(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108985027 B
(45)授权公告日 2022.07.12

(21)申请号 201810540213.1

(22)申请日 2018.05.30

(65)同一申请的已公布的文献号
申请公布号 CN 108985027 A

(43)申请公布日 2018.12.11

(30)优先权数据
2017-108255 2017.05.31 JP

(73)专利权人 佳能株式会社
地址 日本东京都大田区下丸子3-30-2

(72)发明人 太田峻辅

(74)专利代理机构 北京怡丰知识产权代理有限公司 11293
专利代理师 迟军 李艳丽

(51)Int.Cl.
G06F 21/32(2013.01)
G06F 21/46(2013.01)

(56)对比文件
CN 103186734 A,2013.07.03
US 2015020935 A1,2015.01.22
US 2014337542 A1,2014.11.13
CN 101539880 A,2009.09.23
CN 1801816 A,2006.07.12
US 2011078166 A1,2011.03.31
安全牛.《关于FIDO 你了解多少?》.《https://www.aqniu.com/learn/21534.html》.2016,第1-7页.
Kexin Hu等.《The application of cross-domain single sign-on in municipal portal》.《China Communications》.2016,第13卷(第12期),第189-198页.

审查员 刘婷

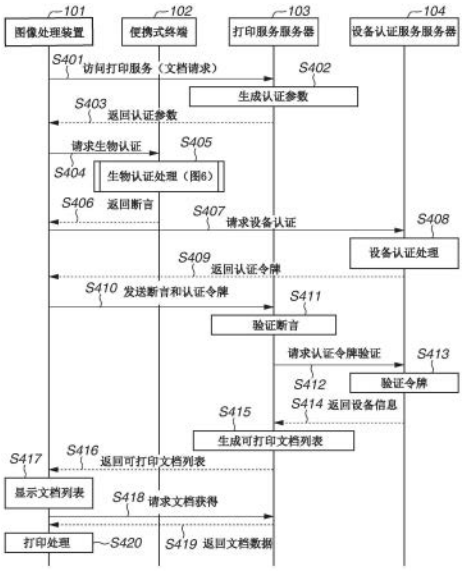
权利要求书4页 说明书12页 附图10页

(54)发明名称

图像处理装置、方法、系统和存储介质

(57)摘要

本发明涉及图像处理装置、方法、系统和存储介质。该图像处理装置与用户的便携式终端通信,其中,便携式终端包括用于生物认证的认证模块。当图像处理装置接收到由服务提供系统发出的验证数据时,图像处理装置使用用于生物认证的便携式终端的认证模块,并请求与服务提供系统合作的设备认证系统发出认证令牌。



CN 108985027 B

1.一种图像处理装置,其包括与便携式终端通信的通信功能,所述便携式终端包括用于生物认证的认证模块和具有防篡改性的存储区域,所述存储区域存储对于认证模块进行认证处理必要的用户的生物信息和当所述生物信息被登记时生成的秘密密钥,所述图像处理装置包括:

存储指令的存储器;以及

处理器,其执行指令以使所述图像处理装置:

在经由网络接收到为使用服务提供系统而生成的验证数据的情况下,将所述验证数据发送至便携式终端;

响应于通过包括在便携式终端中的认证模块对用户的认证处理的成功,从便携式终端接收利用验证数据和存储在存储区域中的秘密密钥而生成的签名数据;

将设备认证的请求发送至设备认证系统;

接收由设备认证系统发出的认证令牌;并且

将签名数据和认证令牌经由网络发送至验证数据的发送源,其中,在通过对应于秘密密钥的公开密钥验证了签名数据,并且通过请求设备认证系统验证认证令牌而获得图像处理装置的标识信息的情况下,服务提供系统向图像处理装置提供服务。

2.根据权利要求1所述的图像处理装置,

其中,服务提供系统将用户标识信息和设备标识信息作为服务提供目的地进行管理,并且

其中,在通过公开密钥验证了签名数据,并且从设备认证系统获得图像处理装置的标识信息的情况下,服务提供系统向图像处理装置提供,与在便携式终端中经生物认证的用户相对应的用户标识信息、和与从设备认证系统获得的图像处理装置的标识信息相关联地管理的服务。

3.根据权利要求1所述的图像处理装置,

其中,经由网络从图像处理装置发送签名数据作为断言信息,并且

其中,认证令牌被设置在断言信息的扩展区域中。

4.根据权利要求1所述的图像处理装置,其中,响应于来自服务提供系统的设备认证的指令,将设备认证的请求发送至设备认证系统。

5.根据权利要求1所述的图像处理装置,其中,在指定便携式终端根据用户对图像处理装置的操作来进行认证处理的情况下,将验证数据从图像处理装置发送至便携式终端。

6.根据权利要求1所述的图像处理装置,

其中,服务提供系统将用户在服务提供系统中登记的数据作为服务,提供给图像处理装置,并且

其中,图像处理装置利用所提供的数据执行打印处理。

7.根据权利要求1所述的图像处理装置,

其中,服务提供系统将用户在服务提供系统中登记的数据作为服务,提供给图像处理装置,并且

其中,图像处理装置利用所提供的数据执行三维形状物体的形成处理。

8.根据权利要求1所述的图像处理装置,其中,生物信息是与用户的指纹、血管、虹膜、声纹和面部图像中的一者或更多者相关的信息。

9.一种用于图像处理装置的方法,所述图像处理装置包括与便携式终端通信的通信功能,所述便携式终端包括用于生物认证的认证模块和具有防篡改性的存储区域,所述存储区域存储对于认证模块进行认证处理必要的用户的生物信息和当所述生物信息被登记时生成的秘密密钥,所述方法包括:

在经由网络接收到为使用服务提供系统而生成的验证数据的情况下,将所述验证数据发送至便携式终端;

响应于通过包括在便携式终端中的认证模块对用户的认证处理的成功,从便携式终端接收利用验证数据和存储在存储区域中的秘密密钥而生成的签名数据;

将设备认证的请求发送至设备认证系统:

接收由设备认证系统发出的认证令牌;以及

将签名数据和认证令牌经由网络发送至验证数据的发送源,

其中,在通过对应于秘密密钥的公开密钥验证了签名数据,并且通过请求设备认证系统验证认证令牌而获得图像处理装置的标识信息的情况下,服务提供系统向图像处理装置提供服务。

10.根据权利要求9所述的方法,其中,

经由网络从图像处理装置发送签名数据作为断言信息,并且

其中,认证令牌被设置在断言信息的扩展区域中。

11.根据权利要求9所述的方法,其中,在指定便携式终端根据用户对图像处理装置的操作来进行认证处理的情况下,将验证数据从图像处理装置发送至便携式终端。

12.一种非临时性计算机可读存储介质,其存储使计算机执行用于图像处理装置的方法的计算机程序,所述图像处理装置包括能够与便携式终端通信的通信功能,所述便携式终端包括用于生物认证的认证模块和具有防篡改性的存储区域,所述存储区域存储对于认证模块进行认证处理必要的用户的生物信息和当所述生物信息被登记时生成的秘密密钥,所述方法包括:

在经由网络接收到为使用服务提供系统而生成的验证数据的情况下,将所述验证数据发送至便携式终端;

响应于通过包括在便携式终端中的认证模块对用户的认证处理的成功,从便携式终端接收利用验证数据和存储在存储区域中的秘密密钥而生成的签名数据;

将设备认证的请求发送至设备认证系统:

接收由设备认证系统发出的认证令牌;以及

将签名数据和认证令牌经由网络发送至验证数据的发送源,

其中,在通过对应于秘密密钥的公开密钥验证了签名数据,并且通过请求设备认证系统验证认证令牌而获得图像处理装置的标识信息的情况下,服务提供系统向图像处理装置提供服务。

13.一种安全认证系统,其包括:

便携式终端,其包括用于生物认证的认证模块和具有防篡改性的存储区域,所述存储区域存储对于认证模块进行认证处理必要的用户的生物信息和当所述生物信息被登记时生成的秘密密钥;

图像处理装置,其包括与便携式终端通信的通信功能;

服务提供系统，其向图像处理装置提供服务；以及

设备认证系统，其发出用于图像处理装置的认证的认证令牌，

其中，图像处理装置包括存储指令的第一存储器和第一处理器，所述第一处理器执行存储在第一存储器中的指令，以使所述图像处理装置在经由网络接收到为使用服务提供系统而生成的验证数据的情况下，将所述验证数据从图像处理装置发送至便携式终端；

其中，便携式终端包括存储指令的第二存储器和第二处理器，所述第二处理器执行存储在第二存储器中的指令，以使所述图像处理装置响应于通过认证模块对用户的认证处理的成功，利用验证数据和存储的秘密密钥生成签名数据；

其中，存储在第一存储器中的指令还使图像处理装置：

从便携式终端接收生成的签名数据；

将设备认证的请求发送至设备认证系统：

接收由设备认证系统发出的认证令牌；并且

将签名数据和认证令牌经由网络从图像处理装置发送至验证数据的发送源，

其中，在通过对应于秘密密钥的公开密钥验证了签名数据，并且通过请求设备认证系统验证认证令牌而获得图像处理装置的标识信息的情况下，服务提供系统向图像处理装置提供服务。

14.根据权利要求13所述的安全认证系统，

其中，在用户的生物信息被登记在认证模块中的情况下，便携式终端生成秘密密钥和公开密钥，并且

其中，公开密钥被从便携式终端发送至服务提供系统，以与用户的用户标识信息相关联地登记在服务提供系统中。

15.一种用于安全认证系统的方法，所述安全认证系统包括：

便携式终端，其包括用于生物认证的认证模块和具有防篡改性的存储区域，所述存储区域存储对于认证模块进行认证处理必要的用户的生物信息和当所述生物信息被登记时生成的秘密密钥；

