(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112464251 B
(45)授权公告日 2024.10.22

(21)申请号 202011547551.1

(22)申请日 2016.04.11

(65)同一申请的已公布的文献号
申请公布号 CN 112464251 A

(43)申请公布日 2021.03.09

(30)优先权数据
14/709170 2015.05.11 US

(62)分案原申请数据
201680027681.8 2016.04.11

(73)专利权人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 K.苏德 J.沃尔克

(74)专利代理机构 中国专利代理(香港)有限公司 72001
专利代理师 吕传奇

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 9/455(2018.01)
G06F 21/10(2013.01)
H04L 9/40(2022.01)

(56)对比文件
Omar等."Component integrity guarantees in software-defined networking infrastructure".017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN).2017, 292-296.

审查员 唐季超

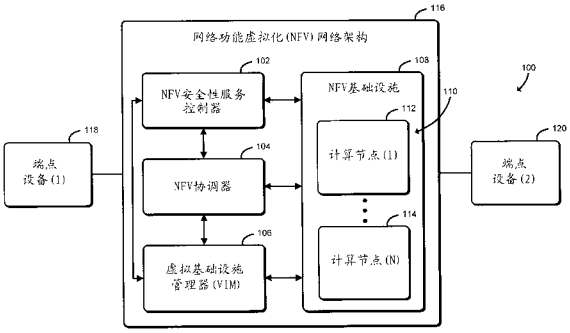
权利要求书3页 说明书23页 附图9页

(54)发明名称

用于虚拟网络功能的安全自举的技术

(57)摘要

用于在网络功能虚拟化(NFV)网络架构中自举虚拟网络功能的技术包括与VNF实例的VBS代理进行安全网络通信的虚拟网络功能(VNF)自举服务(VBS)。VBS代理被配置成在NFV网络架构中执行安全VNF自举捕获协议。相应地,VBS代理可以被配置成经由在VBS与VBS代理之间传送的安全通信向VBS进行登记。所述安全通信包括向VBS传送来自VNF实例在其上被实例化的平台的TEE的安全性引用和安全性凭证请求,以及响应于证实了安全性引用和安全性凭证请求而接收安全性凭证。此外还描述了并且要求保护其他的实施例。



CN 112464251 B

1.一种用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,所述NFV网络系统包括:

硬件处理器;

VNF自举服务VBS;

与VNF实例相关联的VBS代理;以及

管理程序,其中所述管理程序用以:(i)接收用以创生VNF实例的命令,所述命令包括一个启动参数的集合;(ii)验证所接收命令的真实性;(iii)根据启动参数实例化VNF实例(iv)向受信任执行环境TEE登记实例化的VNF实例,以及

其中,所述VBS代理响应于所述VNF实例的实例化被发起,所述VBS代理用以:(i)生成VNF公共/私有密钥对,(ii)使用公共/私有密钥对的VNF公共密钥从TEE请求证实引用,其中所述请求可用于使用TEE的私有密钥计算引用散列并对引用散列进行签名,(iii)响应于已从TEE接收到签名的引用散列,执行与VBS的VBS捕获协议,以将VBS代理与VBS安全地绑定,(iv)激活VNF实例,以及(v)向NFV网络系统的VNF管理器传送指示,指示VNF实例已被激活。

2.根据权利要求1所述的用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,所述NFV网络系统还包括NFV安全控制器,并且其中,所述VBS形成所述NFV安全控制器的一部分。

3.根据权利要求1所述的用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,所述启动参数包括所述VBS的公有密钥、所述VBS的互联网协议IP地址、所述VNF实例的独有标识符,以及所述NFV基础设施平台的独有标识符。

4.根据权利要求1所述的用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,所述VBS还向VIM传送所述启动参数,并且其中,响应于已接收到所述VBS启动参数,所述VIM传送用于所述管理程序创生所述VNF实例的命令。

5.根据权利要求1所述的用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,向所述TEE登记所述实例化的VNF实例包括向所述TEE登记所述启动参数。

6.根据权利要求1所述的用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,其中,所述TEE用以安全地供应所述VBS。

7.根据权利要求6所述的用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,通过所述TEE安全地供应所述VBS包括使用所述TEE与所述VBS之间的带外信道来安全地供应所述VBS。

8.根据权利要求1所述的用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,验证所接收命令的真实性包括所述管理程序验证所述VNF的一个或多个签名。

9.根据权利要求8所述的用于安全地自举虚拟网络功能VNF的网络功能虚拟化NFV网络系统,验证所述VNF的一个或多个签名包括验证所述VNF的签名图像和所述VNF的签名描述符中的至少一个。

10.一种或多种非暂时性机器可读存储介质,包括存储在其上的多个指令,所述多个指令在执行时致使网络功能虚拟化NFV网络系统执行以下操作:

通过NFV网络系统的管理程序接收用以创生自举虚拟网络功能VNF实例的命令,所述命令包括一个启动参数的集合;

通过所述NFV网络系统的管理程序验证所接收命令的真实性;

通过所述NFV网络系统的管理程序根据启动参数实例化VNF实例;

向所述NFV网络系统的受信任执行环境TEE登记实例化的VNF实例;

响应于VNF实例的实例化,通过VNF自举服务VBS代理生成VNF公共/私有密钥对;

通过VBS代理使用公共/私有密钥对的VNF公共密钥从TEE请求证实引用,其中所述请求可用于使用TEE的私有密钥计算引用散列并对引用散列进行签名;

通过所述VBS代理并响应于已从TEE接收到签名的引用散列,执行VBS捕获协议,以将VBS代理与相关联的VBS安全地绑定;

激活VNF实例;以及

向NFV网络系统的VNF管理器传送指示,指示VNF实例已被激活。

11.根据权利要求10所述的一种或多种非暂时性机器可读存储介质,所述启动参数包括所述VBS的公有密钥、所述VBS的互联网协议IP地址、所述VNF实例的独有标识符,以及所述NFV基础设施平台的独有标识符。

12.根据权利要求10所述的一种或多种非暂时性机器可读存储介质,所述多个指令在执行时还致使所述NFV网络系统通过所述TEE安全地供应所述VBS,其中通过所述TEE安全地供应所述VBS包括使用所述TEE与所述VBS之间的带外信道来安全地供应所述VBS。

13.根据权利要求10所述的一种或多种非暂时性机器可读存储介质,其中验证所接收命令的真实性包括验证VNF的签名图像和所述VNF的签名描述符中的至少一个。

14.一种用于安全自举虚拟网络功能VNF的方法,所述方法包括:

通过网络功能虚拟化NFV网络系统的管理程序接收用以创生VNF实例的命令,所述命令包括一个启动参数的集合;

通过所述NFV网络系统的管理程序验证所接收命令的真实性;

通过所述NFV网络系统的管理程序根据启动参数实例化VNF实例;

向所述NFV网络系统的受信任执行环境TEE登记实例化的VNF实例;

响应于VNF实例的实例化,通过VNF自举服务VBS代理生成VNF公共/私有密钥对;

通过VBS代理使用公共/私有密钥对的VNF公共密钥从TEE请求证实引用,其中所述请求可用于使用TEE的私有密钥计算引用散列并对引用散列进行签名;

通过所述VBS代理并响应于已从TEE接收到签名的引用散列,执行VBS捕获协议,以将VBS代理与相关联的VBS安全地绑定;

通过所述VBS代理激活VNF实例;并且

通过所述VBS代理向NFV网络系统的VNF管理器传送指示,指示VNF实例已被激活。

15.根据权利要求14所述的方法,所述启动参数包括所述VBS的公有密钥、所述VBS的互联网协议IP地址、所述VNF实例的独有标识符,以及所述NFV基础设施平台的独有标识符。

16.根据权利要求14所述的方法,还包括通过所述TEE安全地供应所述VBS,其中通过所述TEE安全地供应所述VBS包括使用所述TEE与所述VBS之间的带外信道来安全地供应所述VBS。

17.根据权利要求14所述的方法,验证所述VNF的一个或多个签名包括验证所述VNF的签名图像和所述VNF的签名描述符中的至少一个。

18.一种用于安全自举虚拟网络功能VNF的设备,所述设备包括:

用于接收用以创生VNF实例的命令,所述命令包括一个启动参数的集合的装置;

用于验证所接收命令的真实性的装置;

用于根据启动参数实例化VNF实例的装置;

用于向所述NFV网络系统的受信任执行环境TEE登记实例化的VNF实例的装置;

用于响应于VNF实例的实例化,生成VNF公共/私有密钥对的装置;

用于使用公共/私有密钥对的VNF公共密钥从TEE请求证实引用,其中所述请求可用于使用TEE的私有密钥计算引用散列并对引用散列进行签名的装置;

用于响应于已从TEE接收到签名的引用散列,执行VBS捕获协议,以将VBS代理与相关联的VBS安全地绑定的装置;

用于激活VNF实例的装置;以及

用于向NFV网络系统的VNF管理器传送指示,指示VNF实例已被激活的装置。

19.根据权利要求18所述的设备,所述启动参数包括所述VBS的公有密钥、所述VBS的互联网协议IP地址、所述VNF实例的独有标识符,以及所述NFV基础设施平台的独有标识符。

20.根据权利要求18所述的设备,还包括用于安全地供应所述VBS的装置,其中用于安全地供应所述VBS的装置包括用于使用所述TEE与所述VBS之间的带外信道来安全地供应所述VBS的装置。

21.根据权利要求18所述的设备,用于验证所述VNF的一个或多个签名的装置包括用于验证所述VNF的签名图像和所述VNF的签名描述符中的至少一个的装置。

用于虚拟网络功能的安全自举的技术

[0001] 相关申请的交叉引用

[0002] 本申请是申请号:201680027681.8发明名称:用于虚拟网络功能的安全自举的技术的分案申请。本申请要求2015年5月11日提交的标题为“TECHNOLOGIES FOR SECURE BOOTSTRAPPING OF VIRTUAL NETWORK FUNCTIONS(用于虚拟网络功能的安全自举的技术)”的美国实用专利申请序列号14/709,170的优先权。

背景技术

[0003] 网络运营商和服务提供商通常依赖于各种网络虚拟化技术来管理复杂的大规模计算环境,大规模计算环境诸如高性能计算(HPC)和云端计算环境。举例来说,网络运营商和服务提供商的网络可以依赖于网络功能虚拟化(NFV)部署来部署网络服务(例如防火墙服务、网络地址翻译(NAT)服务、负载平衡服务、深度分组检测(DPI)服务、传输控制协议(TCP)优化服务等等)。这样的NFV部署通常使用NFV基础设施来协调(例如在商品服务器中的)各种虚拟机(VM)和/或容器以对网络业务执行通常被称作虚拟化网络功能(VNF)的虚拟化网络服务,并且跨越各种VM和/或容器管理网络业务。

[0004] 不同于传统的非虚拟化的部署,虚拟化的部署把网络功能与底层硬件去耦合,这得到高度动态的并且通常能够被在具有通用处理器的市售服务器上执行的网络功能和服务。因此,在必要时可以基于要对网络业务执行的特定功能或网络服务对VNF进行横向缩容(scale-in)/扩容(scale-out)。此外,可以按照每个订户的需求跨地域、在受主控的基础设施上部署VNF等等。

附图说明

[0005] 将作为举例而非限制在附图中说明本文中所描述的概念。为了说明的简明和清晰起见,在附图中示出的各个单元不一定是按比例绘制的。在认为适当的情况下在各幅图当中重复了附图标记以表明相应的或类似的元件。

[0006] 图1是用于在网络功能虚拟化(NFV)网络架构处对网络通信进行处理的系统的至少一个实施例的简化框图,所述系统包括NFV基础设施的一个或多个计算节点;

[0007] 图2是图1的系统的其中一个计算节点的至少一个实施例的简化框图;

[0008] 图3是图1的系统的端点设备的至少一个实施例的简化框图;

[0009] 图4是图1的系统的NFV网络架构的至少一个实施例的简化框图;

[0010] 图5是图1和4的NFV安全性服务控制器的环境的至少一个实施例的简化框图;

[0011] 图6是图4的NFV网络架构的虚拟网络功能(VNF)实例的环境的至少一个实施例的简化框图;

[0012] 图7是可以由图5的NFV安全性服务控制器执行的用于初始化安全VNF自举的方法的至少一个实施例的简化流程图;

[0013] 图8是用于安全地自举图4的NFV网络架构的其中一个VNF实例的通信流的至少一个实施例的简化流程图;

[0014] 图9是可以由图6的VNF实例的VNF自举服务(VBS)代理执行的用于执行安全VNF自举捕获协议的方法的至少一个实施例的简化流程图;

[0015] 图10是用于在图4的NFV网络架构的其中一个VNF实例处执行安全VNF自举捕获协议的通信流的至少一个实施例的简化流程图;以及

[0016] 图11是可以由图4的NFV网络架构的其中一个平台的受信任执行环境(TEE)执行的用于实施TEE引用(quoting)操作的方法的至少一个实施例的简化流程图。

具体实施方式

[0017] 虽然本公开内容的概念可以有多种修改和替换形式,但是其具体实施例在附图中作为举例示出了并且在本文中进行详细描述。但是应当理解的是,并不意图把本公开内容的概念限制到所公开的特定形式,而是相反意图涵盖与本公开和所附权利要求一致的所有修改、等效方案和替换方案。

[0018] 在说明书中对“一个实施例”、“实施例”、“说明性实施例”等等的引用表明所描述的实施例可以包括特定的特征、结构或特性,但是每一个实施例可以或者可以不必包括该特定的特征、结构或特性。此外,这样的短语不一定指代相同的实施例。此外,当结合某一实施例描述特定的特征、结构或特性时,所主张认为的是:与不管是否被明确描述的其他实施例相结合地来实现这样的特征、结构或特性是落在本领域技术人员的知识范围之内的。此外还应当理解到,包括在“A、B和C的至少其中之一”形式的列表中的项目可以意味着:(A);(B);(C);(A和B);(A和C);(B和C);或者(A、B和C)。类似地,采用“A、B或C的至少其中之一”形式列出的项目可以意味着:(A);(B);(C);(A和B);(A和C);(B和C);或者(A、B和C)。

[0019] 在某些情况下,所公开的实施例可以采用硬件、固件、软件或者其任意组合来实施。所公开的实施例还可以被实施成由一个或多个瞬时性或非瞬时性机器可读(例如计算机可读)存储介质携带或者存储在其上的指令,所述指令可以由一个或多个处理器读取并执行。机器可读存储介质可以被具体实现成任何存储设备、机构或者用于存储或传送采用机器可读取的形式的信息的其他物理结构(例如易失性或非易失性存储器、介质盘或者其他介质设备)。

[0020] 在附图中,一些结构或方法特征可能是按照具体的安排和/或排序而示出的。但是应当理解到,可能并不需要这样的具体安排和/或排序。在一些实施例中,反而可以按照不同于在说明性附图中所示出的方式和/或次序来安排这样的特征。此外,在特定附图中包括结构或方法特征并不意味着隐含在所有实施例中都需要这样的特征,并且在一些实施例中可以不包括这样的特征或者可以将其与其他特征相组合。

[0021] 现在参照图1,在说明性实施例中,用于在网络功能虚拟化(NFV)网络架构116处对网络业务进行处理的系统100包括若干网络处理组件,若干网络处理组件包括NFV协调器104、虚拟基础设施管理器(VIM)106和NFV基础设施108。此外,NFV网络架构116包括NFV安全性服务控制器102,用于在NFV网络架构116上管理和施行(enforce)安全性监测和安全消息传输(例如设立安全通信信道、对跨越安全通信信道传送的消息进行认证、维护安全通信信道的安全性等等)。作为NFV网络架构116的虚拟网络功能(VNF)实例的初始化处理的一部分,NFV安全性服务控制器102向NFV基础设施108的先前实例化的VNF实例提供安全消息,安全消息指示该VNF实例例执行安全自举。为了这样做,NFV安全性服务控制器102包括VNF自

举服务(参见图4),并且VNF实例包括负责实施安全自举以及传送/接收消息的VNF自举服务(VBS)代理(参见图4)。相应地,VNF实例可以使用VBS代理向NFV安全性服务控制器102登记为可操作的VNF实例并且接收VNF自举信息(诸如启动策略、配置信息),并且安全地登记为可操作的VNF实例。此外,在一些实施例中,VBS代理可以启用VNF实例许可授予和施行。

