



(12) 发明专利申请

(10) 申请公布号 CN 119814456 A

(43) 申请公布日 2025. 04. 11

(21) 申请号 202510017110.7

G06F 21/44 (2013.01)

(22) 申请日 2019.07.01

G06F 21/45 (2013.01)

(30) 优先权数据

16/029,559 2018.07.07 US

(62) 分案原申请数据

201980045450.3 2019.07.01

(71) 申请人 诚信安全服务有限公司

地址 美国加利福尼亚州

(72) 发明人 艾伦·T·迈耶

格雷戈里·A·鲍威尔

(74) 专利代理机构 北京高沃律师事务所 11569

专利代理师 王爱涛

(51) Int. Cl.

H04L 9/40 (2022.01)

H04L 9/32 (2006.01)

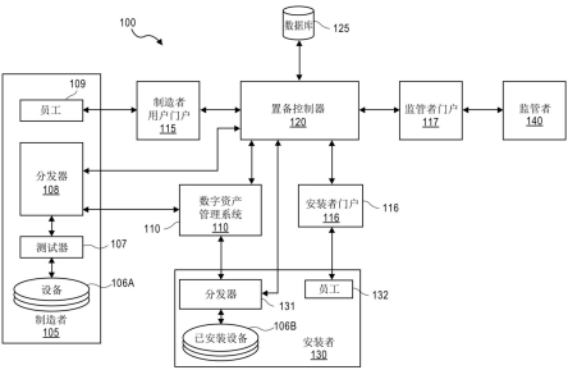
权利要求书6页 说明书33页 附图16页

(54) 发明名称

可缩放证书管理系统、方法及非暂时性计算机可读介质

(57) 摘要

本发明涉及用于安全提供证书的可缩放证书管理系统、方法及非暂时性计算机可读介质。系统可以包括：一个或多个运行注册审批机构的应用平台，该应用平台通信连接到一个或多个执行注册审批机构请求的加密计算的计算引擎；一个或多个运行登记证书颁发机构的应用平台，该应用平台通信连接到一个或多个执行登记证书颁发机构请求的加密计算的计算引擎；一个或多个运行假名证书颁发机构的应用平台，该应用平台通信连接到一个或多个执行假名证书颁发机构请求的加密计算的计算引擎；以及一个或多个运行第一链接权限机构和第二链接权限机构的应用平台，这些应用平台通信连接到一个或多个执行链接权限机构请求的加密计算的计算引擎。



1. 一种用于安全提供证书的可缩放证书管理系统,其中,所述可缩放证书管理系统包括:

一个或多个运行注册审批机构应用的应用平台,其通信连接到一个或多个执行注册审批机构应用请求的加密计算的计算引擎;

一个或多个运行登记证书颁发机构应用的应用平台,其通信连接到一个或多个执行登记证书颁发机构应用请求的加密计算的计算引擎,其中,所述登记证书颁发机构应用可操作为生成登记证书并将登记证书有条件地传输到所述注册审批机构应用;

一个或多个运行假名证书颁发机构应用的应用平台,其通信连接到一个或多个执行假名证书颁发机构应用请求的加密计算的计算引擎,其中,所述假名证书颁发机构应用可操作为生成假名证书并将假名证书有条件地传输到所述注册审批机构应用;

一个或多个运行第一链接权限机构应用的应用平台,其通信连接到一个或多个执行第一链接权限机构应用请求的加密计算的计算引擎;

一个或多个运行第二链接权限机构应用的应用平台,其通信连接到一个或多个执行第二链接权限机构应用请求的加密计算的计算引擎,其中,所述第一链接权限机构应用和所述第二链接权限机构应用可操作为生成链接值并将链接值有条件地传输到所述注册审批机构应用;以及

通信地连接到一个或多个计算引擎的一个或多个负载均衡器,所述一个或多个负载均衡器执行操作,所述操作包括基于所述一个或多个计算引擎的正常状况度量将至少一个请求分发到所述一个或多个计算引擎;以及

其中,所述可缩放证书管理系统将一个或多个证书负载分配给多个计算机化设备中的每个计算机化设备,所述一个或多个证书负载指示在一段时间内将要存储在每个计算机化设备内的假名证书的数量,其中,所述一个或多个证书负载是可分配的,使得每个计算机化设备可以在所述一段时间内存储与其他计算机化设备不同的多个假名证书。

2. 根据权利要求1所述的证书管理系统,其中,所述正常状况度量包括以下中的一项或更多项:所述一个或多个计算引擎的工作温度、所述一个或多个计算引擎的机壳内部的湿度水平、CPU容量、存储容量、所述一个或多个计算引擎的重新启动或重启的频率、自所述一个或多个计算引擎的最近一次重新启动以来的时间、在一段时间内所述一个或多个计算引擎的磁盘故障或存储器故障的次数、直到所述一个或多个计算引擎的排程维护事件前的时间、所述一个或多个计算引擎正在备用电源上运行的指示或者自上次所述一个或多个计算引擎的电源停电或降压以来的持续时间。

3. 根据权利要求1所述的证书管理系统,其中,所述证书管理系统进一步包括一个或多个数据库,其可操作地连接到所述一个或多个运行注册审批机构应用的应用平台、所述一个或多个运行登记证书颁发机构应用的应用平台、所述一个或多个运行假名证书颁发机构应用的应用平台、所述一个或多个运行第一链接权限机构应用的应用平台以及一个或多个运行第二链接权限机构应用的应用平台。

4. 根据权利要求2所述的证书管理系统,其中,所述注册审批机构应用、所述登记证书颁发机构应用、所述假名证书颁发机构应用、所述第一链接权限机构应用、所述第二链接权限机构应用以及所述一个或多个数据库中的每一个可操作为彼此独立地缩放。

5. 根据权利要求1所述的证书管理系统,其中,

所述登记证书颁发机构应用可操作为响应于从所述注册审批机构应用接收到对登记证书的请求而生成登记证书；

所述假名证书颁发机构应用可操作为响应于从所述注册审批机构应用接收到对假名证书的请求而生成假名证书；以及

所述第一链接权限机构应用和所述第二链接权限机构应用可操作为响应于从所述注册审批机构应用接收到对链接值的请求而生成链接值。

6. 根据权利要求1所述的证书管理系统, 其中, 所述注册审批机构应用、所述登记证书颁发机构应用、所述假名证书颁发机构应用、所述第一链接权限机构应用和所述第二链接权限机构应用中的每一个通过包括多个消息队列的消息列队服务而彼此通信连接。

7. 根据权利要求1所述的证书管理系统, 其中,

所述一个或多个运行登记证书颁发机构应用的应用平台是通过第一多个消息队列通信连接到所述一个或多个执行登记证书颁发机构应用请求的加密计算的计算引擎的一个或多个虚拟机；

所述一个或多个运行第一链接权限机构应用的应用平台是通过第二多个消息队列通信连接到所述一个或多个执行第一链接权限机构应用请求的加密计算的计算引擎的一个或多个虚拟机；以及

所述一个或多个运行第二链接权限机构应用的应用平台是通过第三多个消息队列通信连接到所述一个或多个执行第二链接权限机构应用请求的加密计算的计算引擎的一个或多个虚拟机。

8. 根据权利要求7所述的证书管理系统, 其中,

所述第一多个消息队列包括:

第一消息队列, 用于列队待传递到一个或多个运行登记证书颁发机构应用的虚拟机的消息; 以及

第二消息队列, 用于列队待传递到所述一个或多个执行登记证书颁发机构应用请求的加密计算的计算引擎的消息;

所述第二多个消息队列包括:

第三消息队列, 用于列队待传递到一个或多个运行第一链接权限机构应用的虚拟机的消息; 以及

第四消息队列, 用于列队待传递到所述一个或多个执行第一链接权限机构应用请求的加密计算的计算引擎的消息; 以及

所述第三多个消息队列包括:

第五消息队列, 用于列队待传递到一个或多个运行第二链接权限机构应用的虚拟机的消息; 以及

第六消息队列, 用于列队待传递到所述一个或多个执行第二链接权限机构应用请求的加密计算的计算引擎的消息。

9. 根据权利要求7所述的证书管理系统, 其中,

所述第一多个消息队列包括:

第一双向消息队列, 用于列队待传递到及发送自所述一个或多个运行登记证书颁发机构应用的虚拟机的消息; 以及

第二双向消息队列,用于列队待传递到及发送自所述一个或多个执行登记证书颁发机构应用请求的加密计算的计算引擎的消息;

所述第二多个消息队列包括:

第三双向消息队列,用于列队待传递到及发送自所述一个或多个运行第一链接权限机构应用的虚拟机的消息;以及

第四双向消息队列,用于列队待传递到及发送自所述一个或多个执行第一链接权限机构应用请求的加密计算的计算引擎的消息;以及

所述第三多个消息队列包括:

第五双向消息队列,用于列队待传递到及发送自所述一个或多个运行第二链接权限机构应用的虚拟机的消息;以及

第六双向消息队列,用于列队待传递到及发送自所述一个或多个执行第二链接权限机构应用请求的加密计算的计算引擎的消息。

10. 根据权利要求1所述的证书管理系统,其中,

所述一个或多个运行登记证书颁发机构应用的应用平台通过所述一个或更多个负载均衡器的第一负载均衡器通信连接到所述一个或多个执行登记证书颁发机构应用请求的加密计算的计算引擎;

所述一个或多个运行第一链接权限机构应用的应用平台通过所述一个或更多个负载均衡器的第二负载均衡器通信连接到所述一个或多个执行第一链接权限机构应用请求的加密计算的计算引擎;以及

所述一个或多个运行第二链接权限机构应用的应用平台通过所述一个或更多个负载均衡器的第三负载均衡器通信连接到一个或多个执行第二链接权限机构应用请求的加密计算的计算引擎。

11. 根据权利要求10所述的证书管理系统,其中,

所述第一负载均衡器、所述第二负载均衡器和所述第三负载均衡器均包括负载均衡器虚拟机和负载均衡器服务器中的一个或多个;以及

所述负载均衡器虚拟机和所述负载均衡器服务器均配置为跨多个应用平台和多个计算引擎分发工作负载。

12. 根据权利要求11所述的证书管理系统,其中,所述负载均衡器虚拟机和所述负载均衡器服务器均配置为使用轮询调度技术跨多个应用平台和多个计算引擎分发工作负载。

13. 根据权利要求11所述的证书管理系统,其中,所述负载均衡器虚拟机和所述负载均衡器服务器均配置为基于多个应用平台中的每一个和多个计算引擎中的每一个所报告的各自工作负载而跨多个应用平台和多个计算引擎分发工作负载。

14. 根据权利要求1所述的证书管理系统,其中,所述证书管理系统进一步可操作为将有关与计算机化设备相关的证书活动的信息传输到置备控制器以存储在日志中。

15. 根据权利要求1所述的证书管理系统,还包括置备控制器,所述置备控制器可操作为在向所述注册审批机构应用传输对登记证书的请求之前对所述计算机化设备进行认证。

16. 根据权利要求1所述的证书管理系统,其中,登记证书是将公钥证书的持有者标识为包括多个计算机化设备的生态系统中的授权参与者的公钥证书,且其中,所述生态系统中的每个授权参与者能够接收一个或多个启用与多个计算机化设备进行通信的假名证书。

17. 根据权利要求1所述的证书管理系统,其中,所述证书负载可由订户分配。

18. 根据权利要求1所述的证书管理系统,其中,所述可缩放证书管理系统为每个订户分配假名证书使用,指示在一段时间内可用的假名证书的数量。

19. 一种用于安全提供证书的方法,其中,所述方法包括:

执行由注册审批机构应用请求的加密计算,所述注册审批机构应用通信连接到一个或多个执行注册审批机构应用所请求的加密计算的计算引擎;

执行由登记证书颁发机构应用请求的加密计算,所述登记证书颁发机构应用通信连接到一个或多个执行登记证书颁发机构应用所请求的加密计算的计算引擎,其中,所述登记证书颁发机构应用生成登记证书并将登记证书有条件地传输到所述注册审批机构应用;

执行由假名证书颁发机构应用请求的加密计算,所述假名证书颁发机构应用通信连接到一个或多个执行假名证书颁发机构应用所请求的加密计算的计算引擎,其中,所述假名证书颁发机构应用生成假名证书并将假名证书有条件地传输到所述注册审批机构应用;

执行由第一链接权限机构应用请求的加密计算,所述第一链接权限机构应用通信连接到一个或多个执行第一链接权限机构应用所请求的加密计算的计算引擎;

执行由第二链接权限机构应用请求的加密计算,所述第二链接权限机构应用通信连接到一个或多个执行第二链接权限机构应用所请求的加密计算的计算引擎,其中,所述第一链接权限机构应用和所述第二链接权限机构应用生成链接值并将链接值有条件地传输到所述注册审批机构应用;以及

将一个或多个证书负载分配给多个计算机化设备中的每个计算机化设备,所述一个或多个证书负载指示在一段时间内将要存储在每个计算机化设备内的假名证书的数量,其中,所述证书负载是可分配的,使得每个计算机化设备可以在所述一段时间内存储与其他计算机化设备不同的多个假名证书,以及

其中,通信地连接到一个或多个计算引擎的一个或多个负载均衡器执行操作,所述操作包括基于所述一个或多个计算引擎的正常状况度量将至少一个请求分发到所述一个或多个计算引擎。

20. 根据权利要求19所述的方法,其中,所述正常状况度量包括以下中的一项或更多项:所述一个或多个计算引擎的工作温度、所述一个或多个计算引擎的机壳内部的湿度水平、CPU容量、存储容量、所述一个或多个计算引擎的重新启动或重启的频率、自所述一个或多个计算引擎的最近一次重新启动以来的时间、在一段时间内所述一个或多个计算引擎的磁盘故障或存储器故障的次数、直到所述一个或多个计算引擎的排程维护事件前的时间、所述一个或多个计算引擎正在备用电源上运行的指示或者自上次所述一个或多个计算引擎的电源停电或降压以来的持续时间。

21. 根据权利要求19所述的方法,其中,所述方法还包括:

响应于从所述注册审批机构应用接收到对登记证书的请求而生成登记证书;

响应于从所述注册审批机构应用接收到对假名证书的请求而生成所述假名证书;以及

响应于从所述注册审批机构应用接收到对链接值的请求而生成所述链接值。

22. 根据权利要求19所述的方法,还包括将有关与计算机化设备相关的证书活动的信息传输到置备控制器以存储在日志中。

23. 根据权利要求19所述的方法,还包括在向所述注册审批机构应用传输对登记证书

的请求之前对所述计算机化设备进行认证。

24. 根据权利要求19所述的方法, 其中, 登记证书是将公钥证书的持有者标识为包括多个计算机化设备的生态系统中的授权参与者的公钥证书, 且其中, 所述生态系统中的每个授权参与者能够接收一个或多个启用与多个计算机化设备进行通信的假名证书。

25. 根据权利要求19所述的方法, 其中, 所述证书负载可由订户分配。

26. 根据权利要求19所述的方法, 还包括为每个订户分配假名证书使用, 指示在一段时间内可用的假名证书的数量。

27. 一种用于安全提供证书的非暂时性计算机可读介质, 所述非暂时性计算机可读介质包括多条指令, 所述多条指令响应于由处理器执行而使所述处理器执行操作, 所述操作包括:

执行由注册审批机构应用请求的加密计算;

执行由登记证书颁发机构应用请求的加密计算, 其中, 所述登记证书颁发机构应用生成登记证书并将登记证书有条件地传输到所述注册审批机构应用;

执行由假名证书颁发机构应用请求的加密计算, 其中, 所述假名证书颁发机构应用生成假名证书并将假名证书有条件地传输到所述注册审批机构应用;

执行由第一链接权限机构应用请求的加密计算;

执行由第二链接权限机构应用请求的加密计算, 所述第一链接权限机构应用和所述第二链接权限机构应用生成链接值并将链接值有条件地传输到所述注册审批机构应用; 以及

将一个或多个证书负载分配给多个计算机化设备中的每个计算机化设备, 所述一个或多个证书负载指示在一段时间内将要存储在每个计算机化设备内的假名证书的数量, 其中, 所述一个或多个证书负载是可分配的, 使得每个计算机化设备可以在所述一段时间内存储与其他计算机化设备不同的多个假名证书, 以及

其中, 通信地连接到一个或多个计算引擎的一个或多个负载均衡器执行操作, 所述操作包括基于所述一个或多个计算引擎的正常状况度量将至少一个请求分发到所述一个或多个计算引擎。

28. 根据权利要求27所述的非暂时性计算机可读介质, 其中, 所述正常状况度量包括以下中的一项或更多项: 所述一个或多个计算引擎的工作温度、所述一个或多个计算引擎的机壳内部的湿度水平、CPU容量、存储容量、所述一个或多个计算引擎的重新启动或重启的频率、自所述一个或多个计算引擎的最近一次重新启动以来的时间、在一段时间内所述一个或多个计算引擎的磁盘故障或存储器故障的次数、直到所述一个或多个计算引擎的排程维护事件前的时间、所述一个或多个计算引擎正在备用电源上运行的指示或者自上次所述一个或多个计算引擎的电源停电或降压以来的持续时间。

29. 根据权利要求27所述的非暂时性计算机可读介质, 其中, 所述操作还包括:

响应于从所述注册审批机构应用接收到对登记证书的请求而生成登记证书;

响应于从所述注册审批机构应用接收到对假名证书的请求而生成所述假名证书; 以及

响应于从所述注册审批机构应用接收到对链接值的请求而生成所述链接值。

30. 根据权利要求27所述的非暂时性计算机可读介质, 其中所述操作还包括:

将有关与计算机化设备相关的证书活动的信息传输到置备控制器以存储在日志中。

31. 根据权利要求27所述的非暂时性计算机可读介质, 其中所述操作还包括:

在向所述注册审批机构应用传输对登记证书的请求之前对所述计算机化设备进行认证。

32. 根据权利要求27所述的非瞬态计算机可读介质,其中所述证书负载可由订户分配。

33. 根据权利要求27所述的非暂时性计算机可读介质,其中,使所述处理器执行操作,所述操作还包括为每个订户分配假名证书使用,指示在一段时间内可用的假名证书的数量。

可缩放证书管理系统、方法及非暂时性计算机可读介质

[0001] 本申请是申请日为2019年7月1日、申请号为201980045450.3、发明名称为“可缩放证书管理系统架构”的分案申请,该母案申请是2019年7月1日提交到国际专利局的国际申请号PCT/US2019/040064的进中国国家阶段申请,要求在2018年7月7日提交到美国专利局的申请号为16/029,559的优先权,上述申请通过引用完全并入本文。该母案申请涉及申请日为2017年11月14日、申请号为US 15/812,510的美国申请的部分继续申请(其要求申请日为2016年11月14日、申请号为US 62/421,878的美国临时申请的权益);申请日为2016年11月14日、申请号为US 62/421,852的美国临时申请;以及申请日为2017年4月20日、申请号为US 62/487,909的美国临时申请,它们的全部内容通过整体引用归并本文。

技术领域

[0002] 本发明涉及用于安全置备(provision)计算机化设备的系统、设备和方法。

背景技术

[0003] 随着计算机变得越来越小型化和商品化,制造者目前生产越来越多样化的包含一个或多个嵌入式计算机或处理器的设备。计算机化设备中的计算机能够控制设备的操作,能够收集、存储和共享数据,能够与其他计算机和其他计算机化设备进行通信,并能够更新自己的软件等。

[0004] 物联网(IoT)是具有嵌入式处理器、电子器件、软件、数据、传感器、致动器的计算机化物理设备的网络和/或经由数字网络促使这些设备连接和交换数据的网络连接,包括因特网、蜂窝网络和其他无线网络。通常,每个“事物”

[0005] 均可通过其嵌入式计算系统进行唯一标识,并能在现有因特网基础设施内进行交互操作。

[0006] 物联网意义上的“事物”可指多种计算机化设备,诸如消费类家用电器、用于企业 and 公司环境的商用设备、制造机械、农用设施、家居和建筑物中的能耗设备(交换机、电源插座、电器、照明系统、灯泡、电视机、车库开门器、洒水系统、安全系统等)、医疗保健设备、基础设施管理设备、机器人、无人机以及运输设备和交通工具等。

[0007] 例如,大多数(即使不是全部)现代交通工具和运输机械(例如汽车、卡车、飞机、火车、船舶、摩托车、踏板车等)在其子系统中包含数个嵌入式处理器或嵌入式计算机,它们在至少某些方面受计算机控制。类似地,越来越多的现代交通基础设施设备(例如交通信号灯、交通相机、交通传感器、桥梁监控器、桥梁控制系统等)包含至少一个(通常很多)嵌入式处理器或嵌入式计算机系统,它们在至少某些方面受计算机控制。这些运输网络中受计算机控制的元素通常会彼此通信,来回传递各种类型的信息,并且它们可能对其操作作出反应、响应和更改,或者根据以车辆间通信(V2V,Vehicle-to-Vehicle;又称C2C,Car-to-Car)从其他车辆接收/发送到其他车辆的信息和/或以车辆基础设施通信(V2I,Vehicle-to-Infrastructure,又称C2I,Car-to-Infrastructure)从基础设施元素接收/发送到基础设施元素的信息进行安全、正确、高效和可靠的操作。

[0008] 计算机化设备中的计算机根据其软件和/或固件及数据进行操作。为了确保安全正确的操作,计算机化设备必须按照制造者的要求使用正确的软件、固件、可执行指令、数字证书(例如公钥证书)、加密密钥等(下文统称“数字资产”或“软件”)进行正确的初始化和更新,以便物联网仅由执行授权的已知良好软件和数据及设备组成。但是,当未经授权的人员或组织(例如黑客)替换或更改计算机化设备中的软件时,就会出现安全问题。当更旧版本的软件、未经测试的软件、未经批准的软件和/或具有已知漏洞的软件安装到计算机化设备时,也会出现问题。

[0009] 有鉴于此,期望提供改进的用于将数字资产安全置备到计算机化设备中的系统、方法和技术,以防止计算机化设备使用易出差错、运行不当、未经测试、恶意篡改或其他不可取的软件和数据来进行操作。

发明内容

[0010] 本公开涉及用于安全生成和提供某些类型的数字资产(诸如安全凭证和数字证书)的系统、方法和设备。在各种实施方式中,所述系统、方法和设备使用可缩放证书管理系统(CMS)来创建和提供某些类型的数字资产,诸如安全凭证和公钥证书。在一些实施方式中,所述CMS提供诸如登记证书和假名证书等证书,以响应于对此类证书的请求。

