(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102318263 A
(43)申请公布日 2012.01.11

(21)申请号 201080008658.7

(22)申请日 2010.02.04

(30)优先权数据
61/152,957 2009.02.16 US
12/490,837 2009.06.24 US

(85)PCT申请进入国家阶段日
2011.08.15

(86)PCT申请的申请数据
PCT/US2010/023243 2010.02.04

(87)PCT申请的公布数据
WO2010/093559 EN 2010.08.19

(71)申请人 微软公司
地址 美国华盛顿州

(72)发明人 R·V·奥拉德卡 R·P·德索扎

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

(51)Int.Cl.
*H04L 9/32*(2006.01)
*G06F 21/00*(2006.01)

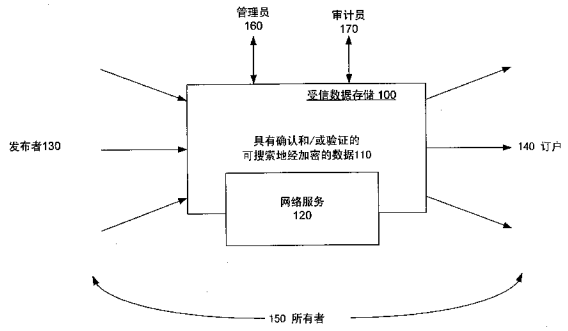
权利要求书 2 页 说明书 19 页 附图 32 页

(54)发明名称

受信云计算和服务框架

(57)摘要

为网络数据服务提供了数字托管模式，包括用于存储在云中的数据的可搜索加密技术、跨多个实体分布信用以避免单个数据点损害。在一个实施例中，密钥生成器、密码技术提供者和云服务提供者每个都被配备为单独的实体，从而使得数据的发布者能够机密地（经加密的）将数据发布给云服务提供者，并且然后选择性地将经加密的数据暴露于请求该数据的订户，该选择性地暴露基于被编码到响应于订户请求所生成的密钥信息中的订户身份信息（例如，订户的角色）。




CN 102318263 A

1. 一种用于订阅数据的方法，包括：

由至少一个订户设备请求 2600 可搜索地经加密的数据的子集；

从密钥生成组件接收 2610 密钥信息，该密钥生成组件基于与所述至少一个订户设备相关联的身份信息生成该密钥信息；

对经加密数据的由该密钥信息中定义的能力所允许的子集进行解密 2620；以及

确认 2630 经加密数据的与该请求一致的正确子集被所述至少一个订户设备接收到。

2. 如权利要求 1 所述的方法，其特征在于，确认 2630 包括：执行数据占有证明以证明正确的子集被所述至少一个订户设备接收到。

3. 如权利要求 1 所述的方法，其特征在于，接收 2610 包括：从在单独的控制区中执行的密钥生成组件接收密钥信息，该密钥生成组件基于从该身份信息中确定的至少一个角色来生成该密钥信息。

4. 如权利要求 1 所述的方法，其特征在于，进一步包括：验证 2930 在接收经加密数据的该子集以前，经加密数据的该子集的内容未曾被删除或修改过。

5. 如权利要求 4 所述的方法，其特征在于，验证 2930 包括：执行检索能力证明以证明该内容未受干扰。

6. 如权利要求 4 所述的方法，其特征在于，确认包括：执行数据占有证明以证明正确的子集被所述至少一个订户设备接收到。

7. 如权利要求 1 所述的方法，其特征在于，接收 2610 包括：从密钥生成组件接收密钥信息，该密钥生成组件基于从该身份信息中确定的至少一个角色来生成该密钥信息。

8. 一种方法，包括：

请求 200 第一实体确认与计算设备相关联的身份信息；

基于从该身份信息中确定的至少一个角色从独立于第一实体操作的第二实体请求 210 和接收密钥信息；

基于该密钥信息根据可搜索加密算法对能够从该计算设备访问的至少一个记录进行加密 220；以及

为至少一个订户角色定义 230 对于所述至少一个记录的至少一个能力以用于选择性地提供对所述至少一个经解密的访问。

9. 如权利要求 8 所述的方法，其特征在于，请求 210 包括：将与该计算设备相关联的凭证匿名。

10. 如权利要求 8 所述的方法，其特征在于，密钥信息的接收 200 包括：接收对与该身份信息相关联的主公钥进行编码的密钥信息。

11. 如权利要求 8 所述的方法，其特征在于，第一实体请求 210 确认身份信息包括：请求表示与同该计算设备相关联的身份信息相关的至少一个角色的令牌信息。

12. 如权利要求 8 所述的方法，其特征在于，定义 230 包括：为商业过程审计员定义至少一个能力。

13. 如权利要求 12 所述的方法，其特征在于，定义 230 包括：为商业过程审计员定义对于经加密的审计日志记录的至少一个能力。

14. 如权利要求 8 所述的方法，其特征在于，定义 230 包括：为管理员定义至少一个能力以监控与服务器过程有关的至少一个记录。

15. 如权利要求 8 所述的方法，其特征在于，定义 230 包括：为一方定义至少一个能力以检索与基于至少一个经加密关键词搜索的诉讼过程有关的至少一个记录。

# 受信云计算和服务框架

## 技术领域

[0001] 本主题公开涉及提供受信云计算和参与者的数据服务的框架、以及基于该框架的相应场景。

## 背景技术

[0002] 以关于一些常规系统的背景技术为例，计算设备在传统上是在设备本地执行应用和数据的。在这种情况下，当数据被访问、处理、存储、高速缓存等等时，这些数据可以通过本地总线、接口和其他数据路径在设备上行进，然而，设备的用户不必担心用户数据的干扰或暴露，除非设备本身丢失或失窃。

[0003] 但是，随着在线和云服务的演进，应用和服务正越来越多地移动到网络提供者，由网络提供者代表用户的设备来执行给定服务的一些或全部。在这种情况下，当用户的数据被上传到服务时、当该数据被服务存储时或者当该数据被从服务检索时，用户关心的可能是：谁可以访问该数据，或者谁可能损坏、干扰该数据。简言之，当用户设备的数据离开物理占有的范围并且进入远离用户的网络环境时，自然而然地造成一旦数据离开用户的物理占有时就关心对该数据的处理。因此，所期望的是增加对云服务和与云服务相联系的数据处理的信任。

[0004] 当今设备和运服务的上述缺点仅仅旨在提供对常规系统的一些问题的总览，并且不旨在是穷尽性的。在仔细阅读了以下具体实施方式后，当今领域的其他问题和各非限制性实施例的对应好处可变得显而易见。

## 发明内容

[0005] 此处提供了简化概述以帮助能够对以下更详细的描述和附图中的示例性、非限制性实施例的各方面有基本或大体的理解。然而，本发明内容并不旨在作为详尽的或穷尽的概览。相反，本发明内容的唯一目的是以简化的形式来提出与一些示例性非限制性实施例相关的一些概念，作为以下各实施例的更为详细的描述的序言。

[0006] 为网络数据服务提供了数字托管模式，包括用于存储在云中的数据的可搜索加密技术、跨多个实体分布信用以避免单个数据点损害。在一个实施例中，密钥生成器、密码技术提供者和云服务提供者每个都被配备为单独的实体，从而使得数据的发布者能够机密地（经加密的）将数据发布给云服务提供者，并且然后选择性地将经加密的数据暴露于请求该数据的订户，该选择性地暴露基于被编码到响应于订户请求所生成的密钥信息中的订户身份信息。

[0007] 出现关于受信云服务生态系统的场景集合，并且下面更详细地描述这些场景和各个其他实施例。

## 附图说明

[0008] 各非限制性实施例参考附图来进一步描述，附图中：

[0009] 图 1 是根据一实施例的受信云服务框架或生态系统的示例性、非限制性框图；

[0010] 图 2 是示出了根据受信云服务生态系统的用于发布数据的示例性、非限制性过程的流程图；

[0011] 图 3 是示出了根据受信云服务生态系统的用于订阅数据的示例性、非限制性过程的流程图；

[0012] 图 4 示出了一个示例性生态系统，该生态系统示出了密钥生成中心、密码技术提供者和云服务提供者 420 的在受信生态系统中的分离；

[0013] 图 5 是示出了用于为企业执行云服务的受信生态系统的其他益处的另一架构图；

[0014] 图 6 是示出了根据受信云服务生态系统的通过存储抽象层 610 来适应于不同存储提供者的另一框图；

[0015] 图 7 示出了与存储抽象服务相联系的存储的其他方面，该存储抽象服务抽象各个存储提供者的存储细节；

[0016] 图 8 是示出了受信云服务生态系统中的各个不同参与者的另一框图；

[0017] 图 9 是受信云计算系统的示例性非限制性实施方式的一些层的代表性视图，在该计算系统中，不同构件可以由不同或相同实体来提供；

[0018] 图 10-11 是流程图和框图，其分别示出了用于以利用后期绑定向发布者提供对数据的受控选择性访问的方式来向数字安全应用发布文档的示例性非限制性的过程和 / 或方法；

[0019] 图 12-13 分别是根据数字安全场景的用于订阅数据的示例性、非限制性过程和 / 或系统的流程图和框图；

[0020] 图 14 示出了使用数字托管模式来通过一个或多个数据中心为企业实现安全外联网的受信云服务生态系统的示例性、非限制性的实施方式；

[0021] 图 15 是示出了基于受信云服务生态系统的另一示例性非限制性场景的流程图，在该生态系统中，给订户提供对由云服务提供者存储的经加密数据的选择性访问；

[0022] 图 16 是示出了应用响应可以基于用户凭证来适应于订户的另一流程图；

[0023] 图 17 是示出了安全记录上传场景的另一流程图，该场景可以针对单方或多方来实现；

[0024] 图 18 是示出了对可搜索地经加密数据存储进行基于角色查询的示例性、非限制性的另一流程图，该数据存储由受信云服务生态系统来实现，例如以供由单方进行自动搜索；

[0025] 图 19 是根据一个或多个场景的受信云服务生态系统在企业、密钥生成中心和云服务提供者间的实施方式的框图；

[0026] 图 20 是示出了多方协作场景的流程图，在该场景中，企业向外部企业提供对其经加密数据中的一些的访问；

[0027] 图 21 是示出了多个企业间的多方自动搜索场景的流程图；

[0028] 图 22 是根据一个或多个场景的受信云服务生态系统在企业、密钥生成中心和云服务提供者间的实施方式的框图；

[0029] 图 23 示出了可以针对受信云服务实现的示例性、非限制性的边缘计算网络 (ECN) 技术；

[0030] 图 24 是示出了根据受信云服务生态系统的密钥生成中心的一个或多个任选方面的框图；

[0031] 图 25-26 示出了一实施例中的确认（例如数据占有证明）到受信数据服务的提供中的合并；

[0032] 图 27 示出了根据受信服务生态系统的示例性的数据服务的数据确认的框图。

[0033] 图 28-29 示出了一实施例中的验证（例如检索能力证明）到受信数据服务的提供中的合并。

[0034] 图 30 示出了根据受信服务生态系统的示例性的数据服务的数据确认的框图；

[0035] 图 31 是示出了基于适于使用服务的不同条件集的独立于服务提供本身的供发布者和订户使用的多个不同覆盖或数字托管垂直面的提供的框图。

[0036] 图 32 是表示其中可实现此处所描述的各实施例的示例性、非限制性联网环境的框图；以及

[0037] 图 33 是表示其中可实现此处所描述的各实施例的一个或多个方面的示例性、非限制性计算系统或操作环境的框图。

## 具体实施方式

[0038] 概览

[0039] 如在背景技术中所讨论的那样，发送给网络服务的数据可能造成隐私方面的不适、篡改的可能性等等，即当数据被从用户的设备传输给网络应用、服务或数据存储时，用户需要对没有恶意第三方能造成损害的充分保证。按照定义，用户失去对数据的控制。因此，所期望的是增加信任，使得数据的发布者和 / 或所有者愿意交出对其数据的物理控制，同时相信：在网络中，除了该发布者或该所有者基于订户的身份给订户赋予特权以外，其数据都将保持隐私性和不受损。

[0040] 对于这一点，为了消除围绕网络服务的常规供应的信任障碍，提供实现上面标识出的目标以及在下面描述的各个实施例中强调的其他优点的受信云计算和数据服务生态系统或框架。术语“云”服务一般所指的概念是，服务不是本地地从用户的设备执行，而是从可通过一个或多个网络被访问的远程设备来递送。由于用户的设备不需要理解在一个或多个远程设备处所发生的事情的细节，因此服务从用户的设备的角度看上去是从“云”递送的。

[0041] 在一个实施例中，系统包括密钥生成器，该密钥生成器生成用于发布或订阅数据的密钥信息。与密钥生成器独立地实现的密码技术提供者基于由密钥生成器所生成的密钥信息实现可搜索的加密 / 解密算法。另外，与密钥生成器和密码技术提供者独立地实现的网络服务提供者提供与由密码技术提供者加密的数据有关的网络服务。

[0042] 相对于可搜索的加密 / 解密算法而言，由一个或多个密码技术提供者实现的可搜索的公钥加密 (PEKS) 方案为任何给定的消息 W 生成陷门 TW，使得 TW 允许检查给定密文是否是对 W 的加密，其中 TW 不揭示关于明文的任何附加信息。根据下面所述的各个实施例，PEKS 方案可以用于基于包含在诸如经加密的消息之类的经加密的数据（例如消息文本）中的关键词对所述经加密的数据确定优先级或进行过滤。因此，可以通过释放相应关键词的能力（有时被密码员称为“陷门”）来给数据接收者提供对经加密数据的与关键词有关的部

分的所选访问。通过这种方式，可以在经加密的数据中检查这些关键词，但是保证不会从订户获悉比该订户的能力所允许的更多东西。

[0043] 为了避免质疑，尽管在此处的一个或多个实施例中将 PEKS 公开为用于实现可搜索加密的算法，但是能够理解，存在多种可替代的算法以用于实现可搜索加密。PEKS 的一些示例性的非限制性的替代方案例如包括不在意 (Oblivious)RAM。因此，在此所使用的术语“可搜索加密”应当不限于任何一种技术，并且因此是指宽范围的如下加密机制或加密机制的组合：所述加密机制允许基于对经加密数据的搜索或查询功能来选择性地访问经加密数据的子集。

[0044] 任选地，可以作为附加好处向生态系统中的数据的订户和发布者提供对结果的确认和 / 或验证。确认提供一种方式来确认由于针对数据的子集的订阅请求而接收的数据项目是正确的项目集合，即数据的本应该接收的正确子集实际已经被接收。密码领域的一种技术是数据占有证明 (PDP)，然而，为了避免质疑，PDP 仅仅是可以被实现的一种示例性算法，并且可以使用实现相同或类似目标的其他算法。可证明数据占有或数据占有证明 (PDP) 是关于如何频繁、有效和安全地验证存储服务器忠实地存储了其客户端的可能大的外包 (outsourced) 数据。存储服务器被假定为在安全性和可靠性方面都不受信任。

[0045] 对结果的验证提供用于检查项目本身的内容的附加机制，即以保证结合订阅请求所接收的项目未曾被任何未授权实体篡改过。密码领域的验证的一个例子是数据占有证明 (PDP)，然而，为了避免质疑，PDP 仅仅是可以被实现的一种示例性算法，并且可以使用实现相同或类似目标的其他算法。在密码领域中已知的另一技术是检索能力 (retrievability) 证明 (POR)，然而，为了避免质疑，POR 仅仅是可以被实现的一种示例性算法，并且可以使用实现相同或类似目标的其他算法。POR 是一种由服务提供者或数据主控者（证明者）对客户端（验证者）进行的紧凑证明，其表示目标文件 F 在客户端可以完全恢复文件 F 并且未发生篡改的意义上而言是完整的。

[0046] 作为附加的选项，生态系统可以实现匿名凭证的概念，由此发布者可以以匿名方式上传关于其自己的信息而不暴露关键细节，并且订户可以受其能力的限制，使得其不能被暴露或被提供对由发布者上传的关键细节的访问。通过这种方式，发布者或订户可以于系统交互，同时仅仅暴露其希望向第三方暴露的那样多的信息。

[0047] 常规的 web 服务已经限于静态客户端服务器布置和用于访问 web 服务的静态地定义的用户策略。然而，当根据经常改变和演进的复杂商务和其他关系来构思许多发布者和订户时，这样的常规 web 服务模型不能是灵活的或者足够安全的。因此，在各个实施例中，启用后期绑定，使得数据和内容的发布者和 / 或所有者可以基于订户是谁、基于订户的能力以及基于他们在寻找什么（例如基于针对数据的请求中所使用的关键词）来改变对经加密内容的访问特权。因此，订户能够选择性地访问的东西与发布者和 / 或所有者对访问特权的改变一致地动态改变，因为订户能力被编码在由运行中的密钥生成器所提供的密钥信息中。因此，为给定请求在为该请求生成密钥的时刻定义订户特权，并且因此该订户特权总是反映关于来自订户的请求的当前策略。

[0048] 在一个实施例中，提供数据存储，其暴露可选择性地访问的（例如可搜索的）经加密数据，其中至少一个发布者向该数据存储发布表示资源的数据。在提供对滥用信任的可能性的划分 (division) 的情况下，第一独立实体执行密钥信息的生成。第二独立实体进而

在存储所发布的数据之前基于由第一独立实体生成的密钥信息来对所发布的数据进行加密。然后，一组网络或云服务针对向该网络服务的请求基于由资源的发布者或所有者所赋予的后期绑定的所选特权来选择性地访问经加密数据。

[0049] 在其他实施例中，数据存储存储可选择性访问的经加密数据，其中订户订阅经加密数据的指定子集。第一独立实体基于与订户相关联的身份信息来生成密钥信息，并且第二独立实体基于由第一独立实体生成的密钥信息来执行该指定子集的解密。网络服务响应于订户的请求，并且基于由所指定子集的发布者或所有者所赋予的后期绑定的所选特权来提供对经加密数据的选择性访问。

[0050] 就此而言，术语“发布者”和“订户”一般分别指发布或订阅受信云服务的数据的任何人。然而在实际中，根据行业、领域或受信云服务生态系统的应用和数字托管模式，发布者和订户将担任更具体的角色。例如，经加密的数据存储的审计员可能基于审计员的角色而具有某些能力，比如标识出电子邮件存储中的某些攻击性关键词的能力，但是被阻止阅读不含攻击性关键词的电子邮件。

[0051] 类似地，受信云服务的服务器的管理员可以被许可观察由该服务器处理的行为和数据事物的日志，但是也可以被限制为不能看见任何客户姓名或信用卡信息。因此，订户的身份可以是限制订户可以访问的数据类型的基础。

[0052] 在此，在构建对云服务的信任的上下文中提出受信生态系统的各种非限制性实施例，然而，在此提供的对生态系统的信任构建是更一般的，并且不限于应用于云服务。更确切而言，在此所述的实施例类似地适用于企业数据中心内的不同服务器或参与者。因此，尽管数据可能从未离开给定实体，但是在此所述的用于构建信任的技术同样适用于企业内的不同过程在单独控制区内操作的情况。在没有跨所有企业过程的可见性的情况下，可能造成类似的不信任，就好像参与者置身于企业之外。例如，服务器云即使在处于管理员的控制之下时或者管理员可能不注意或者为恶意时可能在企业内遭到破坏。

[0053] 除了适用于云中的经加密数据，本发明的各种技术还可以适用于存储在膝上型计算机或其他便携式设备上的数据，因为膝上型计算机可能丢失或失窃。在这种情况下，该设备可能最终为过于好奇或者恶意实体所占有，然而，在此所述的适于保护云中数据的相同技术还可以用于保护服务器或膝上型计算机上的数据。如果本地数据是经加密的，则在没有适当订户凭证的情况下，窃贼将不能理解经加密的本地数据，从而不能出示适当角色或能力来访问该数据。

[0054] 下面提供这些和其他各示例性、非限制性实施例和场景的进一步细节。

[0055] 受信云服务生态系统

[0056] 如所提到的那样，为网络数据服务提供数字托管模式，包括用于存储在云中的数据的可搜索加密技术、跨多个实体的分布信任以避免单个实体造成的损害。在一个实施例中，密钥生成器、密码技术提供者和云服务提供者每个都被配备为单独的实体，从而使得数据的发布者能够机密地（经加密的）将数据发布给服务提供者，并且然后选择性地将经加密的数据暴露于请求该数据的订户，该选择性地暴露基于被编码到响应于订户请求所生成的密钥信息中的订户身份信息。

[0057] 图 1 是根据一实施例的受信云服务框架或生态系统的框图。该系统包括受信数据存储 100，该受信数据存储 100 用于存储可搜索的经加密数据 110 以及订户请求经历确认和

/ 或验证的结果。就此而言，网络服务 120 可以构建在安全数据 110 之上，使得数据的发布者保留对赋予给例如通过网络服务 120 请求该数据的订户 140 的能力的控制。发布者 130 还可以是订户 140，并且反之亦然，并且数据的所有者 150 也可以是发布者 130 和 / 或订户 140。作为一些常见角色和可以定义的相应能力集合的例子，特殊类型的发布者 130 和订户 140 是管理员 160 和审计员 170。

[0058] 例如，管理员 160 可以是对数据 110 的特殊许可集合，以帮助维护对受信数据存储 100 的操作，并且审计员实体 170 可以在审计的范围内帮助维护某些数据的完整性。例如，审计员 170 可能订阅含有攻击性关键词的数据 110 的消息，在这种情况下，审计员 170 在根据所赋予能力受到许可的情况下可以在数据 110 的消息包含这样的攻击行关键词时受到提醒，但是不能阅读其他消息。就此而言，可以基于如下能力构建无数场景 :将发布者数据置于数字托管之下，使得可以分发实现对该数据的选择性访问的密钥。

[0059] 例如，发布者向生态系统认证并且指示要上传到该生态系统的文档集合。该文档基于从生成密钥信息的单独的密钥生成器所接收的密钥信息根据可搜索加密算法被加密。然后，经加密数据被传输给网络服务提供者以供存储该经加密数据，使得经加密数据可以根据基于请求设备的身份信息赋予给该请求设备的所选特权的后期绑定被选择性地访问。将密码技术提供者同经加密数据的存储相分离将附加地隔离经加密的数据免受进一步损害。

[0060] 就此而言，图 2 是示出了根据受信云服务生态系统的用于发布数据的示例性非限制性方法的流程图。在 200，发布者向该系统认证（例如发布者用用户名和口令、LiVE ID 凭证等等登陆）。在 210，密钥信息由诸如密钥生成中心之类的密钥生成器生成，这将在下面的一个或多个实施例中予以描述。在 220，单独的密码技术提供者基于密钥信息对发布者文档集进行加密。在 230，经加密文档与能力一起被上传到例如存储服务提供者之类的网络服务提供者，使得经加密文档可以利用基于请求设备（订户）的身份信息所赋予的所选特权的后期绑定被选择性地访问。

[0061] 例如在订户侧，订户向生态系统认证，并且指示对数据子集的请求（例如对包含给定关键词或关键词集合的文档的子集的查询）。响应于从至少一个订户设备对可搜索地经加密数据的请求，密钥生成组件基于与订户设备相关联的身份信息生成密钥信息。然后，根据在密钥信息中所定义的赋予给该订户设备的特权，经加密数据的子集被解密。

[0062] 图 3 是示出了根据受信云服务生态系统的用于订阅数据的示例性非限制性方法的流程图。在 300，用于订阅数据的方法包括 :认证订户（例如订户用用户名和口令、LiVE ID 凭证等等登陆）。在 310，订户作出对数据的请求。在 320，密钥信息由独立密钥生成实体基于订户请求而生成，其中订户的能力可以在密钥信息中定义。在 330，发布者数据的子集基于在密钥信息中所定义的能力被解密。例如，CSP 可以对该数据进行解密。在 340，使发布者数据的子集可被订户访问，例如订户可以基于由所有者 / 发布者所赋予的可动态定义的能力来对该数据进行下载、查看、处理、改变等等。任选地，用于加密、解密和密钥生成的技术可以由单独的密码技术提供者来提供，但是由任何参与者来主控。

