(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 107111478 B
(45)授权公告日 2020.12.01

(21)申请号 201580049696.X
(22)申请日 2015.09.16
(65)同一申请的已公布的文献号
申请公布号 CN 107111478 A
(43)申请公布日 2017.08.29
(30)优先权数据
14/487,992 2014.09.16 US
(85)PCT国际申请进入国家阶段日
2017.03.15
(86)PCT国际申请的申请数据
PCT/US2015/050348 2015.09.16
(87)PCT国际申请的公布数据
WO2016/044373 EN 2016.03.24
(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 B·J·威尔逊 D·巴格达萨瑞安
(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.
G06F 7/04(2006.01)
H04L 29/06(2006.01)
(56)对比文件
US 2011/0265159 A1,2011.10.27
US 2003/0087629 A1,2003.05.08
CN 102404116 A,2012.04.04
US 8584224 B1,2013.11.12
US 2014/0189808 A1,2014.07.03
US 2014/0189828 A1,2014.07.03
审查员 赵小娟

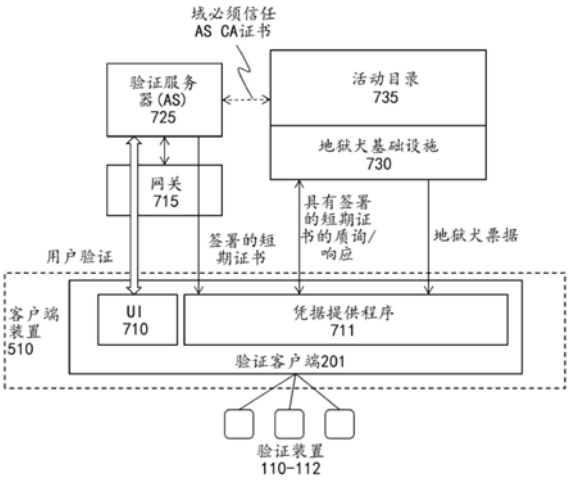
权利要求书3页 说明书12页 附图11页

(54)发明名称

用于在网络架构内集成验证服务的系统和方法

(57)摘要

本发明描述了用于在现有网络基础设施内集成验证服务的系统、设备、方法和机器可读介质。一个实施例包括:网关,所述网关被配置为限制对内部网络的访问;验证服务器,所述验证服务器通信地耦接到所述网关;具有验证客户端的客户端装置,所述验证客户端具有耦接到其上的用于验证用户的多个验证装置,所述验证客户端被配置为与所述验证服务器建立通信信道,并用所述验证服务器注册所述多个验证装置中的一个或多个,所述多个验证装置可用于在注册之后利用所述验证服务器执行在线验证;所述验证客户端响应于经由所述网关获得对所述内部网络的访问的尝试,使用所述注册的验证装置中的一个或多个利用所述验证服务器验证所述用户。



CN 107111478 B

1.一种用于在网络架构内集成验证服务的系统,包括:

网关,所述网关被配置为限制对内部网络的访问;

验证服务器,所述验证服务器通信地耦接到所述网关;

具有验证客户端的客户端装置,所述验证客户端具有耦接到其上的用于验证用户的多个验证装置,所述验证客户端被配置为与所述验证服务器建立通信信道,并用所述验证服务器注册所述多个验证装置中的一个或多个,所述多个验证装置在注册之后利用所述验证服务器执行在线验证;

所述验证客户端响应于经由所述网关获得对所述内部网络的访问的尝试,使用所注册的多个验证装置中的一个或多个利用所述验证服务器验证所述用户;

所述验证服务器响应于成功验证向所述客户端装置提供密码数据结构;

所述客户端装置向所述网关提供所述密码数据结构作为所述成功验证的证明;以及

所述网关利用所述验证服务器查验所述密码数据结构,其中在从所述验证服务器接收到所述密码数据结构有效的指示之后,所述网关提供由所述客户端装置对所述内部网络的访问。

2.根据权利要求1所述的系统,还包括:

浏览器,所述浏览器被配置在所述客户端装置上,其中响应于所述用户经由所述浏览器访问所述内部网络的尝试,所述网关提供浏览器可执行代码,所述浏览器可执行代码在被所述浏览器执行时通过建立所述验证服务器与所述验证客户端之间的通信信道触发所述验证。

3.根据权利要求2所述的系统,其中所述密码数据结构包括票据。

4.根据权利要求3所述的系统,其中所述网关被配置为向所述浏览器提供包括所述浏览器可执行代码的超文本标记语言(HTML)表单,所述HTML表单具有用于输入用户名和一个或多个密码的字段。

5.根据权利要求4所述的系统,其中所述票据包括能够经由所述HTML表单的字段提交到所述网关的随机的数字串或其他形式的一次性密码(OTP)。

6.根据权利要求1所述的系统,其中所述验证服务器使用与用于验证的所述验证装置相关联的密钥来查验由所述网关提供的所述密码数据结构。

7.根据权利要求6所述的系统,其中所述网关使用远程验证拨入用户服务(RADIUS)协议利用所述验证服务器查验所述密码数据结构。

8.根据权利要求1所述的系统,其中所述网关包括安全套接字层(SSL)虚拟专用网络(VPN)网关。

9.一种用于在网络架构内集成验证服务的系统,包括:

网络安全基础设施,所述网络安全基础设施用于为内部网络提供网络安全服务;

验证服务器,所述验证服务器通信地耦接到所述网络安全基础设施;

具有验证客户端的客户端装置,所述验证客户端具有耦接到其上的用于验证用户的多个验证装置,所述验证客户端被配置为与所述验证服务器建立通信信道,并用所述验证服务器注册所述多个验证装置中的一个或多个,所述多个验证装置在注册之后利用所述验证服务器执行在线验证;

所述验证客户端响应于获得对所述内部网络的访问的尝试,使用所述注册的验证装置

中的一个或多个利用所述验证服务器验证所述用户；

所述验证服务器响应于成功验证向所述客户端装置提供密码数据结构；

所述客户端装置使用所述密码数据结构来与所述网络安全基础设施进行验证；以及

所述网络安全基础设施基于与所述验证服务器建立的信任关系来查验所述密码数据结构，所述网络安全基础设施在查验所述密码数据结构后提供由所述客户端装置对所述内部网络的访问。

10.根据权利要求9所述的系统，其中所述密码数据结构包括由所述验证服务器保持的根证书所签署的数字证书，其中所述信任关系包括所述网络安全基础设施信任使用所述根证书生成的签名。

11.根据权利要求10所述的系统，其中所述数字证书包括由所述验证服务器生成的公共密钥/私有密钥对。

12.根据权利要求11所述的系统，其中所述数字证书包括时间戳或指示所述数字证书有效时间长度的其他数据。

13.根据权利要求12所述的系统，其中为了使用所述数字证书来与所述网络安全基础设施进行验证，所述验证客户端将签署由所述网络安全基础设施提供的质询。

14.根据权利要求13所述的系统，其中所述网络安全基础设施被配置为使用所述根证书的公共密钥来查验所述数字证书上的所述签名，所述公共密钥由与所述网络安全基础设施具有信任关系的所述验证服务器提供；并且还被配置为使用来自所述数字证书的公共密钥来查验所述质询上的所述签名。

15.根据权利要求9所述的系统，其中所述网络安全基础设施包括微软活动目录和地狱犬基础设施。

16.根据权利要求9所述的系统，还包括：

网关，所述网关将所述验证客户端耦接到所述验证服务器。

17.一种用于在网络架构内集成验证服务的方法，所述方法包括：

配置网关，以限制对内部网络的访问；

将验证服务器可通信地耦接到所述网关；

配置客户端装置的验证客户端，以与所述验证服务器建立通信通道，并用所述验证服务器注册一个或多个验证装置，所述验证装置在注册之后利用所述验证服务器执行在线验证；

所述验证客户端响应于经由所述网关获得对所述内部网络的访问的尝试，使用所注册的多个验证装置中的一个或多个利用所述验证服务器验证用户；

所述验证服务器响应于成功验证向所述客户端装置提供密码数据结构；

所述客户端装置向所述网关提供所述密码数据结构作为所述成功验证的证明；以及

所述网关利用所述验证服务器查验所述密码数据结构，其中在从所述验证服务器接收到所述密码数据结构有效的指示之后，所述网关提供由所述客户端装置对所述内部网络的访问。

18.根据权利要求17所述的方法，其中浏览器被配置在所述客户端装置上，其中响应于所述用户经由所述浏览器访问所述内部网络的尝试，所述网关提供浏览器可执行代码，所述浏览器可执行代码在被所述浏览器执行时通过建立所述验证服务器与所述验证客户端

之间的通信信道触发所述验证。

19.根据权利要求18所述的方法，其中所述密码数据结构包括票据。

20.根据权利要求19所述的方法，其中所述网关被配置为向所述浏览器提供包括所述浏览器可执行代码的超文本标记语言(HTML)表单，所述HTML表单具有用于输入用户名和一个或多个密码的字段。

21.根据权利要求20所述的方法，其中所述票据包括能够经由所述HTML表单的字段提交到所述网关的随机的数字串或其他形式的一次性密码(OTP)。

22.根据权利要求17所述的方法，其中所述验证服务器使用与用于验证的所述验证装置相关联的密钥来查验由所述网关提供的所述密码数据结构。

23.根据权利要求22所述的方法，其中所述网关使用远程验证拨入用户服务(RADIUS)协议利用所述验证服务器查验所述密码数据结构。

24.根据权利要求17所述的方法，其中所述网关包括安全套接字层(SSL)虚拟专用网络(VPN)网关。

用于在网络架构内集成验证服务的系统和方法

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，本发明涉及用于在网络架构内集成验证服务的系统和方法。

背景技术

[0002] 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，可经由网络发送由验证器生成的得分和/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)。

[0003] 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中描述，这些美国专利申请都被转让给本受让人：序列号13/730,761，名称为“Query System and Method to Determine Authentication Capabilities”(用于确定验证功能的查询系统和方法)；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)；以及序列号14/218,504，名称为“Advanced Authentication Techniques and Applications”(高级验证技术和应用)(下文中称为“504申请”)。在本文中有时将这些申请称为“共同未决的申请”。

[0004] 简单地讲，在这些共同未决的申请描述的验证技术中，用户向客户端装置上的验证装置(或验证器)诸如生物计量装置(例如，指纹传感器)登记。当用户向生物计量装置登记时，(例如，通过轻扫手指、拍摄照片、记录语音等)捕捉生物计量参考数据。用户可随后经由网络向一个或多个服务器(例如，配备有安全交易/验证服务的网站或其他依赖方，如共同未决的申请中所述)注册/预置验证装置；并且随后使用在注册过程中交换的数据(例如，预置到验证装置中的密钥)向那些服务器验证。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。在共同未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标识用户的其他数据)可本地保持在用户的验证装置上，以保护用户的隐私。

