[0035] 如图2所述为单点登录流程的示意图，用户访问业务系统，业务系统会重定向到统一权限管理平台的SP登录发起地址，在统一权限管理平台认证通过后，会向业务系统返回SP登录发起地址的页面并携带请求事件redirect_url参数，用户登录后SP会向浏览器返回并显示用户访问的资源页面。具体步骤如下所述：

[0036] 1.用户在浏览器输入SP业务系统的URL地址；

[0037] 2.浏览器根据用户输入的URL，向SP业务系统请求资源；

[0038] 3.SP业务系统判断用户是否已经在本系统登录(通常是SP业务系统判断存在session信息并且存在用户信息)，若该用户已登录直接跳至步骤(13)，若未登录进行降级检测，若检测通过进行步骤(4)；

[0039] 4.SP业务系统向浏览器返回重定向响应，重定向的地址为“SP登录发起地址”(该地址由统一权限管理平台提供；

[0040] 5.浏览器自动请求统一权限管理平台的“SP登录发起地址”

[0041] 6.用户输入自己的AD域账户和密码后，提交登录；

[0042] 7.浏览器携带账号密码请求统一权限管理平台；

[0043] 8.统一权限管理平台对用户的账号和密码进行认证,认证通过后,生成id_token票据信息;

[0044] 9.统一权限管理平台向浏览器返回重定向响应,重定向的URL地址为“SP回调地址”(该地址由业务系统提供,并在申请密钥时,提供给统一权限管理平台,重定向的URL中包含了id_token;

[0045] 10.浏览器携带着id_token等信息,请求业务系统提供的“SP回调地址”;

[0046] 11.SP业务系统通过SDK(或源码解析)对id_token进行校验;应用系统接收和解析token方法参见:单点登录Token验证

[0047] 12.校验成功后,创建session会话,向浏览器返回用户访问的页面

[0048] 13.用户查看到自己访问的页面资源

[0049] 接口后置登录流程为,统一权限提供一个登录认证接口,接口code是200的情况下代表统一权限管理平台服务正常。如果不是200或者接口调用超时,说明服务出现异常,及时切换登录地址

[0050] 降级策略流程图1所述,若用户未登录则进行降级检测,判断redis跳转标识是否正常,若不正常,重定向到业务系统的登陆地址,若正常,调用统一权限管理平台服务器检测接口进行接口检测。若接口检测正常,则重定向到统一权限管理平台SP发起登陆地址,若检测接口返回错误或超时,则重定向到业务系统的登录地址并进行错误次数计数。当计数值超过预设的阈值时,则将redis跳转标识为不正常;并设置redis标识存在时间(例如设置为半小时),超过存在时间后重置为正常。

[0051] 当redis标识标记为正常时每次都要调用检测接口,标记为不正常时直接重定向业务系统登录地址。

[0052] 本实施例的平台统一认证方法具备了整合企业应用管理能力,是企业现有的应用与新应用的集成节点,使用户能够与人员、内容、应用和流程进行个性化的、安全的互动交流。同时也实现了个性化定制的工作环境,使员工能够高效工作的重要工具。统一权限每天通过文件传输的方式获取各业务系统全量用户文件、用户与角色与权限文件,若业务系统人员信息、角色权限有变动会通过实时接口同步通知统一权限。统一管理用户角色权限信息,对于业务系统来说,不需要花费大量成本维护。

[0053] 实施例2

[0054] 本实施例提供了一种电子设备,包括:一个或多个处理器以及存储器,所述存储器内储存有一个或多个程序,所述一个或多个程序包括用于执行如实施例1所述的平台统一认证方法的指令。

[0055] 本发明的另一个方面,提供了一种计算机可读存储介质,包括供电子设备的一个或多个处理器执行的一个或多个程序,所述一个或多个程序包括用于执行如实施例1所述的平台统一认证方法的指令。

[0056] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到各种等效的修改或替换,这些修改或替换都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以权利要求的保护范围为准。

