(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 106575281 B
(45)授权公告日 2021.03.26

(21)申请号 201580040831.4
(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 106575281 A
(43)申请公布日 2017.04.19
(30)优先权数据
14/448,814 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/US2015/042786 2015.07.30
(87)PCT国际申请的公布数据
WO2016/019089 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 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 15/16(2006.01)
(56)对比文件
US 2005223217 A1,2005.10.06
US 2007234417 A1,2007.10.04
US 2008289019 A1,2008.11.20
US 2013125197 A1,2013.05.16
US 8584224 B1,2013.11.12
US 2012124651 A1,2012.05.17
US 2014201809 A1,2014.07.17
CN 103793632 A,2014.05.14
CN 102187701 A,2011.09.14
US 2002112157 A1,2002.08.15
US 2013276060 A1,2013.10.17
US 2010299738 A1,2010.11.25
审查员 刘董敏

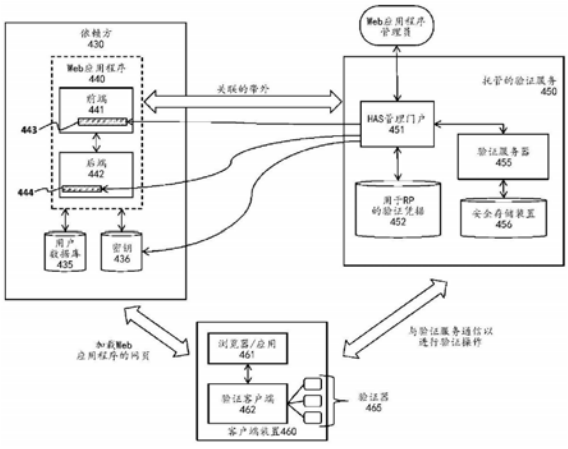
权利要求书3页 说明书10页 附图9页

(54)发明名称

用于实施托管的验证服务的系统和方法

(57)摘要

本发明描述了用于托管的验证服务的系统、设备、方法以及机器可读介质。例如，一种系统的一个实施例包括：托管的验证服务，用于为依赖方提供验证服务，托管的验证服务通过与依赖方共享密钥来注册依赖方；插入到通过所述依赖方托管的应用程序中的第一程序代码组件，所述第一程序代码组件致使访问所述应用程序的客户端装置被重定向到用于与验证相关的功能的所述托管的验证服务；以及托管的验证服务，该托管的验证服务向依赖方传输一个或多个断言，指定在客户端装置和托管的验证服务之间发生的与验证相关的事件，依赖方利用密钥查验断言。



CN 106575281 B

1.一种用于提供认证服务的系统,所述系统包括:

一个或多个硬件平台,其用于托管用于为依赖方提供验证服务的托管的验证服务,所述托管的验证服务和所述依赖方是独立的方,所述托管的验证服务通过与所述依赖方共享密钥来注册所述依赖方,所述托管的验证服务包括管理门户,依赖方管理员通过所述管理门户配置所述托管的验证服务以代表所述依赖方提供验证服务;

由所述托管的验证服务提供的第一程序代码组件,所述第一程序代码组件被插入到通过所述依赖方托管的应用程序中,所述第一程序代码组件致使访问所述应用程序的客户端装置被重定向到用于用户验证和其他与验证相关的功能的所述托管的验证服务,所述用户验证和其他与验证相关的功能包括注册用户客户端设备的一个或多个新验证器以及解除注册一个或多个验证器;以及

所述托管的验证服务基于所述客户端设备和所述托管的验证服务之间发生的多个不同的与验证相关的事件而向所述依赖方直接传输多个断言,由此绕过所述客户端装置,所述多个断言中的每一个断言指定在所述客户端装置和所述托管的验证服务之间发生的一个不同的与验证相关的事件,所述多个断言中的每一个断言包括至少一个指示,其中第一指示指示所述用户已经注册了新验证器,第二断言指示所述用户已经解除注册验证器,以及第三断言指示所述用户已经使用验证器验证了所述托管的验证服务,其中所述依赖方利用所述密钥查验所述多个断言中的每一个断言。

2.根据权利要求1所述的系统,其中所述密钥包括对称断言密钥。

3.根据权利要求2所述的系统,其中所述托管的验证服务利用所述对称断言密钥在所述多个断言中的一个断言中的数据上生成第一签名,所述依赖方使用其所述对称断言密钥的副本生成所述多个断言中的所述一个断言中的所述数据上的第二签名并比较所述第一签名和所述第二签名以查验所述多个断言中的所述一个断言。

4.根据权利要求1所述的系统,其中所述第一程序代码组件包括超文本标记语言HTML代码,并且其中所述应用程序包括Web应用程序。

5.根据权利要求1所述的系统,还包括:

插入到所述依赖方托管的所述应用程序的后端组件中的第二程序代码组件,所述第二程序代码组件安全地存储所述密钥。

6.根据权利要求5所述的系统,其中所述应用程序包括Web应用程序,所述Web应用程序包括所述后端和包括超文本标记语言HTML代码的前端。

7.根据权利要求1所述的系统,其中所述管理门户生成要应用于所述应用程序的前端的前端代码和要应用于所述应用程序的后端的后端代码,所述前端代码可用于将客户端装置重定向到所述托管的验证服务,并且所述后端代码可用于安全地存储和访问所述密钥。

8.根据权利要求1所述的系统,其中所述多个断言中的每一个断言还包括验证器类型、型号和/或强度的指示。

9.一种用于提供认证服务的方法,所述方法包括:

通过与依赖方共享密钥,在托管的验证服务处注册所述依赖方,所述托管的验证服务和所述依赖方是独立的方,所述托管的验证服务包括管理门户,依赖方管理员通过所述管理门户配置所述托管的验证服务以代表所述依赖方提供验证服务;

将由所述托管的验证服务提供的第一程序代码组件插入到通过所述依赖方托管的应

用程序中，所述第一程序代码组件致使访问所述应用程序的客户端装置被重定向到用于用户验证和其他与验证相关的功能的所述托管的验证服务，所述用户验证和其他与验证相关的功能包括注册用户客户端设备的一个或多个新验证器以及解除注册一个或多个验证器；以及

基于所述客户端设备和所述托管的验证服务之间发生的多个与验证相关的事件而从所述托管的验证服务向所述依赖方直接传输多个断言，由此绕过所述客户端装置，所述多个断言中的每一个断言指定在所述客户端装置和所述托管的验证服务之间发生的一个不同的与验证相关的事件，所述多个断言中的每一个断言包括至少一个指示，其中第一断言指示所述用户已经注册了新验证器，第二断言指示所述用户已经解除注册验证器，以及第三断言指示所述用户已经使用验证器验证了所述托管的验证服务，其中所述依赖方利用所述密钥查验所述多个断言中的每一个断言。

10.根据权利要求9所述的方法，其中所述密钥包括对称断言密钥。

11.根据权利要求10所述的方法，其中所述托管的验证服务利用所述对称断言密钥在所述多个断言中的一个断言中的数据上生成第一签名，所述依赖方使用其所述对称断言密钥的副本生成所述多个断言中的所述一个断言中的所述数据上的第二签名并比较所述第一签名和所述第二签名以查验所述多个断言中的所述一个断言。

12.根据权利要求9所述的方法，其中所述第一程序代码组件包括超文本标记语言HTML代码，并且其中所述应用程序包括Web应用程序。

13.根据权利要求10所述的方法，还包括：

插入到所述依赖方托管的所述应用程序的后端组件中的第二程序代码组件，所述第二程序代码组件安全地存储所述密钥。

14.根据权利要求13所述的方法，其中所述应用程序包括Web应用程序，所述Web应用程序包括所述后端和包括超文本标记语言HTML代码的前端。

15.根据权利要求9所述的方法，其中所述管理门户生成要应用于所述应用程序的前端的前端代码和要应用于所述应用程序的后端的后端代码，所述前端代码可用于将客户端装置重定向到所述托管的验证服务，并且所述后端代码可用于安全地存储和访问所述密钥。

