(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 110036597 A
(43)申请公布日 2019.07.19

(21)申请号 201780074954.9

(22)申请日 2017.12.06

(30)优先权数据
15/375,066 2016.12.09 US

(85)PCT国际申请进入国家阶段日
2019.06.03

(86)PCT国际申请的申请数据
PCT/US2017/064791 2017.12.06

(87)PCT国际申请的公布数据
WO2018/106744 EN 2018.06.14

(71)申请人 微软技术许可有限责任公司
地址 美国华盛顿州

(72)发明人 A·布兰克

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华 丁君军

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)

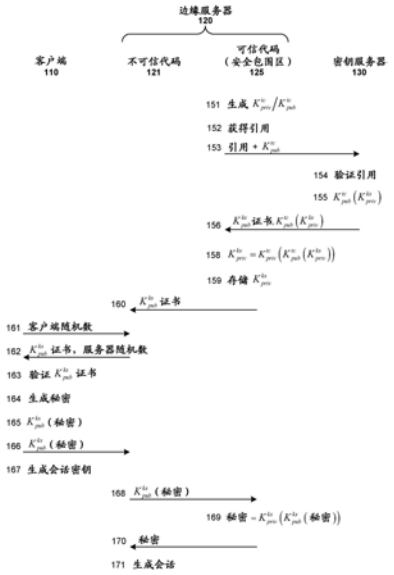
权利要求书3页 说明书9页 附图5页

(54)发明名称

用于由不可信代码使用的安全分布私有密钥

(57)摘要

描述了一种安全密钥系统，其将密钥服务器的私有密钥分布到边缘服务器，以用于在建立与客户端的会话时代表私有密钥的所有者进行加密。为了分布私有密钥，密钥服务器从边缘服务器接收由边缘服务器的安全包围区所生成的引用。引用证明安全包围区的代码。密钥服务器验证引用以确保安全包围区的代码是可信代码。密钥服务器使用边缘服务器的密钥对私有密钥进行加密并且将加密的私有密钥发送到安全包围区。安全包围区的代码使用其密钥对私有密钥进行解密。边缘服务器的不可信代码然后请求安全包围区的代码，以使用私有密钥执行加密动作。



CN 110036597 A

1.一种由计算系统执行的方法,所述方法用于向第二设备提供第一设备的第一密钥,以用于代表所述第一密钥的所有者执行加密动作,所述方法包括:

访问所述第二设备的第二密钥;

从所述第二设备接收由安全包围区生成的引用,所述引用证明所述安全包围区的代码;

验证所述引用以确保所述安全包围区的所述代码是可信代码;

使用所述第二密钥对所述第一密钥进行加密;以及

在所述引用被验证之后,向所述第二设备发送加密的所述第一密钥。

2.根据权利要求1所述的方法,其中所述第二设备是内容递送网络的边缘服务器,并且所述第一设备是所述内容递送网络的客户的密钥服务器,所述客户的内容由所述内容递送网络递送。

3.根据权利要求2所述的方法,其中所述第一密钥被提供给所述内容递送网络的多个边缘服务器,使得每个边缘服务器能够接受传输层安全权证以恢复会话,而不管哪个边缘服务器生成所述权证。

4.根据权利要求1所述的方法还包括:在向所述第二设备发送加密的所述第一密钥之后,

从所述第二设备接收对于所述第一密钥的更新请求;

当妥协准则未被满足时,向所述第二设备发送更新通知;以及

当所述妥协准则被满足时,抑制所述更新通知的所述发送。

5.一种由计算系统执行的方法,所述方法用于获得第一设备的第一密钥,以用于由第二设备代表所述第一密钥的所有者执行加密动作,所述方法包括:

在所述第二设备的安全包围区的控制下,

生成证明所述安全包围区的代码的引用;

指导所述引用被发送到所述第一设备;

从所述第一设备接收所述第一设备的所述第一密钥,所述第一密钥利用所述第二设备的第二密钥被加密;

基于利用所述第二密钥的加密,对所述第一密钥进行解密;以及

将解密的所述第一密钥存储在所述安全包围区内,使得解密的所述第一密钥在所述安全包围区的外部不可访问。

6.根据权利要求5所述的方法,还包括:

在所述第二设备的所述安全包围区的控制下,

从所述第二设备的不可信代码接收对数据执行加密动作的请求;

使用所述第一密钥对所述数据执行所述加密动作以生成结果数据;以及

向所述不可信代码提供所述结果数据。

7.根据权利要求5所述的方法,其中所述第二设备是内容递送网络的边缘服务器,并且所述第一设备是所述内容递送网络的客户的密钥服务器,所述客户的内容由所述内容递送网络递送。

8.一种由计算系统执行的方法,所述方法用于由第二设备代表公共/私有密钥对的私有密钥的所有者建立与客户端的传输层安全会话,所述方法包括:

从所述客户端接收对于建立会话的请求，所述请求包括客户端随机数；

向所述客户端发送公共/私有密钥对的公共密钥证书和服务器随机数；

从所述客户端接收使用所述公共密钥被加密的加密秘密；以及

请求所述计算系统的安全包围区，以使用第一设备的所述私有密钥对加密的所述秘密进行解密，所述安全包围区基于被提供给所述第一设备的引用已经从所述第一设备获得所述私有密钥，所述引用证明所述安全包围区的代码是可信代码。

9.根据权利要求8所述的方法，还包括：

从所述安全包围区接收解密的所述秘密；以及

基于所述客户端随机数、所述服务器随机数和所述秘密，生成用于所述会话的会话密钥。

10.一种密钥服务器，所述密钥服务器用于向边缘服务器提供所述密钥服务器的私有密钥，以用于在建立与客户端的会话时代表所述私有密钥的所有者执行加密动作，所述密钥服务器包括：

计算机可读存储介质，其存储计算机可执行指令，所述计算机可执行指令当被执行时，使得所述密钥服务器：

访问所述边缘服务器的安全包围区的密钥；

从所述边缘服务器接收由所述边缘服务器的所述安全包围区生成的引用，所述引用证明所述安全包围区的代码；

验证所述引用以确保所述安全包围区的所述代码是可信代码；

使用所述边缘服务器的所述安全包围区的所述密钥对所述私有密钥进行加密；以及

在所述引用被验证之后，向所述边缘服务器发送加密的所述私有密钥；以及

处理器，其执行被存储在所述计算机可读存储介质中的所述计算机可执行指令。

11.根据权利要求10所述的密钥服务器，其中所述边缘服务器是内容递送网络的边缘服务器，并且所述密钥服务器是所述内容递送网络的客户的密钥服务器，所述客户的内容由所述内容递送网络递送。

12.根据权利要求11所述的密钥服务器，其中会话密钥被提供给所述内容递送网络的多个边缘服务器，使得每个边缘服务器能够接受传输层安全权证以恢复会话，而不管哪个边缘服务器生成所述权证。

