(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 105580311 B
(45)授权公告日 2019.07.05

(21)申请号 201480052720.0

(22)申请日 2014.09.23

(65)同一申请的已公布的文献号
申请公布号 CN 105580311 A

(43)申请公布日 2016.05.11

(30)优先权数据
14/037,292 2013.09.25 US

(85)PCT国际申请进入国家阶段日
2016.03.24

(86)PCT国际申请的申请数据
PCT/US2014/057051 2014.09.23

(87)PCT国际申请的公布数据
WO2015/048042 EN 2015.04.02

(73)专利权人 亚马逊技术有限公司
地址 美国华盛顿

(72)发明人 格里戈里·布兰奇克·罗特
埃里克·贾森·布朗德万

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 唐文静

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

(56)对比文件
CN 101938461 A,2011.01.05,
CN 101938461 A,2011.01.05,
US 6084969 B2,2000.07.04,
CN 1470972 A,2004.01.28,
US 2013013921 A1,2013.01.10,
CN 102687482 A,2012.09.19,

审查员 田雨润

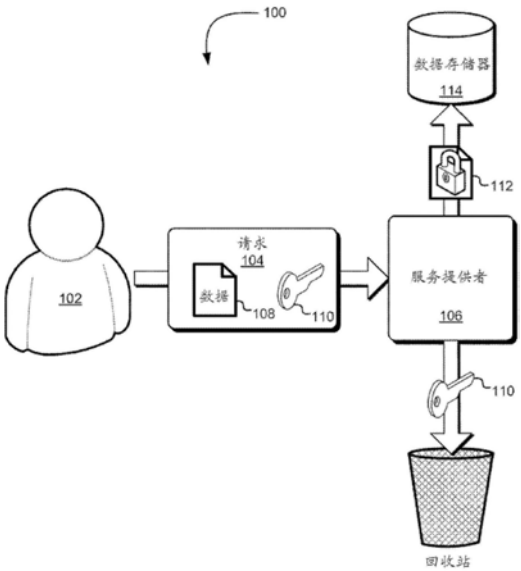
权利要求书2页 说明书18页 附图14页

(54)发明名称

使用请求供应的密钥保护数据安全性的方法和装置

(57)摘要

请求被提交给请求处理实体，其中所述请求包括将用于履行所述请求的密码密钥。所述请求处理实体，在接收到所述请求后，从所述请求提取所述密钥并且使用所述密钥来执行一个或多个密码操作以便履行所述请求。所述一个或多个密码操作可包括通过所述请求处理实体的子系统加密将以加密形式存储的数据/解密已经以加密形式存储的数据。在履行所述请求后，所述请求处理实体可执行一个或多个操作以失去对所述请求中的所述密钥的访问，从而失去使用所述密钥的能力。



CN 105580311 B

1.一种计算机实现的用于保护数据安全性的方法,其包括:

在服务提供者的一个或多个计算机系统的控制下,所述一个或多个计算机系统被配置有可执行指令,

从对应于所述服务提供者的客户的请求者接收请求,所述请求的履行涉及关于所述请求中指定的数据的一个或多个密码操作的执行以及在所述请求中供应的密码密钥的使用,所述服务提供者在一定时间内缺少对所述密码密钥的访问直到接收到所述请求,其中所述请求中的所述密码密钥是用一公钥-私钥对中的公钥加密的对称密钥;

通过作为执行关于所述指定的数据的所述一个或多个密码操作的一部分的使用所述供应的密码密钥来履行所述请求,其中执行关于所述指定的数据的所述一个或多个密码操作包括:使用所述公钥-私钥对中的私钥来解密出所述对称密码密钥;以及,使用解密出的对称密码密钥来执行所述一个或多个密码操作;并且

向数据存储系统提供执行所述一个或多个密码操作的结果;并且

在执行所述一个或多个密码操作的某一时刻后,执行致使所述服务提供者失去对所述密码密钥的访问的一个或多个操作。

2.如权利要求1所述的计算机实现的方法,其中所述解密包括向另一个实体传送所述密码密钥以供解密。

3.一种用于保护数据安全性的装置,其包括:

一个或多个处理器;以及

包括指令的存储器,当由所述一个或多个处理器执行时,所述指令致使所述装置:

通过网络从请求者接收请求,所述请求的履行涉及使用包括在所述请求中供应的密码密钥的信息来执行关于所述请求中指定的数据的一个或多个密码操作,其中所述信息可用来认证所述请求,其中所述请求中的所述密码密钥是用一公钥-私钥对中的公钥加密的对称密钥;

作为接收并认证所述请求的结果,执行关于所述指定的数据的所述一个或多个密码操作,其中执行关于所述指定的数据的所述一个或多个密码操作包括:使用所述公钥-私钥对中的私钥来解密出所述对称密码密钥;以及,使用解密出的对称密码密钥来执行所述一个或多个密码操作;并且

提供执行所述一个或多个密码操作的结果。

4.如权利要求3所述的装置,其中:

所述请求是从数据存储系统读取已加密数据的请求;并且

所述信息可用来使用在所述请求中供应的所述密码密钥来认证所述请求。

5.如权利要求3所述的装置,其中所述信息可用来通过包括至少部分基于不同于在所述请求中供应的所述密码密钥的第二密码密钥生成的电子签名来认证所述请求。

6.如权利要求3所述的装置,其中:

所述一个或多个密码操作包括加密所述指定的数据;并且

提供执行所述一个或多个密码操作的所述结果包括将所述指定的数据以加密形式传送到数据存储系统以用于持久存储。

7.如权利要求3所述的装置,其中所述指令进一步致使所述装置执行一个或多个操作,以便在执行所述一个或多个密码操作之后的某一时刻失去对在所述请求中供应的所述密

码密钥的访问。

8.如权利要求3所述的装置,其中所述装置在一定时间内缺少对所述密码密钥的访问,直到接收到所述请求。

9.如权利要求3所述的装置,其中:

在所述请求中供应的所述密码密钥被供应在呈加密形式的所述请求中;并且

所述装置还包括子装置,所述子装置被配置来安全地存储从所述子装置的外部难以接近的多个密码密钥,所述多个密码密钥包括可用来解密以加密形式供应的所述密码密钥的特定密码密钥;

所述指令进一步致使所述装置致使所述子装置解密以加密形式供应的将用于执行所述一个或多个密码操作的所述密码密钥。

10.如权利要求3所述的装置,其中所述信息可用来通过使用所述密码密钥认证所述请求来认证所述请求。

使用请求供应的密钥保护数据安全性的方法和装置

[0001] 相关申请的交叉引用

[0002] 本申请以引用方式出于所有目的并入2013年9月25日提交的标题为“具有密钥的资源定位符”(RESOURCE LOCATORS WITH KEYS)的美国专利申请号14,037,282和2013年9月25日提交的标题为“使用请求供应的密钥的数据安全性”(DATA SECURITY USING REQUEST-SUPPLIED KEYS)的美国专利申请号14/037,292的全部公开内容。

技术背景

[0003] 在许多语境中,计算资源和相关数据的安全性非常重要。作为实例,组织通常利用计算装置的网络来向它们的用户提供一组稳健的服务。网络通常跨多个地理边界并通常与其他网络连接。例如,组织可支持其使用计算资源的内部网络和由其他人管理的计算资源两者进行的操作。例如,组织的计算机可在使用另一个组织的服务的同时与其他组织的计算机通信以访问和/或提供数据。在许多情况下,组织使用由其他组织管理的硬件来配置并操作远程网络,从而降低基础设施成本并实现其他优点。在具有此类计算资源配置的情况下,确保对它们所持有的资源和数据的访问安全可能具有挑战性,尤其是随着此类配置的大小和复杂性的增长。

[0004] 附图简述

[0005] 将参照附图描述根据本公开的各个实施方案,在附图中:

[0006] 图1示出可实现各个实施方案的环境的说明性实例;

[0007] 图2示出可实现各个实施方案的环境的说明性实例;

[0008] 图3示出根据至少一个实施方案的请求的代表的说明性实例;

[0009] 图4示出根据至少一个实施方案的用于提交请求的过程的说明性实例;

[0010] 图5示出根据至少一个实施方案的用于处理请求的过程的说明性实例;

[0011] 图6示出根据至少一个实施方案的请求的代表的说明性实例;

[0012] 图7示出根据至少一个实施方案的用于处理PUT请求的过程的说明性实例;

[0013] 图8示出根据至少一个实施方案的用于提交GET请求的过程的说明性实例;

[0014] 图9示出根据各个实施方案的请求的代表的说明性实例;

[0015] 图10示出根据至少一个实施方案的用于提交请求的过程的说明性实例;

[0016] 图11示出可实现各个实施方案的环境的说明性实例;

[0017] 图12示出根据至少一个实施方案的用于处理请求的过程的说明性实例;

[0018] 图13示出可实现各个实施方案的环境的说明性实例;

[0019] 图14示出根据至少一个实施方案的用于处理请求的过程的说明性实例;以及

[0020] 图15示出可实现各个实施方案的环境。

[0021] 详述

[0022] 在以下描述中,将描述各个实施方案。出于解释的目的,将阐述具体的配置和细节,以便提供实施方案的透彻理解。然而,对本领域的技术人员将是显而易见的是,没有具体细节的情况下也可以实行实施方案。此外,为了不使所描述的实施方案变得模糊,可能会

省略或简化众所周知的特征。

[0023] 本文描述和建议的技术涉及请求的提交和处理，其中所述请求包括密码密钥。所述请求可由服务提供者(如计算资源服务提供者)的客户生成并且由其提交。处理所述请求可包括使用被包括在请求中的密钥来执行一个活多个密码操作，如关于数据的电子(数字)签名的加密、解密和生成。在一些实施方案中，本文描述和建议的技术用来允许服务器端加密(和/或相关技术如解密)，其中有待用于加密/解密的密钥是由客户端(即，客户装置或代表客户操作)控制的。

[0024] 在各个实施方案中，请求中所提供的密钥的使用被执行以便服务提供者在使用密钥的有限时间之外缺少对密钥的访问。例如，服务提供者可操作数据存储服务。客户可将数据传送到服务提供者以便通过数据存储服务来存储。对服务提供者的请求可包括有待使用来加密数据的密钥。服务提供者可从所述请求获得密钥并且使用所述密钥来加密数据，以便可使用数据存储服务来持久地存储已加密数据。当不再需要密钥时(例如，当数据的加密已经完成时)，服务提供者可执行一个或多个操作以失去对密钥的访问，如通过销毁存储器中的任何密钥副本或允许将其销毁。数据的呈明文形式的任何副本可以类似方式被销毁或允许将其销毁。一旦已经销毁了密钥和明文数据，客户就可确保提供者不能够加密数据。因此，即使提供者处的安全漏洞或其他事件致使对未经客户授权的数据的访问，所述漏洞本身不允许对呈明文形式的数据的访问。

[0025] 根据不同实施方案可以各种方式在请求中提供密钥。例如，在一些实施方案中，所述请求包括呈明文形式的密钥。所述明文密钥可以是有待在对称密钥算法中使用的对称密钥。所述明文密钥还可以是用于不对称密钥算法的公钥-私钥对的公钥，其中服务提供者缺少对密钥对的私钥的访问并且所述私钥可访问能够使用私钥来解密的实体(例如，客户)。在一些实施方案中，请求包括呈加密(包裹)形式的密钥。例如，可对所述密钥进行加密以便可由服务提供者或在服务提供者的指导下的另一个实体解密。用来加密请求中的密钥的密钥可以是与能够解密所述密钥的实体(例如，服务提供者)共享的秘密或公钥-私钥对的公钥，其中所述私钥将由实体使用来解密已加密密钥，以用于处理所述请求。[注意:需要更新段落间距]。

[0026] 在接收到具有密钥的请求后，服务提供者可访问来自所述请求的密钥，从而(如果适用)解密所述密钥或使所述密钥解密，并且随后处理请求。可执行其他操作，如通过验证请求的电子签名或检查请求的履行是否遵循任何适用的策略。下文更详细地论述可能执行的操作的其他细节。

[0027] 图1示出可实现各个实施方案的环境100的说明性实例。在环境100中，客户102将请求104传送到服务提供者106。客户102例如可利用服务提供者106的服务。所述服务提供者可提供与数据相关的任何类型的服务，所述服务可由客户利用。示例性服务包括数据存储服务、数据库服务、处理数据的服务和其他服务。为了向服务提供者106提交请求104，客户102可在一个或多个用户装置的帮助下传送所述请求，所述一个或多个客户装置如个人计算机或膝上型计算机、移动装置、平板计算装置、电子书阅读器和/或如下文结合图15更详细描述的其他装置。另外，可根据客户102的一个或多个自动化过程提交请求104。例如，作为客户102的装置的人类操作员与客户102的装置的浏览器或其他应用的互动的结果可传送请求104。请求104可以是通过网络，如互联网或任何其他网络或下文论述的网络组合

传送的电子请求。在一些实施方案中，例如，请求104是由服务提供者106向网络服务接口提供的网络服务请求。一般来说，可根据各种协议来配置请求104，请求可通过所述协议来以电子方式提交。

[0028] 如图1所示，请求104包括数据108和密码密钥110。所述数据可包括各种类型的信息并且可根据各个实施方案的各种方式格式化。例如，在一些实施方案中，所述数据被组织为文件，如媒体文件。还可以其他方式格式化数据。所述数据可被例如组织以便包括在数据库或其他装置中。如下文更详细论述的密码密钥110可以是用来加密数据108或以其他方式执行关于数据的一个或多个密码操作的密钥。应当注意，如下文将更详细地论述，请求104还可以各种方式包括密码密钥110。例如，在一些实施方案中，请求104包括呈明文形式的密码密钥110。在其他实施方案中，请求104包括呈已加密形式的密码密钥。例如，如下文更详细地论述，可通过另一个密钥对密码密钥110进行加密，以使得与其相关的服务提供者106或另一个系统能够解密已加密的密码密钥110。以此方式，在将来自客户102的请求104提交给服务提供者106后，服务提供者106可使用密码密钥110来加密请求104中所接收到的数据108，从而生成已加密数据112。