图像处理装置，其包括与便携式终端通信的通信功能；

服务提供系统，其向图像处理装置提供服务；以及

设备认证系统，其发出用于图像处理装置的认证的认证令牌，

所述方法包括：

在经由网络接收到为使用服务提供系统而生成的验证数据的情况下，将所述验证数据从图像处理装置发送至便携式终端；

响应于通过认证模块对用户的认证处理的成功，由便携式终端利用验证数据和存储的秘密密钥生成签名数据；

通过图像处理装置从便携式终端接收生成的签名数据；

通过图像处理装置将设备认证的请求发送至设备认证系统：

通过设备认证系统发出图像处理装置的认证令牌；

通过图像处理装置从设备认证系统接收所发出的认证令牌；以及

将签名数据和认证令牌经由网络从图像处理装置发送至验证数据的发送源，

其中，在通过对应于秘密密钥的公开密钥验证了签名数据，并且通过请求设备认证系

统验证认证令牌而获得图像处理装置的标识信息的情况下,服务提供系统向图像处理装置提供服务。

图像处理装置、方法、系统和存储介质

技术领域

[0001] 本公开涉及当使用图像处理装置时控制能够由经生物认证的用户使用的设备的方法。

背景技术

[0002] 近来，快速在线身份验证(FIDO)作为一种新的包括生物认证的认证系统引起了人们关注。

[0003] 与标识(ID)和密码验证中的密码不同，在生物认证中使用的诸如指纹和血管的用户生物信息不能被重写，因此如果这些信息被公开，则会导致安全问题。在FIDO中，认证处理在用户具有的终端上进行，而不是通过互联网在服务器上进行。用户的生物信息在进行认证的终端的安全存储区中被严格管理，而不是被存储在任何网络地址。因此，降低了这些信息被公开的风险。

[0004] 传统上，存在位于公共场所和办公室的系统，该系统在进行认证以确保安全性之后在使用网络服务的设备上向用户提供服务。

[0005] 例如，日本特开2013-191236号公报描述了一种系统，在该系统中，当用户操作图像处理装置时，认证服务器利用从集成电路(IC)卡读取的信息进行认证。对应于成功认证的用户ID的打印作业，从打印服务器下载至图像处理装置。另外，日本特开2013-191236号公报公开了认证服务器利用诸如指纹和手指血管的生物信息进行认证，来替代IC卡认证。

[0006] 期望这样的系统采用包括更安全的生物认证的特殊机制，例如上述FIDO。

发明内容

[0007] 根据本发明的一方面，提供了一种图像处理装置，其包括与便携式终端通信的通信功能，所述便携式终端包括用于生物认证的认证模块和具有防篡改性的存储区域，所述存储区域存储对于认证模块进行认证处理必要的用户的生物信息和当所述生物信息被登记时生成的秘密密钥，所述图像处理装置包括：存储指令的存储器；和处理器，其执行指令以使所述图像处理装置：在经由网络接收到为使用服务提供系统而生成的验证数据的情况下，将所述验证数据发送至便携式终端；响应于通过包括在便携式终端中的认证模块对用户的认证处理的成功，从便携式终端接收利用验证数据和存储在存储区域中的秘密密钥而生成的签名数据；将设备认证的请求发送至设备认证系统；接收由设备认证系统发出的认证令牌；并且将签名数据和认证令牌经由网络发送至验证数据的发送源，其中，在通过对应于秘密密钥的公开密钥验证了签名数据，并且通过请求设备认证系统验证认证令牌而获得图像处理装置的标识信息的情况下，服务提供系统向图像处理装置提供服务。

[0008] 通过以下参照附图对示例性实施例的描述，本发明的其他特征将变得清楚。

附图说明

[0009] 图1例示了根据本公开的系统构造的示例。

[0010] 图2A至图2C例示了根据本公开的各个装置的硬件构造的示例。

[0011] 图3例示了根据本公开的软件的功能框图的示例。

[0012] 图4例示了根据第一示例性实施例的整个序列图。

[0013] 图5A至图5D例示了根据第一示例性实施例的用于调用认证功能的参数。

[0014] 图6是根据第一示例性实施例的关于通过便携式终端的生物认证处理的流程图。

[0015] 图7A至图7C例示了根据第一示例性实施例的通过图像处理装置显示的画面的示例。

[0016] 图8是关于第一应用的流程图。

[0017] 图9例示了便携式终端上显示的针对生物认证的请求画面的示例。

具体实施方式

[0018] 下面将参照附图详细描述本发明的各种示例性实施例。

[0019] 图1例示了根据本公开的系统构造的示例。

[0020] 本系统包括图像处理装置101、打印服务服务器103、设备认证服务服务器104、租户(tenant)管理服务服务器105、和设备管理服务服务器106。图像处理装置101经由网络112连接至便携式终端102。网络111是例如通过诸如因特网的局域网(LAN)、广域网(WAN)、电话线、专用数字线、异步传输模式切换系统(ATM)、帧中继线、有线电视线、用于数据广播的无线电频道中的任一者或者其组合而实现的通信网络。网络112除了上述诸如LAN的网络线之外,还包括诸如蓝牙®的近场通信。

[0021] 图像处理装置101可以是从网络获得数据并且将该数据作为图像数据和物理介质输出的任何设备,例如打印机、复印机、数字医疗机(血压测量设备、室内跑步机(room runner)等)、ATM和三维(3D)打印机(用于打印(形成)三维形状的物体)。另选地,可以在提供用于将作为输出目标的数据供给至图像处理装置的服务的各种服务提供系统中使用打印服务服务器103。打印服务服务器103可以包括积累多用户的文档数据并响应于来自其它装置的请求而提供数据的图像处理装置。

[0022] 下文详细描述系统的示例,其中打印数据被提供给图像处理装置101,并且图像处理装置101打印并输出打印数据。

[0023] 便携式终端102可以是笔记本式个人计算机(PC)、便携式终端(智能手机和平板电脑)或诸如智能手表和智能眼镜的可穿戴终端。

[0024] 设备认证服务服务器104是如下服务器,该服务器构建设备认证系统,并准备利用认证令牌来进行设备认证,从而唯一地识别在设备管理服务服务器106中登记的图像处理装置等。设备认证服务服务器104与打印服务服务器103合作,从而确保打印服务服务器103是合适的图像处理装置。

[0025] 租户管理服务服务器105是在第二示例性实施例中使用的服务器并在下文中详细描述。

[0026] 图2A至图2C例示了本公开的各个装置的硬件构造。

[0027] 图2A是表示打印服务服务器103、设备认证服务服务器104、租户管理服务服务器105、和设备管理服务服务器106的信息处理装置的硬件构造图。这些服务服务器可以包括与通用个人计算机(PC)相类似的硬件。

[0028] 中央处理单元(CPU)201执行存储在只读存储器(ROM)203中的程序、以及从外部存储器210加载至随机存取存储器(RAM)202的操作系统(OS)和应用的程序。换句话说，CPU 201执行存储在可读存储介质中的程序并且用作执行下文描述的流程图中的处理的各个处理单元。RAM202是CPU 201的主存储器并且用作工作区等。键盘控制器204控制从键盘208和定点设备(诸如鼠标、触摸盘、触摸面板或追踪球)(未示出)输入的操作。显示控制器205控制在显示器209上的显示。盘控制器206控制对诸如硬盘(HD)和软盘(FD)的用于存储各种数据的外部存储器210的数据存取。网络接口(I/F)207连接至网络并对连接至网络的其它设备执行通信控制处理。

[0029] 打印服务服务器103、设备认证服务服务器104、租户管理服务服务器105、和设备管理服务服务器106将要通过下文描述的各个服务器管理的信息存储在诸如外部存储器210的存储设备中，该存储设备被包括在设备本身和/或网络上的存储器中。

[0030] 图2B是表示打印机的构造的图像处理装置101的硬件构造图。

[0031] CPU 201包括被存储在ROM 223中的程序(包括用于实现下文所述的各个处理的程序)，并且经由内部总线231综合地控制各个元件。RAM 222用作CPU 221的存储器和工作区。网络I/F 225与外部网络设备定向或双向地交换数据。邻近通信I/F 226是用于诸如蓝牙®的邻近通信的网络I/F，并且包括用于与便携式终端102等通信以交换数据的通信功能的构造。设备控制器227控制打印单元228。CPU 221与RAM 222和ROM 223一起进行程序的执行处理，并且进行将图像数据记录至诸如存储设备224的存储介质的处理。存储设备224用作外部存储设备。输入输出设备230包括进行图像处理装置101中的输入和输出的多种构造。更具体地，输入输出设备230从用户接收输入(按钮输入)并且将对应于输入的信号从输入输出I/F 229发送至各个上述单元。另外，输入输出设备230包括用于将必要的信息提供给用户并接收用户操作的显示设备(诸如触摸面板)。输入输出设备230可以显示并输出(通知)从网络上的服务提供装置提供的数据。

[0032] 输入输出设备230可以包括用于读取原稿并接收作为输入的电子数据的扫描设备。例如在3D打印机中，安装用于形成三维形状的物体的工作台和头部，作为打印单元228。

[0033] 图2C是便携式终端102的硬件构造图。

[0034] CPU 242包括被存储在ROM 244中的程序(包括用于实现下文所述的各个处理的程序)，并且经由内部总线241综合地控制各个元件。RAM 243用作CPU 242的存储器和工作区。网络I/F 247利用无线保真(Wi-Fi®)等与外部网络设备定向或双向地交换数据。CPU 242与RAM 243和ROM 244一起进行程序的执行处理，并且进行将图像数据记录至诸如存储设备245的存储介质的处理。存储设备224用作诸如安全数字(SD)卡等的外部存储设备。

[0035] 可信平台模块(TPM)246是包括用于保护存储数据不受外部访问以便处理并存储机密信息的防篡改性的存储单元。作为包括防篡改性的存储单元的具体示例，假定符合作为产业标准的TPM 2.0(或更高版本)的存储单元。根据本公开，用于生物认证的生物信息或生物信息的特征量、对应于生物信息的秘密密钥等被存储在TPM 246中。在下文的描述中，通过传感器获得的表示生物信息的信号的特征量在一些情况下可以被称作生物信息。生物信息传感器248是读取例如指纹、虹膜、血管、声纹、或面部图像等的用户的生物信息并将信息转换成信号的传感器。生物信息传感器248通过使用专用读取设备、照相机、麦克风等实现。

[0036] 包括显示和输入功能的触摸面板249显示应用画面和键盘，并且当用户使用其手指或专用笔在画面上施加压力时，触摸面板249向外输出关于画面上的触摸位置的信息，作为信息信号。应用使用输出的信息信号，使用户能够经由触摸面板249操作应用。生物信息传感器248和触摸面板249能够通过相互叠置来进行安装，并且被构造成通过对触摸面板249的操作读取用户的指纹信息。

[0037] 与图像处理装置101的邻近通信I/F类似，邻近通信I/F 250是对应于诸如近场通信(NFC)和蓝牙®的邻近通信系统的I/F，并且根据本示例性实施例，经由邻近通信I/F 250进行与图像图例装置101的通信。

[0038] 图3例示了通过在根据本公开的各个装置和设备中包括的软件实现的功能模块的构造。这些构造实现三种主要类型的处理，即“从客户PC 107到打印服务服务器103的打印指令的接收”、“从便携式终端102到打印服务服务器103的认证信息的登记处理”、和“从图像处理装置101到打印服务服务器103的打印请求”。这三种类型的处理在下文中结合图3例示的各个构造的描述进行描述。

