(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 106161354 A
(43)申请公布日 2016.11.23

(21)申请号 201510150292.1

(22)申请日 2015.03.31

(71)申请人 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 皮维

(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)
H04L 9/32(2006.01)

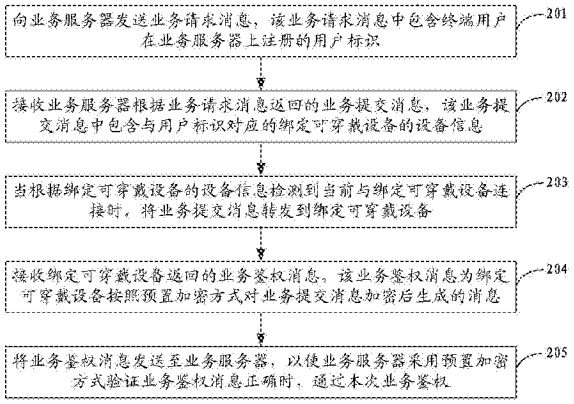
权利要求书7页 说明书14页 附图6页

(54)发明名称

业务鉴权方法、装置、设备及业务服务器

(57)摘要

本申请公开了业务鉴权方法、装置、设备及业务服务器，所述方法包括：当终端设备向业务服务器发送包含终端用户的用户标识的业务请求消息后，业务服务器返回包含与用户标识对应的绑定可穿戴设备的设备信息的业务提交消息，当终端设备检测到与该绑定可穿戴设备连接时，将业务提交消息转发到绑定可穿戴设备，绑定可穿戴设备将按照预置加密方式对业务提交消息加密生成的业务鉴权消息发送到终端设备，当终端设备转发该业务鉴权消息到业务服务器后，由业务服务器采用预置加密方式验证业务鉴权消息正确时，通过本次业务鉴权。本申请实施例采用与终端设备具有绑定关系的可穿戴设备进行业务鉴权，因此简化了业务鉴权操作过程，提高了业务鉴权效率。



CN 106161354 A

1. 一种业务鉴权方法，其特征在于，应用于终端设备，所述方法包括：

向业务服务器发送业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

接收所述业务服务器根据所述业务请求消息返回的业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息；

当根据所述绑定可穿戴设备的设备信息检测到当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

接收所述绑定可穿戴设备返回的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

将所述业务鉴权消息发送至所述业务服务器，以使所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

2. 根据权利要求 1 所述的方法，其特征在于，所述终端设备向业务服务器发送业务请求消息之前，还包括：

当与所述绑定可穿戴设备建立连接时，向所述业务服务器发送绑定请求消息；

接收所述业务服务器根据所述绑定请求消息返回的绑定开通消息，所述绑定开通消息中包含所述用户标识；

将所述绑定开通消息转发给所述绑定可穿戴设备，以使所述绑定可穿戴设备通过不对称加密算法为所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

接收所述绑定可穿戴设备发送的绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息；

将所述绑定应答消息发送至所述业务服务器，以使所述业务服务器保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

3. 根据权利要求 2 所述的方法，其特征在于，所述方法还包括：

将所述终端用户在所述业务服务器上注册的业务校验码发送至所述业务服务器，以使所述业务服务器在验证所述业务校验码正确后，保存所述绑定关系。

4. 根据权利要求 2 所述的方法，其特征在于，

所述绑定应答消息为由所述绑定可穿戴设备添加了第一头信息的消息；

所述将所述绑定应答消息发送至所述业务服务器，包括：当根据所述第一头信息识别出所述绑定应答消息的类型后，将所述绑定应答消息发送至所述业务服务器；

所述将所述业务提交消息转发到所述绑定可穿戴设备，包括：为所述业务提交消息添加第二头信息后，将所述业务提交消息转发到所述绑定可穿戴设备；其中，所述业务鉴权消息为所述绑定可穿戴设备根据所述第二头信息识别所述业务提交消息后，通过所述公钥对所述业务提交消息加密后生成的消息，以使所述业务服务器采用所述私钥验证所述业务鉴权消息是否正确。

5. 根据权利要求 1 至 4 任一所述的方法，其特征在于，所述根据所述绑定可穿戴设备的设备信息检测到当前与所述绑定可穿戴设备连接，包括：

检测是否与待验可穿戴设备连接；

当与待验可穿戴设备连接时，判断所待验可穿戴设备的设备信息是否与所述绑定可穿戴设备的设备信息一致，当一致时，确定所述待验可穿戴设备为所述绑定可穿戴设备。

6. 一种业务鉴权方法，其特征在于，应用于业务服务器，所述方法包括：

接收终端设备发送的业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

根据所述业务请求消息向所述终端设备返回业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息，以使所述终端设备在根据所述绑定可穿戴设备的设备信息确定当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

接收所述终端设备发送的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

7. 根据权利要求 6 所述的方法，其特征在于，所述接收终端设备发送的业务请求消息之前，还包括：

接收所述终端设备发送的绑定请求消息；

根据所述绑定请求消息向所述终端设备返回绑定开通消息，所述绑定开通消息中包含所述用户标识，以使所述终端设备将所述绑定开通消息转发给已建立连接的绑定可穿戴设备后，由所述绑定可穿戴设备通过不对称加密算法为所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

接收所述终端设备发送的绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息；

保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

8. 根据权利要求 7 所述的方法，其特征在于，保存所述绑定关系之前，所述方法还包括：

接收所述终端设备发送的业务校验码，所述业务校验码为所述终端用户在所述业务服务器上注册的校验码；

当验证所述业务校验码与预先保存的所述终端用户的业务校验码一致时，执行保存所述绑定关系。

9. 根据权利要求 6 至 8 任一所述的方法，其特征在于，所述根据所述业务请求消息向所述终端设备返回业务提交消息后，还包括：

接收所述终端设备发送的用户信息，所述用户信息为所述绑定可穿戴设备在接收到所述业务提交消息后，采集的所述终端用户的用户信息；

将所述用户信息呈现在所述本次业务鉴权的业务界面。

10. 一种业务鉴权方法，其特征在于，应用于与终端设备具有绑定关系的绑定可穿戴设备，所述方法包括：

接收终端设备转发的业务提交消息，所述业务提交消息为业务服务器接收到业务请求消息后，向所述终端设备返回的消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识，所述业务提交消息中包含与所述用户标识对应的所述绑定可穿戴设

备的设备信息；

按照预置加密方式对所述业务提交消息进行加密生成业务鉴权消息；

将所述业务鉴权消息发送至所述终端设备，以使所述终端设备将所述业务鉴权消息发送至所述业务服务器后，由所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

11. 根据权利要求 10 所述的方法，其特征在于，所述接收终端设备转发的业务提交消息前，还包括：

接收所述终端设备转发的绑定开通消息，所述绑定开通消息为所述业务服务器接收到绑定请求消息后，向所述终端设备返回的消息，所述绑定开通消息中包含所述用户标识；

通过不对称加密算法为所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

向所述终端设备发送绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息，以使所述终端设备将所述绑定应答消息发送至所述业务服务器后，由所述业务服务器保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

12. 根据权利要求 10 或 11 所述的方法，其特征在于，所述方法还包括：

在接收到所述业务提交消息后，采集所述终端用户的用户信息；

将所述用户信息发送至所述终端设备，以使所述终端设备将所述用户信息转发到所述业务服务器。

13. 根据权利要求 12 所述的方法，其特征在于，所述可穿戴设备包括：低功耗蓝牙 BLE 设备；

所述用户信息包括至少一种下述信息：地理位置信息、用户健康信息。

14. 一种业务鉴权装置，其特征在于，应用于终端设备，所述装置包括：

发送单元，用于向业务服务器发送业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

接收单元，用于接收所述业务服务器根据所述业务请求消息返回的业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息；

检测单元，用于根据所述绑定可穿戴设备的设备信息检测当前是否与所述绑定可穿戴设备连接；

所述发送单元，还用于在检测到与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

所述接收单元，还用于接收所述绑定可穿戴设备返回的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

所述发送单元，还用于将所述业务鉴权消息发送至所述业务服务器，以使所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

15. 根据权利要求 14 所述的装置，其特征在于，

所述发送单元，还用于在发送所述业务请求消息之前，当与所述绑定可穿戴设备建立连接时，向所述业务服务器发送绑定请求消息；

所述接收单元，还用于接收所述业务服务器根据所述绑定请求消息返回的绑定开通消

息，所述绑定开通消息中包含所述用户标识；

所述发送单元，还用于将所述绑定开通消息转发给所述绑定可穿戴设备，以使所述绑定可穿戴设备通过不对称加密算法为所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

所述接收单元，还用于接收所述绑定可穿戴设备发送的绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息；

所述发送单元，还用于将所述绑定应答消息发送至所述业务服务器，以使所述业务服务器保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

16. 根据权利要求 15 所述的装置，其特征在于，

所述发送单元，还用于将所述终端用户在所述业务服务器上注册的业务校验码发送至所述业务服务器，以使所述业务服务器在验证所述业务校验码正确后，保存所述绑定关系。

17. 根据权利要求 15 所述的装置，其特征在于，所述绑定应答消息为由所述绑定可穿戴设备添加了第一头信息的消息；

所述发送单元，具体用于当根据所述第一头信息识别出所述绑定应答消息的类型后，将所述绑定应答消息发送至所述业务服务器；以及，

所述发送单元，具体用于为所述业务提交消息添加第二头信息后，将所述业务提交消息转发到所述绑定可穿戴设备；其中，所述业务鉴权消息为所述绑定可穿戴设备根据所述第二头信息识别所述业务提交消息后，通过所述公钥对所述业务提交消息加密后生成的消息，以使所述业务服务器采用所述私钥验证所述业务鉴权消息是否正确。

18. 根据权利要求 14 至 17 任一所述的装置，其特征在于，所述检测单元包括：

连接检测子单元，用于检测是否与待验可穿戴设备连接；

连接确定子单元，用于当与待验可穿戴设备连接时，判断所待验可穿戴设备的设备信息是否与所述绑定可穿戴设备的设备信息一致，当一致时，确定所述待验可穿戴设备为所述绑定可穿戴设备。

