

接入控制方法及通信设备

相关申请的交叉引用

本申请主张在 2020 年 3 月 20 日在中国提交的中国专利申请号 No.202010203175.8 的优先权，其全部内容通过引用包含于此。

技术领域

本发明涉及无线通信技术领域，尤其涉及一种接入控制方法及通信设备。

背景技术

在一些通信场景中，存在通信设备没有网络的证书却接入网络的场景，例如：终端在出厂时，尚无独立组网的非公共网络（Standalone Non-Public Network, SNPN）的证书（credential），从而无法通过 SNPN 的认证。在没有通过网络认证之前，目前无法获取通信设备的认证相关的信息。

发明内容

本发明实施例提供一种接入控制方法及通信设备，以解决无法获取通信设备的认证相关的信息的问题。

第一方面，本发明实施例提供一种接入控制方法，应用于第一通信设备，包括：

向第一目标端发送第一信息和/或第一指示信息，其中，所述第一信息包括如下至少一项：

第二认证服务器的索引信息，

所述第一通信设备的厂家的相关信息，

所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。

第二方面，本发明实施例提供一种接入控制方法，应用于第二通信设备，包括：

获取第一信息、第一指示信息、合法设备列表和第三信息中的至少一项；

根据所述第一信息、第一指示信息、合法设备列表和第三信息中的至少一项，执行第一操作；

其中，所述第一信息包括如下至少一项：第二认证服务器的索引信息，第一通信设备的厂家的相关信息，所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务；

所述第三信息包括以下至少一项：

所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

第三方面，本发明实施例提供一种接入控制方法，应用于第三通信设备，包括：

确定第三信息；

发送第三信息；

其中，所述第三信息包括如下至少一项：

第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

第四方面，本发明实施例提供一种接入控制方法，应用于第四通信设备，包括：

获取第二信息；

根据所述第二信息，执行第二操作；

其中，所述第二信息包括如下至少一项：

第一终端路由选择策略；

默认DNN信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

第五方面，本发明实施例提供一种接入控制方法，应用于第五通信设备，包括：

发送第二信息，其中，所述第二信息包括如下至少一项：

第一终端路由选择策略；

默认 DNN 信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

第六方面，本发明实施例提供一种通信设备，所述通信设备为第一通信设备，包括：

第一发送模块，用于向第一目标端发送第一信息和/或第一指示信息，其中，所述第一信息包括如下至少一项：

第二认证服务器的索引信息，

所述第一通信设备的厂家的相关信息，

所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。

第七方面，本发明实施例提供一种通信设备，所述通信设备为第二通信设备，包括：

获取模块，用于获取第一信息、第一指示信息和第三信息中的至少一项；

执行模块，用于根据所述第一信息、第一指示信息和第三信息中的至少一项，执行第一操作；

其中，所述第一信息包括如下至少一项：第二认证服务器的索引信息，第一通信设备的厂家的相关信息，所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务；

所述第三信息包括以下至少一项：

所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

第八方面，本发明实施例提供一种通信设备，所述通信设备为第三通信设备，包括：

发送模块，用于发送第三信息；

其中，所述第三信息包括如下至少一项：

第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

第九方面，本发明实施例提供一种通信设备，所述通信设备为第四通信设备，包括：

获取模块，用于获取第二信息；

执行模块，用于根据所述第二信息，执行第二操作；

其中，所述第二信息包括如下至少一项：

用于第一数据通道建立的相关信息；

第二指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互；

所述第一数据通道用于第一通信设备请求与第一网络相关的证书；

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书。

第十方面，本发明实施例提供一种通信设备，所述通信设备为第五通信设备，包括：

发送模块，用于发送第二信息，其中，所述第二信息包括如下至少一项：

用于第一数据通道建立的相关信息；

第二指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互；

所述第一数据通道用于第一通信设备请求与第一网络相关的证书；

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书。

第十一方面，本发明实施例提供一种通信设备，包括处理器、存储器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现第一方面提供的接入控制方法的步骤，或者，实现第二方面提供的接入控制方法的步骤，或者，实现第三方面提供的接入控制方法的步骤，或者，实现第四方面提供的接入控制方法的步骤，或者，实现第五方面提供的接入控制方法的步骤。

第十二方面，本发明实施例提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被所述处理器执行时实现第一方面提供的接入控制方法的步骤，或者，实现第二方面提供的接入控制方法的步骤，或者，实现第三方面提供的接入控制方法的步骤，或者，实现第四方面提供的接入控制方法的步骤，或者，实现第五方面提供的接入控制方法的步骤。

本发明实施例中，向第一目标端发送第一信息和/或第一指示信息，其中，所述第一信息包括如下至少一项：第二认证服务器的索引信息，所述第一通信设备的厂家的相关信息，所述第二认证服务器的地址相关信息；所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。这样可以支持获取到通信设备的认证相关的信息，进一步可以支持在通信设备未获取网络相关的证书情况下时，对通信设备进行认证和配置。具体地，使第一网络能够选取第二认证服务器对第一通信设备进行认证，从而支持终端无与第一网络相关证书的情况下接入第一网络时，对终端进行认证，避免仿冒和不合法终端对第一网络的安全攻击；另一方面支持对第一通信设备进行配置，以支持合法的终端获取与第一网络相关的证书。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 为本发明实施例提供的一种无线通信系统的架构示意图；

图 2 为本发明实施例提供的一种接入控制方法的流程图；

图 3 为本发明实施例提供的另一种接入控制方法的流程图；

图 4 为本发明实施例提供的另一种接入控制方法的流程图；

图 5 为本发明实施例提供的另一种接入控制方法的流程图；

图 6 为本发明实施例提供的另一种接入控制方法的流程图；

图 7 为本发明实施例提供的一种接入控制方法的示意图；

图 8 为本发明实施例提供的另一种接入控制方法的示意图；

图 9 为本发明实施例提供的另一种接入控制方法的示意图；

图 10 为本发明实施例提供的另一种接入控制方法的示意图；

图 11 为本发明提供的一种通信设备的结构图；

图 12 为本发明提供的另一种通信设备的结构图；

图 13 为本发明提供的另一种通信设备的结构图；

图 14 为本发明提供的另一种通信设备的结构图；

图 15 为本发明提供的另一种通信设备的结构图；

图 16 为本发明提供的另一种通信设备的结构图。

具体实施方式

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作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。

本申请的说明书和权利要求书中的术语“包括”以及它的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。此外，说明书以及权利要求中使用“和/或”表示所连接对象的至少其中之一，例如A和/或B，表示包含单独A，单独B，以及A和B都存在三种情况。

在本发明实施例中，“示例性的”或者“例如”等词用于表示作例子、例证

或说明。本发明实施例中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念。

本申请的说明书和权利要求书中的术语“包括”以及它的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。此外，说明书以及权利要求中使用“和/或”表示所连接对象的至少其中之一，例如A和/或B，表示包含单独A，单独B，以及A和B都存在三种情况。

下面结合附图介绍本发明的实施例。本发明实施例提供的信息控制方法及通信设备可以应用于无线通信系统中。该无线通信系统可以为 5G 系统，或者演进型长期演进（Evolved Long Term Evolution, eLTE）系统，或者后续演进通信系统。

下面结合附图介绍本发明的实施例。本发明实施例提供的接入控制方法及通信设备可以应用于图1所示的网络系统，如图1所示的该网络系统包括：终端（UE）、第一网络和第一网络之外的设备，如厂家设备等。

其中，终端可以接入第一网络，如 SNPN（非公共网络），SNPN 中可以是一种 5G 通信网络，比如包括 5G 无线接入网（NG-RAN）、接入和移动管理功能（Access and Mobility Management Function, AMF）、会话管理功能（Session Management Function, SMF）和用户平面功能（User Plane Function, UPF）等。

