(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110166246 B
(45)授权公告日 2022.07.08

(21)申请号 201910284426.7

(22)申请日 2016.03.30

(65)同一申请的已公布的文献号
申请公布号 CN 110166246 A

(43)申请公布日 2019.08.23

(62)分案原申请数据
201610192200.0 2016.03.30

(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心

(72)发明人 孙元博

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

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)

(56)对比文件
US 2009235086 A1,2009.09.17
CN 101291220 A,2008.10.22

审查员 傅琦

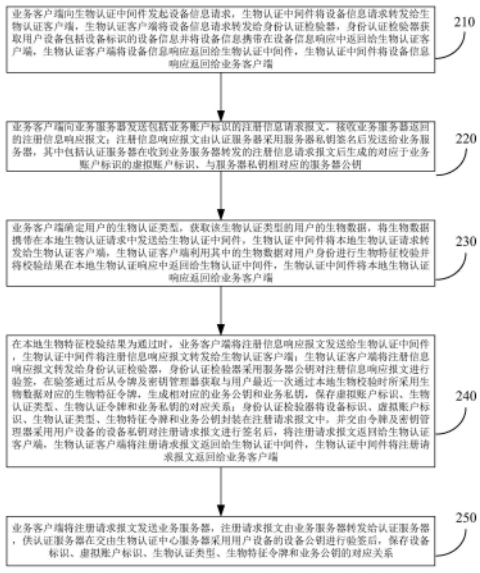
权利要求书5页 说明书18页 附图10页

(54)发明名称

基于生物特征的身份注册、认证的方法和装置

(57)摘要

本说明书提供一种基于生物特征的身份注册方法，应用在用户设备上，包括：向业务服务器发送包括用户的业务账户标识的注册信息请求报文，接收业务服务器返回的注册信息响应报文；所述注册信息响应报文中包括对应于所述业务账户标识的虚拟账户标识；获取所述用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；在生物特征校验结果为通过时，获取与所采用的生物数据对应的生物特征令牌；将虚拟账户标识、用户设备的设备标识、和生物特征令牌封装在注册请求报文中，发送给业务服务器；供认证服务器在收到业务服务器转发的注册请求报文后，保存所述虚拟账户标识、设备标识和生物特征令牌的对应关系，以用来进行身份认证。



CN 110166246 B

1.一种基于生物特征的身份注册方法,应用在用户设备上,包括:

向业务服务器发送包括用户的业务账户标识的注册信息请求报文,接收业务服务器返回的注册信息响应报文;所述注册信息响应报文中包括认证服务器在收到业务服务器转发的注册信息请求报文后生成的对应于所述业务账户标识的虚拟账户标识、以及与服务器私钥相对应的服务器公钥,所述注册信息响应报文采用服务器私钥进行签名;

确定用户的生物认证类型,获取所述生物认证类型的用户的生物数据,采用所述生物数据对用户身份进行生物特征校验;

在生物特征校验结果为通过时,采用服务器公钥对所述注册信息响应报文进行验签,验签通过后获取与所采用的生物数据对应的生物特征令牌;

将虚拟账户标识、用户设备的设备标识、生物认证类型、业务公钥和生物特征令牌封装在注册请求报文中,并采用用户设备的设备私钥对注册请求报文进行签名后发送给业务服务器;供认证服务器在收到业务服务器转发的注册请求报文后,保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系,以用来对所述用户的账户进行身份认证。

2.根据权利要求1所述的方法,所述注册信息响应报文中还包括:认证服务器生成的所述虚拟账户的注册挑战码;

所述注册请求报文中还包括:所述注册挑战码,供认证服务器在收到业务服务器转发的注册请求报文后,根据所述注册挑战码以及发送注册信息响应报文和收到注册请求报文的时间间隔,对注册请求报文进行验证。

3.一种基于生物特征的身份注册方法,应用在认证服务器上,包括:

从业务服务器接收来自用户设备的注册信息请求报文,所述注册信息请求报文中包括业务账户标识;生成对应于所述业务账户标识的虚拟账户标识,将虚拟账户标识和服务器公钥封装在注册信息响应报文中、并采用与服务器公钥相对应的服务器私钥对注册信息响应报文签名后发送给业务服务器,供业务服务器将注册信息响应报文转发给用户设备;

从业务服务器接收来自用户设备的注册请求报文,所述注册请求报文中包括虚拟账户标识、用户设备的设备标识、生物认证类型、业务公钥和用户的生物特征令牌,所述注册请求报文采用用户设备的设备私钥进行签名;

在生物认证中心服务器采用设备标识对应的设备公钥对注册请求报文进行验签且通过验签后,保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系,以用来对所述用户的账户进行身份认证。

4.根据权利要求3所述的方法,所述方法还包括:生成所述虚拟账户的注册挑战码;

所述注册信息响应报文中还包括:所生成的注册挑战码;

所述注册请求报文中还包括:注册挑战码;

所述保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系,包括:当注册请求报文中的注册挑战码与为注册请求报文中虚拟账户生成的注册挑战码相同、并且发送注册信息响应报文和收到注册请求报文的时间间隔在第一预定时长范围内时,保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系。

5.一种基于生物特征的身份认证方法,应用在用户设备上,包括:

向业务服务器发送包括用户设备的设备标识的认证信息请求报文，接收业务服务器返回的认证信息响应报文；所述认证信息响应报文由认证服务器在收到业务服务器转发的认证信息请求报文后生成，其中包括与所述设备标识对应的虚拟账户标识、以及与服务器私钥相对应的服务器公钥，所述认证信息响应报文由认证服务器采用服务器私钥签名后发送给业务服务器；

获取注册时所采用生物认证类型的用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；

在通过生物特征校验后，采用服务器公钥对认证信息响应报文进行验签，在验签通过后获取与所述生物数据对应的生物特征令牌；

向业务服务器发送采用业务私钥进行签名后的认证请求报文，所述认证请求报文中包括设备标识、生物认证类型、所述虚拟账户标识和生物特征令牌，供认证服务器在收到业务服务器转发的认证请求报文后，根据与所述虚拟账户标识、设备标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥对用户进行身份认证。

6.根据权利要求5所述的方法，所述认证信息响应报文中还包括：认证服务器生成的所述虚拟账户的认证挑战码；

所述认证请求报文中还包括：所述认证挑战码，供认证服务器在收到认证请求报文后，根据所述认证挑战码以及发送认证信息响应报文和收到认证请求报文的时间间隔，对认证请求报文进行验证。

7.一种基于生物特征的身份认证方法，应用在认证服务器上，所述认证服务器保存有虚拟账户标识、设备标识、生物认证类型、已注册业务公钥和已注册生物特征令牌的对应关系，所述方法包括：

从业务服务器接收来自用户设备的认证信息请求报文，所述认证信息请求报文中包括用户设备的设备标识；获取对应于所述设备标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在认证信息响应报文中、并采用与服务器公钥相对应的服务器私钥进行签名后发送给业务服务器，供业务服务器将认证信息响应报文转发给用户设备；

从业务服务器接收来自用户设备的认证请求报文，所述认证请求报文中包括用户设备的设备标识、生物认证类型、虚拟账户标识和生物特征令牌，并采用业务私钥进行签名；

获取与认证请求报文中的设备标识、虚拟账户标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥，采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证。

8.根据权利要求7所述的方法，所述方法还包括：生成所述虚拟账户的认证挑战码；

所述认证信息响应报文中还包括：所生成的认证挑战码；

所述认证请求报文中还包括：认证挑战码；

所述获取与认证请求报文中的设备标识、虚拟账户标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥，采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证，包括：当认证请求报文中的认证挑战码与为认证请求报文中虚拟账户生成的认证挑战码相同、并且发送认证信息响应报文和收到认证请求报文的时间间隔在第二预定时长范围内时，获取与认证请求报文中的设备标识、虚拟账户标识、生物认证类型对应的已注册生物特征令牌和已

注册业务公钥，采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证。

9.一种基于生物特征的身份注册装置，应用在用户设备上，包括：

用户注册信息单元，用于向业务服务器发送包括用户的业务账户标识的注册信息请求报文，接收业务服务器返回的注册信息响应报文；所述注册信息响应报文中包括认证服务器在收到业务服务器转发的注册信息请求报文后生成的对应于所述业务账户标识的虚拟账户标识、以及与服务器私钥相对应的服务器公钥，所述注册信息响应报文采用服务器私钥进行签名；

注册生物数据单元，用于确定用户的生物认证类型，获取所述生物认证类型的用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；

注册生物令牌单元，用于在生物特征校验结果为通过时，采用服务器公钥对所述注册信息响应报文进行验签，验签通过后获取与所采用的生物数据对应的生物特征令牌；

用户注册请求单元，用于将虚拟账户标识、用户设备的设备标识、生物认证类型、业务公钥和生物特征令牌封装在注册请求报文中，并采用用户设备的设备私钥对注册请求报文进行签名后发送给业务服务器；供认证服务器在收到业务服务器转发的注册请求报文后，保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

10.根据权利要求9所述的装置，所述注册信息响应报文中还包括：认证服务器生成的所述虚拟账户的注册挑战码；

所述注册请求报文中还包括：所述注册挑战码，供认证服务器在收到业务服务器转发的注册请求报文后，根据所述注册挑战码以及发送注册信息响应报文和收到注册请求报文的时间间隔，对注册请求报文进行验证。

11.一种基于生物特征的身份注册装置，应用在认证服务器上，包括：

注册信息响应单元，用于从业务服务器接收来自用户设备的注册信息请求报文，所述注册信息请求报文中包括业务账户标识；生成对应于所述业务账户标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在注册信息响应报文中、并采用与服务器公钥相对应的服务器私钥对注册信息响应报文签名后发送给业务服务器，供业务服务器将注册信息响应报文转发给用户设备；

注册请求接收单元，用于从业务服务器接收来自用户设备的注册请求报文，所述注册请求报文中包括虚拟账户标识、用户设备的设备标识、生物认证类型、业务公钥和用户的生物特征令牌，所述注册请求报文采用用户设备的设备私钥进行签名；

注册信息保存单元，用于在生物认证中心服务器采用设备标识对应的设备公钥对注册请求报文进行验签且通过验签后，保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

12.根据权利要求11所述的装置，所述装置还包括：注册挑战码生成单元，用于生成所述虚拟账户的注册挑战码；

所述注册信息响应报文中还包括：所生成的注册挑战码；

所述注册请求报文中还包括：注册挑战码；

所述注册信息保存单元具体用于：当注册请求报文中的注册挑战码与为注册请求报文

中虚拟账户生成的注册挑战码相同、并且发送注册信息响应报文和收到注册请求报文的时间间隔在第一预定时长范围内时，保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系。

13.一种基于生物特征的身份认证装置，应用在用户设备上，包括：

认证信息用户单元，用于向业务服务器发送包括用户设备的设备标识的认证信息请求报文，接收业务服务器返回的认证信息响应报文；所述认证信息响应报文由认证服务器在收到业务服务器转发的认证信息请求报文后生成，其中包括与所述设备标识对应的虚拟账户标识、以及与服务器私钥相对应的服务器公钥，所述认证信息响应报文由认证服务器采用服务器私钥签名后发送给业务服务器；

认证生物数据单元，用于获取注册时所采用生物认证类型的用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；

认证生物令牌单元，用于在通过生物特征校验后，采用服务器公钥对认证信息响应报文进行验签，在验签通过后获取与所述生物数据对应的生物特征令牌；

用户认证请求单元，用于向业务服务器发送采用业务私钥进行签名后的认证请求报文，所述认证请求报文中包括设备标识、生物认证类型、所述虚拟账户标识和生物特征令牌，供认证服务器在收到业务服务器转发的认证请求报文后，根据与所述虚拟账户标识、设备标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥对用户进行身份认证。

14.根据权利要求13所述的装置，所述认证信息响应报文中还包括：认证服务器生成的所述虚拟账户的认证挑战码；

所述认证请求报文中还包括：所述认证挑战码，供认证服务器在收到认证请求报文后，根据所述认证挑战码以及发送认证信息响应报文和收到认证请求报文的时间间隔，对认证请求报文进行验证。

15.一种基于生物特征的身份认证装置，应用在认证服务器上，所述认证服务器保存有虚拟账户标识、设备标识、生物认证类型、已注册业务公钥和已注册生物特征令牌的对应关系，所述装置包括：

认证信息响应单元，用于从业务服务器接收来自用户设备的认证信息请求报文，所述认证信息请求报文中包括用户设备的设备标识；获取对应于所述设备标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在认证信息响应报文中、并采用与服务器公钥相对应的服务器私钥进行签名后发送给业务服务器，供业务服务器将认证信息响应报文转发给用户设备；