[0029] 随后可将已加密数据112存储在数据存储系统114中。数据存储系统114(虽然被示出为与服务提供者106分开)可以是服务提供者106的子系统。例如，可向服务提供者106的网络服务器提交请求104，其中所述网络服务器被配置来允许访问数据存储系统114。一般来说，数据存储系统114可作为对客户的服务进行操作，以使得客户可使用服务提供者106的资源来达成存储数据的目的。其他实施方案也包括那些，其中数据存储系统114与服务提供者106分开。数据存储系统114可例如由是服务提供者106和客户102的第三方的实体操作，或在一些实施方案中，数据存储系统114可以是客户102的子系统；也就是说，是客户102的系统的子系统。应当注意，如“客户”和“服务”提供者的术语可具有多个意义并且此类意义在上下文中是清晰的。例如，术语“客户”可以是指支持客户实体的操作的实体(例如，法人实体如组织或个人)或系统(例如，计算装置或计算装置网络)。类似地，术语“服务提供者”可以是指支持服务提供者实体的操作的法人实体或系统。

[0030] 如图1所示，在加密数据108以生成已加密数据112后，服务提供者106可采取致使服务提供者106失去对密码密钥110的访问的一个或多个动作。这在图1中示出为服务提供者106将密码密钥110传递给标记为回收站的图标。应当注意，虽然如图式中所示的为达说明的目的，将密码密钥110传递到回收站中，但是各个实施方案可采取动作以失去对密码密钥110的访问，以致于没有必要涉及密码密钥110的传输。例如，在一些实施方案中，在接收到请求104并且使用密码密钥110后，服务提供者106可执行一个或多个操作以销毁密码密钥110。可根据各个实施方案以各种方式执行密码密钥110的销毁。例如，在一些实施方案中，密码密钥110和请求104未由服务提供者106持久地存储，但被维持在服务提供者106的装置的易失性存储器中。

[0031] 密码密钥110的销毁可通过允许利用其他数据(如接收作为后一请求的一部分的数据)重写存储密码密钥110的一个或多个存储器位置来执行。还可执行其他操作。例如，如果将密码密钥110存储在易失性或非易失性存储器中，那么密码密钥110可通过利用其他数据(如随机数据或非随机数据如零字符串)重写(例如，通过意图销毁密码密钥的一个或多个写操作)用来存储密码密钥110的一个或多个存储器位置来销毁。一般来说，可使用将致

使服务提供者106失去对密码密钥110的访问的任何操作。以此方式，客户102能够向服务提供者106提交具有密码密钥的请求，客户102期望使用所述密码密钥来加密数据108。此外，因为服务提供者106在各个实施方案中被配置来在密码密钥110的使用之后失去对密码密钥110的访问，所以客户102可确保服务提供者在处理请求104后不能够通过解密已加密数据112来访问数据108。换句话说，数据112的安全性最终由客户102控制，其中服务提供者106在有限时间内可访问数据。

[0032] 应当注意，虽然为了说明的目的通篇使用产生已加密数据(和对应的解密数据)的各个过程，但是各个过程可根据其他实施方案变化。例如，用于本文所示的加密的示例性过程展示使用由服务提供者的客户所供应的密钥的加密，并且其中执行加密以使得在一定时间之后，服务提供者失去对已经使用过的密钥的访问。然而，还可使用更多复杂方案，其中使用多于一个密钥来控制对数据的访问。例如，参考图1，在一些实施方案中，可使用由客户以请求供应的密钥以及由服务提供者持有或服务提供者可以其他方式访问的密钥两者来加密数据。以此方式，通过具有解密已加密数据的能力来访问数据108需要客户102与服务提供者106之间的协同动作。在一些实施方案中，例如，可利用一个密钥对数据108进行加密，并且随后利用另一个密钥对所述数据108再次加密。在其他实例中，密码密钥110可与另一个密钥结合以便生成用来加密数据108的又一个密钥。此类变体还可扩展至除客户102和服务提供者106之外的多方，以便需要多个实体的大体协同动作来合法访问已经加密的数据(也就是说访问呈明文形式的数据)。其他变体也被视为是在本公开的范围内。

[0033] 另外，虽然本文所述的各个实施方案示出具有某些类型的数据的请求，但是请求可包括其他类型的数据。例如，请求可包括所述请求的各个参数的数据，所述数据可由服务提供者使用来确定是否和/或如何履行请求。一般来说，如本文所论述的请求被简化以用于说明的目的。例如，请求可包括各种上下文数据，如请求者的身份、发起请求的网络地址、生成所述请求中的一些或全部的实体的身份和/或其他类型的数据。

[0034] 此外，还应当注意，虽然图1示出具有待加密的数据108的请求104，但是在本公开的范围内的请求没有必要具有待加密的数据。例如，在一些实施方案中，请求可具有对数据的引用(例如，数据对象的标识符，所述标识符可以是URL的形式)，所述引用没有必要包括在请求中。处理这种请求可包括使用所述引用来获得数据。作为另一个实例，一些请求可能缺少数据，因为所述请求包括作为一个或多个请求操作的数据检索。检索数据的请求可包括密码密钥，但所述数据可被存储在另一个位置中。处理所述请求可包括访问已加密数据以便使用在所述请求中提供的密码密钥来解密。其他变体也被视为是在本公开的范围内。

[0035] 图2示出根据各个实施方案的服务提供者200的环境的说明性实例。如图2中所示，服务提供者200包括客户接口202。所述客户接口可以是服务提供者200的子系统，所述子系统允许由服务提供者200处理来自客户的请求的提交，如上文结合图1所述。客户接口因此可包括用于为客户提供向服务提供者200提交请求的能力的适当的计算装置。这个客户接口例如可包括被配置来通过互联网或另一种网络接收请求的一个或多个网络服务器。虽然未如此示出，但是其他基础设施也可包括在客户接口202中，如允许客户接口202针对服务提供者200的客户恰当地运行的适当的联网设备。

[0036] 当通过客户接口202接收请求时，所述请求可与适当的认证信息一起被接收。例如，如图2所示，请求204可与所述请求的签名206一起被接收。所述签名可根据各个实施方

案来生成。例如，提交请求204的客户可使用在所述客户与服务提供者200之间共享的秘密信息来生成签名206。作为另一个实例，客户可能已经使用不对称的数字签名方案，以便使用私钥/公钥对的私钥来签署请求204。一般来说，可使用用来认证请求204的任何类型的信息，并且在一些实施方案中，可提交请求而无需这种信息。此外，在一些实施方案中，使用不同于在请求中供应的密码密钥的密码密钥来生成请求的电子签名，尽管在一些实施方案中，使用与在请求中供应的密钥的相同密钥来生成电子签名。

[0037] 然而，如图2所示，当通过客户接口202接收请求204时，(例如，通过服务提供者200的内部网络)将具有签名206的所述请求204提供到服务提供者200的认证系统208。或者，可提供所述请求的足以生成电子签名206的一部分来代替整个请求。认证系统208可以是服务提供者200的子系统，所述子系统被配置来如通过验证由请求提供的电子签名来认证请求。在验证请求204的签名206后，认证系统208可向客户接口202提供签名206是否有效的响应。客户接口202的装置可使用由认证系统208提供的信息，以便确定如何处理请求204。例如，如果认证系统208指示签名206是无效的，则客户接口202可拒绝所述请求。类似地，如果来自认证系统208的信息指示请求204的签名206是有效的，客户接口202可处理请求204。

[0038] 虽然未在图式中示出，但是认证系统208或在服务提供者200内或代表其运行的另一个系统可运行来执行与确定如何处理请求有关的其他操作。例如，认证系统208或与其协同运行的另一个系统可用来检查决定请求是否可被履行的一个或多个策略。可至少部分基于各个因素来进行策略确定，所述因素如提交请求的请求者的身份、一天的某个时间、存储数据或将要存储数据的位置的逻辑标识符以及其他上下文信息。可通过客户接口202或通过适当配置的应用编程接口(API)调用的另一个接口来管理策略。

[0039] 返回图2所示的实施方案，如果认证系统208确定签名206是有效的，则客户接口202可确定处理请求。处理请求可涉及已加密数据210在客户接口202与请求处理基础设施212之间的传递。请求处理基础设施212可包括共同运行以提供服务提供者200的服务的一个或多个装置。例如，如图2所示，请求处理基础设施可包括用来存储代表服务提供者200的客户的数据的多个数据存储系统214。也可包括未示出的包括联网基础设施的其他基础设施。根据可通过客户接口202提交的各种类型的请求数据，例如通过网络在客户接口202与请求处理基础设施212之间的传递可根据各个实施方案以各种方式发生。例如，如果请求204是存储数据的请求，那么客户接口可利用在请求204中提供的密钥来加密所述数据并且将已加密数据210传送到请求处理基础设施212，以便存储在数据存储系统214中的一个或多个中。

[0040] 类似地，如果请求204是检索数据的请求，那么客户接口202可将通信传送到请求处理基础设施212，从而允许将来自数据存储系统214中的一个或多个的数据提供到客户接口202。客户接口202随后可使用在请求204中提供的密钥来解密已加密数据210并且将已解密数据提供到提交请求204的客户。应当注意，图2所示的服务提供者200的环境被简化以用于说明的目的，并且还可包括众多其他装置和子系统，如记录客户对服务提供者200的使用的会计系统。此外，服务提供者200可包括位于不同地理位置以达冗余和/或可用性目的的设施。

[0041] 图3示出根据各个实施方案的请求300的说明性实例，其中所述请求可以是如上文结合图1-2所述的请求。如在图3所示的实例中所示，请求300包括对称密钥，所述对称密钥

可以是用于数据的加密和解密两者的密码密钥。在实施方案中，在请求300中以明文形式提供请求300的对称密钥302。应当注意，虽然在一些实施方案中，在请求300中以明文形式提供对称密钥，但是请求从客户到服务提供者或通常在实体之间的传递可涉及各种协议，以便确保请求300中任何数据的安全性。例如，请求300的传送可涉及传输层安全性(TLS)和/或另一个协议，以使得对称密钥302在从一个实体传送到另一个实体期间被加密。此外，虽然图3示出具有对称密钥302的请求300，但是所述请求300可包括图式中未示出的其他数据。如上文论述的这种数据可包括各种请求参数、认证信息、待加密的数据和/或其他信息。

[0042] 另外，虽然图3示出具有密钥的请求，但是正如本所述和所示的所有请求，可在所述请求中提供各种其他数据，如待运行的数据和/或包括关于请求的上下文信息和不能够验证请求的真实性的认证信息的各种元数据。各种请求参数也可包括在请求中。例如，请求参数可指定，服务器端加密本应用来使用由请求提供的密钥加密数据。如果这种参数不存在和/或指示将不使用服务器端加密，那么可在不执行加密的情况下处理所述请求，无论请求中是否包括密钥。此外，对于与电子签名一起提交的请求来说，参数可指定所述请求的哪一部分用来生成电子签名。这种参数可指示请求的哪一部分应该用于检查电子签名，从而允许在其生成之后如通过添加在履行请求期间待运行的数据来修改请求。一般来说，请求在本公开中被简化以用于说明的目的。

[0043] 图4示出根据各个实施方案的可用来传送请求和接收对请求的响应的的过程400的说明性实例。过程400可由任何合适的系统执行，如由如上文所述和下文结合图15描述的客户的装置。在实施方案中，过程400包括获得402密码密钥。可根据各个实施方案以各种方式获得402所述密码密钥。例如，在一些实施方案中，通过生成密码密钥来获得402所述密码密钥。可使用例如随机数发生器或密钥推导函数如公钥推导函数2(PPKDF2)或Bcrypt来生成密码密钥。也可以其他方式获得402所述密码密钥。例如，可从数据存储装置获取密码密钥。作为另一个实例，密码密钥可以是从存储器获取的或由执行过程400的系统用户输入的口令、密码短语或密码。一般来说，可使用获得获得402密码密钥的任何方式。

[0044] 在已经获得402密码密钥的情况下，过程400可包括生成404具有所获得的密码密钥的请求；也就是说，生成包括所获得的密码密钥的请求。所述请求可通过以适合于传送的方式(也就是说以可由请求将提交至的系统处理的格式)布置用于请求的数据来生成。一旦生成404，就可提交406所生成的请求。可以任何合适的方式，如通过传送到被配置来接收所生成的请求的网络服务器的互联网协议(IP)地址来执行所生成的请求的提交406。在一些实施方案中，可执行其他操作，例如，由统一资源定位符(URL)生成请求。与域名服务(DNS)的通信可发生以获得系统的IP地址，所生成的请求随后被提交406给所述系统。一般来说，可执行提交请求的任何方式。

[0045] 在提交后，可由所生成的请求提交406至的系统处理请求。因此，过程400可包括接收408对请求的响应或所述响应可以是根据提交请求的协议来适当配置的响应。应当注意，不是所有实施方案都需要接收对请求的响应。例如，一些协议可允许在不确认请求已被接收和/或履行的情况下提交请求。作为说明性实例，所述请求可以是存储数据。在一些实施方案中，在可能不需要确认请求的处理的情况下，在提交后，可设想请求已被处理或可能已被处理。

[0046] 图5示出用于处理请求的过程500的说明性实例，其中可如上述接收所述请求并且

可根据如上述如过程400提交所述请求。可以任何合适的系统，如通过运行来提供如上述的客户接口的装置(例如，服务器)来执行过程500。在实施方案中，过程500包括接收502具有密码密钥的请求。可根据各个实施方案以各种方式接收502所述请求。例如，如上所述，可通过网络根据通信协议来提交所述请求并且可因此根据这种协议来接收所述请求。一般来说，可以任何合适的方式来接收502所述请求。

[0047] 在接收到请求后，过程500可包括确定504是否履行所述请求。可根据各个实施方案以各种方式来做出是否履行请求的确定504。例如，如上所述，在一些实例中，所述请求可与请求的电子签名一起被接收。因此，可通过确定签名是否有效来做出确定。可以各种方式执行签名是否有效的确定。例如，执行过程500的系统可验证签名本身或可将签名和请求(或通常是被签署来生成签名的数据)传送到可操作来验证电子签名的另一个系统。此外，如上所述，确定504是否履行请求可包括执行一个或多个策略是否会妨碍履行请求的确定。一般来说，可执行是否履行请求的确定的任何方式。

[0048] 另外，虽然图5和本文所示的其他过程示出是否履行请求的确定，但是在各个实施方案中，系统可履行所有适当配置的请求而无需具有有效的电子签名和/或遵循策略。返回图5所示的实施方案，如果确定504不履行请求(如在签名无效和/或策略妨碍请求的履行时)，过程500可包括拒绝506所述请求。可根据各个实施方案以各种方式拒绝506所述请求。例如，可提供对请求的响应，所述响应指示所述请求被拒绝和/或提供为何拒绝请求的信息。作为另一个实例，可通过不采取任何动作来简单地执行拒绝请求。也就是说，通过不提供对请求的响应并且决不履行请求来进行。一般来说，请求不被履行的任何方式都可视为拒绝请求。

