(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 105103488 B
(45)授权公告日 2019.04.12

(21)申请号 201480020517.5
(22)申请日 2014.02.07
(65)同一申请的已公布的文献号
申请公布号 CN 105103488 A
(43)申请公布日 2015.11.25
(30)优先权数据
13/764,995 2013.02.12 US
(85)PCT国际申请进入国家阶段日
2015.10.09
(86)PCT国际申请的申请数据
PCT/US2014/015410 2014.02.07
(87)PCT国际申请的公布数据
WO2014/126815 EN 2014.08.21
(73)专利权人 亚马逊技术股份有限公司
地址 美国内华达州
(72)发明人 G·B·罗斯 M·J·雷恩
E·J·布兰德怀恩 B·I·普拉特
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 姬利永
(51)Int.Cl.
H04L 9/00(2006.01)
(56)对比文件
US 2008172562 A1,2008.07.17,
US 2008172562 A1,2008.07.17,
US 2008084996 A1,2008.04.10,
US 2008172562 A1,2008.07.17,
CN 102656591 A,2012.09.05,
US 2012314854 A1,2012.12.13,
US 2011154057 A1,2011.06.23,
审查员 尤一名

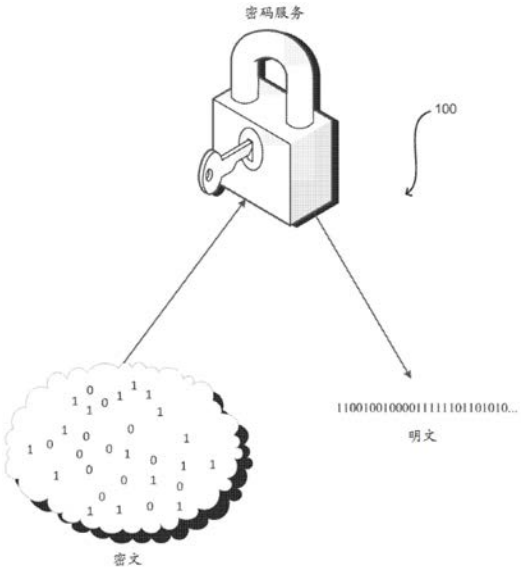
权利要求书2页 说明书38页 附图27页

(54)发明名称

借助相关联的数据的策略施行

(57)摘要

评估向计算机系统提交的请求以查看其与策略的一致性以确保数据安全。明文和相关联的数据用作密码的输入以产生密文。是否可响应于请求而提供对所述密文解密的结果是至少部分基于策略的评估而确定的,策略本身至少部分基于所述相关联的数据。其它策略包括密钥的自动旋转以防止密钥在足够的操作中被使用而允许旨在确定所述密钥的密码攻击。



CN 105103488 B

1.一种用于施行策略的计算机实施的方法,其包括:

接收对密文解密的请求,所述密文已至少部分基于明文和密钥而产生;

至少部分基于可用所述密文和所述密钥验证的数据来确定策略是否允许响应于所述请求而提供所述明文;

至少部分基于声称的相关联的数据和所述密钥来确定所述声称的相关联的数据是否是真实的;

由于确定所述策略允许提供所述明文,响应于所述请求而提供至少所述明文;以及

其中确定所述策略是否允许响应于所述请求而提供所述明文包括确定可用所述密文验证的所述数据的值与所述策略指定的值是否匹配,其中所述策略是指定对所述密钥的使用的一个或多个限制的策略。

2.如权利要求1所述的计算机实施的方法,其中:

所述密文是密码的已认证的加密模式的输出,所述输出还包括至少部分基于与所述密文相关联的所述数据的消息认证码;且

所述方法还包括至少部分基于所述消息认证码来确定声称与所述密文相关联的数据是否是真实的。

3.如权利要求1所述的计算机实施的方法,其中所述密文还至少部分基于可用所述密文和所述密钥验证的所述数据。

4.如权利要求1所述的计算机实施的方法,其中所述策略要求所述请求与和所述密文相关联的所述数据匹配以用于提供所述明文的特性是允许的。

5.如权利要求1所述的计算机实施的方法,其中可用所述密文验证的所述数据对所述策略编码,且确定所述策略是否允许提供所述明文包括从可用所述密文验证的所述数据获得所述策略。

6.如权利要求1所述的计算机实施的方法,其中所述密文对所述策略编码,且确定所述策略是否允许提供所述明文包括从所述密文获得所述策略。

7.如权利要求1所述的计算机实施的方法,其中可用所述密文验证的所述数据对一个或多个属性编码,且确定策略是否允许提供所述明文包括检查所述一个或多个属性与所述策略的属性是否匹配。

8.如权利要求1所述的计算机实施的方法,其中所述密文对一个或多个属性编码,且确定策略是否允许提供所述明文包括检查所述一个或多个属性与所述策略的属性是否匹配。

9.一种计算机系统,其包括:

一个或多个处理器;以及

存储器,其包括指令,所述指令如果由所述一个或多个处理器执行则使所述计算机系统执行以下操作:

验证与请求相关联的信息与密文兼容,所述密文已至少部分基于明文和密钥而产生;

至少部分基于与所述请求相关联的所述信息来分析所述密文和认证信息以确定策略是否允许对所述请求的特定响应;

由于确定所述策略允许所述特定响应,允许对所述请求的所述特定响应,

其中所述认证信息是至少部分基于所述明文和特定信息产生的消息认证码,所述特定信息如果与和所述请求相关联的所述信息不匹配,那么将使所述策略不允许所述特定响

应，

其中所述策略是指定对所述密钥的使用的一个或多个限制的策略。

10.如权利要求9所述的系统，其中：

所述密文是包括所述认证信息的已认证的密文；

所述认证信息包括消息认证码；且

验证与所述请求相关联的所述信息与所述密文兼容包括使用所述消息认证码来检查与所述请求相关联的所述信息的真实性。

11.如权利要求9或10所述的系统，其中与所述请求相关联的所述信息是由密码用来产生所述密文的相关联的数据。

12.如权利要求9或10所述的系统，其中：

与所述请求相关联的所述信息是至少部分基于特定信息产生的；且

所述认证信息指示所述特定信息与和所述请求相关联的所述信息是否匹配。

借助相关联的数据的策略施行

[0001] 相关申请的交叉参考

[0002] 此申请要求2013年2月12日提交的美国专利申请号13/764,995的优先权,所述专利申请的内容以引用的方式全部并入本文中。此申请为了所有目的以引用的方式并入有以下专利申请的全部公开内容:同此同时提交的标题为“AUTOMATIC KEY ROTATION”的共同待决的美国专利申请号13/764,944,同此同时申请的标题为“DATA SECURITY SERVICE”的共同待决的美国专利申请号13/764,963,同此同时申请的标题为“DATA SECURITY WITH A SECURITY MODULE”的共同待决的美国专利申请号13/765,020,同此同时申请的标题为“FEDERATED KEY MANAGEMENT”的共同待决的美国专利申请号13/765,209,同此同时申请的标题为“DELAYED DATA ACCESS”的共同待决的美国专利申请号13/765,239,同此同时申请的标题为“DATA SECURITY SERVICE”的共同待决的美国专利申请号13/765,265,以及同此同时申请的标题为“SECURE MANAGEMENT OF INFORMATION USING A SECURITY MODULE”的共同待决的美国专利申请号13/765,283。

[0003] 背景

[0004] 计算资源和相关联的数据的安全性在许多情况下具有高度重要性。作为示例,组织经常利用计算装置的网络来向其用户提供健全的服务集合。网络经常跨越多个地理边界且经常与其它网络连接。组织(举例来说)可使用计算资源的内部网络和其他人管理的计算资源两者来支持其操作。组织的计算机(举例来说)可与其它组织的计算机通信以在使用另一组织的服务时访问和/或提供数据。在许多实例中,组织使用其它组织管理的硬件来配置和操作远程网络,从而降低基本设施成本和实现其它优点。借助计算资源的此类配置,确保对资源和其持有的数据的访问是安全的可具有挑战,尤其在此类配置的大小和复杂性增长时。

[0005] 附图简述

[0006] 将参照附图描述根据本公开的各种实施方案,在附图中:

[0007] 图1示出表示根据各种实施方案的本公开的各方面的说明性图;

[0008] 图2示出可实施本公开的各方面的环境的说明性示例;

[0009] 图3示出可实施本公开的各方面的环境的说明性示例和根据至少一个实施方案的环境的各种组件中的示例信息流;

[0010] 图4示出根据至少一个实施方案的用于存储密文的说明性进程的示例步骤;

[0011] 图5示出可实施本公开的各方面的环境的说明性示例和根据至少一个实施方案的环境的各种组件中的示例信息流;

[0012] 图6示出根据至少一个实施方案的用于响应于检索数据的请求的说明性进程的示例步骤;

[0013] 图7示出可实施本公开的各方面的环境的说明性示例和根据至少一个实施方案的环境的各种组件中的示例信息流;

[0014] 图8示出根据至少一个实施方案的用于响应于存储数据的请求的说明性进程的示例步骤;

[0015] 图9示出可实施本公开的各方面的环境的说明性示例和根据至少一个实施方案的环境的各种组件中的示例信息流；

[0016] 图10示出根据至少一个实施方案的用于响应于检索数据的请求的说明性进程的示例步骤；

[0017] 图11示出可实施本公开的各方面的环境的说明性示例；

[0018] 图12示出可实施本公开的各方面的环境的说明性示例和根据至少一个实施方案的环境的各种组件中的示例信息流；

[0019] 图13示出根据至少一个实施方案的用于响应于检索数据的请求的说明性进程的示例步骤；

[0020] 图14示出根据至少一个实施方案的用于响应于对数据解密的请求的说明性进程的示例步骤；

[0021] 图15示出根据至少一个实施方案的用于获得已解密的数据的说明性进程的示例步骤；

[0022] 图16示出根据至少一个实施方案的示例密码服务的图解表示；

[0023] 图17示出根据至少一个实施方案的用于配置策略的说明性进程的示例步骤；

[0024] 图18示出根据至少一个实施方案的用于在施行策略时执行密码操作的说明性进程的示例步骤；

[0025] 图19示出根据至少一个实施方案的用于对数据加密的进程的说明性示例；

[0026] 图20示出根据至少一个实施方案的使用安全模块来对数据加密的说明性示例；

[0027] 图21示出根据至少一个实施方案的使用安全模块来对用以加密数据的密钥加密的说明性示例；

[0028] 图22示出根据至少一个实施方案的用于使用相关联的数据施行策略的进程的说明性示例；

[0029] 图23示出根据至少一个实施方案的用于使用相关联的数据和安全模块施行策略的进程的说明性示例；

[0030] 图24示出根据至少一个实施方案的针对策略的状态图的说明性示例；

[0031] 图25示出根据至少一个实施方案的针对策略的另一状态图的说明性示例；

[0032] 图26示出根据至少一个实施方案的用于自动地旋转密钥的进程的说明性示例；

[0033] 图27示出根据至少一个实施方案的用于自动地旋转密钥的进程的说明性示例；

[0034] 图28示出根据至少一个实施方案的可用以跟踪密钥使用的数据库的表示的说明性示例；以及

[0035] 图29图示可实施各种实施方案的环境。

[0036] 详细描述

[0037] 在以下说明书中，将描述各种实施方案。出于解释的目的，阐述具体配置和细节以便提供对实施方案的透彻理解。然而，对本领域技术人员还将清楚的是，可在没有具体细节的情况下实践实施方案。此外，可省略或简化众所周知的特征以便不混淆描述的实施方案。

[0038] 本文中描述和建议的技术允许涉及分布式计算资源的环境中的增强的数据安全。在一个示例中，分布式计算环境包括可通过适当的计算资源实施的一个或多个数据服务。数据服务可允许执行与数据有关的各种操作。作为一个说明性示例，分布式计算环境包括

一个或多个数据存储服务。可将电子请求传输至数据存储服务以执行数据存储操作。示例操作是使用数据存储服务存储数据和使用数据存储服务来检索由数据存储服务存储的数据的操作。包括数据存储服务的数据服务还可执行操纵数据的操作。举例来说，在一些实施方案中，数据存储服务能够对数据加密。

[0039] 本公开的各种实施方案包括分布式计算环境，分布式计算环境包括使用适当的计算资源实施的密码服务。密码服务可由分布式系统实施，分布式系统接收且响应于执行密码操作(诸如明文的加密和密文的解密)的电子请求。在一些实施方案中，密码服务管理密钥。响应于执行密码操作的请求，密码服务可执行使用所管理的密钥的密码操作。举例来说，密码服务可响应于所接收的请求而选择执行密码操作的适当密钥、执行密码操作并提供密码操作的一个或多个结果。在替代配置中，密码服务可产生包络密钥(例如，用以对具体数据项目加密的会话密钥)且将包络密钥传回至调用服务的密码操作的系统。系统接着可使用包络密钥来执行密码操作。

[0040] 在一些实施方案中，密码服务为计算资源服务提供者的多个租户管理密钥。计算资源的租户可以是作为计算资源提供者的客户操作的实体(例如，组织或个人)。客户可远程地和用编程方式配置和操作物理上由计算资源提供者托管的资源。当客户向密码服务提交执行密码操作的请求时(或当实体向密码服务提交请求时)，密码服务可为客户选择密码服务管理的密钥来执行密码操作。密码服务管理的密钥可被安全地管理，使得其它用户和/或数据服务无法访问其他人的密钥。实体(例如，用户、客户、服务)无法访问另一实体的密钥可意味着实体没有获得另一人的密钥的授权的方式，和/或实体没有使管理另一人的密钥的系统在所述实体的指令下使用密钥的授权的方式。举例来说，密码服务可管理密钥，使得对于客户来说，其它客户既无法访问所述客户的密钥，也不能使密码服务使用所述客户的密钥来执行密码操作。作为另一示例，密码服务可管理密钥，使得其它服务(诸如数据存储服务)不能使密码服务使用一些或所有密钥来执行密码操作。可通过适当的安全措施防止对密钥的未被授权的访问，使得(举例来说)未被授权的访问是困难的或不可能的。困难可因为计算的不实际性和/或因为获得访问需要未被授权的行为(例如，非法的、侵权的和/或另外禁止的，诸如授权凭证的泄露)发生。根据各种实施方案的系统可被配置来确保获得对密钥的访问的计算的不实际性的客观测量。此类测量可以是(例如)在使具有计算能力的定义单元(例如，每单位时间的某些操作)的计算机解开对密钥的授权的访问所需的已加密的信息所花的平均时间量方面测量的。

[0041] 如所指出，密码服务可接收来自各种实体(诸如计算资源提供者的客户)的请求。密码服务还可接收来自计算资源提供者内部的实体的请求。举例来说，在一些实施方案中，由计算资源提供者实施的数据服务可将请求传输至密码服务以使密码服务执行密码操作。作为一个示例，客户可将存储数据对象的请求传输至数据存储服务。请求可指示数据对象在存储时应被加密。数据存储服务可将执行密码操作的请求传达至密码服务。密码操作可以是(例如)由数据存储服务用来对数据对象加密的密钥的加密。密码操作可以是数据对象本身的加密。密码操作可以是产生数据存储服务可用来对数据对象加密的包络密钥。

[0042] 根据各种实施方案的系统实施各种安全措施以提供增强的数据安全。举例来说，在各种实施方案中，密码服务可利用其管理的密钥的方式是有限的。举例来说，在一些实施方案中，密码服务被配置来在适当授权时仅使用对应于客户的密钥。如果使用客户的密钥

的请求据称源自客户(即,来自代表客户操作的计算装置),那么密码服务可被配置来要求请求被使用所述客户拥有的适当凭证电子地(数字地)签名。如果使用客户的密钥的请求源自另一数据服务,那么密码服务可被配置来要求数据服务提供客户已向数据服务做出签名的请求的证明。在一些实施方案中,举例来说,数据服务被配置来获得和提供充当已认证的客户请求的证明的令牌。其它安全措施还可建立至包括密码服务的电子环境的配置中。举例来说,在一些实施方案中,密码服务被配置来根据上下文限制密钥使用。作为一个说明性示例,密码服务可被配置来使用密钥以用于对来自客户或来自代表客户行动的数据服务的请求加密。然而,密码服务可被配置来仅使用密钥以用于来自客户(而不是来自另一数据服务)的请求的解密。以此方式,如果数据服务泄露,那么数据服务将不能使密码服务对数据解密。

[0043] 各种安全措施可建立至密码服务和/或其电子环境中。一些安全措施可根据策略管理,所述策略在一些实施方案中是可配置的。作为一个示例,密码服务可利用使得用户能够配置关于密钥的策略的应用编程接口(API)。关于密钥的策略可以是在由密码服务处理时确定密钥是否可用于某些情形的信息。举例来说,策略可限制能够直接使用密钥的用户的身份和/或系统、限制可使用密钥时的时间、限制密钥可用以对其执行密码操作的数据和提供其它限制。策略可提供明确限制(例如,谁不能使用密钥)和/或可提供明确授权(例如,谁可以使用密钥)。另外,策略可具有复杂结构以大体上提供何时可以和不能使用密钥的条件。当接收到使用密钥执行密码操作的请求时,可访问和处理关于密钥的任何策略以确定根据策略请求是否可履行。

[0044] 本公开的各种实施方案涉及与密钥相关联的策略的施行,其中密钥可由密码服务管理。密码服务的用户(诸如托管密码服务的计算资源提供者的客户)可指定将由密码服务施行的关于密钥的策略。策略可对与谁可以指导密码服务使用密钥、密钥可用以执行的什么操作、可使用密钥的情形和/或其它密钥使用有关的限制和/或特权编码。

[0045] 在一实施方案中,与密文相关联的数据用于策略的施行。与密文相关联的数据可以是通过使用密码(诸如高级加密标准(AES)的模式)获得的数据。举例来说,对密码算法的输入可包括将被加密的明文和相关联的数据。密码算法可使用密钥来对明文加密且提供认证输出,诸如使得能够确定相关联的数据是否已更改的消息认证码(MAC)。认证输出可至少部分基于相关联的数据和明文而确定。

[0046] 策略施行可至少部分基于相关联的数据。举例来说,一些策略可要求相关联的数据在已解密的密文(即,明文)被提供之前具有特定值。认证输出(例如,MAC)可用以确保相关联的数据尚未更改,且因此策略的施行被正确地执行。相关联的数据可以是任何合适的数据,且数据本身可由策略明确地或隐含地指定。举例来说,策略可指定仅可在对密文解密的请求由具有用户识别符的用户提交时提供已解密的密文(明文),用户识别符被编码在用以对密文加密的相关联的数据中。以此方式,如果另一用户请求密文的解密(在不冒充具有用户识别符的用户的情况下),请求将因为与策略的冲突而不被履行。作为另一示例,策略可陈述仅可在密文标记有指定的信息时提供已解密的密文。作为又一示例,策略可陈述仅可在密文标记有等于明文的散列、密文的散列或其它指定的值的相关联的数据时提供已解密的密文。一般来说,本公开的实施方案允许在揭示密码算法的输出之前围绕密码算法的输入或输出的充足的策略施行。在一些实施方案中,相关联的数据本身可表示策略。

[0047] 本公开的各种实施方案还允许围绕密钥使用的策略。举例来说，在一些实施方案中，密钥自动地旋转以防止密钥被使用足够时间以实现可揭示密钥的成功的密码攻击。为了防止密钥被使用足够的时间而导致可能的安全缺口，密码服务或利用密钥的其它系统可跟踪用密钥执行的操作。当由密钥识别符(KeyID)识别的密钥用于阈值数目个操作中时，密钥可引退(例如，不可用于未来的加密操作，但可用于未来的解密操作)且用由KeyID识别的新密钥替换。以此方式，新密钥及时地产生。另外，本公开的各种实施方案以对某些实体为透明的方式执行此密钥旋转。作为一个示例，计算资源提供者的客户或其它实体可向密码服务提交使用由KeyID识别的密钥执行操作的请求。密码服务可独立于来自实体的执行密钥旋转的任何请求而执行密钥旋转。从客户或其它实体的角度来看，请求仍可使用指定的KeyID提交，而没有因为密钥已引退且用新密钥替换而必要的任何重新编程或其它重新配置。

[0048] 在一些实施方案中，支持密码或其它服务的多个系统同时访问密钥且用以履行执行密码操作的请求。举例来说，密码服务可利用安全模块的群集，其中至少一些冗余地存储一个或多个密钥。服务可将操作分配给安全模块且维持其自己的计数器。当安全模块使用其自己的分配时(例如，使用密钥执行所分配数目的操作)，服务可检查密钥是否仍可用或密钥是否应引退。应指出，安全模块(或其它计算机系统)可被配置来使用密钥执行多个类型的操作，诸如加密、解密、电子签名产生和类似物。在一些实施方案中，不是所有类型的操作都会使安全模块使用操作分配的一部分。举例来说，解密操作可不导致使用所分配的操作，而加密操作可导致使用所分配的操作。一般来说，在各种实施方案中，导致新信息(例如，密文和/或电子签名)的产生的密码操作可导致使用所分配的操作，而不导致新信息的产生的密码操作可不导致使用所分配的操作。另外，不同类型的操作可导致执行不同数目的密码操作。作为一个示例，明文的加密可至少部分基于明文的大小而在所需的密码操作的量方面变化。举例来说，使用块密码可导致针对所产生的密文的每一块使用所分配的密码操作。

[0049] 如果对于密钥可用的操作的总数仍可用，那么服务可将额外操作分配给安全模块。如果密钥应引退(例如，因为计数器如此指示)，那么服务可使冗余地存储密钥的安全模块引退密钥且用新密钥替换所述密钥，其中新密钥可由一个安全模块产生或另外获得且被安全地传递至剩余安全模块。在一些实施方案中，其它安全模块替代地用完其在较旧密钥下的所分配的操作。如果安全模块故障、变得不可操作、有意地离线(例如，用于维护)和/或另外变得不可用于执行密码操作而不提供关于其已使用一个或多个密钥执行了多少操作的信息，那么服务可将不可用性当作使用了其分配。举例来说，如果安全模块针对密钥集中的每一密钥被分配一百万个操作，且安全模块变得不可操作，那么服务可像安全模块针对密钥集中的每一者执行了一百万个操作一样操作。举例来说，服务可将额外操作分配给安全模块或另一安全模块，从而相应地调整计数器，和/或如果对应计数器指示替换是必要的话，那么可使密钥中的一者或多者引退和被替换。

[0050] 图1是示范本公开的各种实施方案的说明性图100。在一实施方案中，密码服务执行密码操作，密码操作可包括根据一个或多个密码算法的一个或多个计算的应用。如图1中所示，密码服务使用户或服务能够从密文产生明文。在示例配置中，密码服务可用以对密钥加密/解密，且这些密钥可用以对数据(诸如存储在数据存储服务中的数据)加密/解密。举

例来说，密码服务接收从在密钥下加密的密文产生明文的请求。密码服务确定请求者是授权的实体；使用主密钥对密钥解密且将现在已解密的密钥传回至服务，服务可使用已解密的密钥从密文产生明文。在另一配置中，密码服务接收密文且将所接收的密文处理为明文，明文由密码服务作为服务而提供。在此示例中，密文可作为来自授权的实体至密码服务的电子请求的部分而提供给密码服务，授权的实体可以是操作密码服务的计算资源提供者的客户和/或可以是计算资源提供者的另一服务。图1中所示的密码服务可利用一个或多个密码上的强算法来对数据加密。此类密码上的强算法可包括(例如)高级加密标准(AES)、Blowfish、数据加密标准(DES)、三重DES、Serpent或Twofish，且取决于所选择的具体实施方式，可以是非对称的或对称的密钥系统。一般来说，密码服务可利用任何加密和/或解密算法(密码)或算法的组合，其利用由密码服务管理的数据。

[0051] 如下文将更详细地论述，密码服务可用多种方式实施。在一实施方案中，密码服务由根据下文的描述配置的计算机系统实施。计算机系统本身可包括一个或多个计算机系统。举例来说，密码服务可实施为计算机系统的网络，计算机系统共同被配置来根据各种实施方案执行密码操作。或换句话说，计算机系统可以是分布式系统。在一实施方案中，密文是已使用密码算法加密的信息。在图1的示例中，密文是呈加密形式的明文。明文可以是任何信息且在名称不包括文字时，明文和密文可以是用任何合适的形式编码且不必包括文本信息但可包括文本信息的信息。举例来说，如图1中所示，明文和密文包括位的序列。明文和密文还可用其它方式表示，且通常用可借以通过计算机系统执行加密和解密的任何方式表示。

[0052] 图2示出可实施诸如图1中所示的密码服务的环境200的说明性示例。在环境200中，各种组件一起操作以便提供安全数据相关的服务。在此特定示例中，环境200包括密码服务、认证服务、数据服务前端和数据服务后端存储系统。在一实施方案中，密码服务在环境200中被配置来执行密码操作，诸如通过从数据服务前端接收明文和回过来将密文提供给或将包络密钥提供给服务，使得服务可使用包络密钥来执行加密操作。密码服务可执行诸如下文描述的额外功能，诸如用于执行密码操作(诸如将明文转换为密文和将密文解密为明文)的密钥的安全存储。密码服务还可诸如通过施行与其中存储的密钥相关联的策略来执行策略施行中涉及的操作。下文提供可由密码服务施行的示例策略。实施方案中的数据服务前端是被配置来接收和响应于来自各种用户的经由网络传输的请求的系统。请求可以是执行与存储在或将被存储在数据服务后端存储系统中的数据有关的操作的请求。在环境200中，认证服务、密码服务、数据服务前端和数据服务后端存储系统可以是计算资源提供者的系统，计算资源提供者利用系统来向由图2中所示的用户表示的客户提供服务。图2中所示的网络可以是任何合适的网络或网络的组合，包括下文论述的网络。

[0053] 实施方案中的认证服务是被配置来执行用户的认证中涉及的操作的计算机系统。举例来说，数据服务前端可将来自用户的信息提供给认证服务以回过来接收指示用户请求是否真实的信息。可用任何合适的方式执行确定用户请求是否真实且执行认证的方式可在各种实施方案中变化。举例来说，在一些实施方案中，用户电子地签名传输至数据服务前端的消息。电子签名可使用秘密信息(例如，与用户相关联的密钥对的私有密钥)而产生，秘密信息可用于认证实体(例如，用户)和认证服务两者。可将请求和用于请求的签名提供给认证服务，认证服务可使用秘密信息来计算参考签名以用于与所接收的签名进行比较来确定

请求是否真实。如果请求是真实的，那么认证服务可提供数据服务前端可用来向其它服务(诸如密码服务)证明请求是真实的信息，从而使其它服务能够相应地操作。举例来说，认证服务可提供另一服务可分析以验证请求的真实性的令牌。电子签名和/或令牌可具有以各种方式限制的有效性。举例来说，电子签名和/或令牌对于某些时间量可以是有效的。在一个示例中，电子签名和/或令牌至少部分基于将时间戳作为输入的函数(例如，基于散列的消息认证码)而产生，时间戳包括在电子签名和/或令牌中以用于验证。验证提交的电子签名和/或令牌的实体可检查所接收的时间戳是足够当前的(例如，在离当前时间的预定时间量内)且产生用于所接收的时间戳的参考签名/令牌。如果用以产生所提交的电子签名/令牌的时间戳不足够当前和/或所提交的签名/令牌与参考签名/令牌不匹配，那么认证可失败。以此方式，如果电子签名泄露，那么其将仅在短的时间量内有效，从而限制泄露导致的潜在危害。应指出，验证真实性的其它方式也视为在本公开的范围内。

[0054] 实施方案中的数据服务后端存储系统是根据通过数据服务前端接收的请求存储数据的计算机系统。如下文更详细地论述，数据服务后端存储系统可以加密形式存储数据。数据服务后端存储系统中的数据也可以未加密的形式存储。在一些实施方案中，通过数据服务前端实施的API允许请求指定是否应对将存储在数据服务后端存储系统中的数据加密。可根据各种实施方案用各种方式对被加密和存储在数据服务后端存储系统中的数据加密。举例来说，在各种实施方案中，使用密码服务可访问但环境200的一些或所有其它系统不可访问的密钥对数据加密。可通过密码服务对数据编码以用于存储在数据服务后端存储系统中，和/或在一些实施方案中，可通过另一系统(诸如，用户系统或数据服务前端的系统)使用被密码服务解密的密钥对数据加密。下文提供环境200可操作以借以对数据加密的各种方式的示例。

[0055] 环境200(和本文中描述的其它环境)的众多变化视为在本公开的范围内。举例来说，环境200可包括可与密码服务和/或认证服务通信的额外服务。举例来说，环境200可包括可用不同方式存储数据的额外数据存储服务(其可各自包括前端系统和后端系统)。举例来说，一个数据存储服务可提供对数据的主动访问，其中数据存储服务用同步方式执行数据存储服务(例如，检索数据的请求可接收对所检索的数据的同步响应)。另一数据存储服务可提供档案数据存储服务。此档案数据存储服务可利用非同步请求处理。举例来说，检索数据的请求可不接收包括所检索的数据的同步响应。而是，档案数据存储服务可要求在档案数据存储服务准备好提供所检索的数据时提交获得所检索的数据的第二请求。作为另一示例，环境200可包括计量服务，计量服务接收来自密码服务(和/或其它服务)的信息且使用那个信息来产生会计记录。会计记录可用以针对密码服务(和/或其它服务)的使用来给客户开账单。另外，来自密码服务的信息可提供费用应如何产生的指示。举例来说，在一些情况下，客户可因为使用密码服务而被提供账单。在其它情况下，使用密码服务的费用可合至其它服务(诸如利用密码服务作为其操作的部分的数据服务)的使用费用中。可用各种方式(诸如每一操作、每一时间段和/或其它方式)对使用计量并开账单。其它数据服务也可包括在环境200(或本文中描述的其它环境)中。

[0056] 另外，图2描绘用户与数据服务前端交互。应理解，用户可通过图式中未示出的用户装置(例如，计算机)与数据服务前端交互。另外，图2(和图式中其它地方)中描绘的用户还可表示非人类实体。举例来说，在计算机系统上执行的自动化进程可与如本文中描述的

数据服务前端交互。作为一个说明性示例，由图2中的用户表示的实体可以是服务器，服务器使用数据服务前端来将数据存储至数据服务后端存储系统和/或从数据服务后端存储系统检索数据以作为其操作的部分。作为又一示例，由图2中的用户表示的实体可以是作为计算资源提供者的服务提供的实体，计算资源提供者操作图2中的服务中的一者或多者。举例来说，图2中的用户可表示计算资源提供者供应的程序执行服务的虚拟或其它计算机系统。其它变化，包括下文描述的其它环境的变化也视为在本公开的范围内。

