(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 102082665 B
(45)授权公告日 2013.10.23

(21)申请号 200910238551.0

(22)申请日 2009.11.30

(73)专利权人 中国移动通信集团公司
地址 100032 北京市西城区金融大街 29 号

(72)发明人 曹振 刘大鹏 邓辉

(74)专利代理机构 北京鑫媛睿博知识产权代理有限公司 11297
代理人 龚家骅

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 29/06(2006.01)

审查员 马晔

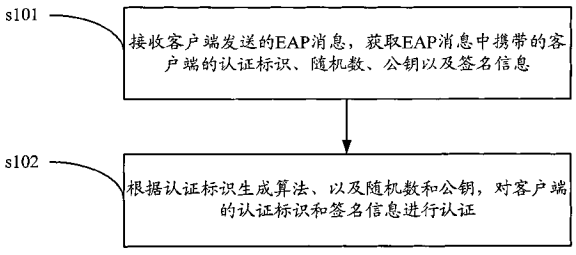
权利要求书3页 说明书6页 附图3页

(54)发明名称

一种 EAP 认证中的标识认证方法、系统和设备

(57)摘要

本发明的实施例公开了一种可扩展认证协议 EAP 认证中的标识认证方法、系统和设备。该方法包括：接收客户端发送的 EAP 消息，获取所述 EAP 消息中携带的所述客户端的认证标识、随机数、公钥以及签名信息；根据认证标识生成算法、以及所述随机数和公钥，对所述客户端的认证标识和签名信息进行认证。通过使用本发明的实施例，利用公开密钥和 EAP 认证标识 ID 的绑定技术来防止认证标识被盗用，彻底的防止了攻击者窃取盗用其他用户认证标识。



CN 102082665 B

1. 一种可扩展认证协议 EAP 认证中的标识认证方法，其特征在于，包括：

客户端根据 RSA 公开密钥算法生成公钥和私钥；

所述客户端根据所述公钥和认证标识生成算法，生成认证标识；

所述客户端接收到 EAP 认证请求时，生成随机数，并根据所述随机数和所述私钥生成签名信息；

所述客户端向认证服务器发送 EAP 消息，所述 EAP 消息中携带所述客户端的认证标识、随机数、公钥以及签名信息；

接收所述客户端发送的 EAP 消息，获取所述 EAP 消息中携带的所述客户端的认证标识、随机数、公钥以及签名信息；

根据所述认证标识生成算法、以及所述随机数和公钥，对所述客户端的认证标识和签名信息进行认证；

其中，所述认证标识生成算法为 SHA-1 单向 Hash 函数，所述客户端根据所述公钥和认证标识生成算法，生成认证标识 ID；具体为：

ID=SHA-1（PK），其中，PK 为所述公钥。

2. 如权利要求 1 所述的方法，其特征在于，所述对所述客户端的认证标识和签名信息进行认证包括：

根据认证标识生成算法以及所述公钥，生成认证标识；所述生成的认证标识与所述客户端发送的 EAP 消息中携带的认证标识相同时，对所述客户端的认证标识的认证成功；否则认证失败；

根据所述客户端的公钥和所述随机数，对所述客户端发送的 EAP 消息中携带的签名信息进行认证；获取认证结果。

3. 如权利要求 1 或 2 中任一项所述的方法，其特征在于，所述客户端发送的 EAP 消息为 EAP 响应消息，所述 EAP 响应消息中携带长度为 160 位的认证标识、以及长度为 24 位的随机数。