[0049] 然而，如果确定履行请求，那么过程500可包括从所述请求提取508密码密钥。随后可使用510所提取的密码密钥来执行一个或多个所请求的密码操作；也就是说执行请求的履行所涉及的一个或多个密码操作。所述一个或多个密码操作可根据各个实施方案和根据所接收到的请求类型而变化。在一些实施方案中，一个或多个密码操作包括加密请求所包括的数据和/或加密其他数据。作为另一个实例，一个或多个密码操作可包括解密请求所引用的和/或在请求中所提供的数据。一般来说，任何类型的密码操作，诸如密钥推导和/或电子签名生成和/或验证可作为一个或多个密码操作的一部分来执行。此外，虽然本文所述的各个说明性实施方案展示单个密码操作诸如加密，但是在履行单个请求时可执行多种类型的密码操作。作为实例，在请求中所提供的一个或多个密钥可用来加密数据并且生成所述数据的电子签名和/或已加密数据，其中所述电子签名可用于稍后验证所述数据已改变。其他变体也被视为是在本公开的范围内。

[0050] 在执行一个或多个密码操作后，过程500可包括提供512对请求的响应。所述响应可根据各个实施方案和根据所做出的请求类型而变化。例如，如果请求是检索数据，那么响应可包括被检索和解密的数据。如果请求是存储数据，那么响应可以是对数据已经存储的确认。校验和或其他验证信息可与响应一起提供。在执行请求的履行中所涉及的一个或过密码操作后的某个时刻，过程500可包括失去514对所提取的密码密钥的访问，其中可以如上述的各种方式失去访问。

[0051] 图6是根据各个实施方案的请求600的说明性实例。如图6所示，不同于上文结合图3所述的请求，请求600包括可以是公钥/私钥对的公钥的客户公钥602，其中所述私钥由客

户持有或代表客户。正如本文所述的其他请求，请求600可包括如上述的其他数据。可如上文结合图4所述来提交请求600。

[0052] 图7示出过程700的说明性实例，所述过程700可用来处理包括如上文结合图6所述的客户公钥的请求。可以任何合适的系统，如提供如上述的客户接口的系统来执行过程700。如图7所示，过程700包括接收702具有客户公钥的PUT请求；也就是说具有作为所述请求的一部分的客户公钥的PUT请求(即，存储数据的请求)。可如上述并且通常以任何合适的方式来接收702所述请求。在接收到702具有客户公钥的PUT请求后，过程700可包括确定704是否履行所述请求，其中是否履行所述请求的确定可如上述做出。如果确定704不应该履行所述请求，那么过程700可包括拒绝706请求，如上所述。然而，如果确定704应该履行请求，那么过程700可包括从请求提取708客户公钥以供使用。在实施方案中，过程700包括获得710加密密钥，其中所述加密密钥可以是如上所述的对称密钥。可如上所述以任何合适的方式获得710加密。例如，可从数据存储器获取或生成加密密钥。所获得的710加密密钥可用来712加密在请求中提供的或由待加密的请求以其他方式请求的数据。客户公钥可用来714加密(包裹)加密密钥。以此方式，可使用对应于客户公钥的私钥来解密已加密的加密密钥。因此，如果执行过程700的提供者没有访问已加密的加密密钥，那么所述提供者不能解密已加密的加密密钥。

[0053] 过程700还可包括存储716已加密数据。已加密数据例如可被传送到数据存储系统以用于其持久存储。可提供718对请求的响应，其中所述响应可包括已加密的加密密钥。执行过程700的系统可失去720对加密密钥的访问，如上所述。以此方式，一旦执行过程700的系统失去720对加密密钥的访问，所述系统就不再具有解密已加密数据的能力，并且通常对应于客户公钥的私钥的使用是必要的以便通过首先解密加密密钥以解密所解密的数据来合法地(即，不需要猜测密钥或另外以未被授权的方式获得对数据的访问)解密已加密数据。

[0054] 应注意，正如本文所述的所有过程，变体被视为是在本公开的范围内。作为实例，图7示出用于处理PUT请求的过程，其中所述请求包括客户公钥。可根据各个实施方案以不同方式处理这种请求。在一些实施方案中，例如，尽管对称加密密钥的使用通常在计算上更加有效，但是客户公钥可用来加密在请求中所接收的数据而不是使用随后由公钥包裹的加密密钥。以此方式，仅可通过能访问对应于客户公钥的私钥的实体来解密数据，所述客户在各个实施方案中可以只是提交请求的所述客户。

[0055] 作为被视为本公开的范围内的变体的另一个实例，已加密的加密密钥可与已加密数据一起存储并且可或可不响应于请求来传送。在解密数据的这种实施方案中，可从存储器获得加密密钥并将其提供到能够解密加密密钥的实体(例如，具有可用来解密加密密钥的私钥的客户)，从而随后可提供回已解密的加密密钥以便允许解密数据。例如，检索数据的客户请求可使得提供者传送具有通知(包括已加密的加密密钥)的初始响应，所述初始响应是加密密钥需要解密。所述客户可解密加密密钥并且将已解密的加密密钥提供回提供者以便允许提供者解密已加密数据并且向客户提供已解密数据。其他变体也可被视为处于本公开的范围内，包括其中将密文以及可用来解密所述密文的已加密密钥从提供者提供给客户的变体。对于例如服务器端加密用于PUT请求而客户端加密用来获得对所存储数据的访问的实施方案来说，提供者可提供用于(例如，通过适当规范用于解密的数据)适当处理数

据的指令或可提供呈客户端库形式的可执行指令，以便确保正确执行解密(即，确保以将会成功解密数据方式执行解密)。

[0056] 图8示出用于通过另一个系统如提供者获得以加密形式存储的数据的过程800的说明性实例，如上所述。可以任何合适的系统，如上所述的提供者的客户装置来执行过程800。在实施方案中，过程800包括获得802已加密的加密密钥。例如，可依据上述过程700或其变体的执行来接收已加密的加密密钥。获得已加密的加密密钥可包括接收已加密的加密密钥或访问来自持久数据存储器的已加密的加密密钥。一般来说，可以任何合适的方式获得802已加密的加密密钥。

[0057] 可使用804用来加密所述加密密钥的对应于公钥的私钥来解密已加密的加密密钥。一旦已经获得已解密的加密密钥，过程800可包括生成806具有已解密的加密密钥的GET请求并且提交(例如，传送)808所生成的GET请求，如上所述。接收GET请求的系统可通过使用所述请求中的加密密钥来解密由加密密钥进行加密的数据来处理所述请求。随后可接收810响应，其中所述响应可包括适当的信息，如已经使用在GET请求中提供的已解密的加密密钥解密的数据。

[0058] 正如本文所述的所有过程，过程800的变体被视为是在本公开的范围内。例如，当已加密的加密密钥与根据已加密的加密密钥加密的数据存储在一起时，可通过从远程存储器获取已加密的加密密钥来获得已加密的加密密钥。作为另一个实例，在一些实施方案中，过程800可包括提交GET请求，所述GET请求通过提供根据已加密的加密密钥来加密的数据来履行。执行过程800的系统可获得已加密数据并且使用已解密的加密密钥来解密已加密数据。换言之，可修改过程800以便在客户端加密数据，即使所述数据是在服务器端加密过的。

[0059] 图9示出各种请求的说明性实例，所述请求可包括根据各个实施方案以各种形式包裹(例如，加密)的密码密钥。例如，图9示出请求902的说明性实例，其具有根据与提供者共享的秘密906加密的对称密钥904，其中与所述提供者共享的所述秘密可以是在客户与提供者之间共享的另一个对称密钥。作为另一个实例，图9示出请求908的实例，所述请求908包括根据提供者公钥912加密的对称密钥910，所述提供者公钥912可以是对应于公钥私钥对的公钥，提供者已访问所述公钥私钥对的对应私钥。另一个请求914包括根据与第三方共享的秘密918加密的对称密钥916。也就是针对客户和提供者两者是第三方的实体。作为又一个实例，图9示出具有根据第三方的公钥924加密的对称密钥922的请求920，其中所述第三方可以是针对客户和提供者的第三方。如上所述，图9所示的请求也可包括另外的信息。

[0060] 图10示出根据各个实施方案的可用来提交请求的过程1000的说明性实例。可以任何合适的系统，如上所述的提供者的客户的系统来执行过程1000。在实施方案中，过程1000包括获得1002密码密钥，其中可如上所述获得1002密码密钥。所获得的密码密钥可用来生成1004包裹的密码密钥，也就是说根据另一个密钥加密所获得的密码密钥。上文结合图9描述包裹的密码密钥的实例。过程1000可包括生成1006具有包裹的密码密钥的请求。也就是说所述请求可被生成来包括包裹的密码密钥。如上所述，随后可提交1008所生成的请求。在各个实施方案中，过程1000还可包括接收1010对提交1008的请求的响应。

[0061] 如上所述，众多实施方案被视为是在本公开的范围内。在一些实施方案中，客户和服务提供者能够互动来实现数据安全性而无需使用第三方系统来解包密码操作所需的密

钥。图11因此示出可实践各个实施方案的环境1100的说明性实例。正如图1，如图11所示，环境1100包括向服务提供者1106提交请求1104的客户1102。在这个实例中，请求1104包括由另一个密钥包裹的加密密钥1108(如由包围所述加密密钥的括号指示)。服务提供者1106访问可用来解包加密密钥的密钥1110，从而允许服务提供者1106使用加密密钥1108来执行密码操作。

[0062] 图12示出过程1200的说明性实例，所述过程1200可用来处理包括包裹的密码密钥的请求。过程1200可由任何合适的系统来执行，如由上文结合图11描述的服务提供者1106的网络服务器。在实施方案中，过程1200包括接收1202具有包裹的密码密钥的请求。可做出1204是否履行请求的确定。如果确定1204不履行请求，那么过程1200可包括拒绝1206请求，如上所述。然而，如果确定1204应该履行请求，那么过程1200可包括从请求提取1208包裹的密码密钥。

[0063] 可获得1210可用来解包密码密钥的密钥。可根据各个实施方案以各种方式执行可用来解包密码密钥的密钥获得。例如，可用来解包包裹的密码密钥的密钥可由执行过程1200的系统存储。可用来解包包裹的密码密钥的密钥的标识符可用来从可由系统存储的其他密钥查找可用来解包包裹的密码密钥的密钥。所述标识符可提供在接收1202的或可以其他方式(如由与提交请求的实体的关联)确定的请求中。一旦已经获得1210可用来解包包裹的密码密钥的密钥，过程1200可包括使用1212所获得的密钥来解包包裹的密码密钥。以此方式，获得未包裹的密码密钥。可使用1214所述未包裹的密码密钥来执行在履行接收1202的请求中所涉及的一个或多个密码操作。如上所述可提供1216对请求的响应并且可失去1218对未包裹的密码密钥的访问。

[0064] 在一些实施方案中，如上所述，第三方的参与是维持数据安全性的一部分。图13因此示出可实践各个实施方案的环境1300的说明性实例。如所示的环境1300包括向服务提供者1306提交请求1304的客户1302，如上所述。还如上所述，请求1304可包括由另一个密钥包裹的加密密钥1308，如上文结合图9描述的。然而，在图13的实例中，服务提供者1306的接收请求的子系统(或在一些实施方案中是服务提供者的所有子系统)不能访问可用来解包加密密钥1308的密钥。因此，环境1300包括密钥管理系统1310，所述未包裹的密码密钥访问可用来解包加密密钥1308的密钥1312。密钥管理系统1310可以是可运行来管理代表服务提供者1306的一个或多个客户的密码密钥的任何系统。

[0065] 可根据各个实施方案以各种方式实现密钥管理系统1310。在一些实施方案中，密钥管理系统是服务提供者1306的可由例如由服务提供者1306托管的硬件安全模块(HSM)或安全地存储密码密钥的另一种类型的安全模块实现的子系统。在一些实施方案中，密钥管理系统1310作为服务提供者1306的另一种服务来实现，所述服务可以是由服务提供者1306提供的若干服务之一并且可通过网络访问客户1302，如下所述。在一些实施方案中，然而，密钥管理系统是如上所述的由针对服务提供者1306和客户1302的第三方实现的系统。在此类实施方案中，客户1302和服务提供者1306均不能访问可用来解包加密密钥1308的密钥，除非可用来解包加密密钥1308的密钥1312与客户1302中的一个或多个或服务提供者1306共享。其他变体也被视为是在本公开的范围内。例如，在一些实施方案中，密钥管理系统1310可作为客户1302的一部分来实现。一般来说，密钥管理系统1310是服务提供者1306必须与其通信以便使用可用来解包加密密钥的密钥1312来解包加密密钥1308或通常已解包

加密密钥1308的系统。服务提供者1306与密钥管理系统1310之间的通信可通过一个或多个网络并且根据一个或多个适当的网络协议来发生。所述网络可以是例如互联网或任何合适的网络，如下所述。

[0066] 图14示出过程1400的说明性实例，所述过程1400可被执行来处理包括如上文结合图13所述的包裹的加密密钥的请求。在实施方案中，过程1400包括接收1402具有包裹的加密密钥的请求，如上所述。如上文结合其他过程所论述，可做出1404是否履行请求的确定，并且如果确定1404不应该履行所述请求，那么过程1400可包括拒绝1406请求。然而，如果确定1404应该履行请求，那么过程1400可包括从请求提取包裹的密码密钥。可将包裹的密码密钥传送1410到解包系统，所述解包系统可以是如上文结合图13描述的密钥管理系统，并且通常所述解包系统可以是能访问可用来解包包裹的密码密钥的密钥的系统。

[0067] 包裹的密码密钥可以请求的形式传送到解包系统，所述请求被适当配置用于由解包系统履行。例如，可根据解包系统可接受的格式来格式化所述请求并且所述请求可包括可由解包系统使用来确定是否履行请求的信息。这种信息可包括例如用来认证传送到解包系统的请求和/或所接收的1402具有包裹的密码密钥的请求的认证信息。也可提供可用来例如确定传送到解包系统的请求的履行是否遵循一个或多个策略的其他信息或所述信息可以是上下文信息，如上所述。另外的信息可包括可用来解包包裹的密码密钥的密钥的标识符。假定解包系统履行所传送1410的请求，过程1400可包括从解包系统接收1412未包裹的密码密钥。可使用1414所述未包裹的密码密钥来执行在履行接收1402的请求中所涉及的一个或多个密码操作。如上所述可提供1416对请求的响应并且可失去1418对未包裹的密码密钥的访问，如上所述。

