(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 104620278 A
(43)申请公布日 2015.05.13

(21)申请号 201280075765.0

(22)申请日 2012.09.12

(85)PCT国际申请进入国家阶段日
2015.03.12

(86)PCT国际申请的申请数据
PCT/US2012/054942 2012.09.12

(87)PCT国际申请的公布数据
WO2014/042632 EN 2014.03.20

(71)申请人 英派尔科技开发有限公司
地址 美国特拉华州

(72)发明人 E·克鲁格里克

(74)专利代理机构 北京市铸成律师事务所 11313
代理人 孟锐

(51)Int.Cl.
G06Q 99/00(2006.01)

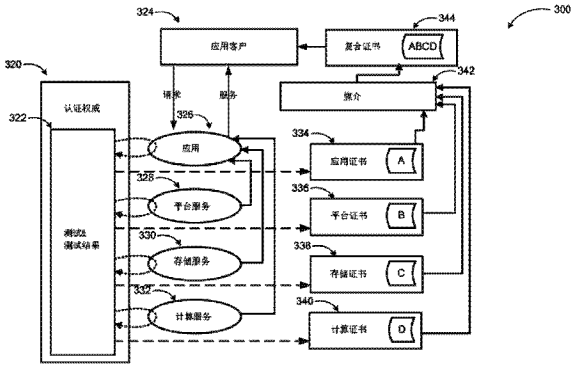
权利要求书5页 说明书13页 附图8页

(54)发明名称

用于保证而不显露基础结构的复合认证

(57)摘要

提供了经由证书媒介来提供复合证书的技术。在一些示例中，证书媒介可以生成复合证书，复合证书捕获了应用的通过认证的行为及其基础的子服务，而不显露提供给客户的子服务的标识。证书媒介可以从认证权威接收各种证书。在其他示例中，认证权威可以生成复合证书，或者认证媒介可以充当至少一部分子服务的认证权威。



CN 104620278 A

1. 一种采用复合认证用于保证的方法，所述方法包括：

在媒介认证服务处接收来自服务应用的用于认证的重定向请求；

从认证权威处请求与所述服务应用和所述服务应用的服务要素相关联的证书；

接收所述证书；

基于所述接收到的证书来构成复合证书，其中所述复合证书禁止所述服务要素的标识；以及

响应于所述重定向请求而提供所述复合证书。

2. 根据权利要求 1 所述的方法，还包括将所述复合证书构成为所述接收到的证书的逻辑组合。

3. 根据权利要求 1 所述的方法，其中所述接收到的证书建立每个服务要素对预先定义的规则、标准和 / 或惯例中的一项或多项的遵守。

4. 根据权利要求 3 所述的方法，还包括：如果两个或两个以上的服务要素按其相应的证书所定义的遵守级别不同，则在所述复合证书中指示最低共同遵守级别。

5. 根据权利要求 3 所述的方法，其中所述证书证明对支付卡行业 (PCI)、健康保险携带和责任法案 (HIPAA)、受控商业列表 (CCL)、ISO 认证或国际武器贸易条例 (ITAR) 中一项或多项的遵守。

6. 根据权利要求 1 所述的方法，还包括：从多个认证权威接收所述证书。

7. 根据权利要求 1 所述的方法，其中所述服务要素包括计算服务、存储服务、平台服务和交互服务中的一项或多项。

8. 根据权利要求 1 所述的方法，还包括：在所述媒介认证服务处，对至少一个所述服务要素执行测试和认证任务中的一项或多项。

9. 根据权利要求 1 所述的方法，还包括：通过选择是否调用所述媒介认证服务来使所述服务应用实现对通过认证的服务和未通过认证的服务定价。

10. 根据权利要求 1 所述的方法，还包括：

使所述服务要素实现提供令牌给所述服务应用；以及

从所述服务应用接收所述令牌以便传送给所述认证权威。

11. 一种采用复合认证用于保证的方法，所述方法包括：

从数据中心所托管的应用接收服务请求，其中所述请求包括认证请求；

将所述认证请求与所述服务请求分离；

从认证权威处请求与所述应用和所述应用的服务要素相关联的证书；

接收所述证书；

基于所述接收到的证书来构成复合证书，其中所述复合证书禁止所述服务要素的标识；以及

响应于所述服务请求而提供所述复合证书。

12. 根据权利要求 11 所述的方法，还包括：将所述复合证书构成为所述接收到的证书的逻辑组合。

13. 根据权利要求 11 所述的方法，还包括：

截取包括所述认证请求的所述服务请求；

将所述认证请求分离；以及

在托管所述应用的所述数据中心的网关或对话边界控制器中的一者处将所述认证请求转送给媒介认证服务。

14. 根据权利要求 11 所述的方法，其中所述应用具有基于服务的体系结构。

15. 根据权利要求 11 所述的方法，其中所述接收到的证书建立每个服务要素对预先定义的规则、标准和 / 或惯例中的一项或多项的遵守。

16. 根据权利要求 15 所述的方法，还包括 ：如果两个或多个服务要素按其相应的证书所定义的遵守级别不同，则在所述复合证书中指示最低共同遵守级别。

17. 根据权利要求 15 所述的方法，其中所述证书证明对支付卡行业 (PCI)、健康保险携带和责任法案 (HIPAA)、受控商业列表 (CCL)、或国际武器贸易条例 (ITAR) 中一项或多项的遵守。

18. 根据权利要求 11 所述的方法，其中所述服务要素包括计算服务、存储服务、平台服务和交互服务中的一项或多项。

19. 根据权利要求 11 所述的方法，还包括 ：从多个认证权威接收所述证书。

20. 根据权利要求 11 所述的方法，还包括 ：通过选择是否调用所述复合证书来使所述应用实现对通过认证的服务和未通过认证的服务定价。

21. 根据权利要求 11 所述的方法，还包括 ：

使所述服务要素实现提供令牌给所述应用 ；以及

从所述应用接收所述令牌以传送给所述认证权威。

22. 一种配置为采用复合认证用于保证的媒介认证服务，所述媒介认证服务包括 ：

一个或多个通信模块，其配置为与数据中心所托管的服务应用和认证权威通信 ；以及

服务器，其配置为 ：

从服务应用处接收用于认证的重定向请求 ；

从认证权威处请求与所述服务应用和所述服务应用的服务要素相关联的证书 ；

接收所述证书 ；

基于所述接收到的证书来构成复合证书，其中所述复合证书禁止所述服务要素的标识 ；以及

响应于所述重定向请求而提供所述复合证书。

23. 根据权利要求 22 所述的媒介认证服务，其中所述服务器还配置为将所述复合证书构成为所述接收到的证书的逻辑组合。

24. 根据权利要求 22 所述的媒介认证服务，其中所述接收到的证书建立每个服务要素对预先定义的规则、标准和 / 或惯例中的一项或多项的遵守。

25. 根据权利要求 24 所述的媒介认证服务，其中所述服务器还配置为 ：如果两个或多个服务要素按其相应的证书所定义的遵守级别不同，则在所述复合证书中指示最低共同遵守级别。

26. 根据权利要求 24 所述的媒介认证服务，其中所述证书证明对支付卡行业 (PCI)、健康保险携带和责任法案 (HIPAA)、受控商业列表 (CCL)、或国际武器贸易条例 (ITAR) 中一项或多项的遵守。

27. 根据权利要求 22 所述的媒介认证服务，其中所述服务器还配置为从多个认证权威接收所述证书。

28. 根据权利要求 22 所述的媒介认证服务，其中所述服务要素包括计算服务、存储服务、平台服务和交互服务中的一项或多项。

29. 根据权利要求 22 所述的媒介认证服务，其中所述媒介认证服务还配置为对至少一个所述服务要素执行测试和认证任务中的一种或多种。

30. 根据权利要求 22 所述的媒介认证服务，其中所述服务器还配置为：通过选择是否调用所述媒介认证服务，使所述服务应用实现对通过认证的服务和未通过认证的服务定价。

31. 根据权利要求 22 所述的媒介认证服务，其中所述服务器还配置为：

使所述服务要素实现提供令牌给所述服务应用；以及

从所述服务应用接收所述令牌以传送给所述认证权威。

32. 一种配置为采用复合认证用于保证的基于云的数据中心，所述数据中心包括：

多个虚拟机，其可操作以便在一个或多个物理机上执行，其中至少一个所述虚拟机托管服务应用，所述服务应用配置为将组合服务提供给客户；以及

数据中心控制器，其配置为：

从所述数据中心托管的所述服务应用接收服务请求，其中所述请求包括认证请求；

将所述认证请求从所述服务请求分离；以及

将所述认证请求转送给媒介认证服务，使得响应于所述服务请求而通过所述媒介认证服务来提供复合证书，所述复合证书包括用于子服务的各个证书，并且禁止服务要素的标识。

33. 根据权利要求 32 所述的数据中心，其中所述媒介认证服务还配置为将所述复合证书构成为所述接收到的证书的逻辑组合。

34. 根据权利要求 32 所述的数据中心，其中所述数据中心控制器是与所述服务应用接口的网关或对话边界控制器中的一个。

35. 根据权利要求 32 所述的数据中心，其中所述媒介认证服务由所述数据中心提供。

36. 根据权利要求 32 所述的数据中心，其中所述证书建立每个服务要素对预先定义的规则、标准和 / 或惯例中的一项或多项的遵守。

37. 根据权利要求 36 所述的数据中心，其中所述媒介认证服务还配置为：如果两个或多个服务要素按其相应的证书所定义的遵守级别不同，则在所述复合证书中指示最低共同遵守级别。

38. 根据权利要求 36 所述的数据中心，其中所述证书证明对支付卡行业 (PCI)、健康保险携带和责任法案 (HIPAA)、受控商业列表 (CCL)、或国际武器贸易条例 (ITAR) 中一项或多项的遵守。

39. 根据权利要求 32 所述的数据中心，其中所述服务要素包括计算服务、存储服务、平台服务和交互服务中的一项或多项。

40. 根据权利要求 32 所述的数据中心，其中所述媒介认证服务还配置为从多个认证权威接收所述证书。

41. 根据权利要求 32 所述的数据中心，其中通过选择是否调用所述复合证书，使所述服务应用实现对通过认证的服务和未通过认证的服务定价。

42. 根据权利要求 32 所述的数据中心，其中所述数据中心控制器还配置为：

使所述服务要素实现提供令牌；以及

将所述令牌提供给所述媒介认证服务。

43. 一种计算机可读存储介质，其中存储有采用复合认证用来保证的指令，所述指令包括：

在媒介认证服务处接收来自服务应用的对于认证的重定向请求；

从认证权威处请求与所述服务应用和所述服务应用的服务要素相关联的证书；

接收所述证书；

基于所述接收到的证书来构成复合证书，其中所述复合证书禁止所述服务要素的标识；以及

响应于所述重定向请求而提供所述复合证书。

44. 根据权利要求 43 所述的计算机可读存储介质，其中所述指令还包括：

将所述复合证书构成为所述接收到的证书的逻辑组合。

45. 根据权利要求 43 所述的计算机可读存储介质，其中所述接收到的证书建立每个服务要素对预先定义的规则、标准和 / 或惯例中的一项或多项的遵守。

46. 根据权利要求 45 所述的计算机可读存储介质，其中所述指令还包括：

如果两个或多个服务要素按其相应的证书所定义的遵守级别不同，则在所述复合证书中指示最低共同遵守级别。

47. 根据权利要求 45 所述的计算机可读存储介质，其中所述证书证明对支付卡行业 (PCI)、健康保险携带和责任法案 (HIPAA)、受控商业列表 (CCL)、或国际武器贸易条例 (ITAR) 中一项或多项的遵守。

