



(12) 发明专利

(10) 授权公告号 CN 119054251 B

(45) 授权公告日 2025. 07. 11

(21) 申请号 202380029138.1

(22) 申请日 2023.03.14

(65) 同一申请的已公布的文献号
申请公布号 CN 119054251 A

(43) 申请公布日 2024.11.29

(30) 优先权数据
17/700,281 2022.03.21 US

(85) PCT国际申请进入国家阶段日
2024.09.20

(86) PCT国际申请的申请数据
PCT/US2023/015214 2023.03.14

(87) PCT国际申请的公布数据
W02023/183165 EN 2023.09.28

(73) 专利权人 亚马逊技术股份有限公司
地址 美国华盛顿州

(72) 发明人 M·苏布兰马尼安 M·A·莱维
B·P·赫斯

(74) 专利代理机构 上海专利商标事务所有限公
司 31100
专利代理师 李炜 周全

(51) Int.Cl.
H04L 9/40 (2006.01)
H04L 9/32 (2006.01)

(56) 对比文件
CN 110932861 A, 2020.03.27
US 2018062855 A1, 2018.03.01

审查员 张巍

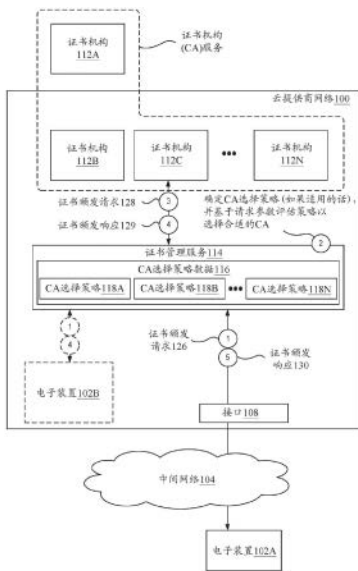
权利要求书3页 说明书16页 附图7页

(54) 发明名称

云提供商网络中的证书机构选择

(57) 摘要

描述了用于证书机构(CA)选择的技术。云提供商网络的证书管理服务从电子装置接收生成证书的第一请求,所述第一请求包括用户的身份的指示和与所述证书相关联的域名的标识。标识适用于第一请求的CA选择策略,所述CA选择策略包括CA选择规则。通过评估CA选择规则来识别生成所述证书的CA,所述CA选择规则将所述域名的至少一部分与所述CA相关联。生成所述证书的第二请求被发送到所标识的CA。来自所述CA的证书或所述证书的标识被返回到所述电子装置。



1. 一种计算机实现的方法,其包括:

由云提供商网络的证书管理服务接收创建第一证书机构选择策略的第一请求,其中所述第一请求包括:(a) 第一域名与证书机构的关联,以及(b) 将所述第一证书机构选择策略与以下至少一者相关联的策略适用性:(i) 用户的身份、(ii) 与所述用户的所述身份相关联的角色、或(iii) 包括所述用户的所述身份的群;

将所述第一证书机构选择策略和所述策略适用性存储在数据存储库中,其中所述第一证书机构选择策略包括将所述第一域名与所述证书机构相关联的证书机构选择规则;

从电子装置并且由证书管理服务接收生成证书的第二请求,其中所述第二请求包括所述用户的所述身份的指示和要与所述证书相关联的第二域名的标识;

至少部分地基于所述策略适用性来标识适用于第二请求的所述第一证书机构选择策略;

至少部分地基于所述第二域名是所述第一域名的子域,评估所述证书机构选择规则以标识所述证书机构;

向所述证书机构发送生成所述证书的第三请求;以及

从所述证书机构向所述电子装置返回所述证书或所述证书的标识。

2. 如权利要求1所述的计算机实现的方法,其中所述第二请求不包括任何证书机构的标识。

3. 如权利要求1所述的计算机实现的方法,其还包括:

在评估所述证书机构选择规则之前:

标识适用于所述第一请求的第二证书机构选择策略;以及

确定所述第二证书机构选择策略不包括与所述第二域名相关联的规则。

4. 一种计算机实现的方法,其包括:

从电子装置并通过云提供商网络的证书管理服务接收生成证书的第一请求,其中所述第一请求包括用户的身份的指示和要与所述证书相关联的域名的标识;

标识适用于所述第一请求的第一证书机构选择策略,其中所述第一证书机构选择策略包括证书机构选择规则;

评估所述证书机构选择规则以标识用以生成所述证书的证书机构,其中所述证书机构选择规则将所述域名的至少一部分与所述证书机构相关联;

向所述证书机构发送生成所述证书的第二请求;以及

从所述证书机构向所述电子装置返回所述证书或所述证书的标识。

5. 如权利要求4所述的计算机实现的方法,其中所述第一请求不包括任何证书机构的标识。

6. 如权利要求4所述的计算机实现的方法,其还包括:

在评估所述证书机构选择规则之前:

标识适用于所述第一请求的第二证书机构选择策略;以及

确定所述第二证书机构选择策略不包括与所述域名相关联的规则。

7. 如权利要求6所述的计算机实现的方法,其中所述第一证书机构选择策略与包括所述用户的所述身份的群相关联,并且所述第二证书机构选择策略与所述用户的所述身份相关联。

8. 如权利要求4所述的计算机实现的方法,其还包括:

由所述证书管理服务接收创建所述第一证书机构选择策略的第三请求,其中所述第三请求包括(a)所述域名的至少一部分与所述证书机构的关联,以及(b)将所述第一证书机构选择策略与以下至少一者相关联的策略适用性:(i)用户的所述身份、(ii)与所述用户的所述身份相关联的角色、或(iii)包括所述用户的所述身份的群;以及

将所述第一证书机构选择策略存储在数据存储库中。

9. 如权利要求8所述的计算机实现的方法,其中所述策略适用性存储在与所述第一证书机构选择策略相关联的元数据中。

10. 如权利要求4所述的计算机实现的方法,其中所述证书机构是(a)被配置为用于由包括所述用户的组织的管理员使用的私有证书机构服务、或者(b)公共证书机构,其中所述公共证书机构是所述云提供商网络或第三方的服务。

11. 如权利要求4所述的计算机实现的方法,其中所述第一证书机构选择策略通过以下各项中的至少一项而适用于所述第一请求:(a)所述第一证书机构选择策略与所述用户的所述身份相关联、(b)所述第一证书机构选择策略与和所述用户的所述身份相关联的角色相关联、(c)所述第一证书机构选择策略与包括所述用户的所述身份的群相关联、或者(d)所述第一证书机构选择策略是默认策略。

12. 如权利要求11所述的计算机实现的方法,其中所述第一证书机构选择策略与地理区域相关联,并且其中所述第一证书机构选择策略还至少部分地基于由所述地理区域中的所述证书管理服务接收到所述第一请求而适用于所述第一请求。

13. 如权利要求4所述的计算机实现的方法,其中所述证书机构是所述用户可用的多个证书机构中的一个证书机构。

14. 一种系统,其包括:

第一个或多个电子装置,用于实现云提供商网络的数据存储服务,所述数据存储服务包括在执行时使得所述数据存储服务存储证书机构选择策略数据的指令;以及

第二个或多个电子装置,用于实现所述云提供商网络的证书管理服务,所述证书管理服务包括在执行时使得所述证书管理服务进行以下操作的指令:

从第三电子装置接收生成证书的第一请求,其中所述第一请求包括用户的身份的指示和要与所述证书相关联的域名的标识;

标识适用于所述第一请求且在所述证书机构选择策略数据中的第一证书机构选择策略,其中所述第一证书机构选择策略包括证书机构选择规则;

评估所述证书机构选择规则以标识用以生成所述证书的证书机构,其中所述证书机构选择规则将所述域名的至少一部分与所述证书机构相关联;

向所述证书机构发送生成所述证书的第二请求;以及

从所述证书机构向所述第三电子装置返回所述证书或所述证书的标识。

15. 如权利要求14所述的系统,其中所述第一请求不包括任何证书机构的标识。

16. 如权利要求14所述的系统,所述证书管理服务包括在执行时使得所述证书管理服务进行以下操作的另外的指令:

在评估所述证书机构选择规则之前:

标识适用于所述第一请求的第二证书机构选择策略;以及

确定所述第二证书机构选择策略不包括与所述域名相关联的规则。

17. 如权利要求16所述的系统,其中所述第一证书机构选择策略与包括所述用户的所述身份的群相关联,并且所述第二证书机构选择策略与所述用户的所述身份相关联。

18. 如权利要求14所述的系统,所述证书管理服务包括在执行时使得所述证书管理服务进行以下操作的另外的指令:

接收创建所述第一证书机构选择策略的第三请求,其中所述第三请求包括 (a) 所述域名的至少一部分与所述证书机构的关联,以及 (b) 将所述第一证书机构选择策略与以下至少一者相关联的策略适用性: (i) 用户的所述身份、(ii) 与所述用户的所述身份相关联的角色、或 (iii) 包括所述用户的所述身份的群;以及

将所述第一证书机构选择策略存储在所述证书机构选择策略数据中。

19. 如权利要求18所述的系统,其中所述策略适用性作为元数据存储在所述证书机构选择策略数据中,并且与所述第一证书机构选择策略相关联。

20. 如权利要求14所述的系统,其中所述证书机构是 (a) 被配置为用于由包括用户的组织的管理员使用的私有证书机构服务、或者 (b) 公共证书机构,其中所述公共证书机构是所述云提供商网络或第三方的服务。

云提供商网络中的证书机构选择

背景技术

[0001] 证书指的是已经被加密保护并且可以实现安全通信的数字文档。证书通常在被称为公共密钥基础设施 (PKI) 的密码系统中使用。PKI 依赖于使用密钥对 (私钥和公钥) 的非对称加密系统来加密和解密数据、对数据进行数字签名等。公钥可以与证明给定公钥的所有者的数字证书相关联。数字证书由充当可信第三方的公共或私有证书机构创建和签名。证书的典型用例是经由安全套接字层 (SSL) / 传输层安全性 (TLS) 保护网络通信, 尽管证书也可以用于其他安全目的, 诸如对文件进行数字签名以确保它们源自证书的持有者。证书可以被称为 X.509 证书 (参考证书系统的行业标准)。

附图说明

[0002] 将参考附图描述根据本公开的各种实施方案, 在附图中:

[0003] 图1是示出根据一些实施方案的用于证书机构选择的环境的图。

[0004] 图2是示出根据一些实施方案的用于配置证书机构选择策略的环境的图。

[0005] 图3是示出根据一些实施方案的示例性证书机构选择策略的图。

[0006] 图4是示出根据一些实施方案的在其中选择不同证书机构的环境的图。

[0007] 图5是示出根据一些实施方案的用于证书机构选择的方法的操作的流程图。

[0008] 图6示出根据一些实施方案的示例性提供商网络环境。

[0009] 图7是根据一些实施方案的向客户提供存储服务 and 硬件虚拟化服务的示例性提供商网络的框图。

[0010] 图8是示出了可以在一些实施方案中使用的示例计算机系统的框图。

具体实施方式

[0011] 本公开涉及用于在处理证书相关请求时从多个证书机构 (CA) 进行 CA 选择的方法、设备、系统和非暂时性计算机可读存储介质。例如, 证书管理服务 (CMS) 可以针对证书创建请求选择合适的 CA (有时称为“发布”证书)。CMS 可以配置有基于请求中指示的一个或多个参数来管控 CA 的选择的一个或多个策略。在接收到来自请求者 (例如, 用户) 的请求时, CMS 可以标识适用于请求的一个或多个策略, 以及然后评估一个或多个策略以确定使用哪个 CA 来满足请求。