19. 一种业务鉴权装置，其特征在于，应用于业务服务器上，所述装置包括：

接收单元，用于接收终端设备发送的业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

发送单元，用于根据所述业务请求消息向所述终端设备返回业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息，以使所述终端设备在根据所述绑定可穿戴设备的设备信息确定当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

所述接收单元，还用于接收所述终端设备发送的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

验证单元，用于采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

20. 根据权利要求 19 所述的装置，其特征在于，

所述接收单元，还用于接收终端设备发送的业务请求消息之前，接收所述终端设备发送的绑定请求消息；

所述发送单元，还用于根据所述绑定请求消息向所述终端设备返回绑定开通消息，所述绑定开通消息中包含所述用户标识，以使所述终端设备将所述绑定开通消息转发给已建立连接的绑定可穿戴设备后，由所述绑定可穿戴设备通过不对称加密算法为所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

所述接收单元，还用于接收所述终端设备发送的绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息；

所述装置还包括：

保存单元，用于保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

21. 根据权利要求 20 所述的装置，其特征在于，

所述接收单元，还用于接收所述终端设备发送的业务校验码，所述业务校验码为所述终端用户在所述业务服务器上注册的校验码；

所述验证单元，还用于当验证所述业务校验码与预先保存的所述终端用户的业务校验码一致时，触发所述保存单元执行保存所述绑定关系。

22. 根据权利要求 19 至 21 任一所述的装置，其特征在于，

所述接收单元，还用于在所述发送单元向所述终端设备返回业务提交消息后，接收所述终端设备发送的用户信息，所述用户信息为所述绑定可穿戴设备在接收到所述业务提交消息后，采集的所述终端用户的用户信息；

所述装置还包括：

呈现单元，用于将所述用户信息呈现在所述本次业务鉴权的业务界面。

23. 一种业务鉴权装置，其特征在于，应用于与终端设备具有绑定关系的绑定可穿戴设备，所述装置包括：

接收单元，用于接收终端设备转发的业务提交消息，所述业务提交消息为业务服务器接收到业务请求消息后，向所述终端设备返回的消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识，所述业务提交消息中包含与所述用户标识对应的所述绑定可穿戴设备的设备信息；

生成单元，用于按照预置加密方式对所述业务提交消息进行加密生成业务鉴权消息；

发送单元，用于将所述业务鉴权消息发送至所述终端设备，以使所述终端设备将所述业务鉴权消息发送至所述业务服务器后，由所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

24. 根据权利要求 23 所述的装置，其特征在于，

所述接收单元，还用于接收终端设备转发的业务提交消息前，接收所述终端设备转发的绑定开通消息，所述绑定开通消息为所述业务服务器接收到绑定请求消息后，向所述终端设备返回的消息，所述绑定开通消息中包含所述用户标识；

所述生成单元，还用于通过不对称加密算法为所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

所述发送单元，还用于向所述终端设备发送绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息，以使所述终端

设备将所述绑定应答消息发送至所述业务服务器后，由所述业务服务器保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

25. 根据权利要求 23 或 24 所述的装置，其特征在于，所述装置还包括：

采集单元，用于在所述接收单元接收到所述业务提交消息后，采集所述终端用户的用户信息；

所述发送单元，还用于将所述用户信息发送至所述终端设备，以使所述终端设备将所述用户信息转发到所述业务服务器。

26. 一种终端设备，其特征在于，包括：处理器；用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为：

向业务服务器发送业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

接收所述业务服务器根据所述业务请求消息返回的业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息；

当根据所述绑定可穿戴设备的设备信息检测到当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

接收所述绑定可穿戴设备返回的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

将所述业务鉴权消息发送至所述业务服务器，以使所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

27. 一种业务服务器，其特征在于，包括：处理器；用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为：

接收终端设备发送的业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

根据所述业务请求消息向所述终端设备返回业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息，以使所述终端设备在根据所述绑定可穿戴设备的设备信息确定当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

接收所述终端设备发送的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

28. 一种可穿戴设备，其特征在于，所述可穿戴设备与终端设备具有绑定关系，包括：

处理器；用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为：

接收终端设备转发的业务提交消息，所述业务提交消息为业务服务器接收到业务请求消息后，向所述终端设备返回的消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识，所述业务提交消息中包含与所述用户标识对应的所述绑定可穿戴设

备的设备信息；

按照预置加密方式对所述业务提交消息进行加密生成业务鉴权消息；

将所述业务鉴权消息发送至所述终端设备，以使所述终端设备将所述业务鉴权消息发送至所述业务服务器后，由所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

业务鉴权方法、装置、设备及业务服务器

技术领域

[0001] 本申请涉及网络通信技术领域，尤其涉及业务鉴权方法、装置、设备及业务服务器。

背景技术

[0002] 随着智能终端的发展和网络应用的普及，用户可以通过终端上安装的各种应用客户端实现各种业务操作，例如，社交类即时通信业务，购物支付类业务等。在实现上述业务过程中，往往需要进行业务鉴权，即设置多重安全验证方式对用户身份进行校验，从而保证业务的安全性，例如，多重安全验证方式包括登录密码、业务校验密码及短信校验码等多重校验方式的组合。但是，由于上述多重安全校验方式需要用户输入多个密码，因此导致业务鉴权过程繁琐，用户体验较差。

发明内容

[0003] 本申请提供业务鉴权方法、装置、设备及业务服务器，以解决现有业务鉴权过程繁琐的问题。

[0004] 根据本申请实施例的第一方面，提供一种业务鉴权方法，应用于终端设备，所述方法包括：

[0005] 向业务服务器发送业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

[0006] 接收所述业务服务器根据所述业务请求消息返回的业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息；

[0007] 当根据所述绑定可穿戴设备的设备信息检测到当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

[0008] 接收所述绑定可穿戴设备返回的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

[0009] 将所述业务鉴权消息发送至所述业务服务器，以使所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0010] 根据本申请实施例的第二方面，提供另一种业务鉴权方法，应用于业务服务器，所述方法包括：

[0011] 接收终端设备发送的业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

[0012] 根据所述业务请求消息向所述终端设备返回业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息，以使所述终端设备在根据所述绑定可穿戴设备的设备信息确定当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

[0013] 接收所述终端设备发送的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设

备按照预置加密方式对所述业务提交消息加密后生成的消息；

[0014] 采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0015] 根据本申请实施例的第三方面，提供另一种业务鉴权方法，应用于与终端设备具有绑定关系的绑定可穿戴设备，所述方法包括：

[0016] 接收终端设备转发的业务提交消息，所述业务提交消息为业务服务器接收到业务请求消息后，向所述终端设备返回的消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识，所述业务提交消息中包含与所述用户标识对应的所述绑定可穿戴设备的设备信息；

[0017] 按照预置加密方式对所述业务提交消息进行加密生成业务鉴权消息；

[0018] 将所述业务鉴权消息发送至所述终端设备，以使所述终端设备将所述业务鉴权消息发送至所述业务服务器后，由所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0019] 根据本申请实施例的第四方面，提供一种业务鉴权装置，应用于终端设备，所述装置包括：

[0020] 发送单元，用于向业务服务器发送业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

[0021] 接收单元，用于接收所述业务服务器根据所述业务请求消息返回的业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息；

[0022] 检测单元，用于根据所述绑定可穿戴设备的设备信息检测当前是否与所述绑定可穿戴设备连接；

[0023] 所述发送单元，还用于在检测到与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

[0024] 所述接收单元，还用于接收所述绑定可穿戴设备返回的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

[0025] 所述发送单元，还用于将所述业务鉴权消息发送至所述业务服务器，以使所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0026] 根据本申请实施例的第五方面，提供另一种业务鉴权装置，应用于业务服务器上，所述装置包括：

[0027] 接收单元，用于接收终端设备发送的业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

[0028] 发送单元，用于根据所述业务请求消息向所述终端设备返回业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息，以使所述终端设备在根据所述绑定可穿戴设备的设备信息确定当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

[0029] 所述接收单元，还用于接收所述终端设备发送的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

[0030] 验证单元，用于采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0031] 根据本申请实施例的第六方面，提供另一种业务鉴权装置，应用于与终端设备具有绑定关系的绑定可穿戴设备，所述装置包括：

[0032] 接收单元，用于接收终端设备转发的业务提交消息，所述业务提交消息为业务服务器接收到业务请求消息后，向所述终端设备返回的消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识，所述业务提交消息中包含与所述用户标识对应的所述绑定可穿戴设备的设备信息；

[0033] 生成单元，用于按照预置加密方式对所述业务提交消息进行加密生成业务鉴权消息；

[0034] 发送单元，用于将所述业务鉴权消息发送至所述终端设备，以使所述终端设备将所述业务鉴权消息发送至所述业务服务器后，由所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0035] 根据本申请实施例的第七方面，提供一种终端设备，包括：处理器；用于存储所述处理器可执行指令的存储器；

[0036] 其中，所述处理器被配置为：

[0037] 向业务服务器发送业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

[0038] 接收所述业务服务器根据所述业务请求消息返回的业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息；

[0039] 当根据所述绑定可穿戴设备的设备信息检测到当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

[0040] 接收所述绑定可穿戴设备返回的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

[0041] 将所述业务鉴权消息发送至所述业务服务器，以使所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0042] 根据本申请实施例的第八方面，提供一种业务服务器，包括：处理器；用于存储所述处理器可执行指令的存储器；

[0043] 其中，所述处理器被配置为：

[0044] 接收终端设备发送的业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

[0045] 根据所述业务请求消息向所述终端设备返回业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息，以使所述终端设备在根据所述绑定可穿戴设备的设备信息确定当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

[0046] 接收所述终端设备发送的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

[0047] 采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0048] 根据本申请实施例的第九方面，提供一种可穿戴设备，所述可穿戴设备与终端设备具有绑定关系，包括：

[0049] 处理器；用于存储所述处理器可执行指令的存储器；

[0050] 其中，所述处理器被配置为：

[0051] 接收终端设备转发的业务提交消息，所述业务提交消息为业务服务器接收到业务请求消息后，向所述终端设备返回的消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识，所述业务提交消息中包含与所述用户标识对应的所述绑定可穿戴设备的设备信息；

