(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110149328 B
(45)授权公告日 2023.01.31

(21)申请号 201910426484.9

(22)申请日 2019.05.22

(65)同一申请的已公布的文献号
申请公布号 CN 110149328 A

(43)申请公布日 2019.08.20

(73)专利权人 平安科技(深圳)有限公司
地址 518033 广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼

(72)发明人 刘潇 吕素刚

(74)专利代理机构 北京市京大律师事务所 11321
专利代理师 苏福念

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/133(2022.01)
H04L 9/32(2006.01)

(56)对比文件
CN 104125063 A,2014.10.29
CN 107689870 A,2018.02.13
CN 109408250 A,2019.03.01
CN 108141444 A,2018.06.08
玩人.钉钉实现企业级微应用免登陆详解.《https://blog.csdn.net/jerryjerryjery/article/details/53199992》.2016,
玩人.钉钉实现企业级微应用免登陆详解.《https://blog.csdn.net/jerryjerryjery/article/details/53199992》.2016,
烟雨惊蛰.钉钉E应用自动登录获取用户信息总结.《https://blog.csdn.net/yanyujingzhe/article/details/89838986?spm=1001.2101.3001.6650.8&utm_medium=distribute.pc_relevan》.2019,

审查员 杨志忠

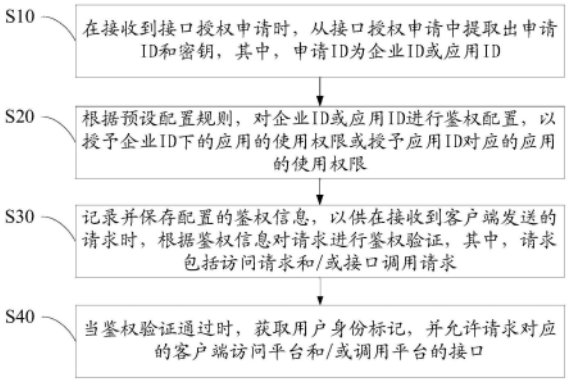
权利要求书2页 说明书8页 附图2页

(54)发明名称

接口鉴权方法、装置、设备及计算机可读存储介质

(57)摘要

本发明属于安全防护技术领域,提供一种接口鉴权方法,包括:在接收到接口授权申请时,从接口授权申请中提取出申请ID和密钥,其中,申请ID为企业ID或应用ID;根据预设配置规则,对企业ID或应用ID进行鉴权配置,以授予企业ID下的应用的使用权限或授予应用ID对应的应用的使用权限;记录并保存配置的鉴权信息,以供在接收到客户端发送的请求时,根据鉴权信息对请求进行鉴权验证;当鉴权验证通过时,获取用户身份标记,并允许请求对应的客户端访问平台和/或调用平台的接口。本发明还提供一种装置、设备及计算机可读存储介质。本发明根据配置的鉴权信息来验证请求的合法性,对合法请求给予正常响应,拒绝非法请求,从而有效保护平台站点资源。



CN 110149328 B

1.一种接口鉴权方法,其特征在于,所述接口鉴权方法包括以下步骤:

在接收到接口授权申请时,从所述接口授权申请中提取出申请ID和密钥,其中,所述申请ID为企业ID或应用ID;

根据预设配置规则,对所述企业ID或所述应用ID进行鉴权配置,以授予所述企业ID下的应用的使用权限或授予所述应用ID对应的应用的使用权限;其中,企业类型的鉴权配置优先级高于应用类型的鉴权配置;如果获取免登授权码以授权给企业使用权限,那么企业下的应用不需要重复单个授权;如果授权给某个应用,那么只有该应用才能访问平台或调用接口获取用户信息;

记录并保存配置的鉴权信息,以供在接收到客户端发送的请求时,根据所述鉴权信息对所述请求进行鉴权验证,其中,所述请求包括访问请求和/或接口调用请求;

当鉴权验证通过时,获取用户身份标记,并允许所述请求对应的客户端访问平台和/或调用平台的接口;

所述用户身份标记是一串唯一的字符串,用于标记当前访问的用户,进而记录当前用户访问平台和/或调用接口所产生的操作记录,形成日志文件,平台利用用户身份标记,即可响应客户端在网站或app应用上的各种业务操作。

2.如权利要求1所述的接口鉴权方法,其特征在于,所述根据预设配置规则,对所述企业ID或所述应用ID进行鉴权配置,以授予所述企业ID下的应用的使用权限或授予所述应用ID对应的应用的使用权限,包括:

若所述申请ID为企业ID,则获取所述企业ID下的所有应用,或若所述申请ID为应用ID,则获取所述应用ID对应的应用;

基于所述密钥及对应企业ID或应用ID,获取免登授权码,以完成所述企业ID下的应用或所述应用ID对应的应用的鉴权配置和使用授权。

3.如权利要求2所述的接口鉴权方法,其特征在于,所述基于所述密钥及对应企业ID或应用ID,获取免登授权码,包括:

