(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112335274 B
(45)授权公告日 2025.01.24

(21)申请号 201980043678.9
(22)申请日 2019.06.19
(65)同一申请的已公布的文献号
申请公布号 CN 112335274 A
(43)申请公布日 2021.02.05
(30)优先权数据
201841024429 2018.06.29 IN
(85)PCT国际申请进入国家阶段日
2020.12.28
(86)PCT国际申请的申请数据
PCT/FI2019/050475 2019.06.19
(87)PCT国际申请的公布数据
WO2020/002764 EN 2020.01.02
(73)专利权人 诺基亚技术有限公司
地址 芬兰埃斯波
(72)发明人 N•斯布坎帕迪 T•尼麦拉
(74)专利代理机构 北京市中咨律师事务所 11247
专利代理师 杨晓光
(51)Int.Cl.
H04L 9/32(2006.01)
H04W 12/084(2021.01)
G06F 21/33(2013.01)
G06F 21/62(2013.01)

(56)对比文件
US 2006041669 A1,2006.02.23
Nokia, S3-181385.Editor's Note on per UE subscription level authorization in NRF.3GPP TSG_SA\WG3_Security.2018,(第TSGS3_91_belgrade期),chapter 13.4.1.1.
Nokia, S3-173225.OAuth based service authorization framework for SBA.3GPP TSG_SA\WG3_Security.2017,(第TSGS3_89_Reno期),chapter 4.1.3, 4.1.4.2.

审查员 庞素琴

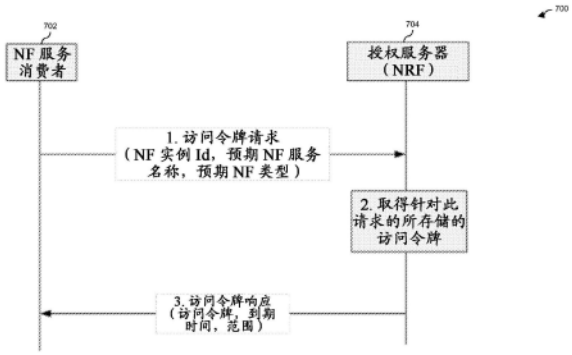
权利要求书5页 说明书9页 附图6页

(54)发明名称

用于通信系统中服务访问的安全管理

(57)摘要

在包括基于服务的架构的通信系统中的授权实体从通信系统中的服务消费者接收对访问给定服务类型的请求。授权实体获得标识针对给定服务类型的多个服务生产者的访问令牌,并将访问令牌发送到服务消费者。



CN 112335274 B

1.一种用于安全管理的方法,所述方法包括:

在包括基于服务的架构的通信系统中的授权实体处,接收来自所述通信系统中的网络功能服务消费者的对访问给定网络功能服务类型的请求;

在所述授权实体处获得访问令牌,所述访问令牌标识针对所述给定网络功能服务类型的多个网络功能服务生产者;以及

将所述访问令牌从所述授权实体发送到所述网络功能服务消费者。

2.根据权利要求1所述的方法,还包括:

在接收来自所述网络功能服务消费者的访问令牌请求之前,所述授权实体在发现步骤中对所述网络功能服务消费者进行认证。

3.根据权利要求1所述的方法,其中,所述获得步骤还包括:从存储设备中取得在发现步骤期间生成的所述访问令牌。

4.根据权利要求1所述的方法,其中,所述授权实体是网络功能存储功能,所述网络功能服务消费者是第一网络功能,所述多个网络功能服务生产者是两个或更多个其他网络功能。

5.根据权利要求1所述的方法,其中,所述访问令牌包括用于在其中被标识的所述多个网络功能服务生产者中的每个网络功能服务生产者的标识符和地址。

6.根据权利要求4所述的方法,其中,用于给定网络功能服务生产者的地址包括统一位置标识符。

7.根据权利要求1所述的方法,其中,所述访问令牌包括JavaScript对象标记Web令牌格式。

8.根据权利要求7所述的方法,其中,针对所述给定网络功能服务类型的所述多个网络功能服务生产者在所述JavaScript对象标记Web令牌格式的受众声明字段中被标识。

9.一种非暂时性计算机可读存储介质,在所述非暂时性计算机可读存储介质中体现有可执行程序代码,所述可执行程序代码在由处理器执行时使得所述处理器执行以下步骤:

在包括基于服务的架构的通信系统中的授权实体处,接收来自所述通信系统中的网络功能服务消费者的对访问给定网络功能服务类型的请求;

在所述授权实体处获得访问令牌,所述访问令牌标识针对所述给定网络功能服务类型的多个网络功能服务生产者;以及

将所述访问令牌从所述授权实体发送到所述网络功能服务消费者。

10.一种用于安全管理的装置,所述装置包括:

在包括基于服务的架构的通信系统中,其中所述通信系统包括授权实体、至少一个网络功能服务消费者、以及网络功能服务生产者;

至少一个处理器,所述至少一个处理器被耦接到与所述授权实体相关联的存储器并被配置为:

接收来自所述网络功能服务消费者的对访问给定网络功能服务类型的请求;

获得标识针对所述给定网络功能服务类型的多个网络功能服务生产者的访问令牌;以及

将所述访问令牌发送到所述网络功能服务消费者。

11.一种用于安全管理的方法,所述方法包括:

从包括基于服务的架构的通信系统中的网络功能服务消费者向所述通信系统中的授权实体发送对访问给定网络功能服务类型的请求;

在所述网络功能服务消费者处从所述授权实体接收访问令牌,其中,所述访问令牌标识所述通信系统中针对所述给定网络功能服务类型的多个网络功能服务生产者;以及

基于一个或多个选择准则,根据所述访问令牌选择所述多个网络功能服务生产者中的一个网络功能服务生产者。

12.根据权利要求11所述的方法,还包括:

所述网络功能服务消费者向所选择的网络功能服务生产者发送服务请求,其中,所述服务请求包括所述访问令牌。

13.根据权利要求12所述的方法,其中,所述服务请求包括应用编程接口服务请求。

14.根据权利要求11所述的方法,还包括:

随后根据同一访问令牌来选择另一个网络功能服务生产者;以及

向所选择的另一个网络功能服务生产者发送服务请求,其中,所述服务请求包括所述访问令牌。

15.一种非暂时性计算机可读存储介质,在所述非暂时性计算机可读存储介质中体现有可执行程序代码,所述可执行程序代码在由处理器执行时使得所述处理器执行以下步骤:

从包括基于服务的架构的通信系统中的网络功能服务消费者向所述通信系统中的授权实体发送对访问给定网络功能服务类型的请求;

在所述网络功能服务消费者处从所述授权实体接收访问令牌,其中,所述访问令牌标识所述通信系统中针对所述给定网络功能服务类型的多个网络功能服务生产者;以及

基于一个或多个选择准则,根据所述访问令牌选择所述多个网络功能服务生产者中的一个网络功能服务生产者。

16.一种用于安全管理的装置,所述装置包括:

在包括基于服务的架构的通信系统中,其中所述通信系统包括授权实体、至少一个网络功能服务消费者、以及网络功能服务生产者;

至少一个处理器,所述至少一个处理器被耦接到与所述网络功能服务消费者相关联的存储器并被配置为:

向所述授权实体发送对访问给定网络功能服务类型的请求;

在所述网络功能服务消费者处从所述授权实体接收访问令牌,其中,所述访问令牌标识所述通信系统中针对所述给定网络功能服务类型的多个网络功能服务生产者;以及

基于一个或多个选择准则,根据所述访问令牌选择所述多个网络功能服务生产者中的一个网络功能服务生产者。

17.一种用于安全管理的方法,所述方法包括:

在包括基于服务的架构的通信系统中的代理单元处接收访问令牌,其中,所述访问令牌标识所述通信系统中针对给定网络功能服务类型的多个网络功能服务生产者并且由所述通信系统中的授权实体响应于所述通信系统中的网络功能服务消费者的对访问所述给定网络功能服务类型的请求而生成;以及

在所述代理单元处,基于一个或多个选择准则,根据所述访问令牌选择所述多个网络

功能服务生产者中的一个网络功能服务生产者。

18.根据权利要求17所述的方法,还包括:

当所述代理单元驻留在所述授权实体与所述网络功能服务消费者之间时,所述代理单元向所述网络功能服务消费者发送用于所选择的网络功能服务生产者的标识信息。

19.根据权利要求17所述的方法,还包括:

当所述代理单元驻留在所述授权实体与所述网络功能服务消费者之间时,所述代理单元随后基于所述一个或多个选择准则中的至少一个选择准则的变化来根据所述访问令牌选择另一个网络功能服务生产者。

20.根据权利要求19所述的方法,还包括:

所述代理单元向所述网络功能服务消费者发送用于随后被选择的网络功能服务生产者的标识信息。

21.根据权利要求17所述的方法,还包括:

当所述代理单元驻留在所述网络功能服务消费者与一个或多个所述网络功能服务生产者之间时,所述代理单元向所述网络功能服务消费者发送用于所选择的网络功能服务生产者的标识信息。

22.根据权利要求21所述的方法,还包括:

当所述代理单元驻留在所述网络功能服务消费者与一个或多个所述网络功能服务生产者之间时,所述代理单元随后基于一个或多个选择准则中的至少一个选择准则的变化来根据所述访问令牌选择另一个网络功能服务生产者。

23.根据权利要求22所述的方法,还包括:

所述代理单元向所述网络功能服务消费者发送用于随后被选择的网络功能服务生产者的标识信息。

24.根据权利要求19所述的方法,其中,发生所述变化的所述选择准则包括以下一个或多个:

负载平衡准则;

可用性准则;以及

维护准则。

25.根据权利要求19所述的方法,其中,所述一个或多个选择准则包括一个或多个运营商配置的策略准则。

26.根据权利要求17所述的方法,其中,所述代理单元驻留在所述授权实体中。

27.根据权利要求17所述的方法,其中,所述代理单元驻留在所述网络功能服务消费者中。

28.根据权利要求17所述的方法,其中,所述代理单元驻留在一个或多个所述网络功能服务生产者中。

29.根据权利要求17所述的方法,其中,所述代理单元从所述授权实体和所述网络功能服务消费者中的一个接收所述访问令牌。

30.一种非暂时性计算机可读存储介质,在所述非暂时性计算机可读存储介质中体现有可执行程序代码,所述可执行程序代码在由处理器执行时使得所述处理器执行以下步骤:

在包括基于服务的架构的通信系统中的代理单元处接收访问令牌,其中,所述访问令牌标识所述通信系统中针对给定网络功能服务类型的多个网络功能服务生产者并且由所述通信系统中的授权实体响应于所述通信系统中的网络功能服务消费者的对访问所述给定网络功能服务类型的请求而生成;以及

在所述代理单元处,基于一个或多个选择准则,根据所述访问令牌选择所述多个网络功能服务生产者中的一个网络功能服务生产者。

31.一种用于安全管理的装置,所述装置包括:

在包括基于服务的架构的通信系统中,其中所述通信系统包括授权实体、至少一个代理单元、至少一个网络功能服务消费者、以及网络功能服务生产者;

至少一个处理器,所述至少一个处理器被耦接到与所述代理单元相关联的存储器并被配置为:

在所述代理单元处接收访问令牌,其中,所述访问令牌标识针对给定网络功能服务类型的多个网络功能服务生产者并且由所述授权实体响应于所述网络功能服务消费者的对访问所述给定网络功能服务类型的请求而生成;以及

基于一个或多个选择准则,根据所述访问令牌选择所述多个网络功能服务生产者中的一个网络功能服务生产者。

32.一种用于安全管理的方法,所述方法包括:

在包括基于服务的架构的通信系统中的网络功能服务消费者处从授权实体接收访问令牌,其中,所述访问令牌标识与所述通信系统中针对给定网络功能服务类型的网络功能服务生产者相对应的多个代理单元;

在所述网络功能服务消费者处,根据所述访问令牌选择所述多个代理单元中的一个代理单元;以及

从所述网络功能服务消费者向所选择的代理单元发送对访问所述给定网络功能服务类型的请求。

33.一种非暂时性计算机可读存储介质,在所述非暂时性计算机可读存储介质中体现有可执行程序代码,所述可执行程序代码在由处理器执行时使得所述处理器执行以下步骤:

在包括基于服务的架构的通信系统中的网络功能服务消费者处从授权实体接收访问令牌,其中,所述访问令牌标识与所述通信系统中针对给定网络功能服务类型的网络功能服务生产者相对应的多个代理单元;

在所述网络功能服务消费者处,根据所述访问令牌选择所述多个代理单元中的一个代理单元;以及

从所述网络功能服务消费者向所选择的代理单元发送对访问所述给定网络功能服务类型的请求。

34.一种用于安全管理的装置,所述装置包括:

在包括基于服务的架构的通信系统中,其中所述通信系统包括授权实体、至少一个代理单元、至少一个网络功能服务消费者、以及网络功能服务生产者;

至少一个处理器,所述至少一个处理器被耦接到与所述网络功能服务消费者相关联的存储器并被配置为:

从所述授权实体接收访问令牌,其中,所述访问令牌标识与针对给定网络功能服务类型的网络功能服务生产者相对应的多个代理单元;

根据所述访问令牌选择所述多个代理单元中的一个代理单元;以及

向所选择的代理单元发送对访问所述给定网络功能服务类型的请求。

用于通信系统中服务访问的安全管理

技术领域

[0001] 该领域通常涉及通信系统,更特别但非排他地,涉及这种系统内的安全管理。

背景技术

[0002] 本节介绍可有助于促进更好地理解本发明的各方面。因此,本节的陈述应从这一角度来阅读,而不应被理解为对现有技术中存在的内容或对现有技术中不存在的内容的承认。

[0003] 第四代(4G)无线移动电信技术,也被称为长期演进(LTE)技术,被设计为提供具有高数据速率的高容量移动多媒体,特别是用于人类交互。下一代或第五代(5G)技术旨在不仅用于人类交互,而且还用于所谓的物联网(IoT)网络中的机器类型通信。

[0004] 虽然5G网络旨在实现大规模IoT服务(例如,数量众多的有限能力设备)和任务关键型IoT服务(例如,要求高可靠性),但是仍以增强型移动宽带(eMBB)服务的形式支持对传统移动通信服务的改进,该增强型移动宽带(eMBB)服务为移动设备提供了改进的无线因特网接入。

[0005] 在示例性通信系统中,诸如移动终端(订户)之类的用户设备(5G网络中的5G UE,或更广泛地,UE)通过空中接口与基站或接入点(在5G网络中被称为gNB)通信。说明性地,接入点(例如,gNB)是通信系统的接入网络的一部分。例如,在5G网络中,接入网络被称为5G系统,并且在标题为“技术规范组服务和系统方面;用于5G系统的系统架构(Technical Specification Group Services and System Aspects;System Architecture for the 5G System)”的5G技术规范(TS)23.501,V15.0.0中被描述,其公开内容通过引用全部并入本文中。通常,接入点(例如,gNB)为UE提供对核心网络(CN)的接入,然后,核心网(CN)为UE提供对其他UE和/或诸如分组数据网络(例如,因特网)之类的数据网络的接入。

[0006] TS 23.501继续定义了基于5G服务的架构(SBA),该架构将服务建模为网络功能(NF),这些网络功能使用表述性状态转移应用编程接口(Restful API)来彼此通信。

[0007] 此外,标题为“技术规范组服务和系统方面;用于5G系统的安全架构和过程(Technical Specification Group Services and System Aspects;Security Architecture and Procedures for the 5G System)”的5G技术规范(TS)33.501,V15.1.0进一步描述了与5G网络相关联的安全管理细节,其内容通过引用全部并入本文中。

[0008] 安全管理是任何通信系统中的重要考虑因素。例如,对访问服务的授权是5G网络中安全管理的一个示例。然而,服务访问授权在已有的5G方法中存在若干挑战。

发明内容

[0009] 示例性实施例提供了改进的用于通信系统中的安全管理特别是关于服务访问授权的安全管理的技术。

[0010] 例如,在一个示例性实施例中,一种方法包括以下步骤。在包括基于服务的架构的通信系统中的授权实体处,接收来自通信系统中的服务消费者的对访问给定服务类型的请

