(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106575326 B
(45)授权公告日 2021.03.02

(21)申请号 201580040813.6
(22)申请日 2015.07.30
(65)同一申请的已公布的文献号
申请公布号 CN 106575326 A
(43)申请公布日 2017.04.19
(30)优先权数据
14/448,747 2014.07.31 US
(85)PCT国际申请进入国家阶段日
2017.01.26
(86)PCT国际申请的申请数据
PCT/US2015/042870 2015.07.30
(87)PCT国际申请的公布数据
WO2016/019127 EN 2016.02.04
(73)专利权人 诺克诺克实验公司
地址 美国加利福尼亚州
(72)发明人 D·巴格达萨瑞安
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 沈锦华
(51)Int.Cl.
G06F 21/31(2013.01)
(56)对比文件
US 2009138727 A1,2009.05.28
US 2011219427 A1,2011.09.08
US 2014189350 A1,2014.07.03
US 2007278291 A1,2007.12.06
Guenther Starnberger等.QT-TAN:Secure Moblie Transaction Authentication.《2009 International Conference on Availability and Security》.2009,
Guenther Starnberger等.QT-TAN:Secure Moblie Transaction Authentication.《2009 International Conference on Availability and Security》.2009,
审查员 张瑀琪

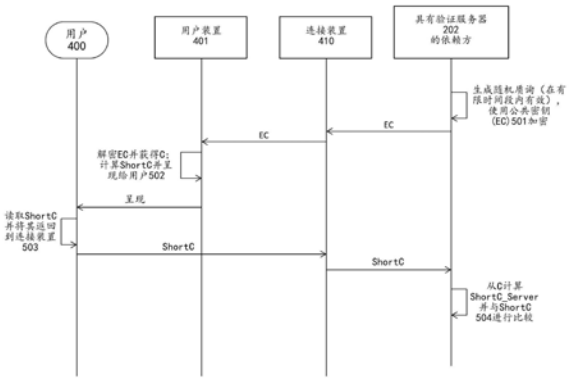
权利要求书3页 说明书9页 附图11页

(54)发明名称

利用非对称加密实施一次性密码的系统和方法

(57)摘要

本专利申请描述了使用非对称加密进行验证的系统、装置、方法和机器可读介质。例如，根据一个实施例的方法包括：在服务器处生成质询；在所述服务器处使用公共加密密钥加密所述质询；将所述加密的质询发送到连接装置，所述连接装置通过网络与所述服务器具有第一连接；将所述加密的质询从所述连接装置提供至用户装置；使用对应于所述公共加密密钥的私有加密密钥来解密所述加密的质询以确定所述质询；转换所述质询为转换的质询，所述转换的质询具有与所述原始质询不同的格式；在所述连接装置处接收所述转换的质询，并且将所述转换的质询从所述连接装置提供给所述服务器；以及在所述服务器处证实所述转换的质询以验证所述用户。



CN 106575326 B

1.一种用于用户验证的方法,包括:

在服务器处生成质询;

将所述质询存储在所述服务器的安全存储中;

在所述服务器处使用公共加密密钥加密所述质询以生成加密的质询;

将来自所述服务器的所述加密的质询发送到连接装置,所述连接装置通过网络与所述服务器具有第一连接;

将所述加密的质询从所述连接装置提供至用户装置,所述连接装置无法访问所述质询;

在所述用户装置处使用对应于所述公共加密密钥的私有加密密钥来解密所述加密的质询以确定所述质询;

在所述用户装置处使用转换技术将所述质询转换为转换的质询,所述转换的质询具有与所述质询不同的格式;

在所述连接装置处接收所述转换的质询,并且将所述转换的质询从所述连接装置提供给所述服务器,其中在所述连接装置处接收所述转换的质询包括:经由耦接到所述连接装置的用户输入装置来接收所述转换的质询的手动用户输入;

在所述服务器处从所述连接装置接收所述转换的质询;

检索来自所述服务器的所述安全存储的所述质询;

使用与用于在所述用户装置处将所述质询转换为转换的质询相同的转换技术将检索的质询转换为服务器转换的质询;以及

通过对比所述转换的质询和所述服务器转换的质询,在所述服务器处证实所述转换的质询以验证所述用户,其中如果所述转换的质询匹配所述服务器转换的质询,则所述用户验证成功。

2.根据权利要求1所述的方法,其中所述质询包括由所述服务器上的随机数发生器生成的随机质询。

3.根据权利要求2所述的方法,其中所述转换技术包括截断所述质询的一部分,并且使用所截断的部分或截断后的剩余部分用于所述转换的质询。

4.根据权利要求3所述的方法,其中所述质询被截断以生成6位转换的质询。

5.根据权利要求1所述的方法,其中所述连接装置包括联网的计算机系统、销售点(PoS)终端或自动取款机(ATM)。

6.根据权利要求5所述的方法,其中所述用户装置包括移动智能电话装置。

7.根据权利要求6所述的方法,其中将所述加密的质询从所述连接装置提供至用户装置包括在所述连接装置的显示器上显示光学代码,并且由所述用户装置读取所述光学代码。

8.根据权利要求7所述的方法,其中所述光学代码包括二维(QR)码或条形码。

9.根据权利要求6所述的方法,其中将所述加密的质询从所述连接装置提供至用户装置包括在所述用户装置和所述连接装置之间建立局域无线通信信道。

10.根据权利要求9所述的方法,其中所述局域无线通信信道包括蓝牙信道、近场通信(NFC)信道、WiFi信道或无线USB信道。

11.根据权利要求3所述的方法,其中证实所述转换的质询包括截断所述服务器上的所

述质询的相同部分，并将在所述服务器上截断的所述转换的质询与由所述连接装置提供的所述转换的质询进行比较。

12.一种用于用户验证的系统，包括：

服务器，生成质询并将所述质询存储在所述服务器的安全存储中；

所述服务器，进一步使用公共加密密钥加密所述质询以生成加密的质询，并将所述加密的质询发送到通过网络与所述服务器具有第一连接的连接装置；

所述连接装置，将所述加密的质询提供给用户装置，所述连接装置无法访问所述质询；

所述用户装置，使用对应于所述公共加密密钥的私有加密密钥来解密所述加密的质询以确定所述质询；

所述用户装置，进一步使用转换技术将所述质询转换为转换的质询，所述转换的质询具有与所述质询不同的格式；

所述连接装置，接收所述转换的质询并将所述转换的质询提供给所述服务器，其中所述连接装置通过经由耦接到所述连接装置的用户输入装置来接收所述转换的质询的手动用户输入接收所述转换的质询；以及

所述服务器，接收来自所述连接装置的所述转换的质询，检索来自所述服务器的所述安全存储的所述质询，并使用与用于在所述用户装置处将所述质询转换为转换的质询相同的转换技术将检索的质询转换为服务器转换的质询；以及

所述服务器，进一步通过对比所述转换的质询和所述服务器转换的质询来证实所述转换的质询以验证所述用户，其中如果所述转换的质询匹配所述服务器转换的质询，则所述用户验证成功。

13.根据权利要求12所述的系统，其中所述质询包括由所述服务器上的随机数发生器生成的随机质询。

14.根据权利要求13所述的系统，其中所述转换技术包括截断所述质询的一部分，并且使用所截断的部分或截断后的剩余部分用于所述转换的质询。

15.根据权利要求14所述的系统，其中所述质询被截断以生成6位转换的质询。

16.根据权利要求12所述的系统，其中所述连接装置包括联网的计算机系统、销售点(PoS)终端或自动取款机(ATM)。

17.根据权利要求16所述的系统，其中所述用户装置包括移动智能电话装置。

18.根据权利要求17所述的系统，其中将所述加密的质询从所述连接装置提供至用户装置包括在所述连接装置的显示器上显示光学代码，并且由所述用户装置读取所述光学代码。

19.根据权利要求18所述的系统，其中所述光学代码包括二维(QR)码或条形码。

20.根据权利要求17所述的系统，其中将所述加密的质询从所述连接装置提供至用户装置包括在所述用户装置和所述连接装置之间建立局域无线通信信道。

21.根据权利要求20所述的系统，其中所述局域无线通信信道包括蓝牙信道、近场通信(NFC)信道、WiFi信道或无线USB信道。

22.根据权利要求14所述的系统，其中证实所述转换的质询包括截断所述服务器上的所述质询的相同部分，并将在所述服务器上截断的所述转换的质询与由所述连接装置提供的转换的质询进行比较。

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

在服务器处生成质询；

将所述质询存储在所述服务器的安全存储中；

在所述服务器处使用公共加密密钥加密所述质询以生成加密的质询；

将来自所述服务器的所述加密的质询发送到连接装置，所述连接装置通过网络与所述服务器具有第一连接；

将所述加密的质询从所述连接装置提供至用户装置，所述连接装置无法访问所述质询；

在所述用户装置处使用对应于所述公共加密密钥的私有加密密钥来解密所述加密的质询以确定所述质询；

在所述用户装置处使用转换技术将所述质询转换为转换的质询，所述转换的质询具有与所述质询不同的格式；

在所述连接装置处接收所述转换的质询，并且将所述转换的质询从所述连接装置提供给所述服务器，其中在所述连接装置处接收所述转换的质询包括：经由耦接到所述连接装置的用户输入装置来接收所述转换的质询的手动用户输入；