[0022] NFV网络架构116的网络处理和安全性监测组件可以被部署在各种虚拟化网络架构中,各种虚拟化网络架构诸如虚拟演进型分组核心(vEPC)基础设施、虚拟化顾客处所装备(vCPE)基础设施或者任何其他类型的运营商虚拟化基础设施。应当认识到,取决于NFV网络架构116被部署在其中的网络架构,NFV网络架构116可以包括一个或多个NFV安全性服务控制器102、一个或多个NFV协调器104、一个或多个VIM 106和/或一个或多个NFV基础设施108。还应当认识到,在一些实施例中,NFV安全性服务控制器102可以与NFV协调器104和/或VIM 106位于同一处,诸如在NFV管理和协调(MANO)架构框架中。

[0023] NFV基础设施108包括一个或多个计算节点110,一个或多个计算节点110能够管理(例如创建、移动、破坏等等)被配置成作为VNF实例运行的(例如在商品服务器中的)若干个VM和/或容器。每一个VNF实例通常依赖于一个或多个VM,所述VM可能正在运行不同的软件和/或进程以便对网络业务实施网络服务(例如防火墙服务、网络地址翻译(NAT)服务、负载平衡服务、深度分组检测(DPI)服务、传输控制协议(TCP)优化服务等等)。此外,为了提供某些网络服务,多个VNF实例可以被创建为服务功能链或VNF转发图(也就是为了实施所期望的网络服务而被以有序序列实施的一系列VNF实例)。

[0024] NFV安全性服务控制器102可以被具体实现为或者通过其他方式包括能够实施本文中所描述的功能的任何类型的硬件、软件和/或固件。正如后面将更加详细地描述的那样,NFV安全性服务控制器102被配置成充当安全性监测协调器。为了这样做,NFV安全性服务控制器102被配置成向遍及NFV网络架构116的组件(例如位于NFV网络架构116中的VNF实例)传送包括各种监测规则的安全性监测策略,各种监测规则包括安全通信路径策略、配置参数以及功能描述符。各种安全性功能可以包括但不限于:确保服务功能链(SFC)供应的安全,施行SFC安全性配置和监测,提供受到机密性保护的令牌,管理受保护策略传输,以及提供VNF间SFC路径保护。

[0025] 为了获取和/或更新安全性监测策略,NFV安全性服务控制器102可以被配置成与一个或多个外部安全性系统(例如Intel®安全性控制器)、安全性数据库和/或安全性策略引擎对接。为了与外部安全性系统进行通信,NFV安全性服务控制器102可以向外部安全服务协调系统递送应用编程器接口(API)和/或安全性策略。在一些实施例中,NFV安全性服务控制器102可以充当受信任第三方以便对跨越NFV网络架构116的各种网络和安全性监测组件的消息进行认证。应当认识到,在一些实施例中,NFV安全性服务控制器102可以具有高于NFV网络架构116的其他网络和安全性监测组件的安全性特权,以便确保NFV安全性服务控制器102的完整性和安全性。

[0026] NFV协调器104可以被具体实现为或者通过其他方式包括能够实施本文中所描述的功能的任何类型的硬件、软件和/或固件,本文中所描述的功能诸如经由VNF管理器(参见图4)管理VNF实例的生命周期(例如实例化、横向扩容/缩容、性能测量、事件相关、终止等等),管理全局资源,对NFV基础设施108的资源请求进行验证和授权,新的VNF实例的加载(on-boarding),和/或者管理对VNF实例的各种策略和封包。举例来说,NFV协调器104可以

被配置成接收来自影响特定VNF的网络运营商的资源请求。在使用中,NFV协调器104基于运营商请求管理任何适用的处理、存储和/或网络配置调节,以便使VNF进入操作中或者使其遵从资源请求。一旦处于操作中,NFV协调器104可以监测VNF的容量和利用率,所述容量和利用率在必要时可以由NFV协调器104进行调节。

[0027] VIM 106可以被具体实现为或者通过其他方式包括能够实施本文中所描述的功能的任何类型的硬件、软件和/或固件。VIM 106被配置成诸如在一个运营商的基础设施子域内控制并且管理NFV基础设施108的计算、存储和网络资源(例如物理和虚拟资源)。此外,VIM 106被配置成收集并转发与VIM 106有关的各种信息,诸如性能测量和事件。

[0028] NFV基础设施108可以被具体实现为或者通过其他方式包括任何类型的虚拟和/或物理处理和存储资源(诸如一个或多个服务器或其他计算节点)以及虚拟化软件。举例来说,说明性的NFV基础设施108包括一个或多个计算节点110。说明性的计算节点110包括第一计算节点,第一计算节点被标示为计算节点(1)112,并包括第二计算节点,第二计算节点被标示为计算节点(N)114(也就是计算节点110当中的“第N个”计算节点,其中“N”是正整数并且标示一个或多个附加的计算节点110)。

[0029] 每一个计算节点110可以被具体实现为能够实施本文中所描述的功能的任何类型的计算或计算机设备,任何类型的计算或计算机设备包括但不限于服务器(例如独立式服务器、机架安放服务器、刀片式服务器等等)、网络电器(例如物理或虚拟电器)、高性能计算设备、web电器、分布式计算系统、计算机、基于处理器的系统、多处理器系统、智能电话、平板计算机、膝上型计算机、笔记本计算机和/或移动计算设备。如图2中所示,在一个实施例中,每一个计算节点110说明性地包括处理器202、输入/输出(I/O)子系统206、存储器208、数据存储设备214、安全时钟216以及通信电路218。当然,计算节点110在其他实施例中可以包括其他或附加的组件,诸如通常在服务器中所见到的那些组件(例如各种输入/输出设备)。此外,在一些实施例中,其中一个或多个说明性组件可以被合并在另一个组件中或者通过其他方式形成另一个组件的一部分。举例来说,存储器208或者其部分在一些实施例中可以被合并在处理器202中。

[0030] 处理器202可以被具体实现为能够实施本文中所描述的功能的任何类型的处理器。举例来说,处理器202可以被具体实现为单核或多核处理器、数字信号处理器、微控制器或者其他处理器或处理/控制电路。说明性的处理器202包括一项或多项受信任执行环境(TEE)支持204或者安全飞地(secure enclave)支持,所述支持可以被计算节点110在建立受信任执行环境过程中加以利用。应当认识到,在一些实施例中,TEE支持204为受信任执行环境提供硬件加强的安全性,在受信任执行环境中正在执行的代码可以被测量、验证或者通过其他方式被确定为是真实可靠的。举例来说,TEE支持204可以被具体实现为Intel®软件防护扩展(SGX)技术。虽然TEE支持204被说明性地示出在处理器202中,但是应当认识到,在一些实施例中,计算节点110的其中一个或多个其他组件可以包括TEE支持204。此外,在一些实施例中,计算节点110的处理器202可以包括安全性引擎(例如后面所讨论的安全性引擎224)、可管理性引擎或者安全性协处理器,其被配置成利用TEE支持204来建立受信任执行环境。

[0031] 存储器208可以被具体实现为能够实施本文中所描述的功能的任何类型的易失性或非易失性存储器或数据存储装置。在操作中,存储器208可以存储在计算节点110的操作

期间所使用的各种数据和软件,诸如操作系统、应用、程序、库以及驱动程序。存储器208经由I/O子系统206可通信地耦合到处理器202,所述I/O子系统206可以被具体实现为促进利用计算节点110的处理器202、存储器208以及其他组件进行的输入/输出操作的电路和/或组件。举例来说,I/O子系统206可以被具体实现为或者通过其他方式包括存储器控制器集线器、输入/输出控制集线器、固件设备、通信链路(也就是点对点链路、总线链路、导线、电缆、光导、印刷电路板迹线等等)和/或用以促进输入/输出操作的其他组件和子系统。

[0032] 说明性的存储器208包括安全存储器210。在一些实施例中,安全存储器210可以被具体实现为存储器208的安全分区;而在其他实施例中,安全存储器210可以被具体实现为计算节点110的单独硬件组件或者被包括在计算节点110的单独硬件组件上。正如本文中所描述的那样,安全存储器210可以存储被供应给计算节点110的各种数据。举例来说,安全存储器210可以存储可以由芯片组和/或受信任执行环境的制造商供应的计算节点110的安全密钥(所述安全密钥例如证实密钥、私有直接匿名证实(DAA)密钥、增强隐私标识(EPID)密钥或者任何其他类型的安全/密码密钥)。安全存储器210还可以存储例如由计算节点110的原始装备制造商(OEM)供应在其中的计算节点110的口令、PIN或其他独有标识符。当然应当认识到,安全存储器210可以存储取决于特定实施例的各种其他数据(例如群组名称、设备标识符、白名单、预期PIN值等等)。在一些实施例中,所供应的数据可以被存储在安全存储器210的只读存储器中。

[0033] 说明性的存储器208还附加地包括基本输入/输出系统(BIOS)212。BIOS 212包括用以在引导处理期间初始化计算节点110的指令(例如在计算节点110的引导期间使用的BIOS驱动程序)。在一些实施例中,计算节点110可以通过主平台固件或预引导(pre-boot)固件(诸如基于统一可扩展固件接口(“UEFI”)规范(所述规范具有由统一EFI论坛公布的几个版本)的Intel ® 平台芯片组或平台BIOS 212的扩展)来促进VNF实例的协调。

[0034] 数据存储设备214可以被具体实现为被配置成用于数据的短期或长期存储的任何类型的(一个或多个)设备,诸如存储器设备和电路、存储器卡、硬盘驱动器、固态驱动器或者其他数据存储设备。在使用中,正如后面所描述的那样,数据存储设备214和/或存储器208可以存储安全性监测策略、配置策略或者其他类似的数据。

[0035] 安全时钟216可以被具体实现为能够提供安全定时信号和通过其他方式实施本文中所描述的功能的任何(多个)硬件组件或电路。例如在说明性实施例中,安全时钟216可以生成与计算节点110的其他时钟源分开并且功能上独立的定时信号。因此在这样的实施例中,安全时钟216可以不受诸如像在计算节点110上执行的软件之类的其他实体的改动的影响或不受所述改动的损害。应当认识到,在一些实施例中,安全时钟216可以被具体实现为(多个)独立组件或电路,而在其他实施例中,安全时钟216可以与另一个组件(例如处理器202)集成在一起或者形成另一个组件(例如处理器202)的一个安全部分。例如在一些实施例中,安全时钟216可以通过芯片上振荡器来实施并且/或者被具体实现为可管理性引擎(ME)的安全时钟。还应当认识到,安全时钟216可以被同步到其他计算节点110的安全时钟,并且粒度可以是能够区分不同消息定时的量级。

[0036] 计算节点110的通信电路218可以被具体实现为能够允许计算节点110与另一个计算节点110、NFV协调器104、VIM 106、端点设备118、120和/或其他所连接的具有网络功能的计算节点之间的通信的任何通信电路、设备或者其集合。通信电路218可以被配置成使用任

何一种或多种通信技术(例如有线或无线通信)和相关联的协议(例如以太网、蓝牙(Bluetooth)®、Wi-Fi®、WiMAX、GSM、LTE等等)来实现这样的通信。说明性的通信电路218包括网络接口卡(NIC)220和交换机222。NIC 220可以被具体实现为可以由计算节点110使用的一个或多个内装板(add-in-board)、子卡(daughtercard)、网络接口卡、控制器芯片、芯片组或者其他设备。举例来说,NIC 220可以被具体实现为通过扩展总线(诸如PCI快线(PCI Express))耦合到I/O子系统206的扩展卡。交换机222可以被具体实现为能够实施网络交换操作和通过其他方式实施本文中所描述的功能的任何(多个)硬件组件或电路,诸如以太网交换机芯片、PCI 快线交换芯片等等。

[0037] 正如前面所讨论的那样,计算节点110还可以包括安全性引擎224,安全性引擎224可以被具体实现为能够在计算节点110上建立受信任执行环境(TEE)的任何(多个)电路组件或电路。具体来说,安全性引擎224可以支持执行代码和/或访问数据,所述执行代码和/或访问数据独立于由计算节点110执行的其他代码并且不受由计算节点110执行的其他代码影响而是安全的。安全性引擎224可以被具体实现为受信任平台模块(TPM)、可管理性引擎(ME)、带外处理器或者其他安全性引擎设备或设备集合(例如ARM®处理器的受信任区块(TZ))。在一些实施例中,安全性引擎224可以被具体实现为合并在计算节点110的芯片上系统(SoC)中的集中式安全性和可管理性引擎(CSME)。

[0038] 再次参照图1,说明性的NFV网络架构116可通信地耦合在两个端点设备118、120之间。在说明性系统100中,第一端点设备被标示成端点设备(1)118,第二端点设备被标示成端点设备(2)120。但是应当认识到,可以通过NFV网络架构116连接任意数目的端点设备。端点设备118、120经由网络(未示出)使用有线或无线技术与NFV网络架构116可通信地耦合,从而形成端点设备(1)可以在其中与端点设备(2)进行通信(反之亦然)的端到端通信系统。相应地,NFV网络架构116可以监测并处理在端点设备118、120之间传送的网络通信业务(也就是网络分组)。

[0039] 端点设备118、120借以进行通信的网络可以被具体实现为任何类型的有线或无线通信网络,包括蜂窝网络(诸如全球移动通信系统(GSM)或长期演进(LTE))、电话网络、数字订户线(DSL)网络、有线网络、局域网或广域网、全球网络(例如因特网)或者其任意组合。例如在一些实施例中,所述网络可以被具体实现为具有vEPC架构的基于NFV的长期演进(LTE)网络。应当认识到,所述网络可以充当集中式网络,并且在一些实施例中所述网络可以可通信地耦合到另一个网络(例如因特网)。相应地,所述网络可以包括多种虚拟和物理网络设备,诸如促进端点设备118、120与NFV网络架构116之间的通信所需要的路由器、交换机、网络集线器、服务器、存储设备、计算设备等等。

[0040] 端点设备118、120可以被具体实现为能够实施本文中所描述的功能的任何类型的计算或计算机设备,包括但不限于智能电话、移动计算设备、平板计算机、膝上型计算机、笔记本计算机、计算机、服务器(例如独立式服务器、机架安放服务器、刀片式服务器等等)、网络电器(例如物理或虚拟电器)、web电器、分布式计算系统、基于处理器的系统和/或多处理器系统。如图3中所示,类似于图2的计算节点110,说明性的端点设备(例如图1的端点设备118、120的其中之一)包括处理器302、输入/输出(I/O)子系统304、存储器306、数据存储设备308、一个或多个外围设备310以及通信电路312。因此,在这里为了描述清楚起见将不重复对于类似组件的进一步描述,并且应当理解的是前面关于计算节点110提供的对于相应

组件的描述同样适用于端点设备118、120的相应组件。

[0041] 当然,端点设备118、120在其他实施例中可以包括其他或附加的组件,诸如通常在能够操作在电信基础设施中的移动计算设备中所见到的那些组件(例如各种输入/输出设备)。此外,在一些实施例中,其中一个或多个说明性组件可以被合并在另一个组件中或者通过其他方式形成另一个组件的一部分。外围设备310可以包括任意数目的输入/输出设备、接口设备和/或其他外围设备。例如在一些实施例中,外围设备310可以包括显示器、触摸屏、图形电路、键盘、鼠标、扬声器系统和/或其他输入/输出设备、接口设备和/或外围设备。

[0042] 现在参照图4,用于NFV网络架构116的VNF的安全自举的图1的NFV网络架构116的一个说明性实施例包括图1的NFV安全性服务控制器102、NFV协调器104、VIM 106和NFV基础设施108以及VNF管理器410。正如前面所描述的那样,在使用中,NFV协调器104管理NFV基础设施108中的VNF实例的生命周期,包括实例化、横向扩容/缩容、性能测量、事件相关、终止等等。为了这样做,NFV协调器104被配置成通过安全通信信道406向VNF管理器410提供指令,以便基于NFV基础设施108的资源管理NFV基础设施108的VNF实例(参见VNF实例440)的初始化和配置(也就是缩放和部署)。

[0043] VNF管理器410还被配置成针对NFV基础设施108的配置和事件报告实施总体协调和适配。VNF管理器410附加地被配置成更新和确保VNF实例的完整性。为了这样做,VNF管理器410被配置成经由安全通信信道414与VIM 106进行通信,以便确定将在其上实例化特定VNF实例的可用物理资源。应当认识到,VIM 106可以使用任何适当的技术、算法和/或机制作出这样的确定。还应当认识到,在一些实施例中,单个VNF管理器410可以负责管理一个或多个VNF实例。换句话说,在一些实施例中,为每一个VNF实例都可以实例化VNF管理器410。

