

身份校验、登录方法、装置及计算机设备

技术领域

[01] 本说明书涉及互联网技术领域，尤其涉及身份校验、登录方法、装置及计算机设备。

背景技术

- 5 [02] 互联网已成为人们生活中很重要的一部分，用户通过互联网能够获取各种服务（如购物、娱乐、内容或社交等等）。随着互联网服务的快速膨胀，形式多样、种类繁多的互联网产品面向用户，用户需要管理大量网站或应用的账户，维护成本非常大。

发明内容

- 10 [03] 为克服相关技术中存在的问题，本说明书实施例提供了身份校验、登录方法、装置及计算机设备。

[04] 根据本说明书实施例的第一方面，提供一种登录方法，包括：

[05] 在服务装置的登录流程被触发后，所述服务装置中的对接模块获取目标主账户的校验信息并发送给身份管理装置；

- 15 [06] 所述身份管理装置接收到所述校验信息后，利用已注册主账户的身份识别信息集对所述目标主账户进行身份校验，在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息，并发送给所述对接模块；

[07] 在所述对接模块接收到所述登录信息后，所述服务装置确定目标子账户并登录服务端。

[08] 可选的，所述校验信息包括：所述目标主账户的标识以及至少一种身份识别信息。

- 20 [09] 可选的，所述目标主账户的标识与对应用户的身份证件号码相关联。

[10] 可选的，所述校验信息所包括的至少一种身份识别信息，基于所述服务装置的安全级别而确定。

[11] 可选的，所述服务装置确定目标子账户，包括：

[12] 若接收到多个子账户的登录信息，展示所述多个子账户后，获取被用户选择的子账

户作为所述目标子账户。

[13]可选的, 所述主账户的身份识别信息集包括如下一类或多类身份识别信息: 网络身份识别信息、个人身份识别信息或生物识别信息。

[14]根据本说明书实施例的第二方面, 提供一种身份管理装置, 包括:

- 5 [15]身份信息管理模块, 用于: 管理已注册主账户、以及所述已注册主账户为至少一个服务装置关联的至少一个子账户; 所述已注册主账户对应有身份识别信息集, 所述子账户用于所述服务装置登录服务端;

[16]身份校验模块, 用于: 接收所述服务装置的对接模块发送的目标主账户的校验信息, 利用所述身份识别信息集对所述目标主账户进行身份校验, 在通过身份校验后获取所述

- 10 目标主账户预先为所述服务装置关联的至少一个子账户的登录信息, 并发送给所述对接模块。

[17]可选的, 所述已注册主账户与对应用户的身份证件信息绑定。

[18]可选的, 所述子账户对应有用于身份校验的身份识别信息子集, 所述身份识别信息子集基于所述服务装置的安全级别而确定。

- 15 [19]可选的, 所述身份识别信息集包括如下一类或多类身份识别信息: 网络身份识别信息、个人身份识别信息或生物识别信息。

[20]可选的, 所述身份信息管理模块, 还用于: 至少基于所述已注册主账户的年龄确定所述已注册主账户的内容等级参数, 并发送给所述对接模块。

[21]可选的, 所述装置还包括: 安全控制模块, 用于:

- 20 [22]获取所述服务装置发送的用户行为数据, 基于所述用户行为数据进行风险控制。

[23]可选的, 所述装置还包括: 安全控制模块, 用于:

[24]在主账户注册阶段, 基于提交的身份识别信息是否与其他已注册主账户的身份识别信息相同进行风险控制。

[25]根据本说明书实施例的第三方面, 提供一种服务装置, 所述服务装置包括:

- 25 [26]对接模块, 用于: 在所述服务装置的登录流程被触发后, 获取目标主账户的校验信息并发送给所述身份管理装置; 以及, 接收所述身份管理装置发送的至少一个子账户的登录信息;