[0052] 按照预置加密方式对所述业务提交消息进行加密生成业务鉴权消息；

[0053] 将所述业务鉴权消息发送至所述终端设备，以使所述终端设备将所述业务鉴权消息发送至所述业务服务器后，由所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0054] 本申请实施例采用与终端设备具有绑定关系的可穿戴设备进行业务鉴权，由于整个业务鉴权过程中终端设备只需要传输可穿戴设备与业务服务器之间的鉴权信息，而不需要终端用户在终端设备上执行输入密码类的操作，因此简化了业务鉴权操作，提高了业务鉴权效率，增强了终端用户在业务操作过程中的用户体验。

[0055] 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，并不能限制本申请。

附图说明

[0056] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并与说明书一起用于解释本申请的原理。

[0057] 图 1 是本申请业务鉴权实施例的应用场景示意图；

[0058] 图 2A 是本申请业务鉴权方法的一个实施例流程图；

[0059] 图 2B 是本申请业务鉴权方法的另一个实施例流程图；

[0060] 图 2C 是本申请业务鉴权方法的另一个实施例流程图；

[0061] 图 3A 是本申请业务鉴权方法的另一个实施例流程图；

[0062] 图 3B 是本申请业务鉴权方法的另一个实施例流程图；

[0063] 图 4 是本申请业务鉴权装置所在设备的一种硬件结构图；

[0064] 图 5 是本申请业务鉴权装置的一个实施例框图；

[0065] 图 6 是本申请业务鉴权装置的另一个实施例框图；

[0066] 图 7 是本申请业务鉴权装置的另一个实施例框图。

具体实施方式

[0067] 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。以下示例性实施例中所描述的实施方式并不代表与本申请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、本申请的一些方面相一致的装置和方法的例子。

[0068] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请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 / 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。

[0069] 应当理解，尽管在本申请可能采用术语第一、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，在不脱离本申请范围的情况下，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……时”或“当……时”或“响应于确定”。

[0070] 参见图 1，是本申请业务鉴权实施例的应用场景示意图：

[0071] 图 1 中，业务服务器可以由第三方业务平台运营商进行设置，通过该业务服务器可以对注册用户提供各种业务应用，为了保证业务应用的安全性，可以在提供业务应用之前对业务进行业务鉴权。假设图 1 中示出的终端用户为业务服务器的注册用户，该终端用户同时持终端设备和可穿戴设备，其中，终端设备可以通过短距离通信方式，例如蓝牙方式与可穿戴设备连接，同时终端设备可以通过有线或无线网络与业务服务器连接。本申请实施例中的终端设备可以具体指手机、平板电脑等，当然，也不排除在 PC(Personal Computer，个人计算机）上的应用；可穿戴设备可以具体指各种 BLE(Bluetooth Low Energy，低功耗蓝牙）设备，例如，智能手环、智能手表等。

[0072] 在传统的业务鉴权场景中，终端用户通过终端设备与业务服务器之间进行交互完成业务鉴权，交互过程中往往会包括输入注册密码、业务密码、短信校验码等繁琐操作，因此业务鉴权过程效率不高；随着可穿戴设备的普及，越来越多的终端用户选择将可穿戴设备与终端设备进行配对连接，从而通过可穿戴设备完成各种附加功能，例如为终端设备解锁，采集终端用户的健康数据等，因此本申请实施例将可穿戴设备应用于业务鉴权过程。如图 1 中，可以由业务服务器预先保存用户标识和可穿戴设备的设备信息的绑定关系，在业务鉴权过程中，当可穿戴设备与终端设备连接时，终端设备通过将可穿戴设备生成的鉴权信息传输到业务服务器，由业务服务器根据预先保存的保定的绑定关系完成业务鉴权。由于整个业务鉴权过程中终端设备只需要传输可穿戴设备与业务服务器之间的鉴权信息，而不需要终端用户在终端设备上执行输入密码类的操作，因此简化了业务鉴权操作，提高了业务鉴权效率，增强了终端用户在业务操作过程中的用户体验。下面将结合附图 1 对本申请实施例进行详细描述。

[0073] 参见图 2A，是本申请业务鉴权方法的一个实施例流程图，该实施例应用在终端设备侧，包括以下步骤：

[0074] 步骤 201：向业务服务器发送业务请求消息，该业务请求消息中包含终端用户在业务服务器上注册的用户标识。

[0075] 本申请实施例中的业务鉴权主要指终端用户通过终端设备上安装的业务 APP(Application，应用）请求完成某种业务操作之前，对业务操作的安全性进行验证的过程。其中，业务操作主要指业务服务器向终端用户提供的各种应用功能，例如，第三方支付服务器向用户提供的对网购物品进行支付操作的支付功能，或者即时通信服务器向用户提供的对网络存储空间内的多媒体文件进行下载操作的下载功能等。

[0076] 为了完成各种业务操作，终端用户可以预先在业务服务器上注册业务账户，从而在基于业务账户登录业务服务器后，进行业务操作。业务账户是可以由业务服务器唯一识别终端用户的信息，其通常包含账户名和账户密码，进一步还可以包含业务密码，其中，账户名中包含的信息可以作为终端用户的用户标识，例如，账户名为 user1@ABC.com，则

“user1”可以作为用户标识。

[0077] 本申请实施例中，终端用户同时持有终端设备和可穿戴设备，该终端设备主要指各种具有网络连接功能的设备，例如，智能手机，平板电脑等，可穿戴设备主要指各种 BLE 设备，例如，智能手环、智能手表等。其中，对应于 BLE 设备，终端设备也同时具有蓝牙功能，当 BLE 设备在与终端设备完成配对后，可以通过蓝牙方式长期连接到该终端设备上，并在连接状态下，向终端设备传输小数据量的信息。因此本实施例可以利用可穿戴设备的上述特性，在业务操作过程中，由业务服务器通过可穿戴设备传输的鉴权信息完成业务鉴权过程。本实施例在实现业务鉴权前，可以先将上述终端设备和可穿戴设备进行绑定，由于每个终端设备可能绑定多个可穿戴设备，因此本申请实施例中将用于业务鉴权的可穿戴设备称为绑定可穿戴设备。

[0078] 其中，在绑定开通阶段，当终端设备与绑定可穿戴设备建立连接时，可以获取对方的设备信息，该设备信息可以包括设备的蓝牙地址和设备标识，设备标识通常可以指设备的 MAC(Media Access Control，介质访问控制层）地址；在终端设备的业务操作界面上，可以向终端用户提供用于进行绑定的选项，当终端用户选择该选项时，可以触发终端设备向业务服务器发送绑定请求消息，业务服务器根据该绑定请求消息，向终端设备返回包含该终端用户的用户标识的绑定开通消息，终端设备将该绑定开通消息转发给所连接的绑定可穿戴设备，绑定可穿戴设备可以通过预置加密方式，例如不对称加密算法，为该用户标识生成公钥和私钥，并向终端设备发送绑定应答消息，该绑定应答消息中可以包含上述私钥和绑定可穿戴设备的设备信息（例如，绑定可穿戴设备的蓝牙地址和设备标识），进一步，还可以包括终端设备的设备信息（例如，终端设备的蓝牙地址和设备标识）；终端设备将上述绑定应答消息发送至业务服务器，业务服务器保存用户标识与上述私钥、绑定可穿戴设备的设备信息、以及终端设备的设备信息之间的绑定关系，以便后续业务服务器基于上述绑定关系进行业务鉴权。可选的，终端设备也可以在发送业务鉴权消息时，同时发送终端用户在业务服务器上注册的业务校验码，相应的，业务服务器可以先验证业务校验码，在该业务校验码正确后，再保存上述绑定关系，以保证绑定开通阶段的安全性。另外，本申请实施例中，终端用户也可以在终端设备的业务界面中解除绑定可穿戴设备与终端设备的绑定关系，例如，终端用户点击解除绑定按钮后，输入注册的业务校验码，当业务服务器验证输入的业务校验码与所保存的业务校验码相同时，从绑定关系列表中删除相应的绑定关系。

[0079] 在业务鉴权阶段，当终端用户在终端设备的业务操作界面上选择执行业务操作时，该终端设备向业务服务器发送业务请求消息，该业务请求消息中可以包含终端用户的用户标识。

[0080] 步骤 202：接收业务服务器根据业务请求消息返回的业务提交消息，该业务提交消息中包含与用户标识对应的绑定可穿戴设备的设备信息。

[0081] 当业务服务器接收到业务请求消息后，可以根据该业务请求消息中携带的用户标识查找预先保存的绑定关系，获得与该用户标识对应的绑定可穿戴设备的设备信息；然后业务服务器向终端设备返回业务提交消息，并在该业务提交消息中携带该绑定可穿戴设备的设备信息。

[0082] 步骤 203：当根据绑定可穿戴设备的设备信息检测到当前与绑定可穿戴设备连接时，将业务提交消息转发到绑定可穿戴设备。

[0083] 当终端设备接收到业务提交消息后，可以检测当前是否与待验可穿戴设备连接，当与待验可穿戴设备连接时，获得该待验可穿戴设备的设备信息，然后判断该待验可穿戴设备的设备信息是否与绑定可穿戴设备的设备信息一致，如果二者一致，则可以确定待验可穿戴设备为绑定可穿戴设备，此时可以将业务提交消息转发到绑定可穿戴设备。

[0084] 步骤 204：接收绑定可穿戴设备返回的业务鉴权消息，该业务鉴权消息为绑定可穿戴设备按照预置加密方式对业务提交消息加密后生成的消息。

[0085] 绑定可穿戴设备接收到业务提交消息后，可以采用预置加密方式对业务提交消息加密后生成业务鉴权消息，并将该业务鉴权消息发送至终端设备。其中，预置加密方式可以指通过在前述绑定开通阶段采用不对称加密算法生成的公钥对业务提交消息进行加密。

