(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106575416 B
(45)授权公告日 2020.12.04

(21)申请号 201580041803.4
(22)申请日 2015.07.30
(65)同一申请的已公布的文献号
申请公布号 CN 106575416 A
(43)申请公布日 2017.04.19
(30)优先权数据
14/448,641 2014.07.31 US
(85)PCT国际申请进入国家阶段日
2017.01.26
(86)PCT国际申请的申请数据
PCT/US2015/042783 2015.07.30
(87)PCT国际申请的公布数据
WO2016/019086 EN 2016.02.04
(73)专利权人 诺克诺克实验公司
地址 美国加利福尼亚州
(72)发明人 R·林德曼
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 沈锦华
(51)Int.Cl.
G06Q 40/00(2012.01)
(56)对比文件
CN 101276448 A,2008.10.01
CN 101101687 A,2008.01.09
CN 101636949 A,2010.01.27
CN 1312510 A,2001.09.12
CN 1882963 A,2006.12.20
CN 103220145 A,2013.07.24
CN 103475666 A,2013.12.25
CN 101051908 A,2007.10.10
CN 102255917 A,2011.11.23
CN 101336436 A,2008.12.31
AU 1539501 A,2001.06.25
US 2009134972 A1,2009.05.28
US 2013191884 A1,2013.07.25
US 5588061 A,1996.12.24
US 2012308000 A1,2012.12.06
审查员 闪赛

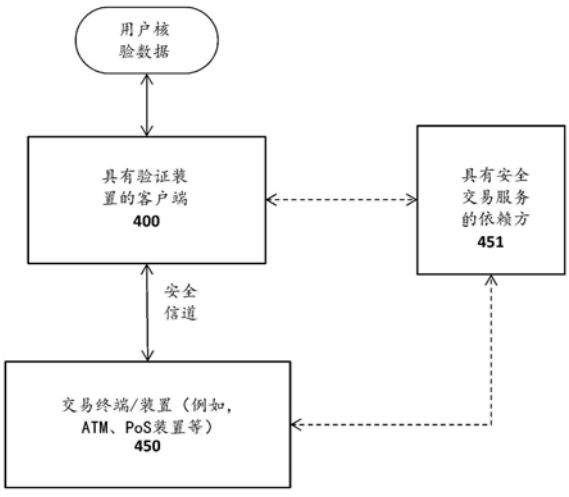
权利要求书2页 说明书15页 附图15页

(54)发明名称

用于向装置验证客户端的系统和方法

(57)摘要

本发明公开了用于向装置验证客户端的系统、设备、方法和机器可读介质。例如，方法的一个实施例包括：向依赖方注册客户端的验证器，注册允许客户端的用户经由网络远程地向所述依赖方验证所述用户；至少使用与所述验证器相关联的第一验证密钥和通过第一核验密钥生成的签名来生成第一验证结构；在所述客户端上缓存所述第一验证结构；向交易装置提供对应于所述第一核验密钥的第二核验密钥；在所述客户端与所述交易装置之间执行验证交易，其中，所述客户端使用与所述第一验证密钥相关联的第二验证密钥来生成第二验证结构，所述交易装置使用所述第二核验密钥来验证所述第一验证结构上的所述签名，并且使用所述第一验证密钥来验证所述第二验证结构。



CN 106575416 B

1.一种用以使用依赖方向交易装置验证客户端的方法,包括:

向所述依赖方注册所述客户端的验证器,所述注册允许所述客户端的用户经由网络远程地向所述依赖方验证所述用户;

至少使用与所述验证器相关联的第一验证密钥和通过第一核验密钥生成的签名在所述依赖方处生成第一验证结构;

在所述客户端上缓存所述第一验证结构;

向所述交易装置提供对应于所述第一核验密钥的第二核验密钥;以及

在所述客户端与所述交易装置之间执行验证交易,其中,所述客户端使用与所述第一验证密钥相关联的第二验证密钥来生成第二验证结构,所述交易装置使用所述第二核验密钥来验证所述第一验证结构上的所述签名,并且使用所述第一验证密钥来验证所述第二验证结构,其中所述第一核验密钥和所述第二核验密钥是相同的密钥,并且/或者所述第一验证密钥和所述第二验证密钥是相同的密钥。

2.根据权利要求1所述的方法,其中所述第一核验密钥是用于生成所述签名的私有密钥,并且向所述交易装置提供的所述第二核验密钥是能够验证所述签名的对应的公共核验密钥。

3.根据权利要求1所述的方法,其中所述第二验证密钥包括与所述验证器相关联的私有验证密钥,并且所述第一验证密钥是对应的公共验证密钥。

4.根据权利要求1所述的方法,其中所述第一验证密钥包括与所述验证器相关联的公共密钥(Uauth.pub),并且所述签名是使用所述第一核验密钥在至少所述公共密钥上生成。

5.一种用以使用依赖方向交易装置验证客户端的方法,包括:

向所述依赖方注册所述客户端的验证器,所述注册允许所述客户端的用户经由网络远程地向所述依赖方验证所述用户;

至少使用与所述验证器相关联的第一验证密钥和通过第一核验密钥生成的签名在所述依赖方处生成第一验证结构;

响应于通过所述交易装置发起交易的用户请求,在所述交易装置上存储所述第一验证结构;

向所述交易装置提供对应于所述第一核验密钥的第二核验密钥;

在所述客户端与所述交易装置之间执行验证交易,其中,所述客户端使用与所述第一验证密钥相关联的第二验证密钥来生成第二验证结构,所述交易装置使用所述第二核验密钥来验证所述第一验证结构上的所述签名,并且使用所述第一验证密钥来验证所述第二验证结构,其中所述第一核验密钥和所述第二核验密钥是相同的密钥,并且/或者所述第一验证密钥和所述第二验证密钥是相同的密钥。

6.根据权利要求5所述的方法,其中所述第一验证密钥包括与所述验证器相关联的公共密钥(Uauth.pub),并且所述签名是使用所述第一核验密钥在至少所述公共密钥上生成。

7.根据权利要求6所述的方法,其中所述第一验证结构包括下列各项的组合:由所述依赖方生成的随机数、所述公共密钥,以及在所述随机数和所述公共密钥的组合上生成的所述签名。

8.根据权利要求6所述的方法,其中所述第一验证结构包括下列各项的组合:由所述依赖方生成的随机数、指示所述第一验证结构能够在所述客户端上缓存的时间量的缓存定时

数据、所述公共密钥，以及在所述随机数、所述缓存定时数据和所述公共密钥的组合上生成的所述签名。

9.根据权利要求6所述的方法，其中所述第二验证结构包括随机数或由所述交易装置提供的值，以及通过至少在所述随机数和/或由所述交易装置提供的所述值上应用所述第二验证密钥而生成的签名。

10.根据权利要求6所述的方法，其中所述第二验证结构包括签名，所述签名通过在与所述交易装置进行交易期间，在安全地显示在所述客户端上的交易文本上应用所述第二验证密钥而生成。

11.根据权利要求10所述的方法，其中，所述签名是由所述交易装置和/或所述依赖方使用所述第一验证密钥来核验。

12.一种用以使用依赖方向交易装置验证客户端的方法，包括：

向所述依赖方注册所述客户端的验证器，所述注册允许所述客户端的用户经由网络远程地向所述依赖方验证所述用户，其中所述验证器包括待注册的生物计量装置；

至少使用与所述验证器相关联的第一验证密钥通过所述依赖方生成第一验证结构；

在所述客户端上缓存所述第一验证结构；以及

在所述客户端与所述交易装置之间执行验证交易，其中，所述客户端使用与所述第一验证密钥相关联的第二验证密钥来生成第二验证结构，所述交易装置使用与所述依赖方的在线或带外连接来验证所述第一验证结构，并且使用所述第一验证密钥来验证所述第二验证结构，其中所述第一验证密钥和所述第二验证密钥是相同的密钥。

13.根据权利要求12所述的方法，其中所述第一验证密钥包括与所述验证器相关联的公共密钥(Uauth.pub)。

14.根据权利要求13所述的方法，其中所述第一验证结构包括下列各项的组合：由所述依赖方生成的随机数、所述公共密钥，以及在所述随机数和所述公共密钥的组合上生成的签名。

15.根据权利要求13所述的方法，其中所述第一验证结构包括下列各项的组合：由所述依赖方生成的随机数、指示所述第一验证结构能够在所述客户端上缓存的时间量的缓存定时数据、所述公共密钥，以及在所述随机数、所述缓存定时数据和所述公共密钥的组合上生成的签名。

用于向装置验证客户端的系统和方法

背景技术

技术领域

[0001] 本发明整体涉及数据处理系统的领域。更具体地讲，本发明涉及用于向装置验证客户端的系统和方法，所述装置诸如离线装置，或者与依赖方的连接性有限的装置。

[0002] 相关领域说明

[0003] 图1示出了具有生物计量装置100的示例性客户端120。正常运行时，生物计量传感器102从用户读取原始生物计量数据(例如，捕捉用户指纹，记录用户声音，拍摄用户的照片，等等)，并且特征提取模块103提取原始生物计量数据的指定特征(例如，注重于指纹的某些区域、某些面部特征等等)。匹配器模块104将所提取的特征133与存储在客户端120上的安全存储装置中的生物计量参考数据110进行比较，并且基于所提取的特征与生物计量参考数据110之间的相似性来生成得分153。生物计量参考数据110通常是登记过程的结果，在登记过程中用户向装置100登记指纹、声音样本、图像或其他生物计量数据。应用程序105可接着使用得分135来确定验证是否成功(例如，得分是否高于某个指定阈值)。

[0004] 还已经设计了使用生物计量传感器经由网络提供安全用户验证的系统。在此类系统中，可经由网络发送由应用程序105生成的得分135和/或其他验证数据，以向远程服务器验证用户。例如，专利申请No.2011/0082801(“‘801申请”)描述了一种在网络上进行用户注册和验证的框架，这种框架提供强验证(例如，防御身份窃取和网络钓鱼)、安全交易(例如，防御交易中的“浏览器中的恶意软件”和“中间人”攻击)和客户端验证令牌的登记/管理(例如，指纹读取器、面部识别装置、智能卡、可信平台模块等等)。

[0005] 本申请的受让人已经开发出对‘801申请中所描述的验证框架的多种改进。这些改进中的一些在以下一组美国专利申请(“共同待决的申请”)中描述，这些美国专利申请全部在2012年12月29日提交并且转让给本受让人：序列号13/730,761，名称为“Query System and Method to Determine Authentication Capabilities”(用于确定验证能力的查询系统和方法)；序列号13/730,776，名称为“System and Method for Efficiently Enrolling,Registering,and Authenticating With Multiple Authentication Devices”(使用多个验证装置有效地进行登记、注册和验证的系统和方法)；序列号13/730,780，名称为“System and Method for Processing Random Challenges Within an Authentication Framework”(用于在验证框架内处理随机质询的系统和方法)；序列号13/730,791，名称为“System and Method for Implementing Privacy Classes Within an Authentication Framework”(用于在验证框架内实施隐私类别的系统和方法)；序列号13/730,795，名称为“System and Method for Implementing Transaction Signaling Within an Authentication Framework”(用于在验证框架内实施交易信令的系统和方法)。

[0006] 简而言之，在这些共同待决的申请描述的验证技术中，用户向客户端的生物计量装置登记，以生成生物计量模板数据(例如，通过轻扫手指、拍摄照片、记录语音等)；经由网

络(例如,如共同待决的申请中所述的配备有安全交易服务的网站或其他依赖方)向一个或多个服务器注册生物计量装置;随后使用在注册过程中交换的数据(例如,预置到生物计量装置中的加密密钥)与那些服务器验证。一旦通过验证,用户便获许与网站或其他依赖方执行一个或多个在线交易。在共同待决的申请所描述的框架中,敏感信息(诸如指纹数据和可用于唯一地识别用户的其他数据)可本地保持在用户的客户端装置(例如,智能电话、笔记本计算机等等)上,以保护用户的隐私。

附图说明

[0007] 可结合下列附图从以下具体实施方式更好地理解本发明,其中:

[0008] 图1示出了具有生物计量验证能力的示例性客户端装置;

[0009] 图2A和图2B示出了安全验证系统架构的两个不同实施例;

[0010] 图2C是示出可如何将密钥注册到验证装置中的事务图;

[0011] 图3A和图3B示出了使用安全显示器进行安全交易确认的实施例;

[0012] 图4示出了用未建立关系的装置执行交易验证的本发明的一个实施例;

[0013] 图5A和图5B是示出用于执行交易验证的两个不同实施例的事务图;

[0014] 图6示出了本发明的一个实施例中采用的额外架构特征;

[0015] 图7至图8示出了本发明的不同实施例中采用的不记名令牌的不同实施例;

[0016] 图9示出了示例性的“离线”和“半离线”验证场景;

[0017] 图10示出了客户端和/或服务器的示例性系统架构;以及

[0018] 图11示出了客户端和/或服务器的另一个示例性系统架构。

具体实施方式

[0019] 下文描述用于实施高级验证技术及相关联应用的设备、方法和机器可读介质的实施例。在整个描述中,出于解释的目的,本文陈述了许多特定细节以便透彻理解本发明。然而,本领域的技术人员将容易明白,可在没有这些特定细节中的一些的情况下实践本发明。在其他情况下,为免模糊本发明的基本原理,已熟知的结构和装置未示出或以框图形式示出。

[0020] 下文论述的本发明的实施例涉及具有验证能力(诸如生物计量装置或PIN输入)的客户端装置。这些装置在本文中有时称为“令牌”、“验证装置”或“验证器”。尽管某些实施例注重于面部识别硬件/软件(例如,用于识别用户面部并且跟踪用户的眼球运动的相机和相关联软件),但有些实施例可利用额外的生物计量装置,包括(例如)指纹传感器、声音识别硬件/软件(例如,用于识别用户声音的麦克风和相关联软件)以及光学识别能力(例如,用于扫描用户视网膜的光学扫描器和相关联软件)。验证能力还可包括非生物计量装置,诸如可信平台模块(TPM)和智能卡。