13.一种边缘服务器，所述边缘服务器用于获得密钥服务器的私有密钥，以用于在建立与客户端的会话时代表所述私有密钥的所有者执行加密动作，所述边缘服务器包括：

计算机可读存储介质，其存储计算机可执行指令，所述计算机可执行指令当被执行时，使得所述边缘服务器在所述边缘服务器的安全包围区的控制下：

生成证明所述安全包围区的代码的引用；

指导所述引用被发送到所述密钥服务器；

从所述密钥服务器接收所述密钥服务器的所述私有密钥，所述私有密钥利用所述边缘服务器的所述安全包围区的密钥被加密；

基于利用所述边缘服务器的所述安全包围区的所述密钥的加密，对所述私有密钥进行解密；以及

将解密的所述私有密钥存储在所述安全包围区内，使得解密的所述私有密钥在所述安

全包围区的外部不可访问;以及

处理器,其执行被存储在所述计算机可读存储介质中的所述计算机可执行指令。

14.根据权利要求13所述的边缘服务器,其中所述计算机可执行指令还使得所述边缘服务器在所述边缘服务器的所述安全包围区的控制下:

从所述边缘服务器的不可信代码接收对加密数据进行解密的请求;

使用所述私有密钥对所述加密数据进行解密;以及

向所述不可信代码提供解密的所述数据。

15.一种边缘服务器,所述边缘服务器用于代表公共/私有密钥对的私有密钥的所有者建立与客户端的传输层安全会话,所述边缘服务器包括:

计算机可读存储介质,其存储计算机可执行指令,所述计算机可执行指令当被执行时,使得所述边缘服务器:

从所述客户端接收对于建立会话的请求,所述请求包括客户端随机数;

向所述客户端发送用于公共/私有密钥对的公共密钥证书和服务器随机数;

从所述客户端接收使用所述公共密钥被加密的加密预先主秘密;以及

请求所述边缘服务器的安全包围区的可信代码,以使用所述私有密钥对所述加密预先主秘密进行解密,所述安全包围区基于由所述安全包围区生成并且被提供给所述密钥服务器的引用已经从密钥服务器获得所述私有密钥,所述引用证明所述安全包围区的代码是可信代码;以及

处理器,其执行被存储在所述计算机可读存储介质中的所述计算机可执行指令。

用于由不可信代码使用的安全分布私有密钥

背景技术

[0001] 传输层安全(“TLS”)是广泛地用于经由因特网安全地通信的加密协议。TSL确保通信的隐私性和完整性以及通信方的真实性。确保通信的隐私性,因为每个通信(或者消息)利用仅对通信方已知的对称密钥而被加密。使用消息验证码确保完整性。使用公共/私有密钥对确保通信方的真实性。

[0002] 客户端通过初始地向服务器发送包括“客户端随机数”的消息与服务器建立TLS会话。作为响应,服务器利用“服务器随机数”和公共密钥证书进行响应。客户端随机数和服务器随机数是由客户端和服务器分别地生成的随机数,尽管随机数可以包括时间戳。公共密钥验证包括服务器的公共密钥以及服务器的公共密钥证书。客户端然后向服务器发送使用公共密钥加密的“预先主秘密”。预先主秘密是数据块,其可以根据客户端随机数和服务器随机数而被生成。客户端然后使用算法根据客户端随机数、服务器随机数和预先主秘密来创建TLS会话密钥。当服务器接收到预先主秘密时,服务器利用其私有密钥对其进行解密。服务器然后使用相同算法根据客户端随机数、服务器随机数和预先主秘密来创建TLS会话密钥。客户端和服务器可以然后通过使用TLS会话密钥(其是对称密钥)的其自己的副本加密和解密通信来安全地通信。

[0003] 想要向其用户(例如,订阅者)提供内容的一些组织(例如,新组织和电子商务公司)可以订约以使中介将内容分发给用户。内容递送网络(“CDN”)是这样的中介的示例。CDN是可以全球地部署的代理服务器的分布式网络。CDN可以具有经由高速通信骨干网连接到服务器的边缘服务器。连接的服务器可以是托管客户的内容的CDN服务器或者可以是托管内容的客户服务器。边缘服务器代表客户与用户建立TLS会话。一旦针对客户和用户建立TLS会话,则CDN向用户提供客户的内容。CDN可以将内容高速缓存在边缘服务器处以当服务内容时改进响应时间。

[0004] 当代表客户建立TLS会话时,边缘服务器需要向客户端(即,用户的设备)发送其客户的公共密钥证书,并且需要具有利用其客户的私有密钥解密的预先主秘密。对于边缘服务器而言,存储其客户的私有密钥可能是危险的。如果甚至一个边缘服务器被妥协(例如,由网络攻击),则可以窃取所有私有密钥。

[0005] 避免妥协的边缘服务器的该风险的一个技术是不将客户的任何私有密钥存储在边缘服务器上。当预先主秘密需要由客户的私有密钥解密时,边缘服务器向客户的密钥服务器发送请求以对被包括在请求中的预先主秘密进行解密。客户的密钥服务器对预先主秘密进行解密并且经由安全信道将解密的预先主秘密发送到边缘服务器。虽然该技术避免妥协的边缘服务器的风险,该技术要求与密钥服务器的往返通信以用于建立的每个TLS会话,其在金钱和计算资源方面是昂贵的并且延迟TLS会话的建立。

发明内容

[0006] 描述了一种安全密钥系统,其中第一设备将第一设备的第一密钥提供到第二设备,以用于代表第一密钥的所有者执行加密动作。在一些实施例中,第一设备从第二设备接

收由安全包围区(enclave)所生成的引用(quote)。引用证明安全包围区的代码和第二设备的第二密钥。第一设备验证引用以确保安全包围区的代码是可信代码并且第二密钥用于安全包围区。第一设备使用第二设备的第二密钥对第一密钥进行加密。在验证引用之后,第一设备向第二设备发送加密的第一密钥。

[0007] 在一些实施例中,第二设备在第二设备的安全包围区的控制下生成引用并且指导引用和第二密钥被发送到第一设备。第二设备然后从第一设备接收第一设备的第一密钥,其利用第二设备的第二密钥被加密。第二设备然后基于利用第二密钥的加密对第一密钥进行解密并且将解密的第一密钥存储在安全包围区内,使得解密的第一密钥在安全包围区的外部是不可访问的。在安全包围区外部执行的第二设备的不可信代码然后请求安全包围区的可信代码使用第一密钥对数据执行加密动作并且将结果数据提供到不可信代码。

[0008] 提供本发明内容以引入以在具体实施方式中下面进一步描述的简化形式的概念的选择。本发明内容不旨标识要求保护的主题的关键特征或基本特征,其也不旨在被用于要求保护的主题的范围。

