(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104115465 A
(43)申请公布日 2014.10.22

(21)申请号 201380006159.8

(22)申请日 2013.01.18

(30)优先权数据
61/589,125 2012.01.20 US

(85)PCT国际申请进入国家阶段日
2014.07.21

(86)PCT国际申请的申请数据
PCT/US2013/022105 2013.01.18

(87)PCT国际申请的公布数据
WO2013/109857 EN 2013.07.25

(71)申请人 交互数字专利控股公司
地址 美国特拉华州

(72)发明人 A·莱切尔 Y·C·沙阿
V·K·乔伊

(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.
H04L 29/06(2006.01)
H04W 12/06(2006.01)

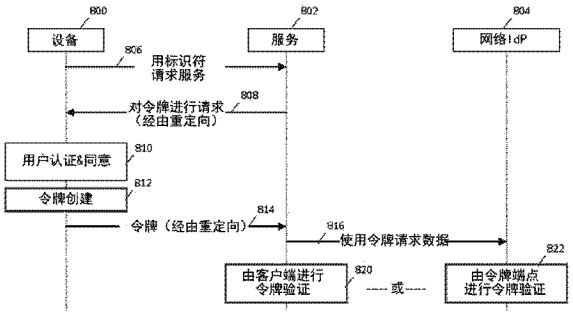
权利要求书4页 说明书28页 附图14页

(54)发明名称

具有本地功能的身份管理

(57)摘要

用户设备(U)可在本地执行功能,例如在位于U内的可信模块上。例如,U可以经由本地身份提供方功能执行与单点登录协议(例如,开放ID连接)相关联的功能。例如,U可以生成能够由服务提供方用来取得用户信息(例如,身份信息和/或用户属性)的身份令牌和接入令牌。用户属性可经由用户信息端点来取得,所述用户信息端点可本地位于所述U上,或者位于网络实体上。服务提供方可以基于其使用令牌取得的信息来授权用户接入服务。



CN 104115465 A

1. 一种在包括经由网络通信的用户设备 (UE)、身份提供方 (IdP) 以及服务提供方 (SP) 的系统中的方法，该方法包括 ：

接收对令牌的请求，其中对所述令牌的所述请求响应于对接入由所述服务提供方提供的服务的请求 ；

在所述 UE 处，响应于对所述令牌的所述请求，根据对所述令牌的所述请求创建身份 (ID) 令牌 ；以及

经由所述 UE 发出所述 ID 令牌，其中所述 ID 令牌被验证以为所述 UE 提供对所述服务的接入。

2. 根据权利要求 1 所述的方法，其中所述 ID 令牌在位于所述 UE 内的可信环境中被安全地创建。

3. 根据权利要求 1 所述的方法，该方法还包括 ：

接收授权请求以为所述 SP 创建接入令牌，其中所述授权请求由所述 UE 的用户批准 ；以及

在所述 UE 处，响应于所述授权请求，创建与所述授权请求的所述用户批准相关联的所述接入令牌。

4. 根据权利要求 3 所述的方法，其中所述授权请求的所述用户批准经由所述 UE 的策略而被自动接收。

5. 根据权利要求 3 所述的方法，其中所述接入令牌包括指示用户信息端点的位置的信息，其中一旦验证了所述接入令牌，所述用户信息端点就向所述 SP 提供所请求的用户属性。

6. 根据权利要求 5 所述的方法，其中所述接入令牌的验证包括对所述用户同意将所请求的用户属性释放到所述 SP 的验证。

7. 根据权利要求 5 所述的方法，其中所述接入令牌在位于所述 UE 内的可信环境中被安全地创建，并且其中所述接入令牌的验证包括对所述可信环境有效的验证。

8. 根据权利要求 5 所述的方法，其中所述用户信息端点位于所述 UE 或经由所述网络与所述 SP 通信的网络实体中的至少一者上。

9. 根据权利要求 3 所述的方法，其中所述 ID 令牌和所述接入令牌根据开放 ID 连接协议来创建。

10. 根据权利要求 3 所述的方法，其中所述 ID 令牌和所述接入令牌在位于所述 UE 内的可信环境中被安全地创建，所述方法还包括 ：

使用所述可信模块确定所述用户的认证状态 ；以及

在所述认证状态指示所述用户尚未被认证的情况下，在所述可信环境处认证所述用户。

11. 根据权利要求 1 所述的方法，该方法还包括 ：

接收授权请求以为所述 SP 创建接入令牌 ；

在所述 UE 处，基于所述授权请求，创建第一接入令牌和第二接入令牌，所述接入令牌与所述服务和所述用户相关联。

12. 根据权利要求 11 所述的方法，其中所述第一接入令牌包括指示第一用户信息端点的位置的信息，其中一旦验证了所述第一接入令牌，所述第一用户信息端点就向所述 SP 提

供第一请求的用户属性，而所述第二接入令牌包括指示第二用户信息端点的位置的信息，其中一旦验证了所述第二接入令牌，所述第二用户信息端点就向所述 SP 提供第二请求的用户属性，且其中所述第一用户信息端点位于所述 UE 上，而所述第二用户信息端点位于经由所述网络与所述 SP 通信的网络实体上。

13. 根据权利要求 12 所述的方法，其中由所述第一用户信息端点提供的所述第一请求的用户属性由所述用户分类为机密数据，而由所述第二用户信息端点提供的所述第二请求的用户属性由所述用户分类为非机密数据。

14. 根据权利要求 2 所述的方法，其中所述 SP 是开放 ID 连接客户端，以及所述可信环境是本地开放 ID 身份提供方 (OP)。

15. 一种在包括经由网络通信的用户设备 (UE)、身份提供方 (IdP) 以及服务提供方 (SP) 的系统中的方法，该方法包括：

在所述 UE 处：

接收对用户数据的请求；

接收对释放所述用户数据的同意部分的用户同意；

响应于所述用户同意，生成与所述 SP 相关联的接入令牌；以及

向所述 SP 发出所述接入令牌，其中一旦验证了所述接入令牌，所述用户数据的所述同意部分被释放到所述 SP。

16. 根据权利要求 15 所述的方法，其中所请求的用户数据包括多个用户属性，其中所述多个用户属性中的至少一者不是被释放的所述用户数据的所述同意部分的一部分。

17. 根据权利要求 15 所述的方法，该方法还包括：

使用签名对所述接入令牌进行签名，所述签名包括所述 UE 的标识符或位于所述 UE 内的可信环境的标识符中的至少一者。

18. 根据权利要求 15 所述的方法，该方法还包括：

使用由所述 UE 和经由所述网络与所述 SP 通信的所述 IdP 共享的机密来对所述接入令牌进行签名。

19. 根据权利要求 15 所述的方法，其中用户信息端点位于所述 UE 内，所述方法还包括：

在所述用户信息端点处接收所述接入令牌；以及

响应于接收到所述接入令牌，向所述 SP 提供所述用户数据的所述同意部分。

20. 一种在包括经由网络通信的用户设备 (UE) 以及服务提供方 (SP) 的系统中的方法，该方法包括：

在所述 SP 处，接收对接入由所述 SP 提供的服务的请求，所述请求包括所述 UE 的用户的标识符或所述 UE 的标识符中的至少一者；

在所述 SP 处，响应于对接入的所述请求，接收身份 (ID) 令牌和第一接入令牌；以及

在所述 SP 处，响应于所述接入令牌的验证，从第一用户信息端点取得第一用户属性，其中所述第一用户信息端点位于所述 UE 上。

21. 根据权利要求 20 所述的方法，该方法还包括：

在所述 SP 处，使用存储在所述 SP 上的机密来验证所述 ID 令牌的签名；以及

响应于所述验证，授权所述 UE 接入所述服务。

22. 根据权利要求 20 所述的方法，该方法还包括：

将所接收到的 ID 令牌发送至校验 ID 端点以进行验证；以及

将所接收到的第一接入令牌发送至所述第一用户信息端点以进行验证，从而将所述 ID 令牌和接入令牌视为不透明的值。

23. 根据权利要求 20 所述的方法，该方法还包括：

响应于对接入的所述请求，接收第二接入令牌；

在所述 SP 处，响应于所述第二接入令牌的验证，从第二用户信息端点取得第二用户属性，其中所述第二用户信息端点位于经由所述网络与所述 SP 通信的网络实体上；以及

在所述 SP 处，合并所述第一用户属性和所述第二用户属性。

24. 一种无线发射 / 接收单元 (WTRU)，该 WTRU 包括：

包括可执行的指令的存储器；以及

与所述存储器通信的处理器，在由所述处理器执行所述指令时，所述指令使得所述处理器完成以下操作：

接收对令牌的请求，其中对所述令牌的所述请求响应于对接入由服务提供方 (SP) 提供的服务的请求；

响应于对所述令牌的所述请求，根据对所述令牌的所述请求创建身份 (ID) 令牌；以及

发出所述 ID 令牌，其中所述 ID 令牌被验证以为所述 WTRU 提供对所述服务的接入。

25. 根据权利要求 24 所述的 WTRU，其中所述处理器还被配置成执行所述指令以执行以下操作：

接收授权请求以为所述 SP 创建接入令牌，其中所述授权请求由所述 WTRU 的用户批准；以及

响应于所述授权请求，创建与所述授权请求的所述用户批准相关联的所述接入令牌。

26. 根据权利要求 25 所述的 WTRU，其中所述接入令牌包括指示用户信息端点的位置的信息，其中一旦验证了所述接入令牌，所述用户信息端点向所述 SP 提供所请求的用户属性。

27. 根据权利要求 26 所述的 WTRU，其中所述接入令牌的验证包括对所述用户同意将所请求的用户属性释放到所述 SP 的验证。

28. 根据权利要求 25 所述的 WTRU，其中所述用户信息端点位于所述 WTRU 或经由所述网络与所述 SP 通信的网络实体中的至少一者上。

29. 根据权利要求 24 所述的 WTRU，其中所述处理器还被配置成执行所述指令以执行以下操作：

接收授权请求以为所述 SP 创建接入令牌；

在所述 WTRU 处，基于所述授权请求，创建第一接入令牌和第二接入令牌，所述接入令牌与所述服务和所述用户相关联。

30. 根据权利要求 29 所述的 WTRU，其中所述第一接入令牌包括指示第一用户信息端点的位置的信息，其中一旦验证了所述第一接入令牌，所述第一用户信息端点就向所述 SP 提供第一请求的用户属性，而所述第二接入令牌包括指示第二用户信息端点的位置的信息，其中一旦验证了所述第二接入令牌，所述第二用户信息端点就向所述 SP 提供第二请求的用户属性，且其中所述第一用户信息端点位于所述 WTRU 上，而所述第二用户信息端点位于

经由网络与所述 SP 通信的网络实体上。

具有本地功能的身份管理

[0001] 相关申请的交叉引用

[0002] 本申请要求享有2012年1月20日提交的美国临时专利申请No.61/589,125的权益，该申请的全部内容通过引用结合于此。

背景技术

[0003] 移动设备越来越多地用于接入因特网服务。因特网服务通常需要安全交易来保护敏感数据。这种安全性测量通常以数据需求（例如，用户名、个人身份号码(pin)、和/或密码）的形式给用户造成身份和认证负担。无线电信网络可以实施各种形式的认证。服务提供方也可以寻找各种用户属性来认证用户、识别用户、和/或确定用户的接入网络服务的等级。

[0004] 已经提出了单点登录(SSO)方案，该方案旨在为用户减少繁琐的用户认证。开放ID协议是使单点登录成为可能的协议中的一个示例。开放ID2.0协议和较新的开放ID连接协议是最普遍的开放ID协议。在下文中，单独的术语“开放ID协议”意味着涵盖各种形式的开放ID协议中的任意一者，包括开放ID2.0和开放ID连接。如果要讨论特定的协议，其将被专门标识出。

[0005] 当前用于SSO的方法（例如，开放ID协议）通常需要网络身份提供方实施各种SSO机制。这些方法可给定用户对他/她的身份信息的有限的控制，因为所述身份信息由SSO身份提供方处理，并可导致易受安全性攻击的用户数据和通信。

发明内容

[0006] 在此描述了用于对用户设备(UE)实施身份管理机制（例如与开放ID连接协议相关联的机制）的系统、方法和装置。在示例实施方式中，用户设备(UE)和服务提供方(SP)可以经由网络通信。UE的用户可以请求接入由SP提供的服务。该SP可以请求身份(ID)令牌来认证用户和/或UE的身份。UE可以根据请求创建ID令牌。例如，所述ID令牌可在位于UE内的可信环境中被安全地创建。这种可信环境可由通用集成电路卡(UICC)、可信模块、安全环境等等、或者上述的任意合适的组合来实施。经由可信环境，UE例如可以向SP发出ID令牌。该ID令牌可以被验证以为UE提供对由SP提供的服务的接入。该UE还可以响应于接收到由用户批准的授权请求来创建接入令牌。所述接入令牌可与由UE从SP请求的服务相关。因此，接入令牌可与授权请求的用户批准相关联。例如，SP可以发出授权请求以接收关于用户的附加信息，例如用户属性。该UE可以向SP发出接入令牌，并且一旦验证了所述接入令牌，该SP可以接收其所请求的用户属性。ID令牌和接入令牌可以根据开放ID连接协议在UE处生成。例如，所述令牌可以在位于UE内的可信模块中被安全地生成。

[0007] 在另一个示例实施方式中，UE可以提供与由SP请求的服务相关的接入令牌。这种接入令牌可以由提供所请求的服务的SP来兑换(redeem)。UE可以响应于接收到对用户数据的请求来生成接入令牌。接入令牌可以包括指示用户信息端点的位置的信息。例如，

SP 可以使用该位置来从所述用户信息端点取得用户数据。一旦验证了接入令牌，用户信息端点可以向 SP 提供所请求的用户属性。用户信息端点可以位于 UE 内的可信模块、经由网络与 SP 通信的网络实体、或者上述的组合上。例如，UE 可以创建与服务和 UE 的用户相关联的第一接入令牌和第二接入令牌。所述第一接入令牌可以包括指示第一用户信息端点的位置的信息，其中一旦验证了第一接入令牌，该第一用户信息端点向 SP 提供第一请求的用户属性。所述第二接入令牌可以包括指示第二用户信息端点的位置的信息，其中一旦验证了第二接入令牌，该第二用户信息端点向 SP 提供第二请求的用户属性。所述第一用户信息端点可以位于 UE 上，例如，位于可信模块上，而所述第二用户信息端点可以位于经由网络与 SP 通信的网络实体上。例如，由所述第一用户信息端点提供的所述第一请求的用户属性可以由用户分类为机密数据，而由所述第二用户信息端点提供的所述第二请求的用户属性可以由用户分类为非机密数据。为了服务 UE/ 用户，SP 可以将具有不同安全性类别且从他们各自的用户信息端点获取的第一和第二用户属性合并。

[0008] 在替换实施方式中，除了 SP 之外或在 SP 之外，接入令牌能够由接收该令牌的其他方 (party) 进行兑换。

附图说明

[0009] 更详细的理解可以从下述结合附图并且举例给出的描述中得到，其中：

[0010] 图 1 是示出了网络中的示例接口的框图；

[0011] 图 2 是根据示例实施方式的具有 HTTP 重定向消息的开放 ID 协议的流程图；

[0012] 图 3 是示出了根据开放 ID 连接协议的示例实施的示例性发现过程的流程图；

[0013] 图 4 是示出了用于取得配置信息的示例性协议流的流程图；

[0014] 图 5 是示出了示例性注册协议流的流程图；

[0015] 图 6 是开放 ID 连接协议的示例实施的流程图；

[0016] 图 7 是使用授权请求的示例开放 ID 连接呼叫流的流程图；

[0017] 图 8 是根据示例实施方式的具有本地令牌创建的示例呼叫流的图示；

[0018] 图 9 示出了根据示例实施方式的具有共享预建立的共享机密 S 的本地 OP 的示例协议流的流程图；

[0019] 图 10 是根据示例实施方式的开放 ID 协议的呼叫流，其中用户信息端点在本地位于 UE 上；

[0020] 图 11 是根据示例实施方式的开放 ID 协议的呼叫流，其中用户数据在本地被存储，并且用户数据存储在网络实体上；

[0021] 图 12A 是可以在其中实施一个或多个所公开的实施方式的示例通信系统的系统图示；

[0022] 图 12B 是可以在图 12A 示出的通信系统内使用的示例无线发射 / 接收单元 (WTRU) 的系统图示；以及

[0023] 图 12C 是可以在图 12A 示出的通信系统内使用的示例无线电接入网和示例核心网的系统图示。

具体实施方式

[0024] 下面详细的描述被提供以对示例性实施方式进行说明，并且不意图限制本发明的保护范围、应用性或配置。可以对元件和步骤的功能和排列作出各种修改，而不背离本发明的精神和保护范围。

[0025] 在此描述了用于管理用户和/或用户设备(UE)的身份的各种方法和系统。尽管此处的实施方式是按照开放ID连接协议的上下文进行描述的，但实施方式不限于实施开放ID连接协议，并且可以例如实施其他单点登录(SSO)协议和/或联邦身份协议。类似地，尽管在此将开放ID实体用作参考，但实施方式不限于开放ID实体，并且所述开放ID实体可扩展成执行与开放ID实体相同或类似的功能的其他实体。例如，如在此处所使用的，术语中继方(RP)和客户端可指服务提供方(SP)，例如，服务网站。术语开放ID身份提供方(OP)和授权服务器可指网络身份提供方(IdP)或认证端点(AEP)。术语用户设备(UE)可指任意合适的无线发射/接收单元(WTRU)，如在此进一步描述的。

[0026] 在一个示例实施方式中，认证端点(例如，OP服务器)的认证功能可以由位于UE内的本地安全性模块来实施。例如，移动设备的本地代理(例如，诸如安全性模块、可信模块等之类的可信环境)可以用作网络侧身份提供方的代理。本地安全性模块可以用于执行可认证和/或授权UE的终端用户的功能。本地安全性模块可以被称作本地身份提供方，并且可以用于基于开放ID协议(例如，开放ID连接)来认证终端用户。术语本地开放ID可以用于指示本地SSO实施的子集，其中SSO的实施和/或身份管理是根据开放ID协议的(例如，开放ID连接)。例如，本地开放ID可以用于指示可由位于本地的实体或可信环境执行的OP的功能。本地OP是可用于指示在本地位于设备上执行开放ID服务器(例如，授权服务器)的功能或功能的子集的实体或模块的术语。

[0027] 根据示例实施方式，本地OP可以使用基于令牌的协议流。这种令牌可以被发出至SP(例如，RP)。令牌可用于从身份提供方和/或从用户信息端点取得关于用户的信息(例如，属性)。如在此所使用的，用户属性可指与用户相关联的任意信息元素。示例用户信息(例如，属性)包括而不限于用户的年龄和地址，并且这种属性可由SP使用令牌来取得。例如，SP可以使用令牌来取得信息，而无需该令牌携带该信息。

[0028] 在此描述的实施方式可以使用令牌来进行认证。可以使用诸如URL和/或电子邮件地址之类的各种标识符。诸如开放ID连接的认证协议可以便于用户属性和/或身份信息的安全交换。

[0029] 图1示出了说明根据示例实施方式的示例通信接口的框图。移动设备(例如，UE100)可以连接至因特网，而在公共因特网上不是可直接寻址的。在示例场景中，UE100和在该UE100上运行的服务和/或应用不能由外面的实体(例如，网络服务提供方102)到达。UE100上的本地服务(例如，本地OP104)可以经由UE100上的浏览器106到达，和/或通过移动网络运营商(MNO)108的管理后台系统来到达。例如，如果本地OP104由MNO108发出并安装在SIM卡上，本地服务可以经由空中(OTA)管理来接入。例如，诸如服务提供方102之类的一些网络服务可直接与在UE100上运行的服务通信。

[0030] 在其中UE100经由MNO网络108连接至因特网的示例配置中，可以根据图1示出的实施方式来标识示例性通信路径/接口。在接口(IF)112处，UE100中的浏览器106可例如通过使用HTTP(S)请求来联系基于网络的服务(例如，SP102)。所述SP102可以对HTTP(S)请求进行应答，和/或发送响应至浏览器106。在示例场景中，SP102可在接收到请求之前

