(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106161359 B
(45)授权公告日 2019.09.17

(21)申请号 201510155552.4

(22)申请日 2015.04.02

(65)同一申请的已公布的文献号
申请公布号 CN 106161359 A

(43)申请公布日 2016.11.23

(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 蒋龙

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 103716794 A,2014.04.09,
CN 103716794 A,2014.04.09,
CN 102421097 A,2012.04.18,
CN 104219626 A,2014.12.17,
US 2010070766 A1,2010.03.18,
US 2003076961 A1,2003.04.24,
CN 103178969 A,2013.06.26,

审查员 李珍珍

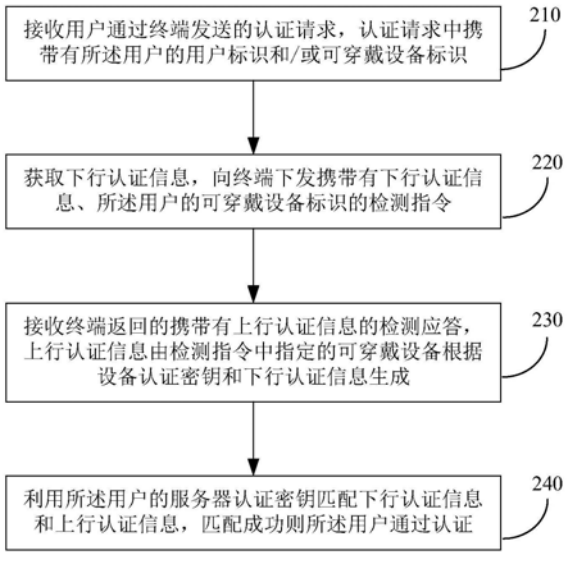
权利要求书7页 说明书15页 附图6页

(54)发明名称

认证用户的方法及装置、注册可穿戴设备的方法及装置

(57)摘要

本申请提供一种认证用户的方法，应用在保存有用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系的服务器上，包括：接收用户通过终端发送的认证请求，认证请求中携带有所述用户的用户标识和/或可穿戴设备标识；获取下行认证信息，向终端下发携带有下行认证信息、所述用户的可穿戴设备标识的检测指令；接收终端返回的携带有上行认证信息的检测应答，上行认证信息由检测指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，设备认证密钥与服务器认证密钥相同或相对应；利用用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则用户通过认证。通过本申请的技术方案，减轻了用户负担，提高了用户获取网络服务的效率。



CN 106161359 B

1.一种认证用户的方法,应用在服务器上,其特征在于,所述服务器保存有用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系,所述方法包括:

接收用户通过终端发送的认证请求,所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识;

获取下行认证信息,向终端下发携带有下行认证信息、所述用户的可穿戴设备标识的检测指令;

接收终端返回的携带有上行认证信息的检测应答,所述上行认证信息由检测指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成,所述设备认证密钥与服务器认证密钥相同或相对应;所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备;

利用对应于所述可穿戴设备标识的服务器认证密钥匹配下行认证信息和上行认证信息,匹配成功则所述用户通过认证。

2.根据权利要求1所述的方法,其特征在于,所述服务器还保存有用户的用户公钥,所述用户公钥对应于所述用户的用户标识、可穿戴设备标识和服务器认证密钥,与保存在终端的用户私钥为一对密钥;

所述终端返回的检测应答由保存在终端的用户私钥签名;

所述方法还包括:根据所述用户的用户公钥对所述终端的检测应答进行签名校验,如果校验失败则用户认证失败。

3.根据权利要求1所述的方法,其特征在于,所述服务器还保存有终端标识,所述终端标识对应于所述用户的用户标识、可穿戴设备标识和服务器认证密钥;

所述认证请求中还包括:发送认证请求的终端标识;

所述方法还包括:如果对应于认证请求中用户标识或可穿戴设备标识的终端标识,与发送认证请求的终端标识不同,则用户认证失败。

4.根据权利要求1至3任意一项所述的方法,其特征在于,所述服务器还保存有服务器私钥,所述服务器私钥与保存在终端的终端公钥为一对密钥;

所述方法还包括:用服务器私钥对检测指令进行签名。

5.根据权利要求1至3任意一项所述的方法,其特征在于,所述检测指令和检测应答通过服务器与终端之间的加密通道传输。

6.根据权利要求1至3任意一项所述的方法,其特征在于,所述服务器为支付服务器,所述认证请求为支付请求;

所述方法还包括:向通过认证的用户提供支付服务。

7.一种认证用户的方法,应用在接入用户可穿戴设备的终端上,其特征在于,所述方法包括:

根据用户的操作向服务器发送认证请求,所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识;

接收服务器的检测指令,所述检测指令中携带有下行认证信息和可穿戴设备标识;

将下行认证信息发送给所述检测指令中指定的可穿戴设备,接收所述可穿戴设备返回的上行认证信息;所述上行认证信息由所述可穿戴设备根据保存的设备认证密钥和下行认证信息生成,所述设备认证密钥与保存在服务器的服务器认证密钥相同或相对应;所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备;

向服务器发送携带有上行认证信息的检测应答；

接收服务器根据所述上行认证信息、下行认证信息和对应于所述可穿戴设备标识的服务器认证密钥确定的用户认证结果。

8.根据权利要求7所述的方法，其特征在于，所述终端保存有所述用户的用户私钥，所述用户私钥与保存在服务器的用户公钥为一对密钥；

所述方法还包括：用所述用户的用户私钥对检测应答进行签名。

9.根据权利要求7或8所述的方法，其特征在于，所述终端保存有终端公钥，所述终端公钥与保存在服务器的服务器私钥为一对密钥；

所述服务器下发的检测指令由服务器私钥签名；

所述方法还包括：根据终端公钥对所述服务器的检测指令进行签名校验，如果校验失败则拒绝所述检测指令。

10.根据权利要求7或8所述的方法，其特征在于，所述认证请求为支付请求，所述终端在用户认证结果为通过认证后，完成用户的支付操作。

11.一种注册可穿戴设备的方法，应用在服务器上，其特征在于，包括：

接收用户通过终端发送的可穿戴设备注册请求，所述注册请求中携带有所述用户的用户标识和可穿戴设备标识；

获取对应于所述可穿戴设备标识的服务器认证密钥和设备认证密钥，向终端下发携带有设备认证密钥、所述用户的可穿戴设备标识的写入指令；

接收终端返回的写入应答，如果写入应答表明设备认证密钥已成功保存在所述写入指令中指定的可穿戴设备中，则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系；所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备；所述对应关系用来通过采用设备认证密钥和服务器认证密钥认证所述指定的可穿戴设备，来认证所述用户。

12.根据权利要求11所述的方法，其特征在于，所述保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系，包括：

向终端下发密码确认请求；

接收终端携带有用户密码的密码确认应答，如果用户密码正确，则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系。

13.根据权利要求11或12所述的方法，其特征在于，所述终端返回的写入应答中还包括所述终端生成的用户公钥；

所述保存用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系，还包括：保存所述用户的用户标识、可穿戴设备标识、服务器认证密钥和用户公钥的对应关系。

14.根据权利要求11或12所述的方法，其特征在于，所述服务器还保存有服务器私钥和服务器公钥；所述服务器私钥与保存在终端的终端公钥为一对密钥；所述服务器公钥与保存在终端的终端私钥为一对密钥；

所述方法还包括：用服务器私钥对写入指令进行签名；

所述方法还包括：采用服务器公钥对所述终端的写入应答进行签名校验，如果校验失败则拒绝所述注册请求。

15.一种注册可穿戴设备的方法，应用在终端上，其特征在于，包括：

根据用户的操作向服务器发送可穿戴设备注册请求，所述注册请求中携带有所述用户的用户标识和可穿戴设备标识；

接收服务器的写入指令，所述写入指令中携带有设备认证密钥、所述用户的可穿戴设备标识；

对写入指令中指定的可穿戴设备执行写入设备认证密钥的操作；所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备；

向服务器发送写入应答，所述写入应答中携带写入设备认证密钥是否成功的消息，供服务器在收到写入设备认证密钥成功的消息后，保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系；所述对应关系由服务器用来通过采用设备认证密钥和服务器认证密钥认证所述指定的可穿戴设备，来认证所述用户；所述服务器认证密钥与所述设备认证密钥相同或相对应。

16.根据权利要求15所述的方法，其特征在于，所述方法还包括：在向服务器发送写入应答后，接收服务器的密码确认请求，将用户输入的用户密码携带在密码确认应答中返回至服务器。

17.根据权利要求15或16所述的方法，其特征在于，所述方法还包括：当写入设备认证密钥的操作成功后，生成所述用户的用户私钥和用户公钥，保存所述用户私钥；

所述写入应答中还携带有所述用户的用户公钥。

18.根据权利要求15或16所述的方法，其特征在于，所述终端保存有终端公钥和终端私钥；所述终端公钥与保存在服务器的服务器私钥为一对密钥；所述终端私钥与保存在服务器的服务器公钥为一对密钥；

所述方法还包括：采用终端公钥对所述服务器的写入指令进行签名校验，如果校验失败则拒绝所述写入指令；

所述方法还包括：用终端私钥对写入应答进行签名。

19.一种认证用户的装置，应用在服务器上，其特征在于，所述服务器保存有用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系，所述装置包括：

认证请求接收单元，用于接收用户通过终端发送的认证请求，所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识；

检测指令下发单元，用于获取下行认证信息，向终端下发携带有下行认证信息、所述用户的可穿戴设备标识的检测指令；

检测应答接收单元，用于接收终端返回的携带有上行认证信息的检测应答，所述上行认证信息由检测指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，所述设备认证密钥与服务器认证密钥相同或相对应；所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备；

匹配单元，用于利用对应于所述可穿戴设备标识的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证。

20.根据权利要求19所述的装置，其特征在于，所述服务器还保存有用户的用户公钥，所述用户公钥对应于所述用户的用户标识、可穿戴设备标识和服务器认证密钥，与保存在终端的用户私钥为一对密钥；

所述终端返回的检测应答由保存在终端的用户私钥签名；

所述装置还包括:检测应答校验单元,用于根据所述用户的用户公钥对所述终端的检测应答进行签名校验,如果校验失败则用户认证失败。

21.根据权利要求19所述的装置,其特征在于,所述服务器还保存有终端标识,所述终端标识对应于所述用户的用户标识、可穿戴设备标识和服务器认证密钥;

所述认证请求中还包括:发送认证请求的终端标识;

