(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103460738 B
(45)授权公告日 2018.06.01

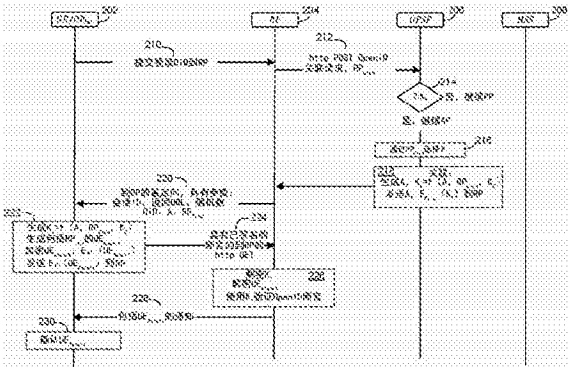
(21)申请号 201280017807.5
(22)申请日 2012.03.23
(65)同一申请的已公布的文献号
申请公布号 CN 103460738 A
(43)申请公布日 2013.12.18
(30)优先权数据
61/466,662 2011.03.23 US
61/466,852 2011.03.23 US
61/525,575 2011.08.19 US
(85)PCT国际申请进入国家阶段日
2013.09.23
(86)PCT国际申请的申请数据
PCT/US2012/030352 2012.03.23
(87)PCT国际申请的公布数据
WO2012/129503 EN 2012.09.27
(73)专利权人 交互数字专利控股公司
地址 美国特拉华州
(72)发明人 I·查 L·J·古乔内 A·施米特 A·莱切尔 Y·C·沙阿
(74)专利代理机构 北京润平知识产权代理有限公司 11283
代理人 陈潇潇 刘国平
(51)Int.Cl.
H04W 12/06(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 101156412 A,2008.04.02,说明书第5页第18行-第31页第20行,图1-15.
CN 101160778 A,2008.04.09,全文.
US 2008132931 A1,2008.04.14,全文.
CN 101164086 A,2008.04.16,全文.
Nokia Corporation, Nokia Siemens Networks.General Issues with SIP Digest.《3GPP TSG SA WG3 Security - S3#62》.2011,第1-2节.
审查员 孙鹏
权利要求书1页 说明书28页 附图17页

(54)发明名称

用于使网络通信安全的方法和用户设备

(57)摘要

可以建立网络实体间的安全通信以用于执行网络实体的认证和/或验证。例如,用户设备(UE)可以与能够发布用于用户/UE认证的用户身份的身份提供方建立安全信道。UE还可以与能够经由网络向UE提供服务的服务提供方建立安全信道。身份提供方甚至可以与服务提供方建立安全信道以用于执行安全通信。这些安全信道中每个安全信道的建立可以使每个网络实体能够向其他网络实体认证。安全信道还可以使UE能够验证已经与其建立安全信道的服务提供方是用于访问服务的预期的服务提供方。



CN 103460738 B

1.一种在包括用户设备UE、网络应用功能NAF和引导服务器功能BSF的系统中的方法，该方法包括：

在所述UE处建立所述UE与所述BSF之间的传输层安全TLS隧道，该TLS隧道具有与之相关联的TLS主密钥；

响应于来自所述BSF的质询，在所述UE处生成随机数并计算认证响应；

在所述UE处接收指示所述UE的用户的成功认证的消息，所述成功认证导致第二密钥的导出，该第二密钥不同于所述TLS主密钥；以及

在所述UE处导出随后用于所述UE与所述NAF之间的安全通信的第三密钥，该第三密钥的导出取决于所述第二密钥和所述TLS主密钥。

2.根据权利要求1所述的方法，其中计算所述认证响应的步骤是使用一个或多个会话发起协议摘要SIP-digest凭证执行的。

3.根据权利要求1所述的方法，其中所述第二密钥是普通引导架构GBA会话密钥Ks，并且导出所述第三密钥的步骤包括：

使用GBA协议从所述Ks导出所述第三密钥，其中所述第三密钥是应用特定的密钥Ks_NAF。

4.根据权利要求3所述的方法，该方法还包括使用所述Ks_NAF在所述UE与所述NAF之间进行安全通信。

5.根据权利要求3所述的方法，其中所述Ks包括完整性密钥或保密性密钥中的至少一者。

6.一种被配置成与网络应用功能NAF和引导服务器功能BSF通信的用户设备UE，该UE包括存储器，在该存储器上存储有计算机可执行指令；以及处理器，被配置成执行所述计算机可执行指令以执行下述：

建立所述UE与所述BSF之间的传输层安全TLS隧道，该TLS隧道具有与之相关联的TLS主密钥；

响应于来自所述BSF的质询，生成随机数并计算认证响应；

接收指示所述UE的用户的成功认证的消息，所述成功认证导致第二密钥的导出，该第二密钥不同于所述TLS主密钥；以及

导出随后用于所述UE与所述NAF之间的安全通信的第三密钥，该第三密钥的导出取决于所述第二密钥和所述TLS主密钥。

7.根据权利要求6所述的UE，其中所述处理器还被配置成执行所述计算机可执行指令以使用一个或多个会话发起协议摘要SIP-digest凭证计算所述认证响应。

8.根据权利要求6所述的UE，其中所述第二密钥是普通引导架构GBA会话密钥Ks，并且所述处理器还被配置成执行所述计算机可执行指令以使用GBA协议从所述Ks导出所述第三密钥，其中所述第三密钥是应用特定的密钥Ks_NAF。

9.根据权利要求8所述的UE，其中所述处理器还被配置成执行所述计算机可执行指令以使用所述Ks_NAF在所述UE与所述NAF之间进行安全通信。

10.根据权利要求8所述的UE，其中所述Ks包括完整性密钥或保密性密钥中的至少一者。

用于使网络通信安全的方法和用户设备

[0001] 相关申请的交叉引用

[0002] 本申请要求2011年3月23日申请的美国临时专利申请No.61/466,662、2011年8月19日申请的美国临时专利申请No.61/525,575以及2011年3月23日申请的美国临时专利申请No.61/466,852的权益，所述申请的全部内容以引用的方式结合于此。

背景技术

[0003] 在通信网络中，网络实体之间的各种通信形式可能容易受到第三方的攻击。例如，根据一个实施方式，用户设备可以尝试从服务提供方经由通信网络接入服务(例如网站)，这个接入尝试和/或来自用户设备的其他通信可以被第三方或中间人(MitM)拦截。例如，这个第三方可以当做预期的(intended)服务提供方来获得与用户设备相关联的信息的接入，例如认证信息(例如用户名和/或密码)。如果第三方成功从用户设备获得认证信息，则第三方可以将认证信息用于非预期的或恶意的目的。例如，第三方可以当做用户设备接入服务和/或来自预期的服务提供方的其他信息。

[0004] 在一个实施方式中，网络通信易受攻击，因为通信没有被充分保护和/或通信被发送而没有合适地保证通信正被发送到的网络实体是用于接收通信的可信(authentic)的或预期的网络实体。例如，可以使用单方认证协议例如经由公共密钥的传输来实施网络通信，其可以使得网络通信易于受到第三方或MitM攻击。

发明内容

[0005] 本发明内容用于以简单的形式介绍各种概念，其在下面具体实施方式中 进一步描述。

[0006] 在此描述的系统、方法和装置实施方式用于在服务提供方和用户设备(UE)之间建立安全通信。例如，网络通信可以在包括UE、服务提供方和/或身份提供方的系统中实施。安全信道可以在UE和服务提供方之间建立。认证参数可以被发送到身份提供方用于执行使用身份提供方的UE的认证。在UE可以确定指示UE成功认证的UE认证断言(assertion)。例如UE认证断言可以从外部网络实体接收到或在UE本地确定。UE可以验证已经与其建立安全信道的服务提供方是预期的服务提供方。预期的服务提供方可以包括预期从其接收服务或执行对其认证以用于接入该服务的服务提供方。可以使用在使用身份提供方的UE认证期间和/或安全信道建立期间生成的至少一个参数来将服务提供方验证为预期的服务提供方。

[0007] 根据另一示例实施方式，UE可以被配置成建立与服务提供方的安全通信。UE可以包括在其上存储有计算机可执行指令的存储器，以及配置成执行计算机可读指令的处理器。UE可以被配置成建立UE与服务提供方之间的安全信道。UE可以向身份提供方发送认证参数用于执行使用身份提供方的UE认证。可以在UE确定指示UE成功认证的认证断言。例如，UE认证断言可以从外部网络实体接收或在UE本地确定。UE还可以被配置成验证已经与其建立安全信道的服务提供方是用于为服务执行认证的预期的服务提供方。预期的服务提供方可以包括预期从其接收服务和/或执行对其认证以用于接入该服务的服务提供方。UE可以

使用在使用身份提供方的UE认证期间和/或安全信道建立期间生成的至少一个参数来验证服务提供方为预期的服务提供方。

[0008] 根据另一示例实施方式，安全信道可以在身份提供方和服务提供方之间建立。例如可以经由身份提供方和服务提供方之间的安全信道在服务提供方处接收密钥信息。例如，通过使用接收到的密钥信息，安全信道还可以在服 务提供方和UE之间建立。在服务提供方，可以接收到指示UE认证的认证断言。认证断言可以在服务提供方处使用经由身份提供方和服务提供方之间的安全信道和/或服务提供方和UE之间的安全信道接收的信息被验证。

[0009] 本发明内容用于以简单的形式介绍下面在具体实施方式中进一步描述的概念的选择。本发明内容不意图建立所要求主题的关键特征或必要特征，也不意图用于限制所要求的主题的范围。而且，所要求的主题不局限于本公开内容任何部分提到的解决任何或所有缺陷的任何限制。

附图说明

[0010] 通过给定的示例并结合附图，可以从下面的说明中得到更详细的理解，其中：

[0011] 图1是用于建立身份提供方和用户设备(UE)之间的安全信道的提供(provisioning)阶段的示例消息流图；

[0012] 图2是用于使用本地身份提供方的认证阶段的示例消息流图；

[0013] 图3是用于服务提供方认证的消息交换的示例消息流图；

[0014] 图4是用于服务提供方认证的消息交换的另一示例消息流图；

[0015] 图5是显示使用UE和服务提供方之间预先建立的安全信道为本地提供方认证建立安全信道的示例消息流图；

[0016] 图6是普通引导(Bootstrap)架构(GBA/GBA_H)协议的示例的示例消息流图；

[0017] 图7是用于将传输层安全(TLS)和GBA与会话初始协议摘要(SIP-Digest)认证绑定的示例消息流图；

[0018] 图8显示了示例通信系统图，该通信系统实施本地认证实体/身份提供方以及云/远程计算服务；

[0019] 图9显示了使用SIP-Digest认证并包括服务提供方认证的示例消息流 图；

[0020] 图10显示了到身份提供方的服务提供方认证的示例协议的示例消息流图；

[0021] 图11显示了本地身份提供方的提供阶段的示例消息流图；

[0022] 图12显示了本地断言提供方的示例认证阶段的示例消息流图；

[0023] 图13A是可以在其中实施一个或多个公开的实施方式的示例通信系统的系统图；

[0024] 图13B是可以用于图13A所示的通信系统中的示例无线发射/接收单元(WTRU)的系统图；

[0025] 图13C是可以用于图13A所示的通信系统中的示例无线电接入网(RAN)和示例核心网的系统图；

[0026] 图13D是根据实施方式的示例RAN和核心网的另一系统图；以及

[0027] 图13E是根据实施方式的示例RAN和核心网的另一系统图。

具体实施方式

[0028] 在此公开的系统、方法和装置实施方式用于例如网络实体(例如用户/用户设备(UE)、服务提供方和/或身份提供方)之间的安全通信。如在此所述,安全通信可以经由使用实体间共享密钥/秘密或使用公共/私用密钥建立的网络实体间的安全信道进行。这些安全信道可以用来阻止例如来自例如中间人(MitM)攻击的第三方攻击。

[0029] 在此描述的实施方式中,安全通信可以使用共享密钥或共享秘密以识别用于发送和/或接收通信的预期的、经过认证的实体来进行。例如共享密钥或共享秘密可以用来以指示网络实体可信性的方式来加密或签名在网络实体间发送的消息。

[0030] 在示例实施方式中,在此描述的安全通信可以基于和/或绑定至开放ID (OpenID)认证协议。在OpenID认证中,服务提供方可以是依赖方(RP)和/或身份提供方可以是OpenID身份提供方(OP)。OpenID认证可以包括OpenID和/或称为本地OpenID的变量的使用,在所谓的本地OpenID中,OpenID中的OP的一些功能由本地实体(例如UE、网关、智能卡、通用集成电路卡(UICC)等等)执行。

[0031] 在此描述在OpenID认证流中RP的认证。这可能例如在用户/UE和RP不具有信任关系的情况下有用,该信任关系例如使用来自例如AAA数据库的RP可接入的用于UE的网站证书和/或一组凭证来建立。另一实施方式可以包括如在此描述的本地OP-RP私用共享秘密的建立。

[0032] 本地移动单点登录(SSO)是一术语,用来共同地指示SSO和/或有关身份管理功能的部分或全部(其传统上由例如基于网络(web)的SSO服务器执行),由基于本地的实体或模块(例如驻留在UE、智能卡或UICC的安全环境)执行,该实体或模块可以是通信设备本身的部分或全部,或者其中这样的实体或模块物理上或逻辑上位于(例如位于本地,例如经由网关连接等等)通信设备和/或其用户附近很近的位置。例如实体/模块可以嵌入设备,附着至设备,和/或通过本地接口、线缆或短距离无线方式连接至设备。

[0033] 本地OpenID可以用作术语以指示本地移动SSO的类型,从而SSO或身份管理基于OpenID协议。例如本地OpenID可以用来指示OpenID身份提供方(OP或IdP)的功能,其可以由位于本地的实体/模块执行。

[0034] 本地IdP是一术语,用来指示执行本地认证和/或断言功能的本地实体或模块。例如本地IdP可以为本地OpenID执行OpenID服务器的认证和/或断言功能。缩写OP_{loc}可以用来表示实施OpenID功能的本地IdP,然而本地IdP可以执行类似的功能,并且可以不需要实施OpenID协议。本地IdP的一个功能可以是通过关于用户和/或设备身份的断言便于用户和/或设备的认证。在示例实施方式中,这样的认证断言可以从本地IdP发送到运行在设备上的浏览器代理(BA),其可以将认证断言转发到外部RP。当本地IdP提供的功能被主要局限于提供这样的认证断言时,本地IdP可以称为本地断言实体(LAE)。

[0035] 本地IdP可以处理、创建、管理、和/或发送认证断言消息到一个或多个外部接收方。认证断言消息可以断言关于用户或设备的一个或多个身份验证的状态。例如,在OpenID协议中,例如RP的第三方可以是认证断言消息接收方之一。本地IdP还可以使用加密技术,例如共享密钥或公共/私用密钥变型来签名认证断言消息。

[0036] 本地OpenID实施可以使用一个或多个加密密钥,例如根会话密钥。根会话密钥可

以意图针对RP和驻留在UE上的OP_{loc}之间的使用。这样的密钥可以作为RP和OP之间的根会话密钥，可以从该根会话密钥导出其他密钥。本地OpenID方法还可以使用认证断言密钥，其可以用来签名用于用户认证的认证断言消息的一个或多个。这样的认证断言密钥可以从根会话密钥中导出。

[0037] 本地OpenID实施可以使用称为OpenID服务器功能(OPSF)的服务，它的角色是生成、共享和/或分发本地IdP和/或RP可以使用的秘密。在示例实施方式中，OPSF和本地IdP可以被外部RP看作单个实体。OPSF可以能够验证本地OpenID发布的签名，和/或可以由RP例如经由公共互联网直接可达(reachable)。在设备上的浏览器可以通过修改设备上的本地DNS解析模块被重定向到本地IdP，由此OPSF的地址映射到本地IdP。

[0038] OpenID实施可以使用服务，该服务便于发现代表RP的本地IdP。这样的服务可以由例如Op-agg表示。

[0039] 在此公开的是使用OpenID(包括，例如OpenID和/或本地OpenID)实施的安全系统、方法以及装置。在此描述的实施方式的一些可以例如在UE实施。用户设备可以传送OpenID请求到OP。OP可以被用于如在此进一步 描述的认证UE和/或RP。

[0040] 实施方式被描述用于RP到本地OP的透明委托(transparent delegated)认证。根据在此描述的实施方式，公开的协议显示使用OpenID和/或利用例如OP_{loc}的签名的认证断言的本地提供方来如何执行RP认证。如在此所述，可以添加质询(challenge)值和/或随机数用于重放保护(例如图1中协议的步骤112和120)。

[0041] 在此描述认证RP的实施的一方面可以包括OPSF节点的委托认证的方面。它可以遵循通用质询-响应策略，其中OP_{loc}提出质询RP_{Chv}。这个质询可以由OPSF以合适的方式加密，由此可信的RP能够解密该质询。例如，RP和OPSF可以共享秘密$K_{r,o}$，其可以被用于加密和解密该质询。

[0042] 图1显示了示例提供阶段(PP)的消息流图。如图1所示，提供阶段可以包括UE/OP1oc102、RP104、OPSF106和/或本地订阅服务(HSS)108。UE/OP_{loc}102可以在110提交登录标识符(例如，如超文本传送协议(http)地址或电子邮件的OpenID标识符(OID))到RP104。在110的消息可以包括RP质询值RP_{Chv}。RP质询值RP_{Chv}是RP104可以合适响应的值以证明它的可信性。例如，这可以是一次性使用的随机值。在112，RP104可以发送关联请求(例如http POST(发送)OpenID关联请求)到OPSF106。关联请求可以包括RP凭证RP_{Cred}，其对应于RP104和/或RP质询值RP_{Chv}。RP_{Cred}可以是RP104的标识符，其可以允许OPSF106来选择在OPSF106和RP104之间共享的正确的预先共享的密钥$K_{r,o}$。如果OPSF106使用其他方式(例如因特网URL)识别RP，则RP_{Cred}可以从消息发送中省略。在114，OPSF106可以确定OPSF106和UE/OP_{loc}102之间的共享秘密K_0是否已经被提供。如果被提供，那么OPSF106可以进行认证阶段(AP)(例如，如图2所示)。如果没有被提供，那么提供阶段可以继续。

[0043] 在116，OPSF106可以基于例如RP_{Cred}或RP104的另一信任的标识符 选择共享秘密$K_{r,o}$。OPSF106可以在118执行与RP104的关联。OPSF106可以在118生成关联句柄(handle)A和/或签名密钥S。签名密钥S可以基于关联句柄A的函数被生成。OPSF106可以发送关联句柄A和签名密钥S到RP104。签名密钥S可以用共享密钥$K_{r,o}$加密，其可以例如称为$EK_{r,o}(S)$。在120，RP104可以发送重定向消息到E/OP_{loc}102。重定向消息可以包括例如会话ID、返回URL、随机数、登录标识符(例如OID)和/或关联句柄A的参数。在122，UE/OP_{loc}102可以发送请求

(例如http GET(获取)请求)到OPSF106。请求(例如http GET请求)可以包括例如会话ID、返回URL、随机数、登录标识符(例如OID)和/或关联句柄A的参数。

[0044] 在124,OPSF106可以从HSS108获得认证向量和/或其他信息。在126,OPSF106可以发送认证质询到UE/OP_{1oc}102。在128,UE/OP_{1oc}102可以计算认证响应,并发送认证响应到OPSF106。在130,OPSF106可以确认(validate)认证响应并生成在OPSF106和UE/OP_{1oc}102之间共享的共享秘密K_0。在认证响应确认之后共享秘密K_0的生成可以将UE/OP_{1oc}102和OPSF106之间的安全关联的建立绑定到这个认证。例如,如图1所示,这个绑定可以是对共享秘密K_0的生成的认证响应的确认的程序性绑定。在132,UE/OP_{1oc}102可以生成共享秘密K_0。在134,OPSF106可以在认证UE/OP_{1oc}102之后生成认证断言消息UE_{Assert}。认证断言可以包括由K_0加密的RP_{Cred}和RP_{Chv},其例如可以称为$K_0(RP_{Cred},RP_{Chv})$。这个认证断言,包括$K_0(RP_{Cred},RP_{Chv})$,可以向UE/OP_{1oc}102指示OPSF106已经认证RP104,使得可以确保UE/OP_{1oc}102正在与合法的RP104交谈。在一个示例实施方式中,RP_{Cred}可以是用于可由UE/OP_{1oc}102识别的RP104的名称(或其他文本值)。OPSF106还可以用签名密钥S加密认证断言消息UE_{Assert},其可以例如称为$E_S(UE_{Assert})$。在136,OPSF106可以发送重定向消息到UE/OP_{1oc}102。重定向消息可以用已签名的断言消息重定向UE/OP_{1oc}102到RP104。在138, UE/OP_{1oc}102可以发送具有已签名的断言消息的请求(例如http GET请求)到RP104。在140,RP104可以使用共享密钥$K_{r,o}$解密签名密钥S,和/或通过解密$E_S(UE_{Assert})$使用签名密钥S验证认证断言消息(例如OpenID断言消息)。在142,RP104可以发送包括认证断言UE_{Assert}的通知到UE/OP1oc102。在144,UE/OP1oc102可以通过解密RP_{Chv}和/或RP_{Cred}确认认证断言UE_{Assert}。

[0045] 如图1所示,可以实施协议,其中可以建立OPSF106和UE/OP_{1oc}102之间的共享秘密K_0。在示例实施方式中,提供阶段之前或期间,OPSF106和UE/OP_{1oc}102可以不共享秘密。当这个协议运行时,这个共享的秘密可以例如使用网络实体HSS108通过包括基于网络的认证而被建立。通过在UE_{Assert}中包括RP_{Chv}和RP_{Cred},用K_0加密,可以向UE/OP_{1oc}102保证接收的消息源自由RP_{Cred}标识的RP104。通过比较RP_{Cred}所要求的身份与RP104的身份,UE/OP_{1oc}102可以验证没有其他RP接收到认证信息,并且RP104是UE/OP_{1oc}102期望向其执行认证的预期的RP。UE_{Assert}中的信息片(piece)RP_{Cred}可以用OPSF106生成的某显式陈述(statement)RP_{Assert}替换来表示到UE102的RP104身份。UE_{Assert}可以是用签名密钥S签名的被签名的OpenID断言消息。

[0046] 图1还显示了RP104可以被认证到(例如隐式地认证)到UE/OP_{1oc}102。如果RP104是由RP_{Cred}识别的可信RP(从那时起,它能够解密签名密钥S),则RP104可以执行UE/OP_{1oc}102的OpenID认证。由OPSF106在协议中向RP104认证的唯一UE/OP_{1oc}102可以认证RP104。在示例实施方式中,协议流可以不从本地OpenID认证修改。另外,网络认证可以维持不受影响。额外的加密操作可以在协议中的一方或多方实施以保证进一步的保护。

[0047] 对于用于本地OpenID与普通引导架构(GBA)(例如,3GPP GBA)的交互工作的可能实施,如果存在UE/OP_{1oc}102和OPSF106之间的预先共享的秘密K_0,则可以实施协议。

[0048] 图2显示了认证阶段(AP)的示例消息流图。例如,认证阶段可以实施UE/OP_{1oc}202、RP204、OPSF206和/或HSS208。图2所示的协议流可以独立应用,或例如如果不存在预先共享的密钥,与图1所述协议提供阶段结合用于使用UE/OP_{1oc}102和OPSF106之间的共享秘密建立安全信道。

