



(12)发明专利

(10)授权公告号 CN 106464667 B

(45)授权公告日 2020.01.10

(21)申请号 201580016066.2

(72)发明人 冯成燕 王江胜

(22)申请日 2015.02.09

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274

(65)同一申请的已公布的文献号
申请公布号 CN 106464667 A

代理人 申健

(43)申请公布日 2017.02.22

(51)Int.Cl.

H04L 29/06(2006.01)

(85)PCT国际申请进入国家阶段日
2016.09.26

(56)对比文件

US 2008065778 A1,2008.03.13,

CN 101572707 A,2009.11.04,

CN 104980438 A,2015.10.14,

US 2010005319 A1,2010.01.07,

(86)PCT国际申请的申请数据
PCT/CN2015/072565 2015.02.09

审查员 张枫

(87)PCT国际申请的公布数据
W02016/127294 ZH 2016.08.18

(73)专利权人 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

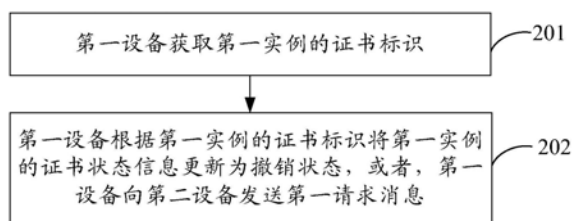
权利要求书7页 说明书22页 附图6页

(54)发明名称

一种证书管理方法、设备及系统

(57)摘要

本发明公开了一种证书管理方法、设备及系统,涉及通信领域,能够解决虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。具体方案为:第一设备获取第一实例的证书标识,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,第一请求消息用于请求撤销第一实例的证书。本发明用于证书管理。



1. 一种证书管理方法,其特征在于,应用于虚拟网络系统,包括:

第一设备获取第一实例的证书标识,所述第一实例为终止的实例;

所述第一设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态,或者,所述第一设备向第二设备发送第一请求消息,所述第一请求消息包含所述第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书;

所述第一设备获取第一实例的证书标识之前,还包括:

所述第一设备接收第一实例发送的第一实例的证书信息,所述第一实例发送的第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;

所述第一设备根据所述第一实例发送的第一实例的证书信息存储或更新所述第一实例的证书信息。

2. 根据权利要求1所述的方法,其特征在于,

所述第一实例的标识包括所述第一实例的ID,所述第一实例的证书标识包括所述第一实例的证书序列号。

3. 根据权利要求2所述的方法,其特征在于,

所述第一实例的ID为虚拟网络功能VNF ID,或虚拟网络功能组件VNFC ID,或虚拟机VM ID,或虚拟容器VC ID。

4. 根据权利要求1-3任一项所述的方法,其特征在于,所述第一设备接收第一实例发送的第一实例的证书信息之前,还包括:

所述第一设备向所述第一实例发送查询消息,所述查询消息包括所述第一实例的标识;

所述第一设备接收第一实例发送的第一实例的证书信息,包括:

所述第一设备接收所述第一实例发送的上报消息,所述上报消息包含所述第一实例发送的第一实例的证书信息。

5. 根据权利要求1所述的方法,其特征在于,所述第一设备获取第一实例的证书标识之前,还包括:

所述第一设备接收第三设备发送的第二请求消息,所述第二请求消息包含所述第一实例的标识,所述第二请求消息用于指示终止所述第一实例;

所述第一设备根据所述第二请求消息终止所述第一实例。

6. 根据权利要求5所述的方法,其特征在于,所述第一设备根据所述第二请求消息终止所述第一实例之后,还包括:

所述第一设备向所述第三设备发送第二确认消息,所述第二确认消息包含所述第一实例的标识,所述第二确认消息用于指示确认终止所述第一实例。

7. 根据权利要求5或6所述的方法,其特征在于,

所述第三设备为网络功能虚拟化编排器NFVO。

8. 根据权利要求1所述的方法,其特征在于,所述第一设备获取第一实例的证书标识之前,还包括:

所述第一设备接收第四设备发送的第一指示信息,所述第一指示信息用于指示所述第一实例崩溃,所述第一指示信息包含所述第一实例的标识,所述第一指示信息由所述第四设备通过第五设备转发至所述第一设备。

9. 根据权利要求8所述的方法,其特征在于,

所述第四设备为网络功能虚拟化基础设施NFVI,所述第五设备为虚拟设备管理器VIM。

10. 根据权利要求9所述的方法,其特征在于,所述第一设备接收第四设备发送的第一指示信息之后,还包括:

所述第一设备向所述VIM及所述NFVI发送第二指示信息,所述第二指示信息用于指示所述VIM删除所述第一实例对应的资源,并指示所述NFVI删除所述第一实例的证书及所述第一实例的证书对应的密钥。

11. 根据权利要求1所述的方法,其特征在于,所述第一设备获取第一实例的证书标识之前,还包括:

当所述第一设备检测到所述第一实例崩溃时,所述第一设备终止所述第一实例。

12. 根据权利要求1所述的方法,其特征在于,所述第一设备向第二设备发送第一请求消息之后,还包括:

所述第一设备接收所述第二设备发送的第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

13. 根据权利要求1-3、5-6、8-12中任一项所述的方法,其特征在于,所述第一设备获取第一实例的证书标识之后,还包括:

所述第一设备根据所述第一实例的证书标识删除所述第一实例的证书信息。

14. 根据权利要求1-3、5-6、8-12中任一项所述的方法,其特征在于,所述第一设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态,包括:

所述第一设备在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

15. 根据权利要求1-3、5-6、8-12中任一项所述的方法,其特征在于,

所述第一实例为虚拟网络功能VNF实例或虚拟网络功能组件VNFC实例。

16. 根据权利要求1-3、5-6、8-12中任一项所述的方法,其特征在于,

所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

17. 根据权利要求1-3、5-6、8-12中任一项所述的方法,其特征在于,

所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

18. 一种证书管理方法,其特征在于,应用于虚拟网络系统,包括:

第二设备接收第一设备发送的第一请求消息,所述第一请求消息包含第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书;

所述第二设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态;

其中,所述第二设备接收第一设备发送的第一请求消息之前,包括:

所述第一设备获取所述第一实例的证书标识,所述第一实例为终止的实例;

所述第一设备获取所述第一实例的证书标识之前,还包括:

所述第一设备接收所述第一实例发送的所述第一实例的证书信息,所述第一实例发送的所述第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;所述第一设备根据所述第一实例发送的第一实例的证书信息存储或更新所述第一实例的证书信息。

19. 根据权利要求18所述的方法, 其特征在于, 所述第二设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态, 包括:

所述第二设备在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

20. 根据权利要求18或19所述的方法, 其特征在于, 所述第二设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态之后, 还包括:

所述第二设备向所述第一设备发送第一确认消息, 所述第一确认消息用于指示确认撤销所述第一实例。

21. 根据权利要求18-19任一项所述的方法, 其特征在于,

所述第一实例为VNF实例或虚拟网络功能组件VNFC实例。

22. 根据权利要求18-19任一项所述的方法, 其特征在于,

所述第二设备为证书中心CA/注册中心RA, 或NFVO, 或在线证书状态协议OCSP服务器。

23. 根据权利要求18-19任一项所述的方法, 其特征在于,

所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

24. 一种第一设备, 其特征在于, 应用于虚拟网络系统, 包括:

获取单元, 用于获取第一实例的证书标识, 所述第一实例为终止的实例;

在所述获取单元获取第一实例的证书标识后,

证书管理单元, 用于根据所述获取单元获取的所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态;

或者, 发送单元, 用于向第二设备发送第一请求消息, 所述第一请求消息包含所述第一实例的证书标识, 所述第一请求消息用于请求撤销所述第一实例的证书;

所述第一设备还包括接收单元, 用于接收第一实例发送的第一实例的证书信息, 所述第一实例发送的第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;

所述证书管理单元, 还用于根据所述接收单元接收的所述第一实例发送的第一实例的证书信息存储或更新所述第一实例的证书信息。

25. 根据权利要求24所述的设备, 其特征在于,

所述第一实例的标识包括所述第一实例的ID, 所述第一实例的证书标识包括所述第一实例的证书序列号。

26. 根据权利要求25所述的设备, 其特征在于,

所述第一实例的ID为虚拟网络功能VNF ID, 或虚拟网络功能组件VNFC ID, 或虚拟机VM ID, 或虚拟容器VC ID。

27. 根据权利要求24-26任一项所述的设备, 其特征在于,

所述发送单元, 还用于向所述第一实例发送查询消息, 所述查询消息包括所述第一实例的标识;

所述接收单元, 还用于接收所述第一实例发送的上报消息, 所述上报消息包含所述第一实例发送的第一实例的证书信息。

28. 根据权利要求24所述的设备, 其特征在于,

所述第一设备还包括接收单元, 用于接收第三设备发送的第二请求消息, 所述第二请求消息包含所述第一实例的标识, 所述第二请求消息用于指示终止所述第一实例;

所述第一设备还包括实例管理单元,用于根据所述接收单元接收的所述第二请求消息终止所述第一实例。

29. 根据权利要求28所述的设备,其特征在于,

所述发送单元,还用于向所述第三设备发送第二确认消息,所述第二确认消息包含所述第一实例的标识,所述第二确认消息用于指示确认终止所述第一实例。

30. 根据权利要求28或29所述的设备,其特征在于,

所述第三设备为网络功能虚拟化编排器NFVO。

31. 根据权利要求24所述的设备,其特征在于,

所述第一设备还包括接收单元,用于接收第四设备发送的第一指示信息,所述第一指示信息用于指示所述第一实例崩溃,所述第一指示信息包含所述第一实例的标识,所述第一指示信息由所述第四设备通过第五设备转发至所述第一设备。

32. 根据权利要求31所述的设备,其特征在于,

所述第四设备为网络功能虚拟化基础设施NFVI,所述第五设备为虚拟基础设备管理器VIM。

33. 根据权利要求32所述的设备,其特征在于,

所述发送单元,还用于向所述VIM及所述NFVI发送第二指示信息,所述第二指示信息用于指示所述VIM删除所述第一实例对应的资源,并指示所述NFVI删除所述第一实例的证书及所述第一实例的证书对应的密钥。

34. 根据权利要求24所述的设备,其特征在于,

所述第一设备还包括实例管理单元,用于当检测到所述第一实例崩溃时,所述第一设备终止所述第一实例。

35. 根据权利要求24所述的设备,其特征在于,

所述第一设备还包括接收单元,用于接收所述第二设备发送的第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

36. 根据权利要求24-26、28-29、31-35中任一项所述的设备,其特征在于,

所述证书管理单元,还用于根据所述第一实例的证书标识删除所述第一实例的证书信息。

37. 根据权利要求24-26、28-29、31-35中任一项所述的设备,其特征在于,

所述证书管理单元,具体用于在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

38. 根据权利要求24-26、28-29、31-35中任一项所述的设备,其特征在于,

所述第一实例为虚拟网络功能VNF实例或虚拟网络功能组件VNFC实例。

39. 根据权利要求24-26、28-29、31-35中任一项所述的设备,其特征在于,

所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

40. 根据权利要求24-26、28-29、31-35中任一项所述的设备,其特征在于,

所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

41. 一种第二设备,其特征在于,应用于虚拟网络系统,包括:

接收单元,用于接收第一设备发送的第一请求消息,所述第一请求消息包含第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书;

证书管理单元,用于根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态;

其中,

所述接收单元接收第一设备发送的第一请求消息之前:

所述第一设备获取所述第一实例的证书标识,所述第一实例为终止的实例;

所述第一设备获取所述第一实例的证书标识之前,还包括:

所述第一设备接收所述第一实例发送的所述第一实例的证书信息,所述第一实例发送的所述第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;所述第一设备根据所述第一实例发送的第一实例的证书信息存储或更新所述第一实例的证书信息。

42. 根据权利要求41所述的设备,其特征在于,

所述证书管理单元,具体用于在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

43. 根据权利要求41或42所述的设备,其特征在于,

所述第二设备还包括发送单元,用于向所述第一设备发送第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

44. 根据权利要求41-42任一项所述的设备,其特征在于,

所述第一实例为VNF实例或虚拟网络功能组件VNFC实例。

45. 根据权利要求41-42任一项所述的设备,其特征在于,

所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

46. 根据权利要求41-42任一项所述的设备,其特征在于,

所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

47. 一种第一设备,其特征在于,应用于虚拟网络系统,包括:处理器、存储器、总线、发送器,所述处理器、所述存储器及所述发送器通过所述总线相互连接;