在所述服务器处从所述连接装置接收所述转换的质询；

检索来自所述服务器的所述安全存储的所述质询；

使用与用于在所述用户装置处将所述质询转换为转换的质询相同的转换技术将检索的质询转换为服务器转换的质询；以及

通过对比所述转换的质询和所述服务器转换的质询，在所述服务器处证实所述转换的质询以验证所述用户，其中如果所述转换的质询匹配所述服务器转换的质询，则所述用户验证成功。

24.根据权利要求23所述的机器可读介质，其中所述质询包括由所述服务器上的随机数发生器生成的随机质询。

25.根据权利要求24所述的机器可读介质，其中所述转换技术包括截断所述质询的一部分，并且使用所截断的部分或截断后的剩余部分用于所述转换的质询。

利用非对称加密实施一次性密码的系统和方法

背景技术

技术领域

[0001] 本发明整体涉及数据处理系统的领域。更具体地讲，本发明涉及用于利用非对称加密实施一次性密码的系统和方法。

[0002] 相关领域说明

[0003] 还已经设计了使用生物计量传感器经由网络提供安全用户验证的系统。在此类系统中，可经由网络发送由验证器生成的得分和/或其他验证数据，以向远程服务器验证用户。例如，专利申请No.2011/0082801(“‘801申请”)描述了一种在网络上进行用户注册和验证的框架，这种框架提供强验证(例如，防御身份窃取和网络钓鱼)、安全交易(例如，防御交易中的“浏览器中的恶意软件”和“中间人”攻击)和客户端验证令牌的登记/管理(例如，指纹读取器、面部识别装置、智能卡、可信平台模块等等)。

[0004] 本申请的受让人已经开发出对‘801申请中所描述的验证框架的多种改进。这些改进中的一些在以下一组美国专利申请中描述，这些美国专利申请都被转让给本受让人：序列号13/730,761，名称为“Query System and Method to Determine Authentication Capabilities”(用于确定验证功能的查询系统和方法)；序列号13/730,776，名称为“System and Method for Efficiently Enrolling,Registering,and Authenticating With Multiple Authentication Devices”(使用多个验证装置有效地进行登记、注册和验证的系统和方法)；序列号13/730,780，名称为“System and Method for Processing Random Challenges Within an Authentication Framework”(用于在验证框架内处理随机质询的系统和方法)；序列号13/730,791，名称为“System and Method for Implementing Privacy Classes Within an Authentication Framework”(用于在验证框架内实施隐私类别的系统和方法)；序列号13/730,795，名称为“System and Method for Implementing Transaction Signaling Within an Authentication Framework”(用于在验证框架内实施交易信令的系统和方法)；以及序列号14/218,504，名称为“Advanced Authentication Techniques and Applications”(高级验证技术和应用)(下文中称为“‘504申请”)。在本文中有时将这些申请称为(“共同未决的申请”)。

[0005] 简单地讲，在这些共同未决的申请描述的验证技术中，用户向客户端装置上的验证装置(或验证器)诸如生物计量装置(例如，指纹传感器)登记。当用户向生物计量装置登记时，(例如，通过轻扫手指、拍摄照片、记录语音等)捕捉生物计量参考数据。用户可随后经由网络向一个或多个服务器(例如，配备有安全交易服务的网站或其他依赖方，如共同未决的申请中所述)注册/预置验证装置；并且随后使用在注册过程中交换的数据(例如，预置到验证装置中的密钥)向那些服务器验证。一旦通过验证，用户便获许与网站或其他依赖方执行一个或多个在线交易。在共同未决的申请所描述的框架中，敏感信息(诸如指纹数据和可用于唯一地标识用户的其他数据)可本地保持在用户的验证装置上，以保护用户的隐私。

[0006] ‘504申请描述了多种额外的技术，包括以下技术：设计复合验证器、智能地生成验

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

附图说明

[0007] 可结合下列附图从以下具体实施方式更好地理解本发明，其中：

[0008] 图1A至图1B示出了安全验证系统架构的两个不同实施例；

[0009] 图2是示出可如何将密钥预置到验证装置中的交易图；

[0010] 图3示出了显示远程验证的交易图；

[0011] 图4示出了在依赖方验证服务器和用户装置之间配置的连接装置；

[0012] 图5示出了使用非对称加密实施一次性密码的本发明的一个实施例；

[0013] 图6A至图6B示出了验证服务器的一个实施例的额外细节；

[0014] 图7示出了用户装置的一个实施例的额外细节；

[0015] 图8示出了用于实施本文所描述的客户端和/或服务器的示例性数据处理架构；以及

[0016] 图9示出了用于实施本文所描述的客户端和/或服务器的另一示例性数据处理架构。

具体实施方式

[0017] 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。

[0018] 下文论述的本发明的实施例涉及具有用户核实功能(诸如生物计量形式或PIN输入)的验证装置。这些装置在本文中有时称为“令牌”、“验证装置”或“验证器”。尽管某些实施例注重于面部识别硬件/软件(例如，用于识别用户面部并且跟踪用户的眼球运动的相机和相关联软件)，但有些实施例可利用额外的生物计量装置，包括(例如)指纹传感器、声音识别硬件/软件(例如，用于识别用户声音的麦克风和相关联软件)以及光学识别能力(例如，用于扫描用户视网膜的光学扫描器和相关联软件)。用户验证功能还可包括非生物计量形式，如PIN输入。验证器可使用装置，如可信平台模块(TPM)、智能卡和安全元件，来进行密码操作与密钥存储。

[0019] 在移动式生物计量的具体实施中，生物计量装置远程于依赖方。如本文所用，术语“远程”意味着生物计量传感器不是其以通信方式耦接到的计算机的安全边界的一部分(例如，生物计量传感器未嵌入到与依赖方计算机相同的物理外壳中)。举例来说，生物计量装置可经由网络(例如，因特网、无线网络链路等)或经由外围输入(诸如USB端口)耦接到依赖方。在这些条件下，依赖方可能无法知道装置是否为得到依赖方授权的装置(例如，提供可接受等级的验证强度和完整性保护的装置)以及/或者黑客是否已经危及或甚至已经替换了生物计量装置。生物计量装置的置信度取决于装置的特定实施。

[0020] 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。

[0021] 本文中有时使用术语“依赖方”来不仅指尝试与之进行用户交易的实体(例如,执行用户交易的网站或在线服务),也指安全交易服务器(有时称为代表那个实体实施的,该实体可执行本文所述的基础验证技术)。安全交易服务器可由依赖方拥有并且/或者在依赖方的控制下,或者可在作为商业安排的一部分向依赖方提供安全交易服务的第三方的控制下。

[0022] 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。

[0023] 示例性系统架构和交易

[0024] 图1A至图1B示出了包括用于注册/预置验证装置(有时也称为“预置”)和验证用户的客户端和服务器端组件的系统架构的两个实施例。图1A所示的实施例使用基于web浏览器插件的架构来与网站通信,而图1B所示的实施例不需要web浏览器。本文所描述的各种技术,诸如向验证装置登记用户、向安全服务器注册/预置验证装置以及核验用户可在这些系统架构中的任一者上实施。因此,虽然图1A所示的架构用于展示下述若干实施例的操作,但相同的基本原理可在图1B所示的系统上容易地实施(例如,通过删除浏览器插件105,该浏览器插件充当用于在服务器130与客户端上的安全交易服务101之间通信的中介)。

[0025] 首先转到图1A,所示实施例包括配备有一个或多个用于登记和核验最终用户的验证装置110至112(这些验证装置在本领域中有时称为验证“令牌”或“验证器”)的客户端100。如上所述,验证装置110至112可包括生物计量装置,诸如指纹传感器、声音识别硬件/软件(例如,用于识别用户声音的麦克风和相关联软件)、面部识别硬件/软件(例如,用于识别用户面部的相机和相关联软件)和光学识别功能(例如,用于扫描用户视网膜的光学扫描器和相关联软件),并且支持非生物计量形式(诸如PIN核验)。验证装置可使用可信平台模块(TPM)、智能卡或安全元件用于加密操作以及密钥存储。

[0026] 验证装置110至112通过由安全交易服务101暴露的接口102(例如,应用程序编程接口或API)以通信方式耦接到客户端。安全交易服务101是用于经由网络与一个或多个安全交易服务器132至133通信以及用于与在web浏览器104的环境内执行的安全交易插件105介接的安全应用程序。如图所示,接口102还可提供对客户端100上的安全存储装置120的安全访问,该安全存储装置存储与每个验证装置110至112相关的信息,诸如装置识别代码、用户识别代码、受验证装置保护的用户登记数据(例如,所扫描的指纹或其他生物计量数据),以及用于执行本文所述安全验证技术的由验证装置包封的密钥。例如,如下文详细论述,唯一密钥可被存储到每个验证装置中并且在经由网络(诸如因特网)与服务器130通信时使用。

[0027] 如下文论述，安全交易插件105支持某些类型的网络交易，诸如与网站131或其他服务器的HTTP或HTTPS交易。在一个实施例中，响应于由安全企业或Web目的地130内的网络服务器131(下文中有时简称为“服务器130”)插入到网页HTML代码中的特定HTML标签来启动安全交易插件。响应于检测到此类标签，安全交易插件105可将交易转发到安全交易服务101以进行处理。另外，对于某些类型的事务(例如，诸如安全密钥交换)，安全交易服务101可开启与当地交易服务器132(即，与网站位于同一地点)或异地交易服务器133的直接通信信道。

