



(12)发明专利申请

(10)申请公布号 CN 108964921 A

(43)申请公布日 2018.12.07

(21)申请号 201810520186.1

(22)申请日 2018.05.28

(30)优先权数据

10-2017-0065578 2017.05.26 KR

(71)申请人 三星SDS株式会社

地址 韩国首尔市

(72)发明人 朴贤哲 曹宰赫 梁熙星 申铉培

(74)专利代理机构 北京铭硕知识产权代理有限公司 11286

代理人 姜长星 张川绪

(51)Int.Cl.

H04L 9/32(2006.01)

H04L 29/06(2006.01)

G06K 7/10(2006.01)

权利要求书2页 说明书9页 附图5页

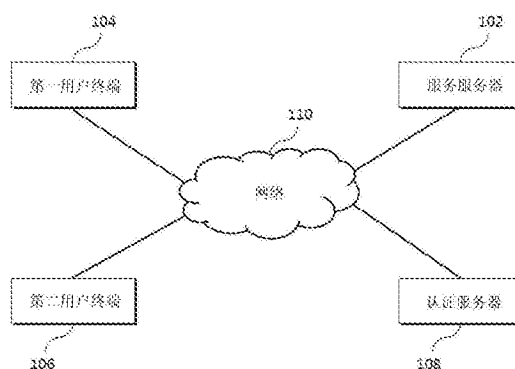
(54)发明名称

认证系统、认证方法和服务服务器

(57)摘要

本发明涉及一种认证系统、认证方法和服务服务器。根据本发明的实施例的认证系统包括：服务服务器，根据用户的认证请求而从认证服务器接收第一认证请求消息，并将包含在所述第一认证请求消息中的随机数转换为光学代码；第一用户终端，从所述服务服务器接收所述光学代码，并显示所述光学代码；以及，第二用户终端，通过根据从所述服务服务器接收第二认证请求消息而拍摄显示的所述光学代码而识别出所述随机数，并利用所述随机数、所述第二认证请求消息以及所述用户的生物信息来认证所述用户。

100



1. 一种认证系统,其中,包括:

服务服务器,根据用户的认证请求而从认证服务器接收第一认证请求消息,并将包含在所述第一认证请求消息中的随机数转换为光学代码;

第一用户终端,从所述服务服务器接收所述光学代码,并显示所述光学代码;以及

第二用户终端,通过根据从所述服务服务器接收第二认证请求消息而拍摄显示的所述光学代码而识别出所述随机数,利用所述随机数、所述第二认证请求消息以及所述用户的生物信息来认证所述用户。

2. 如权利要求1所述的认证系统,其中,所述服务服务器通过从所述第一认证请求消息中排除所述随机数而生成所述第二认证请求消息。

3. 如权利要求2所述的认证系统,其中,所述第二用户终端通过将识别出的所述随机数添加到所述第二认证请求消息,来获取所述第一认证请求。

4. 如权利要求1所述的认证系统,其中,所述光学代码包括二维码和条形码中的一种以上。

5. 如权利要求1所述的认证系统,其中,所述第二用户终端是移动设备。

6. 一种认证方法,其中,包括如下步骤:

在服务服务器,根据用户的认证请求而从认证服务器接收第一认证请求消息;

在所述服务服务器,将包含在所述第一认证请求消息中的随机数转换为光学代码;

在第一用户终端,显示所述光学代码;

在第二用户终端,通过根据从所述服务服务器接收第二认证请求消息而拍摄显示的所述光学代码而识别所述随机数;以及

在第二用户终端,利用所述随机数、所述第二认证请求消息以及所述用户的生物信息来认证所述用户。

7. 如权利要求6所述的认证方法,其中,还包括如下的步骤:

在所述服务服务器,通过从所述第一认证请求消息排除所述随机数而生成所述第二认证请求消息。

8. 如权利要求7所述的认证方法,其中,

在认证所述用户的步骤之前,还包括如下的步骤:

在所述第二用户终端,通过将识别出的所述随机数添加到所述第二认证请求消息,来获取所述第一认证请求消息。

9. 如权利要求6所述的认证方法,其中,所述光学代码包括二维码和条形码中的一个以上。

10. 如权利要求6所述的认证方法,其中,所述第二用户终端是移动设备。

11. 一种服务服务器,其中,包括:

数据接收部,根据用户的认证请求,从认证服务器接收第一认证请求消息;

数据处理部,将包含在所述第一认证请求消息中的随机数转换为光学代码,并通过从所述第一认证请求消息排除所述随机数而生成第二认证请求消息;以及

数据传输部,向第一用户终端和第二用户终端分别传输所述光学代码以及所述第二请求消息。

12. 如权利要求11所述的服务服务器,其中,所述光学代码包括二维码和条形码中的一

个以上。

13. 如权利要求11所述的服务服务器,其中,所述第二用户设备为移动设备。

14. 一种服务服务器的认证方法,其中,包括如下的步骤:

根据用户的认证请求,从认证服务器接收第一认证请求消息;

将包含在所述第一认证请求消息中的随机数转换为光学代码;

通过从所述第一认证请求消息中排除所述随机数而生成第二认证请求消息;以及

向第一用户终端和第二用户终端分别传输所述光学代码以及所述第二认证请求消息。

15. 如权利要求14所述的认证方法,其中,所述光学代码包括二维码和条形码中的一个以上。

16. 如权利要求14所述的认证方法,其中,所述第二用户设备为移动设备。

认证系统、认证方法和服务服务器

技术领域

[0001] 本发明涉及一种线上快速身份认证(FIDO:Fast Identity Online)技术。

背景技术

[0002] FIDO认证表示利用指纹、虹膜、面部信息等用户的生物信息来认证用户的技术。与使用用户的ID和密码的现有的认证方式相比,FIDO认证具有安全、方便的优点。