[0012] 在现代基于云的环境中, 可以存在多个 CA 并多个 CA 提供不同的服务。一些 CA 可以颁发公共证书 (例如, 用于在保护遍历诸如因特网的公共网络的通信或者与用户的组织之外的实体的通信中使用), 而其他 CA 可以颁发私有证书 (例如, 用于在保护私有网络上的组织内部云托管资源之间或者相关用户之间的通信中使用)。用户通常不知道将他们的证书相关请求定向到哪个 CA。例如, 当请求新证书时, 用户通常不知道证书必须从哪个 CA 颁发, 并且可能无意中从错误的 CA 获得证书。为了应对这些挑战, 特别地, 本文中描述的 CMS CA 选择简化了基于云的环境中用户的证书相关请求的过程。除了其他益处之外, CMS CA 选择还增加了用户可以获得新证书的速度, 减少了证书的发布中的错误, 并减轻了向用户通信传

送特定证书请求或特定类型证书请求的适当CA的管理负担。

[0013] 图1是示出根据一些实施方案的用于证书机构选择的环境的图。提供商网络100 (或“云”提供商网络) 为用户提供使用各种类型的计算相关资源中的一者或多者的能力, 所述计算相关资源诸如计算资源 (例如, 执行虚拟机 (VM) 实例和/或容器、执行批作业、执行代码而不预配置服务器)、数据/存储资源 (例如, 对象存储、块级存储、数据档案存储、数据库和数据库表等)、网络相关资源 (例如, 配置虚拟网络 (包括多组计算资源)、内容分发网络 (CDN)、域名服务 (DNS))、应用程序资源 (例如, 数据库、应用程序构建/部署服务)、访问策略或角色、身份策略或角色、机器图像、路由器以及其他数据处理资源等。这些和其他计算资源可作为服务提供, 所述服务诸如: 可执行计算实例的硬件虚拟化服务、可存储数据对象的存储服务等。提供商网络100的用户 (或“客户”) 可使用与客户账户相关联的一个或多个用户账户, 但可根据使用情境在一定程度上可互换地使用这些项。用户可以经由一个或多个接口108跨一个或多个中间网络104 (例如, 互联网) 与提供商网络100交互, 诸如通过使用应用编程接口 (API) 调用、经由被实施为网站或应用的控制台等。API是指客户端和服务端之间的接口和/或通信协议, 使得如果客户端发出预定义格式的请求, 则客户端应接收特定格式的响应或发起定义的动作。在云提供商网络场境中, API提供网关以通过允许客户从云提供商网络获得数据或在云提供商网络内引起动作来使客户访问云基础设施, 从而使得能够开发与托管在云提供商网络中的资源和服务交互的应用。API还可使云提供商网络的不同服务能够彼此交换数据。接口108可为提供商网络100的控制平面的一部分或充当控制平面的前端, 所述控制平面包括支持并实现可更直接地提供给客户的服务的“后端”服务。

[0014] 例如, 云提供商网络 (或仅称为“云”) 通常是指可访问的虚拟化计算资源 (诸如计算、存储和联网资源、应用以及服务) 的大型池。云可提供对可配置计算资源的共享池的方便、按需网络访问, 所述计算资源可响应于客户命令而以编程方式置配和发布。可动态地置配和重新配置这些资源以调节到可变负载。因此, 云计算可被认为是经由可公开访问的网络 (例如, 互联网、蜂窝通信网络) 作为服务交付的应用以及提供这些服务的云提供商数据中心中的硬件和软件两者。

[0015] 云提供商网络可被形成多个区域, 其中区域是云提供商将数据中心聚集在其中的地理区域。每个区域包括经由私有高速网络 (例如, 光纤通信连接) 彼此连接的多个 (例如, 两个或更多个) 可用区 (AZ)。AZ (也被称为“区”) 提供包括一个或多个数据中心设施的隔离式故障域, 所述一个或多个数据中心设施相对于另一个AZ中的数据中心设施具有单独的电源、单独的联网和单独的冷却。数据中心是指容纳云提供商网络的服务器并且为云提供商网络的服务器提供电源和冷却的物理建筑或外壳。优选地, 一个区域内的AZ被定位成彼此相距足够远, 使得自然灾害 (或其他导致故障的事件) 不会同时影响多于一个AZ或使多于一个AZ离线。

[0016] 用户可经由可公开访问的网络 (例如, 互联网、蜂窝通信网络), 例如通过转接中心 (TC) 连接到云提供商网络的AZ。TC是将用户链接到云提供商网络的主要主干位置并且可并置于其他网络提供商设施 (例如, 互联网服务提供商 (ISP)、电信提供商) 处并 (例如, 经由VPN或直接连接) 安全地连接到AZ。每个区域可操作两个或更多个TC以实现冗余。区域连接到全球网络, 所述全球网络包括将每个区域连接到至少一个其他区域的私有联网基础设施 (例如, 由云提供商控制的光纤连接)。云提供商网络可通过边缘位置和区域性边缘缓存服

务器从位于这些区域之外但与这些区域联网的接入点(或“POP”)递送内容。计算硬件的这种划分和地理分布使得云提供商网络能够在全局范围内以高度的容错性和稳定性为用户提供低延时的资源访问。

[0017] 一般来说,提供商网络的业务和操作可广泛地细分为两个类别:逻辑控制平面上承载的控制平面操作和逻辑数据平面上承载的数据平面操作。数据平面表示用户数据通过分布式计算系统的移动,而控制平面表示控制信号通过分布式计算系统的移动。控制平面通常包括跨一个或多个控制服务器分配并由一个或多个控制服务器实施的一个或多个控制平面组件。控制平面业务通常包括管理操作,诸如系统配置和管理(例如,资源放置、硬件容量管理、诊断监测、系统状态信息)。数据平面包括在提供商网络上实施的用户资源(例如,计算实例、容器、块存储卷、数据库、文件存储)。数据平面业务通常包括非管理操作,诸如将用户数据传送到用户资源以及从用户资源传送用户数据。控制平面组件通常在与数据平面服务器分开的一组服务器上实施,并且控制平面业务和数据平面业务可通过单独/不同的网络发送。

[0018] 为了提供这些和其他计算资源服务,提供商网络100通常依赖于虚拟化技术。例如,虚拟化技术可为用户提供控制或使用计算资源(例如,“计算实例”,诸如使用来宾操作系统(O/S)的VM,所述来宾操作系统使用可或不可进一步在底层主机O/S之上操作的管理程序来操作;可或不可在VM中操作的容器;可在没有底层管理程序的情况下在“裸金属”硬件上执行的计算实例)的能力,其中可使用单个电子装置来实施一个或多个计算资源。因此,用户可直接使用由提供商网络托管的计算资源(例如,由硬件虚拟化服务提供)来执行各种计算任务。另外地或替代地,用户可通过提交将由提供商网络执行的代码(例如,经由按需代码执行服务)来间接地使用计算资源,所述提供商网络进而使用一个或多个计算资源来执行代码,通常用户不具有对所涉及的底层计算实例的任何控制或知识。

[0019] 如上所讨论那样以及如现在图1中所示,本文中公开的实施方案包括针对证书请求选择合适的CA的提供商网络100的证书管理服务(CMS)114。如所示出那样,可以颁发证书的多个CA服务是可用的。特别地,CA 112A至112N包括提供商网络100外部的CA 112A和提供商网络100内部的CA 112B至112N。CA 112可以是公共或私有CA。公共CA颁发通常在公众可访问的网络(例如,因特网)上使用的证书,而私有CA颁发在私有网络(例如,私有公司内部网)中使用的证书。附加地,CA 112可以是云提供商的服务、云提供商和请求证书的用户的服务、或者由包括请求证书的用户的组织的管理员设置和配置的服务。

[0020] 用户可以使用CMS114来创建和管理证书相关的资源。各种请求类型包括证书创建、证书更新和证书删除。至少在证书创建和更新的情况下,因为特定请求可能调用多个CA中的一个,所以CMS可以通过接收请求并选择适当的CA来处理请求,而充当CA的接口。为了帮助处理CA选择,CMS可以配置有基于请求中指示的一个或多个参数来管控CA的选择的一个或多个策略。在接收到来自请求者(例如,用户)的请求时,CMS可以标识适用于请求的一个或多个策略,以及然后评估一个或多个策略以确定使用哪个CA来满足请求。

[0021] CA选择策略包括要应用于证书相关请求的一个或多个CA选择规则。CA选择策略可以与用户、角色、用户群等相关联。参考图3示出并描述了示例性CA选择策略。在较高层级下,CMS114使用CA选择策略来基于证书相关请求中包括的一个或多个参数来标识适当的CA。如所示出那样,CMS114在CA选择策略数据116中具有多个CA选择策略118A至118N。可以

由CMS114使用数据存储库(未示出)来存储和访问CA选择策略数据116。示例性数据存储装置是由诸如本文中别处所述的虚拟化数据存储服务提供的虚拟数据存储库。

[0022] 除了处理CA的选择之外,CMS114可以提供与创建、存储和更新用于保护用户的网站和应用的公共和私有证书(例如,SSL/TLS X.509证书)和密钥相关的许多其他特征。经由CMS114创建的证书可以保护单个域名、多个特定域名、通配符域或它们的组合。用户还可导出由CMS114管理的由私有证书机构签名的证书,以在用户内部PKI中的任何地方使用。

[0023] 如上文所指示,SSL/TLS证书允许web浏览器和其他应用程序标识网站并且使用SSL/TLS协议与网站建立加密的网络连接。证书在被称为公共密钥基础设施(PKI)的密码系统中使用。PKI为一方提供了使用证书来确认另一方身份的方法(如果双方都信任第三方的话),其中第三方被称为证书机构。

[0024] 在一些实施方案中,CMS114为期望部署受管理的证书相关资源的用户提供至少两种不同的选项。例如,CMS114可为需要使用TLS的安全web存在的用户提供公共证书管理服务。在一些实施方案中,由CMS114创建的证书相关资源可经由云提供商提供的其他服务(例如,经由负载平衡服务、内容分发网络(CDN)服务、API网关服务或用户可能已经部署端点资源的其他服务)部署到用户资源,或者以其他方式返回给请求用户。CMS114还可提供实现到期证书的自动更新的特征。

[0025] 在一些实施方案中,CMS114还提供私有证书机构服务。例如,私有证书机构服务可用于组织内的私人用途。在建立安全的加密通信信道时,每个端点使用证书和密码技术来向另一个端点证明其身份。内部API端点、web服务器、VPN用户、IoT装置和许多其他应用程序使用私有证书来建立其安全操作所需的加密通信信道。用户可创建其自身的证书机构(CA)层次结构并且用它颁发证书来对用户、计算机、应用程序、服务和其他装置进行验证。

[0026] 在一些实施方案中,由CMS114管理的证书相关资源与许多特性相关联。例如,在一些实施方案中,由CMS114颁发的证书是经过域验证的。由CMS114颁发的证书的主题字段标识域名,因此当用户请求证书时,用户会验证请求中指定的所有域的所有权或控制权。可通过使用电子邮件、DNS或CMS114所支持的其他方法来验证指定域的所有权或控制权。

[0027] 在一些实施方案中,由CA 112颁发的证书可与定义的有效期(例如,13个月或任何其他时间段)相关联。CMS114还可管理更新证书以及在所述证书更新之后预配置证书的过程。在一些实施方案中,由CA 112颁发的证书受到主流浏览器(Google Chrome、Microsoft Internet Explorer和Microsoft Edge、Mozilla Firefox等)和操作系统的信任。