[0068] 本公开的实施方案可鉴于以下条款来描述：

[0069] 1.一种计算机实现的方法，其包括：

[0070] 在服务提供者的一个或多个计算机系统的控制下，所述一个或多个计算机系统被配置有可执行指令，

[0071] 从对应于所述服务提供者的客户的请求者接收请求，所述请求的履行涉及关于由所述请求提供的数据的一个或多个密码操作的执行以及在所述请求中供应的密码密钥的使用，所述服务提供者在一定时间内缺少对所述密码密钥的访问直到接收到所述请求；

[0072] 通过作为执行关于所述指定数据的所述一个或多个密码操作的一部分的使用所述供应的密码密钥来履行所述请求；并且

[0073] 向数据存储系统提供执行所述一个或多个密码操作的结果；并且

[0074] 在执行所述一个或多个密码操作的某一时刻后，执行致使所述服务提供者失去对所述密码密钥的访问的一个或多个操作。

[0075] 2.如条款1所述的计算机实现的方法，其中履行所述请求包括解析所述请求以从呈明文形式的所述请求提取所述密钥。

[0076] 3.如条款1至2所述的计算机实现的方法，其中：

[0077] 所述密码密钥是公钥-私钥对的公钥，所述服务提供者缺少对其的访问；并且

[0078] 所述一个或多个密码操作包括使用所述公钥执行对称算法。

[0079] 4.如前述条款中任一项所述的计算机实现的方法，其中：

[0080] 在所述请求中供应的所述密码密钥由另一个密钥加密；

[0081] 所述方法还包括致使在所述请求中供应的所述密码密钥被解密;并且

[0082] 使用所述供应的密码密钥来执行所述一个或多个密码操作包括使用所述已解密的供应的密码密钥来执行所述一个或多个密码操作。

[0083] 5.如前述条款中任一项所述的计算机实现的方法,其中致使在所述请求中供应的所述密码密钥解密包括向另一个实体传送所述密码密钥以供解密。

[0084] 6.一种系统,其包括:

[0085] 一个或多个处理器;以及

[0086] 包括指令的存储器,当由所述一个或多个处理器执行时,所述指令致使所述系统:

[0087] 通过网络从请求者接收请求,所述请求的履行涉及使用包括在所述请求中供应的密码密钥的信息来执行关于所述请求中指定的数据的一个或多个密码操作,其中所述信息可用来认证所述请求;

[0088] 作为接收并认证所述请求的结果,执行关于所述指定数据的所述一个或多个密码操作;并且

[0089] 提供执行所述一个或多个密码操作的结果。

[0090] 7.如条款6所述的系统,其中:

[0091] 所述请求是从数据存储系统读取已加密数据的请求;并且

[0092] 所述信息可用来使用在所述请求中供应的所述密码密钥来认证所述请求。

[0093] 8.如条款6至7所述的系统,其中所述信息可用来通过包括至少部分基于不同于在所述请求中供应的所述密码密钥的第二密码密钥生成的电子签名来认证所述请求。

[0094] 9.如条款6至8所述的系统,其中:

[0095] 所述一个或多个密码操作包括加密所述指定的数据;并且

[0096] 提供执行所述一个或多个密码操作的所述结果包括将所述指定的数据以加密形式传送到数据存储系统以用于持久存储。

[0097] 10.如条款6至9所述的系统,其中所述指令进一步致使所述系统执行一个或多个操作,以便在执行所述一个或多个密码操作之后的某一时刻失去对在请求中供应的所述密码密钥的访问。

[0098] 11.如条款6至10所述的系统,其中:

[0099] 在所述请求中供应的所述密码密钥呈加密形式;并且

[0100] 所述指令进一步致使所述系统获得呈解密形式的所述密码密钥;并且

[0101] 执行所述一个或多个密码操作利用呈解密形式的所述密码密钥。

[0102] 12.如条款6至11所述的系统,其中:

[0103] 在所述请求中供应的所述密码密钥是公钥-私钥对的公钥;并且

[0104] 执行关于所述指定数据的所述一个或多个密码操作包括:

[0105] 利用对称密钥加密所述指定数据;并且

[0106] 使用所述公钥加密所述对称密钥。

[0107] 13.如条款6至12所述的系统,其中所述系统在一定时间内缺少对所述密码密钥的访问,直至接收到所述请求。

[0108] 14.如条款6至13所述的系统,其中:

[0109] 在所述请求中供应的所述密码密钥被供应在呈加密形式的所述请求中;并且

[0110] 所述系统还包括子系统，所述子系统被配置来安全地存储从所述子系统的外部难接近的多个密码密钥，所述多个密码密钥包括可用来解密以加密形式供应的所述密码密钥的特定密码密钥；

[0111] 所述指令进一步致使所述系统致使所述子系统解密以加密形式供应的将用于执行所述一个或多个密码操作的所述密码密钥。

[0112] 15.如条款6至14所述的系统，其中所述信息可用来通过使用所述密码密钥认证所述请求来认证所述请求。

[0113] 16.一种非暂时性计算机可读存储介质，其具有存储在其上的指令，当由计算机系统的一个或多个处理器执行时，所述指令致使所述计算机系统：

[0114] 生成被格式化用于服务提供者的应用编程接口的应用编程接口请求，所述应用编程接口请求包括密码密钥并且使用所包括的密码密钥来指定将要由所述服务提供者关于数据执行的一个或多个密码操作；并且

[0115] 允许所述生成的应用编程接口请求与至少部分基于所述请求生成的认证信息一起通过网络传送到服务提供者，从而致使所述服务提供者使用所述密码密钥来执行关于所述数据的所述一个或多个密码操作。

[0116] 17.如条款16所述的非暂时性计算机可读存储介质，其中：

[0117] 所述应用编程接口请求是将数据存储在所述服务提供者的数据存储系统中；并且

[0118] 所述一个或多个密码操作包括在将数据存储于所述数据存储系统中之前加密所述数据。

[0119] 18.如条款16至17所述的非暂时性计算机可读存储介质，其中：

[0120] 所述应用编程接口请求是在数据存储系统中检索数据，所述数据被以加密形式存储在所述数据存储系统中；并且

[0121] 所述一个或多个密码操作包括在从所述数据存储系统检索数据之后解密所述数据。

[0122] 19.如条款16至18所述的非暂时性计算机可读存储介质，其中所述密码密钥以加密形式包括在所述应用编程接口请求中，以使得所述服务提供者能够使用加密形式的所述密码密钥来获得非加密形式的所述密码密钥，以供用于执行所述一个或多个密码操作。

[0123] 20.如条款16至19所述的非暂时性计算机可读存储介质，其中所述密码密钥难以访问所述服务提供者，直到接收到所述请求。

[0124] 21.如条款16至20所述的非暂时性计算机可读存储介质，其中所述传送的应用编程接口请求缺少所述数据。

[0125] 22.如条款16至21所述的非暂时性计算机可读存储介质，其中至少部分基于不同于所述应用编程接口请求中所包括的所述密码密钥的另一个密码密钥来生成所述认证信息。

[0126] 23.如条款16至22所述的非暂时性计算机可读存储介质，其中所述应用编程接口请求还包括所述服务提供者所需的信息，以便确定所述请求的履行是否遵循可适用于所述请求的一个或多个策略。

[0127] 如在本公开中多次指出，众多变体被认为是在本公开的范围内。例如，如所论述的，众多变体利用对称和/或不对称的密码原语。对称密钥算法可包括用于执行关于数据的

密码操作的各种方案，包括分组密码、流密码以及数字签名方案。示例性对称密钥算法包括但不限于，高级加密标准(AES)、数据加密标准(DES)、三重DES(3DES)、Serpent、Twofish、blowfish、CAST5、RC4以及国际数据加密算法(IDEA)。对称密钥算法还可包括用来生成单向函数的输出的那些算法，并且包括但不限于利用基于散列的消息认证码(HMAC)、通用消息认证码(MAC)、PBKDF2以及Bcrypt的算法。对称密钥算法还可包括用于执行关于数据的密码操作的各种方案。示例性算法包括但不限于利用Diffie-Hellman密钥交换协议、数字签名标准(DSS)、数字签名算法、ElGamal算法、椭圆曲线算法、密码认证的密钥协商技术、pallier密码系统、RSA加密算法(PKCS#1)、Cramer-Shoup密码系统、YAK认证的密钥协商协议、NTRUEncrypt密码系统、McEliece密码系统的算法以及其他算法。椭圆曲线算法包括椭圆曲线Diffie-Hellman(ECDH)密钥协商方案、椭圆曲线集成加密方案(ECIES)、椭圆曲线数字签名算法(ECDSA)、ECMQV密钥协商方案以及ECQV隐式证书方案。其他算法和算法的组合也被视为是在本公开的范围内。

[0128] 另外，如上所述，本公开的各种实施方案涉及使用请求中所包括的密码密钥来执行各种密码操作。虽然密钥被论述成用来执行所述操作，但是应当注意，本公开的各个实施方案包括密钥在使用之前以某种方式变换的那些实施方案。作为实例，在请求中的密钥是密码的情况下，所述口令在使用之前可进行变换(例如，利用密钥推导函数)以执行另外的密码操作。此外，虽然本公开论述特定类型的密钥(例如，加密密钥)，但是此类密钥在使用之前可以类似方式进行变换。其他变体包括在请求中提供多个密钥以及请求参数和/或所述请求的格式化指示应该如何使用多个密钥的那些实施方案。

[0129] 被视为处于本公开的范围内的其他变体包括利用预设的统一资源定位符(URL)的实施方案。参考如图1所示的包括服务提供者的客户的环境，客户可预生成包括URL的一部分的电子签名和/或其他信息(如密码密钥)的URL。所述客户可向另一个实体提供所述URL，并且另一个实体可利用所述URL来将请求提交给服务提供者，从而致使服务提供者在所述客户的授权下执行一个或多个操作。服务提供者可接收与URL一起提交的请求、验证电子签名并且使用所述URL中提供的密钥来执行一个或多个操作。以此方式，实现了各种便利，所述便利涉及在客户控制下通过密钥进行的服务器端加密和解密以及提供者在非必要时不能访问密钥。预设URL和其变体的使用在同时提交的美国专利申请号14/037,282、标题为“具有密钥的资源定位符”(Resource Locators With Keys)中详细论述，所述专利申请以全文引用方式并入。

[0130] 图15示出用于实现根据各个实施方案的各方面的示例性环境1500的各方面。如将了解，尽管出于解释目的使用基于网络的环境，但是可视情况使用不同环境来实现各个实施方案。环境包括电子客户端装置1502，电子客户端装置可包括可操作来在适当网络1504上发送和接收请求、消息或信息并且将信息传送回装置用户的任何适当装置。此类客户设备的实例包括个人计算机、手机、手持通信设备，笔记本计算机、平板计算机、机顶盒，个人数据助理、嵌入式计算机系统、电子书阅读器等。网络可包括任何适当网络，包括内部网、互联网、蜂窝网、局域网或任何其他此类网络或上述网络的组合。此类系统所用的组件可以至少部分地取决于所选网络和/或环境的类型。用于通过此类网络通信的协议和组件是众所周知的，因而本文不再详细论述。网络上的通信可通过有线或无线连接及其组合来实现。在这个实例中，网络包括互联网，因为环境包括用于接收请求并且响应于所述请求而提供内

容的网络服务器1506，然而对于其他网络来说，可使用服务类似目的的替代装置，如本领域技术人员所显而易见的。

[0131] 所示环境包括至少一个应用程序服务器1508和数据存储器1510。应当理解，可以存在可以链接起来或以其它方式来配置的若干应用程序服务器、层或其它元件、过程或组件，这些应用程序服务器、层或其它元件、过程或组件可交互来执行如从适合的数据存储器获取数据的任务。如本文所使用的服务器可以各种方式来实现，诸如硬件装置或虚拟计算机系统。在一些情境中，服务器可以是指在计算机系统上实行的编程模块。如本文所使用的，术语“数据存储器”指代能够存储、访问和检索数据的任何装置或装置组合，所述装置的装置组合可包括任何标准、分布式或集群式环境中的任何组合和任何数目的数据服务器、数据库、数据存储装置和数据存储介质。应用程序服务器可包括任何适当硬件和软件，所述硬件和软件视执行客户端装置的一个或多个应用程序的各方面的需要而与数据存储器集成、处置应用程序的一些(甚至是大多数)数据访问和业务逻辑。应用程序服务器可提供与数据存储器协作的存取控制服务，并且能够生成将要传送到用户的内容、如文本、图片、音频和/或视频，在这个实例中，所述内容可以超文本标记语言(“HTML”)、可扩展标记语言(“XML”)或另一种适当结构化语言的形式由网络服务器向用户提供。所有请求和响应的处置以及客户端装置1502与应用程序服务器1508之间的内容递送可由网络服务器来处置。应当理解，网络服务器和应用程序服务器不是必要的，且仅仅是示例性组件，因为本文所论述的结构化代码可在如本文其他地方所论述的任何适当装置或主机上执行。此外，除非上下文另外清楚规定，否则如由单个装置执行的本文所述的操作可由可形成分布式系统的多个装置共同执行。

[0132] 数据存储器1510可包括若干单独的数据表、数据库或其他数据存储机构和介质，用来存储与本公开的特定方面相关的数据。举例来说，所示数据存储器可包括用于存储生成数据1512和用户信息1516的机构，生成数据和用户信息可用于提供用于生成端的内容。数据存储器还被示出为包括用于存储日志数据1514的机构，所述日志数据可用于报告、分析或其他此类目的。应当理解，可能存在可能需要存储在数据存储器中的许多其它方面，如页面图像信息和访问权信息，所述方面可视情况存储在上文列出的机构中的任何机构中或存储在数据存储器1510的中额外机构中。数据存储器1510可通过与它关联的逻辑来操作，以便从应用程序服务器1508接收指令，并且响应于所述指令而获取、更新或以其他方式处理数据。在一个实例中，用户通过由所述用户操作的装置可以针对某种类型的项目提交搜索请求。在此状况下，数据存储器可能访问用户信息来验证用户的身份，并且可访问目录详细信息以获取有关所述类型的项目的信息。接着可将信息如以网页上的结果列表的形式返回给用户，用户能够通过用户装置1502上的浏览器来查看所述网页。可在浏览器的专用页面或窗口中查看到感兴趣的特定项目的信息。然而，应当注意，本公开的实施方案不必受限于网页背景，但可能更普遍适用于处理一般的请求，其中所述请求在内容上不是必需的请求。