其中,所述处理器,用于获取第一实例的证书标识,所述第一实例为终止的实例;

在所述处理器获取第一实例的证书标识后,

所述处理器,还用于根据获取的所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态;

或者,所述发送器,用于向第二设备发送第一请求消息,所述第一请求消息包含所述第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书;

所述第一设备还包括接收器,用于接收第一实例发送的第一实例的证书信息,所述第一实例发送的第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;

所述处理器,还用于根据所述接收器接收的所述第一实例发送的第一实例的证书信息存储或更新所述第一实例的证书信息。

48. 根据权利要求47所述的设备,其特征在于,

所述第一实例的标识包括所述第一实例的ID,所述第一实例的证书标识包括所述第一实例的证书序列号。

49. 根据权利要求48所述的设备,其特征在于,

所述第一实例的ID为虚拟网络功能VNF ID,或虚拟网络功能组件VNFC ID,或虚拟机VM

ID,或虚拟容器VC ID。

50. 根据权利要求47-49任一项所述的设备,其特征在于,

所述发送器,还用于向所述第一实例发送查询消息,所述查询消息包括所述第一实例的标识;

所述接收器,还用于接收所述第一实例发送的上报消息,所述上报消息包含所述第一实例发送的第一实例的证书信息。

51. 根据权利要求47所述的设备,其特征在于,

所述第一设备还包括接收器,用于接收第三设备发送的第二请求消息,所述第二请求消息包含所述第一实例的标识,所述第二请求消息用于指示终止所述第一实例;

所述处理器,还用于根据所述接收器接收的所述第二请求消息终止所述第一实例。

52. 根据权利要求51所述的设备,其特征在于,

所述发送器,还用于向所述第三设备发送第二确认消息,所述第二确认消息包含所述第一实例的标识,所述第二确认消息用于指示确认终止所述第一实例。

53. 根据权利要求51或52所述的设备,其特征在于,

所述第三设备为网络功能虚拟化编排器NFVO。

54. 根据权利要求47所述的设备,其特征在于,

所述第一设备还包括接收器,用于接收第四设备发送的第一指示信息,所述第一指示信息用于指示所述第一实例崩溃,所述第一指示信息包含所述第一实例的标识,所述第一指示信息由所述第四设备通过第五设备转发至所述第一设备。

55. 根据权利要求54所述的设备,其特征在于,

所述第四设备为网络功能虚拟化基础设施NFVI,所述第五设备为虚拟基础设备管理器VIM。

56. 根据权利要求55所述的设备,其特征在于,

所述发送器,还用于向所述VIM及所述NFVI发送第二指示信息,所述第二指示信息用于指示所述VIM删除所述第一实例对应的资源,并指示所述NFVI删除所述第一实例的证书及所述第一实例的证书对应的密钥。

57. 根据权利要求47所述的设备,其特征在于,

所述处理器,还用于当检测到所述第一实例崩溃时,所述第一设备终止所述第一实例。

58. 根据权利要求47所述的设备,其特征在于,

所述第一设备还包括接收器,用于接收所述第二设备发送的第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

59. 根据权利要求47-49、51-52、54-58中任一项所述的设备,其特征在于,

所述处理器,还用于根据所述第一实例的证书标识删除所述第一实例的证书信息。

60. 根据权利要求47-49、51-52、54-58中任一项所述的设备,其特征在于,

所述处理器,具体用于在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

61. 根据权利要求47-49、51-52、54-58中任一项所述的设备,其特征在于,

所述第一实例为虚拟网络功能VNF实例或虚拟网络功能组件VNFC实例。

62. 根据权利要求47-49、51-52、54-58中任一项所述的设备,其特征在于,

所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

63. 根据权利要求47-49、51-52、54-58中任一项所述的设备,其特征在于,

所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

64. 一种第二设备,其特征在于,应用于虚拟网络系统,包括:处理器、存储器、总线及接收器,所述处理器、所述存储器及所述接收器通过所述总线相互连接;

其中,所述接收器,用于接收第一设备发送的第一请求消息,所述第一请求消息包含第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书;

所述处理器,用于根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态;

其中,

所述接收器接收第一设备发送的第一请求消息之前:

所述第一设备获取所述第一实例的证书标识,所述第一实例为终止的实例;

所述第一设备获取所述第一实例的证书标识之前,还包括:

所述第一设备接收所述第一实例发送的所述第一实例的证书信息,所述第一实例发送的所述第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;所述第一设备根据所述第一实例发送的所述第一实例的证书信息存储或更新所述第一实例的证书信息。

65. 根据权利要求64所述的设备,其特征在于,

所述处理器,具体用于在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

66. 根据权利要求64或65所述的设备,其特征在于,

所述第二设备还包括发送器,用于向所述第一设备发送第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

67. 根据权利要求64-65中任一项所述的设备,其特征在于,

所述第一实例为VNF实例或虚拟网络功能组件VNFC实例。

68. 根据权利要求64-65中任一项所述的设备,其特征在于,

所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

69. 根据权利要求64-65中任一项所述的设备,其特征在于,

所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

70. 一种虚拟网络系统,其特征在于,包括:第一设备及第二设备;

其中,所述第一设备为权利要求24-40任一项所述的第一设备,所述第二设备为权利要求41-46任一项所述的第二设备;

或者,所述第一设备为权利要求47-63任一项所述的第一设备,所述第二设备为权利要求64-69任一项所述的第二设备。

一种证书管理方法、设备及系统

技术领域

[0001] 本发明涉及通信领域,尤其涉及一种证书管理方法、设备及系统。

背景技术

[0002] NFV (Network Function Virtualization,网络功能虚拟化)通过在通用的服务器、交换机、存储器等硬件设备上建立VNF (Virtualised Network Function,虚拟网络功能)实现部分网络功能,使得这些网络功能在通用的硬件设备上运行,不需要配置新的专用网元设备,能够极大的增强网络部署的灵活性,并且降低了投资成本。

[0003] 在通过NFV技术实现网络功能的过程中,虚拟网络内部VNF之间互相通信,或者VNF与外部网络通信都存在安全隐患,因此,现有技术中采用IPSec (Internet Protocol Security,互联网协议安全)或TLS (Transport Layer Security,传输层安全协议)等技术建立网络中的连接。这些安全技术需要相互通信的双方配置证书,证书包含通信双方用于验证的密钥及算法。

[0004] 在虚拟化场景下,VNF是一组软件,在需要的时候进行实例化和终止。所谓VNF的实例化,是指为一个VNF分配资源和安装软件的过程;所谓终止,是指解除对该VNF分配的资源的过程。在实现上述功能的过程中,发明人发现,当VNF实例终止后,分配给该VNF实例的资源回收后可能会分配给其他VNF,此时,原来VNF实例存储证书信息的存储资源分配给了其他VNF,这就使得原来VNF实例的证书会被其他VNF获取,导致签发给原VNF或VNFC (Virtualised Network Function Component,虚拟网络功能组件)实例的证书可能被攻击者非法获取,降低了虚拟网络系统的通信安全。

发明内容

[0005] 本发明的实施例提供一种证书管理方法、设备及系统,能够解决虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0006] 为达到上述目的,本发明的实施例采用如下技术方案:

[0007] 第一方面,本发明实施例提供一种证书管理方法,应用于虚拟网络系统,包括:

[0008] 第一设备获取第一实例的证书标识,所述第一实例为终止的实例;

[0009] 所述第一设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态,或者,所述第一设备向第二设备发送第一请求消息,所述第一请求消息包含所述第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书。

[0010] 结合第一方面,在第一方面的第一种可能的实现方式中,所述第一设备获取第一实例的证书标识之前,还包括:

[0011] 所述第一设备接收第一实例发送的第一实例的证书信息,所述第一实例发送的第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;

[0012] 所述第一设备根据所述第一实例发送的第一实例的证书信息存储或更新所述第

一实例的证书信息。

[0013] 结合第一方面的第一种可能的实现方式,在第一方面的第二种可能的实现方式中,

[0014] 所述第一实例的标识包括所述第一实例的ID,所述第一实例的证书标识包括所述第一实例的证书序列号。

[0015] 结合第一方面的第二种可能的实现方式,在第一方面的第三种可能的实现方式中,

[0016] 所述第一实例的ID为虚拟网络功能VNF ID,或虚拟网络功能组件VNFC ID,或虚拟机VM ID,或虚拟容器VC ID。

[0017] 结合第一方面的第一种可能的实现方式至第一方面的第三种可能的实现方式中任一实现方式,在第一方面的第四种可能的实现方式中,所述第一设备接收第一实例发送的第一实例的证书信息之前,还包括:

[0018] 所述第一设备向所述第一实例发送查询消息,所述查询消息包括所述第一实例的标识;

[0019] 所述第一设备接收第一实例发送的第一实例的证书信息,包括:

[0020] 所述第一设备接收所述第一实例发送的上报消息,所述上报消息包含所述第一实例发送的第一实例的证书信息。

[0021] 结合第一方面,在第一方面的第五种可能的实现方式中,所述第一设备获取第一实例的证书标识之前,还包括:

[0022] 所述第一设备接收第三设备发送的第二请求消息,所述第二请求消息包含所述第一实例的标识,所述第二请求消息用于指示终止所述第一实例;

[0023] 所述第一设备根据所述第二请求消息终止所述第一实例。

[0024] 结合第一方面的第五种可能的实现方式,在第一方面的第六种可能的实现方式中,所述第一设备根据所述第二请求消息终止所述第一实例之后,还包括:

[0025] 所述第一设备向所述第三设备发送第二确认消息,所述第二确认消息包含所述第一实例的标识,所述第二确认消息用于指示确认终止所述第一实例。

[0026] 结合第一方面的第五种可能的实现方式或第一方面的第六种可能的实现方式,在第一方面的第七种可能的实现方式中,

[0027] 所述第三设备为网络功能虚拟化编排器NFVO。

[0028] 结合第一方面,在第一方面的第八种可能的实现方式中,

[0029] 所述第一设备获取第一实例的证书标识之前,还包括:

[0030] 所述第一设备接收第四设备发送的第一指示信息,所述第一指示信息用于指示所述第一实例崩溃,所述第一指示信息包含所述第一实例的标识,所述第一指示信息由所述第四设备通过第五设备转发至所述第一设备。

[0031] 结合第一方面的第八种可能的实现方式,在第一方面的第九种可能的实现方式中,

[0032] 所述第四设备为网络功能虚拟化基础设施NFVI,所述第五设备为虚拟基础设备管理器VIM。

[0033] 结合第一方面的第九种可能的实现方式,在第一方面的第十种可能的实现方式

中,所述第一设备接收第四设备发送的第一指示信息之后,还包括:

[0034] 所述第一设备向所述VIM及所述NFVI发送第二指示信息,所述第二指示信息用于指示所述VIM删除所述第一实例对应的资源,并指示所述NFVI删除所述第一实例的证书及所述第一实例的证书对应的密钥。

[0035] 结合第一方面,在第一方面的第十一种可能的实现方式中,所述第一设备获取第一实例的证书标识之前,还包括:

[0036] 当所述第一设备检测到所述第一实例崩溃时,所述第一设备终止所述第一实例。

[0037] 结合第一方面,在第一方面的第十二种可能的实现方式中,所述第一设备向第二设备发送第一请求消息之后,还包括:

[0038] 所述第一设备接收所述第二设备发送的第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

[0039] 结合第一方面至第一方面的第十二种可能的实现方式中任一实现方式,在第一方面的第十三种可能的实现方式中,所述第一设备获取第一实例的证书标识之后,还包括:

[0040] 所述第一设备根据所述第一实例的证书标识删除所述第一实例的证书信息。

[0041] 结合第一方面至第一方面的第十三种可能的实现方式中任一实现方式,在第一方面的第十四种可能的实现方式中,所述第一设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态,包括:

[0042] 所述第一设备在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

[0043] 结合第一方面至第一方面的第十四种可能的实现方式中任一实现方式,在第一方面的第十五种可能的实现方式中,

[0044] 所述第一实例为虚拟网络功能VNF实例或虚拟网络功能组件VNFC实例。

[0045] 结合第一方面至第一方面的第十五种可能的实现方式中任一实现方式,在第一方面的第十六种可能的实现方式中,

[0046] 所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0047] 结合第一方面至第一方面的第十六种可能的实现方式中任一实现方式,在第一方面的第十七种可能的实现方式中,

[0048] 所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0049] 第二方面,本发明实施例提供一种证书管理方法,应用于虚拟网络系统,包括:

[0050] 第二设备接收第一设备发送的第一请求消息,所述第一请求消息包含第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书;

[0051] 所述第二设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态。

[0052] 结合第二方面,在第二方面的第一种可能的实现方式中,所述第二设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态,包括:

[0053] 所述第二设备在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

[0054] 结合第二方面或第二方面的第一种可能的实现方式,在第二方面的第二种可能的实现方式中,所述第二设备根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态之后,还包括:

[0055] 所述第二设备向所述第一设备发送第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

[0056] 结合第二方面至第二方面的第二种可能的实现方式中任一实现方式,在第二方面的第三种可能的实现方式中,

[0057] 所述第一实例为VNF实例或虚拟网络功能组件VNFC实例。

[0058] 结合第二方面至第二方面的第三种可能的实现方式中任一实现方式,在第二方面的第四种可能的实现方式中,

[0059] 所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0060] 结合第二方面至第二方面的第四种可能的实现方式中任一实现方式,在第二方面的第五种可能的实现方式中,

[0061] 所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0062] 第三方面,本发明实施例提供一种第一设备,应用于虚拟网络系统,包括:

[0063] 获取单元,用于获取第一实例的证书标识,所述第一实例为终止的实例;

[0064] 在所述获取单元获取第一实例的证书标识后,

[0065] 证书管理单元,用于根据所述获取单元获取的所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态;

[0066] 或者,发送单元,用于向第二设备发送第一请求消息,所述第一请求消息包含所述第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书。

[0067] 结合第三方面,在第三方面的第一种可能的实现方式中,

[0068] 所述第一设备还包括接收单元,用于接收第一实例发送的第一实例的证书信息,所述第一实例发送的第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;

[0069] 所述证书管理单元,还用于根据所述接收单元接收的所述第一实例发送的第一实例的证书信息存储或更新所述第一实例的证书信息。

[0070] 结合第三方面的第一种可能的实现方式,在第三方面的第二种可能的实现方式中,

[0071] 所述第一实例的标识包括所述第一实例的ID,所述第一实例的证书标识包括所述第一实例的证书序列号。

[0072] 结合第三方面的第二种可能的实现方式,在第三方面的第三种可能的实现方式中,

[0073] 所述第一实例的ID为虚拟网络功能VNF ID,或虚拟网络功能组件VNFC ID,或虚拟机VM ID,或虚拟容器VC ID。

[0074] 结合第三方面的第一种可能的实现方式至第三方面的第三种可能的实现方式中任一实现方式,在第三方面的第四种可能的实现方式中,

[0075] 所述发送单元,还用于向所述第一实例发送查询消息,所述查询消息包括所述第一实例的标识;

[0076] 所述接收单元,还用于接收所述第一实例发送的上报消息,所述上报消息包含所述第一实例发送的第一实例的证书信息。

- [0077] 结合第三方面,在第三方面的第五种可能的实现方式中,
- [0078] 所述第一设备还包括接收单元,用于接收第三设备发送的第二请求消息,所述第二请求消息包含所述第一实例的标识,所述第二请求消息用于指示终止所述第一实例;
- [0079] 所述第一设备还包括实例管理单元,用于根据所述接收单元接收的所述第二请求消息终止所述第一实例。
- [0080] 结合第三方面的第五种可能的实现方式,在第三方面的第六种可能的实现方式中,
- [0081] 所述发送单元,还用于向所述第三设备发送第二确认消息,所述第二确认消息包含所述第一实例的标识,所述第二确认消息用于指示确认终止所述第一实例。
- [0082] 结合第三方面的第五种可能的实现方式或第三方面的第六种可能的实现方式,在第三方面的第七种可能的实现方式中,
- [0083] 所述第三设备为网络功能虚拟化编排器NFVO。
- [0084] 结合第三方面,在第三方面的第八种可能的实现方式中,
- [0085] 所述第一设备还包括接收单元,用于接收第四设备发送的第一指示信息,所述第一指示信息用于指示所述第一实例崩溃,所述第一指示信息包含所述第一实例的标识,所述第一指示信息由所述第四设备通过第五设备转发至所述第一设备。
- [0086] 结合第三方面的第八种可能的实现方式,在第三方面的第九种可能的实现方式中,
- [0087] 所述第四设备为网络功能虚拟化基础设施NFVI,所述第五设备为虚拟基础设备管理器VIM。
- [0088] 结合第三方面的第九种可能的实现方式,在第三方面的第十种可能的实现方式中,
- [0089] 所述发送单元,还用于向所述VIM及所述NFVI发送第二指示信息,所述第二指示信息用于指示所述VIM删除所述第一实例对应的资源,并指示所述NFVI删除所述第一实例的证书及所述第一实例的证书对应的密钥。
- [0090] 结合第三方面,在第三方面的第十一种可能的实现方式中,
- [0091] 所述第一设备还包括实例管理单元,用于当检测到所述第一实例崩溃时,所述第一设备终止所述第一实例。
- [0092] 结合第三方面,在第三方面的第十二种可能的实现方式中,
- [0093] 所述第一设备还包括接收单元,用于接收所述第二设备发送的第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。
- [0094] 结合第三方面至第三方面的第十二种可能的实现方式中任一实现方式,在第三方面的第十三种可能的实现方式中,
- [0095] 所述证书管理单元,还用于根据所述第一实例的证书标识删除所述第一实例的证书信息。
- [0096] 结合第三方面至第三方面的第十三种可能的实现方式中任一实现方式,在第三方面的第十四种可能的实现方式中,
- [0097] 所述证书管理单元,具体用于在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

[0098] 结合第三方面至第三方面的第十四种可能的实现方式中任一实现方式,在第三方面的第十五种可能的实现方式中,

[0099] 所述第一实例为虚拟网络功能VNF实例或虚拟网络功能组件VNFC实例。

[0100] 结合第三方面至第三方面的第十五种可能的实现方式中任一实现方式,在第三方面的第十六种可能的实现方式中,

[0101] 所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0102] 结合第三方面至第三方面的第十六种可能的实现方式中任一实现方式,在第三方面的第十七种可能的实现方式中,

[0103] 所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0104] 第四方面,本发明实施例提供一种第二设备,应用于虚拟网络系统,包括:

[0105] 接收单元,用于接收第一设备发送的第一请求消息,所述第一请求消息包含第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书;

[0106] 证书管理单元,用于根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态。

[0107] 结合第四方面,在第四方面的第一种可能的实现方式中,

[0108] 所述证书管理单元,具体用于在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

[0109] 结合第四方面或第四方面的第一种可能的实现方式,在第四方面的第二种可能的实现方式中,

[0110] 所述第二设备还包括发送单元,用于向所述第一设备发送第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

[0111] 结合第四方面至第四方面的第二种可能的实现方式中任一实现方式,在第四方面的第三种可能的实现方式中,

[0112] 所述第一实例为VNF实例或虚拟网络功能组件VNFC实例。

[0113] 结合第四方面至第四方面的第三种可能的实现方式中任一实现方式,在第四方面的第四种可能的实现方式中,

[0114] 所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0115] 结合第四方面至第四方面的第四种可能的实现方式中任一实现方式,在第四方面的第五种可能的实现方式中,

[0116] 所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0117] 第五方面,本发明实施例提供一种第一设备,应用于虚拟网络系统,包括:处理器、存储器、总线、发送器,所述处理器、所述存储器及所述发送器通过所述总线相互连接;

[0118] 其中,所述处理器,用于获取第一实例的证书标识,所述第一实例为终止的实例;

[0119] 在所述处理器获取第一实例的证书标识后,

[0120] 所述处理器,还用于根据获取的所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态;

[0121] 或者,所述发送器,用于向第二设备发送第一请求消息,所述第一请求消息包含所

述第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书。

[0122] 结合第五方面,在第五方面的第一种可能的实现方式中,

[0123] 所述第一设备还包括接收器,用于接收第一实例发送的第一实例的证书信息,所述第一实例发送的第一实例的证书信息包括所述第一实例的标识及所述第一实例的证书标识;

[0124] 所述处理器,还用于根据所述接收器接收的所述第一实例发送的第一实例的证书信息存储或更新所述第一实例的证书信息。

[0125] 结合第五方面的第一种可能的实现方式,在第五方面的第二种可能的实现方式中,

[0126] 所述第一实例的标识包括所述第一实例的ID,所述第一实例的证书标识包括所述第一实例的证书序列号。

[0127] 结合第五方面的第二种可能的实现方式,在第五方面的第三种可能的实现方式中,

[0128] 所述第一实例的ID为虚拟网络功能VNF ID,或虚拟网络功能组件VNFC ID,或虚拟机VM ID,或虚拟容器VC ID。

[0129] 结合第五方面的第一种可能的实现方式至第五方面的第三种可能的实现方式中任一实现方式,在第五方面的第四种可能的实现方式中,

[0130] 所述发送器,还用于向所述第一实例发送查询消息,所述查询消息包括所述第一实例的标识;

[0131] 所述接收器,还用于接收所述第一实例发送的上报消息,所述上报消息包含所述第一实例发送的第一实例的证书信息。

[0132] 结合第五方面,在第五方面的第五种可能的实现方式中,

[0133] 所述第一设备还包括接收器,用于接收第三设备发送的第二请求消息,所述第二请求消息包含所述第一实例的标识,所述第二请求消息用于指示终止所述第一实例;

[0134] 所述处理器,还用于根据所述接收器接收的所述第二请求消息终止所述第一实例。

[0135] 结合第五方面的第五种可能的实现方式,在第五方面的第六种可能的实现方式中,

[0136] 所述发送器,还用于向所述第三设备发送第二确认消息,所述第二确认消息包含所述第一实例的标识,所述第二确认消息用于指示确认终止所述第一实例。

[0137] 结合第五方面的第五种可能的实现方式或第五方面的第六种可能的实现方式,在第五方面的第七种可能的实现方式中,

[0138] 所述第三设备为网络功能虚拟化编排器NFVO。

[0139] 结合第五方面,在第五方面的第八种可能的实现方式中,

[0140] 所述第一设备还包括接收器,用于接收第四设备发送的第一指示信息,所述第一指示信息用于指示所述第一实例崩溃,所述第一指示信息包含所述第一实例的标识,所述第一指示信息由所述第四设备通过第五设备转发至所述第一设备。

[0141] 结合第五方面的第八种可能的实现方式,在第五方面的第九种可能的实现方式中,

[0142] 所述第四设备为网络功能虚拟化基础设施NFVI,所述第五设备为虚拟设备管理器VIM。

[0143] 结合第五方面的第九种可能的实现方式,在第五方面的第十种可能的实现方式中,

[0144] 所述发送器,还用于向所述VIM及所述NFVI发送第二指示信息,所述第二指示信息用于指示所述VIM删除所述第一实例对应的资源,并指示所述NFVI删除所述第一实例的证书及所述第一实例的证书对应的密钥。

[0145] 结合第五方面,在第五方面的第十一种可能的实现方式中,

[0146] 所述处理器,还用于当检测到所述第一实例崩溃时,所述第一设备终止所述第一实例。

[0147] 结合第五方面,在第五方面的第十二种可能的实现方式中,

[0148] 所述第一设备还包括接收器,用于接收所述第二设备发送的第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