所述装置还包括:终端标识校验单元,用于在对应于认证请求中用户标识或可穿戴设备标识的终端标识,与发送认证请求的终端标识不同时,用户认证失败。

22.根据权利要求19至21任意一项所述的装置,其特征在于,所述服务器还保存有服务器私钥,所述服务器私钥与保存在终端的终端公钥为一对密钥;

所述装置还包括:检测指令签名单元,用于用服务器私钥对检测指令进行签名。

23.根据权利要求19至21任意一项所述的装置,其特征在于,所述服务器为支付服务器,所述认证请求为支付请求;

所述装置还包括:支付服务单元,用于向通过认证的用户提供支付服务。

24.一种认证用户的装置,应用在接入用户可穿戴设备的终端上,其特征在于,所述装置包括:

认证请求发送单元,用于根据用户的操作向服务器发送认证请求,所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识;

检测指令接收单元,用于接收服务器的检测指令,所述检测指令中携带有下行认证信息和可穿戴设备标识;

上行认证信息单元,用于将下行认证信息发送给所述检测指令中指定的可穿戴设备,接收所述可穿戴设备返回的上行认证信息;所述上行认证信息由所述可穿戴设备根据保存的设备认证密钥和下行认证信息生成,所述设备认证密钥与保存在服务器的服务器认证密钥相同或相对应;所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备;

检测应答发送单元,用于向服务器发送携带有上行认证信息的检测应答;

认证结果接收单元,用于接收服务器根据所述上行认证信息、下行认证信息和对应于所述可穿戴设备标识的服务器认证密钥确定的用户认证结果。

25.根据权利要求24所述的装置,其特征在于,所述终端保存有所述用户的用户私钥,所述用户私钥与保存在服务器的用户公钥为一对密钥;

所述装置还包括:检测应答签名单元,用于用所述用户的用户私钥对检测应答进行签名。

26.根据权利要求24或25所述的装置,其特征在于,所述终端保存有终端公钥,所述终端公钥与保存在服务器的服务器私钥为一对密钥;

所述服务器下发的检测指令由服务器私钥签名;

所述装置还包括:检测指令校验单元,用于根据终端公钥对所述服务器的检测指令进行签名校验,如果校验失败则拒绝所述检测指令。

27.根据权利要求24或25所述的装置,其特征在于,所述认证请求为支付请求,所述终端在用户认证结果为通过认证后,完成用户的支付操作。

28.一种注册可穿戴设备的装置,应用在服务器上,其特征在于,包括:

注册请求接收单元,用于接收用户通过终端发送的可穿戴设备注册请求,所述注册请

求中携带有所述用户的用户标识和可穿戴设备标识；

写入指令下发单元，用于获取对应于所述可穿戴设备标识的服务器认证密钥和设备认证密钥，向终端下发携带有设备认证密钥、所述用户的可穿戴设备标识的写入指令；

写入应答接收单元，用于接收终端返回的写入应答，如果写入应答表明设备认证密钥已成功保存在所述写入指令中指定的可穿戴设备中，则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系；所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备；所述对应关系用来通过采用设备认证密钥和服务器认证密钥认证所述指定的可穿戴设备，来认证所述用户。

29.根据权利要求28所述的装置，其特征在于，所述写入应答接收单元包括：

密码确认请求下发模块，用于在写入应答表明设备认证密钥已成功保存在所述写入指令中指定的可穿戴设备中时，向终端下发密码确认请求；

密码确认应答接收模块，用于接收终端携带有用户密码的密码确认应答，如果用户密码正确，则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系。

30.根据权利要求28或29所述的装置，其特征在于，所述终端返回的写入应答中还包括所述终端生成的用户公钥；

所述写入应答接收单元保存所述用户的用户标识、可穿戴设备标识、服务器认证密钥和用户公钥的对应关系，包括：保存所述用户的用户标识、可穿戴设备标识、服务器认证密钥和用户公钥的对应关系。

31.根据权利要求28或29所述的装置，其特征在于，所述服务器还保存有服务器私钥和服务器公钥；所述服务器私钥与保存在终端的终端公钥为一对密钥；所述服务器公钥与保存在终端的终端私钥为一对密钥；

所述装置还包括：写入指令签名单元，用于用服务器私钥对写入指令进行签名；

所述装置还包括：写入应答校验单元，用于采用服务器公钥对所述终端的写入应答进行签名校验，如果校验失败则拒绝所述注册请求。

32.一种注册可穿戴设备的装置，应用在终端上，其特征在于，包括：

注册请求发送单元，用于根据用户的操作向服务器发送可穿戴设备注册请求，所述注册请求中携带有所述用户的用户标识和可穿戴设备标识；

写入指令接收单元，用于接收服务器的写入指令，所述写入指令中携带有设备认证密钥、所述用户的可穿戴设备标识；

写入操作执行单元，用于对写入指令中指定的可穿戴设备执行写入设备认证密钥的操作；所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备；

写入应答发送单元，用于向服务器发送写入应答，所述写入应答中携带写入设备认证密钥是否成功的消息，供服务器在收到写入设备认证密钥成功的消息后，保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系；所述对应关系由服务器用来通过采用设备认证密钥和服务器认证密钥认证所述指定的可穿戴设备，来认证所述用户；所述服务器认证密钥与所述设备认证密钥相同或相对应。

33.根据权利要求32所述的装置，其特征在于，所述装置还包括：密码确认请求接收单元，用于在向服务器发送写入应答后，接收服务器的密码确认请求，将用户输入的用户密码携带在密码确认应答中返回至服务器。

34.根据权利要求32或33所述的装置，其特征在于，所述装置还包括：用户密钥生成单元，用于当写入设备认证密钥的操作成功后，生成所述用户的用户私钥和用户公钥，保存所述用户私钥；

所述写入应答中还携带有所述用户的用户公钥。

35.根据权利要求32或33所述的装置，其特征在于，所述终端保存有终端公钥和终端私钥；所述终端公钥与保存在服务器的服务器私钥为一对密钥；所述终端私钥与保存在服务器的服务器公钥为一对密钥；

所述装置还包括：写入指令校验单元，用于采用终端公钥对所述服务器的写入指令进行签名校验，如果校验失败则拒绝所述写入指令；

所述装置还包括：写入应答签名单元，用于用终端私钥对写入应答进行签名。

36.一种支付方法，其特征在于，包括：

接收用户通过支付客户端发送的支付请求，所述支付请求中携带有用户的用户标识和/或可穿戴设备标识；

获取下行认证信息，并向支付客户端下发包括下行认证信息以及可穿戴设备标识的认证指令；

接收支付客户端返回的携带有上行认证信息的认证响应信息，所述上行认证信息由认证指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，所述设备认证密钥与服务器认证密钥相同或相对应；所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备；

利用对应于所述可穿戴设备标识的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证，并在认证通过后进行支付操作。

37.根据权利要求36所述的方法，其特征在于，所述支付请求为用户通过在支付客户端上选择的表示由可穿戴设备进行支付的信息所触发。

38.一种支付方法，其特征在于，包括：

响应于用户在支付客户端上的支付操作，向服务器发送支付请求，所述支付请求中携带有用户的用户标识和/或可穿戴设备标识；

接收服务器下发的包括下行认证信息和可穿戴设备标识的认证指令，并将所述下行认证信息发送至可穿戴设备，以便由可穿戴设备利用自身保存的设备认证密钥和下行认证信息生成上行认证信息；所述可穿戴设备为具有所述可穿戴设备标识的可穿戴设备；

接收可穿戴设备返回的上行认证信息，并发送至服务器，以便服务器根据上行认证信息对用户进行认证，并在认证通过后进行支付操作。

39.根据权利要求38所述的支付方法，其特征在于，用户在支付客户端上的支付操作具体为用户选择的表示由可穿戴设备进行支付的操作。

40.一种可穿戴设备的支付方法，其特征在于，包括：

接收支付客户端发送的支付认证信息，所述支付认证信息包括服务器基于支付客户端发送的用户的支付请求所下发的下行认证信息；

根据保存的设备认证密钥和下行认证信息生成上行认证信息，并将所述上行认证信息发送至支付客户端，以便由支付客户端将上行认证信息发送至服务器，使得服务器可基于上行认证信息对用户进行认证，并在认证通过后进行支付操作。

41.根据权利要求40所述的方法,其特征在于,还包括:

响应于用户通过支付客户端下发的支付绑定请求,将支付绑定请求中携带的设备认证密钥保存。

42.一种支付装置,其特征在于,包括:

支付请求接收单元,用于接收用户通过支付客户端发送的支付请求,所述支付请求中携带有用户的用户标识和/或可穿戴设备标识;

认证指令下发单元,用于获取下行认证信息,并向支付客户端下发包括下行认证信息以及可穿戴设备标识的认证指令;

认证响应接收单元,用于接收支付客户端返回的携带有上行认证信息的认证响应信息,所述上行认证信息由认证指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成,所述设备认证密钥与服务器认证密钥相同或相对应;所述指定的可穿戴设备为具有所述可穿戴设备标识的可穿戴设备;

支付匹配单元,用于利用对应于所述可穿戴设备标识的服务器认证密钥匹配下行认证信息和上行认证信息,匹配成功则所述用户通过认证,并在认证通过后进行支付操作。

43.根据权利要求42所述的装置,其特征在于,所述支付请求为用户通过在支付客户端上选择的表示由可穿戴设备进行支付的信息所触发。

44.一种支付装置,其特征在于,包括:

支付请求发送单元,用于响应于用户在支付客户端上的支付操作,向服务器发送支付请求,所述支付请求中携带有用户的用户标识和/或可穿戴设备标识;

认证指令接收单元,用于接收服务器下发的包括下行认证信息和可穿戴设备标识的认证指令,并将所述下行认证信息发送至可穿戴设备,以便由可穿戴设备利用自身保存的设备认证密钥和下行认证信息生成上行认证信息;所述可穿戴设备为具有所述可穿戴设备标识的可穿戴设备;

认证响应发送单元,用于接收可穿戴设备返回的上行认证信息,并发送至服务器,以便服务器根据上行认证信息对用户进行认证,并在认证通过后进行支付操作。

45.根据权利要求44所述的装置,其特征在于,用户在支付客户端上的支付操作具体为用户选择的表示由可穿戴设备进行支付的操作。

46.一种可穿戴设备的支付装置,其特征在于,包括:

支付认证信息接收单元,用于接收支付客户端发送的支付认证信息,所述支付认证信息包括服务器基于支付客户端发送的用户的支付请求所下发的下行认证信息;

