(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117178519 A
(43)申请公布日 2023.12.05

(21)申请号 202280029581.4

(22)申请日 2022.01.27

(30)优先权数据
17/198,815 2021.03.11 US

(85)PCT国际申请进入国家阶段日
2023.10.19

(86)PCT国际申请的申请数据
PCT/US2022/014087 2022.01.27

(87)PCT国际申请的公布数据
WO2022/191932 EN 2022.09.15

(71)申请人 甲骨文国际公司
地址 美国加利福尼亚

(72)发明人 V·辛格 J·拉杰普特 A·斯里瓦斯塔瓦

(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
专利代理师 林小枫

(51)Int.Cl.
H04L 9/40(2006.01)

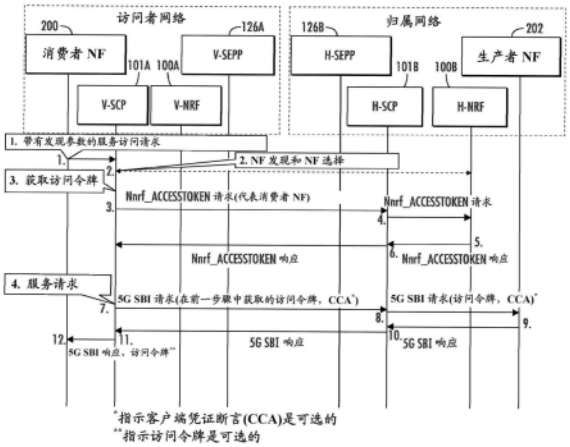
权利要求书3页 说明书13页 附图14页

(54)发明名称

用于服务通信代理(SCP)处的委托授权的方法、系统和计算机可读介质

(57)摘要

用于服务通信代理(SCP)处的委托授权的方法,包括从不支持基于访问令牌的授权的消费者网络功能(NF)截取基于服务的接口(SBI)请求。所述方法还包括作为访问令牌授权客户端进行操作以代表消费者NF获得第一访问令牌。所述方法还包括使用第一访问令牌使消费者NF能够访问由需要基于访问令牌的授权的第一生产者NF提供的服务。SCR还可以起代表不支持基于访问令牌的授权的NRF的访问令牌授权服务器的作用。



CN 117178519 A

1.一种用于在服务通信代理SCP处的委托授权的方法,所述方法包括:

在包括至少一个处理器和存储器的第一SCP处:

从不支持基于访问令牌的授权的第一消费者网络功能NF截取基于服务的接口SBI请求;

作为访问令牌授权客户端代理进行操作以代表第一消费者NF获得第一访问令牌;以及

使用第一访问令牌使第一消费者NF能够访问由需要基于访问令牌的授权的第一生产者NF提供的服务。

2.按照权利要求1所述的方法,其中作为访问令牌授权客户端代理进行操作包括与NF储存库功能NRF进行信令通信以获得第一访问令牌。

3.按照权利要求2所述的方法,其中与所述NRF进行信令通信以获得第一访问令牌包括:

代表第一消费者NF生成访问令牌请求;

向所述NRF发送所述访问令牌请求;以及

从所述NRF接收包括第一访问令牌的访问令牌响应。

4.按照权利要求3所述的方法,其中生成所述访问令牌请求包括从所述SBI请求的用户代理报头提取要包括在所述访问令牌请求中的至少一些属性的值。

5.按照权利要求4所述的方法,其中提取至少一些属性的值包括从所述SBI请求的用户代理报头提取第一消费者NF的NF实例ID。

6.按照任一前述权利要求所述的方法,其中接收SBI请求包括从第一消费者NF接收SBI服务请求,并且其中使用第一访问令牌使第一消费者NF能够访问由第一生产者NF提供的服务包括:

将第一访问令牌插入所述SBI服务请求中;

将包括第一访问令牌的所述SBI服务请求转发给第一生产者NF;

从第一生产者NF接收SBI服务响应;以及

将所述SBI服务响应转发给第一消费者NF。

7.按照任一前述权利要求所述的方法,其中接收SBI请求包括从第一消费者NF接收SBI服务访问请求,并且其中使用第一访问令牌使第一消费者NF能够访问由第一生产者NF提供的服务包括:

基于响应于所述SBI服务访问请求而进行的委托发现和NF选择来生成SBI服务请求;

将第一访问令牌插入所述SBI服务请求中;

将包括第一访问令牌的SBI服务请求转发给第一生产者NF;

从第一生产者NF接收SBI服务响应;以及

将所述SBI服务响应转发给第一消费者NF。

8.按照任一前述权利要求所述的方法,包括:

从第二消费者NF或第二SCP接收访问令牌请求;

响应于来自第二消费者NF或第二SCP的所述访问令牌请求,作为代表不支持访问令牌授权的NF储存库功能NRF的访问令牌授权服务器代理进行操作;以及

与第二消费者NF或第二SCP和第二生产者NF进行信令通信,以使第二消费者NF能够访问由第二生产者NF提供的服务。

9.按照权利要求8所述的方法,其中作为访问令牌授权服务器代理进行操作包括:

响应于所述访问令牌请求,生成第二访问令牌;以及

将包括第二访问令牌的访问令牌响应发送给第二消费者NF或第二SCP。

10.按照权利要求8所述的方法,其中与第二生产者NF进行信令通信以使第二消费者NF能够访问由第二生产者提供的服务包括:

从第二消费者NF或第二SCP接收包括第二访问令牌的第二SBI服务请求;

从第二SBI服务请求中移除第二访问令牌;

将第二SBI服务请求转发给第二生产者NF;

从第二生产者NF接收SBI服务响应;以及

将所述SBI服务响应转发给第二消费者NF或第二SCP。

11.一种用于服务通信代理SCP处的委托授权的系统,所述系统包括:

第一SCP,第一SCP包括至少一个处理器和存储器;和

由所述至少一个处理器实现的访问令牌授权客户端代理,用于从不支持基于访问令牌的授权的第一消费者网络功能NF截取基于服务的接口SBI请求,作为访问令牌授权客户端进行操作以代表第一消费者NF获得第一访问令牌,以及使用第一访问令牌使第一消费者NF能够访问由需要基于访问令牌的授权的第一生产者NF提供的服务。

12.按照权利要求11所述的系统,其中所述访问令牌授权客户端代理被配置为与NF储存库功能NRF进行信令通信以获得第一访问令牌。

13.按照权利要求12所述的系统,其中所述访问令牌授权客户端代理被配置为通过以下方式与所述NRF进行信令通信以获得第一访问令牌:

代表第一消费者NF生成访问令牌请求;

向所述NRF发送所述访问令牌请求;以及

从所述NRF接收包括第一访问令牌的访问令牌响应。

14.按照权利要求13所述的系统,其中所述访问令牌授权客户端代理被配置为通过从所述SBI请求的用户代理报头提取要包括在所述访问令牌请求中的至少一些属性的值来生成所述访问令牌请求。

15.按照权利要求14所述的系统,其中由所述访问令牌授权客户端代理提取的值包括来自所述SBI请求的用户代理报头的第一消费者NF的NF实例ID。

16.按照权利要求11至15任一所述的系统,其中所述SBI请求包括SBI服务请求,并且所述访问令牌授权客户端代理被配置为通过以下方式使用第一访问令牌使第一消费者NF能够访问服务:

将第一访问令牌插入所述SBI服务请求中;

将包括第一访问令牌的所述SBI服务请求转发给第一生产者NF;

从第一生产者NF接收SBI服务响应;以及

将所述SBI服务响应转发给第一消费者NF。

17.按照权利要求11至16任一所述的系统,其中所述SBI请求包括来自第一消费者NF的SBI服务访问请求,并且所述访问令牌授权客户端代理被配置为通过以下方式使用第一访问令牌使第一消费者NF能够访问由第一生产者NF提供的服务:

基于响应于所述SBI服务访问请求而进行的委托发现和NF选择来生成SBI服务请求;

将第一访问令牌插入所述SBI服务请求中;

将包括第一访问令牌的所述SBI服务请求转发给第一生产者NF;

从第一生产者NF接收SBI服务响应;以及

将所述SBI服务响应转发给第一消费者NF。

18.按照权利要求11至17任一所述的系统,包括访问令牌授权服务器代理,所述访问令牌授权服务器代理用于:从第二消费者NF或第二SCP接收访问令牌请求;响应于来自第二消费者NF的所述访问令牌请求,作为代表不支持访问令牌授权的NF储存库功能NRF的访问令牌授权服务器进行操作;以及与第二消费者NF或第二SCP和第二生产者NF进行信令通信,以使第二消费者NF能够访问由第二生产者NF提供的服务。

19.按照权利要求18所述的系统,其中在作为访问令牌授权服务器进行操作时,所述访问令牌授权服务器代理被配置为:

响应于所述访问令牌请求,生成第二访问令牌;以及

将包括第二访问令牌的访问令牌响应发送到第二消费者NF或第二SCP,并且其中所述访问令牌授权服务器代理被配置为通过以下方式与第二消费者NF或第二SCP和第二生产者NF进行信令通信,以使第二消费者NF能够访问由第二生产者NF提供的服务:

从第二消费者NF或第二SCP接收包括第二访问令牌的第二SBI服务请求;

从第二SBI服务请求中移除第二访问令牌;

将所述SBI服务请求转发给第二生产者NF;

从第二生产者NF接收SBI服务响应;以及

将所述SBI服务响应转发给第二消费者NF。

20.一种非临时性计算机可读介质,所述非临时性计算机可读介质上存储有可执行指令,所述可执行指令在由计算机的处理器执行时控制所述计算机进行步骤,所述步骤包括:

从不支持基于访问令牌的授权的消费者网络功能NF截取基于服务的接口SBI请求;

作为访问令牌授权客户端进行操作以代表消费者NF获得第一访问令牌;以及

使用第一访问令牌使所述消费者NF能够访问由需要基于访问令牌的授权的生产者NF提供的服务。

用于服务通信代理(SCP)处的委托授权的方法、系统和计算机可读介质

[0001] 优先权声明

[0002] 本申请要求2021年3月11日提交的美国专利申请序列号17/198,815的优先权,该申请的公开内容通过引用整体并入本文中。

技术领域

[0003] 本文中描述的主题涉及网络安全和公共陆地移动网络(PLMN)间兼容性。更具体地,本文中描述的主题涉及用于SCP处的委托授权的方法、系统和计算机可读介质。

背景技术

[0004] 在5G电信网络中,提供服务的网络功能被称为生产者网络功能(NF)或NF服务生产者。消费服务的网络功能被称为消费者NF或NF服务消费者。网络功能可以是生产者NF、消费者NF或者两者兼有,取决于网络功能是在消费服务、生产服务还是既在消费服务又在生产服务。术语“生产者NF”和“NF服务生产者”在本文中可互换使用。类似地,术语“消费者NF”和“NF服务消费者”在本文中可互换使用。

[0005] 给定的生产者NF可以具有许多服务端点,其中服务端点是由生产者NF托管的一个或多个NF实例的联系点。服务端点由网际协议(IP)地址和端口号的组合或完全限定域名来识别,完全限定域名解析为托管生产者NF的网络节点上的IP地址和端口号。NF实例是提供服务的生产者NF的实例。给定的生产者NF可以包括不止一个NF实例。还应注意的是,多个NF实例可以共享同一个服务端点。

[0006] 生产者NF向网络功能储存库功能(NRF)注册。NRF维护可用NF实例的服务简档,服务简档识别由每个NF实例支持的服务。术语“服务简档”和“NF简档”在本文中可互换使用。消费者NF可以订阅接收关于已经向NRF注册的生产者NF实例的信息。

[0007] 除了消费者NF之外,可以订阅接收关于NF服务实例的信息的另一种类型的网络节点是服务通信代理(SCP)。SCP向NRF订阅并获得关于生产者NF服务实例的可达性和服务简档信息。消费者NF连接到服务通信代理,并且服务通信代理对提供所需服务的生产者NF服务实例之间的流量进行负载平衡,或者直接将流量路由到目的生产者NF实例。

[0008] 除了SCP之外,在生产者NF和消费者NF之间路由流量的中间代理节点的其他例子是安全边缘保护代理(SEPP)。SEPP是用于保护在不同的5G公共陆地移动网络(PLMN)之间交换的控制平面流量的网络节点。因此,SEPP对在PLMN之间发送的所有应用程序编程接口(API)消息进行消息过滤、监管和拓扑隐藏。

[0009] 当一个PLMN或网络功能支持OAuth 2.0授权而另一个PLMN或网络功能不支持OAuth 2.0授权时,发生5G通信网络中的一个问题。按照在因特网工程任务组(IETF)请求评议(RFC)6749中规定的OAuth 2.0授权框架,寻求访问可从资源服务器获得的受保护资源的授权客户端首先从授权服务器获得访问令牌。在客户端获得访问令牌之后,客户端向资源服务器发送服务请求。资源服务器核实访问令牌并提供对受保护资源的访问。

[0010] 在5G通信网络的上下文中,NF服务消费者起OAuth 2.0资源客户端的作用,NF服务生产者起OAuth 2.0资源服务器的作用,而NRF起授权服务器的作用。因此,寻求访问由NF服务生产者提供的服务的NF服务消费者与NRF进行信令通信以获得访问令牌从而访问由NF服务生产者提供的资源。在NF服务消费者从NRF获得访问令牌之后,NF服务消费者向NF服务生产者发送服务请求,其中服务请求包括访问令牌。NF服务生产者验证访问令牌,并提供对NF服务消费者请求的服务的访问。

[0011] 虽然OAuth 2.0授权框架致力于在5G通信网络中提供授权,但是如果从不支持OAuth 2.0授权的消费者NF向需要OAuth 2.0访问令牌的生产者NF发送服务请求,则该服务请求将被拒绝。类似地,如果支持OAuth 2.0授权的消费者NF向不支持OAuth 2.0授权的NRF发送访问令牌请求,则发出请求的消费者NF将无法获得访问令牌。