认证请求接收单元，用于从业务服务器接收来自用户设备的认证请求报文，所述认证请求报文中包括用户设备的设备标识、生物认证类型、虚拟账户标识和生物特征令牌，并采用业务私钥进行签名；

身份认证单元，用于获取与认证请求报文中的设备标识、虚拟账户标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥，采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证。

16.根据权利要求15所述的装置，所述装置还包括：认证挑战码生成单元，用于生成所

述虚拟账户的认证挑战码；

所述认证信息响应报文中还包括：所生成的认证挑战码；

所述认证请求报文中还包括：认证挑战码；

所述身份认证单元具体用于：当认证请求报文中的认证挑战码与为认证请求报文中虚拟账户生成的认证挑战码相同、并且发送认证信息响应报文和收到认证请求报文的时间间隔在第二预定时长范围内时，获取与认证请求报文中的设备标识、虚拟账户标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥，采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证。

17.一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求1到2任意一项所述的方法。

18.一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求3到4任意一项所述的方法。

19.一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求5到6任意一项所述的方法。

20.一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求7到8任意一项所述的方法。

21.一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求1到2任意一项所述的方法。

22.一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求3到4任意一项所述的方法。

23.一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求5到6任意一项所述的方法。

24.一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行如权利要求7到8任意一项所述的方法。

基于生物特征的身份注册、认证的方法和装置

[0001] 本申请是申请号为201610192200.0、申请日为2016年3月30日的中国发明专利申请《基于生物特征的身份注册、认证的方法和装置》的分案申请。

技术领域

[0002] 本说明书涉及网络通信技术领域，尤其涉及一种基于生物特征的身份注册方法和装置、一种基于生物特征的身份认证方法和装置。

背景技术

[0003] 随着生物识别技术的发展，通过计算机与光学、声学、生物传感器和生物统计学等技术手段的结合，利用人体固有的指纹、人脸、虹膜、声音等生理特性进行个人身份的鉴定，已经成为可能。

[0004] 移动互联的蓬勃发展为生物识别技术提供了新的应用平台，例如采用指纹、人脸等在用户设备上可以登录账户、实现支付，而无需记忆并输入密码。由于更倾向于采用生物识别来进行身份认证的通常是移动支付等关键应用，因此安全性成为注册和认证过程中需要最为优先考虑的重要因素。

发明内容

[0005] 有鉴于此，

[0006] 本说明书提供一种基于生物特征的身份注册方法，应用在用户设备上，包括：

[0007] 向业务服务器发送包括用户的业务账户标识的注册信息请求报文，接收业务服务器返回的注册信息响应报文；所述注册信息响应报文中包括认证服务器在收到业务服务器转发的注册信息请求报文后生成的对应于所述业务账户标识的虚拟账户标识、以及与服务器私钥相对应的服务器公钥，所述注册信息响应报文采用服务器私钥进行签名；

[0008] 确定用户的生物认证类型，获取所述生物认证类型的用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；

[0009] 在生物特征校验结果为通过时，采用服务器公钥对所述注册信息响应报文进行验签，验签通过后获取与所采用的生物数据对应的生物特征令牌；

[0010] 将虚拟账户标识、用户设备的设备标识、生物认证类型、业务公钥和生物特征令牌封装在注册请求报文中，并采用用户设备的设备私钥对注册请求报文进行签名后发送给业务服务器；供认证服务器在收到业务服务器转发的注册请求报文后，保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

[0011] 本说明书提供的一种基于生物特征的身份注册方法，应用在认证服务器上，包括：

[0012] 从业务服务器接收来自用户设备的注册信息请求报文，所述注册信息请求报文中包括业务账户标识；生成对应于所述业务账户标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在注册信息响应报文中、并采用与服务器公钥相对应的服务器私钥对注册信

息响应报文签名后发送给业务服务器，供业务服务器将注册信息响应报文转发给用户设备；

[0013] 从业务服务器接收来自用户设备的注册请求报文，所述注册请求报文中包括虚拟账户标识、用户设备的设备标识、生物认证类型、业务公钥和用户的生物特征令牌，所述注册请求报文采用用户设备的设备私钥进行签名；

[0014] 在生物认证中心服务器采用设备标识对应的设备公钥对注册请求报文进行验签且通过验签后，保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

[0015] 本说明书提供的一种基于生物特征的身份认证方法，应用在用户设备上，包括：

[0016] 向业务服务器发送包括用户设备的设备标识的认证信息请求报文，接收业务服务器返回的认证信息响应报文；所述认证信息响应报文由认证服务器在收到业务服务器转发的认证信息请求报文后生成，其中包括与所述设备标识对应的虚拟账户标识、以及与服务器私钥相对应的服务器公钥，所述认证信息响应报文由认证服务器采用服务器私钥签名后发送给业务服务器；

[0017] 获取注册时所采用生物认证类型的用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；

[0018] 在通过生物特征校验后，采用服务器公钥对认证信息响应报文进行验签，在验签通过后获取与所述生物数据对应的生物特征令牌；

[0019] 向业务服务器发送采用业务私钥进行签名后的认证请求报文，所述认证请求报文中包括设备标识、生物认证类型、所述虚拟账户标识和生物特征令牌，供认证服务器在收到业务服务器转发的认证请求报文后，根据与所述虚拟账户标识、设备标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥对用户进行身份认证。

[0020] 本说明书提供的一种基于生物特征的身份认证方法，应用在认证服务器上，所述认证服务器保存有虚拟账户标识、设备标识、生物认证类型、已注册业务公钥和已注册生物特征令牌的对应关系，所述方法包括：

[0021] 从业务服务器接收来自用户设备的认证信息请求报文，所述认证信息请求报文中包括用户设备的设备标识；获取对应于所述设备标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在认证信息响应报文中、并采用与服务器公钥相对应的服务器私钥进行签名后发送给业务服务器，供业务服务器将认证信息响应报文转发给用户设备；

[0022] 从业务服务器接收来自用户设备的认证请求报文，所述认证请求报文中包括用户设备的设备标识、生物认证类型、虚拟账户标识和生物特征令牌；

[0023] 获取与认证请求报文中的设备标识、虚拟账户标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥，采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证。

[0024] 本说明书还提供了一种基于生物特征的身份注册装置，应用在用户设备上，包括：

[0025] 用户注册信息单元，用于向业务服务器发送包括用户的业务账户标识的注册信息请求报文，接收业务服务器返回的注册信息响应报文；所述注册信息响应报文中包括认证服务器在收到业务服务器转发的注册信息请求报文后生成的对应于所述业务账户标识的虚拟账户标识、以及与服务器私钥相对应的服务器公钥，所述注册信息响应报文采用服务

器私钥进行签名；

[0026] 注册生物数据单元，用于确定用户的生物认证类型，获取所述生物认证类型的用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；

[0027] 注册生物令牌单元，用于在生物特征校验结果为通过时，采用服务器公钥对所述注册信息响应报文进行验签，验签通过后获取与所采用的生物数据对应的生物特征令牌；

[0028] 用户注册请求单元，用于将虚拟账户标识、用户设备的设备标识、生物认证类型、业务公钥和生物特征令牌封装在注册请求报文中，并采用用户设备的设备私钥对注册请求报文进行签名后发送给业务服务器；供认证服务器在收到业务服务器转发的注册请求报文后，保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

[0029] 本说明书提供的一种基于生物特征的身份注册装置，应用在认证服务器上，包括：

[0030] 注册信息响应单元，用于从业务服务器接收来自用户设备的注册信息请求报文，所述注册信息请求报文中包括业务账户标识；生成对应于所述业务账户标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在注册信息响应报文中、并采用与服务器公钥相对应的服务器私钥对注册信息响应报文签名后发送给业务服务器，供业务服务器将注册信息响应报文转发给用户设备；

[0031] 注册请求接收单元，用于从业务服务器接收来自用户设备的注册请求报文，所述注册请求报文中包括虚拟账户标识、用户设备的设备标识、生物认证类型、业务公钥和用户的生物特征令牌，所述注册请求报文采用用户设备的设备私钥进行签名；

[0032] 注册信息保存单元，用于在生物认证中心服务器采用设备标识对应的设备公钥对注册请求报文进行验签且通过验签后，保存所述虚拟账户标识、设备标识、生物认证类型、业务公钥和生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

[0033] 本说明书提供的一种基于生物特征的身份认证装置，应用在用户设备上，包括：

[0034] 认证信息用户单元，用于向业务服务器发送包括用户设备的设备标识的认证信息请求报文，接收业务服务器返回的认证信息响应报文；所述认证信息响应报文由认证服务器在收到业务服务器转发的认证信息请求报文后生成，其中包括与所述设备标识对应的虚拟账户标识、以及与服务器私钥相对应的服务器公钥，所述认证信息响应报文由认证服务器采用服务器私钥签名后发送给业务服务器；

[0035] 认证生物数据单元，用于获取注册时所采用生物认证类型的用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；

[0036] 认证生物令牌单元，用于在通过生物特征校验后，采用服务器公钥对认证信息响应报文进行验签，在验签通过后获取与所述生物数据对应的生物特征令牌；

[0037] 用户认证请求单元，用于向业务服务器发送采用业务私钥进行签名后的认证请求报文，所述认证请求报文中包括设备标识、生物认证类型、所述虚拟账户标识和生物特征令牌，供认证服务器在收到业务服务器转发的认证请求报文后，根据与所述虚拟账户标识、设备标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥对用户进行身份认证。

[0038] 本说明书提供的一种基于生物特征的身份认证装置，应用在认证服务器上，所述认证服务器保存有虚拟账户标识、设备标识、生物认证类型、已注册业务公钥和已注册生物

特征令牌的对应关系，所述装置包括：

[0039] 认证信息响应单元，用于从业务服务器接收来自用户设备的认证信息请求报文，所述认证信息请求报文中包括用户设备的设备标识；获取对应于所述设备标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在认证信息响应报文中、并采用与服务器公钥相对应的服务器私钥进行签名后发送给业务服务器，供业务服务器将认证信息响应报文转发给用户设备；

[0040] 认证请求接收单元，用于从业务服务器接收来自用户设备的认证请求报文，所述认证请求报文中包括用户设备的设备标识、生物认证类型、虚拟账户标识和生物特征令牌，并采用业务私钥进行签名；

[0041] 身份认证单元，用于获取与认证请求报文中的设备标识、虚拟账户标识、生物认证类型对应的已注册生物特征令牌和已注册业务公钥，采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证。

[0042] 本说明书提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述应用在用户设备上的基于生物特征的身份注册方法所述的方法。

[0043] 本说明书提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述应用在认证服务器上的基于生物特征的身份注册方法所述的方法。

[0044] 本说明书提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述应用在用户设备上的基于生物特征的身份认证方法所述的方法。

[0045] 本说明书提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述应用在认证服务器上的基于生物特征的身份认证方法所述的方法。

[0046] 本说明书提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述应用在用户设备上的基于生物特征的身份注册方法所述的方法。

[0047] 本说明书提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述应用在认证服务器上的基于生物特征的身份注册方法所述的方法。

[0048] 本说明书提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述应用在用户设备上的基于生物特征的身份认证方法所述的方法。

[0049] 本说明书提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器运行时，执行上述应用在认证服务器上的基于生物特征的身份认证方法所述的方法。

[0050] 由以上技术方案可见，本说明书的实施例中，在身份注册时用户设备将对应于用户注册时采用的生物数据的生物特征令牌上传至认证服务器，从而将设备标识、虚拟账户

标识和生物特征令牌的对应关系注册给认证服务器，由认证服务器保存；在身份认证时，用户设备将通过本地生物特征校验的生物数据对应的生物特征令牌上传至认证服务器，由认证服务器根据设备标识、虚拟账户标识、上传的和已注册的生物特征令牌来对账户进行身份认证；由于恶意软件很难获取到生物特征令牌，也就难以通过认证服务器的身份验证，增加了用户账户的安全性。