上行认证信息生成单元,用于根据保存的设备认证密钥和下行认证信息生成上行认证信息,并将所述上行认证信息发送至支付客户端,以便由支付客户端将上行认证信息发送至服务器,使得服务器可基于上行认证信息对用户进行认证,并在认证通过后进行支付操作。

47.根据权利要求46所述的装置,其特征在于,所述装置还包括:支付绑定单元,用于响应于用户通过支付客户端下发的支付绑定请求,将支付绑定请求中携带的设备认证密钥保存。

认证用户的方法及装置、注册可穿戴设备的方法及装置

技术领域

[0001] 本申请涉及互联网技术领域，尤其涉及一种认证用户的方法及装置和一种注册可穿戴设备的方法及装置。

背景技术

[0002] 随着互联网技术的飞速发展，用户越来越多的利用网络来完成各种活动，如办公、娱乐、购物、理财等等。用户通常从多个服务提供商那里获得这些服务，用户在各个服务提供商的服务器上进行注册，每次获得服务时都需要向服务器提供账号和密码，以便服务器对用户进行认证，并提供对应的服务。

[0003] 出于安全考虑，用户应尽量避免在多个服务提供商处使用相同的账号和密码。当用户希望获得的服务逐渐增多时，记住每个服务提供商处的账号和对应的密码就成为用户日渐沉重的负担。同时，随着网络服务日益遍及到生活的方方面面，用户总是需要输入账号和密码来完成认证，操作繁琐，降低了获得网络服务的效率。

发明内容

[0004] 有鉴于此，本申请提供了一种认证用户的方法，应用在服务器上，所述服务器保存有用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系，所述方法包括：

[0005] 接收用户通过终端发送的认证请求，所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识；

[0006] 获取下行认证信息，向终端下发携带有下行认证信息、所述用户的可穿戴设备标识的检测指令；

[0007] 接收终端返回的携带有上行认证信息的检测应答，所述上行认证信息由检测指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，所述设备认证密钥与服务器认证密钥相同或相对应；

[0008] 利用所述用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证。

[0009] 本申请提供的一种认证用户的方法，应用在接入用户可穿戴设备的终端上，所述方法包括：

[0010] 根据用户的操作向服务器发送认证请求，所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识；

[0011] 接收服务器的检测指令，所述检测指令中携带有下行认证信息和可穿戴设备标识；

[0012] 将下行认证信息发送给所述检测指令中指定的可穿戴设备，接收所述可穿戴设备返回的上行认证信息；所述上行认证信息由所述可穿戴设备根据保存的设备认证密钥和下行认证信息生成，所述设备认证密钥与保存在服务器的服务器认证密钥相同或相对应；

[0013] 向服务器发送携带有上行认证信息的检测应答；

[0014] 接收服务器根据所述上行认证信息、下行认证信息和服务器认证密钥确定的用户认证结果。

[0015] 本申请提供了一种注册可穿戴设备的方法，应用在服务器上，包括：

[0016] 接收用户通过终端发送的可穿戴设备注册请求，所述注册请求中携带有所述用户的用户标识和可穿戴设备标识；

[0017] 获取所述用户的服务器认证密钥和设备认证密钥，向终端下发携带有设备认证密钥、所述用户的可穿戴设备标识的写入指令；

[0018] 接收终端返回的写入应答，如果写入应答表明设备认证密钥已成功保存在所述写入指令中指定的可穿戴设备中，则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系。

[0019] 本申请提供的一种注册可穿戴设备的方法，应用在终端上，包括：

[0020] 根据用户的操作向服务器发送可穿戴设备注册请求，所述注册请求中携带有所述用户的用户标识和可穿戴设备标识；

[0021] 接收服务器的写入指令，所述写入指令中携带有设备认证密钥、所述用户的可穿戴设备标识；

[0022] 对写入指令中指定的可穿戴设备执行写入设备认证密钥的操作；

[0023] 向服务器发送写入应答，所述写入应答中携带写入设备认证密钥是否成功的消息。

[0024] 本申请还提供了一种认证用户的装置，应用在服务器上，所述服务器保存有用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系，所述装置包括：

[0025] 认证请求接收单元，用于接收用户通过终端发送的认证请求，所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识；

[0026] 检测指令下发单元，用于获取下行认证信息，向终端下发携带有下行认证信息、所述用户的可穿戴设备标识的检测指令；

[0027] 检测应答接收单元，用于接收终端返回的携带有上行认证信息的检测应答，所述上行认证信息由检测指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，所述设备认证密钥与服务器认证密钥相同或相对应；

[0028] 匹配单元，用于利用所述用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证。

[0029] 本申请提供的一种认证用户的装置，应用在接入用户可穿戴设备的终端上，所述装置包括：

[0030] 认证请求发送单元，用于根据用户的操作向服务器发送认证请求，所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识；

[0031] 检测指令接收单元，用于接收服务器的检测指令，所述检测指令中携带有下行认证信息和可穿戴设备标识；

[0032] 上行认证信息单元，用于将下行认证信息发送给所述检测指令中指定的可穿戴设备，接收所述可穿戴设备返回的上行认证信息；所述上行认证信息由所述可穿戴设备根据保存的设备认证密钥和下行认证信息生成，所述设备认证密钥与保存在服务器的服务器认证密钥相同或相对应；

[0033] 检测应答发送单元，用于向服务器发送携带有上行认证信息的检测应答；

[0034] 认证结果接收单元，用于接收服务器根据所述上行认证信息、下行认证信息和服务器认证密钥确定的用户认证结果。

[0035] 本申请提供了一种注册可穿戴设备的装置，应用在服务器上，包括：

[0036] 注册请求接收单元，用于接收用户通过终端发送的可穿戴设备注册请求，所述注册请求中携带有所述用户的用户标识和可穿戴设备标识；

[0037] 写入指令下发单元，用于获取所述用户的服务器认证密钥和设备认证密钥，向终端下发携带有设备认证密钥、所述用户的可穿戴设备标识的写入指令；

[0038] 写入应答接收单元，用于接收终端返回的写入应答，如果写入应答表明设备认证密钥已成功保存在所述写入指令中指定的可穿戴设备中，则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系。

[0039] 本申请提供的一种注册可穿戴设备的装置，应用在终端上，包括：

[0040] 注册请求发送单元，用于根据用户的操作向服务器发送可穿戴设备注册请求，所述注册请求中携带有所述用户的用户标识和可穿戴设备标识；

[0041] 写入指令接收单元，用于接收服务器的写入指令，所述写入指令中携带有设备认证密钥、所述用户的可穿戴设备标识；

[0042] 写入操作执行单元，用于对写入指令中指定的可穿戴设备执行写入设备认证密钥的操作；

[0043] 写入应答发送单元，用于向服务器发送写入应答，所述写入应答中携带写入设备认证密钥是否成功的消息。

[0044] 本申请提供了一种支付方法，包括：

[0045] 接收用户通过支付客户端发送的支付请求，所述支付请求中携带有用户的用户标识和/或可穿戴设备标识；

[0046] 获取下行认证信息，并向支付客户端下发包括下行认证信息以及可穿戴设备标识的认证指令；

[0047] 接收支付客户端返回的携带有上行认证信息的认证响应信息，所述上行认证信息由认证指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，所述设备认证密钥与服务器认证密钥相同或相对应；

[0048] 利用所述用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证，并在认证通过后进行支付操作。

[0049] 本申请提供的一种支付方法，包括：

[0050] 响应于用户在支付客户端上的支付操作，向服务器发送支付请求，所述支付请求中携带有用户的用户标识和/或可穿戴设备标识；

[0051] 接收服务器下发的包括下行认证信息和可穿戴设备标识的认证指令，并将所述下行认证信息发送至可穿戴设备，以便由可穿戴设备利用自身保存的设备认证密钥和下行认证信息生成上行认证信息；

[0052] 接收可穿戴设备返回的上行认证信息，并发送至服务器，以便服务器根据上行认证信息对用户进行认证，并在认证通过后进行支付操作。

[0053] 本申请提供的一种可穿戴设备的支付方法，包括：

[0054] 接收支付客户端发送的支付认证信息，所述支付认证信息包括服务器基于支付客户端发送的用户的支付请求所下发的下行认证信息；

[0055] 根据保存的设备认证密钥和下行认证信息生成上行认证信息，并将所述上行认证信息发送至支付客户端，以便由支付客户端将上行认证信息发送至服务器，使得服务器可基于上行认证信息对用户进行认证，并在认证通过后进行支付操作。

[0056] 本申请提供了一种支付装置，包括：

[0057] 支付请求接收单元，用于接收用户通过支付客户端发送的支付请求，所述支付请求中携带有用户的用户标识和/或可穿戴设备标识；

[0058] 认证指令下发单元，用于获取下行认证信息，并向支付客户端下发包括下行认证信息以及可穿戴设备标识的认证指令；

[0059] 认证响应接收单元，用于接收支付客户端返回的携带有上行认证信息的认证响应信息，所述上行认证信息由认证指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，所述设备认证密钥与服务器认证密钥相同或相对应；

[0060] 支付匹配单元，用于利用所述用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证，并在认证通过后进行支付操作。

[0061] 本申请提供的一种支付装置，包括：

[0062] 支付请求发送单元，用于响应于用户在支付客户端上的支付操作，向服务器发送支付请求，所述支付请求中携带有用户的用户标识和/或可穿戴设备标识；

[0063] 认证指令接收单元，用于接收服务器下发的包括下行认证信息和可穿戴设备标识的认证指令，并将所述下行认证信息发送至可穿戴设备，以便由可穿戴设备利用自身保存的设备认证密钥和下行认证信息生成上行认证信息；

[0064] 认证响应发送单元，用于接收可穿戴设备返回的上行认证信息，并发送至服务器，以便服务器根据上行认证信息对用户进行认证，并在认证通过后进行支付操作。

[0065] 本申请还提供了一种可穿戴设备的支付装置，包括：

[0066] 支付认证信息接收单元，用于接收支付客户端发送的支付认证信息，所述支付认证信息包括服务器基于支付客户端发送的用户的支付请求所下发的下行认证信息；

[0067] 上行认证信息生成单元，用于根据保存的设备认证密钥和下行认证信息生成上行认证信息，并将所述上行认证信息发送至支付客户端，以便由支付客户端将上行认证信息发送至服务器，使得服务器可基于上行认证信息对用户进行认证，并在认证通过后进行支付操作。