[0005] 504申请描述了多种额外的技术，包括以下技术：设计复合验证器、智能地生成验

证保证等级、使用非侵入式用户核验、将验证数据传送到新的验证装置、用客户端风险数据扩充验证数据、自适应地应用验证策略，以及创建信任圈等等。

[0006] 增强依赖方的基于网络或其他网络使能的应用对在共同未决的申请中所述的远程验证技术的利用通常需要所述应用直接与验证服务器集成。这对此类验证的采用构成障碍，因为依赖方将需要付出努力来更新其应用以与验证服务器集成，以便获得由共同未决的申请中所述的技术提供的验证灵活性。

[0007] 在某些情况下，依赖方可能已经与联合解决方案集成，因此简单的集成路径是简单地将在线验证支持集成到联合解决方案中。不幸的是，这种方法没有解决其他传统系统(诸如VPN、Windows Kerberos部署)的问题，这些系统缺乏对联合协议的认识(因此可能被增加了在线验证功能的联合服务器置于前端)，或者缺乏足够的使得能够直接集成在线验证功能的可扩展性。因此，对于某些依赖方应用程序而言，必须解决的关键问题是找到一种使它们能够集成在线验证系统而不需要修改应用程序自身的代码的方式。

发明内容

[0008] 一种用于在网络架构内集成验证服务的系统，包括：网关，所述网关被配置为限制对所述内部网络的访问；验证服务器，所述验证服务器通信地耦接到所述网关；具有验证客户端的所述客户端装置，所述验证客户端具有耦接到其上的用于验证用户的多个验证装置，所述验证客户端被配置为与所述验证服务器建立通信信道，并用所述验证服务器注册所述多个验证装置中的一个或多个，所述多个验证装置在注册之后利用所述验证服务器执行在线验证；所述验证客户端响应于经由所述网关获得对所述内部网络的访问的尝试，使用所注册的多个验证装置中的一个或多个利用所述验证服务器验证所述用户；所述验证服务器响应于成功验证向所述客户端装置提供密码数据结构；所述客户端装置向所述网关提供所述密码数据结构作为所述成功验证的证明；以及所述网关利用所述验证服务器查验所述密码数据结构，其中在从所述验证服务器接收到所述密码数据结构有效的指示之后，所述网关提供由所述客户端装置对所述内部网络的访问。

[0009] 一种用于在网络架构内集成验证服务的系统，包括：网络安全基础设施，所述网络安全基础设施用于为所述内部网络提供网络安全服务；验证服务器，所述验证服务器通信地耦接到所述网络安全基础设施；具有验证客户端的所述客户端装置，所述验证客户端具有耦接到其上的用于验证用户的多个验证装置，所述验证客户端被配置为与所述验证服务器建立通信信道，并用所述验证服务器注册所述多个验证装置中的一个或多个，所述多个验证装置在注册之后利用所述验证服务器执行在线验证；所述验证客户端响应于获得对所述内部网络的访问的尝试，使用所述注册的验证装置中的一个或多个利用所述验证服务器验证所述用户；所述验证服务器响应于成功验证向所述客户端装置提供密码数据结构；所述客户端装置使用所述密码数据结构来与所述网络安全基础设施进行验证；以及所述网络安全基础设施基于与所述验证服务器建立的信任关系来查验所述密码数据结构，所述网络安全基础设施在查验所述密码数据结构后提供由所述客户端装置对所述内部网络的访问。

[0010] 一种用于在网络架构内集成验证服务的方法，所述方法包括：配置网关，以限制对所述内部网络的访问；将验证服务器可通信地耦接到所述网关；配置所述客户端装置的验证客户端，以与所述验证服务器建立通信通道，并用所述验证服务器注册一个或多个验证

装置，所述验证装置在注册之后利用所述验证服务器执行在线验证；所述验证客户端响应于经由所述网关获得对所述内部网络的访问的尝试，使用所注册的多个验证装置中的一个或多个利用所述验证服务器验证用户；所述验证服务器响应于成功验证向所述客户端装置提供密码数据结构；所述客户端装置向所述网关提供所述密码数据结构作为所述成功验证的证明；以及所述网关利用所述验证服务器查验所述密码数据结构，其中在从所述验证服务器接收到所述密码数据结构有效的指示之后，所述网关提供由所述客户端装置对所述内部网络的访问。

附图说明

[0011] 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：

[0012] 图1A至图1B示出了安全验证系统架构的两个不同实施例；

[0013] 图2是示出了可如何将密钥注册到验证装置中的交易图；

[0014] 图3示出了显示远程验证的交易图；

[0015] 图4示出了用于通过安全套接字层(SSL)虚拟专用网络(VPN)网关将用户连接到内部网络的系统；

[0016] 图5示出了用于在网络基础设施内集成验证服务器的系统的一个实施例；

[0017] 图6示出了使用集成在网络基础设施内的验证服务器执行验证的方法的一个实施例；

[0018] 图7示出了用于在Kerberos基础设施内集成验证服务器的系统的一个实施例；

[0019] 图8示出了使用集成在Kerberos基础设施内的验证服务器执行认证的方法的一个实施例；

[0020] 图9示出了用于服务器和/或客户端的计算机架构的一个实施例；以及

[0021] 图10示出了用于服务器和/或客户端的计算机架构的一个实施例。

具体实施方式

[0022] 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。

[0023] 下文论述的本发明的实施例涉及具有用户核实功能(诸如生物计量形式或PIN输入)的验证装置。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)。用户验证功能还可包括非生物计量形式，如PIN输入。验证器可使用装置，如可信平台模块(TPM)、智能卡和安全元件，来进行密码操作与密钥存储。

[0024] 在移动式生物计量的具体实施中，生物计量装置可远程于依赖方。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强度和完整性保护的装置)以及/或者黑客是否已经危及或甚至已经替换了生物计量装置。生物计量装置的置信度取决于装置的特定实施。

[0025] 本文中使用的术语“本地”指的是用户正亲自在特定位置处(诸如在自动取款机(ATM)或销售点(POS)零售结账处)进行交易的事实。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发起交易的任何系统的环境中实施本发明的基本原理。

[0026] 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),也指安全交易服务器(有时称为代表那个实体实施的,该实体可执行本文所述的基础验证技术)。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,或者可在作为商业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。

[0027] 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。

[0028] 示例性在线验证架构和交易

[0029] 图1A至图1B示出了包括用于注册验证装置(有时也称为“预置”)和验证用户的客户端组件和服务器端组件的系统架构的两个实施例。图1A所示的实施例使用基于web浏览器插件的架构来与网站通信,而图1B所示的实施例不需要web浏览器。本文所述的各种技术诸如向验证装置登记用户、向安全服务器注册验证装置和核验用户可在这些系统构架中的任一者上实施。因此,虽然图1A所示的架构用于展示下述若干实施例的操作,但相同的基本原理可在图1B所示的系统上容易地实施(例如,通过删除浏览器插件105,该浏览器插件充当用于在服务器130与客户端上的安全交易服务101之间通信的中介)。

[0030] 首先转到图1A,所示实施例包括配备有一个或多个用于登记和核验最终用户的验证装置110至112(这些验证装置在本领域中有时称为验证“令牌”或“验证器”)的客户端100。如上所述,验证装置110至112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,用于扫描用户视网膜的光学扫描器和相关联软件),并且支持非生物计量形式(诸如PIN核验)。验证装置可使用可信平台模块(TPM)、智能卡或安全元件用于加密操作以及密钥存储。

[0031] 验证装置110至112通过由安全交易服务101暴露的接口102(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101是用于经由网络与一个或多个安

全交易服务器132至133通信以及用于与在web浏览器104的环境内执行的安全交易插件105介接的安全应用程序。如图1A所示，接口102还可提供对客户端100上的安全存储装置120的安全访问，该安全存储装置存储与每个验证装置110至112相关的信息，诸如装置识别代码、用户识别代码、受验证装置保护的用户登记数据(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安全验证技术的由验证装置包封的密钥。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并且在经由网络(诸如因特网)与服务器130通信时使用。

[0032] 如下文论述，安全交易插件105支持某些类型的网络交易，诸如与网站131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130内的网络服务器131(下文中有时简称为“服务器130”)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105可将交易转发到安全交易服务101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101可开启与当地交易服务器132(即，与网站位于同一地点)或异地交易服务器133的直接通信信道。

[0033] 安全交易服务器132至133耦接到安全交易数据库120，安全交易数据库120用于存储用户数据、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，应当指出的是，本发明的基本原理不需要分离图1A所示的安全企业或web目的地130内的逻辑组件。例如，网站131和安全交易服务器132至133可在单个物理服务器或分开的多个物理服务器内实施。此外，网站131和交易服务器132至133可在用于执行下文所述的功能的一个或多个服务器上所执行的集成软件模块内实施。

[0034] 如上所述，本发明的基本原理不限于图1A所示的基于浏览器的架构。图1B示出了另选的具体实施，其中独立应用程序154利用由安全交易服务101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154被设计为建立与一个或多个网络服务151的通信会话，这些网络服务依赖于安全交易服务器132至133来执行下文详细描述的用户/客户端验证技术。

[0035] 在图1A和图1B所示的任一个实施例中，安全交易服务器132至133可生成密钥，这些密钥接着被安全地传输到安全交易服务101并存储到安全存储装置120内的验证装置中。另外，安全交易服务器132至133管理服务器端上的安全交易数据库120。

[0036] 与远程注册验证装置并向依赖方进行验证相关的某些基本原理将结合图2-图3进行描述，然后详细介绍使用安全通信协议建立信任的本发明实施例。

[0037] 图2示出了用于在客户端上注册验证装置(诸如图1A至图1B中客户端100上的装置110至112)(有时称为“预置”验证装置)的一系列交易。为了简单起见，安全交易服务101和接口102被组合在一起作为验证客户端201，包括安全交易服务器132至133的安全企业或Web目的地130被表示为依赖方202。

[0038] 在注册验证器(例如，指纹验证器、语音验证器等)期间，在验证客户端201和依赖方202之间共享与验证器相关联的密钥。回顾图1A至图1B，密钥存储在客户端100的安全存储装置120和由安全交易服务器132至133使用的安全交易数据库120内。在一个实施例中，密钥是由安全交易服务器132至133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，使用了不对称密钥。在该实施例中，可以由安全交易服务器132至133生成公共/

私有密钥对。公共密钥然后可由安全交易服务器132至133存储，并且相关私有密钥可存储在客户端上的安全存储装置120中。在一个另选的实施例中，密钥可在客户端100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132至133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。

[0039] 在一个实施例中采用一种安全密钥预置协议以通过安全通信信道与客户端共享密钥。密钥预置协议的一个示例是动态对称密钥预置协议(DSKPP)(例如，参见请求注释(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。在一个特定实施例中，客户端生成公共/私有密钥对并向服务器发送公共密钥，可以利用证明密钥证明它们。