[0021] 在移动式生物计量的具体实施中,生物计量装置可远离依赖方。如本文所用,术语“远程”意味着生物计量传感器不是其以通信方式耦接到的计算机的安全边界的一部分(例如,生物计量传感器未嵌入到与依赖方计算机相同的物理外壳中)。举例来说,生物计量装置可经由网络(例如,因特网、无线网络链路等)或经由外围输入(诸如USB端口)耦接到依赖方。在这些条件下,依赖方可能无法知道装置是否为得到依赖方授权的装置(例如,提供可

接受等级的验证和完整性保护的装置)以及/或者黑客是否已经危及生物计量装置。生物计量装置的置信度取决于装置的特定实施。

[0022] 然而,如下文所论述,用于验证用户的验证技术可能涉及非位置组件,诸如经由网络与远程服务器和/或其他数据处理装置的通信。此外,尽管本文中描述了特定实施例(诸如ATM和零售点),但应该指出的是,可在由最终用户在其内本地或远程发起交易的任何系统的环境中实施本发明的基本原理。

[0023] 本文中有时使用术语“依赖方”来不仅指尝试与之进行用户交易的实体(例如,执行用户交易的网站或在线服务),也指代表那个实体实施的安全交易服务器(其可执行本文所述的基础验证技术)。提供远程验证能力的安全交易服务器可由依赖方拥有并且/或者在依赖方的控制下,或者可在作为业务安排的一部分向依赖方提供安全交易服务的第三方的控制下。

[0024] 本文中使用的术语“服务器”指的是在一个硬件平台上(或跨多个硬件平台)执行的软件,其经由网络从客户端接收请求,然后作为响应来执行一个或多个操作,并且将响应传输到客户端,该响应通常包括操作的结果。服务器对客户端请求做出响应,从而向客户端提供或帮助向客户端提供网络“服务”。值得注意的是,服务器不限于单个计算机(例如,用于执行服务器软件的单个硬件装置),而是实际上可散布在多个硬件平台上,有可能位于多个地理位置处。

[0025] 本文所述的本发明的实施例包括用于针对通过安全交易装置发起的交易验证用户的技术。举例来说,交易可为提款、转账或其他用户发起的操作,交易装置可为自动取款机(ATM)、销售点(PoS)交易装置或能够代表用户执行交易的其他装置。交易可涉及例如在配备有交易装置的零售店或其他零售点完成支付以购买商品或服务、经由交易装置提取资金、对交易装置执行维护,或需要针对其进行用户验证的任何其他交易。

[0026] 本发明的一个实施例提供了用于在本地、甚至在装置离线(即,未连接到后端验证服务器)或半离线(即,仅周期性地连接到后端验证服务器)的情况下验证用户身份(即,核验用户)的技术。在一个实施例中,用户的客户端装置拥有缓存后端验证服务器(例如,代表依赖方操作)所生成的验证请求的能力,并且所述装置被提供有核验从用户的客户端装置传输到该装置的验证响应所需要的数据。

[0027] 在讨论本发明的这些实施例的细节之前,本文先提供对远程用户验证技术的概述。这些和其他远程用户验证技术在共同待决的申请中有所描述,这些共同待决的申请被转让给本申请的受让人并且以引用方式并入本文。

[0028] 远程用户验证技术

[0029] 图2A和图2B示出了包括用于远程验证用户的客户端侧组件和服务器侧组件的系统架构的两个实施例。图2A所示的实施例使用基于浏览器插件的架构来与网站通信,而图2B所示的实施例不需要浏览器。本文所述的各种验证技术和相关联的应用程序可在这些系统架构中的任一个上实施。例如,本文所述的客户端装置内的验证引擎可被实施为包括接口202的安全交易服务201的一部分。然而,应该指出的是,上文所述的实施例可使用除了图2A和图2B所示的那些之外的硬件与软件的逻辑布置来实施。

[0030] 转到图2A,图示实施例包括配备有一个或多个验证装置210至212的客户端200,这些验证装置用于登记和验证最终用户。如上所述,验证装置210至212可包括生物计量装置,

诸如指纹传感器、声音识别硬件/软件(例如,用于识别用户声音的麦克风和相关联软件)、面部识别硬件/软件(例如,用于识别用户面部的相机和相关联软件)和光学识别功能(例如,用于扫描用户的视网膜的光学扫描器和相关联软件);以及非生物计量装置,诸如可信平台模块(TPM)和智能卡。用户可通过提供生物计量数据(例如,在指纹装置上轻扫手指)来登记生物计量装置,安全交易服务201可将这些生物计量数据作为生物计量模板数据(经由接口202)存储在安全存储装置220中。

[0031] 尽管安全存储装置220被示出为在验证装置210至212的安全周界之外,但在一个实施例中,每个验证装置210至212可具有其自身的集成安全存储装置。另外,每个验证装置210至212可按加密方式保护生物计量参考数据记录(例如,使用对称密钥包裹这些数据记录,以使存储装置220安全)。

[0032] 验证装置210至212通过由安全交易服务201暴露的接口202(例如,应用程序编程接口或API)以通信方式耦接到客户端。安全交易服务201是用于经由网络与一个或多个安全交易服务器232至233通信以及用于与在web浏览器204的环境内执行的安全交易插件205介接的安全应用程序。如图所示,接口202还可提供对客户端200上的安全存储装置220的安全访问,该安全存储装置存储与验证装置210至212中的每一个相关的信息,诸如装置识别代码(诸如验证器证实ID(AAID))、用户识别代码、用户登记数据(例如,所扫描的指纹或其他生物计量数据),以及用于执行本文所述的安全验证技术的密钥。例如,如下文详细论述,唯一密钥可被存储到每个验证装置中,随后在经由网络(诸如因特网)与服务器230通信时使用。

[0033] 如下文论述,安全交易插件205支持某些类型的网络交易,诸如与网站231或其他服务器的HTTP或HTTPS交易。在一个实施例中,响应于由安全企业或Web目的地230内的网络服务器231(下文中有时简称为“服务器230”)插入到网页HTML代码中的特定HTML标签来启动安全交易插件。响应于检测到此类标签,安全交易插件205可将交易转发到安全交易服务201以进行处理。另外,对于某些类型的事务(例如,诸如安全密钥交换),安全交易服务201可开启与当地交易服务器232(即,与网站位于同一地点)或异地交易服务器233的直接通信信道。

[0034] 安全交易服务器232至233耦接到安全交易数据库240以存储用户数据、验证装置数据、密钥以及支持下文所述的安全验证交易所需要的其他安全信息。然而,应该指出的是,本发明的基本原理不需要分离图2A所示的安全企业或web目的地230内的逻辑组件。例如,网站231和安全交易服务器232至233可在单个物理服务器或单独物理服务器内实施。此外,网站231和交易服务器232至233可在一个或多个服务器上所执行的集成软件模块内实施,以执行下文所述的功能。

[0035] 如上所述,本发明的基本原理不限于图2A所示的基于浏览器的架构。图2B示出替代性具体实施,其中独立应用程序254利用由安全交易服务201提供的功能来经由网络验证用户。在一个实施例中,应用程序254被设计为建立与一个或多个网络服务251的通信会话,这些网络服务依赖于安全交易服务器232至233来执行下文详细描述的用户/客户端验证技术。

[0036] 在图2A和图2B所示的任一个实施例中,安全交易服务器232至233可生成密钥,这些密钥接着被安全地传输到安全交易服务201并存储到安全存储装置220内的验证装置中。

另外，安全交易服务器232至233管理服务器端上的安全交易数据库240。

[0037] 图2C示出了用于注册验证装置的一系列事务。如上所述，在注册期间，在验证装置与安全交易服务器232至233中的一个之间共享密钥。密钥存储在客户端200的安全存储装置220和由安全交易服务器232至233使用的安全交易数据库220内。在一个实施例中，密钥是由安全交易服务器232至233中的一个生成的对称密钥。然而，在下文论述的另一个实施例中，可使用不对称密钥。在该实施例中，公共密钥可由安全交易服务器232至233存储，并且第二相关私有密钥可存储在客户端上的安全存储装置220中。此外，在另一个实施例中，密钥可在客户端200上生成(例如，由验证装置或验证装置接口而不是安全交易服务器232至233生成)。本发明的基本原理不限于任何特定类型的密钥或生成密钥的方式。

[0038] 安全密钥预置协议(诸如动态对称密钥预置协议(DSKPP))可用于经由安全通信信道与客户端共享密钥(例如，见意见征求稿(RFC)6063)。然而，本发明的基本原理不限于任何特定密钥预置协议。

[0039] 转到图2C所示的具体细节，一旦用户登记或用户核验完成，服务器230便生成随机生成的质询(例如，密码随机数)，客户端必须在装置注册期间呈现此质询。该随机质询可在有限时间段内有效。安全交易插件检测随机质询并将其转发到安全交易服务201。作为响应，安全交易服务发起与服务器230的带外会话(例如，带外事务)，并使用密钥预置协议与服务器230通信。服务器230使用用户名定位用户、验证随机质询、在已经发送装置的证实代码(例如，AAID)的情况下验证该证实代码，并且在安全交易数据库220中为用户创建新条目。该服务器还可生成密钥或公共/私有密钥对，将密钥写入数据库220，并使用密钥预置协议将密钥发送回安全交易服务201。一旦完成，验证装置与服务器230便在使用对称密钥的情况下共享相同密钥，或者在使用不对称密钥的情况下共享不同密钥。

[0040] 图3A示出了用于基于浏览器的具体实施的安全交易确认。虽然示出了基于浏览器的具体实施，但相同的基本原理可使用独立应用程序或移动装置应用程序来实施。

[0041] 此安全交易确认被设计为向某些类型的交易(例如，金融交易)提供更强的安全性。在图示实施例中，用户在进行交易之前确认每个交易。使用图示技术，用户确认他/她究竟想要进行何种交易，并确实进行他/她在图形用户界面(GUI)的窗口301中看到的交易。换句话讲，该实施例确保“中间人”(MITM)或“浏览器中间人”(MITB)无法修改交易文本来进行用户没有确认的交易。

[0042] 在一个实施例中，安全交易插件205在浏览器环境中显示窗口301以展示交易细节。安全交易服务器201周期性地(例如，以随机间隔)核验窗口中所示的文本没有正被任何人篡改(例如，通过在所显示的文本上生成散列/签名)。在不同的实施例中，验证装置具有可信用户界面(例如，用于提供符合全球平台组织(GlobalPlatform)的可信UI的API)。

[0043] 以下例子将帮助突出显示该实施例的操作。用户从商家网站选择商品并选择“结账”。商家网站将交易发送到服务提供商(例如，PayPal)，该服务提供商具有实施本文所述的本发明的一个或多个实施例的安全交易服务器232至233。商家网站验证用户并完成交易。

[0044] 安全交易服务器232至233接收交易细节(TD)，并且将“安全交易”请求放在HTML页面中并发送到客户端200。安全交易请求包括交易细节和随机质询。安全交易插件205检测对交易确认消息的请求并将所有数据转发到安全交易服务201。在不使用浏览器或插件的

实施例中，可将该信息直接从安全交易服务器发送到客户端200上的安全交易服务。

[0045] 就基于浏览器的具体实施来说，安全交易插件205向用户显示具有交易细节的窗口301(例如，在浏览器环境中)，并要求用户提供验证以确认交易。在不使用浏览器或插件的实施例中，安全交易服务201、应用程序254(图2B)或验证装置210可显示窗口301。安全交易服务201启动计时器并验证正向用户显示的窗口301的内容。可随机选择验证周期。安全交易服务201确保用户在窗口301中看到有效交易细节(例如，生成有关细节的散列，并通过与正确内容的散列相比较来核验内容是否准确)。如果检测到内容已被篡改，则阻止生成确认令牌/签名。

[0046] 在用户提供有效核验数据(例如，通过在指纹传感器上轻扫手指)之后，验证装置核验用户，并使用交易细节和随机质询生成加密签名(有时称为“令牌”)(即，根据交易细节和随机数计算得到签名)。这允许安全交易服务器232至233确保尚未在服务器与客户端之间修改交易细节。安全交易服务201将所生成的签名和用户名发送到安全交易插件205，该安全交易插件将签名转发到安全交易服务器232至233。安全交易服务器232至233使用用户名标识用户并核验签名。如果验证成功，则向客户端发送确认消息并处理交易。

[0047] 本发明的一个实施例实施一种查询策略，其中安全交易服务器将服务器策略传输到客户端，该服务器策略指示服务器所接受的验证功能。客户端接着分析服务器策略以标识其支持的以及/或者用户已经表明想要使用的验证功能的子组。客户端接着使用与所提供的策略匹配的验证令牌子组注册和/或验证用户。因此，对客户端的隐私具有较小影响，因为不需要客户端传输关于其验证功能的详尽信息(例如，所有其验证装置)或可用于唯一地识别客户端的其他信息。

[0048] 以举例而非限制的方式，客户端可包括许多用户核验功能，诸如指纹传感器、声音识别功能、面部识别功能、眼球/光学识别功能、PIN核验等等。然而，出于隐私原因，用户可能不希望向请求服务器透露所有其功能的细节。因此，通过使用本文所述的技术，安全交易服务器可将服务器策略传输到客户端，该服务器策略指示其支持(例如)指纹、光学或智能卡验证。客户端可接着将服务器策略与其自己的验证功能进行比较，并选择一个或多个可用验证选项。

[0049] 本发明的一个实施例采用安全交易服务器上的交易签署，使得不需要在服务器上维持任何交易状态就能维持与客户端的会话。具体地讲，可将窗口301内所显示的诸如交易文本等交易细节发送到由服务器签署的客户端。服务器可接着通过验证签名来验证由客户端接收的已签署的交易响应是否有效。服务器不需要永久性地存储交易内容，因为对于大量客户端而言，这样做会消耗大量存储空间并且会导致对服务器的拒绝服务类型攻击的可能性。