[0149] 结合第五方面至第五方面的第十二种可能的实现方式中任一实现方式,在第五方面的第十三种可能的实现方式中,

[0150] 所述处理器,还用于根据所述第一实例的证书标识删除所述第一实例的证书信息。

[0151] 结合第五方面至第五方面的第十三种可能的实现方式中任一实现方式,在第五方面的第十四种可能的实现方式中,

[0152] 所述处理器,具体用于在已经存储的证书吊销列表CRL中增加所述第一实例的证书标识。

[0153] 结合第五方面至第五方面的第十四种可能的实现方式中任一实现方式,在第五方面的第十五种可能的实现方式中,

[0154] 所述第一实例为虚拟网络功能VNF实例或虚拟网络功能组件VNFC实例。

[0155] 结合第五方面至第五方面的第十五种可能的实现方式中任一实现方式,在第五方面的第十六种可能的实现方式中,

[0156] 所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0157] 结合第五方面至第五方面的第十六种可能的实现方式中任一实现方式,在第五方面的第十七种可能的实现方式中,

[0158] 所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0159] 第六方面,本发明实施例提供一种第二设备,应用于虚拟网络系统,包括:处理器、存储器、总线及接收器,所述处理器、所述存储器及所述接收器通过所述总线相互连接;

[0160] 其中,所述接收器,用于接收第一设备发送的第一请求消息,所述第一请求消息包含第一实例的证书标识,所述第一请求消息用于请求撤销所述第一实例的证书;

[0161] 所述处理器,用于根据所述第一实例的证书标识将所述第一实例的证书状态信息更新为撤销状态。

[0162] 结合第六方面,在第六方面的第一种可能的实现方式中,

[0163] 所述处理器,具体用于在已经存储的证书吊销列表CRL中增加所述第一实例的证

书标识。

[0164] 结合第六方面或第六方面的第一种可能的实现方式,在第六方面的第二种可能的实现方式中,

[0165] 所述第二设备还包括发送器,用于向所述第一设备发送第一确认消息,所述第一确认消息用于指示确认撤销所述第一实例。

[0166] 结合第六方面至第六方面的第二种可能的实现方式中任一实现方式,在第六方面的第三种可能的实现方式中,

[0167] 所述第一实例为VNF实例或虚拟网络功能组件VNFC实例。

[0168] 结合第六方面至第六方面的第三种可能的实现方式中任一实现方式,在第六方面的第四种可能的实现方式中,

[0169] 所述第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0170] 结合第六方面至第六方面的第四种可能的实现方式中任一实现方式,在第六方面的第五种可能的实现方式中,

[0171] 所述第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0172] 第七方面,本发明实施例提供一种虚拟网络系统,包括第一设备及第二设备。

[0173] 其中,所述第一设备为第三方面或第三方面的任意一种可能的实现方式中所描述的第一设备,所述第二设备为第四方面或第四方面的任意一种可能的实现方式中所描述的第二设备;

[0174] 或者,所述第一设备为第五方面或第五方面的任意一种可能的实现方式中所描述的第一设备,所述第二设备为第六方面或第六方面的任意一种可能的实现方式中所描述的第二设备。

[0175] 本发明实施例提供的一种证书管理方法、设备及系统,第一设备获取第一实例的证书标识,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

附图说明

[0176] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0177] 图1为本发明实施例提供的一种网络功能虚拟化系统结构示意图;

[0178] 图2为本发明实施例提供的一种证书管理方法流程示意图;

[0179] 图3为本发明实施例提供的另一种证书管理方法流程示意图;

[0180] 图4为本发明另一实施例提供的一种证书管理方法流程示意图;

[0181] 图5为本发明又一实施例提供的一种证书管理方法流程示意图;

- [0182] 图6为本发明再一实施例提供的一种证书管理方法流程示意图；
- [0183] 图7为本发明实施例提供的一种第一设备结构示意图；
- [0184] 图8为本发明实施例提供的一种第二设备结构示意图；
- [0185] 图9为本发明另一实施例提供的一种第一设备结构示意图；
- [0186] 图10为本发明另一实施例提供的一种第二设备结构示意图。

具体实施方式

[0187] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0188] 本发明的实施例提供一种网络功能虚拟化系统,参照图1所示,该网络功能虚拟化系统10包括NFV0(Network Functions Virtualization Orchestrator,网络功能虚拟化编排器)101、VNFM(Virtualized Network Function Manager,虚拟网络功能管理器)102、VIM(Virtualised Infrastructure Manager,虚拟基础设施管理器)103、OSS/BSS(Operations and Business Support Systems,运营和业务支撑系统)104、EMS(Element Management System,网元管理系统)105、VNF106、NFVI(Network Function Virtualization Infrastructure,网络功能虚拟化基础设施)107。

[0189] 其中,NFV0101,用于对NFV(Network Function Virtualization,网络功能虚拟化)的基础设施资源及软件资源进行网络侧的编排和管理,以及在NFVI107上实现NFV业务拓扑。

[0190] VNFM102,用于对VNF(Virtualised Network Function,虚拟网络功能)实例的生命周期进行管理。

[0191] VIM103,用于控制和管理实现计算、存储和网络资源以及它们的虚拟化的实体。

[0192] OSS/BSS104,用于网络管理、系统管理、计费、账务、客户服务等等。

[0193] EMS105,管理一个或多个网络单元。

[0194] VNF106,对应于传统非虚拟化网络中的PNF(Physical network function,物理网络功能),如虚拟化的EPC(Evolved Packet Core,演进分组核心)节点,实现特定的网络功能。VNF可以由多个更低级别的组件,即VNFC(Virtualised Network Function Component,虚拟网络功能组件)来组成。一个VNF可以部署在多个VM(Virtual Machine,虚拟机)上,每个VM入驻(host)一个VNFC。

[0195] NFVI107,由硬件资源、虚拟资源及虚拟层组成,是提供所需虚拟资源的实体。

[0196] 基于上述图1所示的网络功能虚拟化系统10,本发明实施例提供一种证书管理方法,应用于第一设备,优选的,第一设备可以是图1所示的网络功能虚拟化系统10中的VNFM102,或者,该第一设备也可以是EM(Element Management,网元管理器)。参照图2所示,本实施例提供的证书管理方法包括以下步骤:

[0197] 201、第一设备获取第一实例的证书标识。

[0198] 第一实例为终止的实例。可选的,第一实例可以是VNF实例或VNFC实例。第一实例的证书标识可以包括第一实例的证书序列号。

[0199] 可选的,步骤201之前,第一设备可以接收第一实例发送的第一实例的证书信息,第一实例发送的第一实例的证书信息包括第一实例的标识及第一实例的证书标识;第一设备根据第一实例发送的第一实例的证书信息存储或更新第一实例的证书信息。

[0200] 进一步可选的,在一种应用场景中,第一实例初始安装证书时,将第一实例的证书信息发送至第一设备。在另一种应用场景中,第一设备向第一实例查询证书信息,具体的,第一设备向第一实例发送查询消息,查询消息包括第一实例的标识;第一设备接收第一实例发送的上报消息,上报消息包含第一实例发送的第一实例的证书信息。

[0201] 优选的,第一实例的标识包括第一实例的ID (Identifier,标识),第一实例的ID可以是VNF ID,或VNFC ID,或VM ID,或VC ID (Virtual Container Identifier,虚拟容器标识),第一实例的证书标识包括第一实例的证书序列号。

[0202] 另外,可选的,第一设备终止第一实例有两种情况,以图1所示的网络功能虚拟化系统10为例,当然,本实施例只是以这两种情况为例进行说明,并不代表本发明局限于此。

[0203] 第一种情况,网络功能虚拟化系统10主动终止第一实例,此时,第一设备接收第三设备发送的第二请求消息,第二请求消息包含第一实例的标识,第二请求消息用于指示终止第一实例;第一设备根据第二请求消息终止该第一实例。可选的,第一设备还可以向第三设备发送第二确认消息,第二确认消息包含第一实例的标识,第二确认消息用于指示确认终止第一实例。优选的,第三设备可以是图1所示的网络功能虚拟化系统10中的NFV0101。

[0204] 第二种情况,第一实例因为崩溃等原因被动终止。

[0205] 此时,可选的,第一设备检测到第一实例崩溃时,终止该第一实例。或者,可选的,第四设备检测到第一实例崩溃时,第一设备接收第四设备发送的第一指示信息,第一指示信息用于指示第一实例崩溃,第一指示信息包含第一实例的标识,第一指示信息由第四设备通过第五设备转发至第一设备;第一设备根据第一指示信息终止该第一实例。

[0206] 可选的,第一设备还可以向第三设备发送第二确认消息。此处,优选的,在图1所示的网络功能虚拟化系统10中,第三设备可以是NFV0101,第四设备可以是NFVI107,第五设备可以是VIM103。此时,可选的,第一设备可以向NFVI107及VIM103发送第二指示信息,第二指示信息用于指示VIM删除第一实例对应的资源,并指示NFVI删除第一实例的证书及第一实例的证书对应的密钥。

[0207] 202、第一设备根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息。

[0208] 可选的,第一设备将第一实例的证书状态信息更新为撤销状态时,可以是第一设备在已经存储的CRL (Certificate Revocation List,证书吊销列表) 中增加第一实例的证书标识,或者更新证书状态列表,在证书状态列表中将第一实例的证书状态更改为撤销状态。当然,此处只是举例说明两种具体的可实现方式,对于第一设备如何更新证书状态信息本发明不做限制。

[0209] 或者,第一设备可以向第二设备发送第一请求消息,该第一请求消息包含第一实例的证书标识,第一请求消息用于指示撤销第一实例的证书。其中,本发明中的第二设备可以是CA (Certificate Authority,认证中心)/RA (Registration Authority,注册中心),或OCSP (Online Certificate Status Protocol,在线证书状态协议) 服务器,或图1所示的网络功能虚拟化系统10中的NFV0101。

[0210] 对于步骤202,在通信系统中,哪个设备接收第一请求消息取决于哪个设备维护证书状态信息。如果是第一设备维护证书状态信息,则第一设备终止第一实例后直接更新证书状态信息即可;如果是NFV0101维护证书状态信息,则第一设备将第一请求消息发送至NFV0101;如果是CA/RA维护证书状态信息,则第一设备可以直接向CA/RA发送第一请求消息,或通过NFV0101向CA/RA发送第一请求消息;如果是OCSP服务器维护证书状态信息,第一设备通过CA/RA转发,或通过NFV0101及CA/RA转发,将证书撤销请求发送至OCSP服务器。

[0211] 此处,值得说明的是,第一设备与第二设备之间可能不止一个中间节点,本发明对此不作限制。

[0212] 另外,可选的,如果第一设备存储了第一实例的证书信息,当第一设备终止第一实例后,可以根据第一实例的证书标识删除第一实例的证书信息。

[0213] 步骤202之后,可选的,如果第一设备向第二设备发送第一请求消息,则第一设备还可以接收第二设备发送的第一确认消息,第一确认消息用于指示确认撤销第一实例。

[0214] 因为在每个证书使用之前,需要验证该证书是否合法,如果第一实例的证书被攻击者非法获取,这里,主要在于证书中的私钥被非法获取,通过本实施例的证书管理方法,在第一实例终止后,将第一实例的证书状态信息更改为撤销状态,如果第一实例的证书被攻击者非法获取,在使用之前,就能验证出该证书已经被撤销,无法使用该证书,避免了第一实例终止后,该第一实例的证书中的私钥可能被非法获取从而仿冒VNF实例身份,威胁网络系统的通信安全。

[0215] 本发明实施例提供的证书管理方法,第一设备获取第一实例的证书标识,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,这样,如果第一实例的整数被攻击者非法获取,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0216] 基于图1所示的网络功能虚拟化系统10,结合上述图2对应的实施例,本发明实施例提供另一种证书管理方法,应用于第二设备,可选的,第二设备可以是CA/RA、NFV0或OCSP(Online Certificate Status Protocol,在线证书状态协议)服务器。参照图3所示,包括以下步骤:

[0217] 301、第二设备接收第一设备发送的第一请求消息。

[0218] 第一请求消息包含第一实例的证书标识,第一请求消息用于指示撤销第一实例的证书。可选的,第一实例的证书标识包括第一实例的证书序列号。可选的,第一实例可以是VNF实例或VNFC实例。

[0219] 可选的,结合图1所示的网络功能虚拟化系统10,当第二设备是CA/RA、第一设备为VNFM102时,第一设备可以通过NFV0101与第二设备进行信息传输。