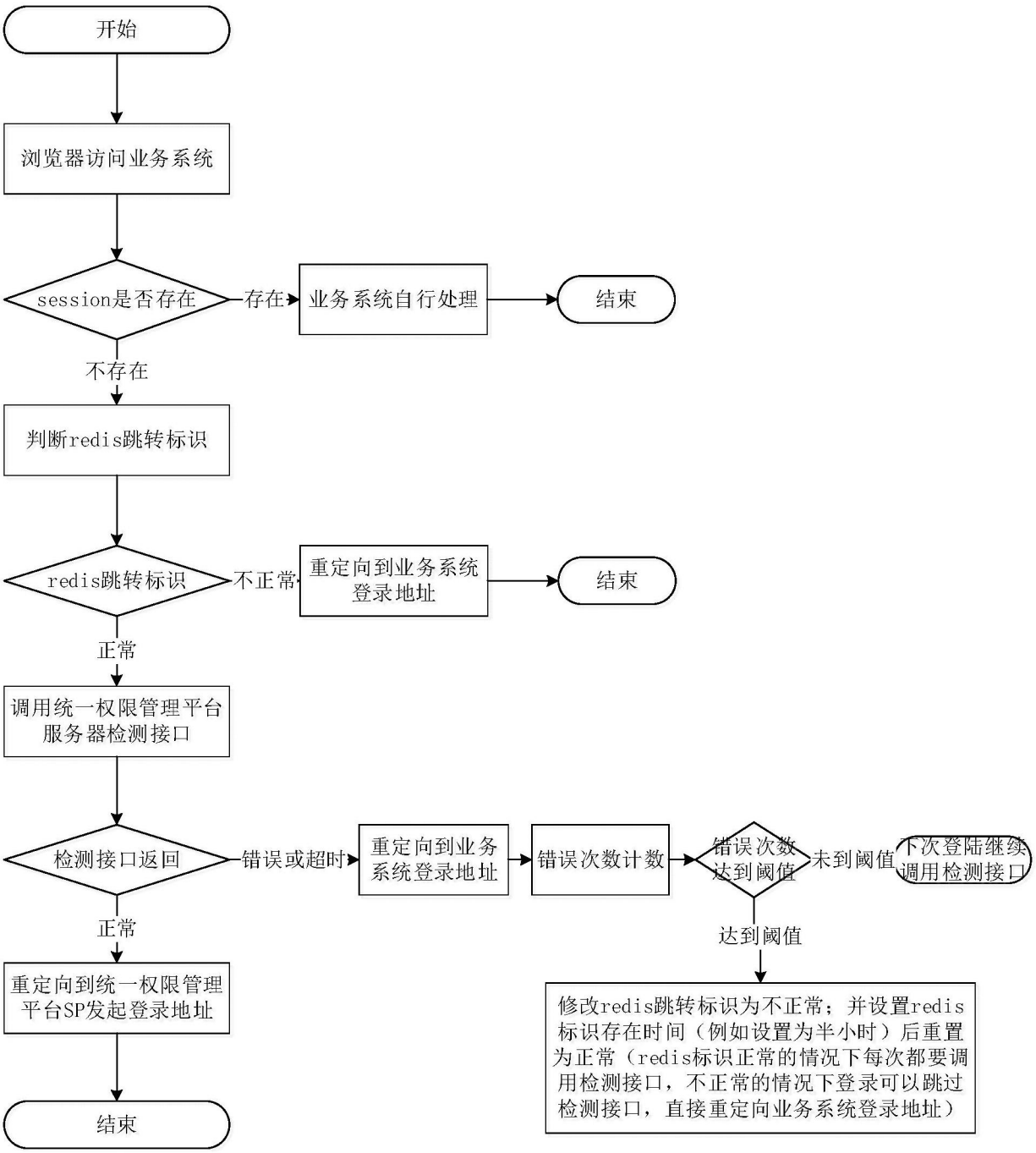

开始
浏览器访问业务系统
session是否存在
存在
业务系统自行处理
结束
不存在
判断redis跳转标识
redis跳转标识
不正常
重定向到业务系统登录地址
结束
正常
调用统一权限管理平台服务器检测接口
检测接口返回
错误或超时
重定向到业务系统登录地址
错误次数计数
错误次数达到阈值
未到阈值
下次登陆继续调用检测接口
达到阈值
修改redis跳转标识为不正常；并设置redis标识存在时间（例如设置为半小时）后重置为正常（redis标识正常的情况下每次都要调用检测接口，不正常的情况下登录可以跳过检测接口，直接重定向业务系统登录地址）
正常
重定向到统一权限管理平台SP发起登录地址
结束