不发起与浏览器 106 的通信。IF114 可用于浏览器 106 和内部本地 OP104。浏览器 106 可以例如经由 HTTP(S) 和 / 或经由中间件软件实体（例如，Java 小程序 (applet)、Javascript 小部件 (widget)、OS API 等）与位于 UE100 内的本地 OP104 通信。本地 OP104 可以例如使用 HTTP 响应对来自浏览器、应用和 / 或 API 的请求进行响应。在示例配置中，本地 OP104 可在接收到请求之前不发起与浏览器 106 的通信。

[0031] IF116 可以被称作反向信道。使用该反向信道 116，SP102 可以联系 IdP 服务器 110（例如，使用 HTTP），和 / 或 IdP 服务器 110 可以联系服务提供方 102（例如，使用 HTTP）。在不涉及浏览器 106 或用户设备 100 的情况下，经由 IF116 的通信可以发生。IF118 可用于 IdP110 和 MNO 网络 108。正如图 1 中的椭圆虚线所指示的，IdP110 可以是独立的，或者可以是 MNO 网络 108 的一部分。IdP 服务器 110 可以由 MNO 网络 108 的内部实体到达（例如，使用 HTTP 和 / 或专有接口）。IdP 服务器 110 可以能够与 MNO 网络 108 的内部实体通信。在示例配置中，IdP 服务器 110 是否可以与 MNO 网络 108 的内部实体进行通信可以取决于 MNO 防火墙规则和 / 或策略。IF120 可以被称作空中 (OTA) 管理接口 120。该 OTA 接口 120 可用于 MNO 网络 108 和本地 OP104。例如，MNO 网络 108 中的实体可使用该 OTA 管理接口 120 来与 UICC/SIM 卡上的应用通信。从本地 OP104 的应用到 MNO 网络 108 上的实体的连接可受制于 MNO 防火墙规则。取决于本地 OP104 和 / 或 IdP110 的应用的所有权，IF122 可用于或不可用于本地 OP104 和 / 或 IdP 服务器 110。例如，在 IF122 的两个实体（例如，本地 OP104 和 IdP110）之间的直接通信信道（例如，使用 SMS、OTA 等）可以在两个实体由 MNO 运营和 / 或所有时建立、和 / 或征得 MNO 的同意来建立。在示例配置中，MNO 可以启用在 IF122 处的通信信道。通信 IF124 在 SP102 和本地 OP104 之间不可用。例如，在 UE100 不是可公共寻址的时，从服务提供方 102 到 UE100 或在该 UE100 上运行的本地 OP 服务 104 的直接通信不可用。IF126 可用于浏览器 106 和 IdP110。例如，浏览器 106 可经由 HTTP 请求到达 IdP110。该 IdP 服务器 110 可以对浏览器 106 的 HTTP 请求进行响应。

[0032] 接口可用性（例如，经由 IF122 通信的能力）可取决于通信端点和 / 或所述端点之间的通信路径的控制。在示例配置中，IF122 在 OP110 和本地 OP104 处于 MNO 的控制下时是可用的，以及 OP110 和本地 OP104 之间的通信通过 SP102 和本地 OP104 之间的物理通信路径来实现。

[0033] 在示例实施方式中，本地 OP104 可以向 SP102 发出令牌。该令牌可由 SP102 授予 (present) 给网络 IdP/OP110。这种令牌可用于取得数据。在其中通信接口不可用于 SP102 向本地 OP104 授予令牌的示例配置中，网络 IdP/OP110 可以验证该令牌是否由合法的本地 OP104 发出。IdP/OP110 还可以确定所述令牌是否有效。例如，确定令牌是否有效可包括验证所述令牌是否已经期满。

[0034] 仍然参考图 1，从 SP102 到本地 OP104 的间接通信可以经由 UE100 的浏览器 106 通过重定向消息的方式来进行。SP102 可以发送包括 URL 的 HTTP3xx 消息以重定向浏览器 106。例如，根据开放 ID 协议，URL 可以是对应于 IdP 认证端点 (AEP) 的 URL。SP102 可例如通过发现机制来获知 IdP 认证端点。UE100 可以将 URL 解析成 AEP 的服务器的网际协议 (IP) 地址。例如，具有安装在 UE100 上的本地 OP104 的 UE100 可以将 URL 解析成本地 OP 服务器 104 的本地 IP 地址。

[0035] 图 2 是示出了示例 HTTP 重定向消息的流程图。图 2 所示的信息流可使用可在实施

开放 ID 协议时使用的间接通信来实施。UE 的浏览器 202 可通过请求接入由 SP204 提供的服务来发起与 SP204 的通信。该请求可包括用于接入服务的 HTTP 请求。在 206 处，SP204 可对该请求进行响应，并且可发送数据至本地 OP200，作为在 206 处的重定向消息的一部分（例如，数据可在 HTTP 消息的参数中被传递）。在 208 处，浏览器 202 可以解析成本地 OP200 的本地地址。浏览器 202 可以通过在 210 处发送消息来跟随其在 206 处接收到的重定向消息至本地 OP200。例如，浏览器 202 可经由对 DNS 查找和 / 或助手软件（例如，Java 小程序）的修改来跟随所述重定向。例如，URL/ 地址的 DNS 解析可经由主文件来进行，和 / 或可由 Java 小程序请求者 (supplicant) 来促进。在 212 处，本地 OP 操作可以发生。例如，在 212 处，UE 的用户可与该 UE 一起被认证。在 214 和 216 处，本地 OP200 可例如经由可发送浏览器 202 至 SP204（在 216 处）的另一个重定向（在 214 处）将信息传递到 SP204。信息和 / 或数据可以在 HTTP 消息的参数中被传递。在示例配置中，从 SP204 到本地 OP200 的直接通信不可用。

[0036] 开放 ID 连接协议使得各种类型的客户端（例如，基于浏览器的、移动和 / 或 javascript 客户端）能够请求和接收关于身份和认证会话的信息。在开放 ID 连接的各种示例实施中，身份数据可以被加密，OP 可以被发现，以及高级会话管理（例如，退出）可以被启用。在开放 ID 连接的示例实施中，用户标识符可以基于电子邮件地址和 / 或 URL。例如，在从用户获得授权（例如，经由基于开放授权 (OAuth) 的呼叫流）时，服务提供方可以被允许访问用户拥有的内容和 / 或简档数据。

[0037] 根据开放 ID2.0 协议的示例实施，客户端机密（例如，在身份提供方 (IdP/OP) 和 SP/ 客户端之间的共享机密）可以针对每个用户来建立（例如，按照认证协议运行）。该共享机密可以在发现过程期间在 OP 和服务之间建立。例如，该共享机密可以从长期机密中取得，和 / 或其可以通过本地 OP 实例来计算。根据开放 ID 连接协议的示例实施，客户端机密可以包括令牌。例如，身份 (ID) 令牌可由 OP 进行签名，并且客户端可验证该令牌（例如，在 OP 提供的令牌端点的帮助下）、和 / 或该客户端可独立地验证该令牌签名。在示例实施方式中，OP 可在发现和 / 或注册过程期间提供密钥。例如，在发现之后，可在客户端和 OP 之间执行注册。在示例配置中，注册协议步骤可不特定于用户。例如，密钥可用于对令牌进行签名，并且该密钥可以是用于多个用户的通用密钥。在示例实施方式中，令牌及其签名可由本地 OP 创建。例如，密钥可用于本地 OP，并且该 OP 可使用所述密钥来创建签名。

[0038] 图 3 示出了根据开放 ID 连接的示例实施的示例发现过程。可被称作 SP 的客户端 300 可以寻找开放 ID 身份提供方 302 的信息（例如，端点 URL）。获得令人满意的 (sought-after) 信息的过程可以被称作发现。SP 可以获知提供方信息（例如，经由带外机制），并因此可以跳过根据开放 ID 协议的示例实施的发现。在另一个示例实施中，客户端 300 可以使用简单网络发现 (SWD) 来发现信息。在 SWD 中，例如，在 306 处，UE 的用户可以向客户端 300 提供用户的标识符。该用户可以被称作委托人。在 306 处，客户端 300 可以识别所述标识符的主机。该主机可指拥有 (host)SWD 服务的服务器。委托人和 / 或主机信息可由终端用户在所述标识符中提供。所述标识符可以例如是 XRI、电子邮件、URL 等等。在 306 处，客户端 300 可以向用户提供的标识符施加标准化和 / 或提取规则，以确定委托人和 / 或主机。参考图 3，例如，委托人可指电子邮件，而主机可指在提供的电子邮件地址中“@”的右边的每一项内容。在 308 处，客户端 300 可以使用 HTTP 获得 (HTTP GET) 请求从提供

方 302 请求位置（例如，URL）。在 310 处，OP302 可以返回包括位置信息（例如，认证端点和 / 或授权端点的地址）的信息。

[0039] 作为发现的一部分，客户端 300 可以取得配置信息（例如，参见图 4）。在 400 处，客户端 300 可以请求配置信息。这种配置信息在开放 ID 提供方 302 处（例如，在公知的 URL/ 可指向 JSON 文档的开放 id 配置处）可用。可使用 TLS 来保护通信。在 402 处，作为对请求的响应，开放 ID 提供方 302 可以返回可包括关于开放 ID 提供方 302 的配置的属性（例如，信息）的 JSON 文档。所述信息可例如包括关于端点的信息和 / 或公共密钥位置信息。例如，端点信息可包括 :认证和 / 或授权端点的 URL ;令牌端点的 URL ;用户信息 (User Info) 端点的 URL ;和 / 或校验 ID 端点的 URL。JSON 网络密钥文档可以包括提供方的 JSON 网络密钥 (JWK) 文档的 URL。所述 JWK 文档可以具有 JSON 结构，该 JSON 结构可以提供一组公共密钥。这种密钥可用于对 JSON 网络令牌（例如，ID 令牌）进行签名。

[0040] 图 5 示出了根据开放 ID 连接协议的示例实施的示例注册过程。客户端 300 可以向开放 ID 提供方 302 注册，以获得客户端 ID 和 / 或客户端机密。在 500 处，客户端 300 可以发出请求至发现的提供方 302 的注册端点。在 502 处，可以向客户端 300 发出响应。该响应可以包括 JSON 文档。所述 JSON 文档可以包括客户端 ID 和 / 或客户端机密。TLS 可用于保护通信。

[0041] 继续参考图 5，客户端机密可以在注册期间、在客户端 /SP300 与 IdP302 之间建立。所述客户端机密可以用作针对可等待执行授权码流的客户端的认证凭证。在授权码流中，在客户端请求接入令牌时或在客户端想要刷新接入令牌时，客户端可以使用客户端机密来向提供方的令牌端点进行认证。根据示例实施，HMAC 签名可用于对 ID 令牌进行签名。在这种实施中，客户端机密可用作签名密钥。RP 可试图使用其存储的客户端机密，例如以在 HMAC 被用作签名机制的情况下验证令牌签名。例如，HMAC 对称签名可由本地 OP 使用。所述本地 OP 可获知用于 SP 的客户端机密，例如以创建 HMAC 签名。

[0042] 在用户登录客户端时可以执行或不执行注册。在开放 ID 连接协议的示例实施中，客户端机密可以根据服务和 IdP 来建立，以使服务可以具有其自己与 IdP 的客户端机密。在开放 ID2.0 协议的示例实施中，相关联的机密可以针对服务与 IdP 之间的每个用户认证过程来创建。例如，所述相关联的机密可以用于对身份声明消息进行签名，并且客户端可以验证该签名。在示例开放 ID 连接实施中，客户端机密可以是客户端认证凭证。因此，相关联的机密的作用可以由 ID 令牌上的签名来实施。ID 令牌上的签名可例如使用提供方 JWK 密钥来创建。

[0043] 根据开放 ID 连接协议的示例实施，发现和注册过程可以在 SP 与网络上的 IdP 之间进行，以使客户端机密和 / 或在两个实体之间交换的其他信息的可用性可以被限制到 SP 和网络 IdP。

[0044] 在开放 ID 连接协议的各种示例实施中，ID 令牌可以用作 OAuth 接入令牌。例如，ID 令牌可以在 OP 处用认证数据（例如，用户标识符）来交换。该 ID 令牌可以携带编码后的数据。对接入令牌的请求可以允许服务提供方访问用户标识符和 / 或附加简档数据（例如，诸如地址、年龄等之类的用户属性）。例如，ID 令牌的数据格式可以是可包括 JSON 数据的 JWT。

[0045] 在此描述的实施方式可以使用例如 ID 令牌和 / 或接入令牌之类的各种令牌类型。

这种令牌可以根据开放 ID 连接协议来实施。例如，ID 令牌可以包括关于认证事件的信息，并且可以使得服务提供方能够验证用户是否已经在 IdP 处被认证。为了启用验证，例如，ID 令牌可以包括编码后的数据。接入令牌可以例如是 OAuth 承载令牌。接入令牌可以允许接收服务来兑换令牌（例如，在用户信息端点处）。服务提供方可以兑换接入令牌，例如以接收用户信息（例如，用户属性 / 要求）。服务提供方可以使用 ID 令牌来认证用户。在示例实施方式中，服务可以请求接入令牌来取得未被包括在 ID 令牌中的附加数据。例如，服务提供方可以请求接入令牌来从端点获得数据。

[0046] 根据开放 ID 连接协议的示例实施，ID 令牌可以具有 JWT 格式。JWT 可以包括例如用户的实际认证的 JSON 属性。例如，ID 令牌可以包括可被编码为 JWT 的下列数据：

[0047] iss——这可指响应的发出者的唯一标识符；

[0048] user_i——这可指用户本地唯一和 / 或从未重分配的标识符，其旨在由客户端来使用（例如，24400320 或 AItOawmwtWwcT0k51BayewNvutrJUqsvl6qs7A4）。根据示例实施，其长度不可超过 255 个 ASCII 字符；

[0049] aud——这可指 ID 令牌所预期的听众 (audience)。例如，“aud”可以是 RP 的 OAuth 客户端 _id(client_id)；

[0050] exp——这可以包括整数和 / 或可以标识期满时间，其中在该期满时间时或之后 ID 令牌可以被接受以进行处理。该参数的处理可以取决于当前日期 / 时间是否在值中所列出的期满日期 / 时间之前。例如，考虑到时钟偏移，实施者可以提供余地。所述值可以是从在 UTC 中测得的 1970-01-01T0:0:0Z 直到所期望的日期 / 时间的秒数；

[0051] iso29115——这可提供实体认证保证。例如，该数据参数可以指定所执行的认证的实体认证保证等级；以及

[0052] nonce——如果授权请求包括随机请求值，则该值可以被设定为与所述请求值相同的值。

[0053] 下面示出了根据开放 ID 连接协议的示例实施的 ID 令牌的示例内容。该示例 ID 令牌可以从客户端发送至校验 ID 端点。下面的部分示出了从服务到端点的示例请求，其中所述请求包括示例令牌：

[0054] POST/id_token HTTP/1.1

[0055] 主机 (Host):server.example.com

[0056] 内容 - 类型 (Content-Type):application/x-www-form-encoded

[0057] id_token = eyJ0eXAiOiJKV1QiL

[0058] 下一部分示出了可由端点返回至服务提供方的示例令牌的 (JSON) 内容的示例：

[0059] HTTP/1.1200OK

[0060] Content-Type:application/json

[0061] {

[0062] "iss":"http://server.example.com",

[0063] "user_id":"248289761001",

[0064] "aud":"http://client.example.com",

[0065] "exp":1311281970

[0066] }

[0067] 示例令牌可以使用 JSON 网络签名 (JWS) 和 / 或 JSON 网络加密 (JWE) 来被签名和 / 或加密。用于签名和 / 或加密的密钥可以例如是 JSON 网络密钥。

[0068] JWT 中的属性可以被编码为 JSON 对象。JWT 可以是具有要素 (component) 的组合的字符串。示例要素包括 JWT 报头分段、JWT 属性分段、以及 JWT 加密分段。JWT 报头分段可以包括可描述被应用至报头和属性分段的加密操作的基础 64url*(base64url*) 编码的 JSON。JWT 属性分段可以包括对属性进行编码的 base64url* 编码的 JSON 对象。JWT 加密分段可以包括保护 JWT 报头和属性分段的内容的 base64url* 编码的加密材料。示例性基础 64 编码可以移除尾随的“＝”字符。

[0069] 在开放 ID 连接协议的示例实施中，令牌上的签名可以是有效的 JSON 网络令牌签名 (JWS)。使用 JWS 的签名令牌可以具有包括关于签名算法的信息的报头，和 / 或可以包括指向用于签名的密钥的指针。用于 JWS 的签名算法可以包括下列算法，但是实施方式并不限于下列签名算法：

[0070] HS256 HMAC 使用 SHA-256 哈希算法；

[0071] HS384 HMAC 使用 SHA-384 哈希算法；

[0072] HS512 HMAC 使用 SHA-512 哈希算法；

[0073] RS256 RSA 使用 SHA-256 哈希算法；

[0074] RS384 RSA 使用 SHA-384 哈希算法；

[0075] RS512 RSA 使用 SHA-512 哈希算法；

[0076] ES256 ECDSA 使用 P-256 曲线 (curve) 和 SHA-256 哈希算法；

[0077] ES384 ECDSA 使用 P-384 曲线和 SHA-384 哈希算法；和 / 或

[0078] ES512 ECDSA 使用 P-521 曲线和 SHA-512 哈希算法。

[0079] 如上所示，基于所选择的签名算法，例如可以支持不同的密钥类型。在示例实施中，RP 可以选择自己验证 ID 令牌上的签名，因此，RP 可能需要获知验证密钥。指向所述密钥的指针可以是报头的一部分。例如，所述指针可以是 jku(例如，JSON 网络密钥 URL) 参数，其可以包括指向一组 JSON 编码的公共密钥的 URL。在示例实施中，x5u 参数可以包括指向 X.509 公共密钥证书或证书链 (例如，对应于所述密钥) 的 URL。报头参数可以由创建令牌和令牌签名的实体设置。如果 HMAC 签名被用于对 ID 令牌进行签名，客户端机密可以被用作签名密钥。示例接入令牌可以例如是 OAuth 承载令牌。示例接入令牌例如可以在用户信息端点处被使用，以获取用户信息 (例如，身份属性和 / 或用户信息)。

[0080] 服务提供方 (客户端) 可以独立地执行 ID 令牌的验证。例如，客户端可以验证令牌而无需联系发出 IdP 服务器。用于验证的密钥材料可以由客户端在发现过程中 (例如，在 JSON 网络密钥 URL 参数中) 接收。

[0081] 根据示例实施方式，服务提供方可以将 ID 令牌视为不透明的值，并且可以将他们递交至校验 ID 端点，以进行验证。在这种实施方式中，服务提供方可以从校验 ID 端点接收关于用户认证的信息。ID 令牌上的签名和 / 或加密可以例如使用 JSON 网络密钥。该密钥可经由注册中的 JSON 网络密钥参数和 / 或公共密钥 (例如，在 x5u 报头参数中引用的) 而可用于客户端。

[0082] 图 6 示出了根据开放 ID 连接协议的示例实施的示例呼叫流。图 6 中的示例呼叫流可以由例如尚未向 OP(例如，授权服务器 604) 注册共享机密的服务提供方 (例如，客户

端 602) 使用。在其中服务提供方尚未向身份提供方注册共享机密的示例开放 ID 连接实施中，服务提供方可以直接从身份提供方请求 ID 令牌，如图 6 的 610 处所示。

[0083] 在其中服务提供方已经向身份提供方注册了共享机密的另一个开放 ID 连接实施中，服务提供方可以跟随授权 (auth) 码流 (参见图 7)，其中服务提供方可以接收安全的授权码而不是令牌。所述授权码例如可以在身份提供方处用 ID 令牌进行交换。服务提供方可以使用预建立的共享机密 (例如，与身份提供方的) 以在用 ID 令牌兑换授权码时认证所述服务提供方。