附图说明

[0009] 图1是图示在一些实施例中采用安全密钥系统的方面的处理的示图。

[0010] 图2是图示在一些实施例中采用安全密钥系统的计算机系统的部件的块图。

[0011] 图3是图示在一些实施例中安全密钥系统的供应密钥服务器私有密钥的部件处理的流程图。

[0012] 图4是图示在一些实施例中安全密钥系统的可信代码的获得密钥服务器私有密钥部件的处理的流程图。

[0013] 图5是图示在一些实施例中安全密钥系统的不可信代码的建立会话部件的处理的流程图。

具体实施方式

[0014] 描述了用于安全地分布密钥并且安全地使用分布密钥的方法和系统。在一些实施例中,安全密钥系统将第一设备的第一密钥(例如,私有密钥)提供到第二(或者中间人)设备,以用于代表第一密钥的所有者对数据执行密码动作(例如,加密数据或者解密数据),以生成结果数据(例如,加密数据或者解密数据)。例如,第一密钥可以是公共/私有密钥对的私有密钥,第一设备可以是作为CDN的客户的私有密钥的所有者的密钥服务器,并且第二设备可以是CDN的边缘服务器。为了分布密钥,第一设备从第二设备接收由第二设备的安全包围区所生成的引用。安全包围区是处理器的硬件特征,其控制可信代码的执行、保护可信代码和其数据二者,并且关于其正执行的代码提供证明(被称为“引用”)。处理器的安全包围区可以从主存储器取回加密可信代码和加密数据,并且对可信代码和数据进行解密,并且将解密的可信代码和数据存储在仅由安全包围区可访问的存储器中。安全包围区然后执行可信代码。安全包围区可以具有公共/私有密钥对并且在引用中包括利用其私有密钥加密的可信代码的散列。安全包围区的示例是英特尔公司的软件保护扩展包围区。第二设备还具有在安全包围区外部执行的不可信代码。术语“可信代码”指代在安全包围区内执行的代码,并且术语“不可信代码”指代在安全包围区外部执行的代码。在其比可信代码更易受妥

协的意义上,不可信代码是不可信的。

[0015] 在第一设备接收到由第二设备发送的引用之后,第一设备验证引用以确保安全包围区的代码是第一设备期望安全包围区执行的可信代码。在验证引用之后,第一设备向第二设备发送第一密钥,其利用第二设备的可信代码的第二密钥被加密。例如,第二密钥可以是CDN的公共/私有密钥对的公共密钥,可信代码可以具有私有密钥,并且密钥服务器可以具有对公共密钥证书的访问。作为另一示例,第二密钥可以是由可信代码和密钥服务器共享的对称密钥。在接收到第一设备的加密的第一密钥时,第二设备的可信代码利用第二密钥对第一设备的第一密钥进行解密并且安全地将第一设备的第一密钥存储在第二设备的安全包围区中。随后地,第二设备的不可信代码可以请求可信代码以使用第一设备的第一密钥对数据进行加密或者解密。以这种方式,第一设备的第一密钥可以安全地由第二设备的安全包围区存储并且被用于对数据进行加密和解密。如此,使第一设备的第一密钥免于在第二设备上执行的不可信代码窃取第一设备的第一密钥的风险。

[0016] 在一些实施例中,CDN的边缘服务器在初始化时,指导其安全包围区加载可信代码。安全包围区可以然后生成证明已经被加载的可信代码的引用。可信代码可以然后指导边缘服务器的不可信代码将引用发送到客户的密钥服务器。作为响应,边缘服务器接收客户的加密的私有密钥,并且不可信代码将加密的私有密钥提供给可信代码。可信代码然后利用其私有密钥(或者共享对称密钥)对客户的私有密钥解密并且安全地存储客户的解密的私有密钥。在与客户的用户建立TLS会话的过程期间,边缘服务器的不可信代码请求安全包围区的可信代码对预先主秘密进行解密,其已经利用客户的公共密钥被加密。在接收到加密的预先主秘密时,可信代码利用客户的私有密钥将预先主秘密解密并且将解密的预先主秘密提供给不可信代码。不可信代码可以然后使用解密的预先主秘密生成会话密钥。一旦客户的私有密钥安全地被存储在安全包围区中,则不可信代码可以通过依赖于安全包围区的可信代码将预先主秘密解密反复地与客户的用户建立TLS会话。以这种方式,在不要求与用于每个TLS会话的客户的密钥服务器的往返通信的情况下,可以建立TSL会话。此外,CDN的客户的私有密钥可以安全地由每个边缘服务器的安全包围区存储。

[0017] 图1是图示在一些实施例中采用安全密钥系统的方面的处理的示图。客户端110、边缘服务器120和密钥服务器130相互作用以安全地将密钥服务器的私有密钥存储在边缘服务器处并且与客户端建立TLS会话。边缘服务器包括不可信代码121和可信代码125。可信代码由安全包围区执行,并且不可信代码协调TLS会话的建立并且提供其他边缘服务器功能(诸如递送内容)。在步骤151-159中,可信代码与密钥服务器相互作用以获得密钥服务器的私有密钥。在步骤151中,可信代码可以生成公共/私有密钥对$K^{tc}_{priv}/K^{tc}_{pub}$。在步骤152中,可信代码(或者不可信代码)从证明可信代码和公共密钥K^{tc}_{pub}的安全包围区获得引用。在步骤153中,可信代码指导引用和公共密钥K^{tc}_{pub}被发送到密钥服务器。在步骤154中,密钥服务器验证引用以确保期望的可信代码在安全包围区中执行并且确保公共密钥K^{tc}_{pub}由在安全包围区中执行的可信代码提供(例如,生成或者获得)。在步骤155中,密钥服务器利用可信代码的公共密钥K^{ks}_{pub}对密钥服务器的私有密钥K^{ks}_{priv}加密。在步骤156中,密钥服务器将密钥服务器的加密的私有密钥K^{ks}_{priv}并且可选地密钥服务器的公共密钥K^{ks}_{pub}证书发送到可信代

码。在步骤158中，可信代码利用可信代码的私有密钥K_{priv}^{tc}对密钥服务器的加密的私有密钥K_{priv}^{ks}解密。在步骤159中，可信代码将密钥服务器的解密的私有密钥K_{priv}^{ks}存储在安全包围区中。在步骤160中，可信代码可以将密钥服务器的公共密钥K_{pub}^{ks}证书提供到不可信代码，以用于向客户的用户的客户端提供。

[0018] 稍后，在步骤161-171中，针对客户的用户建立TLS会话。在步骤161中，客户端向不可信代码发送包括客户端随机数的请求以与CDN的客户建立TLS会话。在步骤162中，不可信代码通过向客户端发送服务器随机数和密钥服务器的公共密钥K_{pub}^{ks}证书而做出响应。在步骤163中，在接收到密钥服务器的公共密钥K_{pub}^{ks}证书时，客户端验证证书用于密钥服务器的公共密钥K_{pub}^{ks}。在步骤164中，客户端生成预先主秘密。在步骤165中，客户端利用密钥服务器的公共密钥K_{pub}^{ks}对预先主秘密加密。在步骤166中，客户端向不可信代码发送加密的预先主秘密。在步骤167中，客户端使用客户端随机数、服务器随机数和预先主会话来生成会话密钥。在步骤168中，在接收到加密的预先主秘密时，不可信代码请求安全包围区的可信代码对预先主秘密进行解密。在步骤169中，可信代码使用密钥服务器的私有密钥K_{priv}^{ks}对预先主秘密解密。在步骤170中，可信代码向不可信代码提供解密的预先主秘密。在步骤171中，不可信代码使用客户端随机数、服务器随机数和预先主秘密来生成会话密钥。客户端和不可信代码然后使用其会话密钥的相应副本对TLS会话的通信加密。备选地，不可信代码可以将加密的预先主秘密连同服务器随机数和客户端随机数一起提供给可信代码。在这样的情况下，可信代码对预先主秘密进行解密并且生成和存储会话密钥。当不可信代码需要将TLS会话的通信加密或者解密时，不可信代码请求可信代码使用会话密钥对通信加密或者解密。

