(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111460406 B
(45)授权公告日 2023.11.14

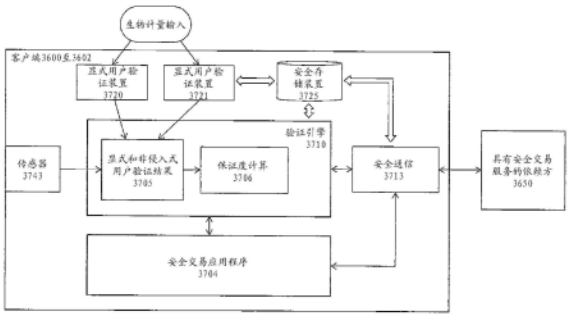
(21)申请号 202010235627.0
(22)申请日 2014.03.20
(65)同一申请的已公布的文献号
申请公布号 CN 111460406 A
(43)申请公布日 2020.07.28
(30)优先权数据
61/804,568 2013.03.22 US
14/066,384 2013.10.29 US
14/145,439 2013.12.31 US
14/145,466 2013.12.31 US
14/145,533 2013.12.31 US
14/145,607 2013.12.31 US
14/218,504 2014.03.18 US
(62)分案原申请数据
201480025959.9 2014.03.20
(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 M·布里赛尼奥 B·J·威尔逊
R·盖桑乌帕利 D·巴格达萨瑞安
R·多拉基亚 W·J·布兰克
R·林德曼 I·波利万伊
A·乌马
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
专利代理师 沈锦华
(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/32(2013.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)
(56)对比文件
EP 2343679 A1,2011.07.13
CN 1446331 A,2003.10.01
US 2009094164 A1,2009.04.09
US 2010235637 A1,2010.09.16
US 2011047608 A1,2011.02.24
US 5613012 A,1997.03.18
WO 03065169 A2,2003.08.07
审查员 甄红欣
权利要求书2页 说明书66页 附图66页

(54)发明名称

高级验证技术和应用

(57)摘要

本申请涉及高级验证技术和应用。例如,一种方法的一个实施例包括:接收识别一组可接受验证功能的策略;确定一组客户端验证功能;以及基于所述所确定的一组客户端验证功能来筛选所述一组可接受验证功能,以得出筛选出的一个或多个验证功能的组以用于验证所述客户端的用户。



CN 111460406 B

1.一种客户端装置,所述客户端装置包括:

一或多个验证器,所述验证器用于向依赖方验证所述客户端装置的用户,每一验证器包括多个验证组件,所述客户端装置内的所述验证组件中的每一者在所述验证器被使用的环境内执行不同的功能;以及

在所述客户端装置上的组件验证逻辑,所述组件验证逻辑用于在允许所述验证组件在所述客户端装置上组合以形成所述验证器之前向一个或多个其他验证组件证实所述多个验证组件中的至少一个验证组件的模型或完整性,其中向第二验证组件证实第一验证组件的模型或完整性包括:

从所述第二验证组件接收质询;

使用所述第一验证组件的密钥对所述质询生成签名或消息验证代码MAC;以及

由所述第二验证组件验证所述签名或MAC;以及

其中向所述依赖方验证所述用户包括:

读取来自用户的生物计量验证数据并基于与生物计量参考数据的比较而确定是否成功地验证所述用户;

建立与远程依赖方的通信;以及

与所述依赖方执行证实交易以通过以下操作向所述依赖方证实生物计量装置的模型和/或完整性:接收来自于所述依赖方的质询,使用证实密钥签署所述质询以生成签名,以及将所述签名发送至所述依赖方,其中所述依赖方使用所述依赖方的密钥验证所述签名是有效的。

2.根据权利要求1所述的客户端装置,其中所述验证组件包括验证用户的用户验证组件和建立与所述依赖方的安全通信的验证内核组件。

3.根据权利要求1所述的客户端装置,其中所述验证组件包括安全地向所述用户显示信息的显示组件和建立与所述依赖方的安全通信的验证内核组件。

4.根据权利要求1所述的客户端装置,其中所述密钥包括私有密钥且其中所述第二验证组件使用相应的公共密钥和所述质询来验证所述签名。

5.根据权利要求1所述的客户端装置,其中所述质询包括随机生成的随机数。

6.根据权利要求1所述的客户端装置,其中所述至少一个验证组件包括由所述组件验证逻辑管理的组件验证密钥CAK对,所述CAK对可用于证实所述至少一个验证组件的所述模型和/或完整性。

7.根据权利要求6所述的客户端装置,其中所述多个验证组件的每一验证组件包括由所述组件验证逻辑管理的CAK对,每一验证组件的所述CAK对可用于证实所述多个验证组件中除了该验证组件之外的每一者的模型和/或完整性。

8.根据权利要求1所述的客户端装置,其中所述验证器包括第一验证器,所述客户端装置进一步包括第二验证器,所述第二验证器与所述第一验证器共享所述多个验证组件中的至少一者。

9.根据权利要求8所述的客户端装置,其中所述验证组件包括验证用户的用户验证组件、安全地向所述用户显示信息的显示组件和建立与所述依赖方的安全通信的验证内核组件,其中至少所述验证内核组件在所述第一验证器和所述第二验证器之间是共享的。

10.根据权利要求1所述的客户端装置,其中所述组件中的至少一者作为可信应用程序

而执行,所述可信应用程序在所述客户端装置上的可信执行环境TEE中执行。

11.根据权利要求10所述的客户端装置,其中所述组件中的至少一者作为在所述客户端装置内定义的安全元件SE而执行。

12.根据权利要求11所述的客户端装置,其中所述组件中的至少一者使用可信用户接口而执行。

13.根据权利要求1所述的客户端装置,其中证实所述至少一个验证组件的所述模型和/或完整性使用直接匿名证实DAA方案来执行。

14.根据权利要求1所述的客户端装置,其中证实所述至少一个验证组件的所述模型和/或完整性进一步包括:检验包含至少一个组件的公共密钥的证书的撤销状态。

15.根据权利要求1所述的客户端装置,其中组件的不同组合经组合以形成不同的验证器,其中所述组件中的至少一些在验证器之间是共享的且其中所述不同的验证器中的每一者由所述依赖方使用唯一的验证器证实ID AAID码来识别。

16.根据权利要求1所述的客户端装置,其中不同的验证组件经组合以形成不同的验证器,其中所述不同的验证组件中的至少一些在验证器之间是共享的且其中所述不同的验证组件中的每一者由所述依赖方使用唯一的组件ID码来唯一地识别。

17.根据权利要求1所述的客户端装置,其中所述依赖方包括云服务。

18.根据权利要求1所述的客户端装置,其进一步包括:

客户端应用程序和/或浏览器以与所述依赖方建立远程通信,其中所述验证器使用经由所述客户端应用程序和/或浏览器建立的所述远程通信向所述依赖方验证所述客户端装置的所述用户。

高级验证技术和应用

[0001] 分案申请的相关信息

[0002] 本案是分案申请。该分案的母案是申请日为2014年03月20日、申请号为201480025959.9、发明名称为“高级验证技术和应用”的发明专利申请案。

技术领域

[0003] 本发明整体涉及数据处理系统的领域。更具体地讲,本发明涉及高级用户验证技术和相关联应用。

背景技术

[0004] 相关申请的交叉引用

[0005] 本申请要求2013年3月22日提交的名称为“Advanced Methods of Authentication And Its Applications”(高级验证方法及其应用)的共同待决的美国临时专利申请No.61/804,568的权益和优先权。

[0006] 本申请是2013年10月29日提交的名称为“Apparatus and Method For Implementing Composite Authenticators”(用于实施复合验证器的设备和方法)的美国专利申请14/066,384的部分继续申请。

[0007] 本申请还是2013年12月31日提交的名称为“System and Method For Non-Intrusive,Privacy-Preserving Authentication”(用于非侵入式隐私保护验证的系统和方法)的美国专利申请14/145,439的部分继续申请,该美国专利申请也要求2013年3月22日提交的名称为“Advanced Methods of Authentication And Its Applications”(高级验证方法及其应用)的共同待决的美国临时专利申请No.61/804,568的权益和优先权。

[0008] 本申请还是2013年12月31日提交的名称为“System and Method For Adaptive User Authentication”(用于自适应用户验证的系统和方法)的美国专利申请14/145,466的部分继续申请,该美国专利申请也要求2013年3月22日提交的名称为“Advanced Methods of Authentication And Its Applications”(高级验证方法及其应用)的共同待决的美国临时专利申请No.61/804,568的权益和优先权。

[0009] 本申请还是2013年12月31日提交的名称为“System and Method For Location-Based Authentication”(用于基于位置的验证的系统和方法)的美国专利申请14/145,533的部分继续申请,该美国专利申请也要求2013年3月22日提交的名称为“Advanced Methods of Authentication And Its Applications”(高级验证方法及其应用)的共同待决的美国临时专利申请No.61/804,568的权益和优先权。

[0010] 本申请还是2013年12月31日提交的名称为“System and Method For Confirming Location Using Supplemental Sensor and/or Location Data”(用于使用补充传感器和/或位置数据确认位置的系统和方法)的美国专利申请14/145,607的部分继续申请,该美国专利申请也要求2013年3月22日提交的名称为“Advanced Methods of Authentication And Its Applications”(高级验证方法及其应用)的共同待决的美国临时专利申请No.61/

804,568的权益和优先权。

[0011] 相关领域说明

[0012] 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)。

[0013] 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)。

[0014] 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:No.13/730,761,Query System and Method to Determine Authentication Capabilities(用于确定验证能力的查询系统和方法);No.13/730,776,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);13/730,780,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);No.13/730,791,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);No.13/730,795,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)。

[0015] 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、记录声音等等);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,如共同待决的申请中所描述)注册生物计量装置;并且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)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。

[0016] 验证器,诸如上文描述的那些验证器,需要某种形式的用户交互,如轻扫手指或输入密码。这些“普通”验证器旨在在给定时间点验证用户。另外,还可使用“无声”验证器在给

定时间点验证用户的装置(而非用户)。这些无声验证器可依赖于从用户的装置提取的信息,而不需要用户交互(例如,发送机器ID)。

[0017] 然而,在某些使用案例中,要求显式用户交互存在过多阻力(例如,近场通信(NFC)支付、要求验证但未绑定到高价值交易的频繁使用的应用程序),而"无声"验证技术(诸如发送机器ID)则不充分确定装置仍然由合法用户持有。

[0018] 研究团体已经提出了若干种"连续"验证方法,诸如Anthony J.Nicholson,"Mobile Device Security Using Transient Authentication","IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.5,NO.11,pp.1489-1502(November 2006)(Anthony,J,Nicholson.使用瞬时验证的移动装置安全。IEEE移动计算学报,2006-11,5(11):1489-1502);Mohammad O.Derawi,"Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition"(2010)(Mohammad O.Derawi,移动电话上使用生物计量步态识别的不醒目用户验证。2010);Koichiro Niinuma,Anil K.Jain,"Continuous User Authentication Using Temporal Information"(Koichiro,Niinuma,Anil,K,Jain.使用时间信息的连续用户验证。http://www.cse.msu.edu/biometrics/Publications/Face/NiinumaJain_ContinuousAuth_SPIE10.pdf)。工业上甚至已经采用这些方法中的一些,诸如BehavioSec,"Measuring FAR/FRR/EER in Continuous Authentication,"Stockholm,Sweden(2009)(BehavioSec.在连续验证中测量FAR/FRR/EER.瑞典斯德哥尔摩:2009)。这些方法总体上提供合法用户仍持有装置的保证等级而不会向验证过程增加阻力,但这些方法注重于单种形式(即,使用可穿戴的令牌、步态识别、面部和服装颜色识别,以及用户的键盘输入)。

[0019] 然而,存在的一个问题是,直接向依赖方提供位置数据或其他个人数据(例如,面部图像、服装颜色、步态或打字特征……)或环境数据(例如,温度、湿度、WLAN SSID…)以对风险评估进行补充的做法,在有些世界区域中侵犯了用户的隐私。因此,需要更高级的远程验证技术,这种技术既要具有非侵入式,又要充分保护最终用户的隐私。

[0020] 另外,当前验证方法(例如,密码、指纹验证等等)的强度随时间推移几乎恒定,但所导致的风险却基于执行验证的当前环境(例如,正在使用的机器、机器所连接到的网络等等)而变化。基于当前检测到的风险来选择并且/或者组合验证形式将是有利的。

[0021] 在考虑提高验证的保证等级时,我们想到了提高显式验证方法的等级的典型方法,如要求使用更复杂的密码,或者使用更准确的生物计量方法,如指纹或面部识别。实际上,验证的保证等级(或从其衍生的交易风险)还取决于其他数据,诸如是否从与之前相同的装置执行验证,以及验证的位置是否实际上靠近上次成功验证的位置(例如,下午1点在旧金山进行验证并且同一天下午2点在东京进行验证貌似对于一个人来说是不现实的)。

[0022] 密码仍是主要的显式验证方法。遗憾的是,密码容易受到攻击并且那些攻击伸缩自如。另外,输入密码是麻烦的,尤其是在如智能电话等小型装置上。因而,许多用户根本不使用基于密码的保护方法来锁定其电话,或者他们使用微不足道的PIN码。

[0023] 一些智能电话正使用指纹传感器来提供较便利的验证方式。使用生物计量形式来进行验证已经因为不能提供足够的抗欺骗攻击能力以及由于可能无法恰当保护生物计量参考数据而引入的隐私问题而受到诟病。

[0024] 目前已经提出了结合使用多种生物计量形式的各种"融合"方法。其中,有些方法

通过降低错误拒绝率(FRR)来解决可用性问题;有些方法通过降低错误接受率(FAR)来解决安全性问题。因而,这些方法目前已经提出了静态融合算法。遗憾的是,这种方式仍然导致保证等级视“其他输入”(如上文所述)而变化。

[0025] 对于某些类别的交易,与交易相关联的风险性可能与正在执行交易的位置密不可分。在其他情况下,可能仅期望在使用更强验证机制的情况下允许进行交易;例如,从公司的物理场所内进行的交易所需的验证可能比从位于公司没有业务的偏远地区的星巴克进行的交易要少。

[0026] 然而,出于多种原因可能不易得到可靠的位置数据。例如,最终用户的装置可能没有GPS能力;用户可能位于Wifi三角测量数据不可用或不可靠的位置;网络提供商可能不支持提供手机发射塔三角测量能力来增强GPS或WiFi三角测量能力。用于推断装置位置的其他方法可能没有足够的保证等级来满足组织的需要;例如,用于确定地理位置的反向IP查找可能粒度不够,或者可能被设计用于掩蔽用户装置的真实网络起源的代理掩蔽。

[0027] 在这些情况下,设法评估交易风险性的组织可能需要额外数据为自己提供关于个人位于特定地理区域内的额外保证,以推动验证决策。

[0028] 组织部署验证的另一个挑战是,使验证机制的“强度”与特定用户的环境(位置、装置、软件、操作系统)、用户或装置做出的请求(对访问受限信息或进行特定操作的请求)以及组织的管理策略所呈现的内在风险匹配。

[0029] 目前为止,组织不得不依赖于对用户验证需要的相当静态的响应:组织评估用户在正常执行的操作期间将面临的风险,以及任何适用法规的强制规定,然后部署验证方案来防御风险并实现合规。要做到这一点,组织通常需要部署多种验证方案来解决不同用户可能面临的多种多样的风险,而这可能管理起来特别昂贵并且麻烦。

[0030] 共同待决的申请中所描述的技术提供允许组织识别用户装置上能够用于验证的现有能力的抽象概念。这个抽象概念使组织不需要部署多种不同验证方案。然而,组织仍需要用于在必要时调用“正确”验证机制的方式。现有的具体实施未向组织提供描述什么验证机制在哪些情况下适用的能力。因此,组织将有可能需要将其验证策略编纂成代码,而这使得解决方案脆弱不堪,并且需要在将来改变代码才能使用新的验证装置/令牌。

[0031] 如今,主要使用浏览器应用程序通过万维网进行电子金融交易。Amazon.com、戴尔和沃尔玛等网站经由其在线门户网站出售数十亿美元的商品,而银行和经纪机构允许其客户在帐户之间在线转移数十亿美元的资金。这些网站等所面临的一个挑战是,如何检测欺诈活动。欺诈交易可能使这些公司损失数十亿美元。

[0032] 对付欺诈交易的第一道防线是用户的密码。然而,罪犯可通过多种技术获得密码。有时,密码的复杂性不够,并且可易于通过暴力攻击来猜中或确定。而有时,恶意软件、蠕虫或病毒会使用户的计算机受到感染。于是,可通过记录按键或者扫描存储器或硬盘存储装置来获得密码。如果实际装置被偷走,则可从保留在存储器或存储装置中的数据找回密码。一旦密码泄露,罪犯就能够访问帐户并且提取或转移资金。

[0033] 为了设法防止因用户密码被攻破而造成损失,处理金融交易的网站采用了风险评估,在风险评估中,使用了各种度量来确定发起交易的人员是否实际上是拥有该帐户的用户。交易时间、交易位置和交易环境等因素都是评估交易是否有风险的良好方式。例如,如果用户通常不在晚上使用帐户进行任何活动,则与下午3:00相比,将较不可能在凌晨3:00

发起交易。同样，如果用户生活在美国，但在韩国发起交易，则这种位置差异将是一种警告标志。最后，如果正在处理的金额在量值上明显不同于往常，则这也是潜在欺诈的另一个信号。

[0034] 遗憾的是，Web浏览器对网站能够获得客户端系统的什么信息设置了非常严格的限制。因为浏览器将用户的机器暴露到外部(并且可能是恶意的)世界，所以泄漏非必要的任何数据都会对其自身造成安全风险。当然，记录交易时间、交易位置(例如，经由用户的IP地址)和交易量值是可行的。网站当前使用所有这些数据来确定交易是否具有欺诈性。然而，除了浏览器所提供的这些基本信息片段之外，网站没有其他信息来用于风险评估。由于对浏览器能够获得什么信息的限制，对用户交易的风险评估不是非常精确。

发明内容

[0035] 在至少一个方面，本申请涉及一种客户端装置，所述客户端装置包括：一或多个验证器，所述验证器用于向依赖方验证所述客户端装置的用户，每一验证器包括多个验证组件，所述客户端装置内的所述验证组件中的每一者在所述验证器被使用的环境内执行不同的功能；以及在所述客户端装置上的组件验证逻辑，所述组件验证逻辑用于在允许所述验证组件在所述客户端装置上组合以形成所述验证器之前向一个或多个其他验证组件证实所述多个验证组件中的至少一个验证组件的模型或完整性，其中向所述依赖方验证所述用户包括：读取来自用户的生物计量验证数据并基于与生物计量参考数据的比较而确定是否成功地验证所述用户；建立与远程依赖方的通信；以及与所述依赖方执行证实交易以通过以下操作向所述依赖方证实生物计量装置的模型和/或完整性：接收来自于所述依赖方的质询，使用证实密钥签署所述质询以生成签名，以及将所述签名发送至所述依赖方，其中所述依赖方使用所述依赖方的密钥验证所述签名是有效的。

附图说明

[0036] 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：

[0037] 图1示出配备有生物计量装置的示例性客户端；

[0038] 图2示出非侵入式隐私保护验证器(NIPPA)的一个实施例；

[0039] 图3用图形示出在“合法用户状态”期间和在合法用户状态之后的本发明的一个实施例的操作；

[0040] 图4示出非侵入式隐私保护验证方法的一个实施例；

[0041] 图5示出一个实施例中用于基于位置的验证的距离函数；

[0042] 图6用图形示出使用扩展合法用户状态窗口的本发明的一个实施例的操作；

[0043] 图7示出根据本发明的一个实施例的自适应验证模块；

[0044] 图8示出自适应验证方法的一个实施例；

[0045] 图9用图形示出根据一个实施例的自适应验证；

[0046] 图10示出具有多个组件的复合验证器的一个实施例。

[0047] 图11示出两个验证器共享组件的一个实施例。

[0048] 图12示出包括管理用于验证组件的组件验证密钥(CAK)对的组件验证逻辑的验证器的一个实施例。

[0049] 图13示出事务图,其示出了两个组件之间的验证的一个实施例。

[0050] 图14示出根据本发明的一个实施例的静态验证器。

[0051] 图15示出根据本发明的一个实施例的动态验证器。

[0052] 图16示出其上可实施本发明实施例的示例性系统架构。

[0053] 图17示出用于执行验证策略的位置感知应用程序的系统的一个实施例;

[0054] 图18示出一组示例性验证策略规则;

[0055] 图19示出根据本发明的一个实施例的方法;

[0056] 图20示出本发明的一个实施例,其中由其他对等装置或网络装置的接近性确定或确认位置;

[0057] 图21示出使用环境传感器的验证系统的一个实施例;

[0058] 图22示出使用环境传感器的验证方法的一个实施例;

[0059] 图23示出用于自适应地应用验证策略的系统的一个实施例;

[0060] 图24示出用于自适应地应用验证策略的方法的一个实施例;以及

[0061] 图25示出配备有生物计量装置的示例性客户端;

[0062] 图26示出包括眼动跟踪模块和面部识别模块的验证引擎的一个实施例;

[0063] 图27示出本发明的一个实施例中所采用的网页的示例性热图;

[0064] 图28A至图28B示出可向最终用户显示的示例性文本、图形、照片、视频、空白区域和其他内容;

[0065] 图29示出用于执行基于眼动跟踪和面部识别的验证的方法的一个实施例;

[0066] 图30示出可在其中实施本发明实施例的不同架构布置。

[0067] 图31示出包括客户端风险评估代理的客户端架构的一个实施例;

[0068] 图32示出客户端风险评估代理使用的示例性类型的客户端配置数据;

[0069] 图33示出用于在验证期间执行客户端风险评估的方法的一个实施例;

[0070] 图34示出执行与本地装置的安全交易的客户端的一个实施例;

[0071] 图35示出用于执行与本地装置的安全交易的客户端架构的一个实施例;

[0072] 图36示出用于执行与本地装置的安全交易的方法的一个实施例;

[0073] 图37示出用于在线交易用户确认的系统的一个实施例;

[0074] 图38示出在用于在线交易用户确认的系统中所使用的客户端的一个实施例的细节;

[0075] 图39示出用于在线交易用户确认的方法的一个实施例;

[0076] 图40示出用于从可信客户端装置向新客户端装置委托信任的系统的一个实施例;

[0077] 图41示出用于从可信客户端装置向新客户端装置委托信任的系统的一个实施例的额外细节;

[0078] 图42示出用于从可信客户端装置向新客户端装置委托信任的方法的一个实施例;

[0079] 图43示出用于在装置之间同步专用数据的系统的一个实施例;

[0080] 图44示出用于将装置添加到信任圈的方法的一个实施例;

[0081] 图45示出用于在装置之间同步数据的方法的一个实施例;

[0082] 图46A至图46B示出可在其中实施本发明实施例的不同示例性架构布置。

[0083] 图47是示出可如何发现客户端装置上的验证装置的事务图。

[0084] 图48是示出用户可如何向验证装置登记的事务图。

[0085] 图49是示出可如何将密钥注册到验证装置中的事务图。

[0086] 图50是示出可如何在验证框架内实施用户验证的事务图。

[0087] 图51是示出可如何验证交易细节的事务图。

[0088] 图52示出根据本发明的一个实施例实施的查询策略筛选器。

[0089] 图53是示出如何在本发明的一个实施例中实施查询策略的注册操作的事务图。

[0090] 图54示出用于实施多个验证装置处理的架构的一个实施例。

[0091] 图55A至图55C示出用于多验证装置处理的本发明的三个实施例。

[0092] 图56A至图56B示出用于检测随机质询超时并对其做出响应的事务图。

[0093] 图57示出根据本发明的一个实施例的用于实施隐私类别的架构。

[0094] 图58是根据本发明的一个实施例的用于实施隐私类别的事务图。

[0095] 图59示出用于使用签名验证交易的架构的一个实施例。

[0096] 图60至图61示出用于执行本发明实施例的计算机系统的示例性实施例。

具体实施方式

[0097] 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。

[0098] 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。

[0099] 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“远离”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，生物计量传感器未与依赖方计算机嵌入到相同的物理外壳中)。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。

[0100] 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。

[0101] 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)。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。

[0102] 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。

[0103] A.非侵入式隐私保护验证

[0104] 本发明的一个实施例使用“普通”验证技术(例如,轻扫手指、输入代码等)来训练验证系统识别非侵入式验证情形。另外,一个实施例在需要验证时向依赖方返回装置的验证状态,而非诸如机器ID等敏感信息。

[0105] 下文描述的本发明的一些实施例可完全无阻力地工作(即,不需要任何显式用户验证)。可利用行为技术或其他技术来连续测量指示装置由经授权用户持有的当前保证的保证等级。可例如基于自从上次显式用户验证(例如,使用PIN或手指轻扫进行SIM卡或电话解锁)以来已经过去的时间来计算保证等级。假设已经过去的时间量在特定阈值(例如,5秒、5分钟、1小时等)内,则装置可被视为处于“合法用户状态”并且保证等级被设为最大值(例如,在-100到100的标准化尺度下为100)。

[0106] 在合法用户状态之后,可基于自从显式用户验证以来过去的时间与指示装置由经授权用户持有的其他变量(例如,基于从装置传感器检测到的非侵入式输入)的组合来测量保证等级。例如,可使用加速度计或其他类型的传感器以及被设计为从用户的正常步行模式生成步态“指纹”的软件和/或硬件,来测量用户的生物计量步态。另外,可跟踪、存储距合法用户的常去目的地的距离并且随后用于确定保证等级。例如,如果用户正从已知为用户的家或办公室的位置连接到依赖方,则保证等级可被设为相对较高的值,而如果装置正从未知位置或遥远的位置连接,则保证等级可被调整到较低等级。

[0107] 可执行各种其他类型的非侵入式测量来确定装置是否由经授权用户持有,包括(例如)客户端装置所连接到的网络或装置的身份,诸如蓝牙装置、近场通信(NFC)装置、Wifi装置(诸如路由器或接入点)、智能手表、其他计算装置、Nymi手环,等等。Wifi装置可包括够得着的Wifi网络的可见性,诸如家中的个人Wifi路由器,以及同事或家庭成员使用的具Wifi功能的计算机。另外,可利用客户端装置的某些特定特征(诸如加速度传感器特征和数码相机传感器图案噪声)来进行非侵入式测量。还可分析正常用户交互的触摸屏手势并将其存储为参考数据,并且可以分析正常用户交互时的用户打字行为并将其存储为参考数据。当然,前述内容仅仅是几个例子;本发明的基本原理不限于任何的非侵入式变量组。

[0108] 最终结果是可在验证响应中将合法用户仍持有装置的保证等级发送到依赖方。在一个实施例中,通过密钥(例如,在注册阶段中建立并证实的依赖方特定密钥,如下文论述)“签署”或以其他方式验证保证等级。在一个实施例中,保证等级被标准化为-100到100之间的值,其中-100意味着“几乎确定其不是合法用户”,0意味着“不知道”,100意味着“几乎确

定其是合法用户”。

[0109] 在一个实施例中，如果保证等级对于预期交易是不可接受的，则依赖方可要求客户端装置使用额外的“普通”验证器响应。不管要求什么等级的验证，有一个实施例不向依赖方公开个人数据，而是使用专用于一个特定依赖方的密码密钥来向依赖方验证验证器。

[0110] 图2中示出用于提供非侵入式隐私保护验证的架构的一个实施例，该架构包括非侵入式隐私保护验证器(NIPPA)210，而非侵入式隐私保护验证器(NIPPA)210包括用于基于来自非侵入式验证机制230(例如，位置、步态测量等)和一个或多个显式用户验证装置220至221(例如，指纹传感器、用于输入ID代码的输入装置等)的输入来确定当前保证等级的保证度计算器212。在一个实施例中，显式用户验证装置220至221包括如图1所示的相同或相似架构。

[0111] 在图2所示的实施例中，非侵入式验证230包括位置验证模块231，这个模块用于使用位置传感器241以及存储在用户/位置数据存储装置245(例如，其可被实施为文件系统或数据库)内的历史位置数据或用户指定的位置数据执行基于位置的验证。以举例而非限制的方式，位置传感器241可包括GPS装置和/或用于检测客户端200所连接到的当前接入点或手机发射塔(其可用于估计装置的当前位置)的模块。可使用能够提供与用户的位置相关的数据的任何传感器。位置验证模块231确定客户端装置的当前位置对保证等级的影响。例如，如果装置当前位于“家”或“办公室”位置(根据历史位置数据或用户指定的位置数据245)，则可上调保证等级；而如果装置当前位于遥远的未知位置，则可下调保证等级。除了在一个实施例中在“合法用户状态”期间自动训练系统(如本文描述)之外，用户具有将某些位置手动指定为“可信”并且因此具有高保证等级(例如，当用户在家或在办公室时)的能力。位置验证模块231的结果提供到保证度计算模块212，在保证度计算模块212中，可以将位置验证模块231的结果计入到当前保证等级计算中。

[0112] 用户行为验证模块232依赖于一个或多个用户行为传感器242来确定当前用户行为与历史用户行为(存储在用户与位置数据存储装置245中)一致的程度。例如，用户行为传感器242可提供加速度计测量值，用户行为验证模块可使用加速度计测量值来确定当前持有装置200的用户的步态。之后，用户行为验证模块可将这些测量值与用户的已知步态(在先前显式用户验证之后收集并且存储在存储装置245中)进行比较，得出合法用户持有装置的置信等级。结果提供到保证度计算模块212，然后在保证度计算模块212中计入到当前保证等级计算中。

[0113] 各种其他/额外验证装置233可从其他/额外传感器243收集数据以执行验证计算，验证计算的结果提供到保证度计算模块212，以计入在当前保证等级计算中。

[0114] 虽然在图2中示出为单独模块，但位置验证模块231、用户行为模块232和任何其他验证模块233可形成保证度计算模块212的一部分。本发明的基本原理可使用模块的各种不同逻辑布置来实施。

[0115] 如图所示，在一个实施例中，保证度计算模块212在测量自从上次显式用户验证以来已经过去的时间量时依赖于计时器211。如下文详细的论述，自从上次显式用户验证以来已经过去的时间量可用于确定装置当前是否处于“合法用户状态”并且相应地调整保证度测量值。

[0116] 一旦保证度计算模块212得出当前保证度测量值，其便可将测量值传送到经由安

全通信模块213建立的依赖方(在一个实施例中为云服务)。例如,每个验证器220至221(包括非侵入式验证器230)可在注册操作(在验证之前)中交换依赖方特定的且经过证实的密钥。在验证操作中返回的保证等级可为通过依赖方特定的验证密钥签署/加密的消息的一部分。另外,如下文论述,该消息还可包括由依赖方生成的随机数(例如,随机质询)。

[0117] 在一个实施例中,安全存储装置225是被提供用于存储与每个验证器相关联并且被安全通信模块213用于与依赖方建立安全通信的验证密钥的安全存储装置。

[0118] 如所提及的,在一个实施例中,NIPPA 210利用现有(显式)用户验证技术(例如,基于密码的系统登录、SIM卡解锁等)在每次此类成功验证之后的定义时间窗(多达T1秒)内维持“合法用户”状态。NIPPA 210可从各种传感器241至243周期性地测量用户行为,并且在处于“合法用户”状态时,NIPPA 210可根据测量值更新其内部参考数据向量。在未处于“合法用户”状态时,NIPPA 210可基于当前测量值来计算距参考数据向量的标准化“距离”。这个“距离”被视为合法用户仍持有验证器的确定性。

[0119] 当被要求验证用户时,NIPPA 210可检查确定其是否处于“合法用户”状态。如果是,则视为验证成功并且返回最大保证等级(例如,100)。如果未处于“合法用户”状态,则NIPPA 210可返回由保证度计算模块212基于最新测量值计算出的保证等级。NIPPA 210可接着组合保证等级和相应测量值tm与当前时间tc的时间差td(td＝tc-tm)。在一个实施例中,这个过程使用以下逻辑来完成:

[0120] (1)如果(保证等级>＝0),则所得保证等级＝保证等级*(最大(T0-td,0)/T0),其中T0是最大可接受时间差;以及

[0121] (2)如果(保证等级<0),则所得保证等级＝保证等级。

[0122] 图3中示出根据以上公式的本发明的一个实施例的操作。在时间t1处,用户执行显式验证(例如,轻扫手指、输入PIN以解锁SIM卡等)。直到t1+T1的时间窗被视为“合法用户”状态。如所提及的,可在合法用户状态内训练非侵入式验证器。例如,可测量用户的步态,并且/或者可记录用户所访问的位置并且随后用于执行非侵入式验证。

[0123] 在时间t2(未处于合法用户状态)处,保证度计算模块212基于非侵入式验证器来计算保证等级。所得结果为正值,这代表装置有可能在合法用户的完全控制下。在这个计算之后,保证等级随时间推移而降低(例如,合法用户可能将装置暴露给了非合法人员)。例如,在时间t3处,保证等级已经比时间t2处的值显著变小。在一个实施例中,仅周期性计算非侵入式保证等级,以免消耗过多的功率和CPU性能。

[0124] 在t5处,发生另一个非侵入式保证等级计算。此时,所得结果为负,这代表装置有可能不在合法用户的完全控制下。这个负保证等级直到基于非侵入式验证器来执行另一个计算(例如,在时间t6处)时才发生改变。

[0125] 图4至5中示出根据一个实施例的方法。该方法可在诸如图2所示的系统架构等系统架构内实施,但不限于任何特定系统架构。

[0126] 在401处,发生显式验证事件,诸如在指纹传感器上轻扫手指或输入PIN以解锁装置。还可启动计时器来测量自从显式验证事件以来已经过去的时间。在402处,进入合法用户状态;在403处,可测量用户行为的各个方面并存储下来以供以后参考(例如,位置、用户步态等)。如果在404处确定在合法用户状态期间发生了验证请求(例如,从与依赖方的交易产生),则在405处选择最大保证等级并且在420处发送到依赖方。

[0127] 在406处，系统退出合法用户状态(例如，因为计时器指示已经过去指定的时间量)。在407处，系统周期性地通过将来自传感器的数据与在操作403中存储的内部参考数据进行比较来测量用户行为。举例来说，可将与用户步态相关联的测量值(在处于合法用户状态时收集)与当前步态测量值(在407处收集)进行比较，并且可计算两者之间的相关性(称为距参考数据的“距离”)。如果在408处确定在未处于合法用户状态时收到验证请求，则在409处，基于距内部参考数据的距离并且可能基于自从显式验证事件以来的时间来计算当前保证等级。接着在420处将保证等级传输到依赖方。

[0128] 转到图5，如果在501处确定传输到依赖方的保证等级对于与用户的当前交易为可接受的，则依赖方可向客户端装置发送指示验证成功的响应。如果不可接受，则在503处，依赖方可向客户端发送指示需要额外验证的响应(例如，如果非侵入式验证不充分，则有可能需要显式用户验证)。

[0129] 在替代实施例中，依赖方可最初指定特定交易所需要的保证等级，并且系统将确保满足所需要的保证等级，在非侵入式验证技术不充分的情况下系统有可能使用显式用户验证来确保。之后，系统可向依赖方发送验证成功的指示(而非保证等级)。

[0130] 如上所述，本发明的一个实施例计算距一组已知用户位置的距离以确定保证等级。参见图6，可使用基于位置的测量值(例如，诸如GPS)来如下地计算“距离”函数。

[0131] 在预处理操作中，所有测量位置(Ln)都会分配给其最近的“区域”。区域被定义为具有半径r(例如，10米)的圆圈。这些区域被设置为使得用最小数量的区域覆盖所有Ln。从区域集合中移除覆盖少于M个位置的所有区域(即，因为这些位置不被视为用户的“频繁”位置)。

[0132] 接着使用“距离＝(当前位置(Lc)到区域(Rn)的最近中心的距离)/r”来确定“距离”(d)，其中r是区域的半径。如果Lc在现有区域内，则这个值小于或等于1；如果Lc在外部，则这个值可变得很大。接着使用下式计算保证等级：保证等级＝最大(100-50*floor(d)，-100)；保证等级的值在-100至100的范围内。

[0133] 在有些上述实施例中，假设的是合法用户在显式验证之后的特定时间窗内仍持有客户端装置，或者假设当前行为非常类似于测得的行为。然而，上述实施例仅在显式验证之后的特定时间窗内更新行为参考数据。

[0134] 如图7所示，本发明的一个实施例除了合法用户状态的标准时间窗之外，还使用扩展时间窗来更新行为参考数据(即，训练系统)。因而，可如下地定义整个时间窗(包括标准时间窗和扩展时间窗)：(1)如果在成功显式用户验证之后的合法用户状态时间窗(即，t1...t1+T1)内，或(2)如果返回的保证等级将高于某个阈值T(例如，T＝90，在例如t2、t4等处)。将阈值设为0是不合需要的，因为这将使得攻击者很容易将行为参考“转变”为对他有利。

[0135] B.自适应验证技术

[0136] 图8示出用于实施自适应验证技术的本发明的一个实施例。如在上文论述的实施例中，这个实施例包括一个或多个用于执行非侵入式验证(例如，基于位置、所感测到的用户行为等)的非侵入式验证模块230，以及一个或多个用于执行显式用户验证(例如，需要PIN、指纹扫描等)的显式验证模块222。另外，如在先前的实施例中，保证度计算模块212基于(例如)自从上次显式验证以来的时间(由计时器211提供)和/或由各种验证模块230、222

提供的验证数据来计算保证度。安全通信模块213建立与依赖方250的安全通信(例如,使用安全加密密钥,如上文论述)。

[0137] 在一个实施例中,自适应验证模块800动态地在可用的非侵入式验证技术和显式/侵入式验证技术当中进行选择以得出对于与依赖方250的当前交易而言足够的保证等级。或者,或另外,依赖方250上的自适应验证模块810可执行验证选择技术来得出足够的保证等级。不管是在客户端装置200上(通过自适应验证模块800)还是在依赖方250上(通过自适应验证模块810)实施验证选择技术,本发明的基本原理仍然相同。

[0138] 此外,图8所示的"依赖方"250可表示可信第三方服务器,可信第三方服务器可代表依赖方实施本文所述的验证技术并且将结果提供给依赖方。因此,尽管以"依赖方"描述本发明的实施例,但本发明的基本原理可使用在由依赖方操作的网络的周界之外的服务器来实施。

[0139] 如下文更详细的论述,在一个实施例中,自适应验证模块810包括风险引擎812以基于与客户端装置相关联的变量(例如,基于当前IP地址、IP包往返延迟时间等)来确定风险等级。另外,保证等级增益分析组件811可确定要得到可接受的保证等级必须将当前保证等级增加的量。尽管图8中将这些元件示出为依赖方的自适应验证模块810的组件,但这些元件还可在同时仍符合本发明的基本原理的情况下在客户端的自适应验证模块800内实施。

[0140] 在一个实施例中,一旦客户端装置200连接到依赖方250(例如,以发起交易),风险引擎812便基于当前可用的所有数据来确定风险(或保证等级)。可用数据可包括,例如客户端装置200的地理位置(例如,从IP地址得出或由移动网络运营商提供)、在客户端装置200与依赖方250之间传输的包的往返延迟时间、在客户端装置200与依赖方250之间发送的网络包的跳数、由在客户端装置200上执行的用户代理发送的特定"用户代理"字符串,等等。在一个实施例中,风险引擎812接着评估这些数据以得出隐式"风险得分"(或与风险得分负相关的初始保证等级),这一得分可用于确定针对给定交易验证用户所需要的额外保证度的量。

[0141] 在一个实施例中,基于隐式风险得分,依赖方810或客户端装置800上的自适应验证模块确定一组有可能使整体保证等级增大到预期交易所需要的等级(即,当与初始保证等级/隐式风险得分组合时)的一个或多个验证模块222、230。在一个实施例中,保证等级增益分析模块811确定所需要的增益,并且自适应验证模块800、810获得关于所需保证等级增益的指示以作为参数。自适应验证模块800、810接着使用这个"增益"参数来确定一组最便利的验证技术(非侵入式230和/或显式222)以便实现(至少)所需的增益。自适应验证模块800可在对依赖方250的响应中加入对选定验证技术组的形式描述(例如,作为经验证的扩展)。依赖方250可接着验证所得的整体保证等级是否满足所需等级。

[0142] 以举例而非限制的方式,自适应验证模块800可组合多种验证形式,诸如装置指纹识别(例如,识别传感器缺陷或相机传感器图案噪声);环境信息(例如,基于GPS的位置;从WIFI网络得出的位置;到其他小配件(如Nymi)、智能手表(pebble)或外围设备(如头戴式耳机)的有线或无线连接的存在等);行为数据(例如,用户从口袋中取出装置的方式、打字行为、步态等);自从装置处于"可信"状态以来的时间;以及可能的使用实现保证等级所需(剩余)增益所需要的一种或多种验证形式(生物计量或其他方式)的新显式验证的结果。

[0143] 以上技术的结果是用户可选择最便利的验证方法。如果装置是智能电话，这可能只是获得了电话的使用权限而已(见上文)。也可不要求用户选择验证方法并且随后需要用户进行另一种显式验证，而是由依赖方250将关于所需保证等级增益的指示发送到自适应验证器800、810，所述自适应验证器800、810识别一组侵入性最小的验证技术。自适应验证模块800、810并不总是需要显式(侵入式)用户验证(如输入PIN或轻扫手指)，也不是单独基于非侵入式形式。相反，这种验证器选择(客户端侧上的)所有可用形式的恰当组合，以便实现所需的保证等级增益。

[0144] 如上文详细的论述，自从装置处于可信状态以来的时间非常重要，因为入侵/欺骗形式可能需要时间。例如，如果用户的电话遗失，而有人尝试入侵该电话，则可能需要一天的时间才能够从显示器捕捉指纹、制作适用的橡胶指套并且随后将其用于获取访问权限。因此，在自从上次处于可信状态过去24小时或更少时间之后要求输入PIN，将足以抵御这种类型的攻击。下一个等级的攻击是在获得使用权限之前捕捉指纹的攻击。这些攻击实际上较少看到。然而，如果依赖方250需要抵御此类攻击，则自适应验证模块800、810可能需要考虑位置数据或者其他小配件或外围设备的存在，以便接受生物计量形式。

[0145] 图9中示出根据本发明的一个实施例的方法。如上文论述，如本文所使用的“依赖方”可为依赖于对用户准确验证的实际方或可为代表依赖方验证用户的第三方服务。

[0146] 在901处，客户端装置连接到依赖方以执行交易(例如，登录在线账户的交易、货币交易等)。在902处，依赖方分析与客户端装置相关的任何可用数据，确定风险值以及验证用户需要的所需保证等级增益。例如，这些数据可指示用户正从未知网络位置(例如，用户先前从未去过的外国)连接到依赖方并且/或者客户端与依赖方之间的网络路由跳数或延迟时间高于阈值。在这种情况下，可将风险值设为相对较高的值(或，相反地，隐式保证等级可较低)。然而，如果用户最近恰好向装置显式验证过(例如，输入PIN)，则这往往会降低风险等级(或提高隐式保证等级)。

[0147] 可基于完成交易所需要的保证等级确定保证等级增益。可(例如)使用诸如下式的公式来计算：隐式保证等级+保证等级增益＝所需保证等级，或保证等级增益＝所需保证等级-隐式保证等级。可在同时仍符合本发明的基本原理的情况下使用各种其他公式来确定保证等级增益。

[0148] 在903处，接收关于所需要的保证等级增益的指示。如果在904处确定非侵入式验证技术足以实现保证等级增益，则在905处使用这些技术来验证用户。如果不是，则在907处，实施一种或多种显式验证形式，其中有可能与一种或多种非侵入式验证形式结合实施。如所提及的，可选择对最终用户最不繁琐的形式(例如，基于用户指定的偏好)。

[0149] 图10用图形示出上文所述的本发明的实施例可如何评估保证等级以确定验证形式。在时间t1处，用户执行显式验证(例如，轻扫手指、输入PIN等)。在时间t2处，依赖方要求保证等级增益为al4的验证。非侵入式验证形式实现高于al4的保证等级al1，所以不需要触发显式验证。

[0150] 相反，在时间t4处，依赖方要求保证等级增益为al4的验证。非侵入式验证形式在那个时间将仅实现al5(如图所示)。因而，在这种情况下，自适应验证器模块将选择至少一种显式验证形式来将保证等级从al5提高到al4。

[0151] 本发明的一个实施例以保护最终用户的隐私的方式采用隐式的基于位置的验证

技术。如上所述，与依赖方共享用户的当前位置(例如，由GPS提供)会产生严重的隐私问题。因此，用户常常不愿意共享此类数据。

[0152] 为了解决这些问题，本发明的一个实施例在执行隐式用户验证时使用地理位置作为因素，但不向依赖方公开用户的位置。可单独实施这个实施例，也可结合上文所述的其他非侵入式验证技术230和/或显式验证技术222(例如，作为较大的综合验证过程的一部分)来实施这个实施例。也可不从客户端装置传输实际位置，而是仅(至少部分地)基于地理位置数据传输保证等级，从而保护用户的隐私。

[0153] 一个实施例采用以下操作向依赖方登记和注册用户/装置：

[0154] 1。用户挑选并指定其向网站执行验证时通常所在的一个或多个位置。这些位置可为在预定英里数内或特定位置内的区域(如办公室、家、交通路线等)。所选择的位置可本地存储在客户端装置上并且不发送到依赖方。这些操作可由上文所述的位置验证模块231执行。

[0155] 2。在一个实施例中，在登记完成之后，客户端装置经由安全通信信道与依赖方共享密钥(例如，使用本文所述的安全通信模块213和其他注册技术)。

[0156] 在一个实施例中，在验证期间执行以下操作：

[0157] 1。客户端装置使用一种或多种地理定位技术确定其当前位置(例如，使用位置传感器241(诸如嵌入式GPS芯片)检索当前位置)。

[0158] 2。客户端上的位置验证模块231将当前位置与已经登记的位置进行比较并且产生指示距离的得分(例如，从0到100)。保证度计算模块212可接着将得分放到保证度计算中(如上文所述)。

[0159] 3。客户端装置生成签名，对得分/保证等级进行签署，然后发送到依赖方250以用于最终验证。

[0160] C.复合验证器

[0161] 本文所述的本发明的一些实施例采用客户端侧“验证器”，这些“验证器”包含以下安全性相关功能：

[0162] 1.存储并使用密码证实密钥

[0163] 2.生成、存储并使用密码验证密钥

[0164] 3.本地用户验证或验证用户存在与否

[0165] 4.向最终用户安全显示信息

[0166] 在一个实施例中，一些上述功能(例如，3和4)是任选的。另外，本发明的一个实施例包括实施以下安全性目标的验证器：

[0167] 1.确保证实密钥：(a)仅用于证实由FIDO验证器生成并保护的验证密钥；并且(b)从不离开FIDO验证器边界。

[0168] 2.如果要求支持本地用户验证(有时也称为“用户验证”)，则确保：(a)软件应用程序(例如，向验证器中“输入”PIN的恶意软件)无法绕过/伪造验证；(b)保护验证数据的机密性(例如，恶意软件既无法访问用户输入的PIN也无法访问参考数据)；并且(c)在生成新验证密钥之前要求进行用户验证并且在使用此类验证密钥之前达到时间。

[0169] 一种实施验证器的方式是，在由单个保护壳保护的单个模块中实施负责以上功能的所有组件。例如，可在于可信执行环境(TEE)中运行的可信应用程序(TA)中(例如，在支持

可信执行的客户端平台上)实施整个验证器。在这种具体实施中,TA被签署,从而确保验证器无法被修改并且TEE在执行时保护TA。

[0170] 在本发明的一个实施例中,每个验证器在逻辑上细分为多个独立组件,每个组件包括独立的安全和验证能力。例如,在图11中,并不是在由单个壳保护的单个模块中实施负责上述功能的所有组件,而是使用两个分开的独立验证器组件实施验证器1100:用户验证组件(UVC)1101和验证器内核(AK)1103,它们分别具有其自己的保护逻辑1110和1112。在这个例子中,AK 1103安全地为验证器1100管理证实密钥1104和验证密钥1105,并且UVC 1101管理用户验证/存在性功能1106和安全显示功能1107(其特定例子在下文中以及在共同待决的申请中描述)。

[0171] 如下文详细的论述,每个组件的保护逻辑1110、1112可包括组件验证引擎,用于向在客户端装置上执行的一个或多个其他组件验证每个组件(例如,见图13和相关联文本)。另外,保护逻辑可利用内建到客户端平台的额外硬件/软件保护机制(例如,诸如安全元件(SE)、信任链技术、可信用户接口技术、基于OS的保护机制等)。下文陈述与这些实施例中的每个实施例相关联的细节。

[0172] 图12示出本发明的一个实施例,在该实施例中由一组受保护验证器组件构建多个逻辑验证器1201和1202。具体地讲,用于逻辑验证器1201的组件构建块包括用于管理用户验证和存在性的用户验证组件(UVC)1210;用于确保向最终用户显示的信息恰好是交易确认的信息(即,“所见即所签”或WYSIWYS)的显示组件(DC)1212;以及用于安全地管理证实密钥1215(用于作为注册过程的一部分向依赖方证实验证器的模型和/或完整性)和验证密钥1216(用于对每个依赖方使用唯一的验证密钥建立与依赖方的安全通信)的验证器内核(AK)组件1214。用于逻辑验证器1202的组件构建块包括用于管理用户验证和存在性的UVC 1220,以及用于安全地管理证实密钥1215和验证密钥1216的验证器内核(AK)组件1214。因此,在这个例子中,多个逻辑验证器共享同一基础AK组件1214以用于管理和保护密钥。在本发明的其他实施例中,可在多个验证器之间共享其他类型的组件。如上文所论述,每个组件都具有自己的独立保护逻辑,以用于确保满足上文所陈述的安全性目标。

[0173] 以此方式由多个组件构建的验证器被称为“复合验证器”,因为这种验证器由分开的独立组件构成,这些独立组件各自具有自己的保护壳。复合验证器方法的一个好处是,一旦针对一个验证器构建了组件,便可跨多个验证器使用该组件,因而能够更有效地构建新的安全验证器。例如,如图12所示,在两个逻辑验证器1201和1202之间共享同一验证器内核组件1214。另外,每个验证器组件都可以针对其特定需要优化的方式来实施。以举例而非限制的方式,基于面部识别的验证器(其生物计量分割和匹配算法可能太大而无法在安全元件(SE)或可信执行环境(TEE)内实施)仍可利用SE/TEE来保护其证实密钥和用户验证密钥。在这个例子中,用户验证组件(例如,包括分割和匹配算法)可在SE/TEE外部运行,而验证内核组件可在SE/TEE内实施。相似地,在TEE中实施的基于指纹的验证器仍可利用SE验证内核来保护其证实密钥和用户验证密钥并且因此抵御基于硬件的攻击(例如,如差分功率分析(DPA))。

[0174] 在一个实施例中,实施以下安全措施为本文所述的组件验证器提供可接受等级的安全性(例如,对于满足上文指定的安全性目标为“可接受”的)。这些安全措施将参考图13进行描述,图13示出与图12中用于实施验证器1201的各个组件1210、1212、1214相关联的额

外细节。

[0175] 1.安全措施(SM)1:在一个实施例中,每个组件(例如,图12至13所示的用户验证组件1210、显示组件1212或验证内核1214)都具有自己的“组件验证密钥”对(CAK)(例如,分别是CAK对1304、1305和1306),用于(有可能相互地)向其他组件注册并且验证发送到其他组件的消息。如图13所指出的那样,每个组件1210、1212、1214分别包括组件验证逻辑1301、1302、1303,用于分别使用CAK对1304、1305、1306进入组件间验证事务。在一个实施例中,CAK对1304、1305、1306是公共/私有密钥对,但本发明的基本原理不限于此类具体实施。在这个具体实施中,每个组件被提供有其需要向其验证的那些组件的公共密钥。例如,UVC 1210知道DC和AK的公共密钥(或至少能够验证公共密钥)1321;DC 1212知道UVC和AK的公共密钥1321;AK 1214知道DC和UVC的公共密钥。在一个实施例中,在启动时,组件最初通过与必须要通信的其他组件共享公共密钥来进入与那些组件的注册事务。该组件可接着使用下文描述的技术向那些组件进行验证。

[0176] 2.安全措施(SM)2:每个组件都能够通过验证其从之接收消息的其他组件的公共CAK来验证这些其他组件。例如,在图13中,AK 1214可验证其支持的所有UVC 1210和DC 1212的公共CAK(即,CAK对1304和1305中的公共密钥)。如果实施相互验证,则UVC和DC也可验证AK 1214的公共CAK(即,在CAK对1306中)。

[0177] 图14是示出可如何实施两个组件(AK 1214与DC 1212)之间的验证的事务图。在事务1400处,AK的组件验证逻辑1303生成质询并且在事务1401中将其发送到DC的组件验证逻辑1302。在一个实施例中,质询是组件验证逻辑1303选择的随机数字或随机数。在操作1402中,DC的组件验证逻辑1302使用来自其CAK对1305的私有密钥对质询生成签名并且可能生成额外数据(例如,用户是否已经批准交易的内容)。如本领域的技术人员所理解的那样,生成签名可能涉及使用私有密钥对质询实施散列函数。在事务1403处,DC的组件验证逻辑1302将签名发送回到AK的组件验证逻辑1303,以进行验证。AK的组件验证逻辑1303现在知道该质询(例如,其先前生成的随机数)、使用DC的CAK对的私有密钥生成的签名,以及DC的CAK对的公共密钥。在事务1404中,AK的组件验证逻辑1303使用DC的CAK对的公共密钥来使用随机数字验证签名,从而验证DC。如果实施相互验证,则DC也可使用一组类似事务验证AK 1214的公共密钥。

[0178] 3.安全措施(SM)3:视特定的具体实施而定,可利用额外安全机制来保护组件之间的通信。这些额外安全机制在图13中以补充硬件/软件保护机制1310示出。以举例而非限制的方式,这些硬件/软件保护机制1310可包括内建到客户端平台的那些机制,诸如安全元件(SE)、信任链技术、可信用户接口技术、OS层级访问控制机制、白盒加密、代码混淆和运行时完整性保护,等等。通过使用(例如)ARM® TrustZone™或类似技术,操作系统可将对AK的应用程序编程接口(API)的访问仅限于可信程序(例如,诸如合法UVC和DC)。又如,操作系统还可向对AK的任何API调用添加UVC的或DC的包识别符。然而,应该指出的是,本发明的基本原理不限于上文论述的特定硬件/软件保护机制。

[0179] 举例来说,在一个实施例中,AK 1214实施为安全元件中的小程序,该小程序为密码密钥提供良好的保护机制,但没有用户接口。UVC 1210在可信执行环境内可实施为硬件(例如,指纹传感器)和可信应用程序的组合,两者均利用ARM TrustZone或类似技术。DC 1212可使用如全局平台所定义的“可信用户接口”能力实施为可信应用程序。因此,在这个

实施例中，当用户在指纹传感器上轻扫手指时，可信应用程序启动并且对照所存储的参考数据验证指纹数据。接着，可信应用程序将得分发送到实施为安全元件的AK 1214，接着AK 1214进入与依赖方1320的一系列验证事务以验证用户(例如，如共同待决的申请中所述)。

[0180] 另外，可使用白盒加密、代码混淆和运行时完整性保护的组合将一个不同的UVC实施为在富OS(例如，安卓系统)中运行的软件组件。该UVC可例如使用集成摄像机和面部识别软件。可使用白盒加密、代码混淆和运行时完整性保护的组合并且提供基于PIN的用户验证方法，将另一个UVC实施为在富OS上运行的可信应用程序或软件。

[0181] 因此，本文所述的基于组件的方法能够轻松适应不同验证技术的要求。例如，有些类型的验证(诸如声音识别和面部识别)需要使用普通富操作系统来实施为软件组件，这是由于这些验证类型具有大量存储要求和硬件接口要求。所有这些不同类型的验证可借助利用同一AK组件(可如所论述的那样实施为安全元件)的不同UVC组件以安全可信方式来实施。

[0182] 需注意的是，通过使用以上方法，各种部件使用密码保护(例如，签署)的消息在逻辑上进行通信。这种逻辑通信仍可由某个其他实体(例如，诸如下文论述的安全交易逻辑)“促进”。此外，在一个实施例中，本文所述的逻辑组件间消息传送对于依赖方1320而言为透明的，该依赖方1320直接与验证器内核1214进入证实和验证事务(例如，分别使用证实密钥1215和验证密钥1216)。在一个实施例中，AK使用证实密钥1215在注册期间验证验证器的模型和/或完整性。例如，依赖方可发送AK使用证实密钥1215来签署的质询。依赖方接着使用对应密钥来验证签名(例如，如果证实密钥为私有密钥，则使用公共密钥)。一旦验证器已经向依赖方注册，便向那个依赖方分配验证密钥1216。AK接着使用与依赖方相关联的验证密钥1216确保在注册之后与那个依赖方安全通信。

[0183] 作为额外的安全措施，在一个实施例中，每个组件的组件验证逻辑1301至1303都可在检测到组件泄露的情况下删除其CAK对。

[0184] 可利用本发明的基本原理实施两种不同类型的复合验证器：“静态”复合验证器和“动态”复合验证器。

[0185] 静态复合验证器

[0186] 参见图15，在一个实施例中，具有以下特性的复合验证器1501在本文中称为“静态”复合验证器：

[0187] 1.对于每个验证器1501，依赖方1320能够/需要访问公共证实密钥(对应于证实密钥对215，而不是公共“组件验证密钥”(CAK)1304、1306)；并且

[0188] 2.对于每个受支持的组件组合(例如，UVC、DC和AK)，已经预先指定了特定验证器证实ID(AAID)1505。

[0189] 因此，如图15所示，对于静态复合验证器，每个相异验证器1501由其特定AAID 1505识别。AK拥有一个或多个证实密钥215并且还选择一个预定义AAID(和相关证实密钥)以在与依赖方1320执行交易时使用。

[0190] 因为从不与依赖方1320共享CAK对，所以CAK对可为验证器特定的，而不影响用户的隐私。这还意味着可在检测到对独立组件的成功入侵的情况下单独撤销此类密钥。因为CAK不用作(公开可见的)“证实密钥”，所以组件的入侵不被视为等同于验证器的入侵。另外，因为复合验证器1501的通信和安全机制在验证器外部不可见，所以静态复合验证器的

具体实施不影响定义验证器1501与依赖方1320之间的交互的规范。在一个实施例中，每个组件1510、1514都被分配有可类似于AAID的唯一组件ID，但其仅与AK 1514相关(而不与RP或任何其他外部实体相关)。

[0191] 作为额外优化，在一个实施例中，可将在线证书状态协议(OCSP，RFC2560)用作每个CAK证书的撤销检验方法(例如，“验证”)。更具体地讲，AK 1514可要求对与公共CAK相关的UVC或DC的证书的足够近的OCSP响应，以便接受传入消息。AK 1514还可具有用于所有AAID的单一证实密钥，或者AK 1514可任选地针对每个AAID分别有一个证实密钥，或是它们的组合。

[0192] 在一个实施例中，AK可维持静态AAID列表。或者，如果是用于更新列表的已签署“AAID更新”消息的一部分，则AAID可接受从外部实体(例如，UVC/DC)接收到的AAID。在一个实施例中，AAID更新消息具有以下结构：签名(signing_key，AAID|AK组件ID|UVC/DC的公共CAK)。AK供应商可拥有私有signing_key。公共signing_key要么直接是AK的TrustStore的一部分(在TrustStore具体实施中)要么可使用存储在TrustStore中的某个证书来验证(即，链接到此类证书)。