[0044] NFV网络架构116附加地包括经由通信信道404可通信地耦合到NFV协调器104的操作支持系统和商业支持系统(OSS/BSS)402。OSS/BSS 402可以被具体实现为能够实施本文中所描述的功能的任何类型的计算或者计算节点,所描述的功能诸如支持电话网络中的各种端到端的电信服务。在一些实施例中,OSS/BSS 402可以被配置成支持管理功能(诸如网络清单、服务供应、网路配置和故障管理),并且支持可以由OSS/BSS 402支持的端到端电信服务的各种商业功能,诸如产品管理、顾客管理、收益管理、订单管理等等。

[0045] NFV安全性服务控制器102经由安全通信信道416可通信地耦合到NFV协调器104。应当认识到,在一些实施例中,NFV安全性服务控制器102和NFV协调器104可以位于同一处,诸如在MANO架构框架中。此外,NFV安全性服务控制器102经由安全通信信道428可通信地耦合到VIM 106,并且NFV协调器104经由安全通信信道408可通信地耦合到VIM 106。NFV网络架构116的安全通信信道(例如安全通信信道406、安全通信信道414等等)可以通过安全密钥(例如会话密钥和/或其他密码密钥)而受到保护,所述安全密钥由NFV安全性服务控制器102使用来建立信任根部(RoT)以便建立所述通信信道。在一些实施例中,所述安全密钥可以被具体实现为可以被周期性地刷新的成对会话密钥。因此,NFV安全性服务控制器102可以被配置成充当认证服务器。

[0046] NFV安全性服务控制器102包括VNF自举服务(VBS)420,VNF自举服务(VBS)420被配置成管理NFV基础设施108中的VNF实例的VBS代理(后面将进一步描述)。在使用中,VBS 420从信任锚的角度管理安全自举过程(也就是执行图9和10的安全VNF自举捕获协议)。相应

地,在一些实施例中,NFV安全性服务控制器102可以附加地包括受信任执行环境(TEE)422,VBS 420可以驻留在受信任执行环境(TEE)422中。但是应当认识到,在一些实施例中,VBS 420可以驻留在NFV安全性服务控制器102的外部,诸如驻留在专用的VBS服务器上。在这样的实施例中,VBS 420仍然可以在TEE中运行。

[0047] 此外,说明性的NFV安全性服务控制器102与安全性审计和法务(forensic)数据库426对接。安全性审计和法务数据库426被具体实现为包括相对于NFV网络架构116的各种安全性监测组件的安全性审计信息的安全数据库。安全性审计信息可以包括与NFV网络架构116的安全性有关的任何信息,所述信息例如包括配置改变日志、网络踪迹、调试踪迹、应用踪迹等等。在说明性的NFV网络架构116中,安全性审计和法务数据库426附加地被配置成与NFV网络架构116的其他网络和安全性监测组件对接,其他网络和安全性监测组件诸如VIM 106和分布在NFV网络架构116上的各种NFV安全性服务代理,正如后面将更加详细地讨论的那样。在一些实施例中,与安全性审计和法务数据库426对接的说明性NFV网络架构116的各种安全性监测组件可以使用安全时钟(例如图2的安全时钟216)对在安全性审计和法务数据库426处接收到的日志加时间标记以用于安全存储。

[0048] 正如前面所描述的那样,在使用中,VIM 106通过经由安全通信信道478安全地传送的消息控制并管理NFV基础设施108的虚拟和物理(即硬件)计算、存储和网络资源的分配。此外,在一些实施例中,VIM 106可以被配置成收集并且向安全性审计和法务数据库426安全地转发NFV基础设施108计算、存储和网络资源(例如物理和虚拟的)的性能测量和事件。说明性的VIM 106包括VIM控制器430。VIM控制器430被配置成充当云端操作系统VNF安装和激活服务。例如在一些实施例中,VIM控制器可以被具体实现为网络策略控制器或联网服务控制器(例如软件定义的联网(SDN)控制器或开放栈中子(OpenStack Neutron),或者被具体实现为计算服务控制器(例如开放栈新星(Openstack Nova))。附加地或替换地,在一些实施例中,VIM控制器430可以被具体实现为映像服务控制器、身份服务控制器等等。

[0049] NFV基础设施108包括可以从中部署VNF实例的计算节点110的所有硬件和软件组件(也就是虚拟计算、存储和网络资源,虚拟化软件,硬件计算、存储和网络资源等等)。应当认识到,NFV基础设施108的物理和/或虚拟组件可以跨越不同的位置、数据中心、地域、提供商等等。此外还应当认识到,NFV基础设施108的各个组件借以用来进行通信和接口的网络可以被视为包括在NFV基础设施108中。

[0050] 说明性的NFV基础设施108包括若干VNF实例440和运营商基础设施460。运营商基础设施460包括一个或多个平台470、图2的BIOS 212以及管理程序462。运营商基础设施460可以包括用于部署VNF实例440的多个不同的网络基础设施。相应地,运营商可以使用所述多个不同的网络基础设施在NFV基础设施108(即物理基础设施)上或者在另一个运营商的物理基础设施上进行部署,以及在第三方云端主控的基础设施上和/或在顾客处所处的顾客装备上等等进行部署。举例来说,部署情形可以包括操作在私有云端模型中的单一运营商、在混合云端中主控虚拟网络运营商的网络运营商、受主控的网络运营商、公共云端模型中受主控的通信和应用提供商、顾客处所/装备上的受管理网络服务等等。

[0051] 说明性的平台470包括第一平台,第一平台被标示成平台(1)472,并且包括第二平台,第二平台被标示成平台(N)474(也就是“第N个”平台,其中“N”是正整数并且标示一个或多个附加平台)。每一个平台470包括图2的I/O子系统206、NIC 220(或交换机222)和数据存

储装置。每一个平台470附加地包括该平台所独有的标识符(例如BIOS 212(UEFI)标识符),标识符可以被存储在安全位置(例如安全存储器210)中。所述独有平台标识符可以是硬件标识符的组合散列或全局唯一标识符(GUID)、原始装备制造商(OEM)板标识符、BIOS/UEFI库存单位(SKU)标识符、现场可更换单元(FRU)标识符、操作系统版本标识符等等。

[0052] 说明性的平台(1)472附加地包括TEE 476。TEE 476可以由CSME、SGX、IE、ME或者物理的、虚拟的(即基于软件的)或固件的TPM(例如由安全分区、安全性协处理器或单独处理器核心等等构成的安全性引擎224上的固件的TPM)在安全环境(例如处理器202的TEE支持204)中建立。此外,可以利用NFV安全性服务控制器102通过安全供应规程在平台(1)472中安全地供应TEE 476。在一些实施例中,可以利用NFV安全性服务控制器102通过自举实施所述安全供应规程。附加地或替换地,在一些实施例中,可以离线实施所述安全供应规程。

[0053] 管理程序462或虚拟机监视器(VMM)被配置成建立和/或利用NFV基础设施108的各种虚拟化的硬件资源(例如虚拟存储器、虚拟操作系统、虚拟联网组件等等)。此外,管理程序462可以促进跨越VNF实例440的通信。说明性的管理程序462包括一个或多个云端操作系统代理464,一个或多个云端操作系统代理464可以被配置成加强云端服务发现、服务协商和/或服务构成。在一些实施例中,管理程序462可以附加地包括TEE 466,TEE 466被配置成按照类似于TEE 476的方式但是在NFV基础设施108的虚拟(或管理程序)层级运作。

[0054] 在使用中,管理程序462通常经由用于运行每一个VNF实例440的一个或多个VM和/或容器来运行VNF实例440。在一些实施例中,VNF实例440可以包括账单功能、虚拟交换机(v交换机)、虚拟路由器(v路由器)、防火墙、网络地址翻译(NAT)、DPI、演进型分组核心(EPC)、移动性管理实体(MME)、分组数据网络网关(PGW)、服务网关(SGW)和/或其他虚拟网络功能。在一些实施例中,特定的VNF实例440可以具有多个子实例,多个子实例可以在单个平台(平台472)上或者跨越不同的平台(例如平台472和平台474)执行。换句话说,当被虚拟化时,传统上由与特定平台位于同一处的物理硬件处理的网络功能可以作为若干VNF实例440跨越一个或多个平台480而被分布。

[0055] 每一个VNF实例440可以包括一个或多个VNF实例。例如在一些实施例中,任何VNF实例440可以把服务功能链的多个VNF实例集束起来。此外,每一个VNF实例可以包括一个或多个VNF组件(VNFC)(未示出)。应当认识到,VNF实例440可以被具体实现为任何适当的虚拟网络功能;类似地,VNFC可以被具体实现为任何适当的VNF组件。VNFC是协作起来以给出一个或多个VNF实例440的功能的过程和/或实例。例如在一些实施例中,VNFC可以是VNF实例440的子模块。类似于VNF实例440,应当认识到VNFC可以跨越一个或多个平台470而被分布。还应当认识到,特定的VNF实例440可以跨越多个平台470而被分布,并且仍然形成建立在其中一个平台470上的VNF实例440的一部分。在这样的实施例中,VNF实例440和/或VNFC可以执行在相同的平台(例如平台472或平台474)上或者执行在相同的数据中心内但是执行在不同的平台470上。此外在一些实施例中,VNF实例440和/或VNFC可以跨越不同的数据中心而执行。类似于促进跨越VNF实例440的通信的管理程序462,管理程序462可以附加地促进跨越VNFC的通信。

[0056] 说明性的VNF实例440包括被标示成VNF(1)442的第一VNF实例、被标示成VNF(2)444的第二VNF实例以及被标示成VNF(N)446(也就是“第N个”VNF,其中“N”是正整数并且标示一个或多个附加VNF实例)的第三VNF实例。每一个VNF实例440被配置成作为虚拟联网设

备(例如v交换机、v路由器、防火墙、NAT、DPI、EPC、MME、PGW、SGW等等)来执行。在一些实施例中,一个或多个VNF实例440可以包括能够实施特定虚拟功能或服务的服务功能链。其中一个或多个VNF实例440可以包括用以在用户数据平面处对网络业务进行处理的分组处理器(未示出),诸如Intel®数据平面开发工具套件(Intel® DPDK)。

[0057] 类似于每一个平台470所独有的标识符,每一个VNF实例440包括独有标识符。VNF实例440的独有VNF实例标识符可以是VNF实例440的映像的组合散列或GUID、VNF描述符标识符、VNF命令行标识符、VNF OEM标识符、VNF销售商标识符和/或VNFC标识符。相应地,所述独有VNF实例标识符可以由NFV安全性服务控制器102、VIM 106和/或VNF管理器410在与VNF实例440进行安全地通信时使用。举例来说,VIM 106可以使用独有VNF实例标识符经由安全通信信道478在NFV基础设施108处发起创生(spinning up)VNF实例。类似地,VNF管理器410可以在经由安全通信信道418与特定VNF实例440设立管理会话时使用独有VNF实例标识符。

[0058] 每一个说明性VNF实例440包括VBS代理(也就是VNF(1)442的VBS代理448、VNF(2)444的VBS代理450和VNF(N)446的VBS代理452),用于安全地自举每一个VNF实例440,从而使得VNF实例440能够被安全地供应,诸如为之供应根凭证。此外,每一个说明性VNF实例经由安全通信信道424以及运营商基础设施460(也就是经由安全通信信道454、456、458)与NFV安全性服务控制器102的VBS 420进行安全网络通信。

[0059] 正如后面将更加详细地描述的那样,每一个VBS代理448、450、452被配置成实施安全自举过程(也就是执行图9和10的安全VNF自举捕获协议)。为了这样做,每一个VBS代理448、450、452被配置成实例化先前创生的VNF实例,创建将在运行安全自举过程时被用于与NFV安全性服务控制器102通信的安全性的公共/私有密钥对(也就是公共密钥和私有密钥),并且运行安全自举过程。应当认识到,在一些实施例中,NFV基础设施108可以附加地包括其他VNF实例,所述其他VNF实例并不包括VBS代理。

[0060] 正如先前所描述的那样,VNF实例440可以使诸如可能在服务功能链中所需要的多于一个VNF集束。在这样的实施例中,所述安全自举过程可以被用来自举整个服务功能链。此外,在其中沿着控制平面和数据平面把VNF实例440作为因素考虑进去的实施例中,安全自举过程可以被利用在一对第一、一对多或多对多的控制平面和数据平面的VNF实例中。

[0061] 现在参照图5,在使用中,NFV安全性服务控制器102在操作期间建立环境500。NFV安全性服务控制器102的说明性环境500包括安全通信模块510和图4的VNF自举服务420。此外,VNF自举服务420包括VBS代理通信模块520、VBS代理登记模块530。

[0062] 环境500的各种模块可以被具体实现为硬件、固件、软件或其组合。举例来说,环境500的各种模块、逻辑和其他组件可以形成NFV安全性服务控制器102的硬件组件的一部分,或者通过其他方式由NFV安全性服务控制器102的硬件组件建立。因此,在一些实施例中,环境500的任何其中一个或多个模块可以被具体实现为电气设备的电路或集合(例如安全通信电路、VBS代理通信电路和VBS代理登记电路等等)。附加地或替换地,在一些实施例中,其中一个或多个说明性模块可以形成另一个模块和/或其中一个或多个说明性模块和/或子模块的一部分,所述另一个模块和/或其中一个或多个说明性模块和/或子模块可以被具体实现为单独的或独立的模块。

[0063] 安全通信模块510被配置成促进NFV安全性服务控制器102与NFV网络架构116的各种网络处理组件之间的安全通信(也就是消息)。为了这样做,安全通信模块510被配置成确

保NFV安全性服务控制器102与NFV网络架构116的各种网络处理组件(例如VIM 106、VNF管理器410等等)之间的通信路径的安全。相应地,在一些实施例中,安全通信模块510可以实施各种密钥管理功能、密码功能、安全通信信道管理和/或其他安全性功能。举例来说,安全通信模块510可以被配置成通过使用周期性刷新的成对会话密钥确保NFV安全性服务控制器102与图4的VNF管理器410之间的通信信道(例如安全通信信道412)的安全,从而确保NFV安全性服务控制器102与VNF管理器410之间的通信的安全性。

[0064] 类似于安全通信模块510,VBS代理通信模块520被配置成促进和管理VBS 420与NFV基础设施108的VNF实例440的VBS代理之间的安全通信(也就是消息)。VBS代理登记模块530被配置成当执行安全自举过程时登记VBS代理。为了这样做,VBS代理登记模块530包括VBS代理验证模块532和VBS代理安全性凭证模块534。

[0065] VBS代理验证模块532被配置成验证VBS代理的安全自举参数(例如数值和散列)。为了这样做,VBS代理验证模块532被配置成验证在VBS捕获协议的执行期间接收自VBS代理的安全性引用(security quote)的真实性,这在后面更加详细地描述。附加地或替换地,在一些实施例中,VBS代理验证模块532可以被配置成实施白名单检查,以便基于由VBS 420或安全性控制器102在VBS 420的安全供应期间接收到的一个或多个供应参数来验证VBS 420的配置。在一些实施例中,VBS代理验证模块532可以附加地或替换地被配置成使用不重数会话(nonce session)检测VBS代理与VBS 420之间的消息的活性(也就是说消息尚未诸如在回放攻击中到期),这也在后面更进一步地描述。附加地或替换地,在一些实施例中,VBS代理验证模块532可以被配置成验证在VBS捕获协议的执行期间接收自VBS代理的VBS代理的VNF实例的公共密钥的真实性。

[0066] VBS代理安全性凭证模块534被配置成为在VBS捕获协议的执行期间正在登记的VBS代理提供有效的安全性凭证(例如证书、签名的散列结果等等)。为了这样做,VBS代理安全性凭证模块534可以被配置成响应于VBS代理验证模块532已经验证了VNF实例的安全性引用和公共密钥的真实性以及已经证实了消息的活性(也就是说消息诸如在回放攻击中没有死去)而创建或获取有效安全性凭证。