4. 如权利要求 1 所述的方法，其特征在于，所述对客户端的认证标识和签名信息进行认证后，还包括：

对所述客户端的认证标识和签名信息的认证通过后，根据所述客户端的认证标识对应的 EAP 认证方法，对所述客户端进行 EAP 认证。

5. 一种认证服务器，其特征在于，包括：

获取单元，用于接收客户端发送的 EAP 消息，获取所述 EAP 消息中携带的所述客户端的认证标识、随机数、公钥以及签名信息；

认证单元，用于根据认证标识生成算法、以及所述随机数和公钥，对所述客户端的认证标识和签名信息进行认证；

其中，所述认证标识生成算法为 SHA-1 单向 Hash 函数，所述认证服务器接收客户端发送的 EAP 消息前，还包括：

所述客户端根据 RSA 公开密钥算法生成公钥和私钥；

所述客户端根据所述公钥和认证标识生成算法，生成认证标识；

所述客户端接收到 EAP 认证请求时，生成随机数，并根据所述随机数和所述私钥生成签名信息；

所述客户端向认证服务器发送 EAP 消息，所述 EAP 消息中携带所述客户端的认证标识、随机数、公钥以及签名信息；

所述客户端根据所述公钥和认证标识生成算法，生成认证标识 ID；具体为：

ID=SHA-1（PK），其中，PK 为所述公钥。

6. 如权利要求 5 所述的认证服务器，其特征在于，所述认证单元具体用于：

根据认证标识生成算法以及所述公钥，生成认证标识；所述生成的认证标识与所述客户端发送的 EAP 消息中携带的认证标识相同时，对所述客户端的认证标识的认证成功；否则认证失败；

根据所述客户端的公钥和所述随机数，对所述客户端发送的 EAP 消息中携带的签名信息进行认证；获取认证结果。

7. 如权利要求 5 所述的认证服务器，其特征在于，还包括：

配置单元，用于存储每一客户端认证标识对应的 EAP 认证方法，并提供给所述认证单元；

所述认证单元，还用于对所述客户端的认证标识和签名信息的认证通过后，根据所述客户端的认证标识对应的 EAP 认证方法，对所述客户端进行 EAP 认证。

8. 一种客户端，其特征在于，包括：

密钥生成单元，用于根据 RSA 公开密钥算法生成公钥和私钥；

认证标识生成单元，用于根据所述公钥和认证标识生成算法，生成认证标识；

签名信息生成单元，用于接收到 EAP 认证请求时，生成随机数，并根据所述随机数和所述私钥生成签名信息；

EAP 消息发送单元，用于向认证服务器发送 EAP 消息，所述 EAP 消息中携带所述客户端的认证标识、随机数、公钥以及签名信息；

所述认证标识生成单元根据所述公钥和认证标识生成算法，生成认证标识 ID；具体为：

ID=SHA-1（PK），其中，PK 为所述公钥

其中，所述认证标识生成算法为 SHA-1 单向 Hash 函数。

9. 一种 EAP 认证系统，其特征在于，包括：

客户端，用于向认证服务器发送 EAP 消息，所述 EAP 消息中携带所述客户端的认证标识、随机数、公钥以及签名信息；

认证服务器，用于接收所述客户端发送的 EAP 消息，获取所述 EAP 消息中携带的所述客户端的认证标识、随机数、公钥以及签名信息；根据认证标识生成算法、以及所述随机数和公钥，对所述客户端的认证标识和签名信息进行认证；

其中，所述认证标识生成算法为 SHA-1 单向 Hash 函数，所述认证服务器接收客户端发送的 EAP 消息前，还包括：

所述客户端根据 RSA 公开密钥算法生成公钥和私钥；

所述客户端根据所述公钥和认证标识生成算法，生成认证标识；

所述客户端接收到 EAP 认证请求时，生成随机数，并根据所述随机数和所述私钥生成签名信息；

所述客户端向认证服务器发送 EAP 消息，所述 EAP 消息中携带所述客户端的认证标识、

随机数、公钥以及签名信息；

所述客户端根据所述公钥和认证标识生成算法，生成认证标识 ID；具体为：

ID=SHA-1（PK），其中，PK 为所述公钥。

一种 EAP 认证中的标识认证方法、系统和设备

技术领域

[0001] 本发明涉及通讯技术领域，尤其涉及一种 EAP 认证中的标识认证方法、系统和设备。

背景技术

[0002] EAP(Extensible Authentication Protocol，可扩展认证协议）是一种提供网络接入认证的可扩展框架，可以支持不同的认证方法。EAP 一般承载在互联网二层协议之上，用户只有在完成 EAP 规定的认证之后才能进行合法的网络通信，不能正确认证的用户则不能进行数据通信。许多网络都使用 EAP 作为接入认证的标准协议，如 802.11、WIMAX(Worldwide Interoperability forMicrowave Access，微波存取全球互通）等。EAP 是互联网安全认证的基础，其包括三个实体：客户端，认证者，AAA(Authentication/Authorization/Accounting，认证 / 授权 / 计费）服务器。其原理如下：认证者向客户端发起一个认证标识符请求 (EAP Request/ID)，客户端返回自己的认证标识符 (EAPResponse/ID)，认证者把客户端的认证标识转发给 AAA 服务器，服务器通过本地配置判断此客户端应该进行何种具体的认证方法（如 EAP-MD5，EAP-TLS 等），然后开始发起具体的认证过程。在认证过程中，认证者对 EAP 的认证消息在客户端和 AAA 服务器之间进行透传，由于不执行具体的认证计算，认证者作为接入点不需要实现具体的认证方法；客户端和 AAA 服务器进行认证相关的安全计算，因此保持了网络的可扩展性。

