(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110175439 A
(43)申请公布日 2019.08.27

(21)申请号 201910461003.8

(22)申请日 2019.05.29

(71)申请人 深圳前海微众银行股份有限公司
地址 518052 广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座

(72)发明人 向非能 冯庆磊 殷跃 夏运 陈振拥 钟玉峰

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
G06F 21/31(2013.01)

权利要求书2页 说明书11页 附图2页

(54)发明名称

用户管理方法、装置、设备及计算机可读存储介质

(57)摘要

本发明公开了一种用户管理方法、装置、设备及计算机可读存储介质。该方法包括：在接收到业务系统发送的身份认证请求时，获取待认证用户的用户账号和输入密码；根据用户账号检测待认证用户是否已绑定Token；若否，则根据用户账号获取初始密码，验证输入密码与初始密码是否相匹配，并将第一验证结果返回至业务系统，以使业务系统根据第一验证结果判断是否允许所述待认证用户进行登录；若是，则根据用户账号获取安全密码，验证输入密码与安全密码是否相匹配，并将第二验证结果返回至业务系统，由业务系统根据第二验证结果判断是否允许待认证用户进行登录。本发明能避免在金融机构的不同平台需记忆多个账号和密码的不便，并提高用户管理效率。

CN 110175439 A

1.一种用户管理方法,其特征在于,所述用户管理方法包括:

在接收到业务系统发送的身份认证请求时,根据所述身份认证请求获取待认证用户的用户账号和输入密码;

根据所述用户账号检测所述待认证用户是否已绑定令牌Token;

若否,则根据所述用户账号获取初始密码,验证所述输入密码与所述初始密码是否相匹配,并将第一验证结果返回至所述业务系统,以使得所述业务系统根据所述第一验证结果判断是否允许所述待认证用户进行登录;

若是,则根据所述用户账号获取安全密码,验证所述输入密码与所述安全密码是否相匹配,并将第二验证结果返回至所述业务系统,以使得所述业务系统根据所述第二验证结果判断是否允许所述待认证用户进行登录。

2.如权利要求1所述的用户管理方法,其特征在于,所述将第一验证结果返回至所述业务系统的步骤之后,还包括:

生成Token绑定提示信息,并将所述Token绑定提示信息发送至所述业务系统;

在接收到业务系统基于所述Token绑定提示信息返回的Token绑定请求时,根据所述Token绑定请求获取Token序列号,并将所述Token序列号与所述用户账号进行绑定,以用于获取对应Token发送的Token码,所述Token码作为安全密码用于身份认证。

3.如权利要求2所述的用户管理方法,其特征在于,所述安全密码还包括PIN码,所述用户管理方法还包括:

生成个人识别密码PIN码设定提示信息,并将所述PIN码设定提示信息发送至所述业务系统;

在接收到业务系统基于所述PIN码设定提示信息返回的PIN码设定请求时,根据所述PIN码设定请求获取PIN码,并将所述PIN码与所述用户账号进行关联存储。

4.如权利要求1所述的用户管理方法,其特征在于,所述用户管理方法还包括:

在接收到账号分配指令时,根据所述账号分配指令获取目标分配用户的用户信息;

基于所述目标分配用户的用户信息和预设生成规则生成对应的用户账号和初始密码,并将所述用户账号、所述初始密码与所述目标分配用户的用户信息进行关联存储。

5.如权利要求1-4任一项所述的用户管理方法,其特征在于,所述用户管理方法还包括:

在接收到权限设定请求时,根据所述权限设定请求获取权限设定信息,所述权限设定信息包括目标用户账号、目标权限信息和目标业务系统;

根据所述目标权限信息在预设用户权限列表中更新所述目标用户账号的用户权限信息,并将所述目标用户账号和更新后的用户权限信息同步至所述目标业务系统。

6.如权利要求5所述的用户管理方法,其特征在于,所述用户管理方法还包括:

在接收到离职用户列表时,根据所述离职用户列表获取对应的离职用户账号;

对所述预设用户权限列表中与所述离职用户账号对应的用户权限信息进行清除处理,并将经清除处理后的预设用户权限列表同步至各业务系统。

7.如权利要求6所述的用户管理方法,其特征在于,所述用户管理方法还包括:

在接收到权限上报信息时,提取所述权限上报信息中的用户账号,记作上报用户账号;

检测所述上报用户账号中是否存在所述离职用户账号;

若存在，则生成对应的提示信息，并将所述提示信息发送至预设管理端，以使得管理人员根据所述提示信息在对应的业务系统中删除与所存在的离职用户账号对应的用户权限信息。

8.一种用户管理装置，其特征在于，所述用户管理装置包括：

第一获取模块，用于在接收到业务系统发送的身份认证请求时，根据所述身份认证请求获取待认证用户的用户账号和输入密码；

第一检测模块，用于根据所述用户账号检测所述待认证用户是否已绑定令牌Token；

第一验证模块，用于若否，则根据所述用户账号获取初始密码，验证所述输入密码与所述初始密码是否相匹配，并将第一验证结果返回至所述业务系统，以使得所述业务系统根据所述第一验证结果判断是否允许所述待认证用户进行登录；

第二验证模块，用于若是，则根据所述用户账号获取安全密码，验证所述输入密码与所述安全密码是否相匹配，并将第二验证结果返回至所述业务系统，以使得所述业务系统根据所述第二验证结果判断是否允许所述待认证用户进行登录。

9.一种用户管理设备，其特征在于，所述用户管理设备包括：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用户管理程序，所述用户管理程序被所述处理器执行时实现如权利要求1至7中任一项所述的用户管理方法的步骤。