[0057] 举例来说，图3示出可实施本公开的各种实施方案的环境300的说明性示例。与图2一样，图3中的环境包括认证服务、数据服务前端系统(数据服务前端)、密码服务和数据服务后端存储系统。认证服务、数据服务前端、密码服务和数据服务后端存储系统可诸如上文结合图2所描述进行配置。举例来说，用户可通过合适的通信网络访问数据服务前端，但此网络在图式中未示出。在图3中示出的示例环境300中，提供表示信息流的箭头。在此示例中，用户将PUT请求传输至数据服务前端。PUT请求可以是将指定的数据存储在数据服务后端存储系统中的请求。响应于PUT请求，数据服务前端可确定PUT请求是否真实，即用户是否已用所请求的操作可根据系统实施的认证策略执行的方式提交请求。

[0058] 在图3中，图示了可如何进行此类认证决定的说明性示例。在此特定示例中，数据服务前端向认证服务提交认证请求。认证服务可使用认证请求来确定来自用户的PUT请求是否真实。如果请求是真实的，那么认证服务可将认证证明提供给数据服务前端。认证证明可以是可由另一服务(诸如密码服务)用来独立地确定接收到了真实请求的电子令牌或其它信息。在一个说明性示例中，PUT请求与用于PUT请求的签名一起传输。通过认证服务提供PUT请求和其签名，认证服务独立地计算签名如果真实应该是什么。如果认证服务产生的签名与用户提供的该签名匹配，那么认证服务可确定PUT请求是真实的且作为响应可提供认证证明。确定PUT请求是否真实还可包括关于策略施行的一个或多个操作。举例来说，如果签名有效但策略另外指示PUT请求不应完成(例如，请求是在策略不允许的时间期间提交的)，那么认证服务可提供指示请求不真实的信息。(然而，应指出，此策略施行可由环境300的其它组件执行。)认证服务可诸如通过使用认证服务和用户共享的密钥产生签名。如所指出，认证证明可以是另一服务(诸如密码服务)可根据其独立地验证请求真实的信息。举例来说，使用图3中所示的密码服务的示例，认证证明可至少部分基于认证服务和密码服务两者共享的密钥(诸如其它服务不可访问的密钥)而产生。

[0059] 如图3中所示，数据服务前端在接收到来自认证服务的认证证明后将明文和认证证明提供给密码服务。可根据API调用或其它电子请求而将明文和认证证明提供给密码服务(例如，加密API调用)。密码服务可分析认证证明以确定是否对明文加密。

[0060] 应指出，可将额外信息提供给密码服务。举例来说，用以对明文加密的密钥的识别符可被提供作为来自数据服务前端(其又可已接收来自用户的识别符)的API调用的输入参数。然而，应指出，识别符可不被传输至密码服务。举例来说，在各种实施方案中，可另外确定使用哪一密钥来对明文加密。举例来说，从数据服务前端传输至密码服务的信息可包括与用户相关联的信息，诸如用户的识别符和/或与用户相关联的组织，诸如已由用户代表提交PUT请求的客户的识别符。此信息可由密码服务使用以确定将被使用的默认密钥。换句话说，密钥可由可用以确定密钥的信息隐含地指定。一般来说，可用任何合适的方式执行将被使用的密钥的确定。另外，在一些实施方案中，密码服务可产生或选择密钥且提供稍后将被

使用的所产生或所选择的密钥的识别符。另一示例API参数可以是客户账户的主密钥的识别符，加密操作正被针对所述客户账户执行。

[0061] 如图3中所示，如果认证证明对于密码服务来说是充分的以使明文被加密，那么密码服务可执行一个或多个密码操作。在一实施方案中，一个或多个密码操作可包括产生将用以对明文加密的包络密钥的操作。包络密钥可以是随机产生的对称密钥或密钥对的私有密钥。在产生包络密钥之后，密码服务可用API调用中指定的主密钥对包络密钥加密且使已加密的包络密钥被持久地存储(例如，通过将已加密的密钥存储在存储服务或一些其它耐久存储装置中)或丢弃。另外，密码服务可将包络密钥的明文版本以及和已加密的包络密钥发送至数据服务前端。数据服务接着可使用包络密钥的明文版本来对明文(即，与加密请求相关联的数据)加密，且使包络密钥与用以对包络密钥加密的主密钥的识别符关联存储在持久存储装置中。另外，数据服务可丢弃包络密钥的明文版本。因而，在一实施方案中，在数据服务丢弃包络密钥的明文版本之后，其将不再能够对密文解密。

[0062] 在替代实施方案中，密码操作可涉及对明文加密。举例来说，密码服务对明文加密且将密文提供给数据服务前端存储系统。数据服务前端接着可根据其操作将密文提供给数据服务后端存储系统以用于持久存储。其它信息也可从数据服务前端传输至数据服务后端存储系统。举例来说，用以对明文加密以产生密文的密钥的识别符可与密文一起提供以用于由数据服务后端存储系统存储。还可提供其它信息，诸如识别用户和/或用户的组织的元数据。

[0063] 与本文中描述的所有环境一样，众多变化视为在本公开的范围内。举例来说，环境300的各种组件中的信息流可与所示出的信息流不同。举例来说，从一个组件通过中间组件流动至另一组件的信息(例如，从认证服务至密码服务的数据和/或从密码服务至数据服务后端存储系统的数据)可直接地和/或通过环境300的其它中间组件(其未必包括在图式中)提供给其目的地。作为另一示例，提供PUT请求(和下文的GET请求)以用于说明的目的。然而，可使用用于执行所描述的操作的任何合适的请求。

[0064] 图4示出根据实施方案的进程400的说明性示例，进程400可用以将数据存储在数据存储服务中。进程400可(例如)由图3中所示的数据服务前端执行。进程400(或本文中描述的任何其它进程，或其变化和/或组合)中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执行，且可实施为在一个或多个处理器上通过其硬件或组合共同地执行的代码(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)。代码可(例如)以计算机程序的形式存储在计算机可读存储介质上，计算机程序包括可由一个或多个处理器执行的多个指令。计算机可读存储介质可以是非暂时性的。

[0065] 如图4中说明，进程400包括接收402PUT请求。PUT请求可经由网络电子地接收且可包括与请求相关联的信息，诸如认证所需的信息，诸如PUT请求的电子签名。响应于已接收PUT请求，进程400可包括提交404认证请求。举例来说，在进程400中执行的系统可向诸如上文结合图3描述的单独的认证服务提交(例如，经由适当地配置的API调用)认证请求。类似地，执行其自己的认证的数据服务前端可向由数据服务前端实施的认证模块提交认证请求。一般来说，认证请求可根据各种实施方案用任何合适的方式提交。

[0066] 在提交认证请求后，通过认证请求提交404至的实体接收406认证响应。举例来说，参看图3，认证服务可将包括供其它服务使用的认证的证明的响应提供给数据服务前端。也

可传输其它信息，诸如认证是否成功的指示。可确定408请求是否真实。请求的真实性可取决于由实体(诸如，由认证服务，或共同地执行此类检查的实体的组合)检查的一个或多个因素。真实性可(例如)要求请求提供必要的有效凭证(例如，检查的实体共享的密钥产生的电子签名)和/或策略允许请求被履行。从提交404认证请求和接收认证响应的系统的角度来看，真实性可取决于所接收的认证响应。因此，在一实施方案中，确定408请求是否真实可至少部分基于所接收的认证响应而执行。举例来说，如果认证不真实，那么认证响应如此指示且可相应地进行确定408。类似地，响应可诸如通过不包括请求真实时将包括的信息而隐含地指示认证请求是真实的。如果确定408PUT请求不真实，那么可拒绝410PUT请求。拒绝PUT请求可用任何合适的方式执行且可取决于执行进程400的各种实施方案。举例来说，拒绝410PUT请求可包括将消息传输至提交PUT请求的用户。消息可指示请求被拒绝。拒绝请求还可包括提供关于请求为何被拒绝的信息，诸如电子签名不正确或可用于确定如何解决导致PUT请求不真实或不被授权的任何问题的其它理由。

[0067] 如果确定408PUT请求是真实的和被授权的，那么在一实施方案中，进程400包括执行412导致明文被加密的一个或多个密码操作。举例来说，可向密码服务提交提供将用于执行一个或多个密码操作的密钥的请求(例如，适当地配置的API调用)。提供给密码服务的请求可与PUT请求是真实的证明一起提供，使得密码服务可独立地确定是否执行密码操作(例如，对明文加密并提供密文或产生可用以对明文加密的包络密钥)。然而，在各种实施方案中，可不将认证证明提供给密码服务，且举例来说，密码服务可根据其接收的请求操作。举例来说，如果密码服务接收到来自数据服务前端的请求，那么密码服务可依赖于数据服务前端已独立地验证请求的认证的事实。在此实施方案和其它实施方案中，数据服务前端可借助密码服务认证其本身以提供额外安全层。密码服务可产生或另外获得密钥、对所获得的密钥加密或另外获得已加密的密钥(例如，来自存储器)且响应于请求而提供所获得的密钥和已加密的所获得的密钥。可使用至密码服务的请求中识别的密钥对所获得的密钥加密。所获得的密钥可用以对明文加密，且在对明文加密之后，可丢弃所获得的密钥(例如，不能撤回地从存储器移除)。在替代实施方案中，执行进程400的系统可产生或另外获得用以执行一个或多个密码操作的密钥、将所获得的密钥提供给密码服务以被加密。

[0068] 在一些实施方案中，执行一个或多个密码操作可导致产生密文。可存储414因为一个或多个密码操作而产生的密文以用于在稍后时间的可能检索。如上文所指出，存储密文可包括存储将在稍后时间实现密文的解密的额外信息。举例来说，密文可与用以将明文加密为密文的密钥的识别符一起存储，使得具有那个识别符的密钥可在稍后用以对密文解密以获得明文。密文的存储也可用任何合适的方式执行。举例来说，密文的存储可由诸如上文描述的数据服务后端存储系统执行。

[0069] 图5相应地示出环境500的说明性示例和说明可如何获得明文的信息流。在此示例中，环境500包括认证服务、密码服务、数据服务前端和数据服务后端存储系统。认证服务、密码服务、数据服务前端和数据服务后端存储系统可以是诸如上文描述的系统。如图5中所示，数据服务前端被配置来接收来自用户的GET请求和作为响应提供明文。为了进行此操作，数据服务前端还可被配置来向认证服务提交认证请求，认证服务本身可被配置来在适当时将认证证明提供给数据服务前端。数据服务前端还可被配置来将请求发送至密码服务以使该密码服务执行与对数据解密相关的一个或多个密码操作。在使用包络密钥的实施方

案中，数据服务可向密码服务提交请求(例如，API调用)，请求包括或指定已加密的包络密钥(或已加密的包络密钥的识别符)认证证明，和用以对至密码服务的包络密钥加密的主密钥的识别符。密码服务可确定认证证明是否充分以允许操作，且在认证证明充分时对包络密钥解密。可将已解密的包络密钥发送回至数据服务，数据服务可使用密钥来对已加密的明文解密。数据服务接着可丢弃已解密的明文密钥。

[0070] 在替代实施方案中，数据服务前端可被配置来将所接收的认证证明和密文一起提供给密码服务以供密码服务解密。密码服务可相应地被配置来确定认证证明是否充分以允许密文的解密，且在认证证明充分时使用适当的密钥(可由数据服务前端向密码服务识别)对密文解密，且将已解密的密文(明文)提供给数据服务前端。为了将密文提供给密码服务，数据服务前端可被配置来获得(例如，经由适当地配置的API调用)来自数据服务后端存储系统的密文。

[0071] 图6示出根据各种实施方案的可用以获得明文的进程600的说明性示例。进程600可(例如)由上文结合图5所示的数据服务前端系统(数据服务前端)执行，但进程600和其变化可由任何合适的系统执行。在一实施方案中，进程600包括接收602来自用户的GET请求(或其它适当的请求)。接收GET请求可诸如上文结合其它类型的请求所描述而执行。在接收602GET请求后，可向认证服务或用诸如上文描述的任何方式提交604认证请求。可相应地接收认证响应。至少部分基于所接收的认证响应，可确定608GET请求是否真实。如果确定608GET请求不真实，那么进程600可包括拒绝610请求，如上文所描述，拒绝请求可根据各种实施方案用各种方式执行。

[0072] 如果确定608GET请求是真实的，那么进程600可包括从存储装置检索密文。从存储装置检索612密文可用任何合适的方式执行。举例来说，参照上文结合图5论述的环境500，数据服务前端可向数据服务后端存储系统提交对密文的请求，且作为响应可接收密文。一般来说，可用任何合适的方式从存储装置获得密文。在接收密文后，进程600可包括执行614与对密文解密相关的一个或多个操作。举例来说，在一实施方案中，数据存储服务可将执行与对密文解密相关的一个或多个密码操作614的请求发送至密码服务。在一个示例配置中，数据服务可将API调用发送至密码服务，API调用包括已加密的包络密钥(或已加密的包络密钥的识别符)认证证明，和用以对至密码服务的包络密钥加密的主密钥的识别符。密码服务可确定认证证明是否充分以允许操作，且在认证证明充分时对包络密钥解密。可将已解密的包络密钥发送回至数据服务，数据服务可使用密钥来对已加密的明文解密。

[0073] 在另一配置中，可将密文提供给密码服务，诸如上文结合图5描述的密码服务。也可将其它信息提供给密码服务，诸如可由密码服务用来确定是否对密文解密的认证的证明。另外，在一些实施方案中，可将由密码服务用来对密文解密的密钥的识别符提供给密码服务。然而，在其它实施方案中，可向密码服务隐含地指示密钥。举例来说，密码服务可使用向密码服务指示的与客户相关联的默认密钥。一般来说，可使用密码服务可借以确定使用哪一密钥来对密文解密的任何方式。

[0074] 如图6中所示，在对密文解密之后，进程600可包括提供616对GET请求的响应。提供对GET请求的响应可根据各种实施方案用各种方式执行。举例来说，提供对GET请求的响应可包括提供明文。在其它实施方案中，明文可以是用以对其它已加密的信息解密的密钥，其它已加密的信息则是响应于GET请求而提供的。一般来说，取决于在本公开的特定实施方案

中的明文的作用，提供对GET请求的响应可用各种方式执行。

[0075] 如所指出，本公开的各种实施方案允许数据由数据存储服务用各种方式存储。图7示出根据此实施方案的环境700的说明性示例，其中箭头指示信息流。如图7中所示，环境700包括诸如上文描述的认证服务、密码服务、数据服务前端和数据服务后端存储系统。在此特定示例中，数据服务前端是被配置来接收来自各种用户的PUT请求的计算机系统。PUT请求可包括或指定将由数据服务后端存储系统存储的数据对象。PUT请求还可指定将用以对数据对象加密的密钥的密钥识别符。数据服务前端还可被配置来与诸如上文描述的认证服务交互，以便向密码服务提供认证证明，密码服务可操作以接收密钥和密钥识别符且作为响应提供由密钥识别符识别的密钥加密的密钥。数据服务前端接着可导致存储在数据服务后端存储系统中。可被存储的数据可包括由密钥加密的数据对象。可被存储的数据还可包括由密钥识别符识别的密钥加密的密钥。如本文中其它地方论述，已加密的数据对象和已加密的密钥可存储在不同服务中。

[0076] 如图7中所示，数据服务前端被配置来将已加密的信息提供给数据服务后端存储系统以用于存储。在此示例中，数据服务前端被配置来提供在密钥下加密的数据对象和在具有KeyID的另一密钥下加密的密钥。应指出，出于说明的目的，花括号符号用以表示加密。明确地说，花括号内的信息是在下标中指定的密钥下加密的信息。举例来说，$\{Data\ Object\}_{Key}$表示数据“Data Object”是在密钥“Key”下加密的。应指出，密钥识别符也可出现在使用此花括号符号的下标中。当密钥识别符出现在下标中时，花括号内的信息在由密钥识别符识别的密钥下加密。举例来说，$\{Data\ Object\}_{KeyID}$表示数据对象“Data Object”是在由密钥识别符“KeyID”识别的密钥下加密的。类似地，$\{Key\}_{KeyID}$表示密钥“Key”是在由密钥识别符“KeyID”识别的密钥下加密的。换句话说，本公开在下标中使用密钥和密钥识别符两者且下标的含义根据上下文应为清楚的。密文可包括可用以确定相关联的解密密钥的身份的额外元数据。

[0077] 图8示出可执行以将数据对象存储在数据存储系统(诸如上文结合图7描述的数据服务后端存储系统)中的进程800的说明性示例。进程800可由任何合适的系统(诸如由上文结合图7描述的数据服务前端系统)执行。在一实施方案中，进程800包括接收802对数据对象的PUT请求。接收对数据对象的PUT请求可用诸如上文描述的任何合适的方式执行。应指出，数据对象可结合请求接收或可从另一服务接收。举例来说，请求可包括数据对象的识别符，数据对象可使用识别符从另一服务获得。与上文描述的其它进程一样，在一实施方案中，进程800包括提交804认证请求和接收806认证响应。接收806的认证响应可用以确定808PUT请求是否为真实的请求。如果确定808PUT请求不真实，那么进程800可包括拒绝810诸如上文描述的请求。如果确定808PUT请求是真实的，那么进程800可包括获得812密钥识别符(KeyID)，诸如用以对包络密钥加密的主密钥的keyID。获得812KeyID可用任何合适的方式执行且获得KeyID的方式可根据各种实施方案而变化。举例来说，如图7中所示，PUT请求可指定KeyID。作为另一示例，用户或另外与用户相关联的身份可用以获得识别符或默认密钥。作为另一示例，密文可提供相关联的密钥ID的指示。作为又一示例，一个或多个策略确定可用以确定获得哪一密钥识别符。

[0078] 在一实施方案中，进程800还包括产生814密钥，诸如包络密钥。产生密钥可由(例如)密码服务或请求来自密码服务的密码操作的服务(例如，数据存储服务)用任何合适的

方式执行。举例来说，密钥可使用密钥导出函数使用至密钥导出函数的适当输入而产生。示例密钥导出函数包括IEEE Std 1363 2000中定义的KDF1、ANSI X9.42中定义的密钥导出函数和基于HMAC的密钥导出函数，诸如RFC 5869中指定的基于HMAC的提取与扩展密钥导出函数(HKDF)。作为另一示例，密钥可由随机或伪随机数产生器、硬件熵源或诸如国家标准与技术研究院特别刊物(NIST SP)800-90A指定的确定性随机位产生器产生。应指出，尽管图8示出进程800包括产生814密钥，但密钥可用其它方式(诸如通过从存储装置检索)获得。换句话说，密钥可能已预先产生。

[0079] 继续图8中说明的进程800，在一实施方案中，进程800包括使用816所产生的密钥来对数据对象加密。举例来说，在密码服务产生密钥的实施方案中，密码服务可将密钥、KeyID和密钥的已加密副本提供给数据服务。举例来说，参看图7，数据服务前端可从密码服务接收包络密钥和用以对包络密钥加密的主密钥的KeyID以及任何其它相关信息，诸如认证证明。加密密钥的明文副本接着可用以对数据对象加密。可丢弃加密密钥的明文副本且接着可存储818已加密的数据对象以及已加密的密钥。举例来说，参看图7，数据服务前端可将已加密的数据对象和已加密的密钥传输至数据服务后端存储系统以用于存储。在服务产生密钥的配置中，服务可将密钥和KeyID提供给密码服务。举例来说，数据服务前端可将包络密钥和用以对包络密钥加密的主密钥的KeyID以及任何其它相关信息(诸如认证证明)发送至密码服务。加密密钥的明文副本接着可用以对数据对象加密。服务可丢弃加密密钥的明文副本且接着可存储已加密的数据对象以及已加密的密钥。举例来说，参看图7，数据服务前端可将已加密的数据对象和已加密的密钥传输至数据服务后端存储系统以用于存储。

[0080] 可在没有密钥的明文版本的情况下存储已加密的数据对象和已加密的包络密钥，即，数据服务后端存储系统和一个或多个其它系统不可访问明文密钥。可用任何合适的方式使数据对象被加密的密钥(例如，主密钥)不可访问。在一些实施方案中，此通过将密钥存储在仅密码服务可访问的存储器中而实现。在一些其它实施方案中，此可通过将主密钥存储在硬件或其它安全模块中或另外在硬件或其它安全模块的保护下而实现。在一些实施方案中，存储明文包络密钥的存储器位置(例如，数据服务的存储器)可被允许被重写或存储密钥的存储器位置可被有意地重写以将密钥呈现为对数据服务前端不可访问。作为另一示例，明文包络密钥可维持在最终停止存储密钥的易失性存储器中。以此方式，包络密钥仅在其使用由KeyID识别的密钥解密或另外用未被授权的方式获得时(诸如通过在没有KeyID识别的密钥的情况下解开密钥，这在计算上可能不实际)可访问。换句话说，需要由KeyID识别的密钥以获得对在其下对数据对象加密的密钥的授权的访问。因此，如果图7的数据服务后端存储系统泄露，那么此泄露将不提供对未加密的数据对象的访问，因为对数据对象解密将需要访问密钥，密钥仅可通过使用由KeyID识别的密钥解密或通过计算上不可行的其它方式获得。

[0081] 如所指出，本公开的各种实施方案允许用户用安全的方式存储数据对象并检索数据对象。图9相应地示出可用以从存储装置获得数据对象的环境900的说明性示例。如图9中所示，环境900包括认证服务、密码服务、数据服务前端系统和数据服务后端存储系统。认证服务、密码服务、数据服务前端和数据服务后端存储系统可以是诸如上文描述的计算机系统。如图9中所示，数据服务前端系统被配置来接收数据对象请求且作为响应提供数据对象。为了作为响应提供数据对象，在此实施方案中数据存储前端系统被配置来与如图9中所

示的认证服务、密码服务和数据服务后端存储系统交互。举例来说，在各种实施方案中，数据服务前端系统被配置来向认证服务提交认证请求且响应于所述请求接收认证证明。作为另一示例，数据服务前端被配置来将由KeyID识别的密钥加密的密钥和认证证明提供给密码服务，密码服务可操作以至少部分基于认证证明确定是否提供密钥和如果确定提供密钥则将密钥提供给数据服务前端。数据服务前端还可被配置来将其它信息(诸如KeyID)提供给密码服务。但在一些实施方案中，可向密码服务隐含地指示KeyID，诸如通过与提供给密码服务的其它信息的关联。还应指出，在一些实施方案中，用户结合向数据服务前端提交请求而将KeyID提供给数据服务前端。而且，如图9中所示，在一实施方案中，数据服务前端被配置来向数据服务后端存储系统请求数据对象且作为响应接收由密钥加密的数据对象和由KeyID识别的密钥加密的密钥。在一些实施方案中，密码服务可操作以拒绝执行不是使用与指定的KeyID相关联的密钥产生的密文的解密。

[0082] 在一实施方案中，数据服务前端被配置来使用从密码服务接收的密钥来对数据对象解密且向用户提供已解密的数据对象。图10相应地示出根据各种实施方案的可用以提供已解密的对象的进程1000的说明性示例。进程1000可由任何合适的系统(诸如结合图9描述的数据服务前端系统)执行。在一实施方案中，进程1000包括接收1002对数据对象的GET请求。接收对数据对象的GET请求可用诸如上文结合其它类型的请求描述的任何合适的方式执行。举例来说，对数据对象的GET请求可包括用以认证请求的信息和/或其它信息。与本文中描述的其它进程一样，在一实施方案中，进程1000相应地包括向认证系统提交1004认证请求和接收1006认证响应。提交认证请求和接收认证响应可用诸如上文描述的任何合适的方式执行。认证响应可用以确定1008GET请求是否真实。如果确定1008GET请求不真实，那么在一实施方案中进程1000包括拒绝1010请求。然而，如果确定1008GET请求是真实的，那么在一实施方案中进程1000包括从存储装置检索1012已加密的数据对象和已加密的密钥。举例来说，数据服务前端系统可从上文结合图9所示的数据服务后端存储系统获得已加密的数据对象和已加密的密钥。

[0083] 在一实施方案中，进程1000包括将已加密的包络密钥提供1014给密码服务。将已加密的包络密钥提供1014给密码服务可用任何合适的方式执行，且可与其它信息(诸如使密码服务能够确定是否对已加密的密钥解密的认证证明)一起提供。另外，将已加密的包络密钥提供1014给密码服务可包括提供已加密包络密钥的授权的解密所需的密钥的识别符以使密码服务能够从由密码服务管理的多个密钥中选择由识别符识别的密钥。然而，如上文所指出，密钥可被隐含地识别。密码服务可相应地选择适当的密钥且对已加密的密钥解密。因此，在一实施方案中，进程1000包括从密码服务接收1016已解密的包络密钥。举例来说，如果密码服务确定认证证明是有效的和/或已加密的解密根据任何适用策略是允许的，那么密码服务可将已解密的密钥提供给试图对数据对象解密的系统。接着可使用已解密的包络密钥对数据对象解密1018。接着可向请求者(诸如提交GET请求的用户或其它系统)提供1020已解密的数据对象。

[0084] 在许多情况下，用户(即，一般来说是利用密码服务的装置)需要与密码服务直接交互。图11相应地示出允许对密码服务的直接用户访问的环境1100的说明性示例。在环境1100中包括认证服务、数据服务前端和数据服务后端存储系统。认证服务、数据服务前端和数据服务后端存储系统可如上文所描述。举例来说，数据服务前端可被配置来接收并响应

于经由合适的网络来自如图11中所示的用户的请求。作为响应经由网络来自用户的请求的部分，数据服务前端还可被配置来与认证服务交互，以便确定用户请求是否真实和/或施行关于请求的策略。数据服务前端还可被配置来与数据服务后端存储系统交互以作为履行用户请求的部分。用户请求可包括(例如)将数据存储在后端存储系统中的PUT请求和从数据服务后端存储系统检索数据的GET请求。如上文，还可根据各种实施方案使用其它请求，诸如删除存储在数据服务后端存储系统中的数据的请求，更新存储在数据服务后端存储系统中的数据的请求和类似物。

[0085] 在图11的特定示例中，在环境1100中，密码服务包括密码服务前端和数据服务后端。与数据服务前端一样，密码服务前端被配置来接收和响应经由网络来自用户的请求。密码服务前端还被配置来与认证服务交互以确定用户请求是否真实。确定用户请求是否真实可用诸如上文描述的简单方式执行。应指出，尽管密码服务前端和数据服务前端与相同认证服务交互，但密码服务前端和数据服务前端可与不同的认证服务交互。另外，密码服务前端可被配置来在响应于用户请求时施行策略。

[0086] 在一实施方案中，密码服务前端被配置来与密码服务后端交互。密码服务后端根据从密码服务前端接收的指令配置以执行密码操作。密码操作包括加密、解密和散列计算以及其它。环境1100可(例如)由用户使用以使明文被密码服务加密，使得已加密的数据可存储在数据服务后端存储系统中。下文提供环境1100的此使用的示例。另外，下文还提供示例密码服务的示例细节。

[0087] 数据可用诸如上文描述的任何合适的方式存储在数据服务后端存储系统中。举例来说，可在环境1100中使用用于将已加密的数据存储在上文描述的后端存储系统中的技术。举例来说，尽管未示出，但数据服务前端可与密码服务前端通信以使密码服务后端对数据加密，所述数据接着可存储在数据服务后端存储系统中。已加密的数据可以是数据对象和/或用以对数据对象加密的已加密的密钥。在环境1100中，也可用其它方式将数据放置到数据服务后端存储系统中。举例来说，用户可提供将由密码服务加密的明文且作为响应可接收密文。用户接着可与数据服务前端交互或可向数据服务前端提交请求以请求将密文存储在数据服务后端存储系统中。在此示例中，数据服务前端可用任何方式存储密文。举例来说，数据服务前端和后端存储系统可被配置为不关心数据是否被加密。

[0088] 另外，与本文中所示的所有环境一样，额外前端系统可在逻辑上位于用户与数据服务前端和密码服务前端以及可能的其它前端系统之间，以便协调系统之间的动作。举例来说，在一些实施方案中，用户可与前端系统交互，前端系统本身与密码服务前端和数据服务前端交互使得从用户的角度来看操作较简单。举例来说，用户可请求对数据对象加密和存储数据对象，且前端系统通过与密码服务前端和数据服务前端的适当交互来响应所述请求。然而，从用户的角度来看，这可由单一请求执行。其它变化也在本公开的范围内。

[0089] 图12示出可用以实施本公开的各种实施方案的环境1200的说明性示例。在图12中，环境1200被配置来使用户能够将密文存储在数据服务后端存储系统中。如图12中所示，相应地，环境1200包括数据服务前端、数据服务后端存储系统、认证服务、密码服务前端和密码服务后端。数据服务后端存储系统、数据服务前端、认证服务、密码服务前端和密码服务后端可以是诸如上文结合图11描述的系统。举例来说，如图12中所示，数据服务前端被配置来接收并响应用户请求，且还可被配置来施行关于用户请求的策略。作为响应请求的部

分，数据服务前端可被配置来向认证服务提交认证请求且作为响应作为响应接收认证证明。在成功认证后，数据服务前端还可被配置来与数据服务后端存储系统交互以从数据服务后端存储系统获得已加密的数据对象和可能未加密的数据对象，接着可向用户提供已加密的数据对象和可能未加密的数据对象。

[0090] 如图12中所示，密码服务前端还被配置来向认证服务提交认证请求且作为响应接收认证证明。认证证明可用以从密码服务后端获得服务。举例来说，密码服务前端可被配置来将密文与认证证明一起提供给密码服务后端，且密码服务后端可被配置来对密文解密且回过来提供密文。如图12中所示，密文可以是已加密的密钥且密码服务后端可对已加密的密钥解密且将已解密的密钥(即明文密钥)提供给密码服务前端，密码服务前端还被配置来向用户提供明文密钥。用户接着可使用密钥来对从数据服务前端接收的已加密的数据对象解密或对存储在用户的域内(例如，用户操作或控制的数据中心或计算机系统内)的已加密的数据对象解密。在此示例中，用户可能已从数据服务前端获得已加密的密钥。举例来说，用户可能已向数据服务前端提交对数据对象和/或用以对数据对象加密的密钥的请求。尽管在图11中示出为单一请求，但可进行对数据对象和密钥两者的单独请求。如图11中所示，数据服务前端可从数据服务后端存储系统获得已加密的数据对象和已加密的密钥，且向用户提供已加密的数据对象和已加密的密钥。

[0091] 应指出，与本文中所示的所有环境一样，变化被视为在本公开的范围内。举例来说，图12示出向用户提供在密钥下加密的数据对象和由密钥识别符识别的另一密钥加密的密钥。还可使用进一步加密等级。举例来说，数据对象可在仅用户可访问(和/或环境1200的其它组件不可访问)的密钥下加密。用以对数据对象加密的密钥也可在仅用户可访问的密钥下加密。在此示例中，对环境1200的组件的未被授权的访问(用户不存在)仍不提供对数据对象的未加密的内容的访问，这是因为对于授权的解密仍需要对用户的密钥的访问。