[0084] 再次参考图 6，在用户 /UE600 请求接入由客户端 602 提供的服务时，客户端 602 可以不向授权服务器 604 注册机密。在 606 处，用户 600 可以通过使用开放 ID 标识符 (例如，电子邮件地址) 请求接入服务。所述标识符可以包括用户名和开放 ID IdP(OP) 的域。所述 OP 可以提供用于发现和认证的端点。在 608 处，客户端 602(服务提供方) 可以准备授权请求，并且可以将该请求发送至用户 600。所述请求可以包括期望的请求参数。在 610 处，授权请求可以使用 HTTP 重定向而被发送至授权服务器 604(例如，经由用户)。在 612 处，授权服务器 604 可以认证所述用户 600，并因此授权服务器 604 可以被称作认证端点 (AEP)。在示例配置中，授权服务器 604 可以认证用户 600，除非用户 600 已经被认证过并且该认证尚未期满。例如，用户 600 的当前认证状态可以为“真”，以使用户 600 不需要在 612 处进行重新认证。在 614 处，授权服务器 604 可以从用户 600 获取同意或授权，以允许令牌发出。在示例配置中，用户 600 可以建立可避免用户同意 / 授权的策略。例如，用户 600 可在先前的协议运行时点击“记住这个决定”复选框。在 616 处，令牌可以被创建，并且授权服务器 604 可以用接入令牌和 / 或 ID 令牌将用户 600 发送回至客户端 602(在 618 处)。在示例实施中，在 620 处，客户端 602 可以在校验 ID 端点 628 处确认所述 ID 令牌。在 622 处，客户端 602 可以接收具有用户的身份的 ID 令牌响应。在 624 处，客户端 602 可以例如使用接入令牌来接入用户信息端点 630。客户端 602 可以在接入所述用户信息端点 630 之后接收用户信息响应 (例如，所请求的用户属性)。

[0085] 参考图 7，服务提供方 (例如，客户端 702) 可已经向身份提供方 (例如，授权服务器 704) 注册了共享机密。在 706 处，用户 /UE700 可请求接入由客户端 702 提供的服务。在 706 处，该接入可以通过向客户端 702 提供用户 700 的标识符来被请求。这种标识符可以例如包括开放 ID 标识符。客户端 702 可以准备可包括所期望的请求参数的授权请求，并且在 708 处，该客户端 702 可以将所述请求发送至用户 700。在 710 处，客户端 702 可以使用 HTTP 重定向将所述请求发送至认证端点 (AEP)713(例如，授权服务器 704)(例如，经由用户 700)。在 704 处，如果用户 700 当前尚未被认证，AEP713(例如，授权服务器 704) 可以认证用户 700。在 714 处，如果已经获取了用户同意 / 授权的策略还未生效 (in place)，授权服务器 704 可以获取用户 700 的同意 / 授权。在 716 处，授权服务器可以创建授权 (auth) 码，并且可以在 718 处，使用授权码将用户 700 重定向至客户端 702。在 720 处，客户端 702 可以使用授权码在令牌端点 734 处请求声明。在 724 处，客户端 702 可以从令牌端点 734 接收所述声明。所述声明可以包括响应体中的接入令牌和 / 或 ID 令牌。在 725 处，客户端 702 可以例如在校验 ID 端点 736 处确认该 ID 令牌。在 728 处，客户端 702 可以从校验 ID 端点 736 接收 ID 令牌响应。这种 ID 令牌响应可以包括终端用户 700 的身份。在 730 处，客户端 702 可以例如使用接入令牌来接入用户信息端点 738。在 732 处，客户端 702 可以从

用户信息端点 738 接收用户信息响应。在示例实施中，服务提供方（例如，客户端 702）可以验证在步骤 718 中接收到的 ID 令牌，并且可以基于从所述 ID 令牌获取的身份信息来授权接入。在用户信息端点 738 处使用接入令牌来取得身份属性可以是客户端 702 的选择。

[0086] 在一个示例实施方式中，使得开放 ID 连接协议能够被实施的机制可以在 UE 上本地执行。例如，用户可以被本地认证，对应于用户的身份属性可以被本地管理，由用户对身份属性的释放可以被本地授权，以及用户信息端点可以在本地位于 UE 上。在示例实施方式中，诸如本地 OP 之类的本地可信环境可以安全地认证用户、从用户获取授权、和 / 或创建令牌。在本地创建的令牌可以例如由服务提供方 (SP) 使用，以从各个端点取得用户认证数据和 / 或用户身份信息（例如，属性）。如在此所描述的，令牌可以包括用于网络身份提供方 (IdP) 验证所述令牌是否已经由授权的 UE 和 / 或授权的本地 OP 发出并且所述令牌是否已经期满的信息。为了确定令牌是否已经期满，例如，令牌可以在用户认证之时被标记时间戳。

[0087] 图 8 示出了根据示例实施方式的其中令牌可以在本地被创建的示例协议流的流程图。在 806 处，UE（例如，设备 800）可以请求接入由服务提供方 802 提供的服务。请求可以包括设备 800 的用户的标识符。在 808 处，服务提供方 802（客户端）可以经由重定向消息从设备 800 请求令牌。因此，UE 可以接收对令牌的请求，其中所述对令牌的请求响应于对接入由服务提供方提供的服务的请求。在 808 处的请求可以包括对根据开放 ID 连接协议的 ID 令牌的请求。在 808 处的请求可以包括对根据开放 ID 连接协议的接入令牌的请求。例如，接入令牌可以由服务提供方 802 请求，以使服务提供方能够取得设备 800 的用户的属性。属性可与用户的身份相关。例如，如果服务提供方 802 确定其不需要附加的属性或用户信息，服务提供方 802 可以决定不对接入令牌进行请求。

[0088] 仍然参考图 8，在 810 处，用户可以给出对设备 800 向服务提供方 802 发出令牌的同意（批准）。例如，接入令牌可以表示可允许服务提供方 802 访问来自用户信息 (info) 端点的指定的一个或多个属性的同意（例如，由用户给定）。例如，在本地生成的接入令牌可以包括可允许用户信息端点识别其中访问已经被授权的指定属性的数据。例如，如果服务提供方 802 请求访问多个属性，并且用户同意授权访问（在 810 处）所请求的属性中的一些，根据示例实施方式，用户信息端点可以释放授权的信息，并且可以不释放尚未由用户授权的属性。

[0089] 例如，UE（例如，设备 800）可以接收对用户数据的请求，并且可以接收对释放用户数据的同意部分的用户同意。响应于所述用户同意，设备 800 可以生成可与服务提供方 802 相关联的接入令牌。设备 800 可以向服务提供方 802 发出接入令牌，其中一旦验证了接入令牌，所述用户数据的同意部分被释放至服务提供方 802。所请求的用户数据可以包括多个用户属性，其中所述多个用户属性中的至少一者不是被释放的所述用户数据的同意部分的一部分。如在此进一步描述的，根据示例实施方式，用户信息端点可以位于设备 800 内，并且接入令牌可以在这种用户信息端点处被接收。响应于接收到所述接入令牌，设备 800 可以向服务提供方 802 提供所述用户数据的同意部分。

[0090] 在 812 处，令牌可以在设备 800 上创建。例如，响应于对令牌的请求，设备 800 可以根据对所述令牌的所述请求来创建身份令牌。在示例实施方式中，令牌可以在位于设备 800 内的可信环境（例如，本地 OP）上被安全地创建。在 812 处，接入令牌可以在设备 800

上生成。这种接入令牌例如可以包括允许网络实体确定哪个或哪些属性可由服务提供方802取得的信息。在814处，该令牌可以发向服务提供方802。例如，身份(ID)令牌可以经由UE(例如，设备800)被发出，其中所述ID令牌被验证以提供UE对服务的接入。例如，在820处，服务提供方802可以验证令牌(例如，ID令牌)。在示例实施方式中，服务提供方802可以校验ID令牌上的签名，以验证该令牌是否有效。用于验证的密钥材料可已由服务提供方802在发现过程中(例如，在JSON网络密钥URL参数中)接收。在服务提供方802确认该ID令牌签名之后，服务提供方802可以校验在ID令牌中编码的字段，以进一步确认所述ID令牌。例如，“iss”(发出者)字段可以包括令牌发出者的唯一标识符，例如SP根据用户提供的标识符发现的IdP的唯一标识符。“aud”(听众)字段可以识别令牌所期望的听众。因此，听众字段可以包括服务提供方802的客户端_id。“exp”(期满)字段可以标识期满时间，其中，在该期满时间之后，令牌不被接受。在具有期满时间的示例配置中，如果当前时间在“exp”日期和时间之后，对应的ID令牌已期满。服务提供方可以验证和确认所述ID令牌是否已经期满。

[0091] 在816处，用户信息端点(例如，网络IdP)可以被授予接入令牌。该接入令牌可以包括来自步骤810的同意信息。在示例实施方式中，服务提供方(SP)802可以将接入令牌视为不透明的值。这种接入令牌可以被称作不携带签名的不透明的承载令牌。在816处，接入令牌可以针对各个令牌端点来使用以取得用户属性和/或其他信息。令牌例如可以包括设备800的标识符(例如，设备800的本地OP的标识符)。这种标识符可以通知网络IdP804该发出设备800或发出本地OP的唯一身份。设备800和/或设备800的本地OP的这种标识符可以被包含在令牌的签名中。在822处，例如，所述标识符可以允许网络IdP804识别和确认由本地OP发出的令牌。标识符可以允许令牌创建和令牌验证在至少两个不同的实体中发生，如图8所示。例如，网络实体(例如，网络IdP804)可能被要求经由令牌验证端点822来验证令牌。该端点822可以根据在上面描述的用于验证ID令牌的示例步骤来验证接入令牌。网络IdP804可以将验证的结果返回至服务提供方802。在服务提供方802接受ID令牌并信任其内容之前需要成功的验证。例如，服务提供方可以不信任电子邮件地址属于当前会话的用户，直到令牌被验证。一旦成功验证，服务提供方802可以采取行动，例如，将经验证的用户添加到其用户数据库，允许接入其提供的服务等等。

[0092] 在其中本地OP发出令牌的示例实施方式中，本地OP可以获知机密以对令牌进行签名。例如，本地OP可以获知已经被提供给在发现过程中向IdP注册的服务提供方的机密。如在此处所描述的，服务提供方可以发送令牌(例如，ID令牌)至校验ID端点。该端点可以解码JWT编码和/或可以验证签名。在示例配置中，服务提供方可以验证ID令牌而不是校验ID端点(例如，参见图8的820)。例如，ID令牌JWT可以用JWK密钥进行签名。例如，作为利用身份提供方的发现过程的结果，该密钥对于服务提供方是已知的。

[0093] 在此所描述的设备的各种实施方式可以在本地创建令牌(例如，通过本地OP)。例如，本地OP可以获知机密来创建令牌签名。在示例实施方式中，HMAC签名可以被使用。例如，本地OP可以具有对包括针对服务的客户端机密的列表的接入。该列表例如可以由MNO(例如，使用OTA信道)维持、更新和/或管理。

[0094] 根据使用HMAC签名的另一个实施，本地OP可以例如使用听众字段，和/或可以查询MNO服务端点(例如，通过安全通信信道)，以从网络IdP获得相应的机密。例如，查询提

供方的 JSON 网络密钥文档的 URL 可以获得密钥的标识符。本地 OP 可以做出安全的和 / 或经认证的请求，以获得密钥材料。请求可以例如通过引入通信步骤和 / 或通过可独立于用户认证的协议运行（例如，在低利用率的时候密钥材料的加载）而在认证时发生。

[0095] 在另一个示例实施方式中，机密可以从共享机密 S 和 / 或听众字段内容中得出。例如，本地 OP 可以计算客户端密钥。密钥推导功能可以由网络 IdP 使用，例如以计算客户端机密（例如，基于长期机密 S）。客户端机密可以与本地 OP 实例共享。在发现过程中，例如，网络 IdP 可以使用 KEF 来计算客户端机密。本地 OP 可以计算相同的客户端机密。

[0096] JSON 网络签名 (JWS) 可以允许为所签名的 JWT 使用报头字段。例如，报头字段可以用于传达关于密钥的信息，例如，已经用于签名的信息。“jku”参数可以指向可拥有公共密钥的 JSON 网络密钥 (JWK)URL。“kid”密钥 id 参数可以指示哪个密钥可能已经被使用。在替换的实施方式中，报头可以包括字段“x5u”，其可指向 URL（例如，用于 X.509 公共密钥证书）。网络中的 OP 可以为一个或多个本地 OP 实例创建密钥和 / 或证书，和 / 或可以为服务 / 客户端提供 URL，例如以提取公共密钥证书。本地 OP 可以包括私有密钥，和 / 或可以包括指向 URL 的指针，例如指向针对 JWS 的报头中对应的公共密钥证书的 URL。在示例实施方式中，本地 OP 可以根据 JWT 来对 ID 令牌进行编码，可以应用签名，并且可以发送该 ID 令牌至服务提供方。

[0097] 本地 OP 可以配备有密钥对。例如，私有密钥可以被安全地存储（例如，在本地 OP 中）。网络 OP 可以获知公共密钥，并且可选地，可以获知针对该公共密钥所对应的证书。网络 OP 可以用作证书管理机构 (CA)，并且可以自己创建证书，或者网络 OP 可以获得经证明的公共密钥（例如，来自第三方 CA）。在其中本地 OP 配备有密钥对的示例实施方式中，用户可希望访问服务提供方（例如，于第一时间内），并且可以进入电子邮件地址。服务提供方可以提取用户名和 / 或 OP 主机，和 / 或可以执行发现和 / 或注册步骤。例如，服务提供方（例如，网站）可能之前未被用户和 / 或 OP 观测到。服务提供方（客户端）可向网络 OP 进行注册，并且该网络 OP 可以提供包括经证明的公共密钥列表的 JWK URL。所述服务提供方可以例如使用对 ID 令牌和 / 或用于一个或多个属性的接入令牌的请求来将用户代理（例如，浏览器）重定向至授权服务器。

[0098] 设备的内部路由可以使得用户代理可以被定向到本地 OP 实例。本地 OP 可以在本地认证用户。在示例实施方式中，本地 OP 可以提取所请求的属性（例如，要求），和 / 或可以校验用户属性的可用性。所请求的属性在网络中可用或不可用。例如，本地 OP 可以获得用户同意（例如，授权）以创建接入令牌。授权可以给定服务提供方到所请求的属性的至少一部分的接入。用户在之前可已经被给予释放数据的同意（例如，通过点击“始终同意释放”复选框）。这种同意可以被存储，例如，以由于未来的决定。本地 OP 可以创建 ID 令牌，并且可以例如通过使用私有密钥来对令牌进行签名。证书的 URL 可以被放入令牌的 JWS 报头的 x5u 字段中。本地 OP 可以创建接入令牌并且可以向其应用签名。接入令牌可以由服务提供方视为不透明的值，并且可以不包括数据。接入令牌可以被兑换（例如，在网络或设备中的用户信息端点处）。所述同意可以在令牌中被编码。接入令牌中的同意决定的编码类型可以与实施有关。本地 OP 可以使用 ID 令牌和接入令牌来将用户代理重定向至例如客户端端点。用于重定向用户代理的 URL 可以由服务提供方在初始请求（例如，参数重定向 _uri）中提供。服务提供方可以希望自己验证 ID 令牌签名。例如，服务提供方可以

从 URL（例如，在令牌的报头中的 x5u 参数中提供的 URL）请求公共密钥和 / 或证书。在示例实施方式中，服务提供方可以使用 ID 令牌（例如，用于令牌验证请求）来联系 OP 的校验 ID 端点。该通信可通过客户端机密的使用来保护，所述客户端机密可例如在服务提供方与 OP 之间共享。校验 ID 端点可例如通过校验来自令牌报头的签名来验证令牌是否由授权的本地 OP 实例发出，其中，校验来自令牌报头的签名例如通过使用在报头的 x5u 参数中提供的公共密钥进行。校验 ID 端点可以将令牌验证的结果返回至服务提供方。

[0099] 由于 ID 令牌验证的结果，服务提供方可以获知用户标识符和 / 或该标识符的发出者。例如，如果服务提供方不请求接入令牌（例如，服务提供方不需要提供到所请求的服务的接入的附加数据），认证协议可以结束，并且服务提供方可以向用户提供所请求的数据 / 服务。如果已由服务提供方请求了接入令牌，并且该接入令牌被发至服务提供方，该服务提供方可以在到用户信息端点的请求中使用接入令牌，例如以取得用户信息（例如，属性）。根据示例实施方式，所述接入令牌可以包括用户属性。本地 OP 可以取得属性、可以创建令牌、和 / 或可以对令牌进行签名。根据示例实施方式，服务提供方可自动验证令牌的有效性，并且可以取得所期望的信息（例如，用户属性或要求）。

[0100] 用户信息端点可以验证所述令牌是否由有效和授权的本地 OP 发出。该端点可以验证用户是否同意释放所请求的数据。本地 OP 的有效性的验证可以通过验证接入令牌上的 JWS 签名来完成。用户同意的验证可以修改接入令牌的内部结构，例如以携带与用户同意相关联的信息。一旦验证完毕，用户信息端点可返回所请求的属性至服务提供方（例如，以 JSON 格式）。服务提供方可以创建用户的用户简档的本地副本（例如，使用接收到的属性）和 / 或可以提供对服务的接入。根据示例实施方式，如果用户再次访问服务提供方，注册和 / 或发现步骤可以不由服务提供方执行。用户可以被指导执行认证和授权，并且在令牌验证之后，用户可以直接登录服务提供方。

[0101] 在示例性实施方式中，私有密钥可以存在于安全环境中。本地 OP 可以在安全可信环境（例如，安全性模块、可信模块等等）中在本地创建密钥对，并且可以将所述私有密钥存储在安全元件中。网络 OP 可以创建针对对应的私有密钥的证书，和 / 或可以向服务提供方提供该证书（例如，一经请求）。如在此所描述的，符号 K 可以表示密钥对，pu(K) 可以表示公共密钥，pr(K) 可以表示私有密钥，以及 cert(K,C) 可以表示针对 pu(K) 的证书。例如，cert(K,C) 可以由密钥 C 的所有者发出，和 / 或其可以使用密钥 pr(C) 来被创建，和 / 或其可以使用 pu(C) 来被验证。

[0102] 一旦在安全元件中安装了本地 OP 小程序，例如，该小程序可生成根密钥对 R、可将 pr(R) 存储在该安全元件中、并且可从安全元件发出者或制造商（例如，从智能卡制造商）获得证书 cert(R,I)。该证书可由发出者进行存储，并可被存储在安全元件中。

[0103] 根据示例实施方式，本地 OP 可以被登记在 OP 服务器功能 (OPSF) 的域中。该登记例如可以在移动设备上的本地 OP 应用被安装或首次启动时触发。OPSF 可以提供可由本地 OP 使用的登记端点，例如以向 OPSF 登记新的密钥对。

[0104] 本地 OP 可以生成开放 ID 应用指定的密钥对 O_1、可以创建 cert(O_1,R)（例如，可以使用 pr(R) 来对 pu(O_1) 进行签名），并且可以将 cert(O_1,R) 和 cert(R,I) 递交至 OPSF 的登记端点。该登记端点可以校验 cert(R,I)，例如以验证本地 OP 是否已由值得信任的发出者创建和发出。例如，该验证可以包括校验针对发出者密钥 I 的证书，并且可以包括 OCSP 校验

（例如，其可以确定证书是否有效）。OPSF 登记端点可校验 cert(O_1, R) 以验证密钥 pu(O_1) 是否已由本地 OP 实例创建。

[0105] 本地 OP 可以使用密钥来创建令牌签名。例如，OPSF 可以使证书（例如，链）可用于 RP（例如，在证书端点处）。OPSF 可以存储该证书及其证书链。根据示例实施方式，一个或多个证书可以在证书端点处可用。可替换地，OPSF 可以创建针对 O_1 的证书，其可以是 cert(O_1, P)。OPSF 可以使证书 cert(O_1, P) 在证书端点处可用。在各种实施方式中，OPSF 可以在证书端点处将证书的 URL 返回至本地 OP（例如，可以被加密和 / 或签名）。OPSF 可以应用交叉证书，例如，并因此可以集成 OPSF 域 PKI 与安全元件发出者域。

[0106] 本地 OP 可以将用于证书（例如，cert(O_1, R) 和 / 或 cert(O_1, P)，这可以取决于使用的方法）的 URL（例如，所接收到的）包括在令牌报头中，如在此所描述的。例如，本地 OP 可以使用 pr(O_1) 密钥来创建令牌签名。

