(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 5 月 24 日 (24.05.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/090183 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2016/105886

(22) 国际申请日: 2016 年 11 月 15 日 (15.11.2016)

(25) 申请语言: 中文

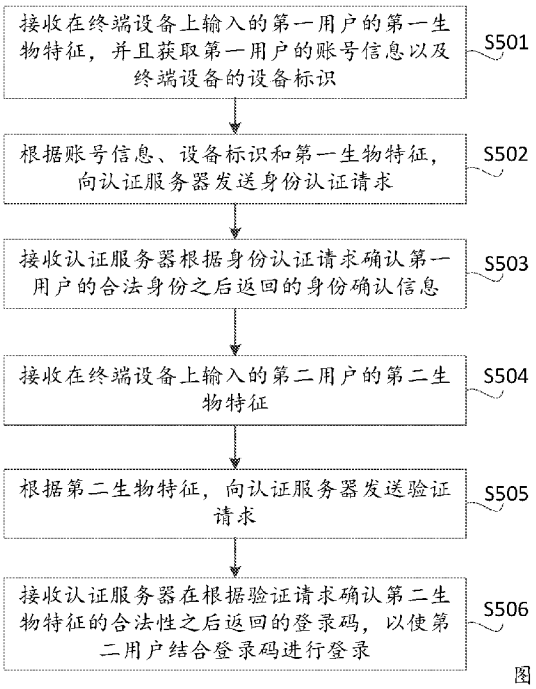
(26) 公布语言: 中文

(71) 申请人: 深圳达闼科技控股有限公司 (CLOUDMINDS (SHENZHEN) HOLDINGS CO., LTD.) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。

(72) 发明人: 张站朝 (ZHANG, Zhanchao); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。 王振凯 (WANG, Zhenkai); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。 鄂鹏 (E, Peng); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。 陈超 (CHEN, Chao); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。 李静 (LI, Jing); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。 李坤 (LI, Kun); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室（入驻深圳市前海商务秘书有限公司）, Guangdong 518000 (CN)。

(54) **Title:** IDENTITY AUTHENTICATION METHOD, TERMINAL DEVICE, AUTHENTICATION SERVER AND ELECTRONIC DEVICE

(54) **发明名称**: 一种身份认证的方法、终端设备、认证服务器及电子设备



S501 RECEIVING A FIRST BIOLOGICAL FEATURE, INPUT ON A TERMINAL DEVICE, OF A FIRST USER, AND ACQUIRING ACCOUNT INFORMATION ABOUT THE FIRST USER AND A DEVICE IDENTIFIER OF THE TERMINAL DEVICE

S502 ACCORDING TO THE ACCOUNT INFORMATION, THE DEVICE IDENTIFIER AND THE FIRST BIOLOGICAL FEATURE, SENDING AN IDENTITY AUTHENTICATION REQUEST TO AN AUTHENTICATION SERVER

S503 RECEIVING IDENTITY CONFIRMATION INFORMATION RETURNED AFTER THE AUTHENTICATION SERVER CONFIRMS A VALID IDENTITY OF THE FIRST USER ACCORDING TO THE IDENTITY AUTHENTICATION REQUEST

S504 RECEIVING A SECOND BIOLOGICAL FEATURE, INPUT ON THE TERMINAL DEVICE, OF A SECOND USER

S505 ACCORDING TO THE SECOND BIOLOGICAL FEATURE, SENDING A VERIFICATION REQUEST TO THE AUTHENTICATION SERVER

S506 RECEIVING A LOGIN CODE RETURNED AFTER THE AUTHENTICATION SERVER CONFIRMS THE VALIDITY OF THE SECOND BIOLOGICAL FEATURE ACCORDING TO THE VERIFICATION REQUEST, SO THAT THE SECOND USER PERFORMS LOGIN BY USING THE LOGIN CODE

图 5

(57) **Abstract:** An identity authentication method, a terminal device, an authentication server and an electronic device. The method comprises: receiving an input biological feature of a first user, and acquiring account information about the first user and a device identifier of a terminal device; sending an identity authentication request to an authentication server; receiving identity confirmation information returned by the authentication server; receiving an input biological feature of a second user; sending a verification request to the authentication server; and receiving a login code returned by the authentication server, so that the second user performs login by

WO 2018/090183 A1

[见续页]

(74) 代理人：深圳市爱迪森知识产权代理事务所（普通合伙）(SHENZHEN AIDISEN INTELLECTUAL PROPERTY OFFICE)；中国广东省深圳市南山区南海大道4050号上海汽车大厦703室, Guangdong 518057 (CN)。

(81) 指定国（除另有指明，要求每一种可提供的国家保护）：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：
— 包括国际检索报告（条约第21条(3)）。

using the login code. By means of the method, on a terminal device where a first user is successfully authenticated, the terminal device can be taken as a device for authentication and login of a second user, and identities of the first user and the second user are sequentially authenticated on the same device, so that the second user can successfully perform login only on the premise that the first user provides a guarantee, ensuring that the second user uses a security device for login and thereby ensuring the security and reliability.

(57) 摘要：一种身份认证的方法、终端设备、认证服务器及电子设备，该方法包括：接收输入的第一用户的生物特征，并且获取第一用户的账号信息以及终端设备的设备标识；向认证服务器发送身份认证请求；接收认证服务器返回的身份确认信息；接收输入的第二用户的生物特征；向认证服务器发送验证请求；接收认证服务器返回的登录码，第二用户结合该登录码进行登录。该方法能够在第一用户认证成功的终端设备上，将该终端设备作为第二用户进行认证登录的设备，通过在同一设备上先后认证第一用户和第二用户身份，实现在第一用户提供担保的前提下，第二用户才能够顺利登录，保证第二用户使用安全设备进行登录，从而保证安全性和可靠性。

一种身份认证的方法、终端设备、认证服务器及电子设备

技术领域

本发明涉及计算机技术领域，特别是涉及一种身份认证的方法、终端设备、认证服务器及电子设备。

背景技术

移动办公是指利用终端设备无线接入移动通信网络进行办公的办公模式。由于移动办公摆脱时间和场所局限，办公人员可随时进行随身化的公司管理和沟通，大大提高办公人员的效率，因此，移动办公深受欢迎。

对于安全要求比较高的领域，例如：金融领域，若办公人员随意地使用终端设备进行办公，会加大金融涉密的风险。为了提高金融领域中移动办公的安全性，通常为有需要移动办公的办公人员配置终端设备，并且将终端设备、办公人员的指纹和办公人员的账号进行认证绑定，只允该办公人员使用绑定的终端设备和账号进行办公。但是，在金融领域中，通常会涉及主管对下属进行认证授权处理的情况，若主管和下属外出，并且主管没有携带自身配置的终端设备，则无法实现对下属进行授权处理的，即使是下属自身配置的终端设备是可靠的设备，但是主管仍然无法使用下属自身配置的终端设备，主管只能回到办公室或者取回自身配置的终端设备才能进行认证授权处理，大大影响办公效率。

发明内容

本发明主要解决的技术问题是提供一种身份认证的方法、终端设备、认证服务器及电子设备，其目的旨在解决现有身份认证的方法只针对独立的个人认证，当需要认证人进行身份认证，而认证人的终端设备不在身边时，认证人无法通过其他终端设备进行身份认证或授权的技术

问题。

为解决上述技术问题，本发明采用的一个技术方案是：提供一种授身份认证的方法，包括：接收在终端设备上输入的第一用户的第一生物特征，并且获取所述第一用户的账号信息以及所述终端设备的设备标识；根据所述账号信息、设备标识和第一生物特征，向认证服务器发送身份认证请求；接收所述认证服务器根据所述身份认证请求确认所述第一用户的合法身份之后返回的身份确认信息；接收在所述终端设备上输入的第二用户的第二生物特征；根据所述第二生物特征，向所述认证服务器发送验证请求；接收所述认证服务器在根据所述验证请求确认所述第二生物特征的合法性之后返回的登录码，以使所述第二用户结合所述登录码进行登录。

可选地，所述身份认证请求是依据第一生物特征所绑定的私钥对账号信息、第一生物特征和设备标识进行加密生成的。

可选地，所述私钥是在所述第一生物特征被检验通过之后获取得到的。

可选地，所述验证请求是依据第一生物特征所绑定的私钥对所述第二生物特征进行加密生成的。

为解决上述技术问题，本发明采用的另一个技术方案是：提供一种身份认证的方法，包括：接收终端设备发送的身份认证信息，所述身份认证信息携带所述第一用户的账号信息、第一用户的第一生物特征和所述终端设备的设备标识；在根据所述身份认证信息确认所述第一用户的合法身份之后，向所述终端设备返回身份确认信息；接收所述终端设备发送的验证请求，所述验证请求携带第二用户的第二生物特征；在根据所述验证请求确认所述第二生物特征的合法性之后，生成与所述第二用户对应的登录码；向所述终端设备发送所述登录码，以使所述第二用户结合所述登录码进行登录。