[0040] 转到图2所示的具体细节，要启动注册流程，依赖方202生成随机生成的质询(例如，密码随机数)，验证客户端201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。作为响应，验证客户端201发起与依赖方202的带外安全连接(例如，带外交易)，并使用密钥预置协议(例如，上文提到的DSKPP协议)与依赖方202通信。为了发起安全连接，验证客户端201可以向依赖方202返回随机质询(可能带有在随机质询上生成的签名)。此外，验证客户端201可以传输用户的身份(例如，用户ID或其他代码)和要预置注册的验证装置的身份(例如，利用唯一地标识被预置验证装置类型的验证证明ID(AAID))。

[0041] 该依赖方利用用户名或ID代码(例如，在用户账户数据库中)定位用户，(例如，使用签名或简单地比较随机质询与发送过的质询)证实随机质询，证实验证装置的验证代码(如果发送了验证代码(例如，AAID))，并在安全交易数据库(例如，图1A至图1B中的数据库120)中为用户和验证装置创建新条目。在一个实施例中，依赖方维护其接受验证的验证装置的数据库。它可以利用AAID(或其他验证装置代码)查询此数据库以确定正在预置的验证装置是否可接受进行验证。如果是，那么它将继续进行注册过程。

[0042] 在一个实施例中，依赖方202为被预置的每个验证装置生成验证密钥。它向安全数据库写入密钥，并利用密钥预置协议向验证客户端201发回密钥。一旦完成，验证装置与依赖方202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。例如，如果使用不对称密钥，那么依赖方202可以存储公共密钥并向验证客户端201提供私有密钥。在从依赖方202接收私有密钥时，验证客户端201向验证装置中预置密钥(在与验证装置相关联的安全存储装置之内存储密钥)。然后它可以在验证用户期间使用该密钥(如下所述)。在一个另选的实施例中，密钥由验证客户端201生成并使用密钥预置协议向依赖方202提供密钥。在任一种情况下，一旦完成预置，验证客户端201和依赖方202均具有密钥，且验证客户端201通知依赖方已完成。

[0043] 图3示出了用于向预置的验证装置验证用户的一系列交易。一旦完成装置注册(如图2中所述)，依赖方202将接受由客户端上的本地验证装置生成的验证响应(有时称为“令牌”)作为有效的验证响应。

[0044] 转向图3中所示的具体细节，响应于用户发起与依赖方202的需要验证的交易(例如，发起从依赖方网站进行支付，访问私有用户账户数据等)，依赖方202生成包括随机质询(例如，密码随机数)的验证请求。在一个实施例中，随机质询具有与其关联的时间限制(例如，它在指定的一段时间内是有效的)。依赖方还可以标识要由验证客户端201用于验证的验证器。如上所述，依赖方可以预置客户端上可用的每个验证装置并为每个预置的验证器存储公共密钥。因此，它可以使用验证器的公共密钥或可以使用验证器ID(例如，AAID)来标

识要使用的验证器。或者，它可以为客户端提供验证选项的列表，用户可以从该列表进行选择。

[0045] 响应于接收到验证请求，可以为用户呈现请求验证的图形用户界面(GUI)(例如，形式为验证应用/应用的网页或GUI)。用户然后进行验证(例如，在指纹读取器上轻扫手指等)。作为响应，验证客户端201生成验证响应，该验证响应包含随机质询上的签名，带有与验证器相关联的私有密钥。它还可以包括其他相关数据，例如，验证响应中的用户ID代码。

[0046] 在接收验证响应时，依赖方可以证实随机质询上的签名(例如，使用与验证器相关联的公共密钥)并确认用户的身份。一旦完成验证，用户便获许进入与依赖方的安全交易，如图所示。

[0047] 可以使用安全通信协议，例如传输层安全(TLS)或安全套接字层(SSL)在依赖方201和验证客户端202之间建立用于图2至图3所示的任何或所有交易的安全连接。

[0048] 用于集成验证服务与网络架构的系统和方法

[0049] 许多传统系统可以支持除用户名和密码之外的验证方法。例如，安全套接字层(SSL)虚拟专用网络(VPN)系统支持使用一次性密码(OTP)。诸如Kerberos的系统允许用户使用数字证书对网络或服务进行验证。

[0050] 本文所述的本发明实施例利用这些特征对在线验证服务和此类传统系统进行集成，而不需要对传统系统本身进行任何改变(除了配置改变之外)。

[0051] 为了增强安全套接字层(SSL)虚拟专用网络(VPN)的安全性，企业部署基于OTP方法的第二因素验证解决方案。诸如RSA SecurID或OATH之类的解决方案要求用户携带OTP生成器，并且结合用户名和密码输入由该生成器生成的OTP以向VPN进行验证。

[0052] 图4示出了被配置为与SSL VPN网关415组合操作的OTP查验服务器425。在操作中，用户打开web浏览器410并导航到SSL VPN网关415，SSL VPN网关415呈现包含用户ID字段412和密码字段413的基于HTML的登录表单411。用户可以在UID字段412中输入用户ID，并且在密码字段413中输入OTP(单独或者附加到用户的静态密码)。在通过HTML表单411输入用户名和密码之后，用户将结果提交到SSL VPN网关415。

[0053] SSL VPN网关415针对用户存储420查验用户名和密码(例如，验证用户名存在并且输入正确的密码)，并且通过将用户输入的OTP提供给OTP查验服务器425来查验OTP。如果OTP查验服务器425提供肯定的应答，查验OTP，SSL VPN网关415授予用户对受保护的内部网络430的访问。

[0054] 如上所述，在上述例子中，SSL VPN网关415可以呈现单独的表单元素以启用OTP的输入，而在其他情况下，SSL VPN网关415可以仅依赖于用户将其OTP附加到表单的密码字段中的密码。此外，如果用户存储420查验不接受主用户名和密码，则SSL VPN网关415可以立即拒绝访问。SSL VPN网关415和OTP查验服务器425之间的通信可以由SSL VPN网关供应商或OTP查验服务器供应商提供的插件来促进。然而，大多数SSL VPN网关支持远程验证拨入用户服务(RADIUS;参见RFC 2865)集成。因此，OTP解决方案提供的RADIUS支持避免了OTP服务器提供商开发SSL VPN网关指定连接器的需要。

[0055] 如图5所示，本发明的一个实施例依赖于SSL VPN网关515的现有特征，以在不改变网络基础设施的情况下集成在线验证技术(例如，诸如上文关于图1A-图1B和图3所述的那些技术)。如图所示，该实施例包括可能以与上述OTP查验服务器425相同(或相似)的方式通

信地耦接到SSL VPN网关515的验证服务器202。验证服务器202还通过验证客户端201通信地耦接到客户端装置510,以使用一个或多个验证装置110-112(例如,指纹验证器、语音验证器、视网膜扫描验证器等)验证用户。虽然验证服务器202经由图5中的浏览器耦接到验证客户端201(例如,以与图1A中所示的实施例类似的方式),但是本发明的基本原理不限于基于浏览器的实施。

[0056] 在一个实施例中,SSL VPN网关515、浏览器510和验证服务器202之间的交互如下。用户打开web浏览器510并导航到SSL VPN网关515,SSL VPN网关515呈现包含诸如JavaScript的浏览器可执行代码512的网页511。在一个实施例中,浏览器可执行代码512通过与验证服务器202建立通信信道并触发验证客户端201验证用户来触发验证。在一个实施例中,验证服务器202和客户端201进入一系列验证交易,诸如上文参照图3所述的那些。例如,验证服务器202可以生成包括随机质询(例如,密码随机数)的验证请求,并且可以(或可以不)识别要由验证客户端201用于验证的验证器110-112。响应于接收到验证请求,可以为用户呈现请求验证的图形用户界面(GUI)(例如,形式为验证应用/应用的网页或GUI)。用户然后进行验证(例如,在指纹读取器上轻扫手指等)。作为响应,验证客户端201生成验证响应,该验证响应包含随机质询上的签名,带有与验证器相关联的私有密钥。它还可以包括其他相关数据,例如,验证响应中的用户ID代码。在接收验证响应时,验证服务器202查验随机质询上的签名(例如,使用与验证器相关联的公共密钥)并确认用户的身份。在一个实施例中,JavaScript或其他浏览器可执行代码512在验证服务器202和验证客户端201之间传递上述验证消息。

[0057] 在一个实施例中,响应于成功验证,验证服务器202生成密码数据结构并将其传递到浏览器510,该密码数据结构在本文中被称为“票据”。在一个实施例中,票据包括能够经由HTML表单511的字段提交到SSL VPN网关515的随机的数字串或其他形式的一次性密码(OTP)。例如,如上所述,可以在用于票据的HTML表单511中定义单独的字段,或者可以将票据附加到用户的静态密码的末端。不管如何输入票据,在一个实施例中,JavaScript或其他浏览器可执行代码512将票据提交到SSL VPN网关515。一旦接收到,SSL VPN网关515通过与验证服务器202的通信查验票据(例如,向验证服务器提供票据并接收指示票据有效的通信)。例如,在从SSL VPN网关515接收到票据和其他用户数据(例如,用户ID或其他形式的标识符)时,验证服务器202可以将票据与提供给浏览器510的票据进行比较。如果票据匹配,则验证服务器202向SSL VPN网关515发送“验证成功”消息。如果票据不匹配,则验证服务器向SSL VPN网关515发送“验证失败”消息。在一个实施例中,SSL VPN网关515使用RADIUS(尽管本发明的基本原理不限于任何特定协议)对照验证服务器202查验票据。一旦验证,SSL VPN网关515授予用户对受保护的内部网络530的访问。

[0058] 重要的是,SSL VPN网关515和验证服务器202之间的交易可以以与由OTP查验服务器425提供的成功/失败消息相同的方式(例如,使用相同的协议和数据字段)来实施。因此,SSL VPN网关515无需被重新配置就可以实施本文所述的本发明实施例,从而简化了实施并减少了与之相关联的时间和费用。

[0059] 在上述方法中,SSL VPN登录页面511可以被定制为包括自定义JavaScript或其他浏览器可执行代码512,以触发验证。当然,可以在用户没有安装验证客户端201的情况下实施替代实施例。

[0060] 另外,通过JavaScript或其他浏览器可执行代码512与SSL VPN网关515的通信可以通过用户通常用于向SSL VPN网关515验证的相同HTML表单511来促进。目标将是使用默认SSL VPN的HTML表单511中的现有密码或OTP字段来传递由JavaScript或其他可执行代码获得的票据(再一次,简化和减少与实施上述技术相关联的时间和费用)。

[0061] 因为这些技术解决了针对大量VPN解决方案的良好限定的问题而无需开发VPN专用集成,所以实现这种集成将需要相对少的努力,并且允许验证服务提供商(即,管理验证服务器202和客户端201的实体)提供用于递送安全远程访问的打包解决方案。