[0019] 在一些实施例中，当满足妥协准则时，安全密钥系统可以采用各种安全技术。当CDN已经以某种方式妥协时，可以满足妥协准则。例如，CDN的安全代理可以向密钥服务器报告何时确定边缘服务器已经妥协(例如，感染上病毒)。

[0020] 一种安全技术采用私有密钥更新过程确保如果边缘服务器的不可信代码妥协，则边缘服务器的可信代码使用私有密钥停止。具有密钥服务器的私有密钥的边缘服务器的可信代码可以(周期性地)向密钥服务器发送用于私有密钥的更新过程。如果针对边缘服务器妥协准则不满足(例如，如由安全代理所报告的)，则密钥服务器向边缘服务器的可信代码发送更新的通知。在接收到通知时，可信代码继续使用密钥服务器的私有密钥。如果针对边缘服务器妥协准则满足，则密钥服务器抑制更新的通知的发送。如果边缘服务器的可信代码不接收更新的通知，则可信代码使用私有密钥停止。

[0021] 另一种安全技术采用密码更新过程确保如果边缘服务器的不可信代码妥协，则边缘服务器的可信代码使用私有密钥停止。虽然被描述为“密码”更新过程，但是更新过程可以与其他类型的凭证(诸如数字签名、令牌、证书等)一起使用。安全包围区的可信代码可以被提供有当请求可信代码利用私有密钥解密或者加密时将由不可信代码提供的访问密码。当不可信代码提供匹配访问密码的密码时，可信代码使用私有密钥执行加密/解密。可信代码可以(周期性地)请求提供私有密钥的密钥服务器确认访问密码仍然有效。如果妥协准则未满足，则密钥服务器发送确认。在接收到确认时，可信代码继续使用访问密码。如果妥协

准则满足，则密钥服务器抑制确认的发送。如果确认未由边缘服务器的可信代码接收，则可信代码使用访问密码停止，使得将拒绝来自提供访问密码的不可信代码的后续加密/解密请求。

[0022] 在一些实施例中，CDN可以具有各自可以接受TLS权证以恢复会话的多个边缘服务器。在这样的情况下，密钥服务器的会话密钥可以被分布到边缘服务器中的每个边缘服务器，使得每个边缘服务器可以接受权证，而不管哪个边缘服务器生成权证。

[0023] 在一些实施例中，安全密钥系统可以被用于将第一设备的私有密钥分布到第二设备，以用于由第一设备的私有密钥的任何使用。例如，安全密钥系统主要地被描述为支持依赖于RSA加密来获得被用于生成会话密钥的预先主秘密的基于RSA的TLS握手。安全密钥系统还可以与依赖于Diffe-Hellman短暂(“DHE”)或者椭圆曲线Diffie-Hellman短暂(“ECDHE”)密钥交换的TLS握手一起使用。

[0024] 图2是图示在一些实施例中采用安全密钥系统的计算机系统的部件的块图。CDN的边缘服务器220经由通信信道250与客户的用户的客户端210通信。边缘服务器经由通信信道240与客户的密钥服务器230通信。客户端、边缘服务器和密钥服务器是计算设备。通信信道可以是因特网、蜂窝网络、广域网等。边缘服务器220包括不可信代码221和可信代码225。可信代码在边缘服务器的处理器的安全包围区229中执行。不可信代码包括建立会话部件222、控制会话部件223和密钥存储库224。依赖于可信代码利用密钥服务器的私有密钥对数据进行解密，建立会话部件协调与客户端的TLS会话的建立。控制会话部件在其已经建立之后控制TLS会话。密钥存储库224可以被用于存储用于TLS会话的会话密钥。可信代码包括获得密钥服务器私有密钥部件226、解密部件227和密钥存储库228。获得密钥服务器密钥部件协调将密钥服务器的私有密钥获得并且安全存储在密钥存储228中，其是安全包围区的一部分。解密部件负责对TLS会话的预先主秘密进行解密。密钥服务器包括供应密钥服务器私有密钥部件231和密钥存储库232。供应密钥服务器私有密钥部件协调将被存储在密钥存储库232中的密钥服务器的私有密钥提供到边缘服务器的可信代码。

[0025] 采用安全密钥系统的客户端的计算系统、边缘服务器和密钥服务器可以包括中央处理单元、输入设备、输出设备(例如，显示设备和扬声器)、存储设备(例如，存储器和磁盘驱动器)、网络接口、图形处理单元、加速度计、蜂窝无线电链路接口、全球定位系统，等等。计算系统可以包括数据中心的服务器、大规模并行系统等。计算系统可以访问包括计算机可读存储介质和数据传输介质的计算机可读介质。计算机可读存储介质是不包括暂态传播信号的有形存储装置。计算机可读存储介质的示例包括存储器(诸如主存储器、高速缓存存储器和辅助存储器(例如，DVD)和其他存储装置)。计算机可读存储介质上可以已经记录在其上或者可以编码有实现安全密钥系统的计算机可执行指令或者逻辑。数据传输介质被用于经由暂态传播信号传送信号或者经由有线或无线连接传送载波(例如，电磁)。

[0026] 可以在由一个或多个计算机、处理器或者其他设备执行的计算机可执行指令(诸如程序模块和部件)的一般上下文中描述安全密钥系统。通常，程序模块或者部件包括执行特定任务或者实现数据类型的例程、程序、对象、数据结构，等等。通常，程序模块的功能可以被组合或者被分布，如在各种实施例中所期望的。安全密钥系统的方面可以使用例如专用集成电路(ASIC)在硬件中被实现。

[0027] 图3是图示在一些实施例中安全密钥系统的供应密钥服务器私有密钥的处理的流

程图。供应密钥服务器私有密钥部件300协调将密钥服务器的私有密钥供应给边缘服务器。在块301中，部件从边缘服务器接收边缘服务器的安全包围区的引用和公开密钥。引用证明可信代码和公共密钥。在块302中，部件验证引用是用于期望的可信代码和接收到的公共密钥。假定验证了引用，在块303中，部件向可信代码发送利用可信代码的公共密钥加密的密钥服务器的私有密钥。在块304中，部件可以向可信代码发送密钥服务器的公共密钥，并且其然后完成。在一些实施例中，由安全密钥系统采用的公共密钥可以在各种其他源(诸如凭证授权)之前和/或从其获得。