[0012] 当服务消费者的PLMN支持OAuth 2.0授权,而服务生产者的PLMN不支持OAuth 2.0授权时,可能会发生这些类型的不兼容性问题,反之亦然。当来自一个供应商的NF支持OAuth 2.0授权,而来自其他供应商的NF不支持OAuth 2.0授权时,也可能发生这些类型的不兼容性问题。

[0013] 鉴于这些和其他困难,需要一种在存在OAuth 2.0授权不兼容性时,改进网络功能之间的互操作性的方法。

发明内容

[0014] 用于服务通信代理(SCP)处的委托授权的方法包括从不支持基于访问令牌的授权的第一消费者网络功能(NF)截取基于服务的接口(SBI)服务请求。所述方法还包括作为访问令牌授权客户端代理进行操作以代表第一消费者NF获得第一访问令牌。所述方法还包括使用第一访问令牌使第一消费者NF能够访问由需要基于访问令牌的授权的第一生产者NF提供的服务。

[0015] 按照本文中描述的主题的另一个方面,作为访问令牌授权客户端代理进行操作包括与NF储存库功能(NRF)进行信令通信以获得第一访问令牌。

[0016] 按照本文中描述的主题的另一个方面,与所述NRF进行信令通信以获得第一访问令牌包括:代表第一消费者NF生成访问令牌请求;向所述NRF发送所述访问令牌请求;以及从所述NRF接收包括第一访问令牌的访问令牌响应。

[0017] 按照本文中描述的主题的另一个方面,生成所述访问令牌请求包括从所述SBI请求的用户代理报头提取要包括在所述访问令牌请求中的至少一些属性的值。

[0018] 按照本文中描述的主题的另一个方面,提取至少一些属性的值包括从所述SBI请求的用户代理报头提取第一消费者NF的NF实例ID。

[0019] 按照本文中描述的主题的另一个方面,接收SBI请求包括从第一消费者NF接收SBI服务请求,并且使用第一访问令牌使第一消费者NF能够访问由第一生产者NF提供的服务包括:将第一访问令牌插入所述SBI服务请求中;将包括第一访问令牌的所述SBI服务请求转发给第一生产者NF;从第一生产者NF接收SBI服务响应;以及将所述SBI服务响应转发给第一消费者NF。

[0020] 按照本文中描述的主题的另一个方面,接收SBI请求包括从第一消费者NF接收SBI服务访问请求,并且使用第一访问令牌使第一消费者NF能够访问由第一生产者NF提供的服

务包括:基于响应于所述SBI服务访问请求而进行的委托发现和NF选择来生成SBI服务请求;将第一访问令牌插入所述SBI服务请求中;将包括第一访问令牌的所述SBI服务请求转发给第一生产者NF;从第一生产者NF接收SBI服务响应;以及将所述SBI服务响应转发给第一消费者NF。

[0021] 按照本文中描述的主题的另一个方面,用于SCP处的委托授权的方法包括从第二消费者NF或第二SCP接收访问令牌请求;响应于来自第二消费者NF或第二SCP的所述访问令牌请求,作为代表不支持访问令牌授权的NF储存库功能(NRF)的访问令牌授权服务器代理进行操作;以及与第二消费者NF或第二SCP和第二生产者NF进行信令通信,以使第二消费者NF能够访问由第二生产者NF提供的服务。

[0022] 按照本文中描述的主题的另一个方面,作为访问令牌授权服务器代理进行操作包括:响应于所述访问令牌请求,生成第二访问令牌;以及将包括第二访问令牌的访问令牌响应发送到第二消费者NF或第二SCP。

[0023] 按照本文中描述的主题的另一个方面,与第二生产者NF或第二SCP进行信令通信,以使第二消费者NF能够访问由第二生产者NF提供的服务包括:从第二消费者NF接收包括第二访问令牌的第二SBI服务请求;从第二SBI服务请求中移除第二访问令牌;将第二SBI服务请求转发给第二生产者NF;从第二生产者NF接收SBI服务响应;以及将所述SBI服务响应转发给第二消费者NF或第二SCP。

[0024] 按照本文中描述的主题的另一个方面,生成第二访问令牌包括生成OAuth 2.0访问令牌,所述OAuth 2.0访问令牌包括具有语法上正确的声明的虚拟访问令牌。

[0025] 按照本文中描述的主题的另一个方面,提供一种用于服务通信代理(SCP)处的委托授权的系统。所述系统包括第一SCP,第一SCP包括至少一个处理器和存储器。所述系统还包括由所述至少一个处理器实现的访问令牌授权客户端代理,用于从不支持基于访问令牌的授权的第一消费者网络功能(NF)截取基于服务的接口(SBI)请求,作为访问令牌授权客户端进行操作以代表第一消费者NF获得第一访问令牌,以及使用第一访问令牌使第一消费者NF能够访问由需要基于访问令牌的授权的第一生产者NF提供的服务。

[0026] 按照本文中描述的主题的另一个方面,所述访问令牌授权客户端代理被配置为与NF储存库功能(NRF)进行信令通信以获得第一访问令牌。

[0027] 按照本文中描述的主题的另一个方面,所述访问令牌授权客户端代理被配置为通过以下方式与所述NRF进行信令通信以获得第一访问令牌:代表第一消费者NF生成访问令牌请求;向所述NRF发送所述访问令牌请求;以及从所述NRF接收包括第一访问令牌的访问令牌响应。

[0028] 按照本文中描述的主题的另一个方面,所述访问令牌授权客户端代理被配置为通过从所述SBI请求的用户代理报头提取要包括在所述访问令牌请求中的至少一些属性的值来生成所述访问令牌请求。

[0029] 按照本文中描述的主题的另一个方面,由所述访问令牌授权客户端代理提取的值包括来自所述SBI请求的用户代理报头的第一消费者NF的NF实例ID。

[0030] 按照本文中描述的主题的另一个方面,所述SBI请求包括来自第一消费者NF的SBI服务请求,并且所述访问令牌授权客户端代理被配置为通过以下方式使用第一访问令牌使第一消费者NF能够访问服务:将第一访问令牌插入所述SBI服务请求中;将包括第一访问令

牌的所述SBI服务请求转发给第一生产者NF;从第一生产者NF接收SBI服务响应;以及将所述SBI服务响应转发给第一消费者NF。

[0031] 按照本文中描述的主题的另一个方面,所述SBI请求包括来自第一消费者NF的SBI服务访问请求,并且所述访问令牌授权客户端代理被配置为通过以下方式使用第一访问令牌使第一消费者NF能够访问由第一生产者NF提供的服务:基于响应于所述SBI服务访问请求而进行的委托发现和NF选择来生成SBI服务请求;将第一访问令牌插入所述SBI服务请求中;将包括第一访问令牌的所述SBI服务请求转发给第一生产者NF;从第一生产者NF接收SBI服务响应;以及将所述SBI服务响应转发给第一消费者NF。

[0032] 按照本文中描述的主题的另一个方面,用于SCP处的委托授权的系统包括访问令牌授权服务器代理,所述访问令牌授权服务器代理用于从第二消费者NF或第二SCP接收访问令牌请求;响应于来自第二消费者NF的所述访问令牌请求,作为代表不支持访问令牌授权的NF储存库功能(NRF)的访问令牌授权服务器进行操作;以及与第二消费者NF或第二SCP和第二生产者NF进行信令通信,以使第二消费者NF能够访问由第二生产者NF提供的服务。

[0033] 按照本文中描述的主题的另一个方面,在作为访问令牌授权服务器进行操作时,所述访问令牌授权服务代理被配置为:响应于所述访问令牌请求,生成第二访问令牌;以及将包括第二访问令牌的访问令牌响应发送到第二消费者NF或第二SCP。

[0034] 按照本文中描述的主题的另一个方面,所述访问令牌授权服务器代理被配置为通过以下方式与第二消费者NF或第二SCP和第二生产者NF进行信令通信,以使第二消费者NF能够访问由第二生产者NF提供的服务:从第二消费者NF或第二SCP接收包括第二访问令牌的第二SBI服务请求;从第二SBI服务请求中移除第二访问令牌;将所述SBI服务请求转发给第二生产者NF;从第二生产者NF接收SBI服务响应;以及将所述SBI服务响应转发给第二消费者NF或第二SCP。

[0035] 按照本文中描述的主题的另一个方面,提供一种其上存储有可执行指令的非临时性计算机可读介质,所述可执行指令在由计算机的处理器执行时,控制所述计算机进行步骤。所述步骤包括从不支持基于访问令牌的授权的消费者网络功能(NF)截取基于服务的接口(SBI)请求。所述步骤还包括作为访问令牌授权客户端代理进行操作以代表第一消费者NF获得第一访问令牌。所述步骤还包括使用第一访问令牌使消费者NF能够访问由需要基于访问令牌的授权的生产者NF提供的服务。

[0036] 本文中描述的主题可以用与硬件和/或固件结合的软件来实现。例如,本文中描述的主题可以用处理器执行的软件来实现。在一种示例性实现中,本文中描述的主题可以使用其上存储有计算机可执行指令的非临时性计算机可读介质来实现,所述计算机可执行指令在由计算机的处理器执行时控制计算机执行步骤。适合于实现本文中描述的主题的示例性计算机可读介质包括非临时性计算机可读介质,比如盘存储器设备、芯片存储器设备、可编程逻辑器件和专用集成电路。另外,实现本文中描述的主题的计算机可读介质可以位于单一设备或计算平台上,或者可以分布在多个设备或计算平台上。

附图说明

[0037] 图1是图解说明示例性5G系统网络架构的网络图;

[0038] 图2A是图解说明在使用OAuth 2.0授权框架访问5G通信网络中的服务时交换的示

例性消息的消息流图,其中该消息流用于没有委托发现的间接PLMN间通信(模型C);

[0039] 图2B是图解说明在使用OAuth 2.0授权框架访问5G通信网络中的服务时交换的示例性消息的消息流图,其中该消息流用于具有委托发现的间接PLMN间通信(模型D);

[0040] 图3A是图解说明当消费者NF不支持OAuth 2.0授权而生产者NF需要OAuth 2.0授权作为允许访问生产者NF提供的服务的条件时交换的示例性消息的消息流图,其中该消息流用于没有委托发现的间接PLMN间通信(模型C);

[0041] 图3B是图解说明当消费者NF支持OAuth 2.0授权而NRF不支持OAuth 2.0授权时交换的示例性消息的消息流图,其中该消息流用于没有委托发现的间接PLMN间通信(模型C);

[0042] 图3C是图解说明当消费者NF支持OAuth 2.0授权而NRF不支持OAuth 2.0授权时交换的示例性消息的消息流图,其中该消息流用于具有委托发现的间接PLMN间通信(模型D);

[0043] 图4是图解说明当SCP作为代表不支持OAuth 2.0授权的消费者NF的OAuth 2.0授权客户端代理进行操作时委托的OAuth 2.0授权的消息流图,其中该消息流用于具有委托发现的间接PLMN间通信(模型D);

[0044] 图5A是图解说明当SCP作为代表不支持OAuth 2.0授权的NRF的OAuth 2.0授权服务器代理进行操作时交换的示例性消息的消息流图,其中该消息流用于没有委托发现的间接PLMN间通信(模型C);

[0045] 图5B是图解说明当SCP作为代表不支持OAuth 2.0授权的NRF的OAuth 2.0授权服务器代理进行操作时交换的示例性消息的消息流图,其中该消息流用于具有委托发现的间接PLMN间通信(模型D);

[0046] 图6是图解说明能够代表NF服务消费者和不支持OAuth 2.0授权的NRF进行被委托的OAuth 2.0授权的SCP的框图;

[0047] 图7A是图解说明代表不支持OAuth 2.0授权的消费者NF进行被委托的OAuth 2.0授权的示例性处理的流程图;

[0048] 图7B是更详细地图解说明图7A的作为代表不支持OAuth 2.0授权的消费者NF的访问令牌授权客户端代理进行操作的步骤的流程图;

[0049] 图7C是更详细地图解说明图7A的使用访问令牌使不支持OAuth2.0授权的消费者NF能够访问由需要OAuth 2.0授权的生产者NF提供的服务的步骤的流程图;

[0050] 图8A是图解说明当消费者NF支持OAuth 2.0授权而生产者NF不支持OAuth 2.0授权时,作为代表不支持OAuth 2.0授权的NRF的OAuth2.0授权服务器代理进行操作,并便利对服务的访问的示例性处理的流程图;

[0051] 图8B是更详细地图解说明图8A的作为代表不支持OAuth 2.0授权的NRF的OAuth 2.0授权服务器代理进行操作的步骤的流程图;

[0052] 图8C是更详细地图解说明图8A的当消费者NF支持OAuth 2.0授权而生产者NF不支持OAuth 2.0授权时,与生产者NF和消费者NF进行信令通信,以使消费者NF能够访问生产者NF提供的服务的步骤的流程图。

具体实施方式

[0053] 图1是图解说明示例性5G系统网络架构的框图。图1中的架构包括NRF 100和SCP 101,它们可以位于同一归属公共陆地移动网络(HPLMN)中。如上所述,NRF 100可以维护可

用的生产者NF服务实例及其支持的服务的简档,并允许消费者NF或SCP订阅并被通知新的/更新的生产者NF服务实例的注册。SCP 101还可以支持服务发现和生产者NF实例的选择。SCP 101可以进行消费者NF和生产者NF之间的连接的负载平衡。

[0054] NRF 100是生产者NF实例的NF或服务简档的储存库。为了与生产者NF实例通信,消费者NF或SCP必须从NRF 100获得生产者NF实例的NF或服务简档。NF或服务简档是在3GPP TS29.510中定义的JavaScript对象表示法(JSON)数据结构。NF或服务简档定义包括完全限定域名(FQDN)、网际协议(IP)版本4(IPv4)地址或IP版本6(IPv6)地址中的至少一个。

[0055] 在图1中,任何网络功能都可以是消费者NF、生产者NF或两者兼有,取决于它们是在请求服务、提供服务还是既在请求服务又在提供服务。在图解所示的例子中,NF包括在网络中进行策略相关操作的PCF 102、管理用户数据的UDM功能104以及提供应用服务的应用功能(AF)106。

