(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 101069402 B
(45)授权公告日 2010.11.03

(21)申请号 200580041107.X
(22)申请日 2005.09.30
(30)优先权数据
PCT/EP2004/012052 2004.10.26 EP
(85)PCT申请进入国家阶段日
2007.05.30
(86)PCT申请的申请数据
PCT/EP2005/010590 2005.09.30
(87)PCT申请的公布数据
WO2006/045402 EN 2006.05.04
(73)专利权人 意大利电信股份公司
地址 意大利米兰
(72)发明人 保罗·德卢蒂斯
加埃塔诺·迪卡普里奥
科拉多·莫伊索
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 康建忠
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
H04W 12/06(2009.01)
(56)对比文件
WO 2004/064442 A1,2004.07.29, 全文.
US 2003/0163733 ,2003.08.28, 全文.
WO 01/67716 A1,2001.09.13, 全文.
CN 1346561 A,2002.04.24, 全文.
WO 01/03402 A1,2001.01.11, 全文.
审查员 田琳琳

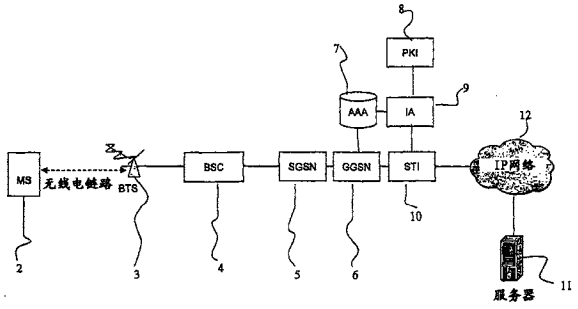
权利要求书 3 页 说明书 19 页 附图 11 页

(54)发明名称

透明地验证访问web服务的移动用户的方法和系统

(57)摘要

本发明涉及一种用于验证第一网络(例如,GPRS/GSM网络)的订户以通过第二网络访问应用服务的系统和方法,其中,第二网络是分组数据网络(PDN),例如,互联网。根据本发明优选实施例的系统包括:移动站MS(2),连接到蜂窝式网络,并且适于产生包含在数据包中的访问请求消息,用符合应用层协议的语法来表示所述访问请求消息;分配服务器AAA(7),适于向所述订户分配在所述第二网络中的地址(订户地址)并提供订户地址与第一订户标识符之间的映射;网关(6)(例如,GGSN),其将第一网络连接到第二网络并向MS 2分配订户地址;服务令牌注入器STI(10),与网关(6)链接,并适于截取从端点站产生并通过网关(6)被定向到第二网络的数据包,在数据包中至少捕获订户地址;标识局逻辑实体(9),与STI 10链接并适于执行以下功能:从第一逻辑实体接收订户地址和访问请求消息,识别访问请求消息的应用层协议,向分配服务器请求第一订户标识符,根据应用层协议产生验证令牌,其中所述令牌包括第二订户标识符,并将所述验证令牌关联到访问请求消息。



CN 101069402 B

1. 一种用于验证第一网络的订户以通过第二网络访问应用服务的方法，其中，第二网络是分组数据网络 (PDN)，并且对应用服务的访问是以封装在数据包中的访问请求消息的形式的，所述数据包包括被分配给所述订户的所述第二网络中的订户地址，以及用符合应用层协议的语法表示的所述访问请求消息，所述方法包括以下步骤 ：

a) 截取到第二网络的访问请求消息 ；

b) 识别应用层协议 ；

c) 提供所述订户地址与第一网络中的第一订户标识符之间的映射 ；

d) 根据所述应用层协议，产生包括第二订户标识符的第一验证令牌，所述第二订户标识符关联到所述第一订户标识符 ；

e) 将所述第一验证令牌关联到访问请求消息 ；以及

f) 将带有关联到所述访问请求消息的所述第一验证令牌的访问请求消息发送到第二网络。

2. 如权利要求 1 所述的方法，其中，第二网络是 IP 网络，订户地址是 IP 地址。

3. 如权利要求 1 或 2 所述的方法，其中，第一网络是移动网络。

4. 如权利要求 3 所述的方法，其中，移动网络是分组交换蜂窝式网络。

5. 如权利要求 4 所述的方法，其中，分组交换蜂窝式网络是 GPRS 网络。

6. 如权利要求 4 所述的方法，其中，分组交换蜂窝式网络是 EDGE 或 UMTS 网络。

7. 如权利要求 1 所述的方法，其中，第一订户标识符与第二订户标识符彼此不同。

8. 如权利要求 7 所述的方法，其中，第一网络是 GSM 网络，第一订户标识符是基于 SIM 的标识。

9. 如权利要求 8 所述的方法，其中，基于 SIM 的标识是关联到 GSM 网络中的订户的 IMSI。

10. 如权利要求 7 所述的方法，其中，第二订户标识符是关联到第一订户标识符的假名。

11. 如上述权利要求 1 或 2 所述的方法，其中，步骤 e) 包括在访问请求消息中包括第一验证令牌。

12. 如上述权利要求 1 或 2 所述的方法，在步骤 d) 之后还包括以下步骤 ：用数字签名加密第一验证令牌。

13. 如上述权利要求 1 或 2 所述的方法，其中，用符合访问请求消息的应用层协议的语法来表示所述第一验证令牌。

14. 如上述权利要求 1 或 2 所述的方法，其中，从 SIP、HTTP 和 HTTP 上的 SOAP 的组中选择应用层协议。

15. 如权利要求 1 所述的方法，其中，应用层协议是 SIP 或 HTTP，根据 SAML 标准来指定所述第一验证令牌。

16. 如权利要求 1 所述的方法，其中，第一网络是固定接入网络。

17. 如权利要求 16 所述的方法，其中，固定接入网络使用数字订户线路 (xDSL) 接入技术。

18. 如权利要求 16 所述的方法，其中，第一订户标识符是登录 ID。

19. 如权利要求 1 所述的方法，在步骤 f) 之后还包括以下步骤 ：

g) 在应用服务通过所述第二网络接收带有所述关联的第一验证令牌的所述访问请求；

h) 产生对所述接收的访问请求消息的第一响应消息；

i) 产生第二验证令牌并将所述第二验证令牌包括在所述第一响应消息中；

j) 截取包括所述第二验证令牌的所述第一响应消息；

k) 从所述第一响应消息提取所述第二验证令牌，以及

l) 检验所述第二验证令牌，如果验证是肯定的，则将第二响应消息发送到第一网络。

20. 如权利要求 19 所述的方法，在步骤 g) 之后还包括以下步骤：检验所述第一验证令牌。

21. 一种用于验证多个第一网络的订户以访问应用服务的方法，其中，通过权利要求 1 的方法实施对来自每个第一网络的订户的验证。

22. 如权利要求 1 或 21 所述的方法，还包括步骤：提供第一验证令牌与所请求的应用服务之间的映射。

23. 如权利要求 22 所述的方法，其中，在第一验证令牌与所请求的应用服务之间的映射包括：从访问请求消息提取所请求的服务的 URI。

24. 如权利要求 22 所述的方法，其中，第二订户标识符是关联到第一订户标识符并关联到所请求的应用服务的假名。

25. 一种用于验证第一网络的订户以通过第二网络访问应用服务的系统，其中，第二网络是分组数据网络 (PDN)，所述系统包括：

订户站 (2、68)，耦合到第一网络，并且适于产生封装在数

据包中的访问请求消息，用符合应用层协议的语法来表示所述访问请求消息；

分配服务器 (7、26)，适于向所述订户分配在所述第二网络中的订户地址并提供所述订户地址与第一网络中的第一订户标识符之间的映射；

网关 (6、29)，适于执行以下功能：从订户站 (2) 接收访问请求消息，将第一网络连接到第二网络并且向订户站分配由所述分配服务器 (7,26) 返回的订户地址；

第一逻辑实体 (10、65)，与网关 (6、29) 链接，并且适于截取从订户站 (2、18) 产生的并通过网关 (6、29) 被定向到第二网络的数据包，并且至少在所述数据包中捕获所述订户地址，以及

第二逻辑实体 (9、64)，与第一逻辑实体 (10、65) 链接并适于执行以下功能：

从第一逻辑实体接收订户地址和访问请求消息，

识别访问请求消息的应用层协议，

向分配服务器请求第一订户标识符，以及

根据应用层协议产生第一验证令牌，所述令牌包括关联到所述第一订户标识符的第二订户标识符，

其中，第一逻辑实体或第二逻辑实体适于将所述第一验证令牌关联到访问请求消息。

26. 如权利要求 25 所述的系统，其中，分配服务器 (7、26) 和网关 (6、29) 包括在第一网络中。

27. 如权利要求 25 所述的系统，其中，第一逻辑实体 (10、65) 和第二逻辑实体 (9、64) 包括在第一网络中。

28. 如权利要求 25 所述的系统，其中，第一网络是移动网络，订户站 (2) 是经由无线链路耦合到第一网络的移动站。

29. 如权利要求 28 所述的系统，其中，第一网络是分组交换蜂窝式网络。

30. 如权利要求 28 或 29 之一所述的系统，其中，网关 (6) 是 GGSN。

31. 如权利要求 25 所述的系统，其中，分配服务器 (7、26) 是认证 - 授权 - 计费 (AAA) 服务器。

32. 如权利要求 25 所述的系统，其中，第二网络是 IP 网络 (12、22)。

33. 如权利要求 25 所述的系统，还包括 ：证明逻辑实体 (8、63)，其在逻辑上链接到第二逻辑实体 (9、64) 并适于加密第一验证令牌。

34. 如权利要求 25 所述的系统，其中，第一逻辑实体 (10、65) 是应用层防火墙。

35. 如权利要求 25 所述的系统，其中，第一网络是固定接入网络，订户站是经由有线链路 (67) 耦合到第一网络的用户宅室设备 (68)。

36. 如权利要求 35 所述的系统，其中，第一用户标识符是登录 ID。

37. 如权利要求 25 所述的系统，其中，所述第一逻辑实体 (10、65) 还适于截取通过第二网络发送的并通过网关 (6、29) 定向到所述订户站 (2、68) 的响应消息。

38. 如权利要求 37 所述的系统，其中，所述响应消息包括第二验证令牌。

透明地验证访问 web 服务的移动用户的方法和系统

技术领域

[0001] 本发明涉及一种用于对于分组数据网络（例如，互联网）识别第一网络的订户的验证方法和系统。具体说来，开发本发明以便通过使用与移动网络中的订户相关的订户标识，而将本发明用于对分组数据网络验证移动网络的订户的过程。

背景技术

[0002] 从远程位置访问专用或公共分组数据网络 (PDN)（例如，互联网）的用户数量正在急剧增长。此外，不管人们在什么位置，均可向他们提供多媒体服务的景象推动了使用分组交换连接（例如，使用互联网协议 (IP)）的蜂窝网络的发展，其中，使用分组交换连接意味着虚拟连接总是可用于网络中的任意其它端点。基于分组的无线通信服务的标准包括：通用分组无线业务 (GPRS)、用于 GSM 演进的增强数据率 (EDGE) 以及通用移动电信服务 (UMTS)。

[0003] 近来，由于成本的降低以及连接性能前所未有的增强，在用户室内安装了越来越多的高速数据通信系统。作为示例，这些数据通信系统工作于公共交换电话网络 (PSTN) 的相同铜双绞线上，以便连接到互联网。尽管通过普通电话线的互联网连接还可使用其它高速调制解调器，但是所述互联网连接通常通过数字订户线路 (DSL) 接入技术来进行。DSL 使用专门的调制解调器，以便通过用于将电话服务带入家庭的标准铜线实现订户的家庭与最近电话中心局之间的高速数据传送。存在若干种 DSL 通信方案（通常称为 xDSL 技术），但是商业上可用的最普通形式之一是 ADSL（异步 DSL），其中，下行（到订户）数据率比上行（来自订户）数据率快几倍。

[0004] 近年来受到关注的另一接入技术是光纤到户 (FTTH) 的高速宽带接入系统，其中，光纤从电话交换机进入订户的室内。

[0005] 在短程无线互联网连接中，具有内置无线性能的计算机或手持设备（例如，PDA）使用无线电技术在接入点或网关内的任何地方发送和接收数据，其中，所述接入点或网关充当广播和接收基站并充当无线网络与有线网络之间的接口。例如，无线装置与接入点之间的无线电技术可基于 IEEE 802.11 标准 (Wi-Fi ® 规范）或 IEEE 802.16 标准 (WiMAX 规范）。

[0006] 宽带接入技术使得服务运营商能够扩展他们提供给商业用户和家庭用户两者的内容和服务。例如，用户可向一个或多个服务运营商预订多种服务或应用，诸如语音服务、互联网访问服务、视频服务、游戏服务等。可通过诸如 DSL 线路的单个网络连接来传递可经由专用或公共 PDN（例如，互联网）提供的这些服务和 / 或应用。

[0007] 另一方面，数量持续增长的可在 PDN 上提供的服务在诸如按每次会话付费的情况下，仅准许授权用户对需要订阅的服务或者根据其用户的简档定制的服务进行访问。某些传统验证程序使用密码（例如，通过自动装置识别的字符串），其允许用户访问受保护的文件或输入 / 输出装置。

[0008] 申请人考虑了以下内容。首先，对于用户，基于密码的验证系统必然是不透名的，

所述用户当进入服务时必须输入他的密码。当用户想要在会话期间访问多个服务时，上述处理就变得特别不方便。其次，尽管密码在技术上易于实现，但是由于密码易被复制或盗用，所以密码容易泄漏。

[0009] 移动通信系统控制由相应于授权用户的移动基站使用的网络的资源。在传统的全球移动通信系统 (GSM) 中，移动站 (MS) 包括订户标识模块 (SIM)，所述用户标识模块包含订户的信息，所述信息包括用于允许 MS 访问 GSM 系统的网络基础结构的数据。由于 SIM 提供识别各个用户的唯一手段，所以可将 SIM 看作安全装置；所述 SIM 使用密码和固有计算性能来存储秘密信息，所述秘密信息决不会在外部以原始形式被泄漏。

[0010] 在传统 GSM 网络系统中，几个数据库可用于呼叫控制以及验证和安全目的，所述数据库典型地为：归属位置寄存器 (HLR)、拜访位置寄存器 (VLR)、验证中心 (AU) 和设备标识寄存器 (EIR)。对于向网络运营商注册的所有用户，永久数据（诸如用户的简档）以及临时数据（诸如用户的当前位置）被存储在 HLR 中。在对用户进行呼叫的情况下，总是首先查询 HLR 以确定用户的当前位置。VLR 负责一组位置区域，并存储当前处于其负责的区域的那些用户的数据。这其中包括部分永久用户数据，这些数据已经被从 HLR 发送到 VLR 以进行更快的访问。但是所述 VLR 还可分配并存储诸如临时标识的本地数据。AUC 产生并存储与安全性有关的数据（诸如用于验证和加密的密钥），而 EIR 注册设备数据，而不是订户数据。