[0039] 图3例示的打印服务服务器103、设备认证服务服务器104和租户管理服务服务器105中的各个单元作为程序被存储在ROM 203中并且通过CPU 201在RAM 202上执行。图像处理装置101中的各个单元作为程序被存储在ROM 223中并且通过CPU 221在RAM 222上执行。类似地，便携式终端102中的各个单元作为程序被存储在ROM 244中并且通过CPU 242在RAM 243上执行。

[0040] <<从客户PC 107到打印服务服务器103的打印指令的接收>>

[0041] 首先，用户利用客户PC 107等登录至打印服务服务器103的打印服务，并且选择打印目标文档作为对打印服务服务器103的打印指令。此时，客户PC 107的用户可以从存储在设备管理服务服务器106(下文中描述)中的设备数据中，选择并指定能够打印选择的文档的图像处理装置。当不选择和指定图像处理装置时，可以确定任何图像处理装置能够进行打印。

[0042] 打印服务服务器103的打印指令接收单元311接收打印指令，打印指令包括打印目标文档的数据和表示能够进行打印的图像处理装置的设备信息。打印数据管理单元318以下文示出的表A中表示的格式，存储包括在打印指令中的数据。文档的数据包括诸如文档名称、数据文件、表示文件存储地址的信息的属性信息。

[0043] 在表A中，文档名称是由用户选择的作为打印指令的文档的名称，并且在下文所述的打印流程中被显示在图像处理装置101上。文档数据是待打印的文档的二进制数据。用户标识信息(ID)是唯一地表示指示打印的用户的ID。用户ID是从在用户登录至打印服务后发出打印指令时起能够指定用户的信息。打印设备ID是用于识别当用户指示打印时指定的设备的设备标识信息。当用户不指定打印时的设备时，设置诸如“*”的特定的标记作为表示任何设备均能进行打印的信息。打印服务服务器103能够通过表A管理能够进行打印的用户和能够打印的设备，作为服务提供目的地。

[0044] 表A

[0045]

文档名称	文档数据	用户ID	打印设备ID
aaa.doc	010100101010101010...	user001	dev001
bbb.ppt	001010010101001111...	user003	dev002,dev003

ccc.txt	0111110101101110111...	user004	*
:	:	:	

[0046] 使用客户PC 107的用户预先以一般的方法,针对打印服务服务器103生成使用打印服务的诸如ID和密码的用户账号。另外,当指示打印时,用户使用作为用户账号的用户ID和密码登录至打印服务并进行打印指示。根据本示例性实施例,预先生成的ID和密码的组合被称为传统凭证。传统凭证被存储在存储设备中并通过用户管理单元312管理。

[0047] 设备管理服务服务器106的设备登记请求接收单元391从图像处理装置101的设备登记请求单元355接收设备登记请求。包括在设备登记请求中的设备信息通过存储设备上的设备信息管理单元392管理。要管理的信息是诸如设备ID、产品名称和其安装地址的信息,当用户指示打印时,能够通过这些信息确定能够打印的设备。

[0048] 当稍后要打印的文档数据从客户PC 107登记时,打印服务服务器103可以使客户PC 107的用户能够指定图像处理装置进行打印。因此,打印服务服务器103向客户PC 107显示设备列表。因此,打印服务服务器103从设备管理服务服务器106的设备信息管理单元392请求设备信息。打印服务服务器103向客户PC 107提供基于设备信息的设备列表。

[0049] 利用客户PC 107的web浏览器进行从客户PC 107向打印服务服务器103的、对可以是图像处理装置的处理目标的数据的登记和对图像处理装置的选择。因此,可以是图像处理装置的处理目标的数据的登记和图像处理装置的选择可以从便携式终端102进行。

[0050] <<从便携式终端102到打印服务服务器103的认证信息的登记处理>>

[0051] 便携式终端102的认证信息登记请求单元331访问打印服务并开始认证信息的登记处理。对于打印服务服务器103对响应于在便携式终端102中进行的成功的生物认证而经便携式终端102认证的用户进行认证来说,认证信息是必要的。认证信息包括将在下文详细描述的公开密钥、认证信息ID等。认证信息在网络上流转,因此不包括用于生物认证的用户特定生物信息和响应于生物信息而生成的秘密密钥。当打印服务是通过web浏览器等访问的应用时,认证信息登记请求单元331可以通过JavaScript®实现;或者当存在用于打印服务的应用时,认证信息登记请求单元331可以在应用中实现。

[0052] 当响应于来自便携式终端102的用户的指令而开始登记处理时,打印服务服务器103的打印服务请求从便携式终端102输入传统凭证。用户经由web浏览器和便携式终端102的应用输入用于登录到打印服务的传统凭证。当传统凭证被正确输入且成功认证时,能够在打印服务服务器103上针对用户进行不同于传统凭证的认证信息的登记处理。

[0053] 便携式终端102的生物信息输入单元332经由生物信息传感器248从用户接收诸如指纹信息的生物信息的输入。生物信息管理单元333将输入的生物信息与用于识别生物信息的生物信息ID相关联,并将关联的信息存储在TPM 246中。根据本公开,生物信息管理单元333、认证请求接收单元334、和生物认证单元335被安装作为,用于利用诸如生物信息传感器248和TPM 246的硬件来控制便携式终端102中的生物认证的认证模块。认证模块还被称作认证器。认证信息登记请求单元331和其它模块可以作为认证模块的一部分来实现。

[0054] 在输入生物信息后,生物认证单元335生成对应于生物信息的公开密钥和秘密密钥对。生物信息管理单元333将生成的秘密密钥,与用于识别对应于该秘密密钥的生物信息的生物信息ID、传统凭证、表示打印服务服务器103的ID等相关联,并在TPM 246中存储和管理被关联的信息。存储的存储信息的示例参照表B进行描述。

[0055] 表B

[0056]

认证信息 ID	服务 ID	秘密密钥	生物信息 ID
407c-8841-79d	print.com	1faea2da-a269-4fa7-812a-509470d9a0cb	d493a744
:	:	:	

[0057] 表B中的认证信息ID列存储有通过生物信息管理单元333唯一地分配给各个登记信息的标识信息(ID)。服务ID列存储有表示用户合作的系统(根据本示例性实施例,打印服务服务器103)并且是顶级域和二级域的信息的ID。秘密密钥列存储有秘密密钥。生物信息ID列存储有由用户输入的对应于特征量信息(生物信息)的ID,特征量信息与诸如指纹的信息一一对应。

[0058] 上述公开密钥作为认证信息与在表B中相关联地管理的认证信息ID一起,通过认证信息登记请求单元331发送给打印服务服务器103。打印服务服务器103的认证信息登记单元314将接收到的认证信息与传统凭证相关联地存储在存储设备中。要存储的信息的示例参照表C描述。

[0059] 表C

[0060]

认证信息ID	公开密钥	用户ID
407c-8841-79d	AC43C5FB-BFA2-48D1-A71B-FB04ACDA347A	user001
4c04-428b-a7a2	8142CA9F-35C9-4333-948F-BFCE66A74310	user002
:	:	

[0061] 认证信息ID列存储有表B中的认证信息ID列的值。公开密钥列存储有与表B中的秘密密钥成对的公开密钥。换句话说,关于表B中具有相同的认证信息ID的公开密钥和秘密密钥,通过表B中的秘密密钥加密的信息能够通过表C中的公开密钥解密。用户ID被使用和管理从而与传统凭证相关联。

[0062] <<从图像处理装置到打印服务服务器103的请求处理和输出处理>>

[0063] 将描述如下处理,即响应于用户操作任意的图像处理装置101,通过图像处理装置101从打印服务服务器103获得从客户PC 107向打印服务服务器103预先指示待打印的文档,并输出文档。除了图3之外,还参照图4的序列图描述处理。

[0064] 在步骤S401中,响应于用户的操作,图像处理装置101访问打印服务服务器103的打印服务的统一资源定位符(URL)。此时,图像处理装置101的文档请求单元351能够向打印服务服务器103的文档请求接收单元315发出文档请求。针对打印服务服务器103的打印服务尚未进行对操作图像处理装置101的用户的认证。

[0065] 在步骤S402中,用户验证单元316响应于访问打印服务或接收文档请求而生成图5A例示的认证参数501。在步骤S403中,作为对步骤S401中的处理的响应,文档请求接收单元315返回在步骤S402中生成的认证参数501。

[0066] 认证参数501包括断言质疑502和断言扩展区域503。断言质疑502是用于进行质疑响应认证的验证数据。在断言扩展区域503中,扩展参数被存储用于打印服务服务器103以控制关于便携式终端102中的生物认证的处理。

[0067] 在步骤S404中,图像处理装置101的认证请求单元353将生物认证请求与在步骤

S403返回的认证参数501一起，经由NFC或蓝牙®发送至经由网络112连接的便携式终端102的认证请求接收单元334。用户能够通过操作图像处理装置101的显示设备指定便携式终端102针对打印服务服务器103进行生物认证。在这种情况下，图像处理装置101将认证参数传输至便携式终端102。

[0068] 在步骤S405中，生物认证单元335响应于接收到生物认证请求控制生物认证处理。生物认证处理参照图6详细描述。图6例示的流程图用于描述通过便携式终端102的CPU 242执行程序实现的处理。

[0069] 在步骤S611中，生物认证单元335显示如图9例示的请求画面以提示用户输入用于生物认证的生物信息。根据本示例性的实施例，指纹信息作为生物信息处理。然而，可以使用诸如虹膜和面部的其它信息。在步骤S612中，生物信息输入单元332经由生物信息传感器248从用户接收指纹信息的输入并且获得指纹信息的特征量。通过将对个人唯一的特征(例如指纹图案、虹膜图案或血管形状)转换成不损害唯一性的值，来获得特征量。在步骤S613中，生物认证单元335利用通过生物信息传感器248接收到的生物信息确认认证处理的结果。当由用户输入的生物信息已经登记并且认证处理成功时，处理进行至步骤S614。

[0070] 在步骤S614中，生物认证单元335通过参考表B来获得对应于在步骤S613的认证处理中认证的生物信息的秘密密钥，利用秘密密钥执行加密处理，并因此根据断言质疑502生成签名数据。生物认证单元335生成图5B例示的断言信息521。

[0071] 断言信息521包括认证信息522、签名523和客户数据524。关于认证信息522，设置通过表B与在步骤S614中使用的秘密密钥相关联地进行管理的认证信息ID。关于签名523，设置在步骤S614中生成的签名。客户数据524包括图5C例示的构造。