48. 根据权利要求 43 所述的计算机可读存储介质，其中所述指令还包括：

从多个认证权威接收所述证书。

49. 根据权利要求 43 所述的计算机可读存储介质，其中所述服务要素包括计算服务、存储服务、平台服务和交互服务中的一项或多项。

50. 根据权利要求 43 所述的计算机可读存储介质，其中所述指令还包括：

在所述媒介认证服务处，对至少一个所述服务要素执行测试和认证任务中的一种或多种。

51. 根据权利要求 43 所述的计算机可读存储介质，其中所述指令还包括：

通过选择是否调用所述媒介认证服务，使所述服务应用实现对通过认证的服务和未通过认证的服务定价。

52. 根据权利要求 43 所述的计算机可读存储介质，其中所述指令还包括：

使所述服务要素实现提供令牌给所述服务应用；以及

从所述服务应用接收所述令牌以传送给所述认证权威。

53. 一种计算机可读存储介质，其中存储有采用复合认证用于保证的指令，所述指令包括：

从数据中心托管的应用接收服务请求，其中所述请求包括认证请求；

将所述认证请求与所述服务请求分离；

从认证权威处请求与所述应用和所述应用的服务要素相关联的证书；

接收所述证书；

基于所述接收到的证书来构成复合证书，其中所述复合证书禁止所述服务要素的标识；以及

响应于所述服务请求而提供所述复合证书。

54. 根据权利要求 53 所述的计算机可读存储介质，其中所述指令还包括：

将所述复合证书构成为所述接收到的证书的逻辑组合。

55. 根据权利要求 53 所述的计算机可读存储介质，其中所述指令还包括：

截取包括所述认证请求的所述服务请求；

将所述认证请求分离；以及

在托管所述应用的所述数据中心的网关或对话边界控制器中的一者处将所述认证请求转送给媒介认证服务。

56. 根据权利要求 53 所述的计算机可读存储介质，其中所述应用具有基于服务的体系结构。

57. 根据权利要求 53 所述的计算机可读存储介质，其中所述接收到的证书建立每个服务要素对预先定义的规则、标准和 / 或惯例中的一项或多项的遵守。

58. 根据权利要求 57 所述的计算机可读存储介质，其中所述指令还包括：

如果两个以上服务要素按其相应的证书所定义的遵守级别不同，则在所述复合证书中指示最低共同遵守级别。

59. 根据权利要求 57 所述的计算机可读存储介质，其中所述证书证明对支付卡行业 (PCI)、健康保险携带和责任法案 (HIPAA)、受控商业列表 (CCL)、或国际武器贸易条例 (ITAR) 中一项或多项的遵守。

60. 根据权利要求 53 所述的计算机可读存储介质，其中所述服务要素包括计算服务、存储服务、平台服务和交互服务中的一项或多项。

61. 根据权利要求 53 所述的计算机可读存储介质，其中所述指令还包括：

从多个认证权威接收所述证书。

62. 根据权利要求 53 所述的计算机可读存储介质，其中所述指令还包括：

通过选择是否调用所述复合证书，使所述应用实现对通过认证的服务和未通过认证的服务定价。

63. 根据权利要求 53 所述的计算机可读存储介质，其中所述指令还包括：

使所述服务要素实现提供令牌给所述应用；以及

从所述应用接收所述令牌以传送给所述认证权威。

用于保证而不显露基础结构的复合认证

背景技术

[0001] 除非在此处进行说明，否则此处所描述的材料不是本申请权利要求的现有技术并且不因包含在该部分中而承认是现有技术。

[0002] 随着基于云的计算变得更加普遍，云服务会变得更加廉价且更加通用。在一些情况下，基于云的服务应用可构建于其他云服务或平台之上。这些基于服务的云体系结构可以提供用于快速构建强大数据中心应用的灵活的工具。连同云服务的认证一起，基于服务的体系结构可允许在保持期望标准的同时实现复杂目标的商业处理服务的自动发现和构建。云服务认证可以利用证书来建立各服务要素对各自规则、标准和惯例的遵守。通常，可以通过将支持上级应用的较低级子服务的证书暴露于应用客户来确认这些证书。例如，如果特定的存储服务是应用的基础，则可以将用于该特定存储服务的特定证书显露给客户。这意味着，使用服务的任何人都可以得知用来构建上级服务的所有子服务。

[0003] 发明概述

[0004] 本公开一般描述了在基于数据中心的服务环境中采用复合认证来进行保证而不显露基础结构的技术。

[0005] 根据一些示例性的实施例，采用复合认证用于保证的方法可以包括：在媒介认证服务处接收来自服务应用的用于认证的重定向请求；从认证权威处请求与服务应用和服务应用的服务要素相关联的证书；接收证书；基于接收到的证书构成复合证书，其中复合证书禁止服务要素的标识；以及响应于重定向请求而提供复合证书。

[0006] 根据其他的示例性实施例，采用复合证书用于保证的方法可以包括：从数据中心托管的应用接收服务请求，其中所述请求包括认证请求；将认证请求与服务请求分离；从认证权威处请求与应用和应用的服务要素相关联的证书；接收证书；基于接收到的证书构成复合证书，其中复合证书禁止服务要素的标识；以及响应于服务请求而提供复合证书。

[0007] 根据另外的示例性实施例，配置为采用复合认证用于保证的媒介认证服务可以包括：通信模块，其配置为与数据中心和认证权威所托管的服务应用通信；以及服务器。该服务器可配置为：从服务应用接收用于认证的重定向请求；从认证权威处请求与服务应用和服务应用的服务要素相关联的证书；接收证书；基于接收到的证书构成复合证书，其中复合证书禁止服务要素的标识；以及响应于重定向请求而提供复合证书。

[0008] 根据另外的示例性实施例，配置为采用复合认证用于保证的基于云的数据中心可以包括：多个虚拟机，其可操作以在一个或多个物理机上执行，其中至少一个虚拟机托管配置为向客户提供组合服务的服务应用。数据中心还可以包括数据中心控制器，其配置为：从数据中心所托管的服务应用接收服务请求，其中该请求包括认证请求；将认证请求与服务请求分离；以及将认证请求转送给媒介认证服务，使得响应于服务请求而通过媒介认证服务来提供禁止服务要素的标识的由用于子服务的各证书构成的复合证书。

[0009] 根据一些示例性的实施例，计算机可读存储介质可以存储采用复合证书用于保证的指令。所述指令可以包括：在媒介认证服务处接收来自服务应用的用于认证的重定向请求；从认证权威处请求与服务应用和服务应用的服务要素相关联的证书；接收证书；基于

接收到的证书来构成复合证书，其中复合证书禁止服务要素的标识；以及响应于重定向请求而提供复合证书。

[0010] 根据其他的示例性实施例，计算机可读存储介质可以存储采用复合认证用于保证的指令。所述指令可以包括：从数据中心托管的应用接收服务请求，其中所述请求包括认证请求；将认证请求与服务请求分离；从认证权威处请求与应用和应用的服务要素相关联的证书；接收证书；基于接收到的证书构成复合证书，其中复合证书禁止服务要素的标识；以及响应于服务请求而提供复合证书。

[0011] 前面的概述仅仅是示例性的，而不意在以任何方式进行限制。通过参考附图以及下面的详细说明，除了上文所描述的示例性的方案、实施例和特征之外，另外的方案、实施例和特征将变得清晰可见。

附图说明

[0012] 通过下面结合附图给出的详细说明和随附的权利要求，本公开的前述特征以及其它特征将变得更加清晰。应理解的是，这些附图仅描绘了依照本公开的多个实施例，因此，不应视为对本发明范围的限制，将通过利用附图结合附加的具体描述和细节对本公开进行说明，在附图中：

[0013] 图 1 示出了复合认证可用于保证而不显露基础结构的示例的基于数据中心的系统；

[0014] 图 2 示出了示例的系统，其中的应用提供组合服务及其子服务各自向该应用的客户提供单独的证书；

[0015] 图 3 示出了示例的系统，其中通过使用复合证书能够使提供组合服务的应用避免暴露其子服务；

[0016] 图 4A 示出了示例的系统，其中独立的媒介服务管理复合证书；

[0017] 图 4B 示出了示例的系统，其中托管该应用的数据中心管理复合证书；

[0018] 图 5 示出了通用计算设备，其可用于管理用于保证的复合认证而不显露基础结构；

[0019] 图 6 是示出可以通过诸如图 5 中的设备的计算设备执行的示例方法的流程图；以及

[0020] 图 7 示出了示例的计算机程序产品的框图；

[0021] 所有都是依照本文所描述的至少一些实施例来布置的。

[0022] 发明详述

[0023] 在下面的详细说明中，将参考附图，附图构成了详细说明的一部分。在附图中，除非上下文指出，否则相似的符号通常表示相似的部件。在详细说明、附图和权利要求中所描述的示例性实施例不意在限制。可以使用其它实施例，并且可以做出其它改变，而不偏离本文呈现的主题的精神或范围。将易于理解的是，如本文大致描述且如图中所图示的，本公开的方案能够以各种不同配置来布置、替代、组合、分离和设计，所有这些都在本文中明确地构思出。

[0024] 本公开一般尤其涉及与采用复合认证用于保证而不显露基础结构有关方法、装置、系统、设备和 / 或计算机程序产品。

[0025] 简言之，提出了经由证书媒介来提供复合证书的技术。在一些示例中，证书媒介可以生成复合证书，复合证书捕获应用的通过认证的行为及其基础子服务，而不显露用于提供给客户的子服务的标识。证书媒介可以从认证权威接收各证书。在其他示例中，认证权威可以生成复合证书，或者证书媒介可以充当至少一部分子服务的认证权威。

[0026] 图 1 示出了依照本文所描述的至少一些实施例布置的复合认证可用于保证而不显露基础结构的示例的基于数据中心的系统。

[0027] 如图 100 所示，物理数据中心 102 可以包括一个或多个物理服务器 110、111 和 113，多个物理服务器中的每一个可配置为提供一个或多个虚拟机 104。例如，物理服务器 111 和 113 可以配置为分别提供四个虚拟机和两个虚拟机。在一些实施例中，一个或多个虚拟机可以组合到一个或多个虚拟数据中心中。例如，服务器 111 提供的四个虚拟机可以组合到虚拟数据中心 112 中。虚拟机 104 和 / 或虚拟数据中心 112 可配置为经由云 106 向诸如个体用户或企业客户的一组客户 108 提供诸如各种应用、数据存储、数据处理或类似服务的云相关数据 / 计算服务。

[0028] 在一些示例中，一个或多个客户 108 可以经由组合了诸如存储、计算等各种子服务的数据中心向其客户端提供组合服务。客户 108 的客户端可以对来自客户 108 的服务请求认证。这种认证可以由第三方认证权威来提供。认证权威是发布数字证书的实体。数字证书可以通过证书的被指明主体来证明公共密钥的所有权。这允许其他人（依赖方）依赖于通过对应于经认证的公共密钥的私有密钥所做出的签名或断言，在这种信任关系的模型中。因此，认证权威是证书的主体（所有者）和依赖于证书的一方两者都信任的可信第三方。认证权威特点在于许多公共密钥基础结构 (PKI) 方案。VeriSign、Comodo 和 DigiNotar 是一些示例的商业基础认证权威。大量的其他公司为例如其自己的软件提供证书。在一些情况下，在客户端信任的情况下数据中心操作者可以是认证权威，并且在被信任的情况下客户 108 甚至可以是“自签名”认证权威。例如，如果公司 X 为雇员或子公司提供服务，则该公司还可以充当认证权威。在常规环境下，第三方认证权威可以认证组合服务以及单个的子服务，从而向请求客户端标识子服务。在根据实施例的系统中，对于认证单个的子服务而没有向客户端标识它们的组合服务，可以生成复合证书。

