(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113727059 B
(45)授权公告日 2023.10.24

(21)申请号 202111013197.9
(22)申请日 2021.08.31
(65)同一申请的已公布的文献号
申请公布号 CN 113727059 A
(43)申请公布日 2021.11.30
(73)专利权人 成都卫士通信息产业股份有限公司
地址 610041 四川省成都市高新区云华路333号
(72)发明人 任旭斌 张舒黎 周泽恒 段品言 周小东
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 刘翠香
(51)Int.Cl.
H04N 7/15(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)
(56)对比文件
CN 109302412 A,2019.02.01
CN 110602706 A,2019.12.20
CN 110933112 A,2020.03.27
CN 111147471 A,2020.05.12
CN 112291072 A,2021.01.29
CN 1791866 A,2006.06.21
US 2003070072 A1,2003.04.10
US 2009006844 A1,2009.01.01
US 2011038483 A1,2011.02.17
US 2017374058 A1,2017.12.28
US 2018048864 A1,2018.02.15
US 2019013956 A1,2019.01.10
US 2020204990 A1,2020.06.25
宋玲.基于证书实现多媒体会议安全身份认证的方案.计算机工程.2006,(第01期),全文.
审查员 黎媛

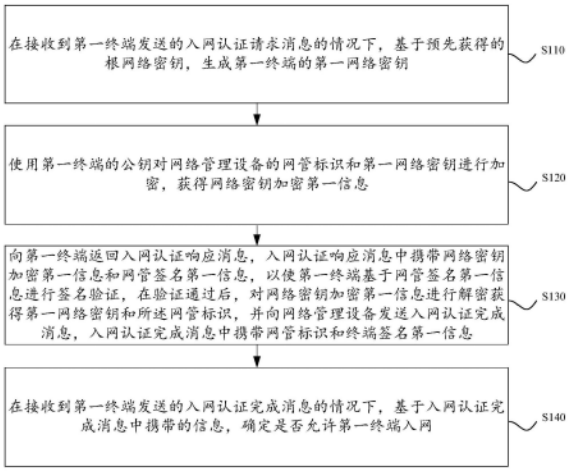
权利要求书2页 说明书13页 附图3页

(54)发明名称

多媒体会议终端入网认证方法、装置、设备及存储介质

(57)摘要

本公开涉及一种多媒体会议终端入网认证方法、装置、设备及存储介质，该方法应用于网络管理设备，该方法包括：在接收到第一终端发送的入网认证请求消息的情况下，基于根网络密钥，生成第一终端的第一网络密钥；向第一终端返回入网认证响应消息，入网认证响应消息中携带网络密钥加密第一信息和网管签名第一信息，以使第一终端获得第一网络密钥和网管标识，并向网络管理设备发送入网认证完成消息；在接收到第一终端发送的入网认证完成消息的情况下，基于入网认证完成消息中携带的信息，确定是否允许第一终端入网。实现了对终端入网的认证管控，使得只有认证通过的终端才能被允许入网，提高了多媒体会议的安全性。



CN 113727059 B

1.一种多媒体会议终端入网认证方法,其特征在于,应用于网络管理设备,所述方法包括:

在接收到第一终端发送的入网认证请求消息的情况下,基于预先获得的根网络密钥,生成所述第一终端的第一网络密钥;

使用所述第一终端的公钥对所述网络管理设备的网管标识和所述第一网络密钥进行加密,获得网络密钥加密第一信息;

向所述第一终端返回入网认证响应消息,所述入网认证响应消息中携带所述网络密钥加密第一信息和网管签名第一信息,以使所述第一终端基于所述网管签名第一信息进行签名验证,在验证通过后,对所述网络密钥加密第一信息进行解密获得所述第一网络密钥和所述网管标识,并向所述网络管理设备发送入网认证完成消息,所述入网认证完成消息中携带所述网管标识和终端签名第一信息;

在接收到所述第一终端发送的所述入网认证完成消息的情况下,基于所述入网认证完成消息中携带的信息,确定是否允许所述第一终端入网。

2.根据权利要求1所述的方法,其特征在于,所述入网认证请求消息中携带有证书相关信息,在接收到第一终端发送的入网认证请求消息的情况下,还包括:

如果所述证书相关信息中包括需要传递证书的标记信息,则在所述入网认证响应消息中携带所述网络管理设备的证书;

或者,如果所述证书相关信息中包括的网管证书序列号与所述网络管理设备的实际证书序列号不同,则在所述入网认证响应消息中携带所述网络管理设备的证书。

3.根据权利要求1所述的方法,其特征在于,所述入网认证请求消息中携带有安全交互机制版本的支持信息,在接收到第一终端发送的入网认证请求消息的情况下,还包括:

在所述入网认证响应消息中携带安全交互机制版本的应答信息,以使所述第一终端与所述网络管理设备基于相同的安全交互机制版本进行交互。

4.根据权利要求1所述的方法,其特征在于,所述入网认证请求消息中携带所述第一终端的随机数,所述入网认证响应消息中还携带所述第一终端的随机数和所述网络管理设备的随机数,所述入网认证完成消息中还携带所述第一终端的随机数和所述网络管理设备的随机数。

5.根据权利要求1所述的方法,其特征在于,所述网络管理设备预先获得广播密钥,所述入网认证响应消息中还携带使用所述第一终端的公钥对所述网管标识和所述广播密钥进行加密获得的广播密钥加密信息。

6.根据权利要求1所述的方法,其特征在于,在接收到第一终端发送的入网认证请求消息的情况下,在所述生成所述第一终端的第一网络密钥之前,还包括:

确定所述入网认证请求消息中是否携带有所述第一终端的证书;

如果没有携带,则确定所述网络管理设备的本地是否缓存有所述第一终端的证书;

如果缓存有,则确定本地缓存的所述第一终端的证书是否有效;

如果有效,则执行所述生成所述第一终端的第一网络密钥的步骤。

7.根据权利要求6所述的方法,其特征在于,在所述入网认证请求消息中没有携带所述第一终端的证书的情况下,还包括:

如果所述网络管理设备的本地没有缓存所述第一终端的证书,或者本地缓存的所述第

一终端的证书无效，则向所述第一终端返回错误消息，以使所述第一终端重新发送所述入网认证请求消息，并在所述入网认证请求消息中携带所述第一终端的证书。

8.根据权利要求6所述的方法，其特征在于，所述入网认证请求中携带有所述第一终端的证书序列号，所述确定本地缓存的所述第一终端的证书是否有效，包括：

如果本地缓存的所述第一终端的证书序列号与所述入网认证请求消息中携带的所述第一终端的证书序列号相同，且不存在所述第一终端的证书的撤销信息，则确定本地缓存的所述第一终端的证书有效，否则，无效。

9.根据权利要求1至8之中任一项所述的方法，其特征在于，在所述第一终端入网之后，还包括：

接收所述第一终端的快速入网认证请求消息，所述快速入网认证请求消息中携带所述第一终端的随机数；

使用所述第一网络密钥对响应相关信息进行加密，获得响应相关加密第一信息，所述响应相关信息包括所述第一终端的随机数和所述网络管理设备的随机数；

向所述第一终端返回快速入网认证响应消息，所述快速入网认证响应消息中携带所述响应相关加密第一信息，以使所述第一终端对所述响应相关加密第一信息进行解密后，返回快速入网认证完成消息，所述快速入网认证完成消息中携带所述第一终端的随机数和所述网络管理设备的随机数；

