(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112602079 B
(45)授权公告日 2024.11.29

(21)申请号 201980055509.7
(22)申请日 2019.08.20
(65)同一申请的已公布的文献号
申请公布号 CN 112602079 A
(43)申请公布日 2021.04.02
(30)优先权数据
10-2018-0099432 2018.08.24 KR
(85)PCT国际申请进入国家阶段日
2021.02.23
(86)PCT国际申请的申请数据
PCT/KR2019/010576 2019.08.20
(87)PCT国际申请的公布数据
WO2020/040525 EN 2020.02.27
(73)专利权人 三星电子株式会社
地址 韩国京畿道
(72)发明人 柳永善 李德基 尹江镇
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 张婧
(51)Int.Cl.
G06F 21/32(2013.01)
G06F 21/60(2013.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)
(56)对比文件
WO 2017044554 A1,2017.03.16
KR 20160086830 A,2016.07.20
审查员 李丹

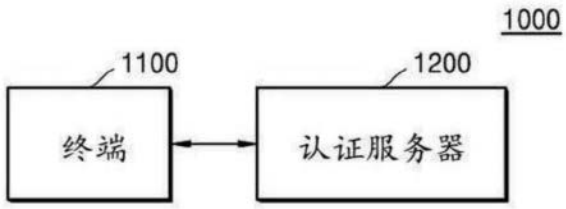
权利要求书2页 说明书17页 附图15页

(54)发明名称

用于认证生物识别信息的方法和装置

(57)摘要

提供了一种用于认证生物识别信息的终端、服务器和系统以及生物识别信息认证方法。一种由终端执行的注册生物识别信息的方法,包括:向服务器发送注册请求和终端的生物识别能力信息;从服务器接收服务器的生物识别能力信息;基于服务器的生物识别能力信息获取用户的生物识别信息;基于用户的生物识别信息获取假名标识符(PI)和辅助数据(AD);以及将PI和AD发送到服务器。



CN 112602079 B

1.一种由终端执行的注册生物识别信息的方法,所述方法包括:

向服务器发送注册请求和终端的生物识别能力信息,其中,终端的生物识别能力信息包括关于由终端支持的生物识别技术的信息;

从服务器接收服务器的生物识别能力信息,其中,服务器的生物特征能力信息包括基于从终端发送到服务器的终端的生物识别能力信息的、关于由服务器支持的生物特征技术的信息;基于接收到的服务器的生物识别能力信息,选择生物识别技术;

基于所选择的生物识别技术,获取用户的生物识别信息;

基于用户的生物识别信息获取假名标识符和辅助数据;以及

向服务器发送假名标识符和辅助数据。

2.根据权利要求1所述的方法,其中:

关于生物识别技术的信息包括生物识别技术的项目和关于被执行以获得模板的算法的信息。

3.根据权利要求1所述的方法,其中:

基于接收到的服务器的生物识别能力信息选择生物识别技术包括:

基于服务器的生物识别能力信息,向用户呈现多个生物识别技术,以及

从用户接收选择所述多个生物识别技术中的一个的输入。

4.根据权利要求1所述的方法,其中:

从服务器接收服务器的生物识别能力信息包括从服务器接收服务器的公钥证书,其中服务器的公钥证书由证书颁发机构颁发。

5.根据权利要求4所述的方法,还包括:

基于服务器的公钥证书,使用服务器的公钥对假名标识符和辅助数据进行加密,

其中,向服务器发送假名标识符和辅助数据包括向服务器发送加密的假名标识符和加密的辅助数据。

6.根据权利要求4所述的方法,其中:

从服务器接收服务器的生物识别能力信息包括从服务器接收质询信息,其中质询信息包括由服务器生成的信息以验证从终端发送的信息的可靠性和完整性。

7.根据权利要求6所述的方法,还包括:

通过使用服务器的公钥,基于服务器的公钥证书对假名标识符、辅助数据和质询信息进行加密,

其中,向服务器发送假名标识符和辅助数据包括向服务器发送加密的假名标识符、加密的辅助数据和加密的质询信息。

8.根据权利要求1所述的方法,其中:

终端通过使用传输层安全信道向服务器发送信息或从服务器接收信息。

9.一种用于通过使用生物识别信息来认证用户的终端,所述终端包括:

输入/输出接口,被配置为发送或接收信息;

生物识别信息输入器,被配置为从用户获取生物识别信息;以及

生物识别信息客户端,

其中,输入/输出接口还被配置为:

向服务器发送注册请求和终端的生物识别能力信息,其中,终端的生物识别能力信息

包括关于由终端支持的生物识别技术的信息,以及

从服务器接收服务器的生物识别能力信息以将服务器的生物识别能力信息发送到生物识别信息客户端,其中,服务器的生物特征能力信息包括基于从终端发送到服务器的终端的生物识别能力信息的、关于由服务器支持的生物特征技术的信息,以及

其中,生物识别信息客户端被配置为:

控制生物识别信息输入器:

基于接收到的服务器的生物识别能力信息,选择生物识别技术;

基于所选择的生物识别技术,获取用户的生物识别信息,

基于用户的生物识别信息获取假名标识符和辅助数据,以及

经由输入/输出接口将假名标识符和辅助数据发送到服务器。

10.根据权利要求9所述的终端,其中:

关于生物识别技术的信息包括生物识别技术的项目和关于被执行以获得模板的算法的信息。

11.根据权利要求9所述的终端,其中:

生物识别信息客户端还被配置为控制生物识别信息输入器基于服务器的生物识别能力信息向用户呈现多个生物识别技术,并在从用户接收到选择所述多个生物识别技术中的一个的输入时基于选择的生物识别技术获取生物识别信息。

12.根据权利要求9所述的终端,其中:

生物识别信息客户端还被配置为经由输入/输出接口接收服务器的公钥证书,其中服务器的公钥证书由证书颁发机构颁发。

13.根据权利要求12所述的终端,其中:

生物识别信息客户端还被配置为基于服务器的公钥证书,用服务器的公钥对假名标识符和辅助数据进行加密;以及

经由输入/输出接口将加密的假名标识符和加密的辅助数据发送到服务器。

用于认证生物识别信息的方法和装置

技术领域

[0001] 本发明涉及生物识别信息的注册以及基于生物识别信息的注册来提供认证生物识别信息的服务的装置和方法。

背景技术

[0002] 生物识别是一种身份验证方法,它涉及提取个人唯一的生物特征,诸如对每个人都不同的指纹、声音、人脸、虹膜和血管,并将它们转换为可处理的信息。随着对安全性的需求变得越来越重要,生物识别技术已被广泛用于认证请求访问室内区域的用户。

[0003] 生物识别技术采用使用人体的部分的各种方法,诸如人脸识别、指纹识别、虹膜识别、血管识别等。与密钥或密码不同的是,个人的特征(诸如脸型、声音、指纹和眼球)不能被窃取或复制供他人使用。此外,由于这些特征具有较低的更改或丢失风险,因此在安全应用中得到了广泛的应用。

[0004] 由于移动通信系统和电子设备的进步,可以提供各种服务。因此,需要基于这些生物识别技术有效地提供服务的方法。

发明内容

[0005] 技术问题

[0006] 需要一种能够使用生物识别信息有效地提供用户认证服务的装置和方法。

[0007] 技术方案

[0008] 根据本公开的一个实施例,由终端执行的注册生物识别信息的方法包括:向服务器发送注册请求和终端的生物识别能力信息;从服务器接收服务器的生物识别能力信息;基于服务器的生物识别能力信息获取用户的生物识别信息;基于用户的生物识别信息获取假名(pseudonymous)标识符(PI)和辅助数据(AD);以及将PI和AD发送到服务器。

[0009] 有益效果

[0010] 提供了一种能够使用生物识别信息有效地提供用户认证服务的装置和方法。

附图说明

[0011] 为了更全面地理解本发明及其优点,现在结合附图参考以下描述,其中类似的附图标记表示类似的部分:

[0012] 图1示出了根据本公开的实施例的生物识别信息认证系统的配置的框图;

[0013] 图2示出了示出根据本公开的实施例的生物识别信息认证系统的详细配置的框图;

[0014] 图3A示出了根据本公开的实施例的注册生物识别信息的方法的流程图;

[0015] 图3B示出了根据本公开的实施例的认证生物识别信息的方法的流程图;

[0016] 图4示出了根据本公开的实施例的注册生物识别信息的方法的流程图;

[0017] 图5示出了根据本公开的实施例的用于说明注册生物识别信息的方法的流程图;

[0018] 图6示出了根据本公开的实施例的认证生物识别信息的方法的流程图；

[0019] 图7示出了根据本公开的实施例的用于说明认证生物识别信息的方法的流程图；

[0020] 图8示出了根据本公开的实施例的注册生物识别信息的方法的流程图；

[0021] 图9示出了根据本公开的实施例的用于说明注册生物识别信息的方法的流程图；

[0022] 图10示出了根据本公开的实施例的认证生物识别信息的方法的流程图；

[0023] 图11示出了根据本公开的实施例的用于说明认证生物识别信息的方法的流程图；

[0024] 图12示出了根据本公开的实施例的用于说明注册和传送生物识别信息的方法的图；

[0025] 图13A示出了根据本公开的实施例的注册和传送生物识别信息的方法的流程图；

[0026] 图13B示出了根据本公开的实施例的注册和传送生物识别信息的方法的流程图；

[0027] 图14示出了根据本公开的实施例的用于说明注册生物识别信息的方法的流程图；

[0028] 图15示出了根据本公开的实施例的用于说明传送生物识别信息的方法的流程图；以及

[0029] 图16示出了根据本公开的实施例的用于说明撤销生物识别信息的方法的流程图。

优选实施例

[0030] 提供了一种能够使用生物识别信息有效地提供用户认证服务的装置和方法。

[0031] 附加方面将在随后的说明书中部分阐述，并且部分地将从说明书中显而易见，或者可以通过本公开的实施例的实践来习得。

[0032] 根据本公开的一个实施例，一种由终端执行的注册生物识别信息的方法包括：向服务器发送注册请求和终端的生物识别能力信息；从服务器接收服务器的生物识别能力信息；基于服务器的生物识别能力信息获取用户的生物识别信息；基于用户的生物识别信息获取假名标识符(PI)和辅助数据(AD)；以及将PI和AD发送到服务器。

具体实施方式

[0033] 以下讨论的图1到16以及用于描述本专利文件中本发明的原理的各种实施例仅作为说明，不应以任何方式解释为限制本发明的范围。本领域技术人员将理解，本发明的原理可以在任何适当布置的系统或设备中实现。

[0034] 将参考附图更全面地描述本公开的实施例。此外，将参考附图详细描述根据本公开的实施例的构造和使用电子设备的方法。在附图中，类似的附图标记或符号是指执行基本相同功能的类似部件或元件。应当理解，尽管包括诸如“第一”、“第二”等序号的术语可在本文中用于描述各种元件或组件，但这些元件或组件不应受到术语的限制。这些术语仅用于区分一个元件或组件与另一个元件或组件。例如，在不脱离本发明的范围的情况下，下面要讨论的第一元件或组件可以被称为第二元件或组件。类似地，第二元件或组件可被称为第一元件或组件。如本文所使用的，术语“和/或”包括一个或多个相关联的所列项目的任何和所有组合。本文中使用的术语仅用于描述本公开的实施例，并不旨在限制本公开的实施例。如本文所使用的，除非上下文另有明确指示，否则单数形式也意在包括复数形式。应进一步理解，当在本说明书中使用术语“包含”和/或“包括”时，规定所述特征、整数、步骤、操作、元件、组件或其组合的存在，但不排除一个或多个其他特征、整数、步骤、操作、元件、组件或其组合的存在或添加。

[0035] 在整个公开中,“a、b或c中的至少一个”表示仅a、仅b、仅c、a和b两者、a和c两者、b和c两者、全部a、b和c或其变体。

[0036] 图1示出了根据本公开的实施例的生物识别信息认证系统1000的配置的框图。

[0037] 参考图1,生物识别信息认证系统1000包括终端1100和认证服务器1200。

[0038] 终端1100可以从用户获取生物识别信息。根据本公开的一个实施例,生物识别信息是指包含生物识别特性的信息,该生物识别特性对于每个用户来说是时不变的和唯一的。例如,生物识别信息可以是关于脸型、虹膜、视网膜、静脉、指纹或脱氧核糖核酸(DNA)中的至少一个的信息。生物识别信息也可称为生物信息。

[0039] 终端1100可以基于生物识别信息来确定用户是否是授权用户。详细地,终端1100可以执行用于注册基于用户的生物识别信息生成的信息的生物识别信息注册过程和生物识别信息认证过程。生物识别信息认证过程涉及将注册信息与请求认证时获取的信息进行比较,并确定用户是否是授权用户。

[0040] 根据本公开的一个实施例,在生物识别信息注册过程中,终端1100可以将基于用户的生物识别信息生成的信息的一部分发送到认证服务器1200,并从认证服务器1200请求注册。此外,当由用户请求认证时,终端1100可以将基于用户的生物识别信息生成的信息的一部分发送到认证服务器1200,并从认证服务器1200接收认证的结果。根据本公开的一个实施例,当由用户请求认证时,终端1100可以请求来自认证服务器1200的附加信息的传输,基于用户的生物识别信息和从认证服务器1200接收的附加信息生成信息,以及将生成的信息的一部分发送到认证服务器1200。从认证服务器1200接收的附加信息可以包括在生物识别信息注册过程期间注册的信息。

[0041] 为了保护用户的生物识别信息免受外部攻击,终端1100和认证服务器1200可以通过使用各种类型的安全技术来发送或接收基于用户的生物识别信息生成的信息。此外,认证服务器1200可以包括用于与终端1100交换数据的服务器和与服务器分离的用于执行处理和存储生物识别信息的操作的生物服务器。然而,这仅仅是示例,并且根据本发明的服务器的配置不限于此。

[0042] 另外,终端1100可以基于从用户获取的生物识别信息来获取模板。模板是指通过基于生物识别信息执行算法处理以分析和提取生物识别信息中的生物识别特性而获得的特征信息,并且可以包括用户的唯一生物识别信息。根据本公开的一个实施例,模板可以包括假名标识符(pseudonymous identifier,以下称为“PI”)和辅助数据(以下称为“AD”)。终端1100可以通过使用模板而不是直接使用用户的生物识别信息来注册和认证生物识别信息来防止生物识别信息泄漏的风险。根据本公开的一个实施例,终端1100可以将终端1100的生物识别能力信息发送到认证服务器1200,同时从认证服务器1200请求注册用户的生物识别信息。生物识别能力信息是指关于由终端1100支持的生物识别技术的信息。生物识别技术可以指经由自动化设备提取用户的唯一生物识别信息以创建模板的技术。生物识别技术也可以被称为Bio认证技术。根据本公开的一个实施例,生物识别能力信息可以包括终端1100可以获取的生物识别信息项(例如,每个用户的脸型、虹膜、视网膜、静脉、指纹、DNA等)和关于被执行以基于生物识别信息获取模板的算法的信息。

[0043] 终端1100可以从认证服务器1200接收认证服务器1200的生物识别能力信息。认证服务器1200的生物识别能力信息可以指认证服务器1200支持的多个生物识别技术中关于

由终端1100支持的生物识别技术的信息。

[0044] 终端1100可以基于认证服务器1200的生物识别能力信息获取用户的生物识别信息,并基于获取的生物识别信息获取模板。终端1100可以将获得的模板中的至少一些发送到认证服务器1200以注册基于用户的生物识别信息生成的信息或认证用户。

