(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118523905 A
(43)申请公布日 2024.08.20

(21)申请号 202310171584.8

(22)申请日 2023.02.20

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 王海光 李铁岩 康鑫 雷中定

(74)专利代理机构 北京市金杜律师事务所 11256
专利代理师 张宁 姚杰

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)

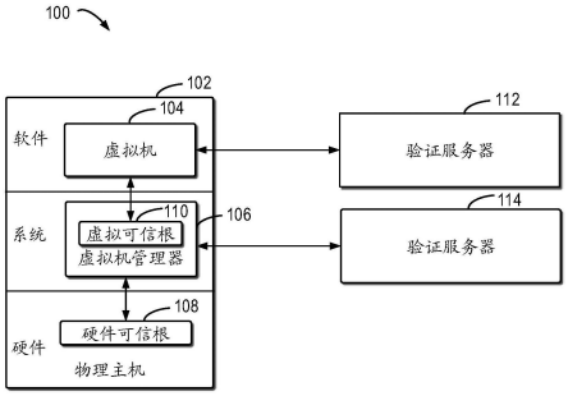
权利要求书7页 说明书28页 附图23页

(54)发明名称

用于获取证书或凭证的方法、装置、设备和存储介质

(57)摘要

本申请提供了用于获取证书或凭证的方法、装置、设备、存储介质和程序产品，涉及数据安全领域。该方法包括在物理主机处向验证服务器发送用于获取加密证书的请求，该请求包括针对虚拟机的虚拟可信根的目标公钥；从验证服务器接收由目标公钥加密的随机数；基于加密的随机数来从物理主机的硬件可信根获取经签名的远程证明信息；向验证服务器发送经签名的远程证明信息和目标公钥；以及从验证服务器接收针对目标公钥的加密证书。本申请的实施例实现了虚拟可信根和硬件可信根的关联关系，改进了对应于硬件可信根的虚拟可信根的验证效率，提高了用户体验。



CN 118523905 A

1.一种用于获取证书的方法,包括:

在物理主机处向验证服务器发送用于获取加密证书的请求,所述请求包括针对虚拟机的虚拟可信根的目标公钥;

从所述验证服务器接收由所述目标公钥加密的随机数;

基于所述加密的随机数来从所述物理主机的硬件可信根获取经签名的远程证明信息,所述经签名的远程证明信息包括针对所述硬件可信根的签名证书;

向所述验证服务器发送所述经签名的远程证明信息和所述目标公钥;以及

从所述验证服务器接收针对所述目标公钥的加密证书。

2.根据权利要求1所述的方法,其中获取所述经签名的远程证明信息包括:

使用与所述目标公钥相对应的目标私钥来对所述加密的随机数进行解密;以及

基于解密的随机数来获取针对所述硬件可信根的本地证明信息,所述本地证明信息包括所述签名证书;

基于所述解密的随机数和所述本地证明信息生成远程证明信息;

使用与所述签名证书相对应的签名私钥对所述远程证明信息进行签名。

3.根据权利要求1所述的方法,其中所述验证服务器是第一验证服务器,所述签名证书是第一签名证书,所述方法还包括:

向第二验证服务器发送所述加密证书以从所述第二验证服务器获取第二签名证书。

4.一种用于提供证书的方法,包括:

响应于从物理主机接收到用于获取加密证书的请求,在验证服务器处生成随机数,所述请求包括针对虚拟机的虚拟可信根的目标公钥;

使用所述目标公钥对所述随机数进行加密;

向所述物理主机发送经加密的所述随机数;

从所述物理主机接收所述目标公钥和经签名的远程证明信息,所述经签名的远程证明信息包括针对所述物理主机的硬件可信根的签名证书;以及

响应于所述经签名的远程证明信息通过验证,向所述物理主机发送加密证书,所述加密证书是针对所述目标公钥的。

5.根据权利要求4所述的方法,所述方法还包括:

通过以下操作来验证所述经签名的远程证明信息:

利用所述签名证书中的验证公钥验证所述签名;以及

确定所述经签名的远程证明信息是否包括所述随机数;以及

响应于所述签名通过验证并且所述经签名的远程证明信息包括所述随机数,确定所述经签名的远程证明信息通过验证。

6.一种用于获取凭证的方法,包括:

在物理主机处向验证服务器发送用于获取凭证的请求;

从所述验证服务器获取随机数;

基于所述随机数和一组公钥,从所述物理主机的硬件可信根获取经签名的远程证明信息,所述经签名的远程证明信息包括针对所述硬件可信根的签名证书;

向所述验证服务器发送回复信息,所述回复信息包括所述经签名的远程证明信息、关于所述一组公钥的指示信息、以及所述随机数;以及

从所述验证服务器获取所述凭证，所述凭证指示所述一组公钥的可信性。

7.根据权利要求6所述的方法，从所述物理主机的硬件可信根获取经签名的远程证明信息包括：

基于所述随机数和所述一组公钥，生成字符串；以及

基于所述字符串来生成目标哈希值；

基于所述目标哈希值，从所述物理主机的硬件可信根获取经签名的远程证明信息。

8.根据权利要求7所述的方法，其中生成所述字符串包括：

通过对所述随机数和所述一组公钥、虚拟机管理器的互联网协议地址、所述虚拟机管理器的远程验证服务的端口号进行链接来形成所述字符串。

9.根据权利要求7所述的方法，其中生成所述字符串包括：

通过将所述一组公钥输入累加器来获得根值；以及

基于所述根值和所述随机数，生成所述字符串。

10.根据权利要求9所述的方法，其中基于所述根值和所述随机数，生成所述字符串包括：

通过对所述随机数、所述根值、虚拟机管理器的互联网协议地址和所述虚拟机管理器的远程验证服务的端口号进行链接来形成所述字符串。

11.根据权利要求7所述的方法，其中基于所述目标哈希值，从所述物理主机的硬件可信根获取经签名的远程证明信息包括：

基于所述目标哈希值，获取针对所述硬件可信根的本地证明信息，所述本地证明信息包括所述签名证书；

基于所述目标哈希值和所述本地证明信息来生成远程证明信息；

使用与所述签名证书相对应的签名私钥对所述远程证明信息进行签名。

12.根据权利要求6所述的方法，其中所述请求是第一请求，所述经签名的远程证明信息是第一经签名的远程证明信息，所述验证服务器是第一验证服务器，所述签名是第一签名，所述方法还包括：

响应于启动虚拟机和对应的虚拟可信根，从所述一组公钥中选择分配给所述虚拟可信根的公钥；

获取针对所述公钥的签名证书；

向第二验证服务器发送注册所述虚拟机的第二请求，所述第二请求包括所述虚拟机的标识；

从所述第二验证服务器接收用于获取证明信息的第三请求，所述第三请求包括由所述第二验证服务器生成的随机数；以及

向所述第二验证服务器发送针对所述虚拟机的经签名的第二远程证明信息以用于确定所述虚拟机的可信状态，所述经签名的第二远程证明信息包括所述签名证书和对应的第二签名。

13.根据权利要求12所述的方法，其中所述第三请求还包括获取证明信息的策略；

其中发送所述经签名的第二远程证明信息包括：

基于所述策略，发送所述经签名的第二远程证明信息。

14.根据权利要求13所述的方法，其中基于所述策略，发送所述经签名的第二远程证明

信息包括：

响应于所述策略指示仅获取针对虚拟机的证明信息，基于所述随机数从所述虚拟可信根获取所述经签名的第二远程证明信息，所述经签名的第二远程证明信息还包括所述物理主机中的虚拟机管理器的互联网协议地址和所述虚拟机管理器的远程验证服务的端口号；

向所述第二验证服务器发送所述经签名的第二远程证明信息；

响应于接收到用于获取所述凭证的第四请求，基于所述签名证书中的公钥，获取所述凭证，所述第四请求包括所述互联网协议地址、所述端口号和所述签名证书；以及

向所述第二验证服务器发送所述凭证以确定所述虚拟机的可信状态。

15.根据权利要求13所述的方法，其中基于所述策略，发送所述经签名的第二远程证明信息包括：

响应于所述策略指示获取针对虚拟机的证明信息和所述凭证，从所述虚拟可信根获取所述经签名的第二远程证明信息；

基于所述公钥来从所述虚拟机管理器获取所述凭证；以及

向所述第二验证服务器发送所述经签名的第二远程证明信息和所述凭证以用于确定所述虚拟机的可信状态。

16.一种用于提供凭证的方法，包括：

在验证服务器处从物理主机接收回复信息，所述回复信息包括经签名的远程证明信息、关于一组公钥的指示信息和随机数，所述经签名的远程证明信息包括针对所述物理主机的硬件可信根的签名证书；

对所述经签名的远程证明信息进行验证；

响应于所述经签名的远程证明信息通过验证，基于所述远程证明信息和所述指示信息，生成所述凭证，所述凭证指示所述一组公钥的可信性；以及

将所述凭证发送给所述物理主机。

17.根据权利要求16所述的方法，其中所述经签名的远程证明信息还包括目标哈希值，其中对所述经签名的远程证明信息进行验证包括：

通过所述签名证书中的公钥验证所述经签名的远程证明信息中的签名；

响应于所述签名通过验证，基于所述随机数和所述指示信息，生成验证哈希值；以及

通过将所述目标哈希值和所述验证哈希值进行比较来验证所述经签名的远程证明信息。

18.根据权利要求17所述的方法，其中所述指示信息包括所述一组公钥，其中生成所述验证哈希值包括：

基于所述随机数和所述一组公钥，生成字符串；以及

基于所述字符串来生成所述验证哈希值。

19.根据权利要求18所述的方法，其中所述回复信息还包括所述物理主机中的虚拟机管理器的互联网协议地址、所述虚拟机管理器的远程验证服务的端口号；

其中生成所述字符串包括：

通过对所述随机数、所述一组公钥、所述互联网协议地址和所述端口号进行链接来形成所述字符串。

20.根据权利要求17所述的方法，其中所述指示信息包括根值，所述根值是通过将所述

一组公钥输入累加器而获得的，其中生成所述验证哈希值包括：

基于所述随机数和所述根值，生成字符串；以及

基于所述字符串来生成所述验证哈希值。

21.根据权利要求20所述的方法，其中所述回复信息还包括所述物理主机中的虚拟机管理器的互联网协议地址、所述虚拟机管理器的远程验证服务的端口号；

其中生成所述字符串包括：

通过对所述随机数、所述根值、所述互联网协议地址和所述端口号进行链接来形成所述字符串。

22.根据权利要求16所述的方法，其中生成所述凭证包括：

通过对远程证明信息进行评估来生成评估结果；

响应于所述评估结果满足预定要求，生成所述凭证，所述凭证包括将所述评估结果。

23.一种用于验证信息的方法，包括：

响应于从物理主机接收到注册所述物理主机中的虚拟机的第一请求，在验证服务器处生成随机数；

向所述物理主机发送用于获取证明信息的第二请求，所述第二请求包括所述随机数；以及

从所述物理主机接收针对所述虚拟机的经签名的远程证明信息和凭证，所述经签名的远程证明信息包括签名证书和对应的签名，所述签名证书是针对从一组公钥中选择的分配给所述虚拟机的公钥的证书，所述凭证指示所述一组公钥的可信性；

基于所述经签名的远程证明信息和所述凭证，确定所述虚拟机的可信状态。

24.根据权利要求23所述的方法，其中所述经签名的远程证明信息还包括所述物理主机中的虚拟机管理器的互联网协议地址和所述虚拟机管理器的远程验证服务的端口号，其中所述第二请求还包括从所述物理主机获取证明信息的策略，所述策略指示仅获取针对虚拟机的证明信息，其中接收针对所述虚拟机的经签名的远程证明信息和凭证包括：

接收所述经签名的远程证明信息；

对所述经签名的远程证明信息进行验证；

响应于所述经签名的远程证明信息通过所述验证，从所述经签名的远程证明信息获取所述签名证书、所述互联网协议地址和所述端口号；

向所述物理主机发送获取凭证的第三请求，所述第三请求包括所述互联网协议地址、所述端口号和所述签名证书；

从所述物理主机接收所述凭证。

25.根据权利要求24所述的方法，其中确定所述虚拟机的可信状态包括：

对所述凭证进行验证；

响应于所述凭证通过验证，确定所述签名证书中的公钥是否被所述凭证支持；以及

响应于所述公钥被所述凭证支持，确定所述虚拟机是可信的。

26.根据权利要求23所述的方法，其中所述第二请求还包括从所述物理主机获取证明信息的策略，所述策略指示获取针对虚拟机的证明信息和所述凭证，其中确定所述虚拟机的可信状态包括：

对所述经签名的远程证明信息和所述凭证进行验证；

响应于所述经签名的远程证明信息和所述凭证通过验证，从所述经签名的远程证明信息获取所述签名证书；

确定所述签名证书中的公钥是否被所述凭证支持；以及

响应于所述公钥被所述凭证支持，确定所述虚拟机是可信的。

27.根据权利要求25或26所述的方法，其中确定所述公钥是否被所述凭证支持包括：

确定所述公钥是否存在于所述凭证中。

28.根据权利要求25或26所述的方法，其中所述凭证包括根值，所述根值是通过将所述一组公钥输入累加器而获得的，其中确定所述公钥是否被所述凭证支持包括：

提取所述凭证中的根值；以及

基于所述根值和所述公钥，确定所述公钥是否被所述凭证支持。

29.一种用于验证信息的方法，包括：

响应于从物理主机接收到注册所述物理主机中的虚拟机的第一请求，在第一验证服务器处向所述物理主机发送获取证明信息的第二请求，所述第二请求包括随机数；

接收针对所述虚拟机的经签名的远程证明信息，所述远程证明信息包括签名证书，所述签名证书是针对从一组公钥中选择的分配给所述虚拟机的公钥的证书；

响应于所述经签名的远程证明信息通过验证，获取所述签名证书；

向第二验证服务器发送用于获取凭证的第三请求，所述第三请求包括所述签名证书；

从所述第二验证服务器获取所述凭证；

基于所述凭证来确定所述虚拟机的可信状态，所述凭证指示一组公钥的可信性。

30.根据权利要求29所述的方法，其中确定所述可信状态包括：

响应于接收到所述凭证，对所述凭证进行验证；

响应于所述凭证通过所述验证，确定所述签名证书的公钥是否被所述凭证支持；以及

响应于所述公钥被所述凭证支持，确定所述虚拟机是可信的。

31.一种用于获取证书的装置，其特征在于，所述装置包括：

请求发送单元，被配置为在物理主机处向验证服务器发送用于获取加密证书的请求，所述请求包括针对虚拟机的虚拟可信根的目标公钥；

随机数获取单元，被配置为从所述验证服务器获取由所述目标公钥加密的随机数；

远程证明信息获取单元，被配置为基于所述加密的随机数来从所述物理主机的硬件可信根获取经签名的远程证明信息，所述经签名的远程证明信息包括针对所述硬件可信根的签名证书；

证明信息和公钥发送单元，被配置为向所述验证服务器发送所述经签名的远程证明信息和所述目标公钥；以及

加密证书接收单元，被配置为以用于从所述验证服务器接收针对所述目标公钥的加密证书。

32.一种用于提供证书的装置，其特征在于，所述装置包括：

随机数生成单元，被置为响应于从物理主机接收到用于获取加密证书的请求，在验证服务器处生成随机数，所述请求包括针对虚拟机的虚拟可信根的目标公钥；

加密单元，被配置为使用所述目标公钥对所述随机数进行加密；

随机数发送单元，被配置为向所述物理主机发送经加密的所述随机数；

远程证明信息接收单元，被配置为从所述物理主机接收所述目标公钥和经签名的远程证明信息，所述经签名的远程证明信息包括针对所述物理主机的硬件可信根的签名证书；以及

证书发送单元，被配置为响应于所述经签名的远程证明信息通过验证，向所述物理主机发送加密证书，所述加密证书是针对所述目标公钥的。

33.一种用于获取凭证的装置，其特征在于，所述装置包括：

请求发送单元，被配置为在物理主机处向验证服务器发送用于获取凭证的请求；

随机数获取单元，被配置为从所述验证服务器获取随机数；

远程证明信息获取单元，被配置为基于所述随机数和一组公钥，从所述物理主机的硬件可信根获取经签名的远程证明信息，所述经签名的远程证明信息包括针对所述硬件可信根的签名证书；

回复信息发送单元，被配置为向所述验证服务器发送回复信息，所述回复信息包括所述经签名的远程证明信息、关于所述一组公钥的指示信息以及所述随机数；以及

凭证获取单元，被配置为从所述验证服务器获取所述凭证，所述凭证指示所述一组公钥的可信性。

34.一种用于提供凭证的装置，其特征在于，所述装置包括：

回复信息接收单元，被配置为在验证服务器处从物理主机接收回复信息，所述回复信息包括经签名的远程证明信息、关于一组公钥的指示信息和随机数，所述经签名的远程证明信息包括针对所述物理主机的硬件可信根的签名证书；

验证单元，被配置为对所述经签名的远程证明信息进行验证；

凭证生成单元，被配置为响应于所述经签名的远程证明信息通过验证，基于所述远程证明信息和所述指示信息，生成所述凭证，所述凭证指示所述一组公钥的可信性；以及

凭证发送单元，被配置为将所述凭证发送给所述物理主机。

35.一种用于验证信息的装置，其特征在于，所述装置包括：

随机数生成单元，被配置为响应于从物理主机接收到注册所述物理主机中的虚拟机的第一请求，在验证服务器处生成随机数；

证明信息获取单元，被配置为向所述物理主机发送用于获取证明信息的第二请求，所述第二请求包括所述随机数；以及

证明信息和凭证接收单元，被配置为从所述物理主机接收针对所述虚拟机的经签名的远程证明信息和凭证，所述经签名的远程证明信息包括签名证书和对应的签名，所述签名证书是针对从一组公钥中选择的分配给所述虚拟机的公钥的证书，所述凭证指示所述一组公钥的可信性；

可信状态确定单元，被配置为基于所述经签名的远程证明信息和所述凭证，确定所述虚拟机的可信状态。

36.一种用于验证信息的装置，其特征在于，所述装置包括：

证明信息获取单元，被配置为响应于从物理主机接收到注册所述物理主机中的虚拟机的第一请求，在第一验证服务器处向所述物理主机发送获取证明信息的第二请求，所述第二请求包括随机数；

远程证明信息接收单元，被配置为接收针对所述虚拟机的经签名的远程证明信息，所

述远程证明信息包括签名证书,所述签名证书是针对从一组公钥中选择的分配给所述虚拟机的公钥的证书;

证书获取单元,被配置为响应于所述经签名的远程证明信息通过验证,获取所述签名证书;

请求发送单元,被配置为向第二验证服务器发送用于获取凭证的第三请求,所述第三请求包括所述签名证书;

凭证获取单元,被配置为从所述第二验证服务器获取所述凭证;

可信状态确定单元,被配置为基于所述凭证来确定所述虚拟机的可信状态,所述凭证指示一组公钥的可信性。

37.一种电子设备,包括:

至少一个计算单元;

至少一个存储器,所述至少一个存储器被耦合到所述至少一个计算单元并且存储用于由所述至少一个计算单元执行的指令,所述指令当由所述至少一个计算单元执行时,使得所述设备执行根据权利要求1-30中任一项所述的方法。

38.一种计算机可读存储介质,其上存储有计算机程序,所述程序被处理器执行时实现根据权利要求1-30中任一项所述的方法。

39.一种计算机程序产品,包括计算机可执行指令,其中所述计算机可执行指令被处理器执行时实现根据权利要求1-30中任一项所述的方法。

用于获取证书或凭证的方法、装置、设备和存储介质

技术领域

[0001] 本申请的实施例主要涉及数据安全领域。更具体地，本申请的实施例涉及用于获取证书或凭证的方法、装置、设备和存储介质。

背景技术

[0002] 随着移动互联网的快速发展，越来越多的传统服务如政府服务，移动支付等都转移到了互联网上。移动互联网成了人们生活中不可或缺的基础设施。为了满足人们对服务质量的要求，电信运营商需要不断采用新技术，提供服务部署的敏捷性和网络容量的弹性伸缩能力。网络虚拟化和云化技术为运营商提供了网络快速部署和弹性伸缩的能力。于此同时，网络虚拟化技术打破了原有设备物理边界所带来的安全与可信特性。运营商不在拥有物理设备，而是在自己或者第三方的云平台上运行大量的虚拟设备，因此运营商必须通过新的技术手段保证在虚拟化和云化场景下虚拟化设备的可信性。远程验证技术可以为运营商提供设备可信特性的远程验证能力。然而，在该过程中还存在许多需要解决的问题。

发明内容

[0003] 本申请的实施例提供了一种用于获取证书或凭证的方案。

[0004] 根据本申请的第一方面，提供了一种用于获取证书的方法。该方法包括：在物理主机处向验证服务器发送用于获取加密证书的请求，该包括针对虚拟机的虚拟可信根的目标公钥；从验证服务器接收由目标公钥加密的随机数；基于加密的随机数来从物理主机的硬件可信根获取经签名的远程证明信息，经签名的远程证明信息包括针对硬件可信根的签名证书；向验证服务器发送经签名的远程证明信息和目标公钥；以及从验证服务器接收针对目标公钥的加密证书。

[0005] 通过该方式，本申请的实施例利用硬件可信根的签名证书来生成远程证明信息，然后向验证服务器发送经签名的远程证明信息和目标公钥。通过远程证明信息中包含的硬件可信根的签名证书可以证明发送该远程证明信息的设备是可信的，进而可以确定来自该设备的针对虚拟机的虚拟可信根的目标公钥也是可信的。因此，这种方式实现了虚拟可信根和硬件可信根的关联，解决了虚拟机进行深度证明时面临的硬件可信根设备导致的性能问题，改进了对应于硬件可信根设备的虚拟可信根的验证效率，提高了用户体验。

[0006] 在一些实施例中，其中生成密钥对包括：响应于虚拟可信根被启动，由虚拟可信根生成目标公钥。通过该方式，可以提高虚拟可信根的安全性。

[0007] 在一些实施例中，其中获取经签名的远程证明信息包括：使用与所述目标公钥相对应的目标私钥来对加密的随机数进行解密；以及基于解密的随机数来获取针对硬件可信根的本地证明信息，本地证明信息包括签名证书；基于解密的随机数和本地证明信息生成远程证明信息；使用与签名证书相对应的签名私钥对远程证明信息进行签名。通过该方式，可以快速准确地获取到经签名的远程证明信息，提高了获取信息的准确性和安全性。

[0008] 在一些实施例中，其中验证服务器是第一验证服务器，签名证书是第一签名证书，

该方法还包括:向第二验证服务器发送加密证书以从第二验证服务器获取第二签名证书。通过该方式,提高了获取证书的安全性和效率。

[0009] 根据本申请的第二方面,提供了一种用于提供证书的方法。该方法包括:响应于从物理主机接收到用于获取加密证书的请求,在验证服务器处生成随机数,请求包括针对虚拟机的虚拟可信根的目标公钥;使用目标公钥对随机数进行加密;向物理主机发送经加密的随机数;从物理主机接收目标公钥和经签名的远程证明信息,经签名的远程证明信息包括针对物理主机的硬件可信根的签名证书;以及响应于经签名的远程证明信息通过验证,向物理主机发送加密证书,加密证书是针对目标公钥的。

[0010] 通过该方式,本申请的实施例实现了虚拟可信根和硬件可信根的关联关系,解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题,改进了对应于硬件可信根设备的虚拟可信根的验证效率,提高了用户体验。

[0011] 在一些实施例中,该方法还包括:通过以下操作来验证经签名的远程证明信息:利用签名证书中的验证公钥验证签名;以及确定经签名的远程证明信息是否包括随机数;以及响应于签名通过验证并且经签名的远程证明信息包括随机数,确定经签名的远程证明信息通过验证。通过该方式,可以快速和安全的验证远程证明信息,提高了验证效率和效果。

[0012] 根据本申请的第三方面,提供了一种用于获取凭证的方法。该方法包括:在物理主机处向验证服务器发送用于获取凭证的请求;从验证服务器获取随机数;基于随机数和一组公钥,从物理主机的硬件可信根获取经签名的远程证明信息,经签名的远程证明信息包括针对硬件可信根的签名证书;向验证服务器发送回复信息,回复信息包括经签名的远程证明信息、关于一组公钥的指示信息以及随机数;以及从验证服务器获取凭证,所述凭证指示一组公钥的可信性。

[0013] 通过该方式,本申请的实施例实现了虚拟可信根和硬件可信根的关联关系,解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题,改进了对应于硬件可信根设备的虚拟可信根的验证效率,提高了用户体验。