[0068] 由以上技术方案可见，本申请的实施例通过在服务器和可穿戴设备上设置服务器认证密钥和设备认证密钥，服务器通过与终端的交互，利用设置的服务器认证密钥和设备认证密钥来对指定的可穿戴设备进行认证，从而完成对与该可穿戴设备对应的用户的认证，用户无需记忆账号和密码，也无需在认证过程中输入账号和密码，减轻了用户负担，提高了用户获取网络服务的效率。

附图说明

[0069] 图1是一种本申请应用场景的网络结构图；

[0070] 图2是本申请实施例中一种应用在服务器上的认证用户的方法的流程图；

[0071] 图3是本申请实施例中一种应用在终端上的认证用户的方法的流程图；

[0072] 图4是本申请实施例中一种应用在服务器上的注册可穿戴设备的方法的流程图；

[0073] 图5是本申请实施例中一种应用在终端上的注册可穿戴设备的方法的流程图；

[0074] 图6是服务器、可穿戴设备或终端的一种硬件结构图；

[0075] 图7是本申请实施例中一种应用在服务器上的认证用户的装置的逻辑结构图；

[0076] 图8是本申请实施例中一种应用在终端上的认证用户的装置的逻辑结构图；

[0077] 图9是本申请实施例中一种应用在服务器上的注册可穿戴设备的装置的逻辑结构图；

[0078] 图10是本申请实施例中一种应用在终端上注册可穿戴设备的装置的逻辑结构图。

具体实施方式

[0079] 可穿戴设备是一种可被用户穿戴在身上，或整合到用户衣服或配件中的便携式设备，如手环、智能手表、智能运动鞋、智能服装、智能眼镜、智能头盔、智能戒指等。可穿戴设备具有部分计算功能，可以通过硬件接口或无线局域网连接到智能手机、平板电脑、个人电脑等终端，通过与终端交换数据来实现各种功能。

[0080] 可穿戴设备通常专属于一个用户，有的可穿戴设备会随时随地穿戴在用户身上，在一定程度上，这样的可穿戴设备就代表了用户。本申请的实施例提出一种认证用户的方法，利用可穿戴设备的存储和计算功能来进行对用户的认证，不再需要用户记忆和频繁输入账号及密码，从而解决现有技术中存在的问题。

[0081] 本申请的实施例所应用的一种网络环境如图1所示，可穿戴设备通过硬件接口或无线局域网接入到终端，硬件接口可以是音频接口、USB(Universal Serial Bus，通用串行总线)接口等，无线局域网可以是蓝牙(Bluetooth)、Wi-Fi(Wireless-Fidelity，无线保真)、ZigBee(紫蜂协议)等，终端可以是智能手机、平板电脑、个人电脑等。终端通过通信网络(如互联网和/或移动通信网络)与服务器进行通信，用户在终端上发送到服务器的访问，服务器对用户进行认证。本申请的实施例中对终端的种类、可穿戴设备接入终端的硬件接口或无线局域网协议、通信网络的协议和组网结构、服务器的具体实现方式均不做限定。

[0082] 在本申请的一个实施例中，认证用户的方法在服务器上的流程如图2所示，在终端上的流程如图3所示。

[0083] 本实施例中，在服务器上保存着用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系。用户标识是对该服务器来说某个用户区别于其他用户的唯一身份标识，例如用户名、注册邮箱等；如果该用户和移动终端绑定，还可以是所绑定移动终端的号码、IMEI(International Mobile Equipment Identity，移动设备国际身份码)等。可穿戴设备标识用来唯一代表该穿戴设备，因具体的设备种类和采用的无线局域网协议的不同而不同，通常可以是该可穿戴设备的硬件地址，如MAC(Media Access Control，媒体介入控制)地址。服务器认证密钥保存在服务器上，根据使用该服务器认证密钥的加密算法，与保存在可穿戴设备上的设备认证密钥相同或者相对应。保存在服务器上的可穿戴设备标识和服务器认证密钥一一对应，如果一个用户可以有超过一个的可穿戴设备用于认证，则一个用户标识可能对应于两个或两个以上的可穿戴设备标识和服务器认证密钥。另外需要说明的是，用户标识、可穿戴设备标识和服务器认证密钥的对应关系可以保存在服务器本地，也可

以保存在服务器可访问的其他存储设备，如存储区域网络的磁盘阵列或云存储网络中，本实施例中不做限定。

[0084] 在终端上，步骤310，根据用户的操作向服务器发送认证请求，认证请求中携带有所述用户的用户标识和/或可穿戴设备标识。

[0085] 在服务器上，步骤210，接收用户通过终端发送的认证请求。

[0086] 当用户在终端上向服务器请求需要进行身份认证的服务(如登录、访问个人账户、支付等)时，服务器向终端要求认证用户所需的相关信息。终端向服务器发送认证请求，在认证请求中携带该用户的用户标识、或该用户的可穿戴设备标识、或该用户的用户标识和可穿戴设备标识。

[0087] 服务器收到终端的认证请求后，通过其中的用户标识和/或可穿戴设备标识，可以确定请求认证的是哪个用户。

[0088] 在服务器上，步骤220，获取下行认证信息，向终端下发携带有下行认证信息、该用户的可穿戴设备标识的检测指令。

[0089] 下行认证信息可以是一段认证数据，也可以是利用保存在服务器上的服务器认证密钥将认证数据加密后的密文。服务器可以用任意的方式来获得认证数据，例如随机生成，或者从某个文件或图片中截取一定的字节数；服务器可以在本地自行生成认证数据，也可以从其他服务器上获取；本实施例中均不做限定。

[0090] 在收到终端的认证请求后，服务器提取认证请求中的用户标识和/或可穿戴设备标识，在所保存的用户标识、可穿戴设备标识和服务器认证密钥的对应关系中查找是否包括该标识，如果不包括或者认证请求中的用户标识和可穿戴设备标识不属于同一个用户，则拒绝终端的认证请求；否则服务器获取认证数据，对明文的下行认证信息，服务器将认证数据、该用户的可穿戴设备标识封装在检测指令中，下发给终端；对密文的下行认证信息，服务器用与认证请求中用户标识或可穿戴设备标识对应的服务器认证密钥将认证数据加密后生成下行认证信息，将下行认证信息、该用户的可穿戴设备标识封装在检测指令中，下发给终端。

[0091] 在终端上，步骤320，接收服务器的检测指令，检测指令中携带有下行认证信息和可穿戴设备标识。

[0092] 在终端上，步骤330，将下行认证信息发送给检测指令中指定的可穿戴设备，接收该可穿戴设备返回的上行认证信息；上行认证信息由该可穿戴设备根据保存的设备认证密钥和下行认证信息生成。

[0093] 终端收到服务器的检测指令，从中提取出可穿戴设备标识和下行认证信息，把下行认证信息发送给检测指令中指定的可穿戴设备(即具有检测指令中可穿戴设备标识的可穿戴设备)。如果检测指令中指定的可穿戴设备尚未接入终端，则终端需要先按照该可穿戴设备支持的无线局域网协议，完成与该可穿戴设备的连接。

[0094] 如前所述，服务器指定的可穿戴设备上保存有与服务器认证密钥相同或者相对应的设备认证密钥。可穿戴设备收到下行认证信息后，对明文的下行认证信息，可穿戴设备利用设备认证密钥对下行认证信息进行加密，生成密文的上行认证信息；对密文的下行认证信息，可穿戴利用设备认证密钥对下行认证信息进行解密，生成明文的上行认证信息。明文的下行认证信息对应于密文的上行认证信息，密文的下行认证信息对应于明文的上行认证

信息。可穿戴设备将上行认证信息返回给终端。

[0095] 在终端上，步骤340，向服务器发送携带有上行认证信息的检测应答。

[0096] 终端收到可穿戴设备返回的上行认证信息后，将上行认证信息封装在检测应答中发送给服务器。检测应答中通常还携带有该可穿戴设备标识。

[0097] 在服务器上，步骤230，接收终端返回的携带有上行认证信息的检测应答。

[0098] 在服务器上，步骤240，利用该用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则该用户通过认证。

[0099] 服务器收到终端返回的检测应答，从中提取上行认证信息，利用该用户的服务器认证密钥来判断上行认证信息和下行认证信息是否匹配，以确定该用户的认证结果。具体而言，对明文的上行认证信息，可以将上行认证信息和用来生成密文的认证数据进行比对，或者将上行认证信息用服务器认证密钥加密后和下行认证信息进行比对，如果相同则该用户通过认证，否则认证失败；对密文的上行认证信息，可以用服务器认证密钥将其解密后和下行认证信息进行比对，如果相同则该用户通过认证，否则认证失败。

[0100] 服务器将用户是否通过认证的认证结果返回给终端。

[0101] 在终端上，步骤350，接收服务器根据上行认证信息、下行认证信息和服务器认证密钥确定的用户认证结果。

[0102] 本实施例中，在服务器上和可穿戴设备上设置相同或相对应的服务器认证密钥和设备认证密钥，服务器通过与终端的交互，利用保存在可穿戴设备上的设备认证密钥和保存在服务器上的服务器认证密钥来对指定的可穿戴设备进行认证，从而完成对与该可穿戴设备对应的用户的认证，用户无需记忆账号和密码，也无需在认证过程中输入账号和密码，减轻了用户负担，提高了用户获取网络服务的效率。

[0103] 在一种实现方式中，可以在服务器上保存用户的用户公钥，在终端上保存该用户的用户私钥，不同的用户标识使用不同的用户公钥和用户私钥，用户公钥与用户私钥为非对称加密中的一对密钥。服务器上保存的用户公钥对应于该用户的用户标识、可穿戴设备标识和服务器认证密钥。这种实现方式中，终端用保存的用户私钥对检测应答中携带的数据(包括上行认证信息，还可以包括可穿戴设备标识、用户标识等其他数据)进行签名，将签名后的检测应答发送给服务器；服务器用该用户的用户公钥对检测应答进行签名校验，如果通过校验，则执行步骤240，进行上行认证信息和下行认证信息的匹配，如果未能通过签名校验，则通知终端认证失败。这种实现方式要求某个用户利用可穿戴设备进行认证时所接入的终端要保存有该用户的用户私钥，可以实现更好的安全性。