[0220] 或者,可选的,当第二设备是OCSP服务器、第一设备为VNFM102时,第一设备和第二设备可以通过CA/RA进行信息传输,或者第一设备和第二设备可以通过NFV0101和CA/RA进行信息传输。

[0221] 302、第二设备根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态。

[0222] 具体可选的,第二设备可以根据第一实例的证书标识在已经存储的CRL中增加第一实例的证书标识;或者第二设备更新证书状态列表,对于第二设备如何更新证书状态信息本发明不做限制。

[0223] 可选的,第二设备还可以向第一设备发送第一确认消息,第一确认消息用于指示确认撤销第一实例。

[0224] 因为在每个证书使用之前,需要验证该证书是否合法,如果第一实例的证书被攻击者非法获取,这里,主要在于证书中的私钥被非法获取,通过本实施例的证书管理方法,在第一实例终止后,将第一实例的证书状态信息更改为撤销状态,如果第一实例的证书被攻击者非法获取,在使用之前,就能验证出该证书已经被撤销,无法使用该证书,避免了第一实例终止后,该第一实例的证书中的私钥可能被非法获取从而仿冒VNF实例身份,威胁网络系统的通信安全。

[0225] 本发明实施例提供的证书管理方法,第二设备接收第一设备发送的第一请求消息,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0226] 基于图1所示的网络功能虚拟化系统10,结合上述图2和图3对应的实施例,本发明另一实施例提供一种证书管理方法,本实施例以第一设备为VNFM,第二设备为CA/RA为例进行说明,当然,本实施例只是举例说明,并不代表本发明局限于此,第一设备也可以是EM,第二设备也可以是NFVO或OCSP服务器。参照图4所示,本实施例提供的证书管理方法包括以下步骤:

[0227] 401、NFVO接收到终止第一实例的请求。

[0228] 可选的,终止第一实例的请求来自OSS或者VNFM,或者EM触发VNFM发送该请求。值得说明的是,第一实例可以是VNF实例或VNFC实例。

[0229] 可选的,NFVO可以验证该请求的有效性,也可以验证该VNF/VNFC实例是否存在。

[0230] 402、NFVO向VNFM发送第二请求消息。

[0231] 第二请求消息包含第一实例的标识,第二请求消息用于指示终止第一实例。可选的,第一实例的标识包括第一实例的ID (Identifier,标识),第一实例的ID可以是VNF ID,或VNFC ID,或VM ID,或VC ID (Virtual Container Identifier,虚拟容器标识)。

[0232] 403、VNFM终止第一实例。

[0233] 具体的,VNFM根据第二请求消息中包含的第一实例的标识将对应的第一实例终止。

[0234] 404、VNFM向NFVO发送第二确认消息。

[0235] 可选的,第二确认消息包含第一实例的标识,第二确认消息用于指示确认终止第一实例。

[0236] 405、VNFM获取第一实例的证书标识。

[0237] 可选的,VNFM可以根据存储的第一实例的证书信息获取第一实例的标识对应的第一实例的证书标识,并根据第一实例的证书标识确认要撤销的第一实例证书,第一实例的证书信息包括第一实例的标识及第一实例的证书标识。第一实例的证书标识包括第一实例

的证书序列号。

[0238] 406、VNFM向CA/RA发送第一请求消息。

[0239] 第一请求消息包含第一实例的证书标识,第一请求消息用于指示撤销第一实例的证书。

[0240] 407、CA/RA根据第一实例的证书标识更新CRL。

[0241] 可选的,CA/RA根据第一实例的证书标识更新CRL。具体可选的,CA/RA在CRL中增加第一实例的证书标识。其中,可选的,CRL的更新间隔可能是固定的,CA/RA在收到VNFM发送的第一请求消息后,在下一个更新时刻发布更新的CRL,对此,本发明不做限制。

[0242] 408、CA/RA向VNFM发送第一确认消息。

[0243] 可选的,第一确认消息包含第一实例的证书标识,第一确认消息用于指示确认撤销第一实例的证书。

[0244] 409、VNFM根据第一实例的证书标识删除第一实例的证书信息。

[0245] 可选的,步骤404之后,还包括:

[0246] 410、删除对第一实例配置的资源。

[0247] 删除对第一实例配置的资源即为将分配给第一实例的资源回收。具体可选的,VIM删除该第一实例对应的资源,NFVI删除该第一实例的证书及该第一实例的证书对应的密钥。特别地,如果有TPM(Trusted Platform Module,可信平台模块)等安全硬件存储的话,要在硬件中删除。

[0248] 可选的,NFVO还可以向OSS/BSS或VNFM发送第一实例终止的确认消息。

[0249] 本发明实施例提供的证书管理方法,第一设备获取第一实例的证书标识,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0250] 基于图1所示的网络功能虚拟化系统10,结合上述图2和图3对应的实施例,本发明又一实施例提供一种证书管理方法,本实施例以第一设备为VNFM,第二设备为CA/RA为例进行说明,当然,本实施例只是举例说明,并不代表本发明局限于此,第一设备也可以是EM,第二设备也可以是NFVO或OCSP服务器。参照图5所示,本实施例提供的证书管理方法包括以下步骤:

[0251] 501、VNFM检测到第一实例崩溃时,终止第一实例。

[0252] 可选的,第一实例可以是VNF实例或VNFC实例。

[0253] 可选的,VNFM可以通过检测其与第一实例之间的心跳报文确定第一实例是否崩溃,在一种应用场景中,可选的,第一实例每隔一个时间周期向VNFM发送一个心跳报文,以此证明该第一实例运行正常,如果VNFM在规定的时间内没有接收到心跳报文,则证明第一实例崩溃,当然此处只是举例说明,并不代表本发明局限于此,另外,对于心跳报文发送的时间周期,本发明不做限制,可以根据具体情况自行设定。

[0254] 502、VNFM向NFVO发送第二指示信息。

[0255] 可选的,第二指示信息用于指示VIM删除第一实例对应的资源,并指示NFVI删除第

一实例的证书及第一实例的证书对应的密钥。

[0256] 503、删除对第一实例配置的资源。

[0257] 删除对第一实例配置的资源即为将分配给第一实例的资源回收。具体可选的,VIM删除该第一实例对应的资源,NFVI删除该第一实例的证书及该第一实例的证书对应的密钥。特别地,如果有TPM等安全硬件存储的话,要在硬件中删除。

[0258] 504、VNFM获取第一实例的证书标识。

[0259] 可选的,VNFM可以根据存储的第一实例的证书信息获取第一实例的标识对应的第一实例的证书标识,并根据第一实例的证书标识确认要撤销的第一实例证书,第一实例的证书信息包括第一实例的标识及第一实例的证书标识。第一实例的证书标识包括第一实例的证书序列号。

[0260] 505、VNFM向CA/RA发送第一请求消息。

[0261] 第一请求消息包含第一实例的证书标识,第一请求消息用于指示撤销第一实例的证书。

[0262] 具体可选的,VNFM将第一请求消息发送至NFVO,由NFVO将第一请求消息转发至CA/RA。

[0263] 506、CA/RA根据第一实例的证书标识更新CRL。

[0264] 可选的,CA/RA根据第一实例的证书标识更新CRL。具体可选的,CA/RA在CRL中增加第一实例的证书标识。其中,可选的,CRL的更新间隔可能是固定的,CA/RA在收到VNFM发送的第一请求消息后,在下一个更新时刻发布更新的CRL,对此,本发明不做限定。

[0265] 507、CA/RA向VNFM发送第一确认消息。

[0266] 具体可选的,CA/RA将第一确认消息发送至NFVO,由NFVO将第一确认消息转发至VNFM。可选的,第一确认消息包含第一实例的证书标识,第一确认消息用于指示确认撤销第一实例的证书。

[0267] VNFM接收到第一确认消息后,可以根据第一实例的证书标识删除第一实例的证书信息。

[0268] 本发明实施例提供的证书管理方法,第一设备获取第一实例的证书标识,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0269] 基于图1所示的网络功能虚拟化系统10,结合上述图2和图3对应的实施例,本发明再一实施例提供一种证书管理方法,本实施例以第一设备为VNFM,第二设备为OCSP服务器为例进行说明,当然,本实施例只是举例说明,并不代表本发明局限于此,第一设备也可以是EM,第二设备也可以是NFVO或CA/RA。参照图6所示,本实施例提供的证书管理方法包括以下步骤:

[0270] 601、NFVI检测到第一实例崩溃时,向VNFM发送第一指示信息。

[0271] 第一指示信息用于指示第一实例崩溃,第一指示信息包含第一实例的标识,进一步可选的,第一实例可以是VNF实例或VNFC实例,第一实例的标识包括第一实例的ID

(Identifier,标识),第一实例的ID可以是VNF ID,或VNFC ID,或VM ID,或VC ID。

[0272] 优选的,第一指示信息由VIM转发至VNFM。

[0273] 602、VNFM向NFVO发送第二指示信息。

[0274] 优选的,VNFM向VIM及NFVI发送第二指示信息,第二指示信息用于指示VIM删除第一实例对应的资源,并指示NFVI删除第一实例的证书及第一实例的证书对应的密钥。603、删除对第一实例配置的资源。

[0275] 删除对第一实例配置的资源即为将分配给第一实例的资源回收。

[0276] 具体可选的,VIM删除该第一实例对应的资源,NFVI删除该第一实例的证书及该第一实例的证书对应的密钥。特别地,如果有TPM等安全硬件存储的话,要在硬件中删除。

[0277] 604、VNFM获取第一实例的证书标识。

[0278] 可选的,VNFM可以根据存储的第一实例的证书信息获取第一实例的标识对应的第一实例的证书标识,并根据第一实例的证书标识确认要撤销的第一实例证书,第一实例的证书信息包括第一实例的标识及第一实例的证书标识。第一实例的证书标识包括第一实例的证书序列号。

[0279] 605、VNFM向OCSP服务器发送第一请求消息。

[0280] 第一请求消息包含第一实例的证书标识,第一请求消息用于请求撤销第一实例的证书。

[0281] 具体可选的,VNFM将第一请求消息发送至CA/RA,由CA/RA将第一请求消息转发至OCSP服务器。

[0282] 606、OCSP服务器根据第一实例的证书标识更新证书状态列表。

[0283] 具体可选的,OCSP服务器根据第一实例的整数标识在证书状态列表中将第一实例的证书状态更改为撤销状态。

[0284] 607、OCSP服务器向VNFM发送第一确认消息。

[0285] 具体可选的,OCSP服务器将第一确认消息发送至CA/RA,由CA/RA将第一确认消息转发至VNFM。可选的,第一确认消息包含第一实例的证书标识,第一确认消息用于指示确认撤销第一实例的证书。

[0286] VNFM接收到第一确认消息后,可以根据第一实例的证书标识删除第一实例的证书信息。

[0287] 本发明实施例提供的证书管理方法,第一设备获取第一实例的证书标识,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0288] 基于上述图2对应的实施例,本发明实施例提供一种第一设备,用于执行上述图2对应的实施例中所描述的证书管理方法,优选的,应用于图1所示的网络功能虚拟化系统10中,该第一设备可以是VNFM102,或者,该第一设备也可以是EM。参照图7所示,该第一设备70包括:获取单元701,证书管理单元702以及发送单元703。