[0045] 图2示出了示出根据本公开的实施例的生物识别信息认证系统的详细配置的框图。

[0046] 参考图2,生物识别信息认证系统包括终端1100和服务器1200。终端1100包括生物识别信息客户端1110、输入/输出(I/O)接口1120、生物识别信息输入器1130和安全储存器1140。

[0047] 生物识别信息客户端1110执行处理生物识别信息的操作。生物识别信息客户端1110可以基于经由生物识别信息输入器1130获取的生物识别信息来获取模板,并控制安全储存器1140来存储模板。根据本公开的一个实施例,生物识别信息客户端1110位于终端1100的安全区域中,以阻止来自外部的访问。或者,生物识别信息客户端1110可以包括硬件安全模块(HSM)。HSM是一个专用的密码处理器,配备有密钥管理系统,可以确保硬件和密码两者安全。HSM可以使用经过物理安全认证的芯片。换句话说,HSM可以防止在硬件和软件方面未经授权地访问存储在芯片中的信息。

[0048] I/O接口1120可以接收来自用户10的输入,或者经由与用户10的交互向用户10提供处理结果。此外,I/O接口1120可以在与服务器1200通信时发送或接收信息。根据本公开的一个实施例,I/O接口1120可以是web浏览器或移动操作系统(OS)中的本机应用程序。

[0049] 生物识别信息输入器1130从用户10获取生物识别信息。生物识别信息输入器1130可以包括用于获取生物识别信息的传感器。可以由生物识别信息输入器1130获取的生物识别信息可以取决于终端1100的生物识别能力信息而变化。

[0050] 安全储存器1140基于由生物识别信息客户端1110的控制,存储诸如生物识别信息或安全密钥的需要安全性的信息,如下所述。根据本公开的一个实施例,安全储存器1140可以包括可信执行环境(TEE)或安全元件(SE)。然而,安全储存器1140不是根据本发明的终端1100的基本组件,或者当安全密钥没有存储在终端1100中时,可以不使用安全储存器1140。

[0051] 图3A和3B分别示出了注册基于生物识别信息生成的信息的方法和基于注册的信息认证用户的方法。

[0052] 图3A示出了根据本公开的实施例的生物识别信息注册方法的流程图。参考图3A,终端可以基于生物识别信息获得模板并存储获得的模板。

[0053] 终端获取用户的生物识别信息(S311)。用户的生物识别信息可以基于终端的生物识别能力信息而变化。

[0054] 终端可以基于获取的生物识别信息获取PI和AD(S321)。详细地,终端可以通过使用特征提取器从获取的生物识别信息中提取特征值。终端可以通过使用PI编码器(PIE)获得构成可更新生物识别参考(RBR)的PI和AD,其中RBR是可以从特征值更新的生物识别信息认证参考。

[0055] PI是可更新的个体标识符。基于生物识别信息获得PI作为散列值,包含基于从生物识别信息中提取的特征值获得的信息。然而,由于PI不包含用于重构生物识别信息的信息,因此即使当PI泄漏到外部时,也可以防止用户的生物识别信息的泄漏。AD是允许创建多

个PI的多样化数据,并且例如可以包含随机数或生成的密钥。换句话说,AD有助于从相同的生物识别特性生成多个PI。当获得PI和相对应的AD时,终端可以删除生物识别信息和提取的特征值。

[0056] 终端存储获得的PI和AD(S331)。当用户随后请求认证时,基于用户的生物识别信息获得的PI和AD可以用作认证用户的参考。

[0057] 图3B示出了根据本公开的实施例的生物识别信息认证方法的流程图。

[0058] 终端获取用户的生物识别信息(S312)。用户的生物识别信息可以基于终端的生物识别能力信息而变化。根据本公开的一个实施例,当由用户请求认证时,终端可以请求用户基于生物识别能力信息从支持的多条生物识别信息当中选择要被用于认证的生物识别信息,并经由生物识别信息输入器获取选择的生物识别信息。终端可以通过使用PI记录器(PIR)基于生物识别信息和存储的AD获得识别的PI(以下称为"PI*")(S322)。PI*是在认证时获得的PI,用于执行用户认证,即,验证用户的真实身份。与当从用户的生物识别信息获取PI时不同,基于生物识别信息和与PI一起预先获取的AD来生成PI*。

[0059] 终端基于PI*和存储的PI之间的比较结果执行生物识别认证过程(S332)。终端可以通过使用PI比较器(PIC)将PI*与PI进行比较,并基于比较结果提供认证结果。

[0060] 图4示出了根据本公开的实施例的生物识别信息注册方法的流程图。参考图4,终端可以向服务器发送获得的PI和AD。

[0061] 终端可以向服务器发送终端的生物识别能力信息,同时请求服务器注册与用户的生物识别信息相关的信息(S410)。

[0062] 终端可以接收服务器的生物识别能力信息(S420)。服务器的生物识别能力信息可以是与终端支持的生物识别技术相关的信息。基于从终端发送到服务器的生物识别能力信息,可以从服务器支持的多个生物识别技术中选择生物识别技术。

[0063] 终端可以基于服务器的生物识别能力信息获取用户的生物识别信息(S430)。终端可以经由生物识别信息输入器从用户获取生物识别信息。根据本公开的一个实施例,终端可以请求用户基于服务器的生物识别能力信息,从多条支持的生物识别信息中选择要用于认证的生物识别信息,并经由生物识别信息输入器获取选择的生物识别信息。

[0064] 终端基于获取的用户的生物识别信息获得PI和相对应的AD(S440)。PI和AD可以基于终端用于获得它们的算法以各种方式确定。根据本公开的一个实施例,终端可以经由生物识别信息客户端获得PI和AD。

[0065] 终端将获得的PI和AD发送到服务器(S450)。服务器可以通过存储从终端接收的PI和AD来完成生物识别信息注册过程。

[0066] 图5示出了根据本公开的实施例的用于说明生物识别信息注册方法的流程图。详细地,图5是用于说明参考图4描述的、根据本公开的实施例的生物信息注册方法中包括终端和服务器的生物信息认证系统的操作的流程图。

[0067] 用户10可以从终端的I/O接口1120请求服务连接(S501)。用户对服务连接的请求可以通过执行应用程序或web浏览器来作出。

[0068] I/O接口1120可以请求来自服务器1210的连接(S502)。连接请求可以使用超文本传输协议(HTTP)协议进行。传输层安全(TLS)信道可以被创建为I/O接口1120和服务器1210之间的安全通信信道(S503)。

[0069] I/O接口1120可以向服务器1210发送终端的生物识别能力信息和需要传输用户BioEnroll请求的注册请求(S504)。注册请求可以包括用于标识用户10的ID。

[0070] 服务器1210确定服务器1210的生物识别能力(S505)。详细地,服务器1210可以基于从终端发送到服务器1210的生物识别能力信息,从服务器1210支持的多个生物识别技术中选择与终端支持的生物识别技术相关的信息。服务器1210可以基于选择的信息获取服务器1210的生物识别能力信息。

[0071] 当服务器1210支持的生物识别技术不包括终端支持的生物识别技术时,服务器1210向I/O接口1120发送失败信号并终止注册过程(S506)。

[0072] 服务器1210可以在请求生物服务器1220创建用户BioEnroll请求的同时将用户的ID发送到生物服务器1220(S507)。根据本公开的一个实施例,服务器1210可以将服务器1210的生物识别能力信息发送到生物服务器1220,或者在不发送生物识别能力信息的情况下自主地管理生物识别能力信息。

[0073] 生物服务器1220可以将用户BioEnroll请求发送到服务器1210(S508)。服务器1210可以向I/O接口1120发送用户BioEnroll请求(S509)。在这种情况下,由服务器1210发送的用户BioEnroll请求可以包括在操作S505中获取的服务器的生物识别能力信息。I/O接口1120可以向生物识别信息客户端1110发送用户BioEnroll请求(S510)。

[0074] 生物识别信息客户端1110请求用户10选择生物识别技术并输入关于选择的生物识别技术的生物识别信息(S511)。详细地,当基于服务器的生物识别能力信息可支持多个生物识别技术时,生物识别信息客户端1110可以允许用户选择他或她所期望的生物识别技术(S512)并基于选择的生物识别技术获取生物识别信息(S513)。

[0075] 生物识别信息客户端1110可以基于获取的生物识别信息生成PI和相对应的AD(S514)。生物识别信息客户端1110可以基于在操作S512中由用户10选择的生物识别技术选择用于生成PI和AD的算法。

[0076] 生物识别信息客户端1110向I/O接口1120发送用户BioEnroll响应(S515)。用户BioEnroll响应可以包括在操作S514中生成的PI和AD。

[0077] 包括PI和AD的用户BioEnroll响应通过服务器1210被发送到生物服务器1220(S516和S517)。

[0078] 生物服务器1220可以存储接收的PI和AD(S518)。生物服务器1220可以存储与用户的ID相关联的接收的PI和AD。换句话说,根据参考图5描述的本公开的实施例,生物识别信息认证系统可以通过使用用户的个人终端而不是专用终端来在生物服务器1220中创建用于生物识别信息认证的数据库。

[0079] 图6示出了根据本公开的实施例的生物识别信息认证方法的流程图。参考图6,终端可以将获得的PI*发送到服务器。

[0080] 终端可以向服务器发送终端的生物识别能力信息,同时请求服务器通过使用与用户的生物识别信息相关的信息来认证用户(S610)。

[0081] 终端可以从服务器接收服务器的生物识别能力信息和AD(S620)。服务器的生物识别能力信息可以是与终端支持的生物识别技术相关的信息。可以基于从终端发送到服务器的生物识别能力信息,从与服务器存储的用户信息相关的生物识别技术中选择生物识别技术。可以根据生物识别信息注册过程注册AD,并且基于选择的生物识别技术获取AD。根据本

公开的一个实施例,服务器可以选择适合于认证的生物识别技术和与其对应的用户的AD,并将选择的生物识别技术和用户的AD提供给终端。

[0082] 终端可以基于服务器的生物识别能力信息获取用户的生物识别信息(S630)。终端可以经由生物识别信息输入器从用户获取生物识别信息。根据本公开的一个实施例,终端可以请求用户基于服务器的生物识别能力信息,从多条支持的生物识别信息中选择要用于认证的生物识别信息,并经由生物识别信息输入器获取选择的生物识别信息。

[0083] 终端基于获取的生物识别信息和由服务器发送的AD获得PI*(S640)。根据本公开的一个实施例,终端可以经由生物识别信息客户端获得PI*。

[0084] 终端将获得的PI*发送到服务器(S650)。然后,服务器可以将从终端接收的PI*与注册期间存储的PI进行比较,以将认证结果返回给终端。

[0085] 图7示出了根据本公开的实施例的用于说明生物识别信息认证方法的流程图。详细地,图7是用于说明参考图6描述的、根据本公开的实施例的生物信息认证方法中包括终端和服务器的生物信息认证系统的操作的流程图。

[0086] 用户10可以从终端的I/O接口1120请求服务连接(S701)。用户对服务连接的请求可以通过执行应用程序或web浏览器来作出。

[0087] I/O接口1120可以请求来自服务器1210的连接(S702)。可以使用HTTP协议作出连接请求。TLS信道可以被创建为I/O接口1120和服务器1210之间的安全通信信道(S703)。

[0088] I/O接口1120可以向服务器1210发送生物识别能力信息和需要传输用户BioAuth请求的认证请求(S704)。该认证请求可以包括用于标识请求认证的用户10的ID。

[0089] 服务器1210确定其生物识别能力(S705)。详细地,服务器1210可以基于从终端发送到服务器1210的生物识别能力信息来从服务器1210支持的并且对应于用户10的注册的信息的多个生物识别技术中选择与终端支持的生物识别技术相关的信息。服务器1210可以基于选择的信息获取服务器1210的生物识别能力信息。根据本公开的一个实施例,服务器1210可以获取适合于认证的生物识别技术。替代地,根据本公开的另一实施例,服务器1210可以将基于多个生物识别技术的生物识别能力信息发送到生物服务器1220(S707),并从生物服务器1220接收用于选择适合于关于用户10的注册的信息的生物识别技术的信息以及与选择的生物识别技术相对应的AD。

[0090] 当终端不支持服务器1210支持并且对应于用户10的注册的信息的生物识别技术时,服务器1210向I/O接口1120发送失败(FAIL)信号并终止认证过程(S706)。

[0091] 服务器1210可以向生物服务器1220发送用户ID,同时请求生物服务器1220创建用户BioAuth请求(S707)。根据本公开的一个实施例,如参考操作S705所述的,服务器1210可以向生物服务器1220发送生物识别能力信息,或者在不发送生物识别能力信息的情况下自主地管理生物识别能力信息。

[0092] 生物服务器1220可以向服务器1210发送用户BioAuth请求(S708)。用户BioAuth请求可以包括与基于服务器1210的生物识别能力信息选择的生物识别技术相对应的至少一个AD。

[0093] 服务器1210可以向I/O接口1120发送用户BioAuth请求(S709)。在这种情况下,由服务器1210发送的用户BioAuth请求可以包括在操作S705中获取的服务器的生物识别能力信息。I/O接口1120可以向生物识别信息客户端1110发送用户BioAuth请求(S710)。

[0094] 生物识别信息客户端1110请求用户10选择生物识别技术并输入关于选择的生物识别技术的生物识别信息(S711)。详细地,当基于服务器1210的生物识别能力信息可支持多个生物识别技术时,生物识别信息客户端1110可以允许用户10选择他或她所期望的生物识别技术(S712)并基于选择的生物识别技术获取生物识别信息(S713)。

[0095] 生物识别信息客户端1110可以基于获取的生物识别信息和从服务器1210接收的AD来生成PI*(S714)。生物识别信息客户端1110可以基于在操作S712中由用户10选择的生物识别技术来选择用于生成PI*的算法。

[0096] 生物识别信息客户端1110向I/O接口1120发送用户BioAuth响应(S715)。用户BioAuth响应可以包括在操作S714中生成的PI*。

[0097] 包括PI*的用户BioAuth响应通过服务器1210被发送到生物服务器1220(S716和S717)。

[0098] 生物服务器1220可以将接收的PI*与注册的PI进行比较,以确定用户认证的结果(S718)。生物服务器1220可以通过服务器1210向终端发送关于认证结果的信息(S719和S720)。

[0099] 图8示出了根据本公开的实施例的生物识别信息注册方法的流程图。

[0100] 参考图8,终端可以通过使用公钥和证书认证来将获取的PI和AD安全地发送到服务器。

[0101] 终端可以向服务器发送终端的生物识别能力信息,同时请求服务器注册与用户的生物识别信息相关的信息(S810)。

[0102] 终端可以接收服务器的生物识别能力信息、服务器的公钥证书和质询信息(challenge information)(S820)。服务器的生物识别能力信息可以是与终端支持的生物识别技术相关的信息。可以基于从终端发送到服务器的生物识别能力信息,从服务器支持的多个生物识别技术中选择生物识别技术。服务器的公钥证书可以是由认证机构(CA)颁发的用于服务器的私钥的证书。质询信息可以是由服务器生成和存储的信息,以验证由终端发送的信息的可靠性和完整性。