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用户管理程序，所述用户管理程序被处理器执行时实现如权利要求1至7中任一项所述的用户管理方法的步骤。

用户管理方法、装置、设备及计算机可读存储介质

技术领域

[0001] 本发明涉及金融科技(Fintech)技术领域，尤其涉及一种用户管理方法、装置、设备及计算机可读存储介质。

背景技术

[0002] 随着计算机技术的发展，越来越多的技术(大数据、分布式、区块链Blockchain、人工智能等)应用在金融领域，传统金融业正在逐步向金融科技(Fintech)转变，但由于金融行业的安全性、实时性要求，也对技术提出了更高的要求。

[0003] 在许多金融企业或机构中，往往存在多个业务系统，以给各部门分别提供对应的业务功能。然而，有些业务系统的数据是相关联的，员工往往需要使用多个业务系统，特别是对于管理者，通常需要查看多个业务系统的数据，对应的，需要登录多个系统进行查看。目前，由于身份认证都是在各业务系统内部进行的，因此不同的业务系统需要采用不同的账号和密码进行登录，这样用户需记忆多个账号和密码，较为不便，同时，系统管理者也需要为员工分别注册多个业务系统的账号并进行管理，导致用户管理效率也较低。

发明内容

[0004] 本发明的主要目的在于提供一种用户管理方法、装置、设备及计算机可读存储介质，旨在避免用户需要记忆多个账号和密码的不便，同时提高用户管理效率。

[0005] 为实现上述目的，本发明提供一种用户管理方法，所述用户管理方法包括：

[0006] 在接收到业务系统发送的身份认证请求时，根据所述身份认证请求获取待认证用户的用户账号和输入密码；

[0007] 根据所述用户账号检测所述待认证用户是否已绑定令牌Token；

[0008] 若否，则根据所述用户账号获取初始密码，验证所述输入密码与所述初始密码是否相匹配，并将第一验证结果返回至所述业务系统，以使得所述业务系统根据所述第一验证结果判断是否允许所述待认证用户进行登录；

[0009] 若是，则根据所述用户账号获取安全密码，验证所述输入密码与所述安全密码是否相匹配，并将第二验证结果返回至所述业务系统，以使得所述业务系统根据所述第二验证结果判断是否允许所述待认证用户进行登录。

[0010] 可选地，所述将第一验证结果返回至所述业务系统的步骤之后，还包括：

[0011] 生成Token绑定提示信息，并将所述Token绑定提示信息发送至所述业务系统；

[0012] 在接收到业务系统基于所述Token绑定提示信息返回的Token绑定请求时，根据所述Token绑定请求获取Token序列号，并将所述Token序列号与所述用户账号进行绑定，以用于获取对应Token发送的Token码，所述Token码作为安全密码用于身份认证。

[0013] 可选地，所述安全密码还包括PIN码，所述用户管理方法还包括：

[0014] 生成个人识别密码PIN码设定提示信息，并将所述PIN码设定提示信息发送至所述业务系统；

[0015] 在接收到业务系统基于所述PIN码设定提示信息返回的PIN码设定请求时，根据所述PIN码设定请求获取PIN码，并将所述PIN码与所述用户账号进行关联存储。

[0016] 可选地，所述用户管理方法还包括：

[0017] 在接收到账号分配指令时，根据所述账号分配指令获取目标分配用户的用户信息；

[0018] 基于所述目标分配用户的用户信息和预设生成规则生成对应的用户账号和初始密码，并将所述用户账号、所述初始密码与所述目标分配用户的用户信息进行关联存储。

[0019] 可选地，所述用户管理方法还包括：

[0020] 在接收到权限设定请求时，根据所述权限设定请求获取权限设定信息，所述权限设定信息包括目标用户账号、目标权限信息和目标业务系统；

[0021] 根据所述目标权限信息在预设用户权限列表中更新所述目标用户账号的用户权限信息，并将所述目标用户账号和更新后的用户权限信息同步至所述目标业务系统。

[0022] 可选地，所述用户管理方法还包括：

[0023] 在接收到离职用户列表时，根据所述离职用户列表获取对应的离职用户账号；

[0024] 对所述预设用户权限列表中与所述离职用户账号对应的用户权限信息进行清除处理，并将经清除处理后的预设用户权限列表同步至各业务系统。

[0025] 可选地，所述用户管理方法还包括：

[0026] 在接收到权限上报信息时，提取所述权限上报信息中的用户账号，记作上报用户账号；

[0027] 检测所述上报用户账号中是否存在所述离职用户账号；

[0028] 若存在，则生成对应的提示信息，并将所述提示信息发送至预设管理端，以使得管理人员根据所述提示信息在对应的业务系统中删除与所存在的离职用户账号对应的用户权限信息。

[0029] 此外，为实现上述目的，本发明还提供一种用户管理装置，所述用户管理装置包括：

[0030] 第一获取模块，用于在接收到业务系统发送的身份认证请求时，根据所述身份认证请求获取待认证用户的用户账号和输入密码；

[0031] 第一检测模块，用于根据所述用户账号检测所述待认证用户是否已绑定令牌Token；

[0032] 第一验证模块，用于若否，则根据所述用户账号获取初始密码，验证所述输入密码与所述初始密码是否相匹配，并将第一验证结果返回至所述业务系统，以使得所述业务系统根据所述第一验证结果判断是否允许所述待认证用户进行登录；

[0033] 第二验证模块，用于若是，则根据所述用户账号获取安全密码，验证所述输入密码与所述安全密码是否相匹配，并将第二验证结果返回至所述业务系统，以使得所述业务系统根据所述第二验证结果判断是否允许所述待认证用户进行登录。