[0289] 其中,获取单元701,用于获取第一实例的证书标识,第一实例为终止的实例。

- [0290] 在获取单元701获取第一实例的证书标识后，
- [0291] 证书管理单元702，用于根据获取单元701获取的第一实例的证书标识将第一实例的证书状态信息更新为撤销状态。
- [0292] 或者，发送单元703，用于向第二设备发送第一请求消息，第一请求消息包含第一实例的证书标识，第一请求消息用于指示撤销第一实例的证书。
- [0293] 第一设备70还可以包括接收单元704。
- [0294] 可选的，在第一种应用场景中，
- [0295] 接收单元704，用于接收第一实例发送的第一实例的证书信息，第一实例发送的第一实例的证书信息包括第一实例的标识及第一实例的证书标识。
- [0296] 证书管理单元702，还用于根据接收单元704接收的第一实例发送的第一实例的证书信息存储或更新第一实例的证书信息。
- [0297] 可选的，第一实例的标识包括第一实例的ID，第一实例的证书标识包括第一实例的证书序列号。
- [0298] 进一步可选的，第一实例的ID为虚拟网络功能VNF ID，或虚拟网络功能组件VNFC ID，或虚拟机VM ID，或虚拟容器VC ID。
- [0299] 可选的，发送单元703，还用于向第一实例发送查询消息，查询消息包括第一实例的标识。
- [0300] 接收单元704，还用于接收第一实例发送的上报消息，上报消息包含第一实例发送的第一实例的证书信息。
- [0301] 可选的，在第二种应用场景中，
- [0302] 接收单元704，用于接收第三设备发送的第二请求消息，第二请求消息包含第一实例的标识，第二请求消息用于指示终止第一实例。
- [0303] 第一设备70还包括实例管理单元705，用于根据接收单元704接收的第二请求消息终止第一实例。
- [0304] 进一步可选的，发送单元703，还用于向第三设备发送第二确认消息，第二确认消息包含第一实例的标识，第二确认消息用于指示确认终止第一实例。
- [0305] 第三设备可以是网络功能虚拟化编排器NFVO。
- [0306] 可选的，在第三种应用场景中，
- [0307] 接收单元704，用于接收第四设备发送的第一指示信息，第一指示信息用于指示第一实例崩溃，第一指示信息包含第一实例的标识，第一指示信息由第四设备通过第五设备转发至第一设备。
- [0308] 可选的，第四设备为网络功能虚拟化基础设施NFVI，第五设备为虚拟基础设备管理器VIM。
- [0309] 可选的，发送单元703，还用于向VIM及NFVI发送第二指示信息，第二指示信息用于指示VIM删除第一实例对应的资源，并指示NFVI删除第一实例的证书及第一实例的证书对应的密钥。
- [0310] 或者，可选的，实例管理单元705，用于当检测到第一实例崩溃时，第一设备终止第一实例。
- [0311] 另外，可选的，接收单元704，还可以用于接收第二设备发送的第一确认消息，第一

确认消息用于指示确认撤销第一实例。

[0312] 可选的,证书管理单元702,还用于根据第一实例的证书标识删除第一实例的证书信息。

[0313] 可选的,证书管理单元702,具体用于在已经存储的证书吊销列表CRL中增加第一实例的证书标识。

[0314] 可选的,第一实例为虚拟网络功能VNF实例或虚拟网络功能组件VNFC实例。

[0315] 可选的,第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0316] 可选的,第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0317] 本发明实施例提供的第一设备,第一设备获取第一实例的证书标识,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0318] 基于上述图3对应的实施例,本发明实施例提供一种第二设备,用于执行上述图3对应的实施例中所描述的证书管理方法,参照图8所示,该第二设备80包括:接收单元801和证书管理单元802。

[0319] 其中,接收单元801,用于接收第一设备发送的第一请求消息,第一请求消息包含第一实例的证书标识,第一请求消息用于请求撤销第一实例的证书。

[0320] 证书管理单元802,用于根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态。

[0321] 可选的,证书管理单元802,具体用于在已经存储的证书吊销列表CRL中增加第一实例的证书标识。

[0322] 在一种应用场景中,第二设备80还包括发送单元803,用于向第一设备发送第一确认消息,第一确认消息用于指示确认撤销第一实例。

[0323] 可选的,第一实例为VNF实例或虚拟网络功能组件VNFC实例。

[0324] 可选的,第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0325] 本发明实施例提供的第二设备,第二设备接收第一设备发送的第一请求消息,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0326] 基于上述图2对应的实施例,本发明另一实施例提供一种第一设备,用于执行上述图2对应的实施例中所描述的证书管理方法,优选的,应用于图1所示的网络功能虚拟化系统10中,该第一设备可以是VNFM102,或者,该第一设备也可以是EM。参照图9所示,该第一设备90包括:至少一个处理器901、存储器902、总线903和发送器904,该至少一个处理器901、存储器902和发送器904通过总线903连接并完成相互间的通信。

[0327] 该总线903可以是ISA (Industry Standard Architecture, 工业标准体系结构) 总线、PCI (Peripheral Component, 外部设备互连) 总线或EISA (Extended Industry Standard Architecture, 扩展工业标准体系结构) 总线等。该总线903可以分为地址总线、数据总线、控制总线等。为便于表示, 图9中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。其中:

[0328] 存储器902用于执行本发明方案的应用程序代码, 执行本发明方案的应用程序代码保存在存储器中, 并由处理器901来控制执行。

[0329] 该存储器可以是只读存储器ROM或可存储静态信息和指令的其他类型的静态存储设备, 随机存取存储器RAM或者可存储信息和指令的其他类型的动态存储设备, 也可以是电可擦可编程只读存储器EEPROM、只读光盘CD-ROM或其他光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质, 但不限于此。这些存储器通过总线与处理器相连接。

[0330] 处理器901可能是一个中央处理器901 (Central Processing Unit, 简称为CPU), 或者是特定集成电路 (Application Specific Integrated Circuit, 简称为ASIC), 或者是被配置成实施本发明实施例的一个或多个集成电路。

[0331] 处理器901, 用于调用存储器902中的程序代码, 在一种可能的实施方式中, 当上述应用程序被所述处理器901执行时, 实现如下功能。

[0332] 处理器901, 用于获取第一实例的证书标识, 第一实例为终止的实例。

[0333] 在处理器901获取第一实例的证书标识后,

[0334] 处理器901, 还用于根据获取的第一实例的证书标识将第一实例的证书状态信息更新为撤销状态。

[0335] 或者, 发送器904, 用于向第二设备发送第一请求消息, 第一请求消息包含第一实例的证书标识, 第一请求消息用于请求撤销第一实例的证书。

[0336] 第一设备90还可以包括接收器905,

[0337] 可选的, 在第一种应用场景中,

[0338] 接收器905, 用于接收第一实例发送的第一实例的证书信息, 第一实例发送的第一实例的证书信息包括第一实例的标识及第一实例的证书标识。

[0339] 处理器901, 还用于根据接收器905接收的第一实例发送的第一实例的证书信息存储或更新第一实例的证书信息。

[0340] 可选的, 第一实例的标识包括第一实例的ID, 第一实例的证书标识包括第一实例的证书序列号。

[0341] 可选的, 第一实例的ID为虚拟网络功能VNF ID, 或虚拟网络功能组件VNFC ID, 或虚拟机VM ID, 或虚拟容器VC ID。

[0342] 可选的, 发送器904, 还用于向第一实例发送查询消息, 查询消息包括第一实例的标识。

[0343] 接收器905, 还用于接收第一实例发送的上报消息, 上报消息包含第一实例发送的第一实例的证书信息。

[0344] 可选的, 在第二种应用场景中,

[0345] 接收器905,用于接收第三设备发送的第二请求消息,第二请求消息包含第一实例的标识,第二请求消息用于指示终止第一实例。

[0346] 处理器901,还用于根据接收器905接收的第二请求消息终止第一实例。

[0347] 可选的,发送器904,还用于向第三设备发送第二确认消息,第二确认消息包含第一实例的标识,第二确认消息用于指示确认终止第一实例。

[0348] 进一步可选的,第三设备为网络功能虚拟化编排器NFVO。

[0349] 可选的,在第三种应用场景中,

[0350] 接收器905,用于接收第四设备发送的第一指示信息,第一指示信息用于指示第一实例崩溃,第一指示信息包含第一实例的标识,第一指示信息由第四设备通过第五设备转发至第一设备。

[0351] 可选的,第四设备为网络功能虚拟化基础设施NFVI,第五设备为虚拟设备管理器VIM。

[0352] 进一步可选的,发送器904,还用于向VIM及NFVI发送第二指示信息,第二指示信息用于指示VIM删除第一实例对应的资源,并指示NFVI删除第一实例的证书及第一实例的证书对应的密钥。

[0353] 或者,可选的,处理器901,还用于当检测到第一实例崩溃时,第一设备终止第一实例。

[0354] 可选的,处理器901,还用于根据第一实例的证书标识删除第一实例的证书信息。

[0355] 可选的,处理器901,具体用于在已经存储的证书吊销列表CRL中增加第一实例的证书标识。

[0356] 可选的,第一实例为虚拟网络功能VNF实例或虚拟网络功能组件VNFC实例。

[0357] 可选的,第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0358] 可选的,第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0359] 本发明实施例提供的第一设备,第一设备获取第一实例的证书标识,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0360] 基于上述图3对应的实施例,本发明另一实施例提供一种第二设备,用于执行上述图3对应的实施例中所描述的证书管理方法,参照图10所示,该第二设备100包括:至少一个处理器1001、存储器1002、总线1003和接收器1004,该至少一个处理器1001、存储器1002和接收器1004通过总线1003连接并完成相互间的通信。

[0361] 该总线1003可以是ISA (Industry Standard Architecture,工业标准体系结构)总线、PCI (Peripheral Component,外部设备互连)总线或EISA (Extended Industry Standard Architecture,扩展工业标准体系结构)总线等。该总线1003可以分为地址总线、数据总线、控制总线等。为便于表示,图10中仅用一条粗线表示,但并不表示仅有一根总线或一种类型的总线。其中:

[0362] 存储器1002用于执行本发明方案的应用程序代码,执行本发明方案的应用程序代码保存在存储器中,并由处理器1001来控制执行。

[0363] 该存储器可以是只读存储器ROM或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器RAM或者可存储信息和指令的其他类型的动态存储设备,也可以是电可擦可编程只读存储器EEPROM、只读光盘CD-ROM或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质,但不限于此。这些存储器通过总线与处理器相连接。

[0364] 处理器1001可能是一个中央处理器1001(Central Processing Unit,简称为CPU),或者是特定集成电路(Application Specific Integrated Circuit,简称为ASIC),或者是被配置成实施本发明实施例的一个或多个集成电路。

[0365] 处理器1001,用于调用存储器1002中的程序代码,在一种可能的实施方式中,当上述应用程序被所述处理器1001执行时,实现如下功能。

[0366] 接收器1004,用于接收第一设备发送的第一请求消息,第一请求消息包含第一实例的证书标识,第一请求消息用于请求撤销第一实例的证书。

[0367] 处理器1001,用于根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态。

[0368] 可选的,处理器1001,具体用于在已经存储的证书吊销列表CRL中增加第一实例的证书标识。

[0369] 可选的,在一种应用场景中,第二设备100还包括发送器1005,用于向第一设备发送第一确认消息,第一确认消息用于指示确认撤销第一实例。

[0370] 可选的,第一实例为VNF实例或虚拟网络功能组件VNFC实例。

[0371] 可选的,第二设备为证书中心CA/注册中心RA,或NFVO,或在线证书状态协议OCSP服务器。

[0372] 可选的,第一设备为虚拟网络功能管理器VNFM或网元管理器EM。

[0373] 本发明实施例提供的第二设备,第二设备接收第一设备发送的第一请求消息,根据第一实例的证书标识将第一实例的证书状态信息更新为撤销状态,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0374] 基于上述图2、图3、图4、图5和图6对应的实施例,本发明实施例提供一种虚拟网络系统,用于执行上述图2、图3、图4、图5和图6对应的实施例中所描述的证书管理方法,结合图1所示的网络功能虚拟化系统10,优选的,本实施例提供的虚拟网络系统可以包含图1所示的网络功能虚拟化系统,本实施例提供的虚拟网络系统包括:第一设备和第二设备。

[0375] 其中,第一设备为图7对应的实施例中所描述的第一设备,第二设备为图8对应的实施例中所描述的第二设备。

[0376] 或者,第一设备为图9对应的实施例中所描述的第一设备,第二设备为图10对应的实施例中所描述的第二设备。

[0377] 本发明实施例提供的虚拟网络系统,第一设备获取第一实例的证书标识,根据第

一实例的证书标识将第一实例的证书状态信息更新为撤销状态,或者,第一设备向第二设备发送第一请求消息,当使用非法获取的第一实例的证书时,可以验证出该第一实例的证书已经被撤销,获取到第一实例的证书也无法使用,解决了虚拟网络系统中VNF实例终止后,VNF实例证书对应的私钥可能被攻击者非法获取,从而仿冒VNF实例身份,导致虚拟网络系统的通信安全降低的问题。