[0193] 图15所示的用户装置1500的架构，还包括用于建立与依赖方1320的通信的浏览器/应用程序1510，以及用于启用与验证器的通信的安全交易逻辑1520。例如，如图所示，在一个实施例中，安全交易逻辑1520通过向各种组件暴露应用程序编程接口(API)来实现每个验证器1501的组件1510、1514之间的消息传递。因此，在这个实施例中，组件之间的所有通信(诸如注册数据和消息的交换)都经由安全交易逻辑1520来发生。举例来说，安全交易逻辑1520可实施为共同待决的申请(在下文中陈述关于该申请的多个部分)中所描述的“安全交易服务”。浏览器/应用程序1510可用于经由网络(诸如因特网)建立与依赖方1320的通信。

[0194] 动态复合验证器

[0195] 参见图16，在以下情况下，具有以下特性的复合验证器1601是“动态复合验证器”：

[0196] 1.“验证密钥”(CAK)1604、1604被当作证实密钥，使得依赖方1320具有并且需要相关公共密钥来验证证实消息(例如，在OSTP规范中称为“密钥注册数据”)；并且组件

[0197] 2.依赖方1320接收多个AAID 1602、1603(取决于验证器1601中组件的数量)。在一个实施例中，依赖方1320经由安全交易逻辑1620和浏览器/应用程序1610将验证器1601的所有组件1610、1614的AAID 1602、1603作为从AK 1614发送的注册消息的一部分接收。尽管图16仅示出UVC 1610和AK 1614，但替代实施例(诸如图3所示)向RP 1320发送AK、DC和UVC的AAID。然而，如所提及，本发明的基本原理不限于用于实施验证器的任何特定组的组件。在一个实施例中，发送到RP 1320的注册消息还具有多个(链接)签名，其中一个签名具有AK的证实密钥1605，并且其他每个组件(例如，UCC的证实密钥1604和DC的证实密钥(未示出))都各自有一个签名。如所提及，在一个实施例中，当且仅当信任与其他组件的通信时，AK 1614才在自己发往RP 1320的证实消息中包括其他组件的证实消息。

[0198] 因此，通过动态组合多个组件(或，换句话讲，组合两个验证器来得到一个新的验证器)来实施动态构成的验证器1601。因为在这个具体实施中CAK与RP相关，所以在一个实施例中，为了保护用户的隐私，CAK应当不是验证器所特定的。相反，CAK要么被预先生成/注入为共享密钥，要么使用直接匿名证实(DAA)方案来验证，其中DAA方案是实现可信平台的

验证并同时保护用户隐私的密码协议。因为多个AAID和链接证实消息对RP为可见的，所以动态复合验证器的具体实施会影响验证器1601与依赖方1320之间使用的验证规范。

[0199] UVC/DC断言验证

[0200] 不管使用动态验证器还是静态验证器，在一个实施例中，UVC 210和DC 212向AK 214都发送其输出数据，诸如用户验证结果(UVC)和用户对所显示的交易文本的接受(DC)，以便可根据在AK 214与依赖方1320之间所采用的验证规范进行处理。

[0201] 对于注册，在具有静态验证器的实施例中，UVC 210和DC 212可向AK 214发送密钥注册消息，该消息包含组件ID(而非AAID)，其中组件ID是与AAID相似但仅与AK相关的识别符。在一个实施例中，密钥注册消息的用户验证密钥是空的，并且密钥注册消息由CAK签署而不是由证实密钥签署。

[0202] 对于验证，在一个实施例中，UVC 210和DC 212创建由CAK(不是用户验证密钥)签署的消息。

[0203] 在本发明的一个实施例中，由AK实施以下验证步骤：

[0204] 1.查找包含可接受公共CAK列表的内部信任库。公共CAK可要么直接存储在TrustStore中，要么可针对每个CAK各自存在链接到TrustStore中的根证书的公共密钥证书。

[0205] 2.AK使用公共CAK验证来自UVC和/或DC的传入数据的签名(例如，如上文相对于SM1和SM2所论述)。

[0206] 3.检验额外的平台特定保护机制，诸如传入数据的包ID，或使用类似的平台提供的保护机制。

[0207] 4.检验包含UVC或DC的公共CAK的证书的撤销状态。因为AK仅对极少数证书/密钥(即，当前UVC或DC的证书/密钥)的撤销信息感兴趣，所以可利用在线证书状态协议(OCSP)(上文提及)撤销检验。假定AK不具有网络连接，因此OCSP响应预期作为来自UVC和/或DC的传入数据的一部分。

[0208] 优化的验证方法

[0209] 可在一个实施例中实施进一步优化，其中与对称密钥操作相比，不对称密钥操作太过昂贵。在这种情况下，由UVC和/或DC创建的、发送到AK的密钥注册消息包含对称密钥SK(例如，代替如上所述的空用户验证密钥字段)。由UVC生成并且发送到AK的修改密钥注册数据消息，可使用AK的公共CAK(或属于目标组件的某个其他可信公共密钥)来加密。由UVC和/或DC生成并且发送到AK的修改签名消息，并没有使用CAK来不对称地签署，而是其使用用SK计算出的基于散列的消息验证代码(HMAC)来保护。AK使用作为密钥注册数据消息的一部分接收的对称密钥来验证HMAC。

[0210] D.位置感知验证技术

[0211] 本发明的一个实施例实施允许基于正用于验证的客户端装置的物理位置来选择验证机制的验证策略。例如，客户端和/或服务器可确定客户端装置的物理位置，并且将那个位置馈送到评估一组有序策略规则的策略引擎。在一个实施例中，这些规则规定了位置类别以及在客户端位置与规则中的位置定义一致的情况下必须应用的一个或多个验证机制。

[0212] 如图17所示，本发明的一个实施例包括具有验证策略引擎1710的客户端装置

1700,所述验证策略引擎1710用于实施本文所述的位置感知验证策略。具体地讲,这个实施例包括位置类别确定模块1740,该模块用于使用由位置传感器1741(例如,GPS装置)提供的客户端装置1700的当前位置来识别当前位置“类别”。如下文详细的论述,可定义不同位置“类别”,包括已知地理点和/或区域。可连续更新位置类别数据并且将其存储在永久性位置数据存储装置1745(例如,快闪存储装置或其他永久性存储装置)中。位置类别确定模块1740可接着将传感器1741提供的当前位置与所定义的“类别”进行比较,以确定客户端装置1700的当前位置类别。

[0213] 在一个实施例中,依赖方1750为每个交易指定待由验证策略引擎1710实施的验证策略(如由从依赖方到验证策略引擎的虚线指示)。因此,可为每个依赖方的验证要求唯一地定制验证策略。另外,可基于当前交易来确定所需要的验证等级(如由验证策略定义)。例如,需要转移大量金钱的交易可要求相对较高的验证保证阈值,而非货币交易可要求相对较低的验证保证阈值。因此,本文所描述的位置感知验证技术对于某些交易可能是充分的,但对于某些交易,可与更严格的验证技术组合使用。

[0214] 在一个实施例中,位置类别确定模块1740将所确定的类别提供给验证策略模块1711,所述验证策略模块1711实施一组规则以识别待用于所确定类别的验证技术1712。以举例而非限制的方式,图18示出一组示例性规则1至5,这些规则指定可针对每个所定义的位置类别1至5使用的一种或多种验证技术1至5。虽然在图18中示出为表格数据结构,但本发明的基本原理不限于任何特定类型的数据结构来实施规则组。

[0215] 一旦验证策略引擎1710选择了一组验证技术1712,验证策略引擎1710便可使用一个或多个显式用户验证装置1720至1721和/或非侵入式验证技术1742至1743来实施这些技术,以向依赖方1750验证用户。以举例而非限制的方式,显式用户验证1720至1721可包括要求用户输入密码,诸如PIN、指纹验证、声音或面部识别,以及视网膜扫描,等等。

[0216] 非侵入式验证技术1742至1743可包括用户行为传感器1742,该传感器收集与用户行为相关的数据以用于验证用户。例如,可使用加速度计或其他类型的传感器1742以及被设计为生成用户的正常步行模式的步态“指纹”的软件和/或硬件,来测量用户的生物计量步态。如下文论述,可使用其他传感器1743收集用于验证的数据。例如,可收集网络数据,用于识别客户端装置1700的本地邻近处的网络/计算装置(例如,已知的对等计算机、接入点、手机发射塔等)。

[0217] 在一个实施例中,安全存储装置1725是用于存储与每个验证装置1720至1721相关联的验证密钥的安全存储装置。如下文论述,验证密钥可用于经由安全通信模块1713建立与依赖方1750的安全通信信道。

[0218] 可定义符合本发明的基本原理的各种不同位置“类别”。以举例而非限制的方式,可定义以下位置类别:

[0219] 类别1:客户端位于指定位置的给定半径内。在这个类别中,如果当前客户端位置位于以指定纬度和经度为中心的由具有给定半径的圆圈限定的区域内,则应用相关联的验证策略。

[0220] 类别2:客户端位于指定边界区内。在这个类别中,如果客户端位于由一组有序纬度和经度对定义的多边形(例如,闭合多边形)所限定的区域内,则应用相关联的验证策略。

[0221] 类别3:客户端位于指定边界外部。在这个类别中,如果客户端位于由一组有序纬

度和经度对定义的多边形(例如,闭合多边形)所限定的区域外部,则应用相关联的验证策略。

[0222] 在一个实施例中,使用上文定义的类别和策略规则的布尔组合定义额外类别。例如,布尔运算AND、OR、NOT和布尔运算的嵌套允许表达复杂条件。此类策略可用于(例如)实施在客户端位于公司所拥有的多种设施之一中时应用的策略。

[0223] 可使用各种不同机制确定客户端的当前物理位置(在图17中大体上表示为位置传感器1741),包括但不限于以下各项:

[0224] GPS:嵌入式GPS传感器可直接提供客户端位置的详情。新出现的标准试图增加位置验证,旨在提供解决当前GPS方案中的缺点的能力。

[0225] 地理IP查找:可借助对客户端IP地址的反向查找来确定客户端位置的粗略近似位置。然而,通过这种方法获得的位置的可信度需要对照已知遭侵入主机的黑名单来交叉检验IP地址、使代理提供商匿名或被设计为使主机的源IP地址模糊的类似方案。

[0226] 手机发射塔三角测量:客户端、服务器与无线运营商基础设施之间的集成可允许客户端和服务器使用蜂窝信号强度三角测量以高分辨率确定物理位置。

[0227] Wi-Fi接入点三角测量:一种用于确定物理位置的较高分辨率方法是对具有已知物理位置的附近Wifi接入点的信号强度进行三角测量。这种方法对于确定设施内装置的位置尤其有效。

[0228] 位置位移推断:装置的确切位置可为未知的,但是出于评估策略的目的可将位置的统计概率用作近似值。可通过记录装置的位置相对于具有已知位置的起始点的变化来进行计算;用户的装置可能在过去具有已知起始点,并且在此期间已经移动了一个已知或估计距离和方位,这样便可计算出近似位置。计算从起始点的位移的可能方法可包括使用从加速度计收集的测量值(即,使用加速度计来基于步态测量值测量用户步行了多远)、来自一组已知固定信号源的信号强度的变化以及其他方法推断所行进的距离。

[0229] 图19示出了用于实施位置感知验证策略的方法的一个实施例。该方法可在图17至18所示的系统架构的环境中内执行,但不限于任何特定系统架构。

[0230] 在1901处,使用一种或多种可用技术(例如,GPS、三角测量、对等/网络装置检测等)识别客户端的位置。在1902处,基于一组现有策略规则识别当前位置的一个或多个位置类别(以及可能的布尔类别组合)。在1903处,根据位置类别识别一种或多种验证技术。例如,如果客户端装置当前位于已知为用户的家或办公室的位置,或在另一个可信位置的限定半径内,则可要求进行最少的验证(或不要求验证)。相反,如果客户端装置当前位于未知位置和/或已知为不可信的位置,则可要求进行较严格的验证(例如,生物计量验证,诸如指纹扫描、PIN输入等)。在1904处,采用验证技术,并且如果在1905处确定验证成功,则在1906处对需要验证的交易进行授权。

[0231] 如上所述,可基于当前交易来确定所需要的验证等级。例如,需要转移大量金钱的交易可要求相对较高的验证保证阈值,而非货币交易可要求相对较低的验证保证阈值。因此,本文所描述的位置感知验证技术对于某些交易可能是充分的,但对于某些交易,可与更严格的验证技术组合使用。

[0232] 如果验证不成功,则在1907处阻止交易。在这个阶段,可永久性地阻止交易或者可请求执行额外的验证步骤。例如,如果用户输入的PIN不正确,则可要求用户重新输入PIN并

且/或者执行生物计量验证。

[0233] 本文所述的本发明的实施例为验证系统提供了很多好处。例如,所述实施例可用于有效阻止来自未授权位置的访问,从而通过限制准许用户尝试验证的位置(例如,由位置类别定义)来减少未授权访问。另外,本发明的实施例可选择性地要求执行较强验证来对位置特定风险做出响应。例如,依赖方可在用户正从已知位置进入交易时使验证的不便性减到最小,同时仍然保持在用户/客户端正从未知位置或意外位置连接时要求较强验证的能力。此外,本发明的实施例使得能够对信息进行位置感知访问。或者,依赖方可使用位置中心策略向用户提供对位置特定信息的额外访问。以举例而非限制的方式,当位于沃尔玛的用户在自己的移动电话上登录自己的Amazon.com账户时,可准许其访问来自Amazon.com的特价商品。

[0234] 如上所述,可使用多种不同技术确定客户端装置1700的位置。在一个特定实施例中,“位置”的定义可不关联到一组物理坐标(如使用GPS时),而是由一组对等装置或其他类型的网络装置的存在来规定。例如,在工作时,客户端的无线网络适配器(例如,Wifi适配器、蓝牙适配器、LTE适配器等)可始终“看到”一组对等网络装置(例如,其他计算机、移动电话、平板计算机等)和网络基础设施装置(例如,Wifi接入点、手机发射塔等)。因此,在用户工作时可利用这些装置的存在来验证。可以类似方式由装置的存在来定义其他位置,诸如当用户在家时。

[0235] 例如,通过使用本文所述的技术,可将某个位置定义为“与我的同事在一起”或“在工作”,其中可将已知由用户的同事拥有的一组对等装置的存在作为需要由验证策略减轻的风险的代理。例如,如果用户被一组已知对等装置或其他类型的网络装置围绕,则可认为用户的风险比在没有检测到已知装置的情况下低。

[0236] 图20示出一个实施例,其中“位置”由一组对等装置和其他网络装置定义。在所示出的例子中,客户端装置1700“看到”两个不同的对等装置2005和2006(例如,客户端计算机、移动电话、平板计算机等);两个不同的无线接入点2010和2011;以及两个不同的手机发射塔2020和2021。如本文所用,客户端装置1700可在没有与每个其他装置形式上建立连接的情况下“看到”。例如,客户端可看到连接到工作LAN的多种对等装置并且/或者可看到那些装置所生成的无线信号,而不管客户端是否连接到那些装置。相似地,客户端装置1700可看到多种不同Wifi接入点(例如,来自附近宾馆、咖啡店、工作Wifi接入点的Wifi)的基本服务集标识(BSSID)。客户端装置1700还可看到多种不同的手机发射塔2020和2021,可能甚至可看到由不同小区运营商运营的那些手机发射塔。可利用这些装置的存在为用户的工作位置定义位置“指纹”。

[0237] 如图所示,客户端装置1700上的装置接近检测逻辑2001可捕捉与可见装置相关的数据,并且将结果与历史装置接近数据2004进行比较。可随时间推移并且/或者通过训练过程生成历史装置接近数据2004。例如,在一个实施例中,用户可(手动地,或在客户端1700提示时)指定何时他/她在工作、在家或在其他位置。作为响应,装置接近检测逻辑2001可检测附近的装置并且将结果永久性地存储为历史装置接近数据2004。当用户随后返回到该位置时,装置接近检测逻辑2001可将其当前“看到”的装置与存储为历史接近数据2004的装置进行比较,以生成两者之间的相关性。一般来讲,相关性越强,客户端越有可能位于指定位置处。随着时间的推移,可在历史装置接近数据2004中使经常看到的装置的优先级高于其他

装置(例如,因为这些装置往往提供较准确的与用户工作位置的相关性)。

[0238] 在一个实施例中,验证策略引擎1710可使用由装置接近检测逻辑2001提供的相关性结果来确定用户针对每个依赖方1750所需要的验证等级。例如,如果存在高相关性(即,高于指定阈值),则验证策略引擎可不要求最终用户执行显式验证。相反,如果用户的当前位置与历史装置接近数据2004之间的相关性较低(即,低于指定阈值),则验证策略引擎1710可要求执行较严格的验证(例如,生物计量验证,诸如指纹扫描和/或请求输入PIN)。

[0239] 在一个实施例中,装置接近检测逻辑2001识别客户端附近已验证的一组其他装置。例如,如果用户的若干名同事已经成功验证,则与允许用户使用较不可靠的验证器访问某些数据相关联的风险可能较小,这只是因为用户正在他/她的同伴面前进行操作。在这个实施例中,可利用经由诸如802.11n等标准的对等通信从对等装置收集验证令牌,这些验证令牌可用于证明那些对等装置已经过验证。

[0240] 在另一个实施例中,装置接近检测逻辑2001还可检测与用户的客户端配对的先前已验证装置(例如,诸如用户的移动电话或平板计算机)。正尝试验证的同一个用户所使用的另一个已验证装置的存在,可用作验证决策的输入,尤其是在访问同一个应用程序时。

[0241] 在一个实施例中,收集历史装置接近数据2004并在多个装置之间共享,并且可将历史装置接近数据2004存储并保留在中间验证服务上。例如,可跟踪各个位置中的多组对等装置和网络装置的历史并且将其存储在每个装置上的可供装置接近检测逻辑2001访问的中央数据库中。接着可将这个数据库用作输入,以确定来自特定位置的尝试验证的风险。

[0242] E.用于使用补充传感器和/或位置数据确认位置的实施例

[0243] 如上所述,本发明的一个实施例利用来自移动装置的额外传感器1743的数据向用于验证的风险计算提供补充输入。这些补充输入可提供能够帮助确认或驳斥最终用户的装置的位置的额外等级的保证。

[0244] 如图21所示,提供关于装置位置的补充保证的额外传感器1743,可包括温度传感器2101、湿度传感器2102和压力传感器2103(例如,气压或高度计压力传感器)。在一个实施例中,传感器分别提供温度、湿度和压力读数,验证策略引擎1710的补充数据相关性模块2140使用这些读数与已知的与位置传感器1741提供的位置(或使用本文描述的各种其他技术得出的位置)有关的补充数据2110建立相关性。接着,验证策略模块1711使用相关性结果为给定交易选择一种或多种验证技术1712。如图21所指示,补充位置数据2110可包括从外部源(例如,因特网或其他移动装置)和本地数据源(例如,在已经知道装置由合法用户持有期间收集的历史数据)收集的数据。

[0245] 补充数据相关性模块2140可使用额外传感器1743以多种不同方式提供的数据与补充位置数据2110建立相关性。例如,在一个实施例中,补充位置数据2110包括位置传感器1741提供的位置处的当前本地气象状况。补充数据相关性模块2140将从额外传感器1743收集的湿度、温度或气压与实时本地天气数据2110进行比较,识别传感器数据与本地状况不一致的情况。例如,如果客户端装置的GPS读数指示装置在室外,但温度、湿度或气压与本地天气状况不一致,则补充数据相关性模块2140可生成低相关性得分并且该位置可被认为是较不可信的。因此,验证策略模块1711可要求执行较严格的验证技术1712(例如,指纹、PIN输入等)来批准交易。

[0246] 又如,补充数据相关性模块2140可将高度计压力传感器2103提供的海拔与声称位

置的已知地理或网络拓扑(具有补充位置数据2110)进行比较,识别表明声称位置不真实的差异。例如,如果用户的声称位置的反向IP查找将位置识别为在安地斯山脉,但来自装置的高度计数据指示装置在海平面处,则补充数据相关性模块2140可生成低相关性得分并且该位置可被认为是较不可信的。由于低相关性得分的缘故,验证策略模块1711可尝试使用较强验证来减轻交易的较高风险。

[0247] 在一个实施例中,补充数据相关性模块2140将从用户装置上的传感器1743收集的数据与临近区域中的多个其他最终用户进行比较,以识别表明用户不是在与那些已知用户相同的物理位置中进行操作的异常状况。例如,如果识别到正在同一物理区域中操作的一组已验证用户,并且所有那些用户的装置都表明该区域的本地温度为10℃,则补充数据相关性模块2140可对温度传感器2101指示本地温度为20℃的最终用户生成低相关性得分。因而,验证策略1711可要求执行较严格的验证技术1712。

[0248] 再如,补充数据相关性模块2140可针对特定用户将当前读数与历史数据进行比较。例如,如所提及的,可在已经知道用户持有装置1700期间(例如,在显式验证之后的时间段)分析传感器数据。接着,补充数据相关性模块2140可寻找本地数据的间断,以识别可疑行为。例如,如果用户的环境温度通常在10℃到20℃之间浮动并且用户的当前环境温度为30℃,则这可表明用户不在典型位置,从而生成低相关性,并致使验证策略模块1711要求对交易执行额外等级的审查。

[0249] 补充数据相关性模块2140可在同时仍符合本发明的基本原理的情况下,在传感器数据与补充位置数据之间建立各种不同类型的相关性。例如,可使用各种已知相关性机制来确定两组数据之间的统计关系。在一个实施例中,提供给验证策略引擎1711的相关性得分包括指示相关性水平的标准化值(例如,介于0与1之间)。在一个实施例中,可针对所检测到的传感器1743与补充位置数据2110之间的差异设置各种阈值水平。例如,如果温度传感器2101测量到的温度与(从其他装置或因特网收集的)当前温度相差3度以上,则可触发第一阈值(导致相关性得分变低)。与当前温度每额外相差3度都可接着导致满足新的阈值(导致相关性得分相应降低)。然而,应该指出的是,这些仅仅是本发明的一个实施例的例子;本发明的基本原理不限于建立相关性的任何特定方式。

[0250] 图22中示出根据本发明的一个实施例的方法。在2201处,读取客户端装置目前(例如,经由装置上的GPS模块)报告的当前位置。在2202处,针对所报告的位置收集补充位置数据,连同来自客户端装置的传感器数据。如上所述,可本地或远程(例如,在因特网上从其他客户端和/或服务器)收集补充位置数据,并且补充位置数据可包括诸如所报告位置的当前温度、压力和/或湿度等数据。可由温度传感器、气压或高度计压力传感器和/或湿度传感器提供传感器数据。

[0251] 在2203处,在补充位置数据与装置传感器所提供的传感器数据之间建立相关性。在一个实施例中,相对较高的相关性将在2204处导致相对较高的相关性得分,而较低的相关性将导致相对较低的相关性得分。如所提及的,在一个实施例中,相关性得分是指示传感器读数与补充数据之间的相似性的标准化值(例如,介于0与1之间)。

[0252] 在2205处,(至少部分地)基于相关性得分选择一种或多种验证技术。例如,如果提供相对较低的相关性得分,则可选择较严格的验证技术,而如果存在相对较高的相关性,则可选择较不严格的验证技术(有可能是不要求最终用户执行显式验证的那些技术)。

[0253] 如果在2206处确定用户使用选定技术成功地进行了验证，则在2207处允许交易进行。如果不是，则在2208处阻止交易。

[0254] 上述实施例实现了许多益处。例如，这些实施例为从其他源收集的位置数据提供额外水平的保证：允许组织补充从其他源(IP、GPS等)收集的位置数据，以便获得关于位置是真实的额外保证。另外，本发明的实施例可阻止来自未授权位置的交易，从而通过限制用户可甚至尝试验证的位置来减少未授权访问。此外，这些实施例可迫使利用较强验证对位置特定风险作出响应(例如，依赖方可在用户正从已知位置访问信息时使验证的不便性减到最小，且同时仍然保持在用户/客户端正从未知位置或意外位置或者无法使用多个输入充分证明真实性的位置访问时要求执行较强验证的能力)。

[0255] F.基于客户端验证能力的验证策略自适应应用

[0256] 如图23所示，本发明的一个实施例包括自适应验证策略引擎2345，其允许组织-例如，具有安全交易服务的依赖方1750(下文中简称为“依赖方”)-指定哪些类型的验证对于特定交互类别而言为恰当的。如图所示，自适应验证策略引擎2345可实施为在依赖方1750处执行的验证引擎2311内的模块。在这个实施例中，自适应验证策略引擎2345根据策略数据库2325来执行，并且策略数据库2325含有用于现有验证装置2329、验证装置类别2328、交互类别2327和验证规则2326的数据。

[0257] 在一个实施例中，验证装置数据2329包含与已知与客户端1700一起使用的显式用户验证装置1720至1721中的每一个相关联的数据。例如，策略数据库2325可包括用于“有效性模型123”指纹传感器的条目，以及与这个传感器有关的技术细节，诸如传感器(例如，在密码安全硬件、EAL 3证书等中)存储敏感数据的方式和错误接受率(指示传感器在生成用户验证结果时有多可靠)。

[0258] 在一个实施例中，验证装置类别2328基于验证装置的能力来指定验证装置2329的逻辑分组。例如，可针对(1)指纹传感器定义一个特定验证装置类别2328，所述指纹传感器(2)在已通过EAL 3认证的密码安全硬件中存储敏感数据，并且(3)使用错误接受率小于千分之一的生物计量匹配过程。另一个装置类别2328可为(1)面部识别装置，其(2)不在密码安全硬件中存储敏感数据，并且(3)使用错误接受率小于两千分之一的生物计量匹配过程。因此，满足以上标准的指纹传感器或面部识别具体实施将添加到恰当的验证装置类别2328中。

[0259] 可使用各种单独属性定义验证装置类别，诸如验证因素的类型(例如，指纹、PIN、面部)、硬件的安全保证等级、保密信息的存储位置、验证器执行密码操作的位置(例如，在安全芯片或安全附件中)以及多种其他属性。可使用的另一组属性与客户端上执行“匹配”操作的位置相关。例如，指纹传感器可在指纹传感器自身上的安全存储装置中捕捉和存储指纹模板，并且在指纹传感器硬件自身内对照那些模板执行所有验证，从而形成高度安全的环境。作为另外一种选择，指纹传感器可仅是捕捉指纹的图像但使用主CPU上的软件来执行所有捕捉、存储和比较操作的外围设备，从而形成较不安全的环境。也可使用与“匹配”具体实施相关联的各种其他属性来定义验证装置类别(例如，是在(还是不在)安全元件、可信执行环境(TEE)或其他形式的安全执行环境中执行匹配)。

[0260] 当然，这些仅仅是用于示出验证装置类别的概念的例子。可在同时仍符合基础原理的情况下指定各种额外的验证装置类别。此外，应该指出的是，视如何定义验证装置类别

而定，单个验证装置可被归类到多个装置类别。

[0261] 在一个实施例中，可周期性地更新策略数据库2325，以在新验证装置2329上市时将其包括在内以及新验证装置类别2328的数据，其中新验证装置类别2328有可能包含新验证装置2329可归类到的新类别。这些更新可由依赖方和/或负责为依赖方提供更新的第三方(例如，出售依赖方使用的安全交易服务器平台的第三方)执行。

[0262] 在一个实施例中，基于依赖方2325提供的特定交易来定义交互类别2327。例如，如果依赖方是金融机构，则可根据交易的币值对交互进行分类。“高值交互”可被定义为涉及(例如，转账、提取等)$5000或更多金额的类别；“中值交互”可被定义为涉及$500与$4999之间的金额的类别；“低值交易”可被定义为涉及$499或更少的金额的类别。

[0263] 除了所涉及的金额之外，还可基于所涉及的数据的敏感性来定义交互类别。例如，公开用户的机密数据或其他私有数据的交易可被归类为“公开机密的交互”，而不公开此类数据的交易可被定义为“不公开机密的交互”。可使用不同变量和多种最低水平、最高水平和中间水平来定义各种其他类型的交互。

[0264] 最后，可定义涉及验证装置2329、验证装置类别2327和/或交互类别2327的一组验证规则2326。以举例而非限制的方式，特定验证规则可指定对于(如交互类别2327所指定的)“高值交易”，仅可使用在已通过EAL 3认证的密码安全硬件中存储敏感数据并且使用错误接受率小于千分之一的生物计量匹配过程的指纹传感器(如被指定为验证装置类别2328的那样)。如果指纹装置不可用，则验证规则可定义可接受的其他验证参数。例如，可要求用户输入PIN或密码并且还回答一系列的个人问题(例如，用户先前向依赖方提供的个人问题)。可利用为验证装置和/或验证装置类别指定的任何上述单独属性定义规则，诸如验证因素类型(例如，指纹、PIN、面部)、硬件的安全保证等级、保密信息的存储位置、验证器执行密码操作的位置。

[0265] 作为另外一种选择或除此之外，可在规则中指定只要其他值是足够的，某些属性就能够采用任何值。例如，依赖方可指定必须使用指纹装置，并且该指纹装置在硬件中存储种子并且在硬件中执行计算，但不关心硬件的保证等级(如由包含满足这些参数的验证装置的列表的验证装置类别2328所定义)。

[0266] 此外，在一个实施例中，规则可仅指定只可使用特定验证装置2329来验证特定类型的交互。例如，组织可指定只有“有效性模型123指纹传感器”是可接受的。

[0267] 另外，可使用一条规则或一组规则为交互创建验证策略的整齐有序组合。例如，这些规则可针对各个验证策略指定策略组合，从而允许创建准确反映依赖方的验证偏好的丰富策略。这种做法将允许(例如)依赖方指定指纹传感器是优选的，但如果没有指纹传感器可用，则基于可信平台模块(TPM)的验证或面部识别同样可优选作为下一个最佳替代方案(例如，以优先级顺序)。

[0268] 在一个实施例中，当确定是否准许与客户端1700的交易时，自适应验证策略引擎2345依赖交互类别2327、验证装置类别2328和/或验证装置数据2329实施验证规则2326。例如，作为对客户端装置1700的用户尝试进入与依赖方网站或其他在线服务2346的交易的响应，自适应验证策略引擎2345可识别适用的一个或多个交互类别2327的组和相关联的验证规则2326。其可接着经由与客户端装置1700上的自适应验证策略模块2350(在图23中示出为客户端的验证引擎2310内的组件)的通信来应用这些规则。自适应验证策略模块2350可

接着识别一种或多种验证技术2312的组以符合指定的验证策略。例如，如果依赖方的自适应验证策略引擎2345指定一组已设定优先级的验证技术，则自适应验证策略模块2350可选择客户端1700上可用的最高优先级验证技术。

[0269] 验证技术2312的结果提供到保证度计算模块2340，该保证度计算模块2340生成当前用户是合法用户的保证等级。在一个实施例中，如果保证等级足够高，则客户端将把成功验证的结果传送到依赖方的验证引擎2311，之后该验证引擎2311将准许交易。

[0270] 在一个实施例中，来自客户端装置传感器1741至1743的数据还可由保证度计算模块2340用来生成保证等级。例如，位置传感器(例如，GPS装置)可指示客户端装置1700的当前位置。如果客户端装置处于预期位置(例如，在家或在工作中)，则保证度计算模块2340可使用该信息来提高保证等级。相反，如果客户端装置1700处于意外位置(例如，用户先前从未到访的外国)，则保证度计算模块2340可使用该信息来降低保证等级(从而要求执行较严格的显式用户验证来达到可接受的保证等级)。如上文论述，可将各种额外传感器数据(诸如温度、湿度、加速度计数据等)综合到保证等级计算中。

[0271] 图23中所示的系统可基于将客户端验证能力和其他信息传送到依赖方的特异性来不同地操作。例如，在一个实施例中，可将每个显式用户验证装置1720和1721的具体型号，以及客户端装置1700上的安全硬件/软件和传感器1741至1743的特定详情传送到依赖方1750。因而，在这个实施例中，自适应验证策略引擎2345可基于针对当前交易实施的验证规则和与客户端相关联的风险来明确地识别所需的验证模式。例如，自适应验证策略模块2345可针对给定交易请求经由安装在客户端上的“有效性模型123”指纹传感器进行验证。

[0272] 在另一个实施例中，为了保护用户的隐私，可仅提供对客户端装置1700的验证能力的一般描述。例如，客户端装置可传达其具有在已通过EAL 3认证的密码安全硬件中存储敏感数据并且/或者使用错误接受率小于N分之一的生物计量匹配过程的指纹传感器的消息。客户端装置可指定与其他验证装置的能力和规范相关的类似一般信息，而不公开那些装置的具体型号。接着，自适应验证策略引擎2345可使用这些一般信息在数据库2325内将验证装置归类到适用的验证装置类别2338。作为对执行交易的请求的响应，如果特定验证装置的类别足以完成交易，则自适应验证策略模块2345可接着指示客户端装置1700使用该特定验证装置。

[0273] 在又一个实施例中，客户端装置1700不向依赖方传送与其验证能力相关的任何数据。相反，在这个实施例中，自适应验证策略模块2345传达所需要的验证等级，并且客户端上的自适应验证策略模块2350选择满足那个验证等级的一种或多种验证技术。例如，自适应验证策略模块2345可传达当前交易被归类为“高值交易”(由交互类别2327指定)的消息，对于所述“高值交易”仅可使用某些类别的验证装置。如所提及的，自适应验证策略模块2345还可以已设定优先级的方式传达验证类别。基于该信息，客户端上的自适应验证策略模块2350可接着选择当前交易所需的一种或多种验证技术2312。

[0274] 如图23所指示，客户端装置1700可包括其自己的策略数据库2390，以用于存储/高速缓存每个依赖方的策略数据。策略数据库2390可包括存储在依赖方的策略数据库2325内的数据的子集。在一个实施例中，在数据库2390中针对每个依赖方存储了一组不同的策略数据(反映每个依赖方的不同验证策略)。在这些实施例中，特定交易类别(例如，“高值交易”、“低值交易”等)的仅有指示可为足以供客户端装置1700上的自适应验证策略模块2350

选择必要的验证技术2312的信息(即,因为可在本地策略数据库2390内找到与各种交易类型相关联的规则)。因而,自适应验证策略模块2345可仅指示当前交易的交互类别,自适应验证策略模块2350使用该交互类别来基于与该交互类别相关联的规则识别验证技术2312。

[0275] 图24中示出基于客户端装置能力来执行自适应验证的方法。该方法可在图23所示的系统上实施,但不限于任何特定系统架构。

[0276] 在2401处,客户端尝试与依赖方执行交易。以举例而非限制的方式,客户端可输入支付信息进行在线购买或尝试在银行账户之间转移资金。在2402处,对交易进行归类。例如,如上文论述,可基于诸如所涉及的金额或所涉及的信息敏感性等变量来使交易与特定交互类别相关联。

[0277] 在2403处,识别与该交易类别相关联的一个或多个规则。回到上例,如果交易被归类为"高值交易",则可选择与这种交易类型相关联的规则。在2404处,执行与该交易类型相关联的规则,并且如上文论述,向客户端发送指示完成交易的验证要求的信息。如上文论述,此过程可涉及识别特定验证装置、识别验证装置的类别,或仅仅指示需要实施的特定规则(例如,如果客户端在本地保留了这些规则的复本)。

[0278] 在任何情况下,在2405处,基于经由规则和客户端的验证能力指定的要求来选择一组验证技术,这种验证技术由一种或多种验证技术组成。如果在2406处确定验证成功,则在2407处准许交易。如果不是,则在2408处阻止交易(或向用户请求执行额外验证)。

[0279] 通过本文所述的本发明的实施例可实现许多益处。例如,这些实施例减少了在依赖方处集成验证能力所需要的工作量。例如,不需要编写代码来编纂验证策略,可通过简单的图形用户界面配置规则。要完成集成,依赖方只需要针对交互类别(例如:"大笔金额转移")定义策略并且在与策略引擎交互以确定待利用的正确验证机制时使集成代码使用相应的策略识别符。

[0280] 此外,这些实施例简化了验证策略管理。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。

[0281] 最后,这些实施例允许将来对验证技术进行改进。在有新的验证装置可用时,组织可评估其应对新风险或新兴风险的适宜性。要集成新近可用的验证装置,仅需要将验证装置添加到策略即可;不必编写新代码来立即部署新能力。

[0282] G.用于在验证期间进行眼动跟踪的系统和方法

[0283] 一般来讲,如果(a)使用秘密信息进行验证或(b)很难产生假输入,则验证技术在应对欺骗方面具有良好的稳健性。如今,大多数系统依赖于基于密码的验证。密码易于复制,所以需要保密。因此,密码攻击通常集中在获取用户密码方面。最近的攻击已经表明,存储验证密码的服务器较为脆弱。

[0284] 与基于密码的验证相比,使用生物计量进行验证时,生物计量信息通常是公开的。例如,可从用户触摸过的(几乎)任何物体上取得用户的指纹。相似地,用户的面部通常不会隐藏起来,因此可被任何人看见并捕捉,而且常常会在社交网络上公布。

[0285] 在真实世界中,在看一个人时我们可以依赖于我们自己的识别能力,因为很难"造出"具有相同生物计量特性的另一个人。例如,同样很难"造出"具有相同面部和习性的另一个人。这就是为什么政府在护照、身份证、驾驶证和其他文件上放置面部图片的原因。然而,

在虚拟世界中，我们不必“造出”具有相同面部的另一个人来欺骗系统，只要造出计算机将识别的某些东西(如面部的图片)即可。换句话讲，“这寓意着，生物计量学只有在验证器能够验证两件事情时才奏效：一是验证时生物计量信息来自人，二是生物计量信息匹配存档的主生物计量信息”(见在本说明书的权利要求书之前提供的参考文献列表中的参考文献1)。

[0286] 过去，对自动面部识别的研究集中于使用静态图像和视频可靠地识别面部。参见例如下面的参考文献2。存在若干种相对稳健的面部识别技术并且在当前市面上可买到多种系统(见参考文献3)。然而，很少有人注意“活性”检测，即“确认生物计量信息与存档的主生物计量信息一致”。在若干种使用情况下，要么不需要欺骗防御，要么仍由人类执行欺骗防御(例如，在执法应用中)。

[0287] 一方面，笔记本计算机和智能电话等计算装置普遍都配备了相机，另一方面，密码这种最流行的验证方法具有缺点，这两个方面推动了生物计量验证方法、尤其是面部识别的流行。面部识别作为验证方法的第一次大规模“试验”出现在谷歌安卓4(又称“冰淇淋三明治”)中，且基于静态图像识别。但是使用照片便可以轻易骗过这些技术(见参考文献4)。尽管安卓4.1(又称“软心豆粒糖”)采用了改进的方法，加入了某种活性检测，但是在计算机显示器上向相机依序呈现两张照片(一张睁眼照片，一张经过电子修改的闭眼照片)仍可轻松欺骗过关(见参考文献5)。

[0288] 虽然也许有人会说这个缺点是由于移动装置上的资源限制而造成的，但这也说明，可供PC使用的商用软件，甚至是对反欺骗检测的研究，尚未非常成熟。本申请的受让人使用基于PC的面部识别软件进行了测试，测试结果表明：

[0289] 即使将安全设置设为“高”，在基于Windows 7®的Samsung Series5®笔记本计算机上运行的Cogent BioTrust 3.00.4063也根本不执行活性检查。在普通计算机监视器上显示的简单面部图像足以成功骗过系统。

[0290] 在Macbook Air ®上运行的KeyLemon 2.6.5执行简单的眨眼测试，作为活性检验。只需展示如下一系列的3个图像便可成功骗过系统：(1)面部的真实图像(例如，由网络摄像头创建)；(2)真实图像的修改图像，在这种修改图像中，对眼睛进行了重新上色，使得眼睛看起来似乎是闭上的；(3)又是真实图像。

[0291] 比较不同算法时，反欺骗检测不是标准测试(诸如NIST生物计量供应商测试)的一部分。参见例如参考文献6至8。2011年由若干位研究人员组织的第一批已知公开赛之一(见参考文献9)展示了一些算法的早期成功，但是这些算法基于分辨率为320×240像素的视频。典型计算装置提供的前置摄像头的分辨率为至少640×480像素。

[0292] 图25示出具有用于执行面部识别的生物计量装置2500的示例性客户端2520。正常运行时，生物计量传感器2502(例如，相机)从用户读取原始生物计量数据(例如，拍摄用户的照片)，并且特征提取模块2503提取原始生物计量数据的指定特征(例如，注重于某些面部特征等)。匹配器模块2504将所提取的特征与客户端2520上的安全存储装置中存储的生物计量模板数据2510进行比较，并且基于所提取的特征与生物计量模板数据2510之间的相似性来生成得分和/或“是/否”响应。生物计量模板数据2510通常是登记过程的结果，用户在登记过程中向装置2500登记面部图像或其他生物计量数据。接着，应用程序2505可使用

得分或“是/否”结果来确定验证是否成功。

[0293] 可从多个潜在攻击点来欺骗面部识别系统(见参考文献10、11),这些攻击点在图25中标识为(1)至(8)。已经有确保生物计量模板(6)的完整性(例如,通过使用电子签名)并且保护特征提取(3)、特征向量(4)、匹配器(5)及其最终结果(8)的完整性(例如,通过应用(a)白盒加密方法、(b)代码混淆和(c)装置绑定的组合)的熟知保护机制。

[0294] 可信计算组织的方法中以及ARM TrustZone的潜在扩展中(至少理论上)涵盖了防止向特征提取单元(2)重新播放旧捕捉数据的保护机制。基本上,方法是向传感器添加密码保护机制(例如,HMAC或电子签名)并且以防篡改方式封装传感器,这类似于当前智能卡芯片中所使用的保护机制。接着,特征提取引擎可验证传入数据的完整性。

[0295] 尽管下文所述的本发明的实施例利用眼动跟踪技术来确认用户的“活性”,但在一个实施例中,这些技术与一种或多种检测假生物计量的现有技术(见参考文献1)组合使用。这个领域目前正在研究中。现有研究已经确定了针对假生物计量的四种不同类别的防御方法(见参考文献12):

[0296] 1.数据驱动的特征化

[0297] a.静态图像

[0298] i.通过重新扫描图像并且分析2D傅立叶频谱来检测分辨率降低(参考文献13)

[0299] ii.利用真实面部与图像印制品的不同反射特征。其理论基于朗伯反射特性(参考文献14)

[0300] iii.利用打印缺陷造成的真实面部与图像印制品的不同微观纹理(参考文献15)。

[0301] iv.利用打印图像上的降质和加噪并结合其他方法(参考文献16)。

[0302] b.视频

[0303] v.每个相机传感器都有自己的特征,重新捕捉监视器上所显示的视频会造成伪影。可利用这点来检测欺骗(参考文献12)。

[0304] vi.如果使用图像进行欺骗,面部和背景之间会存在相依性(参考文献17)。

[0305] vii.如果是欺骗攻击,面部的活动通常会较僵硬(参考文献18)。

[0306] c.静态图像与视频的组合(参考文献12)。

[0307] 2.用户行为建模(参考文献12)。

[0308] 3.用户交互需求(参考文献12)。

[0309] 4.额外装置(参考文献12)。

[0310] 仅基于现有传感器技术的最有效非侵入式机制似乎是基于动作检测、纹理检测和活性检测的组合。参见参考文献9。

[0311] 纹理差异

[0312] 可检测对打印并重新扫描图片造成的影响。从直观上可以清楚看出,打印和重新扫描图像后,图像的质量并没有改善。参考文献15中的研究表明,可通过分析微观纹理来在算法上检测差异:“仔细查看真实面部与面部印制品之间的差异可以发现,人脸和印制品反射光的方式是不同的,因为人脸是复杂的非刚性3D物体,而照片可被看作是平面刚性物体。”

[0313] 这种算法已经对照NUAA图片欺骗数据库中包括的图像进行过测试。据报告,使用未优化C++代码在具有3GB RAM的2.4GHz英特尔酷睿2双核CPU上处理图像的平均性能为

16.5ms。

[0314] 红外线,而非可见光

[0315] 很难在红外光谱中显示图像或视频。因此,如参考文献19中所提出的基于捕捉面部热图像的活性检测,将比以可见光捕捉图像更稳健。遗憾的是,红外传感器很昂贵,因此未纳入一般的笔记本计算机、平板计算机或智能电话中。

[0316] 基于光流的方法

[0317] 真实面部是三维物体。在正常交谈中面部通常会移动。预期面部中央部分的2D运动,即,与相机的距离较近的部分的2D运动,比与相机的距离较远的面部区域的2D运动高(参考文献20、21、22)。对于这种类型的检测,需要包含至少3个连续图像的序列。

[0318] 参考文献21中的研究是SART-2项目(用于移动工作站的生物计量安全系统)的一部分。

[0319] 运动图片,而非静态图像

[0320] 在参考文献23中描述了基于眨眼的活性检测方法。这种方法似乎对于简单的基于照片的欺骗攻击相当稳健。除了识别面部之外,该方法还定位眼睛并且检查在所观测到的图像序列中是否能够看到闭眼。如从安卓4.1的大规模试验中看到,这种方法对于“photoshop”攻击明显不是非常稳健。参见参考文献5。

[0321] 一般来讲,为了欺骗此类基于运动图片的系统,攻击者必须生成小图像序列并且必须向传感器展示该序列。在具有强大图像编辑器、免费视频编辑器和平板PC的世界中,这是非常容易做到的。

[0322] 此类方法以“公知交互”为特征,即,攻击者事先知道所需要的交互并且能够准备匹配的图像序列。

[0323] 在参考文献23中,将场景和眨眼的情形纳入了分析中。在英特尔酷睿2双核2.8GHz的2GB RAM上测得的性能为大约每视频帧50毫秒(20fps)。

[0324] 质询响应方法

[0325] 在生物计量的环境中,质询响应被定义为:

[0326] 一种通过引出来自个体的直接响应来确认人员存在的方法。响应可以是自愿的,也可以是非自愿的。在自愿响应中,最终用户将有意识地对系统所呈现的事物做出反应。在非自愿响应中,最终用户的身体自动地对刺激做出响应。可利用质询响应保护系统免受攻击。

[0327] (National Science&Technology Council's Subcommittee on Biometrics)

[0328] 多模态系统

[0329] 目前已经提出多模态系统来改善生物计量方法抵御欺骗攻击、噪声数据等的稳健性。参见参考文献25。

[0330] 参考文献26中分析了模拟欺骗攻击对此类多模态系统的影响。得出的主要结果是,并非所有融合方案都能改善抵御欺骗攻击的稳健性,这意味着在一些融合方案中,只需欺骗单个生物计量方法便足以欺骗整个多模态系统。使用真实欺骗攻击对现有方案进行的分析得到了类似的结果。参见参考文献27。

[0331] 一般来讲,存在三种不同类别的多模态系统:

[0332] 1)成功欺骗单个特征便足以欺骗整个系统的系统。针对小FRR优化多模态系统通

常会导致此类结果。

[0333] 2)具有以下情况的系统：

[0334] a)必须欺骗不止一个特征才能成功欺骗整个系统;并且

[0335] b)欺骗这个多模态系统中的任何一个特征都不比欺骗单模态系统中的相同特征复杂。

[0336] 3)具有以下情况的系统

[0337] a)必须欺骗不止一个特征才能成功欺骗整个系统;并且

[0338] b)欺骗这个多模态系统中的任何一个特征都比欺骗单模态系统中的相同特征更复杂。下文所述的本发明的实施例属于这一类。

[0339] 本发明的一个实施例将眼动跟踪作为验证过程的一部分来执行以测量对屏幕上随机布置和显示的不同关注区的响应。例如,可向用户展示混合文本、空白区域、图像和视频剪辑的一系列随机屏幕布局,从而以非侵入式的方式引发用户的眼球运动。同时,使用眼动跟踪技术来确认眼球正以预期方式对屏幕布局做出反应。接着可结合该信息与面部识别技术来验证仍存在预期的面部。此外,如上文论述,可将眼动跟踪技术和面部识别技术与其他技术(例如,基于位置的验证、非侵入式用户存在检测、指纹扫描等)结合使用以达到对合法用户持有装置的足够保证等级。

[0340] 阅读网页或其他内容类型不涉及眼球沿着内容进行平滑移动,涉及一系列短暂停留(称为“凝视”)和快速“扫视”。所得的一系列凝视和扫视被称为“扫描路径”。扫描路径可用于分析认知意向、兴趣和特色(“眼动跟踪”参见en.wikipedia.org/wiki/Eye_tracking处的当前维基百科文章)。“热图”是显示一组人在观看网页或电子邮件时凝视什么区域的集合表示(见Hartzell,“Crazy Egg Heatmap Shows Where People Click on Your Website”(Nov 30,2012)(Hartzell.Crazy Egg热图显示人们点击您网站的哪些部分。www.michaelhartzell.com/Blog/bid/92970/Crazy-Egg-Heatmap-shows-where-people-click-on-your-website,2012-11-30)。

[0341] 如图26所示,本发明的一个实施例包括客户端装置2600上的验证引擎2610,其包括用于执行面部识别的面部识别模块2604和用于执行本文所述的眼动跟踪操作的眼动跟踪模块2605。在一个实施例中,面部识别模块2604和眼动跟踪模块2605分析客户端装置上的相机2602捕捉的视频图像序列2603,以执行相应操作。

[0342] 为了执行面部识别操作,面部识别模块2604依赖于存储在安全面部识别数据库2646内的面部识别模板。具体地讲,如上文论述,面部识别模块2604内的匹配逻辑将从视频图像2603提取的面部特征与存储在面部识别数据库2646中的面部模板数据进行比较,并且基于所提取的特征与面部模板数据之间的相似性生成“得分”。如先前论述,存储在数据库2646中的面部模板数据可由登记过程生成,在登记过程中用户向客户端装置2600登记面部图像或其他生物计量数据。接着可将面部识别模块2604生成的得分与来自其他验证模块(例如,诸如下文论述的眼动跟踪模块2605)的得分综合,以形成保证等级2606,保证等级2606表示合法用户正发起当前交易的保证度。在一个实施例中,每个得分都必须达到特定阈值,才能针对特定交易生成足够的保证等级2606。在一个实施例中(假定已达到阈值),可将得分相加或使用其他数学公式进行综合(例如,可对得分进行加权、求平均值、相加或以任何其他方式进行综合)。

[0343] 为了执行眼动跟踪分析，眼动跟踪模块2605依赖于存储在安全眼动跟踪数据库2645内的眼动跟踪模板。虽然示出为单独的数据库，但眼动跟踪数据库和面部识别数据库可实际上是同一个安全数据库。在一个实施例中，眼动跟踪模板指定将在客户端装置的显示器2601上向用户显示的文本、图形、图片、视频和/或空白区域(一些例子在下面的图28A至28B中示出)，并且还有可能指定显示这些内容的次序。另外，眼动跟踪模板包括指定用户眼球响应于向用户显示的内容而产生的预期运动特征的数据(例如，呈热图的形式，见下文)。眼动跟踪模块2605内的匹配逻辑将用户眼球的预期运动与(从视频图像捕捉的)实际运动进行比较，从而基于预期运动与实际运动之间的相似性得出“得分”。如所提及的，可接着将该得分与来自其他验证模块(例如，诸如面部识别模块2604)的得分进行综合，以形成保证等级2606。存储在数据库2646中的眼动跟踪模板数据可使用其他用户和/或装置的实际用户响应于每个所显示的网页或其他显示图像做出的眼球运动的记录来编译。例如，如同面部识别模板，可作为登记过程的一部分生成眼动跟踪模板，在登记过程中用户向装置2600登记他/她的眼球运动。

[0344] 在一个实施例中，眼动跟踪模块2605确定正显示的图像(可包括文本、图形、视频、图片和/或空白区域)与用户眼球运动之间的相关性。例如，如果在显示器的右下角显示运动视频，则绝大多数用户将把注意力转到这个区域。因此，如果眼动跟踪模块2605检测到用户的眼球已经在指定时间周期(例如，2秒)内移动到这个区域，则眼动跟踪模块2605将检测到用户眼球与模板之间存在高相关性，从而得到相对较高的得分。相反，如果用户的眼球没有移动到这个区域(或根本没有移动)，则眼动跟踪模块2605将检测到低相关性，从而得到相应的低得分。

[0345] 如图26所示，可在客户端装置2600上配置各种其他显式用户验证装置2620至2621和传感器2643。这些验证装置和传感器可提供验证引擎2610在生成保证等级2606时将使用的额外验证数据(在必要时)(即，除了本文所述的眼动跟踪和面部识别之外)。例如，传感器可包括位置传感器(例如，GPS)，用以确定客户端装置2600的位置。如果客户端装置处于预期位置，则验证引擎可使用该数据来提高保证等级2606。相反，如果客户端装置处于不寻常位置(例如，另一个国家)，则这可对保证等级2606造成负面影响。这样，可以非侵入方式生成验证数据(即，使用在没有来自最终用户的显式输入的情况下收集的传感器数据)。

[0346] 另外，另一种非侵入式技术涉及验证引擎2610监视自上次显式用户验证以来已经过去的时间。例如，如果用户最近(例如，在10分钟内)已经使用指纹或其他生物计量装置2620至2621进行过验证或已经输入过密码，则验证技术将使用这个信息来提高保证等级2606。相反，如果用户已经几天未进行显式验证，则验证技术可要求面部识别模块2605和眼动跟踪模块2605执行较严格的验证(例如，可要求执行比平常更高的与模板数据的相关性，以针对当前交易将保证等级提高到可接受的值)。

[0347] 在一个实施例中，安全存储装置2625是被提供用于存储与每个验证器相关联并且被安全通信模块2613用于与依赖方(例如，云服务2650或其他类型的网络服务)建立安全通信的验证密钥的安全存储装置。

[0348] 图27中示出针对网页生成的示例性“热图”。彩色编码表示用户在观看时凝视的网页的区域。红色指示最高凝视量(意味着用户往往较频繁地观看这些区域)，之后是黄色(指示较少凝视)、蓝色(指示更少凝视)，接着是无色(指示没有凝视或低于阈值量的凝视)。

[0349] 在设计网页时，作为可用性分析的一部分执行眼动跟踪和热图分析。研究(例如，见参考文献29、30)发现，Web用户80％的时间花在观看页面折痕上方的信息。虽然用户确实会滚动屏幕，但用户仅将20％的注意力分配给折痕下方的信息。Web用户69％的时间花在观看页面的左半面，30％的时间花在观看右半面。因此，常规布局更有可能使网站盈利。

[0350] 在监视器上呈现所显示的静态面部图像或视频等欺骗攻击可被眼动跟踪模块2605检测到，因为扫描路径将很可能与屏幕布局不相关。可使用不同类型的眼动跟踪方法：具有高准确性的专用设备和使用标准网络摄像头的基于软件的方法(见参考文献33)。

[0351] 图28A示出在客户端装置显示器2601上显示的文本2805以及图像和/或视频2801的示例性分组。在一个实施例中，该分组集成到网页中。然而，本发明的基本原理不限于基于Web的组织。该分组也可为屏幕保护程序或其他应用程序的一部分。在一个实施例中，同时显示文本2805和图像/视频2801。在另一个实施例中，首先显示文本，之后显示图像/视频2801。在任一情况下，预期的是，用户的眼球都将指向显示器2601的右下角(在该处显示图像/视频2801)。

[0352] 图28B示出包括文本区域2805和三个图像/视频元素2800至2802的另一个例子。在一个实施例中，首先显示图像/视频元素2800，接着显示图像/视频元素2801，之后显示图像/视频元素2802。在此类情况下，用户的眼球应从显示器的右上角移动到右下角，接着移动到左下角。

[0353] 在一个实施例中，由眼动跟踪模块2605随机选择特定图像/视频元素2800至2802和其他内容类型，从而使得更难以预计和欺骗。另外，不同图像/视频元素2800至2802所在的特定位置是随机选择的。在此类情况下，眼球运动模板可指定用于显示内容的特定操作模式，但将不指定实际内容或实际位置。相反，由眼动跟踪模块2605选择内容和位置，眼动跟踪模块2605接着将假设用户的眼球应被吸引到正显示的内容并且基于检测到的程度生成相关性和得分。

[0354] 另外，眼动跟踪模块2605可使用现有内容，诸如依赖方2650的现有网页或装置上本地存储的图像，而不是生成自己的内容。例如，如果依赖方是金融机构并且用户正尝试进入金融交易，则可显示通常在交易期间显示的网页。在此类情况下，眼动跟踪模块2605可从眼动跟踪数据库2645检索网页的热图(诸如图27所示)并且确定是否存在与热图和最终用户正观看的位置的相关性。

[0355] 概括地说，本文所述的实施例可呈现混合文本、空白区域、图像和视频剪辑的一系列随机屏幕布局并且连续跟踪用户的眼球，从而产生所捕捉的扫描路径。接着在所捕捉的扫描路径与预期的扫描路径之间建立相关性。另外，本发明的一个实施例可接着重新验证仍识别到面部。

[0356] 并非所有人都同样被相同图像或图像序列吸引。例如，一些人更多地被技术吸引，而不是被动物、文本、已知或未知的人脸或人体、神秘符号或甚至数学公式吸引。据此，眼动跟踪模块2605的一个实施例学习由不同类型的图像触发的眼球运动的个人特定特征。接着使用来自视频图像2603的测得特征与参考数据(存储在眼动跟踪数据库2645中)的相似度来生成保证等级2606(即，合法用户的眼球正跟随在显示器2601上显示的“质询”图像、视频和其他内容的确定性)。

[0357] 图29中示出根据本发明的一个实施例的方法。该方法可在诸如图26所示的系统架

构内实施，但不限于任何特定系统架构。

[0358] 在2901处，针对给定用户和/或交易选择特定眼动跟踪模板，并且在2902处，在根据模板显示内容时捕捉用户面部的图像序列。例如，模板可指定内容的类型、内容的位置和显示内容的时序。或者，模板可仅大致指定眼动跟踪类型，而眼动跟踪模块2605可确定如何、何处和何时显示内容。

[0359] 不管如何选择和显示内容，都在2903处执行面部识别，并且在2904处使用所捕捉的图像序列执行眼动跟踪分析。在2905处，基于所捕捉的图像与面部模板之间的相关性生成面部保证等级。相似地，在2906处，基于用户眼球的运动与用户眼球的预期运动之间的相关性生成眼动跟踪保证等级。

[0360] 虽然在图29中示出为并行操作2903/2905和2904/2906，但可先执行面部识别操作2903/2905，接着可仅在面部识别操作得到高相关性/保证等级的情况下执行眼动跟踪操作2904/2906(或反之亦然)。

[0361] 在2907处，确定面部验证和眼动跟踪的综合结果是否足以允许进行当前交易。如果是，则在2909处准许交易。如果不是，则在2908处不允许交易或要求执行额外验证技术来提高保证等级。例如，在这个阶段，可要求用户在指纹传感器上轻扫手指或输入与用户帐户相关联的PIN。如果在2910处确定额外验证技术是足够的，则在2909处准许交易。

[0362] H.用于在验证期间收集并利用客户端数据以供风险评估的系统和方法

[0363] 一些类型的验证器是非常值得信任的，而有些则不是。因此，对于验证器，依赖方可具有某个保证度范围，并且可使用某些类型的客户端数据执行风险评估(例如，以上调或下调该保证度)。例如，如果远程验证器具有安全元件或可信执行环境(TEE)，则可使用证实密钥安全地签署该验证。证实密钥留在安全元件内部，任何外部实体均无法访问。实际验证操作也在安全元件内部执行。通过使用证实密钥签名，依赖方能够确定地知道有远程验证器负责验证尝试。

[0364] 如果远程验证器不含安全元件，则必须在软件中进行证实签署，而这会为攻击开启大门。一种减轻这个问题的方式是将证实密钥存储在受软件保护的“白盒”中。证实密钥无法离开白盒，并且会对验证尝试执行签署。然而，由于执行验证的代码与执行证实签署的白盒是分离的(并且白盒是基于软件的)，所以与使用安全元件或可信执行环境(TEE)相比，这种方式较不值得信任。