[0003] 不同的认证方法有不同的安全强度，比如说 EAP-MD5 仅让服务器认证客户端，客户端没有能力认证服务器，而 EAP-TLS 则能够支持服务器和客户端的双向认证，具有相对更高的安全强度。这样造成了伪造认证标识符的攻击形式，假设用户 A 使用的是 EAP-MD5，攻击者 M 窃取了用户 A 的认证标识向服务器发起认证，服务器则会向 M 发起 EAP-MD5 的认证，使得攻击者 M 较容易入侵网络。

[0004] 为了克服现有技术中存在的伪造认证标识符的问题，现有技术中提供了以下解决方式。

[0005] 方法一是忽略认证标识交互，由于现有技术中规定 EAP 认证标识的交互是可选的，因此提出可以忽略 EAP 认证开始的认证标识交互，对所有的用户使用同一个初始的认证方法，在 EAP 安全隧道建立起来之后再交换认证标识。因此其通过避免 EAP 认证标识的交互过程来防止伪造认证标识的攻击。该方法存在的问题在于，其并不能作为一个通用的方案，因为目前很多场景和认证方法都需要 AAA 服务器获知客户端的认证标识。

[0006] 方法二是通过交换一个匿名的方式来防止攻击者伪造标识，具体的，可以使用在 EAP 开始的认证标识交换过程中使用一个省略用户 ID 的网络地址标识，如”@example.net” 来标识客户端；或在 EAP 认证标识交互中使用“匿名 + 域名”的方式来提供 ID 保护，如同一域 (example.net) 下的用户使用”anonymous@example.net”作为统一的认证标识。由于此 NAI 中没有用户的标识信息，用户的标识不会被窃取。但是该方法存在的问题在于，虽然在 NAI 中没有用户的标识信息，但是攻击者仍然能够轻易伪造此 NAI 信息来进行 ID 欺骗，因此

该方法只保护了用户的 ID 不在明文传输中泄露，不能防止伪造 ID 的攻击行为。

发明内容

[0007] 本发明的实施例提供一种 EAP 认证中的标识认证方法、系统和设备，用于防止攻击者窃取盗用其他用户的 EAP 认证标识。

[0008] 本发明的实施例提供了一种 EAP 认证中的标识认证方法，包括：

[0009] 接收客户端发送的 EAP 消息，获取所述 EAP 消息中携带的所述客户端的认证标识、随机数、公钥以及签名信息；

[0010] 根据认证标识生成算法、以及所述随机数和公钥，对所述客户端的认证标识和签名信息进行认证。

[0011] 其中，所述接收客户端发送的 EAP 消息前，还包括：

[0012] 所述客户端根据 RSA 公开密钥算法生成公钥和私钥；

[0013] 所述客户端根据所述公钥和认证标识生成算法，生成认证标识；

[0014] 所述客户端接收到 EAP 认证请求时，生成随机数，并根据所述随机数和所述私钥生成签名信息；

[0015] 所述客户端向认证服务器发送 EAP 消息，所述 EAP 消息中携带所述客户端的认证标识、随机数、公钥以及签名信息。

[0016] 其中，所述对所述客户端的认证标识和签名信息进行认证包括：

[0017] 根据认证标识生成算法以及所述公钥，生成认证标识；所述生成的认证标识与所述客户端发送的 EAP 消息中携带的认证标识相同时，对所述客户端的认证标识的认证成功；否则认证失败；

[0018] 根据所述客户端的公钥和所述随机数，对所述客户端发送的 EAP 消息中携带的签名信息进行认证；获取认证结果。

[0019] 其中，所述客户端发送的 EAP 消息为 EAP 响应消息，所述 EAP 响应消息中携带长度为 160 位的认证标识、以及长度为 24 位的随机数。

[0020] 其中，所述认证标识生成算法为 SHA-1 单向 Hash 函数。

[0021] 其中，所述对客户端的认证标识和签名信息进行认证后，还包括：

[0022] 对所述客户端的认证标识和签名信息的认证通过后，根据所述客户端的认证标识对应的 EAP 认证方法，对所述客户端进行 EAP 认证。

[0023] 本发明的实施例还提供了一种认证服务器，包括：

[0024] 获取单元，用于接收客户端发送的 EAP 消息，获取所述 EAP 消息中携带的所述客户端的认证标识、随机数、公钥以及签名信息；

[0025] 认证单元，用于根据认证标识生成算法、以及所述随机数和公钥，对所述客户端的认证标识和签名信息进行认证。

[0026] 其中，所述认证单元具体用于：

[0027] 根据认证标识生成算法以及所述公钥，生成认证标识；所述生成的认证标识与所述客户端发送的 EAP 消息中携带的认证标识相同时，对所述客户端的认证标识的认证成功；否则认证失败；