[0028] 在一些实施方案中,每个CMS114证书包括至少一个完全合格域名(FQDN),并且用户可根据需要添加附加名称。例如,为www.example.com创建证书的用户还可添加名称www.example.net(如果用户使用任一名称进入站点的话)。CMS114还允许用户在域名中使用星号(*)来创建含有通配符名称的证书,所述证书可保护同一域中的若干站点。例如,*example.com保护www.example.com和images.example.com。在一些实施方案中,证书还指定算法和密钥长度。CMS114可例如支持若干公共密钥算法,包括但不限于:2048位RSA、4096位RSA、256位椭圆黄金曲线(Elliptic Prime Curve)、384位椭圆黄金曲线等。证书可与如本文所描述的其他参数相关联。

[0029] 如上所述,一个与证书相关的请求是新证书的创建(或发行)。现在参考圈出的数字1至5来描述CMS114的与证书的创建相关的示例性操作集合。

[0030] 在圆圈“1”,使用电子装置102A的用户使用由CMS114提供的API、基于网络的控制台、CLI或其他接口向CMS114发送针对新证书的请求126。请求通常包括用户的身份(或角色)的指示以及与所请求的证书相关联的域名的标识。用户的身份的指示可以是用户在向提供商网络100认证时获得的安全令牌或其他凭证。域名可以是完全合格的域名、子域、通配符域等(例如,*.`example.com`、`images.example.com`、*.`blog.example.com`等)。在一些实施方案中,域名是将使用证书来保护通信的实体的身份的某种其他指示。

[0031] 在圈“2”,CMS114通过使用请求中的用户的所指示的身份标识适用于请求的策略来处理请求。例如,CMS114可以确定任何CA选择策略118是否适用于与请求中指示的用户的身份相关联的用户账户、用户角色或用户群。在一些实施方案中,CMS114通过查询便于用户账户的创建和分组的组织服务(未示出)来确定与用户的身份相关联的角色和/或群。基于用户的身份、角色和/或群,CMS114标识适用的一个或多个CA选择策略118。CMS114然后使用请求中包括的域名来评估所标识的一个或多个CA选择策略118,以确定是否针对请求指定了CA。如果没有策略是适用的或者如果不存在适用策略中的规则,CMS114可以将请求定向到默认CA。

[0032] 在一些实施方案中,CMS114如下选择(或解析)适当的CA 112。首先,CMS114检查在请求126中是否指定了特定CA 112。如果在请求126中没有指定CA 112,CMS114可以检查一个或多个用户、角色和/或群策略是否适用于请求(通常从最特定到最不特定)。例如,CMS114可以检查用户级策略是否存在,并针对请求中标识的域名指定CA 112。如果不存在用户级策略、或者存在用户级策略但不适用于域名,则CMS114检查对于用户是否存在群级策略,并为针对请求中标识的域名指定CA 112。如果不存在群级策略、或者存在群级策略但不适用于域名,则CMS114检查是否针对用户的组织指定了默认CA。如果没有针对用户的组织指定默认CA,则针对全部未解决的请求,CMS114可以遵从默认CA。

[0033] 在一些实施方案中,CMS114在云提供商网络100的多个区域中具有足迹。此外,特定区域可能对CA具有不同的遵从要求,因此,例如,在“区域X”可用的CA可能在“区域Y”不可用。因此,CA选择策略数据116可以包括区域特定的策略(未示出)。当标识适用策略时,CMS114可以检查是否在具有区域特定的策略的区域中接收到请求。如果在具有区域特定的策略的区域中接收到请求,则CMS114可以从区域特定的策略中解析一个或多个适用策略。

[0034] 在圈“3”,CMS114至少部分地基于请求126向适当的CA 112(例如,默认CA、基于CA选择策略的标识和评估的CA、请求126中指定的CA等)发送证书发布请求128。在这个示例中,CMS114向CA 112C发送请求128并从CA 112C接收响应129。在圆圈“4”,CMS114从CA 112C接收证书发布响应129。响应129可以包括颁发的证书或对存储在证书数据存储库(未示出)中的所颁发的证书的引用。

[0035] 在圆圈“5”,CMS114至少部分地基于证书发布响应129向电子装置102A发送证书发布响应130。同样,响应130可以包括所颁发的证书或对存储在证书数据存储库(未示出)中的所颁发的证书的引用。

[0036] 在一些实施方案中,证书颁发请求和证书颁发响应可以分别源自和返回到提供商网络100内的电子装置102B。

[0037] 图2是示出根据一些实施方案的用于配置证书机构选择策略的环境的图。现在参考圈出的数字1至2来描述与CA选择策略的配置相关的CMS114的示例性操作集合。

[0038] 在圆圈“1”,诸如PKI管理员的用户使用电子装置202A向CMS 114发送请求226以配置CA选择策略118。例如,这样的用户可能负责或者另外地期望在组织内配置CA选择规则集合,以应用于组织的用户、角色和/或群。这种用户定义适用于群或角色的CA选择策略的能力减轻了组织内协调证书颁发的负担。

[0039] 在一些实施方案中,CA选择策略118的定义通常包括一个或多个规则以及策略适用的用户或用户群的标识。规则将域名或其他标识符与将与CA (例如,图1中的CA 112中的一个) 相关联的证书相关联。策略对特定用户或用户群的适用性的标识允许CMS114确定是否将策略作为证书相关请求的一部分进行评估。参考图3示出并描述了示例性CA选择策略。

[0040] 在一些实施方案中,将应用策略或规则的选定用户或角色可基于用户帐户、角色、用户群、组织或其他用户或角色分组的选择而选择,其中此类用户帐户、角色、用户群和组织可使用由云提供商网络100提供的身份和访问管理服务或使用由配置策略的组织控制的身份和访问管理系统来定义。

[0041] 示例性配置请求226包括创建新CA选择策略的请求、更新现有CA选择策略的请求以及删除CA选择策略的请求。创建新CA选择策略的请求通常包括一个或多个规则以及策略适用的用户或用户群的标识。更新现有CA选择策略的请求通常包括要更新的策略的标识(通常利用创建策略时返回的策略标识符标识、或者当用户列出现有策略时标识)以及对策略进行的任何更新。例如,更新可以采取对策略中指定的适用性或规则进行单独添加或删除的形式,或者采用新的适用性或规则来替换策略的现有适用性或规则。删除现有CA选择策略的请求通常包括要删除的策略的标识。

[0042] 在一些实施方案中,配置请求226通过由CMS114提供的API、基于网络的控制台、CLI或其他接口提交。例如,期望配置证书颁发策略的用户可登录到由CMS114提供的基于web的控制台,并且提供指示用户期望配置CA选择策略的输入。然后,基于web的控制台可提供请求用于配置策略的输入的一组指导性界面和界面元素。

[0043] 在圈“2”,CMS114处理请求226。例如,CMS114响应于策略创建请求创建新的CA选择策略、响应于策略删除请求删除现有的CA选择策略、或者响应于策略更新请求更新现有策略。CMS114可以存储新创建的证书、更新现有证书或从证书数据存储库(未示出)删除证书。在一些实施方案中,CMS114向配置请求226的发起者返回所创建、更新或删除的策略的标识。

[0044] 在一些实施方案中,策略配置请求可以源自提供商网络100内的电子装置102B。

[0045] 图3是示出根据一些实施方案的示例性证书机构选择策略300的图。如所示出那样,CA选择策略通常包括一个或多个规则以及策略适用的用户或用户群的标识。示例性CA选择策略300包括适用性301和规则302。在这个示例中,适用性301是针对群“DEV_TEAM”,因此与这个群相关联的用户可以具有由CMS114应用的CA选择策略300(例如,如果没有更特定的策略适用)。如所讨论的那样,在一些实施方案中,策略的适用性可以与作为与相应策略相关联的元数据的策略数据(例如,规则)分离地存储。

[0046] 规则302将域名或其他标识符303与CA 304(诸如CA 112)的标识符相关联。示例CA选择策略300包括四个规则。一个规则将域subramanian.com的子域与具有标识符“CA012”的CA相关联。另一规则将域hess.com的子域与具有标识符“CA345”的CA相关联。另一规则将域levy.com的子域与具有标识符“CA678”的CA相关联。另一规则将全部未指定(例如,默认)

的域与具有标识符“CA9AB”的CA相关联。CA标识符304(例如,“CA012”、“CA345”、“CA678”和“CA9AB”)可以直接或间接标识各种CA(例如,经由网络地址、别名、域名等)。

[0047] 例如,诸如CA选择策略118和300的CA选择策略可以被存储为包含策略中所包含的规则的结构化表示(例如,JSON格式)以及可能的策略的适用性的文本文档或其他数据结构。例如,每个策略和/或规则可以被指定并存储在标识策略或规则适用的一个或多个用户或群以及一个或多个规则的结构化表示中。如本文所述,特定CA选择策略的适用性可以与策略一起存储,或者作为与策略本身分离的元数据存储。对于每个策略,关于CA选择策略数据中的策略的这种元数据可以包括策略的标识符和这个策略的适用性。CMS114可以评估策略适用性元数据,以确定是否有任何策略适用于给定的证书相关请求。

[0048] 图4是示出根据一些实施方案的在其中选择不同证书机构的环境的图。如所示出那样,云提供商网络100包括两个CA——表示为“CA_A”的公共CA 412A和表示为“CA_B”的私有CA 412B。CA选择策略数据416包括与用户相关联的CA选择策略418A、与包括用户的群相关联的CA选择策略418B以及默认CA策略420。CA选择策略418A包括指示与subramanian.com的子域相关联的证书请求将通过CA_A(CA 412A)处理的规则。CA选择策略418B包括指示与hess.com的子域相关联的证书请求将通过CA_B(CA 412B)处理的规则。并且默认CA 420标识CA_A(CA 412A)。

[0049] 在这个示例中,由电子装置402的用户通过一个或多个中间网络104(例如,互联网)经由到云提供商网络100的一个或多个接口108向CMS114提交三个证书创建请求。参考圈出的1A至3A描述与第一请求相关联的操作;参考圈出的1B至3B描述与第二请求相关的操作;并且参考圈出的1C至3C来描述与第三请求相关联的操作。

[0050] 在第一证书创建请求中,在圆圈“1A”处,使用电子装置402的用户向CMS114发送对新证书的请求。请求包括用户的身份的指示。在这个示例中,我们假设用户的身份是“用户A”。请求还包括要为其创建证书(blog.subramanian.com)的域名。在圆圈“2A”,CMS114标识CA选择策略418A与用户A相关联(例如,基于所包括的适用性数据或其他元数据)。CMS114然后使用请求的内容评估策略。在此,CA选择策略418A包括指示用于subramanian.com的子域的证书将通过CA_A(CA 412A)颁发的规则。在圆圈“3A”,CMS114向所标识的CA(CA_A)发送请求。然后,发布响应(无论是证书还是对证书的引用)经由CMS114从CA 412A发送回到电子装置402。

[0051] 在第二证书创建请求中,在圆圈“1B”处,使用电子装置402的用户向CMS114发送对新证书的请求。再次,请求包括用户(用户A)的身份的指示。请求还包括要为其创建证书(docs.hess.com)的域名。在圆圈“2B”,CMS114首先标识并检查与用户A相关联的CA选择策略418A,并确定CA策略418A不具有适用于hess.com域的规则。CMS114还标识适用于包括所标识的用户的群或角色的群(或角色)CA选择策略418B。在此,群CA选择策略418B包括指示用于hess.com的子域的证书将通过CA_B(CA 412B)颁发的规则。在圆圈“3B”处,CMS114向所标识的CA(CA_B)发送请求。然后,发布响应(无论是证书还是对证书的引用)经由CMS114从CA 412B发送回到电子装置402。