[0003] 通常,在这种FIDO认证技术中,利用FIDO私钥对在用户终端通过认证用户的生物信息而生成的认证消息和从FIDO服务器传递的随机数进行电子签名而生成签名值,而在FIDO服务器中利用FIDO公钥验证所述签名值,从而将其结果发送到服务服务器。

[0004] 然而,根据现有的FIDO认证技术,在从FIDO服务器向用户终端传递随机数的过程中,存在其随机数因恶意软件(malicious software)等而泄露的风险,在此情况下,提供要求较高的安全性的服务(例如,查看银行交易记录、信用卡支付等)时存在困难,并且会对用户产生巨大的危害。

[0005] [现有技术文献]

[0006] [专利文献]

[0007] 韩国公开专利公报第10-2013-0050039号(2013.05.15)

发明内容

[0008] 本发明的实施例用于在线上快速身份认证(FIDO:Fast Identity Online)过程中加强电子签名的安全性。

[0009] 根据本发明的示例性的实施例,提供一种认证系统,其包括:服务服务器,根据用户的认证请求而从认证服务器接收第一认证请求消息,并将包含在所述第一认证请求消息中的随机数转换为光学代码;第一用户终端,从所述服务服务器接收所述光学代码,并显示所述光学代码;以及,第二用户终端,通过根据从所述服务服务器接收第二认证请求消息而拍摄显示的所述光学代码而识别出所述随机数,并利用所述随机数、所述第二认证请求消息以及所述用户的生物信息来认证所述用户。

[0010] 所述服务服务器可以通过从所述第一认证请求消息中排除所述随机数而生成所述第二认证请求消息。

[0011] 所述第二用户终端可以将识别到的所述随机数添加到所述第二认证请求消息,来获取所述第一认证请求。

[0012] 所述光学代码包括二维码(QR code)和条形码中的一种以上。

[0013] 所述第二用户终端可以是移动设备。

[0014] 根据本发明的另一实施例,提供一种认证方法,其包括如下步骤:在服务服务器,根据用户的认证请求而从认证服务器接收第一认证请求消息;在所述服务服务器,将包含在所述第一认证请求消息中的随机数转换为光学代码;在第一用户终端,显示所述光学代码;在第二用户终端,通过根据从所述服务服务器接收第二认证请求消息而拍摄显示的所

述光学代码而识别出所述随机数;以及,在第二用户终端,利用所述随机数、所述第二认证请求消息以及所述用户的生物信息来认证所述用户。

[0015] 在所述认证方法中,在接收第一认证请求消息的步骤之后,还包括如下的步骤:在所述服务服务器,通过从所述第一认证请求消息中排除所述随机数而生成所述第二认证请求消息。

[0016] 在认证所述用户的步骤之前,还可以包括如下的步骤:在所述第二用户终端,将识别出的所述随机数添加到所述第二认证请求消息,从而获取所述第一认证请求消息。

[0017] 所述光学代码包括二维码(QR code)和条形码中的一种以上。

[0018] 所述第二用户终端可以是移动设备。

[0019] 根据本发明的另一实施例,提供一种服务服务器,其包括:数据接收部,根据用户的认证请求,从认证服务器接收第一认证请求消息;数据处理部,将包含在所述第一认证请求消息中的随机数转换为光学代码,并通过从所述第一认证请求消息中排除所述随机数而生成第二认证请求消息;以及,数据传输部,向第一用户终端和第二用户终端分别传输所述光学代码以及所述第二请求消息。

[0020] 所述光学代码包括二维码(QR code)和条形码中的一种以上。

[0021] 所述第二用户终端可以是移动设备。

[0022] 根据本发明的另一实施例,提供一种认证方法,其包括如下的步骤:在数据接收部,根据用户的认证请求,从认证服务器接收第一认证请求消息;在数据处理部,将包含在所述第一认证请求消息中的随机数转换为光学代码;在所述数据处理部,通过从所述第一认证请求消息中排除所述随机数而生成第二认证请求消息;以及,在数据传输部,向第一用户终端和第二用户终端分别传输所述光学代码以及所述第二请求消息。

[0023] 所述光学代码包括二维码(QR code)和条形码中的一种以上。

[0024] 所述第二用户终端可以是移动设备。

[0025] 根据本发明的实施例,服务服务器并非将认证过程所需要的数据按照原样传输给第一用户终端和第二用户终端,而是将所述数据分割后将分割的所述数据分别向第一用户终端和第二用户终端传输,从而能够提高认证过程的安全性。

[0026] 另外,根据本发明的实施例,通过第二用户终端所具有的光学模块来拍摄在第一用户终端显示的光学代码,从而能够容易地识别认证过程所需要的随机数,据此无需蓝牙模块等短距离无线通信模块的添加也能方便地确保与第一用户终端和第二用户终端之间的接近性(proximity)。

附图说明

[0027] 图1是示出根据本发明的一实施例的认证系统的详细构成的框图。

[0028] 图2是示出根据本发明的一实施例的服务服务器的详细构成的框图。

[0029] 图3是示出根据本发明的一实施例的第二用户终端的详细构成的框图。

[0030] 图4是用于说明根据本发明的一实施例的认证方法的流程图。

[0031] 图5是用于图示并说明适合在示例性的实施例中使用的包括计算装置的计算环境的框图。

[0032] 符号说明

[0033]	10:计算环境	12:计算装置
[0034]	14:处理器	16:计算机可读存储介质
[0035]	18:通信中线	20:程序
[0036]	22:输入输出接口	24:输入输出装置
[0037]	26:网络通信接口	100:认证系统
[0038]	102:服务服务器	104:第一用户终端
[0039]	106:第二用户终端	108:认证服务器
[0040]	110:网络	150:用户
[0041]	202:数据接收部	204:数据处理部
[0042]	206:数据传输部	302:认证单元
[0043]	304:认证客户端	306:服务模块
[0044]	308:光学模块	