[0011] GSM 明确地在用户与设备之间进行区分并分别处理他们。已定义若干订户和设备标识符；需要它们来管理订户移动性并对所有留有的网络部件进行寻址。国际移动站设备标识 (IMEI) 作为一种序列号，唯一地识别国际间的移动站 (MS)。由设备制造商分配 IMEI，并由网络运营商将其注册，所述网络运营商将 IMEI 存储在 EIR 中。每个注册的用户（即，订户）由它的国际移动订户标识 (IMSI) 唯一识别。所述 IMSI 典型地存储于 SIM 中。只有将具有有效 IMSI 的 SIM 插入具有有效 IMEI 设备，MS 才可操作。移动站的“实际电话号码”是移动订户 ISDN 号 (MSISDN)。将所述移动订户 ISDN 号分配给订户（即，他或她的 SIM），从而移动站装置可具有若干取决于 SIM 的 MSISDN。

[0012] 通用分组无线业务 (GPRS) 是为数字蜂窝网络（例如，GSM 或个人通信服务 -PCS）设计的服务，其最初针对 GSM 而开发。GPRS 大大提高并简化了对分组数据网络（例如，对互联网）的无线访问。GPRS 应用分组无线电原理，以在移动站与外部分组数据网络之间通过有效的方式来传送用户数据包。可直接将用户数据包从 GPRS 移动站路由到其它 GPRS 终端或 PDN，或者直接将用户数据包从所述其它 GPRS 终端或 PDN 路由到所述 GPRS 移动站。在当前版本的 GPRS 中支持基于互联网协议 (IP) 的网络（例如，全球互联网或专用 / 公司内联网）。

[0013] GPRS 对网络资源和无线电资源的使用进行优化，并且不掌管对安装的 GSM 基础结构的移动交换中心 (MSC) 基站的改变。为了结合到现有 GSM 体系结构，GPRS 体系结构通常包括网关 GPRS 支持节点 (GGSN) 和服务 GPRS 支持节点 (SGSN)。位于与 MSC 相同分层级别的 GGSN 充当到诸如互联网的其它分组数据网络的网关。SGSN 是服务节点，其实现到启用 GPRS 的移动装置的虚拟连接并能够传递数据。SGSN 将数据发送到移动站，从移动站接收数据，并保存关于移动站 (MS) 的位置的信息。SGSN 在 MS 与 GGSN 之间通信。

[0014] GPRS 安全性功能典型地等同于现有 GSM 安全性。SGSN 基于与现有 GSM 中相同的

算法、密钥和准则来执行验证和密码设置程序。GPRS 使用针对分组数据传输优化的密码算法。

[0015] 为了在成功附 GPRS 之后与外部 PDN 交换数据包，MS 必须申请一个或多个在 PDN 中使用的地址，例如，在 PDN 是 IP 网络的情况下，MS 必须申请 IP 地址。所述地址被称为 PDP 地址（分组数据协议地址）。对于每个会话，创建所谓的 PDP 语境，其描述会话的特征。其包含 PDP 类型（例如，IPv4）、请求的服务质量 (QoS) 以及用作到 PDN 的访问点的 GGSN 的地址。将所述语境存储在 MS、SGSN 和 GGSN 中。在活动 PDP 语境下，移动站对于外部 PDN "可视"，并且移动站能够发送和接收数据包。所述两个地址，PDP 与 IMSI 之间的映射使得 GGSN 能够在 PDN 与 MS 之间传送数据包。用户可以在给定时间使若干同时的 PDP 语境处于活动状态。

[0016] 第 01/67716 号 WO 专利申请描述了一种将移动终端的 MSISDN 号与临时分配的 IP 地址关联以在无线应用协议 (WAP) 网络中用于验证、计费和个性化处理的方法。

[0017] 第 01/03402 号 WO 专利申请描述了一种用于在第二网络（例如，IP 网络）中识别第一网络（即，GPRS 网络）的订户的方法，其中，将第二网络的地址分配给订户。产生关于第二网络的地址（例如，IP 地址）与订户的标识之间的映射的信息，并将所述信息发送到第二网络。所述订户的标识可以是订户的 IMSI 和 / 或 MSISDN。

[0018] 申请人已注意到：通过将订户的标识关联到 IP 地址来验证对 IP 网络的访问通常容易受到 IP 包的电子欺骗，其允许互联网上的入侵者有效地冒充本地系统的 IP 地址。此外，所述两个网络应该直接连接（利用可行的可路由专用 IP 地址），或者它们需要兼容的地址规划。

[0019] 第 01/17310 号 WO 专利申请描述了一种用于通过应用 GSM 安全性原理来验证请求访问 PDN 的用户的系统。经由接入网络将远程主机连接到 PDN，将 MS 耦合到与 PDN 连接的移动网络。响应于接收对 PDN 的用户请求，PDN 产生验证令牌，并经由接入网络和远程主机将所述验证令牌发送到用户，所述用户通过移动网络将验证令牌发送回 PDN，其中，PDN 比较验证令牌，以确定是否准许用户访问 PDN。

[0020] 申请人注意到公开的验证系统对于用户不透明，用户必须等待验证并且不得不将接收的验证令牌发送回 PDN。此外，由于远程服务器必须知道用户的电话号码，所以公开的系统可危及用户的隐私。

[0021] 第 2004/0132429 号美国专利申请描述了这样一种方法和系统，所述方法和系统能够在不必专门知道移动终端编程或任何 POP3 或 SMTP 参数的情况下，提供经由移动通信网络对电子邮件帐户的访问。使用默认 POP3/SMTP 服务器来预先配置移动终端。为了访问电子邮件帐户，使用标准 POP3/SMTP 经由移动网络在移动终端客户机与代理服务器之间建立通信。可只是基于用户的 MSISDN 来准许用户访问电子邮件帐户。

[0022] 可将通用移动电信服务 (UMTS) 看作 GSM/GPRS 网络的直接进化。UMTS 的安全功能基于在 GSM 中实施的内容（诸如对订户的验证），而某些安全功能已经被添加并且某些现有的安全功能已经被改善。

[0023] 分组交换采用作为比较短的消息数据块的数据包。所述数据包可以如在异步传输模式 (ATM) 中那样具有固定长度，或者可以如在帧中继或互联网协议 (IP) 中那样具有可变长度。一种期望的情况为基于分组的无线网络基础结构支持互联网电话。互联网电话或 IP

电话指的是一种将互联网性能与PSTN功能合并的应用。IP电话应用能够实现实时语音通信量通过互联网基础结构的传输以及与现有PSTN基础结构的无缝结合。尽管IP电话主要集中在语音呼叫方面，通常称为IP语音或VoIP，但是IP电话也可用于携带其它音频或多媒体应用，诸如传真、视频和调制解调器数据。

[0024] 为支持IP电话而研发的协议是会话启动协议(SIP)。SIP是用于设立，修改和撤销多媒体会话的信令传输协议，并且与它使用的协议结合向潜在的会话参与者描述通信会话的会话特征。这些会话包括互联网多媒体会议、互联网电话呼叫和多媒体分布。用于创建会话的SIP INVITE携带允许参与者在一组兼容媒体类型方面达成一致的会话描述。SIP通过向用户的当前位置代理请求或将所述请求重新定向到用户的当前位置来支持用户移动性。通常，实时协议(RTP)用于在通信会话期间交换多媒体(音频、语音或数据)，但是SIP允许使用任何传输协议。SIP使用客户机-服务器模型，其中，客户机发起SIP请求，服务器对请求作出响应。在SIP中，端点实体称为用户实体，其既作为客户机(用户代理客户机)，即，SIP请求的发起者，也作为返回响应的服务器(用户代理服务器)。

[0025] 在可被看作敌对环境的互联网中部署SIP，其中，SIP部件和消息可暴露于各种安全威胁和攻击。在基于SIP的系统中，可在不同的层实现验证措施，所述不同的层包括应用层、传输层和网络层。

[0026] 在2004年8月31日从互联网上在http://www.ietf.org/internet-dratfs/draft-tschofenig-sip-saml-00.txt下载的H.Tschofenig等人的“Using SAML for SIP”中提出一种使用与SIP合作的安全声明标记语言(SAML)来实现授权机制的方法。描述一种增强的声明网络的标识方案，其中，所述增强基于由验证服务(AS)声明的属性。想要与第二用户的第一用户将SIP INVITE发送到她的优选AS。根据选择的SIP安全机制，摘要验证S/MIME或传输层安全被用来向AS提供关于第一用户标识的有力保证。在第一用户被验证和授权之后，将SAML声明附于SIP消息。

[0027] 随着开始通过互联网提供越来越多的服务，提供用于访问所述服务的有效和安全单一签入(SSO)机制变得非常重要。通过互联网提供的服务通常分布于多个服务器上，所述服务器处于相对于彼此的远程位置。通过SSO机制，用户可通过在一个或少量服务器上运行的验证程序来验证他的标识并授权使用分布于多个远程服务器的多个服务。

[0028] 第01/72009号WO专利申请公开了一种SSO验证机制，其中，将令牌发送到请求被授权访问服务的用户。所述令牌可仅在一段时间内有效。将与验证有关的功能与服务分离，并且在会话期间不需要为访问多个服务中的新服务而重新进行验证。在发送令牌之前，用户通过表明他的凭证(例如，用户名和密码)为授权访问服务而进行注册。

[0029] 自由联盟计划是用于联合标识和基于标识的服务的开放标准组织。它提供用于SSO的标准，其允许用户在实现自由的位置一次性签入，并且当导向另一实现自由的位置时可进行无缝的签入，而不需要再次验证。在http://www.projectliberty.org/resourse/whitepapers公开的“Liberty ID-WSF-Web Services Framework”提供对自由ID-WSF的部件的概述。消息保护机制可包括基于令牌的机制，诸如根据Web服务安全(WS-安全)规范传播在SOAP头部块中的SAML声明。

[0030] 第2004/064442号WO专利申请公开了一种用于向在跨国移动网络运营商的分组无线电网络漫游的用户提供SSO服务的电信方法和系统，所述跨国移动网络运营商包括国

家网络运营商的联盟，这些国家网络运营商中的一个持有用户的预订。该电信系统还包括多个服务提供者，所述多个提供者已经就向作为包括在所述联盟中的任何国家网络运营商的订户的用户提供SSO服务与跨国移动网络运营商联盟签署了服务协议。每个服务提供者包括：用于将用户重新定向到作为联盟中的入口点的全球SSO前端基础结构的装置；用于从用户接收令牌的装置，其中，所述令牌是验证声明（SAML声明）或它的索引；用于从产生声明的位置检索声明的装置以及用于核查所述位置可信的装置。

[0031] 第2003/0163733号美国专利申请公开了一种电信系统，其包括用于对访问服务提供者的用户重新定向的装置，所述用户向与所述第二移动网络运营商达成协议的第二移动网络的验证代理机预订第一移动网络运营商。第一移动网络运营商和第二移动网络运营商属于某一联盟，并且验证代理机充当所述联盟到验证提供者的入口点。用户为了执行SSO服务请求向它们的验证提供者呈现不明确的标识，例如，MSISDN/IMSI。

发明内容

[0032] 本发明涉及一种验证第一网络的订户以便访问可通过作为分组数据网络(PDN)的第二网络访问的应用服务的方法和系统。应用服务指的是在应用层定义的服务，在这种环境下，应用层可表示为在传输层之上的层。具体说来，可由在开放系统互连(OSI)模型中定义的层7或根据TCP/IP协议的层5(通过不受限的方式)来表示应用层。应用服务的示例是通常由使用诸如HTTP、GET/POST、SMTP或SOAP的协议的客户机应用所使用的Web服务、通常通过浏览器的使用而访问的Web站点或者VoIP。

[0033] 申请人已注意到存在以下处理：就所述网络内的高级的安全性来验证诸如GSM网络的第一网络的订户。

[0034] 申请人还注意到：同样在第一网络是固定线路接入网络的情况下，可就所述网络内的高级安全性确认订户标识的有效性。在固定接入网络使用与公共交换电话网络(PSTN)共享的有线线路的情况下，诸如，在xDSL技术的情况下，在用户宅室设备(CPE)与到PDN的网关之间的通信使用安全和典型地专门有线链路，例如，标准电话铜线或光纤。

[0035] 虽然诸如Wi-Fi ®连接的无线连接由于到PDN的无线链路而传统上表征为相对低级的安全性，但是已经提出了解决方案，其确保网络访问的相对高级的安全性。高级安全性解决方案的示例是IEEE802.11i安全标准，该安全标例如在http://www.embedded.com/showArticle.jhtml？articleID＝34400002于2005年9月20日从互联网下载的D.Halasz的“IEEE 802.11i andwireless security”中有所描述。

[0036] 申请人已发现在第一网络中定义的订户标识可用于在应用层验证订户，在所述应用层操作通过PDN的应用服务。具体说来，根据本发明，可透明地验证订户以访问应用服务。

[0037] 在本发明的优选实施例中，请求通过PDN的服务的订户的第一网络是分组交换移动网络。更优选地，分组交换移动网络是基于GSM的GPRS标准。PDN通常是移动网络外部的网络，例如，IP网络。本发明同样应用于在相同的移动网络中主管掌管应用服务的应用服务器的情况，其中，订户从所述相同的移动网络开始会话，但是通过外部PDN来访问所述服务器。例如，应用服务器可位于移动运营商的增值服务(VAS)平台，其由IP网络来提供。具体说来，PDN可以是服务提供者的专用或公共网络。

[0038] 在本发明的另一实施例中，请求通过 PDN 的服务的订户的第一网络是固定接入网络，其中，订户通过使用用户宅室设备 (CPE)，诸如链接到 PC 的 DSL 调制解调器或链接到例如电视机或 TV 机顶盒的外围装置的家用网关，来访问 PDN。CPE 通过相对安全的有线线路或无线链路而上行链接到接入网络，所述有线线路或无线链路诸如专门电话线路、专门光纤或嵌入 IEEE 802.11i 安全标准的无线连接。

[0039] 根据本发明的优选实施例，固定接入网络是 xDSL 接入网络。

[0040] 对访问应用服务（以下也称为服务）的请求具有在应用层定义的访问请求消息的形式。

[0041] 本发明的一方面涉及一种用于验证第一网络的订户以通过第二网络访问应用服务的方法，其中，第二网络是分组数据网络 (PDN)，并且对应用服务的访问具有包含在数据包中的访问请求消息的形式，所述数据包包括被分配给所述订户的所述第二网络中的地址（订户地址），并且用符合应用层协议的语法表示所述访问请求消息，所述方法包括以下步骤：