[0133] 每个服务器通常将包括提供用于所述服务器的一般管理和操作的可执行程序指令的操作系统，并且通常将包括存储指令的计算机可读存储介质(例如，硬盘、随机存取存储器、只读存储器等)，当由服务器的处理器执行时，所述指令允许服务器实行其期望的功能。操作系统的适合实现方式和服务器的一般功能是众所周知的或可商购的，并且易于由

本领域普通技术人员实现，尤其是根据本文中的公开来实现。

[0134] 在一个实施方案中，环境是利用通过通信链路、使用一个或多个计算机网络或直接连接来互连的若干计算机系统和组件的分布式计算环境。然而，本领域普通技术人员应理解，这种系统可在具有比图15所示的组件更少或更多数量的组件的系统中同样顺利地操作。因此，图15中的系统1500的描绘本质上应视为说明性的，并且不限制本公开的范围。

[0135] 各个实施方案可进一步在广泛范围的操作环境中实现，在一些情况下，所述环境可包括一个或多个用户计算机、计算装置或可用于操作多个应用程序中的任一个的处理装置。用户或客户端装置可包括多个通用个人计算机中的任何一个，如运行标准操作系统的台式计算机、膝上型计算机或平板计算机，以及运行移动软件并且能够支持多个网络连接协议和消息传递协议的蜂窝装置、无线装置和手持式装置。这种系统还可包括多个工作站，所述工作站运行各种可商购得的操作系统和用于如开发和数据库管理等目的的其他已知应用程序中的任一个。这些装置还可包括其他电子装置，如虚拟终端、薄型客户端、游戏系统和能够通过网络通信的其他装置。

[0136] 本公开的各个实施方案利用本领域技术人员可能熟悉的至少一种网络来使用各种各样可商购得的协议中的任一种支持通信，所述模型和协议如传输控制协议/互联网协议(“TCP/IP”)、在开放系统互连(“OSI”)模型的各个层中操作的协议、文件传送协议(“FTP”)、通用即插即用(“UpnP”)、网络文件系统(“NFS”)、公共互联网文件系统(“CIFS”)以及AppleTalk。网络例如可以是例如局域网、广域网、虚拟专用网、互联网、内部网、外联网、公共交换电话网、红外网络、无线网络以及上述网络的任何组合。

[0137] 在利用网络服务器的实施方案中，网络服务器可以运行各种各样服务器或中间层应用程序中的任一种，包括超文本传输协议(“HTTP”)服务器、FTP服务器、公共网关接口(“CGI”)服务器、数据服务器、Java服务器和业务应用程序服务器。服务器还能够响应于来自用户装置的请求而执行程序或脚本，如通过执行可以实施为以任何编程语言(如Java®、C、C#或C++)或任何脚本语言(如Perl、Python或TCL)以及其组合写成的一个或多个脚本或程序的一个或多个网络应用程序。所述服务器还可包括数据库服务器，包括但不限于那些可商购的Oracle®、Microsoft®、Sybase®和IBM®。

[0138] 环境可包括如上文所论述的各种各样数据存储区以及其他存储器和存储介质。这些可驻留在各种各样位置，如在一个或多个计算机本地(和/或驻留在一个或多个计算机中)的存储介质上，或远离网络上的计算机中的任何或所有计算机。在实施方案的特定集中，信息可驻留在本领域技术人员熟悉的存储区域网(“SAN”)中。类似地，用于执行属于计算机、服务器或其他网络装置的功能的任何必要的文件可视情况本地或远程存储。在系统包括计算机化装置的情况下，这个这种装置可包括可通过总线电耦合的硬件元件，所述元件包括例如至少一个中央处理单元(“CPU”或“处理器”)、至少一个输入装置(例如，鼠标、键盘、控制器、触摸屏或小键盘)和至少一个输出装置(例如，显示装置、打印机或扬声器)。这种系统还可包括一个或多个存储装置，如硬盘驱动器、光存储装置和如随机存取存储器(“RAM”)或只读存储器(“ROM”)的固态存储装置、以及可移动媒体装置、存储卡、闪存卡等。

[0139] 此类装置还可包括计算机可读存储介质读取器、通信装置(例如，调制解调器、网卡(无线或有线)、红外线通信装置等)和工作存储器，如上文所论述。计算机可读存储介质读取器可与计算机可读存储介质连接或被配置来接收计算机可读存储介质，计算机可读存

储介质表示远程、本地、固定和/或可移动存储装置以及用于暂时和/或更永久地含有、存储、传输和检索计算机可读信息的存储介质。系统和各种装置通常还将包括位于至少一个工作存储器装置内的多个软件应用程序、模块、服务系统或其他元件，包括操作系统和应用程序，如客户端应用程序或网络浏览器。应当了解，替代实施方案可具有与上述实施方案不同的众多变体。例如，也可使用定制硬件，和/或特定元件可以在硬件、软件(包括可移植软件，如小程序)或两者中实现。此外，可以采用与如网络输入/输出装置的其他计算装置的连接。

[0140] 用于含有代码或部分代码的存储介质和计算机可读介质可包括本领域已知或已使用的任何适当介质，包括存储介质和通信介质，如但不限于以用于存储和/或传输信息(如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术所实现的易失性和非易失性、可移动和不可移动的介质，包括RAM、ROM、电可擦可编程只读存储器(“EEPROM”)、闪存或其他存储器技术、只读光盘驱动器(“CD-ROM”)、数字通用光盘(DVD)或其他光学存储器、磁盒、磁带、磁盘存储装置或其他磁性存储装置，或可用于存储所需信息且可由系统装置访问的任何其他介质。基于本文所提供的公开内容和教义，本技术领域普通技术人员将了解实现各个实施方案的其他方式和/或方法。

[0141] 因此，应在说明性意义而不是限制性意义上理解本说明书和附图。然而，将显而易见的是：在不脱离如在权利要求书中阐述的本发明的更宽广精神和范围的情况下，可以对其做出各种修改和改变。

[0142] 其他变体也在本公开的精神内。因此，尽管所公开的技术可容许各种修改和替代构造，但在附图中已示出并且在上文中详细描述所示的其特定实施方案。然而，应当了解，并不旨在将本发明限制于所公开的一种或多种具体形式，相反地，旨在涵盖落在如所附权利要求书限定的本发明的精神和范围内的所有修改、替代构造和等效物。

[0143] 在描述所公开实施方案的上下文中(尤其是在以下权利要求书的上下文中)，术语“一个(a，an)”和“所述”以及类似指称对象的使用应解释为涵盖单数和复数两者，除非在本文另外地指示或明显地与上下文矛盾。术语“包含”、“具有”、“包括”和“含有”应解释为开放式术语(即，意味着“包括但不限于”)，除非另外地注解。术语“连接的”(当未更改且是指物理连接时)应解释为部分地或全部地纳入在以下解释内：附接至或结合在一起，即使存在介入物。除非本文另外指明，否则本文中值范围的列举仅仅意图用作个别地表示属于所述范围的各单独值的速记方法，并且犹如本文个别描述地那样将各单独值并入到本说明书中。除非此外另有指出或与上下文矛盾，否则术语“集合”(例如“项目集合”)的使用被解释为包括一个或多个成员的非空集合。此外，除非此外另有指出或与上下文矛盾，对应集合的术语“子集”没有必要表示对应集合的真子集，而对应集合的子集可以是相等的。

[0144] 除非另外特别规定或另外与上下文矛盾，连接语言，如具有形式“A、B、以及C中的至少一个”或“A、B以及C中的至少一个”的短语另外与上下文一起理解为一般用来呈现的是，项目、术语等可以是A或B或C，或A和B和C的集合的任何非空子集。例如，在具有用于上文连接短语的三个成员的集合的说明性实例中，“A、B、以及C中的至少一个”和“A、B以及C中的至少一个”是指以下集合中的任一个：{A}、{B}、{C}、{A，B}、{A，C}、{B，C}、{A，B，C}。因此，此类连接性语言一般并非意在暗示某些实施方案需要存在A中的至少一个、B中的至少一个以及C中的至少一个。

[0145] 可按任何合适的顺序来执行本文所述的过程操作，除非本文另外指明或明显地与上下文矛盾。本文所述的过程(或变体和/或其组合)的一些或全部可在配置有可执行指令的一个或多个计算机系统的控制下实行，并且可作为共同地在一个或多个处理器上执行的代码(例如，可执行指令、一个或多个计算机程序或一个或多个应用程序)、由硬件或其组合来实施。代码可以例如包括可由一个或多个处理器执行的多个指令的计算机程序的形式存储在计算机可读储存介质上。计算机可读储存介质可以是非暂时性的。

[0146] 本文所提供的任何以及所有实例或示例性语言(例如，“如”)的使用仅意图更好地说明本发明的实施方案，并且除非另外要求保护，否则不会对本发明的范围施加限制。本说明书中的语言不应解释为将任何非要求保护的要素指示为实践本发明所必需。

[0147] 本文中描述了本公开的优选实施方案，包括发明人已知用于执行本发明的最佳模式。阅读上述说明后那些优选实施方案的变体对于本领域的普通技术人员可以变得显而易见。发明人希望技术人员视情况采用此类变体，并且发明人意图以不同于如本文所特别描述的方式来实践本公开的实施方案。因此，经适用的法律许可，本公开的范围包括在此附加的权利要求中叙述的所有主题的改良形式和等价物。此外，除非本文另外指示或明显地与上下文矛盾，否则本公开的范围涵盖其所有可能变体中的上述元素的任何组合。

[0148] 本文所引用的所有参考文献(包括出版物、专利申请和专利)据此以引用方式并入，其程度等同于每个参考文献单独地且具体地被表示为以引用方式并入本文并且以其全文在本文得以陈述。