[0049] 如图2所示，在210，UE/OP_{1oc}202可以向RP204提交登录标识符(例如，如http地址或电子邮件的OpenID标识符(OID))。在212，RP204可以发送关联请求(例如http POST OpenID关联请求)到OPSF206。关联请求可以包括标识RP204的RP凭证RP_{Cred}。在214，OPSF206可以确定共享密钥K_0是否已被确定或提供，并且如果没有，则协议在提供阶段中继续进行K_0的提供。如果K_0已经被提供，则协议可以继续进行认证阶段。例如，在216，OPSF206可以基于对应于RP204的RP_{Cred}选择共享密钥$K_{r,o}$。在218，OPSF206可以执行与RP204的关联。OPSF206可以生成关联句柄A和/或共享密钥K_1。共享密钥K_1可以是OPSF206、UE/OP_{1oc}202和/或RP204之间的共享密钥，其例如根据关联句柄A、RP_{Cred}和/或共享密钥K_0的函数被生成。例如，UE/OP_{1oc}202和/或OPSF206可以被配置成生成共享密钥K_1。RP204可以接收共享密钥K_1并使用它用于与UE/OP_{1oc}202的安全通信。OPSF206可以发送关联句柄A和加密的K_1到RP204，其中K_1由共享密钥$K_{r,o}$加密，其例如可以称为$EK_{r,o}(K_1)$。在220，RP204可以发送消息到UE/OP_{1oc}202，该消息包括例如会话ID、返回URL、随机数、登录标识符(例如OID)、关联句柄A和/或RP_{Cred}的参数。在220的消息可以是重定向消息，其例如重定向UE/OP_{1oc}202到RP204。在222，UE/OP_{1oc}202可以生成K_1。例如，K_1可以根据关联句柄A、RP_{Cred}和/或K_0的函数被生成。在222，UE/OP_{1oc}202可以执行本地认证，并且在222可以生成包括RP_{Chv}的认证断言消息UE_{Assert}，和/或可以用密钥K_1加密UE_{Assert}，其例如可以称为$EK_1(UE_{Assert})$。例如UE_{Assert}可以是OpenID断言消息。UE/OP_{1oc}202可以发送加密的断言消息UE_{Assert}到 RP204。在224，UE/OP1oc202可以发送具有已签名的断言的请求(例如httpGET请求)到RP204。在226，RP204可以使用$K_{r,o}$解密K_1。RP204可以在226使用解密的K_1解密认证断言消息UE_{Assert}。RP204可以使用共享密钥K_1验证OpenID断言。在228，RP204可以发送包括认证断言消息UE_{Assert}的通知到UE/OP_{1oc}202。在230，UE/OP_{1oc}202可以确认认证断言消息UE_{Assert}。

[0050] 通过确认在228接收的UE_{Assert}中的信息匹配在224发送的UE_{Assert}中的信息，UE/OP_{1oc}202可以被保证在228接收到的信息源自被RP_{Cred}标识的RP204，且在210UE/OP_{1oc}202向该RP204发送登录信息。例如，通过将RP_{Cred}中所要求的身份与RP104的身份进行比较，UE/OP_{1oc}202可以验证没有其他RP接收到认证信息，并且RP104是UE/OP_{1oc}102期望向其执行认证的预期的RP。

[0051] 可以通过在UEAssert中包括新鲜(fresh)的质询RP_{Chv}确保认证的新鲜性(freshness)。UE/OP_{1oc}202可以通过验证其包括这个质询值来确认接收到的UE_{Assert}，如果该RP204能够用真实(genuine)的K_1解密UEAssert，则RP204可以知道该质询值，真实的K1可以由UE/OP_{1oc}202和RP204共享。真实的K_1的使用可以证明RP204拥有被OPSF206和由RP_{Cred}标识的RP共享的$K_{r,o}$。

[0052] 根据示例实施方式，RP认证可以使用OP而无需本地OpenID来执行(例如使用非本地OpenID)。OpenID协议中包含的RP认证可以包括对OpenID协议本身的改变和/或对OP和/或RP实施的改变。RP认证可以添加安全益处，例如提供针对假冒或流氓(rogue)RP可能攻击的对策。对于OpenID(或本地OpenID)在UE上的实施可以不受任何这样的RP认证的影响。例如，UE可以不包括本地OP功能并且可以在实施方式中不能发送质询RPChv到RP。RP认证可以包括OP和RP之间的质询响应步骤，其中OP可以发送具有新鲜性证明的质询到RP(例如经由加密的随机数)。RP可以使用预先 建立的共享秘密$K_{r,o}$来解密这个随机数并返回回答(answer)到OP。可替换地或额外地，随机数可以不被加密，并且被RP在其回答中签名。对认

证质询的响应可以作为对OP认证质询的直接响应，或者它可以被整合到重定向消息中，其可以从UE发送到OP。在任一情况下，OP可以在参与UE认证之前具有RP认证的可靠证据。这可以允许在RP认证失败的情况下停止协议，和/或在这样的RP认证失败的情况下节省UE和OP之间的通信努力。OP可以接着直接传送针对失败的RP认证的信息到UE。

[0053] 图3显示了用于RP304认证的消息交换示例部分的消息流图。消息流图包括UE302、RP304和OP306之间的通信。在认证失败的情况下，OP306可以强制与UE302的超文本传送协议安全(HTTPS)通信，和/或通知UE302该失败。否则，可以继续OpenID认证。

[0054] 如图3所示，在308，UE302可以提交登录标识符(例如OID)到RP304。RP304可以在310发送关联请求(例如http POST OpenID关联请求)到OP306。在310的关联请求可以包括RP_{Cred}。在312，OP306可以例如基于RP_{Cred}或RP304的另一被信任的标识符选择OP306和RP304之间的共享秘密$K_{r,o}$。在314，OP306执行与RP304的关联。在314，OP306可以生成关联句柄A、签名密钥S、和/或RP_{Chv}。RP_{Chv}可以使用$K_{r,o}$被加密，其例如可以称为$EK_{r,o}(RP_{Chv})$。OP306可以发送关联句柄A、签名密钥S和/或$EK_{r,o}(RP_{Chv})$到RP304。

[0055] 在316，RP304可以使用共享密钥$K_{r,o}$解密RP_{Chv}。在318，RP304可以经由UE302发送消息到OP306，该消息可以包括例如会话ID、返回URL、随机数、登录标识符(例如OID)、关联句柄A和/或RP_{Chv}的参数。例如，在318的消息可以包括重定向消息，其可以重定向UE302到OP306。在320，UE302可以发送消息(例如http GET请求)到OP306。在320的消息可以包括例如会话ID、返回URL、随机数、登录标识符(例如OID)、关联句柄 A和/或RP_{Chv}的参数。在322，OP306可以用RP_{Chv}确认RP304的身份。在324，如果RP304的身份被确定为无效，则OP306可以在326发送通知到UE302，指示RP304无效(例如经由HTTPS通知指示RP304无效)。如果RP304的身份有效，可以在328继续认证(例如OpenID认证)和/或OP306可以发送通知，指示RP304的身份有效(未示出)。

[0056] 在另一实施方式中，如果RP304建立了与OP306的安全关联，对应的步骤可以被修改以将来自OP306的质询结合到协议中以用于建立安全关联。在关联建立期间，OP306和RP304可以建立消息认证码(MAC)密钥，其可以用来签名认证断言消息UE_{Assert}。这个密钥使用临时秘密密钥被加密发送，临时秘密密钥在OP306和RP304之间协商(例如使用迪菲－赫尔曼(Diffie-Hellman，DH)程序)。除了临时秘密密钥，OP306可以包括响应于RP304的随机数。该随机数可以使用例如临时秘密密钥(例如DH密钥)被加密。

[0057] RP304可以基于协商的密钥(例如DH密钥)解密随机数和/或MAC密钥。RP304可以使用其自身的预先建立的$K_{r,o}$密钥来加密或签名从OP306接收到的随机数。RP304可将这个密钥作为参数加入重定向消息，该重定向消息可以例如被发送到UE302。因为UE302可以遵循到OP306的重定向，OP306可以接收到已签名的或加密的随机数，并且可以使用共享密钥Kr，o来认证RP304。在认证失败的情况下，OP306可以发送警告消息到UE302来保护它免受未认证的RP的攻击。在成功RP认证的情况下，OP306可以继续该协议。

[0058] 在示例实施方式中，OP306可以能够发送信息到RP304，其中OP306和RP304之间没有建立关联(例如OpenID中的无状态(stateless)模式)。在无状态(stateless)模式中，例如在发现期间，OP306和RP304之间可以交换信息。然而，这并不保证该发现包括OP306(例如在委托发现的情况下，其中用户标识符例如可以是在http://myblog.blog.com，和/或可以指向在http://myblog.myopenid.com的OP的OpenID OP端点URL)。因此，在myopenid.com

的OP306可以不直接被涉及在发现中并且可以在这个阶段不能认证RP304。

[0059] 如果OP306能够在发现步骤期间提供信息到RP304(用户标识符页面并不在OP306本身托管(host)),OP306可以动态生成随机数作为发现信息页面的一部分和/或将它与HTTP请求RP304的标识符相关联(例如URL或电子邮件地址)。OP306可以希望RP304签名或加密这个随机数和/或在重定向消息中包括该信息。

[0060] OP306可以强制使用HTTPS。例如,UE302可以被OP306重定向到使用HTTPS,使得UE302和OP306之间任何随后的通信可以用HTTPS来保护。这个特征可被OpenID标准实施显式地允许,例如OpenID认证2.0。这样的保护可以使得例如阻止对从OP306到UE302的OpenID认证质询消息的中间人(MitM)攻击。这可以允许在RP认证失败的情况下以受保护的方式发送警告信息到UE302。

[0061] 在此描述的示例实施方式针对分割(split)终端实施。分割终端实施可以指两个实体驻留在网络的用户侧的情形。例如认证代理(AA)和浏览代理(BA)可以与UE(例如UE302)相关联和/或驻留在该UE上。AA可以执行认证步骤,而BA可以是服务的观察者或消费实体。在分割终端实施的示例中,用户可以打开浏览器来从例如RP304的RP获取某服务(例如网站)。RP304可以执行与OP306和用户的AA一些步骤(例如关联和/或发现)。例如,UE302可以被OP306联系。OP306和UE302可以基于例如BA可以不知道的GBA网络凭证来执行认证。例如,如果OP306和AA之间的认证成功,则BA可以获得对在RP304的服务的接入。可以实施多种变型。每种变型可以包括例如AA和BA之间的物理信道(其例如可以是本地接口 (例如蓝牙®等))或逻辑信道等等。可以通过用户将AA上显示的信息输入BA来创建逻辑信道,由此例如两个会话可以逻辑上结合。

[0062] 移动网络运营商(MNO)的自己的服务和/或第三方服务提供方的服务可以被提供到UE302或者MNO知道的设备。如果MNO想使用户将不同/多个设备连接单个认证者(例如UE302),则可以使用分割终端实施。

[0063] 用于分割终端实施的示例选项可以包括其中两个会话之间的加密绑定被创建的那些。实施还可以包括AA向用户显式凭证信息的情形,用户可以将该凭证信息在BA中输入来向RP304进行认证(例如使用在此描述的逻辑信道)。

[0064] 作为替代的或额外的,凭证可以在BA和AA之间的安全本地链路上发送(例如使用在此描述的物理信道)。在这个实施中,AA可以用作认证令牌(token)/密码生成器。在示例实施方式中,BA可以从AA接收共享密钥K_1和认证断言消息UE_{Assert},其可以用$K_{r,o}$加密并且例如可以称为$EK_{r,o}(K1, UE_{Assert})$,并且发送它们到RP304。这个信息可以被RP304用来认证用户。在示例实施方式中,可以用本地断言提供方建立分割终端实施,本地断言提供方在UE302/AA内生成认证断言消息UE_{Assert}。

[0065] 添加的安全功能可以依据基于本地OpenID的认证被实施。认证可以基于本地OpenID来提供私用秘密(例如图4中在410和414所示加密密钥E)。这个秘密可以用来例如建立OP_{loc}和/或它驻留在的信任环境(例如智能卡或其他被信任的计算环境)和RP之间的私用、安全信道。可替换地,安全信道可以在UE的某相对非安全部分中具有端点(endpoint),其可以称为UE平台。

[0066] 在此描述的选项用于绑定这样的安全信道到本地OpenID认证。在示例实施方式中,安全信道可以用UE平台和RP建立,并且本地OpenID认证可以在这个安全信道内被执行。

这个示例实施方式对于某些实施是充分的，但 可能不满足其他的安全需求。例如建立安全信道的UE不如OP_{1oc}所驻留在的被信任的环境(智能卡或其他被信任的计算环境)安全。来自相同被信任的环境并被定向到RP的私用数据可以在在UE中具有相对不安全的内在节点的信道上传输。因此，可替换的实施方式可以被实施，其可以允许OP_{1oc}，和/或它所驻留在的被信任的计算环境，来与独立于UE平台的属性的RP交换秘密，以及将信息的这样的私用属性绑定到至RP的本地OpenID认证。

[0067] 图4显示了示例实施方式的消息流图，该实施方式创建和/或实施本地认证实体(例如UE/OP_{1oc}402)和RP404之间的安全信道。图4所示的流图包括UE/OP_{1oc}402、RP404和/或OPSF406之间的通信。如在408所指示，本地OpenID认证可以至多在UE/OP_{1oc}402在410生成已签名的认证断言所在的点被执行。在410，UE/OP_{1oc}402可以生成签名密钥S，其可以使用密钥导出函数(KDF)从关联句柄A和共享密钥K_0的函数中导出。共享密钥K_0可以在UE/OP_{1oc}402和OPSF406之间共享以用于安全通信。签名密钥S可以是例如OpenID签名密钥。UE/OP_{1oc}402可以执行本地认证，并且认证断言消息UE_{Assert}可以在410生成并可以包括加密的种子值(Seed)。Seed可以用于隐藏两方或更多方之间的共享秘密。例如因为共享秘密可以不在各方之间传送，所以可以隐藏共享秘密。可代替的是Seed可以被传送并可以用来在共享秘密的各方(例如本地地)导出共享秘密。

[0068] 认证断言消息UE_{Assert}可以例如是OpenID断言。UE/OP_{1oc}402可以用签名密钥S(称为E_S(Seed))加密Seed，其可以对于OPSF406、UE/OP_{1oc}402和/或RP404是私用的。在可替换实施方式中，UE/OP_{1oc}402可以使用从S导出的密钥以预先确定的方式加密Seed。UE/OP_{1oc}402可以以预先确定的方式从Seed生成加密密钥E，RP404例如可以知道该方式。UE/OP_{1oc}402可以用签名密钥S签名认证断言消息UE_{Assert}。从本地认证生成加密密钥E可以绑定UE/OP_{1oc}402和RP404之间安全信道的建立到这个本地认证。

[0069] 在412，UE/OP_{1oc}402可以发送具有已签名的断言UE_{Assert}的消息(例如http GET请求)到RP404。在414，RP404可以验证认证断言消息UE_{Assert}并使用签名密钥S来解密Seed信息。RP404可以基于Seed信息生成加密密钥E。例如RP可以以预先确定的方式从Seed信息生成加密密钥E，UE/OP_{1oc}402可以知道该方式。加密密钥E可以对UE/OP_{1oc}402和RP404是私用的。

[0070] RP404可以用加密密钥E加密先前被验证的认证断言UE_{Assert}，并且将其发送回UE/OP_{1oc}402。例如，在416，RP404可以发送通知到UE/OP_{1oc}402，该通知包括认证断言消息UE_{Assert}，例如其可以用加密密钥E(EE(UE_{Assert}))加密。这可以提供秘密建立的证实(confirmation)到UE/OP_{1oc}402。UE/OP_{1oc}402可以在418通过使用加密密钥E解密认证断言消息UE_{Assert}来确认该认证断言消息UE_{Assert}。通过确认在416接收到的UE_{Assert}中的消息匹配在412发送的消息UE_{Assert}，UE/OP_{1oc}402可以被保证在416接收的消息源自预期的RP404。例如，通过比较在416从RP404接收的通知中的Seed与在410UE_{Assert}中包括的Seed，UE/OP_{1oc}402可以验证没有其他RP接收到认证消息，并且RP404是UE/OP_{1oc}402期望向其执行认证的预期的RP。UE/OP_{1oc}402可以信任在418的这个验证，作为RP404获得了密钥S的指示，RP404能够通过密钥S解密Seed和导出E。在420，加密密钥E可以被用来(例如在另一协议中)建立UE/OP_{1oc}402和RP404之间的安全信道。可以被用来建立这个安全信道的一个示例协议可以包括TLS-PSK协议，其可以是接受预先共享密钥作为输入并基于预先共享密钥实现安全信道的

普通TLS协议的变型。因特网工程任务组(IETF)在请求注解(RFC)文档4279和4785中阐述了TLS-PSK的一个示例实施方式。

[0071] 如图4所示，加密密钥E的导出可以使用对Seed的了解和KDF来执行，其可以是公开的。Seed可以被RP404知道，并被保护不被其他的知道，因为它用签名密钥S来加密。S可以由OPSF406通过安全信道(例如基于证 书的传输层安全(TLS))泄露给RP404。UE402可以获得拥有签名密钥S的RP404的证实，因为RP404可以将$E_E(UE_{Assert})$发送回UE402，如果RP404能够解密Seed，则它能够这么做。因此，UE402可以从RP404获得密钥证实。图4所示的协议流可以与RP认证协议结合，例如在此描述的RP认证协议，以能够实现安全通信。

[0072] 虽然示出Seed信息可以用来导出实体间的私用、共享密钥，但是私用、共享密钥可以用其他方式导出。例如实施方式可以实施迪菲一赫尔曼密钥建立。

[0073] 如在此所述，一些初始值，例如Seed，可以在希望建立共享秘密的实体间传送。Seed的加密可以用来保护Seed免受中间人攻击。使用签名密钥S或从S导出的密钥的特定加密可以用来绑定到本地OpenID认证。加密的通知消息可以用来绑定到本地OpenID认证。这可以添加秘密建立的到$UE/OP_{1oc}402$的证实的特征。

[0074] 秘密的建立可以通过RP404发送在重定向消息中的加密的Seed到$UE/OP_{1oc}402$而更早地在本地OpenID协议流中开始。

[0075] 在另一实施方式中，RP404可以是在到期望安全信道的端点的路径上的中间节点。在这个情况下，RP404可以从这个端点接收Seed，该端点可以是服务器，$UE/OP_{1oc}402$可以希望与其建立安全信道，并且RP404可以用作到服务器的认证，以及可选的授权、网关。加密密钥E可以被用在另一协议中来建立$UE/OP_{1oc}402$、或UE平台和RP404之间的安全信道。用于以这个方式使用加密密钥E的候选协议可以包括TLS-PSK协议，其可以是接受预先共享密钥作为输入并基于预先共享密钥实现安全信道的TLS协议的变型。在一些实施方式中，秘密的建立可以与RP认证结合。

[0076] 图5是显示使用UE-RP预先建立的安全信道和认证后的密钥证实的用于本地OpenID认证的安全信道的建立的流程图。例如，安全信道建立可以 允许$UE/OP_{1oc}502$或UE平台和RP504来建立安全信道，并继续本地OpenID认证。图5所示的流程图可以在认证期间用来证实到RP504的安全信道密钥，以及例如可以被绑定到认证。这可以通过从安全信道，例如传输层安全(TLS)隧道，提取密钥材料XS，和/或从XS导出绑定响应B_{res}来完成。

[0077] 如图5所示，$UE/OP_{1oc}502$和RP504可以在508建立安全信道。例如，可以使用TLS建立安全信道。在510，$UE/OP_{1oc}502$可以提交登录标识符(例如OID)到RP504。在512，RP504可以发送关联请求(例如http POST OpenID关联请求)到OPSF506。在514，OPSF506可以执行与RP504的关联。例如，OPSF506可以生成关联句柄A和/或共享密钥K_1。共享密钥K_1可以是OPSF506、RP504和/或$UE/OP_{1oc}502$之间的共享密钥。共享密钥K_1可以从关联句柄A和/或共享密钥K_0导出。OPSF506可以发送关联句柄A和/或共享密钥K_1到RP504。

[0078] 在516，RP504可以发送重定向消息到$UE/OP_{1oc}502$，该重定向消息重定向$UE/OP_{1oc}502$到OP，该OP本地驻留在$UE/OP_{1oc}502$上。重定向消息可以包括例如会话ID、返回URL、随机数、登录标识符(例如OID)和/或关联句柄A的参数。在518，$UE/OP_{1oc}502$可以执行本地认证，并且可以生成共享密钥K_1。共享密钥K_1可以从关联句柄和/或共享密钥K_0生成。从本地认证生成共享秘密K_1可以绑定$UE/OP_{1oc}502$和RP506之间安全信道的建立到这个本地认证。UE/

OP_{1oc}502可以从安全信道提取密钥材料XS，并且可以从XS生成绑定响应B_{res}(B_{res}=g(XS))。根据示例实施方式，绑定响应B_{res}的导出可以通过使用具有额外随机数(例如关联句柄A)的MAC算法完成。UE/OP_{1oc}502可以在认证断言消息UE_{Assert}中包括绑定响应B_{res}。B_{res}可以被包括在认证断言消息UE_{Assert}的如OpenID所允许的扩展字段中。认证断言消息UE_{Assert}可以由UE/OP_{1oc}502使用共享密钥K_1来签名，其例如可以称为SigK_1(UE_{Assert})。在520，UE/OP_{1oc}502可以发送已签名的认证断言消息SigK_1 (UE_{Assert})到RP504。例如，已签名的认证断言消息可以在http GET请求中发送。在示例实施方式中，XS可以不直接用在到RP504的消息中，因为这可能泄露关于安全信道的信息给攻击者。

[0079] RP504可以在522使用共享密钥K_1验证已签名的断言SigK_1(UE_{Assert})。例如在成功验证来自UE/OP_{1oc}502的认证断言之后，RP504可以从RP504具有的安全信道密钥材料XS*导出比较值B_{res}*，并且发现它与接收到的B_{res}一致。例如，RP504可以从安全信道提取密钥材料XS*，从密钥材料XS*生成绑定响应B_{res}*(B_{res}*=g(XS*))，并验证绑定响应B_{res}*等于在已签名的断言中指示的并验证绑定响应B_{res}。RP504可以知道被认证方是安全信道端点，因为它拥有用于认证协议在其上运行的信道的正确安全信道密钥，其可以用做安全信道密钥的密钥证实。RP504验证绑定响应B_{res}*等于绑定响应B_{res}，接着可以成功确定认证，并且UE/OP_{1oc}502和RP504之间的信道是安全的。在524，RP504可以发送通知到UE/OP_{1oc}502，指示认证成功并且信道是安全的。

[0080] 如图5所示，可以使用TLS建立安全信道。UE/OP_{1oc}502和RP504可以在协议中包括密钥证实，其向RP504保证被认证(例如由OpenID认证)方还可以是先前建立的安全信道的端点。图5所示的示例实施方式可以包括使用OP_{1oc}作为用于密钥证实、安全信道建立以及认证的信任锚(anchor)。试图达到相同、类似安全而不使用OP_{1oc}(例如使用外部OP)的实施方式可以在RP504和网络OP之间发生额外通信步骤。图5所示的示例实施方式可以减轻中间人(MitM)攻击，例如MitM初始在安全(TLS)信道的建立将其自身建立例如为TLS中继的这种攻击。在此描述的实施方式可以使MitM被RP504显式地检测到。

[0081] 如果不期望使用认证断言的扩展字段，则XS可以用于密钥证实。例如UE/OP_{1oc}502可以导出签名密钥K_1'=g(K_1,XS)(未显示)，并且使用它来 签名认证断言。RP504可以做相同事情的来验证已签名的断言。一旦成功，RP504可以同时实现认证和用于安全信道的密钥证实。这可以达到减少语义成本，因为MitM的存在可以不再从认证的失败中可辨别。