[0365] 最后，如果没有所有以上各项，也可完全在软件中进行整个验证操作。这种方式是最不安全的，因为验证代码和证实密钥本身均可能受到危及。

[0366] 在任何上述例子中，如果依赖方能够收集客户端数据来确定正在执行验证的特定方式，使得能够在执行验证时(例如，在生成保证等级时，如下文论述)评估客户端风险，则将是有益的。

[0367] 通过经由额外数据改善风险评估，本发明的一个实施例通过收集客户端数据并且评估与每个客户端相关联的风险来避免欺诈交易。接着可利用与客户端相关联的风险等级来指定针对特定交易验证用户时必须使用的验证技术。为了评估风险，本发明的一个实施例确定(1)可用于风险计算的数据类型，(2)如何获得Web浏览器无法安全提供的额外数据，以及(3)如何以不危及用户隐私的方式进行评估。

[0368] 病毒、蠕虫和恶意软件使计算机受感染的其中一个最大原因是，操作系统最近尚

未更新从而未关闭潜在漏洞。操作系统中的这些漏洞一旦被公众知晓，就很容易被犯罪分子利用。系统在没有更新的情况下运行越久，能够被利用的潜在漏洞就越多，并且密码可能受恶意代码危及的风险也越高。Web浏览器不允许网站访问用户计算机的更新历史。假如网站访问了，则网站可基于已知在其系统上的漏洞来识别潜在受害者。因此，本发明的一个实施例作为安全代理来运行，该安全代理作为本机应用程序(而非浏览器插件)来执行，用于收集客户端数据以确定当前操作系统版本和/或操作系统的更新近况。

[0369] 用户计算机受到恶意代码感染后，其中一种抵御恶意代码的方法是使用防病毒软件(例如，Windows® Defender®)。即使恶意代码已经渗透到系统中，防病毒软件也将至少向用户警告已经发生了一些坏事情，从而限制最终造成的损害。用户可更改帐户密码并且核查最近的交易。然而，如果没有安装防病毒软件，或者安装了防病毒软件但最近尚未运行防病毒软件，则用户很可能不知道其计算机上存在恶意代码。在那台计算机上发生的交易具有较高的欺诈风险。Web浏览器将不会透露是否在计算机上安装了防病毒软件。因此，在一个实施例中，本机代理应用程序定位并收集客户端配置数据以确定是否已经安装了防病毒软件，并且如果安装了，还确定防病毒杀毒软件更新并且/或者运行的近况。

[0370] 另一种抵御方法(尤其是在抵御蠕虫方面)是防火墙。如果在用户的机器上安装并启用了软件防火墙，这会大大减少攻击入口点的数量。通常将服务于从随机因特网主机经由导线发来的任何请求的开放端口会被削弱。因此，即使正在侦听端口的服务具有未修补的安全漏洞，风险也会被消除，因为不允许任何通信访问该服务。另一方面，在没有软件防火墙的情况下运行的计算机受蠕虫感染的可能性大得多，尤其是在其最近尚未更新的情况下。通过端口扫描，Web浏览器可间接检测成效有限的防火墙。因此，在一个实施例中，本机代理应用程序定位并收集防火墙配置数据以确定是否安装了防火墙，并且如果安装了，还确定防火墙的更新近况。

[0371] 如果用户的计算机实体失窃，则犯罪分子可收集大量信息并且用于实行欺诈。如果用户的机器受密码保护，并且优选地，整个硬盘驱动器被加密为那个密码，则由于盗窃而泄露信息的风险会被降低。如果没有进行密码保护，则可评估成具有较高的风险等级。因此，在一个实施例中，本机代理应用程序确定硬盘驱动器内容是否已被加密并且使用该信息作为其对客户端的风险评估的一部分。

[0372] 另外，如上文论述，如果客户端使用安全元件或可信执行环境(TEE)来执行验证，则依赖方可具有客户端提供的验证系合法的高确定度。如果远程验证器不含安全元件，则可利用受软件保护的“白盒”来保护证实数据(例如，证实密钥)。然而，如所提及的，由于执行验证的代码与执行证实签署的白盒是分离的(并且白盒是基于软件的)，所以与使用安全元件或可信执行环境(TEE)相比，这种方式较不值得信任。最后，如果没有所有以上各项，也可完全在软件中进行整个验证操作(如所提及的，这是最不安全的操作方式)。本发明的一个实施例允许依赖方收集上述客户端数据以确定正在执行验证的特定方式，使得能够在执行验证时评估客户端风险。

[0373] 如图30所示，在本发明的一个实施例中，客户端装置3000包括客户端风险评估代理3004，客户端风险评估代理3004收集各种类型的客户端配置数据3050并且作为响应，计算客户端3000的风险等级。在一个实施例中，客户端风险评估代理3004是本机代码代理应用程序，设计为直接在客户端3000的本机操作系统(OS)3010内运行。因此，客户端风险评估

代理3004不受与浏览器插件和其他类型的程序代码相关联的限制，出于安全原因，这些浏览器插件和程序代码访问客户端数据的能力受到限制。换句话讲，准许客户端风险评估代理3004收集在浏览器环境中运行的HTML和Javascript代码不被准许访问的数据。因此，即使可在浏览器环境内实施，验证引擎3010仍将能够访问由客户端风险评估代理3004提供的额外风险分析(但应该指出的是，验证引擎3010在同时仍符合本发明的基本原理的情况下不需要在浏览器背景内实施)。

[0374] 在一个实施例中，验证引擎3010包括保证等级计算模块3006，该模块用于计算与合法用户持有客户端装置3000的可能性对应的保证等级。随后可使用此保证等级来确定是否通过网络完成与远程依赖方3051的待决交易(例如，诸如金融交易、在线购买、访问用户账户中的机密信息等)。在一个实施例中，依赖方3051可指定给定交易所需要的保证等级。例如，对于涉及大额转账的金融交易，依赖方3051可能需要比(例如)涉及访问用户的电子邮件账户的交易相对更高的保证等级。虽然示出为单个实体，但“依赖方”可包括配备有用于执行本文所述的基础验证技术的单独安全交易服务器的网站或其他在线服务。

[0375] 在一个实施例中，保证等级计算模块3006将保证等级(例如，指定为值、百分比、代码等)传输到依赖方3051，而不公开由客户端风险评估代理3004收集的任何机密用户信息，从而保护用户的隐私。在另一个实施例中，保证等级计算模块3006知道当前交易所需要的保证等级，确定保证等级是否足够高，并且将关于交易是被准许还是拒绝的指示传输到依赖方3051，而同样不向依赖方3051公开用户的私人信息。

[0376] 在一个实施例中，客户端装置3000与依赖方3051之间的通信经由安全通信模块3013来保护，该安全通信模块3013可使用第一密钥加密传出通信并且使用第二密钥解密传入通信。在对称密钥加密方案中，第一密钥和第二密钥是相同的。在不对称密钥加密方案中，密钥是不同的。然而，本发明的基本原理不限于任何特定类型的加密。

[0377] 在一个实施例中，除了客户端风险评估代理3004所提供的风险数据之外，保证等级计算模块3006还基于当前用户验证结果3005来确定保证等级。具体地讲，用户验证结果3005可包括经由一个或多个显式用户验证装置3020至3021的当前或最近显式用户验证的结果。这可包括(例如)经由指纹装置的指纹验证、经由相机和面部识别硬件/软件的面部识别验证、经由麦克风和声音识别硬件/软件的声音识别、使用相机和相关联硬件/软件的视网膜扫描、最终用户经由小键盘进行的密码/PIN输入，和/或各种其他类型的显式用户验证装置和/或技术。

[0378] 在一个实施例中，安全存储装置3025以密码保护每个用户验证装置3020至3021的生物计量参考数据记录(例如，使用对称密钥包裹数据以使得存储装置3025安全)。尽管安全存储装置3025被示出为在验证装置3020至3021的安全周界之外，但在一个实施例中，每个验证装置3020至3021可具有其自己的集成安全存储装置来以密码保护生物计量参考数据记录。

[0379] 除了显式用户验证之外，验证引擎3010的一个实施例从传感器3043收集数据以供保证度计算模块3006用来生成保证等级。举例来说，传感器3043可包括位置传感器(诸如GPS传感器)以指示用户的当前位置。如果客户端装置3000处于预期位置，诸如用户的工作地或住宅，则这增加了用户是合法用户的可能性。相反，如果用户处于意外位置，诸如用户先前从未到访的外国，则这增加了用户不是合法用户的可能性。因此，在一个实施例中，保

证度计算模块3006将趋于在用户处于预期位置的情况下提高保证等级并且在用户处于意外位置的情况下降低保证等级。

[0380] 可使用各种其他传感器3043(诸如温度传感器、湿度传感器和加速度计)来收集与用户验证相关的数据。例如,温度/湿度传感器可提供当前温度/湿度,可将所述当前温度/湿度与由位置传感器指定的位置的已知温度/湿度进行比较。如果这些值明显不同,则这可指示客户端装置3000正被欺骗。声称位置与温度/湿度的比较可在远程服务器(诸如下文相对于图46A至46B所述的安全交易服务器4632)处进行。在另一个实施例中,装置上的加速度计可用于测量用户的步态并且将这些测量值与用户的已知步态进行比较。如果步态匹配(在指定阈值内),则这增加了合法用户持有客户端装置3000的可能性。

[0381] 如图31所示,可收集并使用与确定风险相关的各种类型的客户端配置数据,包括(例如)硬件数据3101、操作系统数据3102和应用程序数据3103。以举例而非限制的方式,硬件数据3101可包括客户端装置型号、处理器名称/类型、引导ROM版本和管理控制器版本。操作系统数据3102可包括当前操作系统版本、OS更新日期和当前引导模式(例如,从硬盘驱动器引导)。应用程序数据3103可包括关于防火墙是否激活、防火墙类型和版本的指示、关于是否安装了防病毒软件以及当前版本和对病毒定义文件的更新的指示、关于防病毒软件是否激活(例如,在运行期间积极监视客户端装置)的指示、上次全面和/或部分病毒扫描的指示以及最近病毒扫描的结果。另外,应用程序数据3103或OS数据3102可包括关于数据是以加密还是以其他安全方式存储在用户的持久性存储装置(例如,硬盘驱动器、快闪存储器等)上的指示。

[0382] 如所提及,在一个实施例中,保证等级计算模块3006考虑由客户端风险评估代理3004提供的风险评估数据和用户验证结果3005两者以得出合法用户正尝试当前交易的保证等级。以举例而非限制的方式,如果客户端配置数据3050指示当前客户端没有活动的防火墙或病毒检测软件,则其可向保证度计算模块3006报告该客户端呈现比启用这些特征的客户端高的风险。相似地,如果病毒检测软件最近(例如,在阈值时间段内)尚未被更新或执行,则客户端风险评估代理3004可向保证等级计算模块3006报告升高的风险。可在同时仍符合本发明的基本原理的情况下以多种方式指定风险等级。例如,风险等级可基于百分比(例如,0%=最小风险,100%=最大风险,并且介于两者间的所有数字均表示不同等级的中间风险)或以某个标度计的数值(例如,1=最小风险,10=最高风险,并且介于两者间的所有数字均表示不同等级的中间风险)。

[0383] 不管如何提供风险数据,在一个实施例中,保证等级计算模块3006均基于由客户端风险评估代理3004提供的风险数据来确定所需要的验证等级。例如,如果客户端风险评估指示相对高的风险值(例如,10当中的9或10),则保证等级计算模块3006可能需要更可靠的和/或显式的用户验证(诸如PIN/密码输入和/或指纹扫描)来针对当前交易验证用户。相反,如果客户端风险评估指示相对低的风险(例如,10当中的1或2),则保证等级计算模块3006可能需要针对当前交易进行非侵入式用户验证,诸如基于位置的验证和/或依赖于最近显式用户验证来进行当前交易。

[0384] 应该指出的是,为简单起见,将图31中的数据以表格格式布置。实际客户端配置数据150可以各种不同格式存储,包括二进制文件、分层文件系统布置、链表和OS注册表格式等等。本发明的基本原理不限于任何特定配置数据格式。

[0385] 如图30所指示，在一个实施例中，客户端风险评估代理3004能够通过OS访问客户端配置数据3050(例如，通过对由OS暴露的应用程序编程接口(API)进行适当调用)。在另一个实施例中，客户端风险评估代理3004直接从存储数据的基础文件系统访问客户端配置数据3050。在一个实施例中，客户端风险评估代理3004能够安全访问基础配置数据。可实施各种安全特征以确保配置数据3050的安全性，诸如信任链技术和安全区域。

[0386] 允许向网站提供额外风险信息的一个考虑因素是不忽略浏览器为什么不首先提供这个信息的合理性。当然，恶意网站可充分利用这个信息并且Web浏览器开发者有很好的理由来使该信息不被恶意网站获取。因此，如所提及，在一个实施例中，基础客户端配置数据3050不被直接提供到依赖方3051。相反，在一个实施例中，由客户端风险评估代理3004直接在客户端装置上评估客户端风险数据，并且风险值被提供到保证等级计算。依赖方3051只需要知道验证是否成功(如果事先指定保证等级的话)和/或当前保证等级。这样就保护了客户端的配置数据3050不被公开。

[0387] 图32中示出用于在验证期间评估客户端风险的方法的一个实施例。该方法可在图30至31所示的架构上实施，但不限于任何特定系统架构。

[0388] 在3201处，检索与客户端风险有关的客户端配置数据。这可包括(例如)防火墙或病毒检测软件的存在及当前状态和/或操作系统的当前版本(例如，OS的更新近况)。在3202处，评估客户端配置数据以确定客户端的风险值(例如，百分比、数值或能够指定风险等级的其他数据)。在3203处，使用客户端风险评估来确定保证等级。在一个实施例中，较高风险值需要较高保证等级(例如，风险值10可能需要高于90％的保证等级)。在另一个实施例中，基于所评估的风险来计算保证等级本身。例如，如上所述，风险值可被包括作为用于确定当前保证等级的许多变量(包括先前或当前用户验证)之一。

[0389] 在3204处，选择验证技术，其在成功完成的情况下将使保证等级提高到当前交易的可接受等级。例如，如果风险高，则可能需要显式用户验证。如果风险低，则先前最近验证或非侵入式验证可为足够的。

[0390] 在3205处，确定验证是否成功。如果是，则在3208处准许交易。如果不是，则在3206处，可能需要一种或多种额外验证技术或可能不允许交易。例如，如果当前保证等级不足，则可要求用户输入先前向依赖方3051提供的保密信息，或用户可提供其他/额外验证。如果在3207处确定额外验证技术是足够的，则在3208处准许交易。如果不是，则在3206处不允许交易。

[0391] I.用于针对本地交易执行验证的系统和方法

[0392] 本文所述的本发明的实施例包括用于针对通过本地安全交易装置发起的本地交易验证用户的技术。举例来说，本地交易可为提款、转账或其他用户发起的操作，并且安全交易装置可为ATM或能够执行金融交易的其他本地装置。相似地，本地交易可涉及在配备有本地安全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。

[0393] 如图33所示，在一个实施例中，具有生物计量验证装置和相关联软件的客户端装置3300通过网络向具有安全交易服务的依赖方3351验证以在本地安全交易装置3350上执行交易。具体地讲，当客户端装置3300的用户希望在本地与安全交易装置3350执行交易时，其发起与依赖方3351的一系列验证事务(其例子在下文中描述)。例如，可能需要用户在客户端装置3300上的指纹读取器上轻扫手指以及/或者经由客户端小键盘输入PIN或其他密

码。随后可将验证的结果从客户端装置3300传输到依赖方3351而不传输用户的私有数据(例如,指纹数据、PIN或任何其他私有用户数据),从而保护用户的隐私。

[0394] 响应于成功验证,依赖方3351可向本地安全交易装置3350传输信号以执行操作。例如,如果本地安全交易装置是ATM,则信号可指示ATM发放指定量的现金。如果本地安全交易装置3350是零售结账装置,则可传输成功支付的指示并且可记入用户账户的借方。

[0395] 另外,如图33所示,可在客户端装置3300与本地安全交易装置3350之间建立本地安全通信信道以补充用户验证过程。可使用客户端装置3300和本地安全交易装置3350上的无线通信接口,利用各种无线通信技术建立本地安全信道,所述无线通信技术诸如近场通信(NFC)、蓝牙或WiFi(例如,802.11x信道)等等。例如,当在本地安全交易装置3350附近时,客户端装置3300可经由其无线接口与本地安全交易装置3350的无线接口执行近场通信(NFC)握手,并且建立本地安全信道以在验证期间交换数据。

[0396] 本地安全信道的唯一存在性组成验证数据,因为其确立客户端装置3300的当前位置。因此,依赖方3351可在验证过程中使用此信息作为客户端装置3300的当前位置的证据。在一个实施例中,依赖方3351可将由本地安全交易装置3350提供的位置与由客户端装置3300报告的当前GPS位置进行比较以确认两个位置值是否匹配。

[0397] 另外,依赖方3351可将密码或其他验证数据传输到客户端装置3300,客户端装置3300可接着通过本地安全信道将密码或其他验证数据转送到本地安全交易装置3350以验证客户端装置。例如,在一个实施例中,依赖方3351将条形码传输到客户端装置3300并且将对应代码传输到本地安全交易装置。本地安全交易装置3350可接着使用条形码扫描器或相机读取条形码(例如,从客户端装置3300的显示器)以执行验证(即,将从依赖方接收的代码与从条形码读取的代码进行比较)。或者,本地安全交易装置3350可将从条形码读取的代码传输到依赖方,依赖方将接着确认代码是否匹配。相反,依赖方3351可将密码或其他验证数据传输到本地安全交易装置3350,本地安全交易装置3350将接着把这些数据转送到客户端装置3300以用于验证。因此,本地安全信道可用于针对多种验证技术交换数据。

[0398] 如所提及,在一个特定实施例中,本地安全交易装置3350是ATM装置。ATM机是易受攻击的装置,因为其输入/输出控件(例如,读卡器、键盘、屏幕、相机等)都暴露给“外界”,并且它们容易受到篡改。例如,可容易地用低技术装置(诸如隐藏的磁条读取器、镜子和摄影机)窃取借记卡记录和pin。在一个实施例中,使用涉及客户端3300与依赖方3351之间的通信的远程验证技术来为ATM机提供显著改进的验证。当与这种远程验证集成时,ATM本身不需要具有传统输入/输出控件,诸如读卡器、触摸屏或键盘。其需要的仅仅只是网络连接和用于发放现金的狭槽。验证本身可在配备有生物计量验证装置的顾客的客户端装置3300上执行。

[0399] 在一个实施例中,对于现金提取,用户将来到ATM机附近并且发起远程验证应用程序以向依赖方3351验证。用户将接着输入提款金额并且在移动装置的指纹传感器上轻扫其手指(或用户进行如下文论述的任何其他类型的验证)。当向依赖方3351确认了用户的存在性和真实性时,从ATM的狭槽发放指定量的货币。

[0400] 该实施例不仅提供更强的验证,而且还将复杂且昂贵的ATM转换为简单且可靠的取款机,这种取款机的构建和维护明显更便宜。这些新型ATM可使用很长时间。它们不需要频繁更新,因为直接在客户端装置3300和/或依赖方的安全交易服务器3351上引入了对生

物计量相关验证功能的所有更新。

[0401] 图34中示出本发明的一个实施例的额外架构细节。如图所示，该实施例的客户端装置3300包括本地验证应用程序3304，该应用程序与本地安全交易装置3350和依赖方3351两者进行通信以协调本文所述的各种本地验证技术。在一个实施例中，本地验证应用程序3304建立与本地安全交易装置3350的本地安全信道，并且验证引擎3310向依赖方执行远程验证以验证合法用户持有客户端装置3300。

[0402] 在一个实施例中，验证引擎3310通过进入与依赖方的安全交易服务器的一系列交易来执行验证，如上文提及的共同未决的专利申请中所述。例如，这些事务可包括登记过程，在登记过程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、记录声音等)。登记可在依赖方的安全交易服务器的指导下进行或可由用户自主地进行。用户可接着通过网络向安全交易服务器注册生物计量装置，并且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)向那些服务器验证。

[0403] 在一个实施例中，验证引擎3310包括保证等级计算模块3306，该模块用于计算与合法用户持有客户端装置3300的可能性对应的保证等级。随后可使用此保证等级来确定依赖方3351是否应授权本地安全交易装置3350处的本地交易(例如，诸如金融交易、零售购买、访问用户账户中的机密信息等)。在一个实施例中，依赖方3351可指定给定交易所需要的保证等级。例如，对于涉及大额转账的金融交易，依赖方3351可能需要比(例如)涉及访问用户的账户的交易相对更高的保证等级。

[0404] 在一个实施例中，保证等级计算模块3306将保证等级(例如，指定为值、百分比、代码等)传输到依赖方3351，而不公开任何机密用户信息，从而保护用户的隐私。在另一个实施例中，保证等级计算模块3306知道当前交易所需要的保证等级，确定保证等级是否足够高，并且将关于交易是被准许还是拒绝的指示传输到依赖方3351，而同样不向依赖方3351公开用户的私人信息。

[0405] 在一个实施例中，客户端装置3300与依赖方3351之间的通信经由安全通信模块3313来保护，该安全通信模块3013可使用第一密钥加密传出通信并且使用第二密钥解密传入通信。在对称密钥加密方案中，第一密钥和第二密钥是相同的。在不对称密钥加密方案中，密钥是不同的。然而，本发明的基本原理不限于任何特定类型的加密。

[0406] 在一个实施例中，保证等级计算模块3306至少部分地基于当前用户验证结果3305来确定保证等级，当前用户验证结果可包括经由一个或多个显式用户验证装置3320至3321的当前或最近显式用户验证的结果。这可包括(例如)经由指纹装置的指纹验证、经由相机和面部识别硬件/软件的面部识别验证、经由麦克风和声音识别硬件/软件的声音识别、使用相机和相关联硬件/软件的视网膜扫描、最终用户经由小键盘进行的密码/PIN输入，和/或各种其他类型的显式用户验证装置和/或技术。

[0407] 在一个实施例中，安全存储装置3325以密码保护每个用户验证装置3320至3321的生物计量参考数据记录(例如，使用对称密钥包裹数据以使得存储装置3325安全)。尽管安全存储装置3325被示出为在验证装置3320至3321的安全周界之外，但在一个实施例中，每个验证装置3320至3321可具有其自己的集成安全存储装置来以密码保护生物计量参考数据记录。

[0408] 除了显式用户验证之外，验证引擎3310的一个实施例从传感器3343收集数据以供保证度计算模块3306用来生成保证等级。举例来说，传感器3343可包括位置传感器(诸如GPS传感器)以指示用户的当前位置。如果客户端装置3300处于预期位置，诸如本地安全交易装置3350的已知附近，则这增加了用户是合法用户的可能性。相反，如果GPS读数指示用户不在本地安全交易装置3350附近，则这指示发起交易的用户不是合法用户。因此，在一个实施例中，保证度计算模块3306将趋于在用户处于预期位置的情况下提高保证等级并且在用户处于意外位置的情况下降低保证等级。

[0409] 可使用各种其他传感器3343(诸如温度传感器、湿度传感器和加速度计)来收集与用户验证相关的数据。例如，温度/湿度传感器可提供当前温度/湿度，可将所述当前温度/湿度与由位置传感器指定的位置的已知温度/湿度进行比较。如果这些值明显不同，则这可指示客户端装置3300正被欺骗。声称位置和温度/湿度的比较可在远程服务器(诸如依赖方3351所使用的安全交易服务器)上进行。在另一个实施例中，装置上的加速度计可用于测量用户的步态并且将这些测量值与用户的已知步态进行比较。如果步态匹配(在指定阈值内)，则这增加了合法用户持有客户端装置3300的可能性。

[0410] 可在同时仍符合本发明的基本原理的情况下以多种方式实施本地验证应用程序3304。例如，在一个实施例中，针对依赖方3351专门设计本地验证应用程序3304。例如，如果依赖方是银行机构(例如，富国银行(Wells Fargo®))，则本地验证应用程序3304可为由/为这家银行专门设计的应用程序。在另一个实施例中，可在多个依赖方当中共享同一本地验证应用程序3304，例如作为通用本地验证应用程序。此外，尽管在图34中示出为单独的逻辑组件，但图34中所示的验证引擎3310可集成在本地验证应用程序3304内。在另一个实施例中，本地验证应用程序3304可为Web浏览器或在Web浏览器环境内执行的应用程序(例如，当用户进入本地安全交易装置3350附近或连接到依赖方网页以发起交易时)。

[0411] 本地验证应用程序3304可执行多种本地功能，具体取决于依赖方所需要的具体实施。例如，在一个实施例中，本地验证应用程序3304接收由依赖方3351提供的密码(或其他验证数据)并且将密码安全地传输到本地安全交易装置3350以进行验证(例如，经由条形码或使用如上文论述的其他通信技术)。或者，在一个实施例中，用户可在本地安全交易装置3350中手动输入密码。相似地，可将由本地安全交易装置3350接收的验证数据(诸如密码)转送到本地验证应用程序3304，本地验证应用程序3304接着将验证数据转送到验证引擎3310和/或依赖方3351(例如，作为客户端装置3300的位置的证据)。

[0412] 图35中示出用于执行客户端装置的验证的方法的一个实施例。该方法可在图33至34所示的架构上实施，但不限于任何特定系统架构。

[0413] 在3501处，客户端进入本地安全交易装置(例如，ATM)附近，并且在3502处，经由本地信道与本地安全交易装置建立安全连接。如所提及，可使用近场通信、蓝牙、Wifi或客户端装置和本地安全交易装置两者支持的任何其他类型的协议来实施本地信道。在一些实施例中，可不需要操作3502。例如，当客户端装置能够以合法用户持有客户端装置的高保证等级向依赖方验证时，并且如果客户端装置能够向依赖方验证其当前位置，则本地信道可为不必要的。

[0414] 在3503处，客户端装置经由网络向依赖方验证。用于生成合法用户持有装置的保证等级的任何可用技术均可用于此操作。例如，用户可通过在生物计量指纹装置上轻扫手

指、捕捉面部图像以用于面部识别、以及/或者输入密码来执行显式验证。或者，可执行非侵入式验证技术，诸如确定用户最近(例如，在指定时间段内)是否已经向客户端装置显式地验证和/或使用传感器数据，诸如位置数据、温度/压力数据和/或加速度计数据。

[0415] 不管如何生成保证等级，都可以保护用户隐私的方式(例如，不提供专门识别客户端装置的数据)经由网络将验证的结果提供给依赖方。例如，如先前提及，可将保证等级本身和/或对验证成功或失败的指示提供给依赖方，而不公开任何机密的用户信息。

[0416] 如果在3504处确定验证成功，则在3507处准许本地交易。在一个实施例中，这涉及依赖方传输指示本地安全交易装置执行一个或多个操作的信号。例如，如果本地安全交易装置是ATM，则所述操作可包括发放用户指定量的现金。如果本地安全交易装置是借记装置(例如，在零售店或用户正进行购买的其他位置)，则由依赖方传输的信号可确认对交易的支付(并且相应地记入用户账户的借方)。应该指出的是，这些仅仅是示例性例子。可在同时仍符合本发明的基本原理的情况下采用各种替代应用程序。

[0417] 如果在3504处的验证不成功(例如，因为未达到可接受的保证等级)，则在3505处，拒绝交易并且/或者可能需要一种或多种额外验证技术。例如，可能需要用户使用一种或多种额外技术提供额外验证(例如，在初始验证是指纹的情况下输入密码，等等)。如果在3506处确定额外技术是足够的，则在3507处准许交易。如果不是，则再次拒绝交易并且/或者尝试额外验证技术。

[0418] J.用于在线交易的用户确认

[0419] 在许多场景中，完成与依赖方的交易可能需要一个或多个其他用户的批准。以举例而非限制的方式，家长可能想要批准由孩子发起的金融交易，指挥官可能需要批准由士兵发起的交易，管理人员可能需要批准由雇员发起的商业交易，并且密码密钥管理系统可能需要多个用户批准特定交易之后方可进行该特定交易。

[0420] 本发明的一个实施例使用本文所述的技术来经由网络提供强用户验证，从而启用多用户确认应用程序。图36中示出一个此类例子，该图示出具有远程验证功能的客户端装置3600，其由尝试发起与具有安全交易服务的依赖方3650(下文中简称为“依赖方”)的交易的用户控制。在一个实施例中，客户端装置3600的用户使用本文所述的一种或多种远程验证技术(例如，提供生物计量输入，诸如在指纹传感器上轻扫手指、输入PIN或密码，等等)向依赖方3650验证。

[0421] 在图示实施例中，其他客户端装置3601至3602具有向依赖方注册为客户端装置3600的用户的“批准人”的用户。因此，对于某些类型的交易(例如，涉及超过指定阈值的金额的金融交易)，依赖方可能需要客户端装置3601至3602的用户的批准。如下文论述，本文所述的远程验证技术用作批准过程的一部分。

[0422] 在一个实施例中，响应于客户端装置3600的用户的成功验证，依赖方3650处的通知生成逻辑向具有注册为“批准人”的用户的其他客户端装置3601至3602发送通知，该通知指示客户端装置3600的用户正尝试完成交易。可根据本发明的基本原理以多种方式发送通知。例如，如果客户端装置3601至3602是移动装置，则可向客户端装置3601至3602发送推送通知。作为另外一种选择或除此之外，可经由电子邮件、文本消息(例如，SMS)、即时消息或能够向客户端装置3601至3602递送消息的任何其他技术发送通知。

[0423] 在一个实施例中，通知包括客户端装置3600的用户正尝试的交易的细节。例如，如

果交易是金融交易，则通知可包括正被处理的特定金额以及正被执行的金融交易的类型(例如，提款、账户间转账等等)。或者，通知可包括链接(诸如超链接或其他类型的指针)，其将客户端装置3601至3602的用户引导到依赖方上的批准服务。一旦选择链接，就可向客户端装置3601至3602的用户提供交易的细节(例如，以网页或用于提供信息的其他有用格式)。

[0424] 在一个实施例中，在对通知做出响应并且审查交易的细节后，客户端装置3601至3602的用户可通过向依赖方执行远程验证(例如，使用本文所述的多因素验证技术)并且指示批准交易来确认请求。

[0425] 图37中示出本发明的一个实施例中所采用的客户端装置3600至3602的额外架构细节。具体地讲，该实施例的客户端装置3600至3602包括安全交易应用程序3704，该应用程序用于与依赖方3650通信并且协调本文所述的交易批准技术。安全交易应用程序3704可为独立应用程序，其经由安全应用程序编程接口(API)与验证引擎3710介接。或者，安全交易应用程序3704可被实施为移动装置应用程序或Web浏览器插件。

[0426] 除了协调本文所述的用户确认过程之外，在一个实施例中，安全交易应用程序3704还确保向每个用户显示的文本是与交易相关的实际文本。例如，应用程序3704可在安全窗口内显示文本并且要求用户提供验证以确认交易。该应用程序可启动计时器并且周期性地验证正向用户显示的当前窗口的内容(例如，通过在内容上生成签名)。可随机选择验证周期。因此，该应用程序持续确保每个用户在窗口内看到有效交易细节(从而确保交易文字尚未被“中间人”攻击修改)。如果该应用程序检测到内容已被篡改，则其阻止生成对交易的确认。

[0427] 在一个实施例中，在用户提供有效验证(例如，在指纹传感器上轻扫手指)之后，客户端装置识别用户并生成具有交易细节(例如，所显示的文本)和从依赖方提供的随机质询的令牌(密码签名)(例如，令牌可为对交易细节和随机数的签名)。这允许依赖方3650确保尚未在服务器与客户端之间修改交易细节。在一个实施例中，应用程序3704将所生成的令牌和用户名发送到依赖方，依赖方接着使用该用户名识别用户并且验证令牌。如果验证成功，则向客户端发送确认消息并处理交易。

[0428] 可针对源自客户端装置3600的交易请求/确认以及针对源自客户端装置3601至3602的用户的批准事务实施以上技术。

[0429] 返回到图37，在一个实施例中，可经由客户端装置3600至3602上的验证引擎3710执行验证，该验证引擎被设计为与依赖方3650执行一系列事务以远程验证每个用户。例如，如共同未决的申请中所描述，可采用验证框架和相关联的验证技术，其中用户向客户端的生物计量装置3720至3721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、记录声音等等)；经由网络向一个或多个依赖方3650(例如，配备有安全交易服务的网站或其他依赖方)注册生物计量装置；并且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)向那些依赖方3650验证。在一个实施例中，向依赖方“注册”包括针对每个用户验证装置3720至3721与依赖方交换对称或不对称密钥并将密钥存储在与每个验证装置3720至3721相关联的安全存储装置3725内。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，见请求注解(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。

[0430] 在验证阶段中，密钥用于(例如)生成签名、验证签名、以及/或者加密客户端3600至3602与依赖方3650之间的通信。一旦通过验证，用户便获许执行一个或多个在线交易。另外，在一个实施例中，敏感信息(诸如指纹数据和可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。

[0431] 在一个实施例中，验证引擎110包括保证等级计算模块3706，该模块用于计算与合法用户持有客户端装置100的可能性对应的保证等级。其可接着使用此保证等级来确定依赖方3650是否应授权当前交易。在一个实施例中，依赖方3650可指定给定交易所需要的保证等级。例如，对于涉及大额转账的金融交易，依赖方3650可需要比(例如)不涉及货币兑换或仅访问用户信息的交易相对更高的保证等级。

[0432] 在一个实施例中，保证等级计算模块106将保证等级(例如，指定为值、百分比、代码等)传输到依赖方3650，而不公开任何机密用户信息，从而保护用户的隐私。在另一个实施例中，保证等级计算模块3706知道当前交易所需要的保证等级，确定保证等级是否足够高，并且将关于交易是被准许还是拒绝的指示传输到依赖方3650(而不向依赖方3650公开用户的私人信息)。

[0433] 在一个实施例中，客户端装置3600至3602与依赖方3650之间的通信经由安全通信模块3713来保护，该安全通信模块3713可使用第一密钥加密传出通信并且使用第二密钥解密传入通信。在对称密钥加密方案中，第一密钥和第二密钥是相同的。在不对称密钥加密方案中，密钥是不同的。然而，本发明的基本原理不限于任何特定类型的加密。

[0434] 在一个实施例中，保证等级计算模块3706至少部分地基于当前用户验证结果3705来确定保证等级，当前用户验证结果可包括经由一个或多个显式用户验证装置3720至3721的当前或最近显式用户验证的结果。这可包括(例如)经由指纹装置的指纹验证、经由相机和面部识别硬件/软件的面部识别验证、经由麦克风和声音识别硬件/软件的声音识别、使用相机和相关联硬件/软件的视网膜扫描、最终用户经由小键盘进行的密码/PIN输入，和/或各种其他类型的显式用户验证装置和/或技术。

[0435] 在一个实施例中，安全存储装置3725以密码保护每个用户验证装置3720至3721的生物计量参考数据记录(例如，使用对称密钥包裹数据以使得存储装置3725安全)。尽管安全存储装置3725被示出为在验证装置3720至3721的安全周界之外，但在一个实施例中，每个验证装置3720至3721可具有其自己的集成安全存储装置来以密码保护生物计量参考数据记录。

[0436] 除了显式用户验证之外，验证引擎3710的一个实施例通过从传感器3743收集数据以供保证度计算模块3706用来生成保证等级，来执行非侵入式验证。举例来说，传感器3743可包括位置传感器(诸如GPS传感器)以指示用户的当前位置。如果客户端装置3600至3602处于预期位置，诸如已知附近(例如，“家”或“办公室”位置)，则这增加了用户是合法用户的可能性。相反，如果GPS读数指示用户不处于预期位置，则这指示发起交易的用户不是合法用户。因此，在一个实施例中，保证度计算模块3706将在用户处于预期位置的情况下提高保证等级并且在用户处于意外位置的情况下降低保证等级。

[0437] 可使用各种其他传感器3743(诸如温度传感器、湿度传感器和加速度计)来收集与用户验证相关的数据。例如，温度/湿度传感器可提供当前温度/湿度，可将所述当前温度/湿度与由位置传感器指定的位置的已知温度/湿度进行比较。如果这些值明显不同，则这可

指示客户端装置3600至3602正被欺骗。声称位置和温度/湿度的比较可在远程服务器(诸如依赖方3650所使用的安全交易服务器)上进行。在另一个实施例中,装置上的加速度计可用于测量用户的步态并且将这些测量值与用户的已知步态进行比较。如果步态匹配(在指定阈值内),则这增加了合法用户持有客户端装置3600至3602的可能性。

[0438] 另一种非侵入式验证技术包括测量自从上次成功用户验证以来已经过去的时间量。例如,如果用户最近已经执行了显式用户验证(例如,就在几分钟之前在指纹读取器上轻扫手指),则这将往往指示合法用户仍持有客户端装置(从而导致高基线保证等级)。相反,如果上次显式验证已经是几小时或几天之前了,则可能需要新的显式用户验证来达到可接受的保证等级。

[0439] 图38中示出根据本发明的一个实施例的方法。在3801处,客户端的用户触发需要N个其他用户确认的交易。例如,依赖方处的用户账户可指示由用户发起的某些类型的交易(或所有交易)需要一个或多个其他用户确认。例如,用户的账户可将用户识别为未成年人,从而需要一个或多个家长或监护人授权。在3801处,还通过实施本文所述的一种或多种验证技术来验证用户。

[0440] 在3802处,服务器选择必须确认用户所触发的交易的N个其他用户。例如,在检测到用户发起交易后,依赖方可查询其用户数据库,以确定交易需要确认以及能够确认该交易的用户的身份。在一个实施例中,能够确认交易的所有用户的子组可实际上确认交易。例如,在一个实施例中,如果用户是有两位家长的未成年人,则可向两位家长发送通知,但任一位家长的确认都将允许交易继续进行。相似地,可有10个用户被授权确认商业交易,但只需要其中2个确认来允许交易继续进行。

[0441] 在一个实施例中,可将推送通知发送到能够确认交易的那些用户的客户端装置(例如,如果用户具有能够接收推送通知的客户端装置)。作为另外一种选择或除此之外,可经由电子邮件、文本消息(例如,SMS)、即时消息或能够向客户端装置递送消息的任何其他技术发送通知。在一个实施例中,可向服务器注册用户以通过两个或更多个通信信道接收确认消息。例如,用户可接收包含确认请求的推送通知和电子邮件两者。

[0442] 不管如何发送确认请求,在3803处,N个用户的全部或子组均在确认过程中向服务器执行验证。任何远程验证技术可用于验证用户并确认交易。例如,用户可通过向先前已经向依赖方注册的客户端上的生物计量装置提供生物计量数据(例如,在指纹扫描器上轻扫手指)来确认交易。如上所述,可经由能够安全地显示文本和其他信息(即,确保当用户确认交易时,他/她已经查看描述交易的实际未更改文本)的安全交易应用程序向用户提供与交易相关联的细节。

[0443] 一旦在3804处确定最小指定数量的用户已经确认了请求,便在3807处准许交易。该方法的一个实施例启动确认计时器以测量自从发送确认请求以来已经过去的时间量。一旦在3805处确定确认计时器已经达到阈值(例如,几小时、一天等),便在3806处不允许交易。方法在3804处等待最小指定数量的用户确认请求,直到达到计时器阈值。

[0444] K.用于委托信任的系统和方法

[0445] 现有验证系统不允许使用可信客户端上的注册验证器启用新验证器。例如,如果用户的电话上有她已经向多个网站注册的指纹传感器,并且接着她在电话上安装了声音验证器,则她无法自动地向她注册指纹传感器的所有网站注册其声音验证器。相反,在这种情

况下,用户必须逐步通过相同的登记和注册过程来向依赖方注册声音验证器。相似地,如果用户购买了具有一组新验证器的新装置,则用户必须向服务器重新登记和重新注册所有新验证器。

[0446] 下文描述的本发明的实施例允许用户容易地使用已经启用并向一个或多个依赖方注册的可信客户端装置来启用并注册新客户端装置上的验证器。具体地讲,这些实施例可用于启用新验证器、启用新客户端装置、以及在多个客户端装置之间保持注册同步。

[0447] 图39提供根据本发明的一个实施例的信任委托的高级概览。可信装置3902(即,具有向一个或多个依赖方3950注册的验证器的装置)建立与用户的新客户端装置3900的安全连接。建立安全连接的具体方式与本发明的基本原理无关。可使用各种技术,诸如近场通信(NFC)、蓝牙、Wifi Direct、使用快速响应(QR)代码以及建立HTTPS连接。在一个实施例中,装置可交换安全连接所需要的大型随机令牌(LRT),并且可通过向在线服务提供所捕捉的LRT来建立连接并且经由该服务自举安全通信。

[0448] 在一个实施例中,一旦在可信客户端装置3902与新客户端装置3900之间建立安全连接,便实施安全协议(下文详细描述)以将注册数据从可信装置传送并集成到新装置。一旦已经传送注册内容,便在新客户端装置3900与依赖方3950之间实施另一个安全协议(例如,在一个实施例中为HTTPS)来验证注册内容。

[0449] 尽管本文所述的实施例注重于传送用于与依赖方3950的验证事务的验证数据,但为了符合本发明的基本原理,可不需要依赖方。例如,可信装置3902可建立安全连接以向新客户端装置3900提供验证数据,而在系统中不会涉及任何依赖方(例如,以提供用于在本地向新客户端装置3900验证的验证数据)。

[0450] 如图40所示,可分别在新装置3900和可信装置3902上执行信任委托模块4000至4001,以建立安全连接、交换注册内容、以及向每个依赖方3950上的安全交易服务4004验证注册内容。如本文所用,“可信验证器”是用户已经向一个或多个依赖方注册的验证器。“新验证器”是用户希望使用当前用于可信验证器的所有依赖方注册内容进行启用的验证器。因此,如果验证引擎3711先前已经向依赖方注册了一个或多个用户验证装置3720至3721,则该验证引擎被视为可信验证器。一个实施例的目标是将新装置3900的验证引擎3710从新验证器转变为可信验证器。“可信装置”是具有可信验证器的装置,“新装置”是具有新验证器的装置。

[0451] 信任委托是指使用可信验证器启用新验证器的过程。因此,信任委托的先决条件是:用户具有可信装置;用户具有新装置;用户想要从可信装置向新装置委托信任。

[0452] 返回到图40,在一个实施例中,用户发起新客户端装置3900上的信任委托应用程序4000和可信客户端装置上的信任委托应用程序4001,以建立初始安全连接。在一个实施例中,信任委托应用程序可为移动装置应用程序,其专门被设计来执行本文所述的信任委托操作。在另一个实施例中,信任委托应用程序可为响应于用户指示他/她希望执行信任委托而执行的浏览器插件(例如,经由具有嵌入式Javascript或其他小程序或可执行程序代码的网页)。此外,信任委托应用程序4000至4001可为较大应用程序(诸如被设计为管理向依赖方的验证的验证应用程序)内的软件模块。然而,应该指出的是,本发明的基本原理不限于信任委托应用程序4000至4001的任何特定具体实施。

[0453] 在一个实施例中,为了批准可信装置3902上的信任委托操作,用户在本地向可信

装置上的验证引擎3711验证(例如,向用户验证装置3722至3723提供生物计量输入)。相似地,在一个实施例中,用户可在本地向新客户端装置3900上的验证引擎3710验证。这两个验证步骤可提供对信任委托应用程序4000至4001执行委托过程的授权。

[0454] 如所提及,信任委托应用程序4000至4001可利用其相应客户端装置3900、3902上可用的任何通信接口来建立安全连接(例如,用于蓝牙连接的蓝牙接口、用于NFC连接的NFC接口等)。

[0455] 一旦建立安全连接,在一个实施例中,可信客户端3902的信任委托应用程序4001便提供指示向依赖方注册的可信客户端上的密钥数量(N)的数据。作为响应,在一个实施例中,信任委托应用程序4000生成N个新装置密钥对(ND_Uauth),密钥对包括一个私有密钥(ND_Uauth.priv)和一个公共密钥(ND_Uauth.pub),并且信任委托应用程序4000将这N个新装置公共密钥发送到可信装置3902上的信任委托应用程序4001。

[0456] 在一个实施例中,信任委托应用程序4001接着用对应的可信装置私有密钥(TD_Uauth.priv)签署这N个新装置公共密钥中的每一个,以生成与N个新装置公共密钥中的每一个相关联的签名(TD_Uauth.sig)。在一个实施例中,“对应”的私有密钥是与向对应的依赖方进行的特定注册相关联的私有密钥。信任委托应用程序4001还可向所生成的签名中插入时戳,该时戳可随后由依赖方用来验证发生信任委托的确切时间。在一个实施例中,可信客户端3902的信任委托应用程序4001接着将每个所生成的签名以及与每个依赖方相关联的其他注册数据传输到新客户端3900上的信任委托应用程序4000。每个依赖方的数据可包括:一个或多个依赖方ID代码(例如,识别依赖方处的服务的应用程序ID代码)、在依赖方处为用户注册的用户名、在验证期间由依赖方用来定位恰当密钥的密钥ID代码、以及与验证过程相关的任何其他数据。

[0457] 在一个实施例中,一旦信任委托应用程序4000接收到签名和其他注册数据,其便将这些数据集成到本地安全存储装置3725中,使得其可随后在新客户端装置3900连接到依赖方3950时使用。

[0458] 在一个实施例中,在注册数据已存储在本地安全存储装置3725中之后,信任委托应用程序4000可执行一系列自举操作,以利用新客户端装置3900上的向先前已经向可信客户端装置3902注册的依赖方(例如,网站、服务等)进行的已委托注册。或者,所描述的自举操作可由验证引擎3710本身执行(经由与安全交易服务4004的直接通信,如图40所示)。不管新客户端装置3900上的哪个特定软件组件执行这些操作,本发明的基本原理都保持不变。

[0459] 具体地讲,在一个实施例中,依赖方3950的安全交易服务4004检测到在新客户端装置3900上存在使用由安全交易服务4002和信任委托应用程序4000支持的远程验证协议的注册内容。在一个实施例中,安全交易服务4004可最初要求用户从新客户端装置3900执行生物计量验证或其他形式的验证(例如,输入安全代码)。另外,在该阶段,安全交易服务4004可验证插入到签名中的时戳并确保时戳不早于阈值时间量。

[0460] 假设用户成功地以可接受的保证等级提供生物计量或其他验证数据,则信任委托应用程序4000和/或新验证器3710准备包括以下三个断言的响应:

[0461] 1.对与依赖方相关联的新装置公共密钥(ND_Uauth.pub)的证实。在一个实施例中,该证实包括在公共密钥上生成的签名(例如,使用依赖方的公共密钥)。

[0462] 2.使用与依赖方相关联的新装置私有密钥(ND_Uauth.priv)的断言。在一个实施例中,为了生成该断言,使用私有密钥来在依赖方已知的内容(例如,诸如从依赖方发送的随机质询)上生成签名。因为向依赖方提供了公共密钥(在步骤1中),所以依赖方可解密该内容,从而验证私有密钥是否用于加密该内容。

[0463] 3.先前由可信客户端装置生成并且与用于该特定依赖方的新装置公共密钥相关联的签名(TD_Uauth.sig),以及由依赖方用来定位公共密钥的密钥ID(TD_Uauth.keyid)(例如,使得其可使用该密钥ID来查询其安全交易数据库4025以检索公共密钥)。

[0464] 在一个实施例中,接着在远程验证响应中将所有以上数据传输到依赖方的安全交易服务4004。

[0465] 在一个实施例中,在接收到以上断言之后,安全交易服务4004可执行以下验证:

[0466] 1.使用密钥ID定位可信装置的公共密钥(TD_Uauth.pub);

[0467] 2.使用可信装置的公共密钥(TD_Uauth.pub)验证由可信装置生成的签名(TD_Uauth.sig);

[0468] 3.使用装置的公共密钥(ND_Uauth.pub)验证由新装置的私有密钥生成的签名(ND_Uauth.sig);以及

[0469] 4.验证对与依赖方相关联的新装置公共密钥(ND_Uauth.pub)的证实。

[0470] 在一个实施例中,使用依赖方的私有密钥执行此验证。

[0471] 图41中示出用于安全地将注册数据从可信装置传送到新装置的方法的一个实施例,并且图42中示出用于向依赖方验证注册数据的方法的一个实施例。尽管这些方法可在图39至40所示的系统架构的环境内实施,但本发明的基本原理不限于任何特定系统架构。

[0472] 首先转到图41,在4101处,新装置建立与可信装置的安全通信信道并确定要生成的密钥对的数量(N)。如所提及,这可为可信装置向依赖方注册的密钥对的数量。

[0473] 在4102处,新装置生成N个新的公共/私有密钥对。在利用对称密钥的替代具体实施中,新装置可生成要与依赖方共享的单个(对称)密钥。在4103处,将N个公共密钥发送到可信装置,并且在4104处,可信装置用对应私有密钥签署每个公共密钥以生成签名。在4105处,将签名连同用于依赖方的其他注册数据(例如,密钥ID、应用程序ID等)发送到新装置。最后,在4106处,将所有注册数据和签名集成在由验证引擎使用的本地安全数据库内。

[0474] 现在转到图42,在4201处,新客户端(已经执行了图41的委托操作)建立与依赖方的安全连接。在4202处,依赖方检测到存在已经被委托给新装置的现有注册内容。作为响应,在4203处,依赖方向新装置发出验证请求。用户可接着使用一种或多种生物计量或其他验证技术进行验证。如上文论述,在4204处,新装置准备响应,该响应包括对新装置公共密钥的证实、用新装置私有密钥生成的签名(例如,在质询上)、以及用可信装置的私有密钥生成的签名和相关联的密钥ID。在4205处,将响应中的所有数据传输到依赖方,并且在4206处,依赖方验证响应中包含的数据(参见上文了解一个实施例的细节)。如果验证成功,则在4207处,用户正尝试的交易被获准。

[0475] 本文所述的技术可用于在不同装置上的两个验证器之间委托信任(如上所述)。另外,在一个实施例中,这些技术可用于在同一装置上的两个验证器之间委托信任。在这种情况下,不需要建立两个装置之间的安全连接,但可在装置内的两个验证器之间执行所有其他操作。

[0476] 此外,应该指出的是,所涉及的一些操作可以各种方式来实施。例如,用于委托信任的安全协议可由信任装置而不是新装置发起。在任一种情况下,新装置(或,更具体地讲,新装置上的验证器)可生成多个新密钥对(ND_Uauth),并且可信装置上的验证器可签署这些密钥对中的公共密钥。

[0477] L.用于隐私增强型数据同步的系统和方法

[0478] 所存在的当前系统用于使用云服务在多个客户端装置之间同步数据。当用户在装置上创建新文档(例如,拍摄照片、创建文字处理文档等)或修改现有文档时,用户所订购的云服务将通常“在云中”存储新文档/已修改文档的复本。当用户从第二装置(例如,在工作地的计算机或由不同家庭成员所使用的另一个装置)访问云服务时,云服务可被配置为同步该装置。

[0479] 存在的一个问题是:数据经常在云服务中以未加密格式存储,这使得数据容易受到各种类型的网络攻击和联邦机构的查询。

[0480] 下文所述的本发明的实施例提供一组协议和技术,它们允许以隐私增强方式在装置之间同步数据。通过使用这些协议和技术,云服务不再访问呈明文(例如,未加密格式)的数据,从而保护用户的隐私。

[0481] 首先应该指出的是,下文所述的用于在装置之间同步数据的技术并不依赖于本文所述的高级验证技术。例如,可在如针对本发明的其他实施例所描述的远程用户验证系统的环境外采用这些同步技术。然而,这些同步技术可用于针对这些远程用户验证实施例执行同步。例如,在一个实施例中,可使用这些同步技术在多个装置之间同步用于用户所访问的每个网站或其他在线服务的注册数据。

[0482] 如本文所用,“圈子”意指用户所信任的装置组成的网络,并且“圈子id”意指识别圈子的识别符(例如,无法轻易猜到的识别符)。“圈子云”意指用于存储关于圈子和信任链(下文定义)的信息并且充当客户端装置的通信枢纽的在线服务。在一个实施例中,圈子云不存储任何机密数据(至少不呈未加密格式)。术语“d.pub”是指装置的公共密钥,“d.priv”是指装置的私有密钥,并且d.pub/d.priv是指装置d的不对称公共/私有密钥对。在一个实施例中,d.priv从不离开装置d。“信任链”意指存储在圈子云上的持久性数据,其包含关于用户所信任的装置及其关系的信息。“圈子信道”意指由圈子云提供的安全通信信道,其由两个(或更多个)装置用来在它们之间交换和同步数据。

[0483] 本发明的一个实施例包括用于允许新用户装置(a)加入圈子并且(b)随后与圈子同步的协议和相关联技术。将结合图43描述这些实施例,该图示出三个客户端装置4301至4303,其分别具有用于实施本文所述的协议和技术的隐私同步应用程序4311至4313,以及用于存储加入和同步所使用的数据的安全数据存储装置4321至4332。装置4301在本文中有时称为装置d1,装置4302有时称为装置d2,装置4303有时称为装置d3。

[0484] 在一个实施例中,通过包括多个存储服务器的圈子云4350执行加入和同步。圈子云4350内的信任链4360维持定义装置4301至4303之间的信任关系的数据,如下文所述。圈子信道4370包括由圈子云提供的安全通信信道,其由两个或更多个装置用来交换和同步数据。

[0485] a.加入圈子

[0486] 装置4302(d2)加入属于用户的装置4301(d1)和4303(d3)组成的现有网络(即,可

信装置的“圈子”)。只有在已经是现有圈子的一部分的另一个装置4301授权的情况下,装置4302才能加入那个圈子。

[0487] 图44中示出用于使用可信装置4301授权新装置4302的方法的一个实施例。在4401处,用户在现有可信装置4301上授权新装置4302。例如,在一个实施例中,用户可发起可信装置4301上的隐私同步应用程序4311和新客户端装置4302上的隐私同步应用程序4312。

[0488] 在4402处,在一个实施例中,隐私同步应用程序4311至4312致使装置4301至4302建立安全连接。可使用各种技术建立安全连接,诸如近场通信(NFC)、蓝牙、Wifi Direct、使用快速响应(QR)代码以及建立HTTPS连接。

[0489] 在4403处,装置4301将安全数据发送到新装置4302,本文中将该数据称为“join1_data”。在一个实施例中,join1_data包括以下字段:{d1.pub,sk.sym,circle-id},其中d1.pub是装置4301的公共密钥,sk.sym是装置4301所生成的随机生成的会话密钥,并且circle-id是识别装置4302正加入的圈子的唯一识别代码。

[0490] 在4404处,装置4302读取join1_data并且准备响应,该响应可包括以下各项:

[0491] • HMAC(sk.sym,d2.pub|T)|d2.pub|T,其中T是时戳

[0492] • trust-block1＝S(d2.priv,d1.pub)|d1.pub|d2.pub

[0493] 请注意,HMAC代表基于散列的消息验证代码。在以上实施例中,通过使用HMAC或类似算法将装置4302的公共密钥与时戳连在一起并且用sk.sym保护该结果的完整性来生成HMAC。另外,trust-block1包括使用装置4302的私有密钥在装置4301的公共密钥上生成的签名。在一个实施例中,trust-block1条目还包括时戳(T)。

[0494] 返回到图44,在4405处,装置4302安全连接到圈子云4350并且传输包括HMAC和trust-block1的响应。圈子云4350存储由装置4301接收的数据,并且等待装置4301连接。

[0495] 在4406处,装置4301使用圈子id连接到圈子云,验证装置4302在操作4405中的响应中所包含的数据的完整性,并且生成trust-block2。具体地讲,在一个实施例中,装置4301使用sk.sym读取并验证d2.pub和T的完整性(例如,使用sk.sym解密d2.pub和T)。装置4301接着使用其自己的私有密钥d1.priv签署d2.pub,并生成trust-block2＝S(d1.priv,d2.pub)|d2.pub|d1.pub,其包括用d1 priv在d2.pub上生成的签名。在一个实施例中,trust-block2还包括时戳(T)。装置4301接着将以上包括trust-block2的数据发送到圈子云4350。

[0496] 在4407处,圈子云4350将这两个信任块添加到信任链4360。在一个实施例中,在以上操作之后,装置4302加入与圈子id相关联的圈子。这个圈子中的所有装置4301、4303信任装置4302,并且装置4302信任所有这些装置。请注意,任何可信装置均可使用本文所述的技术授权新装置。

[0497] b.与圈子同步

[0498] 在这个过程中,属于同一圈子的装置4301至4303在它们之间同步数据。可紧接这个过程之后实施不同的应用程序特定的子协议。例如,在线云存储应用程序可能想要保持用户的数据在所有装置上同步并且将加密复本保留在圈子云上。另一个应用程序可将消息传播到圈子中的装置。例如,在一个实施例中,可跨圈子中的所有装置同步一个装置用来向远程依赖方验证的注册数据。可在同时仍符合本发明的基本原理的情况下实施各种其他应用程序和子协议。所有此类子协议可使用下文所述的基本过程块。

[0499] 信任链

[0500] 如“加入圈子”过程(图44)中所展示,进入信任链4360的是断言装置2受装置1信任的证据。因此,信任链4360是一连串授权块,其中的每一个断言两个装置之间的信任关系。在一个实施例中,信任链是可交换的,这意味着如果装置4301信任装置4302,则装置4302信任装置4301。如果存在断言装置4301信任装置4302的块而不存在断言装置4302信任装置4301的块,则信任链4360被视为破裂。在一个实施例中,信任链4360还是可传递的,这意味着如果装置4301信任装置4302并且装置4302信任装置4303,则装置4301信任装置4303。在一个实施例中,信任链是圈子id特定的,并且不包含关于装置的任何机密信息。

[0501] 在一个实施例中,信任链4360包括多个信任块并且每个块包括以下数据:{di.pub,dj.pub,S(di.priv,dj.pub),S(dj.priv,di.pub)}-即,每个装置的公共密钥,以及使用每个装置的私有密钥在每个其他装置的公共密钥上生成的签名。

[0502] 以上断言意味着装置di信任装置dj并且反之亦然。在一个实施例中,装置4301至4302使用信任链4360来确定并验证哪些装置在圈子中。在装置验证它们在同一个圈子中之后,它们可使用圈子信道4370来在它们之间同步加密数据。

[0503] 在一个实施例中,为了确定装置di是否与装置dj在相同的圈子中,执行以下操作:(a)构造有向图,其中每个节点是信任链中的装置并且每个箭头对应于信任链中的块,并且(b)确定是否存在连接di与dj的直连路径。

[0504] 圈子信道

[0505] 在一个实施例中,实施图45所示的过程以在同一圈子中的其他装置之间同步数据。在图示例子中,装置4301(d1)是具有新数据并且想要发送到其他装置的装置。在4501处,装置4301下载与圈子id相关联的信任链4360,从信任链识别同一圈子中的其他装置(例如,装置4302至4303),并且使用信任链获得同一圈子中的其他装置的公共密钥。

[0506] 在4502处,装置4301生成随机加密密钥(REK)(例如,使用已知的随机数生成技术)。在4503处,装置4301针对圈子中的每个其他装置得出双向会话密钥(SK)。在一个实施例中,装置4301使用Diffie-Hellman密钥交换算法相对于每个其他装置得出SK。Diffie-Hellman是一种熟知的算法,其允许彼此先前不了解的两方共同建立共享秘密密钥。在这种情况下,例如,如果第一装置具有密钥对并且将其公共密钥提供给第二装置,则第二装置可独立地使用其私有密钥和第一装置的公共密钥来自动得出新密钥(在本申请中为SK)(并且反之亦然)。在一个实施例中,装置4301使用这些技术来为每个其他装置4302、4303生成不同SK。

[0507] 在4504处,装置4301针对每个装置用每个导出的SK加密REK并且将恰当的公共密钥与其绑定在一起。例如,对于分别针对装置di和dj生成SKi和SKj的装置d1,其使用会话密钥来如下加密REK:

[0508] {d1.pub,di.pub,E(SKi,REK)}(对于装置di)