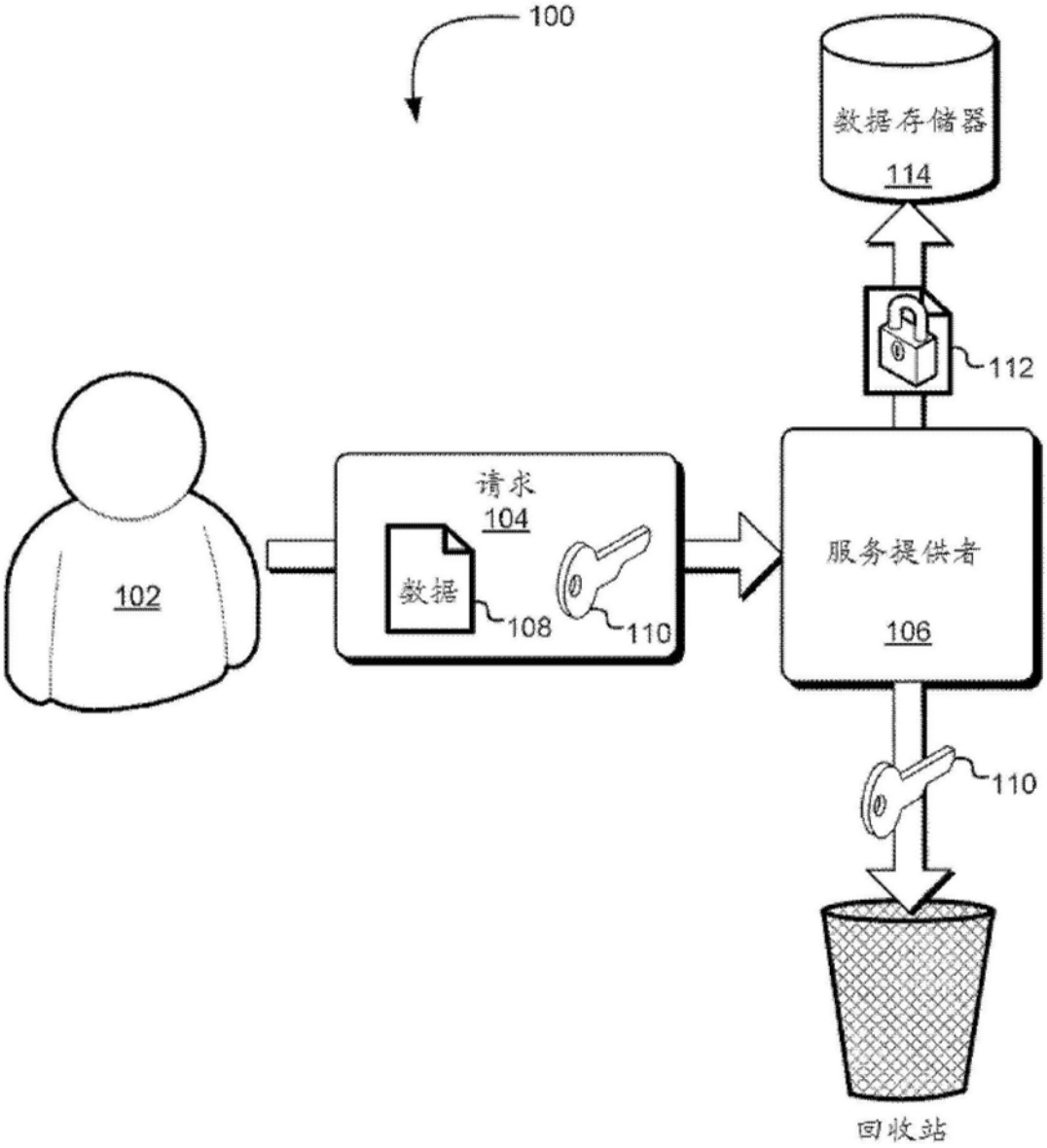


图1

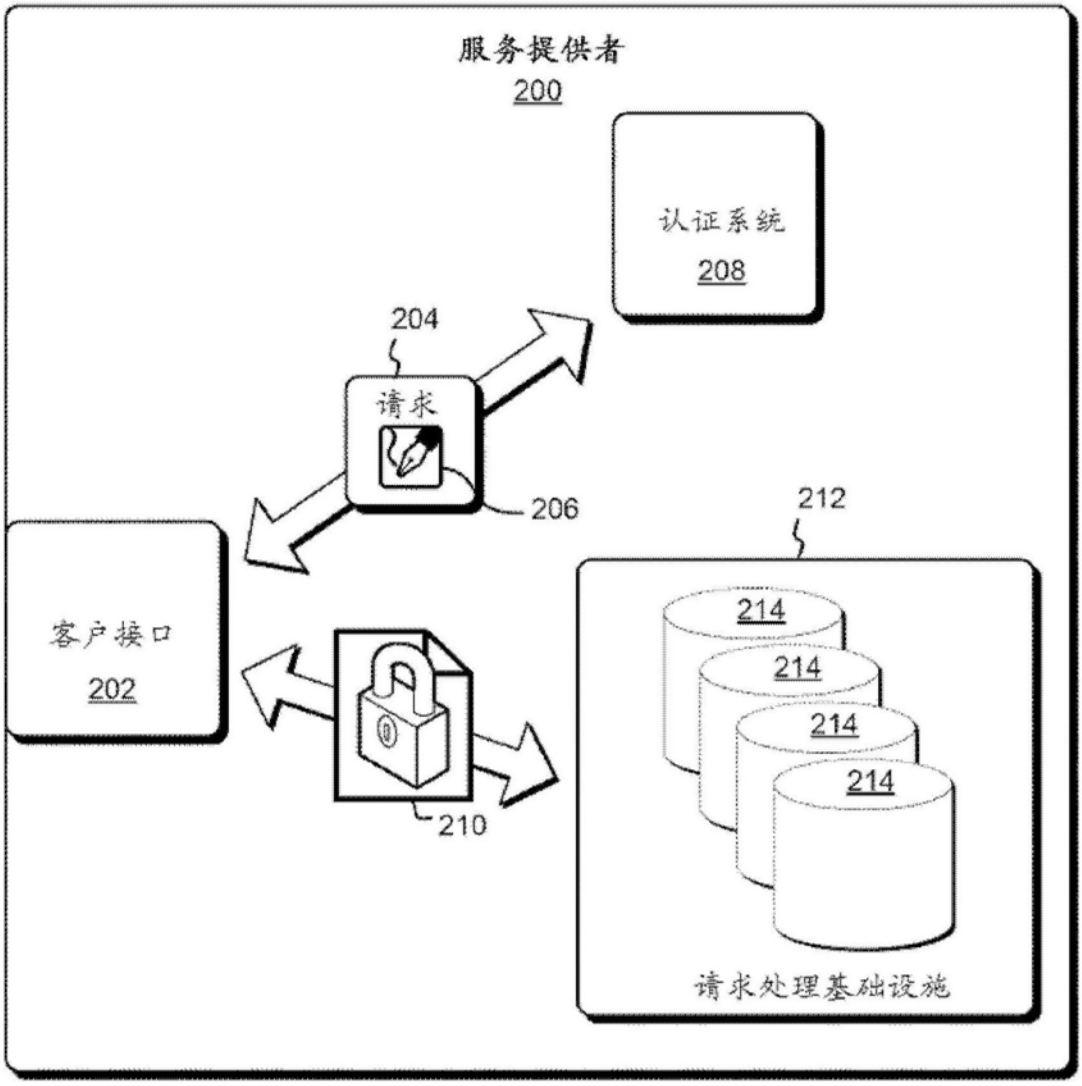

服务提供者
200
认证系统
208
204
请求
206
212
客户接口
202
214
214
214
214
210
请求处理基础设施

图2

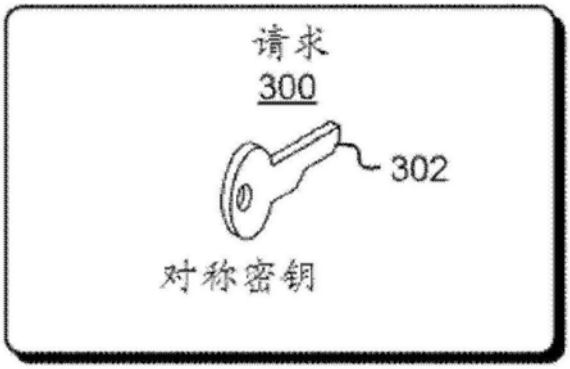

请求
300
302
对称密钥

图3

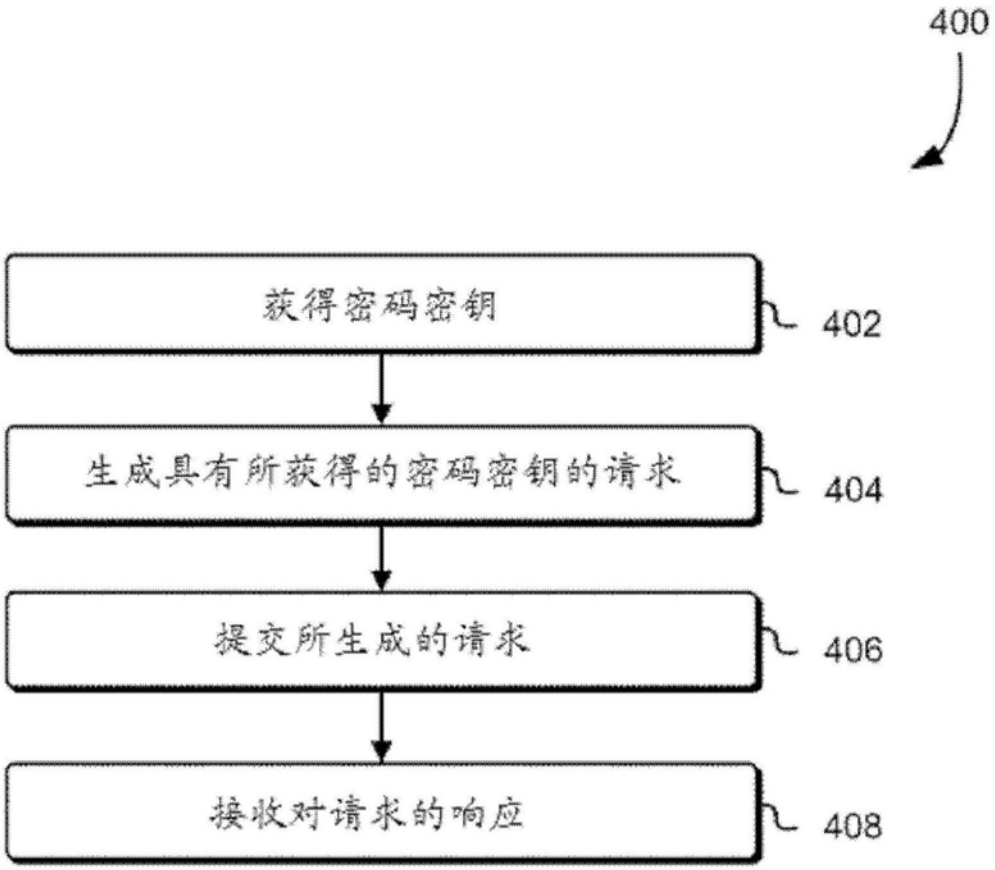

400
获得密码密钥
402
生成具有所获得的密码密钥的请求
404
提交所生成的请求
406
接收对请求的响应
408

图4

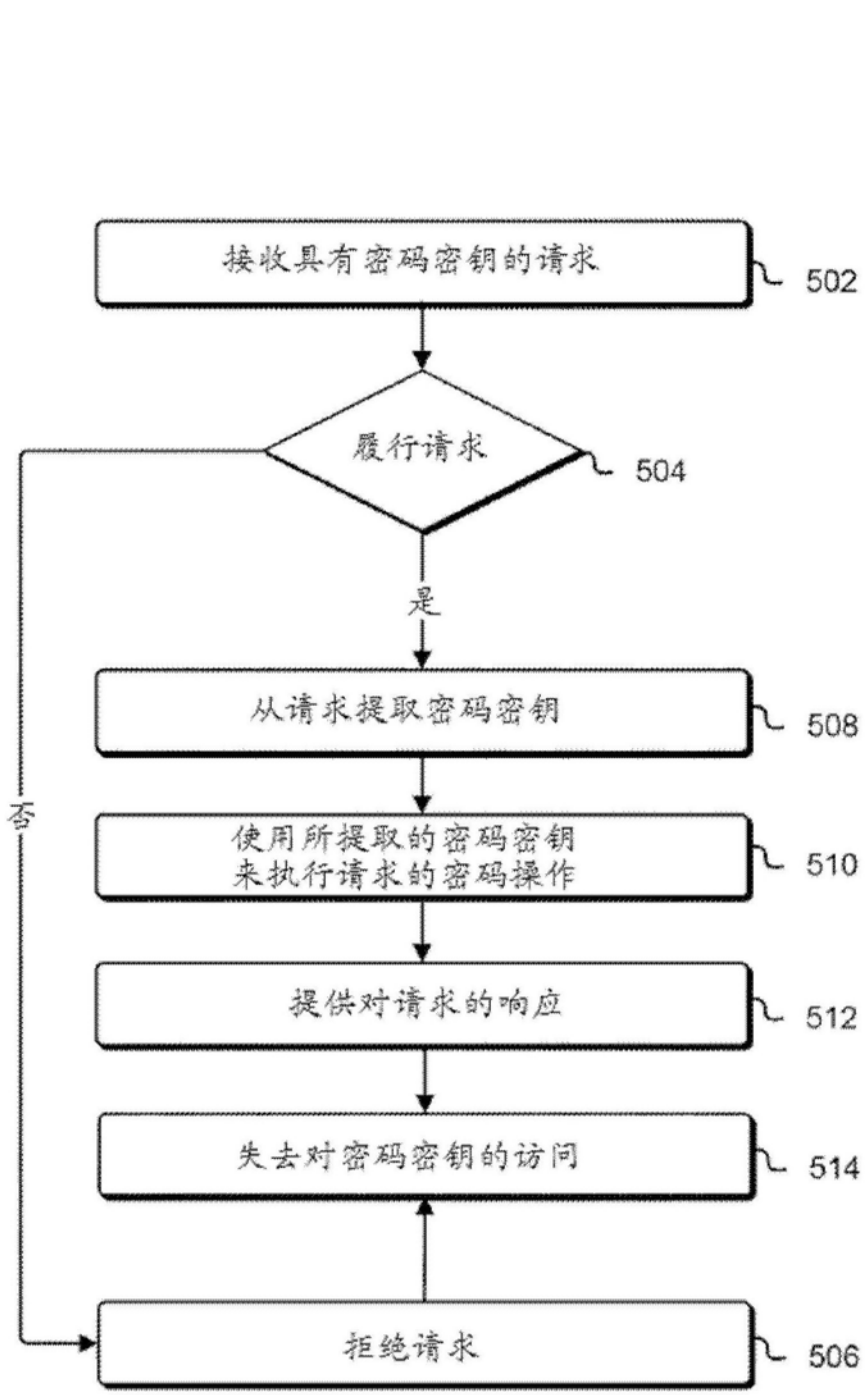

500
接收具有密码密钥的请求
502
履行请求
504
是
否
从请求提取密码密钥
508
使用所提取的密码密钥
来执行请求的密码操作
510
提供对请求的响应
512
失去对密码密钥的访问
514
拒绝请求
506

图5

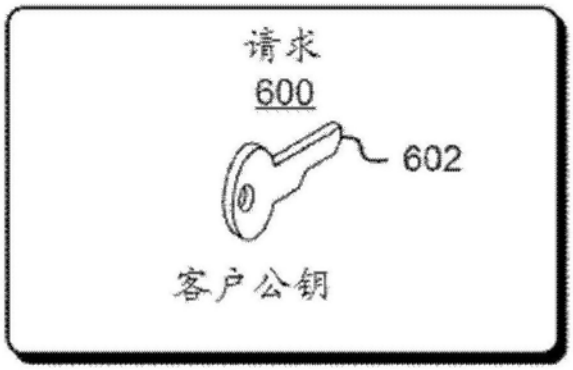


图6

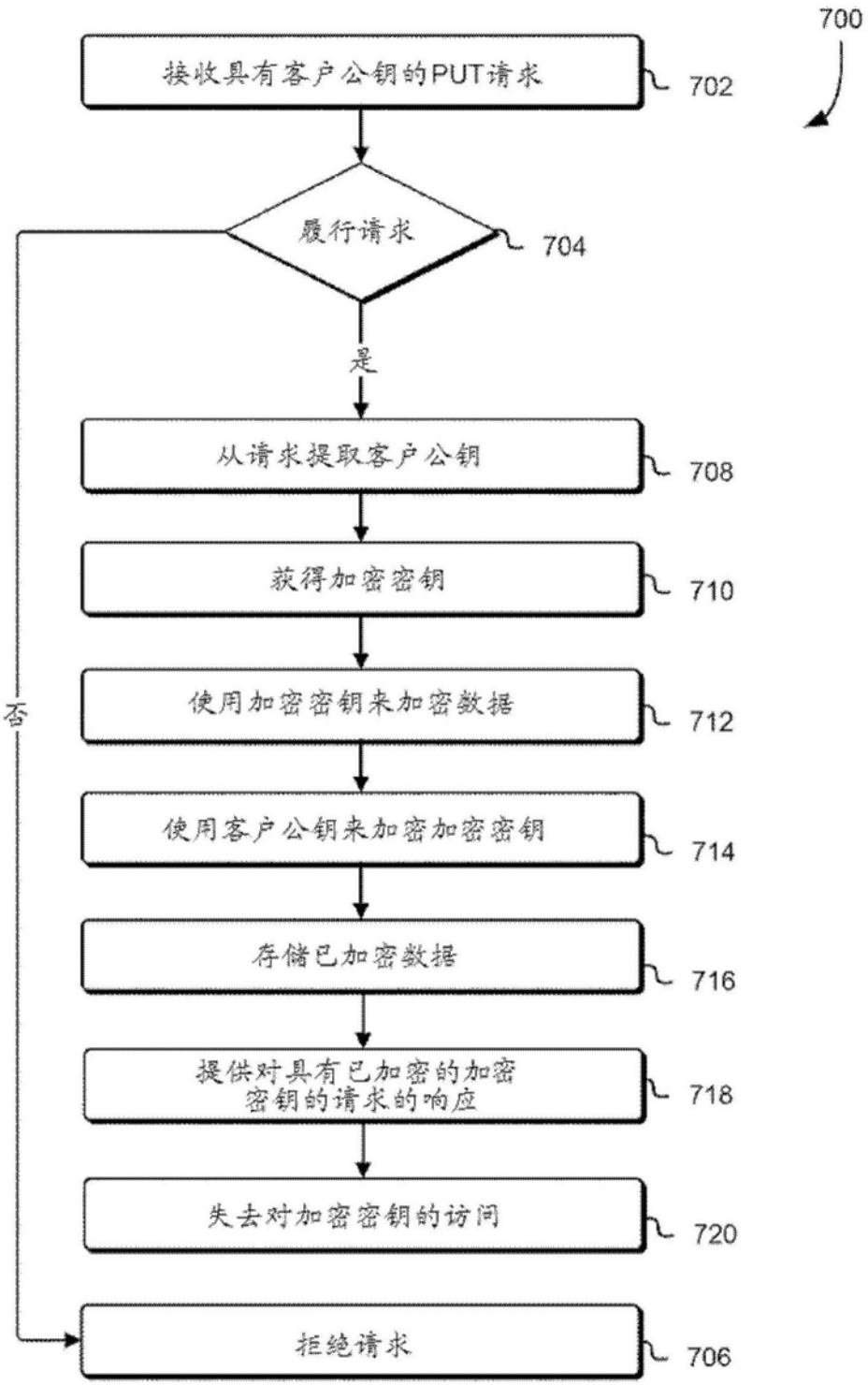

700
接收具有客户公钥的PUT请求
702
履行请求
704
是
否
从请求提取客户公钥
708
获得加密密钥
710
使用加密密钥来加密数据
712
使用客户公钥来加密加密密钥
714
存储已加密数据
716
提供对具有已加密的加密密钥的请求的响应
718
失去对加密密钥的访问
720
拒绝请求
706