[0028] 安全交易服务器132至133耦接到安全交易数据库120，安全交易数据库120用于存储用户数据、验证装置数据、密钥以及支持下文所述的安全验证交易所需要的其他安全信息。然而，应当指出的是，本发明的基本原理不需要分离图1A所示的安全企业或web目的地130内的逻辑组件。例如，网站131和安全交易服务器132至133可在单个物理服务器或分开的多个物理服务器内实施。此外，网站131和交易服务器132至133可在用于执行下文所述的功能的一个或多个服务器上所执行的集成软件模块内实施。

[0029] 如上所述，本发明的基本原理不限于图1A所示的基于浏览器的架构。图1B示出了另选的具体实施，其中独立应用程序154利用由安全交易服务101提供的功能来经由网络验证用户。在一个实施例中，应用程序154被设计为建立与一个或多个网络服务151的通信会话，这些网络服务依赖于安全交易服务器132至133来执行下文详细描述的用户/客户端验证技术。

[0030] 在图1A和图1B所示的任一个实施例中，安全交易服务器132至133可生成密钥，这些密钥接着被安全地传输到安全交易服务101并存储到安全存储装置120内的验证装置中。另外，安全交易服务器132至133管理服务器端上的安全交易数据库120。

[0031] 与远程预置验证装置和利用依赖方验证相关联的某些基本原理将参考图2至图5来描述，随后使用安全通信协议来建立信任的本发明的实施例的详细描述。

[0032] 图2示出了用于在客户端(诸如，图1A至图B中的客户端100上的装置110至112)预置验证装置的一系列交易。“预置”有时也被称为“注册”。为了简单起见，安全交易服务101和接口102被组合在一起作为验证客户端201，包括安全交易服务器132至133的安全企业或Web目的地130被表示为依赖方202。

[0033] 在预置验证器(例如，指纹验证器、语音验证器等)期间，在验证客户端201和依赖方202之间共享与验证器相关联的密钥。回顾图1A至图1B，密钥存储在客户端100的安全存储装置120和由安全交易服务器132至133使用的安全交易数据库120内。在一个实施例中，密钥是由安全交易服务器132至133中的一个生成的对称密钥。然而，在下文论述的另一个实施例中，使用了不对称密钥。在该实施例中，可以由安全交易服务器132至133生成公共/私有密钥对。公共密钥然后可由安全交易服务器132至133存储，并且相关私有密钥可存储在客户端上的安全存储装置120中。在一个另选的实施例中，密钥可在客户端100上生成(例如，由验证装置或验证装置接口而不是安全交易服务器132至133生成)。本发明的基本原理不限于任何特定类型的密钥或生成密钥的方式。

[0034] 在一个实施例中采用一种安全密钥预置协议以通过安全通信信道与客户端共享密钥。密钥预置协议的一个示例是动态对称密钥预置协议(DSKPP)(例如，参见请求注释(RFC)6063)。然而，本发明的基本原理不限于任何特定密钥预置协议。在一个特定实施例

中，客户端生成公共/私有密钥对并向服务器发送公共密钥，可以利用证明密钥证明它们。

[0035] 转到图2所示的具体细节，要启动注册流程，依赖方202生成随机生成的质询(例如，密码随机数)，验证客户端201必须在装置注册期间呈现此质询。该随机质询可在有限时间段内有效。作为响应，验证客户端201发起与依赖方202的带外安全连接(例如，带外交易)，并使用密钥预置协议(例如，上文提到的DSKPP协议)与依赖方202通信。为了发起安全连接，验证客户端201可以向依赖方202返回随机质询(可能带有在随机质询上生成的签名)。此外，验证客户端201可以传输用户的身份(例如，用户ID或其他代码)和要预置注册的验证装置的身份(例如，利用唯一地标识被预置验证装置类型的验证证明ID(AAID))。

[0036] 该依赖方利用用户名或ID代码(例如，在用户账户数据库中)定位用户，(例如，使用签名或简单地比较随机质询与发送过的质询)证实随机质询，证实验证装置的验证代码(如果发送了验证代码(例如，AAID))，并在安全交易数据库(例如，图1A至图1B中的数据库120)中为用户和验证装置创建新条目。在一个实施例中，依赖方维护其接受验证的验证装置的数据库。它可以利用AAID(或其他验证装置代码)查询此数据库以确定正在预置的验证装置是否可接受进行验证。如果是，那么它将继续进行注册过程。

[0037] 在一个实施例中，依赖方202为被预置的每个验证装置生成验证密钥。它向安全数据库写入密钥，并利用密钥预置协议向验证客户端201发回密钥。一旦完成，验证装置与依赖方202便在使用对称密钥的情况下共享相同密钥，或者在使用不对称密钥的情况下共享不同密钥。例如，如果使用不对称密钥，那么依赖方202可以存储公共密钥并向验证客户端201提供私有密钥。在从依赖方202接收私有密钥时，验证客户端201向验证装置中预置密钥(在与验证装置相关联的安全存储装置之内存储密钥)。然后它可以在验证用户期间使用该密钥(如下所述)。在一个另选的实施例中，密钥由验证客户端201生成并使用密钥预置协议向依赖方202提供密钥。在任一种情况下，一旦完成预置，验证客户端201和依赖方202均具有密钥，且验证客户端201通知依赖方已完成。

[0038] 图3示出了用于向预置的验证装置验证用户的一系列交易。一旦完成装置注册(如图2中所述)，依赖方201将接受由客户端上的本地验证装置生成的验证响应(有时称为“令牌”)作为有效的验证响应。

[0039] 转向图3中所示的具体细节，响应于用户发起与依赖方202的需要验证的交易(例如，发起从依赖方网站进行支付，访问私有用户账户数据等)，依赖方202生成包括随机质询(例如，密码随机数)的验证请求。在一个实施例中，随机质询具有与其关联的时间限制(例如，它在指定的一段时间内是有效的)。依赖方还可以标识要由验证客户端201用于验证的验证器。如上所述，依赖方可以预置客户端上可用的每个验证装置并为每个预置的验证器存储公共密钥。因此，它可以使用验证器的公共密钥或可以使用验证器ID(例如，AAID)来标识要使用的验证器。或者，它可以为客户端提供验证选项的列表，用户可以从该列表进行选择。

[0040] 响应于接收到验证请求，可以为用户呈现请求验证的图形用户界面(GUI)(例如，形式为验证应用/应用的网页或GUI)。用户然后进行验证(例如，在指纹读取器上轻扫手指等)。作为响应，验证客户端201生成验证响应，该验证响应包含随机质询上的签名，带有与验证器相关联的私有密钥。它还可以包括其他相关数据，例如，验证响应中的用户ID代码。

[0041] 在接收验证响应时，依赖方可以证实随机质询上的签名(例如，使用与验证器相关

联的公共密钥)并确认用户的身份。一旦完成验证,用户便获许进入与依赖方的安全交易,如图所示。

[0042] 可以使用安全通信协议,例如传输层安全(TLS)或安全套接字层(SSL)在依赖方201和验证客户端202之间建立用于图2至图3所示的任何或所有交易的安全连接。

[0043] 利用非对称加密实施一次性密码的系统和方法

[0044] 下文所述的本发明的实施例包括用于利用非对称加密实施一次性密码(OTP)的技术。OTP方案通常基于对称密钥加密,其中客户端实体和服务器实体共享单个对称密钥,并且使用相同的密钥获得该OTP。相比之下,本发明所公开的实施例基于非对称密钥,其允许实施更安全的服务器而不需要存储秘密。

[0045] 目前广泛使用的一次性密码(OTP)方案有三种类型:(1)基于时间的OTP(TOTP);(2)基于计数器的OTP;(3)基于质询/响应的OTP。当前的解决方案针对所有这些类型的OTP使用基于对称密钥的方案。在该方案中,使用相同的对称密钥提前预置OTP装置和服务器。作为验证事件的响应,该OTP装置基于(1)时间,(2)内置计数器或(3)服务器提供的质询来生成特殊的加密响应,并将该响应提供给服务器以进行核验。然后,服务器使用相同的对称密钥来获得相同的加密值,并将其与OTP装置提供的加密值进行比较。如果这些加密值匹配,则认为验证成功。

[0046] 一个特定的案例涉及“离线”验证,其适用于OTP装置不与服务器直接连接的场景。在OTP装置生成加密响应后,将响应截断为6位数字,然后显示给用户。用户将该6位数字输入客户端装置,客户端装置将此数字发送至服务器。然后,服务器使用相同的截断算法来获得相同的数字。获得数字之后,其将所获得的数字与OTP装置生成的数字进行比较。然而,由于服务器存储着密钥,因此它是黑客的攻击目标。维护服务器中的密钥通常需要在数据中心使用昂贵的硬件安全模块(HSM)。

[0047] 本发明的一个实施例实施基于非对称加密的OTP方案。非对称加密的优点是服务器将存储公共密钥而不是私有密钥(如对称密钥)。这消除了保护服务器中密钥的机密属性的负担,并允许更容易、更安全的部署。