[0050] 图3B中示出了本发明的一个实施例，其示出网站或其他网络服务311正在发起与客户端200的交易。例如，用户可能已在网站上选择了要购买的商品，并且可能已准备好结账付款。在图示例子中，网站或服务311将交易提交到安全交易服务器312，该安全交易服务器包括用于生成和核验签名(如本文所述)的签名处理逻辑313和用于执行客户端验证(例如，使用先前所述的验证技术)的验证逻辑314。

[0051] 在一个实施例中，从安全交易服务器312发送到客户端200的验证请求包括随机质询(诸如密码随机数)(如上所述)、交易细节(例如，为完成交易而呈现的特定文本)、和由签

名处理逻辑313使用私有密钥(仅安全交易服务器知道)在随机质询和交易细节上生成的签名。

[0052] 一旦客户端接收到以上信息,用户便可接收有关需要用户核验才能完成交易的指示。作为响应,用户可(例如)在指纹扫描器上轻扫手指,拍摄照片,对着麦克风说话,或执行针对给定交易所准许的任何其他类型的验证。在一个实施例中,一旦用户已经成功通过验证装置210的核验,客户端便将以下各项传输回服务器:(1)随机质询和交易文本(两者均由服务器在先前提供给客户端),(2)证明用户成功地完成验证的验证数据,以及(3)签名。

[0053] 安全交易服务器312上的验证模块314可接着确认用户已经正确地验证,并且签名处理逻辑313使用私有密钥在随机质询和交易文本上重新生成签名。如果该签名与客户端所发送的签名匹配,则服务器可验证交易文本与其最初从网站或服务311接收时相同。这节约了存储和处理资源,因为不需要安全交易服务器312将交易文本(或其他交易数据)永久性地存储在安全交易数据库120内。

[0054] 用于向离线装置或连接性有限的装置验证客户端的系统和方法

[0055] 如所提及的,本发明的一个实施例包括用于在本地、甚至在用户装置和所述装置离线(即,未连接到依赖方的后端验证服务器)或半离线(即,用户装置未连接到依赖方,但所述装置连接到依赖方)的情况下验证用户(即,核验用户)的技术。图4示出了一种这样的布置,其中,具有先前向依赖方451注册过的验证装置的客户端400与交易装置450建立安全信道以便完成交易。以举例而非限制的方式,交易装置可为ATM、零售点处的销售点(PoS)交易装置、物联网(IoT)装置,或者能够与客户端400建立信道并且允许用户执行交易的任何其他装置。可使用任何无线通信协议来实施信道,这些无线通信协议以举例而非限制的方式,包括近场通信(NFC)和蓝牙(例如,如蓝牙核心规范版本4.0中提出的蓝牙低功耗(BTLE)协议)。当然,本发明的基本原理不限于任何特定通信标准。

[0056] 如虚线箭头所指示,客户端400与依赖方451之间的连接和/或交易装置450与依赖方451之间的连接可能是偶尔发生的,或者可能不存在。支付领域内的实际应用程序通常依赖于此类“离线”使用情况。例如,拥有客户端400(例如,智能电话)的用户在交易时可能未与依赖方451连接,但可能想要通过向交易装置450验证来授权交易(例如,支付)。然而,在本发明的一些实施例中,客户端400和/或交易装置450的确与依赖方451交换一些信息(尽管未必在本文所述的验证或交易确认过程期间交换)。

[0057] 按照惯例,已使用机密诸如即将被装置(例如,PoS交易装置或ATM)获取的个人识别号码(PIN)来实施用户核验。然后,所述装置将创建与依赖方的在线连接以便核验机密,或者将要求用户的验证器(例如,EMV银行卡)核验PIN。这种具体实施有几个缺点。该具体实施可能需要在线连接,但在线连接有时可能可用,但不总是可用。该具体实施还要求用户将长期有效机密输入承受肩窥风险和经受其他攻击的潜在不可信的装置中。另外,该具体实施本质上与特定的用户核验方法(例如,这种情况下的PIN)绑定。最后,该具体实施要求用户记住诸如PIN之类的机密,这对于用户来说可能不方便。

[0058] 本文所述的验证技术允许用户依赖于他/她自身的客户端的验证能力,所以在用户核验方法与安全性方面提供了明显更大的灵活性。具体地讲,在一个实施例中,用户客户端上的移动应用程序在该客户端连接到依赖方的时间期间缓存依赖方提供的验证请求。验证请求可包括与上述的验证请求相同(或相似)的信息(例如,与验证器相关联的随机数和

公共密钥)以及附加信息,该附加信息包括依赖方生成的验证请求(的至少一部分)上的签名、核验密钥和指示验证请求在其内将保持有效的时间段(或相反,验证请求在其之后将过期的时间)的潜在定时数据。在一个实施例中,移动应用程序可缓存多个此类连接请求(例如,针对每个交易装置或交易装置类型有一个请求)。

[0059] 在一个实施例中,在客户端/移动应用程序不能够与依赖方连接的情况下,已缓存的验证请求随后可用于与交易装置进行交易。在一个实施例中,移动应用程序基于已缓存的包含serverData和从交易装置接收的额外数据的验证请求,触发对验证响应的创建。然后将验证响应传输到交易装置,该交易装置随后使用依赖方所提供的核验密钥(例如,在交易装置与依赖方连接的时间期间)来核验该验证响应。具体地讲,交易装置可使用依赖方提供的密钥来核验包含在验证响应中的serverData上的签名。在一个实施例中,依赖方使用私有依赖方核验密钥来生成签名,并且交易装置使用对应的公共依赖方核验密钥(由依赖方向交易装置提供)来核验该签名。

[0060] 一旦交易装置核验完毕从验证响应提取的serverData,然后就可使用从验证请求提取的公共密钥(例如,Uauth.pub)来核验客户端/移动应用程序所生成的验证响应(例如,当客户端直接向依赖方验证时,采用与依赖方进行的上述核验相同或类似的方式)。

[0061] 在下文所述的替代性实施例中,依赖方直接向交易装置(而不是通过客户端装置上的移动应用程序)提供验证请求。在该实施例中,交易装置可以在从客户端上的移动应用程序接收到完成交易的请求时,要求来自依赖方的验证请求。一旦交易装置获得所述验证请求,就可以如上所述验证该请求和验证响应(例如,通过生成签名,并将该签名与现有签名进行比较)。

[0062] 图5A是示出在客户端400缓存验证请求的一个实施例中,客户端400、交易装置450与依赖方之间的交互的事务图。该实施例有时被称为“全离线”实施例,因为其不要求交易装置450具有与依赖方的现有连接。

[0063] 在501处,客户端请求来自依赖方的可缓存验证请求。在502处,依赖方生成可缓存验证请求;在503处,验证请求被发送到客户端;在504处,客户端缓存验证请求。在一个实施例中,验证请求包括与即将用于验证的验证器相关联的公共密钥(Uauth.pub),以及使用依赖方核验密钥(RPVerifyKey)在公共密钥和随机数上生成的签名。如果使用不对称密钥,则依赖方用来生成签名的RPVerifyKey是具有对应的公共RPVerifyKey的私有密钥,依赖方已向交易装置提供该对应的公共RPVerifyKey(可能远在处理用户验证请求之前)。

[0064] 在一个实施例中,验证请求还包括指示验证请求在其间将保持有效的时间长度的定时信息(例如,MaxCacheTime)。在该实施例中,可缓存验证请求的签名可通过公共验证密钥、随机数与MaxCacheTime的组合来生成(例如,ServerData=Uauth.pub|MaxCacheTime|serverNonce|Sign(RPVerifyKey,Uauth.pub|MaxCacheTime|serverNonce))。在一个实施例中,验证响应包括不止一个验证密钥(例如,针对能够验证用户的每个验证器有一个验证密钥),并且可通过所有这些密钥(例如,连同随机数和MaxCacheTime一起)生成签名。

[0065] 如所提及的,交易装置450或旨在执行验证请求/响应的离线核验的任何装置需要知道公共RPVerifyKey。该扩展是必需的,因为交易装置完全不清楚在依赖方处注册的验证密钥(即,用户装置与交易装置之间未建立任何关系)。因此,依赖方必须以安全的方式向交易装置(或其他装置)传送有关哪些密钥即将用于验证响应核验的信息。交易装置将核验

MaxCacheTime,以确定已缓存的验证请求是否依然有效(以便遵守依赖方的有关已缓存的验证请求可使用多长时间的策略)。

[0066] 在505处,客户端建立与交易装置的安全连接并发起交易。例如,如果交易装置是PoS交易装置,则交易可涉及借记或信贷交易。如果交易装置是ATM,则交易可涉及现金提取或维护任务。本发明的基本原理不限于任何特定类型的交易装置或安全连接。另外,在505处,客户端可将已缓存的验证请求传输到交易装置。

[0067] 作为响应,在506处,交易装置可传输装置身份信息(例如,交易装置识别代码)、随机质询(随机数)以及任选地,以定义的语法完成交易的交易文本。然后,随机质询/随机数将被加密地绑定到验证响应。该机制允许装置核验用户核验是新生成的,尚未被缓存/重复使用。

[0068] 为了支持诸如上述的交易确认(例如,参见图3A和图3B以及相关联文本),可能需要交易装置创建交易的标准化且人可读的表示。如本文所用,“标准化”意指能够由依赖方解析(例如,用于如下述操作511中所指示的最终核验)并且/或者能够由交易装置解析的格式。该格式需要是人可读的,因为交易确认要求验证器在客户端400的安全显示器上显示这些交易确认。这种编码的例子可为XML,此时XSLT用于可视化。

[0069] 在507处,为了生成验证响应,显示验证用户界面,用于指导用户使用特定的验证器在客户端上执行验证(例如,在指纹传感器上轻扫手指、输入PIN码、对着麦克风说话,等等)。一旦用户提供验证,客户端上的验证引擎就核验用户的身份(例如,将从用户收集的验证数据与存储在验证器的安全存储装置中的用户核验参考数据进行比较),并使用与验证装置相关联的私有密钥在随机质询上(可能还在交易装置ID和/或交易文本上)加密并/或生成签名。然后在508处,将验证响应传输到交易装置。

[0070] 在509处,如果所述验证引擎尚未将验证响应传输到交易装置,交易装置就使用公共RPVerifyKey来核验serverData(在505处接收)上的签名。一旦serverData得到核验,交易装置便知道与用于执行验证的验证器相关联的公共密钥(Uauth.pub)。交易装置使用该密钥来核验所述验证响应。例如,交易装置可使用公共验证密钥来解密或核验在随机数和任何其他相关信息(例如,交易文本、交易装置ID等)上生成的签名。如果交易装置执行了交易确认,则在508处,该交易装置可通过验证在交易文本上生成并且包含在验证响应中的签名来核验客户端上显示的交易文本。代替具有加密安全的serverData结构,交易装置还可使用与依赖方的在线连接(如果该连接可用(半离线情况))来核验未签名的serverData。

[0071] 在510处,取决于验证是成功还是失败,分别向客户端发送成功指示或失败指示。如果成功,则交易装置将允许交易(例如,记入帐户的借方/贷方来完成购买、支付现金、执行管理任务等)。如果失败,则交易装置将不允许交易并且/或者请求额外验证。

[0072] 如果存在与依赖方的连接,则在511处,交易装置可传输对依赖方的验证响应和/或交易文本(假定依赖方是负责核验交易文本的实体)。可在依赖方处记录交易的记录,并且/或者依赖方可核验交易文本并确认交易(未示出)。

[0073] 图5B是示出在交易装置具有与依赖方的连接并且从依赖方接收验证请求的一个实施例中,客户端400、交易装置450与依赖方之间的交互的事务图。该实施例有时被称为“半离线”实施例,因为尽管客户端未连接到依赖方,但交易装置450与依赖方连接。

[0074] 在521处,客户端发起交易,从而建立与交易装置的安全连接(例如,NFC、蓝牙等)。

在522处，交易装置作出响应，要求来自依赖方的验证请求。在523处，依赖方生成验证请求，然后在524处，将验证请求发送到交易装置。如在图5A所示的实施例中，验证请求可包括与客户端上即将用于验证的验证器相关联的公共密钥(Uauth.pub)，以及使用依赖方核验密钥(RPVerifyKey)在公共密钥和随机数上生成的签名。如果使用不对称密钥，则依赖方用来生成签名的RPVerifyKey是具有对应的公共RPVerifyKey的私有密钥，依赖方向交易装置提供该对应的公共RPVerifyKey(可能远在处理用户验证请求之前)。代替具有加密安全的serverData结构，交易装置还可使用与依赖方的在线连接(如果该连接可用(半离线情况))来核验未签名的serverData。

[0075] 在一个实施例中，serverData还包括指示验证请求在其间将保持有效的时间长度的定时信息(例如，MaxCacheTime)。在该实施例中，serverData的签名可通过公共验证密钥、随机数与MaxCacheTime的组合来生成(例如，ServerData＝Uauth.pub|MaxCacheTime|serverNonce|Sign(RPVerifyKey,Uauth.pub|MaxCacheTime|serverNonce))。在一个实施例中，验证响应包括不止一个验证密钥(例如，针对每个验证器有一个验证密钥)，并且可通过所有这些密钥(例如，连同随机数和MaxCacheTime一起)生成签名。

[0076] 在一个实施例中，图5B中的事务图的剩余部分基本上如图5A中所示那样操作。在525处，交易装置可传输身份信息(例如，交易装置识别代码)、随机质询(随机数)以及任选地，以定义的语法完成交易的交易文本。然后，随机质询/随机数将被加密地绑定到验证响应。该机制允许装置核验用户核验是新生成的，尚未被缓存。

[0077] 为了支持诸如上述的交易确认(例如，参见图3A和图3B以及相关联文本)，可能需要交易装置创建交易的标准化且人可读的表示。如本文所用，“标准化”意指能够由依赖方解析(例如，用于如下述操作511中所指示的最终核验)并且/或者能够由交易装置解析的格式。该格式需要是人可读的，因为交易确认要求验证器在客户端400的安全显示器上显示这些交易确认。这种编码的例子可为XML，此时XSLT用于可视化。