图7

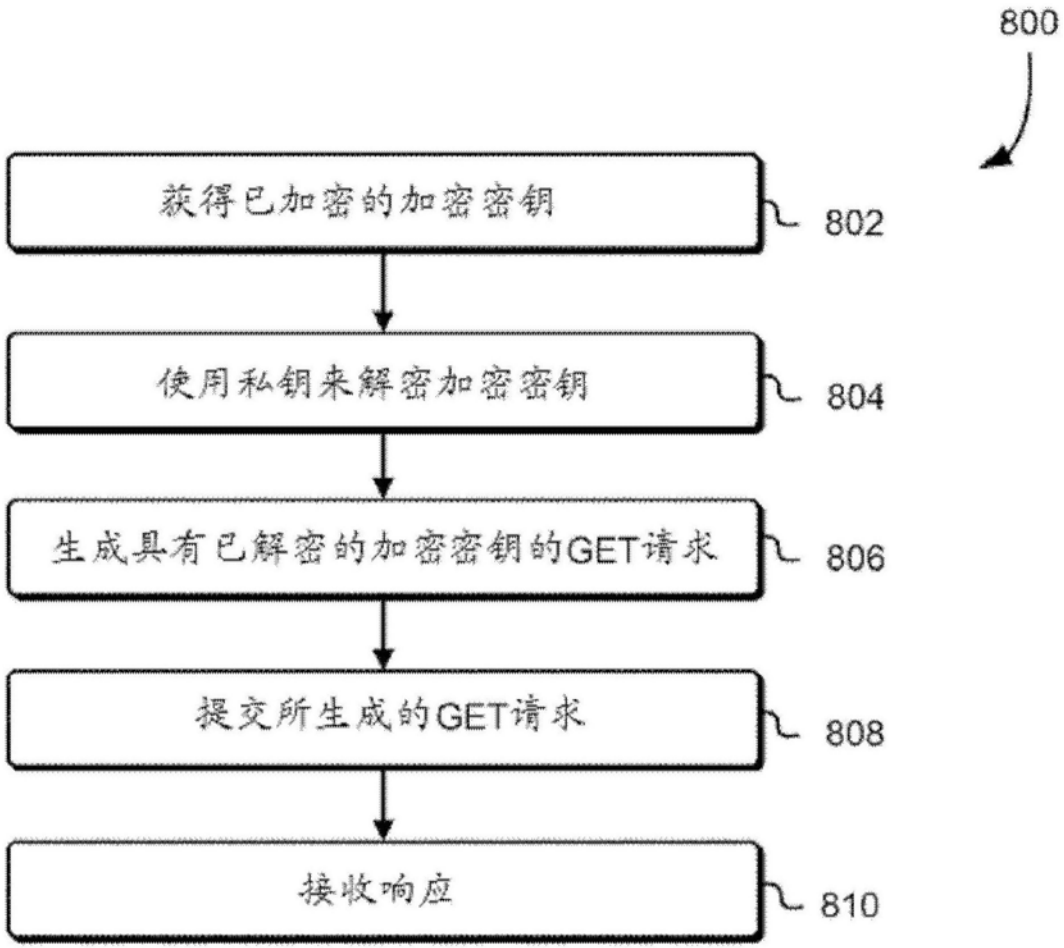

800
获得已加密的加密密钥
802
使用私钥来解密加密密钥
804
生成具有已解密的加密密钥的GET请求
806
提交所生成的GET请求
808
接收响应
810

图8

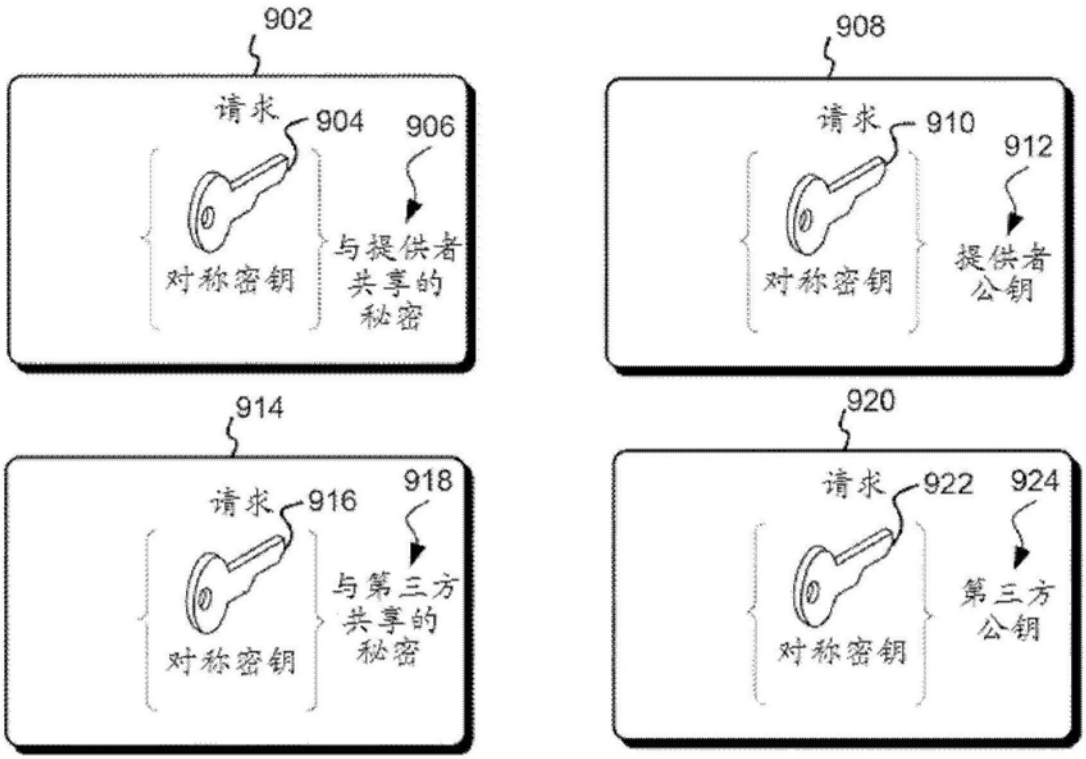

902
请求
904
906
对称密钥
与提供者共享的秘密
908
请求
910
912
对称密钥
提供者公钥
914
请求
916
918
对称密钥
与第三方共享的秘密
920
请求
922
924
对称密钥
第三方公钥