[0034] 此外，为实现上述目的，本发明还提供一种用户管理设备，所述用户管理设备包括：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用户管理程序，所述用户管理程序被所述处理器执行时实现如上所述的用户管理方法的步骤。

[0035] 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

存储介质上存储有用户管理程序,所述用户管理程序被处理器执行时实现如上所述的用户管理方法的步骤。

[0036] 本发明提供一种用户管理方法、装置、设备及计算机可读存储介质,在接收到业务系统发送的身份认证请求时,根据该身份认证请求获取待认证用户的用户账号和输入密码;根据用户账号检测该待认证用户是否已绑定Token;若检测到待认证用户还未绑定Token,则根据该用户账号获取初始密码,验证输入密码与初始密码是否相匹配,并将第一验证结果返回至业务系统,以使得业务系统根据第一验证结果判断是否允许该待认证用户进行登录;若检测到待认证用户已绑定Token,则根据该用户账号获取安全密码,验证输入密码与安全密码是否相匹配,并将第二验证结果返回至业务系统,以使得业务系统根据第二验证结果判断是否允许该待认证用户进行登录。通过上述方式,本发明可实现多个业务系统之间的身份认证共享,用户可使用同一账号和密码登录各业务系统,进而通过同一用户管理系统对各业务系统身份认证请求进行身份认证,因此,本发明可避免用户记忆多个业务系统的账号和密码,同时,相比于现有技术中系统管理者需要为用户分别注册多个业务系统的账号并进行管理,本发明简化了用户账号的管理,可提高用户管理效率。

附图说明

[0037] 图1为本发明实施例方案涉及的硬件运行环境的设备结构示意图;

[0038] 图2为本发明用户管理方法第一实施例的流程示意图;

[0039] 图3为本发明用户管理方法第二实施例的流程示意图;

[0040] 图4为本发明用户管理装置第一实施例的功能模块示意图。

[0041] 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

[0042] 应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0043] 参照图1,图1为本发明实施例方案涉及的硬件运行环境的设备结构示意图。

[0044] 本发明实施例用户管理设备可以是智能手机,也可以是PC(Personal Computer,个人计算机)、平板电脑、便携计算机等终端设备。

[0045] 如图1所示,该用户管理设备可以包括: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),可选用户接口1003还可以包括标准的有线接口、无线接口。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。

[0046] 本领域技术人员可以理解,图1中示出的用户管理设备结构并不构成对用户管理设备的限定,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。

[0047] 如图1所示,作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及用户管理程序。

[0048] 在图1所示的终端中,网络接口1004主要用于连接后台服务器,与后台服务器进行数据通信;用户接口1003主要用于连接客户端,与客户端进行数据通信;而处理器1001可以用于调用存储器1005中存储的用户管理程序,并执行以下用户管理方法的各个步骤。

[0049] 基于上述硬件结构,提出本发明用户管理方法的各实施例。

[0050] 本发明提供一种用户管理方法。

[0051] 参照图2,图2为本发明用户管理方法第一实施例的流程示意图。

[0052] 在本实施例中,该用户管理方法包括:

[0053] 步骤S10,在接收到业务系统发送的身份认证请求时,根据所述身份认证请求获取待认证用户的用户账号和输入密码;

[0054] 本实施例的用户管理方法是由用户管理设备实现的,其中,该用户管理设备中搭载有UM系统(User Management,用户管理系统),用于进行身份认证和权限管理,该UM系统可支持多种登录协议,保证各业务系统均可接入,其中,通过统一设置UM系统的接口,以实现支持多种登录协议,UM系统所支持的协议有HTTP(Hyper Text Transfer Protocol,超文本传输协议)认证接口、LDAP(Lightweight Directory Access Protocol,轻量目录访问协议)登陆协议和SSO(Single Sign On,单点登录)单点登录,HTTP认证接口适合JAVA应用系统后台直接对接;LDAP登陆协议适合外购和开源系统,这些系统通常只能使用LDAP登陆协议;SSO单点登陆适合应用系统特别多,用户只需要在浏览器上登陆一个系统,即可在该浏览器上免登陆使用其它系统。各业务系统在接入时,可根据各业务系统的类型选择对应的协议进行接入。

[0055] 在本实施例中,各业务系统在接收到用户在进行登录时触发的身份认证请求时,将该身份认证请求转发至UM系统,此时,UM系统在接收到业务系统发送的身份认证请求时,根据该身份认证请求获取待认证用户的用户账号和输入密码。

[0056] 步骤S20,根据所述用户账号检测所述待认证用户是否已绑定令牌Token;

[0057] 在获取到待认证用户的用户账号和输入密码之后,根据用户账号检测该待认证用户是否已绑定Token(令牌)。需要说明的是,UM系统在创建用户账号时,会生成对应的初始密码(具体过程可参照下述实施例),并下发给各用户,但为保证账号的安全性,还会要求用户领取硬Token(一种硬件设备,可生成6位随机数字用于身份验证),并将用户账号与硬Token的序列号进行绑定(具体的绑定过程可参照下述实施例),用户后续可基于该硬Token产生的动态Token码进行登录。此外,需要说明的是,Token码还可以基于软Token来产生,其中,软Token通常是一段算法,集成在APP页面显示6位随机数字用于身份验证,利用手机的私密性和便携性来给用户带来更好体验。因此,令牌Token可选是硬Token显示的序列号,也可选是UM系统生成并发送至APP页面显示的序列号,该序列号可选为6位随机数字。