[0042] a) 截取到第二网络的访问请求消息；

[0043] b) 识别应用层协议；

[0044] c) 提供所述订户地址与第一网络中的第一订户标识符之间的映射；

[0045] d) 产生包括第二订户标识符的第一验证令牌；

[0046] e) 将所述第一验证令牌与访问请求消息关联；以及

[0047] f) 将带有关联的第一验证令牌的访问请求消息发送到第二网络。

[0048] 本发明的另一方面涉及一种用于验证第一网络的订户以通过第二网络访问应用服务的系统，其中，第二网络是分组数据网络 (PDN)，所述系统包括：

[0049] 订户站，耦合到第一网络，并且适于产生包含在数据包中的访问请求消息，用符合应用层协议的语法来表示所述访问请求消息；

[0050] 分配服务器，适于向所述订户分配在所述第二网络中的地址（订户地址）并提供所述订户地址与第一网络中的第一订户标识符之间的映射；

[0051] 网关，适于执行以下功能：从订户站接收访问请求消息，将第一网络连接到第二网络并且向订户站分配订户地址；

[0052] 第一逻辑实体，与网关链接并适于截取从订户站产生并通过网关被定向到第二网络的数据包，并且至少在数据包中捕获订户地址，以及

[0053] 第二逻辑实体，与第一逻辑实体链接并适于执行以下功能：

[0054] 从第一逻辑实体接收订户地址和访问请求消息，

[0055] 识别访问请求消息的应用层协议，

[0056] 向分配服务器请求第一订户标识符，以及

[0057] 根据应用层协议产生第一验证令牌，所述令牌包括第二订户标识符，

[0058] 其中，第一逻辑实体或第二逻辑实体适于将验证令牌关联到访问请求消息。

附图说明

[0059] 图 1 示出本发明的实施例，其中，请求服务的订户的第一网络是 GPRS 系统，而第二网络是 IP 网络。

[0060] 图 2 描述根据第一网络是移动网络的本发明实施例存储在标识局 (IA) 中的信息表的示例。

[0061] 图 3 示出根据本发明优选实施例的对在应用服务器中主管的 Web 服务器的访问操作的处理示图。

[0062] 图 4 示出根据本发明另一实施例的连接到外部 NGN IP 网络的分组交换网络的框图。

[0063] 图 5 示意性示出根据本发明另一实施例的通过 NGN 到在 SIP 服务器中主管的 SIP 服务的访问操作的处理示图。

[0064] 图 6 显示根据本发明优选实施例的示例到在应用服务器中主管的 Web 站点的访问操作的处理示图。

[0065] 图 7 示出本发明的替换实施例，其中，请求服务的订户的第一网络是固定网络 (ADSL)，而第二网络是 IP 网络。

[0066] 图 8 描述根据第一网络是固定网络的本发明实施例存储在标识局 (IA) 中的信息表的示例。

[0067] 图 9 示出根据本发明另一优选实施例到在应用服务器中主管的 Web 服务的访问操作的处理示图。

[0068] 图 10 示出本发明的实施例，其中，请求服务的用户是多个（第一）网络的订户，而第二网络是 IP 网络。

[0069] 图 11 示意性示出根据本发明另一实施例在手动验证的情况下的处理示图。

具体实施方式

[0070] 图 1 示出本发明的优选实施例。在图 1 的实施例中，第一网络是 GPRS 系统，而第二网络是 IP 网络 12。图 1 的实施例可代表以下的示例性情况，其中，GPRS 网络的订户想要从她 / 他的移动站 (MS)2 通过 IP 网络访问在应用服务器 11 中主管的 Web 站点的服务。MS 2 以无线电方式连接到基站收发器 (BTS)2，其连接到基站控制器 (BTS)4。BTS 和 BSC 的组合功能通常称为基站子系统 (BSS)。从那里，服务 GPRS 支持节点 (SGSN)5 提供到 GGSN 的访问，所述 GGSN 用作到数据网络的网关，在这种情况下，所述数据网络为 IP 网络 12。SGSN 5 典型地基于与现有 GSM 中相同的算法、密钥和准则来执行验证和密码设置程序。

[0071] MS 2 可以是移动电话，MS 2 包括订户标识模块 (SIM)，所述 SIM 携带标识和验证信息，通过它们，蜂窝网络可识别蜂窝网络内的 MS 终端并授权它在网络中工作。

[0072] 为了发送和接收 GPRS 数据，MS 2 需要激活分组数据地址，即，该实施例中的 IP 地址，其将被用于访问服务。当订户请求服务时，MS 2 通过在 GGSN 6 终止的无线电网络来发送请求。使用特定协议，GGSN 将请求发送到认证 - 授权 - 计费 (AAA) 服务器 7，所述 AAA 服务器本身是公知的。作为示例，所述 AAA 服务器可以是远程验证拨入用户服务 (RADIUS) 服务器或动态主机配置协议 (DHCP) 服务器。在 AAA 服务器是 RADIUS 服务器的情况下，GGSN 包括 RADIUS 客户机，以便使用 RADISU 协议与 AAA 服务器通信。根据标准 GPRS 程序，AAA 服务器可基于任何数量的属性来验证订户，所述属性诸如网络访问标识符 (NAI) 或国际移动订户标识 (IMSI)。IMSI 是仅明确地与特定订户关联的标识号。IMSI 通常由移动网络运营商来分配，并且追踪对可行的特定订户的计费和服务供应。通常在 SIM 中携带 IMSI。

[0073] 或者，移动站国际 ISDN 号 (MSISDN) 可用来识别移动网络中的订户。然而，由于更多 MSISDN（即，电话号码）可关联到相同的 IMSI，所以 IMSI 是优选（但非限制）的订户标识符。

[0074] AAA 服务器向 MS 分配 IP 地址，随后将所述地址返回 GGSN。GGSN 向 MS 分配 IP 地址。用于地址分配的协议对于 GPRS 网络是特定的，并通常称为 PDP 语境激活。AAA 包含数据库，其中，分配的 IP 地址被关联到订户标识，例如，IMSI。

[0075] 应理解到：尽管示例访问分配给 MS 2 的 IP 地址，但是可由 GGSN 将多于一个的 IP 地址分配给同一 MS。在这种情况下，根据 GPRS 规范，GGSN 可存储关于关联到 MS 的活动连接 (PDP 语境）的信息，并且可检验由 MS 在数据分组传输中使用的 IP 地址是否是由 GGSN 向 MS 分配的 IP 地址之一。

[0076] 应注意到：GPRS-GSM 网络的 SGSN 5、GGSN 6 和 AAA 7 处于相同的域，该域表征为 GSM 安全性方案。

[0077] 根据本发明的优选实施例，逻辑实体（软件模块）10（以下称为安全令牌注入器 (STI)）在逻辑上链接到 GGSN 6。定位 STI 以控制从 GPRS/GSM 网络进入的通信量。具体说来，STI 截取从移动站产生并通过 GGSN 6 被定向到 IP 网络 12 的数据包。

[0078] 数据包（例如，互联网包）是核心数据块连同附加的必要地址和管理信息，以允许网络将数据传递到正确的目的地。数据包开始于由应用给出的核心数据。通过若干层的头部来封装核心数据，其中，可根据 OSI 模型来描述所述层。在该（非限定）描述内，当数据包经过称为封装的机制时，每层对所述数据包进行修改。核心数据包含应用层消息，该消息通过符合应用层协议的语法来表示。应用层协议的示例为 FTP（文件传输协议）、HTTP（超文本传输协议）、SOAP（简单对象访问协议）或 SIP。

[0079] 请求访问服务器或访问服务功能或操作的应用层消息在所述情况下被称为访问请求消息。在所述情况下，访问请求消息并非必然描述在会话启动时对加入服务的请求，而且描述对访问功能或由服务提供的操作的请求。在 SIP 中访问请求消息的示例是“INVITE”消息：当用户代理客户机期望发起会话（例如，音频、视频或游戏）时，它指定“INVITE”请求。“INVITE”请求请服务器建立会话（例如，语音呼叫）。在另一示例中，当请求 Web 页时，利用检索期望的数据所必需的信息（例如，URL）来创建“get”消息。作为示例，携带“get”消息的应用层协议是 HTTP。在这种情况下，“get”消息包括 HTTP GET 头部，其作为在应用层对于服务（在这种情况下，指的是通过互联网检索 Web 页的服务）的访问请求消息的示例。

[0080] 可通过在传输控制协议 (TCP) 和互联网协议 (IP) 这两个广泛使用的协议之后的互联网协议栈（也称为 TCP/IP 栈）来描述根据其运行互联网的协议堆栈。TCP/IP 栈的协议集合覆盖 OSI 7 层模型中的 5 层。使用所述 TCP/IP 栈，通常将消息嵌入应用头部（通常，该应用头部实际上包括若干头部）和应用层主体（或净荷）两者中。头部具有根据应用层协议的标准格式，而净荷包含直达应用的信息并且数据不需要符合标准头部或格式。HTTP 中头部的示例为诸如 GET 消息的消息类型和请求的 Web 页的 URL。下一层是传输层，其添加通常在 TCP 或用户数据报协议 (UDP) 中定义的头部的层。在网络层（在也称为 IP 层的互联网）中，该头部 (IP 头部）包含从源到目的地获得数据包所需的信息，其包括源地址和目的地地址，所述地址即为机器号码。

[0081] STI 10 至少操作在网络层，并且捕获离开 GGSN 6 的数据包。如果 STI 仅操作在网络层或仅到达传输层，则由于 STI 无法识别在数据包中携带的应用消息，例如，其无法识别是否是访问请求消息或者在哪个应用层协议携带所述消息，所以 STI 需要捕获离开 GGSN（并定向到 IP 地址）的所有数据包。在 STI 还操作在应用层的情况下，其可识别访问请求消息并区分不同的应用层协议。例如，如果还操作在应用层，则可将 STI 编程为仅截取 SIP 访问请求消息，并且使按照其它协议编制的消息通过。

[0082] 可用于实现 STI 模块的技术之一是应用层防火墙的技术。商用的察觉应用的防火墙的示例为 Cisco PIX、Check Point Firewall-1 ® 和 Xtradyne 的 WS-DBC。

[0083] STI 在携带访问请求消息的数据包中必须截取的最少信息是关于订户地址的在网络层的信息，例如，在互联网中，指的是分配到订户（即，到 MS）的 IP 地址。通常，如以下进一步详细描述的，STI 将需要关于目的地地址的信息，以在验证处理的末尾发送携带所述消息的数据包。优选地，由 STI 在截取数据包时提取所述信息。然而，这是非限制性的特点，因为可将 STI 配置为将消息发送到验证系统已定义的目的地地址。应注意到：目的地地址不必是消息被定向的应用服务器的地址。例如，根据 SIP 协议，可将消息定向到 SIP 代理，该 SIP 代理随后将消息寻址到在消息头部中包括的应用层地址中指定的应用服务器。

[0084] 包含在由 STI 10 捕获的数据包中的信息的至少一部分被传递到软件部件 9，该软件部件 9 称为标识局 (IA)，操作在应用层上。IA 负责管理访问外部 PDN（即，IP 网络 12）的订户的标识。IA 至少从 STI 接收订户 IP 地址和关于访问请求消息的应用层协议的信息。可通过从 STI 接收数据包（如果 STI 最高仅操作在网络 / 传输层，则所述数据包为“闭合封装”）来获得所述关于访问请求消息的应用层协议的信息，或者如果 STI 还操作在应用层上，则可通过接收诸如协议类型（例如，SOAP、HTTP、SIP）的特定信息来获得所述信息。从应用层操作的 STI 接收的其它信息可包括：消息类型（例如，INVITE 或 REGISTER）以及需要的服务的通用资源标识符 (URI)，例如，Web 页的 URL。

[0085] IA 9 可通过从 STI 10 得知请求服务的移动站 MS 2（订户）的 IP 地址以及通过询问 AAA 7 而得知订户的标识来识别所述移动站 MS 2，其中，所述 AAA 7 包含分配的 IP 地址与订户标识之间的映射。作为订户标识，优选地，由 IA 提取 IMSI。

[0086] 优选地，IA 存储关于订户标识和他 / 她请求的服务的信息。关于请求的服务的信息可以是服务提供者的 IP 地址和 / 或 URI，以及 / 或者在服务提供者使用不同的协议提供更多服务的情况下（例如，对电子邮件帐户使用 POP3，对 Web 导航使用 HTTP），所述信息是服务所使用的协议。在图 2 中，描述存储在 IA 中的信息表的示例。所示的表为想要访问一个或多个服务的订户 A、B 和 C 提供映射，所述服务表征为服务提供者 SP-1、SP-2 等。在图 2 的示例中，订户通过他们的 IMSI 来识别。优选地，由 IA 为每个订户创建伪 PS，例如，创建与订户的 IMSI 相应的 PS。或者，如图 2 所示，可为订户产生更多的假名 (pseudonym)，其中，每个假名表征由订户请求的特定服务。作为优选，创建假名，以便避免公开诸如 IMSI 的敏感数据，这将在以下的描述中更加清楚。

[0087] 在检验订户的标识之后（例如，通过将 IP 地址和与订户相关的 IMSI 映射），IA 根据访问请求消息的应用层协议来产生软件令牌。例如，在用于 Web 服务的 SOAP 消息的情况下，可根据 WS 安全规范来定义所述令牌。将所述令牌插入访问请求消息，例如，作为插入消息的现有应用头部的字段或作为在消息中添加的新的应用头部。

[0088] 根据 STI 操作在哪一层，可由 IA 将令牌插入消息中，或者 IA 可命令 STI 将令牌插入消息中。后一种选择假设 STI 也操作在应用层上。在任何一种情况下，STI 将修改的访问请求消息（即，包含令牌）发送到应用服务器 11，应用服务器 11 接收验证的消息。

[0089] 可通过（在应用服务器 11 上运行的）应用服务来确认消息的验证，例如，可通过检验令牌并随后将其发送到服务的应用逻辑的特定应用服务器软件来确认消息的验证。控制验证的框架的示例为 SunJava 系统访问管理器，其为基于开发 Java 2 平台的体系结构。

[0090] 验证令牌包括关联到在移动网络中定义的订户标识的订户标识符，所述移动网络典型地位于移动运营商的域中，并且所述标识符诸如 IMSI 或 MSISDN。

[0091] 优选地，包括在令牌中的订户标识符是关联到基于 SIM 的标识（例如，IMSI 或 MSISDN）的假名。尽管本发明不排除在验证令牌中使用在移动网络中定义的订户标识，但是假名的使用保护了订户的隐私，并防止公开诸如 IMSI 的敏感信息，从而避免安全威胁（例如，在移动运营商的计费处理中进行舞弊）。或者，标识符可以是由移动运营商根据（例如）订户的信用分配给订户的授权串 / 代码。尽管优选的是标识符唯一明确地相应于订户标识，但是可为一组订户（例如，按照年龄的分组）分配相同的授权串 / 代码。