具体实施方式

[0045] 以下,参阅附图而对本发明的具体实施形态进行说明。为了有助于对本说明书中记载的方法、装置和/或系统的全面理解,提供以下的详细说明。然而,这只是示例,本发明并非局限于此。

[0046] 在说明本发明的实施例的过程中,如果判断为对有关本发明的公知技术的具体说明有可能对本发明的要义造成不必要的混乱,则省略其具体说明。并且,后述的术语作为虑及本发明中的功能而定义的术语,其可能因使用者、运用者的意图或惯例等而不同。因此,要将贯穿整个说明书的内容作为基础而对其进行定义。具体说明中使用的术语仅用于记载本发明的实施例,其绝非限定性术语。除非明确不同地使用,否则单数形态的表述包括复数形态的含义。在说明中,“包括”或“具有”之类的表述用于指代某些特性、数字、步骤、操作、要素及其一部分或者组合,不应解释为将所记载项以外的一个或者其以上的其他特性、数字、步骤、操作、要素及其一部分或组合的存在性或者可存在性予以排除。

[0047] 图1是示出根据本发明的一实施例的认证系统100的详细构成的框图。如图1所示,根据本发明的一实施例的认证系统100包括服务服务器102、第一用户终端104、第二用户终端106以及认证服务器108,并且这些要素可以通过网络110而彼此连接。在此,网络110可以作为包括移动通信运营商所提供的3G网络、4G网络或LTE网络、WiBro网络等包通信网络以及有线/无线互联网的较宽的含义而使用。

[0048] 服务服务器102是用于向用户提供证券交易服务、银行交易服务等各种服务的装置,例如,可以是证券公司服务器、银行服务器、信用卡公司服务器、保险公司服务器等。服务服务器102可以向第一用户终端104和第二用户终端106提供服务模块(未示出),并且用户可以通过设置于第一用户终端104和第二用户终端106的服务模块而从服务服务器102接收各种服务。所述服务模块例如可以是证券公司应用、银行应用等。

[0049] 此时,服务服务器102、第一用户终端104、第二用户终端106和认证服务器108可以为了提供所述服务而执行针对所述用户的认证过程。在本实施例中,所述认证过程例如可以是FIDO认证过程。FIDO认证表示利用指纹、虹膜、面部信息等用户的生物信息来认证用户的技术。

[0050] 为此,第一用户终端104从用户接收认证请求(针对服务服务器102或者由服务服务器102提供的服务模块的登录请求),并将其传输给服务服务器102。服务服务器102从第一用户终端104接收用户的认证请求,并向认证服务器108传输所述用户的认证请求。所述用户的认证请求中可以包括诸如用户的姓名、ID、密码等用户信息以及与期望接收的服务相关的各种交易数据(transaction data)等。

[0051] 之后,服务服务器102可以从认证服务器108接收第一认证请求消息。所述第一认证请求消息可以包括一次性随机数、认证政策、所述交易数据等。所述随机数可以利用数字、文字或者这些的组合来构成,并从认证服务器108生成。并且,所述认证政策是与在认证用户时使用的认证单元(未示出)的种类、认证方法等相关的信息,其可以从认证服务器108生成。

[0052] 服务服务器102从认证服务器108接收第一认证请求消息,进而将包含在第一认证请求消息中的随机数转换为光学代码,并向第一用户终端104传输所述光学代码。在此,光学代码是能够存储设定的大小以内的信息(例如,数字最多为大约7000字,文字最多为大约4200字,二进制最多为大约2900字节等)的代码,例如,可以是二维码(QR code)、条形码等。

[0053] 并且,服务服务器102生成第二认证请求消息,并向第二用户终端106传输所述第二认证请求消息。此时,服务服务器102可以通过从第一认证请求消息中排除所述随机数而生成第二认证请求消息。第二认证请求消息例如可以包括认证政策、交易数据等。

[0054] 如上所述,服务服务器102可以向第一用户终端104和第二用户终端106分别传输与随机数对应的光学代码和排除了所述随机数的第二认证请求消息。即,服务服务器102并非将认证过程所需的数据按照原样传输给第一用户终端104和第二用户终端106,而是将所述数据分割后将分割的数据分别传输给第一用户终端104和第二用户终端106传输,从而能够提高认证过程的安全性。

[0055] 第一用户终端104是用于从服务服务器102接收各种服务(例如,诸如证券买卖等证券交易服务、诸如转账、查看余额、查看交易记录等银行交易服务等)的装置。在本实施例中,第一用户终端104例如可以是台式计算机等非移动(non-mobile)设备。然而本发明不限于此,第一用户终端104例如还可以是笔记本计算机、平板个人计算机、个人数字助理(PDA: Personal Digital Assistants)等移动设备。

[0056] 第一用户终端104可以从用户接收认证请求并将其传输给服务服务器102,并且可以从服务服务器102接收光学代码。之后,第一用户终端104可以通过显示模块(未示出)显示所述光学代码。

[0057] 第二用户终端106是用于执行针对所述用户的认证过程的装置,例如可以是智能电话、平板个人计算机、PDA、智能手表等可穿戴设备等。在本实施例中,第二用户终端106可以是用户可携带的移动设备。

[0058] 第二用户终端106可以从服务服务器102接收第二认证请求消息,并且响应于接收所述第二认证请求消息而向用户请求拍摄显示于第一用户终端104的光学代码。第二用户终端106可以根据用户的输入而通过安装或连接于第一用户终端104的光学模块来拍摄显示于第一用户终端104的光学代码,从而识别所述随机数。在此,光学模块是用于拍摄所述光学代码的装置,例如可以是相机、二维码阅读器、条形码阅读器等。

[0059] 并且,第二用户终端106可以通过所述随机数的识别来认证所述用户。具体地,第

二用户终端106可以将识别出的所述随机数添加到从服务服务器102接收的第二认证请求消息而获取第一认证请求消息,并利用所述第一认证请求消息和用户的生物信息来认证所述用户。