图9

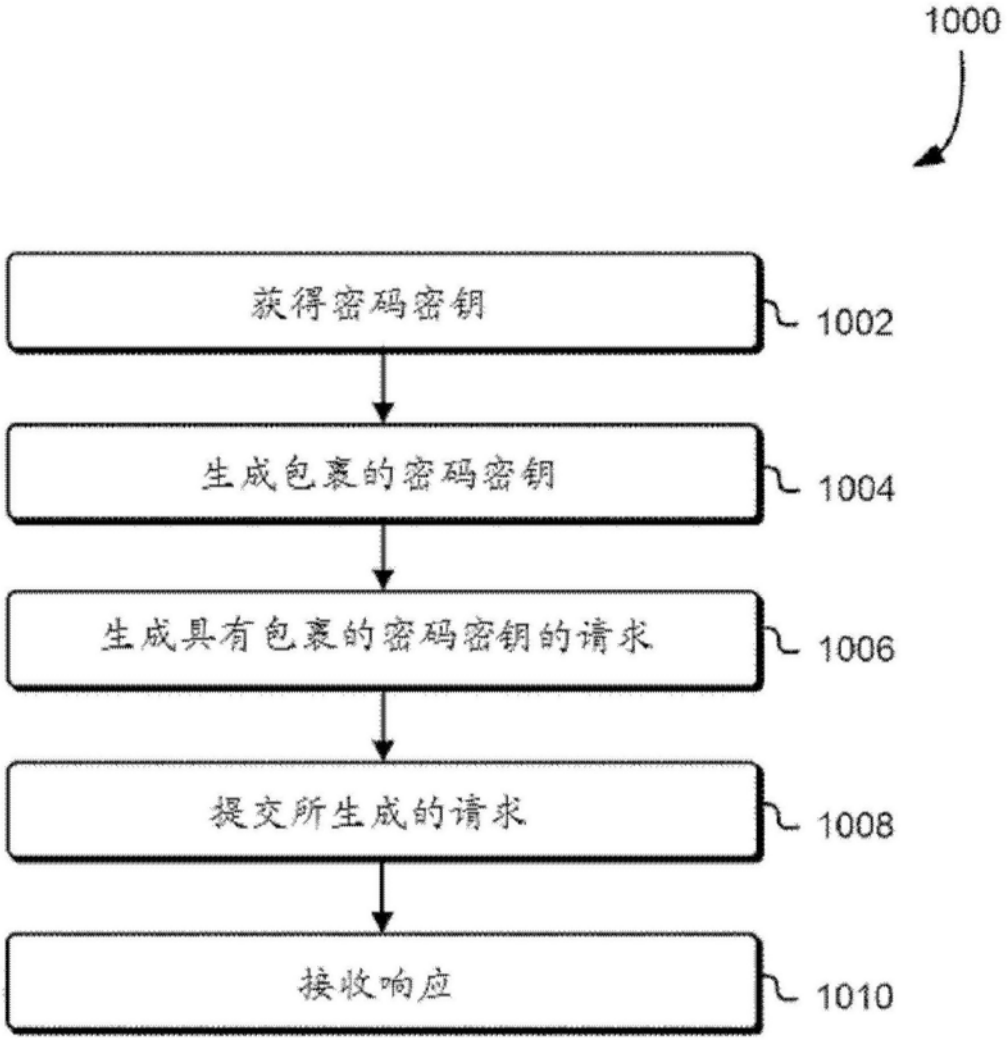

1000
获得密码密钥
1002
生成包裹的密码密钥
1004
生成具有包裹的密码密钥的请求
1006
提交所生成的请求
1008
接收响应
1010

图10

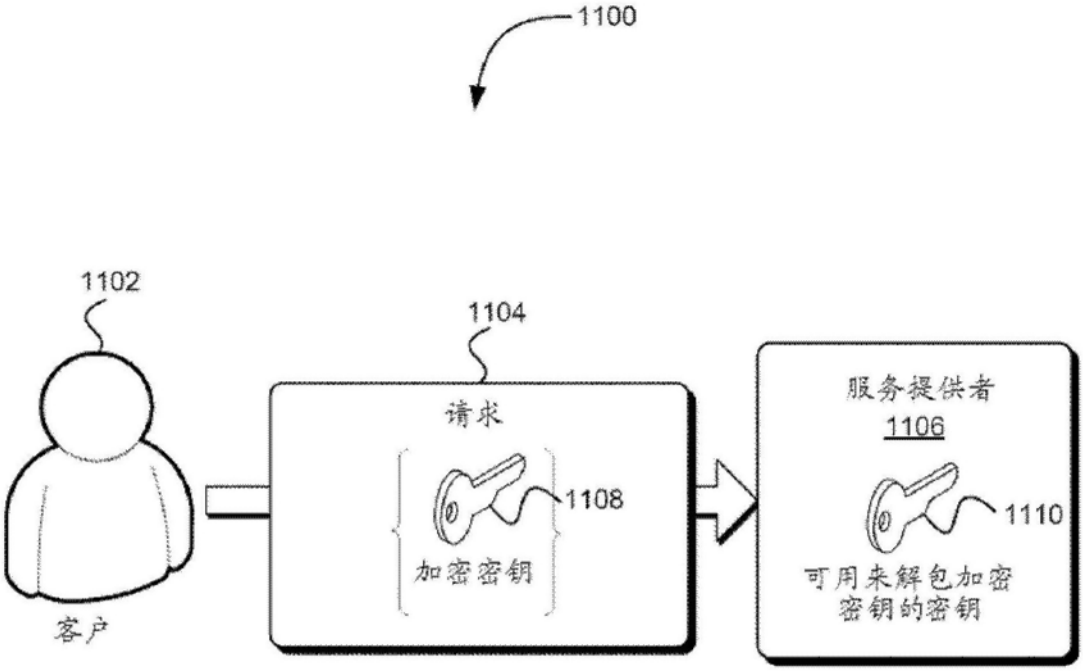


图11

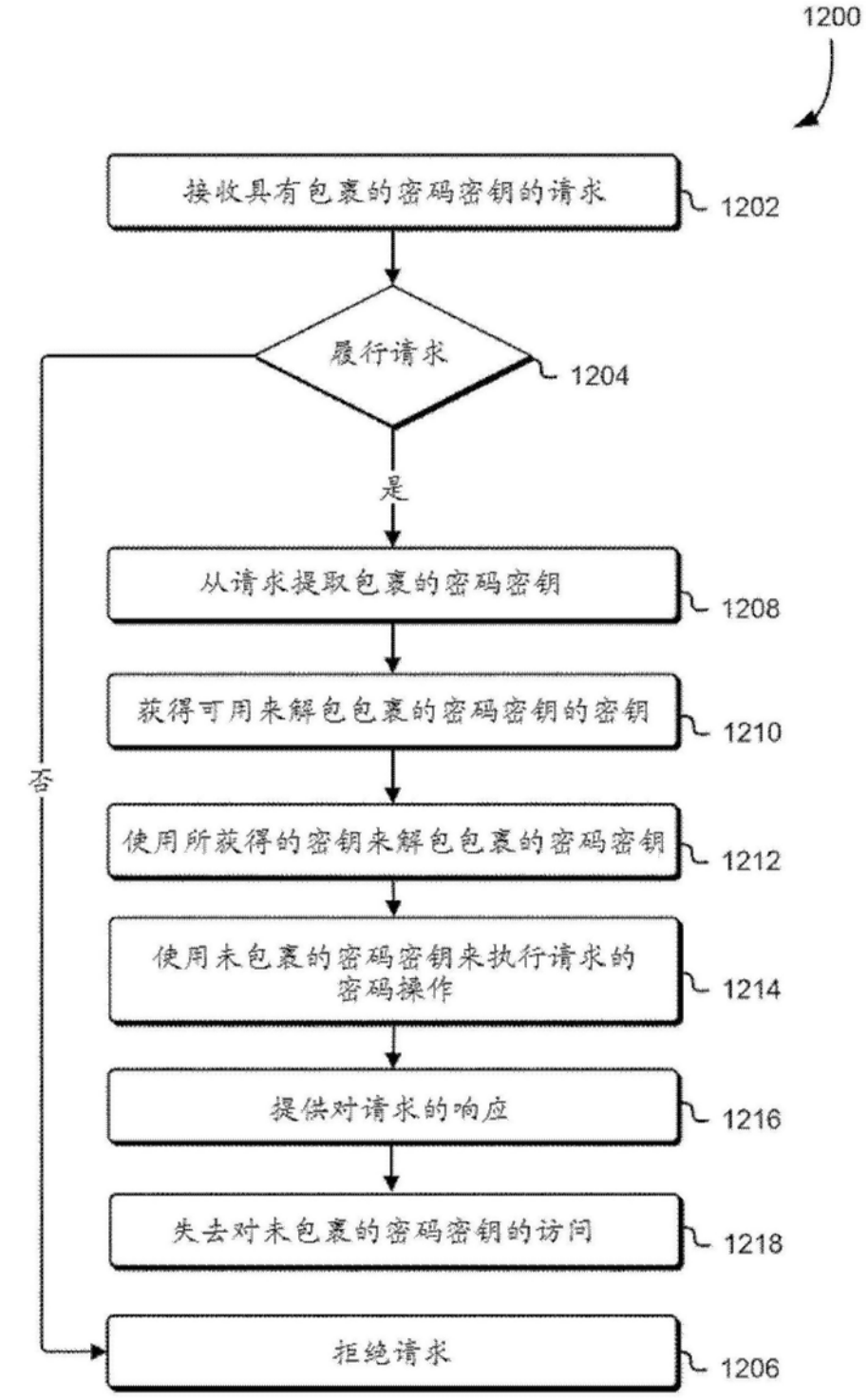

1200
接收具有包裹的密码密钥的请求
1202
履行请求
1204
是
否
从请求提取包裹的密码密钥
1208
获得可用来解包包裹的密码密钥的密钥
1210
使用所获得的密钥来解包包裹的密码密钥
1212
使用未包裹的密码密钥来执行请求的密码操作
1214
提供对请求的响应
1216
失去对未包裹的密码密钥的访问
1218
拒绝请求
1206

图12

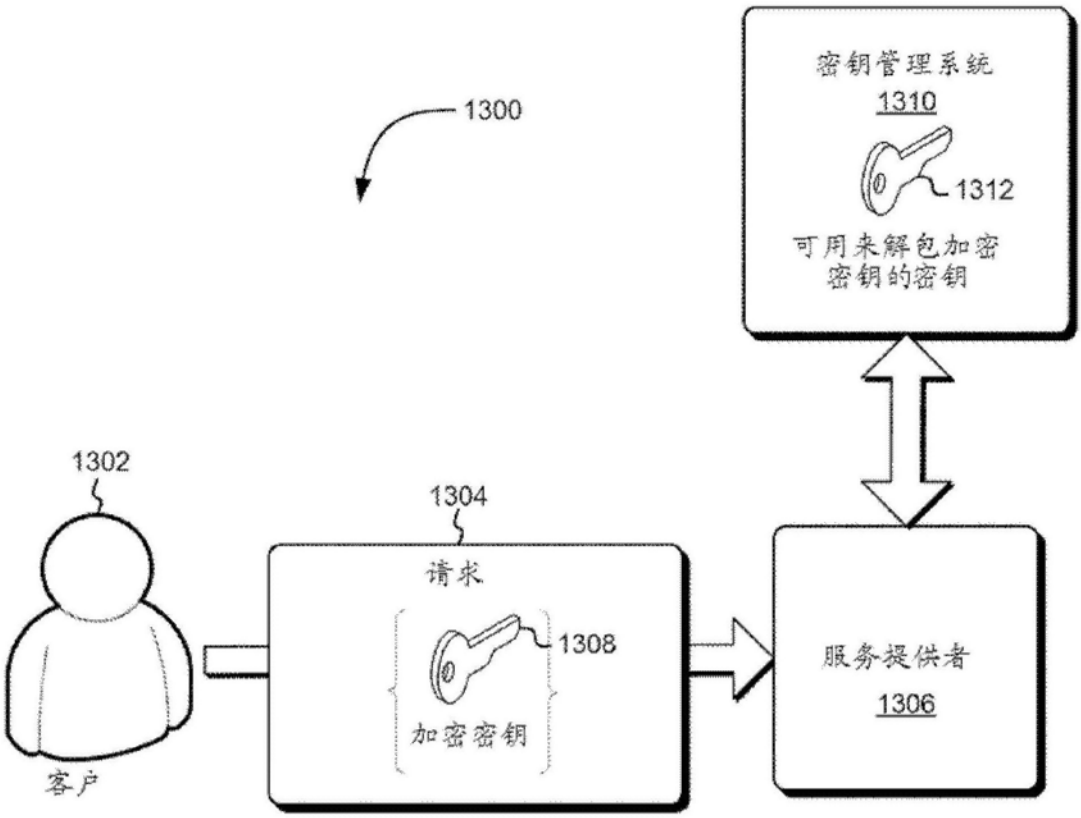

1300
密钥管理系统
1310
1312
可用来解包加密密钥的密钥
1302
1304
请求
1308
加密密钥
服务提供者
1306
客户

图13

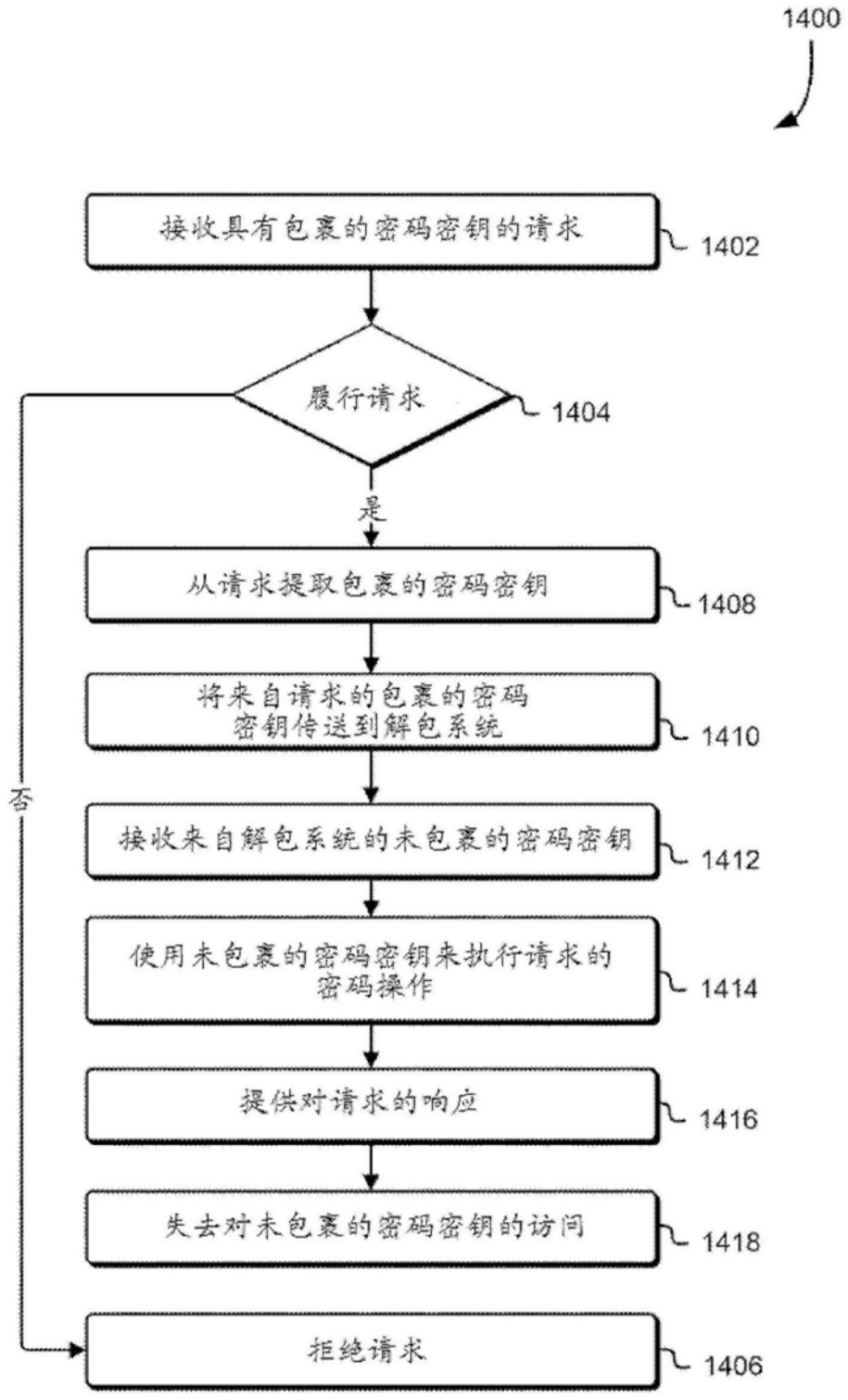

1400
接收具有包裹的密码密钥的请求
1402
履行请求
1404
是
否
从请求提取包裹的密码密钥
1408
将来自请求的包裹的密码密钥传送到解包系统
1410
接收来自解包系统的未包裹的密码密钥
1412
使用未包裹的密码密钥来执行请求的密码操作
1414
提供对请求的响应
1416
失去对未包裹的密码密钥的访问
1418
拒绝请求
1406

图14

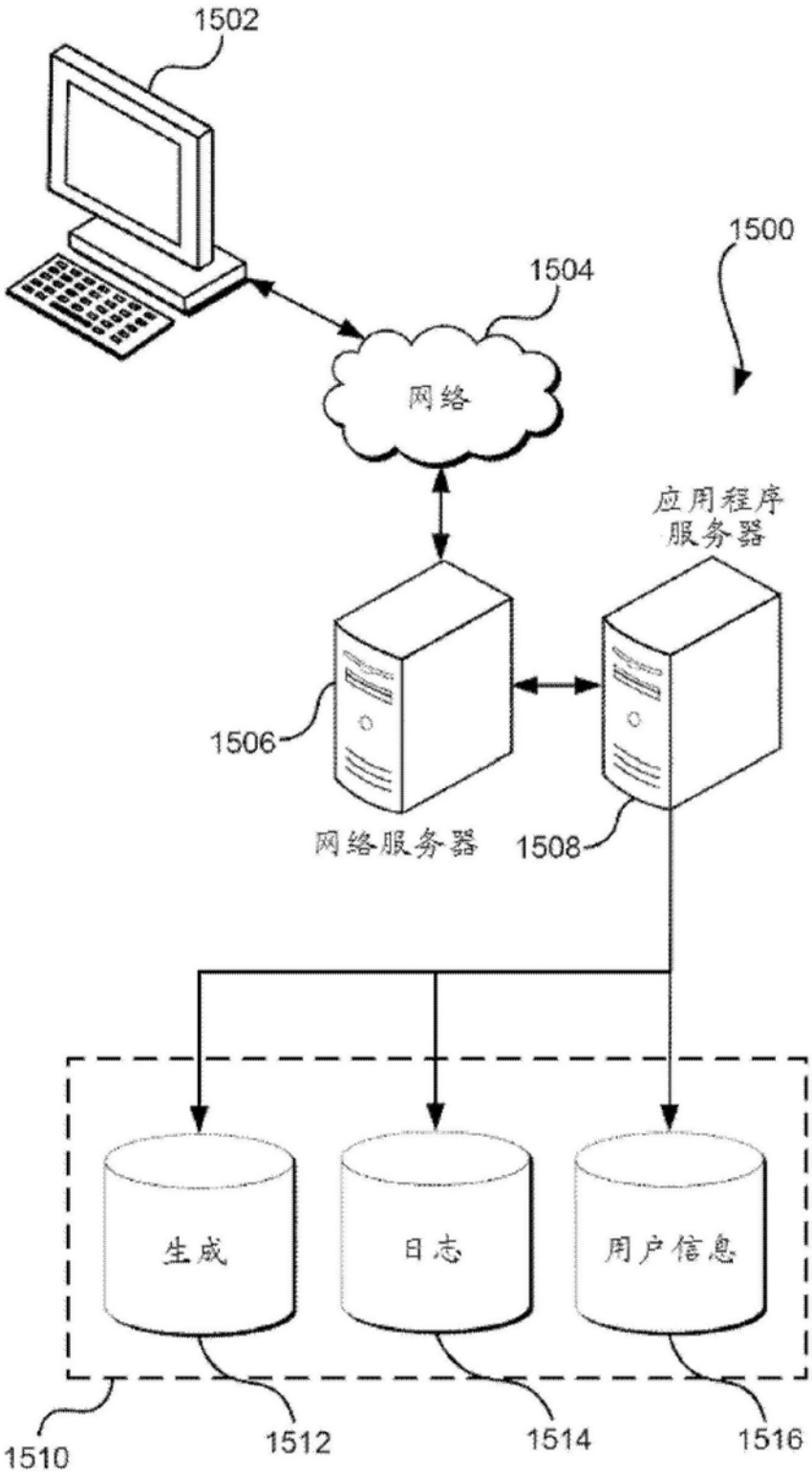

1502
1500
1504
网络
应用程序
服务器
1506
网络服务器
1508
生成
日志
用户信息
1510
1512
1514
1516

图15