[0078] 在526处，为了生成验证响应，显示验证用户界面，用于指导用户使用特定的验证器在客户端上执行验证(例如，在指纹传感器上轻扫手指、输入PIN码、对着麦克风说话，等等)。一旦用户提供验证，客户端上的验证引擎就核验用户的身份(例如，将从用户收集的验证数据与存储在验证器的安全存储装置中的用户核验参考数据进行比较)，并使用与验证装置相关联的私有密钥在随机质询上(可能还在交易装置ID和/或交易文本上)加密并/或生成签名。然后在527处，将验证响应传输到交易装置。

[0079] 在528处，如果所述验证引擎尚未将验证响应传输到交易装置，交易装置就使用公共RPVerifyKey来核验serverData(在524处接收)上的签名。一旦serverData得到核验，交易装置便知道与用于执行验证的验证器相关联的公共密钥(Uauth.pub)。交易装置使用该密钥来核验所述验证响应。例如，交易装置可使用公共验证密钥来解密或核验在随机数和任何其他相关信息(例如，交易文本、交易装置ID等)上生成的签名。如果交易装置执行了交易确认，则在528处，该交易装置可通过验证在交易文本上生成并且包含在验证响应中的签名来核验客户端上显示的交易文本。代替具有加密安全的serverData结构，交易装置还可使用与依赖方的在线连接(如果该连接可用(半离线情况))来核验未签名的serverData。

[0080] 在529处，取决于验证是成功还是失败，分别向客户端发送成功指示或失败指示。如果成功，则交易装置将允许交易(例如，记入帐户的借方/贷方来完成购买、支付现金、执

行管理任务等)。如果失败,则交易装置将不允许交易并且/或者请求额外验证。

[0081] 在530处,交易装置可传输对依赖方的验证响应和/或交易文本(假定依赖方是负责核验交易文本的实体)。可在依赖方处记录交易的记录,并且/或者依赖方可核验交易文本并确认交易(未示出)。

[0082] 如图6所示,在一个实施例中,在客户端上执行移动应用程序601,以结合验证客户端602(其可以是图2B中所示的安全交易服务201和接口202)来执行本文所述的操作。具体地讲,移动应用程序601可使用传输层安全(TLS)协议或其他安全通信协议,来打开到交易装置450上执行的web应用程序611的安全信道。交易装置上的web服务器612还可打开安全信道来与依赖方451通信(例如,以便如上所述那样检索验证请求并且/或者向依赖方451提供更新)。验证客户端602可直接与依赖方451通信,以例如检索可缓存的验证请求(如上文详细讨论的那样)。

[0083] 在一个实施例中,验证客户端602可识别依赖方和具有“AppID”的任何经授权的移动应用程序601,其中“AppID”是与依赖方可用的每个应用程序相关联的唯一代码。在依赖方提供多种在线服务的一些实施例中,用户在单个依赖方可拥有多个AppID(依赖方为每种服务提供一个AppID)。

[0084] 在一个实施例中,通过AppID识别的任何应用程序可具有识别用于与依赖方连接的允许机制和/或应用程序类型的多个“方面(facet)”。例如,特定依赖方可允许经由Web服务并且经由不同的特定于平台的移动应用程序(例如,Android应用程序、iOS应用程序等)进行访问。这些项中的每一个可使用不同的“FacetID”来识别,如图所示,依赖方可向验证引擎提供该“FacetID”。

[0085] 在一个实施例中,调用移动应用程序601将其AppID传递到验证客户端602所暴露的API。在每个平台上,验证客户端602识别调用应用程序601,并确定其FacetID。然后,该验证客户端解析AppID,并且检查该FacetID是否包含在依赖方451提供的TrustedApp列表中。

[0086] 在一个实施例中,可使用诸如图7和图8中所示的不记名令牌来实施上文所述的可缓存验证请求。在本文所述的本发明的实施例中,令牌接收方(交易装置450)需要能够在不要求与令牌发布方(依赖方)建立另一个“在线”连接的情况下,对令牌、验证响应以及令牌与验证响应的绑定进行核验。

[0087] 应当区分两类不记名令牌:

[0088] 1。只能由接收方(例如,交易装置450)使用到发布方(例如,依赖方451)的不同信道来核验的令牌,令牌发布与令牌核验之间必须存在这类令牌。这类令牌在本文中被称为“未签名令牌”。

[0089] 2。由于其具有加密结构(例如,因为其包含下述数字签名)而能够被接收方核验的令牌,该数字签名能够使用从令牌发布方接收的数据来核验(这种方式适合在特定令牌发布之前使用)。这类令牌在本文中被称为“已签名令牌”。

[0090] 术语“已签名令牌结构”在本文中用来指包含Uauth.pub密钥的已签名令牌和包含该令牌的已签名结构这两者。

[0091] 将已签名令牌绑定到验证密钥

[0092] 如图7所示,在一个实施例中,为了将已签名令牌绑定到验证密钥,令牌发布方(例如,依赖方451):(a)将验证公共密钥(Uauth.pub)702添加到(待)签名令牌的待签名部分

701;以及(b)将该已签名令牌加入验证响应的待签名部分。通过此操作,令牌接收方(例如,交易装置450)能够通过验证签名703(例如,上文所述的公共RPVerifyKey)来核验令牌。如果核验成功,则如前讨论的,令牌接收方能够提取公共密钥(Uauth.pub),并使用该公共密钥来核验所述验证响应。

[0093] 将未签名令牌绑定到验证密钥

[0094] 如图8所示,为了将未签名令牌802绑定到验证密钥,在一个实施例中,令牌发布方(例如,依赖方451)创建(至少)覆盖原始令牌802和待签名数据801(包括验证公共密钥(Uauth.pub))的已签名结构。能够通过使用与私有签名密钥相关的公共密钥(例如,上文所述的RPVerifyKey对)来验证签名803,从而核验所述已签名结构。需要与令牌接收方(例如,交易装置450)共享该公共签名密钥。能够在生成签名密钥对之后进行一次共享,这种方式适合在生成第一已签名结构之前使用。

[0095] 本文所述的技术既支持"全离线"具体实施(即,交易装置450在交易时未连接到依赖方451),又支持"半离线"具体实施(即,交易装置在交易时连接到依赖方451,但客户端未连接到该依赖方)。

[0096] 甚至在全离线的情况下,仍期望交易装置450经由主机不时地连接到依赖方451。例如,主机可收集存储在交易装置450中的所有响应以便将其发送到依赖方,还可更新(如果需要的话)已撤销Uauth密钥(例如,自最后一次连接以来已经撤销的公共验证密钥)的列表。

[0097] 一些实施例还支持纯(会话)验证以及交易确认。甚至在交易确认的情况下,如果交易装置450将交易文本连同验证响应一起提交到依赖方451,则依赖方451能够核验交易。

[0098] 本文所述的技术有几个不同的使用案例/应用。例如:

[0099] 1。支付用户已经向支付服务提供商(PSP)注册了他/她的验证器(例如,智能电话)。用户想要使用得到PSP授权的销售点装置(PoS),在某些商家处验证支付,但该PoS未与PSP建立可靠而永久的在线连接(例如,在公交车中)。在该例子中,PoS可被实施为交易装置450,PSP可被实施为上文所述的依赖方451,从而在尽管没有可靠而永久的连接的情况下,也允许进行交易。

[0100] 2。物联网公司已经安装几个嵌入式装置(例如,在工厂、建筑物等中)。此类装置的维护由签约方雇用的技术人员执行。为执行维护,技术人员必须向装置验证,以便证明他/她有执行该项任务的资格。作了如下一些假定(基于实际的框架条件):

[0101] a。技术人员无法向每个此类装置执行注册(因为此类装置过多)。

[0102] b。由于技术人员为数众多、此类技术人员的变动也相当大,所以无法保证每个装置上的合格技术人员列表始终是最新的。

[0103] c。在维护时,所述装置和技术人员的计算机都没有可靠的网络连接。

[0104] 使用上文所述的技术,公司能够一次(例如,在安装时)将信任锚(例如,公共RPVerifyKey)注入所有装置中。然后,每个技术人员向签约方(例如,依赖方451,其可为技术人员的雇主)注册。使用以上技术,技术人员将能够向每个装置验证。

[0105] 上文所述的本发明的实施例可以在任何系统中实施,在该系统中,具有验证能力的客户端向依赖方注册,并且在该客户端与装置之间执行验证操作,所述装置(a)代表依赖方起作用,并且(b)在交易时处于离线状态(即,未与客户端已经向其注册的依赖方原始服

务器建立可靠的网络连接)。在这种情况下,客户端从原始服务器接收可缓存的验证请求并缓存该验证请求。一旦需要验证响应,客户端便计算验证响应并且将其发送到装置。

[0106] 在另一个实施例中,客户端以加密安全方式将(在验证请求中接收的)信道绑定数据添加到所述响应。通过此操作,依赖方的原始服务器能够核验该请求已被合法客户端(而不是某个中间人)接收。

[0107] 在一个实施例中,依赖方将额外的已验证数据添加到所述响应,所述已验证数据诸如Uauth.pub密钥(其允许装置核验该验证或交易确认响应),而不必联系依赖方服务器以检索已批准的Uauth.pub密钥。在另一个实施例中,依赖方要求客户端的用户先成功地执行验证,再发布"可缓存"验证请求(以防出现拒绝服务攻击)。在一个实施例中,依赖方要求客户端指出,需要的请求是可缓存的还是不可缓存的。如果是可缓存的,则依赖方可能需要所述响应中额外的验证数据(例如,上文所述的MaxCacheTime)。

[0108] 在一个实施例中,装置(诸如交易装置450)未与依赖方建立直接的网络连接,而是使用单独的计算机(在本文中有时称为"主机")来与依赖方"同步"。该主机检索从装置收集的所有验证响应,并且将其转移到依赖方。另外,主机还可将已撤销Uauth密钥的列表复制到装置,以确保验证响应中不使用任一个已撤销密钥。

[0109] 在一个实施例中,装置(诸如交易装置450)向客户端发送随机值(例如,随机数),然后客户端以加密方式添加该随机值,作为对验证响应的扩展(在对该验证响应进行签名之前)。该已签名随机值用来证明装置的新鲜度。

[0110] 在一个实施例中,客户端的验证器添加当前时间Ta,作为对验证响应的扩展(在对该验证响应进行签名之前)。所述装置/交易装置可将该时间与当前时间Td进行比较,只在Ta与Td之间的差值可接受时(例如,在该差值小于两分钟(abs(Td-Ta)<2min)的情况下)接受该响应。

[0111] 在一个实施例中,依赖方向可缓存请求添加已验证的(即,已签名的)截止时间。如上所述,所述装置/交易装置只有在截止时间之前接收到所述响应时,才会接受该响应并将其视作有效的。

[0112] 在一个实施例中,依赖方向可缓存请求添加已验证的(即,已签名的)数据块(例如,上文提及的"已签名令牌结构"),该数据块包括额外信息,诸如(但不限于)公共密钥、截止时间、最大交易值(例如,安全断言标记语言(SAML)断言、OAuth令牌、JSON Web签名(JWS)对象等)。所述装置/交易装置只有在已签名的数据块能够被核验为有效并且内容可接受的情况下,才可接受该响应并将其视作有效的。

[0113] 在一个实施例中,依赖方只将未签名令牌添加到可缓存验证请求,但交易装置在交易时具有与依赖方的在线连接。交易装置在交易时使用与依赖方的在线连接来核验未签名令牌的真实性。

[0114] 图9示出了根据本发明的一个实施例的示例性"离线"和"半离线"验证场景。在该实施例中,拥有计算装置910的用户已经与依赖方930建立关系,并且可向依赖方验证。然而,在一些情况下,用户想要与已经与依赖方930建立关系、但未必已经与用户的计算装置910建立关系的装置970执行交易(例如,验证交易确认)。就该实施例而言,如果连接920和连接921在相关时间(例如,用户的计算装置910向装置970验证的时间,或者用户的计算装置910与装置970之间进行交易的时间)不存在或不稳定,则该交易被称为"全离线"。就该实

施例而言，如果用户的计算装置910与依赖方930之间的连接920不稳定，但装置970与依赖方930之间的连接921是稳定的，则该交易被称为“半离线”。需注意，在该实施例中，要求用户的计算装置910与装置970之间的连接922在相关时间是稳定的。还期望验证器连接到用户的计算装置910。连接922可使用任何类型的通信信道/协议来实施，包括但不限于：蓝牙、蓝牙低功耗(BTLE)、近场通信(NFC)、Wifi、全球移动通信系统(GSM)、通用移动通信系统(UTMS)、长期演进(LTE)(例如，4G LTE)与TCP/IP。

[0115] 示例性数据处理装置

[0116] 图10是示出可在本发明的一些实施例中使用的示例性客户端和服务器的框图。应当理解，尽管图10示出计算机系统的各种组件，但其并非意图表示互连组件的任何特定架构或方式，因为此类细节与本发明并不密切相关。应当理解，具有更少组件或更多组件的其他计算机系统也可与本发明一起使用。

[0117] 如图10所示，计算机系统1000，其为一种形式的数据处理系统，包括总线1050，该总线与处理系统1020、电源1025、存储器1030和非易失性存储器1040(例如，硬盘驱动器、快闪存储器、相变存储器(PCM)等)耦接。总线1050可通过如本领域中熟知的各种桥接器、控制器和/或适配器来彼此连接。处理系统1020可从存储器1030和/或非易失性存储器1040检索指令，并执行这些指令以执行如上所述的操作。总线1050将以上组件互连在一起，并且还将那些组件互连到可选底座1060、显示控制器与显示装置1070、输入/输出装置1080(例如，NIC(网络接口卡)、光标控件(例如，鼠标、触摸屏、触摸板等)、键盘等)和可选无线收发器1090(例如，蓝牙、WiFi、红外等)。

[0118] 图11是示出可在本发明的一些实施例中使用的示例性数据处理系统的框图。例如，数据处理系统190可为手持式计算机、个人数字助理(PDA)、移动电话、便携式游戏系统、便携式媒体播放器、平板计算机或手持式计算装置(其可包括移动电话、媒体播放器和/或游戏系统)。又如，数据处理系统1100可为网络计算机或在另一个装置内的嵌入式处理装置。