上述厂家设备可以是终端的厂家（vendor，也可称作提供商）的相关设备，例如：vendor 服务器、应用功能（Application function, AF）和验证、授权和记账（Authentication、Authorization、Accounting, AAA）服务器。

上述厂家设备可以对终端进行认证，或者 SNPN 通过厂家设备的信息对终端进行认证。

需要说明的是，图 1 所示的网络系统中仅是本发明实施例提供的接入控制方法及通信设备可应用的一个举例说明，本发明实施例对此不作限定，例如：上述网络系统还可以包括：

统一数据管理 (Unified Data Management, UDM)、网络开放功能 (network exposure function, NEF) 和配置服务器 (Config server)。

另外, 还可以应用于 4G、6G 等通信系统。

本发明实施例提供的接入控制方法还可以解决如下技术问题:

问题 1, 需要解决在 UE 没有与第一网络相关的证书接入第一网络时, 如何选择认证服务器的问题。

场景 1: 第一网络 (如 SNPN) 的终端 UE 出厂时, 还没有 SNPN 的证书 (如 credential), 无法通过 SNPN 的认证。一种思路是 UE 先初始接入 SNPN, SNPN 为 UE 配置证书 UE 再根据新配置的证书接入 SNPN。

在 UE 没有 SNPN 的证书初始接入 SNPN 的过程中, 由于 SNPN 无法验证 UE, 就只能允许所有请求接入的 UE, 比如建立用户面 PDU 会话到证书的配置服务器等。由于无 SNPN 内的认证机制, 要依赖证书的配置服务器再去触发对 UE 的认证。认证失败后, 再释放 UE 连接, PDU 会话资源等。

这样的无认证先分配资源的方式, 一方面存在攻击的隐患, 即 SNPN 的不合法的 UE 都发起初始接入, 耗费光 SNPN 的资源; 另一方面, 仿冒 UE 可能会冒充合法 UE 接入。

因此, 在 UE 没有 SNPN 的证书初始接入 SNPN 的过程中, 也需要对 UE 进行认证。一种可行的方法是通过 UE 的出厂的厂家的认证服务器进行认证。UE 的厂家在 UE 出厂时可以为 UE 配置能够让厂家的认证服务器可以认证的证书。SNPN 和厂家的服务器间可以开放接口, 实现 UE 接入 SNPN 后, 通过 UE 与厂家的认证服务器的认证, 实现 UE 与 SNPN 之间相互认证。由于 SNPN 的 UE 的厂家可能有多个, 因此存在多个厂家的认证服务器。因此, 需要解决在 UE 没有与第一网络相关的证书接入第一网络时, 如何选择认证服务器的问题。

场景二: 另外, 国际移动设备识别码 (International Mobile Equipment Identity, IMEI) 或永久设备标识符 (Permanent Equipment Identifier, PEI) 中包含了跟踪区域码 (Tracking area cod, TAC) 信息可以用于标识厂家。但一个厂家的 TAC 只能覆盖几百个终端。用 TAC 标识厂家需要不断地同步给 SNPN, 造成维护的复杂度。因此, 需要解决如何高效地选择厂家的认证服务

器的问题。

一种可选的方法是，由厂家相关设备与第一网络开放接口，向第一网络提供认证服务器的地址信息与认证服务器索引信息间的映射信息。当无第一网络相关证书的 UE 接入第一网络时，UE 提供认证服务器的索引信息。由第一网络根据 UE 提供的认证服务器的索引信息与厂家提供的第一网络提供认证服务器的地址信息与认证服务器索引信息间的映射信息，确认认证服务器的地址，向所述认证服务器发起对 UE 的认证请求。所述认证服务器可以为 UE 的厂家的相关信息。

另一种可选的方法是，由厂家相关设备与第一网络间相互认证，获得可信的认证服务器的地址相关信息。当无第一网络相关证书的 UE 接入第一网络时，UE 提供认证服务器的地址相关信息。由第一网络根据 UE 提供的认证服务器的地址相关信息与外部提供的认证服务器的地址相关信息，确认认证服务器的地址相关信息可信，向所述认证服务器发起对 UE 的认证请求。

场景 3：当第一网络的终端只有一个厂家时，只有一个厂家的认证服务器。当尚无与第一网络相关的证书的终端接入第一网络时，第一网络不能区分终端是为了其他受限服务接入（如紧急业务）的终端，还是为了配置与第一网络相关的证书才接入第一网络的终端。对后者，才需要通过厂家的认证服务器对终端进行认证。因此，需要解决是否通过外部认证服务器对终端进行认证的问题。

一种可选的方法是 UE 接入第一网络时，发送第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。根据所述第一指示信息，第一网络可以确定是否通过外部认证服务器（如终端厂家的认证服务器）对终端进行认证。

问题 2：需要解决 UE 如何获取证书配置服务器的地址相关信息的问题。

第一网络(如 SNPN)的终端 UE 出厂时，还没有与第一网络相关的证书，也没有所述证书的配置服务器的相关信息。

一种可选的方法是 UE 的厂家为 UE 配置所述配置服务器的地址相关信息或者索引信息。所述配置服务器与第一网络是意义对应的，还需要额外配置第一网络的信息。

另一种可选的方法是 UE 接入第一网络，认证通过后，由第一网络向 UE 提供所述配置服务器的地址相关信息或者索引信息。由于 UE 认证通过，此时 UE 与第一网络间相互信任。不难理解，此时提供的配置服务器的地址相关信息是可信的。

问题 3，认证服务器对 UE 认证通过后，可以证明 UE 的身份，而非仿冒的 UE。但如何确认 UE 是否为第一网络的合法 UE，是否允许为 UE 配置与第一网络相关的证书的问题还需要解决。

一种可选的方法是，认证服务器对 UE 认证通过表示 UE 是第一网络的合法 UE。即认证服务器但认证 UE 是 UE 而且认证 UE 是第一网络的合法 UE

另一种可选的方法是，认证服务器对 UE 认证通过后，由第一网络确认 UE 是第一网络的合法 UE。

问题 4，UE 请求配置服务器为其配置与第一网络相关的证书，配置服务器也需要确认 UE 是第一网络的合法 UE 或者确认 UE 允许被配置与第一网络相关的证书，才会对 UE 进行证书配置。

一种可选的方法是 UE 与认证服务器间经过配置服务器，实现相互认证。可以通过开放配置服务器和认证服务器的接口，实现 UE-配置服务器-认证服务器之间相互认证。由于 SNPN 的 UE 的厂家可能有多个，因此存在多个厂家的认证服务器。因此，需要解决在 UE 没有与第一网络相关的证书请求配置服务器为其配置与第一网络相关的证书时，如何选择认证服务器的问题。该问题类比问题 1

另一种可选的方法是，配置服务器依赖第一网络对 UE 的合法认证，只要是 UE 通过 SNPN 能接入配置服务器，则认为 UE 合法。第一网络对 UE 的合法认证同问题 3。

问题 5，第一网络（如 SNPN）的终端 UE 出厂时，还没有与第一网络相关的证书，也没有在第一网络下请求 PDU 会话建立的相关参数的配置，比如：NSSAI，SSC Mode，DNN 等。需要解决 UE 发起第一 PDU 会话建立请求所需要的信息获取的问题，所述第一 PDU 会话用于请求配置与第一网络相关的证书。

一种可选的方法是，为配置服务器的地址配置终端路由选择策略。并且

只允许 UE 访问所述配置服务器。

本发明一种可选实施例中，第一网络包括 SNPN。

本发明一种可选实施例中，证书 (credential) 可以也可以称为安全信息，包括可以用于认证和/或加密的参数等，如根密钥。所述根密钥可以用于导出 CK, IK。