[0067] 现在参照图6,在使用中,每一个VNF实例(图4的VNF实例442、444、446)在操作期间建立环境600。相应的VNF实例的说明性环境600包括安全通信模块610和VBS代理(例如图4的其中一个VBS代理448、450、452)。说明性VBS代理包括VBS代理的VBS通信模块620和VBS捕获协议执行模块630。环境600的各种模块可以被具体实现为硬件、固件、软件或其组合。举例来说,环境600的各种模块、逻辑和其他组件可以形成NFV安全性服务代理的硬件组件的一部分或者通过其他方式由NFV安全性服务代理的硬件组件建立。因此,在一些实施例中,环境600的其中任何一个或多个模块可以被具体实现为电气设备的电路或集合(例如安全通信电路、VBS通信电路和VBS捕获协议执行电路等等)。附加地或替换地,在一些实施例中,其中一个或多个说明性模块可以形成另一个模块和/或其中一个或多个说明性模块和/或子模块的一部分,并且可以被具体实现为单独的或独立的模块。

[0068] 安全通信模块610被配置成促进去到和来自VBS代理的数据(也就是消息)的安全传送。类似于安全通信模块610,VBS通信模块620被配置成诸如在安全自举过程期间促进和管理VBS代理与NFV安全性服务控制器102的VBS 420之间的安全通信(例如登记数据、验证数据、配置数据等等)。VBS捕获协议执行模块630被配置成执行在图9和10中描述的安全VNF

自举捕获协议。为了这样做,VBS捕获协议执行模块630被配置成创建公共/私有密钥对(也就是公共密钥和私有密钥),并且从在其上实例化VNF实例的平台的TEE(例如图4的平台472的TEE 476)请求安全性引用(例如证实引用或者可以从中验证或认证TEE的数字签名值)。相应地,TEE可以证实VBS代理的身份和配置(例如运行正确的VBS代理,通过正确的启动参数进行配置,VBS代理生成了所请求的公共密钥)。此外,可以实施远程证实以检测可能的安全性威胁,诸如网络分组篡改、网络分组破坏、网络分组内的恶意内容等等。

[0069] 现在参照图7,在使用中,VNF实例(例如图4的其中一个VNF实例440)可以执行用于初始化安全VNF自举的方法700。方法700开始于框702,其中VNF实例确定是否诸如从图4的OSS/BSS 402接收到了实例化触发器。应当认识到,在一些实施例中,可以在VNF实例被创建之后自动实施实例化。如果没有的话,方法700循环回到框702以继续等待接收实例化触发器。如果接收到实例化触发器,则所述方法前进到框704。在框704处,VNF实例基于一个启动参数(也就是启动要求)的集合而实例化。应当认识到,实例化的VNF实例并非活跃(也就是说该VNF实例并未在处理着网络业务)。

[0070] 在框706处,VNF实例运行将在图9和10中更加详细地描述的安全VNF自举捕获协议。在框708处,VNF实例确定是否诸如从NFV安全性服务控制器102或VNF管理器410接收到表明要激活该VNF实例(也就是开始处理网络业务)的激活信号。如果没有的话,方法700循环回到框708以继续等待接收激活信号。如果接收到激活信号,则方法700前进到框710。在框710处,VNF实例获取特定于将由该VNF实例实施的操作的启动策略和配置信息。

[0071] 在框712处,VNF实例安全地登记为可操作的VNF实例。为了这样做,VNF实例向VBS 420安全地传送登记请求消息。在框714处,VNF实例确定是否响应于在框714处传送的登记请求消息而接收到登记确认。如果没有的话,则方法700循环回到框714以继续等待登记确认。如果接收到登记确认,则方法700前进到框716。在框716处,VNF实例诸如通过可以与登记确认一起接收的VNF管理器的IP地址而识别相应的VNF管理器(例如VNF管理器410)。应当认识到,在一些实施例中,在NFV网络架构116中可以存在多个VNF管理器。相应地,在这样的实施例中,可以通过与对应于VNF实例的VNF管理器相关联的独有标识符来识别该VNF管理器,所述标识符可以由NFV安全性服务控制器102提供给VNF实例。因此,在这样的实施例中,VNF实例可以在前进之前向NFV安全性服务控制器102请求所述独有标识符。

[0072] 在框718处,VNF实例连接到所识别出的VNF管理器。相应地,所识别出的VNF管理器可以管理VNF实例的生命周期(例如实例化、更新、查询、缩放、终止等等)。在一些实施例中,在框720处,VNF实例允许VNF许可授予和施行。相应地,可以(例如由关心VNF实例440所产生的收益的VNF销售商)跟踪和施行被指派给每一个VNF实例440的许可。为了这样做,在一些实施例中,可以向VNF管理器、NFV安全性服务控制器102和/或专用的许可管理服务器传送VNF许可信息(例如许可编号、独有VNF实例标识符等等)。在框722处,VNF实例实施为之实施化该VNF实例的操作(即服务或功能)。

[0073] 现在参照图8,用于安全地自举NFV网络架构116的VNF实例(例如图4的其中一个VNF实例440)的通信流800的实施例。说明性的通信流800包括NFV协调器104、VIM 106的VIM控制器430、管理程序462的云端操作系统代理464、NFV基础设施108的管理程序462、其中一个VNF实例440的其中一个VBS代理(例如VBS代理448、VBS代理450或VBS代理452)、平台472的TEE 476、NFV安全性服务控制器102的VBS 420以及VNF管理器410。说明性的通信流800附

加地包括若干消息流,其中一些消息流可以被分开执行或被一起执行,这取决于实施例。

[0074] 在消息流802处,NFV协调器104向VIM控制器430安全地传送接收自OSS/BSS 402的VNF实例化触发器。VNF实例化触发器可以包括签名VNF映像和签名VNF描述符的签名。签名VNF描述符是描述VNF映像的要求和/或必要元素(包括启动参数(也就是启动要求))的数据结构。在消息流804处,TEE 476安全地供应VBS 420。为了这样做,TEE 476把供应参数以及将在其上实例化VNF的平台所独有的标识符(也就是独有平台标识符)提供到VBS驻留在其上的安全性控制器102。相应地,在一些实施例中,TEE 422可以被用来安全地供应VBS 420。所述供应参数包括VBS 420的公共密钥和VBS 420的标识符,诸如IP地址、DNS等等。正如前面所描述的那样,所述独有平台标识符可以是硬件标识符的组合散列或GUID、OEM板标识符、BIOS/UEFI SKU标识符、FRU标识符、操作系统版本标识符等等。在一些实施例中,TEE 476可以使用带外(OOB)通信技术安全地供应VBS 420,以便传送VBS 420的公共密钥和VBS 420标识符以及用于安全地供应VBS 420可能需要的任何其他供应项目。

[0075] 在消息流806处,VIM控制器430验证与VNF实例化触发器一起接收到的信息的签名,所述信息诸如有签名VNF描述符和签名VNF映像。在一些实施例中,所述签名VNF映像可以包括多于一个签名VNF映像。在这样的实施例中,所述多于一个签名VNF映像可以被缝合在一起,并且作为一组VNF映像再次被签名,或者作为分开的签名VNF映像被递送。相应地,与签名VNF映像相关联的每一个签名在VIM控制器430处被验证。

[0076] 在消息流810处,VIM控制器430安全地传送基于VNF映像和描述符创生VNF实例的命令。所述创生命令附加地包括一组VBS参数(也就是VBS 420的细节),所述一组VBS参数可以包括VBS 420的公共密钥、VBS 420的IP地址、VBS 420的域名服务器(DNS)、VBS 420的完全合格域名(FQDN)、VBS 420的统一资源定位符(URL)等等。

[0077] 在消息流812处,管理程序462基于签名VNF映像和签名VNF描述符创生VNF实例(例如其中一个VNF实例440)。为了这样做,管理程序462在消息流814处验证VNF签名(例如签名VNF映像、签名VNF描述符的签名等等),并且在消息流816处创建VNF实例。在消息流818处,管理程序462向TEE 476进行登记。为了这样做,管理程序462安全地传送所创建的VNF实例所独有的标识符。所述独有VNF实例标识符可以是VNF映像实例标识符的组合散列或GUID、VNF描述符标识符、VNFC标识符的构成、VNF命令行标识符、VNF OEM标识符、VNF销售商标识符等等。此外,管理程序462可以安全地传送VNF实例的配置信息。

[0078] 在消息流820处,VBS代理创建用于VNF实例的公共/私有密钥对(也就是公共密钥和私有密钥)。在消息流822处,VBS代理从TEE 476获取安全性引用。相应地,可以实施远程证实以便检测可能的安全性威胁,诸如网路分组篡改、网络分组破坏、网络分组内的恶意内容等等。为了这样做,VBS代理可以向TEE 476安全地传送VNF标识信息,诸如独有平台标识符、独有VNF实例标识符等等。

[0079] 在消息流824处,VBS 420与VNF管理器410一起实施安全白名单处理。换句话说,VBS 420把VNF实例添加到将由VNF管理器410管理的得到认可(也就是被授予特权或者通过其他方式得到准许)的VBS代理的列表或寄存器。为了这样做,VBS 420可以向VNF管理器410安全地传送VNF标识信息(例如独有VNF实例标识符)以及一个或多个VBS参数(例如VBS 420的IP地址、VBS 420的DNS等等)。

[0080] 在消息流826处,VBS代理执行在图9和10中示出的安全VNF自举捕获协议。在消息

流828处,VBS代理激活VNF实例。换句话说,在VNF实例处启用网络业务处理。在消息流830处,VBS 420向VNF管理器410安全地传送包括独有VNF实例标识符的VNF已激活消息,用以表明VNF实例现在是活跃的。类似地,在消息流832处,VBS代理向VNF管理器410安全地传送VNF已激活消息,用以表明VNF实例已被激活。相应地,VNF已激活消息包括独有VNF实例标识符。

[0081] 现在参照图9,在使用中,VBS代理(例如图4的VBS代理448、VBS代理450或VBS代理452)可以执行用于执行安全VNF自举捕获协议的方法900。方法900开始于框902,其中VBS代理向VBS 420安全地传送开始消息。所述开始消息可以被具体实现为向VBS 420通知对应的VBS代理已经发起的任何类型的消息。在框904处,VBS代理把开始消息与不重数一起安全地传送,所述不重数由该VBS代理生成的将被用于安全认证的不重数(例如由VBS代理发出的用以检测VBS 420处的回放的随机挑战)。在框906处,VBS代理安全地接收来自VBS 420的开始响应消息。在框908处,VBS代理接收在框904处与开始消息一起传送的不重数以作为开始响应消息的一部分。此外,在框910处,VBS代理接收由VBS 420生成的不重数以作为开始响应消息的一部分。相应地,可以对开始响应消息实施活性检测,以便证明响应的活性。此外,在框912处,VBS代理接收由VBS 420使用VBS 420的私有密钥签名的开始响应消息。

[0082] 在框914处,VBS代理向VBS 420安全地传送登记请求消息。为了这样做,在框916处,VBS代理安全地传送由TEE 476使用TEE 476的私有密钥签名的安全性引用以作为登记请求消息的一部分。将在后面更加详细地描述安全性引用的计算,安全性引用是数字签名值,安全性引用的接收者可以从数字签名值认证所述数字签名值的传送者。相应地,可以实施远程证实以便检测可能的安全性威胁,诸如网络分组篡改、网络分组破坏、网络分组内的恶意内容等等。此外,在框918处,VBS代理安全地传送由VBS代理使用VNF的私有密钥签名的用以请求安全性凭证(例如证书、签名散列结果等等)的安全性凭证请求以作为登记请求消息的一部分。在一些实施例中,所述安全性凭证请求可以包括在VBS 420和VBS代理处生成的每一个不重数以及VNF实例的公共密钥。附加地或替换地,在一些实施例中,所述发证请求还可以包括由TEE 476使用TEE 476的私有密钥签名的引用。

[0083] 在框920处,VBS代理安全地接收来自VBS 420的登记请求消息响应。在框922处,由VBS代理接收到的登记请求消息响应包括有效安全性凭证。此外,在框924处,由VBS代理接收到的登记请求消息响应包括相应的VNF管理器(例如图4的VNF管理器410)的IP地址。在框926处,VBS代理所接收到的登记请求消息响应由VBS 420使用VBS 420的私有密钥签名。

[0084] 现在参照图10,用于由VBS代理(例如图4的VBS代理448、VBS代理450或VBS代理452)执行安全VNF自举捕获协议的通信流1000的实施例。说明性的通信流1000包括其中一个VNF实例440(例如)的其中一个VBS代理、平台472的TEE 476以及NFV安全性服务控制器102的VBS 420。说明性的通信流1000附加地包括若干消息流,其中一些消息流可以被分开地执行或被一起执行,这取决于实施例。

[0085] 在消息流1002处,VBS代理向VBS 420安全地传送包括不重数(例如用于认证的任意数)的开始消息。在消息流1004处,VBS 420向VBS代理安全地传送开始响应消息,开始响应消息包括来自VBS代理的不重数和另一个不重数(例如另一个用于认证的任意数字)。此外,所述开始响应消息由VBS 420使用VBS 420的私有密钥签名。在消息流1006处,VBS代理向VBS 420安全地传送登记请求消息。登记请求消息包括由TEE 476使用TEE 476的私有密钥签名的安全性引用(参见图11)。登记请求消息附加地包括安全性凭证请求,所述安全性

凭证请求包括来自VBS代理的不重数和来自VBS 420的不重数这二者以及VBS代理在其上被初始化的VNF实例的公共密钥。此外,安全性凭证请求由VBS代理使用VNF实例的私有密钥签名。由TEE 476计算并签名的安全性引用是将在图11中更加详细地描述的TEE引用操作的结果。

[0086] 在消息流1008处,VBS 420验证接收自VBS代理的由TEE 476签名的安全性引用。在消息流1010处,VBS 420实施一系列白名单检查以便验证VBS 420被正确地配置。相应地,在一些实施例中,VBS 420可以通过验证被用来安全地供应VBS 420的由TEE 476发送的供应参数(参见消息流804)来实施白名单检查。附加地或替换地,在一些实施例中,VBS 420可以通过相对于供应VBS 420的TEE在其上被实例化的平台的安全性策略(例如安全引导策略、TPM策略、版本控制策略等等)验证所接收到的独有平台标识符是有效的而实施白名单检查。此外,在一些实施例中,VBS 420可以实施白名单检查b从而检查附加策略的有效性,诸如用于许可有效性检查(例如基于独有VNF实例标识符)。此外,在一些实施例中,VBS 420可以附加地或替换地验证VBS代理是否被准许与VBS 420进行通信以作为白名单检查的一部分,这诸如是通过验证VBS代理已经向VBS 420登记而进行。

[0087] 在消息流1012处,VBS 420通过验证接收自VBS代理的VNF实例的不重数会话和公共密钥来验证安全性凭证请求。为了这样做,VBS 420实施活性检查以便使用会话不重数(也就是由VBS代理生成的不重数以及由VBS 420生成的不重数)检测任何延迟的或回放攻击。所述会话不重数可以是被用来检测攻击的随机数,随机数的值与对应于在其间传送的消息的流相关联地被存储。相应地,可以针对每一个流检查会话不重数以便检测所传送的消息的活性(也就是说该会话尚未到期)以及辨别在VBS 420可能正执行的多个流之间的不同。

[0088] 在消息流1014处,VBS 420在验证安全性凭证请求之后创建或获取有效安全性凭证(例如安全证书、签名散列结果等等)。应当认识到,可以按照任意顺序实施消息流1008到1014,但是在一些实施例中,可以由提供用于会话到期的时间线的VBS 420使用本地安全性策略。相应地,消息流1008到1014的实施顺序可以是基于当前活跃或者正由VBS 420缓冲的会话的数目、可用于VBS的计算资源、会话时间到期约束等等。

[0089] 在消息流1016处,VBS 420向VBS代理安全地传送登记响应。登记响应消息包括由VBS代理生成的不重数、由VBS 420生成的不重数、有效安全性凭证、负责管理VBS代理的VNF管理器410的标识符(例如IP地址、DNS、FQDN、URL等等)、被列入白名单的VNF管理器的集合、得到授权的VNFC(如果适用的话)的集合、独有VNF实例标识符以及一项或多项策略。所述一项或多项策略可以包括向VBS代理提供关于如何实施特定服务或功能的引导或指令的任何类型的策略,诸如安全性监测策略、联网策略、网络分组处理策略等等。此外,登记请求消息响应由VBS使用VBS 420的私有密钥签名。应当认识到,在一些实施例中,登记响应消息可以包括附加的和/或替换的参数。