附图说明

[0051] 图1是本说明书实施例应用场景的一种网络结构图；

[0052] 图2是本说明书实施例一中一种应用在用户设备上、基于生物特征的身份注册方法的流程图；

[0053] 图3是本说明书实施例一中一种应用在认证服务器上、基于生物特征的身份注册方法的流程图；

[0054] 图4是本说明书实施例一中一种用户设备、业务服务器、认证服务器与生物认证中心服务器之间身份注册的交互流程图；

[0055] 图5是本说明书实施例二中一种应用在用户设备上、基于生物特征的身份认证方法的流程图；

[0056] 图6是本说明书实施例二中一种应用在认证服务器上、基于生物特征的身份认证方法的流程图；

[0057] 图7是本说明书实施例二中一种用户设备、业务服务器与认证服务器之间身份认证的交互流程图；

[0058] 图8是本说明书实施例中用户设备或认证服务器的一种硬件结构图；

[0059] 图9是本说明书实施例中一种应用在用户设备上基于生物特征的身份注册装置的逻辑结构图；

[0060] 图10是本说明书实施例中一种应用在认证服务器上、基于生物特征的身份注册装置的逻辑结构图；

[0061] 图11是本说明书实施例中一种应用在用户设备上基于生物特征的身份认证装置的逻辑结构图；

[0062] 图12是本说明书实施例中一种应用在认证服务器上、基于生物特征的身份认证装置的逻辑结构图。

具体实施方式

[0063] 在基于用户设备的生物识别应用中，用户的生物数据由用户设备采集，生物识别可以在用户设备上进行，也可以由服务器进行。由于向服务器上传这些图像或视频数据往往会消耗大量的流量，本说明书的实施例中，生物识别在用户设备上完成。

[0064] 本说明书实施例应用场景的一种网络结构如图1所示，用户设备与业务服务器、业务服务器与认证服务器之间通过通信网络相互可访问。其中，用户设备是具有生物特征识别功能的终端设备，可以是手机、平板电脑、PC(Personal Computer，个人电脑)、笔记本等设备；业务服务器用来接收用户通过用户设备发起的业务请求(包括注册和认证请求)，并向用户设备发送对其请求的响应；认证服务器用来对用户账户进行身份认证；业务服务器

或认证服务器可以是一个物理或逻辑服务器，也可以是由两个或两个以上分担不同职责的物理或逻辑服务器、相互协同来实现本说明书实施例中业务服务器或认证服务器的各项功能。本说明书实施例对用户设备、业务服务器和认证服务器的种类，以及用户设备与业务服务器之间、业务服务器与认证服务器之间通信网络的类型、协议等均不做限定。

[0065] 本说明书的实施例一描述一种基于生物特征的身份注册方法，该方法应用在用户设备上的流程如图2所示，应用在认证服务器上的流程如图3所示。

[0066] 本说明书的实施例中，用户设备上运行有以下功能模块：业务客户端、生物认证中间件、生物认证客户端、身份认证检验器和令牌及密钥管理器。这些功能模块可以是一个独立的软件、某个独立软件的组成部分、或软件与硬件相结合的实现，本说明书的实施例对其具体实现不做限定。

[0067] 本说明书的实施例中，用户设备上保存有设备私钥，由令牌及密钥管理器保存和使用；生物认证中心服务器可以从本地或其他可访问的网络存储位置获取到用户设备的设备标识与该用户设备的设备公钥的对应关系，同一个用户设备的设备私钥与设备公钥相对应。认证服务器可以通过网络访问生物认证中心服务器。设备私钥可以在设备出厂前预存在用户设备上；也可以由用户设备、生物认证中心服务器或某个其他的网络节点生成相对应的设备私钥和设备公钥后，分别交由用户设备和生物认证中心服务器保存；本说明书的实施例不做限定。

[0068] 在用户设备上，步骤210，业务客户端向生物认证中间件发起设备信息请求，生物认证中间件将设备信息请求转发给生物认证客户端，生物认证客户端将设备信息请求转发给身份认证检验器，身份认证检验器获取用户设备包括设备标识的设备信息并将设备信息携带在设备信息响应中返回给生物认证客户端，生物认证客户端将设备信息响应返回给生物认证中间件，生物认证中间件将设备信息响应返回给业务客户端。

[0069] 当用户在用户设备上的业务客户端启动利用生物特征进行身份验证的注册流程时，业务客户端向生物认证中间件发起设备信息请求，生物认证中间件将设备信息请求转发给生物认证客户端，生物认证客户端将设备信息请求转发给身份认证检验器。

[0070] 身份认证检验器获取用户设备的设备信息，其中包括设备标识，还可以包括设备型号、生产厂商等。可以采用用户设备的硬件标识来作为设备标识，例如用户设备的UUID(Universally Unique Identifier，通用唯一识别码)、MAC(Media Access Control，媒体接入控制)地址、蓝牙地址等。

[0071] 身份认证检验器将所获取的设备信息携带在设备信息响应中返回给生物认证客户端，生物认证客户端将设备信息响应返回给生物认证中间件，生物认证中间件将设备信息响应返回给业务客户端。

[0072] 在用户设备上，步骤220，业务客户端向业务服务器发送包括业务账户标识的注册信息请求报文，接收业务服务器返回的注册信息响应报文；注册信息响应报文由认证服务器采用服务器私钥签名后发送给业务服务器，其中包括认证服务器在收到业务服务器转发的注册信息请求报文后生成的对应于业务账户标识的虚拟账户标识、与服务器私钥相对应的服务器公钥。

[0073] 在认证服务器上，步骤310，从业务服务器接收来自用户设备的注册信息请求报文，注册信息请求报文中包括业务账户标识；生成对应于业务账户标识的虚拟账户标识，将

虚拟账户标识和服务器公钥封装在注册信息响应报文中，采用与服务器公钥相对应的服务器私钥对注册信息响应报文签名后，发送给业务服务器，供业务服务器将注册信息响应报文转发给用户设备。

[0074] 用户设备的业务客户端向业务服务器发送注册信息请求报文，注册信息请求报文中包括业务账户标识。业务账户标识是该业务服务器上唯一对应于进行身份注册的用户账户的信息，例如可以是该业务系统中用户账户的名称、编码等等。注册信息请求报文中还可以包括用户设备的设备标识。业务服务器将注册信息请求报文转发给认证服务器。

[0075] 由于认证服务器可能为多个不同的业务系统提供认证服务，这些业务系统分别拥有各自的业务账户，为了避免这些业务系统中的业务账户标识有重复时导致认证服务器上难以区分不同的用户账户，认证服务器在收到注册信息请求报文后，生成对应于该业务账户(即对应于该业务系统中的该业务账户)的虚拟账户标识。虚拟账户标识在认证服务器上唯一对应于某个业务系统中的某个业务账户，本说明书实施例对生成虚拟账户标识的方式不做限定，例如，可以将业务系统标识与用户在该业务系统的业务账户标识来作为虚拟账户标识；再如，可以将该业务系统的该用户账户在认证服务器上登记注册账户的数据库中的索引来作为虚拟账户标识。

[0076] 需要说明的是，如果虚拟账户标识的生成方式不能确保对相同业务系统的相同业务账户生成同样的虚拟账户标识，则认证服务器要保存所生成的虚拟账户标识与业务系统的业务账户的对应关系(或者保存虚拟账户标识与设备标识的对应关系)，以便在后续的身份认证流程中，能够将与注册流程中相同的虚拟账户标识分配给同一个业务系统的同一个用户账户。

[0077] 认证服务器上预先保存有相对应的服务器私钥和服务器公钥，在生成虚拟账户标识后，认证服务器将虚拟账户标识和服务器公钥封装在注册信息响应报文中，采用服务器私钥对注册信息响应报文签名后，发送给业务服务器。业务服务器将注册信息响应报文转发给用户设备的业务客户端。

[0078] 在用户设备上，步骤230，业务客户端确定用户的生物认证类型，获取该生物认证类型的用户的生物数据，将生物数据携带在本地生物认证请求中发送给生物认证中间件，生物认证中间件将本地生物认证请求转发给生物认证客户端，生物认证客户端利用其中的生物数据对用户身份进行生物特征校验并将校验结果在本地生物认证响应中返回给生物认证中间件，生物认证中间件将本地生物认证响应返回给业务客户端。

[0079] 业务客户端确定用户在本业务系统中进行身份认证时所采用的生物认证类型，并请求用户提供该类型的生物数据。业务客户端可以在用户设备支持的生物认证类型(即用户设备具有的生物特征识别功能)中按照预置的优先级选择其中的一种，也可以将本业务系统接受并且该用户设备支持的几种生物认证类型显示给用户供其选择，本说明书的实施例不做限定。生物认证类型可以是指纹、声音、虹膜、人脸等。

[0080] 用户的生物数据可以是业务客户端确定的生物认证类型中该用户设备能够识别的任何一个特定对象，例如对指纹而言，可以是任何一个手指的指纹；对虹膜而言，可以是任意一只眼睛的虹膜。

[0081] 在业务客户端获取到所确定生物认证类型的生物数据后，将生物数据封装在本地生物认证请求中发送给生物认证中间件，生物认证中间件将本地生物认证请求转发给生物

认证客户端。

[0082] 生物认证客户端利用其中的生物数据对用户身份进行生物特征校验。生物特征校验的具体方式可以参照现有技术中用户设备的生物特征识别方式来实现，例如可以是与用户设备上本地预先保存的样本数据进行比对，如果匹配程度满足某些预定条件，则生物特征校验成功。在校验完成后，生物认证客户端将是否通过的校验结果封装在本地生物认证响应中返回给生物认证中间件，生物认证中间件将本地生物认证响应返回给业务客户端。

[0083] 在用户设备上，步骤240，在本地生物特征校验结果为通过时，业务客户端将注册信息响应报文发送给生物认证中间件，生物认证中间件将注册信息响应报文转发给生物认证客户端；生物认证客户端将注册信息响应报文转发给身份认证检验器，身份认证检验器采用服务器公钥对注册信息响应报文进行验签，在验签通过后从令牌及密钥管理器获取与用户最近一次通过本地生物校验时所采用生物数据对应的生物特征令牌，生成相对应的业务公钥和业务私钥，保存虚拟账户标识、生物认证类型、生物认证令牌和业务私钥的对应关系；身份认证检验器将设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥封装在注册请求报文中，并交由令牌及密钥管理器采用用户设备的设备私钥对注册请求报文进行签名后，将注册请求报文返回给生物认证客户端，生物认证客户端将注册请求报文返回给生物认证中间件，生物认证中间件将注册请求报文返回给业务客户端。

[0084] 业务客户端从生物认证中间件返回的本地生物认证响应中提取本地生物特征校验结果，如果结果为未通过，则身份注册流程以失败结束。当本地生物特征校验结果为通过时，业务客户端将注册信息响应报文发送给生物认证中间件，生物认证中间件将注册信息响应报文转发给生物认证客户端；生物认证客户端将注册信息响应报文转发给身份认证检验器。

[0085] 身份认证检验器从注册信息响应报文中提取服务器公钥，采用该服务器公钥对注册信息响应报文进行验签，如果验签未通过，则说明注册信息响应报文很可能并非来自于可靠的认证服务器，注册流程以失败结束。在验签通过后，身份认证检验器向令牌及密钥管理器请求生物特征令牌。令牌及密钥管理器将与用户最近一次通过本地生物校验时所采用生物数据(即业务客户端在步骤230中用来进行本地生物特征校验时所获取的生物数据)对应的生物特征令牌返回给身份认证检验器。

[0086] 生物特征令牌是该用户设备上唯一对应于用于校验该生物数据的样本数据的特征量或索引值。也就是说，用户的每个手指的指纹分别对应于一个不同的生物特征令牌，人脸的对应于另外一个不同的生物特征令牌；每次用户采用拇指进行生物特征校验时，用户设备采集的拇指指纹数据都是用拇指指纹的样本数据进行校验，因而这些拇指指纹数据都对应于同一个生物特征令牌。本说明书对生物特征令牌的形式和生成生物特征令牌的具体方式不做限定，例如可以是对该样本数据或该样本数据的一部分应用摘要算法后得到的信息摘要，也可以是一个对应于该样本数据的随机数。

[0087] 身份认证检验器生成相对应的业务公钥和业务私钥，保存注册信息响应报文中的虚拟账户标识、用户最近一次通过本地生物校验时所采用的生物认证类型、令牌及密钥管理器返回的生物特征令牌、与生成的业务私钥的对应关系。身份认证检验器将设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥封装在注册请求报文中，将注册请求报文发送给令牌及密钥管理器。令牌及密钥管理器读取保存的用户设备的设备私钥，用设

备私钥对注册请求报文进行签名后，将注册请求报文返回给身份认证检验器，身份认证检验器将注册请求报文返回给生物认证客户端。

[0088] 生物认证客户端将注册请求报文返回给生物认证中间件，生物认证中间件将注册请求报文返回给业务客户端。

[0089] 在用户设备上，步骤250，业务客户端将注册请求报文发送业务服务器，注册请求报文由业务服务器转发给认证服务器，供认证服务器在交由生物认证中心服务器采用用户设备的设备公钥进行验签后，保存设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥的对应关系，以用来对用户账户进行身份认证。