[0029] 图 2 示出了依照本文所描述的至少一些实施例布置的提供组合服务及其子服务的应用各自向应用的客户提供单独的证书的示例的系统。

[0030] 如图 200 所示，应用客户 224 可以请求并接收来自应用 226 的服务。应用 226 可以操作于平台服务 228（例如，提供硬件体系结构和 / 或软件架构以及其他以便运行应用的基于云的服务）之上。应用 226 还可以由存储服务 230（即，提供数据存储的服务，通常是基于云的服务）、计算服务 232（即，提供处理 / 计算能力的服务，通常是基于云的服务）、和 / 或任何其他服务支持。认证权威 220 可配置为对应用 226、平台服务 228、存储服务 230 和 / 或计算服务 232 执行测试且获得测试结果 222。对应用 226 或子服务的测试可以包括测试应用处置各种数据量的容量、在繁忙条件下（例如，大量的客户端请求）的响应性、响应速度等。测试结果 222 可以与应用 / 服务是否遵守特定的规则、标准和 / 或惯例有关。

[0031] 基于测试结果 222、商业处理文档、审查或其他评估，认证权威 220 可以向应用和 / 或其子服务发布证书，其中每个证书可以证明关联的实体拥有某些属性或者满足某些条件。条件可以基于行业标准或客户端要求。例如，存储容量、数据传输速度、处理容量、安全

级别等可以被定义为客户端请求条件。诸如数据处理容量、安全性等应用和/或子服务特征可视为针对该条件进行认证的特性。在示例的方案中，认证权威 220 可以发布应用证书 234，证明应用 226 拥有属性“A”。认证权威 220 还可以发布平台证书 236，证明平坦服务 228 拥有属性“B”。认证权威 220 可以进一步发布存储证书 238，证明存储服务 230 拥有属性“C”。并且，认证权威 220 可以发布计算证书 240，证明计算服务 232 拥有属性“D”。在一些实施例中，可以涉及到多于一个的认证权威。例如，应用证书 234 可以由一个认证权威发布，而平台证书 236 可以由不同的认证权威发布。在一些实施例中，多个认证权威可以发布用于单个应用或服务的证书。

[0032] 当应用客户 224 接收到来自应用 226 的通过认证的服务时，应用客户 224 还可以请求并接收所有的证书 234、236、238 和 240，从而确认认证权威 220 对接收到的服务的认证。

[0033] 向应用客户 224 提供证书 234、236、238 和 240 中的每一证书可以意味着，应用客户 224 可以接收关于成为应用 226 的基础/支持应用 226 的具体服务的标识信息。例如，平台证书 236 可以标识平台服务 228，存储证书 238 可以标识存储服务 230，计算证书 240 可以标识计算服务 232。然而，在一些实施例中，应用 226 的提供者可能不想公开支持应用 226 的具体服务。例如，利用其他服务的创造性的组合（有时称为“混聚”）的应用的提供者可能不想显露所组合的具体服务的标识。客户或竞争者能够容易地复制所标识的应用或者可以在应用 226 不充当媒介的情况下来使用它们。

[0034] 一种可能的解决方案可以是允许应用 226 通过例如利用通过认证的属性的逻辑组合由证书 234、236、238 和 240 来构成交叉证书。例如，应用 226 可以通过利用分别来自证书 234、236、238 和 240 的属性的逻辑组合来构造交叉证书，证明应用 226 所提供的服务具有属性“A”、“B”、“C”和“D”。然而，该方法可能不安全，因为应用 226 能够伪造证书信息/属性和/或呈现来自其不再使用的服务或者其有时使用的服务的证书。例如，应用 226 可以在少量的时间内使用通过认证的存储服务 238，而大多时候依赖于未通过认证（以及推测上较廉价）的存储服务。即使仅仅是极少使用通过认证的存储服务 230，应用 226 随后也能够通过提供包括来自证书 238 的信息（用于存储服务 230）的单个的匿名化证书来操纵客户。另一方面，在一些情形下使用如上所述的自认证。例如，应用 226 可以开发复合认证，特别是基于合同期而允许某级别的离线审查或金融担保的情况下。

[0035] 图 3 示出了依照本文所描述的至少一些实施例布置的可使提供组合服务的应用能够通过使用复合证书来避免暴露其子服务的示例性的系统。

[0036] 如图 300 所示，应用客户 324（类似于图 2 中的应用客户 224）可以请求且接收来自应用 326（类似于图 2 中的应用 226）的服务。类似于图 2 所示的情形，应用 326 可以操作于平台服务 328 上，而且还得到存储服务 330 和/或计算服务 332 的支持。认证权威 320（类似于图 2 所示的认证权威 220）可以对应用 326、平台服务 328、存储服务 330 和/或计算服务 332 执行测试 322。认证权威 320 随后可以发布证书 334、336、338 和/或 340，证明分别与应用 326、平台服务 328、存储服务 330 和/或计算服务 332 相关联的某些属性。

[0037] 然而，如果客户正在请求通过认证的服务（以及因此还请求证书），而不是直接向应用客户 324 提供证书 334、336、338 和/或 340（如图 2 中的情况），则可以将证书提供给媒介 342。在一些实施例中，媒介 342 可以与认证权威（例如，认证权威 320）、数据中心或

一些其他受尊重或可信的实体或代表相关联或者可由它们来提供。在一些实施例中，媒介342自身可以对应用226、平台服务228、存储服务230和/或计算服务232进行遵守测试和/或认证，而不是认证权威320来进行或者与认证权威320一起来进行。

[0038] 然后，例如通过在单个证书中包含属性的逻辑组合（例如，属性“A”、“B”、“C”和“D”），媒介342可以基于证书334、336、338和/或340来生成复合证书344。应用326随后可以将来自应用客户324的任意认证请求引导至媒介342，媒介342随后可以将复合证书344提供给应用客户324。在一些实施例中，当客户324接收到来自应用326的请求服务时，媒介342将复合证书344提供给应用客户324。在其他实施例中，在提供被请求的服务之前，可以将复合证书344提供给应用客户324。还可以在被请求的服务之后提供复合证书344。认证可进一步是对话或批次层级且可以与任意时机相关联。

[0039] 单个的证书（和/或复合证书344）可任选地包括其他信息。例如，单个的证书可以包括关于应用326、平台服务328、存储服务330和/或计算服务332是否遵守支付卡行业(PCI)标准、关于技术公开的政府限制（例如，国际武器贸易条例或ITAR）、保健行业标准（例如，健康保险携带和责任法案或HIPAA）、受控商业列表(CCL)、ISO认证或任何其他适合的标准的信息。在一些示例中，如果所包含的证书/属性不都遵守特定标准，则复合证书不能声明对该特定标准的遵守。在这些情形下，复合证书可以反映所包含的证书/属性共有的最低遵守级别。

[0040] 图4A示出了依照本文描述的至少一些实施例布置的示例的系统，其中独立的媒介服务管理复合证书。

[0041] 如图400所示，一个或多个应用客户424（例如图2/3中的客户224/324）可以从一个或多个应用426（例如，图2/3中的应用226/326）请求服务。应用426可以由数据中心402托管，数据中心402类似于图1所描述的数据中心102。认证权威420（类似于图2/3中的认证权威220/320）可以向媒介442（类似于图2中的媒介342）提供与应用426相关联的子服务证书448。例如，子服务证书448可以是如图2/3中所述的平台证书236/336、存储证书238/338、和/或计算证书240/340。媒介442随后可以将子服务证书448组合成复合证书444（类似于图3中的复合证书342）。当应用426将所请求的服务提供给应用客户424时，媒介442也可以将复合证书444提供给应用客户424。在一些实施例中，应用426可以在其提供所请求服务时引导媒介442提供复合证书444。

[0042] 图4B示出了依照本文所描述的至少一些实施例布置的示例性的系统，其中托管应用的数据中心管理复合证书。

[0043] 图4B中的图450中类似标记的元件表现与图4A中的图400中方式类似。然而，在图450中，数据中心402处的网关（或对话边界控制器、网络处理器或类似物）452可以提供服务/认证请求的重定向或将其拷贝给媒介442，媒介442本身可以是诸如VM实例的实体。流量的截取可以提供实施的简易性，而无需对应用重新编程来处理认证（通过媒介）的过程。网关452可以提供与应用426的接口且可以是如上所述的应用426的部分或者是数据中心的单独的部分。

[0044] 具体地，网关452可以截取从应用客户424发到应用426的通过认证的服务请求。网关452可以将服务请求与认证请求分离，然后将服务请求传递到应用426。网关452可以将证书请求转送给媒介442，媒介442可以如上所述构造复合证书444并且将其提供给应用

客户 424。应用 426 可以通过网关 452 将请求的服务提供给应用可客户 424。如此配置的数据中心能够提供“作为服务的复合证书”，而不必修改应用 426。因此，应用 426 的提供者能够通过仅选择数据中心辅助的复合证书服务而隐藏应用 426 之下的子服务。

[0045] 在一些实施例中，针对具体的客户，可以调整通过认证的服务的提供。例如，应用（例如，图 2、图 3 和图 4A/B 中的应用 226、326 和 426）可配置为将不同定价的通过认证的未通过认证的服务传送给不同的客户。在一些示例中，应用可以利用证书媒介（例如，图 2、图 3 和图 4A 中的媒介 242、342 和 444，或者图 4B 中的网关 452）将通过认证的服务传送给客户，而将未通过认证的服务传送给不同的客户，而无需使用证书媒介且无需生成发送给客户的证书。可以基于服务请求或流量来源、对话级别、特定会话（例如，基于登录信息）或任意其他适合的参数来确定服务之间的这种区别（即，是提供通过认证的服务还是未通过认证的服务）。

[0046] 在其他示例中，应用之下的各个子服务可以各自向应用提供令牌。反过来，应用随后可以将令牌传送给认证权威以使认证权威独立地或者作为应用证书（例如，图 2 中的应用证书 234）的替代将复合证书传送给应用客户。

[0047] 图 5 示出了依照本文所描述的至少一些实施例布置的可用来管理用于保证的复合证书而不显露基础结构的通用计算设备。

[0048] 例如，如本文所描述的，计算设备 500 可用来管理用于保证的复合认证，而不显露基础结构。在示例性的基础配置 502 中，计算设备 500 可以包括一个或多个处理器 504 和系统存储器 506。存储器总线 508 可用于处理器 504 与系统存储器 506 之间通信。通过内虚线内的那些组件在图 5 中示出了基础配置 502。

[0049] 根据期望的配置，处理器 504 可以为任意类型，包括但不限于微处理器（μP）、微控制器（μC）、数字信号处理器（DSP）或其任意组合。处理器 504 可以包括诸如级别一超高速缓存 512 的一级或多级超高速缓存、处理器核 514 和寄存器 516。示例的处理器核 514 可以包括算术逻辑单元（ALU）、浮点单元（FPU）、数字信号处理核（DSP Core）或其任意组合。示例的存储器控制器 518 还可与处理器 504 一起使用，或者在一些实施方式中，存储器控制器 518 可以是处理器 504 的内部部件。

[0050] 根据所需的配置，系统存储器 506 可以是任意类型，包括但不限于易失性存储器（诸如 RAM）、非易失性存储器（诸如 ROM、闪存等）或其任意组合。系统存储器 506 可以包括操作系统 520、一个或多个应用 522 以及程序数据 524。应用 522 可以包括复合模块 526，该复合模块 526 可管理如本文所述的用于保证的复合认证而不显露基础结构。在一些实例中，程序数据 524 可以包括证书数据 528 或类似数据，以及其他数据，如本文所描述的。