- [27]登录模块,用于:在所述对接模块接收到所述登录信息后,确定目标子账户并登录服务端。
- [28]可选的,所述目标主账户的标识与对应用户的身份证件号码相关联。
- [29]可选的,所述校验信息所包括的至少一种身份识别信息,基于所述服务装置的安全
- 5 级别而确定。
- [30]可选的,所述对接模块,还用于接收所述目标子账户对应的主账户的内容等级参数;
- [31]所述服务装置还包括展示模块,用于:根据所述内容等级参数确定所展示的服务内容并展示。
- [32]根据本说明书实施例的第四方面,提供一种身份校验方法,所述方法包括:
- 10 [33]接收服务装置的对接模块发送的目标主账户的校验信息;
- [34]利用已注册主账户对应的身份识别信息集对所述目标主账户进行身份校验;其中,所述已注册主账户为至少一个服务装置预先关联有至少一个子账户;所述子账户用于所述服务装置登录服务端;
- [35]在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户
- 15 的登录信息,并发送给所述对接模块。
- [36]根据本说明书实施例的第五方面,提供一种登录方法,所述方法包括:
- [37]在登录流程被触发后,获取目标主账户的校验信息并发送给所述身份管理装置;
- [38]接收所述身份管理装置发送的至少一个子账户的登录信息;
- [39]从所述至少一个子账户中确定目标子账户并登录服务端。
- 20 [40]根据本说明书实施例的第六方面,提供一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其中,所述处理器执行所述程序时实现如下方法:
- [41]接收服务装置的对接模块发送的目标主账户的校验信息;
- [42]利用已注册主账户对应的身份识别信息集对所述目标主账户进行身份校验;其中,
- 25 所述已注册主账户为至少一个服务装置预先关联有至少一个子账户;所述子账户用于所述服务装置登录服务端;
- [43]在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户

的登录信息，并发送给所述对接模块。

[44]根据本说明书实施例的第七方面，提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如下方法：

5 [45]在登录流程被触发后，获取目标主账户的校验信息并发送给所述身份管理装置；

[46]接收所述身份管理装置发送的至少一个子账户的登录信息；

[47]从所述至少一个子账户中确定目标子账户并登录服务端。

[48]本说明书的实施例提供的技术方案可以包括以下有益效果：

10 [49]本说明书实施例中，身份管理装置用于统一管理用户身份，该装置与其他服务方独立，可不与服务方的服务装置绑；用户可注册主账户，该主账户用于登录身份管理装置，同时，可基于主账户关联一个或多个子账户，所述子账户对应各个服务方，用于所述服务装置登录服务端。基于上述方案，用户在登录服务装置时，由身份管理装置对用户的主账户进行身份校验，在校验通过后，采用预先为所述服务装置关联的其中一个子账户登录服务端。

15 [50]基于此，用户只需要记住主账户及身份识别信息，即可登录多个不同的服务装置，并且，用户可为服务装置关联多个子账户，从而满足用户的个性化需求；另一方面，由于用于登录服务装置的子账户都与主账户关联，因此可以根据身份追溯到身份管理装置侧的主账户，从而为网络安全提供保障。

20 [51]应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书。

附图说明

[52]此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本说明书的实施例，并与说明书一起用于解释本说明书的原理。

25 [53]图 1A 是本说明书根据一示例性实施例示出的一种身份管理装置与服务装置的应用场景示意图。

[54]图 1B 是本说明书根据一示例性实施例示出的一种用户注册主账户的示意图。

[55]图 1C 是本说明书根据一示例性实施例示出的一种用户的主账户与子账户的示意图。

[56]图 2A 是本说明书根据一示例性实施例示出的一种登录方法的流程图。

[57]图 2B 是本说明书根据一示例性实施例示出的一种 APP 上用户注册的示意图。

[58]图 2C 是本说明书根据一示例性实施例示出的一种用户修改身份识别信息的示意图。

[59]图 2D 和图 2E 分别是本说明书根据一示例性实施例示出的一种不同场景下对应不同
5 身份识别信息子集的示意图。

[60]图 2F 是本说明书根据一示例性实施例示出的一种内容分级的示意图。

[61]图 2G 是本说明书根据一示例性实施例示出的一种身份回溯的示意图。

[62]图 2H 是本说明书根据一示例性实施例示出的一种挖掘黄牛团伙的示意图。

[63]图 3 是本说明书根据一示例性实施例示出的一种登录方法的流程图。

10 [64]图 4 是本说明书根据一示例性实施例示出的另一种登录方法的流程图。

[65]图 5 是本说明书实施例服务装置/身份管理装置所在计算机设备的一种硬件结构图。

具体实施方式

[66]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施
15 例中所描述的实施方式并不代表与本说明书相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的装置和方法的例子。