[0063] 在一个实施例中，订户设备的身份信息包括该订户的角色。例如，审计员角色、管理员角色或其他预先指定的角色可以被发布者 / 所有者用作限制或赋予对可搜索地经加密的数据存储的各部分的访问的基础。

[0064] 图 4 示出了示例性的生态系统，该生态系统示出了密钥生成中心 (CKG)400、密码技术提供者 (CTP)410 和云服务提供者 (CSP)420 的分离，由此消除单个实体在受信生态系统中造成损害的可能性。就此而言，客户 430 包括数据的发布者和 / 或订户。可选地，CKG 400 可以基于例如由 CTP 410 提供的参考软件、开源软件和 / 或软件开发工具包 (SDK) 来构建，从而使得多方的构建块能够自己创建这样的组件或者对第三方实现这样的生态系统组件感到满意。在一个实施例中，SDK 由 CTP 410 来提供，并且可以被一个或多个参与者用户用于主控或实现 CKG 400、下面将更详细描述的计算和存储抽象 (CSA) 和 / 或密码客户端库。任选地，SDK 可以从 CTP 分发给主控 CKG 400 的实体。

[0065] 一般而言，CKG 400、CTP 410 或 CSP 420 中的每个都可以根据给定实施方式被细分为子组件，然而总体分离被保留以维持信任。例如，诸如主公钥 (MPK) 递送 402、客户端库下载器 404、密钥提取器 406、信任验证器 408 或者其他子组件之类的 CKG 实体 401 可以以子集的形式分开地提供、或者作为集成组件一起提供。诸如用于编码和解码的户端应用 412、可替代的加密技术 414、用于与 CKG 对接的应用 416、其他密码构建块 418 等等之类的 CTP 实体 411 也可以以子集形式分开地提供或者一起提供。此外，可以分别认为 CSP 420 是诸如 CSP 422、426、主控存储服务 424 和服务主控 428 之类的许多单独的服务提供者，或者这样的服务可以一起提供。

[0066] 能够理解，由受信生态系统中的一个或多个参与者主控的 CKG 或 CKG 实例不需要是单个单片实体。更确切而言，CKG 可以被分成多个（冗余）实体，这些实体协作以生成密钥，使得操作即使在参与者的小子集离线的情况下仍然可以继续。在一个实施例中，任选地，参与者的集合即使在这些参与者的小子集已经被对手损害或者以其他方式变为不可用或不受信任时仍然可以整体上受到信任。

[0067] 图 5 是示出了用于为企业 500 执行云服务的受信生态系统的其他好处的另一架构图。例如，企业 500 可以包括不同组织 502、504、506、508。该图中的不同组织 502、504、506、508 示出了 :组织可以采取相对于实现用于使用系统或密钥生成的策略而言那样多或那样少的所有权。例如，组织 502 实现其自己的策略 512，但是使用集中式密钥生成器 522，而组织 504 选择实现其自己的密钥生成器 524 并且实现其自己的策略 514。组织 506 还实现其自己的策略，但是依靠第三方 CKG 526，而组织 508 选择依靠第三方策略提供者 518 和独立 CKG 528。

[0068] 就此而言，为了发布数据，发布者 540 基于来自 CKG 522 的输出获得用于对数据进行加密的公用参数 535。基于公用参数，数据在 545 由发布者设备 540 使用独立密码技术提供者来加密。经加密数据被上传到存储抽象服务 550，该存储抽象服务 550 隐藏与由诸如 CSP 572、574、576 或 578 之类的一个或多个 CSP 存储经加密数据相联系的存储语义。在订户设备 560 上，对数据的请求导致从 CKG 522 生成私用密钥 565。私用密钥 565 包括如下信息 :该信息使得订户设备 560 能够通过在 555 对数据进行解密来选择性地访问可搜索地经加密的数据。再次，从 CSP 570 检索数据的语义被存储抽象服务 550 隐藏。而且，被赋予给订户设备 560 的特权是由于由发布者 / 所有者所赋予的能力的后期绑定而产生的特权的当前集合。

[0069] 从图 5 中能够理解，要么为企业、要么为消费者的多个数据所有者可以如在此所述的那样参与受信生态系统以建立受信关系。在这种情况下，每个所有者都可以主控或控

制其自己的CKG(例如组织504的CKG 524),使得对数据的请求或查询被转发给相应CKG以从所请求数据的所有共有者收集所需的密钥。

[0070] 图6是示出了通过存储抽象层610来适应于不同存储提供者的另一框图。利用受信生态系统,分别具有客户端应用640、642的桌面630、632可以如上所述的那样发布或订阅数据,从而向密钥生成中心620发起对用于对数据进行加密和解密的密钥信息的请求。类似地,服务644、646、648也可以是生态系统中的发布者和/或订户。就此而言,为了由私用云存储600、SQL数据服务存储602、或简单存储web服务604等等中的任一进行存储或提取,存储抽象服务610(如名称所隐含的那样)抽象出关于远离客户端的一个或多个特定存储库的特性。

[0071] 就此而言,为了避免质疑,图6针对多种情况。在一种情况下,图6通过存储抽象服务(有时亦称计算和存储抽象(CSA))涵盖了存储提供者(将其抽象为个体)的非居间化。另外,图6涵盖了如下场景:数据被分割和/或扇出(例如为了冗余)为可以为相同或不同类型的多个后端存储提供者的场景,使得原始数据即使在后端存储提供者之一(或少数)意外地或无意地删除或改变其数据副本时仍然可以被重构。

[0072] 图7示出了与包括服务器操作系统(OS)714和存储服务712的存储抽象服务710相联系的存储的其他方面,该存储抽象服务710抽象私用云存储700、SQL数据存储702、简单存储web服务存储704等等的存储细节。客户端可以是分别具有客户端应用740和742的桌面750或752。密钥生成中心720可以包括在服务器OS 724上执行的密钥生成器应用722。就此而言,具有活动目录736、服务器OS 734和安全令牌服务(STS)732的组织730可以是生态系统中的发布者或订户。就此而言,存储传输格式(STF)是标准交换格式,其可以用于在多个库的范围内交换经加密数据和元数据。例如,组织730可能希望在存储服务提供者700、702或704间传输电子邮件数据,在这种情况下可以使用STF。

[0073] 图8是示出了受信生态系统820中的各个不同参与者的另一框图。如上面所提到的那样,有利地,企业800可以将数据量的存储和维护从现场推卸给云存储服务提供者,其中云存储服务提供者更适于处理这样的数据量,同时维持数据将不会对错误的订户解密的舒适性,因为企业维持对针对经加密数据所定义的能力的控制。例如,组织802可以操作诸如SharePoint之类的协作应用812。就此而言,组织802可以为SharePoint数据建立数字托管或者受信域。策略832和CKG 834可以由第一数据中心830来实现,该第一数据中心830用于通过为受信域定义密钥信息845来建立安全空间。

[0074] 然后,例如发布者814之类的另一组织804可以基于从CKG 834获得的密钥信息对数据进行加密,此时,第二数据中心840的计算和存储抽象组件842处理在第三数据中心850处(例如在CSP 852中)存储可搜索地经加密的数据的细节。反过来,当组织804的订户816请求数据时,私钥或密钥信息作为提取865的一部分被递送给订户816。接着,基于包括为订户定义的能力的私钥信息,由该订户所请求的数据在875被解密,其中假定该订户具有特权,并且抽象层842再次处理底层存储852的细节。

[0075] 图9是受信云计算系统的示例性非限制性实施方式的一些层的代表性视图,在该计算系统中,不同构件可以由不同或相同实体来提供。在层栈的底部是数学和密码库986,其用于实现加密/解密算法。可以提供各种密码方案的定义的抽象作为细节库986与可搜索密码方案982的实际实施之间的中间层984。层982、984和986一起形成较大的密码服

务层 980，该密码服务层 980 在与软件的抽象层 960 组成服务 (SaaS) 应用生态系统时形成实现受信数字托管 970 及其存储的基础。抽象层 960 包含用于实现数字托管模式的基本语言，即诸如 SetUp()（建立 ()）、Encrypt()（加密 ()）、Extract()（提取 ()）、Decrypt()（解密 ()）之类的命令。

[0076] 处于抽象层 960 之上的是层 950，该层 950 捆绑到各种更具体的平台技术（例如 SDS、Azure、备份 / 归档、RMS、STS 等等）中。处于捆绑到各种具体平台技术中的层 950 之上的是使用受信数字托管 900 的各种 SaaS 应用。示例性的非限制性图示示出了 :数字托管应用 900 可以由单个公司 910 或由伙伴 930 或者由二者来实现。例如，公司 910 可以实现诸如下列服务 :高性能计算 (HPC)、eDiscovery 和合法发现 914、Live 服务 916（例如 DBox）、备份 / 归档即服务 918、审计日志——商业过程和监控 920、或者其他云服务 922。伙伴 930 云进而实现诸如下列服务 :eLetterOfCredit 932、HPc 即垂直面 (Verticals) 服务 934、eHealth 服务、安全外联网 938、顺应性 940、诉讼支持 942 等等。

[0077] 基于受信云服务生态系统的场景

[0078] 在图 9 的上半部没有深入讨论由于在密钥生成器、密码提供者和云服务提供者的划分中固有的经提高的信任而可以在云服务中实现的应用类型。就此而言，在已经实现了这样受信云服务生态系统的情况下，可以实现丰富的服务和场景的集合，这些服务和场景利用在此所述的受信生态系统的一个或多个好处。

[0079] 例如，图 10 是一个示例性非限制性过程的流程图，该过程用于以利用上述后期绑定向发布者提供对数据的受控选择性访问的方式来向数字安全应用发布文档。在 1000，对设备进行认证（例如设备用用户名和口令、口令凭证、生物凭证、Live ID 凭证等等登陆）。在 1010，文档被上传并且标签被输入。在 1020，所述标签被发送给托管代理，并且作为响应，从托管代理接收经散列的标签。就此而言，所述标签可以如所提到的那样来提供，或者可替代地可以通过全文索引来自动地从有效载荷（记录、文档）中提取。在 1030，客户端利用发布者的密钥信息对文档进行加密，并且所述文档与订户相对于这些文档的能力一起被发送给安全数字云存储提供者。在 1040，安全数字云存储提供者例如将经加密的团块 (blob) 发送给存储服务（例如相对于存储抽象层）。

[0080] 图 11 示出了在受信生态系统中的不同参与者的上下文中的图 10，其中在该图中标出了图 10 的动作。就此而言，以客户端 1110 的凭证 1100 开始，进行 1000。接着，在客户端 1110 处进行 1010。接着，在 1020 表示将标签发送给托管代理 1120 以及接收经散列的标签的步骤。接着，客户端 1110 对文档进行加密，并且将其发送给数字安全服务 1130，这如 1030 所示。最后，经加密的团块被发送给存储服务 1140，这由 1040 来表示。然后，如果能力与文档一起被发送或者之后被更新，可以给订户赋予对用户的子集的访问，因此允许。

[0081] 图 12 是用于订阅置于数字安全中材料的示例性、非限制性过程的流程图。在 1200，订户被认证，并且客户端设备将标签发送给托管代理，该托管代理在 1210 作为响应发回经散列的标签。然后，客户端在 1220 将经散列的标签发送给数字安全服务，并且经散列的标签被解释以了解 :在 1230，该客户端是否有权让其搜索请求全部或部分地由存储服务来执行。

[0082] 图 13 表示与图 11 类似的覆盖在参与者上的图 12 的动作 :动作 1200 针对客户端 1310 及其凭证 ;动作 1210 针对客户端 1310 和托管代理 1320 ;动作 1220 针对客户端 1310

和数字安全服务 1330 ;以及动作 1230 针对数字安全服务 1330 和存储服务 1340。

[0083] 在图 11 和 13 中,托管代理 1120、1320 可以是 CKG、或者 CKG 的组件。可替代地,托管代理 1120、1320 可以是由单独的参与者主控的 CKG 实例,由此托管代理 1120、1320 是代表客户端进行加密 / 解密的受信实体。就此而言,参与者间的设计折衷和关系可以规定托管代理 1120、1320 的功能和范围。例如,对于低端客户端而言,可能需要将客户端功能推卸给受信代理服务以执行繁重的处理。

[0084] 图 14 示出了使用数字托管模式来通过一个或多个数据中心为企业实现安全外联网的受信云服务的示例性、非限制性的实施方式。如所提到的那样,受信计算生态系统可以包括密钥生成中心 1400,该密钥生成中心 1400 与密码技术提供者 (CTP)1410 分开地实现,该密码技术提供者 1410 提供参考实施方式以供用于实现与生态系统一致的同一个或多个云服务提供者 (CSP)1420 分开实现的密码技术。在安全外联网的示例性非限制性的实施方式中,1480 示出了 :企业维护共享库 1470( 例如 SharePoint) 和设计或分析应用的库 1460 以供与共享库 1470 中的文档结合使用。商业软件 1440( 例如前哨 (Sentinel)) 可以监控具有桌面 1450 的计算机的应用或服务器性能等等。

[0085] 就此而言,在受信云服务生态系统中,当使用桌面 1450 的订户从存储中寻求可以选择性地访问并且被加密的信息时,安全令牌服务 1430 可以递送某些信息以标识出订户 1482,并且 CKG 1400 可以通过第一数据中心的 CKG 层 1402 的接口被咨询,这由 1484 示出。CKG 1400 返回密钥信息,然后,该密钥信息如 1486 所示的那样可以用于通过存储抽象服务 1422 选择性地访问由数据服务 1424 所持有的数据。因此,任何类型的数据都可以在企业的范围内根据企业中的订户的角色来选择性地共享。

[0086] 图 15 是示出了基于受信云服务生态系统的另一示例性非限制性场景的流程图,在该生态系统中,给订户提供对由例如企业内的 CSP 存储的经加密数据的选择性访问。最初,订户设备还未获取访问经加密数据的特权。然而,通过在 1500 例如通过与应用交互来作出对一些或全部经加密数据的请求,应用自动地与相应 STS 通信以用于在 1510 获得声明 (Claim)( 密码学中的用语 )。在 1520,应用与 CKG 通信以获得密钥信息,该密钥信息编码有关于订户的能力的信息 ( 能力有时在密码学的用语中被称为陷门,但是术语“能力”不限于通常出现术语“陷门”的上下文 )。最后,应用在 1530 将密钥信息提供给 CSP,CSP 允许以订户能力所允许的程度来对经加密的数据进行搜索或查询。

[0087] 图 16 是示出了应用响应可以基于登陆信息适应于订户的另一流程图。例如,在 1600,用户 ID 信息被应用接收。在 1610,应用从 STS 获得相关声明。在 1620,基于用户充当的与用户 ID 信息相关联的一个或多个角色,体验可以被调整为与那些角色的特权 / 限制相称。例如,作为公司的经加密数据的视图来呈现公司的主要财务部门的用户体验可以并且应当是与提供给邮件室雇员的公司经加密数据的视图不同的用户体验。图 16 可以适用于单方或多方登陆场景。

[0088] 图 17 是示出了安全记录上传场景的另一流程图,该场景可以针对单方或多方来实现。在 1700,记录和关键词被应用接收,其例如是由具有该应用的设备的用户提供或指定的。在 1710,应用获得主公钥 (MPK) 并且应用公钥加密关键词可搜索 (PEKS) 算法。MPK 可以任选地被应用高速缓存。在 1720,应用例如通过存储抽象层将经加密的记录输入到 CSP 库中。

[0089] 图 18 是示出了对可搜索地经加密数据存储进行基于角色查询的示例性、非限制性的另一流程图，该数据存储由受信云服务生态系统来实现，例如以供由单方进行自动搜索。在 1800，联合查询被应用接收或发起。在 1810，应用从 STS 获得相关声明。例如，STS 将用户的角色映射到合适的查询组，并且返回给定角色的合法查询集合。在 1820，应用提交经过滤的声明和查询，使得可以有效地提交对应于该查询的声明、而不是所有的声明。任选地，CKG 将陷门声明返回给应用（或者拒绝该声明）。在 1830，应用对远程索引执行陷门声明。基于对远程索引的处理，结果可以被应用接收，并且通过该应用例如基于用户角色使用客户呈现来将结果呈现给用户。

[0090] 图 19 是受信云服务生态系统在企业 1920、CKG 1910 和 CSP 1900 间的实施方式的框图，其中图 15-18 的上述动作通过相同的附图标记来突出。这些场景始于用户 1924 向应用 1922 标识他自己或她自己。STS 1926 用于结合去往和来自 CKG 1910 的信息的交换来建立信任 1930，从而将密钥信息返回给应用 1922 以供用于根据场景的目标对来自 CSP 1900 的数据进行加密或解密。

[0091] 图 20 是示出了多方协作场景的流程图，在该场景中，企业向外部企业提供对其经加密数据中的一些的访问。例如，制造商可以给供应商赋予对其存储在受信云中的数据的访问，并且反之亦然。就此而言，在 2000，给企业 2 的 STS 指定资源提供者，并且企业 1 的应用继续进行以获得对云中的资源提供者所提供的资源的访问的声明。在 2010，企业 1 的 STS 被指定作为身份提供者。就此而言，应用为由企业 1 处的订户所定义的角色或角色集合获得声明，这由身份提供者来促进。在 2020，应用基于由企业 2 控制的可许可资源以及基于由订阅实体所定义的许可 / 能力来检索声明。在图 20，尽管仅仅描绘了一个 STS，但是应当注意，在数字托管或联合信任覆盖中可以存在多个身份提供者 STS 和 / 或多个资源提供者 STS。

[0092] 图 21 是示出了例如诸如企业 1 和企业 2 之类的多个企业间的多方自动搜索场景的流程图。在 2000，联合查询被企业 1 的应用接收或发起以供执行。在 2110，应用从资源提供者（企业 2）的 STS 获得相关声明。任选地，该资源提供者可以在组织标签中指定。STS 可以任选地执行用户角色到查询组的映射，使得返回针对该用户角色的合法查询集合。在 2120，应用基于该用户角色提交经过滤的声明和查询，使得可以有效地提交对应于该查询的声明、而不是所有的声明。任选地，CKG 将能力返回给应用（例如陷门声明），或者 CKG 拒绝该声明。在 2130，应用对远程索引执行陷门声明。基于对远程索引的处理，结果可以被应用接收，并且通过该应用例如基于用户角色使用定制呈现来将结果呈现给用户。

[0093] 在图 18 和 21 中，该方法包括接收联合查询或者以其他方式发起联合查询的步骤。就此而言，任选地，联合查询也可以被密码保护，使得没有陷门（或能力）的接收者（要么为客户端、要么为服务提供者）可以分解联合查询并且确定其组成部分。

[0094] 图 22 是受信云服务生态系统在企业 2220、2230、CKG 2210 和 CSP 2200 间的实施方式的框图，其中图 20-21 的上述动作通过相同的附图标记来突出。例如，用户 2224 可以向应用 2222 标识他自己或她自己。企业 2220 的 STS 2226 和企业 2230 的 STS 2232 协作以结合去往和来自 CKG 2210 的信息的交换来建立信任 2230，从而将密钥信息返回给应用 2222 以供用于根据场景的目标对来自 CSP 2200 的数据进行加密或解密。

[0095] 图 23 示出了可以针对受信云服务实现的示例性、非限制性的边缘计算网络 (ECN)

技术。就此而言，结合彼此独立操作的受信云组件给多个动态计算节点 2370、2372、2374、2376 动态地分配计算带宽。例如，密钥生成中心 2320、存储抽象服务 2310、组织 2330 和组织 2340 可以如所示那样被实现为涵盖多组织业务或诸如上述场景之类的其他场景。密钥生成中心 2320 包括密钥生成器 2322 和服务器 OS 2324。存储抽象服务 2310 包括存储服务组件 2312 和服务器 OS 2314。组织 2330 包括 STS 2332、AD 2336 和服务器 OS 2334。组织 2340 包括 STS 2334、AD 2346 和服务器 OS 2344。服务器 OS 2314、2324、2334、2344 协作以在服务器的范围内实现 ECN。任何存储提供者或抽象 2302 都可以用于存储数据，例如可以使用 SQL 数据服务。通过这种方式，一个或多个桌面 2350、2352 可以分别通过客户端应用 2360、2362 发布或订阅数据。

[0096] 图 24 是示出了根据受信云服务生态系统的密钥生成中心 2410 的一个或多个任选方面的框图。最初，诸如桌面 2460、2462 之类的计算设备的集合和相应的客户端应用 2470、2472 或者服务或服务器 2474、2476、2478 等等是云内容递送网络 2450 的潜在发布者和 / 或订户。然而，在满足来自该计算设备集合中的任何计算设备的请求以前，密钥生成中心最初为了获得发布者的信任而充当管理人，该密钥生成中心基于公钥对数据进行加密并且基于数据订户的能力向其发放私钥。

[0097] 在示例性的非限制性的交互中，来自计算设备的请求最初被提供 2400，并且 CKG 2410 的主控者在 2480 向 CKG 工厂 2402 请求 CKG 2410 的实例。接着，在 2482 进行用户认证 2404。接着，任何基于使用的计费 2484 可以由计费系统 2406 应用以供 CKG 工厂 2402 使用。接着，租赁 CKG 在 2486 被 CKG 工厂 2402 物化，其可以包括 MPK 递送组件 2412、客户端库下载器 2414、密钥提取器 2416 和信任确认器 / 验证器 2418。

[0098] MPK 递送组件 2412 在 2488 将 MPK 递送给 CDN 2450。客户端库下载器 2414 将密码库下载到请求客户端，这些密码库可以与要发布的数据的加密或者该设备订阅的数据的解密结合使用。接着，客户端基于从与信任验证器 2418 协作的密钥提取器 2416 所接收的密钥信息来作出提取给定文档集合的请求，该信任验证器 2418 可以基于在 2494 验证订户的 STS 拇指纹、例如基于与该请求所涉及的组织的不同 STS 2420、2422、2424、2426 进行通信来确认订户具有某些能力。如在其他实施例中，可以提供存储抽象服务 2440 来抽象数据库服务 2430（例如 SQL）的存储细节。

[0099] 图 25 是与网络服务 2520 的递送相联系的受信存储 2500 的示例性非限制性的框图，该受信存储 2500 包括具有确认和 / 或验证的可搜索地经加密的数据 2510。在该实施例中，订户 2540 或订户 2540 所使用的应用可以作为访问经加密存储 2500 的某些部分的请求的一部分来请求对通过请求确认实际接收的项目也是本应当接收的项目而返回的项目进行确认证明。就此而言，图 25 示出了可搜索加密技术与确认技术的组合。任选地，该系统还可以与基于声明的身份和访问管理相集成，这在此处的其他实施例中予以描述。就此而言，如在此处的各个实施例中所描述的那样，亦称联合信任覆盖的数字托管模式可以无缝地与更传统的基于声明的认证系统相集成。

[0100] 在图 25 中，受信数据存储 2500 或服务提供者或数据存储的主控者执行证明步骤，而数据的所有者（例如订户设备）执行确认。数据存储 2500 是受信的，因为用户可以相信其提供强力的保证，但是能够理解，物理实体实际上主控该数据，并且一些参与者不是完全受信的。

[0101] 图 26 是用于订阅的包括确认步骤的示例性、非限制性过程的流程图。在 2600，可搜索地经加密的数据的子集被从订户设备接收。在 2610，密钥信息被从密钥生成实例中生成，该密钥生成实例基于订户设备的身份信息生成该密钥信息。在 2620，根据在密钥信息中所定义的赋予给该订户设备的能力，经加密数据的子集被解密。在 2630，该子集中表示的项目可以被确认（例如数据占有的证明），并且数据在 2640 被访问。