本发明一种可选实施例中，与第一网络相关的证书可以包括用于接入第一网络的证书。所述用于接入第一网络的证书可以包括能够被第一网络的认证服务器直接认证的证书，或间接认证的证书。通过第一网络之外的认证服务器认证可以理解为间接认证。不难理解，此时，配置服务器可以为 UE 配置能够被第一网络直接认证的证书或配置能够被第一网络直接认证的证书。

本发明一种可选实施例中，与第一网络相关的证书可以包括以下至少一项：与第一网络直接相关的证书，用于接入第一网络正常服务的证书，能够被第一网络的认证服务器直接认证的证书，接入第一网络非受限服务的证书。不难理解，此时，配置服务器可以为 UE 配置能够被第一网络直接认证的证书。

本发明另一种可选实施例中，与第一网络无关的证书可以包括以下至少一项：与第一网络非直接相关的证书。与第一网络非直接相关的证书可以包括不能够通过第一网络的认证服务器直接认证的证书。通过第一网络之外的认证服务器认证的证书可以理解为与第一网络无关或无直接相关的证书。

本发明一种可选实施例中，第二证书可以包括以下至少一项：

与第一网络无关的证书，

当终端不具有与第一网络相关的证书的情况下用于接入第一网络的证书，

当终端为请求配置与第一网络相关的证书的情况下用于接入第一网络的证书，

接入第一网络的受限服务的证书，

第一通信设备厂家为第一通信设备配置的证书，

能够被第二认证服务器认证的证书。

本发明一种可选实施例中，所述受限服务包括以下至少一项：仅允许控制面，不允许用户面，仅允许访问第一服务器（可以包括配置服务器），仅

允许证书下载应用。一种实施方式中，通过控制面为终端配置与第一网络相关的证书。因此可以限制终端接入第一网络仅允许控制面。另一种实施方式中，通过用户面为终端配置与第一网络相关的证书。因此不难理解，所述受限服务可以仅终端允许访问第一服务器。仅允许访问第一服务器包括：终端在第一网络建立的数据通道仅用于访问第一服务器。

本发明一种可选实施例中，所述第一服务器包括配置服务器。所述第一服务器能够处理为终端配置与第一网络相关的证书的请求。所述配置服务器能够为通信设备配置与第一网络相关的证书。第一服务器可以是归属第一网络的服务器。

本发明一种可选实施例中，所述第一服务器为终端配置与第一网络相关的证书的请求时，可以向第二认证服务器请求验证终端，此处，第一服务器为认证的中间服务器。

本发明一种可选实施例中，初始认证包括当终端不具有与第一网络相关的证书接入第一网络的情况下，第一网络对终端进行的认证。不难理解，初始认证属于间接认证。

本发明一种可选实施例中，所述配置服务器也称为第一服务器。

本发明一种可选实施例中，与第一网络相关的证书，与第一网络相关证书第一网络相关证书可以混用，代表同一个意思。

本发明一种可选实施例中，厂家的相关信息可以简称为厂家信息或厂家的信息。所述厂家的相关信息包括：厂家标识信息（如 Vendor ID，或 TAC）。

本发明一种本发明实施例中，服务器的地址相关信息可以包括如下至少一项：IP地址，MAC地址，端口号，全限定域名（Fully Qualified Domain Name，FQDN），统一资源定位符（Uniform Resource Locator，URL），操作系统标识信息、应用标识信息。认证服务器的地址相关信息，或第一服务器的地址相关信息同所述服务器地址相关信息。

本发明一种本发明实施例中，除非特指说明（如第一网络的认证服务器），所述认证服务器为第二认证服务器的简称。所述第二认证服务器包括终端厂家的认证服务器，

本发明实施例中，可选的，获取可以理解为生成、从配置获得、接收、

通过请求后接收、通过自学习获取、根据未收到的信息推导获取或者是根据接收的信息处理后获得，具体可根据实际需要确定，本发明实施例对此不作限定。比如当未收到设备发送的某个能力指示信息时可推导出该设备不支持该能力。

可选的，发送可以包含广播，系统消息中广播，响应请求后返回。

可选的，预配置的可以称为默认的。

在本发明一种可选实施例中，数据通道可以包括但不限于以下之一：PDU会话，PDN连接，QoS流，承载，互联网安全协议（Internet Protocol Security, IPsec）通道，其中，承载可以是演进的无线接入承载（Evolved Radio Access Bearer, E-RAB）、无线接入承载（Evolved Radio Access Bearer, RAB）、数据无线承载（Data Radio Bearer, DRB）、信令无线承载（signalling radio bearers, SRB）等。

本发明一种可选实施例中，通信设备可以包括以下至少一项：通信网元和终端。

本发明一种实施例中，通信网元可以包括以下至少一项：核心网网元和无线接入网网元。

本发明实施例中，核心网网元（CN网元）可以包括但不限于如下至少一项：核心网设备、核心网节点、核心网功能、核心网网元、移动管理实体（Mobility Management Entity, MME）、接入移动管理功能（Access Management Function, AMF）、会话管理功能（Session Management Function, SMF）、用户平面功能（User Plane Function, UPF）、服务网关（serving GW, SGW）、PDN网关（PDN Gate Way, PDN网关）、策略控制功能（Policy Control Function、PCF）、策略与计费规则功能单元（Policy and Charging Rules Function, PCRF）、GPRS服务支持节点（Serving GPRS Support Node, SGSN）、网关GPRS支持节点（Gateway GPRS Support Node, GGSN）、统一数据管理（Unified Data Management, UDM）、统一数据仓储（Unified Data Repository, UDR）、归属用户服务器（Home Subscriber Server, HSS）、应用功能（Application Function, AF）、集中式网络配置（Centralized network configuration, CNC）。

本发明实施例中，无线接入网（Radio Access Network, RAN）网元可以

包括但不限于至少以下之一：无线接入网设备、无线接入网节点、无线接入网功能、无线接入网单元、第三代合作伙伴计划（Third Generation Partnership Project, 3GPP）无线接入网、非 3GPP 无线接入网、集中单元（Centralized Unit, CU）、分布式单元（Distributed Unit, DU）、基站、演进型基站（evolved Node B, eNB）、5G 基站（gNB）、无线网络控制器（Radio Network Controller, RNC）、基站（NodeB）、非 3GPP 互操作功能（Non-3GPP Inter Working Function, N3IWF）、接入控制（Access Controller, AC）节点、接入点（Access Point, AP）设备或无线局域网（Wireless Local Area Networks, WLAN）节点、N3IWF。

基站，可以是全球移动通信系统（Global System for Mobile Communications, GSM）或码分多址（Code Division Multiple Access, CDMA）中的基站（Base Transceiver Station, BTS），也可以是宽带码分多址（Wideband Code Division Multiple Access, WCDMA）中的基站（NodeB），还可以是 LTE 中的演进型基站（evolutional Node B, eNB 或 e-NodeB）及 5G 基站（gNB），本发明实施例并不限定。

本发明实施例中，UE 即终端。终端可以包括支持终端功能的中继和/或支持中继功能的终端。终端也可以称作终端设备或者用户终端（User Equipment, UE），终端可以是手机、平板电脑（Tablet Personal Computer）、膝上型电脑（Laptop Computer）、个人数字助理（Personal Digital Assistant, PDA）、移动上网装置（Mobile Internet Device, MID）、可穿戴式设备（Wearable Device）或车载设备等终端侧设备，需要说明的是，在本发明实施例中并不限定终端的具体类型。

本发明实施例提供的方法及通信设备可以应用于无线通信系统中。该无线通信系统可以为第五代移动通信（Fifth-generation, 5G）系统，或者演进的分组系统（Evolved Packet System, EPS），或者后续演进通信系统。本发明实施例无线通信网络可以为第五代移动通信网络（Fifth-generation system, 5GS）或 LTE 网络。