基于所述密钥及对应企业ID或应用ID,申请token令牌;

基于所述token令牌,申请ticket凭证;

基于所述ticket凭证,调用JSAPI签名算法,得到code免登授权码。

4.如权利要求2所述的接口鉴权方法,其特征在于,在所述基于所述密钥及对应企业ID或应用ID,获取免登授权码之后,还包括:

将获取的所述免登授权码下发给所述接口授权申请对应的客户端进行保存和使用。

5.如权利要求1所述的接口鉴权方法,其特征在于,所述根据所述鉴权信息对所述请求进行鉴权验证,包括:

查找本地存储的所述鉴权信息中是否存在与所述请求携带的第一免登授权码相匹配的第二免登授权码;

若所述第一免登授权码与所述第二免登授权码相匹配,则验证所述第一免登授权码与所述第二免登授权码。

6.如权利要求5所述的接口鉴权方法,其特征在于,所述验证所述第一免登授权码与所述第二免登授权码,包括:

分别计算所述第一免登授权码和所述第二免登授权码的哈希值;

读取并验证所述第一免登授权码或所述第二免登授权码的有效期。

7.如权利要求6所述的接口鉴权方法，其特征在于，在所述验证该免登授权码之后，还包括：

若计算的哈希值两者相等且第一/第二免登授权码在有效期内，则判定鉴权验证通过；

若计算的哈希值两者不相等或第一免登授权码不在有效期内或第二免登授权码不在有效期内，则判定鉴权验证不通过。

8.一种接口鉴权装置，其特征在于，所述接口鉴权装置包括：

接收提取模块，用于在接收到接口授权申请时，从所述接口授权申请中提取出申请ID和密钥，其中，所述申请ID为企业ID或应用ID；

鉴权配置模块，用于根据预设配置规则，对所述企业ID或所述应用ID进行鉴权配置，以授予所述企业ID下的应用的使用权限或授予所述应用ID对应的应用的使用权限；其中，企业类型的鉴权配置优先级高于应用类型的鉴权配置；如果获取免登授权码以授权给企业使用权限，那么企业下的应用不需要重复单个授权；如果授权给某个应用，那么只有该应用才能访问平台或调用接口获取用户信息；

记录保存模块，用于记录并保存配置的鉴权信息，以供在接收到客户端发送的请求时，根据所述鉴权信息对所述请求进行鉴权验证，其中，所述请求包括访问请求和/或接口调用请求；

允许使用模块，用于当鉴权验证通过时，获取用户身份标记，并允许所述请求对应的客户端访问平台和/或调用平台的接口；

所述用户身份标记是一串唯一的字符串，用于标记当前访问的用户，进而记录当前用户访问平台和/或调用接口所产生的操作记录，形成日志文件，平台利用用户身份标记，即可响应客户端在网站或app应用上的各种业务操作。

9.一种接口鉴权设备，其特征在于，所述接口鉴权设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的接口鉴权程序，所述接口鉴权程序被所述处理器执行时实现如权利要求1至7中任一项所述的接口鉴权方法的步骤。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有接口鉴权程序，所述接口鉴权程序被处理器执行时实现如权利要求1至7中任一项所述的接口鉴权方法的步骤。

接口鉴权方法、装置、设备及计算机可读存储介质

技术领域

[0001] 本发明涉及安全防护技术领域，尤其涉及一种接口鉴权方法、装置、设备及计算机可读存储介质。

背景技术

[0002] 随着通信技术的不断发展，各种不同的通信技术标准均得到了广泛的应用，现有的系统平台一般都需要通过接口来调用和获取数据，然而若没有对接口进行鉴权管理，用户可以通过互联网随意接入平台并任意调用接口，进而使平台资源被大量占用，影响平台的维护管理和运营。因此在项目应用工程中，对不同第三方接入本平台时，需要进行鉴权配置，同时第三方的授权形式不一，鉴权过程中需要处理的逻辑业务复杂多变，不利于管理且容易导致数据混乱或不兼容，进而存在一定的安全隐患。

发明内容

[0003] 本发明的主要目的在于提供一种接口鉴权方法、装置、设备及计算机可读存储介质，旨在改进接口鉴权方式，满足不同业务需求和保护平台站点资源。

[0004] 为实现上述目的，本发明提供的一种接口鉴权方法，所述接口鉴权方法包括以下步骤：

[0005] 在接收到接口授权申请时，从所述接口授权申请中提取出申请ID和密钥，其中，所述申请ID为企业ID或应用ID；

[0006] 根据预设配置规则，对所述企业ID或所述应用ID进行鉴权配置，以授予所述企业ID下的应用的使用权限或授予所述应用ID对应的应用的使用权限；

[0007] 记录并保存配置的鉴权信息，以供在接收到客户端发送的请求时，根据所述鉴权信息对所述请求进行鉴权验证，其中，所述请求包括平台访问请求和/或平台接口调用请求；