[0051] 计算设备 500 可具有附加的特征或功能以及附加的接口以便于基础配置 502 与任何所需的设备和接口之间的通信。例如，总线 / 接口控制器 530 可用于利于基础配置 502 与一个或多个数据存储设备 532 之间经由存储接口总线 534 的通信。数据存储设备 532 可以是一个或多个可移除存储设备 536、一个或多个非可移除存储设备 538 或者其组合。可移除存储设备和非可移除存储设备的示例包括诸如软盘驱动器和硬盘驱动器（HDD）的磁盘设备、诸如压缩盘（CD）驱动器或数字多功能盘（DVD）驱动器的光盘驱动器、固态驱动器（SSD）和磁带驱动器，仅列举了几个。示例的计算机存储介质可以包括以用于诸如计算机可读指令、数据结构、程序模块或其它数据的信息的存储的任何方法或技术实现的易失性和

非易失性的介质以及可移除和非可移除的介质。

[0052] 系统存储器506、可移除存储设备536和非可移除存储设备538是计算机存储介质的示例。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存(flash memory)或其它存储器技术、CD-ROM、数字多功能盘(DVD)、固态驱动器或其它光学存储设备、磁盒、磁带、磁盘存储设备或其它磁存储设备、或者可用于存储所需信息并且可由计算设备500访问的任何其它介质。任意这样的计算机存储介质可以是计算设备500的部件。

[0053] 计算设备500还可以包括接口总线540,该接口总线用于方便从各接口设备(例如,一个或多个输出设备542、一个或多个外围设备接口544和一个或多个通信设备546)经由总线/接口控制器530到基础配置502的通信。一些示例的输出设备542包括图形处理单元548和音频处理单元550,其可配置为经由一个或多个A/V端口552与诸如显示器或扬声器的各外部设备通信。一个或多个示例的外围设备接口544包括串行接口控制器554或并行接口控制器556,其可配置为经由一个或多个I/O端口558与诸如输入设备(例如,键盘、鼠标、笔、语音输入设备、触摸输入设备等)或其它外围设备(例如,打印机、扫描仪等)的外部设备通信。示例的通信设备566包括网络控制器560,其可布置成便于经由一个或多个通信端口564通过网络通信链路与一个或多个其他计算设备562的通信。一个或多个其他计算设备562可以包括数据中心处的服务器、客户设备和类似设备。

[0054] 网络通信链路可以是通信介质的一个示例。通信介质通常可通过计算机可读指令、数据结构、程序模块或诸如载波或其它传输机制的调制数据信号中的其它数据来具体化,并且可以包括任何信息输送介质。“调制数据信号”可以是使得其特性中的一个或多个以将信号中的信息编码的方式设定或改变的信号。通过举例而不是限制的方式,通信介质可以包括诸如有线网络或直接线连接的有线介质,以及诸如声波、射频(RF)、微波、红外(IR)和其它无线介质的无线介质。如本文所使用的术语计算机可读介质可以包括存储介质和通信介质两者。

[0055] 计算设备500可以实现为通用或专用服务器、主机或包括上述任意功能的类似计算机的一部分。计算设备500还可以实现为包括膝上型计算机和非膝上型计算机配置两者的个人计算机。

[0056] 示例性的实施例还可以包括用于管理用于保证的复合认证而不显露基础结构的方法。这些方法能够以任意种方法来实施,包括本文所描述的结构。一种这样的方式可以是通过在本公开描述的类型的设备的机器操作。另一种可选的方式可以是与一位或多位执行一些操作的人类操作员相结合来执行方法的各操作中的一项或多项,而其他操作可以通过机器来执行。这些人类操作员无需彼此并置,但是各自可配有执行程序的一部分的机器。在其他示例中,人类交互可以自动进行,例如按照可以机器自动化的预先标准。

[0057] 图6是示出依照本文所描述的至少一些实施例布置的可以通过诸如图5的设备500的计算设备执行的示例性的方法的流程图。

[0058] 示例的方法可以包括如框622、624、626和/或628中的一个或多个图示的一个或多个操作、功能或动作,在一些实施例中可以通过诸如图5中的计算设备500的计算设备来执行。框图622-628中所描述的操作还可以存储为诸如计算设备610的计算机可读介质620的计算机可读介质中的计算机可执行指令。

[0059] 示例性的用于实施复合证书的处理可以开始于框622,“从认证权威处请求用于服

务应用和应用的服务要素的证书”，其中从认证权威（例如，图 2、图 3 和图 4A/B 中的认证权威 220、320 和 / 或 420）请求用于应用（例如，图 2、图 3 和图 4A/B 中的应用 226、326 和 / 或 426）和成为应用的基础的子服务要素（例如，图 2 和图 3 中的平台服务 228/328、存储服务 230/330、和 / 或计算服务 232/332）的证书（例如，图 2、图 3 和图 4A/B 中的应用证书 234/334、平台证书 236/336、存储证书 238/338、计算证书 240/340、和 / 或证书 448）。在一些示例中，媒介（例如，图 2、图 3 和图 4A 中的媒介 232、342 和 442，或者图 4B 中的网关 452）可以请求证书，并且媒介可以响应于来自应用的认证请求和 / 或来自应用客户（例如，图 2、图 3 和图 4A/B 中的客户 224、324 和 424）的认证请求而请求证书。在其他示例中，认证权威可以请求证书，特别是在如上所述的基于令牌的情形下。

[0060] 框 622 之后是框 624，“接收证书”，其中证书请求者接收所请求的证书。

[0061] 框 624 之后是框 626，“基于接收到的证书构成复合证书，而不显露服务要素标识”，其中接收到的证书可用于形成复合证书，而不显露成为应用的基础的各子服务或服务要素的标识。例如，与各个服务要素证书中的每一个相关联的经查证属性可进行逻辑组合且包含在复合证书中，如上所述。在一些示例中，复合证书关于一个或多个规则、标准或惯例的总体遵守级别可以通过与具体属性相关的证书中的最低共同遵守级别来确定，如上所述。在其他示例中，认证权威、媒介或数据中心网关可构造复合证书。

[0062] 最后，框 626 之后是框 628，“将复合证书提供给服务应用的客户”，其中在框 626 中形成的复合证书可以提供给已经从服务应用请求了服务的客户。在一些示例中，构造复合证书的认证权威、媒介或数据中心网关可以将复合证书提供给客户。

[0063] 图 7 示出了依照本文所描述的至少一些实施例布置的示例性的计算机程序产品的框图。

[0064] 在一些示例中，如图 7 所示，计算机程序产品 700 可以包括信号承载介质 702，信号承载介质 702 可以包括一条或多条机器可读指令 704，当通过例如处理器执行时，这些指令可以提供上文所描述的功能。因此，例如，参考图 5 中的处理器 504，认证应用 522 可以响应于通过介质 702 传送给处理器 504 的指令 704 而承担图 7 所示的一项或多项任务，从而执行与本文所描述的管理用于保证的复合认证而不显露基础结构相关联的动作。根据本文所述的一些实施例，一些指令可以包括例如 ：从认证权威处请求用于服务应用和应用的服务要素的认证 ；接收证书 ；基于接收到的证书来构成复合证书，而不显露服务要素标识，和 / 或将复合证书提供给服务应用的客户。

[0065] 在一些实现方式中，图 7 所示的信号承载介质 702 可以包含计算机可读介质 706，诸如但不限于硬盘驱动器、固态驱动器、压缩盘 (CD)、数字多功能盘 (DVD)、数字磁带、存储器等。在一些实施方式中，信号承载介质 702 可以包含可记录介质 708，诸如但不限于存储器、读 / 写 (R/W)CD、R/W DVD，等等。在一些实施方式中，信号承载介质 702 可以包含通信介质 710，诸如但不限于数字和 / 或模拟通信介质（例如，光纤电缆、波导、有线通信链路、无线通信链路等）。因此，例如，程序产品 700 可以通过 RF 信号承载介质传送到处理器 704 的一个或多个模块，其中信号承载介质 702 由无线通信介质 710（例如，符合 IEEE 802.11 标准的无线通信介质）来传送 .

[0066] 根据一些示例，采用复合认证用于保证的方法可以包括 ：在媒介认证服务处接收来自服务应用的用于认证的重定向请求 ；从认证权威处请求与服务应用和服务应用的服务

要素相关联的证书；接收证书；基于接收到的证书来构成复合证书，其中复合证书禁止服务要素的标识；以及响应于重定向请求而提供复合证书。

[0067] 根据一些实施例，该方法还可以包括：将复合证书构成为接收到的证书的逻辑组合。接收到的证书可以建立每个服务要素对预先定义的规则、标准和/或惯例的遵守。该方法还可以包括：如果两个以上的服务要素按其相应的证书所限定的遵守级别不同，则在复合证书中指示最低共同遵守级别。证书可以证明对支付卡行业(PCI)、健康保险携带和责任法案(HIPAA)、受控商业列表(CCL)、ISO认证或国际武器贸易条例(ITAR)的遵守。

[0068] 根据其他的实施例，该方法还可以包括：从多个认证权威处接收证书。服务要素可以包括计算服务、存储服务、平台服务和/或交互服务。该方法还可以包括：在媒介认证服务处对至少一个服务要素执行测试和/或认证任务；通过选择是否调用媒介认证服务来使服务应用能够对通过认证的服务和未通过认证的服务定价；和/或使所述服务要素能够将令牌提供给服务应用；以及从服务应用接收令牌以便传送给认证权威。

[0069] 根据其他的示例，采用复合认证用于保证的方法可以包括：从数据中心托管的应用接收服务请求，其中该请求包含认证请求；将认证请求与服务请求分离；从认证权威处请求与应用和应用的服务要素相关联的证书；接收证书；基于接收到的证书来构成复合证书，其中复合证书禁止服务要素的标识；以及响应于服务请求而提供复合证书。

[0070] 根据一些实施例，该方法还可以包括：将复合证书构成为接收到的证书的逻辑组合；截取包含认证请求的服务请求；将认证请求分离；和/或在托管应用的数据中心的网关或对话边界控制器中的一者处将认证请求转送给媒介认证服务。应用可以具有基于服务的体系结构。接收到的证书可以建立每个服务要素对预先定义的规则、标准和/或惯例的遵守。该方法还可以包括：如果两个以上服务要素按其相应的证书所限定的遵守级别不同，则在复合证书中指示最低共同遵守级别。证书可以证明对支付卡行业(PCI)、健康保险携带和责任法案(HIPAA)、受控商业列表(CCL)、ISO认证或国际武器贸易条例(ITAR)的遵守。

[0071] 根据其他的实施例，该方法还可以包括：从多个认证权威处接收证书。服务要素可以包括计算服务、存储服务、平台服务和/或交互服务。该方法还可以包括：通过选择是否调用媒介认证服务来使应用能够对通过认证的服务和未通过认证的服务定价；和/或使服务要素能够将令牌提供给应用，以及从应用接收令牌以便传送给认证权威。

[0072] 根据另外的示例，配置为采用复合认证用于保证的媒介认证服务可以包括：通信模块，其配置为与数据中心和认证权威所托管的服务应用通信；以及服务器。该服务器可配置为：接收来自服务应用的用于认证的重定向请求；从认证权威处请求与服务应用和服务应用的服务要素相关联的证书；接收证书；基于接收到的证书来构成复合证书，其中复合证书禁止服务要素的标识；以及响应于重定向请求而提供复合证书。

[0073] 根据一些实施例，该服务还可以配置为将复合证书构成为接收到的证书的逻辑组合。接收到的证书可以建立每个服务要素对预先定义的规则、标准和/或惯例的遵守。该服务可进一步配置为：如果两个以上服务要素按其相应的证书所限定的遵守级别不同，则在复合证书中指示最低共同遵守级别。证书可以证明对支付卡行业(PCI)、健康保险携带和责任法案(HIPAA)、受控商业列表(CCL)、ISO认证或国际武器贸易条例(ITAR)的遵守。