[0058] 若否,则执行步骤S31:根据所述用户账号获取初始密码,验证所述输入密码与所述初始密码是否相匹配,并将第一验证结果返回至所述业务系统,以使得所述业务系统根据所述第一验证结果判断是否允许所述待认证用户进行登录;

[0059] 若检测到待认证用户还未绑定Token,说明该待认证用户当前应当是采用初始密码进行登录的,此时,则根据该用户账号获取初始密码,验证输入密码与初始密码是否相匹配,并将第一验证结果返回至业务系统,以使得业务系统根据第一验证结果判断是否允许该待认证用户进行登录。其中,若输入密码与初始密码相匹配,则验证成功,业务系统接收

到UM系统返回的验证成功的验证结果时，可允许该待认证用户进行登录；若输入密码与初始密码不匹配，则验证失败，业务系统接收到UM系统返回的验证失败的验证结果时，则不允许该待认证用户进行登录，并提示待认证用户账号或密码错误。

[0060] 若是，则执行步骤S32：根据所述用户账号获取安全密码，验证所述输入密码与所述安全密码是否相匹配，并将第二验证结果返回至所述业务系统，以使得所述业务系统根据所述第二验证结果判断是否允许所述待认证用户进行登录。

[0061] 若检测到待认证用户已绑定Token，说明该待认证用户当前应当是采用安全密码进行登录的，此时，则根据该用户账号获取安全密码，验证输入密码与安全密码是否相匹配，并将第二验证结果返回至业务系统，以使得业务系统根据第二验证结果判断是否允许该待认证用户进行登录。其中，该安全密码可以为动态生成的Token码，还可以是由动态生成的Token码与用户设定的PIN(Personal Identification Number，个人识别密码)码组成的密码。若输入密码与安全密码相匹配，则验证成功，业务系统接收到UM系统返回的验证成功的验证结果时，可允许该待认证用户进行登录；若输入密码与安全密码不匹配，则验证失败，业务系统接收到UM系统返回的验证失败的验证结果时，则不允许该待认证用户进行登录，并提示待认证用户账号或密码错误。

[0062] 本发明在银行等金融机构的用户管理系统中，接收到各个业务系统发送的身份认证请求时，先根据上述操作过程进行身份认证，实现多个业务系统之间的身份认证共享，避免了用户记忆多个业务系统的账号和密码，同时，相比于系统管理者需要为用户分别注册多个业务系统的账号并进行管理，本发明简化了用户账号的管理，可提高银行等金融机构的用户管理效率，降低了银行等金融机构的管理成本。

[0063] 本发明实施例提供一种用户管理方法，在接收到业务系统发送的身份认证请求时，根据该身份认证请求获取待认证用户的用户账号和输入密码；根据用户账号检测该待认证用户是否已绑定Token；若检测到待认证用户还未绑定Token，则根据该用户账号获取初始密码，验证输入密码与初始密码是否相匹配，并将第一验证结果返回至业务系统，以使得业务系统根据第一验证结果判断是否允许该待认证用户进行登录；若检测到待认证用户已绑定Token，则根据该用户账号获取安全密码，验证输入密码与安全密码是否相匹配，并将第二验证结果返回至业务系统，以使得业务系统根据第二验证结果判断是否允许该待认证用户进行登录。通过上述方式，本发明实施例可实现多个业务系统之间的身份认证共享，用户可使用同一账号和密码登录各业务系统，进而通过同一用户管理系统对各业务系统身份认证请求进行身份认证，因此，本发明实施例可避免用户记忆多个业务系统的账号和密码，同时，相比于现有技术中系统管理者需要为用户分别注册多个业务系统的账号并进行管理，本发明实施例简化了用户账号的管理，可提高用户管理效率。

[0064] 进一步地，在上述步骤S31之后，该用户管理方法还包括：

[0065] 步骤A，生成Token绑定提示信息，并将所述Token绑定提示信息发送至所述业务系统；

[0066] 在本实施例中，在检测到待认证用户还未绑定Token后，为保证用户账号的安全性，需提醒用户及时绑定Token，具体的，UM系统可生成Token绑定提示信息，并将该Token绑定提示信息发送至业务系统，此时，业务系统可在用户端显示对应的提示窗口，以显示该Token绑定提示信息，来提醒该用户绑定Token。对应的，用户可领取硬Token，并在对应的绑

定界面填写领取到的硬Token的序列号，以触发Token绑定请求，业务系统在接收到该Token绑定请求时，将该Token绑定请求转发至UM系统。

[0067] 步骤B，在接收到业务系统基于所述Token绑定提示信息返回的Token绑定请求时，根据所述Token绑定请求获取Token序列号，并将所述Token序列号与所述用户账号进行绑定，以用于获取对应Token发送的Token码，所述Token码作为安全密码用于身份认证。

[0068] UM系统在接收到业务系统基于该Token绑定提示信息返回的Token绑定请求时，根据该Token绑定请求获取Token序列号，并将该Token序列号与用户账号进行绑定，以用于获取对应Token发送的Token码，其中，该Token码作为安全密码用于身份认证。其中，根据安全密码的类型，用户可直接用该Token码作为密码进行登录，还可以将Token码与用户设定的PIN码作为安全密码进行登录。

[0069] 需要说明的是，在具体实施例中，上述步骤A可由业务系统执行，业务系统在接收到Token绑定请求时，将所述Token绑定请求转发至UM系统，进而UM系统执行步骤：根据所述Token绑定请求获取Token序列号，并将所述Token序列号与所述用户账号进行绑定。

