(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110383757 A
(43)申请公布日 2019.10.25

(21)申请号 201680091615.7

(22)申请日 2016.12.16

(85)PCT国际申请进入国家阶段日
2019.06.14

(86)PCT国际申请的申请数据
PCT/US2016/067191 2016.12.16

(87)PCT国际申请的公布数据
WO2018/111302 EN 2018.06.21

(71)申请人 维萨国际服务协会
地址 美国加利福尼亚州

(72)发明人 Q·王

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈洁 钱慰民

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/06(2006.01)

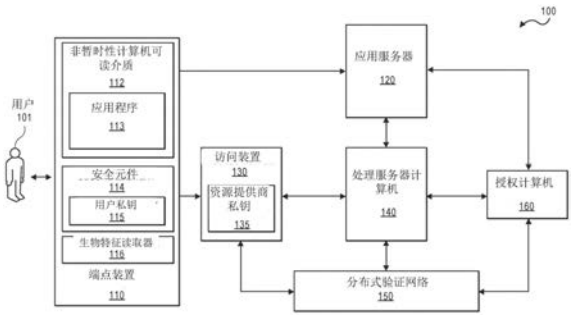
权利要求书2页 说明书18页 附图5页

(54)发明名称

用于安全处理电子身份的系统和方法

(57)摘要

本发明公开了一种用于使用端点装置提供识别的方法。端点装置可以包括唯一且可以被安全存储的电子身份。电子身份连同签名的交互数据和密码可以传递到访问装置。访问装置可以生成具有所述密码的授权请求,并且可以将其发送到远程服务器计算机进行进一步处理。



CN 110383757 A

1.一种方法,其包括:

由端点装置从访问装置接收交互数据;

由所述端点装置生成包括所述交互数据和用户的电子身份的交互记录,所述电子身份从与所述用户相关联的信息的组合用数学方法导出;

由所述端点装置检索所述用户的私钥;

由所述端点装置使用所述用户的私钥对所述交互记录进行签名;

由所述端点装置使用与限制使用参数相关联的限制使用密钥至少对所述交互数据进行加密,以形成密码;以及

由所述端点装置向所述访问装置传输所述密码和签名的交互记录,其中所述密码随后在授权请求消息中被转发到服务器计算机,并且其中所述服务器计算机被配置成解密所述密码并且验证所述电子身份。

2.根据权利要求1所述的方法,其中还使用资源提供商的私钥对所述交互记录进行签名,并且所述交互记录还包括交易时间戳。

3.根据权利要求1所述的方法,其中所述密码对交易金额、不可预知数和应用交易计数器进行编码。

4.根据权利要求1所述的方法,其中所述端点装置包括生物特征读取器。

5.根据权利要求1所述的方法,所述服务器计算机利用分布式网络验证所述电子身份,所述分布式网络包括区块链。

6.根据权利要求1所述的方法,其中至少对所述交互数据进行加密包括至少对包括所述电子身份的交互记录进行加密。

7.根据权利要求1所述的方法,其中所述电子身份是与所述用户相关联的信息的散列。

8.根据权利要求1所述的方法,其中所述授权请求消息是ISO 8583消息。

9.根据权利要求1所述的方法,还包括:

由所述端点装置接收所述用户的生物特征样本;

由所述端点装置将所接收的生物特征样本与存储的生物特征样本比较,并且确定生物特征所接收的生物特征样本与所述存储的生物特征样本匹配。

10.根据权利要求1所述的方法,其中所述端点装置是移动电话。

11.一种端点装置,包括:

处理器;以及

非暂时性计算机可读介质,所述非暂时性计算机可读介质包括代码,所述代码用于指示所述处理器执行一种方法,所述方法包括:

由所述端点装置从访问装置接收交互数据,

由所述端点装置生成包括所述交互数据和用户的电子身份的交互记录,所述电子身份从与所述用户相关联的信息的组合用数学方法导出,

由所述端点装置检索所述用户的私钥,

由所述端点装置使用所述用户的私钥对所述交互记录进行签名,

由所述端点装置使用与限制使用参数相关联的限制使用密钥至少对所述交互数据进行加密,以形成密码,以及

由所述端点装置向所述访问装置传输所述密码和签名的交互记录,其中所述密码随后

在授权请求消息中被转发到服务器计算机，并且其中所述服务器计算机被配置成解密所述密码并且验证所述电子身份。

12.根据权利要求11所述的端点装置，其中还使用资源提供商的私钥对所述交互记录进行签名，并且所述交互记录还包括交易时间戳。

13.根据权利要求11所述的端点装置，所述服务器计算机利用分布式网络验证所述电子身份，所述分布式网络包括区块链。

14.根据权利要求11所述的端点装置，其中传输还包括传输密钥索引。

15.根据权利要求11所述的端点装置，其中从应用服务器检索所述限制使用密钥。

16.根据权利要求11所述的端点装置，所述电子身份是与所述用户相关联的信息的散列。

17.根据权利要求16所述的端点装置，其中所述授权请求消息是ISO8583消息。

18.一种被配置成处理用户的电子身份的服务器计算机，所述服务器计算机包括：

网络接口；

处理器；

非暂时性计算机可读介质，所述非暂时性计算机可读介质包括代码，所述代码用于指示所述处理器执行一种方法，所述方法包括：

从访问装置接收包括密码和动态数据集的授权请求消息，其中所述密码包括加密的交互数据和用户的电子身份；

基于所述动态数据集确定与限制使用参数相关联的限制使用密钥；

使用所述限制使用密钥解密所述密码；

验证与所述限制使用密钥相关联的限制使用参数；

验证所述用户的电子身份；以及

如果所述电子身份和所述限制使用参数得到验证，则批准所述授权请求消息或将所述授权请求消息转发给授权实体。

19.根据权利要求18所述的服务器计算机，其中所述电子身份也被加密并且是所述密码的一部分。

用于安全处理电子身份的系统和方法

背景技术

[0001] 在当今的技术环境中，用户通过将认证数据注册到可确认注册用户的服务提供商来认证其身份，这是很常见的。如果确定用户是值得信赖的，并且应获得授权，则注册的认证数据被用户使用来获得对资源的访问。

[0002] 例如，个人可能希望建立一个追踪其资产(例如现金或财产所有权)的账户。此账户可以由诸如银行的中央机构管理，中央机构在中央数据库中存储关于用户的认证数据。然后，用户可使用认证数据证明其身份，并显示对账户及其中资产的所有权证明。当用户希望进入入口或访问资源时，用户可以向资源的提供商呈现注册的认证数据(例如，名称和账号)。然后，资源提供商可以将认证数据转发给中央机构，以便机构可以认证注册的账户持有人的身份，并确定是否存在足够的资产量可足以支付资源(即大于交易金额的资金量)。然后，中央机构可以决定授权交易，从而向资源提供商提供其将得到充分报酬的保证。

[0003] 以这种方式运行的大多数授权系统要求用户维护许多不相同的认证数据，以便管理属于同一个所有者的分散在许多个账户的资产。例如，用户可以向许多信用机构展示其身份(姓名、地址、社会保障号码等)，然后可以收到注册给他的多个信用卡号码，以便跟踪在每次交易期间资产和信用移动的方式。这可能使账户注册和使用对用户而言很繁琐，因为涉及多个账户的维护，每个账户在不相同的数据库中被管理。

[0004] 此外，在交易期间，认证数据(例如，信用卡号、地址等)必须在某种程度上保密，以便数据不能被窃取并用于盗窃某人的身份，并获得其资产。通常，会执行令牌化计划和别名到隐藏认证数据的映射，以隐藏敏感信息。这能证明既费用高又不安全，原因是映射和存储需要由专用的中央服务器和数据库执行，专用的中央服务器和数据库可能会被黑客攻击，从而暴露每个人的认证数据和身份。黑客也可以以这种方式改变记录，这可能难以争辨，因为记录可能只存在于现在受损的单个位置。此外，提供了认证数据的装置也可能被黑客侵入或窃取，并且可以被假装为用户的个人使用。

[0005] 本发明的实施例单独地以及共同地解决这些问题和其它问题。

发明内容

[0006] 本公开的实施例涉及用于安全处理电子身份的系统和方法。

[0007] 本发明的一个实施例涉及一种方法，由端点装置从访问装置接收交互数据；由所述端点装置生成包括所述交互数据和用户的电子身份的交互记录，所述电子身份从与所述用户相关联的信息的组合用数学方法导出；由所述端点装置检索所述用户的私钥；由所述端点装置使用所述用户的私钥对所述交互记录进行签名；由所述端点装置使用与限制使用参数相关联的限制使用密钥对至少所述交互数据加密，以形成密码；以及由所述端点装置向所述访问装置传输所述密码和签名的交互记录，其中所述密码随后在授权请求消息中被转发到服务器计算机，并且其中所述服务器计算机被配置成解密所述密码并验证所述电子身份。

[0008] 本发明的另一实施例涉及被配置成执行上述方法的服务器计算机。

[0009] 本发明的另一实施例涉及一种方法。所述方法包括:从访问装置接收包括密码和动态数据集的授权请求消息,其中所述密码包括加密的交互数据和用户的电子身份;基于所述动态数据集确定与限制使用参数相关联的限制使用密钥;使用所述限制使用密钥解密所述密码;验证与所述限制使用密钥相关联的限制使用参数;验证所述用户的电子身份;如果所述电子身份和所述限制使用参数得到验证,则批准所述授权请求消息或将所述授权请求消息转发给授权实体。

[0010] 下文进一步详细描述本发明的这些和其它实施例。

附图说明

[0011] 图1示出根据本发明的实施例的用于进行交易的系统的框图。

[0012] 图2示出根据本发明的实施例的处理服务器计算机的框图。

[0013] 图3示出根据本发明的实施例的注册和提供方法的泳道图。

[0014] 图4示出根据本发明的实施例的交易过程的泳道图。

[0015] 图5描绘根据本发明的实施例的电子记录的示例。

[0016] 图6示出根据本发明的实施例的用于验证交易的过程流程图。

[0017] 图7示出根据本发明的实施例的用于安全处理电子身份的方法的流程图。

具体实施方式

[0018] 本发明的实施例涉及安全处理电子身份。在一些实施例中,可以安全地存储电子身份,并且在展示个人身份的证据时诸如通过生物特征验证时,可以使用电子身份。可以使用电子身份识别交互记录中的互动方,该交互记录被添加到不可改变的电子记录中。在本发明的实施例中,在交互记录被传输以进行处理时,交互记录可以被加密,并且仅当满足特定的限制使用参数时有效。

[0019] 本发明的实施例解决了典型授权系统中可能存在的多个缺陷。首先,根据本发明的实施例,交互记录可以包括使用私钥创建的签名。私钥可以是用户唯一的,并且可以存储在只能由用户使用生物特征验证访问的安全元件中。这防止个人在未经用户同意的情况下代表用户进行交互。

[0020] 其次,交互记录可以被加密,因此阻止未经授权人员拦截交互记录并改变或使用交互记录的内容,例如以欺诈方式使用电子身份。在一些实施例中,可使用由限制使用参数限定的限制使用密钥来加密交互记录。这可能限制如果端点装置和用户生物特征数据都受到某种损害时未授权个人可能会造成的危害。

[0021] 最后,在本发明的实施例中,可以通过可信实体的分布式网络验证电子身份。分布式网络中的每个实体可以拥有公共验证密钥,该密钥可以用于确认由存储在端点装置的安全元件中的私钥生成的签名。每个可信实体还可以验证电子记录中的交互记录。

[0022] 在论述本发明的一些实施例的细节之前,对一些术语的描述可有助于理解各种实施例。

[0023] “服务器计算机”可包含功能强大的计算机或计算机集群。例如,服务器计算机可以是大型主机、小型计算机集群或作为一个单元运作的一组服务器。在一个实例中,服务器计算机可以是耦合到网络服务器的数据库服务器。服务器计算机可耦连到数据库,且可包