求。授权实体处获得标识针对给定服务类型的多个服务生产者的访问令牌,并将访问令牌发送到服务消费者。

[0011] 在另一个实施例中,一种方法包括以下步骤。在包括基于服务的架构的通信系统中的服务消费者向通信系统中的授权实体发送对访问给定服务类型的请求。服务消费者从授权实体接收访问令牌,其中,该访问令牌标识通信系统中针对给定服务类型的多个服务生产者。基于一个或多个选择准则,根据访问令牌选择多个服务生产者中的一个服务生产者。

[0012] 在另一个实施例中,一种方法包括以下步骤。在包括基于服务的架构的通信系统中的代理单元处接收访问令牌,其中,该访问令牌标识通信系统中针对给定服务类型的多个服务生产者并且由通信系统中的授权实体响应于通信系统中的服务消费者的对访问给定服务类型的请求而生成。在代理单元处,基于一个或多个选择准则,根据访问令牌选择多个服务生产者中的一个服务生产者。在附加实施例中,代理单元向服务消费者发送用于所选择的服务生产者的标识信息。

[0013] 在又一个实施例中,一种方法包括以下步骤。在包括基于服务的架构的通信系统中的服务消费者处从授权实体接收访问令牌,其中,该访问令牌标识与通信系统中针对给定服务类型的服务生产者相对应的多个代理单元。服务消费者根据访问令牌选择多个代理单元中的一个代理单元,并向所选择的代理单元发送对访问给定服务类型的请求。

[0014] 进一步的示例性实施例以其中体现有可执行程序代码的非暂时性计算机可读存储介质的形式来提供,该可执行程序代码在被处理器执行时使得处理器执行上述步骤。更进一步的示例性实施例包括具有被配置为执行上述步骤的处理器和存储器的装置。

[0015] 本文描述的实施例的这些和其他特征和优点将从附图和以下详细描述中变得更加显而易见。

附图说明

[0016] 图1示出可实现一个或多个示例性实施例的通信系统。

[0017] 图2示出用于提供安全管理的利用其可实现一个或多个示例性实施例的网络单元/功能。

[0018] 图3示出具有在受访网络与归属网络之间以及在受访网络和归属网络内进行交互的网络功能的利用其可实现一个或多个示例性实施例的通信系统架构。

[0019] 图4示出根据示例性实施例的用于通信系统中的服务访问授权的方法。

[0020] 图5示出根据示例性实施例的用于生成在通信系统中服务访问授权中使用的访问令牌的方法。

[0021] 图6示出根据示例性实施例的在通信系统中的服务访问授权中使用的访问令牌的至少一部分。

[0022] 图7示出根据示例性实施例的用于在通信系统中的服务发现的方法。

具体实施方式

[0023] 本文将结合示例性通信系统和用于在通信系统中提供安全管理的关联技术来说明实施例。然而,应当理解,权利要求的范围不限于所公开的特定类型的通信系统和/或过

程。可以使用替代过程和操作在各种其他类型的通信系统中实施实施例。例如,虽然在使用3GPP系统单元的无线蜂窝系统(诸如3GPP下一代系统(5G))的上下文中进行了说明,但是所公开的实施例可以以直接的方式适应于各种其他类型的通信系统。

[0024] 根据在5G通信系统环境中实现的示例性实施例,一个或多个3GPP技术规范(TS)和技术报告(TR)提供了与一个或多个示例性实施例交互的网络单元/功能和/或操作的进一步说明,例如,在上面提及的3GPP TS 23.501和3GPP TS 33.501。其他3GPP TS/TR文档提供了本领域普通技术人员将认识到的其他常规细节。然而,虽然非常适合于5G相关的3GPP标准,但是这些实施例并非旨在限于任何特定标准。

[0025] 示例性实施例涉及与用于5G网络的基于服务的架构(SBA)相关联的安全管理。在描述这样的示例性实施例之前,下面首先在图1和2的上下文中描述5G网络的主要组件的一般说明。

[0026] 图1示出了其中实现示例性实施例的通信系统100。应当理解,在通信系统100中所示的单元旨在表示在系统内提供的主要功能,例如,UE接入功能、移动性管理功能、认证功能、服务网关功能等。因此,图1中所示的框是指5G网络中提供这些主要功能的特定单元。然而,在其他实施例中,其他网络单元用于实现所表示的一些或全部主要功能。另外,应当理解,图1中并未示出5G网络的所有功能。而是呈现了有助于解释示例性实施例的功能。随后的附图描绘了一些附加的单元/功能。

[0027] 因此,如图所示,通信系统100包括经由空中接口103与接入点(gNB)104通信的用户设备(UE)102。在一些实施例中,UE 102是移动台,并且这样的移动台可以包括例如移动电话、计算机、或任何其他类型的通信设备。因此,本文所使用的术语“用户设备”旨在被广义地进行解释,以涵盖各种不同类型的移动台、订户台站、或更一般地通信设备,包括诸如插入膝上型计算机或其他设备(诸如智能手机)中的数据卡的组合之类的示例。这样的通信设备还旨在涵盖通常被称为接入终端的设备。

[0028] 在一个实施例中,UE 102包括通用集成电路卡(UICC)部分和移动设备(ME)部分。UICC是UE的用户相关部分,并且包含至少一个通用订户标识模块(USIM)和合适的应用软件。USIM安全地存储永久性订阅标识符及其相关密钥,其用于识别和认证接入网络的订户。ME是UE的用户无关部分,并且包含终端设备(TE)功能和各种移动终端(MT)功能。

[0029] 注意,在一个示例中,永久性订阅标识符是UE的国际移动订户标识(IMSI)。在一个实施例中,IMSI的长度是固定的15个数位,并且包括3个数位的移动国家代码(MCC)、3个数位的移动网络代码(MNC)、以及9个数位的移动台识别号码(MSIN)。在5G通信系统中,IMSI被称为订阅永久性标识符(SUPI)。如果IMSI用作SUPI,则MSIN提供订户标识。因此,通常仅需要对IMSI的MSIN部分进行加密。IMSI的MNC和MCC部分提供路由信息,服务网络使用该路由信息路由到正确的归属网络。在SUPI的MSIN被加密时,它被称为订阅隐藏标识符(SUCI)。

[0030] 接入点104示例性地是通信系统100的接入网络的一部分。这种接入网络例如包括具有多个基站和一个或多个相关联的无线电网络控制功能的5G系统。在一些实施例中,基站和无线电网络控制功能是在逻辑上分离的实体,但在一些实施例中,它们在相同的物理网络单元(例如,基站路由器或毫微微蜂窝接入点)中实现。

[0031] 在该示例性实施例中,接入点104可操作地耦接到移动性管理功能106。在5G网络中,移动性管理功能由接入和移动性管理功能(AMF)实现。在一些实施例中,安全锚功能

(SEAF)也通过AMF将UE与移动性管理功能相连来实现。如本文所使用的,移动性管理功能是通信系统的核心网络(CN)部分中的单元或功能(即,实体),其管理或以其他方式参加与UE的接入和移动性(包括认证/授权)操作(通过接入点104)以及其他网络操作。AMF在本文中也更一般地被称为接入和移动性管理实体。

[0032] 在该示例性实施例中,AMF 106可操作地耦接到归属订户功能108,即,驻留在订户的归属网络中的一个或多个功能。如图所示,这些功能中的一些包括统一数据管理(UDM)功能以及认证服务器功能(AUSF)。AUSF和UDM(单独地或共同地)在本文中也更一般地被称为认证实体。另外,归属订户功能包括但不限于网络切片选择功能(NSSF)、网络开放功能(NEF)、网络功能存储功能(NRF)、策略控制功能(PCF)、以及和应用功能(AF)。

[0033] 需要注意的重要一点是在诸如5G系统之类的SBA通信系统中,控制平面使用服务模型方法,其中组件(NF)查询NRF以通过应用编程接口(API)发现彼此并进行通信。NF服务发现和授权方法将在下面进一步详细描述。