可选地，所述身份确认信息是确定所述账号信息、第一用户的第一生物特征和所述设备标识存在对应关系时生成的。

为解决上述技术问题，本发明采用的另一个技术方案是：提供一种

终端设备，包括：生物特征识别模块，用于进行生物特征识别；第一接收模块，用于接收在终端设备上输入的第一用户的第一生物特征；第一获取模块，用于获取所述第一用户的账号信息以及所述终端设备的设备标识；第一发送模块，用于根据所述账号信息、设备标识和第一生物特征，向认证服务器发送身份认证请求；第二接收模块，用于接收所述认证服务器根据所述身份认证请求确认所述第一用户的合法身份之后返回的身份确认信息；第三接收模块，用于接收在所述终端设备上输入的第二用户的第二生物特征；第二发送模块，用于根据所述第二生物特征，向所述认证服务器发送验证请求；第四接收模块，用于接收所述认证服务器在根据所述验证请求确认所述第二生物特征的合法性之后返回的登录码，以使所述第二用户结合所述登录码进行登录。

可选地，所述终端设备还包括：第一加密模块，用于依据第一生物特征所绑定的私钥对账号信息、第一生物特征和设备标识进行加密。

可选地，所述终端设备还包括：第二获取模块，用于在所述第一生物特征被检验通过之后，获取所述私钥。

可选地，所述终端设备还包括：第二加密模块，用于依据第一生物特征所绑定的私钥对所述第二生物特征进行加密。

为解决上述技术问题，本发明采用的另一个技术方案是：提供一种认证服务器，包括：第一接收模块，用于接收终端设备发送的身份认证信息，所述身份认证信息携带所述第一用户的账号信息、第一用户的第一生物特征和所述终端设备的设备标识；第一返回模块，用于在根据所述身份认证信息确认所述第一用户的合法身份之后，向所述终端设备返回身份确认信息；第二接收模块，用于接收所述终端设备发送的验证请求，所述验证请求携带第二用户的第二生物特征；生成模块，用于在根据所述验证请求确认所述第二生物特征的合法性之后，生成与所述第二用户对应的登录码；第二返回模块，用于向所述终端设备发送所述登录码，以使所述第二用户结合所述登录码进行登录。

为解决上述技术问题，本发明采用的另一个技术方案是：提供一种电子设备，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上述方法。

为解决上述技术问题，本发明采用的另一个技术方案是：提供一种非易失性计算机可读存储介质，所述计算机可读存储介质存储有计算机可执行指令，该计算机可执行指令被一个或多个处理器执行，以使所述至少一个处理器能够执行上述方法。

为解决上述技术问题，本发明采用的另一个技术方案是：提供一种计算机程序产品，所述计算机程序产品包括存储在非易失性计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，该程序指令被一个或多个处理器执行，以使所述至少一个处理器执行上述方法。

本发明的有益效果是：区别于现有技术的情况，本发明能够在先由终端设备采集第一用户的第一生物特征，获取第一用户的账号信息以及所述终端设备的设备标识，然后根据第一生物特征、账号信息和设备标识，验证到第一用户的合法身份，以及确定终端设备归属所述第一用户所有，从而确定了该终端设备的可靠性，并且第一用户起到对后续验证第二用户的身份时起到担保的作用，第二用户使可靠的移动终端采集第二用户的第二生物特征，并进行认证，有利于保证第二用户的数据的安全性，有效地降低第二用户的数据被盗窃的风险，另外，第二用户通过使用可靠的第二方终端设备进行生物认证，可以使得第二用户可以脱离强制配置的终端设备进行生物认证，方便第二用户的操作。

附图说明

图1是本发明实施例一提供的一种身份认证的应用场景图；

图2是本发明实施例一提供的第一用户通过终端设备向认证服务器注册的流程图；

图3是本发明实施例二提供的一种终端设备实施方式的结构示意图；

图4是本发明实施例三提供的一种认证服务器实施方式的结构示意图；

图5是本发明实施例四提供的一种身份认证方法的流程示意图；

图6是本发明实施例五提供的一种身份认证方法的流程示意图；

图7是本发明实施例六提供的一种身份认证方法的流程示意图；

图8是本发明实施例七提供的一种执行身份认证方法的电子设备的结构示意图。

具体实施方式

下面结合附图和实施方式对本发明进行详细说明。

实施例一

请参阅图 1，图 1 是本发明实施例提供的一种身份认证的应用场景图。该身份认证系统 20 包括终端设备 21 和认证服务器 22，其中，终端设备 21 配置有生物特征识别模块，该生物特征识别模块用于识别生物特征，其中，生物特征是指对用户进行唯一性标识的特征，在本实施例中，生物特征可以包括指纹、面像、虹膜或者掌纹等特征。终端设备 21 可以为智能手机、平板电脑、PDA（Personal Digital Assistant，掌上电脑）等等。

终端设备 21 接受输入的第一用户的第一生物特征，并且获取该第一用户的账号信息以及该终端设备 21 的设备标识。例如，本实施例中该终端设备 21 配置有指纹识别模块，该指纹识别模块能够识别指纹。第一用户首先在终端设备 21 上进入指纹识别界面，生物特征识别模块通过扫描该界面手指获取指纹信息，并验证该指纹信息。第一用户的第一生物特征即指纹信息验证成功后，终端设备 21 通过该指纹信息获取与该指纹信息对应的账号信息，具体的账号信息可以为，该第一用户的姓名，性别，年龄，工作职位等信息。终端设备 21 进一步获取该设备的设备标识，例如该终端设备 21 为智能手机，则获取该智能手机的手机型号、手机名称、出厂序列号、生产日期等证明该智能手机的设备标识。在本实施例中，第一用户的账号信息也可以通过直接输入获取得到。

在获取到第一用户的账号信息、生物特征和该设备的设备标识后，终端设备 21 进一步的向认证服务器 22 发送身份认证请求，其中，该身

份认证请求携带第一用户的账号信息、生物特征和该终端设备的设备标识。

认证服务器 22 根据获取到的账号信息、生物特征和终端设备 21 的设备标识以验证第一用户的身份是否属实及判断该第一用户是否为该终端设备 21 的所有人，当第一用户的身份属实且为该终端设备 21 的所有人，则向终端设备 21 返回身份认证通过消息。

终端设备 21 接收认证服务器 22 返回的身份认证通过消息。通过对第一用户进行身份认证，证实第一用户身份属实，且第一用户为该终端设备 21 的所有人，从而保证了终端设备 21 的可靠性。

终端设备 21 进一步通过生物特征识别模块接收输入的第二用户的生物特征，以获取第二用户的生物特征，具体的获取方法同第一用户的获取方法。在第二用户的第二生物特征获取成功后，向认证服务器 22 发送验证请求，其中，该验证请求携带第二用户的生物特征，通过该验证请求，认证服务器 22 能够验证第二生物特征的合法性，以确定第二用户的身份是否属实。

进一步的，在确认第二生物特征的合法性之后，认证服务器 22 生成与第二用户对应的登录码，并向终端设备 21 返回该登录码。终端设备 21 接收认证服务器 22 返回的登录码，第二用户则可以凭借该登录码在终端设备 21 上进行登录，具体的，该登录码可以为二维码，也可以为短信验证码等。

本发明实施例对终端设备 21 的所有者，即为第一用户，进行身份认证，在证实该第一用户的身份属实且为该终端设备 21 的所有人之后，再接收第二用户的生物特征，根据第二用户的生物特征对第二用户进行身份验证。在第二用户的身份验证通过之后，第二用户能够进一步将该终端设备作为登录的设备进行登录，以解决自己的终端设备不在身边，无法登录的问题。通过在同一设备上先后认证第一用户和第二用户身份，在第一用户提供担保的前提下，使得第二用户才能够顺利登录，保证第二用户使用安全设备进行登录，从而保证安全性和可靠性。

为了提高终端设备 21 和认证服务器 22 之间传输的数据的安全性，

可以对终端设备 21 和认证服务器 22 之间传输的数据进行加密处理。具体的，终端设备 21 先验证第一用户的第一生物特征，验证通过后，依据第一生物特征所绑定的私钥对第一用户的账号信息、第一生物特征和终端设备 21 的设备标识进行加密，生成第一加密数据，并且根据第一加密数据生成身份认证请求。

进一步的，终端设备 21 在向认证服务器 22 发送该身份认证请求。具体的，终端设备 21 向认证服务器 22 发送身份认证请求的步骤包括：终端设备 21 向认证服务器 22 发送携带第一加密数据的身份认证请求；认证服务器 22 在接收到身份认证请求之后，对身份认证请求进行解释，获取第一加密数据，再通过预设公钥对第一加密数据进行解密处理获取第一用户的账号信息、第一生物特征以及终端设备 21 的设备标识，然后根据第一用户的账号信息、第一生物特征以及终端设备 21 的设备标识对第一用户的身份进行身份认证。