含用于服务于来自一个或多个客户端计算机的请求的任何硬件、软件、其它逻辑，或前述内容的组合。服务器计算机可包括一个或多个计算设备，并可使用多种计算结构、布置和编译中的任一种来服务于来自一个或多个客户端计算机的请求。

[0024] “应用服务器”可以是被配置成为端点装置提供远程支持的任何计算装置。应用服务器可以与安装在端点装置上并且从端点装置执行的计算机可执行指令集(例如，移动应用程序)相关联。应用服务器可以为端点装置提供任何合适的服务和/或处理。例如，应用服务器可代表端点装置执行计算。在一些实施例中，应用服务器可维护一个或多个用户的账户。在一些情况下，应用服务器可以能够为个体生成电子身份，这可以用于在交互期间认证个体。应用服务器还可存储与端点装置的操作有关的任何协议和/或用户偏好。

[0025] “端点装置”可以是能够与另一电子装置(例如，应用服务器)建立通信会话且传输/接收来自所述装置的数据的任何电子装置。端点装置可具有下载和/或执行移动应用程序的能力。端点装置可以包括移动通信装置(例如，手机)、个人计算机、笔记本电脑、可穿戴设备和/或物联网设备，例如智能电视、冰箱、恒温器等。端点装置的其它示例可以包括具有远程通信功能的移动车辆(例如，汽车、摩托车、船舶等)。

[0026] “移动通信装置”可以是具有与通信有关的主要功能的任何便携式电子装置。例如，移动通信装置可以是智能手机、个人数据助理(PDA)，或任何其它合适的手持装置。

[0027] “区块链”可以是一种分布式数据库，其维护不断增长的记录列表，以防篡改和修订。区块链可以包含多个交互记录区块。区块链中的每个区块还可以包含时间戳和上一个区块的链接。例如，每个区块可以包含或附加到上一个区块的散列。换句话说，区块链中的交易记录可存储为一系列“区块”或包含在给定时间周期内发生的数笔交易的记录的永久性文件。在区块完成并经过验证之后，可以通过合适的节点将区块附加到区块链。在本发明的实施例中，区块链可以是分布式的，并且可以在验证网络中的每个节点处维护区块链的副本。验证网络中的任何节点随后可以使用区块链来验证交易。区块链的安全性可以使用加密方案获得。

[0028] “密码密钥”可以是任何位串，以供密码算法使用以将明文变换成密文或将密文变换成明文。密码密钥可包含对称密钥和非对称密钥。密码密钥可用于对交易进行签名和/或验证签名的交易。例如，可使用私钥对密码货币交易进行签名。可接着使用对应于私钥的公钥来验证签名的交易。

[0029] “电子身份”可以是用于识别实体(例如，个人或装置)的任何合适的字符或符号串。在一些实施例中，电子身份可以从与用户相关联的信息用数学方法导出。例如，在一些实施例中，电子身份可以是通过对多个实体可用的一个或多个输入值(客户姓名、国家代码等)进行散列运算计算出的值。以此方式，电子身份可以由具有先决条件信息的任何实体独立生成。电子身份可以是被改变(例如，散列运算和/或加密)的与用户相关联的信息。例如，在一些实施例中，电子身份可以从国家代码、客户姓名、出生日期和社会保障号的最后四位数字的组合导出，例如SHA256(USA*JOHN SMITH*19700101*1234)。对此值进行散列运算可能导致看似随机的字符串，例如754WD2E2513BF546050C2D079FF5D65AB6E318E，这可以是电子身份。在一些实施例中，电子身份与密码相关联，所述密码是为了访问与电子身份相关联的任何交互记录提供的。电子身份有时可以称为“eID”或电子标识符。

[0030] “电子记录”可以是以电子方式存储的一个或多个交易的任何记录。例如，电子记

录可以包括与电子身份相关联的许多个交互记录。在一些实施例中，可以通过识别与特定电子身份相关联的分布式环境中记录的每个交互记录来编译电子记录。在一些实施例中，电子记录可以包括由电子身份相关联的用户生成的并使用与所述用户相关联的私钥签名的部分。在一些实施例中，电子记录可以是区块链的形式或者可以包括在区块链中。

[0031] “交互记录”可以是在与电子身份相关联的用户和另一实体之间发生的任何交易指示。在一些实施例中，电子记录中的每个交互记录都可以使用与所述实体相关联的私钥进行签名，使得可以使用与所述实体相关联的公钥来验证它们。交互记录可以包含用户特定信息的位置指示(例如，数据库表中的地址)。

[0032] “私钥”是一种由一方保密的密码密钥类型。私钥可用于对交易进行签名，使得可使用验证网络对其进行验证。

[0033] “公钥”可以是一种分发给某个实体或可供某个实体使用(而不是持有相应私钥的一方)的密码密钥类型。在一些实施例中，密钥可以是公开可用的，而在其它情况下，可以将密钥分发到网络中的节点，但网络本身可能无法供公众访问。公钥可供验证网络的节点使用，使得可由节点来对与公钥相关联的签名的交易进行验证。

[0034] 术语“验证”和其派生词可以指利用信息来确定基础主题在一组给定的情况下是否有效的过程。验证可以包含任何信息比较以确保某些数据或信息是正确的、有效的、准确的、合法的和/或信誉良好的。在本公开中描述的一些验证示例中，电子记录可以使用私钥进行签名，并使用公钥进行验证。

[0035] “验证网络”可以是被配置成提供对交易的验证的任何一组节点(计算机系统和部件)。验证网络可包括利用若干节点的分布式计算环境，所述若干节点使用一个或多个计算机网络或直接连接经由通信链路互连。验证网络可在任何适当网络上实施，所述网络包含内联网、因特网、蜂窝式网络、局域网或任何其它此类网络或其组合。在一些实施例中，验证网络中的每个节点都可以是属于特定组或组织的计算装置。

[0036] 现在将描述本发明的一些实施例的细节。

[0037] 图1示出根据本发明的实施例的用于进行交易的系统100的框图。系统100可以包括用于管理账户的应用服务器120、用于处理接收到的交易的处理服务器计算机140、用于验证身份和记录的分布式验证网络150以及用于对记录进行评估和授权的授权计算机160。

[0038] 在图1中，属于用户101的端点装置110可以用于发起与访问装置130的交易或交互。对应于交互的数据可以通过处理服务器计算机140、分布式验证网络150和/或授权计算机160认证、核实、验证和授权。可以使用存储在端点装置110上的用户101的电子身份处理交互。电子身份的存储和管理以及管理其使用的参数可以由应用服务器120支持，该应用服务器可以接收、传输和/或更新存储在应用程序113中的数据。

[0039] 根据本公开的实施例，端点装置110可以包括能够使用存储的电子身份与实体交互的任何合适的计算装置。端点装置可以包括至少一个处理器、存储器、一个或多个通信接口以及生物特征读取器116。

[0040] 端点装置110可以包括一个或多个通信接口，所述一个或多个通信接口被配置成实现端点装置110与另一电子装置(例如，应用服务器120和/或访问装置130)之间的通信。通信接口可以用于将数据传输到服务器和访问装置以及从服务器和访问装置接收数据，以便执行交易。在一些实施例中，通信接口可包含长程和短程通信手段。例如，通信接口可包

含天线，所述天线被配置成连接到蜂窝式网络，以便实现与所描绘架构的各种其它组件的通信。端点装置110可以包括多于一个通信接口，以便通过多个通信信道进行通信。例如，端点装置110可以包括用于与应用服务器120通信的网络接口以及用于与访问装置130交互的非接触式接口(例如NFC芯片)。

[0041] 端点装置110的存储器可以包括安全执行环境，例如安全存储器。在一些实施例中，安全存储器可以包括安全元件114。安全元件(SE)114可以是防篡改平台(通常是单芯片安全微控制器)，其能够根据一组标识很好的可信机构所阐述的规则和安全要求来安全地托管应用程序以及其机密和密码数据(例如，密钥管理)。由端点装置110接收的敏感信息(例如，用户私钥115)可以存储在安全元件114中。安全元件114可以存储可以用来对交互记录进行签名的用户私钥115。用户私钥115可以是保密的且对其它实体未知，并且可以与对应公钥相关联，所述对应公钥可以分配给可信实体以验证使用用户私钥115签名的交互。根据一个实施例，公钥可以是对端点装置110唯一的装置ID。

[0042] 根据本公开的实施例，端点装置110的存储器还可以包括非暂时性计算机可读介质112，该非暂时性计算机可读介质包括使得处理器执行某些功能的计算机可执行指令。例如，计算机可读介质112可以包括应用程序113。应用程序113可以是移动应用程序，例如数字钱包应用程序或移动银行应用程序。应用程序113可以包括指示端点装置110创建交互记录和对交互记录进行签名的代码。

[0043] 端点装置110还可以与为端点装置110提供后端支持的应用服务器120建立连接。例如，应用服务器120可以生成电子身份，并且可以提供用于保持身份安全的后端支持。在一些实施例中，在执行应用程序113中的指令时，端点装置110可以与应用服务器120建立通信会话，其中应用服务器120代表应用程序113执行至少一些处理。在一些实施例中，应用服务器120可以维护与端点装置110和/或用户101相关联的账户。应用服务器120维护的账户可以存储与用户有关的数据。例如，应用服务器120可以存储用户数据(例如，人口统计或其它合适的信息)、与用户有关的文档(例如，银行结单、财产契约等)或任何其它合适的用户数据。根据一个实施例，从授权计算机160获得用户数据。应用服务器120可以在从应用程序113接收请求时，将其维护的至少一部分用户数据编译到电子记录中。电子记录可以与用户的电子身份相关联。应用服务器120通过对用户数据进行散列运算来创建电子身份，然后将其提供到端点装置110。根据一个实施例，由授权计算机160生成电子身份，并且提供给应用服务器120。

[0044] 在本发明的一个实施例中，应用服务器120可以分发数据或从分布式验证网络150接收数据。应用服务器120可以直接地或通过处理服务器计算机140与分布式验证网络150中的实体进行通信。在另一个实施例中，应用服务器120和处理服务器计算机140可以是同一实体。处理服务器计算机140可以被配置成使用由应用服务器120提供的数据、参数、密钥和算法处理密码。处理服务器计算机140可以解密交互数据，并且可以提交交互数据来授权计算机160对交互进行授权。授权计算机160可以基于存储在电子记录中的至少一部分数据对交互进行授权。例如，授权计算机160可以评估电子记录以确认有足够量的资产足以支付交易。在一个实施例中，授权计算机160可以是分布式验证网络150中的可信实体。

[0045] 在交易或交互期间，根据系统100，用户101使用端点装置110与资源提供商进行电子交互。端点装置110可以在应用程序113中存储用户101的电子身份。为了在交易中使用电

子身份，用户101可以提供认证数据。根据本发明的实施例，可以使用应用程序113给端点装置110提供认证数据。认证数据可以包括由应用服务器120生成且唯一地分配给用户101的用户私钥115。私钥115可能已经由应用服务器120生成。

[0046] 当用户101与资源提供商交互时，应用程序113可以使用用户私钥115对与用户101的电子身份相关联的交互记录进行签名。用户101和资源提供商之间的交互可以使用端点装置110和访问装置130之间的通信进行。例如，访问装置130可以位于资源提供商(例如，在商家位置)处，并且用户101可以通过使用端点装置110的近场通信功能与访问装置130通信，从而与资源提供商交互。访问装置130可以是接收资源或产品信息(例如，通过扫描产品的条码或其它产品标识符)来生成诸如交易金额等交互数据的POS终端。交易金额可以显示给用户101，并且访问装置130可以请求用户101提供用于支付交易金额的方法，使得可以授权访问资源。在另一个实施例中，访问装置130可以是允许用户通过互联网与资源提供商交互的网络网关。根据一个实施例，资源提供商可以是分布式验证网络150的可信实体，或者可以是能够与分布式验证网络150的可信实体通信的实体。