[0048] 图4提供了根据本发明的一个实施例的系统架构的概述。在本实施例中,用户装置401是存储私有密钥并生成验证断言的实体,并且连接装置410是与依赖方验证服务器402和用户装置401都具有连接的实体。例如,在一个实施例中,用户装置401可以是移动装置诸如iPhone™或Android™,并且连接装置410可以是台式计算机、销售点(PoS)终端、自动取款机(ATM),或与依赖方验证服务器402具有连接的任何其他装置。

[0049] 在一个实施例中,验证服务器402存储与由用户装置401存储的私有密钥相对应的公共密钥。可使用上面相对于图2所讨论的密钥预置技术(例如,使用DSKPP或其他密钥预置协议)在用户装置401和验证服务器402上预置密钥。

[0050] 在一个实施例中,与用户装置401的连接是单向的;也就是说,用户装置401可从连接装置410读取消息,但不能发送消息。例如,连接装置410可显示二维(QR)码、条形码或其他光学代码,以向用户装置401传递信息(例如,下面讨论的加密的质询)。用户装置401可使用已知技术(例如,用相机或扫描仪装置捕获光学代码)来读取和解译光学代码。

[0051] 在一个替代实施例中,用户装置401和连接装置410之间的连接是使用局域通信技术诸如近场通信(NFC)、蓝牙(例如,低功耗蓝牙(BTLE))或无线USB实施的双向连接。

[0052] 在一个实施例中，依赖方验证服务器402是核验由用户装置401生成的加密断言的实体。然而，用户装置401不需要与验证服务器402具有直接连接。本发明的实施例包括两个阶段：预置和验证。在预置阶段中，向用户装置401和验证服务器402预置加密密钥(例如，使用如图2所示的密钥预置技术)。然而，与现有的OTP方案不同，在预置期间，验证服务器402被提供有公共密钥，并且用户装置401被提供有私有密钥。

[0053] 假设用户装置401已经被提供有私有密钥，并且验证服务器402被提供有对应的公共密钥，本发明的一个实施例根据图5所示的交易图操作。

[0054] 在501处，依赖方验证服务器402生成随机质询(C)，并且使用与存储在用户装置401上的私有密钥相对应的公共密钥对其进行加密：EC＝加密(公共密钥，C)，其中C是随机质询，EC是加密的质询。验证服务器402将C存储在其存储器中，并且将EC发送到如图所示的将EC传送到用户装置401的连接装置410。

[0055] 在502处，用户装置401利用其私有密钥解密EC，并获得随机询问：C＝解密(私有密钥，EC)。用户装置401然后将C转换为简化值，诸如缩短版本的C(“ShortC”)。在一个实施例中，这通过将C截断成N位数字(例如，其中N＝6)来实现：ShortC＝截断(C)。然而，在仍符合本发明的基本原理的情况下，可实施各种其他技术以将C转换成ShortC。例如，在一个实施例中，可从C中选择来自某些指定位位置的位，并将其组合以形成ShortC。

[0056] 在503处(例如，在用户装置401的显示器上)向用户400呈现ShortC之后，用户400在连接装置410上输入ShortC，该连接装置在验证响应消息中将其发送回验证服务器402。用户装置401还可以请求用户在该阶段执行验证(例如使用用户装置401上的验证器，诸如指纹读取器)。

[0057] 在504处，在接收到包含ShortC的验证响应消息时，验证服务器从存储器读取C，并且使用与用户装置401相同的算法截断C。例如：ShortC_Server＝截断(C)(如果截断用于生成ShortC)。然后，验证服务器402将从用户装置401接收的ShortC与ShortC_Server进行比较。如果它们匹配，则该用户验证成功。如果不匹配，则验证失败。

[0058] 图6A中示出了验证服务器402的一个实施例。如图所示，与用户装置上的私有密钥相关联的公共密钥605可被存储在安全存储器604中，并且由加密模块603使用以加密随机质询(C)606。如所指出的那样，随机数发生器601可用于生成C 606，所述C然后可被存储在安全存储器604中(并且随后在接收到验证响应时被检索)。如上所述，随后将加密的随机质询(EC)发送到连接装置。

[0059] 图6B示出了验证服务器402的一个实施例中，用于证实用户610发送的包括ShortC的验证响应的组件。在一个实施例中，转换逻辑608从存储器604读取C，并且使用与用户装置401所使用的算法相同的算法截断C以生成ShortC：ShortC_Server＝截断(C)。比较器逻辑615然后将接收自用户的ShortC 610与ShortC_Server进行比较。如果它们匹配，则该用户验证成功。如果不匹配，则验证失败。

[0060] 图7示出了根据本发明的一个实施例的在用户装置401上采用的逻辑。解密模块703使用存储在安全存储器704中的私有密钥705对由验证服务器402发送的加密的质询(EC)600进行解密。如上所述，私有密钥705对应于用于执行加密的公共密钥605。然后，转换模块706转换解密的随机质询C，从而得到呈现给用户的ShortC 710。如上所述，虽然在一个实施例中使用截断，但是本发明的基本原理不限于任何特定类型的二进制或数字转换。

[0061] 虽然上面阐述了若干个具体细节，但是在仍然符合本发明的基本原理的情况下，可采用各种不同的加密实施、转换技术和随机质询。例如，非对称算法可以是一种公共密钥加密算法，诸如RSA、椭圆曲线加密法(ECC)或使用非对称密钥实施加密的其他算法。在一个实施例中，使用密钥长度为128或256位的高级加密标准(AES)。另外，连接装置410可经由QR码、NFC、蓝牙、WiFi或任何其他通信技术将EC传送到用户装置401。

[0062] 在一个实施例中，验证服务器402并非如上所述明确存储C，而是通过并入机制(诸如时间戳、换行以及类似的技术)将其与EC一起发送至客户端装置401用于进一步验证。例如：

[0063] C'＝E(服务器换行密钥，C|时间戳)并且EC＝E(公共密钥，C)

[0064] 此外，上述依赖方(即，具有用于实施本发明实施例的验证服务器的实体)可以是包括在线服务提供商、在线零售服务或企业服务器的任何实体。

[0065] 在一个实施例中，在连接装置410上运行并与验证服务器402通信的软件可在Web浏览器或专有应用程序(例如，专门设计用于与依赖方及其验证服务器通信的应用程序)中实施。另外，在用户装置上运行的软件(参见例如图7)，从连接装置读取EC 600并显示ShortC可在Web浏览器或专有应用程序中实施。此外，在一个实施例中，驻留在用户装置401上用于安全保护私有密钥705并获得ShortC而不向其他组件泄露私有密钥的逻辑，在硬件中实施或者作为固件在加密硬件(诸如智能卡)上实施。

[0066] 示例性数据处理装置

[0067] 图8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8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。

[0068] 如图8所示，计算机系统800，其为一种形式的数据处理系统，包括总线850，该总线与处理系统820、电源825、存储器830和非易失性存储器840(例如，硬盘驱动器、快闪存储器、相变存储器(PCM)等)耦接。总线850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820可从存储器830和/或非易失性存储器840检索指令，并执行这些指令以执行如上所述的操作。总线850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860、显示控制器与显示装置870、输入/输出装置880(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890(例如，蓝牙、WiFi、红外等)。

[0069] 图9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900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900可为网络计算机或在另一个装置内的嵌入式处理装置。

[0070] 根据本发明的一个实施例，数据处理系统900的示例性架构可用于上文所述的移动装置。数据处理系统900包括处理系统920，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920与存储器910、电源925(其包括一个或多个电池)、音频输入/输出940、显示控制器与显示装置960、可选输入/输出950、输入装置970和无线收发器930耦接。应当理解，在本发明的某些实施例中，图9中未示出的其他组件也可为数据处理系统900的

一部分，并且在本发明的某些实施例中，可使用比图9所示更少的组件。另外，应当理解，图9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。

[0071] 存储器910可存储数据和/或程序以供数据处理系统900执行。音频输入/输出940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960可包括图形用户界面(GUI)。无线(例如，RF)收发器930(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970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950可为底座的连接器。

[0072] 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。

[0073] 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。

[0074] 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。

[0075] 本发明的实施例可包括如上文陈述的各种步骤。这些步骤可体现为致使通用处理器或专用处理器执行某些步骤的机器可执行指令。或者，这些步骤可由包含用于执行这些步骤的硬连线逻辑的特定硬件组件执行，或由编程的计算机组件和定制硬件组件的任何组合执行。