当然，第二用户的生物特征也可以通过预设秘钥加密后发送至认证服务器进行验证。具体的，终端设备 21 首先通过预设私钥对第二用户的生物特征进行加密，生成第二加密数据，并且根据第二加密数据生成验证请求，并向认证服务器 22 发送该验证请求，其中，该验证请求携带第二加密数据。认证服务器 22 根据预设公钥对第二加密数据进行解密获取第二用户的生物特征。

需要说明的是：公钥和私钥是在用户在认证服务上注册时就得到的。本实施例所指的公钥和私钥都是预设的，其中，预设公钥和预设私钥为配对秘钥，并且预设的私钥与认证服务器 22 进行配对，预设公钥与终端设备 21 进行配对。认证服务器 22 在接收到身份认证请求时，根据身份认证请求的源地址选择配对的预设公钥。第一用户和第二用户均有与其绑定的终端设备 21，认证服务器 22 记录有该绑定关系，认证服务器 22 所记录的该绑定关系和配对的预设公钥可以由管理者直接输入至认证服务器 22，也可以第一用户和第二用户自行到认证服务器 22 进行注册形成的，以下对第一用户自行到认证服务器 22 进行注册的过程进行具体说明，请参阅图 2，包括：

步骤 S101：接收第一用户在终端设备 21 上输入注册的设备标识、账号信息和密码；

步骤 S102：向认证服务器 22 发送该设备标识、账号信息和密码；

步骤 S103：认证服务器 22 对该设备标识、账号信息和密码进行验证；

步骤 S104：在验证通过之后，返回给终端设备 21 的账号验证通过消息以及发送一个随机码 ；

步骤 S105：接收第一用户在终端设备 21 中录入的生物特征；

步骤 S106：终端设备 21 根据第一用户的生物特征生成对应的公钥和私钥；

步骤 S107：将第一用户生成的公钥和生物特征值发送给认证服务器 22。

步骤 S108：认证服务器 22 根据第一用户的设备标识和账号信息建立第一用户与终端设备 21 的绑定关系；认证服务器 22 根据第一用户的生物特征值建立与第一用户的对应关系。

即为：移动设备终端设备 21 的设备标识、用户的用户标识和用户的生物特征建立绑定关系，移动设备终端设备 21 的设备标识与接收到的公钥建立对应关系。

可选地，在第一用户向认证服务器 22 进行成功注册之后，终端设备 21 本地也可以保留第一用户的生物特征，在接收到输入的第一用户的生物特征时，先判断接收到的生物特征与终端设备 21 本地存储的生物特征是否匹配，若匹配，则本地认证通过，若不匹配，则提示当前用户不是终端设备 21 的所有者的提示信息。

可选地，在认证服务器 22 根据验证请求确认第二生物特征的合法性之后，生成与第二用户对应的登录码，并向终端设备 21 返回该登录码，该登录码还可以携带第二用户的账号信息。终端设备 21 在接收到登录码之后，还可以显示第二用户的账号信息，以使第一用户获知当前第二用户是谁，并且第二用户是否可靠。

可选地，在认证服务器 22 根据验证请求确认第二生物特征的合法

性之后，生成与第二用户对应的登录码，并向终端设备 21 返回该登录码，认证服务器 22 还可以向终端设备 21 返回将终端设备 21 认证为第二用户进行登录的信息。

可选地，终端设备 21 可以向认证服务器 22 发送第二用户的登录信息，认证服务器 22 根据该登录信息判断到第二用户不是通过自己绑定的设备登录，而是通过认证过的其它可靠的终端设备 21 登录。

值得说明的是：终端设备 21 上所执行的各个操作和认证服务器 22 上所执行的各个操作都通过日志记录，以方便在以后审计追溯时，可以查看到什么时间，谁认证谁，用哪个设备进行的整个身份认证的过程等操作。

本发明实施例对终端设备 21 的所有者，即为第一用户，进行身份认证，在证实该第一用户的身份属实且为该终端设备 21 的所有人之后，再接收第二用户的生物特征，根据第二用户的生物特征对第二用户进行身份验证。在第二用户的身份验证通过之后，第二用户能够进一步将该终端设备作为登录的设备进行登录，以解决自己的终端设备不在身边，无法登录的问题。通过在同一设备上先后认证第一用户和第二用户身份，在第一用户提供担保的前提下，使得第二用户能够顺利登录，保证了整个认证过程的安全性和可靠性。

在整个对第一用户的身份认证请求和第二用户的验证请求过程中，认证服务器利用终端设备先前发送过来的公钥对登录码进行加密，发送给终端设备，由于终端设备的私钥只存在于终端设备中，即使这段通过公钥加密过的登录码明文，被恶意截取，截取方也无法通过像解析对称密码的方式来解析这段密文，保证了该登录码密文能够安全的，只被拥有私钥的终端设备来解析出正确的登录码。同时，对于公钥，无论是认证服务器还是终端设备而言，都是公开的，故无需考虑采用可靠的信道进行密码分发，大大降低了开发难度。

实施例二

请参阅图 3，图 3 是本发明实施例二提供的一种终端设备的结构示意图。终端设备 30 包括生物特征识别模块 301、第一接收模块 302、第

一获取模块 303、第一发送模块 304、第二接收模块 305、第三接收模块 306、第二发送模块 307 和第四接收模块 308。

生物特征识别模块 301，用于进行生物特征识别。其中，生物特征是指对用户进行唯一性标识的特征，在本实施例中，生物特征可以包括指纹、面像、虹膜或者掌纹等特征。终端设备 21 可以为智能手机、平板电脑、PDA（Personal Digital Assistant，掌上电脑）等等。

第一接收模块 302，用于通过生物特征识别模块 301 接收输入的第一用户的生物特征。

第一获取模块 303，用于获取第一用户的账号信息以及终端设备的设备标识。具体的账号信息可以为，该第一用户的姓名，性别，年龄，工作职位等信息。终端设备，例如为智能手机，则获取该智能手机的手机型号、手机名称、出厂序列号、生产日期等证明该智能手机的设备标识。

第一发送模块 304，用于向认证服务器发送身份认证请求，其中，身份认证请求携带第一用户的生物特征、账号信息以及终端设备的设备标识。

第二接收模块 305，用于接收认证服务器在根据第一用户的生物特征、账号信息以及终端设备的设备标识对第一用户的身份成功认证后返回的身份认证通过消息。

第三接收模块 306，用于通过生物特征识别模块 301 接收输入的第二用户的生物特征。

第二发送模块 307，用于向认证服务器发送验证请求，其中，该验证请求携带第二用户的生物特征。

第四接收模块 308，用于接收认证服务器在根据验证请求确认第二生物特征的合法性之后返回的登录码，第二用户可结合该登录码进行登录。

为了提高终端设备和认证服务器之间传输的数据的安全性，终端设备和认证服务器之间传输的数据可以进行加密处理，终端设备 30 还可以包括第一加密模块 309 ，第二获取模块 310 和第二加密模块 311。

第一加密模块 309，用于依据第一生物特征所绑定的私钥对账号信息、第一生物特征和设备标识进行加密。

第二获取模块 310，用于在第一生物特征被检验通过之后，获取私钥。

第二加密模块 311，用于依据第一生物特征所绑定的私钥对第二生物特征进行加密。

本实施例提供的终端设备，在证实该第一用户的身份属实且为该终端设备 21 的所有人之后，再接收第二用户的生物特征，根据第二用户的生物特征对第二用户进行身份验证。在第二用户的身份验证通过之后，第二用户能够进一步将该终端设备作为登录的设备进行登录，以解决自己的终端设备不在身边，无法登录的问题。同时，利用私钥对第一用户的账号信息、第一生物特征和设备标识以及第二用户的第二生物特征进行加密，保证传输的安全性，在发送给接收端时，文件被恶意截取，也能保证安全性。

实施例三

请参阅图 4，图 4 是本发明实施例三提供的一种认证服务器的示意图。认证服务器 40 包括第一接收模块 401、第一返回模块 402、第二接收模块 403、生成模块 404、第二返回模块 405。

第一接收模块 401，用于接收终端设备发送的身份认证信息，该身份认证信息携带第一用户的账号信息、第一用户的第一生物特征和终端设备的设备标识。

第一返回模块 402，用于在根据身份认证信息确认第一用户的合法身份之后，向终端设备返回身份确认信息。

第二接收模块 403，用于接收终端设备发送的验证请求，该验证请求携带第二用户的第二生物特征。

生成模块 404，用于在根据验证请求确认所述第二生物特征的合法性之后，生成与第二用户对应的登录码。

第二返回模块 405，用于向所述终端设备发送所述登录码，以使所述第二用户结合所述登录码进行登录。

本实施例提供的认证服务器通过对第一用户进行身份认证和对第二用户进行验证，在第二用户的身份验证通过之后，使得在第一用户提供担保的前提下，第二用户能够顺利登录，保证了整个认证过程的安全性和可靠性。