[0074] 根据其他的实施例，服务器可进一步配置为从多个认证权威处接收证书。服务要素可以包括计算服务、存储服务、平台服务和/或交互服务。媒介认证服务可以进一步配置

为对至少一个服务要素执行测试和/或认证任务。服务器可进一步配置为通过选择是否调用媒介认证服务来使服务应用能够对通过认证的服务和未通过认证的服务定价，和/或使服务要素能够将令牌提供给服务应用；以及从服务应用接收令牌以便传送给认证权威。

[0075] 根据另外的示例，配置为采用复合认证用于保证的基于云的数据中心可以包括：多个虚拟机，其可操作以便在一个或多个物理机上执行，其中至少一个虚拟机托管配置为将组合服务提供给客户的服务应用。数据中心还可以包括数据中心控制器，其配置为从数据中心托管的服务应用接收服务请求，其中请求包括认证请求；将认证请求与服务请求分离；以及将认证请求转送给媒介认证服务，使得响应于服务请求而通过媒介认证服务来提供禁止服务要素的标识的由用于子服务的各证书构成的复合证书。

[0076] 根据一些实施例，媒介认证服务可进一步配置为将复合证书构成为接收到的证书的逻辑组合。数据中心控制器可以是与服务应用接口的网关或对话边界控制器。媒介认证服务可由数据中心来提供。证书可以建立每个服务要素对一个或多个预先定义的规则、标准和/或惯例的遵守。媒介认证服务可进一步配置为：如果两个以上服务要素按其相应的证书所限定的遵守级别不同，则在复合证书中指示最低共同遵守级别。

[0077] 根据其他实施例，证书可以证明对支付卡行业(PCI)、健康保险携带和责任法案(HIPAA)、受控商业列表(CCL)、或国际武器贸易条例(ITAR)的遵守。服务要素可以包括计算服务、存储服务、平台服务和交互服务中的一项或多项。媒介认证服务可进一步配置为从多个认证权威处接收证书。通过选择是否调用复合证书，使服务应用能够对通过认证的服务和未通过认证的服务定价。数据中心控制器可进一步配置为使服务药物能够提供令牌且将令牌提供给媒介认证服务。

[0078] 根据一些示例，计算机可读存储介质可以存储采用复合认证用于保证的指令。所述指令可以包括：在媒介认证服务处接收来自服务应用的用于认证的重定向请求；从认证权威处请求与服务应用和服务应用的服务要素相关联的证书；接收所述证书；基于接收到的证书来构成复合证书，其中复合证书禁止服务要素的标识；以及响应于重定向请求而提供复合证书。

[0079] 根据一些示例，指令可进一步包括将复合证书构成为接收到的证书的逻辑组合。接收到的证书可以建立每个服务要素对预先定义的规则、标准和/或惯例的遵守。指令还可以包括：如果两个以上服务要素按其相应的证书所限定的遵守级别不同，则在复合证书中指示最低共同遵守级别。证书可以证明对支付卡行业(PCI)、健康保险携带和责任法案(HIPAA)、受控商业列表(CCL)、ISO认证或国际武器贸易条例(ITAR)的遵守。

[0080] 根据其他的实施例，指令还可以包括从多个认证权威处接收证书。服务要素可以包括计算服务、存储服务、平台服务和/或交互服务。指令还可以包括：在媒介认证服务处对至少一个服务要素执行测试和/或认证任务；通过选择是否调用媒介认证服务，使服务应用能够对通过认证的服务和未通过认证的服务定价；和/或使服务要素能够将令牌提供给服务应用；以及从服务应用接收令牌以便传送给认证权威。

[0081] 根据其他的示例，计算机可读存储介质可以存储采用复合认证用于保证的指令。所述指令可以包括：从数据中心托管的应用接收服务请求，其中该请求包含认证请求；将认证请求与服务请求分离；从认证权威处请求与应用和应用的服务要素相关联的证书；接收证书；基于接收到的证书来构成复合证书，其中复合证书禁止服务要素的标识；以及响

应于服务请求而提供复合证书。

[0082] 根据一些实施例，指令还可以包括将复合证书构成为接收到的证书的逻辑组合；截取包含认证请求的服务请求；将认证请求分离；和/或在托管应用的数据中心的网关或对话边界控制器中的一者处将认证请求转送到媒介认证服务。应用可具有基于服务的体系结构。接收到的证书可以建立每个服务要素对预先定义的规则、标准和/或惯例的遵守。指令还可以包括：如果两个以上的服务要素按其相应的证书所限定的遵守级别不同，则在复合证书中指示最低共同遵守级别。证书可以证明对支付卡行业(PCI)、健康保险携带和责任法案(HIPAA)、受控商业列表(CCL)、ISO认证或国际武器贸易条例(ITAR)的遵守。

[0083] 根据其他的实施例，指令还可以包括：从多个认证权威处接收证书。服务要素可以包括计算服务、存储服务、平台服务和/或交互服务。指令还可以包括：通过选择是否调用媒介认证服务，使应用能够对通过认证的服务和未通过认证的服务定价；和/或使服务要素能够将令牌提供给应用，以及从应用接收令牌以传送给认证权威。

[0084] 在系统方案的硬件实现和软件实现之间保留了极小的区别；硬件或软件的使用通常是（但并不总是，因为在一些背景下硬件和软件之间的选择会变得重要）表示成本相对于效率权衡的设计选择。存在各种可以实现（例如，硬件、软件和/或固件）本文所描述的过程和/或系统和/或其它技术的媒介物，并且优选的媒介物将随着部署过程和/或系统和/或其它技术的背景而变化。例如，如果实施者判定速度和精度重要，则实施者可以选择主硬件和/或固件媒介物；如果灵活性重要，则实施者可以选择主软件实现；或者，另外可选地，实施者可以选择硬件、软件和/或固件的一些组合。

[0085] 前面的详细说明已经通过框图、流程图和/或示例阐述了设备和/或过程的各个实施例。在这些框图、流程图和/或示例包含一项或多项功能和/或操作的程度上，本领域技术人员将理解的是可以通过各种各样的硬件、软件、固件或几乎其任意组合来单独地和/或统一地实现这些框图、流程图或示例内的每项功能和/或操作。在一个实施例中，本文所描述的主题的多个部分可经由专用集成电路(ASIC)、现场可编程门阵列(FPGA)、数字信号处理器(DSP)或其它集成格式来实现。然而，本领域技术人员将理解的是，在本文公开的实施例的一些方案可以整体地或部分地等同地实现为集成电路、在一个或多个计算机上运行的一个或多个计算机程序（例如，实现为在一个或多个计算机系统上运行的一个或多个程序）、在一个或多个处理器上运行的一个或多个程序（例如，实现为在一个或多个微处理器上运行的一个或多个程序）、固件、或几乎任何组合，并且根据本公开的内容，设计电路和/或编写用于软件和/或固件的代码将在本领域技术人员的技能范围内。

[0086] 本公开不受在本申请中所描述的特定实施例限制，这些特定实施例意在为各个方案的示例。本领域技术人员显而易见的是，能够进行各种改进和变型，而不偏离其精神和范围。根据前面的说明，除了本文列举的那些之外，在本公开范围内的功能上等同的方法和装置对于本领域技术人员而言将是显而易见的。旨在这些改进方案和变型例落在随附权利要求书的范围内。连同这些权利要求书所给予权利的等同方案的整个范围内，本公开仅受随附权利要求书限制。将理解的是，本公开不限于特定的方法、试剂、化合物组成或生物系统，当然这些可以变化。还应理解的是，本文所使用的术语仅是为了描述特定实施例的目的，而不意在限制。

[0087] 另外，本领域技术人员将理解的是，本文所描述的主题的机制能够以各种形式分

布为程序产品，并且本文所描述的主题的示例性实施例适用，无论实际上用于实施分布的特定类型的信号承载介质如何。信号承载介质的示例包括但不限于以下：可记录型介质，诸如软盘、硬盘驱动器、压缩盘 (CD)、数字多功能盘 (DVD)、数字带、计算机存储器等；以及传输型介质，诸如数字和 / 或模拟通信介质（例如，光纤电缆、波导、有线通信链路、无线通信链路等）。

[0088] 本领域技术人员将理解的是，在本领域内常见的是以本文阐述的方式来描述设备和 / 或过程，此后利用工程实践将这些所描述的设备和 / 或过程集成到数据处理系统中。也即，本文所描述的设备和 / 或过程的至少一部分可以通过合理量的实验集成到数据处理系统中。本领域技术人员将理解的是，典型的数据处理系统通常包括如下中的一种或多种：系统单元壳体、视频显示设备、诸如易失性和非易失性存储器的存储器、诸如微处理器和数字信号处理器的处理器、诸如操作系统的计算实体、驱动器、图形用户接口、和应用程序、诸如触摸板或触摸屏的一个或多个交互设备、和 / 或包括反馈环和控制电动机（例如，用于感测门架系统的位置和 / 或速度的反馈；用于移动和 / 或调整部件和 / 或量的控制电动机）的控制系统。

[0089] 典型的数据处理系统可利用任何适合的商业上提供的部件来实现，诸如在数据计算 / 通信和 / 或网络计算 / 通信系统中常见的部件。本文所描述的主题有时说明了包含在不同的其它部件内的不同部件或与不同的其它部件连接的不同部件。应理解的是，这些所描绘的体系结构仅是示例性的，并且实际上可以实施实现相同功能的许多其它体系结构。在概念意义上，实现相同功能的任何部件的布置有效地“关联”，使得实现期望功能。因此，在此处组合以实现特定功能的任何两个部件可视为彼此“关联”，使得实现期望功能，无论体系结构或中间部件如何。同样，任意两个如此关联的部件还可视为彼此“可操作地连接”、或“可操作地耦合”以实现期望的功能，并且能够如此关联的任意两个部件还可视为彼此“能够可操作地耦合”以实现期望功能。能够可操作耦合的具体示例包括但不限于能够物理上连接和 / 或物理交互的部件和 / 或能够无线交互和 / 或无线交互的部件和 / 或逻辑上交互和 / 或能够逻辑上交互的部件。

[0090] 关于本文中基本上任何复数和 / 或单数术语的使用，本领域技术人员能够根据上下文和 / 或应用适当地从复数变换成单数和 / 或从单数变换成复数。为了清晰的目的，本文中明确地阐明了各单数 / 复数的置换。

[0091] 本领域技术人员将理解，一般地，本文所使用的术语，尤其是随附权利要求（例如，随附权利要求的主体）中所使用的术语，通常意在为“开放式”术语（例如，术语“包括”应当解释为“包括但不限于”，术语“具有”应解释为“至少具有”，术语“包括”应解释为“包括但不限于”，等等）。本领域技术人员还理解，如果意图表达引导性权利要求记述项的具体数量，该意图将明确地记述在权利要求中，并且在不存在这种记述的情况下，不存在这样的意图。例如，为辅助理解，下面的随附权利要求可能包含了引导性短语“至少一个”和“一个或多个”的使用以引导权利要求记述项。然而，这种短语的使用不应解释为暗指不定冠词“一”或“一个”引导权利要求记述项将包含该所引导的权利要求记述项的任何特定权利要求局限于仅包含一个该记述项的实施例，即使当同一权利要求包括了引导性短语“一个或多个”或“至少一个”以及诸如不定冠词“一”或“一个”的（例如，“一”和 / 或“一个”应当解释为表示“至少一个”或“一个或多个”）；这同样适用于对于用于引导权利要求记述项的

定冠词的使用。另外，即使明确地记述了被引导的权利要求记述项的具体数量，本领域技术人员将理解到这些记述项应当解释为至少表示所记述的数量（例如，没有其它修饰语的裸记述“两个记述项”表示至少两个记述项或两个以上的记述项）。