[0086] 步骤 205：将业务鉴权消息发送至业务服务器，以使业务服务器采用预置加密方式验证业务鉴权消息正确时，通过本次业务鉴权。

[0087] 终端设备将接收到的业务鉴权消息发送到业务服务器，业务服务器采用预置加密方式验证业务鉴权消息是否正确，其中，预置加密方式可以指通过在前述绑定开通阶段采用不对称加密算法生成的私钥对业务鉴权消息进行解密，结合步骤 202 的描述可知，业务服务器可以在根据用户标识查找预先保存的绑定关系时，获得与该用户标识对应的私钥。当业务服务器验证该业务鉴权消息正确时，确定本次业务鉴权通过，完成本次业务操作过程。

[0088] 可选的，当可穿戴设备在接收到业务提交消息后，还可以采集终端用户的用户信息，例如，地理位置信息、用户健康信息等，并在向终端设备发送业务鉴权消息时，同时发送该用户信息，由终端设备将该用户信息转发到业务服务器，当业务服务器确定本次业务鉴权通过时，可以同时记录上述用户信息，从而对该终端用户在业务操作过程中产生的所有信息进行完整存储，或者，业务服务器也可以将用户信息呈现在本次业务鉴权的业务界面，以丰富终端用户在业务操作过程中的趣味性，例如，当用户信息为用户心率时，可以呈现如下信息“您的心率达到 150，下次别这么紧张哦”，又例如，当用户信息为用户海拔高度时，可以呈现如下信息“您在海拔 6000 米的地方完成本次业务操作，超越了 10000 名用户”。

[0089] 参见图 2B，是本申请业务鉴权方法的另一个实施例流程图，该实施例应用在业务服务器侧，包括以下步骤：

[0090] 步骤 211：接收终端设备发送的业务请求消息，该业务请求消息中包含终端用户在业务服务器上注册的用户标识。

[0091] 步骤 212：根据业务请求消息向终端设备返回业务提交消息，该业务提交消息中包含与用户标识对应的绑定可穿戴设备的设备信息，以使终端设备在根据绑定可穿戴设备的设备信息确定当前与绑定可穿戴设备连接时，将业务提交消息转发到绑定可穿戴设备。

[0092] 步骤 213：接收终端设备发送的业务鉴权消息，该业务鉴权消息为绑定可穿戴设备按照预置加密方式对业务提交消息加密后生成的消息。

[0093] 步骤 214：采用预置加密方式验证业务鉴权消息正确时，通过本次业务鉴权。

[0094] 参见图 2C，是本申请业务鉴权方法的另一个实施例流程图，该实施例应用在可穿戴设备侧，包括以下步骤：

[0095] 步骤 221：接收终端设备转发的业务提交消息，该业务提交消息为业务服务器接收到业务请求消息后，向终端设备返回的消息，该业务请求消息中包含终端用户在业务服

务器上注册的用户标识，该业务提交消息中包含与用户标识对应的绑定可穿戴设备的设备信息。

[0096] 步骤 222：按照预置加密方式对业务提交消息进行加密生成业务鉴权消息。

[0097] 步骤 223：将业务鉴权消息发送至终端设备，以使终端设备将业务鉴权消息发送至业务服务器后，由业务服务器采用预置加密方式验证业务鉴权消息正确时，通过本次业务鉴权。

[0098] 上述图 2B 和图 2C 所示的实施例与图 2A 所示实施例的主要不同在于，执行实施例的主体设备不同，而业务鉴权过程一致，因此业务鉴权的具体过程可参见图 2A 所示实施例的相关描述，在此不再赘述。需要说明的是，采用本申请实施例实现业务鉴权时，也可以兼容现有的业务鉴权方式，即在终端用户未选择将绑定可穿戴设备用于业务鉴权时，仍然可以采用现有的密码输入方式等实现业务鉴权，对此本申请实施例不进行限制。

[0099] 由上述图 2A 至图 2C 所示的实施例可见，这些实施例采用与终端设备具有绑定关系的可穿戴设备进行业务鉴权，由于整个业务鉴权过程中终端设备只需要传输可穿戴设备与业务服务器之间的鉴权信息，而不需要终端用户在终端设备上执行输入密码类的操作，因此简化了业务鉴权操作，提高了业务鉴权效率，增强了终端用户在业务操作过程中的用户体验。

[0100] 参见图 3A，是本申请业务鉴权方法的另一个实施例流程图，该实施例结合图 1 示出的应用场景，通过绑定可穿戴设备 (BLE 设备)、终端设备和业务服务器之间的交互，详细描述了绑定开通过程，包括以下步骤：

[0101] 步骤 301：终端设备与 BLE 设备建立蓝牙连接。

[0102] 本实施例中，假设终端用户已在业务服务器上注册业务账户，其中假设注册的用户 ID(Identification，标识) 为“USER”，业务校验码为“abcdef”。业务服务器可以在数据库中保存注册的用户 ID 与业务校验码之间的对应关系，其中，可以直接保存该用户 ID “USER”，也可以由业务服务器生成具有固定长度且唯一的数字作为用户 ID，对此本申请实施例不进行限制。

[0103] 当终端设备与 BLE 设备建立蓝牙连接后，终端设备可以记录 BLE 设备的设备信息，包括 BLE 设备的蓝牙地址和 BLE 设备 ID，同时 BLE 设备可以记录终端设备的设备信息，包括终端设备的蓝牙地址和终端设备 ID。

[0104] 步骤 302：终端设备向业务服务器发送请求与 BLE 设备进行绑定的绑定请求消息。

[0105] 在终端用户通过所注册的业务账户登录业务服务器后，如果终端用户在终端设备呈现的业务界面上选择了绑定选项，例如，点击绑定按钮，则终端设备向业务服务器发送绑定请求消息。

[0106] 步骤 303：业务服务器根据绑定请求消息向终端设备返回绑定开通消息。

[0107] 本步骤中，该绑定开通消息中可以包含终端用户的用户 ID 和第一防重放信息 (challenge)，该第一 challenge 可以用于标识该绑定请求消息的唯一性。

[0108] 步骤 304：终端设备对该绑定开通消息进行加密获得加密绑定开通消息。

[0109] 本步骤中，终端设备可以为绑定开通消息添加头信息，该头信息用于表示该绑定开通消息的类型，为了保证与 BLE 设备之间消息传输的安全性，终端设备可以进一步采用预先与 BLE 设备协商的对称加密算法对绑定开通消息进行加密。

[0110] 步骤 305 :终端设备通过建立的蓝牙连接将加密绑定开通消息发送至 BLE 设备。

[0111] 步骤 306 :BLE 设备对加密绑定开通消息进行解密,获得绑定开通消息。

[0112] BLE 设备接收到加密绑定开通消息后,对应于步骤 304 的描述,该 BLE 设备可以通过预先与终端设备协商的对称加密算法对加密绑定开通消息进行解密,并根据头信息识别出消息类型后,确定接收到绑定开通消息,此时 BLE 设备可以获得绑定开通消息中携带的用户 ID。

[0113] 步骤 307 :BLE 设备为绑定开通消息生成绑定应答消息。

[0114] 本步骤中,BLE 设备通过不对称加密算法为该用户 ID 生成公钥和私钥,并保存用户 ID 与公钥的对应关系,然后在生成的绑定应答消息中携带私钥、BLE 设备的设备信息和终端设备的设备信息。

[0115] 步骤 308 :BLE 设备对该绑定应答消息进行加密获得加密绑定应答消息。

[0116] 本步骤中,BLE 设备可以对绑定应答消息添加头信息,该头信息用于表示该绑定应答消息的类型,然后仍然采用预先与终端设备协商的对称加密算法对绑定应答消息进行加密。

[0117] 步骤 309 :BLE 设备通过建立的蓝牙连接将加密绑定应答消息发送至终端设备。

[0118] 步骤 310 :终端设备对加密绑定应答消息进行解密,获得绑定应答消息。

[0119] 终端设备接收到加密绑定应答消息后,对应于步骤 308 的描述,该终端设备可以通过预先与 BLE 设备协商的对称加密算法对加密绑定应答消息进行解密,并根据头信息识别出消息类型后,确定接收到绑定应答消息,并在该绑定应答消息中携带第一 challenge,以使业务服务器通过该第一 challenge 识别该绑定应答消息对应于步骤 303 中的绑定开通消息。

[0120] 步骤 311 :终端设备将业务校验密码和绑定应答消息传输给业务服务器。

[0121] 步骤 312 :业务服务器验证该业务校验码有效后,保存终端用户与 BLE 设备之间的绑定关系。

[0122] 本步骤中,业务服务器可以根据用户 ID 查找终端用户的注册信息,获得终端用户注册的业务校验码为“abcdef”,比较接收到的业务校验码与“abcdef”相同时,在绑定关系列表中保存用户 ID “USER”与绑定应答消息中携带的私钥、BLE 设备的设备信息、以及终端设备的设备信息之间的绑定关系。

[0123] 参见图 3B,是本申请业务鉴权方法的另一个实施例流程图,该实施例结合图 1 示出的应用场景,在图 3A 所示实施例的基础上,通过绑定可穿戴设备 (BLE 设备)、终端设备和业务服务器之间的交互,详细描述了业务鉴权过程,包括以下步骤 :

[0124] 步骤 321 :终端设备向业务服务器发送业务请求消息,该业务请求消息中包含用户 ID。

[0125] 当终端用户在终端设备的业务界面上进行业务操作时,例如,进行支付操作,则终端设备向业务服务器发送包含用户 ID 的业务请求消息。

[0126] 步骤 322 :业务服务器根据业务请求消息中的用户 ID 查找绑定关系,获得与该用户 ID 对应的绑定信息。

[0127] 结合图 3A 所示实施例可知,当业务服务器根据用户 ID 查找绑定关系列表时,可以获得与该用户 ID 对应的私钥、BLE 设备的设备信息和终端设备的设备信息。

[0128] 步骤 323 :业务服务器向终端设备发送业务提交消息。

[0129] 本步骤中,业务服务器可以生成包含 BLE 设备的设备信息 (BLE 设备的蓝牙地址和 BLE 设备 ID) 和第二防重放信息 (challenge) 的业务提交消息,该第二 challenge 可以用于标识该业务提交消息的唯一性。