[0092] 可选地，IA 在将产生的令牌发送到 STI 之前，将所述令牌传递到公共密钥基础结构 (PKI) 服务 8，作为示例，所述 PKI 服务 8 通过经由非对称加密将数字签名添加到令牌来证明所述令牌，而非对称加密本身是公知的。PKI 8 可以是如 Entrust PKI 或 VeriSign ® 的商用框架或如 OpenSSL 的免费软件 / 开放源工具。

[0093] 本发明的验证系统具有的优点在于其对订户透明，所述订户在请求服务之后，仅看见验证的结果 :访问服务或拒绝访问。

[0094] 包含 STI 和 IA 的验证软件平台可以在移动网络运营商的直接控制下。

[0095] 尽管 STI 10 和 IA 9 被示为 GGSN 6 外部的分离部件，但是可在 GGSN 之内实现 STI 10 和 IA 9，例如，将其实现为嵌入 GGSN 的 GPRS 标准控制逻辑中的软件模块。由于这样将消除 GGSN 与 STI 之间的物理连接，所以可提高 STI 针对网络层攻击的安全性。

[0096] 模块 STI 和 IA 可以是用诸如 Java、C、C++ 和 CORBA 的标准语言实现的软件部件，并且可安装在本身公知的硬件部件上。

[0097] 图 3 示出根据本发明优选实施例对在应用服务器中主管的 Web 服务的访问操作的处理示图。在图 3 所示的处理流程中相互作用的主要部件具有与参照图 1 描述的部件相同的一般逻辑功能，并且用相同的标号指示。

[0098] 在图 3 所示的实施例中，MS 2 可以是包括启用数据的客户机的蜂窝电话，用于在分组交换蜂窝式网络（诸如 GPRS、EDGE 或 UMTS）内的连接和数据传送。例如，可将蜂窝电话（通过有线或无线链路）链接到采用电话来连接到分组交换网络的个人计算机。在蜂窝式网络外部的域中主管应用服务器 11，所述域通过公共 IP 网络连接到服务器。

[0099] 在图 3 中，作为示例，MS 通过使用 SOAP 协议请求访问在公共 IP 网络中提供的服务“abc”，所述 SOAP 协议是基于 XML 的语言，其用于向 Web 服务传递数据并从 Web 服务传递数据。可将 SOAP 消息包含在 HTTP 消息中（在应用层）。作为示例，SOAP 请求可以是头部中的 HTTP POST 或 HTTP GET 请求，而 SOAP 消息包含在主体中，例如，在图 3 中，给出的 HTTP POST 请求 id 的示例，即，“POST/abc HTTP/1.1”。步骤 31 通过简化的方式表示 MS 2 与 GGSN6 之间的相互作用，其对于 MS 访问外部网络是必需的。在步骤 31 期间，由 AAA 7 至少在数据会

话的持续期间识别和授权 MS，所述 AAA7 将 IP 地址分配给 MS 并在存储器中存储 IP 地址与订户标识之间的映射信息。在该实施例中，订户标识包括 IMSI。在步骤 31 的蜂窝式网络内的授权和验证阶段之后，由 GGSN 将在数据包中携带的访问请求消息转发到外部网络（步骤 32）。步骤 32 的虚线表示在没有根据本发明的验证机制的情况下，消息经过的逻辑路径，即，消息被发送到应用服务器 11，所述应用服务器 11 随后将通过用于验证的询问 / 响应机制来询问用户。

[0100] 根据本发明，在步骤 32，由位于 GGSN 6 与公共网络之间的 STI10 来截取包含访问请求消息的数据包。STI 从截取的数据包提取订户的 IP 地址（即，用于会话而分配给 MS 的地址），优选地，还提取 IP 目的地地址（即，应用服务器 11 的地址）。STI 随后将应用消息（在这种情况下为 SOAP 消息）和订户的 IP 地址转发给 IA 9（步骤 33）。

[0101] 如果 STI 操作在低于应用层的层上，则作为示例，通过向 IA 转发应用头部，将消息自动转发到 IA。反之，如果 STI 操作在应用层上，则 STI 识别在应用层消息中使用的协议，在这种情况下，所述协议为 HTTP 协议上的 SOAP。在所述的任何一种情况下，IA 得知订户的 IP 地址以及消息所符合的应用层协议。作为示例，可通过以公共对象请求代理机体系结构 (CORBA)（诸如接口定义语言 (IDL)）指定的接口或以 Web 服务语言（诸如 Web 服务描述语言 (WSDL)）指定的接口来产生 STI 与 IA 之间的信息传输。

[0102] 在步骤 34，IA 9 询问 AAA 7 以确定 GSM 网络中订户（通过 MS2 连接到蜂窝式网络）的标识，所述标识相应于在数据包中捕获的源 IP 地址。在步骤 35，AAA 7 通过向 IA 提供关联到 IP 地址的订户标识（在这种情况下，由 IMSI 表示）来响应于所述询问。

[0103] 在下一步骤（步骤 35），IA 产生包括订户标识符的令牌。作为示例，可根据 WS 安全规范来定义令牌，例如，字符串（在图 3 中指示为 <WS> 令牌）。优选地，包括在令牌中的标识符是由 IA 创建并关联到 IMSI 的假名。如在图 2 中示出的示例，诸如在为相同订户创建更多假名（即，相同的 IMSI）以访问会话内的不同服务的情况下，在单一签入 (SSO) 访问机制的情况下，可将所述标识符关联到服务提供者。至少在会话的持续期间，IA 追踪假名与在蜂窝式网络中定义的订户标识（即，IMSI）之间的映射。

[0104] 以下示例为以 XML 格式标识并符合 OASIS（结构化信息标准促进组织）开放标准的（简化）SAML 令牌：

[0105] <saml:Assertion MajorVersion="1" MinorVersion="0"

[0106] AssertionID="128.9.167.32.12345678"

[0107] Issuer="Operator.com"

[0108] <IssueInstant="2004-12-03T10:02:00Z"> <saml:Conditions

[0109] NotBefore="2004-12-03T10:00:00Z"

[0110] NotAfter="2004-12-03T10:05:00Z"/>

[0111] <saml:AuthenticationStatement

[0112] AuthenticationMethod="<GSM>"

[0113] AuthenticationInstant="2001-12-03T10:02:00Z">

[0114] <saml:Subject>

[0115] <saml:NameIdentifier

[0116] SecurityDomain="operator.com"Name="PSEUDONYM"/>

[0117] </saml:Subject>

[0118] </saml:AuthenticationStatement>

[0119] </saml:Assertion>

[0120] 上述示例的 SAML 令牌声明名称为“PSEUDONYM”的用户的标识（即，由 IA 给出的标识符），其被关联到在 GSM 网络中定义的标识。优选地，SAML 令牌包含关于用于授权访问服务的验证方法的信息，在这种情况下，其由 GSM 安全方案（用 <GSM> 来指示）来定义。其它可选信息是验证的发布者（用 operator.com 来指示）以及令牌有效性的条件（用命令 NotBefore 和 NotAfter 来指示）。

[0121] 可选地，将令牌转发到 PKI 8 服务，以向令牌附加数字签名或根据已知加密机制来对其进行加密（步骤 36）。在步骤 37，PKI 返回用数字签名证明和 / 或通过加密确保安全的令牌。在图 3 中，用 DS 来指示证明 / 加密的令牌（<WS> 令牌）。

[0122] 紧接着步骤 35（或者在包括 PKI 服务的情况下，紧接着步骤 37），IA 创建新的访问请求消息，用“New-soap”来指示，其包括产生的令牌。优选地，新消息是从 MS 发送的访问请求消息，其中，如 OASIS WS 安全规范所述，将令牌添加在 SOAP 封装中，作为附加字段。在步骤 38，将新的访问请求消息（包括令牌）传递到 STI 以进行传输。STI 先前在它的存储器中复制并存储提取出信息的数据包，随后将接收的访问请求消息发送到应用服务器 11（步骤 39）。

[0123] 如果数字签名被附加到令牌，则应用服务器通过询问 PKI 服务来检验数字签名（步骤 40）。例如，PKI 检验令牌的数字签名证书是否有效。

[0124] 最终，通过令牌接收到对订户标识的验证的应用服务器 11 向验证的订户提供所请求的服务（步骤 41）。

[0125] 应注意到：在图 3 中描述的验证机制对于用户是透明的，所述用户不需要输入用于访问服务的证明。此外，验证机制允许通过 SSO 机制对多个服务进行透明访问，所述 SSO 机制通常预先假设在提供服务的服务提供者（标识联盟）中间存在协议。

[0126] 图 4 示出根据本发明另一实施例的连接到外部 IP 网络的分组交换网络的框图。MS 2 以无线电方式链接到分组交换移动网络 13，例如，UMTS 网络。尽管没有详细示出，但是移动网络 13 包括 AAA 服务器和 GGSN。在该实施例中，IP 网络是下一代网络 (NGN)15，其作为基于分组的网络，允许基于分组的互联网与电话网络之间的趋同，并支持各种类型的用户通信量（包括语音、数据和视频）。NGN 技术的应用是语音转 IP(VoIP)。在该示例中，NGN 网络中的呼叫 / 会话功能基于会话启动协议 (SIP)。根据图 4 所示的实施例，移动电话 MS 2 通过 NGN 15 将 SIP 消息寻址到 SIP 服务器 14。由验证平台 17 截取离开移动网络 13 的 GGSN 的 SIP 消息。验证平台 17 包括 STI 10、IA 9，并且可选地包括 PKI 8，它们与参照图 1 描述的 STI 10、IA 9 和 PKI 8 具有相同的一般逻辑功能。在验证之后，SIP 服务器 14 总是通过 NGN 15 将 SIP 消息转发到 SIP 电话 16，SIP 电话 16 为包括客户机应用（即，用户代理客户机和用户代理服务器）的 IP 节点，所述客户机应用用于向其它电话发起呼叫和从其它电话接收呼叫，其中，所述 SIP 电话 16 为基于 IP 的电话或陆上线路 / 蜂窝电话，并且作为示例，可安装在个人计算机上。SIP 消息的示例是从移动电话 2 发起以与 SIP 电话 16 建立多媒体呼叫（例如，视频会议）的请求。

[0127] 在图 5 示意性示出通过 NGN 到在 SIP 服务器中主管的 SIP 服务的访问操作的处理

示图。MS 2 通过使用 SIP 协议来请求访问在 NGN 中提供的服务。作为示例，所述服务是视频会议会话的设立，该服务可通过 INVITE 命令来请求。作为示例，SIP 消息可以是“INVITE sip :name@acme.comSIP/2.0”，其中，name@acme.com 是 Request_URI，其为指定 SIP 消息的目的地的 SIP URI（例如，URL）。Request_URI 可以是用户或在 SIP 电话中定义的用户代理服务器。在该示例中，Request_URI 是由 SIP 电话 16 定义的用户。可通过 TCP 或 UDP 在网络层传输 SIP 消息。

[0128] 步骤 50 以简化的方式表示 MS 2 与 GGSN 6 之间的相互作用，其对于 MS 访问外部网络是必需的。在步骤 50 期间，至少在数据会话的持续期间，由 AAA 7 识别和授权 MS，所述 AAA 7 将 IP 地址分配给 MS，并在存储器中存储 IP 地址与订户标识（例如，IMSI）之间的映射信息。在步骤 50 的移动网络内的授权和验证阶段之后，由 GGSN 将在数据包中携带的访问请求消息转发到外部网络（步骤 51）。步骤 51 的虚线表示在没有根据本发明的验证机制的情况下，消息经过的逻辑路径，即，消息被发送到 SIP 服务器 15。

[0129] 根据本发明，在步骤 52，由位于 GGSN 与 NGN 之间的 STI 10 来截取 SIP 消息。STI 从截取的数据包提取源 IP 地址（即，分配给 MS 的地址）和目的地 IP 地址，即，可处理请求并将 INVITE 消息转发到正确的被呼叫者（由 SIP URI 来指示）的 SIP 服务器的地址。STI 随后将 SIP 消息和订户 IP 地址转发到 IA 9（步骤 52）。

[0130] 在步骤 53，IA 9 询问 AAA 7 以确定订户标识，所述标识相应于在包含 SIP 消息的数据包中捕获的源 IP 地址。在步骤 54，AAA 7 通过向 IA 提供被关联到 IP 地址的订户标识（在这种情况下，由 IMSI 表示）来响应于所述询问。

[0131] 在下一步骤（步骤 54），IA 产生包括订户标识符的令牌。作为示例，可根据 SAML 规范来定义令牌（在图 5 中指示为 [SAML] 令牌）。优选地，所述标识符是由 IA 创建并关联到 IMSI 的假名。

[0132] 可选地，将令牌转发到 PKI 8 服务，以向令牌附加数字签名和 / 或根据已知加密机制来对其进行加密（步骤 55）。在步骤 56，PKI 返回用数字签名证明和 / 或通过加密确保安全的令牌。在图 5 中，用 DS 来指示证明 / 加密的令牌（[SAML] 令牌）。

[0133] 紧接着步骤 54（或者在包括 PKI 服务的情况下，紧接着步骤 56），IA 创建新的访问请求消息，用“New SIP header”来指示，其包括产生的令牌。优选地，新消息是从 MS 发送的访问请求消息，其中，如在图 5 中由 SIP 头部 61 所示，将令牌添加在 SIP 头部中，作为 SIP 协议中描述的附加字段。在 DS（[SAML] 令牌）之间的字段“SAML-Payload”是由 IETF 定义的关键字，它用于识别 SAML 令牌头部。

[0134] 将新的访问请求消息（包括令牌）传递到 STI 以进行传输（步骤 57）。STI 随后将接收的 SIP 消息 61 指向 SIP 服务器 14（步骤 58）。

[0135] 如果数字签名被附加到令牌，则应用服务器通过询问 PKI 服务来检验数字签名（步骤 59）。

[0136] 最终，通过令牌接收到对订户标识的验证的应用服务器 14 通过将“200 OK”消息发送到 MS 来发送对 INVITE 消息的肯定响应（步骤 60），该肯定响应为对 INVITE 的标准 SIP 肯定响应。随后可在端点之间建立使用 RTP 的视听流。