[0011] 在各种实施方式中,所述CMS具有可缩放架构,其包括注册审批机构、一个或多个链接权限机构、假名证书颁发机构和登记证书颁发机构。一种示例CMS可以包括一个或多个运行注册审批机构应用的应用平台,该应用平台通信连接到一个或多个执行注册审批机构应用所需的加密计算的计算引擎。该一个或多个应用平台可以包括一个或多个虚拟机(VM)或一个或多个硬件平台(例如服务器、计算机或能够托管和执行软件应用的其他计算机硬件)。所述系统还可以包括一个或多个运行登记证书颁发机构的应用平台,该应用平台通信连接到一个或多个执行登记证书颁发机构所需的加密计算的计算引擎。登记证书颁发机构应用可操作为生成登记证书并将登记证书有条件地传输到注册审批机构应用。所述示例CMS可以进一步包括一个或多个运行假名证书颁发机构应用的VM,该VM通信连接到一个或多个执行假名证书颁发机构所需的加密计算的计算引擎;假名证书颁发机构应用可操作为生成假名证书并将假名证书有条件地传输到注册审批机构应用。所述CMS还可以包括一个或多个运行第一链接权限机构和第二链接权限机构的VM,这些VM通信连接到一个或多个执行第一链接权限机构和第二链接权限机构所需的加密计算的计算引擎。第一链接权限机构应用和第二链接权限机构应用可操作为生成链接值并将链接值有条件地传输到注册审批机构应用。

[0012] 在一些实施方式中,一种用于证书安全提供给置备控制器的可缩放CMS包括:一个或多个运行注册审批机构应用的应用平台,该应用平台通信连接到一个或多个执行注册审批机构应用所需的加密计算的计算引擎;一个或多个运行登记证书颁发机构应用的应用平台,该应用平台通信连接到一个或多个执行登记证书颁发机构应用所需的加密计算的计算引擎,该登记证书颁发机构应用可操作为生成登记证书并将登记证书有条件地传输到注册审批机构应用;一个或多个运行假名证书颁发机构应用的应用平台,该应用平台通信连接到一个或多个执行假名证书颁发机构应用所需的加密计算的计算引擎,该假名证书颁发机构应用可操作为生成假名证书并将假名证书有条件地传输到注册审批机构应用;一个或多

个运行第一链接权限机构应用的应用平台,该应用平台通信连接到一个或多个执行第一链接权限机构应用所需的加密计算的计算引擎;以及一个或多个运行第二链接权限机构应用的应用平台,该应用平台通信连接到一个或多个执行第二链接权限机构应用所需的加密计算的计算引擎。链接权限机构应用可操作为生成链接值并将链接值有条件地传输到注册审批机构应用。

[0013] 在其他实施方式中,所述CMS可以进一步包括一个或多个数据库,该数据库可操作地连接到一个或多个运行注册审批机构应用的应用平台、一个或多个运行登记证书颁发机构应用的应用平台、一个或多个运行假名证书颁发机构应用的应用平台、一个或多个运行第一链接权限机构应用的应用平台以及一个或多个运行第二链接权限机构应用的应用平台。

[0014] 在又一些其他实施方式中,注册审批机构应用、登记证书颁发机构应用、假名证书颁发机构应用、第一链接权限机构应用、第二链接权限机构应用以及一个或多个数据库中的每一个可操作为彼此独立地缩放。

[0015] 在还一些其他实施方式中,登记证书颁发机构应用可操作为响应于从注册审批机构应用接收到对登记证书的请求而生成登记证书;登记证书颁发机构应用可操作为响应于从注册审批机构应用接收到对假名证书的请求而生成假名证书;以及第一链接权限机构应用和第二链接权限机构应用可操作为响应于从注册审批机构应用接收到对链接值的请求而生成链接值。

[0016] 在一些实施方式中,注册审批机构应用、登记证书颁发机构应用、假名证书颁发机构应用、第一链接权限机构应用和第二链接权限机构应用中的每一个通过包括多个消息队列的消息队列服务而彼此通信连接。

[0017] 在某些实施方式中,一个或多个运行登记证书颁发机构应用的应用平台是通过第一多个消息队列通信连接到一个或多个执行登记证书颁发机构应用所需的加密计算的计算引擎的一个或多个虚拟机;一个或多个运行第一链接权限机构应用的应用平台是通过第二多个消息队列通信连接到一个或多个执行第一链接权限机构应用所需的加密计算的计算引擎的一个或多个虚拟机;以及一个或多个运行第二链接权限机构应用的应用平台是通过第三多个消息队列通信连接到一个或多个执行第二链接权限机构应用所需的加密计算的计算引擎的一个或多个虚拟机。

[0018] 根据具有第一多个消息队列、第二多个消息队列和第三多个消息队列的某些实施方式,第一多个消息队列包括:第一消息队列,用于列队待传递到一个或多个运行登记证书颁发机构应用的虚拟机的消息;以及第二消息队列,用于列队待传递到一个或多个执行登记证书颁发机构应用所需的加密计算的计算引擎的消息;第二多个消息队列包括:第三消息队列,用于列队待传递到一个或多个运行第一链接权限机构应用的虚拟机的消息;以及第四消息队列,用于列队待传递到一个或多个执行第一链接权限机构应用所需的加密计算的计算引擎的消息;以及第三多个消息队列包括:第五消息队列,用于列队待传递到一个或多个运行第二链接权限机构应用的虚拟机的消息;以及第六消息队列,用于列队待传递到一个或多个执行第二链接权限机构应用所需的加密计算的计算引擎的消息。

[0019] 在具有第一多个消息队列、第二多个消息队列和第三多个消息队列的其他实施方式中,第一多个消息队列包括:第一双向消息队列,用于列队待传递到及发送自一个或多个

运行登记证书颁发机构应用的虚拟机的消息;以及第二双向消息队列,用于列队待传递到及发送自一个或多个执行登记证书颁发机构应用所需的加密计算的计算引擎的消息;第二多个消息队列包括:第三双向消息队列,用于列队待传递到及发送自一个或多个运行第一链接权限机构应用的虚拟机的消息;以及第四双向消息队列,用于列队待传递到及发送自一个或多个执行第一链接权限机构应用所需的加密计算的计算引擎的消息;以及第三多个消息队列包括:第五双向消息队列,用于列队待传递到及发送自一个或多个运行第二链接权限机构应用的虚拟机的消息;以及第六双向消息队列,用于列队待传递到及发送自一个或多个执行第二链接权限机构应用所需的加密计算的计算引擎的消息。

[0020] 在所述CMS的其他实施方式中,一个或多个运行登记证书颁发机构应用的应用平台通过第一负载均衡器通信连接到一个或多个执行登记证书颁发机构应用所需的加密计算的计算引擎;一个或多个运行第一链接权限机构应用的应用平台通过第二负载均衡器通信连接到一个或多个执行第一链接权限机构应用所需的加密计算的计算引擎;以及一个或多个运行第二链接权限机构应用的应用平台通过第三负载均衡器通信连接到一个或多个执行第二链接权限机构应用所需的加密计算的计算引擎。

[0021] 在所述CMS包括第一负载均衡器、第二负载均衡器和第三负载均衡器的某些实施方式中,每个负载均衡器可以包括以下一个或多个:负载均衡器虚拟机和负载均衡器服务器;以及负载均衡器虚拟机和负载均衡器服务器均配置为跨多个应用平台和多个计算引擎分发工作负载。

[0022] 在具有负载均衡器虚拟机和负载均衡器服务器的其他实施方式中,负载均衡器虚拟机和负载均衡器服务器均配置为使用轮询调度技术跨多个应用平台和多个计算引擎分发工作负载。

[0023] 在包括负载均衡器虚拟机和负载均衡器服务器的又一些其他实施方式中,负载均衡器虚拟机和负载均衡器服务器均配置为基于多个应用平台中的每一个和多个计算引擎中的每一个所报告的各自工作负载而跨多个应用平台和多个计算引擎分发工作负载。

[0024] 在各种实施方式中,置备控制器可操作为:代表计算机化设备向注册审批机构应用传输对登记证书的请求;从注册审批机构应用接收登记证书,该登记证书可由登记证书颁发机构应用生成;将登记证书传输到计算机化设备;代表计算机化设备向注册审批机构应用传输对多个假名证书的请求;从注册审批机构应用接收多个假名证书,该多个假名证书可由假名证书颁发机构应用生成;将多个假名证书传输到计算机化设备;创建并保留与计算机化设备相关联的日志;以及存储有关计算机化设备的证书活动的信息。

[0025] 在置备控制器可操作为创建并保留日志的一些实施方式中,置备控制器进一步可操作为将有关与计算机化设备相关的证书活动的信息传输到置备控制器以存储在日志中。

[0026] 在置备控制器可操作为向注册审批机构应用传输对登记证书的请求的某些实施方式中,置备控制器进一步可操作为在向注册审批机构应用传输对登记证书的请求之前对计算机化设备进行认证。

[0027] 在其他实施方式中,登记证书可以是将公钥证书的持有者标识为包括多个计算机化设备的生态系统中的授权参与者的公钥证书,并且生态系统中的每个授权参与者能够接收一个或多个启用与多个计算机化设备进行通信的假名证书。

[0028] 在一些实施方式中,一种用于置备一个或多个计算机化设备的系统包括:分发器,

该分发器通信连接到计算机化设备,并可操作为接收数字资产并将该数字资产加载到计算机化设备中;数字资产管理系统,该数字资产管理系统经由第一安全通信信道连接到分发器,并可操作为生成数字资产并将该数字资产有条件地传输到分发器;以及置备控制器,该置备控制器经由第二安全通信信道连接到分发器,且经由第三安全通信信道连接到数字资产管理系统,并可操作为指导数字资产管理系统将数字资产传输到分发器。由于不存在数字资产,在将数字资产加载到计算机化设备中之前,计算机化设备可能不运作或仅部分功能运作。数字资产可以是数字证书、加密密钥和可执行软件中的至少一种。在某些实施方式中,所述系统可以与可缩放CMS进行交互或从可缩放CMS接收凭证。

[0029] 在各种实施方式中,所述系统可以进一步包括第二分发器,该第二分发器经由第四安全通信信道连接到数字资产管理系统,且在分发器断连之后通信连接到计算机化设备,并可操作为接收第二数字资产并将第二数字资产加载到计算机化设备中,并且置备控制器进一步可操作为指导数字资产管理系统将第二数字资产传输到分发器。在将第二数字资产加载到计算机化设备中之后,该计算机化设备可以全功能运作。

[0030] 在各种实施方式中,所述数字资产管理系统可以进一步包括:一个或多个运行注册审批机构应用的应用平台,该应用平台通信连接到一个或多个执行注册审批机构应用所需的加密计算的计算引擎;一个或多个运行登记证书颁发机构应用的应用平台,该应用平台通信连接到一个或多个执行登记证书颁发机构应用所需的加密计算的计算引擎;一个或多个运行假名证书颁发机构应用的应用平台,该应用平台通信连接到一个或多个执行假名证书颁发机构应用所需的加密计算的计算引擎;一个或多个运行第一链接权限机构应用的应用平台,该应用平台通信连接到一个或多个执行第一链接权限机构应用所需的加密计算的计算引擎;以及一个或多个运行第二链接权限机构应用的应用平台,该应用平台通信连接到一个或多个执行第二链接权限机构应用所需的加密计算的计算引擎。

[0031] 在其他实施方式中,所述数字资产管理系统可以进一步包括一个或多个数据库,该数据库可操作地连接到一个或多个运行注册审批机构应用的应用平台、一个或多个运行登记证书颁发机构应用的应用平台、一个或多个运行假名证书颁发机构应用的应用平台、一个或多个运行第一链接权限机构应用的应用平台以及一个或多个运行第二链接权限机构应用的应用平台。

[0032] 在另一些其他实施方式中,所述系统可以进一步包括:门户,该门户可操作地连接到置备控制器并认证计算机化设备的制造者且使得该制造者能够管理给计算机化设备的置备;以及/或者门户,该门户可操作地连接到置备控制器并认证计算机化设备的安装者且使得该安装者能够管理给计算机化设备的置备,并且/或者该门户可操作地连接到置备控制器并认证计算机化设备的监管者且使得该监管者能够监管给计算机化设备的置备。

[0033] 在又一些其他实施方式中,置备控制器进一步可操作为将数字资产(例如可执行软件映像)传输到分发器,以加载到计算机化设备中。在还一些其他实施方式中,置备控制器进一步可操作为创建并保留与数字设备相关联且存储有关该数字设备的置备活动的信息的日志,并且分发器进一步可操作为将有关与该数字设备相关的置备活动的信息传输到置备控制器以存储在日志中。

[0034] 在再一些其他实施方式中,置备控制器进一步可操作为在指导数字资产管理系统传输数字资产之前对数字设备进行认证。

附图说明

[0035] 附图纳入说明书并构成说明书一部分,说明本发明实施方式,并结合发明内容来阐释本发明的原理。图中:

[0036] 图1是示出根据本发明实施方式的用于安全置备的系统示例的框图;

[0037] 图2是示出根据本发明实施方式的用于安全置备计算机化设备的过程示例的泳道图;

[0038] 图3是示出根据本发明实施方式的用于安全置备计算机化设备的过程另一示例的泳道图;

[0039] 图4A是根据本发明实施方式的用于通过消息队列实现可缩放且安全的数字资产管理系统的系统示例的第一部分框图;

[0040] 图4B是根据本发明实施方式的用于通过消息队列实现可缩放且安全的证书管理系统的系统示例的第二部分框图;

[0041] 图5A是示出根据本发明实施方式的用于安全提供诸如证书等凭证的过程示例的第一部分泳道图;

[0042] 图5B是示出根据本发明实施方式的用于安全提供诸如证书等凭证的过程示例的第二部分泳道图;

[0043] 图6A是根据本发明实施方式的用于通过双向消息队列实现可缩放且安全的证书管理系统的系统示例的第一部分框图;

[0044] 图6B是根据本发明实施方式的用于通过双向消息队列实现可缩放且安全的证书管理系统的系统示例的第二部分框图;

[0045] 图7A是根据本发明实施方式的用于通过负载均衡器实现可缩放且安全的证书管理系统的系统示例的第一部分框图;

[0046] 图7B是根据本发明实施方式的用于通过负载均衡器实现可缩放且安全的证书管理系统的系统示例的第二部分框图;

[0047] 图8是根据本发明实施方式的用于通过轮询调度请求实现可缩放且安全的证书管理系统的系统示例的框图;

[0048] 图9是根据本发明实施方式的用于通过基于工作负载的请求实现可缩放且安全的证书管理系统的系统示例的框图;

[0049] 图10A是根据本发明实施方式的用于通过消息队列实现可缩放且安全的数字资产管理系统的系统示例的第一部分框图;

[0050] 图10B是根据本发明实施方式的用于通过消息队列实现可缩放且安全的证书管理系统的系统示例的第二部分框图;以及

[0051] 图11是可用于托管根据本发明实施方式的系统和方法的计算系统示例的框图。

具体实施方式

[0052] 现将具体参照本发明的各种实施方式,结合附图说明这些实施方式。简明起见,各附图中使用相同的附图标记指代相同或相似的部分。

[0053] 为了确保在现场进行安全且正确的操作,在制造期间需要通过置备数字资产(诸如安全资产)来正确地初始化嵌入式设备,譬如车用电子控制单元(ECU)。数字资产可包括

各种加密密钥、唯一标识符、数字证书和软件。在多数情形下,这些数字资产和制造工厂的来源位于不同的地理位置,常规上,这些地理位置经由不安全的因特网通信互连。因此,期望创建从这些数字资产的来源到设备的端对端安全信道,使得恶意方或偶然者无法访问或修改数字资产。

[0054] 传统用于端对端保护的网络安全协议(诸如TLS/SSL)的缺陷在于,它们需要预先共享的密钥或某些机密安全材料预先存在于通信双方。这就产生了周期性的技术问题,即,为了置备数字资产,必须预先存在一些初始机密材料。这个问题包括如何保护初始机密材料。该问题对于计算机化设备尤其严重,因为通常在制造期间将单版本的初始软件加载到计算机化设备上以简化物流。如果此初始软件必须包含初始安全材料,则这需要存在全局机密。结果,破坏初始安全材料将导致破坏置备到所有设备上的所有数字资产,因为它们全部共享相同的全局机密。根据本公开的系统、方法和设备解决了常规置备系统的这些及其他问题。

[0055] 置备一般是指为通过适当的数据和软件准备计算机化设备而采取的一组动作。它也可以包括在设备运行环境中正确安装设备以使其准备操作所采取的一组动作。这些动作包括将适当的数字资产(例如操作系统、设备驱动程序、中间件、应用、数字证书等)加载到设备的数字存储(例如存储器)中,并适当地定制并配置设备上的某些数字资产(视需要),这些数字资产可以是每个特定设备的唯一数字资产。这些动作还可以包括验证计算机化设备是由合法设备制造者创建的合法设备,而非副本或伪造设备。

[0056] 这些动作还可以包括将设备正确安装到其操作环境中,以及测试设备以验证其是否正常运行。可能由一个制造者构建设备,随后又由另一个制造者将设备安装到更大型的系统或设备中,例如由零部件制造者构建的板载单元(OBU)可以安装到由汽车制造商制造的汽车中,因此安全置备仅已知良好设备的能力变得复杂化。安装不正确的设备可能无法正常运作。

[0057] 根据本发明的各种实施方式提供了对包括IoT设备在内的计算机化设备的安全置备。这类实施方式用于防止或禁止对计算机化设备使用的数字资产进行恶意、疏忽或错误的篡改、更改、更新或发布,并防止或禁止对计算机化设备及其软件进行错误安装。

[0058] 根据本发明的各种实施方式还可以产生安全置备过程中可用于分析和解决以后发现问题的审计日志、记录、报告等。

[0059] 根据本发明的各种实施方式还可以提供可作为服务提供给设备和系统制造者的安全置备和管理平台。

[0060] 图1是示出根据本发明实施方式的用于安全置备计算机化设备的系统100示例的框图。如图1中的示例所示,系统100包括置备控制器120。置备控制器120可以实施为服务器计算机(例如具有至少一个处理器和相关联的存储器),其嵌入式硬件安全模块(HSM)安全生成并存储数字安全资产并安全执行各种加密和敏感计算。HSM保护数字安全资产(诸如加密密钥)和其他敏感数据免遭攻击者可能访问。在各种实施方式中,置备控制器120运作为:认证系统100的用户并与其安全通信;与一个或多个分发器108、131安全通信并对其进行管理;与数字资产管理系统(DAMS)110安全通信并指导其操作;创建并存储置备记录;创建、存储并分发置备记录;创建、存储并分发审计日志;创建并分发证书,以加密方式将DAMS110与分发器108、131元素绑定在一起;如果用户和受管设备不再受信任,则视需要将其撤消;以

及创建并分发关键密钥和数据的安全加密备份,以供异地存储,从而实现业务连续性和灾难恢复。

[0061] 如图1中的示例所示,置备控制器120通信连接到数据库125,该数据库125可以存储有关安全置备设备106a、106b(可统称106)的数据、信息和数字资产。

[0062] 置备控制器120还安全通信连接到制造者的用户门户115,该用户门户115可以例如实施为服务器或置备控制器120的接口。在各种实施方式中,设备制造者105的员工109可以使用制造者的用户门户115与置备控制器120(因此与DAMS 110)对接并管理其设备置备活动。在各种实施方式中,制造者的用户门户115可以从员工用户109收集标识信息,诸如用户名、密码、双因素标识数据、面部识别图像、指纹等,并将标识信息提供给置备控制器120。置备控制器120可以在允许员工109访问安全置备系统100之前对员工109进行认证。例如,置备控制器120可以查找与员工用户109相关联且先前已经验证并存储在其数据库125中的标识信息,并将所存储的标识信息与制造者的用户门户115所收集的标识信息进行比较。替代地,置备控制器120或DAMS的用户门户115可以与用户的企业标识和认证系统集成,这将确定员工109是否获授权使用系统100。在各种实施方式中,置备控制器120或DAMS的用户门户115可以为成功认证的员工109赋予角色,以将他们的动作约束在系统100内。在一些实施方式中,仅当两组识别信息匹配,置备控制器120才会允许访问。

[0063] 类似地,置备控制器120还通信连接到安装者的用户门户116,该用户门户116可以例如实施为服务器或置备控制器120的接口。在各种实施方式中,设备安装者的员工132可以使用安装者的用户门户116与置备控制器120(因此与DAMS110)对接并管理其设备安装和置备活动。置备控制器120可以在允许员工132之前对员工132进行认证,并在允许员工132访问安全置备系统100且对系统执行授权功能之前为他们分配角色。

[0064] 同样类似地,置备控制器120还通信连接到监管者门户117,该门户117可以例如实施为服务器或置备控制器120的接口。在各种实施方式中,监管者140一旦获置备控制器120认证,便可使用监管者门户117与置备控制器120对接并管理对制造者104、安装者130、设备106和/或安装在设备106中的软件/数字资产的审查和批准。置备控制器120可以在允许监管者140访问安全置备系统100之前对监管者140进行认证。在系统100的一些实施方式中,监管者140和监管者门户117可为任选。

[0065] 置备控制器120进一步通信连接到DAMS110。在各种实施方式中,DAMS 110可以实施为服务器、设备或者安全装置和/或服务器的系统。DAMS110经由分发器108、131或其他安全且经认证的连接从待置备的终端实体设备安全检索公钥,并安全供应安装在设备106中的数字证书和相关数据。此外,DAMS110经由分发器108、131从制造者105和安装者130安全接收关于计算机化设备106的置备、安装、功能等的状态信息。此外,如图1所示,DAMS110可以在单个站点或多个站点执行此置备。如参照图2详述,DAMS110可以包括以下主要元素:根证书颁发机构(CA)、策略生成器、CRL生成器、失当行为权限机构、中间CA、登记CA、链接权限机构、假名CA和注册审批机构。

[0066] DAMS110添加了新功能,并改进了William Whyte等人于2013年12月在2013年IEEE车辆联网会议(VNC)发表的论文“用于V2V通信的安全凭证管理系统(A Secure Credential Management System for V2V Communications)”中描述的部件和功能。在各种实施方式中,DAMS110包括多阶段编程和灵活管理(例如允许包含监管者140)。DAMS110的各种实施方

式还启用允许单个DAMS110向不同的订户提供不同级别的置备的能力。DAMS110的各种实施方式还启用允许订户在一个时间段内(例如每周)分配不同的数字证书使用以及不同的证书负载(诸如一周,而非常规系统中的三年)的能力。DAMS110的各种实施方式还可以提供特定于订户的URL,以便特定制造者的计算机化设备106(例如OEM的车辆)能够停留在制造者的范围内(例如其URL显示其名称)。