[0107] 本地 OP 可能需要更新签名密钥 O_1 和 / 或证书。例如，该证书的有效性可以在密钥可以被使用时进行校验。更新过程可以在期满日期接近时触发。

[0108] 签名密钥 O_1 可以用新生成的密钥对 O_2 来替换。例如，可以向 OPSF 域登记新的公共验证密钥。旧的验证密钥可仍旧可用（例如，于过渡周期内在其旧的 URL 处）。在示例实施方式中，客户端可以针对令牌签名验证使用密钥。OPSF 可以获知最新发出的 ID 令牌的有效性周期，并且旧的证书（例如 cert(O_1, R) 或 cert(O_1, P)）可以于该有效性周期内可用。如果不知道有效性周期，例如，实体可以同意针对过渡周期的最小持续时间，其中在该过渡周期中，旧的证书仍然可用。OPSF 可以生成证书，其可以创建先前的 cert(O_1, P)，并且其可以创建 cert(O_2, P)。新的密钥对 O_2 可使用旧的密钥对 O_1 来登记（例如，cert(O_2, O_1) 可以在登记中使用），以及密钥链（例如，密钥历史）可以被建立。旧的 / 先前的 / 期满的签名密钥可以被删除。

[0109] 在登记的另一个示例实施方式中，本地 OP 可以例如在协议流中动态地生成密钥对。例如，本地 OP 和 OPSF 可以共享长期机密 (K_L)。密钥对可以被创建，和 / 或可基于随机的种子值和 / 或是可以对于 OPSF 已知的长期共享机密。随机种子可以被传递至 OPSF，并且该 OPSF 可以重新计算密钥。私有密钥在本地 OP 和网络中可用。

[0110] 如在此所描述的，本地 OP 可以接收令牌请求消息，并且可以生成令牌签名。例如，在生成令牌签名时，本地 OP 可以生成随机种子值 S。该本地 OP 可以例如基于 S 和长期机密 K_L 来计算新的密钥对。可用于对令牌进行签名的公共密钥和令牌报头的 x5t URL 参数可以被设定成动态 URL（例如，在 OPSF 的证书端点处）。动态 URL 可以包括作为参数的种子 S（例如，http://opsf.org/cert.php ? seed = 1234）。基于接收到的参数 S 和 / 或长期机密 K_L，证书端点例如可以计算本地 OP 计算的密钥对。该证书端点可以生成针对公共密钥的证书。OPSF 可以删除私有密钥，和 / 或可以在动态 URL（例如，http://opsf.org/cert.php ? seed = 1234）处提供公共密钥证书。如果客户端接收到令牌并查询 URL（例如，http://opsf.org/cert.php ? seed = 1234），OPSF 可生成正确的密钥对，并且可向客户端提供证书。如果密钥和 / 或证书已经被创建，例如，OPSF 可以直接向客户端提供证书。

[0111] 图 9 示出了具有与认证 (auth) 服务器 906 共享预建立的共享机密 S 的本地 OP900 的示例协议流的流程图。在示例场景中，本地 OP 可以不配备有可用于创建 ID 令牌上的非对称签名的私有密钥。例如，HMAC 签名可用于令牌签名。在替换的示例场景中，在网络 OP（例

如，认证服务器 906）与客户端（例如，服务提供方 904）之间建立的密钥可用于令牌签名的创建，例如，以使客户端可自动确认该签名。

[0112] 参考图 9，在 908 处，用户可经由 UE 的浏览器 902 请求接入由服务提供方 904 提供的服务。在 908 处，浏览器 902 可向服务提供方 904 提供诸如开放 ID 标识符之类的标识符。服务提供方 904 可以准备可包括对 ID 令牌和接入令牌的请求的授权请求，并且在 910 处，该服务提供方 904 可以经由重定向消息将该请求发送至浏览器 902。在 910 处的请求可以包括对根据开放 ID 连接协议的 ID 令牌的请求。在 910 处的请求可以包括对根据开放 ID 连接协议的接入令牌的请求。例如，接入令牌可由服务提供方 904 请求，以使该服务提供方 904 能够取得 UE 的用户的属性。在 912 处，该请求可以经由重定向消息从 UE 上的浏览器 902 转发至 UE 上的可信模块（例如，本地 OP900）。在 914 处，UE 的用户可以由本地 OP900 验证。在 916 处，用户可以给出对 UE 向服务提供方 904 发出令牌的同意（批准）。例如，授权请求可以由 UE 的用户批准。进一步地，响应于授权请求，在 UE 处，与授权请求的用户批准相关联的接入令牌可以被创建。在示例实施方式中，授权请求的用户批准可以经由存储在 UE 上的策略自动被接收。

[0113] 仍旧参考图 9，在 918 处，令牌可以在本地 OP900 处被创建。信息可以被添加到所述令牌。例如，对令牌的扩展可以将信息添加到令牌的 JSON 数据结构中。在示例实施方式中，令牌可以包括：

[0114] {

[0115] "iss":（例如，http://server.example.com），

[0116] "user_id":（例如，248289761001），

[0117] "aud":（例如，http://client.example.com"），

[0118] "exp":（例如，1311281970），

[0119] "lop_id":（例如，可以表示本地 OP 的标识符，例如 11223344556677），

[0120] "timestamp":（例如，可以表示具有格式 YYYYMMDDhhmmss[.s…]Z' 的时间时间戳，例如时间 20111012143815Z），和 / 或

[0121] "lop_sig":（例如，可表示使用 HMAC SHA1（{lop_id| 时间戳 }）的签名，例如 572400e4ec56fdce9549777bf67d70041f53a6aa）

[0122] }

[0123] 例如，在 918 处，HMAC_SHA1 签名可以使用作为密钥的共享机密 S 来计算。该签名可以根据本地 OP ID 的串联和 / 或用户认证的时间戳来计算。在另一个示例令牌中，数据可以根据 JSON、例如通过创建本地 OP 字段组来构成，如下列示出的：

[0124]

{

"iss": (例如，http://server.example.com),

"user_id": (例如，248289761001),

"aud": (例如，http://client.example.com),

"exp": (例如，1311281970),

"local_openid": {

"lop_id": "(例如，可以是本地 OP 的标识符，例如 11223344556677),

"timestamp": "(例如，20111012143815Z), 和/或

"lop_sig": (例如，可以是使用 HMAC SHA1({lop_id|时间戳})的

[0125]

签名，例如 572400e4ec56fdce9549777bf67d70041f53a6aa)

}

}

[0126] 如所描述的，内容可以被添加到 ID 令牌，并且有效的 HMAC SHA1 签名可以被创建。例如，可用于签名的密钥可以是客户端机密。信息可以被添加到 JSON 令牌，和 / 或其内部结构可以被修改。根据示例实施方式，服务提供方可以忽略令牌中的附加字段，和 / 或服务提供方可以将该令牌视为不透明的值。

[0127] 如在此描述的，可创建令牌签名的密钥可以是客户端机密。例如，客户端机密可以例如在注册过程中，在客户端（服务提供方）与认证服务器 (OPSF) 之间建立。认证服务器可以向本地 OP 提供客户端机密列表，例如以使得本地 OP 能够创建正确的令牌签名。例如，认证服务器可使用空中管理方法来将客户端机密列表装入本地 OP 实例。当新的客户端机密被注册（例如，用于新的客户端和 / 或现有的客户端）时，本地 OP 中的列表可以被更新。例如，令牌请求中的听众 (aud) 参数（其可以是客户端的 URL）可以标识正请求令牌的客户端。听众参数可由本地 OP 使用，例如以在本地 OP 存储器中找到对应的客户端机密。

[0128] 在另一个示例实施方式中，客户端机密可从认证服务器中查询。例如，本地 OP 可获得对为令牌创建有效的 HMAC 签名的客户端机密的了解。为了使本地 OP 获知该客户端机密，一旦请求，认证服务器可以向本地 OP 提供客户端机密。在这种规定中，本地 OP 可以从可在令牌请求中接收的听众参数中提取客户端名称。本地 OP 可以例如在特定的端点处建立与认证服务器的经认证的和 / 或安全的连接。本地 OP 可以请求客户端的客户端机密。该客户端机密可以用于创建签名。例如，认证服务器可以提供客户端机密端点 https://op.org/clients.php。这种客户端机密端点可以使用 TLS 加密和 / 或可以被认证。在根据实施方式的示例性协议运行中，在创建令牌签名之前，本地 OP 可以与客户端机密端点连接，可以认证该客户端机密端点，并且可以请求诸如 https://op.org/clients.php ? client_audience = audience 之类的资源。在示例资源中，听众可以等于来自所接收到的听众字段

的内容。客户端机密端点可以将客户端机密返回至本地 OP。之后，本地 OP 可以使用该机密来创建有效的签名。

[0129] 在又一个示例实施方式中，客户端机密可以从认证服务器和本地 OP 中的长期机密得出。例如，客户端机密可以在注册过程中、例如在客户端与网络 OP 之间被建立。根据在此描述的实施方式，本地 OP 和网络 IdP/OP（认证服务器）可以共享长期机密。用于创建长期共享机密的各种方法在此处被描述。例如，长期共享机密可以被嵌入在本地 OP 应用中（例如，在安装时）。长期共享机密可以经由 MNO 的 OTA 管理操作来生成。长期共享机密可以例如通过从网络认证协议运行的密钥导出来创建。共享机密可以用作网络 IdP/OP（认证服务器）与设备 / 本地 OP 之间的可信锚点。该机密可以例如通过安全元件的安全性特征（例如，SIM 卡和 / 或嵌入的安全性元件）在本地 OP 中得以保护。

[0130] 在客户端的示例性注册过程中，认证服务器可以使用密钥导出函数 (KDF) 中的长期机密和来自客户端的听众参数。例如，网络 OP 可以导出客户端机密，以使客户端机密＝KDF（听众、长期机密）。在示例性认证协议运行中，本地 OP 可以从令牌请求报头中读取听众字段，并且可以将相同的 KDF 应用于听众字段和长期机密，以计算客户端机密。该客户端机密之后可用于创建令牌签名。

[0131] 再次参考图 9，在 910 处，授权请求可以被集成在令牌（例如接入令牌）中。来自客户端（例如，服务提供方 904) 的原始授权请求可以被集成在令牌中，例如以确保发出的接入令牌可以针对所请求的资源而被兑换。在示例场景中，本地 OP900 可以在本地令牌创建过程中授权对数据的访问，并且所述数据可以由网络提供，或者由本地 OP900 本地提供。在示例场景中，例如在对网络使用令牌时，请求可以被改变。所述令牌可以包括关于到网络的授权请求的信息。例如，授权请求可以经由重定向消息从服务提供方发送至授权服务器 /OP906。当本地 OP900 如在此所描述的被使用时，在 910 和 912 处，授权请求可以经由重定向发送至本地 OP900。服务提供方 904 可以使用开放 ID 连接范围来指定接入特权，所述接入特权在对接入令牌的授权请求中被请求。例如，与接入令牌相关联的范围可以确定可在其被用于接入 OAuth2 保护的端点时可用的资源。

[0132] 示例性范围包括开放 ID 范围，该开放 ID 范围可以通知授权服务器客户端正在做出开放 ID 请求。在示例配置中，如果开放 ID 范围未被指定，则授权服务器可以将请求视为通用 OAuth2.0 请求，并且可以不执行开放 ID 过程。简档范围例如可以请求默认的简档信息。电子邮件范围可以请求电子邮件地址。地址范围可以请求地址。

[0133] 除了范围参数以外，授权请求可以包括可允许客户端（例如，服务提供方 904) 建立请求结构的开放 ID 请求对象。例如，开放 ID 请求对象可以作为编码后的 JWT 和 / 或作为可指向开放 ID 请求对象的 URL 被传递。

[0134] 下面是在 JWT 编码前开放 ID 请求对象的示例，其可以按照开放 ID 连接协议实施：

[0135]

```
{
"response_type": "code id_token",
"client_id": "s6BhdRkqt3",
"redirect_uri": "https://client.example.com/cb",
"scope": "openid profile",
"state": "af0ifjsldkj",
"userinfo":
```


[0136]


```
{
    "claims":
    {
    "name": null,
    "nickname": {"optional": true},
    "email": null,
    "verified": null,
    "picture": {"optional": true},
    },
    "format": "signed"
}
"id_token":
{
    "max_age": 86400,
    "iso29115": "2"
}
}
```


[0137] 下面是可按照开放 ID 连接协议实施的编码后的 JWT 的示例。

[0138]

JWT algorithm = HS256

HMAC HASH Key = 'aaa' (例如，这可以是用于对 JWT 进行签名的密钥的 id)

JSON Encoded Header = "{"alg":"HS256","typ":"JWT"}"

JSON Encoded Payload = "{"response_type":"code id_token",

"client_id":"s6BhdRkqt3",

"redirect_uri":"https://client.example.com/cb",

"scope":"openid profile",

"state":"af0ifjsldkj",

"userinfo":{"claims":{"name":null,"nickname":{"optional":true},

[0139]

"email":null,"verified":null,

"picture":{"optional":true}},"format":"signed"},

"id_token":{"max_age":86400,"iso29115":"2"}}"

JWT =

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyZXNwb25zZV90eXBlIjoiY29kZSBpZF90b2tlbiIsImNsaWVudF9pZCI6InM2QmhkUmtxdDMiLCJyZWRpcmVjdF91cmkiOiJodHRwczpcL1wvY2xpZW50LmV4YW1wbGUuY29tXC9jYiIsInNjb3BlIjoib3BlbmlkIHByb2ZpbGUiLCJzdGF0ZSI6ImFmMGlmanNsZGtqIiwidXNlcmluZm8iOnsiY2xhaW1zIjp7Im5hbWUiOm51bGwsIm5pY2tuYW1lIjp7Im9wdGlvbmFsIjp0cnVlfSwiZW1haWwiOm51bGwsInZlcmlmaWVkIjpudWxsLCJwaWN0dXJlIjp7Im9wdGlvbmFsIjp0cnVlfX0sImZvcm1hdCI6InNpZ25lZCJ9LCJpZF90b2tlbiI6eyJtYXhfYWdlIjo4NjQwMCwiaXNvMjkxMTUiOiIyIn19.2OiqRgrbrHkA1FZ5p_7bc_RSdTbH-wo_Agk-ZRpD3wY

[0140] 下面是可根据开放 ID 连接协议实施的授权请求的示例：

[0141] https://server.example.com/authorize ?

[0142] response_type = code%02id_token

[0143] &client_id = s6BhdRkqt3

[0144] &redirect_uri = https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb

[0145] &scope = openid

[0146] &state = af0ifjsldkj

[0147] &request = eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyZXNwb25zZV90eXBlIjoiY29kZSBpZF90b2tlbiIsImNsaWVudF9pZCI6InM2QmhkUmtxdDMiLCJyZWRpcmVjdF91cmkiOiJodHRwczpcL1wvY2xpZW50LmV4YW1wbGUuY29tXC9jYiIsInNjb3BlIjoib3Blbmlk IHByb2ZpbGUiLCJzdGF0ZSI6ImFmMGlmanNsZGtqIiwidXNlcmluZm8iOnsiY2xhaW1zIjp7Im5hbWUiOm51bGwsIm5pY2tuYW1lIjp7Im9wdGlvbmFsIjpOcnVlfSwiZW1haWwiOm51bGwsInZlcmlmaWVkIjpudWxsLCJwaWN0dXJlIjp7Im9wdGlvbmFsIjpOcnVlfX0sImZvcm1hdCI6InNpZ251ZCJ9LCJpZF90b2tlbiI6eyJtYXhfYWdlIjo4NjQwMCwiaXNvMjkxMTUiOiIyIn19.2OiqRgrbrHkA1FZ5p_7bc_RSdTbH-wo_Agk-ZRpD3wY

[0148] 再次参考图9，授权请求（例如，在此示出的授权请求）例如可以经由HTTP重定向发送至本地OP（例如，参见图9中的910和912）。本地OP900可以校验该请求是否有效和/或可以认证该用户。本地OP900可以创建可在920和922处经由重定向消息被发向服务提供方904的令牌。服务提供方904可以使用令牌例如以从ID令牌端点926和/或用户信息端点928获得数据。

[0149] 在示例实施方式中，分别到令牌端点926和928的请求924和930可不包括原始请求对象。在这种请求（例如，请求924和930）中，令牌可以例如由令牌端点926和928接收，并且没有对信息正被服务提供方904请求以及信息正在被授权而由服务提供方904访问的指示。在这种请求中，本地OP900可以通过将JWT编码的请求在令牌发向服务提供方904之前添加到该令牌中来将所请求的信息传达给令牌端点。例如，令牌可以携带请求信息，并且该请求信息可由令牌端点估计。请求JWT例如可以由本地OP900进行签名，以防止攻击（例如，在服务可在用户的授权之后改变请求的情况下的攻击）。在932和934处，令牌签名可以使用共享机密S在各自的端点处被验证。在ID令牌签名被验证之后，在936处，用户的认证信息（例如，用户标识符）可以被提供至服务提供方904。在接入令牌签名被验证之后，在938处，用户的简档信息（例如，由服务提供方904请求的用户属性或用户要求）可以被提供至服务提供方904。包括请求信息的令牌的示例被提供如下：

[0150]

```
{
"iss": "http://server.example.com", //可以按照开放ID连接实施
"user_id": "248289761001", //可以按照开放ID连接实施
"aud": "http://client.example.com", //可以按照开放ID连接实施
"exp": 1311281970, //可以按照开放ID连接实施
```

[0151]

"local_openid": {
"lop_id": "11223344556677", //可以是本地 OP 使用的标识符
"timestamp": "20111012143815Z", // ‘YYYYMMDDhhmmss[.s...]Z’
"request":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyZXNwb25zZV90eXBlIjoiY29kZSBpZF90b2tlbi
IsImNsa
WVudF9pZCI6InM2QmhkUmtxdDMiLCJyZWRpcmVjdF91cmkiOiJodHRwczpcL1wvY2xpZW50
LmV4YW1wbGUuY29t
XC9jYiIsInNjb3BlIjoib3BlbmlkIHByb2ZpbGUiLCJzdGF0ZSI6ImFmMGlmanNsZGtqIiwidXNlcm
luZm8iOns
iY2xhaW1zIjp7Im5hbWUiOm51bGwsIm5pY2tuYW1lIjp7Im9wdGlvbmFsIjp0cnVlfSwiZW1haW
wiOm51bGwsIn
ZlcmlmaWVkIjpudWxsLCJwaWN0dXJlIjp7Im9wdGlvbmFsIjp0cnVlfX0sImZvcm1hdCI6InNpZ2
5lZCJ9LCJpZ
F90b2tlbiI6eyJtYXhfYWdlIjo4NjQwMCwiaXNvMjkxMTUiOiIyIn19.2OiqRgrbrHkA1FZ5p_7bc_RSdTbH-woAgk-ZRpD3wY",
"lop_sig": "a0a52ecf404981d579dab41439b10e0cdfb48f91"
//可以是使用 HMAC SHA1 ({lop_id|时间戳|请求})的签名
}
}

[0152] 参考上面的示例令牌，签名 log_sig（本地 OP_ 签名）可以按照串联的 lop_id（本地 OP_id）、时间戳和请求来计算。令牌可以由本地 OP 进行签名，例如以使签名可由服务提供方和 / 或身份提供方的令牌端点验证。根据示例实施方式，授权码可以包括请求信息。

[0153] 如在此所描述的，用户数据（例如，属性）可以在用户信息端点处被存储。这种用户信息端点可以位于网络实体、云等等上，并且可以从所述网络或云访问用户数据。图 10

示出了根据另一个示例实施方式的呼叫流，其中用户信息端点本地位于 UE 上。用户数据（例如，机密信息）可以本地存储在 UE1000、UE1000 内的 UICC、位于 UE1000 内的可信模块 1002 等上。允许本地存储的用户数据的认证和传输的机制被提供。根据所示的实施方式，用户信息端点可以位于可信模块 1002 上。

[0154] 在示例场景中，用户可能想要某些机密信息（例如，他 / 她的社会保险号 (SSN)），其中所述机密信息本地存储在 UE1000 上。这种本地存储的信息可以被存储在安全 / 可信的硬件模块 1002 或 UICC 上，而不是存储在网络 / 云中。可由多个利益相关者（例如，OP/OPSF 和 UE 内的用户）控制和配置的本地策略可以授权将存储在 UE1000 中的机密信息释放到服务提供方 RP/ 客户端 1006。