[0070] 本实施例中，为保障用户账号的安全性，可通过Token码进行登录，因此，本实施例中在检测到待认证用户还未绑定Token后，提醒用户及时绑定Token，进而将Token绑定请求中的Token序列号与用户账号进行绑定，以用于获取对应Token发送的Token码，进而将该Token码用于后续的身份认证。通过上述方式，可保障用户账号的安全性。

[0071] 为进一步保障用户账号的安全性，该安全密码除可包括Token码外，还可以包括PIN码，在上述步骤B之后，该用户管理方法还包括：

[0072] 步骤C，生成个人识别密码PIN码设定提示信息，并将所述PIN码设定提示信息发送至所述业务系统；

[0073] 在本实施例中，为进一步保障用户账号的安全性，可采用双因素验证方式，即用户预先设定一PIN码，然后将Token码与用户设定的PIN码作为保密密码进行验证，通过该种双因素验证方式，可以避免硬Token和用户账号被窃取时账号被他人登录，从而可进一步保证用户账号的安全性。

[0074] 在本实施例中，在用户绑定完Token之后，还可以进一步地提示用户设定PIN码，具体的，UM生成个人识别密码PIN码设定提示信息，并将该PIN码设定提示信息发送至业务系统。此时，业务系统可在用户端显示对应的提示窗口，以显示该PIN码设定提示信息，来提醒该用户设定PIN码。对应的，用户可在对应的PIN码设定界面设置PIN码，以触发PIN码设定请求，业务系统在接收到该PIN码设定请求时，将该PIN码设定请求转发至UM系统。

[0075] 步骤D，在接收到业务系统基于所述PIN码设定提示信息返回的PIN码设定请求时，根据所述PIN码设定请求获取PIN码，并将所述PIN码与所述用户账号进行关联存储。

[0076] UM系统在接收到业务系统基于该PIN码设定提示信息返回的PIN码设定请求时，根据该PIN码设定请求获取PIN码，并将该PIN码与用户账号进行关联存储，以用于后续与接收到的Token码组成安全密码，来进行身份认证。

[0077] 需要说明的是，在具体实施例中，上述步骤C可由业务系统执行，业务系统在接收到PIN码设定请求时，将所述PIN码设定请求转发至UM系统，进而UM系统执行步骤：根据所述PIN码设定请求获取PIN码，并将所述PIN码与所述用户账号进行关联存储。

[0078] 本实施例中，为进一步保障用户账号的安全性，可通过Token码和用户设定的PIN

码组成密码以进行登录，因此，本实施例中在检测到待认证用户绑定Token之后，还可以提醒用户及时设定PIN码，进而将PIN码设定请求中的PIN码与用户账号进行关联存储，以用于后续与接收到的Token码组成安全密码，来进行身份认证。通过上述方式，实现了双因素验证方式，可进一步保障用户账号的安全性。

[0079] 进一步地，在上述实施例中，在步骤S10之前，该用户管理方法还包括：

[0080] 步骤E，在接收到账号分配指令时，根据所述账号分配指令获取目标分配用户的用户信息；

[0081] 在本实施例中，当雇佣了新员工时，可通过该UM系统自动为他们分配用户账号和初始密码。具体的，管理人员可在UM系统中选择账号分配选项，进而在对应的配置界面输入新员工的用户信息后，触发账号分配指令。此时，UM系统在接收到账号分配指令时，根据该账号分配指令获取目标分配用户的用户信息。其中，用户信息可以包括但不限于用户姓名、身份证号、性别、年龄、用户所属部门等。

[0082] 步骤F，基于所述目标分配用户的用户信息和预设生成规则生成对应的用户账号和初始密码，并将所述用户账号、所述初始密码与所述目标分配用户的用户信息进行关联存储。

[0083] 然后，基于该目标分配用户的用户信息和预设生成规则生成对应的用户账号和初始密码，其中，该预设生成规则可根据实际情况进行设定，例如，可以以用户的姓名拼音及当前员工编号作为用户名，以用户的身份证后6位作为初始密码；或者以用户的姓名作为用户名，以当前员工编号作为初始密码，此处仅作举例，不作为对本发明的具体限定。该用户账号和初始密码可用于各业务系统。

[0084] 在生成用户账号和初始密码后，将用户账号、初始密码与目标分配用户的用户信息进行关联存储，以便于后续进行身份认证和用户查询等。

[0085] 在本实施例中，可通过UM系统统一设定用户账号和初始密码，该用户账号和初始密码可用于各业务系统，而无需各个业务系统分别为用户设定用户账号和初始密码，可提高用户管理效率，同时，也可以避免用户记忆多套账号和密码。

[0086] 由于现有的用户权限管理也是在各业务系统内部进行的，无法实现对权限的统一设定和管理，对此，基于上述各实施方式，提出本发明用户管理方法的第二实施例。具体的，参照图3，在本实施例中，该用户管理方法还包括：

[0087] 步骤S40，在接收到权限设定请求时，根据所述权限设定请求获取权限设定信息，所述权限设定信息包括目标用户账号、目标权限信息和目标业务系统；

[0088] 在本实施例中，员工可通过ITSM系统(IT Service Management，IT服务管理系统)，即事件审批系统来申请用户权限，当审批通过后，ITSM系统会生成对应的权限设定请求；或，管理人员可通过ITSM系统的权限编辑工具来设定用户的用户权限，进而可触发权限设定请求。之后，ITSM系统会将权限设定请求发送至UM系统。此时，UM系统在接收到权限设定请求时，可根据该权限设定请求获取权限设定信息，其中，权限设定信息包括目标用户账号、目标权限信息和目标业务系统，权限设定可以包括权限的更改、删除、新增等操作，涉及用户角色关系变更、角色权限关系变更、角色维护、权限维护等。