[0137] 参照回图 4，尽管将验证平台 17 示为处于移动网络的外部，但是可在移动网络 13 中（即，在移动运营商的安全域中）实现验证平台 17。

[0138] 图 6 示出根据本发明优选实施例的示例，对在应用服务器中主管的 Web 站点的访问操作的处理示图。对 Web 站点的访问来自于电路交换移动网络（诸如 GSM）或来自 GPRS，它们通过使用无线应用协议 (WAP) 连接到 IP 网络。根据本发明，MS 2（例如，GSM 电话）包含截取 WAP 数据的微浏览器。使用诸如 UDP 的网络协议来发送所述 WAP 数据。应用服务器可以是专门的 WAP 服务器或传统 Web 服务器。由 GGSN 6 来执行蜂窝是网络到外部网络的网关的逻辑功能。

[0139] 作为示例，图 6 所示的实施例可应用于由自由联盟计划定义的标识联盟框架 (ID-EF)。ID-EF 基于 SAML 标准并提供基于标准 SOAP 的验证以及到标识提供者的单一签入服务接口。

[0140] 在图 6 中，作为示例，MS 通过使用 HTTP 协议请求访问在公共 IP 网络中提供的服务“abc”在图 6 中，给出 HTTP GET 请求的示例，即，“GET/abc HTTP/1.1”。步骤 71 通过简化的方式表示 MS 2 与 GGSN6 之间的相互作用，其对于 MS 访问外部网络是必需的。在步骤 71 期间，由 AAA 7 至少在数据会话的持续期间识别和授权 MS，所述 AAA7 将 IP 地址分配给 MS 并在存储器中存储 IP 地址与订户标识之间的映射信息。在该实施例中，订户标识包括 IMSI。在步骤 71 的蜂窝式网络内的授权和验证阶段之后，由 GGSN 将在数据包中携带的访问请求消息转发到外部网络（步骤 72）。步骤 72 的虚线表示在没有根据本发明的验证机制的情况下，消息经过的逻辑路径，即，消息被发送到 Web/WAP 服务器。

[0141] 根据本发明，在步骤 72，由位于 GGSN 与公共网络之间的 STI 10 来截取包含访问请求消息的数据包。STI 从截取的数据包提取订户的 IP 地址（即，用于会话而分配给 MS 的地址）以及 IP 目的地地址（即，应用服务器 11 的地址）。STI 随后将应用消息（在这种情况下为 HTTPGET 消息）和订户的 IP 地址转发给 IA 9（步骤 73）。

[0142] 在步骤 74，IA 9 询问 AAA 7 以确定订户（通过 MS 2 连接到蜂窝式网络）的标识，所述标识相应于在数据包中捕获的源 IP 地址。在步骤 75，AAA 7 通过向 IA 提供关联到 IP 地址的订户标识（在这种情况下，由 IMSI 表示）来响应于所述询问。

[0143] 在下一步骤（步骤 76），IA 产生包括订户标识符的令牌。优选地，所述包括在令牌中的标识符是由 IA 创建并关联到 IMSI 的假名。作为示例，可根据 SAML 规范来定义所述令牌（在图 6 中指示为 [SAML] 令牌）。优选地，所述标识符是由 IA 创建并关联到 IMSI 的假名。

[0144] 可选地，将令牌转发到 PKI 8 服务，以向令牌附加数字签名和 / 或根据已知加密机制来对其进行加密（步骤 76）。在步骤 77，PKI 返回用数字签名证明和 / 或通过加密确保安全的令牌。在图 6 中，用 DS 来指示证明 / 加密的令牌（[SAML] 令牌）。

[0145] 紧接着步骤 75（或者在包括 PKI 服务的情况下，紧接着步骤 77），IA 根据由自由联盟定义的标准创建充当到 SAML 声明的指针的“伪象”。所述伪象在图 6 中用“Artifact(SAML)”来指示。随后在步骤 78 将伪象提供给 STI。在步骤 79，STI 将包含“Artifact(SAML)”的 HTTP GET 消息发送到 Web/WAP 服务器。在步骤 80 期间，已接收到包含伪象的访问请求消息的服务器请求 IA 提供与伪象相应的 SAML 令牌。在接收到包括作出请求的移动订户的标识符的 SAML 令牌之后，识别（并授权）所述订户，服务器（即，服务提供者）随后将肯定响应“welcome”发送到 MS（步骤 81）。

[0146] 图 7 示出本发明的另一优选实施例，其中，请求服务的订户的第一网络是 ADSL 接

入网络，而第二网络是 IP 网络。图 7 的实施例可代表以下的示例性情况，其中，ADSL 网络的订户想要从她 / 他的个人计算机 (PC)2 通过 IP 网络访问在应用服务器 24 中主管的 Web 站点的服务。在该示例中，通过标准串行 USB（通用串行总线）接口将 PC18 连接到 ADSL 调制解调器 19。PC 18 和 ADSL 调制解调器 19 通常被称为用户宅室设备 (CPE)68。然而，可考虑替换 CPE，诸如连接到一个或多个 PC、IP 电话或连接到 TV 机顶盒的住宅网关。因此，通常采用 CPE 来发起，路由或终止电信，并且作为示例，通过从 PC 键盘输入登录 ID 和密码或通过从住宅网关进行自动验证（例如，通过包括在智能卡或嵌入住宅网关的固件中的代码串）来提供对访问 PDN 的验证请求。重点在于所述验证在接入网络内进行以授权访问 PDN（例如，互联网）。

[0147] 经由 CPE 68 将订户与 DSL 接入复用器 (DSLAM)30 连接。DSLAM 30 包括复用器 / 解复用器，并且用户线路（即，有线链路 67）连接到位于中央局（运营商室内）66 的 DSLAM 内的分配的 ADSL 终端单元。DSLAM 30 上行链接到宽带网络访问服务器 (BNAS)29，器提供包括路由或服务选择的应用层会话管理。CPE 驻留在端点用户位置（例如，家庭或办公室），其在图 7 中用标号 20 示意性示出。CPE 与 DSLAM 之间的连接为有线链路 67，其通常为标准铜制电话线。传统模拟电话（即，简易老式电话系统 (POTS)23）可选择性地经由相同的有线链路 67 与 PSTN 25 连接。因此，有线链路 67 可携带 POTS 信号与 DSL 信号两者。BNAS 29 连同 DSLAM 30 用作到外部分组数据网络的网关，在所述情况下，外部分组数据网络是 IP 网络 22。注意到以下情况很重要 :CPE 与 DSLAM 之间的通信使用用户室内与中央局之间的专门有线链路，由此确保在 DSL 基础结构内通信的高级安全性。

[0148] BNAS 处理对请求访问 IP 网络的订户的验证，以便授权所述订户进行访问。由认证、授权和计费 (AAA) 服务器 26 来实施登录验证。AAA 服务器 26 执行类似与在图 1 的实施例中描述的 AAA 服务器的逻辑操作。具体说来，AAA 服务器包含数据库，其中，将分配的 IP 地址关联到 xDSL 网络内的订户标识。根据已知方法，对访问 PDN 的验证（可称为登录验证）可基于以密码为基础的机制、智能卡或加密令牌。优选的登录验证机制使用登录 ID，其通常是关联到密码的用户名，当请求连接到外部数据网络时由订户输入。还可将订户 ID 包括在智能卡中。登录 ID 的使用允许在可采用相同订户站的不同用户之间进行区分，作为示例，所述用户为通过相同 PC 连接的用户。或者，可通过 PSTN 的呼叫线路标识 (CLI) 在 ADSL 基础结构内识别所述订户。

[0149] 根据本发明，安全令牌注入器 (STI)65 在逻辑上链接到 BNAS 29。定位 STI 以控制从 ADSL 网络进入的通信量。具体说来，STI 65 截取从 CPE 68 产生并通过 BNAS 29 被定向到 IP 网络 22 的数据包。

[0150] STI 65 至少操作在网络层，并且捕获离开 BNAS 29 的数据包。如果 STI 仅操作在网络层或仅到达传输层，则由于 STI 无法识别在数据包中携带的应用消息，例如，其无法识别是否是访问请求消息以及在哪个应用层协议携带所述消息，所以 STI 需要捕获离开 BNAS（并定向到 IP 网络）的所有数据包。在 STI 还操作在应用层的情况下，其可识别访问请求消息并区分不同的应用层协议。例如，如果还操作在应用层，则可将 STI 编程为仅截取 HTTP 访问请求消息，并且使按照其它协议编制的消息通过。

[0151] STI 65 的一般逻辑功能类似于参照图 1 描述的 STI 10 的一般逻辑功能。具体说来，STI 在携带访问请求消息的数据包中必须截取的最少信息是关于订户地址的在网络层

的信息，例如，在互联网中，指的是分配到订户的 IP 地址。

[0152] 包含在由 STI 65 捕获的数据包中的信息的至少一部分被传递到软件部件标识局 (IA)64，其操作在应用层上。IA 负责管理访问外部 PDN（即，IP 网络 22）的订户的标识。IA 至少从 STI 接收订户 IP 地址和关于访问请求消息的应用层协议的信息。可通过从 STI 接收数据包（如果 STI 最高仅操作在网络 / 传输层，则所述数据包为“闭合封装”）来获得所述关于访问请求消息的应用层协议的信息，或者如果 STI 还操作在应用层上，则可通过接收诸如协议类型的特定信息来获得所述信息。

[0153] IA 64 的逻辑功能基本上与参照图 1 描述的那些逻辑功能相同。具体说来，IA 通过从 STI 65 得知请求服务的订户的 IP 地址以及通过询问 AAA 26 而得知订户的标识来识别所述订户（即，作为示例，经由智能卡登录或通过 CLI 来识别订户站），其中，所述 AAA 26 包含分配的 IP 地址与订户标识之间的映射。

[0154] 优选地，IA 存储关于订户标识和他 / 她请求的服务的信息。关于请求的服务的信息可以是服务提供者的 IP 地址和 / 或 URI，以及 / 或者在服务提供者使用不同的协议提供更多服务的情况下（例如，对电子邮件帐户使用 POP3，对 Web 导航使用 HTTP），所述信息是服务所使用的协议。在图 8 中，描述存储在 IA 64 中的信息表的示例。所示的表为想要访问一个或多个服务的订户 A、B 和 C 提供映射，所述服务表征为服务提供者 SP-1、SP-2 等。在图 8 的示例中，订户通过他们的登录 ID（例如，用户名和密码 (LOGIN-A、LOGIN-B 等)）来识别。优选地，由 IA 为每个订户创建伪 PS，例如，创建与订户的登录 ID 相应的 PS。或者，如图 8 所示，可为订户产生更多的假名，其中，每个假名表征由订户请求的特定服务。作为优选，创建假名，以便避免公开诸如 CLI 或登录 ID 的敏感数据。

[0155] 在检验订户的标识之后（例如，通过将 IP 地址和与订户相关的登录 ID 映射），IA 根据访问请求消息的应用层协议来产生软件令牌。例如，将所述令牌插入访问请求消息，作为插入消息的现有应用头部的字段或作为在消息中添加的新的应用头部。

[0156] 根据 STI 操作在哪一层，可由 IA 将令牌插入消息中，或者 IA 可命令 STI 将令牌插入消息中。后一种选择假设 STI 也操作在应用层上。在任何一种情况下，STI 将修改的访问请求消息（即，包含令牌）发送到应用服务器 24，应用服务器 24 接收验证的消息。

[0157] 验证令牌包括关联到在固定接入网络中定义的订户标识的订户标识符。

[0158] 优选地，包括在令牌中的订户标识符是关联订户标识（例如，CLI 或登录 ID）的假名。尽管本发明不排除在验证令牌中使用在 PSTN 或固定接入网络中定义的订户标识，但是假名的使用保护了订户的隐私，并防止公开敏感信息。或者，标识符可以是由 PSTN 运营商根据（例如）订户的信用分配给订户的授权串 / 代码。尽管优选的是标识符唯一明确地相应于订户标识，但是可为一组订户（例如，按照年龄的分组）分配相同的授权串 / 代码。

[0159] 可选地，IA 64 在将产生的令牌发送到 STI 之前，将所述令牌传递到公共密钥基础结构 (PKI) 服务 63，所述 PKI 服务 63 通过经由非对称加密将数字签名添加到令牌来证明所述令牌，而非对称加密本身是公知的。

[0160] 尽管 STI 65 和 IA 64 被示为 BNAS 29 外部的分离部件，但是可在 BNAS 之内优选地实现 STI 65 和 IA 64，例如，将其实现为嵌入 BNAS 的控制逻辑中的软件模块。由于这样将消除 BNAS 与 STI 之间的物理连接，所以可提高 STI 针对网络层攻击的安全性。

[0161] 尽管在数字订户线路 (DSL) 技术（特别是 ADSL 技术）的情况下参照图 7 和图 9 描

述了本发明的实施例，但是应理解：本发明并不受限于 xDSL 技术。事实上，还可在本发明的其它实施例中使用其它接入接入和 / 或网络配置，例如但不受限于：混合同轴光纤 (HFC)、无线连接 (例如，WiFi ® 或 WiMAX)、光纤到户 (FTTH) 和 / 或以太网。

[0162] 图 9 示出对在应用服务器中主管的 Web 站点的访问操作的处理示图。在处理流程中相互作用的主要部件具有与参照图 7 所描述的部件相同的一般逻辑功能，并使用相同的标号来指示。在所述实施例中，订户站通过使用 SOAP 协议请求访问在公共 IP 网络中提供的服务“abc”。作为示例，HTTP 请求可以是 HTTP POST，例如，“POST/abcHTTP/1.1”。订户站在该实施例中作为链接到 ADSL 调制解调器的端点用户外围装置 18(例如，PC)，在步骤 91 通过本身已知的方式在 ADSL 基础结构内进行验证。即，步骤 91 通过简化的方式表示 PC 18(经由 DSL 调制解调器) 与 BNAS 29 之间的相互作用，其对于订户站访问外部网络是必需的。在验证阶段内，AAA 7 至少在数据会话的持续期间将 IP 地址分配给订户站并在存储器中存储 IP 地址与订户标识之间的映射信息。随后从 ADSL 接入网络授权订户站来访问 IP 服务，并向订户分配 IP 地址。

[0163] 在步骤 91 的接入网络内的授权和验证阶段之后，在步骤 92，由 BNAS 将在数据包中携带的访问请求消息转发到外部网络。步骤 92 的虚线表示在没有根据本发明的验证机制的情况下，消息经过的逻辑路径，即，消息被发送到应用服务器 24。

[0164] 根据本发明，在步骤 92，由位于 BNAS 29 与公共网络之间的 STI65 来截取包含访问请求消息的数据包。STI 从截取的数据包提取订户的 IP 地址 (即，用于会话而分配给订户站的地址)，优选地，还提取 IP 目的地地址 (即，应用服务器 24 的地址)。STI 随后将应用消息 (在这种情况下为 SOAP 消息) 和订户的 IP 地址转发给 IA 64(步骤 93)。