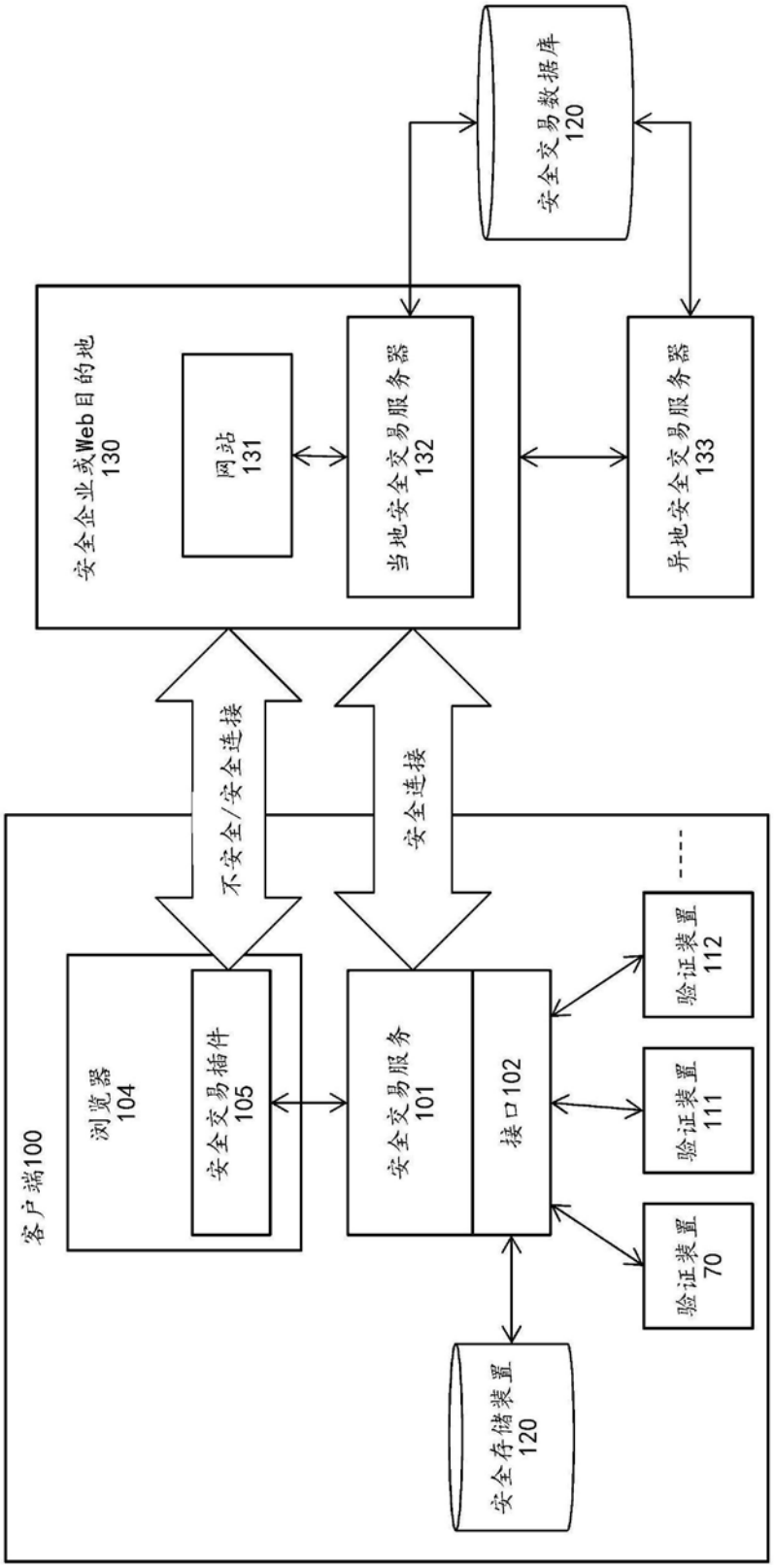

安全交易数据库
120
安全企业或Web目的地
130
网站
131
当地安全交易服务器
132
异地安全交易服务器
133
不安全/安全连接
安全连接
客户端100
浏览器
104
安全交易插件
105
安全交易服务
101
接口102
验证装置
112
验证装置
111
验证装置
70
安全存储装置
120

图1A

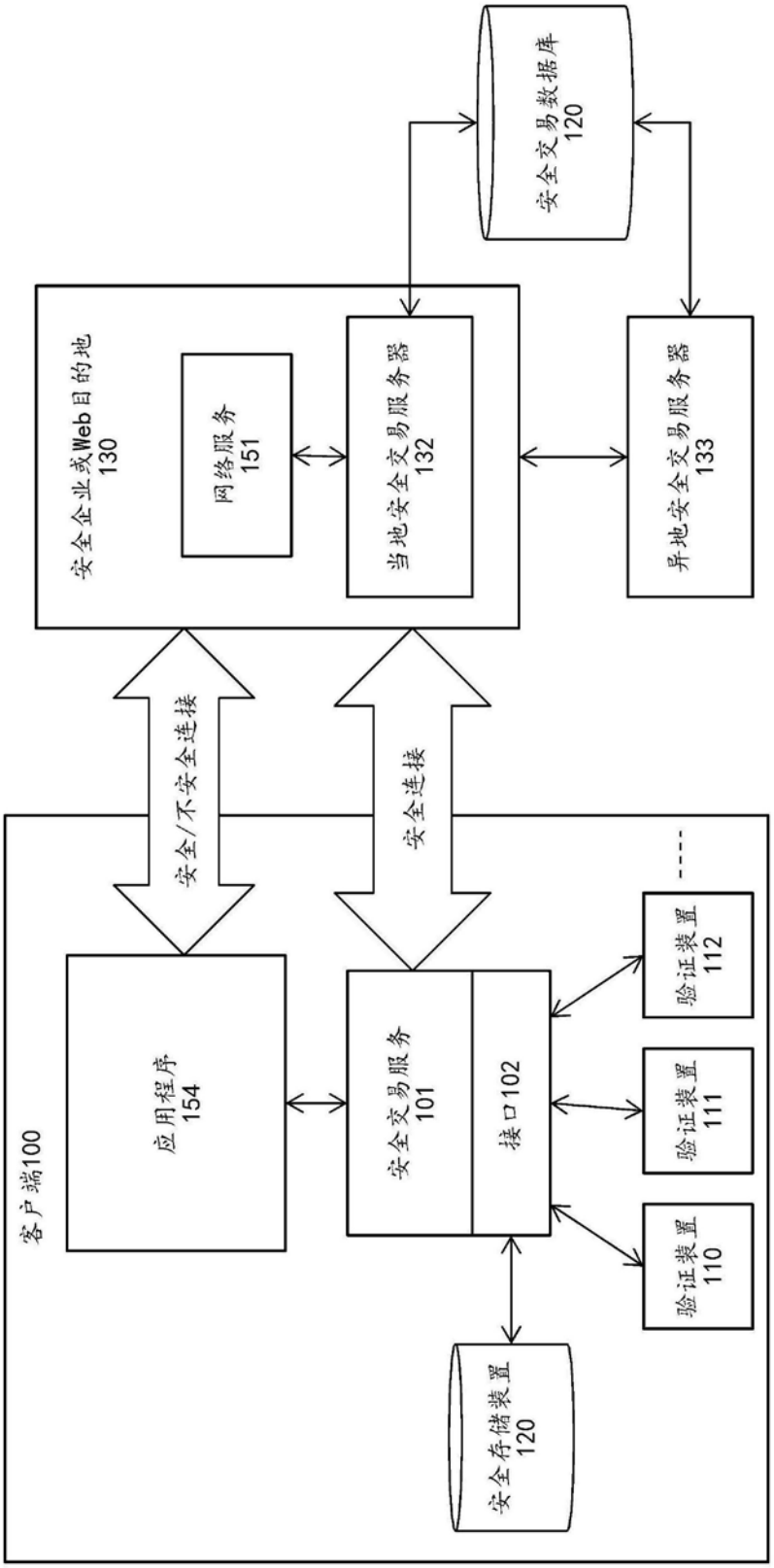

安全交易数据库
120
安全企业或Web目的地
130
网络服务
151
当地安全交易服务器
132
异地安全交易服务器
133
安全/不安全连接
安全连接
客户端100
应用程序
154
安全交易服务
101
接口102
验证装置
112
验证装置
111
验证装置
110
安全存储装置
120