[0103] 终端可以基于服务器的生物识别能力信息获取用户的生物识别信息(S830)。终端可以经由生物识别信息输入器从用户获取生物识别信息。根据本公开的一个实施例,终端可以请求用户基于服务器的生物识别能力信息,从多条支持的生物识别信息中选择要用于认证的生物识别信息,并经由生物识别信息输入器获取选择的生物识别信息。

[0104] 终端基于获取的用户的生物识别信息获得PI和相对应的AD(S840)。可以基于终端用于获得它们的算法来以各种方式确定PI和AD。根据本公开的实施例,终端可以经由生物识别信息客户端获得PI和AD。

[0105] 终端可以通过使用基于服务器的公钥证书获得的公钥来加密获得的PI和AD以及从服务器接收的质询信息(S850)。详细地,终端可以通过使用CA颁发的证书从接收自服务器的服务器的公钥证书中获取服务器的公钥。终端可以基于获得的服务器公钥对PI和AD以及从服务器接收的质询信息进行加密。

[0106] 终端向服务器发送加密的PI、AD和质询信息(S860)。服务器可以用其私钥来解密从终端接收的加密PI、AD和质询信息。服务器可以通过使用质询信息来验证接收的信息的可靠性和完整性,并且当验证成功时,存储PI和AD以完成生物识别信息注册过程。

[0107] 图9示出了根据本公开的实施例的用于说明生物识别信息注册方法的流程图。详细地,图9是用于说明参考图8描述的、根据本公开的实施例的生物信息注册方法中包括终端和服务器的生物信息认证系统的操作的流程图。

[0108] 用户10可以从终端的I/O接口1120请求服务连接(S901)。用户对服务连接的请求可以通过执行应用程序或web浏览器来作出。

[0109] I/O接口1120可以请求来自服务器1210的连接(S902)。可以使用HTTP协议作出连接请求。TLS信道可以被创建为I/O接口1120和服务器1210之间的安全通信信道(S903)。

[0110] I/O接口1120可以向服务器1210发送生物识别能力信息和需要传输用户BioEnroll请求的注册请求(S904)。认证请求可以包括用于标识请求认证的用户10的ID。

[0111] 服务器1210确定其生物识别能力(S905)。详细地,服务器1210可以基于从终端发送到服务器1210的生物识别能力信息来从服务器1210支持的并且对应于用户10的注册的信息的多条生物识别技术中选择与终端支持的生物识别技术相关的信息。服务器1210可以基于选择的信息获取服务器1210的生物识别能力信息。

[0112] 当服务器1210支持的生物识别技术不包括终端支持的生物识别技术时,服务器1210向I/O接口1120发送FAIL信号并终止认证过程(S906)。

[0113] 服务器1210可以在请求生物服务器1220创建用户BioEnroll请求的同时向生物服务器1220发送用户ID(S907)。根据本公开的一个实施例,服务器1210可以向生物服务器1220发送生物识别能力信息,或者在不发送生物识别能力信息的情况下自主地管理生物识别能力信息。

[0114] 生物服务器1220可以生成质询信息CH(S908)。该质询信息CH可以是由服务器1210生成的用于验证由终端发送的信息的可靠性和完整性的信息。

[0115] 此外,生物服务器1220可以生成其公钥对,该公钥对包括用于数据发送和接收的私钥S_SK和公钥S_PK。生物服务器1220可以将公钥S_PK发送到CA 1230(S909)。CA 1230可以向生物服务器1220提供公钥证书,该公钥证书包括用CA 1230的私钥加密的生物服务器1220的公钥S_PK(S910)。生物服务器1220向服务器1210发送用户BioEnroll请求(S911)。在这种情况下,用户BioEnroll请求可以包括通过使用生物服务器1220的私钥SK和由CA 1230颁发的公钥证书对在操作S908中生成的质询信息CH和生物识别能力信息进行加密而获得的信息。服务器1210向I/O接口1120发送用户BioEnroll请求(S912)。

[0116] I/O接口1120向生物识别信息客户端1110发送用户BioEnroll请求(S913)。

[0117] 生物识别信息客户端1110可以验证包含在用户BioEnroll请求中获取的生物服务器1220的公钥证书(S914)。详细地,生物识别信息客户端1110可以持有包括CA的公钥并由CA 1230颁发的证书。生物识别信息客户端1110可以通过使用CA的证书从生物服务器1220的公钥证书验证和获取生物服务器1220的公钥S_PK。生物识别信息客户端1110可以通过使用生物服务器1220的公钥S_PK来解密被加密的质询信息CH和生物识别能力信息。

[0118] 生物识别信息客户端1110请求用户10选择生物识别技术并输入关于选择的生物识别技术的生物识别信息(S915)。详细地,当基于服务器的生物识别能力信息可支持多个生物识别技术时,生物识别信息客户端1110可以允许用户10选择他或她所期望的生物识别技术(S916)并基于选择的生物识别技术获取生物识别信息(S917)。

[0119] 生物识别信息客户端1110可以基于获取的生物识别信息来获得PI和相对应的AD

(S918)。生物识别信息客户端1110可以基于在操作S916中由用户10选择的生物识别技术来选择用于生成PI和AD的算法。

[0120] 生物识别信息客户端1110可以通过使用基于公钥证书获取的生物服务器1220的公钥S_PK来加密获得的PI和AD以及从服务器1210发送的质询信息CH(S919)。

[0121] 生物识别信息客户端1110向I/O接口1120发送用户BioEnroll响应(S920)。用户BioEnroll响应可以包括在操作S919中加密的PI、AD和质询信息CH。

[0122] 包括加密PI、AD和质询信息CH的用户BioEnroll响应通过服务器1210被发送到生物服务器1220(S921和S922)。

[0123] 生物服务器1220用其私钥S_SK解密被加密的PI、AD和质询信息CH(S923)。

[0124] 生物服务器1220通过使用在操作S923中获取的质询信息CH来验证接收的信息的可靠性和完整性(S924)。根据本公开的一个实施例,生物服务器1220可以通过将在操作S923中获取的质询信息CH与存储的质询信息进行比较来验证接收的信息的完整性。根据本公开的一个实施例,由生物服务器1220存储的质询信息可以在预定时间段内变化。生物服务器1220可以将在操作S923中获取的质询信息CH与存储的质询信息进行比较,并且当它们彼此不匹配时,确定用户登记响应已经过期。

[0125] 当在操作S924中验证成功时,生物服务器1220可以存储接收的PI和AD(S925)。生物服务器1220可以存储与用户ID关联的接收的PI和AD。根据参考图9描述的本公开的一个实施例,生物识别信息认证系统可以通过使用用户的个人终端而不是专用终端来创建用于生物服务器1220中的生物识别信息认证的数据库,同时确保终端和服务器1210之间的信息安全。

[0126] 图10示出了根据本公开的实施例的生物识别信息认证方法的流程图。

[0127] 参考图10,终端可以通过使用公钥和证书认证来安全地接收AD并向服务器发送PI*。

[0128] 终端可以向服务器发送终端的生物识别能力信息,同时从服务器请求与用户的生物识别信息相关的信息的注册(S1010)。

[0129] 终端可以从服务器接收服务器的生物识别能力信息、服务器的公钥证书、AD和质询信息(S1020)。服务器的生物识别能力信息可以是与终端支持的生物识别技术相关的信息。可以基于从终端发送到服务器的生物识别能力信息,从与服务器存储的关于用户的信息相关的多条生物识别技术中选择生物识别技术。可以根据生物识别信息注册过程来注册AD,并且基于选择的生物识别技术获取AD。根据本公开的一个实施例,服务器可以选择适合于认证的生物识别技术和与其对应的用户的AD,并将选择的生物识别技术和用户的AD提供给终端。服务器的公钥证书可以是由CA颁发的用于服务器的私钥的证书。质询信息可以是由服务器生成和存储的信息,以验证终端发送的信息的可靠性和完整性。

[0130] 终端可以基于服务器的生物识别能力信息获取用户的生物识别信息(S1030)。终端可以经由生物识别信息输入器从用户获取生物识别信息。根据本公开的一个实施例,终端可以请求用户基于服务器的生物识别能力信息,从多条支持的生物识别信息中选择要用于认证的生物识别信息,并经由生物识别信息输入器获取选择的生物识别信息。

[0131] 终端基于获取的用户的生物识别信息和从服务器接收的AD(S1040)来获得PI*。根据本公开的一个实施例,终端可以经由生物识别信息客户端获得PI*。

[0132] 终端可以通过使用基于服务器的公钥证书获得的公钥来加密获得的PI*和从服务器接收的质询信息(S1050)。详细地,终端可以通过使用CA颁发的证书从接收自服务器的服务器公钥证书中获取服务器的公钥。终端可以使用获取的服务器公钥对从服务器接收的PI*和质询信息进行加密。

[0133] 终端向服务器发送加密的PI*和质询信息(S1060)。服务器可以用其私钥解密从终端接收的加密的PI*和质询信息。服务器可以通过使用质询信息来验证接收的信息的可靠性和完整性,并且当验证成功时,将接收的PI*与注册期间存储的PI进行比较,以将认证结果返回给终端。

[0134] 图11示出了根据本公开的实施例的生物识别信息认证方法的流程图。详细地,图11是用于说明参考图10描述的、根据本公开的实施例的生物信息认证方法中包括终端和服务器的生物信息认证系统的操作的流程图。

[0135] 用户10可以从终端的I/O接口1120请求服务连接(S1101)。用户对服务连接的请求可以通过执行应用程序或web浏览器来作出。

[0136] I/O接口1120可以请求来自服务器1210的连接(S1102)。可以使用HTTP协议作出连接请求。TLS信道可以被创建为I/O接口1120和服务器1210之间的安全通信信道(S1103)。

[0137] I/O接口1120可以向服务器1210发送生物识别能力信息和需要发送用户BioAuth请求的认证请求(S1104)。认证请求可以包括用于标识请求认证的用户10的ID。

[0138] 服务器1210确定其生物识别能力(S1105)。详细地,服务器1210可以基于从终端发送到服务器1210的生物识别能力信息来从服务器1210支持的并且对应于用户10的注册信息的多条生物识别技术中选择与终端支持的生物识别技术相关的信息。服务器1210可以基于选择的信息获取服务器1210的生物识别能力信息。根据本公开的一个实施例,服务器1210可以获取适合于认证的生物识别技术。替代地,根据本公开的另一实施例,在操作S1107中,服务器1210可以向生物服务器1220发送基于多个生物识别技术的生物识别能力信息,并从生物服务器1220接收用于选择适合于用户10的注册信息的生物识别技术的信息以及与选择的生物识别技术相对应的AD。

[0139] 当服务器1210支持并且对应于用户10的注册的信息的生物识别技术不包括终端支持的生物识别技术时,服务器1210向I/O接口1120发送FAIL信号并终止认证过程(S1106)。

[0140] 服务器1210可以向生物服务器1220发送用户的ID,同时请求生物服务器1220创建用户BioAuth请求(S1107)。根据本公开的一个实施例,服务器1210可以向生物服务器1220发送生物识别能力信息,或者在不发送生物识别能力信息的情况下自主地管理生物识别能力信息。

[0141] 生物服务器1220可以生成质询信息CH(S1108)。质询信息CH可以是由服务器1210生成的用于验证由终端发送的信息的可靠性和完整性的信息。

[0142] 此外,生物服务器1220可以生成其公钥对,该公钥对包括用于数据发送和接收的私钥S_SK和公钥S_PK。生物服务器1220可将公钥S_PK发送到CA 1230(S1109)。CA 1230可以向生物服务器1220提供公钥证书,该公钥证书包括用CA 1230的私钥加密的生物服务器1220的公钥S_PK(S1110)。生物服务器1220向服务器1210发送用户BioAuth请求(S1111)。在这种情况下,用户BioAuth请求可以包括通过使用生物服务器1220的私钥S_PK加密在操作

S1108中生成的质询信息CH、服务器的生物识别能力信息、以及与基于生物识别能力信息选择的生物识别技术相对应的至少一个AD而获得的信息,以及由CA 1230颁发的公钥证书。服务器1210向I/O接口1120发送用户BioAuth请求(S1112)。

[0143] I/O接口1120向生物识别信息客户端1110发送用户BioAuth请求(S1113)。

[0144] 生物识别信息客户端1110可以验证包含在用户BioAuth请求中的生物服务器1220的公钥证书(S1114)。详细地,生物识别信息客户端1110可以持有包括CA的公钥并由CA 1230颁发的证书。生物识别信息客户端1110可以通过使用CA的证书从生物服务器1220的公钥证书验证和获取生物服务器1220的公钥S_PK。生物识别信息客户端1110可以通过使用生物服务器1220的公钥S_PK来解密被加密的质询信息CH和生物识别能力信息。

[0145] 生物识别信息客户端1110请求用户10选择生物识别技术并输入关于选择的生物识别技术的生物识别信息(S1115)。详细地,当基于服务器的生物识别能力信息可支持多个生物识别技术时,生物识别信息客户端1110可以允许用户10选择他或她所期望的生物识别技术(S1116)并基于选择的生物识别技术获取生物识别信息(S1117)。

[0146] 生物识别信息客户端1110可以基于获取的生物识别信息和从服务器1210接收的AD来生成PI*和相应的AD(S1118)。生物识别信息客户端1110可以基于在操作S1116中由用户10选择的生物识别技术来选择用于生成PI*的算法。

[0147] 生物识别信息客户端1110可以通过使用基于公钥证书获取的生物服务器1220的公钥S_PK来加密获得的PI*和从服务器1210发送的质询信息CH(S1119)。

[0148] 生物识别信息客户端1110向I/O接口1120发送用户BioAuth响应(S1120)。用户BioAuth响应可以包括在操作S1119中加密的PI*和质询信息CH。

[0149] 包括加密的PI*和质询信息CH的用户BioAuth响应通过服务器1210被发送到生物服务器1220(S1121和S1122)。

[0150] 生物服务器1220用其私钥S_SK解密被加密的PI*和质询信息CH(S1123)。

[0151] 生物服务器1220通过使用在操作S1123中获取的质询信息CH来验证接收的信息的可靠性和完整性(S1124)。根据本公开的一个实施例,生物服务器1220可以通过将在操作S1123中获取的质询信息CH与存储的质询信息进行比较来验证接收的信息的完整性。根据本公开的一个实施例,由生物服务器1220存储的质询信息可以在预定时间段内变化。生物服务器1220可以将在操作S1123中获取的质询信息CH与存储的质询信息进行比较,并且当它们彼此不匹配时,确定用户BioAuth响应已经过期。

[0152] 当在操作S1124中验证成功时,生物服务器1220可以将接收的PI*与注册的PI进行比较以确定用户认证的结果。生物服务器1220可以通过服务器1210向终端发送关于认证结果的信息(S1126和S1127)。

[0153] 根据参考图11描述的本公开的实施例,生物识别信息认证系统可以执行基于生物识别信息的认证过程,同时确保终端和服务器1210之间的信息的安全。

[0154] 图12示出了根据本公开的实施例的用于说明注册和传送生物识别信息的方法的图。根据本公开的一个实施例,生物识别信息认证系统1000可以通过使用由快速在线身份认证(FIDO)联盟定义的FIDO通用认证框架(UAF)来对生物识别信息执行注册和认证。参考图12,用户可以通过使用第一终端1100,然后额外地或独占地使用第二终端1300作为新终端来基于FIDO访问生物识别信息认证系统1000,如下面参考图12更详细地描述的。