[0047] 端点装置110还可以包括使用生物特征读取器116从用户101获得的生物特征参考模板。生物特征参考模板可以存储在端点装置110上，并且可以与由用户101发起的交互期间提供的生物特征样本模板匹配。用户101可以使用生物特征读取器116向端点装置110提供生物特征模板。生物特征参考模板和生物特征样本模板可以被应用程序113比较，如果模板匹配，可以临时授予对用户私钥115的访问。

[0048] 根据本发明的实施例，用户101可以选择使用存储在端点装置110上的电子身份进行交易。当用户101准备好请求或支付访问时，其可以通过例如选择端点装置110的显示器上的应用程序图标来访问应用程序113。应用程序113然后可以发起或提示用户101发起与访问装置130的通信。例如，应用程序113可以提示用户101紧靠访问装置130保持端点装置110，以便交互数据可以传输到端点装置110。在一个实施例中，访问装置110在提交交互式数据之前使用资源提供商密钥135对交互数据进行签名。例如，访问装置110可以在将交互数据发送到端点装置110之前将数字签名附加到交互数据。在此示例中，交互数据可以至少包括交易的交易金额、资源提供商标识符(例如，商家标识符)、不可预知数和/或访问装置标识符(例如，终端ID)。一旦交互数据已从访问装置130传输到端点装置110，端点装置110可以生成包括交互数据(例如交易金额、交易时间戳、商家数据、产品数据等)的交互记录以及用户101的电子身份。在一个实施例中，电子身份可以是添加到交互记录或可以是交互记录一部分的关于用户101的信息(例如，姓名、出生日期、社会保障号等)的散列。

[0049] 为了在交互中使用电子身份，用户101可以使得端点装置110用用户私钥115对交互记录进行签名。应用程序113可以提示用户101向生物特征读取器116呈现其生物特征样本，以便启动签名。用户101然后可以呈现其生物特征样本(例如，指纹、语音、虹膜等)，这些样本与存储在端点装置110上的生物特征参考模板进行匹配。如果模板匹配，则授予用户私钥115的临时访问权限，然后使用用户私钥115对交互记录进行签名。所得数字签名可以附加到交互记录或作为交互记录的一部分。

[0050] 根据一个实施例，交互记录可以传输回访问装置130，以便资源提供商可以用其秘密资源提供商私钥135对交互进行签名。稍后可以与验证用户签名的相同方式验证资源提供商的签名。用于验证签名的对应公钥可以在交互之前或期间分发到分布式验证网络150。

一旦双方已对交互记录进行签名，则交互记录可以发送回端点装置110，以便在传输到处理服务器计算机140之前，交互记录可以在应用程序113中被加密。

[0051] 在一些实施例中，如果交易中双方已对交互记录进行签名，则交互记录可以在提交进行处理前被加密。已签名的交互记录可以由端点装置110从访问装置130接收，并且可以使用加密算法和限制使用密钥来由应用程序113对交互记录进行加密。根据本发明的实施例，可以使用动态数据集(例如由限制使用参数限定的限制使用密钥)来加密交互记录。动态数据集在以下意义上可为限制使用：动态数据集仅可用于受限时间或数目有限的交易，且在动态数据集耗尽其限制使用时可能需要续订、刷新、更新或补充。例如，动态数据集可包括限制使用密钥(LUK)，其在交易期间用作生成交易密码的密钥。

[0052] LUK可与限制LUK的使用的一个或多个限制使用阈值集相关联，其中一旦LUK的使用被耗尽或超出一个或多个限制使用阈值集，便将拒绝使用所述LUK进行的另外的交易，即使交易中使用的基本电子身份仍然信誉良好。实施的一个或多个限制使用阈值集可以由应用服务器120确定，并且可以通过处理服务器计算机140来验证。根据一个实施例，在交互期间限制使用参数的状态可以包括在交互记录中或附加到交互记录中，并且可以存储在电子记录中。例如，每个交互记录可以包括除当前交易之外特定LUK已经使用的次数。然后可以通过读取电子记录中的条目，来评估限制使用参数。在另一个实施例中，LUK和相关联的限制使用参数存储在由应用服务器120管理的关系数据库中。

[0053] 一个或多个限制使用阈值集可包含以下各项中的至少一个：指示LUK为有效的持续时间的存活时间；其中LUK有效的预定交易数目；和/或指示其中LUK有效的一个或多个交易合计的总交易金额的累计交易金额；或其任何组合。例如，LUK可能有效地存活五天，且在从生成LUK起过去五天后使用所述LUK进行的交易可能被拒绝。作为另一实例，LUK可对于累积交易金额五百美元有效，且已对于总数超过五百美元的交易使用所述LUK之后使用所述LUK进行的交易可能被拒绝。

[0054] 应当理解，上述限制使用值只是示例，并且可以使用其它使用限制。例如，交互使用限制的数量可设置为2到10范围内的交互次数，或者在5到50范围内的交易次数等，并且累积交易金额可设置为100美元至5,000美元的范围内的值，或者10美元到1000美元范围内的值等。

[0055] 在其中LUK与超过一个限制使用阈值相关联的实施例中，当超出任何一个限制使用阈值时，或当超出限制使用阈值的某种组合时，LUK的使用可以耗尽。因此，当超出或即将超出任何一个限制使用阈值时，或者超出或即将超出限制使用阈值的某种组合时，可触发LUK的补充。在补充前，应用服务器120可以向端点装置110或用户101的另一装置发送通知，提示用户101补充存储在应用程序113中的动态数据集。可以由使用应用程序113的用户101要求补充，并且可能需要进一步认证，诸如用户名和密码、生物特征验证等。在动态数据集中的LUK和其它数据的补充可以由应用服务器120执行，该应用服务器可以向应用程序113和处理服务器计算机140传达这些更改。

[0056] 动态数据集还可包含与LUK相关联并以明文与密码一起发送的密钥索引。密钥索引可包含与LUK生成有关的信息。例如，在一些实施例中，密钥索引可用作种子以生成其对应LUK。密钥索引可包含指示何时生成LUK的时间信息(例如，时间戳)，和/或可包含补充计数器值，所述计数器值指示LUK已针对特定账户、移动应用程序或端点装置续订或补充的次

数等。在一些实施例中，补充计数器值可指示LUK在预定时间段内补充的次数，且在每个预定时间段过去时可重置补充计数器值。此预定时间段可例如对应于可从时间信息确定的最小的时间单位，但可使用其它预定时间段。例如，如果密钥索引中包含的时间信息指示当前LUK最晚生成于几点钟，则计数器值可指示LUK在所述时间内已补充的次数。在一些实施例中，LUK可包含应用程序交易计数器值，其指示在生成LUK时由应用程序113先前已经进行的交易的数目，或者可包含由应用服务器120或由参与处理交易的合适的实体(例如处理服务器计算机140或授权计算机160)生成的伪随机不可预知数。根据一个实施例，可以使用算法来生成不可预知数，算法在每次交易中改变之前的不可预知数。应理解，密钥索引可包含与LUK的生成相关的一条或多条信息，且密钥索引中包含的一条或多条或所有信息可用作生成LUK的种子。

[0057] 一旦生成密码，端点装置110可以将密码和动态数据集传输到访问装置130。访问装置130然后可以生成包括密码和动态数据集的授权请求消息，并将其发送到处理服务器计算机140。

[0058] 处理服务器计算机140可接收授权请求消息。处理服务器计算机140然后可以继续解密授权请求消息中的密码，使得电子身份可以被认证并且可以验证和授权该交互。处理服务器计算机140可以通过确定对称限制使用密钥来解密密码，可以使用这些密钥对由端点装置110使用以生成密码的加密算法进行反向计算。处理服务器计算机140可以通过与应用服务器120通信来确定或检索对称限制使用密钥。例如，处理服务器计算机140可以通过向应用服务器120发送动态数据集中的密钥索引和/或其它数据来确定对称限制使用密钥。然后，应用服务器120可以通过在数据库中查询具有与动态数据集匹配的特征的密钥来检索对称限制使用密钥。密钥特征可以是关系数据库的形式，其中每个密钥都与其对应的动态数据集链接。所检索的密钥然后可以发送到处理服务器计算机140。

[0059] 一旦处理服务器计算机140已确定并获得对称限制使用密钥，处理服务器计算机140可以使用对称限制使用密钥解密密码。例如，对称限制使用密钥可以被输入到对加密算法进行反向计算并输出签名的交互记录的函数中。在解密时，可以评估交互记录的内容以进行处理，交互记录的内容包括交互方的交互数据、电子身份以及签名。

[0060] 在解密密码之后，处理服务器计算机140可以验证与限制使用密钥相关联的限制使用参数是有效的。例如，处理服务器计算机140可以通过引用电子记录或通过从应用服务器120检索数据来评估限制使用密钥已经使用的次数。例如，处理服务器计算机140可以确定限制使用密钥已经使用了5次，这可能是在需要补充之前可以使用限制使用密钥的最大次数。然后，处理服务器140可以认为交互无效，并且可以将授权响应消息提交到访问装置130指示拒绝交互。根据一个实施例，限制使用参数的状态还可以通过分布式验证网络150通过与可信实体确认电子记录中的条目来确认。

[0061] 如果限制使用参数有效，那么处理服务器计算机140可以通过与分布式验证网络150中的可信实体进行通信，来认证交互记录和电子身份。例如，处理服务器计算机140可以读取交互记录中的电子身份，并且可以确定涉及电子身份的交互的电子记录。电子记录可以区块链格式存在于分布式分类账中。例如，处理服务器计算机140可以通过编译包含用户的电子身份的区块链条目列表来确定电子记录。分布式验证网络150中的可信实体然后可以评估电子记录和其中包含的交互记录和电子身份的真实性。

[0062] 分布式验证网络150可包括在许多个远程节点间实施的分布式环境，所述远程节点中的每一个表示一个计算系统或组件。在一些实施例中，分布式验证网络150内的每个远程节点可以包含可以对照彼此验证的电子记录的副本。在一些实施例中，远程节点中的至少一些可以分别由签名实体、处理实体和/或授权实体中的至少一个拥有和/或操作。在一些实施例中，分布式验证网络150可以包括由各自属于特定组或已获得特定认证的实体操作的许多计算装置。分布式验证网络150中的一个或多个远程节点可以用来验证交易期间的交互记录，并且可以用来确定信任和相关联的交易风险。

[0063] 根据至少一些实施例，分布式验证网络150可以包括联合和/或基于权限的环境。例如，为了加入或使用分布式验证网络150，实体可能需要经过证实或以其它方式认证。例如，验证网络110可以要求每个实体都遵守信托服务管理(TSM)策略和/或规则。在一些示例中，根据实体类型，不同的实体可能受到不同的策略的约束。例如，与银行机构相关联的服务器可能会自动获得信任，但与个人相关联的服务器可能需要从银行机构获得认证。在这些示例中，仅可信实体可以访问分布式验证网络150。

[0064] 分布式验证网络150可以包括多个节点，所述多个节点可以各自验证签名，并确认其接收到匹配结果。节点之间的共识可用于接受或拒绝交互记录。共识可以根据投票结构确定，其中至少50％的节点必须验证交互记录。在另一个实施例中，投票可以被加权，使得更值得信赖的实体对商定的结果具有更大的权力。例如，银行可以拥有投票，其权重是由商家做出的投票的两倍，所得投票计数可以相对于预定阈值保持以达成共识。