[0008] 当鉴权验证通过时，获取用户身份标记，并允许所述请求对应的客户端访问平台和/或调用平台的接口。

[0009] 可选地，所述根据预设配置规则，对所述企业ID或所述应用ID进行鉴权配置，以授予所述企业ID下的应用的使用权限或授予所述应用ID对应的应用的使用权限，包括：

[0010] 若所述申请ID为企业ID，则获取所述企业ID下的所有应用，或若所述申请ID为应用ID，则获取所述应用ID对应的应用；

[0011] 基于所述密钥及对应企业ID或应用ID，获取免登授权码，以完成所述企业ID下的应用或所述应用ID对应的应用的鉴权配置和使用授权。

[0012] 可选地，所述基于所述密钥及对应企业ID或应用ID，获取免登授权码，包括：

[0013] 基于所述应用密钥及对应企业ID或应用ID，申请token令牌；

[0014] 基于所述token令牌，申请ticket凭证；

[0015] 基于所述ticket凭证，调用JSAPI签名算法，得到code免登授权码。

[0016] 可选地，在所述基于所述密钥及对应企业ID或应用ID，获取免登授权码之后，还包括：

[0017] 将获取的所述免登授权码下发给所述接口授权申请对应的客户端进行保存和使用。

[0018] 可选地，所述根据所述鉴权信息对所述请求进行鉴权验证，包括：

[0019] 查找本地存储的所述鉴权信息中是否存在与所述请求携带的第一免登授权码相匹配的第二免登授权码；

[0020] 若所述第一免登授权码与所述第二免登授权码相匹配，则验证所述第一免登授权码与所述第二免登授权码。

[0021] 可选地，所述验证所述第一免登授权码与所述第二免登授权码，包括：

[0022] 分别计算所述第一免登授权码和所述第二免登授权码的哈希值；

[0023] 读取并验证所述第一免登授权码或所述第二免登授权码的有效期。

[0024] 可选地，在所述验证该免登授权码之后，还包括：

[0025] 若计算的哈希值两者相等且第一/第二免登授权码在有效期内，则判定鉴权验证通过；

[0026] 若计算的哈希值两者不相等或第一免登授权码不在有效期内或第二免登授权码不在有效期内，则判定鉴权验证不通过。

[0027] 此外，为实现上述目的，本发明还提供一种接口鉴权装置，所述接口鉴权装置包括：

[0028] 接收提取模块，用于在接收到接口授权申请时，从所述接口授权申请中提取出申请ID和密钥，其中，所述申请ID为企业ID或应用ID；

[0029] 鉴权配置模块，用于根据预设配置规则，对所述企业ID或所述应用ID进行鉴权配置，以授予所述企业ID下的应用的使用权限或授予所述应用ID对应的应用的使用权限；

[0030] 记录保存模块，用于记录并保存配置的鉴权信息，以供在接收到客户端发送的请求时，根据所述鉴权信息对所述请求进行鉴权验证，其中，所述请求包括访问请求和/或接口调用请求；

[0031] 允许使用模块，用于当鉴权验证通过时，获取用户身份标记，并允许所述请求对应的客户端访问平台和/或调用平台的接口。

[0032] 此外，为实现上述目的，本发明还提供一种接口鉴权设备，所述接口鉴权设备包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的接口鉴权程序，所述接口鉴权程序被所述处理器执行时实现如上述中任一项所述的接口鉴权方法的步骤。

[0033] 此外，为实现上述目的，本发明还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有接口鉴权程序，所述接口鉴权程序被处理器执行时实现如上述中任一项所述的接口鉴权方法的步骤。

[0034] 本发明首先是在接收到接口授权申请时，从接口授权申请中提取出申请ID和密钥，其中，申请ID为企业ID或应用ID，然后根据预设配置规则，对企业ID或应用ID进行鉴权配置，以授予企业ID下的应用的使用权限或授予应用ID对应的应用的使用权限。记录并保存配置的鉴权信息，以供在接收到客户端发送的请求时，根据鉴权信息对请求进行鉴权验证，进而当鉴权验证通过时，获取用户身份标记，并允许请求对应的客户端访问平台和/或

调用平台的接口。本发明提供企业/应用鉴权两种方式，在接收到接口授权申请时响应申请并进行鉴权配置，以授权申请方使用权限，鉴权配置方式更灵活。以及在接收到请求时，根据配置的鉴权信息来验证请求的合法性，对合法请求给予正常响应，拒绝非法请求，从而达到安全防护、有效保护平台站点资源的有益效果。

附图说明

[0035] 图1为本发明实施例方案涉及的接口鉴权设备运行环境的结构示意图；

[0036] 图2为本发明接口鉴权方法一实施例的流程示意图；

[0037] 图3为图2步骤S20一实施例的细化流程示意图；

[0038] 图4为本发明接口鉴权装置一实施例的功能模块示意图。

[0039] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0040] 应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