[0165] 如果 STI 操作在低于应用层的层上，则作为示例，通过向 IA 转发应用头部，将消息自动转发到 IA。反之，如果 STI 操作在应用层上，则 STI 识别在应用层消息中使用的协议，在这种情况下，所述协议为 HTTP 协议上的 SOAP。在所述的任何一种情况下，IA 得知订户的 IP 地址以及消息所符合的应用层协议。作为示例，可通过以公共对象请求代理机体系结构 (CORBA)(诸如接口定义语言 (IDL)) 指定的接口或以 Web 服务语言 (诸如 Web 服务描述语言 (WSDL)) 指定的接口来产生 STI 与 IA 之间的信息传输。

[0166] 在步骤 94，IA 64 询问 AAA 26 以确定 PSTN 中订户的标识，所述标识相应于在数据包中捕获的源 IP 地址。在步骤 95，AAA 26 通过向 IA 提供关联到 IP 地址的订户标识 (在这种情况下，由登录 ID 表示) 来响应于所述询问。

[0167] 在下一步骤 (步骤 96)，IA 产生包括订户标识符的令牌。作为示例，可根据 WS 安全规范来定义令牌，例如，字符串 (在图 9 中指示为 <WS> 令牌)。优选地，包括在令牌中的标识符是由 IA 创建并关联到登录 ID 的假名。如在图 8 中示出的示例，诸如在为相同订户创建更多假名 (即，相同的登录 ID) 以访问会话内的不同服务的情况下，在单一签入 (SSO) 访问机制的情况下，可将所述标识符关联到服务提供者。至少在会话的持续期间，IA 追踪假名与在 PSTN 中定义的订户标识 (例如，登录 ID 或 CLI) 之间的映射。

[0168] 可选地，将令牌转发到 PKI 63 服务，以向令牌附加数字签名或根据已知加密机制来对其进行加密 (步骤 97)。在步骤 98，PKI 返回用数字签名证明和 / 或通过加密确保安全的令牌。在图 9 中，用 DS 来指示证明 / 加密的令牌 (<WS> 令牌)。

[0169] 紧接着步骤 95(或者在包括 PKI 服务的情况下，紧接着步骤 97)，IA 创建新的访问

请求消息，用“New-soap”来指示，其包括产生的令牌（步骤 98）。在步骤 98，将新的访问请求消息（包括令牌）传递到 STI 以进行传输。作为示例，新消息是从订户站发送的访问请求消息，其中，如 OASIS WS 安全规范所述，将令牌添加在 SOAP 封装中，作为附加字段。STI 先前在它的存储器中复制并存储提取出信息的数据包，随后将接收的访问请求消息发送到应用服务器 24（步骤 99）。

[0170] 如果数字签名被附加到令牌，则应用服务器通过询问 PKI 服务来检验数字签名（步骤 100）。例如，PKI 检验令牌的数字签名证书是否有效。

[0171] 最终，通过令牌接收到对订户标识的验证的应用服务器 14 向验证的订户提供所请求的服务（步骤 101）。

[0172] 应注意到：在图 9 中描述的验证机制对于用户是透明的，所述用户不需要输入用于访问服务的证明。此外，验证机制允许通过 SSO 机制对多个服务进行透明访问，所述 SSO 机制通常预先假设在提供服务的服务提供者（标识联盟）中间存在协议。

[0173] 近年来，以下情况变得越来越普遍：用户是多个电信网络的订户，由此想要或需要访问来自不同网络的应用服务。如参照图 2 到图 8 所述，可为相同的订户创建不同的随机数，所述订户进入可（但不受限于）由不同服务提供者传送的不同应用服务。申请人注意到：可通过假名在服务应用（即，对于服务提供者）识别用户，所述假名对于用户访问服务的不同网络而言是相同的。图 10 示意性示出用户是多于电信网络（即，ADSL 接入网络 121、无线 (WiFi ®接入网络 124、GPRS/GSM 网络 128 和 UMTS 网络 126)）的订户。用户可从网络 121、124、126 或 128 通过 IP 网络 120 发送对在应用服务器 129 的应用服务的请求。在第一网络内激活 AP 地址，在第一网络中，产生所述请求，并由总是位于第一网络内的 AAA 服务器（未示出）将其关联到标识符。根据本发明的优选实施例，将安全令牌注入器 (STI) 在逻辑上链接到每个第一网络的访问网关或接入点（例如，BNAS、GGSN），其充当到 IP 网络的网关，其中，订户向所述第一网络请求应用服务。STI 的 122、123、125 和 127 截取分别发源于网络 121、1 24、126 和 127 的访问请求消息。尽管没有在附图中示出，但是将每个 STI 在逻辑上链接到标识局 (IA)，所述 IA 负责管理订户标识，所述订户通过 IP 网络访问应用服务。将参照前面的实施例更加详细地描述 STI 和 IA 的功能和逻辑操作。具体说来，每个第一网络的 IA 从捕获的 IP 地址得知订户标识，并将假名关联到 IP 地址，该 IP 地址不仅识别订户（通过它在第一网络内与订户标识的关联），而且涉及请求的应用服务。为了能够将请求的服务与假名关联，IA（或者在 IA 操作在应用层情况下的 STI）需要从访问请求消息提取所请求的服务的 URI。通过得知 URI，可将订户标识符关联到涉及服务的假名，然后将其插入访问请求消息。可由运行所请求的服务的服务提供者创建涉及服务的假名，然后将其传送到 IA。有几种解决方案可执行所述传送。所述传送也可通过以下方式来执行：通过由 IA 提供并由服务提供者使用的某些供应工具的脱线方式，或者在运行时间通过诸如由用于支持标识联盟的自由联盟协会所指定的工具。

[0174] 应注意到：同样在该实施例中，由第一网络确保订户标识，其中，用户向所述第一网络请求服务。

[0175] 多网络访问的可行方案可以是以下用户的方案，所述用户为多个网络的订户，例如，所述网络为 GPRS、UMTS 和固定接入网络，其中，所述固定接入网络诸如通过 PSTN 的电话线路的 xDSL，这些网络由多平台运营商来管理。

[0176] 申请人已注意到：某些服务需要在客户机（即，订户站）与服务器之间的相互验证。换言之，当采用通过诸如互联网的外部网络的某些服务时，用户会需要或想要知道他或她是否真正与期望或正确的服务器进行通信。如果远程计算机能够模拟服务器的行为，则会哄骗或欺骗用户，使其认为他或她在与正确的服务器通信中。例如，传统上认为关于金融机构、它们的客户以及金融交易的信息对于安全性和可信度非常敏感。现在，作为示例，通常在互联网银行中使用非对称密钥对加密以确保安全性和秘密性。

[0177] 图 11 是示出根据本发明优选实施例，在相互验证的情况下，通过 PDN 对在应用服务器中主管的服务的访问的简化处理示图。在步骤 113，可作为移动站或 CPE 的订户站 110 请求在应用服务器 112 中主管的服务。在该示例中，所述消息是 POST 类型的 HTTP 访问请求消息。总是在步骤 113，根据本发明的方法（在前面的实施例中更加详细地描述），由 STI 111 截取所述消息，创建令牌（即，令牌 -c）并将其关联到所述消息。STI 随后将带有相关的令牌的消息发送到应用服务器（步骤 114）。在接收到消息（并可选地检验所述验证的有效期）之后，服务器 112 创建应答令牌（即，令牌 -c），其被输入对接收 POST 消息的肯定响应“Welcome”。作为示例，根据诸如 SAML 声明的标准，令牌 -s 可以是通过运行应用服务（例如，Java Servlet 或微软活动服务器页）的软件实现的字符串。或者，由逻辑上链接到服务器的逻辑实体（附图中未示出）优选地在服务提供者室内产生令牌 -s。应用实体可以定位在应用服务器前端的应用防火墙。

[0178] 由 STI 111 来截取包括令牌 -s 并由应用服务器 112 发送到订户站 110 的响应消息，所述 STI 111 从响应消息提取令牌 -s 并检验它的有效性。可通过数字签名或通过网络运营商（假设 STI 位于运营商室内）与服务提供者之间共享的例如对称密钥的私钥来检验所述有效性。如果令牌 -s 的有效性被肯定地验证，则 STI 将截取的肯定响应消息“Welcome”发送到订户站（步骤 116），或者 STI 创建将被发送到订户站 10 的新的肯定响应消息。否则，STI 截取通信，并将出错消息发送到订户站（附图中未示出）。

[0179] 在该实施例中，假设 STI 操作在应用层上，由此 STI 不仅可截取从应用服务器发送的响应消息，而且提取令牌 -s。应理解到：在 STI 最高操作到传输层的情况下，STI 111 截取响应消息，随后将其发送到 IA（在图 11 中未示出），所述 IA 提取应用层令牌 -s 并检验它的有效性。

[0180] 优选地，为了避免被未授权方截取或偷窃令牌 -s，可通过加密来保护所述令牌，或将所述令牌关联到生存期。

[0181] 还值得注意到：验证服务器的机制具有对端点用户透明的优点。

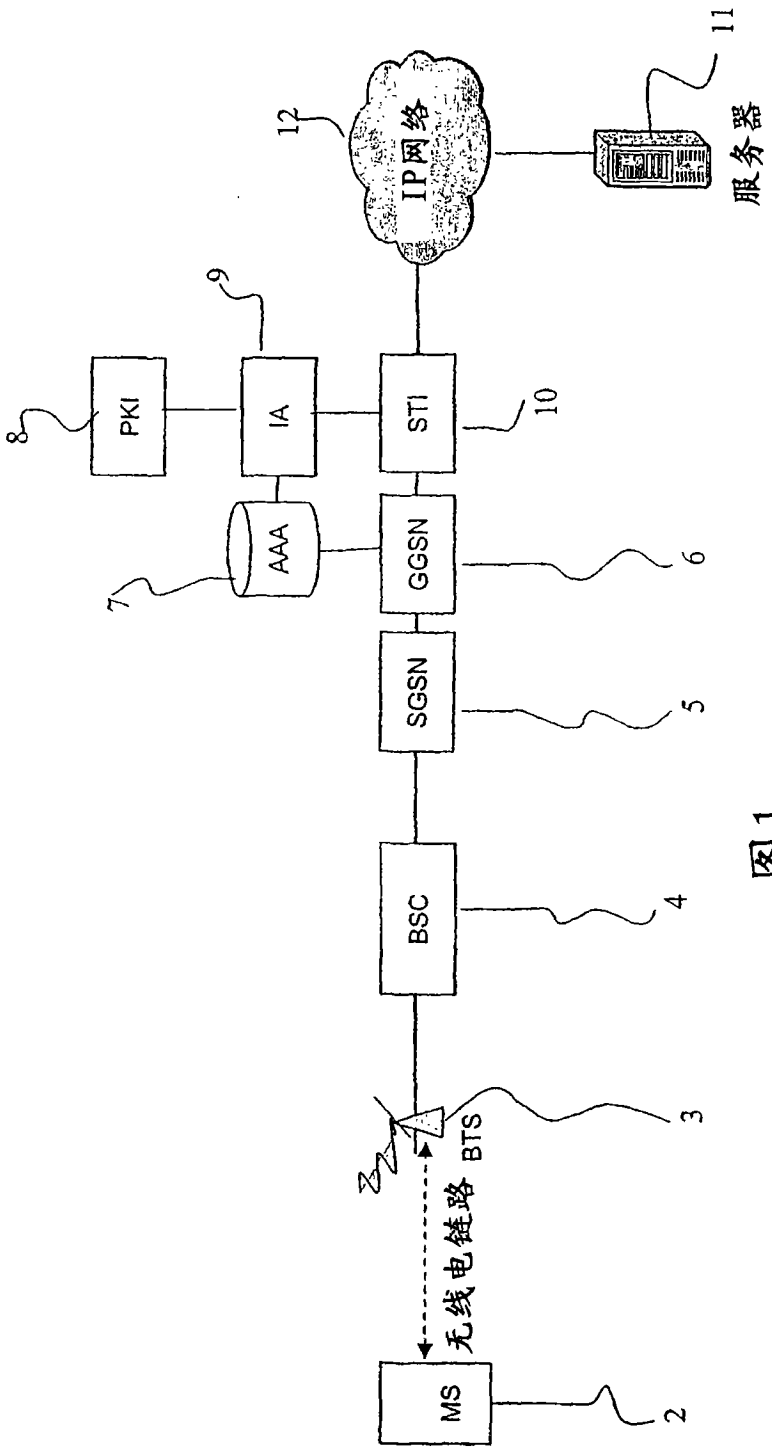

IP网络
12
11
服务器
9
PKI
IA
STI
10
8
AAA
GGSN
7
6
SGSN
5
BSC
4
3
BTS
无线电链路
MS
2

图1

表

标识	服务提供者	假名
IMSI-A	SP-1	PS-A1
IMSI-A	SP-2	PS-A2
IMSI-A	SP-3	PS-A3
IMSI-B	SP-1	PS-B1
IMSI-B	SP-4	PS-B4
IMSI-C	SP-5	PS-C5
..	..	..
..	..	..