[0028] 图4是图示在一些实施例中安全密钥系统的可信代码的获得密钥服务器私有密钥的处理的流程图。获得密钥服务器私有密钥部件400在安全包围区中执行并且协调从密钥服务器获得私有密钥。在块401中，部件生成或者以其他方式获得用于可信代码的公共/私有密钥对。在被生成并且仅被用于获得密钥服务器的一个私有密钥的意义上，公共/私有密钥对可以是短暂的。在块402中，部件从用于可信代码的安全包围区和用于可信代码的公共密钥获得引用。在块403中，部件向密钥服务器发送引用和可信代码的公共密钥证书。在块404中，部件可以接收密钥服务器的公共密钥证书。在块405中，部件从密钥服务器接收利用可信代码的公共密钥加密的密钥服务器的私有密钥。在块406中，部件验证密钥服务器的公共密钥证书。假定验证了证书，在块407中，部件使用可信代码的私有密钥对密钥服务器的私有密钥进行解密。在块408中，部件将密钥服务器的解密的私有密钥安全地存储在安全包围区内并且然后完成。

[0029] 图5是图示在一些实施例中安全密钥系统的不可信代码的建立会话部件的处理的流程图。建立会话部件500代表CDN的客户控制与客户端的TLS会话的建立。在块501中，部件从客户端接收建立包括客户端随机数的TLS会话的请求。在块502中，部件向客户端发送密钥服务器的公共密钥证书。在块503中，部件向客户端发送服务器随机数。在块504中，部件接收利用密钥服务器的公共密钥加密的预先主秘密。在块505中，部件请求可信代码对加密的预先主秘密进行解密。在块506中，部件从可信代码接收解密的预先主秘密。在块507中，部件使用客户端随机数、服务器随机数和预先主秘密来生成会话密钥。部件然后完成。不可信代码可以然后控制与会话密钥的TLS会话加密通信。

[0030] 以下段落描述了安全密钥系统的方面的各种实施例。安全密钥系统的实现可以采用各种实施例的任何组合。可以通过具有执行被存储在实现安全密钥系统的计算机可读存储介质上的计算机可执行指令的处理器的计算设备来执行下文所描述的处理。

[0031] 在一些实施例中，提供了一种由计算系统执行的方法，其用于将第一设备的第一密钥提供到第二设备，以用于代表第一密钥的所有者执行加密动作。方法访问第二设备的第二密钥。方法从第二设备接收由安全包围区所生成的引用。引用证明安全包围区的代码。方法验证引用以确保安全包围区的代码是可信代码。方法使用第二密钥来加密第一密钥。方法在验证了引用之后，向第二设备发送加密的第一密钥。在一些实施例中，第二密钥是第二设备的公共/私有密钥对的公共密钥。在一些实施例中，方法接收第二密钥的公共密钥证书。在一些实施例中，第二设备的公共/私有密钥对是短暂的。在一些实施例中，第一密钥是第一设备的公共/私有密钥对的私有密钥。在一些实施例中，方法向第二设备发送第一设备的公共密钥证书。在一些实施例中，第二密钥是由安全包围区的代码和第一设备共享的对称密钥。在一些实施例中，第二设备是内容递送网络的边缘服务器，并且第一设备是其内容

由内容递送网络递送的内容递送网络的客户的密钥服务器。在一些实施例中，第一密钥被提供给内容递送网络的多个边缘服务器，使得每个边缘服务器能够接受传输层安全权证以恢复会话，而不管哪个边缘服务器生成权证。在一些实施例中，方法在将加密的第一密钥发送到第二设备之后，从第二设备接收针对第一密钥的更新请求，并且当妥协准则未被满足时，向第二设备发送更新的通知，并且当妥协准则被满足时，抑制更新的通知的发送。在一些实施例中，第二设备使用第一密钥以代表第一密钥的所有者与客户端建立传输层安全会话。

[0032] 在一些实施例中，提供了一种计算系统，其用于获得第一设备的第一密钥，以用于由第二设备代表第一密钥的所有者执行加密动作。方法在第二设备的安全包围区的控制下执行。方法生成证明安全包围区的代码的引用。方法指导引用被发送到第一设备。方法从第一设备接收第一设备的第一密钥，其利用第二设备的第二密钥加密。方法基于利用第二密钥的加密，对第一密钥进行解密。方法将解密的第一密钥存储在安全包围区内，使得解密的第一密钥在安全包围区的外部是不可访问的。在一些实施例中，方法还在第二设备的安全包围区的控制下，从第二设备的不可信代码接收对数据执行加密动作的请求，使用第一密钥对数据执行加密动作以生成结果数据，并且向不可信代码提供结果数据。在一些实施例中，加密动作是或者解密或者加密数据。在一些实施例中，加密动作是或者创建或者验证数字签名。在一些实施例中，第二密钥是第二设备的公共/私有密钥对的公共密钥。在一些实施例中，方法还向第一设备发送用于第二密钥的公共密钥证书。在一些实施例中，第一密钥是第一设备的公共/私有密钥对的私有密钥。在一些实施例中，方法还接收第一设备的公共密钥证书。在一些实施例中，第二密钥是由安全包围区的代码和第一设备共享的对称密钥。在一些实施例中，第二设备是内容递送网络的边缘服务器，并且第一设备是其内容由内容递送网络递送的内容递送网络的客户的密钥服务器。在一些实施例中，方法在接收到第一密钥之后，向第一设备发送用于第一密钥的更新请求，并且当更新的通知被接收时，继续使用第一密钥，并且当更新的通知未被接收时，抑制第一密钥的使用。在一些实施例中，安全包围区的代码被提供有访问凭证，并且方法接收使用包括提供的凭证的第一密钥加密的加密请求，并且当提供的凭证匹配访问凭证时，使用第一密钥执行加密。在一些实施例中，方法在安全包围区的控制下，请求来自第一设备的访问凭证仍然有效的确认，并且当确认未被接收时，抑制访问凭证的使用，使得将拒绝提供访问凭证的后续加密请求。

[0033] 在一些实施例中，提供了一种由计算系统执行的方法，其用于由第二设备代表公共/私有密钥对的私有密钥的所有者建立与客户端的传输层安全会话。方法从客户端接收建立会话的请求，请求包括客户端随机数。方法向客户端发送公共/私有密钥对的公共密钥证书和服务器随机数。方法从客户端接收使用公共密钥加密的加密秘密。方法请求计算系统的安全包围区使用第一设备的私有密钥对加密秘密进行解密。安全包围区可能已经基于被提供到第一设备的引用从第一设备获得私有密钥，引用证明安全包围区的代码是可信代码。在一些实施例中，方法从安全包围区接收解密的秘密，并且基于客户端随机数、服务器随机数和密码，生成用于会话的会话密钥。在一些实施例中，安全包围区的请求还包括请求安全包围区基于客户端随机数、服务器随机数和秘密生成会话密钥，并且存储会话密钥。在一些实施例中，方法请求安全包围区使用会话密钥对会话的数据进行加密。