[0014] 在一些实施例中,该方法还包括:由物理主机中的虚拟机管理器生成一组公钥。通过该方式,可以快速准确地获取一组公钥。

[0015] 在一些实施例中,从物理主机的硬件可信根获取经签名的远程证明信息包括:基于随机数和一组公钥,生成字符串;以及基于字符串来生成目标哈希值;基于目标哈希值,从物理主机的硬件可信根获取经签名的远程证明信息。通过该方式,可以提高数据的安全性,并且改进了验证效果。

[0016] 在一些实施例中,其中生成字符串包括:通过对随机数、一组公钥、虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号进行链接来形成字符串。通过该方式,可以快速的生成字符串,并且提高了字符串的安全性。

[0017] 在一些实施例中,其中生成字符串包括:通过将一组公钥输入累加器来获得根值;以及基于根值和随机数,生成字符串。通过该方式,可以快速的生成字符串,并且提高了字符串的安全性。

[0018] 在一些实施例中,其中基于根值和随机数,生成字符串包括:通过对随机数、根值、虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号进行链接来形成字符串。通过该方式,可以快速的形成字符串,并且提高了字符串的安全性。

[0019] 在一些实施例中，其中指示信息包括根值。通过该方式，可以提高密钥的验证效率。

[0020] 在一些实施例中，其中指示信息包括一组公钥。通过该方式，可以提高密钥的验证效率和安全性。

[0021] 在一些实施例中，其中基于所述目标哈希值，从所述物理主机的硬件可信根获取经签名的远程证明信息包括：基于目标哈希值，获取针对硬件可信根的本地证明信息，本地证明信息包括签名证书；基于目标哈希值和述本地证明信息来生成远程证明信息；使用与签名证书相对应的签名私钥对远程证明信息进行签名。通过该方式，可以提高远程证明信息的安全性。

[0022] 在一些实施例中，其中请求是第一请求，经签名的远程证明信息是第一经签名的远程证明信息，验证服务器是第一验证服务器，签名是第一签名，该方法还包括：响应于启动虚拟机和对应的虚拟可信根，从一组公钥中选择分配给虚拟可信根的公钥；获取针对公钥的签名证书；向第二验证服务器发送注册虚拟机的第二请求，第二请求包括虚拟机的标识；从第二验证服务器接收用于获取证明信息的第三请求，第三请求包括由第二验证服务器生成的随机数；以及向第二验证服务器发送针对虚拟机的经签名的第二远程证明信息以用于确定虚拟机的可信状态，经签名的第二远程证明信息包括签名证书和对应的第二签名。通过该方式，可以快速的通过硬件可信根的可信性确定出虚拟机的可信状态，提高了可信状态确定效率，改进了用户体验。

[0023] 在一些实施例中，其中第三请求还包括获取证明信息的策略；其中发送经签名的第二远程证明信息包括：基于策略，发送经签名的第二远程证明信息。通过该方式，可以采用多种方式获取远程证明信息，提高了用户体验。

[0024] 在一些实施例中，其中基于策略，发送经签名的第二远程证明信息包括：响应于策略指示仅获取针对虚拟机的证明信息，基于随机数从虚拟可信根获取经签名的第二远程证明信息，经签名的第二远程证明信息还包括物理主机中的虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号；向第二验证服务器发送经签名的第二远程证明信息；响应于接收到用于获取凭证的第四请求，基于签名证书中的公钥，获取凭证，第四请求包括互联网协议地址、端口号和签名证书；以及向第二验证服务器发送凭证以确定虚拟机的可信状态。通过该方式，可以快速的通过硬件可信根的可信性确定出虚拟机的可信状态，提高了可信状态确定效率，改进了用户体验。

[0025] 在一些实施例中，其中基于策略，发送经签名的第二远程证明信息包括：响应于策略指示获取针对虚拟机的证明信息和凭证，从虚拟可信根获取经签名的第二远程证明信息；基于公钥来从虚拟机管理器获取凭证；以及向第二验证服务器发送经签名的第二远程证明信息和凭证以用于确定虚拟机的可信状态。通过该方式，可以快速的通过硬件可信根的可信性确定出虚拟机的可信状态，提高了可信状态确定效率，改进了用户体验。

[0026] 根据本申请的第四方面，提供了一种用于提供凭证的方法。该方法包括：在验证服务器处从物理主机接收回复信息，回复信息包括经签名的远程证明信息、关于一组公钥的指示信息和随机数，经签名的远程证明信息包括针对物理主机的硬件可信根的签名证书；对经签名的远程证明信息进行验证；响应于经签名的远程证明信息和目标哈希值通过验证，基于远程证明信息和指示信息，生成凭证，凭证指示一组公钥的可信性；以及将凭证发

送给物理主机。

[0027] 通过该方式，本申请的实施例实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，改进了对应于硬件可信根设备的虚拟可信根的验证效率，提高了用户体验。

[0028] 在一些实施例中，其中所述经签名的远程证明信息包括还包括目标哈希值，其中对经签名的远程证明信息进行验证包括：通过签名证书中的公钥验证经签名的远程证明信息中的签名；响应于签名通过验证，基于随机数和指示信息，生成验证哈希值；以及通过将目标哈希值和验证哈希值进行比较来验证经签名的远程证明信息。通过该方式，可以快速的验证经签名的远程证明信息，提高了验证效率。

[0029] 在一些实施例中，其中指示信息包括一组公钥，其中生成验证哈希值包括：基于随机数和一组公钥，生成字符串；以及基于字符串来生成验证哈希值。通过该方式，可以快速的生成哈希值，从而提高验证效率和安全性。

[0030] 在一些实施例中，其中回复信息还包括物理主机中的虚拟机管理器的互联网协议地址、虚拟机管理器的远程验证服务的端口号；其中生成字符串包括：通过对随机数、一组公钥、互联网协议地址和端口号进行链接来形成字符串。通过该方式，可以提高字符串的生成效率，提高了生成字符串的效率。

[0031] 在一些实施例中，其中指示信息包括根值，根值是通过将一组公钥输入累加器而获得的，其中生成验证哈希值包括：基于随机数和根值，生成字符串；以及基于字符串来生成验证哈希值。通过该方式，可以快速的验证字符串，并且提高了字符串验证的安全性。

[0032] 在一些实施例中，其中回复信息还包括物理主机中的虚拟机管理器的互联网协议地址、虚拟机管理器的远程验证服务的端口号；其中生成字符串包括：通过对随机数、根值、互联网协议地址和端口号进行链接来形成字符串。通过该方式，可以快速的生成字符串，并且提高了字符串的安全性。

[0033] 在一些实施例中，凭证还包括互联网协议地址和端口号。通过该方式，可以提供更多的信息。

[0034] 在一些实施例中，其中生成凭证包括：通过对远程证明信息进行评估来生成评估结果；将评估结果加入凭证。通过该方式，可以提供更多的信息，并且提高了凭证内容的全面性。

[0035] 在一些实施例中，其中生成凭证包括：通过对远程证明信息进行评估来生成评估结果；响应于评估结果满足预定要求，生成凭证，凭证包括将评估结果。通过该方式，可以生成满足预定要求的凭证，进一步验证了远程证明信息。

[0036] 在一些实施例中，该方法还包括：响应于从物理主机接收到用于获取凭证的请求，生成随机数；以及向物理主机发送随机数。通过该方式，可以用于提高获取凭证的准确性。

[0037] 根据本申请的第五方面，提供了一种用于验证信息的方法。该方法包括：响应于从物理主机接收到注册物理主机中的虚拟机的第一请求，在验证服务器处生成随机数；向物理主机发送用于获取证明信息的第二请求，第二请求包括随机数；以及从所述物理主机接收针对虚拟机的经签名的远程证明信息和凭证，经签名的远程证明信息包括签名证书和对应的签名，签名证书是针对从一组公钥中选择的分配给虚拟机的公钥的证书，凭证指示一组公钥的可信性；基于经签名的远程证明信息和凭证，确定虚拟机的可信状态。

[0038] 通过该方式，本申请的实施例实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，改进了对应于硬件可信根设备的虚拟可信根的验证效率，提高了用户体验。

[0039] 在一些实施例中，其中经签名的远程证明信息还包括物理主机中的虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号，其中第二请求还包括从物理主机获取证明信息的策略，策略指示仅获取针对虚拟机的证明信息，其中接收针对虚拟机的经签名的远程证明信息和凭证包括：接收经签名的远程证明信息；对经签名的远程证明信息进行验证；响应于经签名的远程证明信息通过验证，从经签名的远程证明信息获取签名证书、互联网协议地址和端口号；向物理主机发送获取凭证的第三请求，第三请求包括互联网协议地址、端口号和签名证书；从所述物理主机接收所述凭证。通过该方式，可以快速的获取到用于证明物理主机可信的证明信息。

[0040] 在一些实施例中，其中确定所述虚拟机的可信状态包括：对凭证进行验证；响应于凭证通过验证，确定签名证书中的公钥是否被凭证支持；以及响应于公钥被凭证支持，确定虚拟机是可信的。通过该方式，可以基于硬件可信根的可信性确定虚拟可信根的可信性，改进了确定虚拟机的可信性的效率，提高了验证效率。

[0041] 在一些实施例中，其中第二请求还包括从物理主机获取证明信息的策略，策略指示获取针对虚拟机的证明信息和凭证，其中确定虚拟机的可信状态包括：对经签名的远程证明信息和凭证进行验证；响应于经签名的远程证明信息和凭证通过验证，从经签名的远程证明信息获取签名证书；确定签名证书中的公钥是否被凭证支持；以及响应于公钥被凭证支持，确定虚拟机是可信的。通过该方式，可以基于硬件可信根的可信性确定虚拟可信根的可信性，改进了确定虚拟机的可信性的效率，提高了验证效率。

[0042] 在一些实施例中，其中确定公钥是否被凭证支持包括：确定公钥是否存在于凭证中。通过该方式，可以快速的验证公钥是否可用，提高了公钥的验证效率。

[0043] 在一些实施例中，其中凭证包括根值，根值是通过将一组公钥输入累加器而获得的，其中确定公钥是否被凭证支持包括：提取凭证中的根值；以及基于根值和公钥，确定公钥是否被凭证支持。通过该方式，可以快速的验证公钥是否可用，提高了公钥的验证效率。

[0044] 根据本申请的第六方面，提供了一种用于验证信息的方法。该方法包括：响应于从物理主机接收到注册物理主机中的虚拟机的第一请求，在第一验证服务器处向物理主机发送获取证明信息的第二请求，第二请求包括随机数；接收针对虚拟机的经签名的远程证明信息，远程证明信息包括签名证书，签名证书是针对从一组公钥中选择的分配给虚拟机的公钥的证书；响应于经签名的远程证明信息通过验证，获取签名证书；向第二验证服务器发送用于获取凭证的第三请求，该第三请求包括签名证书；从第二验证服务器获取凭证；基于凭证来确定虚拟机的可信状态，凭证指示一组公钥的可信性。

[0045] 通过该方式，本申请的实施例实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，改进了对应于硬件可信根设备的虚拟可信根的验证效率，提高了用户体验。

[0046] 在一些实施例中，其中确定可信状态包括：响应于接收到凭证，对凭证进行验证；响应于凭证通过验证，确定签名证书的公钥是否被凭证支持；以及响应于公钥被凭证支持，确定虚拟机是可信的。通过该方式，可以快速的虚拟机是否可信，提高了检测效率。

[0047] 在一些实施例中，其中确定签名证书的公钥是否被凭证支持包括：确定公钥是否存在于凭证中。通过该方式，可以快速的确定公钥是否是被支持的，提高了验证效率。

[0048] 在一些实施例中，其中凭证包括根值，根值是通过将一组公钥输入累加器而获得的，其中确定签名证书的公钥是否被凭证支持包括：提取凭证中的根值；以及基于根值和公钥，确定公钥是否被凭证支持。通过该方式，可以快速的确定公钥是否是被支持的，提高了验证效率。

[0049] 根据本申请的第七方面，提供了一种用于获取证书的装置。该装置包括：请求发送单元，被配置为在物理主机处向验证服务器发送用于获取加密证书的请求，请求包括针对虚拟机的虚拟可信根的目标公钥；随机数获取单元，被配置为从验证服务器获取由目标公钥加密的随机数；远程证明信息获取单元，被配置为基于加密的随机数来从物理主机的硬件可信根获取经签名的远程证明信息，经签名的远程证明信息包括针对硬件可信根的签名证书；证明信息和公钥发送单元，被配置为向验证服务器发送经签名的远程证明信息和目标公钥；以及加密证书接收单元，被配置为从验证服务器接收针对目标公钥的加密证书。

[0050] 根据本申请的第八方面，提供了一种用于提供证书的装置。该装置包括：随机数生成单元，被置为响应于从物理主机接收到用于获取加密证书的请求，在验证服务器处生成随机数，请求包括针对虚拟机的虚拟可信根的目标公钥；加密单元，被配置为使用目标公钥对随机数进行加密；随机数发送单元，被配置为向物理主机发送经加密的随机数；远程证明信息接收单元，被配置为从物理主机接收目标公钥和经签名的远程证明信息，经签名的远程证明信息包括针对物理主机的硬件可信根的签名证书和对应的签名；以及证书发送单元，被配置为响应于经签名的远程证明信息通过验证，向物理主机发送加密证书，加密证书是针对目标公钥的。

[0051] 根据本申请的第九方面，提供了一种用于获取凭证的装置。该装置包括：请求发送单元，被配置为在物理主机处向验证服务器发送用于获取凭证的请求；随机数获取单元，被配置为从验证服务器获取随机数；远程证明信息获取单元，被配置为基于随机数和一组公钥，从物理主机的硬件可信根获取经签名的远程证明信息，经签名的远程证明信息包括针对硬件可信根的签名证书；以及回复信息发送单元，被配置为向验证服务器发送回复信息，回复信息包括经签名的远程证明信息、关于一组公钥的指示信息以及随机数；凭证获取单元，被配置为从验证服务器获取凭证，该凭证指示一组公钥的可信性。

[0052] 根据本申请的第十方面，提供了一种用于提供凭证的装置。该装置包括：回复信息接收单元，被配置为在验证服务器处从物理主机接收回复信息，回复信息包括经签名的远程证明信息、关于一组公钥的指示信息和随机数，经签名的远程证明信息包括针对物理主机的硬件可信根的签名证书；验证单元，被配置为对经签名的远程证明信息进行验证；凭证生成单元，被配置为响应于经签名的远程证明信息通过验证，基于远程证明信息和指示信息，生成凭证，凭证指示一组公钥的可信性；以及凭证发送单元，被配置为将凭证发送给物理主机。

[0053] 根据本申请的第十一方面，提供了一种用于验证信息的装置。该装置包括：随机数生成单元，被配置为响应于从物理主机接收到注册物理主机中的虚拟机的第一请求，在验证服务器处生成随机数；证明信息获取单元，被配置为向物理主机发送用于获取证明信息的第二请求，第二请求包括随机数；以及证明信息和凭证接收单元，被配置为从所述物理主

机接收针对虚拟机的经签名的远程证明信息和凭证，经签名的远程证明信息包括签名证书和对应的签名，签名证书是针对从一组公钥中选择的分配给虚拟机的公钥的证书，凭证指示一组公钥的可信性；可信状态确定单元，被配置为基于所述经签名的远程证明信息和所述凭证，确定所述虚拟机的可信状态。

[0054] 根据本申请的第十二方面，提供了一种用于验证信息的装置。该装置包括：证明信息获取单元，被配置为响应于从物理主机接收到注册物理主机中的虚拟机的第一请求，在第一验证服务器处向物理主机发送获取证明信息的第二请求，第二请求包括随机数；远程证明信息接收单元，被配置为接收针对虚拟机的经签名的远程证明信息，远程证明信息包括签名证书，签名证书是针对从一组公钥中选择的分配给虚拟机的公钥的证书；证书获取单元，被配置为响应于经签名的远程证明信息通过验证，获取签名证书；凭证获取单元，被配置为向第二验证服务器发送用于获取凭证的第三请求，第三请求包括签名证书；凭证获取单元，被配置为从第二验证服务器获取凭证；可信状态确定单元，被配置为基于凭证来确定虚拟机的可信状态，凭证指示一组公钥的可信性。

[0055] 根据本申请的第十三方面，还提供了一种电子设备，包括：至少一个计算单元；至少一个存储器，所述至少一个存储器被耦合到所述至少一个计算单元并且存储用于由所述至少一个计算单元执行的指令，所述指令当由所述至少一个计算单元执行时，使得所述设备执行根据本申请的第一方面至第六方面任一方面所述的方法。

[0056] 根据本申请的第十四方面，还提供了一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行时实现根据本申请的第一方面至第六方面任一方面所述的方法。

[0057] 根据本申请的第十五方面，还提供了一种计算机程序产品，包括计算机可执行指令，其中所述计算机可执行指令被处理器执行时实现根据本申请的第一方面至第六方面任一方面所述的方法。

[0058] 可以理解地，上述提供的第七方面到第十二方面的装置、第十三方面的电子设备、第十四方面的计算机存储介质、或第十五方面的计算机程序产品用于执行第一方面到第六方面所提供的方法。因此，关于第一方面至第六方面的解释或者说明同样适用于第七方面至第十五方面。此外，第七方面至第十五方面所能达到的有益效果可参考对应方法中的有益效果，此处不再赘述。了

附图说明

[0059] 结合附图并参考以下详细说明，本申请各实施例的上述和其他特征、优点及方面将变得更加明显。在附图中，相同或相似的附图标注表示相同或相似的元素，其中：

[0060] 图1示出了本申请的多个实施例能够在其中实现的示例环境的示意图；

[0061] 图2示出了根据本申请的一些实施例的用于获取证书的示意流程图；

[0062] 图3示出了根据本申请的一些实施例的用于提供证书的示意流程图；

[0063] 图4示出了根据本申请的一些实施例的用于获取证书和提供证书的过程的示意流程图；

[0064] 图5示出了根据本申请的一些实施例的系统架构的示意图；

[0065] 图6示出了根据本申请的一些实施例的用于获取凭证和验证信息的示意图；

[0066] 图7示出了根据本申请的一些实施例的凭证的示例；

[0067] 图8示出了根据本申请的一些实施例的用于获取凭证的示意流程图；

[0068] 图9示出了根据本申请的一些实施例的用于提供凭证的示意流程图；

[0069] 图10示出了根据本申请的一些实施例的用于验证信息的示意流程图；

[0070] 图11示出了根据本申请的一些实施例的用于验证信息的示意流程图；

[0071] 图12示出了根据本申请的一些实施例的用于获取护照的过程的示意流程图；

[0072] 图13示出了根据本申请的一些实施例的用于进行远程证明的示意流程图；

[0073] 图14示出了根据本申请的一些实施例的用于获取护照的过程的示意流程图；

[0074] 图15示出了根据本申请的一些实施例的用于进行远程证明的示意流程图；

[0075] 图16示出了根据本申请的一些实施例的用于进行远程证明的示意流程图；

[0076] 图17示出了根据本申请的一些实施例的用于进行远程证明的示意流程图；

[0077] 图18示出了根据本申请的一些实施例的用于获取证书的装置的框图；

[0078] 图19示出了根据本申请的一些实施例的用于提供证书的装置的框图；

[0079] 图20示出了根据本申请的一些实施例的用于获取凭证的装置的框图；

[0080] 图21示出了根据本申请的一些实施例的用于提供凭证的装置的框图；

[0081] 图22示出了根据本申请的一些实施例的用于验证信息的装置的框图；

[0082] 图23示出了根据本申请的一些实施例的用于验证信息的装置的框图；以及

[0083] 图24示出了能够实施本申请的多个实施例的计算设备的框图。

具体实施方式

[0084] 下面将参照附图更详细地描述本申请的实施例。虽然附图中显示了本申请的某些实施例，然而应当理解的是，本申请可以通过各种形式来实现，而且不应该被解释为限于这里阐述的实施例，相反提供这些实施例是为了更加透彻和完整地理解本申请。应当理解的是，本申请的附图及实施例仅用于示例性作用，并非用于限制本申请的保护范围。

[0085] 在本申请的实施例的描述中，术语“包括”及其类似用语应当理解为开放性包含，即“包括但不限于”。术语“基于”应当理解为“至少部分地基于”。术语“一个实施例”或“该实施例”应当理解为“至少一个实施例”。术语“第一”、“第二”等等可以指代不同的或相同的对象。下文还可能包括其他明确的和隐含的定义。

[0086] 如上所述，远程验证主要是为了保证计算机硬件平台的可信性。远程证明的证据主要由验证方的可信计算模块提供。目前主要包括可信平台模块(Trusted Platform Module，TPM)1.0和2.0，以及可信平台控制模块(Trusted Platform Control Module，TPCM)等。TPM可信平台模块的结构，主要包括输入输出，密钥，密钥管理，哈希算法，度量，可信报告根等模块。TPM的主要功能是为验证方提供了一个独立的度量模块，并可以把度量结果发送给外部的依赖方或者验证方。随着系统虚拟化和云化的进展，远程证明也被扩展到了虚拟机的度量。为了度量虚拟机，提出了虚拟化可信平台模块(virtualized Trusted Platform Module，vTPM)的概念。vTPM采用软件的方式，实现了TPM的大部分功能，包括可信度量根，可信报告根和可信存储根等，并提供类似TPM的接口，使得上层协议可以重用已有的针对TPM设计的大部分协议。vTPM由于是软件实现，难以独立提供可信的度量报告，需要依赖底层的硬件可信根提供支持，因此，在设计上需要保证信任链能够从底层的硬件可信

根延伸到上层的vTPM。

[0087] 为了解决上问题,存在两种传统的解决方案。一个传统方案是利用TPM的身份认证密钥(Attestation Identity Key,AIK)的可信性确定vTPM提供的远程证明的可信性。在该方案中vTPM的AIK是否可信,需要由TPM来保证。该方案把vTPM中的AIK密钥对与TPM的AIK的公私钥进行绑定。但是该方案主要从学术的角度出发,没有考虑如何与现有标准结合。因此,难以将该方案应用于实际中。另一个传统方案是在路由器之间传递基于远程证明证据的方法。在该方案中路由器之间使用加标签的护照进行远程验证,实现了路由器设备远程证明证据的评估结果的共享。但是该方案是基于硬件可信根设计的,不支持虚拟可信根。因此,也不支持虚拟可信根和深度证明。

[0088] 至少为了解决上述问题中的一些问题和其他潜在问题,在本申请的实施例中,在物理主机处生成针对虚拟机的虚拟可信根的密钥对,然后向验证服务器发送用于获取证书的请求以从验证服务器获取由目标公钥加密的随机数。接着物理主机基于加密的随机数来从物理主机的硬件可信根获取经签名的远程证明信息,经签名的远程证明信息包括针对硬件可信根的签名证书和对应的签名。最后物理主机向验证服务器发送经签名的远程证明信息和目标公钥以用于从验证服务器接收针对所述目标公钥的加密证书,加密证书是在经签名的远程证明信息通过验证后而被生成的。基于这样的方式,实现了虚拟可信根和硬件可信根的关联关系,解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题,改进了对应于硬件可信根设备的虚拟可信根的验证效率,提高了用户体验。

[0089] 图1示出了本申请的多个实施例能够在其中实现的示例环境100的示意图。如图1所示,环境100包括物理主机102。物理主机102划分为三层,第一层是硬件层,包括物理主机的各种硬件部件,如中央处理单元、存储器、硬件可信根(Root of Trust,RoT)108;第二层是系统层106,系统层106用于运行操作系统以及虚拟机管理软件,其包括虚拟机管理器106;第三层是软件层,软件层用于运行各种应用软件,包括虚拟机,容器或者虚拟网络功能模块等。硬件可信根108作为可信计算机系统中作为信任的基点。硬件可信根108包括授权的证书,其能够证明硬件可信根108是经过认证授权的,因此是可信的。虚拟机管理器106包括虚拟可信根(virtualized Root of Trust,vRoT)110。虚拟可信根110用于证明虚拟机104的可信性。

[0090] 图1中还示出了验证服务器114。为了便于描述,验证服务器114也可以称为第一验证服务器。验证服务器114对于从虚拟机管理器106接收的信息进行验证,主要负责管理物理主机,包括物理主机的远程验证评估、下发虚拟机启动和停止等功能。在一些实施例中,验证服务器114根据从硬件可信根108中获取的信息来对由虚拟管理器106提供的针对虚拟机的密钥对中的公钥进行验证,来生成加密证书或身份证书。在一些实施例中,验证服务器114根据由虚拟机管理器提供的硬件可信根108的信息和用于虚拟机的一组公钥来提供凭证。该凭证包括针对硬件可信根的签名证书以及与硬件可信根相对应的一组公钥。因此,验证服务器114用于基于硬件可信根的可信性来确定用于虚拟可信根的公钥的可信性。备选地或附加地,第一验证服务器可以是提供多个功能的多个服务器,例如云管。在一个示例中,验证服务器114可以是云平台提供方,其用于验证云平台中的物理主机的可信性。