图 2

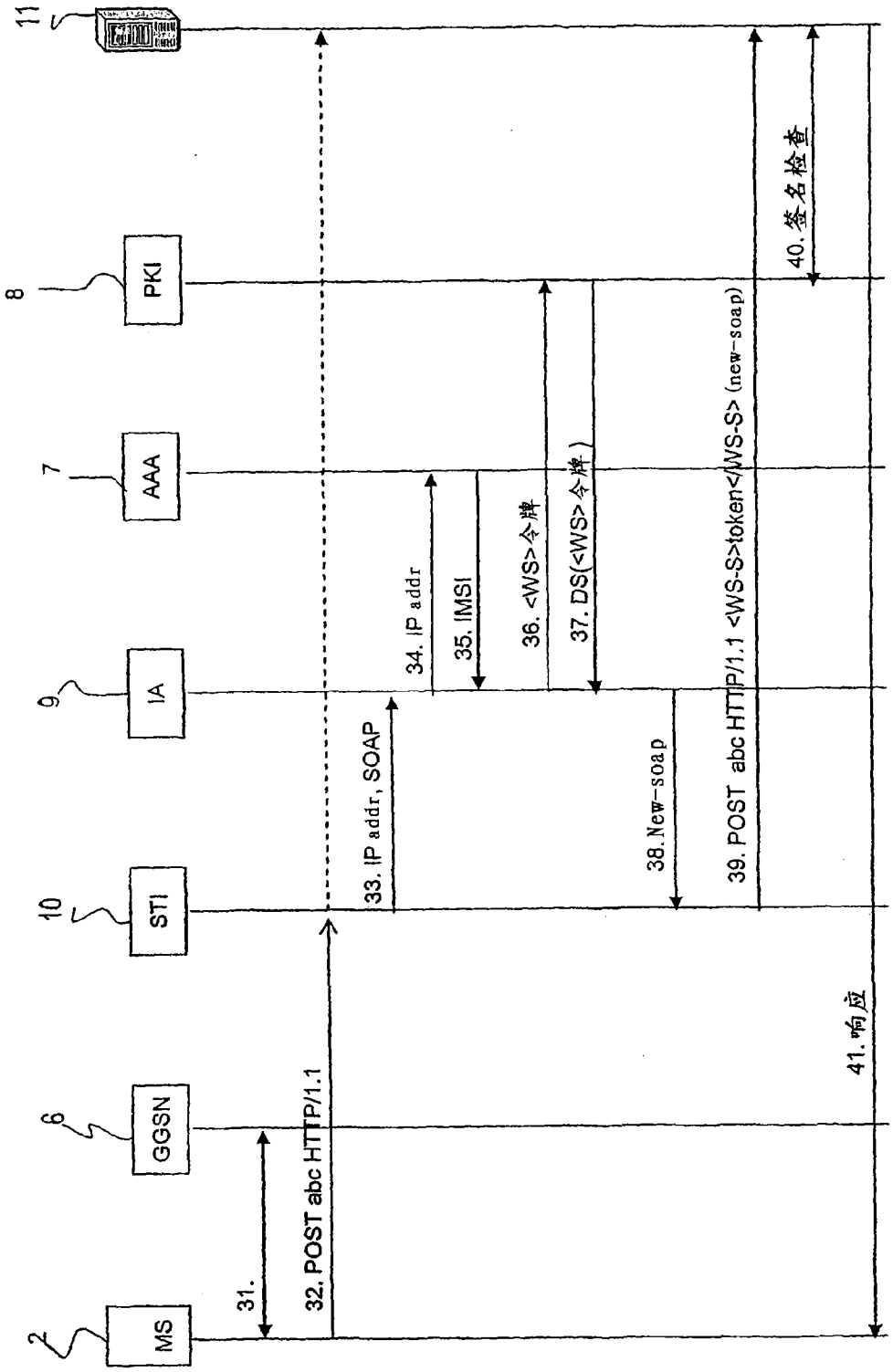

11
8
PKI
7
AAA
9
IA
10
STI
6
GGSN
2
MS
31.
32. POST abc HTTP/1.1
33. IP addr, SOAP
34. IP addr
35. IMSI
36. <WS>令牌
37. DS(<WS>令牌)
38. New-soap
39. POST abc HTTP/1.1 <WS-S>token</WS-S> (new-soap)
40. 签名检查
41. 响应

图 3

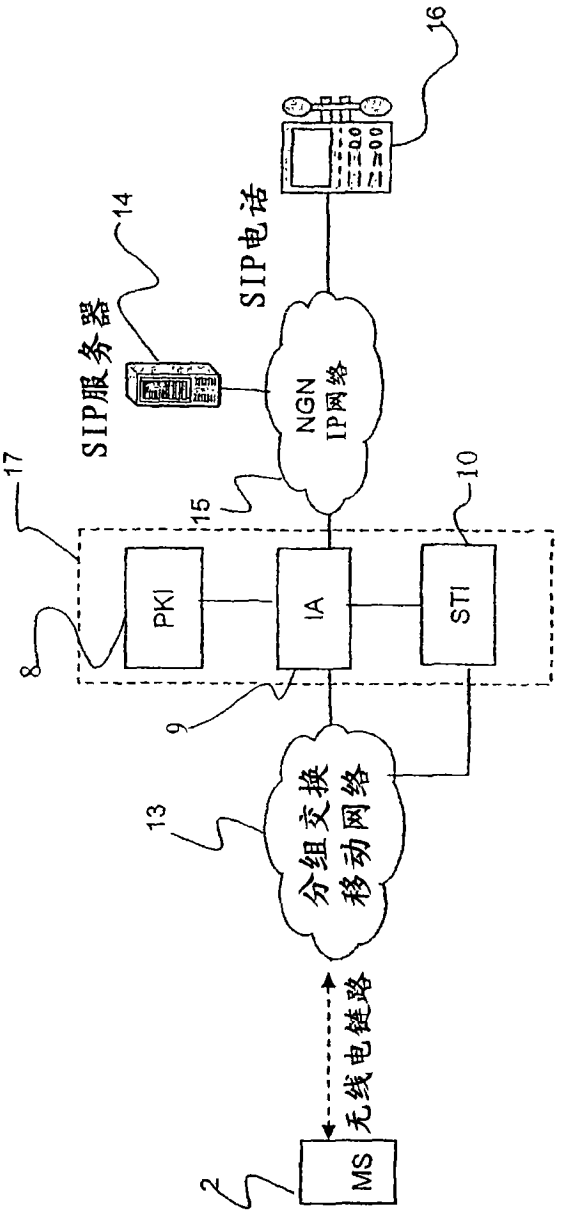

16
SIP电话
14
SIP服务器
NGN
IP网络
17
15
10
PKI
IA
STI
8
9
13
分组交换
移动网络
无线电链路
MS
2

图 4

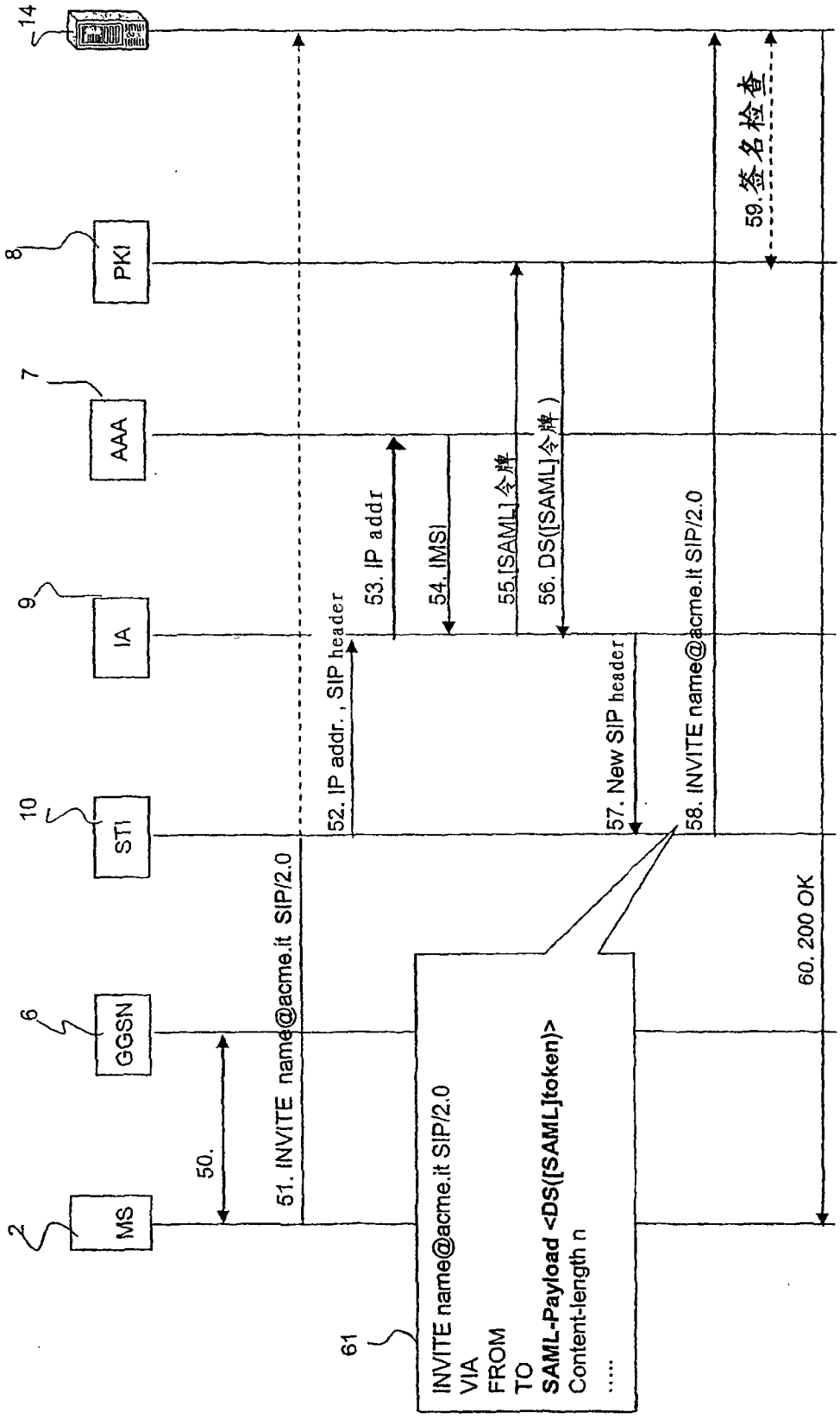

14
8
PKI
7
AAA
9
IA
10
STI
6
GGSN
2
MS
59. 签名检查
53. IP addr
54. IMSI
55.[SAML]令牌
56. DS([SAML]令牌)
52. IP addr., SIP header
57. New SIP header
58. INVITE name@acme.it SIP/2.0
50.
51. INVITE name@acme.it SIP/2.0
60. 200 OK
61
INVITE name@acme.it SIP/2.0
VIA
FROM
TO
SAML-Payload <DS([SAML]token)>
Content-length n
.....

图 5

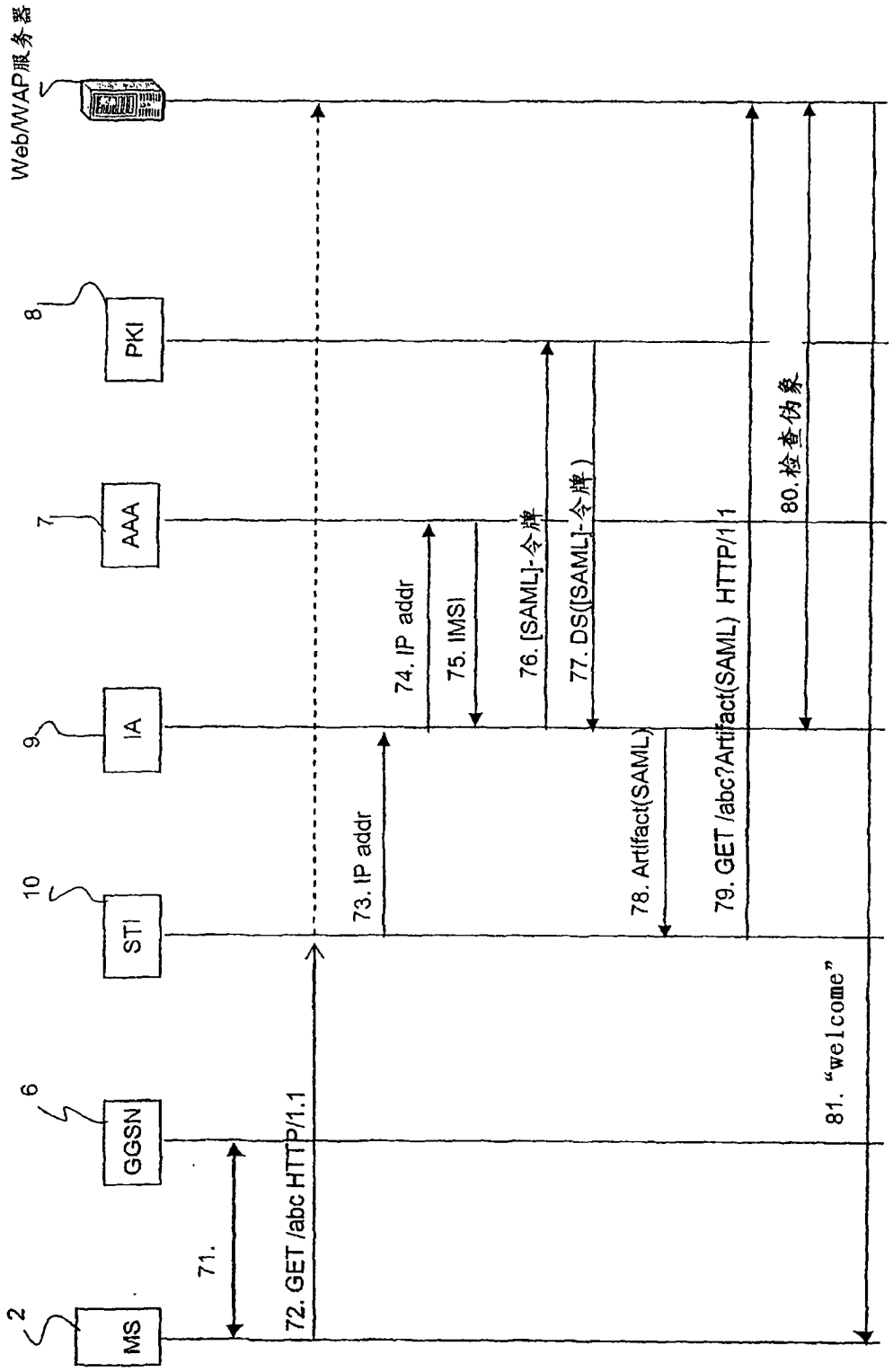

Web/WAP服务器
PKI
8
AAA
7
IA
9
STI
10
GGSN
6
MS
2
71.
72. GET /abc HTTP/1.1
73. IP addr
74. IP addr
75. IMSI
76. [SAML]-令牌
77. DS([SAML]-令牌)
78. Artifact(SAML)
79. GET /abc?Artifact(SAML) HTTP/1.1
80. 检查伪象
81. "welcome"