[0065] 一旦电子身份已经过认证，处理服务器计算机140就可以将包括签名的交互记录和电子身份的授权请求消息传输到授权计算机160。授权计算机160可以基于与电子身份相关联的至少一部分电子记录授权交易和/或交互。例如，授权计算机160可以确定电子记录中的某些交互记录对应于资金和/或资产的转移。授权计算机160可以是银行，银行可以验证有足够的资金和/或资产归属于电子身份，以支付交易的交易金额。授权计算机然后可以提交授权响应消息，该授权响应消息包括对处理服务器计算机140的批准或拒绝的指示，其可以被转发到访问装置130和/或应用服务器120，以通知相关方。在一个实施例中，授权计算机160可以是分布式验证网络中的节点之一，并且可以同时执行交互记录的认证和授权两者。

[0066] 授权计算机160然后可以通过处理服务器计算机140和/或应用服务器120将授权响应消息发送到访问装置130和/或端点装置110。授权计算机160或处理服务器计算机140可以将交互记录添加到电子记录并将更新的电子记录分发到分布式验证网络150和应用服务器120。如果交互或交易已获批准，则可以最终确定交易并且交易记录可以被发布/附加到每个实体的电子记录副本上。然后，用户101可以被授予访问权限，并且可以正式分配适当的资产。

[0067] 图2示出根据本发明的实施例的处理服务器计算机的框图。处理服务器计算机200可以是例如图1的处理服务器计算机140。处理服务器计算机200可以包括一个或多个处理器201，以用于根据本发明的实施例执行指令以用于执行任务。处理服务器计算机200还可以包括用于通过网络(诸如互联网)发送和接收消息的网络接口202。处理服务器计算机200还可以包括计算机可读介质203，其可以是例如存储器。计算机可读介质203和网络接口202可以耦合到一个或多个处理器201。

[0068] 存储器可存储可以在处理器201上加载和执行的程序指令，以及在执行这些程序期间生成的数据。取决于服务器的配置和类型，存储器可以是易失性的(例如随机存取存储器(RAM))和/或非易失性的(例如只读存储器(ROM)、闪存等)。处理服务器计算机200还可以包括额外存储装置，例如，可移动存储装置或不可移动存储装置，其包括但不限于磁存储器、光盘和/或磁带存储器。磁盘驱动器及其相关联的计算机可读介质可以为处理服务器计算机200提供计算机可读指令、数据结构、程序模块和其它数据的非易失性存储。在一些实施例中，计算机可读介质可以包含多种不同类型的存储器，例如，静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)或ROM。存储器可以包括操作系统和一个或多个用于实施文中公开的特征的应用程序或服务。计算机可读介质203还可以包含记录数据，所述记录数据提供与用户和/或账户相关联的数据。

[0069] 计算机可读介质203可以包括多个模块，所述多个模块可以各自包括用于根据本发明的实施例执行特定功能的代码。所述模块可以包括用于处理密码的密码处理模块203A。根据本发明的实施例，密码处理模块203A可以包括指示处理器201确定与密码相关联的对称限制使用密钥的代码。例如，密码处理模块203A可以指示处理服务器计算机200接收标识符，诸如识别限制使用密钥的动态密钥索引。密码处理模块203A还可以指示处理服务器计算机200通过访问数据库或通过网络接口202与应用服务器通信来检索相关联解密密钥或对称限制使用密钥。应用服务器可以是图1的应用服务器120，并且可以将对称限制使用密钥和限制使用参数发送到处理服务器计算机200。

[0070] 密码处理模块203A可以指示处理服务器计算机200使用解密密钥解密密码。这可以通过例如将密码连同解密密钥输入到解密函数中来实现。所得到解密函数的输出可以是消息，诸如包括电子身份的交互记录，以及识别消息起源的一个或多个签名。密码处理模块203A还可以包括用于通过将动态数据集与限制使用参数比较来评估限制使用参数和动态数据集的代码。例如，限制使用参数可以是指定限制使用密钥仅可用于5个交易的数据，处理服务器计算机200可以接收在每个交易期间递增的动态应用交易计数器(ATC)。如果ATC等于5，则限制使用密钥(LUK)可能被视为超出其限制使用阈值，密码处理模块203A可以指示处理服务器计算机200拒绝交易。或者，如果动态数据集满足限制使用参数，则密码处理模块203A可以确定LUK是有效的。

[0071] 计算机可读介质203还可以包括认证模块203B，以用于根据本发明的实施例认证电子身份。认证模块203B可以包括用于执行以下操作的代码：读取电子身份、确定与电子身份相关联的电子记录、确定与电子身份相关联的公钥以及通过网络接口202与可信计算机通信来验证电子记录中的每个交互记录。认证模块203B还可以包括用于接收有关验证结果的数据的代码。可以评估验证结果以确定由访问控制模块203C确定的动作过程。例如，访问控制模块203C可以包括用于基于验证结果对电子身份的真实性生成“是”或“否”的指示的指令。访问控制模块203C可以包括基于诸如与请求方相关联的真实性和/或信任的预定标准，用于控制对资源的访问的任何数量的逻辑条件。

[0072] 计算机可读介质203还可以包括授权处理模块203D，以用于接收、格式化和传输授权请求消息和授权响应消息。授权处理模块203D可以指示处理服务器计算机200将包括交互记录和电子身份的授权请求消息通过网络接口202传输到授权计算机。授权请求消息还可以包括与交互相关的风险评分或信任评分。授权处理模块203D还可以包括从授权计算机

接收授权响应消息的指令。授权处理模块203D还可以包括向访问装置和/或应用服务器(分别例如图1的访问装置130和应用服务器120)转发授权响应消息的指令。

[0073] 计算机可读介质203还可以包括风险分析模块203E,以用于评估与请求的交互相关联的风险等级或风险评分。例如,风险分析模块203E可以包括用于接收交易数据、商家数据、用户数据等并输出风险评分(例如,0至100)以基于预定规则量化评估的交易风险的逻辑。计算机可读介质还可以包括交易监控模块203F,以用于识别与交互相关的可疑行为。例如,交易监控模块203F可以包括用于评估交互记录的逻辑。交易监控模块203F还可以生成通过网络接口202发送的警报。

[0074] 图3示出根据本发明的实施例的注册和提供过程的图。根据实施例,用户101首先发起注册请求S301。例如,用户301可以将识别信息填写在端点装置310上显示的注册表格,识别信息诸如全名、地址、出生日期等。然后,在S302中,用户301可以通过选择命令端点装置310提交注册请求的“提交”按钮将表格提交到应用服务器320,所述注册请求包括识别信息。选择和命令可以由存储在端点装置310上的应用程序提供和发起。例如,应用程序可以是移动银行应用程序、数字钱包应用程序、密钥生成应用程序、电子护照应用程序、电子机票应用程序等。应用程序可以由应用服务器320提供和支持,并且还可以与处理服务器计算机340和/或授权计算机360相关联。

[0075] 应用服务器320可以接收注册请求和其中包含的识别信息。应用服务器320然后可以为用户301创建账户,并且可以开始为用户301生成电子身份的过程。应用服务器320可以将识别信息提交到授权计算机360以接收可用于生成识别用户301的秘密散列的额外信息。应用服务器320可以请求包括识别信息的身份请求S303中的额外信息。例如,应用服务器320可以向授权计算机发送包括用户姓名、地址等的身份请求。本示例中的授权计算机可以是银行机构或政府机构的发行方计算机。发行方计算机可以接收识别信息并且可以确认用户的身份。然后,发行方计算机可以在身份响应S304中向应用服务器320发送诸如社会保障号、主账号等的额外信息。应用服务器320然后可以通过对识别信息和/或接收的额外信息进行散列运算来生成电子身份。例如,电子身份可以包括国家代码、客户姓名、出生日期和社会保障号的最后四位数字的组合,例如SHA256(USA*JOHN SMITH*19700101*1234)。对此值进行散列运算可产生看似随机的字符串,例如754WD2E2513BF546050C2D079FF5D65AB6E318E。应用服务器可以将此散列链接到用户账户。

[0076] 一旦生成电子身份,应用服务器320就可以为用户301生成秘密私钥。应用服务器320还可以基于私钥生成公共验证密钥。电子身份和公钥可以存储在数据库中,并链接到用户301的账户;但是,秘密私钥可以直接传输到端点装置310以用于存储,并且可以不由应用服务器320记录。通过将公钥链接到用户301的账户数据(诸如识别信息、装置ID、账号等),公钥可以与由应用服务器320管理的关系数据库中的用户301链接。

[0077] 在S305中,应用服务器320然后可以将私钥、电子身份和公钥发送到端点装置310,以用于提供。提供数据可以由存储在端点装置310上的应用程序接收,该应用程序可以将私钥存储在端点装置310的安全元件中。根据一个实施例,应用程序可以将电子身份和公钥存储在专用于应用程序的端点装置310的存储器的一部分中。在另一个实施例中,电子身份和/或公钥可以不存储在端点装置310上,而是可以基于云计算的方式在交易期间从应用服务器320检索。在又一实施例中,电子身份可以与密码相关联,所述密码是为了访问与电子

身份相关联的任何交互记录提供的。

[0078] 在成功提供到端点装置310之后，应用程序可以将生物特征请求S306在端点装置310的显示器上显示给用户。请求可以提示用户301提供生物特征样本，其可以稍后用于验证用户301并授权访问安全存储的私钥。例如，端点装置310可以提示用户301向耦合到端点装置310的指纹读取器出示其手指之一。类似地，端点装置310可以提示用户301说出一个短语，该短语可用于在验证期间分析用户的声音。在另一示例中，端点装置310的前面摄像头可捕获用户的面部图像，并且可以稍后使用该图像来确认用户并允许其根据本发明的实施例进行交易。

[0079] 然后，用户可以在S307中提供其生物特征样本。端点装置310然后可以捕获生物特征样本并将样本转换成数据。然后，可以将数据存储在端点装置310上作为生物特征参考模板，根据本发明的实施例其可以被检索并用于生物特征验证。端点装置310然后可以向应用服务器320发送确认请求S308。应用服务器320可以接收请求，并且可以尝试确认系统为用户301正确设置好。

[0080] 应用服务器320可以首先向适当的实体分发数据。例如，在S309中，应用服务器320可以将用户的公钥和电子身份分发到处理服务器计算机340。在一个实施例中，处理服务器计算机340和应用服务器320由同一实体提供。例如，应用服务器320和处理服务器计算机340可以是提供安全支付解决方案的支付处理网络。处理服务器计算机301可以接收电子身份和公钥并使用它们来维护和验证与电子身份相关的电子记录。电子身份和公钥还可以分别在S310和S311中分发给分布式验证网络350和/或授权计算机360。分布式验证网络350中的每个节点可以存储与电子身份相关联的电子记录，并且节点可以稍后使用电子身份和公钥来识别、验证和维护电子记录。在一个实施例中，授权计算机360可以是分布式验证网络350中的节点之一。

[0081] 授权计算机360、分布式验证网络350和处理服务器计算机340然后可以分别在S312、S313和S314中发送确认。确认可以包括已创建电子记录并且每个实体存储一个副本的指示。应用服务器320可以接收确认，然后可以生成确认响应S315到端点装置310。端点装置310然后可以将确认响应S316显示给用户301，使得用户301可以确认其电子身份已成功注册。

[0082] 用户301然后可以请求生成或补充限制使用参数，使得用户301可以安全地使用电子身份进行交易。用户301可以例如通过选择由应用程序提供的“补充密钥”选项提交限制使用请求S317。在一个实施例中，限制使用请求可能需要进一步认证，诸如密码或不同于用于授予对秘密私钥访问权限的生物特征验证的验证形式。认证数据可以由端点装置310和/或应用服务器320存储和验证。