[0090] 应当认识到,在一些实施例中,安全性引用可以是可扩展的,以便例如包括用以支持VNF实例在其上被实例化的平台的附加组件的附加的和/或替换的信息。举例来说,所述附加信息可以包括平台能力掩码、平台NIC和/或交换机掩码、用于平台的服务功能链(SFC)策略、安全性凭证标识符的列表等等。相应地,不同于在不安全和不可缩放的环境中使用静态映像的传统运营商云端网络,所述安全VNF自举捕获协议的动态性质可以减少静态配置

和安全性选项的量或者对静态配置和安全性选项的需求,这可以允许虚拟化运营商云端网络的更加动态的横向扩容/缩容。

[0091] 现在参照图11,在使用中,受信任执行环境(例如图4的TEE 476)可以执行用于针对VBS代理(例如图4的VBS代理448、VBS代理450或VBS代理452)实施TEE引用操作的方法1100。方法1100开始于框1102,其中TEE对VBS代理的一个启动参数集合应用散列函数,从而生成散列结果。所述启动参数可以包括可以被用来启动VNF和/或VBS代理的实例的任何参数。为了这样做,在框1104处,TEE对VNF实例的映像、VNF实例的描述符、VNF实例所独有的标识符(也就是独有VNF实例标识符)和/或VNF实例在其上被实例化的平台所独有的标识符(也就是独有平台标识符)应用散列函数,从而生成散列结果。相应地,TEE可以在其加载VNF时应用第一散列函数,这是因为TEE知道所有VNF启动参数以便启动VNF。换句话说,TEE可以在没有接收来自VBS代理的任何输入的情况下应用第一散列函数。

[0092] 在框1106处,TEE对VBS 420的一个VBS标识符集合以及其中一个或多个VBS代理启动参数应用散列函数,从而生成第二散列结果。所述VBS标识符集合可以包括可以被用来标识VBS 420的任何信息,诸如VBS 420的公共密钥、VBS 420的IP地址、VBS 420的DNS、VBS 420的FQDN、VBS 420的URL等等。为了这样做,在框1108处,TEE对VBS 420的公共密钥、VBS 420的IP地址、独有VNF实例标识符、独有平台标识符应用所述散列函数。在一些实施例中,在框1106处应用散列函数之前,可以对VBS 420的VBS标识符集合应用另一个散列函数。附加地或替换地,在一些实施例中,在框1102处应用的散列函数的散列结果可以附加地作为输入被包括在框1106处应用的散列函数中。

[0093] 在框1110处,TEE对VNF实例的公共密钥应用散列函数,从而生成散列结果。应当认识到,在一些实施例中,在框1106处应用的散列函数的散列结果可以附加地作为输入被包括在框1110处应用的散列函数中。类似于第一散列函数,TEE可以在不接收来自VBS代理的任何输入的情况下应用框1106的散列函数。在框1112处,TEE对框1102、1106和1110的所有散列结果应用散列函数,从而生成最终散列结果。在框1114处,TEE使用TEE的私有密钥对最终散列结果签名,从而生成安全性引用。

[0094] 示例

[0095] 下面将提供本文中所公开的技术的说明性示例。所述技术的实施例可以包括后面所描述的示例当中的任何一个或多个以及其任意组合。

[0096] 示例1包括用于在网络功能虚拟化(NFV)网络架构中自举虚拟网络功能(VNF)的VNF实例的虚拟网络功能自举服务(VBS)代理,所述VBS代理包括VBS捕获协议执行模块,用以:(i)向NFV网络架构的VBS传送开始消息,其中VBS可通信地耦合到VBS代理,并且其中所述开始消息提供表明VBS代理被实例化的指示;(ii)响应于开始消息的传送,接收来自VBS的开始响应消息;(iii)响应于接收到开始响应消息,向VBS传送登记请求消息,其中登记请求消息包括可用来将VBS代理认证为登记请求消息的传送者的安全性引用以及用以向VBS请求安全性凭证的安全性凭证请求;以及(iv)接收来自VBS的登记响应消息,其中登记响应消息包括表明安全性引用和安全性凭证请求已被VBS证实的安全性凭证。

[0097] 示例2包括示例1的主题,并且其中开始消息包括第一不重数,开始响应消息由VBS使用VBS的私有密钥签名并且包括第一不重数以及由VBS生成的第二不重数,安全性凭证请求由VNF实例使用VNF实例的私有密钥签名并且包括第一不重数、第二不重数以及VNF实例

的公共密钥,登记响应消息由VBS使用VBS的私有密钥签名并且还包括第一不重数、第二不重数、负责管理VBS代理的VNF管理器的标识符、被列入白名单的VNF管理器的集合、由VBS授权的VNF组件(VNFC)的集合、独有VNF实例标识符以及一项或多项策略,并且所述策略包括可由VBS代理使用来实施特定功能的指令。

[0098] 示例3包括示例1和2当中的任一个的主题,并且其中VBS捕获协议执行模块还获取由受信任执行环境(TEE)使用TEE的私有密钥签名的安全性引用,其中TEE位于VNF实例在其上被实例化的平台上。

[0099] 示例4包括示例1-3当中的任一个的主题,并且其中VBS捕获协议执行模块还:(i)接收来自NFV网络架构的NFV协调器的实例化触发器;以及(ii)初始化VBS代理,其中传送开始消息包括响应于接收到实例化触发器而传送开始消息。

[0100] 示例5包括示例1-4当中的任一个的主题,并且其中初始化VBS代理包括:(i)创建VNF实例的公共/私有密钥对,其中VNF实例的公共/私有密钥对包括公共密钥和私有密钥;以及(ii)从VNF实例在其上被创建的平台的受信任执行环境(TEE)获取安全性引用,其中所述安全性引用由TEE使用TEE的私有密钥签名。

[0101] 示例6包括示例1-5当中的任一个的主题,并且其中VBS捕获协议执行模块还:(i)生成安全性凭证请求;以及(ii)响应于已经接收到来自VBS的开始响应消息,使用VNF实例的私有密钥对安全性凭证请求签名。

[0102] 示例7包括示例1-6当中的任一个的主题,并且其中VBS捕获协议执行模块还响应于已经接收到安全性凭证而激活VNF实例以便活跃地处理由VNF实例接收到的网络业务。

[0103] 示例8包括示例1-7当中的任一个的主题,并且其中VBS捕获协议执行模块还向NFV网络架构的VNF管理器传送指示,所述指示向VNF管理器表明(i)VNF实例是活跃的并且(ii)VNF实例的配置将由VNF管理器管理,其中所述指示包括VNF实例标识符,VNF实例标识符是VNF实例所独有的并且可用来把VNF实例添加到VNF管理器处的得到授权的VNF实例的白名单。

[0104] 示例9包括示例1-8当中的任一个的主题,并且其中接收来自VBS的登记响应消息还包括接收可通信地耦合到VBS代理的VNF管理器的标识符。

[0105] 示例10包括示例1-9当中的任一个的主题,并且其中接收VNF管理器的标识符包括接收网际协议(IP)地址、域名服务器(DNS)、完全合格域名(FQDN)、统一资源定位符(URL)的至少其中之一。

[0106] 示例11包括示例1-10当中的任一个的主题,并且其中VBS捕获协议执行模块还响应于接收到VNF管理器的标识符而使用VNF管理器的标识符连接到VNF管理器。

[0107] 示例12包括示例1-11当中的任一个的主题,并且其中VBS捕获协议执行模块还响应于已经接收到VNF管理器的标识符而向VNF管理器传送VNF许可信息,其中VNF许可信息包括可用来跟踪与VNF实例相关联的许可的使用的信息。

[0108] 示例13包括一种用于在网络功能虚拟化(NFV)网络架构中自举虚拟网络功能的方法,所述方法包括:由NFV网络架构的VNF实例的VNF自举服务(VBS)代理向可通信地耦合到VBS代理的NFV网络架构的VBS传送开始消息,其中所述开始消息提供表明VBS代理被实例化的指示;由VBS代理响应于开始消息而接收来自VBS的开始响应消息;由VBS代理响应于接收到开始响应消息而向VBS传送登记请求消息,其中登记请求消息包括可用来将VBS代理认证

为登记请求消息的传送者的安全性引用以及用以向VBS请求安全性凭证的安全性凭证请求;以及由VBS代理接收来自VBS的登记响应消息,其中登记响应消息包括表明安全性引用和安全性凭证请求当中的每一项已被VBS证实的安全性凭证。

[0109] 示例14包括示例13的主题,并且其中传送开始消息包括传送第一不重数,接收开始响应消息包括接收由VBS使用VBS的私有密钥签名的开始响应消息并且包括第一不重数以及由VBS生成的第二不重数,传送安全性凭证请求包括传送由VNF实例使用VNF实例的私有密钥签名的安全性凭证请求并且包括第一不重数、第二不重数以及VNF实例的公共密钥,接收登记响应消息包括接收由VBS使用VBS的私有密钥签名的登记响应消息并且还包括第一不重数、第二不重数、负责管理VBS代理的VNF管理器的标识符、被列入白名单的VNF管理器的集合、由VBS授权的VNF组件(VNFC)的集合、独有VNF实例标识符以及一项或多项策略,并且所述策略包括可由VBS代理使用来实施特定功能的指令。

[0110] 示例15包括示例13和14当中的任一个的主题,并且还包括由VBS代理获取由受信任执行环境(TEE)使用TEE的私有密钥签名的安全性引用,其中TEE位于VNF实例在其上被实例化的平台上。

[0111] 示例16包括示例13-15当中的任一个的主题,并且还包括:由VBS代理接收来自NFV网络架构的NFV协调器的实例化触发器;以及初始化VBS代理,其中传送开始消息包括响应于接收到实例化触发器而传送开始消息。

[0112] 示例17包括示例13-16当中的任一个的主题,并且其中初始化VBS代理包括:(i)创建公共/私有密钥对,其中VNF实例的公共/私有密钥对包括公共密钥和私有密钥;以及(ii)从VNF实例在其上被创建的平台的受信任执行环境(TEE)获取安全性引用,其中所述安全性引用由TEE使用TEE的私有密钥签名。

[0113] 示例18包括示例13-17当中的任一个的主题,并且还包括:(i)生成安全性凭证请求;以及(ii)响应于已经接收到来自VBS的开始响应消息,使用VNF实例的私有密钥对安全性凭证请求签名。

[0114] 示例19包括示例13-18当中的任一个的主题,并且还包括:响应于接收到安全性凭证,激活VNF实例以便活跃地处理由VNF实例接收到的网络业务。

[0115] 示例20包括示例13-19当中的任一个的主题,并且还包括向NFV网络架构的VNF管理器传送指示,所述指示向VNF管理器表明(i)VNF实例是活跃的并且(ii)VNF实例的配置将由VNF管理器管理,其中所述指示包括VNF实例标识符,VNF实例标识符是VNF实例独有的并且可用来把VNF实例添加到VNF管理器处的得到授权的VNF实例的白名单。

[0116] 示例21包括示例13-20当中的任一个的主题,并且其中接收来自VBS的登记响应消息还包括接收可通信地耦合到VBS代理的VNF管理器的标识符。

[0117] 示例22包括示例13-21当中的任一个的主题,并且其中接收VNF管理器的标识符包括接收网际协议(IP)地址、域名服务器(DNS)、完全合格域名(FQDN)、统一资源定位符(URL)的至少其中之一。

[0118] 示例23包括示例13-22当中的任一个的主题,并且还包括响应于接收到VNF管理器的标识符而使用VNF管理器的标识符连接到VNF管理器。

[0119] 示例24包括示例13-23当中的任一个的主题,并且还包括响应于已经接收到VNF管理器的标识符而向VNF管理器传送VNF许可信息,其中VNF许可信息包括可用来跟踪与VNF实

例相关联的许可的使用的信息。

[0120] 示例25包括一种计算设备,所述计算设备包括处理器以及已经在其中存储有多条指令的存储器,所述指令在由处理器执行时使得所述计算设备实施权利要求13-24当中的任一条的方法。

[0121] 示例26包括一种或多种机器可读存储介质,所述一种或多种机器可读存储介质包括存储在其上的多条指令,所述指令响应于被执行而导致计算设备实施权利要求13-24当中的任一条的方法。

[0122] 示例27包括用于在网络功能虚拟化(NFV)网络架构中自举虚拟网络功能(VNF)的网络功能虚拟化(NFV)网络架构的VNF实例的虚拟网络功能(VNF)自举服务(VBS)代理,所述方法包括:用于向可通信地耦合到VBS代理的NFV网络架构的VBS传送开始消息的装置,其中所述开始消息提供表明VBS代理被实例化的指示;用于响应于开始消息而接收来自VBS的开始响应消息的装置;用于响应于接收到开始响应消息而向VBS传送登记请求消息的装置,其中登记请求消息包括可用来将VBS代理认证为登记请求消息的传送者的安全性引用以及用以向VBS请求安全性凭证的安全性凭证请求;以及用于接收来自VBS的登记响应消息的装置,其中登记响应消息包括表明安全性引用和安全性凭证请求当中的每一项已被VBS证实的安全性凭证。

[0123] 示例28包括示例27的主题,并且其中用于传送开始消息的装置包括用于传送第一不重数的装置,用于接收开始响应消息的装置包括用于接收由VBS使用VBS的私有密钥签名的开始响应消息的装置并且包括第一不重数以及由VBS生成的第二不重数,用于传送安全性凭证请求的装置包括用于传送由VNF实例使用VNF实例的私有密钥签名的安全性凭证请求的装置并且包括第一不重数、第二不重数以及VNF实例的公共密钥,用于接收登记响应消息的装置包括用于接收由VBS使用VBS的私有密钥签名的登记响应消息的装置并且还包括第一不重数、第二不重数、负责管理VBS代理的VNF管理器的标识符、被列入白名单的VNF管理器的集合、由VBS授权的VNF组件(VNFC)的集合、独有VNF实例标识符以及一项或多项策略,并且所述策略包括可由VBS代理使用来实施特定功能的指令。

[0124] 示例29包括示例27和28的主题,并且其中用于接收来自VBS的登记响应消息的装置还包括用于接收可通信地耦合到VBS代理的VNF管理器的标识符的装置。

[0125] 示例30包括示例27-29的主题,并且还包括用于响应于接收到VNF管理器的标识符而使用VNF管理器的标识符连接到VNF管理器的装置。

[0126] 示例31包括示例27-30的主题,并且还包括用于响应于已经接收到VNF管理器的标识符而向VNF管理器传送VNF许可信息的装置,其中VNF许可信息包括可用来跟踪与VNF实例相关联的许可的使用的信息。

[0127] 示例32包括用于在网络功能虚拟化(NFV)网络架构中自举虚拟网络功能的NFV网络架构方法的虚拟网络功能(VNF)自举服务(VBS),所述VBS包括VBS代理通信模块,用以:(i)接收来自可通信地耦合到VBS的NFV网络架构的VNF实例的VBS代理的开始消息,其中所述开始消息提供表明VBS代理已被实例化的指示;(ii)响应于接收到开始消息,向VBS代理传送开始响应消息;(iii)响应于传送了开始响应消息,接收来自VBS代理的登记请求消息,其中登记请求消息包括安全性引用以及用以向VBS请求安全性凭证的安全性凭证请求;(iv)响应于已经接收到登记请求消息的安全性凭证请求,对安全性引用进行证实,以便把

VBS代理认证为登记请求消息的传送者;以及(v)响应于证实了安全性引用,向VBS代理传送登记响应消息,其中登记响应消息包括表明安全性引用已被VBS证实的安全性凭证。

[0128] 示例33包括示例32的主题,接收开始消息包括接收第一不重数,传送开始响应消息包括传送由VBS使用VBS的私有密钥签名的开始响应消息,其中开始响应消息包括第一不重数以及由VBS生成的第二不重数,并且接收安全性凭证请求包括接收由VNF实例使用VNF实例的私有密钥签名的安全性凭证请求,其中安全性凭证请求包括第一不重数、第二不重数以及VNF实例的公共密钥。

[0129] 示例34包括示例32和33的主题,其中传送登记响应消息包括传送由VBS使用VBS的私有密钥签名的登记响应消息,其中登记响应消息还包括第一不重数、第二不重数、负责管理VBS代理的VNF管理器的标识符、被列入白名单的VNF管理器的集合、由VBS授权的VNF组件(VNFC)的集合、独有VNF实例标识符以及一项或多项策略,并且其中所述一项或多项策略包括可由VBS代理使用来实施特定功能的指令。