[0060] 作为一示例,第二用户终端106通过指纹传感器、面部识别器等认证单元(未示出)来认证用户的生物信息,并使包含在所述第一认证请求消息中的随机数和交易信息包含在表示所述认证结果的认证消息中,并利用预先存储的私钥对其进行电子签名,从而生成签名值。此时,第二用户终端106可以通过对包含所述随机数和和交易数据的认证消息进行哈希运算而获取第一哈希值,并利用私钥对所述第一哈希值进行加密,从而生成所述签名值。所述私钥例如可以是线上快速身份认证(FIDO:Fast Identity Online)私钥,可以从第二用户终端106生成。并且,第二用户终端106在进行用户认证之前参照包含在所述第一认证请求消息中的认证政策来确定用于用户的认证过程的认证单元的种类。

[0061] 之后,第二用户终端106可以向第一用户终端104传输所述认证消息以及签名值。第一用户终端可以将所述认证消息和签名值作为针对用户的认证请求的响应而向服务服务器102传输,并且服务服务器102可以向认证服务器108传输所述认证消息以及签名值。

[0062] 认证服务器108是用于认证用户的装置,例如,可以是FIDO服务器。认证服务器108根据用户的认证请求而生成一次性随机数,并且可以向服务服务器102传输包括所述随机数的第一认证请求消息。如上所述,第一认证请求消息例如可以包括一次性随机数、认证政策、交易数据等。

[0063] 并且,认证服务器108可以从服务服务器102接收认证消息以及签名值,并验证所述签名值。

[0064] 例如,认证服务器108可以利用已发布的公钥(即,对应于所述私钥的公钥)来验证所述签名值。所述公钥例如可以是FIDO公钥,其可以从第二用户终端106生成并发布至认证服务器108。

[0065] 之后,认证服务器108可以向服务服务器102传输认证结果,并且服务服务器102可以向第一用户终端104传输所述认证结果。

[0066] 如上所述,根据本发明的实施例,从服务服务器102分别向第一用户终端104和第二用户终端106传输与随机数对应的光学代码和排除所述随机数的第二认证请求消息,并且从第二用户终端106拍摄所述光学代码而识别所述随机数,从而获取所述第一认证请求消息,据此,能够从根源上阻断所述随机数在所述随机数的传递过程中泄露的风险。

[0067] 并且,根据本发明的实施例,通过第二用户终端106所具备的光学模块来拍摄显示于第一用户终端104的光学代码,从而能够容易地识别认证过程所需要的随机数。在此情况下,用户利用自身持有的第二用户终端106而方便地确保与第一用户终端104之间的接近性,并且无需为了确保第一用户终端104和第二用户终端106之间的接近性而在第一用户终端104设置蓝牙模块等近距离通信模块。

[0068] 即,根据本发明的实施例,在利用不同种类的设备(例如,台式计算机等非移动设备和只能电话等移动设备)进行认证过程时,无需单独地设置额外设备,仅通过设备的现有功能和模块即能够方便地执行认证过程。

[0069] 图2是示出根据本发明的一实施例的服务服务器102的详细构成的框图。如图2所示,根据本发明的一实施例的服务服务器102包括数据接收部202、数据处理部204和数据传

输部206。

[0070] 数据接收部202从认证服务器108接收第一认证请求消息。数据接收部202可以从第一用户终端104接收用户的认证请求,并且下述的数据传输部206可以向认证服务器108传输所述用户的认证请求。数据接收部202可以从认证服务器108接收作为所述用户的认证请求的响应的第一认证请求消息。

[0071] 数据处理部204将从认证服务器108接收的第一认证请求消息分割。具体地,数据处理部204将包含在所述第一认证请求消息中的随机数转换为光学代码,并通过从所述第一认证请求消息中排除所述随机数而生成第二认证请求消息。即,数据处理部204可以将所述第一认证请求消息分割为对应于随机数的光学代码和不包含所述随机数的第二认证请求消息。

[0072] 数据传输部206向第一用户终端104和第二用户终端106分别传输所述光学代码以及所述第二认证请求消息。据此,第一用户终端104可以显示所述光学代码,并且第二用户终端106可以拍摄显示于第一用户终端104的所述光学代码而识别出所述随机数。并且,如上所示,数据传输部206可随着数据接收部202从第一用户终端104接收用户的认证请求而将所述用户的认证请求向认证服务器108传输。

[0073] 图3是示出根据本发明的一实施例的第二用户终端106的详细构成的框图。如图3所示,根据本发明的一实施例的第二用户终端106包括认证单元302、认证客户端304、服务模块306和光学模块308。

[0074] 认证单元(Authenticator) 302是用于认证用户的生物信息的装置,例如,可以是指纹传感器、面部识别器、虹膜识别装置和语音识别装置等。认证单元302可以内置或贴附于第二用户终端106,但是不限于此,其还可以构成为与第二用户终端106分开的装置。并且,认证单元302可以发布一对私钥(例如,FIDO私钥)和公钥(例如,FIDO公钥)。所述私钥例如可以存储于认证单元302的内部数据库(未示出),并且所述第一公钥可以发布至认证服务器108。

[0075] 并且,认证单元302认证用户的生物信息,并使随机数和交易数据包含在表示所述认证结果的认证消息中,并通过存储的私钥对其进行签名。之后,认证单元302可以通过认证器特定模块(ASM:Authenticator Specific Module,未示出)而向认证客户端304传输认证消息以及签名值。

[0076] 认证客户端304是向认证单元302请求用户认证的模块,例如,可以是FIDO客户端。此时,认证客户端304可以参照包含在所述第一认证消息中的认证政策而确定将要用于用户的认证的认证单元的种类。

[0077] 认证客户端304可以向认证单元302请求用户认证,并向服务模块306传递从认证单元302接收的认证消息和签名值。

[0078] 服务模块306是从服务服务器102提供的应用软件,例如,可以是证券公司应用、银行应用等。服务模块306从服务服务器102接收第二认证请求消息,并向用户请求从第一用户终端104显示的光学代码的拍摄。