[0052] 在第三证书创建请求中,在圆圈“1C”处,使用电子装置402的用户向CMS114发送对新证书的请求。再次,请求包括用户(用户A)的身份的指示。请求还包括要为其创建证书(images.levy.com)的域名。在圆圈“2C”,CMS114首先标识并检查与用户A相关联的CA选择

策略418A,并确定CA策略418A不具有适用于levy.com域的规则。CMS114还标识适用于包括所标识的用户的群或角色的群(或角色)CA选择策略418B,并确定CA策略418B也不具有适用于levy.com域的规则。CMS114具有指示不通过其他策略处理的请求将通过CA_A(CA 412A)颁发的默认CA策略420。在圆圈“3C”,CMS114向所标识的默认CA(CA_A)发送请求。然后,发布响应(无论是证书还是对证书的引用)经由CMS114从CA 412A发送回到电子装置402。

[0053] 图5是示出根据一些实施方案的用于证书机构选择的方法的操作500的流程图。操作500(或本文描述的其他过程、或变型和/或其组合)中的一些或全部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并且被实施为共同在一个或多个处理器上执行的代码(例如,可执行指令、一个或多个计算机程序或一个或多个应用)。代码例如以包括可由一个或多个处理器执行的指令的计算机程序的形式存储在计算机可读存储介质上。计算机可读存储介质是非暂时性的。在一些实施方案中,操作500中的一个或多个(或全部)由其他图的CMS114执行。

[0054] 操作500包括,在框502,从电子装置并通过云提供商网络的证书管理服务接收生成证书的第一请求,其中第一请求包括用户的身份的指示和要与证书相关联的域名的标识。

[0055] 操作500还包括,在框504,标识适用于第一请求的第一证书机构选择策略,其中第一证书机构选择策略包括证书机构选择规则。

[0056] 操作500还包括,在框506,评估证书机构选择规则以标识用以生成证书的证书机构,其中证书机构选择规则将域名的至少一部分与证书机构相关联。

[0057] 操作500还包括,在框508,向证书机构发送生成证书的第二请求。

[0058] 操作500还包括,在框510,将证书或证书的标识从证书授权机构返回到电子装置。

[0059] 在一些实施方案中,第一请求不包括任何证书机构的标识。

[0060] 在一些实施方案中,在评估证书机构选择规则之前,标识适用于第一请求的第二证书机构选择策略,并且确定第二证书机构选择策略不包括与域名相关联的规则。在这种情况下,例如,第一证书机构选择策略可以与包括用户的身份的群相关联,并且第二证书机构选择策略可以与用户的身份相关联。

[0061] 在一些实施方案中,CMS接收创建第一证书机构选择策略的第三请求,其中第三请求包括(a)域名的至少一部分与证书机构的关联,以及(b)将第一证书机构选择策略与(i)用户的身份、(ii)与用户的身份相关联的角色、或(iii)包括用户的身份的群中的至少一者相关联的策略适用性,并且CMS将第一证书机构选择策略存储在数据存储库中。策略适用性可以存储在与第一证书机构选择策略相关联的元数据中,或者被存储为第一证书机构选择策略的一部分。

[0062] 在一些实施方案中,证书机构是(a)被配置为用于由包括用户的组织的管理员使用的私有证书机构服务、或者(b)公共证书机构,其中公共证书机构是云提供商网络或第三方的服务。

[0063] 在一些实施方案中,第一证书机构选择策略通过以下各项中的至少一项而适用于第一请求:(a)第一证书机构选择策略与用户的身份相关联、(b)第一证书机构选择策略与和用户的身份相关联的角色相关联、(c)第一证书机构选择策略与包括用户的身份的群相关联、或者(d)第一证书机构选择策略是默认策略。

[0064] 在一些实施方案中,第一证书机构选择策略与地理区域相关联,并且其中第一证书机构选择策略至少部分地基于由地理区域中的证书管理服务接收到第一请求而适用于第一请求。

[0065] 在一些实施方案中,证书机构是用户可用的多个证书机构中的一个证书机构。

[0066] 图6示出根据一些实施方案的示例性提供商网络(或“服务提供商系统”)环境。提供商网络600可经由一个或多个虚拟化服务610向客户提供资源虚拟化,所述一个或多个虚拟化服务允许客户购买、租借或以其他方式获得在一个或多个数据中心中的一个或多个提供商网络内的装置上实施的虚拟化资源(包括但不限于计算资源和存储资源)的实例612。本地互联网协议(IP)地址616可与资源实例612相关联;本地IP地址是提供商网络600上的资源实例612的内部网络地址。在一些实施方案中,提供商网络600还可提供客户可从提供商600获得的公共IP地址614和/或公共IP地址范围(例如,互联网协议版本4(IPv4)或互联网协议版本6(IPv6)地址)。

[0067] 常规上,提供商网络600可经由虚拟化服务610允许服务提供商的客户(例如,操作包括一个或多个客户装置652的一个或多个客户网络650A至650C(或“客户端网络”)的客户)使分派或分配给客户的至少一些公共IP地址614与分派给客户的特定资源实例612动态地相关联。提供商网络600还可允许客户将先前映射到分派给客户的一个虚拟化计算资源实例612的公共IP地址614重新映射到也分派给客户的另一虚拟化计算资源实例612。使用由服务提供商提供的虚拟化计算资源实例612和公共IP地址614,服务提供商的客户,诸如客户网络650A至650C的运营商可例如实施客户特定的应用并且在中间网络640(诸如互联网)上呈现客户的应用程序。然后,中间网络640上的其他网络实体620可以生成到由客户网络650A至650C发布的目的地公共IP地址614的流量;流量被路由到服务提供商数据中心,并且在数据中心处经由网络基板被路由到当前映射到目的地公共IP地址614的虚拟化计算资源实例612的本地IP地址616。类似地,来自虚拟化计算资源实例612的响应流量可经由网络基板被路由回到中间网络640上到源实体620。

[0068] 如本文所用的本地IP地址是指例如提供商网络中的资源实例的内部或“私有”网络地址。本地IP地址可在由互联网工程任务组(IETF)的注释请求(RFC)1918保留的地址块内和/或具有由IETF RFC 4193指定的地址格式,并且可在提供商网络内是可变的。源自提供商网络之外的网络流量并不直接路由到本地IP地址;而是,流量使用映射到资源实例的本地IP地址的公共IP地址。提供商网络可包括提供网络地址转换(NAT)或类似功能以执行从公共IP地址到本地IP地址以及从本地IP地址到公共IP地址的映射的联网装置或设备。

[0069] 公共IP地址是由服务提供商或客户分派给资源实例的互联网可变网络地址。例如经由1:1NAT转换路由到公共IP地址的流量,并且将流量转发到资源实例的相应本地IP地址。

[0070] 一些公共IP地址可由提供商网络基础设施分派给特定资源实例;这些公共IP地址可被称为标准公共IP地址,或简称为标准IP地址。在一些实施方案中,标准IP地址到资源实例的本地IP地址的映射是所有资源实例类型的默认启动配置。

[0071] 至少一些公共IP地址可被分配给提供商网络600的客户或由提供商网络的客户获得;然后,客户可将其被分配的公共IP地址分派给分配给客户的特定资源实例。这些公共IP地址可被称为客户公共IP地址,或简称为客户IP地址。并不是像在标准IP地址的情况中那

样由提供商网络600分派给资源实例,而是可由客户例如经由服务提供商提供的API将客户IP地址分派给资源实例。与标准IP地址不同,客户IP地址被分配给客户账户,并且可根据需要或期望由相应客户重新映射到其他资源实例。客户IP地址与客户账户而非特定资源实例相关联,并且客户控制该IP地址直到客户选择释放所述IP地址。与常规的静态IP地址不同,客户IP地址允许客户通过将客户的公共IP地址重新映射到与客户账户相关联的任何资源实例来掩盖资源实例或可用区故障。例如,客户IP地址使得客户能够通过将客户IP地址重新映射到替代资源实例来解决客户的资源实例或软件的问题。

[0072] 图7是根据一些实施方案的向客户提供存储服务和硬件虚拟化服务的示例提供商网络环境的框图。硬件虚拟化服务720向客户提供多个计算资源724(例如,诸如VM的计算实例725)。计算资源724可例如作为服务提供给提供商网络700的客户(例如,实施客户网络750的客户)。每个计算资源724可设有一个或多个本地IP地址。提供商网络700可被配置为将分组从计算资源724的本地IP地址路由到公共互联网目的地以及将分组从公共互联网源路由到计算资源724的本地IP地址。

[0073] 提供商网络700可为例如经由本地网络756耦合到中间网络740的客户网络750提供经由耦合到中间网络740和提供商网络700的硬件虚拟化服务720实施虚拟计算系统792的能力。在一些实施方案中,硬件虚拟化服务720可提供一个或多个API 702,例如web服务接口,经由所述一个或多个API,客户网络750可例如经由客户装置790的控制台794(例如,基于web的应用、独立应用、移动应用等)访问硬件虚拟化服务720提供的功能。在一些实施方案中,在提供商网络700处,客户网络750处的每个虚拟计算系统792可对应于被租赁、租借或以其他方式提供给客户网络750的计算资源724。

[0074] 从虚拟计算系统792和/或另一客户装置790(例如,经由控制台794)的实例,客户可例如经由一个或多个API 702访问存储服务710的功能,以从提供商网络700所提供的虚拟数据存储库716(例如,文件夹或“桶”、虚拟化卷、数据库等)的存储资源718A至718N访问数据以及将数据存储到所述存储资源。在一些实施方案中,虚拟化数据存储网关(未示出)可设置在客户网络750处,该虚拟化数据存储网关可在本地缓存至少一些数据(例如频繁访问的数据或关键数据)并且可经由一个或多个通信信道与存储服务710通信以从本地缓存上传新的或修改后的数据,使得维护主数据存储库(虚拟化数据存储库716)。在一些实施方案中,用户经由虚拟计算系统792和/或另一个客户装置790可经由充当存储虚拟化服务的存储服务710安装并访问虚拟数据存储库716的卷,并且这些卷在用户看来可以是本地(虚拟化)存储798。

[0075] 虽然图7中未示出,但还可经由API 702从提供商网络700内的资源实例访问虚拟化服务。例如,客户、设备服务提供商或其他实体可经由API 702从提供商网络700上的相应虚拟网络之内访问虚拟化服务,以请求分配所述虚拟网络内或另一个虚拟网络内的一个或多个资源实例。

[0076] 说明性系统

[0077] 在一些实施方案中,实施本文描述的技术的一部分或全部的系统可包括通用计算机系统(诸如图8所示的计算机系统800),所述通用计算机系统包括或被配置为访问一个或多个计算机可访问介质。在所示的实施方案中,计算机系统800包括经由输入/输出(I/O)接口830耦合到系统存储器820的一个或多个处理器810。计算机系统800还包括耦合到I/O接

口830的网络接口840。虽然图8将计算机系统800示出为单个计算装置,但在各种实施方案中,计算机系统800可包括一个计算装置或被配置为作为单个计算机系统800一起工作的任何数量的计算装置。

[0078] 在各种实施方案中,计算机系统800可为包括一个处理器810的单处理器系统或包括若干处理器810(例如,两个、四个、八个或另一合适数量)的多处理器系统。处理器810可为能够执行指令的任何合适的处理器。例如,在各种实施方案中,处理器810可为实施多种指令集架构(ISA)中的任何一种(诸如,x86、ARM、PowerPC、SPARC、或MIPS ISA或任何其他合适的ISA)的通用或嵌入式处理器。在多处理器系统中,处理器810中的每一者通常可但未必实施相同的ISA。