[0090] 在认证服务器上，步骤320，从业务服务器接收来自用户设备的注册请求报文，注册请求报文中包括用户设备的设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥，并采用用户设备的设备密钥进行签名；将注册请求报文发送给生物认证中心服务器，接收生物认证中心服务器采用其中设备标识对应的设备公钥对注册请求报文进行验签后返回的验签结果。

[0091] 在认证服务器上，步骤330，在注册请求报文通过验签后，保存设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥的对应关系，以用来对用户账户进行身份认证。

[0092] 业务客户端将生物认证中间件返回的注册请求报文发送给业务服务器。业务服务器将注册请求报文转发给认证服务器。

[0093] 认证服务器将注册请求报文发送给生物认证中心服务器。生物认证中心服务器从接收的注册请求报文中提取设备标识，从可访问的网络存储位置查找与该设备标识对应的设备公钥，利用设备公钥对注册请求报文进行验签，并将验签结果返回给认证服务器。

[0094] 如果验签未通过，认证服务器拒绝注册请求并通知业务服务器，由业务服务器将注册失败的结果通知业务客户端。如果验签结果为通过，认证服务器保存注册请求报文中设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥的对应关系。

[0095] 认证服务器可以向业务服务器返回注册成功的注册响应报文，由业务服务器将注册成功的消息通知用户设备的业务客户端。认证服务器可以在注册响应报文中携带上述对应关系中的虚拟账户标识和生物认证类型，以及与该虚拟账户标识对应的业务账户标识，由业务服务器保存注册成功的注册响应报文中业务账户标识、虚拟账户标识和生物认证类型的对应关系。

[0096] 在一种实现方式中，认证服务器可以在收到注册信息请求报文后，生成虚拟账户标识和该虚拟账户的注册挑战码，注册挑战码的生成方式可以采用各种一次性口令的生成算法，本例中不做限定。认证服务器将虚拟账户标识、服务器公钥和所生成的注册挑战码封装在注册信息响应报文中发送给业务服务器，并启动计时。在生成注册请求报文时，用户设备上的身份认证检验器将注册信息响应报文中的注册挑战码也封装在注册请求报文中。认证服务器收到业务服务器转发的注册请求报文，比对注册请求报文中的注册挑战码和为注册请求报文中虚拟账户生成的注册挑战码，并获取发送注册信息响应报文和收到注册请求报文的时间差。如果两个注册挑战码不同或者该时间差超过第一预定时长，认证服务器拒绝注册请求并通知业务服务器，由业务服务器将注册失败的结果通知业务客户端；如果两个注册挑战码相同并且该时间差不超过第一预定时长，保存注册请求报文中设备标识、虚

拟账户标识、生物认证类型、生物特征令牌和业务公钥的对应关系。

[0097] 本实施例的一种包括注册挑战码的实现方式中，用户设备的各个功能模块、业务服务器、认证服务器与生物认证中心服务器之间的交互流程如图4所示。

[0098] 在本说明书的实施例一中，通过预存在用户设备上的设备私钥和设备公钥来确保用户设备为可信设备，通过服务器公钥和服务器私钥来验证业务服务器的可靠性，从而能够安全的将用户设备的设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥的对应关系注册到认证服务器上用于后续的身份认证，提高了身份注册过程的安全性。

[0099] 本说明书的实施例二描述一种基于生物特征的身份认证方法，该方法应用在用户设备上的流程如图5所示，应用在认证服务器上的流程如图6所示。实施例二中的身份认证流程中采用了与实施例一的身份注册流程中相同的一些技术手段，以下只对实施例二中与实施例一中不同的部分进行说明，相同部分请参见实施例一中的内容，不再重复。

[0100] 在用户设备上，步骤510，业务客户端向生物认证中间件发起设备信息请求，生物认证中间件将设备信息请求转发给生物认证客户端，生物认证客户端将设备信息请求转发给身份认证检验器，身份认证检验器获取用户设备包括设备标识的设备信息并将设备信息携带在设备信息响应中返回给生物认证客户端，生物认证客户端将设备信息响应返回给生物认证中间件，生物认证中间件将设备信息响应返回给业务客户端。

[0101] 当用户在用户设备上的业务客户端启动利用生物特征进行身份验证的认证流程时，业务客户端向生物认证中间件发起设备信息请求，生物认证中间件将设备信息请求转发给生物认证客户端，生物认证客户端将设备信息请求转发给身份认证检验器。

[0102] 身份认证检验器获取用户设备的设备信息，其中包括设备标识，还可以包括设备型号、生产厂商等。身份认证检验器将所获取的设备信息携带在设备信息响应中返回给生物认证客户端，生物认证客户端将设备信息响应返回给生物认证中间件，生物认证中间件将设备信息响应返回给业务客户端。

[0103] 在用户设备上，步骤520，业务客户端向业务服务器发送包括设备标识的认证信息请求报文，接收业务服务器返回的认证信息响应报文；认证信息响应报文由认证服务器采用服务器私钥签名后发送给业务服务器，其中包括认证服务器在收到业务服务器转发的认证信息请求报文后获取的与设备标识对应的虚拟账户标识、和与服务器私钥相对应的服务器公钥。

[0104] 在认证服务器上，步骤610，从业务服务器接收来自用户设备的认证信息请求报文，认证信息请求报文中包括用户设备的设备标识；获取对应于设备标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在认证信息响应报文中，采用与服务器公钥相对应的服务器私钥对认证信息响应报文签名后，发送给业务服务器，供业务服务器将认证信息响应报文转发给用户设备。

[0105] 用户设备的业务客户端向业务服务器发送认证信息请求报文，认证信息请求报文中包括用户设备的设备标识。认证信息请求报文中还可以包括用户的业务账户标识。业务服务器将认证信息请求报文转发给认证服务器。

[0106] 在实施例一的身份注册流程中，认证服务器将设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥的对应关系保存在本地或其他可访问的网络存储位置，保存后的设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥即为实施例二中

已注册的设备标识、已注册的虚拟账户标识、已注册的生物认证类型、已注册的生物特征令牌和已注册的业务公钥。

[0107] 在收到业务服务器转发的认证信息请求报文后，认证服务器从中提取用户设备的设备标识，查找与该设备标识对应的已注册的虚拟账户标识，将找到的虚拟账户标识和服务器公钥封装在认证信息响应报文中，并且采用与服务器公钥相对应的服务器私钥对认证信息响应报文签名后，发送给业务服务器。业务服务器将认证信息响应报文转发给用户设备。

[0108] 在用户设备上，步骤530，业务客户端获取注册时所采用生物认证类型的用户的生物数据，将生物数据携带在本地生物认证请求中发送给生物认证中间件，生物认证中间件将本地生物认证请求转发给生物认证客户端，生物认证客户端利用其中的生物数据对用户身份进行生物特征校验并将校验结果在本地生物认证响应中返回给生物认证中间件，生物认证中间件将本地生物认证响应返回给业务客户端。

[0109] 业务客户端按照在身份注册流程中已确定的生物认证类型向用户请求、并获取用户提供的该生物认证类型的生物数据。业务客户端将用户的生物数据封装在本地生物认证请求中发送给生物认证中间件，生物认证中间件将本地生物认证请求转发给生物认证客户端。

[0110] 生物认证客户端利用生物认证请求中的生物数据对用户身份进行生物特征校验。在校验完成后，生物认证客户端将是否通过的校验结果封装在本地生物认证响应中返回给生物认证中间件，生物认证中间件将本地生物认证响应返回给业务客户端。

[0111] 在用户设备上，步骤540，在本地生物特征校验结果为通过时，业务客户端将认证信息响应报文发送给生物认证中间件，生物认证中间件将认证信息响应报文转发给生物认证客户端；生物认证客户端将认证信息响应报文转发给身份认证检验器，身份认证检验器采用服务器公钥对认证信息响应报文进行验签，在验签通过后从令牌及密钥管理器获取与用户最近一次通过本地生物校验时所采用生物数据对应的生物特征令牌，在保存的虚拟账户标识、生物认证类型、生物特征令牌、和业务私钥的对应关系中获取与该生物认证类型、认证信息响应报文中的虚拟账户标识和生物特征令牌对应的业务私钥，将设备标识、虚拟账户标识、生物认证类型和生物特征令牌封装在认证请求报文中，并采用业务私钥对认证请求报文签名后，返回给生物认证客户端；生物认证客户端将认证请求报文返回给生物认证中间件，生物认证中间件将认证请求报文返回给业务客户端。

[0112] 业务客户端从生物认证中间件返回的本地生物认证响应中提取本地生物特征校验结果，如果结果为未通过，则身份认证流程以失败结束。当本地生物特征校验结果为通过时，业务客户端将认证信息响应报文发送给生物认证中间件，生物认证中间件将认证信息响应报文转发给生物认证客户端；生物认证客户端将认证信息响应报文转发给身份认证检验器。

[0113] 身份认证检验器从认证信息响应报文中提取服务器公钥，采用该服务器公钥对认证信息响应报文进行验签，如果验签未通过，则说明认证信息响应报文很可能并非来自于可靠的认证服务器，认证流程以失败结束。在验签通过后，身份认证检验器向令牌及密钥管理器请求生物特征令牌。令牌及密钥管理器将与用户最近一次通过本地生物校验时所采用生物数据(即业务客户端在步骤530中用来进行本地生物特征校验时所获取的生物数据)对

应的生物特征令牌返回给身份认证检验器。

[0114] 身份认证检验器将用户设备的设备标识、从认证信息响应报文中提取的虚拟账户标识、最近一次本地生物特征校验成功时采用的生物认证类型和令牌及密钥管理器返回的生物特征令牌封装在认证请求报文中。身份认证检验器在保存的虚拟账户标识、生物认证类型、生物特征令牌、和业务私钥的对应关系中，查找到与最近一次本地生物特征校验成功时所采用的生物认证类型、认证信息响应报文中的虚拟账户标识和令牌及密钥管理器返回的生物特征令牌对应的业务私钥，采用该业务私钥对认证请求报文签名后，返回给生物认证客户端。

[0115] 生物认证客户端将认证请求报文返回给生物认证中间件，生物认证中间件将认证请求报文返回给业务客户端。

[0116] 在用户设备上，步骤550，业务客户端将认证请求报文发送业务服务器，认证请求报文由业务服务器转发给认证服务器，供认证服务器根据与虚拟账户标识、设备标识和生物认证类型对应的已注册生物特征令牌和已注册业务公钥对用户进行身份认证。

[0117] 在认证服务器上，步骤620，从业务服务器接收来自用户设备的认证请求报文，认证请求报文中包括用户设备的设备标识、虚拟账户标识、生物认证类型和生物特征令牌，并采用业务私钥进行签名；获取与认证请求报文中的设备标识、虚拟账户标识和生物认证类型对应的已注册生物特征令牌和已注册业务公钥。

[0118] 在认证服务器上，步骤630，采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证。

[0119] 业务客户端将生物认证中间件返回的认证请求报文发送给业务服务器。业务服务器将认证请求报文转发给认证服务器。认证服务器在保存的已注册的设备标识、已注册的虚拟账户标识、已注册的生物认证类型、已注册的生物特征令牌和已注册的业务公钥的对应关系中，查找与认证请求报文中虚拟账户标识、设备标识和生物认证类型对应的已注册生物特征令牌和已注册业务公钥。

[0120] 认证服务器比对认证请求报文中的生物特征令牌与已注册生物特征令牌，并采用已注册业务公钥对认证请求报文进行验签。如果两个生物特征令牌不同、或者验签未通过，认证服务器拒绝认证请求并通知业务服务器，由业务服务器将认证失败的结果通知业务客户端。如果两个生物特征令牌相同并且验签通过，用户通过身份认证，认证服务器将身份认证通过的结果在认证响应报文中回复给业务服务器。业务服务器可以基于身份认证通过的结果进行相应的业务处理，并将身份认证通过的结果和/或业务处理的结果通知业务客户端。