[0028] 根据所述客户端的公钥和所述随机数，对所述客户端发送的 EAP 消息中携带的签

名信息进行认证；获取认证结果。

[0029] 其中，还包括：

[0030] 配置单元，用于存储每一客户端认证标识对应的 EAP 认证方法，并提供给所述认证单元；

[0031] 所述认证单元，还用于对所述客户端的认证标识和签名信息的认证通过后，根据所述客户端的认证标识对应的 EAP 认证方法，对所述客户端进行 EAP 认证。

[0032] 本发明的实施例还提供了一种客户端，包括：

[0033] 密钥生成单元，用于根据 RSA 公开密钥算法生成公钥和私钥；

[0034] 认证标识生成单元，用于根据所述公钥和认证标识生成算法，生成认证标识；

[0035] 签名信息生成单元，用于接收到 EAP 认证请求时，生成随机数，并根据所述随机数和所述私钥生成签名信息；

[0036] EAP 消息发送单元，用于向认证服务器发送 EAP 消息，所述 EAP 消息中携带所述客户端的认证标识、随机数、公钥以及签名信息。

[0037] 本发明的实施例还提供了一种 EAP 认证系统，包括：

[0038] 客户端，用于向认证服务器发送 EAP 消息，所述 EAP 消息中携带所述客户端的认证标识、随机数、公钥以及签名信息；

[0039] 认证服务器，用于接收所述客户端发送的 EAP 消息，获取所述 EAP 消息中携带的所述客户端的认证标识、随机数、公钥以及签名信息；根据认证标识生成算法、以及所述随机数和公钥，对所述客户端的认证标识和签名信息进行认证。

[0040] 与现有技术相比，本发明的实施例具有以下优点：

[0041] 本发明的实施例中，利用公开密钥和 EAP 认证标识 ID 的绑定技术来防止认证标识被盗用，彻底的防止了攻击者窃取盗用其他用户认证标识，而现有的相关的技术没有解决这个问题；另外，其支持不同的 EAP 认证方法，不需要修改已有的 EAP 认证协议，属于通用的解决方法。

附图说明

[0042] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0043] 图 1 是本发明实施例中提供的 EAP 认证中的标识认证方法流程图；

[0044] 图 2 是本发明实施例的应用场景中提供的 EAP 认证中的标识认证方法流程图；

[0045] 图 3 是本发明实施例的应用场景中 EAP Response 消息的结构示意图；

[0046] 图 4 是本发明实施例中提供的认证服务器的结构示意图；

[0047] 图 5 是本发明实施例中提供的客户端的结构示意图。

具体实施方式

[0048] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本发明一部分实施例，而不是全部的实施例。基于本

发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0049] 本发明的实施例提供了一种 EAP 认证中的标识认证方法，如图 1 所示，包括：

[0050] 步骤 s101、接收客户端发送的 EAP 消息，获取 EAP 消息中携带的客户端的认证标识、随机数、公钥以及签名信息；

[0051] 步骤 s102、根据认证标识生成算法、以及随机数和公钥，对客户端的认证标识和签名信息进行认证。

[0052] 本发明的实施例提供了一个具体的应用场景，描述本发明提供的 EAP 认证中的标识认证方法的具体实施方式。

[0053] 本发明的应用场景中，客户端生成 RSA 公钥算法下对应的公钥 PK 和私钥 SK，利用 PK 和认证标识生成算法生成自己对应的 160 位的认证标识，例如采用单向 Hash 函数 SHA-1 作为认证标识生成算法，则 ID = SHA-1(PK)。公钥算法的性质保证了通过公钥 PK 无法推导出私钥 SK，而没有私钥 SK 也无法伪造数字签名信息；单向函数的性质保证了无法根据另外一个 PK' 映射到同样一个 ID.