[0067] 如图所示,置备控制器120还通信连接到分发器108、131。在各种实施方式中,分发器108、131可以实施为安装在公司场所(如图所示)的独立安全装置,或者实施为Web或云服务等。在各种实施方式中,分发器108、131实施为可信端点设备,该可信端点设备优选地经由专用的非因特网通信信道往返于DAMS 110和置备控制器120安全地传输和接收数字资产和其他信息。如图所示,分发器108、131也直接或间接地连接到设备106a、106b,以便将数字资产下载到设备106a、106b并从设备106a、106b接收数据。在各种实施方式中,分发器108、131能够实施为包括服务器计算机(例如具有至少一个处理器和相关联的存储器)的电器箱,其中包括硬件安全模块(HSM)、强化操作系统(OS)、内部防火墙和内部主机入侵检测/防御系统。分发器可以专门设计为在不受信任的环境中进行操作,但仍提供可信且可靠的操作。分发器在其自身与安全置备控制器120和DAMS110之间具有安全的通信信道。该信道用于控制分发器以及发送并检索置备相关的数据和日志信息。分发器还可以具有到测试器107的安全通信信道,用于对设备106进行编程或置备。该信道防止置备数据和日志数据在制造地点的通信网络上遭受泄露或修改。分发器108还可以直接与待编程的设备106建立安全通信信道,使得置备数据不会受到第三方(包括流氓测试器107)破坏或修改。在各种实施方式中,分发器可以从待其置备的设备106收集公钥和其他数据,诸如微处理器序列号。它可以将该信息发送到置备控制器120和/或DAMS 110。它还可以接受来自置备控制器120和/或DAMS110的数据和命令以及其他信息以编程到设备106中。它可以返回其自己的日志数据,并且它可以将来自测试器107的数据返回到置备控制器120和/或DAMS110。

[0068] 如参照设备制造者105所示,分发器108可以通信连接到测试器107(例如计算机化制造设备、产品测试设备等),该测试器107又连接到由制造者105生产的设备106a,诸如OBU设备。制造者105可以包括或可以是制造和/或向市场供应计算机化设备106a的工厂。举许多可行示例之一,计算机化设备106a可以是嵌入式通用集成电路卡(eUICC),其用于电信用蜂窝调制解调器,合并为板载单元(OBU)的一部分,其随后安装在汽车中,以便汽车与交通基础设施设备之间进行通信。它也可以是安装在OBU中的V2V安全微处理器,以便与其他车辆和路侧单元(RSU)进行通信。这些新制造的设备106a必须正确地置备有数字资产,例如来自DAMS110的数字证书,以便正确操作。制造者105的员工109可以使用用户门户115与置备控制器120进行交互,并通过DAMS110管理产品置备活动。

[0069] 如参照安装者130所示,在设备106b安装在其操作环境中之时或之后,分发器131可以备选地直接通信连接到设备106b。安装者130可以包括或可以是计算机化设备106b安装到其操作环境中的工厂或商店,例如,将OBU安装到汽车中。安装时,必须为计算机化设备106b进一步正确置备数字资产,例如来自DAMS 110的附加数字证书,以便正确操作。安装者130的员工132可以使用安装者的用户门户116与置备控制器120进行交互,并通过DAMS110管理产品置备活动。

[0070] 在各种实施方式中,置备控制器120、分发器108、131和DAMS110可以在它们之间具

有不可公开访问的安全通信链路或信道,并且在各种实施方案中,图1所示的所有通信链路可以是不可公开访问的安全通信信道。在各种实施方式中,这些安全信道被加密并相互认证,以防止未授权的端点在该安全基础设施内进行通信。可以使用多种安全机制来保护这些通信信道,以便如果外层受到某种程度的破坏,则内层将保持安全。举例而言,相互认证的TLS隧道可以用作外层,内层使用另一协议,诸如专属安全通信协议。包括系统100的基础设施部件之间的这些安全连接用于保护部件之间的敏感通信并确保它们正确操作。通过使用这些安全路径,置备控制器120和DAMS110能够在部件之间发送数字数据,而不必担心它在传输中受到破坏或修改。也可以通过这些信道传递命令和控制信息。譬如,置备控制器120能够控制将某些数字资产和数据发送到哪个分发器108、131。它也能指令分发器108、131如何将该数据计量给正置备的生产线上的设备106。另外,分发器108、131能够将信息报告回置备控制器120,而不必担心它在传输中受到破坏或修改。例如,安全置备控制器120能够对分发器108、131进行编程,以利用任何类型的数字资产(例如证书、软件、FUSE内容等)来置备多达10000个设备。分发器108、131能够对其正置备的设备进行计数,当置备达到其极限时,它将此报告给置备控制器120。在各种实施方式中,由置备控制器120管理的设备(例如108、110、131、115、116、117)包括如果这些设备不定期与置备控制器120进行通信则促使它们停止操作的功能;因此,如果这些设备被盗,则它们将变得无用。此功能防止丢失/被盗的设备犹如仍位于正确的制造环境一样继续操作并置备设备106。

[0071] 继续参照图1所示的示例,在操作中,位于制造者105处的分发器108从DAMS110安全接收数字资产,并将这些数字资产供应给设备106a的测试器107。当制造者105制造每个设备106a时,测试器107与设备106a进行通信以从设备106a获取信息,诸如其唯一标识号和状态,以及将数字资产下载或以其他方式安装到设备中,诸如数字证书。测试器107还可以将来自设备106a的信息(例如置备状态)供应给分发器108,该分发器108将该信息安全通信到DAMS110和/或置备控制器120。在一些实施方式中,测试器107可以包括软件传输层安全(TLS)代理,该代理在分发器108与设备106a之间安全传输数据,实际上通过使用与每个设备106a相关联的短钥经由分发器108和测试器107在DAMS110与设备106a之间创建安全的加密通信路径。

[0072] 在初始置备设备106之后,制造者105将该设备106a运送到安装者130,该安装者130安装设备106b。在各种实施方式中,在初始置备设备106a之前,该设备106a不运作;而在制造者105初始置备设备106a之后,该设备106a能够部分功能运作,但尚未全功能运作。在这类实施方式中,初始置备使设备仅在安装和进一步最终置备所需的程度上运作,这是使其完全操作所必需的条件。

[0073] 安装者130将设备106b安装到其操作环境中,并且安装者130的员工132经由安装者门户116将这一事实通知给置备控制器120。该通知证明已正确完成安装,并优选地包括向置备控制器120唯一标识设备106b的信息。在一些实施方式中,分发器131可以在向设备106b查询状态和标识信息之后自动通知置备控制器120。在安装者130经由安装者门户116证明他已经正确安装设备106b的各种实施方式中,该证明可以由置备控制器120记录/保存到数据库125中。该证明可以包括有关每个特定安装设备106b的特定测试数据,诸如无线电发射功率测量或GPS天线位置验证。

[0074] 响应于安装通知,置备控制器120验证:(i)设备106b在其数据库125中列为由制造

者105合法制造的设备；(ii) 设备106b在其数据库125中列为已由制造者105成功地初始置备；以及(iii) 安装者130在其数据库125中列为授权安装者。如果该验证成功，则控制器120指导DAMS110发送数字资产(例如假名证书

[0075] (PC))和/或可操作地置备设备106b所需的其它信息，使得设备106b安装到其操作环境中时能够正确运作。

[0076] 在各种实施方式中，监管者140经由监管者门户117与置备控制器120进行交互，以标识、验证和管理安装者130和/或制造者105，使得未经授权的安装者(例如黑客)无法从系统100中获得真实的数字资产。监管者140的员工可以由置备控制器120进行认证，并可以与系统100具有唯一ID，从而能够唯一记录他们的动作。在各种实施方式中，监管者140可以使用监管者门户117来查询置备控制器120，以获得由控制器120记录的信息的副本和报告，诸如证明报告、安装者动作、已制造的设备106a的数目和身份、已安装的完全置备的设备106b的数目和身份等。

[0077] 在各种实施方式中，安装者130必须被置备控制器120认证为已授权，以便与系统100进行交互。为了获得授权，安装者130例如可能必须执行适当的合约文件，声明他们将在目标环境(例如目标车辆或站点等)中正确安装设备106b。监管者140可以例如要求安装者130证明其他合约要素。优选地，每个安装者130在系统100内具有唯一ID，使得他们的动作能够被置备控制器120唯一记录。

[0078] 所描述的系统100及其功能的实施方式能够确保仅对由制造者105制造并由授权安装者130正确安装和测试的设备106充分置备有使设备106进行操作所需的数字资产。置备控制器120产生大量日志并报告在置备过程中的每个阶段由何者采取了何行动，从而提供了常规系统所不具备的关键审计能力。

[0079] 本领域普通技术人员会认识到，图1所示的部件、过程、数据、操作和实施细节皆为解释简明清楚而呈现的示例。在不背离本发明原理的情况下，可使用其他部件、过程、实施细节和变型，因该示例并非旨在限制，而是可能存在许多变型。例如，尽管图1示出仅一个制造者105、仅一个安装者130和仅一个监管者140，但其他实施方式可具有任意数目的这些实体中的每一个。对于另一示例，尽管将DAMS110和置备控制器120示为分立的设备，但其他实施方式可以将它们的功能组合到单个设备(例如单个服务器)中。作为又一示例，这一点同样可适用于门户115-117。对于还一示例，系统100可额外包括资产管理装置

[0080] (AMA，未示出)，参阅申请日为2016年11月14日、申请号为US 62/421,852的美国临时申请，其内容通过引用归并本文。在这样的实施方式中，AMA可以通信连接到置备控制器120和/或分发器108、131和/或DAMS110。在各种实施方式中，AMA可以包括用户友好的GUI和功能，其允许生产协调员简单有效地管理产品(例如设备106)的配置和构建，并允许资产所有者简单有效地管理数字资产的库存。

[0081] 图2是示出根据本发明实施方式的用于安全置备计算机化设备的过程200示例的泳道图。在各种实施方式中，所示的某些或全部过程200或操作可以通过由纯硬件系统或两者兼备的系统在通用计算系统(其可以包括一个或多个处理器或者一个或多个计算子系统)上执行代码来执行。如图2的上方所示，过程200所涉及的实体包括计算机化设备106的制造者105、位于制造者105处的分发器108、置备控制器120和DAMS110。在各种实施方式中，这些实体可以是如参照图1及贯穿本公开所描述的实体，并可以彼此通信。

[0082] 如图2中的示例所示,过程200开始于205,制造者105(例如员工109)向置备控制器130请求数字资产置备服务,其中数字资产将被置备给设备106a(例如供其使用),并且请求可以标识作为数字资产的目的地的设备106a。该请求可以是,例如,制造者105可以正请求针对新产品106A的置备服务,或者对现有产品106B发出新的置备服务请求。在各种实施方式中,该操作可涉及例如经由用户门户115登录到置备控制器130的授权用户。在某些情形下,所请求的数字资产可以是:安全凭证,诸如登记证书;设备106要运行的可执行代码;数字操作参数;等等。登记证书是一种将其持有者标识为生态系统中的授权参与者的公钥证书,在该生态系统(诸如USDOT的V2X生态系统)中,所有参与者皆须共享有效的登记证书,并且授权参与者还能接收假名证书,这些假名证书使得生态系统内的设备106能够进行通信和操作(例如在USDOT的V2X生态系统的示例中,使得车辆与路侧基础设施之间能够进行通信和操作)。

[0083] 在210,置备控制器120判定来自制造者109的用户是否是授权用户。在一些实施方式中,在210,置备控制器120还可以判定待置备的设备106a(例如产品)是否获准与系统100配合使用。在某些情形下,获准设备的清单可以由图1中的监管者140提供,并供置备控制器120用来进行这种判定。

[0084] 如果用户(和/或产品)未经授权,则置备控制器120拒绝对数字资产置备服务的请求(图2未示出)。另一方面,如果授权用户(例如对于授权产品)作出请求(210,是),则置备控制器120指导、指令或以其他方式控制DAMS110履行服务请求,譬如,这是通过向DAMS110传输服务请求指令(在215)。

[0085] 在220,响应于且基于从215接收到请求的条件,DAMS110基于该请求将其自身配置为开始对设备106a的服务。在一些实施方式中,DAMS110还可以向分发器108发送(未示出)指令,以将分发器108配置为服务于设备106a。

[0086] 在222,DAMS110根据205处的请求而为设备106a生成、创建、计算和/或检索数字资产。在各种实施方式中,DAMS110可以创建或生成所请求的数字安全资产,诸如公钥与私钥对以及设备106a的登记证书和假名证书。

[0087] 在操作222的备选实施方式中(图2中未示出),DAMS110从分发器108请求并接收与设备106a相关联的数字资产生成信息,诸如由设备106a生成并从设备106a检索到的登记和假名公钥以及唯一标识设备106a的数据(例如微处理器序列号)。在这样的实施方式中,DAMS110则使用登记和假名公钥来生成数字资产,例如,设备106a的登记证书和合适数目的假名证书。

[0088] 在225,DAMS110将数字资产传输到在205请求数字资产服务的制造者105的分发器108。例如,DAMS110可以将公钥与私钥对、登记证书和假名证书安全传输到制造者105的分发器108。

[0089] 在226,DAMS110将关于数字资产的日志信息传输到置备控制器120。在各种实施方式中,日志信息可以包括描述数字资产的请求和转移的信息,诸如请求者ID、数字资产ID、分发器ID、请求和传输动作的时间戳、接收到的微处理器序列号等。在一些实施方式中,日志信息可以包括数字资产副本。在227,置备控制器120接收日志信息并将该日志信息存储在例如数据库125中。置备控制器120实际上保留对系统100中发生的所有活动的审计追踪,这就允许汇编多种类型的数据,诸如关于制造者105如何及何时构建和置备设备106a的数

据。这样的数据和日志信息可以用于计费以及审计目的。

[0090] 在230,分发器108接收并存储由DAMS110发送的数字资产(例如公钥与私钥对、登记证书和假名证书)。

[0091] 在235,分发器108从设备106a请求并接收数字安全资产,诸如公钥,其能够用于将数字资产从分发器108安全转移到设备106a。各种类型的设备106a能够使用设备106中内置的安全处理器来生成短钥对,并且公钥可以是该短钥对的一部分。在240,分发器108使用数字安全资产(例如公钥)将数字资产(例如登记证书)安全传输到设备106a。在各种实施方式中,分发器108可以使用设备106a的公钥与设备106a形成例如虚拟专用网(VPN),并在其中安全传输数字资产。

[0092] 在各种实施方式中,分发器108可以在其与测试器107之间采用传输层安全

[0093] (TLS)以保证与可以连接到设备106a的测试器107安全通信。在期望直接与设备106a安全通信的实施方式中,所述系统可以对设备106a创建短期公钥对,并使用公钥以及来自分发器108的证书(包含分发器108的公钥)来创建到设备106a的安全隧道。在这样的实施方式中,设备106a将运行带有系统100根公钥的特殊代码,以验证分发器108发送给它的证书。

[0094] 一旦在设备106a或测试器107与分发器108之间建立了安全路径,设备106a便能创建登记与假名公钥对(例如针对V2X生态系统)并将公钥和其他数据导出到分发器108,然后分发器108便能将该数据发送到DAMS110和置备控制器120。如上参照操作222的替选实施方式所述,DAMS110可以使用接收到的公钥来创建登记证书和假名证书,在一些实施方式中,可能存在大量假名证书(例如3000个)。在一种实施方式的替选例中,在操作225,如前所述,DAMS110将这些证书返回给分发器108。在一些其他实施方式中,根据在何处执行置备,DAMS110可以将这些证书传输到分发器131而非分发器108。

[0095] 在一些实施方式中,例如,如果设备106具有其自己的无线或有线通信功能且至少部分地可操作,则分发器108可以与设备106直接通信。在其他实施方式中,分发器108可以经由诸如测试器107的中间设备与设备106间接通信。

[0096] 设备106a接收数字资产并存储该数字资产,以供操作期间使用。例如,如果设备106a是汽车板载单元(OBU)或电子控制单元(ECU),并且数字资产是加入无线网络所需的安全资产(例如公钥证书),则由OBU存储数字安全资产。稍后在汽车中安装并激活OBU时,它将尝试连接到无线网络。在允许OBU连接到网络之前,网络将尝试对OBU进行认证。仅当OBU具有制造者105处的分发器108所提供的数字安全资产,该OBU才能进行认证并加入网络。

[0097] 在245,分发器108从设备106a接收或访问状态信息,该状态信息指示设备106a是否成功接收和安装(例如存储)在240传输的数字资产。

[0098] 在250,分发器108将状态信息传输到置备控制器120。而且,在255,置备控制器120接收并存储与操作227中所存储的日志信息相关联的状态信息。因此,置备控制器120继续针对与每个特定设备106相关联的所有系统100活动的审计跟踪或审计日志。在各种实施方式中,审计日志可以包含:针对每个设备106的指示信息;制造者置备的成功或失败(例如操作235-245);数字资产的身份(和/或数字资产本身的副本);密码类型;等等。

[0099] 在270,如果成功为设备106a置备数字资产,则制造者105将设备发布到市场。例如,制造公司105可以将设备106a物理上运送到要在其操作环境中安装设备的公司(例如图

1中的安装公司130)。在一些实施方式中,设备106a在此时间点可以被完全编程或置备,并能够全功能运作;而在其他实施方式中,设备106a在此时间点可以仅被部分编程或置备,或者不能全功能运作或不运作。

[0100] 图2中描绘的示例仅出于说明目的,而非旨在限制。另外,所描绘过程200的示例目的在于简明清楚地解释符合本公开某些实施方式的某些新颖性和创新性特征,但该示例并非旨在限制,而是可能存在许多变型。例如,虽然图示为以特定顺序执行功能和操作,但所描述的顺序仅作参考,能够执行符合本公开的某些实施方式的各种不同操作顺列。此外,仅出于说明目的,将操作描述为分立的步骤,而在一些实施方式中,多个操作可以同时执行和/或作为单个计算或更大操作的一部分来执行。所描述的操作并非旨在穷举、限制或绝对意义,并且能够修改、插入或删除各种操作。举变型示例,尽管图2大体上以单个数字资产(例如单个数字证书)的上下文来描述,但所述系统和过程将类似地运作为处理多个数字资产(例如两个以上数字证书)。另如,在设备106a不具备安全通信能力的情形下,可省去操作235和240,并且分发器108可使用未加密的通信与设备106b进行通信。

[0101] 再如,在各种实施方式中,置备控制器120或授权机构(诸如专门的签名器)可以类似地传输到分发器108,并使其将另一或附加的数字资产加载到设备106b中,包括诸如软件、固件、FUSE对象、清单文件等数字资产。在这样的实施方式中,置备控制器120可以附加地或替代地从存储中检索、获得或以其他方式访问所请求的数字资产或者指导对所请求的数字资产的访问。例如(图2未示出),置备控制器120或其授权代理可以检索待加载到设备106a中并由设备106a运行的可执行软件映像(例如存储在数据库125中的编译计算机程序),并将该可执行软件映像发送到分发器10以编程到设备中。在各种实施方式中,由置备控制器120访问的数字资产可以仅包含由设备106a的制造者105安全供应、发布和/或授权的软件等,从而不会将任何未授权的软件加载到设备106a中。在一些实施方式中,由置备控制器120检索到的数字资产可以存储在与置备控制器120相关联的存储设备或数据库中,诸如图1的数据库125中。

[0102] 图3是示出根据本发明实施方式的用于安全置备计算机化设备的过程200示例的泳道图。在各种实施方式中,所示的某些或全部过程300或操作可以通过由纯硬件系统或两者兼备的系统在通用计算系统(其可以包括一个或多个处理器或者一个或多个计算子系统)上执行代码来执行。如图3的上方所示,过程300所涉及的实体包括计算机化设备106的安装者130、位于安装者130处的分发器131、置备控制器120和DAMS110。在各种实施方式中,这些实体可以是如参照图1及贯穿本公开所描述的实体,并可以彼此通信。

[0103] 如图3中的示例所示,过程300开始于305,安装者130接收由制造者105制造并发布或运输的设备106b(例如OBU或ECU)(参见图2中的操作270)。在310,安装者130可以将设备106b安装到其操作环境中,诸如安装到更大型的系统中。例如,安装者130可以从制造者105购置OBU的汽车制造商,并且安装者130可以将OBU安装到汽车中。在各种实施方式中,安装设备106b可以包括在安装之后测试设备106b的操作、功能等以及收集相关的状态数据。

[0104] 在一些实施方式中,设备106b可以仅被部分地置备且不全功能运作。例如,设备106b的制造者105可以仅为设备106b置备登记证书,使得设备106b需要被进一步置备有另一数字证书,诸如假名证书,以便获得全功能,例如与另一个全编程的设备106通信的功能。

[0105] 在315,安装者130(例如员工132)将安装状态数据传输到置备控制器120。在各种

实施方式中,安装状态数据包括已安装设备的不变标识符,例如序列号或其他固定的唯一标识信息,诸如密钥对中一旦生成就永不擦除的公钥。安装状态数据还可以包括其他信息,诸如安装者130的唯一标识符、指示如何及何时安装设备106b的信息、关于已安装设备106b上完成的测试结果的信息、证明安装者130根据适用规范安装设备106b的信息、合约要求和/或指令和/或其他类似信息。

[0106] 在320,置备控制器120判定来自安装者130的用户是否是授权用户。若否,则置备控制器120拒绝安装状态通信(图3未示出)。另一方面,如果授权用户正发出请求(320,是),则置备控制器120判定(325)安装状态数据中标识出的设备106b是否是授权设备。在一些实施方式中,置备控制器120可以确定设备106b已授权,这是通过针对先前存储在其数据库125中的信息来验证:1)其数据库125中存在设备106b的记录;2)该记录指示设备106b已在制造者105处成功置备;3)该记录指示设备106b已发送到安装者130(其已在320验证为授权安装者)。

[0107] 如果在安装状态数据中标识的设备未授权,则置备控制器120拒绝安装状态通信(图3未示出)。另一方面,如果在安装状态数据中标识的设备106b已授权(325,是),则在330,置备控制器120存储安装状态数据以及与设备106b相关联的日志信息。例如,如参照图2中的操作227所述,与设备106b相关联的日志信息可能先前已存储在数据库125中。

[0108] 在335,置备控制器120例如通过向DAMS110传输置备安装者130处的设备106b的请求而指导、指令或以其他方式控制DAMS110来履行置备请求。在340,响应于且基于从335接收到请求的条件下,DAMS110生成和/或检索在335所请求的数字资产。在各种实施方式中,如参照图2所述,DAMS110可以创建或生成所请求的数字资产,诸如假名证书或其他公钥证书。在各种实施方式中,DAMS 110或者置备控制器120而非DAMS110可以附加地或替选地从存储中检索、获取或以其他方式访问所请求的数字资产,诸如先前存储在数据库125中的可执行映像,以供设备106b类型的设备中使用。

[0109] 在345,DAMS110将数字资产传输到在315已传输安装状态的安装者130的分发器131。例如,DAMS110可以将假名证书安全传输到安装者130的分发器131。

[0110] 在350,分发器131执行与如参照图2所述的操作230-245相同或相似的操作。在355,分发器131将状态信息传输到置备控制器120。而且,在360,置备控制器120接收并存储与先前存储的有关设备106b的信息相关联的状态信息,诸如在操作227中存储的状态信息。因此,置备控制器120继续针对与每个特定设备106相关联的所有系统100活动的审计跟踪或审计日志。