实施例四

请参阅图 5，图 5 是本发明实施例四提供的一种身份认证方法的流程示意图，该方法包括：

步骤 S501：接收在终端设备上输入的第一用户的第一生物特征，并且获取所述第一用户的账号信息以及所述终端设备的设备标识；

终端设备 21 配置有生物特征识别模块，该生物特征识别模块用于识别生物特征，其中，生物特征是指对用户进行唯一性标识的特征，在本实施例中，生物特征可以包括指纹、面像、虹膜或者掌纹等特征。终端设备 21 可以为智能手机、平板电脑、PDA（Personal Digital Assistant，掌上电脑）等等。终端设备 21 接受输入的第一用户的第一生物特征，并且获取该第一用户的账号信息以及该终端设备 21 的设备标识。例如，本实施例中该终端设备 21 配置有指纹识别模块，该指纹识别模块能够识别指纹。第一用户首先在终端设备 21 上进入指纹识别界面，生物特征识别模块通过扫描该界面手指获取指纹信息，并验证该指纹信息。第一用户的第一生物特征即指纹信息验证成功后，终端设备 21 通过该指纹信息获取与该指纹信息对应的账号信息，具体的账号信息可以为，该第一用户的姓名，性别，年龄，工作职位等信息。终端设备 21 进一步获取该设备的设备标识，例如该终端设备 21 为智能手机，则获取该智能手机的手机型号、手机名称、出厂序列号、生产日期等证明该智能手机的设备标识。在本实施例中，第一用户的账号信息也可以通过直接输入获取得到。

步骤 S502：根据所述账号信息、设备标识和第一生物特征，向认证服务器发送身份认证请求；

在获取到第一用户的账号信息、生物特征和该设备的设备标识后，终端设备 21 进一步的向认证服务器 22 发送身份认证请求，该身份认证

请求用户用于向认证服务器请求对第一用户的身份进行认证。其中，该身份认证请求携带第一用户的账号信息、生物特征和该终端设备的设备标识。认证服务器 22 根据获取到的账号信息、生物特征和终端设备 21 的设备标识以验证第一用户的身份是否属实及判断该第一用户是否为该终端设备 21 的所有人。

步骤 S503：接收认证服务器根据身份认证请求确认第一用户的合法身份之后返回的身份确认信息；

步骤 S504：接收在终端设备上输入的第二用户的第二生物特征；

终端设备 21 进一步通过生物特征识别模块接收输入的第二用户的生物特征，以获取第二用户的生物特征，具体的获取方法同第一用户的获取方法。

步骤 S505：根据第二生物特征，向认证服务器发送验证请求；

在第二用户的第二生物特征获取成功后，向认证服务器 22 发送验证请求，其中，该验证请求携带第二用户的生物特征，通过该验证请求，认证服务器 22 能够验证第二生物特征的合法性。

步骤 S506：接收认证服务器在根据验证请求确认第二生物特征的合法性之后返回的登录码，以使第二用户结合所述登录码进行登录。

具体的，该登录码可以为二维码，也可以为短信验证码等。

本实施例提供的终端设备，在证实该第一用户的身份属实且为该终端设备 21 的所有人之后，再接收第二用户的生物特征，根据第二用户的生物特征对第二用户进行身份验证。在第二用户的身份验证通过之后，第二用户能够进一步将该终端设备作为登录的设备进行登录，以解决自己的终端设备不在身边，无法登录的问题。同时，利用私钥对第一用户的账号信息、第一生物特征和设备标识以及第二用户的第二生物特征进行加密，保证传输的安全性，在发送给接收端时，文件被恶意截取，也能保证安全性。

实施例五

请参阅图 6，图 6 是本发明实施例五提供的一种身份认证方法的流程示意图，上述实施例中对各步骤的解释说明在本实施例同样适用，本

实施方式中，对于身份认证的方法与上述实施例中相同的部分不作描述，重点对身份认证的方法不同的部分进行说明，该方法包括：

步骤 S601：接收在移动设备上输入的第一用户的生物特征。

步骤 S602：获取移动设备本地存储的生物特征。

步骤 S603：判断第一用户的生物特征与移动设备本地存储的生物特征是否匹配，若不匹配则执行步骤 S604，若匹配，则执行步骤 S605。

S604：第一用户不具有使用权限信息提示。

在第一用户的生物特征与终端设备本地存储的生物特征相匹配时，证明第一用户为终端设备的所有者，不匹配则不具有使用权限。

S605：获取第一用户的账号信息以及终端设备的设备标识。

S606：通过预设私钥对第一用户的生物特征，账号信息及终端设备的设备标识进行加密生成加密数据，根据加密数据生成身份认证请求。

S607：向认证服务器发送身份认证请求。

向认证服务器发送携带第一加密数据的身份认证请求，以使认证服务器通过预设公钥对第一加密数据进行解密处理获取第一用户的生物特征、账号信息以及终端设备的设备标识，并且根据第一用户的生物特征、账号信息以及终端设备的设备标识对第一用户的身份进行认证处理，其中，预设公钥和预设私钥为配对秘钥，预设私钥预先存储在终端设备，预设公钥预先存储在认证服务器，并且认证服务器存储有预设公钥与终端设备具有对应关系，认证服务器在接收到身份认证请求之后，通过获取身份认证请求的源地址，获取该身份认证请求来源于哪个终端设备，从而获取与该终端设备对应的预设公钥进行解密。

需要说明的是，每一个第一用户和终端设备在使用之前，需要先向认证服务器进行注册，认证服务器只允认证的终端设备和第一用户访问认证服务器，保证终端设备和第一用户的可靠性，从而提高安全性。预设私钥和预设公钥可以在第一用户通过终端设备向认证服务器注册时生成的，并且预设私钥存储在终端设备的本地，预设公钥存储在认证服务器。在第一用户通过终端设备向认证服务器进行注册时，认证服务器将第一用户的生物特征、账号信息和终端设备的设备标识三者之间进

行绑定，后续进行身份认证时，主要通过生物特征、账号信息和设备标识三者之间的绑定关系进行。

S608：接收认证服务器根据身份认证请求确认第一用户的合法身份之后返回的身份确认信息。

S609：接收在终端设备上输入的第二用户的第二生物特征。

S610：根据第二生物特征，向认证服务器发送验证请求。

通过预设私钥对所述第二用户的生物特征进行加密，生成第二加密数据，根据第二加密数据生成验证请求，并且向认证服务器发送烟瘴请求，其中，验证请求携带所述第二加密数据。

S611：接收所述认证服务器在根据验证请求确认第二生物特征的合法性之后返回的登录码，以使第二用户结合该登录码进行登录。

本发明实施例对终端设备的所有者，即为第一用户，进行身份认证，在证实该第一用户的身份属实且为该终端设备的所有人之后，再接收第二用户的生物特征，根据第二用户的生物特征对第二用户进行身份验证。在第二用户的身份验证通过之后，第二用户能够进一步将该终端设备作为登录的设备进行登录，以解决自己的终端设备不在身边，无法登录的问题。通过在同一设备上先后认证第一用户和第二用户身份，在第一用户提供担保的前提下，使得第二用户能够顺利登录，保证了整个认证过程的安全性和可靠性。

在整个对第一用户的身份认证请求和第二用户的验证请求过程中，认证服务器利用终端设备先前发送过来的公钥对登录码进行加密，发送给终端设备，由于终端设备的私钥只存在于终端设备中，即使这段通过公钥加密过的登录码明文，被恶意截取，截取方也无法通过像解析对称密码的方式来解析这段密文，保证了该登录码密文能够安全的，只被拥有私钥的终端设备来解析出正确的登录码。同时，对于公钥，无论是认证服务器还是终端设备而言，都是公开的，故无需考虑采用可靠的信道进行密码分发，大大降低了开发难度。

实施例六

请参阅图 7，图 7 是本发明实施例五提供的一种身份认证方法的流

程示意图，该方法包括：

步骤 S701：接收终端设备发送的身份认证信息，该身份认证信息携带第一用户的账号信息、第一用户的第一生物特征和终端设备的设备标识。

需要说明的是，认证服务器预先存储各个第一用户的生物特征、设备标识以及与终端设备的设备标识三者之间的绑定关系，该绑定关系可以由第一用户通过终端设备向认证服务器注册时生成的，也可以管理人员直接输入的。认证服务器通过判断第一用户的生物特征、设备标识以及终端设备的设备标识是否具有绑定关系实现对第一用户的身份进行认证。

步骤 S702：在根据身份认证信息确认第一用户的合法身份之后，向终端设备返回身份确认信息；

步骤 S703：接收终端设备发送的验证请求，该验证请求携带第二用户的第二生物特征；

步骤 S704：在根据该验证请求确认第二生物特征的合法性之后，生成与该第二用户对应的登录码。

步骤 S705：向终端设备发送登录码，以使第二用户结合该登录码进行登录。

本实施例提供的认证服务器通过对第一用户进行身份认证和对第二用户进行验证，在第二用户的身份验证通过之后，使得在第一用户提供担保的前提下，第二用户能够顺利登录，保证了整个认证过程的安全性和可靠性。