[0083] 限制使用请求可以在S318中被发送到应用服务器320。限制使用请求可以包括装置ID、用户账号和用户认证数据。应用服务器320可以接收限制使用请求，并且可以为用户301的账户生成或补充限制使用密钥(LUK)。LUK可以与限制使用当前LUK的限制使用参数一起存储在关系数据库中，并且链接到用户301的账户。然后，LUK和限制使用参数可以在限制使用响应S319中传输到端点装置310并存储在端点装置310上。

[0084] 然后，LUK和限制使用参数可以用于在交易中安全地传输用户的电子身份。例如，LUK可以用来生成包括用户的电子身份的密码，所述密码由处理服务器计算机340接收。处

理服务器计算机340可以接收密码，然后与应用服务器320通信，以检索对称解密密钥以及限制使用参数。处理服务器计算机340可以使用对称密钥来解密密码，并验证限制使用参数，以便可以处理电子身份和交易。限制使用参数可在执行交易后被更新，并且当LUK已达到其限制使用阈值时，可以提示用户301。用户301然后可以从图3的S317开始补充限制使用参数。下文进一步描述根据本发明实施例进行的交易。

[0085] 图4示出根据本发明的实施例的交易过程的图。根据图4，用户401可以首先通过在S401中出示其端点装置来发起交易。例如，用户401可以位于商家处的结账柜台处，并且可以使用其手机购买选定商品。一旦用户401出示了其端点装置410，用户401可以使用端点装置410生成并发送交易请求S402。例如，用户401可以打开一个应用程序，该应用程序在靠近访问装置放置时生成交易请求。在另一示例中，用户401可以选择在端点装置410上显示的“购买商品”或支付图标，这可能导致其生成交易请求并将请求发送到访问装置430。

[0086] 交易请求S402可以被发送并由访问装置430接收，其可以生成交易数据，交易数据包括请求的交互或交易的信息，例如，交易时间戳、交易金额、商家数据、产品数据、条款与条件、免责声明、服务协议条款和/或确认和管理所请求交互需要的任何其它相关信息。然后，交互数据可以在S403中发送到端点装置410。

[0087] 端点装置410可以接收交互数据，交互数据可以显示给用户401以供确认。为确认和对交互签名，端点装置410可以在S404中请求用户的生物特征。在S405中，用户401可以检查并确认交互数据，并将其生物特征样本提供至端点装置以便验证。生物特征样本然后可以被端点装置接收并且匹配到存储的生物特征参考模板，以验证请求用户的个人身份。例如，用户401可以向端点装置410的指纹读取器出示其拇指，并且可以对着端点装置410的麦克风说出词语“我同意”。端点装置410然后可以从用户的拇指和语音生成生物特征样本模板，并且可以将样本模板与存储的生物特征参考模板比较以识别匹配。如果在预定阈值内存在匹配，端点装置410可以生成包括交互数据的交互记录。端点装置410可以将用户的电子身份附加到交互记录，然后可以使用用户的私钥对交互记录进行签名。根据本发明的实施例，除非提供了正确的个人标识并验证，否则在交易中不得访问或使用用户的私钥。在一个实施例中，可以对用户提供的生物特征样本的至少一部分进行散列运算并将其附加到交互记录，以在争议解决期间提供用户签名的确认和接收。

[0088] 然后，交互记录可以在S406中被发送到访问装置，以便资源提供商可以使用其私钥对交互记录进行签名。访问装置430可以使用存储的私钥对交互记录进行签名，或者通过将交互记录发送到资源提供商计算机进行签名。然后，资源提供商计算机可以使用资源提供商的私钥对交互记录进行签名，并且可以将签名的交互记录发回到访问装置430或端点装置410。

[0089] 端点装置410然后可以使用限制使用密钥(LUK)对交互记录进行加密。密码可以编码交易数据(例如交易时间戳)，以及在处理过程中可以验证的其它数据(例如不可预知数、应用交易计数器、交易类型等)。密码还可以提供或附加到额外明文数据，例如密钥索引和顺序计数器。然后，可以将密码发送到访问装置430，以便交互记录可以被提交以进行处理。在本发明的替代实施例中，资源提供商可以在用户401签名之前对交互记录进行签名。在这种实施例中，资源提供商的签名可以附加到交互数据，这些数据然后可以提交到端点装置410以便用户签名和加密。

[0090] 一旦在S408中由访问装置403接收密码，访问装置430或耦合到访问装置430的资源提供商计算机可以生成包括密码和明文数据的授权请求消息。在一些实施例中，除了在密码中编码之外或者代替在密码中编码，电子身份可以在明文形式的授权请求消息中。在一些实施例中，授权请求消息不包括银行账号或信用卡账号或借记卡账户或PAN(主账号)。“授权请求消息”可以是被发送以请求授权交易的电子消息。可以将授权请求消息发送到支付处理网络和/或诸如银行等的发行实体。根据一些实施例的授权请求消息可遵守ISO 8583，ISO 8583是用于交换与用户使用支付装置或支付账户进行的支付相关联的电子交易信息的系统的标准。授权请求消息还可包括额外数据元素，例如服务代码、到期日期等等中的一个或多个。授权请求消息还可包括交易信息，例如与当前交易相关联的任何信息，例如交易金额、商家识别符、商家位置等等，以及可以用于确定是否识别和/或授权交易的任何其它信息。授权请求消息还可以包括其它信息，诸如资源提供商或访问装置标识符、商家类别代码等。

[0091] 在S409中，访问装置430可以将授权请求消息发送到处理服务器计算机440以进行处理。处理服务器计算机440可以接收授权请求消息，并且可以开始处理其中包含的数据和密码。处理服务器计算机440可以使用对称限制使用密钥解密密码。例如，密码可以附带密钥索引、动态数据集或可用于识别LUK的起点的任何其它标识符。处理服务器计算机440可以识别出LUK是由应用服务器420生成的，并且可以提交包括密钥索引或标识符的LUK请求S410。应用服务器420然后可以在数据库中查询可以用来解密密码的对称限制使用密钥(LUK)。在S411中，应用服务器420然后可以将对称LUK和任何其它必要的信息(诸如限制使用参数的预期状态)提交到处理服务器计算机440。例如，应用服务器420可以将LUK响应提交到处理服务器计算机440，所述LUK响应包括对称LUK和预期的应用交易计数器值“4”。

[0092] 处理服务器计算机440然后可以接收LUK响应并使用接收的数据来解密和验证密码。然后，处理服务器计算机可以通过将其值与其预期状态进行比较来验证与密码相关联的限制使用参数。例如，处理服务器计算机440可以确定接收的不可预知数“10294812095”与预期的不可预知数“039571590”不匹配，因此可以拒绝交易，而无论其它数据的真实性如何。

[0093] 在一些可选实施例中，如果限制使用参数被视为有效，处理服务器计算机440可以继续认证交互记录中包含的电子身份。处理服务器计算机440可以首先确定与可获得和验证的电子身份相关联的电子记录。

[0094] 处理服务器计算机440可以对区块链或分布式分类账进行访问，所述区块链或分布式分类账维护交互记录的列表，每个交互记录加时间戳，并与一个或多个电子身份和/或签名实体相关联。处理服务器计算机440可以在区域链中查询与接收的电子身份相关联的交互的列表，并且可以将交互记录编译到电子记录中。处理服务器然后可以将验证请求S412发送到分布式验证网络450，其中分布式验证网络450的一个或多个节点被要求验证电子记录中的至少一部分交互记录(以及可选地附加到任何交互记录的签名)。

[0095] 分布式验证网络450中的节点可以各自维护区块链/分布式分类账的副本，并且可以使用存储的公钥验证已编译的电子记录和待处理的交互记录的签名。每个节点都可以通过将交互相关方的每个数字签名和公钥输入验证算法中来验证交互记录。每个节点可以另外选择使用自己的私钥来签名或确认待处理的交易。节点可以就电子身份和相关记录的真

实性达成共识，并且可以在验证响应S413中将结果发送到处理服务器计算机440。

[0096] 处理服务器计算机440可以接收验证响应，并且如果验证产生积极结果，则可以继续交易授权。在一个实施例中，处理服务器计算机440可以基于电子记录的至少一部分或基于其它数据(诸如来自分布式验证网络450的节点中的一个或多个的数据)来确定待处理的交互的风险评分。

[0097] 在S414中，处理服务器计算机440然后可以将授权请求消息转发到授权计算机460。授权请求消息可以包括电子记录和/或电子身份以及风险评分。授权计算机460然后可以基于所接收的信息批准或拒绝交易。例如，授权计算机460可以使用电子身份查找其自己的电子记录副本，并且可以评估电子记录，以确定目前是否有足够的资产与电子身份相关联，以支付待处理的交易金额。在又一个实施例中，授权计算机460可以是分布式验证网络450的节点，并且交互记录的认证和授权可以同时执行。

[0098] 在S415中，授权计算机460可以在授权响应消息中将授权的结果(例如，批准或拒绝)发送到处理服务器计算机440。“授权响应消息”可以是对授权请求消息应答的电子消息应答。授权响应消息可由发行金融机构或支付处理网络产生。授权响应消息可包含(仅作为实例)以下状态指示符中的一个或多个：批准-交易被批准；拒绝-交易未被批准；或呼叫中心-等待更多信息的响应，商家必须呼叫免费授权电话号码。授权响应消息还可包含授权代码，所述授权代码可以是信用卡发卡银行响应于电子消息中的授权请求消息(直接或者通过支付处理网络)返回给商家计算机的指示批准交易的代码。所述代码稍后可充当授权的证据。

[0099] 如果交易已获授权，处理服务器计算机440可以通过将交互记录附加到区块链/分布式分类账来发布待处理的交互记录。此外，验证网络450的节点还可以接收通知，通知交互已获授权，并且可以使用交互记录更新其分类账，从而同步其电子记录的副本。

[0100] 根据一个实施例，在S416a中，授权响应消息可以转发到访问装置430。在S417a中，访问装置430然后可以显示和/或将授权响应消息传输到端点装置410。在另一个实施例中，在S416b中，授权响应消息可以发送到应用服务器420。应用服务器420然后可以创建归属于用户401账户的成功交易的记录。应用服务器420还可以更新与LUK相关联的限制使用参数的状态。应用服务器420然后可以在授权响应消息S417b中向端点装置410提交更新的LUK和/或限制使用参数和授权结果。端点装置410然后可以将授权结果显示给用户401，并且补充存储在装置上的LUK和限制使用参数。

[0101] 在任何一种情况下，如果交易已获授权，则交易记录可以被接受为正式的，并且可以根据交互记录的条款正式分配合适的资产。

[0102] 本公开的实施例可以提供许多有用的应用。例如，本公开的实施例可以为用户提供可用于各种场景的电子识别的单一形式。本发明的实施例允许实体通过用其它可信实体验证来认证用户的身份。可信实体可以是医院、银行、政府、商家或者可以验证之前与用户交互的个人，从而提供信任并保证用户是他们所说的用户。此外，交互在分发到整个信任网络的不可变的电子记录中维护，该记录提供了可达成共识的单一真相源。这允许用户仅使用单个装置安全地识别自己，而不是携带多个ID卡、信用卡、护照、门票、通行证等。

[0103] 图5描绘根据本发明的实施例的电子记录的示例。在图5中，用户501希望使用其电子身份503进行交易。用户501可以通过向端点装置510呈现用户生物特征502来提供他的个

人身份的证据。端点装置510可以为交易生成交互记录511d，并且可以将用户的电子身份503附加到交互记录以及任何其它识别信息(诸如装置ID、交易时间戳等)。在成功验证用户生物特征502后，可以使用用户私钥515对交互记录511进行签名。在提交进行处理之前，交互记录可能会被加密或进行散列运算。例如，可以使用由应用服务器管理的限制使用密钥(LUK)对交互记录511加密。