[0104] 另外，可以将终端标识加入到在服务器上保存用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系中，来限制能够通过接入的可穿戴设备进行用户认证的终端。在这种情况下，服务器上保存有用户的用户标识、可穿戴设备标识、服务器认证密钥和终端标识的对应关系；终端在发送给服务器的认证请求中携带自己的终端标识；服务器收到认证请求后，将在保存的对应关系中查找与认证请求中的用户标识或可穿戴设备标识对应的终端标识，与发送认证请求的终端标识进行比较，如果相同则执行步骤220继续认证过程，如果不同则拒绝终端的认证请求，用户认证失败。这种实现相当于将可穿戴设备和可以通过该可穿戴设备进行用户认证的终端进行了绑定；由于终端(特别是移动终端)通常也专属于一个用户，绑定可穿戴设备和终端可以极大的增加用户认证的安全性。

[0105] 本实施例中的上述认证过程适用于需要认证用户身份的任意场景，如登录时的用户身份认证、用户访问个人账户时的身份认证、用户通过第三方支付平台进行支付时的身份认证等等。在用户通过认证后，服务器即可提供该场景下的后续服务，终端则执行该场景下的后续操作，例如，在本实施例用作支付场景下的身份认证时，终端向支付服务器发送的认证请求为支付请求；在用户通过认证后，支付服务器可以向通过认证的用户提供支付服务；而终端在收到服务器用户通过认证的认证结果后，可以与支付服务器协同完成用户的支付操作。

[0106] 本实施例中，可以将用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系预置在服务器上，将相应的设备认证密钥预置在可穿戴设备上；也可以在上述认证过程前先通过注册过程来在服务器上生成上述对应关系，在可穿戴设备上写入设备认证密钥。

[0107] 本申请的另一个实施例提供了一种注册可穿戴设备的方法，该方法在服务器上的流程如图4所示，在终端上的流程如图5所示。

[0108] 在终端上，步骤510，根据用户操作向服务器发送可穿戴设备注册请求。

[0109] 在服务器上，步骤410，接收用户通过终端发送的可穿戴设备注册请求。

[0110] 用户在终端上向服务器进行可穿戴设备注册，终端按照用户的操作，将可穿戴设备注册请求发送给服务器，注册请求中包括该用户的用户标识和可穿戴设备标识。

[0111] 在服务器上，步骤420，获取该用户的服务器认证密钥和设备认证密钥，向终端下发携带有设备认证密钥、该用户的可穿戴设备标识的写入指令。

[0112] 收到终端的可穿戴设备注册请求后，根据认证过程中对上行认证信息或下行认证信息所采用的加密算法，服务器获取用于该加密算法、对应于可穿戴设备标识的服务器认证密钥和设备认证密钥。服务器认证密钥和设备认证密钥可以是一个密钥(如对称加密算法的密钥)，也可以是一对密钥(如非对称加密算法的公钥和私钥)。服务器可以自己生成，也可以从其他服务器获得服务器认证密钥和设备认证密钥。

[0113] 服务器将获取的设备认证密钥、对应的可穿戴设备标识封装在写入指令中，发送给该终端。

[0114] 在终端上，步骤520，接收服务器的写入指令，该写入指令中携带有设备认证密钥、该用户的可穿戴设备标识。

[0115] 在终端上，步骤530，对写入指令中指定的可穿戴设备执行写入设备认证密钥的操作。

[0116] 终端收到服务器的写入指令后，终端将写入指令中的设备认证密钥发送给可穿戴设备，请求可穿戴设备保存该设备认证密钥。根据可穿戴设备的不同及其设置权限的不同，可穿戴设备可能需要用户对写入操作进行确认后才能完成对设备认证密钥的存储。例如，对手环，用户通常需要进行敲击确认。

[0117] 在终端上，步骤540，向服务器发送写入应答，写入应答中携带写入设备认证密钥是否成功的消息。终端完成与可穿戴设备之间的写入操作后，将写入是否成功的消息封装在写入应答中，发送给服务器。

[0118] 在服务器上，步骤430，接收终端返回的写入应答，如果写入应答表明设备认证密钥已成功保存在写入指令中指定的可穿戴设备中，则保存该用户的用户标识、可穿戴设备

标识和服务器认证密钥的对应关系，可穿戴设备注册成功；如果写入应答中携带的消息是设备认证密钥写入不成功，则注册过程失败。服务器将注册结果发送给终端。

[0119] 服务器可以要求终端提供该用户的密码来增加可穿戴设备注册的安全性。具体而言，服务器收到终端的写入应答，如果写入应答中携带的消息是设备认证密钥已成功保存在可穿戴设备中，则向终端下发密码确认请求，要求终端提供该可穿戴设备标识对应的用户标识的密码；终端收到服务器的密码确认请求，将用户输入的用户密码携带在密码确认应答中返回至服务器；服务器上接收终端携带有用户密码的密码确认应答，如果用户密码正确，则保存该用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系，可穿戴设备注册成功；如果用户密码错误，则拒绝终端的注册请求，注册失败。服务器将注册结果发送给终端。

[0120] 在一种实现方式中，可以在注册过程中自动生成用户的用户公钥和用户私钥。具体而言，当终端将设备认证密钥写入可穿戴设备的操作成功后，终端根据一定算法生成该用户的用户私钥和用户公钥，在本地保存生成的用户私钥，将用户公钥封装在写入应答中发送给服务器；服务器在终端将设备认证密钥写入可穿戴设备成功或验证用户密码正确后，保存该用户的用户标识、可穿戴设备标识、服务器认证密钥和用户公钥的对应关系。

[0121] 一些应用场景中，在服务器上预置有服务器公钥和服务器私钥，在终端上预置有终端私钥和终端公钥，其中服务器公钥与终端私钥为一对密钥，服务器私钥与终端公钥为一对密钥。在这些场景中，认证方法实施例中服务器可以用保存的服务器私钥对检测指令进行签名，将签名后的检测指令发送给终端；终端用保存的终端公钥对接收的检测指令进行签名校验，如果校验失败则拒绝检测指令，认证失败。在注册方法实施例中，服务器可以用保存的服务器私钥对写入指令进行签名，将签名后的写入指令发送给终端；终端用保存的终端公钥对接收的写入指令进行签名校验，如果校验失败则拒绝写入指令，注册失败。终端可以用保存的终端私钥对写入应答进行签名，将签名后的写入应答发送给服务器；服务器用保存的服务器公钥对接收的写入应答进行签名校验，如果校验失败则拒绝终端的注册请求。

[0122] 服务器与终端之间可以通过加密通道来进行通信，以进一步提高可穿戴设备注册和用户认证的安全性。例如认证方法实施例中的检测指令和检测应答、注册方法实施例中的写入指令和写入应答都可以在加密通道中传输。加密通道的实现和所采用加密方法请参见现有技术，不再赘述。

[0123] 在本申请的一个实施例中，运行在终端上的支付客户端利用接入终端的可穿戴设备在支付过程中进行用户身份的认证。本实施例的具体流程如下：

[0124] 在可穿戴设备上，接收支付客户端的支付绑定请求，支付绑定请求中包括该可穿戴设备的设备认证密钥。可穿戴设备响应于用户通过支付客户端下发的支付绑定请求，将支付绑定请求中携带的设备认证密钥保存在本地存储器中；

[0125] 用户在支付客户端上进行支付操作时，选择表示由可穿戴设备进行支付，触发支付客户端对上述用户操作的响应，向服务器发送支付请求，支付请求中携带有用户的用户标识和/或可穿戴设备标识；

[0126] 服务器收到用户通过支付客户端发送的支付请求后，获取下行认证信息，并向支付客户端下发包括下行认证信息以及可穿戴设备标识的认证指令；

[0127] 支付客户端接收服务器下发的认证指令，并将所述下行认证信息在支付认证信息中发送至认证指令中指定的可穿戴设备；

[0128] 可穿戴设备收到支付客户端发送的支付认证信息，从支付认证信息中提取服务器基于支付客户端发送的用户的支付请求所下发的下行认证信息；并根据保存的设备认证密钥和下行认证信息生成上行认证信息，并将上行认证信息发送至支付客户端；

[0129] 支付客户端接收可穿戴设备返回的上行认证信息，将上行认证信息在认证响应信息中发送给服务器；

[0130] 服务器接收支付客户端返回的携带有上行认证信息的认证响应信息，利用该用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则该用户通过认证，并在认证通过后进行支付操作；该用户的服务器认证密钥与认证指令中指定的可穿戴设备的设备认证密钥相同或相对应。

[0131] 本实施例中，通过在服务器上和可穿戴设备上设置相同或相对应的服务器认证密钥和设备认证密钥，利用设备认证密钥和服务器认证密钥来对可穿戴设备进行认证，从而完成与该可穿戴设备对应的用户的支付认证，使得用户可以在支付客户端上用可穿戴设备来进行支付，无需记忆账号和密码，也无需在认证过程中输入账号和密码，减轻了用户负担，提高了支付效率。

[0132] 在本申请的一个应用示例中，用户通过运行在手机终端上的客户端App(应用程序)将手环注册到支付服务器后，可以通过手环完成网络支付而无需输入账号和密码。支付服务器和客户端App上预置有成对的服务器公钥和终端私钥，以及成对的服务器私钥和终端公钥。其中，支付服务器可以运行该客户端App对应的服务端程序的服务器，也可以是支持该客户端App的第三方支付平台的服务器。具体过程如下：

[0133] 用户通过运行在手机终端上的客户端App(以下简称客户端)向支付服务器发送可穿戴设备注册请求，申请开通手环支付，客户端将用户标识(用户在支付服务器的账号)、手机终端标识(IMEI)、手环标识(手环MAC地址)在注册请求中上传给服务器。

[0134] 支付服务器通过预定的算法生成用于认证手环的对称密钥(即相同的服务器认证密钥和设备认证密钥)，将对称密钥和用户标识、手环标识一并通过预置的服务器私钥签名后，封装在写入指令中，通过支付服务器与客户端之间的加密通道发送给客户端。

[0135] 客户端在收到服务端的写入指令后，首先根据预置的终端公钥验证写入指令中数据的合法性，如果数据不合法则直接拒绝写入指令。在通过合法性验证之后，客户端连接写入指令中指定的手环，连接成功后将支付服务器下发的对称密钥写入到手环中。对称密钥写入手环的过程中用户需要敲击手环来对写入操作进行确认，用户敲击手环之后，对称密钥写入手环的存储区域。

[0136] 写入操作成功后，客户端根据用户标识生成一对非对称密钥，对应于用户标识的用户公钥和用户私钥。客户端将写入操作是否成功的结果、手环标识和生成的用户公钥通过预置的终端私钥进行签名，并将签名后的上述信息封装在写入应答中，通过加密通道发送给支付服务器。用户私钥由客户端保存在本地。