[0130] 示例35包括示例32-34的主题,并且其中VBS代理通信模块还接收来自VNF实例在其上被创建的平台的受信任执行环境(TEE)的供应参数的集合,其中所述供应参数可用来安全地供应VBS并且包括(i)VNF实例在其上被创建的平台所独有的平台标识符、(ii)VBS的公共密钥以及(iii)VBS的独有标识符,并且基于所述供应参数而供应VBS。

[0131] 示例36包括示例32-35的主题,并且还包括VBS代理验证模块,用以:(i)响应于接收到登记请求消息,基于TEE的私有密钥验证安全性引用的真实性,其中安全性引用是利用TEE的私有密钥被签名的;(ii)实施白名单检查以便验证VBS的配置;(iii)使用第一和第二不重数检测登记请求消息的活性,以便确保第一和第二不重数尚未到期;以及(iv)验证VNF实例的公共密钥的真实性。

[0132] 示例37包括示例32-36的主题,并且其中实施白名单检查包括验证由VBS接收到的供应参数以便安全地供应VBS。

[0133] 示例38包括示例32-37的主题,并且其中实施白名单检查包括验证平台标识符对应于可由VBS访问的安全性策略的有效平台标识符。

[0134] 示例39包括示例32-38的主题,并且还包括VBS代理安全性凭证模块,所述VBS代理安全性凭证模块响应于(i)已经验证了安全性引用和VNF实例的公共密钥的真实性并且(ii)已经检测到登记请求消息是活跃的而创建安全性凭证。

[0135] 示例40包括示例32-39的主题,并且其中VBS代理通信模块还:(i)创建包括公共密钥和私有密钥的VBS公共/私有密钥对;以及(ii)使用VBS公共/私有密钥对的私有密钥对开始响应消息签名,其中传送开始响应消息包括传送签名的开始响应消息。

[0136] 示例41包括示例32-40的主题,并且其中VBS代理通信模块还使用VBS公共/私有密钥对的私有密钥对登记响应消息签名,其中传送开始响应消息包括传送签名的开始响应消息。

[0137] 示例42包括示例32-41的主题,并且其中向VBS代理传送登记响应消息包括传送可通信地耦合到VBS代理的VNF管理器的标识符,其中所述标识符可用来标识VNF管理器以便建立与VNF管理器的通信信道。

[0138] 示例43包括示例32-42的主题,并且其中传送VNF管理器的标识符包括传送网际协议(IP)地址、域名服务器(DNS)、完全合格域名(FQDN)、统一资源定位符(URL)的至少其中之

一。

[0139] 示例44包括示例32-43的主题,并且其中VBS代理通信模块还向VNF管理器传送VNF已激活消息,所述VNF已激活消息可由VNF管理器使用来设立与VNF实例的通信信道。

[0140] 示例45包括一种用于在网络功能虚拟化(NFV)网络架构中自举虚拟网络功能的方法,所述方法包括:由NFV网络架构的VNF自举服务(VBS)接收来自可通信地耦合到VBS的NFV网络架构的VNF实例的VBS代理的开始消息,其中所述开始消息提供表明VBS代理已被实例化的指示;由VBS响应于接收到开始消息而向VBS代理传送开始响应消息;由VBS响应于传送了开始响应消息而接收来自VBS代理的登记请求消息,其中登记请求消息包括安全性引用以及用以向VBS请求安全性凭证的安全性凭证请求;由VBS响应于接收到登记请求消息的安全性凭证请求而对安全性引用进行证实,从而把VBS代理认证为登记请求消息的传送者;以及由VBS响应于证实了安全性引用而向VBS代理传送登记响应消息,其中登记响应消息包括表明安全性引用已被VBS证实的安全性凭证。

[0141] 示例46包括示例45的主题,接收开始消息包括接收第一不重数,传送开始响应消息包括传送由VBS使用VBS的私有密钥签名的开始响应消息,其中开始响应消息包括第一不重数以及由VBS生成的第二不重数,并且接收安全性凭证请求包括接收由VNF实例使用VNF实例的私有密钥签名的安全性凭证请求,其中安全性凭证请求包括第一不重数、第二不重数以及VNF实例的公共密钥。

[0142] 示例47包括示例45和46的主题,并且其中传送登记响应消息包括传送由VBS使用VBS的私有密钥签名的登记响应消息,其中登记响应消息还包括第一不重数、第二不重数、负责管理VBS代理的VNF管理器的标识符、被列入白名单的VNF管理器的集合、由VBS授权的VNF组件(VNFC)的集合、独有VNF实例标识符以及一项或多项策略,并且其中所述一项或多项策略包括可由VBS代理使用来实施特定功能的指令。

[0143] 示例48包括示例45-47的主题,并且还包括:由VBS接收来自VNF实例在其上被创建的平台的受信任执行环境(TEE)的供应参数的集合,其中所述供应参数可用来安全地提供VBS并且包括(i)VNF实例在其上被创建的平台所独有的平台标识符、(ii)VBS的公共密钥以及(iii)VBS的独有标识符;以及基于所述供应参数而供应VBS。

[0144] 示例49包括示例45-48的主题,并且还包括:由VBS响应于接收到登记请求消息而基于TEE的私有密钥验证安全性引用的真实性,其中安全性引用是利用TEE的私有密钥被签名的;由VBS实施白名单检查以便验证VBS的配置;由VBS使用第一和第二不重数检测登记请求消息的活性,以便确保第一和第二不重数尚未到期;以及由VBS验证VNF实例的公共密钥的真实性。

[0145] 示例50包括示例45-49的主题,并且其中实施白名单检查包括验证由VBS接收到的供应参数以便安全地供应VBS。

[0146] 示例51包括示例45-50的主题,并且其中实施白名单检查包括验证平台标识符对应于可由VBS访问的安全性策略的有效平台标识符。

[0147] 示例52包括示例45-51的主题,并且还包括响应于(i)已经验证了安全性引用和VNF实例的公共密钥的真实性并且(ii)已经检测到登记请求消息是活性的而创建安全性凭证。

[0148] 示例53包括示例45-52的主题,并且还包括:创建包括公共密钥和私有密钥的VBS

公共/私有密钥对;以及使用VBS公共/私有密钥对的私有密钥对开始响应消息签名,其中传送开始响应消息包括传送签名的开始响应消息。

[0149] 示例54包括示例45-53的主题,并且还包括使用VBS公共/私有密钥对的私有密钥对登记响应消息签名,其中传送开始响应消息包括传送签名的开始响应消息。

[0150] 示例55包括示例45-54的主题,并且其中向VBS代理传送登记响应消息包括传送可通信地耦合到VBS代理的VNF管理器的标识符,其中所述标识符可用来标识VNF管理器以便建立与VNF管理器的通信信道。

[0151] 示例56包括示例45-55的主题,并且其中传送VNF管理器的标识符包括传送网际协议(IP)地址、域名服务器(DNS)、完全合格域名(FQDN)、统一资源定位符(URL)的至少其中之一。

[0152] 示例57包括示例45-56的主题,并且还包括向VNF管理器传送VNF已激活消息,所述VNF已激活消息可由VNF管理器使用来设立与VNF实例的通信信道。

[0153] 示例58包括一种计算设备,所述计算设备包括处理器以及已经在其中存储有多条指令的存储器,所述指令在由处理器执行时使得所述计算设备实施权利要求45-57当中的任一条的方法。

[0154] 示例59包括一个或多个机器可读存储介质,所述一个或多个机器可读存储介质包括存储在其上的多条指令,所述指令响应于被执行而导致计算设备实施权利要求45-57当中的任一条的方法。

[0155] 示例60包括用于在网络功能虚拟化(NFV)网络架构中自举虚拟网络功能的NFV网络架构方法的虚拟网络功能(VNF)自举服务(VBS),所述VBS包括:用于接收来自可通信地耦合到VBS的NFV网络架构的VNF实例的VBS代理的开始消息的装置,其中所述开始消息提供表明VBS代理已被实例化的指示;用于响应于接收到开始消息而向VBS代理传送开始响应消息的装置;用于响应于传送了开始响应消息而接收来自VBS代理的登记请求消息的装置,其中登记请求消息包括安全性引用以及用以向VBS请求安全性凭证的安全性凭证请求;用于响应于接收到登记请求消息的安全性凭证请求而对安全性引用进行证实以把VBS代理认证为登记请求消息的传送者的装置;以及用于响应于证实了安全性引用而向VBS代理传送登记响应消息的装置,其中登记响应消息包括表明安全性引用已被VBS证实的安全性凭证。

[0156] 示例61包括示例60的主题,并且其中用于接收开始消息的装置包括用于接收第一不重数的装置,其中用于传送开始响应消息的装置包括用于传送由VBS使用VBS的私有密钥签名的开始响应消息的装置,其中开始响应消息包括第一不重数以及由VBS生成的第二不重数,并且其中用于接收安全性凭证请求的装置包括用于接收由VNF实例使用VNF实例的私有密钥签名的安全性凭证请求的装置,其中安全性凭证请求包括第一不重数、第二不重数以及VNF实例的公共密钥。

[0157] 示例62包括示例60和61的主题,并且其中用于传送登记响应消息的装置包括用于传送由VBS使用VBS的私有密钥签名的登记响应消息的装置,其中登记响应消息还包括第一不重数、第二不重数、负责管理VBS代理的VNF管理器的标识符、被列入白名单的VNF管理器的集合、由VBS授权的VNF组件(VNFC)的集合、独有VNF实例标识符以及一项或多项策略,并且其中所述一项或多项策略包括可由VBS代理使用来实施特定功能的指令。

[0158] 示例63包括示例60-62的主题,并且还包括:用于接收来自VNF实例在其上被创建

的平台的受信任执行环境(TEE)的供应参数的集合的装置,其中所述供应参数可用来安全地供应VBS并且包括(i)VNF实例在其上被创建的平台所独有的平台标识符、(ii)VBS的公共密钥以及(iii)VBS的独有标识符;以及用于基于所述供应参数而供应VBS的装置。

[0159] 示例64包括示例60-63的主题,并且还包括:用于响应于接收到登记请求消息而基于TEE的私有密钥验证安全性引用的真实性的装置,其中安全性引用是利用TEE的私有密钥被签名的;用于实施白名单检查以便验证VBS的配置的装置;用于使用第一和第二不重数检测登记请求消息的活性以便确保第一和第二不重数尚未到期的装置;以及用于验证VNF实例的公共密钥的真实性的装置。

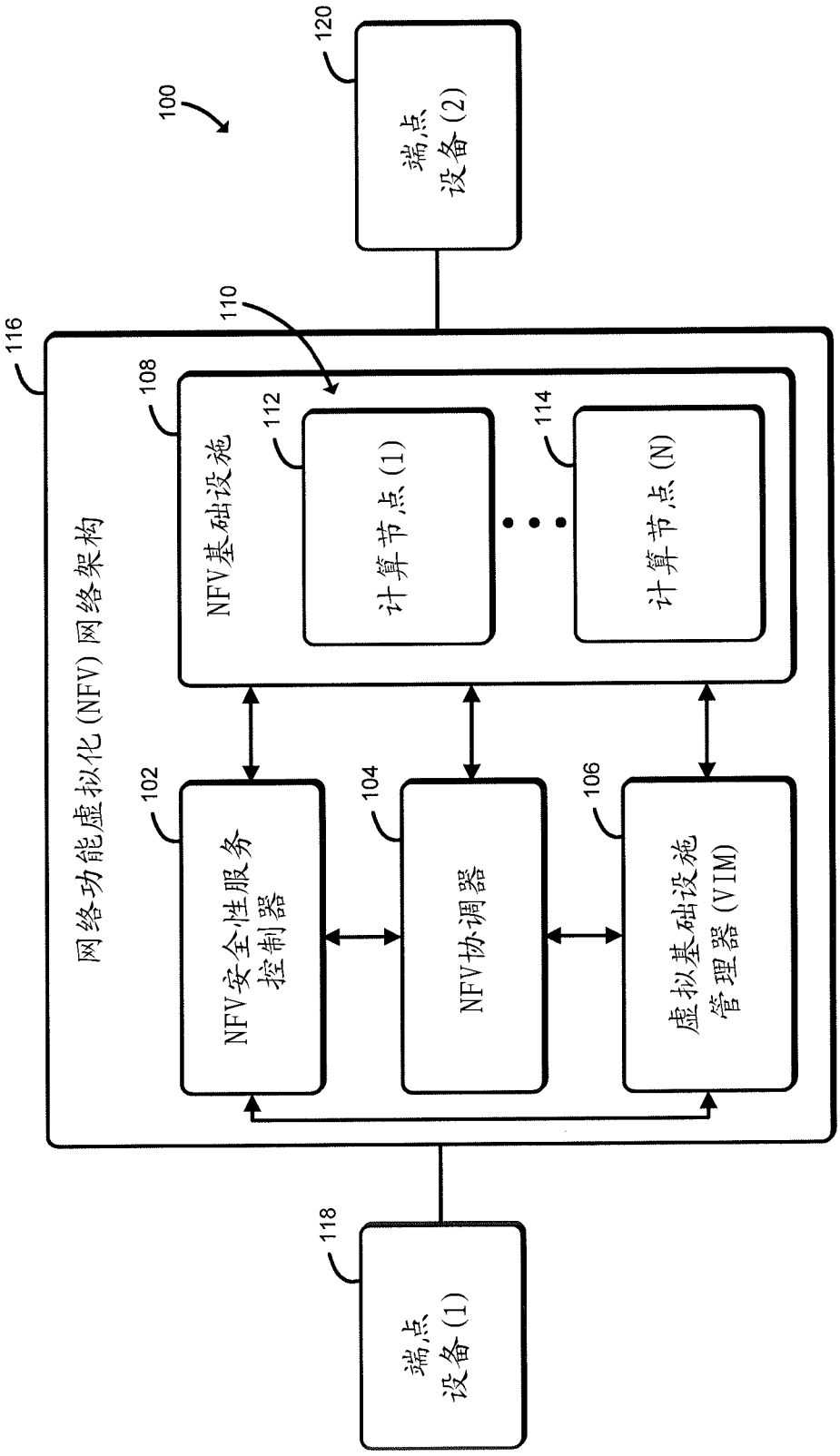

100
120
端点设备(2)
110
116
网络功能虚拟化(NFV)网络架构
108
NFV基础设施
112
计算节点(1)
114
计算节点(N)
102
NFV安全性服务控制器
104
NFV协调器
106
虚拟基础设施管理器(VIM)
118
端点设备(1)

图 1

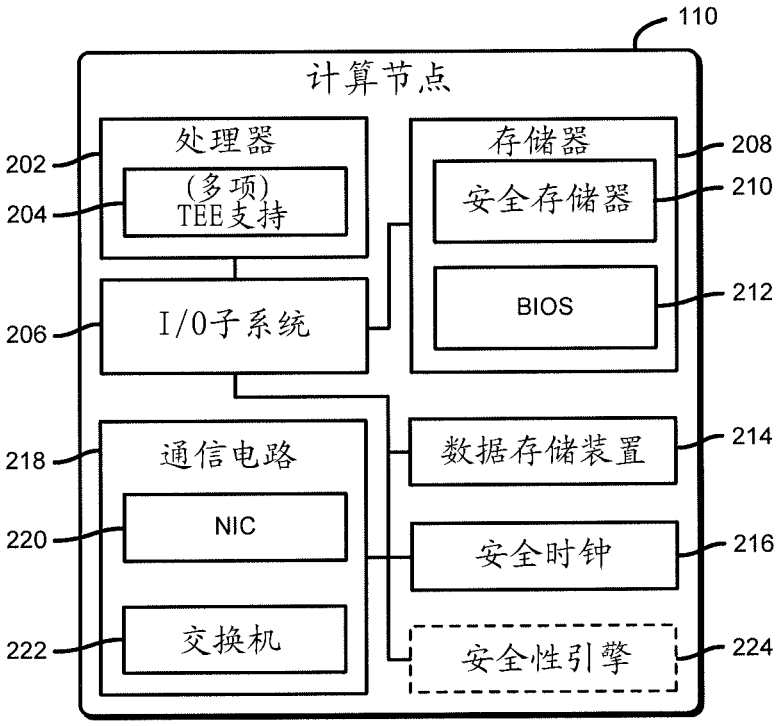

110
计算节点
处理器
202
(多项)
TEE支持
204
I/O子系统
206
存储器
208
安全存储器
210
BIOS
212
通信电路
218
NIC
220
交换机
222
数据存储装置
214
安全时钟
216
安全性引擎
224