[0082] 图5所示的实施方式可以与RP认证结合，例如在此描述的RP认证的实施方式。例如确保信道安全可以如图5所示协议中所示是单侧的。为了使其是双侧的，协议可以与RP认证协议结合，例如图2和图3所示的RP认证协议。为此，UE/OP_{1oc}502可以在认证断言消息中包括加密的质询值EK_1(RP_{Chv})。如果K_1从未泄露给MitM，则UE/OP_{1oc}502，一旦接收到包括RP质询值RP_{Chv}的通知，则可以假设有效的RP504已经成功执行了B_{res}的评价，并且因此MitM可以不存在。因此，如果RP504拥有正确的K_1，则它可以解密RP_{Chv}。

[0083] 在另一实施方式中，RP504可以知道绑定响应B_{res}。例如，B_{res}可以用来加密在通知中的RP质询值RP_{Chv}，通知在524返回到UE/OP_{1oc}502。UE/OP_{1oc}502可以使用K_1'，而不是例如K_0或来加密认证断言消息UE_{Assert}内的RP_{Chv}。接着如果RP504拥有从正确XS值导出的K_1'，则RP504可以提取RP_{Chv}。

[0084] 在此描述的认证和密钥协商协议可以包括用于阻止攻击，例如MitM攻击的各种实

施。一种提供这种保护的方式是建立安全信道，其可以被称为在认证流之前的外部信道，例如TLS隧道。认证可以在这个安全信道内执行。例如称为GBA_H的协议关于由TLS隧道建立的外部认证协议对于攻击是足够安全的。GBA_H可以包括认证程序，其例如基于在TLS上的HTTP摘要。GBA_H的一个示例实施方式显示在第三代合作伙伴计划(3GPP)技术规范(TS)号33.220中。

[0085] 图6显示了示出使用HTTP-SIP摘要的GBA_H协议的示例的消息流图。如图6所示，通信可以使用UE602、BSF604和/或HSS606被执行。在608，UE602可以与BSF604建立TLS隧道。UE602可以在610例如使用TLS隧道发送请求到BSF604。在610的请求包括授权头，授权头包括私用身份，如在612所示。BSF604和HSS606可以在614使用Zh参考点来交换认证信息。例如，如在616所示，Zh BSF604可以使用Zh参考点来从HSS606获取认证向量(AV)和/或用户简档(profile)信息。

[0086] 在618，BSF604可以发送认证质询(例如在HTTP401未授权响应中的认证质询)到UE602。如在620所示，在618的消息包括私用身份信息、子域(realm)、随机数、保护质量(qop)值、认证算法、域(domain)和/或不透明(opaque)。在示例实施方式中，这个信息可以被包括在消息的认证头中。私用身份信息可以包括网络用来识别用户的身份。这个私用身份可使网络能够获取用户简档和/或用于质询的认证向量。在示例实施方式中，子域、随机数、qop值、认证算法、域和/或不透明可以由IETF在RFC文档2617中阐述。在622，UE602可以计算认证响应。UE可以在624发送认证请求到BSF604。如在626所示，认证请求可以包括私用身份信息、子域，随机数、确认随机数(cnonce)、qop值、随机数计数、认证算法，摘要rui和不透明。在示例实施方式中，确认随机数、随机数计数和/或摘要uri可由IETF在RFC文档2617中阐述。在628，BSF604可以计算响应，并比较从UE602中接收的值与在BSF604的计算值。在630，BSF604可以发送消息(例如200OK消息)到UE602，向UE602证实认证成功。这个在630的消息可以包括绑定被信任的标识符(B_TID)和/或密钥Ks的生命时间(lifetime)，如在632所示。在示例实施方式中，B_TID和Ks生命时间可以在3GPP TS号33.220中阐述。在634，UE602和BSF604可以计算Ks_NAF。

[0087] 另一示例实施方式中可以包括TLS外部认证和在此描述的由GBA机制建立的认证之间的绑定。所建议的绑定解决方案可以例如通过UE602增加绑定响应B_{res}到在624的消息来制定。B_{res}可以以BSF604和UE602知道但 MitM不知道的方式依赖安全信道。B_{res}可以以与内部认证(例如AKA)响应类似(或甚至相同)的方式从安全信道导出，但它可以独立于该响应。例如，B_{res}可以不以公共、公知的方式从响应中导出，否则MitM能够用类似的方式导出B_{res}。如果存在MitM，BSF604可以使用来自安全信道BSF604-MitM的参数执行B_{res}的验证，该参数不同于安全信道602-MitM的那些参数。用于这个预先条件可以包括安全信道的唯一性，其可以由协议满足，例如TLS，其中BSF604和UE602可以能够在信道建立中引入它们自己选择的参数(例如随机数)。如果由MitM执行B_{res}的验证和/或重新计算，则B_{res}的验证和/或重新计算可能失败，因为MitM可能不知道如何导出可接受的B_{res}值，而由MitM重新计算GBA响应可能成功。在这种方式中，可以检测到MitM。

[0088] 在示例实施方式中，UE602可以采用TLS加密密钥并使用带有密钥的哈希函数(keyed hash function)H来哈希(hash)该密钥，其中该密钥取决于AKA认证质询。这可以由BSF604在618的消息中提出。例如AV可以合适地格式化并且代替AKA质询值直接供给GBA响

应计算算法。这可以减轻重放并可以绑定安全TLS信道608到GBA认证运行。

[0089] 根据示例实施方式，可以建立安全信道608到质询响应认证618-630的绑定。例如，UE可以在接收到认证质询620(如内部认证质询(inner_auth_challenge))之后，应用具有在608从TLS信道提取的TLS_key(TLS密钥)的摘要算法H(例如HMAC算法)以得到修改的质询*(challenge*)。例如这可以表示为H(TLS_key,inner_auth_challenge->)challenge*。用于TLS的密钥提取方法的示例实施方式由IETF在RFC文档5705中阐述。UE608可以在622计算对由BSF604提出的质询的响应，并且同时使用相同或类似的算法计算绑定响应B_{res}。例如这可以表示为AKA-RESPONSE(inner_auth_challenge)->response;AKA-RESPONSE(challenge*,IK)->B_{res}。UE可以在624将响应和B_{res}发回BSF604。

[0090] BSF604通过检查(check)UE602响应获得对绑定的保证。如果证实了响应，则BSF604知道在通信另一端的实体被认证。如果B_{res}也被证实，其中BSF604使用自己端的TSL密钥用于验证，则被认证的实体还可以是与BSF604具有TLS隧道的一个实体，否则怀疑是MitM。

[0091] 图7是使用SIP-Digest认证绑定TLS和GBA的示例呼叫流图。如图7所示，UE702可以通过发起与BSF704的TLS会话开启引导程序。UE702可以通过BSF704出具的证书来认证BSF704。BSF704在这点可以不要求来自UE702的认证。在708的TLS隧道建立之后，UE702可以在710发送请求消息(例如HTTP GET请求)到BSF704，该请求消息包括私用标识符(例如IP多媒体子系统私用标识符(IMPI))。BSF704可以在712从HSS706请求认证信息(例如AV)。在714，HSS706可以提供被请求的数据(例如包括AV)给BSF704。BSF704可以在716发送认证质询(例如在HTTP401未授权响应中)到UE702。认证质询可以包括认证头和/或随机生成的随机数。除了随机数，认证头还可以包括额外的参数，例如私用身份、子域、qop值、算法信息和/或域。

[0092] 当响应来自BSF704的质询时，如在718所指示，UE702可以生成随机的确认随机数，并且通过使用SIP摘要凭证来计算认证响应。UE702还可以例如使用TLS隧道会话密钥和会话密钥来生成消息认证码(MAC)值B_{res}。TLS隧道会话密钥和/或会话密钥可以例如包括完整性密钥(IK)或保密性密钥(CK)。在示例实施方式中，IK可以代替CK被使用，因为IK可以被指定用于完整性保护的目的。这些密钥可以根据从UE702接收的AV中取得的认证质询RAND来生成。这可以绑定TLS隧道认证与GBA协议。认证质询响应和B_{res}二者可以被输入授权头，并且在请求消息(例如HTTP GET请求消息)中被发送回BSF704(在720)。B_{res}可以用与认证响应相同的算 法来计算，然而它可以用如所述的不同输入参数来计算。

[0093] BSF704可以相对于自己期望的值B_{res}*来检查B_{res}。它可以这样做，因为它知道在计算B_{res}中使用的密钥以及期望的认证响应二者。如果接收到的B_{res}匹配B_{res}*，并且接收到的认证响应匹配它期望的值，则BSF704可以确定UE702是可信的并且由于根据两个比较匹配验证的绑定效果还可以向自己保证，以TLS隧道形成(formation)中认证的UE702是在协议的GBA方面认证的同一个UE702。BSF704可以在722生成引导密钥材料，例如GBA/GAA主会话密钥Ks的密钥生命时间和B-TID。在724，BSF704可以发送包括B-TID和密钥Ks的消息(例如200OK消息)到UE702。UE702和/或BSF704可以使用Ks导出引导密钥材料Ks_NAF。例如，在726，UE702可以根据Ks生成Ks_NAF。Ks_NAF可以用来使Ua参考点安全。

[0094] Ua参考点上用于安全性的应用特定密钥(UE702和网络认证功能(NAF)之间的)(未

示出)可以至少部分地从引导后的密钥经由GBA被导出。例如Ks_NAF可以从Ks=CK||IK导出，其中CK和IK是在714从HSS706传递给BSF704的AV的一部分。如果Ks_NAF从TLS隧道形成期间建立的Ks和主密钥导出Ks_NAF，则绑定可以仍然有效。因此，Ks_NAF可以在UE702和网络之间共享。它可以对任何MitM不可用。

[0095] 在此描述的实施方式可以实施在云计算情形中。根据示例实施方式，本地OpenID的特点和/或技术特征可以被结合来使从具有多租户(multi-tenant)能力的云能够从一个或多个私用设备访问。例如，可以结合本地OP认证、RP认证、秘密建立和/或注册过程。用于组织的计算资源的外包(outsourcing)的至少两个方面可以如在此所述地结合。在一个示例方面，远程、外部、移动和领域工人的现代劳动力等级可以鼓励组织为了工作利用工人的私用设备。在另一示例方面，信息和计算资源可以逐渐地外包到计算机云(例如多租户主基础设施和/或服务器)。在这个双重外包情形中的外包组织的安全要 求可以对为它的实施选择的安全架构设置约束。这些可以在保护目的和/或安全控制方面来描述，其例如可以用来保护组织的财产。

[0096] 用户设备可以认为是不安全的。即使公司数据的完全保护在设备上是不可能的，组织的数据可以尽可能地至少安全地位于云存储器中，例如来防止通过用户设备的数据丢失和/或泄露。做这个的一种方式是允许经由远程桌面应用接入云，远程桌面应用例如可以连接至云中的虚拟工作站。作为益处，这可以允许远程工人和/或虚拟工作站使用不同的操作系统(OS)。例如，用户设备可以是云行安卓(ANDOID)™或苹果(APPLE)®OS的平板电脑，并且可以例如经由某远程桌面协议(RDP)客户端应用连接到微软视窗(MICROSOFT WINDOWS)®虚拟机。用户认证可以通过在用户端的硬件保护措施而安全，例如其可以绑定到智能卡或其他被信任的环境。如在此所1的智能卡或其他被信任的环境被发布(issue)，其可以用本地OpenID使能而用于用户设备的用户。用户账户可以被注册以在如在此所述的智能卡或其他安全环境中使用。

[0097] 云主机可以提供一些安全控制和/或契约保障。使用云服务的组织可以在这样的多租户环境中进一步相对于数据丢失和/或泄漏建立独立的安全控制。作为示例，组织的IT部门可以为云工作站的(虚拟)硬盘驱动安装磁盘加密解决方案。

[0098] 云计算机上的磁盘加密提供的保护可能受到限制。云主机的管理程序(hypervisor)可以在虚拟工作站运行时具有完全的数据访问。当用户登录到工作站时，云主机的管理程序可以监听用来解密硬盘驱动的凭证。磁盘加密可以用一些方式绑定到主机硬件，例如使用基于被信任计算的虚拟支持技术。

[0099] 远程用户设备可以提交秘密数据，例如磁盘加密凭证(例如密码)，到云中的虚拟机。这样的数据可以保护以安全地到达目的地，并且它可以不被 用户知道。凭证可以秘密地存储在智能卡或以传输到指定虚拟机的方式用本地OpenID使能的其他被信任的环境。

[0100] 图8显示了示例通信系统的图，该通信系统实施本地认证实体和云/远程计算服务。如图8所示，在816，公司用户可以从公司814获得例如智能卡818，或其他被信任的环境。智能卡可以是本地OpenID使能的智能卡。智能卡818可以包括例如OP_{loc}。智能卡818可以包括凭证保险库(vault)用于私用访问公司814在其他地方具有的资源，例如在云主机虚拟机(VM)810。在812，公司814可以连接到云主机VM810并存储/上传用户设备802经由智能卡818访问的公司814信息、服务、文档等等。

[0101] 用户可以在820将智能卡818(例如用本地OpenID技术使能来执行OP_{loc}功能的智能卡)插入到用户设备802。用户设备802可以例如是平板电脑、智能电话、移动电话、笔记本电脑、或其他移动设备。用户设备802不要求是移动设备,而可以是其他任何计算设备,被配置成使用智能卡818或其他被信任的环境访问在云主机VM810上的服务。一些应用可以安装在用户设备802上,其可以包括例如远程桌面协议(RDP)客户端来访问在云主机VM810上的远程桌面。到远程桌面的登录可以通过基于网络的网关806中转,该网关806可以当做用于智能卡认证(例如OpenI认证)程序的RP。这个RP806可以驻留在云主机VM810中或可以是独立的实体。RP806可以被提供为到外包公司的安全服务,或者它可以被公司814本身操作。网关RP806可以在808具有到云主机VM810的安全、私用连接。

[0102] 基于本地OpenID的登录可以结合在此描述的至少三个安全特征的一个或多个。例如,基于本地OpenID的登录可以包括:(1)经由OP_{loc}的用户认证;(2)RP806(例如安全网关)到在智能卡818上的OP_{loc}的认证;和/或(3)私用秘密的建立、智能卡818和RP806之间的端到端和可选的进一步委托给云主机VM810。在智能卡818上经由OP_{loc}的用户认证可以包括通过拥有智能卡818和对认证秘密的知晓、以及生物测定用户认证的(至少)两因素(two-factor)认证。认证和/或秘密通信可以在804经由用户设备802和RP806之间安全通信被执行。RP806到智能卡818上的OP_{loc}的认证可以延伸到用户来确保用户连接到指定的公司资源并且非欺诈的站点。例如用于RP806认证的凭证可以被安全地包括在智能卡818中。RP806可以例如将用户设备802的秘密委托给云主机VM810,或作为两个安全信道的中间点。

[0103] 当在智能卡818上的OP_{loc}和RP806之间建立了秘密时,在智能卡818上的凭证保险库可以被解锁。用于在云主机VM810上的数据访问的凭证可以用建立的秘密(例如在卡上)加密和/或提交到云主机VM810。在云主机VM810,凭证可以被解密和验证,且如果验证成功,则秘密可以用来解密用户数据。用户可以经由远程桌面应用在云主机VM810上工作。用户可以例如经由从云主机VM810到公司内部网络的安全连接访问公司资源。

[0104] 图9显示了示例协议流,其使用了SIP摘要认证并包括OpenID中的RP904认证。认证可以包括使用RP904和OP908之间预先共享的密钥$K_{r,o}$的UE902到OP908的认证。而在OpenID认证中的RP认证可以从SIP摘要认证中被引导。图9所示的协议流包括UE902、RP904(例如应用服务器)、OP908(例如单点登录(SSO)服务器)和HSS910之间的通信。RP904和OP908可以在906具有预先建立的共享秘密$K_{r,o}$,其用于使实体之间的通信安全。

[0105] 在如图9所示的协议中,OpenID可以在自身无状态模式中用于UE902认证。步骤912到918的结合可以用于在OP908实现RP904认证。在912,UE902可以登记在网际协议(IP)多媒体子系统(IMS)中。UE902可以在914发送认证请求(例如OpenID认证请求)到RP904。认证请求可以包括认证标识符(例如OID)。RP904可以在916发送重定向请求到UE902。在916的重定向请求可以重定向UE902到OP908。重定向请求可以包括认 证标识符(例如OID)和/或对应于RP904的RP凭证RP_{Cred}。RP_{Cred}可以用与OP908共享的预先共享密钥$K_{r,o}$来签名。在918,UE902可以发送重定向请求消息到OP908。重定向请求消息可以包括在916接收到的认证标识符(例如OID)和/或RP凭证RP_{Cred}。

[0106] 在920,OP908可以使用RP_{Cred}执行RP904的认证,和/或生成RP认证断言。OP908还可以执行共享密钥K_0的检查,以确保UE902和OP908之间的安全通信,该密钥K_0是在UE902和OP908之间的共享密钥。在922,OP908可以确定RP904是否已经被认证。如果RP904在922未被

合适地认证，OP908可以在924发送警告到UE902，指示RP904是坏的RP，并且终止该过程。如果RP904在922被合适地认证，则OP908可以继续协议。在示例实施方式中，如果RP904在926被确定是可信的，则在920的RP904认证断言的生成可以发生。在示例实施方式中(图9中未示出)，如果在922的RP904认证决定被认为是OP908在其中作出关于RP认证决定的点，则RP_{Assert}使用可以在RP904认证决定之后的步骤中从协议中省略。

[0107] 在示例变型中，RP_{Cred}可以是RP904的简单文本标识符(即未用任何密钥签名)，其可以允许OP908选择用于将来使用的正确共享密钥$K_{r,o}$。在这种情况下，如果RP_{Cred}不对应OP908知道的任何RP，则OP908可以决定终止过程并通知902。

[0108] 继续图9所示的示例消息流，可以执行SIP摘要认证。例如，OP908可以在928从HSS910获得SIP摘要认证向量(SD-AV)和/或用户简档信息。OP908可以基于用户凭证(例如用户名/密码)获得这样的信息。OP908还可以从HSS910获得用户凭证、子域、qop值、认证算法和/或哈希H(A1)。在示例实施方式中，子域、qop值、认证算法和/或哈希H(A1)可以由IETF在RFC文档2069和2617中阐述。

[0109] 在930，OP908可以生成随机数并存储随机数和H(A1)。在932，OP908 可以发送认证质询(例如具有认证质询的HTTP401未授权消息)到UE902。认证质询可以包括用户凭证、随机数、子域、qop值和/或认证算法。在934，UE902可以生成确认随机数、H(A1)和/或与OP908共享用于安全通信的秘密密钥K_0。在936，UE902还可以计算质询响应并发送质询响应(例如具有认证响应的HTTP GET消息)到OP908。质询响应可以包括确认随机数、响应、随机数、用户凭证、子域、qop值、认证算法、摘要url、和/或随机数计数。在示例实施方式中，确认随机数、随机数、子域、qop值、认证算法、摘要url和/或随机数计数可以由IETF在RFC文档2617中阐述。共享密钥K_0可以从认证响应导出，该认证响应可以绑定共享密钥K_0到SIP摘要认证。在938，OP908可以检查随机数，计算X响应和/或比较该X响应与从UE902接收到的响应。

[0110] 如果SIP摘要认证成功(例如X响应或其中的某些参数匹配响应或其中的某些参数)，OP908可以在938生成UE认证断言UE_{Assert}和/或共享K_0。在940，OP908可以生成随机数1和/或K_1，其可以是UE902、OP908、和/或RP904之间的共享密钥，用来建立UE902和RP904之间的安全信道。K_1可以由OP908使用针对新鲜性生成中的随机数1生成。K_0可以用来加密随机数1和/或RP认证断言消息RP_{Assert}，其例如可以称为EK_0(随机数1，RP_{Assert})。用K_0加密可以使正确的、被认证的UE902获得RP_{Assert}，其可以是向UE902证实其正在与预期的、可信的RP904通信。OP908可以使用共享密钥$K_{r,o}$来加密密钥K_1和/或UE认证断言消息UE_{Assert}，其例如可以称为$EK_{r,o}$(K1，UE_{Assert})。在942，OP908可以发送重定向消息到UE902，其可以重定向UE902到RP904。重定向消息可以包括EK_0(随机数1，RP_{Assert})和/或$EK_{r,o}$(K1，UE_{Assert})。在示例实施方式中，如在944所示，RP认证断言消息RP_{Assert}可以在协议流中的某点成为废弃的，因为OP908可以是关于RP904可信赖性的决定点。当RP904执行与UE902的通信时，例如执行实 施特定步骤952和/或954，K_1可以被使用来保证UE902正在安全地与预期的RP904通信。

[0111] 在946，UE902可以使用K_0解密随机数1和/或RP认证断言消息RP_{Assert}。通过能够使用K_0解密RP认证断言消息RP_{Assert}，UE902可以证实它正在与预期的、可信的RP904通信。UE902可以获得RP认证断言消息RP_{Assert}和随机数1。UE902可以基于接收到的RP认证断言消息RP_{Assert}来认证RP904。UE902可以使用随机数1生成K_1。用共享密钥K_1加密可以使正确的、被认证的UE902获得UE_{Author}，其可以用作使用服务的访问令牌。在948，UE902可以被重定向到

RP904。在948，UE902可以发送密钥K_1和UE认证断言消息UE_{Assert}到RP904。密钥K_1和UE_{Assert}可以用共享密钥$K_{r,o}$加密，其例如可以称为$EK_{r,o}(K_1, UE_{Assert})$。这个加密可以之前已由OP908执行。在950，RP904可以使用$K_{r,o}$解密$EK_{r,o}(K_1, UE_{Assert})$并获得$UE_{Assert}$和$K_1$。用于UE902的信息可以在950被授权。例如，RP904可以使用K_1来验证UE_{Assert}的签名。在成功验证UE_{Assert}之后，RP904可以生成授权消息UE_{Author}，其例如可以使用密钥K_1加密并称为$EK_1(UE_{Author})$。UE_{Author}可以包括授权信息或授权参数，指示UE902被授权访问在RP904的一个或多个服务。RP904可以在952通知UE902关于UE902是否被授权用于在RP904的服务。例如，RP904可以发送UE认证参数或信息UE_{Author}。UE_{Author}可以用UE902和RP904之间共享的秘密密钥$K_1(EK_1(UE_{Author}))$加密。在954，UE902可以解密$EK_1(UE_{Author})$并使用UE_{Author}从RP90访问所请求的服务。步骤952和/或954可以是实施特定的步骤，其是可选的，并可以取决于UE902和/或RP904的服务实施。例如，这些可以特定于在认证之后给UE902提供普通服务访问的期望应用。如果没有使用这些步骤，则可以不需要K_1。

[0112] 在示例实施方式中，图9所示的协议流可以使用秘密$K_{r,o}$以实现RP904到OP908的认证。例如，如果秘密$K_{r,o}$没有用于签名到OP908的具有RP_{Cred} 的消息（例如在步骤912到918中），则秘密$K_{r,o}$可以被用于认证。例如，如果OP908和RP904已经共享秘密$K_{r,o}$，则这个秘密可以用于与OP908的RP904认证。认证协议（例如OpenId协议）的发现和（可选的）关联创建步骤未在图9所示的协议中示出。在UE902上的实施可以不受任何这样的RP904认证影响。例如，在一个实施方式中，UE902可以不包括OP_{Ioc}功能，以及因此可以不能够发送质询RP_{Chv}到RP。

[0113] 图10显示了具有RP1004到OP1008认证的示例协议的消息流图。在图10中，可以执行UE1002、RP1004（例如应用服务器）、OP1008（例如SSO服务器）和/或HSS1010之间的通信。RP1004和OP1008可以具有预先建立的共享秘密，如在1006所示，用于能够经由安全信道进行安全通信。