[0155] 用户可以通过使用ID和密码认证经由第一终端1100登录到服务。详细地,第一终端1100可以生成其由公钥和私钥组成的公钥对,以存储私钥,并将公钥发送到认证服务器1200。认证服务器1200可以通过将接收的公钥与用户的ID信息一起存储来完成注册过程。此后,当通过登录等对用户进行认证时,第一终端1100可以使用存储的私钥对从认证服务器1200接收的用户认证请求进行签名,并将签名的用户认证请求发送到认证服务器1200。认证服务器1200可以利用存储的公钥来验证签名的用户认证请求,并确定认证结果。

[0156] 在这种情况下,为了将认证模式改变为生物识别信息认证或添加该生物识别信息认证,用户可以发起生物识别信息注册过程,并且在生物识别信息注册过程完成之后,用户基于生物识别信息对自己进行认证。

[0157] 根据本公开的一个实施例,第一终端1100可以通过使用公钥认证仅向认证服务器1200发送认证结果,而不向其发送与生物识别信息相关联的模板。详细地,用户可以经由第一终端1100的生物识别信息输入器将生物识别信息输入到第一终端1100。第一终端1100可以基于生物识别信息获得模板并存储获得的模板。

[0158] 当用户使用ID信息和密码对用户进行认证时,第一终端1100可以生成用于生物识别信息认证的新公钥对以存储私钥,并将公钥发送到认证服务器1200。认证服务器1200可以将接收的公钥与用户的ID信息一起存储以完成注册过程。

[0159] 另外,已经完成用于生物识别信息认证的注册过程的用户可以基于生物识别信息请求认证以访问服务。当用户请求认证时,第一终端1100可以从认证服务器1200请求认证,并且认证服务器1200可以响应于这样的请求向第一终端1100发送用户认证请求。

[0160] 第一终端1100可以响应于来自认证服务器1200的用户认证请求从用户接收生物识别信息,并且通过将基于接收的生物识别信息获得的模板与存储的模板进行比较来认证用户。当用户被认证时,第一终端1100可以使用存储的私钥对从认证服务器1200接收的用户认证请求进行签名,并将签名的用户认证请求发送到认证服务器1200。认证服务器1200可以利用存储的公钥来验证签名的用户认证请求,并确定认证结果。

[0161] 根据本公开的另一实施例,在注册期间,第一终端1100可以将与生物识别信息相关联的模板的至少一部分发送到认证服务器1200。

[0162] 详细地,用户可以经由第一终端1100的生物识别信息输入器将生物识别信息输入到第一终端1100。第一终端1100可以基于生物识别信息获得模板并存储获得的模板。

[0163] 当使用ID信息和密码对用户进行认证时,第一终端1100可以创建用于生物识别信息认证的新公钥对以存储私钥,并将公钥与作为所存储模板的一部分的关于生物识别的信息一起发送到认证服务器1200。认证服务器1200可以通过将接收的公钥和关于生物识别的信息与用户的ID信息一起存储来完成注册过程。

[0164] 另外,已经完成用于生物识别信息认证的注册过程的用户可以基于生物识别信息请求认证以访问服务。当用户请求认证时,第一终端1100可以从认证服务器1200请求认证,并且认证服务器1200可以响应于这样的请求向第一终端1100发送用户认证请求。根据本公开的一个实施例,认证服务器1200可以在用于传输的用户认证请求中包括存储的关于生物识别的信息。

[0165] 第一终端1100可以响应于来自认证服务器1200的用户认证请求从用户接收生物识别信息,并且通过将基于接收的生物识别信息获得的模板与存储的模板进行比较来认证

用户。根据本公开的一个实施例,第一终端1100可以基于存储的模板和生物识别信息,或者基于从认证服务器1200接收的关于生物识别的信息和生物识别信息来获得新模板。当用户被认证时,第一终端1100可以通过使用存储的私钥对从认证服务器1200接收的用户认证请求进行签名,并将签名的用户认证请求发送到认证服务器1200。认证服务器1200可以利用存储的公钥来验证签名的用户认证请求,并确定认证结果。

[0166] 另外,当用户希望经由作为新终端的第二终端1300使用生物识别信息进行认证时,需要从认证服务器1200撤销第一终端1100的公钥,并向认证服务器1200注册第二终端1300的公钥。

[0167] 图13A示出了根据本公开的实施例的注册和传送生物识别信息的方法的流程图。

[0168] 在通过经由基于生物识别信息执行认证的第一终端使用ID信息和密码登录到服务之后,用户经由第一终端向认证服务器注册第一终端的公钥(S1311)。上面已经参考图12提供了对其的详细描述。

[0169] 用户经由第一终端从认证服务器撤销第一终端的公钥(S1321)。当从认证服务器移除公钥时,第一终端可以撤销其存储的私钥。

[0170] 在通过经由基于生物识别信息执行认证的第二终端使用ID信息和密码登录到服务之后,用户经由第二终端向认证服务器注册第二终端的公钥(S1331)。上面已经参考图12提供了对其的详细描述。

[0171] 图13B示出了根据本公开的实施例的注册和传送生物识别信息的方法的流程图。

[0172] 在通过经由执行基于生物识别信息的认证的第一终端使用ID信息和密码登录到服务之后,用户经由第一终端向认证服务器注册第一终端的公钥和基于生物识别信息生成的关于生物特征的信息(S1312)。根据本公开的一个实施例,关于生物识别的信息可以是基于生物识别信息生成的模板的一部分。例如,关于生物识别的信息可以是PI和相对应的AD。上面已经参考图12提供了其详细描述。

[0173] 用户经由第二终端将基于生物识别信息生成的关于生物识别的信息连同第二终端的公钥一起发送到认证服务器(S1322)。根据本公开的一个实施例,由用户发送的关于生物识别的信息可以是PI*。

[0174] 在操作S1332中,认证服务器可以基于注册的关于生物识别的信息来认证用户。认证完成后,认证服务器可以撤销第一终端的公钥,并向认证服务器本身注册第二终端的公钥。参考图13B,生物识别信息认证系统可以提供多个终端之间的服务传送,而无需录入用户的ID信息和密码。

[0175] 图14示出了根据本公开的实施例的用于说明生物识别信息注册方法的流程图。

[0176] 用户10可以从终端的I/O接口1120请求服务连接(S1401)。用户对服务连接的请求可以通过执行应用程序或web浏览器来作出。

[0177] I/O接口1120可以请求来自服务器1210的连接(S1402)。可以使用HTTP协议作出连接请求。TLS信道可以被创建为I/O接口1120和服务器1210之间的安全通信信道(S1403)。

[0178] 用户10可以通过使用传统认证方法(例如,通过输入诸如用户ID和密码的ID信息)来请求认证(S1404)。

[0179] 然后,将用户10输入的信息发送到服务器1210(S1405)。

[0180] 服务器1210基于由用户10输入的ID信息来认证用户10(S1406)。例如,服务器1210

可以通过验证由用户10输入的ID和密码来认证用户。

[0181] 服务器1210基于FIDO协议向生物服务器1220发送请求传输UAF注册请求的注册请求。

[0182] 生物服务器1220基于生物识别信息创建供终端用于认证的策略(S1408)。根据本公开的一个实施例,该策略可以包括将要使用的关于生物识别技术的信息,诸如生物识别信息的项目(例如,每个用户的脸型、虹膜、视网膜、静脉、指纹、DNA等)和关于被执行以基于该生物识别信息来获得模板的算法的信息。

[0183] 生物服务器1220基于FIDO协议向服务器1210发送UAF注册请求(S1409)。UAF注册请求可以包括在操作S1408中创建的策略。

[0184] 服务器1210向I/O接口1120发送UAF注册请求(S1410)。I/O接口1120向生物识别信息客户端1110发送UAF注册请求(S1411)。

[0185] 生物识别信息客户端1110基于UAF注册请求中包含的策略选择要用于认证的生物识别技术(S1412)。详细地,当基于该策略可支持多个生物识别技术时,生物识别信息客户端1110可以请求用户10选择并输入他或她所期望得生物识别技术(S1413)。当生物识别信息客户端1110自身选择或单个生物识别技术可支持时,生物识别信息客户端1110可以请求用户10输入与在操作S1413中选择的生物识别技术相对应的生物识别信息。

[0186] 用户10向生物识别信息客户端1110提供基于选择的生物识别技术获取的生物识别信息(S1414)。

[0187] 生物识别信息客户端1110生成由私钥和公钥组成的公钥对(S1415)。此外,根据本公开的一个实施例,生物识别信息客户端1110基于根据选择的生物识别技术获取的生物识别信息获得模板。根据本公开的实施例,生物识别信息客户端1110可以基于获取的生物识别信息生成PI和相对应的AD。生物识别信息客户端1110可以基于选择的生物识别技术选择用于生成PI和AD的算法。

[0188] 生物识别信息客户端1110将生成的私钥存储在安全储存器1140中(S1416)。

[0189] 生物识别信息客户端1110向I/O接口1120发送UAF注册响应(S1417)。UAF注册响应可以包括在操作S1415中生成的PI、AD和公钥。

[0190] 包括PI、AD和公钥的UAF注册响应通过服务器1210被发送到生物服务器1220(S1418和S1419)。

[0191] 生物服务器1220可以存储接收的PI和AD(S1420)。生物服务器1220可以存储与用户ID相关联的、接收的PI和AD。

[0192] 图15示出了根据本公开的实施例的用于说明传送生物识别信息的方法的流程图。

[0193] 用户10可以从终端的I/O接口1120请求服务连接(S1501)。用户对服务连接的请求可以通过执行应用程序或web浏览器来作出。

[0194] I/O接口1120可以请求来自服务器1210的连接(S1502)。可以使用HTTP协议作出连接请求。TLS信道可以被创建为I/O接口1120和服务器1210之间的安全通信信道(S1503)。

[0195] 用户10可以经由I/O接口1120输入需要将使用的终端传送到当前终端的设备传送请求(传送设备)(S1504)。设备传送请求可以包括用户10的ID信息。

[0196] 由用户10输入的设备传送请求被发送到服务器1210(S1505)。

[0197] 服务器1210向生物服务器1220发送请求传输传送请求的请求(S1506)。

[0198] 生物服务器1220基于生物识别信息生成质询信息和策略,以供终端用于认证(S1507)。质询信息可以是由服务器1210生成和存储的信息,以验证由终端发送的信息的可靠性和完整性。

[0199] 根据本公开的一个实施例,该策略可以包括将要使用的关于生物识别技术的信息,诸如生物识别信息的项目(例如,每个用户的脸型、虹膜、视网膜、静脉、指纹、DNA等)和关于被执行以基于该生物识别信息来获得模板的算法的信息。另外,由于先前在注册期间生成的策略已经向生物服务器1220注册,因此生物服务器1220可以完整地使用注册的策略。

[0200] 生物服务器1220可以在与用户的生物识别信息相关的信息中提取与策略选择的生物识别技术相对应的AD,该AD在注册期间被存储(S1508)。

[0201] 生物服务器1220基于FIDO协议向服务器1210发送传送请求(S1509)。传送请求可以包括在操作S1507中生成的策略和质询信息以及在操作S1508中提取的AD。

[0202] 服务器1210向I/O接口1120发送传送请求(S1510)。I/O接口1120向生物识别信息客户端1110发送传送请求(S1511)。

[0203] 生物识别信息客户端1110基于传送请求中包含的策略选择要用于认证的生物识别技术(S1512)。详细地,当基于该策略可支持多个生物识别技术时,生物识别信息客户端1110可以请求用户10选择并输入他或她所期望得生物识别技术(S1513)。当生物识别信息客户端1110自身选择生物识别技术或单个生物识别技术可被支持时,生物识别信息客户端1110可以请求用户10输入与在操作S1513中选择的生物识别技术相对应的生物识别信息。

[0204] 用户10向生物识别信息客户端1110提供基于选择的生物识别技术获取的生物识别信息(S1514)。

[0205] 生物识别信息客户端1110生成由私钥和公钥组成的公钥对(S1515)。

[0206] 生物识别信息客户端1110基于根据选择的生物识别技术获得的生物识别信息和从服务器1210发送的AD获得PI*(S1516)。

[0207] 生物识别信息客户端1110将生成的私钥存储在安全储存器1140中(S1517)。

[0208] 生物识别信息客户端1110向I/O接口1120发送传送响应(S1518)。传送响应可以包括PI*、公钥和质询信息。

[0209] 包括PI*、公钥和质询信息的传送响应通过服务器1210被发送到生物服务器1220(S1519和S1520)。

[0210] 生物服务器1220通过使用质询信息来验证接收的信息的可靠性和完整性(S1521)。根据本公开的一个实施例,生物服务器1220可以通过将终端发送的质询信息与存储的质询信息进行比较来验证接收的信息的完整性。根据本公开的一个实施例,由生物服务器1220存储的质询信息可以在预定时间段内变化。生物服务器1220可以将接收的质询信息与存储的质询信息进行比较,并且当它们彼此不匹配时,确定传送响应已经过期。

[0211] 当在操作S1521中验证成功时,生物服务器1220可以将接收的PI*与注册的PI进行比较以确定是否许可传送(S1522)。当许可传送时,生物服务器1220可以存储公钥(S1523)。

[0212] 生物服务器1220可以将关于传送结果的信息从生物服务器1220传送到服务器1210(S1524)。

[0213] 图16示出了根据本公开的实施例的用于说明撤销生物识别信息的方法的流程图。

[0214] 用户10可以从终端的I/O接口1120请求服务连接(S1601)。用户对服务连接的请求可以通过执行应用程序或web浏览器来作出。

[0215] I/O接口1120可以请求来自服务器1210的连接(S1602)。可以使用HTTP协议作出连接请求。TLS信道可以被创建为I/O接口1120和服务器1210之间的安全通信信道(S1603)。

[0216] 在接收到关于指示传送已经成功执行并且因此新公钥已经注册的传送结果的信息之后,I/O接口1120可以从生物识别信息客户端1110请求用户认证,以便从用户10请求认证(S1604)。生物识别信息客户端1110可以请求用户10输入生物识别信息(S1605)。

[0217] 由用户10输入的生物识别信息被发送到生物识别信息客户端1110(S1606)。当基于用户的生物识别信息认证用户10时,生物识别信息客户端1110使用存储的私钥对质询信息进行签名(S1607)。

[0218] 生物识别信息客户端1110向I/O接口1120发送传送响应(S1608)。传送响应可以包括签名的质询信息。

[0219] 包括签名的质询信息的传送响应经由服务器1210被发送到生物服务器1220(S1609和S1610)。

[0220] 生物服务器1220通过使用存储在其中的公钥来验证用私钥签名的质询信息(S1611)。

[0221] 当验证完成时,生物服务器1220撤销存储的公钥(S1612)。生物服务器1220向服务器1210发送指示公钥的撤销的UAF注销请求(S1613)。UAF注销请求经由I/O接口1120被发送到生物识别信息客户端1110(S1614和S1615)。

[0222] 生物识别信息客户端1110删除存储在其中的私钥(S1616)。因此,注册的公钥和私钥两者都可以被撤销。

[0223] 生物识别信息客户端1110向I/O接口1120发送UAF注销响应(S1617)。然后经由服务器1210将UAF注销响应发送到生物服务器1220(S1618和S1619)。

[0224] 可以使用硬件组件、软件组件和/或其组合来实现上述终端1100。例如,可以使用一个或多个通用或专用计算机(诸如处理器、控制器、算术逻辑单元(ALU)、数字信号处理器、微型计算机、现场可编程阵列(FPA)、可编程逻辑单元、微处理器或任何其他能够响应和执行指令的设备)来实现本公开的实施例中示出的设备及其组件(PLU)。