[0111] 图3中描绘的过程300示例仅出于说明目的,而非旨在限制。另外,所描绘过程300的示例目的在于简明清楚地解释符合本公开某些实施方式的某些新颖性和创新性特征,而是可能存在许多变型。例如,虽然图示为以特定顺序执行功能和操作,但所描述的顺序仅作为示例,能够执行符合本公开某些实施方式的各种不同操作顺列。此外,仅出于说明目的,将操作描述为分立的步骤,而在一些实施方式中,多个操作可以同时执行和/或作为单个计算或更大操作的一部分来执行。所描述的操作并非旨在穷举、限制或绝对意义,并且能够修改、插入或删除各种操作。

[0112] 图4A和图4B是根据本发明实施方式的用于实现可缩放且安全的证书管理系统(CMS)400的示例架构框图。可缩放CMS 400的各种实施方式可以用于超大量的设备进行交

易和证书生成处理。在各种实施方式中,可缩放CMS 400可以使用多个服务器、HSM、多个计算机或计算引擎以及多个应用平台来实现。在图4A和图4B所示的示例实施方式中,应用平台可以均包括一个或多个虚拟机

[0113] (VM)。在附加或替选的实施方式中,应用平台可以均包括一个或多个硬件平台,例如,能够托管和执行软件应用的应用服务器、计算机或其他计算机硬件。在图4A和图4B的示例中,用于登记证书颁发机构的应用平台430可以是一个或多个运行登记证书颁发机构应用的VM,而用于假名证书颁发机构的应用平台440可以是一个或多个可操作为托管并运行假名证书颁发机构应用的VM。类似地,用于第一链接权限机构的应用平台450可以是一个或多个配置为托管并运行第一链接权限机构应用的VM,而用于第二链接权限机构的应用平台460可以是一个或多个可操作为托管并运行第二链接权限机构应用的VM。可缩放CMS 400的示例可以在私有数据中心、诸如来自亚马逊的Amazon Web服务(AWS)的云数据中心或私有数据中心与云数据中心的混合中心中实现。

[0114] 在一些实施方式中,可缩放CMS 400可以提供安全证书,例如登记证书和假名证书,以供制造者105的分发器108使用,其可以如参照图1和本公开其他部分描述的那样运作。在某些实施方式中,可缩放CMS 400可以与上文参照图1描述的数字资产管理系统(DAMS)110进行交互,以便向分发器108提供证书。

[0115] 如图4A中的示例所示,CMS 400的架构可以包括两个置备控制器120,即主要置备控制器和备用置备控制器,它们优选在单独的服务器中实现。这两个置备控制器120包括使得主要置备控制器中所包含的对象、数据等被复制或其他方式包含在备用(次要)置备控制器中的功能。如果主要置备控制器因任何原因脱机,则备用置备控制器可以联机以替代主要置备控制器。这就提供了置备控制器120的连续可用性(或极高可用性)。在各种实施方式中,主要置备控制器和备用置备控制器可以如参照图1和本公开其他部分所描述。在各种实施方式中,置备控制器120可以采用与本文参照图1中置备控制器120与制造者的分发器108之间的连接和通信所述相同或相似的方式连接到可缩放CMS 400。

[0116] 一般而言,置备控制器120管理包括基础设施的系统元素,使得只有明确授权的元素才能参与到可缩放CMS 400并与之交互。在各种实施方式中,置备控制器120可以与用户(例如制造者105或安装者130)的雇员识别和授权系统集成,或者它可以提供其自己的识别和授权能力,从而只有授权用户才能使用可缩放CMS 400。在一些实施方式中,置备控制器120可以是设备生命周期管理(DLM)控制器,例如主要DLM控制器和备用DLM控制器。在各种实施方式中,置备控制器120可以是按部件类型存在于CMS 400中的控制器。例如,在图4A和图4B中,置备控制器120可以是针对注册审批机构420、登记证书颁发机构430、假名证书颁发机构440和链接权限机构450、460存在的一组或一对控制器。

[0117] 如图4A和图4B所示,可缩放CMS 400的架构包括实施为表述性状态转移

[0118] (REST) Web服务的注册审批机构405、注册审批机构420、注册审批机构计算引擎425、登记证书颁发机构430、登记证书颁发机构计算引擎435、假名证书颁发机构440、假名证书颁发机构计算引擎445、第一链接权限机构450、第一链接权限机构计算引擎455、第二链接权限机构460、第一链接权限机构计算引擎465、消息队列410、411、412、413、414、415、416、417、418、419以及一个或多个数据库470。下述段落介绍了这些部件中的每一个。

[0119] 可缩放CMS 400的架构有利地区分非安全相关应用与安全功能。如图4A和图4B中

的示例所示,注册审批机构420、登记证书颁发机构430、假名证书颁发机构440和链接权限机构450、460实施为它们自己VM上的应用,这些VM在它们自己的专用计算引擎425、435、445、455和465上执行,所有这些计算引擎均与任何非安全相关的应用和功能分离。这样相比常规系统更具技术和安全优势及改进,在常规系统中,HSM的性能更慢,云服务提供者无法供应HSM,或者无法确定系统对HSM的正确管理。在可缩放CMS 400中,在计算引擎(例如计算引擎425、435、445、455和465中的一个或多个)中执行所有需要HSM的加密操作。

[0120] 如图4A和图4B所示,通过将关键的安全功能彼此分离并分离到单独的计算引擎上,例如,由注册审批机构420、登记证书颁发机构430、假名证书颁发机构440和链接权限机构450、460执行的计算密集型加密和安全功能(例如椭圆曲线蝶形展开计算或椭圆曲线数字签名)的执行比现有注册审批机构系统快得多。通过使得“瓶颈”应用可视需要单独缩放,这种设计能够显著改善事务处理。照此,根据本公开的实施方式提供了具有技术优势的特定系统架构,能够减少现有注册审批机构系统相关的瓶颈。譬如,如果注册审批机构405和420上运行的注册审批机构应用需要缩放,则能添加额外的VM,而无需对注册审批机构计算引擎425的安全计算能力作出任何更改。备选地,如果安全计算正在限制性能,则能添加额外的安全注册审批机构计算引擎425。同样的多维缩放也适用于CMS 400的其他部件。与现有的安全凭证管理系统(SCMS)相比,这些能力能够提供显著的性能改进和可缩放性。

[0121] 在图4A和图4B所示的示例中,通过消息子系统或消息列队服务,包括输入消息队列410、411、412、413、414、415、416、417、418和419,注册审批机构405连接到其他部件,且其他部件相互连接。在图4A和图4B的示例实施方式中,输入消息队列410、411、412、413、414、415、416、417、418和419是单向队列,因为这些队列中的消息单向流动(例如从客户端到服务器)。通过为每个VM和计算引擎使用单个输入队列,可以提供简化的技术优势。

[0122] 在一些实施方式中,消息传递服务可以是快速消息列队服务,例如,由Amazon Web 服务提供的亚马逊简单队列服务(SQS)。譬如,根据这样的实施方式,消息队列410、411、412、413、414、415、416、417、418和419可以是SQS消息队列。通过使用输入消息队列410、411、412、413、414、415、416、417、418、419使应用VM与计算引擎彼此通信连接,能够视需要独立地缩放应用VM和计算引擎。换言之,由于用于注册审批机构420、登记证书颁发机构430、假名证书颁发机构440和链接权限机构450、460的各应用平台经由各组输入消息队列通信连接到计算引擎425、435、445、455和465,CMS 400的这些部件以及数据库470皆彼此独立地缩放。

[0123] 如上文所述及图4A和图4B中的非限制性示例所示,注册审批机构405、420、证书颁发机构430、440以及链接权限机构450、460中的每一个可以实施为它们自己虚拟机(VM)上的应用。在附加或备选的实施方式中,注册审批机构405、420、证书颁发机构430、440以及链接权限机构450、460中的一个或多个可以在硬件平台(例如服务器或计算引擎)上执行。下述段落中描述了在应用平台(例如VM或硬件平台)上执行的每个应用的作用和功能。

[0124] 在各种实施方式中,注册审批机构405可以是置备网络中的机构,其验证用户对数字证书或其他类型数字安全资产的请求,并启用证书颁发机构(例如登记证书颁发机构430和假名证书颁发机构440)签发数字证书。在各种实施方式中,注册审批机构405可以类似于公钥基础设施(PKI)系统中已知的注册审批机构。在各种实施方式中,注册审批机构405可以实施为表述性状态转移(REST)Web服务。如图4A示出的用于注册审批机构405的三个“堆

叠”矩形所表示,在各种实施方式中,可能存在多例注册审批机构405同时执行。图4A和图4B的其他“堆叠”元素采用类似的表示。CMS 400的注册审批机构功能为非集中式,因为其功能能够由实施为REST Web服务的多例注册审批机构405和多例注册审批机构420来执行。注册审批机构405、420的主要作用是在签署假名证书颁发机构440不知道哪些证书最终出现在特定计算机化设备中的同时,授予并履行证书置备请求。注册审批机构405、420经由消息队列414、416和418直接与假名证书颁发机构440、链接权限机构450、460进行交互,以便履行它们在CMS 400中的作用。

[0125] 如矩形左下角出现的“DB”箭头所表示,注册审批机构405 (以及图4A和图4B中其他由“DB”箭头示出的部件)可以连接到各自的数据库470。尽管图4A中仅示出单个数据库470,但应当理解,CMS 400可以利用数据存储区或数据库470的集合来进行数据存储和检索。例如,数据库470可以由一个或多个数据库逻辑或物理单元组成,每个逻辑或物理单元具有一个或多个表单,从而在需要时实现数据分离。如本文所用,术语“数据库”是指一个或多个数据库或数据存储区。在某些实施方式中,使用多个数据库470允许注册审批机构405与图4A和图4B中用“DB”箭头示出的其他部件之间的数据分离。例如,这样使用多个数据库470允许注册审批机构405、420、证书颁发机构430、440和链接权限机构450、460之间的数据分离。

[0126] 在优选实施方式中,数据库470是一个或多个快速访问的低延迟数据库的集合。在一些实施方式中,数据库470可以是NoSQL数据库或数据库服务,例如由Amazon Web服务提供的DynamoDB数据服务。在各种实施方式中,存储在数据库470中的数据与应用相关,但可以包括过去签发的证书、各种链接权限机构值、已向其签发证书的设备上的数据、操作员动作等。应当指出,该数据可以采用未加密、经加密或其某种组合的方式存储。

[0127] 在各种实施方式中,可缩放CMS 400包括登记证书颁发机构430和假名证书颁发机构440,因为由注册审批机构405生成的数字证书被划分为不同段,例如,登记数字证书和假名数字证书。

[0128] 登记证书颁发机构430是CMS 400的非中央部件,因为可能存在多例登记证书颁发机构430同时执行。如图4A中登记证书颁发机构430的三个“堆叠”矩形所示,在一些实施方式中,可能存在多例登记证书颁发机构430同时执行。登记证书颁发机构430可以从注册审批机构420接收对登记证书的请求。登记证书颁发机构430的主要作用是履行来自注册审批机构420的请求,以向终端用户设备

[0129] (诸如图1所示的制造者105的分发器108)签发登记证书。如下文参照图5A所述,登记证书颁发机构430直接与注册审批机构420进行交互,以便履行其在CMS 400内的作用。

[0130] 假名证书颁发机构440是CMS 400的非中央部件,因为可能存在多例假名证书颁发机构440同时执行。再者,如图4A中假名证书颁发机构440的三个“堆叠”矩形所示,在各种实施方式中,可能存在多例假名证书颁发机构440并行同时执行。假名证书颁发机构440可以从注册审批机构420接收对假名证书的请求。假名证书颁发机构440的主要作用是履行来自注册审批机构420的请求,以向终端用户设备(诸如图1所示的制造者105的分发器108)签发假名证书。在某些实施方式中,假名证书颁发机构440履行对于V2V功能的短期假名证书的请求。如下文参照图5B所述,假名证书颁发机构440直接与注册审批机构420进行交互,以便履行其在CMS 400内的功能。

[0131] 在各种实施方式中,图4B所示的链接权限机构450、460将证书请求者的身份(即,

证书请求者设备的唯一标识符)链接到所签发的假名证书以备撤销。换言之,第一链接权限机构450和第二链接权限机构460将各自的链接值作为证书请求者设备的唯一标识符提供给所签发的假名证书。第一链接权限机构450和第二链接权限机构460可以从注册审批机构420接收对链接值的请求,然后将所请求的链接值提供给注册审批机构420。如下文参照图5A所述,链接权限机构450、460直接与注册审批机构420进行交互,以便履行对链接值的请求。

[0132] 在各种实施方式中,计算引擎425、435、445、455和465以及置备控制器120包括HSM,其允许这些部件执行安全计算而不会受到黑客的过度威胁。在一些实施方式中,计算引擎425、435、445、455和465可以设计为自身执行安全计算而无需嵌入式HSM,在这样的实施方式中,它们体现为HSM。

[0133] 在各种实施方式中,可以在CMS 400中使用不同的HSM版本。例如,HSM可以包括在计算引擎425、435、445、455和465中的一个或多个内安装为插卡的嵌入式HSM。在这样的示例实施方式中,嵌入式HSM可以作为外围部件互连

[0134] (PCI)HSM或PCI Express (PCIe)HSM安装在一个或多个计算引擎中。同样,例如CMS 400中的HSM可以包括网络附接或网络连接的外置HSM,其与它们自己机箱中的计算引擎分离。

[0135] 本领域普通技术人员会认识到,图4A和图4B所示的部件、过程、数据、操作和实施细节皆为解释简明清楚而呈现的示例。在不背离本发明原理的情况下,可使用其他部件、过程、实施细节和变型,因该示例并非旨在限制,而是可能存在许多变型。

[0136] 图5A和图5B是示出根据本发明实施方式的用于安全提供诸如证书等凭证的示例过程500的泳道图。在各种实施方式中,所示的某些或全部过程500或操作可以通过由纯硬件系统或两者兼备的系统在通用计算系统(其可以包括一个或多个处理器或者一个或多个计算子系统)上执行代码来执行。如图5A和图5B上方所示,过程500所涉及的实体包括位于制造者105处的分发器108,CMS主机的注册审批机构420、链接权限机构450、460、假名证书颁发机构440以及登记证书颁发机构430。在各种实施方式中,这些实体可以是如参照图4A和图4B及贯穿本公开所描述的实体,并可以彼此通信。

[0137] 如图5A中的示例所示,过程500开始于登记相关的操作505-535。登记证书颁发机构430的主要作用是履行来自注册审批机构420的请求,以向终端用户设备(诸如分发器108)签发登记证书。如下文参照登记相关的操作505-535所述,登记证书颁发机构430直接与注册审批机构420进行交互,以便向分发器108签发所请求的登记证书。

[0138] 在505,制造者105的分发器108向注册审批机构420请求登记证书,其中该登记证书将被置备给设备106a(例如供其使用),并且该请求可以标识出作为登记证书的目的地设备106a。该请求可以例如是制造者105处正为新设备106A(例如新产品)请求登记证书的分发器108。如上参照图2所述,登记证书是一种将其持有者标识为生态系统中的授权参与者的公钥证书,在该生态系统(例如USDOT的V2X生态系统)中,所有参与者皆须共享有效的登记证书,并且授权参与者还能接收假名证书,这些假名证书使得生态系统内的设备106能够进行通信和操作(例如在USDOT的V2X生态系统的示例中,使得车辆与路侧基础设施之间能够进行通信和操作)。

[0139] 在510,在注册审批机构420处接收对登记证书的请求,然后将该请求从注册审批

机构420传输到登记证书颁发机构430。在各种实施方式中,该操作可涉及注册审批机构420解密和验证该请求,包括签名验证、使用未批准设备清单(例如黑名单)检查作为登记证书目的地的设备(例如设备106a)的撤销状态,以及判定是否允许请求者(例如分发器108)向注册审批机构420请求登记证书。譬如,操作510可以包括判定来自制造者105的用户是否是授权用户(例如员工109的一部分)。在一些实施方式中,在510,注册审批机构420还可以判定待接收登记证书的设备106a(例如产品)是否已批准与系统100配合使用。在某些情形下,获准设备的清单(例如白名单)可以由图1中的监管者140提供,并供置备控制器120用来进行这种判定。在验证对登记证书的请求之后,将该请求从注册审批机构420传输到登记证书颁发机构430。该请求可以作为由注册审批机构420创建的登记证书生成请求来发送。

[0140] 在515,在登记证书颁发机构430处接收对登记证书的请求。响应于接收到该请求,在520,登记证书颁发机构430生成所请求的登记证书,并将所生成的登记证书传输回注册审批机构420。在525,在注册审批机构420处接收登记证书,并且在530,注册审批机构420将登记证书传输到分发器108。在535,分发器108接收登记证书。此时,分发器108可以将登记证书置备给设备(例如设备106a),使得该设备能够使用该登记证书,并完成登记相关的操作。

[0141] 操作540-599与置备假名证书相关。在540,分发器108向注册审批机构420请求假名证书。假名证书将被置备给设备106a(例如供其使用),并且请求可以标识作为假名证书目的地的设备106a。该请求可以是,例如,制造者105的分发器108向先前接收到登记证书的计算机化设备(例如已登记的设备106A)请求假名证书。假名证书包括一定量值(例如一周价值、一月价值或一年价值)的公钥证书。

[0142] 在545,在注册审批机构420处接收对假名证书的请求,然后该注册审批机构420启动对假名证书的置备。

[0143] 在操作550-570,链接权限机构450、460直接与注册审批机构420进行交互,以便履行对链接值的请求。在550,注册审批机构420将对第一组链接值(LA1)的请求传输到第一链接权限机构450。

[0144] 在555,响应于接收到对第一组链接值的请求,第一链接权限机构450生成第一组链接值并将其传输到注册审批机构420。在557,在注册审批机构420处接收第一组链接值。在560,注册审批机构420将对第二组链接值(LA2)的请求传输到第二链接权限机构460。

[0145] 接下来,如图5B所示,在565,响应于接收到对第二组链接值的请求,第二链接权限机构460生成第二组链接值并将其传输到注册审批机构420。在570,在注册审批机构420处接收第二组链接值。

[0146] 在某些实施方式中,图5A和图5B所示的链接权限机构450、460将证书请求者的身份(即,证书请求者设备的唯一标识符)链接到所签发的假名证书以备撤销。换言之,作为过程500的一部分,第一链接权限机构450和第二链接权限机构460分别将第一组链接值和第二组链接值作为证书请求者设备的唯一标识符提供给由假名证书颁发机构440签发的假名证书。第一链接权限机构450和第二链接权限机构460在操作550和560中接收从注册审批机构420发送的对链接值的请求,然后在操作555和565中将所请求的链接值提供给注册审批机构420。

[0147] 在非限制性示例实施方式中,对链接值的请求和对操作550-570中交换的请求的

响应可以包括具有报头和有效载荷数据项的消息,如下所示:

```
# Registration Authority (RA)-> Linkage Authority-x (LA-x): Initial Linkage Seed
Request {
  header: {
    msgID: mt.MSG_RA_LA_LINKAGE_SEED_REQUEST_MSG,
    taskPosition: "Linkage Authority number 1 or 2"
  },
  payload: {
[0148]   identifier: "Message identifier",
        iMin: Number,
        iMax: Number,
        jMax: Number
        }
  }

# LA-x -> RA: Initial Linkage Seed Response {
```

```

header: {
    msgID: mt.MSG_LA_RA_LINKAGE_SEED_RESPONSE_MSG,
    taskPosition: "Linkage Authority number 1 or 2"
},
payload: {
    identifier: "Incoming Message identifier",
    linkageChainIdentifier: "Linkage Chain ID -- HashedId8 of AES CCM
Encrypted Linkage Seed",
    iMin: Number,
    iMax: Number,
    jMax: Number
}
}

```

RA -> LA-x: PreLinkage Value Chain Request (Chunked 10 iRange at a time)

```

[0149] {
    header: {
        msgID: mt.MSG_RA_LA_PRE_LINKAGE_VALUE_REQUEST_MSG,
        iRangeSegmentChunkSize: "set to 10",
        currentIRangeSegment: "Index of segment in total request",
        taskPosition: "Linkage Authority number 1 or 2"
    },
    payload: {
        identifier: "Incoming Message identifier",
        linkageChainId: "Linkage Chain ID to use to create P Linkage Values
(PLVs)",
        iMin: Number,
        iMax: Number,
        jMax: Number
    }
}

```

```
# LA-x -> RA: PreLinkage Value Chain Response {  
  header: {  
    msgID: mt.MSG_LA_RA_PRE_LINKAGE_VALUE_RESPONSE_MSG,  
    iRangeSegmentChunkSize: "set to 10",  
    currentIRangeSegment: "Index of segment in total request",  
    taskPosition: "Linkage Authority number 1 or 2"  
  },  
  payload: {  
    identifier: "Incoming Message identifier",  
[0150]    preLinkageValues: Array of Encryped Prelinkage values for this segment of i,j  
    tuples,  
    linkageChainIdentifier: "Linkage Chain ID to use to create P Linkage Values  
    (PLVs)",  
    iMin: Number,  
    iMax: Number,  
    jMax: Number  
  }  
}
```

[0151] 继续参照图5B,在575,注册审批机构420将对假名证书的请求传输到假名证书颁发机构430。该请求可以作为由注册审批机构420创建的一批假名证书生成请求发送。

[0152] 在580,在假名证书颁发机构430处接收对假名证书的请求。响应于接收到请求,在585,假名证书颁发机构430生成所请求的假名证书,并将所生成的假名证书传输回注册审批机构420。在590,在注册审批机构420处接收假名证书。

[0153] 在595,分发器108可以向注册审批机构420发送多个请求,以查询所请求的假名证书是否准备就绪(即,生成且可用)。在某些实施方式中,可以在操作540中发送对假名证书的请求之后的任何时间发送操作595中的查询。例如,在操作540中将对假名证书的请求发送到注册审批机构420之后,分发器108则可以周期性向注册审批机构420发送查询以判定所请求的假名证书是否准备就绪。在本例中,可以与操作545-590并行地(即,在生成假名证书的同时)发送操作595中的一个或多个查询。

[0154] 在598,当假名证书准备就绪时,注册审批机构420将假名证书传输到分发器108。在599,分发器108接收假名证书。此时,分发器108可以将假名证书置备给设备(例如设备106a),使得该设备能够使用这些假名证书,并且完成置备假名证书的操作。