[0102] 在许多情况下，所期望的是能够在不需要对经加密数据进行解密的情况下对经加密数据执行 PDP/POR。任选地，PDP 所需的密钥信息可以被编码在曾用可搜索加密被保护的元数据之内。尽管这是管理用于 PDP/POR 的密钥的有效方式，但是应当注意，存在许多高价值的场景，在这些场景中，可以在不需要访问明文内容的情况下对经加密数据执行 PDP/POR。

[0103] 图 27 示出了示例性、非限制性的确认挑战 / 响应协议，其中验证器 2700（例如数据所有者）向证明器 2710（例如数据服务提供者）发出密码挑战 2720。在接收到挑战 2720 以后，证明器 2710 根据数据和挑战来计算响应 2712。然后，挑战响应 2730 被返回给验证器 2700，该验证器 2700 然后执行计算以验证或证明该数据未曾被修改过 2702。

[0104] 在图 27 中总体上示出的确认被称为私用 PDP，但是应当注意，还存在“公用”版本，其中给第三方提供密钥（“公”钥）使得第三方充当根据类似协议的验证器，而不必去了解实际数据。POR，即验证的一个示例，与 PDP 不同，其中 PDP 提供数据是可检索的证明（无论任何破坏 / 修改与否），但是如下面 30 所示，基本协议是相同的，但是文档的结构和实际算法是不同的。此处的受信生态系统的各个实施方式组合可搜索加密和 POR/PDR 以使系统收益并且巩固信任。就此而言，在将数据提交给服务提供者以前，数据被可搜索地加密，并且对数据的后处理可以包括 POR 和 / 或 PDP。

[0105] 另外，如果需要提供更力的保证，则“数据分散 (dispersion)”技术可以任选地覆盖到上述任何一个或多个实施例中。利用数据分散，数据被分发给若干服务提供者以获得对抗任何单个服务提供者中的“大规模不良行为”或者灾难性损失的回复力。使用在此所示的信任机制，该分散以使得独立服务提供者难以串通和破坏数据的方式来执行。这类似于上述分布式 CKG 实施例的概念。

[0106] 图 28 是与网络服务 2520 的递送相联系的受信存储 2500 的另一示例性非限制性的框图，该受信存储 2500 包括具有确认和 / 或验证的可搜索地经加密的数据 2510。具体而言，图 28 示出了验证组件 2850，其用于验证返回给订户 2540 的项目未被篡改或者以其他方式被不经意地改变。上述 PDP 是验证的非限制性示例。

[0107] 图 29 是用于订阅的包括确认步骤的示例性、非限制性过程的流程图。在 2900，可搜索地经加密的数据的子集被从订户设备接收。在 2910，密钥信息被从密钥生成实例中生成，该密钥生成实例基于订户设备的身份信息生成该密钥信息。在 2920，根据在密钥信息中所定义的赋予给该订户设备的能力，经加密数据的子集被解密。在 2930，该子集中表示的项目的内容可以被验证（例如检索能力的证明），并且数据在 2940 被访问。

[0108] 图 30 示出了示例性、非限制性的验证挑战 / 响应协议，其中验证器 3000（例如数据所有者）向证明器 3010（例如数据服务提供者）发出密码挑战 3020。在接收到挑战 3020 以后，证明器 3010 根据数据和挑战来计算响应 3012。然后，挑战响应 3030 被返回给验证器 3000，该验证器 3000 然后执行计算以验证或证明该数据是可检索的 3002。

[0109] 图 31 是示出了非限制性场景的框图，在该场景中，多个独立的联合信任覆盖或者数字托管可以并排存在，或者针对分层方式彼此相叠地存在。在该场景中，存在具有可搜索地经加密的数据 3110 的受信数据存储 3100，各种网络服务 3120 可以基于该数据 3110。例如，网络服务 3120 可以包括作为云服务递送文字处理软件。作为地理分布等的一部分，任选地，可以提供多个覆盖 / 托管 3132、3134、3136，这些覆盖 / 托管每个都适应于不同的应用 / 垂直面 / 顺应性需要 / 统治实体要求，使得发布者 2530 或订户 3150 基于要求的集合或管辖权 / 住所区域来隐式或显示地选择正确的覆盖 / 托管。因此，该覆盖可以改变，但是来自云的后端服务可以保持不变，而不必使核心服务本身的递送复杂化。

[0110] 在此描述了多种示例性、非限制性的实施例，这些实施例示出了受信数据服务的递送。这些实施例不是独立的，而是可以在合适时彼此组合。另外，任何上述实施例都可以被扩展为多个可替代方式。例如，在一个实施例中，受信数据服务提供陷门或能力的到期和撤销，以获得数据访问的更大程度的安全性。在另一任选实施例中，权限管理层被构建到受信数据服务的提供中，例如以保护作为加密 / 解密的一部分附加于内容的权限或者阻止在数据托管中对受版权保护数据的操作，这些操作在明文中是可容易地识别或检测的。因此，在本发明的范围内可以构思在此所述的实施例的任何组合或置换。

[0111] 示例性、非限定性的实施方式

[0112] 数字托管模式的任何示例性实施方式被称为联合信任覆盖 (FTO)。在附录 A 中附有一些关于 FTP 实施方式的附加的非限制性细节。

[0113] 就此而言，数字托管模式仅仅是许多可能的模式和变型方案的一个示例。此外，该模式（其包括发布者、订户、管理员和审计员——以及可能地其他专用角色，这如上述那样）在另一底层 FTO 模式上分层，该底层 FTO 模式对 CTP、CSP、CKG 等等执行“教会和州 (church & state)”分离以维持信任。也可以存在多个独立 FTO 和 DEP，其可以在彼此不干涉并且甚至不知道彼此的存在的情况下共存。而且，可以在云存储服务提供者不协作或者甚至不了解这些模式 / 覆盖的存在的情况下在云存储上覆盖 DEP 和 FTO。

[0114] 更详细而言，FTO 是独立于云中数据服务的服务集合。这些服务由数据服务的运营商以外的多方来运行，并且能够提供关于针对由云服务主控的数据的机密性、篡改检测和不可抵赖性的强力保证。

[0115] 任何伙伴都可以构造和主控这些覆盖服务，例如居间程序服务、确认服务、存储抽象服务等等。这些伙伴可以选择主控参考实施方式或者基于公开可用的格式和协议来构造其自己的实施方式。

[0116] 由于格式、协议和参考实施方式的公开性质，可用直接维持诸如 FTO 的运营商和数据所有者之类的多方间的控制的分离。

[0117] 尽管加密是该解决方案的一个元素，但是在不同方的范围内联合的服务的组织也是该解决方案的一部分。尽管常规的加密技术对于许多场景而言是强制性的，但是它们排除了实现这些场景中的许多场景，比如篡改检测、不可抵赖性、通过组织多个（不受信任）的服务构建信任、搜索数据库等等。

[0118] 补充上下文

[0119] 如上所述，对于某些附加的非限制性上下文而言，受信的云供应集合为构件于信任之上的云实现了应用生态系统。在此所使用的各种技术包括 :CKG——密钥生成中心，一

种实体，其主控多承租人密钥生成中心，例如 Microsoft、VeriSign、Fidelity、、、中的任一都可以主控 CKG。就此而言，多承租人是任选的（例如期望但不是强制性的）。其他术语包括：CTP——密码技术提供者，一种实体，其提供加密技术以供与受信生态系统一起使用，例如 Symantec、Certicom、Voltage、PGP 公司、BitArmor、Enterprise、Guardian、Sovereign Entity 等等中的任一是可以为 CTP 的示例性公司。

[0120] 另外，术语“CSP”——云服务提供者是提供包括存储在内的云服务的实体。各种公司可以提供这样的数据服务。CIV——云索引确认器是用于确认所返回的索引的第二库。CSA——计算和存储抽象对存储后端进行抽象。STF——存储传输格式是用于跨多个库传输数据 / 元数据的通用格式。

[0121] 就此而言，如上所述，一些企业场景包括：使用数据服务技术或应用的工程外联网；设计和工程分析；定义制造商和供应商间的数据关系等等。因此，通过将信任分布在多个实体的范围内使得不存在“过分”受信任的实体或单点损害来为全部多个场景实现了唯一的生态系统。

[0122] 对于关于可搜索加密的某些补充上下文而言，用户通常具有或获得针对关键词的“能力”或“陷门”，并且然后发送请求，其中使用该“能力”将其呈现给服务器。服务器“组合”能力和索引以找出相关的文档或数据。然后，仅仅给用户提供对由该搜索产生的文档的访问（虽然用户可以访问不止这些文档）。

[0123] 如所提到的那样，不应当认为单个算法限制了在此所述的可搜索地经加密的数据存储的提供，然而，下面总体上概述了示例性非限制性算法后面的一些理论，并且提供了可搜索对称加密 (SSE) 模式的初步知识：

[0124] ●消息：m

[0125] ●关键词 $w_1$，…，$w_n$

[0126] ● PRF：H

[0127] ●生成托管密钥

[0128] ●针对 H 选择随机 S

[0129] ●加密

[0130] ●选择随机密钥 K

[0131] ●选择随机固定长度 r

[0132] ●对于 $1 \leqslant i \leqslant n$

[0133] 计算 $a_i = H_S(w_i)$

[0134] 计算 $b_i = H_{ai}(r)$

[0135] 计算 $c_i = b_i \oplus flag$

[0136] 输出 $(E_K(m), r, c_1, \cdots, c_n)$

[0137] ●针对 w 生成陷门或能力

[0138] ● $d = H_{Sj}(w)$

[0139] ●针对 w 进行测试

[0140] ●计算 $p = H_d(r)$

[0141] ●计算 $z = p \oplus c_i$

[0142] ●如果 z = flag，则输出“真”

[0143] ●对 $E_K(m)$ 进行解密以获得 m

[0144] 尽管再次不应当认为限制了在此所述的任何实施例，但是下面是关于公钥加密 w/关键词搜索 (PEKS) 模式的初步知识。

[0145] 公钥加密

[0146] a. PKE = (Gen, Enc, Dec)

[0147] 基于身份的加密

[0148] b. IBE = (Gen, Enc, Extract, Dec)

[0149] c. 生成主密钥

[0150] i. (msk, mpk) = IBE.Gen()

[0151] d. 针对 ID 对 m 进行加密

[0152] i. c = IBE.Enc(mpk, ID, m)

[0153] e. 针对 ID 生成密钥

[0154] i. sk = IBE.Extract(msk, ID)

[0155] f. 解密

[0156] i. m = IBE.Dec(sk, c)

[0157] g. 消息 :m

[0158] h. 关键词 :$w_1$, …, $w_n$

[0159] i. 生成托管密钥

[0160] i. (msk, mpk) = IBE.Gen()

[0161] ii. (pk, sk) = PKE.Gen()

[0162] j. 加密

[0163] k. 对于 $1 \leqslant i \leqslant n$

[0164] i. $c_i$ = IBE.Enc(mpk, $w_i$, flag)

[0165] l. 返回 (PKE.Enc(pk, m), $c_1$, , $c_n$)

[0166] m. 为 w 生成能力或陷门

[0167] i. d = IBE.Extract(msk, w)

[0168] n. 针对 w 进行测试

[0169] o. 对于 $1 \leqslant i \leqslant n$

[0170] i. z = IBE.Dec(d, $c_i$)

[0171] ii. 如果 z = flag，则输出“真”

[0172] 对 $E_K(m)$ 进行解密以获得 m

[0173] 示例性联网和分布式环境

[0174] 本领域普通技术人员可以理解，此处所描述的用于受信云服务框架的方法和设备的各实施例和有关的各实施例可以结合任何计算机或其它客户端或服务器设备来实现，该任何计算机或其它客户端或服务器设备可作为计算机网络的一部分来部署或者被部署在分布式计算环境中，并且可以连接到任何种类的数据存储。就此，此处所描述的各实施例可以在具有任意数量的存储器或存储单元以及出现在任意数量的存储单元上的任意数量的应用程序和进程的任何计算机系统和环境中实现。这包括但不限于具有部署在具有远程或本地存储的网络环境或分布式计算环境中的服务器计算机和客户计算机的环境。

[0175] 附图 32 提供了示例性联网或分布式计算环境的非限制性示意图。该分布式计算环境包括计算对象 3210、3212 等以及计算对象或设备 3220、3222、3224、3226、3228 等，这些计算对象或设备可包括如由应用程序 3230、3232、3234、3236、3238 表示的程序、方法、数据存储、可编程逻辑等。能够理解，对象 3210、3212 等以及计算对象或设备 3220、3222、3224、3226、3228 等可包括不同的设备，比如 PDA、音频 / 视频设备、移动电话、MP3 播放器、膝上型计算机等。

[0176] 每一个对象 3210、3212 等以及计算对象或设备 3220、3222、3224、3226、3228 等可通过通信网络 3240 直接或间接与一个或多个其他对象 3210、3212 等以及计算对象或设备 3220、3222、3224、3226、3228 等进行通信。即使在附图 32 中被示为单个元件，但网络 3240 可包括向附图 32 的系统提供服务的其他计算对象或解释设备，和 / 或可表示未示出的多个互连网络。每个对象 3210、3212 等或 3220、3222、3224、3226、3228 等还可包含诸如应用程序 3230、3232、3234、3236、3238 之类的应用程序，该应用程序可利用 API 或适用于与根据本发明的各实施例来提供的受信云计算服务进行通信或适用于实现受信云计算服务的其他对象、软件、固件和 / 或硬件。

[0177] 存在支持分布式计算环境的各种系统、组件和网络配置。例如，计算系统可以由有线或无线系统、本地网络或广泛分布的网络连接在一起。当前，许多网络被耦合至因特网，后者为广泛分布的计算提供了基础结构并包含许多不同的网络，但任何网络基础结构可用于变得与如各实施例中所描述的技术相关联的示例性通信。

[0178] 因此，可以利用诸如客户端 / 服务器、对等、或混合架构等网络拓扑结构和网络基础结构的主机。在客户端 / 服务器架构中，尤其在联网系统中，客户端通常是访问由例如服务器等另一计算机提供的共享的网络资源的计算机。在图 32 的图示中，作为非限制性示例，计算机 3220、3222、3224、3226、3228 等可被认为是客户端而计算机 3210、3212 等，可被认为是服务器，其中服务器 3210、3212 等提供数据服务，诸如从客户端计算机 3220、3222、3224、3226、3228 等接收数据、存储数据、处理数据、向客户端计算机 3220、3222、3224、3226、3228 发送数据等，但任何计算机都可取决于环境而被认为是客户端、服务器或两者。这些计算设备中的任一个都可以处理数据，或请求可指示此处所描述的技术的经改善的用户简档和相关技术的服务或任务。

[0179] 服务器通常是可通过诸如因特网或无线网络基础架构等远程网络或本地网络访问的远程计算机系统。客户端进程可以在第一计算机系统中活动，而服务器进程可以在第二计算机系统中活动，它们通过通信介质彼此通信，从而提供分布式功能并允许多个客户端利用服务器的信息收集能力。按照用户简档来利用的任何软件对象可以单独提供或跨多个计算设备或对象分布。

[0180] 在其中通信网络 / 总线 3240 是因特网的网络环境中，服务器 3210、3212 等可以是客户端 3220、3222、3224、3226、3228 等通过诸如超文本传输协议 (HTTP) 等多种已知协议中的任一种与其通信的 web 服务器。服务器 3210、3212 等也可担当客户端 3220、3222、3224、3226、3228 等，这是分布式计算环境的特性。

[0181] 示例性计算设备

[0182] 如所提到的那样，此处描述的各实施例适用于其中可能期望实现受信云服务框架的一个或多个部分的任何设备。因此，应当理解，构思了结合此处描述的各实施例使用的手

持式、便携式和其它计算设备和计算对象，即在设备可以结合受信云服务框架来提供某些功能的任何地方。因此，在下面的图 33 中描述的以下通用远程计算机仅是一个示例，且所公开的主题的各实施例可用具有网络 / 总线互操作性和交互的任何客户端来实现。

[0183] 尽管并不是必需的，但各实施例的任意一个可以部分地经由操作系统来实现，以供设备或对象的服务开发者使用，和 / 或被包括在结合可操作组件来操作的应用软件中。软件可以在由诸如客户端工作站、服务器或其他设备等一个或多个计算机执行的诸如程序模块等计算机可执行指令的通用上下文中描述。本领域的技术人员可以理解，网络交互可以用各种计算机系统配置和协议来实施。

[0184] 因此，图 33 示出了其中可实现一个或多个实施例的合适的计算系统环境 3300 的一个示例，但是上面已经弄清楚，计算系统环境 3300 仅为合适的计算环境的一个示例，并且不旨在对各实施例中的任意一个的使用范围或功能提出任何限制。也不应该将计算环境 3300 解释为对示例性操作环境 3300 中示出的任一组件或其组合有任何依赖性或要求。

[0185] 参考图 33，用于实现此处的一个或多个实施例的示例性远程设备可以包括手持式计算机 3310 形式的通用计算设备。手持式计算机 3310 的组件可以包括但不限于 ：处理单元 3320、系统存储器 3330 和将包括系统存储器在内的各种系统组件耦合至处理单元 3320 的系统总线 3321。

[0186] 计算机 3310 通常包括各种计算机可读介质，并可以是可由计算机 3310 访问的任何可用介质。系统存储器 3330 可以包括诸如只读存储器 (ROM) 和 / 或随机存取存储器 (RAM) 等易失性和 / 或非易失性存储器形式的计算机存储介质。作为示例而非限制，存储器 3330 还可以包括操作系统、应用程序、其他程序模块、和程序数据。

[0187] 用户可以通过输入设备 3340 向计算机 3310 输入命令和信息。监视器或其他类型的显示设备也经由接口，诸如输出接口 3350 连接至系统总线 3321。除监视器之外，计算机还可以包括其他外围输出设备，如扬声器和打印机，它们可以通过输出接口 3350 连接。

[0188] 计算机 3310 可使用至一个或多个远程计算机，诸如远程计算机 3370 的逻辑连接在网络化或分布式环境中操作。远程计算机 3370 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其他常见网络节点、或任何其他远程媒体消费或传输设备，并且可以包括上面关于计算机 3310 所描述的任何或全部元件。附图 33 所示的逻辑连接包括诸如局域网 (LAN) 或广域网 (WAN) 等的网络 3371，但也可以包括其他网络 / 总线。这样的联网环境在家庭、办公室、企业范围计算机网络、内联网和因特网中是常见的。

[0189] 如上所述，尽管结合各计算设备、网络和广告架构描述了示例性实施例，但还可将底层概念应用于其中期望结合与云服务的交互来提供信任的任何网络系统和任何计算设备或系统。

[0190] 有多种实现此处描述的一个或多个实施例的方式，例如，使应用和服务能使用受信云服务框架的适当 API、工具包、驱动程序代码、操作系统、控件、独立或可下载的软件对象等等。可以从 API（或其他软件对象）的观点以及从提供根据所描述的实施例中的一个或多个的定点平台的软件或硬件对象来构想各实施例。此处描述的各种实现和实施例可以具有完全采用硬件、部分采用硬件并且部分采用软件、以及采用软件的方面。

[0191] 在本文中使用的词语“示例性”意味着用作示例、实例或说明。为避免疑惑，本文公开的主题不受限于这样的示例。此外，本文描述为“示例性”的任何方面或设计不必解释成

优于其他方面或设计或比其他方面或设计有利，它也不旨在排除本领域的普通技术人员所知的等效示例性结构和技术。而且，就术语“包括”、“具有”、“包含”和其他类似的词语在详细描述或权利要求书中的使用而言，为避免疑惑，这样的术语旨在以类似于术语“包括”作为开放的过渡词的方式解释而不排除任何附加或其他元素。

[0192] 如上所述，此处所述的各种技术可结合硬件或软件，或在适当时以两者的组合来实现。如在此所使用的，术语“组件”、“系统”等同样指的是计算机相关实体，或者是硬件、硬件和软件的组合、软件或执行中的软件。例如，组件可以是，但不限于是，在处理器上运行的进程、处理器、对象、可执行码、执行的线程、程序和 / 或计算机。作为说明，运行在计算机上的应用程序和计算机本身都可以是计算机组件。一个或多个组件可以驻留在进程和 / 或执行线程中，并且组件可以位于一个计算机内和 / 或分布在两个或更多的计算机之间。

[0193] 已经关于若干组件之间的交互描述了前述系统。应该理解，这样的系统和组件可以包括根据前述的各种置换和组合的那些组件或指定的子组件、指定的组件或子组件中的某一些、和 / 或另外的组件。子组件也可以被实现为通信耦合至其他组件而非被包括在父组件（分层）内的组件。另外，应注意到一个或多个组件可被组合成提供聚集功能的单个组件，或被分成若干单独的子组件，且诸如管理层等任何一个或多个中间层可被设置成通信耦合到这样的子组件以便提供集成功能。此处描述的任何组件也可以与在此未具体描述但本领域的技术人员公知的一个或多个其他组件交互。

[0194] 鉴于以上描述的示例性系统，参考各附图的流程图将可以更好地理解依照所公开的主题实现的方法。尽管为了说明简洁起见，作为一系列框示出和描述了方法，但是，应该理解，所要求保护的主题不仅限于所描述框的顺序，一些框可以按与此处所描绘和描述的不同的顺序进行和 / 或与其他框并发地进行。尽管经由流程图示出了非顺序或分支的流程，但可以理解，可实现达成相同或类似结果的各种其他分支、流程路径和框次序。此外，并非全部所示出的方框都是实现下面所描述的方法所必需的。

[0195] 虽然在某些实施例中，说明了客户端侧观点，但要出于避免存在相对应的服务器观点的疑问来理解，反之亦然。类似地，在实施方法的地方，可以提供具有存储和被配置成经由一个或多个组件实施该方法的至少一个处理器的相对应的设备。

[0196] 尽管结合各附图的优选实施例描述了各实施例，但可以理解，可以使用其他类似的实施例，或可以对所描述的实施例进行修改和添加来执行相同的功能而不背离本发明。而且，此处描述的各实施例的一个或多个方面可以在多个处理芯片或设备中实现或跨多个处理芯片或设备实现，且存储可以类似地跨多个设备来实现。因此，本发明不应限于任何单个实施例，而是应该根据所附权利要求书的广度和范围来解释。