[0137] 支付服务器在接收到客户端的写入应答后，先通过预置的服务器公钥对客户端的签名进行验证，如果验证失败则拒绝客户端的注册请求。签名验证通过后，支付服务器向客户端下发密码确认请求，要求客户端提供该用户在支付服务器上的账号的密码。

[0138] 客户端向用户显示输入密码的提示信息，用户在客户端输入其在支付服务器上账号的密码。客户端将接收到的密码在密码确认应答中发送给支付服务器。

[0139] 支付服务端校验密码确认应答中的用户密码，校验通过后将对称密钥(服务器认证密钥)、用户标识、手机终端标识、手环标识和客户端生成的用户公钥的对应关系保存起来，通知客户端手环注册成功，注册过程结束。

[0140] 手环在支付服务器上注册成功后，当用户希望通过手环进行支付时，通过客户端向服务器发送支付的认证请求，认证请求中包括要支付的订单信息、用户标识、手机终端标识和手环标识。

[0141] 收到客户端的认证请求后，支付服务器比较认证请求中的手机终端标识，和保存的对应关系中对应于认证请求中手环标识的手机终端标识，如果不同则拒绝认证请求，支付失败；如果相同，支付服务器生成随机的明文数据，将这一明文数据作为下行认证信息。支付服务器将下行认证信息、用户标识、手环标识用预置的服务器私钥进行签名后，封装在检测指令中，通过与客户端之间的加密通道发送给客户端。

[0142] 客户端在收到支付服务器的检测指令后，首先根据预置的终端公钥验证检测指令中签名数据的合法性，如果数据不合法则拒绝检测指令，支付失败。在通过签名的合法性验证之后，客户端连接检测指令中的指定手环，连接成功后将检测指令中的下行认证信息发送给手环。手环利用保存的对称密钥对下行认证信息进行加密后生成上行认证信息，并将上行认证信息返回至客户端。手环对下行认证信息进行加密的过程不需要用户的敲击确认，可以进一步减少用户操作，优化用户体验。

[0143] 客户端收到手环生成的上行认证信息后，将上行认证信息用本地保存的用户私钥进行签名，将签名后的数据、手环标识封装在检测应答中，通过与支付服务器之间的加密通道发送给支付服务器。

[0144] 支付服务器在收到客户端上传的检测应答后，会根据检测应答中手环标识对应的用户公钥对检测应答进行签名校验，如果签名校验失败则认证请求失败。签名校验成功后，支付服务器用手环标识对应的对称密钥对下行认证信息进行加密，将加密后的数据与检测应答中的上行认证信息进行比对，即比较支付服务器加密的下行认证信息与手环加密的下行认证信息是否相同，相同则向客户端返回认证成功的消息并继续订单的支付；不相同则向客户端返回认证失败的消息。客户端收到认证成功的消息后，与支付服务器一并完成用户订单的支付操作；如果客户端收到认证失败的消息，则通知用户由于认证失败无法完成本次支付。

[0145] 与上述流程实现对应，本申请的实施例还提供了一种应用在服务器上的认证用户的装置、一种应用在接入用户可穿戴设备的终端上的认证用户的装置、一种应用在服务器上的注册可穿戴设备的装置、一种应用在终端上的注册可穿戴设备的装置、一种应用在服务器上的支付装置、一种应用在终端上的支付装置和一种应用在可穿戴设备上的支付装置。这些装置均可以通过软件实现，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，作为逻辑意义上的装置，是通过服务器、终端或可穿戴设备的CPU将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，除了图6所示的CPU、内存以及非易失性存储器之外，装置所在的终端或可穿戴设备通常还包括用于进行无线信号收发的芯片等其他硬件，装置所在的服务器通常还包括用于实现网络通信功能的板卡等其他硬件。

[0146] 图7所示为本实施例提供的一种认证用户的装置，应用在服务器上，所述服务器保存有用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系，所述装置包括认证请求接收单元、检测指令下发单元、检测应答接收单元和匹配单元，其中：认证请求接收单元用于接收用户通过终端发送的认证请求，所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识；检测指令下发单元用于获取下行认证信息，向终端下发携带有下行认证信息、所述用户的可穿戴设备标识的检测指令；检测应答接收单元用于接收终端返回的携带有上行认证信息的检测应答，所述上行认证信息由检测指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，所述设备认证密钥与服务器认证密钥相同或相对应；匹配单元用于利用所述用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证。

[0147] 可选的，所述服务器还保存有用户的用户公钥，所述用户公钥对应于所述用户的用户标识、可穿戴设备标识和服务器认证密钥，与保存在终端的用户私钥为一对密钥；所述终端返回的检测应答由保存在终端的用户私钥签名；所述装置还包括检测应答校验单元，用于根据所述用户的用户公钥对所述终端的检测应答进行签名校验，如果校验失败则用户认证失败。

[0148] 可选的，所述服务器还保存有终端标识，所述终端标识对应于所述用户的用户标识、可穿戴设备标识和服务器认证密钥；所述认证请求中还包括：发送认证请求的终端标识；所述装置还包括：终端标识校验单元，用于在对应于认证请求中用户标识或可穿戴设备标识的终端标识，与发送认证请求的终端标识不同时，用户认证失败。

[0149] 可选的，所述服务器还保存有服务器私钥，所述服务器私钥与保存在终端的终端公钥为一对密钥；所述装置还包括检测指令签名单元，用于用服务器私钥对检测指令进行签名。

[0150] 可选的，所述服务器为支付服务器，所述认证请求为支付请求；所述装置还包括：支付服务单元，用于向通过认证的用户提供支付服务。

[0151] 图8所示为本实施例提供的一种认证用户的装置，应用在接入用户可穿戴设备的终端上，所述装置包括认证请求发送单元、检测指令接收单元、上行认证信息单元、检测应答发送单元和认证结果接收单元，其中：认证请求发送单元用于根据用户的操作向服务器发送认证请求，所述认证请求中携带有所述用户的用户标识和/或可穿戴设备标识；检测指令接收单元用于接收服务器的检测指令，所述检测指令中携带有下行认证信息和可穿戴设备标识；上行认证信息单元用于将下行认证信息发送给所述检测指令中指定的可穿戴设备，接收所述可穿戴设备返回的上行认证信息；所述上行认证信息由所述可穿戴设备根据保存的设备认证密钥和下行认证信息生成，所述设备认证密钥与保存在服务器的服务器认证密钥相同或相对应；检测应答发送单元用于向服务器发送携带有上行认证信息的检测应答；认证结果接收单元用于接收服务器根据所述上行认证信息、下行认证信息和服务器认证密钥确定的用户认证结果。

[0152] 可选的，所述终端保存有所述用户的用户私钥，所述用户私钥与保存在服务器的用户公钥为一对密钥；所述装置还包括检测应答签名单元，用于用所述用户的用户私钥对检测应答进行签名。

[0153] 可选的，所述终端保存有终端公钥，所述终端公钥与保存在服务器的服务器私钥

为一对密钥;所述服务器下发的检测指令由服务器私钥签名;所述装置还包括检测指令校验单元,用于根据终端公钥对所述服务器的检测指令进行签名校验,如果校验失败则拒绝所述检测指令。

[0154] 可选的,所述认证请求为支付请求,所述终端在用户认证结果为通过认证后,完成用户的支付操作。

[0155] 图9所示为本实施例提供的一种注册可穿戴设备的装置,应用在服务器上,从功能上划分,所述装置还包括注册请求接收单元、写入指令下发单元和写入应答接收单元,其中:注册请求接收单元用于接收用户通过终端发送的可穿戴设备注册请求,所述注册请求中携带有所述用户的用户标识和可穿戴设备标识;写入指令下发单元用于获取所述用户的服务器认证密钥和设备认证密钥,向终端下发携带有设备认证密钥、所述用户的可穿戴设备标识的写入指令;写入应答接收单元用于接收终端返回的写入应答,如果写入应答表明设备认证密钥已成功保存在所述写入指令中指定的可穿戴设备中,则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系。

[0156] 可选的,所述写入应答接收单元包括密码确认请求下发模块和密码确认应答接收模块,其中:密码确认请求下发模块用于在写入应答表明设备认证密钥已成功保存在所述写入指令中指定的可穿戴设备中时,向终端下发密码确认请求;密码确认应答接收模块用于接收终端携带有用户密码的密码确认应答,如果用户密码正确,则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系。

[0157] 可选的,所述终端返回的写入应答中还包括所述终端生成的用户公钥;所述密码确认应答接收单元具体用于:接收终端携带有用户密码的密码确认应答,如果用户密码正确,则保存所述用户的用户标识、可穿戴设备标识、服务器认证密钥和用户公钥的对应关系。

[0158] 可选的,所述服务器还保存有服务器私钥和服务器公钥;所述服务器私钥与保存在终端的终端公钥为一对密钥;所述服务器公钥与保存在终端的终端私钥为一对密钥。所述装置还包括写入指令签名单元,用于用服务器私钥对写入指令进行签名;所述装置还包括写入应答校验单元,用于采用服务器公钥对所述终端的写入应答进行签名校验,如果校验失败则拒绝所述注册请求。

[0159] 图10所示为本实施例提供的一种注册可穿戴设备的装置,应用在终端上,从功能上划分,所述装置还包括注册请求发送单元、写入指令接收单元、写入操作执行单元和写入应答发送单元,其中:注册请求发送单元用于根据用户的操作向服务器发送可穿戴设备注册请求,所述注册请求中携带有所述用户的用户标识和可穿戴设备标识;写入指令接收单元用于接收服务器的写入指令,所述写入指令中携带有设备认证密钥、所述用户的可穿戴设备标识;写入操作执行单元用于对写入指令中指定的可穿戴设备执行写入设备认证密钥的操作;写入应答发送单元用于向服务器发送写入应答,所述写入应答中携带写入设备认证密钥是否成功的消息。

[0160] 可选的,所述装置还包括密码确认请求接收单元,用于在向服务器发送写入应答后,接收服务器的密码确认请求,将用户输入的用户密码携带在密码确认应答中返回至服务器。

[0161] 可选的,所述装置还包括用户密钥生成单元,用于当写入设备认证密钥的操作成

功后，生成所述用户的用户私钥和用户公钥，保存所述用户私钥；所述写入应答中还携带有所述用户的用户公钥。

[0162] 可选的，所述终端保存有终端公钥和终端私钥；所述终端公钥与保存在服务器的服务器私钥为一对密钥；所述终端私钥与保存在服务器的服务器公钥为一对密钥；所述装置还包括写入指令校验单元，用于采用终端公钥对所述服务器的写入指令进行签名校验，如果校验失败则拒绝所述写入指令。所述装置还包括写入应答签名单元，用于用终端私钥对写入应答进行签名。