[67]在本说明书使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书。在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和
20 /或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[68]应当理解，尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……
25 时”或“当……时”或“响应于确定”。

[69]互联网服务的产品越来越多，用户需要管理大量网站或应用账户，维护成本巨大。而随着互联网产品频出、服务质量以及用户自身原因，在不同时期用户可能使用不同登

录名、邮箱、手机号、或者设置不同的安全信息如安全问题等，随时间推移，也可能出现用户遗忘早期账户等等问题。

[70]基于此，本说明书实施例提供了一种身份校验及登录方案，如图 1A 所示，是本说明书根据一示例性实施例示出的一种身份管理系统架构示意图，包括由身份管理方设置的身份管理装置 10；与所述身份管理装置对接的一个或多个服务装置（客户端），各个服务装置由服务方提供，可以包括可安装于智能手机或个人计算机等终端设备上的计算机程序等等。

[71]其中，本说明书实施例身份管理装置可以包括部署于身份管理方配置的服务器（也可以是服务集群或云服务器）上的服务端，也可以包括安装于用户设备上的客户端，客户端可以与服务端配合完成身份管理方案。

[72]作为例子，如图 1A 所示，身份管理装置可包括：

[73]身份信息模块 101，用于：管理已注册主账户、以及所述已注册主账户为至少一个服务装置关联的至少一个子账户；所述已注册主账户对应有身份识别信息集，所述子账户用于所述服务装置登录服务端。

[74]身份校验模块 102，用于：接收所述服务装置的对接模块发送的目标主账户的校验信息，利用所述身份识别信息集对所述目标主账户进行身份校验，在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息，并发送给所述对接模块。

[75]本说明书实施例方案中，身份管理装置用于统一管理用户身份，该装置与其他服务方独立，可不与服务方的服务装置绑定。身份管理装置所管理的主账户，可以理解为一个自然人账户，自然人表示生物意义上的一个取得民事资格的主体。如图 1B 所示，用户可采用有效合法的身份证件在身份识别装置注册个人的主账户，注册后，用户可绑定身份识别信息，可选的，可以绑定 3 个以上的身份识别信息，身份识别信息可包括网络身份识别信息、个人身份识别信息或生物识别信息等。

[76]其中，网络身份识别信息可以包括：账户名、账户昵称、密码、手机号码、邮箱地址、密码保护问题和答案等。

[77]个人身份信息，可以包括身份证号码、护照号码或驾驶证号码等。

[78]生物识别信息，可以包括指纹信息、虹膜信息、人脸信息、声纹信息以及未来与生物特征相关的信息等等。

[79]本实施例中，用户所绑定的身份识别信息可构成身份识别信息集，在需要身份校验的情况下，身份管理系统可根据身份识别信息集中的一个或多个身份识别信息对用户身份进行校验。

5 [80]可选的，用户还可添加应急联系人、安全问题等其他安全信息，还可添加兴趣爱好等其他选填信息。

[81]由上述实施例可知，身份管理装置作为身份集中管理中心，每个用户（自然人）对应一套身份识别信息，并且只有一个主账户。可选的，每个自然人有唯一的身份证件（个人身份证、护照或驾驶证等），主账户可以与对应用户的身份证件信息绑定，主账户的标识可以与对应用户的身份证件信息关联，例如，可以采用身份证号码作为主账户的标
10 识，也可以基于身份证号码添加其他标识符后作为主账户的标识。

[82]在该主账户的基础上，用户可以关联一个或多个子账户，一个子账户可对应一个或多个服务装置，用于所述服务装置登录服务端。如图 1C 所示，是本说明书根据一示例性实施例示出的用户与多个子账户的关系示意图，该子账户可以理解为用户在使用不同服务方产品时所采用的角色（也可称为虚拟身份，图 1C 中该自然人可以对应有 N 个身
15 份），每个子账户对应一类服务装置，用户可以针对一个服务装置关联一个或多个子账户。用户可在身份管理系统中关联子账户，也可以是在服务方侧关联子账户。关联子账户的过程中，需要该用户登录身份识别系统的主账户，之后关联基于该主账户的子账户，还可设置头像、昵称等子账户信息，生成子账户标识等等。

[83]在关联有子账户的情况下，基于本实施例的方案，用户登录服务装置的过程，可以
20 理解为：在服务侧首先对用户的主账户进行身份校验，在通过身份校验后，采用该主账户预先为所述服务装置关联的其中一个子账户登录服务端。本说明书实施例提供一种登录方法，如图 2A 所示，包括：