[0225] 尽管已经用各种实施例描述了本发明,但是可以向本领域技术人员建议各种改变和修改。意图在于本发明包含落入所附权利要求范围内的这些改变和修改。

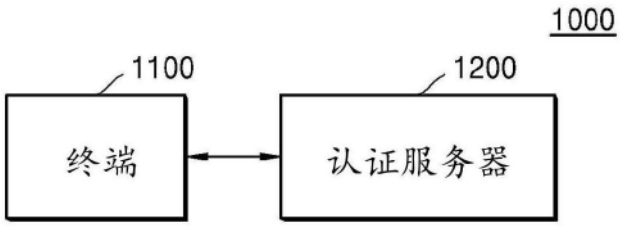

1000
1100
1200
终端
认证服务器

图1

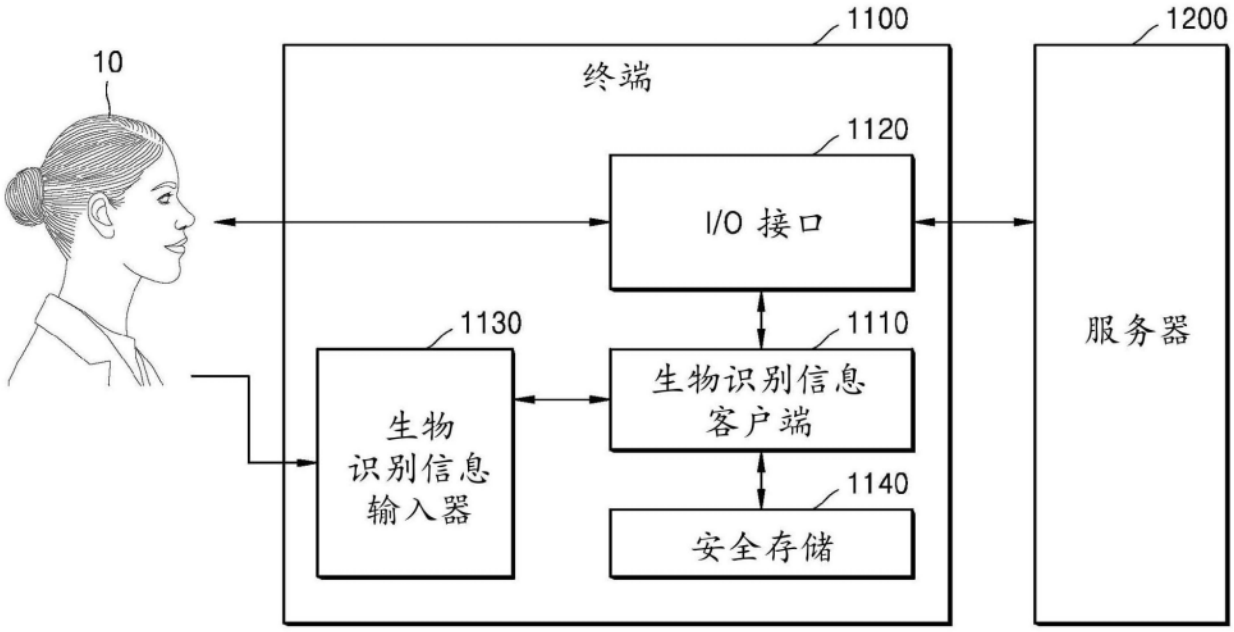

10
1100
终端
1200
1120
I/O 接口
1130
1110
生物识别信息客户端
生物识别信息输入器
1140
安全存储
服务器

图2

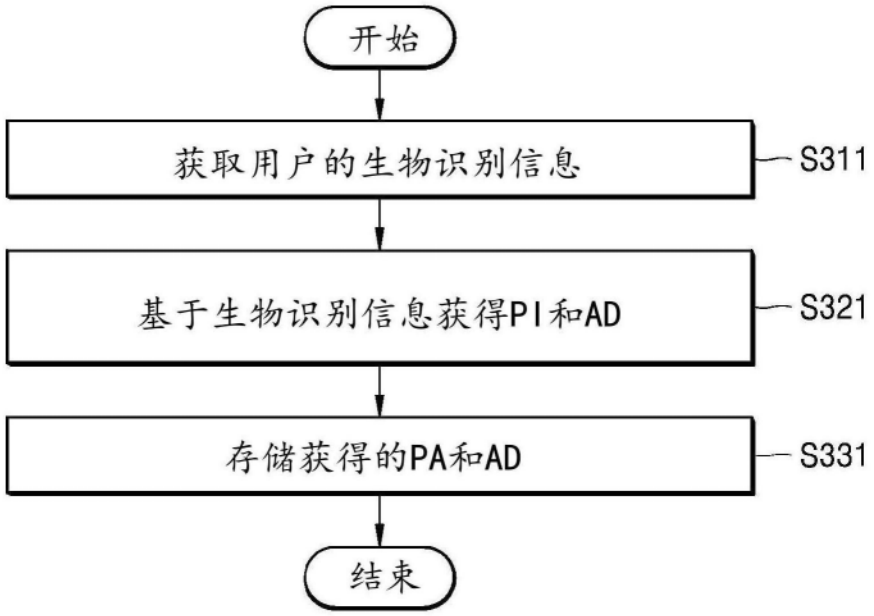

开始
获取用户的生物识别信息
S311
基于生物识别信息获得PI和AD
S321
存储获得的PA和AD
S331
结束

图3A

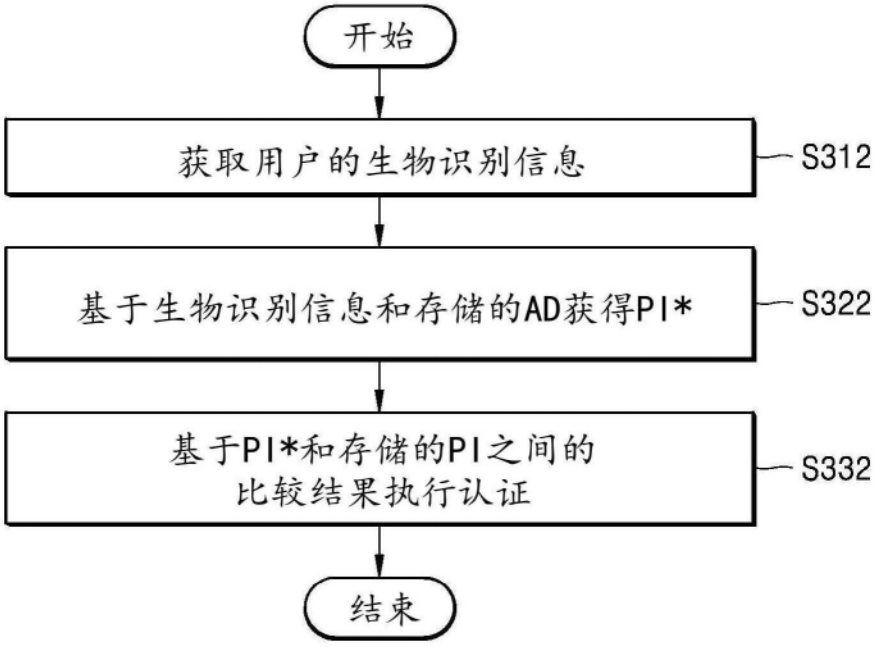

开始
获取用户的生物识别信息
S312
基于生物识别信息和存储的AD获得PI*
S322
基于PI*和存储的PI之间的
比较结果执行认证
S332
结束

图3B

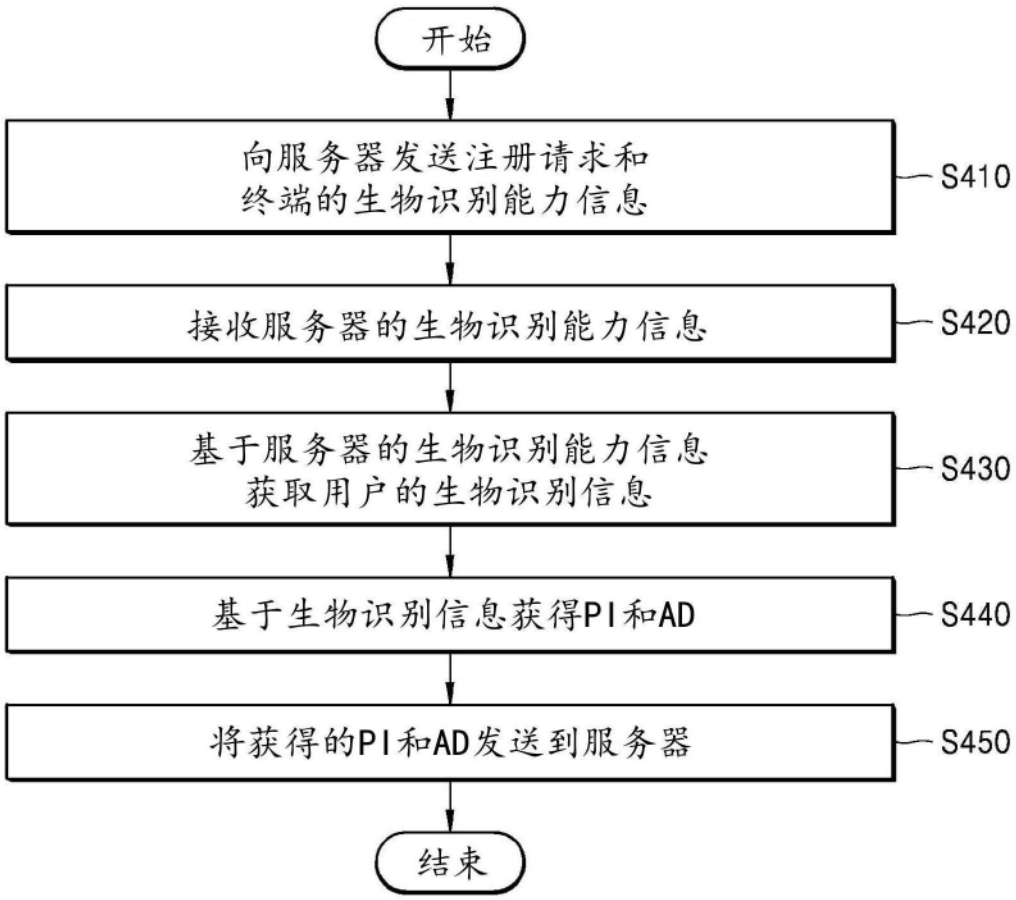

开始
向服务器发送注册请求和
终端的生物识别能力信息
S410
接收服务器的生物识别能力信息
S420
基于服务器的生物识别能力信息
获取用户的生物识别信息
S430
基于生物识别信息获得PI和AD
S440
将获得的PI和AD发送到服务器
S450
结束

图4

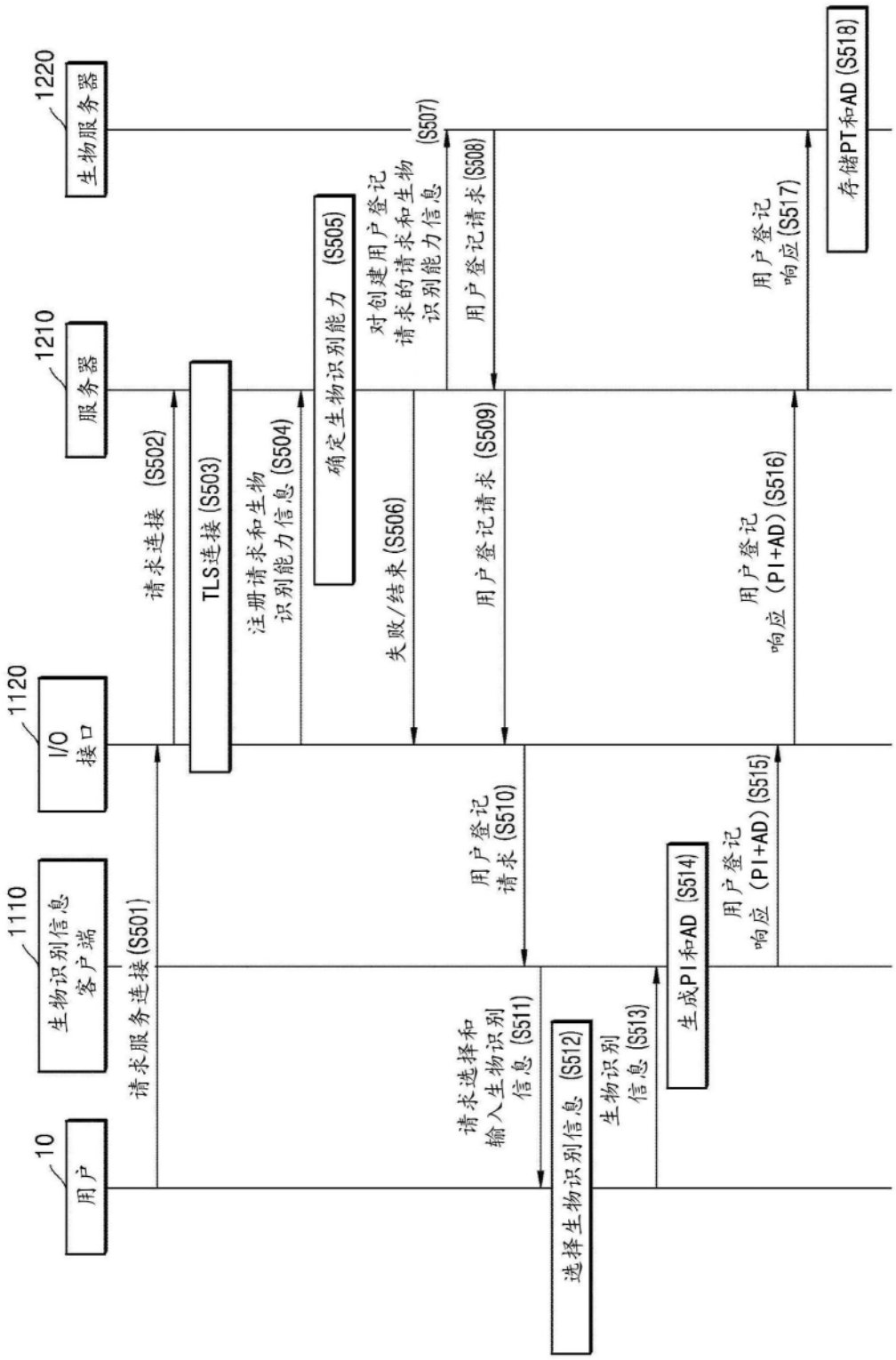

10
用户
1110
生物识别信息客户端
1120
I/O接口
1210
服务器
1220
生物服务器
请求服务连接 (S501)
请求连接 (S502)
TLS连接 (S503)
注册请求和生物识别能力信息 (S504)
确定生物识别能力 (S505)
失败/结束 (S506)
对创建用户登记请求的请求和生物识别能力信息 (S507)
用户登记请求 (S508)
用户登记请求 (S509)
用户登记请求 (S510)
请求选择和输入生物识别信息 (S511)
选择生物识别信息 (S512)
生物识别信息 (S513)
生成PI和AD (S514)
用户登记响应 (PI+AD) (S515)
用户登记响应 (PI+AD) (S516)
用户登记响应 (S517)
存储PT和AD (S518)