[0163] 本申请的实施例提供了一种支付装置，应用在服务器上，从功能上划分，包括支付请求接收单元、认证指令下发单元、认证响应接收单元和支付匹配单元，其中：支付请求接收单元用于接收用户通过支付客户端发送的支付请求，所述支付请求中携带有用户的用户标识和/或可穿戴设备标识；认证指令下发单元用于获取下行认证信息，并向支付客户端下发包括下行认证信息以及可穿戴设备标识的认证指令；认证响应接收单元用于接收支付客户端返回的携带有上行认证信息的认证响应信息，所述上行认证信息由认证指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成，所述设备认证密钥与服务器认证密钥相同或相对应；支付匹配单元用于利用所述用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证，并在认证通过后进行支付操作。

[0164] 可选的，所述支付请求为用户通过在支付客户端上选择的表示由可穿戴设备进行支付的信息所触发。

[0165] 本申请的实施例提供了一种支付装置，应用在终端上，从功能上划分，，包括支付请求发送单元、认证指令接收单元和认证响应发送单元，其中：支付请求发送单元用于响应于用户在支付客户端上的支付操作，向服务器发送支付请求，所述支付请求中携带有用户的用户标识和/或可穿戴设备标识；认证指令接收单元用于接收服务器下发的包括下行认证信息和可穿戴设备标识的认证指令，并将所述下行认证信息发送至可穿戴设备，以便由可穿戴设备利用自身保存的设备认证密钥和下行认证信息生成上行认证信息；认证响应发送单元用于接收可穿戴设备返回的上行认证信息，并发送至服务器，以便服务器根据上行认证信息对用户进行认证，并在认证通过后进行支付操作。

[0166] 可选的，用户在支付客户端上的支付操作具体为用户选择的表示由可穿戴设备进行支付的操作。

[0167] 本申请的实施例提供了一种可穿戴设备的支付装置，应用在可穿戴设备上，从功能上划分，包括支付认证信息接收单元和上行认证信息生成单元，其中：支付认证信息接收单元用于接收支付客户端发送的支付认证信息，所述支付认证信息包括服务器基于支付客户端发送的用户的支付请求所下发的下行认证信息；上行认证信息生成单元用于根据保存的设备认证密钥和下行认证信息生成上行认证信息，并将所述上行认证信息发送至支付客户端，以便由支付客户端将上行认证信息发送至服务器，使得服务器可基于上行认证信息对用户进行认证，并在认证通过后进行支付操作。

[0168] 可选的，所述装置还包括：支付绑定单元，用于响应于用户通过支付客户端下发的支付绑定请求，将支付绑定请求中携带的设备认证密钥保存。

[0169] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

[0170] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0171] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0172] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0173] 还需要说明的是，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、商品或者设备不仅包括那些要素，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、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0174] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

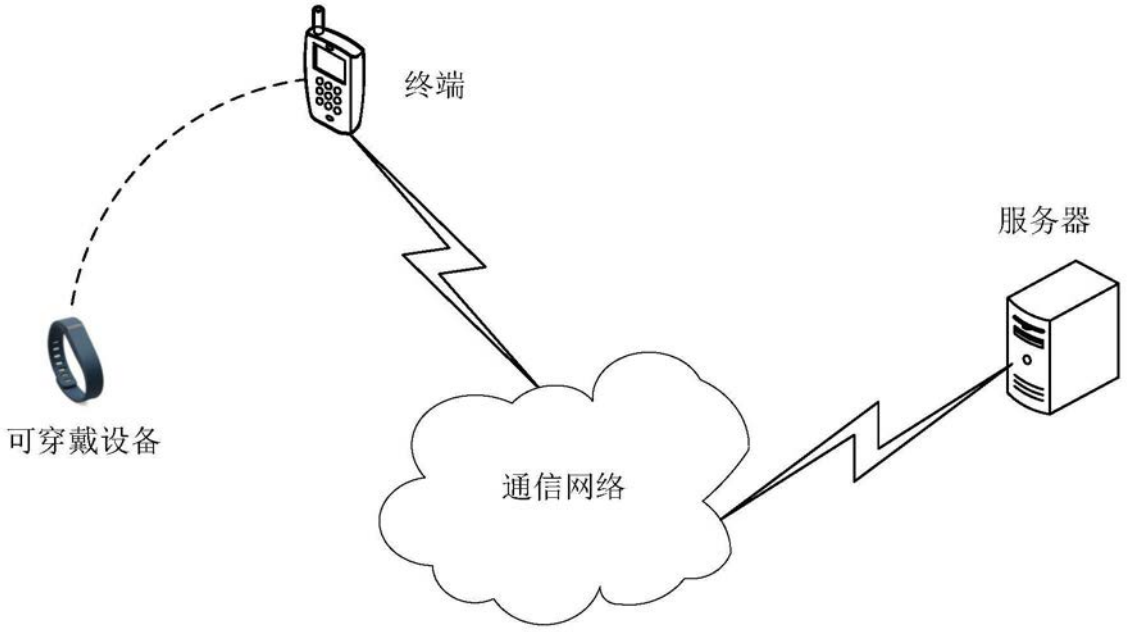

终端
服务器
可穿戴设备
通信网络

图1

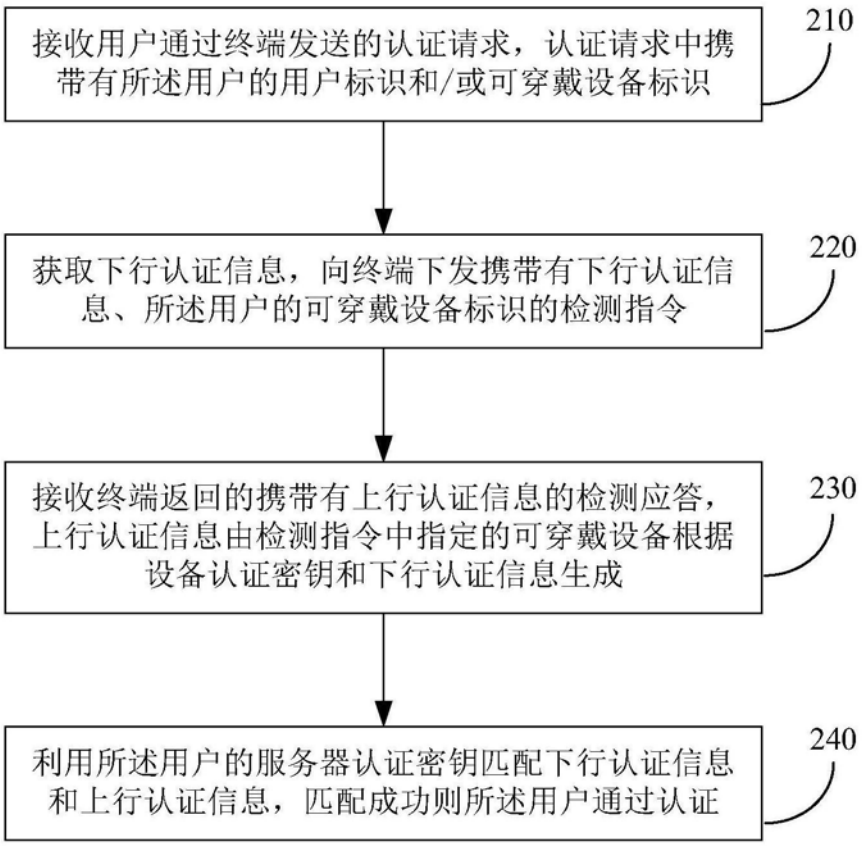

接收用户通过终端发送的认证请求，认证请求中携带有所述用户的用户标识和/或可穿戴设备标识
210
获取下行认证信息，向终端下发携带有下行认证信息、所述用户的可穿戴设备标识的检测指令
220
接收终端返回的携带有上行认证信息的检测应答，上行认证信息由检测指令中指定的可穿戴设备根据设备认证密钥和下行认证信息生成
230
利用所述用户的服务器认证密钥匹配下行认证信息和上行认证信息，匹配成功则所述用户通过认证
240

图2

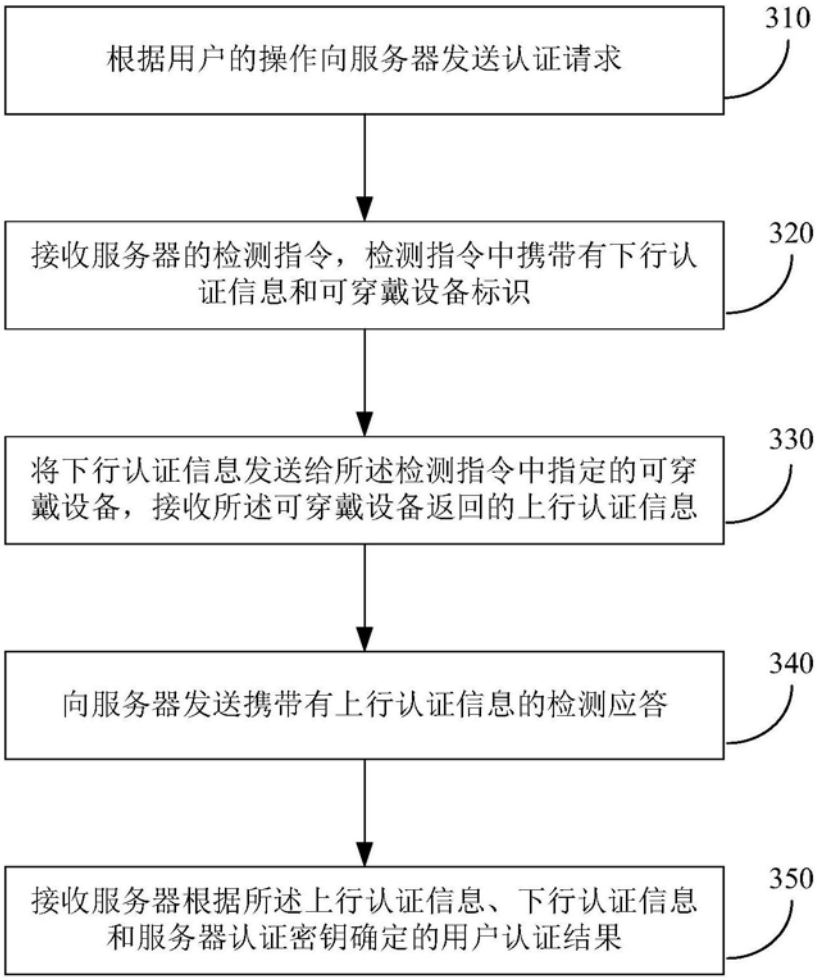

根据用户的操作向服务器发送认证请求
310
接收服务器的检测指令，检测指令中携带有下行认证信息和可穿戴设备标识
320
将下行认证信息发送给所述检测指令中指定的可穿戴设备，接收所述可穿戴设备返回的上行认证信息
330
向服务器发送携带有上行认证信息的检测应答
340
接收服务器根据所述上行认证信息、下行认证信息和服务器认证密钥确定的用户认证结果
350