[84]在步骤 202 中，服务装置的登录流程被触发。

[85]在步骤 204 中，所述服务装置中的对接模块获取目标主账户的校验信息。

25 [86]在步骤 206 中，对接模块将校验信息发送给身份管理装置。

[87]在步骤 208 中，身份管理装置接收所述校验信息，利用已注册主账户的身份识别信息集对所述目标主账户进行身份校验。

[88]在步骤 210 中，身份管理装置在通过身份校验后，获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息。

[89]在步骤 212 中，身份管理装置将登录信息发送给所述对接模块。

[90]在步骤 214 中，所述对接模块接收到所述登录信息后，所述服务装置确定目标子账户并登录服务端。

[91]如图 2B 所示，是本说明书根据一示例性实施例示出的用户在某个服务装置登录服务端的界面示意图，其中服务装置采用安装于智能手机上的 APP 进行示意，在用户点击 APP 上的登录选项（图 2B 中未示出），服务装置的登录流程被触发，如图 2B 所示，首先需要由身份管理系统对用户的主账户进行身份校验。

[92]作为例子，本实施例中，服务装置内置的对接模块可以在服务装置的应用界面示出目标主账户的校验信息获取接口，在图 2B 中具体为主账户标识的输入框，以及“点此输入密码”选项和“点此录入指纹”选项。校验信息用于对当前需要登录用户的主账户进行校验，可以包括目标主账户的标识以及至少一种身份识别信息，用户可以通过上述校验信息获取接口输入主账户标识和身份识别信息。

[93]其中，服务装置中的对接模块需要与身份管理装置进行数据交互。实际应用中，身份管理装置与服务装置由不同厂商所生产，且两者直接进行数据交互，则双方需相互向对方公开信息传输协议，以实现数据交互。然而，双方公开信息传输协议可能会降低安全性，因此，本实施例的对接模块可以由身份管理方提供给服务方，对接模块的具体功能由身份管理方提供，则身份管理方无须向服务方公开较多的数据传输协议。对接模块提供给服务方后，可以由服务方整合，作为服务装置的子模块与身份管理装置进行数据交互，从而可减少安全风险，减少服务方的开发成本和难度。

[94]由前述描述可知，可以利用主账户的身份识别信息集中的一个或多个身份识别信息进行身份校验。可以理解，各个身份识别信息具有不同的重要性或安全性；例如，生物识别信息具有唯一性、破译难度较大且窃取难度也较大，涉及用户的指纹、虹膜等个人生物特征，此类信息的安全级别较高；而邮箱地址、密码等具有可更改特点、破译和可窃取难度也较低，安全级别低于生物识别信息。本实施例中，对于用于校验的身份识别信息，实际应用中可以根据需要灵活配置。

[95]本实施例中，若用户的身份识别信息遗失、需要变更、或需要添加新的身份识别信息，可登录身份识别系统进行身份识别信息的管理。作为例子，身份识别特征按破译以及可窃取的难易程度等因素可划分为多个安全级别，以高、中、低三个安全级别为例，如图 2C 所示，变更身份识别信息的处理过程可包括如下：

[96]变更低安全等级特征：需至少其他两个特征校验通过；

[97]变更中安全等级特征：需至少其他两个特征校验通过，安全问题验证通过；

[98]变更高安全等级特征：需至少其他两个特征校验通过，同时获得应急联系人认可。

[99]实际应用中，互联网服务具有多样性特点，有些互联网服务对安全性的要求会比较
5 高，例如支付等相关服务；而有些互联网服务的登录过程对安全性可以稍微降低要求。
基于此，本说明书实施例中，如图 2D 和 2E 所示，用户（自然人）关联子账户（身份 A），
该身份 A 可用于注册应用或网站，根据不同场景可灵活设置不同的身份识别信息，本实
施例称为身份识别信息子集。例如，一些影音类的服务，可以使用安全级别较低的身份
识别信息子集，如图 2D 和图 2E 中，场景 1 对应有身份识别信息子集（图中以识别组 1
10 为例，包括的身份识别信息为 af_g_1）；一些支付类的服务，可以使用安全级别较高的
身份识别信息子集，如图 2D 和图 2E 中，场景 2 对应有身份识别信息子集（图中以识
别组 2 为例，包括的身份识别信息为 af_g_1 和 af_b_6）；身份识别信息子集由身份识
别信息集中的一个或多个身份识别信息构成。其中，哪一些服务装置具体采用哪一些身
份识别信息子集，可以由服务装置对应的服务方确定，也可以是用户指定，也可以是由
15 身份管理系统方指定，实际应用中可以灵活配置，本实施例对此不作限定。