[0119] 根据本发明的一个实施例，数据处理系统1100的示例性架构可用于上文所述的移动装置。数据处理系统1100包括处理系统1120，其可包括一个或多个微处理器和/或集成电路上的系统。处理系统1120与存储器1110、电源1125(其包括一个或多个电池)、音频输入/输出1140、显示控制器与显示装置1160、可选输入/输出1150、输入装置1170和无线收发器1130耦接。应当理解，在本发明的某些实施例中，图11中未示出的其他组件也可为数据处理系统1100的一部分，并且在本发明的某些实施例中，可使用比图11所示更少的组件。另外，应当理解，图11中未示出的一个或多个总线可用于使如本领域中熟知的各种组件互连。

[0120] 存储器1110可存储数据和/或程序以供数据处理系统1100执行。音频输入/输出1140可包括麦克风和/或扬声器以(例如)播放音乐，以及/或者通过扬声器和麦克风提供电话功能。显示控制器与显示装置1160可包括图形用户界面(GUI)。无线(例如，RF)收发器1130(例如，WiFi收发器、红外收发器、蓝牙收发器、无线蜂窝电话收发器等)可用于与其他数据处理系统通信。所述一个或多个输入装置1170允许用户向系统提供输入。这些输入装置可为小键盘、键盘、触控面板、多点触控面板等。可选的其他输入/输出1150可为底座的连接器。

[0121] 本发明的实施例可包括如上文陈述的各种步骤。这些步骤可体现为致使通用处理

器或专用处理器执行某些步骤的机器可执行指令。或者，这些步骤可由包含用于执行这些步骤的硬连线逻辑的特定硬件组件执行，或由编程的计算机组件和定制硬件组件的任何组合执行。

[0122] 本发明的元件还可被提供为用于存储机器可执行程序代码的机器可读介质。机器可读介质可包括但不限于软盘、光盘、CD-ROM和磁光盘、ROM、RAM、EPROM、EEPROM、磁卡或光卡、或者适合于存储电子程序代码的其他类型的介质/机器可读介质。

[0123] 在整个前述描述中，出于解释的目的，陈述了许多特定细节以便透彻理解本发明。然而，本领域的技术人员将容易明白，可在没有这些特定细节中的一些的情况下实践本发明。例如，本领域的技术人员将容易明白，本文所述的功能模块和方法可被实施为软件、硬件或其任何组合。此外，虽然本文在移动计算环境的情形内描述本发明的一些实施例，但本发明的基本原理不限于移动计算具体实施。在一些实施例中，可使用几乎任何类型的客户端或对等数据处理装置，包括(例如)台式计算机或工作站计算机。因此，应依据所附权利要求书确定本发明的范围和精神。

[0124] 本发明的实施例可包括如上文陈述的各种步骤。这些步骤可体现为致使通用处理器或专用处理器执行某些步骤的机器可执行指令。或者，这些步骤可由包含用于执行这些步骤的硬连线逻辑的特定硬件组件执行，或由编程的计算机组件和定制硬件组件的任何组合执行。

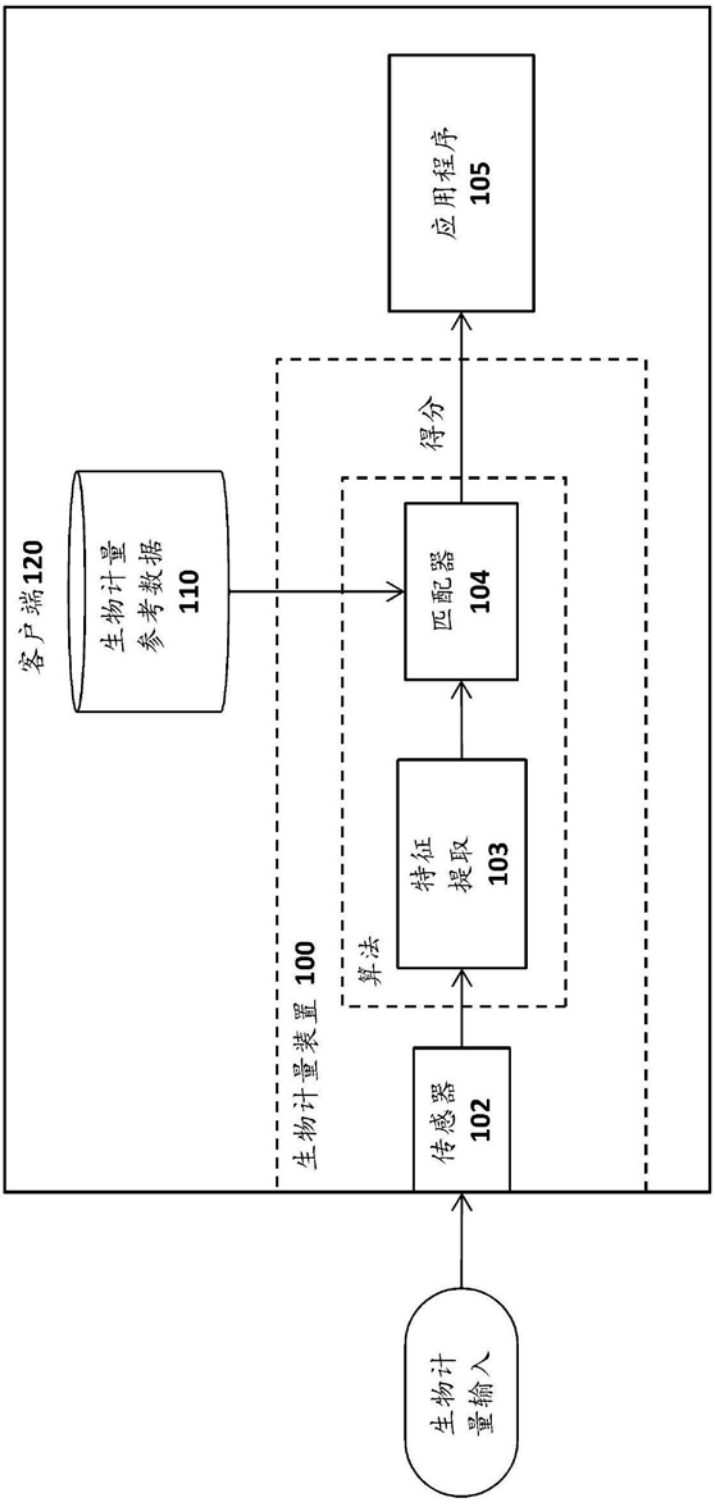

应用程序
105
得分
客户端120
生物计量
参考数据
110
匹配器
104
特征
提取
103
算法
生物计量装置 100
传感器
102
生物计
量输入

图1

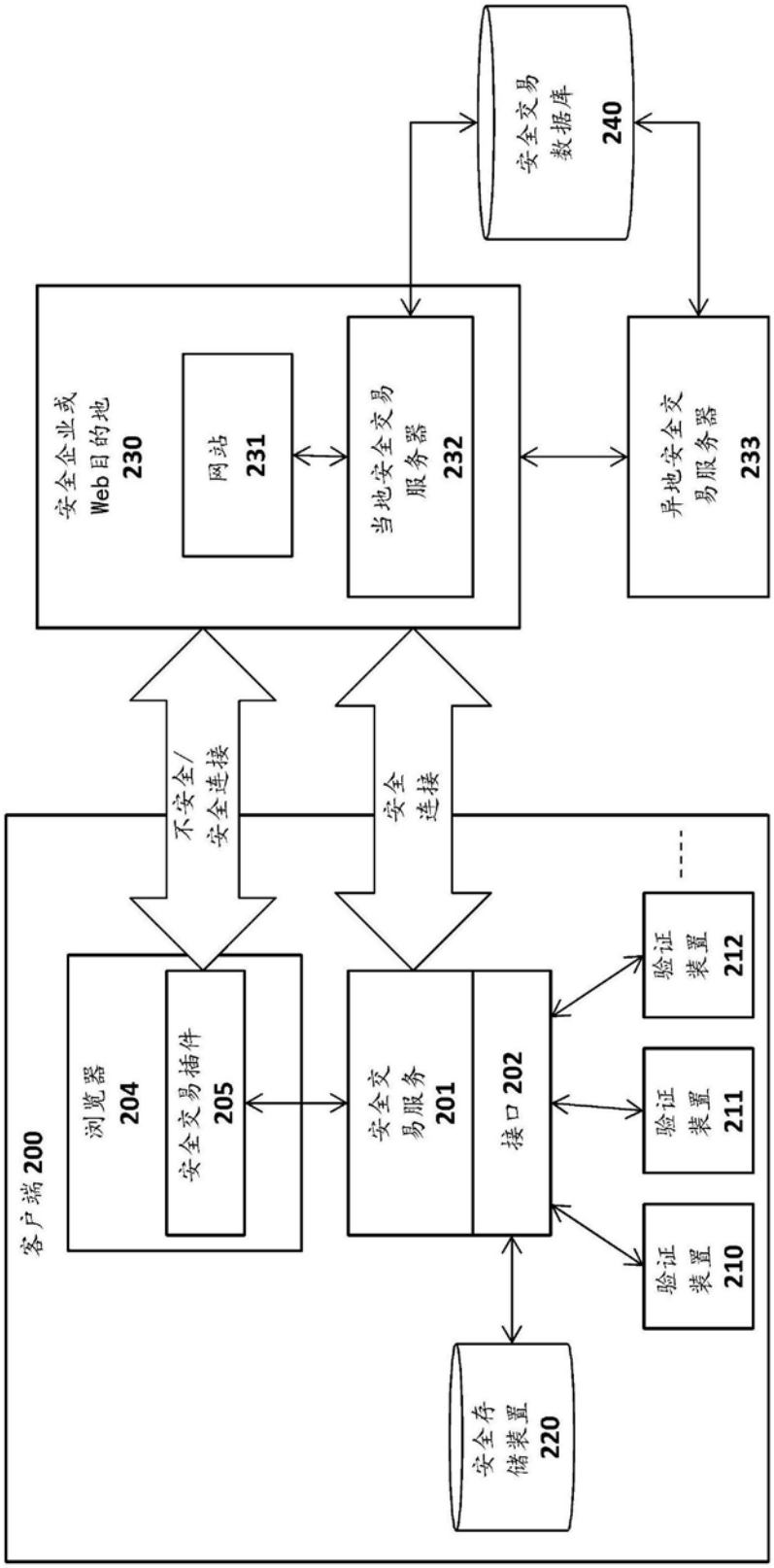

安全交易数据库 240
安全企业或Web目的地 230
网站 231
当地安全交易服务器 232
异地安全交易服务器 233
不安全/安全连接
安全连接
客户端 200
浏览器 204
安全交易插件 205
安全交易服务 201
接口 202
验证装置 212
验证装置 211
验证装置 210
安全存储装置 220

图2A

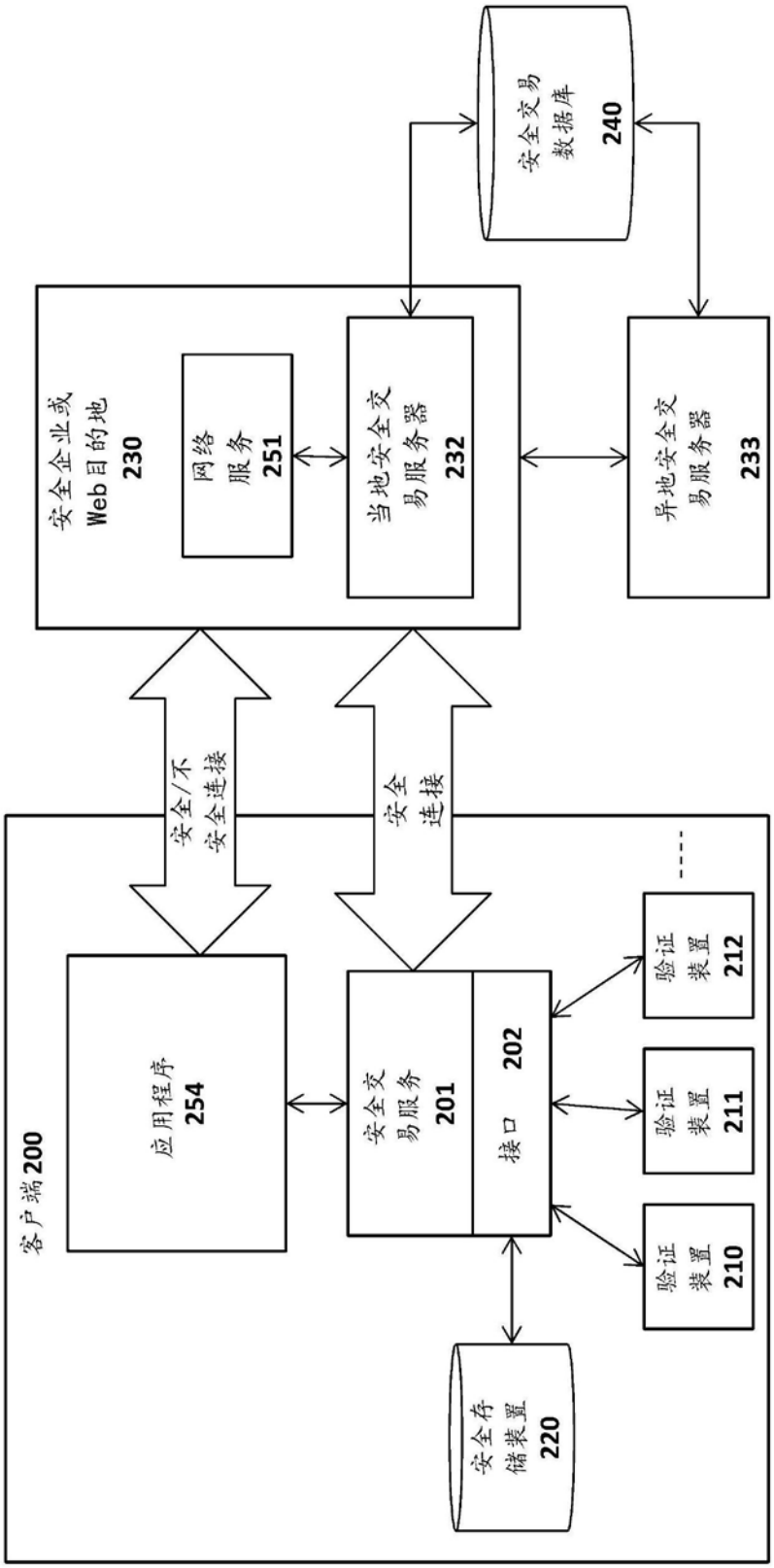

安全交易数据库 240
安全企业或Web目的地 230
网络服务 251
当地安全交易服务器 232
异地安全交易服务器 233
安全/不安全连接
安全连接
客户端 200
应用程序 254
安全交易服务 201
接口 202
验证装置 212
验证装置 211
验证装置 210
安全存储装置 220