[0089] 步骤S50，根据所述目标权限信息在预设用户权限列表中更新所述目标用户账号的用户权限信息，并将所述目标用户账号和更新后的用户权限信息同步至所述目标业务系

统。

[0090] 在获取到权限设定信息之后，根据目标权限信息在预设用户权限列表中更新该目标用户账号的用户权限信息，并将目标用户账号和更新后的用户权限信息同步至目标业务系统，以使得目标业务系统可同步更新对应的用户权限信息。

[0091] 通过上述方式，本实施例可通过UM系统实现对各业务系统的用户权限的统一管理，同时，通过将更新后的用户权限信息同步至业务系统，还可保证即使在UM系统挂掉的情况下，用户也可以使用业务系统，从而可保证业务系统的高可用。

[0092] 进一步的，基于上述第二实施例，提出本发明用户管理方法的第三实施例。

[0093] 在本实施例中，在上述步骤S50之后，该用户管理方法还包括：

[0094] 步骤G，在接收到离职用户列表时，根据所述离职用户列表获取对应的离职用户账号；

[0095] 在本实施例中，当用户离职后，相关部门可整理出离职用户列表，并上传至UM系统，以使得UM系统删除离职用户的权限。具体的，UM系统在接收到离职用户列表时，可根据该离职用户列表获取对应的离职用户账号。其中，该离职用户列表中至少包括离职用户姓名或离职用户账号，若离职用户列表中只包括离职用户姓名时，可根据该用户姓名查找得到对应的离职用户账号；若离职用户列表中只包括离职用户账号时，则可直接提取出该离职用户列表中的离职用户账号。

[0096] 步骤H，对所述预设用户权限列表中与所述离职用户账号对应的用户权限信息进行清除处理，并将经清除处理后的预设用户权限列表同步至各业务系统。

[0097] 然后，对预设用户权限列表中与离职用户账号对应的用户权限信息进行清除处理，并将经清除处理后的预设用户权限列表同步至各业务系统，以使得各业务系统可同步更新对应的用户权限信息。需要说明的是，本实施例中是针对可接入UM系统做权限管理的业务系统。

[0098] 通过上述方式，本实施例中，可智能统一自动清理离职用户的用户权限，无需各个业务系统分别进行清除，可提高用户管理效率，同时可避免用户离职后获取系统数据、造成内部数据泄露的情况，可保障系统数据的安全性。

[0099] 进一步的，基于上述各实施例，提出本发明用户管理方法的第四实施例。

[0100] 在本实施例中，该用户管理方法还包括：

[0101] 步骤I，在接收到权限上报信息时，提取所述权限上报信息中的用户账号，记作上报用户账号；

[0102] 在本实施例中，由于某些金融企业或机构常常外购一些某些系统，如开源系统，由于无法对某些外购和开源系统做系统改造，使得这些业务系统无法接入UM系统做权限管理，因此无法保证这些业务系统没有非法权限，比如说用户离职或者转岗了权限还存在。对此，本实施例中，通过让这些系统进行权限上报的方式，来获取这些业务系统中的用户权限信息，进而通过检测来可发现非法权限，如离职用户权限还在。具体的，在接收到离职用户列表时，还可以通知这些无法接入UM系统做权限管理的业务系统对其系统内的用户权限信息进行权限上报。UM系统在接收到权限上报信息时，提取权限上报信息中的用户账号，记作上报用户账号。

[0103] 步骤J，检测所述上报用户账号中是否存在所述离职用户账号；

[0104] 若存在，则执行步骤K：生成对应的提示信息，并将所述提示信息发送至预设管理端，以使得管理人员根据所述提示信息在对应的业务系统中删除与所存在的离职用户账号对应的用户权限信息。

[0105] 然后，检测上报用户账号中是否存在离职用户账号，若上报用户账号中存在离职用户账号，说明存在非法权限，此时，则生成对应的提示信息，并将提示信息发送至预设管理端，以使得管理人员根据该提示信息在对应的业务系统中删除与所存在的离职用户账号对应的用户权限信息，以免用户离职后仍具有权限、从而获取系统数据而造成内部数据泄露的情况，可保障系统数据的安全性。

[0106] 本发明还提供一种用户管理装置。

[0107] 参照图4，图4为本发明用户管理装置第一实施例的功能模块示意图。

[0108] 如图4所示，所述用户管理装置包括：

[0109] 第一获取模块10，用于在接收到业务系统发送的身份认证请求时，根据所述身份认证请求获取待认证用户的用户账号和输入密码；

[0110] 第一检测模块20，用于根据所述用户账号检测所述待认证用户是否已绑定令牌Token；

[0111] 第一验证模块30，用于若否，则根据所述用户账号获取初始密码，验证所述输入密码与所述初始密码是否相匹配，并将第一验证结果返回至所述业务系统，以使得所述业务系统根据所述第一验证结果判断是否允许所述待认证用户进行登录；

[0112] 第二验证模块40，用于若是，则根据所述用户账号获取安全密码，验证所述输入密码与所述安全密码是否相匹配，并将第二验证结果返回至所述业务系统，以使得所述业务系统根据所述第二验证结果判断是否允许所述待认证用户进行登录。

[0113] 进一步地，所述用户管理装置还包括：

[0114] 第一发送模块，用于生成Token绑定提示信息，并将所述Token绑定提示信息发送至所述业务系统；

[0115] 序列号绑定模块，用于在接收到业务系统基于所述Token绑定提示信息返回的Token绑定请求时，根据所述Token绑定请求获取Token序列号，并将所述Token序列号与所述用户账号进行绑定，以用于获取对应Token发送的Token码，所述Token码作为安全密码用于身份认证。