[0092] 作为另一示例，在图12中所示的环境1200中，数据服务前端和数据服务后端存储系统无法访问由数据服务后端存储系统存储的明文数据，这是因为数据服务前端和数据服务后端存储系统无法访问对已加密的数据解密所需的密钥。然而，在一些实施方案中，可准予数据服务前端和/或数据服务后端存储系统访问。举例来说，在一实施方案中，可向数据服务前端提供对密钥的临时访问以使数据服务前端能够获得已加密的数据、对已加密的数据解密、使用已解密的数据以用于特定目的(例如，编索引)且接着删除或另外失去对已解密的数据的访问。此类动作可由数据服务前端和/或密码服务施行的策略支配，且可需要来自用户的授权。

[0093] 图13示出可用以(诸如)从诸如上文描述的数据服务后端存储系统获得已加密的数据对象和已加密的密钥的进程1300的说明性示例。进程1300(例如)可由上文结合图12描述的数据服务前端系统执行。在一实施方案中，进程1300包括接收1302对已加密的数据对象的GET请求。接收GET请求可用任何合适的方式执行，诸如通过经由到数据服务前端系统的API调用接收请求。由于已接收GET请求，进程1300可包括提交1304认证请求和接收1306认证响应。提交1304认证请求和接收1306认证响应可用诸如上文描述的任何合适的方式执行。认证响应可用以确定1308GET请求是否真实。如果确定1308GET请求不真实，那么进程1300可包括拒绝1310GET请求。拒绝1310GET请求可用诸如上文描述的任何合适的方式执行。然而，如果确定1308GET请求是真实的，那么进程1300可包括提供1312已加密的数据对

象与已加密的密钥，已加密的密钥在解密时可用以对已加密的数据对象解密。应指出，与本文中描述的所有进程一样，众多变化被视为在本公开的范围内。举例来说，进程1300可被配置来在GET请求真实时通过提供已加密的数据对象但不提供已加密的密钥来响应于GET请求。请求者(即提交GET请求的用户或系统)可用其它方式获得已加密的密钥。举例来说，在一些实施方案中，用户可将已加密的密钥本身存储在处于用户的控制下的数据存储系统中。作为另一示例，一个存储服务可存储已加密的数据对象且另一服务可存储已加密的密钥，且用户可从相应服务获得已加密的数据对象和已加密的密钥。作为另一示例，另一服务或用户的第三方可用以存储已加密的密钥且用户可在请求时获得已加密的密钥。一般来说，可使用可提供已加密的密钥的任何方式。

[0094] 如图13中所示，进程1300可导致实体已被提供数据对象和可用以对数据对象解密的已加密的密钥。在各种实施方案中，已加密的密钥必须被解密以便对数据对象解密。图14相应地示出进程1400的说明性示例，进程1400可用以将已解密的密钥提供给实体，实体需要此已解密的密钥以便使用已解密的密钥来用于已加密的数据对象的解密。进程1400可由任何合适的系统(诸如由上文结合图12描述的密码服务前端系统)执行。在一实施方案中，进程1400包括接收1402解密以使用具有指定的KeyID的另一密钥对密钥解密。尽管进程1400是结合密钥的解密描述的，但应指出，进程1400大体上可适合于数据的解密。解密请求可用诸如上文描述的任何合适的方式(例如，经由适当地配置的API调用)接收1402。另外，解密请求可由适于进程1400正被执行的环境的任何实体接收。举例来说，解密请求可源自用户或源自另一系统，诸如上文论述的数据服务前端。解密请求还可包括将被解密的数据(例如，密钥)或对其的参考。KeyID也可用任何合适的方式指定。举例来说，在一些实施方案中，解密请求包括KeyID或对KeyID的参考，即，可用以确定KeyID的信息。如上文所论述，KeyID也可被隐含地指定。举例来说，KeyID可通过与可用数据(诸如提交解密请求的请求者的身份)的关联而获得。举例来说，对应于KeyID的密钥可以是用于请求者或用于被代表提出请求的实体的默认密钥。

[0095] 在一实施方案中，进程1400包括提交1404认证请求和接收1406认证响应。提交1404认证请求和接收1406认证响应可用诸如上文描述的任何合适的方式执行。另外，如上文所描述，所接收的认证响应可用以确定1408GET请求是否真实。如果确定1408GET请求不真实，那么进程1400可包括拒绝1410GET请求。拒绝1410GET请求可用诸如上文描述的任何合适的方式执行。然而，如果确定1408GET请求是真实的，那么进程1400可包括访问用于指定的KeyID和/或用于请求者的策略信息。策略信息可包括其中包括关于KeyID和/或请求者的一个或多个策略的信息。

[0096] 在一实施方案中，所访问的策略信息用以确定1414任何适用策略是否允许具有指定的KeyID的密钥的解密。如果确定1414策略不允许KeyID指定的密钥的解密，那么进程1400可包括拒绝1410诸如上文描述的GET请求。然而，如果确定1414策略允许具有指定的KeyID的密钥的解密，那么进程1400可包括使用KeyID识别的密钥对密钥解密1416。一旦密钥已使用具有KeyID的密钥解密，那么接着可诸如通过经由网络的传输向提交解密请求的请求者(或，在一些实施方案中，另一授权的目的地)提供1418已解密的密钥。

[0097] 如上文论述的环境1200中所示，用户可用各种方式获得已加密的数据对象和用于对数据对象解密的密钥。图15示出根据各种实施方案的可用以获得明文的进程1500的说明

性示例。进程1500可由任何合适的系统(诸如由诸如结合图12描述的用户操作和/或托管的系统)执行。其它合适的系统包括代表用户且未必根据所提供的实时用户输入但可能根据预编程进程操作的系统。

[0098] 在一实施方案中,进程1500包括从数据存储服务接收1502密文。向数据存储服务请求1502密文可用诸如上文描述的任何合适的方式执行。举例来说,执行进程1500的系统可使用上文结合图12所示的环境1200中的适当地配置的API调用和/或通过上文结合图13描述的进程1300请求1502密文。

[0099] 进程1500还可包括接收密文和已加密的密钥。接收密文和已加密的密钥可用任何合适的方式执行。举例来说,可响应于对来自数据存储服务的密文的请求而接收密文和已加密的密钥。然而,一般来说,密文和已加密的密钥可用其它合适的方式接收1504。举例来说,从数据存储服务接收密文的请求可以是非同步请求且密文可按照随后提交的另一请求接收1504。另外,密文和已加密的密钥可在单一响应中提供或可诸如通过不同响应(其可来自相同的或来自不同的系统)单独地获得。作为另一示例,执行进程1500的系统可在本地或另外存储已加密的密钥且已加密的密钥可从本地存储器接收。

[0100] 在一实施方案中,进程1500包括请求使用具有指定的KeyID的密钥对已加密的密钥解密。KeyID可用诸如上文描述的任何合适的方式指定。另外,应指出,执行进程1500的系统可能够用任何合适的方式指定KeyID。举例来说,已加密的密钥和/或与其一起提供的信息可指定KeyID。作为另一示例,执行进程1500的系统可在本地或远程地访问使得能够确定KeyID的信息。举例来说,本地或远程数据库可使数据对象识别符与用以对数据对象加密的密钥的密钥识别符相关联。一般来说,可使用可使系统能够指定KeyID的任何方式。另外,在一些实施方案中,诸如当提供给密码服务的信息足以确定KeyID时,无需指定KeyID。对已加密的密钥的解密的请求1506可用任何合适的方式(诸如结合上文结合图12论述的环境和/或通过执行上文结合图14描述的进程1400)执行。

[0101] 在一实施方案中,进程1500包括接收1508已解密的密钥。接收1508已解密的密钥可用任何合适的方式执行。举例来说,可响应于对已加密的密钥的解密的请求而接收已解密的密钥。作为另一示例,对已加密的密钥的解密的请求可以是非同步请求且可已提交用于接收已解密的密钥的另一请求。一般来说,已解密的密钥可用任何合适的方式接收。另外,与从一个装置流动至另一装置的所有信息一样,信息的传递可使用安全信道执行。举例来说,已解密的密钥可再次被加密以用于由接收已解密的密钥的实体解密。一般来说,任何安全通信方式可用以将信息从一个实体传递至另一实体。

[0102] 一旦已接收1508已解密的密钥,进程1500可包括使用1510已解密的密钥来对密文解密1510且因此获得明文。应指出,与本文中描述的所有进程一样,变化被视为在本公开的范围内。举例来说,进程1500示出按顺序执行对密文的请求和对已加密的密钥的解密的请求。然而,与本文中结合各种进程描述的许多操作一样,在各种实施方案中操作无需按顺序执行。举例来说,如果执行进程1500的系统在请求密文之前访问已加密的密钥,或另外能够如此操作,那么系统可并行地或按与所示的次序不同的次序请求密文和请求已加密的密钥的解密。其它变化也被视为在本公开的范围内。

[0103] 如上文所论述,本公开的各种实施方案涉及提供密码服务。密码服务可由诸如上文描述的密码服务系统提供。图16相应地示出根据各种实施方案的密码服务1600的说明性

示例。如图16中所示且如上文所论述，密码服务1600逻辑上包括前端系统和后端系统。前端系统和后端系统两者可由被配置来执行本文中描述的操作的一个或多个计算机系统实施。举例来说，如图16中所示，密码服务1600的前端系统实施请求API和策略配置API。在一实施方案中，请求API是被配置用于请求通过密码服务执行的密码和其它操作的API。因此，可经由请求API向前端系统做出请求以便使此类密码操作将由密码服务执行。

[0104] 请求API可配置有以下示例高级可用的请求：

[0105] CreateKey(KeyID)

[0106] Encrypt(KeyID,Data,[AAD])

[0107] Decrypt(KeyID,Ciphertext,[AAD])

[0108] Shred(KeyID)

[0109] ReKey(Ciphertext,OldKeyID,NewKeyID).

[0110] 在一实施方案中，CreateKey(KeyID)请求使密码服务创建由在请求中识别的KeyID识别的密钥。在接收请求后，密码服务可产生密钥且使密钥与KeyID相关联。应知道，KeyID可以是但未必是唯一识别符。举例来说，KeyID可识别密钥族。举例来说，在一些实施方案中，执行密钥旋转。密钥旋转可涉及将密钥用其它密钥替换以防止收集足够的已解密的数据以允许实际解开所使用的密码。如果在不同于密码服务的实体的指令下执行，那么使用CreateKey(KeyID)请求可使密码服务创建新密钥来替换由KeyID识别的旧密钥。旧密钥可保持被KeyID识别，但可(例如)仅用于(已使用旧密钥加密的数据的)解密且不用于未来加密。作为另一示例，在一些实施方案中，密码服务的用户提供其自己的密钥识别符，且存在两个不同的客户可能提供相同识别符的可能性。在此类情况下，识别符可不唯一地识别密钥或甚至唯一地识别密钥族。各种措施可适当地解决此问题。举例来说，与密码服务的用户相关联的身份或其它信息可用以识别恰当的密钥或密钥族。在又其它实施方案中，密码服务可随机地、按顺序或使用任何其它方法指派KeyID。

[0111] 应指出，当KeyID不唯一地识别密钥时，各种系统可适当地实现恰当的功能性。举例来说，在各种实施方案中，由KeyID识别的密钥族是有限的。如果请求使用由KeyID识别的密钥的解密操作，那么额外数据(例如，在执行加密时的时间戳)可使得能够确定将要使用的恰当的密钥。在一些实施方案中，密文可包括指示密钥版本的信息。在一些实施方案中，所有可能的密钥用以提供数据的不同解密。因为存在有限数目个密钥，所以恰当的解密可从提供的解密中选择。在一些实施方案中，用一种方式执行借助密钥的解密，所述方式使密码服务能够检测密文不是至少部分基于所述密钥(诸如通过使用认证的加密)而产生的。其它变化也被视为在本公开的范围内。

[0112] Encrypt(KeyID,Data,[AAD])请求可用以使密码服务使用KeyID识别的密钥对指定的数据加密。额外的认证的数据(AAD)可用于各种目的且可以是未必被加密但(例如)由电子签名、消息认证码或一般来说与AAD一起包括的带密钥的散列值认证的数据。在一些实施方案中，产生包括AAD的至少一部分的密文。在一些其它实施方案中，在解密期间单独地提供AAD。在一些其它实施方案中，在解密时间至少部分基于请求和或其它元数据产生AAD，使得解密将仅在元数据通过时成功。在一些实施方案中，策略可约束是否可关于特定AAD执行密码操作。Encrypt(KeyID,Data,[AAD])请求的处理可通过编程逻辑和/或密码服务施行的策略要求AAD含有特定值且AAD是真实的(例如，从原始传输后未修改)。类似地，Decrypt

(KeyID,Ciphertext,[AAD])请求可用以使密码服务使用KeyID识别的密钥对指定的密文解密。可诸如上文所描述而使用Decrypt(KeyID,Ciphertext,[AAD])请求中的AAD。举例来说，Decrypt(KeyID,Ciphertext,[AAD])的处理可通过编程逻辑和/或密码服务施行的策略要求AAD含有特定值且AAD是真实的(例如，从原始传输后未修改)。

[0113] 在一实施方案中，Shred(KeyID)可用以使密码服务电子地撕碎指定的KeyID识别的密钥或密钥族。电子撕碎可包括使密钥不再可访问。举例来说，使用Shred(KeyID)请求可使密码系统命令一个或多个硬件装置对指定的KeyID识别的一个或多个密钥执行安全擦除操作。一般来说，KeyID识别的密钥可用任何合适的方式电子地撕碎，诸如通过用其它数据(例如，一连串零或一或随机字符串)重写对密钥编码的数据。如果密钥存储成在一密钥下加密，那么可电子地撕碎用以对密钥加密的所述密钥，从而导致丢失对密钥的访问。在一些实施方案中，撕碎操作可导致解密操作在未来某一确定的点指示被撕碎的KeyID失效。可使用安全地且永久地毁坏对密钥的任何可能的访问的其它方式。

[0114] 在一实施方案中，ReKey(Ciphertext,OldKeyID,NewKeyID)请求可用以使密码服务在不同密钥下对密文加密。当密码服务接收ReKey(Ciphertext,OldKeyID,NewKeyID)请求时，其可使用OldKeyID识别的密钥来对指定的密文解密，且接着使用NewKeyID识别的密钥来对已解密的密文加密。如果NewKeyID识别的密钥尚不存在，那么密码服务可产生将要使用的密钥且使所产生的密钥与诸如结合上文描述的Create(KeyID)请求描述的指定的NewKeyID相关联。在一些实施方案中，ReKey操作可操作以使数据可在密码服务的隔离的实例之间传送。在一些实施方案中，策略可准许对密文执行rekey操作但可能不准许同一请求者直接对密文解密。在一些实施方案中，ReKey可支持将密文从第一账户内的第一KeyID识别的密钥进行ReKey为第二账户内的KeyID识别的密钥。

[0115] 类似地，前端系统可实施策略配置API，在一实施方案中，策略配置API使用户能够提交对配置用于执行密码操作和其它策略相关的操作的策略的请求。在各种实施方案中，策略可与密钥、密钥群、账户、用户和其它逻辑实体相关联。下文提供可经由策略配置API配置的示例策略。在一实施方案中，密码服务策略配置API包括以下请求：

[0116] SetKeyPolicy(KeyID,Policy)

[0117] Suspend(KeyID,Public Key)

[0118] Reinstate(KeyID,Private Key)

[0119] 在一实施方案中，SetKeyPolicy(KeyID,Policy)请求可用以使密码服务存储关于KeyID识别的密钥(或密钥族)的策略。策略可以是确定所请求的密码操作是否可在特定环境中执行的信息。策略可用声明性访问控制策略语言编码，诸如可扩展访问控制标记语言(XACML)、企业隐私授权语言(EPAL)、亚马逊网络服务访问策略语言、微软SecPol或对执行密码操作必须满足的一个或多个条件编码的任何合适的方式。策略可定义可执行什么操作、何时可执行操作、哪些实体可进行对将被执行的操作的授权的请求、对于授权特定请求需要什么信息和类似物。另外，除了上文给出的示例之外或替代于上文给出的示例，还可使用访问控制列表、与用户相关联的特权和/或操作位掩码来定义和/或施行策略。示例策略出现在下文。

[0120] 在一些实施方案中，密码服务可(例如)使用Suspend(KeyID,Public Key)API调用支持暂停操作。暂停操作使密码服务的客户能够拒绝密码服务的操作者使用或访问密钥。

这对于关心隐蔽的合法命令或密码服务的操作者可能被强制使用密钥执行某一操作的其它情形的客户可为有用的。其对于希望锁定特定数据且将其呈现为在线不可访问的客户也是有用的。在一些实施方案中，暂停操作可包括从客户接收公共密钥和用所接收的公共密钥对给定KeyID指定的密钥加密并撕碎KeyID指定的密钥，使得除非(例如)使用指定KeyID且包括私有密钥的Reinstate(KeyID,Private Key)API调用提供与公共密钥相关联的私有密钥，否则提供者不能访问暂停的密钥。在一些其它实施方案中，暂停操作可涉及使用密码服务管理的另一密钥(其包括(而不限于)出于瞬时暂停操作的目的而创建的密钥)对与指定KeyID相关联的密钥加密。此操作产生的密文可提供给客户且不保留在密码服务内。接着可撕碎KeyID识别的原始密钥。密码服务可操作以接收所提供的密文且重新导入暂停的密钥。在一些实施方案中，密文可用将防止密码服务将解密的版本传回至客户的方式产生。

[0121] 如图16中所示，密码服务1600包括后端系统，在一些实施方案中，后端系统本身包括各种组件。举例来说，在此示例中，后端系统包括请求处理系统，其可以是密码服务1600的被配置来根据通过请求API或策略配置API接收的请求执行操作的子系统。举例来说，请求处理组件可接收经由请求API接收的请求，且策略配置API确定此类请求是否真实和因此可履行，且可履行所述请求。履行请求可包括(例如)执行和/或已执行密码操作。请求处理单元可被配置来与认证接口交互，认证接口使请求处理单元能够确定请求是否真实。认证接口可被配置来与诸如上文描述的认证系统交互。举例来说，当请求由请求处理单元接收时，请求处理单元可利用认证接口来与认证服务交互，认证服务可在适用时提供可被使用以便导致密码操作的执行的认证证明。

[0122] 在此说明性示例中，密码服务1600的后端系统还包括多个安全模块(密码模块)和策略施行模块。安全模块中的一者或多者可以是硬件安全模块，但在各种实施方案中，安全模块可以是根据具有本文中描述的能力配置的任何合适的计算机装置。在一实施方案中，每一安全模块存储与KeyID相关联的多个密钥。每一安全模块可被配置来安全地存储密钥，以便不可由密码服务1600的其它组件和/或其它系统的其它组件访问。在一实施方案中，安全模块中的一些或全部符合至少一个安全标准。举例来说，在一些实施方案中，安全模块各自被验证为符合联邦信息处理标准(FIPS)公告140-1和/或140-2中概述的FIPS，诸如FIPS公告140-2中概述的一个或多个安全等级。另外，在一些实施方案中，每一安全模块在密码模块验证程序(CMVP)下被证明。安全模块可实施为硬件安全模块(HSM)或具有HSM的一些或所有能力的另一安全模块。在一些实施方案中，已验证的模块用以引导操作。在一些实施方案中，客户可配置存储在已验证的模块中且仅由已验证的模块操作的一些密钥和由软件操作的其它密钥。在一些实施方案中，与这些各种选项相关联的性能或成本可不同。

[0123] 安全模块可被配置来根据请求处理单元提供的指令执行密码操作。举例来说，请求处理单元可将密文和KeyID提供给适当的安全模块且将使用与KeyID相关联的密钥来对密文解密且作为响应提供明文的指令提供给所述安全模块。在一实施方案中，密码服务1600的后端系统安全地存储形成密钥空间的多个密钥。安全模块中的每一者可存储密钥空间中的所有密钥；然而，变化被视为在本公开的范围内。举例来说，安全模块中的每一者可存储密钥空间的子空间。由安全模块存储的密钥空间的子空间可重叠，使得密钥在安全模块中冗余地存储。在一些实施方案中，某些密钥可仅存储在指定的地理区域中。在一些实施方案中，某些密钥可仅由具有特定证书或许可证等级的操作者访问。在一些实施方案中，某

些密钥可存储在特定的第三方提供者在与数据存储服务的提供者的合约下操作的模块中且仅可与所述模块一起使用。在一些实施方案中，安全模块的构建控制可要求合法命令设法强制使用密钥，而不是如由客户授权涉及额外实体被强制或额外权限强制动作。在一些实施方案中，可向客户供应对权限的独立选项，其中存储客户的密文且存储其密钥。在一些实施方案中，存储密钥的安全模块可被配置来将审核信息提供给密钥的拥有者，且安全模块可被配置使得审核信息的产生和提供不可由客户制止。在一些实施方案中，安全模块可被配置来独立地验证客户产生的签名，使得提供者(例如，托管安全模块)不能在安全模块存储的密钥下执行操作。另外，一些安全模块可存储密钥空间的全部且一些安全模块可存储密钥空间的子空间。其它变化也被视为在本公开的范围内。在不同的安全模块存储密钥空间的不同子空间的情况下，请求处理单元可配置(诸如)有关系表或其它机制以确定指示哪一安全模块来根据各种请求执行密码操作。

[0124] 在一实施方案中，策略施行模块被配置来从请求处理单元获得信息且至少部分基于那个信息确定是否可执行通过API接收的请求。举例来说，当通过请求API接收执行密码操作的请求时，请求处理单元可与策略施行模块交互以确定请求的履行是否根据任何适用策略(诸如适用于请求中的指定的KeyID的策略和/或其它策略，诸如与请求者相关联的策略)授权。如果策略施行模块允许请求的履行，那么请求处理单元可相应地指示适当的安全模块根据履行请求来执行密码操作。

[0125] 与本文中描述的所有图式一样，众多变化被视为在本公开的范围内。举例来说，图16示出与安全模块分离的策略施行模块。然而，每一安全模块可包括除了或代替示为分离的策略施行模块之外的策略施行模块。因此，每一安全模块可被独立地配置以施行策略。另外，作为另一示例，每一安全模块可包括施行与由单独的策略施行模块施行的策略不同的策略的策略施行模块。众多其它变化被视为在本公开的范围内。

[0126] 如上文所论述，各种策略可由与KeyID相关联的用户配置，使得当请求指定结合对应于KeyID的密钥执行的密码操作时，可施行策略。图17提供根据各种实施方案的用于更新策略的进程1700的说明性示例。进程1700可由任何合适的系统(诸如由诸如上文结合图16描述的密码服务系统)执行。在一实施方案中，进程1300包括接收1302更新用于KeyID的策略的请求。请求可用任何合适的方式接收1302。举例来说，参看图16作为示例，请求可通过上文描述的密码服务1600的前端系统的策略配置API接收。请求可用任何合适的方式接收。

[0127] 在一实施方案中，进程1700包括提交1704认证请求和接收1706认证响应。提交1704认证请求和接收1706认证响应可用诸如上文描述的任何合适的方式执行。而且如上文所描述，所接收的认证响应可用以确定1708更新用于KeyID的策略的请求是否真实。如果确定1708所接收的更新用于KeyID的策略的请求不真实，那么可拒绝1710请求。拒绝1710请求可用如上文描述的任何合适的方式执行。然而，如果确定1708所接收的更新用于KeyID的策略的请求是真实的，那么进程1700可包括访问1712适用于请求者的策略信息。策略信息可以是可根据其施行适用于请求者的任何策略的信息。举例来说，在利用由进程1700执行的密码服务的组织内，仅组织的某些用户可被允许更新用于KeyID的策略。策略信息可指示哪些用户能够使密码服务更新用于KeyID的策略和/或甚至策略是否可根据现有策略更新。举例来说，在一些实施方案中，密码服务可接收施行新策略的请求。密码服务可检查任何现有策略是否允许实行新策略。如果密码服务确定现有策略不允许施行新策略，那么可拒绝请

求。一般来说，策略信息可以是可用于施行适用于请求者的策略的任何信息。

[0128] 如图17中所示，进程1700包括使用访问策略信息来确定1704策略是否允许执行所请求的更新。如果确定1714策略不允许执行所请求的更新，那么进程1700可包括拒绝1710诸如上文描述的请求。然而，如果确定1714策略允许执行所请求的更新，那么进程1700可包括更新1716用于KeyID的策略。更新用于KeyID的策略可包括更新策略信息且根据KeyID或结合KeyID存储更新的策略。更新的策略信息可(例如)由诸如上文结合图16描述的密码服务的策略施行模块存储。

[0129] 策略还可由电子环境的结合密码服务操作的其它组件施行。举例来说，参看上文论述的图2，密码服务可将策略的电子表示提供给数据服务前端以用于由数据服务前端施行。这在数据服务较适合于施行策略的情形中可为有用的。举例来说，策略是否允许动作可至少部分基于数据服务前端可访问且密码服务不可访问的信息。作为一个示例，策略可取决于由数据服务后端存储系统代表与策略相关联的客户存储的数据。

[0130] 如上文所论述，密码服务可包括允许根据关于具有KeyID的密钥的策略施行策略的各种系统。图18相应地示出可用以施行策略的进程1800的说明性示例。进程1800可由任何合适的系统(诸如由诸如上文结合图16描述的密码服务系统)执行。在一实施方案中，进程1800包括接收1802使用具有KeyID的密钥执行一个或多个密码操作的请求。尽管图18将进程1800说明为结合执行一个或多个密码操作的请求执行，但应指出，进程1800可适于与执行未必为密码的操作的任何请求一起使用。上文描述了示例操作。

[0131] 可确定1804所接收的请求是否真实。确定所接收的请求是否真实可用诸如上文描述的任何合适的方式执行。举例来说，确定1804请求是否真实可包括诸如上文所描述提交认证请求和接收认证响应。如果确定1804请求不真实，那么进程1800可包括拒绝1806请求。拒绝1806请求可用诸如上文描述的任何合适的方式执行。然而，如果确定1804请求是真实的，那么进程1800可包括访问1808用于KeyID和/或请求者的策略信息。访问用于KeyID和/或请求的策略信息可用任何合适的方式执行。举例来说，访问用于KeyID和/或请求者的策略信息可通过访问来自存储此策略信息的一个或多个存储系统的存储策略信息而执行。访问策略信息可用以确定1810策略是否允许执行一个或多个操作。

[0132] 如果确定1810策略不允许执行所述一个或多个操作，那么进程1800可包括拒绝1806请求。然而，如果确定策略允许执行所述一个或多个操作，那么进程1800可包括执行1812所请求的一个或多个密码操作。可提供1814执行一个或多个密码操作的一个或多个结果，诸如提供给提交所接收的1802执行一个或多个密码操作的请求的请求者。在一些实施方案中，至少部分从允许的请求和或拒绝的请求导出的信息可通过审核子系统提供。

[0133] 如所论述，本公开的实施方案允许灵活策略配置和施行。在一些实施方案中，策略可陈述哪些服务可在什么环境中执行哪些操作。举例来说，关于密钥的策略可允许数据存储服务使密码服务执行加密操作但不是解密操作。关于密钥的策略还可包括关于密文和/或已解密的明文的一个或多个条件。举例来说，策略可要求密文和/或明文在操作的结果响应于请求被提供之前产生某些散列值(其可以是带密钥的散列值)。策略可指定一个或多个限制和/或准许，其至少部分基于时间、请求源自的因特网协议(IP)、将被加密/解密的内容的类型、AAD和/或其它信息。

[0134] 众多变化被视为在本公开的范围内。举例来说，上文论述的各种实施方案论述与

单独的认证服务的交互。然而，上文论述的环境的组件可具有其自己的授权组件且确定请求是否真实可以或可以不涉及与另一实体的通信。另外，上文论述的环境中的每一者是结合环境允许的特定操作和能力说明的。可组合上文结合不同环境论述的技术，且一般来说，根据本公开的环境可允许各种技术的灵活使用。仅作为一个示例，密码服务可用以在请求后对密钥和其它内容(诸如非密钥数据对象)两者加密。作为另一示例，密码服务可被配置来接收且响应于来自用户(例如，计算资源提供者的客户)和其它服务(例如，数据存储服务)两者的请求。在一些实施方案中，密码服务和/或相关联的认证服务可被配置以用于和移动装置一起使用以执行所存储的数据的加密。在一些实施方案中，至少一个解锁pin可由密码服务验证。在又其它实施方案中，密码服务可接收硬件证明产生的信息以作为操作的部分。在一些实施方案中，密码服务可操作以关于内容提供数字权利管理服务。

[0135] 如上文所论述，本公开的各种实施方案允许充足的策略施行和可配置性。许多密码系统提供认证的加密操作模式，其中可执行密码操作以同时提供对数据的机密性、完整性和真实性保证。机密性可通过明文数据的加密而提供。真实性可针对明文和针对可保持未加密的相关联的数据两者提供。借助此类系统，对密文或相关联的数据的改变可导致密文的解密失效。

[0136] 在一实施方案中，与明文相关联的数据用于策略的施行。图19相应地示出根据各种实施方案的进程1900的说明性示例，进程1900用于以允许使用相关联的数据的策略施行的方式对数据加密。进程1900可由任何合适的系统(诸如密码服务和/或安全模块)执行。如所示，进程1900包括获得1902明文。明文可用任何合适的方式获得。举例来说，在诸如上文描述的服务提供者环境中，用户(例如，客户)可提供将被加密的数据。作为另一示例，获得1902可包括产生密钥(将被加密的)和/或获得将被加密的密钥。可诸如上文所描述而使用密钥。

[0137] 如所示出，进程1900包括获得相关联的数据。相关联的数据可以是与明文相关联或将与明文相关联的任何数据。相关联的数据可以是一个或多个策略至少部分所基于的任何数据。示例出现在下文。另外，相关联的数据可用任何合适的方式编码，诸如可扩展标记语言(XML)、JavaScript对象表示法(JSON)、抽象语法表示法1(ASN1)、YAML不是标记语言(也称作另一种标记语言)(YAML)或另一结构化可扩展数据格式。在一实施方案中，进程1900包括至少部分基于明文和相关联的数据产生1906消息认证码(MAC)和密文。MAC和密文的组合(诸如AES-GCM密码的输出)可称作认证的密文。产生MAC和密文可用任何合适的方式执行且MAC和密文的产生可取决于使用哪一/哪些密码系统。举例来说，在一实施方案中，高级加密标准(AES)支持在CCM模式或GCM模式中操作时的相关联的认证的数据(AAD)，其中CCM表示CBC-MAC计数器，GCM表示伽罗瓦/计数器模式，且CBC表示密码块链。在CCM或GCM模式中使用AES，可提供明文和相关联的数据作为输入以获得明文和相关联的数据两者的密文和MAC的串接对的输出。应指出，尽管出于说明的目的而提供AES-CCM和AES-GCM，但可使用其它认证的加密方案且可相应地修改本文中明确地描述的技术。举例来说，本公开的技术一般来说适用于支持认证的加密模式的对称块密码。另外，根据本公开的各种实施方案将其它加密方案与MAC功能组合。合适的加密方案和MAC功能组合包括(但不限于)加密方案在所选择的明文攻击下在语义上是安全的且MAC功能在所选择的消息攻击下不可伪造的组合。另外，尽管本公开的各种实施方案利用导致对密文和MAC两者编码的单一输出的密文，