[0091] 示例环境100还包括验证服务器112。为了描述方便,验证服务器112也可以称为第二验证服务器。验证服务器112主要负责管理虚拟化的网元,负责下发虚拟网元启动、迁移、

停止、远征验证等功能。验证服务器112用于与虚拟机104进行交互以向虚拟机授予签名证书，或者确定虚拟机104是否可信。在一些实施例中，验证服务器112可以根据从虚拟机104接收的针对虚拟机的加密证书或身份证书来为虚拟机提供签名证书。在一些实施例中，验证服务器112可以在进行虚拟机注册时，根据一定的信息获取策略来从虚拟机、虚拟机管理器106和/或第一验证服务器114获取信息以验证虚拟机104或虚拟网络功能模块是否可信。备选地或附加地，验证服务器可以是提供多个功能的多个服务器，例如网管。在一个示例中，第一验证服务器可以是使用云平台的服务方，其用于验证云平台中的提供的虚拟机。

[0092] 图1示出的物理主机104包括但不限于个人计算机、服务器、手持或膝上型设备、移动设备(诸如移动电话、个人数字助理(PDA)、媒体播放器等)、多处理器系统、消费电子产品、小型计算机、大型计算机、包括上述系统或设备中的任意一个的分布式计算环境等。图1示出的验证服务器114和验证服务器112包括但不限于服务器、多处理器系统、小型计算机、大型计算机、包括上述系统或设备中的任意一个的分布式计算环境等。虽然图1示出一个虚拟机和对应的虚拟可信根，但其仅是示例，而非对本公开的具体限定，在物理主机内可以运行多个虚拟机并且存在与该多个虚拟机对应的多个虚拟可信根。

[0093] 通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0094] 上面结合图1描述了本申请的实施例能够在其中被实现的示例环境100的示意图。下面结合图2描述根据本公开的实施例的用于获取证书的方法200的流程图。方法200可以在图1中的物理主机102及任意合适的计算设备处执行。

[0095] 在框202处，在物理主机处向验证服务器发送用于获取加密证书的请求。其中该请求包括目标公钥。在一些实施例中，虚拟机管理器106在启动虚拟机时会启动虚拟可信根。在启动虚拟可信根时，由虚拟可信根110生成用于虚拟可信根110的密钥对，该密钥对包括目标公钥和目标私钥。备选地或附加地，该目标公钥可以作为虚拟机的身份密钥或背书密钥。例如，为了获取针对该目标公钥的加密证书，物理主机102中的虚拟机管理器106向验证服务器114发送获取加密证书的请求，该请求包括该目标公钥。

[0096] 在框204处，从验证服务器接收由目标公钥加密的随机数。验证服务器114在接收到该请求后，会生成随机数，然后用该目标公钥加密。验证服务器114将加密后的随机数发送到物理主机102。

[0097] 在框206处，基于加密的随机数来从物理主机的硬件可信根获取经签名的远程证明信息。其中经签名的远程证明信息包括针对硬件可信根的签名证书。备选地，经签名的远程证明信息还包括由签名证书进行的签名。例如，物理主机102中根据接收到的随机数能够从硬件可信根108获取经签名的远程证明信息。

[0098] 在一些实施例中，物理主机102接收该加密的随机数，然后使用与所述目标公钥相对应的目标私钥来对加密的随机数进行解密以获取该随机数。如果其他的设备接收到该加密的随机数，由于其不具有与该目标公钥对应的目标私钥，因此不会解密得到该随机数。物理主机102基于解密的随机数来获取到针对硬件可信根的本地证明信息。该本地证明信息包括针对硬件可信根的签名证书，该签名证书表明硬件可信根是可信的。备选地或附加地，本地证明信息还包括由硬件可信根收集的各种信息，如关于基本输入输出系统(Basic Input Output System,BIOS)的信息和关于操作系统的信息等。然后物理主机根据解密的

随机数和本地证明信息生成远程证明信息。例如由随机数和本地证明信息形成信息列表。然后，物理主机102使用与硬件可信根的签名证书相对应的签名私钥对远程证明信息进行签名。

[0099] 在框208处，向验证服务器发送经签名的远程证明信息和目标公钥。例如物理主机102将经签名的远程证明信息和目标公钥发送到验证服务器114。在框210处，从验证服务器接收针对目标公钥的加密证书。验证服务器114验证远程证明信息。在验证通过后将目标公钥的加密证书发送给物理主机。加密证书是在经签名的远程证明信息通过验证后而被生成的。

[0100] 在一些实施例中，物理主机102在从验证服务器114获取到加密证书后，还会向验证服务器112发送加密证书以从第二验证服务器获取签名证书。

[0101] 通过上述方式，利用硬件可信根的签名证书来生成远程证明信息，然后向验证服务器发送经签名的远程证明信息和目标公钥。通过远程证明信息中包含的硬件可信根的签名证书可以证明发送该远程证明信息的设备是可信的，进而可以确定来自该设备的针对虚拟机的虚拟可信根的目标公钥也是可信的。因此，这种方式实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0102] 上面结合图2描述了本申请的实施例用于获取证书的方法的流程图。下面结合图3描述根据本公开的实施例的用于提供证书的方法300的示意流程图。方法300可以在图1中的验证服务器114及任意合适的计算设备处执行。

[0103] 在框302处，确定是否从物理主机接收到用于获取加密证书的请求。例如，验证服务器114确定是否从物理主机102接收到用于获取加密证书的请求。其中该请求可以包括针对虚拟机的虚拟可信根的目标公钥。例如，该目标公钥来自在物理主机处启动虚拟机或启动虚拟可信根时生成的针对虚拟可信根的密钥对。

[0104] 如果从物理主机接收到用于获取加密证书的请求，在框304处，在验证服务器处生成随机数。例如验证服务器114在接收到用于获取加密证书的请求后生成随机数。在框306处，使用目标公钥对随机数进行加密。例如验证服务器114使用该目标公钥对随机数进行加密。在框308处，向物理主机发送经加密的随机数。在框310处，从物理主机接收目标公钥和经签名的远程证明信息。经签名的远程证明信息包括针对物理主机的硬件可信根的签名证书。例如，验证服务器114向物理主机102发送经加密的随机数，然后物理主机102利用该经加密的随机数来生成经签名的远程证明信息，生成远程证明信息的过程可以参见图2的描述。物理主机102再将该经签名的远程证明信息发送给验证服务器114。

[0105] 在框312处，确定经签名的远程证明信息是否通过验证。例如，验证服务器114要对经签名的远程证明信息进行验证。在验证经签名的远程证明信息时，验证服务器需要利用签名证书中的验证公钥验证签名，并且确定经签名的远程证明信息是否包括随机数。在一些实施例中，验证服务器114先利用签名证书中的验证公钥验证签名。如果签名未通过验证公钥的验证，则不再进行后面的操作。如果签名通过了验证公钥的验证，再确定经签名的远程证明信息是否包括随机数。如果不包括随机数，则结束该验证过程。如果经签名的远程证明信息包括随机数，则验证通过。在一些实施例中，验证服务器114先确定经签名的远程证明信息是否包括随机数。如果不包括该随机数，则结束该验证过程。如果包括该随机数，然

后再利用签名证书中的验证公钥验证签名。如果签名不能被验证公钥验证，则结束该验证过程。如果签名被验证公钥验证，则验证通过。上述示例仅是用于描述本公开，而非对本公开的具体限定。

[0106] 如果经签名的远程证明信息通过验证，在框314处，向物理主机发送加密证书，加密证书是针对目标公钥的。附加地，该加密证书包括该目标公钥。例如，验证服务器114在验证了远程证明信息后，验证服务器114利用该目标公钥生成签名证书。然后，向物理主机102发送加密证书。

[0107] 通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0108] 上面结合图2和图3描述了本申请的实施例用于获取证书和提供证书的方法的流程图。下面结合图4描述根据本公开的实施例的用于获取证书和提供证书的流程400的示意图。该流程400可在图1所示的环境中运行。

[0109] 在图4描述的示例中，验证服务器114表示为云管410，验证服务器112表示为网管412。如图4，流程400中包括硬件可信根402、虚拟机管理器404、虚拟可信根406、虚拟机和虚拟网络功能模块408、云管410和网管412。在414处，虚拟机管理器启动虚拟可信根。然后在框416处，虚拟可信根生成密钥对(vEk，vSk)，其中vEk为目标公钥，vSk为目标私钥。接着，虚拟机管理器从虚拟可信根获取418vEk。然后虚拟管理器向云管发送420虚拟可信根证书申请，其携带vEk。接着，云管在框422处生成随机数nonce1。云管使用vEk加密nonce1，并向虚拟机管理器发送424虚拟可信根证书申请挑战，其包括加密后的nonce1。然后虚拟机管理器传递426虚拟可信根证书申请挑战到虚拟可信根。在框428处，虚拟可信根vRoT解密获取nonce1。例如，虚拟可信根vRoT利用目标私钥vSk解密加密后的nonce1。然后，虚拟机管理器从虚拟可信根vRoT获取430解密后的nonce1。然后虚拟机管理器调用虚拟可信根RoT的远程证明接口，并将nonce1作为参数发送432给硬件可信根RoT。硬件可信根RoT向虚拟机管理器返回434经签名的远程证明证据。在该过程中，硬件可信根RoT获取针对硬件可信根的本地信息，例如针对硬件可信根的签名证书、关于物理主机的操作系统和硬件的信息。硬件可信根利用随机数和本地信息形成信息列表，然后使用对应于硬件可信根的签名证书的私钥对信息进行签名。虚拟机管理器向云管发送436回复，包含vEk和经签名的远程证明信息。在框438处，云管验证经签名的远程证明信息。经签名的远程证明信息包括针对硬件可信根的签名证书。因此，验证过程包括通过签名证书的公钥来验证经签名的远程证明信息中的签名和确认虚拟可信根RoT在远程证明证据报告生成的过程中使用了nonce1。这两步验证的先后顺序可以依据需要设置。备选地或附附加，远程证明信息还包括由硬件可信根获取的信息，包括操作系统信息和硬件相关的信息等。在框440处，云管生成加密证书，证书中的公钥是在436处接受到的vEk。然后云管服务器向虚拟机管理器发送442针对vEk的加密证书。虚拟机管理器将接受到的vEk证书发送444给虚拟可信根vRoT。在框446处，虚拟可信根vRoT存储获取的加密证书。接下来，在操作448处，虚拟机使用上述证书从网管获取虚拟机或虚拟网络功能模块的远程证明签名证书vAIK。

[0110] 通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0111] 上面结合图4描述了根据本公开的实施例的用于获取证书和提供证书的流程的示

意图。下面结合图5描述根据本公开的实施例的系统架构的示意图。如图5所示，系统架构500是图1的示例环境的一个具体示例。物理主机102负责运行和管理虚拟机，虚拟网络功能运行在一个或者多个虚拟机上。虚拟机管理器106还包括密钥与凭证管理模块504。密钥与凭证管理模块504在物理主机上的虚拟机管理器106内部，负责生成密钥对，向验证服务器114上的凭证管理模块506发送远程证明，并接收验证服务器114上的凭证管理模块506生成的凭证。虚拟机104包括策略处理模块102，其运行在虚拟机或者物理主机内部，负责处理远程证明中的策略并指示相关的远程证明模块提供相应的远程证明内容。

[0112] 验证服务器114包括凭证管理模块506、验证器510和证书授权模块508。验证器用于对接收的信息进行验证。证书授权模块508用于管理证书的发放。凭证管理模块506用于管理凭证的生成和发送等。为了描述方便我，验证服务器114也可以称为第一验证服务器。凭证管理模块506负责接收物理主机上发送的密钥对列表及其远程证明，并对上述数据处理，生成验证结果，并加入远程证明的原始数据与密钥链接证据，并且对其进行签名，形成凭证，发送给物理主机。验证服务器112包括验证器512和证书授权模块514。验证器512用于对接收的信息进行验证。证书授权模块514用于管理证书的发放。

[0113] 下面结合图6描述根据本申请的一些实施例的用于获取凭证和验证信息的示意图。如图6所求，首先第一验证服务器114在收到物理主机上102的虚拟机管理器发送过来的要获取凭证的请求后，第一验证服务器114的凭证管理模块506向物理主机102上的密钥与凭证管理模块504发送随机数nonce。密钥与凭证管理模块504在接收到随机数nonce后，把先前生成的N对密钥对与随机数nonce一起输入到哈希函数，获取一个哈希值h，然后调用硬件可信根RoT108(例如TPM)接口，并把h作为参数传递给硬件可信根108。硬件可信根108将自身存储的远程证明信息打包签名并发回给密钥与凭证管理模块504。接着密钥与凭证管理模块504将上述证明信息与公钥列表发送给凭证管理模块506。第一验证服务器114的凭证管理模块506对接收到的远程证明信息进行处理，并生成一个凭证，内容包括对物理平台的评估结果、时间戳、原始的远程证明信息、第一验证服务器的证书与签名以及公钥列表的指示信息。例如，公钥列表的指示信息可以为公钥列表本身或者由公钥列表输入累加器生成的根值。然后，将该凭证发送给物理主机102上的密钥与凭证管理模块504。当物理主机102启动一个虚拟机时，虚拟机管理器106从与公钥列表对应的一组密钥对中选定一对密钥(PKi,SKi)，并将上述密钥以及凭证发送给虚拟可信根vRoT 110。当虚拟可信根110收到外部的远程证明请求时，虚拟可信根110可以提供虚拟机104的经签名的远程证明信息。备选地或附加地，该请求中还包括提供信息的策略。在一个示例中，在策略指示提供针对虚拟机的远程证明信息和上述凭证时，由虚拟机104将虚拟可信根提供的远程证明信息和上述凭证一起发送给第二验证服务器112。在另一个示例中，在策略指示仅提供针对虚拟机的远程证明信息时，虚拟机104仅将上述虚拟可信根提供的远程证明信息提供给第二验证服务器112，然后第二验证服务器112通过虚拟机管理器来获取凭证。上述示例仅是用于描述本公开，而非对本公开的具体限定。

[0114] 对于前面描述的凭证，其可以为远程证明护照。图7示出了两凭证的两个示例。一个示例是基于公钥列表的远程证明护照702和基于累加器的远程证明护照。其中基于公钥列表的远程证明护照702包括：护照类型；时间戳：远程证明护照生成时间；有效期：护照可使用的最后期限、超过该期限视为无效；评估结果：服务器对物理主机提供的远程证明材料

进行评估并给出结果;物理主机远程证明材料:物理主机提供的原始远程证明材料:包括物理主机的签名证书(AIK)、平台配置寄存器(Platform Configuration Register,PCR)值以及AIK证书签名,其中PCR值是TPM硬件中的存储软硬件可信记录的寄存器的值;密钥链接证据:主要功能是把vRoT(vTPM)的签名密钥与物理RoT的签名密钥关联起来,从而实现信任传递的连续性,该链接证据包括:公钥算法类型、公钥列表、生成护照时服务器提供的随机数nonce、虚拟机管理器VMM的远程证明服务IP地址和远程验证客户端(Remote Attestation Client,RAC)端口号等;服务器证书;服务器签名等。基于累加器的远程证明护照704与基于公钥列表的远程证明护照702相似,但是其不存储公钥列表,而是使用了累加器输出的根值root_value作为验证某个公钥是否属于该根值指定的护照。

[0115] 上面结合图5-7描述了根据本公开的实施例的证书和用于获取证书和验证证书的架构和的流程的示意图。下面结合图8-图11描述上述架构中物理主机102、验证服务器114和验证服务器之间进行交互的过程。上述交互过程由图5中的物理主机102、验证服务器114和验证服务器112或任意合适的计算设备执行。

[0116] 如图8所示,其示出了根据本申请的一些实施例的在物理主机处102用于获取凭证的示例。在框802处,在物理主机处向验证服务器发送用于获取凭证的请求。例如,物理主机102会先向验证服务器114发送用于获取凭证的请求,在框804处,从验证服务器获取随机数。验证服务器114在收到请求后生成随机数,然后发送给物理主机102。在一些实施例中,物理主机中的虚拟机管理器还生成一组密钥对,然后由一组密钥对中的公钥形成一组公钥。

[0117] 在框806处,基于随机数和一组公钥,从物理主机的硬件可信根获取经签名的远程证明信息。物理主机的虚拟机管理器根据随机数和一组公钥来生成目标哈希值。在一些实施例中,物理主机102根据随机数和一组公钥,生成字符串。然后物理主机根据字符串来生成目标哈希值。在一个示例中,物理主机在生成字符串时,通过对随机数、一组公钥、物理主机制中的虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号进行链接来形成字符串。在另一个示列中,在生成字符串时,物理主机将一组公钥输入累加器来获得根值。然后采用根值和随机数,生成字符串。附加地,计算设备通过对随机数、根值、虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号进行链接来形成字符串。上述示例仅是用于描述本公开,而非对本公开的具体限定。经签名的远程证明信息包括针对硬件可信根的签名证书。备选地,经签名的远程证明信息还包括由签名证书进行的签名和目标哈希值。物理主机102将目标哈希值传递给硬件可信根,硬件可信根获取针对硬件可信根的本地证明信息,该本地证明信息包括签名证书,备选地附加地,本地证明信息还包括由物理主机收集的信息,例如关于硬件的信息、操作系统的信息等;然后基于目标哈希值和本地证明信息来生成远程证明信息。例如由目标哈希值和本地证明信息形成信息列表。然后使用与签名证书相对应的签名私钥对远程证明信息进行签名。

[0118] 在框808处,向验证服务器发送回复信息。其中回复信息包括经签名的远程证明信息、关于一组公钥的指示信息以及随机数。例如物理主机102向验证服务器114发送回复信息,其包括经签名的远程证明信息、关于一组公钥的指示信息和随机数。备选地或附加地,回复信息还包括物理主机中的虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号。在框810处,从验证服务器获取凭证。该凭证指示一组公钥的可信性,例如

指示一组公钥由于硬件可信根可信而被认定为是可信的。验证服务器114在接收到回复信息后，对收到的信息进行验证。在验证通过后生成凭证，发送给物理主机102。在一些实施例中，其中指示信息包括根值，该根值是将一组公钥输入累加器得到的。在一些实施例中，其中指示信息包括一组公钥。

[0119] 附加地，物理主机102还可以基于获取的凭证向验证服务器112注册虚拟机。在一些实施例中，物理主机102在启动虚拟机和对应的虚拟可信根时，会从获取凭证时生成的一组密钥对中选择分配给虚拟可信根的一个密钥对，该密钥对包括公钥和私钥。然后物理主机102获取针对公钥的签名证书。物理主机102可以基于现有的技术来获取针对该公钥的签名证书。然后，物理主机102向验证服务器112发送注册虚拟机的请求，其中包括虚拟机的标识。验证服务器112在接收到注册虚拟机的请求时，生成随机数，然后发送给物理主机102。物理主机102从验证服务器112接收用于获取证明信息的请求，该请求包括由第二验证服务器生成的随机数。然后物理主机基于该随机数获取经签名的远程证明信息，为了描述方便，也可以称为第二远程证明信息。然后物理主机102向验证服务器112发送针对虚拟机的经签名的第二远程证明信息以用于确定虚拟机的可信状态，经签名的第二远程证明信息包括签名证书和对应的第二签名。

[0120] 在一些实施例中，物理主机在接收到随机数后，会利用随机数从虚拟机获取关于虚拟机的本地信息，例如针对虚拟机的签名证书，以及关于虚拟机的其他信息，例如虚拟机使用的软件系统等。然后，用对应于虚拟机的签名证书的私钥对随机数和针对虚拟机的本地进行签名以生成经签名的第二远程证明信息。然后物理主机102将经签名的第二远程证明信息发送给验证服务器112来确定虚拟机的可信状态。

[0121] 备选地或附加地，从验证服务器112接收用于获取证明信息的请求还包括获取证明信息的策略。物理主机102根据该策略向验证服务器112发送信息。该策略包括仅获取针对虚拟机的证明信息或者获取针对虚拟机的证明信息和上述凭证。在一些实施例中，在策略指示仅获取针对虚拟机的证明信息时，物理主机102根据随机数从虚拟可信根获取经签名的第二远程证明信息，其中经签名的第二远程证明信息还包括物理主机中的虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号。然后物理主机102向验证服务器112发送经签名的第二远程证明信息。验证服务器112在接收到第二远程证明信息后，会对远程证明信息进行验证。在远程证明信息通过验证后，验证服务器112会向物理主机112的虚拟机管理器发送用于获取凭证的请求，该请求包括互联网协议地址、端口号和签名证书。物理主机102在接收到用于获取凭证的请求后，物理主机102根据签名证书中的公钥来获取凭证。例如，物理主机的虚拟机管理器会根据签名证书中的公钥在虚拟机管理器中的多个凭证中查找具有该公钥或支持该公钥的凭证。然后物理主机向验证服务器112发送凭证，以用于确定虚拟机的可信状态。验证服务器112在接收到凭证后，会利用获取的凭证来确定虚拟机的可信状态。例如通过凭证中的服务器证书中的公钥来验证凭证的服务器签名，诸如利用由验证服务器114生成的服务器证书的公钥来进行验证。然后验证服务器112还会验证虚拟机的签名证书中的公钥是否由凭证支持，例如公钥是否包含在凭证中，或者是否由验证服务器的根值支持等。

[0122] 在一些实施例中，策略指示获取针对虚拟机的证明信息和凭证。如果策略指示获取针对虚拟机的证明信息和凭证，物理主机102从虚拟可信根获取经签名的第二远程证明

信息。物理主机102还会根据针对虚拟机的公钥来从虚拟机管理器获取凭证。然后物理主机102向验证服务器112发送经签名的第二远程证明信息和凭证以用于确定虚拟机的可信状态。

[0123] 通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0124] 上面结合图8描述了在物理主机处102用于获取凭证的示例。下面结合图9描述提供凭证的过程，图9示出了根据本申请的一些实施例的用于提供凭证的示意流程图。上述过程由图5中的验证服务器114或任意合适的计算设备执行。

[0125] 如图9所示，验证服务器114在从物理主机接收到用于获取凭证的请求时，生成随机数。然后验证服务器114向物理主机发送随机数。如图8所描述的，物理主机根据该随机数会生成回复信息发送给验证服务器114。

[0126] 在框902处，在验证服务器处从物理主机接收回复信息。回复信息包括经签名的远程证明信息、关于一组公钥的指示信息和随机数，经签名的远程证明信息包括针对物理主机的硬件可信根的签名证书。附加地，经签名的远程证明信息还包括由签名证书进行的签名和目标哈希值，目标哈希值基于随机数和一组公钥而被生成的，一组公钥来自物理主机中生成的一组密钥对。

[0127] 在框904处，对经签名的远程证明信息进行验证。例如，验证服务器114在接收到回复信息后，要对经签名的远程证明信息进行验证。在一些实施例中，在对经签名的远程证明信息进行验证时，验证服务器114通过签名证书中的公钥验证经签名的远程证明信息中的签名。如果该签名未通过验证，则结束获取凭证的操作。如果签名通过验证，验证服务器根据回复中的随机数和指示信息，生成验证哈希值。然后将目标哈希值和验证哈希值进行比较，来验证经签名的远程证明信息。在一些实施例中，指示信息包括一组公钥，在生成验证哈希值时，验证服务器114根据随机数和一组公钥，生成字符串。然后对字符串进行哈希操作来生成验证哈希值。备选地或附加地，回复信息还包括物理主机中的虚拟机管理器的互联网协议地址、虚拟机管理器的远程验证服务的端口号；验证服务器114通过对随机数、一组公钥、互联网协议地址和端口号进行链接来形成字符串。在一些实施例中，指示信息包括根值，根值是通过将一组公钥输入累加器而获得的，在生成验证哈希值时，验证服务器114基于随机数和根值，生成字符串。然后验证服务器114基于字符串来生成验证哈希值。附加地，其中回复信息还包括物理主机中的虚拟机管理器的互联网协议地址、虚拟机管理器的远程验证服务的端口号；验证服务器114通过对随机数、根值、互联网协议地址和端口号进行链接来形成字符串。