[0056] 图1中所示的NF还包括会话管理功能(SMF)108,SMF 108管理接入和移动性管理功能(AMF)110与PCF 102之间的会话。AMF 110进行与4G网络中的移动性管理实体(MME)进行的移动性管理操作相似的移动性管理操作。认证服务器功能(AUSF)112为寻求接入网络的用户设备(UE),比如用户设备(UE)114,进行认证服务。

[0057] 网络切片选择功能(NSSF)116为寻求访问与网络切片关联的特定网络能力和特性的设备提供网络切片服务。网络开放功能(NEF)118为寻求获得关于附接到网络的物联网(IoT)设备和其他UE的信息的应用功能提供应用编程接口(API)。NEF 118进行与4G网络中的服务能力开放功能(SCEF)相似的功能。

[0058] 无线电接入网络(RAN)120经由无线链路将用户装备(UE)114连接到网络。可以使用g-Node B(gNB)(图1中未示出)或其他无线接入点来接入无线电接入网络120。用户平面功能(UPF)122可以支持用于用户平面服务的各种代理功能。这种代理功能的一个例子是多路径传输控制协议(MPTCP)代理功能。UPF 122还可以支持性能测量功能,UE 114可以使用该功能来获得网络性能测量结果。图1中还图解说明了数据网络(DN)124,UE通过该数据网络124访问数据网络服务,比如因特网服务。

[0059] SEPP 126过滤来自其他PLMN的传入流量,并对离开归属PLMN的流量进行拓扑隐藏。SEPP 126可以与外部PLMN中的SEPP通信,该SEPP为该外部PLMN管理安全性。因此,不同PLMN中的NF之间的流量可以穿过两个SEPP功能,一个用于归属PLMN,另一个用于外部PLMN。

[0060] 如上所述,5G网络中可能出现的一个问题是缺乏对OAuth 2.0授权的通用支持,这可能导致网络之间的服务不兼容性。图2A是图解说明PLMN之间的OAuth 2.0授权以及使用访问令牌跨PLMN边界访问服务的消息流图。图2A中的消息流用于没有委托发现的间接PLMN间通信,其在3GPP TS23.501的附录E中被定义为模型C。按照模型C的规范,消费者NF通过查询NRF来进行发现。基于发现结果,消费者NF选择生产者NF或NF集。消费者NF然后向SCP发送包含所选择的生产者NF或生产者NF集的地址的SBI服务请求。如果服务请求指定了NF集,则SCP可以与NRF交互以获得选择参数,比如位置、容量等,并使用这些参数来选择生产者NF实例。SCP将SBI服务请求路由到所选择的生产者NF实例。

[0061] 参见图2A中的消息流,在第1行中,消费者NF 200通过经由SCP 101A和101B以及SEPP 126A和126B与NRF 100B进行信令通信来进行NF发现,以选择生产者NF实例或NF集。在第2行中,在选择生产者NF或NF集之后,消费者NF 200向位于访问者网络(触发了访问令牌

请求的UE当前正在其中漫游的访问者PLMN本地的网络)中的NRF 100A发送Nnrf访问令牌请求消息。NRF 100A经由SCP 101A和101B以及SEPP 126A和126B将访问令牌请求消息转发给远程NRF 100B。该转发由图2A中的第2-6行指示。

[0062] 归属NRF 100B判定客户端是否被授权接收访问令牌,并通过发送访问令牌响应消息来返回访问令牌。在第7-11行中,访问令牌响应消息经由SCP 101A和101B、SEPP 126A和126B以及NRF 100A被传送到消费者NF 200。

[0063] 消费者NF 200生成包括访问令牌的SBI服务请求消息,并经由SCP 101A和101B以及SEPP 126A和126B将SBI服务请求消息发送到生产者NF 202,如第12-14行所示。SBI服务请求消息包括访问令牌。SBI请求可以可选地包括客户端凭证断言(CCA)属性,如图2A中的“CCA*”所示。

[0064] 生产者NF 202验证访问令牌并授予消费者NF 200对服务的访问。在第15-17行中,生产者NF 202向消费者NF 200返回SBI服务响应消息。当消费者NF存在于归属网络中而生产者NF存在于访问者或非归属网络中时,发生类似的流。因此,图2A图解说明其中两个不同的网络经由SCP支持OAuth 2.0授权和间接PLMN间通信的情况,结果,访问令牌消息接发和服务请求消息接发是成功的。然而,如果一个或另一个网络不支持OAuth 2.0授权,则服务请求和/或访问令牌消息接发将不会成功。

[0065] 图2B是图解说明具有委托发现和OAuth 2.0授权的间接PLMN间通信的消息流图。具有委托发现的间接通信在3GPP TS23.501的附录E中被定义为模型D。按照模型D,消费者NF不进行NF选择或发现。相反,消费者NF将必要的发现和选择参数添加到发送给SCP的发现请求中。SCP然后与NRF进行发现,获得发现结果,并将SBI服务请求发送到所选择的NF。参见图2B中的消息流,在第1行中,消费者NF 200向SCP 101A发送带有发现和生产者NF选择参数的SBI服务访问请求消息。在第2行中,SCP 101A与NRF 101B进行发现。发现的结果是选择生产者NF 202来处理服务请求消息。然而,在向生产者NF 202发送服务请求消息之前,SCP 101A必须从生产者NF 202的网络中的NRF 100B获得访问令牌。因而,在第3行中,SCP 101A向本地NRF 100A发送访问令牌请求消息。本地NRF 100A经由SCP 101A和101B以及SEPP 126A和126B将访问令牌请求消息转发给远程NRF 100B,如消息流图的第4-6行所示。

[0066] NRF 100B判定客户端是否被授权,并经由SCP 101B和101A以及SEPP 126B和126A返回访问令牌。在图2B中的消息流中,借助第7-10行图解说明了访问令牌的返回。

[0067] 在第11行和第12行中,SCP 101A经由SEPP 126A和126B以及SCP 101B向在由第2行表示的委托发现过程期间选择的生产者NF 202发送SBI服务请求消息。生产者NF 202验证访问令牌,并且在第13-15行中,经由他的SCP 101B和101A以及SEPP 126B和126A向消费者NF 200发送SBI服务响应。传送给消费者NF 200的SBI服务响应可以可选地包括访问令牌,如图2B中的“访问令牌**”所示。

[0068] 当消费者NF在归属网络中而生产者NF在访问者网络中时,发生类似的流。因此,图2B图解说明了其中服务于消费者NF的SCP和生产者NF的网络中的NRF支持OAuth 2.0授权,并且进行具有委托发现的间接PLMN间通信的情况。

[0069] 图3A图解说明没有委托发现的PLMN间间接通信的情况,其中NF服务消费者不支持OAuth 2.0授权,而NF服务生产者需要OAuth 2.0授权。参见图3A,由于本例中的访问者网络不支持OAuth 2.0授权,因此没有发生图2A的第1-11行的获得访问令牌的PLMN间信令。图3A

中的消息流始于第1行,其中消费者NF 200向位于不同PLMN中并且需要访问令牌授权的生产者NF 202发送没有访问令牌的SBI服务请求消息。由于该服务请求不包括访问令牌,因此第2行中的服务请求被归属SEPP 126B拒绝。SEPP 126B拒绝该服务请求,因为3GPP TS 33.501,第13.4.1.2.2节建议提供商SEPP应检查访问令牌中的主体声明的服务PLMN匹配与N32消息中的N32-f上下文ID对应的远程PLMN。由于第2行中的服务请求消息不包括访问令牌,所以没有供SEPP 126B验证的主体声明,因此该消息被拒绝。

[0070] 虽然图3A图解说明了没有委托发现的间接PLMN间通信的情况,其中消费者NF不支持OAuth 2.0授权,而生产者NF支持OAuth 2.0授权,但是图3B图解说明没有委托发现的间接PLMN间通信的情况,其中消费者NF支持OAuth 2.0授权,而生产者NF的网络中的NRF不支持OAuth 2.0授权。参见图3B中的消息流,在第1行中,位于归属网络中的消费者NF 300与位于访问者网络中的NRF 100A进行信令通信以进行服务发现。在该例子中,假设服务发现的结果是选择位于访问者网络中的生产者NF 302来提供所请求的服务。

[0071] 在服务发现之后,在第2行中,消费者NF 300向位于归属网络中的SCP 101B发送访问令牌请求消息。在第3行中,SCP 101B将访问令牌请求发送给NRF 100B。在第4行中,NRF 100B将访问令牌请求转发给SCP 101B,在第5行中,SCP 101B将访问令牌请求路由到远程SCP 101A。在第6行中,SCP 101A将访问令牌请求路由到位于访问者网络中的NRF 100A。在该例子中,访问者NRF 100A不支持OAuth 2.0授权。因而,访问者NRF 100A不能响应访问令牌请求,这导致访问令牌消息接发的失败。结果,消费者NF 300可能无法访问由访问者网络提供的服务。

[0072] 图3C图解说明具有委托发现的间接PLMN间通信的情况,其中消费者NF支持OAuth 2.0授权,而生产者NF不支持OAuth 2.0授权。参见图3C中的消息流,在第1行中,位于归属网络中的消费者NF 300向SCP 101B发送带有发现参数的服务访问请求。在第2行中,SCP 101B与位于访问者网络中的NRF 100A进行信令通信以进行服务发现。在该例子中,假设服务发现的结果是选择位于访问者网络中的生产者NF 302来提供所请求的服务。

[0073] 在服务发现之后,在第3行中,SCP 101B向NRF 100B发送访问令牌请求。在第4行中,NRF 100B将访问令牌请求转发给SCP 101B,在第5行中,SCP 101B将访问令牌请求路由到远程SCP 101A。在第6行中,SCP 101A将访问令牌请求路由到位于访问者网络中的NRF 100A。在该例子中,访问者NRF 100A不支持OAuth 2.0授权。因而,访问者NRF 100A不能响应访问令牌请求,这导致访问令牌消息接发的失败。结果,消费者NF 300可能无法访问由访问者网络提供的服务。

[0074] 为了避免这种困难,本文中描述的SCP起代表不支持基于访问令牌的授权的消费者NF的访问令牌授权客户端代理的作用,以及起代表不支持基于访问令牌授权的NRF的访问令牌授权服务器的作用。对于不支持基于访问令牌的授权的消费者NF,SCP获取访问令牌,并将访问令牌添加到SBI请求中,之后将所述请求转发给生产者NF。SCP可以选择缓存令牌以加快处理速度。SCP可以利用来自消费者NF在SBI服务或SBI服务访问请求中所提供的用户代理报头中的字段来获得用于代表消费者NF创建访问令牌请求的NF类型和NF实例ID。当SCP起OAuth2.0授权服务器作用时,取决于是否进行委托发现,SCP向发出请求的消费者NF或SCP发布访问令牌。

[0075] 图4图解说明具有委托发现的间接PLMN间通信的情况,其中SCP充当代表不支持

OAuth 2.0授权的消费者NF的OAuth 2.0授权客户端代理。参见图4,在消息流图的第1行中,消费者NF 200向SCP 101A发送不带访问令牌的SBI服务访问请求。在第2行中,SCP 101A通过与NRF 100B进行信令通信来代表消费者NF 200进行委托发现,并且委托发现的结果是选择生产者NF 202。

[0076] SCP 101A不是响应于第1行中的服务访问请求来生成SBI服务请求,而是检测到该服务访问请求不包括访问令牌,截取并存储服务访问请求,并且代表消费者NF 200获取访问令牌。获取访问令牌的处理始于消息流图的第3行,其中SCP 101A制定并向SCP 101B发送访问令牌请求,在第4行,SCP 101B将访问令牌请求路由到位于生产者NF 202的PLMN中的NRF 100B。访问令牌请求消息的制定将在下面更详细地描述。NRF 100B验证消费者NF 200,生成包括访问令牌的访问令牌响应,并且在第5行和第6行中,经由SEPP 126B和126A以及SCP 101B将访问令牌响应发送到消费者NF 200的网络。

[0077] SCP 101A接收访问令牌响应,从所述响应中提取访问令牌,基于在第1行中接收到的SBI服务访问请求生成SBI服务请求,并将访问令牌插入所生成的SBI服务请求中。在第7行和第8行中,SCP 101A将带有访问令牌的SBI服务请求转发给生产者NF 202。生产者NF 202使用访问令牌来验证服务请求,并且在第9-11行中,生成SBI服务响应消息并将其发送到消费者NF 200。因此,图4图解说明了SCP 101A起代表不支持OAuth 2.0授权的消费者NF的OAuth 2.0授权客户端代理的作用的情况。

[0078] 在另一个例子中,SCP 101A可以起访问令牌授权服务器的作用。图5A中图解说明了一个这样的例子,图5A图解说明没有委托发现的间接PLMN间通信,其中位于归属网络中并且不支持OAuth 2.0授权的消费者NF 300试图访问由位于访问者网络中的生产者NF 302提供的服务。参见图5A,在第1行中,消费者NF通过与NRF 100A进行信令通信来进行服务发现,并且服务发现的结果是选择生产者NF 302来提供服务。

[0079] 在第2行中,消费者NF 300生成访问令牌请求消息,并将该访问令牌请求转发给SCP 101B。在第3行中,SCP 101B将访问令牌请求转发给NRF 100B。在第4行和第5行中,NRF 100B将访问令牌请求消息转发给NRF 100A。然而,NRF 100A不支持OAuth 2.0授权。因而,代替将访问令牌请求转发给NRF 100A,SCP 101A截取访问令牌请求消息并代表NRF 100A生成访问令牌响应消息。访问令牌响应消息包括由SCP 101A使用SCP 101A本地的信息生成的访问令牌。访问令牌可以在语法上是正确的,因为它包括所有所需的访问令牌声明。在第6-9行中,SCP 101A将访问令牌响应转发给消费者NF 300。