在接收到所述第一终端发送的所述快速入网认证完成消息的情况下，基于所述快速入网认证完成消息中携带的信息，确定是否允许所述第一终端入网。

10.一种多媒体会议终端入网认证装置，其特征在于，运行于网络管理设备，所述装置包括：

网络密钥生成模块，用于在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成所述第一终端的第一网络密钥；

加密信息获得模块，用于使用所述第一终端的公钥对所述网络管理设备的网管标识和所述第一网络密钥进行加密，获得网络密钥加密第一信息；

响应信息返回模块，用于向所述第一终端返回入网认证响应消息，所述入网认证响应消息中携带所述网络密钥加密第一信息和网管签名第一信息，以使所述第一终端基于所述网管签名第一信息进行签名验证，在验证通过后，对所述网络密钥加密第一信息进行解密获得所述第一网络密钥和所述网管标识，并向所述网络管理设备发送入网认证完成消息，所述入网认证完成消息中携带所述网管标识和终端签名第一信息；

入网判定模块，用于在接收到所述第一终端发送的所述入网认证完成消息的情况下，基于所述入网认证完成消息中携带的信息，确定是否允许所述第一终端入网。

11.一种多媒体会议终端入网认证设备，其特征在于，包括：

存储器，用于存储计算机程序；

处理器，用于执行所述计算机程序时实现如权利要求1至9任一项所述的多媒体会议终端入网认证方法的步骤。

12.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1至9任一项所述的多媒体会议终端入网认证方法的步骤。

多媒体会议终端入网认证方法、装置、设备及存储介质

技术领域

[0001] 本公开涉及计算机应用技术领域，特别是涉及一种多媒体会议终端入网认证方法、装置、设备及存储介质。

背景技术

[0002] 随着计算机技术和网络技术的快速发展，音视频等多媒体会议的应用范围越来越广泛。多媒体会议依赖于网络进行，具有高效率、低成本、快捷方便等特点。用户通过各种终端可以加入到多媒体会议中。

[0003] 但是，因为多媒体会议具有一定的私密性，如果任意终端都可以加入，则很可能会产生机密泄露等风险，安全性较低，所以并非所有终端都可以加入，只有预先设定的合法终端才可以加入。而入网是终端加入多媒体会议的前提，为了提高多媒体会议的安全性，如何对终端入网进行认证管控，是目前本领域技术人员急需解决的技术问题。

发明内容

[0004] 本公开的目的是提供一种多媒体会议终端入网认证方法、装置、设备及存储介质，以对多媒体会议中终端入网进行认证管控，提高多媒体会议的安全性。

[0005] 为解决上述技术问题，本公开提供如下技术方案：

[0006] 一种多媒体会议终端入网认证方法，应用于网络管理设备，所述方法包括：

[0007] 在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成所述第一终端的第一网络密钥；

[0008] 使用所述第一终端的公钥对所述网络管理设备的网管标识和所述第一网络密钥进行加密，获得网络密钥加密第一信息；

[0009] 向所述第一终端返回入网认证响应消息，所述入网认证响应消息中携带所述网络密钥加密第一信息和网管签名第一信息，以使所述第一终端基于所述网管签名第一信息进行签名验证，在验证通过后，对所述网络密钥加密第一信息进行解密获得所述第一网络密钥和所述网管标识，并向所述网络管理设备发送入网认证完成消息，所述入网认证完成消息中携带所述网管标识和终端签名第一信息；

[0010] 在接收到所述第一终端发送的所述入网认证完成消息的情况下，基于所述入网认证完成消息中携带的信息，确定是否允许所述第一终端入网。

[0011] 在本公开的一种具体实施方式中，所述入网认证请求消息中携带有证书相关信息，在接收到第一终端发送的入网认证请求消息的情况下，还包括：

[0012] 如果所述证书相关信息中包括需要传递证书的标记信息，则在所述入网认证响应消息中携带所述网络管理设备的证书；

[0013] 或者，如果所述证书相关信息中包括的网管证书序列号与所述网络管理设备的实际证书序列号不同，则在所述入网认证响应消息中携带所述网络管理设备的证书。

[0014] 在本公开的一种具体实施方式中，所述入网认证请求消息中携带有安全交互机制

版本的支持信息，在接收到第一终端发送的入网认证请求消息的情况下，还包括：

[0015] 在所述入网认证响应消息中携带安全交互机制版本的应答信息，以使所述第一终端与所述网络管理设备基于相同的安全交互机制版本进行交互。

[0016] 在本公开的一种具体实施方式中，所述入网认证请求消息中携带所述第一终端的随机数，所述入网认证响应消息中还携带所述第一终端的随机数和所述网络管理设备的随机数，所述入网认证完成消息中还携带所述第一终端的随机数和所述网络管理设备的随机数。

[0017] 在本公开的一种具体实施方式中，所述网络管理设备预先获得广播密钥，所述入网认证响应消息中还携带使用所述第一终端的公钥对所述网管标识和所述广播密钥进行加密获得的广播密钥加密信息。

[0018] 在本公开的一种具体实施方式中，在接收到第一终端发送的入网认证请求消息的情况下，在所述生成所述第一终端的第一网络密钥之前，还包括：

[0019] 确定所述入网认证请求消息中是否携带有所述第一终端的证书；

[0020] 如果没有携带，则确定所述网络管理设备的本地是否缓存有所述第一终端的证书；

[0021] 如果缓存有，则确定本地缓存的所述第一终端的证书是否有效；

[0022] 如果有效，则执行所述生成所述第一终端的第一网络密钥的步骤。

[0023] 在本公开的一种具体实施方式中，在所述入网认证请求消息中没有携带所述第一终端的证书的情况下，还包括：

[0024] 如果所述网络管理设备的本地没有缓存所述第一终端的证书，或者本地缓存的所述第一终端的证书无效，则向所述第一终端返回错误消息，以使所述第一终端重新发送所述入网认证请求消息，并在所述入网认证请求消息中携带所述第一终端的证书。

[0025] 在本公开的一种具体实施方式中，所述入网认证请求中携带有所述第一终端的证书序列号，所述确定本地缓存的所述第一终端的证书是否有效，包括：

[0026] 如果本地缓存的所述第一终端的证书序列号与所述入网认证请求消息中携带的所述第一终端的证书序列号相同，且不存在所述第一终端的证书的撤销信息，则确定本地缓存的所述第一终端的证书有效，否则，无效。

[0027] 在本公开的一种具体实施方式中，在所述第一终端入网之后，还包括：

[0028] 接收所述第一终端的快速入网认证请求消息，所述快速入网认证请求消息中携带所述第一终端的随机数；

[0029] 使用所述第一网络密钥对响应相关信息进行加密，获得响应相关加密第一信息，所述响应相关信息包括所述第一终端的随机数和所述网络管理设备的随机数；

[0030] 向所述第一终端返回快速入网认证响应消息，所述快速入网认证响应消息中携带所述响应相关加密第一信息，以使所述第一终端对所述响应相关加密第一信息进行解密后，返回快速入网认证完成消息，所述快速入网认证完成消息中携带所述第一终端的随机数和所述网络管理设备的随机数；

[0031] 在接收到所述第一终端发送的所述快速入网认证完成消息的情况下，基于所述快速入网完成消息中携带的信息，确定是否允许所述第一终端入网。

[0032] 一种多媒体会议终端入网认证装置，运行于网络管理设备，所述装置包括：

[0033] 网络密钥生成模块，用于在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成所述第一终端的第一网络密钥；