图1B

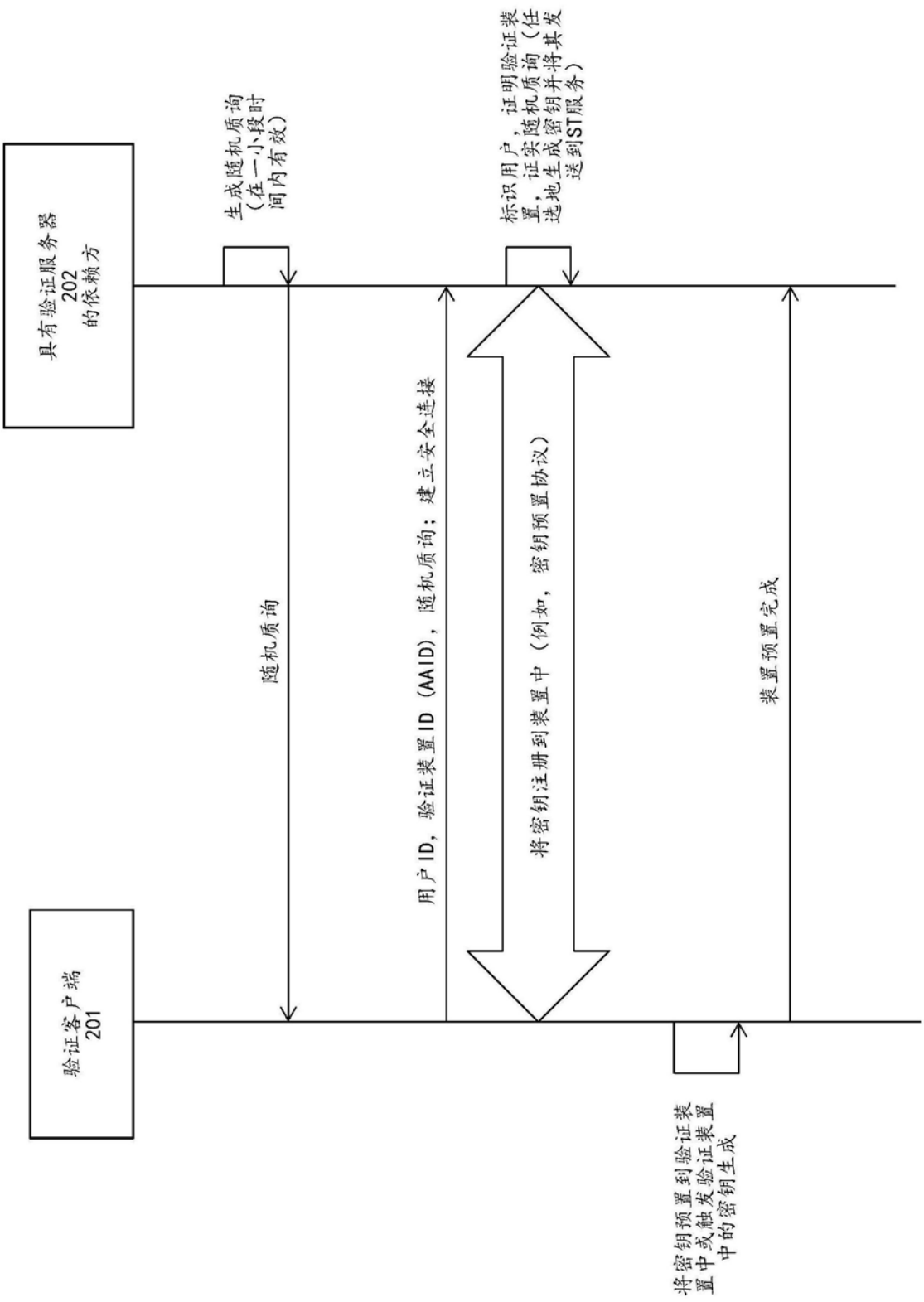

具有验证服务器
202
的依赖方
验证客户端
201
生成随机质询
（在一小段时
间内有效）
标识用户，证明验证装
置，证实随机质询（任
选地生成密钥并将其发
送到ST服务）
随机质询
用户ID，验证装置ID（AAID），随机质询；建立安全连接
将密钥注册到装置中（例如，密钥预置协议）
装置预置完成
将密钥预置到验证装
置中或触发验证装置
中的密钥生成

图2

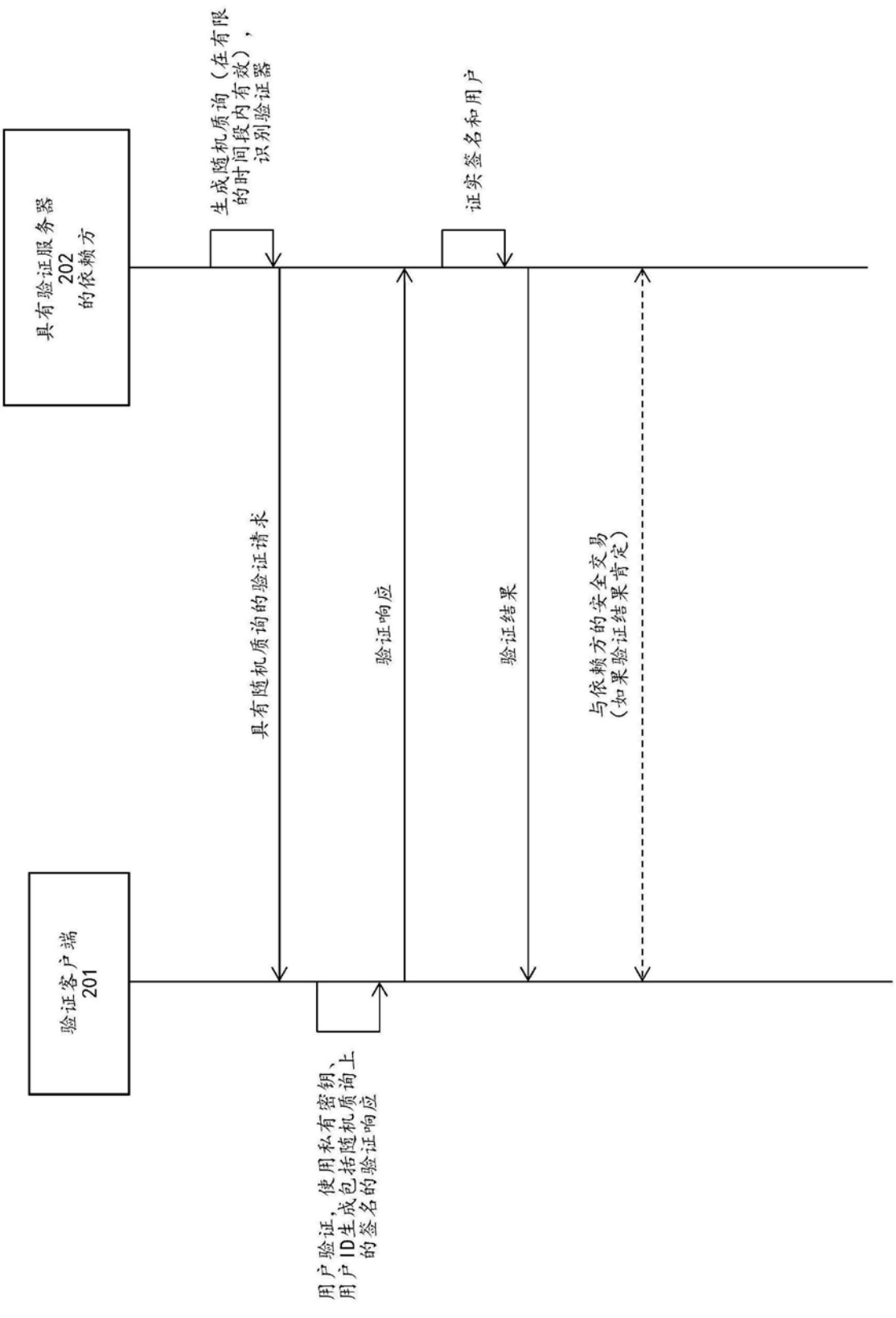

具有验证服务器
202
的依赖方
验证客户端
201
生成随机质询（在有限
的时间段内有效），
识别验证器
证实签名和用户
具有随机质询的验证请求
验证响应
验证结果
与依赖方的安全交易
（如果验证结果肯定）
用户验证，使用私有密钥、
用户ID生成包括随机质询上
的签名的验证响应