实施例七

请参考图 8，图 8 是本发明实施例七提供的一种执行身份认证方法的电子设备的结构示意图。

电子设备 80 包括：一个或多个处理器 81 以及存储器 82，图 8 中以一个处理器 81 为例。

处理器 81 和存储器 82 可以通过总线或者其他方式连接，图 8 中以

通过总线连接为例。

存储器 82 作为一种非易失性计算机可读存储介质，可用于存储非易失性软件程序、非易失性计算机可执行程序以及模块，如本发明实施例中的身份认证方法对应的程序指令/模块（例如，附图 3 所示的模块 301-311，附图 4 所示的模块 401-405）。处理器 81 通过运行存储在存储器 82 中的非易失性软件程序、指令以及模块，从而执行服务器的各种功能应用以及数据处理，即实现上述方法实施例文件读取的方法。

存储器 82 可以包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需要的应用程序；存储数据区可存储根据数据存储装置的使用所创建的数据等。此外，存储器 82 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个存储存储器件、闪存器件、或其他非易失性固态存储器件。在一些实施例中，存储器 82 可选包括相对于处理器 81 远程设置的存储器，这些远程存储器可以通过网络连接至数据存储装置。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

所述一个或者多个模块存储在所述存储器 82 中，当被所述一个或者多个处理器 81 执行时，执行上述任意方法实施例中的身份认证方法，例如，执行以上描述的图 5 中的方法步骤 S501 至 S506，图 6 中的方法步骤 S601 至步骤 S611，图 7 中的方法步骤 S701 至步骤 S705，实现图 3 中的模块 301-311、图 4 中的模块 401-405 的功能。

上述产品可执行本发明实施例所提供的方法，具备执行方法相应的功能模块和有益效果。未在本实施例中详尽描述的技术细节，可参见本申请实施例所提供的方法。

本申请实施例的电子设备可以为服务器，即提供计算服务的设备。服务器的构成包括处理器、硬盘、内存、系统总线等，服务器和通用的计算机架构类似，但是由于需要提供高可靠的服务，因此在处理能力、稳定性、可靠性、安全性、可扩展性、可管理性等方面要求较高。

本实施例提供的电子设备：能够在第一用户认证成功的终端设备上，将该终端设备作为第二用户进行认证登录的设备，通过在同一设备

上先后认证第一用户和第二用户身份，在第一用户提供担保的前提下，使得第二用户能够顺利登录，保证了整个认证过程的安全性和可靠性。

本发明实施例提供了一种非易失性计算机可读存储介质，所述计算机可读存储介质存储有计算机可执行指令，该计算机可执行指令被一个或多个处理器执行，例如图 8 中的一个处理器 81，可使得上述一个或多个处理器可执行上述任意方法实施例中的文件读取的方法，例如，执行以上描述的图 5 中的方法步骤 S501 至 S506，图 6 中的方法步骤 S601 至步骤 S611，图 7 中的方法步骤 S701 至步骤 S705，实现图 3 中的模块 301-311、图 4 中的模块 401-405 的功能。

本发明实施例提供了一种计算机程序产品，当计算机程序被执行时，实现上述任意方法实施例中的数据存储的方法，例如，执行以上描述的图 5 中的方法步骤 S501 至 S506，图 6 中的方法步骤 S601 至步骤 S611，图 7 中的方法步骤 S701 至步骤 S705，实现图 3 中的模块 301-311、图 4 中的模块 401-405 的功能。

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单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。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实施例方案的目的。

通过以上的实施例的描述，本领域普通技术人员可以清楚地了解到各实施例可借助软件加通用硬件平台的方式来实现，当然也可以通过硬件。本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory, ROM)或随机存储记忆体(Random Access Memory, RAM)等。

最后应说明的是：以上实施例仅用以说明本申请的技术方案，而非对其限制；在本申请的思路下，以上实施例或者不同实施例中的技术特

征之间也可以进行组合，步骤可以以任意顺序实现，并存在如上所述的本申请的不同方面的许多其它变化，为了简明，它们没有在细节中提供；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

需要说明的是，本发明的说明书及其附图中给出了本发明的较佳的实施例，但是，本发明可以通过许多不同的形式来实现，并不限于本说明书所描述的实施例，这些实施例不作为对本发明内容的额外限制，提供这些实施例的目的是使对本发明的公开内容的理解更加透彻全面。并且，上述各技术特征继续相互组合，形成未在上面列举的各种实施例，均视为本发明说明书记载的范围；进一步地，对本领域普通技术人员来说，可以根据上述说明加以改进或变换，而所有这些改进和变换都应属于本发明所附权利要求的保护范围。

权 利 要 求 书

1. 一种身份认证的方法，其特征在于，包括：

接收在终端设备上输入的第一用户的第一生物特征，并且获取所述第一用户的账号信息以及所述终端设备的设备标识；

根据所述账号信息、设备标识和第一生物特征，向认证服务器发送身份认证请求；

接收所述认证服务器根据所述身份认证请求确认所述第一用户的合法身份之后返回的身份确认信息；

接收在所述终端设备上输入的第二用户的第二生物特征；

根据所述第二生物特征，向所述认证服务器发送验证请求；

接收所述认证服务器在根据所述验证请求确认所述第二生物特征的合法性之后返回的登录码，以使所述第二用户结合所述登录码进行登录。

2. 根据权利要求 1 所述的方法，其特征在于，

所述身份认证请求是依据第一生物特征所绑定的私钥对账号信息、第一生物特征和设备标识进行加密生成的。

3. 根据权利要求 2 所述的方法，其特征在于，

所述私钥是在所述第一生物特征被检验通过之后获取得到的。

4. 根据权利要求 2 或者 3 所述的方法，其特征在于，

所述验证请求是依据第一生物特征所绑定的私钥对所述第二生物特征进行加密生成的。

5. 一种身份认证的方法，其特征在于，包括：

接收终端设备发送的身份认证信息，所述身份认证信息携带所述第一用户的账号信息、第一用户的第一生物特征和所述终端设备的设备标识；

在根据所述身份认证信息确认所述第一用户的合法身份之后，向所述终端设备返回身份确认信息；

接收所述终端设备发送的验证请求，所述验证请求携带第二用户的

第二生物特征；

在根据所述验证请求确认所述第二生物特征的合法性之后，生成与所述第二用户对应的登录码；

向所述终端设备发送所述登录码，以使所述第二用户结合所述登录码进行登录。

6. 根据权利要求 5 所述的方法，其特征在于，

所述身份确认信息是确定所述账号信息、第一用户的第一生物特征和所述设备标识存在对应关系时生成的。

7. 根据权利要求 5 所述的方法，其特征在于，

所述确认所述第二生物特征的合法性包括：

确定生物特征库存在所述第二生物特征。

8. 一种终端设备，其特征在于，包括：

生物特征识别模块，用于进行生物特征识别；

第一接收模块，用于接收在终端设备上输入的第一用户的第一生物特征；

第一获取模块，用于获取所述第一用户的账号信息以及所述终端设备的设备标识；

第一发送模块，用于根据所述账号信息、设备标识和第一生物特征，向认证服务器发送身份认证请求；

第二接收模块，用于接收所述认证服务器根据所述身份认证请求确认所述第一用户的合法身份之后返回的身份确认信息；

第三接收模块，用于接收在所述终端设备上输入的第二用户的第二生物特征；

第二发送模块，用于根据所述第二生物特征，向所述认证服务器发送验证请求；

第四接收模块，用于接收所述认证服务器在根据所述验证请求确认所述第二生物特征的合法性之后返回的登录码，以使所述第二用户结合所述登录码进行登录。

9. 根据权利要求 8 所述的终端设备，其特征在于，所述终端设备还包括：

第一加密模块，用于依据第一生物特征所绑定的私钥对账号信息、第一生物特征和设备标识进行加密。

10. 根据权利要求 9 所述的终端设备，其特征在于，所述终端设备还包括：

第二获取模块，用于在所述第一生物特征被检验通过之后，获取所述私钥。

11. 根据权利要求 9 或者 10 所述的终端设备，其特征在于，所述终端设备还包括：

第二加密模块，用于依据第一生物特征所绑定的私钥对所述第二生物特征进行加密。

12. 一种认证服务器，其特征在于，包括：

第一接收模块，用于接收终端设备发送的身份认证信息，所述身份认证信息携带所述第一用户的账号信息、第一用户的第一生物特征和所述终端设备的设备标识；

第一返回模块，用于在根据所述身份认证信息确认所述第一用户的合法身份之后，向所述终端设备返回身份确认信息；

第二接收模块，用于接收所述终端设备发送的验证请求，所述验证请求携带第二用户的第二生物特征；

生成模块，用于在根据所述验证请求确认所述第二生物特征的合法性之后，生成与所述第二用户对应的登录码；

第二返回模块，用于向所述终端设备发送所述登录码，以使所述第二用户结合所述登录码进行登录。

13. 一种电子设备，其特征在于，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 任一项所述的方法。

14. 一种电子设备，其特征在于，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 5-7 任一项所述的方法。