[0079] 系统存储器820可存储可由处理器810访问的指令和数据。在各种实施方案中,系统存储器820可使用任何合适的存储器技术来实施,诸如随机存取存储器(RAM)、静态RAM(SRAM)、同步动态RAM(SDRAM)、非易失性/闪存型存储器或任何其他类型的存储器。在所示的实施方案中,实现一个或多个期望功能的程序指令和数据(诸如上述的那些方法、技术和数据)被示出为作为CMS代码825(例如,可执行以全部或部分实现CMS114)和数据826(诸如CA选择策略数据116、416)存储在系统存储器820内。

[0080] 在一些实施方案中,I/O接口830可被配置为协调处理器810、系统存储器820和装置中的任何外围装置(包括网络接口840和/或其他外围接口(未示出))之间的I/O流量。在一些实施方案中,I/O接口830可执行任何必要的协议、时序或其他数据变换以将来自一个组件(例如,系统存储器820)的数据信号转换成合适于由另一个组件(例如,处理器810)使用的格式。在一些实施方案中,例如,I/O接口830可包括支持通过各种类型的外围总线(诸如,外围组件互连(PCI)总线标准或通用串行总线(USB)标准的变体)附接的装置。在一些实施方案中,例如,I/O接口830的功能可被拆分成两个或更多个单独的组件,诸如北桥和南桥。另外,在一些实施方案中,I/O接口830(诸如到系统存储器820的接口)的功能中的一些或全部可直接并入处理器810中。

[0081] 例如,网络接口840可被配置为允许在计算机系统800与附接到一个或多个网络850的其他装置860(诸如,如图1所示的其他计算机系统或装置)之间交换数据。在各种实施方案中,例如,网络接口840可支持经由任何合适的有线或无线通用数据网络(诸如各种类型的以太网网络)进行通信。另外,网络接口840可支持经由电信/电话网络(诸如模拟语音网络或数字光纤通信网络)、经由存储区域网(SAN)(诸如光纤信道SAN)和/或经由任何其他合适类型的网络和/或协议进行通信。

[0082] 在一些实施方案中,计算机系统800包括一个或多个卸载卡870A或870B(包括一个或多个处理器875,并且可能包括一个或多个网络接口840),所述一个或多个卸载卡使用I/O接口830(例如,实施外围部件互连快速(PCI-E)标准的版本或诸如快速路径互连(QPI)或超路径互连(UPI)的另一互连的总线)来连接。例如,在一些实施方案中,计算机系统800可充当托管诸如计算实例的计算资源的主机电子装置(例如,作为硬件虚拟化服务的一部分操作),并且一个或多个卸载卡870A或870B执行可管理在主机电子装置上执行的计算实例的虚拟化管理器。作为示例,在一些实施方案中,一个或多个卸载卡870A或870B可执行计算实例管理操作,诸如暂停和/或取消暂停计算实例、启动和/或终止计算实例、执行存储器转移/复制操作等。在一些实施方案中,这些管理操作可由一个或多个卸载卡870A或870B与由

计算机系统800的其他处理器810A至810N执行的管理程序(例如,根据来自管理程序的请求)协作来执行。然而,在一些实施方案中,由卸载卡870A或870B实施的虚拟化管理器可适应来自其他实体(例如,来自计算实例本身)的请求,并且可不与任何单独的管理程序协作(或不服务于任何单独的管理程序)。

[0083] 在一些实施方案中,系统存储器820可为被配置为存储如上文所描述的程序指令和数据的计算机可访问介质的一个实施方案。然而,在其他实施方案中,可在不同类型的计算机可访问介质上接收、发送、或存储程序指令和/或数据。一般来说,计算机可访问介质可包括任何非暂时性存储介质或存储器介质,诸如磁性或光学介质,例如经由I/O接口830耦合到计算机系统800的磁盘或DVD/CD。非暂时性计算机可访问存储介质还可包括可包括在计算机系统800的一些实施方案中作为系统存储器820或另一种类型的存储器的任何易失性或非易失性介质,诸如RAM(例如,SDRAM、双倍数据速率(DDR) SDRAM、SRAM等)、只读存储器(ROM)等。此外,计算机可访问介质可包括传输介质或经由通信介质(诸如网络和/或无线链路)传送的信号,诸如电信号、电磁信号或数字信号,所述通信介质诸如可经由网络接口840来实施。

[0084] 本文所讨论或提出的各种实施方案可在各种各样的操作环境中实施,在一些情况下,所述操作环境可包括可用于操作许多应用中的任一个的一个或多个用户计算机、计算装置或处理装置。用户装置或客户端装置可包括许多通用个人计算机中的任一个,诸如运行标准操作系统的台式计算机或膝上型计算机,以及运行移动软件并能够支持许多联网和消息传递协议的蜂窝装置、无线装置和手持式装置。这种系统还可包括许多工作站,所述工作站运行各种可商购获得的操作系统和用于诸如开发和数据库管理等目的的其他已知应用中的任一个。这些装置还可包括其他电子装置,诸如虚设终端、瘦客户端、游戏系统和/或能够经由网络进行通信的其他装置。

[0085] 大多数实施方案使用本领域技术人员熟悉的至少一个网络来支持使用各种广泛可用协议中的任一种进行通信,所述协议诸如为传输控制协议/互联网协议(TCP/IP)、文件传送协议(FTP)、通用随插即用(UPnP)、网络文件系统(NFS)、公共互联网文件系统(CIFS)、可扩展消息传递和现场协议(XMPP)、AppleTalk等。网络可包括例如局域网(LAN)、广域网(WAN)、虚拟专用网(VPN)、互联网、内联网、外联网、公共交换电话网(PSTN)、红外网络、无线网络以及其任何组合。

[0086] 在使用web服务器的实施方案中,web服务器可运行各种服务器或中间层应用中的任一种,包括HTTP服务器、文件传送协议(FTP)服务器、通用网关接口(CGI)服务器、数据服务器、Java服务器、业务应用服务器等。服务器还可能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以任何编程语言(诸如Java®、C、C#或C++)或任何脚本语言(诸如Perl、Python、PHP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,包括但不限于可从Oracle(R)、Microsoft(R)、Sybase(R)、IBM(R)等商购获得的数据库服务器。数据库服务器可为关系型或非关系型(例如,“NoSQL”)、分布式或非分布式等。

[0087] 本文公开的环境可包括各种数据存储库以及如上文所讨论的其他存储器和存储介质。这些可驻留在各种位置中,诸如驻留在一个或多个计算机本地(和/或驻留在其中)的存储介质上,或驻留在远离网络上的任何或所有计算机的存储介质上。在一组特定的实施

方案中,信息可驻留在本领域技术人员熟悉的存储区域网(SAN)中。类似地,用于执行归属于计算机、服务器或其他网络装置的功能的任何必要的文件可视情况本地和/或远程地存储。在系统包括计算机化装置的情况下,每个这种装置可包括可经由总线电耦合的硬件元件,所述元件包括例如至少一个中央处理单元(CPU)、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/或至少一个输出装置(例如,显示装置、打印机或扬声器)。这种系统还可包括一个或多个存储装置,诸如盘驱动器、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、闪存卡等。

[0088] 此类装置还可包括计算机可读存储介质读取器、通信装置(例如,调制解调器、网卡(无线或有线)、红外通信装置等)和如上文所描述的工作存储器。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为接纳计算机可读存储介质,所述计算机可读存储介质表示用于暂时地和/或更长久地容纳、存储、传输和检索计算机可读信息的远程、本地、固定和/或可移动的存储装置以及存储介质。所述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许多软件应用、模块、服务或其他元件,包括操作系统和应用程序,诸如客户端应用或web浏览器。应当了解,替代实施方案可具有与上文描述不同的许多变型。例如,也可使用定制硬件,和/或特定元件可在硬件、软件(包括可移植软件,诸如小程序)或两者中实施。此外,可采用与其他计算装置(诸如网络输入/输出装置)的连接。

[0089] 用于容纳代码或代码部分的存储介质和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,诸如但不限于以任何方法或技术实施来存储和/或传输信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的易失性和非易失性介质、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)、闪存存储器或其他存储器技术、光盘-只读存储器(CD-ROM)、数字通用盘(DVD)或其他光学存储装置、磁带盒、磁带、磁盘存储装置或其他磁性存储装置或可用于存储期望的信息并可由系统装置访问的任何其他介质。基于本公开和本文提供的教义,本领域的普通技术人员将了解实施各种实施方案的其他方式和/或方法。

[0090] 在前述描述中,描述了各种实施方案。出于解释目的,阐述了具体配置和细节以便提供对实施方案的透彻理解。然而,本领域技术人员还将显而易见的是,可在没有这些具体细节的情况下实践实施方案。此外,为了不使所描述的实施方案变得模糊,可省略或简化熟知的特征。

[0091] 在本文中使用带括号的文本以及带有虚线边框(例如,大破折号、小破折号、点破折号和点)的框来说明向一些实施方案添加附加特征的可选方面。然而,这种表示法不应被视为意味着这些是仅有的选项或可选操作,和/或在某些实施方案中,带有实线边框的框不是可选的。

[0092] 具有后缀字母的附图标记(例如,718A-718N)可用于指示各种实施方案中可存在所提及实体的一个或多个实例,并且当存在多个实例时,每个实例无需相同,而是可共有一些一般特点或以常见的形式发挥作用。此外,所使用的特定后缀不意味着暗示存在特定数量的实体,除非有相反的具体指示。因此,在各种实施方案中,使用相同或不同后缀字母的两个实体可以具有或不具有相同数量的实例。

[0093] 提及“一个实施方案”、“实施方案”、“示例实施方案”等指示所描述的实施方案可包括特定特征、结构或特性,但每个实施方案可能不一定包括所述特定特征、结构或特性。

此外,此类短语不一定是指同一个实施方案。此外,当结合实施方案来描述特定特征、结构或特性时,应认为,无论是否明确描述,结合其他实施方案来实现此类特征、结构或特性也在本领域技术人员知识范围内。

[0094] 此外,在上文描述的各种实施方案中,除非另有特别指明,否则诸如短语“A、B或C中的至少一者”的析取语言意图被理解为意指A、B或C或其任何组合(例如,A、B和/或C)。类似地,诸如“A、B和C中的至少一者或多者”(或“A、B和C中的一者或多者”)的语言意图被理解为意指A、B或C,或其任何组合(例如,A、B和/或C)。因此,析取语言既不意图也不应被理解为暗示给定实施方案要求A中的至少一者、B中的至少一者和C中的至少一者各自都存在。

[0095] 如本文所用,术语“基于”(或类似)是开放式术语,用于描述影响确定或其他行动的一个或多个因素。应当理解,该术语并不排除可能影响确定或行动的附加因素。例如,确定可能仅基于列出的因素或基于所述因素和一个或多个附加因素。因此,如果行动A“基于”B,则应当理解B是影响行动A的一个因素,但这并不排除所述行动也基于一个或多个其他因素,诸如因素C。然而,在一些情况下,行动A可完全基于B。

[0096] 除非另有明确陈述,否则诸如“一个(a/an)”等冠词通常应被解释为包括一个或多个所描述的项。因此,诸如“被配置为……的装置”或“计算装置”等短语意图包括一个或多个表述的装置。这一个或多个表述的装置可共同被配置为执行所陈述的操作。例如,“被配置为执行操作A、B和C的处理器”可包括被配置为执行操作A的第一处理器与被配置为执行操作B和C的第二处理器一起工作。

[0097] 此外,词语“可”或“可以”是以许可意义(即,意指具有某种可能)来使用,而不是以强制意义(即,意指必须)来使用。词语“包括(include)”、“包括(including)”和“包括(includes)”用于指示开放式关系,并且因此意味着包括但不限于。类似地,词语“具有(have)”、“具有(having)”和“具有(has)”也指示开放式关系,并且因此意味着具有但不限于。本文中使用的术语“第一”、“第二”、“第三”等用作跟在它们后面的名词的标签,并且不暗示任何类型的顺序(例如,空间、时间、逻辑等),除非另外明确指出此类顺序。