[0128] 在框906处，确定经签名的远程证明信息是否通过验证。通过上面描述的验证操作可以确定经签名的远程证明信息是否通过验证。在经签名的远程证明信息通过验证时，在框908处，基于远程证明信息和指示信息，生成凭证，凭证指示一组公钥的可信性，例如指示一组公钥由于硬件可信根可信而被认定为是可信的。备选地或附加地凭证还包括互联网协议地址和端口号。在一些实施例中，验证服务器114在生成凭证时，还会通过对远程证明信息进行评估来生成评估结果；将评估结果加入凭证。例如，对物理主机的性能和操作系统进行评估，生成相应的评估结果加入凭证中。在一些实施例中，验证服务器114在生成凭证时，会对远程证明信息进行评估来生成评估结果。然后确定评估结果是否满足预定要求，例如

评估的硬件是否满足要求。如果评估结果不满足预定要求，则结束操作。如果评估结果满足预定要求，生成凭证，凭证包括将评估结果。在框910处，验证服务器114将凭证发送给物理主机。

[0129] 通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0130] 上面结合图9描述了在验证服务器114用于提供凭证的流程的示例。下面结合图10描述用于验证信息的过程，图10示出了根据本申请的一些实施例的用于验证信息的示意流程图。上述过程由图5中的验证服务器112或任意合适的计算设备执行。

[0131] 在框1002处，确定是否从物理主机接收到注册物理主机中的虚拟机的第一请求。例如，验证服务器112确定是否从物理主机102接收到注册物理主机中的虚拟机的请求。如果从物理主机接收到注册物理主机中的虚拟机的第一请求，在框1004处，在验证服务器处生成随机数。在框1006处，验证服务器向物理主机发送用于获取证明信息的第二请求，第二请求包括随机数。附加地，第二请求还包括策略。例如验证服务器确定物理主机获取证明信息的策略。诸如是只从虚拟机获取针对虚拟机的远程信息，还是从虚拟机获取针对虚拟机的远程信息和上述凭证。如在图8的描述中，物理主机在接收到用于获取证明信息的第二请求后，会基于策略来向验证服务器1112提供针对虚拟机的经签名的远程证明信息和凭证。

[0132] 在框1008处从物理主机接收针对虚拟机的经签名的远程证明信息和凭证。其中经签名的远程证明信息包括签名证书和对应的签名，签名证书是针对从一组公钥中选择的分配给虚拟机的公钥的证书。凭证指示一组公钥的可信性，例如指示一组公钥由于物理主机的硬件可信根可信而被认定为是可信的，其中一组公钥来自由物理主机的虚拟机管理器生成的一组密钥对。在框1010处，基于经签名的远程证明信息和凭证，确定虚拟机的可信状态。

[0133] 在一些实施例，其中经签名的远程证明信息还包括物理主机中的虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号。如果策略指示仅获取针对虚拟机的证明信息，验证服务器1112先接收经签名的远程证明信息。然后，验证服务器对经签名的远程证明信息进行验证。例如利用经签名的远程证明信息中包括的针对虚拟机的签名证书中的公钥来验证签名。如果经签名的远程证明信息未通过验证，则结束操作。如果经签名的远程证明信息通过验证，验证服务器从经签名的远程证明信息获取签名证书、互联网协议地址和端口号。然后验证服务器112向物理主机的虚拟机管理器发送获取凭证的第三请求，第三请求包括互联网协议地址、所端口号和签名证书。物理主机在接收到发送获取凭证的请求后，如针对图8所描述的，物理主机102基于互联网协议地址、端口号和签名证书来获取凭证。然后，物理主机102向验证服务器112发送凭证，以便验证服务器112从物理主机102接收该凭证。在接收到经签名的远程证明信息和凭证后，验证服务器112对凭证进行验证。例如通过凭证中的签名证书中的公钥来验证凭证的服务器签名，诸如利用由验证服务器114生成的服务器证书的公钥来进行验证。如果凭证未通过验证，则结束操作。如果凭证通过验证，确定签名证书中的公钥是否被凭证支持。例如公钥是否包含在凭证中，或者是否由验证服务器的根值支持等。如果公钥未被凭证支持，则结束操作。如果公钥被凭证支持，确定虚拟机是可信的。

[0134] 在一些实施例中，其中策略指示获取针对虚拟机的证明信息和凭证。此时，验证服

务器112先接收经签名的远程证明信息和凭证。然后验证服务器需要对经签名的远程证明信息和凭证进行验证以确定经签名的远程证明信息和凭证是否通过验证。如果经签名的远程证明信息和凭证未通过验证，则结束操作。如果经签名的远程证明信息和凭证通过验证，则经签名的远程证明信息获取签名证书。验证服务器112此时需要确定签名证书中的公钥是否被凭证支持。如果该公钥不被支持，则结束确认过程。如果公钥被凭证支持，确定虚拟机是可信的。在一个示例中，在确定公钥是否被凭证支持时，验证服务器确定公钥是否存在于凭证中。在另一个示例中，凭证包括根值，根值是通过将一组公钥输入累加器而获得的，在确定公钥是否被凭证支持时，验证服务器112提取凭证中的根值。然后验证服务器112根据根值和公钥，确定公钥是否被凭证支持，例如如果根值能被公钥整除，则表明该公钥被根值支持；如果根值不能被公钥整除，则表明该公钥不被根值支持。

[0135] 通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0136] 上面结合图10描述了根据本申请的一些实施例的在验证服务器112处用于验证信息的示意流程图。下面结合图11描述用于验证信息的另一个过程，图11示出了根据本申请的一些实施例的用于验证信息的示意流程图。上述过程由图5中的验证服务器112或任意合适的计算设备执行。

[0137] 在框1102处确定是否从物理主机接收到注册物理主机中的虚拟机的第一请求。如果从物理主机接收到注册物理主机中的虚拟机的第一请求，在框1104处，在第一验证服务器处向物理主机发送获取证明信息的第二请求。其中第二请求包括随机数。例如，验证服务器112向物理主机102发送获取证明信息的第二请求。然后在框1106处，接收针对虚拟机的经签名的远程证明信息。远程证明信息包括签名证书，签名证书是针对从一组公钥中选择的分配给虚拟机的公钥的证书。如图8所述的物理主机在接收到该请求后会生成经签名的远程证明信息发给验证服务器112。在框1108处，确定经签名的远程证明信息是否通过验证。对经签名的远程证明信息进行验证的过程可以参见前面的描述。如果未通过验证，则结束操作。如果经签名的远程证明信息通过验证，在框1110处，获取签名证书。

[0138] 在框1112处，向第二验证服务器发送用于获取凭证的第三请求，第三请求包括签名证书。验证服务器112利用签名证书生成用于获取凭证的请求，然后发送给验证服务器114。在框1114处，从第二验证服务器获取凭证。验证服务器114在接收到请求后，会利用请求中的签名证书来获取凭证。在验证服务器114中，由于其存储了多个凭证。因此，可以利用签名证书中的公钥来查找支持该公钥的凭证。在一个示例中，凭证包括该公钥。在另一个示例中，凭证中的根值由该公钥生成。上述示例仅是用于描述本公开，而非对本公开的具体限定。

[0139] 在框1116处，基于凭证来确定虚拟机的可信状态。凭证指示一组公钥的可信性，例如凭证指示一组公钥由于物理主机的硬件可信根可信而被认定为是可信的。附加地，该组公钥来自一组密钥对。在一些实施例中，在确定可信状态时，验证服务器112在接收到凭证时，会对凭证进行验证。如果凭证未通过验证，则结束操作。如果凭证通过验证，确定签名证书的公钥是否被凭证支持。如果公钥不被凭证支持，则结束操作。如果公钥被凭证支持，确定虚拟机是可信的。在一个示例中，在确定签名证书的公钥是否被凭证支持时，验证服务器112确定公钥是否存在于凭证中。在另一个示例中，凭证包括根值，根值是通过将一组公钥

输入累加器而获得的，在确定签名证书的公钥是否被凭证支持时，验证服务器112提取凭证中的根值。然后验证服务器根据根值和公钥，确定公钥是否被凭证支持。

[0140] 通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0141] 上面结合图8-图11描述系统架构中物理主机102和验证服务器114和验证服务器112之间进行交互的过程。下面结合图12-17描述了根据本公开的实施例的用于获取凭证和验证信息的四个示例。图12-图13描述了用于获取凭证和验证信息的第一个示例；图14-图15描述了用于获取凭证和验证信息的第二个示例。图16描述了用于获取凭证和验证信息的第三个示例；图17描述了用于获取凭证和验证信息的第四个示例。上述示例过程由图5中的物理主机102、验证服务器114和验证服务器112或任意合适的计算设备执行。

[0142] 图12和13提供了基于凭证获取虚可信根远程证明护照的第一个示例过程。凭证的主要功能是提供虚可信根的签名证书AIK中的密钥对与平台的硬件可信根RoT的绑定。该示例过程分为两部分，第一部分为虚拟机管理器从云管获取凭证。第二部分为虚拟机在远程证明过程种使用前面获取的凭证证明硬件平台可信及其与虚可信根提供的签名证书vAIK的关联性。

[0143] 如图12所示，存在硬件可信根1202、虚拟机管理器1204和云管1206。在第一部分流程中，在框1208处，虚拟机管理器生成N对密钥对{PK_i,SK_i}，i＝1,2,…,N,其中N为正整数。然后，虚拟机管理器向云管发送1210远程证明护照获取请求。云管服务器的远程证明管理模块接收到该请求后，生成一个随机数nonce1，并向虚拟机管理器发送1212该随机数。虚拟机管理器接收到noce1后，在框1214处，将noce1、公钥PK_i,i＝1,2,…,N、以及虚拟机管理器的IP地址和端口号等信息进行链接，形成字符串s,s＝nonce1||PK1||PK2||…||IP||端口号。在框1216处，虚拟机管理器将上述字符串s输入到一个哈希函数中，获取一个哈希值，h1＝hash(s)，其中hash()表示哈希函数。虚拟机管理器将h1通过物理接口(如系统调用接口)发送1218给硬件可信根RoT(例如TPM)，要求获取硬件可信根中保存的远程证明信息。在框1220处，硬件可信根把h1作为输入，生成当前的远程证明材料RA1，并使用硬件可信根中保存的可信报告根(Root for Trust Report,RTR)对远程证明材料RA1进行签名。例如，按照现有规范，RA1包含RTR证书，例如TPM规范中的签名证书AIK或者其他的签名证书，例如访问密钥(Access Key,AK)证书。硬件可信根把签名后的远程证明信息发回给虚拟机管理器。虚拟机管理器将上述经签名的远程证明材信息RA1、nonce1、公钥列表(PK_1,PK_2,…,PK_N)、虚拟机管理器IP地址、虚拟机管理器远程证明服务端口号发送1224给云管1206。在框1226处，云管1206验证经签名的远程证明RA1，并使用1214和1216中的方法生成h1’，并将h1’与RA1中包含的h1进行对比，如果一致，则验证通过。在框1228处，云管服务器对RA1中的远程证明材料进行评估，并形成评估结果。云管服务器将远程证明材料、评估结果、nonce1、公钥列表、虚拟机管理器IP地址、端口号、服务器证书等信息按照远程证明护照格式进行组合并签名。云管服务器将形成的远程证明护照发送1230给虚拟机管理器。在框1232处，虚拟机管理器存储在1230中接收到的远程证明护照。

[0144] 图13显示了本示例的第二部分，包括虚拟机管理器1302、虚拟可信根1304、虚拟机1306、云管1308和网管1310。网管、虚拟机、物理主机使用远程证明护照完成虚拟机及承载该虚拟机的物理主机的远程证明。在框1312处，物理主机完成可信启动，虚拟机管理器进入

工作状态，在框1314处，虚拟机管理器向云管服务器申请并获取远程证明护照，获取远程证明护照的过程的具体方法参见图12的描述。当虚拟机管理器启动虚拟机与虚拟可信根时，虚拟机管理器1302选取先前生成凭证或护照时的一组密钥对中一对PK_i,SK_i,，然后传送1316给虚拟可信根。在框1318处，虚拟机为虚拟可信根申请远程证明证书vAIK_i。然后虚拟机向网管服务器发送1320虚拟机注册请求。网管服务器向虚拟机发送1322远程证明请求，并提供随机数nonce2，并指定策略为VM_Only，即仅提供针对虚拟机的信息。在1324处，虚拟机接收到上述远程证明求后，将nonce2发送给虚拟可信根。虚拟可信根生成针对虚拟机的经签名的远程证明信息，并发回给虚拟机。经签名的远程证明信息中包含了vAIK_i证书及由其进行的签名。虚拟机向网管发送1326经签名的远程证明信息，其中包含了虚拟可信根提供的虚拟机证明信息、vAIK_i证书、虚拟机管理器远程证明服务的IP地址和端口号。在框1328处，网管验证虚拟机提供的经签名的远程证明信息。在框1330处，网管从消息中提取vAIK_i证书、虚拟机管理器远程证明服务的IP地址和端口号。然后根据在框1130处获取的IP地址和端口号，网管向虚拟机管理器发送1332用于获取护照的远程证明请求和公钥vAIK_i。在框1334处，虚拟机管理器在接收到请求时，使用vAIK_i中的PK_i获取相应的远程证明护照。虚拟机管理器将该远程证明护照发送1336给网管。在框1338处，网管验证远程证明护照。在框1340处，验证通过后，网管从远程证明护照中提取链接证据，并验证该PK_i是否是该护照所背书的公钥之一。如果不是，则结束操作。如果是，则整个远程证明流程结束。

[0145] 本示例通过定义远程证明护照，为虚拟可信根与硬件可信根建立了安全的关联关系，实现了信任链的扩展，同时本实施例针对远程证明护照的特征，对现有的远程验证协议进行了扩展，从而为虚拟机远程验证提供了完整的解决方案。

[0146] 图14和15提供了基于凭证获取虚可信根vRoT远程证明护照的第二个示例过程。如图14所示，其包括硬件可信根1402、虚拟机管理器1404和云管1406。该过程中的操作1408、1410和1412与图12中对应操作相同。接下来，在框1414处，虚拟机管理器将PK_i,i＝1,2,…,N输入到一个累加器里面，获取根值。然后在框1416处，虚拟机管理器将根值、nonce1、以及其它相关的信息，如虚拟机管理器的IP地址，远程验证服务的端口号等链接成一个字符串，并输入到一个哈希函数h里面，获得哈希值h1。接来下的操作1418、1420和1422与示例一相同。虚拟机管理器将经签名的远程证明信息、nonce1、根值以及其它相关信息，虚拟机管理器的IP地址、远程验证服务的端口号等，发送1424给云管服务器。在框1426处，云管服务器上的远程证明护照管理模块验证经签名的远程证明信息RA1，并确认nonce1、根值、虚拟机管理器的IP地址、远程验证服务端口号等用于哈希值的生成。在框1428处，云管服务器评估远程验证证据，并输出结果，并将该结果与远程证明证据RA1、nonce1、根值与算法、虚拟机管理器IP地址与端口号、服务器证书等信息生成远程验证护照。然后云管对远程验证护照进行签名。操作1430和1432与图12中的对应操作相同。

[0147] 图15显示了网管服务器、虚拟机、物理主机如何使用带有隐私保护的远程证明护照完成虚拟机及承载该虚拟机的物理主机的远程证明。其中，操作1512和1514与第一个示例中的图13中的对应操作相同。虚拟机管理器启动vRoT时，为RoT分配密钥对(PK_i,SK_i)并发送1516给虚拟可信根。操作1518、1520、1522、1524、1526、1528、1530、1532、1534、1536、1538与图13中对应操作相同。• 在框1540处，网管从虚拟机管理器提供的远程证明护照的链接证据中提取根值，验证vAIK_i中的PK_i是否参与了根值的生成，如果是，则完成了对物

理主机和虚拟的验证。否则，表示验证失败。

[0148] 通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0149] 图16提供了基于凭证获取虚可信根vRoT远程证明护照的第三个示例过程。如图16所示，其包括虚拟机管理器1602、虚拟可信根1604、虚拟机1606、云管1608和网管1610。其中操作1612、1614、1616、1618和1620和图13中描述的对应操作相同。网管向VM发送1622远程证明请求，该请求包括随机数，并且策略指定虚拟机可以一起发送虚拟机的的远程证明信息和物理主机的远程证明护照。虚拟机通知1624虚拟可信根提供虚拟机的远程证明信息和物理主机的远程证明护照。虚拟可信根向虚拟机管理器发送1626请求，要求提供与vAIK_i证书相关的远程证明护照。在框1628处，虚拟机管理器使用vAIK_i证书中的公钥PK_i查找相对应的远程证明护照。虚拟机管理器将找到的远程证明护照发送1630给虚拟可信根。虚拟可信根生成针对虚拟机的经签名的远程证明信息，并将经签名的远程证明信息以及远程证明护照一起发送1632给网管。在框1634处，网管服务器验证VM远程验证材料。在框1636处，网管服务器从经签名的远程证明信息获取虚拟机管理器IP、远程验证客户端(Remote Attestation Client，RAC)端口、以及vAIK_i证书中的PK_i。在框1638处，网管服务器验证远程证明护照，验证方法与前述示例相同。在框1640处，网管服务器从远程证明护照中提取链接证据，验证vAIK_i证书的公钥PK_i是否直接或者间接包含在远程证明护照中，如果包含，则完成证明，确认虚拟机/虚拟网络功能模块的可信状态。如果不包含，则结束操作。通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0150] 图17提供了基于凭证获取虚可信根vRoT远程证明护照的第四个示例过程。如图17所示，在操作1712处完成可信启动。在框1714处，生成远程证明护照，生成远程证明护照的过程如示例一中图13所描述的。此外，在生成远程证明护照过程中，云管存储了相应的远程证明护照。图17中的操作1718、1720、1722、1724、1726、1730、1732与图14中的对应操作相同。网管向云管1734发送远程证明护照获取请求，并携带vAIK_i证书。云管查找相应的远程证明护照并返回1736给网管。在框1738处，网管验证远程证明护照。在框1740处，网管验证vAIK_i证书中的PK_i是否直接或间接包含在远程证明护照提供的连接证据中。如包括，则完成证明，确认虚拟机的可信状态，如不包括，则结束验证。通过上述方式，实现了虚拟可信根和硬件可信根的关联关系，解决了虚拟化平台进行深度证明时面临的硬件可信根设备导致的性能问题，从而改进了用户体验。

[0151] 图18进一步示出了根据本申请实施例的用于确定目标车辆的装置1800的框图，装置1800可以包括多个模块，以用于执行如图2中所讨论的过程200中的对应步骤。如图18所示，装置1800包括请求发送单元1802，被配置为在物理主机处向验证服务器发送用于获取加密证书的请求，请求包括针对虚拟机的虚拟可信根的目标公钥；随机数获取单元1804，被配置为从验证服务器获取由目标公钥加密的随机数；远程证明信息获取单元1806，被配置为基于加密的随机数来从物理主机的硬件可信根获取经签名的远程证明信息，经签名的远程证明信息包括针对硬件可信根的签名证书；以及证明信息和公钥发送单元1808，被配置为向验证服务器发送经签名的远程证明信息和目标公钥；加密证书接收单元1810，被配置为从验证服务器接收针对目标公钥的加密证书。

[0152] 在一些实施例中，装置1800还包括：启动生成单元，被配置为响应于虚拟可信根被启动，由虚拟可信根生成目标公钥。

[0153] 在一些实施例中，其中远程证明信息获取单元1806包括：解密单元，被配置为使用与所述目标公钥相对应的目标私钥来对加密的随机数进行解密；以及本地信息获取单元，被配置为基于解密的随机数来获取针对硬件可信根的本地证明信息，本地证明信息包括签名证书；基于随机数的信息生成单元，被配置为基于解密的随机数和本地证明信息生成远程证明信息；命名单元，被配置为使用与签名证书相对应的签名私钥对远程证明信息进行签名。

[0154] 在一些实施例中，其中验证服务器是第一验证服务器，签名证书是第一签名证书，该装置1800还包括：第二签名证书获取单元，被配置为向第二验证服务器发送加密证书以从第二验证服务器获取第二签名证书。

[0155] 图19进一步示出了根据本申请实施例的用于提供证书的装置1900的框图，装置1900可以包括多个模块，以用于执行如图3中所讨论的过程300中的对应步骤。如图1900所示，装置1900包括随机数生成单元1902，被置为响应于从物理主机接收到用于获取加密证书的请求，在验证服务器处生成随机数，请求包括针对虚拟机的虚拟可信根的目标公钥；加密单元1904，被配置为使用目标公钥对随机数进行加密；随机数发送单元1906，被配置为向物理主机发送经加密的随机数；远程证明信息接收单元1908，被配置为从物理主机接收目标公钥和经签名的远程证明信息，经签名的远程证明信息包括针对物理主机的硬件可信根的签名证书；以及证书发送单元1910，被配置为响应于经签名的远程证明信息通过验证，向物理主机发送加密证书，加密证书是针对目标公钥的。

[0156] 在一些实施例中，该位置1900还包括：验证单元，被配置为通过以下操作来验证经签名的远程证明信息：利用签名证书中的验证公钥验证签名；以及确定经签名的远程证明信息是否包括随机数；以及验确定单元，被配置为响应于签名通过验证并且经签名的远程证明信息包括随机数，确定经签名的远程证明信息通过验证。

[0157] 图20进一步示出了根据本申请实施例的用于获取凭证的装置2000的框图，装置2000可以包括多个模块，以用于执行如图8中所讨论的过程800中的对应步骤。如图20所示，装置2000包括请求发送单元2002，被配置为在物理主机处向验证服务器发送用于获取凭证的请求；随机数获取单元2004，被配置为从验证服务器获取随机数；远程证明信息获取单元2006，被配置为基于随机数和一组公钥，从物理主机的硬件可信根获取经签名的远程证明信息，经签名的远程证明信息包括针对硬件可信根的签名证书；以及回复信息发送单元2008，被配置为向验证服务器发送回复信息，回复信息包括经签名的远程证明信息、关于一组公钥的指示信息以及随机数，凭证获取单元2010，被配置为从验证服务器获取凭证凭证指示一组公钥由于硬件可信根可信而被认定为是可信的。

[0158] 在一些实施例中，装置2000还包括：一组公钥生成单元，被配置为由物理主机中的虚拟机管理器生成一组公钥。

[0159] 在一些实施例中，其中远程证明信息获取单元2006包括：字符串生成单元，被配置为基于随机数和一组公钥，生成字符串；以及第一哈希值生成单元，被配置为基于字符串来生成目标哈希值；第一证明信息获取单元，被配置为基于所述目标哈希值，从所述物理主机的硬件可信根获取经签名的远程证明信息。

[0160] 在一些实施例中，其中字符串生成单元包括：第一链接单元，被配置为通过对随机数、一组公钥、虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号进行链接来形成字符串。

[0161] 在一些实施例中，其中字符串生成单元包括：累加单元，被配置为通过将一组公钥输入累加器来获得根值；以及第一字符串生成单元，被配置为基于根值和随机数，生成字符串。

[0162] 在一些实施例中，其中第一字符串生成单元包括：第二链接单元，被配置为通过对随机数、根值、虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号进行链接来形成字符串。

[0163] 在一些实施例中，其中指示信息包括根值。

[0164] 在一些实施例中，其中指示信息包括一组公钥。

[0165] 在一些实施例中，其中第一证明信息获取单元包括：本地证明信息获取单元，被配置为基于目标哈希值，获取针对硬件可信根的本地证明信息，本地证明信息包括签名证书；第一远程证明信息生成单元，被配置为基于目标哈希值和本地证明信息来生成远程证明信息；签名单元，被配置为使用与签名证书相对应的签名私钥对远程证明信息进行签名。

[0166] 在一些实施例中，其中请求是第一请求，经签名的远程证明信息是第一经签名的远程证明信息，验证服务器是第一验证服务器，签名是第一签名，装置2000还包括：分配单元，被配置为响应于启动虚拟机和对应的虚拟可信根，从一组公钥中选择分配给虚拟可信根的公钥；证书获取单元，被配置为获取针对公钥的签名证书；第二请求发送单元，被配置为向第二验证服务器发送注册虚拟机的第二请求，第二请求包括虚拟机的标识；第三请求接收单元，被配置为从第二验证服务器接收用于获取证明信息的第三请求，第三请求包括由第二验证服务器生成的随机数；以及远程证明信息发送单元，被配置为向第二验证服务器发送针对虚拟机的经签名的第二远程证明信息以用于确定虚拟机的可信状态，经签名的第二远程证明信息包括签名证书和对应的第二签名。

[0167] 在一些实施例中，其中第三请求还包括获取证明信息的策略；其中远程证明信息发送单元包括：基于策略的发送单元，被配置为基于策略，发送经签名的第二远程证明信息。