[0155] 例如，用户可能不确信其存储在网络或云上的机密信息的安全性和 / 或私密性。这种信息可以例如包括用户的社会保险号。用户可以选择通过将信息存储在 UE 上来保持该信息私有。在示例配置中，用户可以将一些用户属性（例如，名称、地址等）存储在网络上，而将其他用户属性（例如，SSN、生日等）本地存储在 UE 的安全环境中。在其中用户希望获取金融机构的服务的示例场景中，该机构可以要求用户的 SSN，以使用户接入由该金融机构提供的服务。在可以是基于网络和 / 或本地的成功认证之后，例如，UE 上的策略可以授权将本地存储的 SSN 释放到所述金融机构。在其中 SSN 在本地被存储的这种示例场景中，其他用户信息（例如，非机密用户属性）可以由该机构从网络 / 云中获取。

[0156] 参考图 10，在 1010 处，浏览器代理 (BA)1004 可以发送用户标识符至 SP/ 客户端 / RP1006，并且可以请求接入由 RP1006 提供的服务。在 1012 处，RP1006 可以建立授权请求，并且可以用授权请求将 BA1004 重定向至可信模块 1002（在 1014 处）。在 1016 处，UE1000 的用户可以在 UE1000 处被认证。在 1018 处，UE 可以确定其具有对向 RP1006 发出至少一个令牌的用户同意 / 授权。在 1020 处，可信模块 1002（例如，本地 OP）可以根据开放 ID 连接协议生成令牌。在 1020 处，可信模块 1002 可以对该令牌进行签名。令牌报头可以包括针对 OP1008 的指示符，以确定包括该报头的令牌是否本地生成。在 1022 处，可信模块 1002 之后可以传递包括签名的令牌的重定向消息至 BA1004，该重定向消息可以将 BA1004 重定向至 RP1006（在 1024 处）。签名的令牌中的一者或多者可以包括可根据开放 ID 连接协议进行格式化的接入令牌。例如，在 1020 处，在具有或没有对诸如 OP1008 之类的网络实体的认知的情况下，接入令牌可以经由可信模块 1002 在 UE1000 上本地生成，并且在步骤 1022 和 1024 处，所述接入令牌可以被发送至 SP/ 客户端 /RP1006。与特定用户数据或用户数据的类别相关联的接入令牌可以被约束到与用户信息端点的位置对应的位置（例如，URL），其中所述用户信息端点与接入令牌相关联。在示例配置中，用户数据（例如，属性）可以被分成机密的或非机密的，并且机密数据可以从本地位于 UE1000 上的用户信息端点访问，而非机密数据可以在位于网络上的用户信息端点处被访问。

[0157] 继续参考图 10，在 1026 处，RP1006 可以使用可包括 ID 令牌的有效令牌请求消息来联系在 OP1008 处的校验 ID 端点 1028。如在此描述的，在 1030 处，校验 ID 端点 1030 可以验证令牌签名 S。在 1032 处，校验 ID 端点 1028 可以将用户的认证信息返回至 RP1006。如果已经请求和发出了接入令牌，例如，则客户端 1006 可以使用请求的接入令牌 1034 来请求用户数据。例如，接入令牌可以携带关于用户信息端点 1036 的位置（例如，拥有用户信息端点 1036 的可信模块 1002 的位置）的信息。可替换地，在 1024 处，例如，用户信息端点

的位置信息可以作为重定向消息的一部分被传输，而不是作为接入令牌的一部分被传输。在 1034 处，RP1006 可以例如通过使用如在此所描述的接入令牌从可在本地位于 UE1000 上的用户信息端点 1036 请求用户数据。在 1038 处，可位于可信模块 1002 上的用户信息端点 1036 可以返回所请求的用户数据（例如，社会保险号、地址等）。在示例实施方式中，在 RP1006 接收到用户数据之后，UE1000 可以接收到对由客户端 1006 提供的服务的完全接入。

[0158] 在这里描述的另一个示例实施方式中，接入令牌可以在网络 / 云中生成。例如，网络实体可以替代 UE 生成接入令牌，并且该令牌可以被发送至 SP/ 客户端 /RP。所述接入令牌可以携带关于用户信息端点的位置（例如，URL）的信息，并且该位置可对应于网络 / 云中的实体、或 UE 上的用户信息端点、或 UE 内的可信模块内的用户信息端点。可以在接入令牌的消息主体内携带用户信息端点位置信息。

[0159] 根据示例实施方式，在可能不具有对身份提供方或网络 / 云实体的认知的情况下，可用一个或多个令牌访问的信息可位于 UE 上。可替换地，可用各自的令牌访问的信息可位于网络 / 云上。令牌中的信息可以被签名和 / 或加密，以保护令牌数据不被窃听。这种信息可以被解密以获取令牌信息。这种测量可以确保仅合法的 SP/ 客户端 /RP（具有正确密钥）能够获取令牌。一旦由 SP/ 客户端 /RP 解密了该令牌，SP/ 客户端 /RP 可以向用户信息端点授予令牌。UE 或 UE 上的可信模块和 / 或网络 / 云实体可以生成和 / 或验证令牌，并提供所请求的数据至 SP/ 客户端 /RP。信息元素可以在网络和 UE 之间被分配，或者可以在网络与 UE 之间通用且同步。

[0160] 例如，用户数据可以在本地被存储在 UE 上（例如，在 UICC、可信模块等等上），用户数据可以被存储在网络实体上（例如，在 OP 等上），以及用户数据可以被存储在上述任意合适的组合中。图 11 示出了根据示例实施方式的其中一些用户数据在本地被存储而一些用户数据被存储在网络实体上的呼叫流。参考图 11，以上关于图 10，描述了同样出现在图 10 中的步骤号。在示例配置中，作为机密数据的用户数据可以在本地被存储，而作为非机密数据的用户数据可以被存储在网络 / 云实体上。在替换配置中，数据未被分类，但是可以在本地存储，数据可以存储在网络实体上，或者数据可以存储在上述的组合中。

[0161] 一旦身份令牌的用户认证和验证成功，在 1100 和 1106 处，RP1006 可以请求用户数据（例如，用户属性）。例如，在 1100 处，RP1006 可以使用第一接入令牌来从位于 UE1000 内的可信模块 1002 处的用户信息端点 1102 取得用户数据。这种用户数据可以已被分类为机密数据。第一接入令牌可以包括用户信息端点 1102 的位置信息。在 1104 处，机密用户数据例如可以被提供至 RP1006。在 1106 处，RP1006 可以使用第二接入令牌来从网络实体（例如，OP1008）上的用户信息端点 1108 中取得用户数据。这种用户数据可以已被分类为非机密数据。第二接入令牌可包括用户信息端点 1108 的位置信息（例如，URL），以使 RP1006 从用户信息端点 1108 兑换用户数据。与机密数据相关联的且用于从 UE1000 内的存储器中获取数据的第一接入令牌可以由本地 OP（例如，UE1000 的可信模块 1002）提供。用户信息端点 1102 的位置（例如，URL）还可以由 UE1000 的本地 OP 提供。在示例实施方式中，在数据（例如，机密和非机密数据）由 RP1006 获取之后，其可以在 RP1006 处被合并，并且用于为 UE1000 提供对由 RP1006 提供的服务的接入。所述数据可以在 RP1006 处被合并和使用。

[0162] 因此，如在此所描述的，每个接入令牌或每个用户数据类别（例如，机密的、非机密的、敏感的、通用的等等）可以与用户数据的位置相关联。用户数据的位置可以与 UE 或

诸如UICC之类的可信模块的位置（例如，到UE/UICC的URL）、网络/云中的位置（例如，到网络/云内的实体的URL）、或者他们的组合对应。因此，存储在不同位置中的用户属性可以由SP/客户端/RP请求、处理、合并和使用。

[0163] 举个例子，UE1000可以接收授权请求，以为服务提供方（例如，RP1006）创建接入令牌。基于所述授权请求，在UE处，第一接入令牌可以被创建，以及第二接入令牌可以被创建。接入令牌可与由UE1000的用户和RP1006提供的服务相关联。第一接入令牌可以包括指示第一用户信息端点的位置的信息，其中一旦验证了该第一接入令牌，该第一用户信息端点就向RP1006提供第一请求的用户属性。第二接入令牌可以包括指示第二用户信息端点的位置的信息，其中一旦验证了该第二接入令牌，该第二用户信息端点就向RP1006提供第二请求的用户属性。所述第一用户信息端点可以位于UE100上，而第二用户信息端点可以位于经由网络与RP1006通信的网络实体（例如，OP1008）上。

[0164] 图12A是可以在其中实施所公开的一个或多个实施方式的示例通信系统1400的图示。通信系统1400可以是为多个无线用户提供例如语音、数据、视频、消息发送、广播等内容的多接入系统。该通信系统1400能使多个无线用户通过共享包括无线带宽在内的系统资源来访问这些内容。例如，通信系统1400可以使用一种或多种信道接入方法，如码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)、正交FDMA(OFDMA)、单载波FDMA(SC-FDMA)等等。

[0165] 如图12A所示，通信系统1400可以包括无线发射/接收单元(WTRU)1402a、1402b、1402c、1402d、无线电接入网(RAN)1404、核心网1406、公共交换电话网(PSTN)1408、因特网1410以及其他网络1412，但是应该了解，所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。每一个WTRU1402a、1402b、1402c、1402d都可以是被配置成在无线环境中工作和/或通信的任何类型的设备。举个例子，WTRU1402a、1402b、1402c、1402d可以被配置成传送和/或接收无线信号，并且可以包括用户设备(UE)、移动站、固定或移动订户单元、寻呼机、蜂窝电话、个人数字助理(PDA)、智能电话、膝上型计算机、上网本、个人计算机、无线传感器、消费类电子产品等等。

[0166] 通信系统1400还可以包括基站1414a和基站1414b。每一个基站1414a和1414b可以是被配置成与WTRU1402a、1402b、1402c、1402d中的至少一者无线对接的任何类型的设备，以便促成对一个或多个通信网络（例如核心网1406、因特网1410和/或其他网络1412）的接入。举个例子，基站1414a、1414b可以是基础收发信站(BTS)、节点B、e节点B、家用节点B、家用e节点B、站点控制器、接入点(AP)、无线路由器等等。虽然基站1414a、1414b中的每一个都被描述成是单个部件，但是应该了解，基站1414a、1414b可以包括任何数量的互连基站和/或网络元件。

[0167] 基站1414a可以是RAN1404的一部分，其中该RAN1404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)、中继节点等等。基站1414a和/或基站1414b可以被配置成在可以被称为小区（未显示）的特定地理区域内传送和/或接收无线信号。小区还可以分成小区扇区。例如，与基站1414a相关联的小区可以分成三个扇区。因此在一个实施方式中，基站1414a可以包括三个收发信机，也就是说，小区的每一个扇区都具有一个收发信机。在一个实施方式中，基站1414a可以使用多输入多输出(MIMO)技术，并且由此可以针对小区中的每个扇区使用多个收发信机。

[0168] 基站 1414a、1414b 可以通过空中接口 1416 与 WTRU1402a、1402b、1402c、1402d 中的一者或多者进行通信，其中该空中接口 1416 可以是任何适当的无线通信链路（例如射频 (RF)、微波、红外 (IR)、紫外 (UV)、可见光等等）。该空中接口 1416 可以使用任何适当的无线电接入技术 (RAT) 来建立。

[0169] 更具体地说，如上所述，通信系统 1400 可以是多接入系统，并且可以使用一种或多种信道接入方案，如 CDMA、TDMA、FDMA、OFDMA、SC-FDMA 等等。例如，RAN1404 中的基站 1414a 与 WTRU1402a、1402b、1402c 可以实施诸如通用移动电信系统 (UMTS) 陆地无线电接入 (UTRA) 之类的无线电技术，该无线电技术可以用宽带 CDMA(WCDMA) 来建立空中接口 1416。WCDMA 可以包括诸如高速分组接入 (HSPA) 和 / 或演进型 HSPA(HSPA+) 之类的通信协议。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)。

[0170] 在一个实施方式中，基站 1414a 和 WTRU1402a、1402b、1402c 可以实施诸如演进型 UMTS 陆地无线电接入 (E-UTRA) 之类的无线电技术，该无线电技术可以使用长期演进 (LTE) 和 / 或高级 LTE(LTE-A) 来建立空中接口 1416。

[0171] 在其他实施方式中，基站 1414a 与 WTRU1402a、1402b、1402c 以实施如 IEEE802.16（即全球微波互通接入 (WiMAX)）、CDMA2000、CDMA20001X、CDMA2000EV-DO、临时标准 2000(IS-2000)、临时标准 95(IS-95)、临时标准 856(IS-856)、全球移动通信系统 (GSM)、用于 GSM 演进的增强数据速率 (EDGE)、GSM EDGE(GERAN) 等之类的无线电技术。

[0172] 举例来说，图 12A 中的基站 1414b 可以是无线路由器、家用节点 B、家用 e 节点 B、毫微微小区基站或接入点，并且可以使用任何适当的 RAT 来促成局部区域中的无线连接，例如营业场所、住宅、交通工具、校园等等。在一个实施方式中，基站 1414b 和 WTRU1402c、1402d 可以实施诸如 IEEE802.11 之类的无线电技术来建立无线局域网 (WLAN)。在一个实施方式中，基站 1414b 和 WTRU1402c、1402d 可以实施诸如 IEEE802.15 之类的无线电技术来建立无线个域网 (WPAN)。在又一个实施方式中，基站 1414b 和 WTRU1402c、1402d 可以使用基于蜂窝的 RAT（例如 WCDMA、CDMA2000、GSM、LTE、LTE-A 等等）来建立微微小区或毫微微小区。如图 12A 所示，基站 1414b 可以具有与因特网 1410 的直接连接。由此，基站 1414b 不必需要经由核心网 1406 来接入因特网 1410。

[0173] RAN1404 可以与核心网 1406 进行通信，其中核心网 1406 可以是被配置成向 WTRU1402a、1402b、1402c、1402d 中的一者或多者提供语音、数据、应用和 / 或网际协议上的语音 (VoIP) 服务的任何类型的网络。例如，核心网 1406 可提供呼叫控制、记账服务、基于移动位置的服务、预付费呼叫、因特网连接、视频分发等等，和 / 或执行高级安全功能，例如用户认证。虽然图 12A 中没有显示，但应该了解，RAN1404 和 / 或核心网 1406 可以直接或间接地和使用了与 RAN1404 相同的 RAT 或不同 RAT 的其他 RAN 进行通信。例如，除了与可以使用 E-UTRA 无线电技术的 RAN1404 相连之外，核心网 1406 还可以与另一个使用 GSM 无线电技术的 RAN（未显示）进行通信。

[0174] 核心网 1406 还可以充当 WTRU1402a、1402b、1402c、1402d 接入 PSTN1408、因特网 1410 和 / 或其他网络 1412 的网关。PSTN1408 可以包括提供简易老式电话服务 (POTS) 的电路交换电话网络。因特网 1410 可以包括使用了公共通信协议的全球性互联计算机网络和设备系统，所述公共通信协议例如传输控制协议 (TCP) / 网际协议 (IP) 族中的 TCP、用户数据报协议 (UDP) 和 IP。网络 1412 可以包括由其他服务提供方拥有和 / 或运营的有线或

无线通信网络。例如，网络 1412 可以包括与一个或多个 RAN 相连的另一个核心网，其中所述一个或多个 RAN 可以使用与 RAN1404 相同的 RAT 或不同的 RAT。

[0175] 通信系统 1400 中的 WTRU1402a、1402b、1402c、1402d 的一些或全部可以包括多模能力，也就是说，WTRU1402a、1402b、1402c、1402d 可以包括通过不同无线链路与不同无线网络通信的多个收发信机。例如，图 12A 所示的 WTRU1402c 可以被配置成与可以使用基于蜂窝的无线电技术的基站 1414a 通信，以及与可以使用 IEEE802 无线电技术的基站 1414b 通信。

[0176] 图 12B 是示例 WTRU1402 的系统图示。如图 12B 所示，WTRU1402 可以包括处理器 1418、收发信机 1420、发射 / 接收元件（例如，多个天线）1422、扬声器 / 麦克风 1424、键盘 1426、显示器 / 触摸板 1428、不可移除存储器 1430、可移除存储器 1432、电源 1434、全球定位系统 (GPS) 芯片组 1436 以及其他外围设备 1438。应该了解的是，在符合实施方式的同时，WTRU1402 可以包括前述元件的任何子组合。

[0177] 处理器 1418 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)、现场可编程门阵列 (FPGA) 电路、任意其他类型的集成电路 (IC)、状态机等等。处理器 1418 可以执行信号编码、数据处理、功率控制、输入 / 输出处理和 / 或其他任何能使 WTRU1402 在无线环境中工作的功能。处理器 1418 可以耦合至收发信机 1420，收发信机 1420 可以耦合至发射 / 接收元件 1422。虽然图 12B 将处理器 1418 和收发信机 1420 描述成是独立组件，但是应该了解，处理器 1418 和收发信机 1420 可以同时集成在电子封装或芯片中。处理器 1418 可以执行应用层程序（例如，浏览器）和 / 或无线电接入层 (RAN) 程序和 / 或通信。处理器 1418 可以例如在接入层和 / 或应用层处执行诸如认证、安全密钥协商、和 / 或加密操作之类的安全性操作。

[0178] 在示例实施方式中，WTRU1402 包括处理器 1418 和与所述处理器耦合的存储器。所述存储器可以包括可执行的指令，其中在由所述处理器执行所述指令时，所述指令使得所述处理器执行与在本地执行开放 ID 协议的功能相关联的操作。

[0179] 发射 / 接收元件 1422 可以被配置成通过空中接口 1416 来传送或接收去往或来自基站（例如基站 1414a）的信号。举个例子，在一个实施方式中，发射 / 接收元件 1422 可以是被配置成传送和 / 或接收 RF 信号的天线。在一个实施方式中，举例来说，发射 / 接收元件 1422 可以是被配置成传送和 / 或接收 IR、UV 或可见光信号的发射器 / 检测器。在另一个实施方式中，发射 / 接收元件 1422 可以被配置成传送和接收 RF 和光信号。应当理解的是，发射 / 接收元件 1422 可以被配置成传送和 / 或接收无线信号的任何组合。

[0180] 此外，虽然在图 12B 中将发射 / 接收元件 1422 描述成是单个元件，但是 WTRU1402 可以包括任何数量的发射 / 接收元件 1422。更具体地，WTRU1402 可以使用 MIMO 技术。因此在一个实施方式中，WTRU1402 可以包括两个或更多个用于通过空中接口 1416 传送和接收无线信号的发射 / 接收元件 1422（例如，多个天线）。

[0181] 收发信机 1420 可以被配置成对发射 / 接收元件 1422 将要传送的信号进行调制，以及对发射 / 接收元件 1422 接收的信号进行解调。如上所述，WTRU1402 可以具有多模能力。由此，收发信机 1420 可以包括使得 WTRU1402 经由诸如 UTRA 和 IEEE802.11 之类的多种 RAT 来进行通信的多个收发信机。

[0182] WTRU1402 的处理器 1418 可以耦合至扬声器 / 麦克风 1424、键盘 1426 和 / 或显示器 / 触摸板 1428（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），并且可以接收来自这些设备的用户输入数据。处理器 1418 还可以向扬声器 / 麦克风 1424、键盘 1426 和 / 或显示器 / 触摸板 1428 输出用户数据。此外，处理器 1418 可以从任何适当类型的存储器（例如不可移除存储器 1430 和 / 或可移除存储器 1432）中访问信息，以及将数据存入这些存储器。所述不可移除存储器 1430 可以包括随机存取存储器 (RAM)、只读存储器 (ROM)、硬盘或是其他任何类型的存储器存储设备。可移除存储器 1432 可以包括订户身份模块 (SIM) 卡、存储棒、安全数字 (SD) 存储卡等等。在其他实施方式中，处理器 1418 可以从那些并非物理位于 WTRU1402 的存储器（例如位于服务器或本地计算机（未显示）上的存储器）访问信息，以及将数据存入这些存储器。

[0183] 处理器 1418 可以接收来自电源 1434 的电力，并且可以被配置成分配和 / 或控制用于 WTRU1402 中的其他组件的电力。电源 1434 可以是为 WTRU1402 供电的任何适当的设备。例如，电源 1434 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。