[0041] 参照图1，图1为本发明实施例方案涉及的接口鉴权设备运行环境的结构示意图。

[0042] 如图1所示，该接口鉴权设备可以包括：处理器1001，例如CPU，通信总线1002、用户接口1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard)，网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器，也可以是稳定的存储器(non-volatile memory)，例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0043] 本领域技术人员可以理解，图1中示出的接口鉴权设备的硬件结构并不构成对接口鉴权设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0044] 如图1所示，作为一种计算机可读存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及计算机程序。其中，操作系统是管理和控制接口鉴权设备和软件资源的程序，支持接口鉴权程序以及其它软件和/或程序的运行。

[0045] 在图1所示的接口鉴权设备的硬件结构中，网络接口1004主要用于接入网络；用户接口1003主要用于侦测确认指令和编辑指令等。而处理器1001可以用于调用存储器1005中存储的接口鉴权程序，并执行以下接口鉴权方法的各实施例的步骤。

[0046] 基于上述接口鉴权设备硬件结构，提出本发明接口鉴权方法的各个实施例。

[0047] 参照图2，图2为本发明接口鉴权方法一实施例的流程示意图。

[0048] 本实施例中，接口鉴权方法包括：

[0049] 步骤S10，在接收到接口授权申请时，从接口授权申请中提取出申请ID和密钥，其中，申请ID为企业ID或应用ID；

[0050] 本实施例中，接口授权申请，就是申请平台接口的使用权限的一种请求，可以是用户通过客户端个人申请，也可以是企业管理员通过客户端批量申请，还可以是平台管理员发起的申请。若为用户申请，则授权申请携带的是应用ID，若为企业申请，则授权申请携带的是企业ID，若为平台管理员发起的，则授权申请携带的可以是企业ID也可以是应用ID，具

体根据实际情况而定。需要理解的是，平台是本接口鉴权设备在互联网上提供的一个服务平台。无论是客户端申请，还是平台管理设置，均需要安装配套的应用软件，并通过配套的应用软件来实现发起接口授权申请。

[0051] 本实施例中，接口授权申请携带有申请ID和密钥，其中，身份证(identification，ID)可以是身份标识号、账号、唯一编码、专属号码等，用来区分每个不同的企业或每个不同的应用。密钥是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数。密钥是申请方设置的，比如aodufwen123，zJIWdjf11，1122345等等。

[0052] 本实施例中，平台提供企业/应用两种鉴权方式，具体可以根据自己的业务情况，选择合适的鉴权方式，来实现对平台资源的有效保护。也就是，当平台接收到接口授权申请时，响应该申请，并从该申请中提取出申请ID和密钥，进而为企业/应用配置鉴权。

[0053] 步骤S20，根据预设配置规则，对企业ID或应用ID进行鉴权配置，以授予企业ID下的应用的使用权限或授予应用ID对应的应用的使用权限；

[0054] 本实施例中，鉴权(authentication)是指验证用户是否拥有访问平台和/或调用平台接口的权利。鉴权功能旨在保护平台的内容资源不被非法第三方占用/下载/盗用等，主要通过鉴权配置，实现授予第三方使用接口的权限。预设配置规则是预先设置好的一套为企业ID或应用ID配置鉴权信息的规则。通过鉴权配置，完成授予企业ID下的应用的使用权限或授予应用ID对应的应用的使用权限的配置方案。

[0055] 步骤S30，记录并保存配置的鉴权信息，以供在接收到客户端发送的请求时，根据鉴权信息对请求进行鉴权验证，其中，请求包括平台访问请求和/或平台接口调用请求；

[0056] 本实施例中，对企业ID或应用ID进行鉴权配置，配置得到的鉴权信息需要记录并保存到本地数据库中，进一步地，还将配置的鉴权信息中的免登授权码下发给接口授权申请对应的客户端进行保存和使用。用户在下次通过客户端发起请求时携带免登授权码，进而平台在接收到客户端发送的请求时，即可根据本地存储的鉴权信息对请求携带的免登授权码进行鉴权验证。

[0057] 本实施例中，鉴权信息包括token令牌、ticket凭证和code免登授权码等。可以理解的是，ID-应用-token令牌-ticket凭证-code免登授权码是一一对应保存的。鉴权信息进行验证以判断请求的合法性，对合法请求给予正常响应，拒绝非法请求，从而有效保护平台站点的资源。同时接收到客户端发送的请求可以是访问请求，也可以是调用请求，具体不做任何限定。

[0058] 步骤S40，当鉴权验证通过时，获取用户身份标记，并允许请求对应的客户端访问平台和/或调用平台的接口。

[0059] 本实施例中，鉴权验证的结果有两种，一种是通过，另一种是不通过。由于鉴权验证是验证发起请求的客户端是否具有访问或调用接口的权限，因而当且只有验证通过时，获取用户身份标记，并允许发起请求对应的客户端用户访问平台和/或调用平台的接口。而鉴权验证不通过的，不允许请求对应的客户端访问平台和/或调用平台的接口，也就不需要获取用户身份标记。可以理解的是，平台接口的授权使用必须是先有鉴权配置，再有鉴权验证。若没有配置鉴权信息，则无法授予使用权限，也无需进行鉴权验证。