[0130] 步骤 324 :终端设备根据 BLE 设备的设备信息验证当前与该 BLE 设备连接。

[0131] 本步骤中,终端设备可以根据 BLE 设备的蓝牙地址验证当前与对应的 BLE 设备连接,且该 BLE 设备的 BLE 设备 ID 与绑定开通阶段记录的 BLE 设备 ID 一致时,确定当前与所绑定开通阶段绑定的 BLE 设备连接。

[0132] 步骤 325 :终端设备对该业务提交消息进行加密获得加密业务提交消息。

[0133] 本步骤中,终端设备可以为业务提交消息添加头信息,该头信息用于表示该业务提交消息的类型,并通过预先与 BLE 设备协商的对称加密算法对该业务提交消息进行加密。

[0134] 步骤 326 :终端设备将加密业务提交消息发送至 BLE 设备。

[0135] 步骤 327 :BLE 设备对加密业务提交消息进行解密,获得业务提交消息。

[0136] BLE 设备接收到加密业务提交消息后,对应于步骤 325 中的描述,该 BLE 设备可以通过预先与终端设备协商的对称加密算法对加密业务提交消息进行解密,并根据头信息识别出消息类型为业务提交消息。

[0137] 步骤 328 :BLE 设备通过绑定开通阶段为用户 ID 生成的公钥对业务提交消息进行加密获得业务鉴权消息。

[0138] 本步骤中,BLE 设备可以查找与用户 ID 对应的公钥,然后通过该公钥对业务提交消息进行加密,例如,一种加密方式可以具体指 HOTP(HMAC-Based One-Time Password,基于 HMAC 的一次密码) 算法,其中 HMAC(Hash-based Message Authentication Code,哈希运算消息认证码) 指以一个密钥和一个消息为输入,生成一个消息摘要作为输出的加密方式。

[0139] 步骤 329 :BLE 设备对业务鉴权消息进行加密获得加密业务鉴权消息。

[0140] 本步骤中,BLE 设备仍然采用预先与终端设备协商的对称加密算法对业务鉴权消息进行加密生成加密业务鉴权消息。

[0141] 步骤 330 :BLE 设备将加密业务鉴权消息发送到终端设备。

[0142] 步骤 331 :终端设备对加密业务鉴权消息进行解密,获得业务鉴权消息。

[0143] 对应于步骤 329 的描述,该终端设备可以通过预先与 BLE 设备协商的对称加密算法对加密业务鉴权消息进行解密,获得业务鉴权消息。

[0144] 步骤 332 :终端设备向业务服务器返回业务鉴权消息。

[0145] 本步骤中,终端设备可以在业务鉴权消息中携带第二 challenge,以使业务服务器通过该第二 challenge 识别该业务鉴权消息对应于步骤 323 中的业务提交消息。

[0146] 步骤 333 :业务服务器通过与用户 ID 对应的私钥验证业务鉴权消息正确时,通过本次业务鉴权。

[0147] 本步骤中,业务服务器通过与用户 ID 对应的私钥解密业务鉴权消息,得到 BLE 设备的设备信息,此时业务服务器验证 BLE 设备的设备信息和绑定关系中保存的 BLE 设备的设备信息一致时,确定该业务鉴权消息通过验证。

[0148] 由上述图 3A 和图 3B 所示的实施例可见，该实施例采用与终端设备具有绑定关系的可穿戴设备进行业务鉴权，由于整个业务鉴权过程中终端设备只需要传输可穿戴设备与业务服务器之间的鉴权信息，而不需要终端用户在终端设备上执行输入密码类的操作，因此简化了业务鉴权操作，提高了业务鉴权效率，增强了终端用户在业务操作过程中的用户体验。

[0149] 与前述业务鉴权方法的实施例相对应，本申请还提供了业务鉴权装置的实施例。

[0150] 本申请业务鉴权装置实施例根据业务鉴权装置所具有的不同功能可以应用终端设备、业务服务器、或可穿戴设备上。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，是通过其所在服务器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，如图 4 所示，为本申请业务鉴权装置所在设备的一种硬件结构图，除了图 4 所示的处理器、内存、网络接口、以及非易失性存储器之外，实施例中装置所在的设备通常根据该服务器的实际功能，还可以包括其他硬件，对此不再赘述。

[0151] 参见图 5，为本申请业务鉴权装置的一个实施例框图，该装置应用于终端设备，包括：发送单元 510、接收单元 520 和检测单元 530。

[0152] 其中，发送单元 510，用于向业务服务器发送业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

[0153] 接收单元 520，用于接收所述业务服务器根据所述业务请求消息返回的业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息；

[0154] 检测单元 530，用于根据所述绑定可穿戴设备的设备信息检测当前是否与所述绑定可穿戴设备连接；

[0155] 所述发送单元 510，还用于在检测到与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

[0156] 所述接收单元 520，还用于接收所述绑定可穿戴设备返回的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

[0157] 所述发送单元 510，还用于将所述业务鉴权消息发送至所述业务服务器，以使所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0158] 在一个可选的实现方式中：

[0159] 所述发送单元 510，还可以用于在发送所述业务请求消息之前，当与所述绑定可穿戴设备建立连接时，向所述业务服务器发送绑定请求消息；

[0160] 所述接收单元 520，还可以用于接收所述业务服务器根据所述绑定请求消息返回的绑定开通消息，所述绑定开通消息中包含所述用户标识；

[0161] 所述发送单元 510，还可以用于将所述绑定开通消息转发给所述绑定可穿戴设备，以使所述绑定可穿戴设备通过不对称加密算法为所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

[0162] 所述接收单元 520，还可以用于接收所述绑定可穿戴设备发送的绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息；

[0163] 所述发送单元 510，还可以用于将所述绑定应答消息发送至所述业务服务器，以使所述业务服务器保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

[0164] 在另一个可选的实现方式中：

[0165] 所述发送单元 510，还可以用于将所述终端用户在所述业务服务器上注册的业务校验码发送至所述业务服务器，以使所述业务服务器在验证所述业务校验码正确后，保存所述绑定关系。

[0166] 在另一个可选的实现方式中：

[0167] 所述绑定应答消息为由所述绑定可穿戴设备添加了第一头信息的消息；

[0168] 所述发送单元 510，可以具体用于当根据所述第一头信息识别出所述绑定应答消息的类型后，将所述绑定应答消息发送至所述业务服务器；以及，

[0169] 所述发送单元，具体用于为所述业务提交消息添加第二头信息后，将所述业务提交消息转发到所述绑定可穿戴设备；其中，所述业务鉴权消息为所述绑定可穿戴设备根据所述第二头信息识别所述业务提交消息后，通过所述公钥对所述业务提交消息加密后生成的消息，以使所述业务服务器采用所述私钥验证所述业务鉴权消息是否正确。

[0170] 在另一个可选的实现方式中：

[0171] 所述检测单元 530 可以包括（图 5 中未示出）：

[0172] 连接检测子单元，用于检测是否与待验可穿戴设备连接；

[0173] 连接确定子单元，用于当与待验可穿戴设备连接时，判断所待验可穿戴设备的设备信息是否与所述绑定可穿戴设备的设备信息一致，当一致时，确定所述待验可穿戴设备为所述绑定可穿戴设备。

[0174] 参见图 6，为本申请业务鉴权装置的另一个实施例框图，该装置应用于业务服务器，包括：接收单元 610、发送单元 620 和验证单元 630。

[0175] 其中，接收单元 610，用于接收终端设备发送的业务请求消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识；

[0176] 发送单元 620，用于根据所述业务请求消息向所述终端设备返回业务提交消息，所述业务提交消息中包含与所述用户标识对应的绑定可穿戴设备的设备信息，以使所述终端设备在根据所述绑定可穿戴设备的设备信息确定当前与所述绑定可穿戴设备连接时，将所述业务提交消息转发到所述绑定可穿戴设备；

[0177] 所述接收单元 610，还用于接收所述终端设备发送的业务鉴权消息，所述业务鉴权消息为所述绑定可穿戴设备按照预置加密方式对所述业务提交消息加密后生成的消息；

[0178] 验证单元 630，用于采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0179] 在一个可选的实现方式中：

[0180] 所述接收单元 610，还可以用于接收终端设备发送的业务请求消息之前，接收所述终端设备发送的绑定请求消息；

[0181] 所述发送单元 620，还可以用于根据所述绑定请求消息向所述终端设备返回绑定开通消息，所述绑定开通消息中包含所述用户标识，以使所述终端设备将所述绑定开通消息转发给已建立连接的绑定可穿戴设备后，由所述绑定可穿戴设备通过不对称加密算法为

所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

[0182] 所述接收单元610，还可以用于接收所述终端设备发送的绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息；

[0183] 所述装置还可以包括（图7中未示出）：

[0184] 保存单元，用于保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

[0185] 在另一个可选的实现方式中：

[0186] 所述接收单元610，还可以用于接收所述终端设备发送的业务校验码，所述业务校验码为所述终端用户在所述业务服务器上注册的校验码；

[0187] 所述验证单元630，还可以用于当验证所述业务校验码与预先保存的所述终端用户的业务校验码一致时，触发所述保存单元执行保存所述绑定关系。

[0188] 在另一个可选的实现方式中：

[0189] 所述接收单元610，还可以用于在所述发送单元向所述终端设备返回业务提交消息后，接收所述终端设备发送的用户信息，所述用户信息为所述绑定可穿戴设备在接收到所述业务提交消息后，采集的所述终端用户的用户信息；

[0190] 所述装置还可以包括（图6中未示出）：

[0191] 呈现单元，用于将所述用户信息呈现在所述本次业务鉴权的业务界面。

[0192] 参见图7，为本申请业务鉴权装置的另一个实施例框图，该装置应用于可穿戴设备，包括：接收单元710、生成单元720和发送单元730。

[0193] 其中，接收单元710，用于接收终端设备转发的业务提交消息，所述业务提交消息为业务服务器接收到业务请求消息后，向所述终端设备返回的消息，所述业务请求消息中包含终端用户在所述业务服务器上注册的用户标识，所述业务提交消息中包含与所述用户标识对应的所述绑定可穿戴设备的设备信息；