16.根据权利要求9所述的方法，其中所述一个或多个断言还包括验证器类型、型号和/或强度的指示。

17.一种存储有程序代码的非暂时性机器可读介质，所述程序代码，当被机器执行时，使得所述机器执行以下操作：

通过与依赖方共享密钥，在托管的验证服务处注册所述依赖方，所述托管的验证服务和所述依赖方是独立的方，所述托管的验证服务包括管理门户，依赖方管理员通过所述管理门户配置所述托管的验证服务以代表所述依赖方提供验证服务；

将由所述托管的验证服务提供的第一程序代码组件插入到通过所述依赖方托管的应用程序中，所述第一程序代码组件致使访问所述应用程序的客户端装置被重定向到用于用户验证和其他与验证相关的功能的所述托管的验证服务，所述用户验证和其他与验证相关的功能包括注册用户客户端设备的一个或多个新验证器以及解除注册一个或多个验证器；以及

基于所述客户端设备和所述托管的验证服务之间发生的多个与验证相关的事件而从

所述托管的验证服务向所述依赖方直接传输多个断言，由此绕过所述客户端装置，所述多个断言中的每一个断言指定在所述客户端装置和所述托管的验证服务之间发生的一个不同的与验证相关的事件，所述多个断言中的每一个断言包括至少一个指示，其中第一断言指示所述用户已经注册了新验证器，第二断言指示所述用户已经解除注册验证器，以及第三断言指示所述用户已经使用验证器验证了所述托管的验证服务，其中所述依赖方利用所述密钥查验所述多个断言中的每一个断言。

18.根据权利要求17所述的非暂时性机器可读介质，其中所述密钥包括对称断言密钥。

19.根据权利要求18所述的非暂时性机器可读介质，其中所述托管的验证服务利用所述对称断言密钥在所述多个断言中的一个断言中的数据上生成第一签名，所述依赖方使用其所述对称断言密钥的副本生成所述多个断言中的所述一个断言中的所述数据上的第二签名并比较所述第一签名和所述第二签名以查验所述多个断言中的所述一个断言。

20.根据权利要求17所述的非暂时性机器可读介质，其中所述第一程序代码组件包括超文本标记语言HTML代码，并且其中所述应用程序包括Web应用程序。

用于实施托管的验证服务的系统和方法

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，本发明涉及用于实施托管的验证服务的系统和方法。

[0002] 相关领域说明

[0003] 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)。

[0004] 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)；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”)。这些申请在本文中有时称为(“共同未决的申请”)。

[0005] 简而言之，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。

[0006] ‘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。

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1A至图1B示出了安全验证系统架构的两个不同实施例；

[0009] 图2是示出了可如何将密钥注册到验证装置中的交易图；

[0010] 图3示出了显示远程验证的交易图；

[0011] 图4示出了用于实施托管的验证服务的系统的一个实施例；

[0012] 图5示出了用于向托管的验证服务注册依赖方的方法的一个实施例；

[0013] 图6示出了用于使用托管的验证服务的方法的一个实施例；

[0014] 图7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

[0015] 图8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

[0016] 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，为了避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。

[0017] 下文论述的本发明的实施例涉及具有用户核验功能(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。

[0018] 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，互联网、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。

[0019] 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。

[0020] 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。

[0021] 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。

[0022] 示例性系统架构和交易

[0023] 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侧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)。

[0024] 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。

[0025] 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对接的安全应用程序。如图所示,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,诸如装置标识码、用户标识码、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)、以及由验证装置封装的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并且在经由网络(诸如互联网)与服务器130通信时使用。

[0026] 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Web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，对于某些类型的交易(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。

[0027] 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，应该指出的是，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。

[0028] 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。

[0029] 在图1A至图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。

[0030] 将结合图2至图3描述与向依赖方远程注册验证装置和进行验证相关联的某些基本原理，接下来详细描述本发明利用安全通信协议建立信任的实施例。

[0031] 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。

[0032] 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。

[0033] 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，可以利用证实密钥证实它们。

[0034] 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实ID(AAID))。

[0035] 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)查验随机质询，查验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。

[0036] 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。

[0037] 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。

[0038] 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。

[0039] 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，形式为验证应用程序/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。它还可在验证响应中包括其他相关数据，诸如用户ID代码。

[0040] 在接收验证响应时，依赖方可以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。一旦验证完成，用户便获许进入与依赖方的安全交易，如图所示。

[0041] 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。

[0042] 用于实施托管的验证服务的系统和方法

[0043] 本发明的一个实施例包括托管的验证服务，该托管的验证服务向多个依赖方并行提供完整验证服务器功能，但需要依赖方开发者做出最小的集成工作。

[0044] 典型的验证服务器具体实施部署在依赖方的网络基础架构之内。对于其策略不允许关键安全资产在其自身基础架构外部的大型组织而言，这是一种常见的部署选项。然而，将验证服务器集成到现有基础架构中不是一项简单的任务，可能需要很大的投资。

[0045] 一些依赖方可能更倾向放弃此类投资而与托管的验证服务集成，这样提供了相同的验证服务器能力，同时隐藏集成的复杂性。然而，必须要有充分多的安全机制用于要接受的托管的验证服务。

[0046] 如图4中所示，本发明的一个实施例包括被实施为通过网络(例如，互联网)通信地耦接到依赖方430的在线系统的托管的验证服务(HAS)450，以提供上述验证能力。如图所示，基于HAS的架构涉及三个组件：依赖方(RP)Web应用程序440；托管的验证服务450；以及配置有验证器465、验证客户端462和浏览器或应用程序461的客户端装置460。

[0047] 在一个实施例中，RP Web应用程序440是基于Web的在线服务，例如金融机构网站、社交网络网站、基于Web的电子邮件服务、基于Web的娱乐门户等。它具有订阅了由Web应用程序440提供的服务的用户435的数据库和登录系统。RP Web应用程序440通常被设计有前端组件441和后端组件442。前端组件441可以是利用超文本标记语言(HTML)代码或其他基于Web的代码实施的Web服务器，以响应于用户请求动态地生成网页。后端组件442通常能够访问一个或多个数据库435，并包括业务逻辑，用于检索和/或生成要在前端组件441生成的网页中使用的底层数据。例如，如果依赖方是金融机构，后端代码442可以响应于用户请求访问包含账户数据的数据库435。后端组件442然后可以利用账户数据进行计算和/或简单地向前端组件441提供账户数据，前端组件441然后将包括账户数据或利用网页中的账户数据执行的计算。向用户呈现底层数据的方式通常是由前端组件441定义的。

[0048] 在一个实施例中，托管的验证服务450是具有代表依赖方430部署的验证服务器455的在线服务。如前所述，配备有验证客户端462的客户端装置460可以向验证服务器455注册其验证器465(例如，参见图2)。然后可以由验证服务器455在安全存储装置456中存储与验证器465相关联的密钥和其他凭据(并如图3所示检索以验证最终用户)。在图4中所示的一个实施例中，托管的验证服务450还维护用于为多个RP Web应用程序440存储注册的验证凭据(验证注册)的数据库452。

[0049] 如前所述，客户端装置460可以是膝上型计算机、平板计算机、电话或具有验证客户端462并访问验证器465的任何其他数据处理装置。客户端装置还包括浏览器或应用程序461，以访问由依赖方430提供的服务(例如，访问依赖方网站或其他形式的在线服务)。