[0034] 在一些实施例中，提供了一种密钥服务器，其用于将密钥服务器的私有密钥提供

到边缘服务器，以用于在与客户端建立会话时代表私有密钥的所有者执行加密动作。密钥服务器包括：计算机可读存储介质，其存储计算机可执行指令；以及处理器，其执行被存储在计算机可读存储介质中的计算机可执行指令。指令控制密钥服务器以访问边缘服务器的安全包围区的密钥。指令控制密钥服务器从边缘服务器接收由边缘服务器的安全包围区所生成的引用，引用证明安全包围区的代码。指令控制密钥服务器验证引用以确保安全包围区的代码是可信代码。指令控制密钥服务器使用边缘服务器的安全包围区的密钥对私有密钥进行加密。指令控制密钥服务器在引用被验证之后，向边缘服务器发送加密的私有密钥。在一些实施例中，边缘服务器的密钥是边缘服务器的公共/私有密钥对的公共密钥。在一些实施例中，指令控制密钥服务器接收用于边缘服务器的公共密钥的公共密钥证书。在一些实施例中，指令控制密钥服务器发送用于对应于密钥服务器的私有密钥的公共密钥的公共密钥证书。在一些实施例中，边缘服务器的密钥是由安全包围区的代码和密钥服务器共享的对称密钥。在一些实施例中，边缘服务器是内容递送网络的边缘服务器，并且密钥服务器是其内容由内容递送网络递送的内容递送网络的客户的密钥服务器。在一些实施例中，会话密钥被提供给内容递送网络的多个边缘服务器，使得每个边缘服务器能够接受传输层安全权证以恢复会话，而不管哪个边缘服务器生成权证。在一些实施例中，指令控制密钥服务器在将加密的私有密钥发送到边缘服务器之后：从边缘服务器接收对于私有密钥的更新请求，并且当妥协准则未被满足时，向边缘服务器发送更新的通知，并且当妥协准则被满足时，抑制更新的通知的发送。在一些实施例中，边缘服务器使用私有密钥代表私有密钥的所有者与客户端建立传输层安全会话。

[0035] 在一些实施例中，提供了一种边缘服务器，其用于获得密钥服务器的私有密钥，以用于在与客户端建立会话时代表私有密钥的所有者执行加密动作。边缘服务器包括：计算机可读存储介质，其存储计算机可执行指令；以及处理器，其执行被存储在计算机可读存储介质中的计算机可执行指令。指令控制边缘服务器生成证明安全包围区的代码的引用。指令控制边缘服务器指导引用被发送到密钥服务器。指令控制边缘服务器从密钥服务器接收密钥服务器的私有密钥，其利用边缘服务器的安全包围区的密钥被加密。指令控制边缘服务器基于利用边缘服务器的安全包围区的密钥对私有密钥进行解密。指令控制边缘服务器将解密的私有密钥存储在安全包围区内，使得解密的私有密钥在安全包围区的外部是不可访问的。在一些实施例中，指令控制边缘服务器在边缘服务器的安全包围区的控制下，从边缘服务器的不可信代码接收对加密数据解密的请求，使用私有密钥对加密数据进行解密，并且向不可信代码提供解密数据。在一些实施例中，指令控制边缘服务器在边缘服务器的安全包围区的控制下，从边缘服务器的不可信代码接收对数据加密的请求，使用私有密钥对数据进行加密，并且向不可信代码提供加密数据。在一些实施例中，指令控制边缘服务器在边缘服务器的安全包围区的控制下，从边缘服务器的不可信代码接收生成数字签名的请求，使用私有密钥对数据进行解密，并且向不可信代码提供解密数据。在一些实施例中，指令控制边缘服务器在边缘服务器的安全包围区的控制下，从边缘服务器的不可信代码接收验证数字签名的请求，使用私有密钥对数据进行加密，并且向不可信代码提供加密数据。在一些实施例中，边缘服务器的安全包围区的密钥是边缘服务器的安全包围区的公共/私有密钥对的公共密钥。在一些实施例中，指令控制边缘服务器在边缘服务器的安全包围区的控制下，向密钥服务器发送边缘服务器的安全包围区的公共密钥。在一些实施例中，私有密

钥是密钥服务器的安全包围区的公共/私有密钥对的私有密钥。在一些实施例中，指令控制边缘服务器在边缘服务器的安全包围区的控制下，接收密钥服务器的公共密钥的公共密钥证书。在一些实施例中，边缘服务器的密钥是由安全包围区的代码和密钥服务器共享的对称密钥。在一些实施例中，边缘服务器是内容递送网络的边缘服务器，并且密钥服务器是其内容由内容递送网络递送的内容递送网络的客户的密钥服务器。在一些实施例中，指令控制边缘服务器在边缘服务器的安全包围区的控制下：向密钥服务器发送用于私有密钥的更新请求，并且当更新的通知被接收时，继续使用私有密钥，并且当更新的通知未被接收时，抑制私有密钥的使用。在一些实施例中，其中安全包围区的代码被提供有访问凭证，并且其中计算机可执行指令还使得边缘服务器在边缘服务器的安全包围区的控制下，接收包括使用私有密钥执行加密动作的提供凭证的加密请求，并且当提供凭证匹配访问凭证时，使用私有密钥执行加密动作。在一些实施例中，指令控制边缘服务器在边缘服务器的安全包围区的控制下，请求来自密钥服务器的访问凭证仍然有效的确认，并且当确认未被接收时，抑制访问凭证的使用，使得将拒绝提供访问凭证的后续加密请求。

[0036] 在一些实施例中，提供了一种边缘服务器，其用于代表公共/私有密钥对的私有密钥的所有者建立与客户端的传输层安全会话。边缘服务器包括：计算机可读存储介质，其存储计算机可执行指令；以及处理器，其执行被存储在计算机可读存储介质中的计算机可执行指令。指令控制边缘服务器从客户端接收建立会话的请求。请求可以包括客户端随机数。指令控制边缘服务器向客户端发送用于公共/私有密钥对的公共密钥证书和服务器随机数。指令控制边缘服务器从客户端接收使用公共密钥加密的加密预先主秘密。指令控制边缘服务器请求边缘服务器的安全包围区的可信代码，以使用私有密钥对加密的预先主秘密进行解密。安全包围区可能已经基于由安全包围区所生成并且被提供到密钥服务器的引用从密钥服务器获得私有密钥，引用证明安全包围区的代码是可信代码。在一些实施例中，指令控制边缘服务器：从安全包围区接收解密的预先主秘密，并且基于客户端随机数、服务器随机数和预先主秘密，生成用于会话的会话密钥。在一些实施例中，指令控制边缘服务器请求安全包围区的可信代码，以基于客户端随机数、服务器随机数和预先主秘密生成会话密钥，并且存储会话密钥。在一些实施例中，指令控制边缘服务器请求安全包围区使用会话密钥对会话的数据进行解密。

[0037] 虽然已经以特定于结构特征和/或动作的语言描述了主题，但是将理解到，所附的权利要求中定义的主题不必限于上文所描述的特征或者动作。相反，上文所描述的特定特征和动作被公开为实现权利要求的示例形式。因此，除了如由所附的权利要求的限制之外，本技术不是有限的。