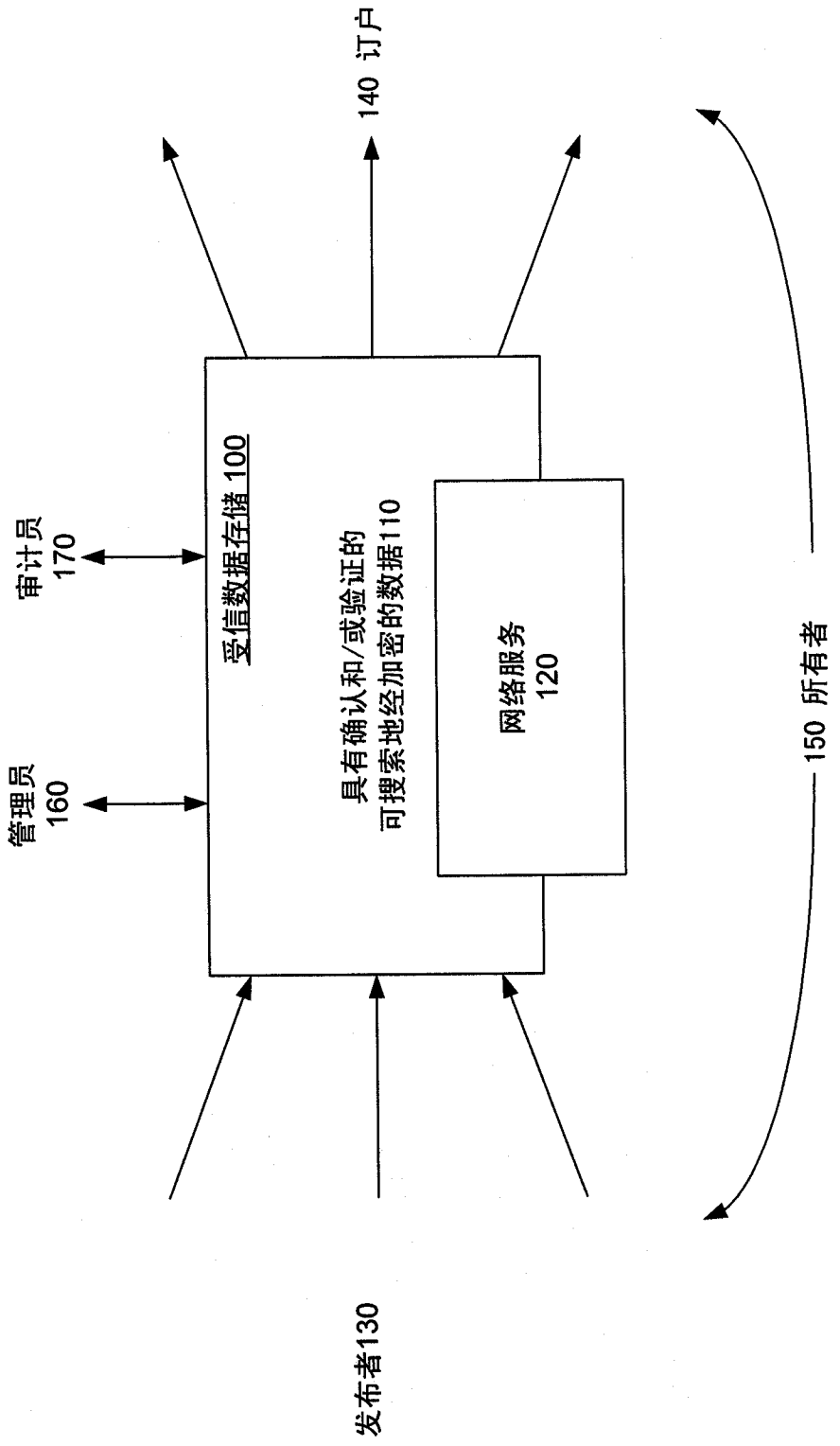

140 订户
审计员
170
管理员
160
受信数据存储 100
具有确认和/或验证的
可搜索地经加密的数据110
网络服务
120
150 所有者
发布者130

图 1

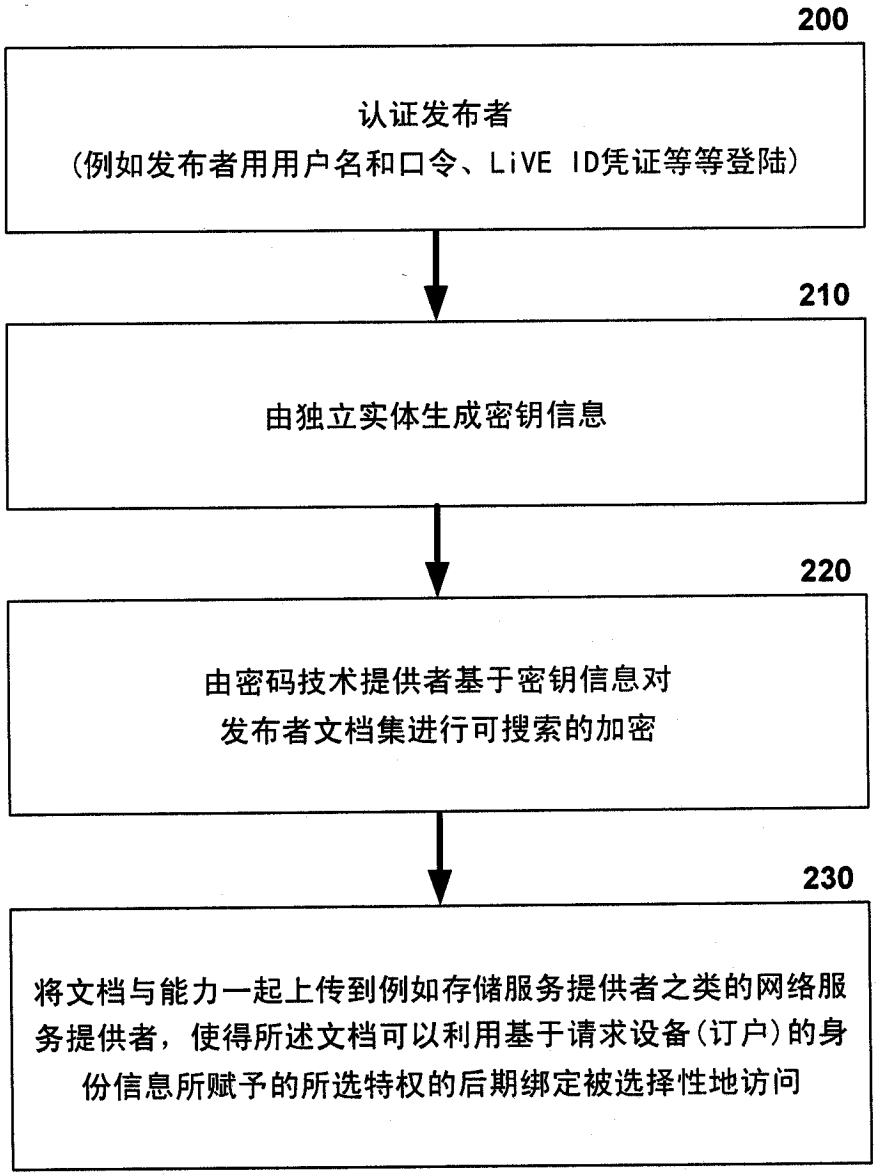

200
认证发布者
(例如发布者用用户名和口令、LiVE ID凭证等等登陆)
210
由独立实体生成密钥信息
220
由密码技术提供者基于密钥信息对
发布者文档集进行可搜索的加密
230
将文档与能力一起上传到例如存储服务提供者之类的网络服务提供者，使得所述文档可以利用基于请求设备(订户)的身份信息所赋予的所选特权的后期绑定被选择性地访问

图 2

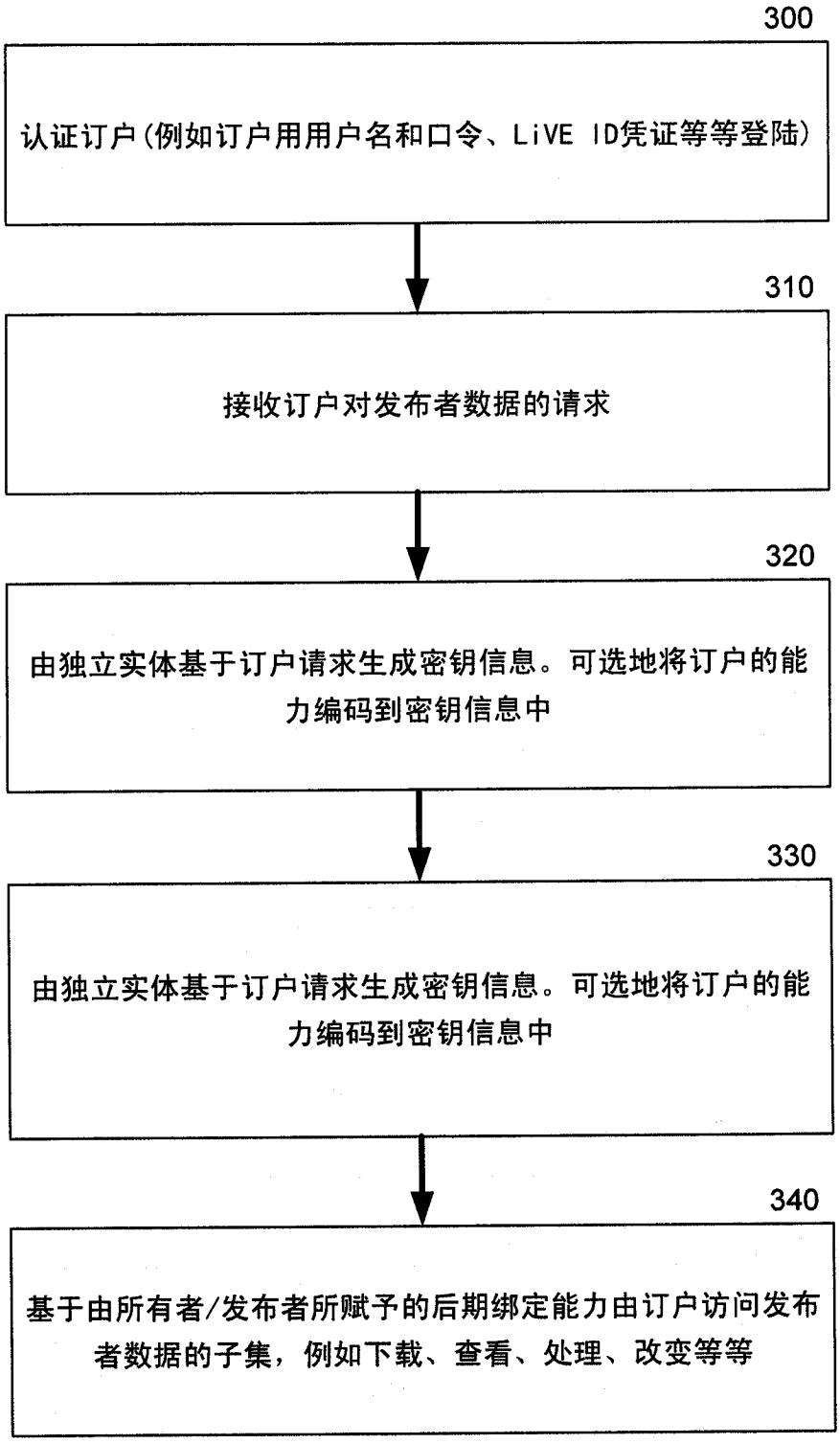

300
认证订户(例如订户用用户名和口令、LiVE ID凭证等等登陆)
310
接收订户对发布者数据的请求
320
由独立实体基于订户请求生成密钥信息。可选地将订户的能力编码到密钥信息中
330
由独立实体基于订户请求生成密钥信息。可选地将订户的能力编码到密钥信息中
340
基于由所有者/发布者所赋予的后期绑定能力由订户访问发布者数据的子集，例如下载、查看、处理、改变等等

图 3

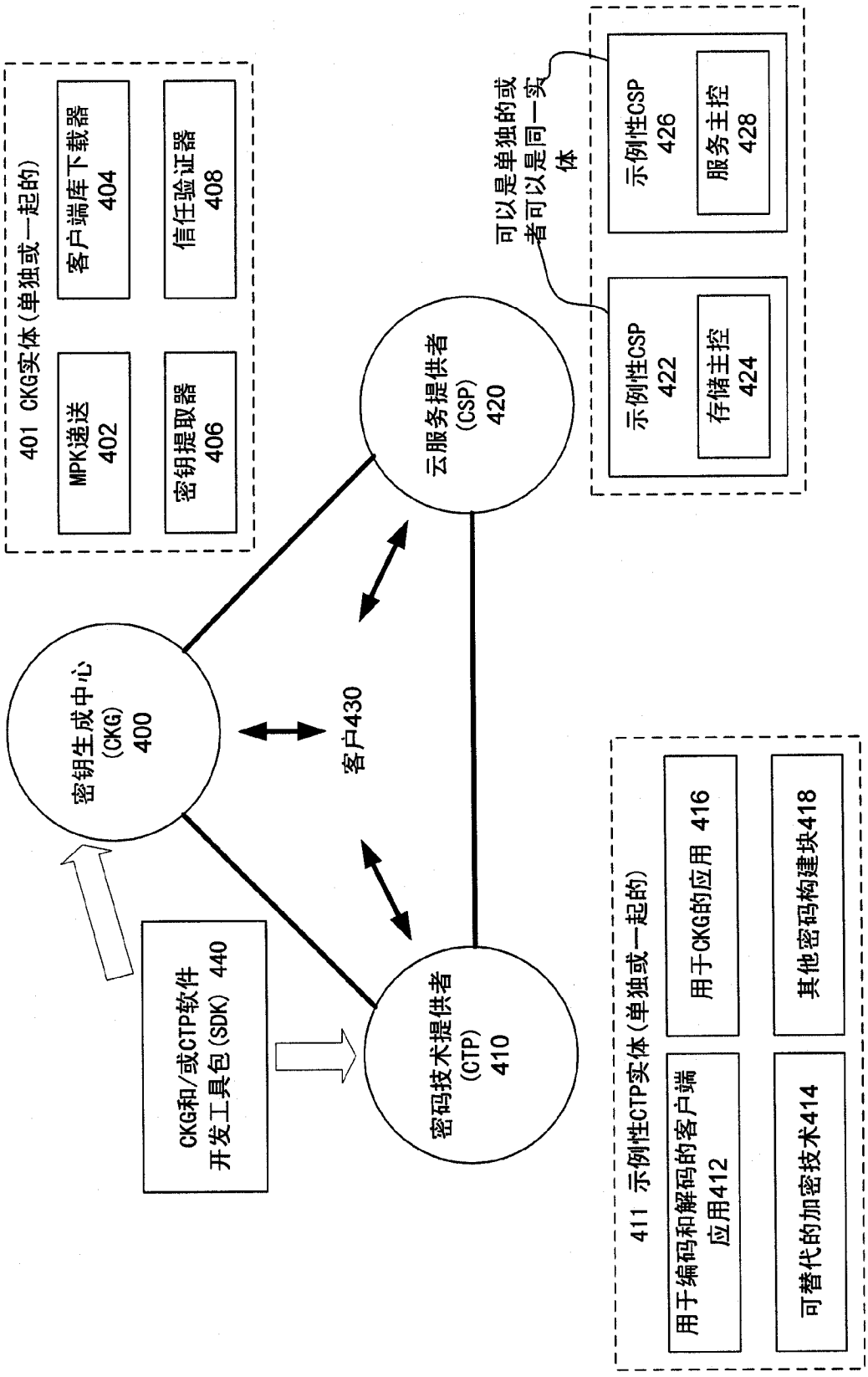

401 CKG实体(单独或一起的)
MPK递送 402
客户端库下载器 404
密钥提取器 406
信任验证器 408
密钥生成中心 (CKG) 400
客户430
云服务提供者 (CSP) 420
可以是单独的或者可以是同一实体
示例性CSP 422
存储主控 424
示例性CSP 426
服务主控 428
CKG和/或CTP软件开发工具包(SDK) 440
密码技术提供者 (CTP) 410
411 示例性CTP实体(单独或一起的)
用于编码和解码的客户端应用412
用于CKG的应用 416
可替代的加密技术414
其他密码构建块418

图 4

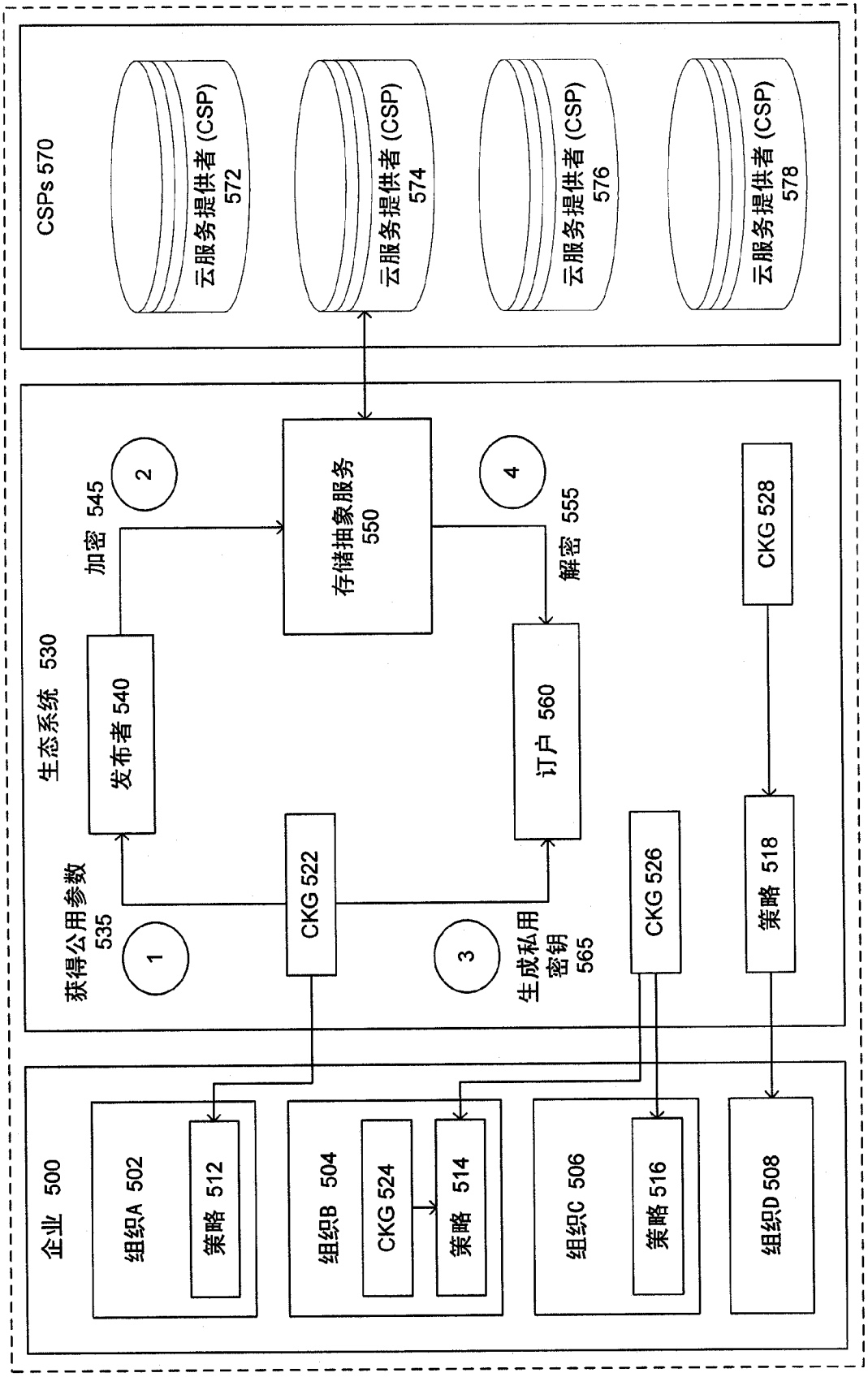

CSPs 570
云服务提供者 (CSP) 572
云服务提供者 (CSP) 574
云服务提供者 (CSP) 576
云服务提供者 (CSP) 578
生态系统 530
存储抽象服务 550
加密 545
解密 555
发布者 540
订户 560
CKG 522
CKG 526
CKG 528
策略 518
获得公用参数 535
生成私用密钥 565
企业 500
组织A 502
策略 512
组织B 504
CKG 524
策略 514
组织C 506
策略 516
组织D 508
1
2
3
4

图 5

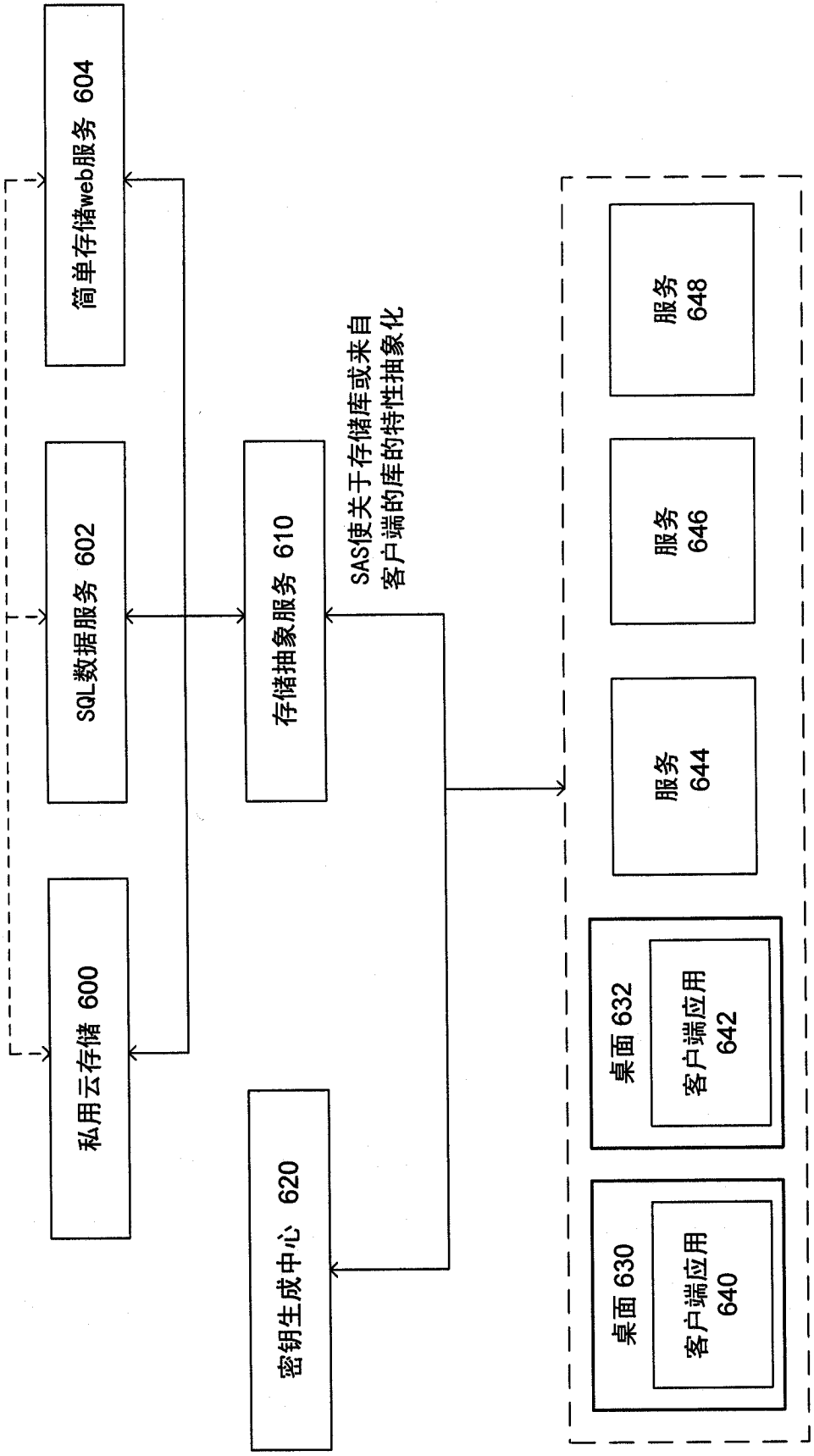

简单存储web服务 604
SQL数据服务 602
私用云存储 600
存储抽象服务 610
SAS使关于存储库或来自
客户端的库的特性抽象化
密钥生成中心 620
服务
648
服务
646
服务
644
桌面 632
客户端应用
642
桌面 630
客户端应用
640