图2B

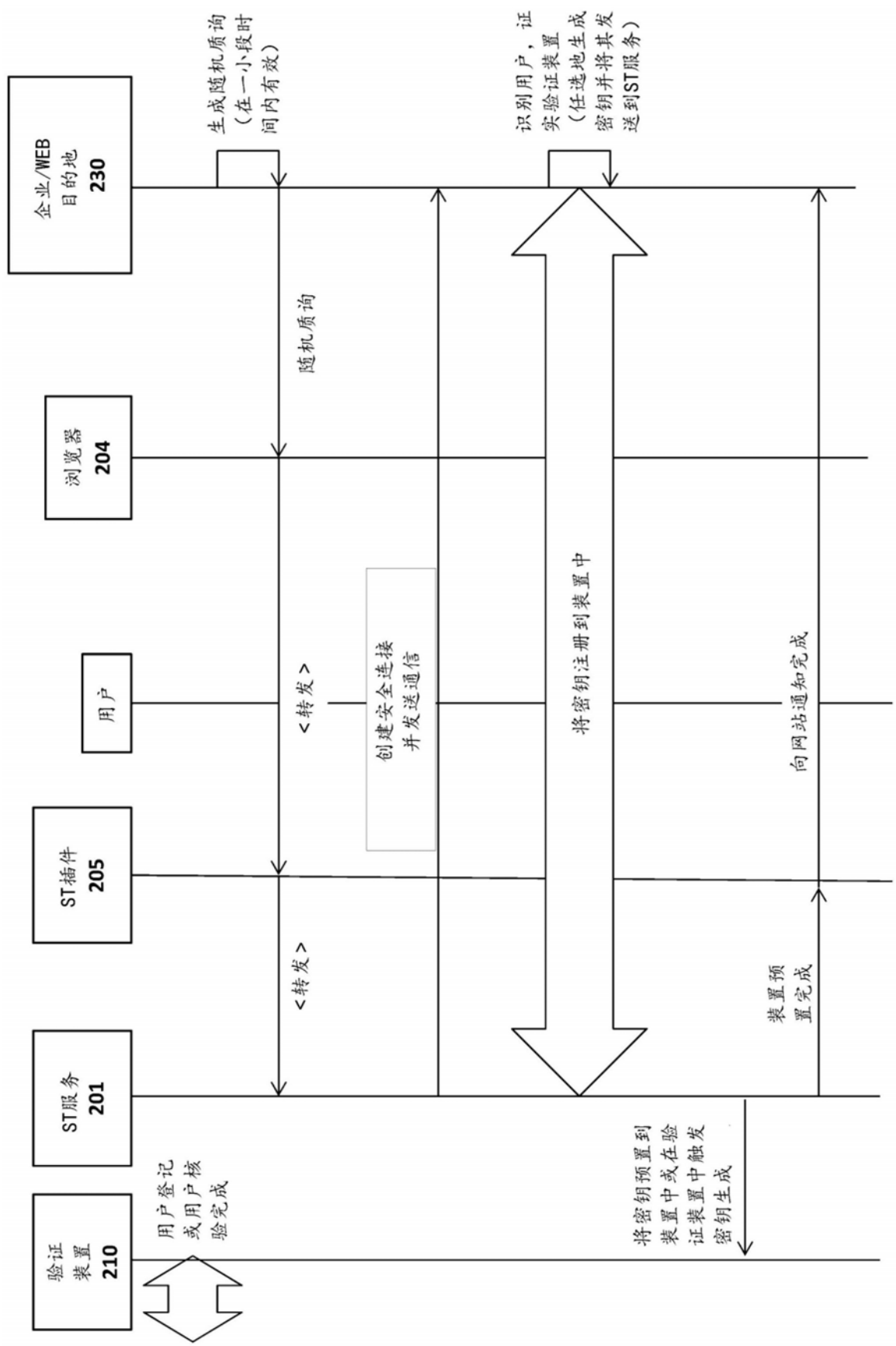

企业/WEB
目的地
230
浏览器
204
用户
ST插件
205
ST服务
201
验证
装置
210
生成随机质询
（在一小段时
间内有效）
随机质询
<转发>
<转发>
创建安全连接
并发送通信
识别用户，证
实验证装置
（任选地生成
密钥并将其发
送到ST服务）
将密钥注册到装置中
向网站通知完成
装置预
置完成
用户登记
或用户核
验完成
将密钥预置到
装置中或在验
证装置中触发
密钥生成

图2C

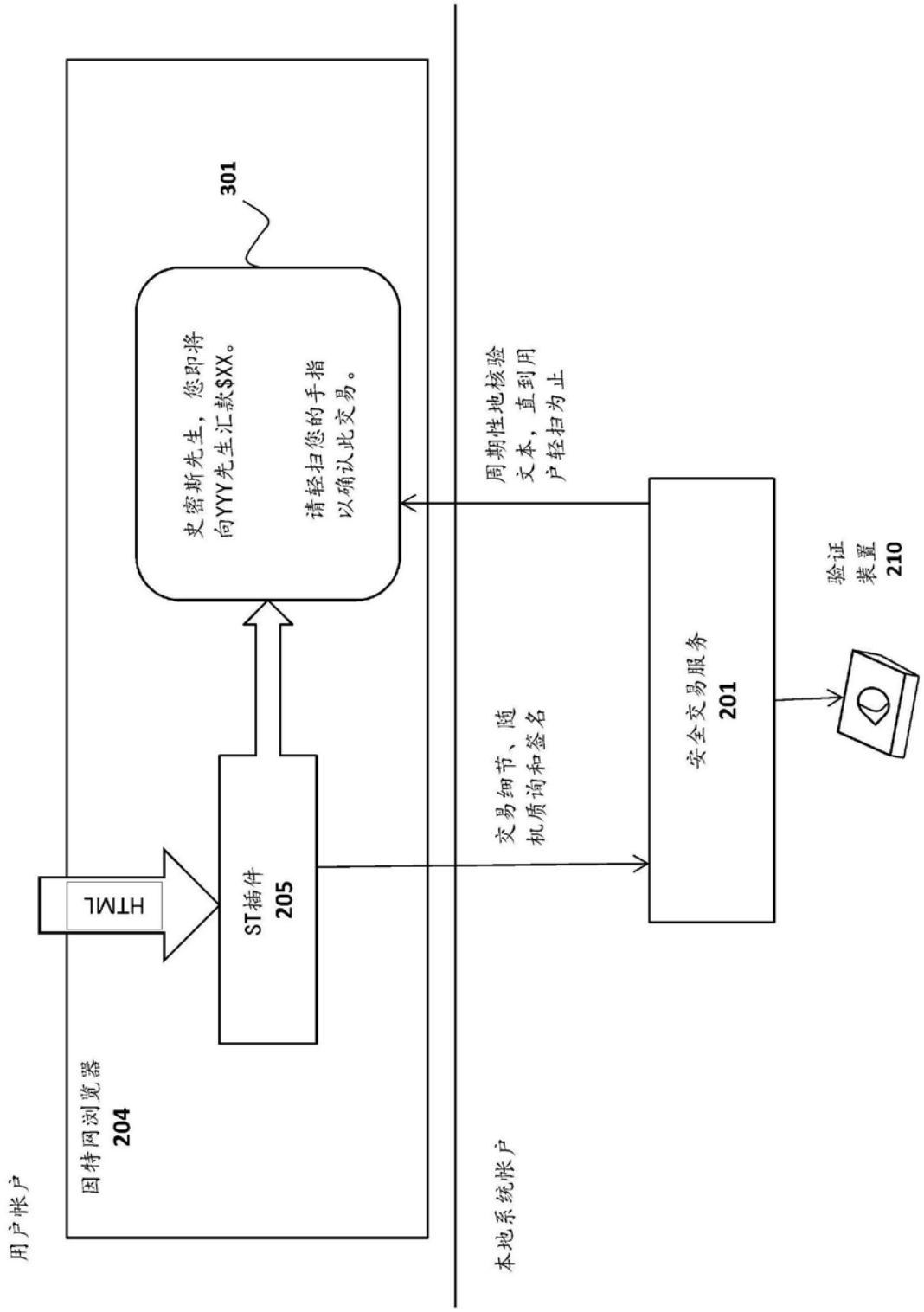

用户帐户
固特网浏览器
204
HTML
ST插件
205
301
史密斯先生，您即将
向YYY先生汇款$XX。
请轻扫您的手指
以确认此交易。
交易细节、随
机质询和签名
本地系统帐户
周期性地核验
文本，直到用
户轻扫为止
安全交易服务
201
验证
装置
210

图3A

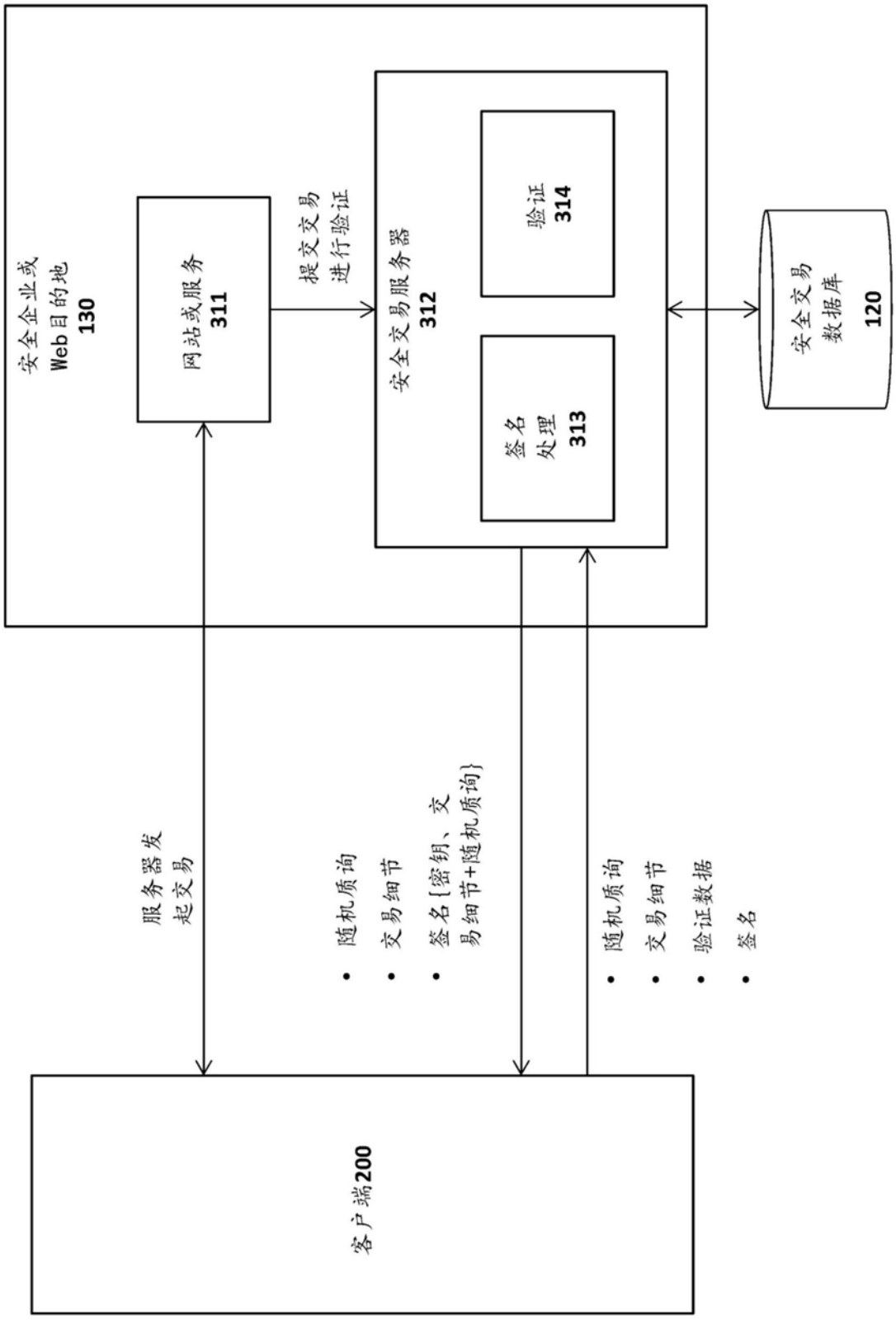

安全企业或
Web目的地
130
网站或服务
311
提交交易
进行验证
安全交易服务器
312
验证
314
签名
处理
313
安全交易
数据库
120
服务器发
起交易
• 随机质询
• 交易细节
• 签名{密钥、交
易细节+随机质询}
• 随机质询
• 交易细节
• 验证数据
• 签名
客户端200

