(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110912685 B
(45)授权公告日 2024.09.13

(21)申请号 201910877388.6

(22)申请日 2019.09.17

(65)同一申请的已公布的文献号
申请公布号 CN 110912685 A

(43)申请公布日 2020.03.24

(30)优先权数据
1815092.0 2018.09.17 GB

(73)专利权人 信特尼有限公司
地址 英国剑桥

(72)发明人 理查德·海顿

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
专利代理师 林强

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
Shahid Raza et al..S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things.IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING.2016,正文I-VII节.

审查员 陈燕

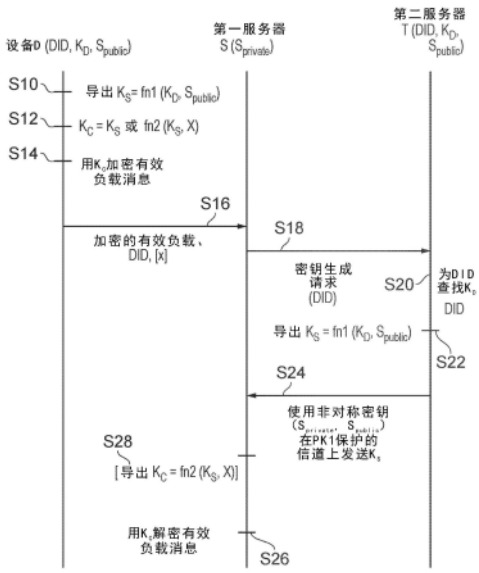
权利要求书2页 说明书8页 附图3页

(54)发明名称

建立受保护通信信道

(57)摘要

本公开涉及建立受保护通信信道。为了在设备D与第一服务器S之间建立第一受保护通信信道,基于设备标识密钥K_D和依赖于第一服务器S的第一服务器公钥S_{public}的公钥信息在设备D处导出对称密钥K_S。在第二服务器T处以相应的方式导出对称密钥K_S。在第二受保护通信信道上将对称密钥K_S从第二服务器T发送到第一服务器S。使用依赖于对称密钥K_S的通信密钥K_C保护所述设备D与所述第一服务器S之间的所述第一受保护通信信道上的通信。这可使得缺少对非对称密钥加密的支持的设备D能够安全地进入与所述第一服务器S的通信。



CN 110912685 B

1.一种用于在设备与第一服务器之间建立第一受保护通信信道的方法,所述第一服务器具有第一服务器公钥,并且所述设备具有与不同于所述第一服务器的第二服务器共享的设备标识密钥;所述方法包括:

基于所述设备标识密钥和依赖于所述第一服务器公钥的公钥信息在所述设备处导出对称密钥;

由所述设备在使用依赖于所述对称密钥的通信密钥所保护的所述第一受保护通信信道上向所述第一服务器发送有效负载消息;以及

响应于所述有效负载消息,所述第一服务器向所述第二服务器发送密钥生成请求以触发所述第二服务器导出所述对称密钥并且在第二受保护通信信道上将所述对称密钥发送到所述第一服务器;

基于所述设备标识密钥和所述公钥信息在所述第二服务器处导出所述对称密钥;以及

使用所述第二受保护通信信道将所述对称密钥从所述第二服务器发送到所述第一服务器。

2.根据权利要求1所述的方法,其中,使用基于非对称密钥的公钥基础设施来保护所述第二受保护通信信道。

3.根据权利要求2所述的方法,其中,用于所述公钥基础设施的非对称密钥包括所述第一服务器公钥和第一服务器私钥。

4.根据权利要求1所述的方法,其中,所述通信密钥与所述对称密钥相同。

5.根据权利要求1所述的方法,其中,基于在所述设备与所述第一服务器之间共享的信息,从所述对称密钥导出所述通信密钥。

6.根据权利要求5所述的方法,其中,在所述设备与所述第一服务器之间共享的信息包括以下项中的至少一者:

与包括所述设备的设备类相关联的类密钥;以及

随机值或伪随机值。

7.根据权利要求1至6中任一项所述的方法,其中,所述公钥信息与所述第一服务器公钥相同。

8.根据权利要求1至6中任一项所述的方法,其中,所述公钥信息包括所述第一服务器公钥的散列,并且具有比所述第一服务器公钥更少的位。

9.根据权利要求1至6中任一项所述的方法,其中,所述设备无法生成用于支持公钥基础设施的非对称密钥。

10.根据权利要求1所述的方法,其中,所述有效负载消息和所述密钥生成请求各自指定所述设备的设备标识符。

11.一种计算机可读存储介质,存储计算机程序,所述计算机程序在被处理器执行时使得所述处理器执行根据权利要求1-10中任一项所述的方法。

12.一种用于建立通信信道的装置,所述装置包括:

设备;

第一服务器;以及

第二服务器,

其中所述设备、所述第一服务器、所述第二服务器中的每一者包括:

处理电路,用于执行数据处理;以及

数据存储装置,存储用于控制所述处理电路执行根据权利要求1至10中任一项所述的方法的计算机程序。

建立受保护通信信道

技术领域

[0001] 本技术涉及在设备与服务器之间建立受保护通信信道。

背景技术

[0002] 可以建立受保护通信信道以保护两个设备之间的传输。例如,受保护通信信道可以基于使用非对称密钥的公钥基础设施。设备可以与它单独访问的私钥和可与其他设备共享的公钥相关联,并且可以提供证明与私钥-公钥对相关联的设备的属性的证书。密钥对可用于提供机密性的保证(例如用公钥加密的消息可仅被具有私钥的设备解密)并且信任设备的身份(例如公钥可由验证者用来验证使用私钥签名的消息的签名,使得如果签名验证成功,则这意味着可将消息假定为源自持有私钥的设备)。

[0003] 然而,支持非对称密钥加密(例如,椭圆曲线加密)的软件算法可能相对复杂并且代码大小大。在非常小的计算设备(诸如传感器、致动器或物联网中的其他设备)中,存储器存储容量和处理能力可能是极其受限的。这可能使得在这样的设备上实现非对称密钥加密不可行。因此,缺少对非对称密钥加密的支持同时保持对设备的身份的机密性和信任的设备可能难以与服务器建立受保护通信信道,其中服务器尚未共享用于保护通信的对称密钥。

发明内容

[0004] 至少一些示例提供一种用于在设备与第一服务器之间建立第一受保护通信信道的方法,所述第一服务器具有第一服务器公钥,并且所述设备具有与不同于所述第一服务器的第二服务器共享的设备标识密钥。该方法包括:基于所述设备标识密钥和依赖于所述第一服务器公钥的公钥信息在所述设备处导出对称密钥;基于所述设备标识密钥和所述公钥信息在所述第二服务器处导出所述对称密钥;使用第二受保护通信信道将所述对称密钥从所述第二服务器发送到所述第一服务器;以及使用依赖于所述对称密钥的通信密钥保护所述设备与所述第一服务器之间的所述第一受保护通信信道上的通信。

[0005] 至少一些示例提供用于控制所述设备、所述第一服务器和所述第二服务器执行上述方法的计算机程序集。

[0006] 至少一些示例提供至少一种存储介质,所述至少一种存储介质存储所述计算机程序集。所述存储介质可以是非暂时性存储介质。

[0007] 至少一些示例提供一种用于第一服务器与设备建立第一受保护通信信道的方法,包括:通过第二受保护通信信道从第二服务器接收从所述第一服务器的第一服务器公钥和在所述设备与所述第二服务器之间共享的设备标识密钥导出的对称密钥;以及使用通信密钥保护在所述第一受保护通信信道上与所述设备的通信,所述通信密钥依赖于从所述第二服务器接收到的所述对称密钥。

[0008] 至少一些示例提供一种用于第二服务器为第一服务器生成对称密钥以在所述第一服务器与设备之间建立第一受保护通信信道的方法,包括:基于在所述第二服务器与所

述设备之间共享的设备标识密钥和依赖于与所述第一服务器相关联的第一服务器公钥的公钥信息,在所述第二服务器处导出所述对称密钥;以及通过第二受保护通信信道将所述对称密钥发送到所述第一服务器。

[0009] 至少一些示例提供一种用于设备与第一服务器建立第一受保护通信信道的方法,包括:基于与不同于所述第一服务器的第二服务器共享的设备标识密钥和依赖于与所述第一服务器相关联的第一服务器公钥的公钥信息,在所述设备处导出对称密钥;以及通过基于依赖于所述对称密钥的通信密钥保护的所述第一受保护通信信道与所述第一服务器进行通信。

[0010] 至少一些示例提供一种计算机程序,所述计算机程序用于控制装置以执行上面讨论的方法中的任一种。存储介质可以存储所述计算机程序。所述计算机程序可以是非暂时性计算机程序。

[0011] 至少一些示例提供一种装置,所述装置包括:用于执行数据处理的处理电路;以及存储用于控制所述处理电路执行上面讨论的方法中的任一种的计算机程序的数据存储装置。

附图说明

[0012] 从以下将结合附图阅读的示例的描述中,本技术的其他方面、特征和优点将变得显而易见,在附图中:

[0013] 图1示意性地示出了包括设备、第一服务器和第二服务器的系统;

[0014] 图2示意性地示出了设备的组件的示例;以及

[0015] 图3示出了用于在设备和第一服务器之间建立第一受保护的通信信道的方法。

具体实施方式

[0016] 设备可能需要与第一服务器建立第一受保护通信信道,其中设备和第一服务器尚未访问用于保护第一受保护通信信道的密钥。因此,可能需要生成密钥并在设备与服务器之间共享这些密钥。然而,对于存储器受限的设备或处理能力有限的设备(其可能缺少对非对称密钥加密中使用的非对称密钥生成操作的支持),安全地(按密钥是安全的不会被第三方窥探的信任程度)生成密钥并将这些密钥分发给第一服务器可能具有挑战性。另外,可能需要向第一服务器提供对将使用密钥通过第一受保护的通信信道进行通信的设备的身份的信任。

[0017] 在下面讨论的技术中,设备可以利用第二服务器能够通过第二受保护通信信道与第一服务器进行通信的事实,使得对称密钥可由第一服务器提供给第二服务器并且被保护免受第三方在传输期间访问。这使得缺少对非对称密钥加密的支持的设备能够更安全地进入到与第一服务器的通信中。