[0034] 接入点104还可操作地耦接到服务网关功能,即,会话管理功能(SMF)110,其可操作地耦接到用户平面功能(UPF)112。UPF 112可操作地耦接到分组数据网络,例如,因特网114。在此没有描述此类网络单元的其他典型操作和功能,因为它们不是示例性实施例的重点并且可以在合适的3GPP 5G文档中找到。

[0035] 应当理解,系统单元的这种特定设置仅仅是示例,并且在其他实施例中,可以使用其他类型和设置的附加或替代单元来实现通信系统。例如,在其他实施例中,系统100包括在此并未明确示出的其他单元/功能。

[0036] 因此,图1的设置仅仅是无线蜂窝系统的一种示例性配置,可以使用多种替代的系统单元配置。例如,虽然在图1中仅示出了单个单元/功能,但这仅是为了简化且明确描述。给定的替代实施例当然可以包括更多数量的这种系统单元,以及通常与常规系统实现相关联的类型的附加或替代单元。

[0037] 还应注意,虽然图1将系统单元示出为单个功能块,但是组成5G网络的各个子网被划分成所谓的网络切片。网络切片(网络分区)包括一系列网络功能(NF)集(即,功能链),每个功能对应于在公共物理基础架构上使用网络功能虚拟化(NFV)的服务类型。可以针对给定服务(例如,eMBB服务、大规模IoT服务、以及关键任务IoT服务)按需实例化网络切片。因此,当创建网络切片或功能的实例时,该网络切片或功能被实例化。在一些实施例中,这涉及在底层物理基础架构的一个或多个主机设备上安装或以其他方式运行网络切片或功能。UE 102被配置为经由gNB 104访问这些服务中的一个或多个。NF还可以访问其他NF的服务。

[0038] 图2是示例性实施例中用于提供安全管理的网络单元/功能的框图。系统200被示出为包括第一网络单元/功能202和第二网络单元/功能204。应当理解,网络单元/功能202和204表示被配置为提供本文所描述的安全管理和其他技术的任何网络单元/功能,例如但不限于AMF、SEAF、UDM、AUSF、NSSF、NEF、NRF、PCF和AF。

[0039] 网络单元/功能202包括被耦接到存储器216和接口电路210的处理器212。网络单元/功能202的处理器212包括安全管理处理模块214,该安全管理处理模块214可以至少部分地以由处理器执行的软件的形式来实现。处理模块214执行结合后续附图以及在本文中以其他方式描述的安全管理。网络单元/功能202的存储器216包括安全管理存储模块218,该安全管理存储模块218存储在安全管理操作期间生成或以其他方式使用的数据。

[0040] 网络单元/功能204包括被耦接到存储器226和接口电路220的处理器222。网络单元/功能204的处理器222包括安全管理处理模块224,该安全管理处理模块224可以至少部分地以由处理器222执行的软件的形式来实现。处理模块224执行结合后续附图以及在本文中以其他方式描述的安全管理。网络单元/功能204的存储器226包括安全管理存储模块228,该安全管理存储模块228存储在安全管理操作期间生成或以其他方式使用的数据。

[0041] 相应的网络单元/功能202和204的处理器212和222例如可以包括微处理器、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、数字信号处理器(DSP)或其他类型的处理设备或集成电路、以及这些元件的部分或组合。这种集成电路设备及其部分或组合是在本文中所使用的术语“电路”的示例。硬件及相关联的软件或固件的各种各样的其他布置可被用于实现示例性实施例。

[0042] 相应的网络单元/功能202和204的存储器216和226可被用于存储由相应的处理器212和222执行以实现本文所描述的功能的至少一部分的一个或多个软件程序。例如,可以使用由处理器212和222执行的软件代码以直接的方式来实现结合后续附图以及在本文中以其他方式描述的安全管理操作和其他功能。

[0043] 因此,存储器216或226中给定的一个存储器因此可以被视为其中体现可执行程序代码的在本文中一般地被称为计算机程序产品或者更一般地被称为处理器可读存储介质的示例。处理器可读存储介质的其他示例可以包括以任何组合形式的磁盘或其他类型的磁或光介质。示例性实施例可以包括制品,其包括此类计算机程序产品或其他处理器可读存储介质。

[0044] 存储器216或226例如可以更特别地包括电子随机存取存储器(RAM),诸如静态RAM(SRAM)、动态RAM(DRAM)或其他类型的易失性或非易失性电子存储器。后者例如可以包括非易失性存储器,诸如闪存存储器、磁RAM(MRAM)、相变RAM(PC-RAM)或铁电RAM(FRAM)。在本文中所使用的术语“存储器”旨在被广义地进行解释,并且可以附加地或可替代地涵盖例如只读存储器(ROM)、基于磁盘的存储器、或其他类型的存储设备、以及这些设备的部分或组合。

[0045] 相应的网络单元/功能202和204的接口电路210和220示例性地包括收发机或允许相关联的系统单元以本文所描述的方式彼此通信的其他通信硬件或固件。

[0046] 从图2中可以看出网络单元/功能202被配置为经由它们各自的接口电路210和220与网络单元/功能204进行通信,反之亦然。此通信涉及网络单元/功能202向网络单元/功能204发送数据,以及网络单元/功能204向网络单元/功能202发送数据。然而,在替代实施例中,其他网络单元可以被可操作地耦接在网络单元/功能202与204之间。在本文中所使用的术语“数据”旨在被广义地进行解释,以涵盖可在网络单元/功能之间(以及在用户设备与核心网络之间)发送的任何类型的信息,包括但不限于消息、标识符、密钥、指示符、用户数据、控制数据等。

[0047] 因此,在一个示例中,网络单元/功能202是NF(诸如AMF),而网络单元/功能204是NRF。在这种情况下,AMF和NRF参加到服务访问授权方法(发现和选择)中并根据需要交换消息/数据。这种服务访问授权方法将在下面进一步详细描述。

[0048] 应当理解,图2中所示的组件的特定设置仅仅是示例,而多种替代配置在其他实施例中使用。例如,任一给定的网络单元/功能可以被配置为合并附加或替代的组件以及支持其他通信协议。

[0049] 诸如UE 102和gNB 104之类的其他系统单元也可以各自被配置为包括诸如处理器、存储器和网络接口之类的组件。这些元件无需在单独的独立处理平台上实现,而是例如可以表示单个公共处理平台的不同功能部分。

[0050] 在给出上述一般性概念的情况下,现在将描述解决某些安全管理问题的示例性实施例。更特别地,示例性实施例提供了用于5G系统的安全管理技术。用于5G系统的架构目前正在3GPP中进行标准化。如上所述,3GPP TS 23.501将5G系统架构定义为基于服务的,例如,基于服务的架构(SBA)。

[0051] 图3描绘了采用包括受访公共陆地移动网络(VPLMN)310的配置的5G架构300,该公共陆地移动网络(VPLMN)310可操作地经由中间的因特网分组交换(IPX)网络320被耦接到归属公共陆地移动网络(HPLMN)330。注意,在VPLMN 310和HPLMN 330之间可操作地耦接的IPX网络能多于一个。图3还示出了在每个PLMN的边缘处存在安全边缘保护代理(SEPP),即,在VPLMN 310中的vSEPP 312和在HPLMN 330中的hSEPP 332。应当理解,在VPLMN 310和HPLMN 330中所示的各种网络功能是已知的,并且在诸如但不限于在上面提及的TS 23.501和TS 33.501之类的各种5G规范中详细描述。

[0052] 如上所述,在5G中,SBA被引入以将服务建模为使用Restful应用编程接口(表述性状态转移API)来彼此通信的网络功能(NF)。在其中两个通信NF在两个不同的PLMN(例如,VPLMN 310和HPLMN 330)中的场景中,通信在两个参加PLMN之间在漫游网络间接口(N32)上发生。