[0060] 本实施例中，平台是开放给海量网络用户进行访问和使用的，每个用户对应一个用户账号。而用户标记是一串唯一的字符串，用于标记当前访问的用户，进而记录当前用户

访问平台和/或调用接口所产生的操作记录，形成日志文件。平台利用用户标记，即可响应客户端在网站或app应用上的各种业务操作，比如针对当前用户进行流程审批、进行打卡考勤查询、进行IM聊天等等所有用户行管的业务操作。

[0061] 本实施例中，提供企业/应用鉴权两种方式，在接收到接口授权申请时响应申请并进行鉴权配置，以授权申请方(企业/应用)使用接口的权限，这两种鉴权方式可相互切换，提供多样化的鉴权方式，鉴权方式更灵活。以及在接收到请求时，根据配置的鉴权信息来验证请求的合法性，对合法请求给予正常响应，拒绝非法请求，从而达到安全防护、有效保护平台站点资源的有益效果。

[0062] 参照图3，图3为图2步骤S20一实施例的细化流程示意图。

[0063] 基于上述实施例，本实施例中，步骤S20，根据预设配置规则，对企业ID或应用ID进行鉴权配置，以授予企业ID下的应用的使用权限或授予应用ID对应的应用的使用权限，包括：

[0064] 步骤S21，若申请ID为企业ID，则获取企业ID下的所有应用，或若申请ID为应用ID，则获取应用ID对应的应用；

[0065] 本实施例中，企业ID相当于企业身份账号，是企业的一种身份证明。企业旗下有一个或多个应用，比如平安企业旗下有平安保险、平安贷款、平安理财等应用，那么申请ID为平安ID，获取到平安保险、平安贷款、平安理财等应。应用ID为应用软件身份账号，比如用户的微信ID账号、微博ID账号、支付宝账号等。那么申请ID为微信应用ID，获取到微信这一应用。

[0066] 步骤S22，基于密钥及对应企业ID或应用ID，获取免登授权码，以完成企业ID下的应用或应用ID对应的应用的鉴权配置和使用授权。

[0067] 本实施例中，鉴权配置，也就是基于密钥与ID，为ID对应的应用获取免登授权码，从而授予应用使用权限。免登授权码就是配置使用权限的一个重要凭证。应用凭借这个免登授权码拥有访问平台或调用平台接口的权限。

[0068] 进一步地，企业类型的鉴权配置优先级高于应用类型的鉴权配置；如授权给企业，企业下的应用都可使用，比如获取免登授权码以授权给企业使用权限，那么企业下的应用不需要重复单个授权。而授权给某个应用，那么只有该应用才能访问平台或调用接口获取用户信息。两种鉴权方式可相互切换，提供多样化的鉴权方式，鉴权方式更灵活。

[0069] 进一步地，步骤S22包括：

[0070] 1、基于应用密钥及对应企业ID或应用ID，申请token令牌；

[0071] 本实施例中，为防止ID和密钥的重复提交，减少用户的输入操作，服务端，即平台会根据ID和密钥确认的使用的用户信息，并生成一个唯一的值，这个值就是token令牌。token令牌是随机字符串，随机生成，且带有时间戳。在实际应用中，由于token令牌的特殊随机性，不同ID不同密钥申请的token令牌会不相同，即使是相同ID相同密钥在不同时间不同场合下申请的token令牌也会不相同。

[0072] 2、基于token令牌，申请ticket凭证；

[0073] 本实施例中，ticket是token产生的临时凭据，是针对某一应用的调用凭证，只含有特定的权限。如果重新申请ticket凭证，则上一个凭据将失效。

[0074] 3、基于ticket凭证，调用JSAPI签名算法，得到code免登授权码。

[0075] 本实施例中，code免登授权码是根据JSAPI签名算法和ticket计算得到的带有时间戳的字符串。需要说明的是，ID-应用-token令牌-ticket凭证-code免登授权码是一一对应保存的。也就是企业ID-所有应用-token令牌-ticket凭证-code免登授权码一一对应，比如使用平安ID为旗下平安保险、平安贷款、平安理财等应用批量申请接口的使用权限，配置得到的鉴权信息包括token令牌、ticket凭证和code免登授权码。应用ID-应用-token令牌-ticket凭证-code免登授权码一一对应，比如使用应用ID，这个ID是用户使用微信的ID号，申请微信使用接口的权限，同样配置得到的鉴权信息包括token令牌、ticket凭证和code免登授权码。