图3

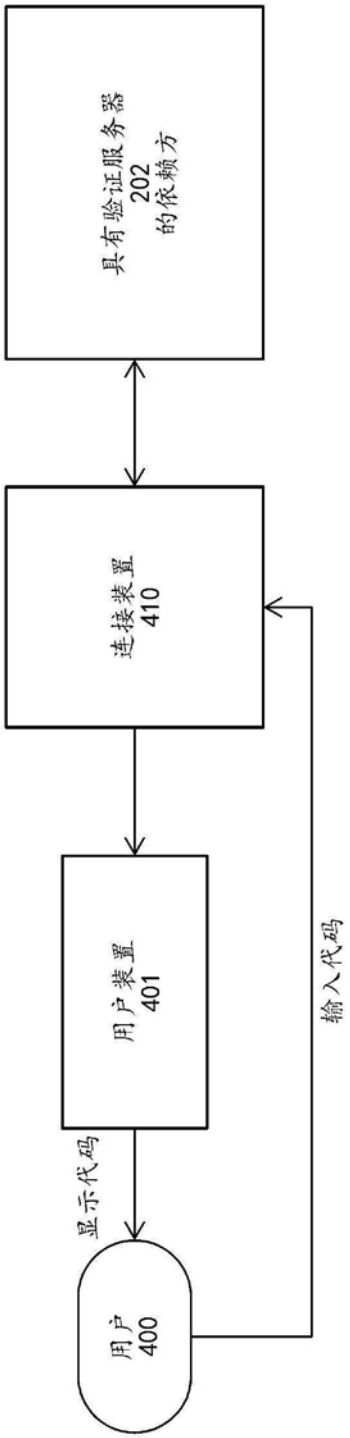


图4

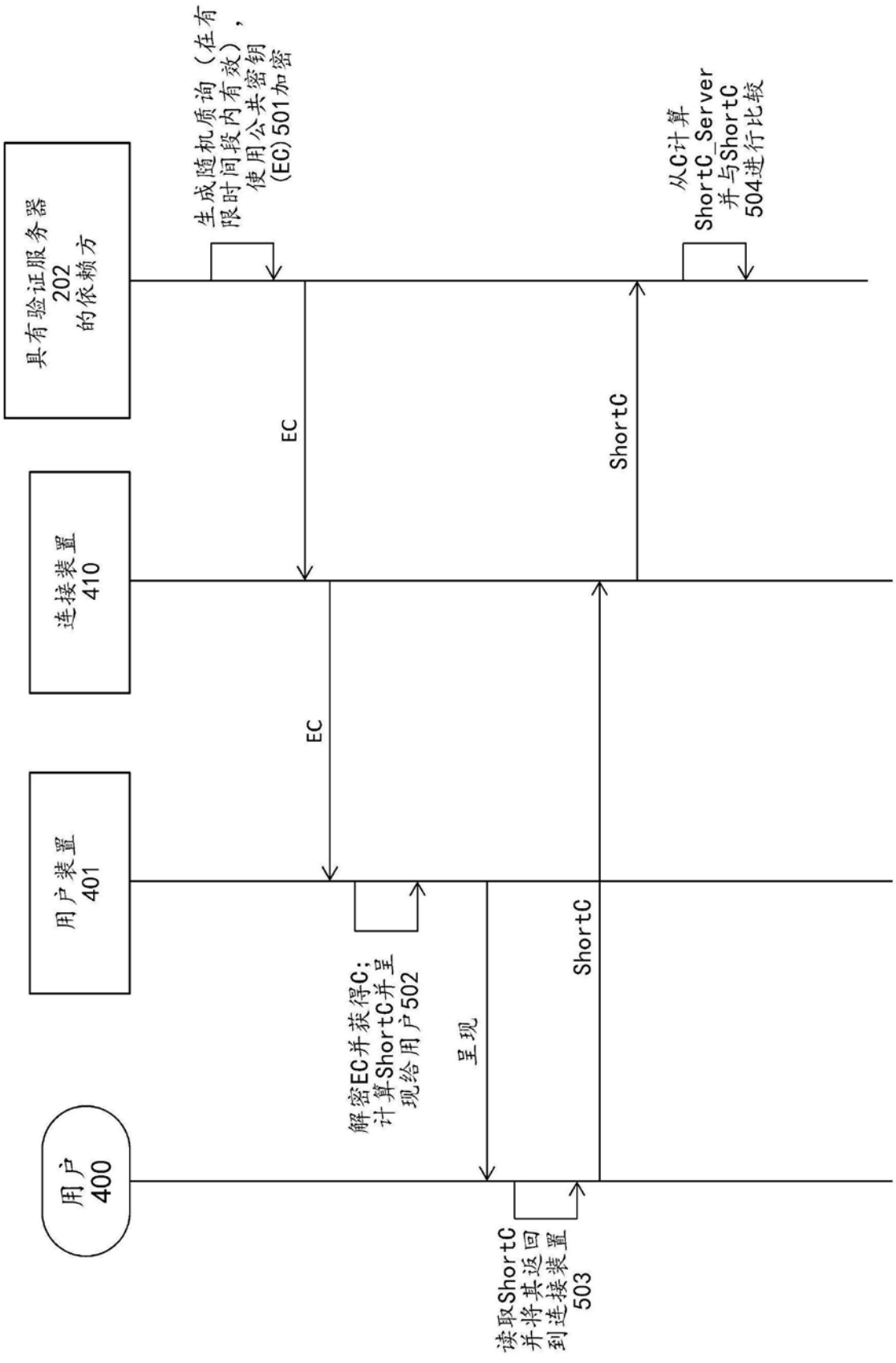

具有验证服务器
202
的依赖方
连接装置
410
用户装置
401
用户
400
生成随机质询（在有限时间段内有效），使用公共密钥(EC)501加密
EC
EC
解密EC并获得C；计算ShortC并呈现给用户502
呈现
读取ShortC并将其返回到连接装置503
ShortC
ShortC
从C计算ShortC_Server并与ShortC504进行比较

图5

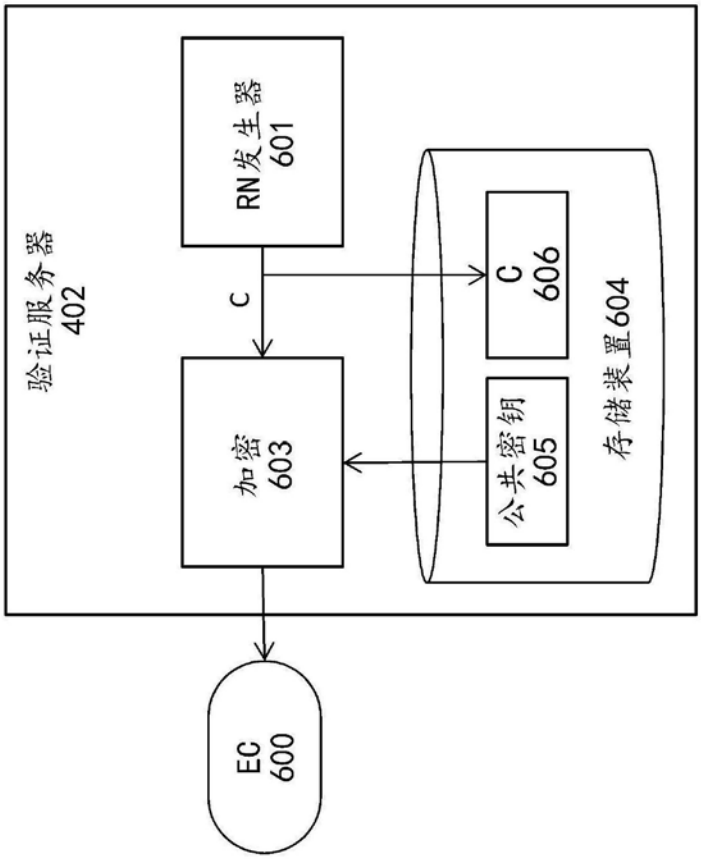


图6A

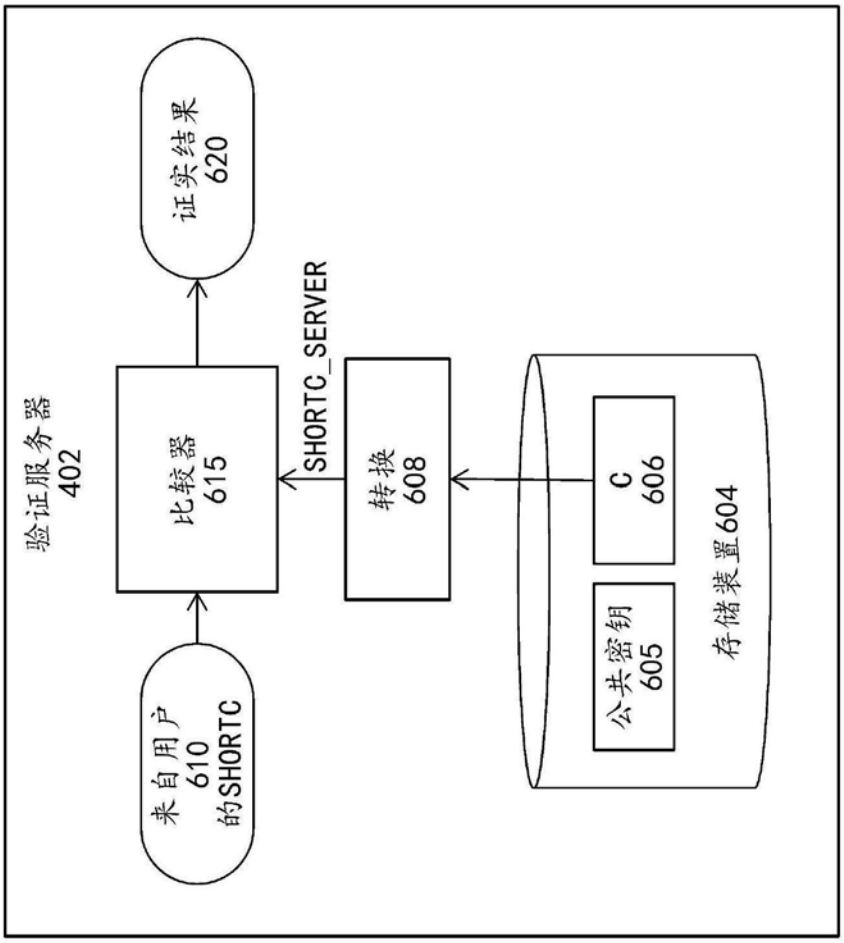

验证服务器
402
来自用户
610
的SHORTC
比较器
615
证实结果
620
SHORTC_SERVER
转换
608
C
606
公共密钥
605
存储装置604