图5

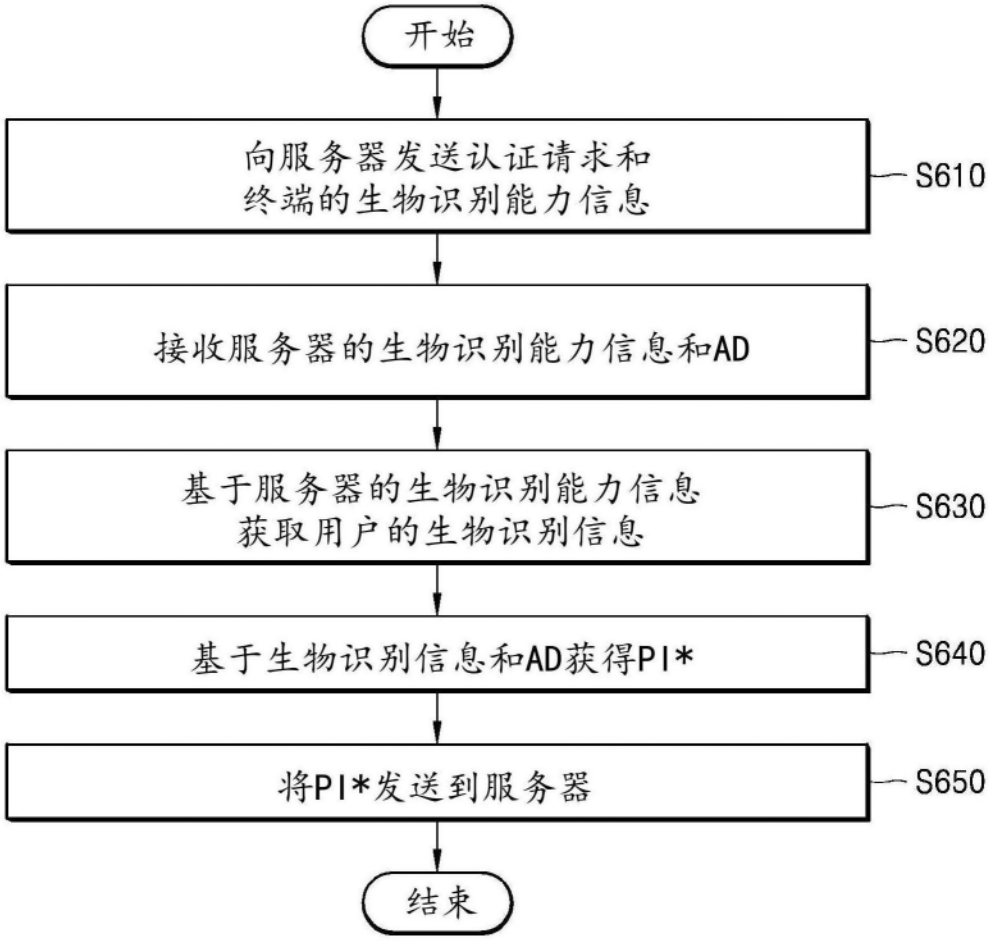

开始
向服务器发送认证请求和
终端的生物识别能力信息
S610
接收服务器的生物识别能力信息和AD
S620
基于服务器的生物识别能力信息
获取用户的生物识别信息
S630
基于生物识别信息和AD获得PI*
S640
将PI*发送到服务器
S650
结束

图6

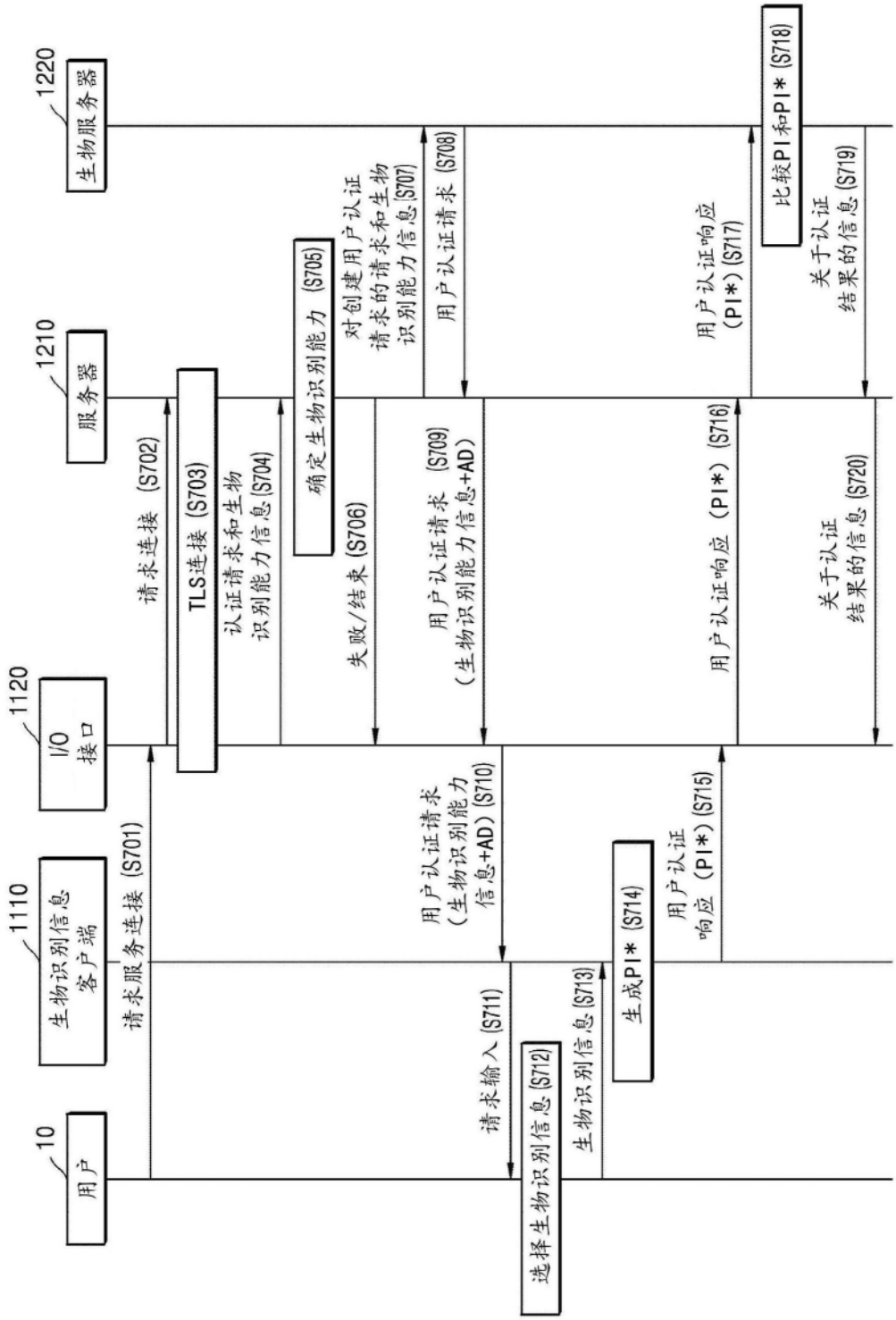

10
用户
1110
生物识别信息客户端
1120
I/O接口
1210
服务器
1220
生物服务器
请求服务连接 (S701)
请求连接 (S702)
TLS连接 (S703)
认证请求和生物识别能力信息 (S704)
确定生物识别能力 (S705)
失败/结束 (S706)
对创建用户认证请求的请求和生物识别能力信息 (S707)
用户认证请求 (S708)
用户认证请求 (S709)
(生物识别能力信息+AD)
用户认证请求 (生物识别能力信息+AD) (S710)
用户认证响应 (PI*) (S716)
用户认证响应 (PI*) (S717)
比较PI和PI* (S718)
关于认证结果的信息 (S719)
关于认证结果的信息 (S720)
请求输入 (S711)
选择生物识别信息 (S712)
生物识别信息 (S713)
生成PI* (S714)
用户认证响应 (PI*) (S715)

图7

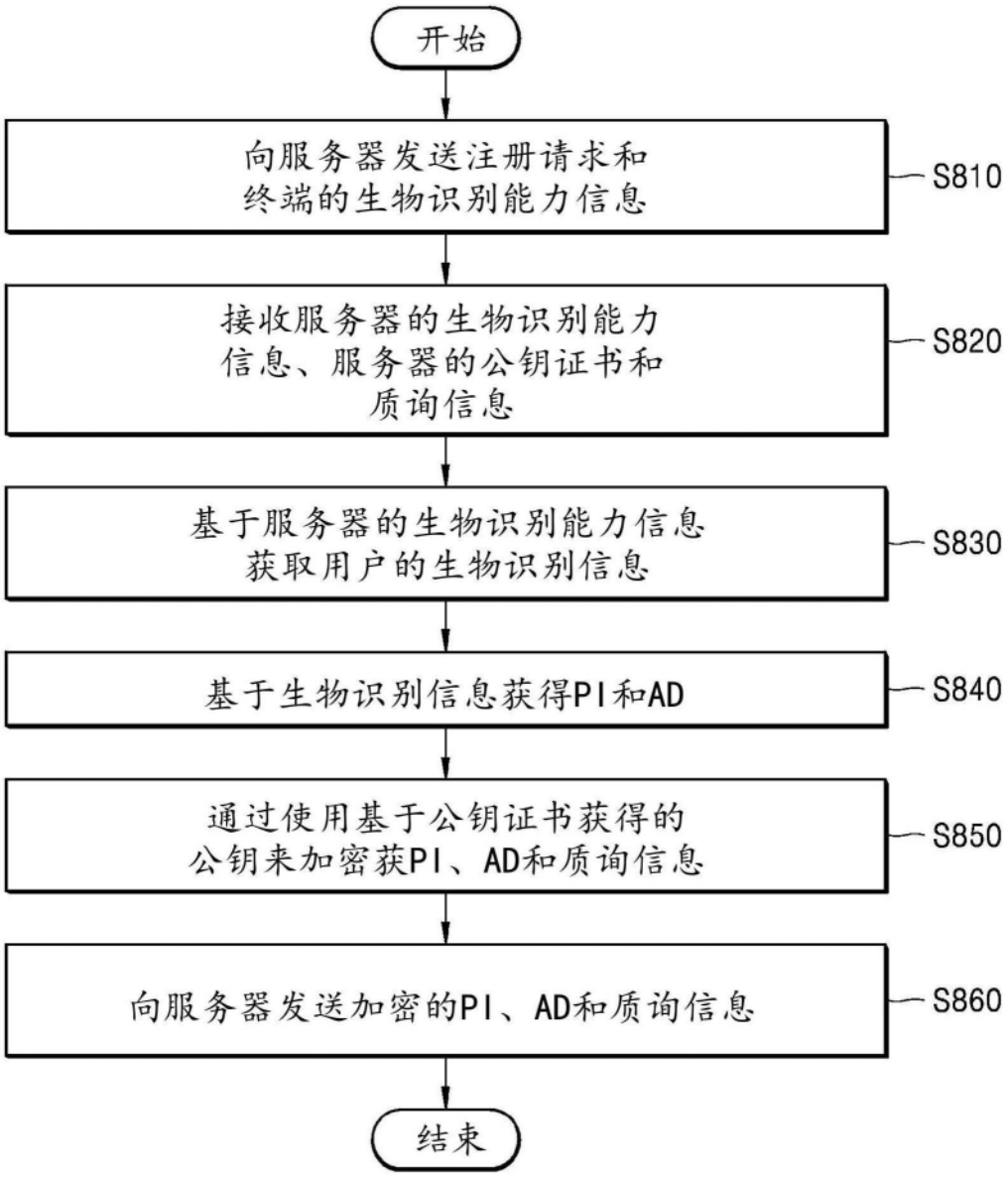

开始
向服务器发送注册请求和
终端的生物识别能力信息
S810
接收服务器的生物识别能力
信息、服务器的公钥证书和
质询信息
S820
基于服务器的生物识别能力信息
获取用户的生物识别信息
S830
基于生物识别信息获得PI和AD
S840
通过使用基于公钥证书获得的
公钥来加密获PI、AD和质询信息
S850
向服务器发送加密的PI、AD和质询信息
S860
结束

图8

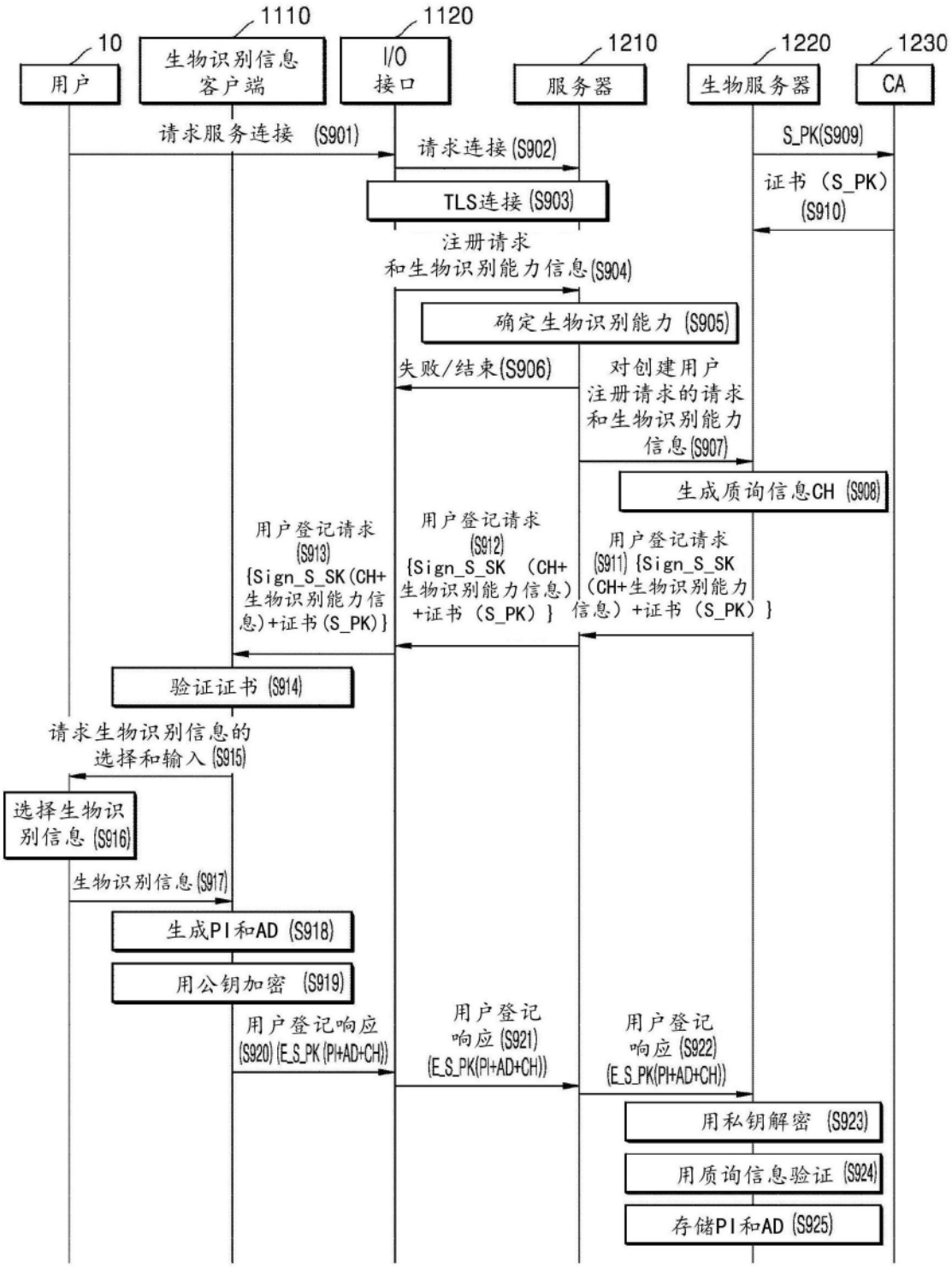

10
用户
1110
生物识别信息客户端
1120
I/O接口
1210
服务器
1220
生物服务器
1230
CA
请求服务连接 (S901)
请求连接(S902)
TLS连接 (S903)
S_PK(S909)
证书（S_PK）(S910)
注册请求和生物识别能力信息(S904)
确定生物识别能力 (S905)
失败/结束(S906)
对创建用户注册请求的请求和生物识别能力信息(S907)
生成质询信息CH (S908)
用户登记请求(S913){Sign_S_SK(CH+生物识别能力信息)+证书(S_PK)}
用户登记请求(S912){Sign_S_SK (CH+生物识别能力信息)+证书（S_PK）}
用户登记请求(S911){Sign_S_SK(CH+生物识别能力信息）+证书（S_PK）}
验证证书 (S914)
请求生物识别信息的选择和输入(S915)
选择生物识别信息(S916)
生物识别信息(S917)
生成PI和AD (S918)
用公钥加密 (S919)
用户登记响应(S920)(E_S_PK(PI+AD+CH))
用户登记响应(S921)(E_S_PK(PI+AD+CH))
用户登记响应(S922)(E_S_PK(PI+AD+CH))
用私钥解密 (S923)
用质询信息验证 (S924)
存储PI和AD (S925)