[0080] 在第10行中,消费者NF 300生成SBI服务请求,并经由SCP 101B和101A以及SEPP 126B和126A将其发送到生产者NF 302,其中该服务请求包括访问令牌。在第11行中,SCP 101A截取SBI服务请求并从服务请求中移除访问令牌,因为生产者NF 302不支持OAuth 2.0授权。在第12行中,SCP 101A将服务请求(不带访问令牌)转发给生产者NF 302。在第13-15行中,生产者NF 302生成SBI服务响应消息并将其发送到消费者NF 300。因此,图5A图解说明了SCP 101A起代表不支持OAuth 2.0授权的NRF的OAuth 2.0授权服务器代理的作用的情况。

[0081] 虽然图5A图解说明了SCP充当OAuth 2.0授权服务器用于没有委托发现的间接PLMN间通信的情况,但是图5B图解说明SCP充当OAuth 2.0授权服务器用于具有委托发现的间接PLMN间通信的情况。参见图5B,在消息流图的第1行中,位于归属网络中的消费者NF

300向SCP 101B发送带有发现参数的服务访问请求消息。在第2行中,SCP 101B通过与位于访问者网络中的NRF 100A进行信令通信来进行委托NF发现和选择。委托发现和NF选择的结果是选择位于访问者网络中的生产者NF 302来提供所请求的服务。

[0082] 在进行委托发现和NF选择之后,在第3行中,SCP 101B生成访问令牌请求消息,并将该访问令牌请求信息转发给NRF 100B。在第4行和第5行中,NRF 100B将访问令牌请求消息转发给NRF 100A。然而,NRF 100A不支持OAuth 2.0授权。代替将访问令牌请求转发给NRF 100A,SCP 101A截取访问令牌请求并代表NRF 100A生成访问令牌响应。访问令牌响应包括由SCP 101A使用SCP 101A本地的信息生成的访问令牌。访问令牌可以在语法上是正确的,因为它包括所有所需的访问令牌声明。在第6-8行中,SCP 101A将访问令牌响应转发给SCP 101B。

[0083] 在第9行中,SCP 101B生成SBI服务请求,并经由SEPP 126B和126A以及SCP 101A将其发送到生产者NF 302,其中该服务请求包括访问令牌。SCP 101A截取SBI服务请求并从服务请求中移除访问令牌,因为生产者NF 302不支持OAuth 2.0授权。在第10行中,SCP 101A将服务请求(不带访问令牌)转发给生产者NF 302。在第11-13行中,生产者NF 302生成SBI服务响应消息并将其发送到消费者NF 300。因此,图5B图解说明了SCP 101A进行委托发现和NF选择,并起代表不支持OAuth 2.0授权的NRF的OAuth 2.0授权服务器代理的作用的情况。

[0084] 图6是图解说明支持本文中描述的OAuth 2.0授权代理的SCP的示例性架构的框图。参见图6,SCP 101A包括至少一个处理器600和存储器602。SCP 101A还包括访问令牌授权客户端代理604,用于进行上面关于图4针对代表不支持OAuth 2.0授权的消费者NF获得OAuth 2.0访问令牌、并生成包括OAuth 2.0访问令牌以使消费者NF能够访问由支持OAuth 2.0授权的生产者NF提供的服务的SBI服务请求消息的委托发现情况描述的操作。对于非委托发现情况,访问令牌授权客户端代理604可以从不支持OAuth 2.0授权的消费者NF获得OAuth 2.0访问令牌并将其插入SBI服务请求消息中。

[0085] SCP 101A还包括访问令牌授权服务器代理606,访问令牌授权服务器代理606代表不支持OAuth 2.0授权的NRF进行OAuth 2.0授权服务器的功能,如上关于图5A和图5B所述。访问令牌授权服务器代理606还可以从预定去往不支持基于访问令牌的授权的生产者NF的服务请求消息中移除访问令牌。访问令牌授权客户端代理604和访问令牌授权服务器代理606可以使用存储在存储器602中的计算机可执行指令来实现,所述计算机可执行指令使处理器600进行上面描述的访问令牌授权客户端和服务器代理操作。

[0086] 图7A是图解说明在SCP进行委托授权的示例性总体处理的流程图,其中SCP起访问令牌授权客户端代理的作用。参见图7A,在步骤700中,该处理包括从不支持基于访问令牌的授权的消费者NF截取用于访问由需要基于访问令牌的授权的生产者NF提供的服务的SBI请求。例如,对于没有委托发现的间接PLMN间通信的情况,SCP 101A可以从消费者NF接收用于访问由生产者NF 202提供的服务的SBI服务请求。对于具有委托发现的间接PLMN间通信的情况,SCP 101A可以从消费者NF接收服务访问请求。

[0087] 在步骤702中,该处理包括作为访问令牌授权客户端代理进行操作以代表消费者NF获得访问令牌。例如,SCP 101A可以起OAuth 2.0授权客户端代理的作用,以代表不支持OAuth 2.0授权的消费者NF获得访问令牌。图7B图解说明图7A中的步骤702的附加细节。参

见图7B,在步骤702A,该处理包括代表消费者NF生成访问令牌请求消息。下面所示的表1说明了必须被包含在访问令牌请求消息中的属性。

[0088]

属性名称	数据类型	提取自
授予_类型	字符串	客户端_凭证

[0089]

nf 实例 Id	Nf 实例 Id	存在于 5GC SBI 请求中的用户代理报头
nf 类型	NF 类型	存在于 5GC SBI 请求中的用户代理报头
目标 Nf 类型	NF 类型	来自 R-URI 的 API 名称
范围	字符串	来自 R-URI 的服务名称
请求者 Plmn	PlmnId	来自 SCP 配置
目标 Plmn	PlmnId	来自目标 FQDN

[0090] 表1:访问令牌请求属性

[0091] 必须被包括在访问令牌请求中的属性的最小集合是授予类型、NF实例ID、NF类型、目标NF类型、范围、请求者PLMN和目标PLMN。授予类型属性可以从填充自SBI服务请求或服务访问请求消息的消费者NF凭证获得。NF实例ID可以从SBI服务请求消息或服务访问请求消息的用户代理报头填充。按照3GPP TS29.500,第5.2.2节,用户代理报头是SBI服务请求消息中的强制性报头。下面所示的表2说明了用户代理参数的结构。

[0092]

用户代理	IETF RFC 7231[11]	该报头主要用于识别 HTTP/2 客户端的 NF 类型。 内容的模式应该以 NF 类型的值开始(例如，udm，见注 1)，后面跟随“.”，之后是任何其他具体信息，如果需要的话。

[0093] 表2:用户代理参数

[0094] 如表2中所示,用户代理参数可以包含识别NF实例的信息,比如NF实例ID。SCP 101A可以从SBI请求消息(即,用于委托发现的服务访问请求或用于非委托发现的服务请求消息)的用户代理报头提取NF实例ID,并使用该信息来填充访问令牌请求消息的NF实例ID属性。类似地,NF类型也可以从SBI请求消息的用户代理报头中获得。

[0095] 返回表1,访问令牌请求的请求者PLMN可以基于SCP 101A的配置的请求者PLMN参数来填充。目标PLMN属性可以根据从SBI请求消息的请求者统一资源标识符(R-URI)提取的API名称来填充。访问令牌请求的范围属性可以根据从SBI请求消息的R-URI提取的服务名称来填充。

[0096] 返回图7B,一旦制定了访问令牌请求,在步骤702B中,SCP 101A就将访问令牌请求

发送到NRF。例如,SCP 101A可以将访问令牌请求消息发送到位于生产者NF所在的PLMN中的NRF 100B。

[0097] 在步骤702C中,该处理包括从NRF接收包括访问令牌的访问令牌响应。例如,SCP 101A可以从NRF 100B接收包括访问令牌的访问令牌响应。

[0098] 返回图7A,在步骤704中,该处理包括使用访问令牌使消费者NF能够访问由生产者NF提供的服务。图7C图解说明图7A中的步骤704的附加细节。参见图7C,取决于进行的是委托发现还是非委托发现,处理略有不同。如果进行委托发现,则控制进行到步骤704A1,其中该处理包括响应于先前接收到的服务访问请求而生成SBI服务请求消息,并且将在步骤702中代表消费者NF获得的访问令牌插入SBI服务请求消息中。例如,SCP 101A可以生成指向在委托发现过程中识别的生产者NF的SBI服务请求,并将它从NRF 100B获得的访问令牌插入SBI服务请求消息中。在步骤704B1中,该处理包括将包括访问令牌的SBI服务请求转发给生产者NF。例如,SCP 101A可以将包括访问令牌的SBI服务请求转发给在委托发现过程中识别的生产者NF。生产者NF随后将使用访问令牌对服务请求进行授权,并对服务请求作出响应。SCP 101A将该响应转发给发送服务访问请求的消费者NF 200。

[0099] 如果未实现委托发现,则控制进行到步骤704A2,在步骤704A2中,SCP 101A将访问令牌插入先前接收到的SBI服务请求中。用于非委托发现情况的消息流与图4中图解所示的类似,除了在第1行中,接收到的消息是SBI服务请求,而不是SBI服务访问请求,并且已经进行了发现之外。不需要图4的第2行中的委托发现消息接发。用于非委托发现情况的剩余步骤与图4中图解所示的剩余步骤相同。因而,在步骤704B2中,SCP 101A将包括访问令牌的SBI服务请求转发给生产者NF。当SCP 101A接收到来自生产者NF的响应时,SCP 101A将该响应转发给消费者NF。因此,图7A-图7C图解说明由SCP进行的委托授权,其中SCP起访问令牌授权客户端代理的作用,在本文中描述的例子中,该访问令牌授权客户端代理是OAuth 2.0授权客户端代理。

[0100] 图8A图解说明由起代表不支持基于访问令牌的授权的NRF的访问令牌授权服务器代理作用的SCP进行的示例性委托授权处理。参见图8A,在步骤800中,该处理包括对于非委托发现的情况从消费者NF接收访问令牌请求,或者在委托发现的情况下从代表消费者NF的远程SCP接收访问令牌请求。例如,SCP 101A可以在非委托发现的情况下(参见图5A)从消费者NF 300接收访问令牌请求,或者在委托发现的情况下(参见图5B)从SCP 101B接收访问令牌请求。

[0101] 在步骤802中,该处理包括响应于访问令牌请求,作为代表不支持基于访问令牌的授权的NRF的访问令牌授权服务器代理进行操作。在图8B中更详细地图解说明了步骤802。参见图8B,在步骤802A,该处理包括响应于访问令牌请求生成访问令牌。例如,SCP 101A可以生成包括在IETF RFC 6749中规定的所需声明的访问令牌。按照在IETF RFC 6749中规定的格式和内容,访问令牌可以在语法上是正确的。然而,访问令牌不必是真实的访问令牌,并且可以是具有语法上正确的字段的虚拟访问令牌,因为如下所述,SCP 101A将在将服务请求消息转发给不支持基于访问令牌的授权的生产者NF之前从服务请求消息中移除访问令牌。

[0102] 在步骤802B中,该处理包括向消费者NF或SCP发送访问令牌响应。例如,SCP 101A可以将它在步骤802A生成的访问令牌响应在非委托发现的情况下发送到发出请求的消费

者NF,或者在委托发现的情况下发送到远程SCP。

[0103] 返回图8A,在步骤804中,该处理包括与生产者NF和消费者NF或SCP进行信令通信,以使消费者NF能够访问服务。图8C中更详细地图解说明了步骤804。参见图8C,与生产者NF和消费者NF或SCP进行信令通信的处理包括在步骤804A中,从消费者NF或SCP接收包括访问令牌的SBI服务请求。例如,SCP 101A可以从NF服务消费者300接收包括SCP 101A生成的NF访问令牌的SBI服务请求(对于非委托发现的情况),或者对于委托发现的情况从SCP 101B接收SBI服务请求。

[0104] 在步骤804B中,该处理包括从SBI服务请求中移除访问令牌。在步骤804C中,该处理包括将SBI服务请求转发给生产者NF。例如,SCP 101A可以从SBI服务请求中移除它生成的访问令牌,并将SBI服务请求转发给生产者NF。因此,图8A-图8C图解说明了SCP在起代表不支持基于访问令牌的授权的NRF的访问令牌授权服务器代理和信令中介的作用时可以进行的示例性步骤。

[0105] 本文中描述的主题的示例性优点包括PLMN之间的改进的互操作性,其中一个PLMN支持基于访问令牌的授权,而另一个PLMN不支持基于访问令牌的授权。在SCP提供该方案是有益的,因为SCP代表多个消费者NF处理消息接发。它也是一种可扩展的方案,因为单个SCP可以为消费者NF和生产者NF或代表消费者NF和生产者NF进行本文中描述的功能。

[0106] 以下各个参考文献的公开内容通过引用整体并入本文中。

[0107] 参考文献

[0108] 1、Hardt,D.“The OAuth 2.0Authorization Framework,”IETF RFC 6749 (October 2012).

[0109] 2、3GPP TS 33.501V17.0.0(2020-12),3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;Security architecture and procedures for 5G system(Release 17).

[0110] 3、3GPP TS29.500V17.1.0(2020-12);3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals;5GSystem;Technical Realization of the Service Based Architecture;Stage 3(Release 17).

[0111] 4、3GPP TS29.510V17.0.0(2020-12);3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals;5GSystem;Network Function Repository Services;Stage 3(Release 17).

[0112] 5、3GPP TS23.501V16.7.0(2020-12);3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;System architecture for the 5G System(5GS);Stage 2(Release 16).