[0098] 可鉴于以下条款来描述所公开技术的至少一些实施方案:

[0099] 1. 一种计算机实现的方法,其包括:

[0100] 由云提供商网络的证书管理服务接收创建第一证书机构选择策略的第一请求,其中第一请求包括:(a)第一域名与证书机构的关联,以及(b)将第一证书机构选择策略与以下至少一者相关联的策略适用性:(i)用户的身份、(ii)与用户的身份相关联的角色、或(iii)包括用户的身份的群;

[0101] 将第一证书机构选择策略和策略适用性存储在数据存储库中,其中第一证书机构选择策略包括将第一域名与证书机构相关联的证书机构选择规则;

[0102] 从电子装置并且由证书管理服务接收生成证书的第二请求,其中第二请求包括用户的身份的指示和要与证书相关联的第二域名的标识;

[0103] 至少部分基于策略适用性来标识适用于第二请求的第一证书机构选择策略;

[0104] 至少部分基于第二域名是第一域名的子域,评估证书机构选择规则以标识证书机构;

[0105] 向证书机构发送生成证书的第三请求;以及

[0106] 从证书机构向电子装置返回证书或证书的标识。

- [0107] 2.如条款1所述的计算机实现的方法,其中第二请求不包括任何证书机构的标识。
- [0108] 3.如条款1-2中任一项所述的计算机实现的方法,其还包括:
- [0109] 在评估证书机构选择规则之前:
- [0110] 标识适用于第一请求的第二证书机构选择策略;以及
- [0111] 确定第二证书机构选择策略不包括与第二域名相关联的规则。
- [0112] 4.一种计算机实现的方法,其包括:
- [0113] 从电子装置并通过云提供商网络的证书管理服务接收生成证书的第一请求,其中第一请求包括用户的身份的指示和要与证书相关联的域名的标识;
- [0114] 标识适用于第一请求的第一证书机构选择策略,其中第一证书机构选择策略包括证书机构选择规则;
- [0115] 评估证书机构选择规则以标识用以生成证书的证书机构,其中证书机构选择规则将域名的至少一部分与证书机构相关联;
- [0116] 向证书机构发送生成证书的第二请求;以及
- [0117] 从证书机构向电子装置返回证书或证书的标识。
- [0118] 5.如条款4所述的计算机实现的方法,其中第一请求不包括任何证书机构的标识。
- [0119] 6.如条款4-5中任一项所述的计算机实现的方法,其还包括:
- [0120] 在评估证书机构选择规则之前:
- [0121] 标识适用于第一请求的第二证书机构选择策略;以及
- [0122] 确定第二证书机构选择策略不包括与域名相关联的规则。
- [0123] 7.如条款6所述的计算机实现的方法,其中第一证书机构选择策略与包括用户的身份的群相关联,并且第二证书机构选择策略与用户的身份相关联。
- [0124] 8.如条款4-7中任一项所述的计算机实现的方法,其还包括:
- [0125] 由证书管理服务接收创建第一证书机构选择策略的第三请求,其中第三请求包括(a)域名的至少一部分与证书机构的关联,以及(b)将第一证书机构选择策略与以下至少一者相关联的策略适用性:(i)用户的身份、(ii)与用户的身份相关联的角色、或(iii)包括用户的身份的群中;以及
- [0126] 将第一证书机构选择策略存储在数据存储库中。
- [0127] 9.如条款8所述的计算机实现的方法,其中策略适用性存储在与第一证书机构选择策略相关联的元数据中。
- [0128] 10.如条款4-9中任一项所述的计算机实现的方法,其中证书机构是(a)被配置为用于由包括用户的组织的管理员使用的私有证书机构服务、或者(b)公共证书机构,其中公共证书机构是云提供商网络或第三方的服务。
- [0129] 11.如条款4-10中任一项所述的计算机实现的方法,其中第一证书机构选择策略通过以下各项中的至少一项而适用于第一请求:(a)第一证书机构选择策略与用户的身份相关联、(b)第一证书机构选择策略与和用户的身份相关联的角色相关联、(c)第一证书机构选择策略与包括用户的身份的群相关联、或者(d)第一证书机构选择策略是默认策略。
- [0130] 12.如条款11所述的计算机实现的方法,其中第一证书机构选择策略与地理区域相关联,并且其中第一证书机构选择策略还至少部分地基于由地理区域中的证书管理服务接收到第一请求而适用于第一请求。

[0131] 13.如条款4-12中任一项所述的计算机实现的方法,其中证书机构是用户可用的多个证书机构中的一个证书机构。

[0132] 14.一种系统,其包括:

[0133] 第一个或多个电子装置,用于实现云提供商网络的数据存储服务,数据存储服务包括在执行时使得数据存储服务存储证书机构选择策略数据的指令;以及

[0134] 第二个或多个电子装置,用于实现云提供商网络的证书管理服务,证书管理服务包括在执行时使得证书管理服务进行以下操作的指令:

[0135] 从第三电子装置接收生成证书的第一请求,其中第一请求包括用户的身份的指示和要与证书相关联的域名的标识;

[0136] 标识适用于第一请求且在证书机构选择策略数据中的第一证书机构选择策略,其中第一证书机构选择策略包括证书机构选择规则;

[0137] 评估证书机构选择规则以标识用以生成证书的证书机构,其中证书机构选择规则将域名的至少一部分与证书机构相关联;

[0138] 向证书机构发送生成证书的第二请求;以及

[0139] 从证书机构向第三电子装置返回证书或证书的标识。

[0140] 15.如条款14所述的系统,其中第一请求不包括任何证书机构的标识。

[0141] 16.如条款14-15中任一项所述的系统,证书管理服务包括在执行时使得证书管理服务进行以下操作的另外的指令:

[0142] 在评估证书机构选择规则之前:

[0143] 标识适用于第一请求的第二证书机构选择策略;以及

[0144] 确定第二证书机构选择策略不包括与域名相关联的规则。

[0145] 17.如条款16所述的系统,其中第一证书机构选择策略与包括用户的身份的群相关联,并且第二证书机构选择策略与用户的身份相关联。

[0146] 18.如条款14-17中任一项所述的系统,证书管理服务包括在执行时使得证书管理服务进行以下操作的另外的指令:

[0147] 接收创建第一证书机构选择策略的第三请求,其中第三请求包括(a)域名的至少一部分与证书机构的关联,以及(b)将第一证书机构选择策略与以下至少一者相关联的策略适用性:(i)用户的身份、(ii)与用户的身份相关联的角色、或(iii)包括用户的身份的群;以及

[0148] 将第一证书机构选择策略存储在证书机构选择策略数据中。

[0149] 19.如条款18所述的系统,其中策略适用性作为元数据存储在证书机构选择策略数据中,并且与第一证书机构选择策略相关联。

[0150] 20.如条款14-19中任一项所述的系统,其中证书机构是(a)被配置为用于由包括用户的组织的管理员使用的私有证书机构服务、或者(b)公共证书机构,其中公共证书机构是云提供商网络或第三方的服务。

[0151] 说明书和附图因此应被视为具有说明性而非限制性意义。然而,将明显的是,在不脱离如在权利要求中所阐述的本公开的更广泛的精神和范围的情况下,可对此进行各种修改和变更。