图 2

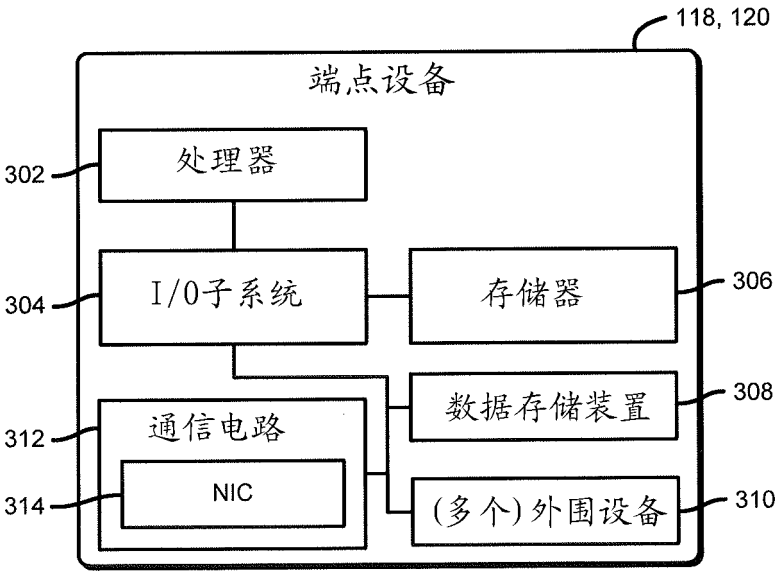

118, 120
端点设备
处理器
302
I/O子系统
304
存储器
306
数据存储装置
308
通信电路
312
NIC
314
(多个)外围设备
310

图 3

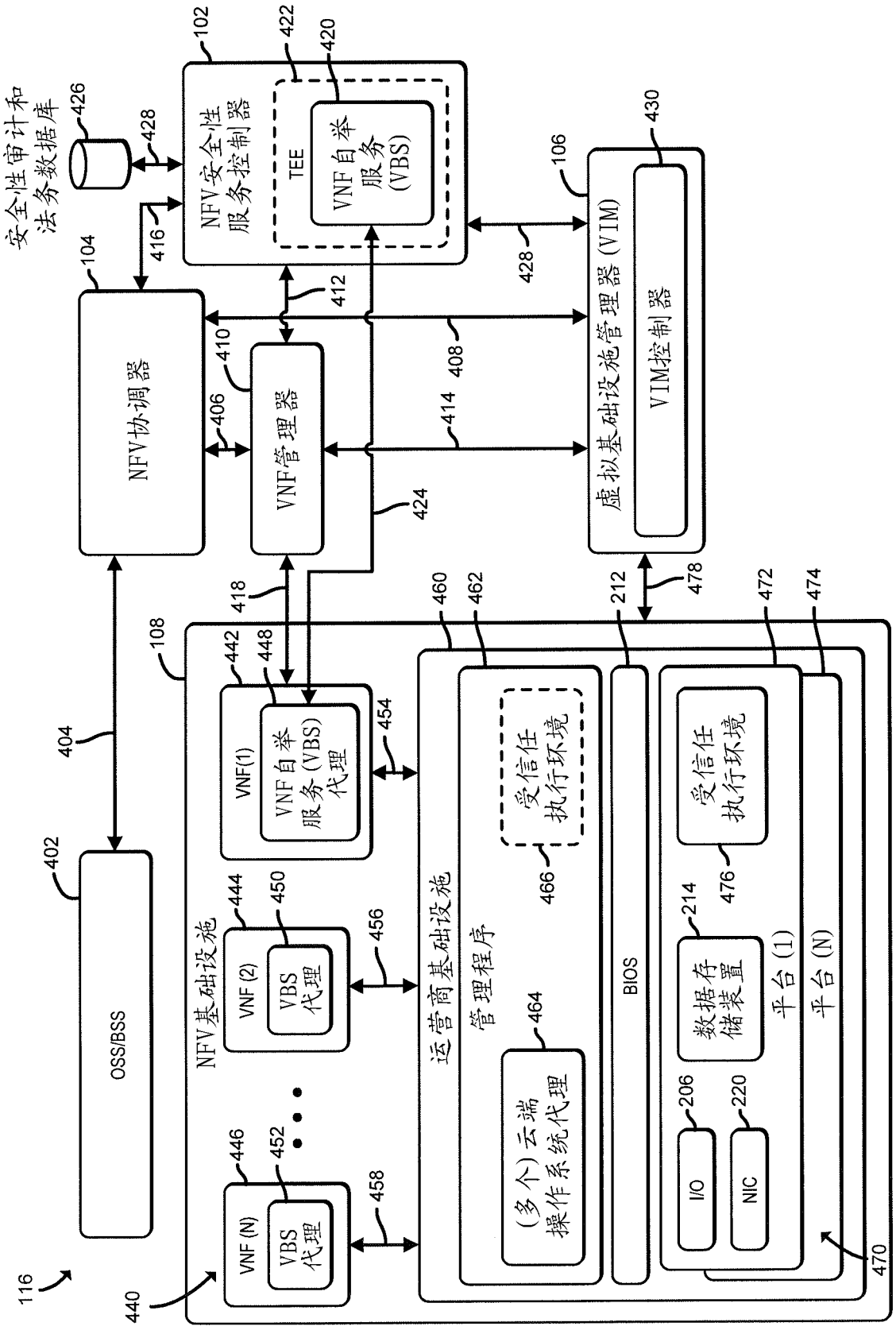

安全性审计和
法务数据库
426
428
102
NFV安全性
服务控制器
422
420
TEE
VNF 自举
服务
(VBS)
106
430
虚拟基础设施管理器 (VIM)
VIM控制器
416
104
NFV协调器
412
410
406
VNF管理器
408
414
424
418
460
462
212
478
472
474
108
404
442
448
VNF(1)
VNF 自举
服务 (VBS)
代理
454
受信任
执行环境
466
402
OSS/BSS
NFV基础设施
444
450
VNF (2)
VBS
代理
456
运营商基础设施
管理程序
BIOS
214
476
数据存
储装置
受信任
执行环境
平台 (1)
平台 (N)
446
452
VNF (N)
VBS
代理
458
(多个) 云端
操作系统代理
464
206
I/O
220
NIC
470
116
440

图 4

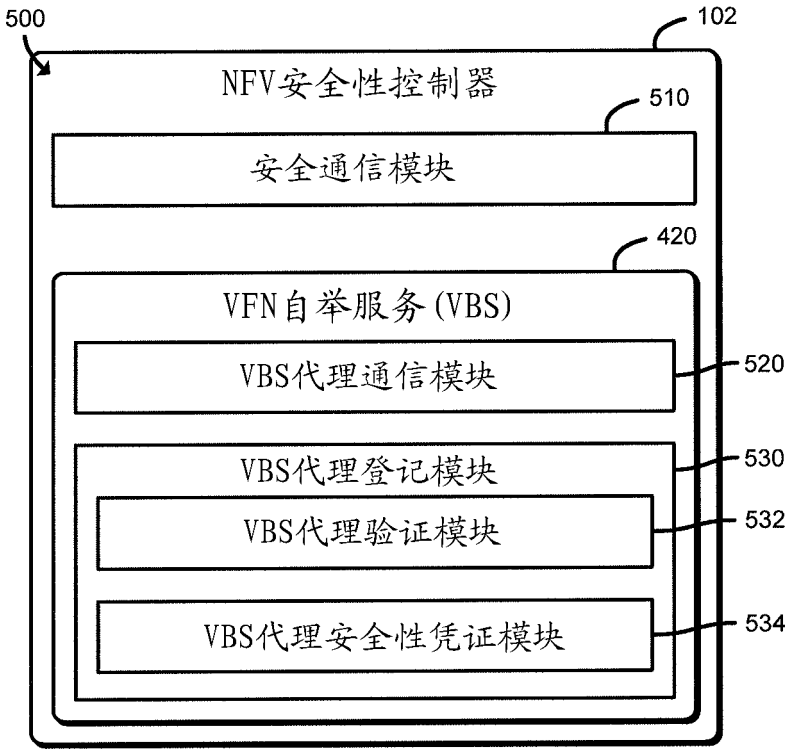

500
102
NFV安全性控制器
510
安全通信模块
420
VFN自举服务(VBS)
VBS代理通信模块
520
VBS代理登记模块
530
VBS代理验证模块
532
VBS代理安全性凭证模块
534

图 5

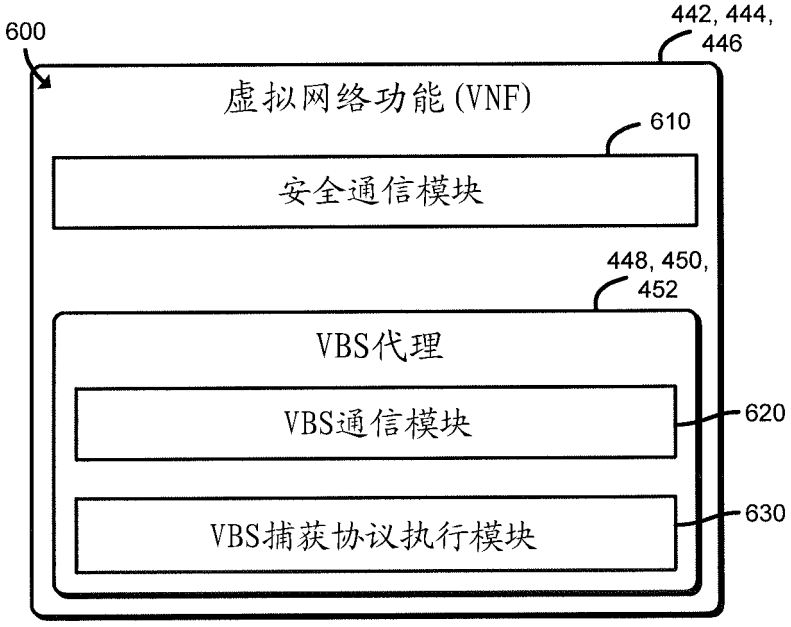

600
442, 444,
446
虚拟网络功能(VNF)
610
安全通信模块
448, 450,
452
VBS代理
VBS通信模块
620
VBS捕获协议执行模块
630

图 6

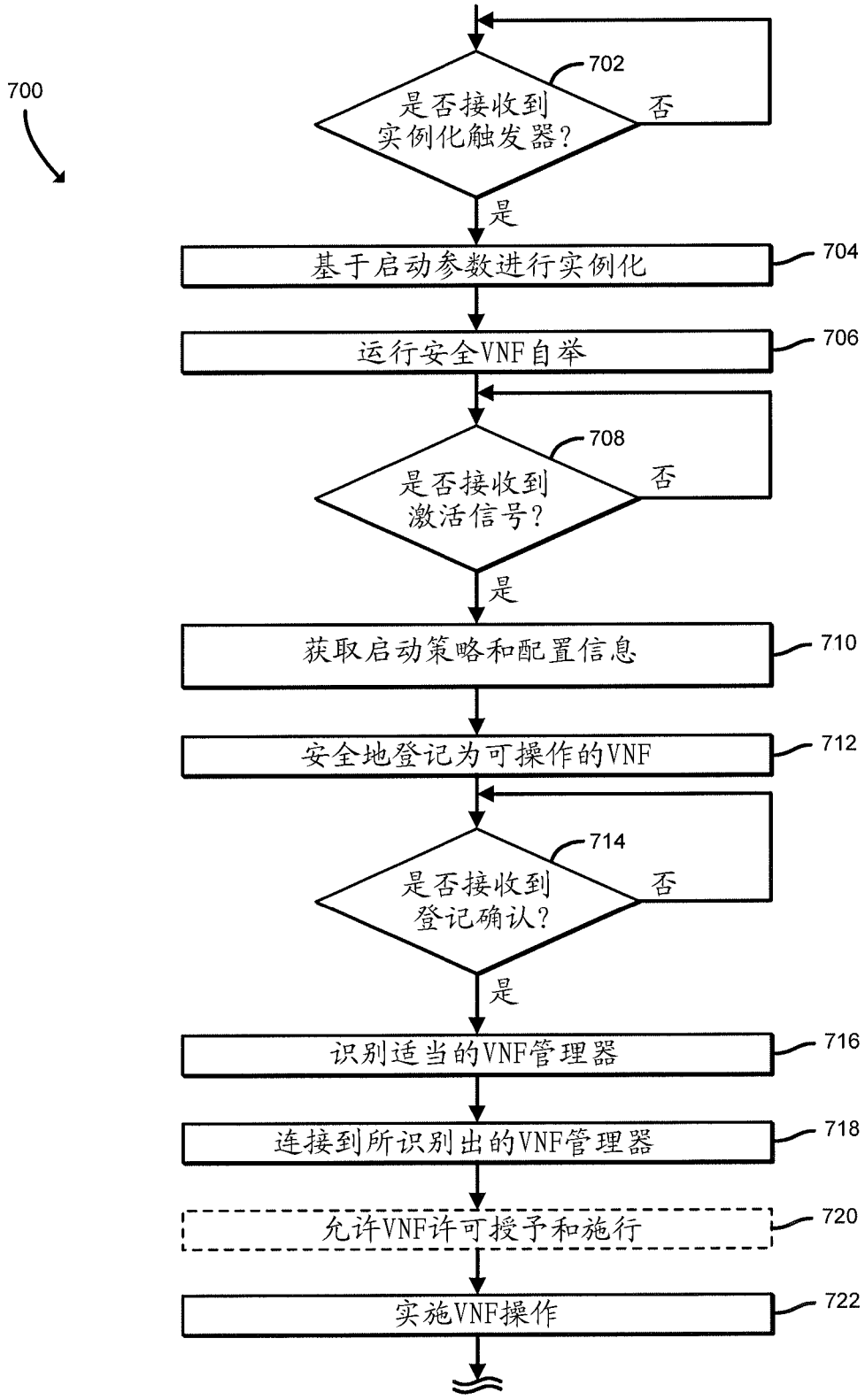

700
是否接收到实例化触发器?
702
否
是
基于启动参数进行实例化
704
运行安全VNF自举
706
是否接收到激活信号?
708
否
是
获取启动策略和配置信息
710
安全地登记为可操作的VNF
712
是否接收到登记确认?
714
否
是
识别适当的VNF管理器
716
连接到所识别出的VNF管理器
718
允许VNF许可授予和施行
720
实施VNF操作
722