[100] 以图 2B 所示实施例为例，该服务装置涉及网络购物，在该场景下，服务装置所
要求的安全级别较高，该服务装置的对接模块可以要求用户输入的身份识别信息包括：
密码和指纹等。

[101] 基于此，对接模块可以获取到用户输入的目标主账户的校验信息，并发送给身
20 份管理装置进行身份校验。身份管理装置接收所述服务装置的对接模块发送的目标主账
户的校验信息，利用所述身份识别信息集对所述目标主账户进行身份校验。若校验通过，
身份管理装置可以到获取所述目标主账户预先为所述服务装置关联的至少一个子账户
的登录信息，并发送给所述对接模块。可选的，该用户针对该服务装置关联有两个子账
户，服务装置可以展示给用户选择其所期望登录的子账户。

25 [102] 其中，若校验失败，身份管理装置也可以发送校验结果给对接模块，使对接模
块禁止登录操作；可选的，若在一定时间窗口内相同场景发生多次连续校验失败，可采
取安全措施如：一定时间内本场景禁止该用户再次校验，或需要自然人登录身份识别系
统通过其他校验手段解除锁定等等。当身份管理系统还可以配置其他的风险控制策略，
如果判定用户的校验环境异常，例如用户处于非常驻地、使用非常用设备时，还可通知

对接模块获取用户更多的身份识别信息等。

[103] 本说明书实施例中，身份管理装置管理有用户的身份信息，可选的，服务方侧可以获取到所登录用户的年龄或性别等身份信息，作为例子，所述对接模块，还用于接收所述目标子账户对应的主账户的内容等级；所述内容等级参数可以包括主账户的年龄或性别等个人信息，也可以是身份管理方与服务方约定好的参数；因此，所述服务装置还包括展示模块，用于：根据所述内容等级确定所展示的服务内容并展示。服务装置可以根据用户的内容等级过滤不符合其内容等级的内容，内容包括但不限于（视频、音频、文章或图片等）。如图 2F 所示，用户（自然人）的内容等级为 lv0，在该用户采用身份 A 登录应用后，内容等级小于等于 lv0 的服务内容可进行展示，内容等级大于 lv0 的服务内容则不可展示，处于不可见状态。可选的，服务方还可结合用户的兴趣爱好推荐其可能感兴趣的内容等等。

[104] 基于本说明书实施例的身份管理装置，可以提高互联网服务的安全性；例如，如图 2G 所示，由于用于登录服务装置的子账户都与主账户关联，因此可以根据身份追溯到身份管理装置侧的主账户（自然人），通过主账户与身份的映射关系亦可方便管理用户在多个互联网服务侧的恶意行为。因此，本实施例的身份管理装置还可包括：安全控制模块，用于：获取所述服务装置发送的用户行为数据，基于所述用户行为数据进行风险控制。身份管理装置可结合各个互联网服务的反馈分析用户行为，为打击违反网络安全事件提供依据。

[105] 以网络黄牛为例，如图 2H 所示，网络黄牛团伙可收集大量自然人的有效身份证件注册自然人账户，在互联网各种优惠、返利等场景通过刷单行为获取利益等。在本说明书实施例方案中，服务方可在优惠、返利等场景中使用生物识别信息校验主账户的身份。可选的，本实施例的身份管理装置还可包括：安全控制模块，用于：在主账户注册阶段，基于提交的身份识别信息是否与其他已注册主账户的身份识别信息相同进行风险控制。例如，在注册阶段，若黄牛团伙只收集有效身份证件，未收集生物特征信息，则在注册阶段，身份管理装置基于已注册账户的身份识别信息，若黄牛团伙采用大量相同的生物识别信息作为身份识别信息进行注册，身份管理装置可以接收到大量与已注册账户相同的身份识别信息，因此可以进行风险控制，例如可以判定出现非法注册、出现黄牛团伙，而在校验身份的过程中，采用生物识别信息等也可极大程度增加黄牛团伙成本。