[0018] 因此,基于设备标识密钥和公钥信息的设备,在设备处和第二服务器处导出对称密钥。设备标识密钥是先前已在设备与第二服务器之间共享的值。公钥信息取决于与第一服务器相关联的第一服务器公钥。第二服务器在第二受保护通信信道上将对称密钥发送到第一服务器。设备和第一服务器可使用取决于对称密钥的通信密钥进入到第一受保护通信信道上的受保护的通信。因此,当第一服务器与第二服务器之间的第二受保护的通信信道

被保护时,这使得对称密钥到第一服务器的分发比通过设备本身更安全。另外,通过使用公钥信息在第一服务器和第二服务器两者处导出对称密钥,对称密钥是特定于设备希望与之进行通信的特定第一服务器而生成的,而不是在多个服务器之间共享的通用密钥,这提高安全性。另外,通过将用于生成对称密钥的公钥信息基于第一服务器的公钥,第二服务器可直接从第一服务器本身或从第三方认证机构获得第一服务器的公钥,这消除了当进入与第一服务器的通信中时在设备与第二服务器之间维护的通信信道的任何需要,因此可有助于节约功率,这对于诸如传感器或物联网中使用的其他小型处理设备的功率受限设备尤其重要。

[0019] 第二受保护通信信道可以是确保真实性(信任通信方的身份)和机密性(信任只有消息的预期接收者可学习消息的内容)的任何信道。例如,第一服务器与第二服务器之间的信道可使用物理安全链路或者使用虚拟专用网络(VPN,例如使用IPSec或SSL)或者使用预共享密钥(PSK)加密消息密或者使用非对称密钥加密。与第一受保护通信信道不同,第一设备可能无法生成非对称密钥并且在设备与第一服务器之间可能没有用于保护通信的预共享密钥材料直到执行本技术的方法为止,可以借助于先前共享的材料或者通过通信信道的物理保护或者通过第一服务器和/或第二服务器可以支持生成非对称密钥使得可在第一服务器与第二服务器之间建立安全信道的事实来保护第二受保护通信信道。

[0020] 在一些示例中,可以使用基于非对称密钥的公钥基础设施来保护第二受保护通信信道。例如,第二服务器可使用第一服务器的公钥来对所发送的对称密钥进行加密,并且消息可由第一服务器使用第一服务器的私钥来解密(以确保机密性)。或者,可以使用非对称密钥来保护第二对称密钥(与由设备和第二服务器生成的对称密钥不同)的传输,然后可使用第二对称密钥来保护将由第二服务器用来为第一受保护通信信道形成通信密钥的(第一)对称密钥的传输。例如,可以使用TLS(传输层安全性),其中非对称密钥加密用于在第二受保护通信信道上共享对称密钥,然后所共享的对称密钥用于保护信道本身上的业务。另外,可以对第二受保护通信信道上的消息进行签名以使得能够验证真实性。因此,存在能使用公钥基础设施来保护第二受保护通信信道的许多方式,但是通常这会利用第一/第二服务器处的更大的资源使用非对称密钥,以允许能力较弱的设备进入到与第一服务器的安全通信。

[0021] 如果非对称密钥用于保护第一服务器与第二服务器之间的通信信道,则在一些示例中,这些非对称密钥可能是非对称密钥对,其中公钥与用于在设备和第二服务器处生成对称密钥的第一服务器公钥不同。

[0022] 然而,在其他示例中,保护第一服务器与第二服务器之间的第二受保护通信信道的公钥基础设施的非对称密钥可以包括第一服务器公钥和第一服务器私钥。也就是说,用于在设备和第二服务器处导出对称密钥的第一服务器公钥可以是与由第二服务器使用来保护到第一服务器的传输的第一服务器公钥相同的密钥。例如第二服务器可以使用第一服务器的公钥来对对称密钥的传输进行加密,以便确保仅具有正确的第一服务器私钥的第一服务器才能够解密对称密钥。或者,与第二受保护通信信道相关联的非对称密钥可以用于在第一服务器与第二服务器之间共享第二对称密钥,然后第二对称密钥可用于保护(第一)对称密钥在第二受保护通信信道上的传输,其中依赖于(第一)对称密钥的通信密钥然后用于保护第一受保护通信信道。

[0023] 因此,通过这种机制,相同的密钥信息既用于导出对称密钥又用于保护对称密钥从第二服务器到第一服务器的传输。这将被视为反直觉的,因为在安全处理算法的领域中,对于两种不同的密钥分发目的使用相同的信息通常会认为对安全性有潜在危害。然而,通过使用相同的第一服务器公钥来导出对称密钥并且保护第二服务器与第一服务器之间的传输,可确保为了与特定服务器通信而生成的密钥既特定于该特定服务器并且仅与该特定服务器共享,因为只有具有第一服务器私钥的第一服务器可读取从第二服务器发送的对称密钥,并且公钥基础设施可提供证明第一服务器的身份的证书,使得可增加设备的信任。

[0024] 在一些实施方式中,用于保护设备与第一服务器之间的第一受保护通信信道上的通信的通信密钥可以与在设备和第二服务器处生成的对称密钥相同。如果可信任第二服务器(例如,第二服务器可以由受信任的认证机构或设备验证服务提供商操作),则此方法可能是最容易实现的并且可以是可接受的。