[0076] 为方便理解token令牌、ticket凭证、code免登授权码之间的差异，举例如下：

[0077] "token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1MzY1NTMxNzgsImFwcElkIjoiNzk5MTc1YTg2ZWY5NDk3MGE3ODUzZjdiZmFhZGI0OTkiLCJ0eXBlIjoidG9rZW4iLCJpYXQiOjE1MzY1NDU5Nzh9.hKixqsfjwSUHEdhFL1fBhnaQDqZqkn0CTy2HzqvcwWE";

[0078] "ticket":"1b8d15063f61.86400.1292922000-2346678-124328";

[0079] "code":"89f5181f65c1578d0165c15a2c290001"。

[0080] 进一步地，在步骤S22之后，接口鉴权方法还包括：将获取的免登授权码下发给接口授权申请对应的客户端进行保存和使用。

[0081] 本实施例中，客户端通过安装的应用程序，使用免登授权码编辑访问请求，并向平台发送访问请求，待验证成功后即可通过接口访问平台。采用免登授权码可节省用户输入账号密码等操作，节省平台验证用户身份的操作。同时避免用户名密码通过明文传输，提高了网络安全性。因而，将获取的免登授权码下发给客户端，也就是是根据接口授权请求携带的ID，对应下发给客户端。

[0082] 本实施例中，企业鉴权配置的，企业下所有应用均可使用免登授权码，而某一应用鉴权配置的，只能是该应用才可以使用。比如A企业平安集团向平台申请接口授权以接入微信小程序，平台采用企业ID和用户设置的密钥根据上述方法得到免登授权码后，将免登授权码返回至该企业，进而只要是该企业下的应用(平安理财、平安钱包等应用)均可使用该免登授权码直接登录微信(平安理财、平安钱包等应用可以通过接口直接打开微信)。用户使用客户端并通过B应用平安贷款向平台申请接口授权以接入微信小程序，平台采用应用ID和用户设置的密钥同样根据上述方法得到免登授权码后，将免登授权码返回至B应用，进而B应用可使用免登授权码直接调用微信小程序(平安贷款可以通过接口直接打开微信)。

[0083] 进一步地，基于上述实施例，本实施例中，根据鉴权信息对请求进行鉴权验证，包括：

[0084] 步骤A，查找本地存储的鉴权信息中是否存在与请求携带的第一免登授权码相匹配的第二免登授权码；

[0085] 本实施例中，鉴权验证请求是否合法，若合法才予以客户端访问或使用平台接口，若不合法则不予响应。在实际应用中，请求携带的第一免登授权码可能是由其他平台鉴权配置得到的，因而验证的过程实际就是将本地存储的免登授权码与请求携带的免登授权码进行比对。为便于分别两者的免登授权码，将请求携带的命名为第一免登授权码，而本地存储的鉴权信息包括多个ID对应应用的免登授权码，因而将本地查找与第一免登授权码匹配的命名为第二免登授权码。

[0086] 步骤B,若第一免登授权码与第二免登授权码相匹配,则验证第一免登授权码与第二免登授权码。

[0087] 本实施例中,若第一免登授权码与第二免登授权码相匹配,说明请求携带的免登授权码是由本平台鉴权配置得到的,进而验证第一免登授权码与第二免登授权码。若第一免登授权码与第二免登授权码不匹配,则不予响应请求,该请求对应的客户端无权限访问平台或调用平台接口。

[0088] 步骤B中,验证第一免登授权码与第二免登授权码,包括:

[0089] 步骤B1,分别计算第一免登授权码和第二免登授权码的哈希值;

[0090] 本实施例中,计算免登授权码的哈希值是利用哈希函数进行计算的,哈希函数(hash function,也称为杂凑函数)是一种密码学函数,它将任意比特长度的输入转化为固定长度的输出。对于任意两个不同的输入,哈希函数计算得出相同结果的概率是极低的,理论上一个免登授权码的哈希值是唯一的,任何改动都会引起哈希值的变化。因此分别计算第一免登授权码和第二免登授权码的哈希值,得到的第一哈希值和第二哈希值,以供鉴权判断。

[0091] 步骤B2,读取并验证第一免登授权码或第二免登授权码的有效期。

[0092] 本实施例中,免登授权码是带有时间戳的字符串,因而分别读取第一免登授权码和第二免登授权码的时间戳,判断第一免登授权码和第二免登授权码是否在有效期内,以供鉴权判断。

[0093] 进一步地,若计算的哈希值两者相等且第一/第二免登授权码在有效期内,则判定鉴权验证通过;若计算的哈希值两者不相等或第一免登授权码不在有效期内或第二免登授权码不在有效期内,则判定鉴权验证不通过。

[0094] 本实施例中,若计算的第一哈希值和第二哈希值两者相等,说明第一免登授权码和第二免登授权码是同一个授权码,那么得到是有效期也一样。该授权码也在有效期内,即可判定鉴权验证通过。需要说明的是,若计算的第一哈希值和第二哈希值两者不相等,说明第一免登授权码和第二免登授权码不是同一个授权码,即可判定鉴权验证不通过。若计算的第一哈希值和第二哈希值两者相等,但不在有效期,说明该授权码失效了,同样判定鉴权验证不通过。鉴权验证防止授权码被恶意修改或破坏,有利于提高互联网安全。