[0114] 如图10所示，UE1002可以在1012发布认证请求（例如OpenID认证请求）到RP1004，其包括登录标识符（例如，如URL或电子邮件地址的OpenID标识符）。RP1004可以在1014发现OP1008。在1016，RP1004可以发送关联请求（例如OpenID关联请求）到OP1008。RP1004和OP1008可以建立迪菲－赫尔曼密钥D-H。OP1008可以生成关联秘密和/或关联句柄，其可以一起被称为关联。在1018，OP1008可以向RP1004发送关联响应，其可以包括关联秘密和随机数0。关联秘密和/或随机数0可以用建立的D-H密钥加密。在1020，RP1004可以解密接收到的加密的随机数0和加密的关联秘密。RP1004可以接着用共享密钥$K_{r,o}$签名随机数0，共享密钥$K_{r,o}$可以是RP1004和OP1008之间共享的预先建立的密钥。HMAC或另一合适的对称签名算法可以被用来签名随机数0。RP1004和OP1008使用已知的机制，例如使用迪菲－赫尔曼密钥交换协议或预先共享的秘密，可以具有共享秘密$K_{r,o}$。利用这个共享的秘密，OP1008和RP1004可以签名消息并验证已用共享秘密$K_{r,o}$签名的各自的消息。

[0115] 在1022，RP1004可以使用重定向消息来重定向UE1002发送的认证请 求。重定向消息可以包括登录标识符（例如，OpenID标识符）、RP1004标识符（RP_{Cred}）和/或已签名的随机数0。例如，UE1002可以被重定向到OP1008。认证请求可以在1024被重定向到OP1008。重定向可以包括登录标识符（OpenID标识符）和/或RP_{Cred}。OP1006可以在1026强制用于与UE1002的通信的HTTPS的使用以用于安全通信。可以通过OP1002的网络服务器的配置（例如地址重写）来执行HTTPS的强制使用。在1028，OP1008可以验证随机数0的签名来认证RP1004。例如，

OP1008可以使用共享密钥$K_{r,o}$验证签名。步骤1028的RP1004认证可以在1030确定，如果它失败了，OP1008可以在1032发送警告消息到UE1002，例如其可以由HTTPS保护，用于指示RP1004认证失败。如果在步骤1028的RP1004认证成功，则协议流可以继续(例如在步骤1034)。

[0116] 在1034，OP1008可以确定OP1008和UE1002之间是否建立了安全信道。例如，OP1008可以确定是否存在有效的密钥K_0。如果有效的密钥K_0存在，则协议流可以前进到步骤1048，生成UE认证断言UE_{Assert}。如果有效的密钥K_0不存在，协议流可以继续执行UE1002的认证。在示例实施方式中，安全信道的建立(例如如图4所示)和UE1002的认证可以在相同协议流中被绑定一起。如在1036所示，OP1008可以发送认证请求到本地订阅服务器(HSS)1010，并且可以基于来自HSS1010用户凭证获得SIP摘要认证向量(SD-AV)和/或用户简档。SD-AV可以包括qop值、认证算法、子域和用户凭证、子域和密码的哈希，称为H(A1)。在多个HSS的环境中，OP1008可以通过询问服务层功能(SLF)获得HSS1010的地址，在该地址存储UE1002的订阅的详情。在1038，OP1008可以生成随机的随机数，可以存储哈希H(A1)和相对于用户凭证的随机数。OP1008可以在1040发送(例如在受保护的HTTPS消息中)认证质询消息(例如如SIP摘要认证质询的401认证质询)到UE1002，该消息可以包括随机数、子域、qop值、认证算法和/或用户凭证。

[0117] 一在1040收到质询，UE1002可以在1042生成随机的确认随机数和H(A1)。UE1002可以基于H(A1)、确认随机数和/或其他信息，例如认证质询中包括的材料，生成共享秘密K_0。共享秘密K_0可以是UE1002和OP1008之间的共享秘密，其可以使UE1002和OP1008之间的通信能够使用安全信道被传送。UE1002可以使用确认随机数和/或认证质询中提供的其他参数，例如随机数、用户凭证和/或qop值，来计算认证响应。在1044，UE1002可以发送质询响应(例如其可以是受保护的HTTPS消息)到OP1008。质询响应可以包括例如确认随机数、随机数、响应、子域、用户凭证、qop值、认证算法、随机数计数和/或摘要url。在1044一接收到响应，OP1008可以使用先前存储的随机数来检查包括在响应中的随机数。如果检查成功，OP1008可以使用先前存储的哈希H(A1)和随机数以及响应中包括的其他参数(例如确认随机数、随机数计数、qop值等等)来计算期望的响应(X响应)，并可以使用该X响应来检查从UE1002接收到的响应。如果检查成功，UE1002的认证可以被认为已经成功。如果检查不成功，认证可以被认为已经失败。如果UE1002被成功认证，则OP1008可以生成共享秘密K_0，其可以基于哈希H(A1)、确认随机数和/或其他信息，例如认证质询中包括的材料而被生成。可替换地或额外地，在1044一接收到响应，OP1008可以创建认证断言UE_{Assert}。UE_{Assert}可以所使用关联秘密来签名，该关联秘密例如可以是在1018的信息中使用的关联秘密。

[0118] 在1050，OP1008可以生成随机的随机数1和/或可以基于K_0和随机数1生成共享秘密K_1。共享秘密K_1可以是UE1002、OP1008和/或RP1004之间的共享秘密，用于建立UE1002和RP1004之间的安全信道。OP1008可以使用K_0加密随机数1，其例如可以称为EK_0(随机数1)，并可以使用$K_{r,o}$加密K_1和已签名的断言消息UE_{Assert}，其例如可以称为$EK_{r,o}$(K_1，已签 名的(UE_{Assert}))。OP1008可以在1052向UE1002发送消息(例如重定向消息)，其可以包括具有到RP1004的重定向的EK_0(随机数1)和/或$EK_{r,o}$(K_1，已签名的(UE_{Assert}))。在1054，UE1002可以使用共享密钥K_0解密EK_0(随机数1)，并可以得到随机数1。UE1002可以基于K_0和随机数1来生成共享秘密K_1。OP1008发送的消息可以在1056被重定向到RP1004。在1056的消息可以包括

$EK_{r,o}(K_1$，已签名的$UE_{Assert})$。在1058，RP1004可以解密$EK_{r,o}(K_1$，已签名的$(UE_{Assert}))$，并得到UE_{Assert}和K_1。RP1004可以使用与OP1008共享的关联秘密来验证断言消息UE_{Assert}的签名。在验证断言消息UE_{Assert}之后，RP1004可以生成用于UE1002授权消息。例如，RP1004可以生成授权信息UE_{Author}并使用K_1来加密UE_{Author}，其例如可以称为$EK_1(UE_{Author})$。RP1004可以在1060通知UE1002关于应用特定的授权信息，其可以被包括在这个消息中，用K_1来加密。UE1002可以在1062使用共享密钥K_1来解密$EK_1(UE_{Author})$并且之后可以访问被请求的服务。

[0119] 在图10中，授权信息或参数UE_{Author}可以特定于应用和/或特定于OP1008。如果UE_{Author}特定于OP1008，则UE_{Author}可以由K_0签名。如果授权信息或参数UE_{Author}可以特定于应用，则UE_{Author}可以由$K_{r,o}$或签名密钥S来签名。传输可与签名密钥S一起工作。

[0120] 在示例实施方式中，图10所示的协议流可以在如此所述的使用分割终端的情形下被实施。

[0121] 在另一示例实施方式中，RP1004认证可以被包括在OP1008和RP1004之间的质询响应步骤中，其中OP1008可以发送具有新鲜性证据的质询到RP1004(例如经由随机数)。RP1004可以使用预先建立的共享秘密$K_{r,o}$来签名这个随机数并返回答复到OP1008。对认证质询的响应可以作为对OP1008认证质询的直接响应，或可以被整合在重定向消息中，其从UE1002发送到OP1008。在任一情形下，OP1008可以具有对RP1004(例如参与 UE认证之前)的认证的可靠证据。这可以允许OP1008在RP1004认证失败的情况下停止协议，并可以在该RP1004认证失败的情况下节省UE1002和OP1008之间的通信努力。OP1008可以直接传送关于RP1004认证失败的信息到UE1002，例如在1032所示。

[0122] 如在此所述。关联可以用于RP1004认证。例如，如果RP1004建立与OP1008的关联，对应的步骤可以被修改来结合来自OP1008的质询。在关联建立期间，OP1008和RP1004可以建立MAC密钥，其可以用于签名认证断言消息。这个密钥可以使用临时秘密密钥被加密发送，临时秘密密钥可以例如使用迪菲－赫尔曼(DH)密钥在OP1008和RP1004之间被协商。除了临时秘密密钥，OP1008可以包括随机数，其在到RP1004的响应中也可以用DH密钥来加密。

[0123] RP1004可以基于协商的DH密钥来解密随机数和MAC密钥。RP1004可以使用它自己预先建立的共享密钥$K_{r,o}$来签名和加密从OP1008接收到的随机数，并且将其作为额外的参数加入到发送至UE1002的重定向消息中。由于UE1002遵循到OP1008的重定向，OP1008可以接收已签名或加密的随机数，并且可以使用共享密钥$K_{r,o}$来认证RP1004。在认证失败的情况下，OP1008可以发送警告消息到UE1002来保护它免受未认证RP的攻击。在RP1004认证成功的情况下，OP1002可以继续该协议。

[0124] 示例实施方式被描述用于使用针对RP1004认证的发现模式。例如，在OP1008和RP1004之间未建立关联的情况下(即OpenID中的无状态模式)，OP1008可以能够发送信息到RP1004。在无状态模式下，OP1008和RP1004之间的信息交换可以在发现期间发生。然而，发现可以或可以不包含OP1008，例如在委托发现的情况下。在委托发现中，用户标识符可以在，例如http://myblog.blog.com，并接着指向在OP1008的OP端点(例如在http://myblog.myopenid.com)。因此，OP1008(例如在myopenid.com)可以 不直接被包含在发现中，并且可以不能在这个阶段认证RP1004。OP1008可以能够在1016、1018的关联期间认证RP1004，代替在1028、1030确定认证，如图10所示。

[0125] 如果OP1008可以能够在发现步骤期间提供额外信息到RP1004(即用户标识符页托

管(host)在OP1008自身),OP1008可以动态地生成随机数作为发现信息页的一部分并将它与进行请求的RP1004的HTTP的标识符(例如URL或电子邮件地址)相关联。OP1008可以接着希望RP1004签名或加密这个随机数,并将信息包括在重定向消息中。

[0126] 如在此所述,OP1008可以保护OP1008和UE1002之间的通信。例如,如在1026所示,OP1008可以强制使用HTTPS(即UE1002可以由OP1008重定向到使用HTTPS使得UE1002和OP1008之间随后任意的通信受到保护)。例如,可以使用TLS。TLS可以通过强制UE1002动态地导入OP1008的证书,或使用预先安装的OP证书来工作。二者可以由BA相对于根证书(例如由根CA签名的)进行检查。这样的保护可以允许它例如在1040阻止对从OP1008到UE1002的认证质询消息的MitM攻击。此外,在RP1004认证失败的情况下,它可以允许OP1008以受保护的方式发送警告消息到UE1002。

[0127] 在此描述的实施方式可以用本地断言提供方实施。在此所述的是示例协议,其使RP认证与OpenID相协调并利用本地断言提供方。当RP和(网络侧)OP之间有联系(例如第一联系)时,所描述的实施方式可以基于RP和OP之间的预先建立的共享秘密$K_{r,o}$能够实现RP的认证。在OpenID的关联模式中,这是关联阶段。

[0128] 图11显示了用本地认证断言提供方的提供阶段的消息流图的示例实施方式。如图11所示,UE1102、RP1104、OP1106和/或HSS1108可以在用本地断言提供方的提供阶段中执行的通信中被实施。在提供阶段中的各个阶 段,随机数可以被实施用于重放保护。

[0129] 如图11所示,UE1102可以在1110提交登录标识符(例如OID)到RP1104。RP1104可以在1112发送关联请求(例如http POST OpenID关联请求)到OP1106。关联请求可以包括RP1104凭证RP_{Cred},其可以用RP1104和OP1106之间共享的共享密钥$K_{r,o}$加密。这个加密的RP_{Cred}可以例如称为$EK_{r,o}(RP_{Cred})$。RP凭证RP_{Cred}可以是包括预先共享秘密或标识符的普通类型的凭证。在1114,OP1106可以确定是否存在共享密钥K_0。如果存在共享密钥K_0,则OP1106可以继续认证阶段(AP)。如果不存在共享密钥K_0,则OP1106可以继续提供阶段。例如OP1106可以前进到步骤1116。

[0130] 在1116,OP1106可以执行与RP1104的关联。例如,OP1106可以生成关联句柄A和/或签名密钥S。签名密钥S可以从关联句柄A的函数中被生成。OP1106可以用$K_{r,o}$加密签名密钥S,其例如可以称为$EK_{r,o}(S)$。OP1106可以发送关联句柄A和/或加密的签名密钥S到RP1104。在1118,RP1104可以发送消息(例如重定向消息)到UE1102,该消息重定向UE1102到OP1106。在1118的消息可以包括参数,例如会话ID、返回URL、随机数、登录标识符(例如OID)和/或关联句柄A。在1120,UE1102可以发送包括从RP1104接收到的参数中的一个或多个的消息(例如http GET请求)到OP1106。例如,在1120的消息可以包括会话ID、返回URL、随机数、登录标识符(例如OID)和/或关联句柄A。

[0131] OP1106可以在1122得到来自HSS1108的SIP摘要认证向量(SD-AV)和/或其他信息。OP1106可以在1124发送认证质询到UE1102。UE1102可以在1126生成共享密钥K_0。UE1102还可以在1126计算认证响应和/或发送认证响应到OP1106。例如,认证响应可以由UE1102使用预先提供的用户凭证(例如用户名或密码)计算。在1128,OP1106可以例如通过比较接收到的响应和从认证向量SD-AV中计算的期望的响应来确认认证响应。一旦 用户/UE1102在OP1106被认证,OP1106可以生成共享密钥K_0,其可以在UE1102和OP1106之间共享。用K_0加密可以保证正确的、被认证的UE1102获得UE_{Author},UE_{Author}可以是用于后来使用服务的服务访

问令牌。在示例实施方式中，K_0可以是随机的数字并且可以使用加密函数来生成。

[0132] 在1130，OP1106可以签名指示用户/UE1102成功认证的认证断言消息UE_{Assert}。例如，OP1106可以使用签名密钥S来签名UE_{Assert}。已签名的UE_{Assert}可以称为$Sig_S(UE_{Assert})$。OP1106可以发送关联句柄A、已签名的断言UE_{Assert}和/或授权消息UE_{Author}到UE1102。已签名的断言UE_{Assert}可以用签名密钥S来加密，其例如可以称为$E_S(Sig_S(UE_{Assert}))$。授权消息UE_{Author}可以使用K_0来加密，其例如可以称为$EK_0(UE_{Author})$。在示例实施方式中，代替加密和签名认证断言消息UEAssert，使用签名密钥S来简单地签名认证断言消息就足够了。关联句柄A、UE_{Assert}和/或UE_{Author}可以在1132在重定向消息中被发送，重定向消息可以重定向UE1102到RP1104。在1134，UE1102可以发送消息(例如http GET请求)到RP1104，该消息可以包括关联句柄、$E_S(Sig_S(UE_{Assert}))$和/和$EK_0(UE_{Author})$。在1136，RP1104可以解密签名密钥S，解密已签名的断言$Sig_S(UE_{Assert})$，使用S验证断言(例如OpenID断言)，和/或解密被加密的授权消息$EK_0(UE_{Author})$。RP1104可以在1138发送包括$EK_0(UE_{Author})$的通知到UE1102。$EK_0(UE_{Author})$可以向指示UE1102指示RP1104已经被验证为合适的RP，并且不是流氓RP或其他MitM，因为通知可以包括流氓RP或其他MitM不能够解密的$EK_0(UE_{Author})$。

[0133] 图11所示的RP认证可以类似地实施在在此所述的其他实施方式中。例如，图11所示的认证实施可以在图2中认证阶段类似地实施。

[0134] 图12显示了根据在此描述的实施方式的用本地断言提供方的示例认证阶段的消息流图。如图12所示，认证阶段可以包括UE1202、RP1204、OP1206和/或HSS1208之间的通信。在示例实施方式中，UE1202可以包括本 地OP功能OP_{loc}，用于执行本地认证和认证断言(例如OpenID认证断言)签名，而OP1206可以是外部OP，其例如可以位于网路。UE1202可以在1210发送登录标识符(例如OID)到RP1204。在1212，RP1204可以发送关联请求消息(例如http POST OpenID关联请求)到OP1206。关联请求消息可以包括对应于RP1204的RP凭证RP_{Cred}。RP_{Cred}可以用共享密钥$K_{r,o}$加密，共享密钥$K_{r,o}$在RP1204和OP1206之间共享。

[0135] 在1214，OP1206可以确定是否已经提供共享密钥K_0，该共享密钥K_0在UE1202和OP1206和之间共享用于这些实体之间的安全通信。如果未提供共享密钥K_0，则协议可以继续提供阶段来提供共享密钥K_0。如果共享密钥K_0已经提供，则协议可以继续认证阶段。在示例实施方式中，OP1206可以不确定是否提供了共享密钥K_0，并且协议流可以在没有该确定的情况下而继续。

[0136] 在1216，OP1206可以执行与RP1204的关联。例如，OP1206可以生成关联句柄A和/或共享密钥K_1。共享密钥K_1可以从例如共享密钥K_0和关联句柄的函数中导出。共享密钥K_1可以用共享密钥$K_{r,o}$来加密，其例如可以称为$EK_{r,o}(K_1)$。关联句柄A和被加密的密钥K_1可以被发送到RP1204。RP1204可以在1218发送消息到UE1202，该消息包括参数，例如会话ID、返回URL、随机数、登录标识符(例如OID)和/或关联句柄A。在1218的消息可以是重定向消息，其重定向UE1202到在UE1202上的OP_{loc}(未示出)以用于认证。在1220，UE1202可以执行本地认证。UE1202可以在1220使用共享密钥K_0和关联句柄的函数来生成共享密钥K_1。用K_0加密可以保证正确的、被认证的UE1202获得UE_{Author}，UE_{Author}可以是用于后来使用服务的服务访问令牌。UE1202可以用共享密钥K_1签名认证断言消息UE_{Assert}，其可以称为$SigK_1(UE_{Assert})$。UE1202可以生成授权信息或参数UE_{Assert}(例如使用在UE1202上的本地OP)。UE1202可以用共享密钥K_0来加密 UE_{Author}，其例如可以称为$EK_0(UE_{Author})$。UE1202可以用共享密钥K_1加密$SigK_1$

(UE_{Assert})和/或$EK_0(UE_{Author})$，其可以称为$EK_1(SigK_1(UE_{Assert}),EK_0(UE_{Author}))$，并且发送关联句柄A和$EK_1(SigK_1(UE_{Assert}),EK_0(UE_{Author}))$到RP1204。如在1222所示，UE1202可以发送具有已签名的断言UE_{Assert}的消息(http GET请求)到RP1204。

[0137] RP1204可以在1224使用共享密钥$K_{r,o}$解密K_1。RP1204可以解密$SigK_1(UE_{Assert})$并可以使用K_1验证认证断言消息UE_{Assert}。在1224，RP1204可以使用K_1解密$EK_0(UE_{Author})$。RP1204可以不能解密UE_{Author}，因为UE_{Author}可以由UE1202和OP1206之间共享的共享密钥K_0加密。在1226，RP1204可以发送通知到UE1202，指示RP1204是UE1202使用K_1建立的安全信道所至的合适RP，而不是流氓RP或其他MitM，因为通知可以包括流氓RP或其他MitM将不能够解密的信息$EK_0(UE_{Author})$。

[0138] 图13A-图13E显示了可以在执行这里所述的实施方式中实施的示例网络系统和设备。图13A是在其中可以实施一个或多个实施方式的示例通信系统1300的系统图。通信系统1300可以是向多个用户提供内容，例如语音、数据、视频、消息发送、广播等的多接入系统。通信系统1300可以使多个无线用户通过系统资源共享(包括无线带宽)访问这些内容。例如，通信系统1300可以使用一种或多种信道接入方法，例如码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)、正交FDMA(OFDMA)、单载波FMDA(SC-FDMA)等。

[0139] 如图13A所示，通信系统1300可以包括无线发射/接收单元(WTRU)1302a、1302b、1302c、1302d，无线电接入网(RAN)1304，核心网1306，公共交换电话网(PSTN)1308、因特网1310和其他网络1312。不过应该理解的是，公开的实施方式考虑到了任何数量的WTRU、基站、网络和/或网络元件。WTRU1302a、1302b、1302c、1302d的每一个可以是配置为在无 线环境中进行操作和/或通信的任何类型的设备。作为示例，可以将WTRU1302a、1302b、1302c、1302d配置为发送和/或接收无线信号，并可以包括用户设备(UE)、基站、固定或者移动用户单元、寻呼器、蜂窝电话、个人数字助理(PDA)、智能电话、笔记本电脑、上网本、个人计算机、无线传感器、消费电子产品等等。

[0140] 通信系统1300还可以包括基站1314a和基站1314b。基站1314a、1314b的每一个都可以是配置为与WTRU1302a、1302b、1302c、1302d中的至少一个无线对接以便于接入一个或者多个通信网络，例如核心网1306、因特网1310和/或网络1312的任何设备类型。作为示例，基站1314a、1314b可以是基站收发信台(BTS)、节点B、演进的节点B(e节点B)、家庭节点B、家庭e节点B、站点控制器、接入点(AP)、无线路由器等等。虽然基站1314a、1314b的每一个被描述为单独的元件，但是应该理解的是，基站1314a、1314b可以包括任何数量互连的基站和/或网络元件。

[0141] 基站1314a可以是RAN1304的一部分，RAN1304还可以包括其他基站和/或网络元件(未显示)，例如基站控制器(BSC)、无线电网络控制器(RNC)、中继节点等。可以将基站1314a和/或基站1314b配置为在特定地理区域之内发送和/或接收无线信号，该区域可以被称为小区(未显示)。小区还可以被划分为小区扇区。例如，与基站1314a关联的小区可以划分为三个扇区。因此，在一种实施方式中，基站1314a可以包括三个收发信机，即每一个用于小区的一个扇区。在另一种实施方式中，基站1314a可以使用多输入多输出(MIMO)技术，因此可以将多个收发信机用于小区的每一个扇区。

[0142] 基站1314a、1314b可以通过空中接口1316与WTRU1302a、1302b、1302c、1302d中的一个或者多个通信，该空中接口1316可以是任何合适的无线通信链路(例如，射频(RF)、微

波、红外(IR)、紫外线(UV)、可见 光等)。可以使用任何合适的无线电接入技术(RAT)来建立空中接口1316。

[0143] 更具体地,如上所述,通信系统1300可以是多接入系统,并可以使用一种或者多种信道接入方案,例如CDMA、TDMA、FDMA、OFDMA、SC-FDMA等等。例如,RAN1304中的基站1314a和WTRU1302a、1302b、1302c可以使用例如通用移动电信系统(UMTS)陆地无线电接入(UTRA)的无线电技术,其可以使用宽带CDMA(WCDMA)来建立空中接口1316。WCDMA可以包括例如高速分组接入(HSPA)和/或演进的HSPA(HSPA+)的通信协议。HSPA可以包括高速下行链路分组接入(HSDPA)和/或高速上行链路分组接入(HSUPA)。

[0144] 在另一种实施方式中,基站1314a和WTRU1302a、1302b、1302c可以使用例如演进的UMTS陆地无线电接入(E-UTRA)的无线电技术,其可以使用长期演进(LTE)和/或高级LTE(LTE-A)来建立空中接口1316。