[0168] 在一些实施例中，其中基于策略的发送单元包括：获取经签名的证明信息的单元，被配置为响应于策略指示仅获取针对虚拟机的证明信息，基于随机数从虚拟可信根获取经签名的第二远程证明信息，经签名的第二远程证明信息还包括物理主机中的虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号；经签名的信息发送单元，被配置为向第二验证服务器发送经签名的第二远程证明信息；凭证获取单元，被配置为响应于接收到用于获取凭证的第四请求，基于签名证书中的公钥，获取凭证，第四请求包括互联网协议地址、端口号和签名证书；以及凭证发送单元，被配置为向第二验证服务器发送凭证以确定虚拟机的可信状态。

[0169] 在一些实施例中，其中基于策略的发送单元包括：经签名的信息获取单元，被配置为响应于策略指示获取针对虚拟机的证明信息和凭证，从虚拟可信根获取经签名的第二远程证明信息；基于公钥的凭证获取信息，被配置为基于公钥来从虚拟机管理器获取凭证；以及信息和凭证发送单元，被配置为向第二验证服务器发送经签名的第二远程证明信息和凭

证以用于确定虚拟机的可信状态。

[0170] 图21进一步示出了根据本申请实施例的用于提供凭证的装置2100的框图，装置2100可以包括多个模块，以用于执行如图9中所讨论的过程900中的对应步骤。如图21所示，装置2100包括回复信息接收单元2102，被配置为在验证服务器处从物理主机接收回复信息，回复信息包括经签名的远程证明信息、关于一组公钥的指示信息和随机数，经签名的远程证明信息包括针对物理主机的硬件可信根的签名证书；验证单元2104，被配置为对经签名的远程证明信息进行验证；凭证生成单元2106，被配置为响应于经签名的远程证明信息通过验证，基于远程证明信息和指示信息，生成凭证，凭证指示一组公钥的可信性；以及凭证发送单元2108，被配置为将凭证发送给物理主机。

[0171] 在一些实施例中，其中经签名的远程证明信息包括还包括目标哈希值，验证单元2104包括：哈希值验证单元，被配置为通过以下操作对经签名的远程证明信息和目标哈希值进行验证：签名验证单元，被配置为通过签名证书中的公钥验证经签名的远程证明信息中的签名；验证哈希值生成单元，被配置为响应于签名通过验证，基于随机数和指示信息，生成验证哈希值；以及比较验证单元，被配置为通过将目标哈希值和验证哈希值进行比较来验证经签名的远程证明信息。

[0172] 在一些实施例中，其中指示信息包括一组公钥，其中验证哈希值生成单元包括：字符串生成单元，被配置为基于随机数和一组公钥，生成字符串；以及基于字符串的哈希值生成单元，被配置为基于字符串来生成验证哈希值。

[0173] 在一些实施例中，其中回复信息还包括物理主机中的虚拟机管理器的互联网协议地址、虚拟机管理器的远程验证服务的端口号；其中第一字符串生成单元包括：第一链接单元，被配置为通过对随机数、一组公钥、互联网协议地址和端口号进行链接来形成字符串。

[0174] 在一些实施例中，其中指示信息包括根值，根值是通过将一组公钥输入累加器而获得的，其中验证哈希值生成单元包括：第二字符串生成单元，被配置为基于随机数和根值，生成字符串；以及验证哈希值生成单元，被配置为基于字符串来生成验证哈希值。

[0175] 在一些实施例中，其中回复信息还包括物理主机中的虚拟机管理器的互联网协议地址、虚拟机管理器的远程验证服务的端口号；其中第二字符串生成单元包括：第二链接单元，被配置为通过对随机数、根值、互联网协议地址和端口号进行链接来形成字符串。

[0176] 在一些实施例中，凭证还包括互联网协议地址和端口号。

[0177] 在一些实施例中，其中凭证生成单元2106包括：第一评估结果生成单元，被配置为通过对远程证明信息进行评估来生成评估结果；加入单元，被配置为将评估结果加入凭证。

[0178] 在一些实施例中，其中凭证生成单元2106包括：第二评估结果生成单元，被配置为通过对远程证明信息进行评估来生成评估结果；判定生成单元，被配置为响应于评估结果满足预定要求，生成凭证，凭证包括将评估结果。

[0179] 在一些实施例中，装置2100还包括：随机数生成单元，被配置为响应于从物理主机接收到用于获取凭证的请求，生成随机数；以及随机数发送单元，被配置为向物理主机发送随机数。

[0180] 图22进一步示出了根据本申请实施例的用于验证信息的装置2200的框图，装置2200可以包括多个模块，以用于执行如图10中所讨论的过程1000中的对应步骤。如图22所示，装置2200包括随机数生成单元2202，被配置为响应于从物理主机接收到注册物理主机

中的虚拟机的第一请求，在验证服务器处生成随机数；证明信息获取单元2204，被配置为向物理主机发送用于获取证明信息的第二请求，第二请求包括随机数；以及证明信息和凭证接收单元2206，被配置为从物理主机接收针对虚拟机的经签名的远程证明信息和凭证，经签名的远程证明信息包括签名证书和对应的签名，签名证书是针对从一组公钥中选择的分配给虚拟机的公钥的证书，凭证指示一组公钥的可信性；可信状态确定单元2208，被配置为基于经签名的远程证明信息和凭证，确定虚拟机的可信状态。

[0181] 在一些实施例中，其中经签名的远程证明信息还包括物理主机中的虚拟机管理器的互联网协议地址和虚拟机管理器的远程验证服务的端口号，其中第二请求还包括从所述物理主机获取证明信息的策略，策略指示仅获取针对虚拟机的证明信息，其中证明信息和凭证接收单元2206包括：第一接收单元，被配置为接收经签名的远程证明信息；第一验证单元，被配置为对经签名的远程证明信息进行验证；获取单元，被配置为响应于经签名的远程证明信息通过验证，从经签名的远程证明信息获取签名证书、互联网协议地址和端口号；请求发送单元，被配置为向物理主机发送获取凭证的第三请求，第三请求包括互联网协议地址、端口号和签名证书；凭证接收单元，被配置为从所述物理主机接收所述凭证。

[0182] 在一些实施例中，可信状态确定单元2208包括凭证验证单元，被配置为对凭证进行验证；第一支持确定单元，被配置为响应于凭证通过验证，确定签名证书中的公钥是否被凭证支持；以及第一虚拟机可信确定单元，被配置为响应于公钥被凭证支持，确定虚拟机是可信的。

[0183] 在一些实施例中，其中第二请求还包括从所述物理主机获取证明信息的策略，策略指示获取针对虚拟机的证明信息和凭证，其中可信状态确定单元2208包括：第二验证单元，被配置为对经签名的远程证明信息和凭证进行验证；签名证书获取单元，被配置为响应于经签名的远程证明信息和凭证通过验证，从经签名的远程证明信息获取签名证书；第二支持确定单元，被配置为确定签名证书中的公钥是否被凭证支持；以及第二虚拟机可信确定单元，被配置为响应于公钥被凭证支持，确定虚拟机是可信的。

[0184] 在一些实施例中，其中第一支持确定单元或第二支持确定单元包括：公钥存在确定单元，被配置为确定公钥是否存在于凭证中。

[0185] 在一些实施例中，其中凭证包括根值，根值是通过将一组公钥输入累加器而获得的，其中第一支持确定单元或第二支持确定单元包括：提取单元，被配置为提取凭证中的根值；以及第三支持确定单元，被配置为基于根值和公钥，确定公钥是否被凭证支持。

[0186] 图23进一步示出了根据本申请实施例的用于验证信息的装置2300的框图，装置2300可以包括多个模块，以用于执行如图11中所讨论的过程1100中的对应步骤。如图23所示，装置2300包括证明信息获取单元2302，被配置为响应于从物理主机接收到注册物理主机中的虚拟机的第一请求，在第一验证服务器处向物理主机发送获取证明信息的第二请求，第二请求包括随机数；远程证明信息接收单元2304，被配置为接收针对虚拟机的经签名的远程证明信息，远程证明信息包括签名证书，签名证书是针对从一组公钥中选择的分配给虚拟机的公钥的证书；证书获取单元2306，被配置为响应于远程证明信息通过验证，获取签名证书；请求发送单元2308，被配置为向第二验证服务器发送用于获取凭证的第三请求，请求包括签名证书；凭证获取单元2310，被配置为用于从第二验证服务器获取凭证；可信状态确定单元2312，被配置为基于凭证来确定虚拟机的可信状态，凭证指示一组公钥的可信

性。

[0187] 在一些实施例中,其中可信状态确定单元2312包括:验证单元,被配置为响应于接收到凭证,对凭证进行验证;支持确定单元,被配置为响应于凭证通过验证,确定签名证书的公钥是否被凭证支持;以及可信确定单元,被配置为响应于公钥被凭证支持,确定虚拟机是可信的。

[0188] 在一些实施例中,其中支持确定单元包括:公钥确定存在单元,被配置为确定公钥是否存在于凭证中。

[0189] 在一些实施例中,其中凭证包括根值,根值是通过将一组公钥输入累加器而获得的,其中支持确定单元包括:提取单元,被配置为提取凭证中的根值;以及公钥支持确定单元,被配置为基于根值和公钥,确定公钥是否被凭证支持。

[0190] 图24示出了可以用来实施本申请内容的实施例的示例设备2400的示意性框图。例如,根据本申请实施例的图1中的物理主机102、第一验证服务器114和第二验证服务器112、图5中的物理主机102、第一验证服务器114和第二验证服务器112可由示例设备2400来实施。如图所示,设备2400包括中央处理单元(CPU)2401,其可以根据存储在只读存储器(ROM)2402中的计算机程序指令或者从存储单元2408加载到随机访问存储器(RAM)2403中的计算机程序指令,来执行各种适当的动作和处理。在RAM2403中,还可存储设备2400操作所需的各种程序和数据。CPU 2401、ROM 2402以及RAM 2403通过总线2404彼此相连。输入/输出(I/O)接口2405也连接至总线2404。

[0191] 设备2400中的多个部件连接至I/O接口2405,包括:输入单元2406,例如键盘、鼠标等;输出单元2407,例如各种类型的显示器、扬声器等;存储单元2408,例如磁盘、光盘等;以及通信单元2409,例如网卡、调制解调器、无线通信收发机等。通信单元2409允许设备2400通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

[0192] 上文所描述的各个过程和处理,例如过程200、300、800、900、1000和1100,可由处理单元2401执行。例如,在一些实施例中,过程200、300、800、900、1000和1100可被实现为计算机软件程序,其被有形地包含于机器可读介质,例如存储单元2408。在一些实施例中,计算机程序的部分或者全部可以经由ROM 2402和/或通信单元2409而被载入和/或安装到设备2400上。当计算机程序被加载到RAM 2403并由CPU 2401执行时,可以执行上文描述的过程200、300、800、900、1000和1100的一个或多个动作。

[0193] 本申请可以是方法、装置、系统、芯片和/或计算机程序产品。芯片可以包括处理单元和通信接口,处理单元可以处理从通信接口接收到的程序指令。计算机程序产品可以包括计算机可读存储介质,其上载有用于执行本申请的各个方面的计算机可读程序指令。

[0194] 计算机可读存储介质可以是可以保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以是——但不限于——电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括:便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式压缩盘只读存储器(CD-ROM)、数字多功能盘(DVD)、记忆棒、软盘、机械编码设备、例如其上存储有指令的打孔卡或凹槽内凸起结构、以及上述的任意合适的组合。这里所使用的计算机可读存储介质不被解释为瞬时信号本身,诸如无线电波或者其他自由传播的电磁波、通

过波导或其他传输媒介传播的电磁波(例如,通过光纤电缆的光脉冲)、或者通过电线传输的电信号。

[0195] 这里所描述的计算机可读程序指令可以从计算机可读存储介质下载到各个计算/处理设备,或者通过网络、例如因特网、局域网、广域网和/或无线网下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光纤传输、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配卡或者网络接口从网络接收计算机可读程序指令,并转发该计算机可读程序指令,以供存储在各个计算/处理设备中的计算机可读存储介质中。

[0196] 用于执行本申请操作的计算机程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、或者以一种或多种编程语言的任意组合编写的源代码或目标代码,所述编程语言包括面向对象的编程语言—诸如Smalltalk、C++等,以及常规的过程式编程语言—诸如“C”语言或类似的编程语言。计算机可读程序指令可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络—包括局域网(LAN)或广域网(WAN)—连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。在一些实施例中,通过利用计算机可读程序指令的状态信息来个性化定制电子电路,例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA),该电子电路可以执行计算机可读程序指令,从而实现本申请的各个方面。

[0197] 这里参照根据本申请实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述了本申请的各个方面。应当理解,流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合,都可以由计算机可读程序指令实现。

[0198] 这些计算机可读程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理单元,从而生产出一种机器,使得这些指令在通过计算机或其它可编程数据处理装置的处理单元执行时,产生了实现流程图和/或框图中的一个或多个方框中规定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中,这些指令使得计算机、可编程数据处理装置和/或其他设备以特定方式工作,从而,存储有指令的计算机可读介质则包括一个制造品,其包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的各个方面的指令。

[0199] 也可以把计算机可读程序指令加载到计算机、其它可编程数据处理装置、或其它设备上,使得在计算机、其它可编程数据处理装置或其它设备上执行一系列操作步骤,以产生计算机实现的过程,从而使得在计算机、其它可编程数据处理装置、或其它设备上执行的指令实现流程图和/或框图中的一个或多个方框中规定的功能/动作。

[0200] 附图中的流程图和框图显示了根据本申请的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分,所述模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个连续的方框实际上可以基本并行地执

行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或动作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0201] 以上已经描述了本申请的各实施方式,上述说明是示例性的,并非穷尽性的,并且也不限于所披露的各实施方式。在不偏离所说明的各实施方式的范围和精神的情况下,对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择,旨在最好地解释各实施方式的原理、实际应用或对市场中的技术的改进,或者使本技术领域的其他普通技术人员能理解本文披露的各实施方式。

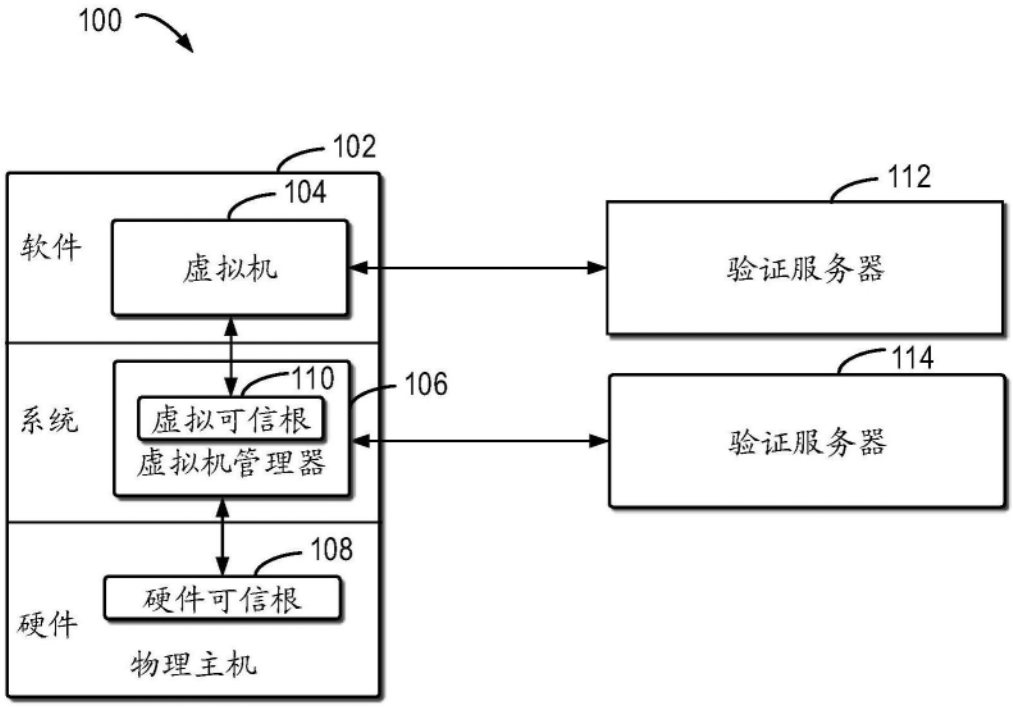

100
102
104
软件
虚拟机
112
验证服务器
系统
110
虚拟可信根
虚拟机管理器
106
114
验证服务器
108
硬件可信根
硬件
物理主机

图1

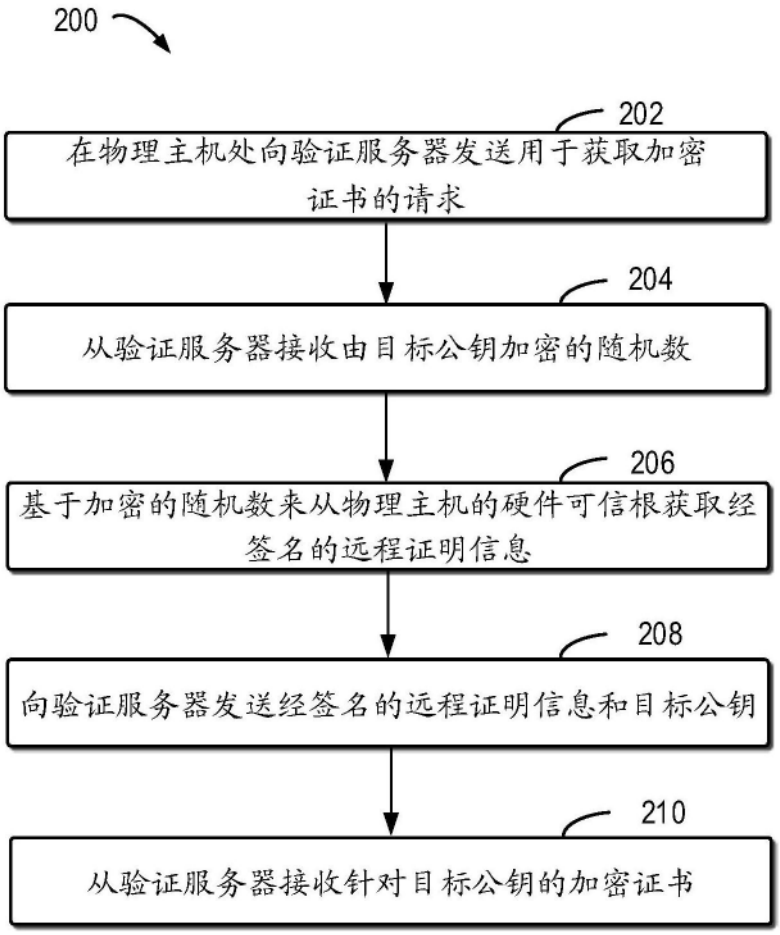

200
202
在物理主机处向验证服务器发送用于获取加密证书的请求
204
从验证服务器接收由目标公钥加密的随机数
206
基于加密的随机数来从物理主机的硬件可信根获取经签名的远程证明信息
208
向验证服务器发送经签名的远程证明信息和目标公钥
210
从验证服务器接收针对目标公钥的加密证书

图2

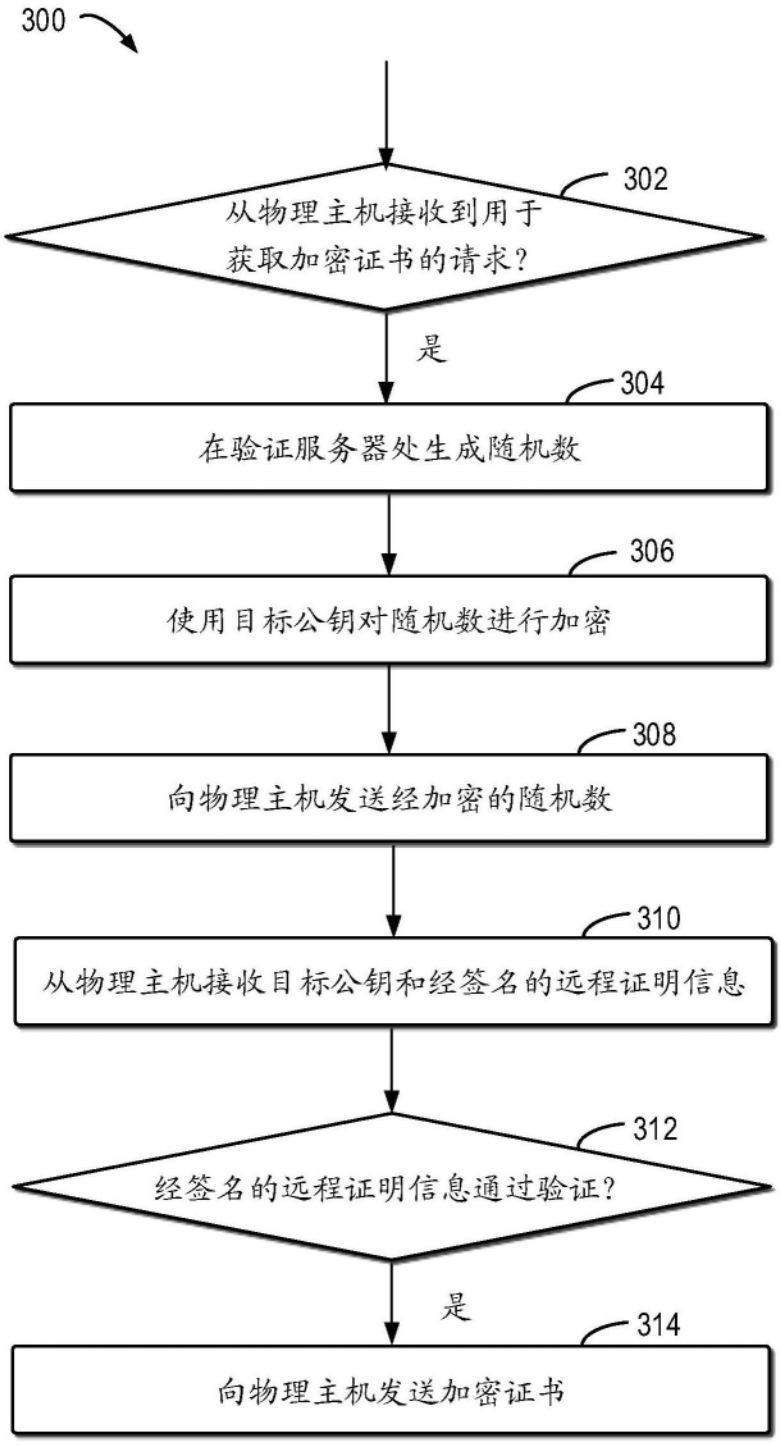

300
302
从物理主机接收到用于获取加密证书的请求?
是
304
在验证服务器处生成随机数
306
使用目标公钥对随机数进行加密
308
向物理主机发送经加密的随机数
310
从物理主机接收目标公钥和经签名的远程证明信息
312
经签名的远程证明信息通过验证?
是
314
向物理主机发送加密证书