[0050] 图4示出了一个实施例，其中RP Web应用程序440与托管的验证服务(下文所述)具有带外关联，且RP Web应用程序的网页管理与托管的验证服务450的通信。图4中所示的托管的验证架构为RP Web应用程序开发者提供了若干好处。具体而言，用户具有与任何其他基于验证的Web应用程序相同的用户体验。此外，依赖方不需要维护内部验证凭据，仅需要在Web应用程序440的后端442和前端441上进行少量集成工作(如下所述)。

[0051] 在一个实施例中，集成过程是通过向托管的验证服务450注册RPWeb应用程序440来发起的。Web应用程序管理员(例如，依赖方信息技术团队的成员)可以具备经由托管的验

证服务管理门户451进行访问的能力，并可以通过提供必要的细节(例如，如下所述，与Web应用程序440相关的信息)来创建账户。在一个实施例中，为依赖方管理员提供验证凭据(例如，秘密代码，诸如PIN或口令)，以提前访问管理门户451。管理员然后可以利用凭据登录到管理门户451中。在一个实施例中，管理门户451是经由管理员的浏览器可以访问的基于Web的门户。然而，本发明的基本原理不限于访问管理门户451的任何特定方式。

[0052] Web应用程序管理员可以为管理门户451提供必要的登录凭据和其他相关信息，例如访问Web应用程序的前端程序代码和后端程序代码需要的网络地址。在一个实施例中，响应于来自Web应用程序管理员向托管的验证服务450注册Web应用程序440的请求，管理门户451生成HTML代码443，该代码被并入Web应用程序440的前端441(例如，Web应用程序的网页)。HTML代码443可以实施于纯Javascript、HTML iframe中或使用与Web应用程序440兼容的任何其他编程语言实施。在一个实施例中，HTML代码将直接与Web应用程序440程序代码(例如，前端代码441)通信。

[0053] 在一个实施例中，托管的验证服务门户451还生成后端代码444，其也并入Web应用程序后端442中。管理门户451生成的HTML代码443和后端代码444两者都被示为应用于图4中Web应用程序440的活动实例。然而，在一个实施例中，可以在执行Web应用程序(例如，应用于海量存储装置上存储的应用程序二进制文件和库)之前执行新代码443至444的安装。

[0054] 在一个实施例中，托管的验证服务门户451还生成密码密钥(例如，对称密钥或证书)，本文称为托管的验证服务“断言密钥”，然后将其存储在Web应用程序后端基础架构中的安全存储装置436中。在一个实施例中，密钥436然后由后端442用于查验托管的验证服务450的断言(如下所述)。在将托管的验证服务代码443至444集成到Web应用程序中并提供密钥436之后，完成了集成。

[0055] 一旦完成了集成过程，Web应用程序用户就能够开始使用客户端验证465与依赖方430进行验证。在一个实施例中，托管的验证服务450提供的HTML代码443将管理包括与验证相关的通信的用户验证体验。在一个实施例中，一旦下载到用户的浏览器461中，HTML代码443就将直接与验证客户端462通信，以将验证客户端462定向到托管的验证服务450上的验证服务器455。在一个实施例中，HTML代码443与插件(例如，图1A中所示的安全交易插件101)通信，该插件安装于客户端装置的浏览器461上，以便能够与托管的验证服务450和验证客户端462进行安全通信。

[0056] 在一个实施例中，托管的验证服务450上的验证服务器455然后将生成验证请求并与验证客户端交换其他与验证相关的消息(例如，参见图2至图3和相关文本)。在完成与验证相关的操作时(例如，注册、用户验证、解除注册等)，托管的验证服务450将经由密码断言使用托管的验证服务证实密钥436通知Web应用程序440。例如，验证服务器455可以使用断言密钥436来生成发送到Web应用程序440的每个断言上的签名。Web应用程序440上运行的后端代码444然后可以通过利用其自己的密钥436副本验证断言以查验签名。类似地，后端代码444可以利用从Web应用程序440向托管的验证服务450发送的任何通信上的密钥436生成签名，其可以利用其密钥副本查验通信。

[0057] 在一个实施例中，从托管的验证服务450发送的断言可以包括与验证器465的预置/注册和通过验证器465进行的验证相关的任何信息。例如，断言可以通知Web应用程序440关于诸如验证装置注册的活动以及与验证装置相关的相关信息，诸如安全长度(例如，

用户X刚刚注册了安全长度为Y的验证器)；用户利用特定验证器或验证器类型的成功验证(例如，用户X刚刚与具有安全长度Y的验证器进行验证)；以及验证器的解除注册(例如，用户X刚刚解除验证器Y的注册)。

[0058] 可以利用安全断言标记语言(SAML)、OAuth、OpenID或任何其他类似的技术实施断言。在一些托管的验证服务架构中，断言可以从托管的验证服务服务器455直接到达Web应用程序440服务器(例如，绕过客户端装置460)。在另选的具体实施中，可以通过客户端装置460发送断言(例如，作为向浏览器461发送的Javascript，浏览器然后向Web应用程序440转发断言)。

[0059] 图5示出了根据本发明的一个实施例，用于向托管的验证服务注册依赖方的方法，图6示出了用于执行操作，例如向托管的验证服务注册和解除注册验证装置和用户验证的方法。该方法可在图4中所示的架构的环境内执行，但不限于任何特定系统架构。

[0060] 在501，依赖方管理员登录到托管的验证服务的管理门户(例如，利用提供的凭据)并提供创建新依赖方账户所需的数据。这可以包括在网络上标识依赖方Web应用程序和潜在验证凭据(例如，用户名/口令)以访问Web应用程序(具体而言，Web应用程序的前端程序代码和后端程序代码)所需的联网数据。

[0061] 在502，响应于来自Web应用程序管理员向托管的验证服务注册Web应用程序的请求，管理门户生成并入Web应用程序的前端(例如，Web应用程序的网页)中的前端代码(例如，HTML代码)和并入Web应用程序后端中的后端代码。此外，在502，托管的验证服务门户生成密码断言密钥(例如，对称密钥或证书)。

[0062] 在503，前端代码、后端代码和断言密钥被传输到依赖方。在504，依赖方将前端代码和后端代码集成到其平台中并安全地存储断言密钥。如前所述，在一个实施例中，继而使用断言密钥查验托管的验证服务断言。

[0063] 现在转向图6，在601，配备有一个或多个验证装置的客户端装置连接到依赖方的网站并下载包含前端代码的网页。在一些情况下，该网页可以包含由前端代码动态生成的代码(而非前端代码自身)。如本文所用，“前端代码”是指用于客户端装置上的前端代码自身和前端代码动态生成的代码两者。

[0064] 在602，前端代码与客户端装置上的验证客户端和托管的验证服务(或者，更精确地讲，托管的验证服务处的验证服务器)建立通信。在603，执行一项或多项交易，例如注册新验证器、执行用户验证和/或解除验证器的注册。

[0065] 在604，托管的验证服务利用断言密钥生成与交易相关的密码断言。例如，密码断言可以指示新的注册验证器、解除注册的验证器、与验证器相关的信息，诸如验证器的准确度/精确度(例如，验证器强度)以及用户与验证器的验证。如上所述，可以利用断言密钥签署密码断言。

[0066] 在605，密码断言被传输到依赖方，在606，利用断言密钥查验该断言。例如，后端代码可以检索断言密钥，生成其自己的签名并将生成的签名与从托管的验证服务发送的签名对比。如果签名匹配，那么查验了该断言，并且用户可获许基于断言执行交易。例如，如果该断言指示用户已经成功向托管的验证服务验证，依赖方可以接受该验证并许可用户完成交易(例如，金融交易、访问私有数据等)。