[0062] 图6中示出根据本发明的一个实施例的方法。该方法可在图5中所示架构的环境内实施,但不限于任何特定系统架构。

[0063] 在601处,用户打开浏览器并导航到SSL VPN网关。在602处,SSL VPN网关呈现包含浏览器可执行代码的页面,以在客户端上触发验证。在603处,浏览器可执行代码建立与验证服务器的连接,以触发用户的验证。在604处,浏览器可执行代码在验证客户端与验证服务器之间交换消息以验证用户(参见例如上文关于图1A-图1B、图3和图5的描述)。一旦验证,验证服务器返回票据。

[0064] 在605处,浏览器可执行代码向SSL VPN网关提交票据,并且在606处,SSL VPN网关针对验证服务器查验票据。如上所述,这可以涉及验证服务器将票据与在操作604中返回的票据进行比较,以确认票据的有效性(例如,经由RADIUS)。在607处,一旦票据有效,SSL VPN网关授予用户对受保护的内部网络的访问。

[0065] 在传统系统接受使用数字证书进行验证的情况下,可以采用与传统系统集成的替代方法。这些解决方案(诸如VPN或使用Kerberos的Windows Active Directory)通常涉及用客户端组件来执行证书验证。

[0066] 不同于上文概述的集成方法,其中客户端上的集成主要是基于浏览器的(例如,使用JavaScript),在该实施例中,验证客户端201的元件被集成到传统解决方案的客户端软件中以实现集成;然而,如前所述,不需要服务器端集成。

[0067] 在图7所示的具体实施例中,验证客户端201配备有用于管理签署的证书的凭据提供程序组件711,其用于经由Kerberos基础设施730获得对网络资源的访问。例如,在一个实施例中,可以使用凭据提供程序组件730经由凭据提供程序框架将验证客户端201集成到Windows®操作系统中。然而,应该指出的是,本发明的基本原理不限于Kerberos实施或任何特定类型的操作系统。

[0068] 该实施例还依赖于验证服务器725与验证客户端201之间的通信,验证客户端201进入一系列验证交易以验证最终用户(例如,如上文关于图1B和图3所述)。在一个实施例中,Active Directory735和Kerberos基础设施730被配置为信任由验证服务器725保持的根证书。一旦用户被验证,验证服务器725发出包括密码公共/私有密钥对的短期证书,其使用由验证服务器725保持的根证书来签署(例如,用根证书的私有密钥签署短期证书)。具体地讲,在一个实施例中,短期证书的公共密钥用根证书的私有密钥签署。除了密钥对之外,短期证书还可以包括指示短期证书有效时间长度(例如,5分钟、1小时等)的时间戳/超时数据。

[0069] 在一个实施例中,一旦凭据提供程序711从验证服务器接收到签名的短期证书,它就与涉及短期证书的Kerberos基础设施730进入质询响应交易。具体地讲,Kerberos基础设

施向凭据提供程序711发送质询(例如,诸如随机数的随机数据),然后凭据提供程序711使用短期证书的私有密钥来签署质询。然后它将短期证书发送到Kerberos基础设施,其(1)使用由验证服务器725(其已被配置为信任)提供的根证书的公共密钥来查验短期证书上的签名;并(2)使用来自短期证书的公共密钥来查验质询上的签名。如果两个签名均有效,则Kerberos基础设施向凭据提供程序711发出Kerberos票据,然后它可以用来获得对由Kerberos基础设施管理的网络资源(诸如文件服务器、电子邮件帐户等)的访问。

[0070] 使用这些技术,可以在不对现有Active Directory735和Kerberos基础设施730进行显著修改的情况下集成验证服务器725和客户端201。相反,所有需要的是Active Directory 735/Kerberos基础设施被配置为信任由验证服务器725保持的根证书。

[0071] 图8示出了用于将在线验证基础设施与传统系统集成的方法的一个实施例。该方法可在图7中所示架构的环境内实施,但不限于任何特定系统架构。

[0072] 在801处,用户打开诸如Windows装置的装置并尝试登录。在802处,触发验证客户端,以验证用户。作为响应,验证客户端使用验证服务器执行在线验证。例如,如上所述,验证客户端可能利用服务器已经预先注册了一个或多个验证装置(例如,指纹验证装置、语音验证装置等)。然后,它可以使用一系列交易(诸如上文关于图1A-图1B和图3所述的那些)来利用服务器进行验证。例如,验证服务器可以向验证客户端发送具有随机质询的验证请求,验证客户端使用与所使用的验证装置相关联的私有密钥来进行签名。然后验证服务器可以使用公共密钥来查验签名。

[0073] 不管用于验证的具体协议如何,如果验证成功,则在803处,验证服务器将短期数字证书返回至验证客户端,其使用由验证服务器维护的根证书的私有密钥进行签署。如上所述,根证书受Active Directory/Kerberos基础设施信任。

[0074] 在804处,然后验证客户端使用短期数字证书向Kerberos基础设施进行验证。例如,Kerberos基础设施可以向验证客户端发送质询(例如,诸如随机数的随机数据),然后验证客户端使用短期证书的私有密钥签署所述质询。然后它将短期证书发送到Kerberos基础设施,其在805处使用由验证服务器(其已被配置为信任)提供的根证书的公共密钥来查验短期证书上的签名;并使用来自短期证书的公共密钥来查验质询上的签名。如果两个签名均有效,则Kerberos基础设施向验证客户端发出Kerberos票据,然后在806处它可以用来获得对由Kerberos基础设施管理的网络资源(诸如文件服务器、电子邮件帐户等)的访问。

[0075] 最终结果是使用验证服务器和验证客户端的在线验证可以用于传统系统的前端验证,从而获得有效在线验证的所有灵活性,而不需要改变后端传统应用基础设施。

[0076] 通过本文所述的本发明的实施例实现了许多有益效果,包括但不限于:

[0077] 减少初始集成工作:允许依赖方部署在线验证,而无需重新编写其应用程序以并入在线验证功能,或启用与第三方联合服务器的集成。

[0078] 简化策略管理:这种方法在代码外部表达验证策略,这使得组织可轻松地在不需要改变代码的情况下更新其验证策略。为反映法规要求的新诠释或响应于对现有验证机制的攻击而做出的变化,变成了策略的简单变化并且可快速生效。

[0079] 能够在未来进行细化:在有新的验证装置和机制可用时,组织可以在解决新的或新出现的风险时评估装置/机制的适宜性。集成新的可用验证装置仅需要将装置添加到策略;无需编写新代码就可以立即部署新功能,甚至是传统应用程序。

[0080] 降低直接令牌成本:传统OTP方法依赖于以每个用户为基础趋向于相对昂贵的物理硬件令牌(尽管它们变得越来越便宜),并且具有丢失/损坏替换成本的问题。本文所述的在线验证方法可以通过利用在终端用户装置上已经可用的能力来显著地降低部署成本,消除为每个终端用户获取专用验证硬件的成本。

[0081] 间接部署成本:OTP方法通常需要IT管理员向OTP验证服务器提供最终用户的令牌;基于软件的桌面OTP生成器在初始部署期间仍然需要帮助台干预。在线验证方法可以通过利用在最终用户的装置上已经可用的能力以及提供用于部署的自助服务注册模型来显著地降低部署成本。

[0082] 改善最终用户体验:OTP方法不仅需要用户携带他们的OTP发生器(其中许多人忘记,这导致需要额外的帮助台成本才能进行临时访问),而且还要手动地将OTP输入到应用程序中。FIDO方法可以通过用更简单的东西替换用户名/密码和OTP条目来显著减少验证对最终用户的影响,例如在指纹传感器上滑动手指。

[0083] 示例性数据处理装置

[0084] 图9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9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。

[0085] 如图9所示,计算机系统900,其为一种形式的数据处理系统,包括总线950,该总线与处理系统920、电源925、存储器930和非易失性存储器940(例如,硬盘驱动器、快闪存储器、相变存储器(PCM)等)耦接。总线950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920可从存储器930和/或非易失性存储器940检索指令,并执行这些指令以执行如上所述的操作。总线950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960、显示控制器与显示装置990、输入/输出装置980(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990(例如,蓝牙、WiFi、红外等)。

[0086] 图10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1000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1000可为网络计算机或在另一个装置内的嵌入式处理装置。

[0087] 根据本发明的一个实施例,数据处理系统1000的示例性架构可用于上文所述的移动装置。数据处理系统1000包括处理系统1020,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1020与存储器1010、电源1025(其包括一个或多个电池)、音频输入/输出1040、显示控制器与显示装置1060、可选输入/输出1050、输入装置1070和无线收发器1030耦接。应当理解,在本发明的某些实施例中,图10中未示出的其他组件也可为数据处理系统1000的一部分,并且在本发明的某些实施例中,可使用比图10所示更少的组件。另外,应当理解,图10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。

[0088] 存储器1010可存储数据和/或程序以供数据处理系统1000执行。音频输入/输出1040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1060可包括图形用户界面(GUI)。无线(例如,RF)收发器1030(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1070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1050可为底座的连接器。