图3

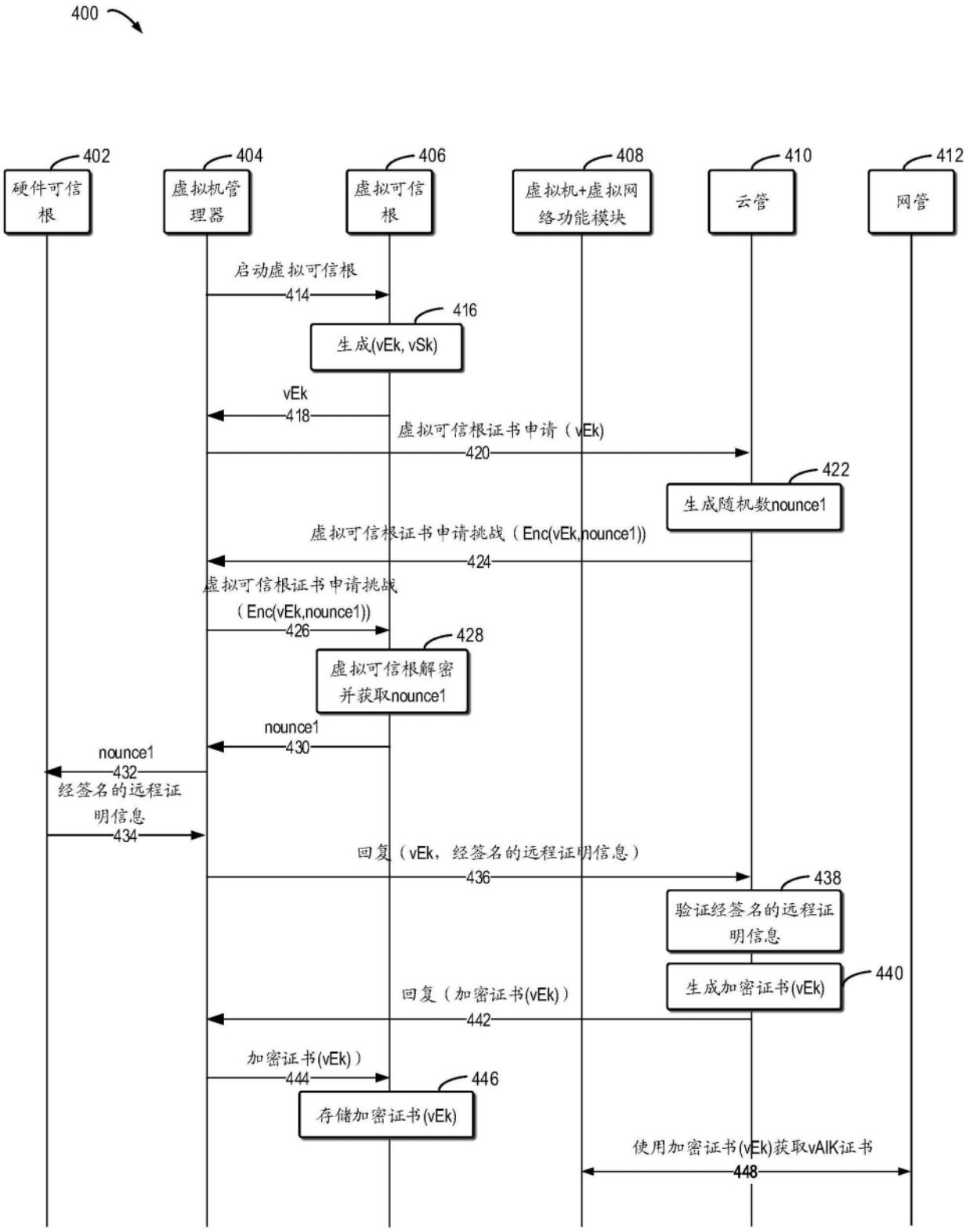

400
402
硬件可信根
404
虚拟机管理器
406
虚拟可信根
408
虚拟机+虚拟网络功能模块
410
云管
412
网管
启动虚拟可信根
414
416
生成(vEk, vSk)
vEk
418
虚拟可信根证书申请（vEk)
420
422
生成随机数nounce1
虚拟可信根证书申请挑战（Enc(vEk,nounce1))
424
虚拟可信根证书申请挑战
（Enc(vEk,nounce1))
426
428
虚拟可信根解密并获取nounce1
nounce1
430
nounce1
432
经签名的远程证明信息
434
回复（vEk，经签名的远程证明信息）
436
438
验证经签名的远程证明信息
生成加密证书(vEk)
440
回复（加密证书(vEk)）
442
加密证书(vEk)）
444
446
存储加密证书(vEk)
使用加密证书(vEk)获取vAIK证书
448

图4

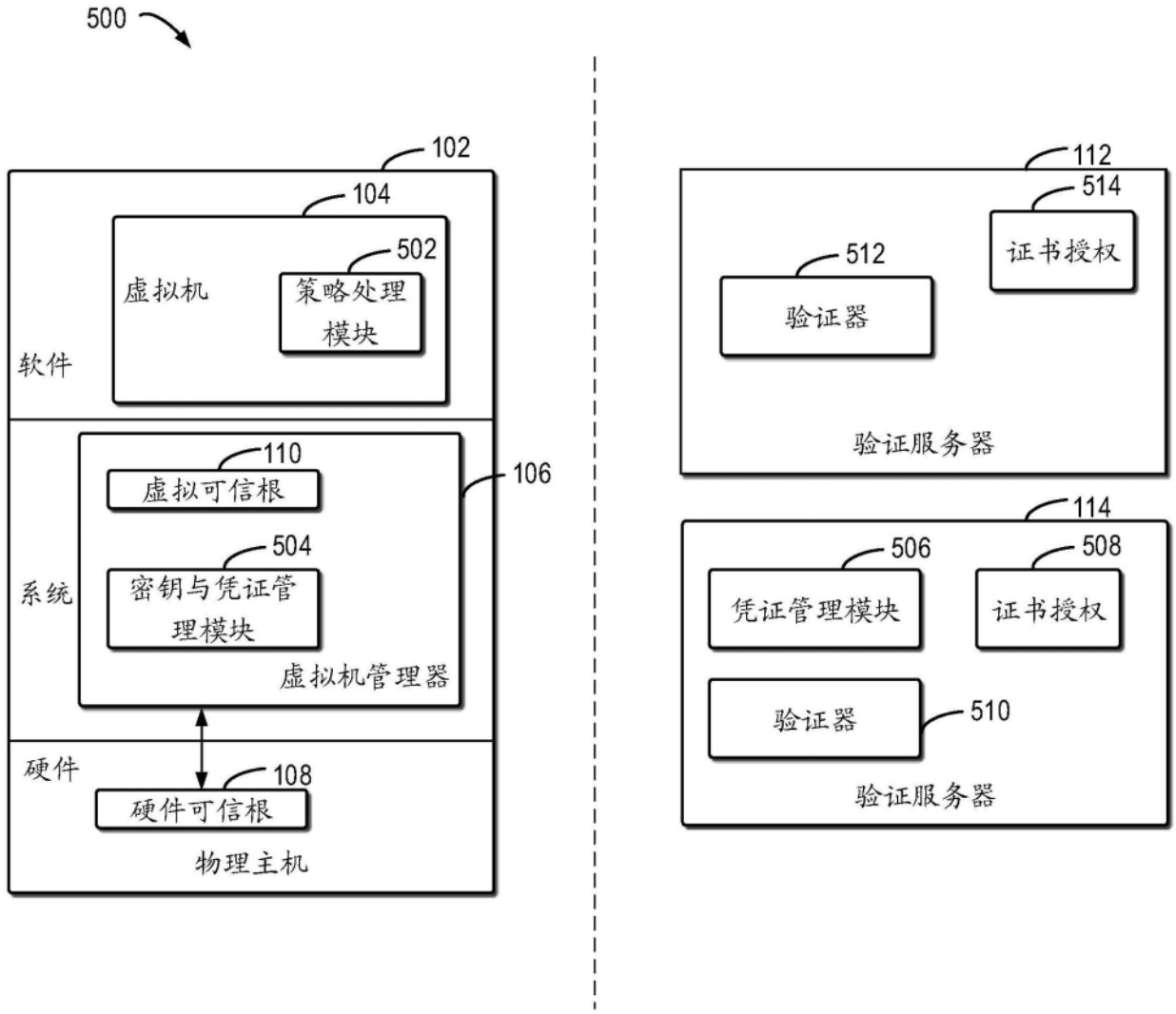

500
102
104
502
虚拟机
策略处理模块
软件
110
虚拟可信根
106
504
密钥与凭证管理模块
系统
虚拟机管理器
硬件
108
硬件可信根
物理主机
112
514
证书授权
512
验证器
验证服务器
114
506
508
凭证管理模块
证书授权
验证器
510
验证服务器

图5

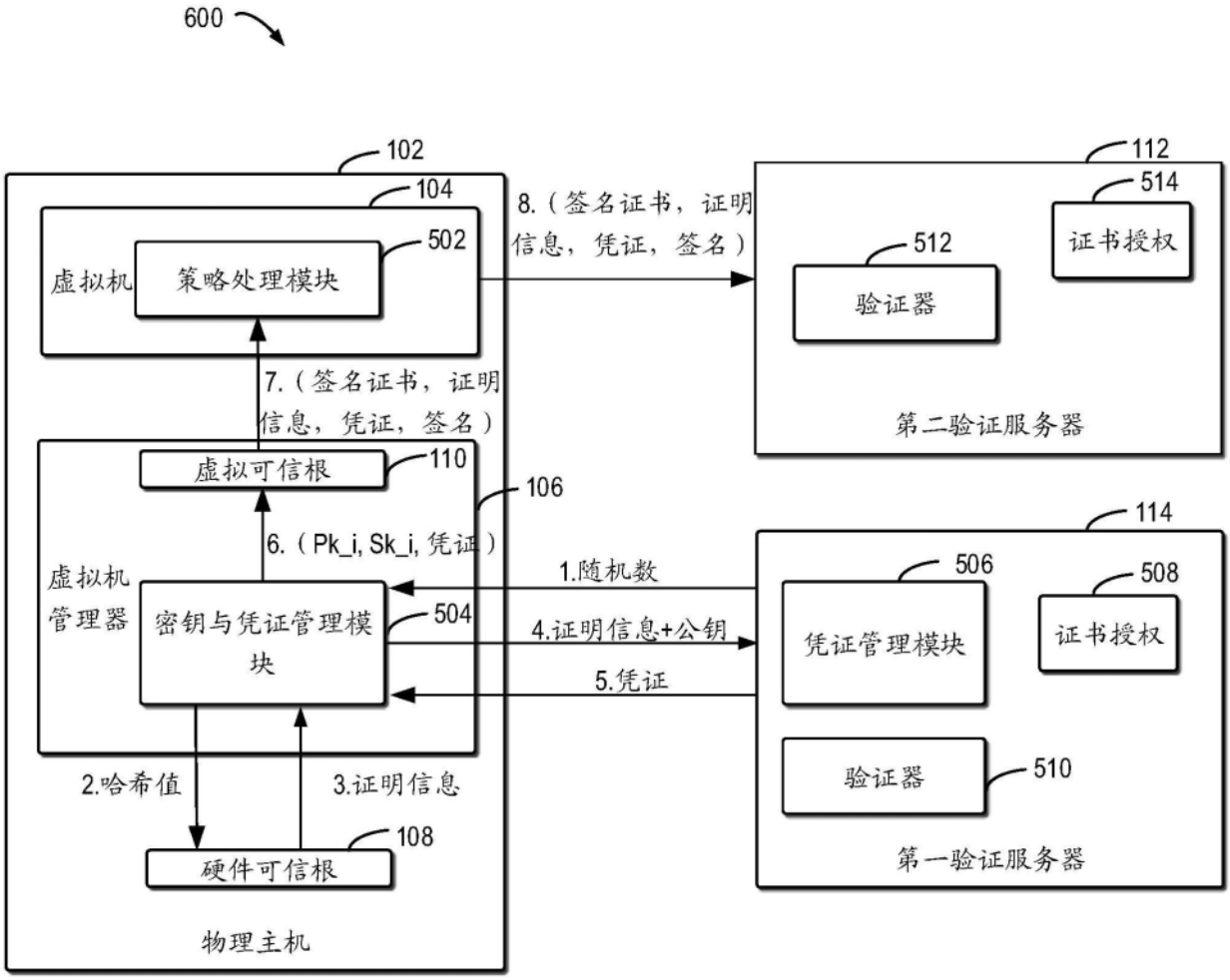

600
102
104
虚拟机
策略处理模块
502
8.（签名证书，证明信息，凭证，签名）
112
514
证书授权
512
验证器
第二验证服务器
7.（签名证书，证明信息，凭证，签名）
虚拟可信根
110
106
6.（Pk_i, Sk_i, 凭证）
虚拟机管理器
密钥与凭证管理模块
504
1.随机数
4.证明信息+公钥
5.凭证
114
506
凭证管理模块
508
证书授权
验证器
510
第一验证服务器
2.哈希值
3.证明信息
108
硬件可信根
物理主机

图6

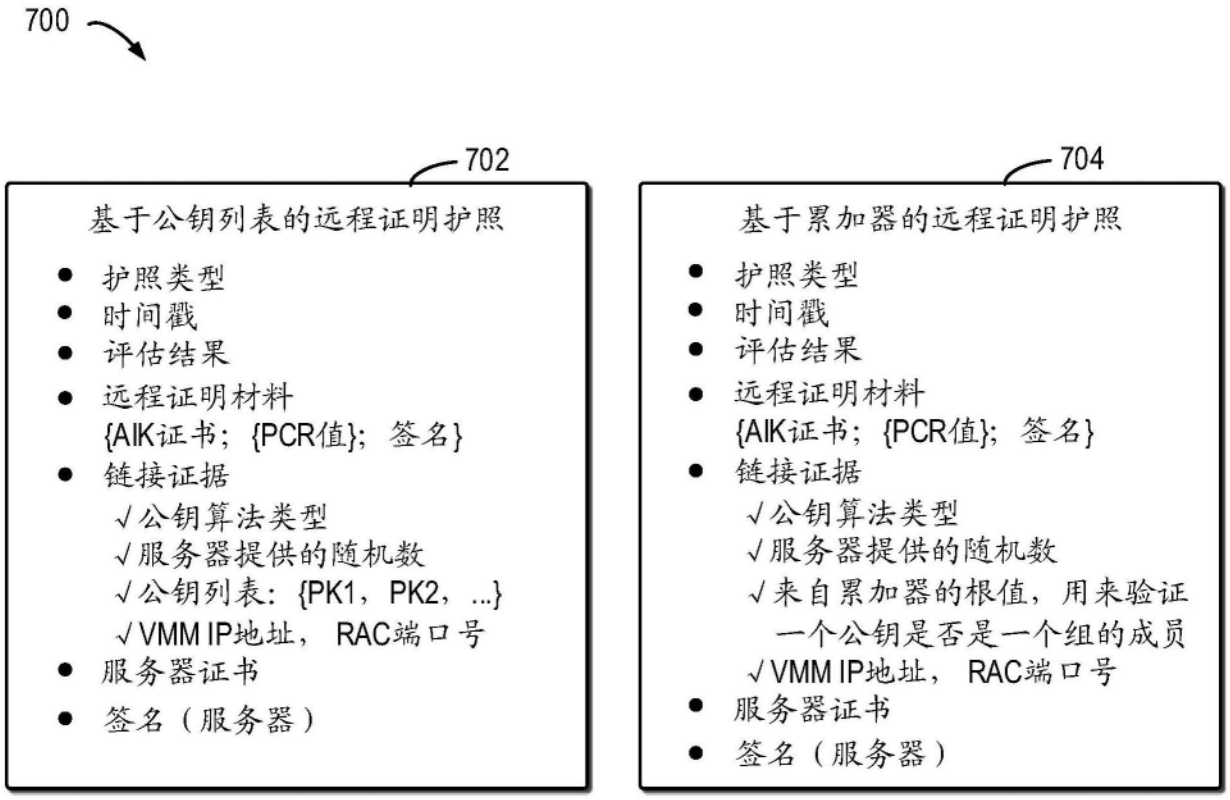

700
702
基于公钥列表的远程证明护照
护照类型
时间戳
评估结果
远程证明材料
{AIK证书；{PCR值}；签名}
链接证据
√公钥算法类型
√服务器提供的随机数
√公钥列表：{PK1，PK2，...}
√VMM IP地址， RAC端口号
服务器证书
签名（服务器）
704
基于累加器的远程证明护照
护照类型
时间戳
评估结果
远程证明材料
{AIK证书；{PCR值}；签名}
链接证据
√公钥算法类型
√服务器提供的随机数
√来自累加器的根值，用来验证一个公钥是否是一个组的成员
√VMM IP地址， RAC端口号
服务器证书
签名（服务器）

图7

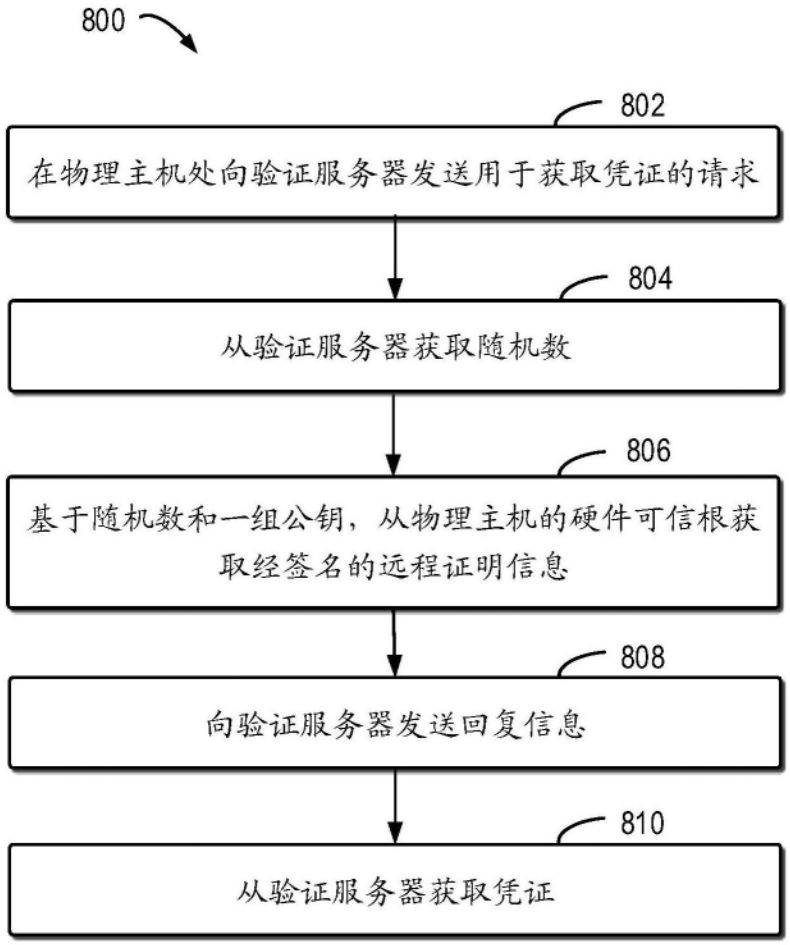

800
802
在物理主机处向验证服务器发送用于获取凭证的请求
804
从验证服务器获取随机数
806
基于随机数和一组公钥，从物理主机的硬件可信根获取经签名的远程证明信息
808
向验证服务器发送回复信息
810
从验证服务器获取凭证

图8

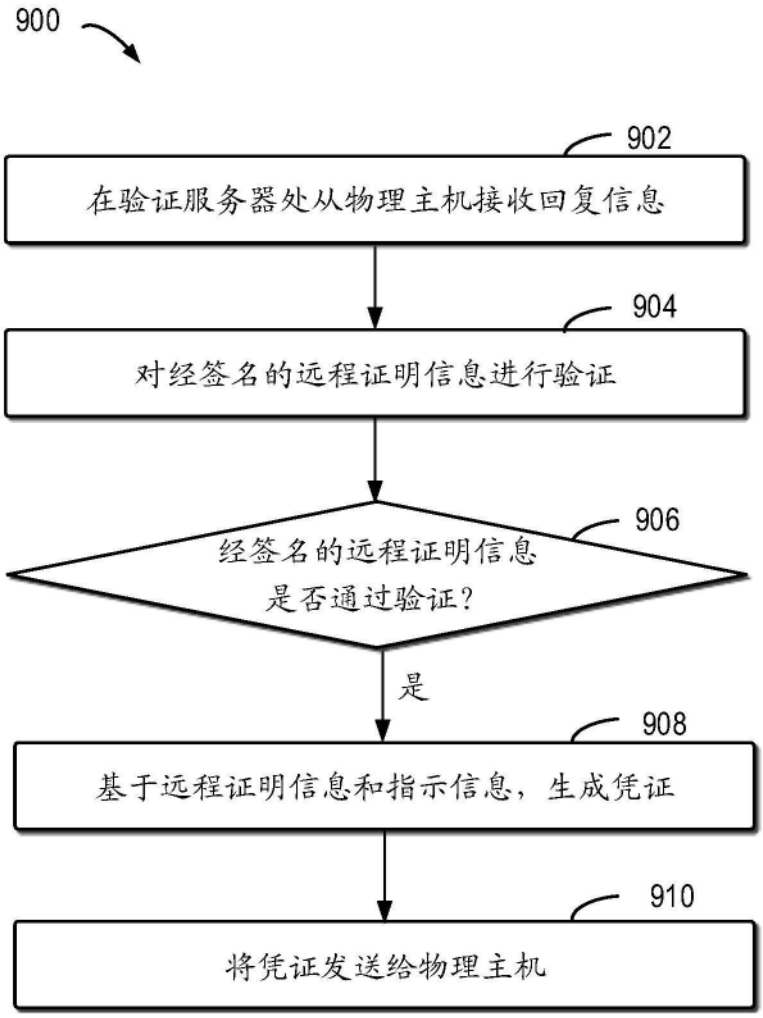

900
902
在验证服务器处从物理主机接收回复信息
904
对经签名的远程证明信息进行验证
906
经签名的远程证明信息
是否通过验证?
是
908
基于远程证明信息和指示信息，生成凭证
910
将凭证发送给物理主机

图9

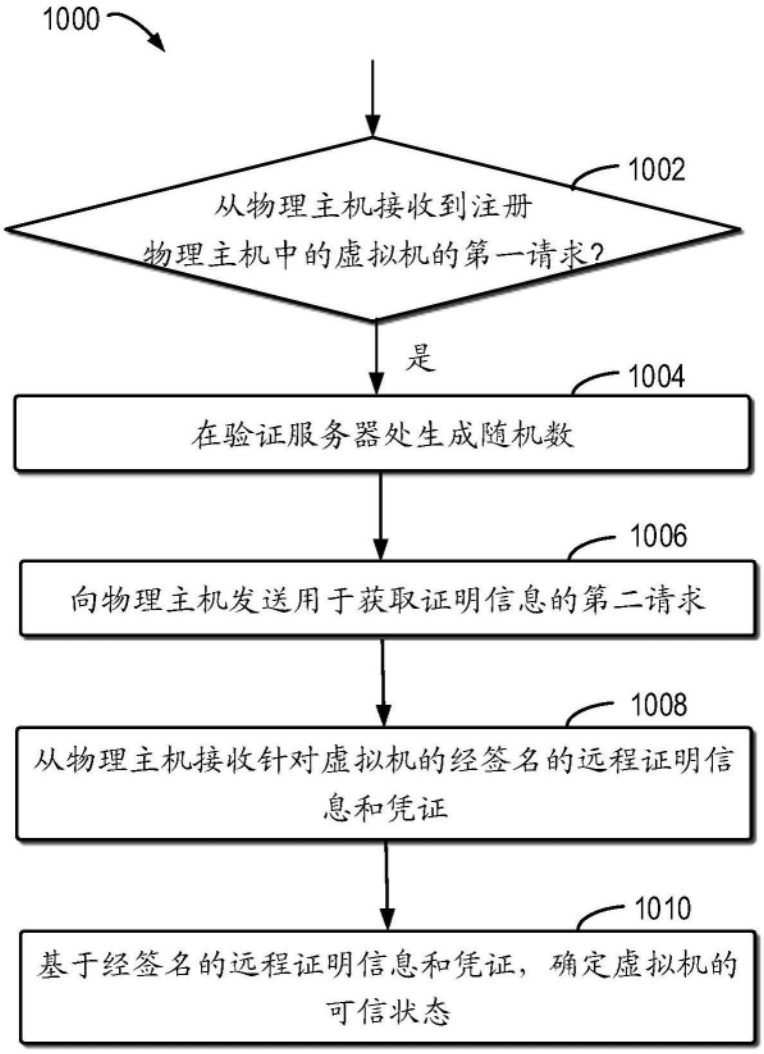

1000
1002
从物理主机接收到注册物理主机中的虚拟机的第一请求?
是
1004
在验证服务器处生成随机数
1006
向物理主机发送用于获取证明信息的第二请求
1008
从物理主机接收针对虚拟机的经签名的远程证明信息和凭证
1010
基于经签名的远程证明信息和凭证，确定虚拟机的可信状态