[0121] 在一种实现方式中，认证服务器可以在收到认证信息请求报文后，生成对应于认证信息请求报文中设备标识的虚拟账户的认证挑战码。认证服务器将虚拟账户标识、服务器公钥和所生成的认证挑战码封装在认证信息响应报文中发送给业务服务器，并启动计时。在生成认证请求报文时，用户设备上的身份认证检验器将认证信息响应报文中的认证挑战码也封装在认证请求报文中。认证服务器收到业务服务器转发的认证请求报文后，比对认证请求报文中的认证挑战码和为认证请求报文中虚拟账户生成的认证挑战码，并获取发送认证信息响应报文和收到认证请求报文的时间差。如果两个认证挑战码不同或者该时间差超过第二预定时长，认证服务器拒绝认证请求并通知业务服务器，由业务服务器将认

证失败的结果通知业务客户端;如果两个认证挑战码相同并且该时间差不超过第二预定时长,采用已注册业务公钥对认证请求报文进行验签,并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证。

[0122] 本实施例的一种包括认证挑战码的实现方式中,用户设备的各个功能模块、业务服务器、认证服务器与生物认证中心服务器之间的交互流程如图7所示。

[0123] 本说明书的实施例二中,采用服务器公钥和服务器私钥来对业务服务器进行验证,采用业务私钥和已注册的业务公钥来对用户设备进行验证,并且用户设备需要提供与已注册信息匹配的设备标识、虚拟账户标识、生物认证类型和生物特征令牌才能通过认证,使得身份认证过程具有极高的安全性。

[0124] 在上述两个实施例中,可以将身份认证检验器和令牌及密钥管理器运行在用户设备上的安全环境中,以增加注册和认证过程的安全程度。例如,可以将身份认证检验器、令牌及密钥管理器与其他软件模块(如进程或线程)隔离运行并且不允许其他软件模块访问其缓存空间(这两个模块也相互隔离运行并且禁止相互访问缓存空间);再如,可以将身份认证检验器、令牌及密钥管理器的代码和存储的文件保存在用户设备上安全程度最高、访问控制最为严格的存储区域。

[0125] 与上述流程实现对应,本说明书的实施例还提供了一种应用在用户设备上的基于生物特征的身份注册装置、一种应用在认证服务器上的基于生物特征的身份注册装置、一种应用在用户设备上的基于生物特征的身份认证装置、和一种应用在认证服务器上的基于生物特征的身份认证装置。上述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,是通过用户设备或认证服务器的CPU(Central Process Unit,中央处理器)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8所示的CPU、内存以及非易失性存储器之外,用户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,认证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。

[0126] 图9所示为本说明书实施例提供的一种基于生物特征的身份注册装置,应用在用户设备上,包括用户注册信息单元、注册生物数据单元、注册生物令牌单元和用户注册请求单元,其中:用户注册信息单元用于向业务服务器发送包括用户的业务账户标识的注册信息请求报文,接收业务服务器返回的注册信息响应报文;所述注册信息响应报文中包括认证服务器在收到业务服务器转发的注册信息请求报文后生成的对应于所述业务账户标识的虚拟账户标识;注册生物数据单元用于获取所述用户的生物数据,采用所述生物数据对用户身份进行生物特征校验;注册生物令牌单元用于在生物特征校验结果为通过时,获取与所采用的生物数据对应的生物特征令牌;用户注册请求单元用于将虚拟账户标识、用户设备的设备标识、和生物特征令牌封装在注册请求报文中,发送给业务服务器;供认证服务器在收到业务服务器转发的注册请求报文后,保存所述虚拟账户标识、设备标识和生物特征令牌的对应关系,以用来对所述用户的账户进行身份认证。

[0127] 可选的,所述用户设备上保存有设备私钥;所述用户注册请求单元具体用于:将虚拟账户标识、用户设备的设备标识、和生物特征令牌封装在注册请求报文中,采用设备私钥对注册请求报文进行签名后,发送给业务服务器。

[0128] 可选的,所述装置还包括:生物类型确定单元,用于确定用户的生物认证类型;所

述注册生物数据单元获取用户的生物数据，包括：获取所述生物认证类型的用户的生物数据；所述注册请求报文中还包括：生物认证类型，供认证服务器在收到业务服务器转发的注册请求报文后，保存所述虚拟账户标识、设备标识、生物特征令牌和生物认证类型的对应关系，以用来对所述用户的账户进行身份认证。

[0129] 可选的，所述注册信息响应报文中还包括：服务器公钥；所述注册响应报文由认证服务器采用与所述服务器公钥对应的服务器私钥进行签名；所述注册生物令牌单元具体用于：在收到注册信息响应报文后，采用所述服务器公钥对所述注册信息响应报文进行验签，在验签通过并且生物特征校验结果为通过时，获取与所采用的生物数据对应的生物特征令牌。

[0130] 可选的，所述装置还包括：业务密钥生成单元，用于在获取生物特征令牌后，生成相对应的业务公钥和业务私钥，保存虚拟账户标识、生物认证令牌和业务私钥的对应关系；所述注册请求报文中还包括：业务公钥，供认证服务器在收到业务服务器转发的注册请求报文后，保存所述虚拟账户标识、设备标识、生物特征令牌和业务公钥的对应关系，以用来对所述用户的账户进行身份认证。

[0131] 可选的，所述注册信息响应报文中还包括：认证服务器生成的所述虚拟账户的注册挑战码；所述注册请求报文中还包括：所述注册挑战码，供认证服务器在收到业务服务器转发的注册请求报文后，根据所述注册挑战码以及发送注册信息响应报文和收到注册请求报文的时间间隔，对注册请求报文进行验证。

[0132] 图10所示为本说明书实施例提供的一种基于生物特征的身份注册装置，应用在认证服务器上，包括注册信息响应单元、注册请求接收单元和注册信息保存单元，其中：注册信息响应单元用于从业务服务器接收来自用户设备的注册信息请求报文，所述注册信息请求报文中包括业务账户标识；生成对应于所述业务账户标识的虚拟账户标识，将虚拟账户标识封装在注册信息响应报文中发送给业务服务器，供业务服务器将注册信息响应报文转发给用户设备；注册请求接收单元用于从业务服务器接收来自用户设备的注册请求报文，所述注册请求报文中包括虚拟账户标识、用户设备的设备标识、和用户的生物特征令牌；注册信息保存单元用于保存所述虚拟账户标识、设备标识和生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

[0133] 可选的，所述注册请求报文采用所述用户设备的设备私钥进行签名；所述装置还包括：设备密钥验签单元，用于将所述注册请求报文发送给生物认证中心服务器，接收生物认证中心服务器采用所述设备标识对应的设备公钥对注册请求报文进行验签后返回的验签结果；所述注册信息保存单元具体用于：在注册请求报文通过验签后，保存所述虚拟账户标识、设备标识和用户的生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

[0134] 可选的，所述注册请求报文中还包括：生物认证类型；所述注册信息保存单元具体用于：保存所述虚拟账户标识、设备标识、生物认证类型和用户的生物特征令牌的对应关系，以用来对所述用户的账户进行身份认证。

[0135] 可选的，所述装置还包括：服务器签名单元，用于采用服务器私钥对注册信息响应报文进行签名；所述注册信息响应报文中还包括：与所述服务器私钥相对应的服务器公钥，供用户设备用来对注册信息响应报文进行验签。

[0136] 可选的，所述注册请求报文中还包括：由用户设备生成的业务公钥，与保存在用户设备上的业务私钥相对应；所述注册信息保存单元具体用于：保存所述虚拟账户标识、设备标识、用户的生物特征令牌和业务公钥的对应关系，以用来对所述用户的账户进行身份认证。

[0137] 可选的，所述装置还包括：注册挑战码生成单元，用于生成所述虚拟账户的注册挑战码；所述注册信息响应报文中还包括：所生成的注册挑战码；所述注册请求报文中还包括：注册挑战码；所述注册信息保存单元具体用于：当注册请求报文中的注册挑战码与为注册请求报文中虚拟账户生成的注册挑战码相同、并且发送注册信息响应报文和收到注册请求报文的时间间隔在第一预定时长范围内时，保存所述虚拟账户标识、设备标识和用户的生物特征令牌的对应关系。

[0138] 图11所示为本说明书实施例提供的一种基于生物特征的身份认证装置，应用在用户设备上，包括认证信息用户单元、认证生物数据单元、认证生物令牌单元和用户认证请求单元，其中：认证信息用户单元用于向业务服务器发送包括用户设备的设备标识的认证信息请求报文，接收业务服务器返回的认证信息响应报文；所述认证信息响应报文由认证服务器在收到业务服务器转发的认证信息请求报文后生成，其中包括与所述设备标识对应的虚拟账户标识；认证生物数据单元用于获取用户的生物数据，采用所述生物数据对用户身份进行生物特征校验；认证生物令牌单元用于在通过生物特征校验后，获取与所述生物数据对应的生物特征令牌；用户认证请求单元用于向业务服务器发送认证请求报文，所述认证请求报文中包括所述虚拟账户标识和生物特征令牌，供认证服务器在收到业务服务器转发的认证请求报文后，根据与所述虚拟账户标识对应的已注册生物特征令牌对用户进行身份认证。

[0139] 可选的，所述用户的生物数据为用户注册时所采用的生物认证类型的生物数据；所述认证请求报文中还包括：所述生物认证类型，供认证服务器在收到业务服务器转发的认证请求报文后，根据与所述虚拟账户标识和生物特征类型对应的已注册生物特征令牌对用户进行身份认证。

[0140] 可选的，所述认证信息响应报文中还包括：服务器公钥；所述认证信息响应报文由认证服务器采用与所述服务器公钥对应的服务器私钥进行签名；所述装置还包括：服务器密钥验签单元，用于在收到认证信息响应报文后，采用所述服务器公钥对所述认证信息响应报文进行验签。

[0141] 可选的，所述用户设备上保存有与所述虚拟账户标识和生物特征令牌对应的业务私钥；所述装置还包括：业务密钥签名单元，用于采用所述业务私钥对认证请求报文进行签名，供认证服务器在收到业务服务器转发的认证请求报文后，根据与所述虚拟账户标识和对应的已注册业务公钥进行验签。

[0142] 可选的，所述认证信息响应报文中还包括：认证服务器生成的所述虚拟账户的认证挑战码；所述认证请求报文中还包括：所述认证挑战码，供认证服务器在收到认证请求报文后，根据所述认证挑战码以及发送认证信息响应报文和收到认证请求报文的时间间隔，对认证请求报文进行验证。

[0143] 图12所示为本说明书实施例提供的一种基于生物特征的身份认证装置，应用在认证服务器上，所述认证服务器保存有虚拟账户标识、设备标识和已注册生物特征令牌的对

应关系，所述装置包括认证信息响应单元、认证请求接收单元和身份认证单元，其中：认证信息响应单元用于从业务服务器接收来自用户设备的认证信息请求报文，所述认证信息请求报文中包括用户设备的设备标识；获取对应于所述设备标识的虚拟账户标识，将虚拟账户标识封装在认证信息响应报文中发送给业务服务器，供业务服务器将认证信息响应报文转发给用户设备；认证请求接收单元用于从业务服务器接收来自用户设备的认证请求报文，所述认证请求报文中包括虚拟账户标识和生物特征令牌；身份认证单元用于根据认证请求报文中的生物特征令牌、以及与认证请求报文中虚拟账户标识对应的已注册生物特征令牌对用户进行身份认证。

[0144] 可选的，所述认证服务器保存有虚拟账户标识、设备标识、生物认证类型和已注册生物特征令牌的对应关系；所述认证请求报文中还包括：生物认证类型；所述身份认证单元具体用于：根据认证请求报文中的生物认证类型和生物特征令牌、以及与认证请求报文中虚拟账户标识对应的生物认证类型和已注册生物特征令牌对用户进行身份认证。

[0145] 可选的，所述装置还包括：服务器密钥签名单元，用于采用服务器私钥对认证信息响应报文进行签名；所述认证信息响应报文中还包括：与所述服务器公钥相对应的服务器公钥，供用户设备用来对认证信息响应报文进行验签。

[0146] 可选的，所述认证服务器保存有虚拟账户标识、设备标识、已注册生物特征令牌和已注册业务公钥的对应关系；所述认证请求报文采用业务私钥进行签名；所述身份认证单元具体用于：在采用对应于所述虚拟账户标识的已注册业务公钥对所述认证请求报文进行验签并通过后，根据认证请求报文中的生物特征令牌、以及与认证请求报文中虚拟账户标识对应的已注册生物特征令牌对用户进行身份认证。

[0147] 可选的，所述装置还包括：认证挑战码生成单元，用于生成所述虚拟账户的认证挑战码；所述认证信息响应报文中还包括：所生成的认证挑战码；所述认证请求报文中还包括：认证挑战码；所述身份认证单元具体用于：当认证请求报文中的认证挑战码与为认证请求报文中虚拟账户生成的认证挑战码相同、并且发送认证信息响应报文和收到认证请求报文的时间间隔在第二预定时长范围内时，根据认证请求报文中的生物特征令牌、以及与认证请求报文中虚拟账户标识对应的已注册生物特征令牌对用户进行身份认证。