但MAC和密文可使用不同的密码产生。另外，尽管MAC用作说明性示例，但也可使用一般来说不称作MAC的其它值，诸如一般散列值、校验和、签名和/或可替代MAC使用的其它值。因此，具有支持相关联的数据的自动加密模式的密码包括使用除了MAC之外或作为MAC的替代的其它密码原语的密码。

[0138] 另外，产生MAC和密文可根据各种实施方案用各种方式执行。举例来说，在一实施方案中，诸如上文所描述将明文提供给安全模块。安全模块可被配置来产生MAC。在其它实施方案中，电子环境的除了安全模块之外的组件产生MAC和密文。在此类实施方案中，安全模块可用以对密钥解密，所述密钥在明文形式时用以产生MAC和密文。一旦产生，就可提供1908MAC和密文(即，认证的密文)。在一些实施方案中，还提供相关联的数据。可在使用进程1900和其变化的各种实施方式中用各种方式提供MAC和密文。举例来说，在一些实施方案中，将MAC和密文诸如上文所描述提供给用户，或诸如上文所描述提供给数据服务，以用于由数据服务处理。另外，如所指出，尽管可提供相关联的数据，但在各种实施方案中，不提供相关联的数据和/或其一般来说以明文形式坚持。作为示例，如果不可独立地获得相关联的数据，那么可不提供相关联的数据。作为说明性示例，如果相关联的数据是装置的持久识别符(例如，存储装置的识别符)，那么可在稍后时间策略施行需要时和/或出于其它目的获得相关联的数据。

[0139] 如上文所论述，本公开的各种实施方案利用安全模块来提供增强的数据安全。图20提供根据各种实施方案的进程2000的说明性示例，进程2000可用以用允许新颖的和充足的策略施行的方式对数据加密。进程2000可由任何合适的系统(诸如密码服务和/或安全模块)执行。如图20中所示，进程2000包括获得明文和相关联的数据。如上文，明文和相关联的数据可在单一通信中、在单独通信中和/或从单独实体接收。一旦获得，将明文、相关联的数据和KeyID提供2004至安全模块。安全模块可诸如上文所描述。另外，安全模块可从参与电子环境(诸如支持密码服务的环境，诸如上文所示)的多个安全模块中选择。KeyID可如上文所描述且可在向密码服务提交的对明文加密的请求中指定或可另外指定。另外，在进程2000的替代实施方案中，可不指定KeyID。举例来说，在一些实施方案中，安全模块可选择KeyID和/或可产生稍后被指派KeyID的密钥。在此类实施方案中，进程2000可被修改以提供来自安全模块的KeyID。

[0140] 回到所示的实施方案，进程2000可包括从安全模块接收2006密文和MAC。密文可在KeyID识别的密钥下加密。MAC可以是对明文和相关联的数据两者的组合的MAC，使得对密文或相关联的数据的改变将导致对MAC的检查失效。如上文，应指出变化包括其中MAC至少部分基于相关联的数据但独立于明文而产生的变化。另外，如上文所论述，密文和MAC可一起提供(诸如从使用AES-CCM或AES-GCM密码的输出)或可单独地提供。一旦从安全模块接收，将MAC和密文提供2008给适当的实体，诸如密码服务或结合密码服务操作的数据服务的用户，诸如上文所描述。

[0141] 如上文所论述，安全模块可用各种方式使用以增强对数据的保护。如上文所论述，在一些实施方案中，安全模块用以对密钥加密，所述密钥(以其明文形式)被使用来对其它数据加密。图21相应地示出可用于此类情形的进程2100的说明性示例。进程2100可由任何合适的系统(诸如密码服务和/或安全模块)执行。在一实施方案中，进程2100包括获得2102明文和相关联的数据，诸如上文所描述。如所示，进程2100包括将已加密的密钥、相关联的

数据和KeyID提供2104至安全模块，KeyID识别可由安全模块用来对已加密的密钥解密的密钥。因此，进程2100包括从使用由KeyID识别的密钥来对已加密的密钥解密的安全模块获得已解密的密钥。一旦获得，密钥可用以对明文加密，从而计算2108密文和MAC。密文可以是明文的加密且MAC可针对(即，至少部分基于)相关联的数据或相关联的数据和明文两者，诸如上文所描述。一旦被加密，进程2100可包括提供2110诸如上文描述的MAC和密文。另外，进程还可包括丢失2112对已解密的密钥的访问，其可用任何合适的方式执行，诸如通过安全擦除操作、重写存储已解密的密钥的存储器、移除存储密钥的易失性存储器的电力和/或系统执行进程2100的任何其它方式(例如，密码系统中不存在安全模块)。尽管并列地说明，但提供相关联的数据、MAC和/或密文与丢失对密钥的访问可按顺序执行，执行的次序可在各种实施方案中变化。

[0142] 图22示出根据各种实施方案的可用以使用相关联的数据施行策略的进程2200的说明性示例。进程2200可由任何合适的系统(诸如密码服务和/或安全模块)执行。在一实施方案中，进程2200包括接收2202执行操作的请求。请求可以是向处理请求的服务提交的任何请求。在一实施方案中，请求是向密码服务提交的执行密码操作的请求。响应于接收2202请求，进程2200可包括获得2204密文、MAC和预期的相关联的数据。获得2204密文、MAC和预期的相关联的数据可用任何合适的方式执行。举例来说，在一些实施方案中，在请求中接收密文、MAC和预期的相关联的数据中的一者或多者。可在单独请求或其它通信中接收和/或从数据存储(诸如本地数据存储)访问密文、MAC和预期的相关联的数据中的两者或两者以上。举例来说，在一实施方案中，接收密文和MAC作为串接对(可能从AES-GCM或AES-CCM密码的输出产生)以作为请求的部分。预期的相关联的数据也可以是请求的部分或可用其它方式识别。举例来说，可直接地或间接地使用请求者的身份来确定相关联的数据。作为特定示例，如果请求是关于存储在存储装置中的数据执行操作，那么获得2204相关联的数据可包括获得数据存储装置的识别符。识别符可明确地识别(例如，作为请求的部分)或隐含地识别(例如，因为其它信息可用以确定数据存储在数据存储装置中)。相关联的数据可以或可另外至少部分基于数据存储装置的识别符。如上文所论述，相关联的数据可在各种实施方案中极大地变化。

[0143] 在一实施方案中，进程2200包括产生2206可用以确定预期的相关联的数据的真实性的参考MAC。举例来说，密文、相关联的数据和适当密钥(其可在请求中识别或可另外确定)用以产生2206参考MAC。产生MAC可用任何合适的方式(诸如通过使用用以获得密文的相同密码)执行。可确定2208参考MAC与所获得的MAC是否匹配。举例来说，在许多密码系统中，MAC在其相等时匹配，但预期在各种实施方案中可使用其它类型的匹配。如果确定2208参考MAC与所获得的MAC匹配，那么在一实施方案中，进程2200包括访问2210至少部分基于相关联的数据的策略信息。访问2210策略信息可包括访问至少部分基于与KeyID相关联的一个或多个策略的来自远程或本地数据存储的一个或多个策略(即，一个或多个策略的电子表示)，KeyID用以产生参考MAC和/或执行另一密码操作。

[0144] 接着可至少部分基于所访问的策略信息确定2212策略是否允许执行所请求的操作(例如，策略是否允许履行请求)。确定策略是否允许执行所请求的操作可包括确定密文是否标记有所访问的策略信息指定的相关联的数据。另外，尽管未说明，但不是至少部分基于相关联的数据的策略信息(例如，基于除了相关联的数据以外的信息的策略)也可用来确

定策略是否允许执行操作。如果确定2212策略允许操作，那么进程2200可包括执行2214操作。然而，如果确定2212策略不允许操作，和/或如果确定2208参考MAC与所获得的MAC不匹配，那么进程2200可包括拒绝2216请求，诸如上文所描述。

[0145] 各种策略可使用上文描述的技术施行。举例来说，如所指出，策略可与密钥相关联，使得当被施行时，策略确定对于密钥可做什么和/或不能做什么。作为一个示例，策略可陈述数据服务可仅针对策略指定的某些类型的操作使用密钥(或，替代地，某些操作对于数据服务是禁止的)。策略还可指定使用中的条件、使用时间、IP地址、可被加密的内容、可被解密的内容和类似物。作为一个说明性示例，一个策略可指定仅在解密的散列与特定值匹配时允许提供解密的结果。因此，如果明文的散列与策略不一致，那么施行策略的密码或其它服务将不提供明文。作为另一示例，策略可指定仅在密文标记有等于指定值或以指定值开始的相关联的数据时允许密文的解密。作为又一示例，策略可指定仅在密文标记有用相关联的数据编码的存储装置的识别符时允许密文的解密。

[0146] 一般来说，策略可指定至少部分基于与密文相关联的数据(即，认证的相关联的数据)的值的限制和/特权。一些额外策略包括指定仅在密文标记有请求解密的计算机的识别符、密文标记有安装(操作地连接)至请求解密的计算机的存储容量的识别符和/或密文标记有其它计算资源的识别符时允许解密的策略。计算资源也可以是由施行策略的计算资源提供者托管的计算资源。其它策略视为在本公开的范围内，诸如至少部分基于在向执行密码算法的实体之外的实体揭示(例如，向施行策略的密码服务之外的用户和/或其它数据服务揭示)密码算法的输出之前的密码算法的输入和/或输出的策略。如上文所指出，策略还可至少部分基于相关联的数据指定对于何时可修改策略的条件。

[0147] 图23示出根据各种实施方案的进程2300的说明性示例，进程2300是上文结合图22论述的进程2200的变化，其中变化说明在施行策略时使用安全模块。在一实施方案中，进程2300包括接收2302对密文解密的请求，密文可以是已加密的密钥或其它已加密的数据。进程2300还包括获得2304密文、MAC和预期的相关联的数据，诸如上文结合图22所描述。如图23中所示，在一实施方案中，进程2300包括使用2306安全模块来对密文解密。使用2306安全模块还可包括从多个安全模块中选择可操作以对密文解密的安全模块，从而产生明文。还可使用2308安全模块以至少部分基于明文和预期的相关联的数据产生参考MAC。应指出，尽管在图23中示出为两个单独步骤，但使用安全模块来对密文解密和产生参考MAC可在单一操作(例如，至安全模块的单一请求)中执行。一旦从安全模块获得，进程2300包括确定2310参考MAC与所获得的MAC是否匹配，诸如上文结合图22所描述。然而，应指出，在一些实施方案中，进程2300可被修改，使得安全模块被提供参考MAC且确定参考MAC与所获得的MAC是否匹配。在此变化中，安全模块可提供指示是否存在匹配的响应。

[0148] 回到图23中所示的实施方案，如果确定2310参考MAC与所获得的MAC匹配，那么进程2300包括访问2312至少部分基于相关联的数据的策略信息，诸如上文结合图22所描述。而且，如上文，尽管未如此说明，但也可访问关于不是至少部分基于相关联的数据的策略的额外策略信息。可确定2314策略是否允许操作。如果确定2314策略允许操作，那么可提供2316明文。如上文结合图22，如果确定2314策略不允许操作和/或如果确定参考MAC与所获得的MAC不匹配，那么进程可包括拒绝2318请求，诸如上文所描述。

[0149] 尽管本公开的各种实施方案是使用密码的认证模式的相关联的数据说明的，但其

它实施方案也视为在本公开的范围内。举例来说，本公开的实施方案一般来说适用于可用密文验证以施行策略的数据的使用。作为说明性示例，策略的表示可与第一明文组合以产生新明文(例如，包括明文和策略的新明文)。新明文可使用合适的密码(诸如AES)来加密以产生密文。当接收到对密文解密的请求时，接收请求的系统可对密文解密，从新明文提取策略，且检查策略是否允许提供第一明文。如果策略不允许提供第一明文，那么可拒绝请求。可代替或除了上文结合密码的认证模式的相关联的数据论述的实施方案之外使用此类实施方案。

[0150] 本公开的各种实施方案还允许指定审核如何发生的条件的关于密钥的策略。举例来说，关于密钥的策略可指定对密钥的审核等级，其中审核等级是确定密码服务如何审核密钥使用的密码服务的参数。审核可由任何合适的系统执行。举例来说，参看图16，请求处理单元可与审核系统(未示出)通信，审核系统可以是密码服务的部分或与密码服务分离。当事件结合密码操作的执行发生时，可向记载信息的审核系统提供相关信息。事件可以是执行密码操作的请求和/或指示是否执行所请求的操作的信息。举例来说，如果用户成功地请求密码服务执行解密操作，那么密码服务可将允许请求和操作被执行的信息提供给审核系统。管理访问事件和一般来说，密码服务的任何交互或操作可记载有可识别事件中涉及的实体的相关信息、描述事件的信息、事件的时间戳和/或其它信息。

[0151] 在一实施方案中，审核等级包括高耐久性等级和低耐久性等级。对于低耐久性等级，对密钥的审核操作可由密码服务最大努力地执行。在根据低耐久性等级审核的情况下，在正常操作期间，审核所有操作，但在密码服务的组件失效的事件中，一些审核数据可丢失。在根据高耐久性等级审核的情况下，在揭示密码操作的结果之前，获得操作已发生的审核记录已耐久地存入至存储器的保证。因为需要确认，高耐久性审核模式中的操作比低耐久性审核模式中的操作慢。审核记录已耐久地存入至存储器的保证可包括来自用以存储审核记录的一个或多个其它系统的确认。因此，参看先前段落，密码服务可延迟向用户提供明文，直到审核系统确认导致明文的解密的记录已耐久地存入至存储器。耐久地存入至存储器可意味着数据已根据获得耐久性的一个或多个条件存储。举例来说，当数据写入至非易失性存储器和/或数据已冗余地存储在多个数据存储装置中(例如，使用擦除编码或其它冗余编码方案)时，数据可耐久地存入至存储器。

[0152] 在一实施方案中，密码服务使用低耐久性和高耐久性审核等级的子等级。举例来说，在一实施方案中，每一等级对应于两个单独的状态：不可变状态和可变状态。状态不可变还是不可变可确定状态之间的转变如何发生和是否发生。举例来说，使用审核耐久性的说明性示例，关于密钥的策略可能够在低耐久性可变与高耐久性可变之间、从低耐久性可变至低耐久性不可变和从高耐久性可变至高耐久性不可变改变。然而，密码服务可被配置，使得一旦用于密钥的策略处于低耐久性不可变或高耐久性不可变，那么禁止转变。因此，一旦用于密钥的策略处于不可变状态，那么策略不能改变。

[0153] 图24示出此系统的状态图的说明性示例，系统一般化为可接通(施行)和切断(未施行)的策略。如图24中所示，用于密钥的策略可接通或切断。当接通且不可变时，策略可改变为接通且不可变(不可改变)或切断且可变(可改变)。类似地，当策略切断但可变时，策略可改变为接通但可变或切断且不可变。应指出，也可获得其它转变，诸如策略从切断但可变至接通且不可变的直接转变。另外，不是所示出的所有转变都可获得。举例来说，在一些情

况下，密钥可能不具有切断且不可变状态。

[0154] 图25示出一般状态图，其示出系统可如何允许适用于密钥的各种策略中的转变。在此示例中，示出三个策略，策略A、策略B和策略C。这些策略中的每一者具有可变和不可变状态，且示出了状态之间可允许的转变和策略。举例来说，不允许来自不可变状态的转变。然而，可变状态中的策略可改变为可变状态中的另一策略。举例来说，关于密钥的策略可从策略A(可变)改变为策略B(可变)。如关于策略B所示，可存在对多个策略可用的转变。举例来说，策略可从策略B改变为策略C或策略A。与图24一样，可包括其它转变和策略且并非所有策略都可具有所有状态。另外，尽管各种示例示出具有不可变和可变状态的策略，但策略可具有两个以上状态，其中每一状态对应于可以或不能执行的一组动作。举例来说，半可变状态可允许在可变状态下将获得的一些但不是所有转变。

[0155] 如所指出，策略可用于除了审核之外的各种操作。举例来说，关于策略转变的以上限制可适用于密钥可撕碎性。举例来说，策略可指示密钥是否可被撕碎(不能撤回地丢失)。策略可具有四个状态：可撕碎-可变；可撕碎-不可变；不可撕碎-可变；和不可撕碎-不可变。如上文，当在不可变状态中时，策略不可改变。作为另一示例，关于密钥是否可从安全模块导出的策略还可具有此四状态策略。

[0156] 策略还可与密钥相关联以防止密钥使用实现安全攻击的弱点。举例来说，在一实施方案中，一个或多个密钥与自动旋转策略相关联，自动旋转策略使密钥在某一使用量后被引退(例如，被标记以便不再可用于加密)。此策略可以是用户可配置的(例如，客户可配置的)策略，用户(例如，客户)激活所述策略和/或提供所述策略的参数。策略还可以是适用于较大密钥集(诸如包括由密码服务代表其客户管理的至少所有密钥的集合)的总策略。以此方式，密钥可在其被使用足够时间而实现密码攻击之前引退，在密码攻击中知道足够的明文和对应的密文提供确定密钥的能力。

[0157] 图26示出根据各种实施方案的可用以按适当间隔旋转密钥的进程2600的说明性示例。进程2600可由任何合适的装置(诸如上文论述的安全模块)执行。在一实施方案中，进程2600包括接收2602使用KeyID识别的密钥执行密码操作的请求。请求可以是从诸如上文描述的密码服务请求处理器接收的请求。请求可以是对数据加密或解密，或一般来说，使用KeyID识别的密钥执行任何密码操作(诸如产生电子签名、另一密钥或至少部分基于密钥的其它信息)的请求。在接收2602请求后，进程2600包括执行2604所请求的操作。执行所请求的操作可包括额外操作，诸如选择执行操作的密钥的适当版本。举例来说，如果操作是加密，那么标记为活跃的密钥可用以加密。如果操作是解密，那么执行操作可包括选择由KeyID识别的密钥的适当版本以解密，其在各种实施方案中是最初用以对数据加密的密钥。密钥可通过各种方式选择。举例来说，在一些实施方案中，密文可包括识别版本、序列号、日期或实现密钥的选择的其它信息的元数据。在一些实施方案中，可尝试每一可能的密钥直到数据被恰当地解密为止，其中恰当的解密可由与密文相关联的明文输出的散列或由相关联的数据的正确性确定。

[0158] 一旦已执行2604密码操作，进程2600包括更新2606用于KeyID识别的活跃密钥的密钥使用计数器。举例来说，如果密码操作导致密钥的单次使用，那么计数器可增加一。类似地，如果密码操作导致密钥的N次(N是正整数)使用，那么计数器可增加N。可确定2608计数器是否超过阈值。阈值可以是分配给KeyID识别的密钥的版本的使用数目。阈值可由密码

服务的管理对密钥的操作的分配的组件提供。阈值还可以是操作的默认数目。如果确定2608计数器超过阈值，那么在一实施方案中，进程2600包括获得2610新密钥。获得新密钥可用任何合适的方式执行。举例来说，如果进程2600由安全模块执行，那么获得新密钥可包括产生新密钥或从另一安全模块获得新密钥，其可由密码服务的操作者策划。将密钥从一个安全模块传递至另一安全模块可通过用提供和接收安全模块可访问的密钥对密钥加密而执行。执行进程2600的安全模块可接收已加密的密钥且对已加密的密钥解密。还可使用公共密钥密钥交换技术。

[0159] 一旦已获得新密钥，在一实施方案中，进程2600可包括将当前活跃密钥标记2612为引退的。将当前活跃密钥标记为引退的可用任何合适的方式(诸如通过改变安全模块维护的数据库中的适当值)执行。另外，进程2600可包括使新密钥与KeyID相关联2614且将新密钥标记为活跃的，诸如通过更新安全模块维护的数据库。尽管未说明，但进程2600还可包括提供新密钥以供另一安全模块使用。如虚线所指示，在新密钥准备好供执行进程2600的安全模块(或其它系统)使用之后的某一时刻，进程可包括接收2602执行另一密码操作的请求且进程2600可如上文所论述进行。另外，如果确定2608计数器不超过阈值，那么进程2600可结束和/或一旦接收2602另一请求就重复。

[0160] 图27示出根据各种实施方案的进程2700的说明性示例，进程2700可用以在密码服务或其它环境中执行密钥的自动旋转。进程2700可由任何合适的系统(诸如密码服务的根据各种实施方案跟踪密钥使用和策划密钥旋转的组件)执行。如图27所示，进程2700包括将对密钥的若干密钥操作(例如，对多个密钥中的每一者的若干操作)分配2702给一个或多个安全模块。作为特定示例，在利用五个安全模块来冗余地存储/使用密钥集的环境中，每一安全模块对于其管理的密钥中的每一者可被分配一百万个操作。被分配操作的安全模块(或其它计算机系统)可托管在多个数据中心中的相同的数据中心中。举例来说，在一些实施方案中，计算资源提供者利用多个地理区域中的多个数据中心中的安全模块来实施地理上分布式密码或其它服务。

[0161] 然而，应指出，可对一些但不是所有密钥进行分配，且对每一密钥的分配可能不相等。分配密钥操作可包括将分配通知提供给已被分配密钥操作的每一安全模块。通知可指定已对每一密钥分配的数目，或在一些实施方案中，至安全模块的通知可指示安全模块重新初始化预编程至安全模块中的计数器或将预编程的数目添加至计数器。在将密钥操作分配2702给安全模块后，可更新用于已对其分配操作的密钥中的每一者的密钥使用计数器。继续以上具体示例，如果五个安全模块中的每一者对于特定KeyID识别的密钥已被分配一百万个操作，那么用于KeyID的计数器可增加(向上或向下，这取决于计数是向上还是向下执行的)五百万。

[0162] 在已被分配密钥操作后，安全模块可执行诸如上文描述的密码操作。安全模块可维持其自己的计数器，所述计数器至少部分基于已进行的分配。在以上示例的情况下，如果安全模块对于特定KeyID识别的密钥已被分配一百万个操作，那么安全模块可将计数器设置为一百万(或一百万以上，如果现有计数器具有剩余操作的话)。在使用密钥执行密码操作后，安全模块可相应地增加其自己的计数器。

[0163] 在某一时刻，可检测2706一个或多个KeyID的分配耗尽事件。耗尽事件可以是一个或多个安全模块丢失或耗尽其分配的任何事件。作为一个示例，安全模块可使用其对特定

KeyID识别的密钥的操作的分配，且检测耗尽事件可包括从安全模块接收安全模块已通过执行对应数目的操作而耗尽其对KeyID的分配(或在耗尽其分配的某一预定阈值内或另外被预测将很快耗尽其分配)的通知。作为另一示例，在一些实施方案中，安全模块被配置来在某些事件后(诸如故障，检测到侵入或其它窜改，或在操作者需要访问安全模块以用于维护时)丢失对存储在其中的密钥(和与密钥相关联的数据，诸如计数器)的访问。因此，耗尽事件可包括因为故障或检测到窜改/侵入有意的动作(诸如使安全模块暂时不能使用以用于维护)而丢失(可能暂时的)安全模块。在此示例中，安全模块可被看作好像使用了其分配，即使其未必执行所分配的数目的操作。然而，应指出，所有此类事件可不包括在某些实施方案中的耗尽事件，诸如当计数器持久地存储且因此甚至在丢失对对应密钥的访问后可恢复时。还应指出，耗尽事件可影响一个以上安全模块。举例来说，影响数据中心中的多个安全模块的停电可导致影响多个安全模块的耗尽事件。

[0164] 在检测到耗尽事件后，可确定2710计数器对于与耗尽事件相关联的密钥中的任一者是否超过阈值。阈值可以是至少部分基于用以执行密码操作的密码的数学属性的操作的预定数目。举例来说，对于具有CBC模式的密码，操作的数目可以或可另外至少部分基于密钥空间的大小除以以下两者的平方的乘积：(1)用块表示的密文的长度；和(2)密文的数目。对于具有CTR模式(诸如AES-GCM)的密码，操作的数目可以或可另外至少部分基于密钥空间的大小除以以下两者的乘积：(1)以块为单位的密文的长度的平方；和(2)密文的数目。如果确定2710计数器对于受耗尽事件影响的密钥中的任一者超过阈值，那么进程2700可包括指示2712一个或多个安全模块(即，与耗尽事件相关联的一个或多个安全模块)获得对其的操作的分配已耗尽的一个或多个新密钥且用新密钥替换受影响的密钥。举例来说，如果安全模块暂时离线(从而导致耗尽事件)，且因此导致对KeyID(但未必是所有KeyID)的计数器超过阈值，那么可指示安全模块获得新密钥，诸如上文所描述(例如，通过产生新密钥、访问来自数据存储器的预先产生的密钥或从另一安全模块获得新密钥)。然而，应指出，可指示与受耗尽事件影响的安全模块不同的安全模块获得新密钥，诸如在使一个安全模块离线且使新的安全模块在线时。用新密钥替换受影响的密钥(由KeyID识别)可包括将受影响的密钥标记为引退的、使新密钥与KeyID(例如，数据库中)相关联且将新密钥标记为活跃的。用新密钥替换受影响的密钥还可包括初始化用于新密钥的计数器(由用新密钥替换受影响的密钥的安全模块维持)，新密钥可以是预编程的值或可以是从执行进程2700的系统获得的值。进程2700还可包括诸如通过相应地更新数据库而将受影响的密钥标记2714为引退的且将新密钥标记2714为活跃的。应指出，执行进程2700的系统可能无法访问受影响的和/或新密钥，且因此，将受影响的密钥标记为引退的且将新密钥标记为活跃的可包括适当地使密钥的识别符与指示引退的或新的值相关联。

[0165] 在一实施方案中，在标记2714后，如果确定2710受影响的密钥中没有一个的计数器超过阈值，那么进程2700可包括2716对仍活跃的受影响的密钥和/或因为执行进程2700的操作而获得的任何新密钥分配额外密钥操作。在分配额外密钥操作后，可更新2704适当的密钥使用计数器，诸如上文所描述。

[0166] 与本文中描述的所有进程一样，变化视为在本公开的范围内。举例来说，在一些实施方案中，安全模块不跟踪其对密钥的使用，但密码或其它服务的另一组件更新用于向任何安全模块提交的使用密钥执行一个或多个操作的每一请求的密钥的计数器。在此类实施

方案中，对于多个密钥中的每一密钥，安全模块的组件可跟踪使用密钥执行操作的请求(或例如，通过请求被成功地履行的确认或其它指示跟踪所执行的操作)，从而相应地更新用于密钥的计数器。当计数器达到阈值时，维持计数器的系统可使所有适当的安全模块引退密钥且用新密钥替换所述密钥(或执行导致密钥被引退的某一其它操作，诸如使具有密钥的安全模块引退密钥和使一个或多个其它安全模块开始使用新密钥)。作为在本公开的范围内的变化的另一示例，在一些实施方案中，当安全模块使用其对密钥操作的分配且导致计数器超过阈值时，可指示安全模块获得新密钥，诸如上文所描述。其它安全模块可继续使用密钥直到其使用了其分配为止。当安全模块使用其分配时，其可获得已替换安全模块中的导致计数器超过阈值的密钥的新密钥。换句话说，可允许安全模块在不得不获得新密钥之前用完其对密钥操作的分配。

[0167] 图28示出用以维护密钥使用的跟踪的数据库的说明性示例表示。数据库可由适当的系统(诸如执行进程2700的系统)维护。在所示的数据库中，列分别对应于KeyID、密钥版本、可用性和计数器。KeyID和密钥版本可如上文所描述。可用性列中的值可指示密钥是引退的还是活跃的(或者密钥是否具有另一状态，如果本公开的各种实施方式支持此类其它状态的话)。如图28中所示，数据库针对KeyID识别的密钥的每一版本(包括所有引退的版本和活跃的版本)具有一行。然而，应指出，数据库中密钥的所有版本可能不足。举例来说，密钥可出于各种安全理由而从存储器永久地移除。移除可(例如)按照客户请求或策略的施行。

[0168] 如图28中所示，所示的数据库还包括用于每一活跃的密钥的计数器。而且，在此特定示例中，数据库包括用于不活跃的密钥的计数器(例如，示出超过阈值的每一密钥的值，从而导致获得新密钥)。然而，在一些实施方案中，可不保留不活跃的密钥的计数器值。计数器可在密钥操作被分配给安全模块时由维护数据库的系统更新。一旦计数器行中的值超过阈值，新的行就可添加至数据库以容纳新密钥来替换计数器值超过阈值的密钥。

[0169] 安全模块可出于其自己的目的而维护类似数据库。举例来说，安全模块可跟踪其自己对密钥的使用，且当安全模块对密钥的使用耗尽分配给安全模块的数目时，安全模块可通知密码服务(或使用安全模块的另一服务)的密钥旋转管理组件，密钥旋转管理组件可(例如)执行进程(诸如上文描述的进程2700)以将额外操作重新分配给安全模块或在可用于密钥的密钥操作的数目已耗尽时使安全模块获得新密钥。

[0170] 用以跟踪密钥使用的数据库可与图28中所示和上文描述的数据库不同。举例来说，额外信息可包括在数据库中，诸如与密钥相关联的元数据，诸如产生时间、引退时间、关于密钥使用所针对的客户的信息和/或在各种实施方案中可为有用的其它信息。另外，尽管出于说明的目的而提供关系表，但可使用支持各种实施方案的存储数据的其它方式。