图10

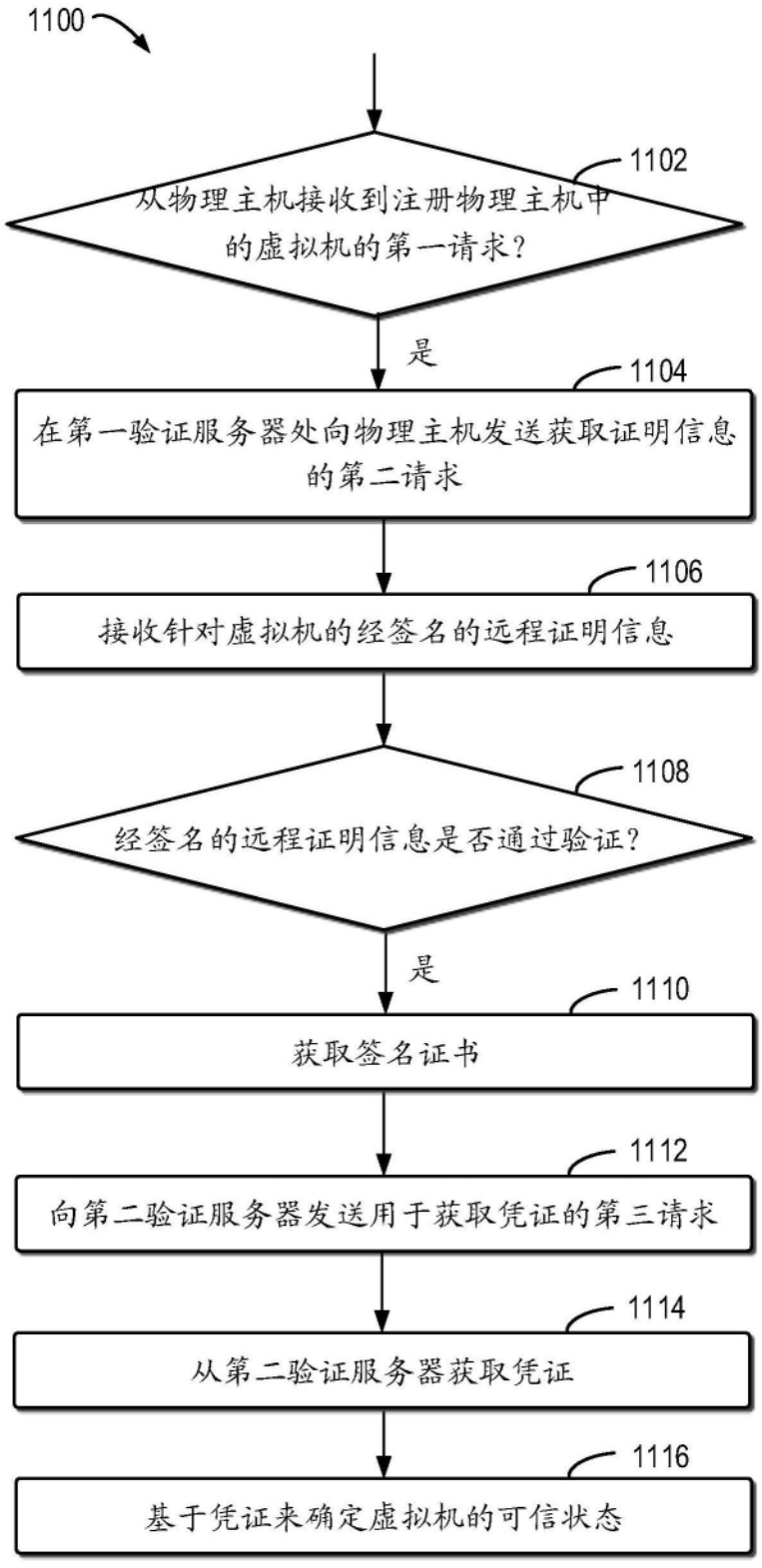

1100
1102
从物理主机接收到注册物理主机中的虚拟机的第一请求？
是
1104
在第一验证服务器处向物理主机发送获取证明信息的第二请求
1106
接收针对虚拟机的经签名的远程证明信息
1108
经签名的远程证明信息是否通过验证？
是
1110
获取签名证书
1112
向第二验证服务器发送用于获取凭证的第三请求
1114
从第二验证服务器获取凭证
1116
基于凭证来确定虚拟机的可信状态

图11

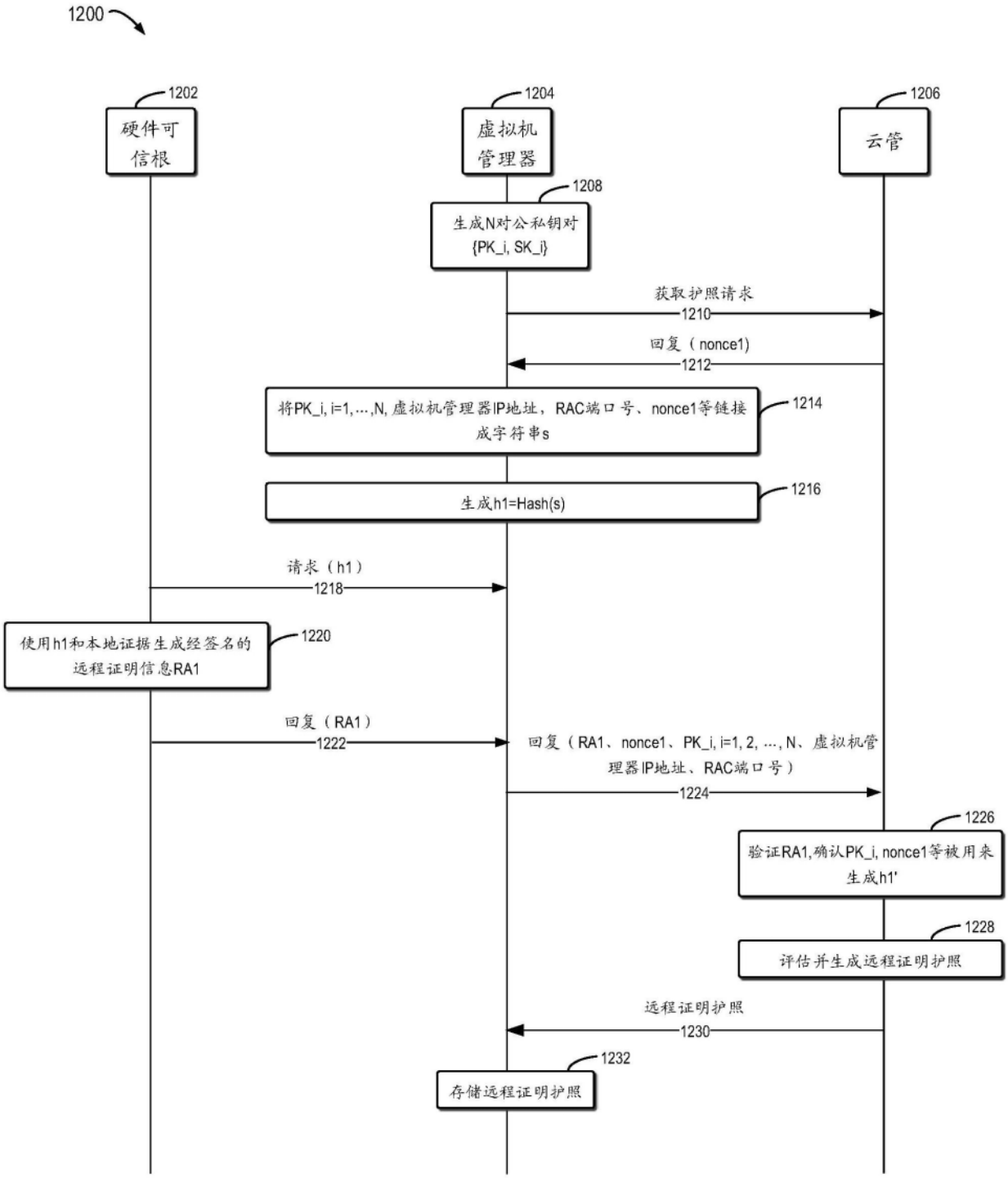

1200
1202
硬件可信根
1204
虚拟机管理器
1206
云管
1208
生成N对公私钥对{PK_i, SK_i}
获取护照请求
1210
回复（nonce1）
1212
将PK_i, i=1,...,N, 虚拟机管理器IP地址，RAC端口号、nonce1等链接成字符串s
1214
生成h1=Hash(s)
1216
请求（h1）
1218
使用h1和本地证据生成经签名的远程证明信息RA1
1220
回复（RA1）
1222
回复（RA1、nonce1、PK_i, i=1, 2, ..., N、虚拟机管理器IP地址、RAC端口号）
1224
1226
验证RA1,确认PK_i, nonce1等被用来生成h1'
1228
评估并生成远程证明护照
远程证明护照
1230
1232
存储远程证明护照

图12

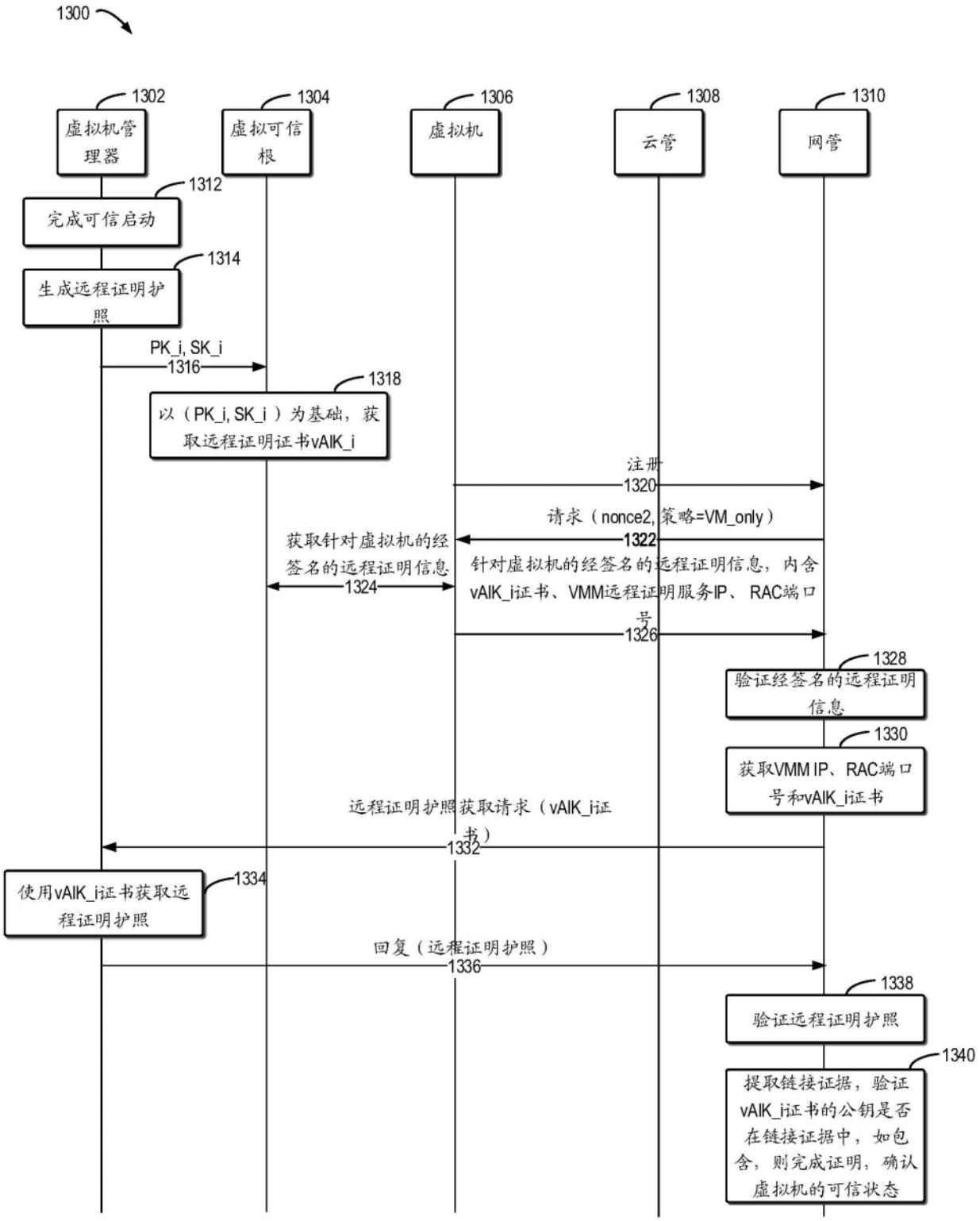

1300
1302
虚拟机管理器
1304
虚拟可信根
1306
虚拟机
1308
云管
1310
网管
1312
完成可信启动
1314
生成远程证明护照
PK_i, SK_i
1316
1318
以（PK_i, SK_i）为基础，获取远程证明证书vAIK_i
注册
1320
请求（nonce2, 策略=VM_only）
1322
获取针对虚拟机的经签名的远程证明信息
1324
针对虚拟机的经签名的远程证明信息，内含vAIK_i证书、VMM远程证明服务IP、RAC端口号
1326
1328
验证经签名的远程证明信息
1330
获取VMM IP、RAC端口号和vAIK_i证书
远程证明护照获取请求（vAIK_i证书）
1332
1334
使用vAIK_i证书获取远程证明护照
回复（远程证明护照）
1336
1338
验证远程证明护照
1340
提取链接证据，验证vAIK_i证书的公钥是否在链接证据中，如包含，则完成证明，确认虚拟机的可信状态

图13

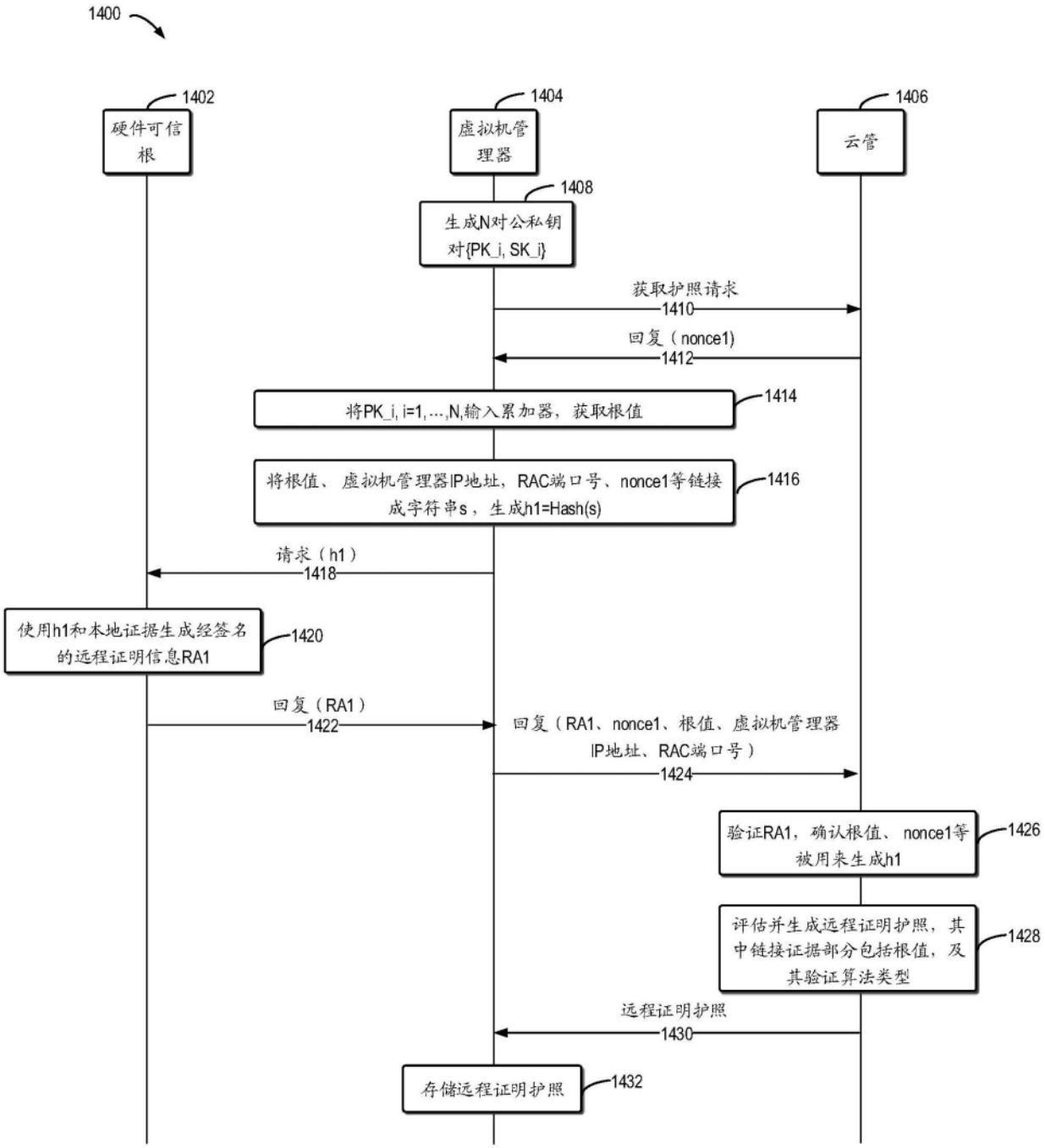

1400
1402
硬件可信根
1404
虚拟机管理器
1406
云管
1408
生成N对公私钥对{PK_i, SK_i}
获取护照请求
1410
回复（nonce1）
1412
将PK_i, i=1,…,N,输入累加器，获取根值
1414
将根值、虚拟机管理器IP地址，RAC端口号、nonce1等链接成字符串s，生成h1=Hash(s)
1416
请求（h1）
1418
使用h1和本地证据生成经签名的远程证明信息RA1
1420
回复（RA1）
1422
回复（RA1、nonce1、根值、虚拟机管理器IP地址、RAC端口号）
1424
验证RA1，确认根值、nonce1等被用来生成h1
1426
评估并生成远程证明护照，其中链接证据部分包括根值，及其验证算法类型
1428
远程证明护照
1430
存储远程证明护照
1432

图14

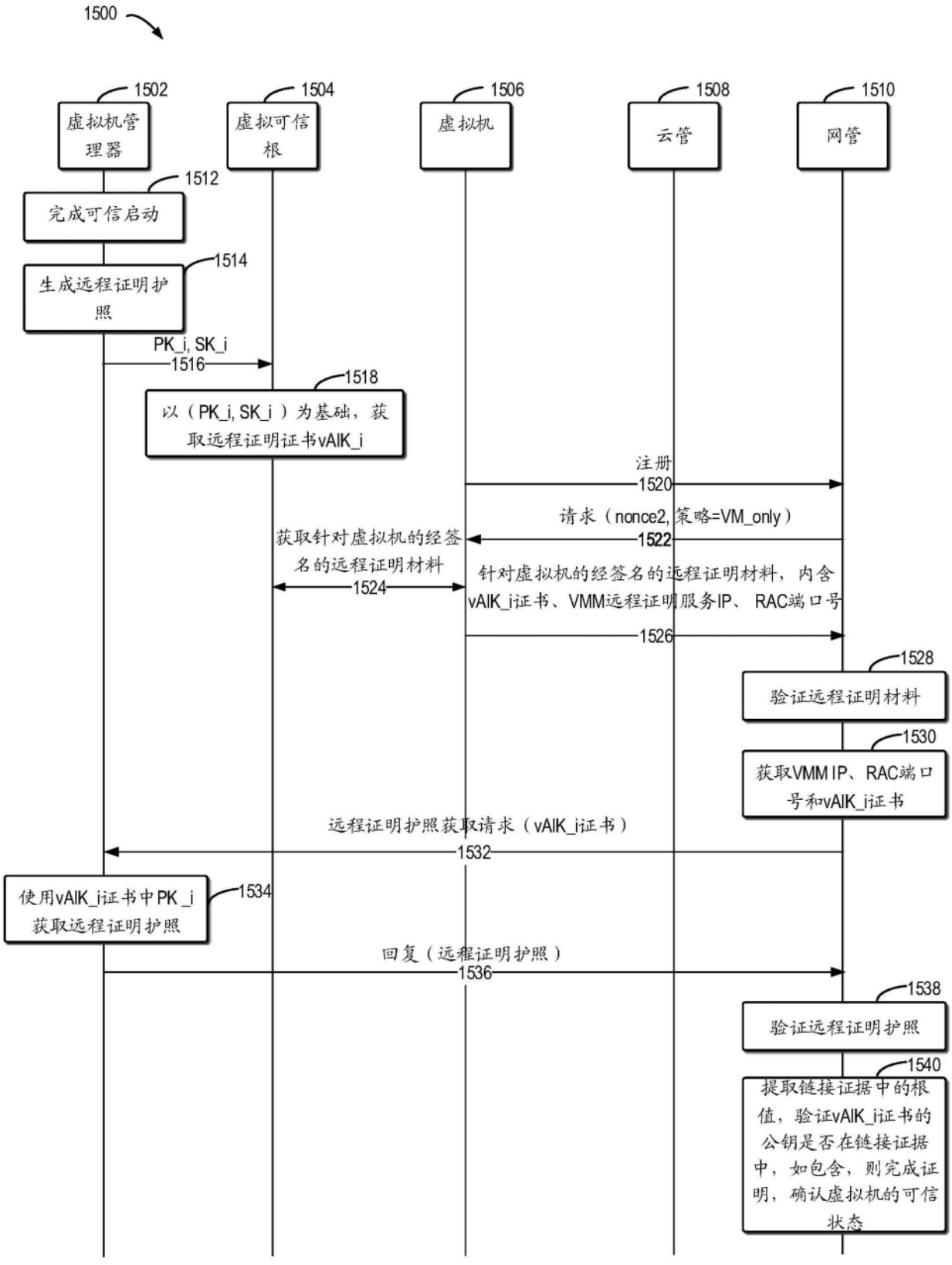

1500
1502
虚拟机管理器
1504
虚拟可信根
1506
虚拟机
1508
云管
1510
网管
1512
完成可信启动
1514
生成远程证明护照
PK_i, SK_i
1516
1518
以（PK_i, SK_i）为基础，获取远程证明证书vAIK_i
注册
1520
请求（nonce2, 策略=VM_only）
1522
获取针对虚拟机的经签名的远程证明材料
1524
针对虚拟机的经签名的远程证明材料，内含vAIK_i证书、VMM远程证明服务IP、 RAC端口号
1526
1528
验证远程证明材料
1530
获取VMM IP、RAC端口号和vAIK_i证书
远程证明护照获取请求（vAIK_i证书）
1532
使用vAIK_i证书中PK_i获取远程证明护照
1534
回复（远程证明护照）
1536
1538
验证远程证明护照
1540
提取链接证据中的根值，验证vAIK_i证书的公钥是否在链接证据中，如包含，则完成证明，确认虚拟机的可信状态

图15

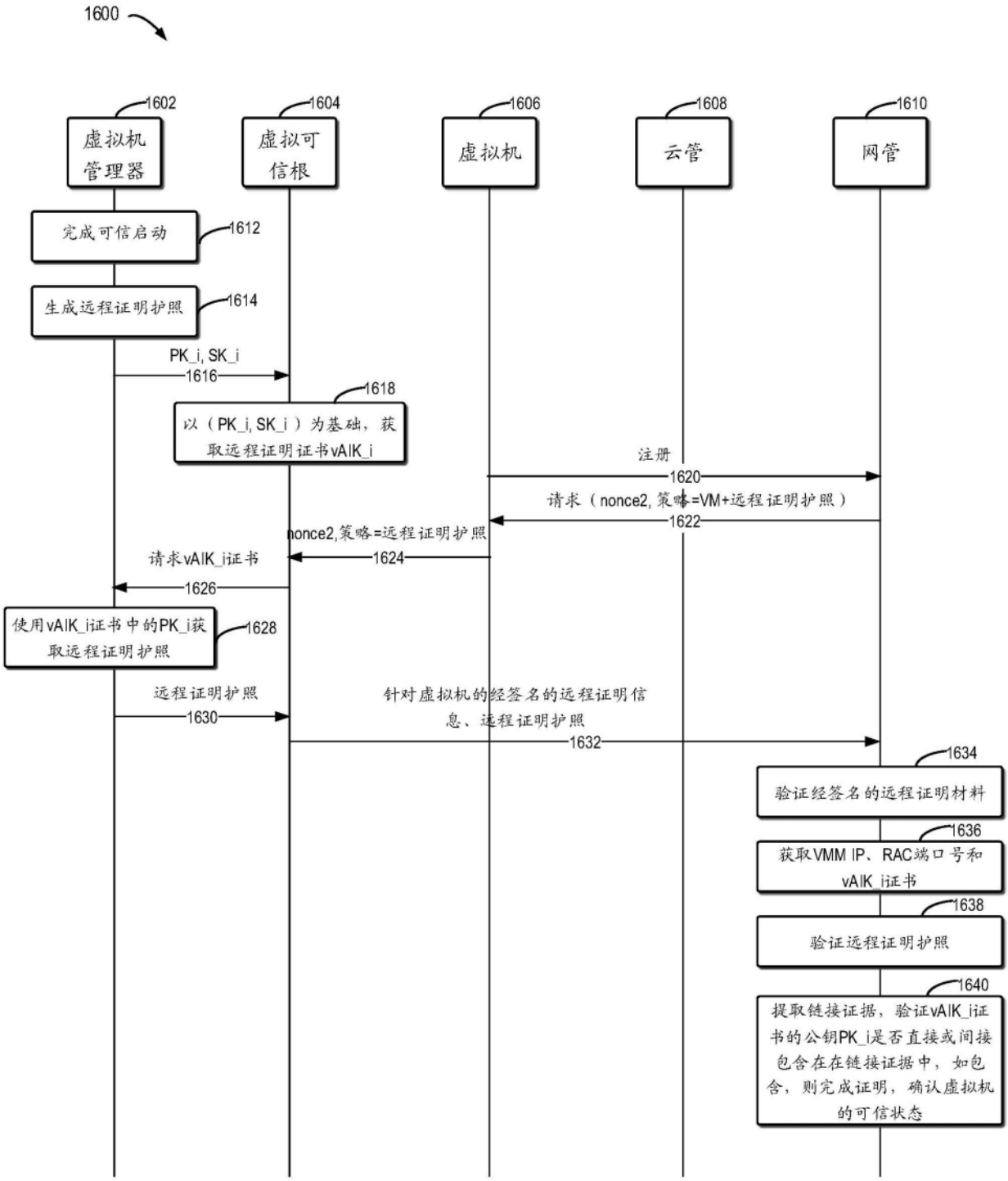

1600
1602
虚拟机管理器
1604
虚拟可信根
1606
虚拟机
1608
云管
1610
网管
完成可信启动
1612
生成远程证明护照
1614
PK_i, SK_i
1616
1618
以（PK_i, SK_i）为基础，获取远程证明证书vAIK_i
注册
1620
请求（nonce2, 策略=VM+远程证明护照）
1622
nonce2,策略=远程证明护照
1624
请求vAIK_i证书
1626
使用vAIK_i证书中的PK_i获取远程证明护照
1628
远程证明护照
1630
针对虚拟机的经签名的远程证明信息、远程证明护照
1632
1634
验证经签名的远程证明材料
1636
获取VMM IP、RAC端口号和vAIK_i证书
1638
验证远程证明护照
1640
提取链接证据，验证vAIK_i证书的公钥PK_i是否直接或间接包含在在链接证据中，如包含，则完成证明，确认虚拟机的可信状态