[106] 由上述实施例可见，本说明书实施例提供的身份管理装置作为身份集中管理中心，能够统一管理用户身份，主账户是基于用户的个人身份而建立（即每个用户唯一对

应一个主账户)，因此不会存在遗失或弃用等情况，因此主账户关联的子账户也不会发生无法继续使用的情况。手机号码或邮箱地址等仅作为用户的主账户的身份识别信息之一，登录服务方的服务装置不直接与手机号关联，用户可随意更换手机号码或邮箱地址等身份识别信息。

- 5 [107] 用户基于主账户，可在相同服务方侧关联多个子账户，一个用户可采用不同身份的子账户登陆服务方的服务器，可以满足用户个性化需求，用户可以通过身份管理装置统一管理所有服务装置的所有子账户。另外，本说明书也能够支持在不同服务场景下灵活设置不同安全级别的身份识别信息子集以校验用户身份。在登录服务装置的过程中，用户的身份识别信息与服务方侧解耦，由身份管理装置校验用户身份。

- 10 [108] 如图 3 所示，是本说明书根据一示例性实施例示出的一种身份校验方法的流程图，所述方法可应用于身份管理装置，包括：

[109] 在步骤 302 中，接收服务装置的对接模块发送的目标主账户的校验信息。

[110] 在步骤 304 中，利用已注册主账户对应的身份识别信息集对所述目标主账户进行身份校验。其中，所述已注册主账户为至少一个服务装置预先关联有至少一个子账户；

- 15 所述子账户用于所述服务装置登录服务端；

[111] 在步骤 306 中，在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息，并发送给所述对接模块。

[112] 如图 4 所示，是本说明书根据一示例性实施例示出的一种登录方法的流程图，所述方法可应用于服务装置，包括：

- 20 [113] 在步骤 402 中，在登录流程被触发后，获取目标主账户的校验信息并发送给所述身份管理装置；

[114] 在步骤 404 中，接收所述身份管理装置发送的至少一个子账户的登录信息；

[115] 在步骤 406 中，从所述至少一个子账户中确定目标子账户并登录服务端。

- [116] 相应地，本说明书实施例还提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如下方法：
- 25

[117] 接收服务装置的对接模块发送的目标主账户的校验信息；

[118] 利用已注册主账户对应的身份识别信息集对所述目标主账户进行身份校验；其

中，所述已注册主账户为至少一个服务装置预先关联有至少一个子账户；所述子账户用于所述服务装置登录服务端；

[119] 在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息，并发送给所述对接模块。

- 5 [120] 相应地，本说明书实施例还提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如下方法：

[121] 在登录流程被触发后，获取目标主账户的校验信息并发送给所述身份管理装置；

[122] 接收所述身份管理装置发送的至少一个子账户的登录信息；

- 10 [123] 从所述至少一个子账户中确定目标子账户并登录服务端。

[124] 本说明书服务装置/身份管理装置的实施例可以应用在计算机设备上，例如服务器或终端设备。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在文件处理的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，
15 如图 5 所示，为本说明书实施例服务装置/身份管理装置所在计算机设备的一种硬件结构图，除了图 5 所示的处理器 510、内存 530、网络接口 520、以及非易失性存储器 540 之外，实施例中装置 531 所在的服务器或电子设备，通常根据该计算机设备的实际功能，还可以包括其他硬件，对此不再赘述。

- [125] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法
20 实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

- 25 [126] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[127] 本领域技术人员在考虑说明书及实践这里申请的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未申请的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的
5 真正范围和精神由下面的权利要求指出。

[128] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。

[129] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保
10 护的范围之内。

权利要求书

1、一种登录方法，包括：

在服务装置的登录流程被触发后，所述服务装置中的对接模块获取目标主账户的校验信息并发送给身份管理装置；

5 所述身份管理装置接收到所述校验信息后，利用已注册主账户的身份识别信息集对所述目标主账户进行身份校验，在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息，并发送给所述对接模块；