[0079] 并且,服务模块306根据用户的输入而与光学模块308联动,进而拍摄显示于第一用户终端104的光学代码,从而将拍摄到的光学代码转换为随机数。服务模块306可以向从服务服务器102接收的第二认证请求消息添加所述随机数而获取第一认证请求消息,并向

认证客户端304传输所述第一认证请求消息。认证客户端304随着从服务模块306接收所述第一认证请求消息,向认证单元302请求用户认证。

[0080] 并且,服务模块306可以从认证客户端304接收认证消息以及签名值,并向第一用户终端104传输所述认证消息以及签名值。

[0081] 光学模块308是用于拍摄显示于第一用户终端104的光学代码的装置,例如可以是相机、二维码阅读器(QR code reader)、条形码阅读器等。光学模块308可以与服务模块306联动而进行工作,并且服务模块306可以根据用户的输入而通过所述光学模块308拍摄显示于第一用户终端104的光学代码。

[0082] 图4是用于说明根据本发明的一实施例的认证方法的流程图。在以下图示的流程图中将所述方法分成了多个步骤而进行了记载,然而还可以由如下的方式来执行:至少一部分步骤交换顺序而执行;至少一部分步骤与其他步骤结合而一起执行;至少一部分步骤省略或分为细分化的步骤而执行;或者附加未图示的一个以上的步骤而执行。

[0083] 首先,第一用户终端104从用户150接收第一认证请求消息(S402)。

[0084] 之后,第一用户终端104向服务服务器102传输所述认证请求(S404)。

[0085] 之后,服务服务器102向认证服务器108传输所述认证请求(S406)。

[0086] 之后,认证服务器108生成一次性随机数(S408)。

[0087] 之后,认证服务器108向服务服务器102传输第一认证请求消息(S410)。如上所示,所述第一认证请求消息可以包括一次性随机数、认证政策、所述交易数据等。

[0088] 之后,服务服务器102向第一用户终端104传输第二认证请求消息(S412)。如上所述,服务服务器102可以通过从第一认证请求消息排除所述随机数而生成第二认证请求消息。第二认证请求消息例如可以包括认证政策、交易数据等。

[0089] 并且,服务服务器102将包含在第一认证请求消息中的随机数转换为光学代码(S414)。在图4中,为了便于说明,图示为在第S412步骤以后执行S414步骤,但是这仅仅是一示例,S414步骤还可以在S412步骤之前执行,或者与S412步骤同时执行。下述的S418步骤与S416步骤和S420步骤也不一定需要按图示于图4的顺序执行,将该顺序互换而执行也无妨。

[0090] 之后,服务服务器102向第一用户终端104传输光学代码(S416)。

[0091] 并且,第二用户终端106的服务模块308从服务服务器102接收第二认证请求消息,进而显示用于输入光学代码的画面(S418)

[0092] 之后,第一用户终端104在画面上显示光学代码(S420)。

[0093] 之后,服务服务器308向用户请求从第一用户终端104显示的光学代码的拍摄(S422)。例如,服务模块308可以在画面上显示用于请求光学代码的拍摄请求的消息。

[0094] 之后,服务模块308根据用户150的输入而与光学模块308联动,从而拍摄从第一用户终端104上显示的光学代码并将其识别(S424、S426)。

[0095] 之后,服务模块308将所述光学代码转换为随机数(S428)。第二用户终端106的服务模块308将所述随机数添加到从服务服务器102接收的第二认证请求消息中,从而获取第一认证请求消息。

[0096] 之后,服务模块308向认证客户端304传输所述第一认证请求消息(S430)。

[0097] 认证客户端304从服务模块308接收所述第一认证请求消息,进而向用户150请求确认生物信息(S432)。在一实施例中,认证客户端304可以输出用于输入指纹的通知消息。

[0098] 之后,认证客户端304与认证单元302联动而认证用户150的生物信息(S434)。作为一实施例,认证客户端304可以通过认证单元302而从用户150接收指纹信息并进行认证。

[0099] 之后,认证客户端304使包括在所述第一认证请求消息中的随机数和交易数据包含在用于表示所述认证结果的认证消息中,并利用预先存储的私钥来对其进行电子签名,从而生成签名值(S436)。

[0100] 之后,认证客户端304向服务模块308传输所述认证消息和签名值(S438)。

[0101] 之后,服务模块308向第一用户终端104传输所述认证消息及签名值(S440)。

[0102] 之后,第一用户终端104将所述认证消息和签名值作为针对用户的认证请求的响应而向服务服务器102传输(S442),并且服务服务器102向认证服务器108传输所述认证消息和签名值(S444)。

[0103] 之后,认证服务器108利用已发布的公钥来验证所述签名值(S446)。认证服务器108利用所述公钥而对所述签名值进行解密,从而获取上述的第一哈希值,并对认证消息(即,签名原文)进行哈希运算(hashing)而获取第二哈希值。认证服务器108可以将第一哈希值和第二哈希值比较,并在所述第一哈希值和第二哈希值相同的情况下判断为签名值的验证完成。

[0104] 如果完成签名值的验证,则认证服务器108向服务服务器102传输包括认证完成消息的认证结果(S448)。如果签名值的验证失败,则认证服务器108可以向服务服务器102传输包括认证失败消息的认证结果。

[0105] 之后,认证服务器108向第一用户终端传输所述认证结果(S450)。

[0106] 图5是用于图示并说明适合在示例性的实施例中使用的包括计算装置的计算环境的框图。在图示的实施例中,各个组件除了以下记载的功能以及能力以外还可具有其他不同的功能以及能力,并且除了以下记载的组件以外还可以包括追加的组件。