图16

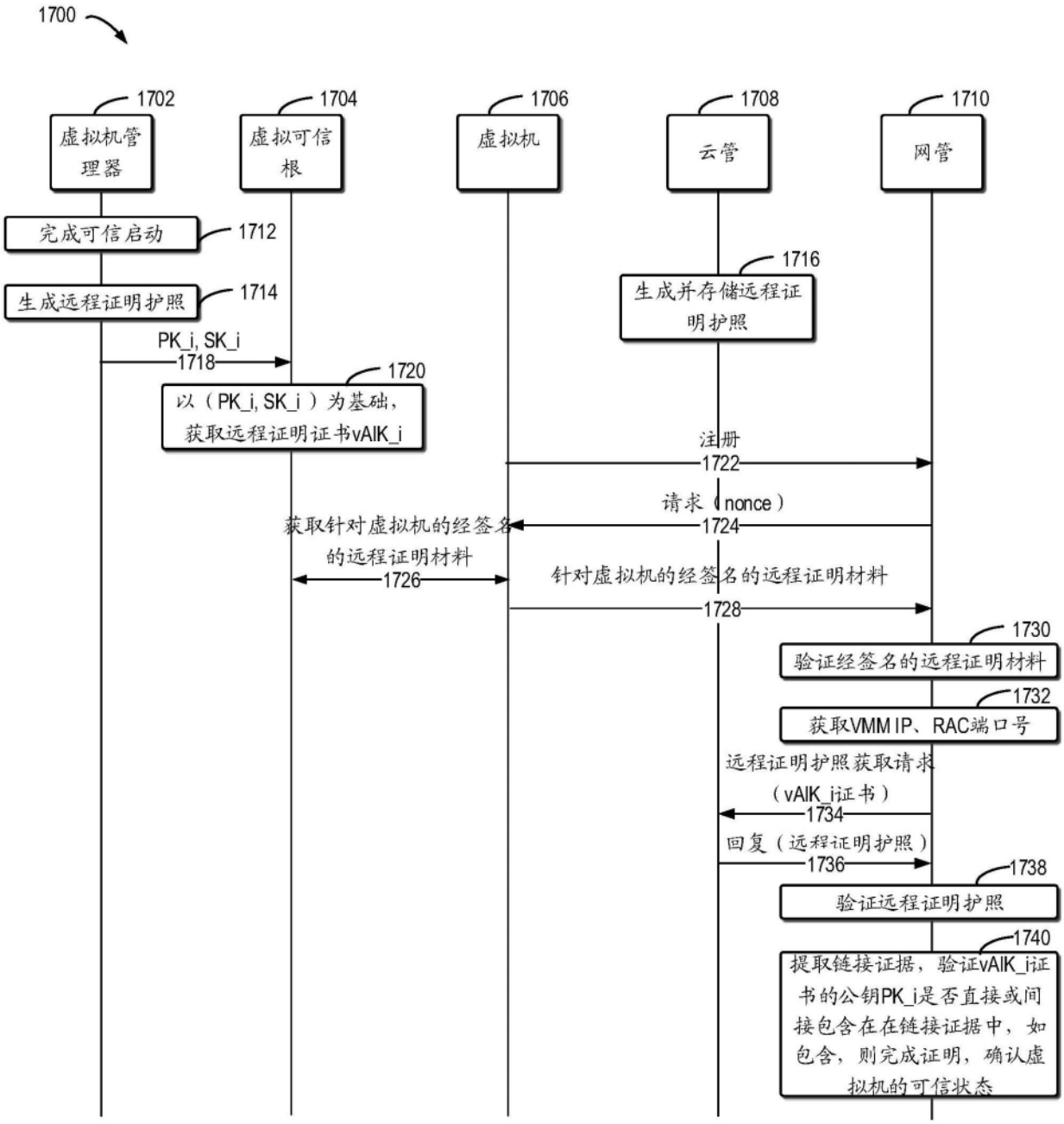

1700
1702
虚拟机管理器
1704
虚拟可信根
1706
虚拟机
1708
云管
1710
网管
完成可信启动
1712
生成远程证明护照
1714
PK_i, SK_i
1718
1720
以（PK_i, SK_i）为基础，获取远程证明证书vAIK_i
1716
生成并存储远程证明护照
注册
1722
请求（nonce）
1724
获取针对虚拟机的经签名的远程证明材料
1726
针对虚拟机的经签名的远程证明材料
1728
1730
验证经签名的远程证明材料
1732
获取VMM IP、RAC端口号
远程证明护照获取请求（vAIK_i证书）
1734
回复（远程证明护照）
1736
1738
验证远程证明护照
1740
提取链接证据，验证vAIK_i证书的公钥PK_i是否直接或间接包含在在链接证据中，如包含，则完成证明，确认虚拟机的可信状态

图17

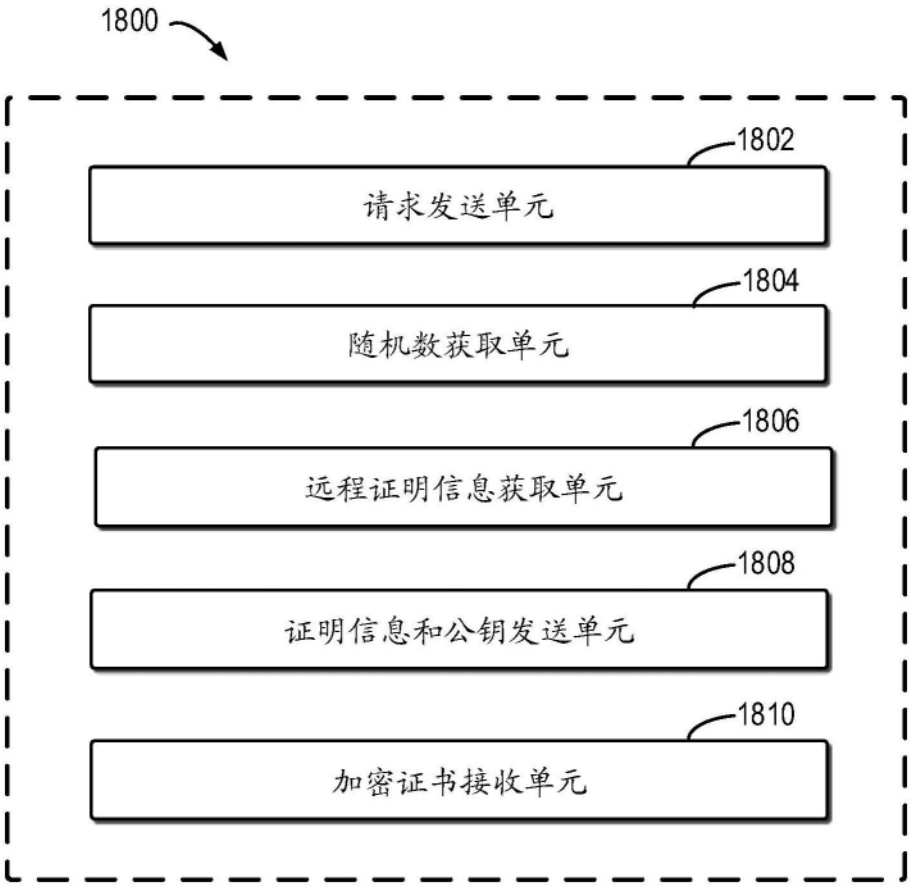

1800
1802
请求发送单元
1804
随机数获取单元
1806
远程证明信息获取单元
1808
证明信息和公钥发送单元
1810
加密证书接收单元

图18

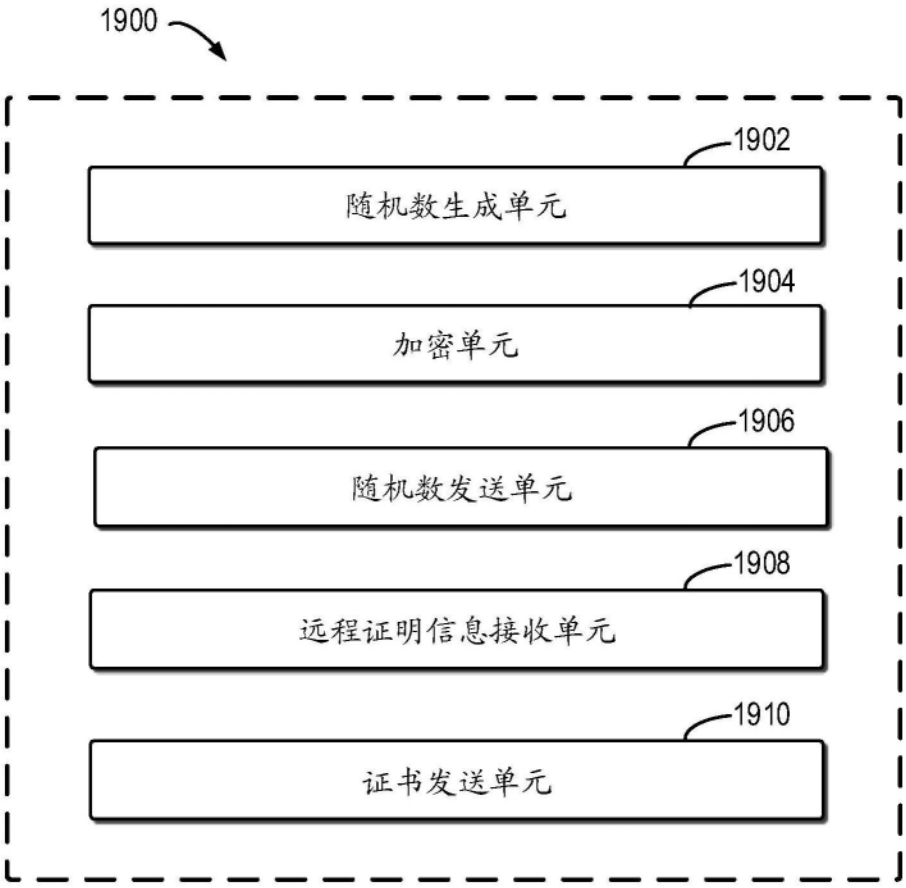

1900
1902
随机数生成单元
1904
加密单元
1906
随机数发送单元
1908
远程证明信息接收单元
1910
证书发送单元

图19

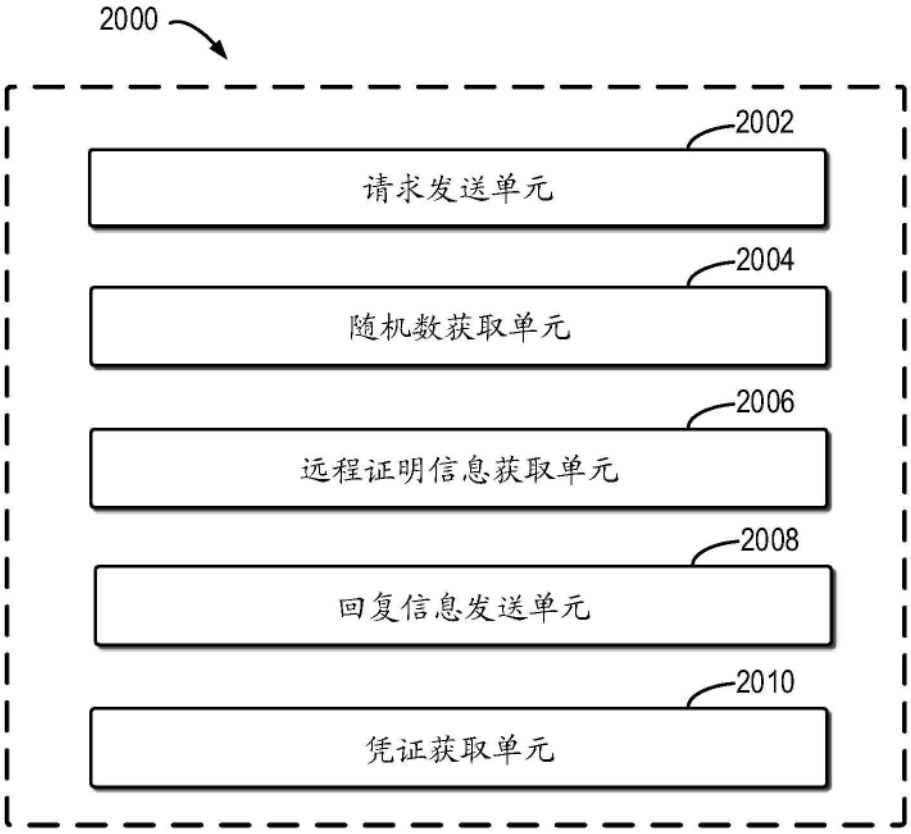

2000
2002
请求发送单元
2004
随机数获取单元
2006
远程证明信息获取单元
2008
回复信息发送单元
2010
凭证获取单元

图20

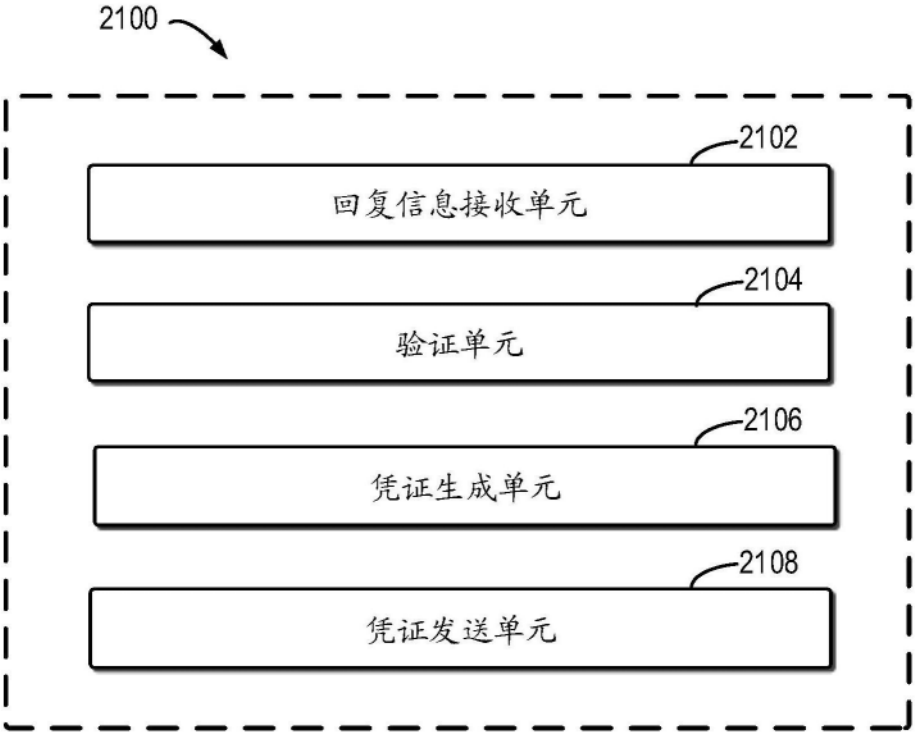

2100
2102
回复信息接收单元
2104
验证单元
2106
凭证生成单元
2108
凭证发送单元

图21

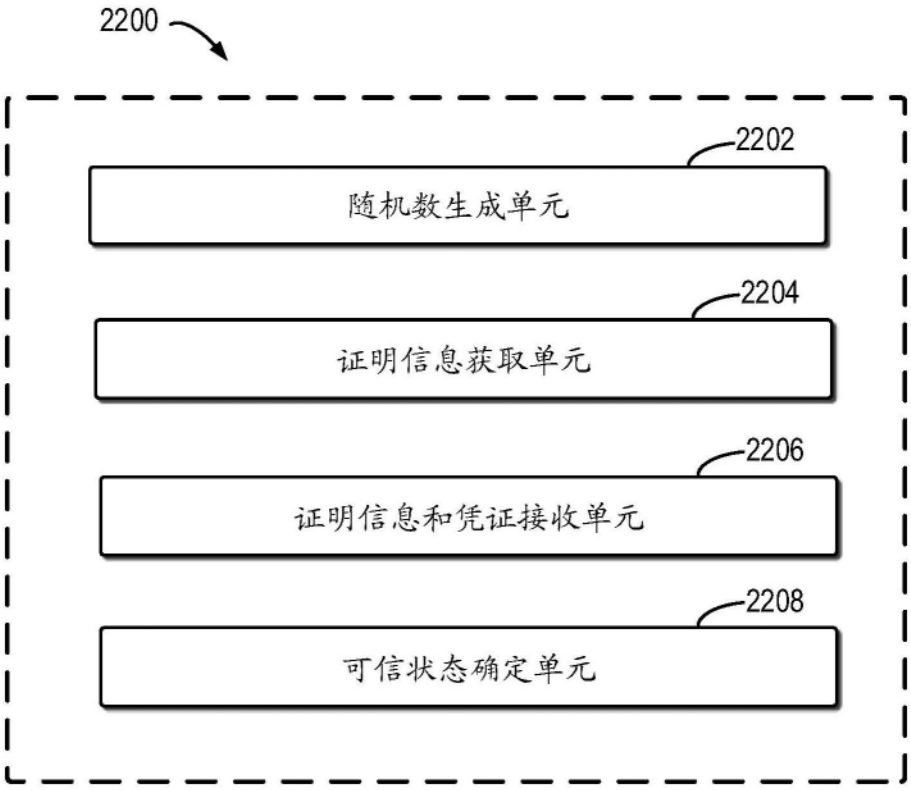

2200
2202
随机数生成单元
2204
证明信息获取单元
2206
证明信息和凭证接收单元
2208
可信状态确定单元

图22

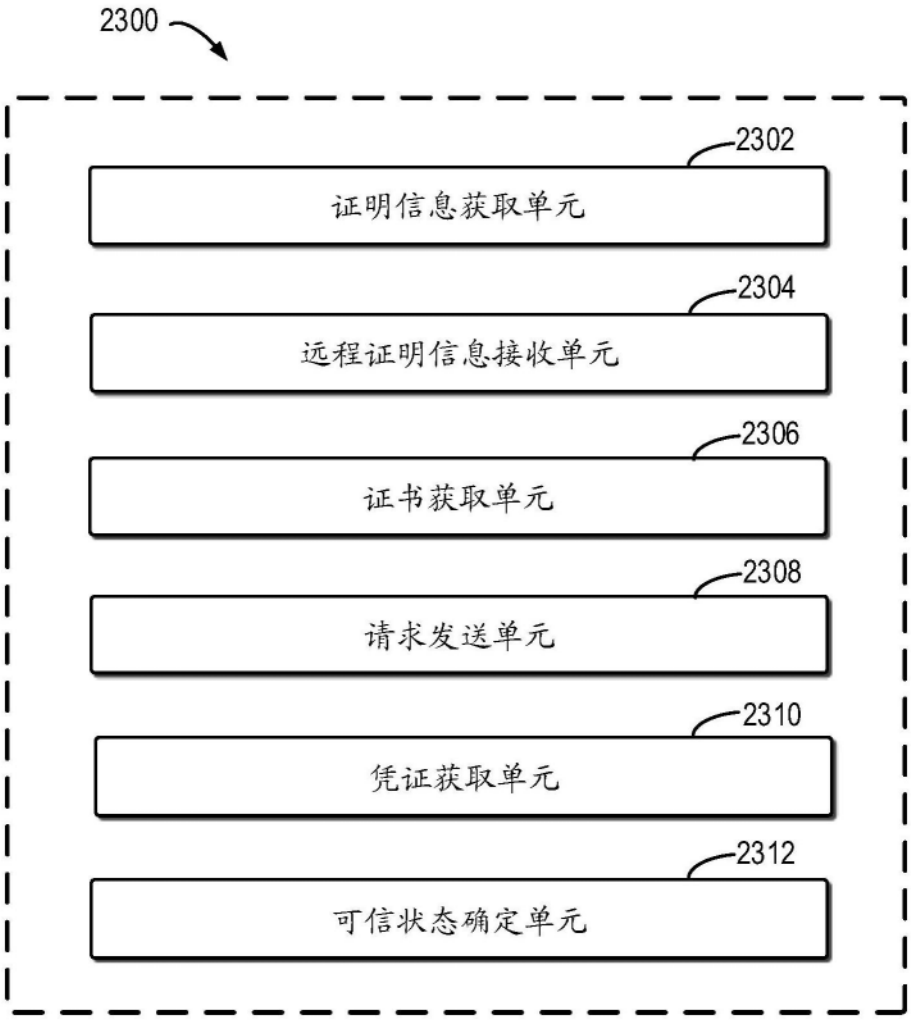

2300
2302
证明信息获取单元
2304
远程证明信息接收单元
2306
证书获取单元
2308
请求发送单元
2310
凭证获取单元
2312
可信状态确定单元

图23

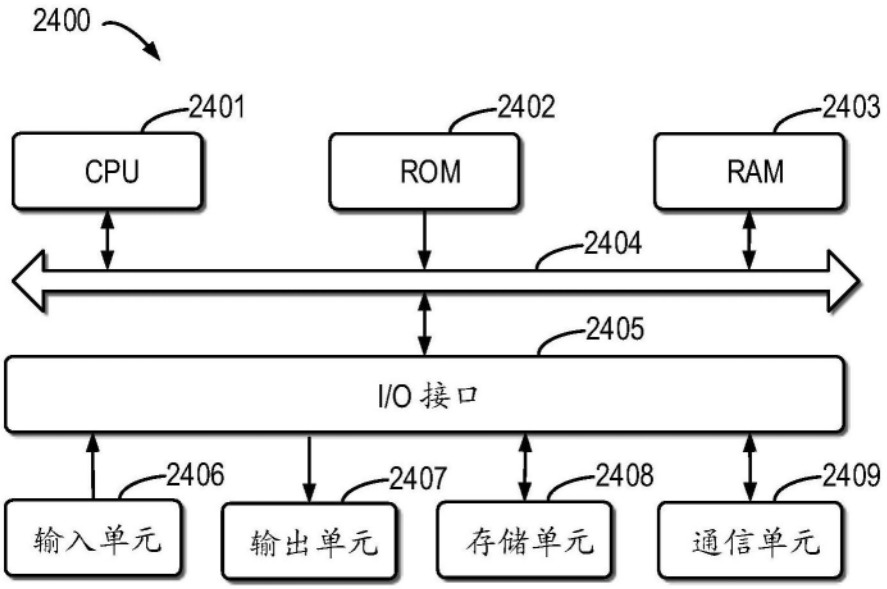

2400
2401
CPU
2402
ROM
2403
RAM
2404
2405
I/O 接口
2406
输入单元
2407
输出单元
2408
存储单元
2409
通信单元

图24