[0072] 将描述客户数据524的构造示例。客户数据524包括断言质疑531、扩展区域532和散列算法533。断言质疑531与在步骤S402中从打印服务服务器103发送的断言质疑502相同。关于扩展区域532，设置任意信息。散列算法533是表达当生成签名523时的散列算法的信息，并且对散列算法533设置诸如S256(＝安全散列算法(SHA)-256)和S384(＝SHA-384)的字符串。

[0073] 现在将返回对图4的序列图的描述。

[0074] 在步骤S406中，作为对步骤S404中的处理的响应，认证请求接收单元334将通过图6例示的处理生成的断言信息521返回至图像处理装置101。

[0075] 在步骤S407中，图像处理装置191的设备认证请求单元352将设备认证请求发送至设备认证服务服务器104的设备认证请求接收单元371。图像处理装置101还发送作为图像处理装置的标识信息的设备ID和存储在图像处理装置的安全区中的密码。

[0076] 在步骤S408中，响应于接收到设备认证请求，设备认证单元373验证在步骤S407中发送的设备ID和密码的组合是否与登记的组合相匹配，并且当组合已被登记时发出认证令牌。发出的认证令牌通过设备认证信息管理单元375与设备ID相关联地存储在储存设备中。在步骤S409中，作为对在步骤S407中的处理的响应，设备认证请求接收单元371将发出的认证令牌返回。

[0077] 在步骤S410中，图像处理装置101的文档请求单元351将断言信息521和认证令牌发送至打印服务服务器103的文档请求接收单元315。作为根据本示例性实施例的向打印服务服务器103的认证令牌的发送方法的示例，文档请求单元351将认证令牌设置给包括在断

言信息521中的客户数据524中的扩展区域532。如通过以下所描述，根据JavaScript Object Notation(JSON)模式等将信息设置给扩展区域532：

[0078] {'devicetoken':'00fde7ed-06bc-4d0f-8773-cb399e73eb6c'}

[0079] 在步骤S411中，打印服务服务器103的用户验证单元316基于包括在接收到的断言信息521中的认证信息ID从表C获得公开密钥信息，并且使用公开密钥验证包括在断言信息521中的签名523。用户验证单元316通过检查数据(确定数据的匹配)进行验证，该数据通过利用针对在步骤S403中的认证参数中设置的断言质疑502所获得的公开密钥对签名523进行解密而获得。当验证被正确进行时，在便携式终端102中经生物认证的用户被视为在打印服务服务器103中成功认证，而作为已登记用户，并且处理进行至步骤S412。当在用户验证单元316中断言信息的验证失败时，文档请求接收单元315将认证失败作为对图像处理装置101的响应(未例示)。

[0080] 在步骤S412中，设备验证请求单元317将包括从图像处理装置101接收到的认证令牌的认证令牌验证请求发送至设备认证服务服务器104的设备验证请求接收单元372。

[0081] 在步骤S413中，设备验证单元374确定由设备认证信息管理单元375管理的发出的认证令牌是否包括与经由设备验证请求接收单元372接收到的认证令牌相匹配的认证令牌。当匹配的认证令牌是确定结果时，验证被认为正确地进行，并且在步骤S414，设备验证请求接收单元372将通过设备认证信息管理单元375与认证令牌相关联地管理的设备ID与验证成功一起返回至打印服务服务器103。当结果不是匹配的认证令牌时，设备验证请求接收单元372将设备验证失败通知返回至打印服务服务器103(未示出)。当设备验证失败时，作为对步骤S410中的处理的响应，打印服务服务器103能够将不存在可打印的文档的通知返回至图像处理装置101。

[0082] 在步骤S415中，文档请求接收单元315基于成功验证的包括在断言信息521中的认证信息ID从表C中指定用户ID。另外，打印数据管理单元318参考表A并提取作为具有指定的用户ID的文档并且能够通过在步骤S414返回的设备ID打印的文档的数据。打印数据管理单元318基于提取的数据生成包括可打印文档的标识信息(文档ID)的文档列表。当表A不包括与用户ID和设备ID相匹配的记录时，打印数据管理单元318生成空白文档列表。

[0083] 在步骤S416中，文档请求接收单元315将在步骤S415生成的文档列表返回至图像处理装置101的文档请求单元351。当在步骤S415中存在与表A中的用户ID相关联的文档，但是不存在通过在步骤S413中获得的设备ID能够打印的文档时，表示该事实的信息可以被加入待返回的响应中。

[0084] 在步骤S417中，列表显示单元354将在步骤S416返回的文档列表显示在图像处理装置101的显示设备上。文档选择单元356接收用户经由显示的列表而进行的选择。参照图7A至图7C描述显示的示例。

[0085] 在图7A中，返回的文档列表(包括文档701、702和703)被显示在图像处理装置101的显示设备上。在便携式终端102经生物认证的用户从列表中选择要打印的文档并按下打印按钮(704)。

[0086] 图7B例示了当针对在步骤S416中返回的响应不存在与在便携式终端102中经生物认证的用户相关联的文档时显示的画面的示例。图7C例示了当不存在利用由在便携式终端102中经生物认证的用户操作的图像处理装置101能够打印的文档时显示的画面的示例。

[0087] 在步骤S418中，文档请求单元351将包括与经由文档选择单元356接收的用户选择相对应的文档ID的获得请求，发送给打印服务服务器103。在步骤S419中，文档请求接收单元315基于在步骤S418中指定的文档ID从表A获得文档数据，并将文档数据返回至图像处理装置101。在步骤S420中，图像处理装置101执行对在步骤S419中接收的数据的打印处理。

[0088] 假设图像处理装置101包括生物认证传感器和TPM，并且在表B和表C中表示的信息预先在图像处理装置101和打印服务服务器103之间登记。在这种情况下，生物认证处理能够在不使用便携式终端102的情况下通过图像处理装置101执行。在这种情况下，步骤S404至S406的处理被省略，并且反而，图6例示的处理通过图像处理装置101执行，并且随后生成断言信息。

[0089] 如上所述，根据第一示例性实施例可以实现结合生物认证和设备认证的设备控制系统。

[0090] 将描述第二示例性实施例。将描述第二示例性实施例与第一示例性实施例之间的不同。

[0091] 根据第一示例性实施例，当从用户PC 107指示打印时，指定能够打印的设备。然而，例如当打印例如公司中的机密文档时，仅公司内的图像处理装置能够打印文档以防止机密文档被公开。即使在这样的情况下，从可用性角度来说，在每次进行打印时均指定图像处理装置是效率很低的。因此，根据本示例性的实施例，增加图像处理装置和用户的租户管理功能，并且属于与发出打印指令的用户相同的租户的图像处理装置能够进行打印。

[0092] 针对本示例性实施例，增加图3例示的租户管理服务服务器105。租户管理服务服务器105管理表示用户和图像处理装置属于哪个租户的信息。

[0093] 参照表描述存储在租户管理服务服务器105的租户信息管理单元382中的数据的示例。

[0094] 表D是用于管理租户和用户之间的关系的用户管理表。租户ID列存储用于唯一表示组织的ID。用户ID列存储对应于上述传统凭证中的用户ID的信息。表D表示用户001和用户002属于租户A，用户003属于租户B。

[0095] 表D

[0096] 用户管理表

[0097]

租户ID	用户ID
租户A	用户001
租户A	用户002
租户B	用户003
...	...

[0098] 表E是用于管理租户和图像处理装置之间的关系的设备管理表的示例。表E表示具有设备ID“dev001”的图像处理装置属于租户A，并且具有设备ID“dev002”和“dev003”的图像处理装置属于租户B。

[0099] 表E

[0100] 设备管理表

[0101]

租户ID	设备ID
租户A	dev001

租户B	dev002
租户C	dev003
...	...

[0102] 当用户使用客户PC 107发出打印指令时,打印指令接收单元311如在第一示例性实施例中描述地接收打印指令。随后,经由租户信息请求单元319向租户信息请求接收单元381请求,发出打印指令的用户所属的租户的信息和属于相同租户的图像处理装置的信息。基于租户信息请求接收单元381接收到的请求,指示的用户所属的租户ID经由租户信息处理单元383从用户管理表(表D)获得。

[0103] 属于获得的租户ID的设备ID从设备管理表(表E)获得,并且信息返回至租户信息请求单元319。信息通过打印数据管理单元318存储在存储设备中,这与第一示例性实施例类似。

[0104] 根据本示例性实施例,在上述图4的步骤S415中,文档请求接收单元315基于成功验证的包括在断言信息521中的认证信息ID,从表C中指定用户ID。另外,文档请求接收单元315检查在步骤S414返回的设备ID是否属于指定的用户ID所属的租户ID表示的租户。当设备ID被确定为属于租户的设备ID时,文档请求接收单元315参照表A并提取对应于指定的用户ID的文档的数据。打印数据管理单元318基于提取的数据生成包括可打印文档的标识信息(文档ID)的文档列表。

[0105] 根据第一和第二示例性实施例,图像处理装置要经受设备认证。然而,在许多情况下,取决于用户,不指定能够打印的设备。在这种情况下,每次均对设备认证服务服务器104做出认证请求,会增大图像处理装置101的处理负荷。

[0106] 根据第一应用,仅当与发出打印指令的用户相关联的文档包括指定打印设备的文档时,图像处理装置101向设备认证服务服务器104做出设备认证请求。

[0107] 图8例示了根据本应用的序列。在下文的描述中省略了与图4所示的处理类似的处理。

[0108] 在步骤S801中,图像处理装置101的文档请求单元351将在步骤S406的处理中获得断言信息发送至打印服务服务器103。根据第一示例性实施例,从设备认证服务服务器104获得的认证令牌被设置给图5C例示的扩展区域532。根据本应用,包括数据未设置于扩展区域的客户数据524(如图5D所示)的断言信息,被发送至打印服务服务器103。

[0109] 在图4的步骤S411的处理之后,在步骤S802中,打印服务服务器103中的文档请求接收单元315参照表A,并搜索与用户ID相关联的文档的数据,该用户ID作为在步骤S411中的验证的结果而被指定。当指定能够打印的设备的文档的数据存在于在表A中搜索的数据中时,执行步骤S803至S812的处理,并且当不存在相关数据时,执行步骤S813的处理。

[0110] 在步骤S803中,作为对步骤S801的处理的响应,打印服务服务器103的文档请求接收单元315指示图像处理装置101进行设备认证。

[0111] 在步骤S804中,作为对设备认证的指令的响应,图像处理装置101将设备认证请求发送至设备认证服务服务器104。步骤S804至S806的处理与在图4中的步骤S407至S409中描述的处理类似,因此这里省略对步骤S804至S806的描述。