[0053] 为了保护通过漫游网络间接口发送的消息中的NF特定内容,5G引入了SEPP作为驻留在PLMN网络的外围处的实体,以保护PLMN免受外部流量的影响,并且附加地实现了针对在服务层的两个网络间网络功能之间交换的所有数据和信令的传输层安全(TLS)和应用层安全(ALS)。例如,在通过漫游N32接口从外部发送消息之前,SEPP对超文本传输协议(HTTP)消息中的信息元素(IE)执行安全管理功能。受保护的HTTP消息被称为N32消息。诸如ALS之类的保护涉及保护在HTTP消息的各部分中发送的信息,包括但不限于HTTP请求/响应行、HTTP报头以及HTTP有效载荷。然而,此消息的一些部分可能需要由在两个SEPP之间的中介(例如,如图3中所示的IPX 330的网络提供商)进行修改。

[0054] 因此,在5G SBA中,PLMN运营商在其网络的边缘处部署SEPP,以进行互操作并从其漫游伙伴网络中的网络功能获得服务。SEPP通过N32接口与一个或多个其他网络中的一个或多个其他SEPP接口连接。作为边缘代理,SEPP实现了如上所述的ALS,以保护在其网络中的网络功能与漫游伙伴网络中的另一个网络功能之间交换的HTTP消息。

[0055] 虽然如图3所示两个NF可以在不同的PLMN中,但同一PLMN中的一些NF也有通信的需要。在任一场景(PLMN间通信或PLMN内通信)中,SBA通信模型都包括使“NF服务消费者”(服务客户端)能够被认证并被授权访问由“NF服务生产者”(服务服务器)提供或以其他方式与其相关联的服务的安全方法。在上面引用的3GPP TS 33.501(版本15)中所支持的授权方法之一是基于OAuth 2.0访问令牌方法。在5G系统中,当使用OAuth 2.0时采用以下模型:(i)NRF是OAuth 2.0授权服务器;(ii)NF服务消费者是OAuth 2.0客户端;以及(iii)NF服务生产者是OAuth 2.0资源服务器。

[0056] NF服务消费者(客户端)经由NRF发现NF服务生产者(资源服务器),然后在调用服务API请求时获得访问令牌以呈现给NF服务生产者。在已有的方法(如在上面引用的3GPP

TS 33.501(版本15)中所描述的)中,访问令牌被绑定到在发现过程结束时由NRF或NF服务消费者选择的特定NF生产者实例。

[0057] 示例性实施例认识到通过将访问令牌绑定到特定的单个NF生产者实例,选择逻辑被防止从NF生产者实例池中进行选择。示例性实施例进一步认识到从实例池中进行选择与以下这些情况相关:当前使用的实例失败的情况,或者当出于负载平衡的目的而期望快速地选择不同的实例时,或者在中间代理实体将会代表NF服务消费者进行选择的情况下。另外,示例性实施例认识到在访问令牌与NF生产者实例之间具有1:1的关联性是次优的,因为每次服务生产者发生变化时,它都迫使NF消费者获得新令牌。实际上,当前的3GPP标准化方案要求NF服务消费者针对每个服务请求取得新的访问令牌,并且这种访问令牌是依据NF服务消费者想要从中获得服务的每个NF生产者实例的。参见在上面引用的3GPP TS 33.501,条款13.4。

[0058] 如将在本文中进一步详细解释的,示例性实施例提供了改进的服务访问授权,其使得服务选择逻辑能够从两个或更多个NF生产者实例中进行选择。例如,在一个实施例中,NRF生成基于JavaScript对象标记(JSON)Web令牌的访问令牌,并用用于一组被发现的生产者NF实例或生产者NF服务实例的端点地址(即,统一资源定位符或URL)来填充该令牌中的受众声明字段。当NF服务消费者在发现步骤之后请求访问令牌时,NRF返回所生成的令牌。NF选择逻辑使用受众声明字段以基于各种因素(诸如但不限于负载平衡)来选择生产者NF实例。

[0059] 图4示出了作为方法400的整个过程的示例。

[0060] 如在步骤402中所示,在NF服务发现过程期间,NRF在访问令牌中捕获所有被发现的NF服务生产者实例的端点地址。

[0061] 在步骤404中,NRF在访问令牌响应消息中将所存储的访问令牌返回给NF服务消费者实例。

[0062] 在步骤406中,选择逻辑(在NF服务消费者或代理中,如在下面将进一步解释的)应用一组准则以基于访问令牌中的条目来选择NF服务生产者实例。如果选择逻辑是在代理中实现的,则该代理可以将所选择的生产者实例的地址提供给NF服务消费者实例。

[0063] 现在将进一步详细描述步骤402、404和406中的每一个。

[0064] 在访问令牌中捕获所有被发现的NF服务生产者实例(步骤402)。作为发现过程的一部分,NRF确定被发现的NF实例或NF服务实例,并将一组被发现的NF实例或NF服务实例的信息经由Nnrf_NFDiscovery_Request响应消息提供给NF服务消费者。该信息包括:用于该组被发现的NF实例或NF服务实例的FQDN(完全限定域名)、IP(因特网协议)地址、或端点地址(即,URL)。发现过程的细节在标题为“技术规范组服务和系统方面;用于5G系统的过程,第2阶段(Technical Specification Group Services and System Aspects;Procedures for the 5G System,Stage 2)”的5G技术规范(TS)23.502,V15.2.0的条款4.17.4中被进一步描述,其内容通过引用全部并入本文中。

[0065] 图5示出了根据示例性实施例的具有附加步骤的方法500,NRF将该附加步骤作为发现过程的一部分来执行。

[0066] 在步骤502中,NRF生成采用JSON Web令牌(JWT)格式的访问令牌,如2015年5月的因特网工程任务组(IETF)征求意见(RFC)7519“JSON Web令牌(JWT)”中所描述的,其公开内

容通过引用全部并入本文中。如将要解释的,此格式被修改为包括多个被发现的服务生产者,如依据下一步骤。

[0067] 在步骤504中,NRF用所有被发现的NF服务生产者实例或NF服务实例的端点地址来填充JSON Web令牌结构中的受众声明字段。在另一个实施例中,如将在下面进一步解释的,访问令牌可以可替代地存储与NF服务生产者实例相对应的代理单元的端点地址。

[0068] 在步骤506中,NRF存储访问令牌,以使得可以在访问令牌响应消息中将其提供给NF服务消费者实例(步骤404)。

[0069] 图6示出了JSON Web令牌(JWT)600的至少一部分,并且具体地示出了受众声明字段如何被用于捕获具有访问令牌的被发现的NF生产者实例的地址。如图所示,JWT 600包括NRF标识字段602(标识生成访问令牌的NRF)、NF消费者标识604(标识请求访问令牌的NF)、以及具有多个NF生产者标识和地址的受众声明字段606。

[0070] 在图6中所示的实施例示例中,受众声明是一个数组,其中该数组的每个元素包括NF实例ID(标识)和被发现的生产者实例的端点地址。关于受众声明如何被格式化的替代实施例是可能的。

[0071] NRF在访问令牌响应消息中返回所存储的请求的访问令牌(步骤404)。在上面引用的3GPP TS 33.501的条款13.4.1.1描述了用于从NRF获得访问令牌的过程。这在服务访问之前由消费者NF实例执行。示例性实施例尤其对已有过程提供了以下改变:

[0072] 1)当NRF从在发现步骤中已针对特定目标NF类型和服务名称进行授权的NF实例ID(服务消费者ID)接收访问令牌请求消息时,NRF跳过再次对NF服务消费者实例的重新授权(这是已有过程中的步骤2)。

[0073] 2)NRF取得在发现过程期间针对此NF实例ID生成的访问令牌(步骤402),并将其在访问令牌响应中提供。

[0074] 如以上在步骤402的上下文中所描述的,访问令牌被填充有被发现的NF服务生产者实例的所有必需信息。

[0075] 图7示出了根据示例性实施例的用于服务发现方法700的修改消息流。更特别地,如步骤1中所示,NF服务消费者702向NRF(授权服务器)704发送访问令牌请求。该访问令牌请求包括NF实例ID、预期NF服务名称、以及预期NF服务类型。在步骤2中,NRF 704取得针对此请求的所存储的访问令牌。然后,在步骤3中,NRF 704向NF服务消费者702发送访问令牌响应,其包括访问令牌、该令牌的到期时间、以及该令牌的范围。