[0148] 本说明书的实施例提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施例中应用在用户设备上的基于生物特征的身份注册方法的各个步骤。

[0149] 本说明书的实施例提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施例中应用在认证服务器上的基于生物特征的身份注册方法的各个步骤。

[0150] 本说明书的实施例提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施例中应用在用户设备上的基于生物特征的身份认证方法的各个步骤。

[0151] 本说明书的实施例提供了一种计算机设备，该计算机设备包括存储器和处理器。

其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施例中应用在认证服务器上的基于生物特征的身份认证方法的各个步骤。

[0152] 本说明书的实施例提供了一种计算机可读存储介质，该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中应用在用户设备上的基于生物特征的身份注册方法的各个步骤。

[0153] 本说明书的实施例提供了一种计算机可读存储介质，该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中应用在认证服务器上的基于生物特征的身份注册方法的各个步骤。

[0154] 本说明书的实施例提供了一种计算机可读存储介质，该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中应用在用户设备上的基于生物特征的身份认证方法的各个步骤。

[0155] 本说明书的实施例提供了一种计算机可读存储介质，该存储介质上存储有计算机程序，这些计算机程序在被处理器运行时，执行本说明书实施例中应用在认证服务器上的基于生物特征的身份认证方法的各个步骤。

[0156] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本申请，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

[0157] 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。

[0158] 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。

[0159] 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。

[0160] 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。

[0161] 本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书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，本说明书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。

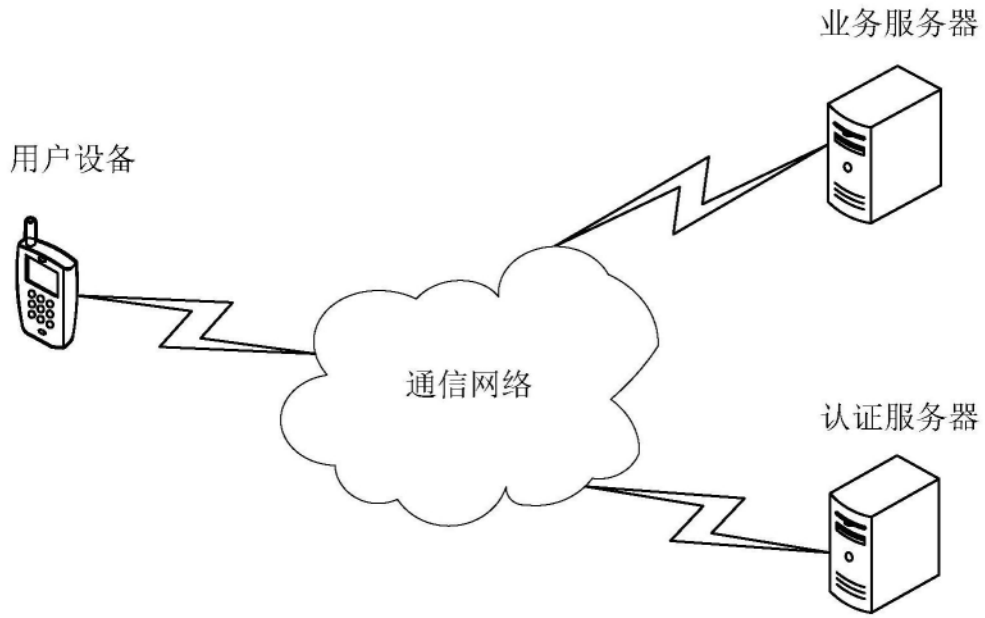


图1

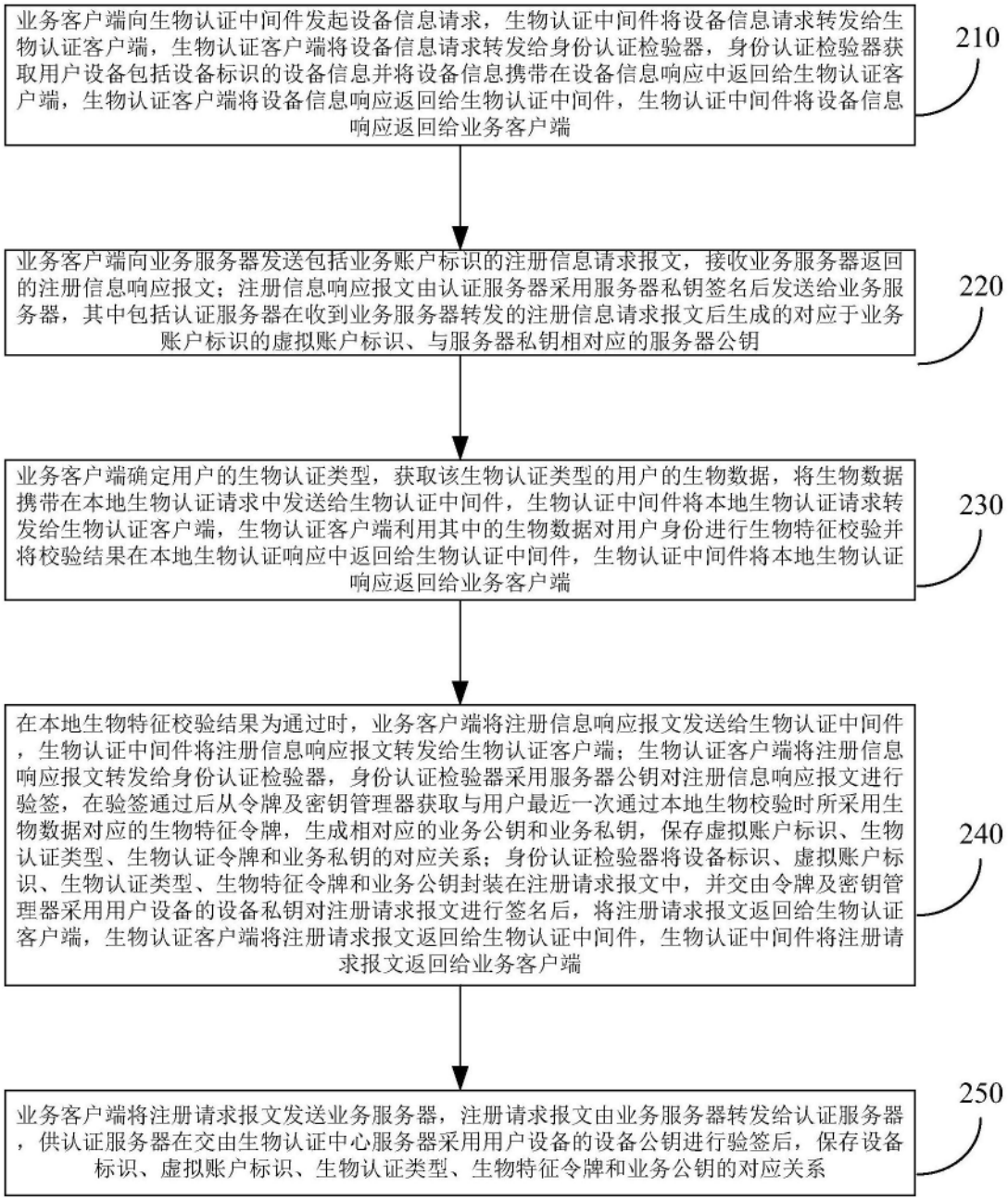

业务客户端向生物认证中间件发起设备信息请求，生物认证中间件将设备信息请求转发给生物认证客户端，生物认证客户端将设备信息请求转发给身份认证检验器，身份认证检验器获取用户设备包括设备标识的设备信息并将设备信息携带在设备信息响应中返回给生物认证客户端，生物认证客户端将设备信息响应返回给生物认证中间件，生物认证中间件将设备信息响应返回给业务客户端
210
业务客户端向业务服务器发送包括业务账户标识的注册信息请求报文，接收业务服务器返回的注册信息响应报文；注册信息响应报文由认证服务器采用服务器私钥签名后发送给业务服务器，其中包括认证服务器在收到业务服务器转发的注册信息请求报文后生成的对应于业务账户标识的虚拟账户标识、与服务器私钥相对应的服务器公钥
220
业务客户端确定用户的生物认证类型，获取该生物认证类型的用户的生物数据，将生物数据携带在本地生物认证请求中发送给生物认证中间件，生物认证中间件将本地生物认证请求转发给生物认证客户端，生物认证客户端利用其中的生物数据对用户身份进行生物特征校验并将校验结果在本地生物认证响应中返回给生物认证中间件，生物认证中间件将本地生物认证响应返回给业务客户端
230
在本地生物特征校验结果为通过时，业务客户端将注册信息响应报文发送给生物认证中间件，生物认证中间件将注册信息响应报文转发给生物认证客户端；生物认证客户端将注册信息响应报文转发给身份认证检验器，身份认证检验器采用服务器公钥对注册信息响应报文进行验签，在验签通过后从令牌及密钥管理器获取与用户最近一次通过本地生物校验时所采用生物数据对应的生物特征令牌，生成相对应的业务公钥和业务私钥，保存虚拟账户标识、生物认证类型、生物认证令牌和业务私钥的对应关系；身份认证检验器将设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥封装在注册请求报文中，并交由令牌及密钥管理器采用用户设备的设备私钥对注册请求报文进行签名后，将注册请求报文返回给生物认证客户端，生物认证客户端将注册请求报文返回给生物认证中间件，生物认证中间件将注册请求报文返回给业务客户端
240
业务客户端将注册请求报文发送业务服务器，注册请求报文由业务服务器转发给认证服务器，供认证服务器在交由生物认证中心服务器采用用户设备的设备公钥进行验签后，保存设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥的对应关系
250

图2

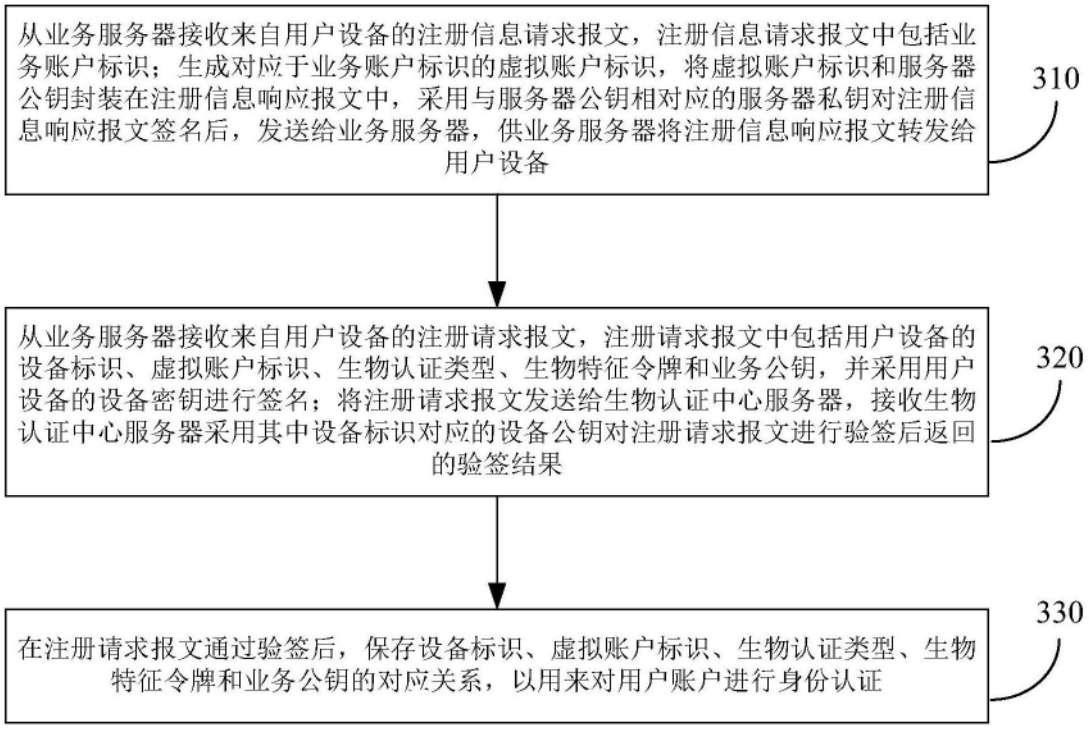

从业务服务器接收来自用户设备的注册信息请求报文，注册信息请求报文中包括业务账户标识；生成对应于业务账户标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在注册信息响应报文中，采用与服务器公钥相对应的服务器私钥对注册信息响应报文签名后，发送给业务服务器，供业务服务器将注册信息响应报文转发给用户设备
310
从业务服务器接收来自用户设备的注册请求报文，注册请求报文中包括用户设备的设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥，并采用用户设备的设备密钥进行签名；将注册请求报文发送给生物认证中心服务器，接收生物认证中心服务器采用其中设备标识对应的设备公钥对注册请求报文进行验签后返回的验签结果
320
在注册请求报文通过验签后，保存设备标识、虚拟账户标识、生物认证类型、生物特征令牌和业务公钥的对应关系，以用来对用户账户进行身份认证
330