[0116] 进一步地，所述安全密码还包括PIN码，所述用户管理装置还包括：

[0117] 第二发送模块，用于生成个人识别密码PIN码设定提示信息，并将所述PIN码设定提示信息发送至所述业务系统；

[0118] 第一关联存储模块，用于在接收到业务系统基于所述PIN码设定提示信息返回的PIN码设定请求时，根据所述PIN码设定请求获取PIN码，并将所述PIN码与所述用户账号进行关联存储。

[0119] 进一步地，所述用户管理装置还包括：

[0120] 第二获取模块，用于在接收到账号分配指令时，根据所述账号分配指令获取目标分配用户的用户信息；

[0121] 第二关联存储模块，用于基于所述目标分配用户的用户信息和预设生成规则生成对应的用户账号和初始密码，并将所述用户账号、所述初始密码与所述目标分配用户的用

户信息进行关联存储。

[0122] 进一步地，所述用户管理装置还包括：

[0123] 第三获取模块，用于在接收到权限设定请求时，根据所述权限设定请求获取权限设定信息，所述权限设定信息包括目标用户账号、目标权限信息和目标业务系统；

[0124] 权限更新模块，用于根据所述目标权限信息在预设用户权限列表中更新所述目标用户账号的用户权限信息，并将所述目标用户账号和更新后的用户权限信息同步至所述目标业务系统。

[0125] 进一步地，所述用户管理装置还包括：

[0126] 第四获取模块，用于在接收到离职用户列表时，根据所述离职用户列表获取对应的离职用户账号；

[0127] 权限清除模块，用于对所述预设用户权限列表中与所述离职用户账号对应的用户权限信息进行清除处理，并将经清除处理后的预设用户权限列表同步至各业务系统。

[0128] 进一步地，所述用户管理装置还包括：

[0129] 账号提取模块，用于在接收到权限上报信息时，提取所述权限上报信息中的用户账号，记作上报用户账号；

[0130] 第二检测模块，用于检测所述上报用户账号中是否存在所述离职用户账号；

[0131] 第三发送模块，用于若存在，则生成对应的提示信息，并将所述提示信息发送至预设管理端，以使得管理人员根据所述提示信息在对应的业务系统中删除与所存在的离职用户账号对应的用户权限信息。

[0132] 其中，上述用户管理装置中各个模块的功能实现与上述用户管理方法实施例中各步骤相对应，其功能和实现过程在此处不再一一赘述。

[0133] 本发明还提供一种计算机可读存储介质，该计算机可读存储介质上存储有用户管理程序，所述用户管理程序被处理器执行时实现如以上任一项实施例所述的用户管理方法的步骤。

[0134] 本发明计算机可读存储介质的具体实施例与上述用户管理方法各实施例基本相同，在此不作赘述。

[0135] 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、物品或者系统不仅包括那些要素，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、物品或者系统所固有的要素。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、物品或者系统中还存在另外的相同要素。

[0136] 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。

[0137] 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如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(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所述的方法。

[0138] 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。

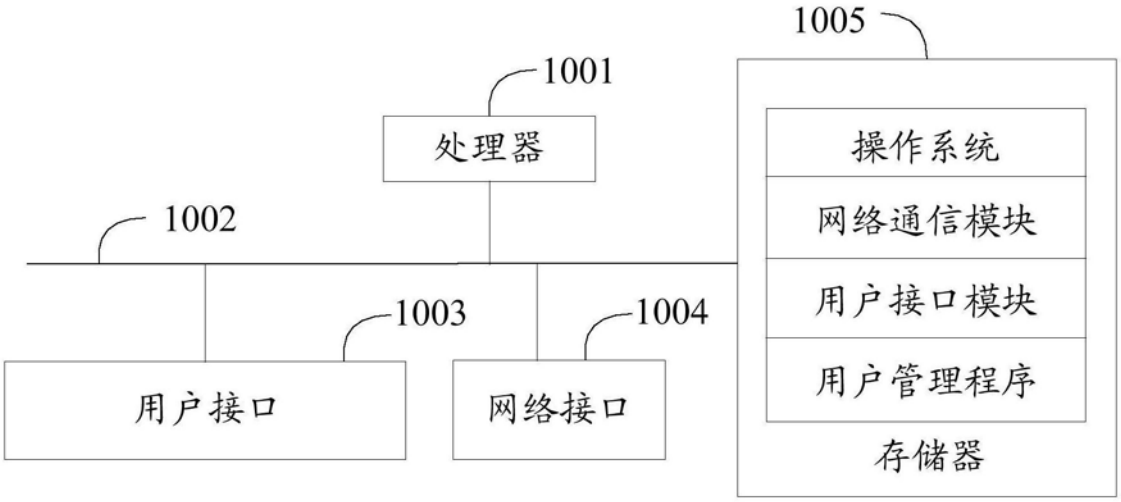
1005
1001
处理器
操作系统
网络通信模块
用户接口模块
用户管理程序
1002
1003
1004
用户接口
网络接口
存储器