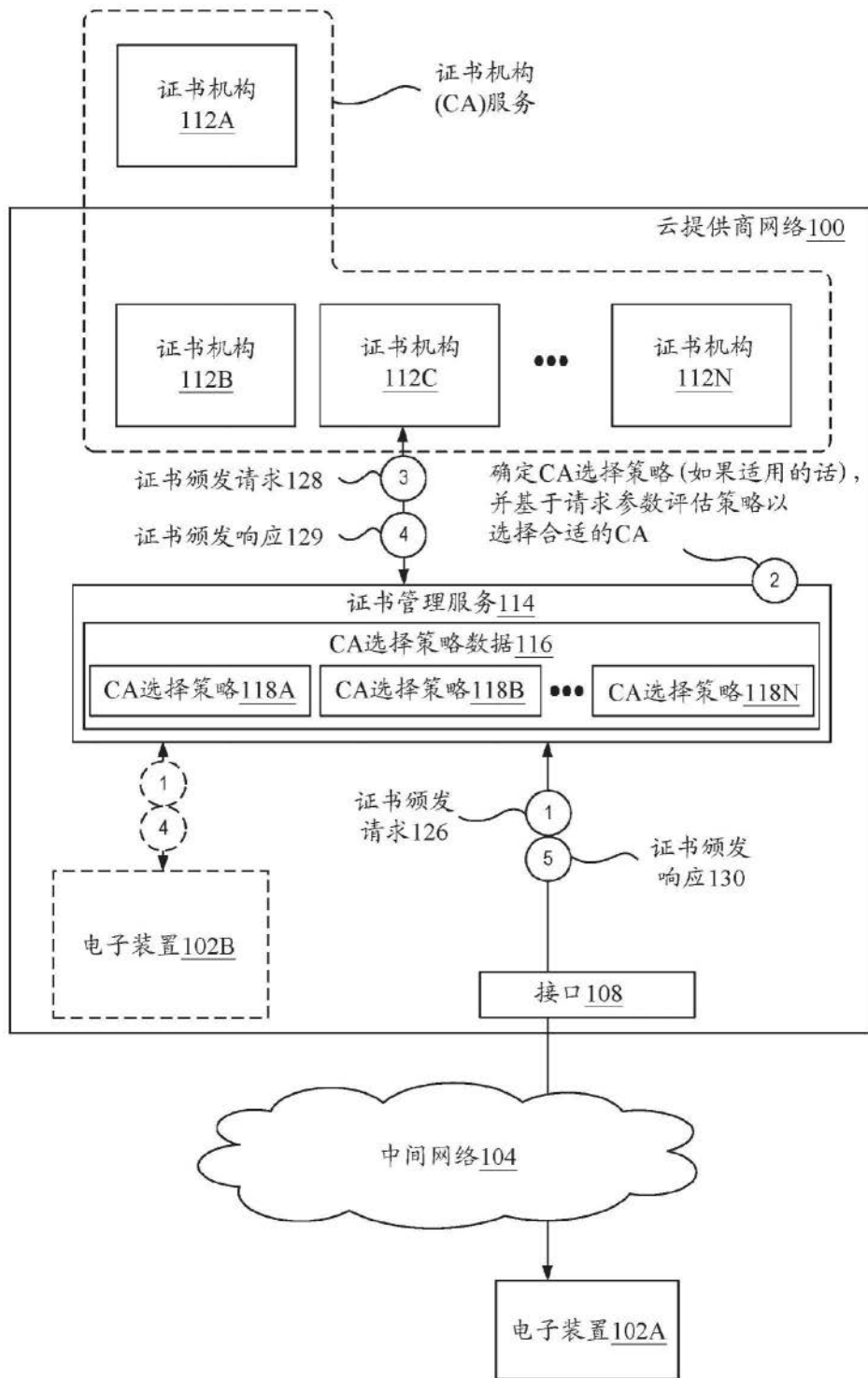


图1

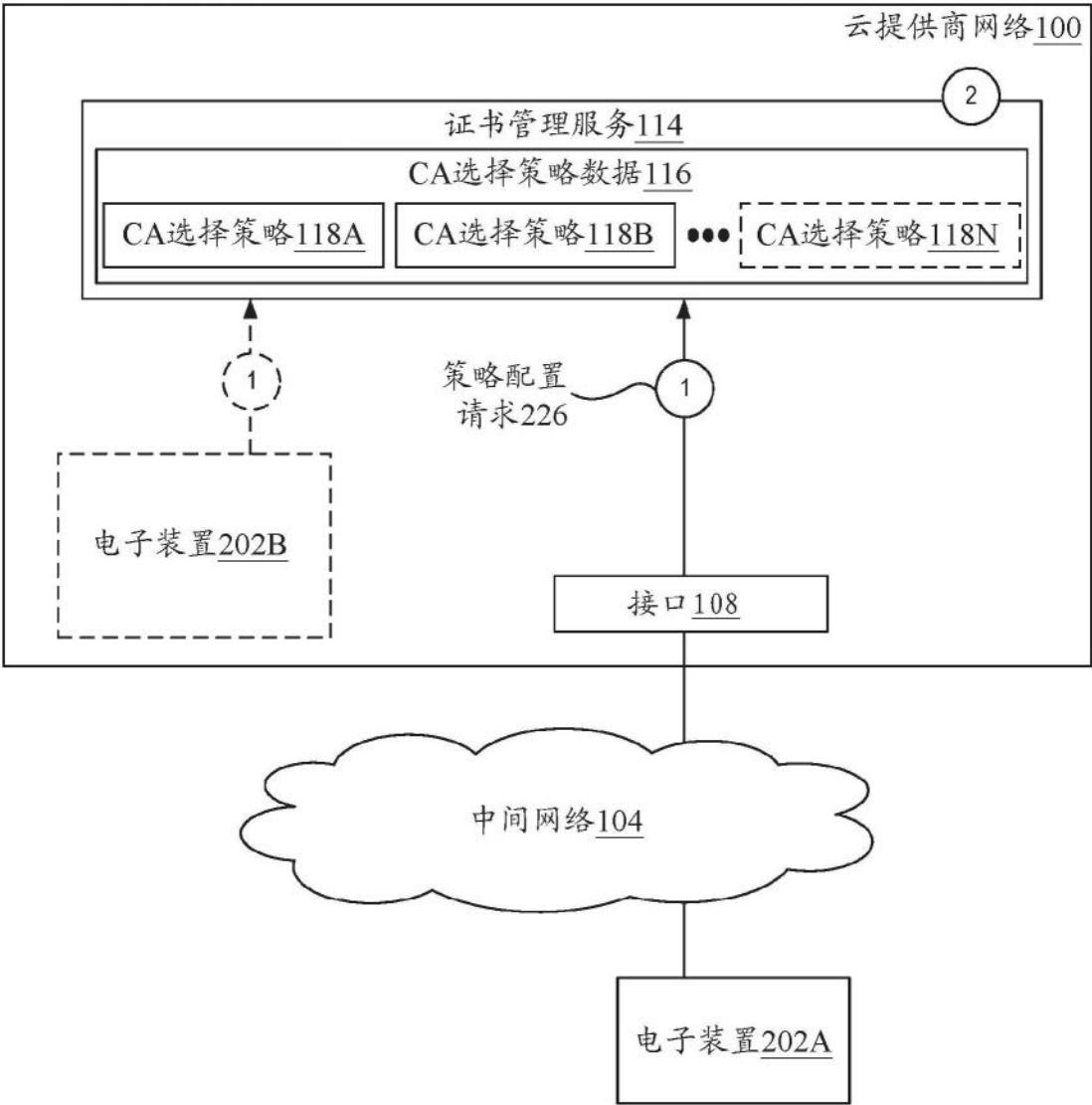


图2

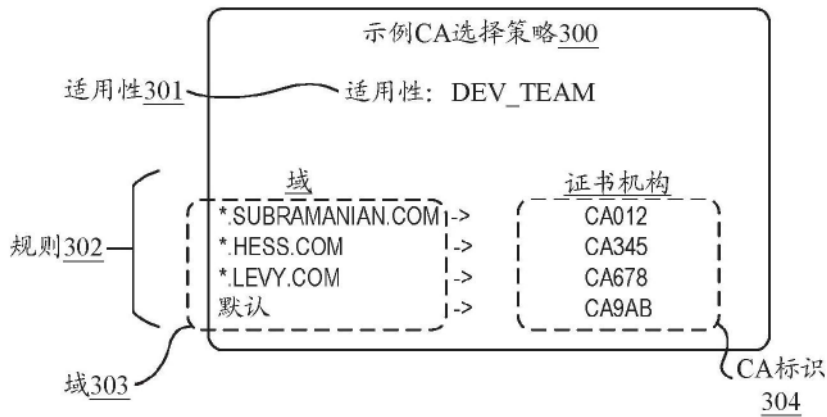


图3

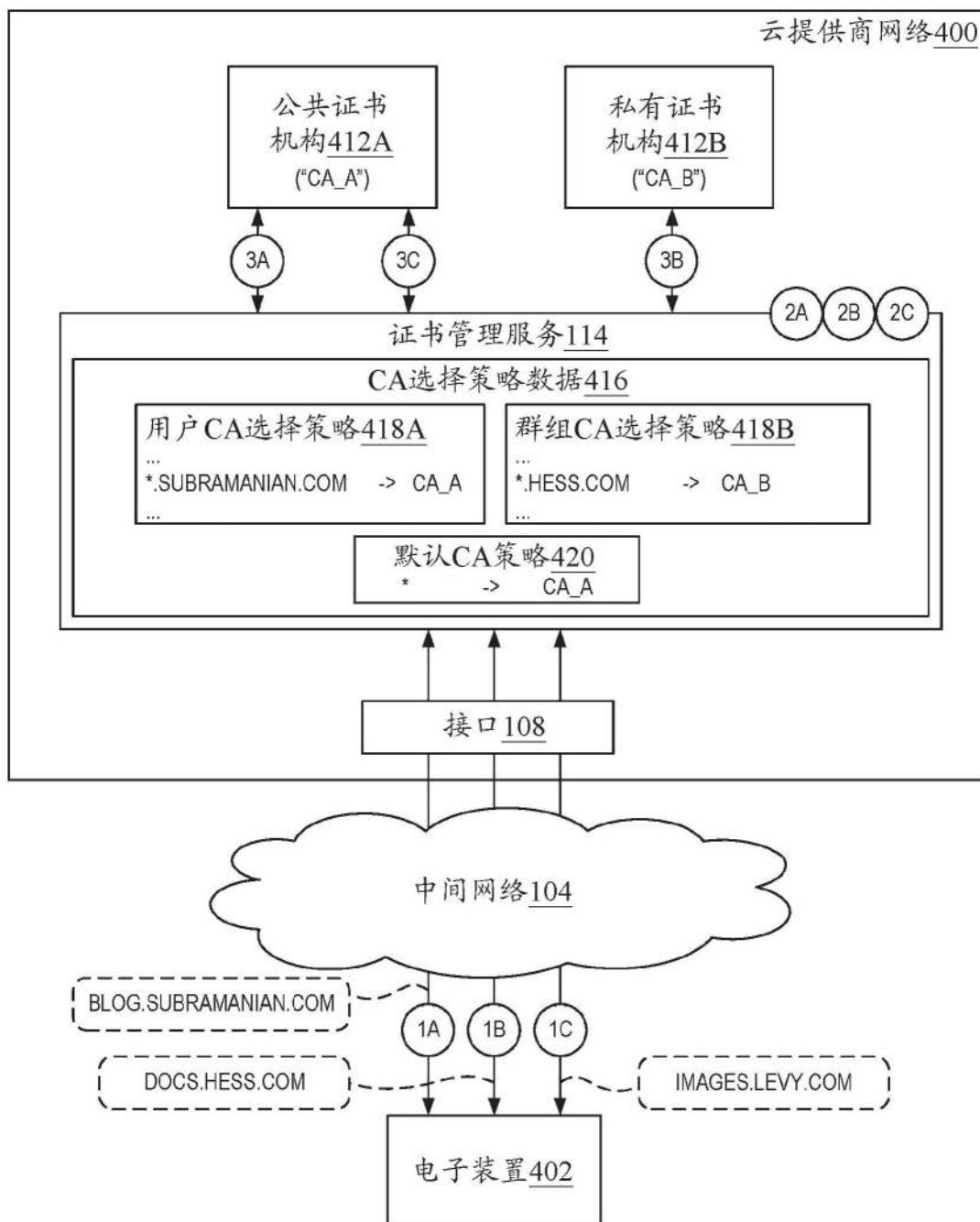


图4