图 6

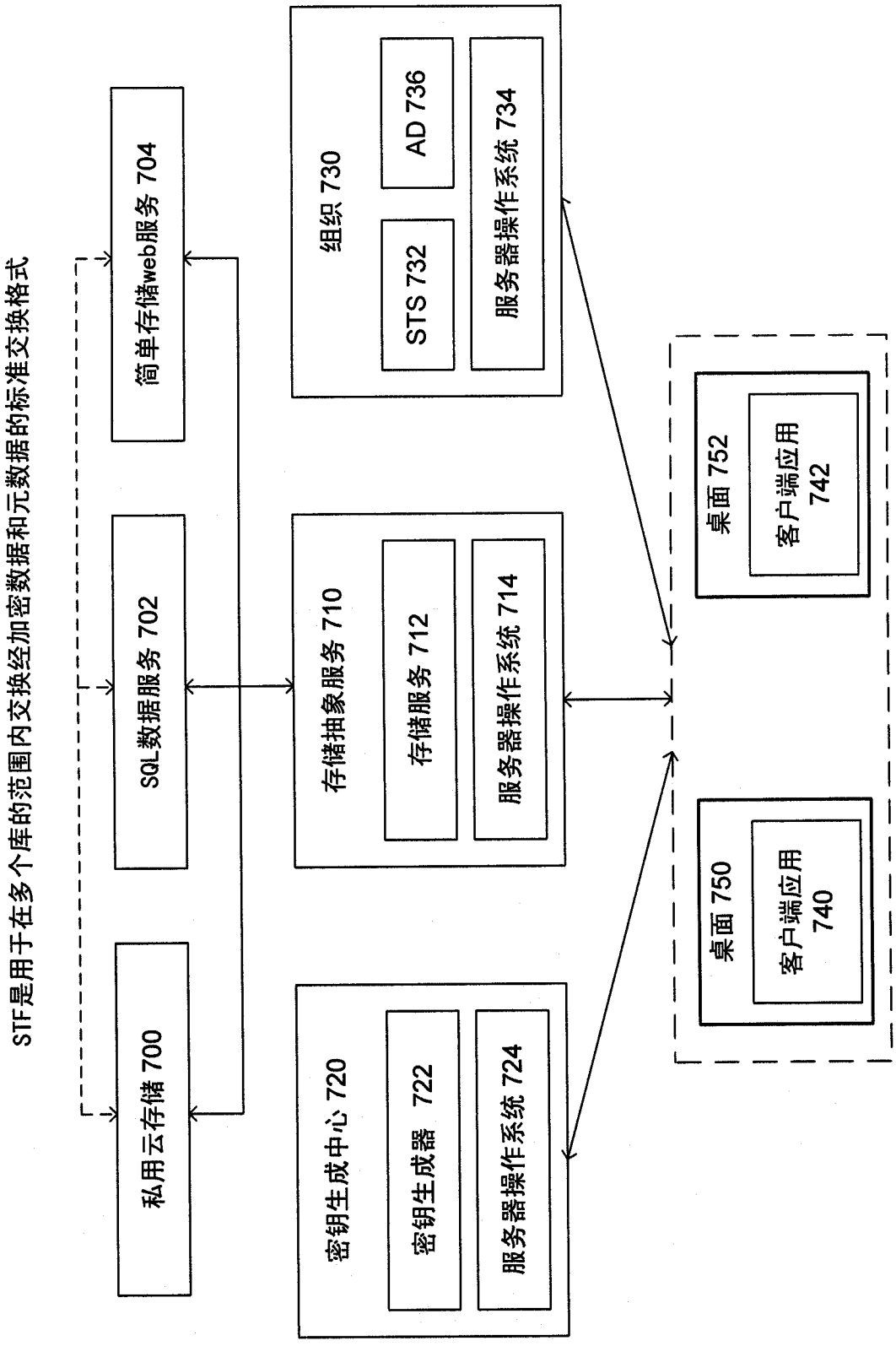

STF是用于在多个库的范围内交换经加密数据和元数据的标准交换格式
简单存储web服务 704
SQL数据服务 702
私用云存储 700
组织 730
AD 736
STS 732
服务器操作系统 734
存储抽象服务 710
存储服务 712
服务器操作系统 714
密钥生成中心 720
密钥生成器 722
服务器操作系统 724
桌面 752
客户端应用 742
桌面 750
客户端应用 740

图 7

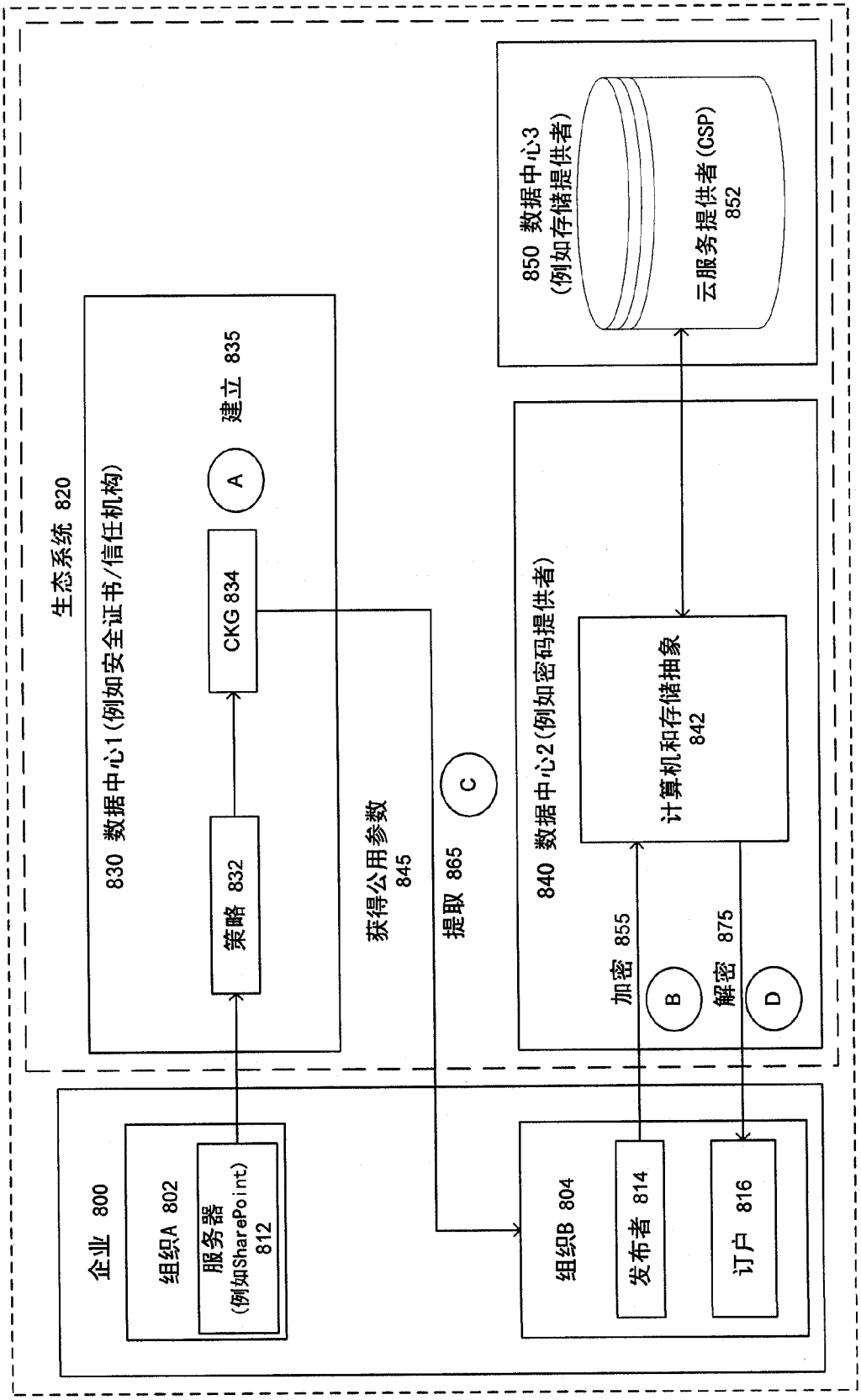

生态系统 820
企业 800
组织A 802
服务器
(例如SharePoint)
812
组织B 804
发布者 814
订户 816
830 数据中心1(例如安全证书/信任机构)
策略 832
CKG 834
建立 835
A
获得公用参数
845
提取 865
C
840 数据中心2(例如密码提供者)
加密 855
B
解密 875
D
计算机和存储抽象
842
850 数据中心3
(例如存储提供者)
云服务提供者(CSP)
852

图 8

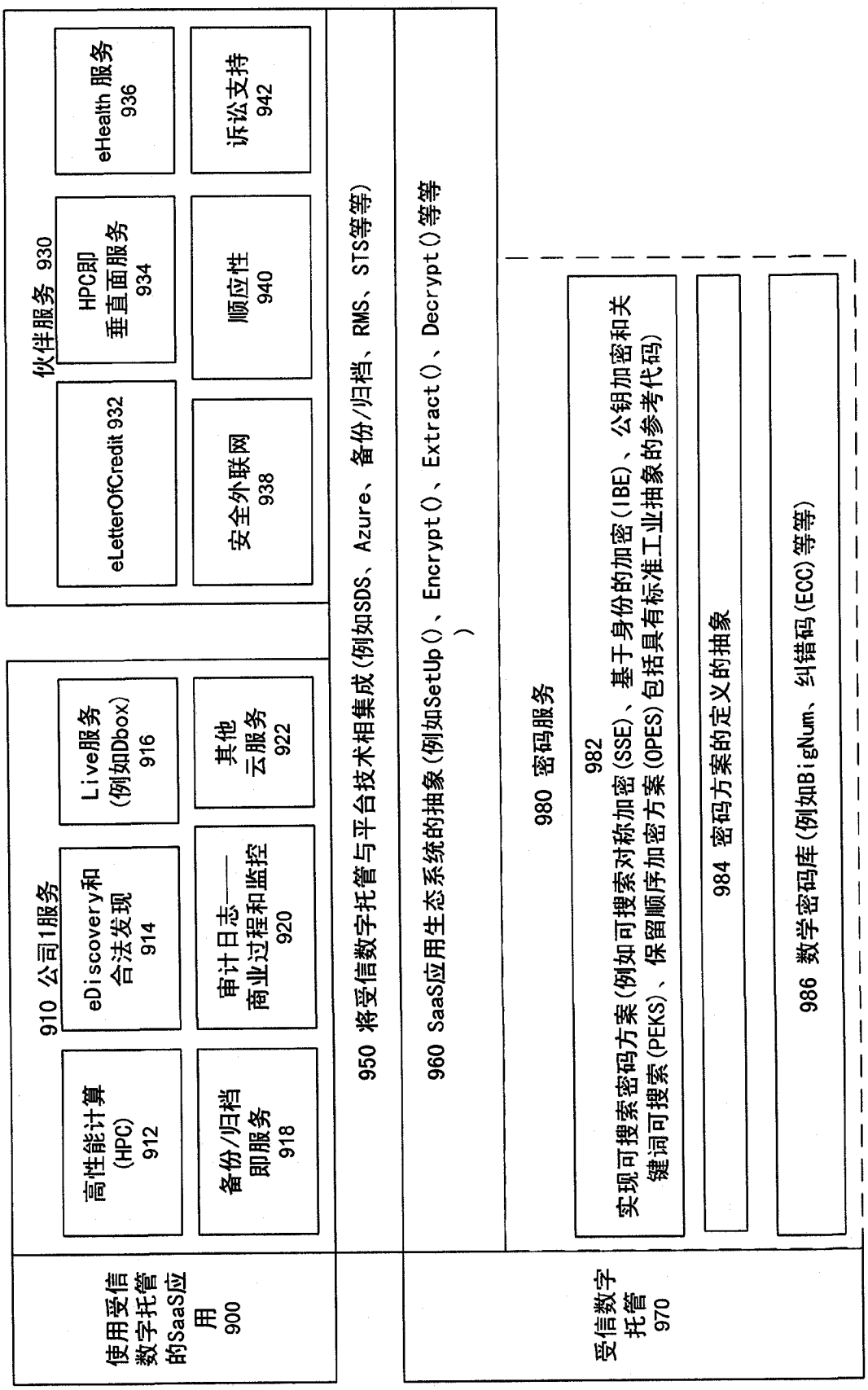

使用受信数字托管的SaaS应用 900
910 公司1服务
高性能计算(HPC) 912
eDiscovery和合法发现 914
Live服务(例如Dbox) 916
备份/归档即服务 918
审计日志——商业过程和监控 920
其他云服务 922
伙伴服务 930
eLetterOfCredit 932
HPC即垂直面服务 934
eHealth 服务 936
安全外联网 938
顺应性 940
诉讼支持 942
950 将受信数字托管与平台技术相集成(例如SDS、Azure、备份/归档、RMS、STS等等)
960 SaaS应用生态系统的抽象(例如SetUp()、Encrypt()、Extract()、Decrypt()等等)
受信数字托管 970
980 密码服务
982 实现可搜索密码方案(例如可搜索对称加密(SSE)、基于身份的加密(IBE)、公钥加密和关键词可搜索(PEKS)、保留顺序加密方案(OPES)包括具有标准工业抽象的参考代码)
984 密码方案的定义的抽象
986 数学密码库(例如BigNum、纠错码(ECC)等等)

图 9

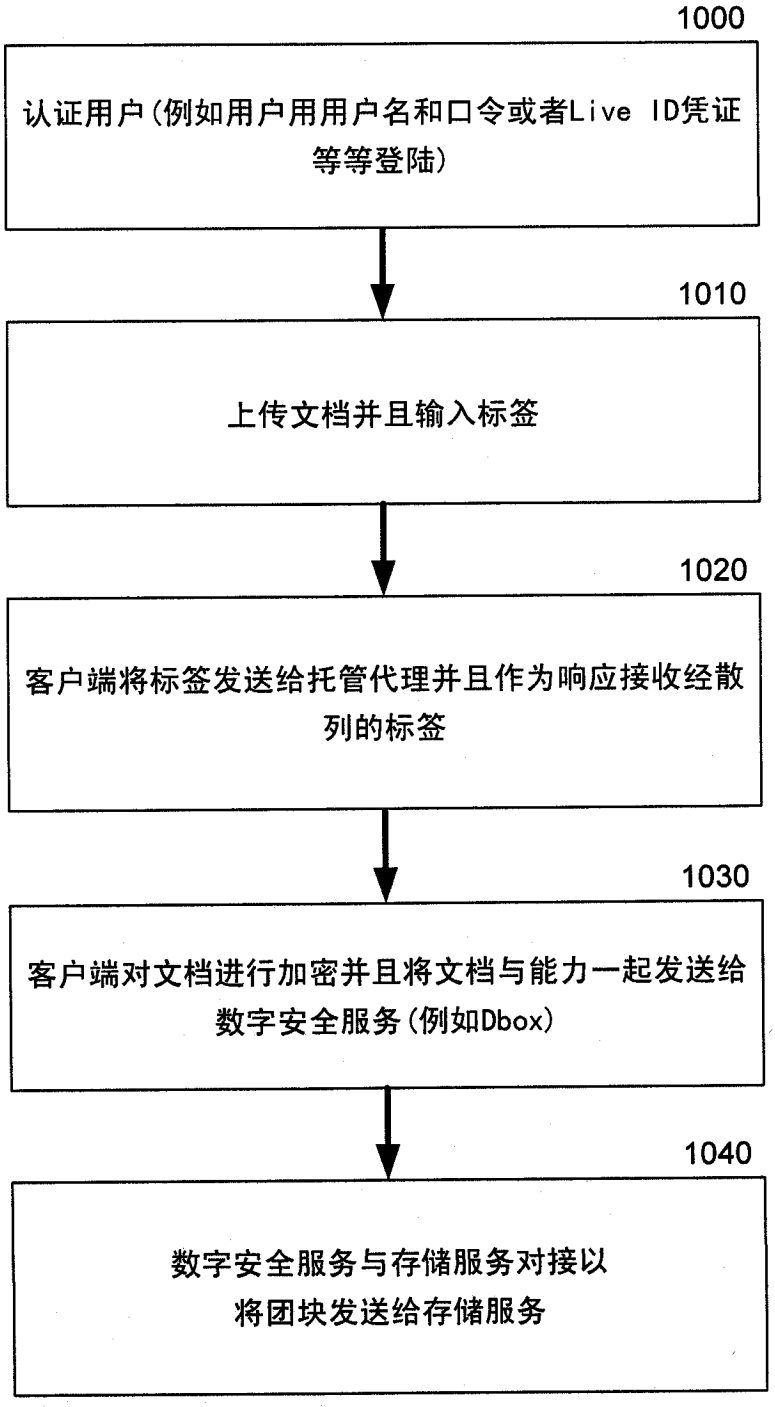

1000
认证用户(例如用户用用户名和口令或者Live ID凭证等等登陆)
1010
上传文档并且输入标签
1020
客户端将标签发送给托管代理并且作为响应接收经散列的标签
1030
客户端对文档进行加密并且将文档与能力一起发送给数字安全服务(例如Dbox)
1040
数字安全服务与存储服务对接以将团块发送给存储服务

图 10

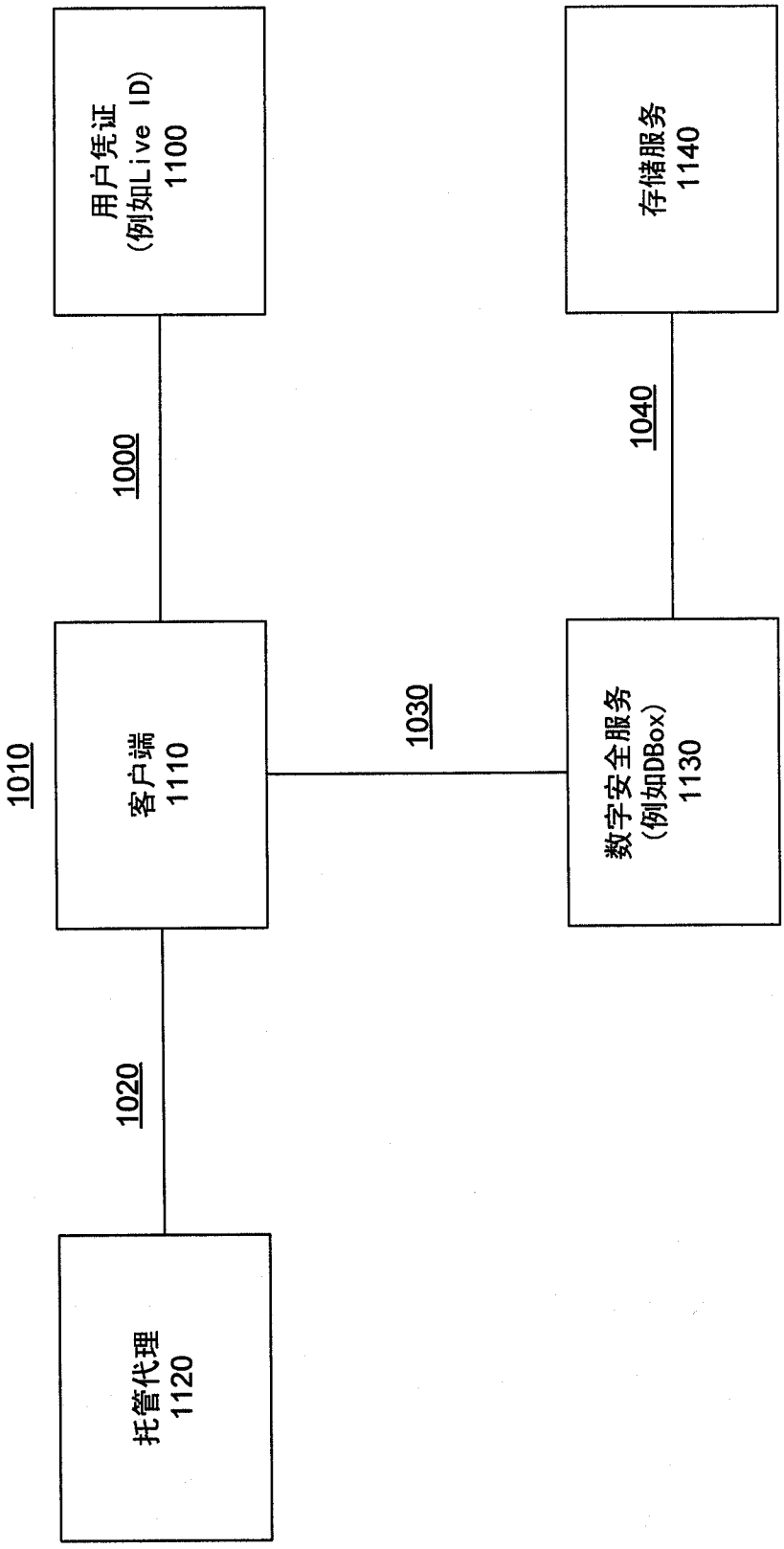

用户凭证
(例如Live ID)
1100
存储服务
1140
1000
1040
1010
客户端
1110
1030
数字安全服务
(例如DBox)
1130
1020
托管代理
1120

图 11

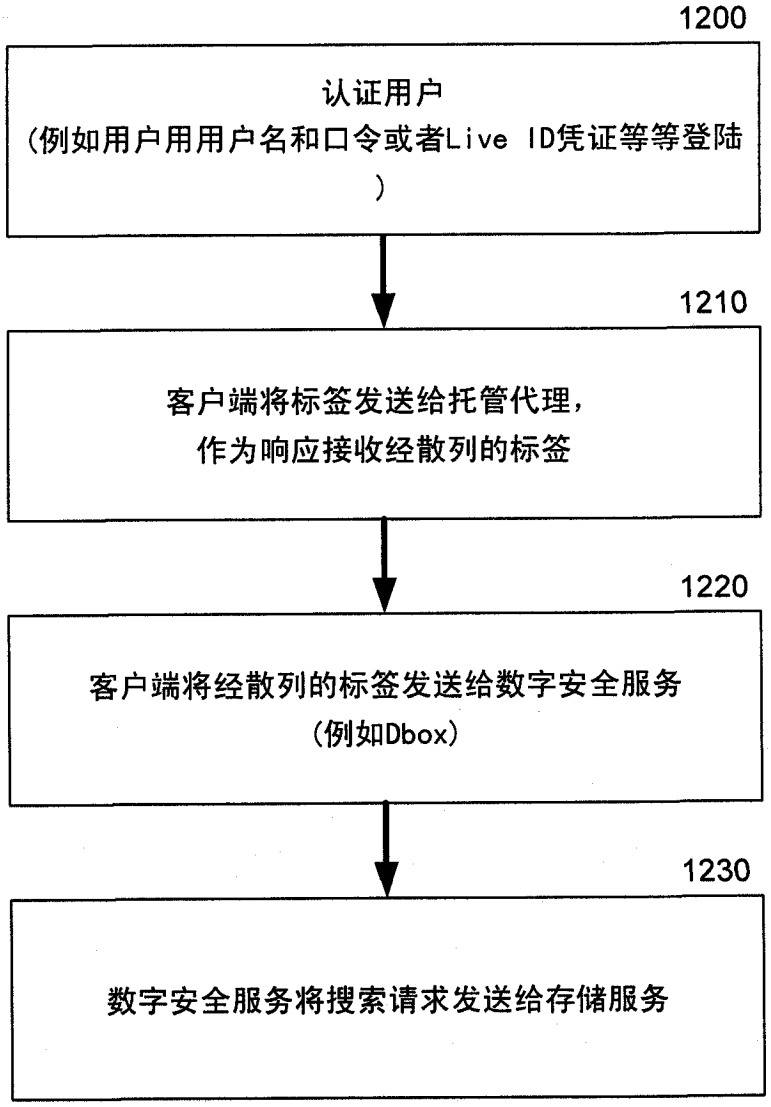

1200
认证用户
(例如用户用用户名和口令或者Live ID凭证等等登陆
)
1210
客户端将标签发送给托管代理，
作为响应接收经散列的标签
1220
客户端将经散列的标签发送给数字安全服务
(例如Dbox)
1230
数字安全服务将搜索请求发送给存储服务