[0112] 在步骤S807中,图像处理装置101将在步骤S806返回的认证令牌增加至在步骤S406返回的断言信息数据,并将上述认证令牌和断言信息数据发送至打印服务服务器103。

步骤S807中发送的断言信息数据中包括的客户数据是，在图5C中例示的认证令牌被设置给扩展区域532的客户数据。

[0113] 步骤S808至S812的处理与在图4中的步骤S411至S415中所述的处理类似，因此这里省略对步骤S808至S812的描述。

[0114] 在步骤S813中，文档请求接收单元315利用与用户ID相关联的文档的数据生成文档列表，该用户ID作为步骤S411中的验证的结果从表A中指定。

[0115] 上文中参照图4描述了步骤S416和后续步骤中的处理，因此这里省略其描述。

[0116] 如上所述，根据第一应用，仅当经生物认证的用户的打印目标文档请求设备认证时，图像处理装置101向设备认证服务服务器104发送设备认证请求。因此，能够减少本系统的负荷。

[0117] 根据上述各个示例性实施例，基于利用图像处理装置的设备ID和密码的设备登记，进行严格的设备认证。

[0118] 根据第二应用，描述了能够用来输出的设备根据图像处理装置的位置信息而受到限制的示例。根据第二应用，表示图像处理装置101的安装地址的位置信息、或者通过连接至图像处理装置101以进行生物认证的便携式终端102获得的位置信息，被包括在断言信息中并且从图像处理装置101发送至打印服务服务器103。打印服务服务器103基于位置信息指定在便携式终端102中经生物认证的用户能够通过图像处理装置101打印的文档的数据。

[0119] 更具体地，当发送断言信息时，如下文所示，位置信息(而不是上述认证令牌)被设置给参照图5C描述的客户数据524中的扩展区域532。在下文的示例中，在geoinfo密钥中设置纬度信息和经度信息:

[0120] {'geoinfo':{'Latitude':57.64911,'Longitude':10.40744}}

[0121] 在步骤S416中，打印服务服务器103仅包括，通过文档列表中的位置信息粗略地指定的图像处理装置能够打印的文档的文档ID。

[0122] 根据第一和第二示例性实施例以及第一和第二应用，打印服务作为示例描述。根据本公开，系统能够类似地作为第三应用实现，其中选自从网络上的服务提供装置获得的列表的数据在步骤S419获得，并且图像处理装置进行三维形状物体的画面输出和打印输出，而不是上述打印处理。

[0123] 另外，根据本公开，输入至图像处理装置的数据(例如扫描数据和拍摄图像)可以基于用户从网络上的服务提供装置获得的存储服务(例如URL和文件夹)的列表中的选择，而被输出至选定的目的地。

[0124] 例如，图像处理装置101根据在步骤S417的定时图像处理装置101的显示设备上的显示，来选择扫描数据被存储到的存储服务。在这种情况下，安装扫描服务服务器(未示出)代替打印服务服务器103作为服务提供装置。包括用户在存储服务的选择中能够使用的服务的列表，被从存储服务提供至图像处理装置101。存储服务通过以与上述示例性实施例类似的方式验证断言信息中的签名来指定用户ID。存储服务的示例可以包括Evernote®和Dropbox®。

[0125] 扫描服务服务器在图4的步骤S411中验证断言信息，并且当指定用户时生成存储服务的列表，用户预先将合作设置给该存储服务。此处生成的存储服务列表包括服务的登

录画面的URL，并且具有如下所示构造：{'storagelist':{'evernote':'http://evernote.com/login'},{'dropbox':'http://dropbox.com/login'}}

[0126] 在步骤S416中返回存储服务列表(代替可打印文档列表)，并且在步骤S417显示在存储服务上。用户从显示的存储服务列表中选择扫描数据被存储到的服务，并进行登录处理。因此扫描服务服务器执行扫描数据到选择的存储服务的存储。

[0127] 其它实施例

[0128] 本公开包括通过适当地组合上述示例性实施例(第一和第二示例性实施例和第一至第三应用)而构成的装置和系统及其方法。

[0129] 另外，可以通过读出并执行记录在存储介质(也可更完整地称为“非临时性计算机可读存储介质”)上的计算机可执行指令(例如，一个或更多个程序)以执行上述实施例中的一个或更多个的功能、并且/或者包括用于执行上述实施例中的一个或更多个的功能的一个或更多个电路(例如，专用集成电路(ASIC))的系统或装置的计算机，来实现本发明的实施例，并且，可以利用通过由所述系统或装置的所述计算机例如读出并执行来自所述存储介质的所述计算机可执行指令以执行上述实施例中的一个或更多个的功能、并且/或者控制所述一个或更多个电路执行上述实施例中的一个或更多个的功能的方法，来实现本发明的实施例。所述计算机可以包括一个或更多个处理器(例如，中央处理单元(CPU)，微处理单元(MPU))，并且可以包括分开的计算机或分开的处理器的网络，以读出并执行所述计算机可执行指令。所述计算机可执行指令可以例如从网络或所述存储介质被提供给计算机。所述存储介质可以包括例如硬盘、随机存取存储器(RAM)、只读存储器(ROM)、分布式计算系统的存储器、光盘(诸如压缩光盘(CD)、数字通用光盘(DVD)或蓝光光盘(BD)TM)、闪存设备以及存储卡等中的一个或更多个。

[0130] 本发明的实施例还可以通过如下的方法来实现，即，通过网络或者各种存储介质将执行上述实施例的功能的软件(程序)提供给系统或装置，该系统或装置的计算机或是中央处理单元(CPU)、微处理单元(MPU)读出并执行程序的方法。

[0131] 虽然参照示例性实施例对本发明进行了描述，但是应当理解，本发明并不限于所公开的示例性实施例。应当对所附权利要求的范围给予最宽的解释，以使其涵盖所有这些变型例以及等同的结构和功能。

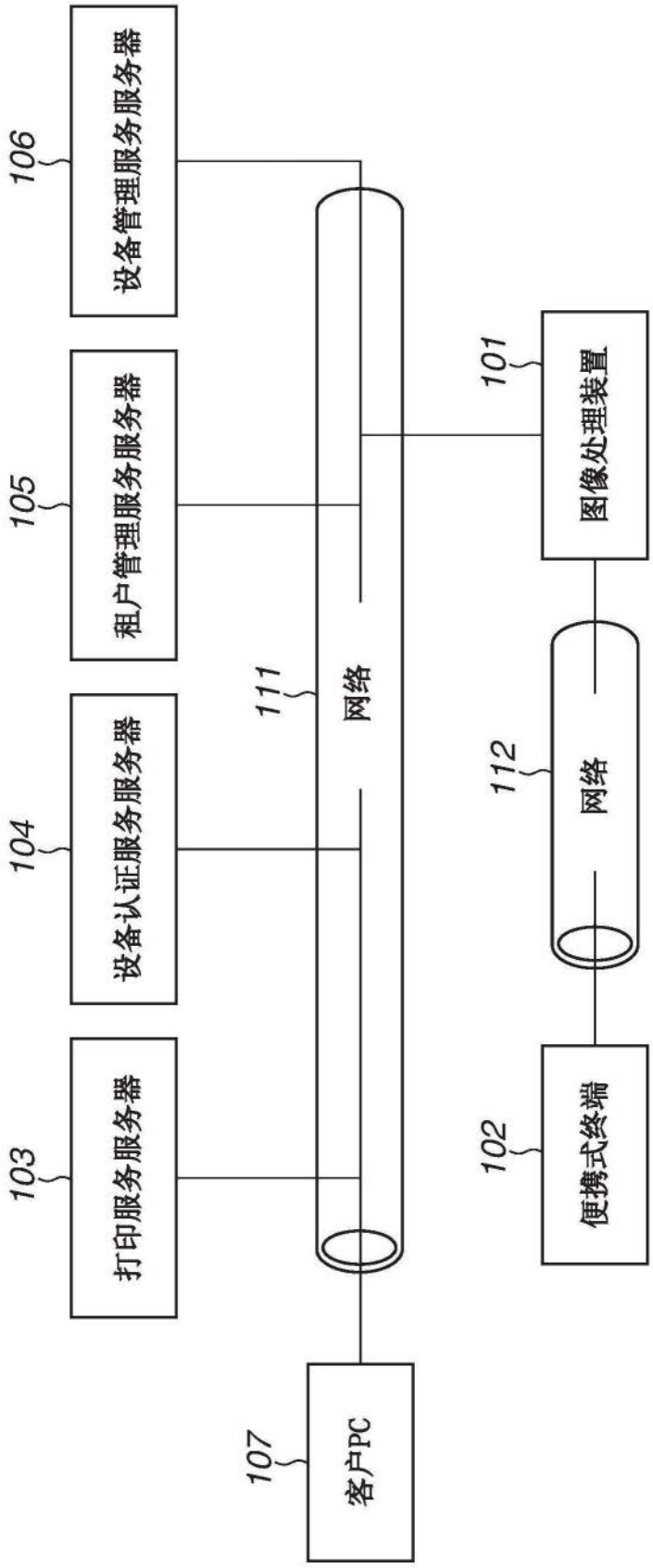

106
设备管理服务服务器
105
租户管理服务服务器
104
设备认证服务服务器
103
打印服务服务器
111
网络
107
客户PC
101
图像处理装置
112
网络
102
便携式终端