[0194] 生成单元720，用于按照预置加密方式对所述业务提交消息进行加密生成业务鉴权消息；

[0195] 发送单元730，用于将所述业务鉴权消息发送至所述终端设备，以使所述终端设备将所述业务鉴权消息发送至所述业务服务器后，由所述业务服务器采用所述预置加密方式验证所述业务鉴权消息正确时，通过本次业务鉴权。

[0196] 在一个可选的实现方式中：

[0197] 所述接收单元710，还可以用于接收终端设备转发的业务提交消息前，接收所述终端设备转发的绑定开通消息，所述绑定开通消息为所述业务服务器接收到绑定请求消息后，向所述终端设备返回的消息，所述绑定开通消息中包含所述用户标识；

[0198] 所述生成单元720，还可以用于通过不对称加密算法为所述用户标识生成公钥和私钥，其中，所述公钥用于对所述业务提交消息加密，所述私钥用于验证所述业务鉴权消息是否正确；

[0199] 所述发送单元730，还可以用于向所述终端设备发送绑定应答消息，所述绑定应答消息中包含所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息，以

使所述终端设备将所述绑定应答消息发送至所述业务服务器后，由所述业务服务器保存所述用户标识与所述私钥、所述绑定可穿戴设备的设备信息、以及所述终端设备的设备信息之间的绑定关系。

[0200] 在另一个可选的实现方式中：

[0201] 所述装置还可以包括（图 7 中未示出）：

[0202] 采集单元，用于在所述接收单元接收到所述业务提交消息后，采集所述终端用户的用户信息；

[0203] 所述发送单元 730，还可以用于将所述用户信息发送至所述终端设备，以使所述终端设备将所述用户信息转发到所述业务服务器。

[0204] 上述装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0205] 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申请方案的目的。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。

[0206] 由上述实施例可见，这些实施例采用与终端设备具有绑定关系的可穿戴设备进行业务鉴权，由于整个业务鉴权过程中终端设备只需要传输可穿戴设备与业务服务器之间的鉴权信息，而不需要终端用户在终端设备上执行输入密码类的操作，因此简化了业务鉴权操作，提高了业务鉴权效率，增强了终端用户在业务操作过程中的用户体验。

[0207] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、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申请的一般性原理并包括本申请未公开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，本申请的真正范围和精神由下面的权利要求指出。

[0208] 应当理解的是，本申请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。本申请的范围仅由所附的权利要求来限制。

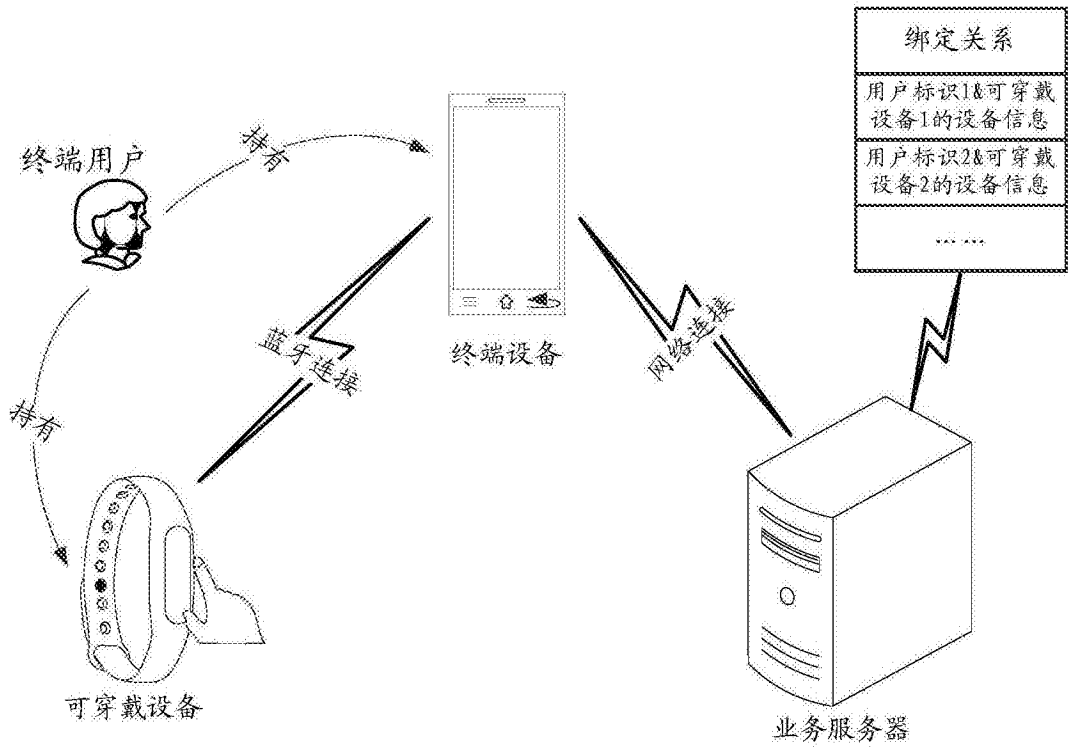

绑定关系
用户标识1&可穿戴设备1的设备信息
用户标识2&可穿戴设备2的设备信息
……
终端用户
持有
蓝牙连接
终端设备
网络连接
持有
可穿戴设备
业务服务器

图 1

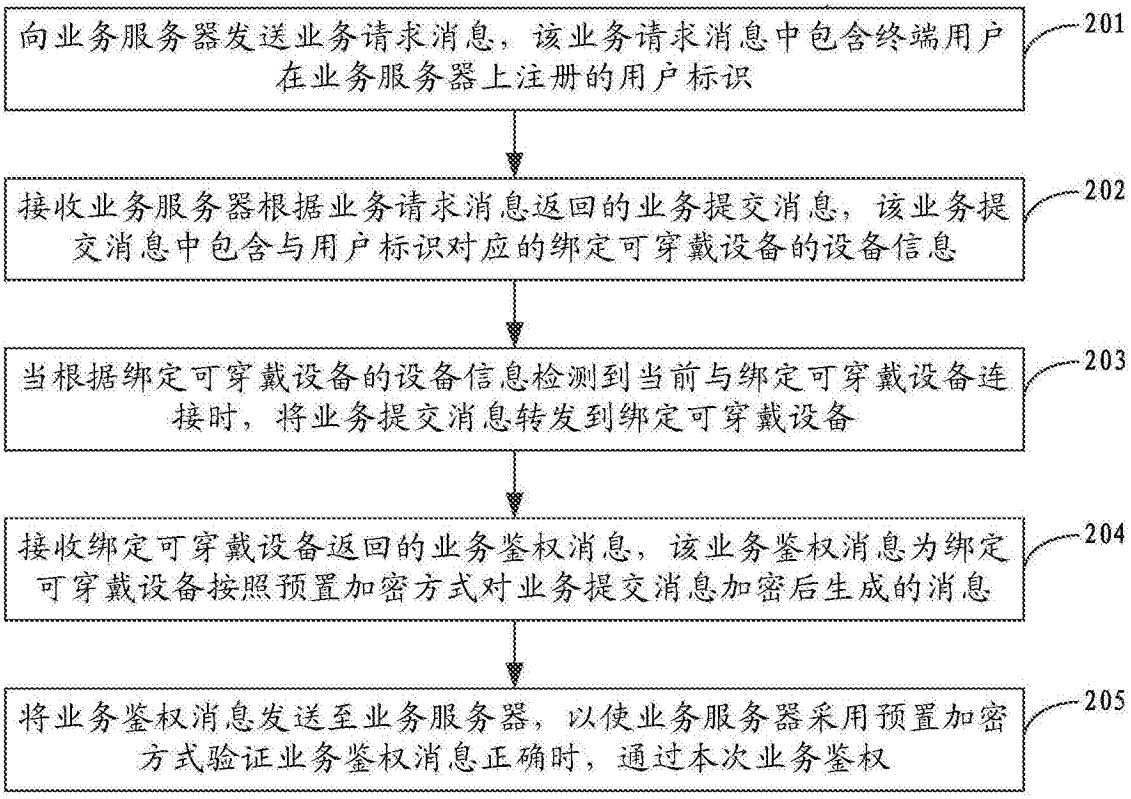

向业务服务器发送业务请求消息，该业务请求消息中包含终端用户在业务服务器上注册的用户标识
201
接收业务服务器根据业务请求消息返回的业务提交消息，该业务提交消息中包含与用户标识对应的绑定可穿戴设备的设备信息
202
当根据绑定可穿戴设备的设备信息检测到当前与绑定可穿戴设备连接时，将业务提交消息转发到绑定可穿戴设备
203
接收绑定可穿戴设备返回的业务鉴权消息，该业务鉴权消息为绑定可穿戴设备按照预置加密方式对业务提交消息加密后生成的消息
204
将业务鉴权消息发送至业务服务器，以使业务服务器采用预置加密方式验证业务鉴权消息正确时，通过本次业务鉴权
205