15. 一种计算机程序产品，其特征在于，所述计算机程序产品包括存储在非易失性计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被电子设备执行时，使所述电子设备执行权利要求 1-4 任一项所述的方法。

16. 一种计算机程序产品，其特征在于，所述计算机程序产品包括存储在非易失性计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被电子设备执行时，使所述电子设备执行权利要求 5-7 任一项所述的方法。

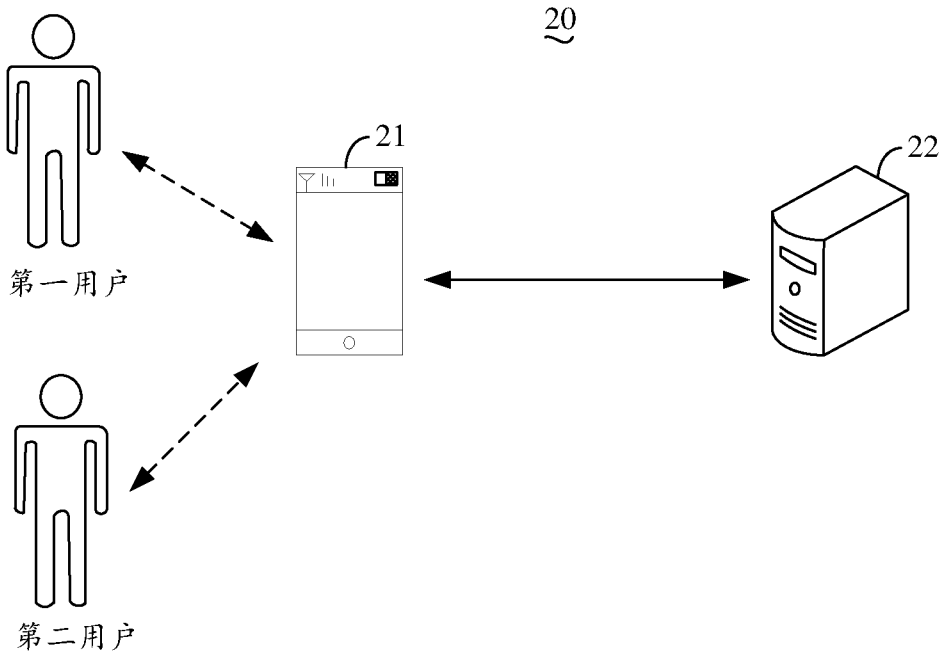

20
21
22
第一用户
第二用户

图 1

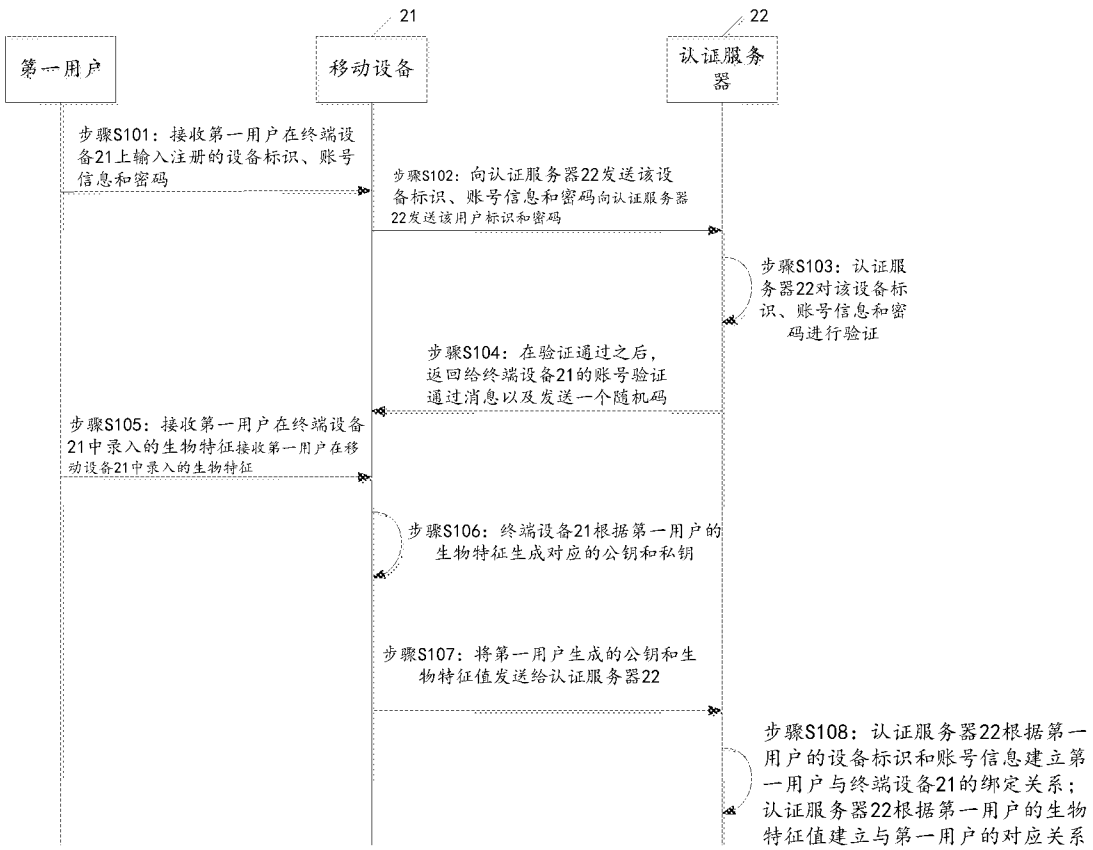

第一用户
21
移动设备
22
认证服务器
步骤S101：接收第一用户在终端设备21上输入注册的设备标识、账号信息和密码
步骤S102：向认证服务器22发送该设备标识、账号信息和密码向认证服务器22发送该用户标识和密码
步骤S103：认证服务器22对该设备标识、账号信息和密码进行验证
步骤S104：在验证通过之后，返回给终端设备21的账号验证通过消息以及发送一个随机码
步骤S105：接收第一用户在终端设备21中录入的生物特征接收第一用户在移动设备21中录入的生物特征
步骤S106：终端设备21根据第一用户的生物特征生成对应的公钥和私钥
步骤S107：将第一用户生成的公钥和生物特征值发送给认证服务器22
步骤S108：认证服务器22根据第一用户的设备标识和账号信息建立第一用户与终端设备21的绑定关系；认证服务器22根据第一用户的生物特征值建立与第一用户的对应关系

图 2

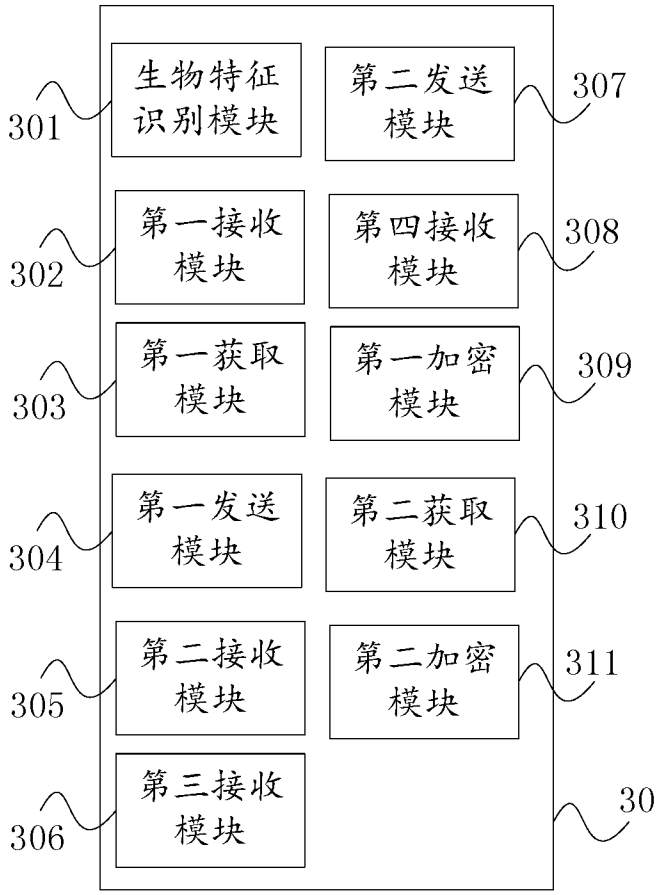

生物特征识别模块
301
第一接收模块
302
第一获取模块
303
第一发送模块
304
第二接收模块
305
第三接收模块
306
第二发送模块
307
第四接收模块
308
第一加密模块
309
第二获取模块
310
第二加密模块
311
30