[0025] 然而,在其他示例中,通信密钥可以与对称密钥不同。例如可以基于设备与第一服务器之间共享的信息从对称密钥导出通信密钥。以这种方式,可以从第二服务器隐藏用于保护设备与第一服务器之间的第一受保护通信信道上的实际通信的密钥。(基于在设备与第一服务器之间共享的信息)应用于对称密钥的任何后处理功能可以用于生成通信密钥。例如,可以应用附加散列(hash)函数。在设备与第一服务器之间共享的信息可例如包括以下中的至少一个:与包括设备的设备类相关联的类密钥(例如,类中的所有设备已知但是第二服务器不知道的密钥)和/或随机或伪随机值。例如,随机或伪随机值可由设备通过第二服务器无法访问的通信路由发送到服务器。例如,随机或伪随机数可以由第一服务器公钥加密的加密形式传输。

[0026] 在一些示例中,由设备和第二服务器两者用于导出对称密钥的公钥信息可以与第一服务器公钥本身完全相同。因此,在一些情况下,第一服务器的整个公钥可以是用于导出对称密钥的函数的输入参数。

[0027] 然而,在其他示例中,公钥信息可包括第一服务器公钥的散列,其具有比第一服务器公钥本身更少的位。在非对称密钥加密中使用的密钥通常非常长,为了减少存储器存储要求并且不需要设备知道第一服务器的完整且可能大的公钥,替代地设备可提供有第一服务器的公钥的散列。第二服务器还可以获得第一服务器的公钥相同的散列,并且使用它来导出对称密钥。

[0028] 设备标识密钥可以是特定于设备的任何值。例如,它可能是在制造期间嵌入在设备中的设备标识符,或在设备内生成的随机数。可以以多种不同的方式与第二服务器共享设备标识密钥。在一个示例中,如果向设备提供了其设备标识密钥的工厂或适配站知道第二服务器的公钥,则它可用第二服务器的公钥对设备标识密钥进行加密,然后第二服务器将能够使用其私钥来对设备标识密钥进行解密。来自工厂或适配站的设备标识密钥的传输能由与工厂或适配方相关联的私钥来签名以证明这是有效设备标识密钥。此传输可以将设备标识密钥与和设备相关联的某个其他标识符相关联,使得稍后可以存储多个不同的设备的设备识别密钥的第二服务器可为第一服务器需要与其进行通信的特定设备查找适当的设备标识密钥。

[0029] 在用于与第二服务器共享设备标识密钥的替代方法中,设备可以向第二服务器发送包含设备标识密钥和设备的相应标识符的加密和签名消息,该相应的标识符使用第二服

务器的公钥来加密并且使用与制造或者认证设备的工厂或适配站相关联的公钥来签名。这可使得设备能够信任只有第二服务器可对其设备标识密钥进行解密,并且使得第二服务器能够信任所接收到的设备标识密钥来自具有证明身份的设备。当通过第一受保护通信信道进入与设备的通信中时,第二服务器对设备的这种信任然后还可以扩展到第一服务器。

[0030] 设备可能无法生成用于支持公钥基础设施的非对称密钥(例如椭圆曲线计算)。用于生成非对称密钥的对的算法通常极其复杂并且要求大量的存储器存储以及功率来运行。对于可能对存储器容量和功率预算具有极端约束的低成本物联网设备来说,这可能是不可行的。

[0031] 在一个示例中,设备可以导出对称密钥,然后在使用通信密钥保护的第一受保护通信信道上向第一服务器发送有效负载消息,然后响应于该有效负载消息,第一服务器可以向第二服务器发送密钥生成请求以触发第二服务器导出对称密钥并且通过第二受保护通信信道将对称密钥发送到第一服务器。因此,上面讨论的方法的一个优点是它使得设备能够使用“即发即忘”方法,其中它仅需要向已经使用通信密钥保护的第一服务器发送一个消息,并且此有效负载消息可以触发第一服务器从第二服务器获得对称密钥,而无需再次与设备进行通信。这对于可以由电池供电的物联网类型设备来说可能是非常有用的,为此节省电力对于改善电池寿命可能是极其重要。相反,如果利用在服务器上而不是在设备上生成密钥的替代技术,则设备将必须请求通信,稍后从服务器接收密钥,然后开始通信,这意味着需要发送多个消息。

[0032] 从设备到第一服务器的有效负载消息(发起通信)以及从第一服务器到第二服务器的密钥生成请求(触发第二服务器导出对称密钥)都可以指定设备的设备标识符。第二服务器可以存储与具有不同的设备标识符的多个不同的设备相关联的设备标识密钥的记录。因此,包括在密钥生成请求中的设备标识符使得第二服务器能够为想要与第一服务器进行通信的设备定位正确的设备标识密钥,并且为该设备生成适当的对称密钥。

[0033] 图1示意性地示出了包括计算设备D、第一服务器S和第二服务器T的系统100。例如,设备D可以例如是物联网(IoT)中的设备,例如加热或空调系统内的温度传感器、用于控制街道照明的致动器或由患者穿戴的将数据反馈给医疗计算系统的心率传感器。应当理解,这些只是设备的可能用途的一些示例。第一服务器S可以是由正在使用来自设备D的数据的服务提供商(例如,医疗保健提供商、银行系统或公共服务提供商)运行的云平台。第二服务器T可以是由安全平台管理服务维护的验证服务器,其可以提供支持第一服务器S确定可安全地与哪些设备D进行通信的认证服务。