[0104] 当在处理过程中接收和解密交互记录时，可以从区块链504识别或编译与电子身份503相关联的电子记录。区块链504中的每个区块可以包含时间戳以及在其之前的区块的散列，从而生成每个连续区块之间的链路。区块可以由使用诸如SHA-256的密码散列函数求散列的交易或交互记录组成。区块还可以由多个交易组成，这些交易在二元树结构(例如，Merkle树)中被浓缩和进行散列运算，以提供更高效的数据存储。

[0105] 为了编译或识别记录，处理服务器计算机可以在区块链中查询包含构成电子身份503的唯一字符串的区块。然后，处理服务器计算机可以通过向可信实体呼叫来验证电子记录中的每个交互记录(例如，记录a、b和c)。每个可信实体或节点可能有其自己的区块链504的副本，并且可以验证每个交互记录或区块在节点之间匹配。每个可信实体还可以使用公钥来验证电子记录中的特定交互记录，其确认附加到交互记录的签名的起源。例如，第一交互记录511a可以由第一可信节点550a验证。第一可信节点550a可以是以前授权或发起涉及电子身份503的交互的政府服务器。例如，用户501可能使用过电子身份503向政府办公室550a1提交投票或进入安全检查点550a2。第一可信节点550a可以使用密钥512A验证第一交互记录511a。密钥512A可以是由第一可信节点550a支持的装置或计算机(诸如政府办公室550a1或安全检查点550a2的计算机)的公钥。密钥512A可以连同附加到第一交互记录511a的对应的签名被输入到验证算法中。如果验证的输出匹配预期结果，则第一可信节点550a可以确认或验证交互记录是有效的，并且未被改变或未被欺骗性地创建。

[0106] 类似地，第二交互记录511b可以由第二可信节点550b验证。第二可信节点550b可以是授权用户501进入车辆550b1的远程服务器。第二可信节点550b可以使用密钥512b验证第二交互记录511b，密钥512b可以是链接到车辆550b1的公共验证密钥，并且由第二可信节点550b存储。另外，第三交互记录511c还可以由第三可信节点550c验证。第三可信节点550c可以是管理用户501拥有的各种IoT装置(例如电视550c1和音频系统550c2)的信任管理服务器。第三可信节点550c可以使用密钥512c来继续验证第三交互记录511c。

[0107] 在电子记录的交互记录已经过验证之后，授权计算机可以基于电子记录的至少一部分授权交互记录511d。例如，授权计算机可以是银行，其确定是否有归属于电子身份503的足够资产来执行特定交易。一旦授权，可以由授权计算机或处理服务器计算机将交互记录511d添加到区块链504。可以通过将前一区块的散列附加到新区块并将这种增加传送到所有可信节点，将交互记录511d在新区块中添加到区块链504，以便他们可以更新自己的区块链504的副本。交互记录511d现在可以是归属于电子身份503的不可改变记录，并且可以稍后用于验证/认证用户在未来交易中的身份。

[0108] 图6示出根据本发明的实施例的用于验证交易的过程流程图。图600中示出的过程可以由逻辑形式的处理服务器计算机执行，并且可以用来确定所提出的交易是否有效。根据图600，在S601中，处理服务器计算机可以首先接收包括加密的交互记录(即密码)的授权请求消息。消息可以从访问装置接收，并且可以包括由一个或多个电子身份请求的交易。在

S602中，处理服务器计算机可以确定是否存在对称限制使用密钥，这些密钥可以解密加密的交互记录。例如，授权请求消息可以包括识别密钥的位置或管理密钥的应用服务器的公共地址的密钥索引。如果存在对称限制使用密钥，则处理服务器计算机可以检索对称密钥并使用它解密密码。否则，在S610中，处理服务器计算机可以使交易失效。

[0109] 一旦密码被解密，处理服务器计算机可以确定相关的限制使用参数是否有效。例如，密码可能已使用限制使用密钥(LUK)进行加密，其中当LUK已用于超过价值1000美元的交易时，交易可能被无效。根据本发明的实施例，如果限制使用参数是有效的，则在S605中，处理服务器计算机可以从共享区块链获取/编译电子记录。电子记录可以与附加到交互记录的电子身份相关联，并且可以由分布式网络中的可信节点验证。处理服务器计算机可以从可信节点接收表明电子记录中列出的交互是否有效的验证响应。

[0110] 处理服务器计算机可以接收验证响应，并且可以在S606中，基于验证响应确定请求交易的电子身份是否是真实和值得信赖的。如果电子身份被认证，则在S607中，处理服务器计算机可以将授权请求消息转发到授权计算机。否则，在S610中，交易可能被无效。授权计算机可以接收授权请求消息，并且可以基于与电子身份相关联的至少一部分电子记录授权基础交易。授权计算机然后可以发送包括批准或拒绝处理服务器计算机的指示的授权响应消息。

[0111] 在步骤S608中，处理服务器计算机可以接收授权响应消息。如果交易已经过授权计算机批准，处理服务器计算机可以将交易在新区块中增加到共享区块链，并且可以在S609中将授权响应消息转发到访问装置。访问装置可以接收授权响应消息，确认交易已经过批准并且被考虑。如果交易未获批准，则在S610中，处理服务器计算机可以转发授权响应消息，其包含拒绝访问装置的指示。

[0112] 本发明的实施例提供若干技术优点。例如，本发明的实施例提供用于以安全方式识别个体的系统。给用户提供为唯一的且可以安全地存储在电子装置上的电子身份。如果用户通过生物特征验证首先提供个人识别，则用户只能使用电子身份识别自己。涉及电子身份的交互维护在可信实体之间共享的区块链的不可改变的区块中。

[0113] 图7示出根据本发明的实施例的用于安全处理电子身份的方法的流程图。根据图700，在S701中，生物特征样本首先由用户向端点装置提供并且匹配到存储的生物特征参考模板。在S702中，生成新的交互记录，交互记录包括用户的电子身份和交互数据。在S703中，使用交互方的私钥对交互记录进行签名。在S704中，限制使用密钥用于生成密码，所述密码对交易时间戳、交易金额、不可预知数、应用交易计数器和交互记录进行编码。

[0114] 在S705中，由处理服务器计算机接收密码。在S706中，处理服务器计算机检索对称限制使用密钥(LUK)并使用它解密密码。在S707中，验证与LUK相关联的限制使用参数。在S708中，基于以前的交互和签名的有效性验证与电子身份相关联的电子记录。在分布式网络的可信节点之间就电子身份的真实性达成共识。

[0115] 在S709中，授权计算机基于电子记录的至少一部分授权交互记录。在S710中，用新的交互记录更新电子记录/区块链，并将更新传达到可信节点，以便它们同步其区块链的副本。在S711中，限制使用参数由应用服务器更新并存储在端点装置或用户账户中。

[0116] 应当理解，对上述附图中描述的实体(包括用户、端点装置、访问装置、处理服务器计算机、应用服务器、分布式验证网络、以及授权计算机)的引用可以引用其它附图中描述

的相同对应实体，例如图1的用户101、端点装置110、应用服务器120、访问装置130、处理服务器计算机140、分布式验证网络150以及授权计算机160。

[0117] 还应理解，本发明的任何实施例都可使用硬件(例如专用集成电路或现场可编程门阵列)和/或使用计算机软件以控制逻辑的形式被实施，其中通用可编程处理器是模块化的或集成的。如本文中所使用，处理器包含单核处理器、在同一集成芯片上的多核处理器，或在单个电路板上或网络化的多个处理单元。基于本公开和本文中所提供的教示，本领域的普通技术人员将知道并且了解使用硬件和硬件与软件的组合来实施本发明的实施例的其它方式和/或方法。

[0118] 本申请中所描述的任何软件组件或功能可被实施为要使用例如Java、C、C++、C#、Objective-C、Swift的任何合适计算机语言或例如Perl或Python的脚本语言，使用例如常规的或面向对象的技术由处理器执行的软件代码。软件代码可作为一系列指令或命令存储在计算机可读介质上以供存储和/或传递，合适的介质包含随机存取存储器(RAM)、只读存储器(ROM)、例如硬盘驱动器或软盘的磁性介质，或例如光盘(CD)或数字通用盘(DVD)的光学介质、闪存存储器等等。计算机可读介质可以是此类存储或传递装置的任何组合。

[0119] 此类程序还可使用适合于经由包含互联网的符合多种协议的有线、光学和/或无线网络传递的载波信号被编码和传递。因此，根据本发明的实施例的计算机可读介质可使用以此类程序编码的数据信号被创建。以程序代码编码的计算机可读介质可与兼容装置一起封装或与其它装置分开提供(例如，经由互联网下载)。任何此类计算机可读介质可驻留在单个计算机产品(例如，硬盘驱动器、CD或整个计算机系统)上或内，并可存在于系统或网络内的不同计算机产品上或内。计算机系统可包含监视器、打印机，或用于向用户提供本文中所提及的任何结果的其它合适的显示器。

[0120] 以上描述是说明性的而不是限制性的。在所属领域的技术人员阅读了本公开后，本发明的许多变化将变得显而易见。因此，本发明的范围不应参考以上描述来确定，而是应参考待决的权利要求以及其完整范围或等效物来确定。

[0121] 在不脱离本发明的范围的情况下，任何实施例的一个或多个特征可与任何其它实施例的一个或多个特征组合。

[0122] 除非明确指示有相反的意思，否则“一个/种(a/an)”或“所述”的叙述旨在表示“一个/种或多个/种”。

[0123] 上文所提及的所有专利、专利申请、公开案和描述都出于所有目的而以其全文引用的方式并入本文中。并非承认它们是现有技术。

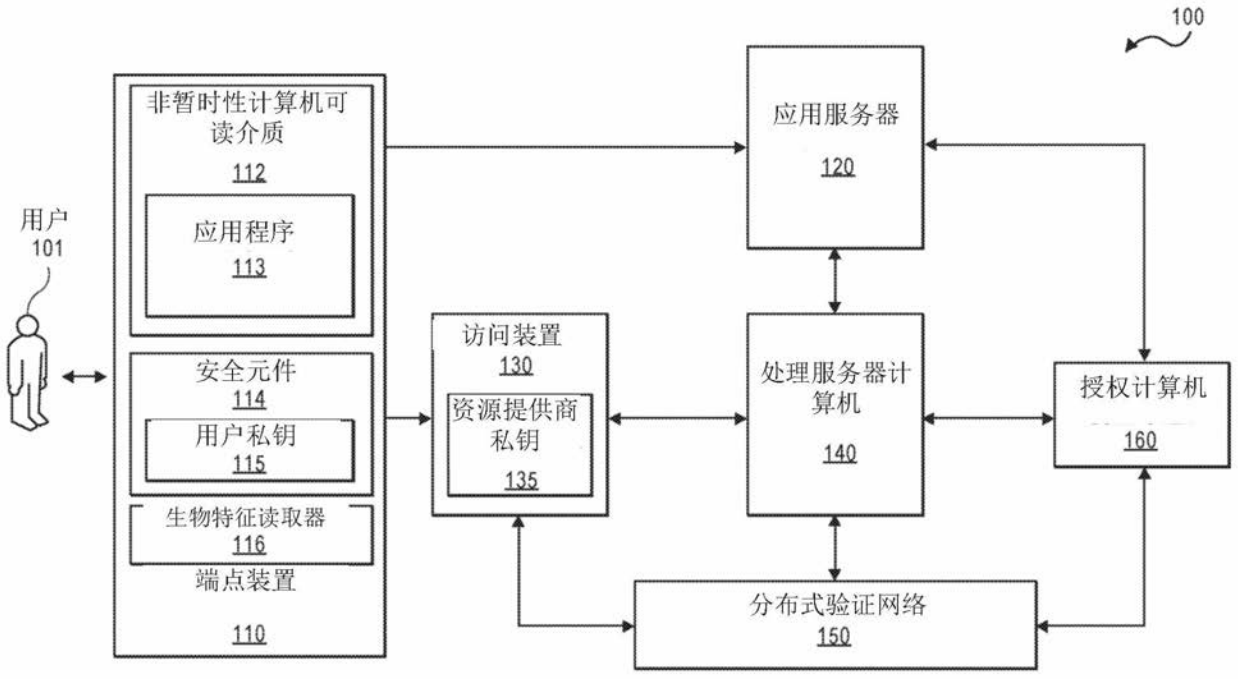

100
非暂时性计算机可读介质
112
应用程序
113
应用服务器
120
用户
101
访问装置
130
资源提供商私钥
135
处理服务器计算机
140
授权计算机
160
安全元件
114
用户私钥
115
生物特征读取器
116
端点装置
110
分布式验证网络
150