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作出创

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。

请参考图 2，本发明实施例提供了一种接入控制的方法，应用于第一通信设备。第一通信设备包括但不限于以下之一：终端（UE）、第一服务器、CN 网元（如 AMF，安全锚功能（Security Anchor Function，SEAF）），所述方法包括：

步骤 201、向第一目标端发送第一信息和/或第一指示信息，其中，所述第一信息包括如下至少一项：

第二认证服务器的索引信息，

所述第一通信设备的厂家的相关信息，

所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。

一种实施方式中，所述第一目标端可以包括：第一网络的通信设备，例如：第一网络中的 AMF，该第一网络可以 SNPN。

另一种实施方式中，所述第一目标端可以包括第一服务器（包括配置服务器，或认证的中间服务器）。

当第一通信设备是终端的情况下，第一目标端可以是第一网络的通信设备或第一服务器。

当第一通信设备是第一网络的 CN 设备（如 AMF）的情况下，第一目标端可以是或第一服务器。

一种实施方式中，所述第一通信设备可以具有第二证书。一种实施方式中，第二认证服务器可以具有第二证书。

可选地，所述第二证书可以包括以下至少一项：

与第一网络无关的证书，

当终端不具有与第一网络相关的证书的情况下用于接入第一网络的证书，

当终端为请求配置与第一网络相关的证书的情况下用于接入第一网络的证书，

接入第一网络的受限服务的证书，

第一通信设备厂家为第一通信设备配置的证书，

能够被第二认证服务器认证的证书。

一种实施方式中，所述第二认证服务器包括至少以下之一：第一网络外的认证服务器、服务提供商的认证服务器，第一通信设备的厂家的认证服务器，具有第二证书或能够认证第二证书的认证服务器。

可选地，所述服务提供商可以在第一网络之外。

一种实施方式中，所述厂家为所述第二认证服务器所属的第一通信设备的厂家。

可选地，所述厂家的相关信息包括：厂家标识信息（如 Vendor ID，或 TAC）。

一种实施方式中，上述第二认证服务器的索引信息可以包含以下至少一项：第二认证服务器的地址相关信息（如 IP，FQDN，或 URL），第二认证服务器归属的终端厂家的标识信息。

一种实施方式中，所述第一指示信息用于请求获取与第一网络相关的证书可以是，通过第一指示信息来请求获取与第一网络相关的证书。

本发明一种可选实施例中，与第一网络相关的证书可以包括以下至少一项：与第一网络直接相关的证书，用于接入第一网络正常服务的证书，能够被第一网络的认证服务器直接认证的证书，接入第一网络非受限服务的证书。不难理解，此时，第一服务器可以为 UE 配置能够被第一网络直接认证的证书。

本发明另一种可选实施例中，与第一网络无关的证书可以包括以下至少一项：与第一网络非直接相关的证书。与第一网络非直接相关的证书可以包括不能够通过第一网络的认证服务器直接认证的证书。通过第一网络之外的认证服务器认证的证书可以理解为与第一网络无关或无直接相关的证书。

本发明实施例中，通过上述可以实现向第一目标终端发送上述第一信息和/或第一指示信息，从而第一目标终端可以根据所述第一信息和/或第一指示信息，执行第一操作，具体如图 3 实施例所述。

示例性的，第一操作包括如下至少一项操作：

确定所述第二认证服务器；

确定向所述第二认证服务器请求对第一通信设备进行认证；

向所述第二认证服务器请求对第一通信设备进行认证；

向第一服务器请求对所述第一通信设备进行认证；

向所述第一服务器发送所述第一信息；

确认所述第一通信设备是否为第一网络的合法设备；

确认是否允许为所述第一通信设备配置所述与第一网络相关的证书；

确认是否允许所述第一网络接受所述第一通信设备的注册请求；

其中，所述第一服务器为能够为所述第一通信设备配置与所述第一网络相关的证书的服务器。

以实现第一网络对第一通信设备的接入控制的目的。

可选的，所述发送第一信息包括：

当满足第一条件时，发送第一信息；

其中，所述第一条件包括以下至少一项：

所述第一通信设备具有第二证书；

所述第一通信设备不具有与第一网络相关的证书；

所述第一通信设备请求接入第一网络；

所述第一通信设备请求接入第一网络的受限服务；

所述第一通信设备请求获取与第一网络相关的证书；

获取到所述第一信息中的至少一项；

获取到对所述第一信息的请求信息；

获取到第一网络支持受限服务的信息；

获取到第一网络支持和/或要求对受限服务进行认证的信息；

获取到第一网络支持和/或要求对所述第一通信设备的认证的信息；

获取到所述第一网络支持向所述第一通信设备配置与所述第一网络相关的证书的信息。

一种实施方式中，获取第一目标端发送的身份请求且身份请求的类型为第一通信设备的厂家相关类型；

其中，所述第二证书如上所述，此处不再赘述。

一种实施方式中，第一网络支持和/或要求对第一通信设备认证可以包括以下至少一项：

第一网络支持和/或要求的第一通信设备经过第一网络与第二认证服务器间实现认证,

第一网络支持和/或要求基于第二证书对第一通信设备进行认证。

其中, 所述第一通信设备可以为不具有与第一网络相关的证书的终端。不难理解, 当终端配置与第一网络相关的证书之前接入第一网络的情况下, 第一网络可以为了更安全的考虑, 要求对终端基于第二证书(如终端厂家为终端配置的证书)进行认证。终端在此要求下, 可以向第一网络提供第二认证服务器的相关索引信息, 以支持认证。

一种实施方式中, 获取到第一网络支持和/或要求对第一通信设备的认证的信息可以包括以下至少一项:

获取到第一网络支持和/或要求对通过第二认证服务器对第一通信设备的认证的信息,

获取到第一网络支持和/或要求对通过第二证书对第一通信设备的认证的信息。

其中, 所述第一通信设备可以为不具有与第一网络相关的证书的终端。

不难理解, 当终端配置与第一网络相关的证书之前接入第一网络的情况下, 第一网络可以为了更安全的考虑, 要求对终端基于第二证书进行认证。终端在此要求下, 可以向第一网络提供第二认证服务器的相关索引信息, 以支持认证。

一种实施方式中, 第一通信设备预配置了第一信息。不难理解, 在第一通信设备出厂时, 其厂家在第一通信设备上预配置了第一信息。

具体地, 与第一网络相关的证书如前文所述, 此处不再赘述。

一种实施方式中, 第一网络可以在小区广播至少以下一项:

第一网络支持受限服务的信息;

第一网络支持和/或要求对受限服务进行认证的信息;

第一网络支持和/或要求对所述第一通信设备的认证的信息;

第一网络支持向所述第一通信设备配置与所述第一网络相关的证书的信息。

一种实施方式中, 所述第一网络支持和/或要求对所述第一通信设备的认

证的信息包括第一网络支持和/或要求的初始认证的信息。所述支持和/或要求的初始认证包括：当第一通信设备不具有与第一网络相关的证书的情况下接入第一网络或第一通信设备请求配置与第一网络相关的证书的步骤前，依然支持和/或要求对第一通信设备进行认证。所述初始认证可以由第一认证服务器与第一通信设备，经过第一网络的执行。