图 12

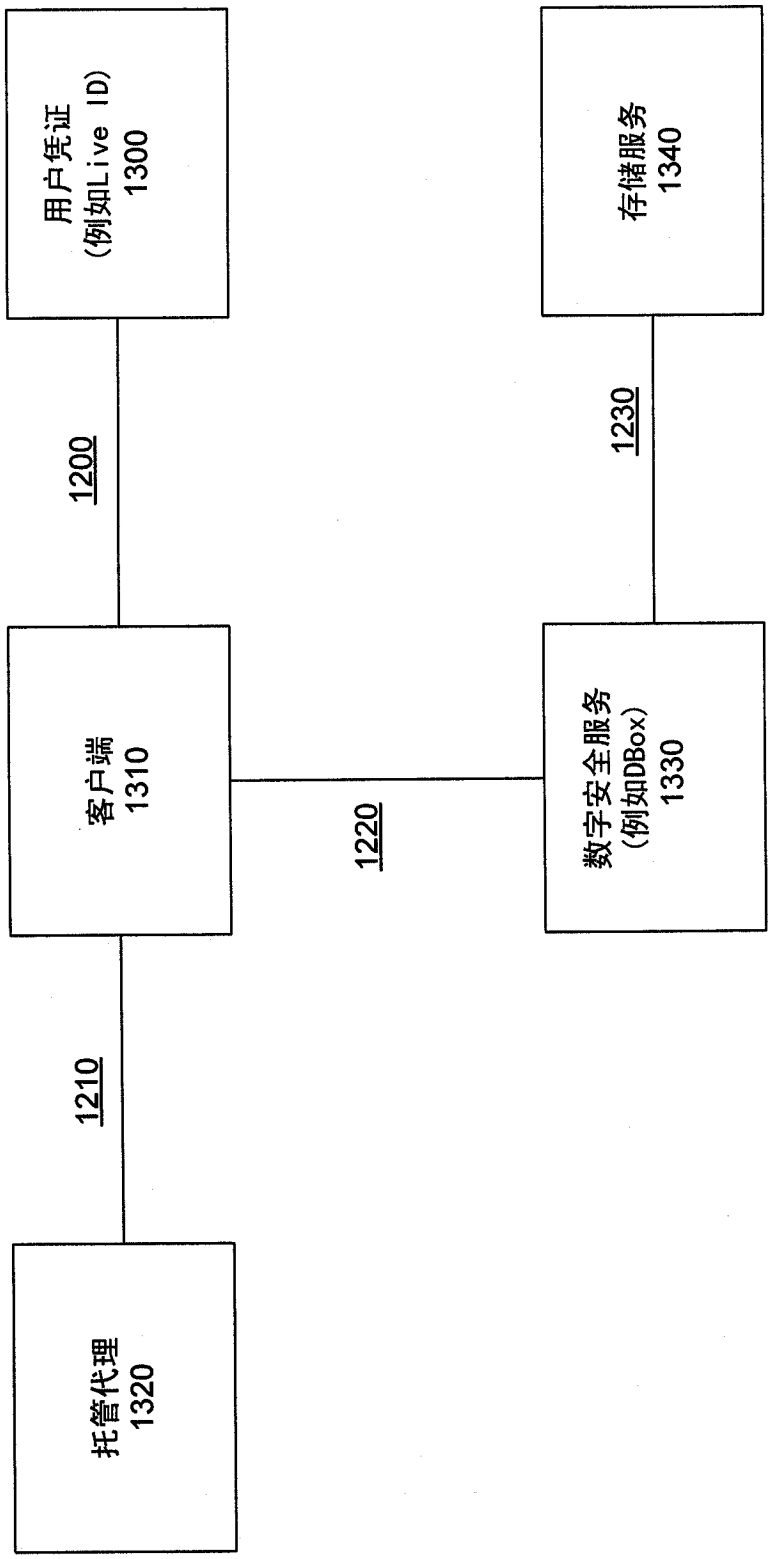

用户凭证
(例如Live ID)
1300
存储服务
1340
1200
1230
客户端
1310
1220
数字安全服务
(例如DBox)
1330
1210
托管代理
1320

图 13

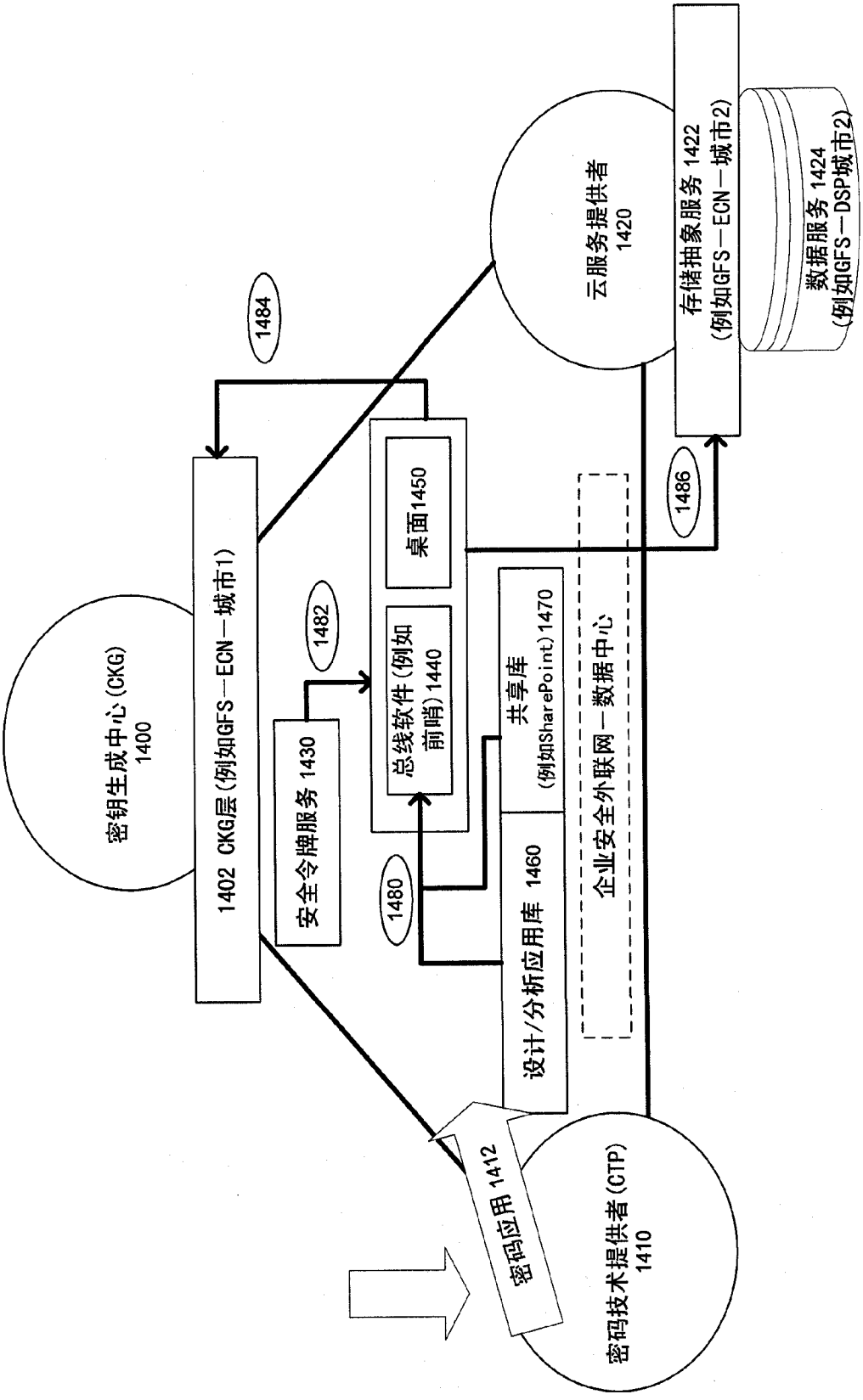

密钥生成中心(CKG)
1400
1402 CKG层(例如GFS—ECN—城市1)
安全令牌服务 1430
1482
总线软件(例如前哨)1440
桌面1450
1484
云服务提供者
1420
存储抽象服务 1422
(例如GFS—ECN—城市2)
数据服务 1424
(例如GFS—DSP城市2)
1486
共享库
(例如SharePoint)1470
1480
设计/分析应用库 1460
企业安全外联网—数据中心
密码应用 1412
密码技术提供者(CTP)
1410

图 14

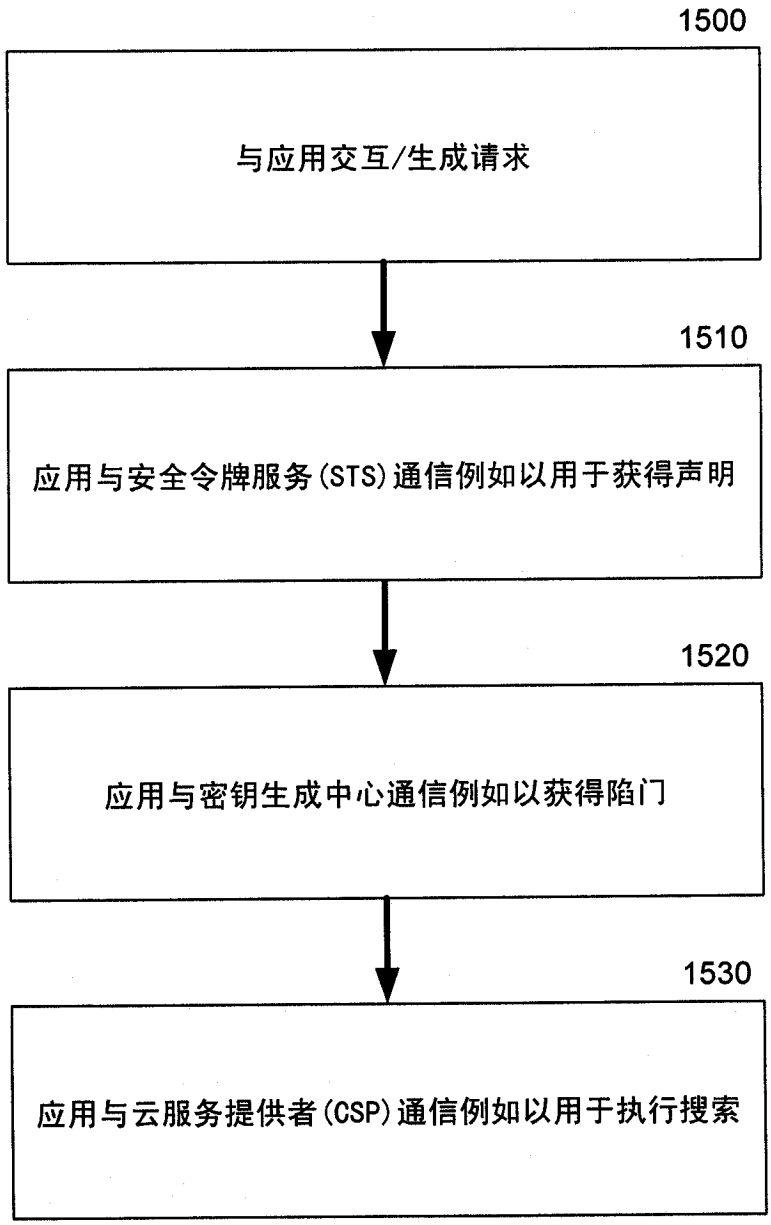

1500
与应用交互/生成请求
1510
应用与安全令牌服务(STS)通信例如以用于获得声明
1520
应用与密钥生成中心通信例如以获得陷门
1530
应用与云服务提供者(CSP)通信例如以用于执行搜索

图 15

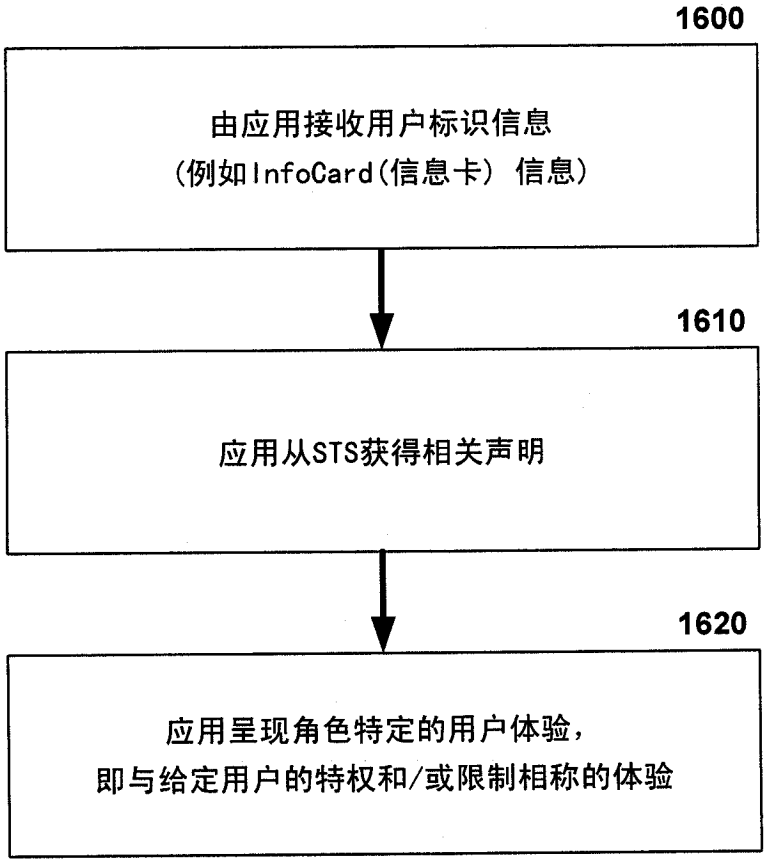

1600
由应用接收用户标识信息
(例如InfoCard(信息卡) 信息)
1610
应用从STS获得相关声明
1620
应用呈现角色特定的用户体验，
即与给定用户的特权和/或限制相称的体验

图 16

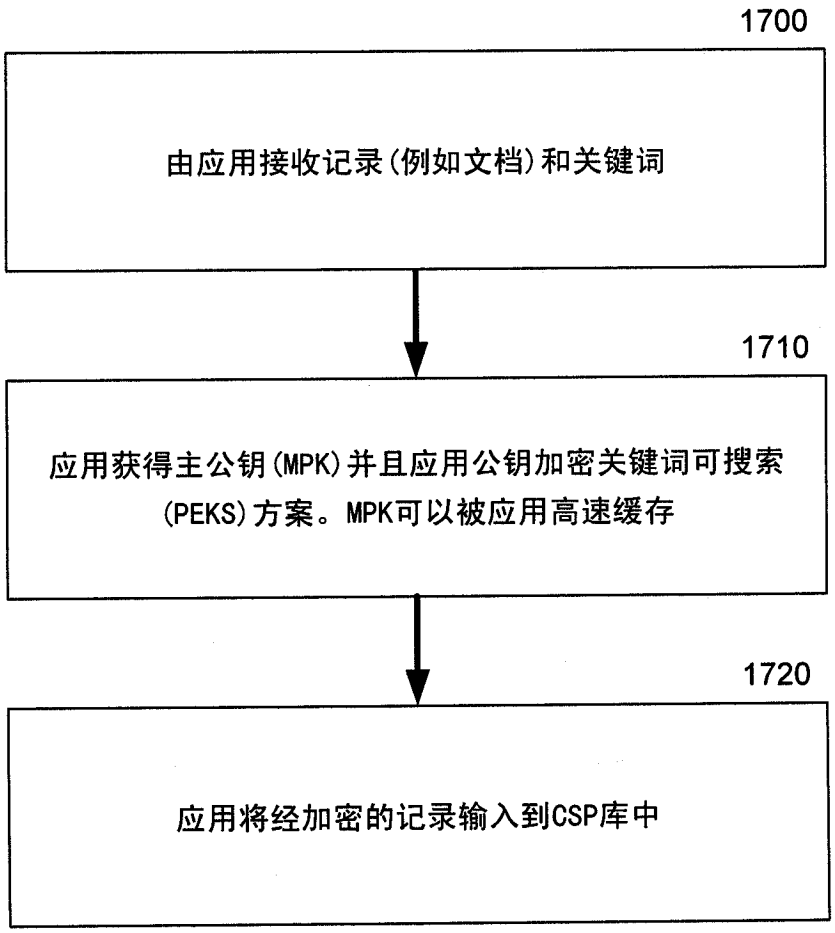

1700
由应用接收记录(例如文档)和关键词
1710
应用获得主公钥(MPK)并且应用公钥加密关键词可搜索(PEKS)方案。MPK可以被应用高速缓存
1720
应用将经加密的记录输入到CSP库中

图 17

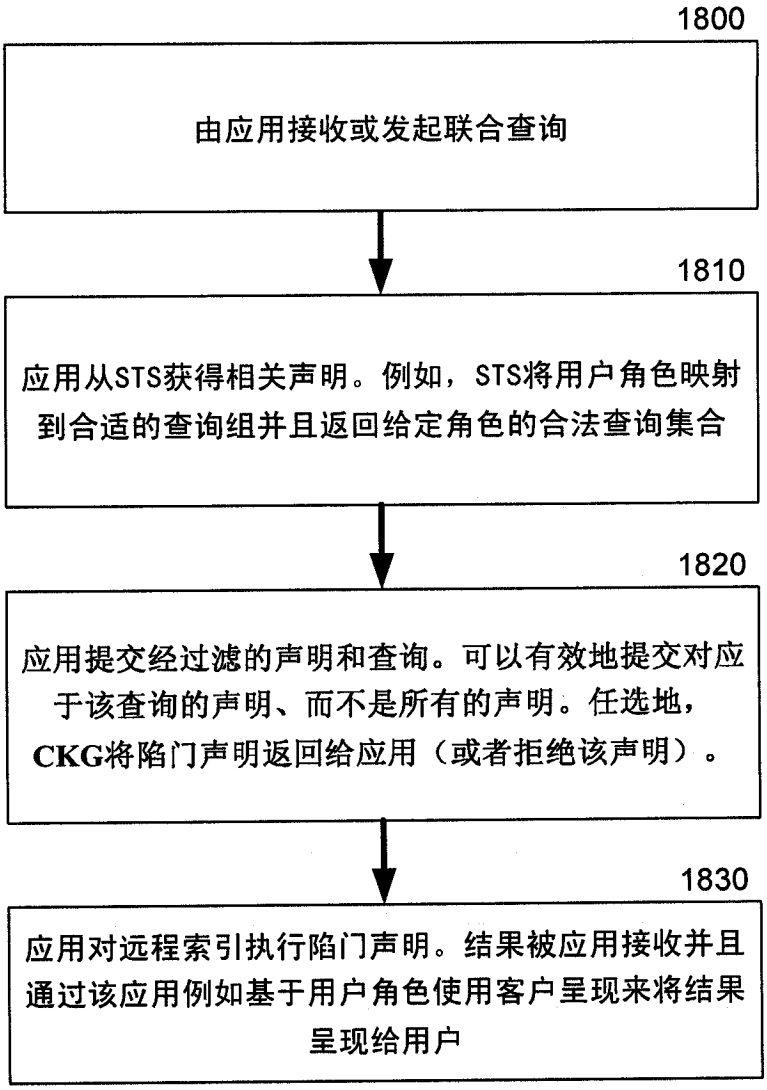

1800
由应用接收或发起联合查询
1810
应用从STS获得相关声明。例如，STS将用户角色映射到合适的查询组并且返回给定角色的合法查询集合
1820
应用提交经过滤的声明和查询。可以有效地提交对应于该查询的声明、而不是所有的声明。任选地，CKG将陷门声明返回给应用（或者拒绝该声明）。
1830
应用对远程索引执行陷门声明。结果被应用接收并且通过该应用例如基于用户角色使用客户呈现来将结果呈现给用户

图 18

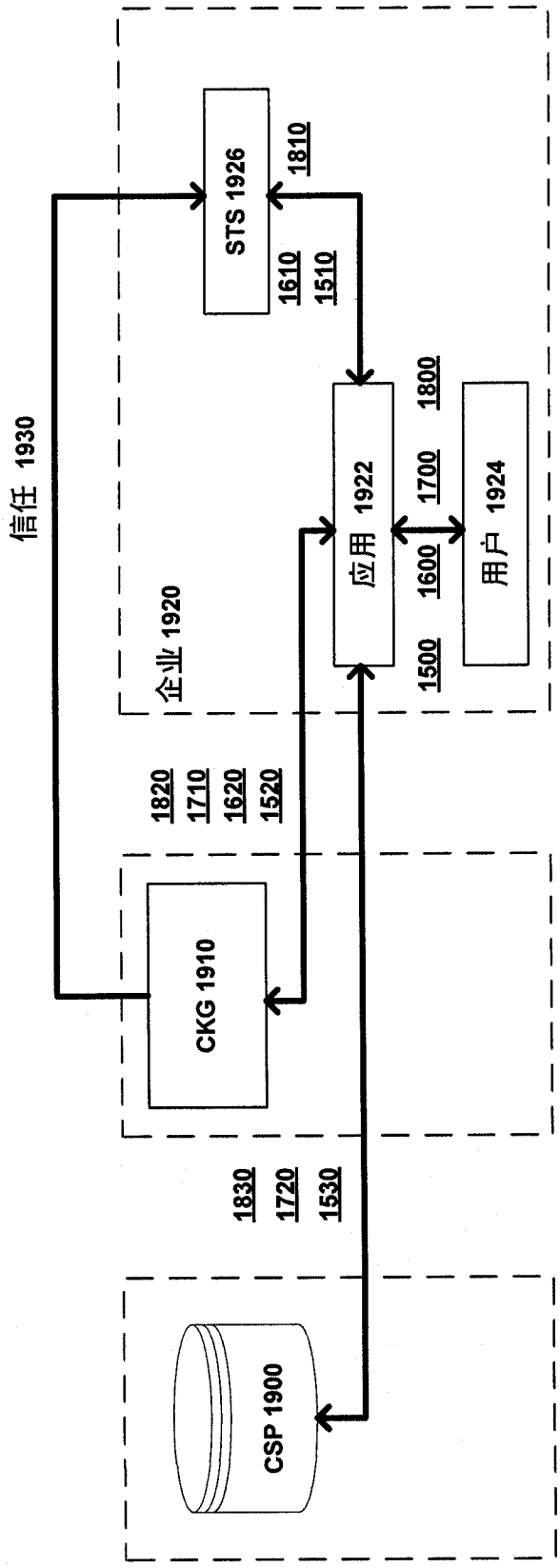

信任 1930
STS 1926
1810
1610
1510
企业 1920
应用 1922
1800
1700
1600
1500
用户 1924
1820
1710
1620
1520
CKG 1910
1830
1720
1530
CSP 1900