[0107] 图示的计算环境包括计算装置12。在一实施例中,计算环境12例如可以是认证系统100或者包含在认证系统中的一个以上的组成部分。

[0108] 计算装置12包括至少一个处理器14、计算机可读存储介质16以及通信总线18。处理器14可以使计算装置12根据前面提及的示例性的实施例而操作。例如,处理器14可以运行存储于计算机可读存储介质16中的一个以上的程序。所述一个以上的程序可以包括一个以上的计算机可执行指令,并且所述计算机可执行指令可以构成为,在通过处理器14执行的情况下使计算装置12执行根据示例性的实施例的操作。

[0109] 计算机可读存储介质16以能够存储计算机可执行的指令至程序代码、程序数据以及/或者其他适合的形式的信息的方式构成。存储于计算机可读存储介质16中的程序20包含可由处理器14执行的指令集。在一实施例中,计算机可读存储介质16可以是存储器(随机存取存储器等易失性存储器、非易失性存储器或者这些存储器的适合的组合形式)、一个以上的磁盘存储设备、光盘存储设备、闪速存储设备、除此之外的可由计算装置12访问并能够存储所期望的信息的其他形式的存储介质或者这些的适合的组合形式。

[0110] 通信总线18相互连接处理器14、计算机可读存储介质16以及计算装置12的其他多样的组件。

[0111] 此外,计算装置12还可以包含提供用于一个以上的输入输出装置24的接口的一个以上的输入输出接口22以及一个以上的网络通信接口26。输入输出接口22以及网络通信接

口26连接到通信总线18。输入输出装置24可以通过输入输出接口22而连接到计算装置12的其他组件。示例性的输入输出装置24可以包括：诸如指示装置（鼠标或者触控板等）、键盘、触摸输入装置（触摸板或者触摸屏等）、语音或者声音输入装置、多样的种类的传感器装置以及/或者拍摄装置等的输入装置；以及/或者诸如显示装置、印刷机、扬声器以及/或者网卡等的输出装置。示例性的输入输出装置24可以作为用于构成计算装置12的一组件而包含在计算装置12的内部，也可以作为区别于计算装置12的独立的装置而连接到计算装置102。

[0112] 以上，对本发明的具有代表性的实施例进行了详细的说明，然而在本发明所属的技术领域中具有基本知识的人员可以理解上述的实施例可在不脱离本发明的范围的限度内实现多种变形。因此，本发明的权利范围不应局限于上述的实施例，本发明的权利范围需要根据权利要求书的范围以及与该权利要求书均等的范围来确定。