[0054] 另外，作为 EAP 认证服务器的 AAA 服务器根据客户端生成的认证标识 ID 在本地配对客户端配置相应的 EAP 认证方法。如客户端 A 使用的认证方法为 EAP-MD5，则 AAA 服务器在配置中，对于客户端 A 的 ID 和 EAP-MD5 方法之间建立映射关系；如用户 B 所使用的认证方法为 EAP-TLS，则 AAA 服务器在配置中，对于客户端 B 的 ID 和 EAP-TLS 方法之间建立映射关系。

[0055] 本发明提供的实施例中，EAP 认证中的标识认证方法如图 2 所示，包括以下步骤：

[0056] 步骤 s201、认证者 (Authenticator) 发起 EAP 认证，向客户端 A(EAP PeerA) 发送 EAP Request/ID 消息。其中认证者可以为网络接入服务器。

[0057] 步骤 s202、客户端 A 生成数字签名，附加公钥信息。

[0058] 具体的，客户端 A 生成随机数 Ra，并根据私钥 SK 和数字签名算法生成数字签名 RS_A。

[0059] 步骤 s203、客户端 A 返回 EAP Response/ID，在消息中携带客户端 A 的认证标识 ID，随机数 Ra，公钥 PK，以及签名信息。

[0060] 其中，客户端 A 在发送的 EAP Response/ID 中，添加预先生成的认证标识假设为 ID_A，除了响应 ID 信息之外，还在 EAP Response/ID 消息中附加自己的公钥 PK_A，随机数 Ra，以及利用 RS_A 签名算法和私钥 SK_A 计算的签名信息。本发明的实施例中，修改后的 EAP Response/ID 的消息格式的一种可用形式可以如图 3 所示。

[0061] 步骤 s204、EAP 标识的认证过程。

[0062] 其中，AAA 服务器接收到客户端 A 返回的认证标识后，计算确认此客户端 A 是否为该标识 ID_A 的合法拥有者。以认证标识算法为单向 Hash 函数 SHA-1 为例，则 AAA 服务器首先检查公式 ID = SHA-1(PK) 是否成立，如果成立，则再利用公钥 PK 检查 EAP Response/ID 消息中包含的数字签名是否正确，如果正确，AAA 服务器则确认此客户端 A 的确是此标识 ID_A 的拥有者，随后发起相应的 EAP 认证过程。

[0063] 通过上述流程，攻击者无法进行伪造认证标识的攻击。首先，虽然攻击者能够窃听到客户端明文传输的 ID 信息和公钥 PK，但是攻击者无法通过公钥推导出私钥，也就不能伪

造出对应的签名信息。其次，攻击者不能通过另外一个公钥来得到相同的 ID，由于 ID 是由 PK 通过单向函数 SHA-1 计算出来的，攻击者不能通过另外一个 PK' 来得到相同的 ID。

[0064] 本发明的实施例提供的方法中，利用公开密钥和 EAP 认证标识 ID 的绑定技术来防止认证标识被盗用，彻底的防止了攻击者窃取盗用其他用户认证标识，而现有的相关的技术没有解决这个问题；另外，其支持不同的 EAP 认证方法，不需要修改已有的 EAP 认证协议，属于通用的解决方法。

[0065] 本发明的实施例提供了一种 EAP 认证系统，包括：

[0066] 客户端，用于向认证服务器发送 EAP 消息，EAP 消息中携带客户端的认证标识、随机数、公钥以及签名信息；

[0067] 认证服务器，用于接收客户端发送的 EAP 消息，获取 EAP 消息中携带的客户端的认证标识、随机数、公钥以及签名信息；根据认证标识生成算法、以及随机数和公钥，对客户端的认证标识和签名信息进行认证。

[0068] 本发明的实施例提供的认证服务器中，其结构如图 4 所示，包括：

[0069] 获取单元 10，用于接收客户端发送的 EAP 消息，获取 EAP 消息中携带的客户端的认证标识、随机数、公钥以及签名信息；

[0070] 认证单元 20，用于根据认证标识生成算法、以及随机数和公钥，对客户端的认证标识和签名信息进行认证。

[0071] 该认证单元 20 具体用于：

[0072] 根据认证标识生成算法以及公钥，生成认证标识；生成的认证标识与客户端发送的 EAP 消息中携带的认证标识相同时，对客户端的认证标识的认证成功；否则认证失败；根据客户端的公钥和随机数，对客户端发送的 EAP 消息中携带的签名信息进行认证；获取认证结果。