[0509] {d1.pub,dj.pub,E(SKj,REK)}(对于装置dj)

[0510] 在该过程的最后,装置di和dj中的每一个能够使用其相应会话密钥(已由每个装置使用Diffie-Hellman独立地得出,如上文论述)解密REK。

[0511] 在4505处,装置4301用REK加密待同步数据——即,E(REK,data-to-be-synced)。如所提及,可以此方式同步任何数据,诸如多媒体文件、效率文档和/或客户端配置数据(例

如,依赖方注册数据,如上文论述),等等。

[0512] 在4507处,装置4301向圈子信道提供用每个SK加密的REK和用REK加密的待同步数据:

[0513] [{d1.pub,di.pub,E(SKi,REK)},{d1.pub,dj.pub,E(SKj,REK)},…]

[0514] E(REK,data-to-be-synced)

[0515] 在已经将该数据提供给圈子信道之后,在4506处,同一圈子中的各个装置下载对应于其公共密钥的记录(例如,用于装置di的{d1.pub,di.pub,E(SKi,REK)}),得出相同SK(例如,SKi),解密REK,并且使用REK解密待同步数据。

[0516] 在一个实施例中,如上所述的“加入圈子”操作可能需要对装置1和装置2进行用户验证。当使用本文所述的远程验证技术实施该协议时,可能需要用户(例如)“轻扫”手指来对两个装置进行验证,从而发起并完成“加入圈子”过程。与此相反,在一个实施例中,如所描述的在装置之间同步数据可能不需要用户验证。

[0517] 本文所述的协议和相关联技术允许构建彼此信任的装置组成的网络。值得注意的是,传输到云和从云传输以及存储在云中的所有数据均被加密。因此,可在多个装置之间同步数据而不在云上存储任何机密数据,从而使用户隐私保护得到改进。

[0518] 上文所述的本发明的实施例实施私有同步协议来实现装置同步,其中参与的云存储装置无法查看任何呈明文的用户数据(即,数据在云中被加密)。这些实施例包括各种新颖且有益的特征,包括但不限于:

[0519] • 一种实施装置同步协议的系统和方法,其中装置具有用于授权其他装置的公共密钥和私有密钥。

[0520] • 一种实施信任链以指示同一圈子内的装置之间的信任关系的系统和方法。

[0521] • 一种系统和方法,其中装置使用Diffie-Hellman或类似密钥交换算法来生成双向会话密钥并且用那些密钥加密数据。

[0522] • 一种系统和方法,其中圈子id的散列存储在圈子云中而非存储在装置本身上。

[0523] • 一种系统和方法,其中圈子云使用质询响应协议来在允许装置将任何数据放入圈子的圈子信道中之前验证该装置。

[0524] • 一种系统和方法,其中使用持久性圈子群组密钥来加密同步数据。

[0525] • 一种应用程序,其使用所描述的私有同步协议来在多个装置之间共享用户的数据(文档、文件、照片等)并将数据的加密备份存储在云上。

[0526] • 一种系统和方法,其中装置的私有密钥(d.priv)和使用此密钥的所有操作在验证器内部实施以经由网络远程验证用户。

[0527] • 一种应用程序,其结合本发明的实施例使用所描述的私有同步协议来执行对新装置的用户控制信任委托,从而在用户的装置之间共享验证器注册内容。

[0528] • 一种应用程序,其结合本发明的实施例使用所描述的私有同步协议来执行对新装置的用户控制信任委托,从而在用户的装置之间共享新注册内容,其中用户不需要在每次向其他装置委托新注册内容时都向验证器进行验证。

[0529] • 属于同一用户并且形成圈子的一组验证器,其中这些验证器使用上文所述的私有同步协议来同步验证密钥对,以便与属于同一圈子的其他验证器共享单个验证器的注册内容。

[0530] M.示例性系统架构

[0531] 应该指出的是,本文中使用术语“依赖方”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)。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。这些区别在下文论述的图46A至46B中列举,这些附图示出“依赖方”可包括网站4631和其他网络服务4651,以及用于代表网站和网络服务执行验证技术的安全交易服务器4632至4633。

[0532] 具体地讲,图46A至46B示出包括用于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46A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46B所示的实施例不需要浏览器。本文所述的各种高级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,上文所述的客户端装置内的验证引擎(例如,230)可被实施为包括接口4602的安全交易服务4601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46A至46B所示的那些之外的硬件与软件的逻辑布置来实施。

[0533] 转到图46A,图示实施例包括配备有一个或多个验证装置4610至4612的客户端4600,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4610至4612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)、以及光学识别功能(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4601可将这些生物计量数据作为生物计量模板数据(经由接口4602)存储在安全存储装置4620中。

[0534] 尽管安全存储装置4620被示出为在验证装置4610至4612的安全周界之外,但在一个实施例中,每个验证装置4610至4612可具有其自己的集成安全存储装置。另外,每个验证装置4610至4612可以密码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得存储装置4620安全)。

[0535] 验证装置4610至4612通过由安全交易服务4601暴露的接口4602(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4601是用于经由网络与一个或多个安全交易服务器4632至4633通信以及用于与在web浏览器4604的环境内执行的安全交易插件4605介接的安全应用程序。如图所示,接口4602还可提供对客户端4600上的安全存储装置4620的安全访问,该安全存储装置4620存储与每个验证装置4610至4612相关的信息,诸如装置识别代码、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并且在经由网络(诸如因特网)与服务器4630通信时使用。

[0536] 除了装置登记之外,安全交易服务4601还可接着经由网络向安全交易服务器4632至4633注册生物计量装置,并且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)向那些服务器验证。验证过程可包括本文所述的任何验证技术(例如,基于显式或非侵入式验证技术在客户端4600上生成保证等级并将结果传输到安全交易服务器4632至4633)。

[0537] 如下文论述,安全交易插件4605支持某些类型的网络交易,诸如与网站4631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4630内的网络服务器4631(下文中有时简称为“服务器4630”)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4605可将交易转发到安全交易服务4601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4601可开启与当地交易服务器4632(即，与网站位于同一地点)或异地交易服务器4633的直接通信信道。

[0538] 安全交易服务器4632至4633耦接到安全交易数据库4640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46A所示的安全企业或web目的地4630内的逻辑组件。例如，网站4631和安全交易服务器4632至4633可在单个物理服务器或单独物理服务器内实施。此外，网站4631和交易服务器4632至4633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。

[0539] 如上所述，本发明的基本原理不限于图46A所示的基于浏览器的架构。图46B示出替代性具体实施，其中独立应用程序4654利用由安全交易服务4601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4654被设计为建立与一个或多个网络服务4651的通信会话，这些网络服务依赖于安全交易服务器4632至4633来执行下文详细描述的用户/客户端验证技术。

[0540] 在图46A至46B所示的任一个实施例中，安全交易服务器4632至4633可生成密钥，这些密钥接着被安全地传输到安全交易服务4601并存储到安全存储装置4620内的验证装置中。另外，安全交易服务器4632至4633管理服务器端上的安全交易数据库4640。

[0541] 图47至51中示出用于执行验证装置发现、登记、注册和验证的一系列示例性事务。上文所述的OSTP协议中已经采用了这些事务的一些方面(参见OSTP框架(2011年3月23日)了解其他细节，所述OSTP框架以引用的方式并入本文中)。对这些事务的基本操作的理解将提供可实施本发明的实施例的环境。

[0542] 下文所述的操作包括检测验证装置(图47)；向验证装置登记用户(图48)；注册验证装置(图49)；向注册的验证装置验证用户(图50)；以及在验证之后实施安全交易(图51)。

[0543] 图47示出用于在客户端机器上检测验证装置的一系列事务。在成功完成装置检测之后，服务器4730拥有关于附接到客户端的验证装置的详尽信息并且将能够评估哪个(哪些)装置最适合与增强型安全基础设施一起使用。只有服务器4730筛选验证装置列表。将向用户提供此列表，并且用户可选择一个(或一组)验证装置来用于进一步验证和实施安全交易。

[0544] 在操作中，用户在浏览器中使用用户名和密码来验证并登录网站。只有在这时需要用户提供用户名和密码。服务器4730确定用户当前没有使用增强型安全性(例如，通过查询安全交易数据库4720)并向用户建议更改为增强型安全性。

[0545] 在一个实施例中，服务器4730在安全交易插件4705检测到的HTML页面中包括“查询装置”标签。响应于检测到此标签，安全交易插件4705将请求重新路由到安全交易服务4701，安全交易服务4701接着准备关于附接到系统的所有验证装置的详尽信息，该信息包括装置的安全特征。在一个实施例中，在传输之前使用预先指定的数据模式以XML格式封装该信息。

[0546] 安全交易插件4705从安全交易服务4701接收该信息，并且在一个实施例中，经由注册的回叫将该信息传递到网页的JavaScript。其接着选择如何在浏览器4704中显示该信息。可向用户展示由网站筛选的列表，并且用户可选择一个或一组验证装置。

[0547] 图48示出用于向验证装置登记用户的一系列事务。在一个实施例中，登记是使用由本文所述的本发明的实施例所提供的增强型安全性的先决条件。登记涉及取得用户的生物计量读数(例如，指纹、声音样本等)，使得同一验证装置可用于在后续交易期间验证用户。可在不与服务器4730交互的情况下单独地在客户端上进行登记操作。被提供用于登记的用户界面可在浏览器扩展件中显示，或者可在单独的应用程序或移动装置应用程序中显示。

[0548] 一检测到装置，就可发起登记操作。用户可选择使用一个或一组已发现的装置来实现增强型安全性。在操作中，用户可在浏览器、应用程序或移动装置应用程序中从所显示的装置列表中选择一个装置。对于图48所示的基于浏览器的具体实施，安全交易插件4705显示装置特定的登记图形用户界面(GUI)。安全交易插件4705将装置识别符和登记请求传输到安全交易服务4701并等待完成。如果已经向客户端上的验证装置登记了用户，则用户可仅需要验证其身份(即，将不需要用户再次登记)。如果用户当前尚未登记，则安全交易服务101通过激活物理验证装置(例如，经由装置接口4702)来开始登记过程。用户接着与安全交易插件4705GUI交互并遵循指定的登记步骤(例如，轻扫手指、对着麦克风说话、拍摄照片等)。一旦完成，便将向验证装置登记了用户。值得注意的是，一旦向装置登记了用户，其便可使用此登记来向任何网站或网络服务进行注册或验证，如本文所述。

[0549] 图49示出用于注册验证装置的一系列事务。在注册期间，在验证装置与安全交易服务器4732至4733中的一个之间共享密钥。密钥存储在客户端4700的安全存储装置4720和由安全交易服务器4732至4733使用的安全交易数据库4720内。在一个实施例中，密钥是由安全交易服务器4732至4733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4732至4733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4720中。此外，在一个实施例(也在下文中论述)中，密钥可在客户端4700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4732至4733生成)。

[0550] 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，见请求注解(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。

[0551] 转到图49所示的具体细节，一旦用户登记或用户验证完成，服务器4730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4701。作为响应，安全交易服务发起与服务器4730的带外会话(例如，带外事务)，并使用密钥供应协议与服务器4730通信。服务器4730使用用户名定位用户，验证随机质询，在已经发送装置的验证代码的情况下验证该验证代码，并且在安全交易数据库4720中为用户创建新条目。其还可生成密钥，将密钥写入到数据库4720，并使用密钥预置协议将密钥发送回到安全交易服务4701。一旦完成，验证装置与服务器4730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。

[0552] 图50示出用于向注册的验证装置验证用户的一系列事务。一旦装置注册完成，服务器4730便将接受由本地验证装置生成的令牌作为有效验证令牌。

[0553] 转到图50所示的具体细节，该图示出基于浏览器的具体实施，用户在浏览器4704中输入服务器4730的统一资源定位符(URL)。在使用独立应用程序或移动装置应用程序(而非浏览器)的具体实施中，用户可输入网络服务的网络地址，或者应用程序或移动装置应用程序可自动尝试连接到该网络地址的网络服务。

[0554] 对于基于浏览器的具体实施，网站在HTML页面中嵌入对已注册装置的查询。这可以在HTML页面中嵌入查询之外的许多方式进行，诸如通过Javascript或使用HTTP标头。安全交易插件4705接收URL并将其发送到安全交易服务4701，安全交易服务4701搜索安全存储装置4720(如所论述，其包括验证装置和用户信息的数据库)并确定是否有用户在该URL内登记。如果是，则安全交易服务4701将与该URL相关联的已预置装置列表发送到安全交易插件4705。安全交易插件接着调用已注册的JavaScript API并将此信息传递到服务器4730(例如，网站)。服务器4730从所发送的装置列表选择恰当的装置，生成随机质询，并将装置信息和参数发送回到客户端。网站显示对应的用户界面并要求用户进行验证。用户接着提供所要求的验证措施(例如，在指纹读取器上轻扫手指、说话以进行声音识别等)。安全交易服务4701识别用户(对于不支持存储用户的装置，可跳过此步骤)，从数据库获得用户名，使用密钥生成验证令牌，并且经由安全交易插件将该信息发送到网站。服务器4730从安全交易数据库4720识别用户，并且通过在服务器4730上生成相同令牌(例如，使用其密钥复本)来验证令牌。一旦验证，验证过程便完成。

[0555] 图51示出用于基于浏览器的具体实施的在验证之后的安全交易。此安全交易被设计为为某些类型的交易(例如，金融交易)提供更强安全性。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/她想要进行什么交易并且进行他/她所看见的在GUI中显示的确切内容。换句话讲，该实施例确保“中间人”无法修改交易文本来进行用户没有确认的交易。

[0556] 在一个实施例中，安全交易插件4705在浏览器环境中显示窗口5101以展示交易细节。安全交易服务器4701周期性地(例如，以随机时间间隔)验证窗口中所示的文本没有正被任何人篡改。

[0557] 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4732至4733。商家网站验证用户并完成交易。

[0558] 安全交易服务器4732至4733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4700。安全交易请求包括交易细节和随机质询(例如，随机数)。安全交易插件4705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4701。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4700上的安全交易服务。

[0559] 对于基于浏览器的具体实施，安全交易插件4705向用户显示具有交易细节的窗口5101(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4701或应用程序4754可显示窗口5101。安全交易服务4701启动计时器并

验证正向用户显示的窗口5101的内容。可随机选择验证周期。安全交易服务4701确保用户在窗口5101中看见有效交易细节。如果它检测到内容已被篡改，则其阻止生成确认令牌。

[0560] 在用户提供有效验证(例如，在指纹传感器上轻扫手指)之后，装置识别用户，并使用交易细节和随机质询生成令牌(密码签名)(即，根据交易细节和随机数计算得到令牌)。这允许安全交易服务器4732至4733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4701将所生成的令牌和用户名发送到安全交易插件4705，安全交易插件4705将令牌转发到安全交易服务器4732至4733。安全交易服务器4732至4733使用用户名识别用户并验证令牌。如果验证成功，则向客户端发送确认消息并处理交易。

[0561] 用于确定客户端验证功能的安全查询策略的系统和方法

[0562] 如所提及，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识别其支持以及/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。

[0563] 以举例而非限制的方式，客户端可包括许多验证功能，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、可信平台模块(TPM)和智能卡等等。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。

[0564] 图52示出用于实施这些技术的客户端-服务器架构的一个实施例。如图所示，在客户端4700上实施的安全交易服务4701包括策略筛选器5201，其用于分析服务器4730所提供的策略并识别要用于注册和/或验证的验证功能子组。在一个实施例中，策略筛选器5201被实施为在安全交易服务4701的环境内执行的软件模块。然而，应该指出的是，策略筛选器5201可在同时仍符合本发明的基本原理的情况下以任何方式来实施，并且可包括软件、硬件、固件或其任何组合。

[0565] 图52中所示的特定具体实施包括安全交易插件4705，其用于使用先前论述的技术建立与安全企业或Web目的地4730(有时简称为“服务器4730”)的通信。例如，安全交易插件可识别由web服务器4731插入到HTML代码中的特定HTML标签。因此，在这个实施例中，将服务器策略提供到安全交易插件4705，安全交易插件4705将其转发到实施策略筛选器5201的安全交易服务4701。

[0566] 策略筛选器5201可通过从客户端的安全存储区域5220读取功能来确定客户端验证功能。如先前论述，安全存储装置5220可包括所有客户端验证功能(例如，所有验证装置的识别代码)组成的存储库。如果用户已经向其验证装置登记了用户，则用户的登记数据被存储在安全存储装置5220内。如果客户端已经向服务器4730注册了验证装置，则安全存储装置还可存储与每个验证装置相关联的加密秘密密钥。

[0567] 通过使用从安全存储装置5220提取的验证数据和由服务器提供的策略，策略筛选器5201可接着识别要使用的验证功能子组。根据配置，策略筛选器5201可识别客户端和服

务器两者所支持的验证功能的完整列表，或可识别完整列表的子组。例如，如果服务器支持验证功能A、B、C、D和E，并且客户端具有验证功能A、B、C、F和G，则策略筛选器5201可向服务器识别共同验证功能的整个子组：A、B和C。或者，如果需要较高隐私等级，如在图52中由用户偏好5230指示，则可向服务器识别更有限的验证功能子组。例如，用户可指示应仅向服务器识别单个共同验证功能(例如，A、B或C之一)。在一个实施例中，用户可针对客户端4700的所有验证功能确立优先化方案，并且策略筛选器可选择服务器和客户端两者共有的最高优先级的验证功能(或N个验证功能的优先化组)。

[0568] 根据服务器4730发起了何种操作(注册还是验证)，安全交易服务4730对筛选的验证装置子组(4710至4712)执行该操作，并经由安全交易插件4705将操作响应发送回到服务器4730，如图52所示。或者，在不依赖于Web浏览器的插件4705组件的实施例中，可将该信息直接从安全交易服务4701传递到服务器4730。

[0569] 图53示出了事务图，其展示使用查询策略事务的一系列示例性注册的额外细节。在图示实施例中，用户先前没有向服务器4730注册装置。因此，在5301处，用户可输入用户名和密码作为初始的一次性验证步骤，在5302处，用户名和密码经由客户端浏览器4704转发到服务器4730。然而，应该指出的是，为了符合本发明的基本原理，不一定需要用户名和密码。

[0570] 因为在5303处确定用户先前未以增强型安全性注册，所以在5304处，服务器4730将其服务器策略传输到客户端。如所提及，服务器策略可包括对服务器4730所支持的验证功能的指示。在图示例子中，经由事务5306将服务器策略传递到安全交易服务4701。

[0571] 在事务5307处，安全交易服务4701将服务器策略与客户端的功能(以及有可能其他信息，诸如装置优先级方案和/或用户偏好，如上所述)进行比较，以得到验证功能的筛选列表。装置的筛选列表(4702)接着生成密钥(5308和5309)，并且接着将这些密钥的公共部分提供到安全交易服务4701，安全交易服务4701又将这些作为注册响应发送回到服务器4730。服务器证实验证装置并将公共密钥存储在安全交易数据库中。此处所采用的令牌证实是在注册期间确认验证装置身份的过程。其允许服务器以密码确保客户端所报告的装置实际上是其声称的那个装置。

[0572] 作为另外一种选择或除此之外，在5307处，可向用户提供审查列表和/或选择要与该特定服务器4730一起使用的特定验证功能的机会。例如，筛选列表可指示使用借助指纹扫描、面部识别和/或声音识别进行的验证的选项。用户可接着选择在向服务器4730验证时使用这些选项中的一个或多个。

[0573] 上文针对在客户端处筛选服务器策略所描述的技术可在上文所述的一系列事务的各种不同阶段(例如，在装置发现、装置注册、装置预置、用户验证等期间)实施。也就是说，本发明的基本原理不限于图53所陈述的该组特定事务和特定事务次序。

[0574] 此外，如先前提及，为了符合本发明的基本原理，不一定需要浏览器插件架构。对于不涉及浏览器或浏览器插件的架构(例如，诸如独立应用程序或移动装置应用程序)，图53所示的事务图(以及本文所公开的事务图的其余部分)可简化，使得浏览器4704被移除，并且安全交易服务4701直接与服务器4730通信。

[0575] 用于有效地向多个验证装置登记、注册和验证的系统和方法

[0576] 本发明的一个实施例能够同时登记、注册和验证多个装置，从而提升效率和用户

体验。例如，不同于一次针对单个装置请求注册和验证，可将装置的列表发送到客户端。可接着在客户端上本地执行的一个操作或一系列顺序操作中将对称或不对称密钥注册到多个装置中。为了验证，可为给定交易同时选择若干个令牌/装置。

[0577] 图54示出用于实施这些技术的客户端-服务器架构的一个实施例。如图所示，在客户端4700上实施的安全交易服务4701包括多装置处理逻辑5401，该逻辑用于执行指定操作，诸如一次登记和注册多个装置而不需要在登记/注册每个装置时与服务器4730进行持续的来回通信。相似地，服务器4730包括多装置处理逻辑，该逻辑用于发布指向多个验证装置的命令。在一个实施例中，多装置处理逻辑5401被实施为在安全交易服务4701的环境内执行的软件模块。然而，应该指出的是，多装置处理逻辑5401可在同时仍符合本发明的基本原理的情况下以任何方式来实施，并且可包括软件、硬件或固件组件或者其任何组合。

[0578] 如在上文所述的实施例中，图54所示的特定具体实施包括安全交易插件4705，其用于建立与服务器4730(如所论述，其可包括网站服务器4731和安全交易服务器4732至4733)的通信。因此，服务器4730经由安全交易插件4705与安全交易服务4701通信。然而，如所提及，为了符合本发明的基本原理，不一定需要基于浏览器的插件架构。

[0579] 服务器4730上的多装置处理逻辑5402可传送待由客户端4700上的多装置处理逻辑5401执行的命令，该多装置处理逻辑5401对多个验证装置4710至4712执行操作。举例来说，多装置处理逻辑5402可生成要向N个验证装置中的每一个注册的N个密钥，并且接着将其连同注册N个装置的命令安全地传输到多装置处理逻辑5401。多装置处理逻辑5401可接着针对所有N个装置(例如，针对验证装置4710至4712)同时或在一系列顺序操作中执行注册而不与服务器进行进一步交互。可接着将单个响应发送到服务器4730以指示所有N个装置的注册完成。

[0580] 图55A至55C中示出一系列示例性多装置事务。图55A示出多装置登记过程，其可在不与服务器4730进行任何交互的情况下执行(例如，可在客户端上的安全交易服务4701的控制下执行向验证装置登记用户)。在替代实施例中，服务器4730可向客户端(未示出)传输请求以向N个装置登记用户。图55B至55C示出用于向服务器4730注册多个装置的两个不同实施例。

[0581] 转到图55A中的登记过程，在5501处，用户表明想要向客户端上的N个验证装置(代表可用验证装置的全部或子组)登记。作为响应，在5502处，调用安全交易插件，并且在5503处，生成装置特定的图形用户界面(GUI)以使用户遍历该过程或向验证装置#1登记。在登记过程中，用户根据指示与安全交易插件交互(例如，通过将手指放置在指纹传感器上方、对着麦克风说话、用摄像头拍摄照片等等)。在一个实施例中，针对N个装置中的每一个执行登记，直到在5504处针对第N个装置的登记完成为止。可向用户呈现不同的装置特定脚本和/或用户界面以向每个单独验证装置登记用户。如先前所论述，在用户向每个装置登记时，可将用户登记数据存储在客户端4700上的安全存储装置720内并使其仅能够通过安全交易服务4701来访问。一旦针对所有N个装置的登记都完成，便可经由事务5504至5505向服务器4730发送通知。

[0582] 不管如何执行登记，一旦完成，便可使用图55B中所示的事务图来向服务器4730注册N个装置。在5510处，服务器4730生成用户特定的随机质询，如先前所述，该随机质询可仅在有限时间窗内有效并且可包括随机生成代码，诸如密码随机数。在5511处，将随机质询连

同向服务器4730注册N个验证装置的命令一起传输。在5512处，安全交易服务4701创建与服务器4730的安全连接，并将用于N个装置的识别数据连同随机质询一起传输。在一个实施例中，安全连接为HTTPS连接。然而，本发明的基本原理不限于任何特定安全连接类型。

[0583] 在5513处，服务器4730证实N个装置，为N个装置中的每一个生成密钥，并且将这N个密钥经由安全连接发送回到安全交易服务。在一个实施例中，使用动态对称密钥预置协议(DSKPP)来经由安全连接与客户端交换密钥。然而，本发明的基本原理不限于任何特定密钥预置技术。或者，在不依赖于DSKPP协议的实施例中，可在每个验证装置中生成密钥并接着将其传输到服务器4730。

[0584] 在5514至5515处，安全交易服务的多装置处理逻辑将N个密钥中的每一个注册到N个装置中的每一个中。如先前所述，每个密钥可被存储在客户端上的安全存储装置720内并与所述安全存储装置内的相应装置相关联。一旦针对每个验证装置完成注册，便在5516处经由安全连接将通知发送到服务器。

[0585] 在一个实施例中，注册到每个验证装置中的密钥是对称密钥。因此，每个密钥的相同复本被存储在客户端上的安全存储装置720和服务器4730上的安全交易数据库4720中。在替代具体实施中，可生成不对称密钥对，其中一个密钥作为公共密钥维持在服务器上的安全交易数据库4720中，并且私有密钥存储在客户端的安全存储装置720中。然而，应该指出的是，本发明的基本原理不限于任何特定类型的加密密钥。

[0586] 图55C中示出替代具体实施，其中在客户端而不是服务器4730上生成密钥。在该具体实施中，在5511处将对注册装置的请求连同随机质询一起接收之后，在1120处，安全交易服务4701的多装置处理逻辑针对N个装置中的每一个生成N个密钥。一旦生成，便在5513至5514处向N个装置中的每一个注册密钥并将注册内容存储在安全存储装置720内，如先前所述。一旦所有密钥都已注册，安全交易服务4701便在5515处将通知连同随机质询(用于验证客户端的身份)一起提供给服务器。服务器4730可接着将注册内容存储在安全交易数据库4720中，如上所述。

[0587] 用于在验证框架内处理随机质询的系统和方法

[0588] 本发明的一个实施例改进了由服务器生成和处理随机质询的方式。在一个实施例中，随机质询包括随机生成的代码，诸如密码随机数。在当前系统中，在服务器将随机质询传输到客户端之后，如果客户端未在指定超时时段内做出响应，则随机质询不再有效，并且客户端将响应于后续验证尝试接收到错误(例如，用户将在指纹读取器上轻扫手指并被拒绝)。

[0589] 在本发明的一个实施例中，客户端自动地检测质询是否已经过期并且透明地向服务器请求新质询(即，在没有用户干预的情况下)。服务器接着生成新的随机质询并将其传输到客户端，客户端可接着用其建立与服务器的安全通信。最终用户体验得以改善，因为用户不会接收到验证请求的错误或拒绝。

[0590] 图56A示出在注册过程的环境内使用的一个此类实施例，并且图56B示出在验证过程的环境内使用的实施例。然而，应该指出的是，可在除了图56A至56B所示的那些之外的其他环境中采用本发明的基本原理。例如，本文所述的技术可与从服务器向客户端传送时间敏感代码的任何过程一起使用。

[0591] 首先转到图56A，在5601处，服务器4730生成随机质询和对超时时段的指示。在一

个实施例中，超时时段包括随机质询被视为有效所在的时间段。在超时时段已经过去之后，随机质询不再被服务器4730视为有效。在一个实施例中，超时时段被简单地指定为随机质询将不再有效时的时间点。一旦达到这个时间点，随机质询便无效。在另一个实施例中，通过使用当前时戳(即，服务器4730生成随机质询的时间)和持续时间来指定超时时段。安全交易服务4701可接着通过将持续时间值相加到时戳来计算随机质询变无效时的时间点，从而计算出超时时间。然而，应该指出的是，本发明的基本原理不限于用于计算超时时段的任何特定技术。

[0592] 不管如何指定或计算超时时段，在5602处，都会将随机质询和超时指示传输到安全交易服务4701(在图示例子中经由浏览器4704和安全交易插件4705)。在5603处，安全交易服务4701基于从服务器4730发送的超时指示检测随机质询是否已经超时并且不再有效。举例来说，用户可能在完成一系列事务之前已经关闭了他/她的客户端机器或合上他/她的笔记本计算机的盖子。如果交易需要用户交互，则用户可能只是已经走开或忽略GUI内显示的消息。

[0593] 在5604处，在检测到随机质询不再有效后，安全交易服务4701将对新的随机质询的请求传输到服务器4730(在图示例子中经由安全交易插件4705和浏览器4704)。在5605处，服务器4730生成新的随机质询和对超时时段的新指示。在一个实施例中，该超时时段与在操作5601中的相同或可被修改。例如，服务器4730可增加超时时段的持续时间以减少与客户端的数据流量，或减少持续时间以提高随机质询所提供的安全等级。在5606处，将新的随机质询和超时指示传输到安全交易服务4701。

[0594] 事务的剩余部分如先前所述那样发生。例如，安全交易服务在5607处开启直接通向服务器的安全连接，以便执行装置注册和密钥交换，如上文结合图49、图55B或图55C所论述。在5608处，服务器4730识别用户(例如，使用用户名或其他ID)，证实验证装置，并为装置生成密钥。如所提及，该密钥可为对称密钥或不对称密钥。在5609处，经由安全连接将密钥传输到安全交易服务4701，并且在5610处，安全交易服务4701将密钥注册到验证装置中。在5611处，将指示注册已完成的通知传输到服务器4730。

[0595] 因此，在图56A所示的实施例中，在服务器4730处生成用于装置注册的密钥，如同在图55B所示的实施例中一样。然而，本发明的基本原理还可在由客户端4700上的安全交易服务4701生成密钥的实施例(诸如上文结合图55C所述的实施例)中使用。

[0596] 图56B示出在验证过程的环境内实施的本发明的一个实施例。在5651处，用户将特定网站URL输入到浏览器4704中并被引导到企业/web目的地服务器4730内的web服务器4731，服务器4730包括安全交易服务器4732至4733。在5652处，将查询发送回到安全交易服务(经由浏览器和插件)以确定向该网站的URL注册哪个(哪些)装置。在5653处，安全交易服务4701查询客户端4700上的安全存储装置720以识别发送回到服务器4730的装置的列表。在5654处，服务器5654选择装置以用于验证，生成随机质询和超时指示，并且在5655处，将该信息发送回到安全交易服务4701。

[0597] 在5656处，安全交易服务5656自动检测在达到超时时段的末尾时随机质询不再有效。如上所述，可采用各种不同的技术来指示和检测超时时段的结束(参见图56A和相关联文本)。在检测到随机质询过期后，在5657处，安全交易服务4701透明地(即，在没有用户干预的情况下)通知服务器4730并请求新的随机质询。作为响应，在5658处，服务器4730生成

新的随机质询和对超时时段的新指示。如所提及，新的超时时段可与先前发送到客户端的超时时段相同或可被修改。在任一种情况下，在5659处，将新的随机质询和超时指示发送到安全交易服务4701。

[0598] 图56B所示的事务图的剩余部分以与如上所述基本相同的方式进行操作(例如，参见图50)。例如，在5660处，显示验证用户界面(例如，引导用户在指纹传感器上轻扫手指)，并且在5661处，用户提供验证(例如，在指纹扫描器上轻扫手指)。在5662处，安全交易服务验证用户的身份(例如，将从用户收集的验证数据与存储在安全存储装置720中的数据进行比较)并使用与验证装置相关联的密钥来加密随机质询。在5663处，将用户名(或其他ID代码)和加密随机质询发送到服务器4730。最后，在5664处，服务器4730使用用户名(或其他ID代码)在安全交易数据库4720内识别用户，并且使用存储在安全交易数据库4720中的密钥解密/验证随机质询以完成验证过程。

[0599] 用于在验证框架内实施隐私类别的系统和方法

[0600] 在一个实施例中，最终用户可预先定义、选择以及/或者修改多个隐私保护类别。可基于能够使用透露的信息识别出客户端的概率来定义隐私类别。在具有相对较高隐私等级的隐私类别，透露关于客户端装置的相对较少信息来执行本文所述的验证技术。在一个实施例中，用户可选择公开在与不同服务器通信时可能的最少量的信息(即，可选择对每个网站或网络服务具有允许的最低隐私影响的交易)。

[0601] 图57示出用于实施隐私类别的高级架构。如图所示，该实施例的安全交易服务4701包括隐私管理逻辑5701，其用于分析从服务器4730接收的对客户端信息(诸如与验证装置有关的信息)的查询，响应于此类查询实施隐私策略，并且生成响应，该响应包含基于使用中的特定隐私类别来收集的客户端信息。在一个实施例中，隐私管理模块5701被实施为在安全交易服务4701的环境内执行的软件模块。然而，应该指出的是，隐私管理模块5701可在同时仍符合本发明的基本原理的情况下以任何方式来实施，并且可包括软件、硬件、固件或其任何组合。

[0602] 隐私管理逻辑5701所利用的隐私类别可被预先指定并存储在客户端4700上(例如，存储在安全存储装置5720内)。在一个实施例中，定义了三个隐私类别：高隐私影响、中隐私影响和低隐私影响。可基于透露的信息能够用于唯一地识别用户/客户端的概率来定义每个隐私类别。例如，针对低隐私影响交易透露的信息可导致经由因特网唯一地识别用户或机器的概率为10％；中隐私影响交易可导致唯一地识别用户或机器的概率为50％；并且高隐私影响交易可导致唯一地识别用户或机器的概率为100％。可在同时仍符合本发明的基本原理的情况下定义各种其他隐私类别等级。

[0603] 在一个实施例中，每个依赖方(例如，每个网站4731或服务4751)可指定所需要的隐私类别或其他隐私阈值。例如，需要高度安全等级的网站和服务可仅允许根据高隐私影响类别的通信，而其他网站/服务可准许使用中隐私影响类别或低隐私影响类别的交互。在一个实施例中，从服务器4730发送的对客户端信息的查询包括指定应检索哪个隐私类别的信息(即，低、中、高)的属性。因此，隐私管理逻辑5701将针对每个依赖方存储最高批准隐私类别的信息。在一个实施例中，每当依赖方要求属于比已批准的隐私类别高的隐私类别的信息时，将提示用户针对该依赖方永久性地批准(或拒绝)此新的隐私类别。响应于用户批准，隐私管理逻辑可存储依赖方(例如，经由URL所识别)与新隐私类别之间的新关联性。

[0604] 尽管在图57中为简单起见将用户偏好5730直接应用于隐私管理逻辑，但应该指出的是，用户可经由基于浏览器的图形用户界面(未示出)来指定偏好。在这种情况下，用户将经由浏览器窗口输入隐私设置。安全交易插件4705将接着将新设置存储到隐私管理逻辑5701，或存储到隐私管理逻辑5701能够访问的配置数据文件。简而言之，本发明的基本原理不限于用于配置隐私管理逻辑的任何特定机制。

[0605] 可在各种隐私类别等级指定各种类型的客户端数据，包括(例如)机器型号识别符、客户端软件信息、客户端功能，以及与在客户端装置上配置的每个验证装置有关的各种等级的信息(例如，装置ID代码、供应商ID代码、装置类别ID等)。可收集这些信息的不同组合以确定上文指定的定义不同隐私类别的百分比。

[0606] 图58示出用于使用已定义的隐私类别向请求方提供信息的一系列事务。在5801处，服务器4730生成包含对客户端装置信息的查询的通知。在5802处，将查询发送到客户端并且最终由安全交易服务4701接收。在5803处，安全交易服务的隐私管理逻辑确定响应的隐私类别并且收集必要信息。如上文所述，可定义N个不同的隐私类别等级，并且安全交易服务4701可选择符合请求方的要求且同时透露尽可能少的关于客户端的信息的隐私类别等级。在5804处，将所收集的信息发送到服务器4730，并且在5805处，服务器将该信息用于与客户端的一个或多个后续交易。

[0607] 用于使用交易签署实施验证框架的系统和方法

[0608] 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。

[0609] 图59中示出本发明的一个实施例，其示出网站或其他网络服务(5901)发起与客户端4700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5901将交易切换到安全交易服务器5902，安全交易服务器5902包括用于生成和验证签名(如本文所述)的签名处理逻辑5903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5904。

[0610] 在一个实施例中，从安全交易服务器5902发送到客户端4700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5903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。

[0611] 一旦客户端接收到以上信息，用户便可接收有关需要验证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，一旦用户已经在客户端4700上成功验证，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。

[0612] 安全交易服务器5902上的验证模块5904可接着确认用户已经正确地验证，并且签名处理逻辑5903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5901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5902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4720内。

[0613] 示例性数据处理装置

[0614] 图60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60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。

[0615] 如图60所示，计算机系统6000，其为一种形式的数据处理系统，包括总线6050，该总线与处理系统6020、电源6025、存储器6030和非易失性存储器6040(例如，硬盘驱动器、快闪存储器、相变存储器(PCM)等)耦接。总线6050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6020可从存储器6030和/或非易失性存储器6040检索指令，并执行这些指令以执行如上所述的操作。总线6050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6060、显示控制器与显示装置6070、输入/输出装置6080(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6090(例如，蓝牙、WiFi、红外等)。

[0616] 图61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6100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6100可为网络计算机或在另一个装置内的嵌入式处理装置。

[0617] 根据本发明的一个实施例，数据处理系统6100的示例性架构可用于上文所述的移动装置。数据处理系统6100包括处理系统6120，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6120与存储器6110、电源6125(其包括一个或多个电池)、音频输入/输出6140、显示控制器与显示装置6160、可选输入/输出6150、输入装置6170和无线收发器6130耦接。应当理解，在本发明的某些实施例中，图61中未示出的其他组件也可为数据处理系统6100的一部分，并且在本发明的某些实施例中，可使用比图61所示更少的组件。另外，应当理解，图61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。

[0618] 存储器6110可存储数据和/或程序以供数据处理系统6100执行。音频输入/输出6140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6160可包括图形用户界面(GUI)。无线(例如，RF)收发器6130(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6170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6150可为底座的连接器。

[0619] 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部件执行，或由编程的计算机部件和定制硬件部件的任何组合执行。

[0620] 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。

[0621] 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。

[0622] 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。

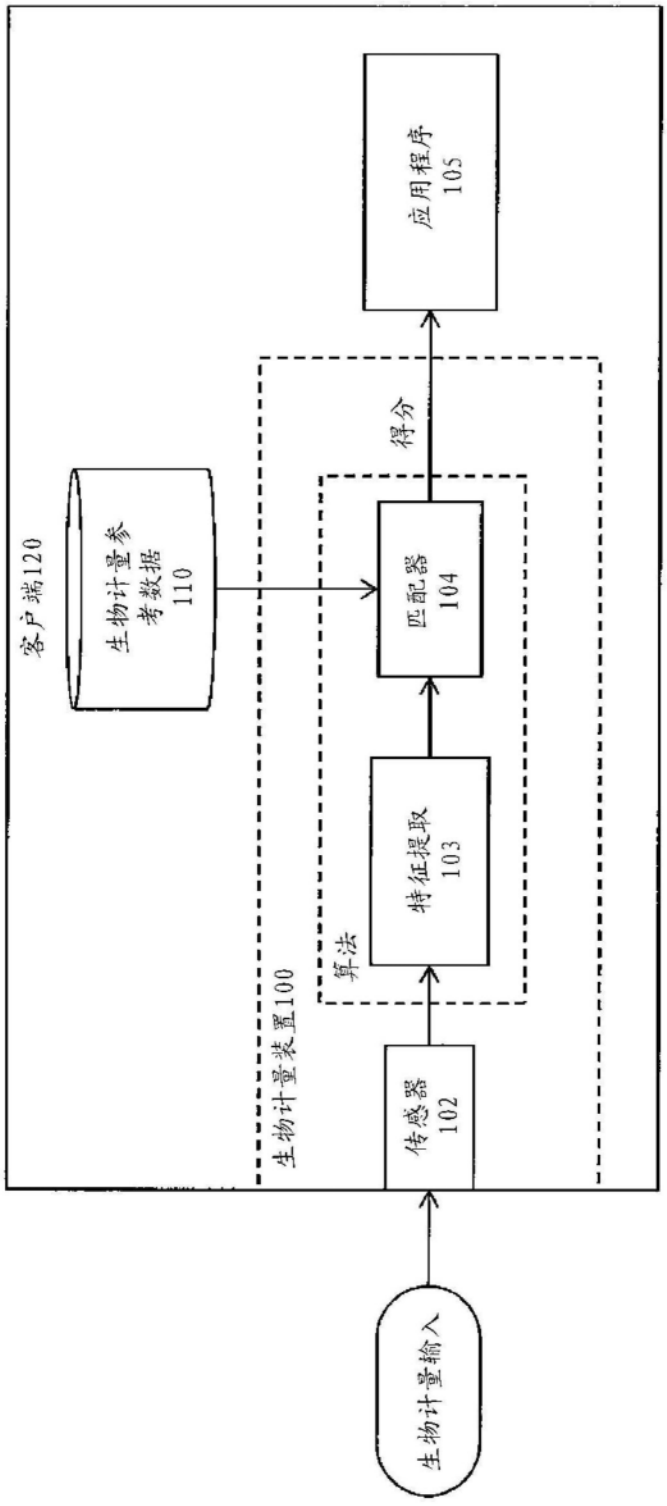

应用程序
105
得分
客户端120
生物计量参
考数据
110
匹配器
104
生物计量装置100
算法
特征提取
103
传感器
102
生物计量输入

图1

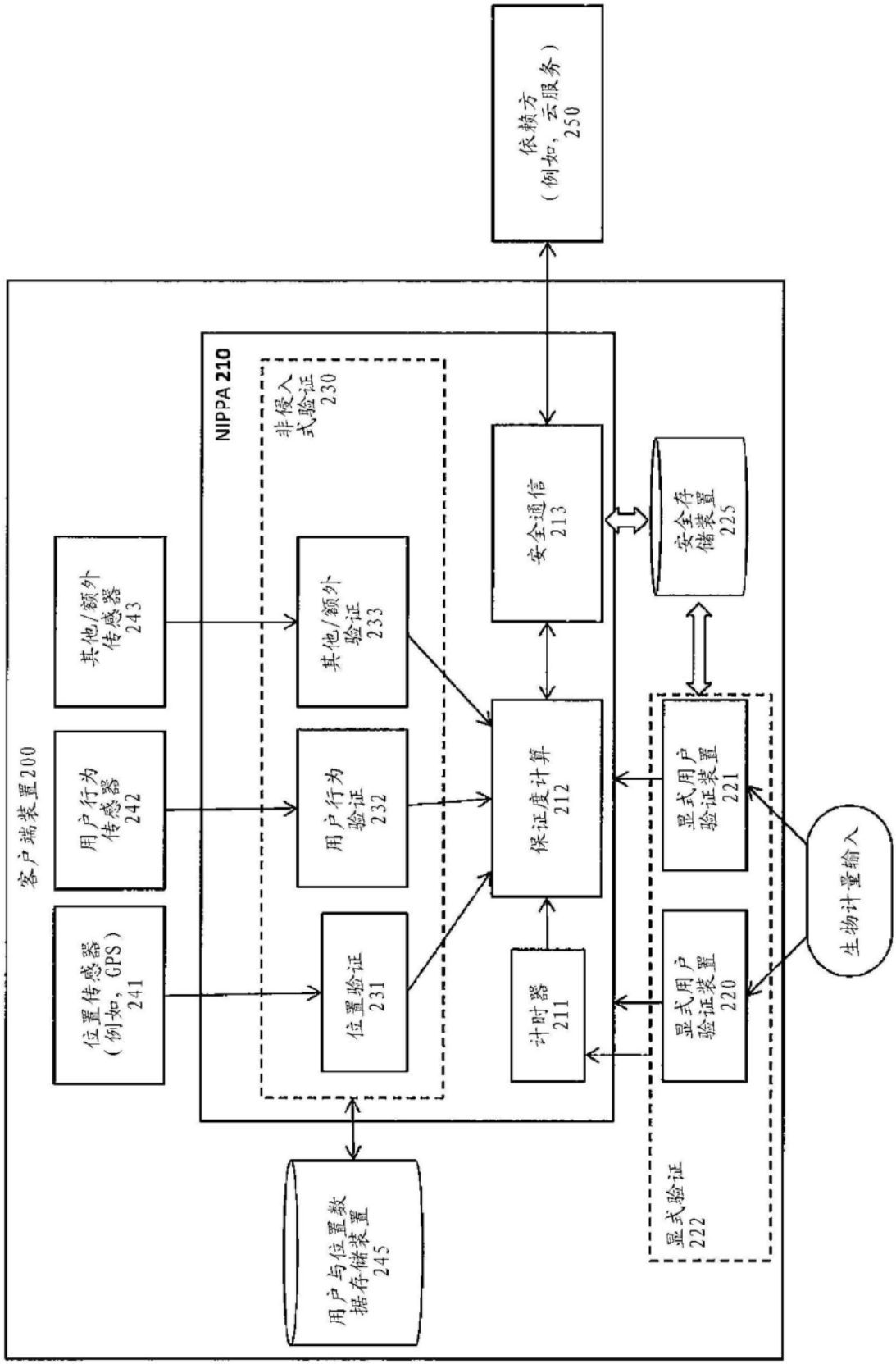

依赖方
（例如，云服务）
250
客户端装置200
NIPPA 210
非侵入式验证
230
其他/额外传感器
243
用户行为传感器
242
位置传感器
（例如，GPS）
241
其他/额外验证
233
用户行为验证
232
位置验证
231
安全通信
213
安全存储装置
225
保证度计算
212
计时器
211
显式用户验证装置
221
显式用户验证装置
220
显式验证
222
生物计量输入
用户与位置数据存储装置
245

图2

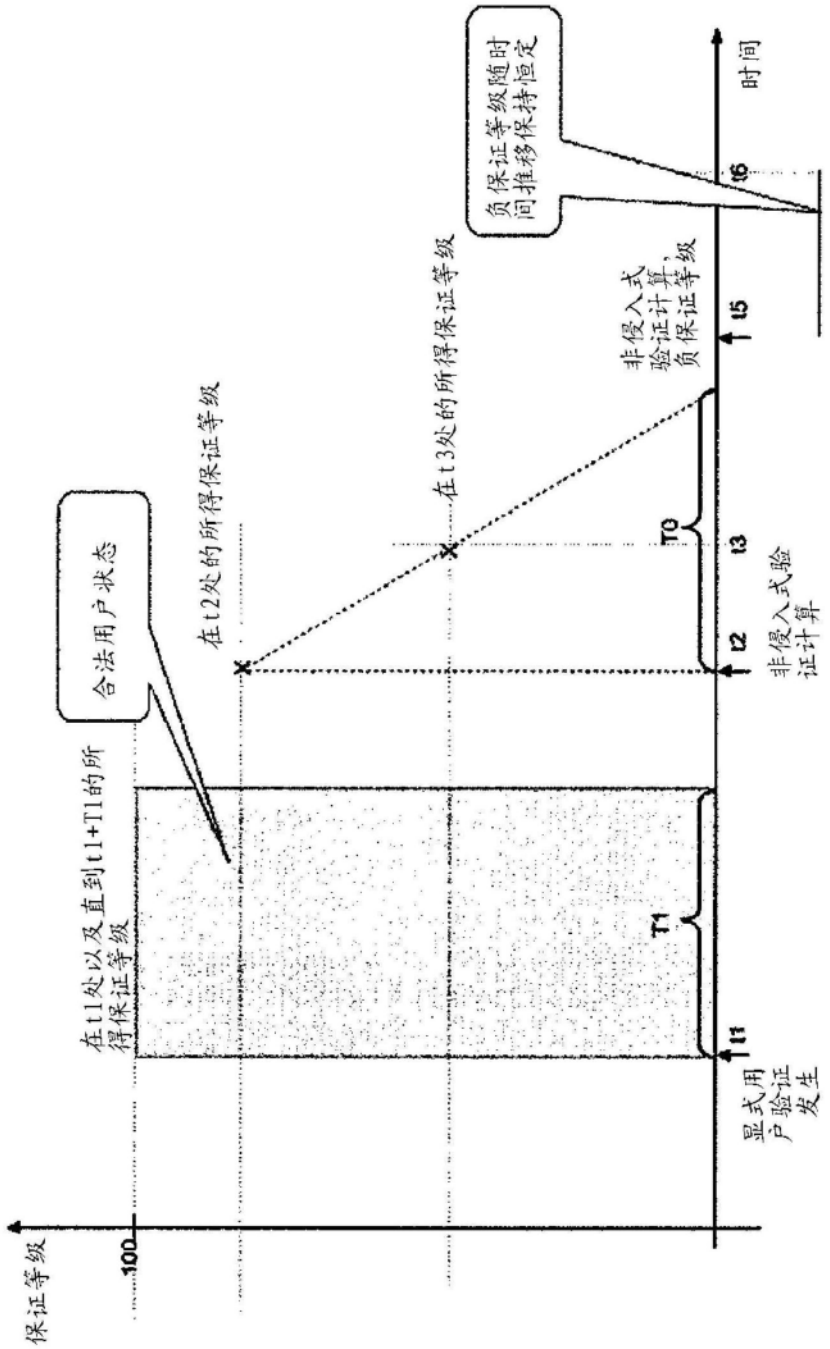

保证等级
100
显式用户验证发生
t1
非侵入式验证计算
t2
非侵入式验证计算，负保证等级
t3
负保证等级随时间推移保持恒定
t5
t6
时间
T0
T1
在t1处以及直到t1+T1的所得保证等级
合法用户状态
在t2处的所得保证等级
在t3处的所得保证等级

图3

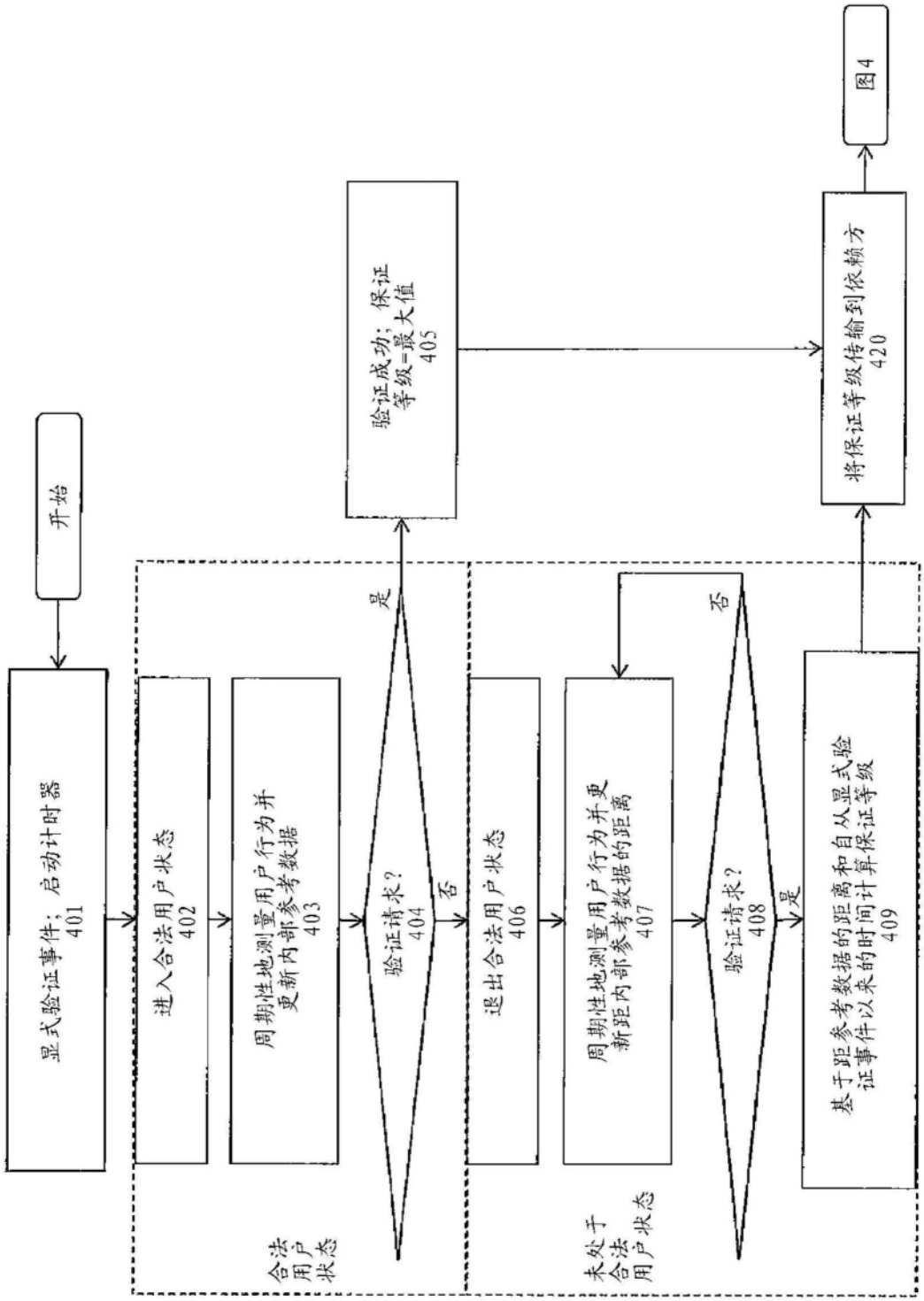

开始
显式验证事件；启动计时器
401
进入合法用户状态
402
周期性地测量用户行为并更新内部参考数据
403
验证请求?
404
是
否
验证成功；保证等级=最大值
405
退出合法用户状态
406
周期性地测量用户行为并更新距内部参考数据的距离
407
验证请求?
408
否
是
基于距参考数据的距离和自从显式验证事件以来的时间计算保证等级
409
将保证等级传输到依赖方
420
图4
合法用户状态
未处于合法用户状态

图4

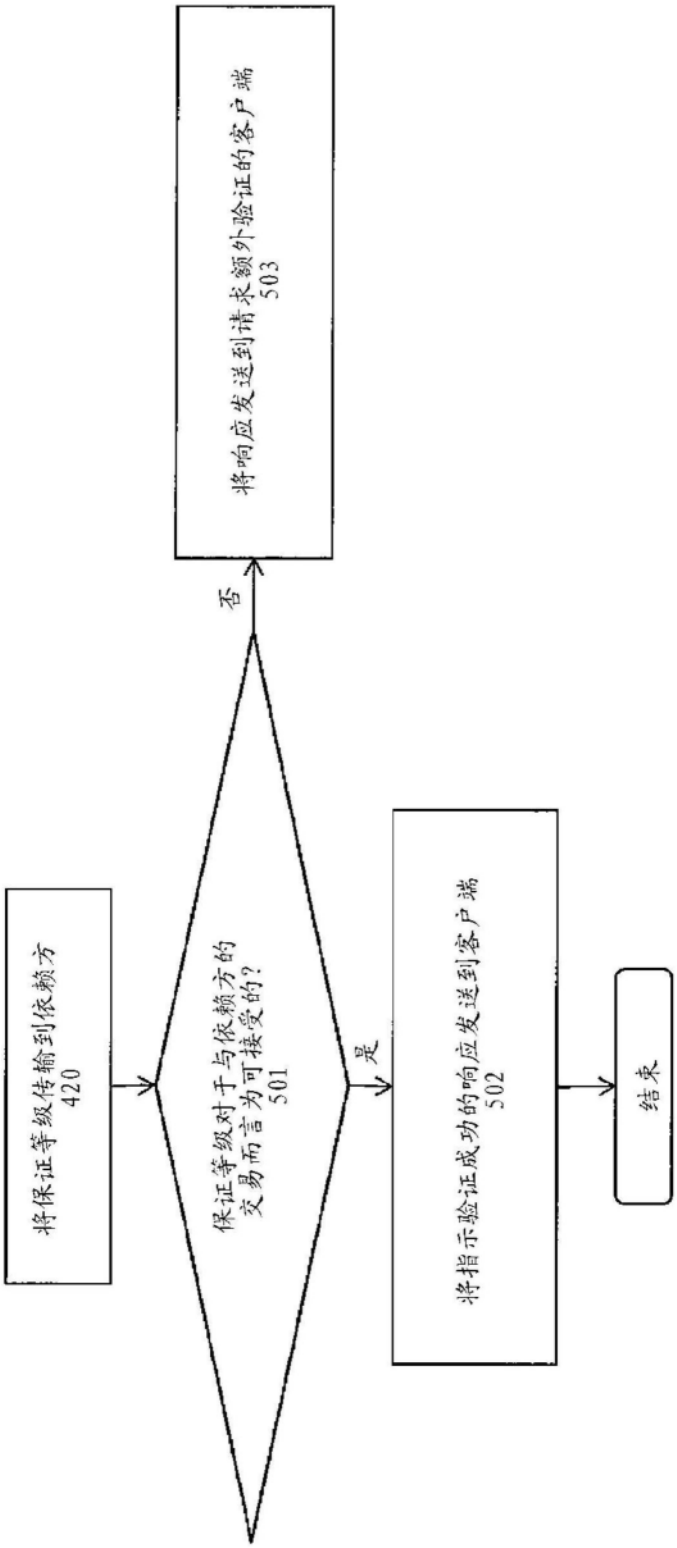

将保证等级传输到依赖方
420
保证等级对于与依赖方的
交易而言为可接受的?
501
否
将响应发送到请求额外验证的客户端
503
是
将指示验证成功的响应发送到客户端
502
结束