[0076] 选择逻辑选择NF服务生产者实例(步骤406)。NF服务消费者实例接收包括访问令牌的访问令牌响应消息。然后,NF服务消费者实例应用一组评估因子,以确定针对服务请求使用哪个NF服务生产者实例。NF服务消费者执行服务请求API,以从所选择的NF服务生产者实例获得服务。访问令牌被包括在该请求中。注意,在一些实施例中,选择逻辑是NF服务消费者实例的一部分,而在其他实施例中,选择逻辑是代理单元的一部分。

[0077] 在给出以上说明性描述的情况下,在下面进一步描述一些示例性实施例。

[0078] 1.基于服务的架构(TS 33.501的版本15),其中,选择是由NF服务消费者实例执行的。这是Rel-15模型,其中,NF服务消费者从NRF获得访问令牌以从所选择的NF生产者实例获得服务,并将此令牌包含在被寻址到NF服务生产者实例的API服务请求中。该实现允许NF服务消费者使用一个访问令牌从多于一个的有资格的NF服务生产者实例获得服务。

[0079] 2.在其中代理用作用于PLMN内NF之间的所有或一些服务层消息的中心枢纽(hub)的架构中。

[0080] a.代理是从由NRF在NF服务发现响应中提供的NF服务生产者列表中选择NF服务生产者的实体。在一些实施例中,代理功能也驻留在NRF它本身中或具有到NRF的专有接口。NRF在NF服务发现响应消息中将此信息提供给NF服务消费者。

[0081] b.NF服务消费者将所获得的访问令牌包括在被寻址到NF服务生产者实例的API服务请求中。

[0082] c.在一些实施例中,代理对API服务请求应用负载平衡,这可导致由代理从在访问令牌中存在的NF生产者实例列表中选择新的NF生产者实例。在一些实施例中,代理还基于除了负载平衡之外的原因来选择NF生产者实例。

[0083] d.代理将服务请求路由到所选择的NF服务生产者实例。

[0084] 3.在其中代理仅在NF服务消费者与NF服务生产者之间的架构中。在此模型中,在NF服务消费者与NRF之间不存在代理。也就是说,代理仅侦听在两个NF之间的通信。

[0085] 因此,在一些实施例中,代理从服务消费者而不是从NRF接收访问令牌。

[0086] 如上面的场景2c中所示,在一些实施例中,代理通过改变由NF服务消费者基于访问令牌中的信息而做出的选择来对API服务请求应用负载平衡、或一些其他与选择相关的功能。

[0087] 在替代实施例中,如上面在图5的步骤504中所述,NRF可以生成存储代理单元的端点地址的访问令牌,而不是存储服务生产者的端点地址的访问令牌。此实施例例如在代理位于两个NF(服务消费者和服务生产者)之间并且服务生产者地址在外部不可见时是很有用的。代理被用作后端中的一个或多个服务生产者实例的门卫。因此,在此替代模型中,NRF用代理(单元)的端点地址来填充受众声明字段。NF服务消费者选择一个地址,并将该消息发送到代理。然后,代理选择服务提供者实例。

[0088] 因此,有利地,在此模型中,服务消费者和与服务生产者相关联的代理单元进行通信。换句话说,在服务消费者与所选择的服务生产者之间没有直接连接。连接通过代理进行。此外,在此模型中,代理可以选择基于负载平衡准则或其他准则来改变所选择的生产者。代理使用访问令牌中的受众声明字段来选择不同的服务生产者。

[0089] 在其他实施例中,代理单元可以驻留在NRF中、驻留在NF服务消费者中、和/或驻留在一个或多个NF服务生产者中。

[0090] 除了负载平衡准则被用于服务生产者选择准则之外,还可以使用其他准则,诸如可用性(例如,服务生产者变得不可用/故障)和/或计划维护(例如,用于软件升级)。此外,在一些实施例中,选择准则包括一个或多个运营商配置的策略准则。

[0091] 因此,应再次强调,本文描述的各种实施例仅通过示例性示例的方式来呈现,并且不应被解释为限制权利要求的范围。例如,替代实施例可以使用与以上在示例性实施例的上下文中描述的那些不同的通信系统配置、用户设备配置、基站配置、密钥对提供和使用过程、消息协议和消息格式。在所附权利要求的范围内的这些和多种其他替代实施例对于本领域技术人员将是显而易见的。

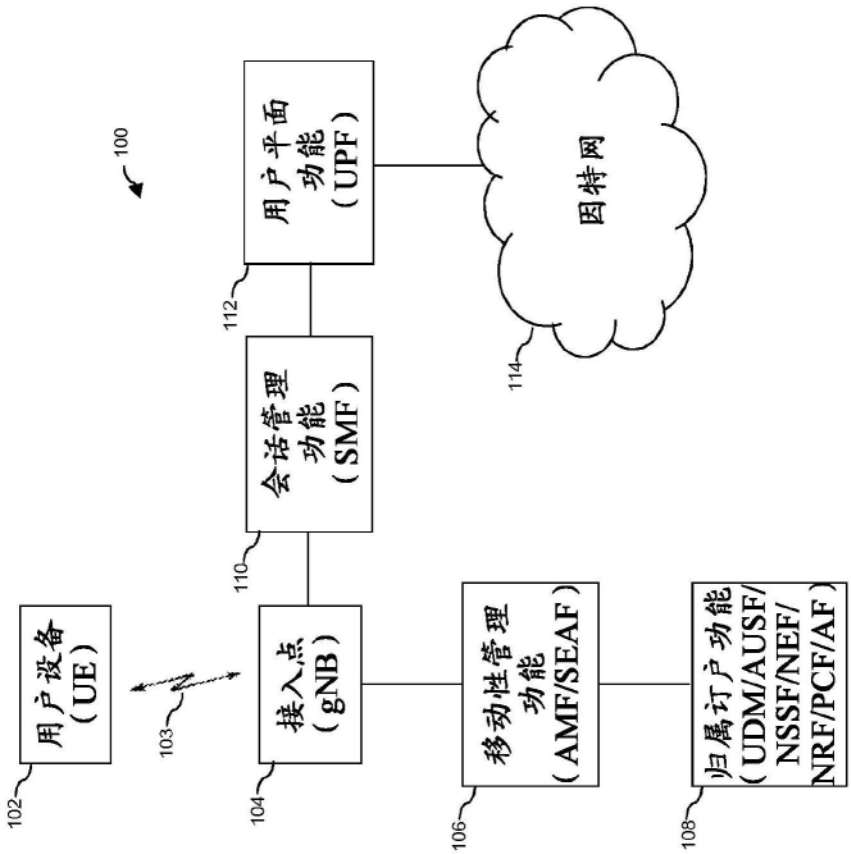

100
用户设备
(UE)
102
103
接入点
(gNB)
104
会话管理
功能
(SMF)
110
用户平面
功能
(UPF)
112
因特网
114
移动性管理
功能
(AMF/SEAF)
106
归属订户功能
(UDM/AUSF/
NSSF/NEF/
NRF/PCF/AF)
108