图 2A

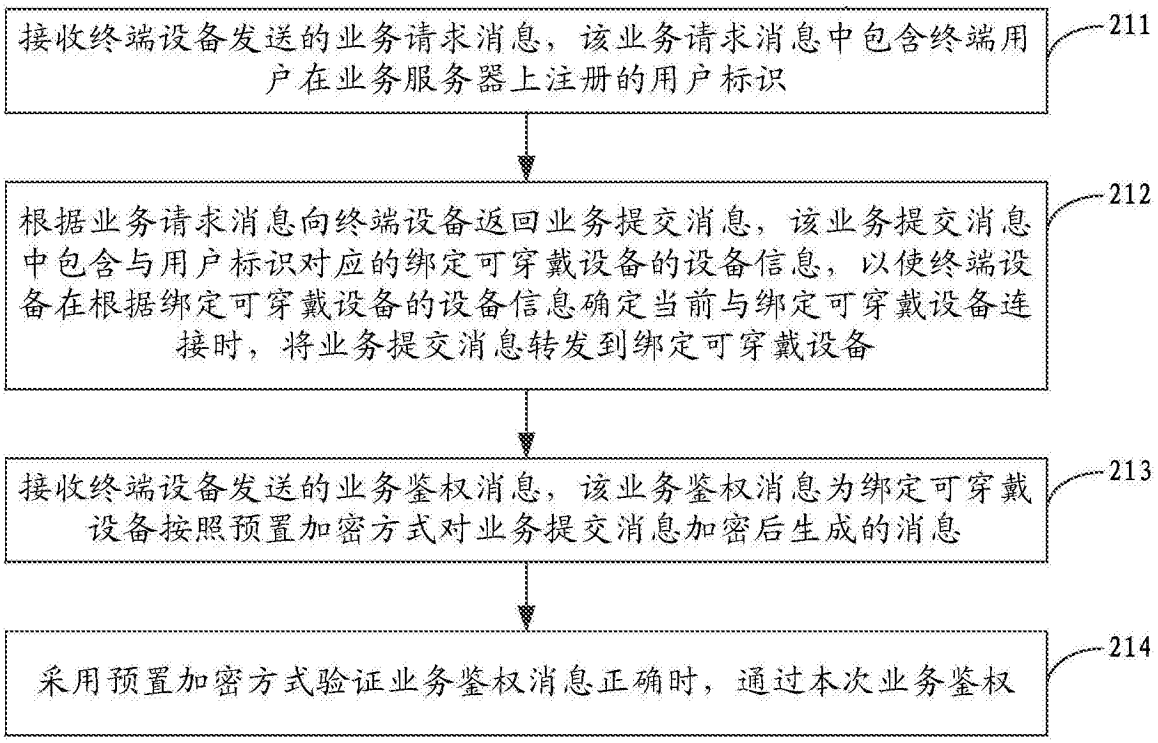

接收终端设备发送的业务请求消息，该业务请求消息中包含终端用户在业务服务器上注册的用户标识
211
根据业务请求消息向终端设备返回业务提交消息，该业务提交消息中包含与用户标识对应的绑定可穿戴设备的设备信息，以使终端设备在根据绑定可穿戴设备的设备信息确定当前与绑定可穿戴设备连接时，将业务提交消息转发到绑定可穿戴设备
212
接收终端设备发送的业务鉴权消息，该业务鉴权消息为绑定可穿戴设备按照预置加密方式对业务提交消息加密后生成的消息
213
采用预置加密方式验证业务鉴权消息正确时，通过本次业务鉴权
214

图 2B

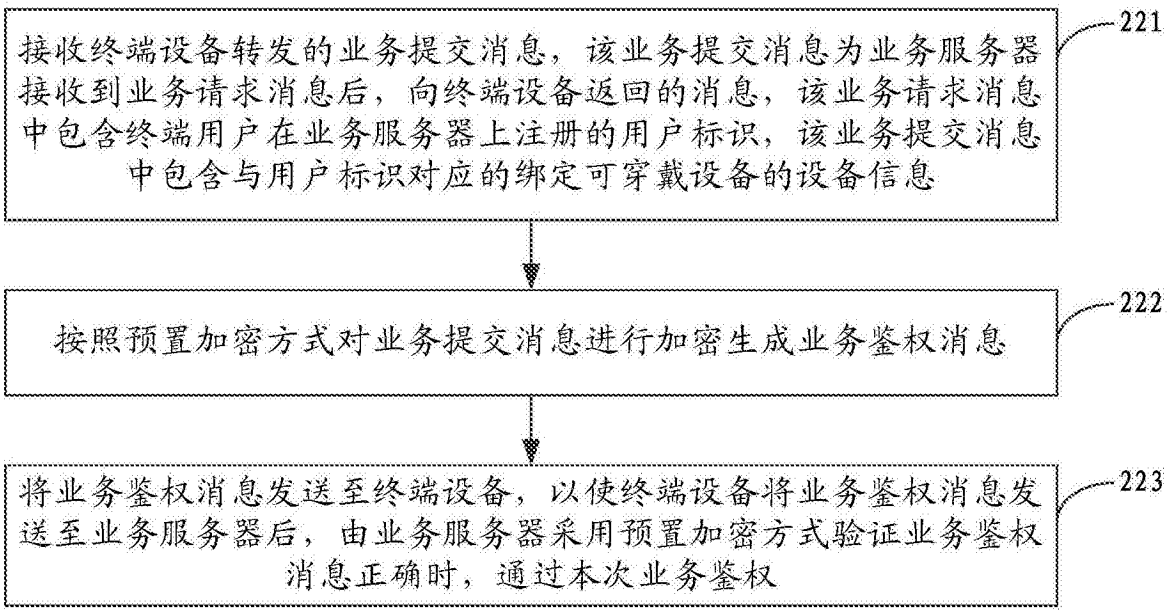

接收终端设备转发的业务提交消息，该业务提交消息为业务服务器接收到业务请求消息后，向终端设备返回的消息，该业务请求消息中包含终端用户在业务服务器上注册的用户标识，该业务提交消息中包含与用户标识对应的绑定可穿戴设备的设备信息
221
按照预置加密方式对业务提交消息进行加密生成业务鉴权消息
222
将业务鉴权消息发送至终端设备，以使终端设备将业务鉴权消息发送至业务服务器后，由业务服务器采用预置加密方式验证业务鉴权消息正确时，通过本次业务鉴权
223

图 2C

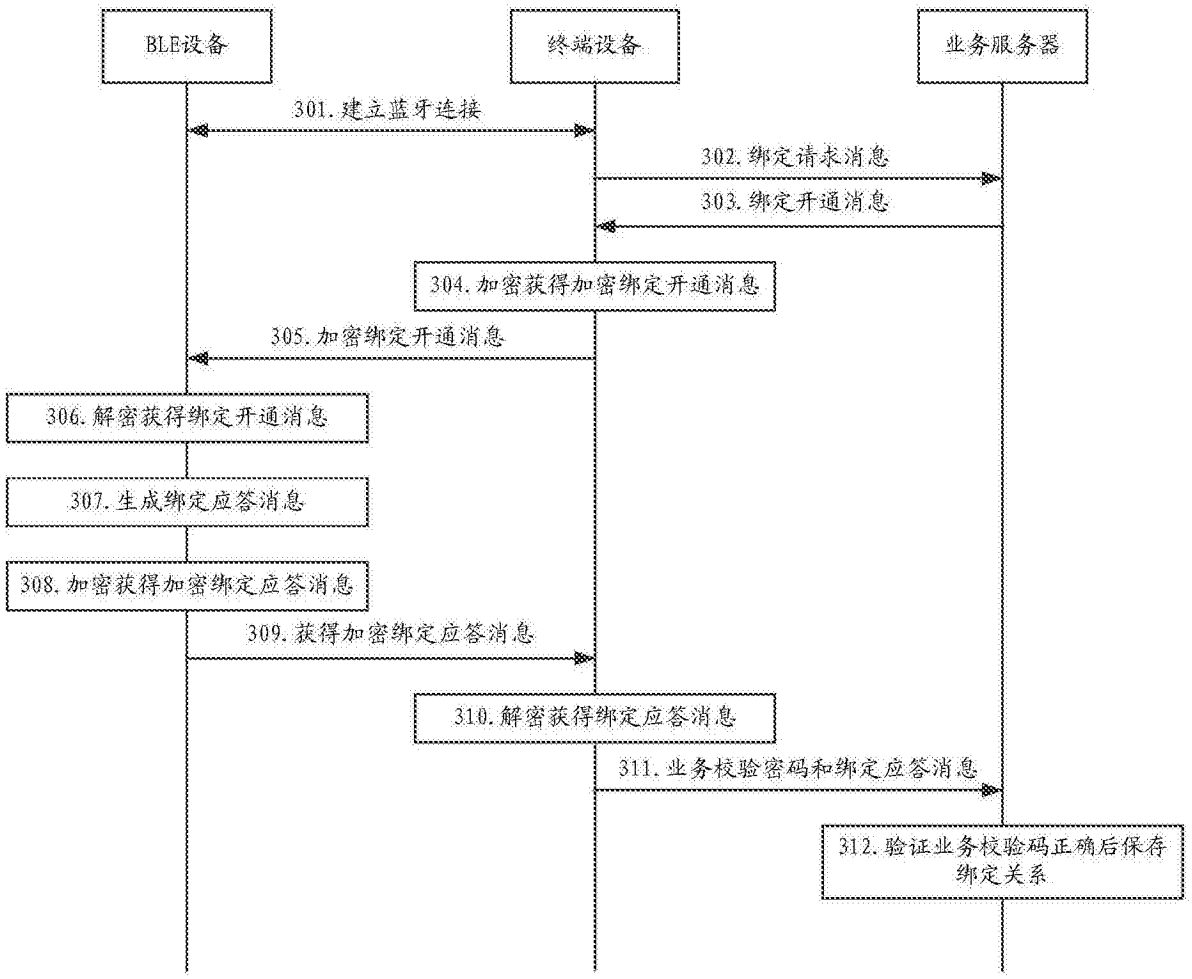

BLE设备
终端设备
业务服务器
301. 建立蓝牙连接
302. 绑定请求消息
303. 绑定开通消息
304. 加密获得加密绑定开通消息
305. 加密绑定开通消息
306. 解密获得绑定开通消息
307. 生成绑定应答消息
308. 加密获得加密绑定应答消息
309. 获得加密绑定应答消息
310. 解密获得绑定应答消息
311. 业务校验密码和绑定应答消息
312. 验证业务校验码正确后保存绑定关系