[0067] 在一个实施例中，可以利用多种不同的协议/语言实施托管的验证服务，多种协

议/语言包括例如安全断言标记语言(SAML)、JavaScript对象表示(JSON)Web签名、OAuth或类似技术,以向依赖方传达托管的验证服务断言。此外,托管的验证服务系统可以为嵌入依赖方网页(例如,其向依赖方的网站传送关于托管的验证服务断言)中的前端和后端代码使用iframe。然而,应该指出的是,本发明的基本原理不限于任何特定协议和/或编程语言。

[0068] 本文描述的本发明的实施例优选现有联邦身份服务器和身份提供商,因为最终用户的隐私得到更好的保护。尽管依赖方自己可以具有关于用户的信息,但这种信息不需要与验证托管的服务(或任何其他依赖方)共享以实施本文描述的托管的验证技术。这与现有的允许依赖方在不同依赖方之间跟踪用户的身份提供商和联邦服务器相反。

[0069] 示例性数据处理装置

[0070] 图7是示出了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7示出了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。

[0071] 如图7所示,计算机系统700,其为一种形式的数据处理系统,包括总线750,该总线与处理系统720、电源725、存储器730和非易失性存储器740(例如,硬盘驱动器、快闪存储器、相变存储器(PCM)等)耦接。总线750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720可从存储器730和/或非易失性存储器740检索指令,并执行这些指令以执行如上所述的操作。总线750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760、显示控制器与显示装置770、输入/输出装置780(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790(例如,蓝牙、WiFi、红外等)。

[0072] 图8是示出了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800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800可为网络计算机或在另一个装置内的嵌入式处理装置。

[0073] 根据本发明的一个实施例,数据处理系统800的示例性架构可用于上文所述的移动装置。数据处理系统800包括处理系统820,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820与存储器810、电源825(其包括一个或多个电池)、音频输入/输出840、显示控制器与显示装置860、可选输入/输出850、输入装置870和无线收发器830耦接。应当理解,在本发明的某些实施例中,图8中未示出的其他组件也可为数据处理系统800的一部分,并且在本发明的某些实施例中,可使用比图8所示更少的组件。另外,应当理解,图8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。

[0074] 存储器810可存储数据和/或程序以供数据处理系统800执行。音频输入/输出840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860可包括图形用户界面(GUI)。无线(例如,RF)收发器830(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870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850可为底座的连接器。

[0075] 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。

[0076] 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。

[0077] 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。

[0078] 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。

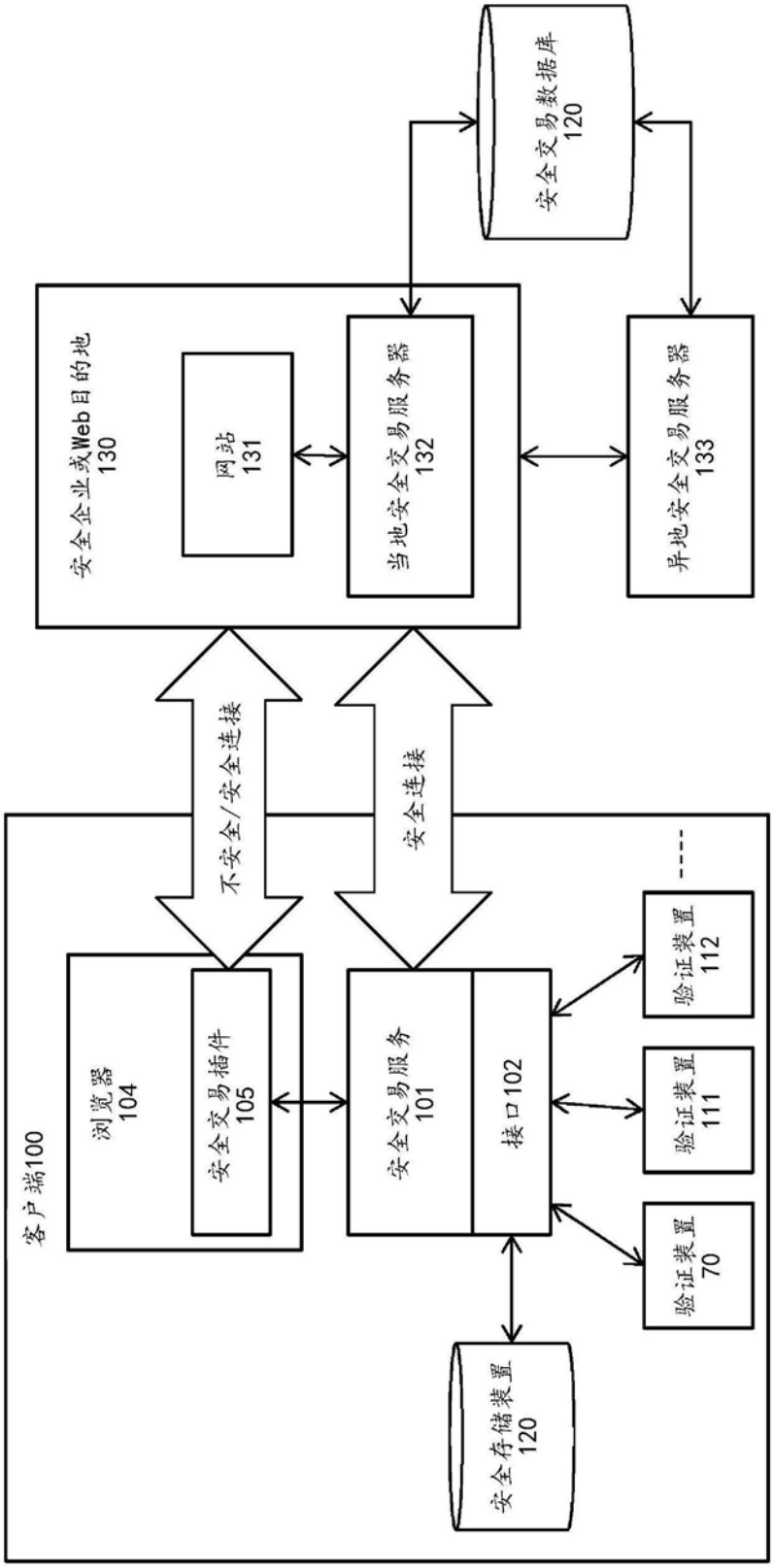

安全交易数据库
120
安全企业或Web目的地
130
网站
131
当地安全交易服务器
132
异地安全交易服务器
133
不安全/安全连接
安全连接
客户端100
浏览器
104
安全交易插件
105
安全交易服务
101
接口102
验证装置
112
验证装置
111
验证装置
70
安全存储装置
120