[0113] 要理解的是,在不脱离本文中描述的主题的范围的情况下,可以改变本文中描述的主题的各种细节。此外,上述描述仅用于举例说明,而不是用于限制,因为本文中描述的主题由如下文中所述的权利要求限定。

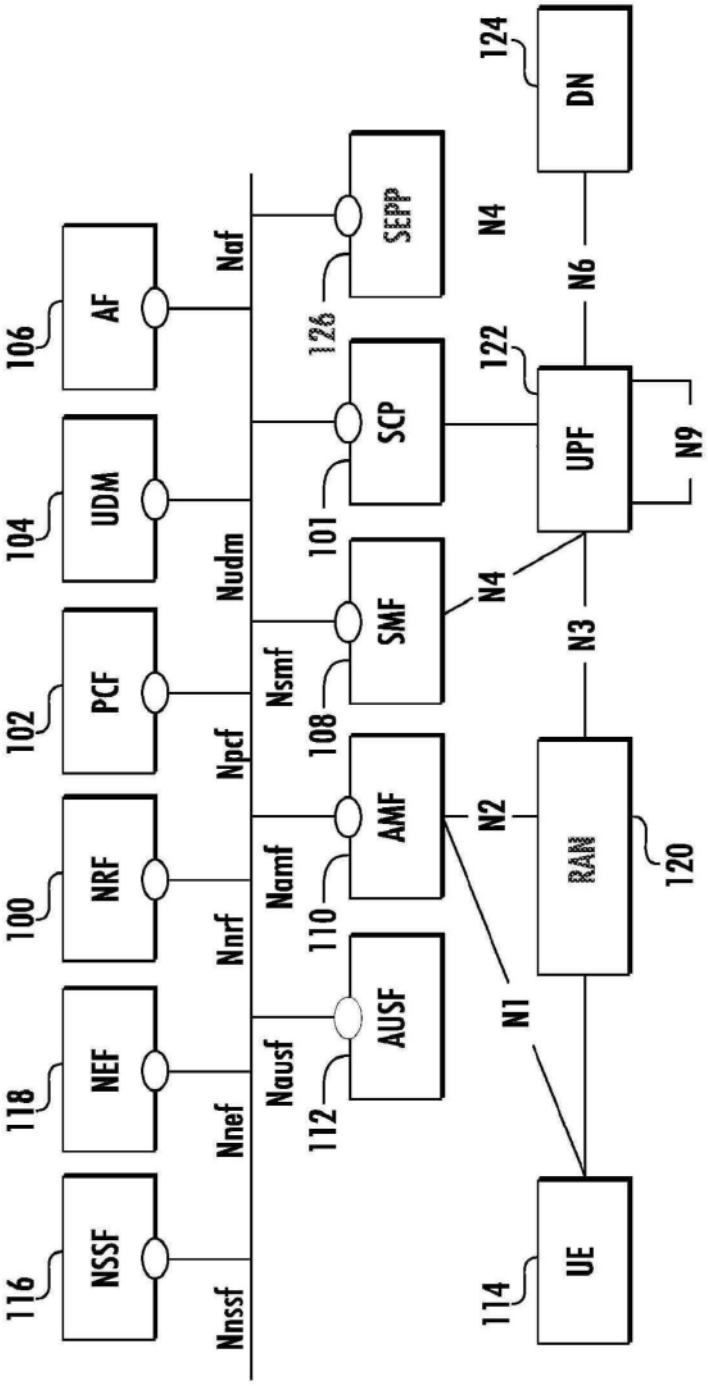

124
DN
N4
N6
SEPP
126
AF
106
Naf
122
UPF
N9
SCP
101
UDM
104
Nudm
N4
N3
SMF
108
Nsmf
PCF
102
Npcf
AMF
N2
RAN
120
110
Namf
NRF
100
Nnrf
N1
AUSF
112
Nausf
NEF
118
Nnef
NSSF
116
Nnssf
UE
114

图1

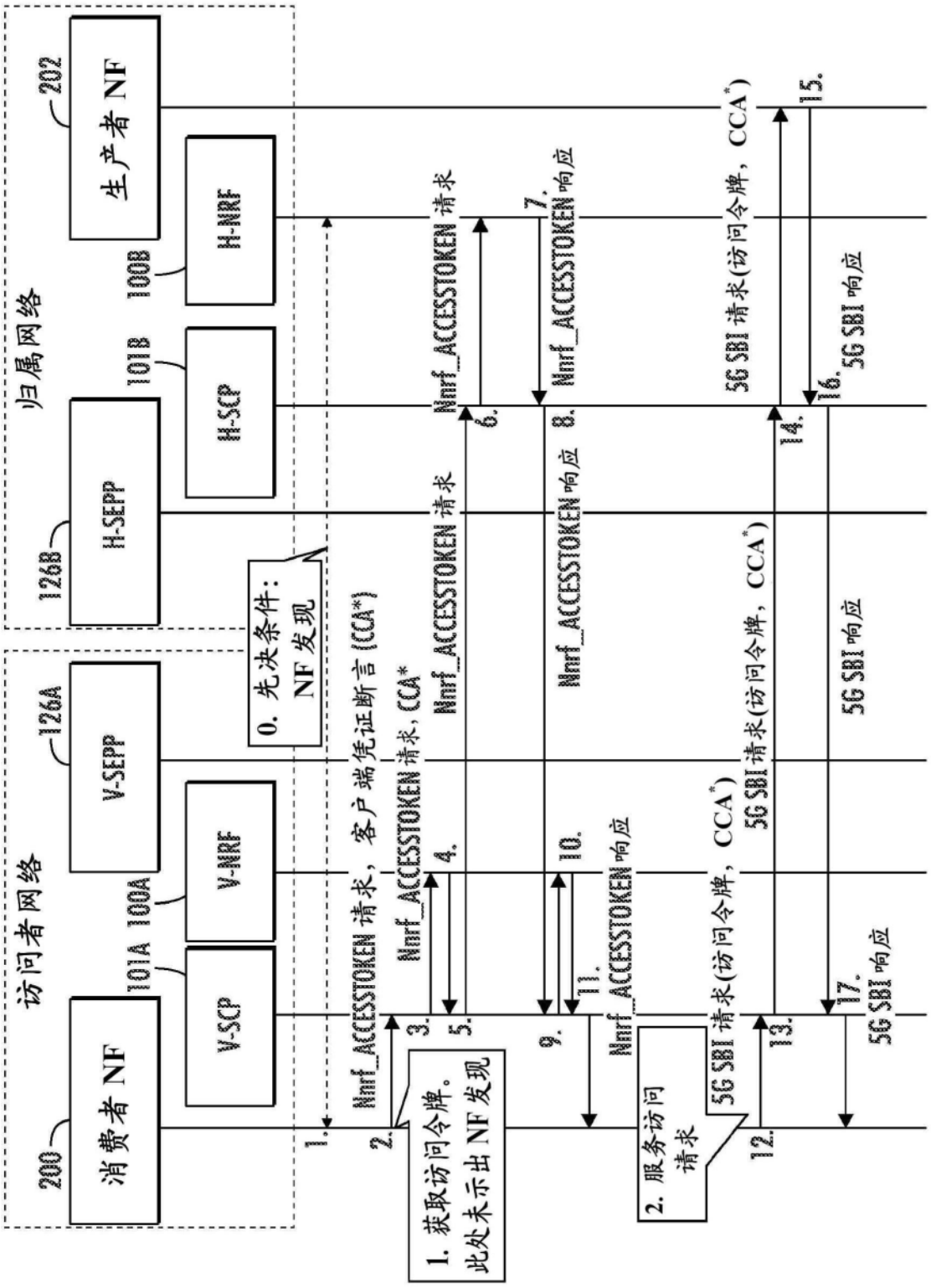

访问者网络
归属网络
消费者 NF
200
V-SCP
101A
V-NRF
100A
V-SEPP
126A
H-SEPP
126B
H-SCP
101B
H-NRF
100B
生产者 NF
202
0. 先决条件：NF 发现
1.
Nnrf_ACCESSTOKEN 请求，客户端凭证断言 (CCA*)
2.
1. 获取访问令牌。此处未示出 NF 发现
3.
Nnrf_ACCESSTOKEN 请求，CCA*
4.
Nnrf_ACCESSTOKEN 请求
5.
6.
Nnrf_ACCESSTOKEN 请求
7.
Nnrf_ACCESSTOKEN 响应
8.
Nnrf_ACCESSTOKEN 响应
9.
10.
Nnrf_ACCESSTOKEN 响应
11.
2. 服务访问请求
5G SBI 请求(访问令牌，CCA*)
12.
5G SBI 请求(访问令牌，CCA*)
13.
5G SBI 请求(访问令牌，CCA*)
14.
5G SBI 响应
15.
16.
5G SBI 响应
17.
5G SBI 响应
*指示客户端凭证断言(CCA)是可选的

图2A

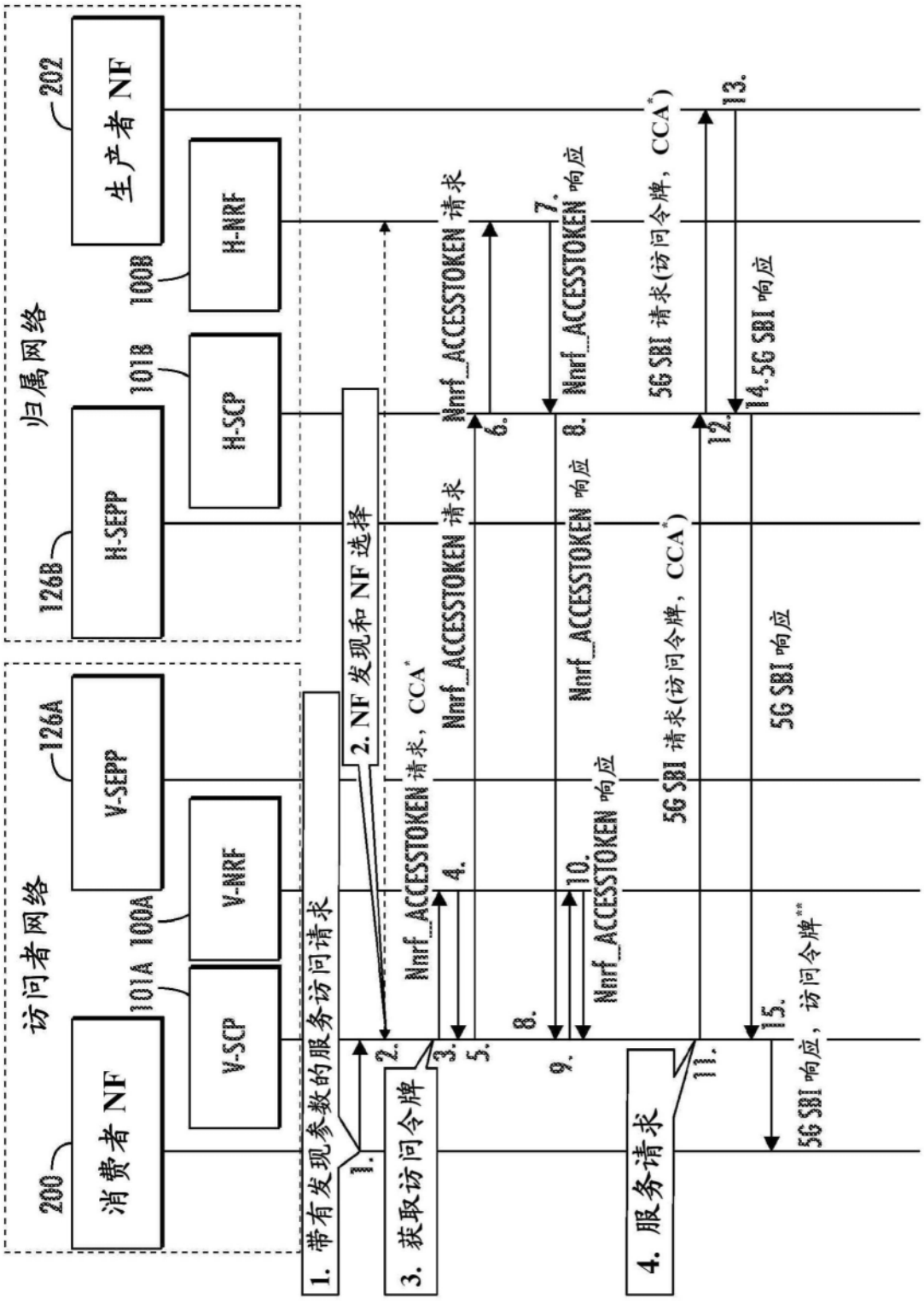

访问者网络
归属网络
消费者 NF
200
V-SCP
101A
V-NRF
100A
V-SEPP
126A
H-SCP
101B
H-NRF
100B
H-SEPP
126B
生产者 NF
202
1. 带有发现参数的服务访问请求
2. NF 发现和 NF 选择
3. 获取访问令牌
4. 服务请求
Nnrf_ACCESSTOKEN 请求，CCA*
Nnrf_ACCESSTOKEN 响应
5G SBI 请求(访问令牌，CCA*)
5G SBI 响应
5G SBI 响应，访问令牌**
*指示客户端凭证断言(CCA)是可选的
**指示访问令牌是可选的