图5

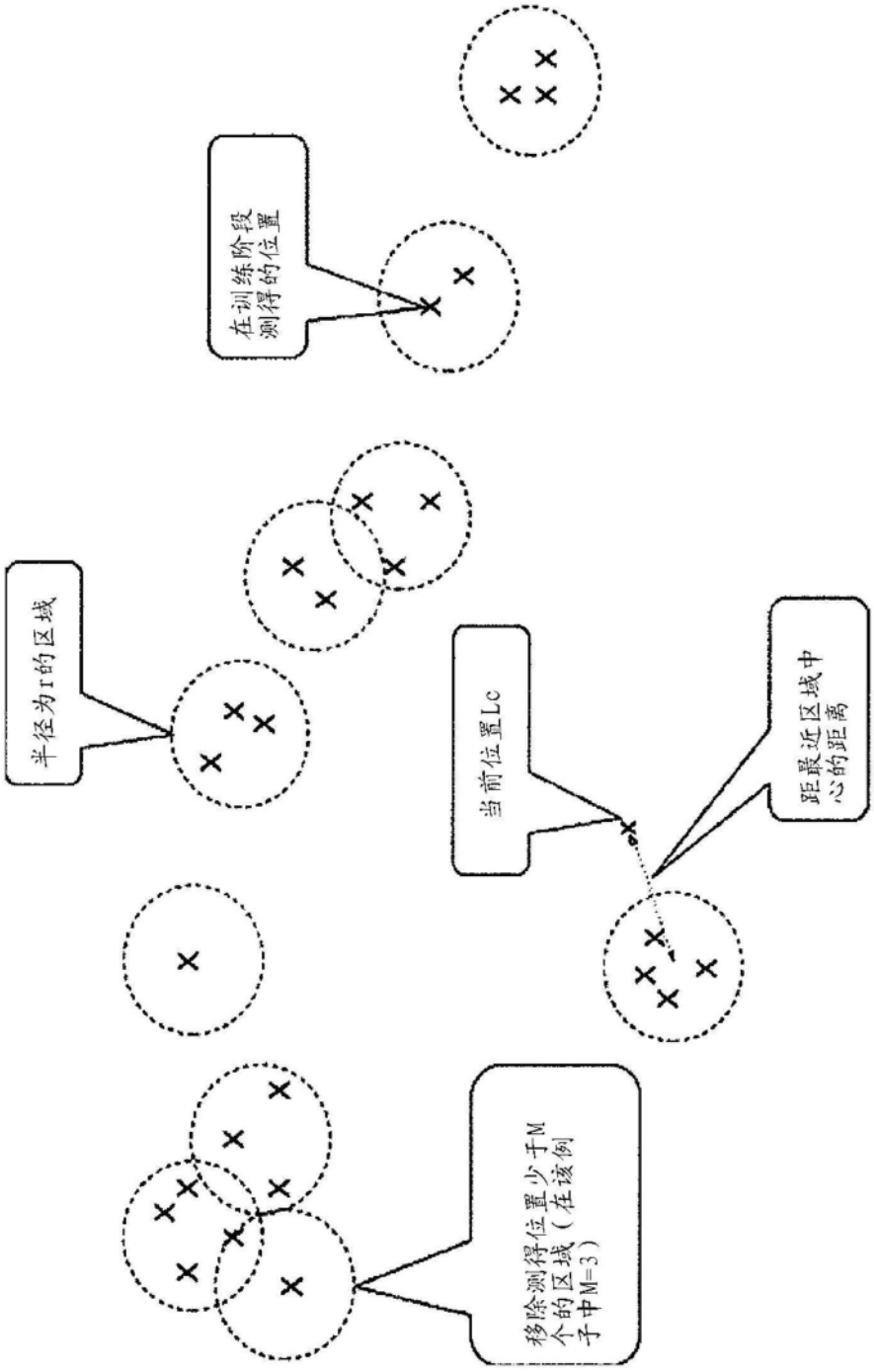

在训练阶段测得的位置
半径为r的区域
当前位置Lc
距最近区域中心的距离
移除测得位置少于M个的区域（在该例子中M=3）

图6

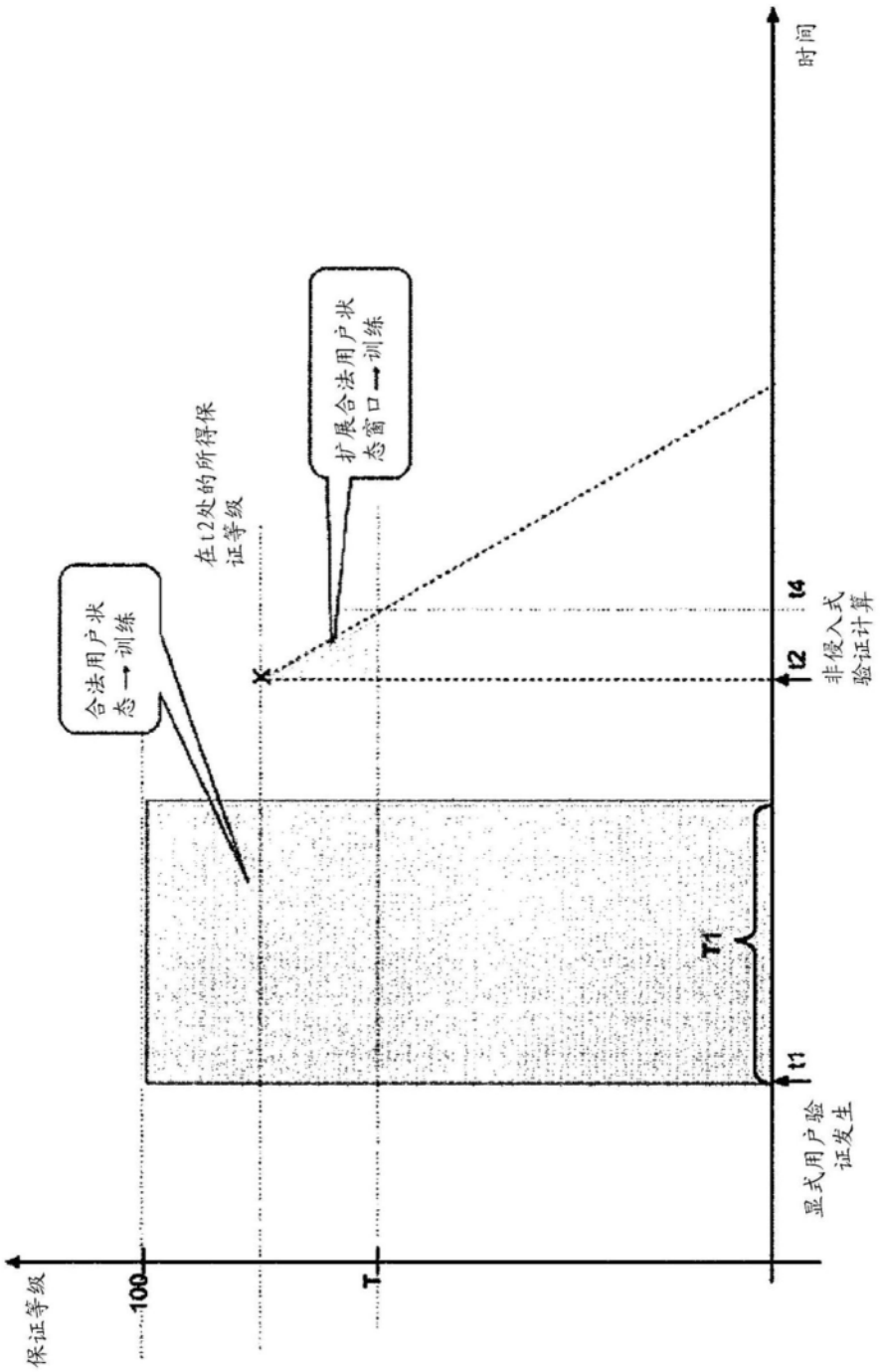

保证等级
100
T
显式用户验证发生
t1
T1
非侵入式验证计算
t2
t4
在t2处的所得保证等级
合法用户状态→训练
扩展合法用户状态窗口→训练
时间

图7

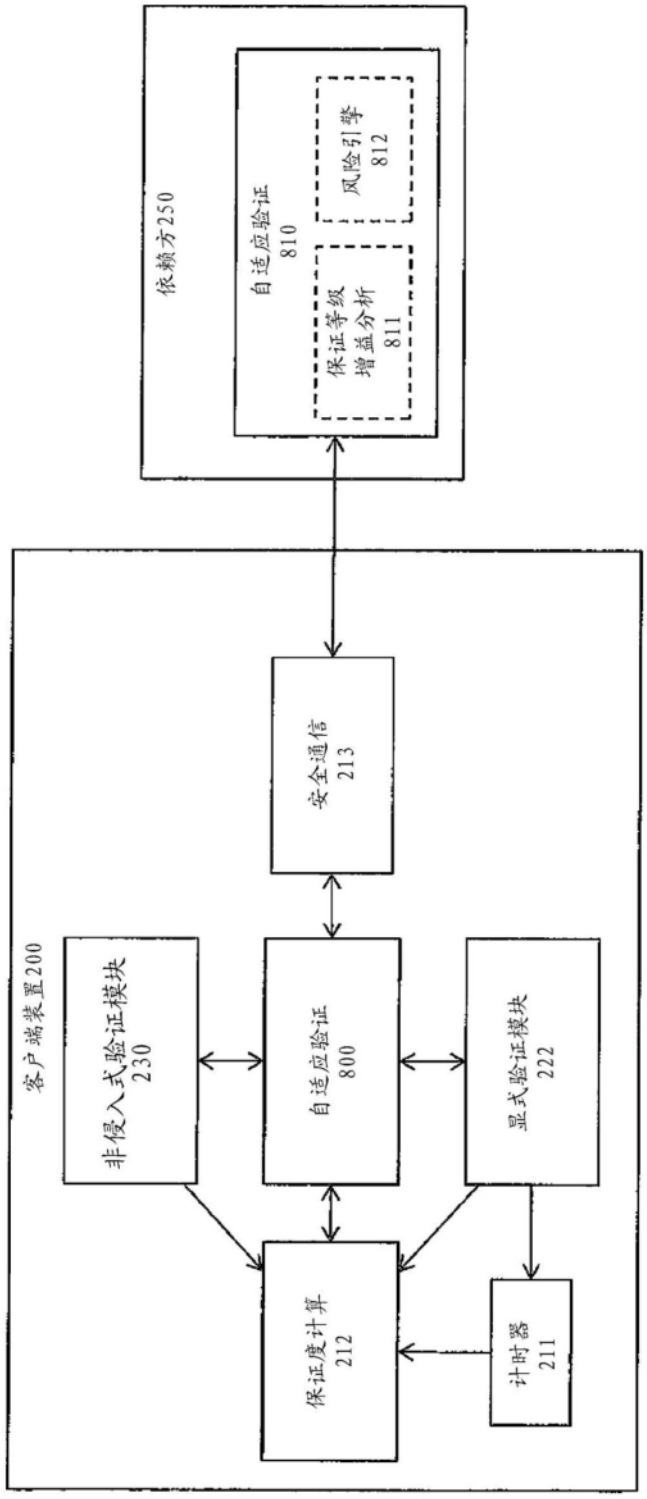

依赖方250
自适应验证
810
保证等级
增益分析
811
风险引擎
812
客户端装置200
安全通信
213
非侵入式验证模块
230
自适应验证
800
显式验证模块
222
保证度计算
212
计时器
211

图8

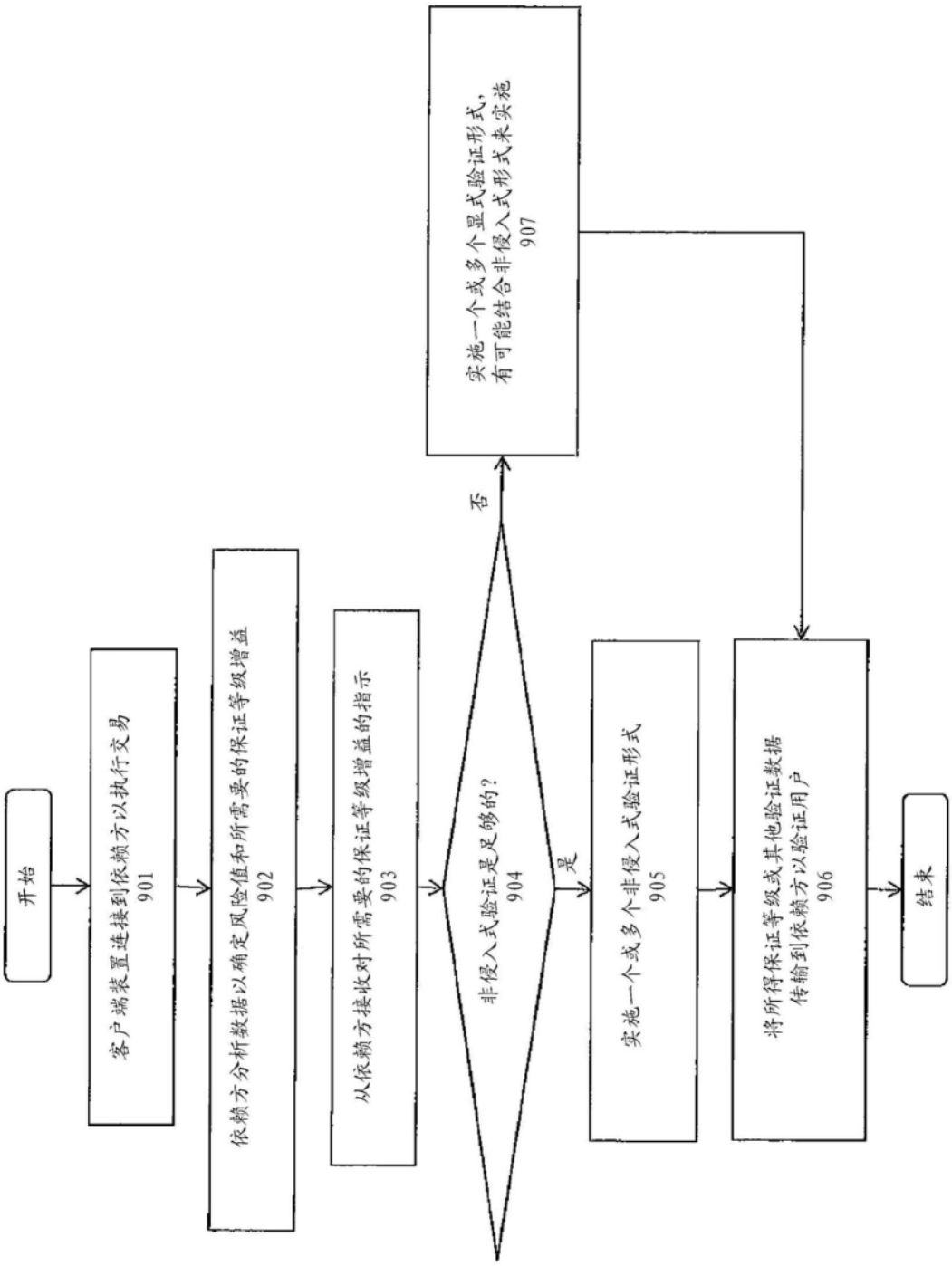

开始
客户端装置连接到依赖方以执行交易
901
依赖方分析数据以确定风险值和所需要的保证等级增益
902
从依赖方接收对所需要的保证等级增益的指示
903
非侵入式验证是足够的?
904
否
实施一个或多个显式验证形式，
有可能结合非侵入式形式来实施
907
是
实施一个或多个非侵入式验证形式
905
将所得保证等级或其他验证数据
传输到依赖方以验证用户
906
结束

图9

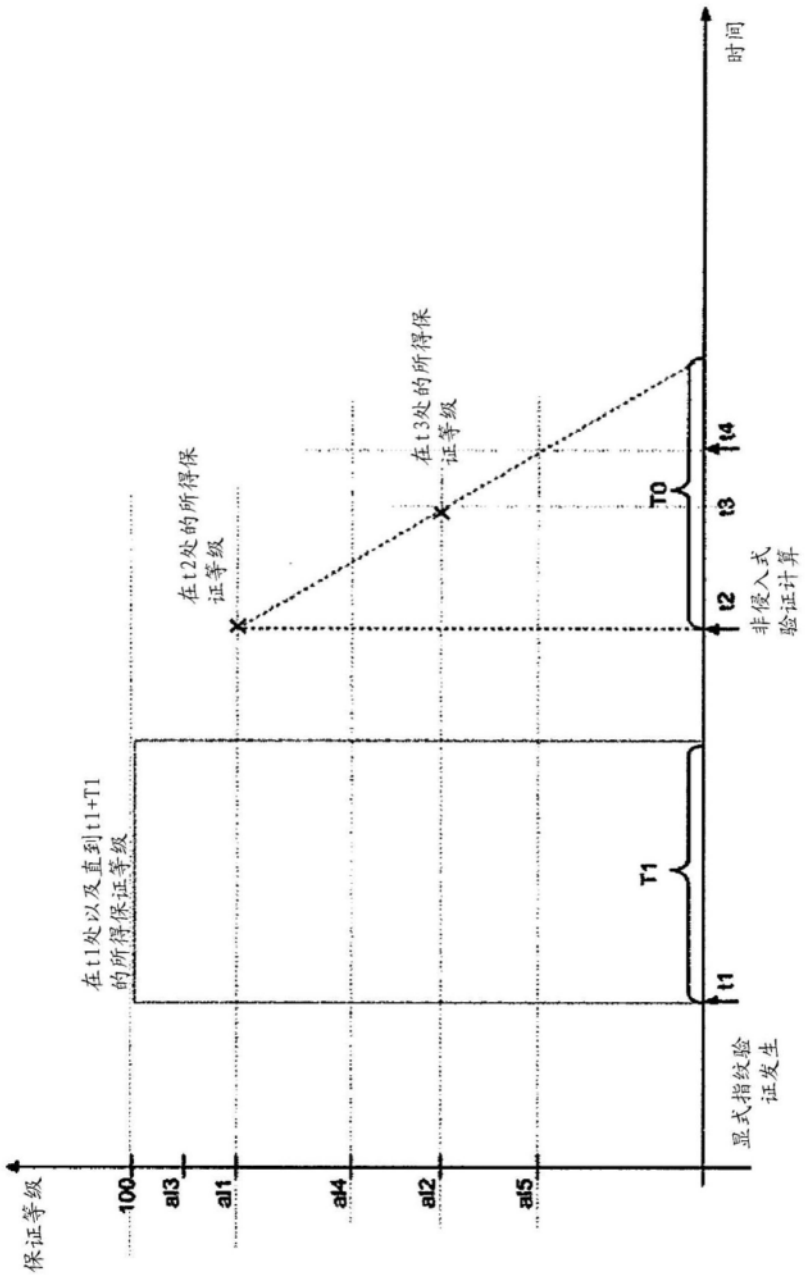

保证等级
100
al3
al1
al4
al2
al5
显式指纹验证发生
t1
T1
在t1处以及直到t1+T1的所得保证等级
在t2处的所得保证等级
在t3处的所得保证等级
T0
t2
非侵入式验证计算
t3
t4
时间

图10

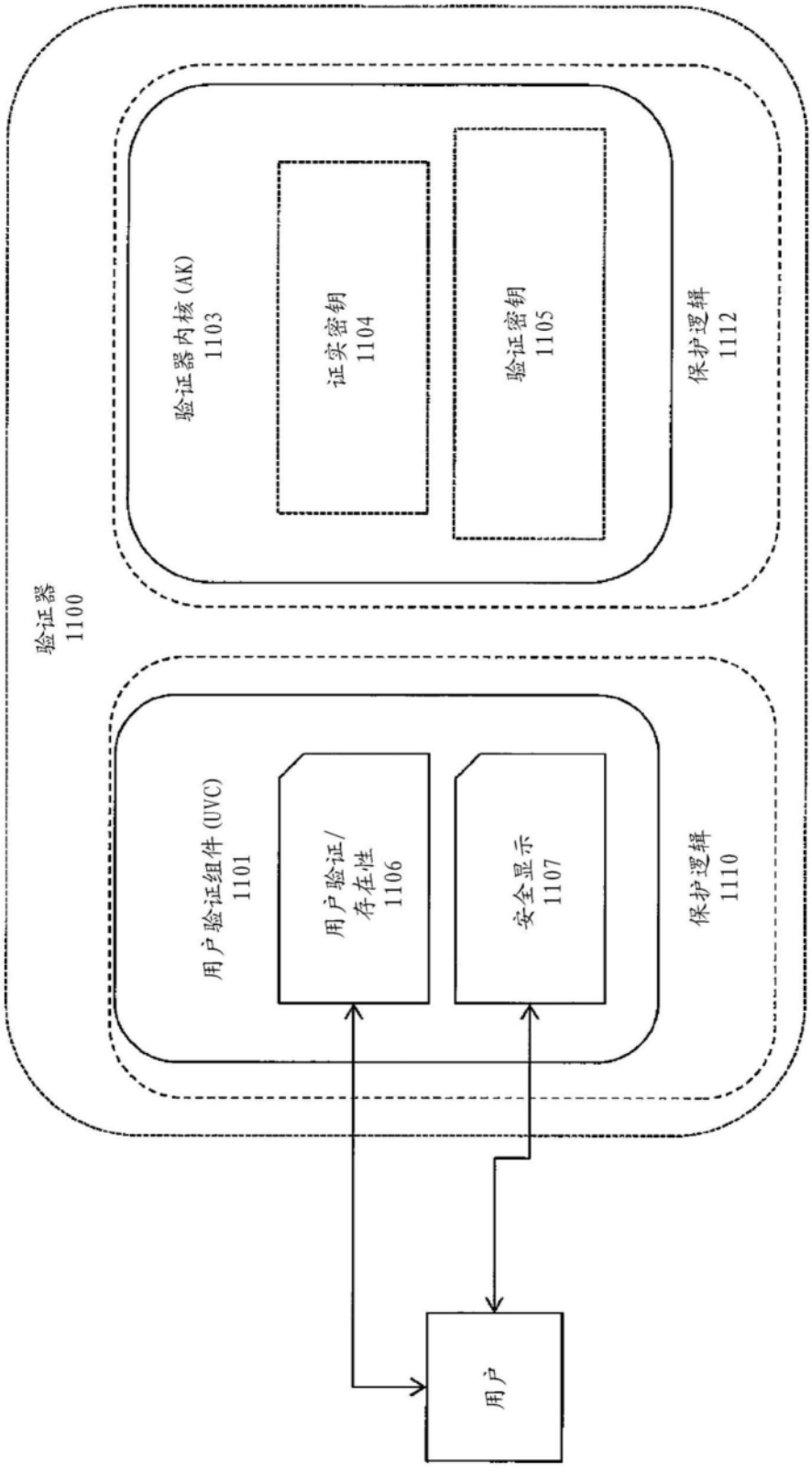

验证器
1100
验证器内核(AK)
1103
证实密钥
1104
验证密钥
1105
保护逻辑
1112
用户验证组件(UVC)
1101
用户验证/
存在性
1106
安全显示
1107
保护逻辑
1110
用户

图11

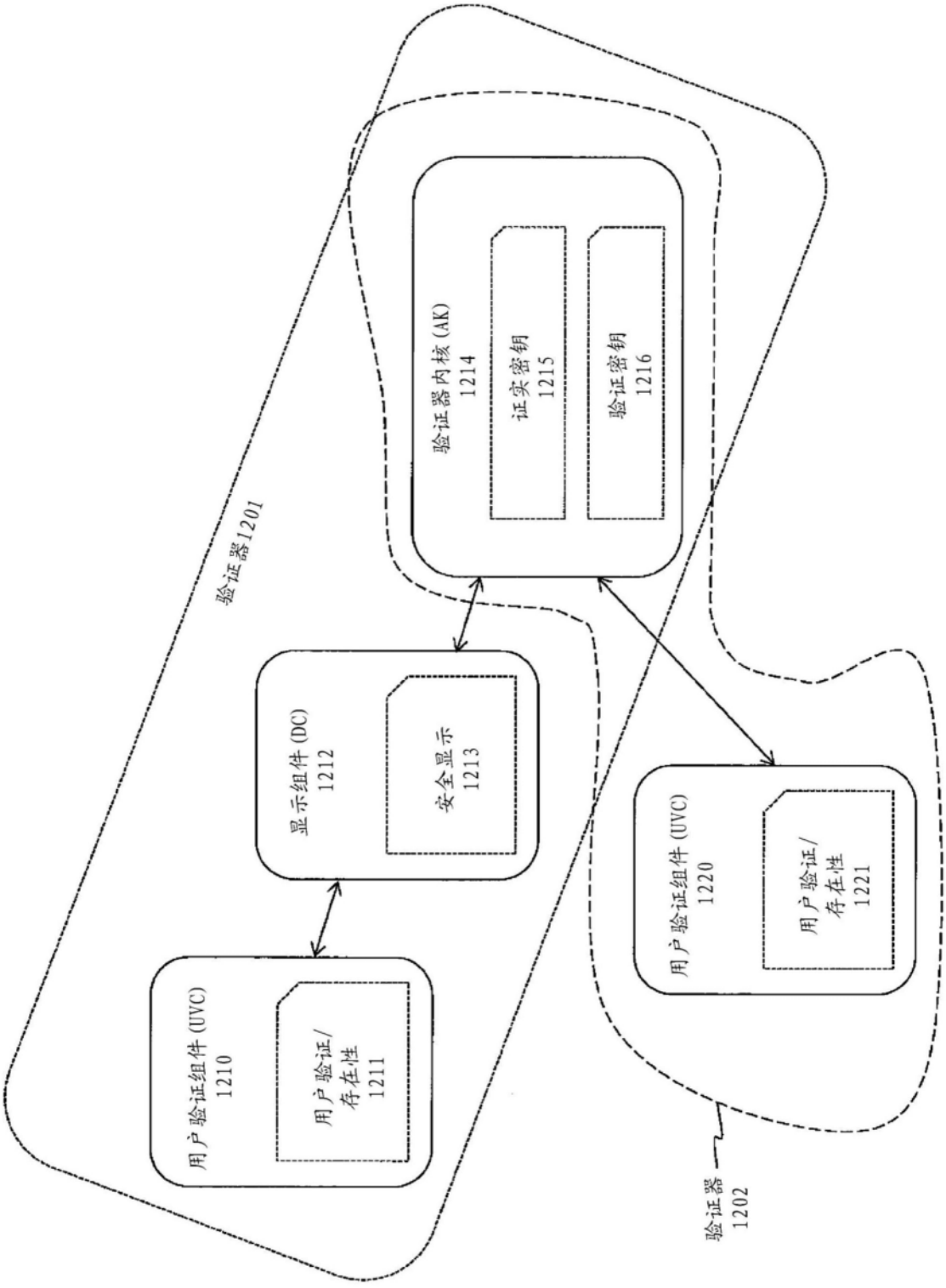

验证器1201
验证器内核 (AK)
1214
证实密钥
1215
验证密钥
1216
显示组件 (DC)
1212
安全显示
1213
用户验证组件 (UVC)
1210
用户验证/
存在性
1211
用户验证组件 (UVC)
1220
用户验证/
存在性
1221
验证器
1202

图12

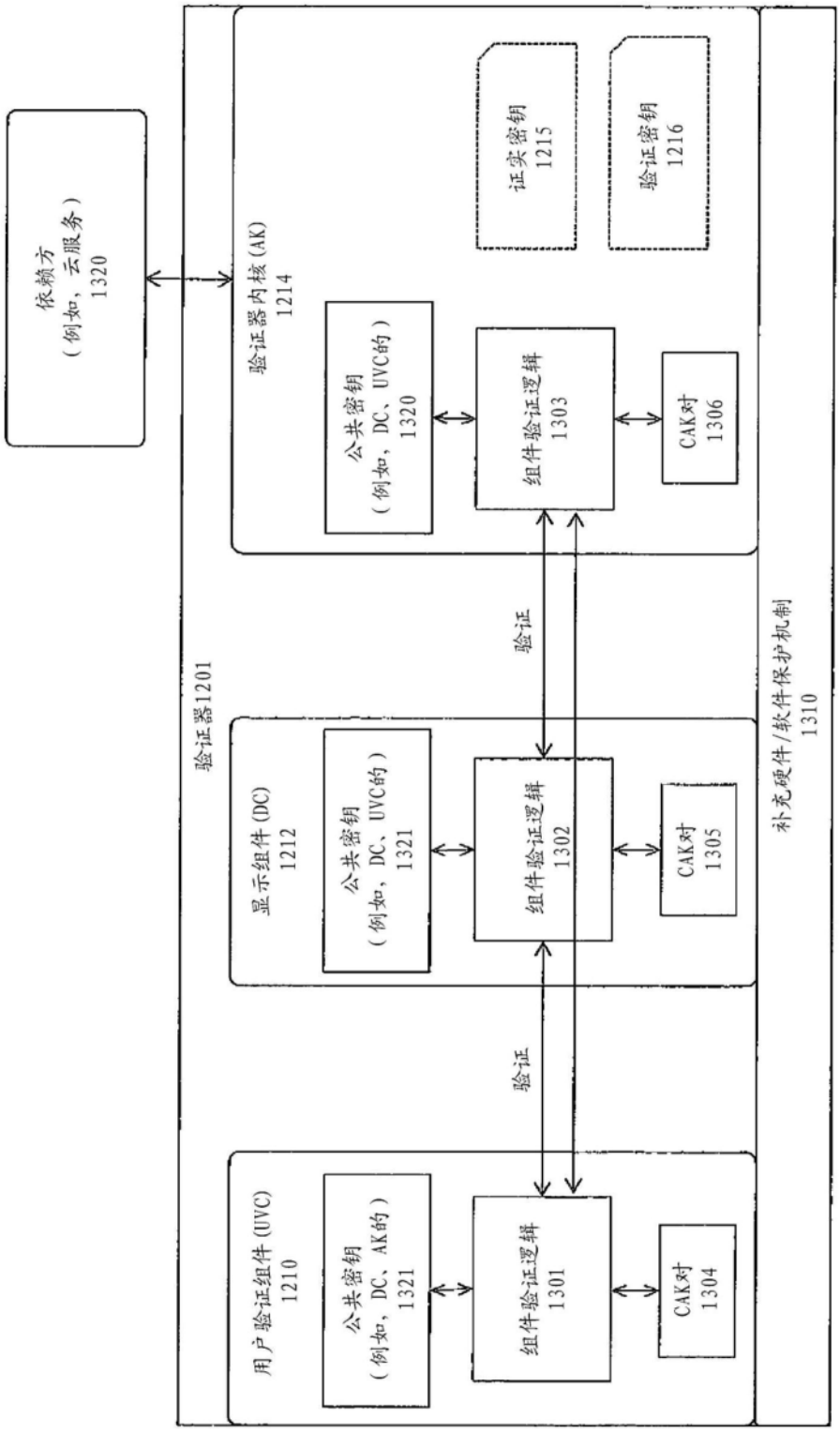

依赖方
（例如，云服务）
1320
验证器1201
验证器内核(AK)
1214
证实密钥
1215
验证密钥
1216
公共密钥
（例如，DC、UVC的）
1320
组件验证逻辑
1303
CAK对
1306
验证
显示组件(DC)
1212
公共密钥
（例如，DC、UVC的）
1321
组件验证逻辑
1302
CAK对
1305
验证
用户验证组件(UVC)
1210
公共密钥
（例如，DC、AK的）
1321
组件验证逻辑
1301
CAK对
1304
补充硬件/软件保护机制
1310

图13

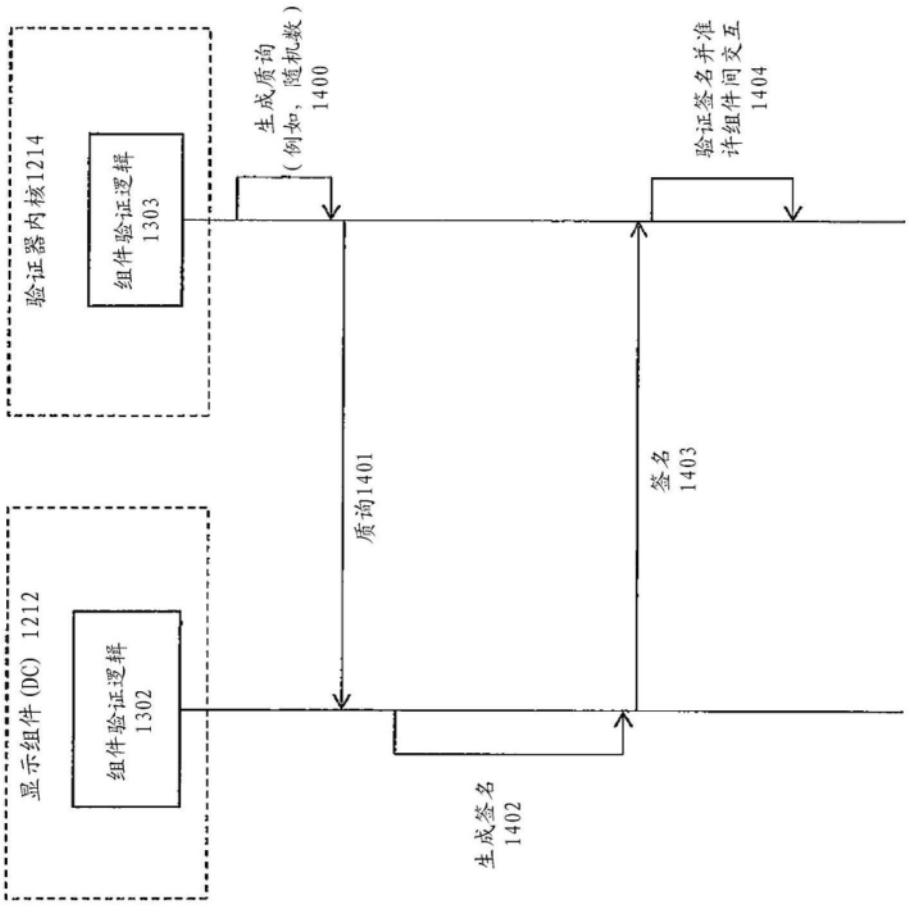

验证器内核1214
组件验证逻辑
1303
显示组件(DC) 1212
组件验证逻辑
1302
生成质询
(例如，随机数)
1400
质询1401
生成签名
1402
签名
1403
验证签名并准
许组件间交互
1404

图14

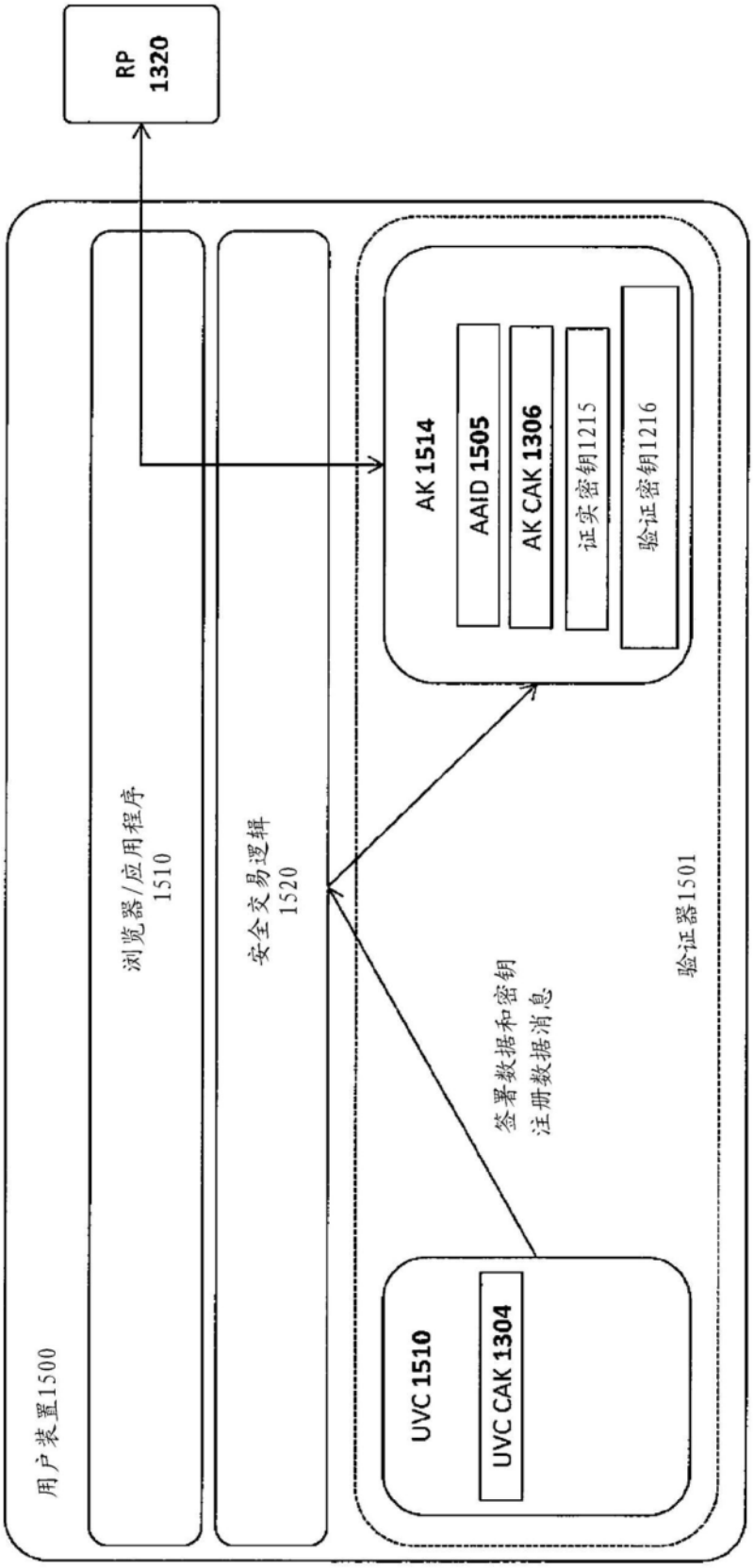

RP
1320
浏览器/应用程序
1510
安全交易逻辑
1520
AK 1514
AAID 1505
AK CAK 1306
证实密钥1215
验证密钥1216
验证器1501
签署数据和密钥
注册数据消息
UVC 1510
UVC CAK 1304
用户装置1500

图15

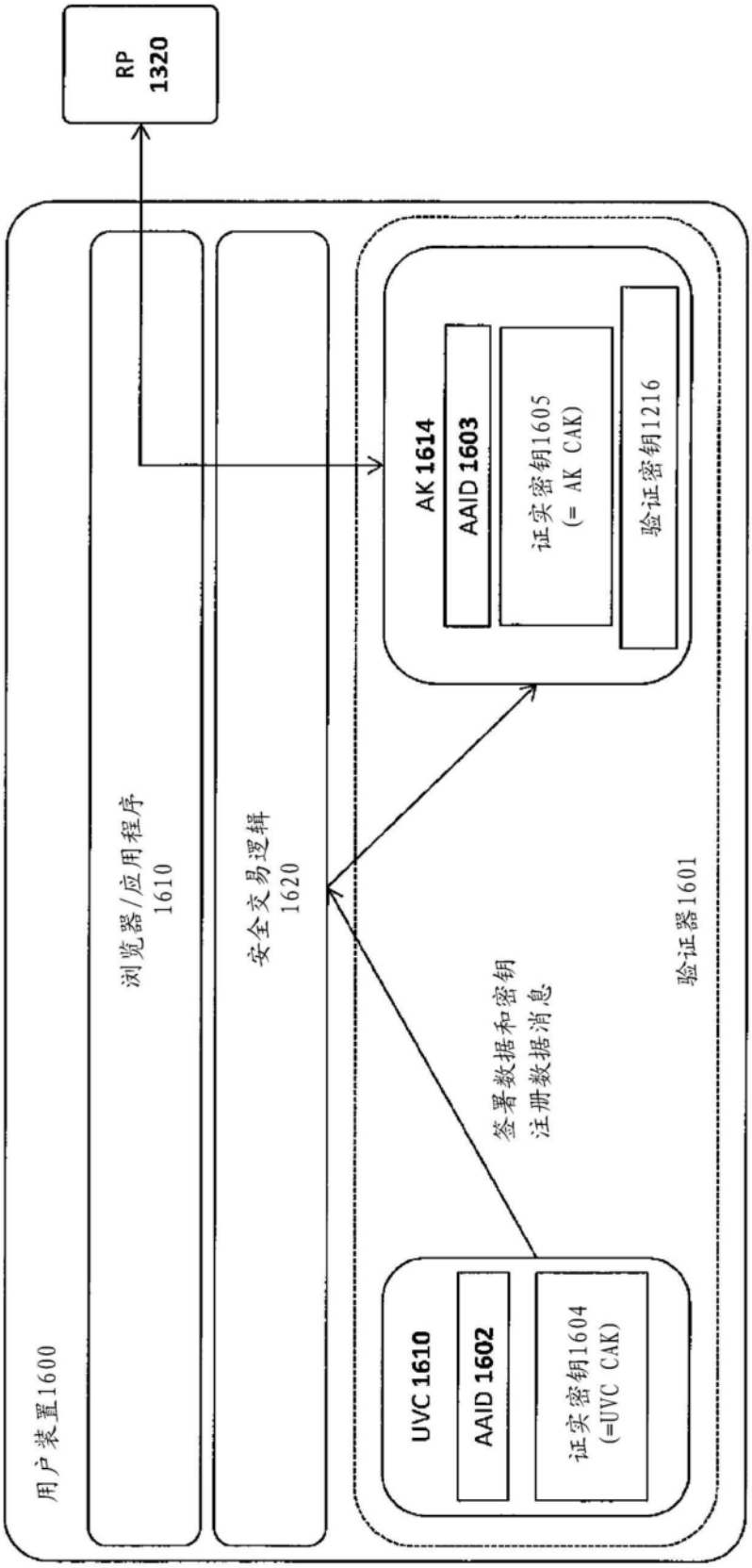

RP
1320
浏览器/应用程序
1610
安全交易逻辑
1620
AK 1614
AAID 1603
证实密钥1605
(= AK CAK)
验证密钥1216
签署数据和密钥
注册数据消息
验证器1601
UVC 1610
AAID 1602
证实密钥1604
(=UVC CAK)
用户装置1600

图16

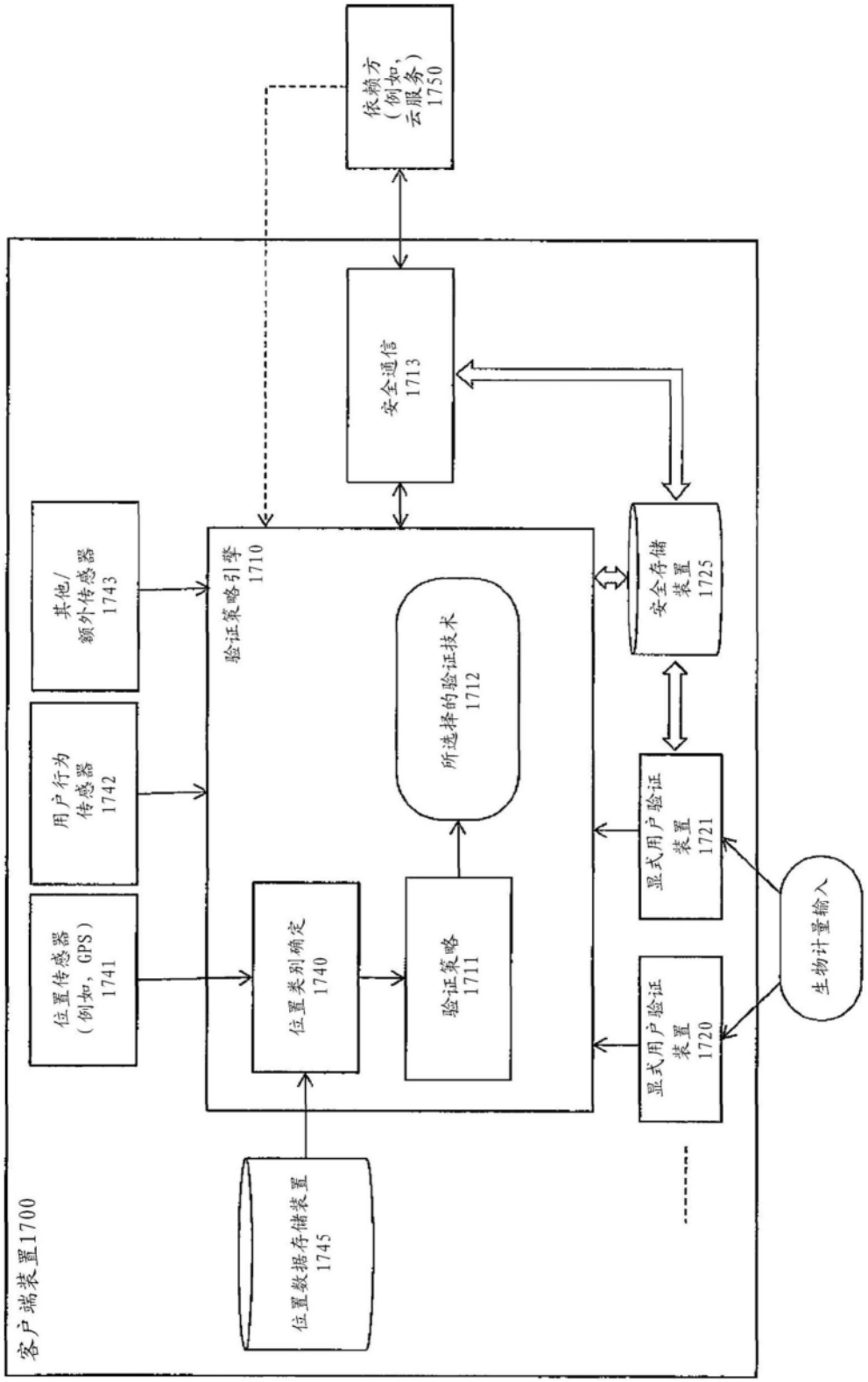

依赖方
（例如，
云服务）
1750
安全通信
1713
客户端装置1700
其他/
额外传感器
1743
用户行为
传感器
1742
位置传感器
（例如，GPS）
1741
验证策略引擎
1710
位置类别确定
1740
验证策略
1711
所选择的验证技术
1712
安全存储
装置
1725
显式用户验证
装置
1721
显式用户验证
装置
1720
生物计量输入
位置数据存储装置
1745

图17

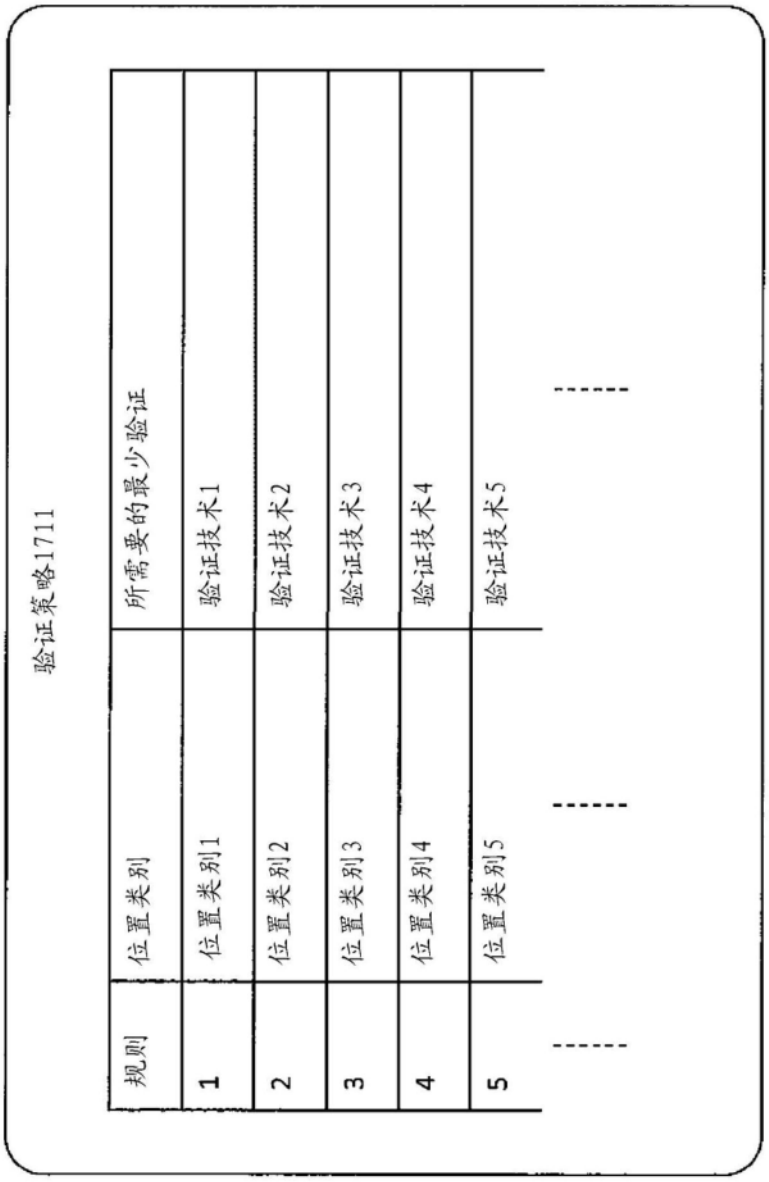

验证策略1711
规则
位置类别
所需要的最少验证
1
位置类别1
验证技术1
2
位置类别2
验证技术2
3
位置类别3
验证技术3
4
位置类别4
验证技术4
5
位置类别5
验证技术5

图18

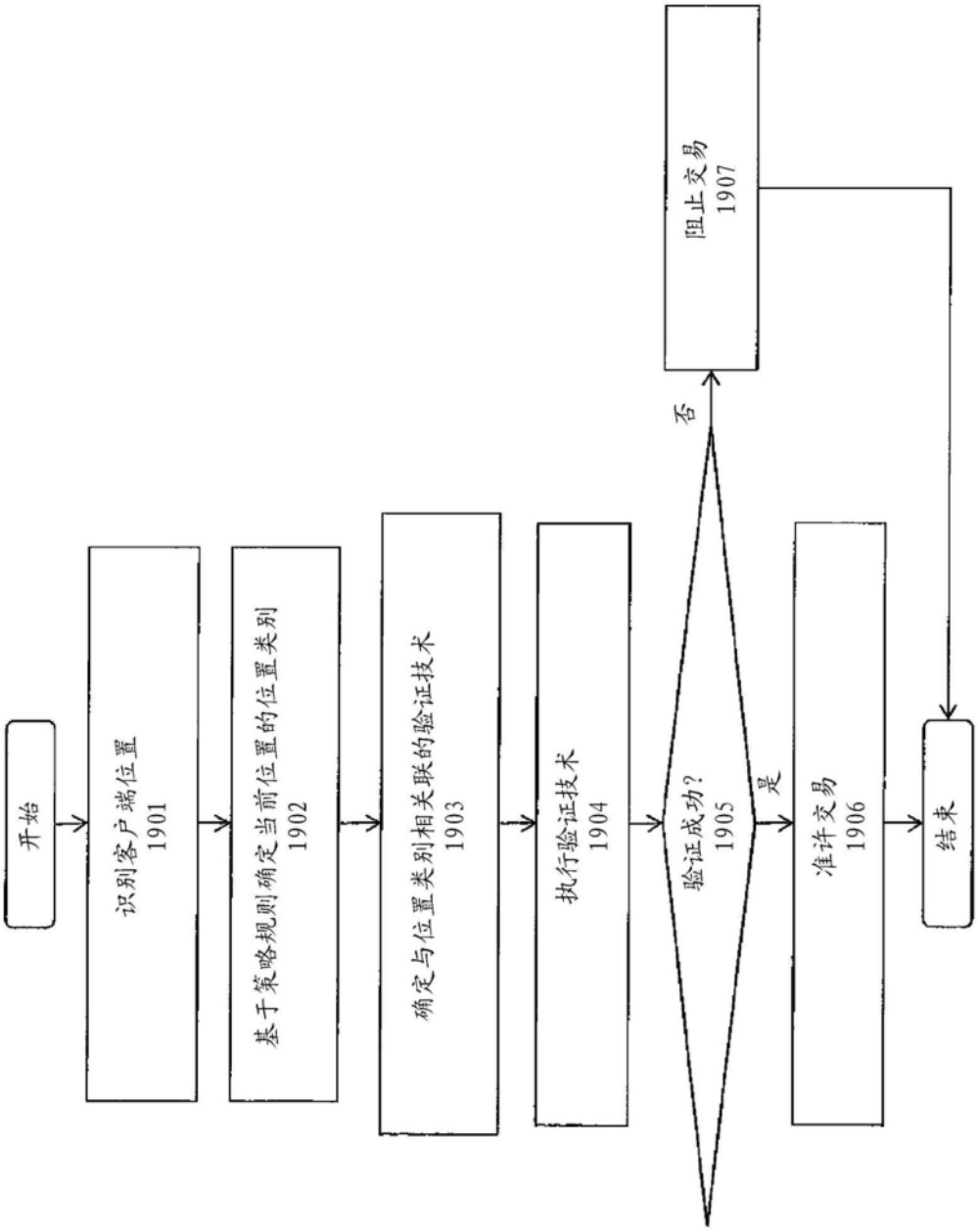

开始
识别客户端位置
1901
基于策略规则确定当前位置的位置类别
1902
确定与位置类别相关联的验证技术
1903
执行验证技术
1904
验证成功?
1905
否
是
阻止交易
1907
准许交易
1906
结束

图19

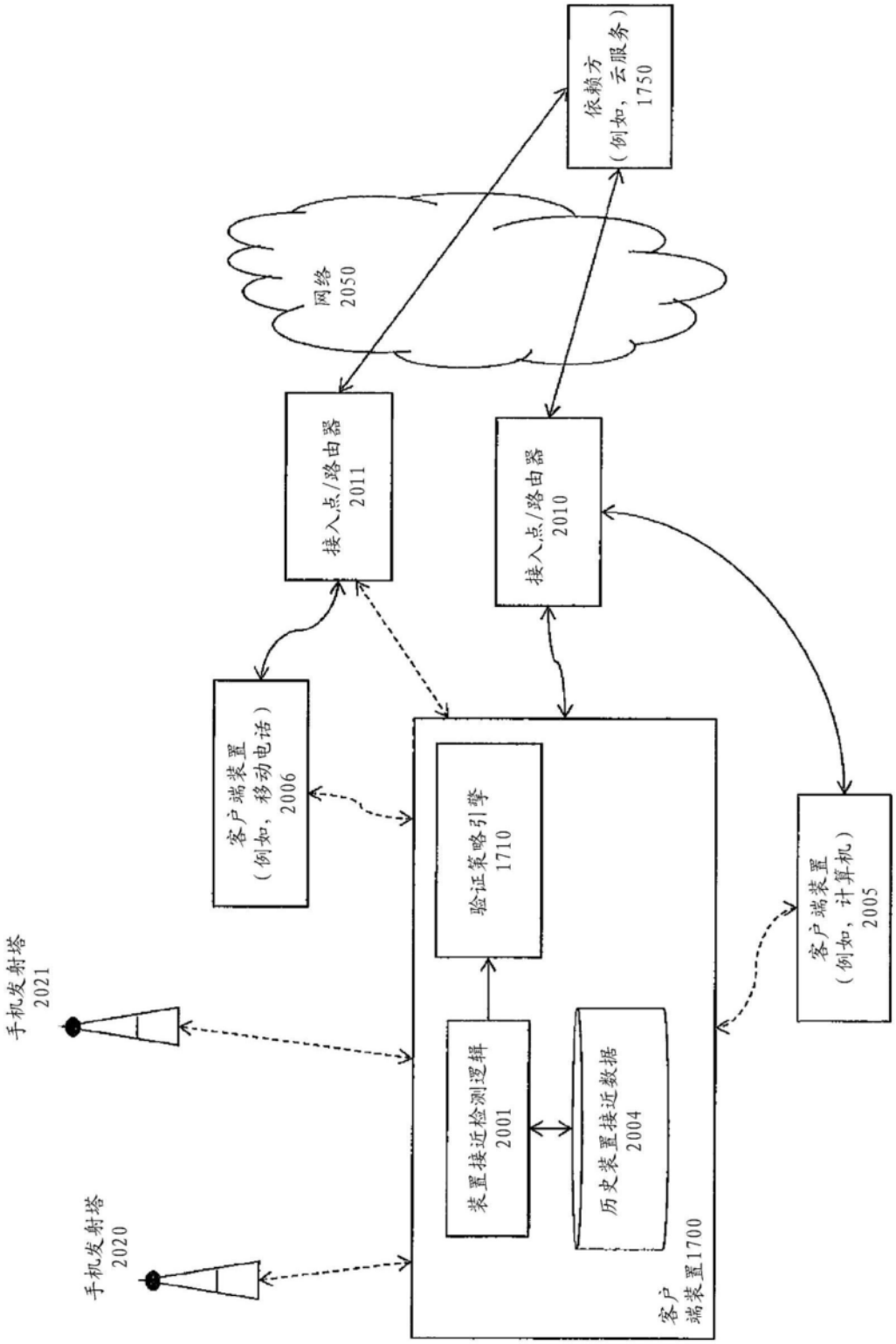

依赖方
（例如，云服务）
1750
网络
2050
接入点/路由器
2011
接入点/路由器
2010
客户端装置
（例如，移动电话）
2006
验证策略引擎
1710
客户端装置
（例如，计算机）
2005
手机发射塔
2021
装置接近检测逻辑
2001
历史装置接近数据
2004
手机发射塔
2020
客户
端装置1700

图20

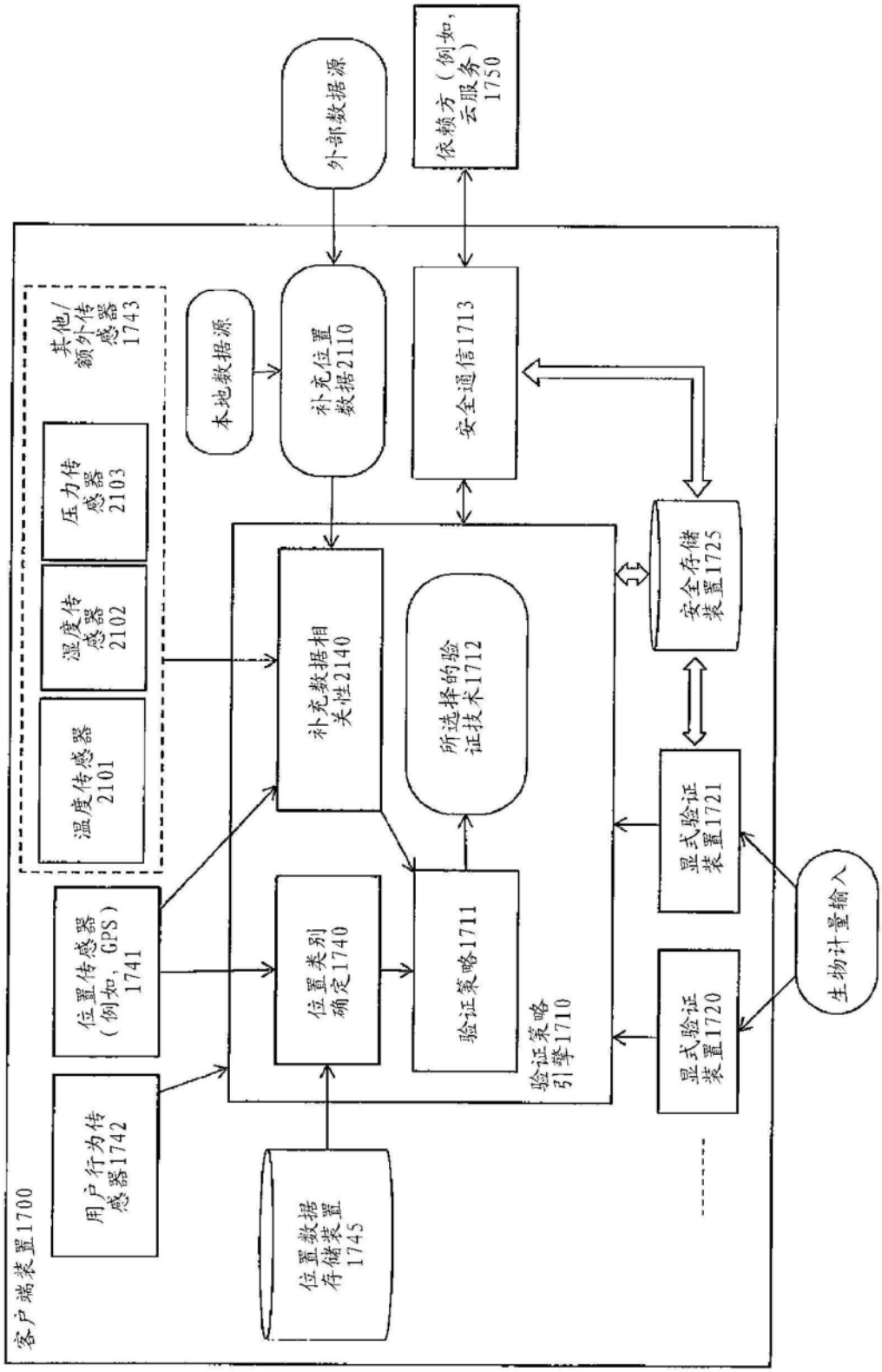

外部数据源
依赖方（例如，云服务）1750
本地数据源
补充位置数据2110
安全通信1713
其他/额外传感器1743
压力传感器2103
湿度传感器2102
温度传感器2101
补充数据相关性2140
所选择的验证技术1712
安全存储装置1725
位置传感器（例如，GPS）1741
位置类别确定1740
验证策略1711
显式验证装置1721
显式验证装置1720
生物计量输入
用户行为传感器1742
位置数据存储装置1745
验证策略引擎1710
客户端装置1700