[0073] 该认证服务器还可以包括：配置单元 30，用于存储每一客户端认证标识对应的 EAP 认证方法，并提供给认证单元 20。

[0074] 认证单元 20，还用于对客户端的认证标识和签名信息的认证通过后，根据客户端的认证标识对应的 EAP 认证方法，对客户端进行 EAP 认证。

[0075] 本发明的实施例提供的客户端中，其结构如图 5 所示，包括：

[0076] 密钥生成单元 50，用于根据 RSA 公开密钥算法生成公钥和私钥；

[0077] 认证标识生成单元 60，用于根据公钥和认证标识生成算法，生成认证标识；

[0078] 签名信息生成单元 70，用于接收到 EAP 认证请求时，生成随机数，并根据随机数和密钥生成单元 50 生成的私钥生成签名信息；

[0079] EAP 消息发送单元 80，用于向认证服务器发送 EAP 消息，EAP 消息中携带认证标识生成单元 60 生成的认证标识、密钥生成单元 50 生成的公钥以及签名信息生成单元 70 生成的随机数和签名信息。

[0080] 本发明的实施例提供的系统和设备中，利用公开密钥和 EAP 认证标识 ID 的绑定技术来防止认证标识被盗用，彻底的防止了攻击者窃取盗用其他用户认证标识，而现有的相关的技术没有解决这个问题；另外，其支持不同的 EAP 认证方法，不需要修改已有的 EAP 认证协议，属于通用的解决方法。

[0081] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可以通

过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

[0082] 本领域技术人员可以理解附图只是一个优选实施例的示意图，附图中的单元或流程并不一定是实施本发明所必须的。

[0083] 本领域技术人员可以理解实施例中的装置中的单元可以按照实施例描述进行分布于实施例的装置中，也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的单元可以合并为一个单元，也可以进一步拆分成多个子单元。

[0084] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

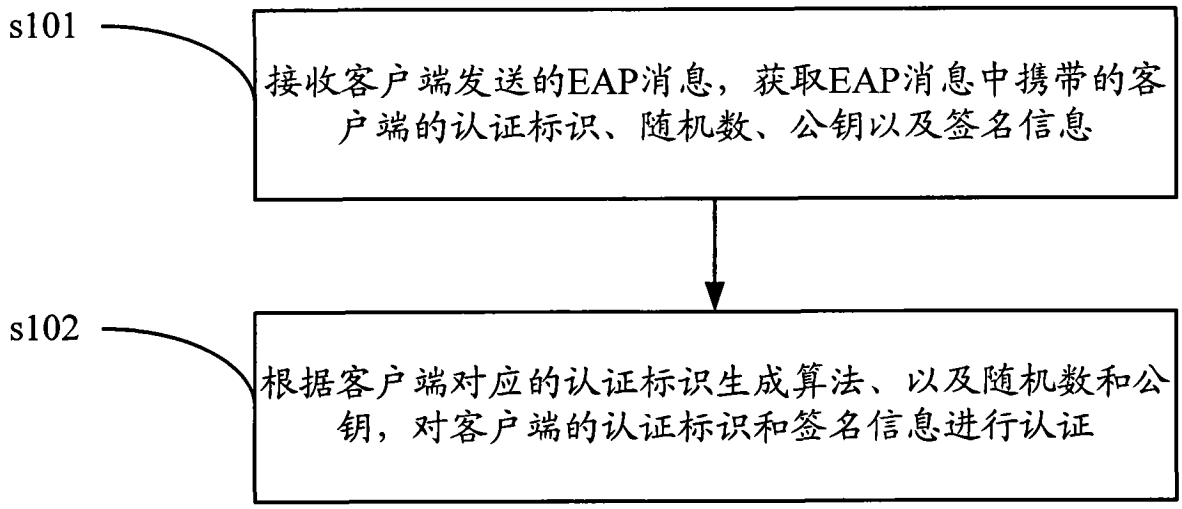

s101
接收客户端发送的EAP消息，获取EAP消息中携带的客户端的认证标识、随机数、公钥以及签名信息
s102
根据客户端对应的认证标识生成算法、以及随机数和公钥，对客户端的认证标识和签名信息进行认证