[0092] 此外，在使用类似于“A、B 和 C 等中的至少一个”的惯用法的那些实例中，通常这样的构造旨在表达本领域技术人员理解该惯用法的含义（例如，“具有 A、B 和 C 中的至少一个的系统”将包括但不限于仅具有 A、仅具有 B、仅具有 C、具有 A 和 B、具有 A 和 C、具有 B 和 C、和 / 或具有 A、B 和 C 等等的系统）。本领域技术人员将进一步理解，呈现两个以上可选项的几乎任何分离词和 / 或短语，无论是在说明书、权利要求或附图中，都应理解为设想包括一项、任一项或两项的可能性。例如，术语“A 或 B”将理解为包括“A”或“B”或“A 和 B”的可能性。

[0093] 另外，在根据马库什组 (Markush group) 描述本公开的特征或方案的情况下，本领域技术人员将理解的是本公开也因此以马库什组的任何独立成员或成员的子组来描述。

[0094] 本领域技术人员将理解的是，为了任何以及全部的目的，诸如在提供所撰写的说明书方面，本文所公开的全部范围也涵盖了任何和全部的可能的子范围及其子范围的组合。能够容易地认识到任何所列范围都充分地描述了同一范围并且使同一范围分解成至少均等的一半、三分之一、四分之一、五分之一、十分之一等等。作为非限制示例，本文所论述的每个范围能够容易地分解成下三分之一、中三分之一和上三分之一，等等。本领域技术人员还将理解的是，诸如“多达”、“至少”、“大于”、“小于”等所有的语言包括所记述的数量并且是指如上文所论述的随后能够分解成子范围的范围。最后，本领域技术人员将理解的是，范围包括每个独立的成员。因此，例如，具有 1-3 个单元的组是指具有 1 个、2 个或 3 个单元的组。类似地，具有 1-5 个单元的组是指具有 1 个、2 个、3 个、4 个、或 5 个单元的组，等等。

[0095] 虽然本文公开了各个方案和实施例，但是其它的方案和实施例对于本领域技术人员而言将是显而易见的。因此，本文所公开的各个方案和实施例是为了示例的目的而不意在限制，真正的范围和精神是通过随附的权利要求表示的。