[0145] 在其他实施方式中,基站1314a和WTRU1302a、1302b、1302c可以使用例如IEEE802.16(即,全球微波接入互操作性(WiMAX))、CDMA2000、CDMA20001X、CDMA2000EV-DO、暂行标准2000(IS-2000)、暂行标准95(IS-95)、暂行标准856(IS-856)、全球移动通信系统(GSM)、GSM演进的增强型数据速率(EDGE)、GSM EDGE(GERAN)等等的无线电技术。

[0146] 图13A中的基站1314b可以是无线路由器、家庭节点B、家庭e节点B或者接入点,例如,并且可以使用任何适当的RAT以方便局部区域中的无线连接,例如商业场所、住宅、车辆、校园等等。在一种实施方式中,基站1314b和WTRU1302c、1302d可以实施例如IEEE802.11的无线电技术来建立无线局域网(WLAN)。在另一种实施方式中,基站1314b和WTRU1302c、1302d可以使用例如IEEE802.15的无线电技术来建立无线个域网(WPAN)。在另一种实施方式中,基站1314b和WTRU1302c、1302d可以使用基于蜂窝的RAT(例如,WCDMA,CDMA2000,GSM,LTE,LTE-A等)来建立 微微小区或毫微微小区。如图13A所示,基站1314b可以具有到因特网1310的直接连接。因此,基站1314b可以不需要经由核心网1306而接入到因特网1310。

[0147] RAN1304可以与核心网1306通信,所述核心网1306可以是被配置为向WTRU1302a、1302b、1302c、1302d中的一个或多个提供语音、数据、应用和/或基于网际协议的语音(VoIP)服务等的任何类型的网络。例如,核心网1306可以提供呼叫控制、计费服务、基于移动位置的服务、预付费呼叫、因特网连接、视频分配等和/或执行高级安全功能,例如用户认证。虽然图13A中未示出,应该理解的是,RAN1304和/或核心网1306可以与使用和RAN1304相同的RAT或不同RAT的其他RAN进行直接或间接的通信。例如,除了连接到正在使用E-UTRA无线电技术的RAN1304之外,核心网1306还可以与使用GSM无线电技术的另一个RAN(未示出)通信。

[0148] 核心网1306还可以充当WTRU1302a、1302b、1302c、1302d接入到PSTN1308、因特网1310和/或其他网络1312的网关。PSTN1308可以包括提供普通老式电话服务(POTS)的电路交换电话网络。因特网1310可以包括使用公共通信协议的互联计算机网络和设备的全球系统,所述协议例如有TCP/IP网际协议组中的传输控制协议(TCP)、用户数据报协议(UDP)和网际协议(IP)。网络1312可以包括被其他服务提供方拥有和/或运营的有线或无线的通信网络。例如,网络1312可以包括连接到一个或多个RAN的另一个核心网,该RAN可以使用和RAN1304相同的RAT或不同的RAT。

[0149] 通信系统1300中的WTRU1302a、1302b、1302c、1302d的某些或全部可以包括多模式

能力，即WTRU1302a、1302b、1302c、1302d可以包括用于在不同无线链路上与不同无线网络进行通信的多个收发信机。例如，图13A中示出的WTRU1302c可被配置为与基站1314a通信，所述基站1314a可以使用基于蜂窝的无线电技术，以及与基站1314b通信，所述基站1314b可以使用IEEE802无线电技术。

[0150] 图13B是WTRU1302示例的系统图。如图13B所示，WTRU1302可以包括处理器1318、收发信机1320、发射/接收元件1322、扬声器/麦克风1324、键盘1326、显示器/触摸板1328、不可移动存储器1330、可移动存储器1332、电源1334、全球定位系统(GPS)芯片组1336和其他外围设备1338。应该理解的是，WTRU1302可以在保持与实施方式一致时，包括前述元件的任何子组合。

[0151] 处理器1318可以是通用处理器、专用处理器、常规处理器、数字信号处理器(DSP)、多个微处理器、与DSP核相关联的一个或多个微处理器、控制器、微控制器、专用集成电路(ASIC)、场可编程门阵列(FPGA)电路、任何其他类型的集成电路(IC)、状态机等等。处理器1318可执行信号编码、数据处理、功率控制、输入/输出处理和/或使WTRU1302运行于无线环境中的任何其他功能。处理器1318可以耦合到收发信机1320，所述收发信机1320可耦合到发射/接收元件1322。虽然图13B描述了处理器1318和收发信机1320是单独的部件，但是应该理解的是，处理器1318和收发信机1320可以一起集成在电子封装或芯片中。

[0152] 发射/接收元件1322可以被配置为通过空中接口1316将信号发送到基站(例如，基站1314a)，或从基站(例如，基站1314a)接收信号。例如，在一种实施方式中，发射/接收元件1322可以是被配置为发送和/或接收RF信号的天线。在另一种实施方式中，发射/接收元件1322可以是被配置为发送和/或接收例如IR、UV或可见光信号的发射器/检测器。在另一种实施方式中，发射/接收元件1322可以被配置为发送和接收RF和光信号两者。应当理解，发射/接收元件1322可以被配置为发送和/或接收无线信号的任何组合。

[0153] 另外，虽然发射/接收元件1322在图13B中描述为单独的元件，但是 WTRU1302可以包括任意数量的发射/接收元件1322。更具体的，WTRU1302可以使用例如MIMO技术。因此，在一种实施方式中，WTRU1302可以包括用于通过空中接口1316发送和接收无线信号的两个或更多个发射/接收元件1322(例如，多个天线)。

[0154] 收发信机1320可以被配置为调制要由发射/接收元件1322发送的信号和/或解调由发射/接收元件1322接收的信号。如上面提到的，WTRU1302可以具有多模式能力。因此收发信机1320可以包括使WTRU1302经由多个例如UTRA和IEEE802.11的RAT通信的多个收发信机。

[0155] WTRU1302的处理器1318可以耦合到下述设备，并且可以从下述设备中接收用户输入数据：扬声器/麦克风1324、键盘1326和/或显示器/触摸板1328(例如，液晶显示器(LCD)显示单元或有机发光二极管(OLED)显示单元)。处理器1318还可以输出用户数据到扬声器/麦克风1324、键盘1326和/或显示/触摸板1328。另外，处理器1318可以从任何类型的适当的存储器访问信息，并且可以存储数据到任何类型的适当的存储器中，例如不可移动存储器1330和/或可移动存储器1332。不可移动存储器1330可以包括随机存取存储器(RAM)、只读存储器(ROM)、硬盘或任何其他类型的存储器设备。可移动存储器1332可以包括GSM用户标识模块(SIM)卡、UICC(SIM卡的UMTS版本)、记忆棒、安全数字(SD)存储卡等等。在其他实施方式中，处理器1318可以从在物理位置上没有位于WTRU1302上，例如位于服务器或家用计

算机(未示出)上的存储器访问信息,并且可以将数据存储在该存储器中。

[0156] 处理器1318可以从电源1334接收电能,并且可以被配置为分配和/或控制到WTRU1302中的其他部件的电能。电源1334可以是给WTRU1302供电的任何适当的设备。例如,电源1334可以包括一个或多个干电池(例如,镍镉(NiCd)、镍锌(NiZn)、镍氢(NiMH)、锂离子(Li-ion)等等), 太阳能电池,燃料电池等等。

[0157] 处理器1318还可以耦合到GPS芯片组1336,所述GPS芯片组1336可以被配置为提供关于WTRU1302当前位置的位置信息(例如,经度和纬度)。另外,除来自GPS芯片组1336的信息或作为其替代,WTRU1302可以通过空中接口1316从基站(例如,基站1314a、1314b)接收位置信息和/或基于从两个或更多个邻近基站接收的信号的定时来确定其位置。应当理解,WTRU1302在保持实施方式的一致性时,可以通过任何适当的位置确定方法获得位置信息。

[0158] 处理器1318可以进一步耦合到其他外围设备1338,所述外围设备1338可以包括一个或多个提供附加特性、功能和/或有线或无线连接的软件和/或硬件模块。例如,外围设备1338可以包括加速计、电子罗盘、卫星收发信机、数字相机(用于照片或视频)、通用串行总线(USB)端口、振动设备、电视收发信机、免提耳机、蓝牙(Bluetooth®)模块、调频(FM)无线电单元、数字音乐播放器、媒体播放器、视频游戏机模块、因特网浏览器等等。

[0159] 图13C是根据实施方式的RAN1304和核心网1306的系统图。如上面提到的,RAN1304可使用UTRA无线电技术通过空中接口1316与WTRU1302a、1302b和1302c通信。RAN1304还可以与核心网1306通信。如图13C所示,RAN1304可以包括节点B1340a、1340b、1340c,节点B1340a、1340b、1340c的每一个包括一个或多个用于通过空中接口1316与WTRU1302a、1302b、1302c、1302d通信的收发信机。节点B1340a、1340b、1340c的每一个可以与RAN1304内的特定小区(未显示)关联。RAN1304还可以包括RNC1342a、1342b。应当理解的是,RAN1304在保持实施方式的一致性时,可以包括任意数量的节点B和RNC。

[0160] 如图13C所示,节点B1340a、1340b可以与RNC1342a通信。此外,节点B1340c可以与RNC1342b通信。节点B1340a、1340b可以经由Iub 接口分别与RNC1342a、1342b通信。RNC1342a、1342b可以经由Iur接口相互通信。RNC1342a、1342b的每一个可以被配置以控制其连接的各个节点B1340a、1340b、1340c。另外,RNC1342a、1342b的每一个可以被配置以执行或支持其他功能,例如外环功率控制、负载控制、准入控制、分组调度、切换控制、宏分集、安全功能、数据加密等等。

[0161] 图13C中所示的核心网1306可以包括媒体网关(MGW)1344、移动交换中心(MSC)1364、服务GPRS支持节点(SGSN)1348、和/或网关GPRS支持节点(GGSN)1350。尽管前述元件的每一个被描述为核心网1306的部分,应当理解的是,这些元件中的任何一个可以被不是核心网运营商的实体拥有或运营。

[0162] RAN1304中的RNC1342a可以经由IuCS接口连接至核心网1306中的MSC1346。MSC1346可以连接至MGW1344。MSC1364和MGW1344可以向WTRU1302a、1302b、1302c提供到电路交换网络(例如PSTN1308)的接入,以便于WTRU1302a、1302b、1302c和传统陆地线路通信设备之间的通信。

[0163] RAN1304中RNC1342a还可以经由IuPS接口连接至核心网1306中的SGSN1348。SGSN1378可以连接至GGSN1350。SGSN1334和GGSN1350可以向WTRU1302a、1302b、1302c提供到分组交换网络(例如因特网1310)的接入,以便于WTRU1302a、1302b、1302c和IP使能设备

之间的通信。

[0164] 如上所述，核心网1306还可以连接至网络1312，网络1312可以包括由其他服务提供方拥有或运营的其他有线或无线网络。

[0165] 图13D是根据实施方式的RAN1304和核心网1306的系统图。如上面提到的，RAN1304可使用E-UTRA无线电技术通过空中接口1316与WTRU1302a、1302b、1302c通信。RAN1304还可以与核心网1306通信。

[0166] RAN1304可包括e节点B1340a、1340b、1340c，但可以理解的是，RAN1304可以包括任意数量的e节点B而保持与各种实施方式的一致性。eNB1340a、1340b、1340c的每一个可包括一个或多个用于通过空中接口1316与WTRU1302a、1302b、1302c通信的收发信机。在一种实施方式中，e节点B1340a、1340b、1340c可以使用MIMO技术。因此，e节点B1340a例如可以使用多个天线来向WTRU1302a发送无线信号和/或从其接收无线信号。

[0167] e节点B1340a、1340b、1340c的每一个可以与特定小区关联(未显示)，并可以被配置为处理无线资源管理决策、切换决策、在上行链路和/或下行链路中的用户调度等等。如图13D所示，e节点B1340a、1340b、1340c可以通过X2接口相互通信。

[0168] 图13D中所示的核心网1306可以包括移动性管理实体(MME)1360、服务网关1362和/或分组数据网络(PDN)网关1364。虽然前述单元的每一个被描述为核心网1306的一部分，应当理解的是，这些单元中的任意一个可以由除了核心网运营商之外的实体拥有和/或运营。

[0169] MME1360可以经由S1接口连接到RAN1304中的e节点B1340a、1340b、1340c的每一个，并可以作为控制节点。例如，MME1342可以负责WTRU1302a、1302b、1302c的用户认证、承载激活/去激活、在WTRU1302a、1302b、1302c的初始附着期间选择特定服务网关等等。MME1360还可以提供控制平面功能，用于在RAN1304和使用例如GSM或者WCDMA的其他无线电技术的其他RAN(未显示)之间切换。

[0170] 服务网关1362可以经由S1接口连接到RAN1304中的eNB1340a、1340b、1340c的每一个。服务网关1344通常可以向/从WTRU1302a、1302b、1302c路由和转发用户数据分组。服务网关1362还可以执行其他功能，例如在eNB间切换期间锚定用户平面、当下行链路数据对于WTRU1302a、1302b、1302c可用时触发寻呼、管理和存储WTRU1302a、1302b、1302c 的上下文(context)等等。

[0171] 服务网关1362还可以连接到PDN网关1364，PDN网关1364可以向WTRU1302a、1302b、1302c提供到分组交换网络(例如因特网1310)的接入，以便于WTRU1302a、1302b、1302c与IP使能设备之间的通信。

[0172] 核心网1306可以便于与其他网络的通信。例如，核心网1306可以向WTRU1302a、1302b、1302c提供到电路交换网络(例如PSTN1308)的接入，以便于WTRU1302a、1302b、1302c与传统陆地线路通信设备之间的通信。例如，核心网1306可以包括IP网关(例如IP多媒体子系统(IMS)服务器)，或者与之通信，该IP网关作为核心网1306与PSTN1308之间的接口。另外，核心网1306可以向WTRU1302a、1302b、1302c提供到网络1312的接入，该网络1312可以包括被其他服务提供方拥有和/或运营的其他有线或无线网络。

[0173] 图13E是根据实施方式的RAN1304和核心网1306的系统图。RAN1304可以是使用IEEE802.16无线电技术通过空中接口1316与WTRU1302a、1302b、1302c进行通信的接入服务

网络(ASN)。如下面进一步讨论的,WTRU1302a、1302b、1302c,RAN1304和核心网1306的不同功能实体之间的链路可以被定义为参考点。

[0174] 如图13E所示,RAN1304可以包括基站1340a、1340b、1340c和ASN网关1370,但应当理解的是,RAN1304可以包括任意数量的基站和ASN网关而与实施方式保持一致。基站1340a、1340b、1340c的每一个可以与RAN1304中特定小区(未示出)关联并可以包括一个或多个通过空中接口1316与WTRU1302a、1302b、1302c通信的收发信机。在一个示例中,基站1340a、1340b、1340c可以使用MIMO技术。因此,基站1340a例如使用多个天线来向WTRU1302a发送无线信号,或从其接收无线信号。基站1340a、1340b、1340c可以提供移动性管理功能,例如切换(handoff)触发、隧道建立、无线电资源管理、业务分类、服务质量策略执行等等。ASN网关1370可以充当业务聚集点,并且负责寻呼、缓存用户资料(profile)、路由到核心网1306等等。

[0175] WTRU1302a、1302b、1302c和RAN1304之间的空中接口1316可以被定义为使用802.16规范的R1参考点。另外,WTRU1302a、1302b、1302c的每一个可以与核心网1306建立逻辑接口(未显示)。WTRU1302a、1302b、1302c和核心网1306之间的逻辑接口可以定义为R2参考点,其可以用于认证、授权、IP主机(host)配置管理和/或移动性管理。

[0176] 基站1340a、1340b、1340c的每一个之间的通信链路可以定义为包括便于WTRU切换和基站间转移数据的协议的R8参考点。基站1340a、1340b、1340c和ASN网关1370之间的通信链路可以定义为R6参考点。R6参考点可以包括用于促进基于与WTRU1302a、1302b、1302c的每一个关联的移动性事件的移动性管理的协议。

[0177] 如图13E所示,RAN1304可以连接至核心网1306。RAN1304和核心网1306之间的通信链路可以定义为包括例如便于数据转移和移动性管理能力的协议的R3参考点。核心网1306可以包括移动IP本地代理(MIP-HA)1372,认证、授权、记账(AAA)服务器1374和网关1376。尽管前述的每个元件被描述为核心网1306的部分,应当理解的是,这些元件中的任意一个可以由不是核心网运营商的实体拥有或运营。

[0178] MIP-HA1372可以负责IP地址管理,并可以使WTRU1302a、1302b、1302c在不同ASN和/或不同核心网之间漫游。MIP-HA1372可以向WTRU1302a、1302b、1302c提供分组交换网络(例如因特网1310)的接入,以促进WTRU1302a、1302b、1302c和IP使能设备之间的通信。AAA服务器1374可以负责用户认证和支持用户服务。网关1376可促进与其他网络互通。例如,网关1376可以向WTRU1302a、1302b、1302c提供电路交换网络(例 如PSTN1308)的接入,以促进WTRU1302a、1302b、1302c和传统陆地线路通信设备之间的通信。此外,网关1376可以向WTRU1302a、1302b、1302c提供网络1312,其可以包括由其他服务提供方拥有或运营的其他有线或无线网络。

[0179] 尽管未在图13E中显示,应当理解的是,RAN1304可以连接至其他ASN,并且核心网1306可以连接至其他核心网。RAN1304和其他ASN之间的通信链路可以定义为R4参考点,其可以包括协调RAN1304和其他ASN之间的WTRU1302a、1302b、1302c的移动性的协议。核心网1306和其他核心网之间的通信链路可以定义为R5参考点,其可以包括促进本地核心网和被访问核心网之间的互通的协议。

[0180] 这里描述的方法可以用计算机程序、软件或固件实现,其包含到由计算机或处理器执行的计算机可读介质中。计算机可读介质的示例包括电子信号(通过有线或者无线连

接发送的)和计算机可读存储介质。计算机可读存储介质的示例包括但不限制为只读存储器(ROM)、随机存取存储器(RAM)、寄存器、缓冲存储器、半导体存储器设备、如内部硬盘和可移动磁盘的磁性介质,磁光介质和光介质,如CD-ROM盘的和数字通用盘(DVD)。与软件相关联的处理器用于实现在WTRU、UE、终端、基站、RNC或任何主计算机中使用的射频收发信机。

[0181] 虽然上述的特征和元素以特定的组合描述,每个特征或元素可以单独使用和与其他特征和元素结合使用。例如,在此描述的协议流步骤不局限于它们被描述的顺序。此外,虽然在此描述的实施方式可以使用OpenID认证描述,但是可以实施其他形式的认证。类似地,在此描述的实施方式可以不局限于OpenID通信或实体。例如RP可以包括任何服务提供方,OP/OPSF可以包括任何身份和/或断言提供方,和/或OP_{loc}可以是任何本地身份和/或断言提供方。而且,在此描述的任何UE的认证可以包括UE的认证,和/或与UE关联的用户的认证。

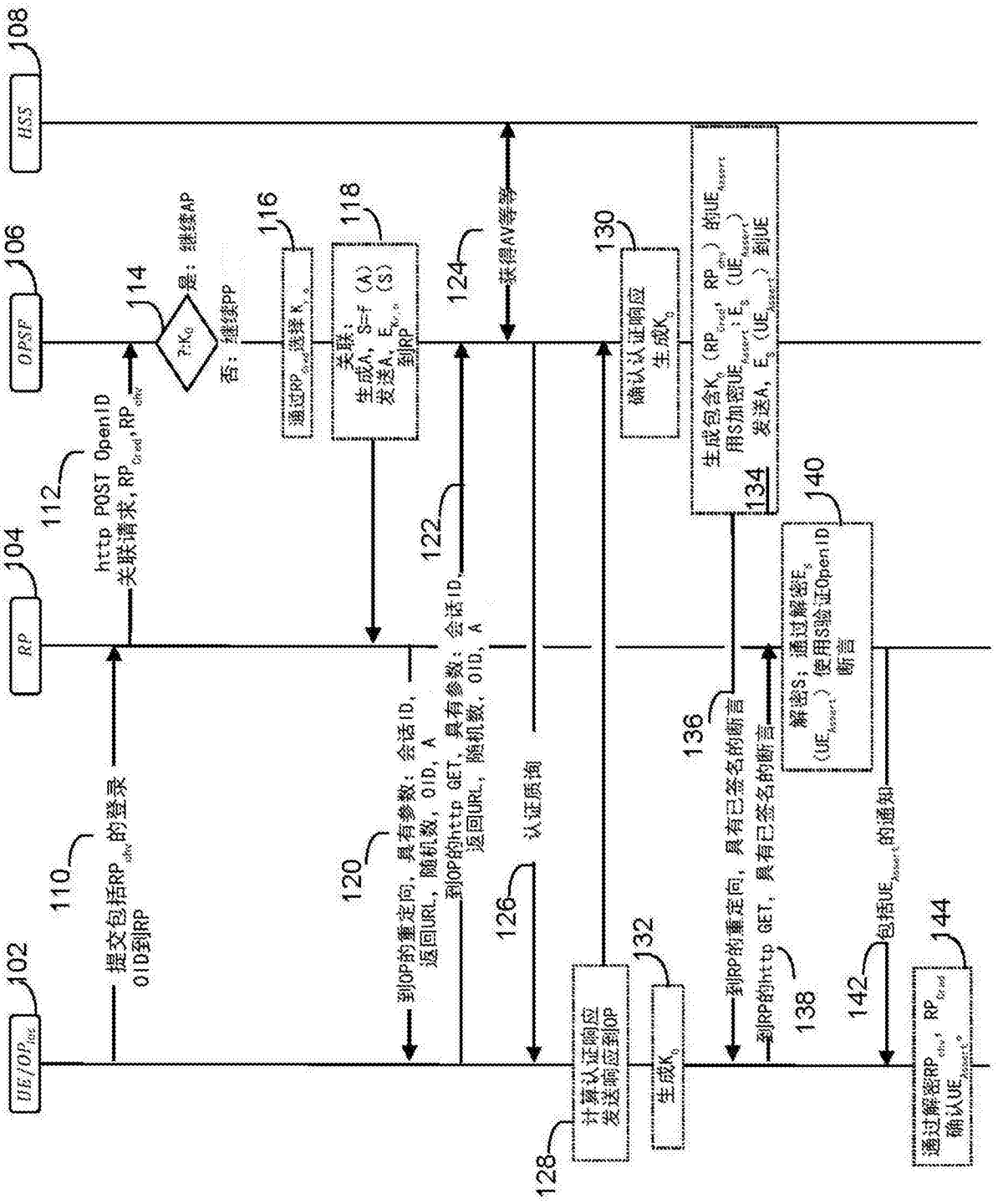

UE/OP
RP
OPSF
HSS
102
104
106
108
110
112
114
116
118
120
122
124
126
128
130
132
134
136
138
140
142
144
提交包括RP的登录OID到RP
http POST OpenID关联请求, RP
?-K
是：继续AP
否：继续PP
通过RP选择K
关联：生成A, S=f(A)(S)发送A, 到RP
到OP的重定向，具有参数：会话ID，返回URL，随机数，OID，A
到OP的http GET，具有参数：会话ID，返回URL，随机数，OID，A
获得AV等等
认证质询
计算认证响应发送响应到OP
确认认证响应生成K
生成K
生成包含K（RP, RP）的UE用S加密UE, E(UE)到UE
发送A, E(UE)到UE
到RP的重定向，具有已签名的断言
到RP的http GET，具有已签名的断言
解密S；通过解密E((UE)')使用S验证OpenID断言
包括UE的通知
通过解密RP, RP确认UE