[0184] 处理器 1418 还可以与 GPS 芯片组 1436 相耦合，该 GPS 芯片组 1436 可以被配置成提供与 WTRU1402 的当前位置相关的位置信息（例如经度和纬度）。作为来自 GPS 芯片组 1436 的信息的补充或替换，WTRU1402 可以通过空中接口 1416 接收来自基站（例如基站 1414a、1414b）的位置信息，和 / 或根据从两个或多个附近基站接收的信号的定时来确定其位置。应该了解的是，在保持符合实施方式的同时，WTRU1402 可以借助任何适当的位置确定方法来获取位置信息。

[0185] 处理器 1418 还可以耦合到其他外围设备 1438，外围设备 1438 可以包括提供附加特征、功能和 / 或有线或无线连接的一个或多个软件和 / 或硬件模块。例如，外围设备 1438 可以包括加速度计、电子指南针、卫星收发信机、数字相机（用于照片和视频）、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®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。

[0186] 图 12C 是根据实施方式的 RAN1404 以及示例核心网 1406 的系统图示。如上所述，RAN1404 可以使用 UTRA 无线电技术通过空中接口 1416 与 WTRU1402a、1402b、1402c 进行通信。RAN1404 还可以与核心网 1406 进行通信。如图 12C 所示，RAN1404 可以包括节点 B1440a、1440b、1440c，该节点 B1440a、1440b、1440c 中的每一个可以包括一个或多个收发信机，用于通过空中接口 1416 与 WTRU1402a、1402b、1402c 进行通信。每一个节点 B1440a、1440b、1440c 可以与 RAN1404 中的特定小区（未显示）相关联。RAN1404 还可以包括 RNC1442a、1442b。应该理解的是，在保持符合实施方式的同时，RAN1404 可以包括任何数量的节点 B 和 RNC。

[0187] 如图 12C 所示，节点 B1440a、1440b 可以与 RNC1442a 进行通信。此外，节点 B1440c 可以与 RNC1442b 进行通信。节点 B1440a、1440b、1440c 可以经由 Iub 接口来与各个 RNC1442a、1442b 进行通信。RNC1442a、1442b 可以经由 Iur 接口彼此进行通信。RNC1442a、1442b 中的每一个可以被配置成控制与之连接的各个节点 B1440a、1440b、1440c。此外，RNC1442a、1442b 中的每一个可以被配置成执行和 / 或支持其他功能，如外环功率控制、负载控制、准许控制、分组调度、切换控制、宏分集、安全功能、数据加密等等。

[0188] 图 12C 中所示的核心网 1406 可以包括媒体网关 (MGW)1444、移动交换中心 (MSC)1446、服务 GPRS 支持节点 (SGSN)1448 和 / 或网关 GPRS 支持节点 (GGSN)1450。虽然每个前述元件被描述成是核心网 1406 的一部分，但应该了解的是，这些元件中的任何一个都可被核心网运营商之外的实体拥有和 / 或运营。

[0189] RAN1404 中的 RNC1442a 可经由 IuCS 接口与核心网 1406 中的 MSC1446 连接。MSC1446 可与 MGW1444 连接。MSC1446 和 MGW1444 可以为 WTRU1402a、1402b、1402c 提供对诸如 PSTN1408 之类的电路交换网络的接入，以便促成 WTRU1402a、1402b、1402c 和传统的陆线通信设备之间的通信。

[0190] RAN1404 中的 RNC1442a 还可以经由 IuPS 接口与核心网 1406 中的 SGSN1448 连接。SGSN1448 可与 GGSN1450 连接。SGSN1448 和 GGSN1450 可以为 WTRU1402a、1402b、1402c 提供对诸如因特网 1410 之类的分组交换网络的接入，以便促成 WTRU1402a、1402b、1402c 和 IP 使能设备之间的通信。

[0191] 如上所述，核心网 1406 还可以与网络 1412 相连接，其中该网络 1412 可以包括由其他服务提供方拥有和 / 或运营的其他有线或无线网络。

[0192] 虽然在上文中描述了采用特定组合的特征和元素，但是本领域普通技术人员将会了解，每一个特征或元素既可以单独使用，也可以与其他特征和元素进行任何组合来使用。此外，本领域的普通技术人员将会了解，在此描述的实施方式仅出于示例性目的而被提供。例如，尽管在此使用本地开放 ID 身份提供方 (OP) 来描述实施方式，但非本地 OP 或外部 OP 可以用于执行类似的功能，反之亦然。此外，这里描述的实施方式可以在引入到计算机可读介质中并供计算机或处理器运行的计算机程序、软件或固件中实施。计算机可读介质的示例包括电信号（通过有线或无线连接传送）以及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局限于只读存储器 (ROM)、随机存取存储器 (RAM)、寄存器、缓冲存储器、半导体存储设备、诸如内部硬盘和可移除磁盘之类的磁介质、磁光介质、以及诸如 CD-ROM 碟片和数字多用途碟片 (DVD) 之类的光介质。与软件相关联的处理器可以用于实施在 WTRU、UE、终端、基站、RNC 或任何主计算机中使用的射频收发信机。

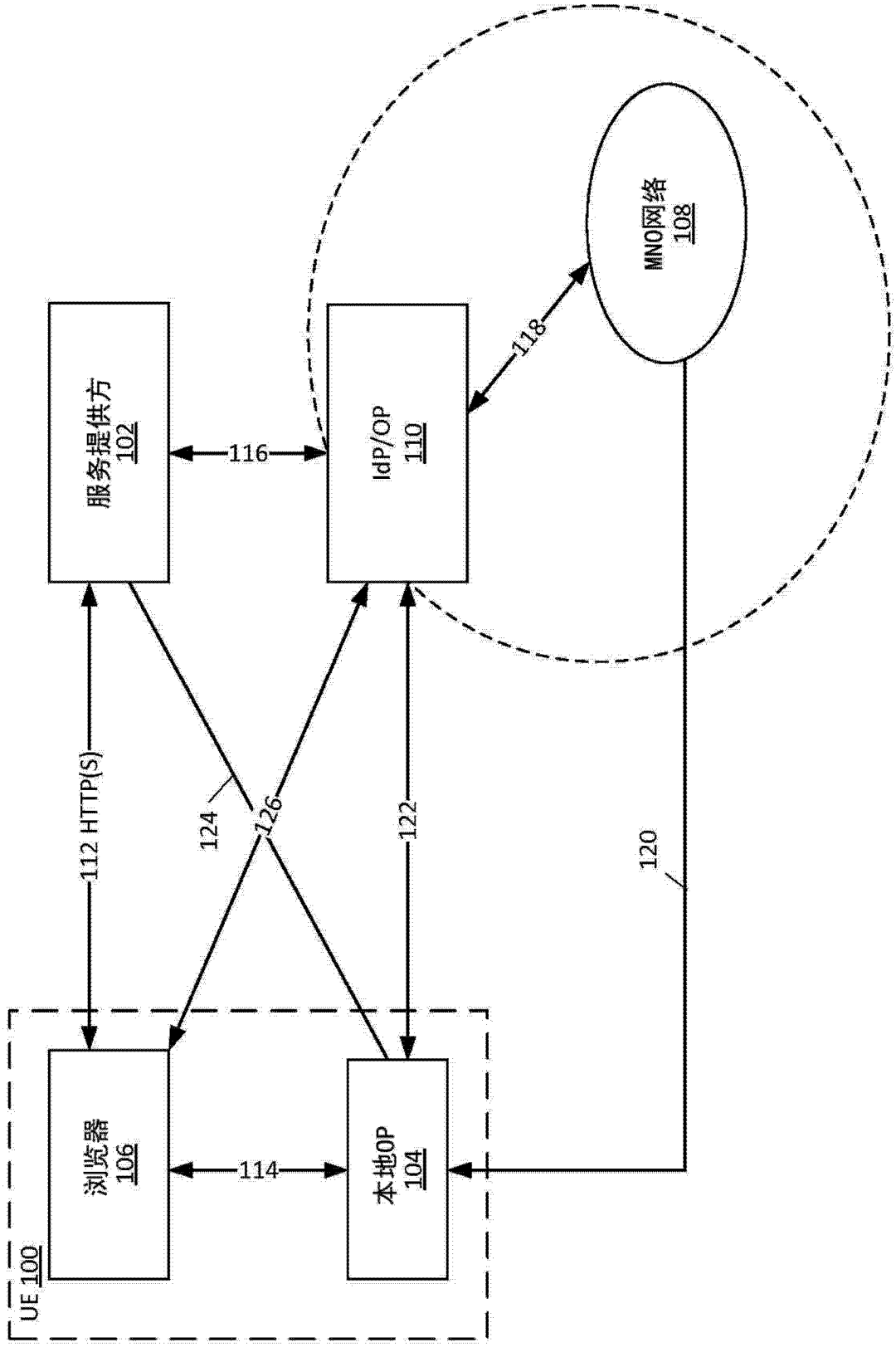

MNO网络
108
服务提供方
102
116
IdP/OP
110
118
112 HTTP(S)
124
126
122
120
浏览器
106
114
本地OP
104
UE 100

图 1

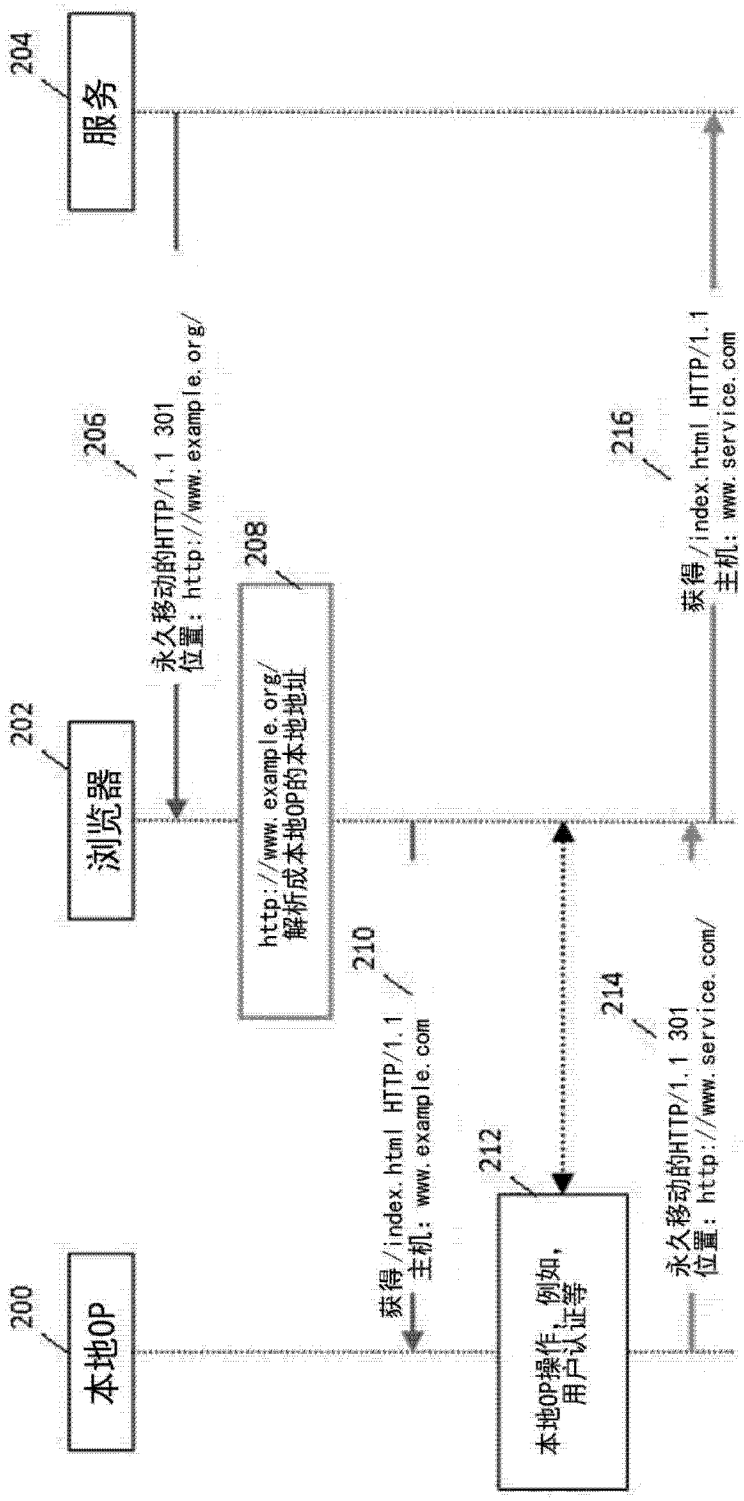

204
服务
206
永久移动的HTTP/1.1 301
位置：http://www.example.org/
208
http://www.example.org/
解析成本地OP的本地地址
202
浏览器
216
获得/index.html HTTP/1.1
主机：www.service.com
210
获得/index.html HTTP/1.1
主机：www.example.com
214
永久移动的HTTP/1.1 301
位置：http://www.service.com/
212
本地OP操作，例如，
用户认证等
200
本地OP

图 2

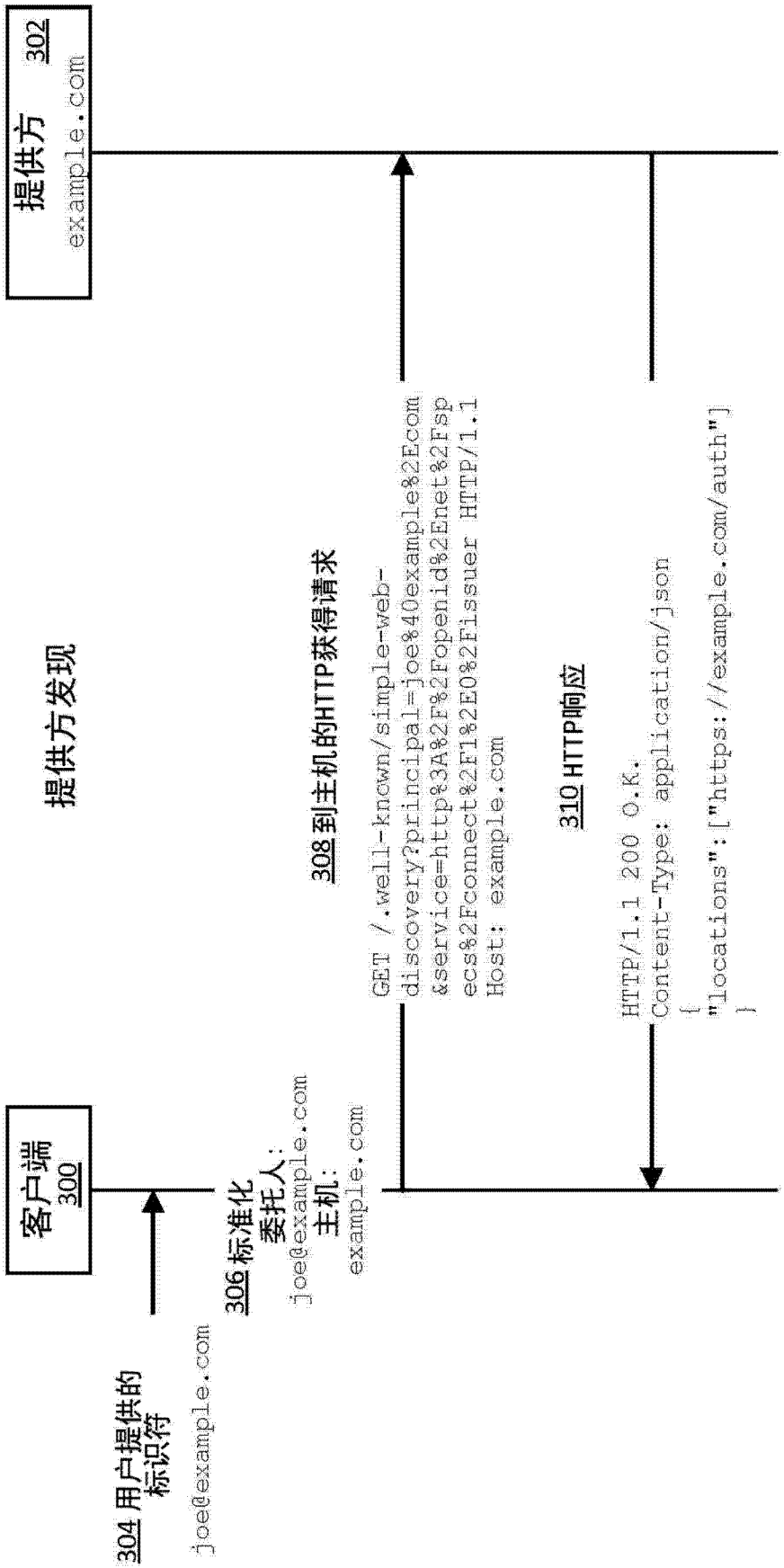

提供方 302
example.com
客户端 300
304 用户提供的标识符
joe@example.com
306 标准化
委托人:
joe@example.com
主机:
example.com
提供方发现
308 到主机的HTTP获得请求
GET /.well-known/simple-web-discovery?principal=joe%40example%2Ecom&service=http%3A%2F%2Fopenid%2Enet%2Fsp&ecs%2Fconnect%2F1%2E0%2Fissuer HTTP/1.1
Host: example.com
310 HTTP响应
HTTP/1.1 200 O.K.
Content-Type: application/json
{
"locations":["https://example.com/auth"]
}

图 3


客户端
300
提供方配置信息
提供方 302
example.com
400 到主机的HTTP获得请求
GET /.well-known/openid-configuration
HTTP/1.1
Host: example.com
402 HTTP响应
HTTP/1.1 200 O.K.
Content-Type: application/json
{
"authorization_endpoint":
"https://example.com/connect/authorize",
"issuer" : "https://example.com",
"token_endpoint": "https://example.com/connect/token"
"user_info_endpoint": "https://example.com/connect/user",
"check_id_endpoint": "https://example.com/connect/check_id",
"refresh_session_endpoint":
"https://example.com/connect/refresh_session",
"end_session_endpoint":
"https://example.com/connect/end_session",
"jwk_document": "https://example.com/jwk.json",
"registration_endpoint":
"https://example.com/connect/register",
"scopes_supported": ["openid"],
"flows_supported": ["code", "token"],
"iso29115_supported":
["http://www.idmanagement.gov/schema/2009/05/icam/openid-
trust-level1.pdf"],
"identifiers_supported": ["public", "ppid"]
}