[0378] 通过以上的实施方式的描述,所属领域的技术人员可以清楚地了解到本发明可以用硬件实现,或固件实现,或它们的组合方式来实现。当使用软件实现时,可以将上述功能存储在计算机可读介质中或作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质,其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是计算机能够存取的任何可用介质。以此为例但不限于:计算机可读介质可以包括RAM(Random Access Memory,随机存储器)、ROM(Read Only Memory,只读内存)、EEPROM(Electrically Erasable Programmable Read Only Memory,电可擦可编程只读存储器)、CD-ROM(Compact Disc Read Only Memory,即只读光盘)或其他光盘存储、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质。此外,任何连接可以适当的成为计算机可读介质。例如,如果软件是使用同轴电缆、光纤光缆、双绞线、DSL(Digital Subscriber Line,数字用户专线)或者诸如红外线、无线电和微波之类的无线技术从网站、服务器或者其他远程源传输的,那么同轴电缆、光纤光缆、双绞线、DSL或者诸如红外线、无线和微波之类的无线技术包括在所属介质的定义中。如本发明所使用的,盘和碟包括CD(Compact Disc,压缩光碟)、激光碟、光碟、DVD碟(Digital Versatile Disc,数字通用光)、软盘和蓝光光碟,其中盘通常磁性的复制数据,而碟则用激光来光学的复制数据。上面的组合也应当包括在计算机可读介质的保护范围之内。