图21

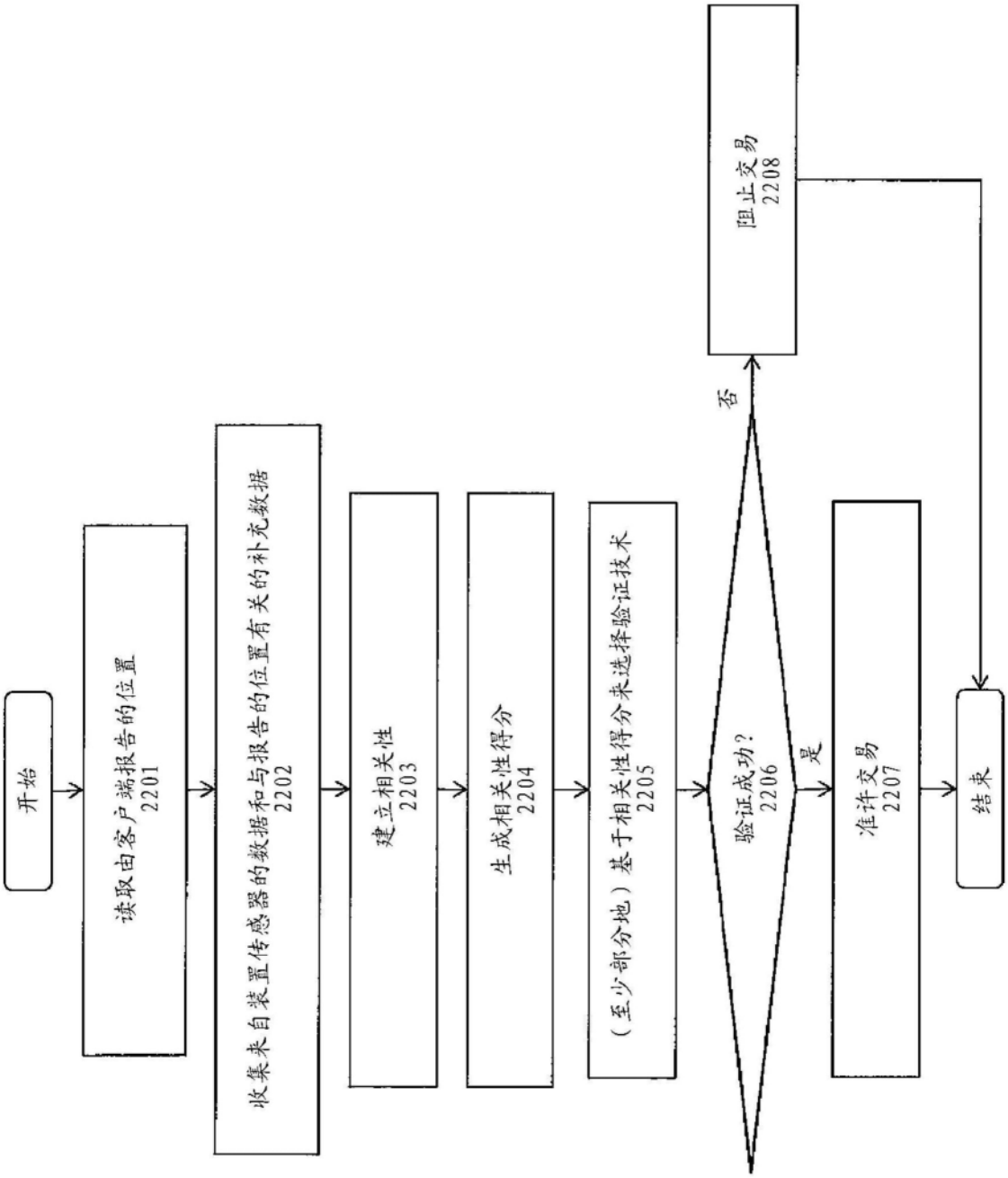

开始
读取由客户端报告的位置
2201
收集来自装置传感器的数据和与报告的位置有关的补充数据
2202
建立相关性
2203
生成相关性得分
2204
（至少部分地）基于相关性得分来选择验证技术
2205
验证成功?
2206
否
是
阻止交易
2208
准许交易
2207
结束

图22

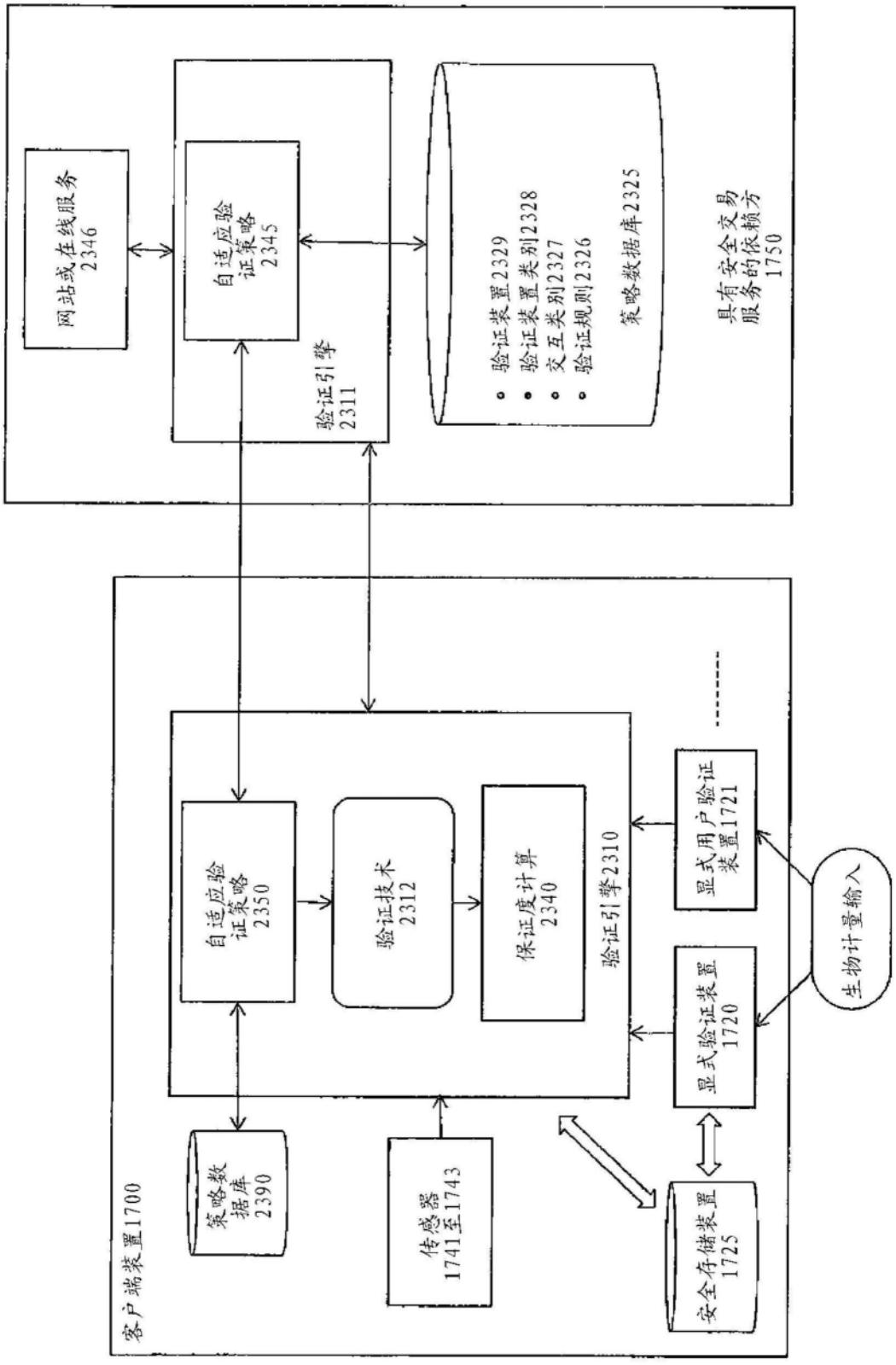

网站或在线服务
2346
自适应验证策略
2345
验证引擎
2311
验证装置2329
验证装置类别2328
交互类别2327
验证规则2326
策略数据库2325
具有安全交易服务的依赖方
1750
客户端装置1700
自适应验证策略
2350
验证技术
2312
保证度计算
2340
验证引擎2310
显式用户验证装置1721
显式验证装置
1720
生物计量输入
策略数据库
2390
传感器
1741至1743
安全存储装置
1725

图23

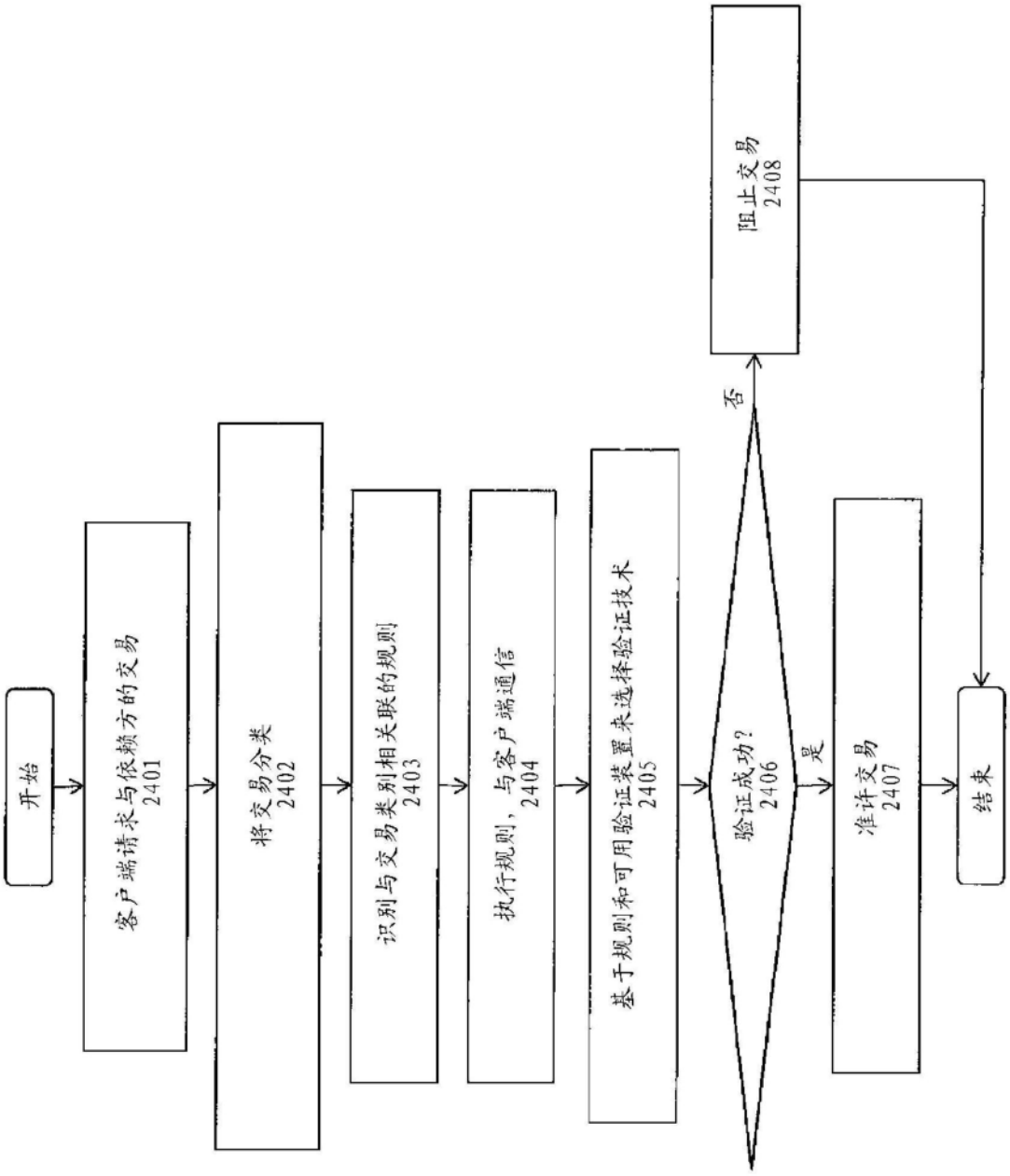
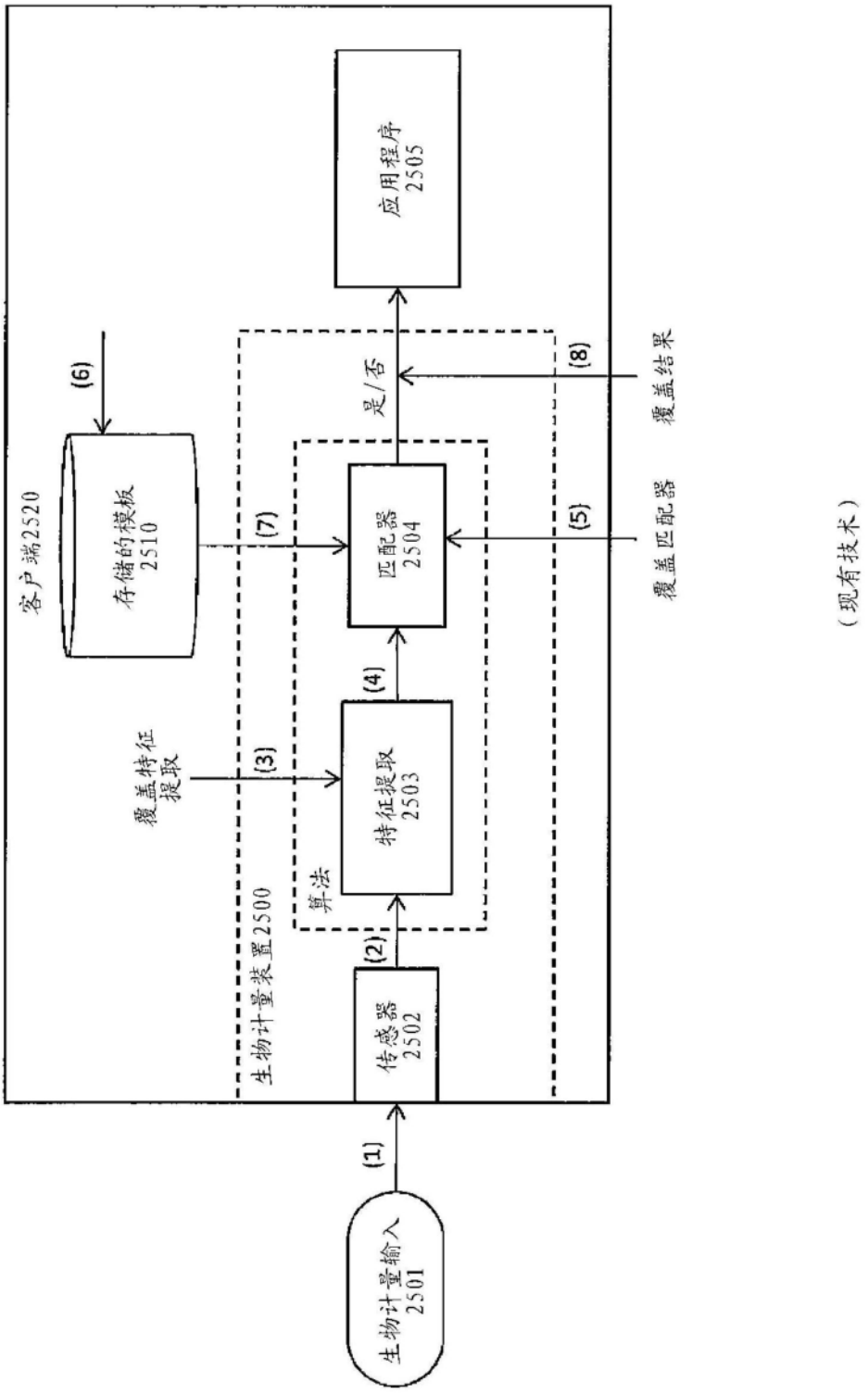

开始
客户端请求与依赖方的交易
2401
将交易分类
2402
识别与交易类别相关联的规则
2403
执行规则，与客户端通信
2404
基于规则和可用验证装置来选择验证技术
2405
验证成功?
2406
否
是
阻止交易
2408
准许交易
2407
结束

图24


生物计量输入
2501
(1)
传感器
2502
(2)
特征提取
2503
(4)
匹配器
2504
(5)
覆盖匹配器
(3)
覆盖特征
提取
(6)
存储的模板
2510
(7)
客户端2520
生物计量装置2500
算法
是/否
(8)
覆盖结果
应用程序
2505

（现有技术）

图25

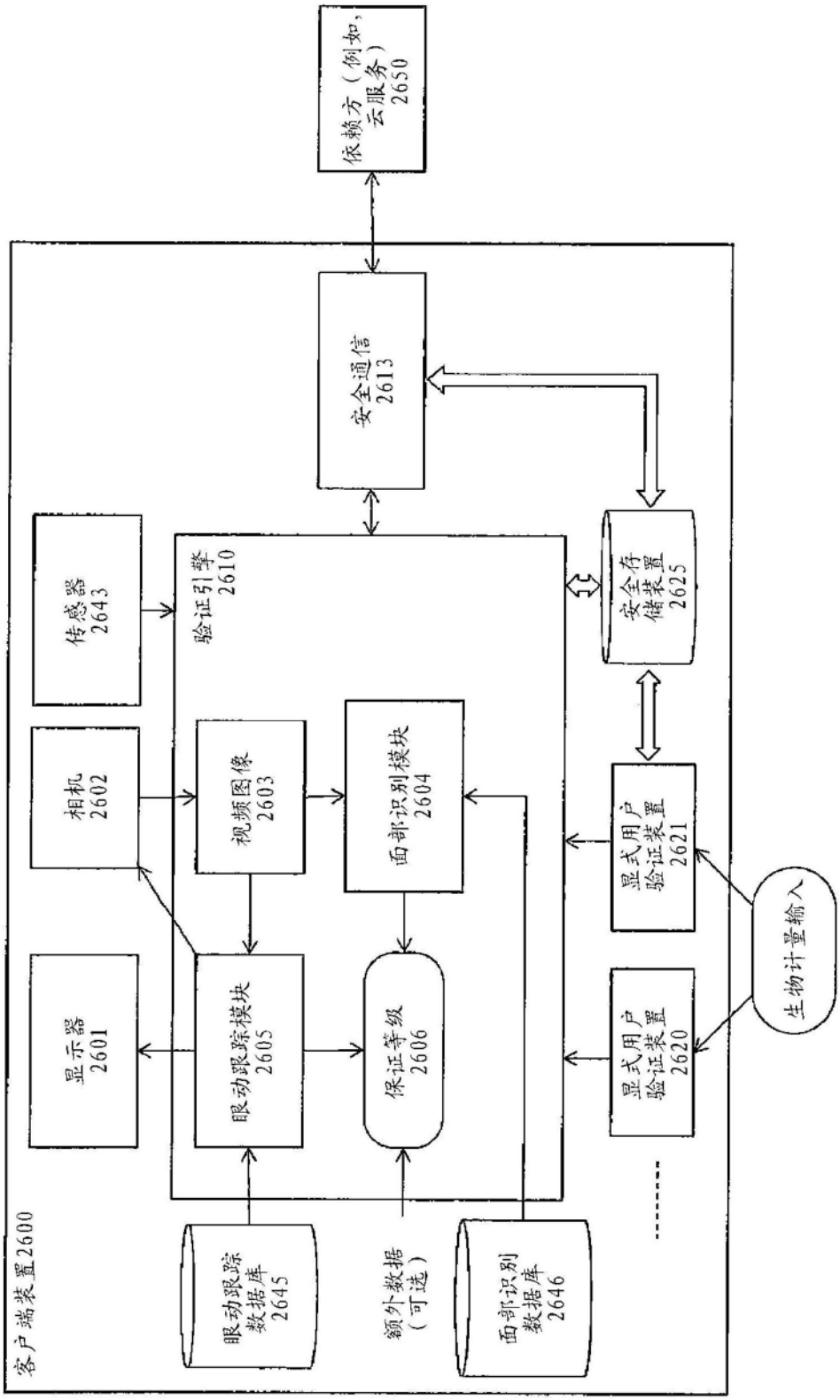

依赖方（例如，云服务）
2650
安全通信
2613
客户端装置2600
验证引擎
2610
传感器
2643
相机
2602
显示器
2601
视频图像
2603
面部识别模块
2604
眼动跟踪模块
2605
保证等级
2606
安全存储装置
2625
显式用户验证装置
2621
显式用户验证装置
2620
生物计量输入
眼动跟踪数据库
2645
额外数据（可选）
面部识别数据库
2646

图26

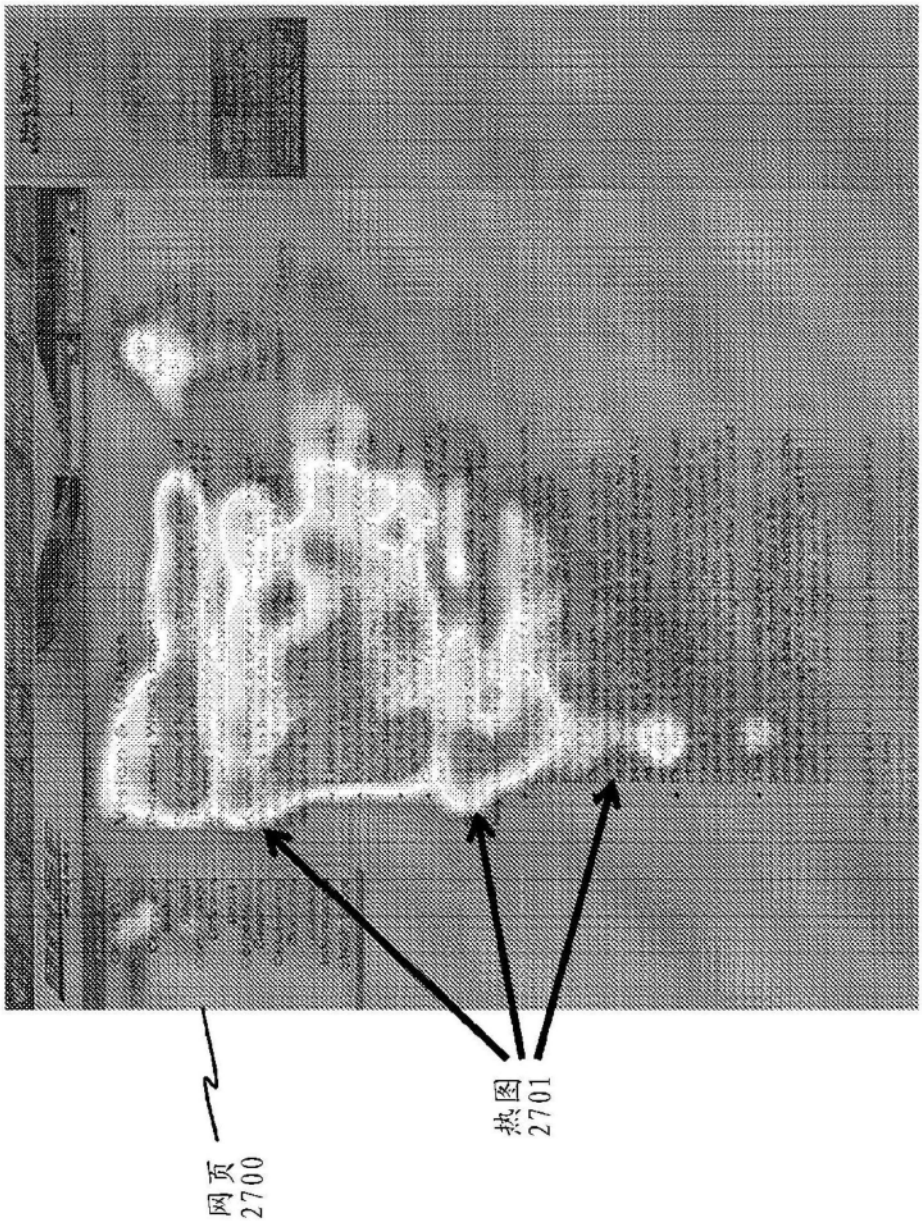


图27

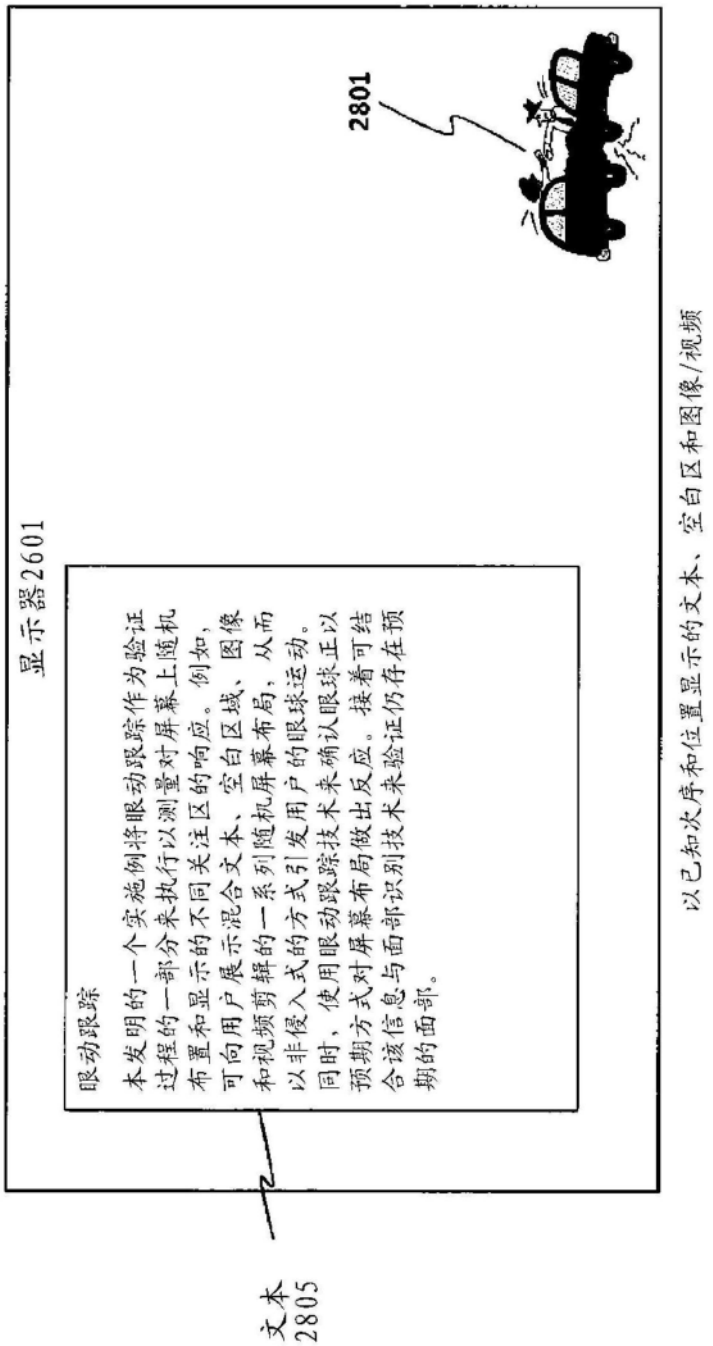

显示器2601
眼动跟踪
本发明的一个实施例将眼动跟踪作为验证过程的一部分来执行以测量对屏幕上随机布置和显示的不同关注区的响应。例如，可向用户展示混合文本、空白区域、图像和视频剪辑的一系列随机屏幕布局，从而以非侵入式的方式引发用户的眼球运动。同时，使用眼动跟踪技术来确认眼球正以预期方式对屏幕布局做出反应。接着可结合该信息与面部识别技术来验证仍存在预期的面部。
2801
以已知次序和位置显示的文本、空白区和图像/视频
文本
2805

图28A

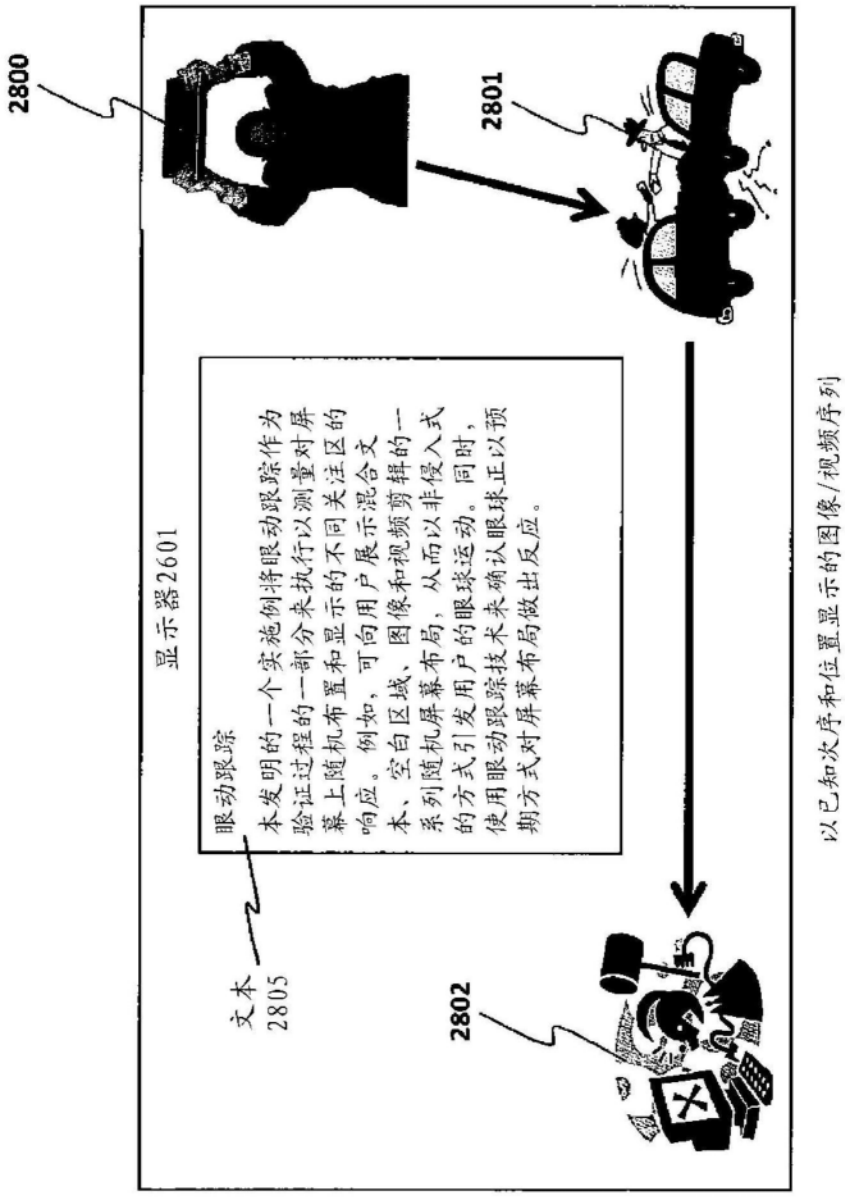

2800
2801
显示器2601
眼动跟踪
本发明的一个实施例将眼动跟踪作为验证过程的一部分来执行以测量对屏幕上随机布置和显示的不同关注区的响应。例如，可向用户展示混合文本、空白区域、图像和视频剪辑的一系列随机屏幕布局，从而以非侵入式的方式引发用户的眼球运动。同时，使用眼动跟踪技术来确认眼球正以预期方式对屏幕布局做出反应。
文本
2805
2802
以已知次序和位置显示的图像/视频序列

图28B

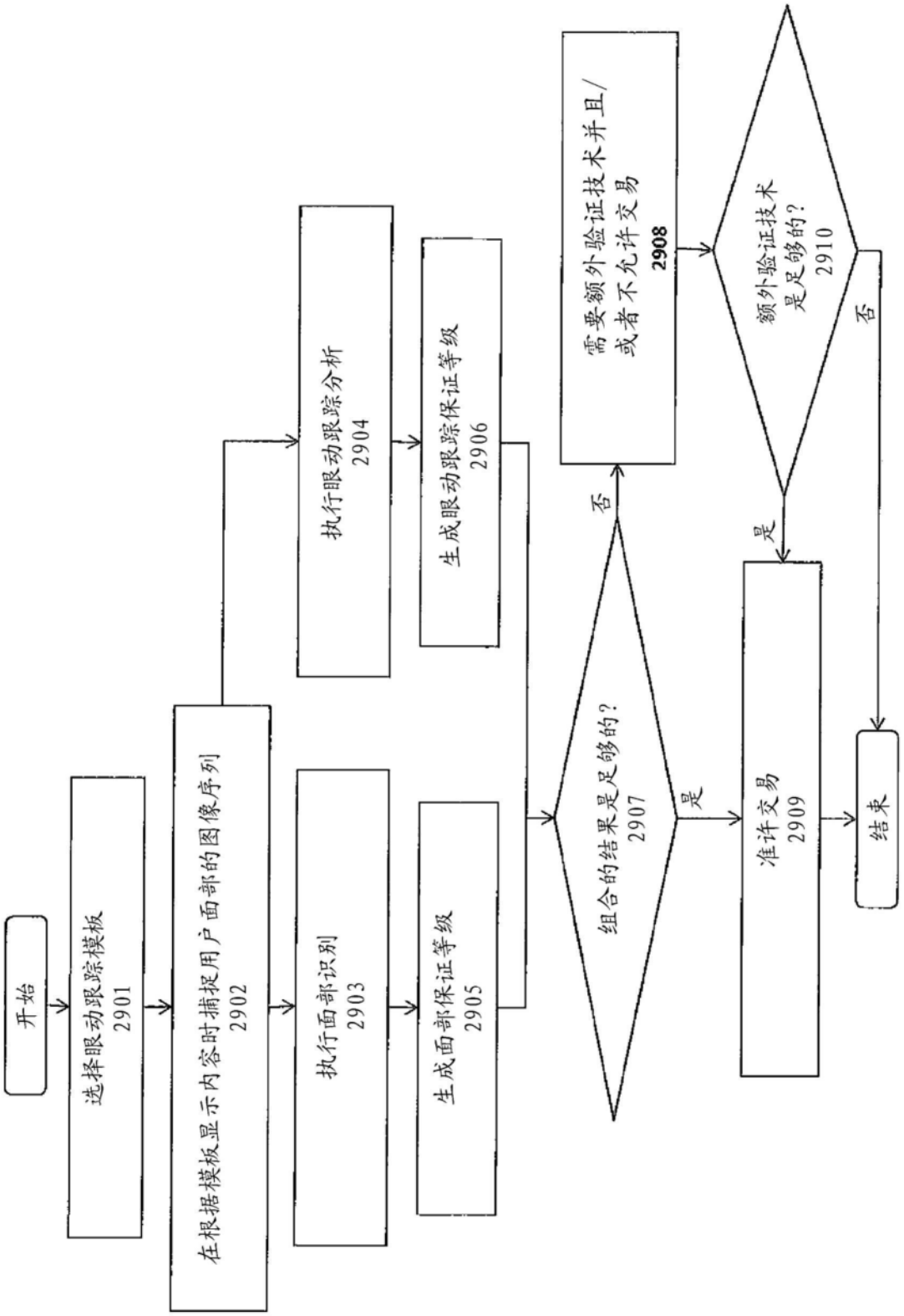

开始
选择眼动跟踪模板
2901
在根据模板显示内容时捕捉用户面部的图像序列
2902
执行面部识别
2903
生成面部保证等级
2905
执行眼动跟踪分析
2904
生成眼动跟踪保证等级
2906
组合的结果是足够的?
2907
否
是
需要额外验证技术并且/或者不允许交易
2908
额外验证技术是足够的?
2910
否
是
准许交易
2909
结束

图29

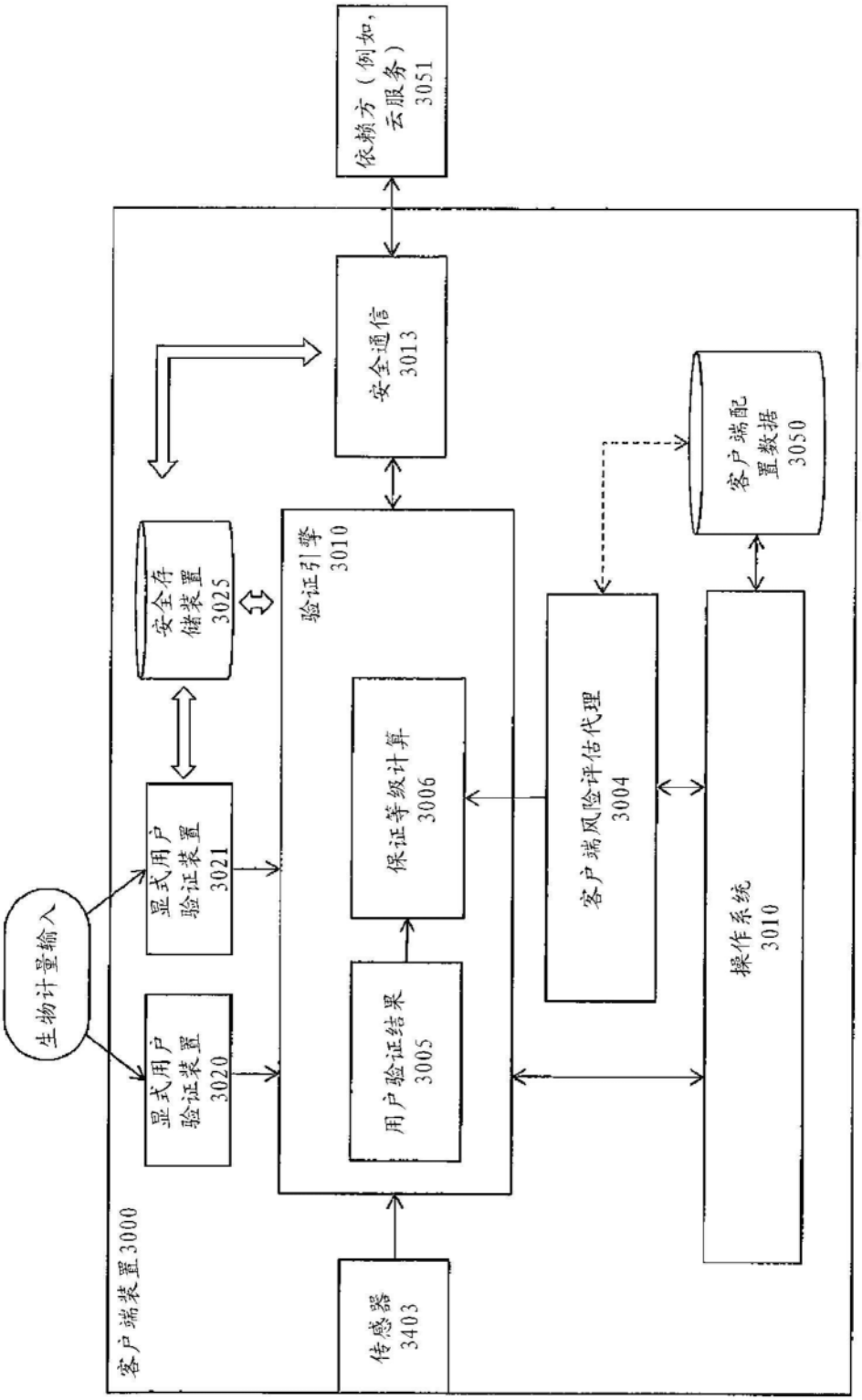

依赖方（例如，云服务）
3051
安全通信
3013
客户端配置数据
3050
安全存储装置
3025
验证引擎
3010
显式用户验证装置
3021
保证等级计算
3006
客户端风险评估代理
3004
生物计量输入
显式用户验证装置
3020
用户验证结果
3005
操作系统
3010
客户端装置3000
传感器
3403

图30

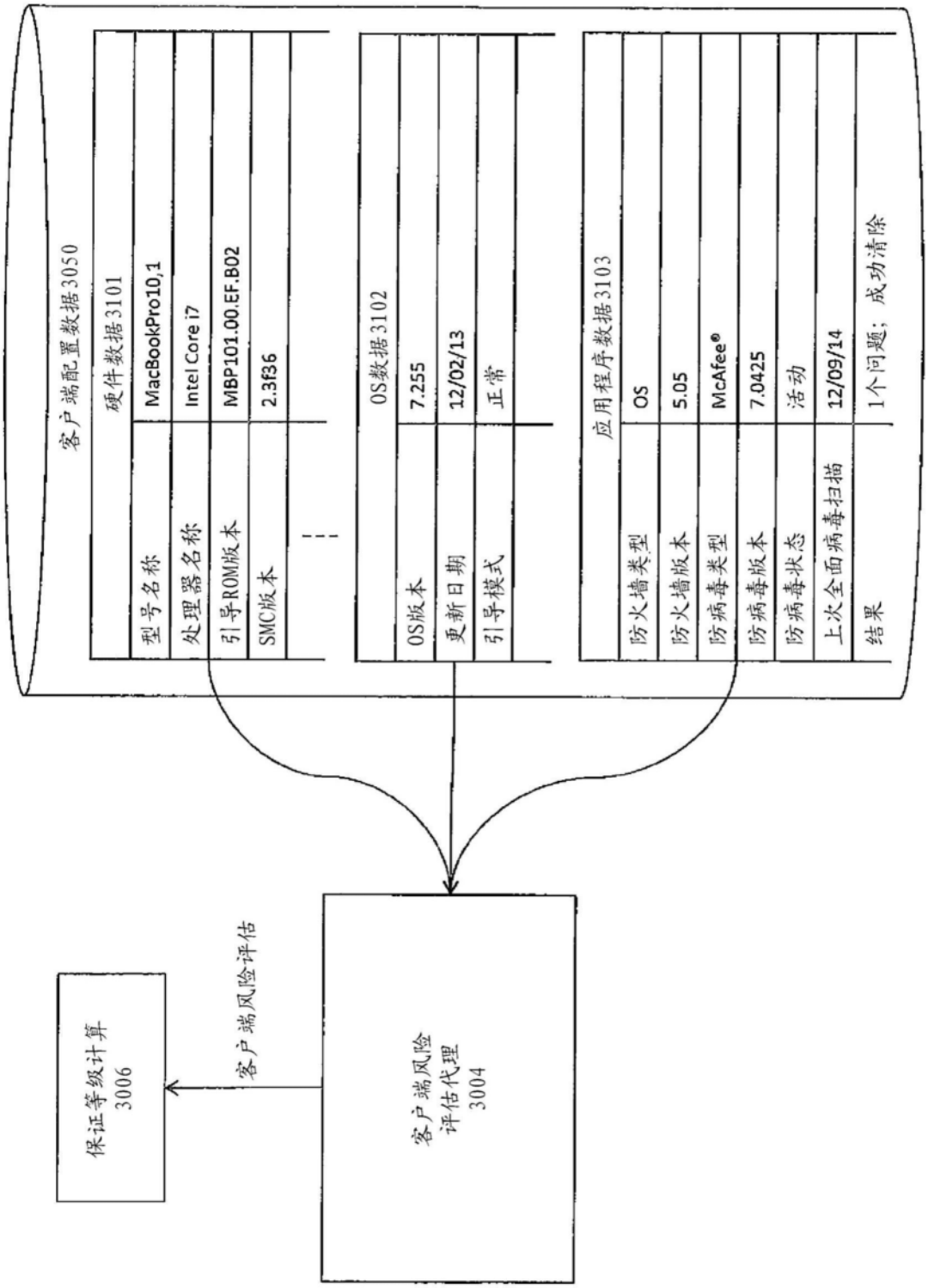

客户端配置数据3050
硬件数据3101
型号名称
MacBookPro10,1
处理器名称
Intel Core i7
引导ROM版本
MBP101.00.EF.B02
SMC版本
2.3f36
OS数据3102
OS版本
7.255
更新日期
12/02/13
引导模式
正常
应用程序数据3103
防火墙类型
OS
防火墙版本
5.05
防病毒类型
McAfee®
防病毒版本
7.0425
防病毒状态
活动
上次全面病毒扫描
12/09/14
结果
1个问题；成功清除
客户端风险评估
3004
客户端风险评估
保证等级计算
3006

图31

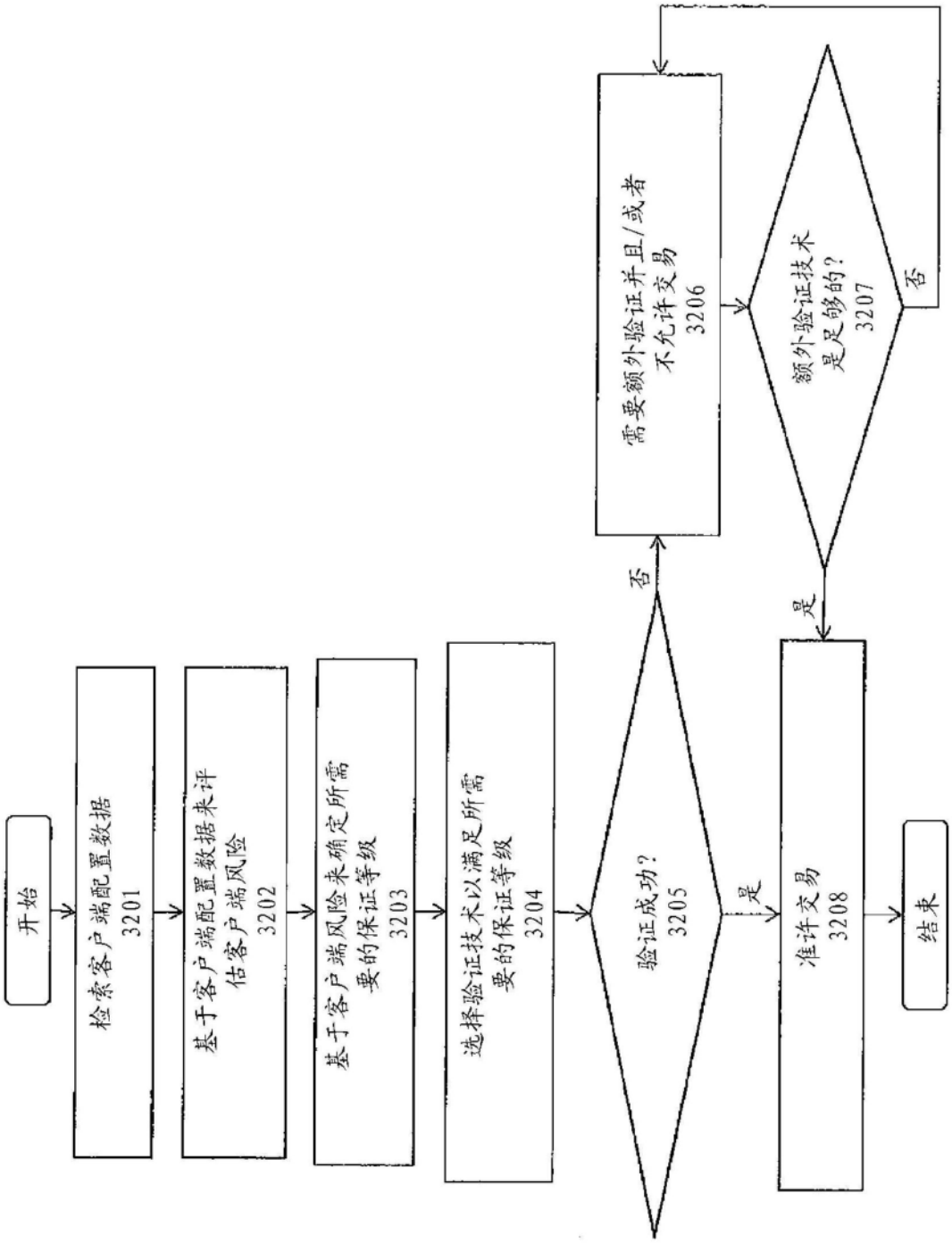

开始
检索客户端配置数据
3201
基于客户端配置数据来评估客户端风险
3202
基于客户端风险来确定所需要的保证等级
3203
选择验证技术以满足所需要的保证等级
3204
验证成功?
3205
否
是
需要额外验证并且/或者不允许交易
3206
额外验证技术是足够的?
3207
否
是
准许交易
3208
结束

图32

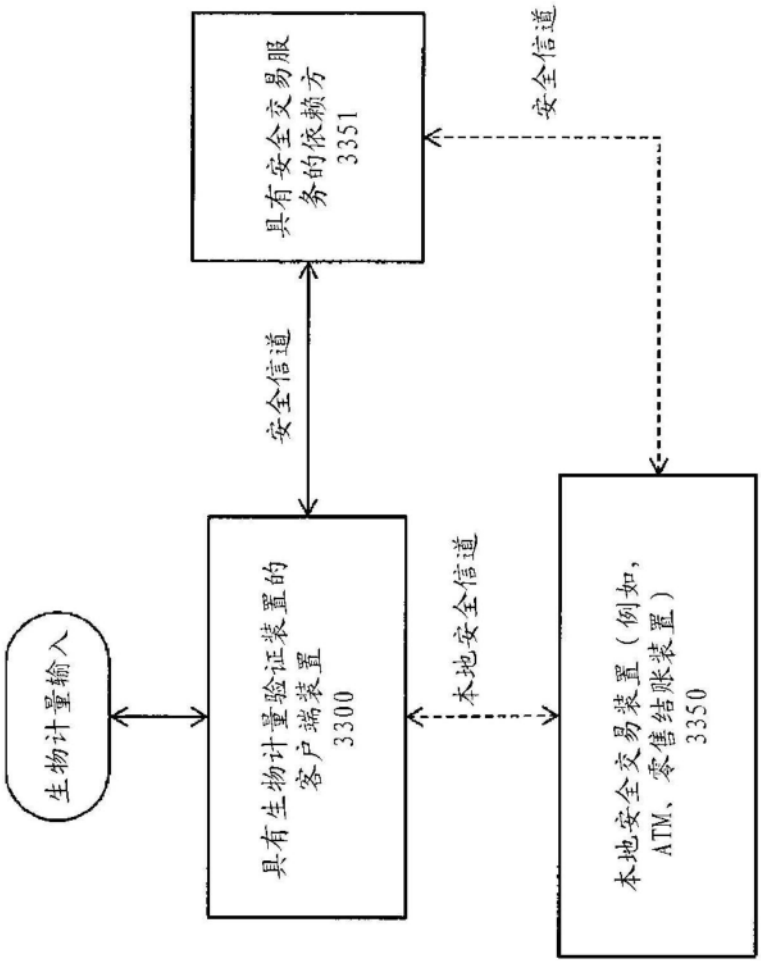

具有安全交易服务的依赖方
3351
安全信道
安全信道
生物计量输入
具有生物计量验证装置的客户端装置
3300
本地安全信道
本地安全交易装置（例如，ATM、零售结账装置）
3350

图33

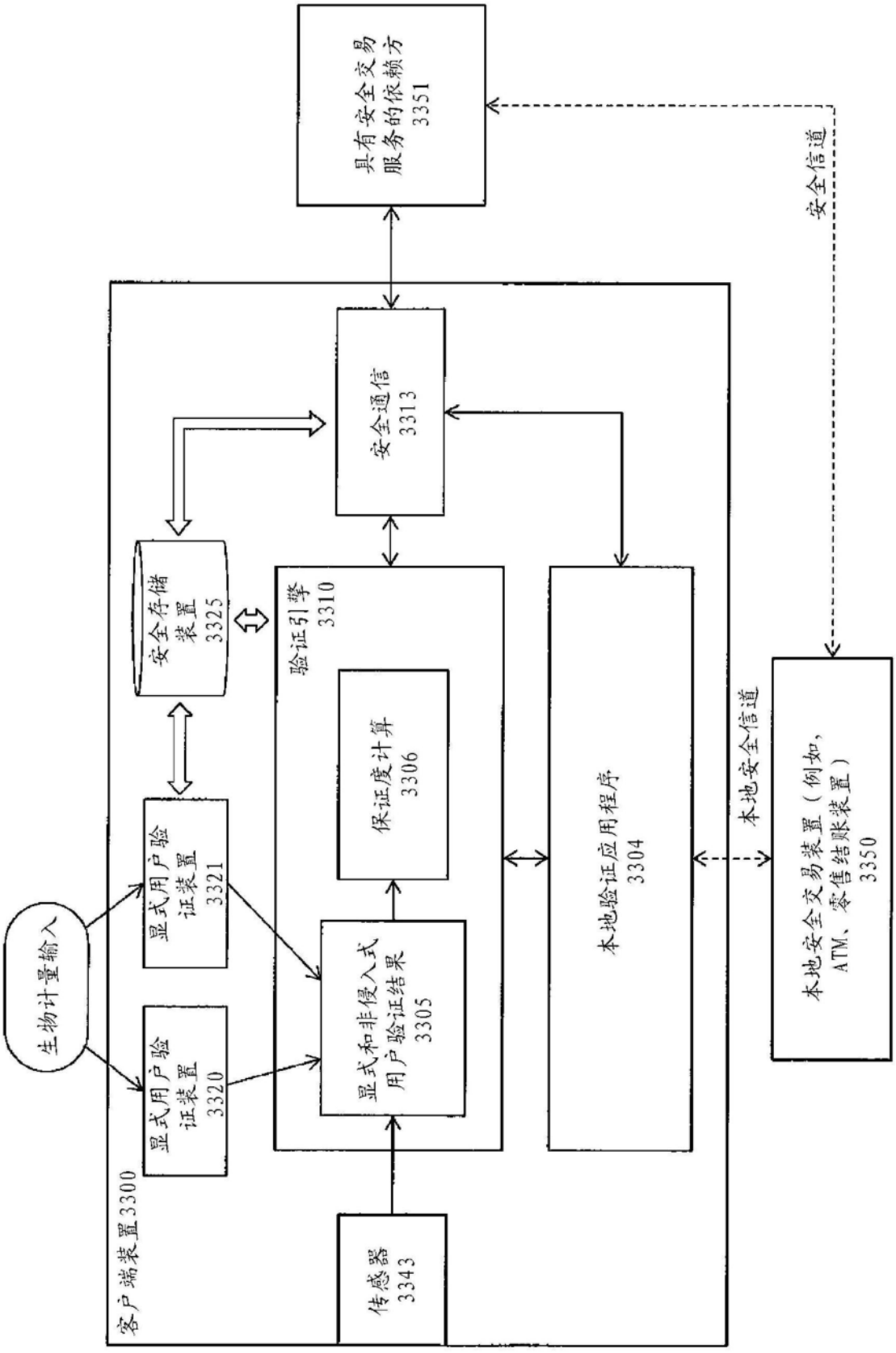

具有安全交易服务的依赖方 3351
安全信道
安全通信 3313
安全存储装置 3325
验证引擎 3310
保证度计算 3306
显式用户验证装置 3321
显式和非侵入式用户验证结果 3305
本地验证应用程序 3304
本地安全信道
本地安全交易装置（例如，ATM、零售结账装置） 3350
生物计量输入
显式用户验证装置 3320
传感器 3343
客户端装置3300

图34

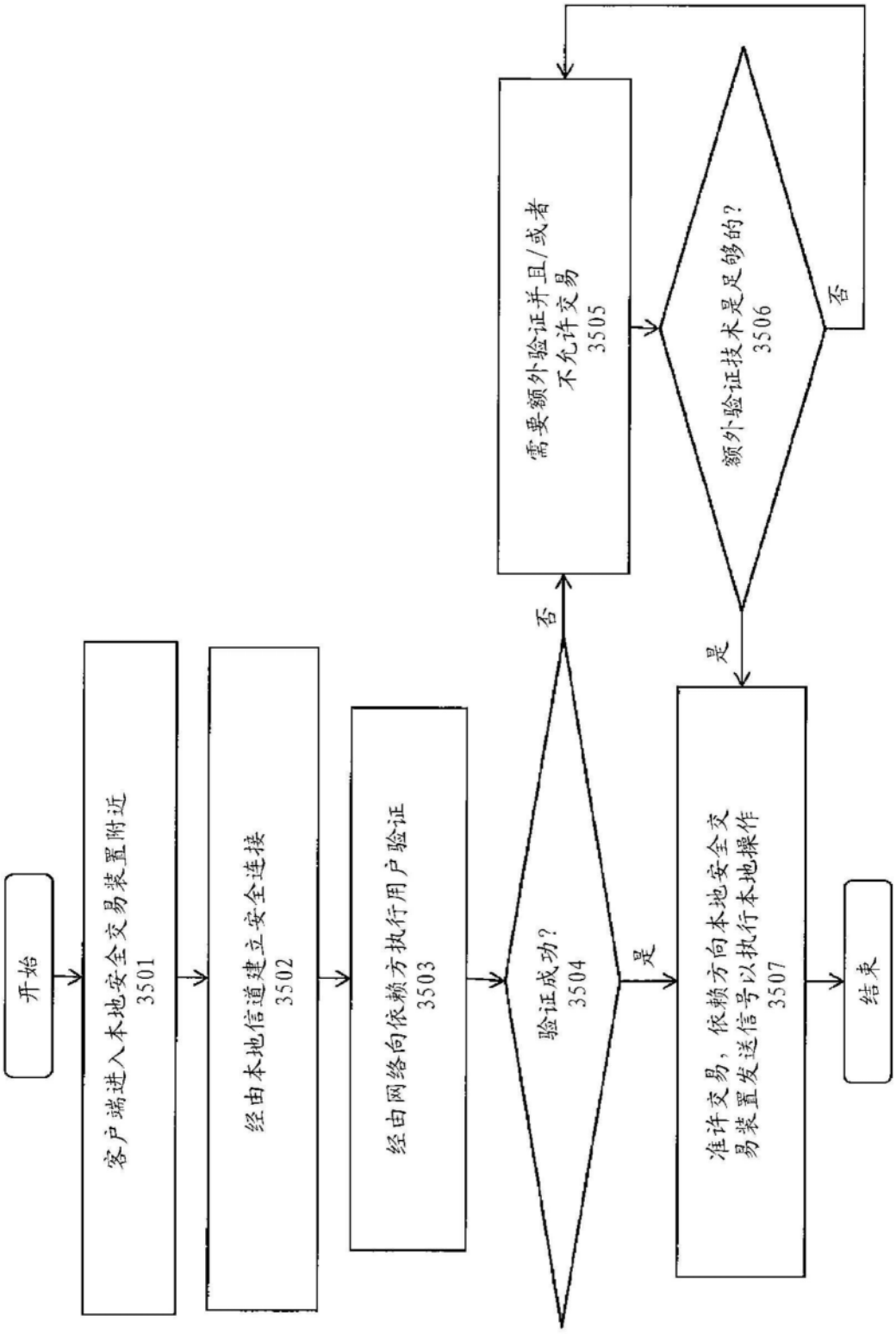

开始
客户端进入本地安全交易装置附近
3501
经由本地信道建立安全连接
3502
经由网络向依赖方执行用户验证
3503
验证成功?
3504
否
是
需要额外验证并且/或者
不允许交易
3505
额外验证技术是足够的?
3506
否
是
准许交易，依赖方向本地安全交
易装置发送信号以执行本地操作
3507
结束