[0171] 本公开的实施方案可鉴于以下条款进行描述：

[0172] 1.一种用于施行策略的计算机实施的方法，其包括：

[0173] 在配置有可执行指令的一个或多个计算机系统的控制下，

[0174] 使用密码的已认证的加密模式以至少部分基于密钥、明文和相关联的数据来产生已认证的密文；

[0175] 使策略与所述密钥相关联，所述策略至少部分基于所述相关联的数据来指定用于提供所述明文的条件；

[0176] 结合使用所述密钥对所述已认证的密文解密的请求接收声称的相关联的数据；

[0177] 至少部分基于所述声称的相关联的数据和所述已认证的密文来验证所述声称的相关联的数据与所述相关联的数据匹配；

[0178] 由于验证所述声称的相关联的数据与所述相关联的数据匹配，至少部分基于所述声称的相关联的数据来确定所述策略是否允许提供所述明文；以及

[0179] 由于确定所述策略允许提供所述明文，提供所述明文。

[0180] 2.如条款1所述的计算机实施的方法，其中所述声称的相关联的数据是所述请求的部分。

[0181] 3.如条款1或2所述的计算机实施的方法，其中所述声称的相关联的数据至少部分基于所述明文。

[0182] 4.如前述条款中任一项所述的计算机实施的方法，其中确定所述策略是否允许提供所述明文也至少部分基于所述已认证的密文。

[0183] 5.一种用于施行策略的计算机实施的方法，其包括：

[0184] 在配置有可执行指令的一个或多个计算机系统的控制下，

[0185] 接收对密文解密的请求，所述密文已至少部分基于明文和密钥而产生；

[0186] 至少部分基于可用所述密文和所述密钥验证的数据来确定策略是否允许响应于所述请求而提供所述明文；以及

[0187] 由于确定所述策略允许提供所述明文，响应于所述请求而提供至少所述明文。

[0188] 6.如条款5所述的计算机实施的方法，其中所述策略是指定对所述密钥的使用的一个或多个限制的策略。

[0189] 7.如条款5或6所述的计算机实施的方法，其中：

[0190] 所述方法还包括至少部分基于声称的相关联的数据和所述密钥来确定所述声称的相关联的数据是否是真实的；且

[0191] 确定所述策略是否允许响应于所述请求而提供所述明文包括确定可用所述密文验证的所述数据的值与所述策略指定的值是否匹配。

[0192] 8.如条款5至7中任一项所述的计算机实施的方法，其中：

[0193] 所述密文是密码的已认证的加密模式的输出，所述输出还包括至少部分基于与所述密文相关联的数据的消息认证码；且

[0194] 所述方法还包括至少部分基于所述消息认证码来确定声称与所述密文相关联的数据是否是真实的。

[0195] 9.如条款5至8中任一项所述的计算机实施的方法，其中所述密文还至少部分基于可用所述密文和所述密钥验证的所述数据。

[0196] 10.如条款5至9中任一项所述的计算机实施的方法，其中所述策略要求所述请求与和所述密文相关联的所述数据匹配以用于提供所述明文的特性是允许的。

[0197] 11.如条款5至10中任一项所述的计算机实施的方法，其中可用所述密文验证的所述数据对所述策略编码，且确定所述策略是否允许提供所述明文包括从可用所述密文验证的所述数据获得所述策略。

[0198] 12.如条款5至11中任一项所述的计算机实施的方法，其中所述密文对所述策略编码，且确定所述策略是否允许提供所述明文包括从所述密文获得所述策略。

[0199] 13.如条款5至12中任一项所述的计算机实施的方法，其中可用所述密文验证的所述数据对一个或多个属性编码，且确定所述策略是否允许提供所述明文包括检查所述一个或多个属性与所述策略的属性是否匹配。

[0200] 14.如前述条款中任一项所述的计算机实施的方法，其中所述密文对一个或多个属性编码，且确定策略是否允许提供所述明文包括检查所述一个或多个属性与所述策略的属性是否匹配。

[0201] 15.一种计算机系统，其包括：

[0202] 一个或多个处理器；以及

[0203] 存储器，其包括指令，所述指令在由所述一个或多个处理器执行时使所述计算机系统执行以下操作：

[0204] 验证与请求相关联的信息与密文兼容；

[0205] 至少部分基于与所述请求相关联的所述信息来分析所述密文和认证信息以确定策略是否允许对所述请求的特定响应；

[0206] 由于确定所述策略允许所述特定响应，允许对所述请求的所述特定响应。

[0207] 16.如条款15所述的系统，其中：

[0208] 所述密文是包括所述认证信息的已认证的密文；

[0209] 所述认证信息包括消息认证码；且

[0210] 验证与所述请求相关联的所述信息与所述密文兼容包括使用所述消息认证码来检查与所述请求相关联的所述信息的真实性。

[0211] 17.如条款15或16所述的系统，其中所述认证信息是所述密文的成分。

[0212] 18.如条款15至17中任一项所述的系统，其中与所述请求相关联的所述信息是用结构化可扩展数据格式编码的。

[0213] 19.如条款15至18中任一项所述的系统，其中所述请求是对所述密文解密的请求。

[0214] 20.如条款15至19中任一项所述的系统，其中与所述请求相关联的所述信息是由密码用来产生所述密文的相关联的数据。

[0215] 21.如条款15至20中任一项所述的系统，其中所述认证信息是至少部分基于明文和特定信息产生的消息认证码，所述特定信息如果与和所述请求相关联的所述信息不匹配，那么将使所述策略不允许所述特定响应。

[0216] 22.如条款15至21中任一项所述的系统，其中：

[0217] 与所述请求相关联的所述信息是至少部分基于特定信息产生的；且

[0218] 所述认证信息指示所述特定信息与和所述请求相关联的所述信息是否匹配。

[0219] 23.如条款15至22中任一项所述的系统，其中所述密码是已认证的加密模式密码。

[0220] 24.一种计算机可读存储介质，其上存储有指令，所述指令在由计算机系统的一个或多个处理器执行时使所述计算机系统执行以下操作：

[0221] 从密文获得明文，所述密文已至少部分基于所述明文和其它输入而产生；

[0222] 至少部分基于所述其它输入来评估策略以确定是否响应于请求而提供所述明文；以及

[0223] 由于确定提供所述明文，响应于所述请求而提供所述明文。

[0224] 25.如条款24所述的计算机可读存储介质，其中所述其它数据是输入至密码以产

生所述密文的相关联的数据。

[0225] 26.如条款24或25所述的计算机可读存储介质，其中：

[0226] 所述计算机系统由服务提供者托管；且

[0227] 所述请求是被代表所述服务提供者的客户提交的。

[0228] 27.如条款26所述的计算机可读存储介质，其中：

[0229] 所述指令还使所述计算机系统从所述客户接收对所述策略编码的信息；且

[0230] 由于已接收到对所述策略编码的所述信息，执行评估所述策略。

[0231] 28.如条款24至27中任一项所述的计算机可读存储介质，其中获得所述明文包括向安全模块提供所述密文和从所述安全模块获得所述明文。

[0232] 29.如条款24至28中任一项所述的计算机可读存储介质，其中评估所述策略还至少部分基于结合所述请求获得的信息。

[0233] 30.如条款24至29中任一项所述的计算机可读存储介质，其中所述策略与用以从所述明文产生所述密文的密钥相关联。

[0234] 31.如条款24至30中任一项所述的计算机可读存储介质，其中所述其它输入包括用标准数据格式编码的属性的集合。

[0235] 32.如条款24至31中任一项所述的计算机可读存储介质，其中所述其它输入对所述策略编码。

[0236] 图29图示用于实施根据各种实施方案的方面的示例环境2900的方面。如将了解，尽管基于Web的环境用于解释的目的，但可在适当时使用不同的环境以实施各种实施方案。环境包括电子客户端装置2902，其可包括可操作以经由适当的网络2904发送和接收请求、消息或信息且将信息传达回至装置的用户的任何适当的装置。此类客户端装置的示例包括个人计算机、手机、手持式消息传递装置、膝上型计算机、机顶盒、个人数据助理、电子书阅读器和类似物。网络可包括任何适当的网络，包括内联网、因特网、蜂窝式网络、局域网或任何其它此类网络或其组合。用于此系统的组件可至少部分取决于所选择的网络和/或环境的类型。用于经由此网络进行通信的协议和组件是众所周知的且本文中将不详细论述。经由网络的通信可由有线或无线连接和其组合实现。在此示例中，网络包括因特网，因为环境包括用于接收请求和响应于请求而服务内容的Web服务器2906，但对于其它网络，可使用服务类似目的的替代装置，如对本领域技术人员将清楚。

[0237] 说明性环境包括至少一个应用服务器2908和数据存储2910。应理解，可存在若干应用服务器、层或其它元件、进程或组件，其可链接或另外配置，其可交互以执行任务，诸如从适当的数据存储获得数据。如本文中所使用，术语“数据存储”指能够存储、访问和检索数据的任何装置或装置的组合，其可包括在任何标准的、分布式或群集环境中的数据服务器、数据库、数据存储装置和数据存储介质的任何组合和数目。应用服务器可包括任何适当的硬件和软件，其用于与执行用于客户端装置的一个或多个应用的方面所需的数据存储集成、处理大部分数据访问和应用的业务逻辑。应用服务器与数据存储合作提供访问控制服务，且能够产生将被传送至用户的内容，诸如文字、图形、音频和/或视频，其在此示例中可由Web服务器以超文本标记语言(“HTML”)、可扩展标记语言(“XML”)或另一适当的结构化语言的形式向用户供应。所有请求和响应的处理，以及内容在客户端装置2902与应用服务器2908之间的递送可由Web服务器处理。应理解，因为本文中论述的结构化代码可在如本文中

其它地方论述的任何适当的装置或主机上执行，所以Web和应用服务器不是必需的且仅为示例组件。

[0238] 数据存储2910可包括若干单独的数据表、数据库或用于存储与特定方面相关的数据的其它数据存储机构和介质。举例来说，所示的数据存储包括用于存储产生数据2912和用户信息2916的机构，其可用以为产生端供应内容。数据存储还示出为包括用于存储日志数据2914的机构，其可用于报告、分析或其它此类目的。应理解，可存在可需要存储在数据存储中的许多其它方面，诸如对于页面图像信息和访问权利信息，其可适当地存储在上文列出的机构中的任一者中或数据存储2910中的额外机构中。数据存储2910通过与其相关联的逻辑可操作以从应用服务器2908接收指令且响应于指令而获得、更新或另外处理数据。在一个示例中，用户可提交对某一类型的项目的搜索请求。在此状况下，数据存储可访问用户信息以验证用户的身份，且可访问目录详细信息以获得关于那个类型的项目的信息。信息接着可传回至用户，诸如在用户能够经由用户装置2902上的浏览器查看的Web页面上列出的结果中。所关注的特定项目的信息可在浏览器的专用页面或窗口中查看。

[0239] 每一服务器通常将包括提供用于那个服务器的一般管理和操作的可执行程序指令的操作系统，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)，所述指令在由服务器的处理器执行时允许服务器执行其希望的功能。用于操作系统的合适的实施方式和服务器的一般功能性是已知的或市售的，且易于由本领域技术人员尤其按照本文中的公开内容实施。在一些实施方案中，操作系统可根据一个或多个验证制度(诸如，评估保证等级(EAL)等级4)配置或在一个或多个验证制度下验证。

[0240] 在一个实施方案中的环境是利用若干计算机系统和组件的分布式计算环境，所述计算机系统和组件经由通信链路使用一个或多个计算机网络或直接连接互连。然而，本领域技术人员将了解，此系统可在具有比图29中所示的较少或较大数目的组件的系统中同样良好地操作。因此，图29中的系统2900的描绘在本质上应看作说明性的，而不限于本公开的范围。

[0241] 各种实施方案还可在广泛多种操作环境中实施，所述操作环境在一些状况下可包括可用以操作多个应用中的任一者的一个或多个用户计算机、计算装置或处理装置。用户或客户端装置可包括若干通用个人计算机(诸如运行标准的操作系统的台式或膝上型计算机)中的任一者，以及运行移动软件且能够支持若干网络连接和消息传递协议的蜂窝式、无线和手持式装置。此系统还可包括出于诸如开发和数据库管理的目的而运行多种市售操作系统和其它已知应用中的任一者的若干工作站。这些装置还可包括其它电子装置，诸如虚拟终端、瘦客户端、游戏系统和能够经由网络通信的其它装置。

[0242] 大多数实施方案利用对于本领域技术人员将为熟悉的至少一个网络以用于支持使用多种市售模型和协议中的任一者的通信，所述模型和协议诸如传输控制协议/因特网协议(“TCP/IP”)、开放式系统互连(“OSI”)、文件传送协议(“FTP”)、通用即插即用(“UpnP”)、网络文件系统(“NFS”)、公共因特网文件系统(“CIFS”)和AppleTalk。网络可以是(例如)局域网、广域网、虚拟专用网络、因特网、内联网、外联网、公共交换电话网络、红外线网络、无线网络和其任何组合。

[0243] 在利用Web服务器的实施方案中，Web服务器可运行多种服务器或中间层应用中的任一者，包括超文本传送协议(“HTTP”)服务器、FTP服务器、公共网关接口(“CGI”)服务器、

数据服务器、Java服务器和业务应用服务器。服务器也可能够响应于来自用户装置的请求而执行程序或脚本，诸如通过执行可实施为用任何编程语言(诸如Java®、C、C#或C++)或任何脚本语言(诸如Perl、Python或TCL)以及其组合编写的一个或多个脚本或程序的一个或多个Web应用。服务器还可包括数据库服务器，其包括(不限于)可从Oracle®、Microsoft®、Sybase®和IBM®购得的服务器。

[0244] 环境可包括如上文论述的多种数据存储以及其它存储器和存储介质。这些可驻存在多种位置，诸如驻存在计算机中的一者或多者本地的存储介质上(和/或驻存在在计算机中的一者或多者中)或驻存在跨越网络远离计算机中的任一者或全部的存储介质上。在实施方案的特定组中，信息可驻存在本领域技术人员熟悉的存储区域网(“SAN”)中。类似地，用于执行归于计算机、服务器或其它网络装置的功能的任何必要的文件可适当地在本地和/或远程地存储。在系统包括计算装置的情况下，每一此装置可包括可经由总线电耦合的硬件元件，元件包括(例如)至少一个中央处理单元(“CPU”)、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)。此系统还可包括一个或多个存储装置，诸如磁盘驱动器、光学存储装置和固态存储装置，诸如随机存取存储器(“RAM”)或只读存储器(“ROM”)以及可移动介质装置、存储卡、快闪卡等。本公开的各种实施方案还可使用定制硬件实施，定制硬件包括(但不限于)定制密码处理器、智能卡和/或硬件安全模块。

[0245] 此类装置还可包括如上文所描述的计算机可读存储介质读取器、通信装置(例如，调制解调器、网络卡(无线或有线)、红外线通信装置等)和工作存储器。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收纳计算机可读存储介质，计算机可读存储介质表示远程的、本地的、固定的和/或可移动存储装置以及用于暂时地和/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若干软件应用、模块、服务或其它元件，包括操作系统和应用程序，诸如客户端应用或Web浏览器。应了解，替代实施方案可具有与上文描述的众多变化。举例来说，也可使用定制硬件和/或特定元件可在硬件、软件(包括便携式软件，诸如小应用)或两者中实施。另外，可采用与其它计算装置(诸如网络输入/输出装置)的连接。

[0246] 用于含有代码或代码的部分的存储介质或计算机可读介质可包括本领域中已知或使用的任何适当的介质，包括存储介质和通信介质，诸如(但不限于)用任何方法或技术实施以用于存储和/或传输信息(诸如计算机可读指令、数据结构、程序模块或其它数据)的易失性和非易失性、可移动和不可移动介质，包括RAM、ROM、电可擦除可编程只读存储器(“EEPROM”)、快闪存储器或其它存储器技术、压缩光盘只读存储器(“CD-ROM”)、数字通用光盘(DVD)或其它光学存储器、磁带盒、磁带、磁盘存储器或其它磁性存储装置或可用以存储所要信息且可由系统装置访问的任何其它介质。基于本文中提供的公开内容和教示，本领域技术人员将了解实施各种实施方案的其它方式和/或方法。

[0247] 因此，说明书和图式应按照说明性的而不是限制性的意义看待。然而，将清楚的是，可在不脱离如权利要求书中阐述的本发明的较宽精神和范围的情况下对本发明进行各种修改和改变。

[0248] 其它变化在本公开的精神内。因此，尽管所公开的技术易于经受各种修改和替代构造，但某些说明的实施方案在图式中进行示出且已在上文详细地描述。然而，应理解，不

希望将本发明限于公开的一个或多个特定形式，而是相反，本发明将涵盖落在如所附权利要求书中定义的本发明的精神和范围内的所有修改、替代构造和等效物。

[0249] 除非本文中另外指示或清楚地与上下文矛盾，否则在描述公开的实施方案的上下文中(尤其在所附权利要求书的上下文中)使用术语“一(a/an)”和“所述”以及类似指代物将解释为涵盖单数和复数两者。除非另外指出，否则术语“包括(comprising)”、“具有”、“包括(including)”和“含有”将解释为开放术语(即，意味着“包括但不限于”)。术语“连接的”将解释为部分或完全含有于其内、附接至或接合在一起，即使存在插入的某物。除非本文中另外指示，否则对本文中值的范围的陈述仅希望充当个别地参考落在范围内的每一单独值的简写方法，且每一单独值并入至说明书中就像其在本文中个别地陈述一样。除非本文中另外指示或另外清楚地与上下文矛盾，否则本文中描述的所有方法可用任何合适的次序执行。本文中提供的任何和所有示例或示范性语言(例如，“诸如”)的使用仅希望较好地阐明本发明的实施方案且不限制本发明的范围，除非另外要求。本说明书中的语言不应解释为将任何非要求的元件指示为对于本发明的实践是必要的。

[0250] 本文中描述了本公开的优选实施方案，包括用于执行本发明的发明者已知的最佳模式。在阅读以上描述后，那些优选实施方案的变化对于本领域技术人员可变得清楚。发明者预期本领域技术人员适当地采用此类变化，且发明者希望与本文中特定地描述不同地实践本发明。因此，本发明包括如由适用法律准许的附加至本发明的权利要求书中陈述的主题的所有修改和等效物。此外，除非本文中另外指示或另外清楚地与上下文矛盾，否则本发明涵盖在其所有可能的变化中的上述元件的任何组合。

[0251] 本文中引用的所有参考物(包括公告、专利申请和专利)特此以引用的方式并入，其并入程度如同每一参考个别地和特定地指示为以引用的方式并入且全部在本文中阐述。

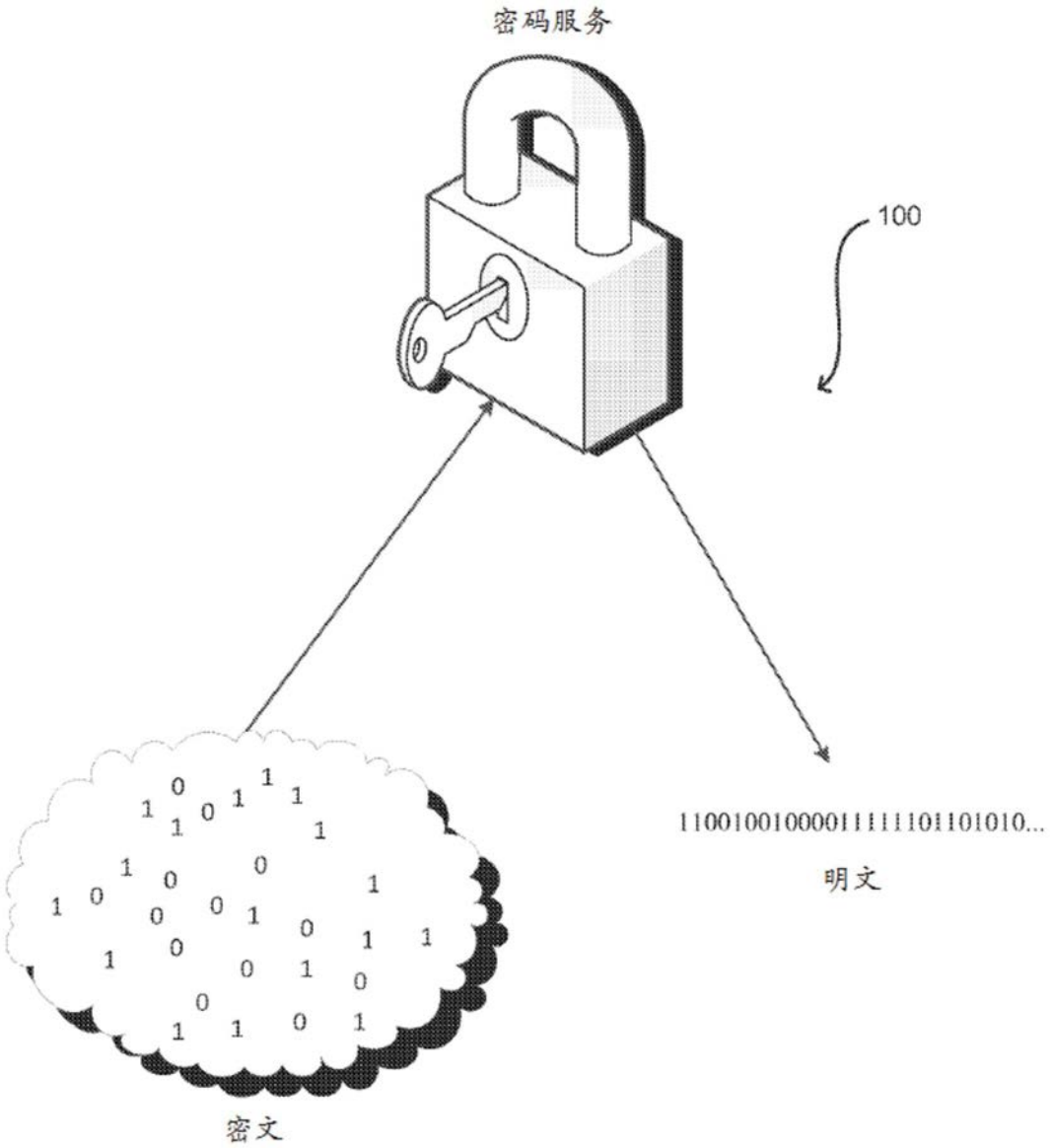


图1

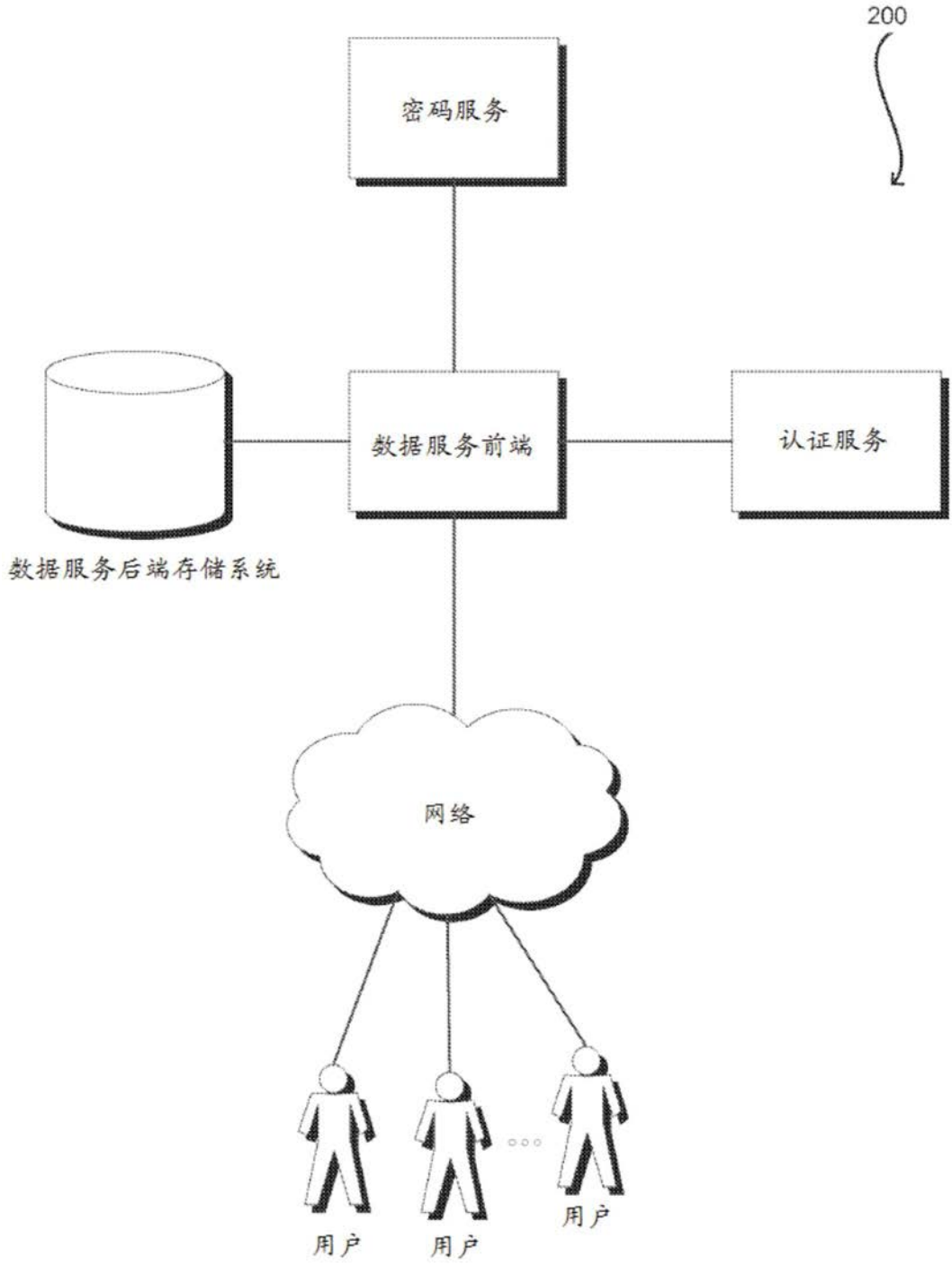


图2

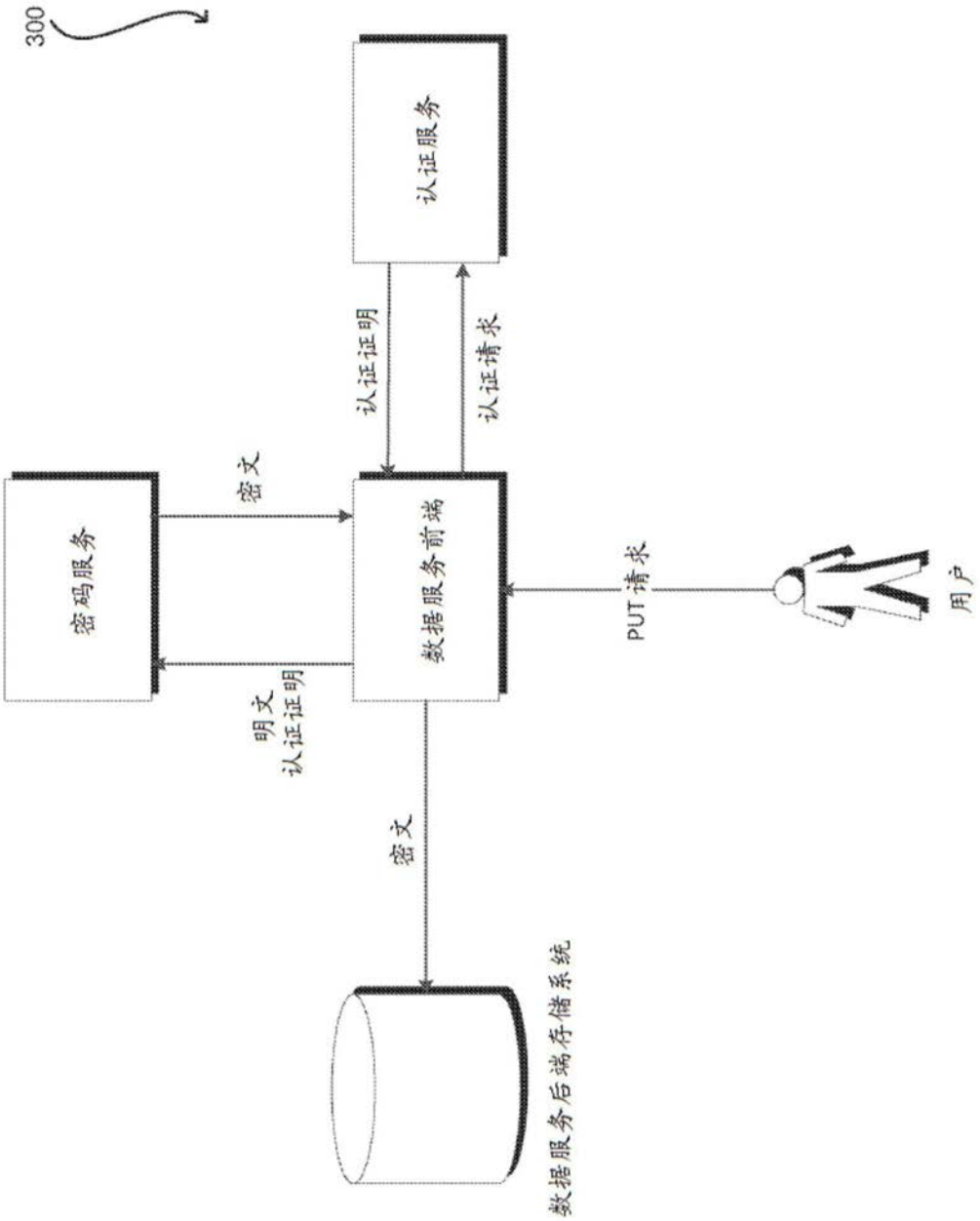

300
认证服务
认证证明
认证请求
密文
密码服务
数据服务前端
PUT 请求
用户
明文
认证证明
密文
数据服务后端存储系统

图3

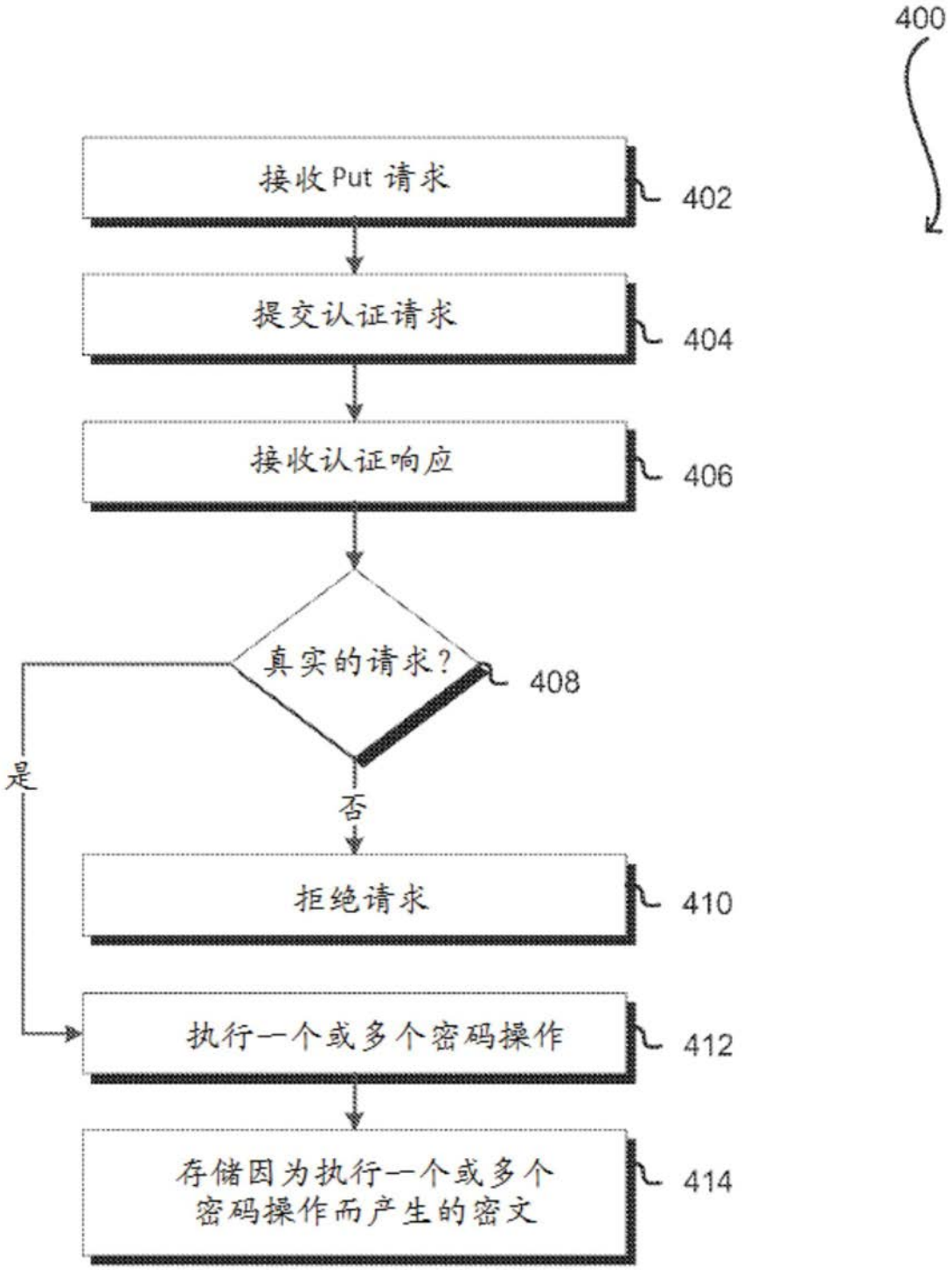

400
接收Put请求
402
提交认证请求
404
接收认证响应
406
真实的请求?
408
是
否
拒绝请求
410
执行一个或多个密码操作
412
存储因为执行一个或多个密码操作而产生的密文
414