图3B

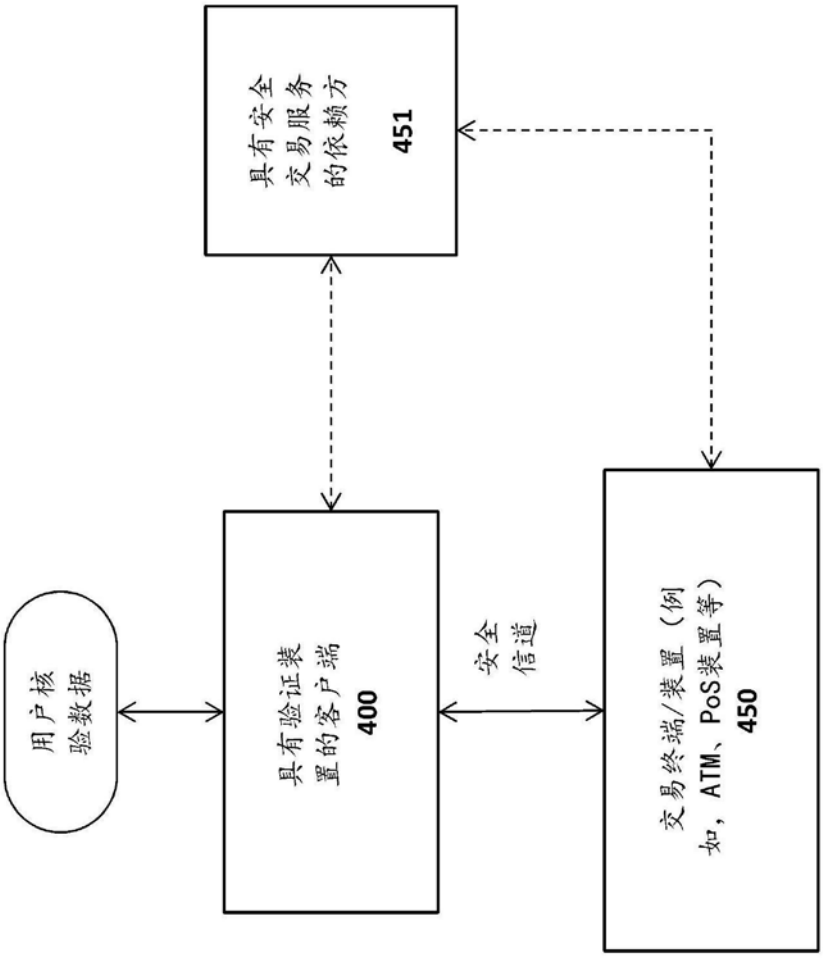

具有安全交易服务的依赖方
451
具有验证装置的客户端
400
用户核验数据
安全信道
交易终端/装置（例如，ATM、PoS装置等）
450

图4

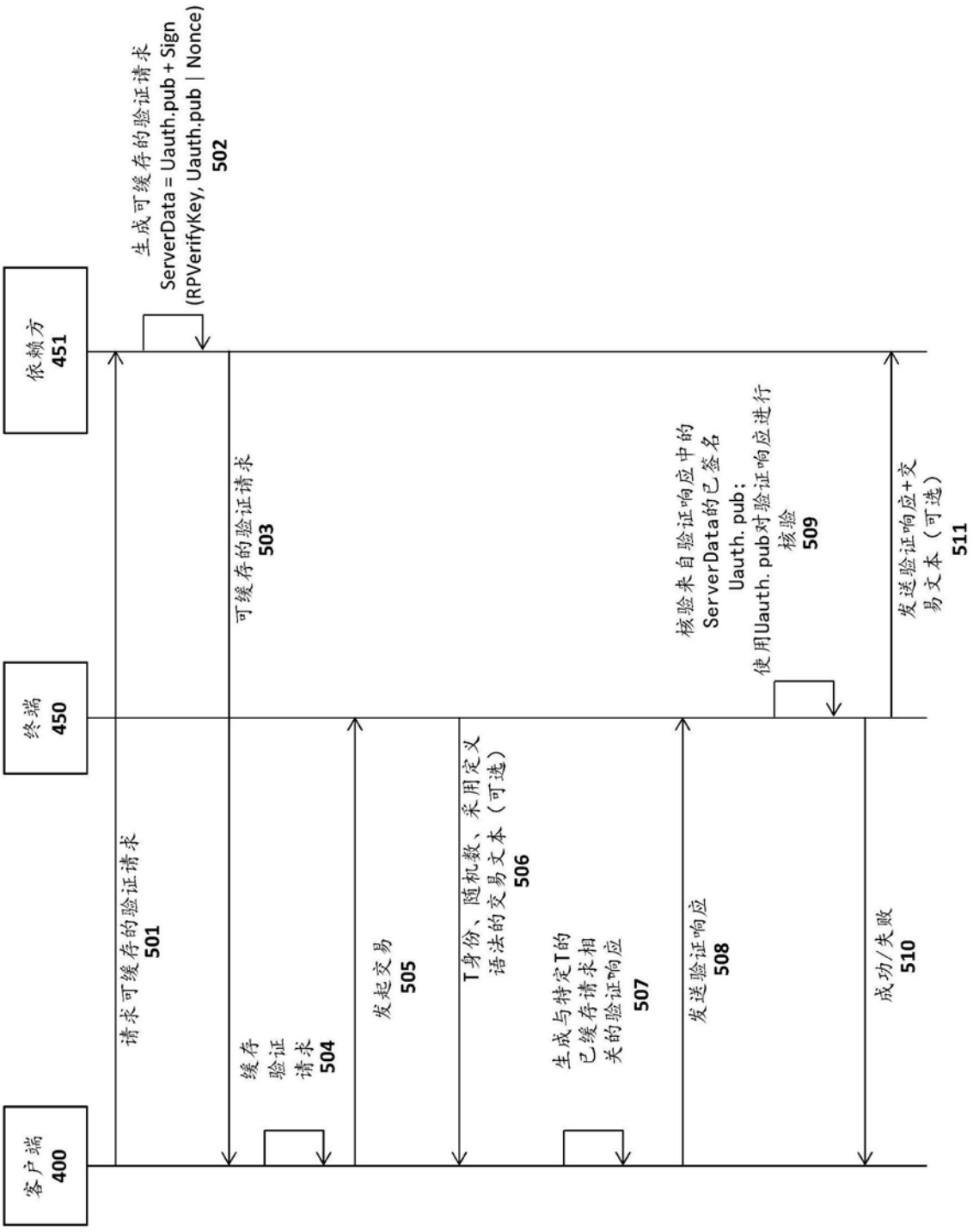

客户端
400
终端
450
依赖方
451
请求可缓存的验证请求
501
生成可缓存的验证请求
ServerData = Uauth.pub + Sign
(RPVerifyKey, Uauth.pub | Nonce)
502
可缓存的验证请求
503
缓存
验证
请求
504
发起交易
505
T身份、随机数、采用定义
语法的交易文本（可选）
506
生成与特定T的
已缓存请求相
关的验证响应
507
发送验证响应
508
核验来自验证响应中的
ServerData的已签名
Uauth. pub；
使用Uauth. pub对验证响应进行
核验
509
成功/失败
510
发送验证响应+交
易文本（可选）
511

图5A

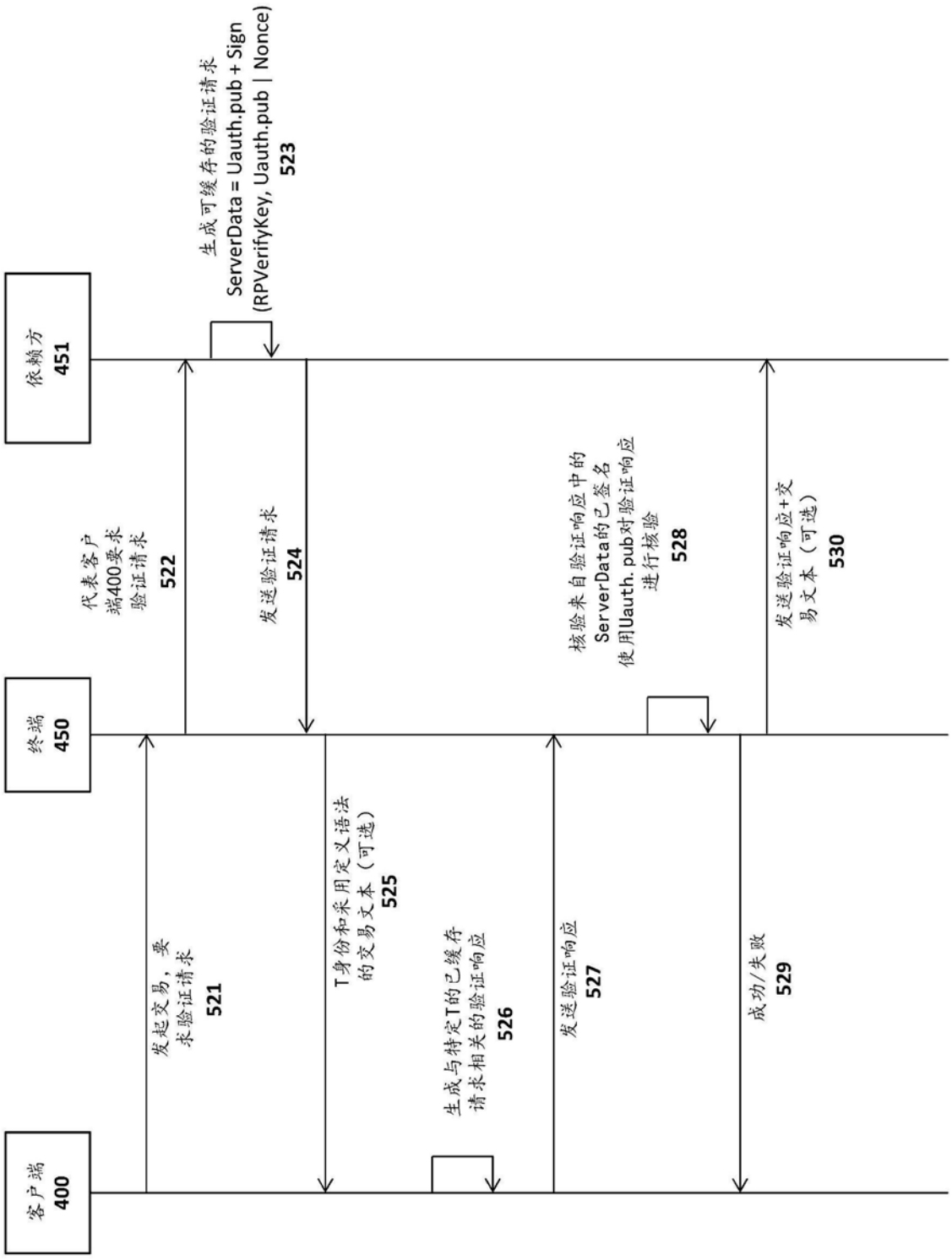

客户端
400
终端
450
依赖方
451
发起交易，要求验证请求
521
代表客户端400要求验证请求
522
生成可缓存的验证请求
ServerData = Uauth.pub + Sign
(RPVerifyKey, Uauth.pub | Nonce)
523
发送验证请求
524
T身份和采用定义语法的交易文本（可选）
525
生成与特定T的已缓存请求相关的验证响应
526
发送验证响应
527
核验来自验证响应中的ServerData的已签名使用Uauth.pub对验证响应进行核验
528
成功/失败
529
发送验证响应+交易文本（可选）
530

图5B

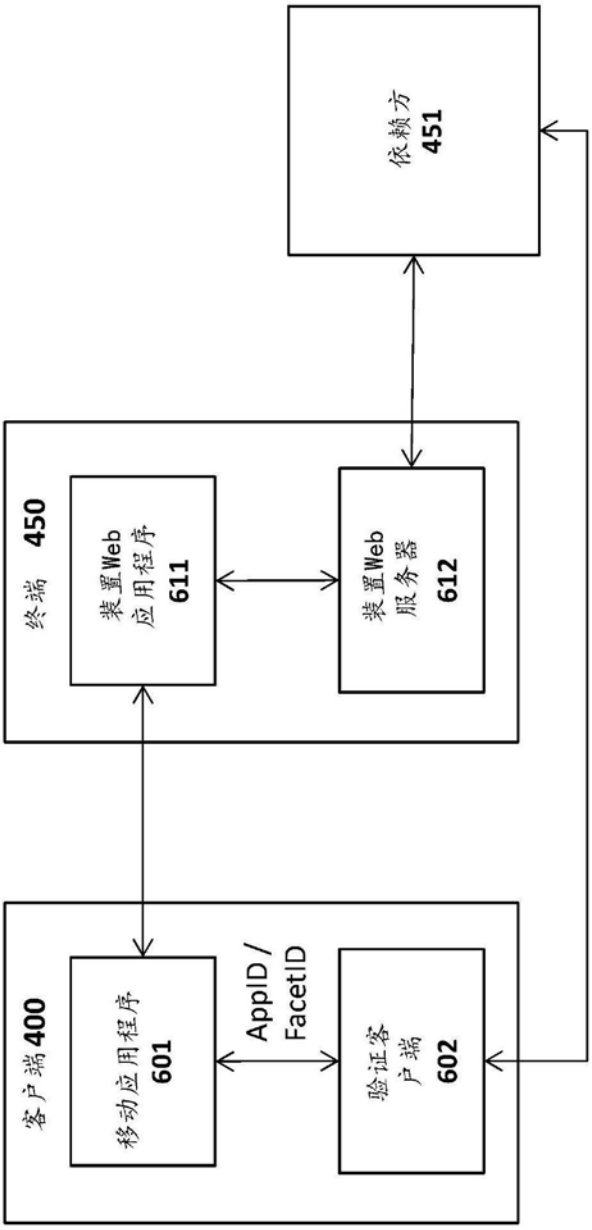

依赖方
451
终端 450
装置Web
应用程序
611
装置Web
服务器
612
客户端400
移动应用程序
601
AppID /
FacetID
验证客
户端
602