图 6

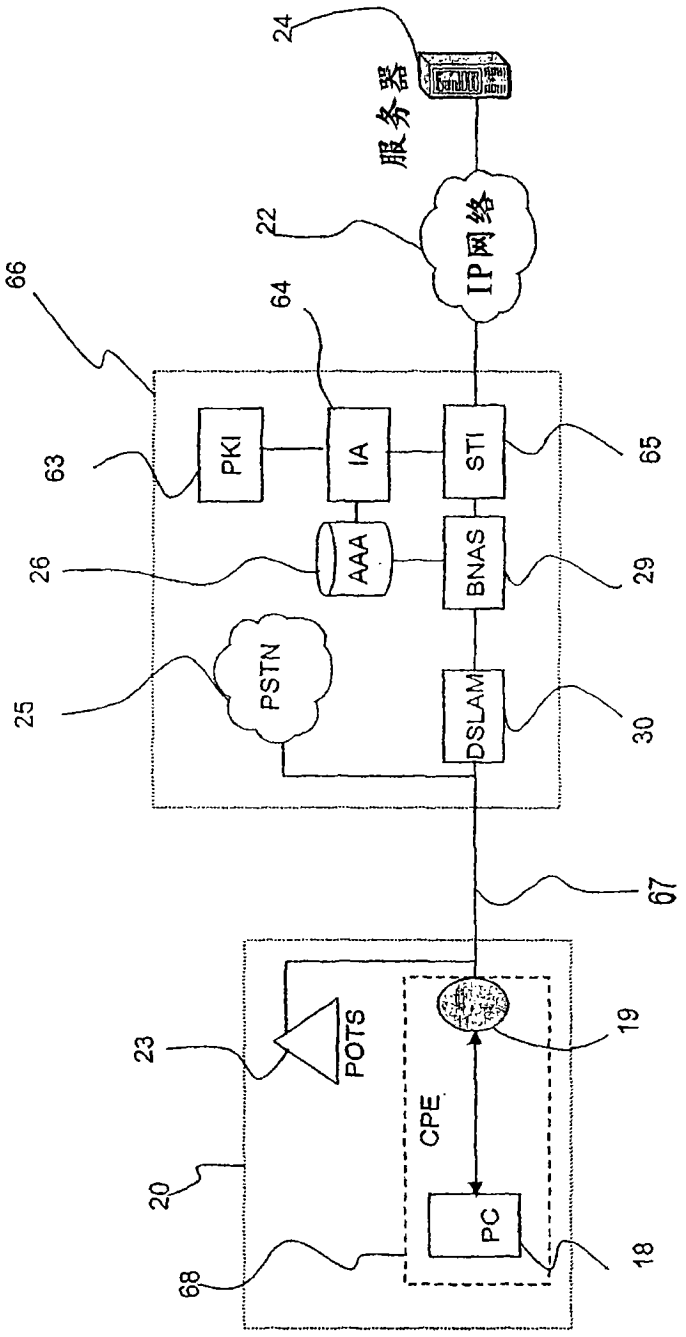

24
服务器
22
IP网络
66
64
63
PKI
IA
STI
65
26
AAA
BNAS
29
25
PSTN
DSLAM
30
67
23
POTS
CPE
19
20
PC
18
68

图7

表

标识	服务提供者	假名
LOGIN-A	SP-1	PS-A1
LOGIN-A	SP-2	PS-A2
LOGIN-A	SP-3	PS-A3
LOGIN-B	SP-1	PS-B1
LOGIN-B	SP-4	PS-B4
LOGIN-C	SP-5	PS-C5
..	..	..
..	..	..

图 8

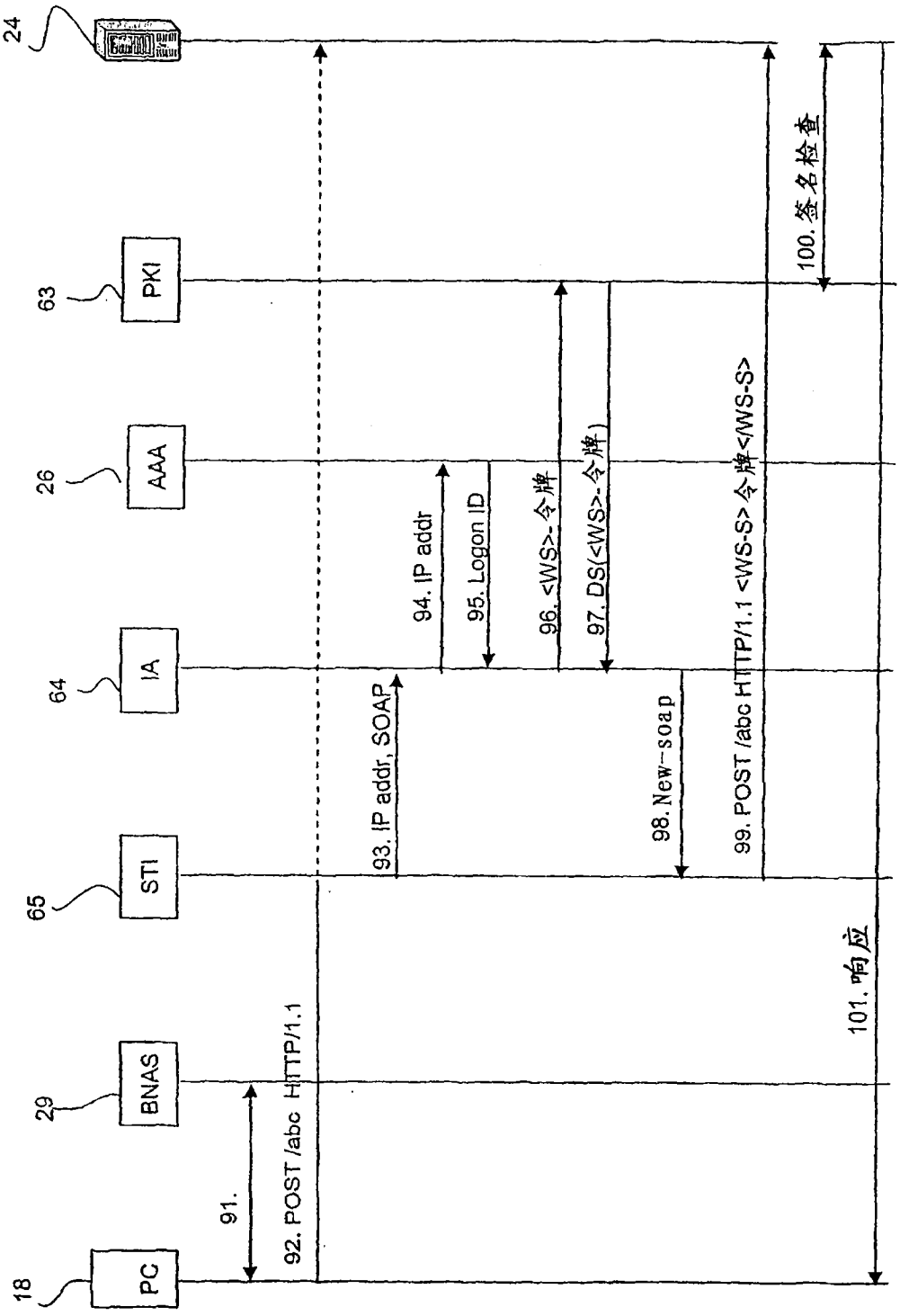

24
63
PKI
26
AAA
64
IA
65
STI
29
BNAS
18
PC
91.
92. POST /abc HTTP/1.1
93. IP addr, SOAP
94. IP addr
95. Logon ID
96. <WS>-令牌
97. DS(<WS>-令牌)
98. New-soap
99. POST /abc HTTP/1.1 <WS-S>令牌</WS-S>
100. 签名检查
101. 响应

图 9

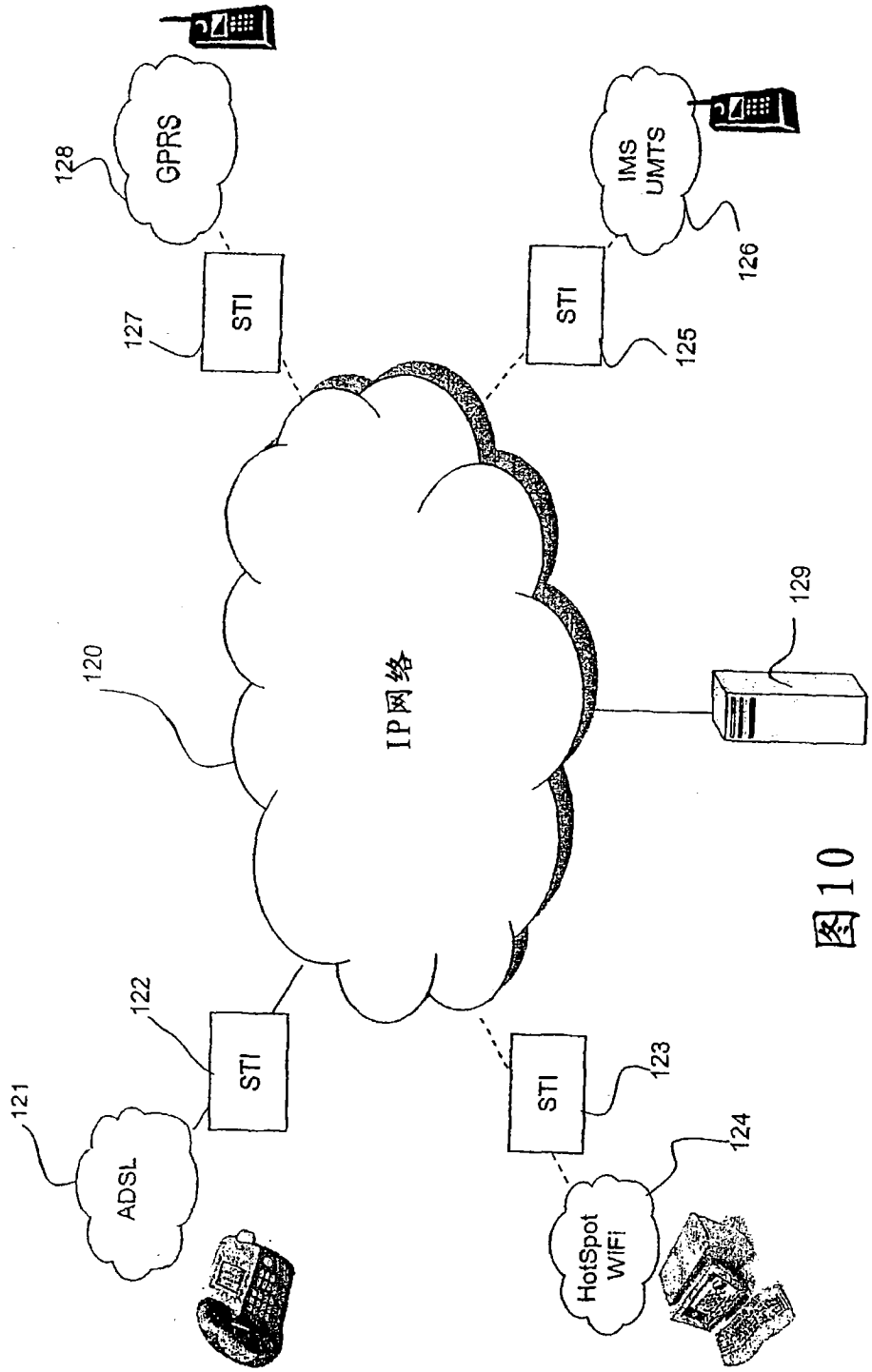

GPRS
128
STI
127
IMS
UMTS
126
STI
125
IP网络
120
129
ADSL
121
STI
122
HotSpot
WiFi
124
STI
123

图10

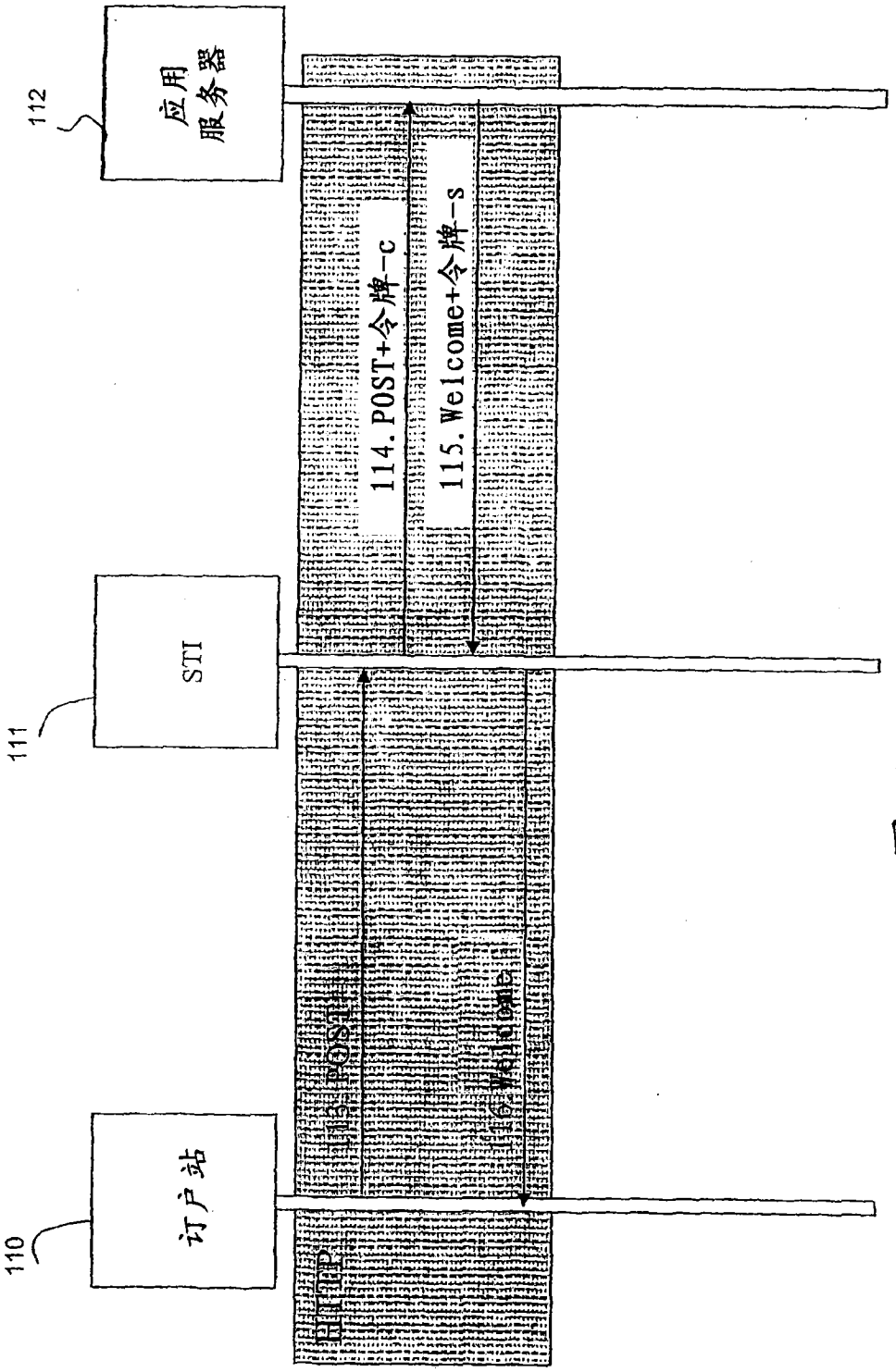

应用服务器
112
STI
111
订户站
110
HTTP
113. POST
114. POST+令牌-c
115. Welcome+令牌-s
116. Welcome

图 11