不难理解，当第一通信设备不具有与第一网络相关的证书的情况下，第一网络依然可以通过第一认证服务器对第一通信设备进行认证。

在一种实施方式中，第一网络在小区广播指示要求初始认证时，第一设备才向第一网络请求第二认证服务器的索引信息。

可选的，所述对所述第一信息的请求信息包括以下至少一项：

对所述第一信息的请求信息包括以下至少一项：

第一请求信息，且所述第一请求信息用于请求所述第一通信设备的厂家信息，

第二请求信息，且所述第二请求信息用于请求所述第二认证服务器的索引信息，

第三请求信息，且所述第三请求信息用于请求所述第二认证服务器的地址相关信息。

一种实施方式中，所述获取第一目标端（如第一网络的 AMF）发送的第一请求信息，且所述第一请求信息用于请求第一通信设备的厂家信息包括：获取第一目标端发送的身份请求且身份请求的类型为第一通信设备的厂家的相关类型（如终端厂家类型）。一种实施方式中，控制面信令发送第一信息和/或第一指示信息。一种实施方式中，通过非接入层接入请求（如注册请求消息，或附着请求消息等）发送第一信息和/或第一指示信息。

可选的，所述发送第一信息的步骤之前，所述方法还包括：

向所述第一目标端发送接入请求和/或发送第一指示信息，

其中，所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。

一种实施方式中，所述第一指示信息可以体现为一种接入的原因（如线资源控制(Radio Resource Control, RRC)原因, 或非接入层(Non-access stratum,

NAS) 层的接入原因), 接入请求或接入的类型。

可选的, 所述发送第一信息的步骤之前, 所述方法还包括:

接收第一目标端发送的以下至少一项信息:

对所述第一信息的请求信息;

第一网络支持受限服务的信息;

第一网络支持和/或要求对受限服务进行认证的信息;

第一网络支持和/或要求对所述第一通信设备的认证的信息;

第一网络支持向所述第一通信设备配置与第一网络相关的证书的信息。

一种实施方式中, 第一目标端接收到第一通信设备接入请求和/或第一指示后, 发送的对第一信息的请求信息。

一种实施方式中, 对所述第一通信设备的认证的信息可以是, 终端厂家的相关信息、第二认证服务器的索引信息、第二认证服务器的地址信息。

可选的, 所述方法还包括:

获取第二信息。第二信息具体如所述第二信息如图 5 实施例所述。

示例性地, 所述第二信息包括如下至少一项:

第一终端路由选择策略 (如 URSP);

默认 DNN 信息设置为空;

默认切片信息设置为空;

用于第一数据通道建立的相关信息;

第二指示信息;

第三指示信息;

第一服务器的地址相关信息;

第二认证服务器的地址相关信息;

其中, 所述第一服务器为能够配置与第一网络相关的证书的服务器;

所述第一终端路由选择策略用于访问第一服务器或证书下载应用;

所述第一数据通道为第一网络中的数据通道;

所述第二指示信息用于指示以下至少一项:

所述第一数据通道用于第一通信设备与第一服务器间的交互,

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

一种实施方式中，所述用于第一数据通道（所述数据通道比如 PDU 会话）建立的相关信息包括以下至少一项：

数据网络名称（Data Network Name, DNN），切片信息（如 NSSAI），会话和服务连续模式（Session and Service Continuity Mode, SSC Mode），SSC Mode，数据通道类型（如 PDU 会话类型）。

一种实施方式中，所述第一数据通道为第一网络中的数据通道且用于下载与第一网络证书数据通道。

一种实施方式中，第一通信设备接收到上述第二信息后，可以建立上述第一数据通道。

通过本发明实施例中，向第一目标端发送第一信息和/或第一指示信息，其中，所述第一信息如前文所述，此处不再赘述。这样一方面能够支持第一网络选取第二认证服务器对第一通信设备进行认证，从而支持终端无与第一网络相关证书的情况下接入第一网络时，对终端进行认证，避免仿冒和不合法终端对第一网络的安全攻击；另一方面支持对第一通信设备进行配置，以支持合法的终端获取与第一网络相关的证书，以接入第一网络的服务。

请参考图 3，本发明实施例还提供一种接入控制方法，应用于第二通信设备，第二通信设备包括但不限于以下之一：第一网络中的通信设备（如 AMF、SEAF，或 AF 等），第一服务器，第二认证服务器，所述方法包括：

步骤 301、获取第一信息、第一指示信息、合法设备列表和第三信息中的至少一项；

步骤 302、根据所述第一信息、第一指示信息、合法设备列表和第三信息中的至少一项，执行第一操作；

其中，所述第一信息包括如下至少一项：第二认证服务器的索引信息，第一通信设备的厂家的相关信息，所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类

型为受限服务；

所述第三信息包括以下至少一项：

所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

一种实施方式中，第三信息提供的是合法的所述第二认证服务器的相关信息。不难理解，可以通过第三信息中的“所述第二认证服务器的地址相关信息”对第一信息的“所述第二认证服务器的地址相关信息”进行对比，确认第一信息中的“所述第二认证服务器的地址相关信息”合法。

一种实施方式中，上述第一信息、第一指示信息和第三信息中的至少一项可以包括：第一信息、第一指示信息和第三信息中的任意一项，或者第一信息、第一指示信息和第三信息中的任意多项的组合。

一种实施方式中，上述第一信息可以参见图 2 所示的实施例中的第一信息，上述第一指示信息可以参见图 2 所示的实施例中的第一指示信息，此处不作赘述。

一种实施方式中，从第一通信设备获取所述第一信息和/或第一指示信息。一种实施方式汇总，从第三通信设备所述第三信息。

一种实施方式中，通过接入请求（如注册请求消息，或附着请求消息等）获取第一信息和/或第一指示信息。

一种实施方式中，上述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息可以确认第二认证服务器的地址相关信息。

可选的，所述第一操作包括如下至少一项：

确定所述第二认证服务器；

确定向所述第二认证服务器请求对第一通信设备进行认证；

向所述第二认证服务器请求对第一通信设备进行认证；

向第一服务器请求对所述第一通信设备进行认证；

向所述第一服务器发送所述第一信息；

确认所述第一通信设备是否为第一网络的合法设备；

确认是否允许为所述第一通信设备配置所述与第一网络相关的证书；

确认是否允许所述第一网络接受所述第一通信设备的注册请求；

其中，所述第一服务器为能够为所述第一通信设备配置与所述第一网络相关的证书的服务器。

所述确定所述第二认证服务器包括确定所述第二认证服务器的地址相关信息。

进一步地，所述确定第二认证服务器的步骤可以包括但不限于如下至少一项：1) 根据第一信息中的“所述第二认证服务器的索引信息”和第三信息中的“所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息”，可以确定第二认证服务器。不难理解，所述确定第二认证服务器可以包括为终端选择一个符合所述第二认证服务器的索引信息的第二认证服务器。

2) 根据第一信息中的“所述第一通信设备的厂家的相关信息”和第三信息中的“所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息”，可以确定第二认证服务器。不难理解，所述确定第二认证服务器可以包括为终端选择“所述第一通信设备的厂家的相关信息”对应的第二认证服务器。

3) 根据第一信息中的“所述第二认证服务器的地址相关信息”和/或第三信息中的“所述第二认证服务器的地址相关信息”，可以确定第二认证服务器。不难理解，所述确定第二认证服务器可以包括为终端选择一个符合第一信息中的“所述第二认证服务器的地址相关信息”的第二认证服务器。通过对比第一信息中的与第三信息中的“所述第二认证服务器的地址相关信息”，可以确认第一信息中的“所述第二认证服务器的地址相关信息”是合法的所述第二认证服务器的地址相关信息。

4) 根据第一指示信息和/或第三信息中的“所述第二认证服务器的地址相关信息”，可以确定第二认证服务器。不难理解，所述确定第二认证服务器可以包括：根据第一指示信息，选择一个第三信息中的“所述第二认证服务器的地址相关信息”对应的第二认证服务器。

进一步地，所述确定向所述第二认证服务器请求对第一通信设备进行认证的步骤可以包括但不限于如下至少一项：

1) 根据第一指示信息和/或第一信息, 可以确定向所述第二认证服务器请求对第一通信设备进行认证;