图6

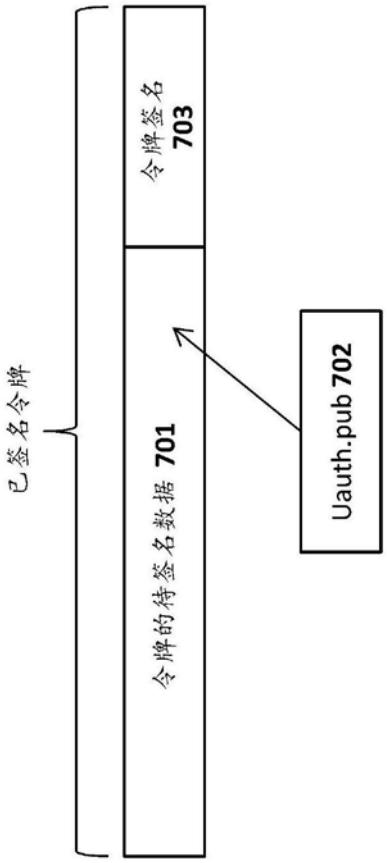


图7

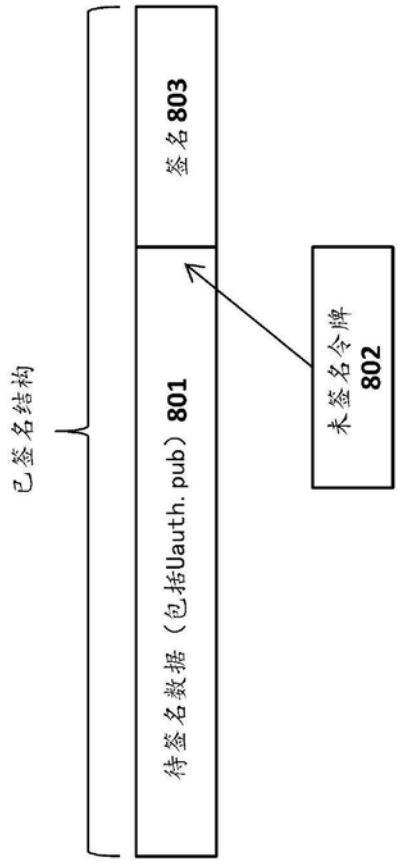


图8

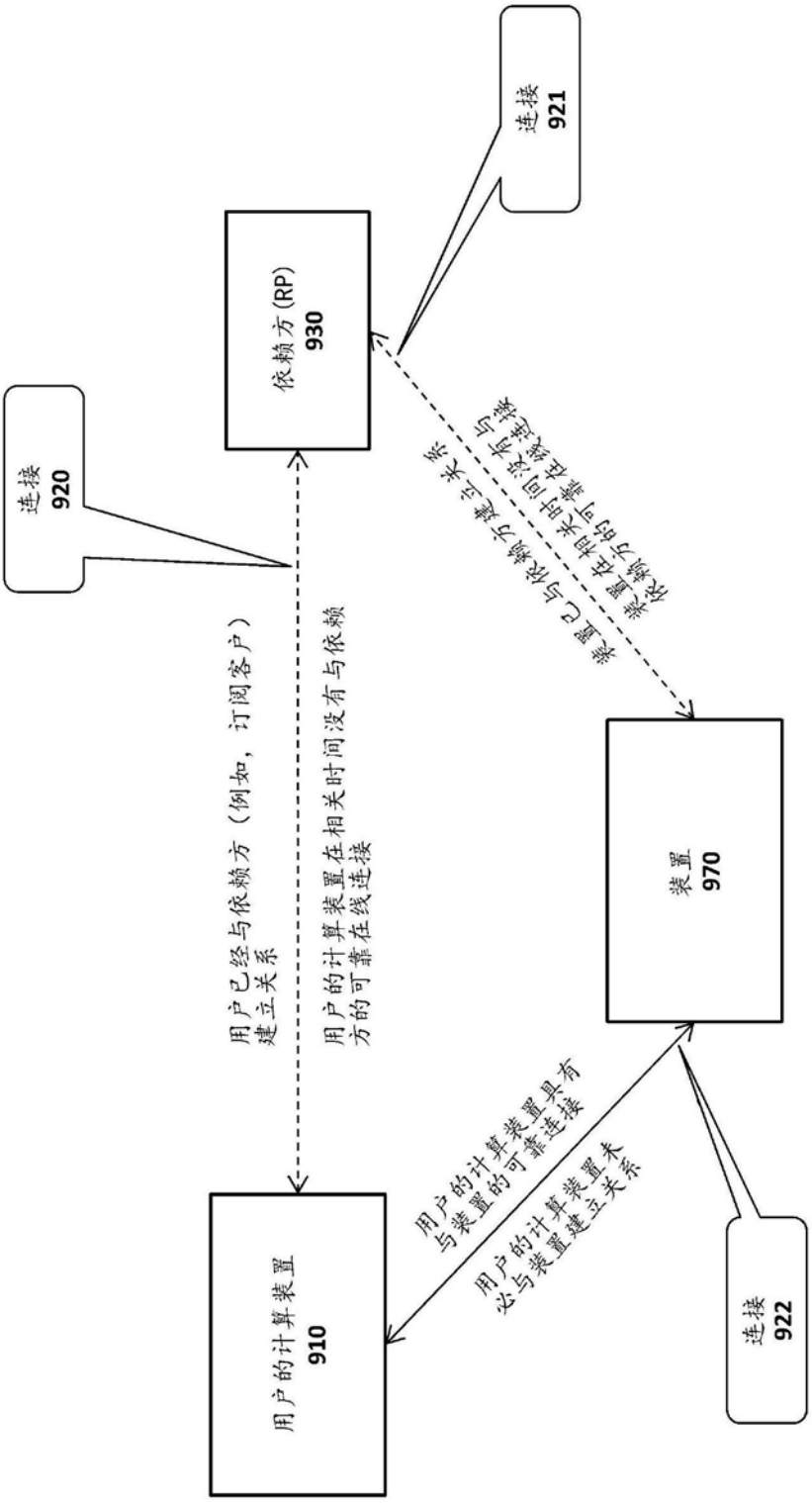

连接
921
依赖方(RP)
930
连接
920
用户已经与依赖方（例如，订阅客户）
建立关系
用户的计算装置在相关时间没有与依赖
方的可靠在线连接
装置已与依赖方建立关系
并且具有用户的可靠连接
装置
970
用户的计算装置具有
与装置的可靠连接
用户的计算装置未
必与装置建立关系
用户的计算装置
910
连接
922

图9

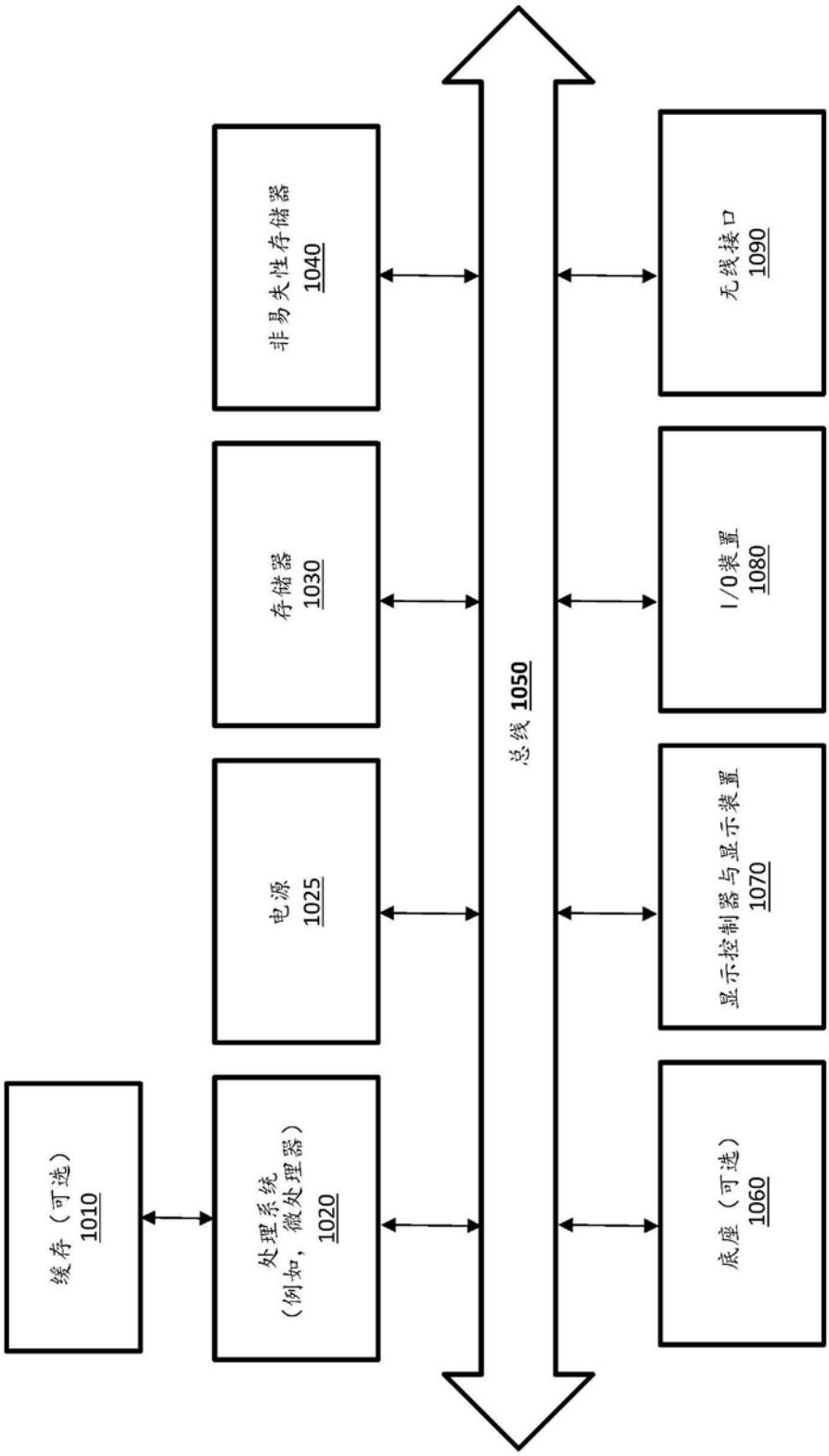

缓存（可选）
1010
处理系统
（例如，微处理器）
1020
电源
1025
存储器
1030
非易失性存储器
1040
总线 1050
底座（可选）
1060
显示控制器与显示装置
1070
I/O装置
1080
无线接口
1090

图10

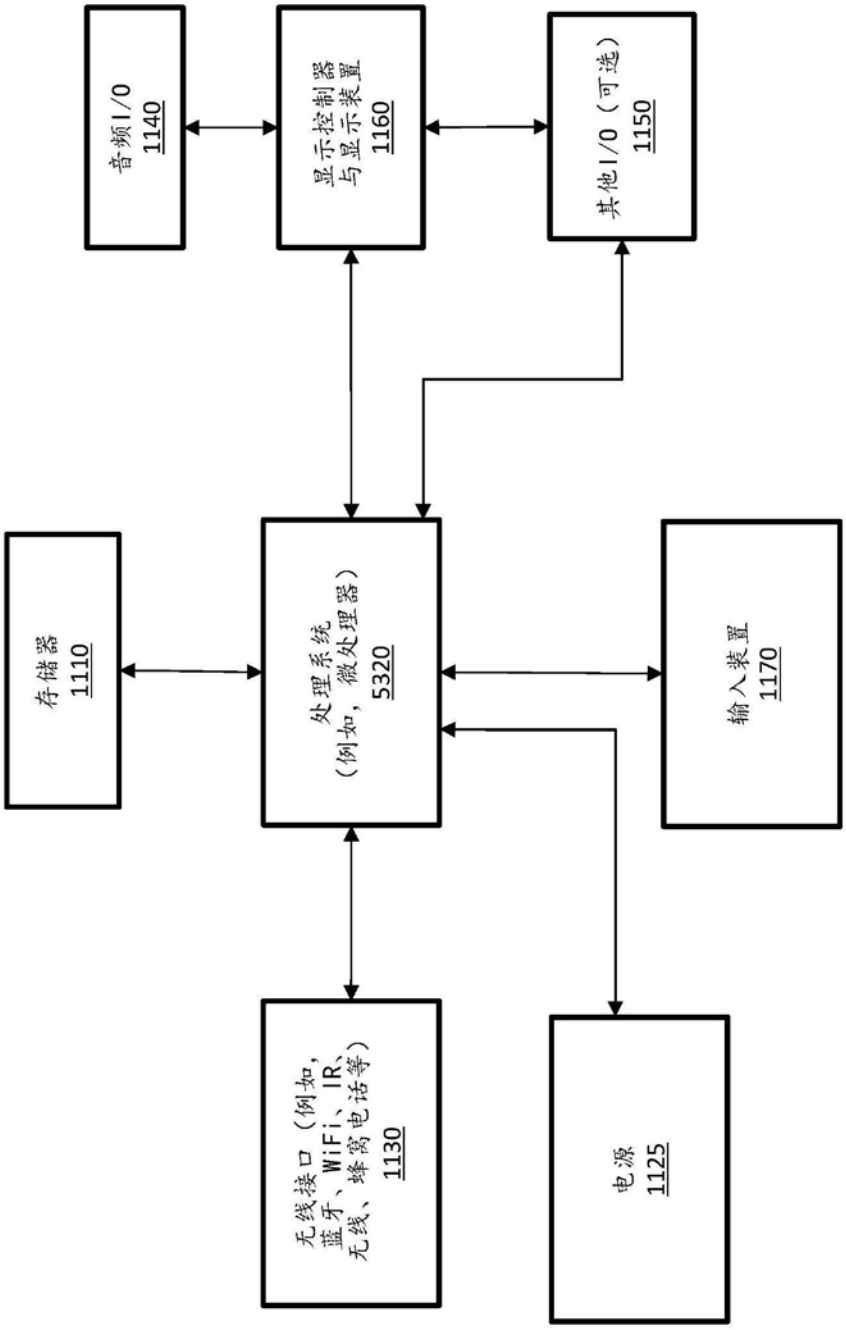

音频I/O
1140
显示控制器
与显示装置
1160
其他I/O（可选）
1150
存储器
1110
处理系统
（例如，微处理器）
5320
输入装置
1170
无线接口（例如，
蓝牙、WiFi、IR、
无线、蜂窝电话等）
1130
电源
1125

图11