图1

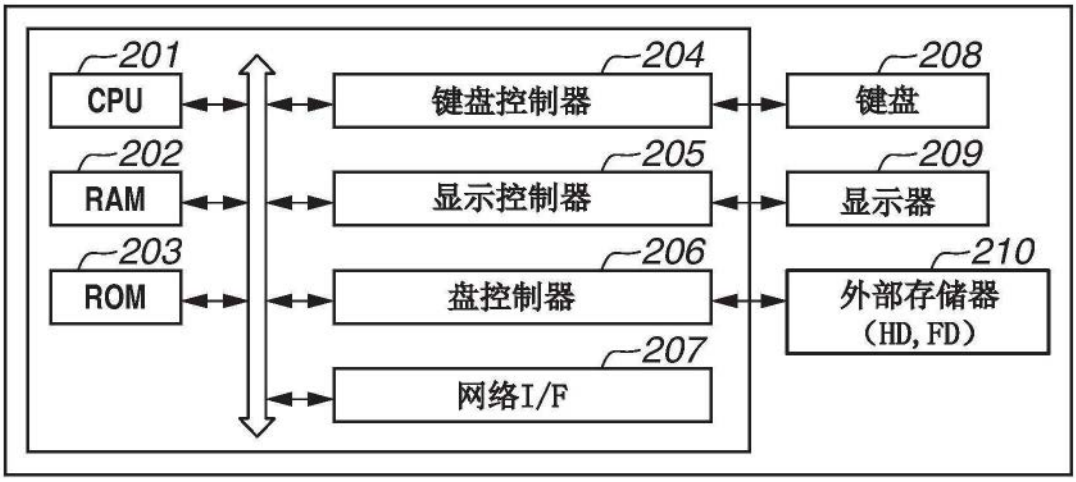

201
CPU
202
RAM
203
ROM
204
键盘控制器
205
显示控制器
206
盘控制器
207
网络I/F
208
键盘
209
显示器
210
外部存储器
(HD,FD)

图2A

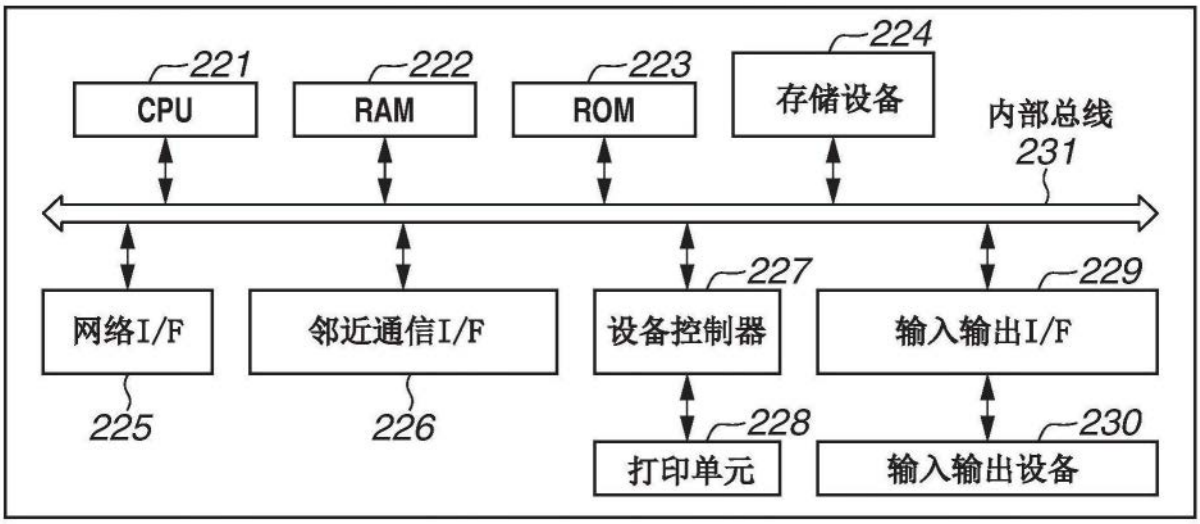

221
CPU
222
RAM
223
ROM
224
存储设备
内部总线
231
网络I/F
225
邻近通信I/F
226
227
设备控制器
228
打印单元
229
输入输出I/F
230
输入输出设备

图2B

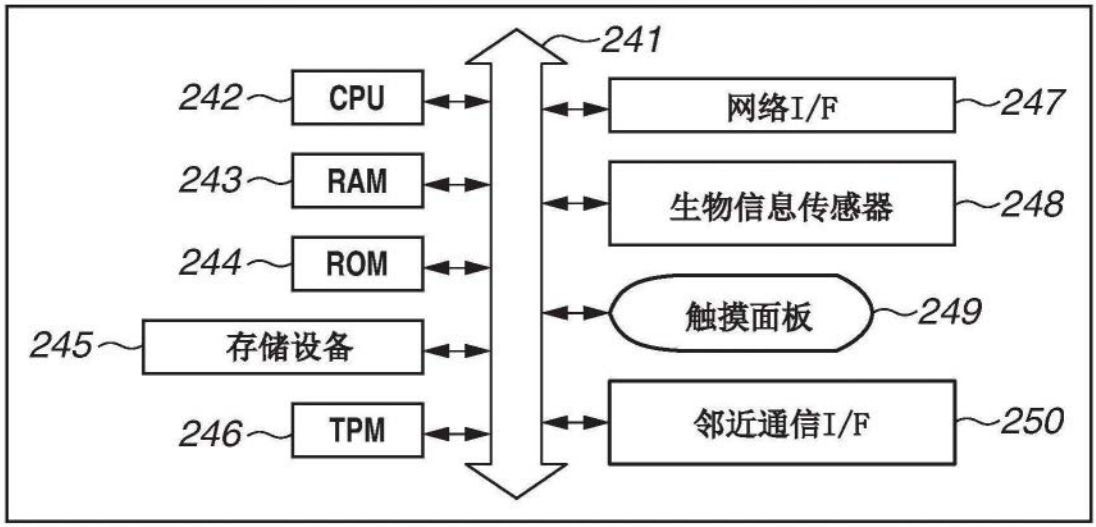

241
242
CPU
243
RAM
244
ROM
245
存储设备
246
TPM
网络I/F
247
生物信息传感器
248
触摸面板
249
邻近通信I/F
250

图2C

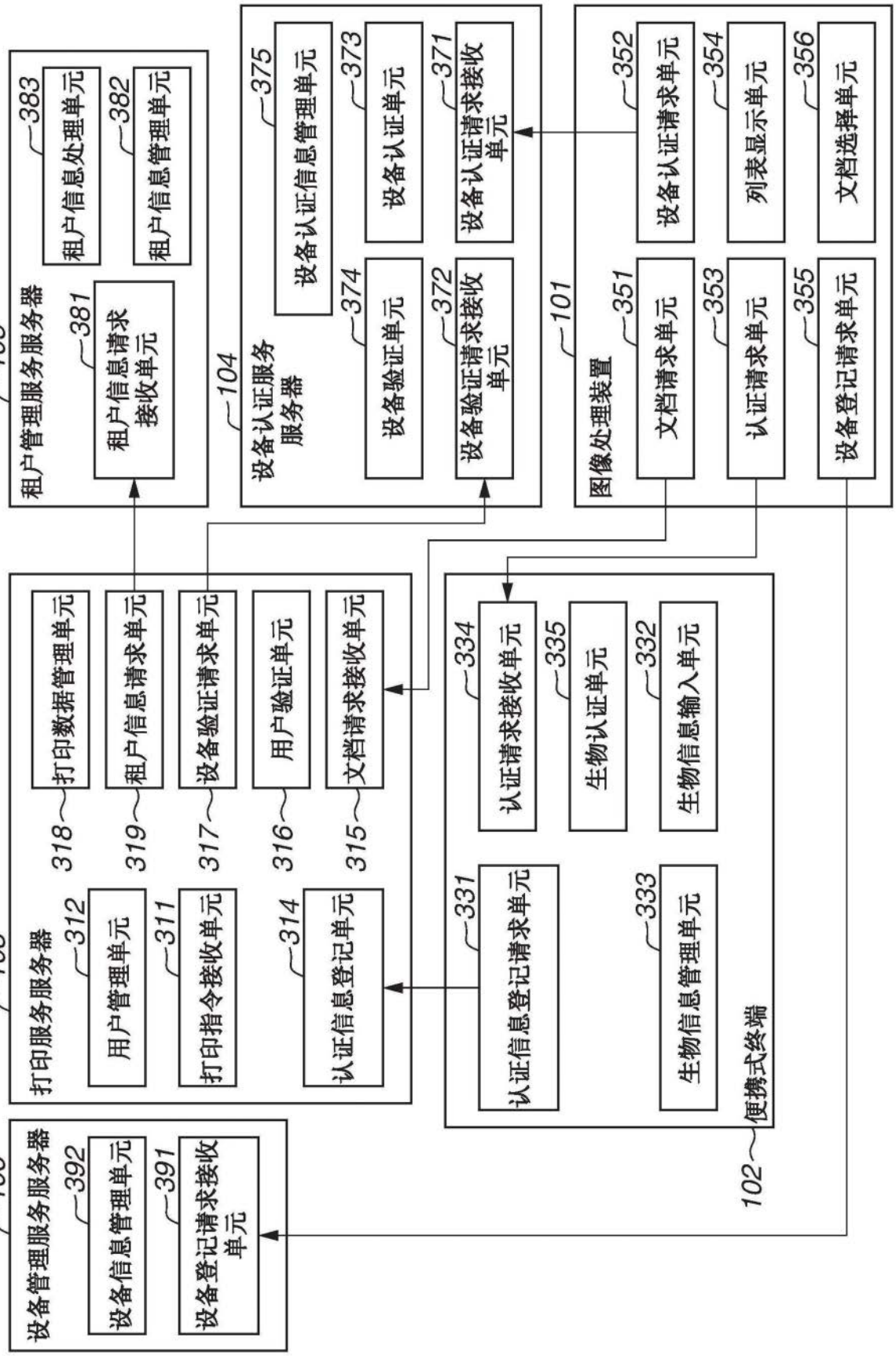

105
租户管理服务服务器
381
租户信息请求接收单元
383
租户信息处理单元
382
租户信息管理单元
104
设备认证服务服务器
375
设备认证信息管理单元
374
设备验证单元
373
设备认证单元
372
设备验证请求接收单元
371
设备认证请求接收单元
101
图像处理装置
351
文档请求单元
352
设备认证请求单元
353
认证请求单元
354
列表显示单元
355
设备登记请求单元
356
文档选择单元
103
打印服务服务器
318
打印数据管理单元
319
租户信息请求单元
317
设备验证请求单元
316
用户验证单元
315
文档请求接收单元
312
用户管理单元
311
打印指令接收单元
314
认证信息登记单元
331
认证信息登记请求单元
334
认证请求接收单元
335
生物认证单元
332
生物信息输入单元
333
生物信息管理单元
102
便携式终端
106
设备管理服务服务器
392
设备信息管理单元
391
设备登记请求接收单元