图1

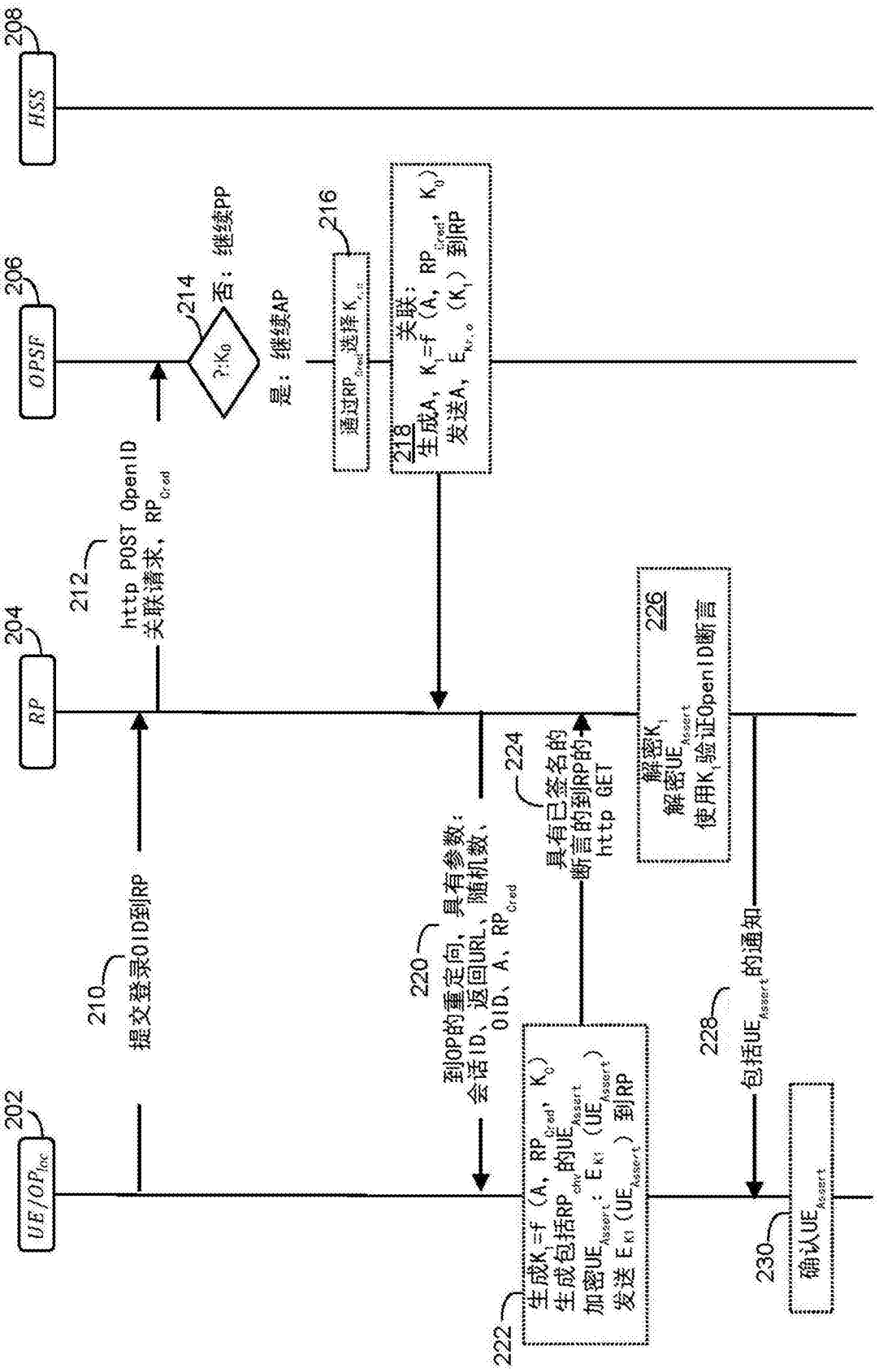

208
HSS
206
OPSF
214
?:K0
否：继续PP
是：继续AP
216
通过RPCred选择Kx,0
218
关联：
生成A，K1=f（A，RPCred，K0）
发送A，EKx,0（K1）到RP
212
http POST OpenID
关联请求，RPCred
204
RP
210
提交登录OID到RP
220
到OP的重定向，具有参数：
会话ID、返回URL、随机数，
OID、A，RPCred
224
具有已签名的
断言的到RP的
http GET
226
解密K1
解密UEAssert
使用K1验证OpenID断言
228
包括UEAssert的通知
202
UE/ORUE
222
生成K1=f（A，RPCred，K0）
生成包括RPCred的UEAssert
加密UEAssert：EK1（UEAssert）
发送EK1（UEAssert）到RP
230
确认UEAssert

图2

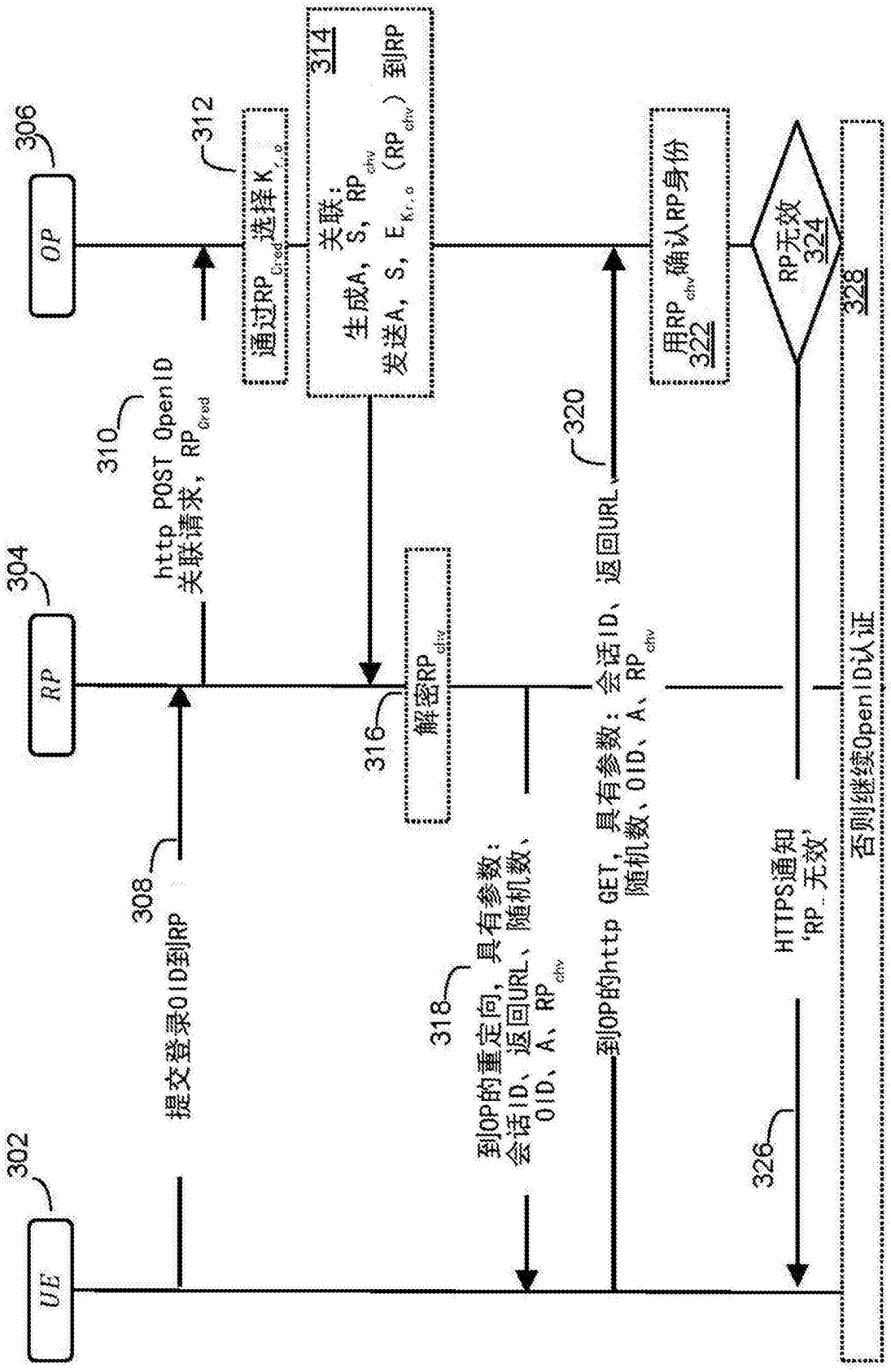

UE
302
OP
306
RP
304
308
提交登录OID到RP
310
http POST OpenID
关联请求，RP_prod
312
通过RP_prod选择K_r,a
314
关联：
生成A，S，RP_chv
发送A，S，E_Kr,a（RP_chv）到RP
316
解密RP_chv
318
到OP的重定向，具有参数：
会话ID、返回URL、随机数、
OID、A、RP_chv
320
到OP的http GET，具有参数：会话ID、返回URL、
随机数、OID、A、RP_chv
322
用RP_chv确认RP身份
324
RP无效
326
HTTPS通知
'RP_无效'
328
否则继续OpenID认证

图3

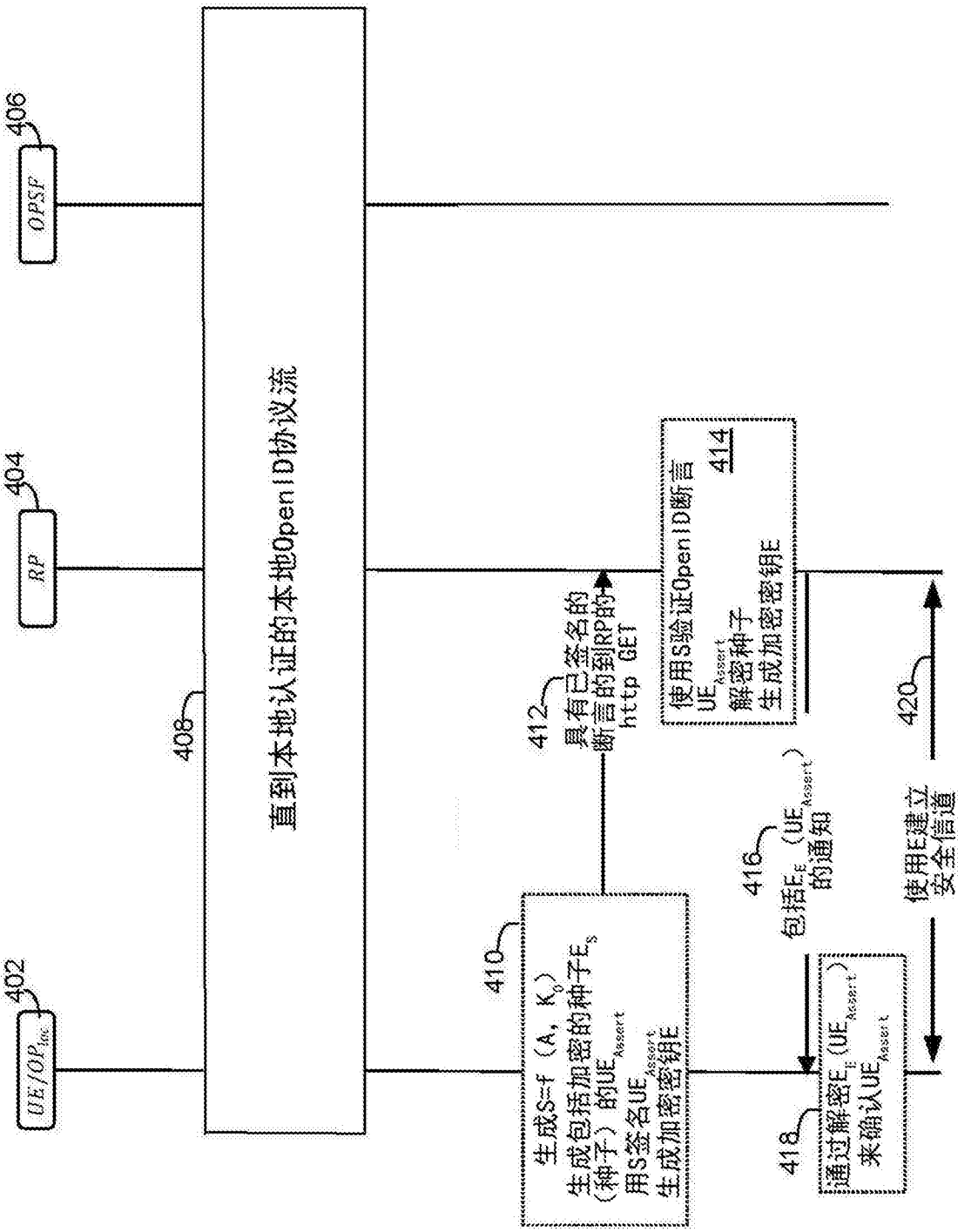

406
OPSF
404
RP
402
UE/OP
408
直到本地认证的本地OpenID协议流
410
生成S=f（A，K0）
生成包括加密的种子ES
（种子）的UEAssert
用S签名UEAssert
生成加密密钥E
412
具有已签名的
断言的到RP的
http GET
414
使用S验证OpenID断言
UEAssert
解密种子
生成加密密钥E
416
包括EE（UEAssert）
的通知
418
通过解密EE（UEAssert）
来确认UEAssert
420
使用E建立
安全信道

图4

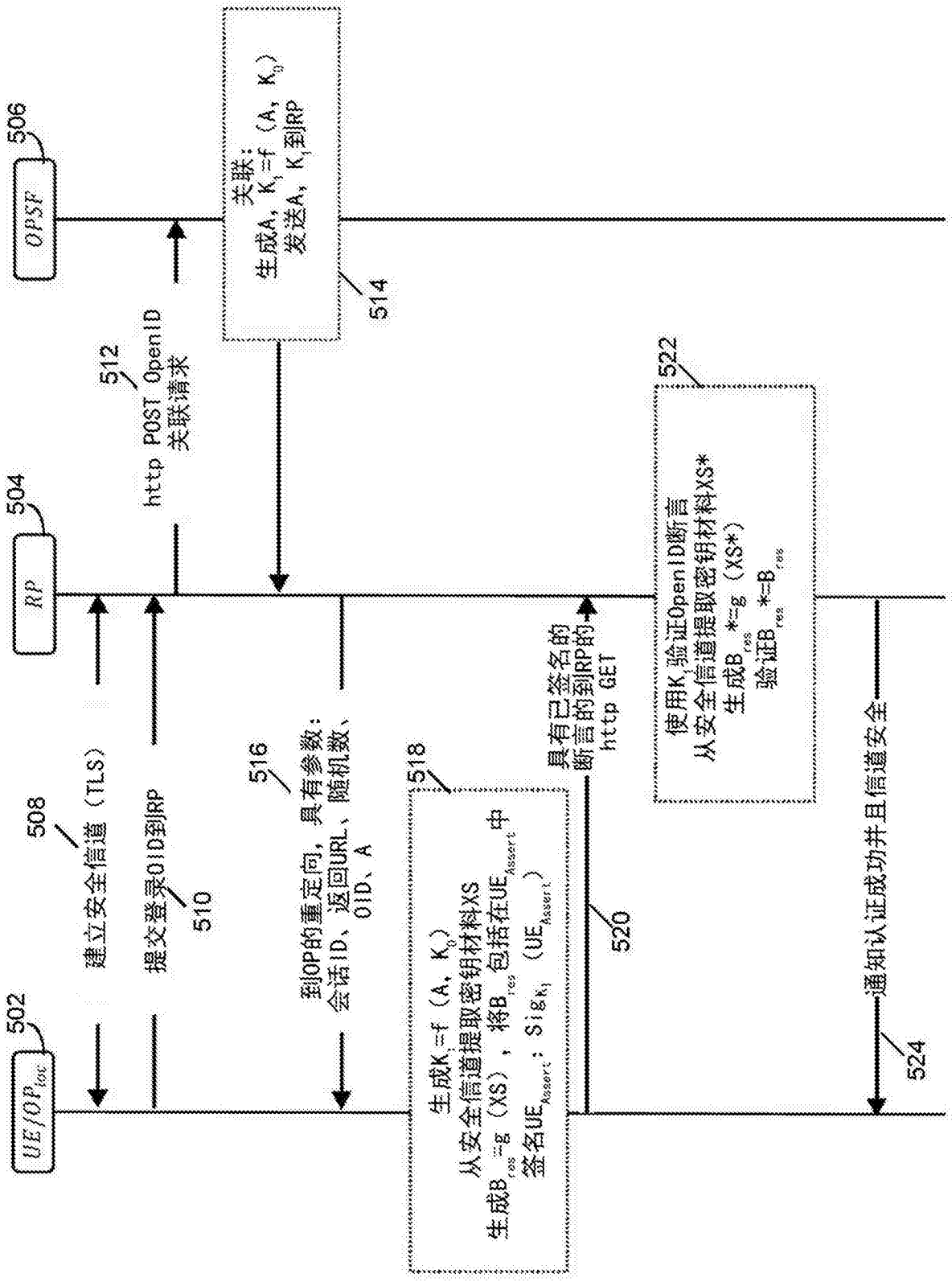

UE/OP
502
RP
504
OPSF
506
建立安全信道（TLS）
508
提交登录OID到RP
510
http POST OpenID
关联请求
512
关联：
生成A，K1=f（A，K0）
发送A，K1到RP
514
到OP的重定向，具有参数：
会话ID、返回URL、随机数、
OID、A
516
生成K1=f（A，K0）
从安全信道提取密钥材料XS
生成Bres=g（XS），将Bres包括在UEAssert中
签名UEAssert；Sigk1（UEAssert）
518
具有已签名的
断言的到RP的
http GET
520
使用K1验证OpenID断言
从安全信道提取密钥材料XS*
生成Bres*=g（XS*）
验证Bres*=Bres
522
通知认证成功并且信道安全
524

图5

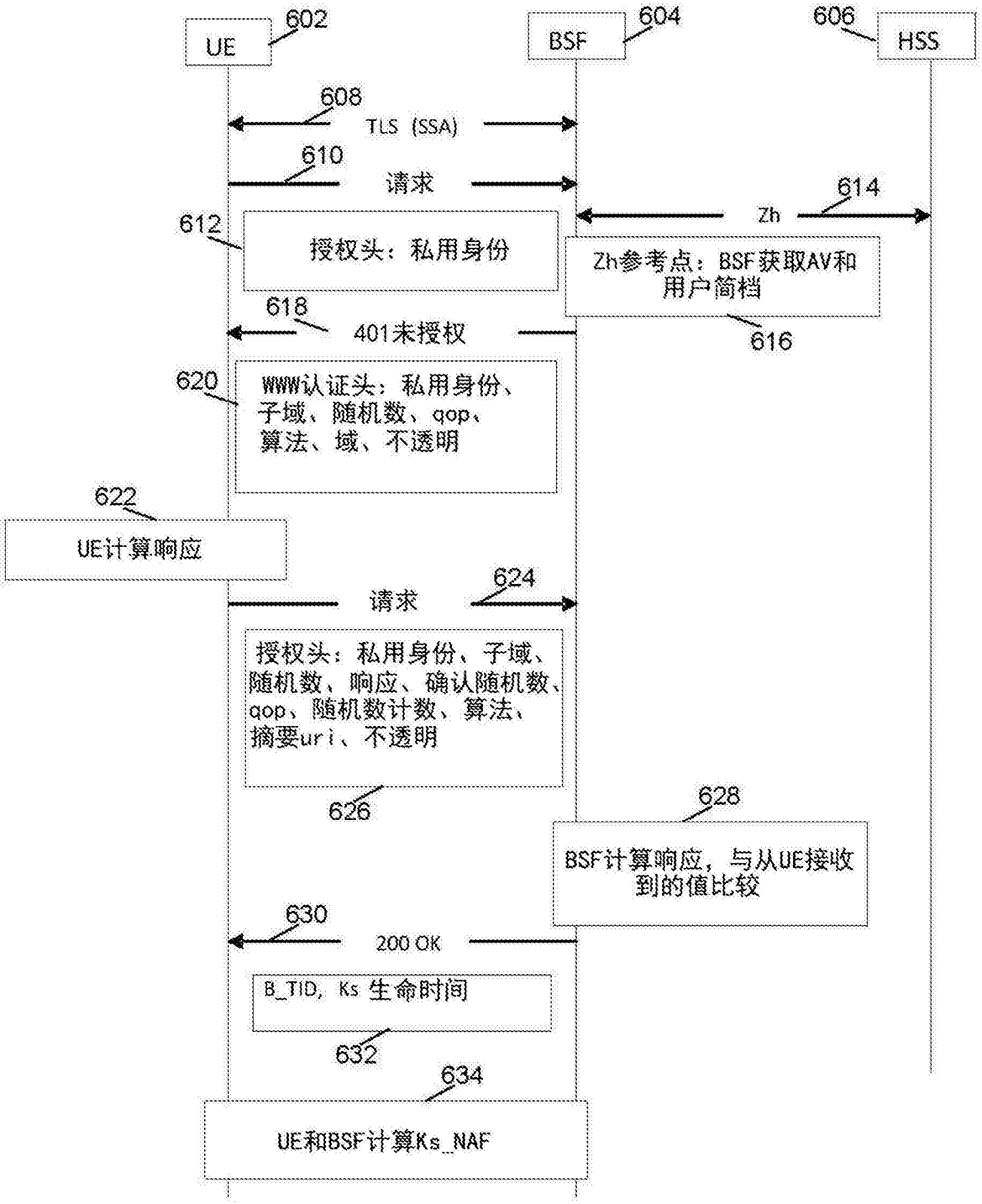

UE
602
BSF
604
606
HSS
608
TLS (SSA)
610
请求
614
Zh
612
授权头：私用身份
Zh参考点：BSF获取AV和用户简档
618
401未授权
616
620
WWW认证头：私用身份、子域、随机数、qop、算法、域、不透明
622
UE计算响应
624
请求
授权头：私用身份、子域、随机数、响应、确认随机数、qop、随机数计数、算法、摘要uri、不透明
626
628
BSF计算响应，与从UE接收到的值比较
630
200 OK
B_TID, Ks 生命时间
632
634
UE和BSF计算Ks_NAF