图1A

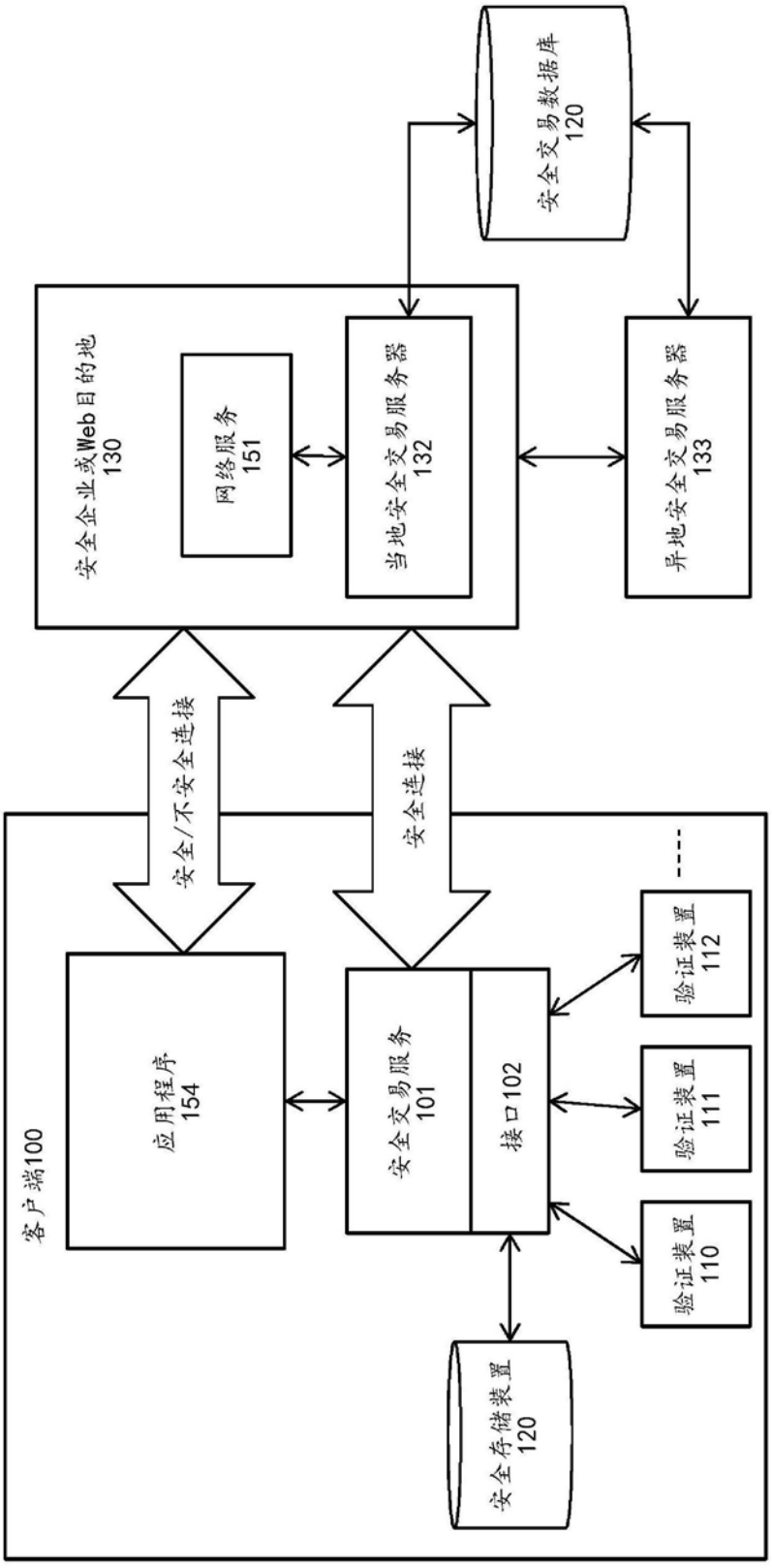

安全交易数据库
120
安全企业或Web目的地
130
网络服务
151
当地安全交易服务器
132
异地安全交易服务器
133
安全/不安全连接
安全连接
客户端100
应用程序
154
安全交易服务
101
接口102
验证装置
112
验证装置
111
验证装置
110
安全存储装置
120

图1B

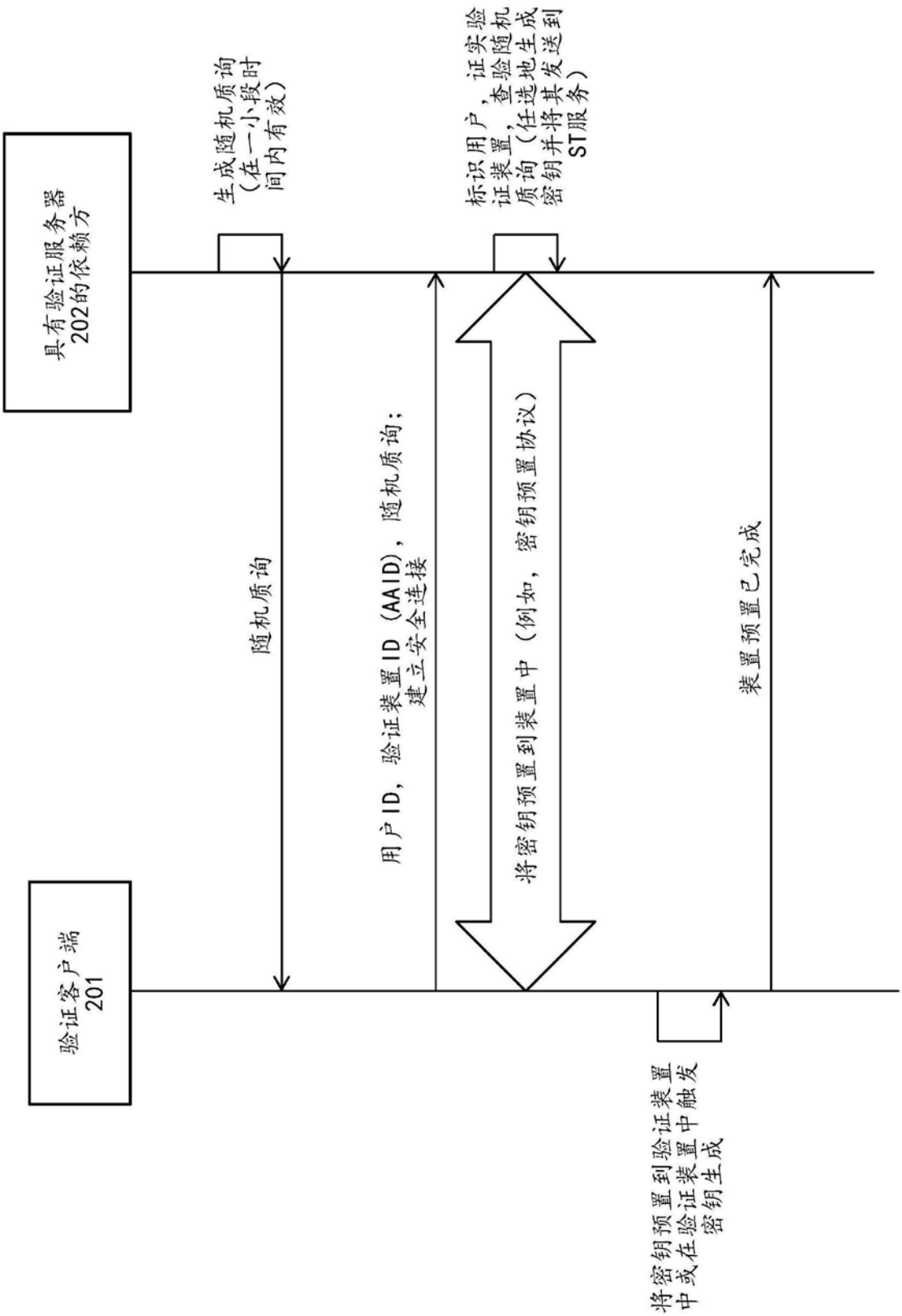

具有验证服务器
202的依赖方
验证客户端
201
生成随机质询
（在一小段时
间内有效）
随机质询
用户ID，验证装置ID（AAID），随机质询；
建立安全连接
标识用户，证实验
证装置，查验随机
质询（任选地生成
密钥并将其发送到
ST服务）
将密钥预置到装置中（例如，密钥预置协议）
装置预置已完成
将密钥预置到验证装置
中或在验证装置中触发
密钥生成