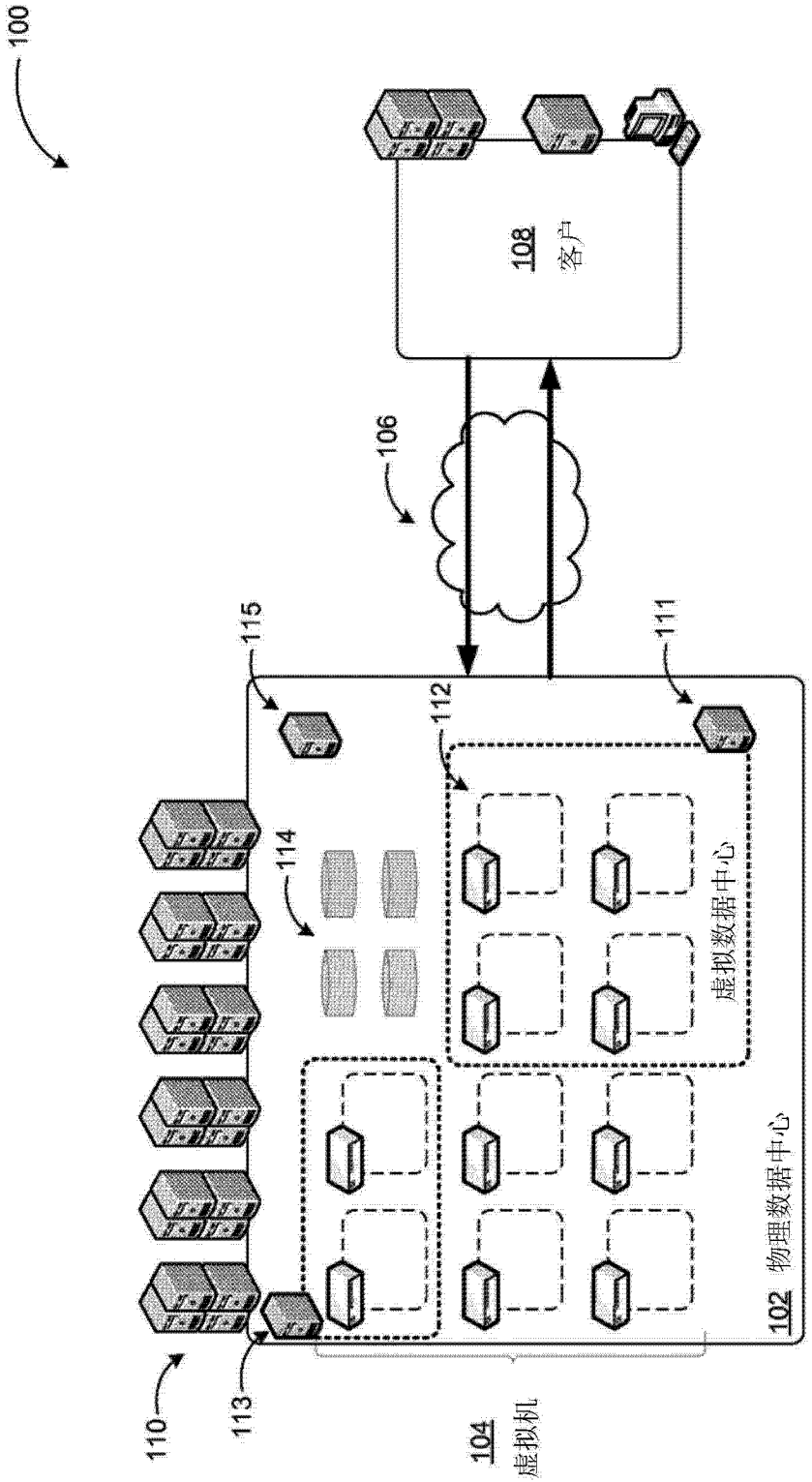

100
108 客户
106
115
111
112
114
虚拟数据中心
102 物理数据中心
110
113
104 虚拟机

图 1

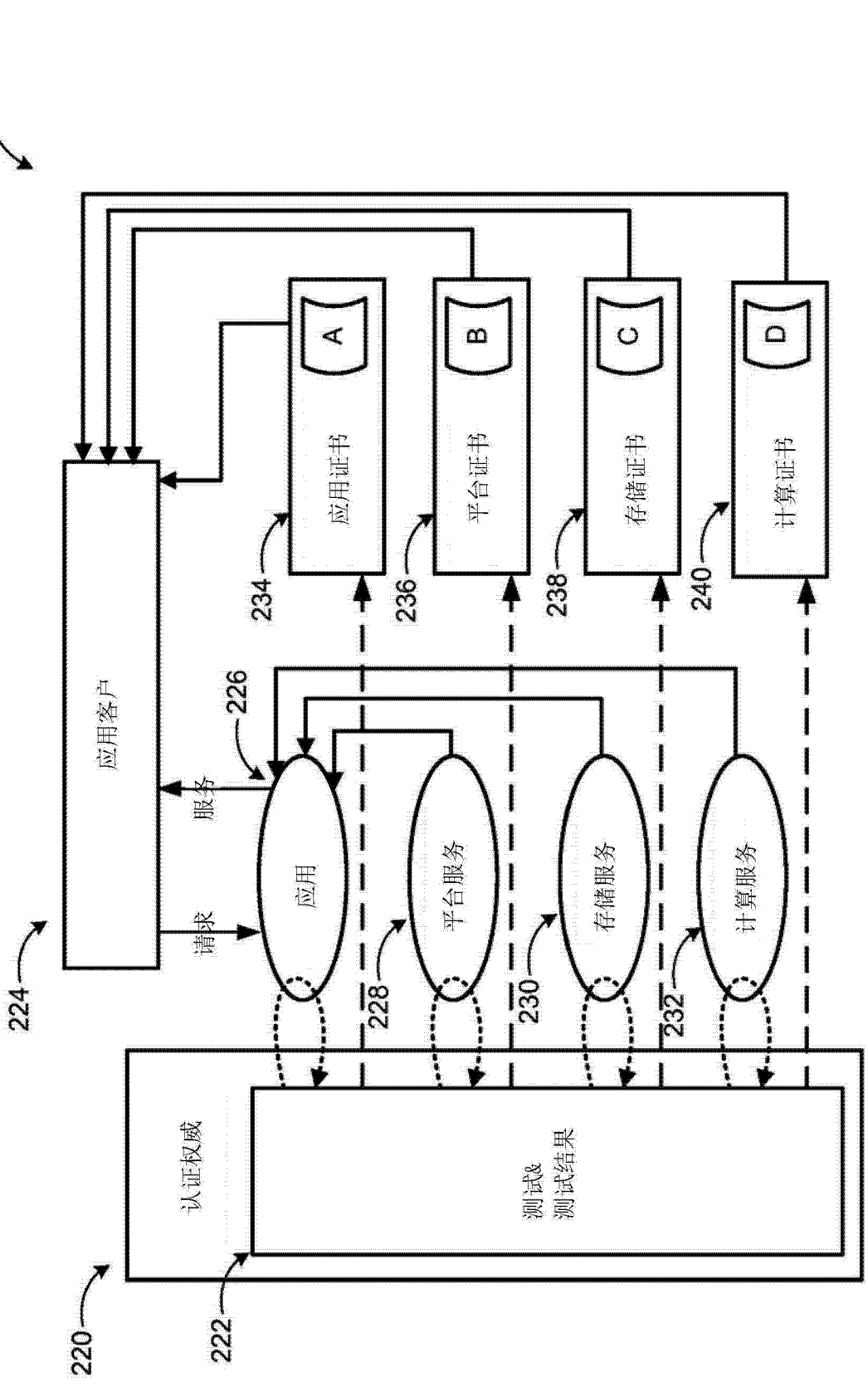

200
A
B
C
D
应用证书
平台证书
存储证书
计算证书
234
236
238
240
应用客户
226
服务
请求
应用
平台服务
存储服务
计算服务
224
228
230
232
认证权威
测试&
测试结果
220
222

图 2

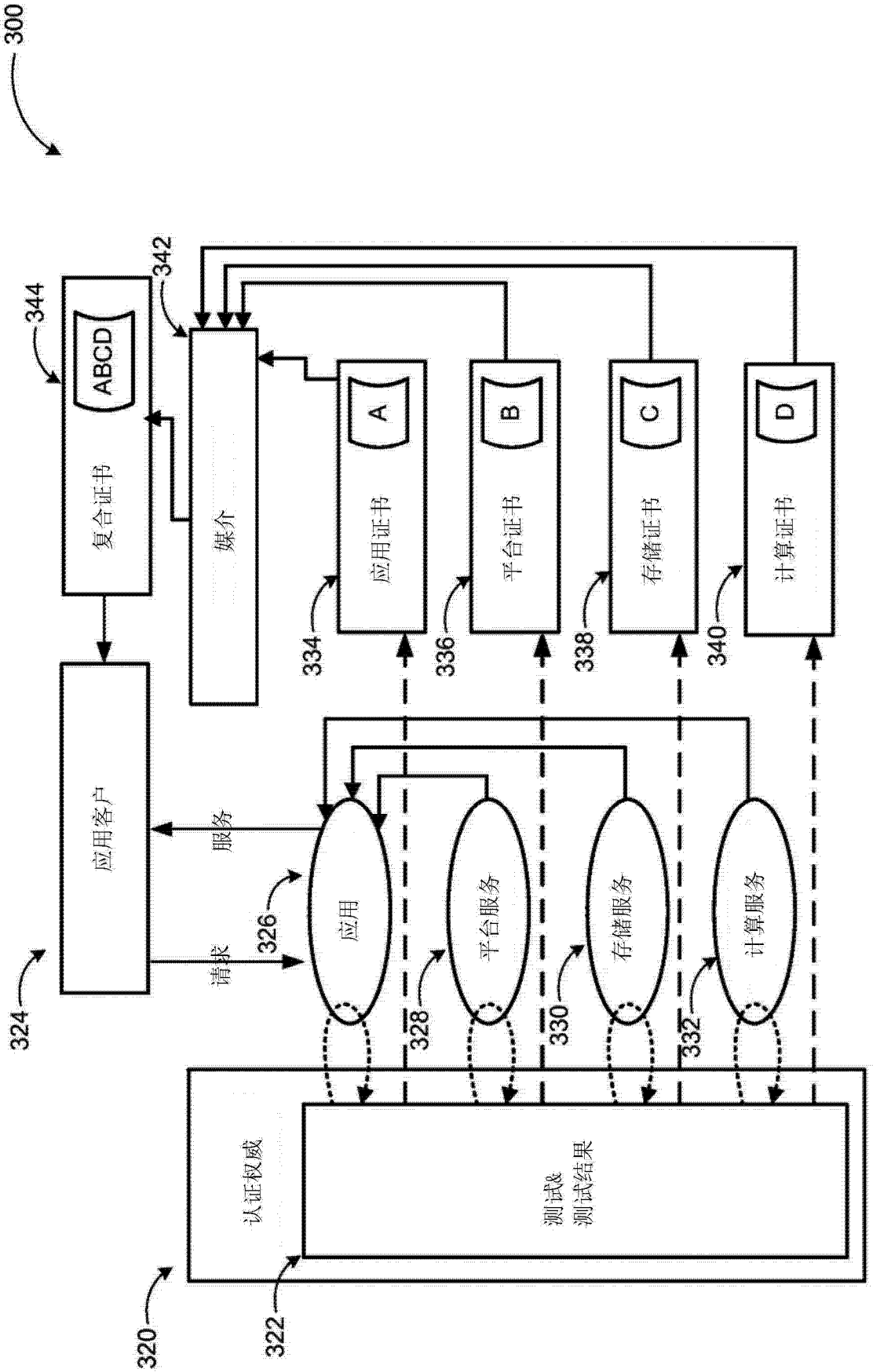

300
342
344
ABCD
复合证书
媒介
A
B
C
D
应用证书
平台证书
存储证书
计算证书
334
336
338
340
应用客户
服务
请求
326
应用
平台服务
存储服务
计算服务
324
328
330
332
认证权威
测试&
测试结果
320
322

图 3

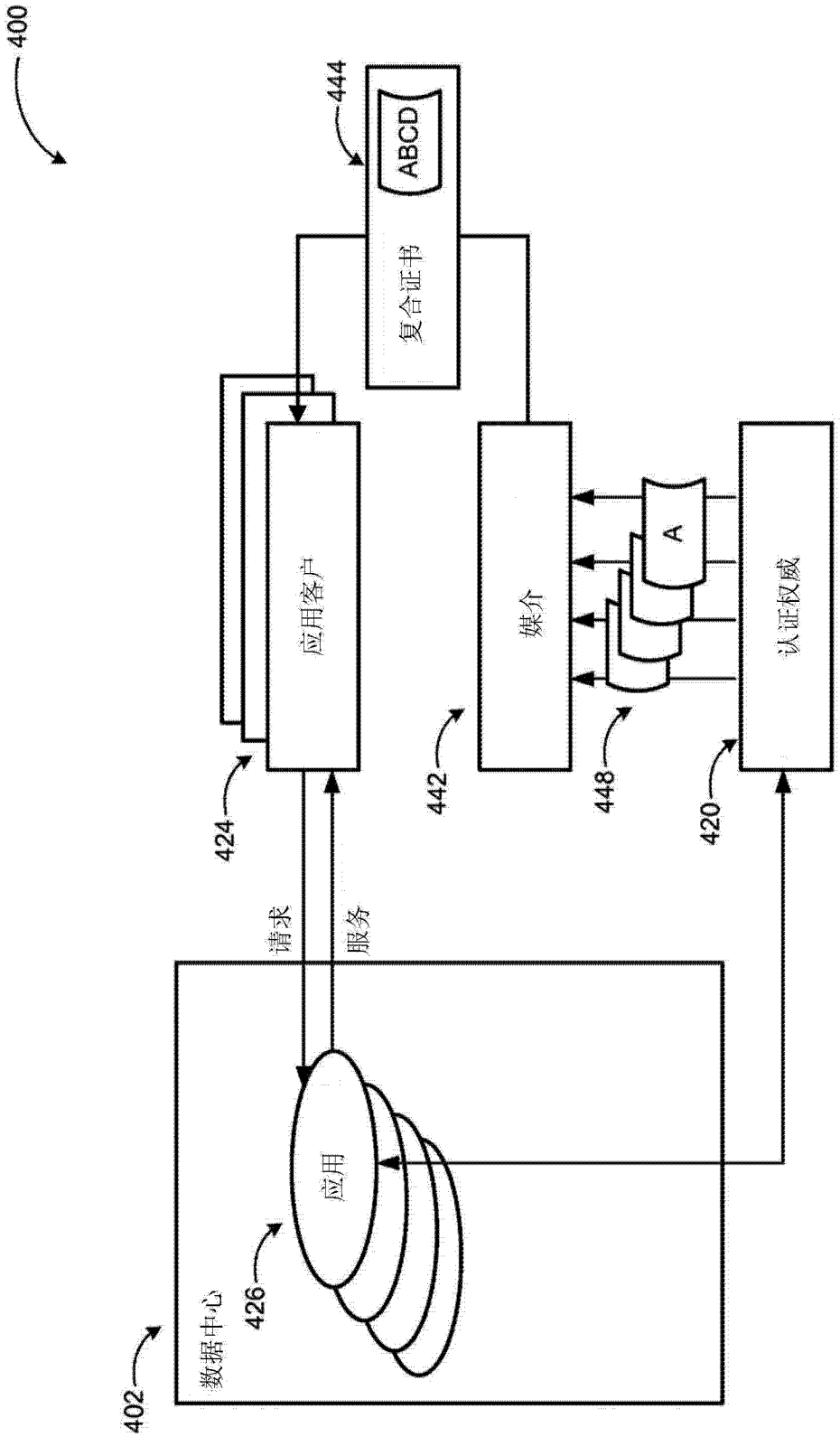

400
444
ABCD
复合证书
应用客户
424
媒介
442
A
448
认证权威
420
请求
服务
应用
426
数据中心
402

图 4A

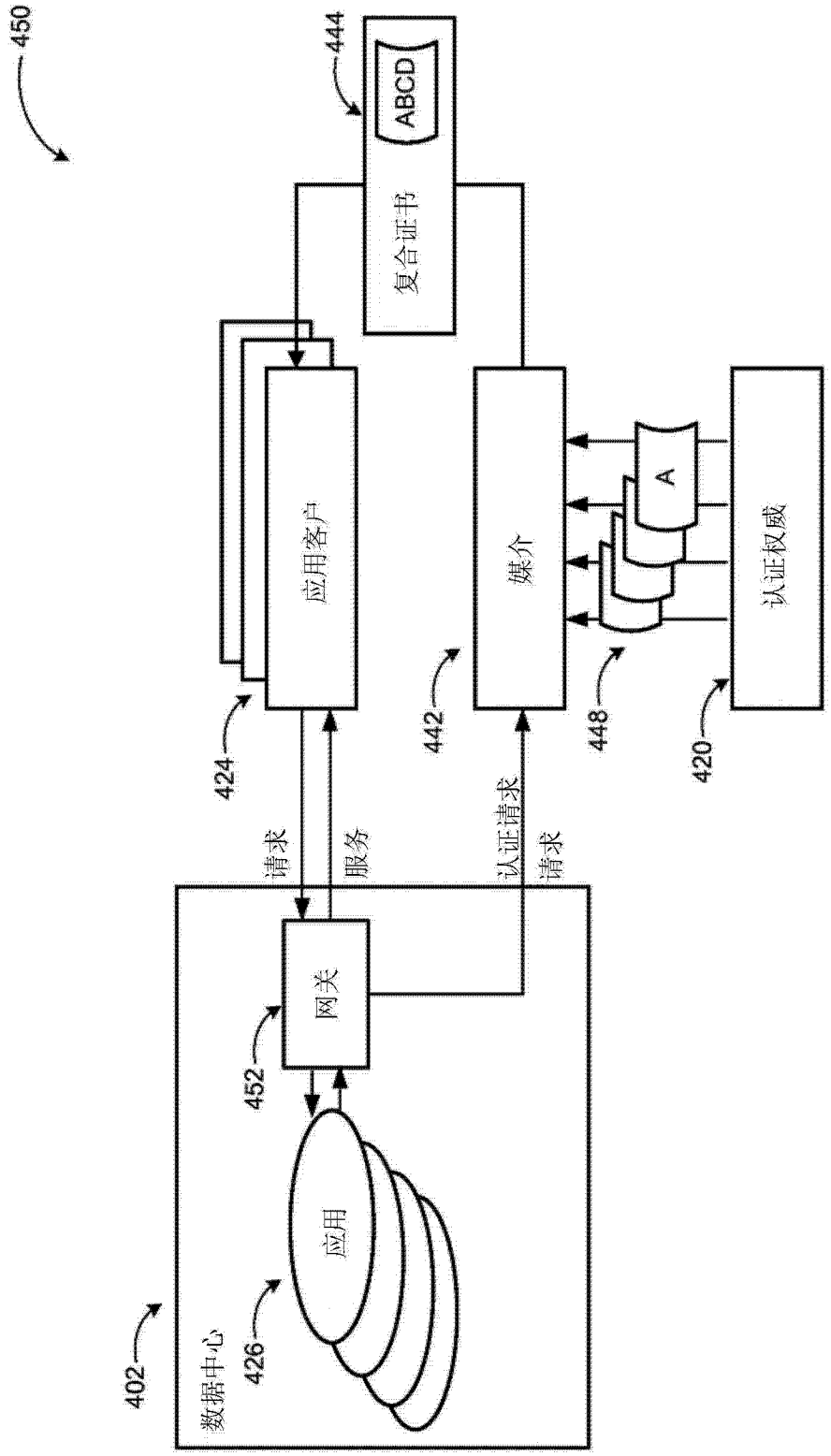

450
444
ABCD
复合证书
应用客户
媒介
A
认证权威
424
442
448
420
请求
服务
认证请求
请求
网关
452
应用
426
数据中心
402