图1

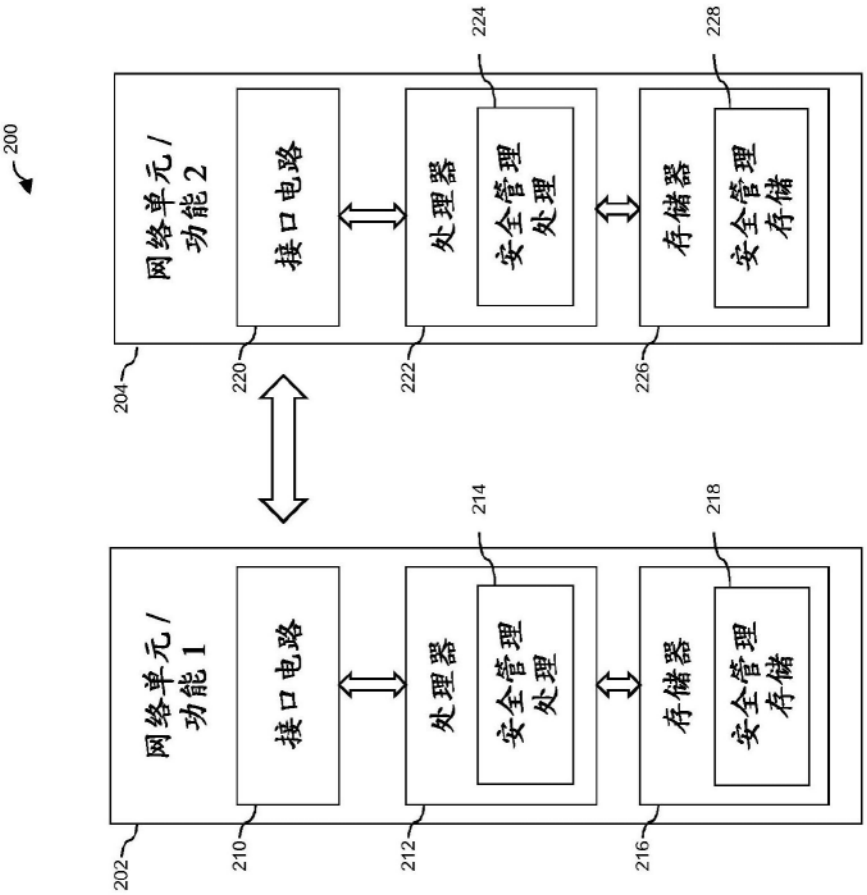

200
网络单元 / 功能 2
接口电路
处理器
安全管理处理
存储器
安全管理存储
204
220
222
224
226
228
网络单元 / 功能 1
接口电路
处理器
安全管理处理
存储器
安全管理存储
202
210
212
214
216
218

图2

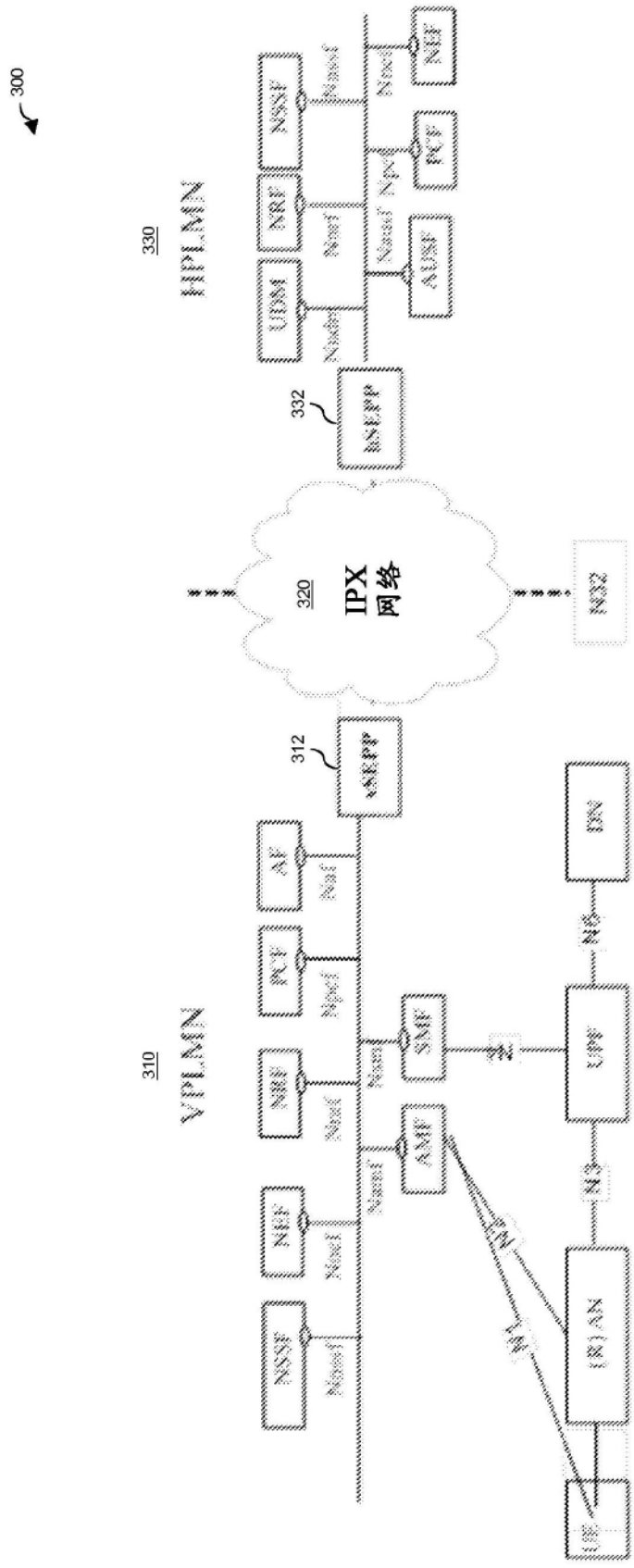

300
330
HPLMN
NSSF
NRF
UDM
NEF
PCF
AUSF
Nnssf
Nnrf
Nudm
Npcf
Nausf
332
N32-FP
320
IPX
网络
N32
312
N32-FP
310
VPLMN
AF
PCF
NRF
NEF
NSSF
SMF
AMF
UPF
DN
N6
N3
N2
N1
(R)AN
UE

图3

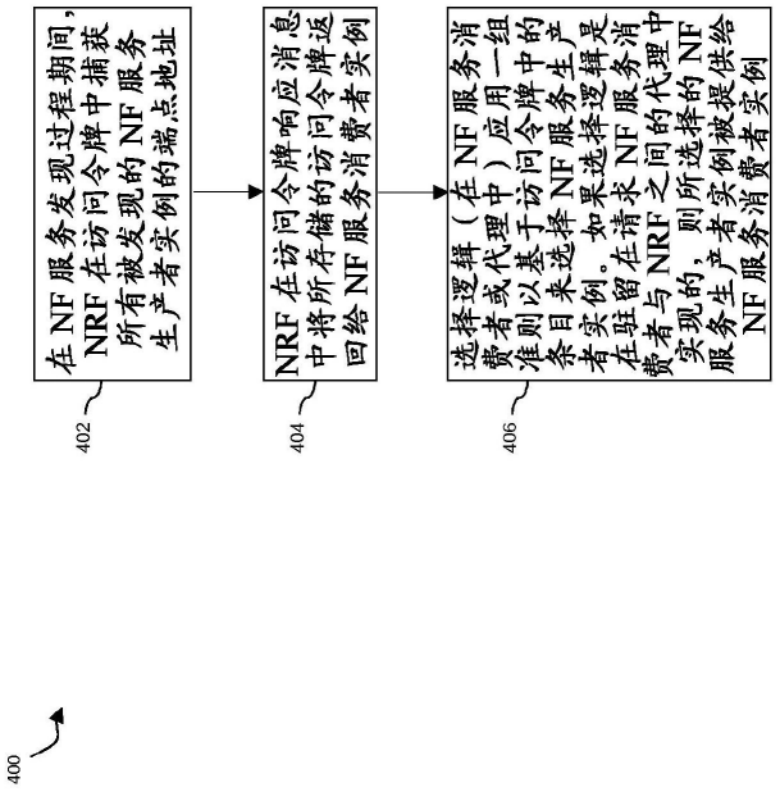

在NF服务发现过程期间，NRF在访问令牌中捕获所有被发现的NF服务生产者实例的端点地址
402
NRF在访问令牌响应消息中将所存储的访问令牌返回给NF服务消费者实例
404
选择逻辑（在NF服务消费者或代理中）应用一组准则以基于访问令牌中的条目来选择NF服务生产者实例。如果选择逻辑是在驻留在请求NF服务消费者与NRF之间的代理中实现的，则所选择的NF服务生产者实例被提供给NF服务消费者实例
406
400