[0089] 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。

[0090] 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。

[0091] 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。

[0092] 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。

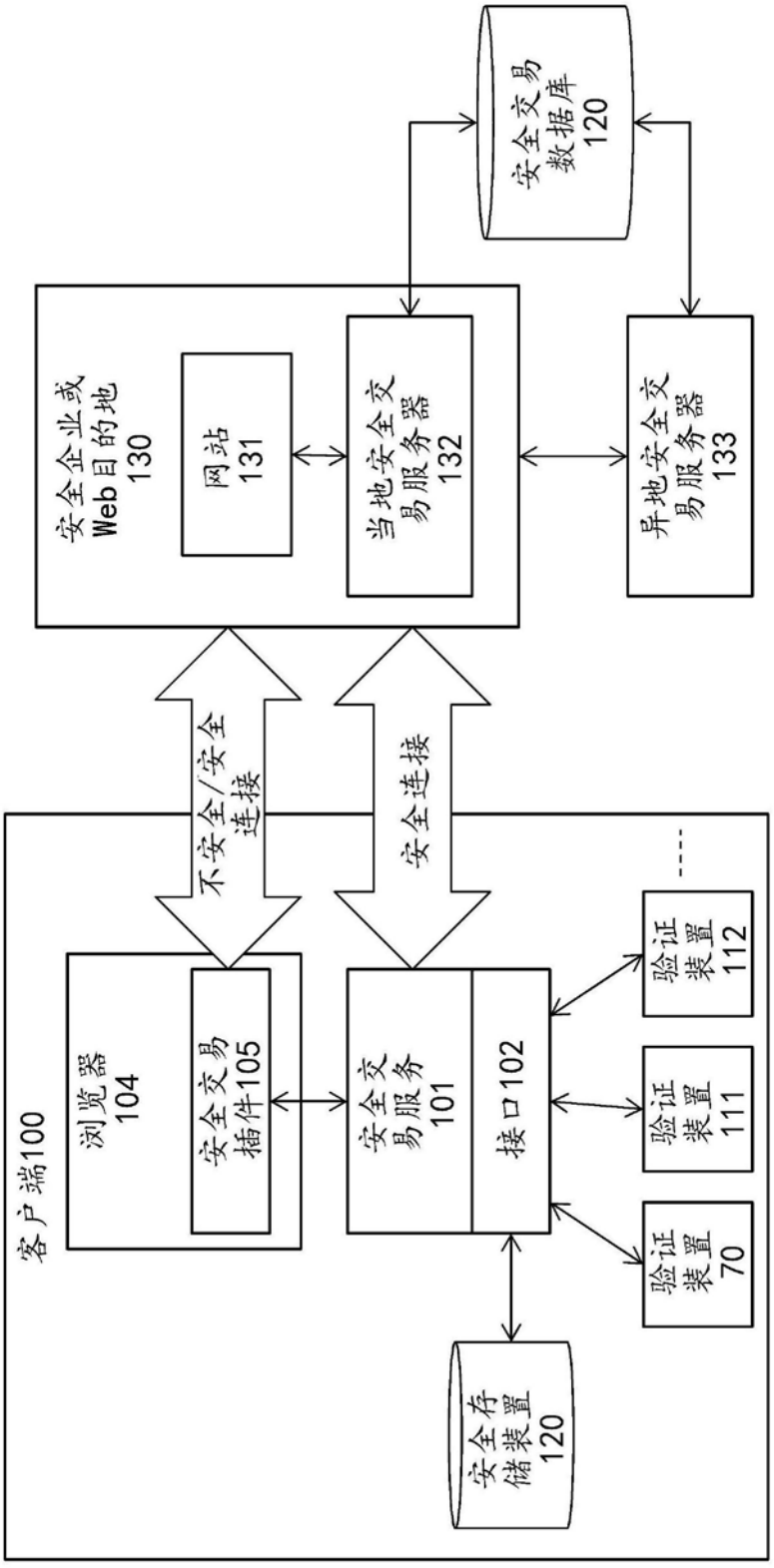

安全交易数据库120
安全企业或Web目的地130
网站131
当地安全交易服务器132
异地安全交易服务器133
不安全/安全连接
安全连接
客户端100
浏览器104
安全交易插件105
安全交易服务101
接口102
验证装置112
验证装置111
验证装置70
安全存储装置120

图1A

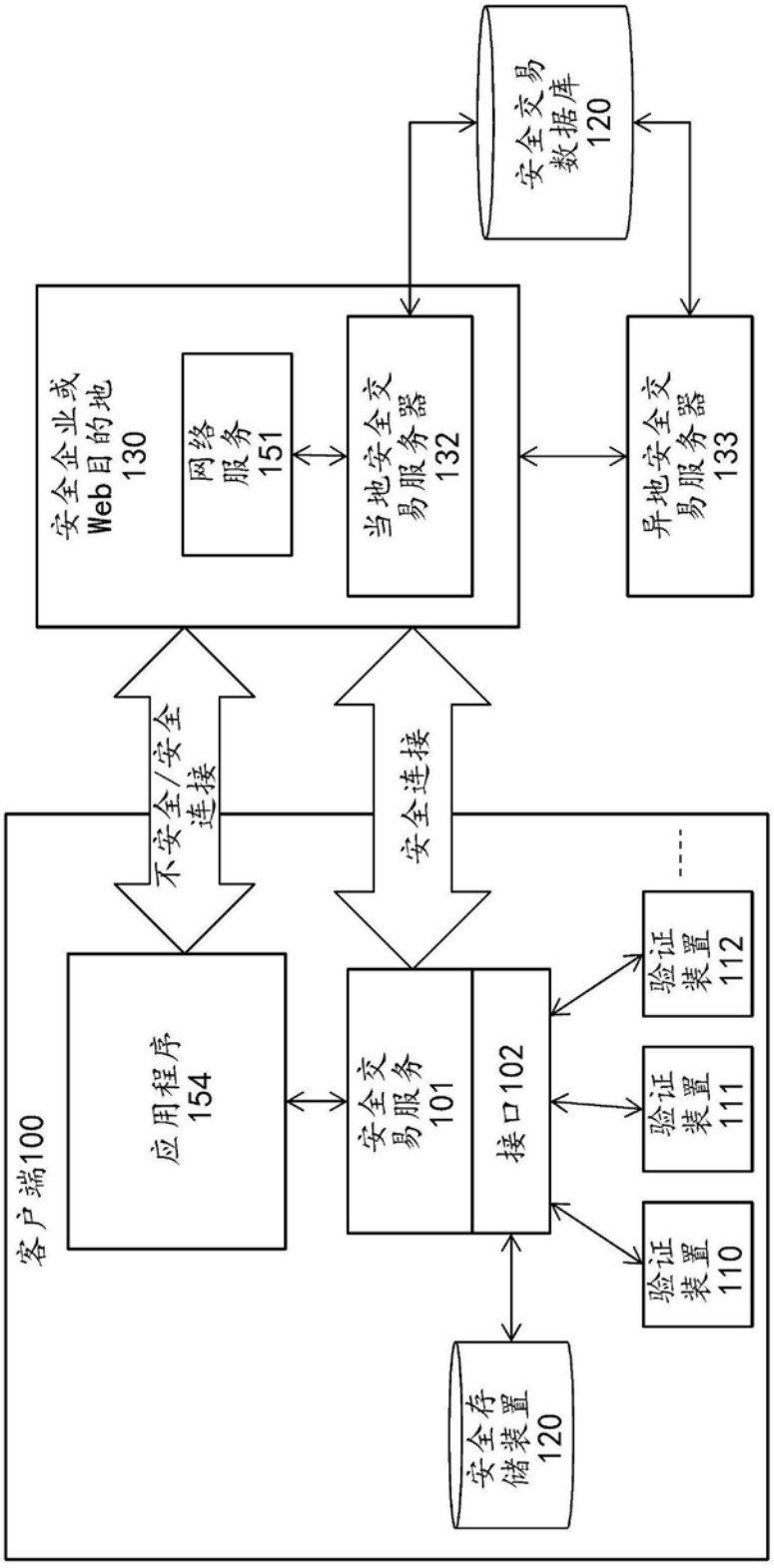

安全交易数据库 120
安全企业或 Web目的地 130
网络服务 151
当地安全交易服务器 132
异地安全交易服务器 133
不安全/安全连接
安全连接
客户端100
应用程序 154
安全交易服务 101
接口102
验证装置 112
验证装置 111
验证装置 110
安全存储装置 120

图1B

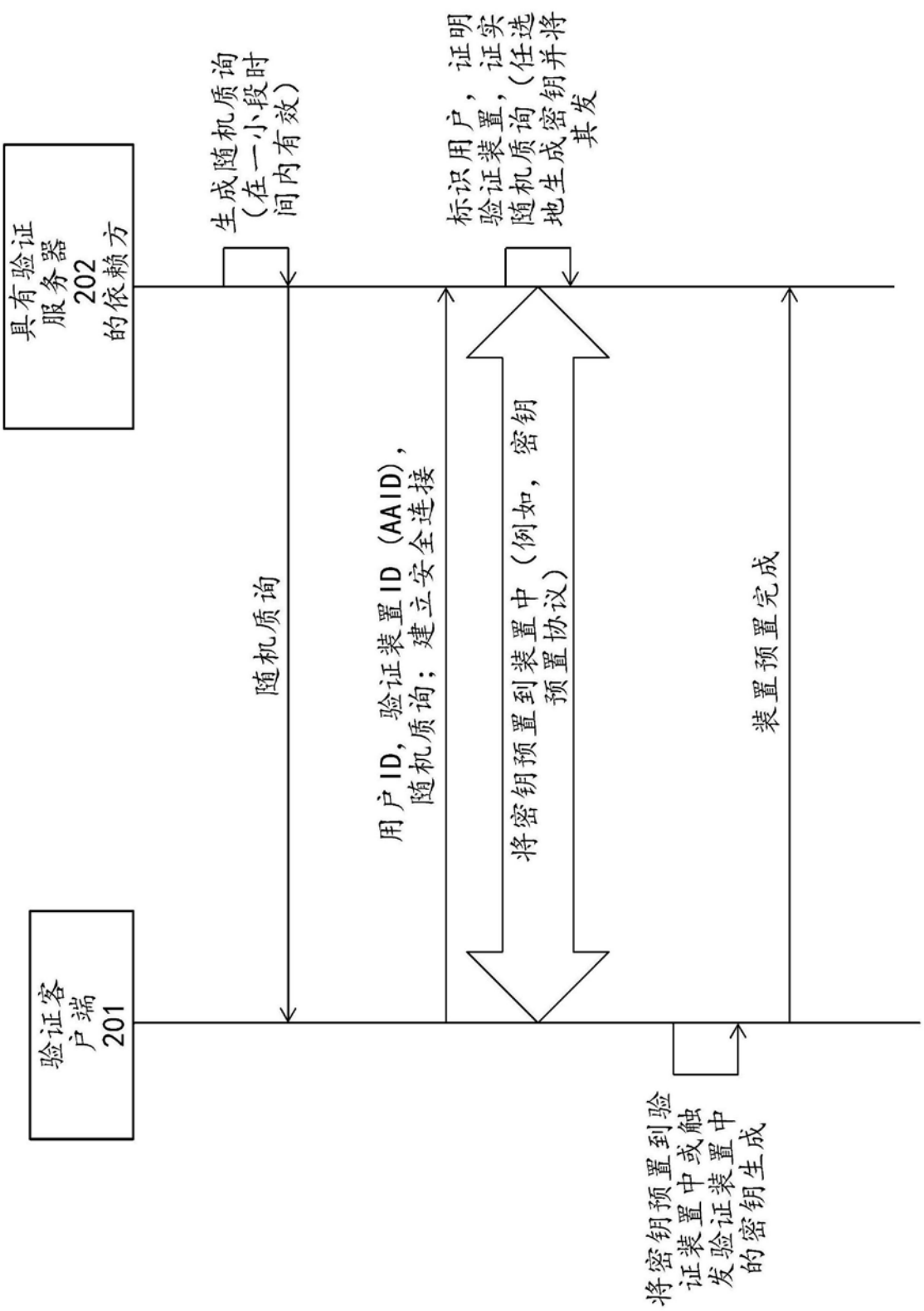

具有验证服务器202的依赖方
验证客户端201
生成随机质询（在一小段时间内有效）
随机质询
用户ID，验证装置ID（AAID），随机质询；建立安全连接
标识用户，证明验证装置，证实随机质询，（任选地生成密钥并将其发
将密钥预置到装置中（例如，密钥预置协议）
装置预置完成
将密钥预置到验证装置中或触发验证装置中的密钥生成