[0034] 加密信息获得模块，用于使用所述第一终端的公钥对所述网络管理设备的网管标识和所述第一网络密钥进行加密，获得网络密钥加密第一信息；

[0035] 响应信息返回模块，用于向所述第一终端返回入网认证响应消息，所述入网认证响应消息中携带所述网络密钥加密第一信息和网管签名第一信息，以使所述第一终端基于所述网管签名第一信息进行签名验证，在验证通过后，对所述网络密钥加密第一信息进行解密获得所述第一网络密钥和所述网管标识，并向所述网络管理设备发送入网认证完成消息，所述入网认证完成消息中携带所述网管标识和终端签名第一信息；

[0036] 入网判定模块，用于在接收到所述第一终端发送的所述入网认证完成消息的情况下，基于所述入网认证完成消息中携带的信息，确定是否允许所述第一终端入网。

[0037] 一种多媒体会议终端入网认证设备，包括：

[0038] 存储器，用于存储计算机程序；

[0039] 处理器，用于执行所述计算机程序时实现上述任一项所述多媒体会议终端入网认证方法的步骤。

[0040] 一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现上述任一项所述多媒体会议终端入网认证方法的步骤。

[0041] 应用本公开实施例所提供的技术方案，网络管理设备在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成第一终端的第一网络密钥，使用第一终端的公钥对网管标识和第一网络密钥进行加密，可以得到网络密钥加密第一信息，向第一终端返回的入网认证响应消息中可以携带网络密钥加密第一信息和网管签名第一信息，第一终端进行签名验证通过后，对网络密钥加密第一信息进行解密可以得到网管标识和第一网络密钥，可以向网络管理设备发送入网认证完成消息，网络管理设备可以基于入网认证完成消息中携带的信息，确定是否允许第一终端入网。实现了对终端入网的认证管控，使得只有认证通过的终端才能被允许入网，提高了多媒体会议的安全性。

附图说明

[0042] 附图是用来提供对本公开的进一步理解，并且构成说明书的一部分，与下面的具体实施方式一起用于解释本公开，但并不构成对本公开的限制。在附图中：

[0043] 图1为本公开实施例中一种多媒体会议终端入网认证方法的实施流程图；

[0044] 图2为本公开实施例中多媒体会议终端入网认证具体流程示意图；

[0045] 图3为本公开实施例中一种多媒体会议终端入网认证装置的结构示意图；

[0046] 图4为本公开实施例中一种多媒体会议终端入网认证设备的结构示意图。

具体实施方式

[0047] 本公开的核心是提供一种多媒体会议终端入网认证方法，该方法可以应用于网络管理设备，网络管理设备可以对涉及到多媒体会议的要入网的终端进行认证管控。网络管理设备可以预先获得根网络密钥。具体的，可以是网络管理设备自身生成根网络密钥，还可以由密钥管理设备进行密钥管理，网络管理设备在接入网络后，向密钥管理设备申请获得

根网络密钥，当然，还可以通过其他方式获得根网络密钥，本公开对此不做限制。为了保障密钥的安全性，网络管理设备在重启接入网络后均可获得根网络密钥，不同时刻获得的根网络密钥不同。

[0048] 网络管理设备对要入网的终端进行认证，只有认证通过才允许终端入网，以对入网终端进行认证管控，提高多媒体会议的安全性。

[0049] 为了使本技术领域的人员更好地理解本公开方案，下面结合附图和具体实施方式对本公开作进一步的详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本公开，并不用于限制本公开。基于本公开中的实施例，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，都属于本公开保护的范围。

[0050] 参见图1所示，为本公开实施例所提供的一种多媒体会议终端入网认证方法的实施流程图，该方法可以包括以下步骤：

[0051] S110：在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成第一终端的第一网络密钥。

[0052] 第一终端可以为要入网的任意一个终端，可以是实体终端，还可以为在实体设备上部署的虚拟终端。第一终端有入网需求时，可以向网络管理设备发出入网认证请求消息，入网认证请求消息中可以携带第一终端的标识。

[0053] 网络管理设备在接收到第一终端发送的入网认证请求消息后，可以基于根网络密钥，生成第一终端的第一网络密钥。具体的，可以通过密钥派生函数对根网络密钥进行作用，生成第一终端的第一网络密钥。

[0054] S120：使用第一终端的公钥对网络管理设备的网管标识和第一网络密钥进行加密，获得网络密钥加密第一信息。

[0055] 网络管理设备生成第一终端的第一网络密钥后，进一步可以使用第一终端的公钥对网络管理设备的网管标识和第一网络密钥进行加密，得到网络密钥加密第一信息。

[0056] 网络管理设备可以预先获得第一终端的公钥，网管标识为识别网络管理设备的唯一标识。网络密钥加密第一信息可以表示为$E_A(PK_A, ID_M||NK_A)$。其中，PK_A表示第一终端的公钥，ID_M表示网络管理设备的网管标识，NK_A表示第一网络密钥。

[0057] S130：向第一终端返回入网认证响应消息，入网认证响应消息中携带网络密钥加密第一信息和网管签名第一信息，以使第一终端基于网管签名第一信息进行签名验证，在验证通过后，对网络密钥加密第一信息进行解密获得第一网络密钥和网管标识，并向网络管理设备发送入网认证完成消息，入网认证完成消息中携带网管标识和终端签名第一信息。

[0058] 网络管理设备获得网络密钥加密第一信息后，可以向第一终端返回入网认证响应消息。在入网认证响应消息中携带网络密钥加密第一信息和网管签名第一信息，还可以携带在入网认证请求消息中获得的第一终端的标识。

[0059] 网络密钥加密第一信息即为使用第一终端的公钥对网络管理设备的网管标识和第一网络密钥进行加密获得的信息，网管签名第一信息可以是网络管理设备使用网管私钥对入网认证响应消息中携带的其他信息进行签名获得的信息。网管签名第一信息可以表示为$Sign(SK_M, ALL)$，其中，SK_M表示网管私钥，ALL表示入网认证响应消息中携带的其他信息。

[0060] 第一终端接收到网络管理设备返回的入网认证响应消息后，可以基于其中携带的

网管签名第一信息进行签名验证。具体的，可以将入网认证响应消息中携带的网管签名第一信息及其他信息传递给验证设备，验证设备基于验证规则得到验证结果，返回给第一终端，这样可以节约第一终端的资源开销。当然具体验证过程也可以在第一终端上完成。第一终端基于网管签名第一信息进行签名验证，如果验证通过，则可以对网络密钥加密第一信息进行解密获得第一网络密钥和网管标识。具体的，可以使用与第一终端的公钥对应的私钥对网络密钥加密第一信息进行解密，获得的第一网络密钥可以用于后续进行数据传输时加密使用。

[0061] 第一终端基于网管签名第一信息进行签名验证并通过后，可以向网络管理设备发送入网认证完成消息。在入网认证完成消息中可以携带网管标识和终端签名第一信息。终端签名第一信息可以是第一终端使用第一网络密钥对入网认证完成消息中携带的其他信息进行签名获得的信息。

[0062] S140：在接收到第一终端发送的入网认证完成消息的情况下，基于入网认证完成消息中携带的信息，确定是否允许第一终端入网。

[0063] 网络管理设备接收到第一终端发送的入网认证完成消息后，可以基于其中携带信息，确定是否允许第一终端入网。如可以通过其中携带的终端签名第一信息，进行签名验证。具体的，可以将入网认证完成消息中携带的终端签名第一信息及其他信息传递给验证设备，验证设备基于验证规则得到验证结果，返回给网络管理设备，这样可以节约网络管理设备的资源开销。当然具体验证过程也可以在网络管理设备上完成。