图1

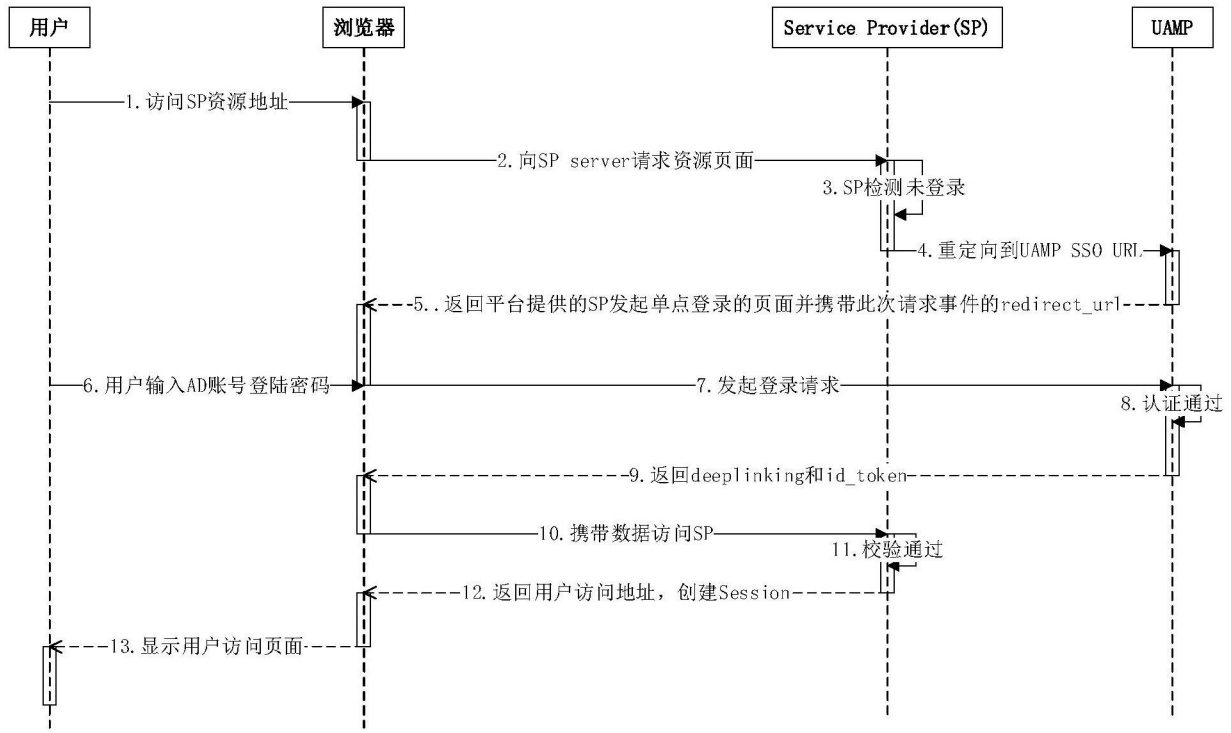

用户
浏览器
Service Provider(SP)
UAMP
1.访问SP资源地址
2.向SP server请求资源页面
3.SP检测未登录
4.重定向到UAMP SSO URL
5..返回平台提供的SP发起单点登录的页面并携带此次请求事件的redirect_url
6.用户输入AD账号登陆密码
7.发起登录请求
8.认证通过
9.返回deeplinking和id_token
10.携带数据访问SP
11.校验通过
12.返回用户访问地址，创建Session
13.显示用户访问页面

图2