图 4

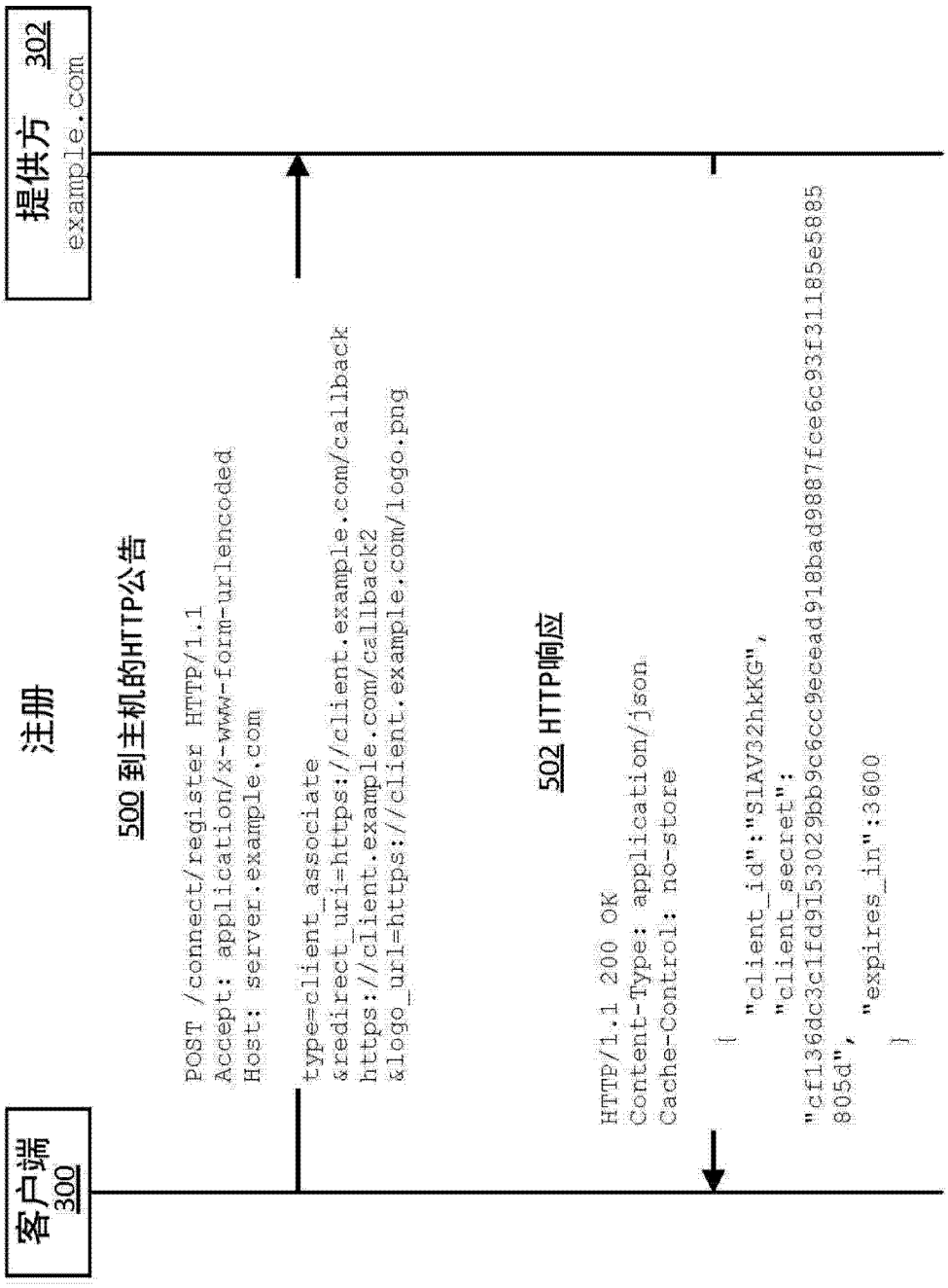

客户端
300
提供方 302
example.com
注册
500 到主机的HTTP公告
POST /connect/register HTTP/1.1
Accept: application/x-www-form-urlencoded
Host: server.example.com
type=client_associate
&redirect_uri=https://client.example.com/callback
https://client.example.com/callback2
&logo_url=https://client.example.com/logo.png
502 HTTP响应
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
{
"client_id":"S1AV32hkKG",
"client_secret":
"cf136dc3c1fd9153029bb9c6cc9ecead918bad9887fce6c93f31185e5885
805d",
"expires_in":3600
}

图 5

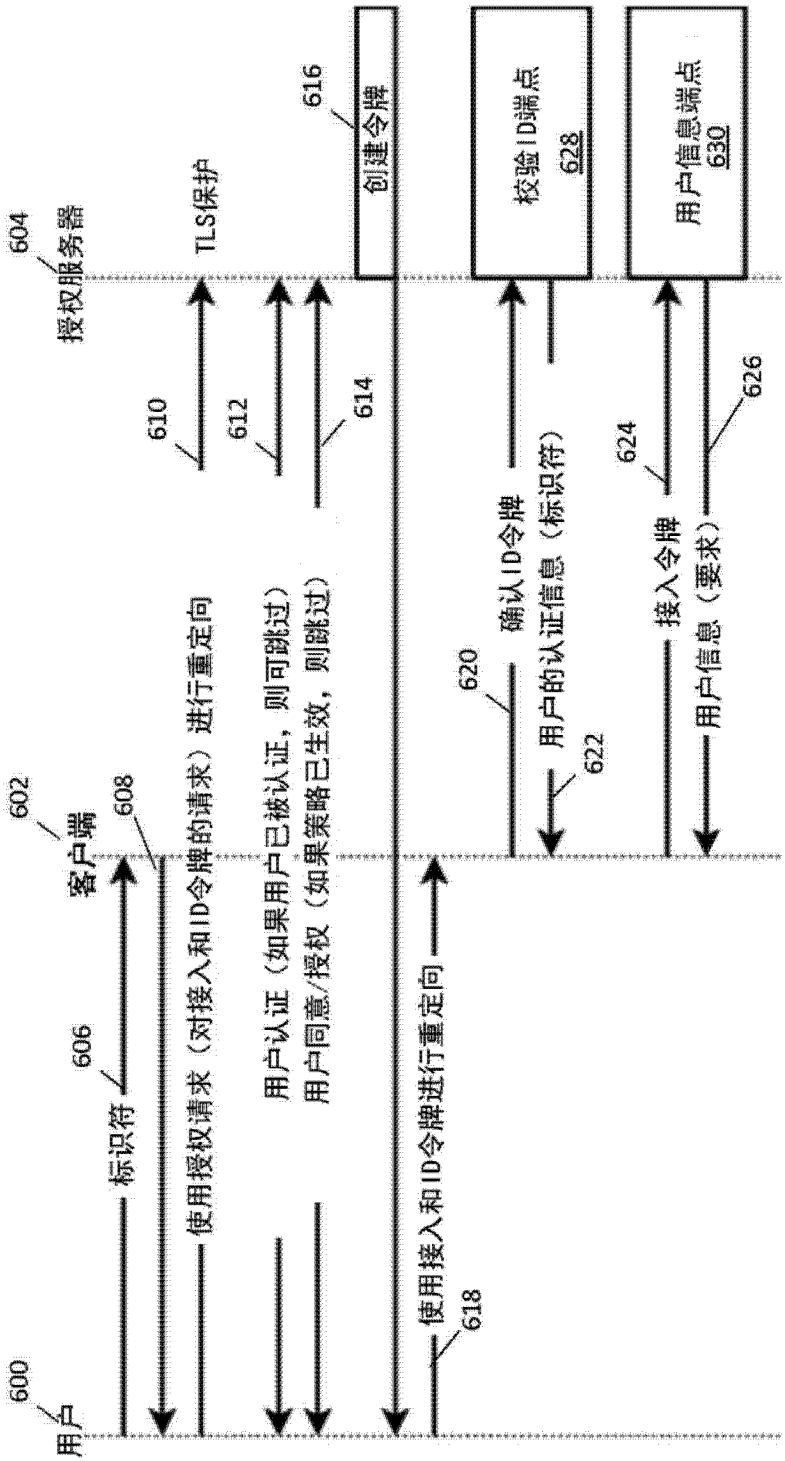

600
用户
602
客户端
604
授权服务器
606
标识符
608
使用授权请求（对接入和ID令牌的请求）进行重定向
610
TLS保护
612
用户认证（如果用户已被认证，则可跳过）
614
用户同意/授权（如果策略已生效，则跳过）
616
创建令牌
618
使用接入和ID令牌进行重定向
620
确认ID令牌
622
用户的认证信息（标识符）
624
接入令牌
626
用户信息（要求）
校验ID端点
628
用户信息端点
630

图 6

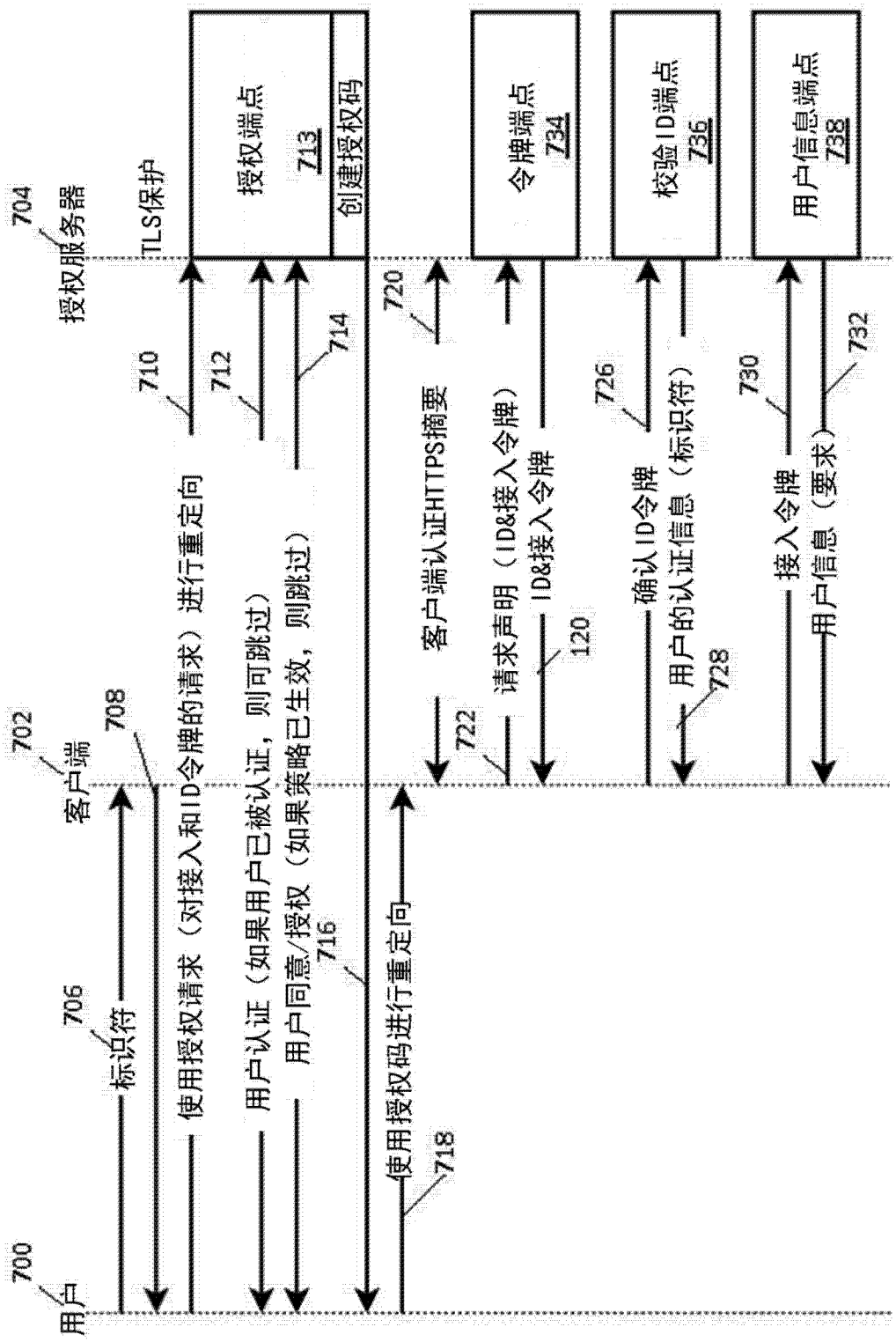

700
用户
702
客户端
704
授权服务器
TLS保护
706
标识符
708
使用授权请求（对接入和ID令牌的请求）进行重定向
710
用户认证（如果用户已被认证，则可跳过）
712
用户同意/授权（如果策略已生效，则跳过）
714
授权端点
713
创建授权码
716
使用授权码进行重定向
718
720
客户端认证HTTPS摘要
722
请求声明（ID&接入令牌）
ID&接入令牌
120
令牌端点
734
726
确认ID令牌
用户的认证信息（标识符）
728
校验ID端点
736
730
接入令牌
用户信息（要求）
732
用户信息端点
738

图 7

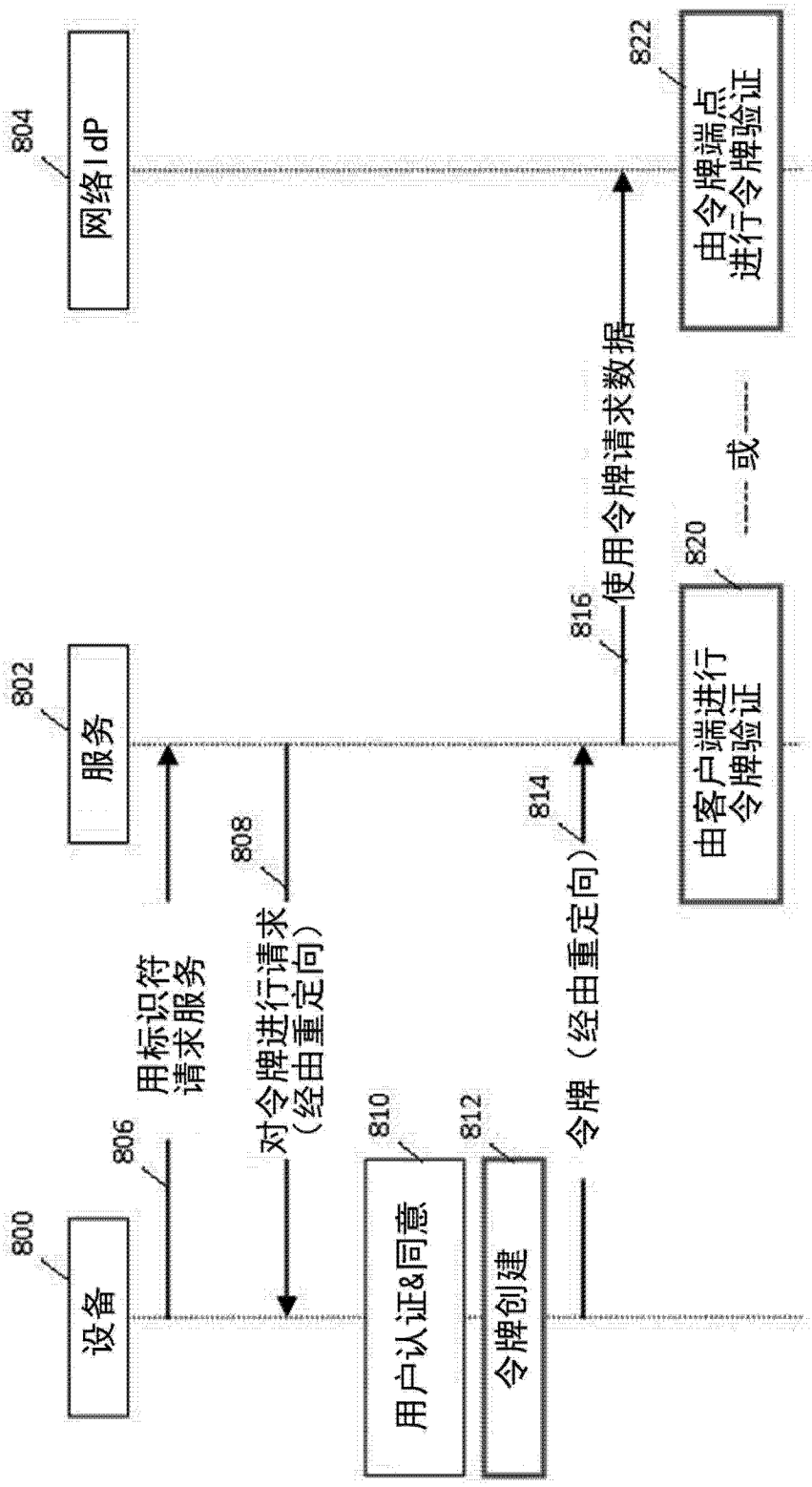

800
设备
802
服务
804
网络IdP
806
用标识符请求服务
808
对令牌进行请求（经由重定向）
810
用户认证&同意
812
令牌创建
814
令牌（经由重定向）
816
使用令牌请求数据
820
由客户端进行令牌验证
822
由令牌端点进行令牌验证
或

图 8

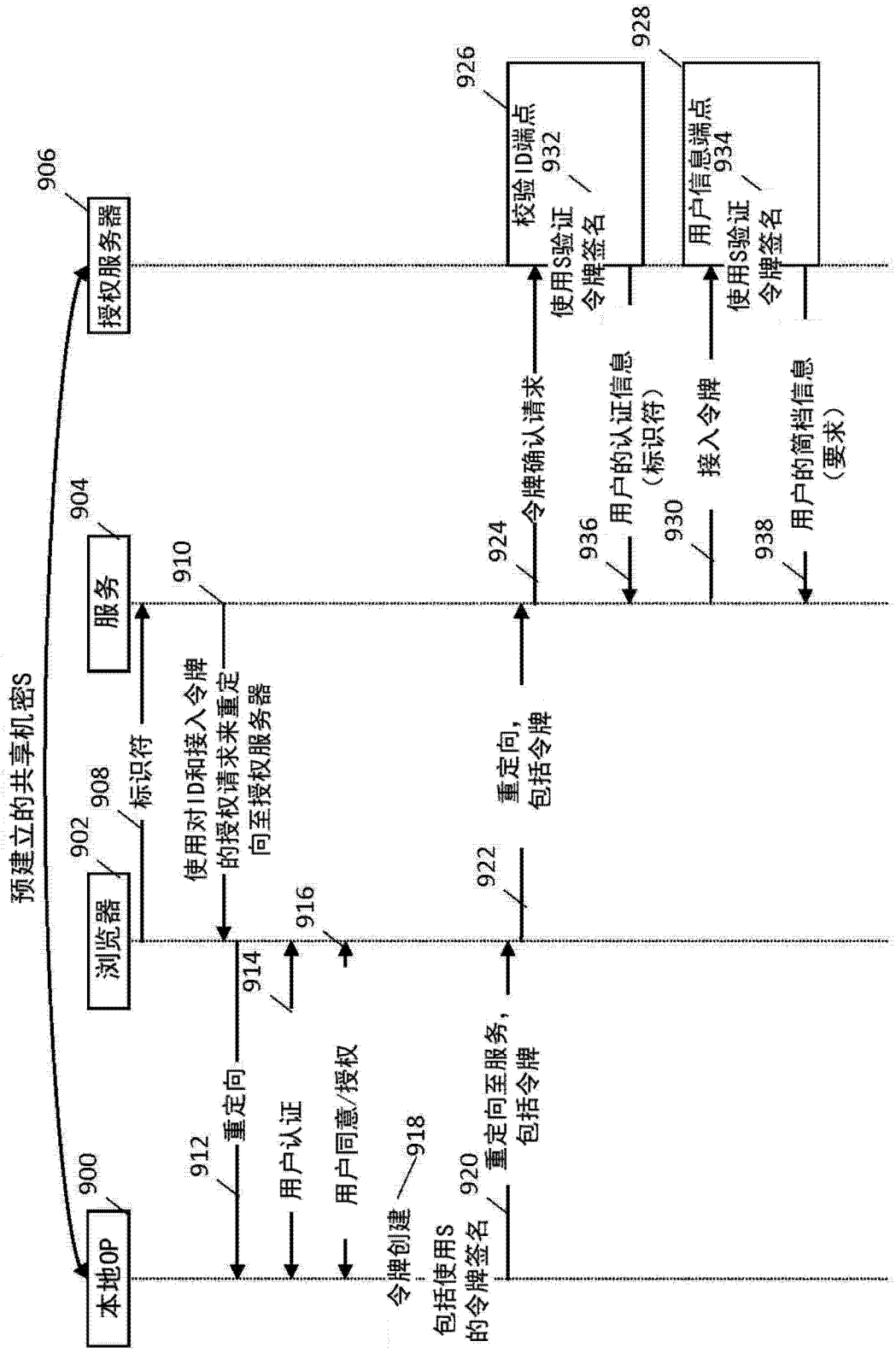

预建立的共享机密S
本地OP
900
浏览器
902
908
标识符
服务
904
910
使用对ID和接入令牌的授权请求来重定向至授权服务器
授权服务器
906
912
重定向
914
用户认证
916
用户同意/授权
918
令牌创建
包括使用S的令牌签名
920
重定向至服务，包括令牌
922
重定向，包括令牌
924
令牌确认请求
926
校验ID端点
932
使用S验证令牌签名
928
936
用户的认证信息（标识符）
930
接入令牌
用户信息端点
934
使用S验证令牌签名
938
用户的简档信息（要求）