图3

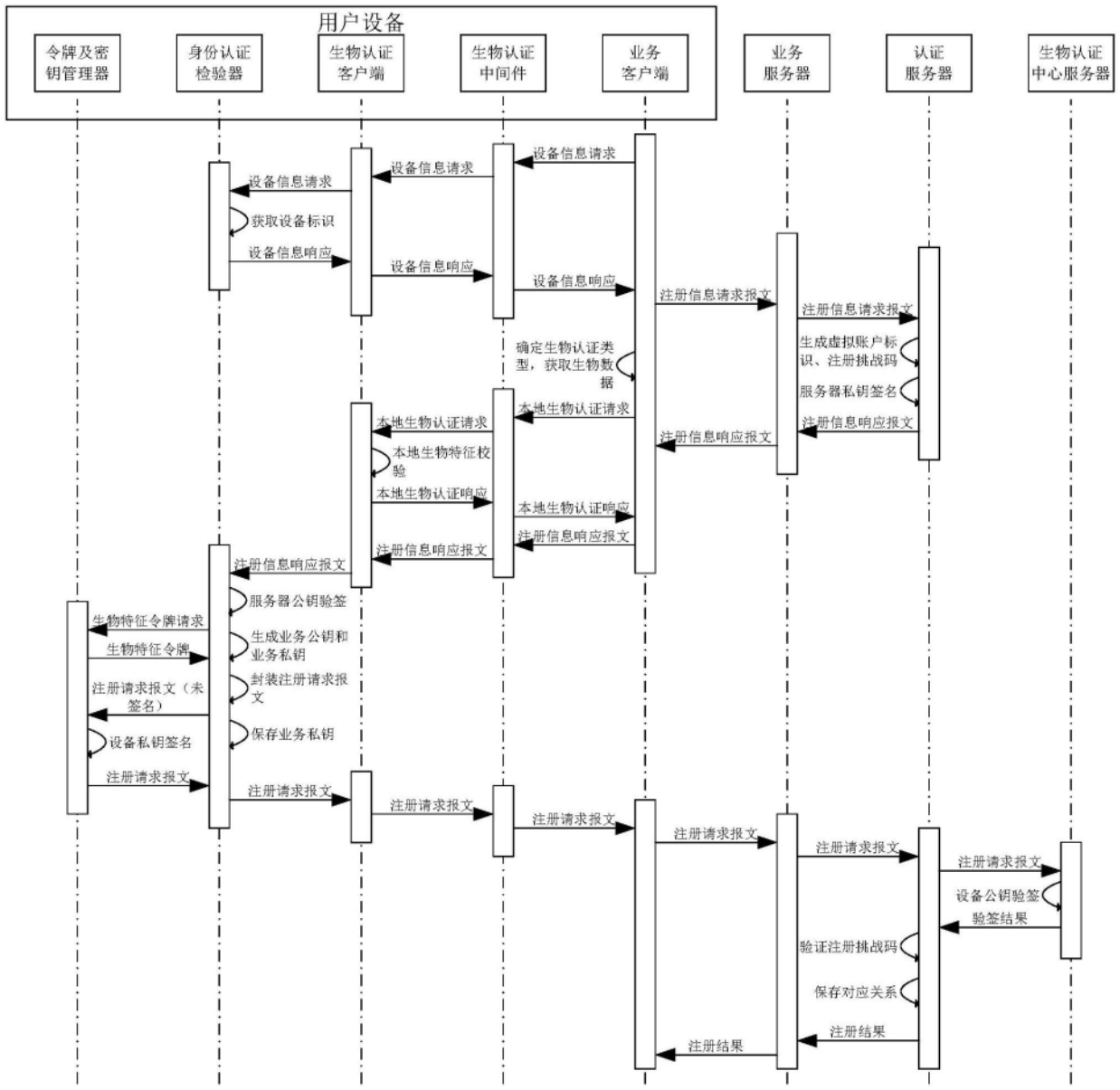

用户设备
令牌及密钥管理器
身份认证检验器
生物认证客户端
生物认证中间件
业务客户端
业务服务器
认证服务器
生物认证中心服务器
设备信息请求
设备信息响应
获取设备标识
注册信息请求报文
注册信息响应报文
生成虚拟账户标识、注册挑战码
服务器私钥签名
确定生物认证类型，获取生物数据
本地生物认证请求
本地生物特征校验
本地生物认证响应
服务器公钥验签
生物特征令牌请求
生物特征令牌
生成业务公钥和业务私钥
封装注册请求报文
注册请求报文（未签名）
保存业务私钥
设备私钥签名
注册请求报文
设备公钥验签
验签结果
验证注册挑战码
保存对应关系
注册结果

图4

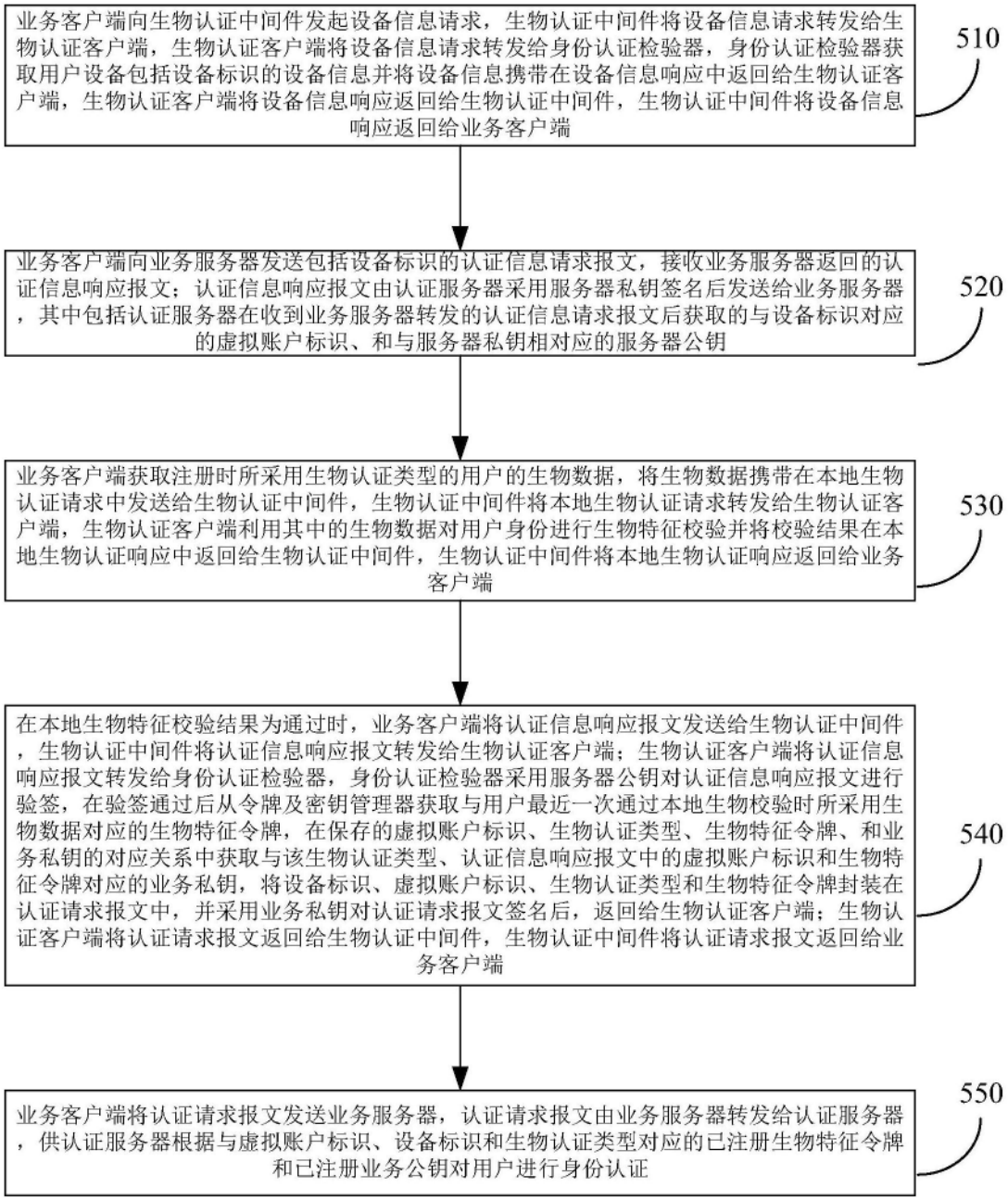

业务客户端向生物认证中间件发起设备信息请求，生物认证中间件将设备信息请求转发给生物认证客户端，生物认证客户端将设备信息请求转发给身份认证检验器，身份认证检验器获取用户设备包括设备标识的设备信息并将设备信息携带在设备信息响应中返回给生物认证客户端，生物认证客户端将设备信息响应返回给生物认证中间件，生物认证中间件将设备信息响应返回给业务客户端
510
业务客户端向业务服务器发送包括设备标识的认证信息请求报文，接收业务服务器返回的认证信息响应报文；认证信息响应报文由认证服务器采用服务器私钥签名后发送给业务服务器，其中包括认证服务器在收到业务服务器转发的认证信息请求报文后获取的与设备标识对应的虚拟账户标识、和与服务器私钥相对应的服务器公钥
520
业务客户端获取注册时所采用生物认证类型的用户的生物数据，将生物数据携带在本地生物认证请求中发送给生物认证中间件，生物认证中间件将本地生物认证请求转发给生物认证客户端，生物认证客户端利用其中的生物数据对用户身份进行生物特征校验并将校验结果在本地生物认证响应中返回给生物认证中间件，生物认证中间件将本地生物认证响应返回给业务客户端
530
在本地生物特征校验结果为通过时，业务客户端将认证信息响应报文发送给生物认证中间件，生物认证中间件将认证信息响应报文转发给生物认证客户端；生物认证客户端将认证信息响应报文转发给身份认证检验器，身份认证检验器采用服务器公钥对认证信息响应报文进行验签，在验签通过后从令牌及密钥管理器获取与用户最近一次通过本地生物校验时所采用生物数据对应的生物特征令牌，在保存的虚拟账户标识、生物认证类型、生物特征令牌、和业务私钥的对应关系中获取与该生物认证类型、认证信息响应报文中的虚拟账户标识和生物特征令牌对应的业务私钥，将设备标识、虚拟账户标识、生物认证类型和生物特征令牌封装在认证请求报文中，并采用业务私钥对认证请求报文签名后，返回给生物认证客户端；生物认证客户端将认证请求报文返回给生物认证中间件，生物认证中间件将认证请求报文返回给业务客户端
540
业务客户端将认证请求报文发送业务服务器，认证请求报文由业务服务器转发给认证服务器，供认证服务器根据与虚拟账户标识、设备标识和生物认证类型对应的已注册生物特征令牌和已注册业务公钥对用户进行身份认证
550