图1

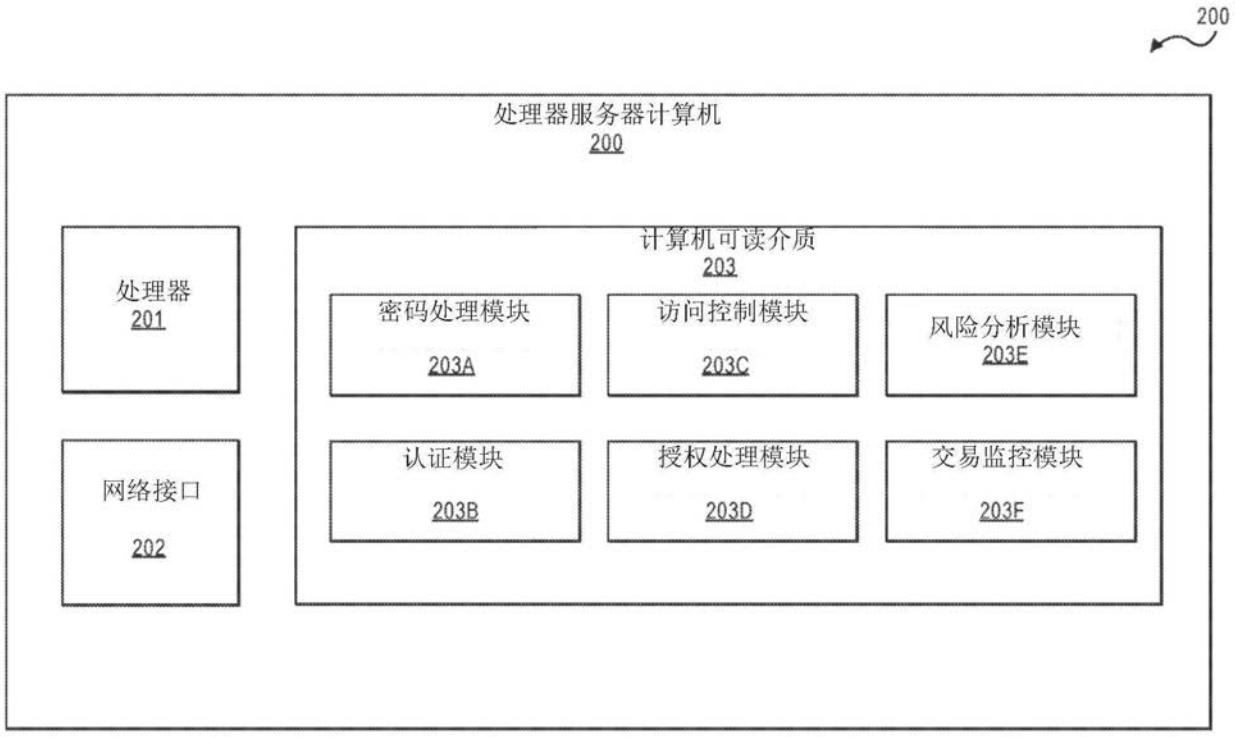

200
处理器服务器计算机
200
处理器
201
网络接口
202
计算机可读介质
203
密码处理模块
203A
访问控制模块
203C
风险分析模块
203E
认证模块
203B
授权处理模块
203D
交易监控模块
203F

图2

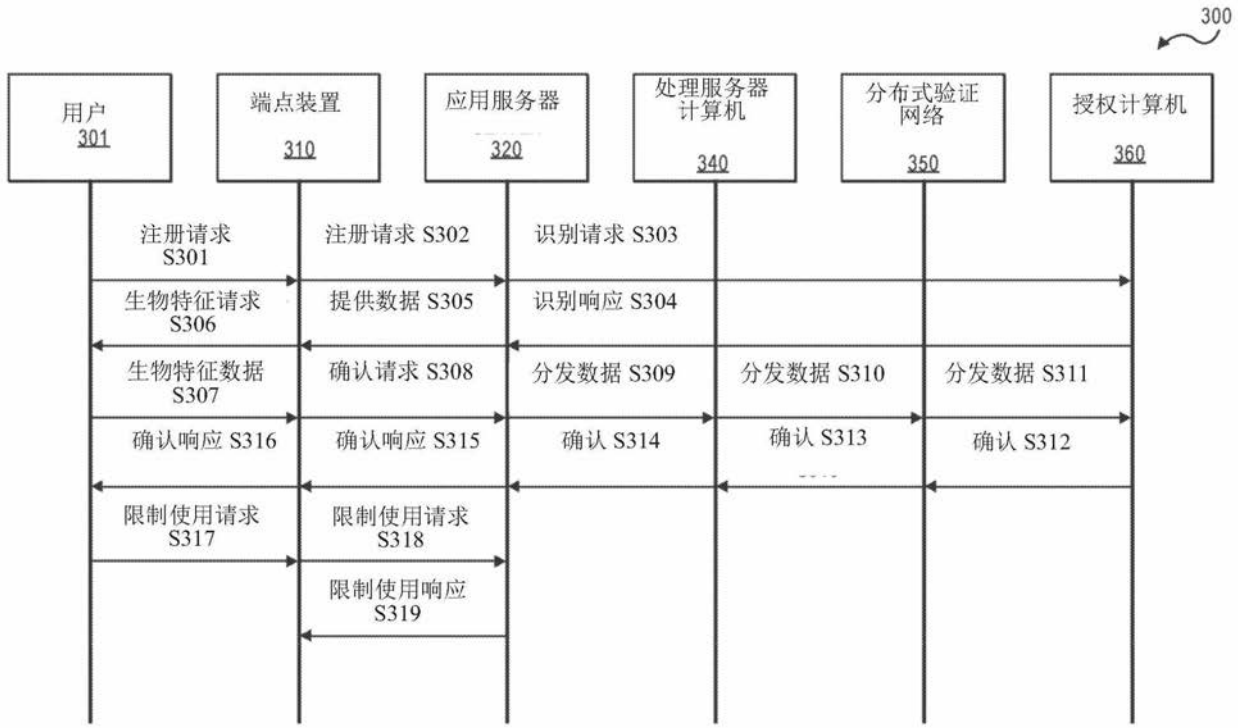

300
用户
301
端点装置
310
应用服务器
320
处理服务器
计算机
340
分布式验证
网络
350
授权计算机
360
注册请求
S301
注册请求 S302
识别请求 S303
生物特征请求
S306
提供数据 S305
识别响应 S304
生物特征数据
S307
确认请求 S308
分发数据 S309
分发数据 S310
分发数据 S311
确认响应 S316
确认响应 S315
确认 S314
确认 S313
确认 S312
限制使用请求
S317
限制使用请求
S318
限制使用响应
S319

图3

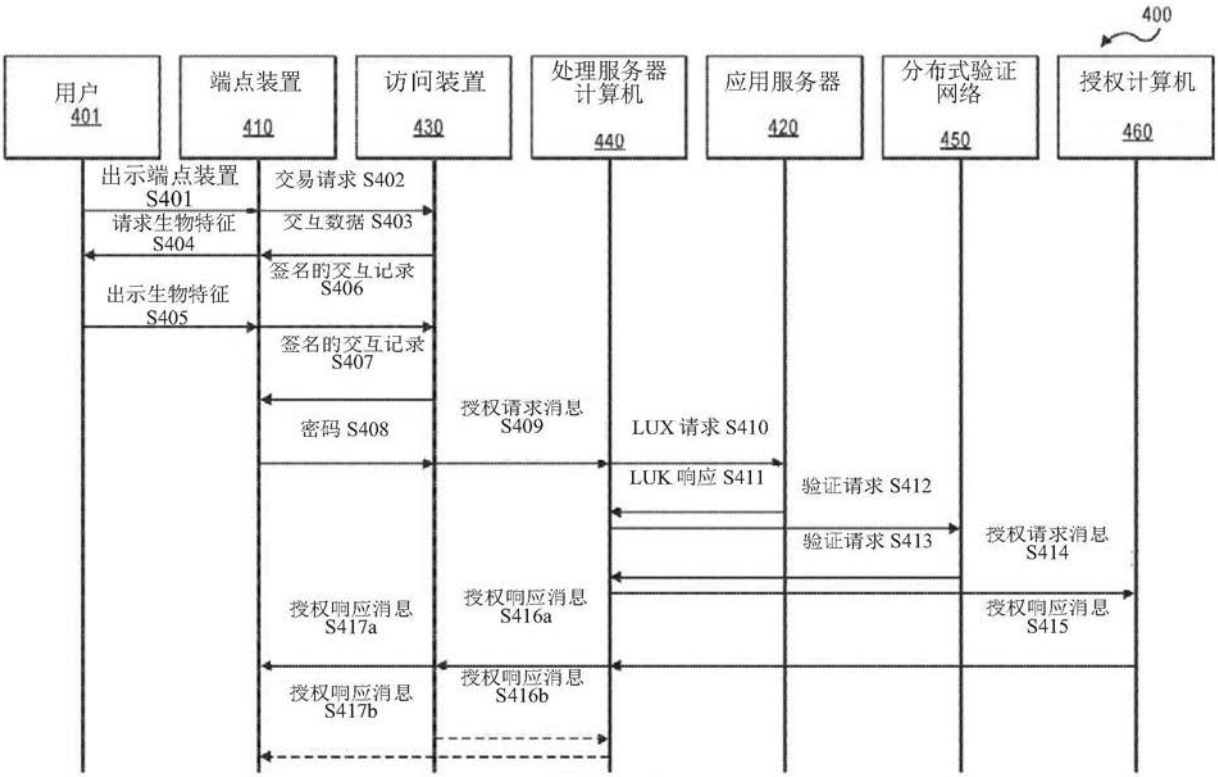

400
用户
401
端点装置
410
访问装置
430
处理服务器
计算机
440
应用服务器
420
分布式验证
网络
450
授权计算机
460
出示端点装置
S401
交易请求 S402
请求生物特征
S404
交互数据 S403
签名的交互记录
S406
出示生物特征
S405
签名的交互记录
S407
密码 S408
授权请求消息
S409
LUX 请求 S410
LUK 响应 S411
验证请求 S412
验证请求 S413
授权请求消息
S414
授权响应消息
S417a
授权响应消息
S416a
授权响应消息
S415
授权响应消息
S417b
授权响应消息
S416b