[0155] 在某些非限制性示例实施方式中,在操作575-590中交换的对假名证书的请求以及对该请求的响应可以包括具有报头和有效载荷数据项的消息,如下所示:

```
# Registration Authority (RA) -> Pseudonym Certificate Authority (PCA):  Generate an
individual Certificate {
  header: {
    msgID: mt.MSG_RA_PCA_CERT_REQUEST_MSG,
    iRangeSegmentChunkSize: "set to 10"
  },
  payload: {
    identifier: "hash of payload minus this field"
    i: Number,
    plv1: "Encrypted PLV from LA1",
    plv2: "Encrypted PLV from LA2",

    seedPublicKey: "Seed Verify Public key",
    encryptKey: "Seed Encrypt Public key",

    startSeconds: "start time for this certificate",
    endSeconds: "end time for this certificate",

    region: "requested region",
    certRequestPermissions: "the cert request permissions from the enrollment cert (will
be turned into app permissions)"
  }
}
# PCA -> RA:  Certificate Response
{
  header: {
    msgID: mt.MSG_PCA_RA_IDENTITY_CERT_RESPONSE_MSG
  },
  payload: {
    data: "Signed and Encrypted SCMS certificate response",
    identifier: "hash of original payload request"
  }
}
```

[0156]

[0157] 图6A和图6B是根据本发明实施方式的利用双向消息队列610、611、612、613、614、

615、616、617、618、619实现可缩放且安全的CMS 600的示例架构的框图。

[0158] 正如上文参照图4A和图4B所描述的CMS 400,可缩放CMS 600的各种实施方式可以用于超大量的设备交易和证书生成处理。在一些实施方式中,可缩放CMS 600可以使用多个服务器、HSM、多个计算机或计算引擎以及多个应用平台(例如VM或硬件平台)来实现。在图6A和图6B所示的示例实施方式中,应用平台可以均包括一个或多个虚拟机(VM)。在附加或替选的实施方式中,应用平台可以均包括一个或多个硬件平台,例如,服务器、计算机或能够执行软件应用的其他计算机硬件。可缩放CMS 600的示例可以在私有数据中心、诸如来自亚马逊的Amazon Web服务(AWS)的云数据中心或私有数据中心与云数据中心的混合中心中实现。为了简明起见,下文仅描述图6A和图6B内与图4A和图4B存在的区别之处。

[0159] 如图6A中的示例所示,CMS 600的架构可以包括两个置备控制器602,即主要置备控制器和备用置备控制器,它们优选在单独的服务器中实现。这两个置备控制器602包括与图4A中的置备控制器102相似的功能,以便出于如上参照图4A所述的失效备援目的,将主要置备控制器中包含的对象、数据等复制或以其他方式包含在备用(次要)置备控制器中。在某些实施方式中,置备控制器602可以是DLM控制器,例如主要DLM控制器和备用DLM控制器。在各种实施方式中,置备控制器602可以是按部件类型存在于CMS 600中的控制器。在图6A和图6B的示例中,置备控制器602可以是针对注册审批机构620、登记证书颁发机构430、假名证书颁发机构440和链接权限机构450、460存在的一对控制器(例如主要控制器和备用控制器)。

[0160] 如图6A和图6B所示,可缩放CMS 600的架构包括实施为REST Web服务的注册审批机构605、注册审批机构620、注册审批机构计算引擎625、登记证书颁发机构630、登记证书颁发机构计算引擎635、假名证书颁发机构640、假名证书颁发机构计算引擎645、第一链接权限机构650、第一链接权限机构计算引擎655、第二链接权限机构660、第一链接权限机构计算引擎665、双向消息队列610、611、612、613、614、615、616、617、618、619以及数据库670。

[0161] 可缩放CMS 600的架构有利地区分非安全相关应用与安全功能。在图6A和图6B的非限制性示例中,注册审批机构620、登记证书颁发机构630、假名证书颁发机构640和链接权限机构650、660实施为它们自己VM上的应用,这些VM在它们自己的专用计算引擎625、635、645、655和665上执行,所有这些计算引擎均与任何非安全相关的应用和功能分离。这样相比常规系统更具技术和安全优势及改进,在常规系统中,HSM的性能更慢,云服务提供者无法供应HSM,或者无法确定系统对HSM的正确管理。在可缩放CMS 600中,在计算引擎(例如计算引擎625、635、645、655和665中的一个或多个)中执行所有需要HSM的加密操作。换言之,在CMS 600中,在计算引擎中执行所有需要HSM的加密操作。

[0162] 如图6A和图6B所示,通过将关键的安全功能彼此分离并分离到单独的计算引擎上,例如,由注册审批机构620、登记证书颁发机构630、假名证书颁发机构640和链接权限机构650、660执行的计算密集型加密和安全功能的执行比现有注册审批机构系统快得多。通过使得“瓶颈”应用可视需要单独缩放,这种设计能够显著改善事务处理。譬如,如果注册审批机构605和620上运行的注册审批机构应用需要缩放,则能添加额外的应用平台(例如VM或硬件平台),而无需对注册审批机构计算引擎625的安全计算能力作出任何更改。同样,例如,如果安全计算正在限制性能,则能添加额外的安全注册审批机构计算引擎625。同样的多维缩放也适用于CMS 600的其他部件。

[0163] 在图6A和图6B所示的示例中,通过双向消息队列610、611、612、613、614、615、616、617、618和619,注册审批机构605连接到其他部件,且其他部件相互连接。在图6A和图6B的示例实施方式中,双向消息队列610、611、612、613、614、615、616、617、618和619是双向队列,因为这些队列中的消息双向流动

[0164] (例如在客户端与服务器之间)。这就提供了将新请求与消息队列中的挂起响应相分离的性能优势。通过使用双向消息队列610、611、612、613、614、615、616、617、618和619使应用平台(例如VM和/或硬件平台)与计算引擎彼此通信连接,应用平台(例如VM和/或硬件平台)和计算引擎能够独立地缩放。在CMS 600中,用于注册审批机构620、登记证书颁发机构630、假名证书颁发机构640和链接权限机构650、660的各应用平台(例如VM和/或硬件平台)经由各组双向消息队列通信连接到计算引擎625、635、645、655和665。

[0165] 在CMS 600中,注册审批机构605(以及图6A和图6B中用“DB”箭头示出的其他部件)可以连接到数据库670。在优选实施方式中,数据库670是快速访问的低延迟数据库。在某些实施方式中,数据库670可以是NoSQL数据库或数据库服务,例如由Amazon Web服务提供的DynamoDB数据服务。在各种实施方式中,存储在数据库670中的数据与应用相关,但可以包括先前签发的证书、各种链接权限机构值(例如链接值)、已向其签发证书的设备上的数据、操作员动作等。该数据可以采用未加密、经加密或其某种组合的方式存储。

[0166] 在各种实施方式中,可缩放CMS 600包括登记证书颁发机构630和假名证书颁发机构640,因为由注册审批机构605生成的数字证书被划分为不同段,例如,登记数字证书和假名数字证书。

[0167] 如图6A中登记证书颁发机构630的三个“堆叠”矩形所示,在一些实施方式中,可能存在多例登记证书颁发机构630同时执行。图6A和图6B的其他“堆叠”元素采用类似的表示。登记证书颁发机构630可以从注册审批机构620接收多个对登记证书的请求。

[0168] 在各种实施方式中,计算引擎625、635、645、655和665以及置备控制器602包括HSM,其允许这些部件执行安全计算而不会受到黑客的过度威胁。在一些实施方式中,计算引擎625、635、645、655和665可以设计为自身执行安全计算而无需嵌入式HSM,在这样的实施方式中,它们体现为HSM。

[0169] 本领域普通技术人员会认识到,图6A和图6B所示的部件、过程、数据、操作和实施细节皆为解释简明清楚而呈现的示例。在不背离本发明原理的情况下,可使用其他部件、过程、实施细节和变型,因该示例并非旨在限制,而是可能存在许多变型。

[0170] 图7A和图7B是根据本发明实施方式的利用负载均衡器710、711、712、713、714、715、716、717、718、719实现可缩放且安全的CMS 700的示例架构的框图。

[0171] 正如上文参照图4和图6所描述的CMS 400和CMS 600,可缩放CMS 700的各种实施方式可以用于超大量的设备交易和证书生成处理。为了简明起见,下文仅描述图7A和图7B内与图4和图6存在的区别之处。在图7A和图7B所示的示例实施方式中,应用平台被描绘为包括一个或多个虚拟机(VM)。在附加或替选的实施方式中,应用平台可以均包括一个或多个硬件平台,例如,应用服务器、服务器场、基于云的服务器、配置为执行应用操作的处理器或能够执行软件应用的其他计算机硬件。

[0172] 如图7A中的示例所示,CMS 700的架构可以包括两个置备控制器702,即主要置备控制器和备用置备控制器,它们优选在单独的服务器中实现。这两个置备控制器702分别包

括与图4A和图6A中的置备控制器120和602相似的功能。换言之,出于如上参照图4A所述的失效备援目的,将主要置备控制器中包含的对象、数据等复制或或以其他方式包含在备用(次要)置备控制器中。

[0173] 如图7A和图7B所示,可缩放CMS 700的架构包括实施为REST Web服务的注册审批机构705、注册审批机构720、注册审批机构计算引擎725、登记证书颁发机构730、登记证书颁发机构计算引擎735、假名证书颁发机构740、假名证书颁发机构计算引擎745、第一链接权限机构750、第一链接权限机构计算引擎755、第二链接权限机构760、第一链接权限机构计算引擎765、负载均衡器710、711、712、713、714、715、716、717、718、719以及数据库770。

[0174] 正如图4和图6中的CMS 400和CMS 600,可缩放CMS 700的架构有利地将非安全相关应用与安全功能分离。如图7A和图7B中的非限制性示例所示,注册审批机构720、登记证书颁发机构730、假名证书颁发机构740和链接权限机构750、760实施为它们自己VM上的应用,这些VM在它们自己的专用计算引擎725、735、745、755和765上执行,所有这些计算引擎均与任何非安全相关的应用和功能分离。在可缩放CMS 700中,在计算引擎(例如计算引擎725、735、745、755和765中的一个或多个)中执行所有需要HSM的加密操作。在CMS 700中,在计算引擎中执行所有需要HSM的加密操作。

[0175] 如图7A和图7B所示,通过将关键的安全功能彼此分离并分离到单独的计算引擎上,例如,由注册审批机构720、登记证书颁发机构730、假名证书颁发机构740和链接权限机构750、760执行的计算密集型加密和安全功能的执行比已知注册审批机构的解决方案快得多。这种设计能够显著改善事务处理,其中通过使得“瓶颈”应用能够按需单独缩放,而不受服务器处理或存储能力的束缚。譬如,如果注册审批机构705和720上运行的注册审批机构应用需要缩放,则能添加额外的应用平台(例如VM或硬件平台),而无需对注册审批机构计算引擎725的安全计算能力作出任何更改。同样,例如,如果安全计算正在限制性能,则能添加额外的安全注册审批机构计算引擎725。同样的多维缩放也适用于CMS 700的其他部件。

[0176] 在图7A和图7B所示的示例中,通过负载均衡器710、711、712、713、714、715、716、717、718和719,注册审批机构705连接到其他部件,且其他部件相互连接。在图7A和图7B的示例实施方式中,负载均衡器710、711、712、713、714、715、716、717、718和719可以实施为虚拟负载均衡器(例如VM上运行的虚拟负载均衡器)或经由专用硬件实施。如图7A和图7B所示,在CMS 700中,每个负载均衡器710、711、712、713、714、715、716、717、718和719插入到每组相似类型的VM或计算引擎前面。这就提供以下益处,即一个或多个客户端仅看到单个服务器端点,并且负载均衡器判定哪个服务器将处理给定的请求。以此方式,负载均衡器710、711、712、713、714、715、716、717、718、719使应用平台(例如VM和/或硬件平台)与计算引擎彼此通信连接。在CMS 700中,用于注册审批机构720、登记证书颁发机构730、假名证书颁发机构740和链接权限机构750、760的各应用平台经由各组负载平衡器通信连接到计算引擎725、735、745、755和765。

[0177] 在各种实施方式中,可缩放CMS 700包括登记证书颁发机构730和假名证书颁发机构740,因为由注册审批机构705生成的数字证书被划分为不同段,例如,登记数字证书和假名数字证书。

[0178] 如图7A中假名证书颁发机构740的三个“堆叠”矩形所示,在各种实施方式中,可能存在多例假名证书颁发机构740同时执行。图7A和图7B的其他“堆叠”元素采用类似的表示。

假名证书颁发机构740可以从注册审批机构720接收对多批假名证书的多个请求(例如对一周价值、一月价值或一年价值的假名证书的请求)。

[0179] 本领域普通技术人员会认识到,图7A和图7B所示的部件、过程、数据、操作和实施细节皆为解释简明清楚而呈现的示例。在不背离本发明原理的情况下,可使用其他部件、过程、实施细节和变型,因该示例并非旨在限制,而是可能存在许多变型。

[0180] 图8是根据本发明实施方式的用于通过轮询调度请求实现可缩放且安全的CMS的系统800示例的框图。为了简明起见,图8仅示出一组应用平台(例如VM和/或硬件平台)820、830、840、850和计算引擎825、835、845、855。应当指出,图8中的应用平台820、830、840、850和计算引擎825、835、845、855能够是如上参照图7所述的用于实现任何注册审批机构720、登记证书颁发机构730、假名证书颁发机构740和链接权限机构750、760的任一组应用平台和计算引擎。正如图7中的CMS 700,在系统800中,在计算引擎中执行所有需要HSM的加密操作,并且应用平台和计算引擎皆独立地缩放。

[0181] 继续参照图8,轮询调度是指使用每个可用服务器(例如每个计算引擎)的知识。在系统800中发送的轮询调度请求使用可用计算引擎(例如计算引擎825、835、845、855)的知识来分发发送到该组计算引擎的请求和消息。

[0182] 为了清楚说明系统800中轮询调度请求的顺序,图中示出可用于应用VM 850的一组放大的计算引擎865、875、885、895。在图8的示例中,存在“n”个应用平台(例如VM和/或硬件平台),并存在“m”个可用计算引擎。要向计算引擎发出请求的客户端(例如应用VM 895)按照图8所示的顺序进行操作。如图所示,来自应用VM 895的第一请求是对CE1(计算引擎865)的请求,第二请求是对CE2(计算引擎875)的请求,依此类推。当到达最后一个CE、即CE_m(计算引擎895)时,客户端(应用VM 895)重新开始于CE1。

[0183] 在系统800中,所有的客户端(例如应用平台820、830、840、850)知道它们需要与之通信的所有服务器(例如一组可用计算引擎)。每个客户端对每个服务器执行轮询调度请求,这样有利地跨所有服务器平均分发工作负载。在某些实施方案中,图7所示的CMS 700的负载均衡器710、711、712、713、714、715、716、717、718、719可以向计算引擎发送轮询调度请求,以跨计算引擎平均分发工作负载。

[0184] 图9是根据本发明实施方式的用于通过基于工作负载的请求来实现可缩放且安全的CMS的系统900示例的框图。为了简明起见,下文仅描述图9内与图7和图8存在的区别之处。

[0185] 正如图8,为了简明清楚起见,图9仅示出一组应用平台920、930、940、950和计算引擎925、935、945、955。应当指出,图9中的应用平台(例如VM和/或硬件平台)920、930、940、950和计算引擎925、935、945、955可以是如上参照图7所述的用于实现任何注册审批机构720、登记证书颁发机构730、假名证书颁发机构740和链接权限机构750、760的任一组应用平台和计算引擎。正如图7中的CMS 700,在系统900中,在计算引擎中执行所有需要HSM的加密操作,并且应用平台(例如VM和/或硬件平台)和计算引擎皆独立地缩放。

[0186] 继续参照图9,通过增加智能以首先查询所使用的每个服务器的工作负载来启用工作负载分发技术。工作负载分发技术是基于工作负载,因为它使用了每个可用服务器(例如每个计算引擎)的工作负载的知识。系统900中发送的请求使用可用计算引擎(例如计算引擎925、935、945、955)的当前工作负载知识来分发发送到该组计算引擎的请求和消息。在

系统900中,基于每个计算引擎各自报告的工作负载将请求发送到计算引擎。

[0187] 为了清楚说明系统900中基于工作负载的请求,图中示出一组放大的计算引擎965、975、985、995,它们将其各自的工作负载报告给应用VM 950。在图9的示例中,“m”是应用平台的数目,而“n”是报告其工作负载的计算引擎的数目。在图9的示例中,工作负载按百分比报告,其中计算引擎975的30%工作负载指示计算引擎975当前正以其总容量的30%运行。类似地,计算引擎965、985和995报告的80%工作负载指示这些计算引擎当前均以其总容量的80%运行。在某些实施方式中,给定计算引擎报告的当前工作负载指示该计算引擎中嵌入的HSM的工作负载。譬如,在计算引擎的处理容量受其HSM执行加密操作的能力束缚或约束的情形下,计算引擎报告的工作负载百分比可以反映HSM的当前工作负载。例如,如果计算引擎975使用的HSM以其处理容量的30%运行,则计算引擎975可以报告它以其总容量的30%运行。在一些实施方式中,工作负载百分比可以是服务器(例如计算引擎)的处理容量、通信容量(例如直接通信链路或无线模块的可用带宽度量)和存储/内存容量的加权度量。在一示例中,可以赋予处理容量、通信容量和存储容量均等的三分之一权重。在本例中,如果计算引擎975使用其中央处理单元(CPU)容量的25%、其通信容量的35%和其可用存储器或存储区的30%,则计算引擎975将报告其工作负载为30%。

[0188] 在某些实施方式中,可以对计算引擎的环境度量进行加权并结合考虑工作负载度量。譬如,可以确定计算引擎的总体正常状况度量,并将其与计算引擎的工作负载度量一同报告。在某些示例中,给定计算引擎的正常状况度量可以作为以下一项或多项的函数:计算引擎的工作温度(例如高于热传感器的平均温度读数可指示CPU、存储器模块或磁盘驱动器容易因过热而停机或故障);

[0189] 计算引擎机壳内部的湿度水平;重新启动或重启的频率(例如热停机或热崩溃);自最近一次重启以来的时间;最近一段时间(例如前一天、前一周或前一月)的磁盘故障或存储器故障次数;直到计算引擎的排程维护事件前的时间(例如软件或固件更新、故障硬件部件的更换);计算引擎正在备用电源上运行的指示;或者自上次计算引擎电源停电或降压以来的持续时间。

[0190] 在附加或替选的实施方式中,可以使用其他权重、度量和指标来确定计算引擎的工作负载。例如,如果执行加密操作的计算引擎历史上受限于CPU容量要大于受限于其通信容量或内存容量,则当确定那些计算引擎的总体工作负载百分比时,赋予CPU容量的权重可以大于赋予其他容量的权重。

[0191] 在系统900中,要向计算引擎发出请求的客户端(例如应用VM 995)基于由计算引擎报告的工作负载进行操作。在图9的示例中,来自应用VM 995的下一个请求将基于其相对较低的30%工作负载而到达CE2(计算引擎975)。换言之,因为计算引擎975具有一组计算引擎965、975、985、995中最低的工作负载。当要将下一个请求从应用VM 995发送到计算引擎时,可以使用CE1(计算引擎965)或CE3(计算引擎985)或CEm(计算引擎995)中的任一个,因为它们皆当前正报告均等80%的工作负载。在每个可用计算引擎报告相同或相似的工作负载的情形下,可以使用顺序请求跨这些负载均等的计算引擎平均分发工作负载。换言之,如果每个可用计算引擎正报告基本上均等或均等的工作负载,则可以使用上文参照图8描述的请求。随时间推移,随着工作负载变化,客户端(应用VM 995)会将后续请求发送到负载最小的可用计算引擎。

[0192] 在系统900中,所有的客户端(例如应用平台920、930、940、950)知道它们需要与之通信的所有服务器(例如一组可用计算引擎)的工作负载。每个客户端可以向每个服务器提交工作负载查询,并使用报告的工作负载有利地跨所有服务器平均分发工作负载。在某些实施例中,图7所示的CMS 700的负载均衡器710、711、712、713、714、715、716、717、718、719可以向计算引擎发送基于工作负载的请求,以跨计算引擎平均分发工作负载。

[0193] 图10A和图10B是根据本发明实施方式的用于实现可缩放且安全的证书管理系统(CMS)400的示例架构框图。为了简明起见,下文仅描述图10A和图10B内与图4A和图4B存在的区别之处。

[0194] 如图10A中的示例所示,CMS1000的架构可以包括两个置备控制器1002,即主要置备控制器和备用置备控制器,它们优选在单独的服务器中实现。这两个置备控制器1002分别包括与图4A和图6A中的置备控制器120和602相似的功能。换言之,出于如上参照图4A所述的失效备援目的,将主要置备控制器中包含的对象、数据等复制或以其他方式包含在备用(次要)置备控制器中。

[0195] 如图10A和10B所示,CMS1000的架构包括实施为REST Web服务的注册审批机构1005、注册审批机构1020、计算引擎1025、1035、1045、1050、1060、消息队列1010、1012、1014、1016、1018以及数据库1070。

[0196] CMS1000的示例可以在私有数据中心、云数据中心或私有数据中心和云数据中心的混合中心中实现。CMS1000的各种实施方式可以用于超大量的设备进行交易和证书生成处理。在各种实施方式中,CMS1000可以使用多个服务器、HSM以及多个用作应用平台的计算机或计算引擎来实现。换言之,如图10A和10B所示,所描述的注册审批机构、证书颁发机构和链接权限机构的应用均运行一个或多个能够托管和执行软件应用的计算引擎。

[0197] CMS1000类似于上文参照图4A和图4B描述的CMS 400,二者区别之处在于,使用计算引擎1025、1035、1045、1050、1060来托管和运行应用。换言之,CMS1000架构是CMS 400架构的备选方案,其中注册审批机构、登记证书颁发机构、假名证书颁发机构和链接权限机构的应用在它们自己的专用计算引擎1025、1035、1045、1050和1060上执行。在CMS1000中,在同样运行相关应用的计算引擎(例如计算引擎1025、1035、1045、1050和1060)中执行所有需要HSM的加密操作。有利地,通过在计算引擎1025、1035、1045、1050、1060上执行应用和加密操作,CMS1000的架构能够减少所需的消息队列数目。

[0198] 在图10A和10B的示例中,计算引擎包括托管并运行注册审批机构应用的注册审批机构计算引擎1025、可操作为托管并运行登记证书颁发机构应用的登记证书颁发机构计算引擎1035、可操作为托管并运行假名证书颁发机构应用的假名证书颁发机构计算引擎1045、可托管并运行第一链接权限机构应用的第一链接权限机构计算引擎1050以及可操作为托管并运行第二链接权限机构应用的第二链接权限机构1060。

[0199] 如图10A和图10B所示,通过消息子系统或消息队列服务,包括输入消息队列1010、1012、1014、1016、1018,注册审批机构1005连接到其他部件,且其他部件相互连接。在图10A和图10B的示例实施方式中,输入消息队列1010、

[0200] 1012、1014、1016、1018是单向队列,因为这些队列中的消息单向流动(例如从客户端到服务器)。通过为每个计算引擎使用单个输入队列,每个计算引擎还托管并运行它们各自的应用,可以提供简化的技术优势。