[0034] 设备D可能希望与第一服务器S建立第一受保护通信信道,但是可能无法生成可用于保证第一受保护通信信道上的通信的非对称密钥。然而,第一服务器S和第二服务器T可以通过第二受保护通信信道来通信,第二受保护通信信道被保护以提供真实性和机密性,例如使用基于非对称密钥的公钥基础设施(PKI)、物理安全信道、VPN或者基于预共享密钥材料。

[0035] 图2示意性地示出了设备D的示例,设备D具有处理电路(例如,中央处理单元(CPU))2以及用于存储数据和由处理电路2执行的程序代码6的存储电路4(存储器)。存储器4还可以存储与公钥基础设施相关联的密钥8或证书。显然,其他数据也可以被存储在存储器4内。在一些情况下,存储器4可以被划分成安全区域和较不安全区域,其中安全区域例如

仅可从处理电路2的可信执行环境访问,而较不安全区域可从可信执行环境和处理电路2的正常执行环境两者访问。可以根据诸如由Arm®有限公司提供的TrustZone®架构的硬件架构来监视和控制处理电路2在可信执行环境与正常执行环境之间的转变。

[0036] 设备D还可以具有用于感测诸如温度、压力、红外辐射等外部条件的一个或多个传感器10、用于向用户显示信息的显示器12、用于接受来自用户的输入手势的用户输入装置14、以及用于例如通过诸如WiFi®、蓝牙®或NFC的无线协议或者通过有线通信(例如以太网)与其他设备进行通信的通信接口16。各种元件2、10、12、14、4、16可以通过至少一条总线18进行通信。

[0037] 应当理解,图2仅是用于设备D的可能架构的一个示例,并且其他示例可以具有图2中未示出的多个其他组件。另外,在一些示例中,设备D可以不具有任何显示器12和/或用户输入装置14。例如,一些物联网设备可以仅感测关于其周围环境的信息并且将所感测到的信息(或从所感测到的信息导出的数据)传送到外部设备,因此可能不需要任何用户界面或显示器。另外,在一些设备中,除了(或代替)传感器10之外,可以提供控制单元或致动器以触发相关控制功能,例如照明或加热系统的控制或警报的发声。

[0038] 第一服务器S和第二服务器T也可以具有与图2中所示类似的CPU 2、存储器4和通信接口16。然而,与设备D相比较,服务器S、T的处理电路2可以比设备D中的处理电路2更强大(能够以更高频率和/或指令吞吐量执行)。类似地,服务器S、T中的存储器4的容量可能比设备D中的存储器的容量大得多。例如,设备D的存储器可能极其受限,因此许多仅具有大约几百kB的持久性存储。另外,服务器S、T不需要包括如图2中所示的传感器10、显示器和/或用户输入装置14。

[0039] 图3示出了用于设备D和第一服务器S建立第一受保护通信信道的方法,其中确信设备D可信任只有第一服务器S能够读取其消息,并且其中第一服务器S信任消息来自正确的设备D。

[0040] 在执行图3的方法之前,设备D和第二服务器T具有共享信息,该共享信息指定标识特定设备D的设备标识符(DID)和设备标识密钥K_D,设备标识密钥K_D是由设备D保持的任何秘密信息,例如随机地或伪随机地生成的数字。在一些示例中,设备标识密钥K_D可以在工厂中被生成并嵌入到设备D中,并且还以安全方式上载到第二服务器T(利用与工厂相关联的非对称密钥保护DID和K_D到第二服务器T的传送)。

[0041] 可替代地,可以在设备D本身内例如通过随机或伪随机数生成器生成设备标识密钥K_D,这可提供更大的安全性。在这种情况下,设备D可以生成包括设备标识符DID和设备标识密钥K_D的消息并且使用与第二服务器相关联的私钥T_{public}来对该消息进行加密,以及用工厂公钥F_{public}对该消息进行签名。在接收到此消息时,第二服务器T然后可基于使用工厂密钥提供的签名来验证该设备被证明且可被信任并且可使用其自己的私钥$T_{private}$来对该消息进行解密以保证仅第二服务器T可接收将设备的标识(DID)绑定到设备将使用的密钥K_D的信息。

[0042] 在该特定示例中,通过基于与第一服务器S相关联的非对称密钥对的公钥基础设施(PKI)来保护第一服务器S与第二服务器T之间的第二受保护通信信道,非对称密钥对包括由第一服务器S保持的私钥$S_{private}$以及第二服务器T和设备D可用的公钥S_{public}。在一些情

况下,设备D不需要看到第一服务器的完整公钥,而是替代地可接收S_{public}的缩减大小散列。在图3的步骤S10,设备D基于包括设备标识密钥K_D和第一服务器公钥S_{public}(或S_{public}的散列)的信息的第一散列函数fn1导出对称密钥K_S。在步骤S12,设备D导出将用于保护设备D与第一服务器S之间的通信信道上的通信的通信密钥K_C。该通信密钥K_C可以与对称密钥K_S相同,或者可通过将另一散列函数fn2应用于包括对称密钥K_S和共享信息X的信息来生成,共享信息X将通过对第二服务器T不可访问的机制与第一服务器S共享。如果第二服务器T可被信任,则第二服务器T知道将在设备D与第一服务器S之间的信道上使用的通信密钥K_C可以是可接受的,并且在这种情况下,K_C等于K_S可以是可接受的。然而,如果需要进一步的安全性,则可以使用与第一服务器S共享的附加信息X哈希K_S以生成K_C。例如,共享信息X可以是由设备D生成的随机或伪随机数,或者可以是特定于包括设备D的设备类的类标识符。第二散列函数fn2可以是与第一散列函数fn1不同的散列函数,或者可替代地函数fn1、fn2可以是相同的散列函数(例如SHA256)。