图2B

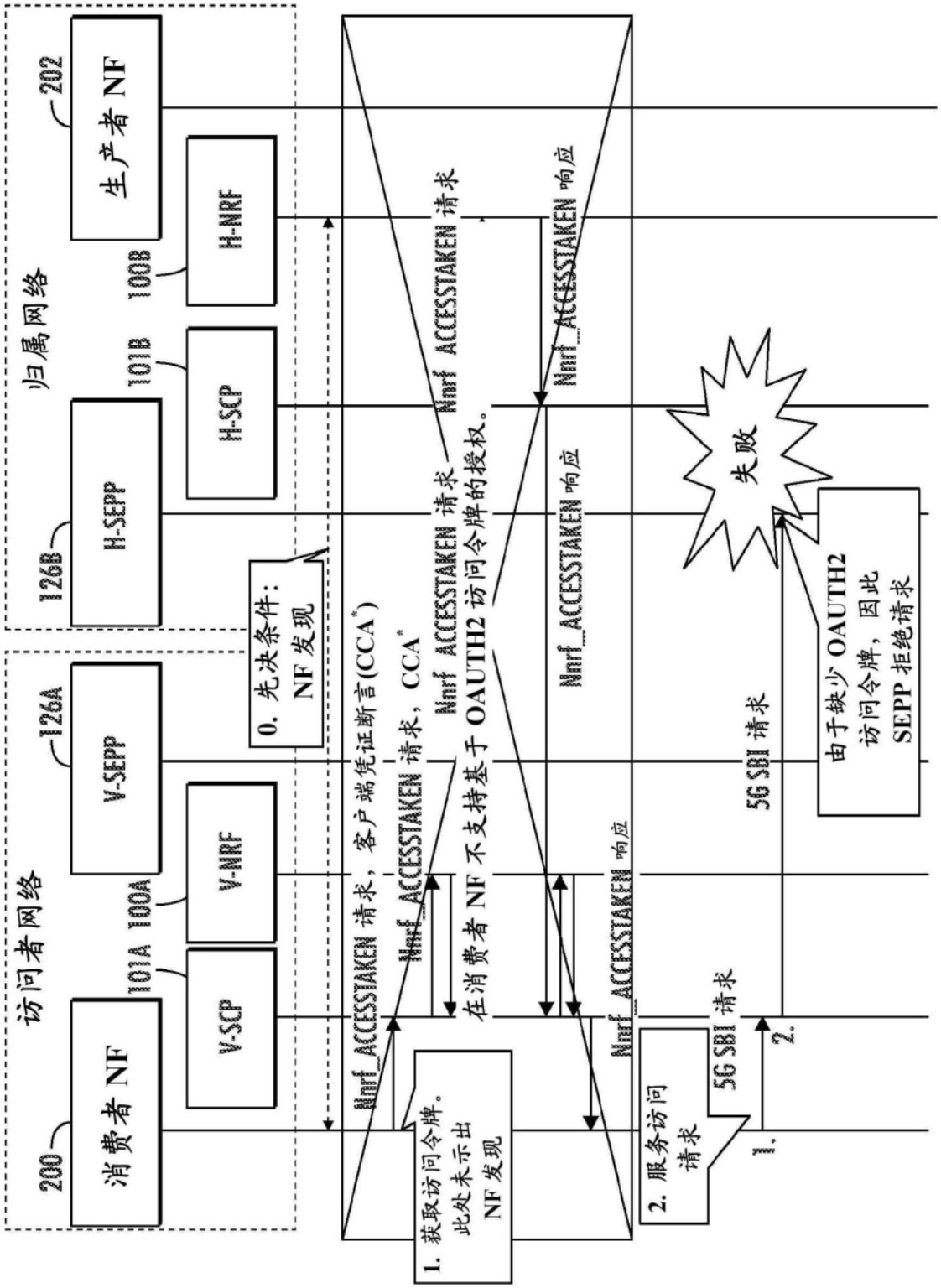

访问者网络
归属网络
200
消费者 NF
101A
V-SCP
100A
V-NRF
126A
V-SEPP
126B
H-SEPP
101B
H-SCP
100B
H-NRF
202
生产者 NF
0. 先决条件：
NF 发现
1. 获取访问令牌。
此处未示出
NF 发现
Nnrf_ACCESSTAKEN 请求，客户端凭证断言(CCA*)
Nnrf_ACCESSTAKEN 请求，CCA*
Nnrf_ACCESSTAKEN 请求
在消费者 NF 不支持基于 OAUTH2 访问令牌的授权。
Nnrf_ACCESSTAKEN 响应
Nnrf_ACCESSTAKEN 响应
Nnrf_ACCESSTAKEN 响应
2. 服务访问
请求
5G SBI 请求
1.
2.
5G SBI 请求
失败
由于缺少 OAUTH2
访问令牌，因此
SEPP 拒绝请求
*指示客户端凭证断言(CCA)是可选的

图3A

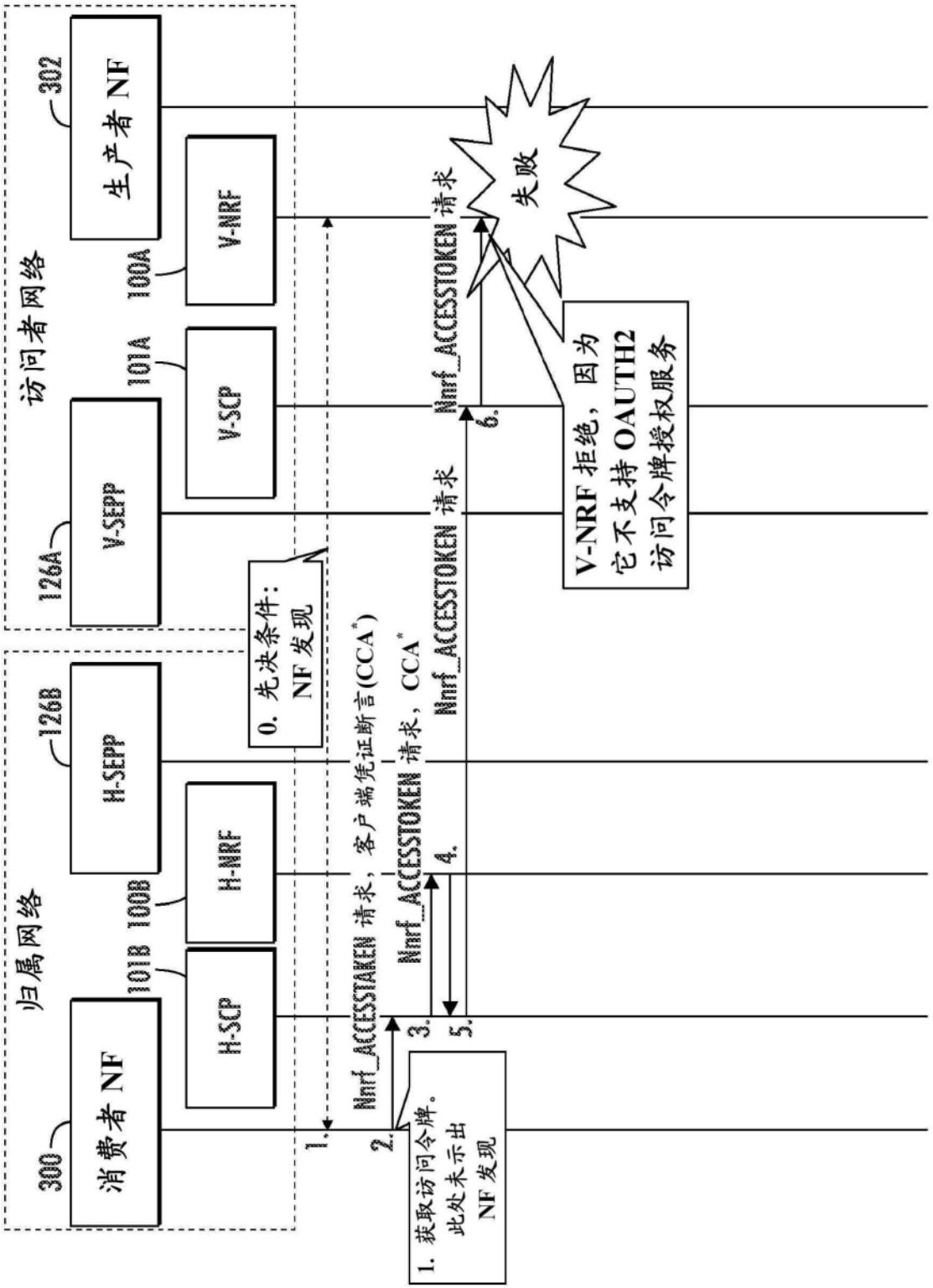

归属网络
访问者网络
消费者 NF
300
H-SCP
101B
H-NRF
100B
H-SEPP
126B
V-SCP
101A
V-NRF
100A
生产者 NF
302
V-SEPP
126A
0. 先决条件：NF 发现
1. Nnrf_ACCESSTAKEN 请求，客户端凭证断言(CCA*)
2. 1. 获取访问令牌。此处未示出 NF 发现
3. Nnrf_ACCESSTOKEN 请求，CCA*
4.
5.
6. Nnrf_ACCESSTOKEN 请求
失败
V-NRF 拒绝，因为它不支持 OAUTH2 访问令牌授权服务
*指示客户端凭证断言(CCA)是可选的

图3B

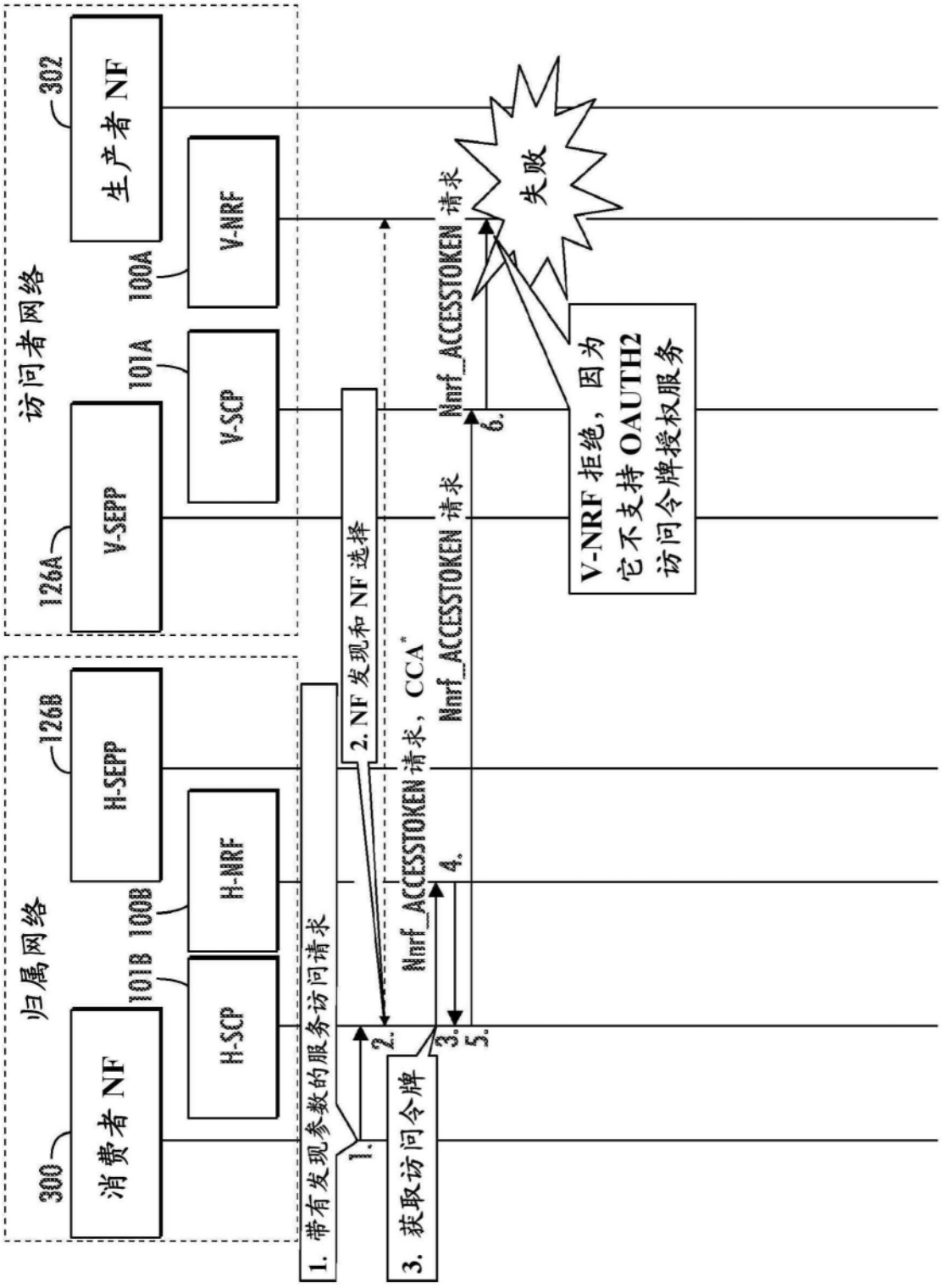

归属网络
消费者 NF
300
101B
H-SCP
100B
H-NRF
H-SEPP
126B
访问者网络
V-SEPP
126A
101A
V-SCP
100A
V-NRF
生产者 NF
302
1. 带有发现参数的服务访问请求
2. NF 发现和 NF 选择
3. 获取访问令牌
Nnrf_ACCESSTOKEN 请求，CCA*
Nnrf_ACCESSTOKEN 请求
Nnrf_ACCESSTOKEN 请求
失败
V-NRF 拒绝，因为
它不支持 OAUTH2
访问令牌授权服务
1.
2.
3.
4.
5.
6.
*指示客户端凭证断言(CCA)是可选的