[0201] 通过使用输入消息队列1010、1012、1014、1016、1018使计算引擎彼此通信连接,这些计算引擎能够视需要独立地缩放。换言之,由于用作注册审批机构、登记证书颁发机构、假名证书颁发机构和链接权限机构应用的应用平台的各计算引擎经由各自的输入消息队列通信连接,CMS1000的这些部件以及数据库1070皆彼此独立地缩放。

[0202] 图11是包括可用于实现根据本发明实施方式的系统和方法的计算系统1100的计算环境1101的示例框图。也可以使用其他部件和/或布置。在一些实施方式中,计算系统1100可以用于至少部分地实现图1至图10中的各种部件,诸如图4和图6至图10中的CMS架构的置备控制器120、DAMS110和计算引擎以及图7中的负载均衡器710-719等。在一些实施方式中,类似于计算系统1100的一系列计算系统可以均定制有专用硬件和/或编程为专用服务器以实现图1至图10中的部件之一,这些部件可以经由网络1135彼此通信。

[0203] 在图11所示的示例中,计算系统1100包括数个部件,诸如CPU 1105、存储器1110、输入/输出(I/O)设备1125、硬件安全模块(HSM)1140以及非易失性存储设备1120。系统1100可以采用各种方式来实现。例如,作为集成平台(诸如服务器、工作站、个人计算机、膝上型计算机等)的实施方式可以包括CPU 1105、存储器1110、非易失性存储设备1120和I/O设备1125。在这样的配置中,部件1105、1110、1120和1125可以通过本地数据总线连接和通信,并可以经由外部I/O连接来访问数据存储库1130(例如实施为单独的数据库系统)。I/O部件1125可以通过直接通信链路(例如硬接线或本地WiFi连接)、通过诸如局域网

[0204] (LAN)或广域网(WAN,诸如蜂窝电话网络或因特网)等网络和/或通过其他合适的连接而连接到外部设备。系统1100可以是独立系统,或者可以是大型系统的子系统。

[0205] CPU 1105可以是一个或多个已知的处理器或处理设备,诸如加利福尼亚州圣塔克拉拉市Intel™公司生产的Core™系列微处理器或者加利福尼亚州森尼韦尔镇AMD™公司生产的Athlon™系列微处理器。存储器1110可以是一个或多个快闪存储设备,其配置为存储由CPU 1105执行或使用以执行与本发明实施方式相关的某些功能、方法和过程的指令和信息。存储设备1120可以是易失性或非易失性、磁性、半导体、磁带、光学或其他类型的存储设备或者计算机可读介质,包括诸如CD和DVD的设备以及旨在长期存储的固态设备。

[0206] 在图示的实施方式中,存储器1110包含从存储设备1120或从远程系统(未示出)加载的一个或多个程序或应用1115,该程序或应用1115被CPU 1105执行时执行根据本发明的各种操作、程序、过程或方法。替选地,CPU 1105可以执行位置远离系统1100的一个或多个程序。例如,系统1100可以经由网络1135访问一个或多个远程程序,该程序被执行时执行与本发明实施方式相关的功能和过程。

[0207] 在一实施方式中,存储器1110可以包括用于执行本文针对置备控制器120、DAMS110和/或分发器118、131描述的专用功能和操作的程序1115。在一些实施方式中,存储器1110还可以包括实现为本发明提供辅助功能的其他方法和过程的其他程序或应用。

[0208] 存储器1110还可以配置有与本发明无关的其他程序(未示出)和/或被CPU 1105执行时执行本领域公知的几种功能的操作系统(未示出)。举例而言,操作系统可以是Microsoft Windows™、Unix™、Linux™、Apple Computers™操作系统或其他操作系统。选择操作系统乃至使用操作系统并非本发明的必要技术特征。

[0209] HSM 1140可以是具有其自己处理器的设备,该处理器安全生成并存储数字安全资产和/或安全执行各种加密和敏感计算。HSM 1140保护数字安全资产(诸如加密密钥)和其

他敏感数据免遭攻击者可能访问。在一些实施方式中,HSM可以是直接附接到计算系统1100的插卡或插板。

[0210] I/O设备1125可以包括一个或多个允许系统1100接收和/或发送数据的输入/输出设备。例如,I/O设备1125可以包括一个或多个允许从用户输入数据的输入设备,诸如键盘、触摸屏、鼠标等。另外,I/O设备1125可以包括一个或多个允许将数据输出或呈现给用户的输出设备,诸如显示屏、CRT监视器、LCD监视器、等离子显示器、打印机、扬声器设备等。I/O设备1125还可包括一个或多个允许计算系统1100例如与其他机器和设备进行数字通信的数字和/或模拟通信输入/输出设备。其他配置和/或数目的输入和/或输出设备可以合并到I/O设备1125中。

[0211] 在所示的实施方式中,系统1100连接到网络1135(诸如因特网、专用网、虚拟专用网、蜂窝网或其他网络或者这些网络的组合),该网络1135又可以连接到各种系统和计算机器,诸如服务器、个人计算机、膝上型计算机、客户端设备等。一般而言,系统1100可以经由网络1135从外部机器和设备输入数据并向外部机器和设备输出数据。

[0212] 在图11所示的示例实施方式中,数据源1130是系统1100外部的独立数据库,诸如数据库125。在其他实施方式中,数据源1130可以由系统1100托管。在各种实施方式中,数据源1130可以管理并存储用于实现根据本发明的系统和方法的数据。例如,数据源1130可以管理并存储包含由系统110置备的每个设备116的状态和日志信息等的数据结构。

[0213] 数据源1130可以包括一个或多个存储信息并可通过系统1100访问和/或管理的数据库。举例而言,数据库1130可以是OracleTM数据库、SybaseTM数据库或其他关系数据库。然而,根据本发明的系统和方法不限于单独的数据结构或数据库,甚至不限于使用数据库或数据结构。

[0214] 本领域普通技术人员应认识到,图11中系统的部件和实施细节皆为解释简明清楚而呈现的示例。可以使用其他部件和实施细节。

[0215] 尽管上述示例使用了诸如OBU、ECU和RSU的计算机化设备的特例,但为了解释清楚起见,本发明不限于那些特例。根据本发明的各种实施方式可以与多种计算机化设备配合使用,诸如医疗设备(例如透析机、输液泵等)、机器人、无人机、自动驾驶车辆、无线通信模块(例如嵌入式通用集成电路卡(eUICC))等。

[0216] 本文描述的应用的各种操作可以至少部分地由一个或多个VM来执行。在附加或替换的实施方式中,本文所述的应用的各种操作可以至少部分地由一个或多个处理器来执行,这些处理器被暂时性配置(例如通过软件)或永久性配置用于执行相关的操作。无论暂时性还是永久性配置,这些处理器皆可构成操作为执行本文所述的一个或多个应用操作、功能和作用的处理器实现的模块。如本文所用,术语“处理器实现的模块”是指使用一个或多个处理器实现的硬件模块。

[0217] 类似地,本文描述的方法可至少部分地由处理器实现,其中一个或多个特定处理器是硬件的示例。例如,一种方法的至少一些操作可由一个或多个处理器或者处理器实现的模块来执行。一个或多个处理器也可操作为在“云计算”

[0218] 环境中支持相关操作的执行或者可操作为SaaS。例如,至少一些操作可通过一组计算机来执行(作为包括处理器的机器的示例),这些操作可经由网络(例如因特网)及经由一个或多个适当的接口(例如API)来访问。

[0219] 某些操作的执行可分发给不仅居于单个机器内而且部署到数个机器上的处理器。在一些示例性实施方案中,处理器或处理器实现的模块可位于单个地理位置上(例如位于办公环境内、制造环境内或服务器机群内)。在其他示例性实施方案中,处理器或处理器实现的模块可分布到数个地理位置上。

[0220] 根据考虑本公开的说明书以及实践本公开的发明内容,本发明的其他实施方式对于本领域技术人员将显而易见。说明书和实施例仅视为示例性,本发明的真正保护范围由所附权利要求书指定。