图 3

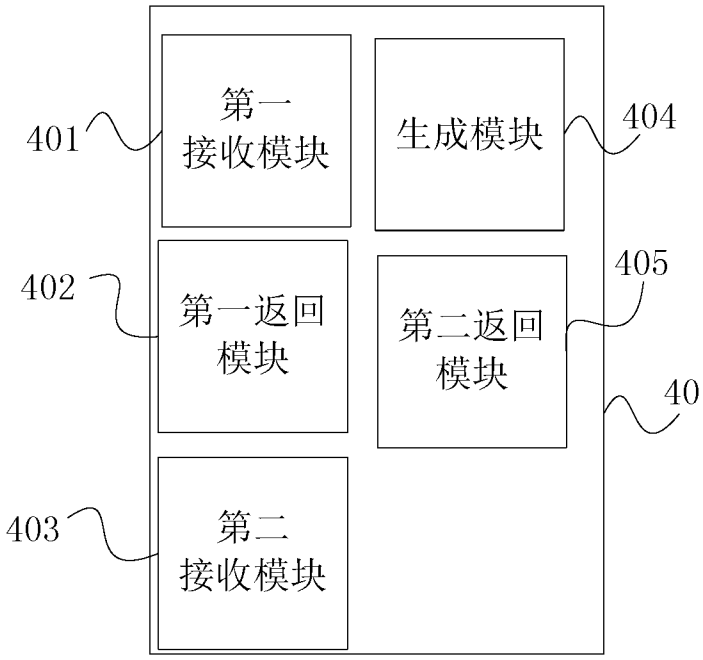

第一接收模块
401
第一返回模块
402
第二接收模块
403
生成模块
404
第二返回模块
405
40

图 4

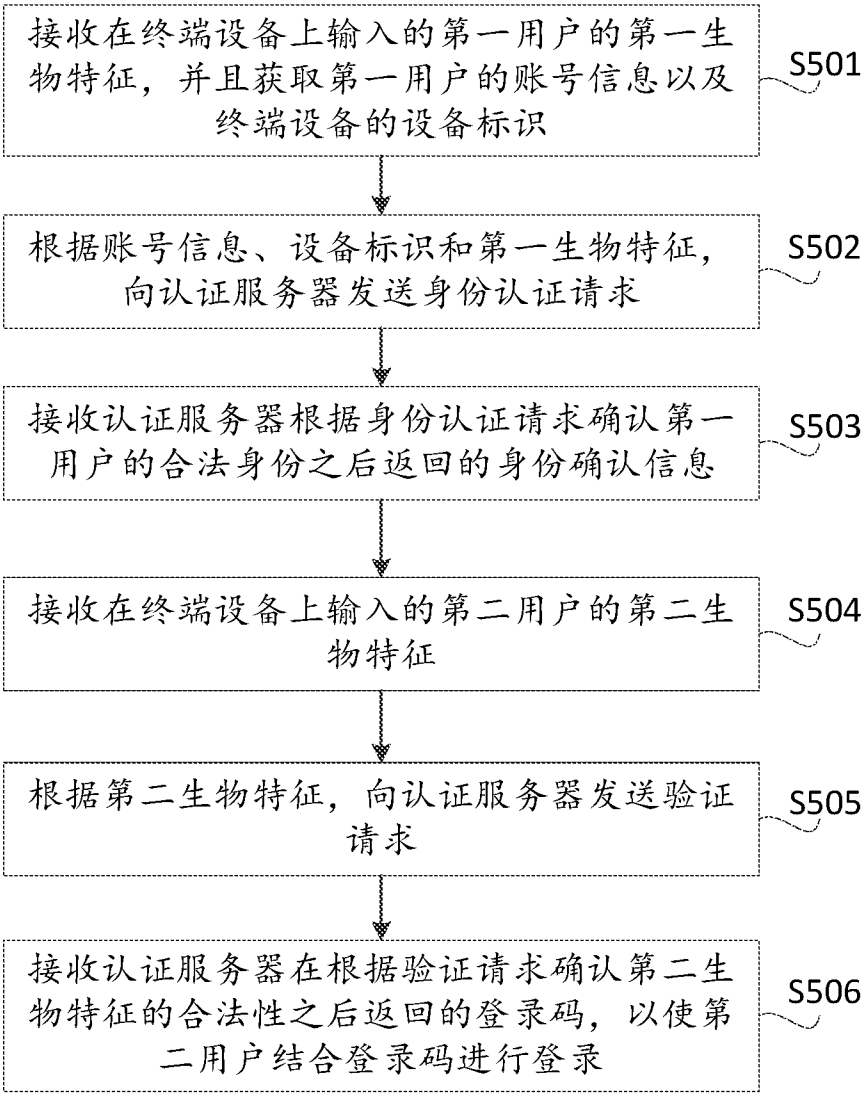

接收在终端设备上输入的第一用户的第一生物特征，并且获取第一用户的账号信息以及终端设备的设备标识
S501
根据账号信息、设备标识和第一生物特征，向认证服务器发送身份认证请求
S502
接收认证服务器根据身份认证请求确认第一用户的合法身份之后返回的身份确认信息
S503
接收在终端设备上输入的第二用户的第二生物特征
S504
根据第二生物特征，向认证服务器发送验证请求
S505
接收认证服务器在根据验证请求确认第二生物特征的合法性之后返回的登录码，以使第二用户结合登录码进行登录
S506

图 5

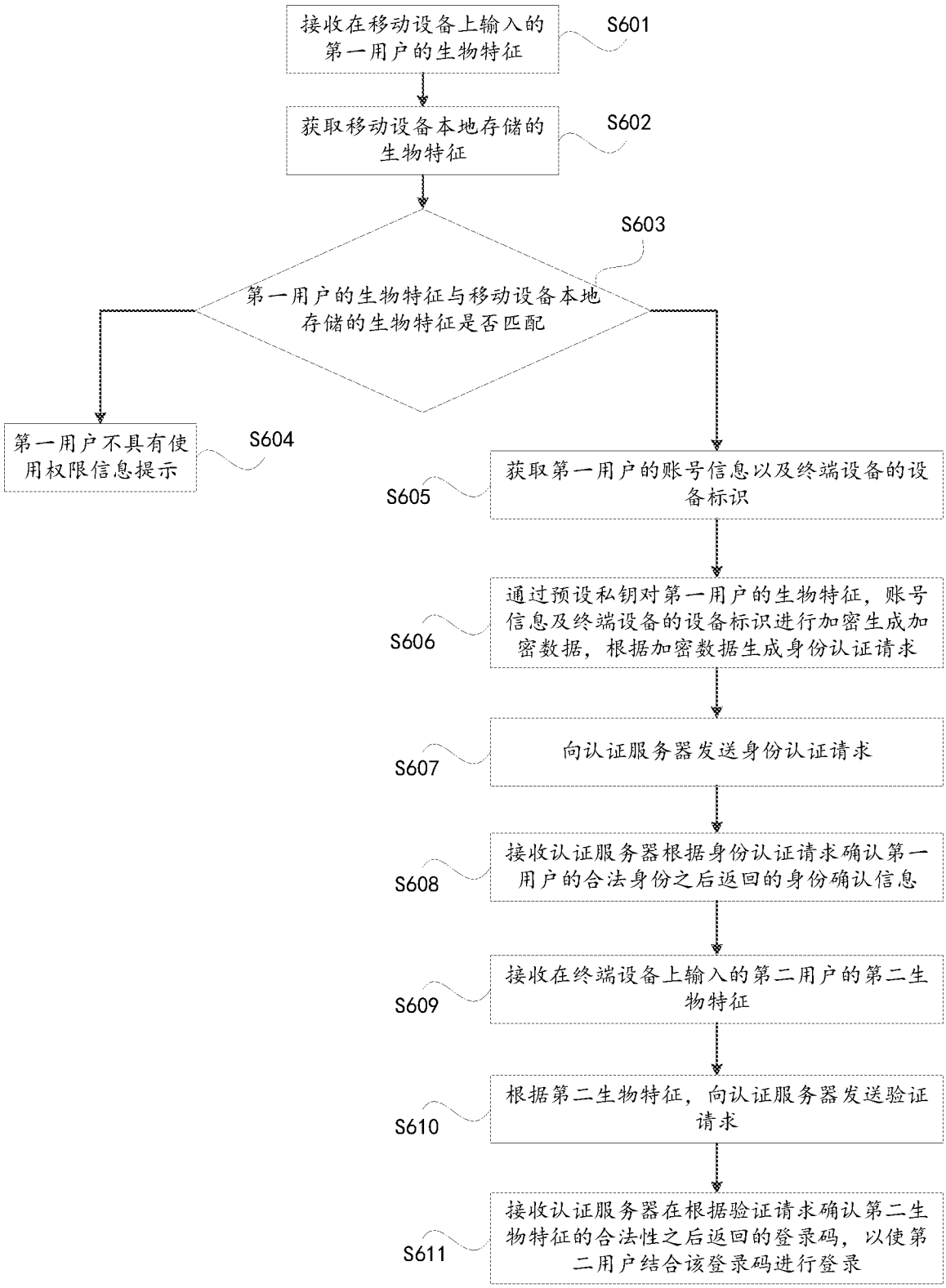

接收在移动设备上输入的第一用户的生物特征
S601
获取移动设备本地存储的生物特征
S602
S603
第一用户的生物特征与移动设备本地存储的生物特征是否匹配
第一用户不具有使用权限信息提示
S604
S605
获取第一用户的账号信息以及终端设备的设备标识
S606
通过预设私钥对第一用户的生物特征，账号信息及终端设备的设备标识进行加密生成加密数据，根据加密数据生成身份认证请求
S607
向认证服务器发送身份认证请求
S608
接收认证服务器根据身份认证请求确认第一用户的合法身份之后返回的身份确认信息
S609
接收在终端设备上输入的第二用户的第二生物特征
S610
根据第二生物特征，向认证服务器发送验证请求
S611
接收认证服务器在根据验证请求确认第二生物特征的合法性之后返回的登录码，以使第二用户结合该登录码进行登录