图 9

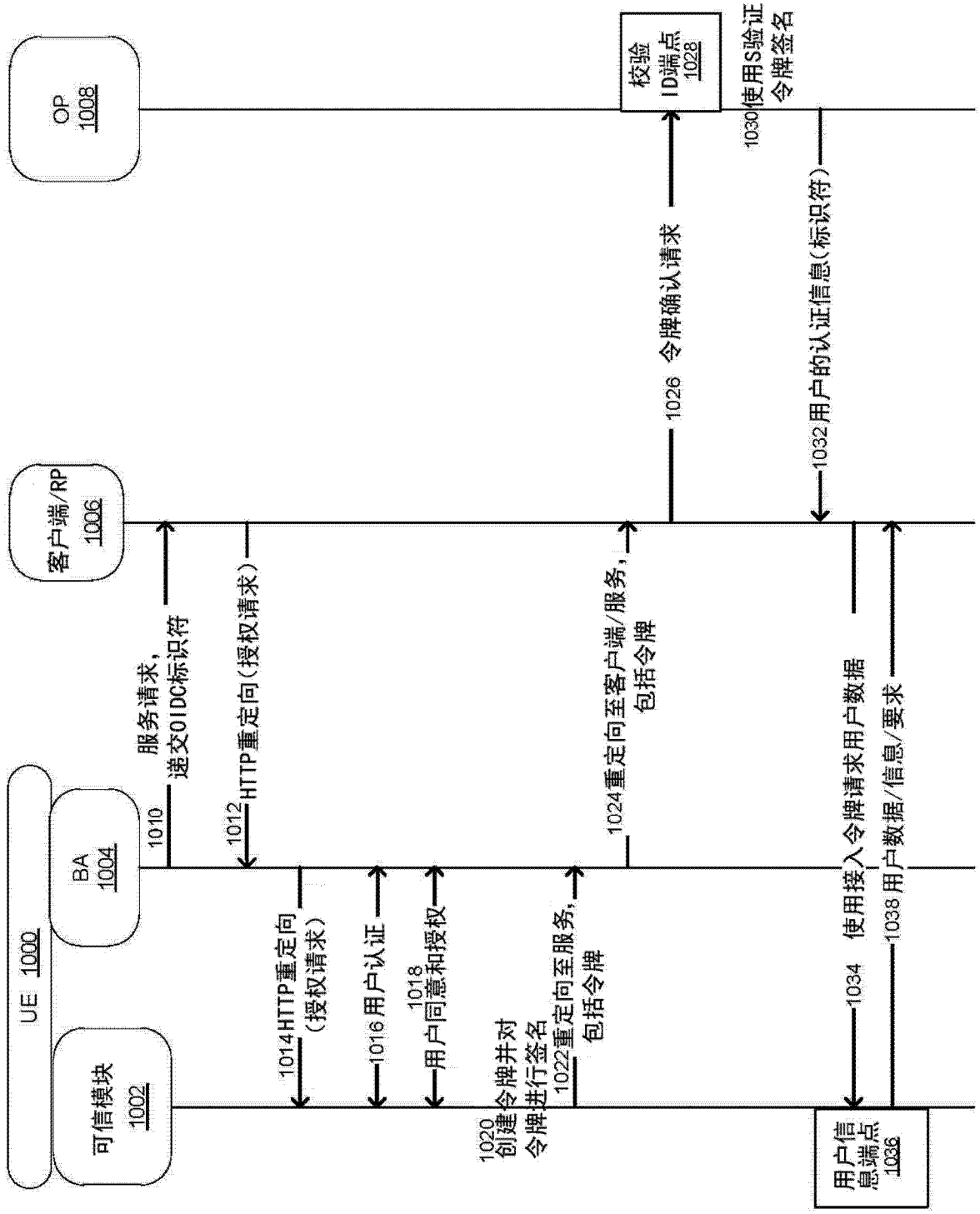

OP 1008
校验 ID端点 1028
1030使用S验证 令牌签名
客户端/RP 1006
1026 令牌确认请求
1032 用户的认证信息(标识符)
服务请求，
递交OIDC标识符
1010
1012 HTTP重定向(授权请求)
1024重定向至客户端/服务，
包括令牌
UE 1000
BA 1004
1014HTTP重定向
(授权请求)
1016 用户认证
1018
用户同意和授权
1020
创建令牌并对
令牌进行签名
1022重定向至服务，
包括令牌
1034 使用接入令牌请求用户数据
1038 用户数据/信息/要求
可信模块 1002
用户信息端点 1036

图 10

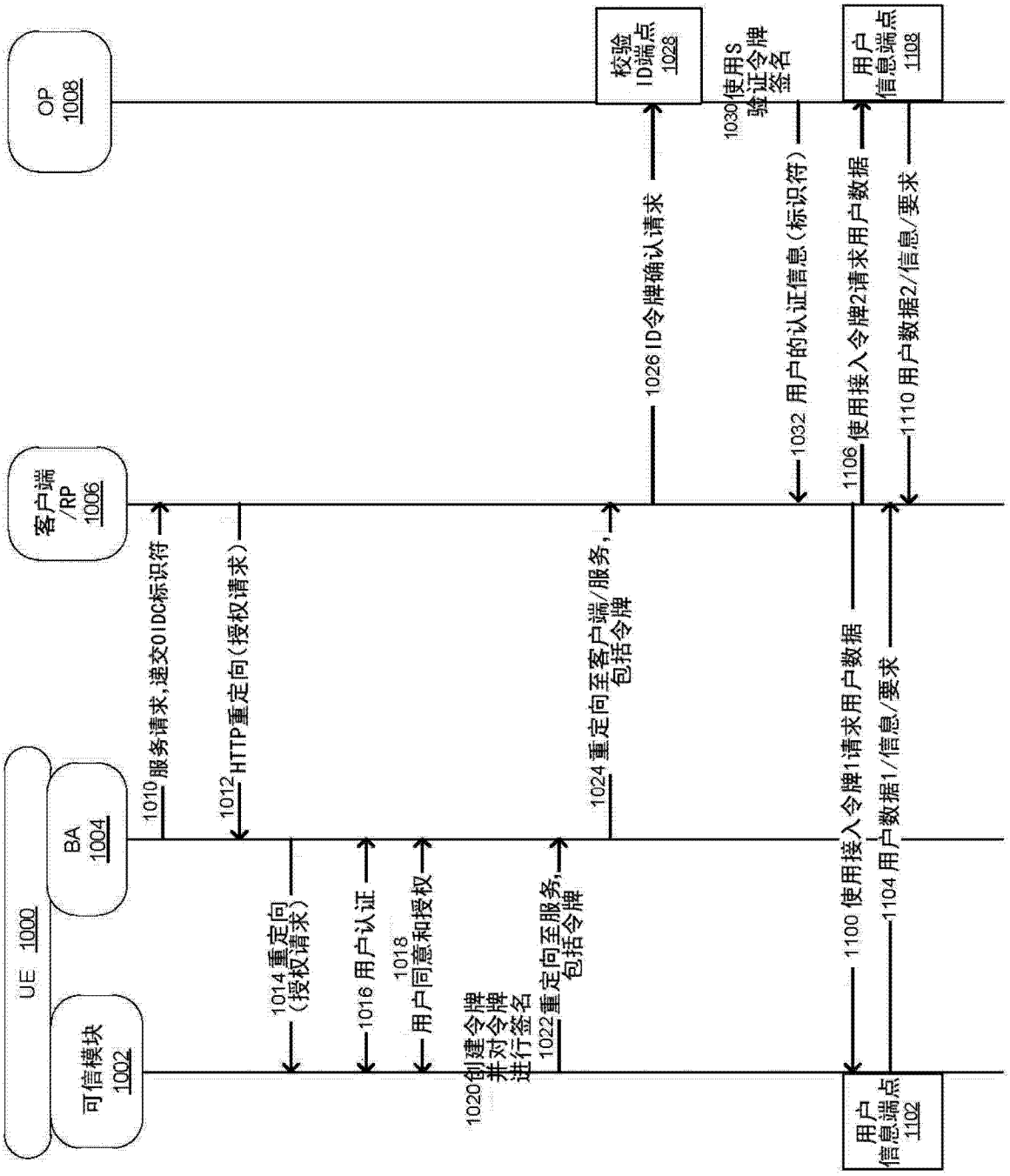

UE 1000
可信模块 1002
BA 1004
客户端/RP 1006
OP 1008
1010 服务请求,递交OIDC标识符
1012 HTTP重定向(授权请求)
1014 重定向(授权请求)
1016 用户认证
1018 用户同意和授权
1020 创建令牌并对令牌进行签名
1022 重定向至服务,包括令牌
1024 重定向至客户端/服务,包括令牌
1026 ID令牌确认请求
校验ID端点 1028
1030 使用S验证令牌签名
1032 用户的认证信息(标识符)
1100 使用接入令牌1请求用户数据
1102 用户信息端点
1104 用户数据1/信息/要求
1106 使用接入令牌2请求用户数据
用户信息端点 1108
1110 用户数据2/信息/要求

图 11

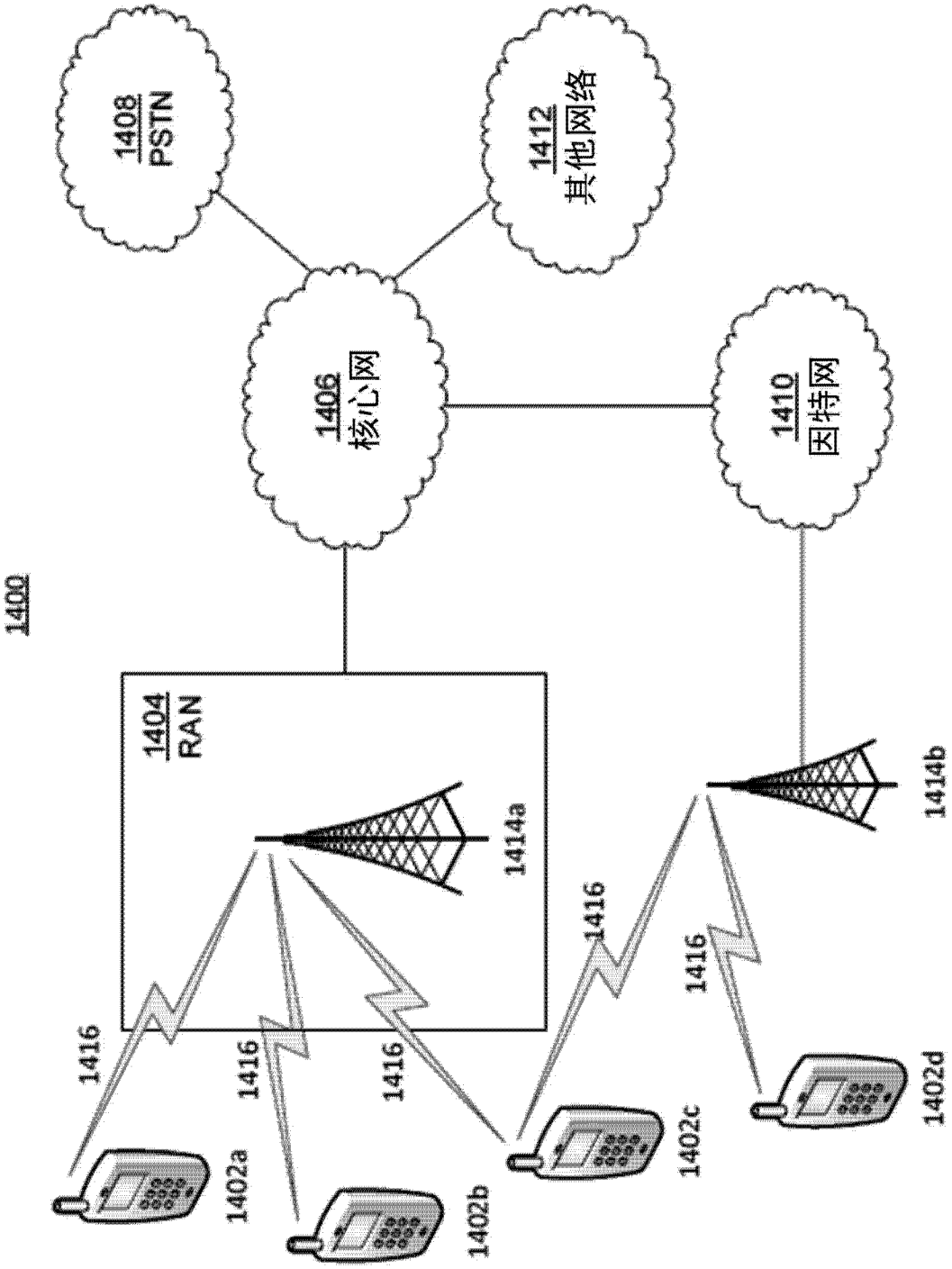

1400
1408 PSTN
1412 其他网络
1406 核心网
1410 因特网
1404 RAN
1414a
1414b
1416
1416
1416
1416
1416
1402a
1402b
1402c
1402d

图 12A

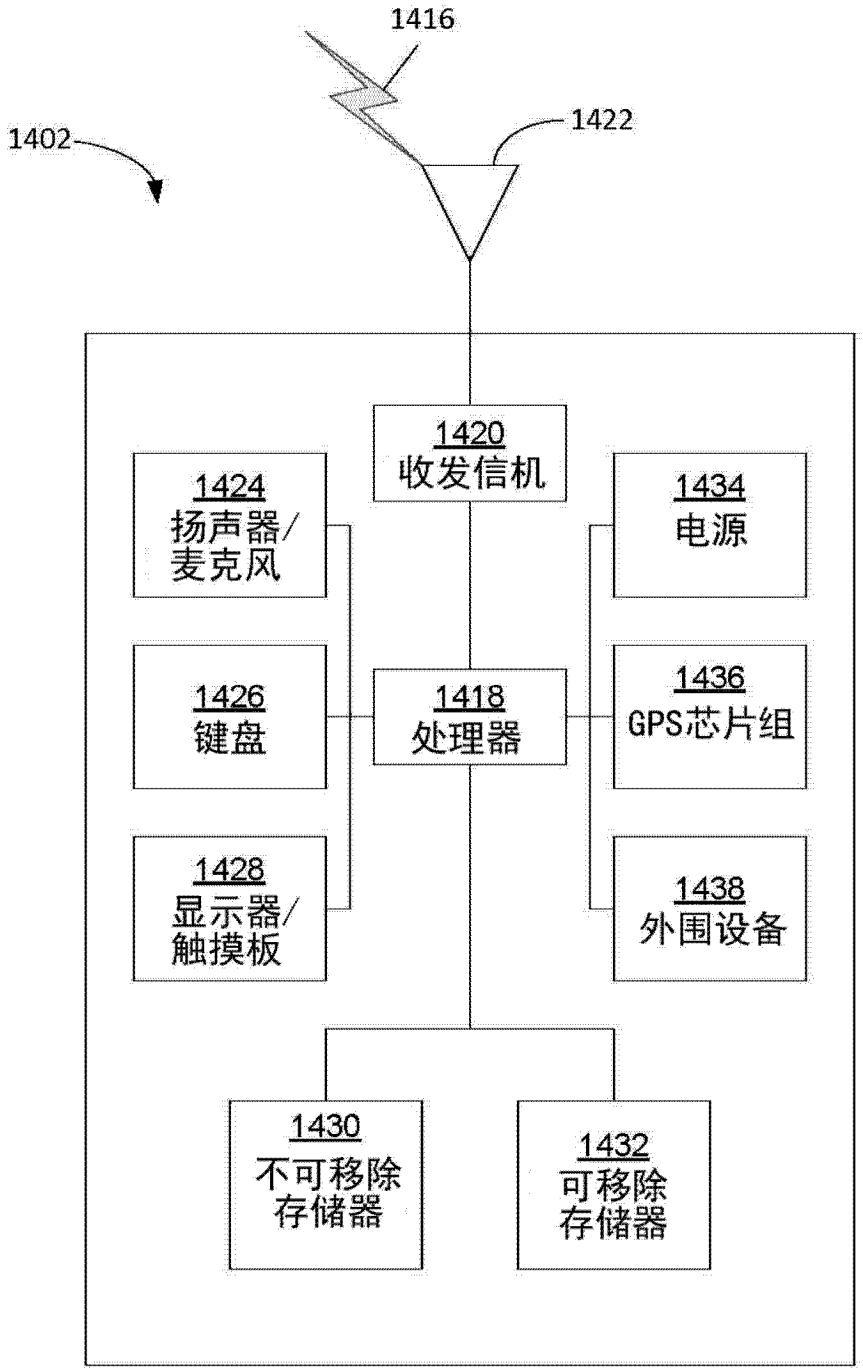

1416
1422
1402
1420
收发信机
1424
扬声器/
麦克风
1434
电源
1426
键盘
1418
处理器
1436
GPS芯片组
1428
显示器/
触摸板
1438
外围设备
1430
不可移除
存储器
1432
可移除
存储器

图 12B

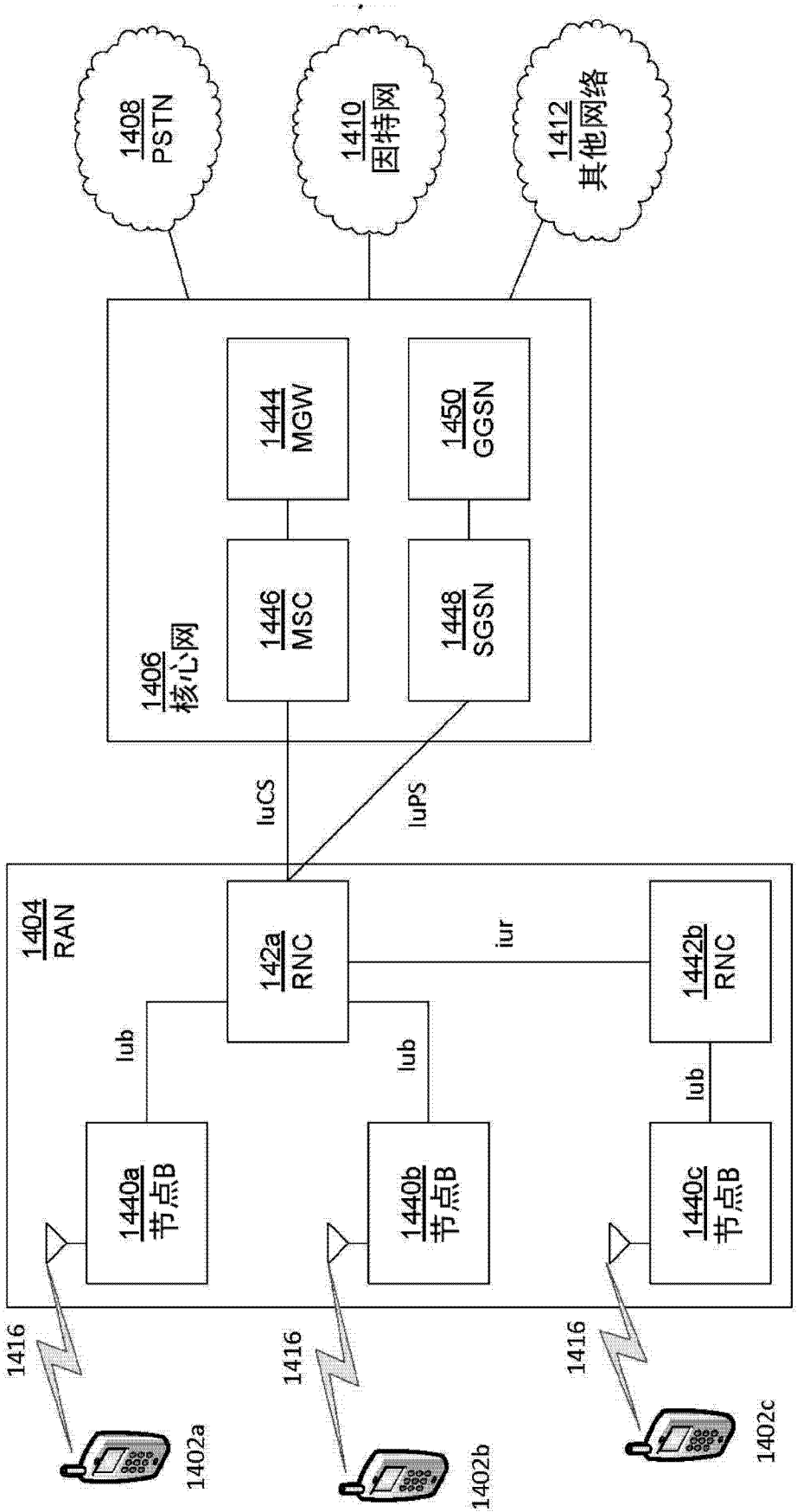

1408
PSTN
1410
因特网
1412
其他网络
1406
核心网
1444
MGW
1450
GGSN
1446
MSC
1448
SGSN
IuCS
IuPS
1404
RAN
142a
RNC
1442b
RNC
iur
Iub
Iub
Iub
1440a
节点B
1440b
节点B
1440c
节点B
1416
1416
1416
1402a
1402b
1402c

图 12C