[0043] 在步骤S14,设备D基于在步骤S12处生成的通信密钥K_C对其希望向第一服务器S发送的有效负载消息进行加密。在步骤S16,设备D将加密后的有效负载消息、设备标识符DID以及可选地共享信息X发送到第一服务器S。因为在步骤S16中加密的有效负载包括设备D希望向第一服务器S发送的实际信息,并且这是自导出对称密钥K_S以来发起的第一消息,所以在发送有效负载之前不需要与第一服务器S进行任何初步通信以建立通信密钥K_C。这对于IoT功率受限设备来说是有用的,因为“即发即忘”方法意味着可减少设备D需要给其通信单元16加电的次数,这有助于节约电力并延长电池寿命。在一些情况下,也可基于第一服务器的公钥S_{public}对加密后的有效负载S16进行加密以确保它仅可由第一服务器S通过使用第一服务器的私钥$S_{private}$解密消息来读取。例如,在消息包括需要从第二服务器T或其他服务器隐藏的共享信息X的情况下,这可能是有用的。

[0044] 响应于在步骤S16接收到加密后的有效负载,在步骤S18,第一服务器向第二服务器T发送密钥生成请求,其指定与有效负载一起接收到的设备标识符DID。作为响应,在步骤S20,第二服务器T在其设备数据库中查找与所指定的设备标识符DID相对应的条目,并且获得在设备D与第二服务器T之间先前共享的设备标识密钥K_D。在步骤S22,第二服务器T基于设备标识密钥K_D和第一服务器的公钥S_{public}(或S_{public}的散列)使用与步骤S10相同的散列函数fn1来导出对称密钥K_S。在步骤S24,第二服务器T生成包含对称密钥K_S的受保护数据传输,该对称密钥K_S使用非对称密钥对$S_{private}$、S_{public}来保护。例如,使用第一服务器的公钥S_{public}加密K_S的传输。在接收时,第一服务器使用其私钥$S_{private}$对消息进行解密,由此获得对称密钥K_S。如果在步骤S12通信K_C等于K_S,则在步骤S24由第一服务器S获得的对称密钥K_S可简单地被用作通信密钥K_C,因此在步骤S26第一服务器S使用通信K_C对在步骤S16接收到的有效负载进行解密。然而,如果在步骤S12设备D基于共享信息X应用了另一个散列,则在步骤S28第一服务器S可以基于在步骤S16接收到的共享信息X应用相应的散列函数fn2,然后在导出通信密钥K_C后,可在步骤S26利用通信密钥K_C对有效负载进行解密。

[0045] 后续通信然后可在设备D与第一服务器S之间继续,使用通信密钥K_C来加密和解密。

[0046] 因此,利用这种方法,利用保护第一服务器S与第二服务器T之间的信道的PKI来增强无法生成非对称密钥的设备D与第一服务器S之间的密钥分发的安全性。由于用于导出通

信密钥的K_C的对称密钥K_S是基于设备特定密钥K_D和第一服务器的公钥S_{public}两者导出的,所以它特定于该对通信设备,并且所以不能被不同的设备D或不同的第一服务器S重用。由于相同的信息S_{public}由第二服务器T用来导出要发送到第一服务器S的对称密钥K_S并且保护在传输信道上到第一服务器S的传输,因此这确保了只有有效的第一服务器S将能够使用通信密钥K_C成功地与设备D进行通信。另外,由于设备标识符DID和设备密钥K_D在设备D与第二服务器T之间的较早共享可以被工厂或其他认证机构证明是有效的,因此可以向第一服务器S提供对设备D的身份的信任。

[0047] 在图3的示例中,通过使用第一服务器的公钥S_{public}对对称密钥K_S进行加密来保护第二受保护通信信道。然而,使用非对称密钥保护K_S的另一方式将是使用非对称密钥对$S_{private}$、S_{public}来保护临时对称密钥K_T的传输,并且然后使用临时对称密钥K_T对K_S从第二服务器T到第一服务器S的传输进行加密。可以为每个密钥生成请求新近生成临时对称密钥K_T。

[0048] 可替代地,可以以不使用PKI的非对称密钥的其他方式保护第二受保护通信信道,例如通过物理安全信道、VPN或者通过基于先前在第一服务器S与第二服务器T之间共享的预共享密钥的加密。

[0049] 在本申请中,术语“被配置为……”用于意指装置的元件具有能够执行所定义的操作的配置。在此上下文中,“配置”意指硬件或软件的互连的布置或方式。例如,装置可以具有提供所定义的操作的专用硬件,或者处理器或其他处理设备可以被编程以执行功能。“被配置为”并不暗示需要以任何方式改变装置元件以提供定义的操作。

[0050] 尽管参考附图在本文中详细描述了本发明的示例性实施例,然而应当理解的是,本发明不限于这些精确的实施例,并且在不脱离如所附权利要求限定的本发明的范围和精神的情况下,本领域的技术人员可在其中实现各种变化和修改。