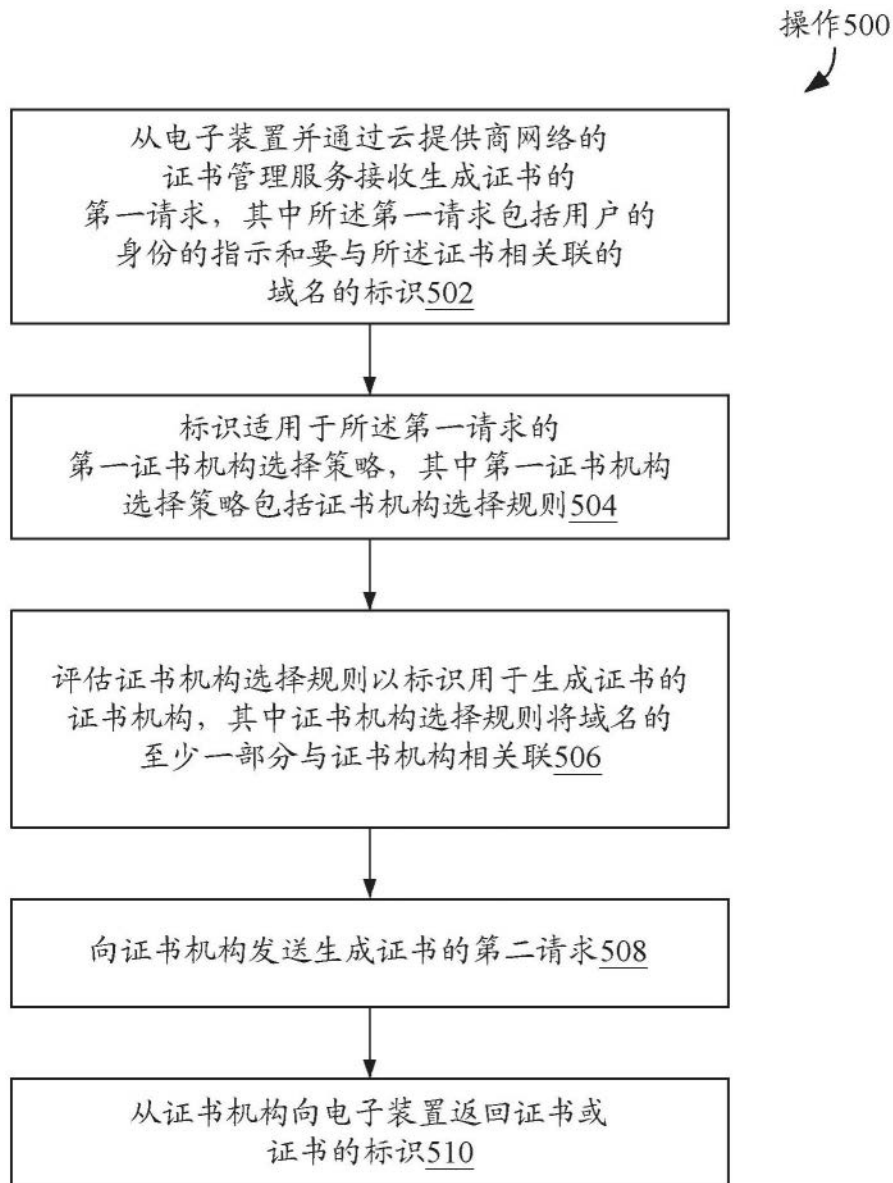


图5

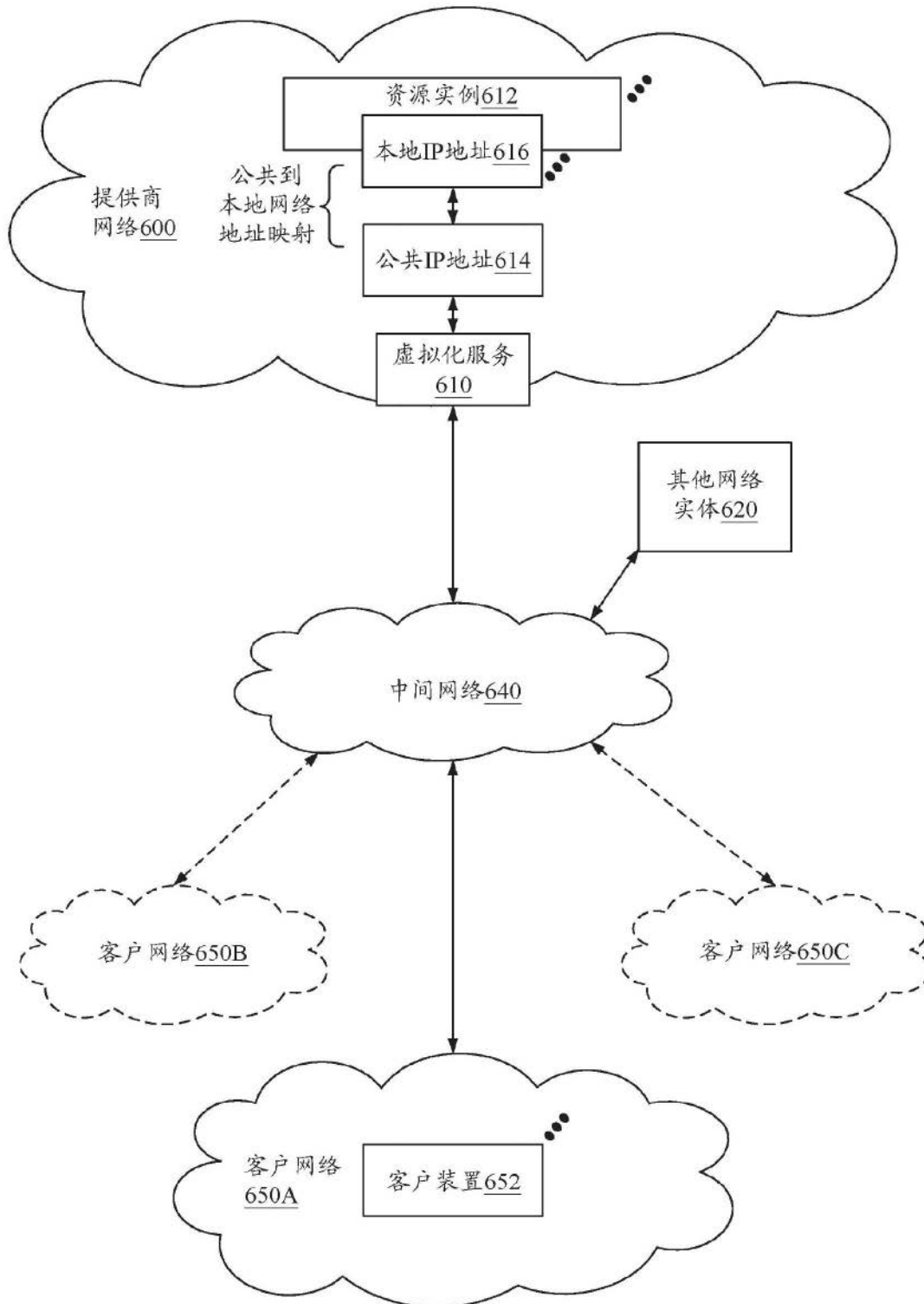


图6

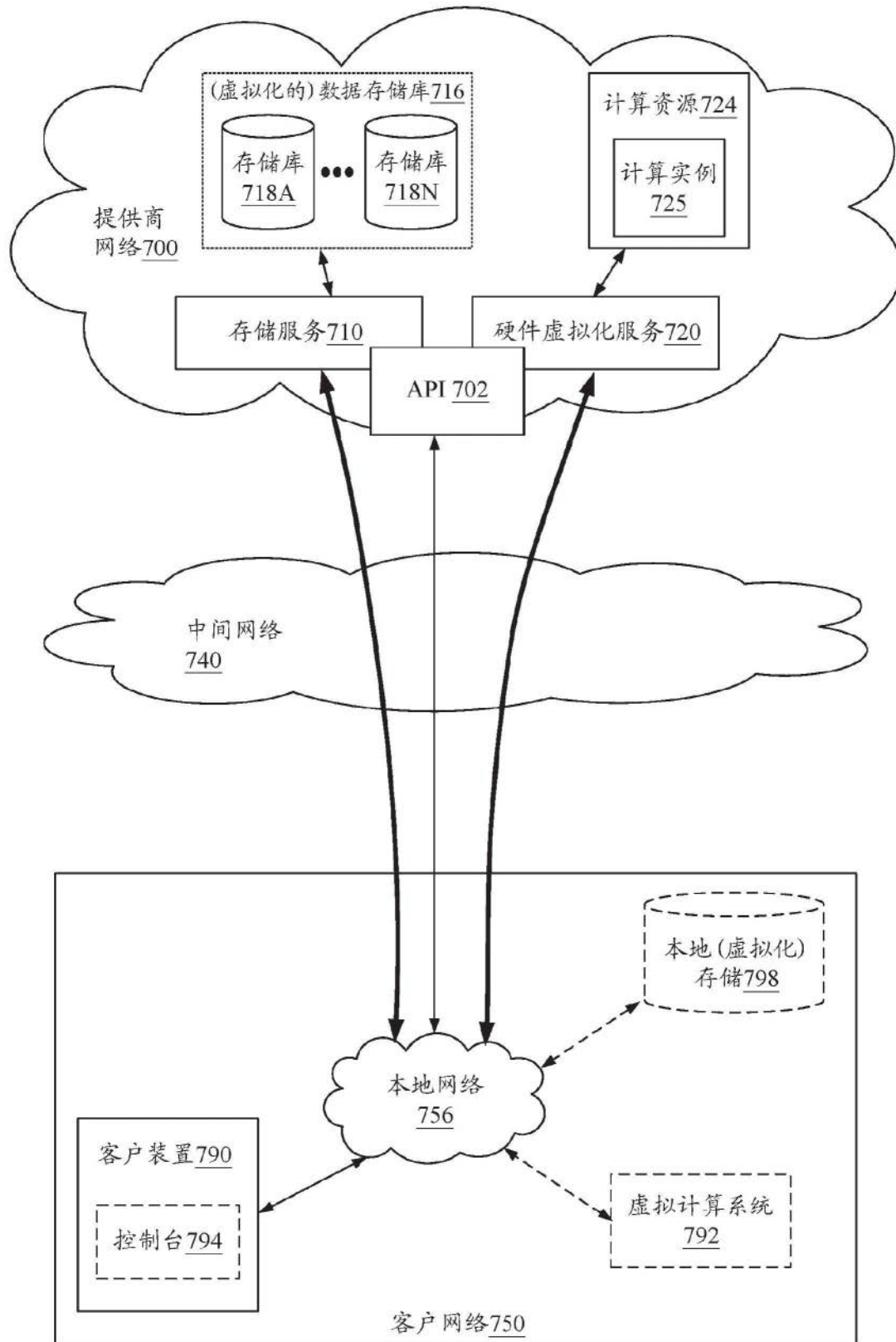


图7

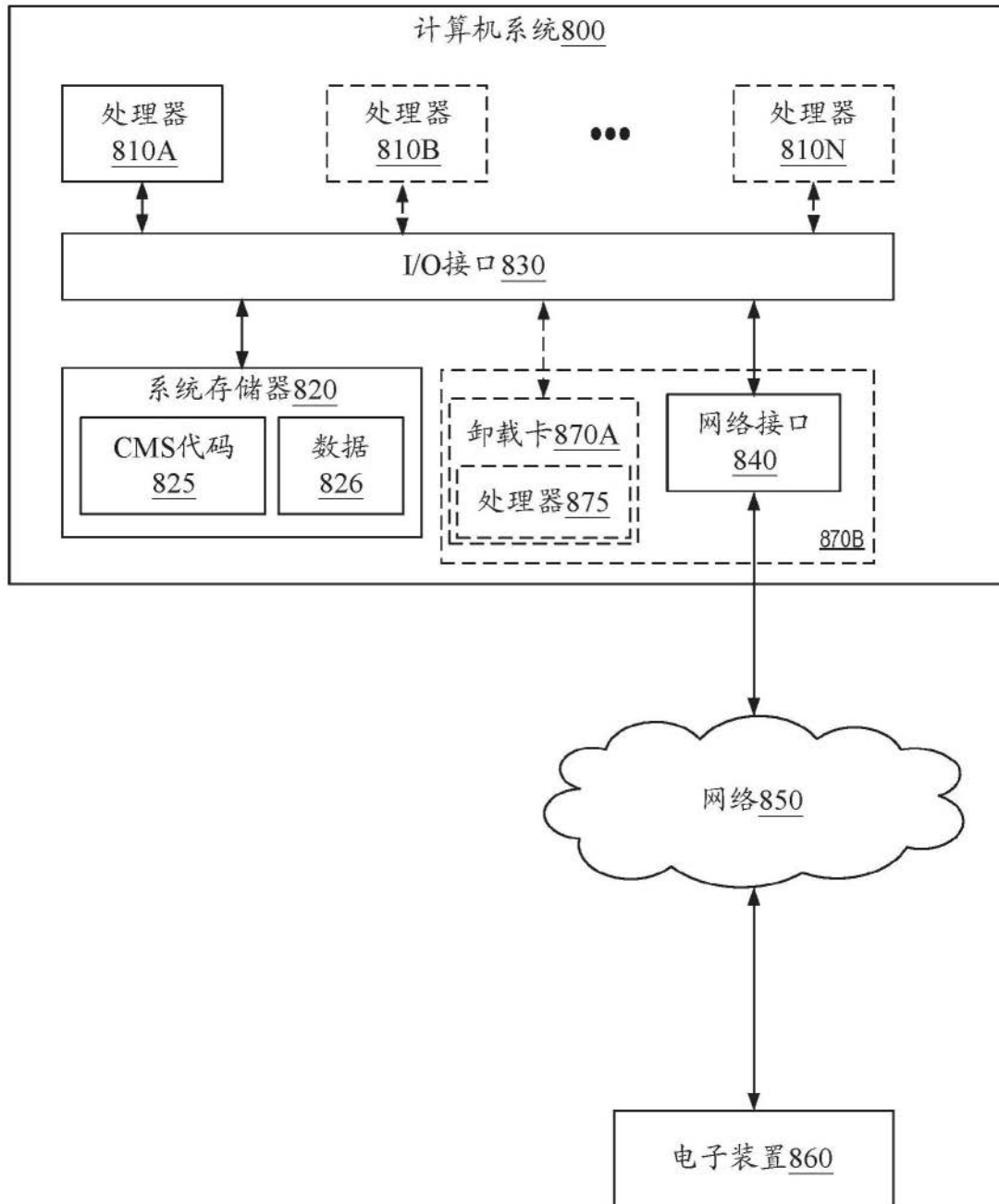


图8