图3

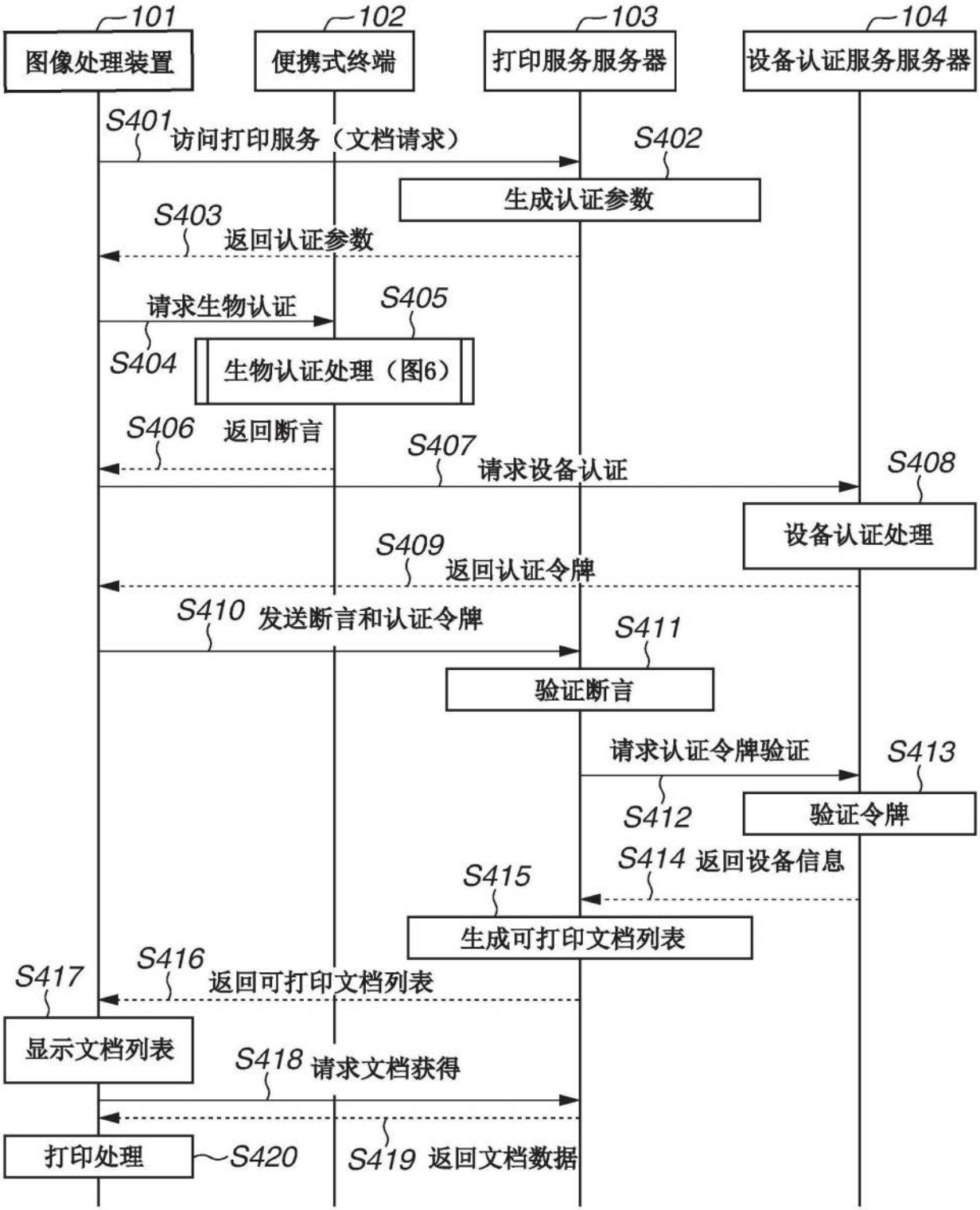

101
图像处理装置
102
便携式终端
103
打印服务服务器
104
设备认证服务服务器
S401
访问打印服务（文档请求）
S402
生成认证参数
S403
返回认证参数
请求生物认证
S405
S404
生物认证处理（图6）
S406
返回断言
S407
请求设备认证
S408
设备认证处理
S409
返回认证令牌
S410
发送断言和认证令牌
S411
验证断言
请求认证令牌验证
S413
S412
验证令牌
S414
返回设备信息
S415
生成可打印文档列表
S416
返回可打印文档列表
S417
显示文档列表
S418
请求文档获得
打印处理
S420
S419
返回文档数据