图3

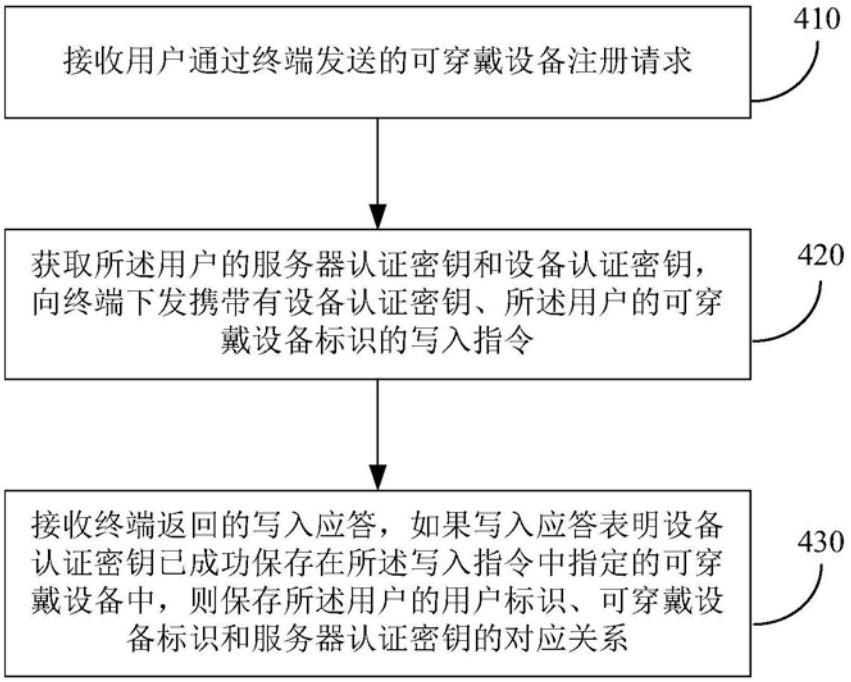

410
接收用户通过终端发送的可穿戴设备注册请求
420
获取所述用户的服务器认证密钥和设备认证密钥，向终端下发携带有设备认证密钥、所述用户的可穿戴设备标识的写入指令
430
接收终端返回的写入应答，如果写入应答表明设备认证密钥已成功保存在所述写入指令中指定的可穿戴设备中，则保存所述用户的用户标识、可穿戴设备标识和服务器认证密钥的对应关系

图4

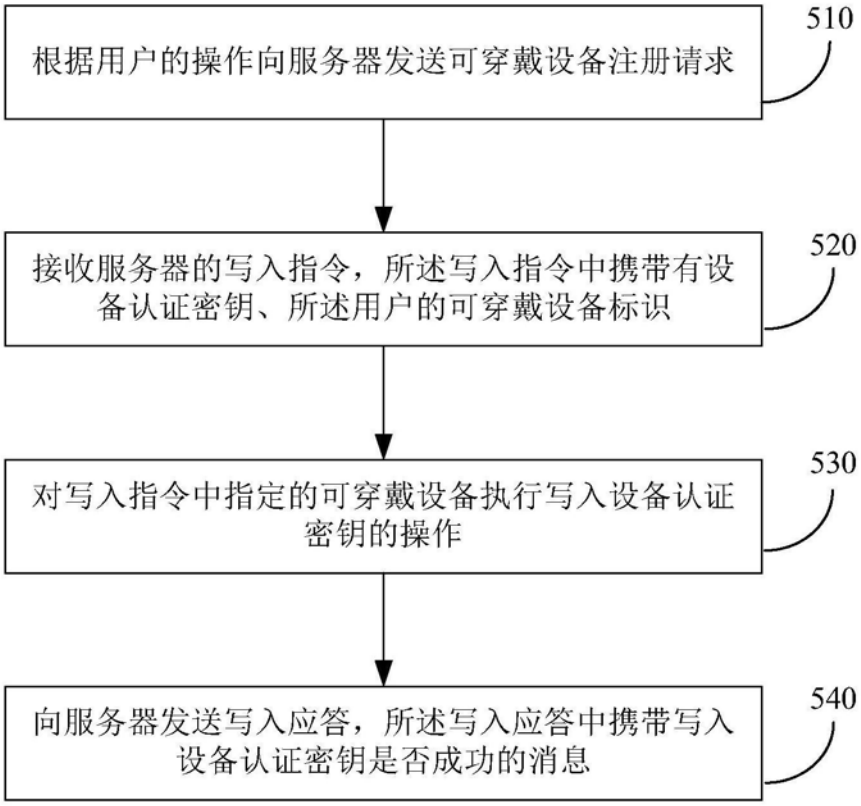

510
根据用户的操作向服务器发送可穿戴设备注册请求
520
接收服务器的写入指令，所述写入指令中携带有设备认证密钥、所述用户的可穿戴设备标识
530
对写入指令中指定的可穿戴设备执行写入设备认证密钥的操作
540
向服务器发送写入应答，所述写入应答中携带写入设备认证密钥是否成功的消息

图5

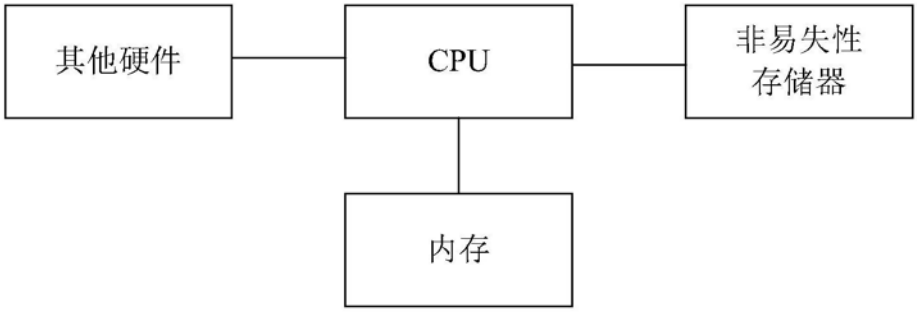


图6

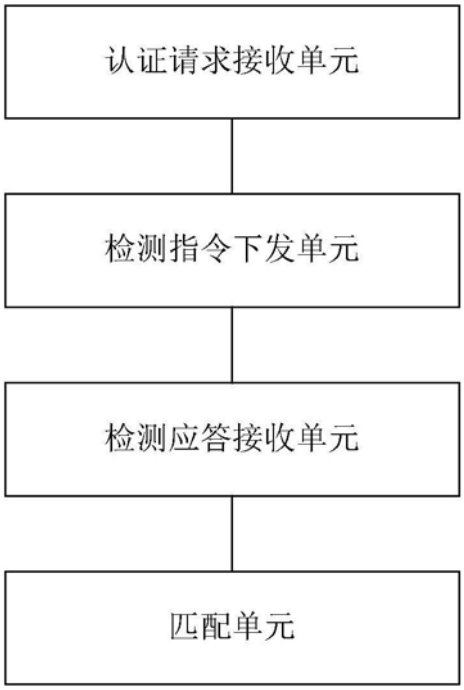


图7

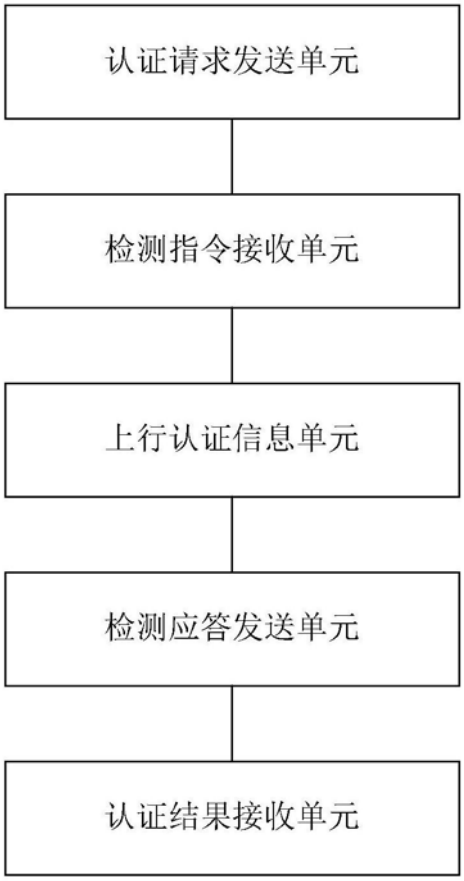

认证请求发送单元
检测指令接收单元
上行认证信息单元
检测应答发送单元
认证结果接收单元

图8


注册请求接收单元
写入指令下发单元
写入应答接收单元

图9

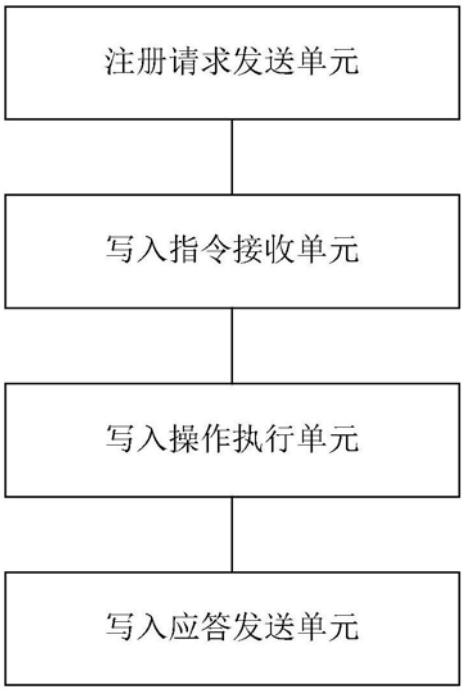


图10