在所述对接模块接收到所述登录信息后，所述服务装置确定目标子账户并登录服务端。

10 2、根据权利要求 1 的方法，所述校验信息包括：所述目标主账户的标识以及至少一种身份识别信息。

3、根据权利要求 2 的方法，所述目标主账户的标识与对应用户的身份证件号码相关联。

15 4、根据权利要求 2 的方法，所述校验信息包括的至少一种身份识别信息，基于所述服务装置的安全级别而确定。

5、根据权利要求 2 的方法，所述服务装置确定目标子账户，包括：

若接收到多个子账户的登录信息，展示所述多个子账户后，获取被用户选择的子账户作为所述目标子账户。

20 6、根据权利要求 1 的方法，所述主账户的身份识别信息集包括如下一类或多类身份识别信息：网络身份识别信息、个人身份识别信息或生物识别信息。

7、一种身份管理装置，包括：

身份信息管理模块，用于：管理已注册主账户、以及所述已注册主账户为至少一个服务装置关联的至少一个子账户；所述已注册主账户对应有身份识别信息集，所述子账户用于所述服务装置登录服务端；

25 身份校验模块，用于：接收所述服务装置的对接模块发送的目标主账户的校验信息，利用所述身份识别信息集对所述目标主账户进行身份校验，在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息，并发送给所述对接模块。

30 8、根据权利要求 7 所述的装置，所述已注册主账户与对应用户的身份证件信息绑定。

9、根据权利要求 7 所述的装置，所述子账户对应有用于身份校验的身份识别信息

子集，所述身份识别信息子集基于所述服务装置的安全级别而确定。

10、根据权利要求 7 所述的装置，所述身份识别信息集包括如下一类或多类身份识别信息：网络身份识别信息、个人身份识别信息或生物识别信息。

11、根据权利要求 7 所述的装置，所述身份信息模块，还用于：至少基于所述
5 已注册主账户的年龄确定所述已注册主账户的内容等级参数，并发送给所述对接模块。

12、根据权利要求 7 所述的装置，所述装置还包括：安全控制模块，用于：

获取所述服务装置发送的用户行为数据，基于所述用户行为数据进行风险控制。

13、根据权利要求 7 所述的装置，所述装置还包括：安全控制模块，用于：

在主账户注册阶段，基于提交的身份识别信息是否与其他已注册主账户的身份识别
10 信息匹配进行风险控制。

14、一种服务装置，所述服务装置包括：

对接模块，用于：在所述服务装置的登录流程被触发后，获取目标主账户的校验信息并发送给所述身份管理装置；以及，接收所述身份管理装置发送的至少一个子账户的
登录信息；

15 登录模块，用于：在所述对接模块接收到所述登录信息后，确定目标子账户并登录服务端。

15、根据权利要求 14 的装置，所述目标主账户的标识与对应用户的身份证件号码相关联。

16、根据权利要求 15 的装置，所述校验信息所包括的至少一种身份识别信息，基
20 于所述服务装置的安全级别而确定。

17、根据权利要求 14 的装置，所述对接模块，还用于接收所述目标子账户对应的主账户的内容等级参数；

所述服务装置还包括展示模块，用于：根据所述内容等级参数确定所展示的服务内容并展示。

25 18、一种身份校验方法，所述方法包括：

接收服务装置的对接模块发送的目标主账户的校验信息；

利用已注册主账户对应的身份识别信息集对所述目标主账户进行身份校验；其中，
所述已注册主账户为至少一个服务装置预先关联有至少一个子账户；所述子账户用于所
述服务装置登录服务端；

30 在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息，并发送给所述对接模块。

19、一种登录方法，所述方法包括：

在登录流程被触发后，获取目标主账户的校验信息并发送给所述身份管理装置；

接收所述身份管理装置发送的至少一个子账户的登录信息；

从所述至少一个子账户中确定目标子账户并登录服务端。

5 20、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如下方法：

接收服务装置的对接模块发送的目标主账户的校验信息；

利用已注册主账户对应的身份识别信息集对所述目标主账户进行身份校验；其中，所述已注册主账户为至少一个服务装置预先关联有至少一个子账户；所述子账户用于所

10 述服务装置登录服务端；

在通过身份校验后获取所述目标主账户预先为所述服务装置关联的至少一个子账户的登录信息，并发送给所述对接模块。

21、一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时实现如下方法：

15 在登录流程被触发后，获取目标主账户的校验信息并发送给所述身份管理装置；

接收所述身份管理装置发送的至少一个子账户的登录信息；

从所述至少一个子账户中确定目标子账户并登录服务端。