图35

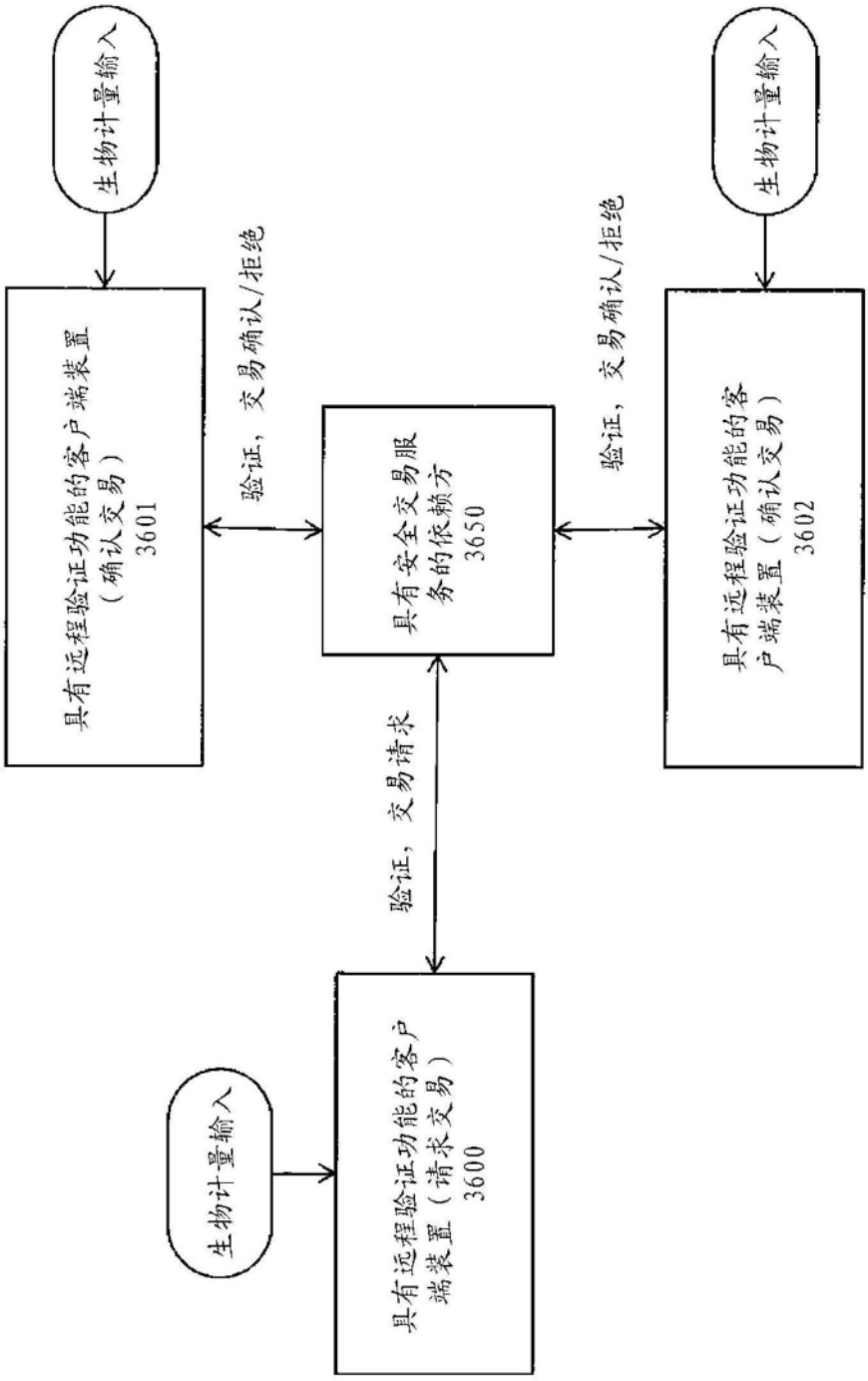

生物计量输入
具有远程验证功能的客户端装置（确认交易）
3601
验证，交易确认/拒绝
具有安全交易服务的依赖方
3650
验证，交易确认/拒绝
生物计量输入
具有远程验证功能的客户端装置（确认交易）
3602
验证，交易请求
生物计量输入
具有远程验证功能的客户端装置（请求交易）
3600

图36

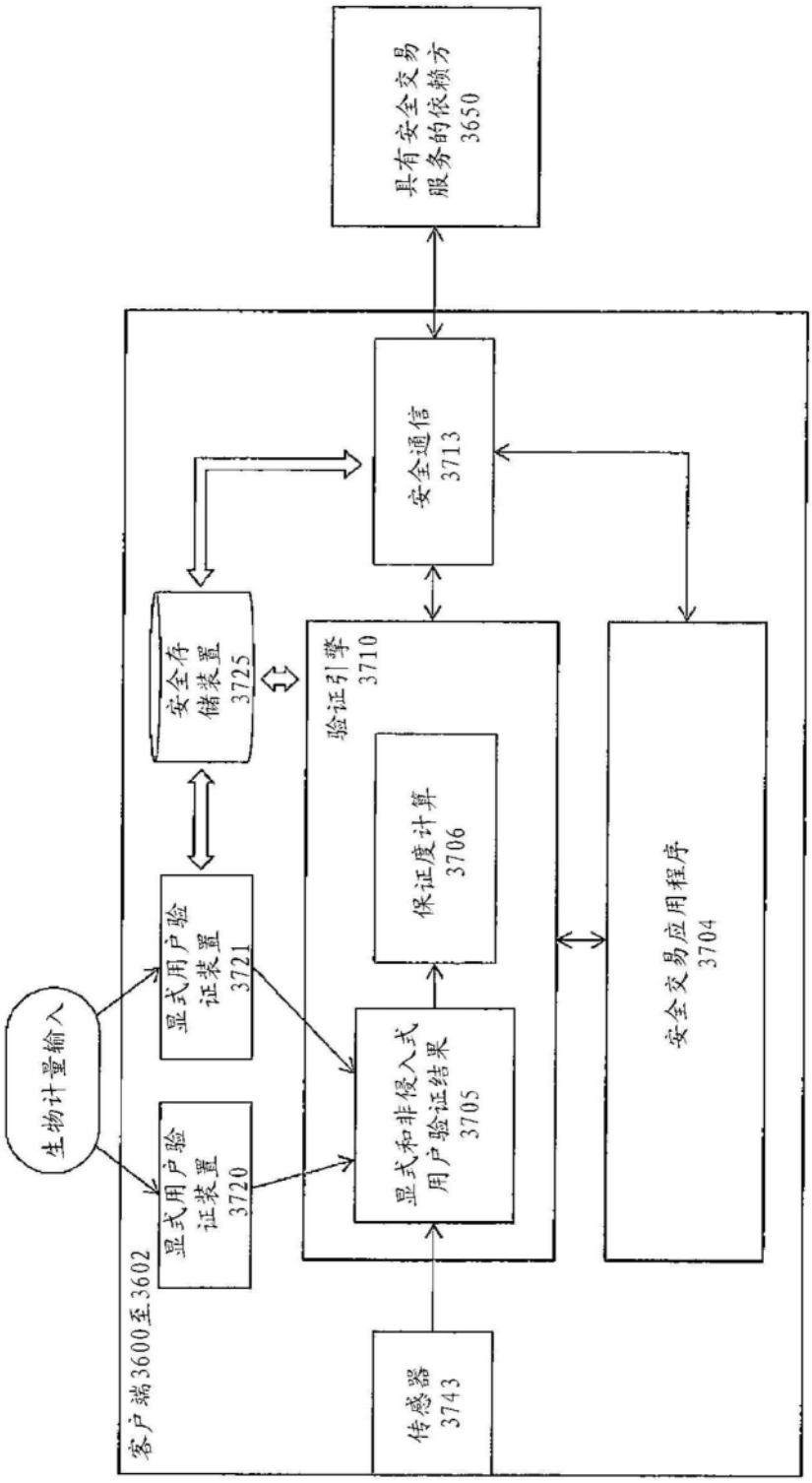

具有安全交易服务的依赖方 3650
安全通信 3713
安全存储装置 3725
验证引擎 3710
保证度计算 3706
显式用户验证装置 3721
显式和非侵入式用户验证结果 3705
安全交易应用程序 3704
生物计量输入
显式用户验证装置 3720
客户端3600至3602
传感器 3743

图37

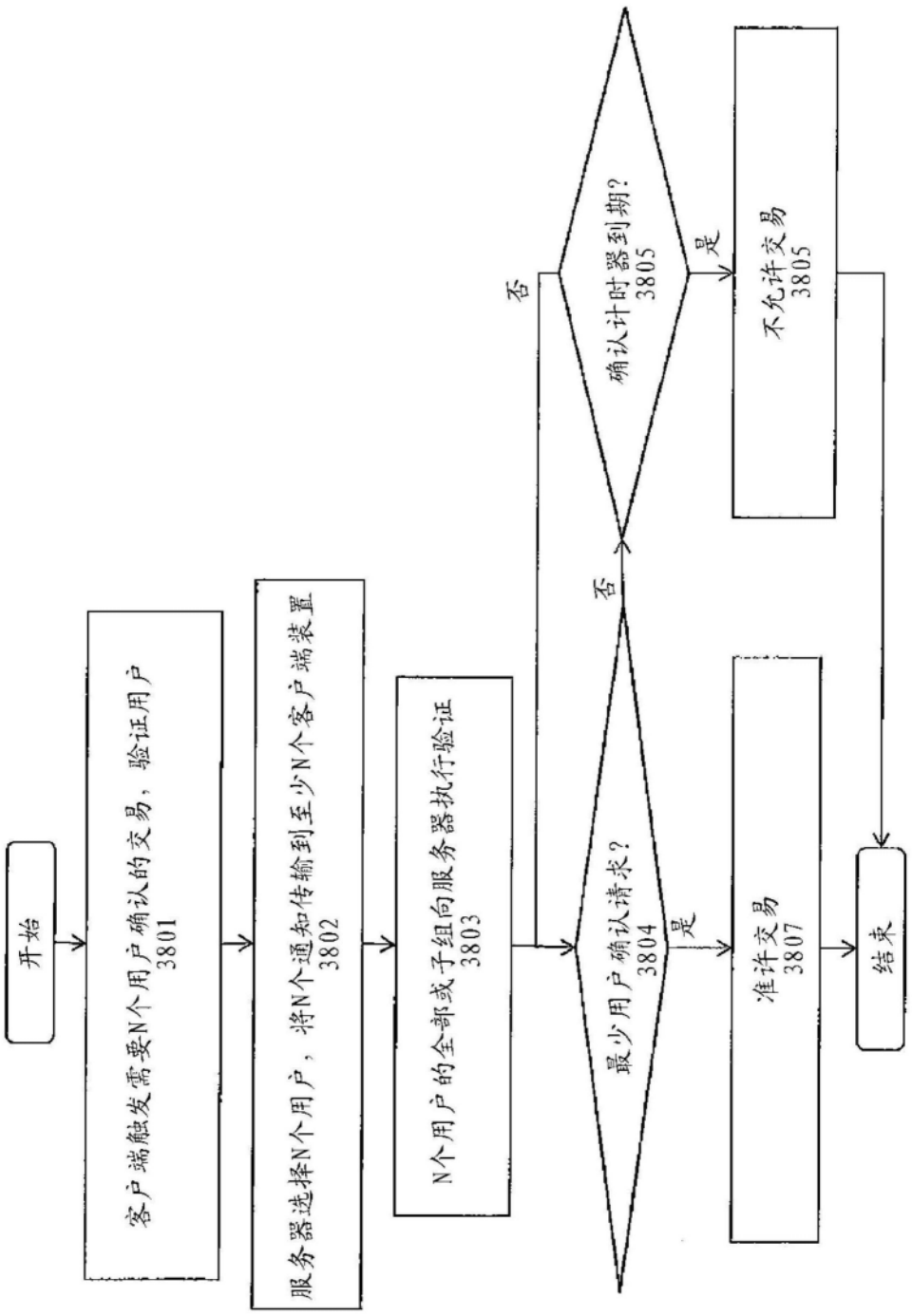

开始
客户端触发需要N个用户确认的交易，验证用户
3801
服务器选择N个用户，将N个通知传输到至少N个客户端装置
3802
N个用户的全部或子组向服务器执行验证
3803
最少用户确认请求?
3804
否
是
确认计时器到期?
3805
否
是
不允许交易
3805
准许交易
3807
结束

图38

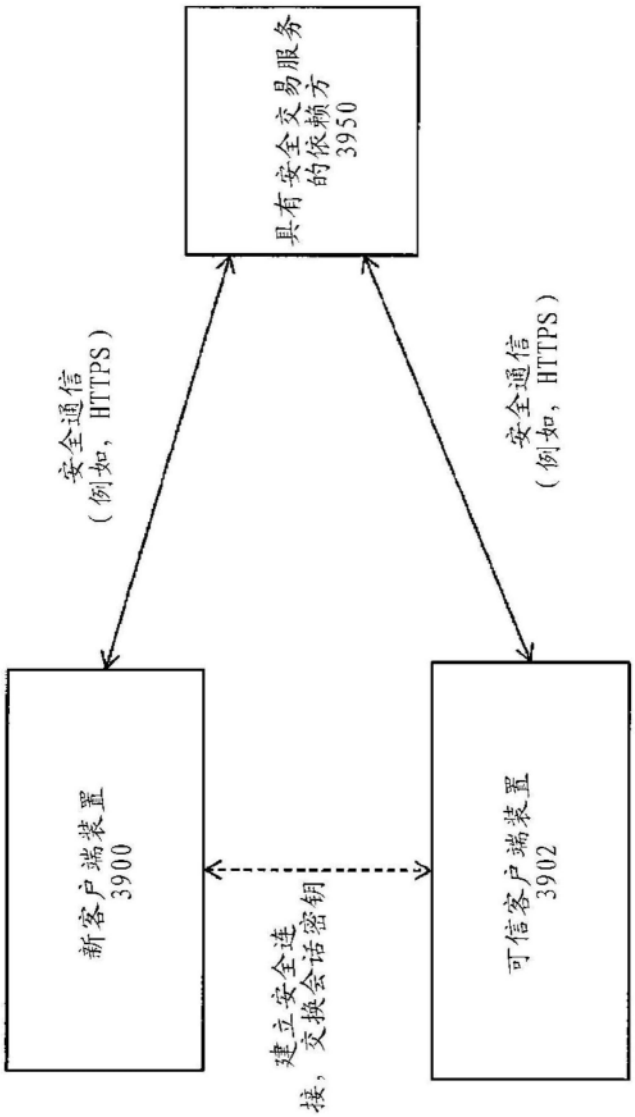

具有安全交易服务的依赖方
3950
安全通信
（例如，HTTPS）
安全通信
（例如，HTTPS）
新客户端装置
3900
可信客户端装置
3902
建立安全连接，交换会话密钥

图39

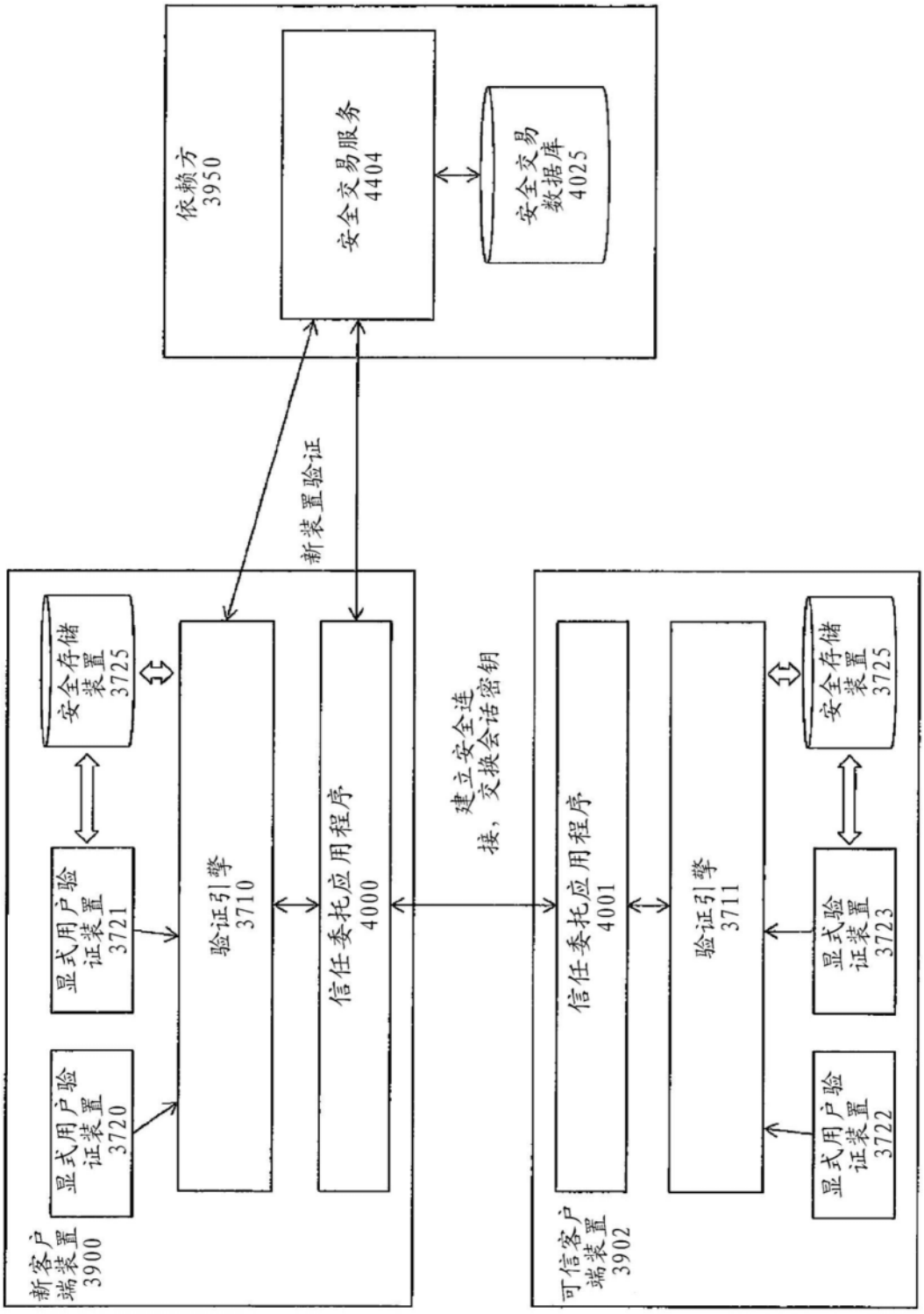

依赖方
3950
安全交易服务
4404
安全交易
数据库
4025
新装置验证
建立安全连
接，交换会话密钥
新客户
端装置
3900
显式用户验
证装置
3720
显式用户验
证装置
3721
安全存储
装置
3725
验证引擎
3710
信任委托应用程序
4000
可信客户
端装置
3902
信任委托应用程序
4001
验证引擎
3711
显式用户验
证装置
3722
显式验
证装置
3723
安全存储
装置
3725

图40

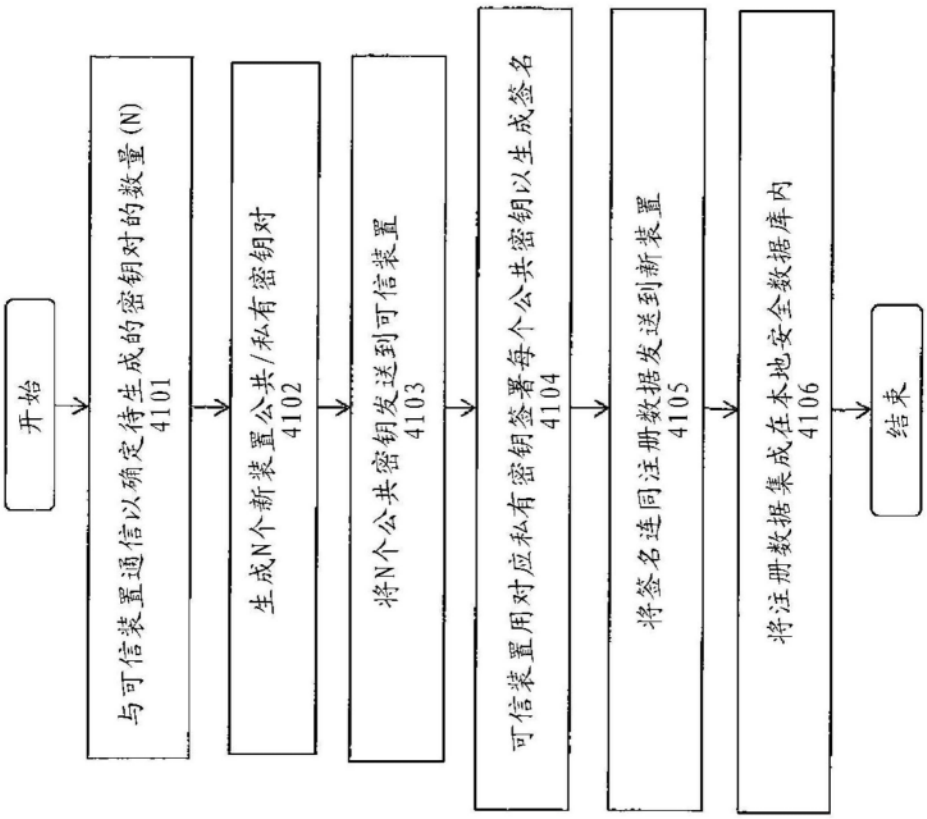

开始
与可信装置通信以确定待生成的密钥对的数量(N)
4101
生成N个新装置公共/私有密钥对
4102
将N个公共密钥发送到可信装置
4103
可信装置用对应私有密钥签署每个公共密钥以生成签名
4104
将签名连同注册数据发送到新装置
4105
将注册数据集成在本地安全数据库内
4106
结束

图41

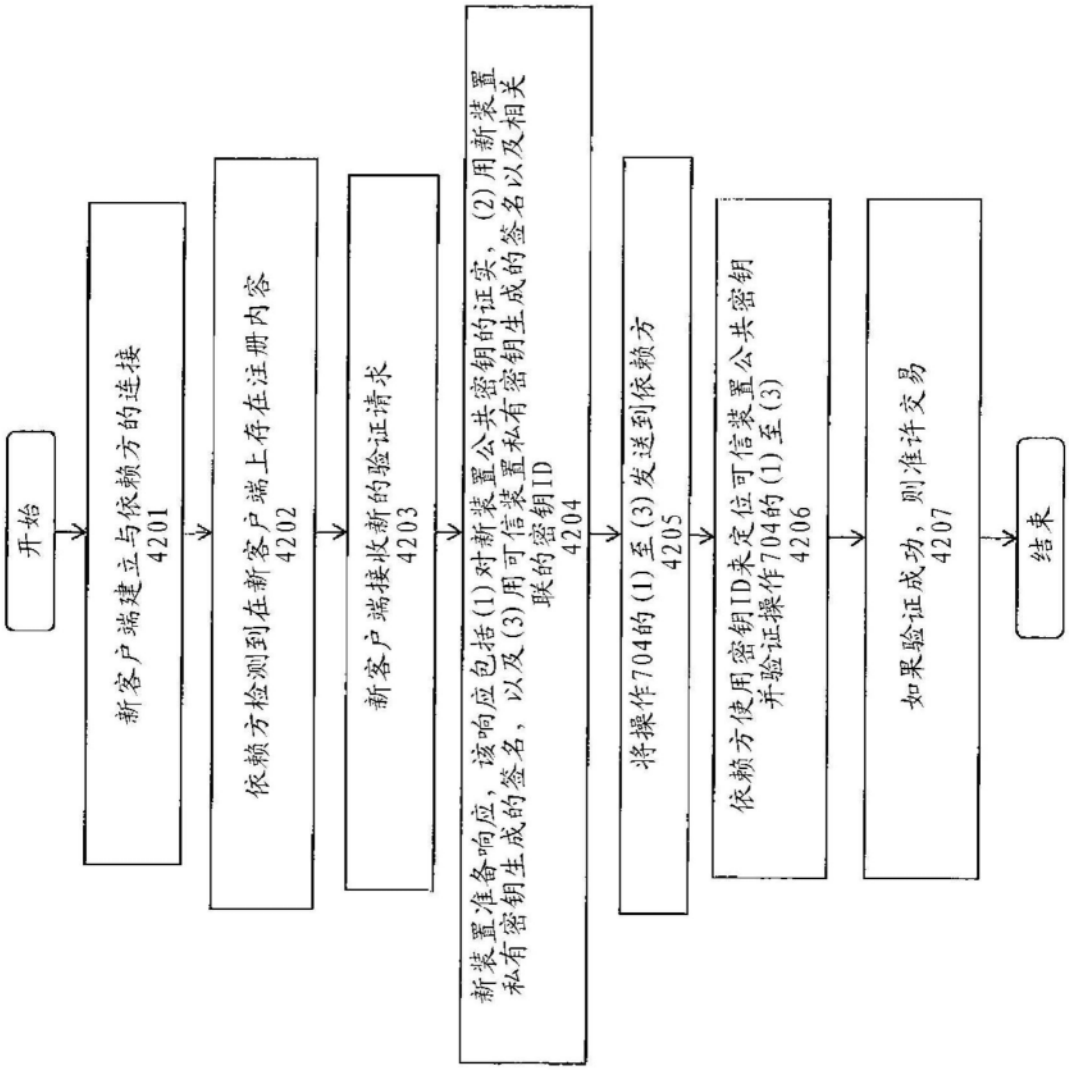

开始
新客户端建立与依赖方的连接
4201
依赖方检测到在新客户端上存在注册内容
4202
新客户端接收新的验证请求
4203
新装置准备响应，该响应包括(1)对新装置公共密钥的证实，(2)用新装置私有密钥生成的签名，以及(3)用可信装置私有密钥生成的签名以及相关联的密钥ID
4204
将操作704的(1)至(3)发送到依赖方
4205
依赖方使用密钥ID来定位可信装置公共密钥并验证操作704的(1)至(3)
4206
如果验证成功，则准许交易
4207
结束

图42

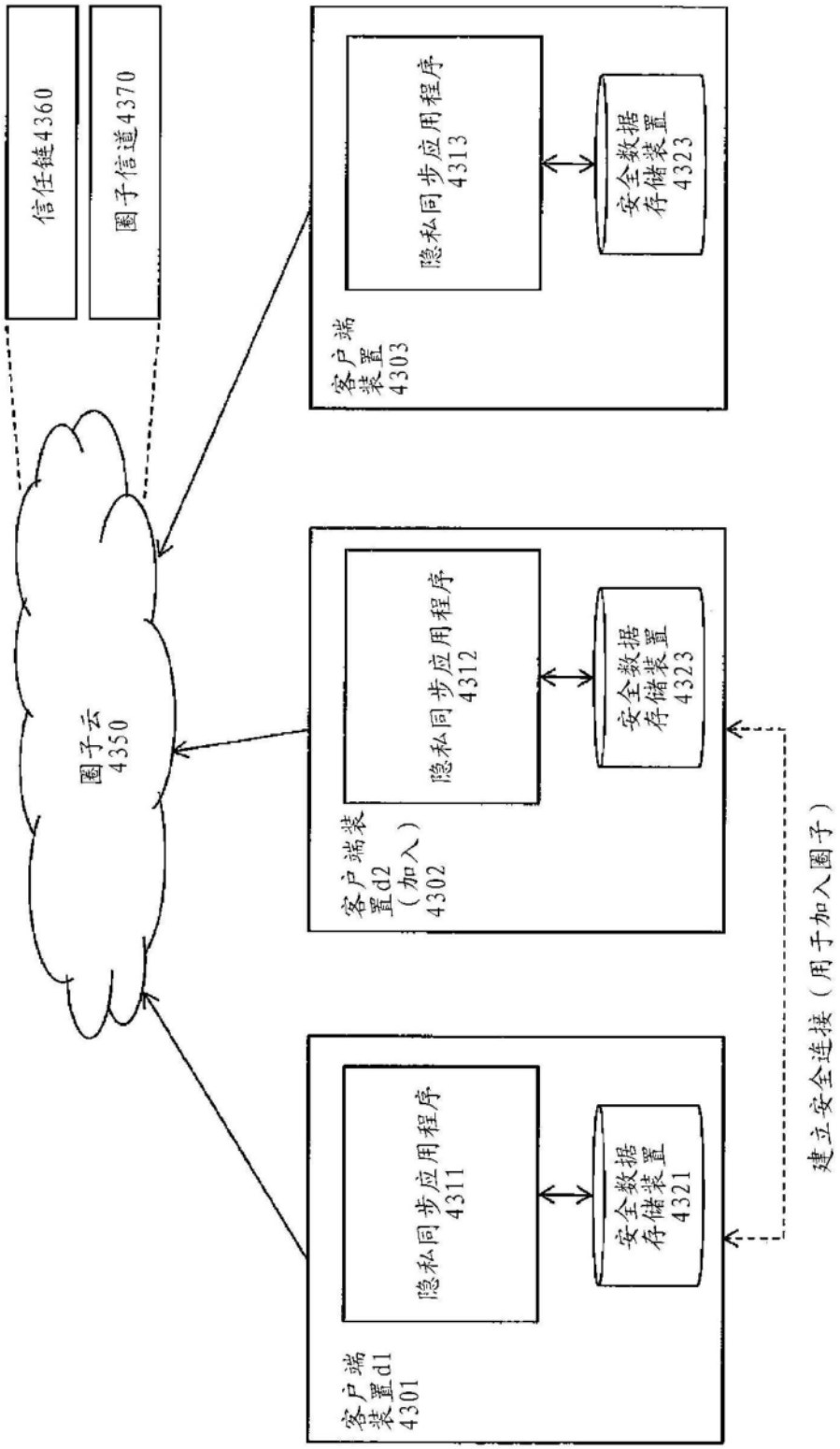

信任链4360
圈子信道4370
圈子云
4350
客户端
装置
4303
隐私同步应用程序
4313
安全数据
存储装置
4323
客户端装
置d2
（加入）
4302
隐私同步应用程序
4312
安全数据
存储装置
4323
客户端
装置d1
4301
隐私同步应用程序
4311
安全数据
存储装置
4321
建立安全连接（用于加入圈子）

图43

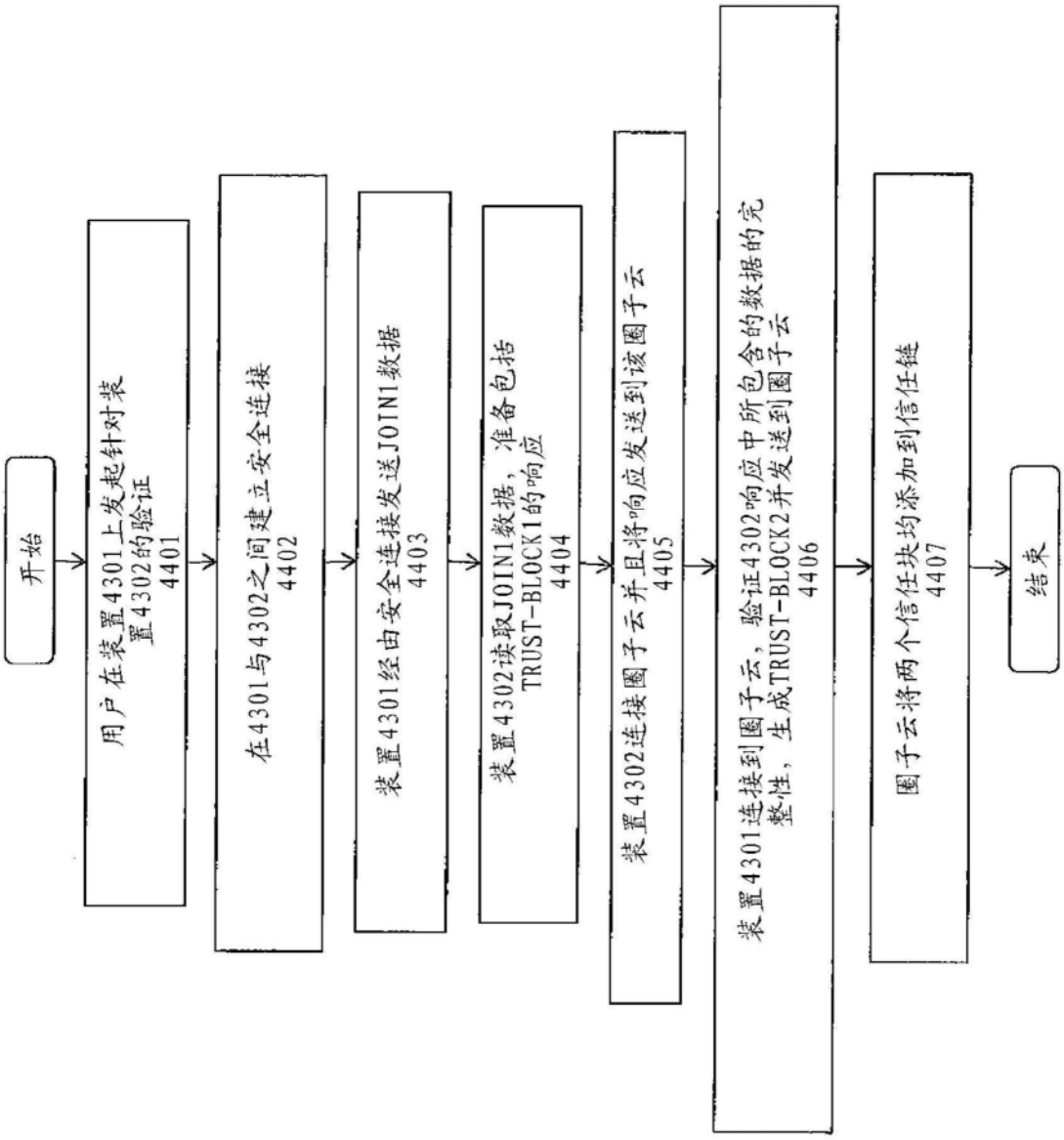

开始
用户在装置4301上发起针对装置4302的验证
4401
在4301与4302之间建立安全连接
4402
装置4301经由安全连接发送JOIN1数据
4403
装置4302读取JOIN1数据，准备包括TRUST-BLOCK1的响应
4404
装置4302连接圈子云并且将响应发送到该圈子云
4405
装置4301连接到圈子云，验证4302响应中所包含的数据的完整性，生成TRUST-BLOCK2并发送到圈子云
4406
圈子云将两个信任块均添加到信任链
4407
结束

图44

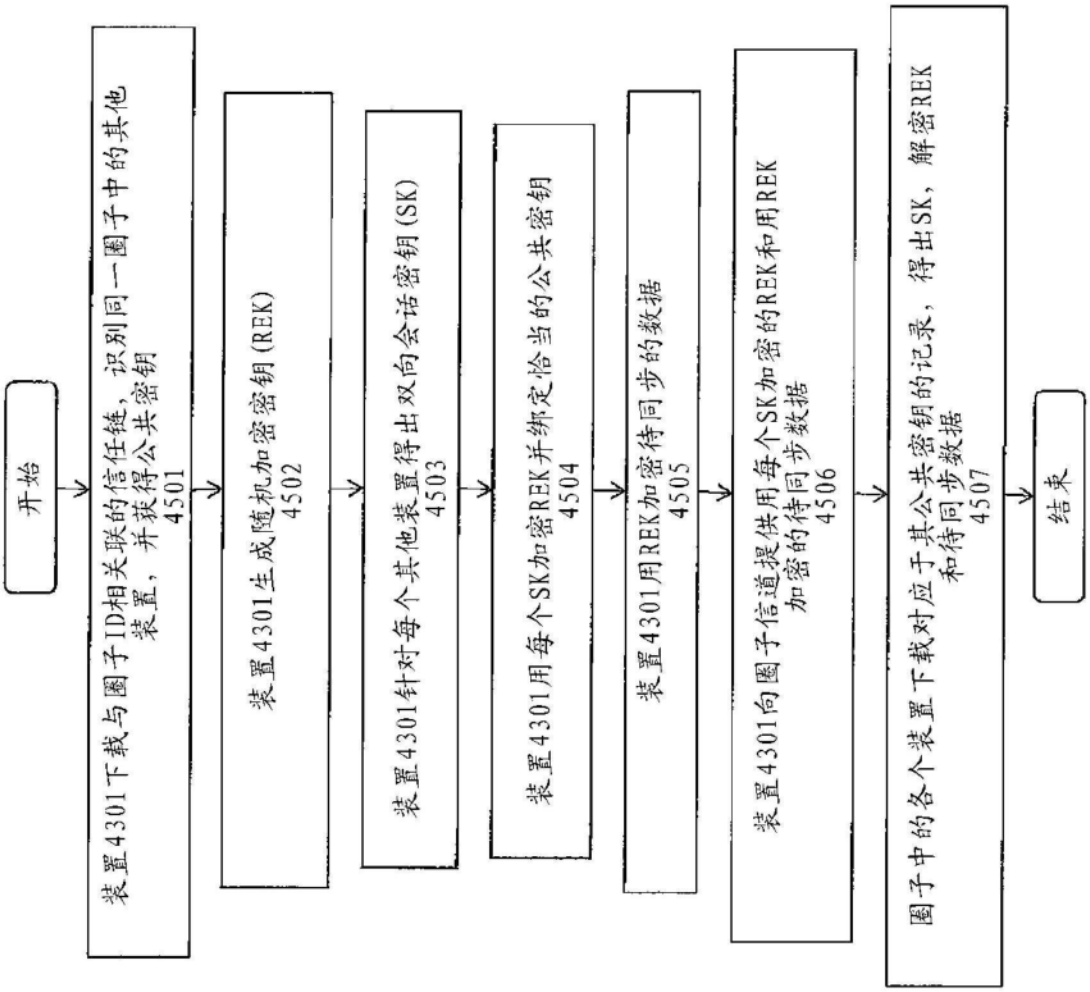

开始
装置4301下载与圈子ID相关联的信任链，识别同一圈子中的其他装置，并获得公共密钥
4501
装置4301生成随机加密密钥(REK)
4502
装置4301针对每个其他装置得出双向会话密钥(SK)
4503
装置4301用每个SK加密REK并绑定恰当的公共密钥
4504
装置4301用REK加密待同步的数据
4505
装置4301向圈子信道提供用每个SK加密的REK和用REK加密的待同步数据
4506
圈子中的各个装置下载对应于其公共密钥的记录，得出SK，解密REK和待同步数据
4507
结束

图45

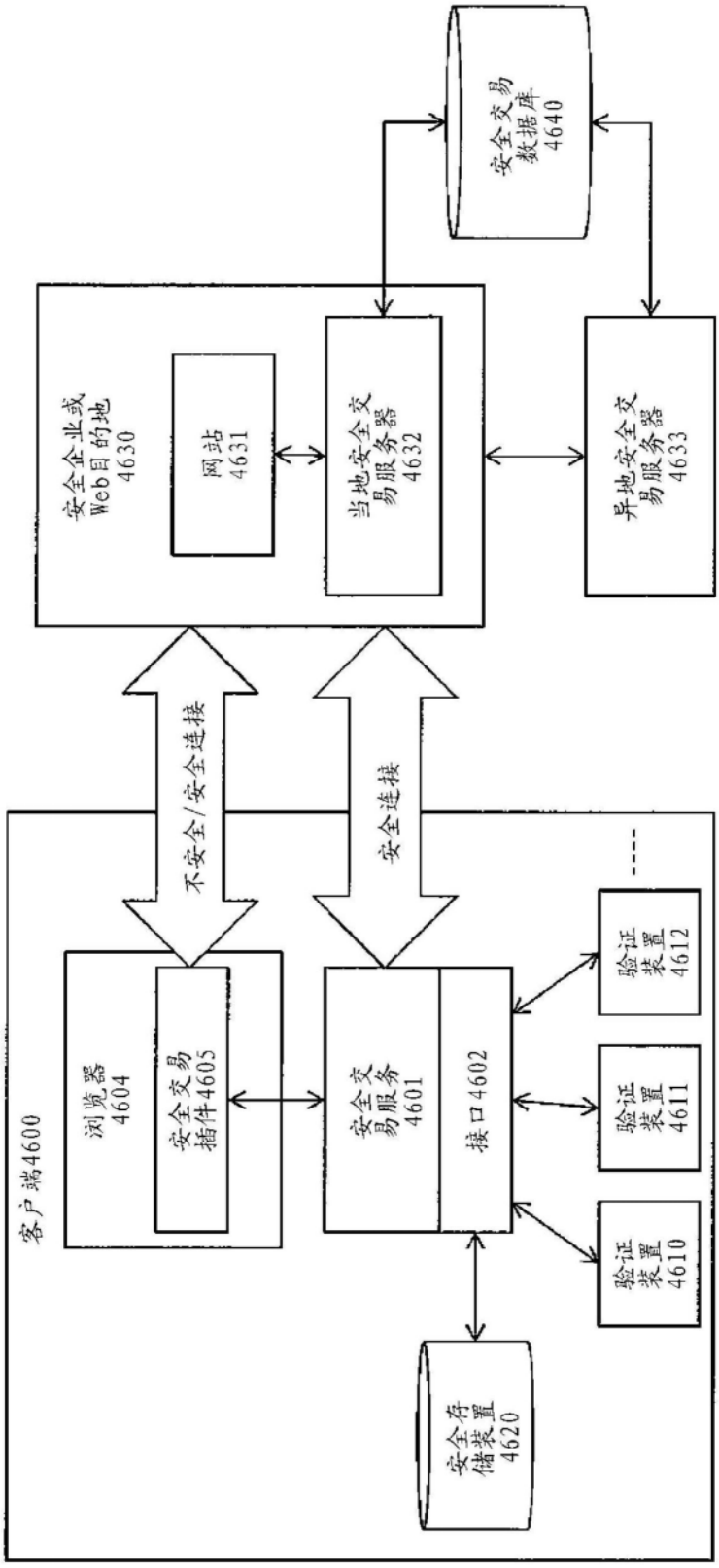

安全交易数据库4640
安全企业或Web目的地4630
网站4631
当地安全交易服务器4632
异地安全交易服务器4633
不安全/安全连接
安全连接
客户端4600
浏览器4604
安全交易插件4605
安全交易服务4601
接口4602
验证装置4612
验证装置4611
验证装置4610
安全存储装置4620

图46A

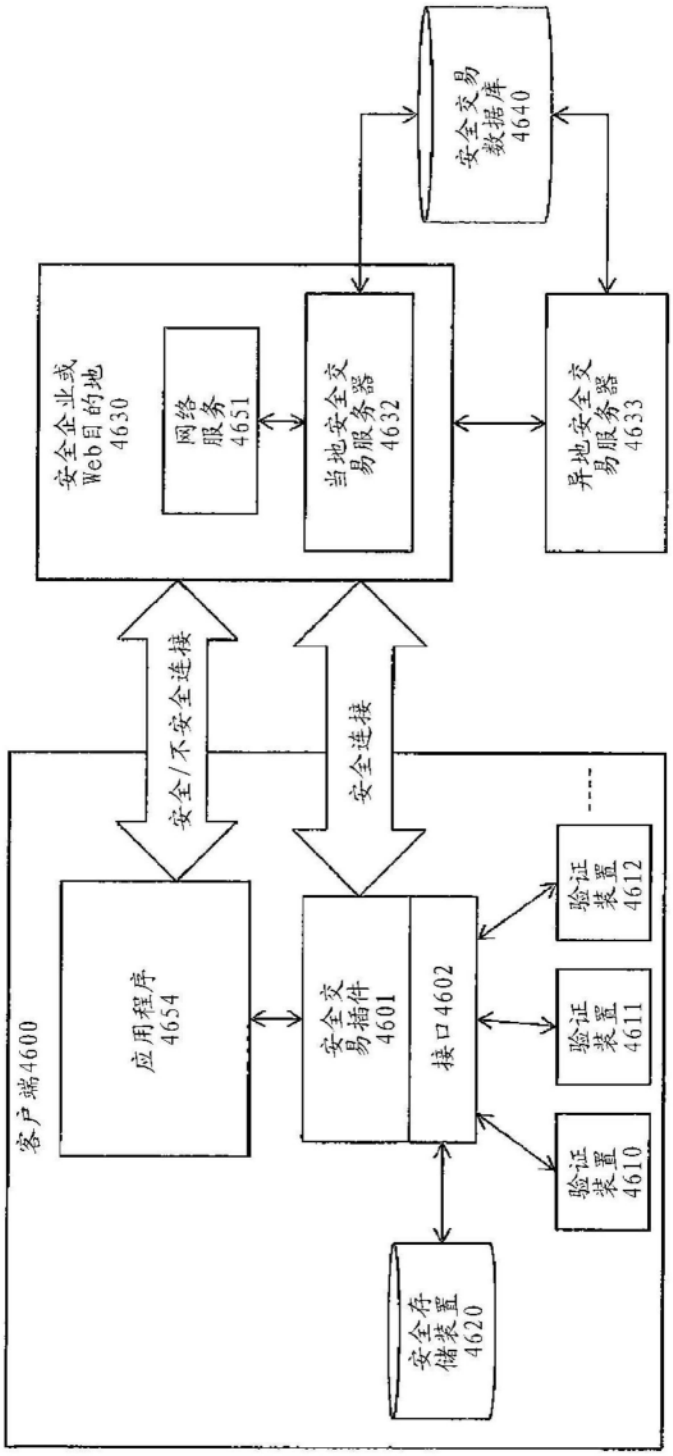

安全交易数据库 4640
安全企业或Web目的地 4630
网络服务 4651
当地安全交易服务器 4632
异地安全交易服务器 4633
安全/不安全连接
安全连接
客户端4600
应用程序 4654
安全交易插件 4601
接口 4602
验证装置 4612
验证装置 4611
验证装置 4610
安全存储装置 4620

图46B

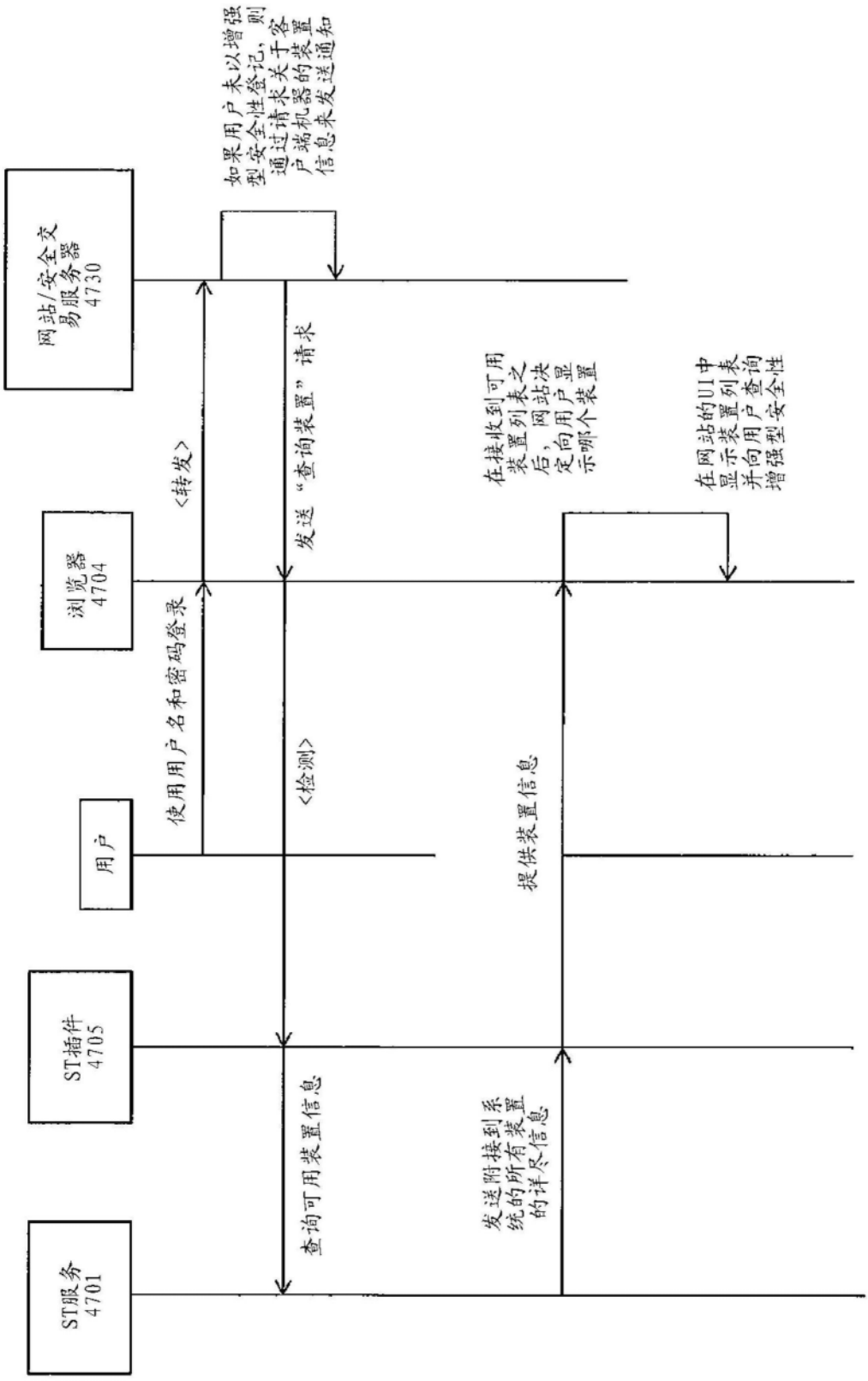

网站/安全交易服务器 4730
浏览器 4704
用户
ST插件 4705
ST服务 4701
如果用户未以增强型安全性登记，则通过请求关于客户端机器的装置信息来发送通知
<转发>
发送“查询装置”请求
使用用户名和密码登录
<检测>
在接收到可用装置列表之后，网站决定向用户显示哪个装置
在网站的UI中显示装置列表并向用户查询增强型安全性
提供装置信息
查询可用装置信息
发送附接到系统的所有装置的详尽信息

图47

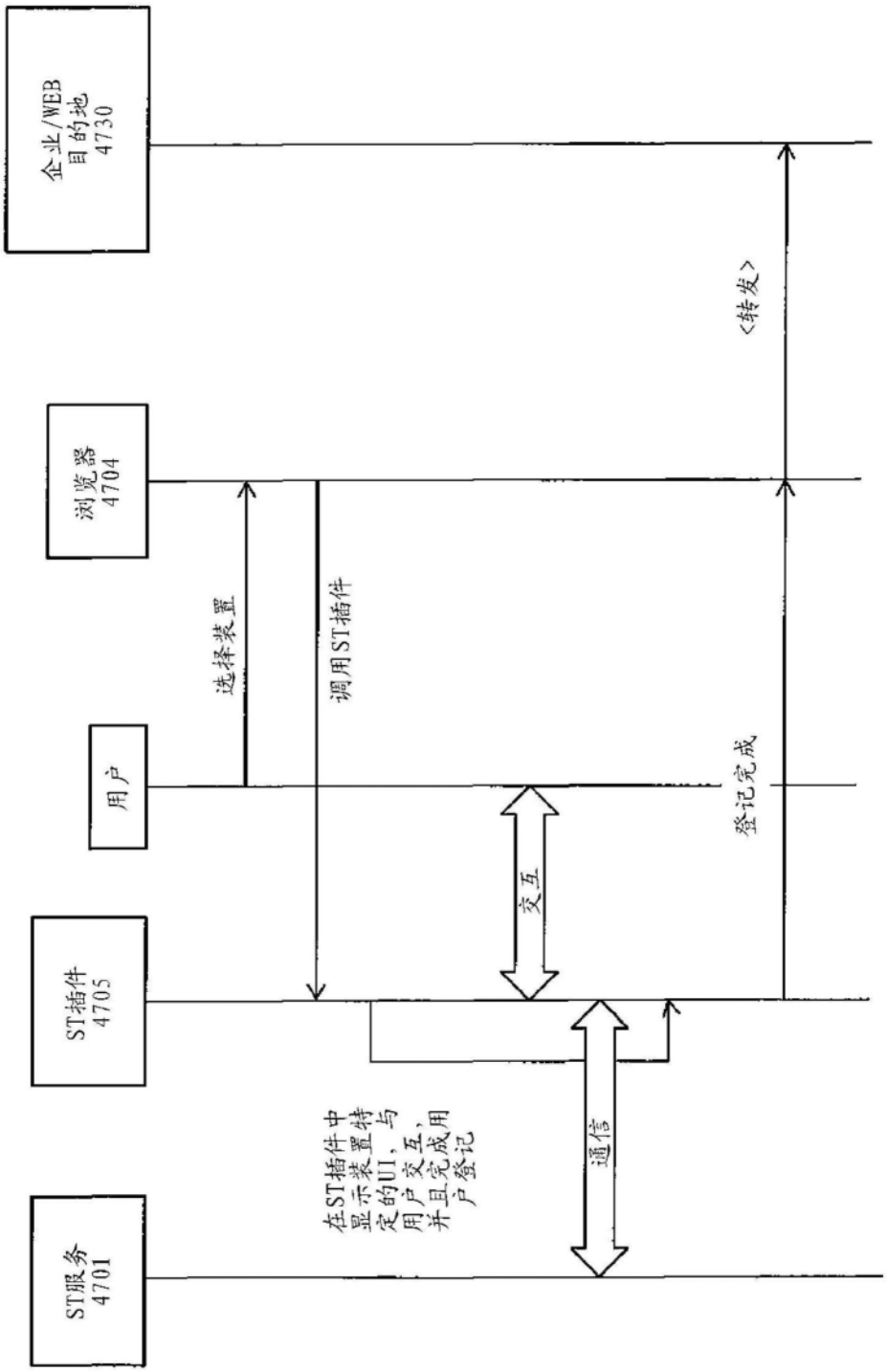

企业/WEB
目的地
4730
浏览器
4704
用户
ST插件
4705
ST服务
4701
选择装置
调用ST插件
交互
登记完成
<转发>
通信
在ST插件中
显示装置特
定的UI，与
用户交互，
并且完成用
户登记

图48

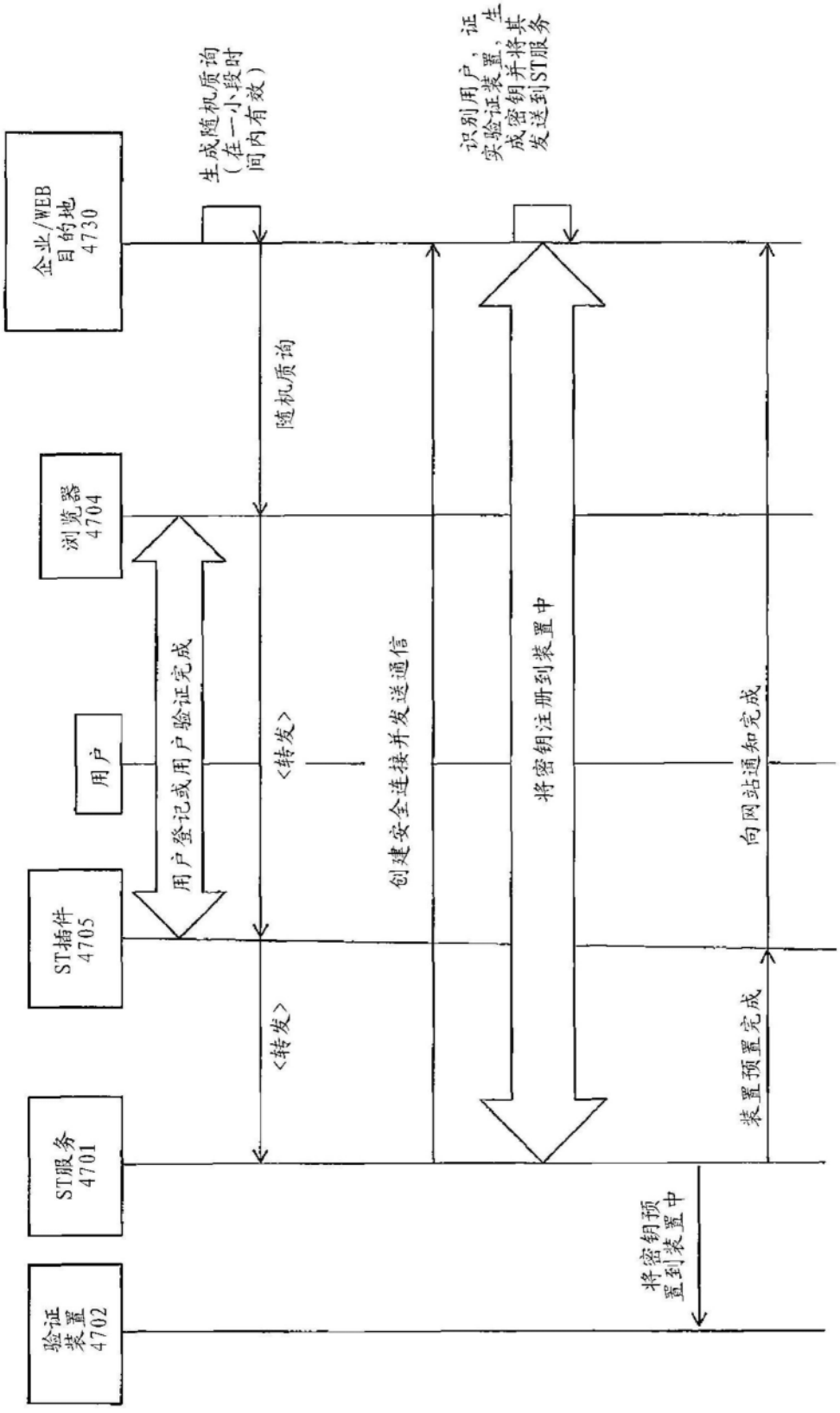

企业/WEB
目的地
4730
浏览器
4704
用户
ST插件
4705
ST服务
4701
验证
装置
4702
生成随机质询
（在一小段时
间内有效）
随机质询
识别用户，证
实验证装置，生
成密钥并将其
发送到ST服务
用户登记或用户验证完成
<转发>
创建安全连接并发送通信
将密钥注册到装置中
向网站通知完成
<转发>
装置预置完成
将密钥预
置到装置中

图49

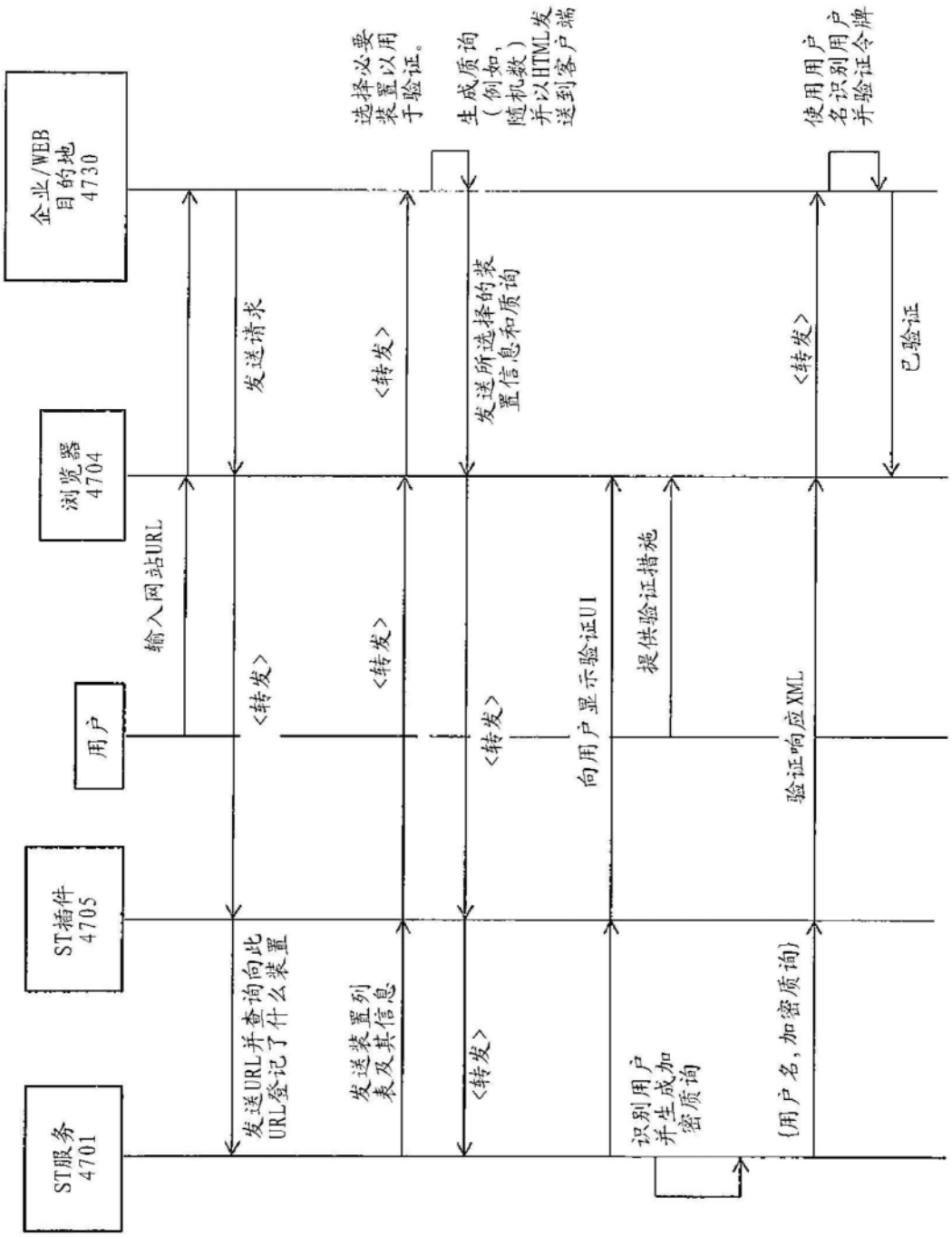

企业/WEB
目的地
4730
浏览器
4704
用户
ST插件
4705
ST服务
4701
输入网站URL
发送请求
选择必要
装置以用
于验证。
生成质询
(例如,
随机数)
并以HTML发
送到客户端
使用用户
名识别用户
并验证令牌
<转发>
发送所选择的装
置信息和质询
已验证
提供验证措施
向用户显示验证UI
验证响应XML
发送URL并查询向此
URL登记了什么装置
发送装置列
表及其信息
识别用户
并生成加
密质询
{用户名,加密质询}