图2

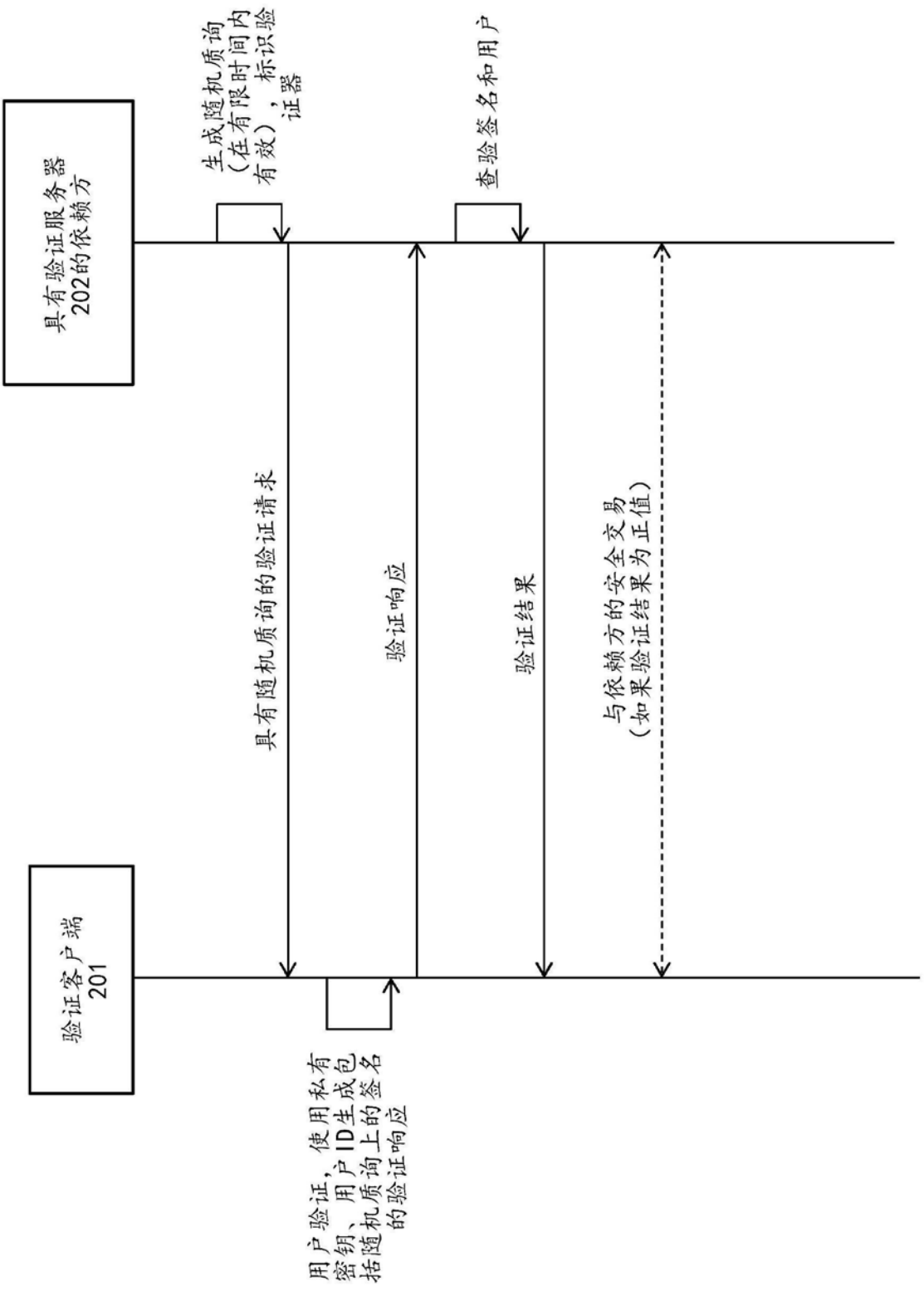

具有验证服务器
202的依赖方
验证客户端
201
生成随机质询
（在有限时间内
有效），标识验
证器
具有随机质询的验证请求
用户验证，使用私有
密钥、用户ID生成包
括随机质询上的签名
的验证响应
验证响应
查验签名和用户
验证结果
与依赖方的安全交易
（如果验证结果为正值）

图3

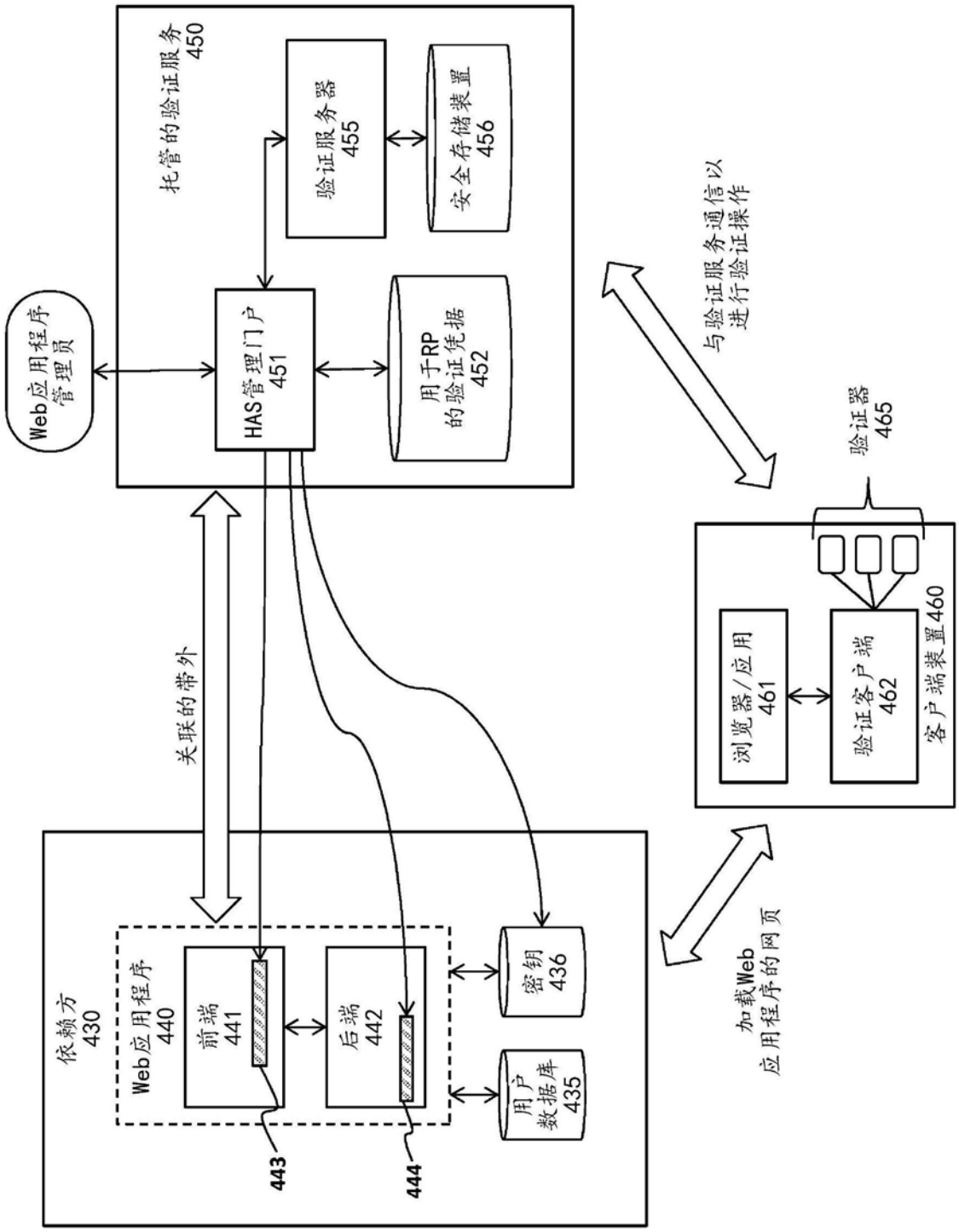

托管的验证服务
450
验证服务器
455
安全存储装置
456
Web应用程序
管理员
HAS管理门户
451
用于RP
的验证凭据
452
与验证服务通信以
进行验证操作
验证器
465
关联的带外
浏览器/应用
461
验证客户端
462
客户端装置460
依赖方
430
Web应用程序
440
前端
441
后端
442
密钥
436
用户
数据库
435
443
444
加载Web
应用程序的网页