图4

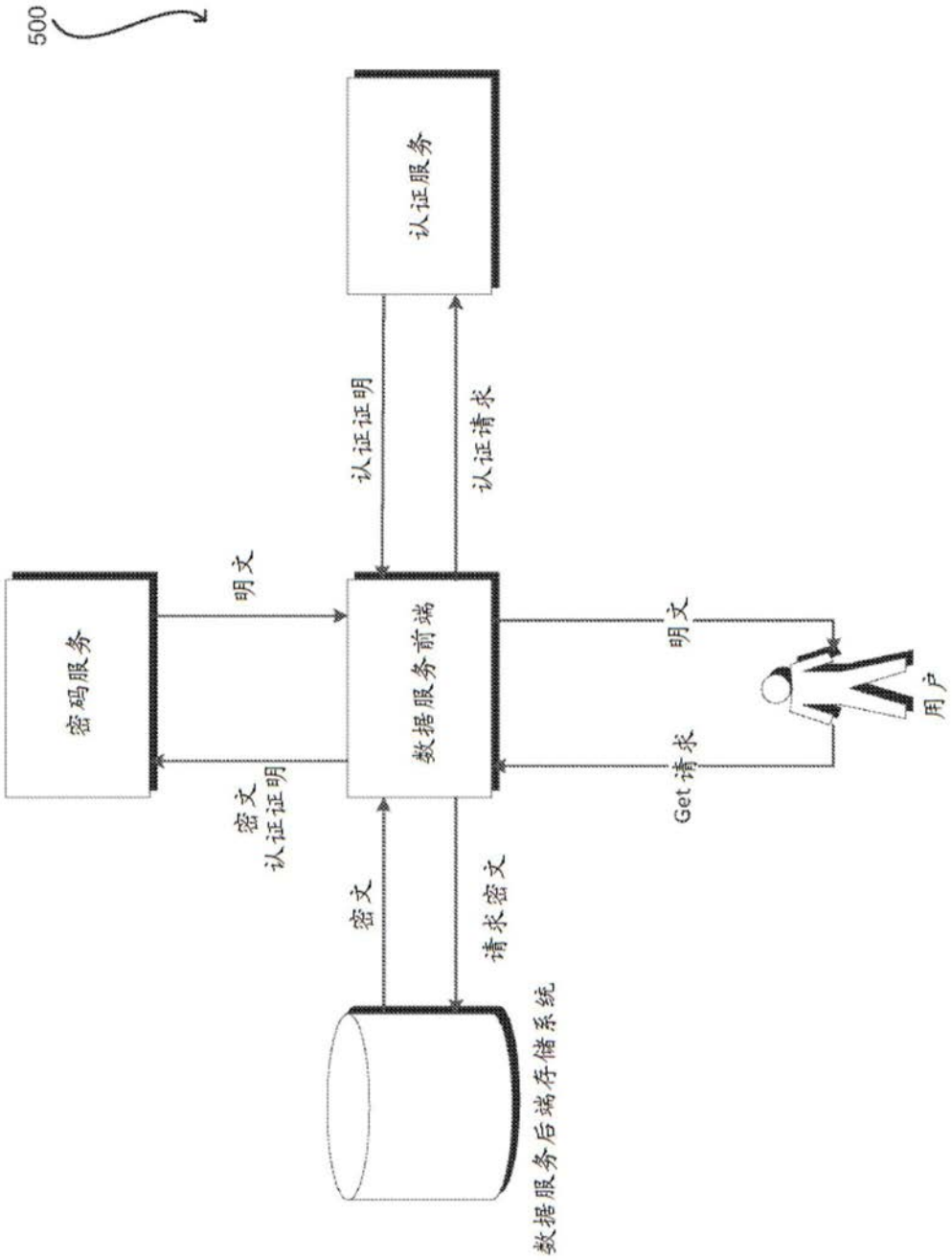

500
认证服务
认证证明
认证请求
密码服务
明文
数据服务前端
明文
用户
密文
认证证明
Get 请求
密文
请求密文
数据服务后端存储系统

图5

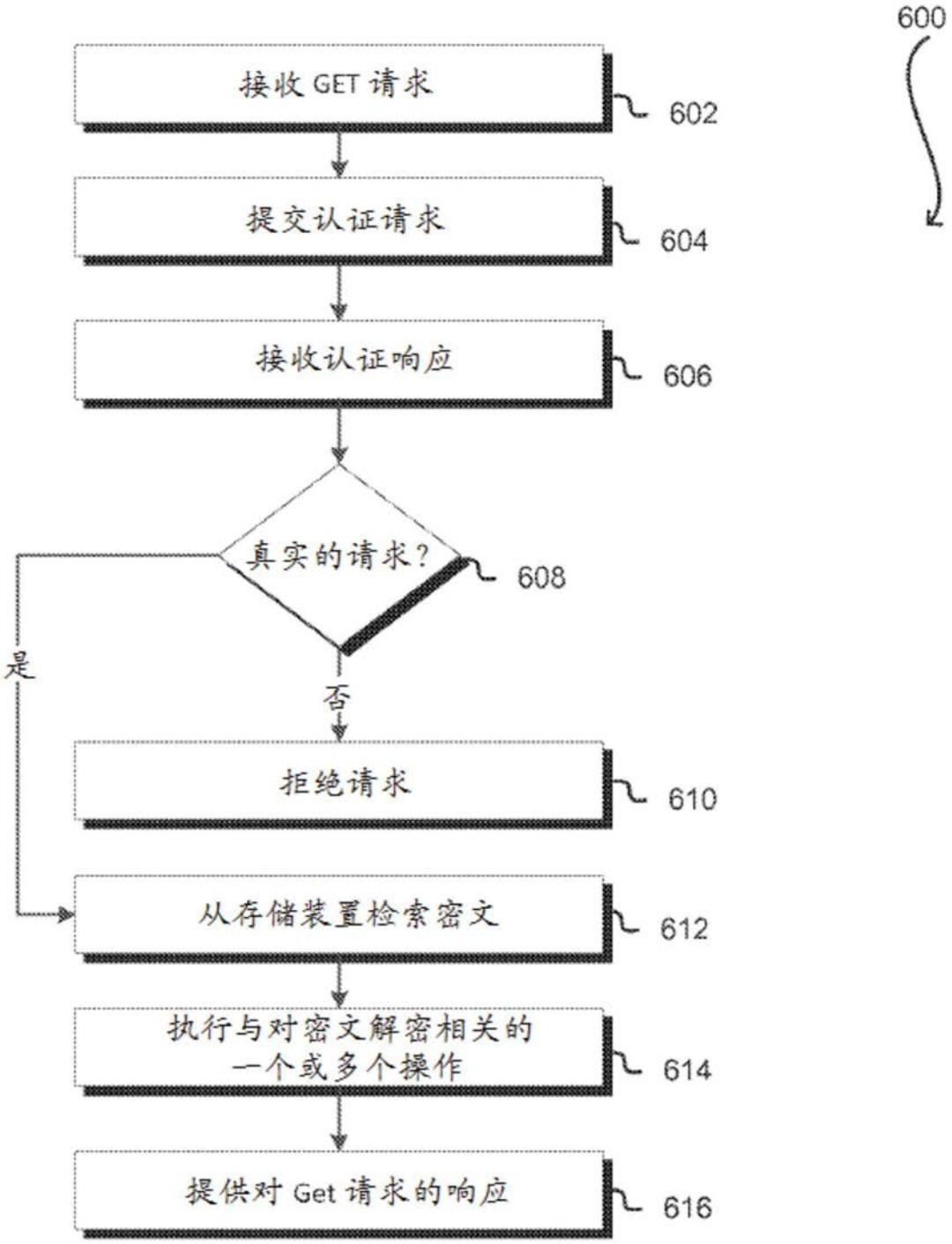

600
接收 GET 请求
602
提交认证请求
604
接收认证响应
606
真实的请求?
608
是
否
拒绝请求
610
从存储装置检索密文
612
执行与对密文解密相关的一个或多个操作
614
提供对 Get 请求的响应
616

图6

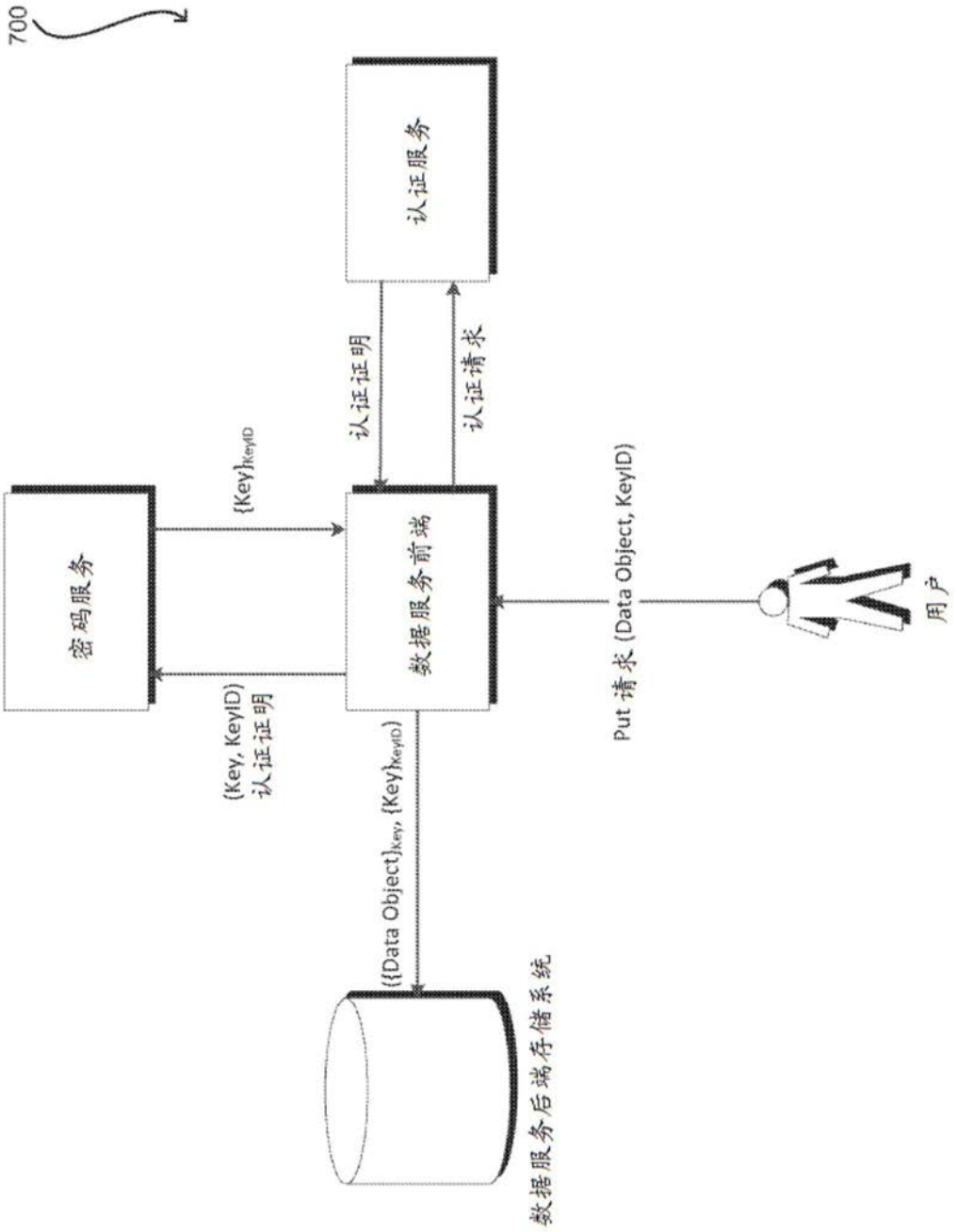

700
认证服务
认证证明
认证请求
{Key}KeyID
密码服务
数据服务前端
用户
Put 请求 (Data Object, KeyID)
(Key, KeyID)
认证证明
{{Data Object}Key, {Key}KeyID}
数据服务后端存储系统

图7

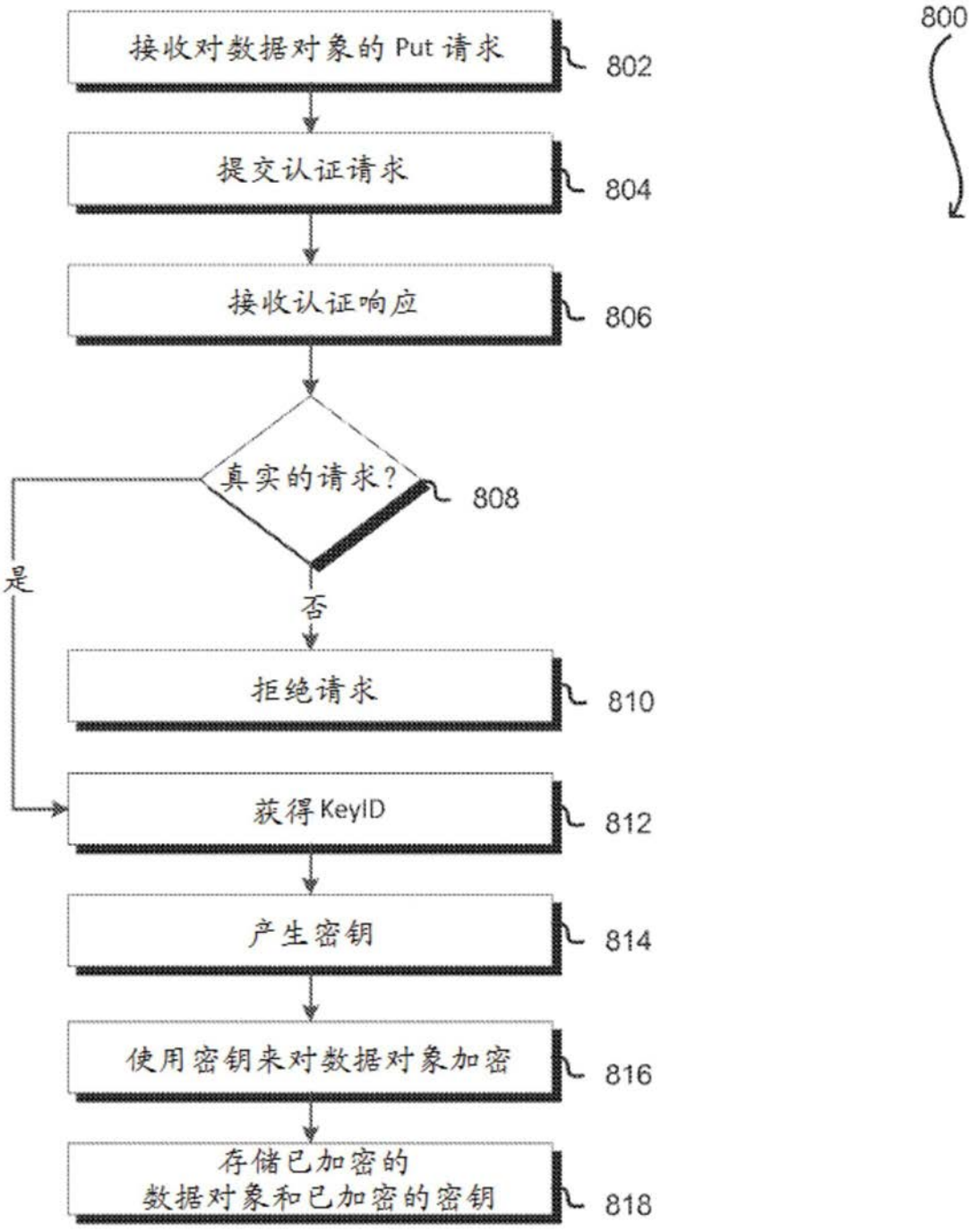

800
接收对数据对象的 Put 请求
802
提交认证请求
804
接收认证响应
806
真实的请求?
808
是
否
拒绝请求
810
获得 KeyID
812
产生密钥
814
使用密钥来对数据对象加密
816
存储已加密的
数据对象和已加密的密钥
818

图8

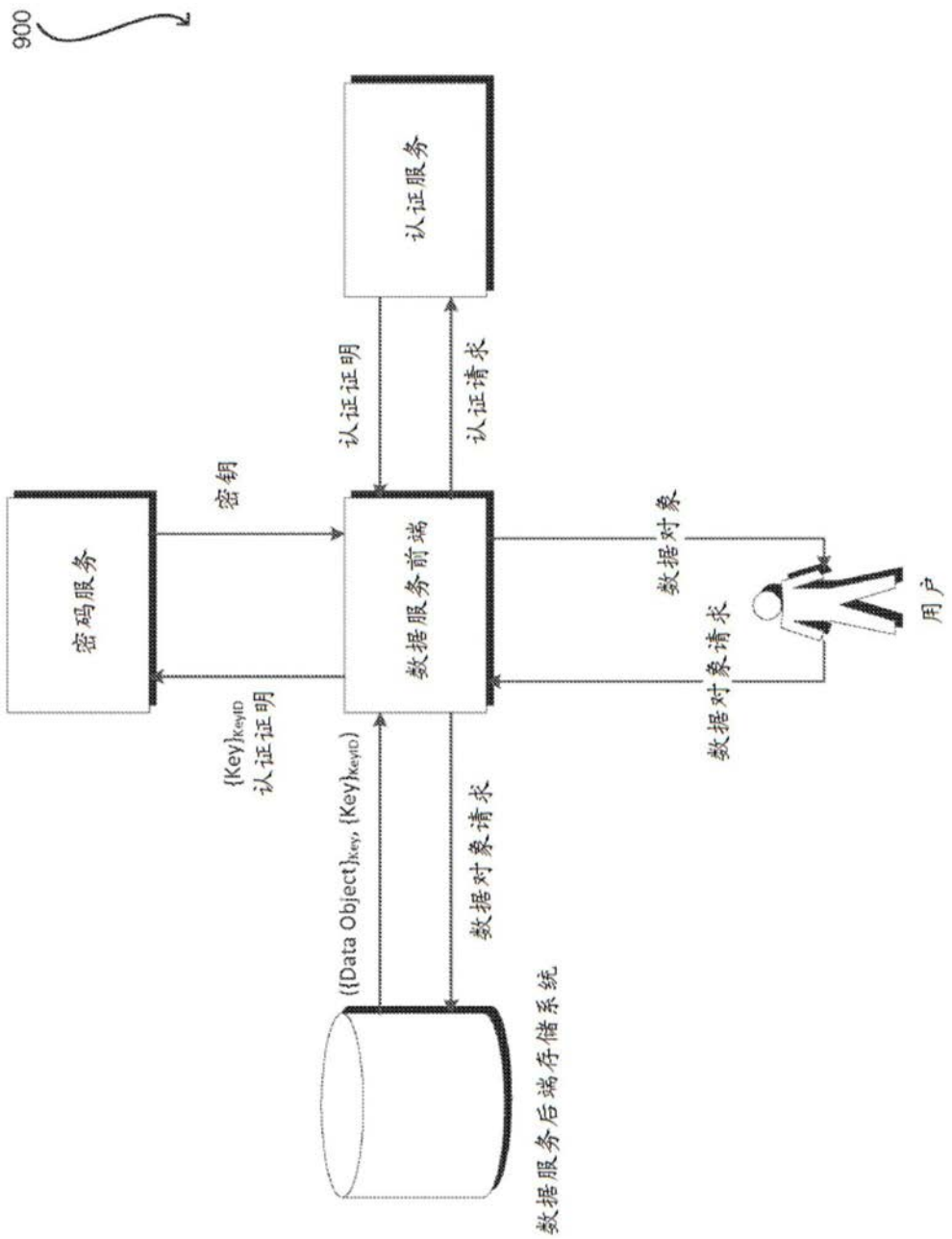

900
认证服务
认证证明
认证请求
密钥
密码服务
数据服务前端
数据对象
数据对象请求
用户
{Key}KeyID
认证证明
{{Data Object}Key, {Key}KeyID}
数据对象请求
数据服务后端存储系统

图9

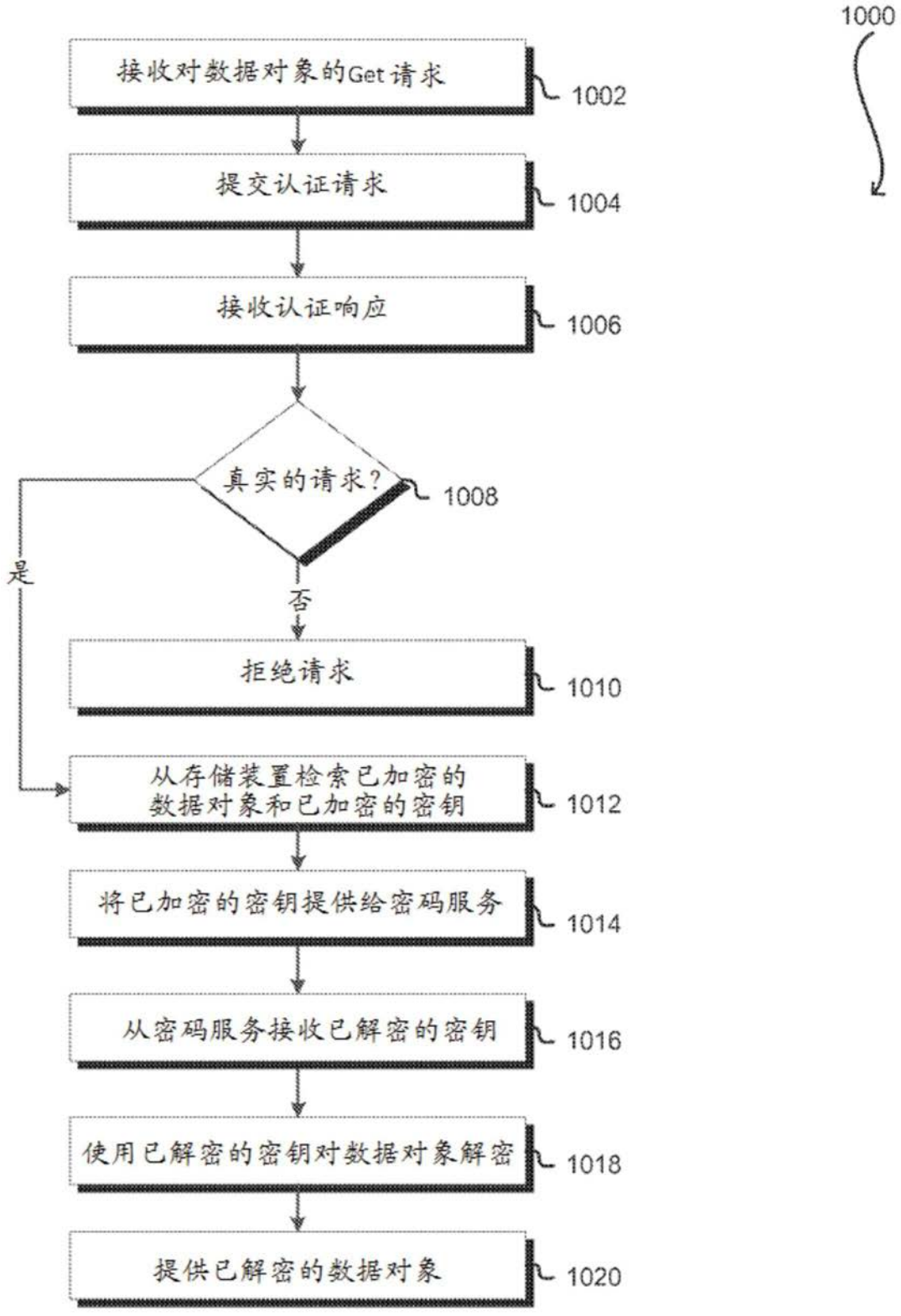

1000
接收对数据对象的Get请求
1002
提交认证请求
1004
接收认证响应
1006
真实的请求?
1008
是
否
拒绝请求
1010
从存储装置检索已加密的
数据对象和已加密的密钥
1012
将已加密的密钥提供给密码服务
1014
从密码服务接收已解密的密钥
1016
使用已解密的密钥对数据对象解密
1018
提供已解密的数据对象
1020

图10

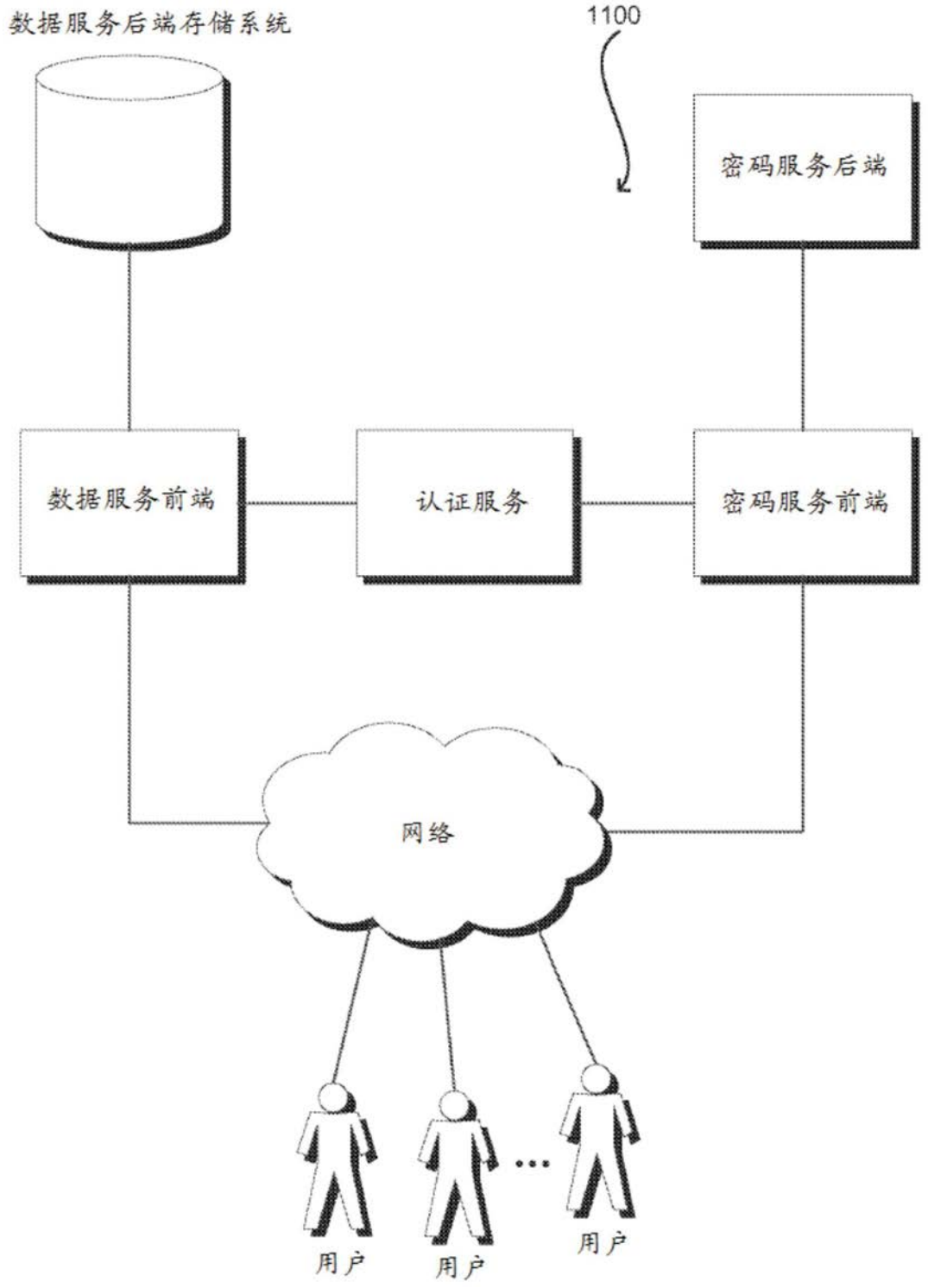


图11

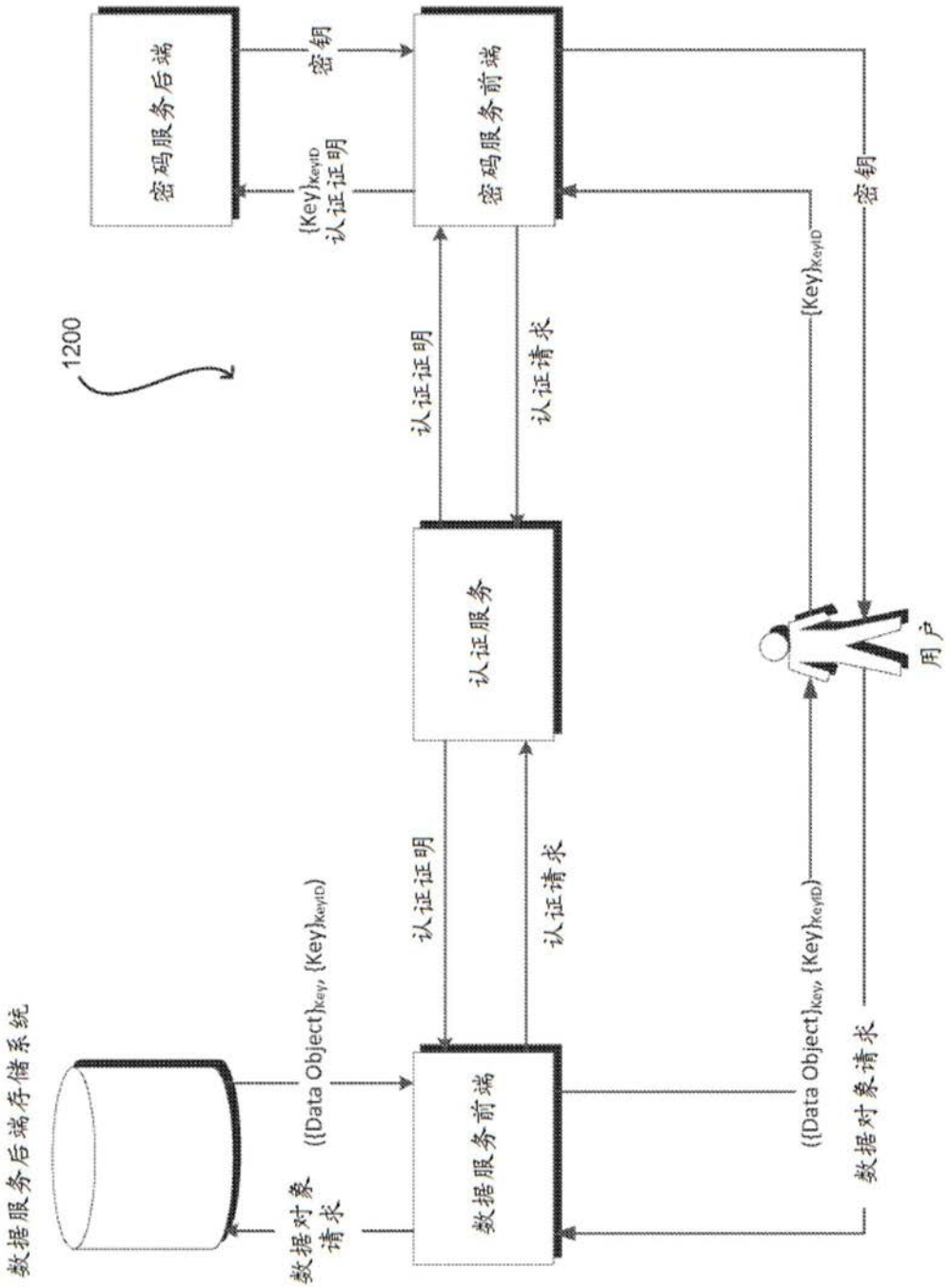

密码服务后端
密钥
{Key}KeyID
认证证明
密码服务前端
1200
认证证明
认证请求
{Key}KeyID
密钥
认证服务
用户
认证证明
认证请求
数据服务后端存储系统
{{Data Object}key, {Key}KeyID}
数据对象
请求
数据服务前端
{{Data Object}key, {Key}KeyID}
数据对象请求