图 6

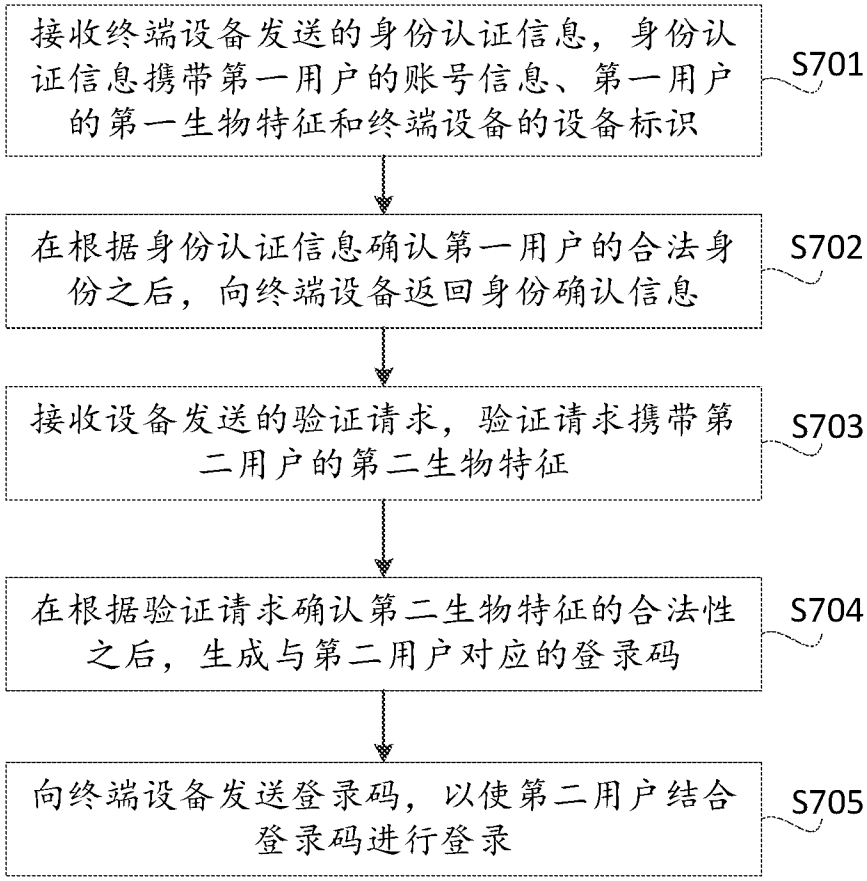

接收终端设备发送的身份认证信息，身份认证信息携带第一用户的账号信息、第一用户的第一生物特征和终端设备的设备标识
S701
在根据身份认证信息确认第一用户的合法身份之后，向终端设备返回身份确认信息
S702
接收设备发送的验证请求，验证请求携带第二用户的第二生物特征
S703
在根据验证请求确认第二生物特征的合法性之后，生成与第二用户对应的登录码
S704
向终端设备发送登录码，以使第二用户结合登录码进行登录
S705

图 7

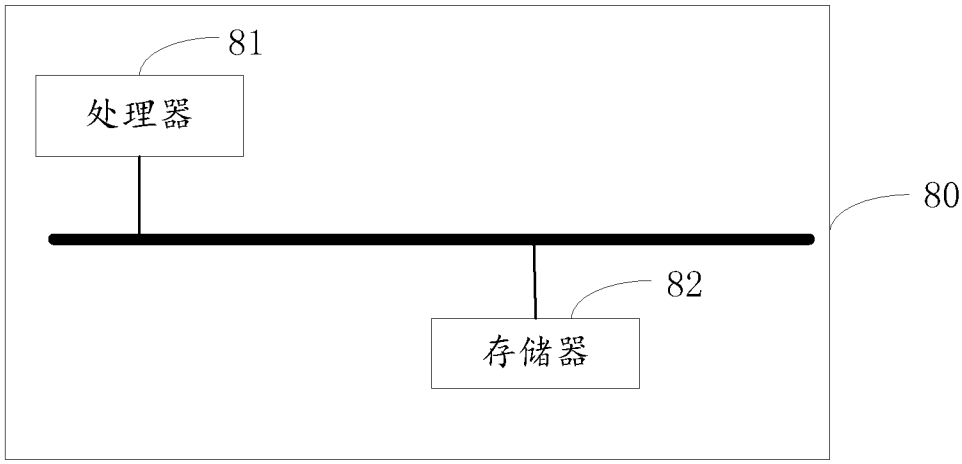

81
处理器
80
82
存储器

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/105886

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: 第一用户, 第二用户, 认证, 验证, 指纹, 生物特征, 身份, 担保, 授权, 访问, 登录, 服务器, 公钥, 密钥, first user, second user, authentic+, fingerprint, biological feature, authorize+, access+, login+, server, public, private, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104079710 A (ZHEJIANG UNIVERSITY), 01 October 2014 (01.10.2014), description, paragraphs [0018]-[0019]	1-16
Y	CN 104735065 A (LENOVO (BEIJING) CO., LTD.), 24 June 2015 (24.06.2015), description, paragraphs [0058]-[0083], [0161]-[0176] and [0210]-[0215]	1-16
A	CN 105931337 A (HANGZHOU YAOGUANG TECHNOLOGY CO., LTD.), 07 September 2016 (07.09.2016), entire document	1-16
A	CN 104966007 A (ONEPLUS TECHNOLOGY (SHENZHEN) CO., LTD.), 07 October 2015 (07.10.2015), entire document	1-16
A	CN 102959922 A (TELEFONAKTIEBOLAGET L M ERICSSON), 06 March 2013 (06.03.2013), entire document	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 July 2017	15 August 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer WANG, Xiaoyan Telephone No. (86-10) 62413916

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/105886

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104079710 A	01 October 2014	None	
CN 104735065 A	24 June 2015	None	
CN 105931337 A	07 September 2016	None	
CN 104966007 A	07 October 2015	WO 2016188268 A1	01 December 2016
CN 102959922 A	06 March 2013	EP 2586171 A1	01 May 2013
		US 2011321132 A1	29 December 2011
		WO 2011160855 A1	29 December 2011

国际检索报告

国际申请号
PCT/CN2016/105886

A. 主题的分类

H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04M

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, CNKI, WPI, EPODOC: 第一用户, 第二用户, 认证, 验证, 指纹, 生物特征, 身份, 担保, 授权, 访问, 登录, 服务器, 公钥, 密钥, first user, second user, authentic+, fingerprint, biological feature, authorize+, access+, login+, server, public, private, key

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 104079710 A (浙江大学) 2014年 10月 1日 (2014-10-01) 说明书第[0018]-[0019]段	1-16
Y	CN 104735065 A (联想北京有限公司) 2015年 6月 24日 (2015-06-24) 说明书第[0058]-[0083]、[0161]-[0176]、[0210]-[0215]段	1-16
A	CN 105931337 A (杭州摇光科技有限公司) 2016年 9月 7日 (2016-09-07) 全文	1-16
A	CN 104966007 A (深圳市万普拉斯科技有限公司) 2015年 10月 7日 (2015-10-07) 全文	1-16
A	CN 102959922 A (瑞典爱立信有限公司) 2013年 3月 6日 (2013-03-06) 全文	1-16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 7月 24日	2017年 8月 15日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王晓燕
传真号 (86-10)62019451	电话号码 (86-10)62413916

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/105886

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	104079710	A	2014年 10月 1日	无			
CN	104735065	A	2015年 6月 24日	无			
CN	105931337	A	2016年 9月 7日	无			
CN	104966007	A	2015年 10月 7日	WO	2016188268	A1	2016年 12月 1日
CN	102959922	A	2013年 3月 6日	EP	2586171	A1	2013年 5月 1日
				US	2011321132	A1	2011年 12月 29日
				WO	2011160855	A1	2011年 12月 29日