图4

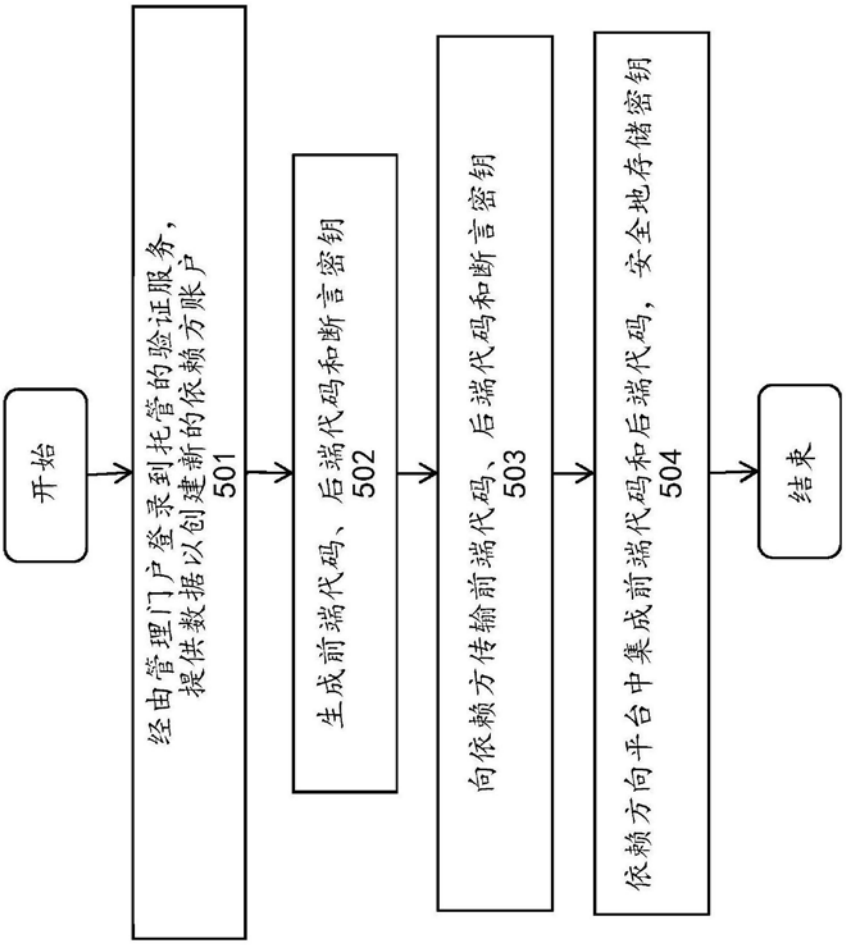

开始
经由管理门户登录到托管的验证服务，提供数据以创建新的依赖方账户
501
生成前端代码、后端代码和断言密钥
502
向依赖方传输前端代码、后端代码和断言密钥
503
依赖方向平台中集成前端代码和后端代码，安全地存储密钥
504
结束

图5

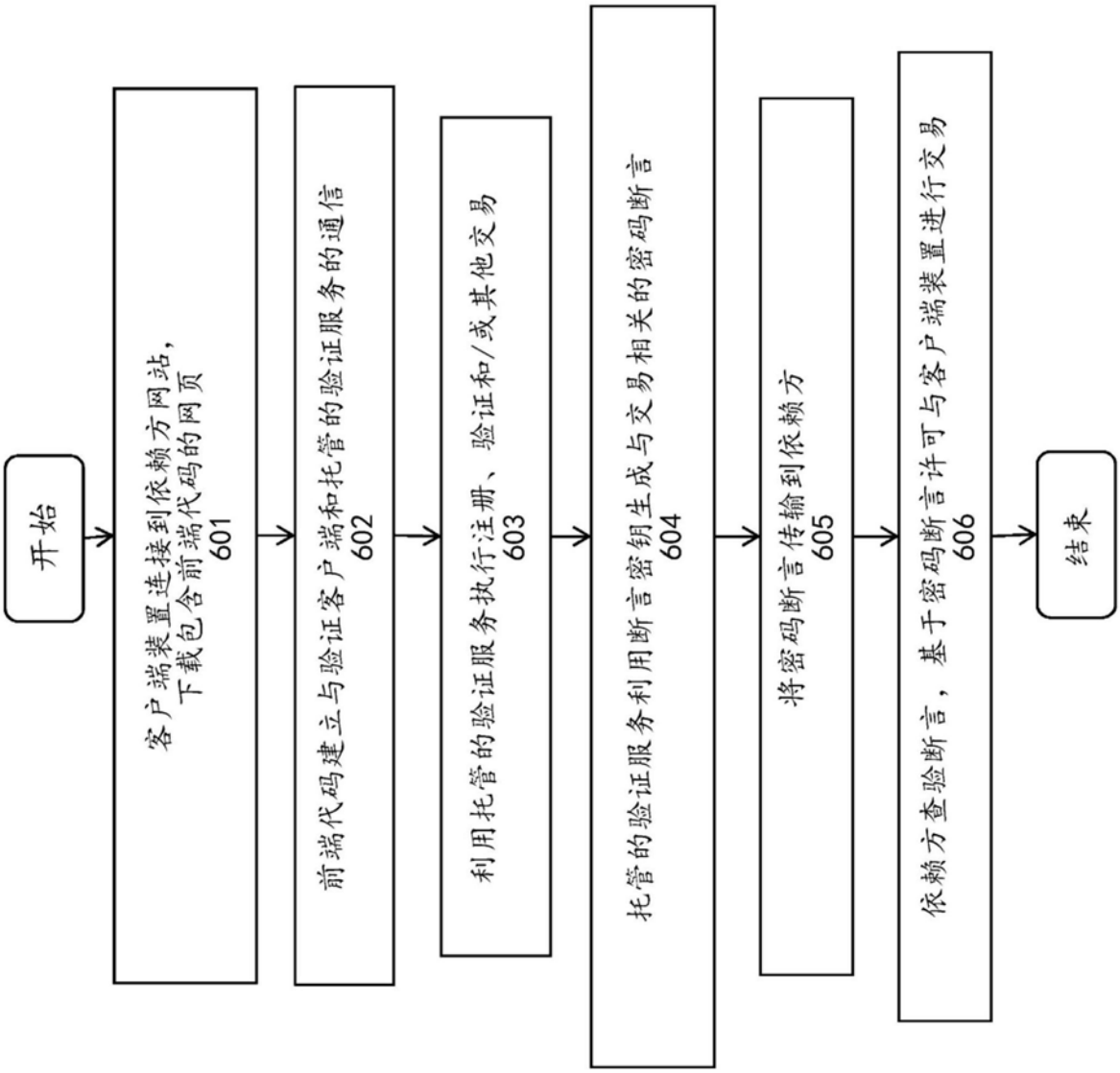

开始
客户端装置连接到依赖方网站，下载包含前端代码的网页
601
前端代码建立与验证客户端和托管的验证服务的通信
602
利用托管的验证服务执行注册、验证和/或其他交易
603
托管的验证服务利用断言密钥生成与交易相关的密码断言
604
将密码断言传输到依赖方
605
依赖方查验断言，基于密码断言许可与客户端装置进行交易
606
结束