图3C

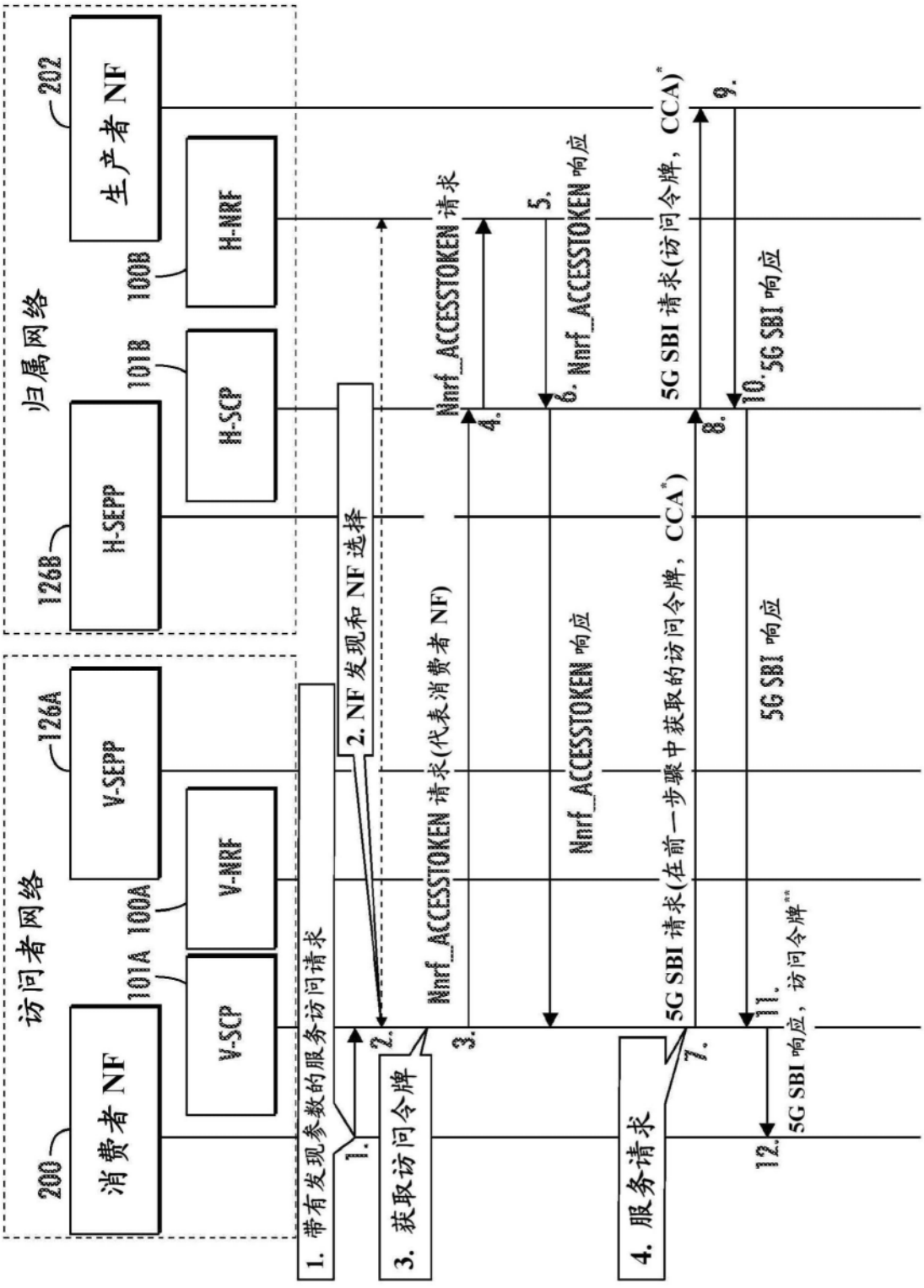

访问者网络
归属网络
消费者 NF
200
V-SCP
101A
V-NRF
100A
V-SEPP
126A
H-SCP
101B
H-NRF
100B
H-SEPP
126B
生产者 NF
202
1. 带有发现参数的服务访问请求
2. NF 发现和 NF 选择
3. 获取访问令牌
4. 服务请求
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
Nnrf_ACCESSTOKEN 请求(代表消费者 NF)
Nnrf_ACCESSTOKEN 响应
5G SBI 请求(在前一步骤中获取的访问令牌，CCA*)
5G SBI 响应
Nnrf_ACCESSTOKEN 请求
Nnrf_ACCESSTOKEN 响应
5G SBI 请求(访问令牌，CCA)*
5G SBI 响应
5G SBI 响应，访问令牌**
*指示客户端凭证断言(CCA)是可选的
**指示访问令牌是可选的

图4

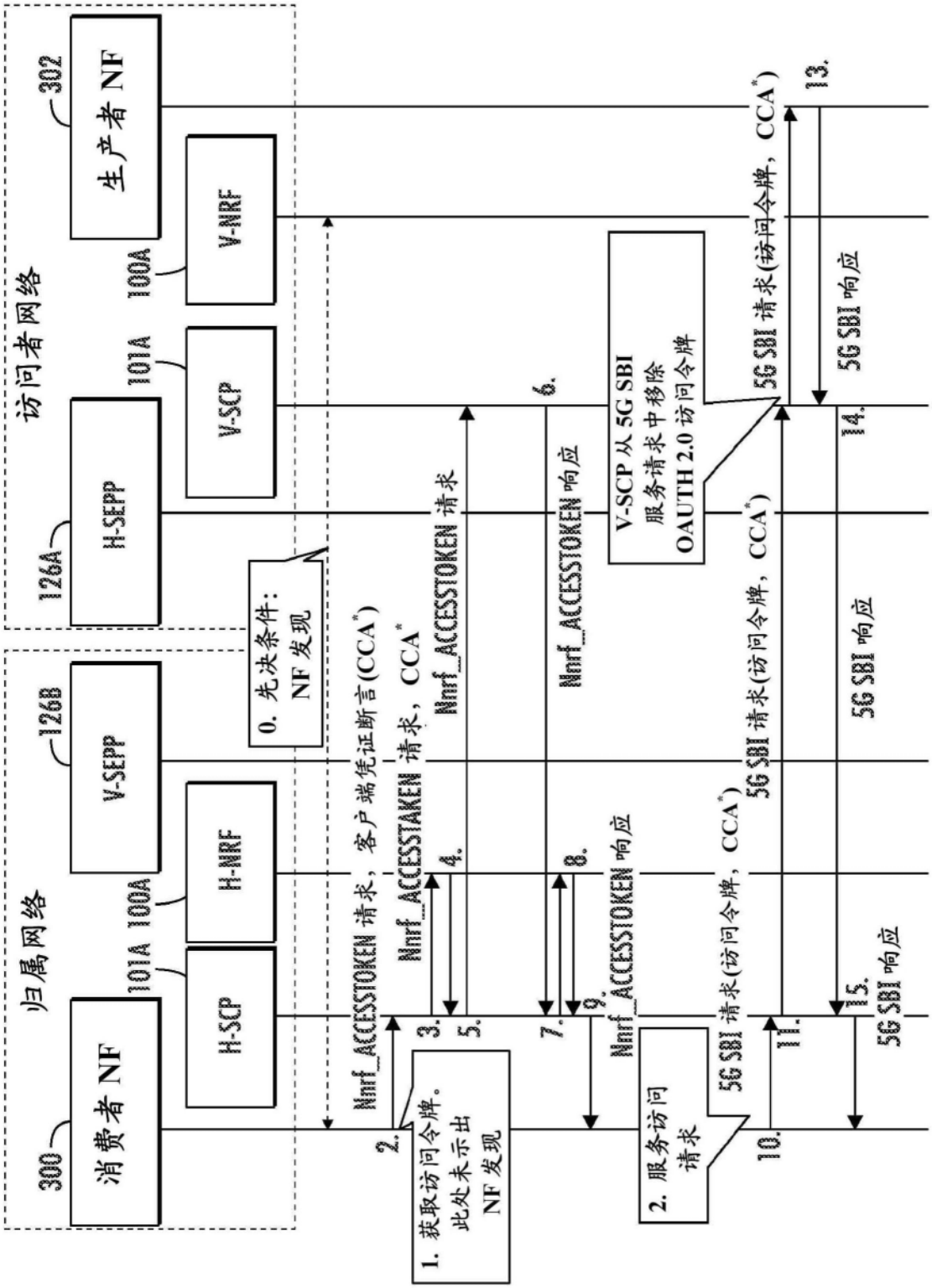

归属网络
访问者网络
消费者 NF
300
101A
H-SCP
100A
H-NRF
V-SEPP
126B
H-SEPP
126A
101A
V-SCP
100A
V-NRF
生产者 NF
302
0. 先决条件：NF 发现
1. 获取访问令牌。此处未示出 NF 发现
2. 服务访问请求
Nnrf_ACCESSTOKEN 请求，客户端凭证断言(CCA*)
Nnrf_ACCESSTAKEN 请求，CCA*
Nnrf_ACCESSTOKEN 请求
Nnrf_ACCESSTOKEN 响应
V-SCP 从 5G SBI 服务请求中移除 OAUTH 2.0 访问令牌
5G SBI 请求(访问令牌，CCA*)
5G SBI 响应
*指示客户端凭证断言(CCA)是可选的

图5A

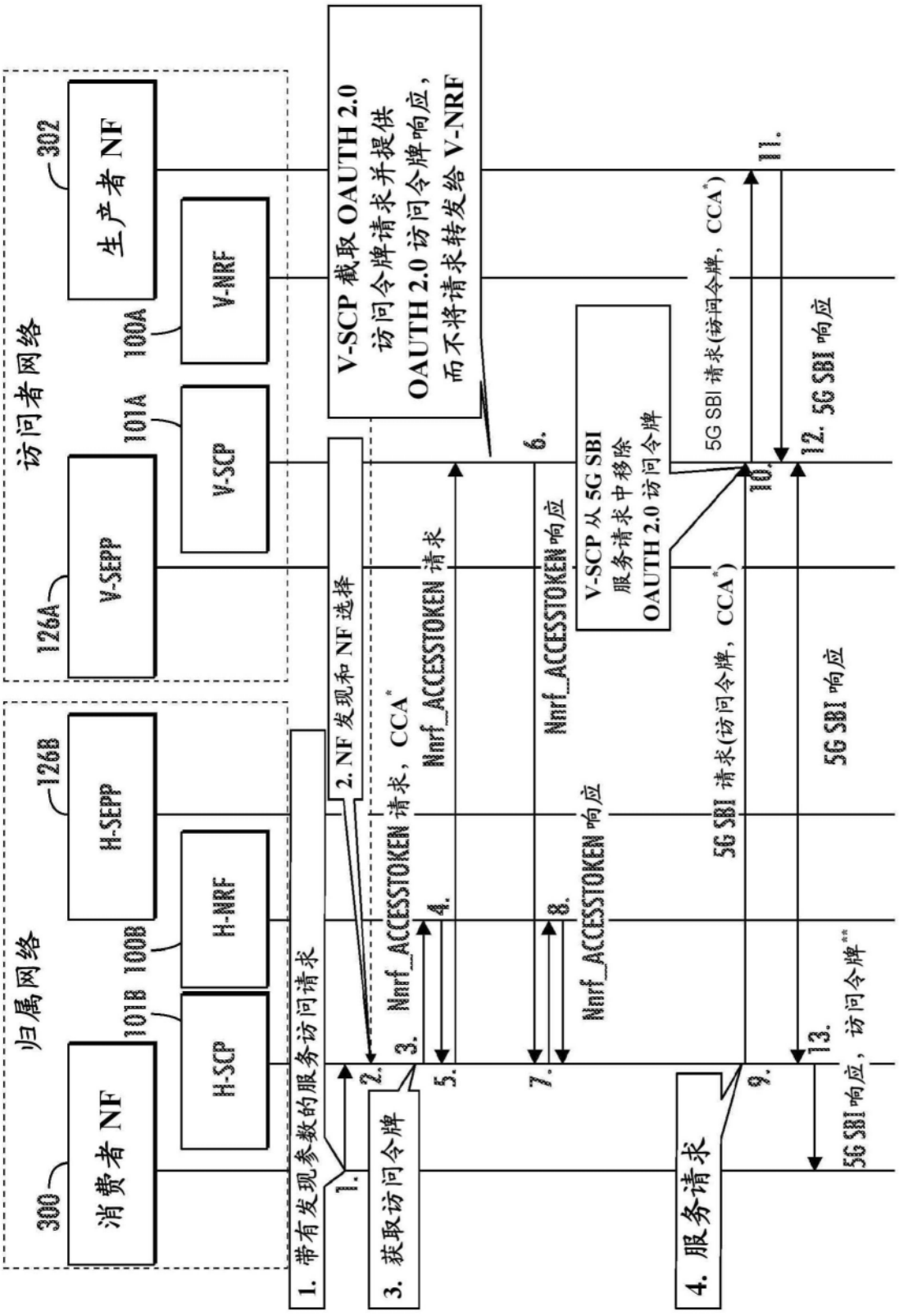

归属网络
消费者 NF
300
H-SCP
101B
H-NRF
100B
H-SEPP
126B
访问者网络
V-SEPP
126A
V-SCP
101A
V-NRF
100A
生产者 NF
302
1. 带有发现参数的服务访问请求
2. NF 发现和 NF 选择
3. 获取访问令牌
4. 服务请求
V-SCP 截取 OAUTH 2.0
访问令牌请求并提供
OAUTH 2.0 访问令牌响应，
而不将请求转发给 V-NRF
V-SCP 从 5G SBI
服务请求中移除
OAUTH 2.0 访问令牌
1. 带有发现参数的服务访问请求
2. NF 发现和 NF 选择
3. Nnrf_ACCESSTOKEN 请求，CCA*
4. Nnrf_ACCESSTOKEN 请求
5.
6.
7.
8. Nnrf_ACCESSTOKEN 响应
Nnrf_ACCESSTOKEN 响应
9. 5G SBI 请求(访问令牌，CCA*)
10.* 5G SBI 请求(访问令牌，CCA*)
11.
12. 5G SBI 响应
5G SBI 响应
13.
5G SBI 响应，访问令牌**
*指示客户端凭证断言(CCA)是可选的
**指示访问令牌是可选的