图4

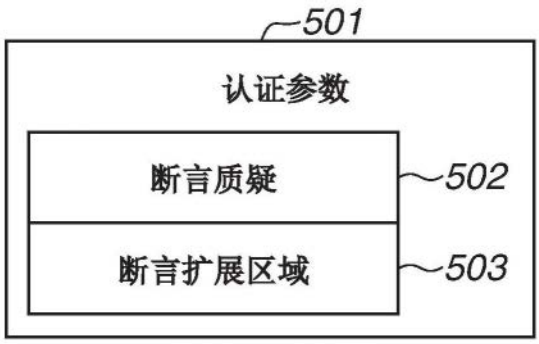

501
认证参数
断言质疑
502
断言扩展区域
503

图5A

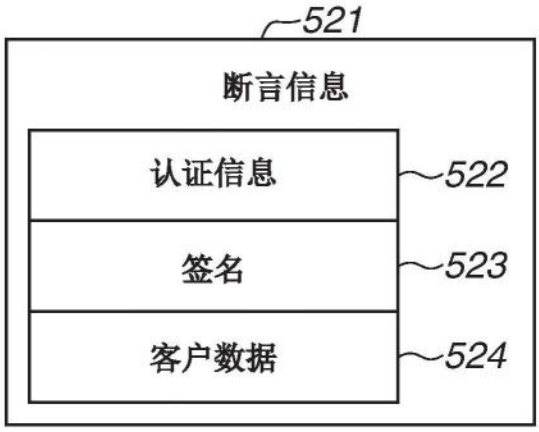

521
断言信息
认证信息
522
签名
523
客户数据
524

图5B

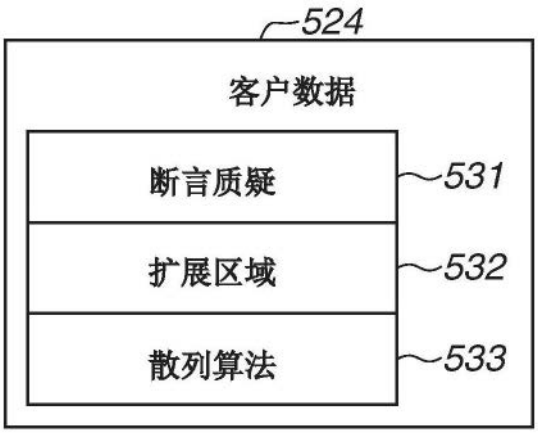

524
客户数据
断言质疑
531
扩展区域
532
散列算法
533

图5C

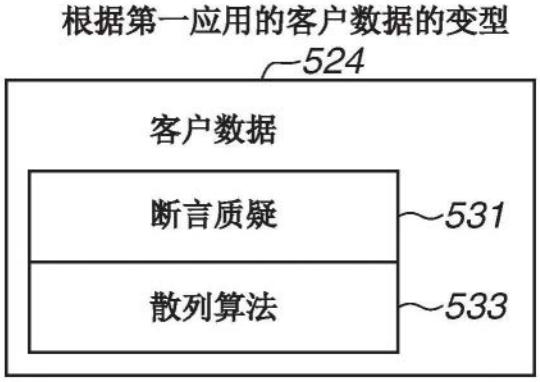

根据第一应用的客户数据的变型
524
客户数据
断言质疑
531
散列算法
533

图5D

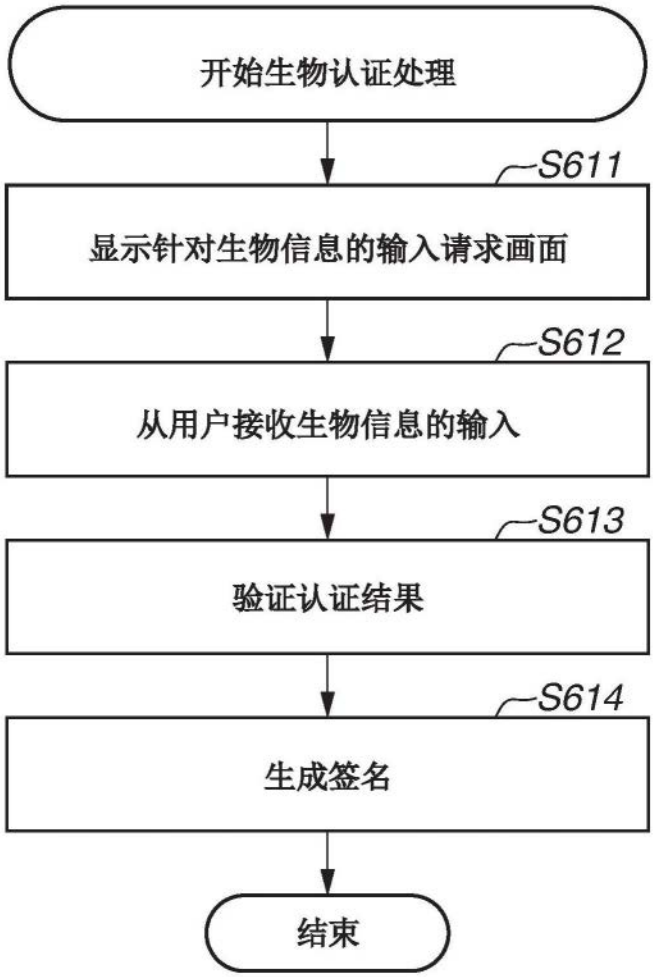

开始生物认证处理
S611
显示针对生物信息的输入请求画面
S612
从用户接收生物信息的输入
S613
验证认证结果
S614
生成签名
结束

图6

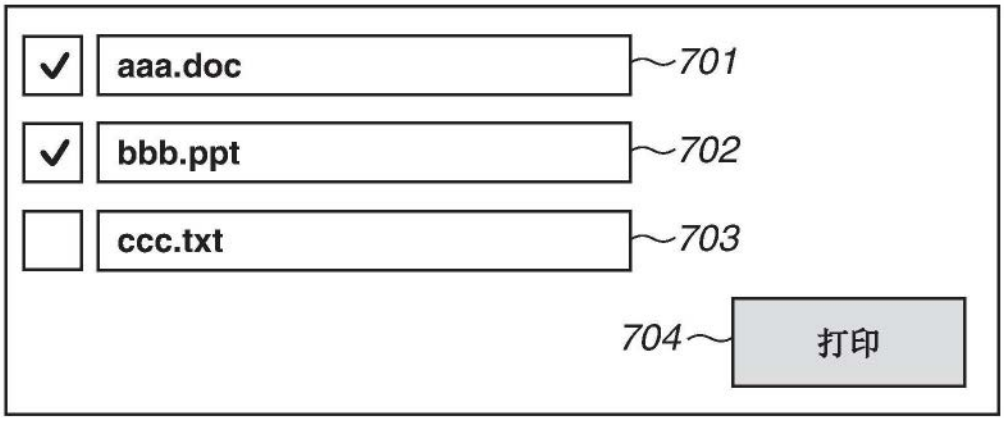

aaa.doc
701
bbb.ppt
702
ccc.txt
703
704
打印

图7A

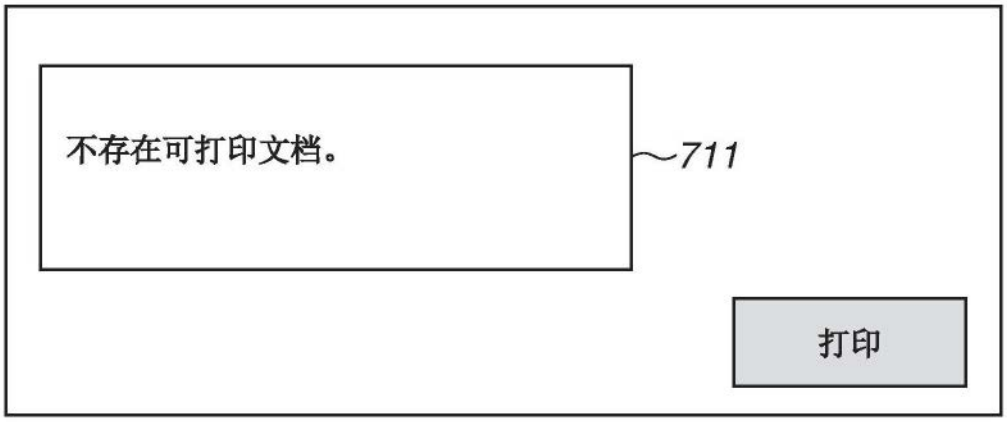

不存在可打印文档。
711
打印

图7B

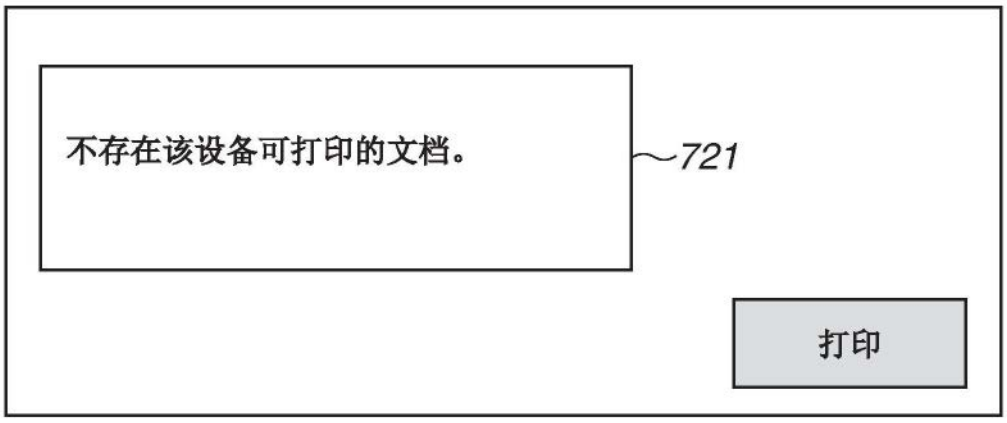

不存在该设备可打印的文档。
721
打印

图7C

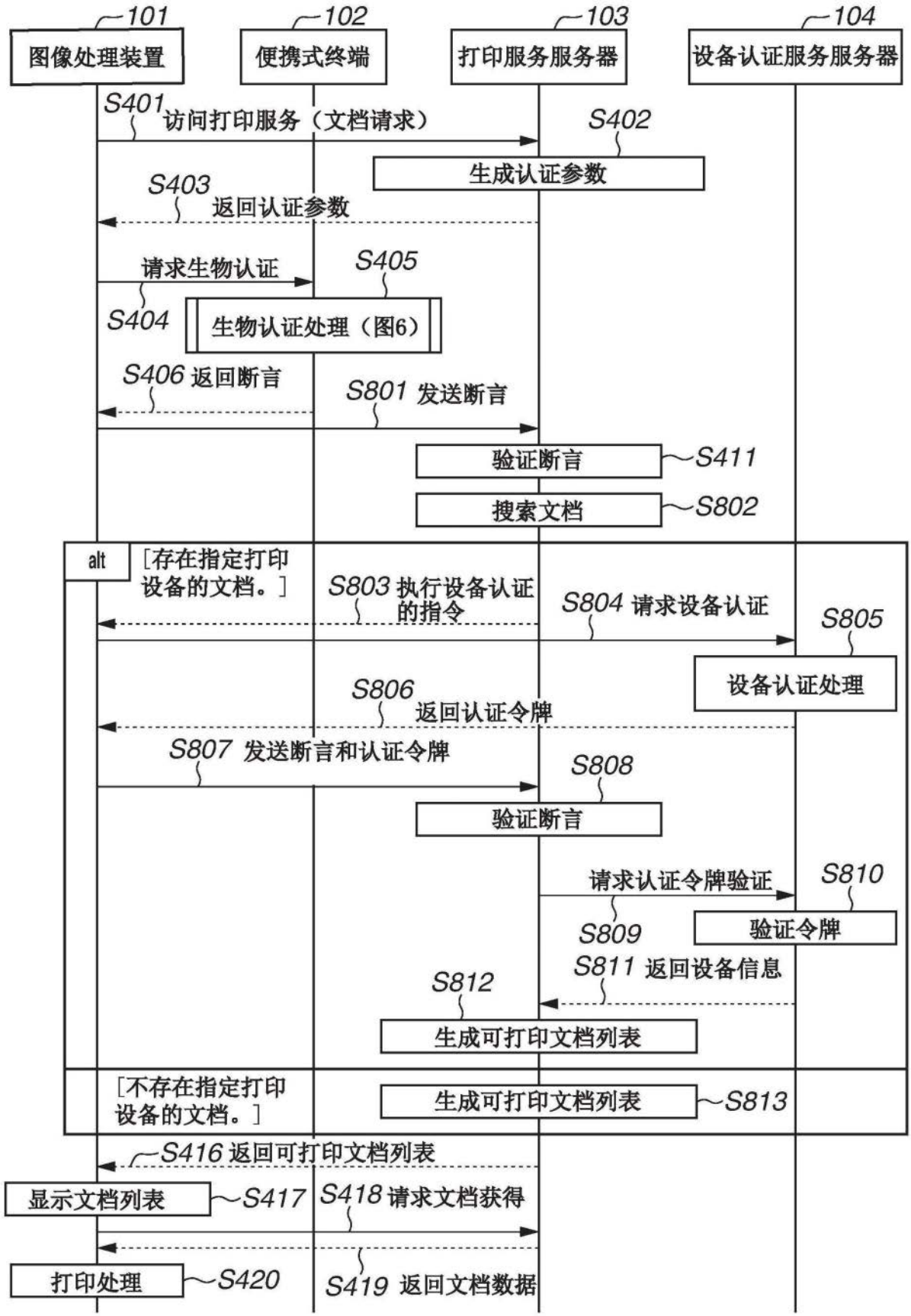

101
图像处理装置
102
便携式终端
103
打印服务服务器
104
设备认证服务服务器
S401
访问打印服务（文档请求）
S402
生成认证参数
S403
返回认证参数
请求生物认证
S405
S404
生物认证处理（图6）
S406 返回断言
S801 发送断言
验证断言
S411
搜索文档
S802
alt
[存在指定打印设备的文档。]
S803 执行设备认证的指令
S804 请求设备认证
S805
设备认证处理
S806
返回认证令牌
S807 发送断言和认证令牌
S808
验证断言
请求认证令牌验证
S810
S809
验证令牌
S811 返回设备信息
S812
生成可打印文档列表
[不存在指定打印设备的文档。]
生成可打印文档列表
S813
S416 返回可打印文档列表
显示文档列表
S417
S418 请求文档获得
打印处理
S420
S419 返回文档数据

图8

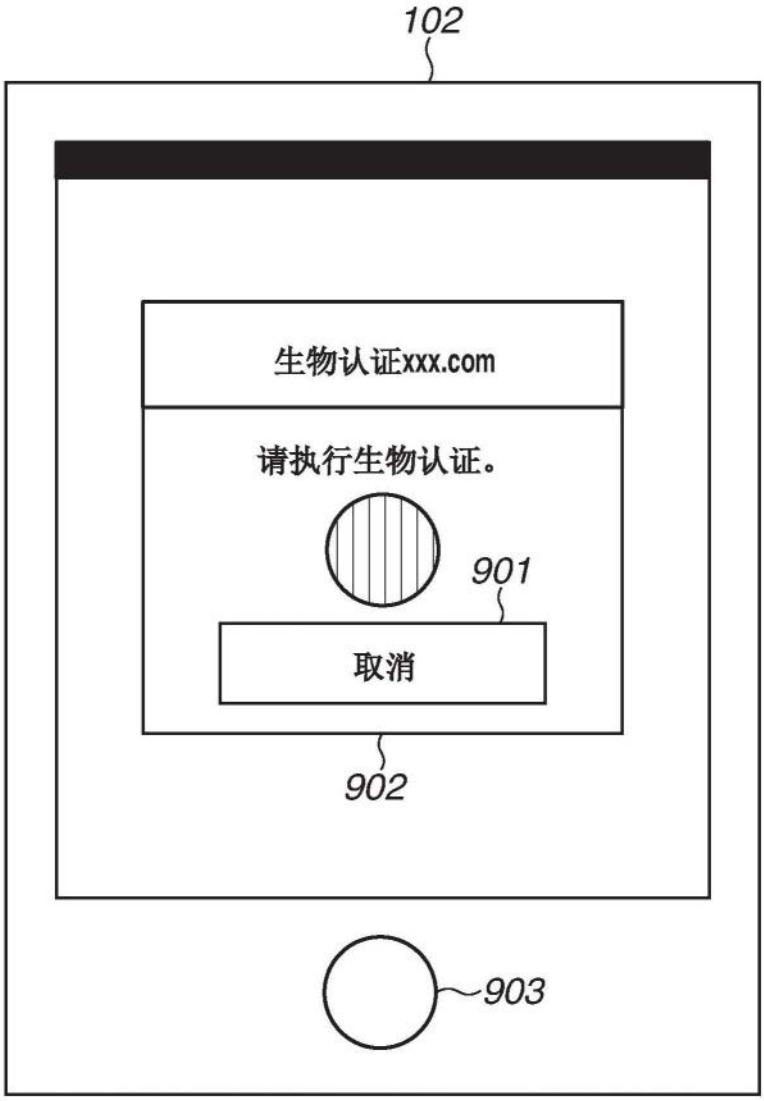


图9