图2

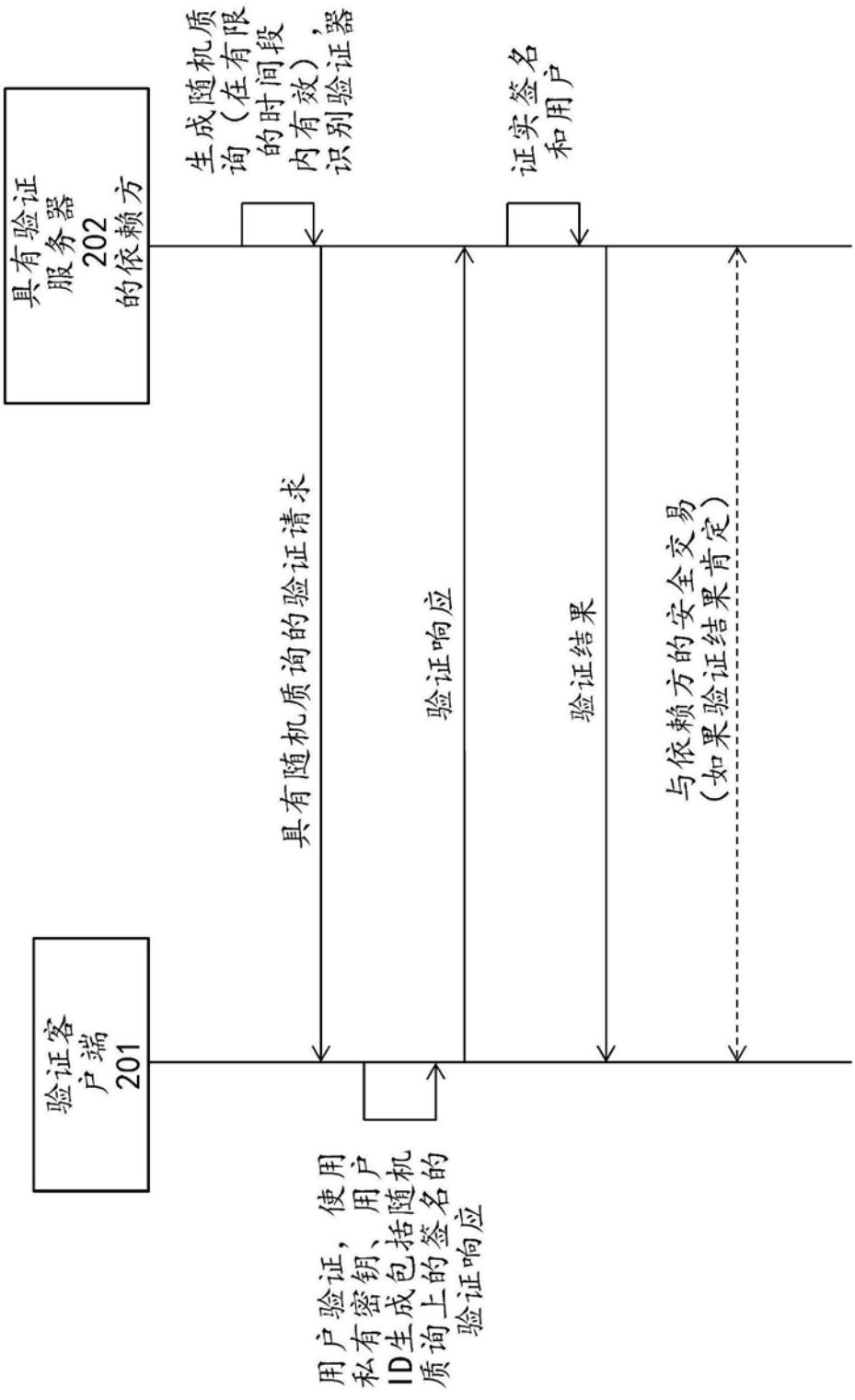

具有验证服务器202的依赖方
验证客户端201
生成随机质询（在有限的时间段内有效），识别验证器
具有随机质询的验证请求
验证响应
证实签名和用户
验证结果
与依赖方的安全交易（如果验证结果肯定）
用户验证，使用私有密钥、用户ID生成包括随机质询上的签名的验证响应

图3

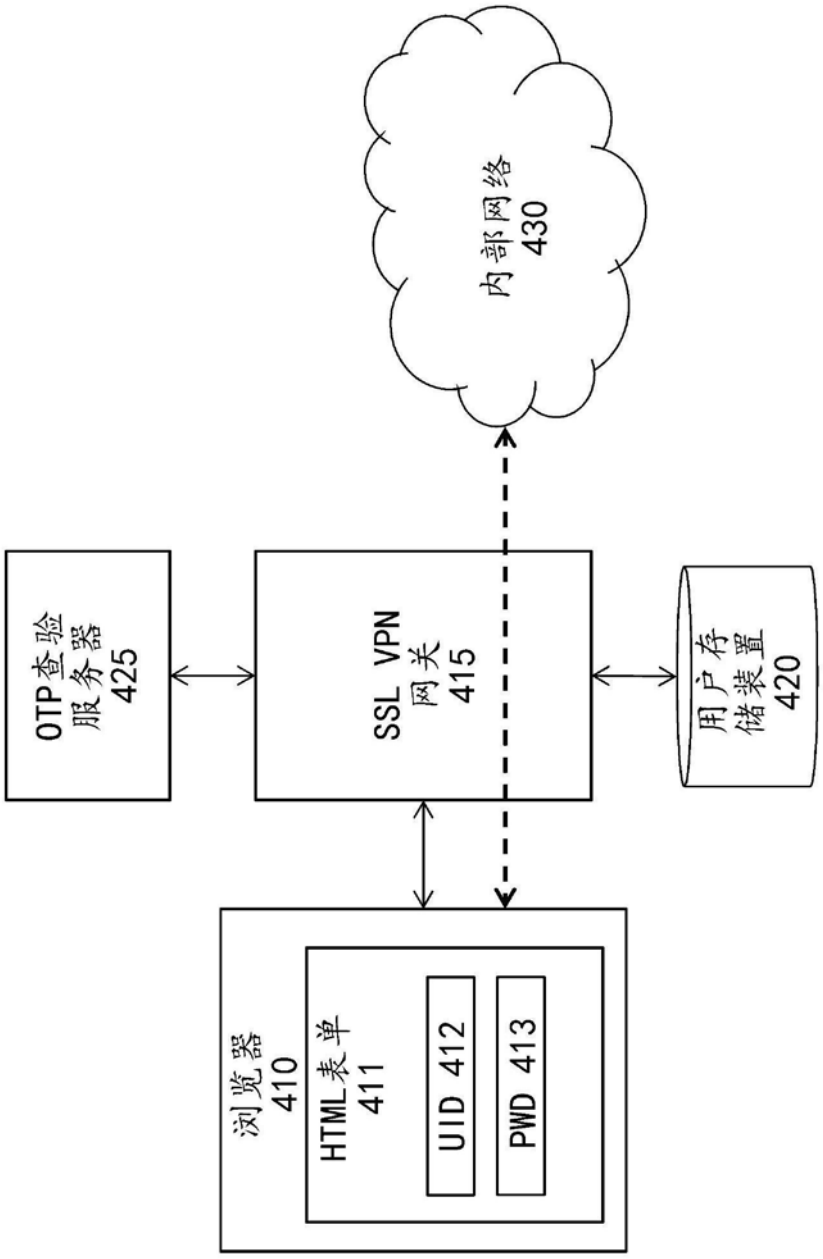

内部网络
430
OTP查验
服务器
425
SSL VPN
网关
415
用户存
储装置
420
浏览器
410
HTML表单
411
UID 412
PWD 413

图4

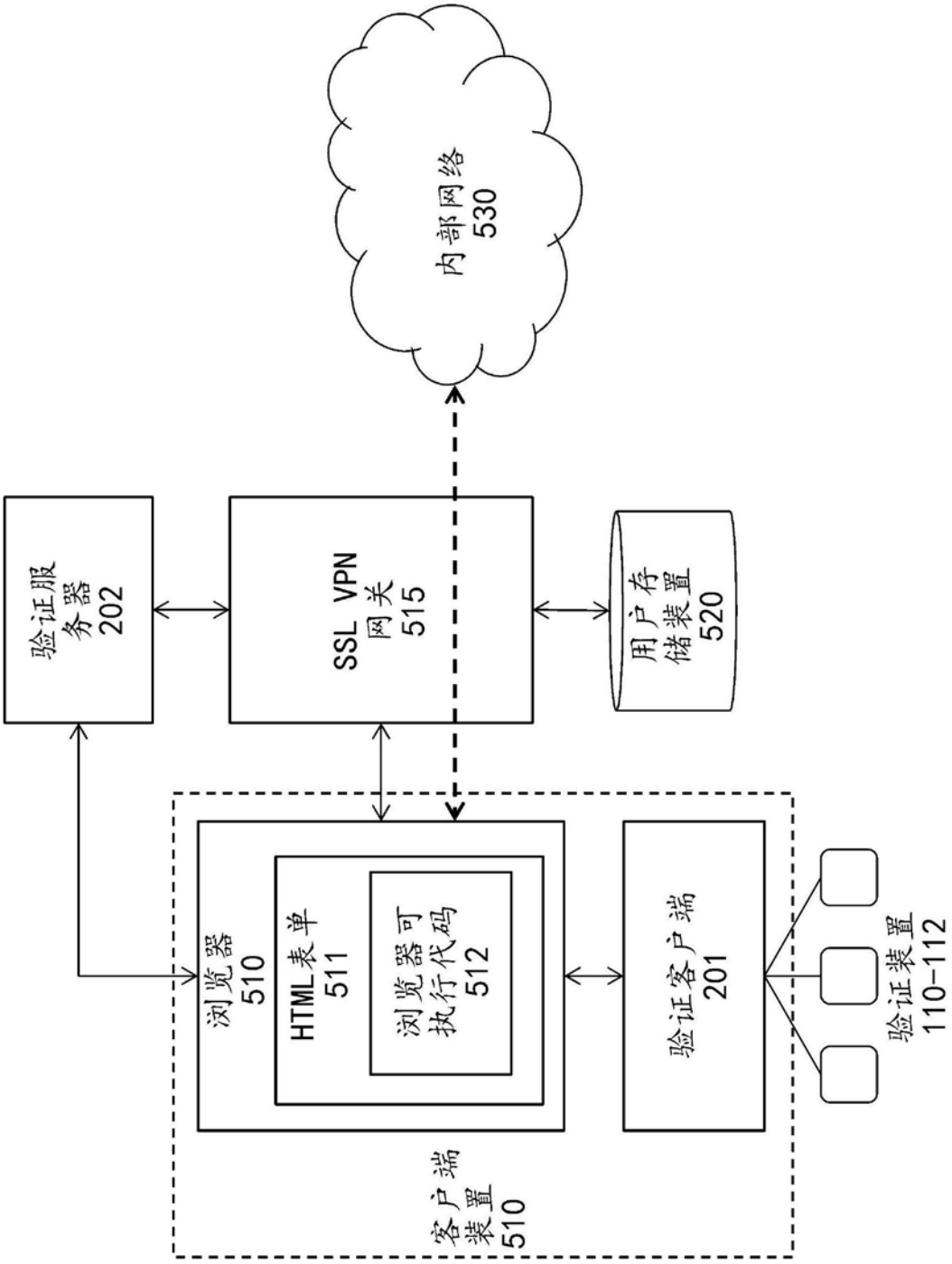

内部网络
530
验证服务器
202
SSL VPN
网关
515
用户存储装置
520
浏览器
510
HTML表单
511
浏览器可执行代码
512
验证客户端
201
验证装置
110-112
客户端装置
510