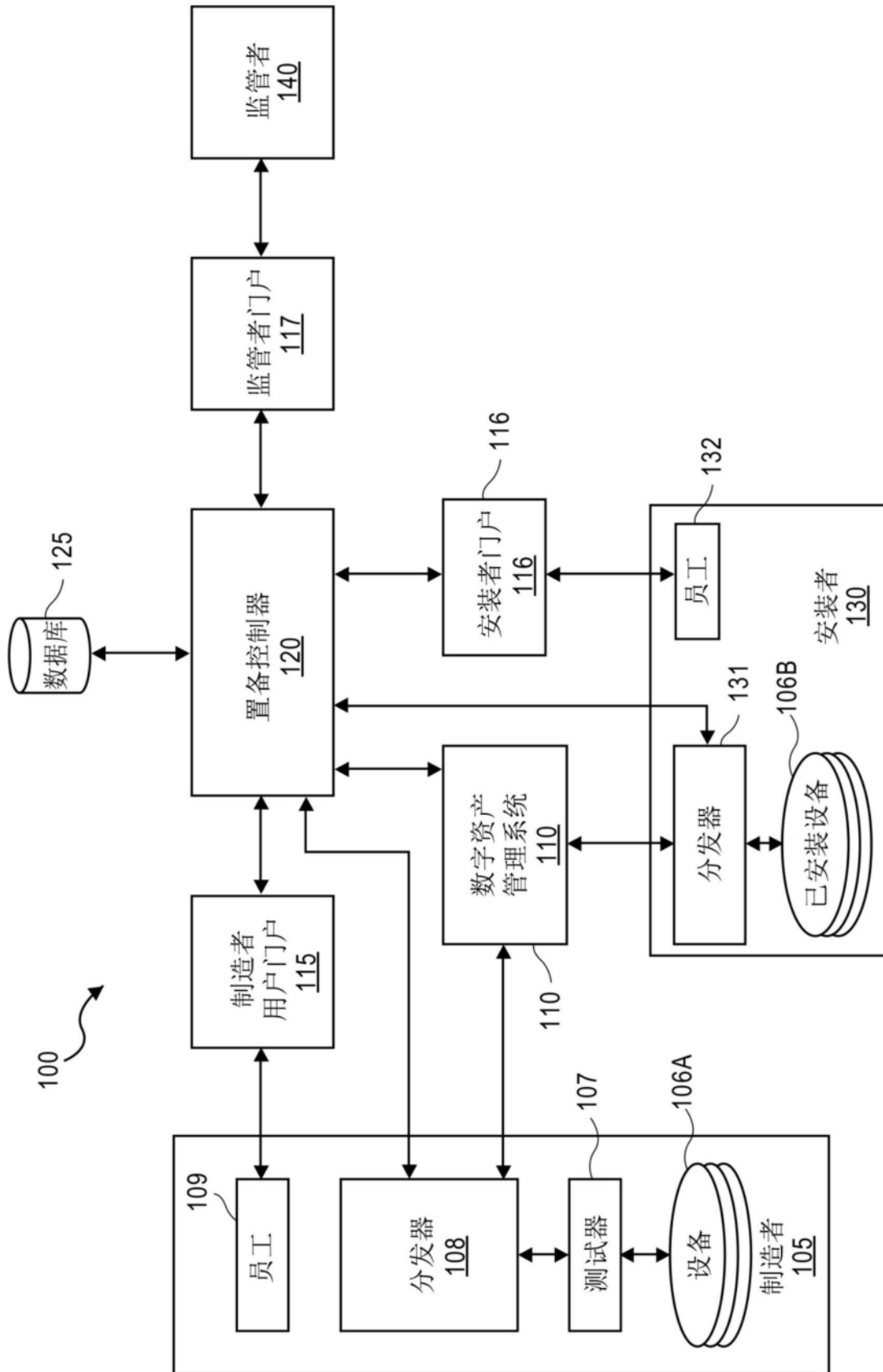


图1

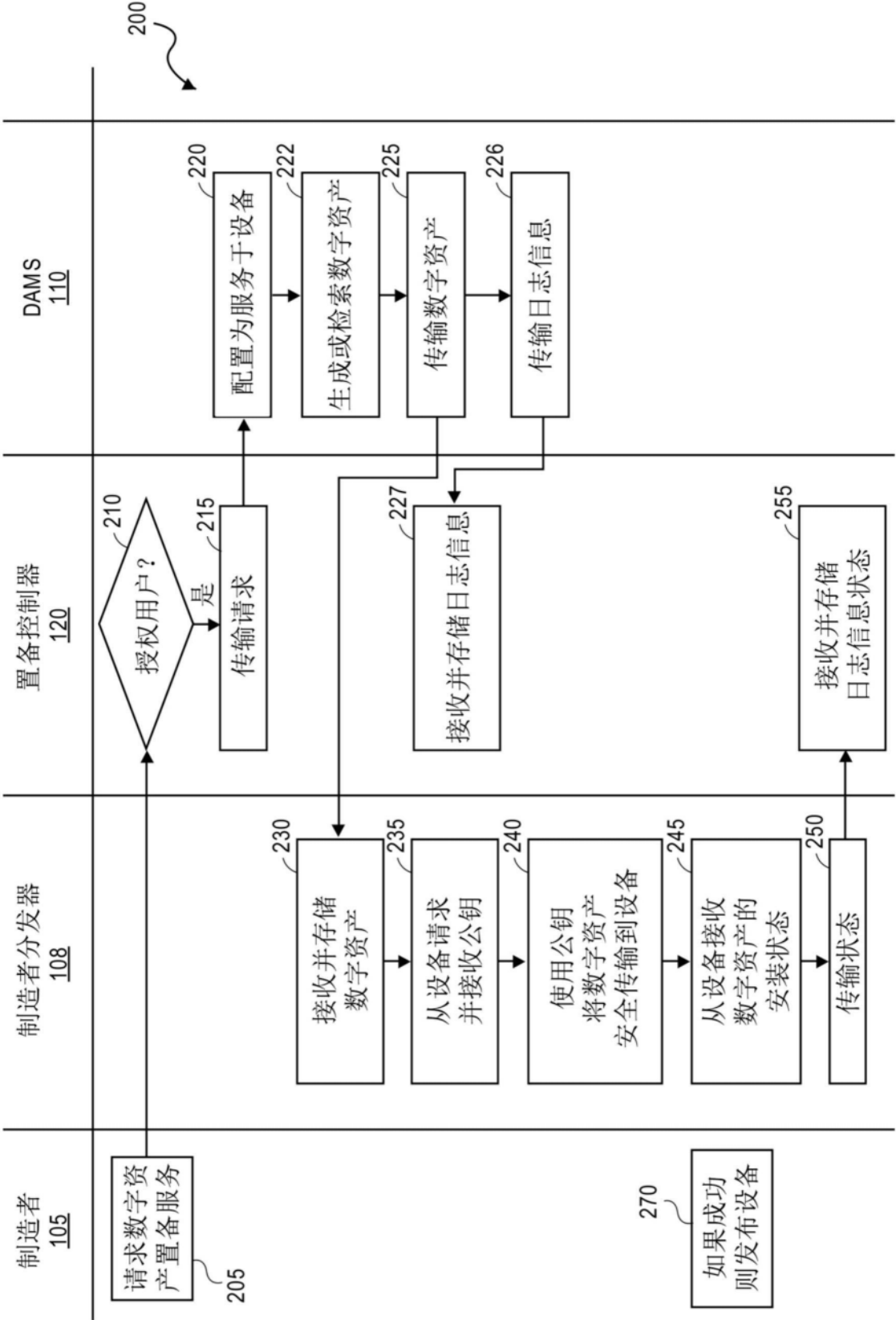


图2

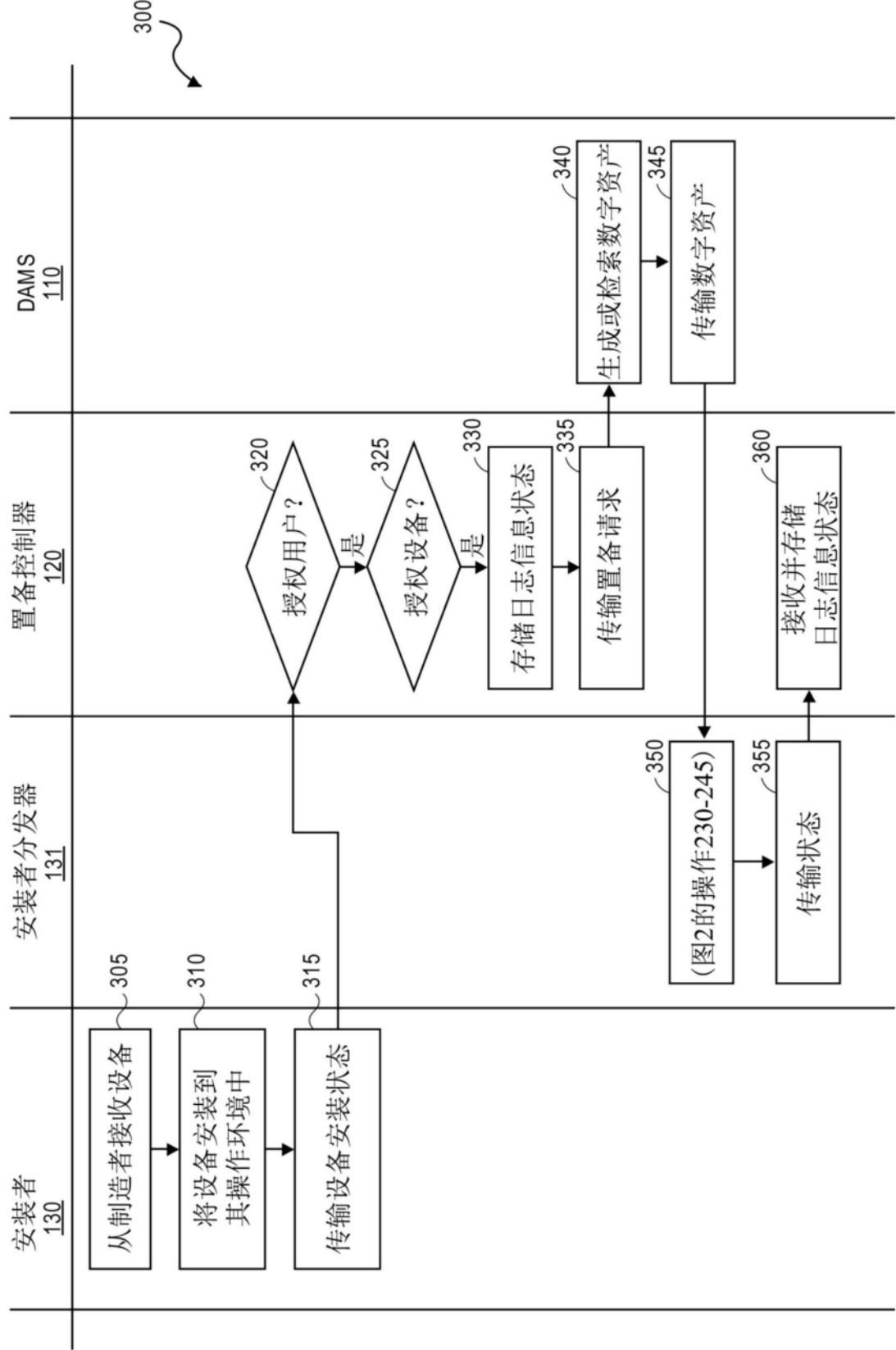


图3

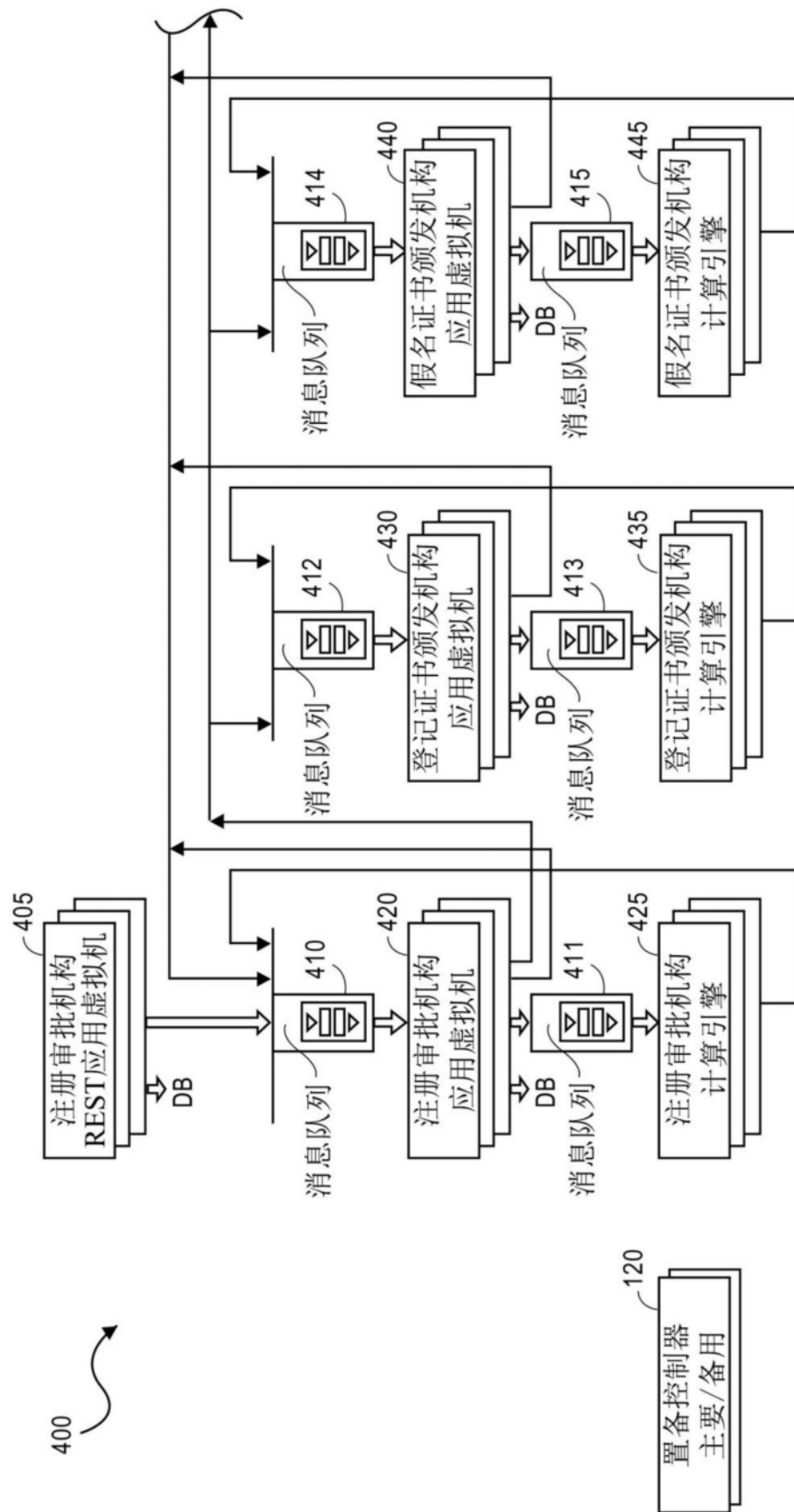


图4A

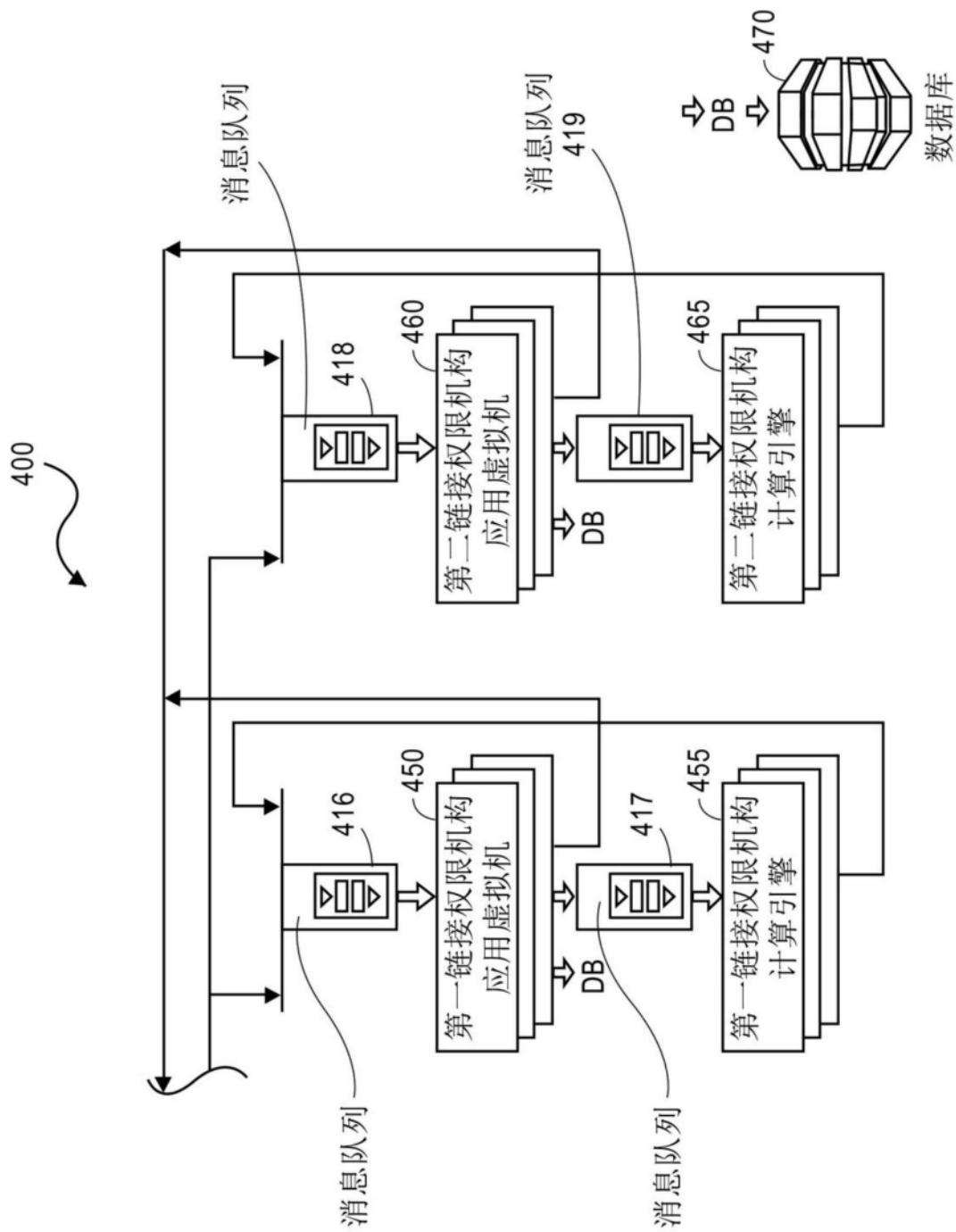


图4B

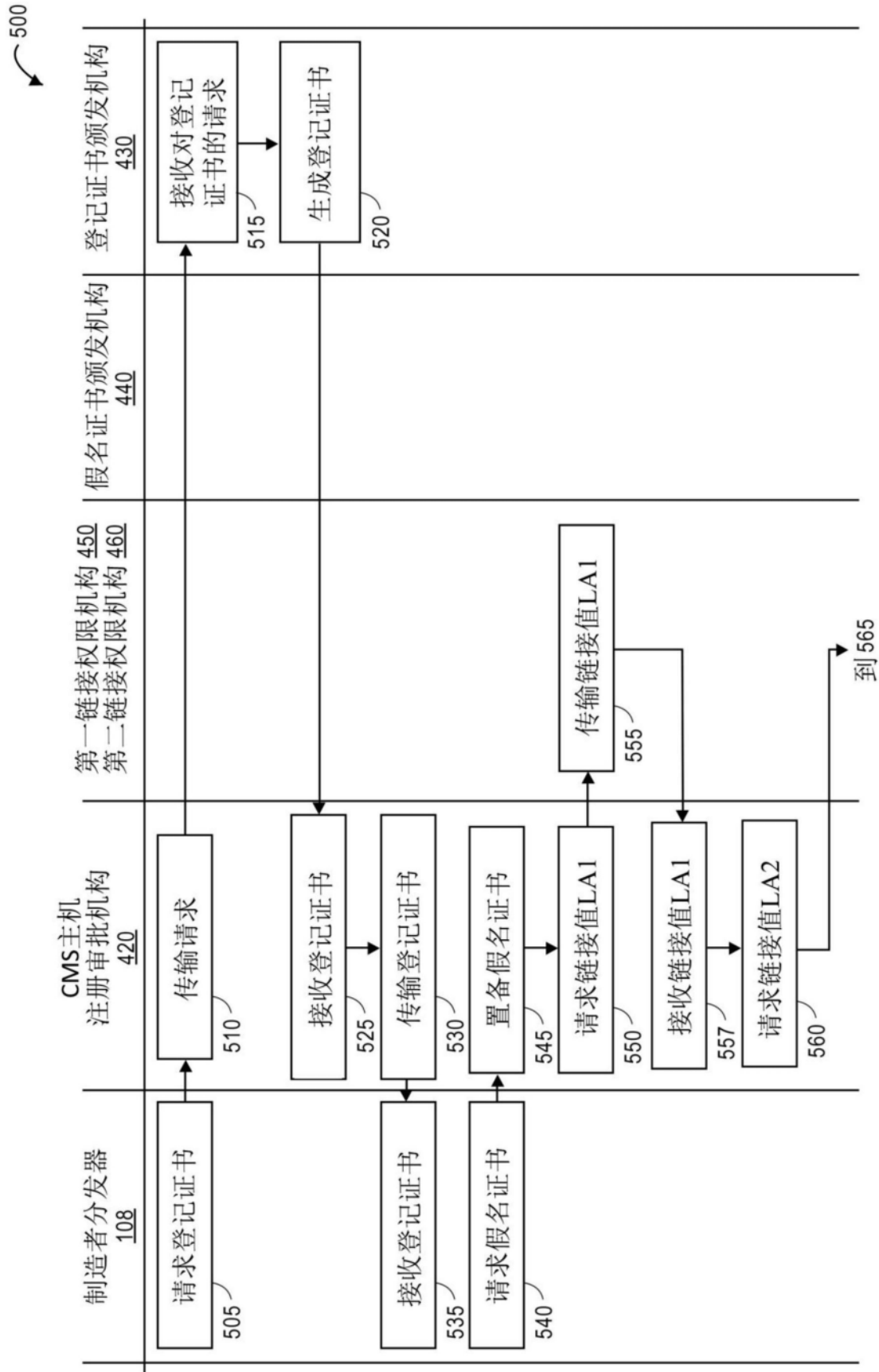


图5A

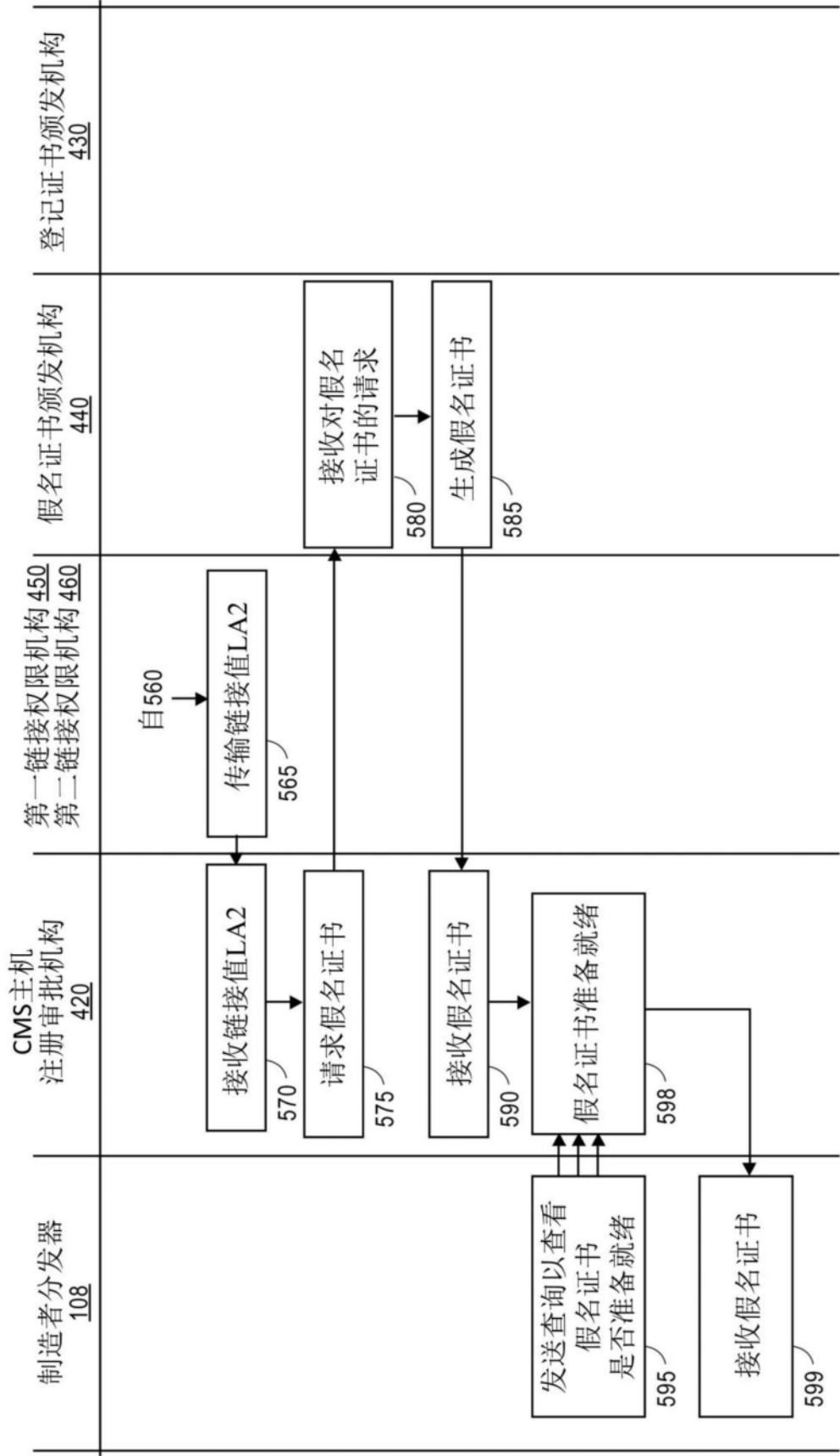


图5B

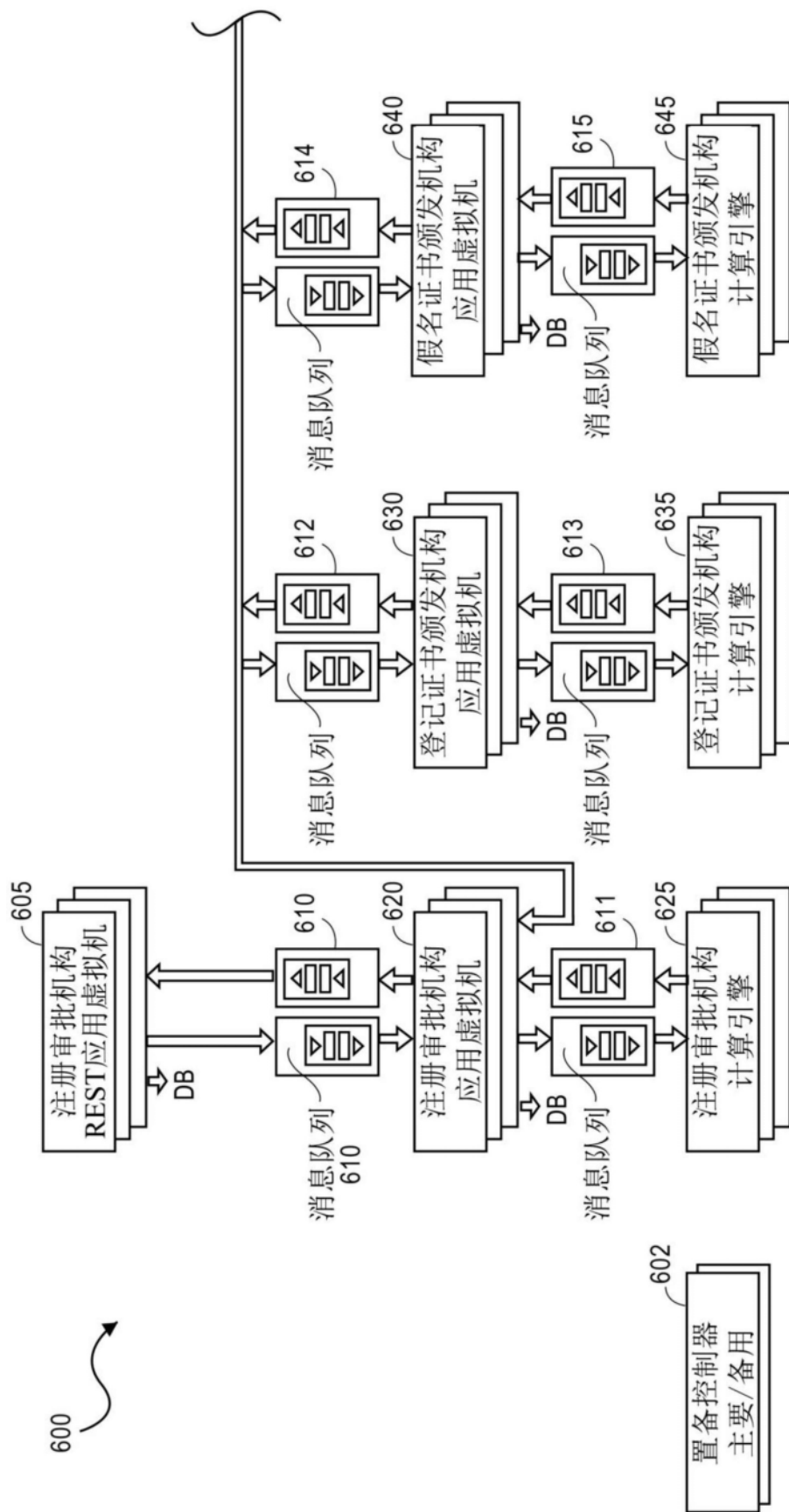


图6A