图 7

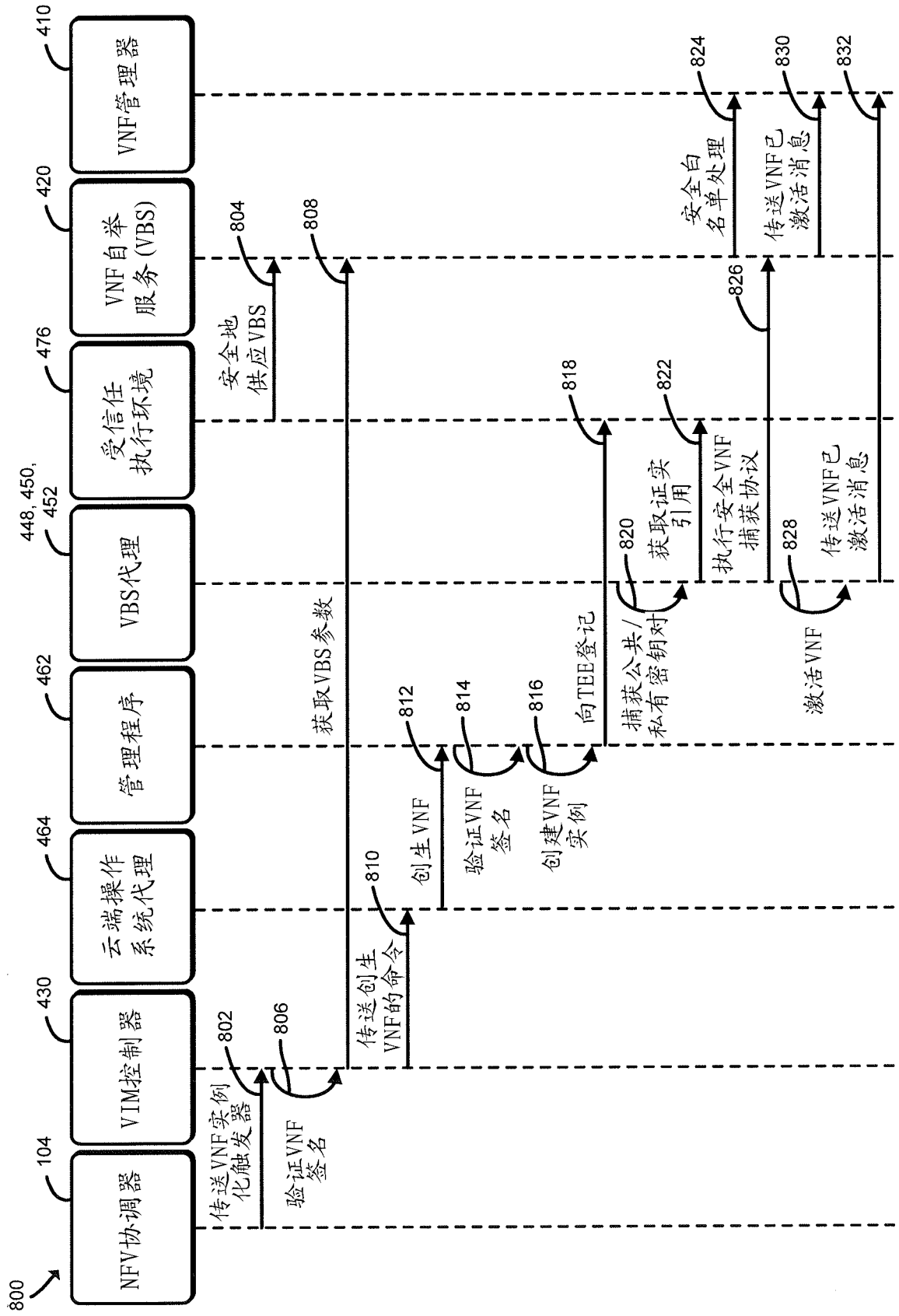

800
NFV协调器
104
VIM控制器
430
云端操作系统代理
464
管理程序
462
VBS代理
448, 450, 452
受信任执行环境
476
VNF自举服务(VBS)
420
VNF管理器
410
802 传送VNF实例化触发器
806 验证VNF签名
804 安全地供应VBS
808 获取VBS参数
810 传送创生VNF的命令
812 创生VNF
814 验证VNF签名
816 创建VNF实例
818 向TEE登记
820 捕获公共/私有密钥对
822 获取证实引用
826 执行安全VNF捕获协议
828 激活VNF
824 安全白名单处理
830 传送VNF已激活消息
832 传送VNF已激活消息

图 8

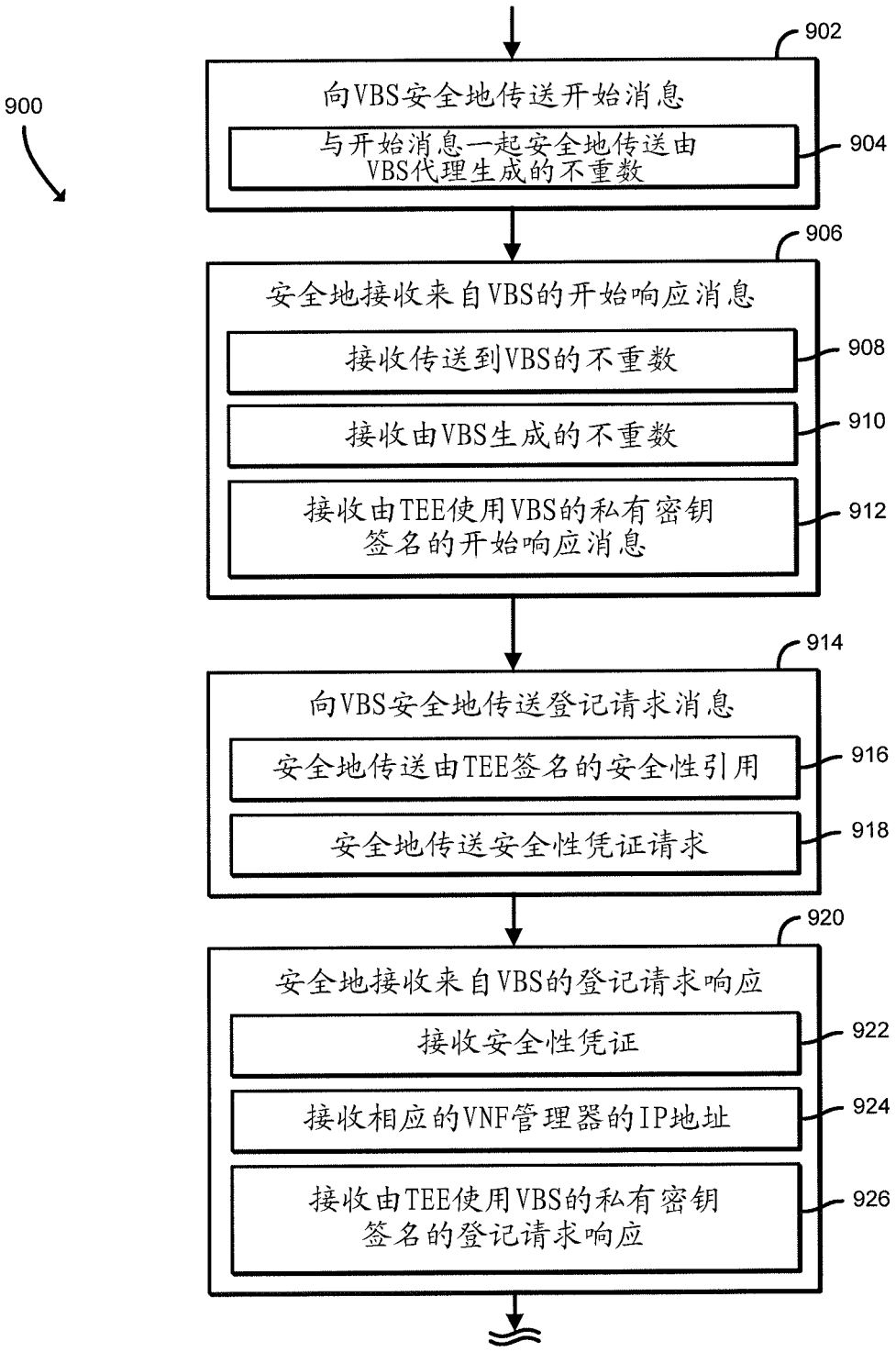

900
902
向VBS安全地传送开始消息
与开始消息一起安全地传送由VBS代理生成的不重数
904
906
安全地接收来自VBS的开始响应消息
接收传送到VBS的不重数
908
接收由VBS生成的不重数
910
接收由TEE使用VBS的私有密钥签名的开始响应消息
912
914
向VBS安全地传送登记请求消息
安全地传送由TEE签名的安全性引用
916
安全地传送安全性凭证请求
918
920
安全地接收来自VBS的登记请求响应
接收安全性凭证
922
接收相应的VNF管理器的IP地址
924
接收由TEE使用VBS的私有密钥签名的登记请求响应
926

图 9

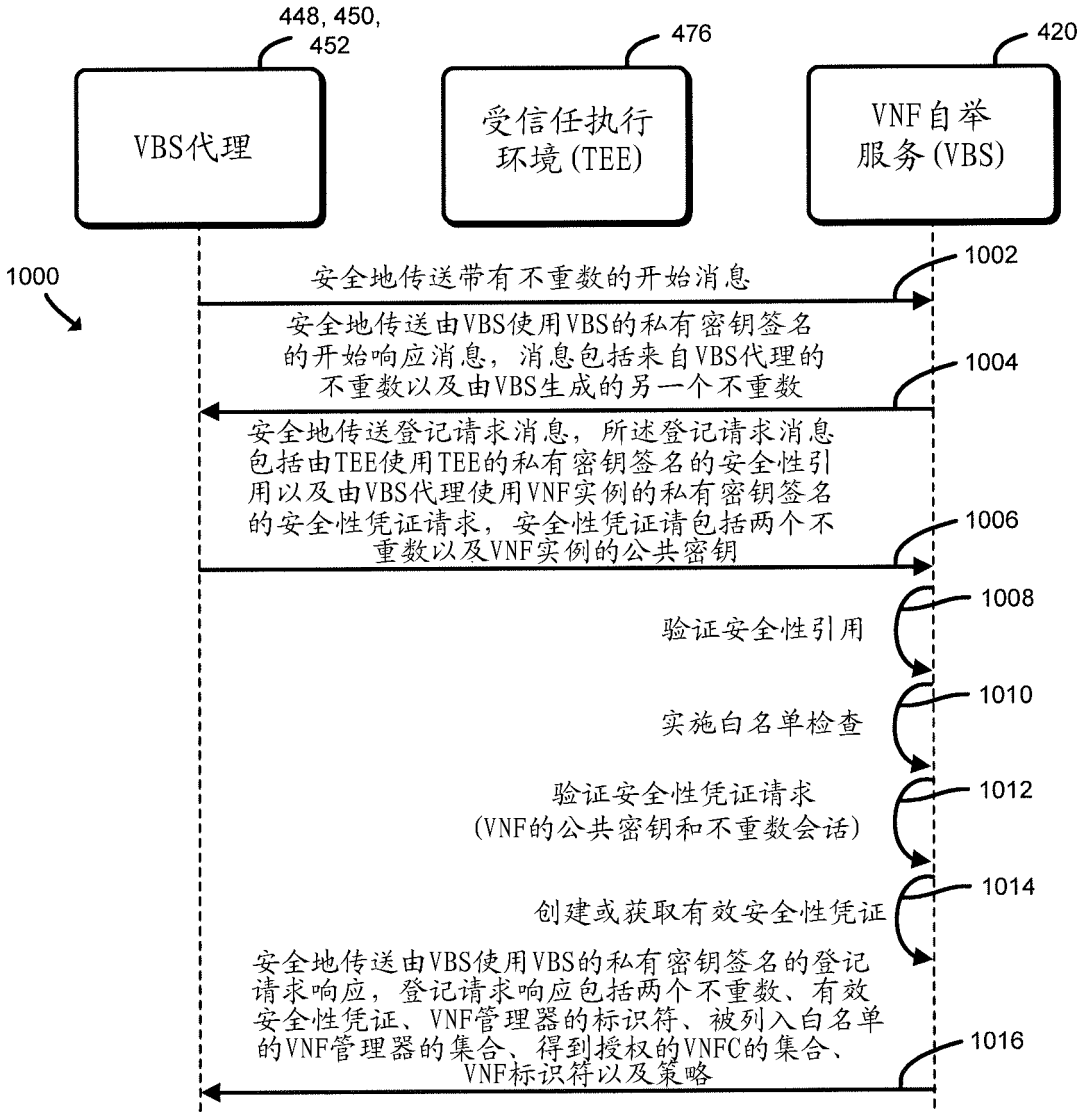

448, 450, 452
476
420
VBS代理
受信任执行环境(TEE)
VNF自举服务(VBS)
1000
1002
安全地传送带有不重数的开始消息
安全地传送由VBS使用VBS的私有密钥签名的开始响应消息，消息包括来自VBS代理的不重数以及由VBS生成的另一个不重数
1004
安全地传送登记请求消息，所述登记请求消息包括由TEE使用TEE的私有密钥签名的安全性引用以及由VBS代理使用VNF实例的私有密钥签名的安全性凭证请求，安全性凭证请包括两个不重数以及VNF实例的公共密钥
1006
1008
验证安全性引用
1010
实施白名单检查
1012
验证安全性凭证请求(VNF的公共密钥和不重数会话)
1014
创建或获取有效安全性凭证
安全地传送由VBS使用VBS的私有密钥签名的登记请求响应，登记请求响应包括两个不重数、有效安全性凭证、VNF管理器的标识符、被列入白名单的VNF管理器的集合、得到授权的VNFC的集合、VNF标识符以及策略
1016

图 10

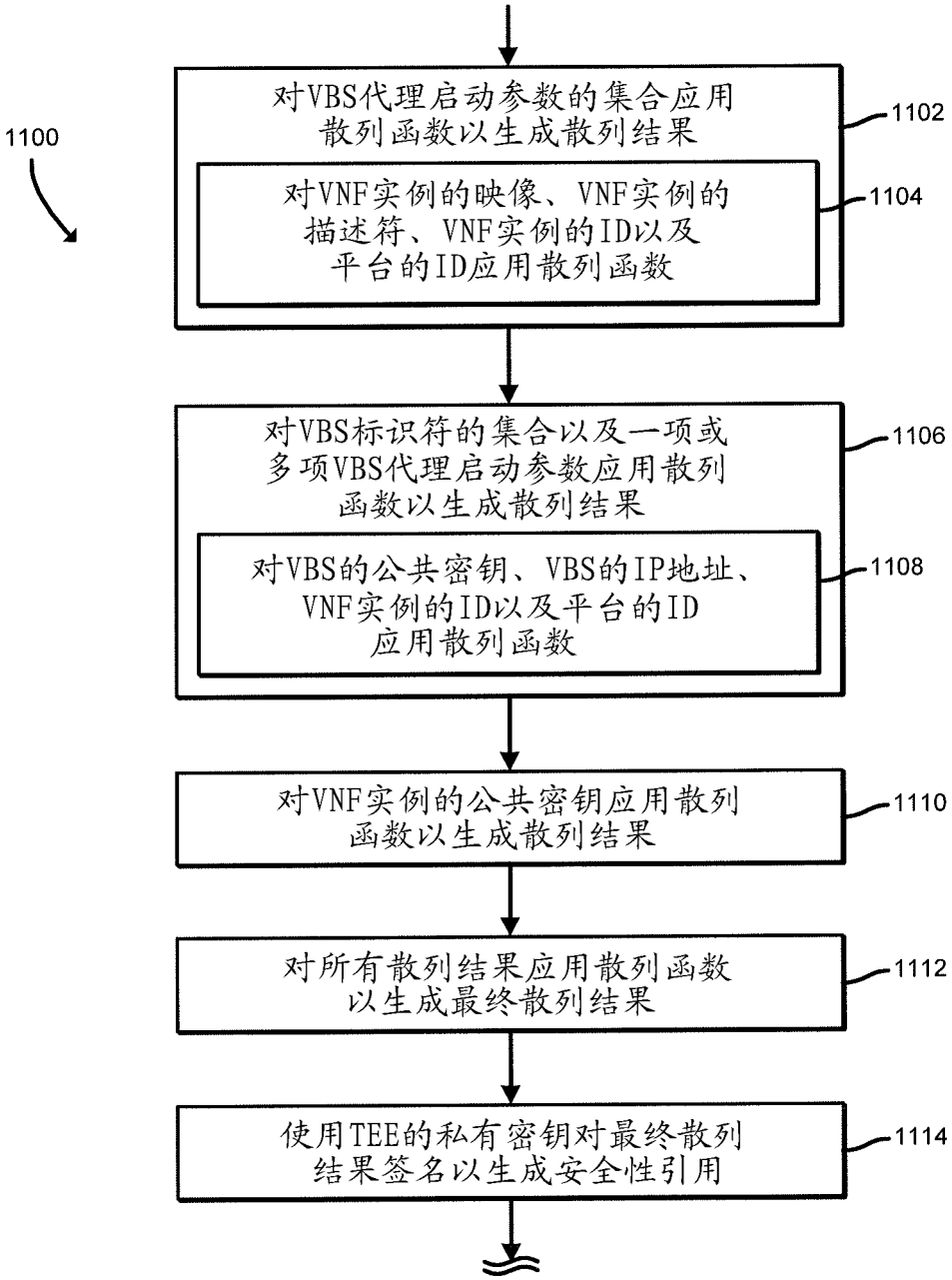

1100
对VBS代理启动参数的集合应用散列函数以生成散列结果
1102
对VNF实例的映像、VNF实例的描述符、VNF实例的ID以及平台的ID应用散列函数
1104
对VBS标识符的集合以及一项或多项VBS代理启动参数应用散列函数以生成散列结果
1106
对VBS的公共密钥、VBS的IP地址、VNF实例的ID以及平台的ID应用散列函数
1108
对VNF实例的公共密钥应用散列函数以生成散列结果
1110
对所有散列结果应用散列函数以生成最终散列结果
1112
使用TEE的私有密钥对最终散列结果签名以生成安全性引用
1114

图 11