[0064] 网络管理设备基于入网认证完成消息中携带的终端签名第一信息，进行签名验证后，根据验证结果，可以确定是否允许第一终端入网。

[0065] 具体的，如果验证结果为验证通过，则可以确定允许第一终端入网，第一终端入网后，进一步可以执行浏览多媒体会议、加入多媒体会议等操作。如果验证结果为验证不通过，则可以确定不允许第一终端入网，可以向第一终端返回验证失败提示信息，第一终端可以重新发送入网认证请求消息，重复执行认证过程。

[0066] 应用本公开实施例所提供的方法，网络管理设备在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成第一终端的第一网络密钥，使用第一终端的公钥对网管标识和第一网络密钥进行加密，可以得到网络密钥加密第一信息，向第一终端返回的入网认证响应消息中可以携带网络密钥加密第一信息和网管签名第一信息，第一终端进行签名验证通过后，对网络密钥加密第一信息进行解密可以得到网管标识和第一网络密钥，可以向网络管理设备发送入网认证完成消息，网络管理设备可以基于入网认证完成消息中携带的信息，确定是否允许第一终端入网。实现了对终端入网的认证管控，使得只有认证通过的终端才能被允许入网，提高了多媒体会议的安全性。

[0067] 在本公开的一个实施例中，在接收到第一终端发送的入网认证请求消息的情况下，在生成第一终端的第一网络密钥之前，该方法还可以包括以下步骤：

[0068] 步骤一：确定入网认证请求消息中是否携带第一终端的证书，如果没有携带，则执行步骤二；

[0069] 步骤二：确定网络管理设备的本地是否缓存有第一终端的证书，如果缓存有，则执行步骤三；

[0070] 步骤三：确定本地缓存的第一终端的证书是否有效，如果有效，则执行生成第一终

端的第一网络密钥的步骤。

[0071] 为便于描述，将上述三个步骤结合起来进行说明。

[0072] 可以理解的是，证书数据量较大，在线传递将会消耗较多网络资源。在本公开实施例中，网络管理设备和终端在获得对端证书后，可以在本地保存。第一终端在请求入网时，发送的第一条入网认证请求消息中可以不携带证书。

[0073] 网络管理设备在接收到第一终端发送的入网认证请求消息后，可以先确定入网认证请求消息中是否携带有第一终端的证书，如果没有携带，则可以进一步确定网络管理设备的本地是否缓存有第一终端的证书。如果本地缓存有，则可以认为之前获得过第一终端的证书，但是证书是否有效还需要进一步确定，即可以再进一步确定本地缓存的第一终端的证书是否有效，如果证书有效，则可以执行生成第一终端的第一网络密钥及其以下步骤的操作。

[0074] 在本公开的一种具体实施方式中，入网认证请求中可以携带第一终端的证书序列号，在确定本地缓存的第一终端的证书是否有效时，可以将本地缓存的第一终端的证书序列号与入网认证请求消息中携带的第一终端的证书序列号进行比较，如果二者相同，则进一步可以确定是否存在第一终端的证书的撤销信息，如果不存在，则可以确定本地缓存的第一终端的证书有效。如果本地缓存的第一终端的证书序列号与入网认证请求消息中携带的第一终端的证书序列号不相同，或者存在第一终端的证书的撤销信息，则可以确定本地缓存的第一终端的证书无效。

[0075] 在本公开的另一种具体实施方式中，在入网认证请求消息中没有携带第一终端的证书的情况下，如果网络管理设备的本地没有缓存第一终端的证书，或者本地缓存的第一终端的证书无效，则可以向第一终端返回错误消息，在错误信息中指明需要第一终端传递签名证书、加密证书中的哪一个或者全部，以使第一终端重新发送入网认证请求消息，并在入网认证请求消息中携带第一终端的证书。在接收到第一终端重新发送的入网认证请求消息后，可以将其中携带的第一终端的证书在本地缓存，这样第一终端再有入网需求时，在入网认证请求消息中没有携带第一终端的证书，也可以基于本地缓存的第一终端的证书对第一终端进行认证。

[0076] 在本公开的一个实施例中，入网认证请求消息中携带有证书相关信息，在接收到第一终端发送的入网认证请求消息的情况下，还包括：

[0077] 如果证书相关信息中包括需要传递证书的标记信息，则在入网认证响应消息中携带网络管理设备的证书；

[0078] 或者，如果证书相关信息中包括的网管证书序列号与网络管理设备的实际证书序列号不同，则在入网认证响应消息中携带网络管理设备的证书。

[0079] 在本公开实施例中，入网认证请求消息中可以携带证书相关信息，该证书相关信息可以包括是否传递证书的标记信息、第一终端的证书序列号、网管证书序列号等。第一终端在有入网需求时，如果本地没有保存有网络管理设备的证书，则可以在入网认证请求消息中携带需要传递证书的标记信息，如果本地保存有网络管理设备的证书，则可以在入网认证请求消息中携带不需要传递证书的标记信息、本地保存的网管证书序列号、自身的证书序列号等证书相关信息。

[0080] 网络管理设备在接收到第一终端发送的入网认证请求消息的情况下，如果证书相

关信息中包括需要传递证书的标记信息，则可以认为第一终端要求网络管理设备传递证书，网络管理设备可以在向第一终端返回的入网认证响应消息中携带网络管理设备的证书。

[0081] 如果证书相关信息中包括的网管证书序列号与网络管理设备的实际证书序列号不同，则可以认为网络管理设备的证书有更新，网络管理设备可以在入网认证响应消息中携带网络管理设备的证书。

[0082] 当然，如果证书相关信息中包括不需要传递证书的标记信息，但是证书相关信息中包括的网管证书序列号与网络管理设备的实际证书序列号不同，也可以在入网认证响应消息中携带网络管理设备的证书。以使第一终端能够基于网络管理设备的证书对网络管理设备进行认证，确认入网认证响应消息的合法性。第一终端收到网络管理设备的证书后，可以在本地缓存该证书，这样可以减少之后对证书的传递，节约网络资源。

[0083] 在本公开的一个实施例中，入网认证请求消息中携带有安全交互机制版本的支持信息，在接收到第一终端发送的入网认证请求消息的情况下，还可以包括以下步骤：

[0084] 在入网认证响应消息中携带安全交互机制版本的应答信息，以使第一终端与网络管理设备基于相同的安全交互机制版本进行交互。

[0085] 在本公开实施例中，第一终端在有入网需求时，向网络管理设备发送的入网认证请求消息中可以携带安全交互机制版本的支持信息，即自身支持的安全交互机制版本，可能有一个或多个。

[0086] 网络管理设备接收到第一终端发送的入网认证请求消息后，可以基于其中携带的安全交互机制版本的支持信息，确定当前要使用的安全交互机制版本，并在入网认证响应消息中携带安全交互机制版本的应答信息，这样可以使得第一终端与网络管理设备基于相同的安全交互版本进行交互，以避免安全交互版本不同导致的入网认证管控出现误判等问题。

[0087] 举例而言，安全交互机制有更新，第一终端支持的安全交互机制版本有v1.0、v2.0，网络管理设备确定当前需要使用安全交互机制的版本为v2.0，其中入网认证响应消息中可以携带v2.0的应答信息，这样第一终端与网络管理设备将均基于v2.0的安全交互机制进行交互。

[0088] 在本公开的一个实施例中，入网认证请求消息中携带第一终端的随机数，入网认证响应消息中还携带第一终端的随机数和网络管理设备的随机数，入网认证完成消息中还携带第一终端的随机数和网络管理设备的随机数。