图 19

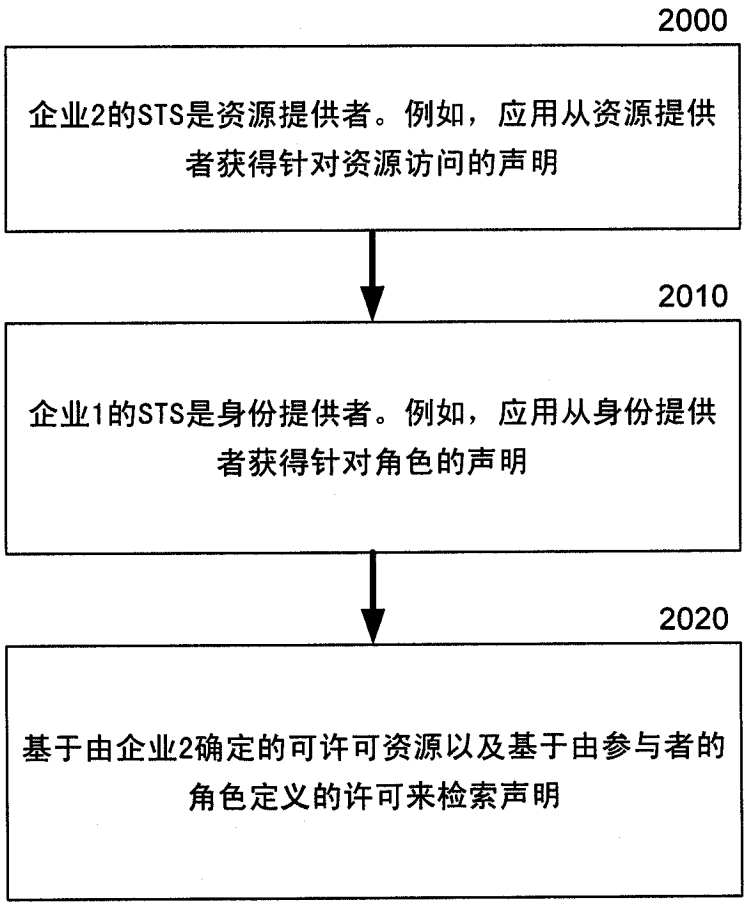

2000
企业2的STS是资源提供者。例如，应用从资源提供者获得针对资源访问的声明
2010
企业1的STS是身份提供者。例如，应用从身份提供者获得针对角色的声明
2020
基于由企业2确定的可许可资源以及基于由参与者的角色定义的许可来检索声明

图 20

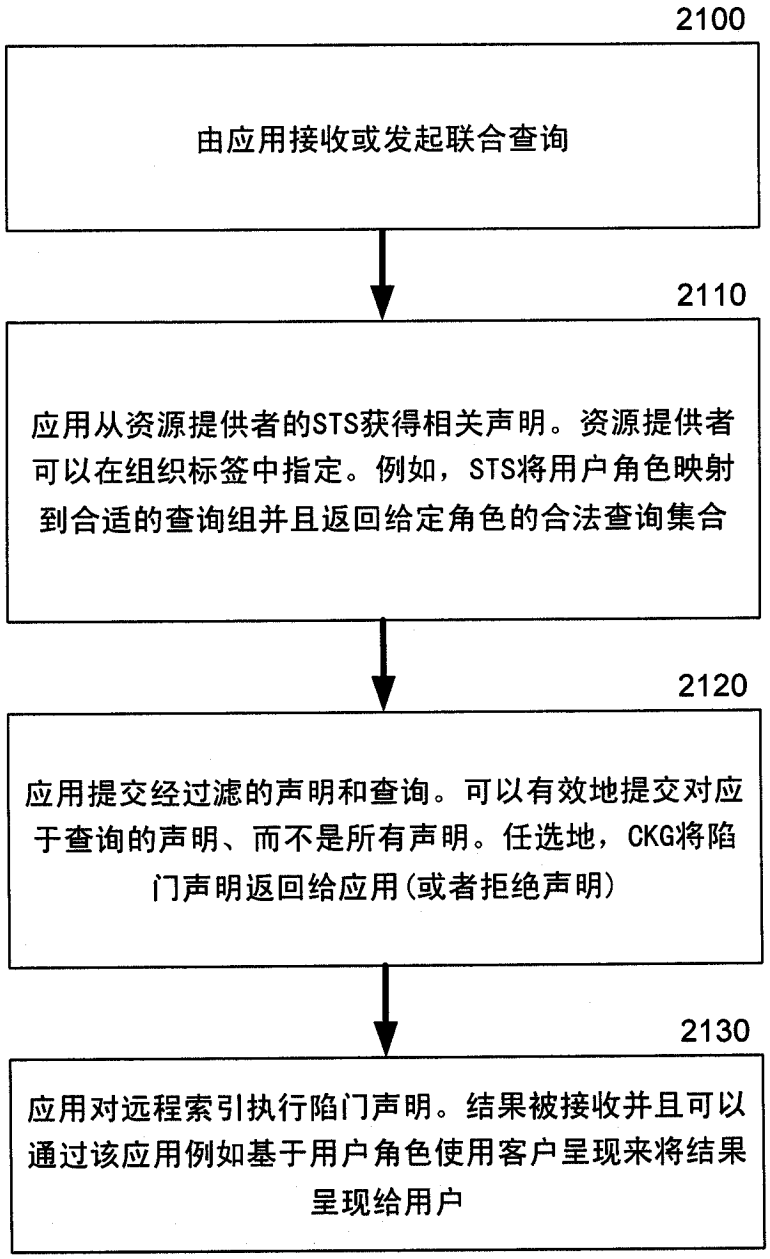

2100
由应用接收或发起联合查询
2110
应用从资源提供者的STS获得相关声明。资源提供者可以在组织标签中指定。例如，STS将用户角色映射到合适的查询组并且返回给定角色的合法查询集合
2120
应用提交经过滤的声明和查询。可以有效地提交对应于查询的声明、而不是所有声明。任选地，CKG将陷门声明返回给应用(或者拒绝声明)
2130
应用对远程索引执行陷门声明。结果被接收并且可以通过该应用例如基于用户角色使用客户呈现来将结果呈现给用户

图 21

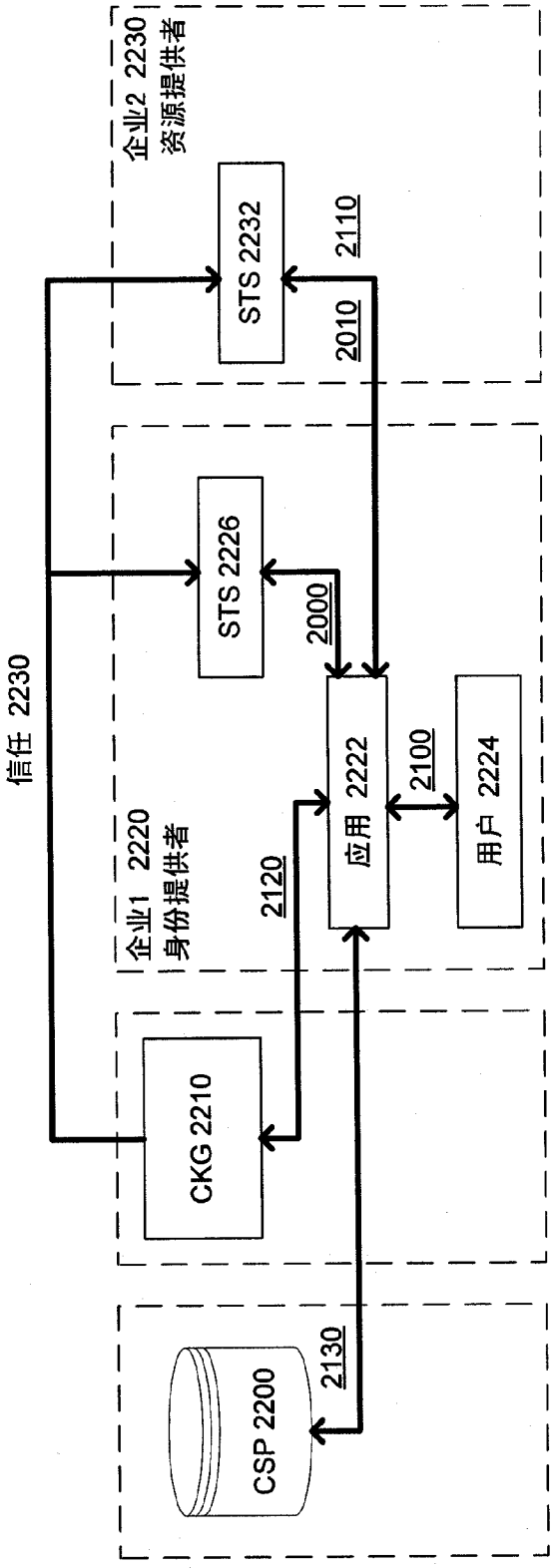

企业2 2230
资源提供者
STS 2232
2110
2010
STS 2226
2000
信任 2230
企业1 2220
身份提供者
应用 2222
2100
用户 2224
2120
CKG 2210
2130
CSP 2200

图 22

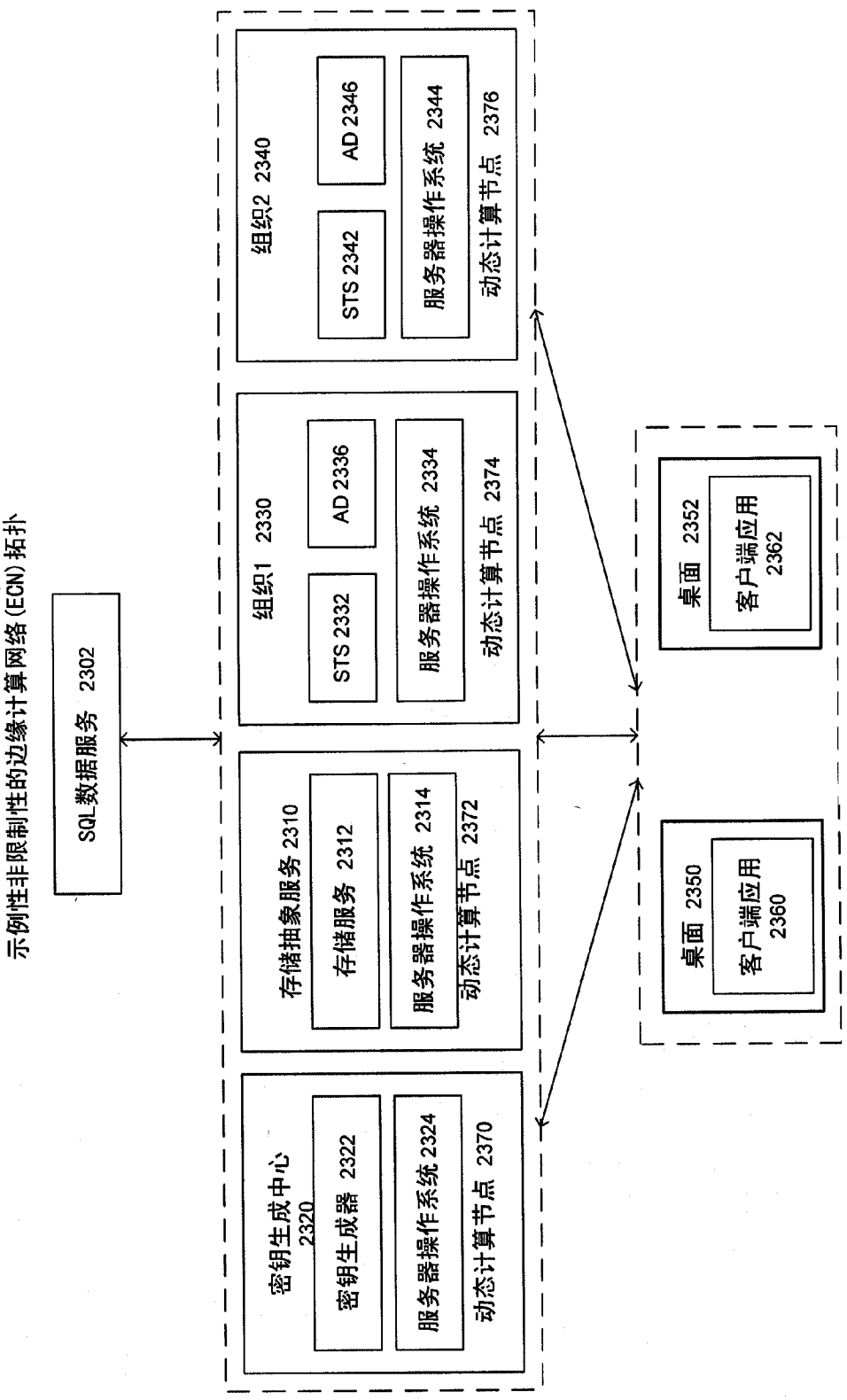

示例性非限制性的边缘计算网络(ECN)拓扑
SQL数据服务 2302
密钥生成中心 2320
密钥生成器 2322
服务器操作系统 2324
动态计算节点 2370
存储抽象服务 2310
存储服务 2312
服务器操作系统 2314
动态计算节点 2372
组织1 2330
STS 2332
AD 2336
服务器操作系统 2334
动态计算节点 2374
组织2 2340
STS 2342
AD 2346
服务器操作系统 2344
动态计算节点 2376
桌面 2350
客户端应用 2360
桌面 2352
客户端应用 2362

图 23

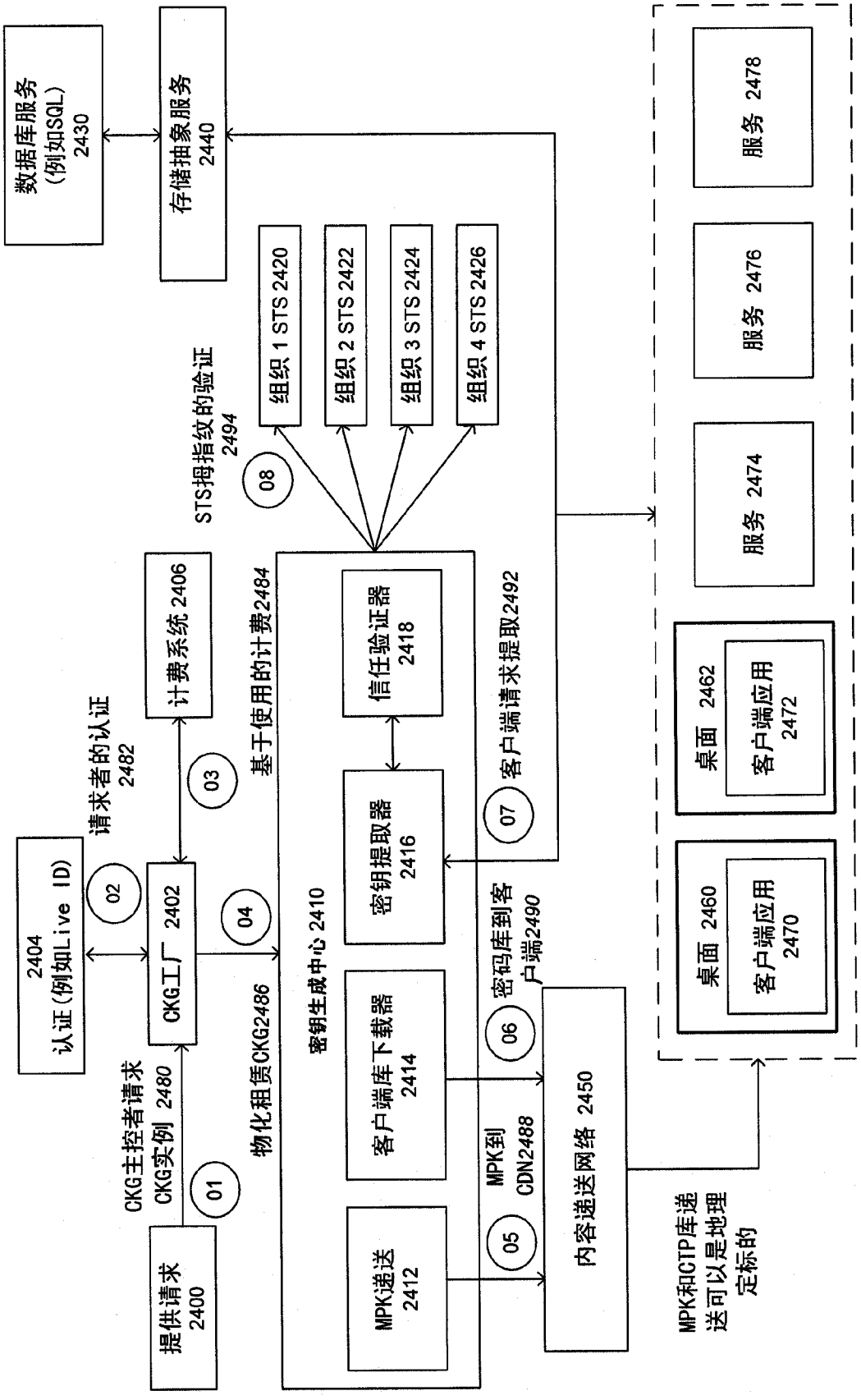

数据库服务
(例如SQL)
2430
存储抽象服务
2440
服务 2478
服务 2476
服务 2474
组织 1 STS 2420
组织 2 STS 2422
组织 3 STS 2424
组织 4 STS 2426
STS拇指纹的验证
2494
08
计费系统 2406
03
基于使用的计费2484
信任验证器
2418
密钥提取器
2416
07
客户端请求提取2492
桌面 2462
客户端应用
2472
桌面 2460
客户端应用
2470
请求者的认证
2482
02
2404
认证(例如Live ID)
CKG工厂 2402
04
密钥生成中心 2410
客户端库下载器
2414
06
密码库到客
户端2490
CKG主控者请求
CKG实例 2480
01
物化租赁CKG2486
MPK递送
2412
05
MPK到
CDN2488
内容递送网络 2450
提供请求
2400
MPK和CTP库递
送可以是地理
定标的

图 24

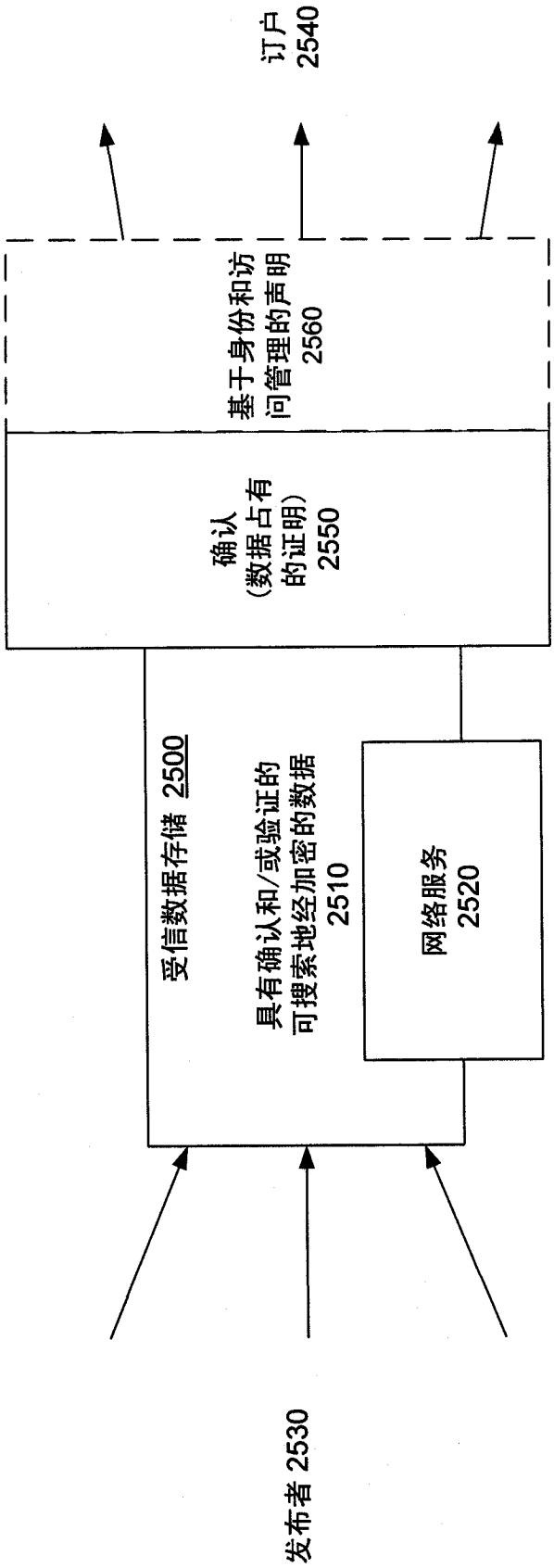

订户
2540
基于身份和访问管理的声明
2560
确认
(数据占有的证明)
2550
受信数据存储 2500
具有确认和/或验证的可搜索地经加密的数据
2510
网络服务
2520
发布者 2530

图 25

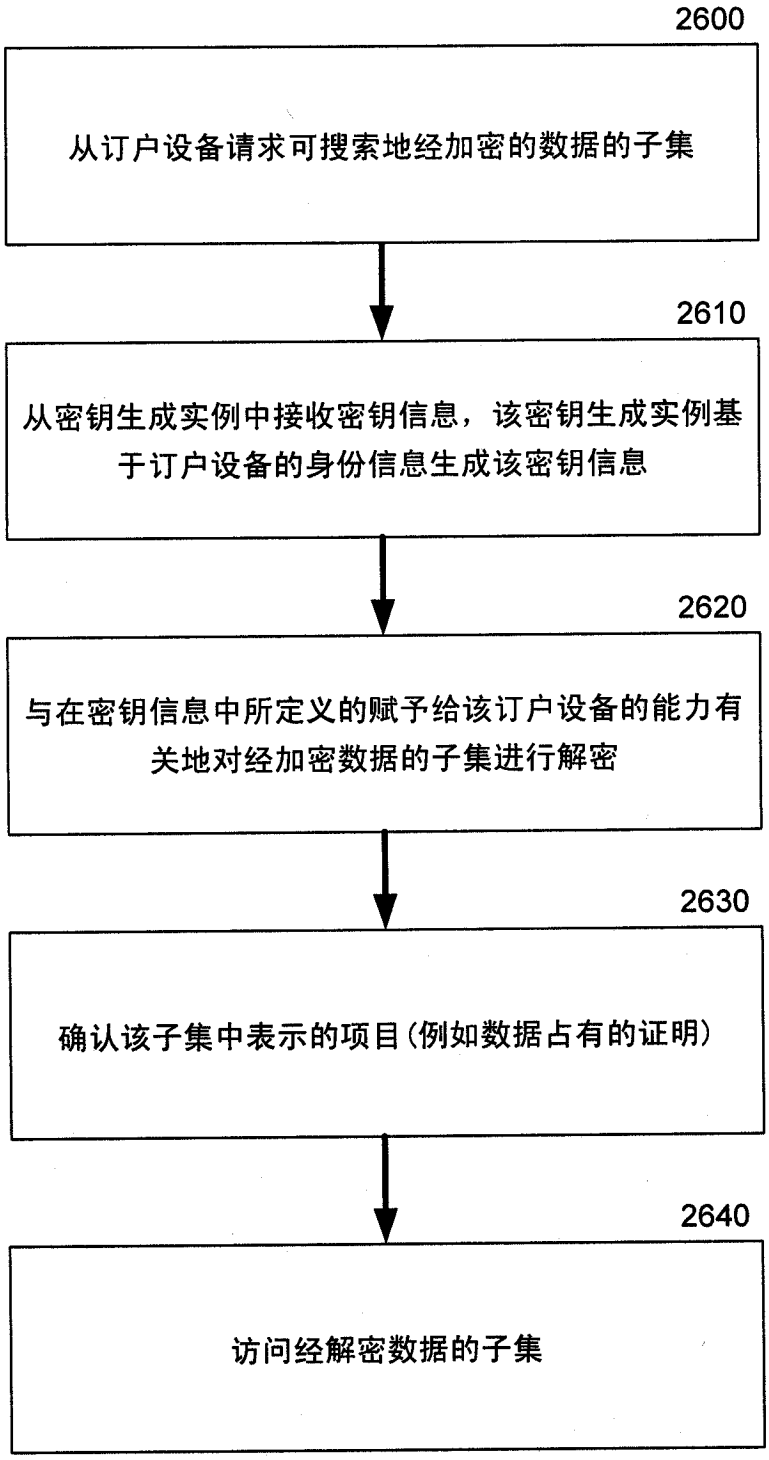

2600
从订户设备请求可搜索地经加密的数据的子集
2610
从密钥生成实例中接收密钥信息，该密钥生成实例基于订户设备的身份信息生成该密钥信息
2620
与在密钥信息中所定义的赋予给该订户设备的能力有关地对经加密数据的子集进行解密
2630
确认该子集中表示的项目(例如数据占有的证明)
2640
访问经解密数据的子集