2) 根据第一指示信息和/或第三信息中的“所述第二认证服务器的地址相关信息”, 可以确定向所述第二认证服务器请求对第一通信设备进行认证。

一种实施方式中, 通过第二认证服务器的认证, 第一网络可以确认第一通信设备是否仿冒设备。第二认证服务器对第一通信设备认证通过的情况下, 可以进一步根据合法设备列表, 确认第一通信设备是否是第一网络的合法设备和/或是否允许为其配置与第一网络相关证书。

另一种实施方式中, 通过第二认证服务器的认证, 第一网络可以确认第一通信设备是否为仿冒设备, 且是否为第一网络的合法设备。一种实施方式中, 所述合法设备可以包括允许配置与第一网络相关的证书的设备(所述设备如终端)。另一种实施方式中, 所述合法设备可以包括不具有与第一网络相关的证书且允许配置与第一网络相关的证书的设备(所述设备如终端)。

一种实施方式中, 所述合法终端列表可以配置在第一网络的用户管理服务器(如 UDM, HSS, 或 UDR) 中。可以从所述用户管理服务器获取合法设备列表。

所述合法设备列表包括如下至少一项: 还未配置与第一网络相关的证书的第一网络的合法通信设备, 允许配置与第一网络相关的证书的通信设备。

可选的, 合法设备列表为合法终端列表。合法终端列表可以是一组终端的信息。一种实施方式中, 所述终端的信息可以包括终端的标识, 如 IMEI, PEI, GPSI, MAC 地址或 SUPI (此时的 SUPI 为非第一网络的 SUPI)。

可选地, 所述合法终端列表可以包含以下至少一项: 还未配置与第一网络相关的证书的第一网络的合法终端, 允许配置与第一网络相关的证书的终端。

不难理解, 一种实施方式中, 通过第二认证服务器的认证, 第一网络可以确认终端是终端(即非仿冒终端), 通过合法终端列表, 第一网络可以确认终端是否是合法的终端, 是否为允许为其配置与第一网络相关证书。

不难理解, 另一种实施方式中, 通过认证服务器的认证, 第一网络可以确认终端是终端且是第一网络的合法终端。即认证服务器中直接认证通过终

端非仿冒的终端而且是第一网络的合法终端，允许配置与第一网络相关的证书。

上述第一服务器也可以称作配置服务器或者认证的中间服务器。

可选的，在所述第一通信设备满足第二条件时，确认所述第一通信设备为所述第一网络的合法设备；

其中，所述第二条件包括如下至少一项：

所述第一通信设备通过所述第二认证服务器的认证；

所述第一通信设备是合法设备列表中的通信设备。

合法设备列表如前文所述，此处不再赘述。

可选地，所述获取第一信息之前，所述方法还包括：

接收第一通信设备的接入请求和/或第一指示信息；其中，所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务；

基于所述接入请求和/或第一指示信息，发送对第一信息的请求信息。

一种实施方式，上述发送对第一信息的请求信息可以是向第一通信设备发送，以请求第一通信设备发送第一信息。

一种实施方式中，从第一通信设备接收第一通信设备的接入请求和/或第一指示信息。

一种实施方式中，向第一通信设备发送对第一信息的请求信息。

可选的，所述对第一信息的请求信息包括以下至少一项：

第一请求信息，且所述第一请求信息用于请求所述第一通信设备的厂家信息，

第二请求信息，且所述第二请求信息用于请求所述第二认证服务器的索引信息，

第三请求信息，且所述第三请求信息用于请求所述第二认证服务器的地址相关信息。

一种实施方式中，所述发送第一请求信息，且所述第一请求信息用于请求第一通信设备的厂家信息包括：发送身份请求（identity request）且身份请求的类型为第一通信设备的厂家的相关类型，如终端厂家类型。

可选的，所述方法还包括：

在确定所述第一通信设备为第一网络的合法设备的情况下，发送第二信息，其中，所述第二信息包括如下至少一项：

用于第一数据通道建立的相关信息；

第二指示信息；

第一服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一数据通道为第一网络中的数据通道；

第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互；

所述第一数据通道用于第一通信设备请求与第一网络相关的证书；

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书。

一种实施方式中，从第一通信设备获取所述第一信息和/或第一指示信息。

一种实施方式中，从第三通信设备获取所述第三信息。

一种实施方式中，通过接入请求（如注册请求消息，或附着请求消息等）获取第一信息和/或第一指示信息。

一种实施方式中，根据第一信息中的“所述第二认证服务器的索引信息”和第三信息中的“所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息”，可以确认第二认证服务器的地址相关信息。

另一种实施方式中，根据第一指示信息和第三信息中的“第二认证服务器的地址相关信息”，可以确认通过第二认证服务器对第一通信设备进行认证和/或确认第二认证服务器的地址相关信息。

通过本实施例中，可以获取第一信息、第一指示信息、合法设备列表和第三信息中的至少一项；根据所述第一信息、第一指示信息、合法设备列表和第三信息中的至少一项，执行第一操作；这样一方面能够支持第一网络选取第二认证服务器对第一通信设备进行认证，从而支持终端无与第一网络相关证书的情况下接入第一网络时，对终端进行认证，避免仿冒和不合法终端对第一网络的安全攻击；另一方面支持对第一通信设备进行配置，以支持合法的终端获取与第一网络相关的证书，以接入第一网络的服务。

请参见图 4，图 4 是本发明实施例提供的另一种接入控制方法，该方法

应用于第三通信设备，第三通信设备包括但不限于以下之一：AF、第二认证服务器、第一通信设备的厂家的相关设备，如图4所示，包括以下步骤：

步骤401、确定第三信息

步骤402、发送第三信息；

其中，所述第三信息包括如下至少一项：

第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

一种实施方式中，上述第三信息是图3所示的实施例中的第三信息，此处不作赘述。

一种实施方式中，所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息，可以用于确认第二认证服务器的地址相关信息。

一种实施方式中，上述发送第三信息可以是向第二通信设备发送第三信息。

可选的，发送所述第二认证服务器的相关信息，包括：

满足第三条件的情况下，发送所述第二认证服务器的相关信息；

所述第三条件包括如下至少一项：

所述第三通信设备与所述第二认证服务器间相互认证通过；

所述第三通信设备与第一网络间相互认证通过。

可选地，所述第三通信设备为第一网络之外的通信设备。

一种实施方式中，上述第三通信设备与所述第二认证服务器间可以是预先相互认证通过。

一种实施方式中，第三通信设备与第一网络间相互认证通过。

通过本实施例中，发送第三信息，使得第二通信设备获取到上述第三信息，

这样能够支持第一网络选取第二认证服务器对第一通信设备进行认证，从而支持终端无与第一网络相关证书的情况下接入第一网络时，对终端进行认证，避免仿冒和不合法终端对第一网络的安全攻击。

请参见图 5，图 5 是本发明实施例提供的另一种接入控制方法，该方法应用于第四通信设备，第四通信设备包括但不限于终端，如图 5 所示，包括以下步骤：

步骤 501、获取第二信息；

步骤 502、根据所述第二信息，执行第二操作；

其中，所述第二信息包括如下至少一项：

第一终端路由选择策略（如 URSP）；

默认 DNN 信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

一种实施方式中，上述第二信息可以参见图 5 所示的实施例中的第二信息，此处不作赘述。

一种实施方式中，上述获取第二信息可以是第一网络获取上述第二信息。

可选的，所述第二操作包括以下至少一项：

建立第一数据通道，且所述第一数据通道满足至少以下之一：所述第一

数据通道用于第一通信设备与第一服务器间的交互，所述第一数据通道用于第一通信设备请求与第一网络相关的证书，所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