[0089] 第一终端在有入网需求时，可以调用密码模块生成一个随机数，在入网认证请求消息中携带该随机数，网络管理设备在接收到第一终端发送的入网认证请求消息后，可以得到第一终端的随机数，网络管理设备也可以调用密码模块生成一个随机数，然后在入网认证响应消息中携带第一终端的随机数和网络管理设备的随机数，第一终端接收到入网认证响应消息后，在向网络管理设备发送的入网认证完成消息中可以携带第一终端的随机数和网络管理设备的随机数。通过对随机数的传递可以加强相互认证的可靠性。第一终端和网络管理设备所能调用的密码模块不同，且在不同时刻调用密码模块生成的随机数不同。

[0090] 在本公开的一个实施例中，网络管理设备还可以预先获得广播密钥，入网认证响应消息中还携带使用第一终端的公钥对网管标识和广播密钥进行加密获得的广播密钥加

密信息。

[0091] 网络管理设备初次接入网络后，或者重启接入网络后，可以获得广播密钥。具体的，可以是网络管理设备本身自动生成广播密钥，还可以是向密钥管理设备申请获得广播密钥。不同时刻获得的广播密钥可以不同。

[0092] 网络管理设备接收到第一终端发送的入网认证请求消息时，可以使用第一终端的公钥对网管标识和广播密钥进行加密获得广播密钥加密信息，在向第一终端返回的入网认证响应消息中还携带广播密钥加密信息，这样第一终端使用私钥对广播密钥加密信息进行解密，可以得到广播密钥。方便后续使用广播密钥对广播信息进行加解密处理，以提高广播信息的传输安全性。

[0093] 为便于理解，以图2所示为例对本公开实施例的具体执行过程进行说明。

[0094] 假设第一终端为终端A，网络管理设备为网管M，密钥管理设备为密管。

[0095] S1：网管M在接入网络后，可以向密管申请根网络密钥NK-root、广播密钥BK；

[0096] S2：终端A向网管M发送入网认证请求消息，入网认证请求消息中可以携带辅助信息Info、终端A的标识ID_A和终端A的随机数R_A。可以约定，终端A发送的第一条入网认证请求消息不携带证书；其中，辅助信息Info可扩展，可以包括以下内容：终端侧支持的安全交互机制的版本、认证类型标识(1实体终端，2虚拟终端，3快速入网)、证书相关信息(是否传递证书，对端证书序列号，本端证书序列号)；终端A的随机数R_A可以是终端A调用密码模块生成的随机数；

[0097] S3：网管M接收到入网认证请求消息后，如果确定本地没有缓存终端A的证书$Cert_A$，或本地缓存的终端A的证书$Cert_A$无效，则向终端A返回错误信息；$Cert_A$为终端A的加密证书和/或签名证书；

[0098] S4：终端A接收到错误信息，重新发送入网认证请求消息，在入网认证请求消息中加入证书；

[0099] S5：网管M接收到入网认证请求消息，验证证书$Cert_A$的有效性，如果有效，则基于根网络密钥，生成终端A的网络密钥NK_A；

[0100] S6：网管M向终端A返回入网认证响应消息，入网认证响应消息中携带辅助信息Info、网管M的随机数R_M、终端A的随机数R_A、终端A的标识ID_A、使用终端A的加密公钥PK_A对网管标识ID_M和网络密钥NK_A的拼接结果进行加密得到的密文、使用终端A的加密公钥PK_A对网管标识ID_M和广播密钥BK的拼接结果进行加密得到的密文、网管M使用签名私钥SK_M对上述所有字段内容的签名值、网管M的证书$Cert_M$等，其中，$Cert_M$为网管M的签名证书和/或加密证书，可以基于接收到的入网认证请求消息中携带的Info确定是否传递该证书；

[0101] S7：终端A接收到入网认证响应消息后，验证签名，验证通过后，向网管M发送入网认证完成消息，入网认证完成消息中可以携带辅助信息Info、网管M的随机数R_M、终端A的随机数R_A、网管标识ID_M、终端A使用签名私钥SK_A对上述所有字段内容的签名值等；

[0102] S8：网管M接收到入网认证完成消息后，验证签名，确定是否允许终端A入网，完成身份认证的过程。

[0103] 需要说明的是，如果终端A为实体终端，则ID_A可以为该实体终端的唯一标识，如果终端A为首席虚拟终端，则ID_A可以为该首席虚拟终端所属实体设备的标识，如果终端A为非首席虚拟终端，则ID_A可以为该非首席虚拟终端的标识。在一个实体设备上可以部署多个虚

拟终端，第一个申请入网的虚拟终端为首席虚拟终端，后续申请入网的虚拟终端为非首席虚拟终端。

[0104] 本公开中网络管理设备对要入网的终端进行认证，只有认证通过才允许终端入网，可以对入网终端进行有效管控，提高多媒体会议的安全性。

[0105] 在本公开的一个实施例中，在第一终端入网之后，该方法还可以包括以下步骤：

[0106] 步骤一：接收第一终端的快速入网认证请求消息，快速入网认证请求消息中携带第一终端的随机数；

[0107] 步骤二：使用第一网络密钥对响应相关信息进行加密，获得响应相关加密第一信息，响应相关信息包括第一终端的随机数和网络管理设备的随机数；

[0108] 步骤三：向第一终端返回快速入网认证响应消息，快速入网认证响应消息中携带响应相关加密第一信息，以使第一终端对响应相关加密第一信息进行解密后，返回快速入网认证完成消息，快速入网认证完成消息中携带第一终端的随机数和网络管理设备的随机数；

[0109] 步骤四：在接收到第一终端发送的快速入网认证完成消息的情况下，基于快速入网完成消息中携带的信息，确定是否允许第一终端入网。

[0110] 为便于描述，将上述几个步骤结合起来进行说明。

[0111] 可以理解的是，第一终端入网之后，可能会因为网络等原因退出，如果还有入网需求，则第一终端会再次发起入网申请。在这种情况下，第一终端可以向网络管理设备发送快速入网认证请求消息，快速入网认证请求消息中可以携带第一终端的随机数，还可以携带第一终端的标识。该随机数可以是第一终端要重新入网时调用密码模块生成的随机数。不同时刻生成的随机数可以不同。

[0112] 网络管理设备接收到第一终端的快速入网认证请求消息后，可以使用第一网络密钥对响应相关信息进行加密，获得响应相关加密第一信息。第一网络密钥可以是网络管理设备基于预先获得的根网络密钥生成的，还可以是之前对第一终端进行入网认证时生成并保存的。响应相关信息可以包括第一终端的随机数和网络管理设备的随机数。

[0113] 网络管理设备获得响应相关加密第一信息后，可以向第一终端返回快速入网认证响应消息，快速入网认证响应消息中携带响应相关加密第一信息，这样第一终端可以使用之前认证时获得的第一网络密钥对响应相关加密第一信息进行解密，得到第一终端的随机数、网络管理设备的随机数等信息，通过随机数可以确定快速入网认证响应消息的真实性，对网络管理设备进行认证。在认证通过的情况下，第一终端可以返回快速入网认证完成消息，在快速入网认证完成消息中携带第一终端的随机数和网络管理设备的随机数，可以使用第一网络密钥对第一终端的随机数和网络管理设备的随机数进行加密处理后添加到快速入网认证完成消息中。

[0114] 网络管理设备在接收到第一终端发送的快速入网认证完成消息的情况下，可以基于快速入网认证完成消息中携带的信息，确定是否允许第一终端入网。如可以基于其中携带的第一终端的随机数和网络管理设备的随机数，进行身份认证，并根据认证结果，确定是否允许第一终端入网。