图 3A

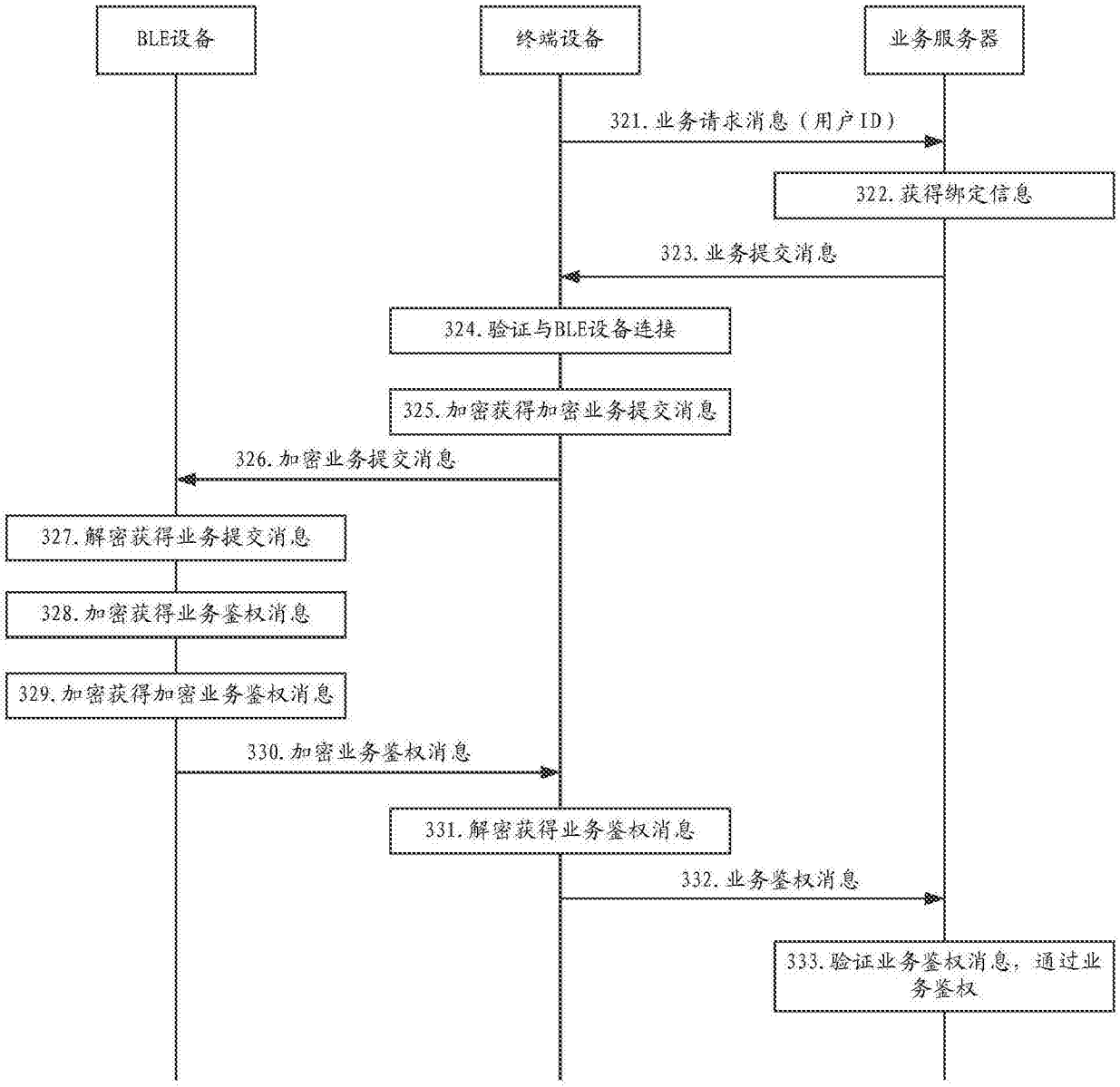

BLE设备
终端设备
业务服务器
321. 业务请求消息（用户ID）
322. 获得绑定信息
323. 业务提交消息
324. 验证与BLE设备连接
325. 加密获得加密业务提交消息
326. 加密业务提交消息
327. 解密获得业务提交消息
328. 加密获得业务鉴权消息
329. 加密获得加密业务鉴权消息
330. 加密业务鉴权消息
331. 解密获得业务鉴权消息
332. 业务鉴权消息
333. 验证业务鉴权消息，通过业务鉴权

图 3B

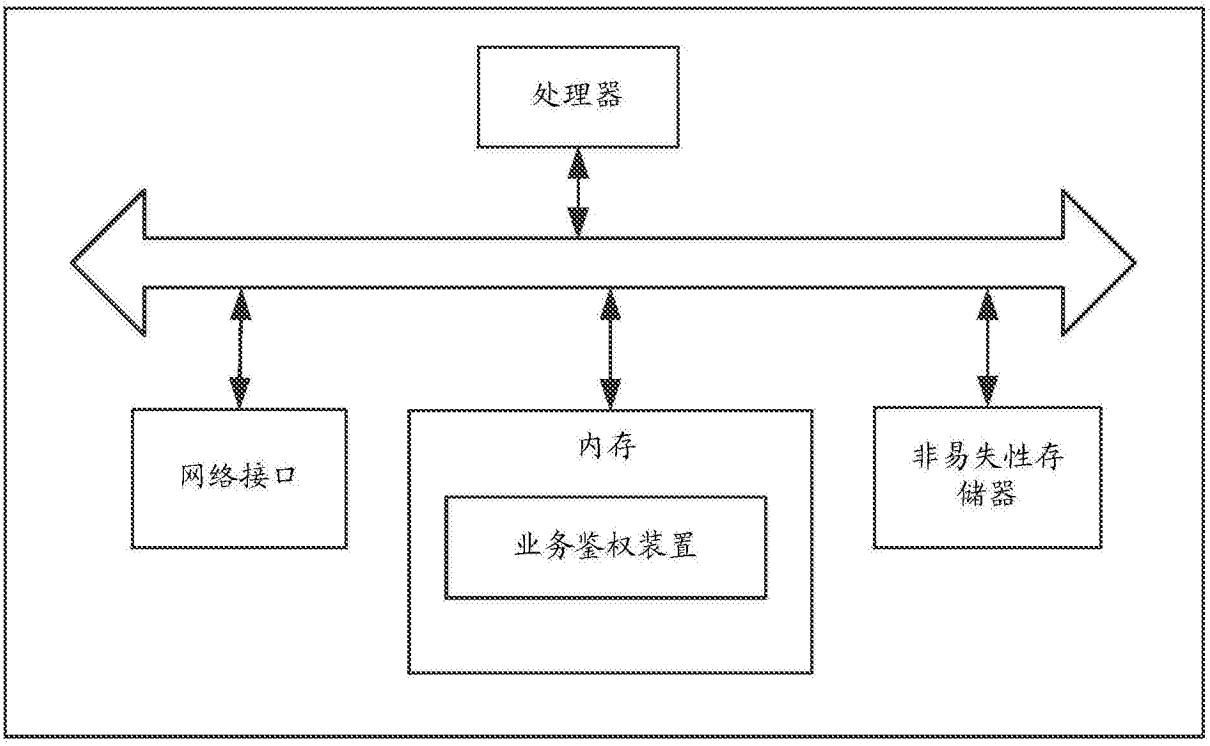


图 4

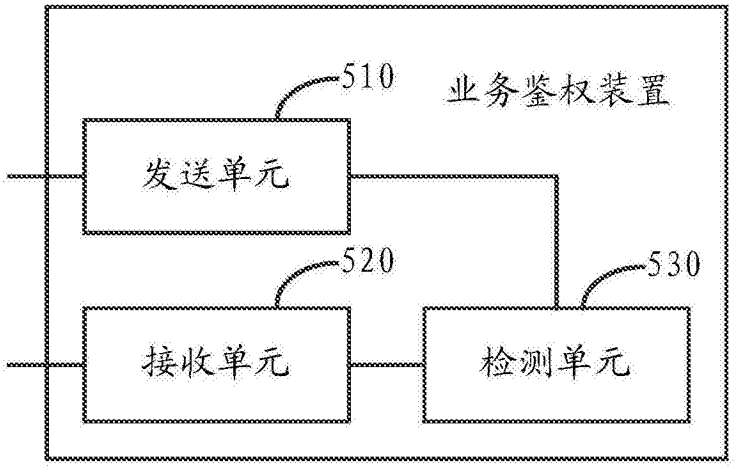


图 5

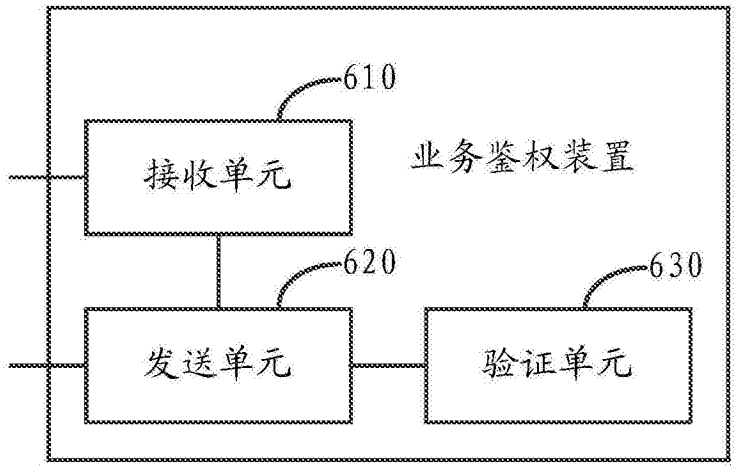

610
接收单元
业务鉴权装置
620
630
发送单元
验证单元

图 6

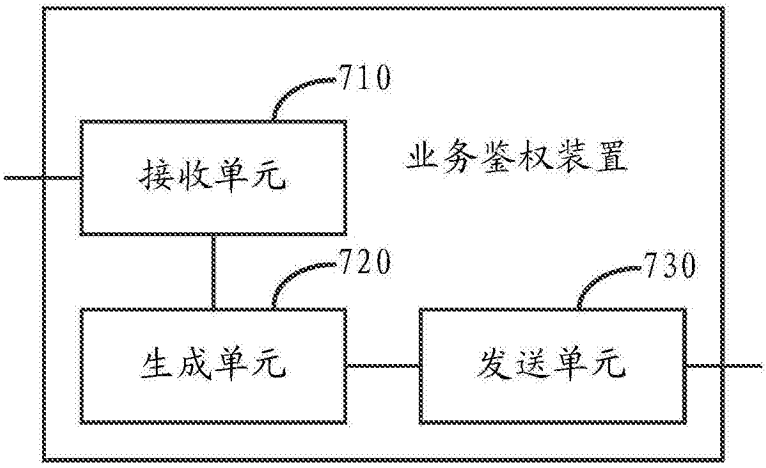

710
接收单元
业务鉴权装置
720
730
生成单元
发送单元

图 7