图 26

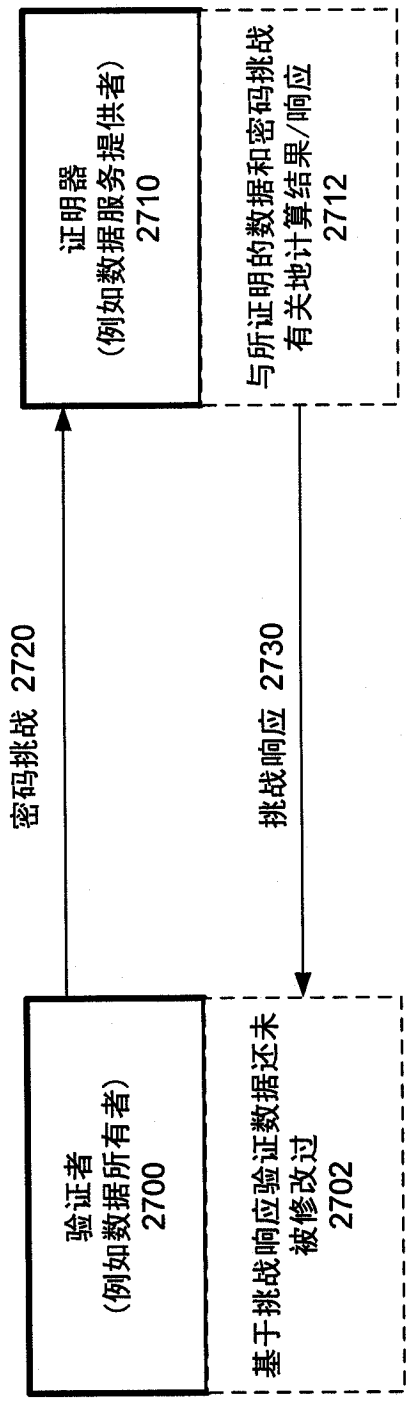

证明器
(例如数据服务提供者)
2710
与所证明的数据和密码挑战
有关地计算结果/响应
2712
密码挑战 2720
挑战响应 2730
验证者
(例如数据所有者)
2700
基于挑战响应验证数据还未
被修改过
2702

图 27

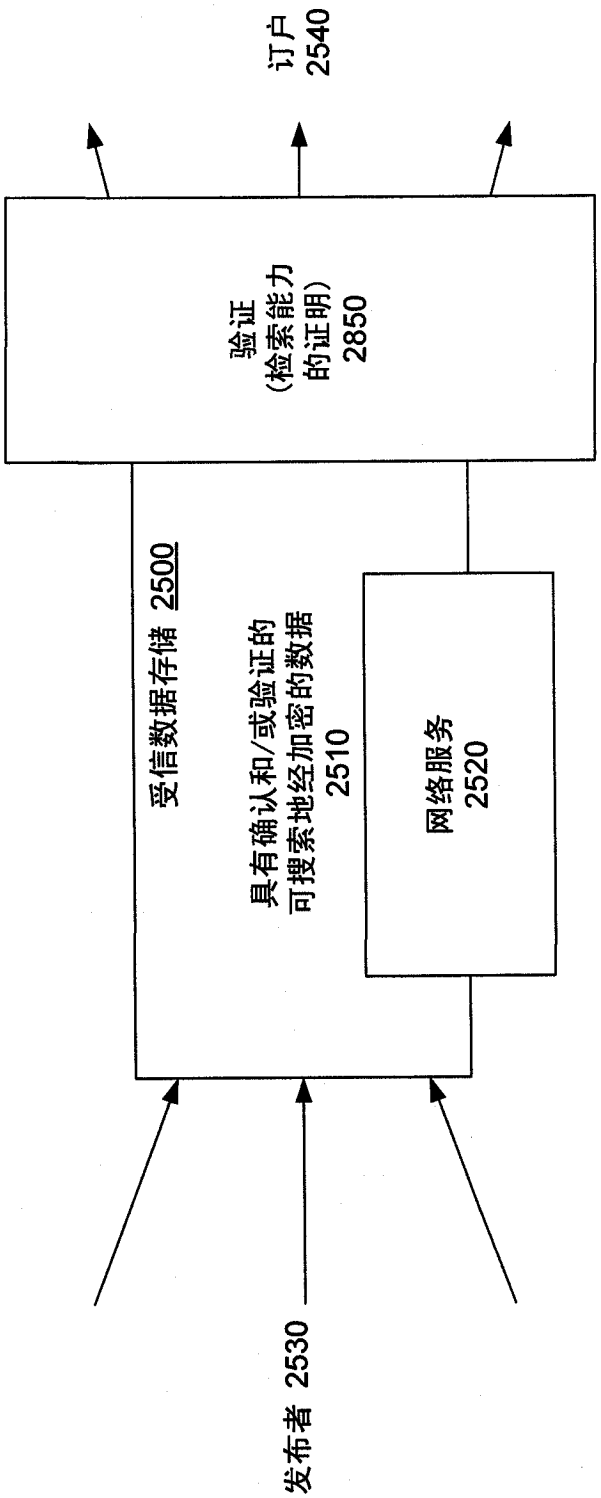

订户
2540
验证
(检索能力
的证明)
2850
受信数据存储 2500
具有确认和/或验证的
可搜索地经加密的数据
2510
网络服务
2520
发布者 2530

图 28

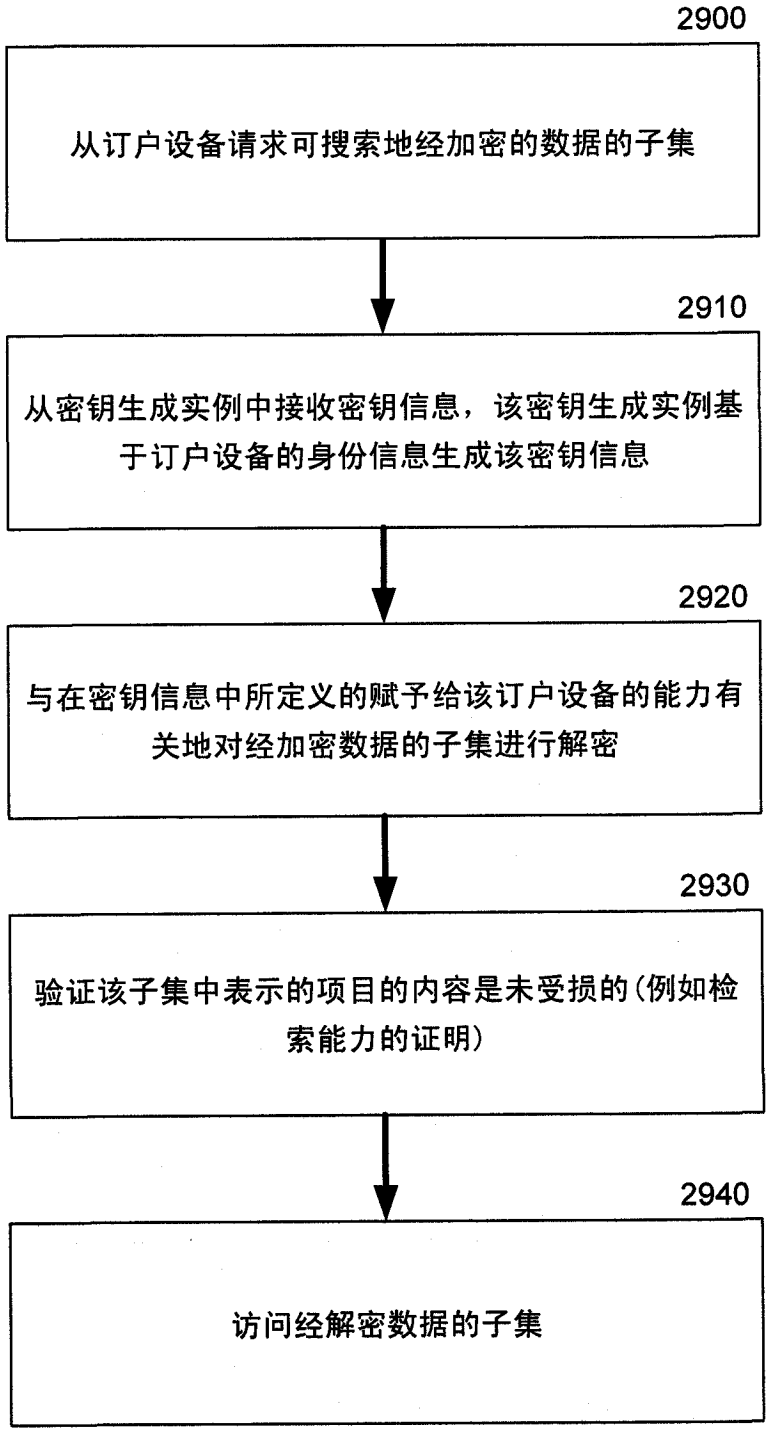

2900
从订户设备请求可搜索地经加密的数据的子集
2910
从密钥生成实例中接收密钥信息，该密钥生成实例基于订户设备的身份信息生成该密钥信息
2920
与在密钥信息中所定义的赋予给该订户设备的能力有关地对经加密数据的子集进行解密
2930
验证该子集中表示的项目的内容是未受损的(例如检索能力的证明)
2940
访问经解密数据的子集

图 29

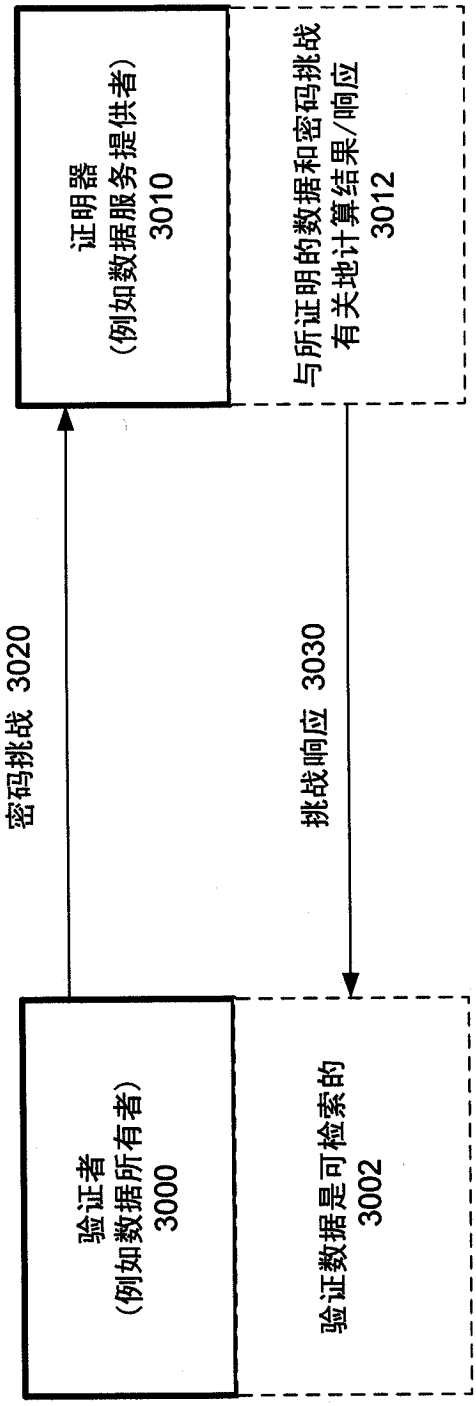

证明器
(例如数据服务提供者)
3010
与所证明的数据和密码挑战有关地计算结果/响应
3012
密码挑战 3020
挑战响应 3030
验证者
(例如数据所有者)
3000
验证数据是可检索的
3002

图 30

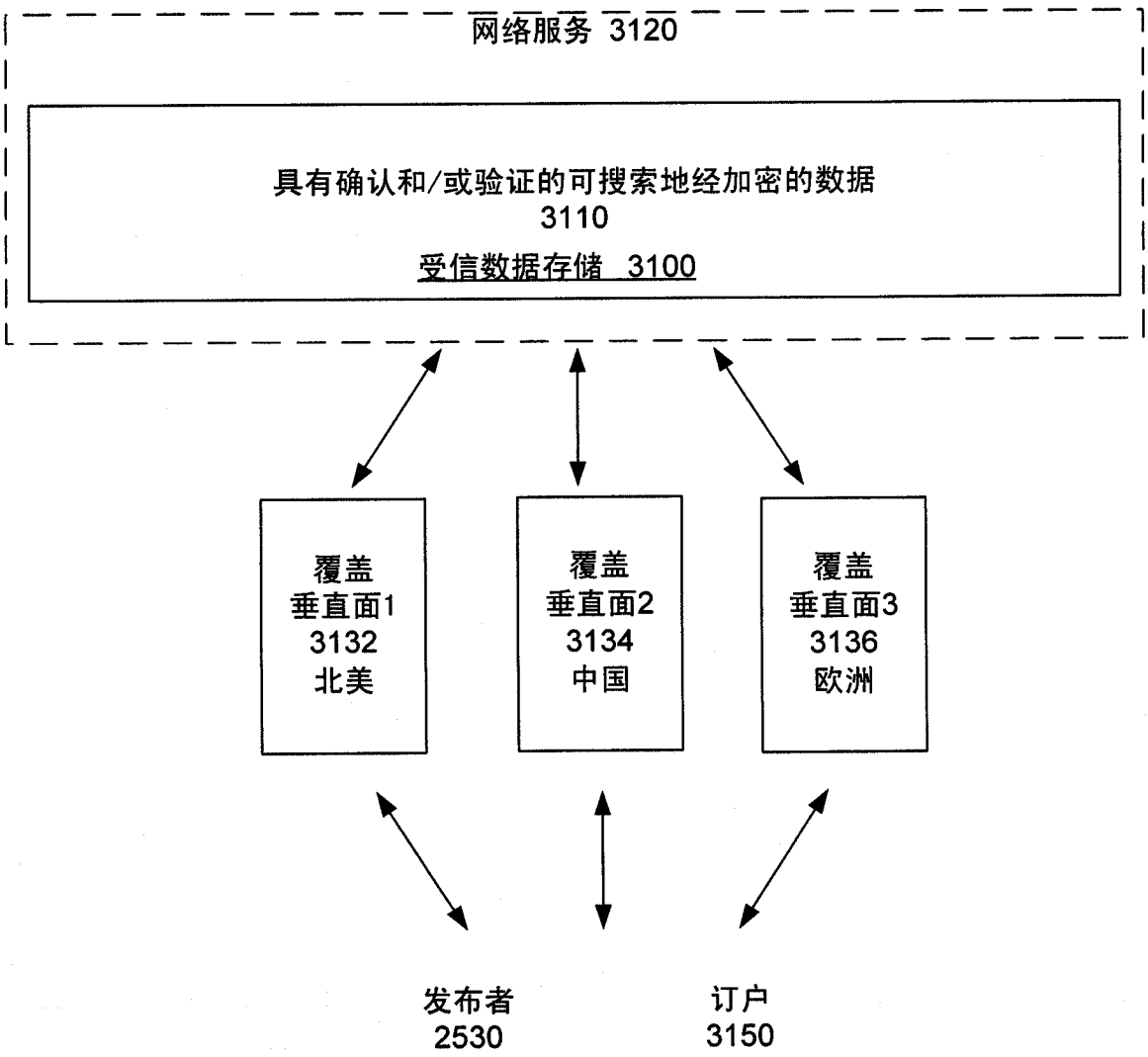

网络服务 3120
具有确认和/或验证的可搜索地经加密的数据
3110
受信数据存储 3100
覆盖
垂直面1
3132
北美
覆盖
垂直面2
3134
中国
覆盖
垂直面3
3136
欧洲
发布者
2530
订户
3150

图 31

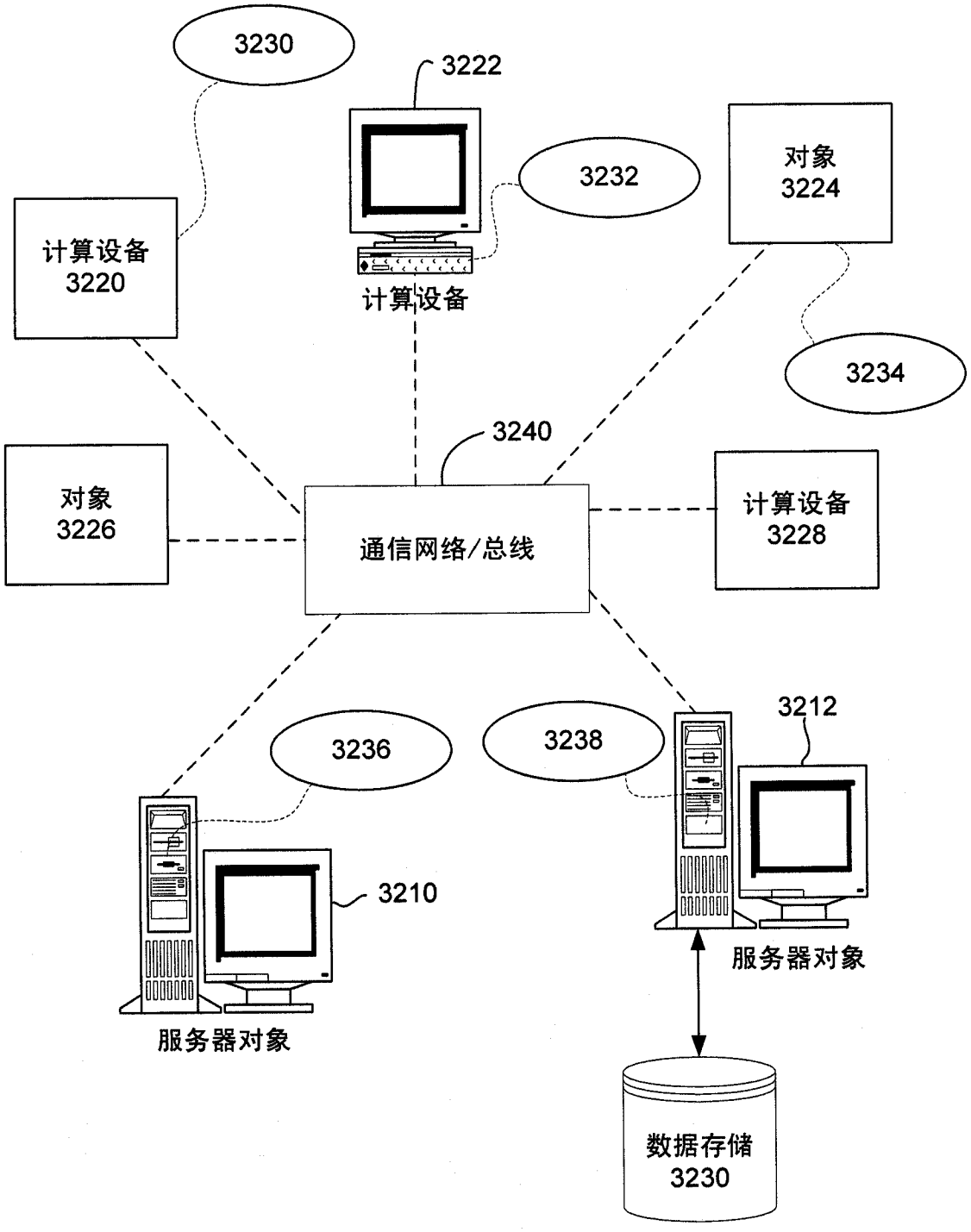

3230
3222
3232
对象
3224
计算设备
3220
计算设备
3234
3240
对象
3226
通信网络/总线
计算设备
3228
3212
3236
3238
3210
服务器对象
服务器对象
数据存储
3230

图 32

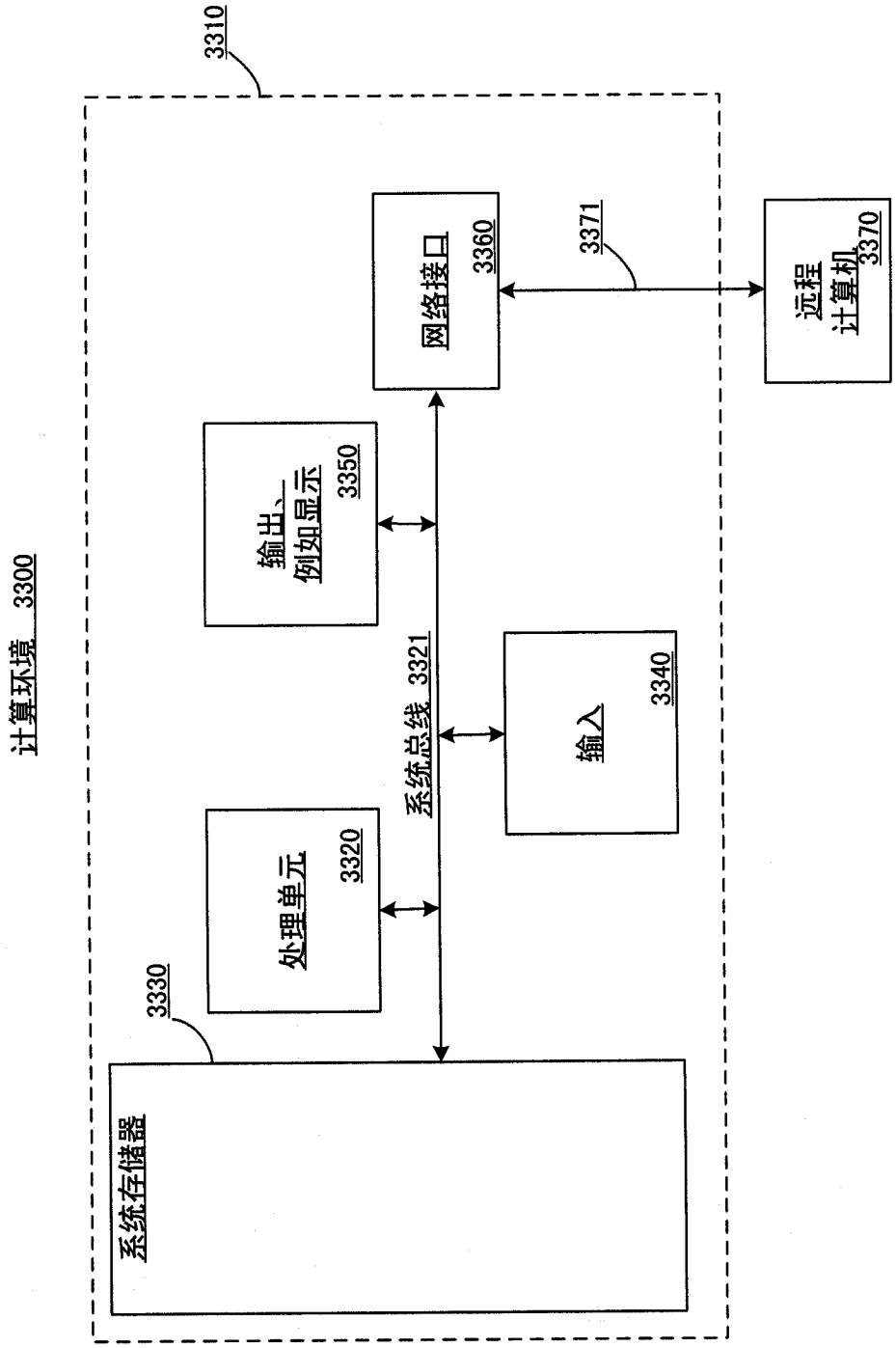

3310
计算环境 3300
网络接口
3360
3371
远程
计算机
3370
输出、
例如显示
3350
系统总线 3321
输入
3340
处理单元
3320
3330
系统存储器

图 33