图1

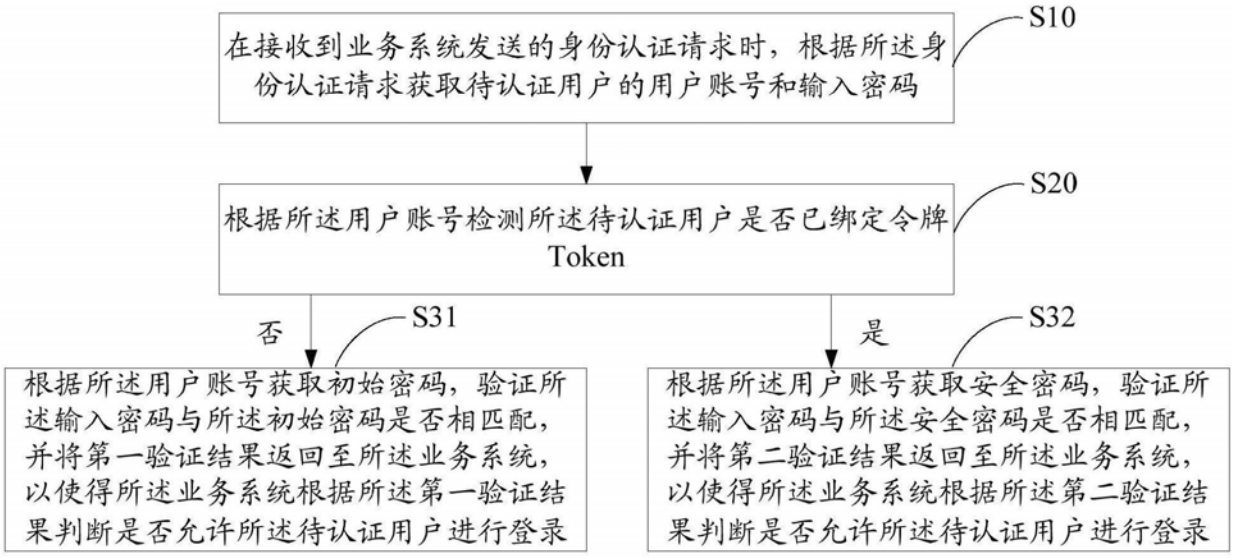
在接收到业务系统发送的身份认证请求时，根据所述身份认证请求获取待认证用户的用户账号和输入密码
S10
根据所述用户账号检测所述待认证用户是否已绑定令牌Token
S20
否
S31
根据所述用户账号获取初始密码，验证所述输入密码与所述初始密码是否相匹配，并将第一验证结果返回至所述业务系统，以使得所述业务系统根据所述第一验证结果判断是否允许所述待认证用户进行登录
是
S32
根据所述用户账号获取安全密码，验证所述输入密码与所述安全密码是否相匹配，并将第二验证结果返回至所述业务系统，以使得所述业务系统根据所述第二验证结果判断是否允许所述待认证用户进行登录

图2

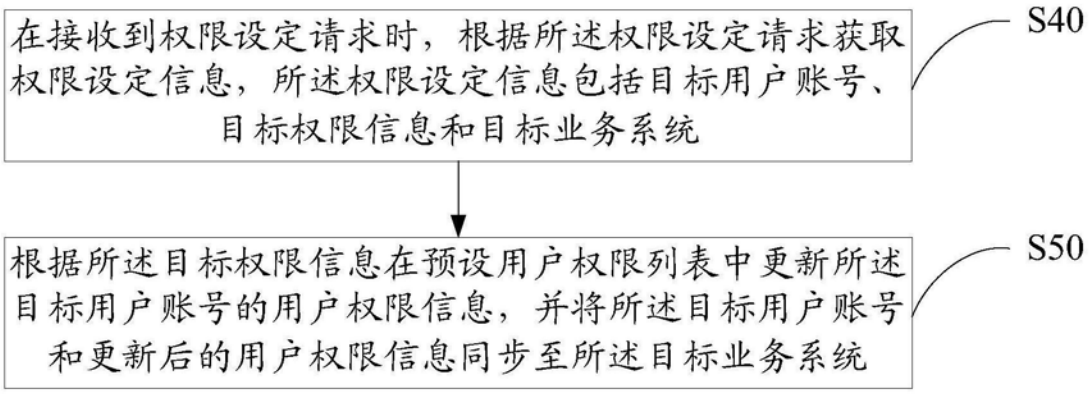
在接收到权限设定请求时，根据所述权限设定请求获取权限设定信息，所述权限设定信息包括目标用户账号、目标权限信息和目标业务系统
S40
根据所述目标权限信息在预设用户权限列表中更新所述目标用户账号的用户权限信息，并将所述目标用户账号和更新后的用户权限信息同步至所述目标业务系统
S50

图3

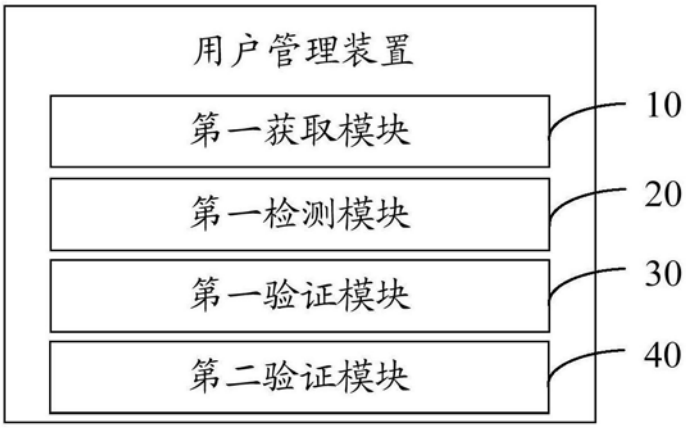
用户管理装置
第一获取模块
10
第一检测模块
20
第一验证模块
30
第二验证模块
40

图4