图 1

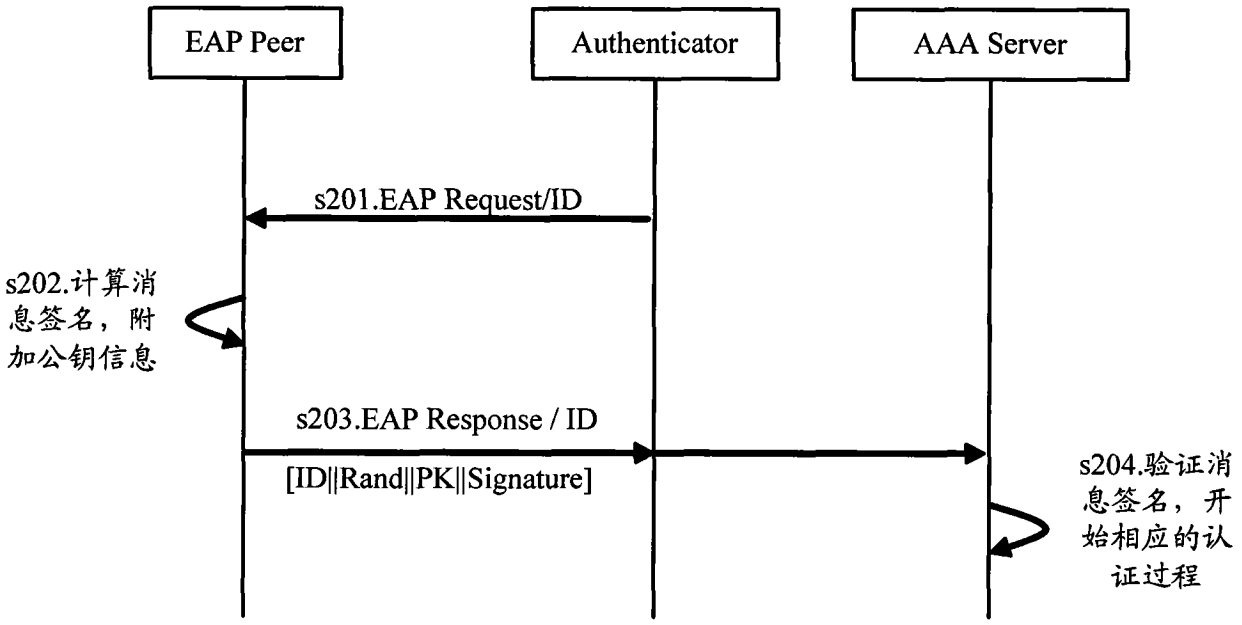

EAP Peer
Authenticator
AAA Server
s201.EAP Request/ID
s202.计算消息签名，附加公钥信息
s203.EAP Response / ID
[ID||Rand||PK||Signature]
s204.验证消息签名，开始相应的认证过程

图 2

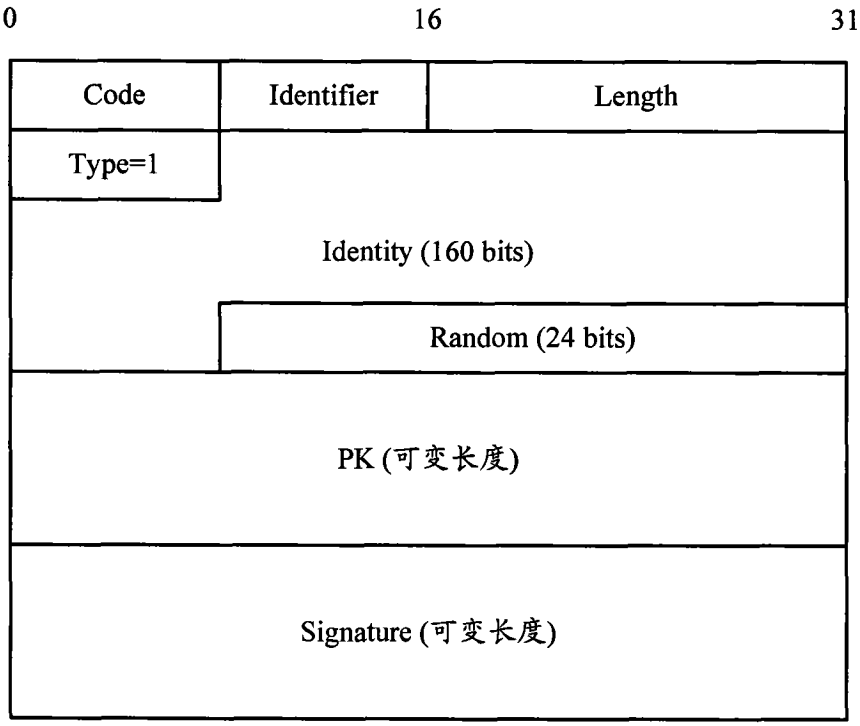

0
16
31
Code
Identifier
Length
Type=1
Identity (160 bits)
Random (24 bits)
PK (可变长度)
Signature (可变长度)