图6

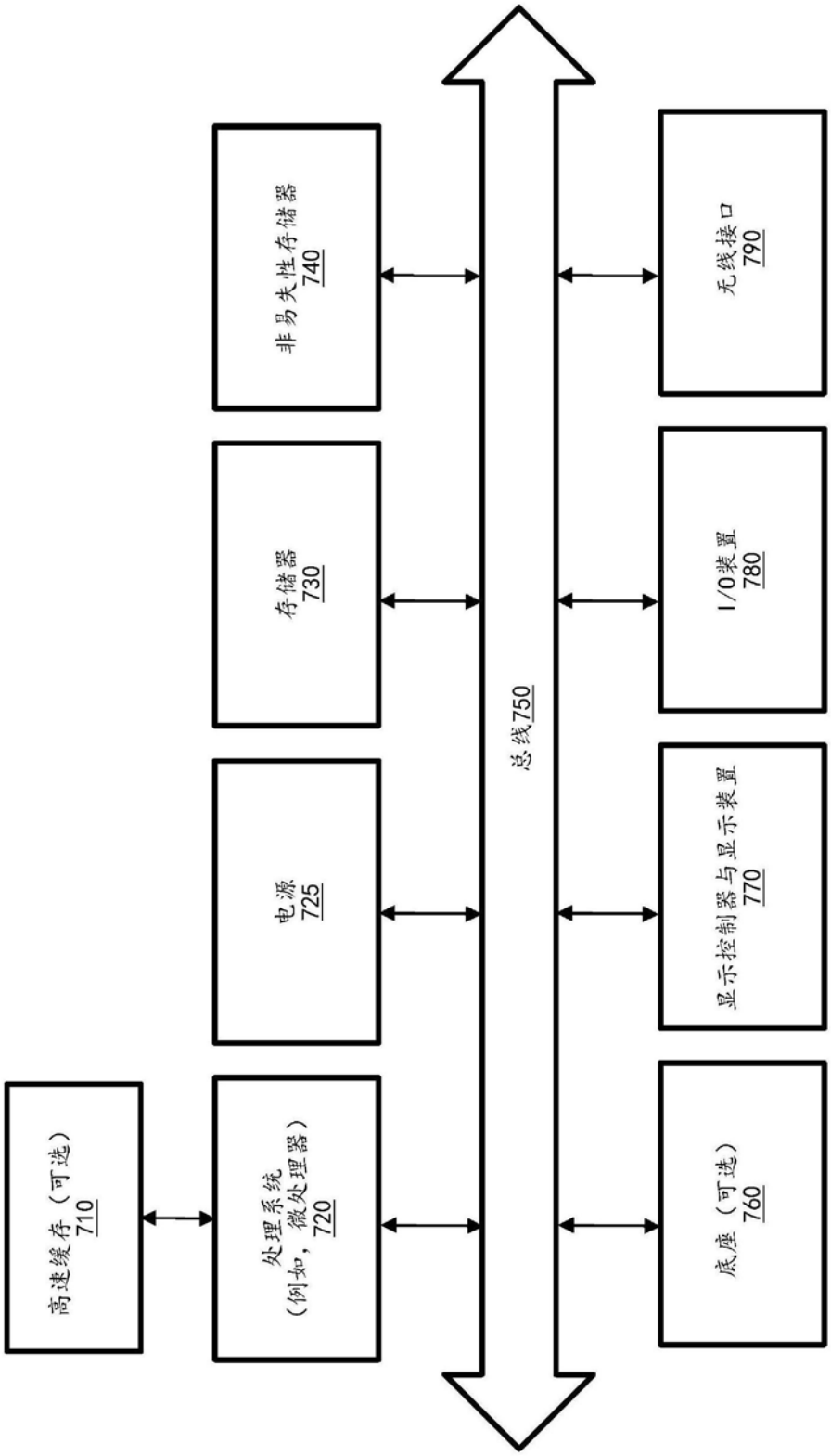

高速缓存（可选）
710
处理系统
（例如，微处理器）
720
电源
725
存储器
730
非易失性存储器
740
总线750
底座（可选）
760
显示控制器与显示装置
770
I/O装置
780
无线接口
790

图7

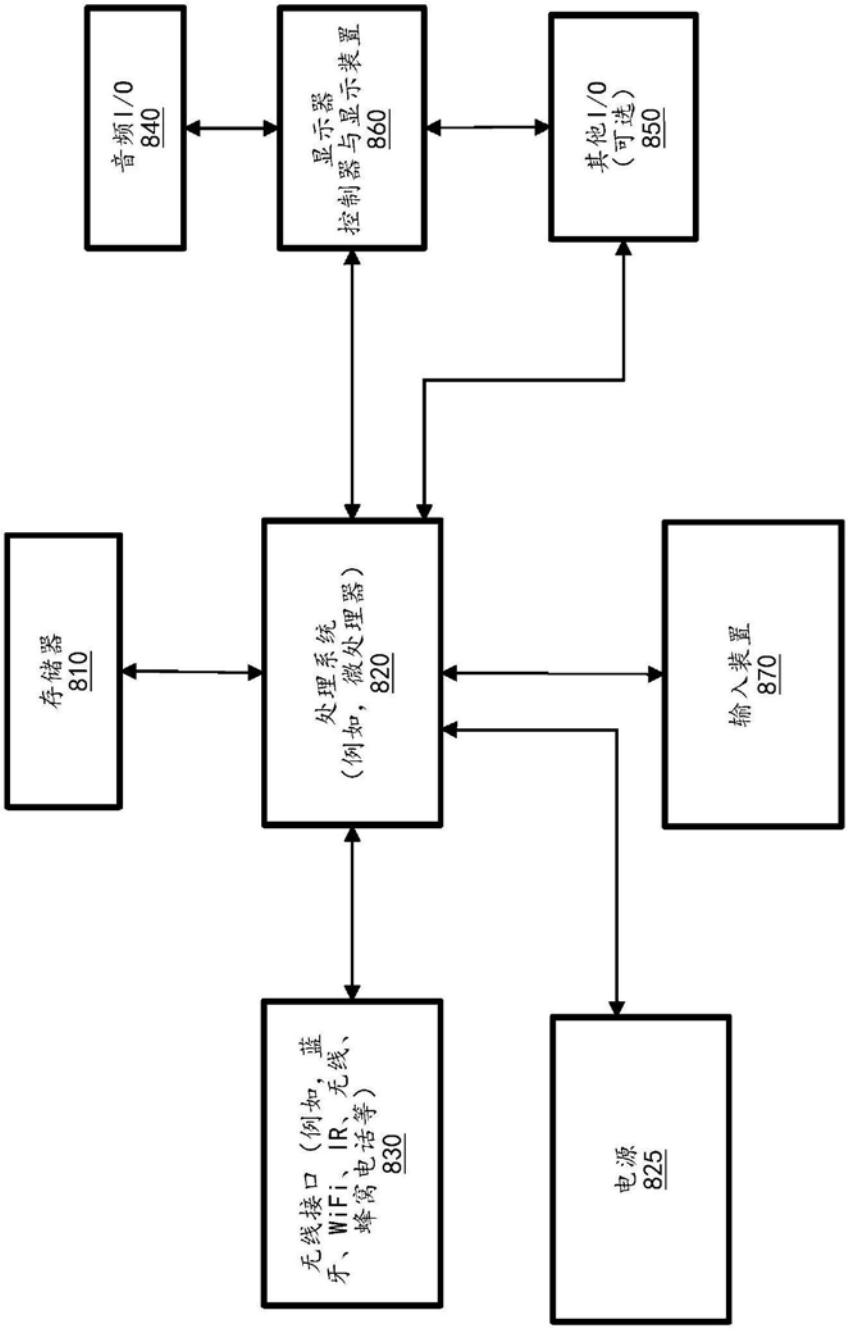

音频I/O
840
显示器
控制器与显示装置
860
其他I/O
（可选）
850
存储器
810
处理系统
（例如，微处理器）
820
输入装置
870
无线接口（例如，蓝牙、WiFi、IR、无线、蜂窝电话等）
830
电源
825

图8