图6

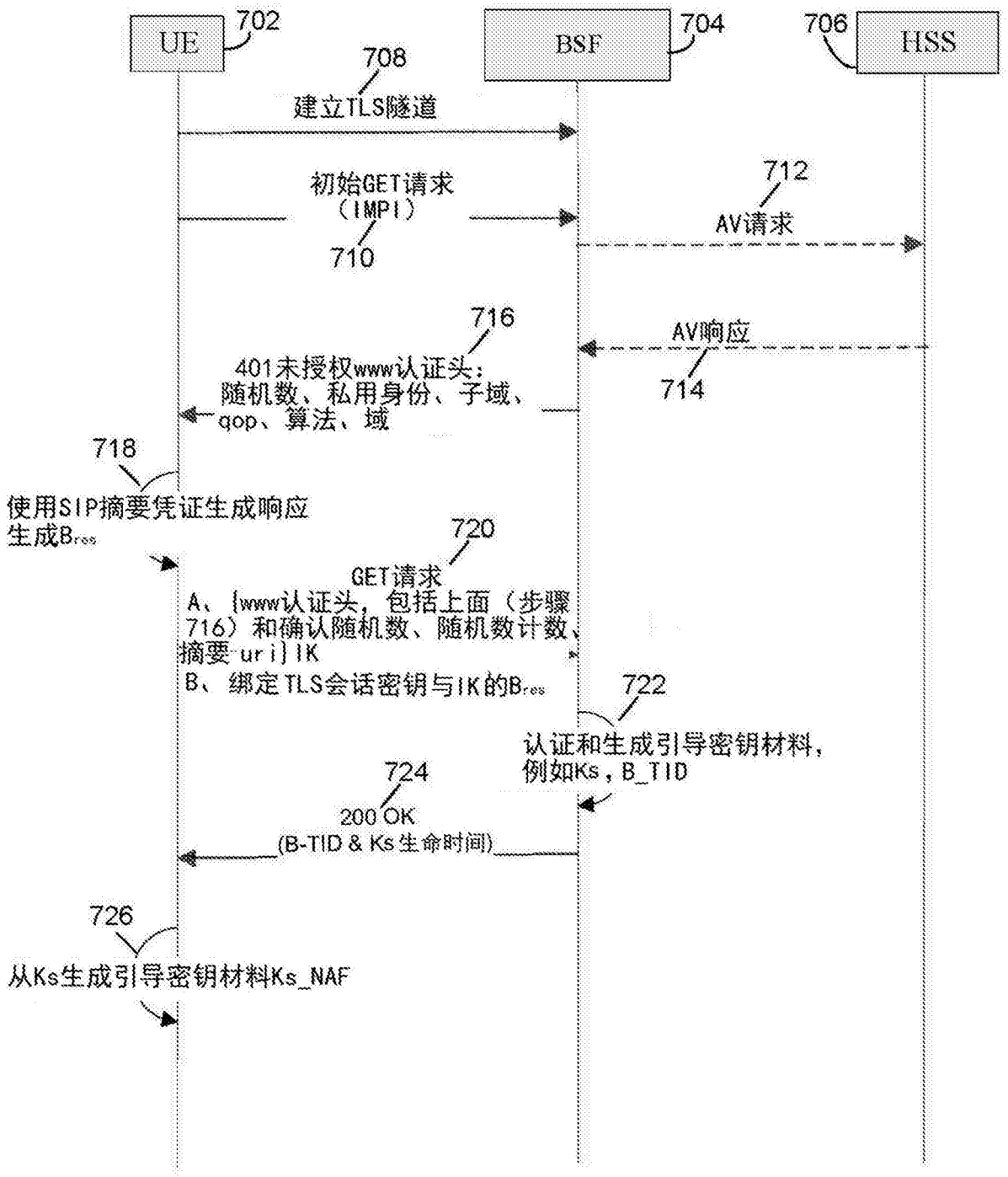

UE
702
BSF
704
706
HSS
708
建立TLS隧道
初始GET请求
（IMPI）
710
712
AV请求
AV响应
714
716
401未授权www认证头：
随机数、私用身份、子域、
qop、算法、域
718
使用SIP摘要凭证生成响应
生成Bres
720
GET请求
A、{www认证头，包括上面（步骤716）和确认随机数、随机数计数、摘要 uri}IK
B、绑定TLS会话密钥与IK的Bres
722
认证和生成引导密钥材料，
例如Ks，B_TID
724
200 OK
(B-TID & Ks 生命时间)
726
从Ks生成引导密钥材料Ks_NAF

图7

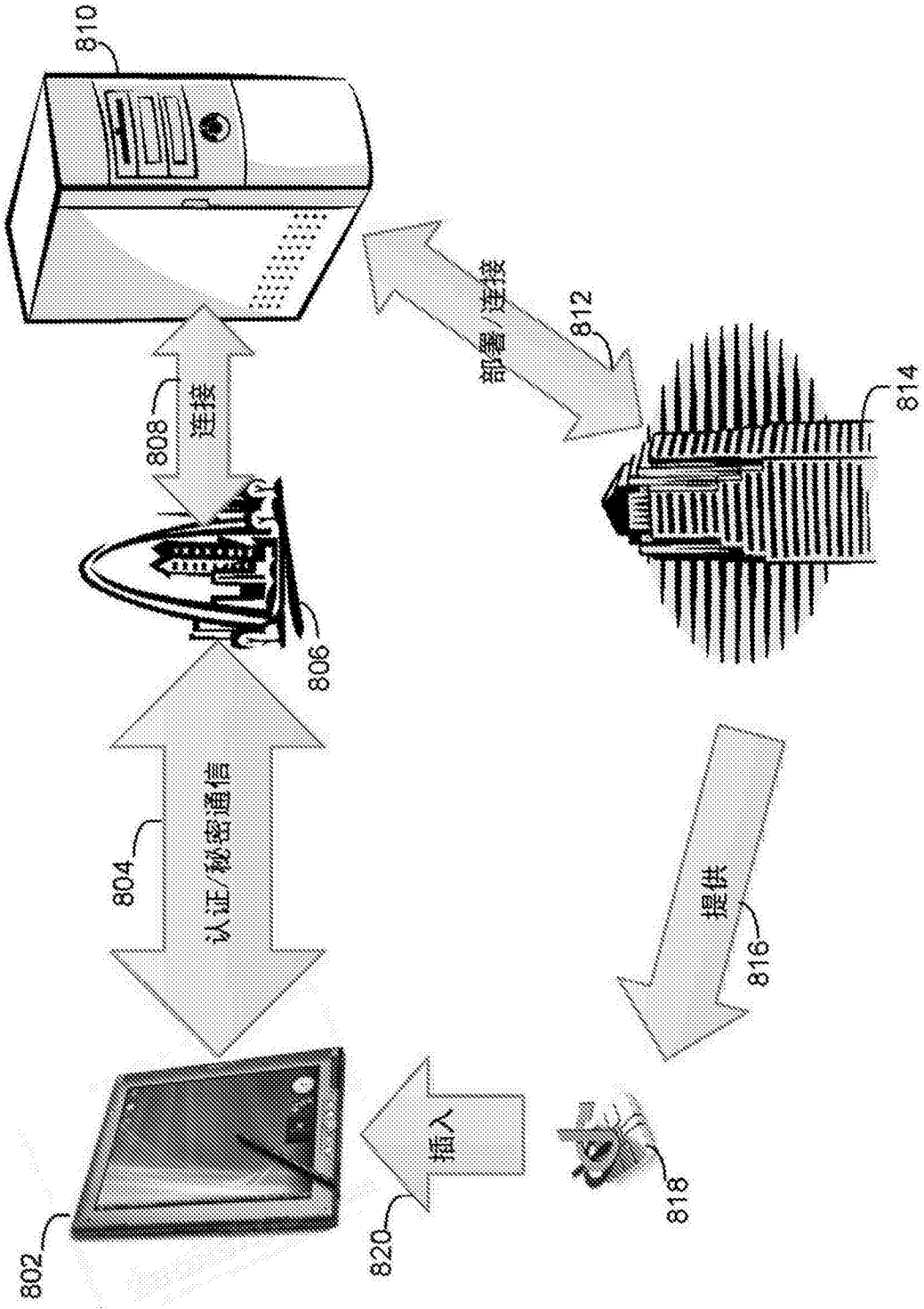


图8

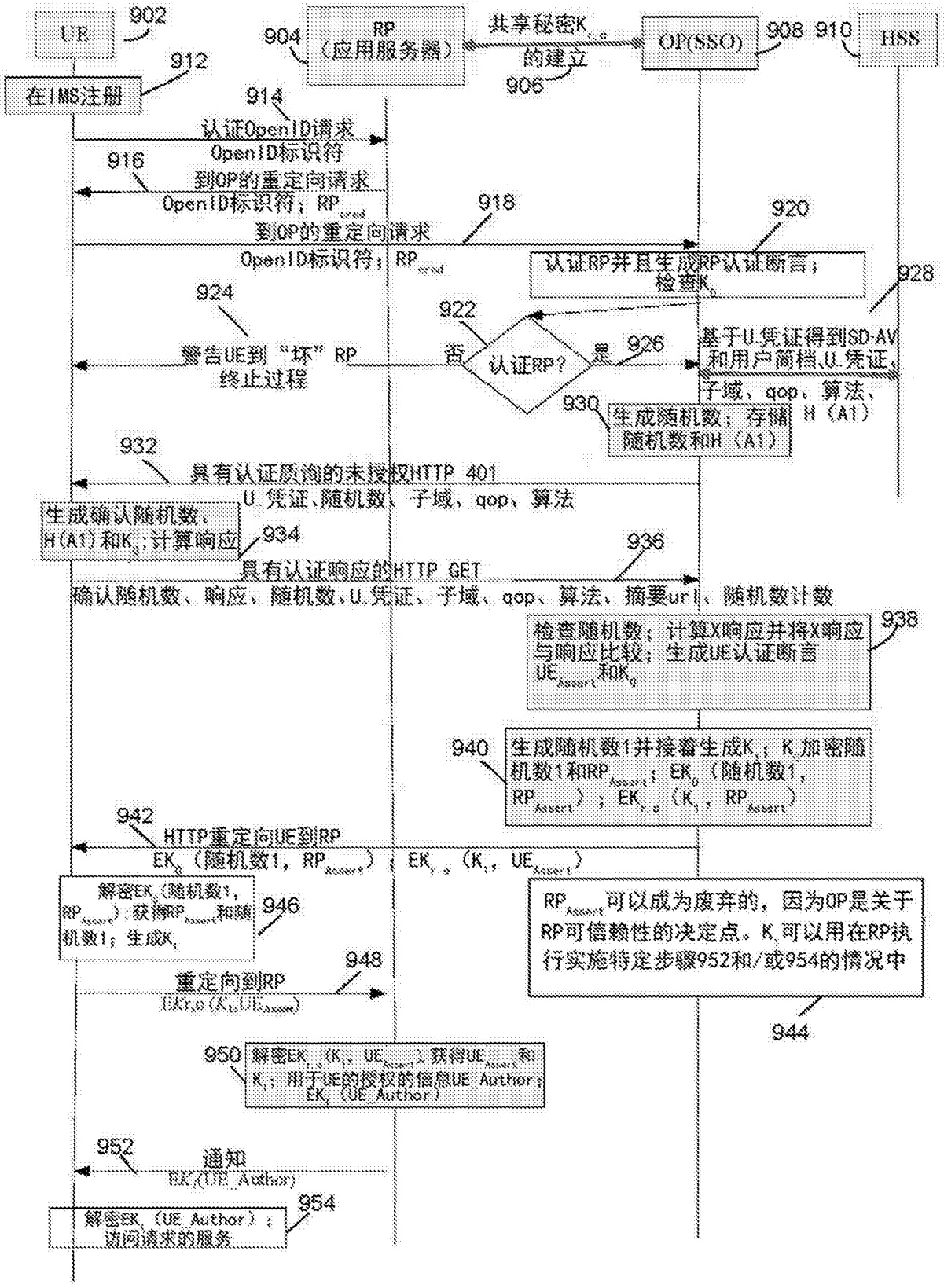

UE
902
RP
（应用服务器）
904
共享秘密K
的建立
906
OP(SSO)
908
910
HSS
912
在IMS注册
914
认证OpenID请求
OpenID标识符
916
到OP的重定向请求
OpenID标识符；RP
918
到OP的重定向请求
OpenID标识符；RP
920
认证RP并且生成RP认证断言；
检查K
928
924
警告UE到“坏”RP
终止过程
922
认证RP？
否
是
926
基于U.凭证得到SD-AV
和用户简档、U.凭证、
子域、qop、算法、
930
生成随机数，存储 H（A1）
随机数和H（A1）
932
具有认证质询的未授权HTTP 401
U.凭证、随机数、子域、qop、算法
生成确认随机数、
H(A1)和K
计算响应
934
具有认证响应的HTTP GET
936
确认随机数、响应、随机数、U.凭证、子域、qop、算法、摘要url、随机数计数
检查随机数；计算X响应并将X响应
与响应比较；生成UE认证断言
UE
和K
938
940
生成随机数1并接着生成K
K
加密随
机数1和RP
；EK
（随机数1，
RP
）；EK
（K
，RP
）
942
HTTP重定向UE到RP
EK
（随机数1，RP
）；EK
（K
，UE
）
解密EK
（随机数1，
RP
）；获得RP
和随
机数1；生成K
946
RP
可以成为废弃的，因为OP是关于
RP可信赖性的决定点。K
可以用在RP执
行实施特定步骤952和/或954的情况中
944
948
重定向到RP
950
解密EK
（K
，UE
）；获得UE
和
K
；用于UE的授权的信息UE_Author；
EK
（UE_Author）
952
通知
954
解密EK
（UE_Author）；
访问请求的服务

图9

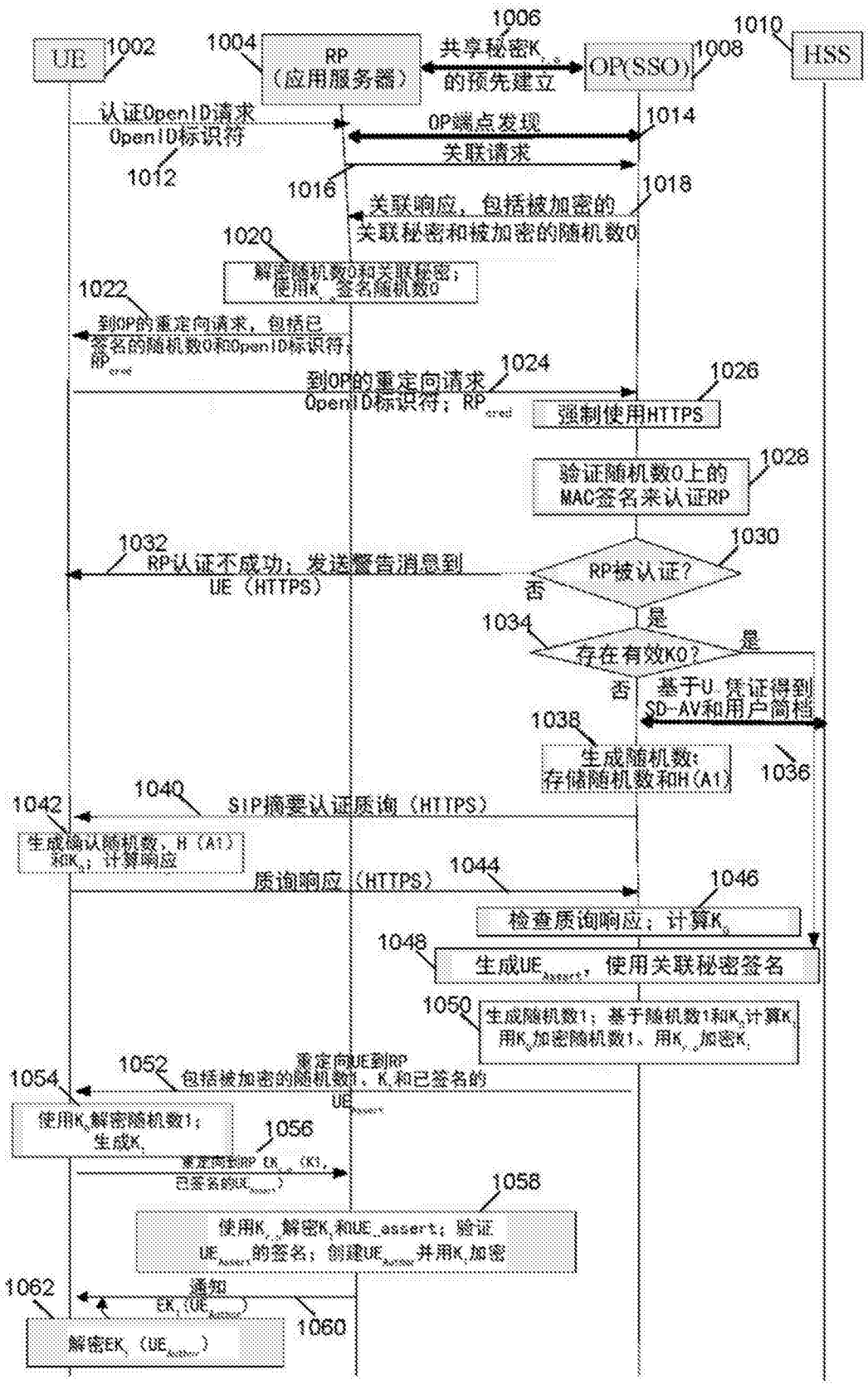

UE
1002
1004
RP
（应用服务器）
1006
共享秘密K
的预先建立
OP(SSO)
1008
1010
HSS
认证OpenID请求
OpenID标识符
1012
OP端点发现
1014
关联请求
1016
关联响应，包括被加密的
关联秘密和被加密的随机数0
1018
1020
解密随机数0和关联秘密；
使用K_c签名随机数0
1022
到OP的重定向请求，包括已
签名的随机数0和OpenID标识符；
RP_cred
1024
到OP的重定向请求
OpenID标识符；RP_cred
1026
强制使用HTTPS
1028
验证随机数0上的
MAC签名来认证RP
1030
RP被认证？
否
是
1032
RP认证不成功，发送警告消息到
UE（HTTPS）
1034
存在有效KO？
是
否
基于U 凭证得到
SD-AV和用户简档
1036
1038
生成随机数；
存储随机数和H(A1)
1040
SIP摘要认证质询（HTTPS）
1042
生成随机数，H（A1）
和K_c，计算响应
1044
质询响应（HTTPS）
1046
检查质询响应；计算K_c
1048
生成UE_assert，使用关联秘密签名
1050
生成随机数1；基于随机数1和K_c计算K_c
用K_c加密随机数1、用K_c加密K_c
1052
重定向UE到RP
包括被加密的随机数1、K_c和已签名的
UE_assert
1054
使用K_c解密随机数1；
生成K_c
1056
重定向到RP EK_c（K_c），
已签名的UE_assert
1058
使用K_c解密K_c和UE_assert；验证
UE_assert的签名；创建UE_assert并用K_c加密
1062
通知
EK_c（UE_assert）
1060
解密EK_c（UE_assert）

图10

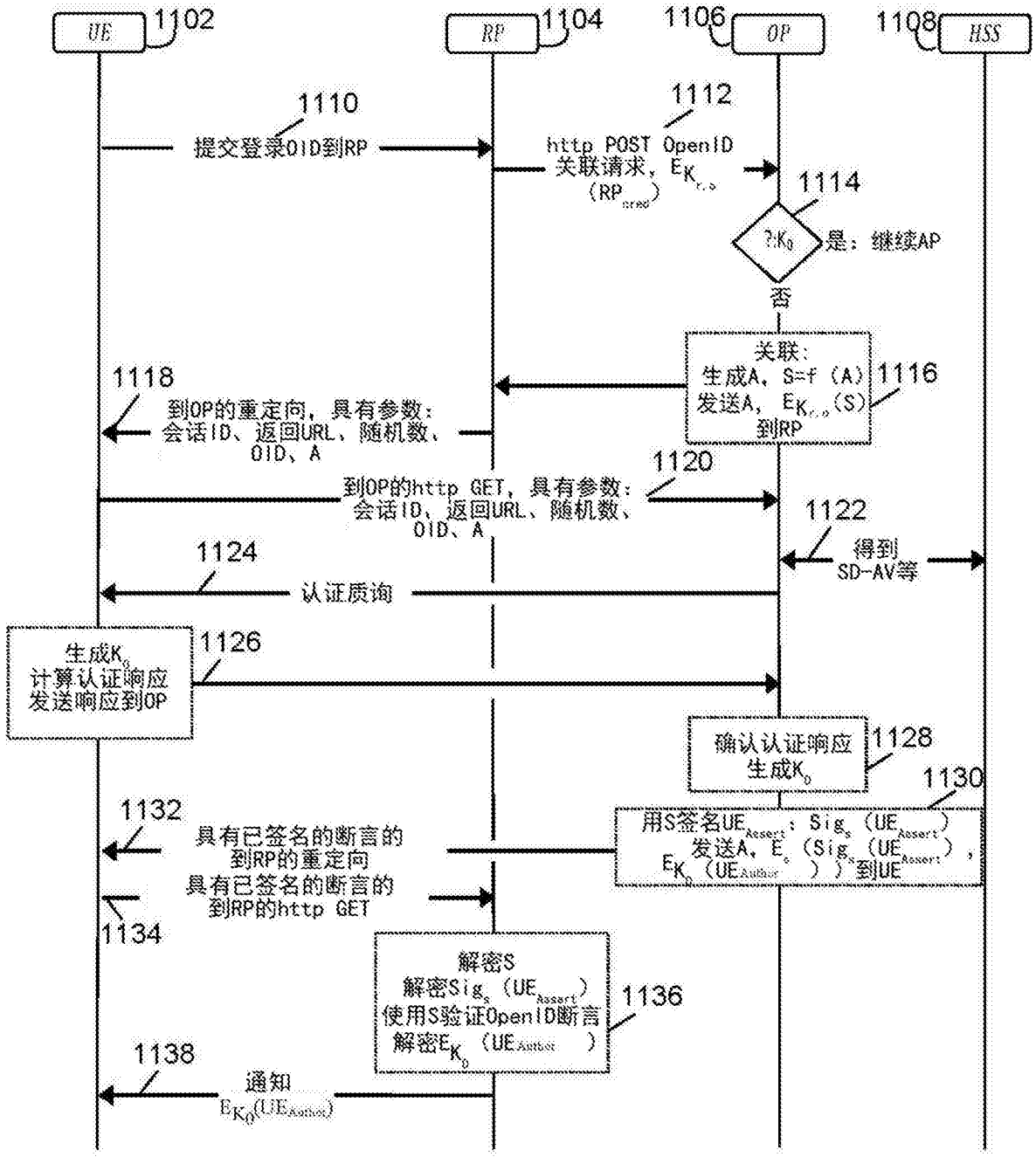

UE
1102
RP
1104
1106
OP
1108
HSS
1110
提交登录OID到RP
1112
http POST OpenID
关联请求，$E_{K_{r,o}}$
(RP_{nred})
1114
?:K_0
是：继续AP
否
关联：
生成A，S=f（A）
发送A，$E_{K_{r,o}}$(S)
到RP
1116
1118
到OP的重定向，具有参数：
会话ID、返回URL、随机数、
OID、A
1120
到OP的http GET，具有参数：
会话ID、返回URL、随机数、
OID、A
1122
得到
SD-AV等
1124
认证质询
生成K_0
计算认证响应
发送响应到OP
1126
确认认证响应
生成K_0
1128
1130
用S签名UE_{Assert}；Sig_s（UE_{Assert}）
发送A，E_s（Sig_s（UE_{Assert}），
E_{K_0}（UE_{Author}））到UE
1132
具有已签名的断言的
到RP的重定向
具有已签名的断言的
到RP的http GET
1134
解密S
解密Sig_s（UE_{Assert}）
使用S验证OpenID断言
解密E_{K_0}（UE_{Author}）
1136
1138
通知
$E_{K_0}(UE_{Author})$