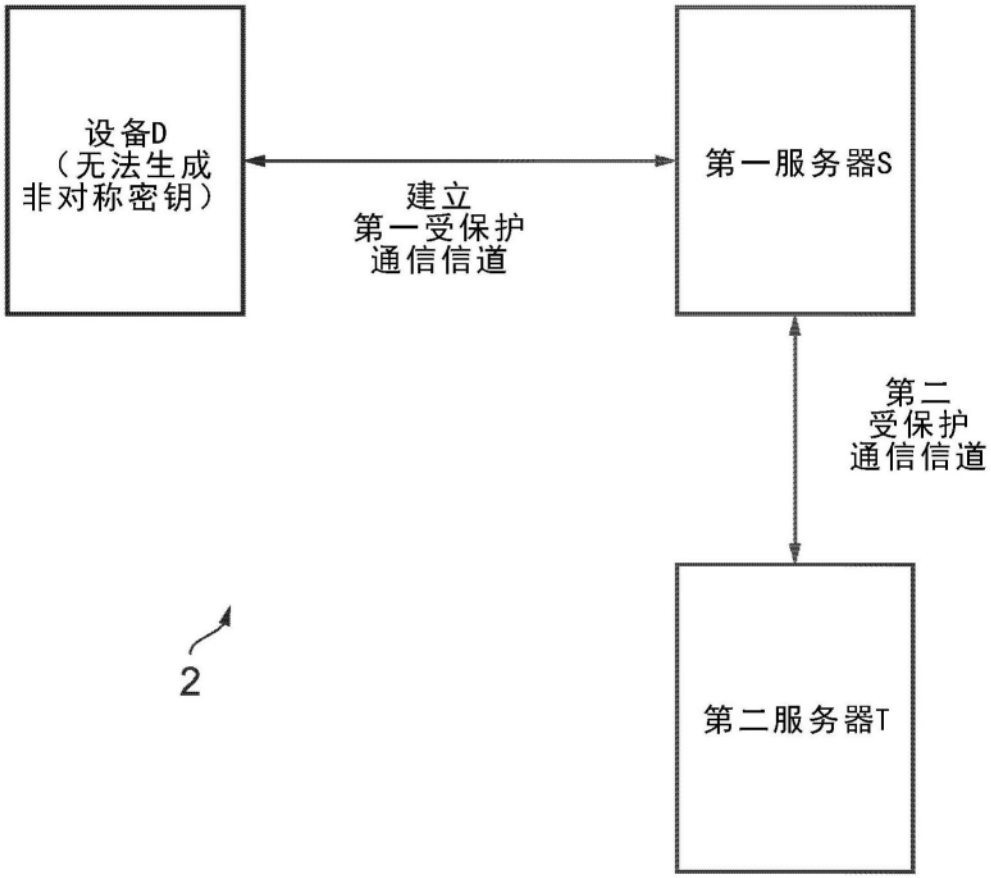


图1

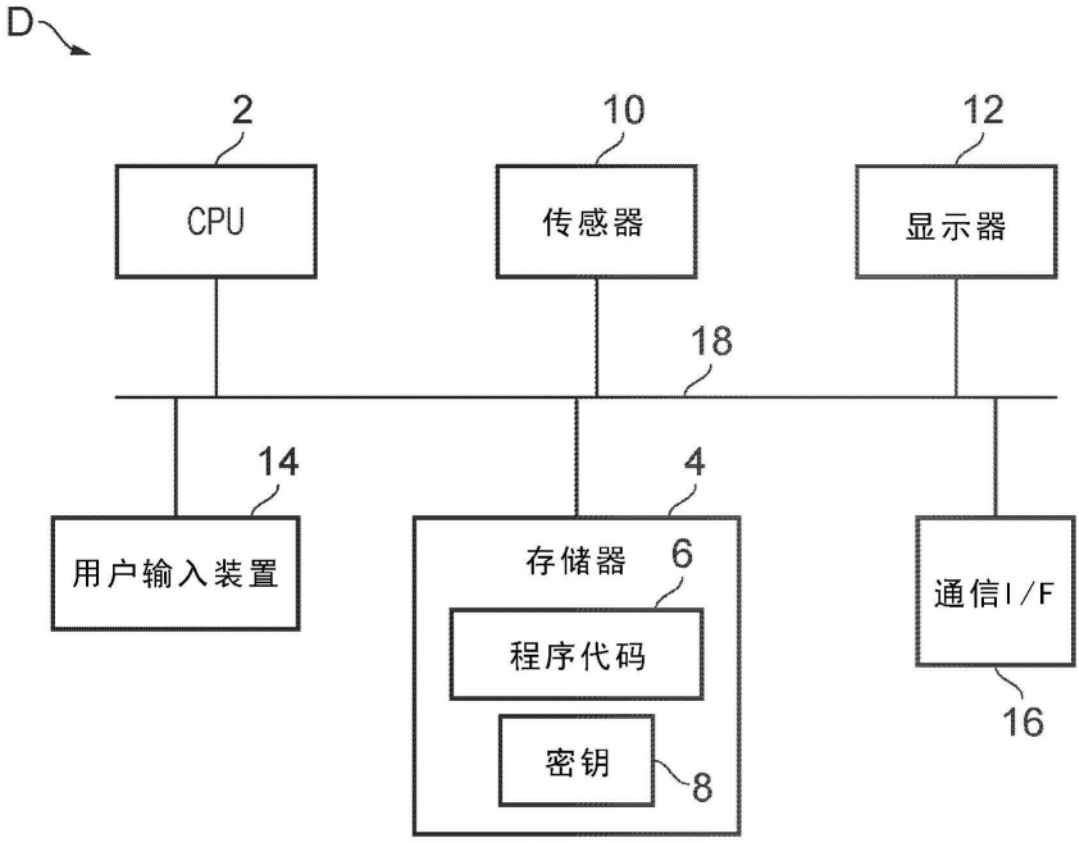


图2

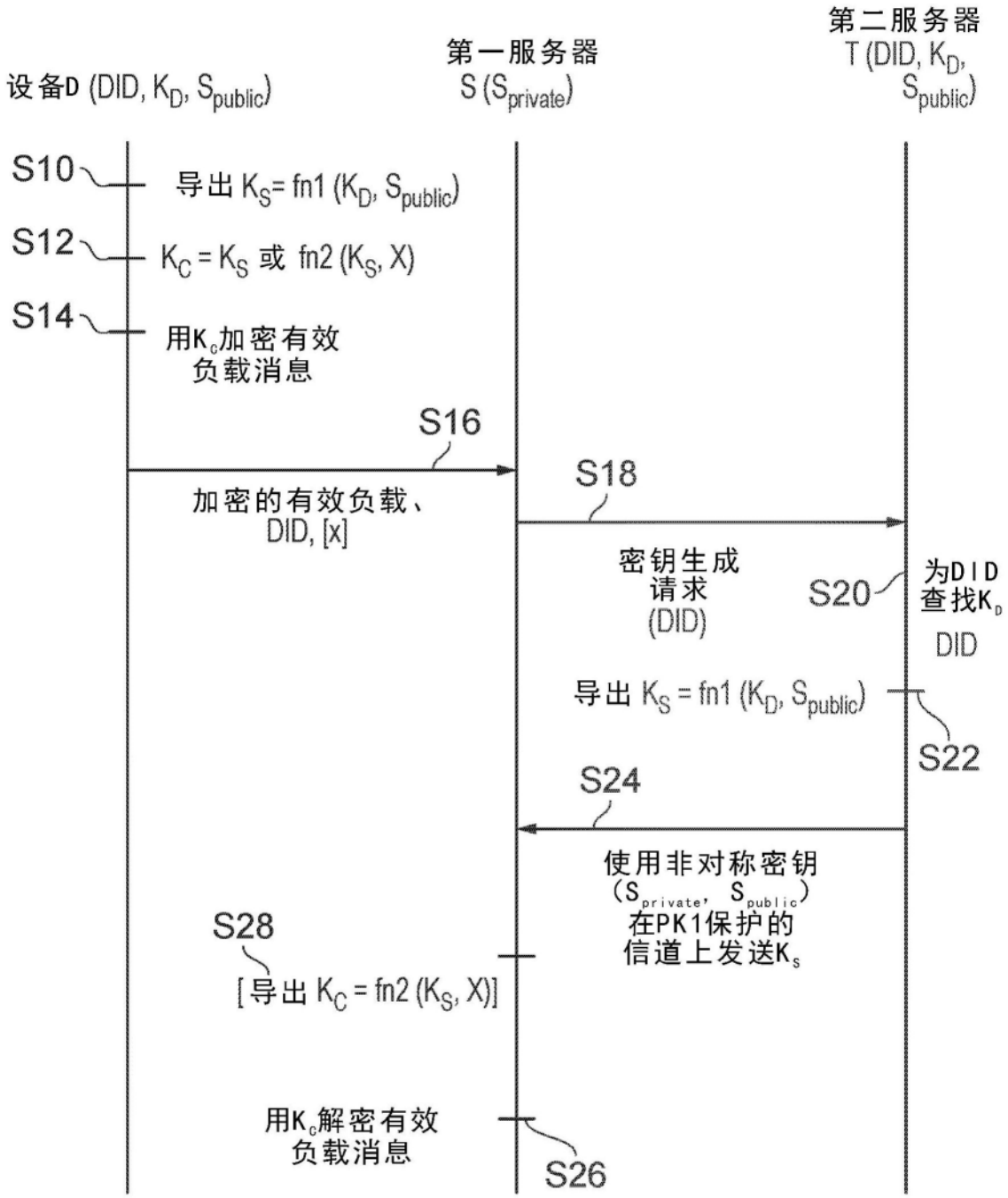

设备D (DID, K_D, S_{public})
第一服务器
S ($S_{private}$)
第二服务器
T (DID, K_D, S_{public})
S10
导出 K_S= fn1 (K_D, S_{public})
S12
K_C = K_S 或 fn2 (K_S, X)
S14
用K_c加密有效负载消息
S16
加密的有效负载、DID, [x]
S18
密钥生成请求 (DID)
S20
为DID查找K_D
DID
导出 K_S = fn1 (K_D, S_{public})
S22
S24
使用非对称密钥 ($S_{private}$, S_{public}) 在PK1保护的信道上发送K_s
S28
[导出 K_C = fn2 (K_S, X)]
用K_c解密有效负载消息
S26

图3