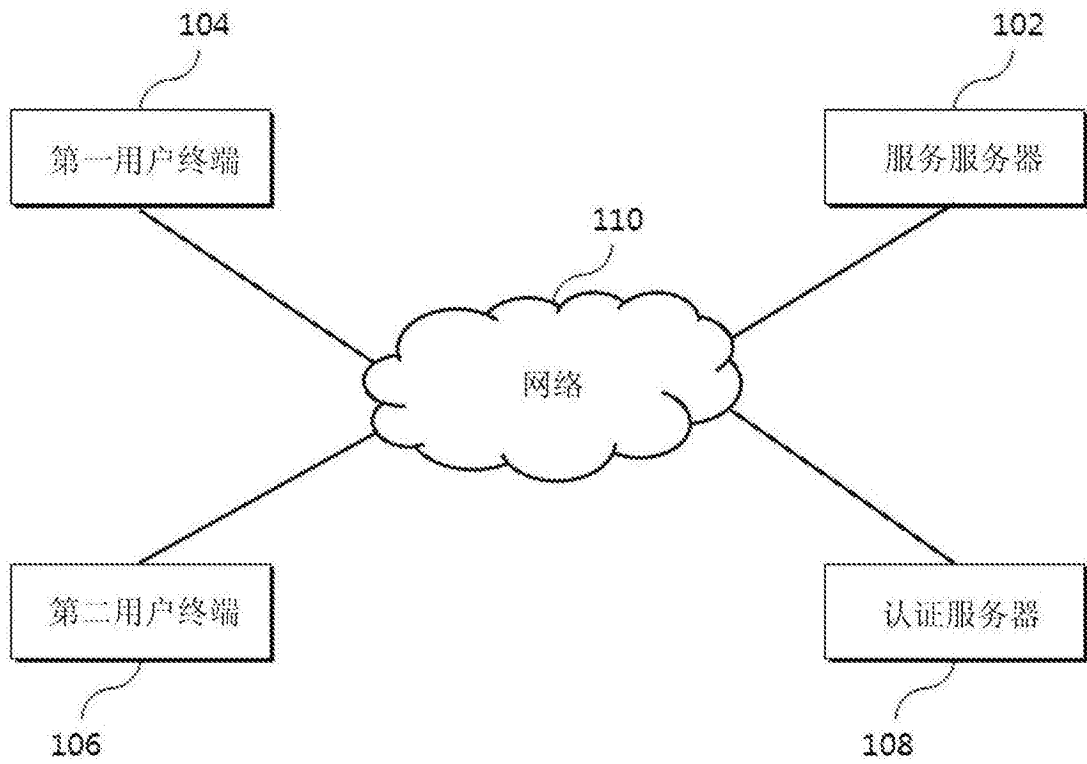
100

图1

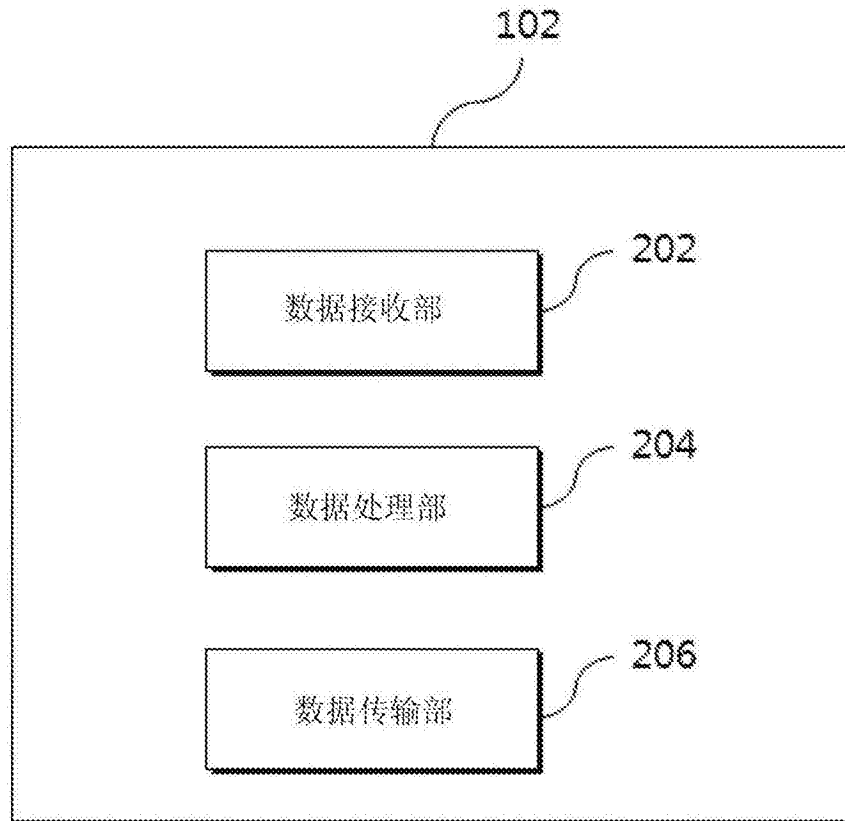


图2

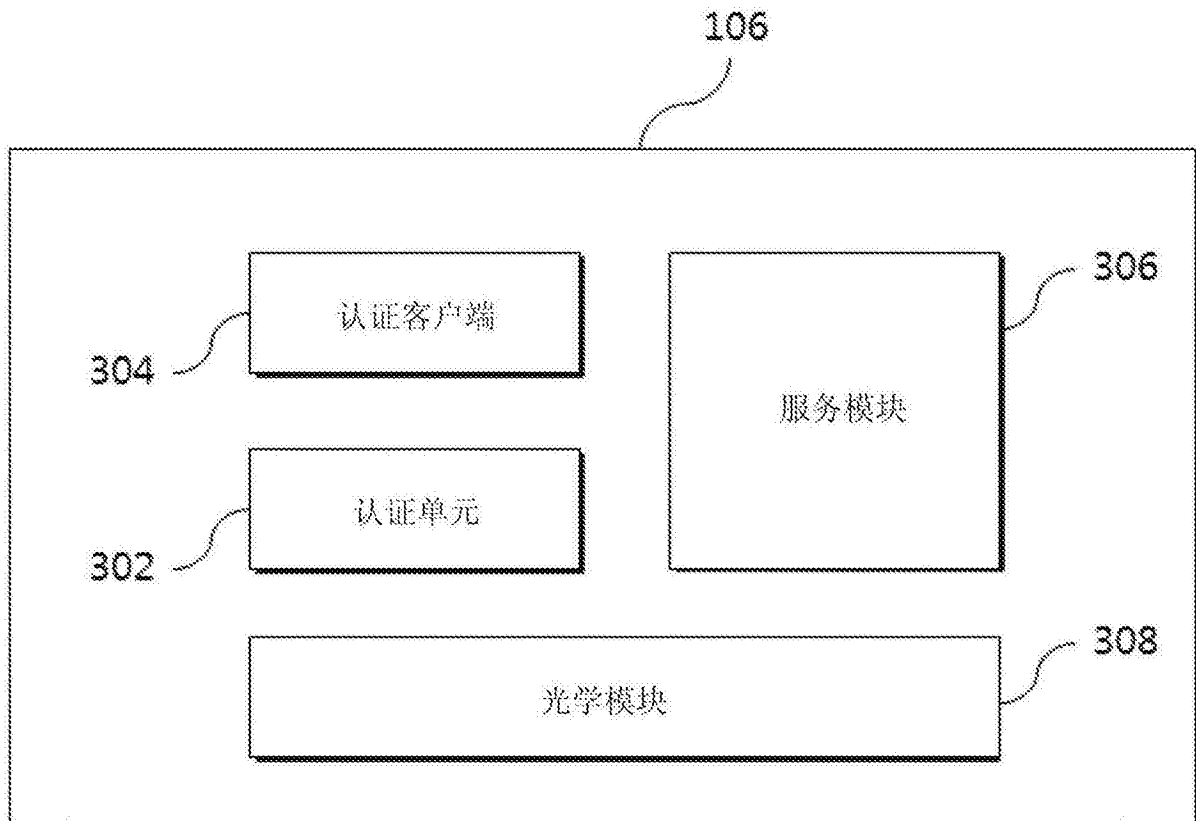