图11

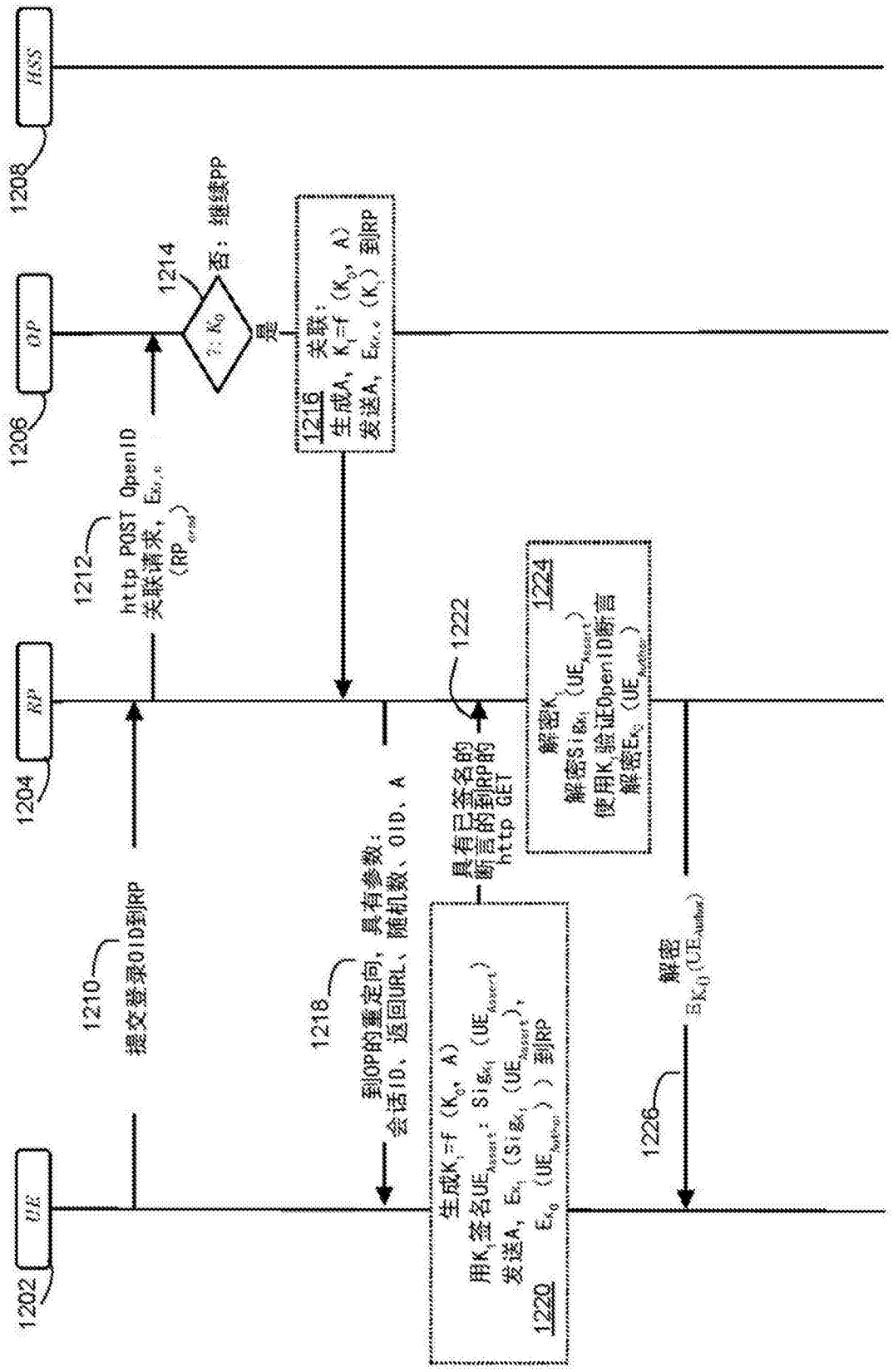

HSS
1208
OP
1206
RP
1204
UE
1202
1214
否：继续PP
是
1216 关联；
生成A，$K_i=f(K_0, A)$
发送A，$E_{K_{i,0}}(K_i)$ 到RP
1212
http POST OpenID
关联请求，$E_{K_{i,0}}$，
(RP_{cred})
1210
提交登录OID到RP
1218
到OP的重定向，具有参数：
会话ID，返回URL，随机数，OID，A
1220
生成$K_i=f(K_0, A)$
用K_i签名UE_{Assert}：$Sig_{K_i}(UE_{Assert})$，
发送A，$E_{K_0}(Sig_{K_i}(UE_{Assert}))$，$E_{K_0}(UE_{Address})$ 到RP
具有已签名的
断言的到RP的
http GET
1222
1224
解密K_i
解密$Sig_{K_i}(UE_{Assert})$
使用K_i验证OpenID断言
解密$E_{K_0}(UE_{Address})$
解密
$E_{K_0}(UE_{Address})$
1226

图12

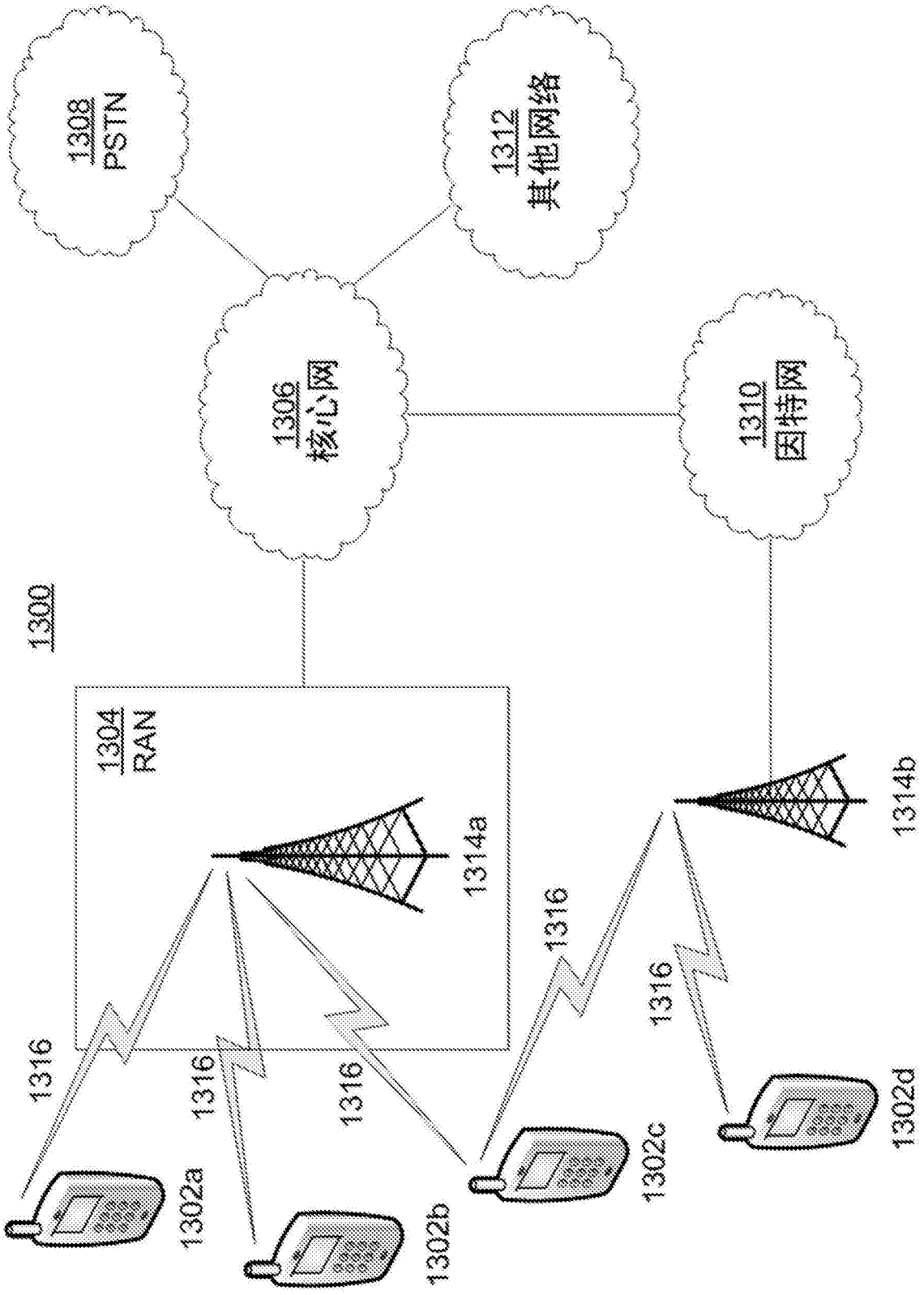

1308
PSTN
1312
其他网络
1306
核心网
1310
因特网
1300
1304
RAN
1314a
1314b
1316
1316
1316
1316
1316
1302a
1302b
1302c
1302d

图13A

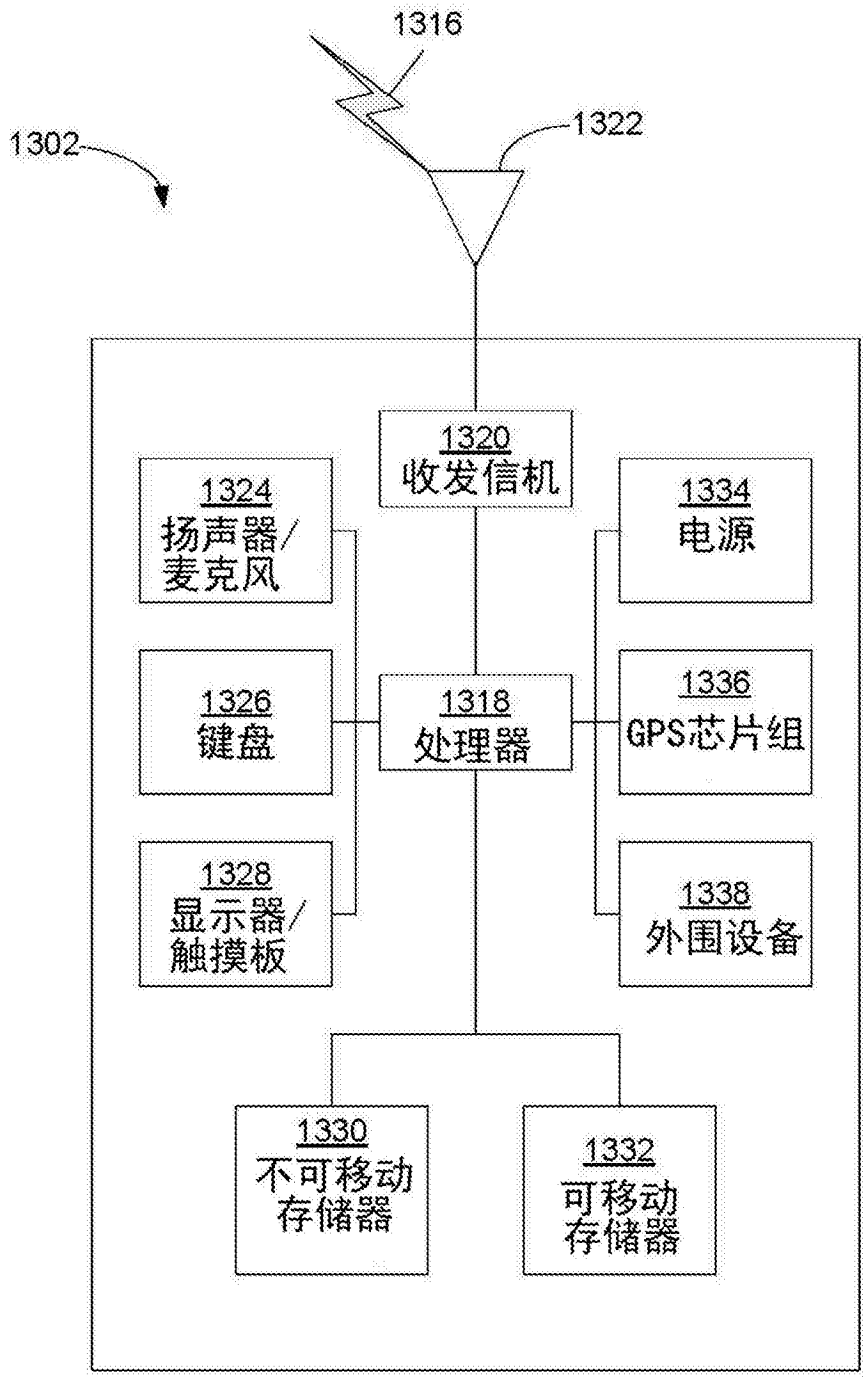

1316
1322
1302
1320
收发信机
1324
扬声器/
麦克风
1334
电源
1326
键盘
1318
处理器
1336
GPS芯片组
1328
显示器/
触摸板
1338
外围设备
1330
不可移动
存储器
1332
可移动
存储器

图13B

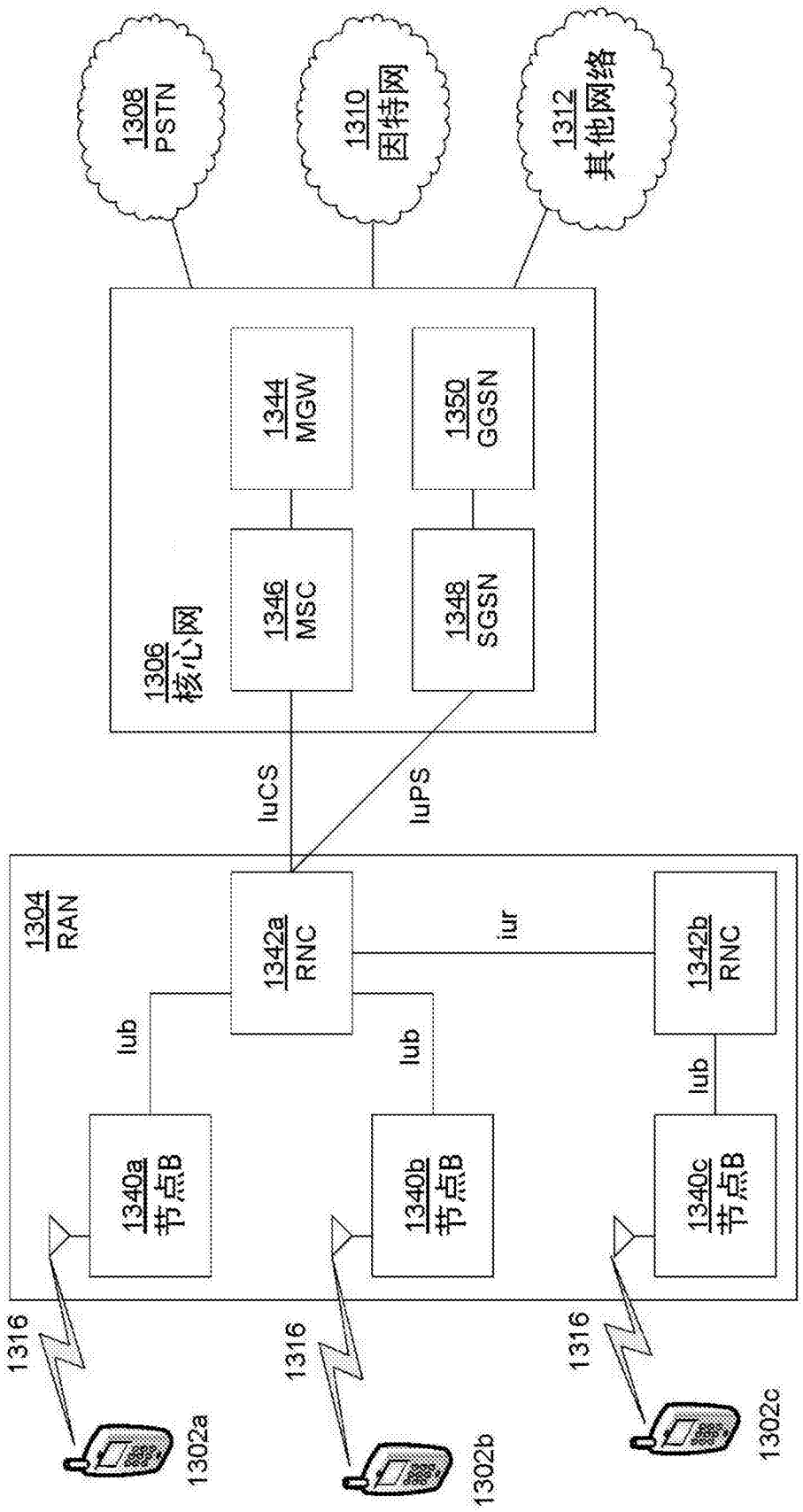

1308
PSTN
1310
因特网
1312
其他网络
1306
核心网
1344
MGW
1346
MSC
1348
SGSN
1350
GGSN
IuCS
IuPS
1304
RAN
1342a
RNC
1342b
RNC
Iur
Iub
Iub
Iub
1340a
节点B
1340b
节点B
1340c
节点B
1316
1316
1316
1302a
1302b
1302c

图13C

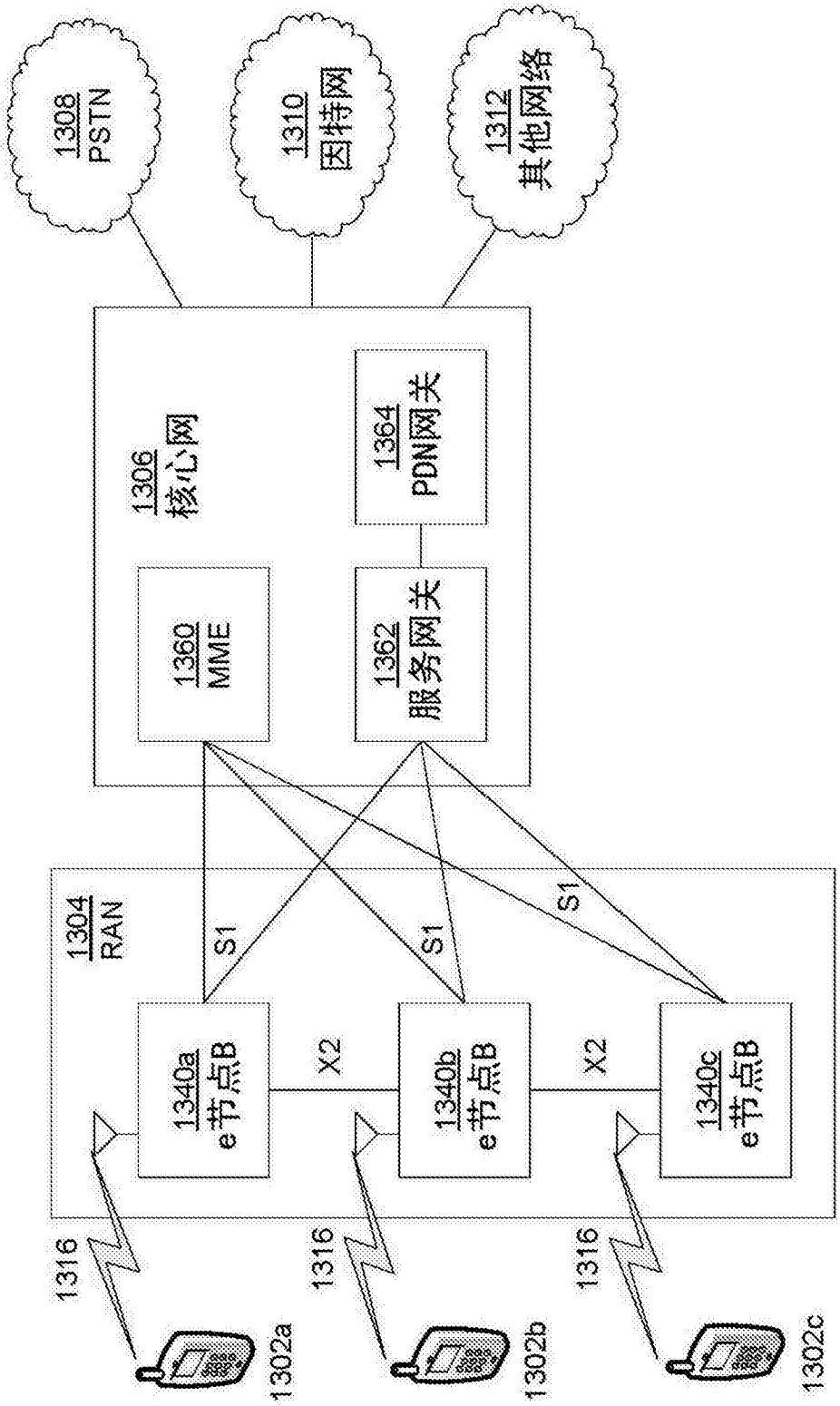

1308
PSTN
1310
因特网
1312
其他网络
1306
核心网
1364
PDN网关
1360
MME
1362
服务网关
1304
RAN
S1
S1
S1
1340a
e节点B
X2
1340b
e节点B
X2
1340c
e节点B
1316
1316
1316
1302a
1302b
1302c

图13D

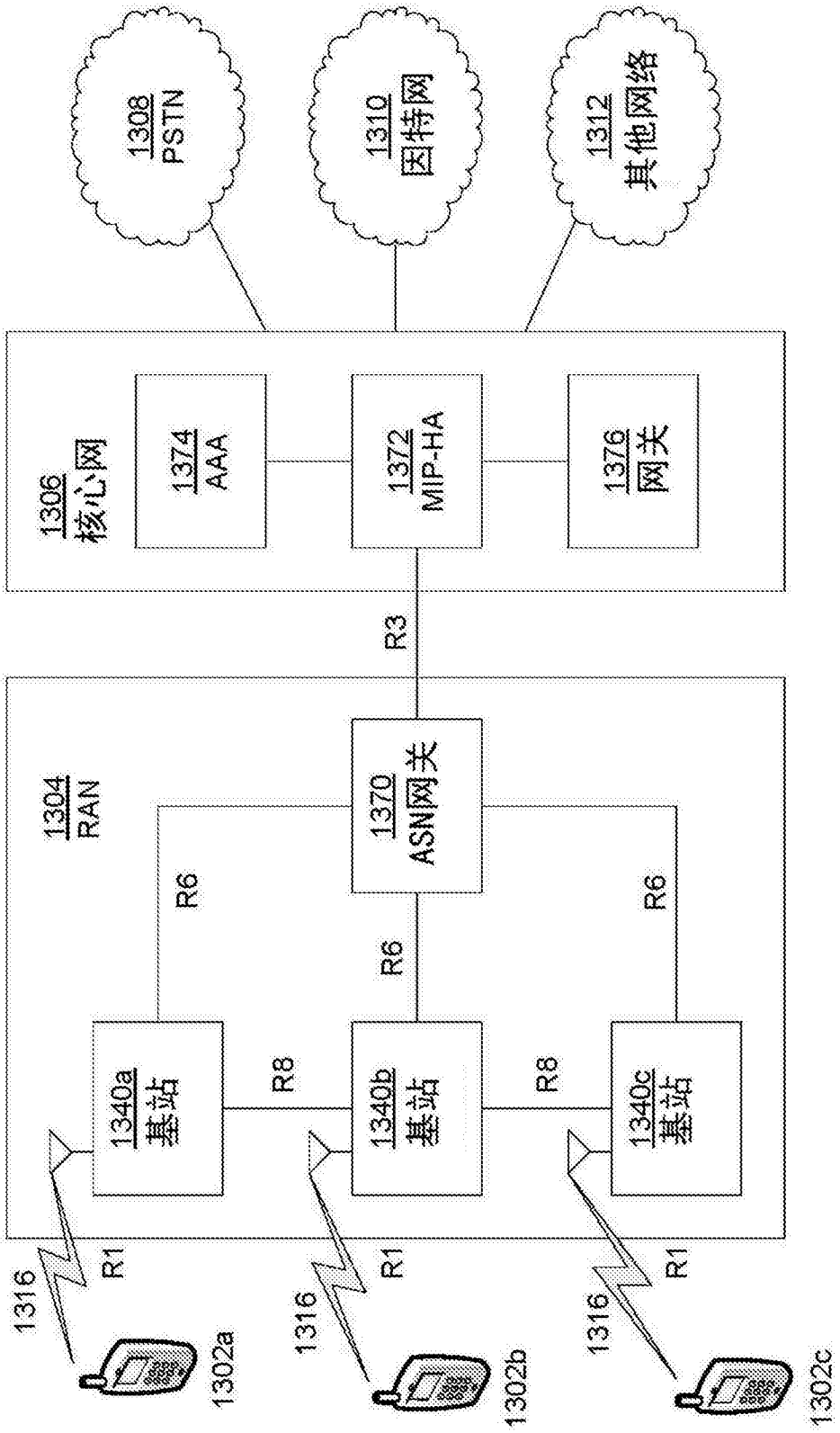

1308
PSTN
1310
因特网
1312
其他网络
1306
核心网
1374
AAA
1372
MIP-HA
1376
网关
R3
1304
RAN
1370
ASN网关
R6
R6
R6
1340a
基站
1340b
基站
1340c
基站
R8
R8
R1
R1
R1
1316
1316
1316
1302a
1302b
1302c

图13E