[0115] 当然，快速入网认证请求消息中还可以携带证书相关信息，如果证书相关信息中包括需要传递证书的标记信息，则网络管理设备在快速入网认证响应消息中携带网络管理

设备的证书，或者，如果证书相关信息中包括的网管证书序列号与网络管理设备的实际证书序列号不同，则在快速入网认证响应消息中携带网络管理设备的证书。第一终端接收到网络管理设备的证书后在本地保存。

[0116] 同时，快速入网认证响应消息中还可以携带证书相关信息，如果证书相关信息中包括需要传递证书的标记信息，则第一终端在快速入网认证完成消息中携带第一终端的证书，或者，如果证书相关信息中包括的终端证书序列号与第一终端的实际证书序列号不同，则第一终端在快速入网认证完成消息中携带第一终端的证书。网络管理设备接收到第一终端的证书后在本地保存。

[0117] 另外，快速入网认证请求消息中可以携带有安全交互机制版本的支持信息，网络管理设备在接收到第一终端发送的快速入网认证请求消息的情况下，还可以在快速入网认证响应消息中携带安全交互机制版本的应答信息，以使第一终端与网络管理设备基于相同的安全交互机制版本进行交互。

[0118] 仍以第一终端为终端A，网络管理设备为网管M为例，对快速入网认证过程进行说明。

[0119] 终端A向网管M发送快速入网认证请求消息，快速入网认证请求中携带辅助信息Info、终端A的标识ID_A和终端A的随机数R_A；

[0120] 网管M接收到快速入网认证请求消息后，向终端A返回快速入网认证响应消息，快速入网认证响应消息中携带辅助信息Info、使用网络密钥NK_A对网管M的随机数R_M、终端A的随机数R_A、终端A的标识ID_A的拼接结果进行加密得到的密文、网管M的证书$Cert_M$等；其中，网管M的证书$Cert_M$为可选，可根据实际情况确定是否传输；

[0121] 终端A接收到快速入网认证响应消息后，向网管M发送快速入网认证完成消息，快速入网认证完成消息可以携带辅助信息Info、使用网络密钥NK_A对网管M的随机数R_M、终端A的随机数R_A的拼接结果进行加密得到的密文、终端A的证书$Cert_A$等；其中，终端A的证书$Cert_A$为可选，可根据实际情况确定是否传输；

[0122] 网管M接收到快速入网认证完成消息后，如果接收到终端A的证书，则将证书缓存于本地指定路径，验证证书$Cert_A$的有效性。对数据进行解密后，通过随机数进行身份认证，确定是否允许终端A入网。

[0123] 本公开中，对于已进行过入网认证的终端执行快速入网认证过程，可以提高终端入网效率。

[0124] 相应于上面的方法实施例，本公开实施例还提供了一种多媒体会议终端入网认证装置，下文描述的多媒体会议终端入网认证装置与上文描述的多媒体会议终端入网认证方法可相互对应参照。

[0125] 参见图3所示，该装置300可以包括以下模块：

[0126] 网络密钥生成模块310，用于在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成第一终端的第一网络密钥；

[0127] 加密信息获得模块320，用于使用第一终端的公钥对网络管理设备的网管标识和第一网络密钥进行加密，获得网络密钥加密第一信息；

[0128] 响应信息返回模块330，用于向第一终端返回入网认证响应消息，入网认证响应消息中携带网络密钥加密第一信息和网管签名第一信息，以使第一终端基于网管签名第一信

息进行签名验证，在验证通过后，对网络密钥加密第一信息进行解密获得第一网络密钥和网管标识，并向网络管理设备发送入网认证完成消息，入网认证完成消息中携带网管标识和终端签名第一信息；

[0129] 入网判定模块350，用于在接收到第一终端发送的入网认证完成消息的情况下，基于入网认证完成消息中携带的信息，确定是否允许第一终端入网。

[0130] 应用本公开实施例所提供的装置，网络管理设备在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成第一终端的第一网络密钥，使用第一终端的公钥对网管标识和第一网络密钥进行加密，可以得到网络密钥加密第一信息，向第一终端返回的入网认证响应消息中可以携带网络密钥加密第一信息和网管签名第一信息，第一终端进行签名验证通过后，对网络密钥加密第一信息进行解密可以得到网管标识和第一网络密钥，可以向网络管理设备发送入网认证完成消息，网络管理设备可以基于入网认证完成消息中携带的信息，确定是否允许第一终端入网。实现了对终端入网的认证管控，使得只有认证通过的终端才能被允许入网，提高了多媒体会议的安全性。

[0131] 在本公开的一种具体实施方式中，入网认证请求消息中携带有证书相关信息，该装置还包括证书携带判定模块，用于：

[0132] 在接收到第一终端发送的入网认证请求消息的情况下，如果证书相关信息中包括需要传递证书的标记信息，则在入网认证响应消息中携带网络管理设备的证书；

[0133] 或者，如果证书相关信息中包括的网管证书序列号与网络管理设备的实际证书序列号不同，则在入网认证响应消息中携带网络管理设备的证书。

[0134] 在本公开的一种具体实施方式中，入网认证请求消息中携带有安全交互机制版本的支持信息，该装置还包括交互版本携带判定模块，用于：

[0135] 在接收到第一终端发送的入网认证请求消息的情况下，在入网认证响应消息中携带安全交互机制版本的应答信息，以使第一终端与网络管理设备基于相同的安全交互机制版本进行交互。

[0136] 在本公开的一种具体实施方式中，入网认证请求消息中携带第一终端的随机数，入网认证响应消息中还携带第一终端的随机数和网络管理设备的随机数，入网认证完成消息中还携带第一终端的随机数和网络管理设备的随机数。

[0137] 在本公开的一种具体实施方式中，网络管理设备预先获得广播密钥，入网认证响应消息中还携带使用第一终端的公钥对网管标识和广播密钥进行加密获得的广播密钥加密信息。

[0138] 在本公开的一种具体实施方式中，该装置还包括证书有效性判定模块，用于：

[0139] 在接收到第一终端发送的入网认证请求消息的情况下，在生成第一终端的第一网络密钥之前，确定入网认证请求消息中是否携带有第一终端的证书；

[0140] 如果没有携带，则确定网络管理设备的本地是否缓存有第一终端的证书；

[0141] 如果缓存有，则确定本地缓存的第一终端的证书是否有效；

[0142] 如果有效，则触发网络密钥生成模块310执行生成第一终端的第一网络密钥的步骤。

[0143] 在本公开的一种具体实施方式中，还包括错误信息返回模块，用于：

[0144] 在入网认证请求消息中没有携带第一终端的证书的情况下，如果网络管理设备的

本地没有缓存第一终端的证书，或者本地缓存的第一终端的证书无效，则向第一终端返回错误消息，以使第一终端重新发送入网认证请求消息，并在入网认证请求消息中携带第一终端的证书。

[0145] 在本公开的一种具体实施方式中，入网认证请求中携带有第一终端的证书序列号，证书有效性判定模块，用于：

[0146] 在本地缓存的第一终端的证书序列号与入网认证请求消息中携带的第一终端的证书序列号相同，且不存在第一终端的证书的撤销信息的情况下，确定本地缓存的第一终端的证书有效，否则，无效。