图6B

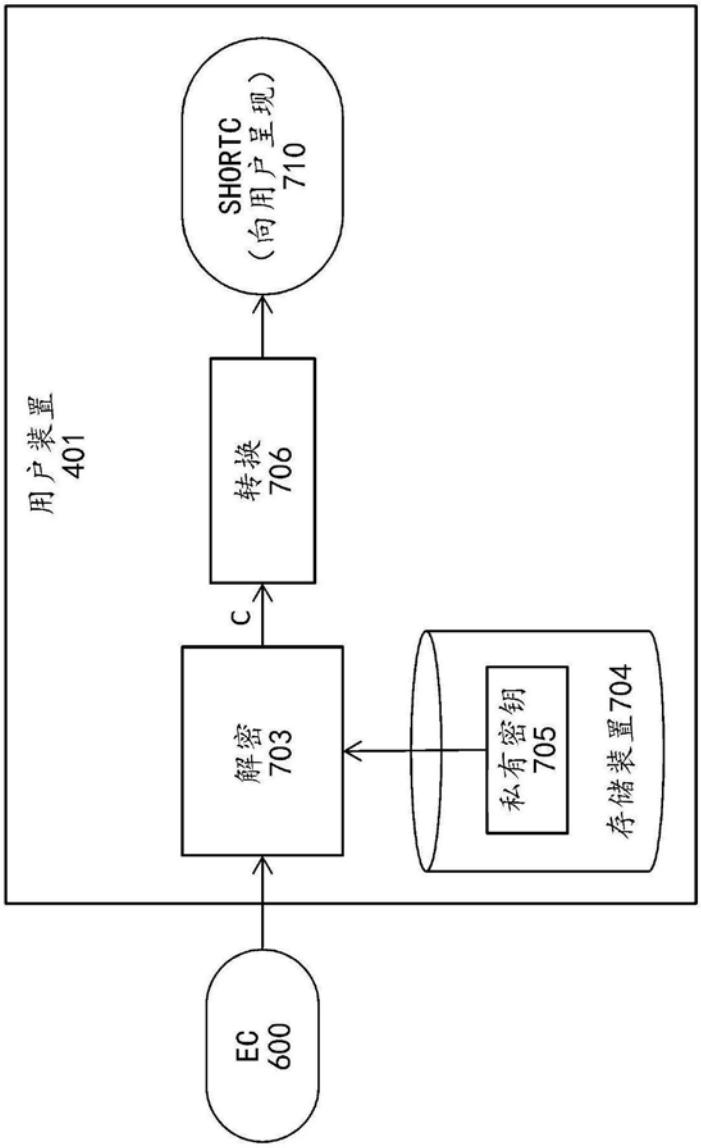

SHORTC
（向用户呈现）
710
转换
706
C
解密
703
私有密钥
705
存储装置704
用户装置
401
EC
600

图7

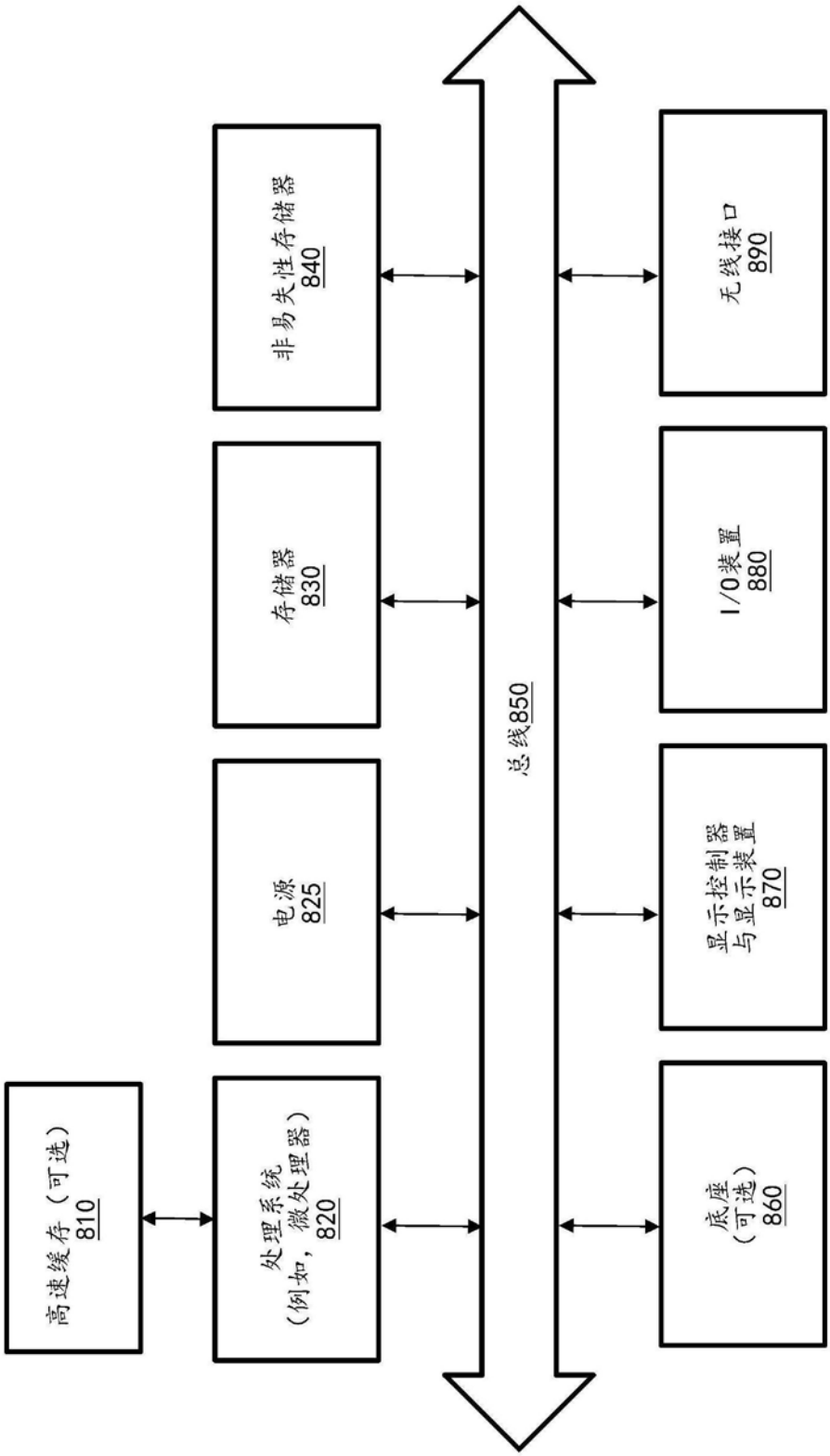

高速缓存（可选）
810
处理系统
（例如，微处理器）
820
电源
825
存储器
830
非易失性存储器
840
总线850
底座
（可选）
860
显示控制器
与显示装置
870
I/O装置
880
无线接口
890

图8

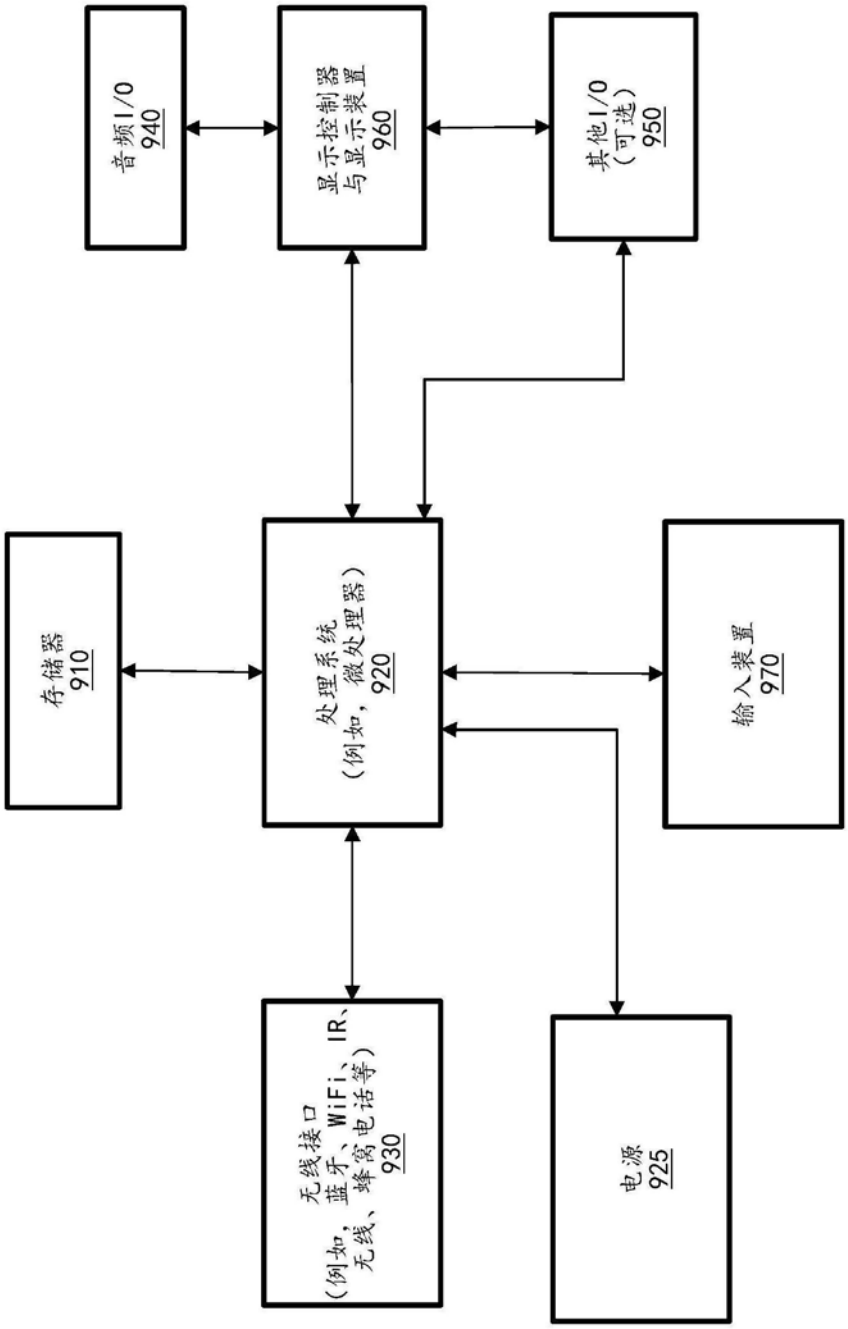

音频I/O
940
显示控制器
与显示装置
960
其他I/O
(可选)
950
存储器
910
处理系统
(例如，微处理器)
920
输入装置
970
无线接口
(例如，蓝牙、WiFi、IR、
无线、蜂窝电话等)
930
电源
925

图9