图4

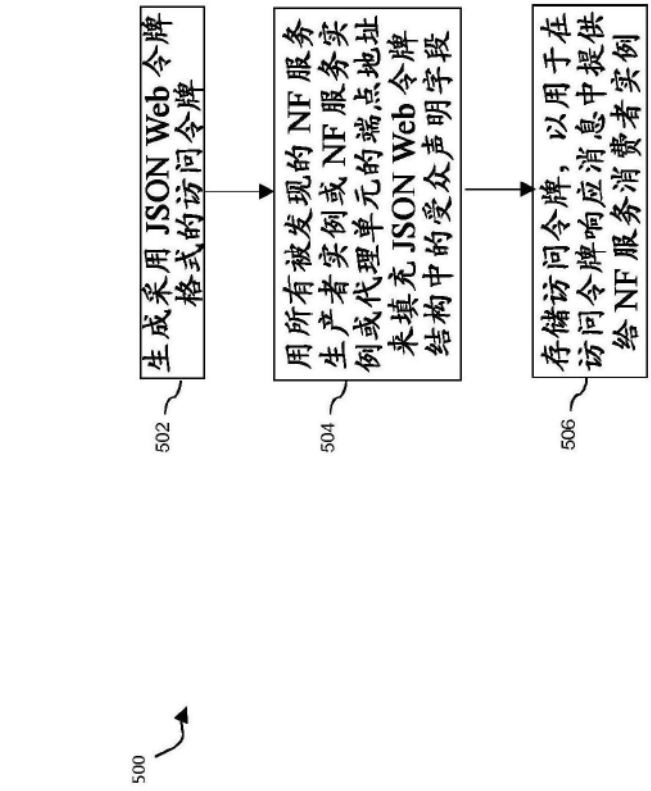

生成采用JSON Web令牌格式的访问令牌
502
用所有被发现的NF服务生产者实例或NF服务实例或代理单元的端点地址来填充JSON Web令牌结构中的受众声明字段
504
存储访问令牌，以用于在访问令牌响应消息中提供给NF服务消费者实例
506
500

图5

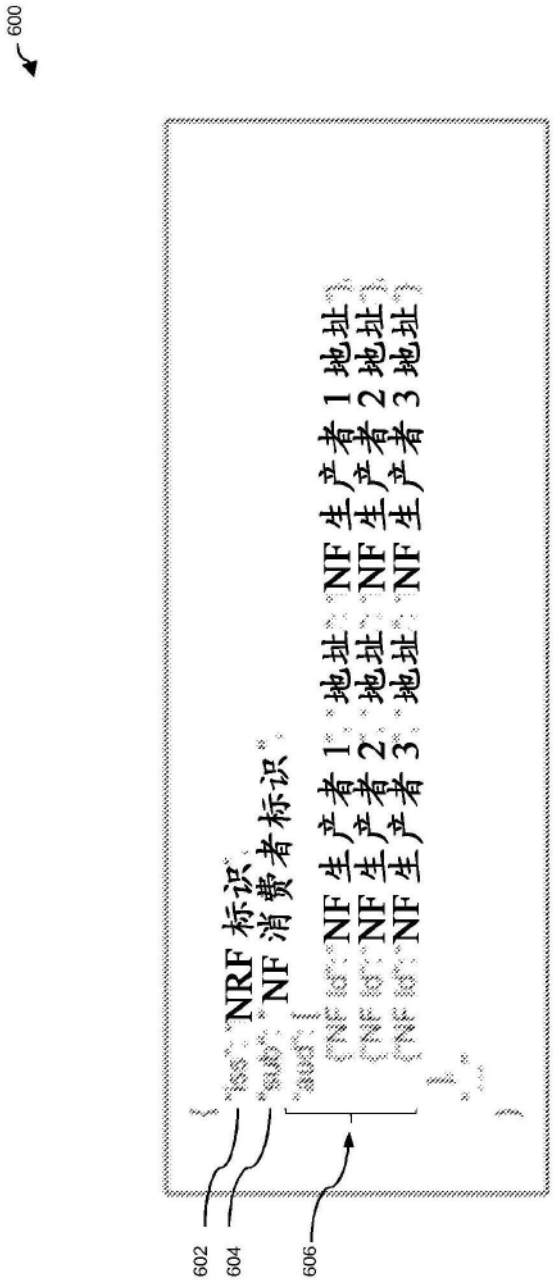

600
"iss": "NRF 标识",
"sub": "NF 消费者标识",
"aud": [
"NF 生产者 1": "地址",
"NF 生产者 2": "地址",
"NF 生产者 3": "地址"
]
602
604
606

图6

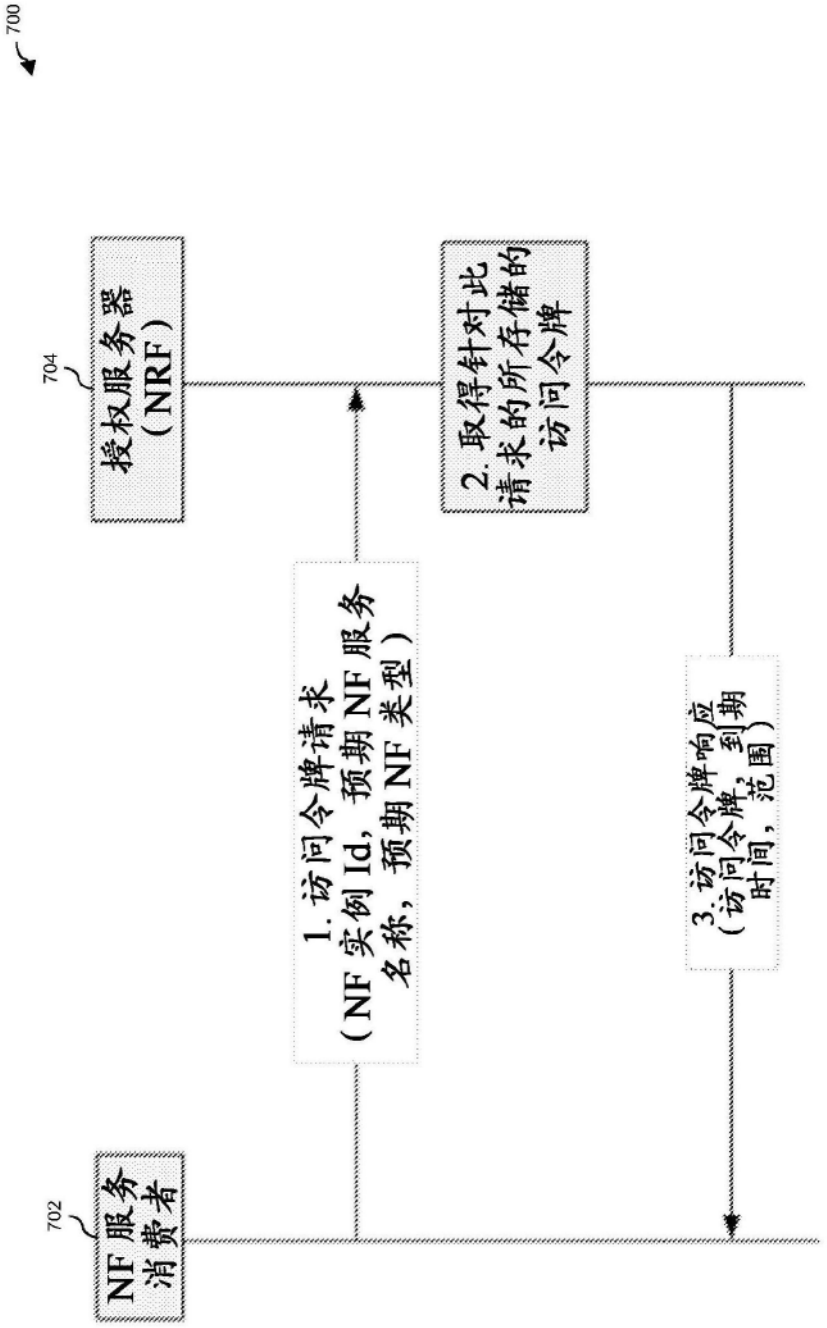

700
授权服务器（NRF）
704
NF服务消费者
702
1. 访问令牌请求（NF实例Id，预期NF服务名称，预期NF类型）
2. 取得针对此请求的所存储的访问令牌
3. 访问令牌响应（访问令牌，到期时间，范围）

图7