图5

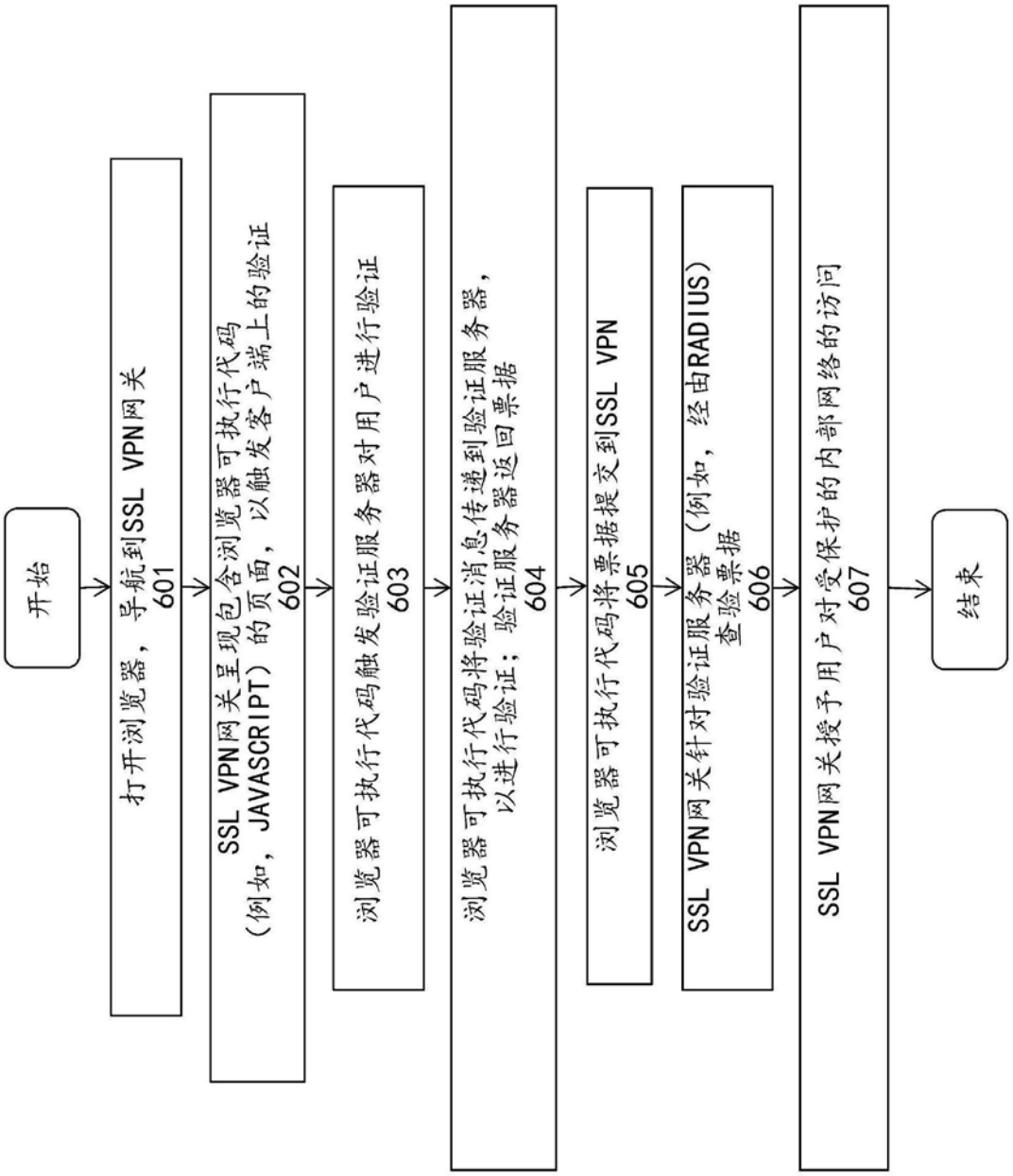

开始
打开浏览器，导航到SSL VPN网关
601
SSL VPN网关呈现包含浏览器可执行代码
（例如，JAVASCRIPT）的页面，以触发客户端上的验证
602
浏览器可执行代码触发验证服务器对用户进行验证
603
浏览器可执行代码将验证消息传递到验证服务器，
以进行验证；验证服务器返回票据
604
浏览器可执行代码将票据提交到SSL VPN
605
SSL VPN网关针对验证服务器（例如，经由RADIUS）
查验票据
606
SSL VPN网关授予用户对受保护的内部网络的访问
607
结束

图6

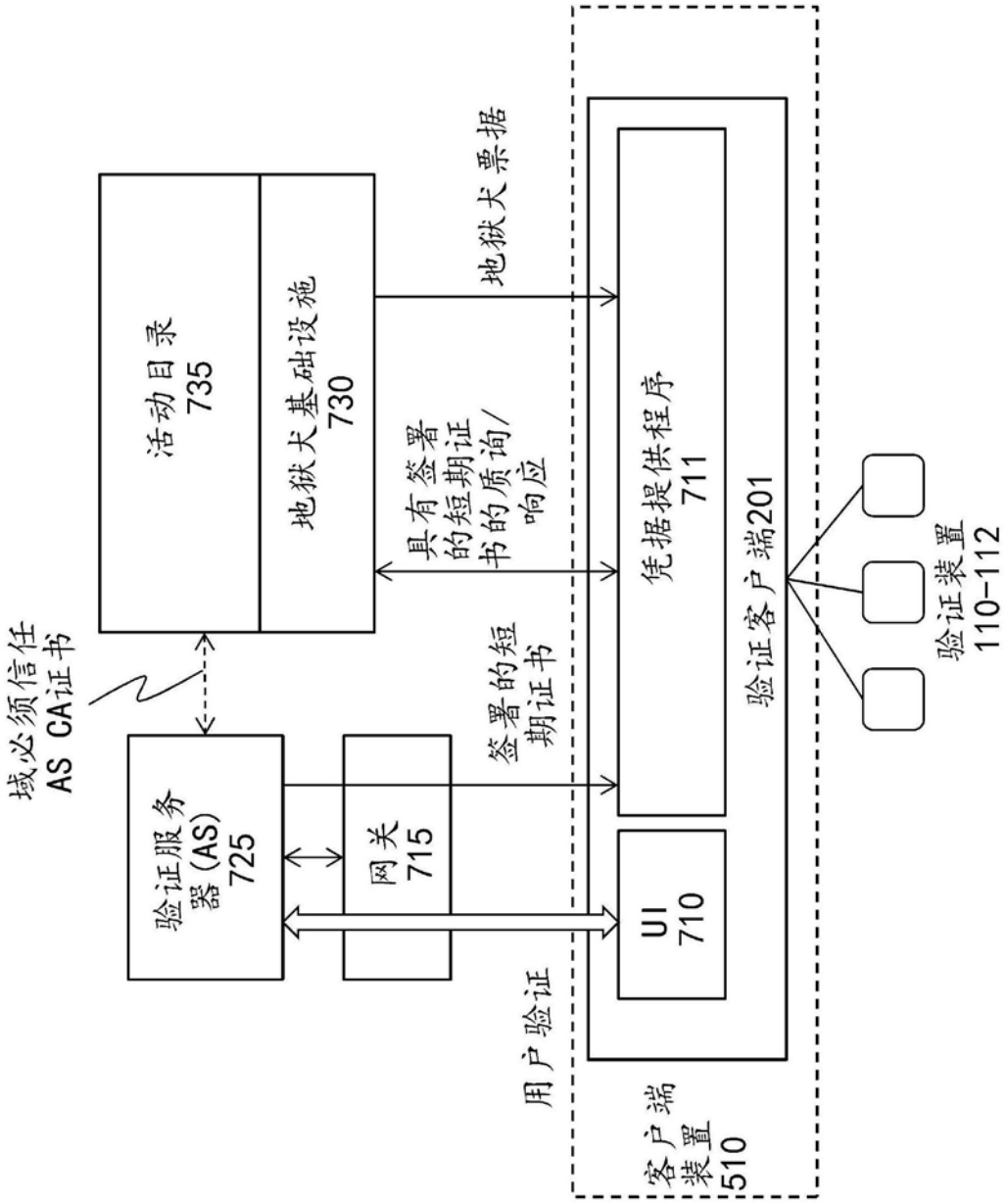

域必须信任
AS CA证书
活动目录
735
地狱犬基础设施
730
地狱犬票据
具有签署的短期证书的质询/响应
签署的短期证书
凭据提供程序
711
验证客户端201
验证装置
110-112
验证服务器(AS)
725
网关
715
UI
710
用户验证
客户端装置
510