[0095] 参照图4,图4为本发明接口鉴权装置一实施例的功能模块示意图。

[0096] 本实施例中,接口鉴权装置包括:

[0097] 接收提取模块10,用于在接收到接口授权申请时,从所述接口授权申请中提取出申请ID和密钥,其中,所述申请ID为企业ID或应用ID;

[0098] 鉴权配置模块20,用于根据预设配置规则,对所述企业ID或所述应用ID进行鉴权配置,以授予所述企业ID下的应用的使用权限或授予所述应用ID对应的应用的使用权限;

[0099] 记录保存模块30,用于记录并保存配置的鉴权信息,以供在接收到客户端发送的请求时,根据所述鉴权信息对所述请求进行鉴权验证,其中,所述请求包括访问请求和/或接口调用请求;

[0100] 允许使用模块40,用于当鉴权验证通过时,获取用户身份标记,并允许所述请求对应的客户端访问平台和/或调用平台的接口。

[0101] 需要说明的是,接口鉴权装置的各个实施例与上述接口鉴权方法的各实施例基本

相同，在此不再详细赘述。

[0102] 此外，本发明还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有接口鉴权程序，所述接口鉴权程序被处理器执行时实现如上述中任一项所述的接口鉴权方法的步骤。

[0103] 本发明计算机可读存储介质具体实施例与上述接口鉴权方法的各实施例基本相同，在此不再详细赘述。

[0104] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0105] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0106] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个可读存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例的方法。

[0107] 上面结合附图对本发明的实施例进行了描述，但是本发明并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本发明的启示下，在不脱离本发明宗旨和权利要求所保护的范围情况下，还可做出很多形式，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，这些均属于本发明的保护之内。