图5

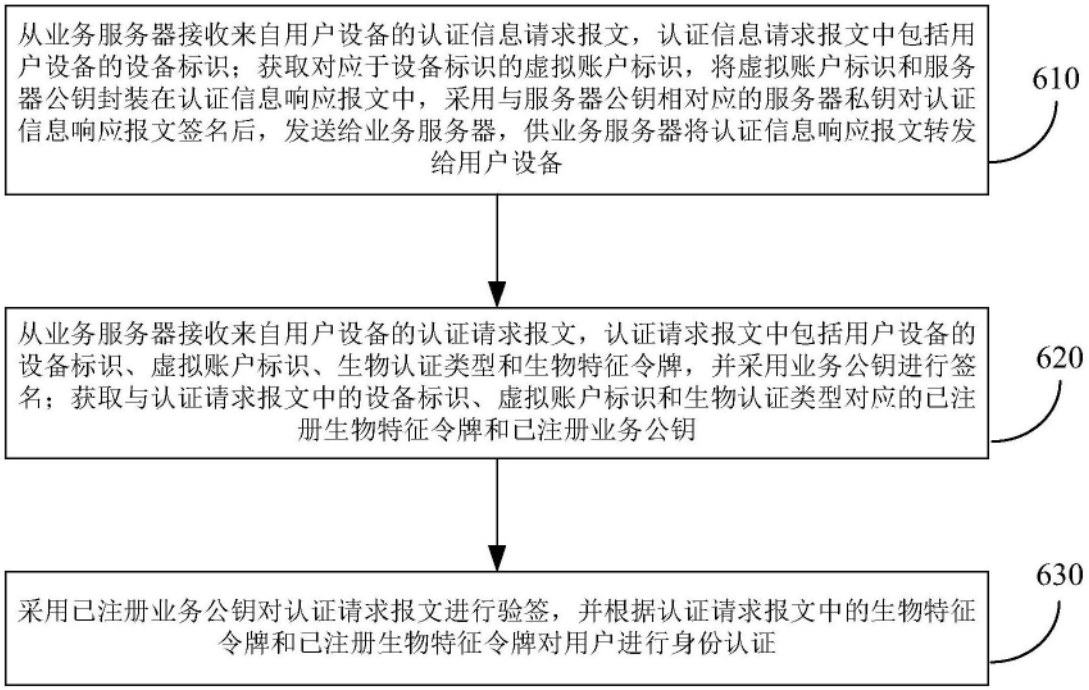

从业务服务器接收来自用户设备的认证信息请求报文，认证信息请求报文中包括用户设备的设备标识；获取对应于设备标识的虚拟账户标识，将虚拟账户标识和服务器公钥封装在认证信息响应报文中，采用与服务器公钥相对应的服务器私钥对认证信息响应报文签名后，发送给业务服务器，供业务服务器将认证信息响应报文转发给用户设备
610
从业务服务器接收来自用户设备的认证请求报文，认证请求报文中包括用户设备的设备标识、虚拟账户标识、生物认证类型和生物特征令牌，并采用业务公钥进行签名；获取与认证请求报文中的设备标识、虚拟账户标识和生物认证类型对应的已注册生物特征令牌和已注册业务公钥
620
采用已注册业务公钥对认证请求报文进行验签，并根据认证请求报文中的生物特征令牌和已注册生物特征令牌对用户进行身份认证
630

图6

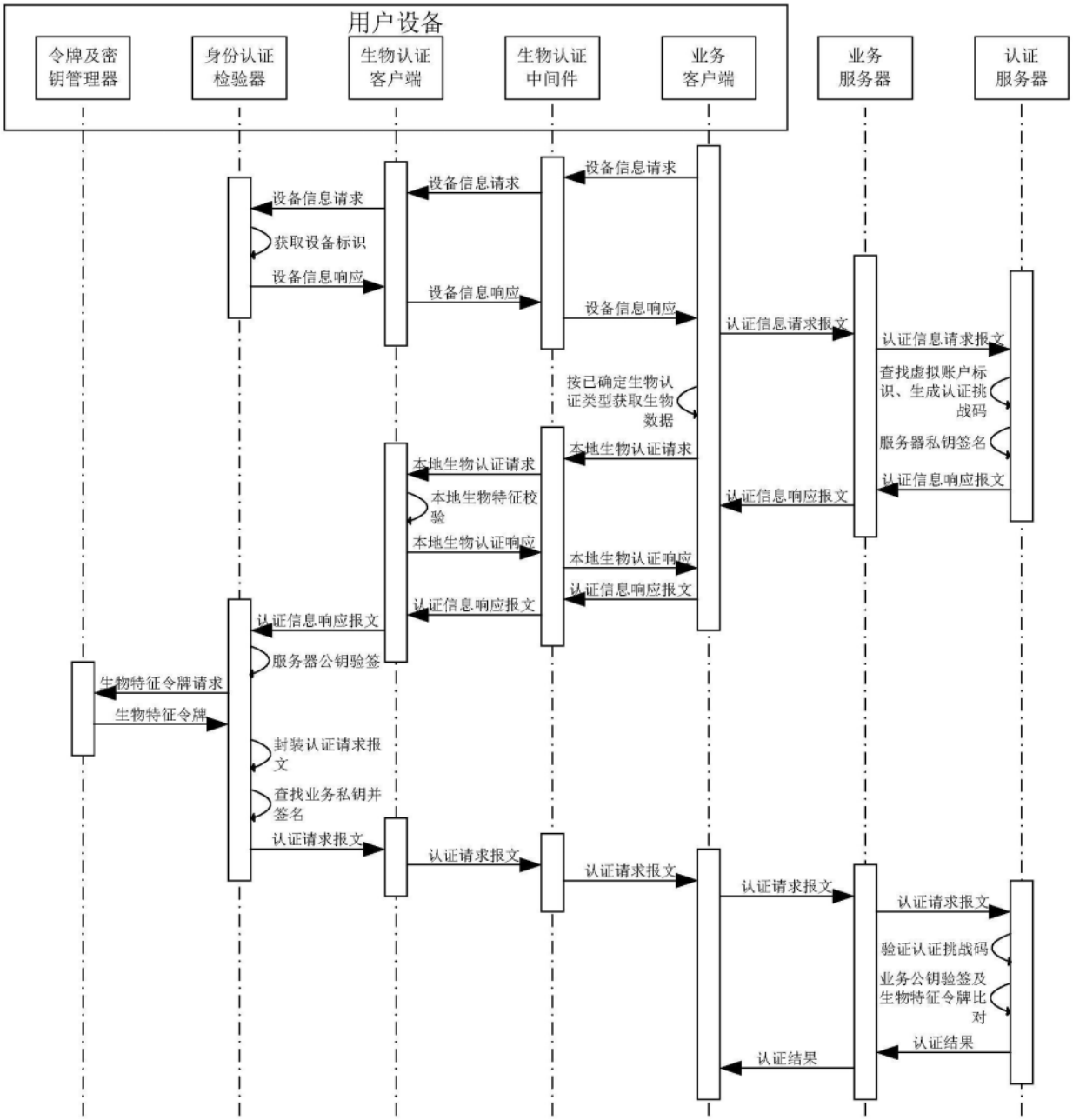

用户设备
令牌及密钥管理器
身份认证检验器
生物认证客户端
生物认证中间件
业务客户端
业务服务器
认证服务器
设备信息请求
设备信息请求
设备信息请求
获取设备标识
设备信息响应
设备信息响应
设备信息响应
认证信息请求报文
认证信息请求报文
按已确定生物认证类型获取生物数据
查找虚拟账户标识、生成认证挑战码
服务器私钥签名
本地生物认证请求
本地生物认证请求
认证信息响应报文
本地生物特征校验
本地生物认证响应
本地生物认证响应
认证信息响应报文
认证信息响应报文
认证信息响应报文
服务器公钥验签
生物特征令牌请求
生物特征令牌
封装认证请求报文
查找业务私钥并签名
认证请求报文
认证请求报文
认证请求报文
认证请求报文
认证请求报文
验证认证挑战码
业务公钥验签及生物特征令牌比对
认证结果
认证结果

图7

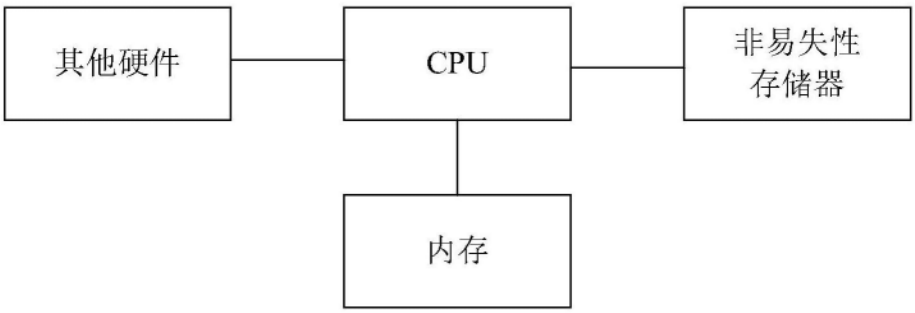


图8

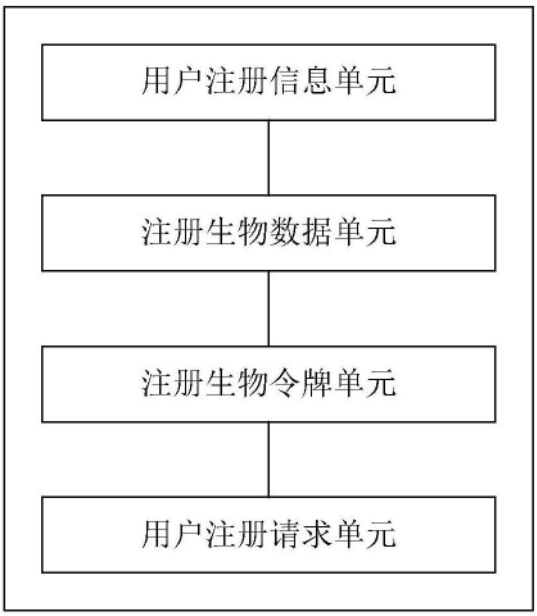


图9

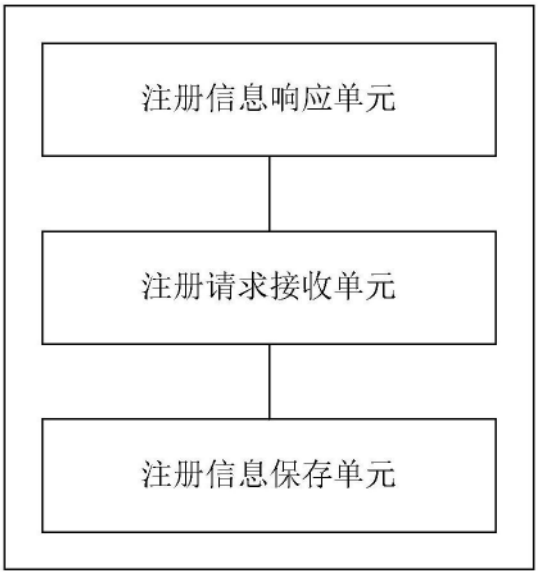

注册信息响应单元
注册请求接收单元
注册信息保存单元

图10

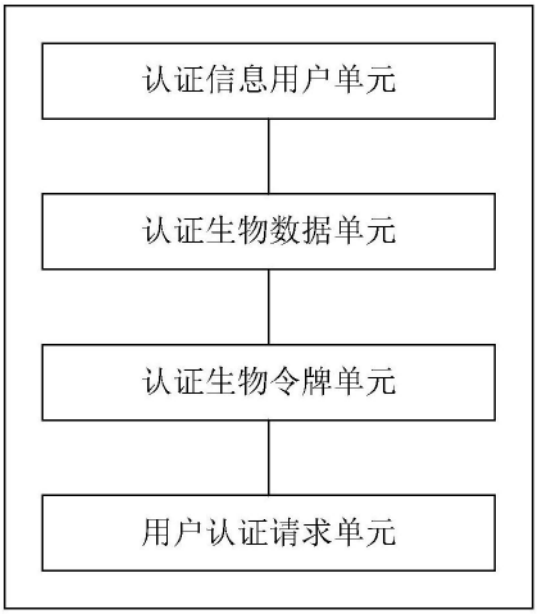

认证信息用户单元
认证生物数据单元
认证生物令牌单元
用户认证请求单元

图11

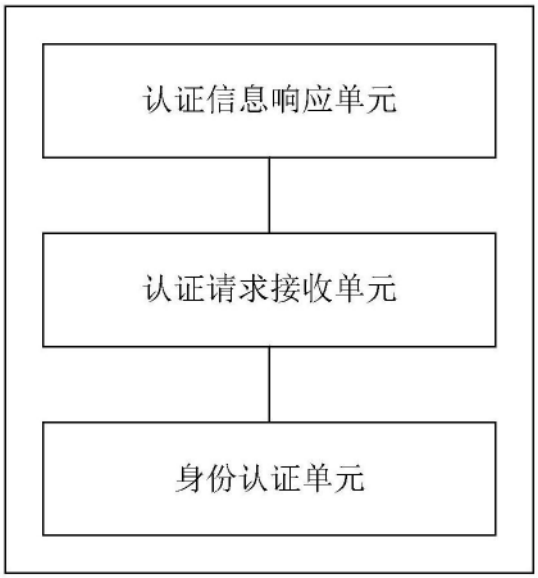


图12