图7

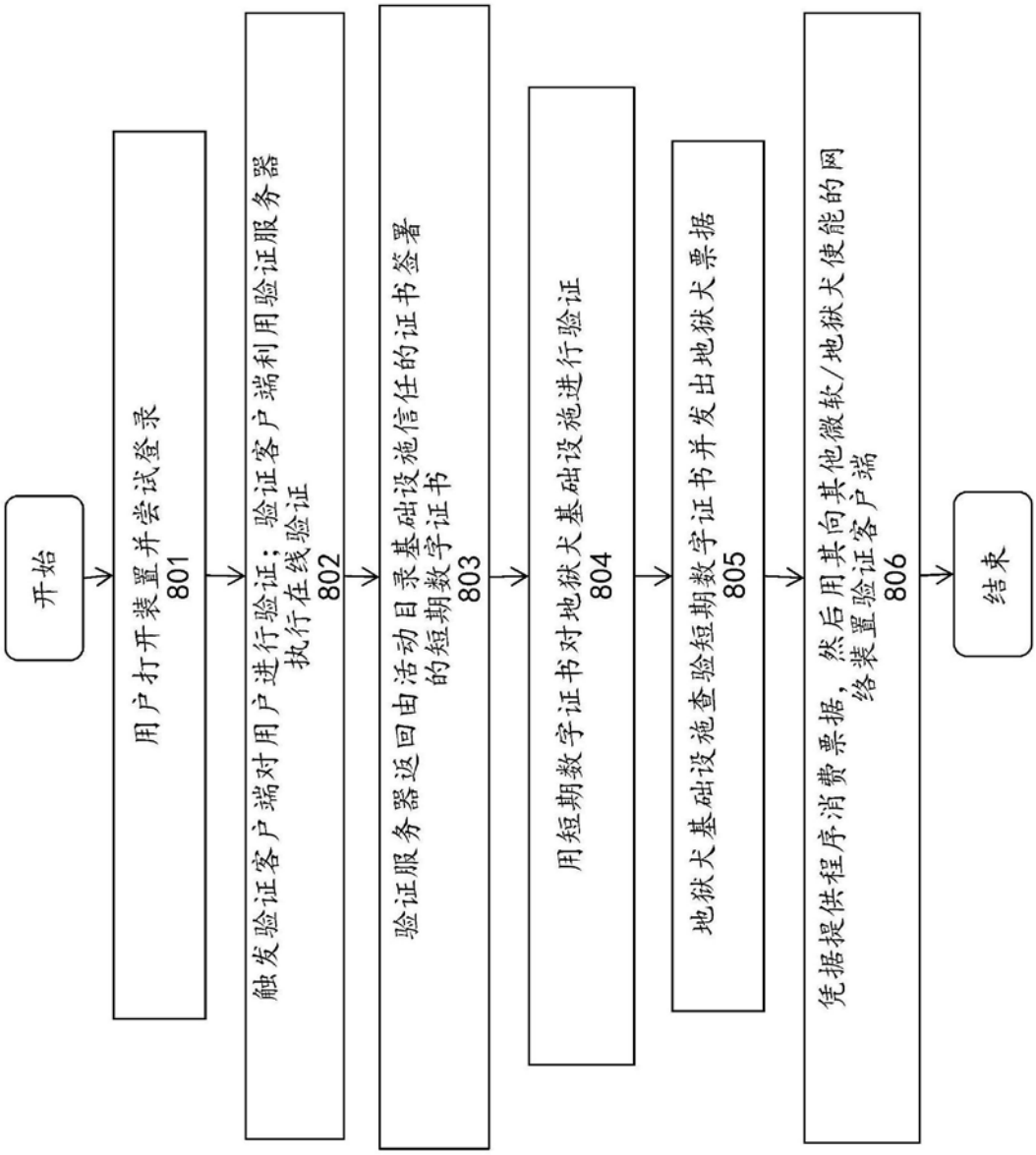

开始
用户打开装置并尝试登录
801
触发验证客户端对用户进行验证；验证客户端利用验证服务器执行在线验证
802
验证服务器返回由活动目录基础设施信任的证书签署的短期数字证书
803
用短期数字证书对地狱犬基础设施进行验证
804
地狱犬基础设施查验短期数字证书并发出地狱犬票据
805
凭据提供程序消费票据，然后用其向其他微软/地狱犬使能的网络装置验证客户端
806
结束

图8

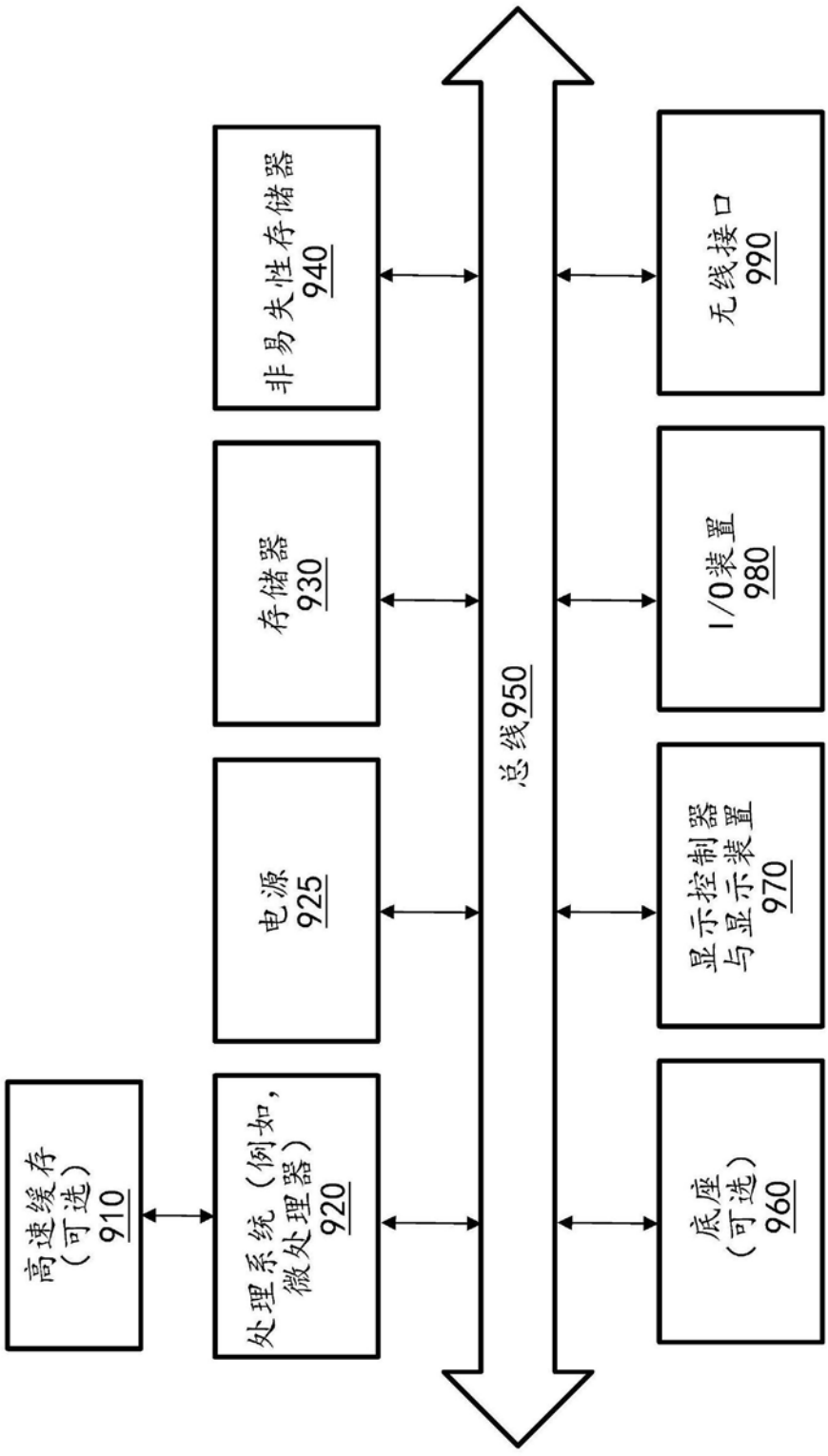

高速缓存（可选）
910
处理系统（例如，微处理器）
920
电源
925
存储器
930
非易失性存储器
940
总线950
底座（可选）
960
显示控制器与显示装置
970
I/O装置
980
无线接口
990

图9

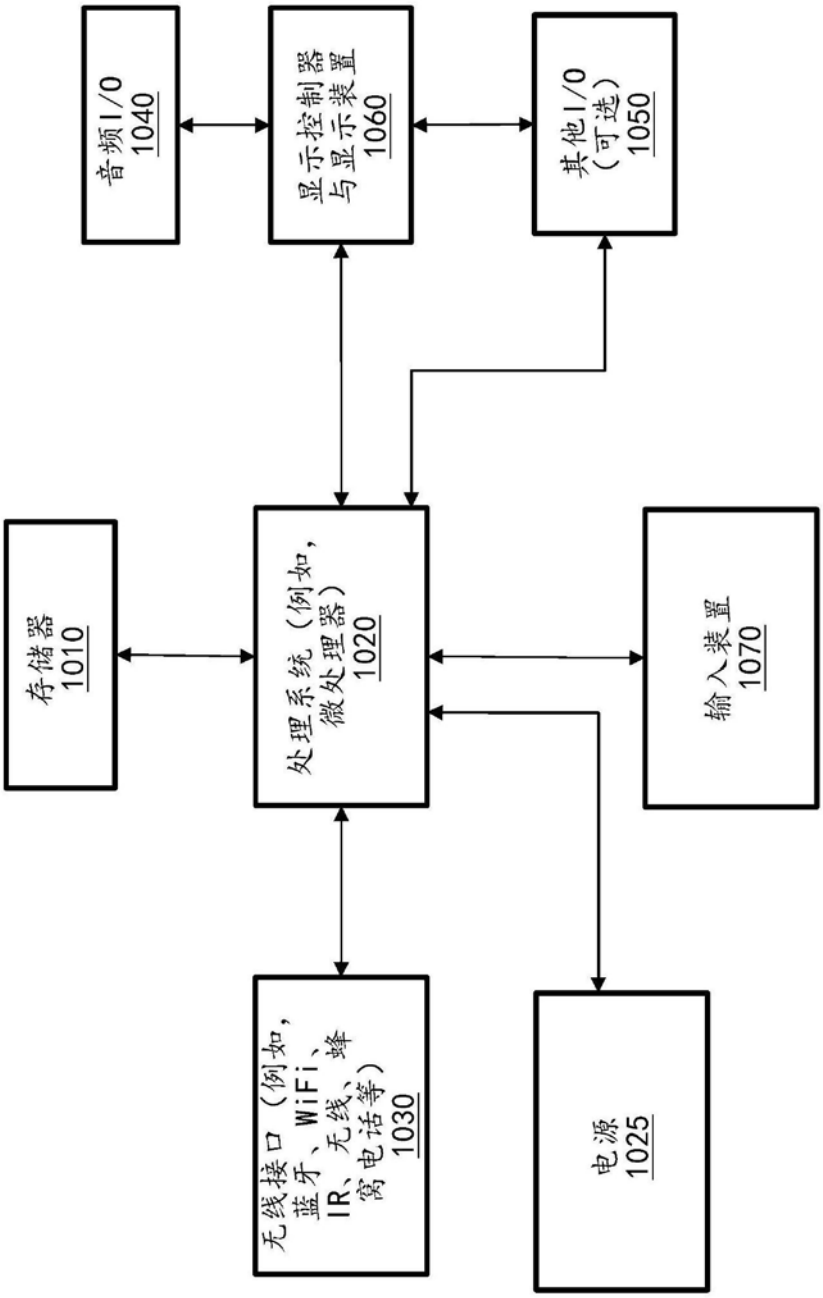

音频I/O
1040
显示控制器
与显示装置
1060
其他I/O
(可选)
1050
存储器
1010
处理系统(例如,
微处理器)
1020
输入装置
1070
无线接口(例如,
蓝牙、WiFi、
IR、无线、蜂
窝电话等)
1030
电源
1025

图10