[0108] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

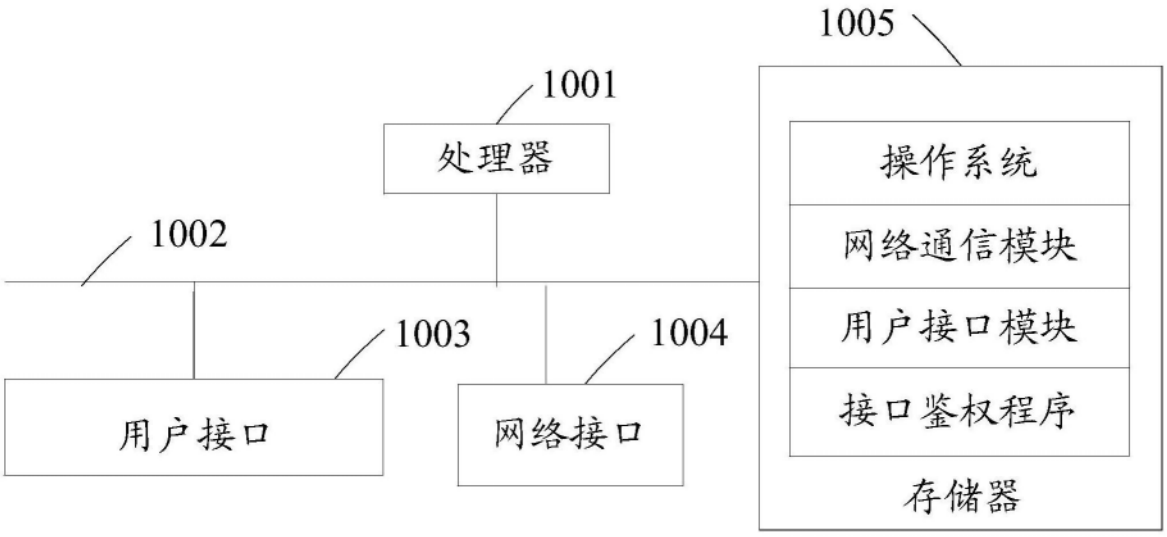

1005
1001
处理器
操作系统
网络通信模块
用户接口模块
接口鉴权程序
1002
1003
1004
用户接口
网络接口
存储器

图1

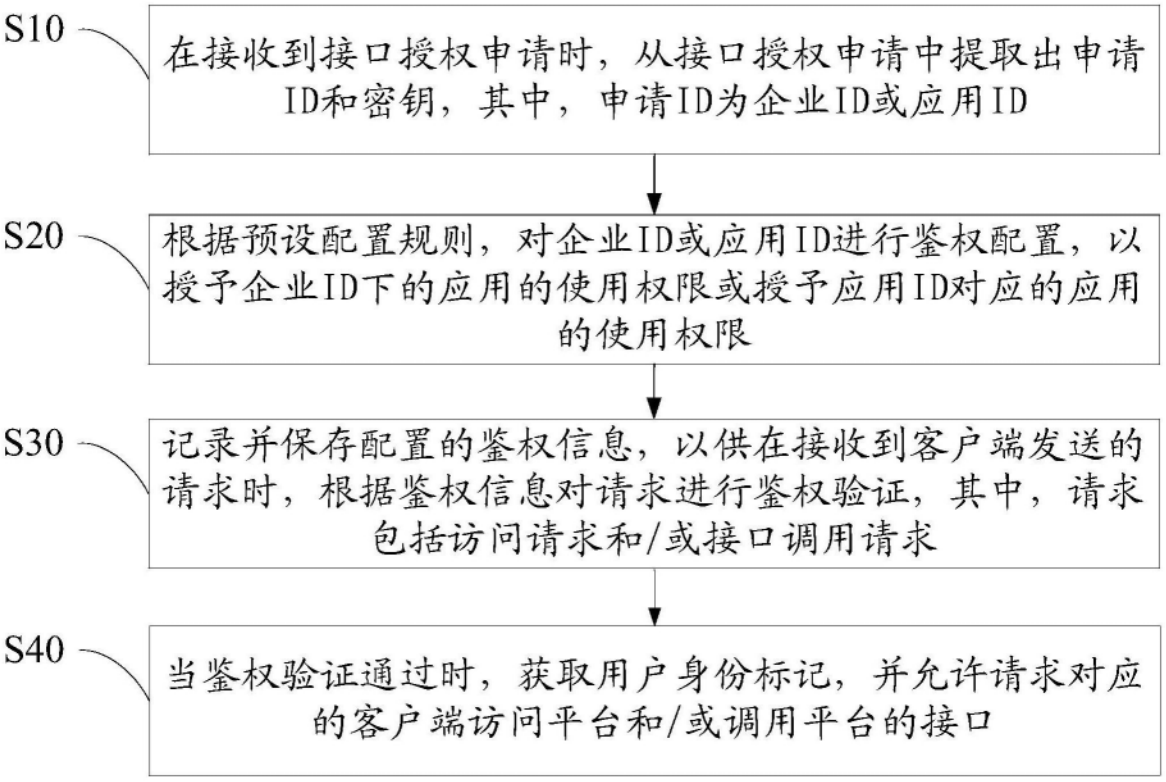

S10
在接收到接口授权申请时，从接口授权申请中提取出申请ID和密钥，其中，申请ID为企业ID或应用ID
S20
根据预设配置规则，对企业ID或应用ID进行鉴权配置，以授予企业ID下的应用的使用权限或授予应用ID对应的应用的使用权限
S30
记录并保存配置的鉴权信息，以供在接收到客户端发送的请求时，根据鉴权信息对请求进行鉴权验证，其中，请求包括访问请求和/或接口调用请求
S40
当鉴权验证通过时，获取用户身份标记，并允许请求对应的客户端访问平台和/或调用平台的接口

图2

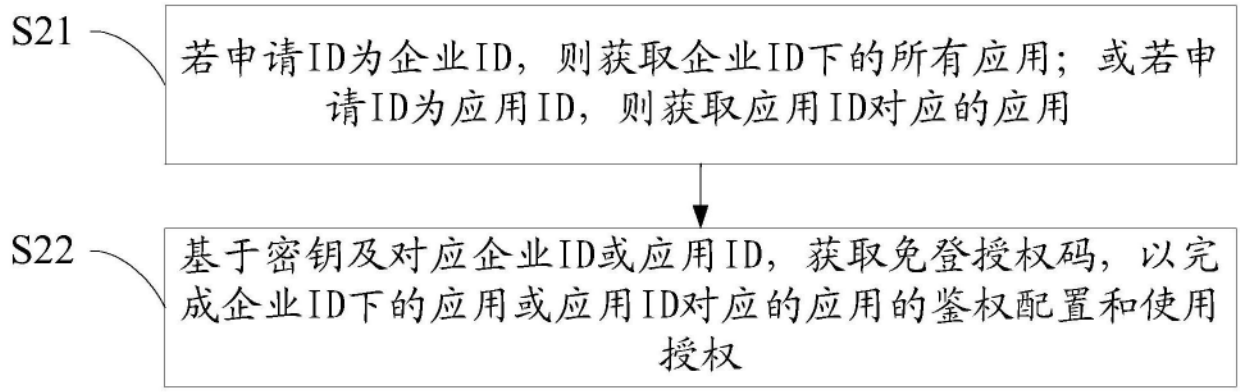

S21
若申请ID为企业ID，则获取企业ID下的所有应用；或若申请ID为应用ID，则获取应用ID对应的应用
S22
基于密钥及对应企业ID或应用ID，获取免登授权码，以完成企业ID下的应用或应用ID对应的应用的鉴权配置和使用授权

图3


接口鉴权装置
接收提取模块10
鉴权配置模块20
记录保存模块30
允许使用模块40

图4