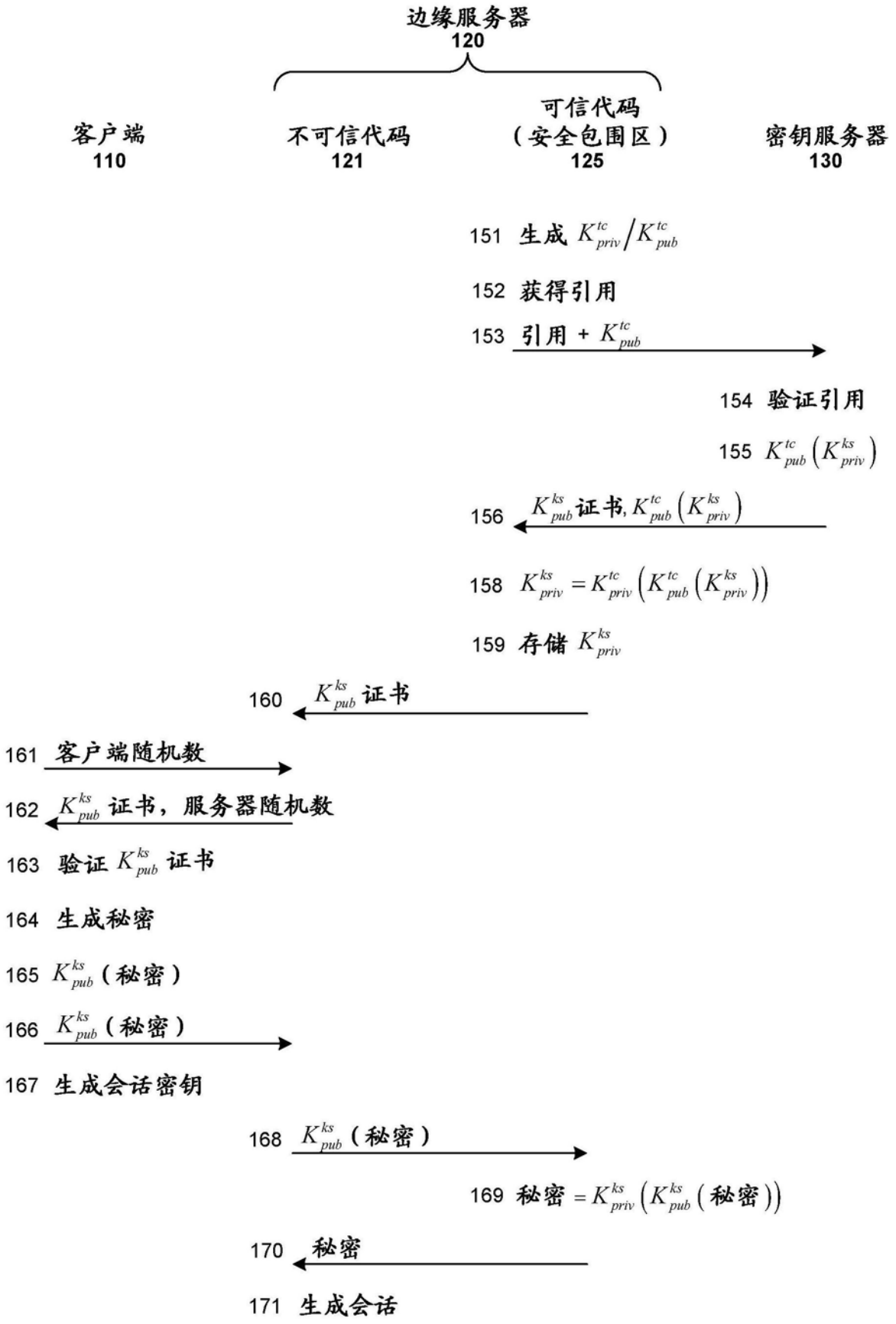

边缘服务器
120
客户端
110
不可信代码
121
可信代码
（安全包围区）
125
密钥服务器
130
151 生成 $K^{tc}_{priv}/K^{tc}_{pub}$
152 获得引用
153 引用 + K^{tc}_{pub}
154 验证引用
155 $K^{tc}_{pub}\left(K^{ks}_{priv}\right)$
156 K^{ks}_{pub} 证书, $K^{tc}_{pub}\left(K^{ks}_{priv}\right)$
158 $K^{ks}_{priv}=K^{tc}_{priv}\left(K^{tc}_{pub}\left(K^{ks}_{priv}\right)\right)$
159 存储 K^{ks}_{priv}
160 K^{ks}_{pub} 证书
161 客户端随机数
162 K^{ks}_{pub} 证书，服务器随机数
163 验证 K^{ks}_{pub} 证书
164 生成秘密
165 K^{ks}_{pub}（秘密）
166 K^{ks}_{pub}（秘密）
167 生成会话密钥
168 K^{ks}_{pub}（秘密）
169 秘密 $=K^{ks}_{priv}\left(K^{ks}_{pub}\left(\text{秘密}\right)\right)$
170 秘密
171 生成会话