[0147] 在本公开的一种具体实施方式中，还包括快速入网认证模块，用于：

[0148] 在第一终端入网之后，接收第一终端的快速入网认证请求消息，快速入网认证请求消息中携带第一终端的随机数；

[0149] 使用第一网络密钥对响应相关信息进行加密，获得响应相关加密第一信息，响应相关信息包括第一终端的随机数和网络管理设备的随机数；

[0150] 向第一终端返回快速入网认证响应消息，快速入网认证响应消息中携带响应相关加密第一信息，以使第一终端对响应相关加密第一信息进行解密后，返回快速入网认证完成消息，快速入网认证完成消息中携带第一终端的随机数和网络管理设备的随机数；

[0151] 在接收到第一终端发送的快速入网认证完成消息的情况下，基于快速入网完成消息中携带的信息，确定是否允许第一终端入网。

[0152] 关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

[0153] 相应于上面的方法实施例，本公开实施例还提供了一种多媒体会议终端入网认证设备，包括：

[0154] 存储器，用于存储计算机程序；

[0155] 处理器，用于执行计算机程序时实现上述多媒体会议终端入网认证方法的步骤。

[0156] 参见图4所示，为根据一示例性实施例示出的一种多媒体会议终端入网认证设备400的框图。例如，多媒体会议终端入网认证设备400可以被提供为一服务器。参照图4，多媒体会议终端入网认证设备400包括处理器410，其数量可以为一个或多个，以及存储器420，用于存储可由处理器410执行的计算机程序。存储器420中存储的计算机程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理器410可以被配置为执行该计算机程序，以执行上述的多媒体会议终端入网认证方法。

[0157] 另外，多媒体会议终端入网认证设备400还可以包括电源组件430和通信组件440，该电源组件430可以被配置为执行多媒体会议终端入网认证设备400的电源管理，该通信组件440可以被配置为实现多媒体会议终端入网认证设备400的通信，例如，有线或无线通信。此外，该多媒体会议终端入网认证设备400还可以包括输入/输出(I/O)接口450。多媒体会议终端入网认证设备400可以操作基于存储在存储器420的操作系统，例如Windows ServerTM，Mac OS XTM，UnixTM，LinuxTM等等。

[0158] 在另一示例性实施例中，还提供了一种包括程序指令的计算机可读存储介质，该程序指令被处理器执行时实现上述的多媒体会议终端入网认证方法的步骤。例如，该计算机可读存储介质可以为上述包括程序指令的存储器420，上述程序指令可由多媒体会议终

端入网认证设备400的处理器410执行以完成上述的多媒体会议终端入网认证方法。

[0159] 以上结合附图详细描述了本公开的优选实施方式，但是，本公开并不限于上述实施方式中的具体细节，在本公开的技术构思范围内，可以对本公开的技术方案进行多种简单变型，这些简单变型均属于本公开的保护范围。例如，可以将消息中携带的信息改变为单独传输的信息。

[0160] 另外需要说明的是，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，可以通过任何合适的方式进行组合，例如入网认证请求消息中同时携带第一终端的标识、随机数等信息。为了避免不必要的重复，本公开对各种可能的组合方式不再另行说明。

[0161] 此外，本公开的各种不同的实施方式之间也可以进行任意组合，只要其不违背本公开的思想，其同样应当视为本公开所公开的内容。

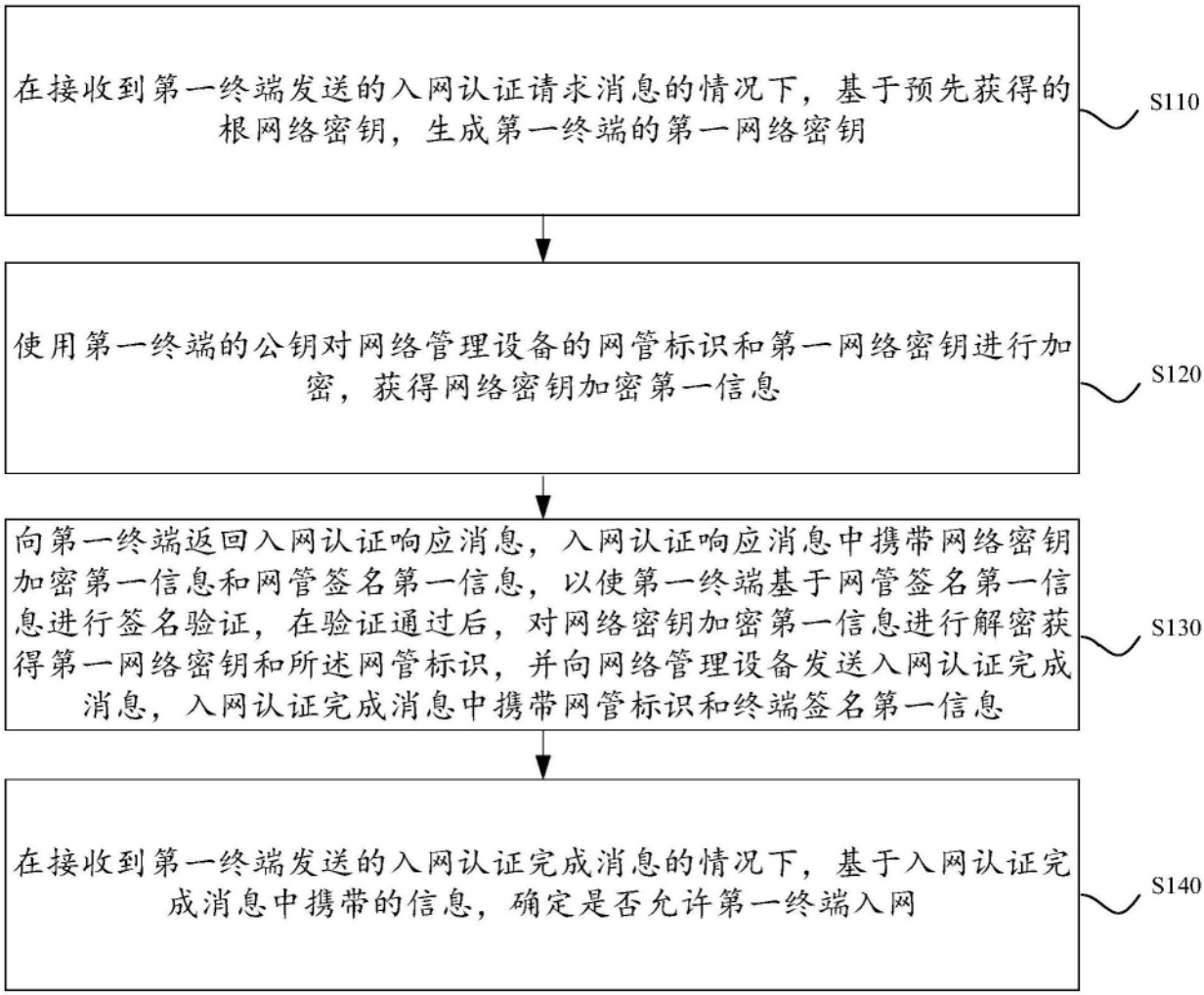

在接收到第一终端发送的入网认证请求消息的情况下，基于预先获得的根网络密钥，生成第一终端的第一网络密钥
S110
使用第一终端的公钥对网络管理设备的网管标识和第一网络密钥进行加密，获得网络密钥加密第一信息
S120
向第一终端返回入网认证响应消息，入网认证响应消息中携带网络密钥加密第一信息和网管签名第一信息，以使第一终端基于网管签名第一信息进行签名验证，在验证通过后，对网络密钥加密第一信息进行解密获得第一网络密钥和所述网管标识，并向网络管理设备发送入网认证完成消息，入网认证完成消息中携带网管标识和终端签名第一信息
S130
在接收到第一终端发送的入网认证完成消息的情况下，基于入网认证完成消息中携带的信息，确定是否允许第一终端入网
S140