图12

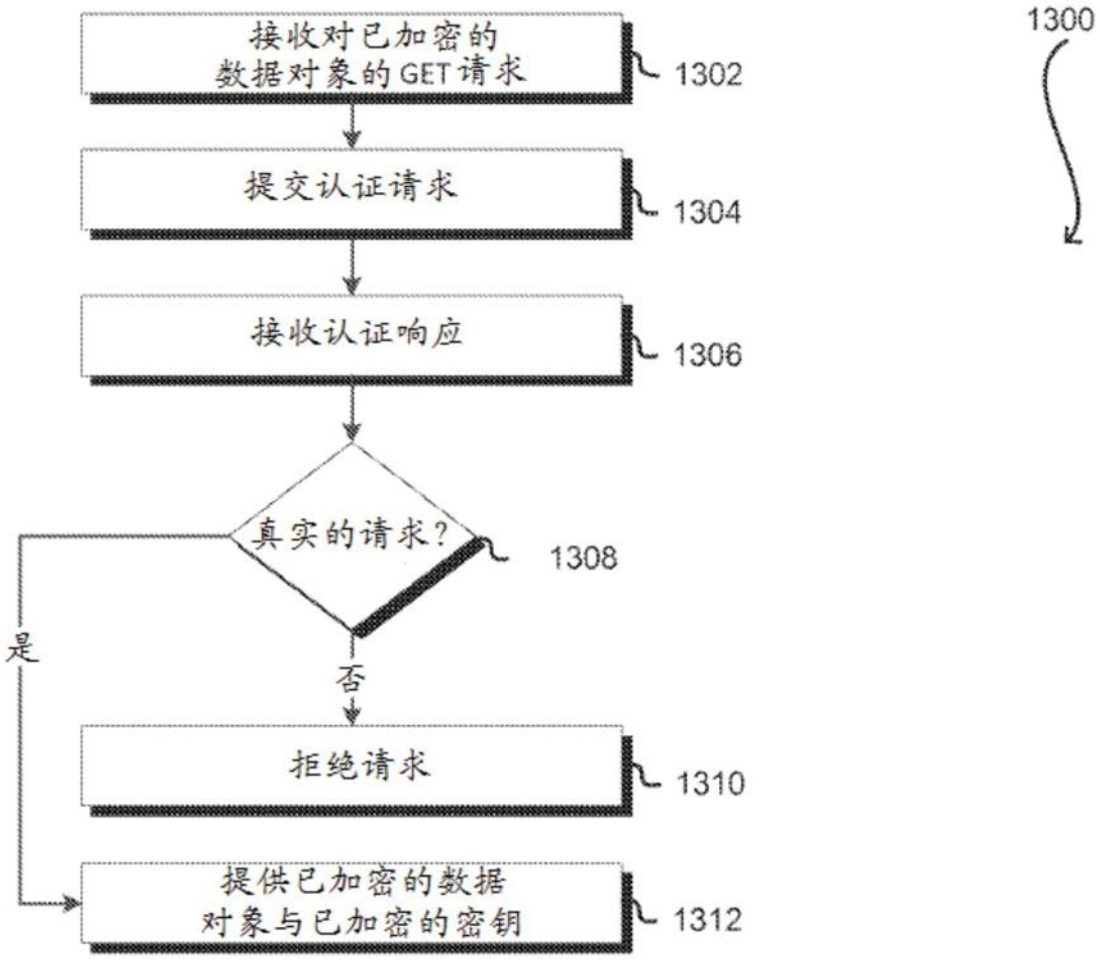

1300
接收对已加密的数据对象的GET请求
1302
提交认证请求
1304
接收认证响应
1306
真实的请求?
1308
是
否
拒绝请求
1310
提供已加密的数据对象与已加密的密钥
1312

图13

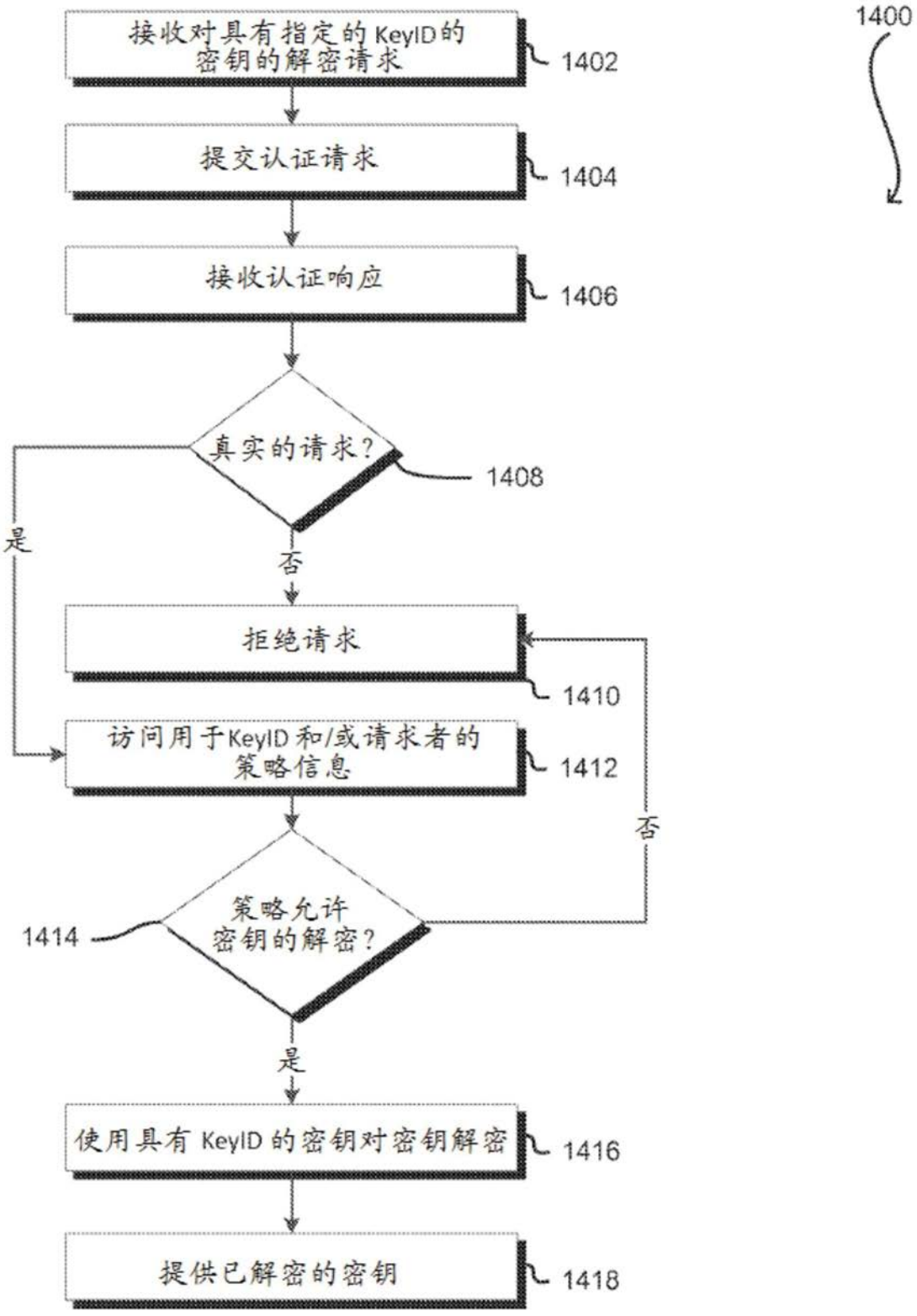

1400
接收对具有指定的KeyID的密钥的解密请求
1402
提交认证请求
1404
接收认证响应
1406
真实的请求?
1408
是
否
拒绝请求
1410
访问用于KeyID和/或请求者的策略信息
1412
否
策略允许密钥的解密?
1414
是
使用具有KeyID的密钥对密钥解密
1416
提供已解密的密钥
1418

图14

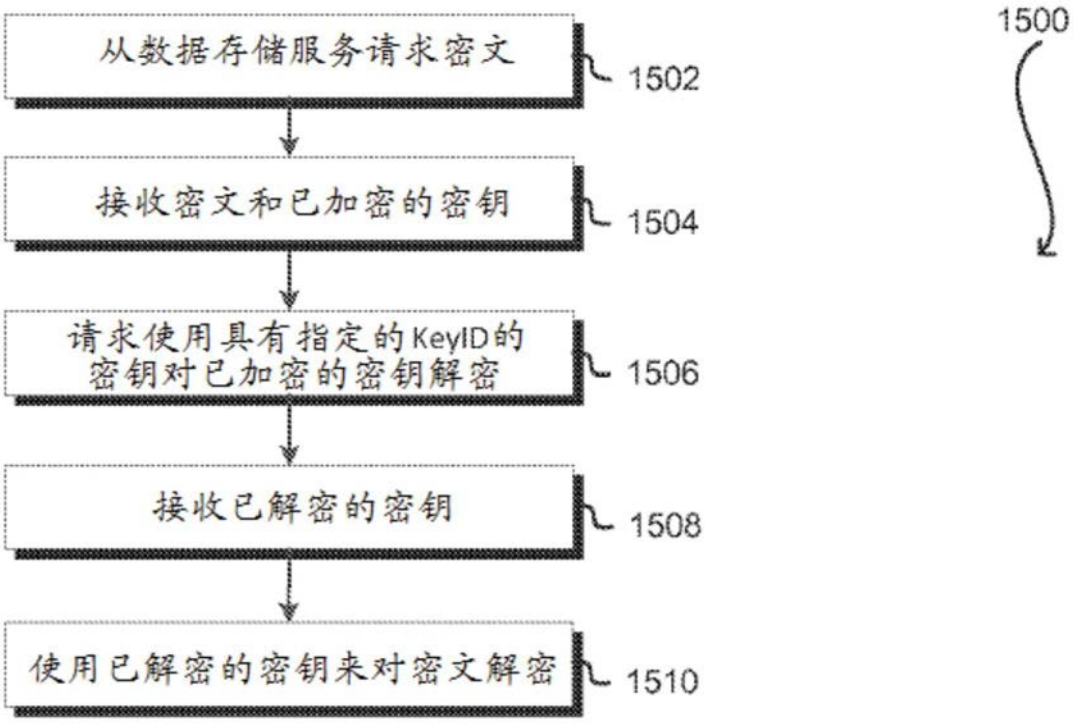

1500
从数据存储服务请求密文
1502
接收密文和已加密的密钥
1504
请求使用具有指定的KeyID的密钥对已加密的密钥解密
1506
接收已解密的密钥
1508
使用已解密的密钥来对密文解密
1510

图15

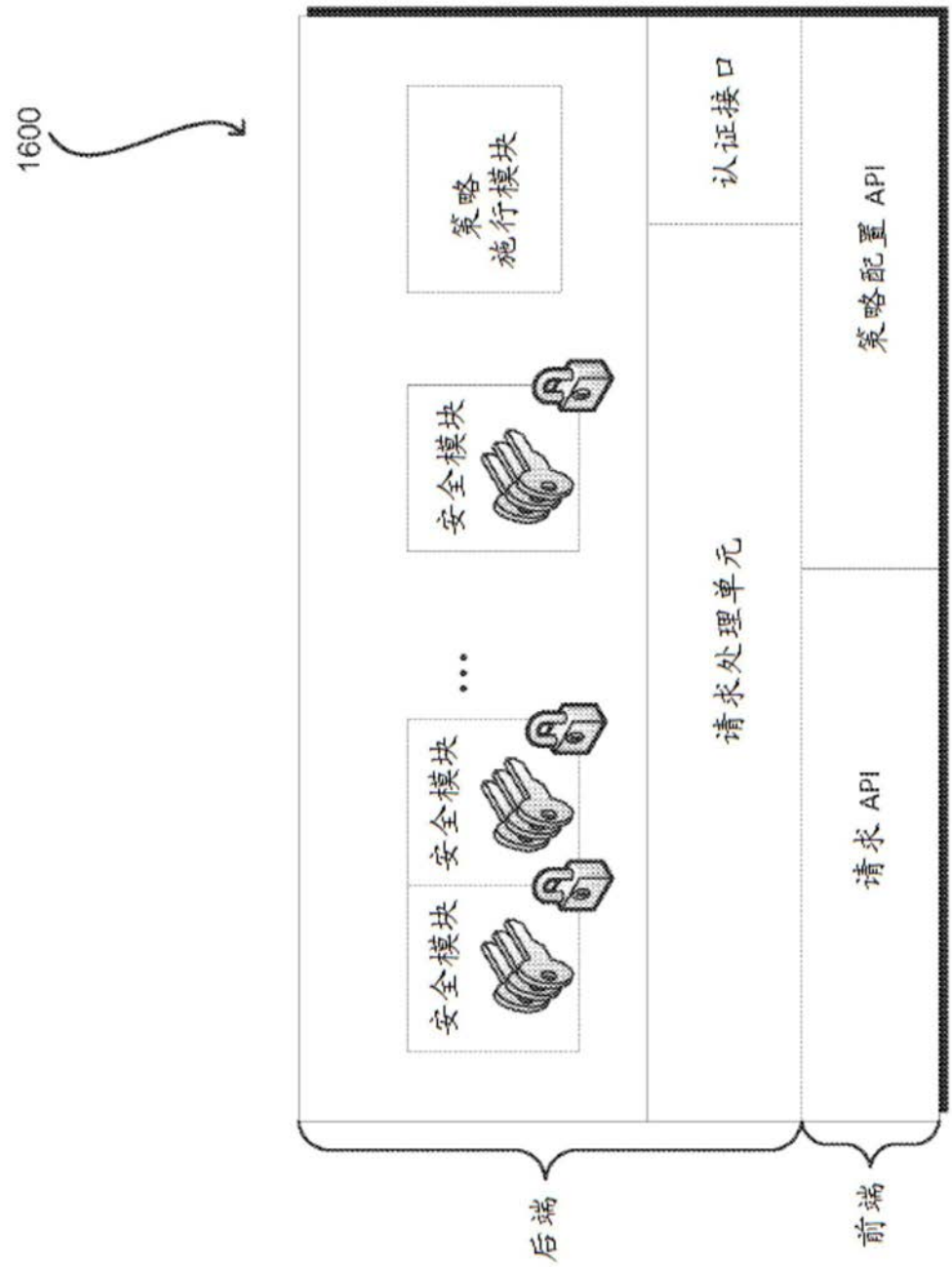


图16

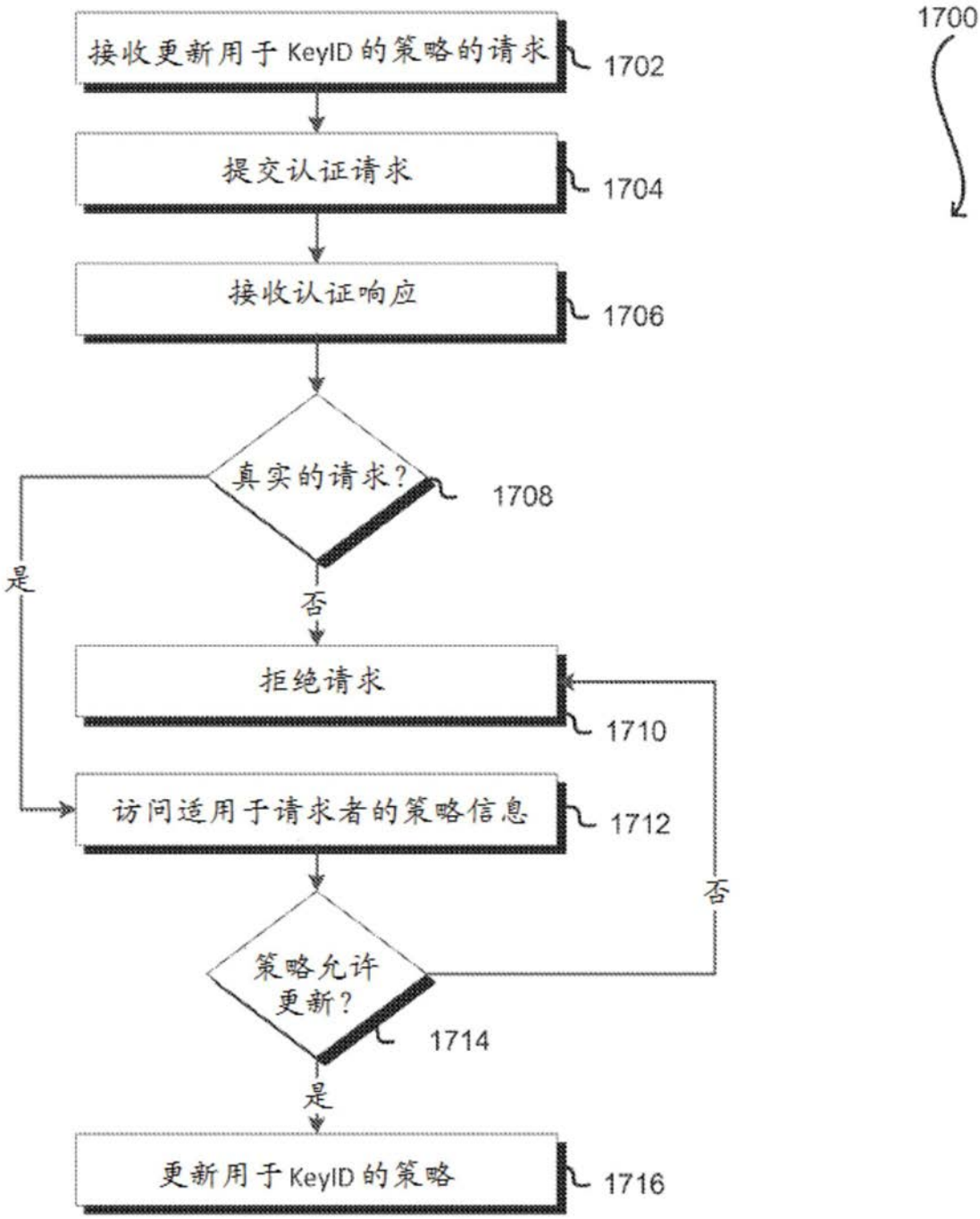

1700
接收更新用于 KeyID 的策略的请求
1702
提交认证请求
1704
接收认证响应
1706
真实的请求?
1708
是
否
拒绝请求
1710
访问适用于请求者的策略信息
1712
否
策略允许更新?
1714
是
更新用于 KeyID 的策略
1716

图17

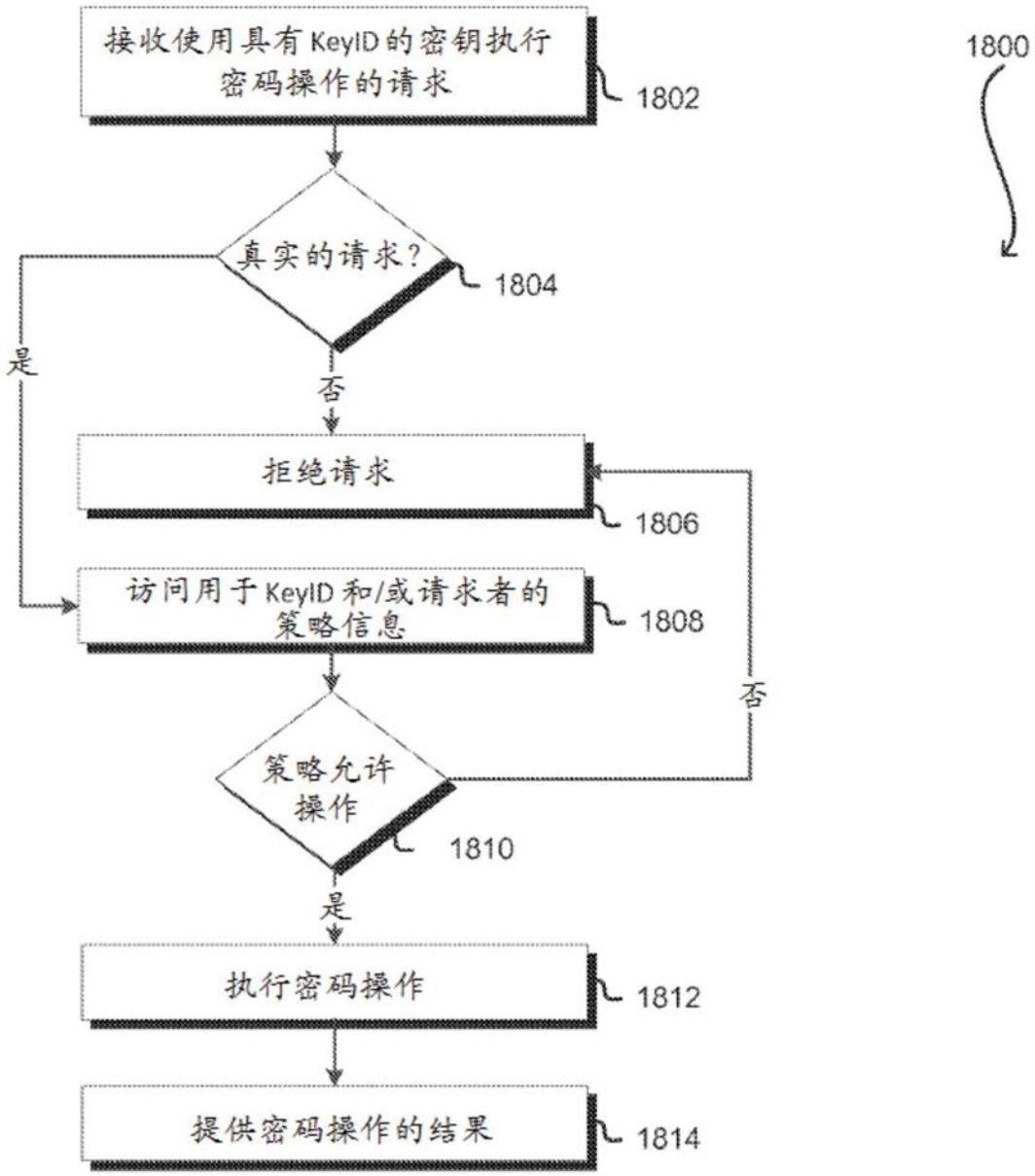

接收使用具有KeyID的密钥执行密码操作的请求
1802
1800
真实的请求?
1804
是
否
拒绝请求
1806
访问用于KeyID和/或请求者的策略信息
1808
否
策略允许操作
1810
是
执行密码操作
1812
提供密码操作的结果
1814

图18

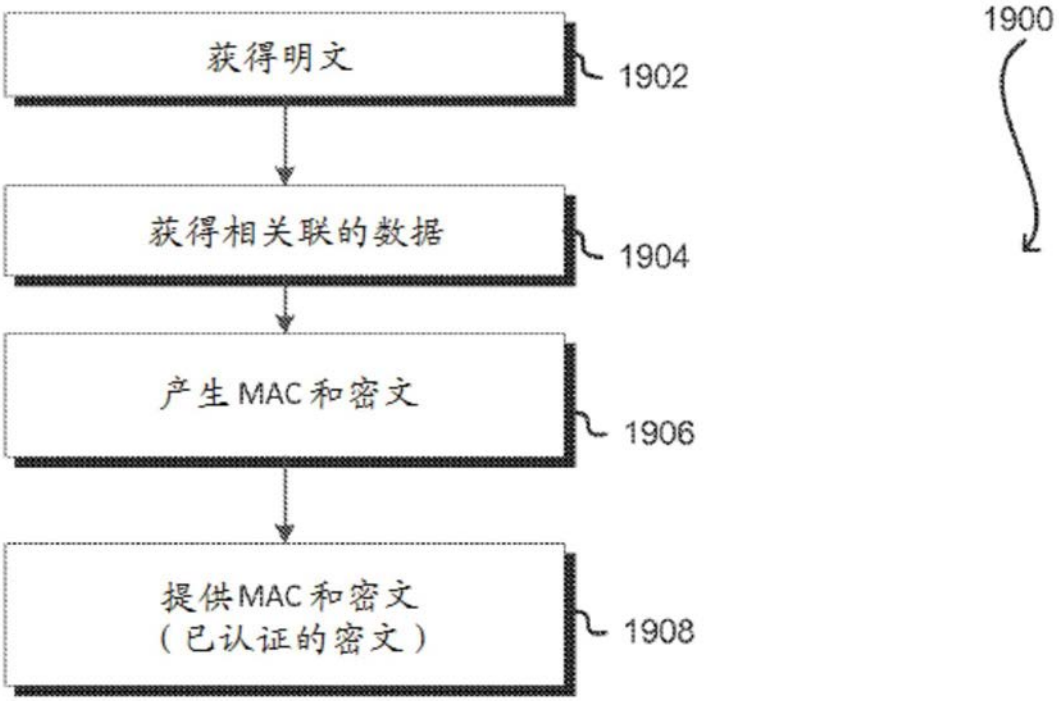

1900
获得明文
1902
获得相关联的数据
1904
产生MAC和密文
1906
提供MAC和密文
（已认证的密文）
1908

图19

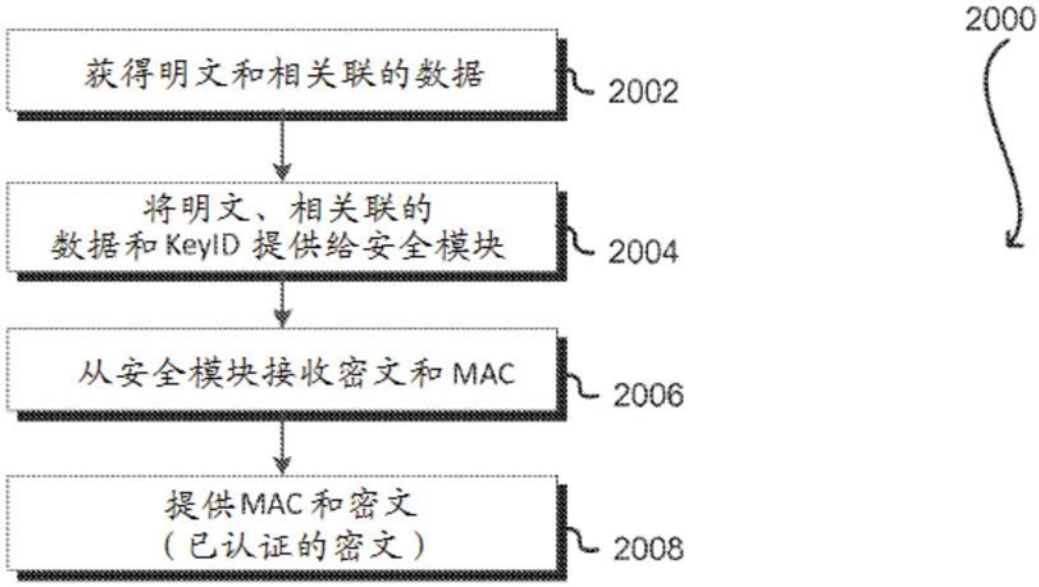

2000
获得明文和相关联的数据
2002
将明文、相关联的
数据和KeyID提供给安全模块
2004
从安全模块接收密文和MAC
2006
提供MAC和密文
（已认证的密文）
2008