图5B

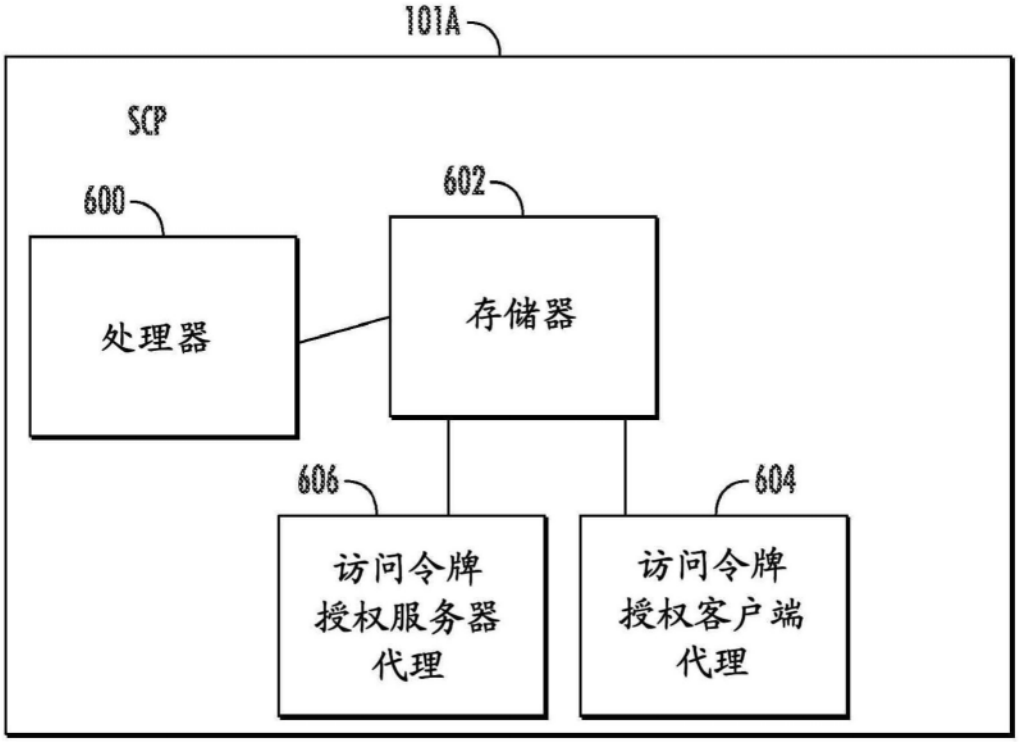

101A
SCP
600
处理器
602
存储器
606
访问令牌
授权服务器
代理
604
访问令牌
授权客户端
代理

图6

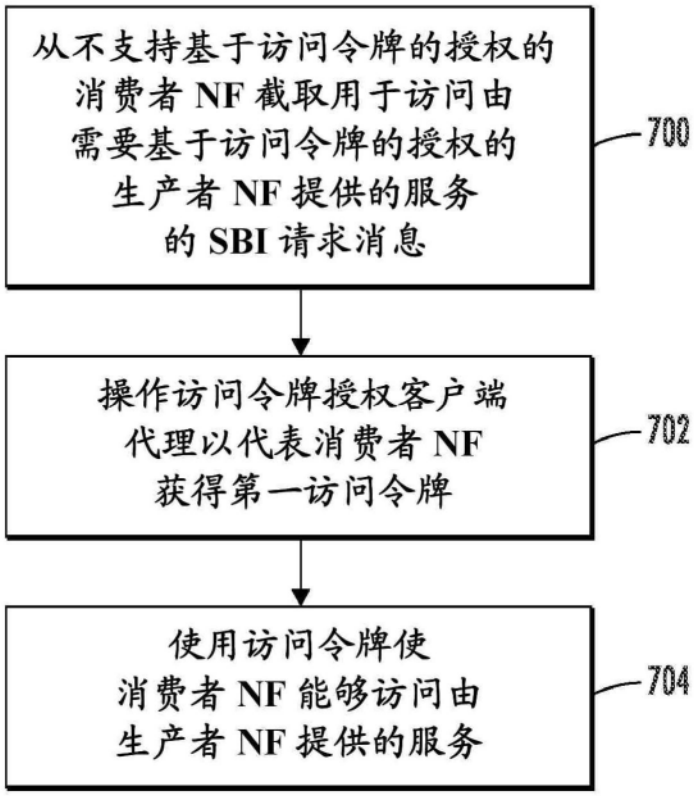

从不支持基于访问令牌的授权的
消费者 NF 截取用于访问由
需要基于访问令牌的授权的
生产者 NF 提供的服务
的 SBI 请求消息
700
操作访问令牌授权客户端
代理以代表消费者 NF
获得第一访问令牌
702
使用访问令牌使
消费者 NF 能够访问由
生产者 NF 提供的服务
704

图7A

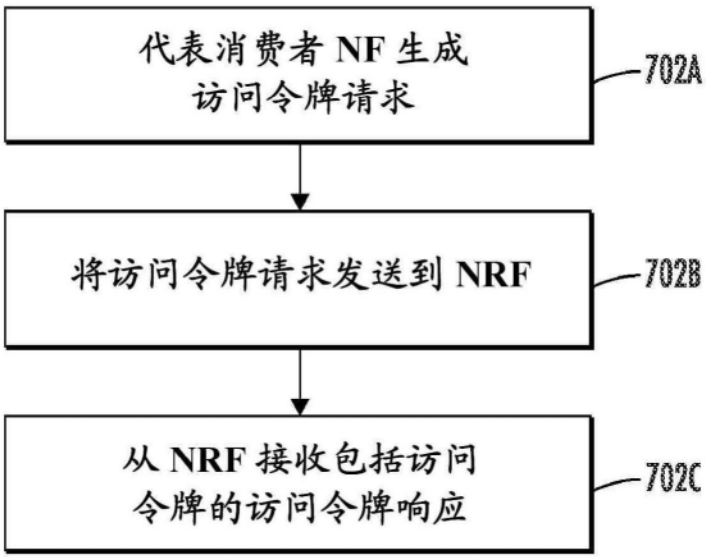

代表消费者 NF 生成
访问令牌请求
702A
将访问令牌请求发送到 NRF
702B
从 NRF 接收包括访问
令牌的访问令牌响应
702C

图7B

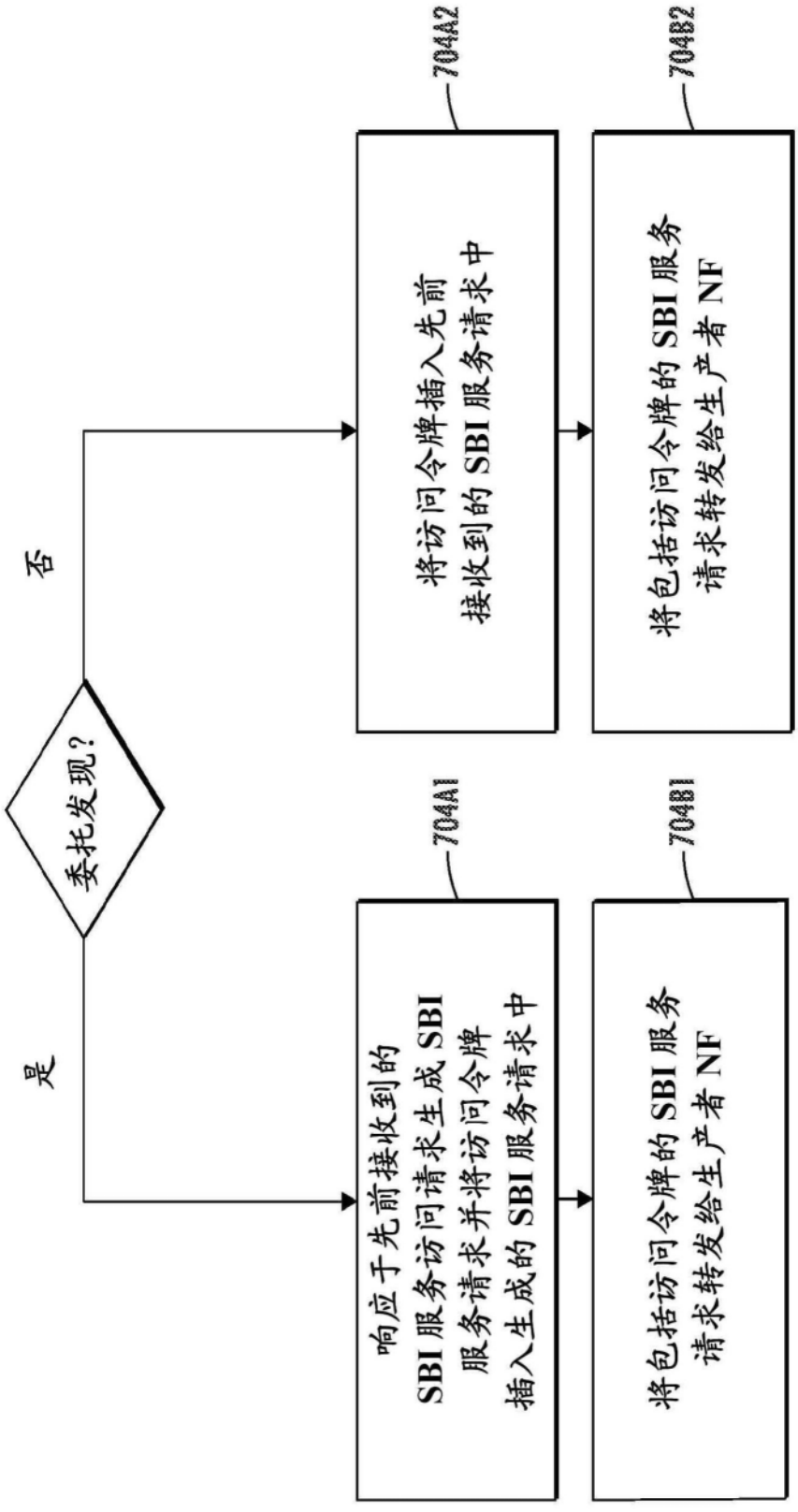

委托发现?
否
是
将访问令牌插入先前接收到的SBI服务请求中
704A2
将包括访问令牌的SBI服务请求转发给生产者NF
704B2
响应于先前接收到的SBI服务访问请求生成SBI服务请求并将访问令牌插入生成的SBI服务请求中
704A1
将包括访问令牌的SBI服务请求转发给生产者NF
704B1

图7C

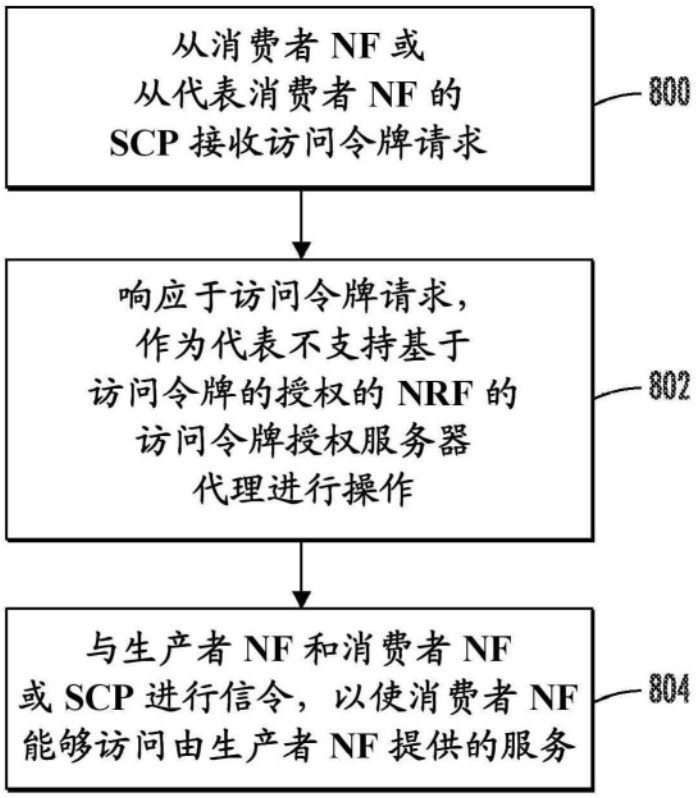

从消费者 NF 或
从代表消费者 NF 的
SCP 接收访问令牌请求
800
响应于访问令牌请求，
作为代表不支持基于
访问令牌的授权的 NRF 的
访问令牌授权服务器
代理进行操作
802
与生产者 NF 和消费者 NF
或 SCP 进行信令，以使消费者 NF
能够访问由生产者 NF 提供的服务
804

图8A

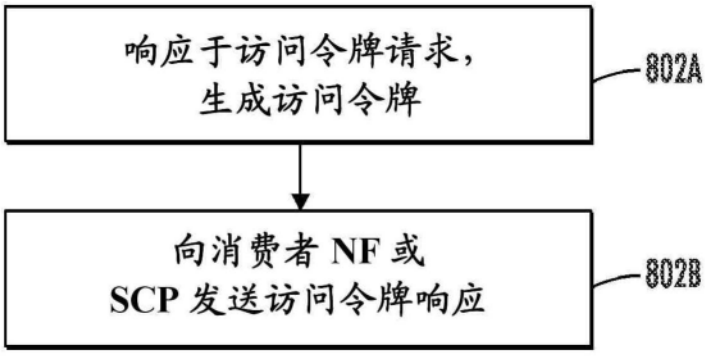

响应于访问令牌请求，
生成访问令牌
802A
向消费者 NF 或
SCP 发送访问令牌响应
802B

图8B

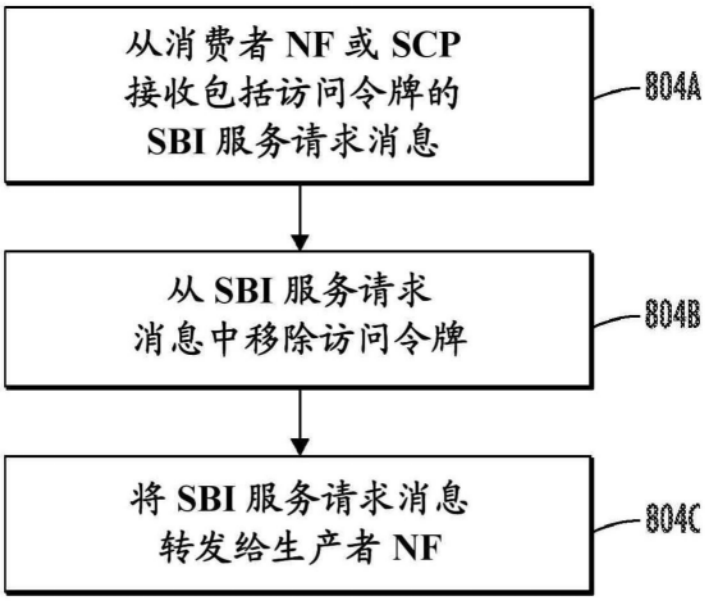

从消费者 NF 或 SCP
接收包括访问令牌的
SBI 服务请求消息
804A
从 SBI 服务请求
消息中移除访问令牌
804B
将 SBI 服务请求消息
转发给生产者 NF
804C

图8C