图1

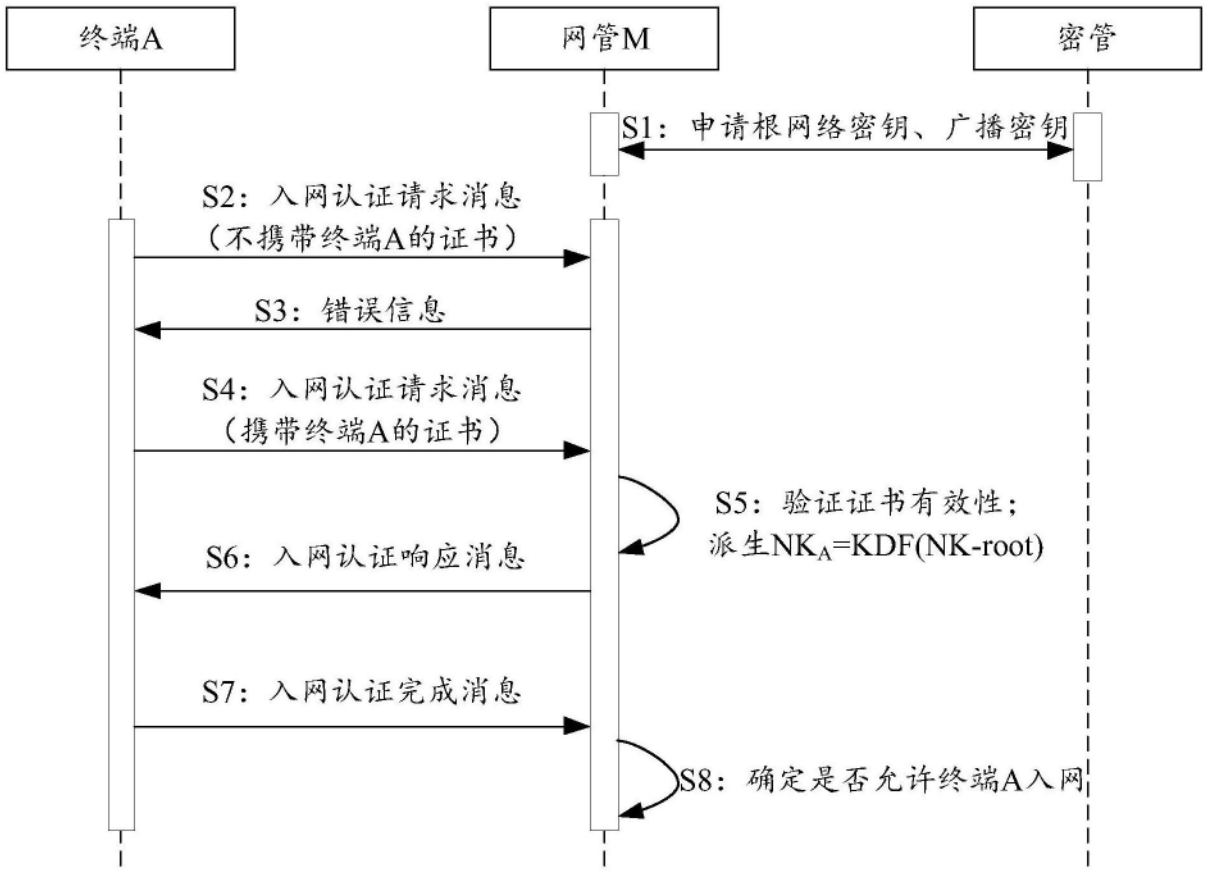

终端A
网管M
密管
S1：申请根网络密钥、广播密钥
S2：入网认证请求消息
（不携带终端A的证书）
S3：错误信息
S4：入网认证请求消息
（携带终端A的证书）
S5：验证证书有效性；
派生NKA=KDF(NK-root)
S6：入网认证响应消息
S7：入网认证完成消息
S8：确定是否允许终端A入网

图2

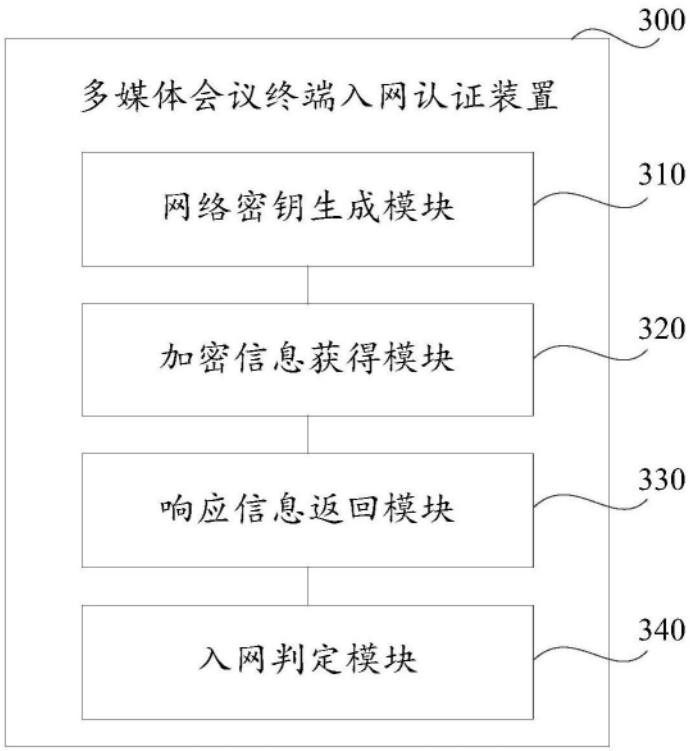

300
多媒体会议终端入网认证装置
网络密钥生成模块
310
加密信息获得模块
320
响应信息返回模块
330
入网判定模块
340

图3

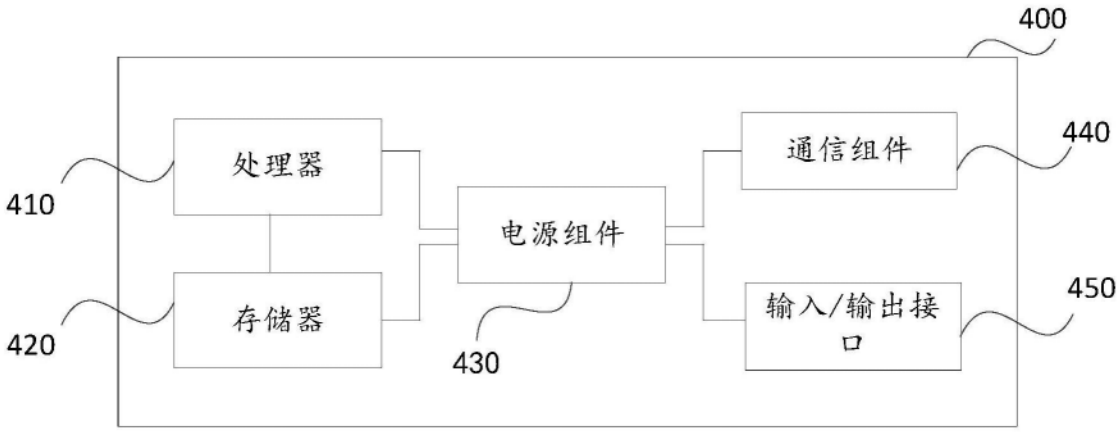

400
处理器
410
存储器
420
电源组件
430
通信组件
440
输入/输出接口
450

图4