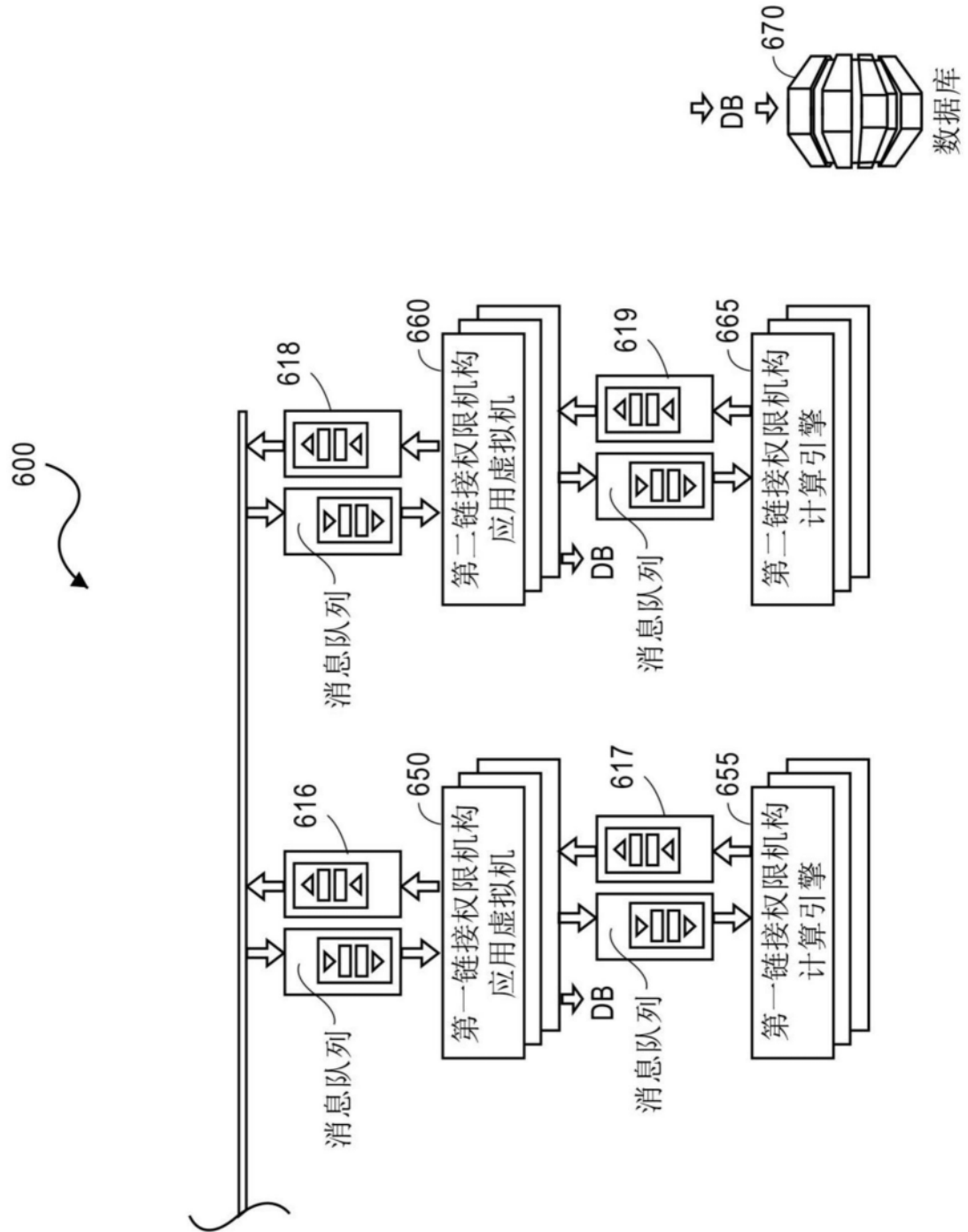


图6B

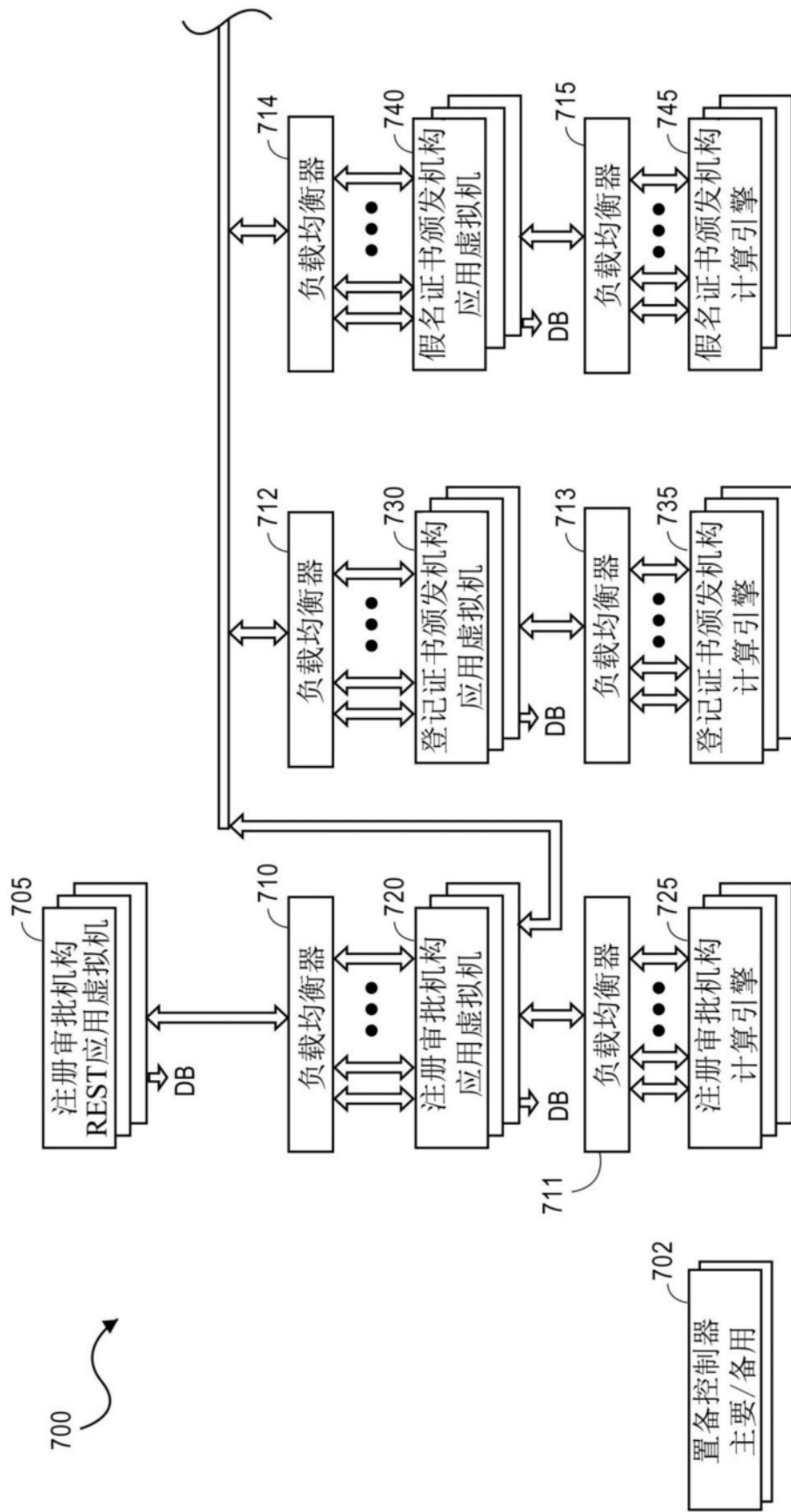


图7A

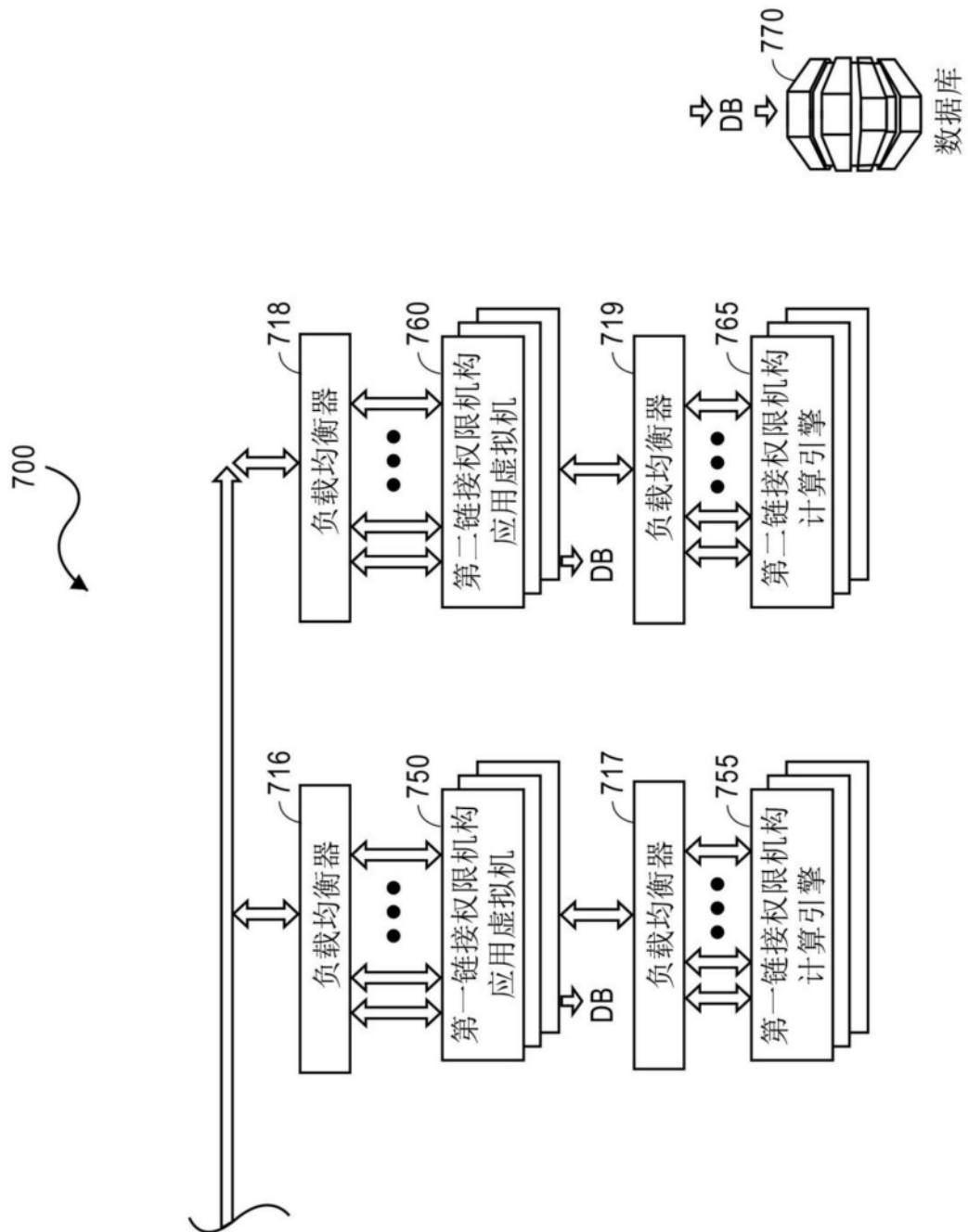


图7B

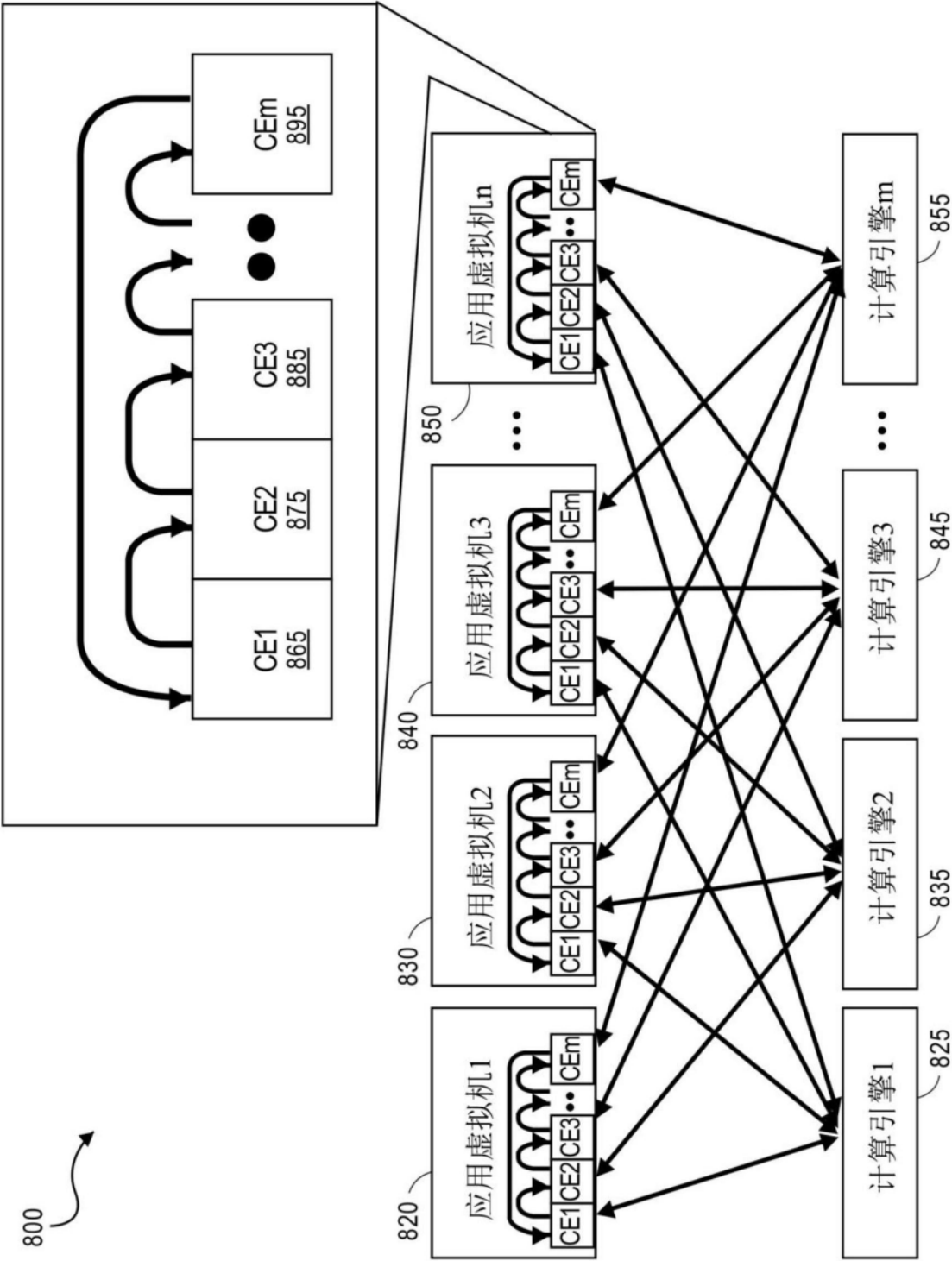


图8

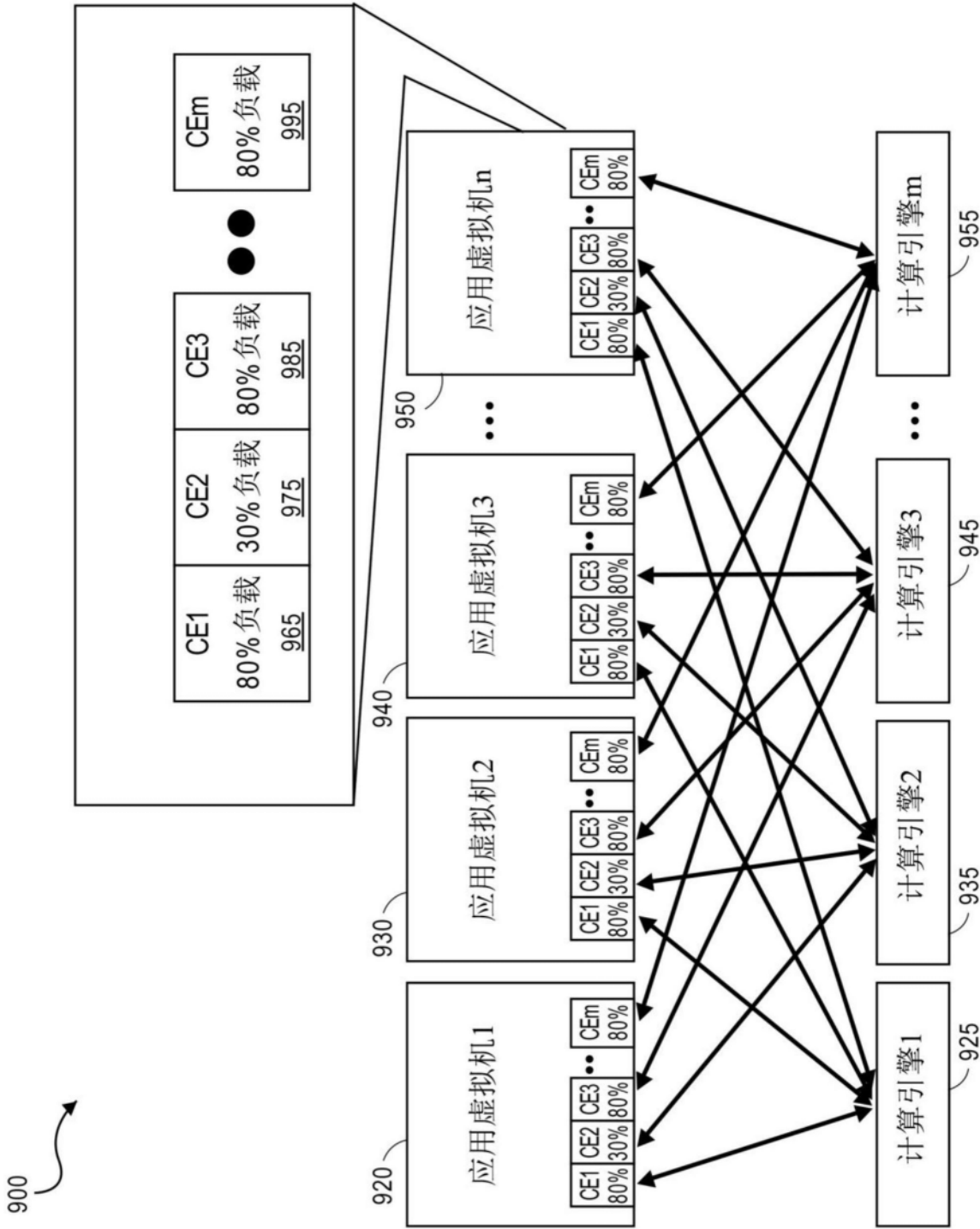


图9

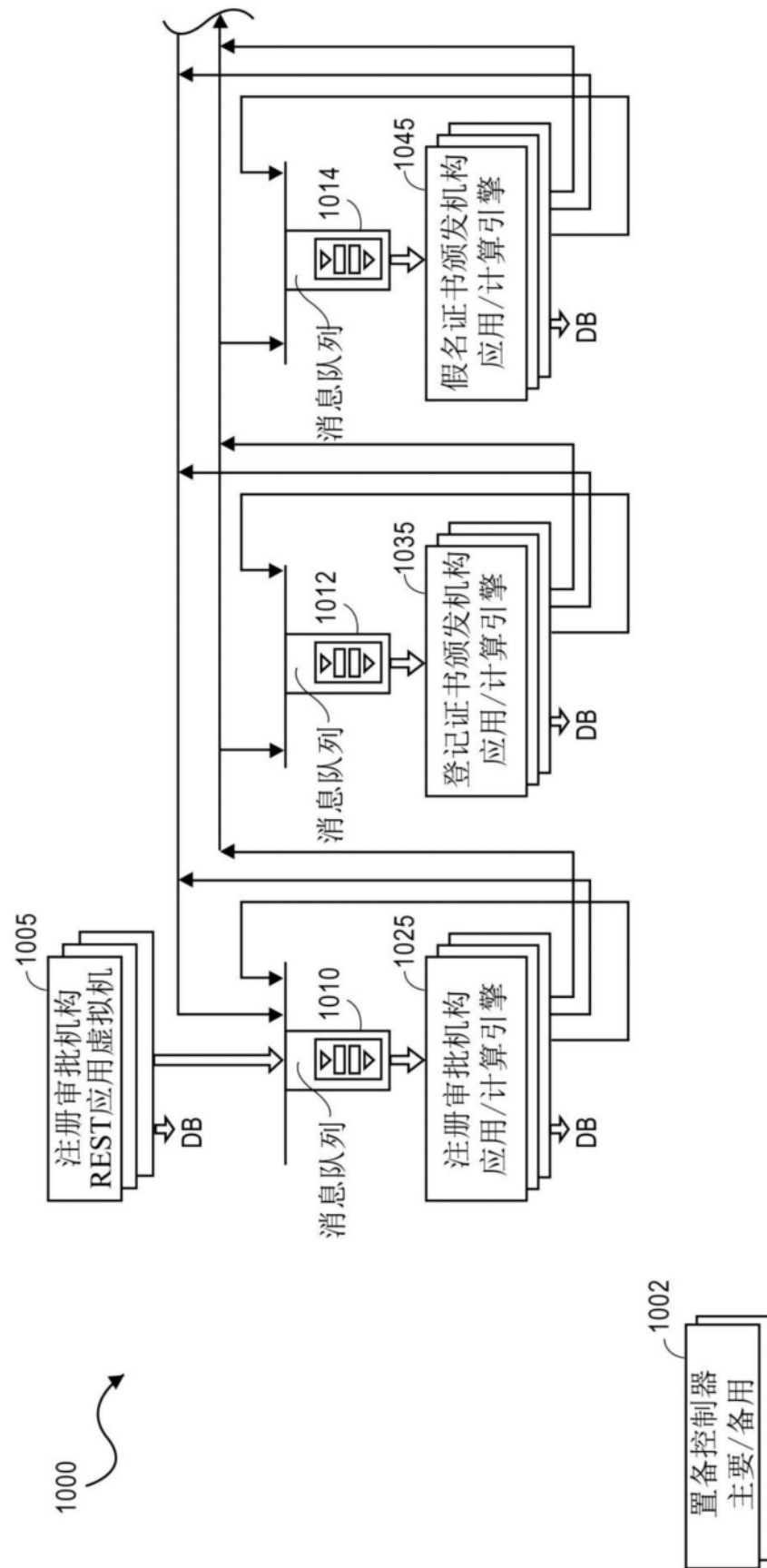


图10A

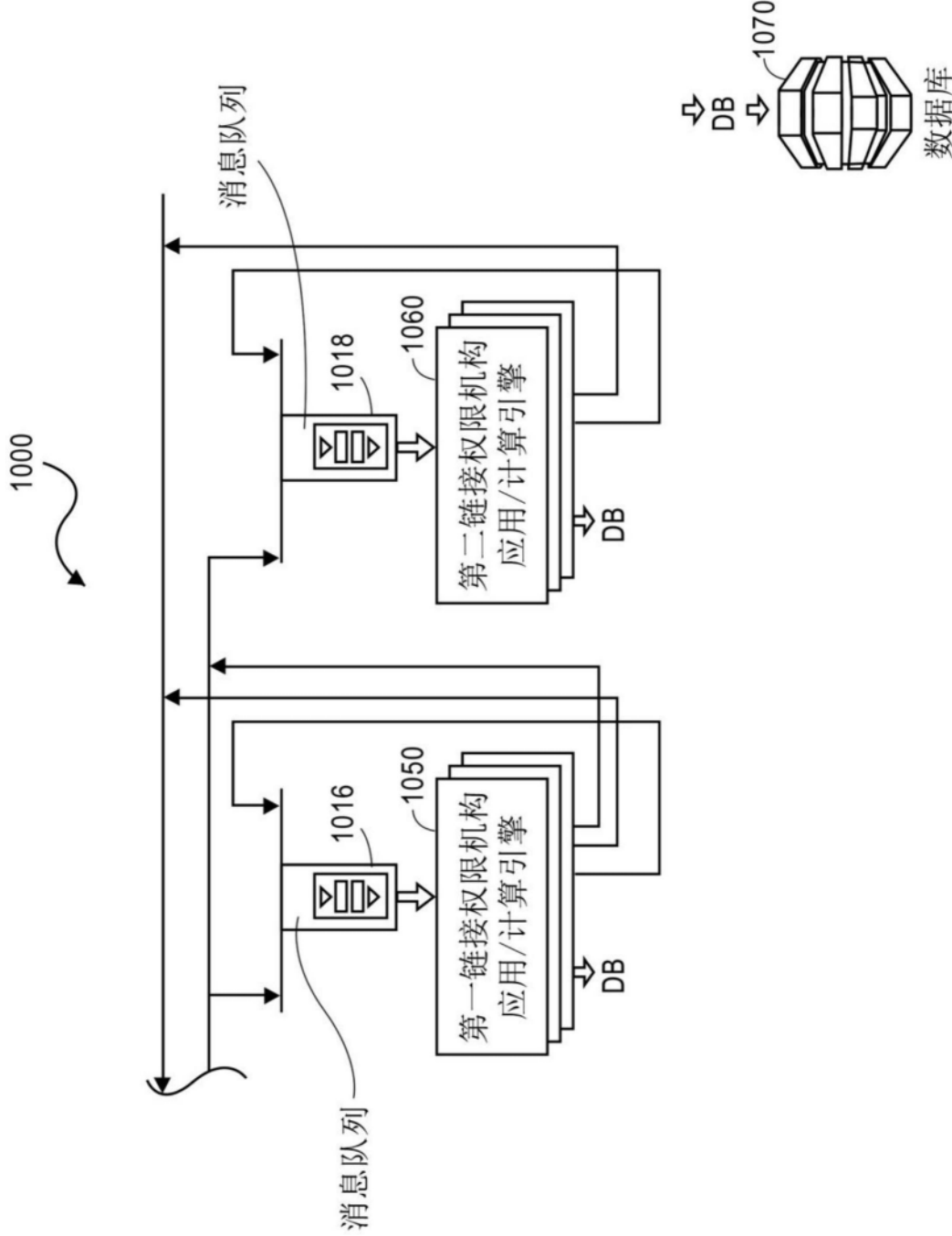


图10B

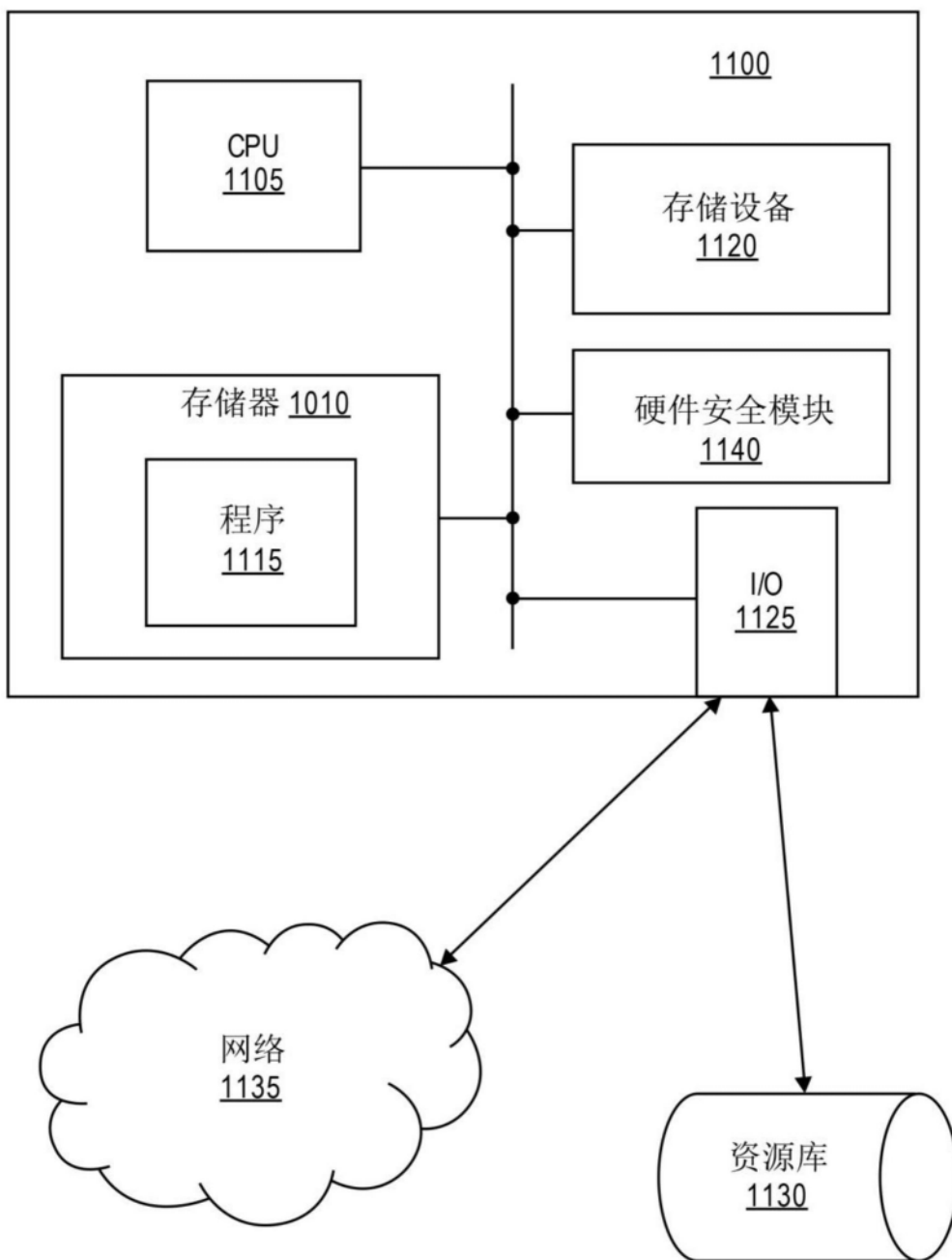


图11