图9

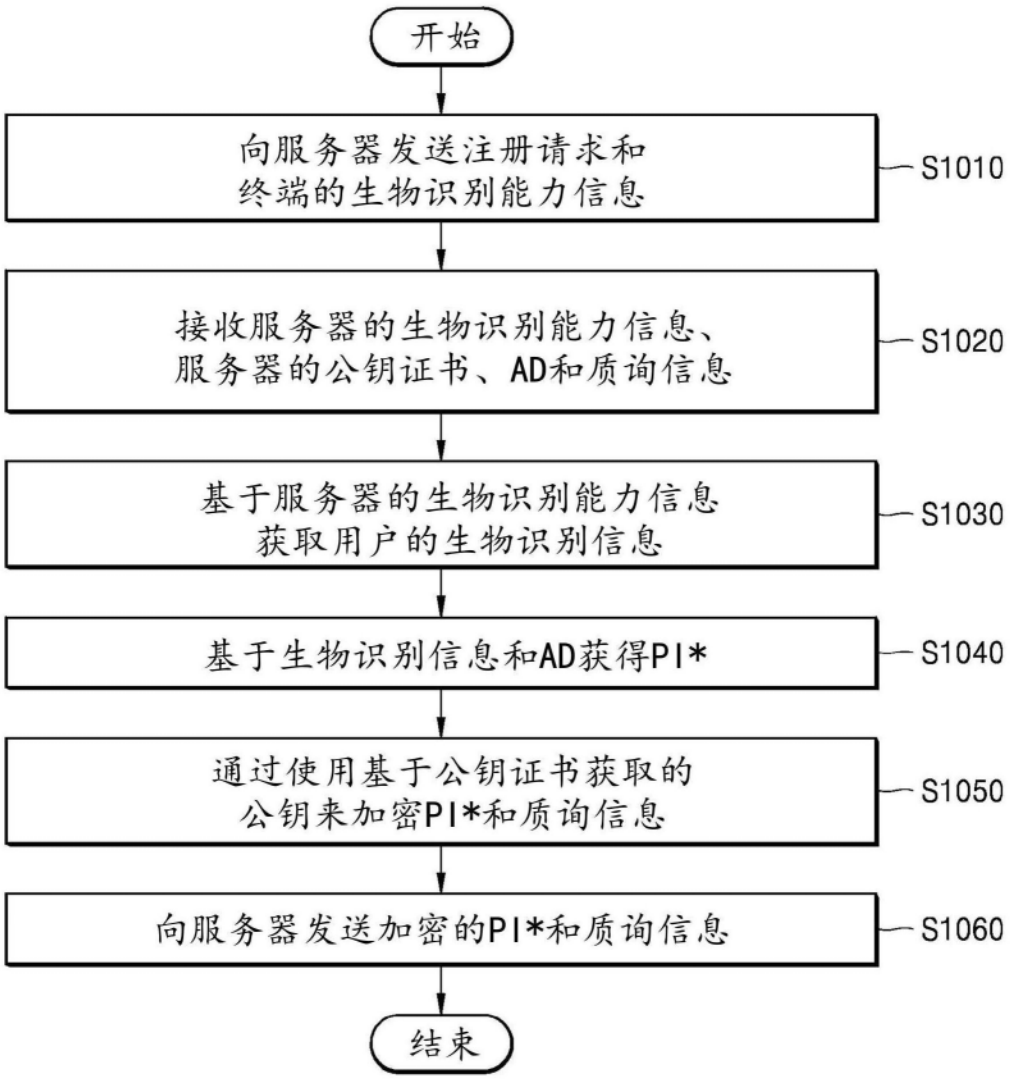

开始
向服务器发送注册请求和
终端的生物识别能力信息
S1010
接收服务器的生物识别能力信息、
服务器的公钥证书、AD和质询信息
S1020
基于服务器的生物识别能力信息
获取用户的生物识别信息
S1030
基于生物识别信息和AD获得PI*
S1040
通过使用基于公钥证书获取的
公钥来加密PI*和质询信息
S1050
向服务器发送加密的PI*和质询信息
S1060
结束

图10

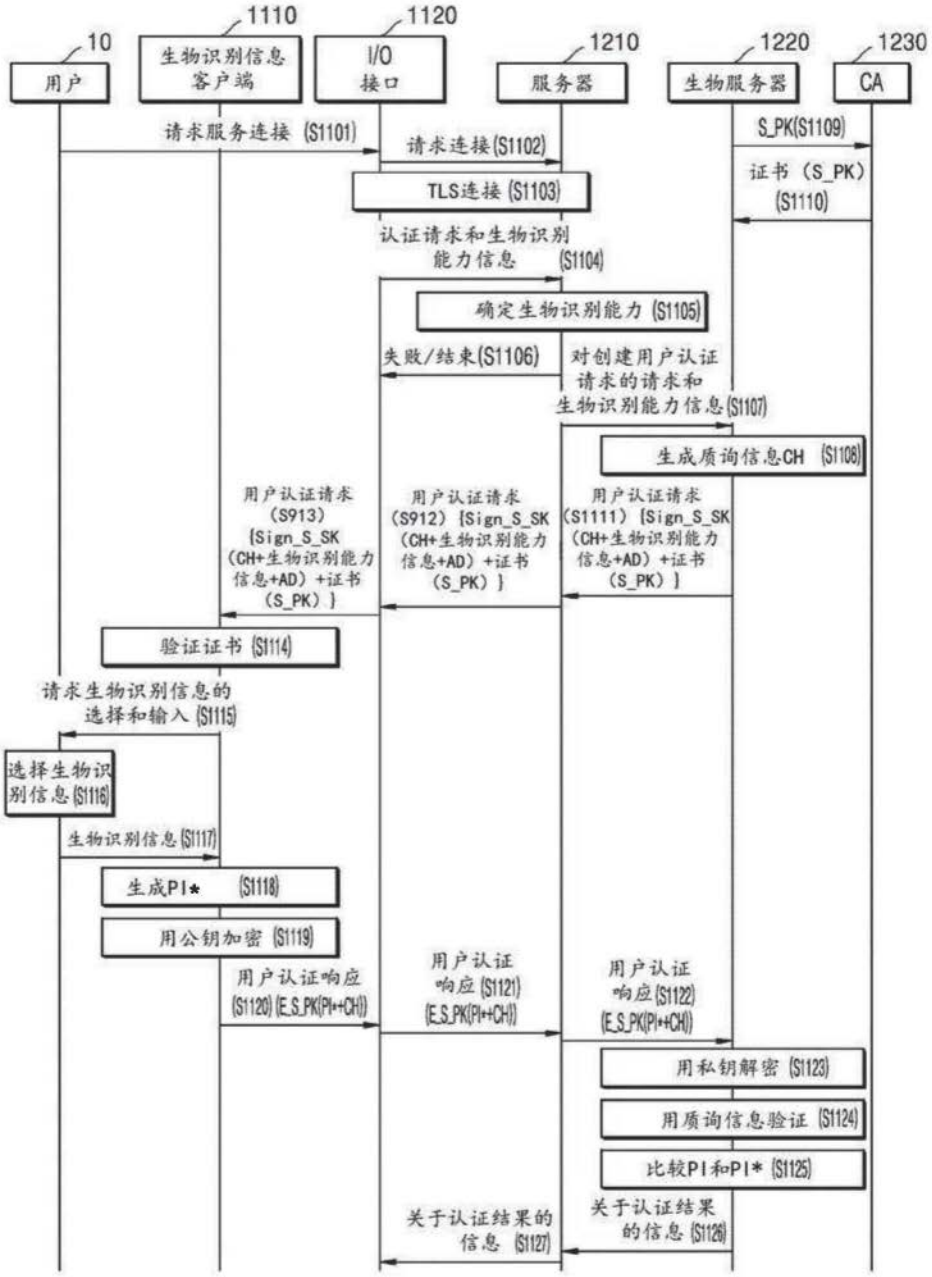

10
用户
1110
生物识别信息客户端
1120
I/O接口
1210
服务器
1220
生物服务器
1230
CA
请求服务连接 (S1101)
请求连接(S1102)
TLS连接 (S1103)
S_PK(S1109)
证书（S_PK）(S1110)
认证请求和生物识别能力信息 (S1104)
确定生物识别能力 (S1105)
失败/结束(S1106)
对创建用户认证请求的请求和生物识别能力信息(S1107)
生成质询信息CH (S1108)
用户认证请求 (S913) {Sign_S_SK (CH+生物识别能力信息+AD) +证书 (S_PK) }
用户认证请求 (S912) {Sign_S_SK (CH+生物识别能力信息+AD) +证书 (S_PK) }
用户认证请求 (S1111) {Sign_S_SK (CH+生物识别能力信息+AD) +证书 (S_PK) }
验证证书 (S1114)
请求生物识别信息的选择和输入 (S1115)
选择生物识别信息(S1116)
生物识别信息(S1117)
生成PI* (S1118)
用公钥加密 (S1119)
用户认证响应 (S1120) (E_S_PK(PI+CH))
用户认证响应 (S1121) (E_S_PK(PI+CH))
用户认证响应 (S1122) (E_S_PK(PI+CH))
用私钥解密 (S1123)
用质询信息验证 (S1124)
比较PI和PI* (S1125)
关于认证结果的信息 (S1126)
关于认证结果的信息 (S1127)

图11

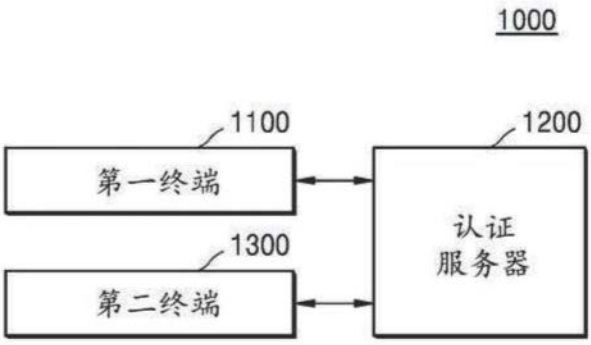

1000
1100
第一终端
1200
认证
服务器
1300
第二终端

图12

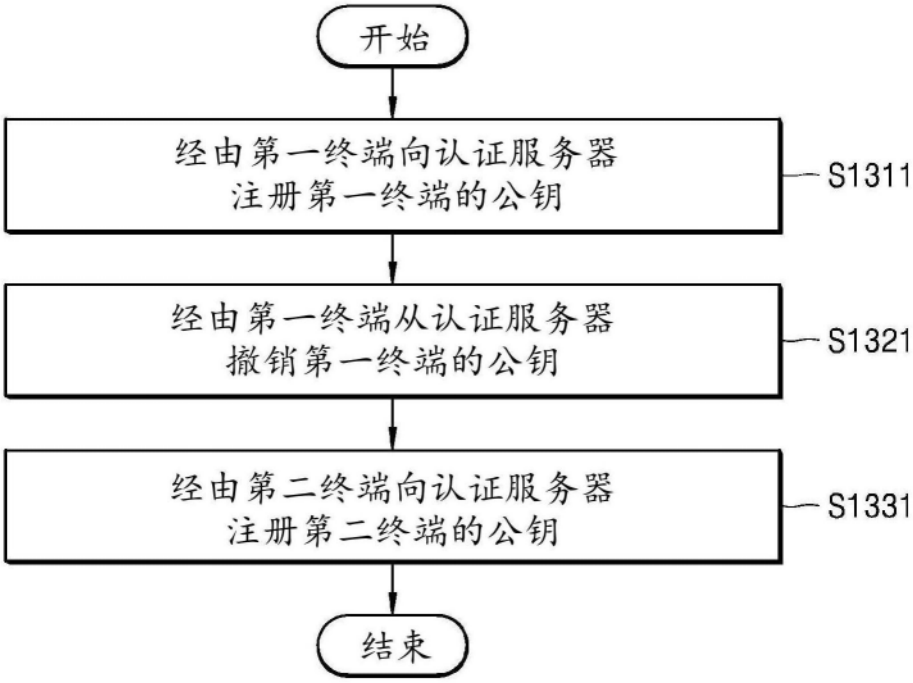

开始
经由第一终端向认证服务器
注册第一终端的公钥
S1311
经由第一终端从认证服务器
撤销第一终端的公钥
S1321
经由第二终端向认证服务器
注册第二终端的公钥
S1331
结束