图 4B

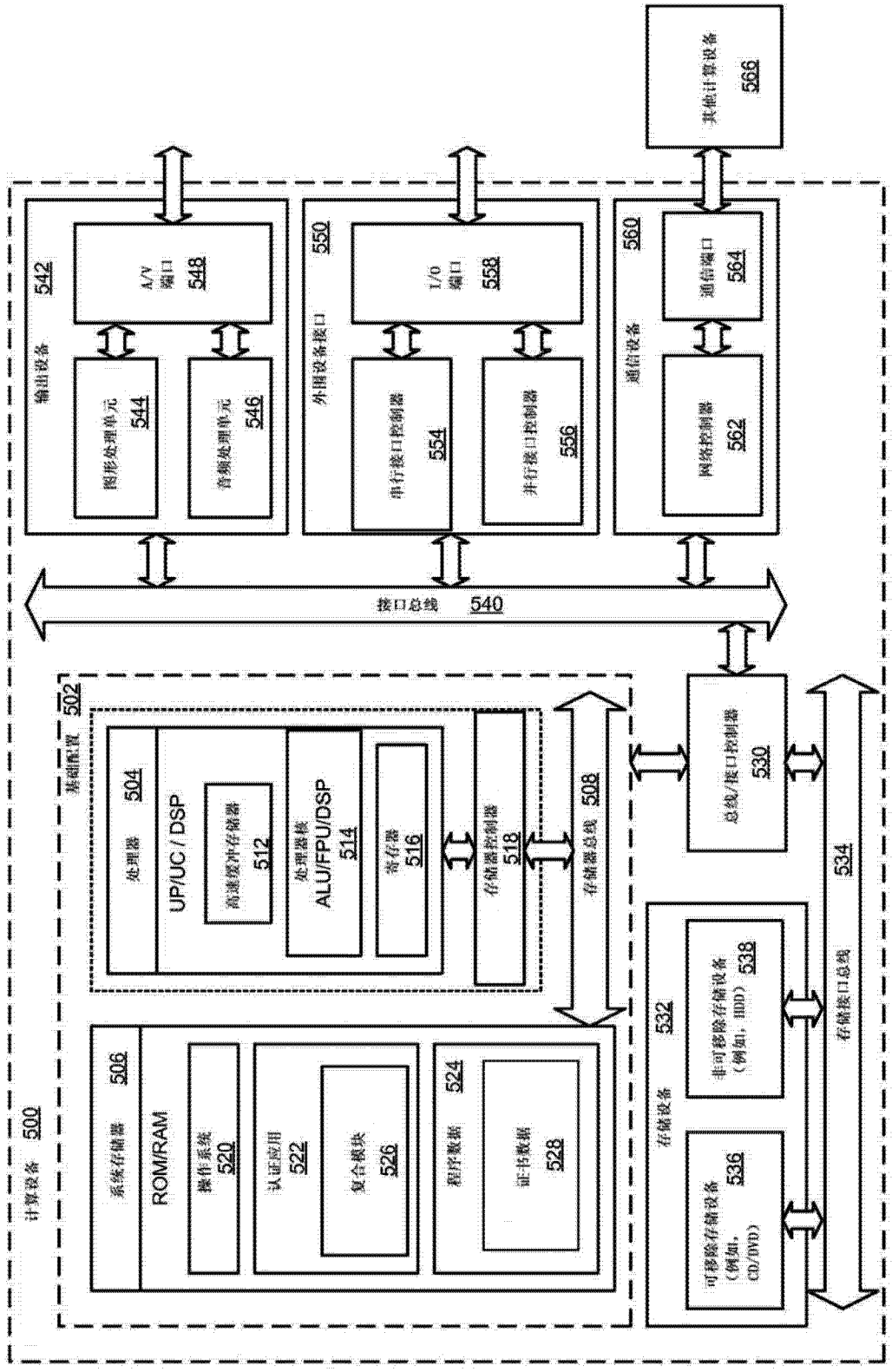

其他计算设备 566
计算设备 500
输出设备 542
A/V 端口 548
图形处理单元 544
音频处理单元 546
外围设备接口 550
I/O 端口 558
串行接口控制器 554
并行接口控制器 556
通信设备 560
通信端口 564
网络控制器 562
接口总线 540
基础配置 502
处理器 504
UP/UC / DSP
高速缓冲存储器 512
处理器核 ALU/FPU/DSP 514
寄存器 516
存储器控制器 518
存储器总线 508
总线/接口控制器 530
系统存储器 506
ROM/RAM
操作系统 520
认证应用 522
复合模块 526
程序数据 524
证书数据 528
存储设备 532
非可移除存储设备（例如，HDD） 538
可移除存储设备（例如，CD/DVD） 536
存储接口总线 534

图 5

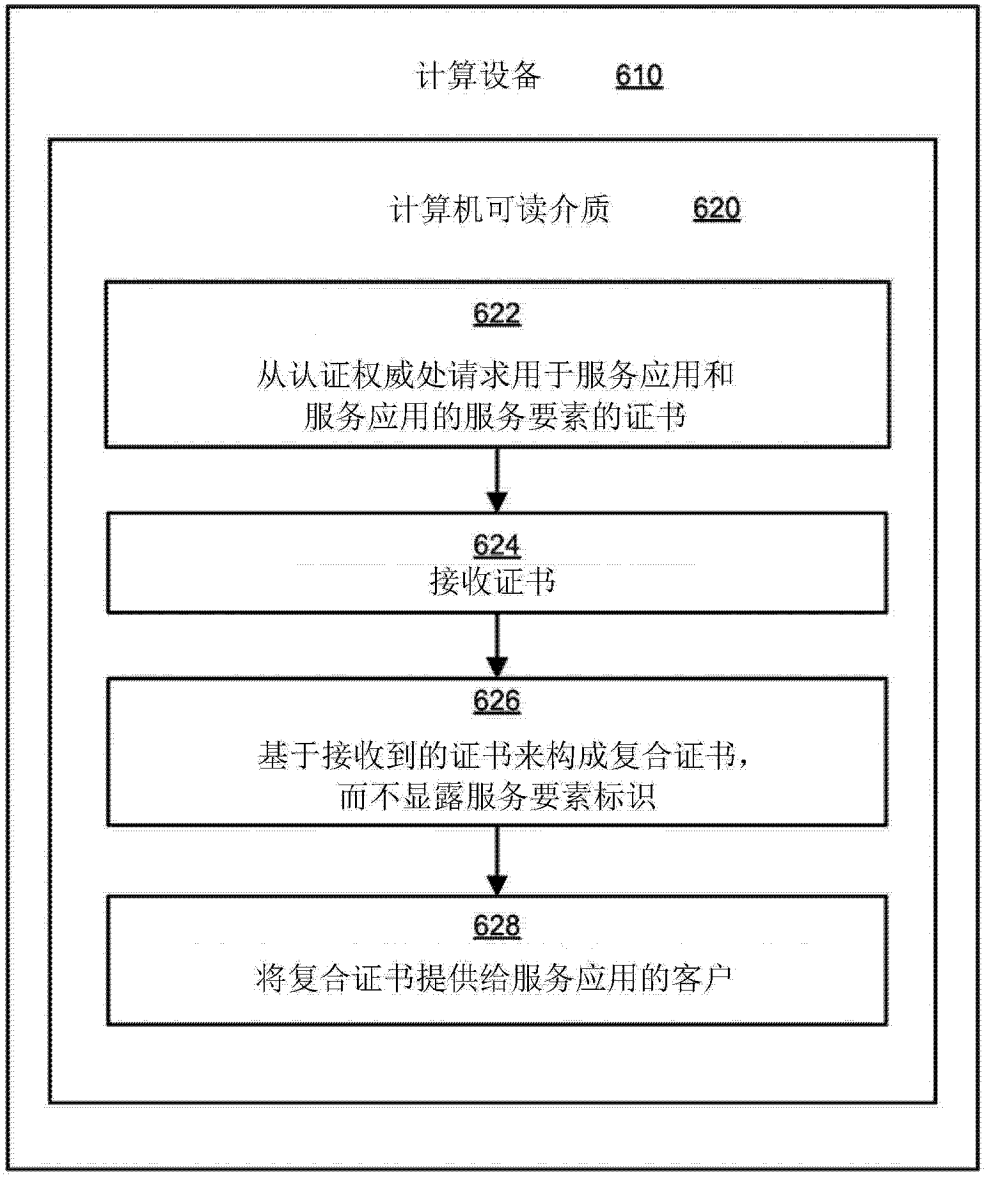

计算设备 610
计算机可读介质 620
622
从认证权威处请求用于服务应用和服务应用的服务要素的证书
624
接收证书
626
基于接收到的证书来构成复合证书，而不显露服务要素标识
628
将复合证书提供给服务应用的客户

图 6

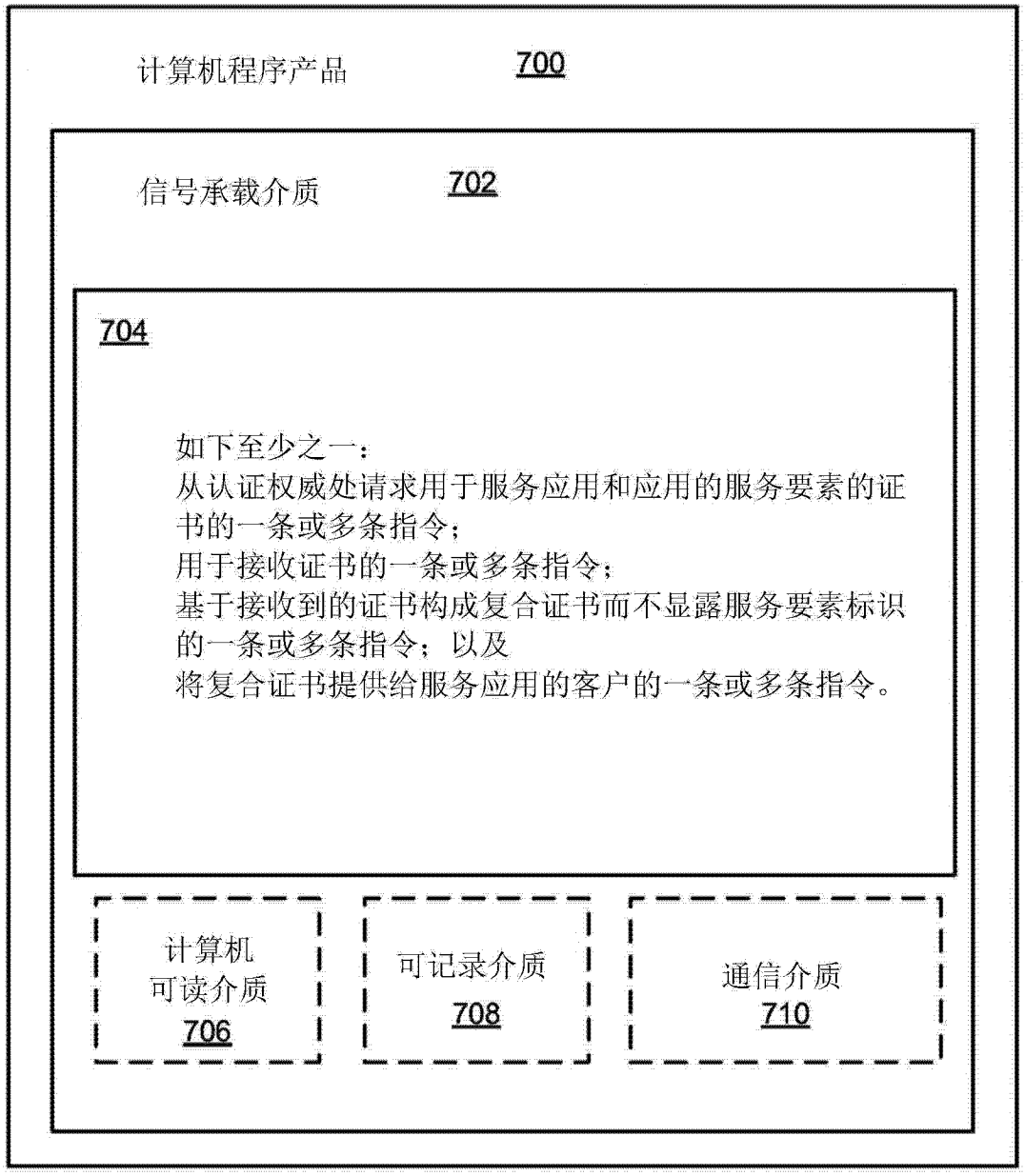

计算机程序产品
700
信号承载介质
702
704
如下至少之一：
从认证权威处请求用于服务应用和应用的服务要素的证书的一条或多条指令；
用于接收证书的一条或多条指令；
基于接收到的证书构成复合证书而不显露服务要素标识的一条或多条指令；以及
将复合证书提供给服务应用的客户的一条或多条指令。
计算机可读介质
706
可记录介质
708
通信介质
710

图 7