图50

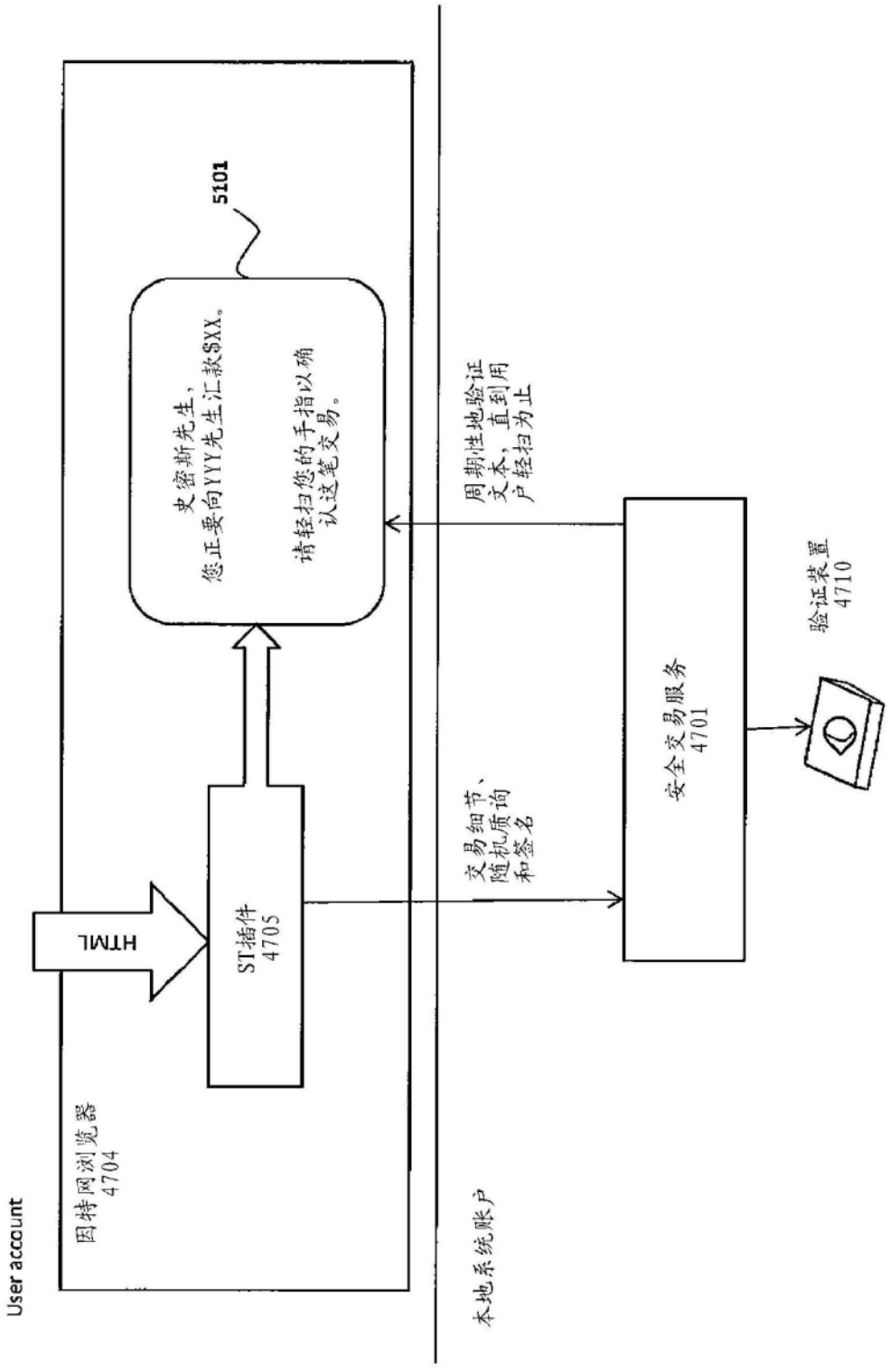

User account
本地系统账户
因特网浏览器
4704
HTML
ST插件
4705
交易细节、
随机质询
和签名
安全交易服务
4701
周期性地验证
文本，直到用
户轻扫为止
验证装置
4710
5101
史密斯先生，
您正要向YYY先生汇款$XX。
请轻扫您的手指以确
认这笔交易。

图51

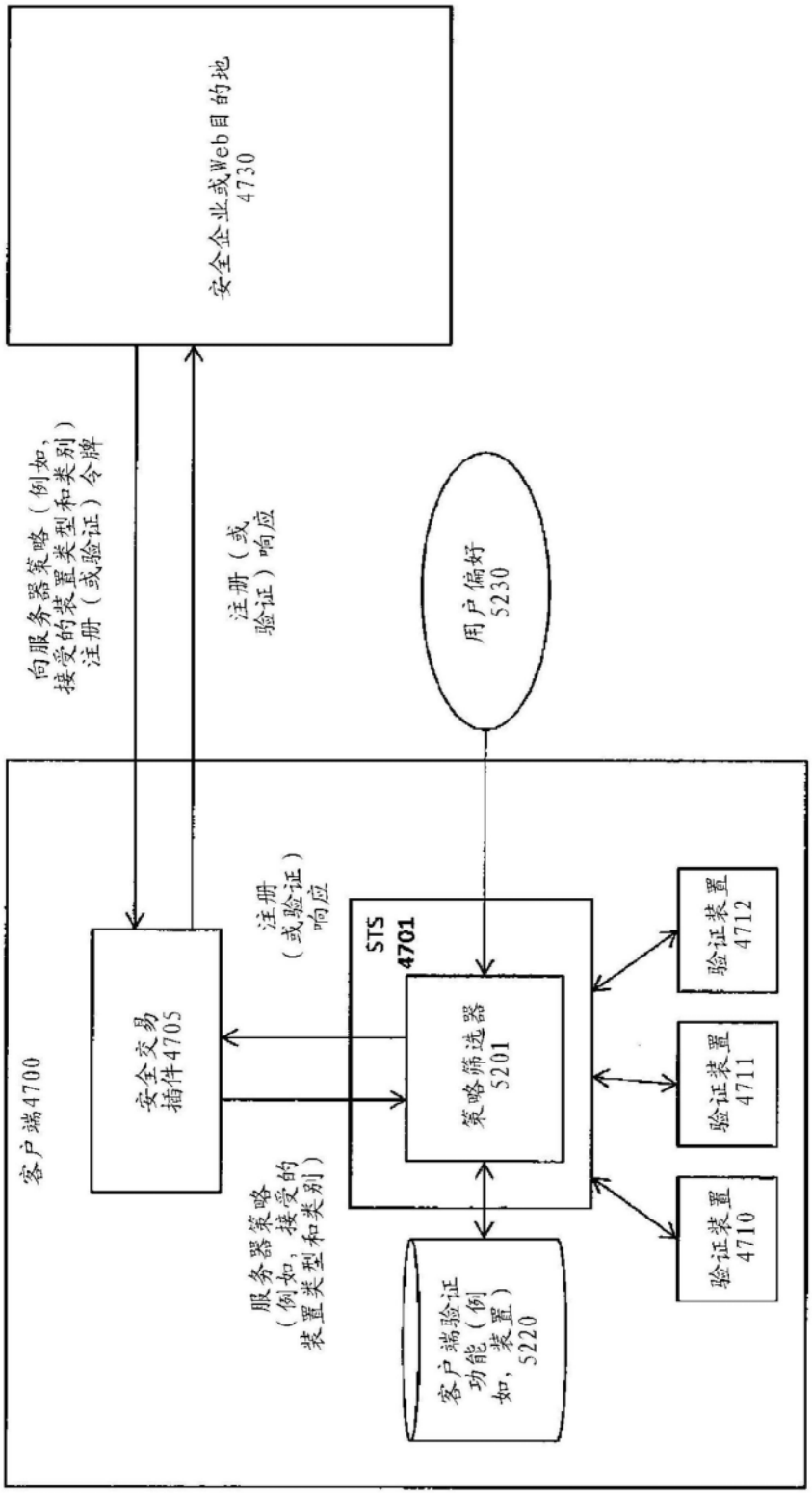

安全企业或Web目的地
4730
向服务器策略（例如，
接受的装置类型和类别）
注册（或验证）令牌
注册（或
验证）响应
用户偏好
5230
客户端4700
安全交易
插件4705
注册
（或验证）
响应
STS
4701
策略筛选器
5201
验证装置
4712
验证装置
4711
验证装置
4710
服务器策略
（例如，接受的
装置类型和类别）
客户端验证
功能（例
如，装置）
5220

图52

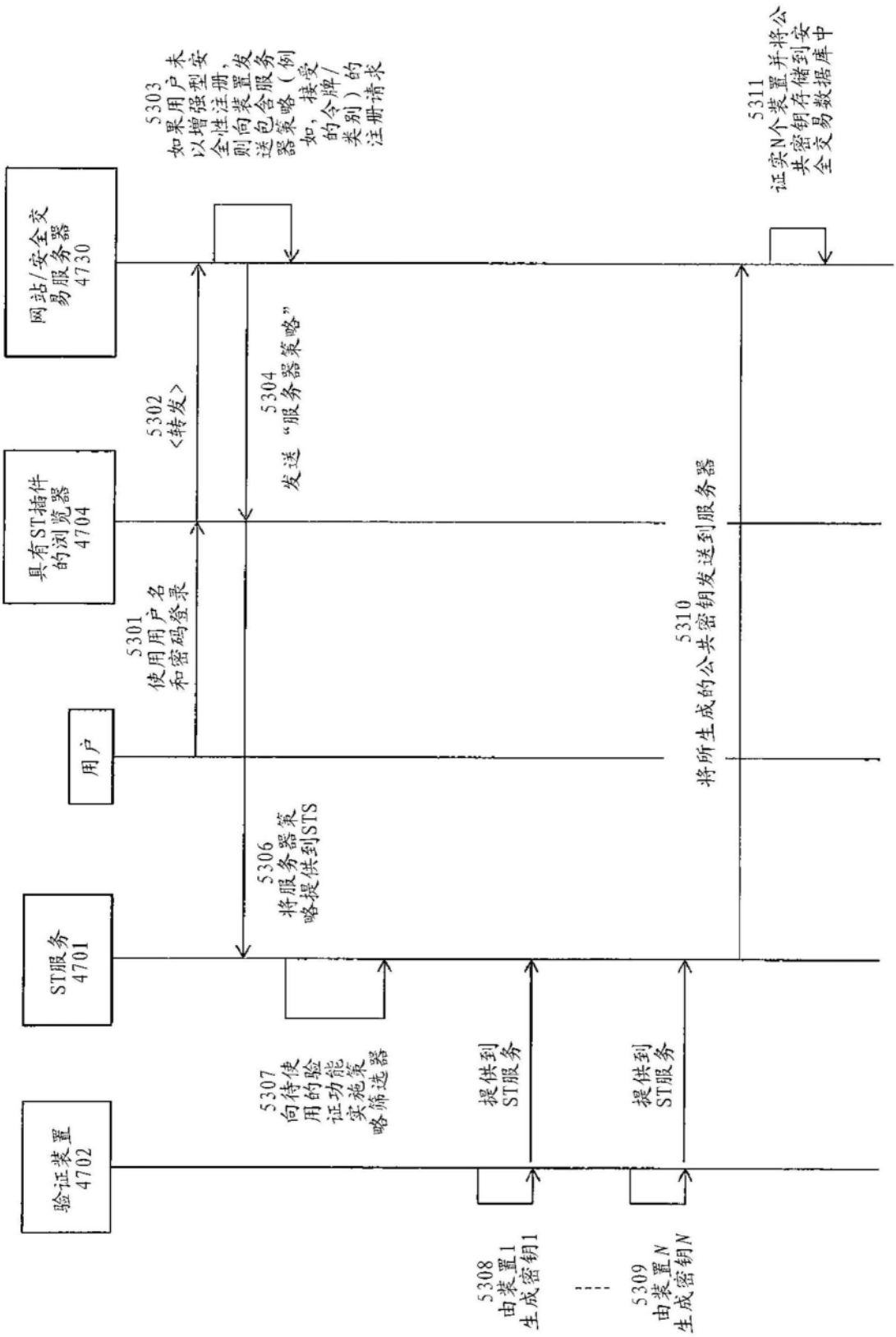

网站/安全交易服务器 4730
具有ST插件的浏览器 4704
用户
ST服务 4701
验证装置 4702
5301 使用用户名和密码登录
5302 <转发>
5303 如果用户未以增强型安全性注册，则向装置发送包含服务器策略（例如，接受的令牌/类别）的注册请求
5304 发送“服务器策略”
5306 将服务器策略提供到STS
5307 向待使用的验证功能实施策略筛选器
5308 由装置1生成密钥1
5309 由装置N生成密钥N
提供到ST服务
提供到ST服务
5310 将所生成的公共密钥发送到服务器
5311 证实N个装置并将公共密钥存储到安全交易数据库中

图53

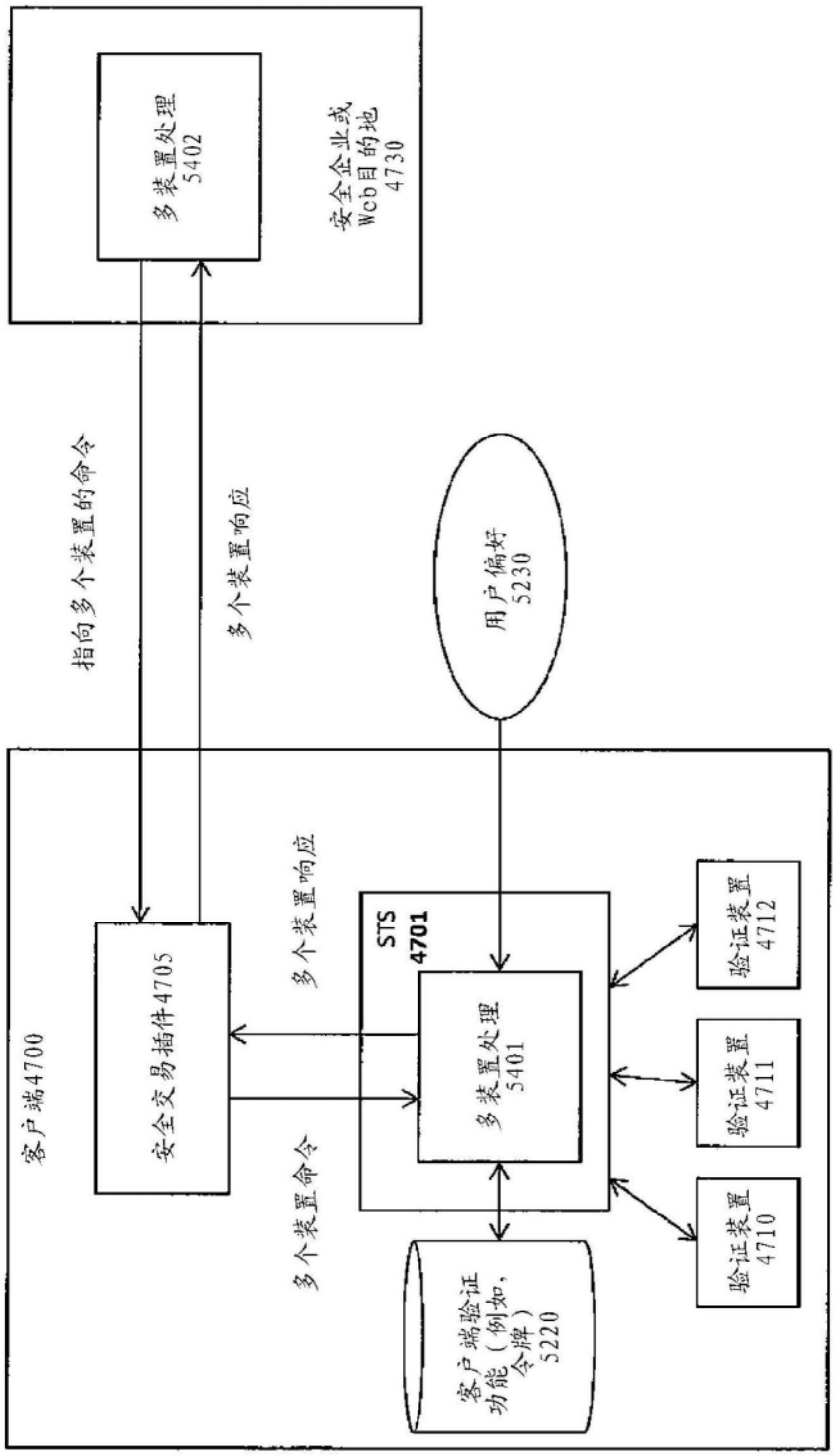

多装置处理
5402
安全企业或
Web目的地
4730
指向多个装置的命令
多个装置响应
用户偏好
5230
客户端4700
安全交易插件4705
多个装置响应
STS
4701
多装置处理
5401
验证装置
4712
验证装置
4711
验证装置
4710
多个装置命令
客户端验证
功能（例如，
令牌）
5220

图54

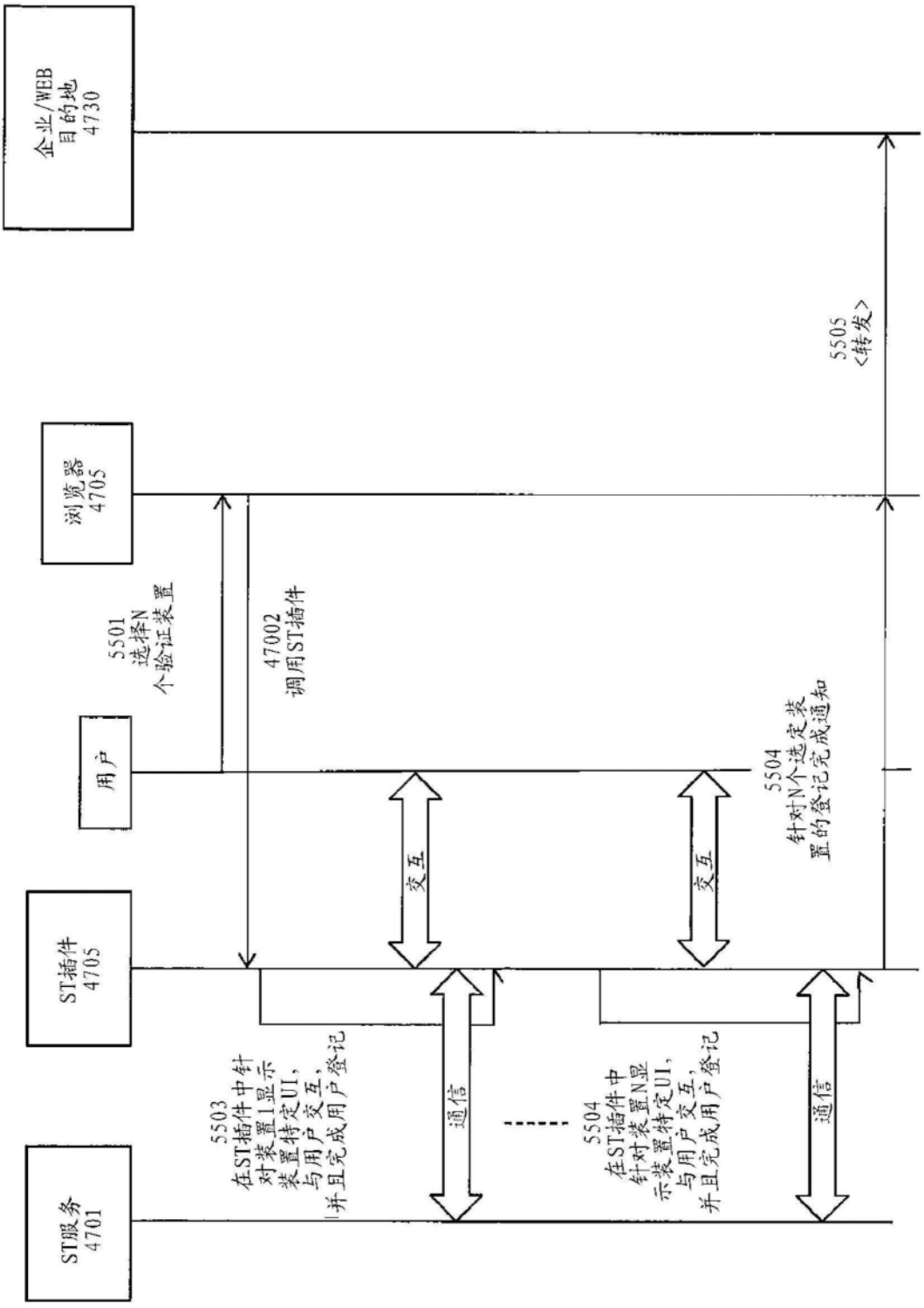

企业/WEB
目的地
4730
浏览器
4705
用户
ST插件
4705
ST服务
4701
5501
选择N
个验证装置
47002
调用ST插件
交互
交互
5504
针对N个选定装
置的登记完成通知
5505
<转发>
5503
在ST插件中针
对装置1显示
装置特定UI,
与用户交互,
并且完成用户登记
通信
5504
在ST插件中
针对装置N显
示装置特定UI,
与用户交互,
并且完成用户登记
通信

图55A

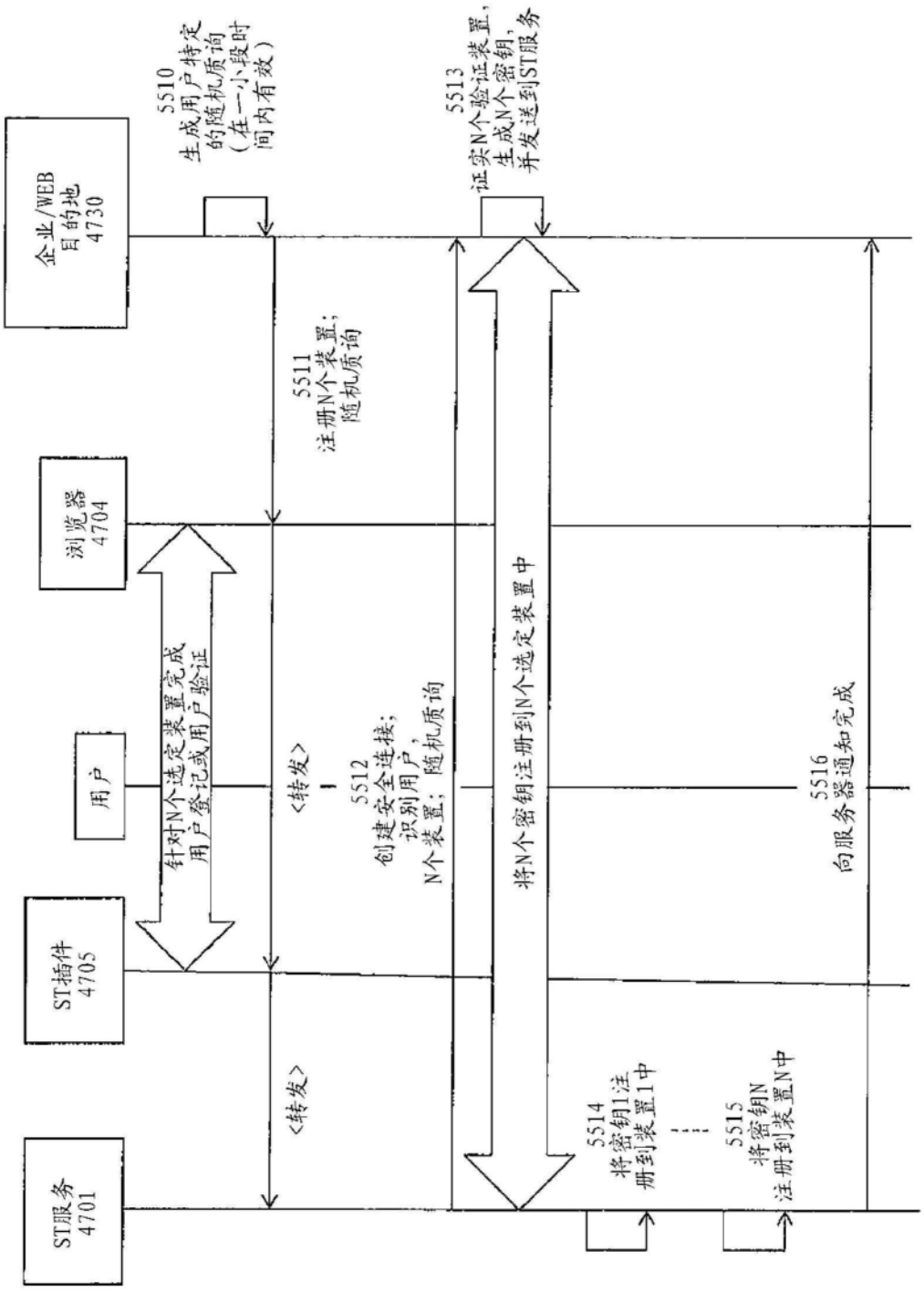

企业/WEB
目的地
4730
浏览器
4704
用户
ST插件
4705
ST服务
4701
5510
生成用户特定的随机质询（在一小段时间内有效）
5511
注册N个装置；随机质询
5512
创建安全连接；识别用户，N个装置；随机质询
5513
证实N个验证装置，生成N个密钥，并发送到ST服务
5514
将密钥1注册到装置1中
5515
将密钥N注册到装置N中
5516
向服务器通知完成
针对N个选定装置完成用户登记或用户验证
<转发>
<转发>
将N个密钥注册到N个选定装置中

图55B

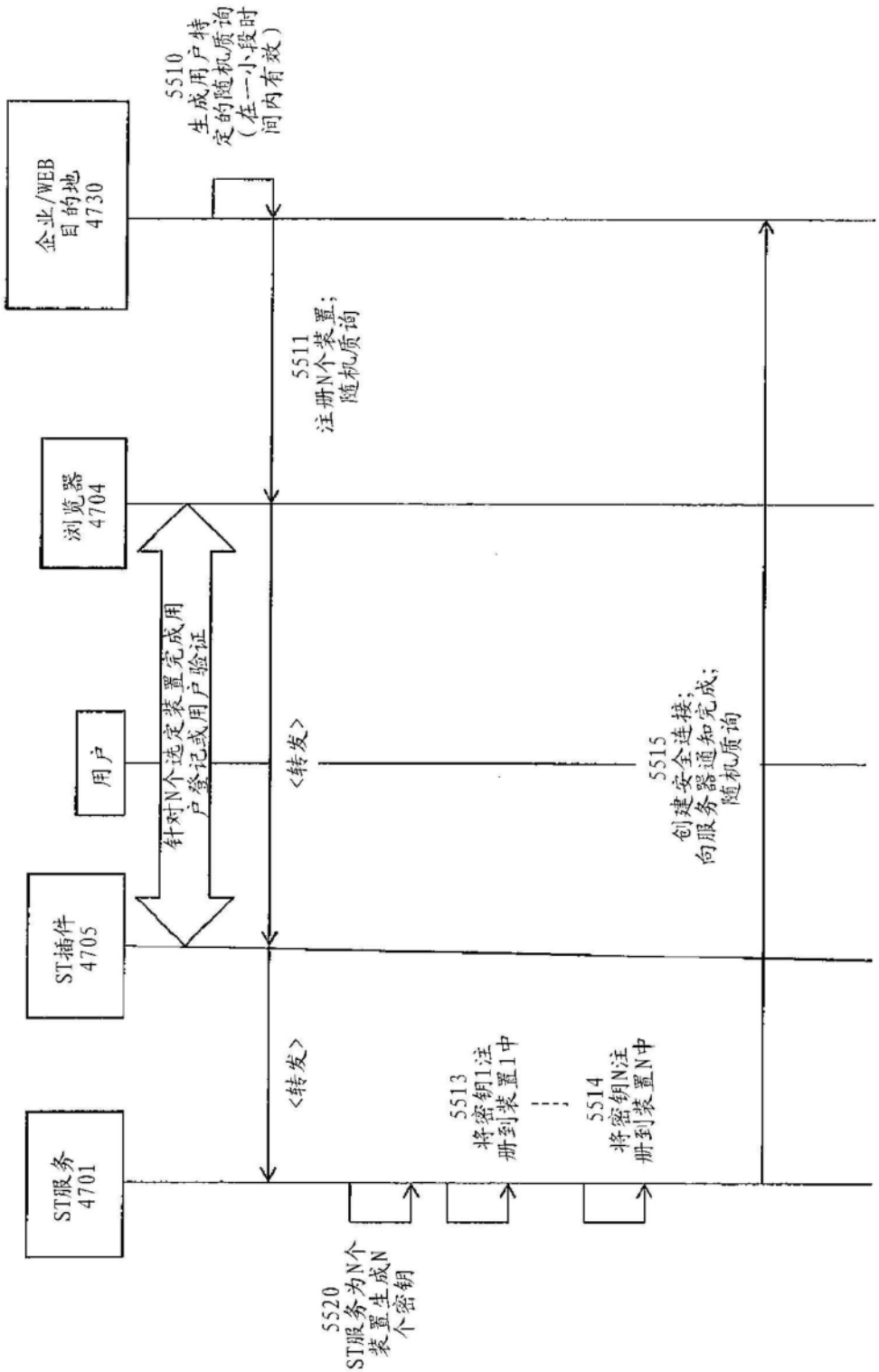

企业/WEB
目的地
4730
5510
生成用户特定的随机质询（在一小段时间内有效）
浏览器
4704
5511
注册N个装置；随机质询
用户
针对N个选定装置完成用户登记或用户验证
ST插件
4705
<转发>
5515
创建安全连接；向服务器通知完成；随机质询
ST服务
4701
<转发>
5513
将密钥1注册到装置1中
5514
将密钥N注册到装置N中
5520
ST服务为N个装置生成N个密钥

图55C

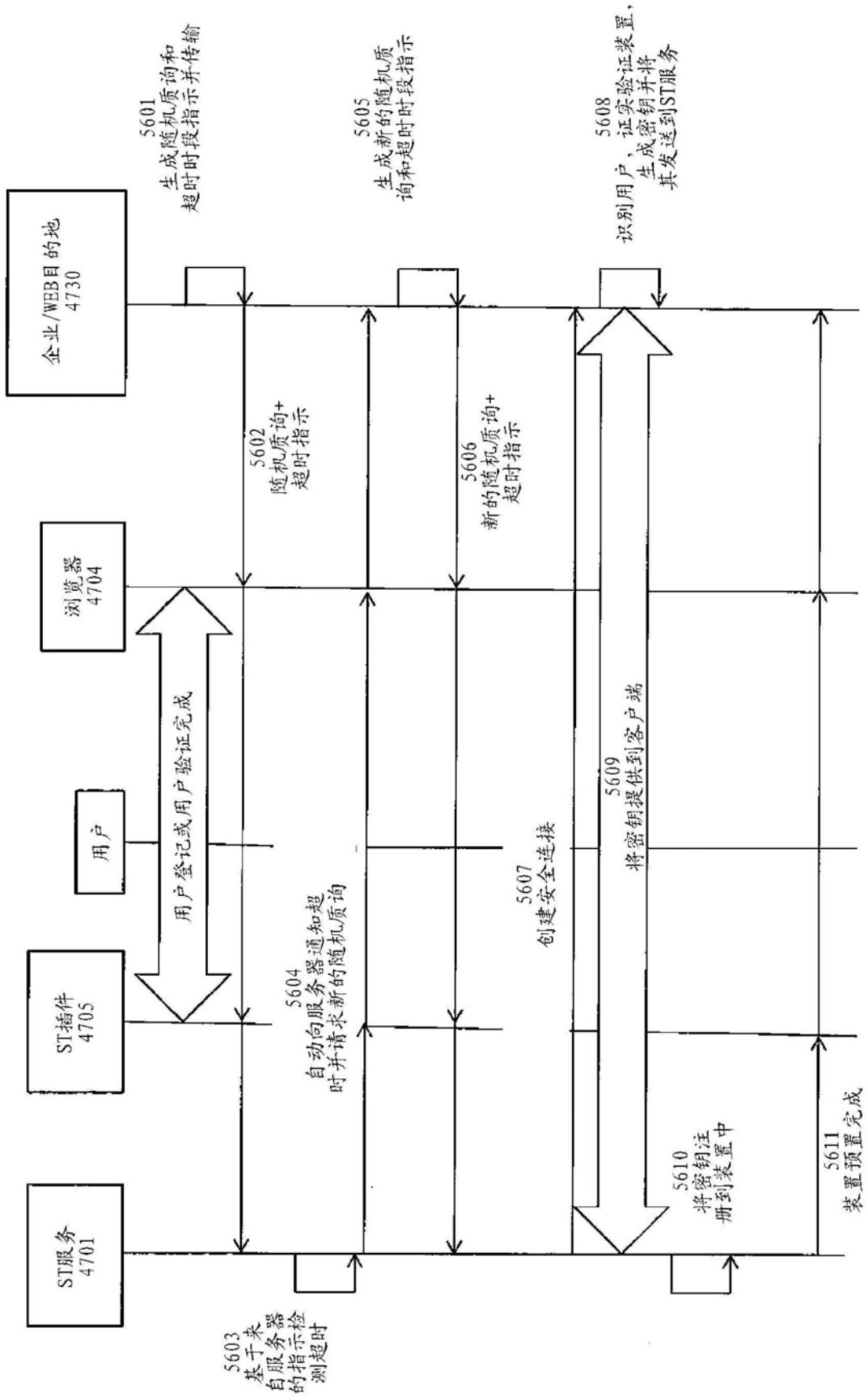

企业/WEB目的地
4730
浏览器
4704
用户
ST插件
4705
ST服务
4701
5601
生成随机质询和
超时时段指示并传输
5602
随机质询+
超时指示
5603
基于来
自服务器
的指示检
测超时
5604
自动向服务器通知超
时并请求新的随机质询
5605
生成新的随机质
询和超时时段指示
5606
新的随机质询+
超时指示
5607
创建安全连接
5608
识别用户，证实验证装置，
生成密钥并将
其发送到ST服务
5609
将密钥提供到客户端
5610
将密钥注
册到装置中
5611
装置预置完成
用户登记或用户验证完成

图56A

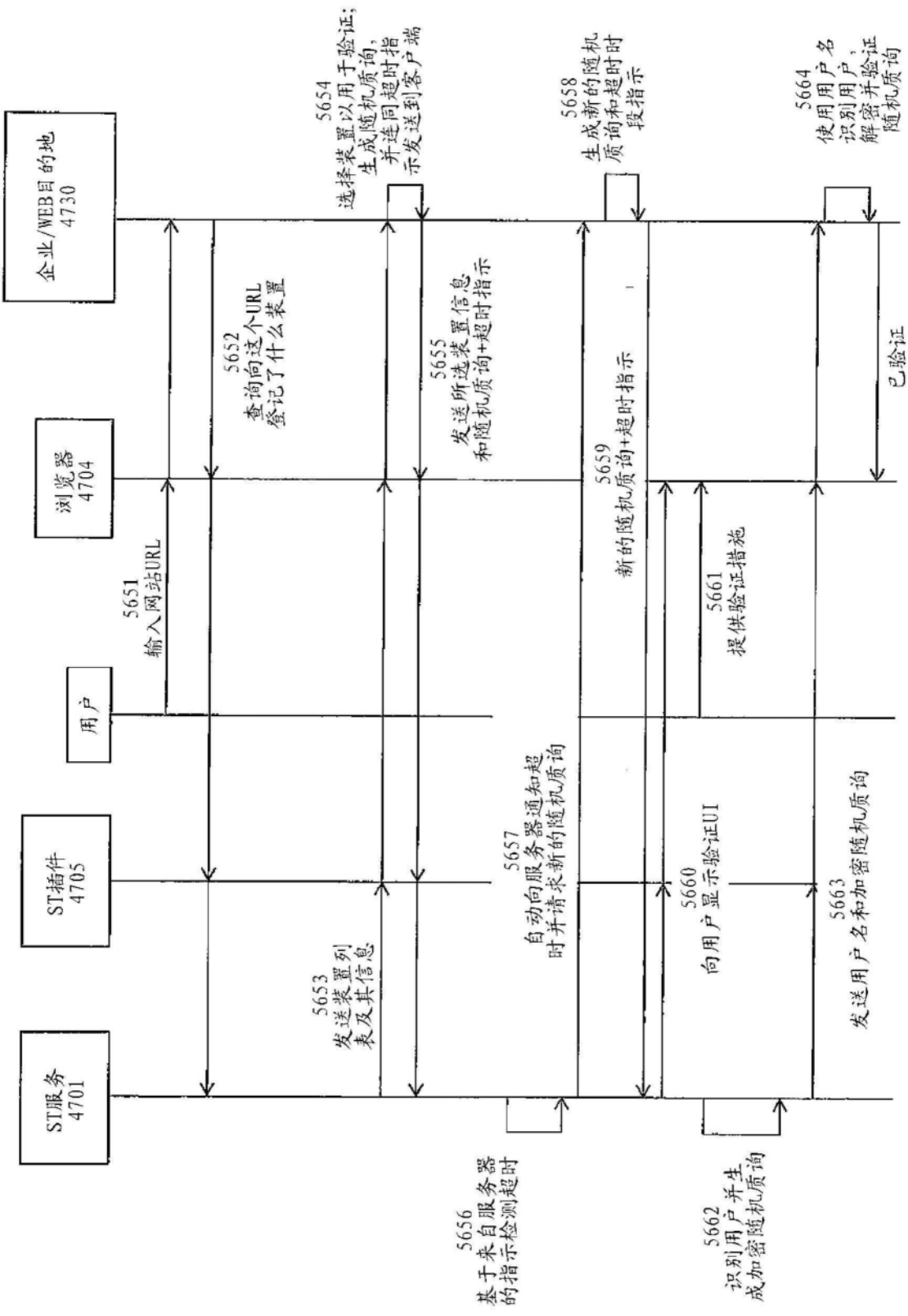

企业/WEB目的地
4730
浏览器
4704
用户
ST插件
4705
ST服务
4701
5651
输入网站URL
5652
查询向这个URL
登记了什么装置
5653
发送装置列
表及其信息
5654
选择装置以用于验证;
生成随机质询,
并连同超时指
示发送到客户端
5655
发送所选装置信息
和随机质询+超时指示
5656
基于来自服务器
的指示检测超时
5657
自动向服务器通知超
时并请求新的随机质询
5658
生成新的随机
质询和超时时
段指示
5659
新的随机质询+超时指示
5660
向用户显示验证UI
5661
提供验证措施
5662
识别用户并生
成加密随机质询
5663
发送用户名和加密随机质询
5664
使用用户名,
识别用户,
解密并验证
随机质询
已验证

图56B

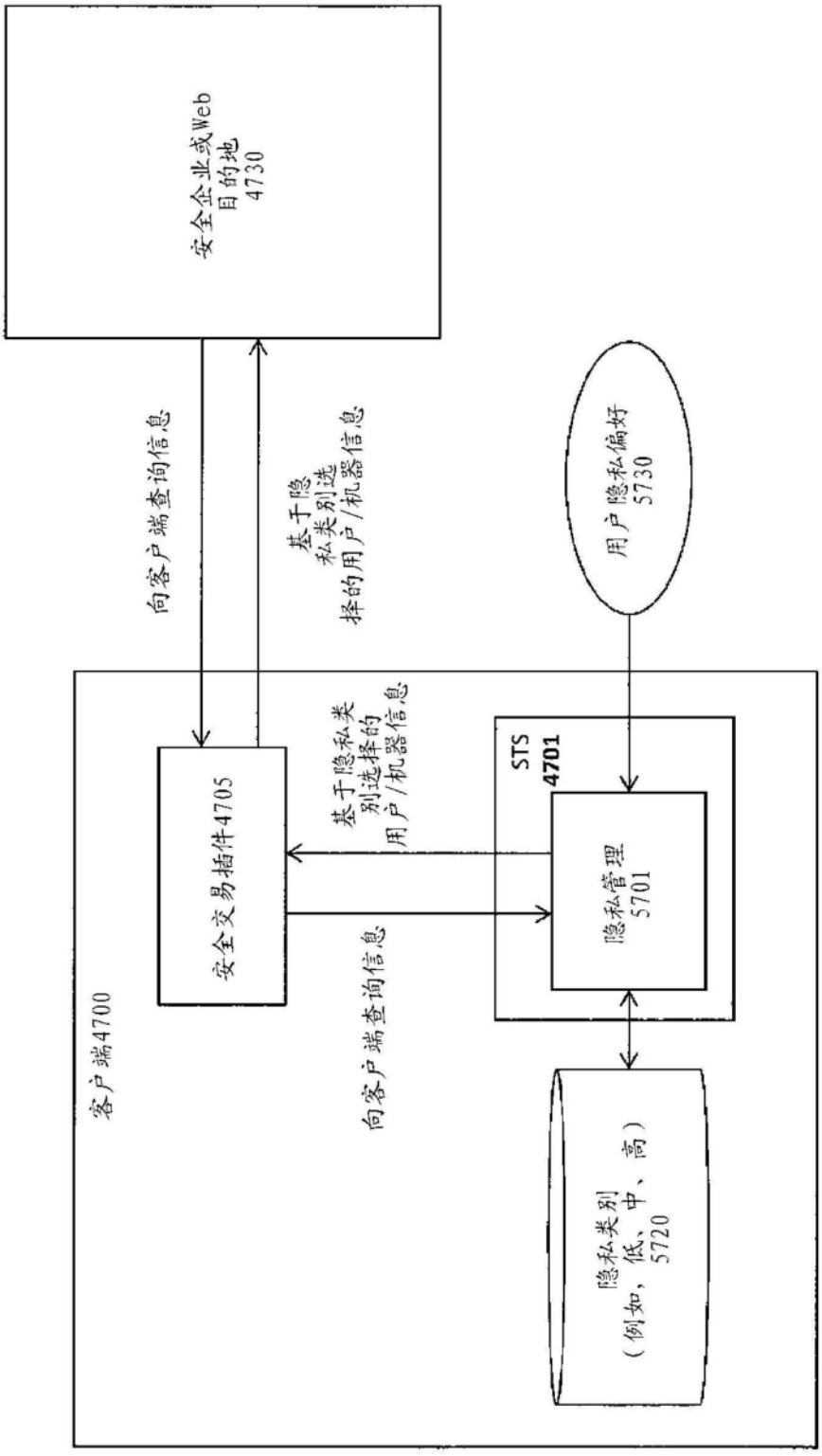

安全企业或Web
目的地
4730
向客户端查询信息
基于隐
私类别选
择的用户/机器信息
用户隐私偏好
5730
客户端4700
安全交易插件4705
基于隐私类
别选择的
用户/机器信息
STS
4701
隐私管理
5701
向客户端查询信息
隐私类别
（例如，低、中、高）
5720

图57

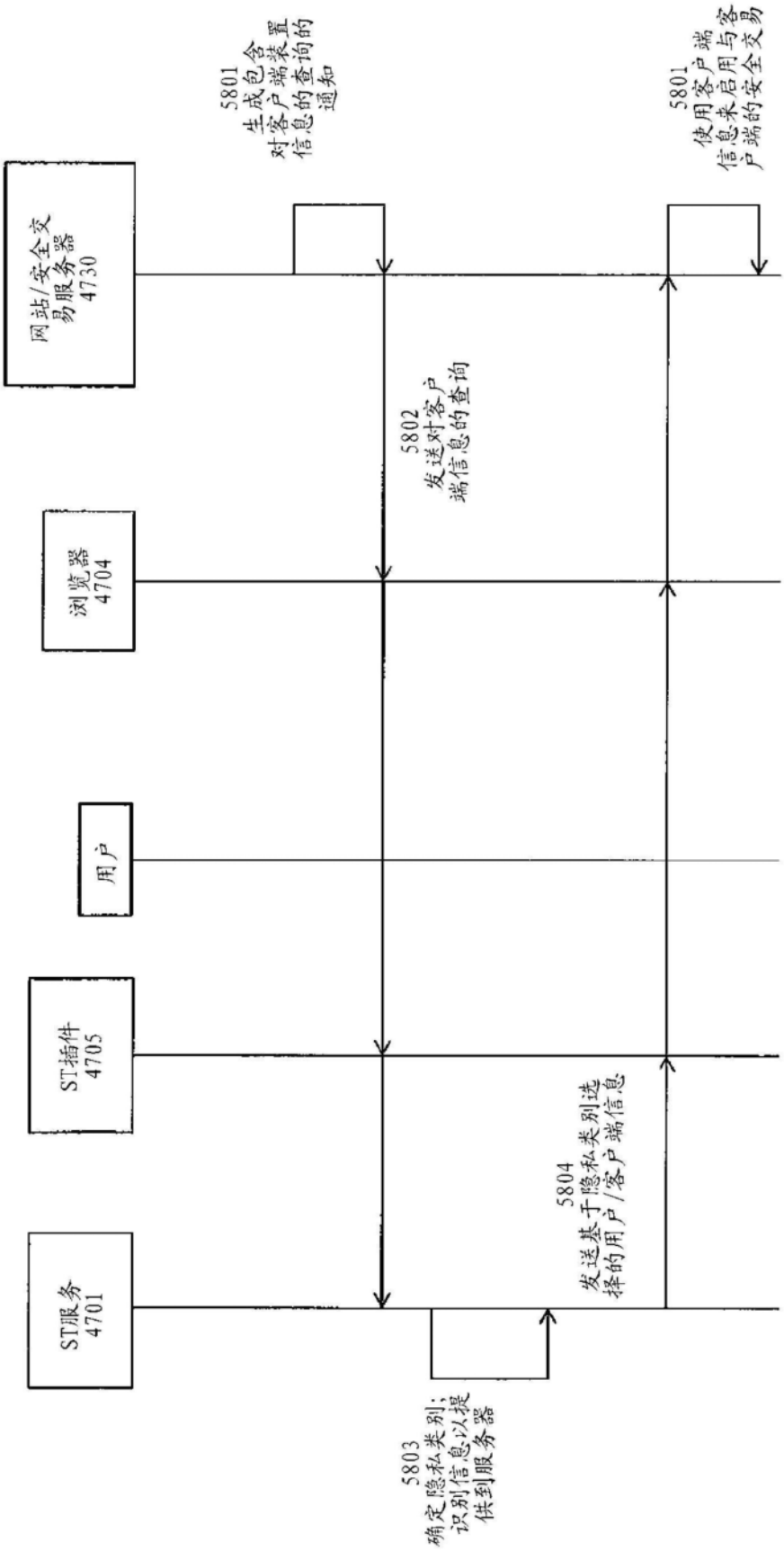

网站/安全交易服务器 4730
浏览器 4704
用户
ST插件 4705
ST服务 4701
5801 生成包含对客户端装置的查询的通知
5802 发送对客户端信息的查询
5803 确定隐私类别；识别信息以提供到服务器
5804 发送基于隐私类别选择的用户/客户端信息
5801 使用客户端信息来启用与客户端的安全交易

图58

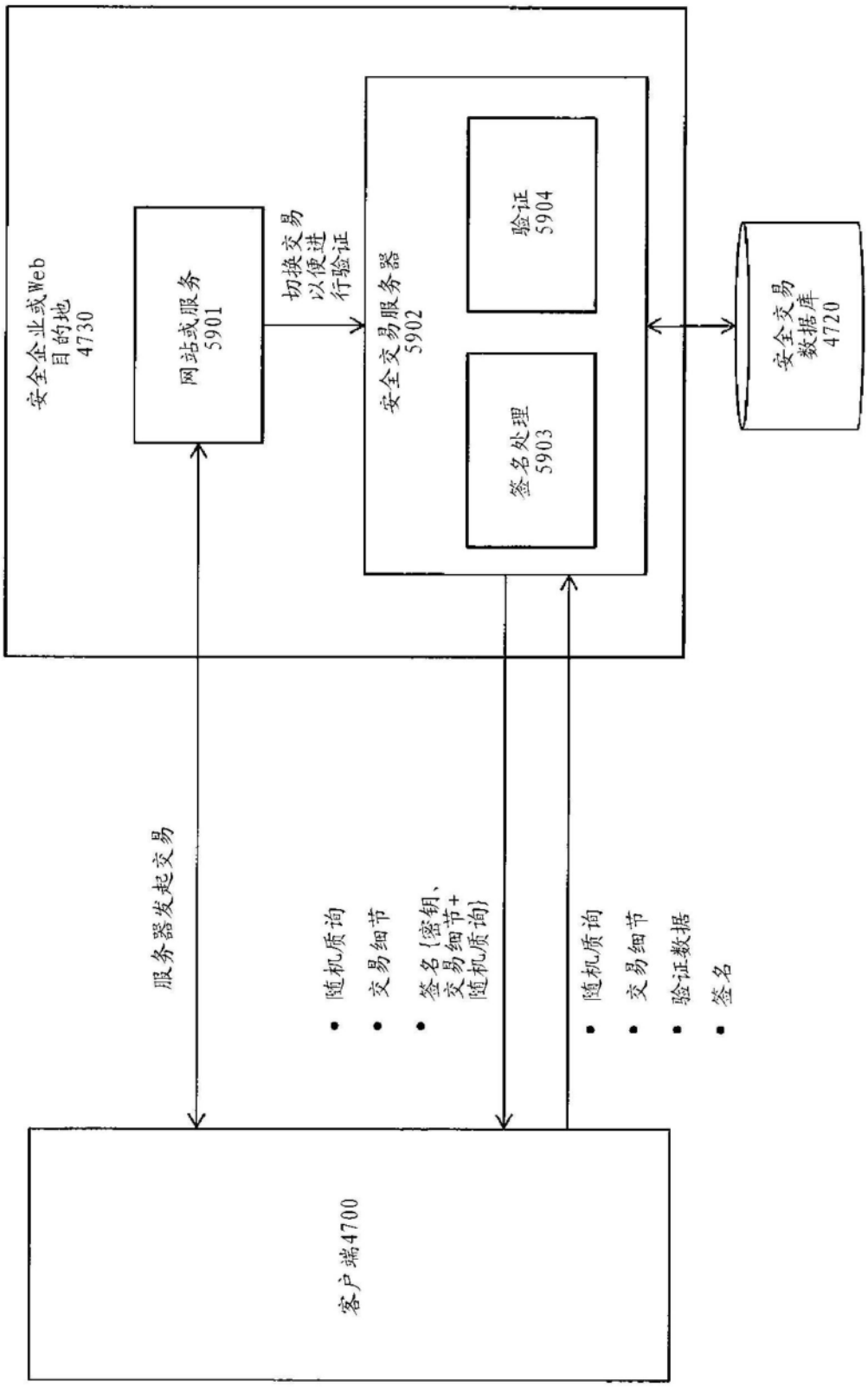

安全企业或Web
目的地
4730
网站或服务
5901
切换交易
以便进
行验证
安全交易服务器
5902
验证
5904
签名处理
5903
安全交易
数据库
4720
服务器发起交易
• 随机质询
• 交易细节
• 签名{密钥、
交易细节+
随机质询}
• 随机质询
• 交易细节
• 验证数据
• 签名
客户端4700

图59

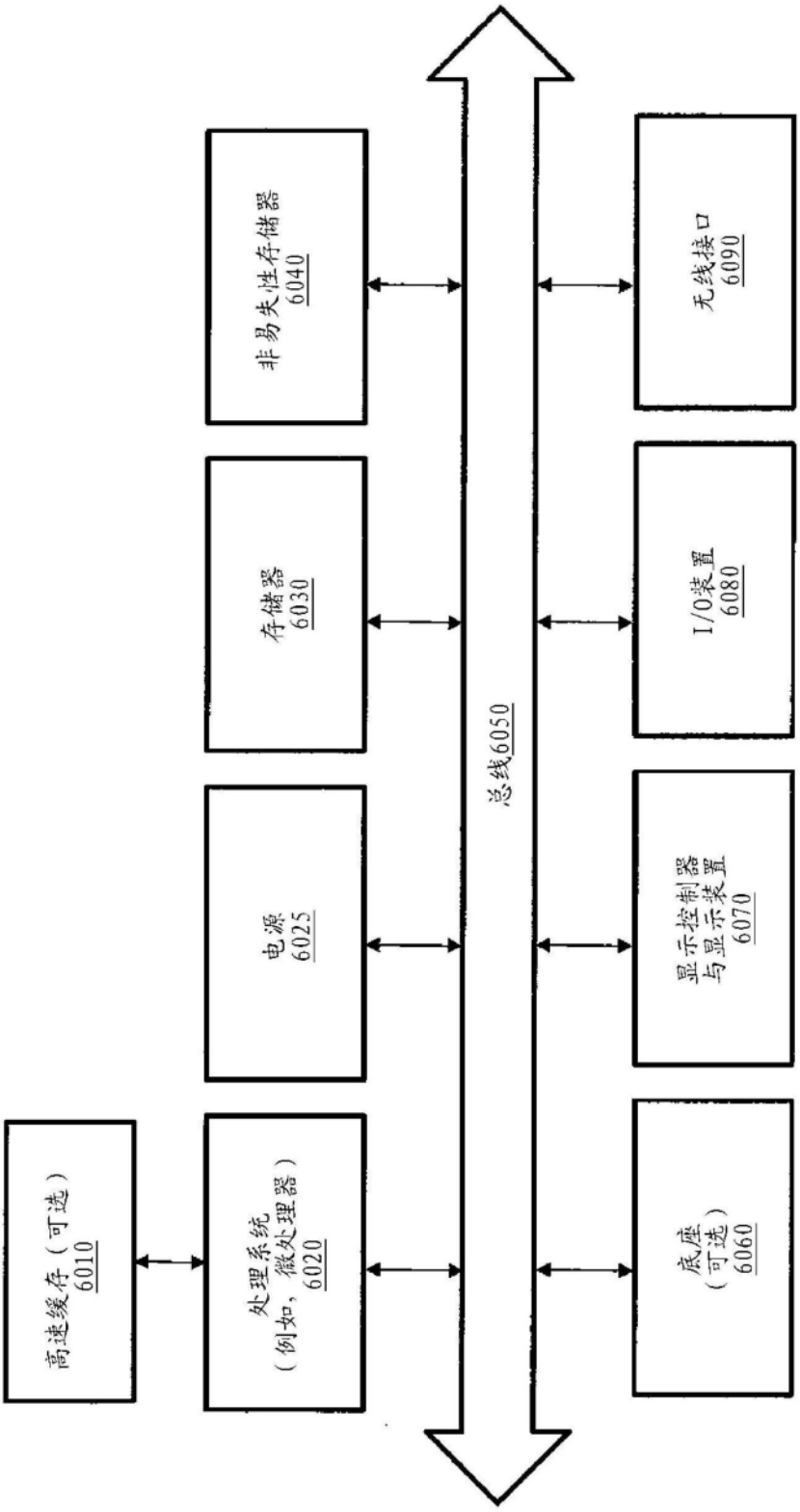

高速缓存（可选）
6010
处理系统
（例如，微处理器）
6020
电源
6025
存储器
6030
非易失性存储器
6040
总线6050
显示控制器
与显示装置
6070
I/O装置
6080
无线接口
6090
底座
（可选）
6060

图60

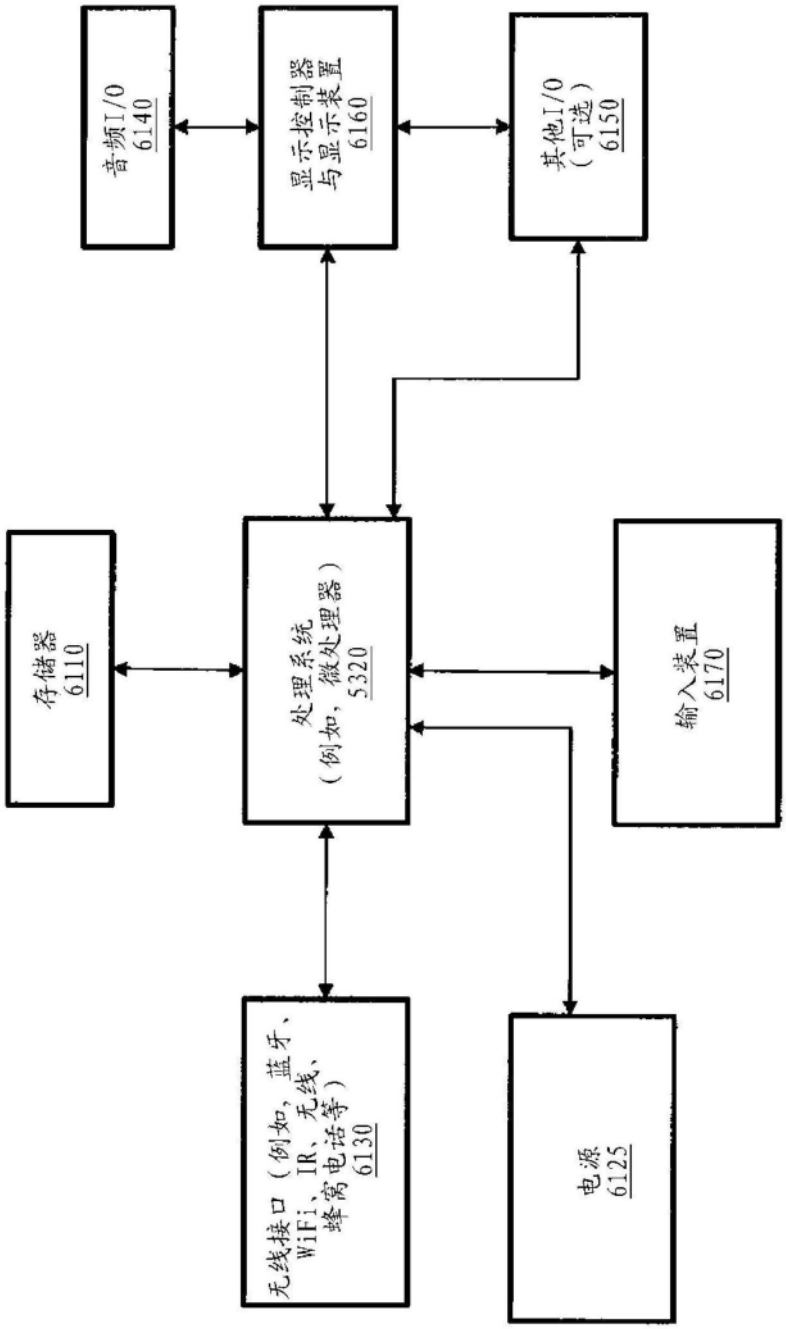

音频I/O
6140
显示控制器
与显示装置
6160
其他I/O
（可选）
6150
存储器
6110
处理系统
（例如，微处理器）
5320
输入装置
6170
无线接口（例如，蓝牙、
WiFi、IR、无线、
蜂窝电话等）
6130
电源
6125

图61