图13A

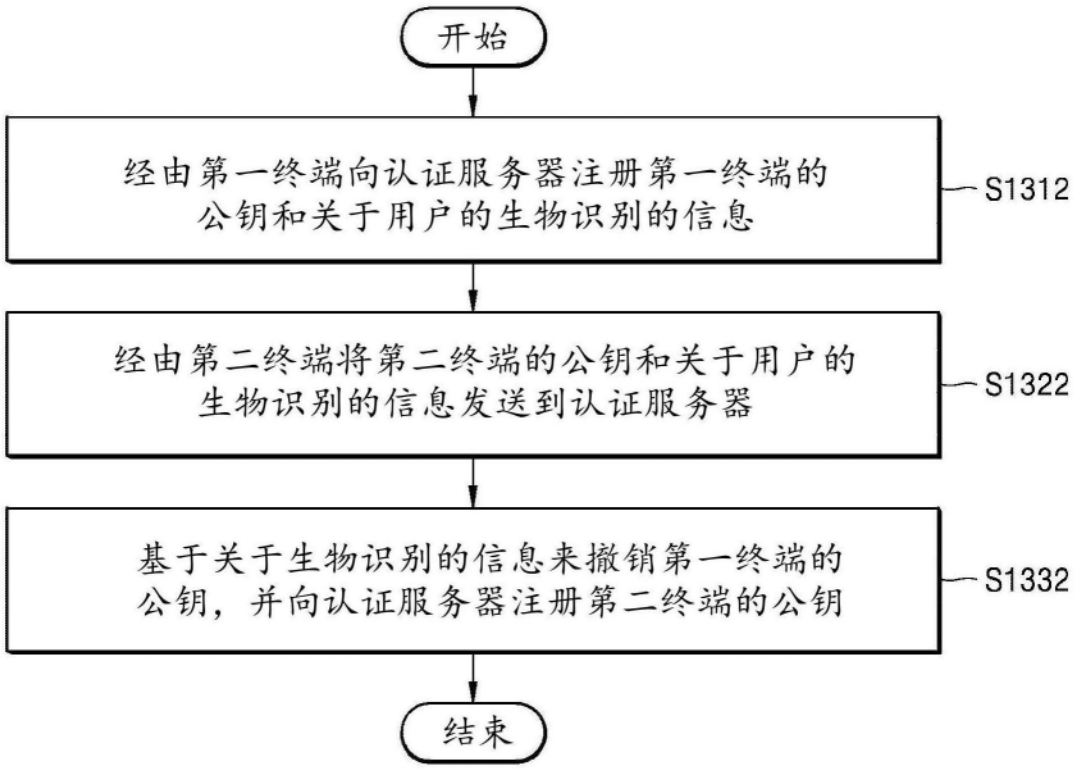

开始
经由第一终端向认证服务器注册第一终端的公钥和关于用户的生物识别的信息
S1312
经由第二终端将第二终端的公钥和关于用户的生物识别的信息发送到认证服务器
S1322
基于关于生物识别的信息来撤销第一终端的公钥，并向认证服务器注册第二终端的公钥
S1332
结束

图13B

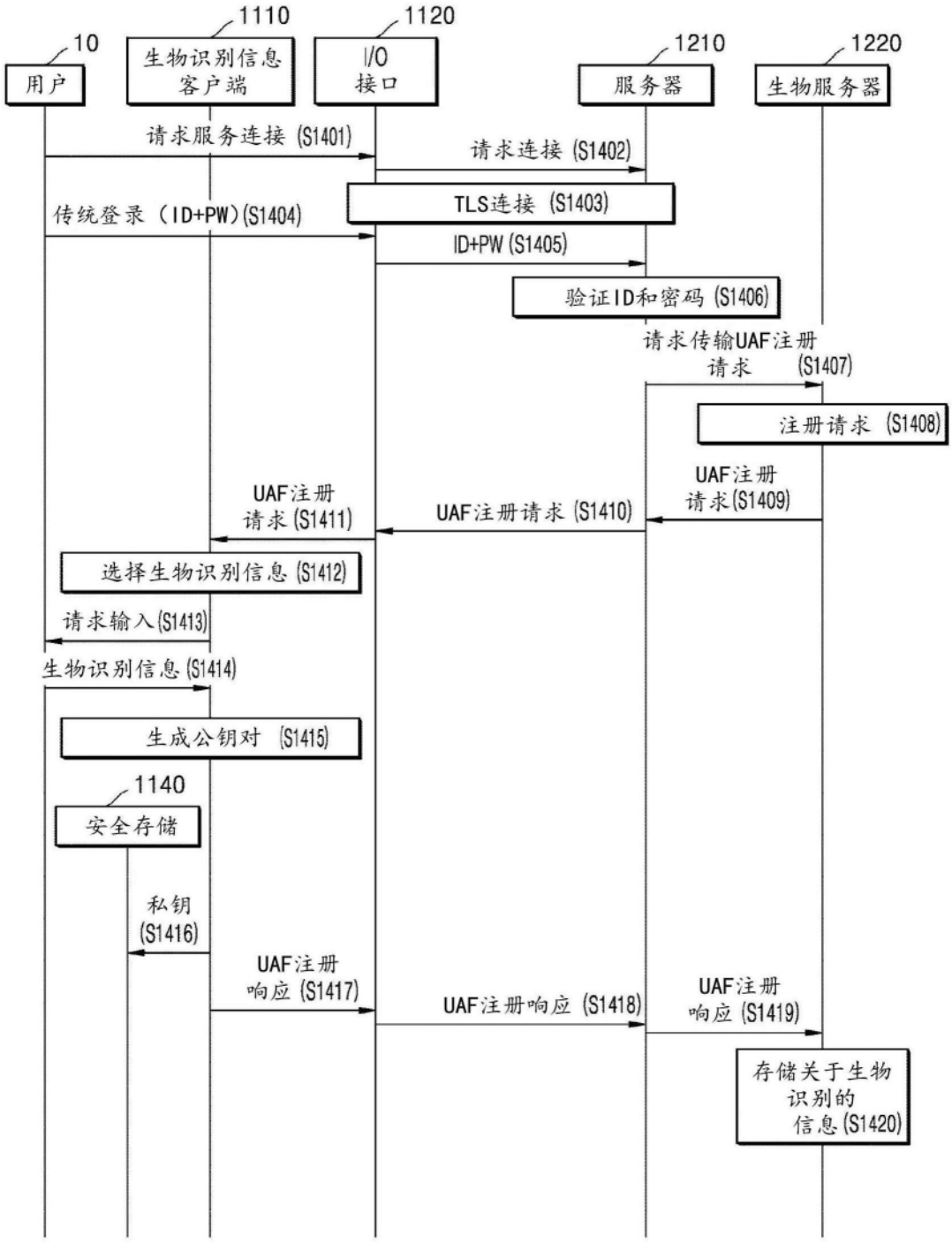

10
用户
1110
生物识别信息客户端
1120
I/O接口
1210
服务器
1220
生物服务器
请求服务连接 (S1401)
请求连接 (S1402)
TLS连接 (S1403)
传统登录（ID+PW）(S1404)
ID+PW (S1405)
验证ID和密码 (S1406)
请求传输UAF注册请求 (S1407)
注册请求 (S1408)
UAF注册请求(S1409)
UAF注册请求 (S1410)
UAF注册请求 (S1411)
选择生物识别信息 (S1412)
请求输入(S1413)
生物识别信息 (S1414)
生成公钥对 (S1415)
1140
安全存储
私钥 (S1416)
UAF注册响应 (S1417)
UAF注册响应 (S1418)
UAF注册响应 (S1419)
存储关于生物识别的信息 (S1420)

图14

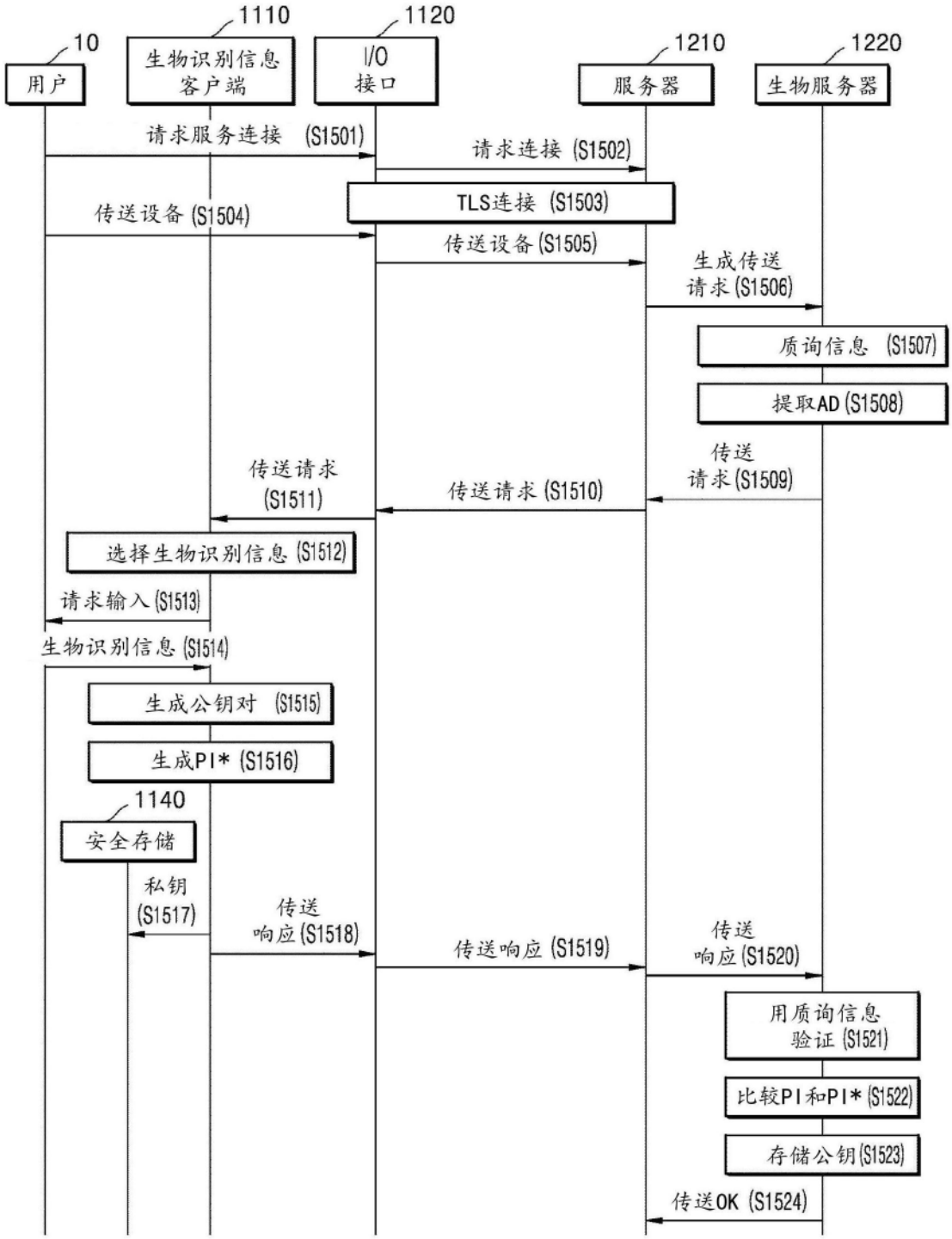

10
用户
1110
生物识别信息客户端
1120
I/O接口
1210
服务器
1220
生物服务器
请求服务连接 (S1501)
请求连接 (S1502)
TLS连接 (S1503)
传送设备 (S1504)
传送设备 (S1505)
生成传送请求 (S1506)
质询信息 (S1507)
提取AD (S1508)
传送请求 (S1509)
传送请求 (S1510)
传送请求 (S1511)
选择生物识别信息 (S1512)
请求输入 (S1513)
生物识别信息 (S1514)
生成公钥对 (S1515)
生成PI* (S1516)
1140
安全存储
私钥 (S1517)
传送响应 (S1518)
传送响应 (S1519)
传送响应 (S1520)
用质询信息验证 (S1521)
比较PI和PI* (S1522)
存储公钥 (S1523)
传送OK (S1524)

图15

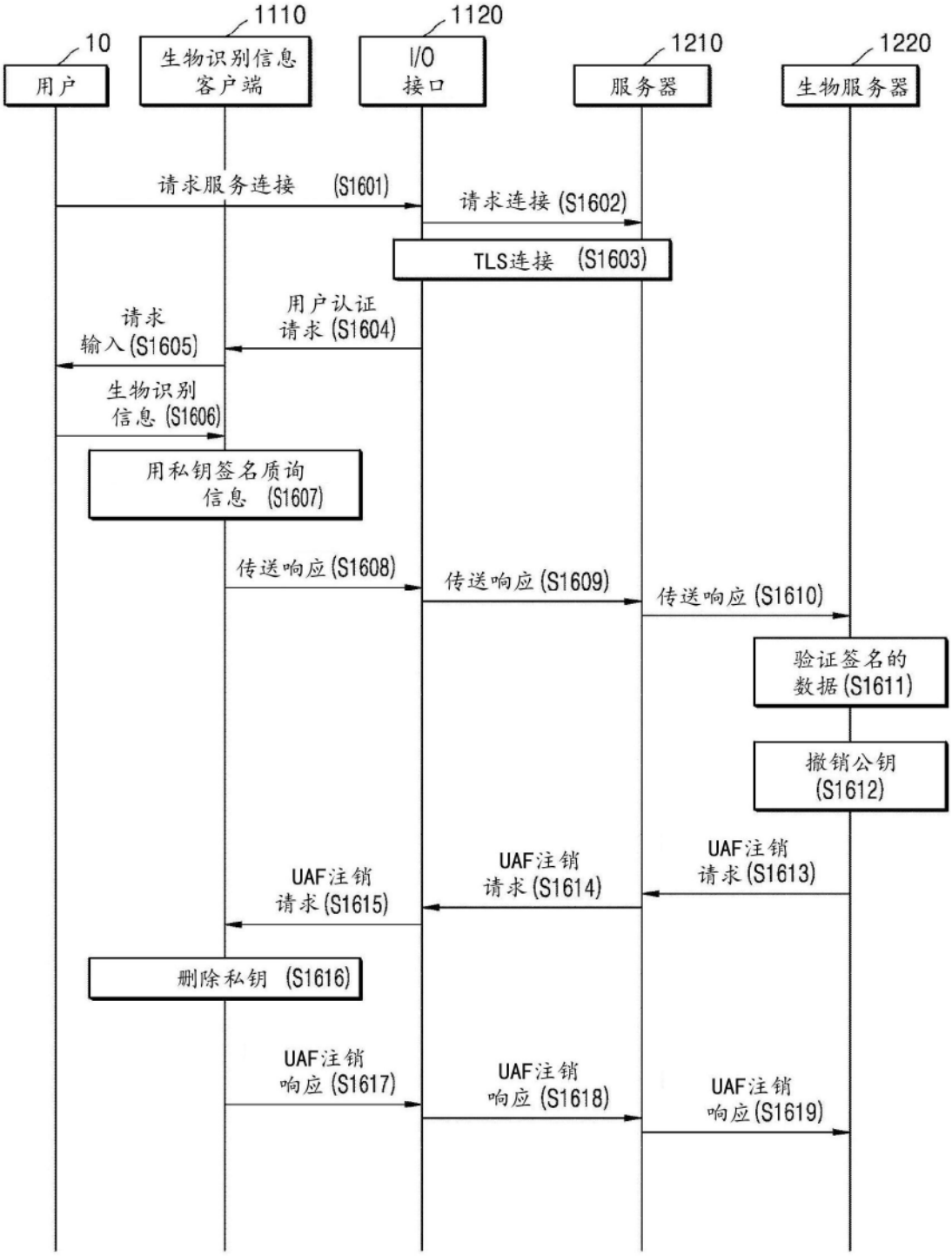

10
用户
1110
生物识别信息客户端
1120
I/O接口
1210
服务器
1220
生物服务器
请求服务连接 (S1601)
请求连接 (S1602)
TLS连接 (S1603)
用户认证请求 (S1604)
请求输入 (S1605)
生物识别信息 (S1606)
用私钥签名质询信息 (S1607)
传送响应 (S1608)
传送响应 (S1609)
传送响应 (S1610)
验证签名的数据 (S1611)
撤销公钥 (S1612)
UAF注销请求 (S1613)
UAF注销请求 (S1614)
UAF注销请求 (S1615)
删除私钥 (S1616)
UAF注销响应 (S1617)
UAF注销响应 (S1618)
UAF注销响应 (S1619)

图16