图1

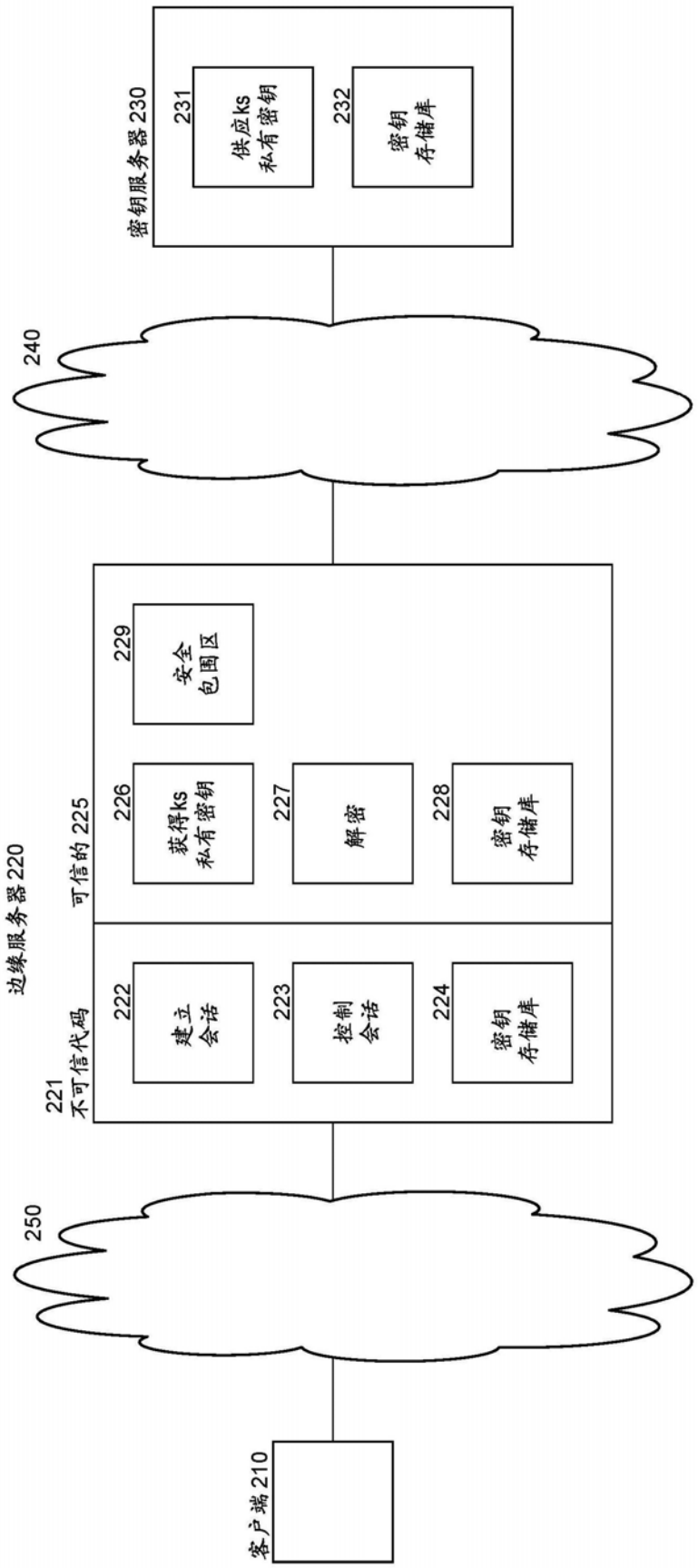

密钥服务器 230
231
供应ks
私有密钥
232
密钥
存储库
240
边缘服务器 220
可信的 225
229
安全
包围区
226
获得ks
私有密钥
227
解密
228
密钥
存储库
不可信代码
221
222
建立
会话
223
控制
会话
224
密钥
存储库
250
客户端 210

图2

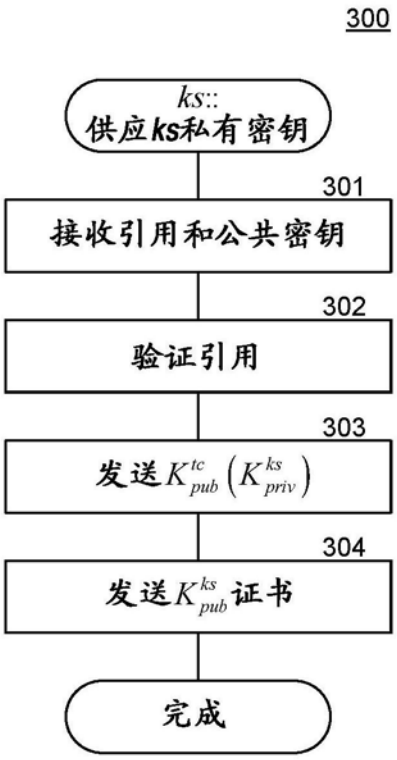

300
ks::
供应ks私有密钥
301
接收引用和公共密钥
302
验证引用
303
发送 $K^{tc}_{pub}\left(K^{ks}_{priv}\right)$
304
发送 K^{ks}_{pub} 证书
完成

图3

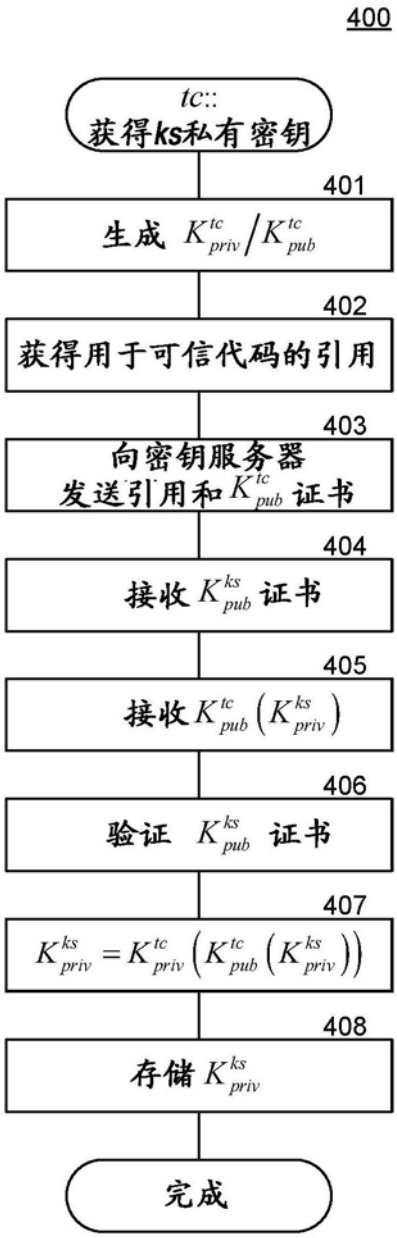

400
tc::
获得ks私有密钥
401
生成 $K^{tc}_{priv}/K^{tc}_{pub}$
402
获得用于可信代码的引用
403
向密钥服务器
发送引用和 K^{tc}_{pub} 证书
404
接收 K^{ks}_{pub} 证书
405
接收 $K^{tc}_{pub}\left(K^{ks}_{priv}\right)$
406
验证 K^{ks}_{pub} 证书
407
$K^{ks}_{priv}=K^{tc}_{priv}\left(K^{tc}_{pub}\left(K^{ks}_{priv}\right)\right)$
408
存储 K^{ks}_{priv}
完成

图4

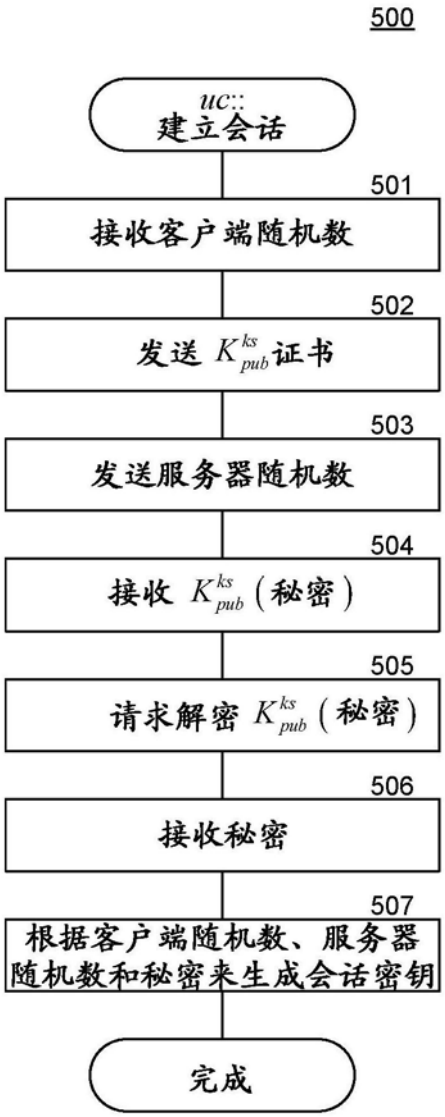

500
uc::
建立会话
501
接收客户端随机数
502
发送 K_{pub}^{ks} 证书
503
发送服务器随机数
504
接收 K_{pub}^{ks} (秘密)
505
请求解密 K_{pub}^{ks} (秘密)
506
接收秘密
507
根据客户端随机数、服务器随机数和秘密来生成会话密钥
完成

图5