图20

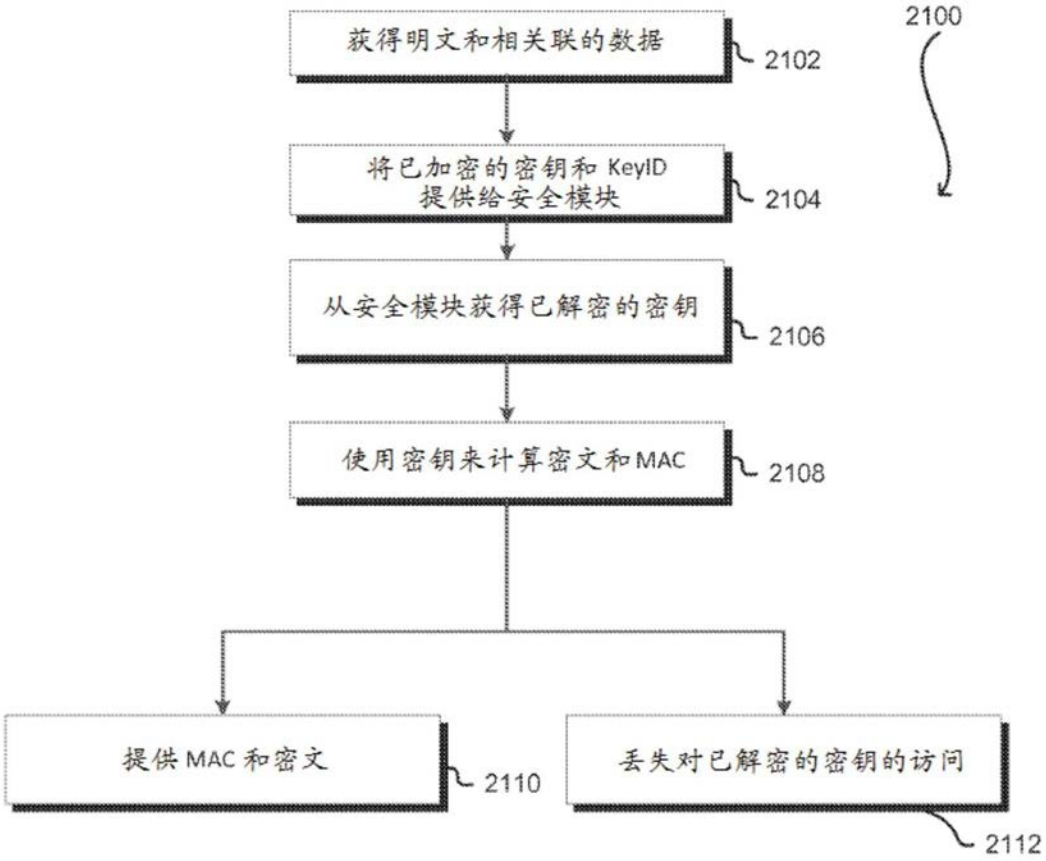

2100
获得明文和相关联的数据
2102
将已加密的密钥和 KeyID
提供给安全模块
2104
从安全模块获得已解密的密钥
2106
使用密钥来计算密文和MAC
2108
提供 MAC 和密文
2110
丢失对已解密的密钥的访问
2112

图21

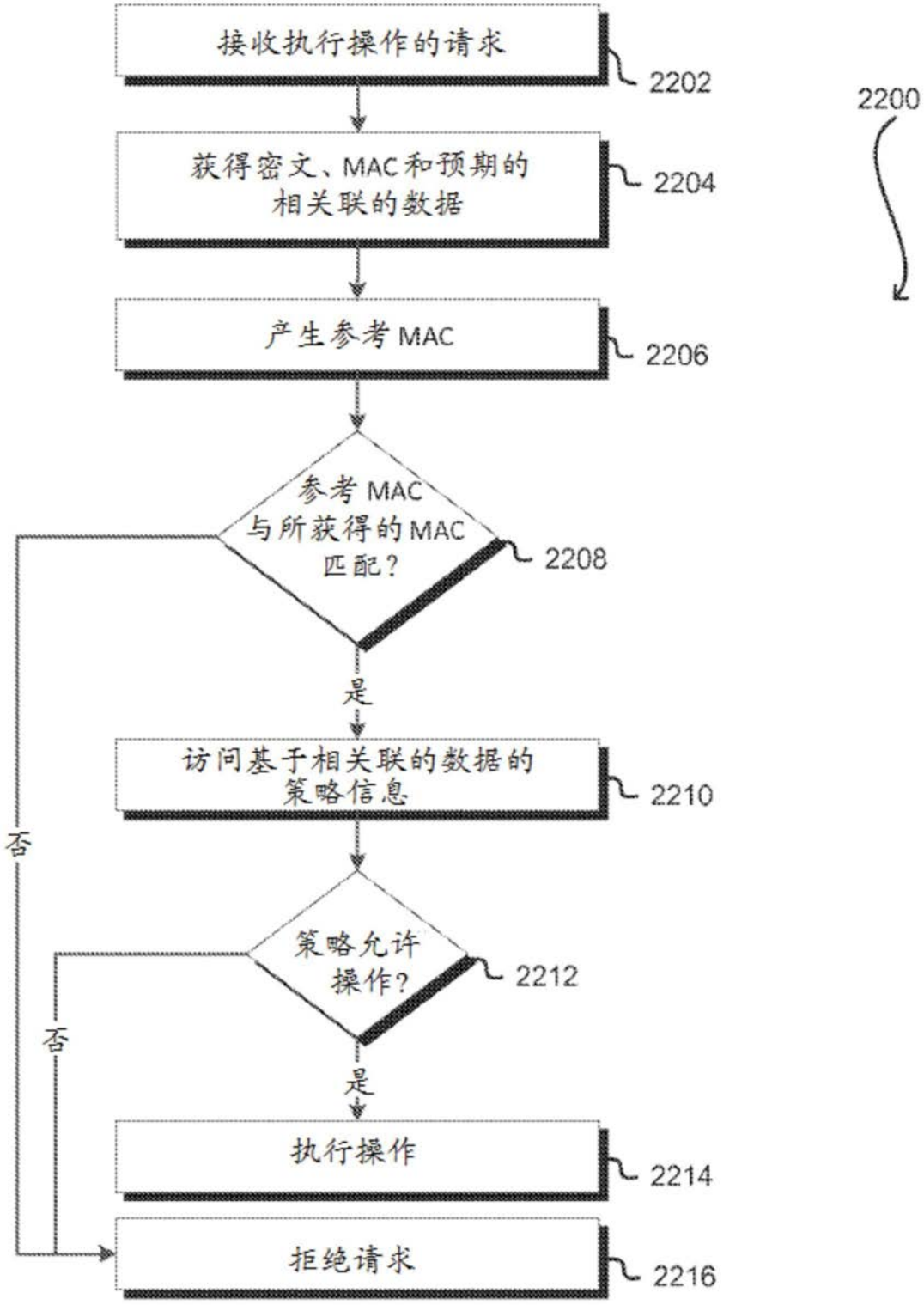

接收执行操作的请求
2202
2200
获得密文、MAC和预期的相关联的数据
2204
产生参考MAC
2206
参考MAC与所获得的MAC匹配？
2208
是
否
访问基于相关联的数据的策略信息
2210
策略允许操作？
2212
否
是
执行操作
2214
拒绝请求
2216

图22

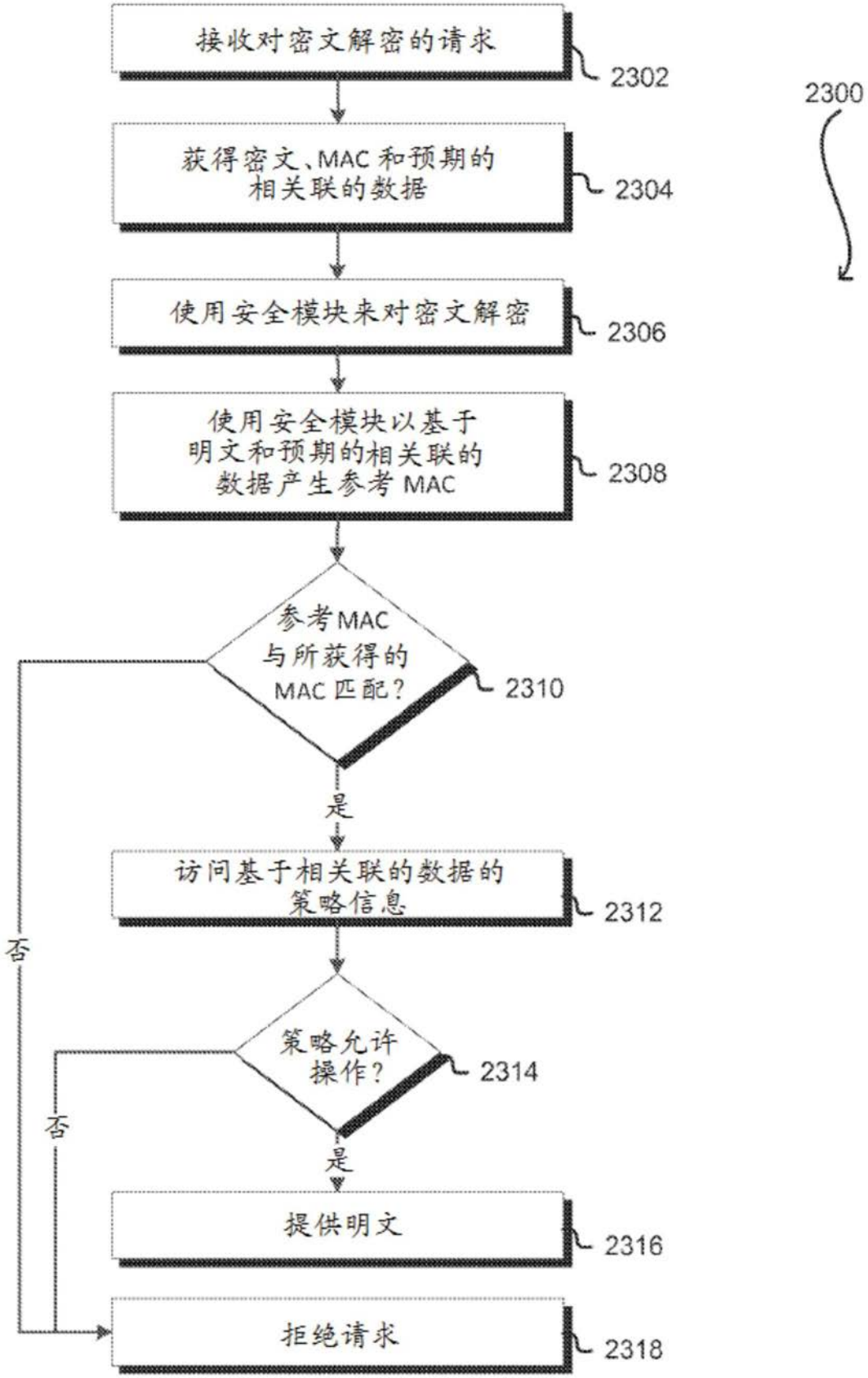

接收对密文解密的请求
2302
2300
获得密文、MAC 和预期的相关联的数据
2304
使用安全模块来对密文解密
2306
使用安全模块以基于明文和预期的相关联的数据产生参考 MAC
2308
参考 MAC 与所获得的 MAC 匹配？
2310
是
否
访问基于相关联的数据的策略信息
2312
策略允许操作？
2314
是
否
提供明文
2316
拒绝请求
2318

图23

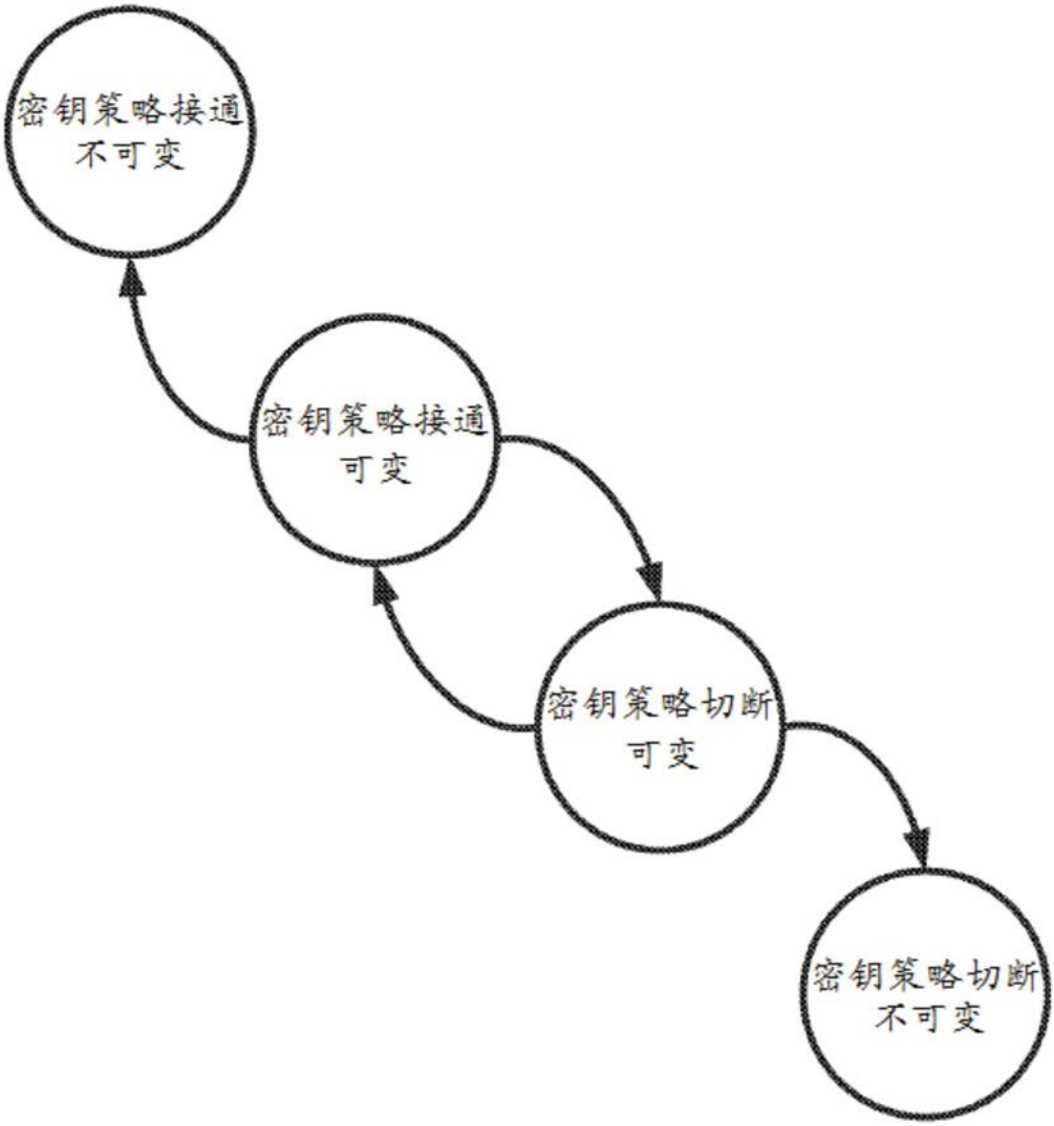


图24

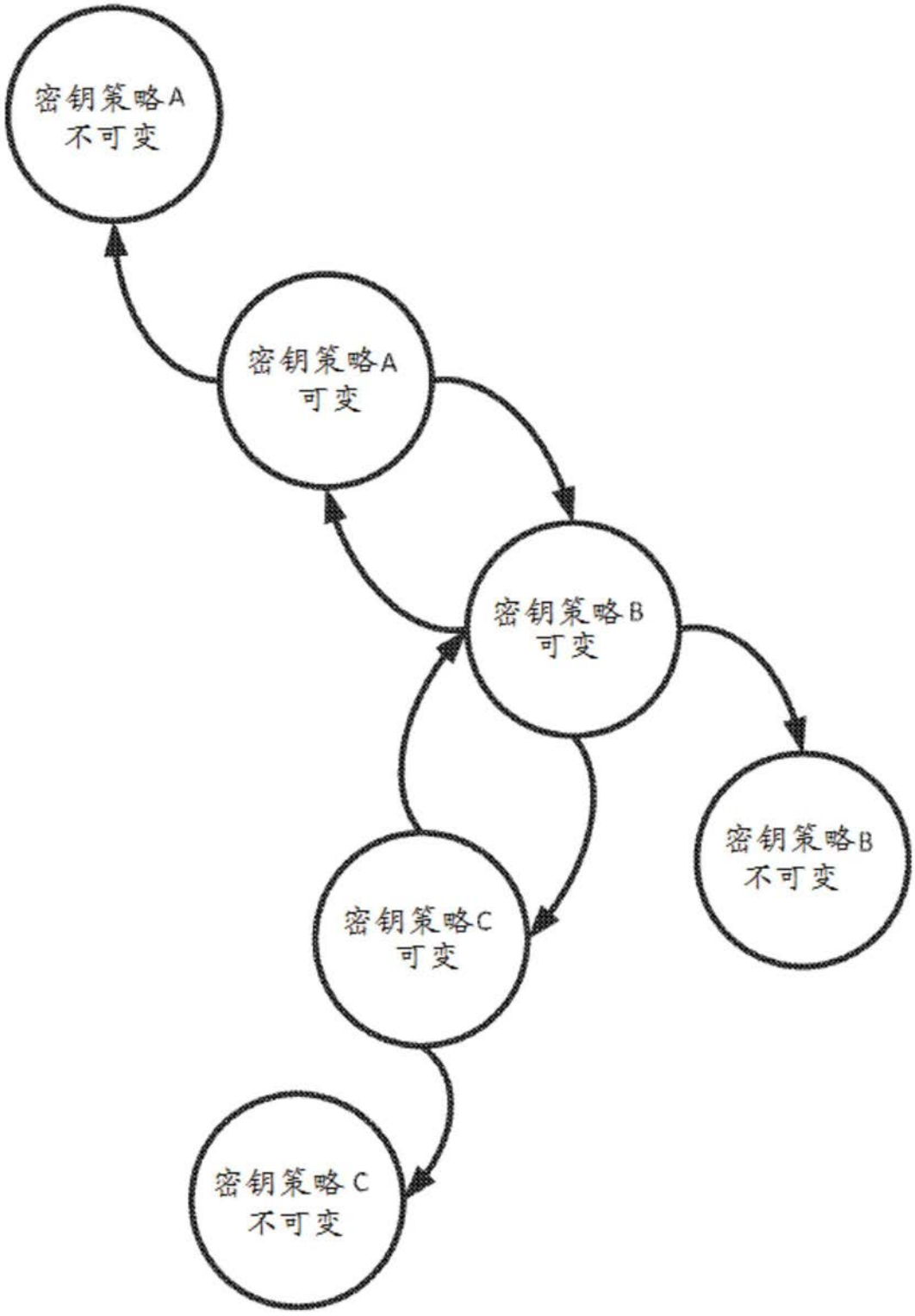


图25

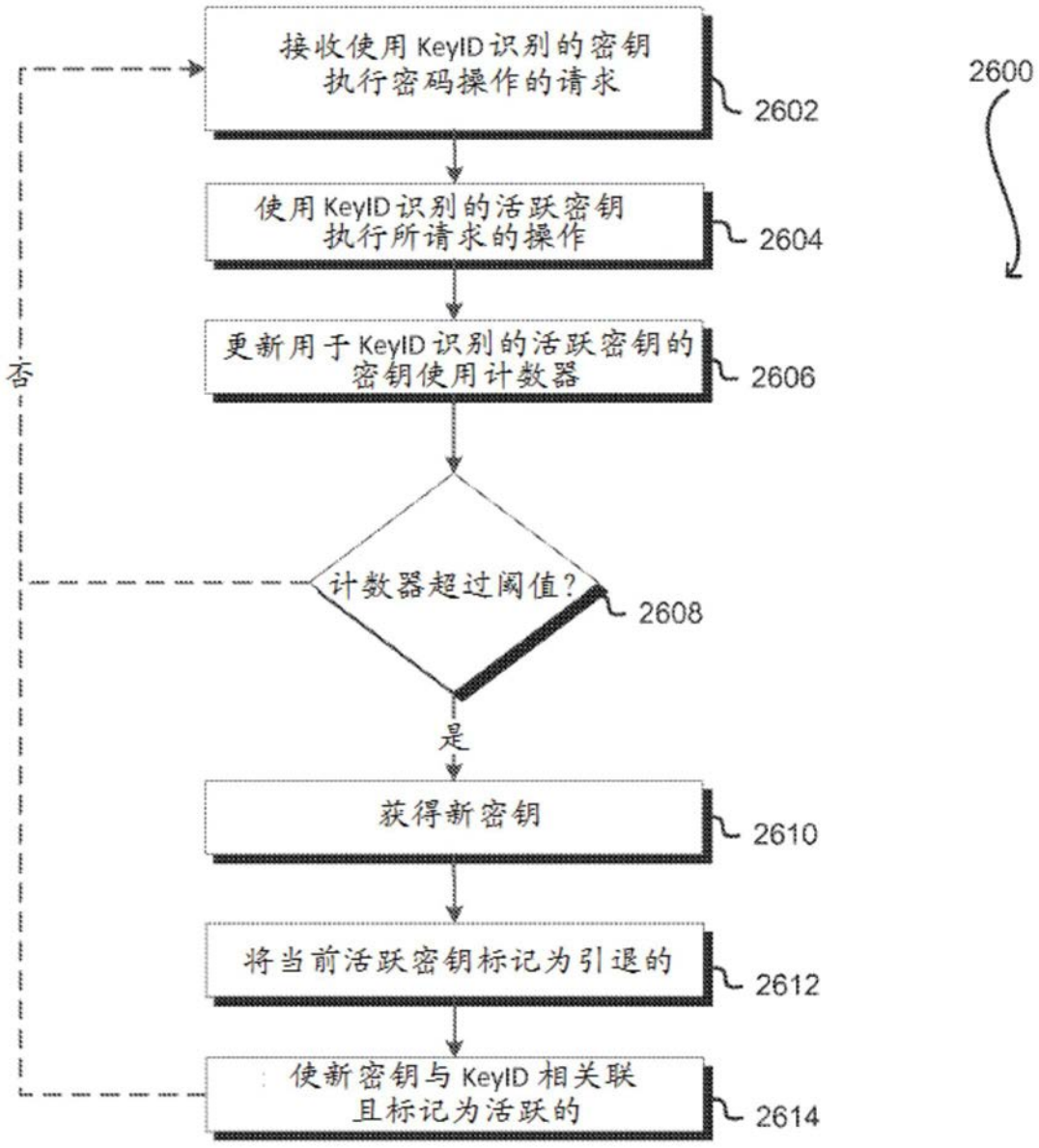

接收使用 KeyID 识别的密钥执行密码操作的请求
2602
使用 KeyID 识别的活跃密钥执行所请求的操作
2604
更新用于 KeyID 识别的活跃密钥的密钥使用计数器
2606
计数器超过阈值?
2608
否
是
获得新密钥
2610
将当前活跃密钥标记为引退的
2612
使新密钥与 KeyID 相关联且标记为活跃的
2614
2600

图26

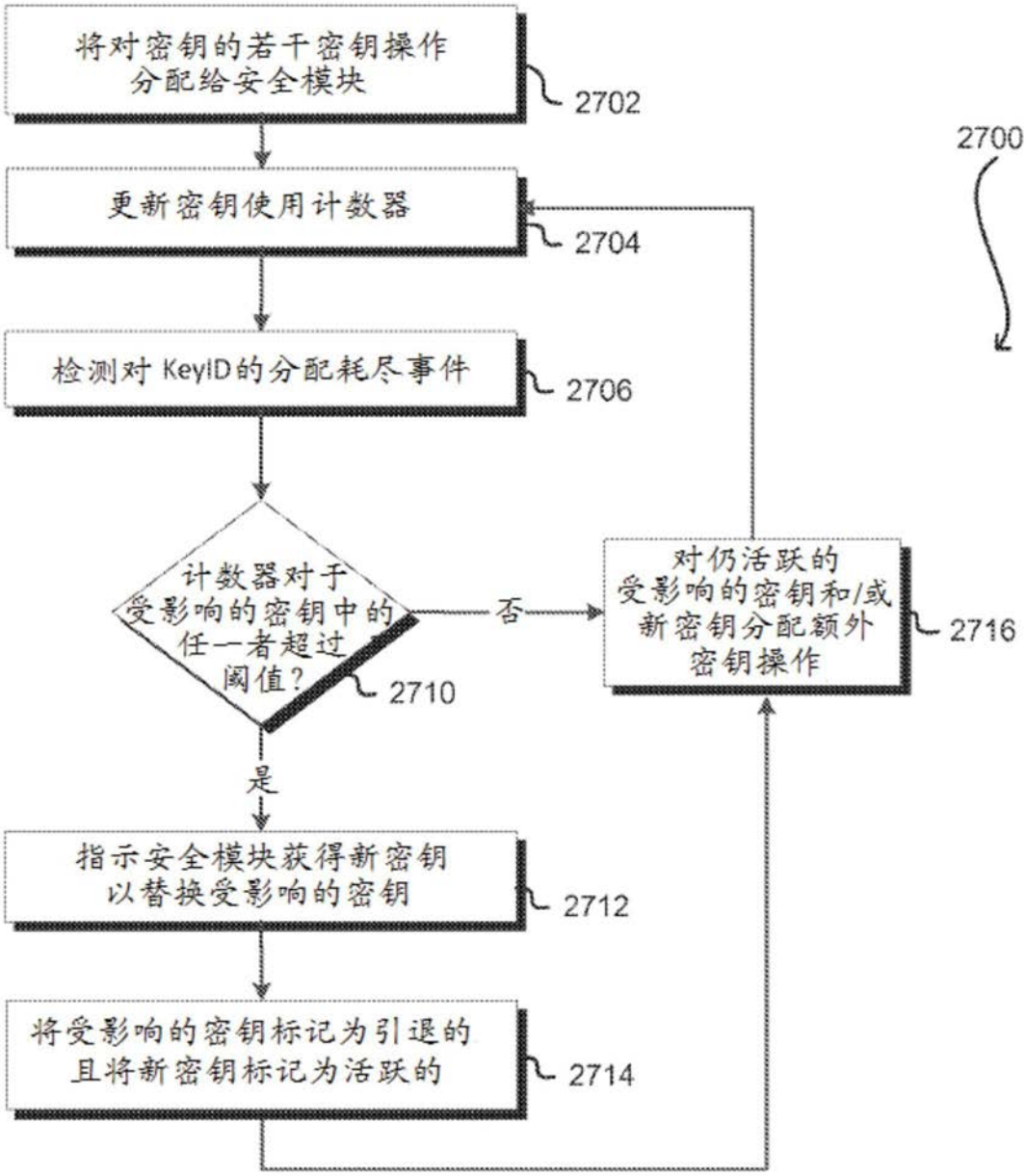

将对密钥的若干密钥操作分配给安全模块
2702
2700
更新密钥使用计数器
2704
检测对 KeyID的分配耗尽事件
2706
计数器对于受影响的密钥中的任一者超过阈值?
2710
否
对仍活跃的受影响的密钥和/或新密钥分配额外密钥操作
2716
是
指示安全模块获得新密钥以替换受影响的密钥
2712
将受影响的密钥标记为引退的且将新密钥标记为活跃的
2714

图27

KeyID	密钥版本	可用性	计数器
⋮	⋮	⋮	⋮
31415926	1	引退的	4294967296
31415926	2	引退的	4294967296
31415926	3	引退的	4294967296
31415926	4	活跃的	1048576
31415927	1	活跃的	2097152
⋮	⋮	⋮	⋮

图28

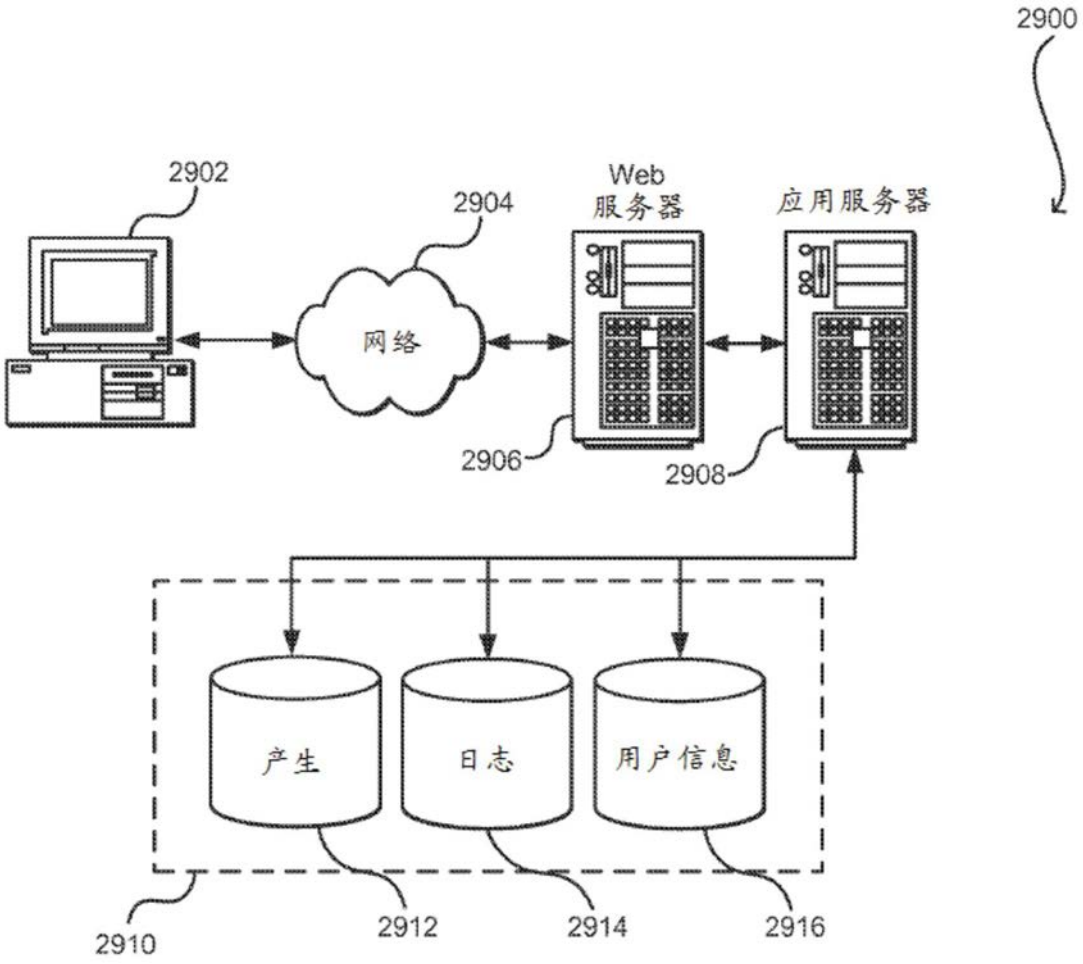


图29