图3

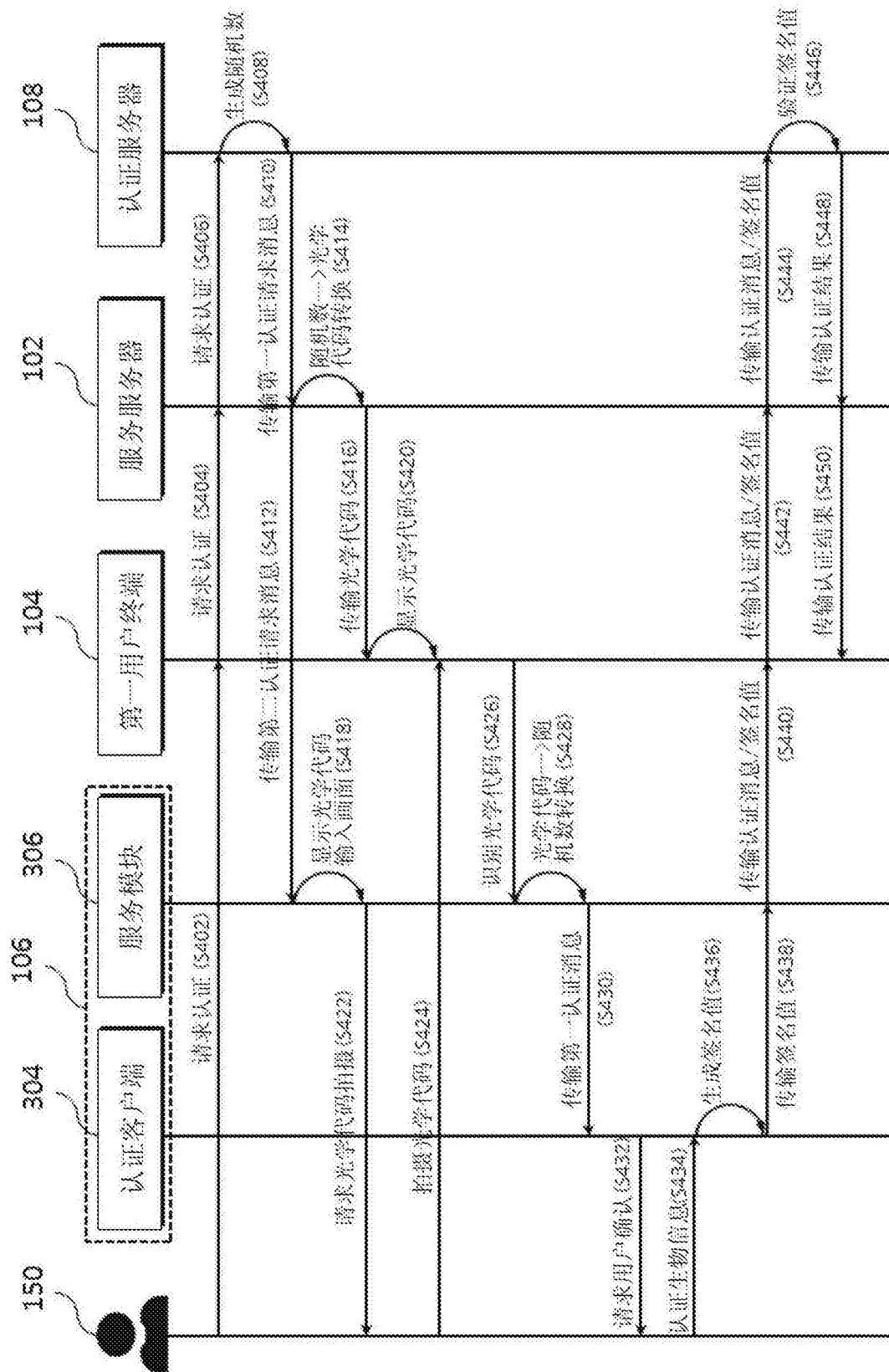


图4

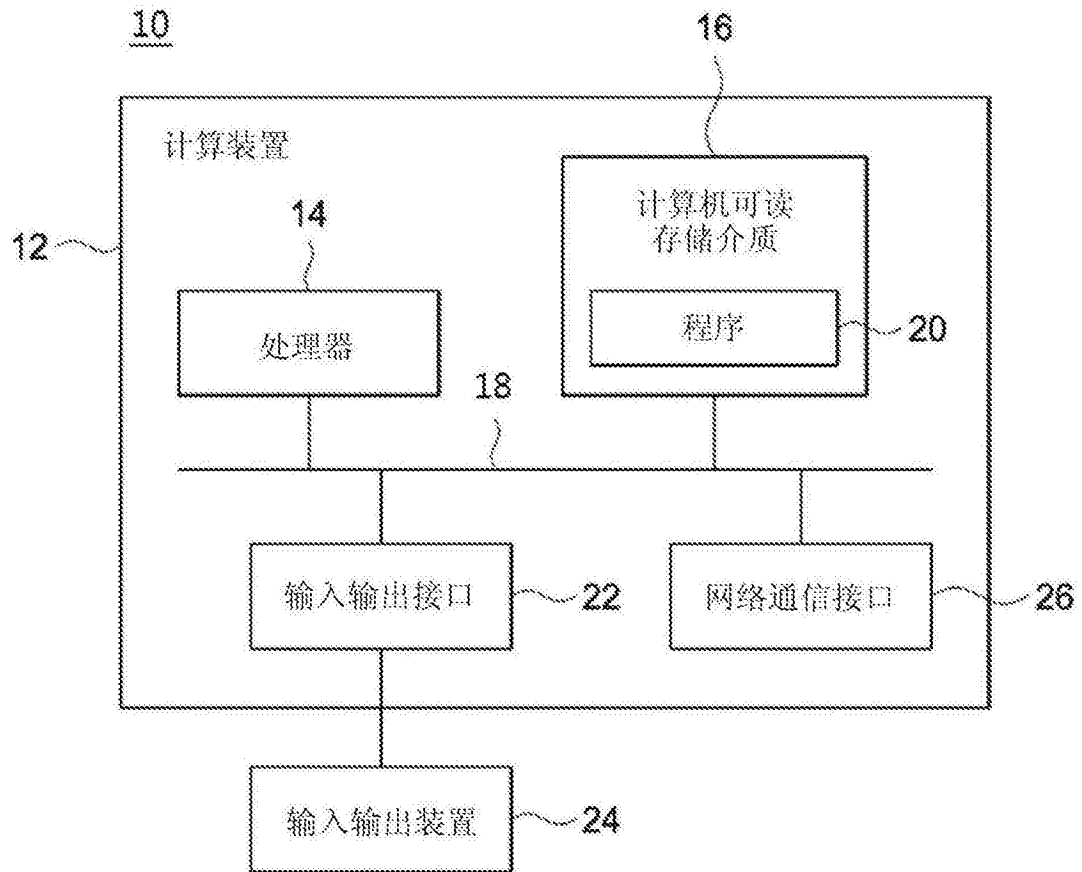


图5