图4

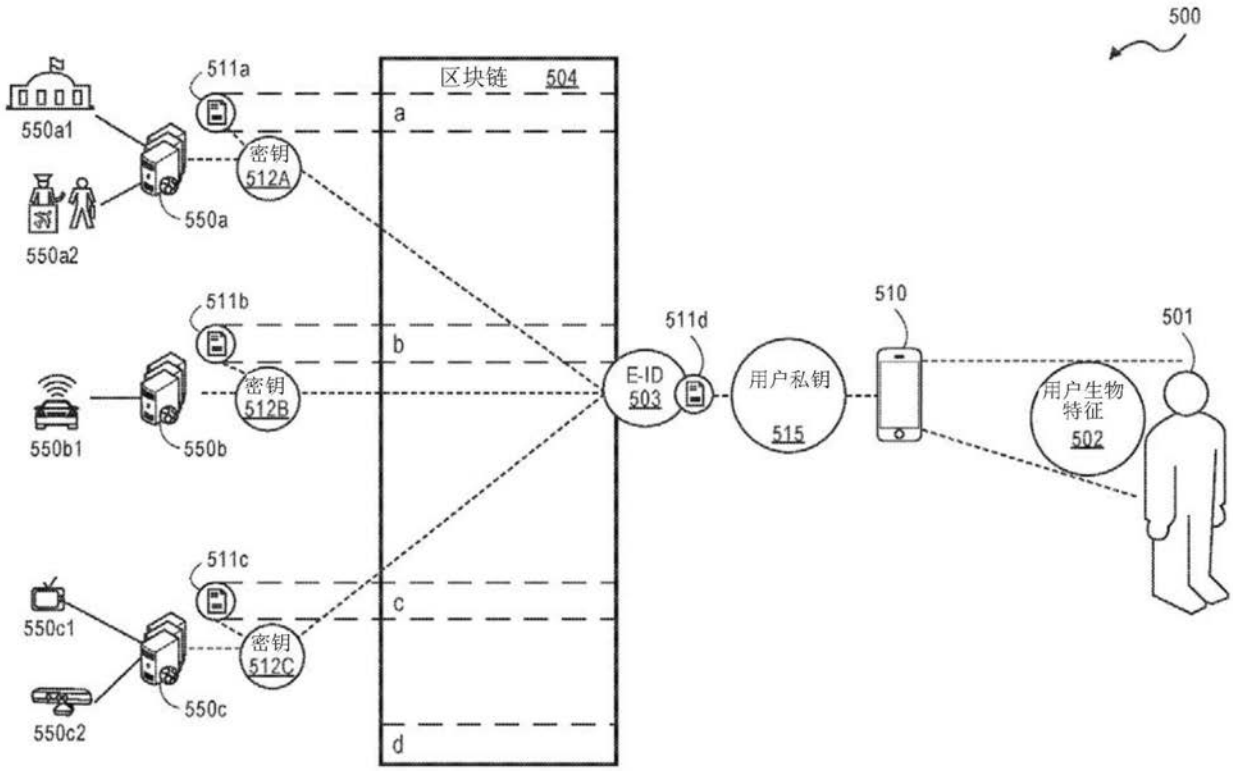

500
区块链 504
a
b
c
d
511a
511b
511c
511d
密钥 512A
密钥 512B
密钥 512C
550a1
550a2
550a
550b1
550b
550c1
550c2
550c
E-ID 503
用户私钥 515
510
501
用户生物特征 502

图5

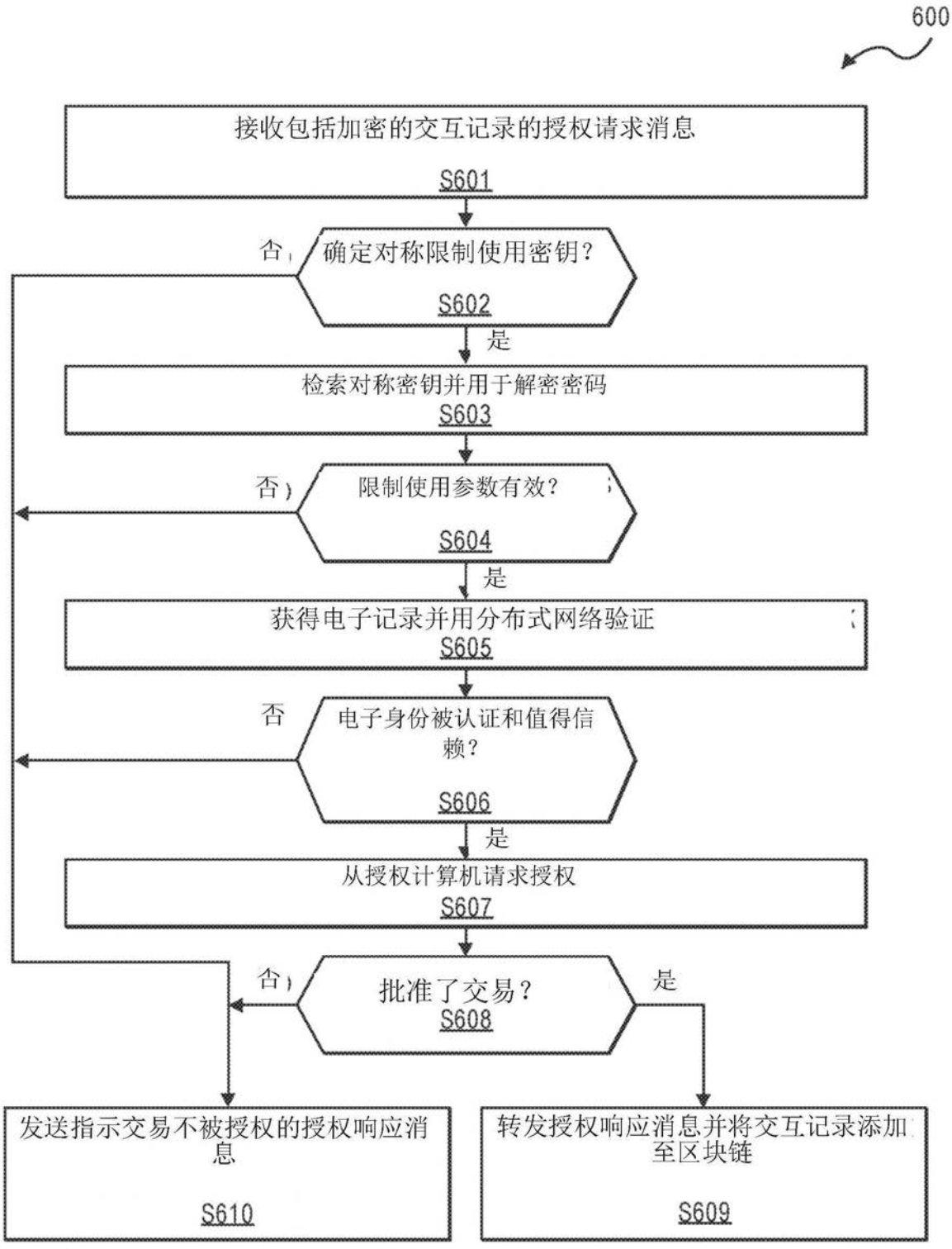

600
接收包括加密的交互记录的授权请求消息
S601
否
确定对称限制使用密钥?
S602
是
检索对称密钥并用于解密密码
S603
否
限制使用参数有效?
S604
是
获得电子记录并用分布式网络验证
S605
否
电子身份被认证和值得信赖?
S606
是
从授权计算机请求授权
S607
否
批准了交易?
S608
是
发送指示交易不被授权的授权响应消息
S610
转发授权响应消息并将交互记录添加至区块链
S609

图6

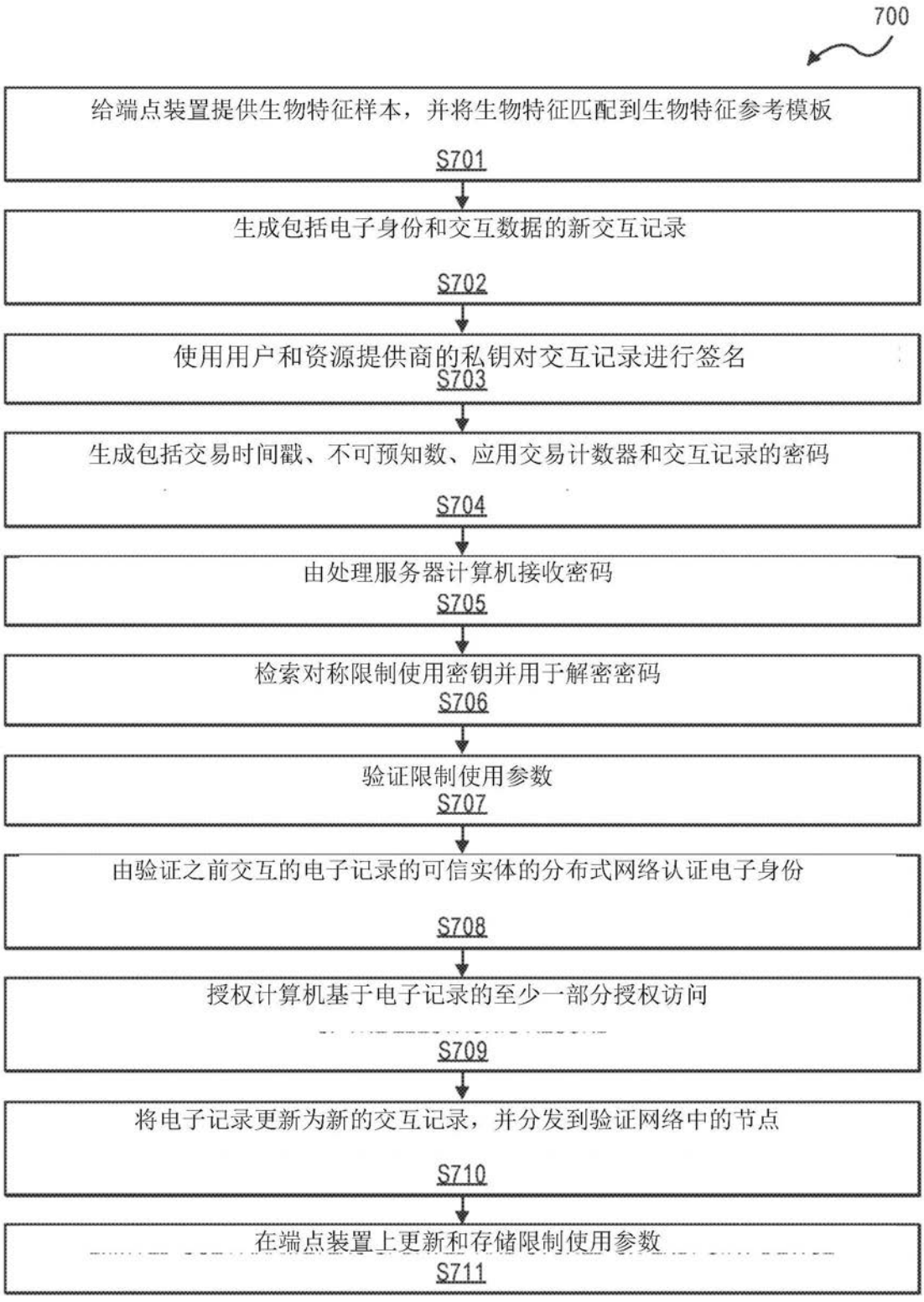

700
给端点装置提供生物特征样本，并将生物特征匹配到生物特征参考模板
S701
生成包括电子身份和交互数据的新交互记录
S702
使用用户和资源提供商的私钥对交互记录进行签名
S703
生成包括交易时间戳、不可预知数、应用交易计数器和交互记录的密码
S704
由处理服务器计算机接收密码
S705
检索对称限制使用密钥并用于解密密码
S706
验证限制使用参数
S707
由验证之前交互的电子记录的可信实体的分布式网络认证电子身份
S708
授权计算机基于电子记录的至少一部分授权访问
S709
将电子记录更新为新的交互记录，并分发到验证网络中的节点
S710
在端点装置上更新和存储限制使用参数
S711

图7