[0379] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应所述以权利要求的保护范围为准。

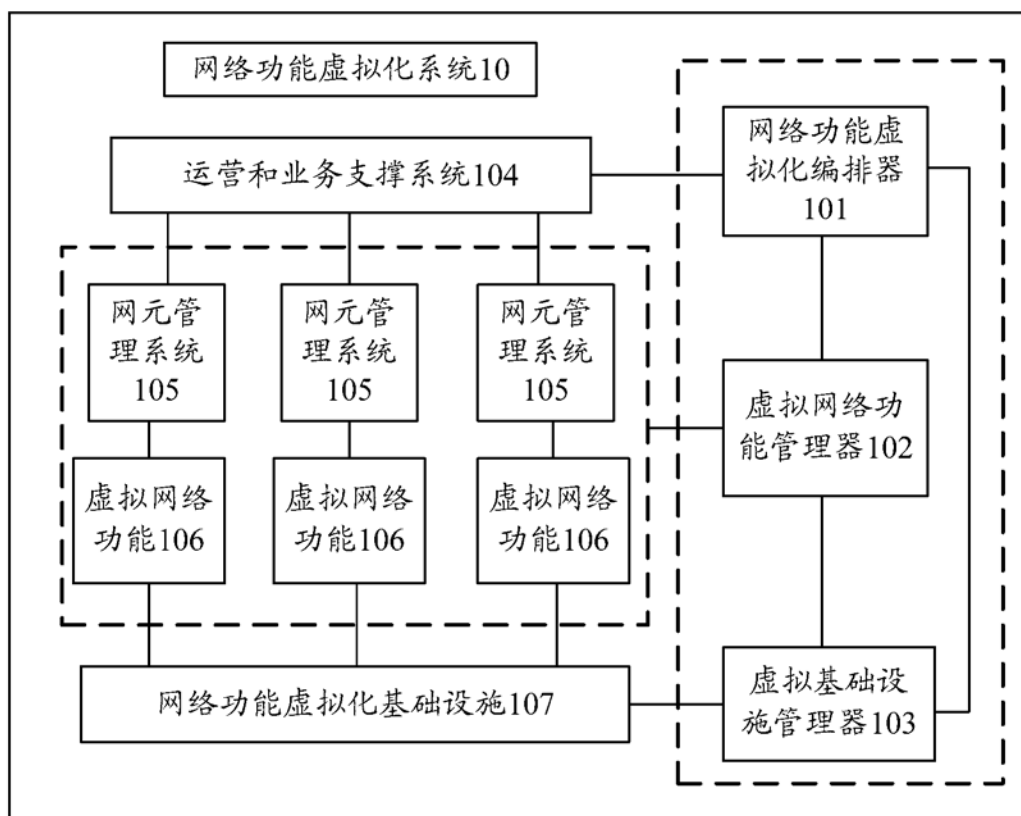


图1

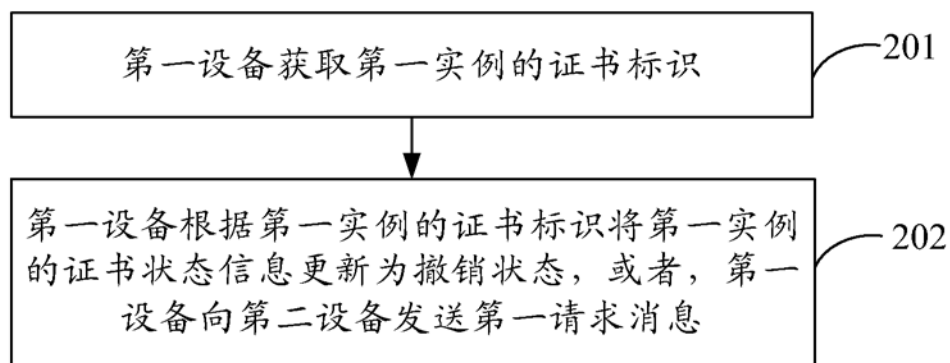


图2

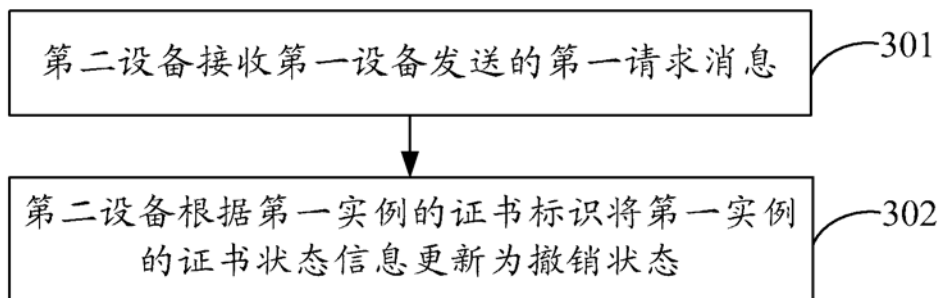


图3

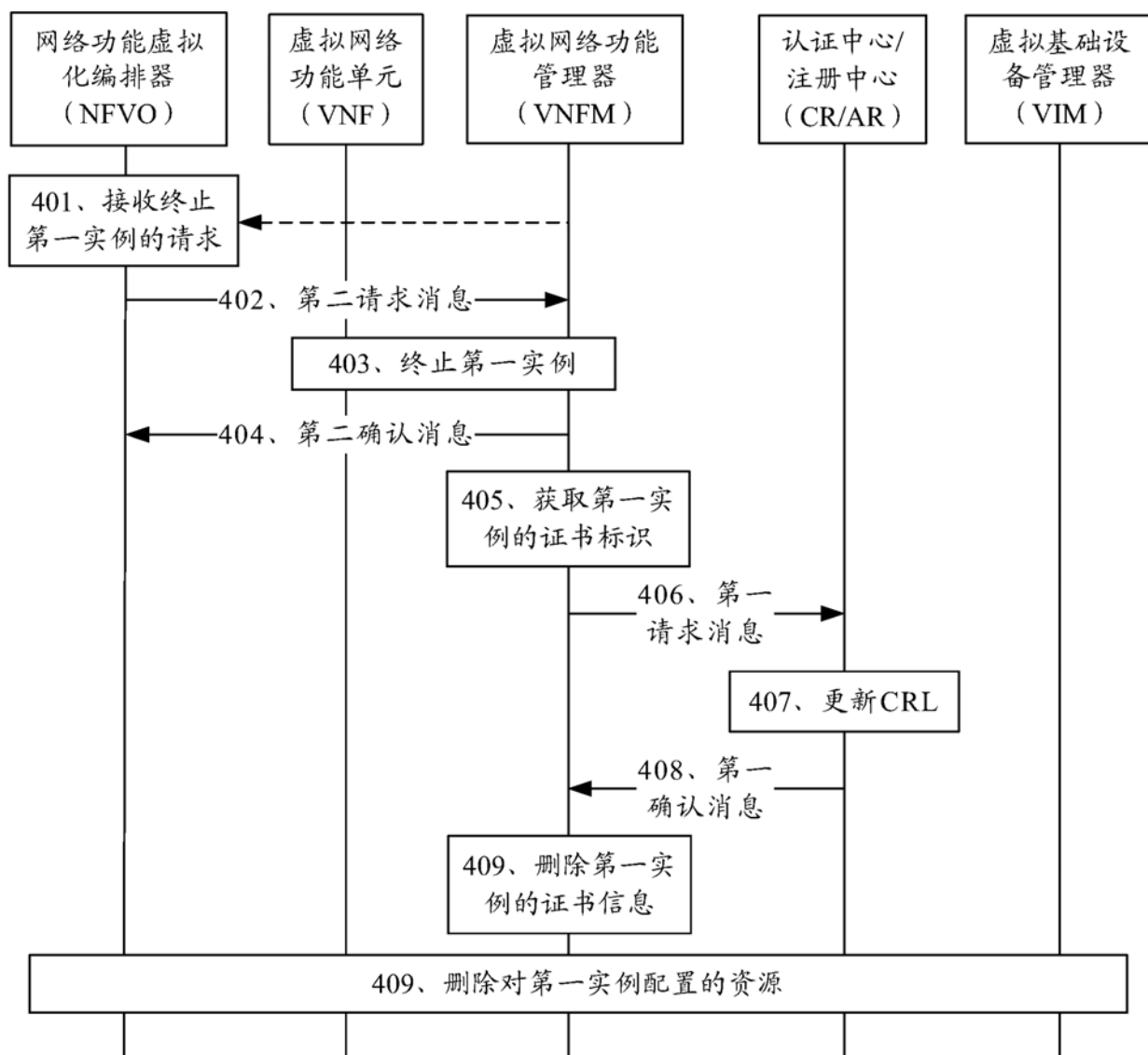


图4

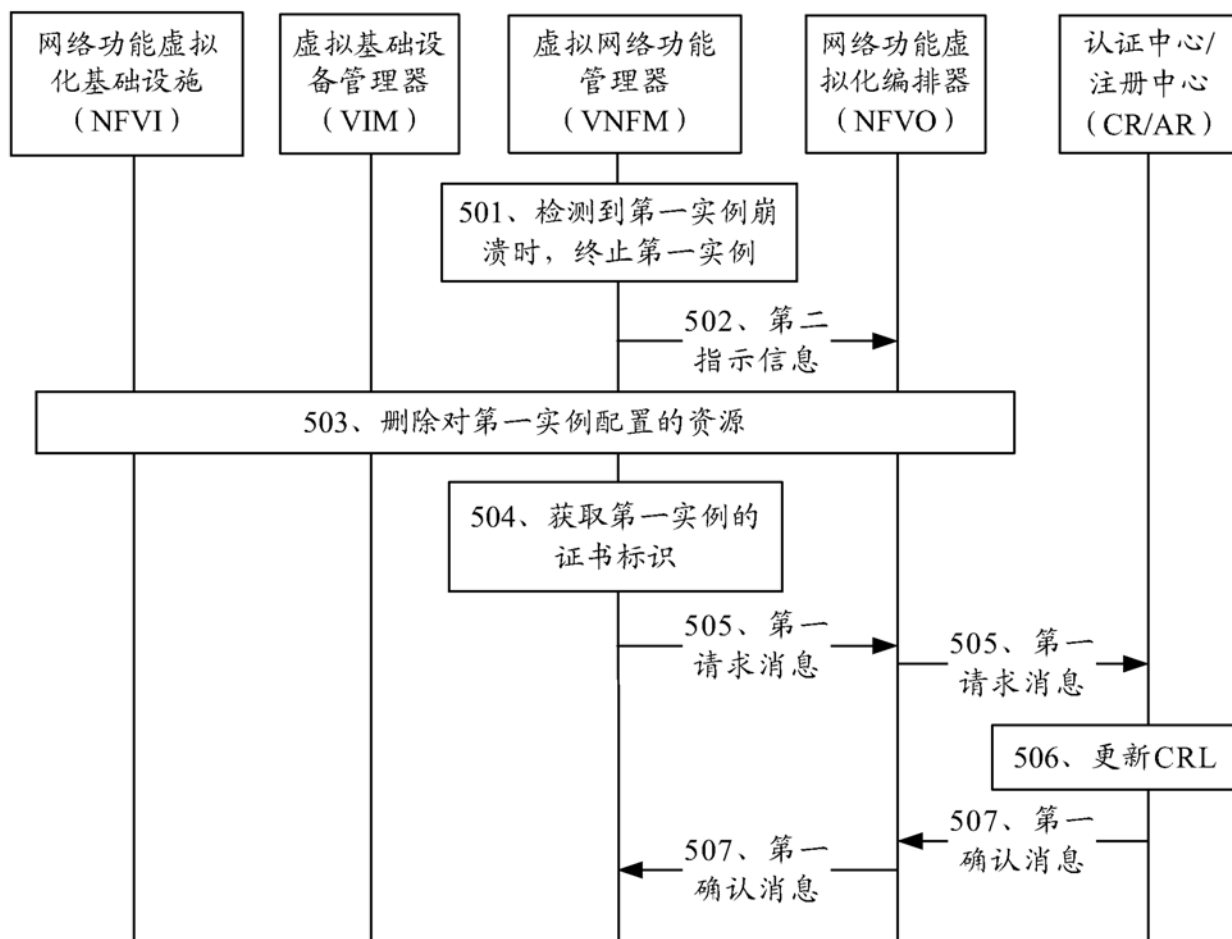


图5

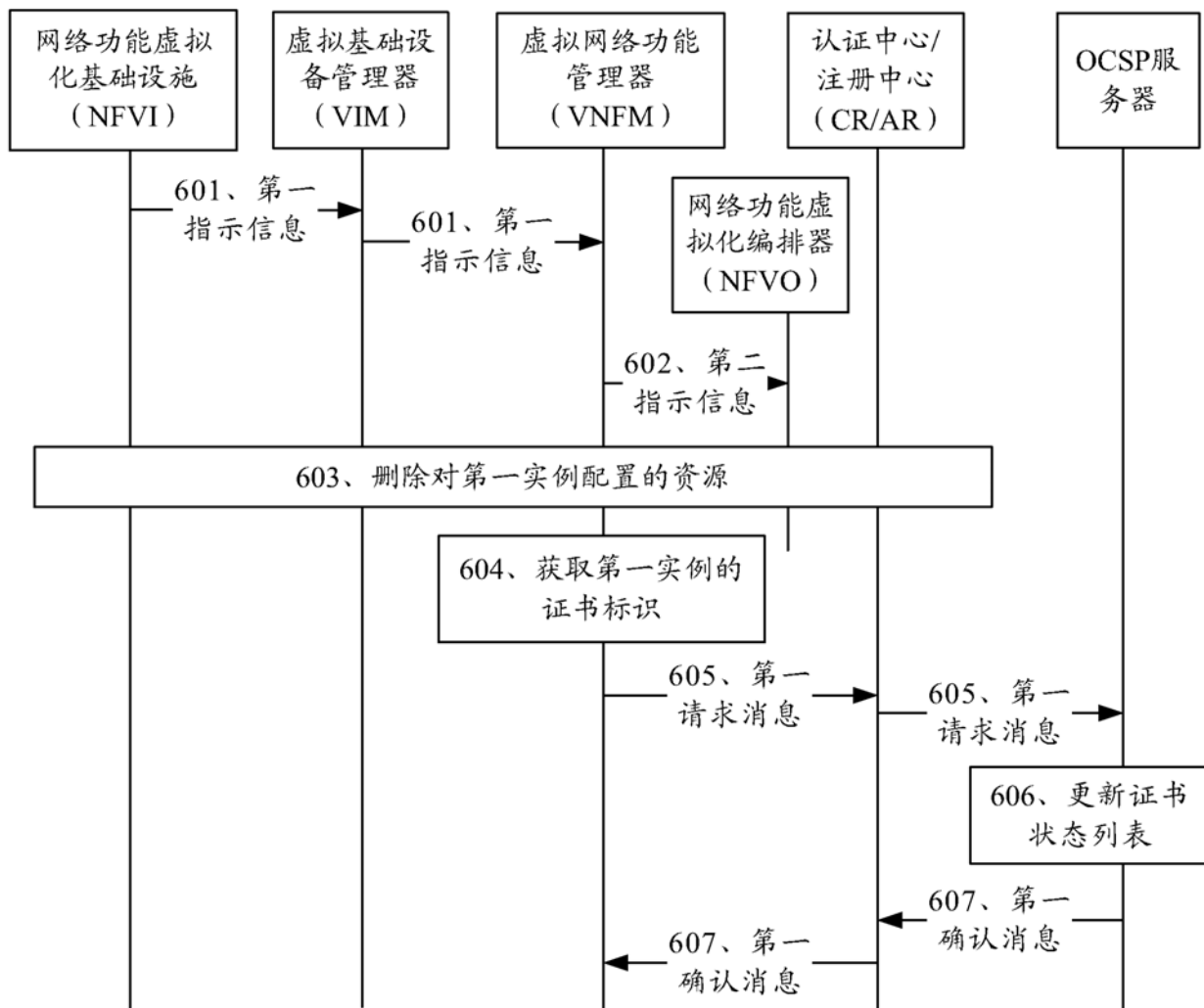


图6

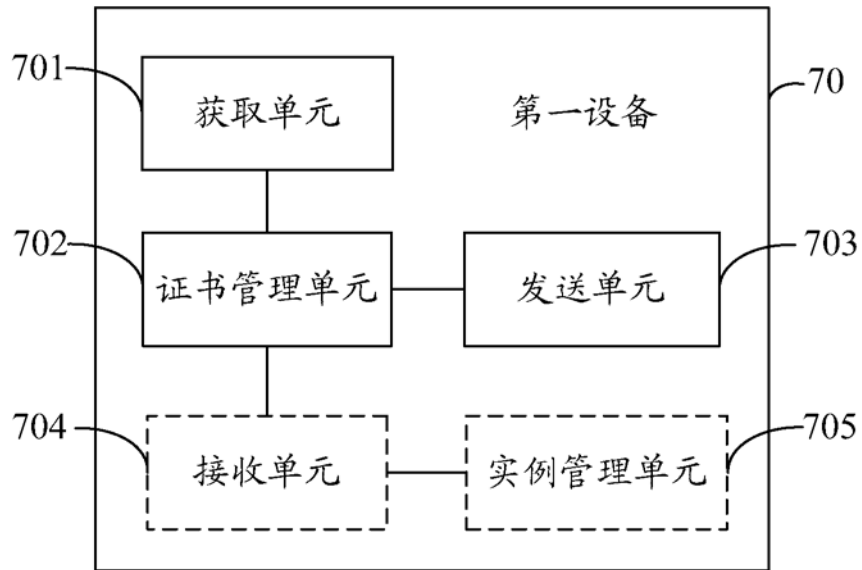


图7

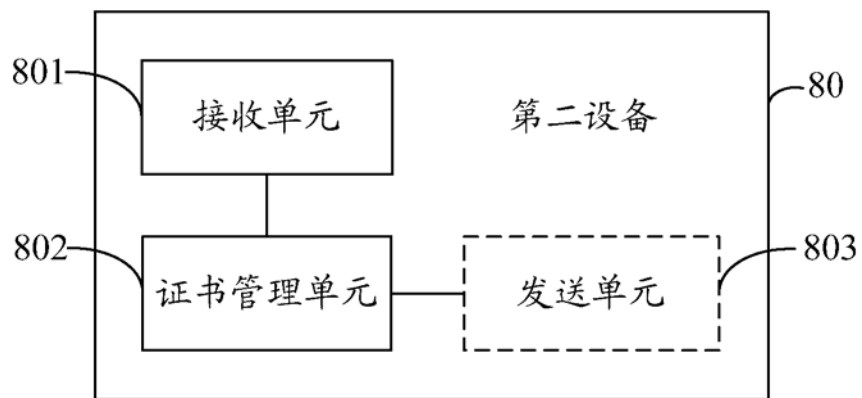


图8

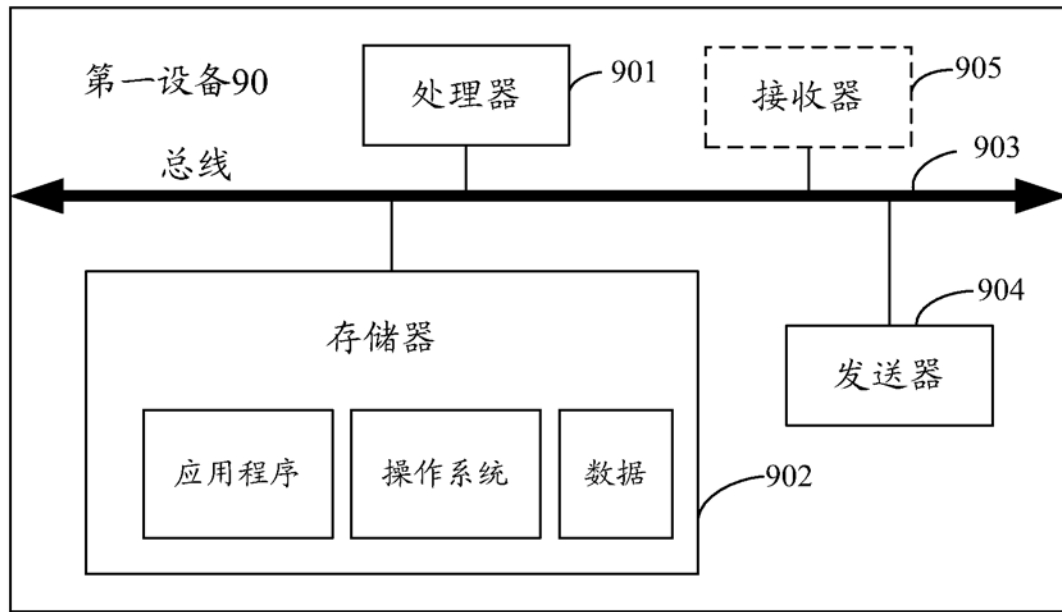


图9

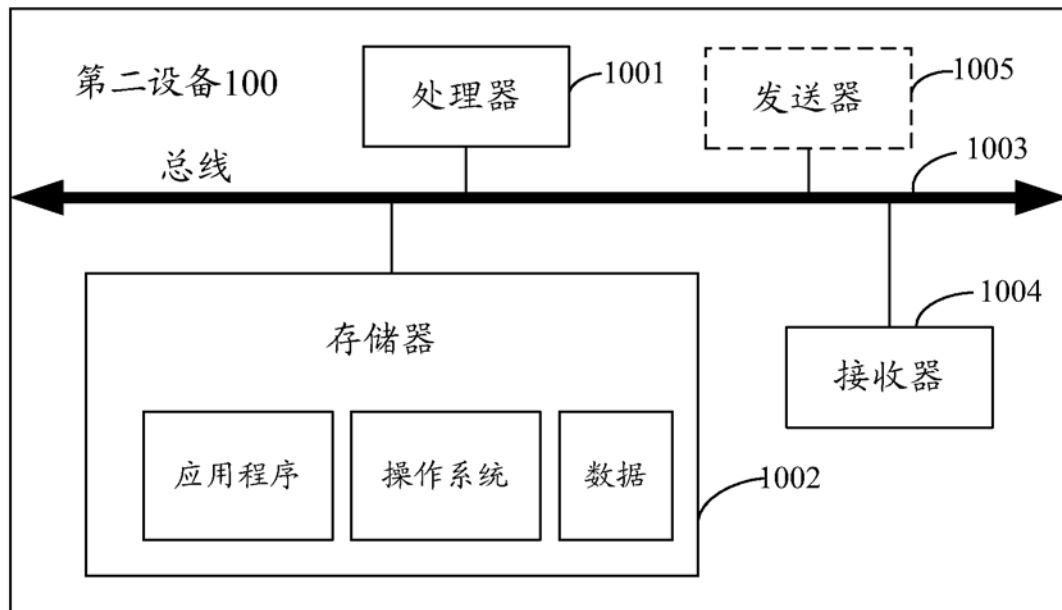


图10