图 3

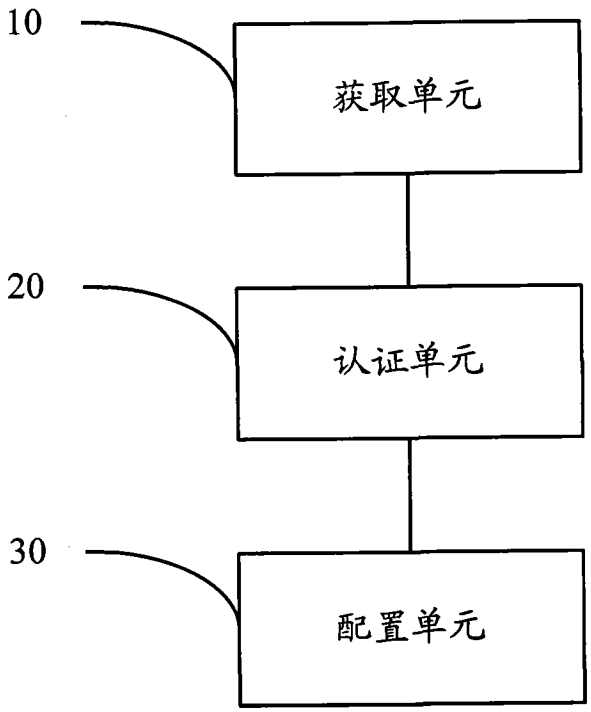

10
获取单元
20
认证单元
30
配置单元

图 4

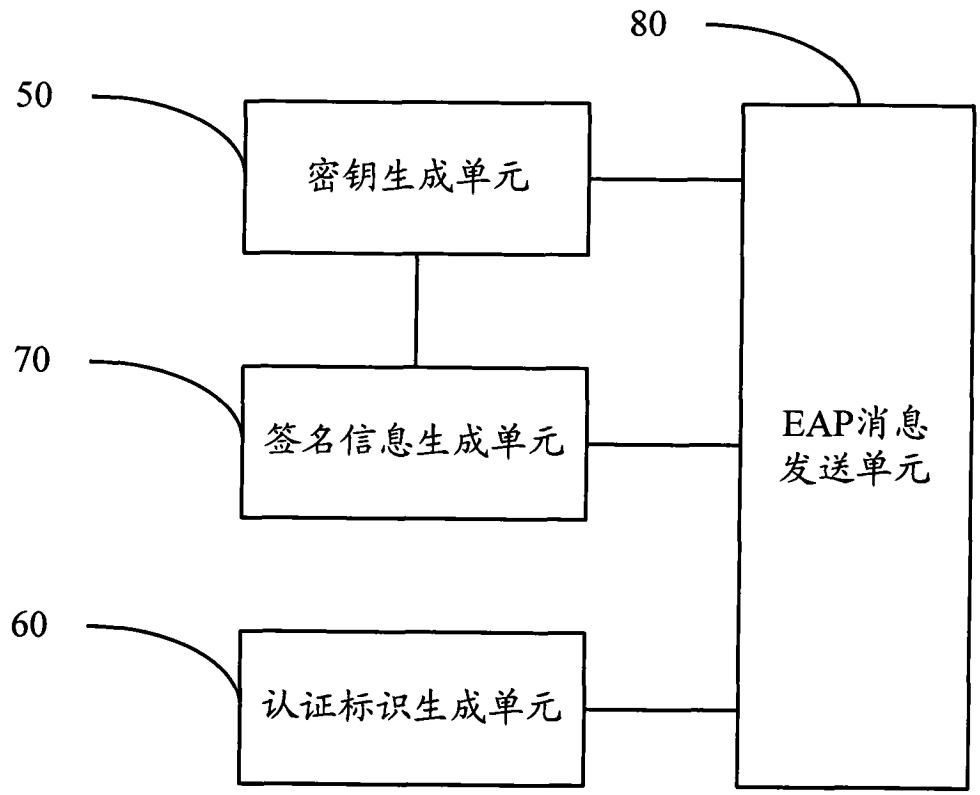


图 5