向第一服务器请求配置与第一网络相关的证书；

向第二认证服务器请求配置与第一网络相关的证书；

拒绝应用层除了目标第一服务器和/或证书下载应用之外访问请求或数据发送请求；

仅允许目标为第一服务器和/或证书下载应用的访问请求或数据发送请求。

一种实施方式中，所述用于第一数据通道（所述数据通道比如 PDU 会话）建立的相关信息包括以下至少一项：

DNN，切片信息（如 NSSAI），SSC Mode，数据通道类型（如 PDU 会话类型）。

一种实施方式中，所述第一数据通道为第一网络中的数据通道且用于下载与第一网络证书数据通道。

一种实施方式中，根据用于第一数据通道建立的相关信息和/或第二指示信息请求建立第一数据通道。

根据第一服务器的地址相关信息，向第一服务器请求配置与第一网络相关的证书。

根据第二认证服务器的地址相关信息，向第二认证服务器请求配置与第一网络相关的证书。不难理解，第二认证服务器根据所述请求，首先对第四通信设备进行验证，验证通过后，再向第一服务器请求为第四通信设备配置与第一网络相关的证书。

通过本实施例中，获取第二信息，并根据所述第二信息，执行第二操作，能够支持终端无与第一网络相关证书的情况下接入第一网络时，获取必要配置，以支持合法的终端获取与第一网络相关的证书，以接入第一网络的服务。

请参见图 6，图 6 是本发明实施例提供的另一种接入控制方法，该方法应用于第五通信设备，第五通信设备包括但不限于以下之一：第一网络的通信设备，如 AMF，如图 6 所示，包括以下步骤：

步骤 601、发送第二信息，其中，所述第二信息包括如下至少一项：

第一终端路由选择策略（如 URSP）；

默认 DNN 信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

可选地，发送第二信息的步骤之前，执行确定第二信息相关操作。

执行确定第二信息的相关操作包括

- 确定第一终端路由选择策略的操作。
- 默认 DNN 信息设置为空或不设置默认 DNN 信息。
- 默认切片信息设置为空或不设置默认（NSSAI）切片信息。

不难理解，除了第一服务器，第一网络不允许终端访问其他的业务。默认 DNN 用于终端的应用或访问目标没有对应的路由选择策略中的 DNN 时，选用默认的 DNN 建立数据通道来访问所述应用或访问目标。因此不配置默认 DNN 便是不允许终端发起其他的业务。默认切片信息用于终端的应用或访问目标没有对应的路由选择策略中的切片信息时，选用默认的切片信息建立数据通道来访问所述应用或访问目标。因此不配置默认切片信息便是不允许终

端发起其他的业务。

可选的，所述确定第一终端路由选择策略的操作包括以下至少一项：

将第一终端路由选择策略中的应用描述设置为第一服务器的地址相关信息（比如将应用描述中设置为的第一服务器的 IP 三元组或者是第一服务器的 FQDN），

将第一终端路由选择策略中的应用描述设置为证书下载应用信息（比如将应用描述中设置为的证书下载应用），

将第一终端路由选择策略中的应用描述设置为受限服务的 DNN。

所述证书下载应用用于请求第一服务器配置与第一网络相关的证书。

一种实施方式中，可以通过控制面信令配置与第一网络相关的证书。不难理解，此时，可以通过第三指示信息限制不允许用户面，仅允许控制面。

可选的，在满足第四条件的情况下，执行确定第二信息相关操作和/或发送第二信息；

其中，所述第四条件可以包括：

终端接入第一网络的受限服务或接收到终端发送的第一指示信息；

确认终端初始认证通过或确认所述终端通过所述第二认证服务器的认证；

确认所述第一通信设备是非仿冒设备；

确认所述终端为第一网络的合法设备或终端是合法设备列表中的通信设备；

确认终端允许被配置所述第一网络相关的证书。

可选地，向终端发送第二信息。

能够支持终端无与第一网络相关证书的情况下接入第一网络时，获取必要配置，以支持合法的终端获取与第一网络相关的证书，以接入第一网络的服务。下面结合具体应用场景对本发明实施例的接入控制方法进行说明。

本发明实施例的应用场景 1：

本发明实施例的应用场景 1 主要描述 UE、SNPN 和第二认证服务器之间的接入控制，如图 7 所示，包括以下步骤：

步骤 1：AF 向第一网络发送第三信息（第二认证服务器的相关信息）。

第三信息包括以下至少一项：第二认证服务器的索引信息与第二认证服务器地址信息的映射信息，第二认证服务器地址信息。

所述第二认证服务器的索引信息与第二认证服务器地址信息的映射信息中的第二认证服务器的索引信息可以索引到其映射的第二认证服务器地址信息。

AF 可以为终端厂家的 AF。

AF 可以通过第一网络的 NEF 向第一网络的 UDM 发送所述信息。

步骤 2：UE 向第一网络的 AMF 发起注册请求。

可选地，在所述注册请求中包含第二认证服务器的索引信息。或者只提供终端的厂家信息。

第二认证服务器的索引信息可以包含以下至少一项：第二认证服务器的地址信息（如 IP，FQDN，URL），第二认证服务器归属的终端厂家的标识信息。

步骤 3（可选地）：AMF 向 UE 发送身份认证请求（identity request），且身份认证类型（identity type）设置为以下至少一致：终端厂家（如 Vendor ID）等相关类型、第二认证服务器索引信息、第二认证服务器地址信息。

UE 在身份认证响应（identity response）中包含第二认证服务器的索引信息，比如 UE vendor 的标识信息。

步骤 4（可选地）：AMF 向 UDM 发送所述第二认证服务器的索引信息，获取认证服务器的地址信息。

UDM 根据第二认证服务器的索引信息与第二认证服务器地址信息的映射信息、第二认证服务器的索引信息，可以确认第二认证服务器的地址信息。

UDM 向 AMF 发送第二认证服务器的地址信息。

一种实施方式中，步骤 4 采用的是非 UE 相关的信令过程。

步骤 5：AMF 执行第一操作，所述第一操作包括以下至少一项：

确定第二认证服务器的地址，

向第二认证服务器请求认证（Authentication/Security）终端，

确认终端是否为第一网络的合法终端或是否允许配置与第一网络相关的证书的终端。

一种实施方式中，从 AF 获取第二认证服务器的索引信息与第二认证服务器地址信息的映射信息。

另一种实施方式中，从终端获取第二认证服务器的索引信息。

进一步地，当满足合法终端条件时，可以确认终端是第一网络的合法终端。合法终端条件可以包括至少以下一项：终端通过第二认证服务器的认证，终端是合法终端列表中的终端。所述合法终端可以是允许配置与第一网络相关的证书的终端。

步骤 6：当确认终端是第一网络的合法终端时，向终端发送第二信息和注册接受消息。

所述第二信息如图 5 实施例所述。示例性的，所述第二信息包括以下至少一项：

用于受限服务的 PDU 会话建立的相关信息（如 DNN、切片信息、SSC 等），

第一服务器的地址相关信息。

一种实施方式中，在发送注册接收消息中包括：第一服务器的地址相关信息。

步骤 7：UE 与 SNPN 建立会话。

步骤 8：UE 与配置服务器之间传输 SNPN 证书（credential）配置请求和配置响应。

本发明实施例的应用场景 2：

本发明实施例的应用场景 2 主要描述 UE、SNPN、配置服务器和第二认证服务器之间的接入控制，如图 8 所示，包括以下步骤：

步骤 1（可选地）：配置服务器获取第三信息（或称为第二认证服务器的相关信息）。

第二认证服务器的相关信息包括以下至少一项：第二认证服务器的索引信息与第二认证服务器地址信息的映射信息，第二认证服务器地址信息。

所述第二认证服务器的索引信息与第二认证服务器地址信息的映射信息中的第二认证服务器的索引信息可以索引到其映射的第二认证服务器地址信息。

步骤 2: UE 向第一网络的 AMF 发起接入请求, 发送第二认证服务器的索引信息。

第二认证服务器的索引信息可以包含以下至少一项: 第二认证服务器的地址信息 (如 IP, FQDN, URL), 第二认证服务器归属的终端厂家的标识信息。

步骤 3 (可选地): AMF 向 UDM 发送所述第二认证服务器的索引信息, 获取认证服务器的地址信息。

UDM 根据第二认证服务器的索引信息与第二认证服务器地址信息的映射信息、第二认证服务器的索引信息, 可以确认第二认证服务器的地址信息。

UDM 向 AMF 发送第二认证服务器的地址信息。

一种实施方式中, 步骤 4 采用的是非 UE 相关的信令过程。

步骤 4: AMF 执行以下操作至少一项:

确定第二认证服务器的地址,

向第一网络的配置服务器请求认证终端,

向第一网络的配置服务器发送第二认证服务器的地址信息或第二认证服务器的索引信息。

配置服务器执行以下操作至少一项:

确定第二认证服务器的地址,

向第二认证服务器请求认证终端。

认证完成步骤后, AMF 执行以下操作至少一项:

确认终端是否为第一网络的合法终端或是否允许配置与第一网络相关的证书的终端,

确认是否允许终端注册。

进一步地, 当满足合法终端条件时, 可以确认终端是第一网络的合法终端。合法终端条件可以包括至少以下一项: 终端通过第二认证服务器的认证, 终端是合法终端列表中的终端。所述合法终端可以是允许配置与第一网络相关的证书的终端。

步骤 5: 当确认终端是第一网络的合法终端时, 向终端发送第二信息和注册接受消息。

所述第二信息如图 5 实施例所述。示例性的，所述第二信息包括以下至少一项：

用于受限服务的 PDU 会话建立的相关信息（如 DNN、切片信息、SSC 等），

第一服务器的地址相关信息。

一种实施方式中，在发送注册接收消息中包括：第一服务器的地址相关信息。

步骤 6：UE 与 SNPN 建立会话。

步骤 7：UE 与配置服务器传输 SNPN 证书（credential）配置。

本发明实施例的应用场景 3：

本发明实施例的应用场景 3 主要描述 UE、配置服务器和认证服务器之间的接入控制，如图 9 所示，包括以下步骤：

步骤 1（可选地）：配置服务器获取第二认证服务器的相关信息。

第二认证服务器的相关信息包括以下至少一项：第二认证服务器的索引信息与第二认证服务器地址信息的映射信息，第二认证服务器地址信息。

所述第二认证服务器的索引信息与第二认证服务器地址信息的映射信息中的第二认证服务器的索引信息可以索引到其映射的第二认证服务器地址信息。

步骤 2：UE 向第一网络的 AMF 发起注册请求。

AMF 向终端发送第二信息和注册接受消息。

所述第二信息包括以下至少一项：

用于受限服务的 PDU 会话建立的相关信息（如 DNN、切片信息、SSC 等），

第一服务器的地址相关信息。

一种实施方式中，在发送注册接收消息中包括：第一服务器（如配置服务器）的地址相关信息。

步骤 3：UE 与第一网络 PDU 会话建立。所述 PDU 会话为受限服务的 PDU 会话。

另一种可选的方式中，SMF 向终端发送第二信息。

步骤 4: UE 向配置服务器发起配置请求。UE 向配置服务器发送第二认证服务器的索引信息。

第二认证服务器的索引信息可以包含以下至少一项: 认证服务器的地址信息 (如 IP, FQDN, URL), 认证服务器归属的终端厂家的标识信息。

步骤 5: 配置服务器执行以下操作至少一项:

确定第二认证服务器的地址,

向第二认证服务器请求认证终端。

认证完成步骤后, 配置服务器执行以下操作至少一项:

确认终端是否为第一网络的合法终端或是否允许配置与第一网络相关的证书的终端,

进一步地, 当满足合法终端条件时, 可以确认终端是第一网络的合法终端。合法终端条件可以包括至少以下一项: 终端通过第二认证服务器的认证, 终端是合法终端列表中的终端。所述合法终端可以是允许配置与第一网络相关的证书的终端。

步骤 6: 当确认终端是第一网络的合法终端时, 向终端配置与第一网络相关的证书 (credential)。

本发明实施例的应用场景 4

本发明实施例的应用场景 4 主要描述 UE 和配置服务器之间的接入控制, 如图 10 所示, 包括以下步骤:

步骤 1: UE 向第一网络的 AMF 发起注册请求。

AMF 向终端发送第二信息和注册接受消息。

所述第二信息如图 5 实施例所述。示例性的, 所述第二信息包括以下至少一项:

用于受限服务的 PDU 会话建立的相关信息 (如 DNN、切片信息、SSC 等),

第一服务器的地址相关信息。

一种实施方式中, 在发送注册接收消息中包括: 第一服务器 (如配置服务器) 的地址相关信息。

步骤 2: UE 与第一网络 PDU 会话建立。所述 PDU 会话为受限服务的 PDU

会话。

另一种可选的方式中，SMF 向终端发送第二信息。

步骤 3：UE 向配置服务器发起配置请求。

步骤 4：配置服务器对终端进行认证。

认证完成步骤后，配置服务器执行以下操作至少一项：

确认终端是否为第一网络的合法终端或是否允许配置与第一网络相关的证书的终端；

进一步地，当满足合法终端条件时，可以确认终端是第一网络的合法终端。合法终端条件可以包括至少以下一项：终端通过第二认证服务器的认证，终端是合法终端列表中的终端。所述合法终端可以是允许配置与第一网络相关的证书的终端。

步骤 5：当确认终端是第一网络的合法终端时，向终端配置与第一网络相关的证书。

本发明实施例中，可以实现如下：

UE 刚出厂接入 SNPN 时或接入 SNPN 的配置服务器时，提供标识 UE 厂家（vendor）的相关信息，SNPN 收到后用于选择 UE 厂家的第二认证服务器（如 AAA）对 UE 进行认证。

SNPN 可以定义的新的 identity 类型获取 UE 的厂家等第二认证服务器的索引信息。

SNPN 向 UE 发送配置服务器的地址相关信息，用于 UE 通过用户面向配置服务器发起配置请求或者 SNPN 通过控制面向配置服务器为 UE 请求与第一网络相关的证书

通过本发明实施例，一方面可以支持 UE 无 SNPN 的证书时接入 SNPN 时，对 UE 进行认证和配置，避免仿冒和不合法 UE 的安全攻击；另一方面支持对 UE 进行 SNPN 的证书配置。

请参见图 11，图 11 是本发明实施例提供的一种通信设备的结构图，所述通信设备为第一通信设备，如图 11 所示，通信设备 1100 包括：

第一发送模块 1101，用于向第一目标端发送第一信息和/或第一指示信息，其中，所述第一信息包括如下至少一项：

第二认证服务器的索引信息，
所述第一通信设备的厂家的相关信息，
所述第二认证服务器的地址相关信息；
所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。

可选的，所述发送第一信息包括：
当满足第一条条件时，发送第一信息；
其中，所述第一条条件包括以下至少一项：
所述第一通信设备具有第二证书；
所述第一通信设备不具有与第一网络相关的证书；
所述第一通信设备请求接入第一网络；
所述第一通信设备请求接入第一网络的受限服务；
所述第一通信设备请求获取与第一网络相关的证书；
获取到所述第一信息中的至少一项；
获取到对所述第一信息的请求信息；
获取到第一网络支持受限服务的信息；
获取到第一网络支持和/或要求对受限服务进行认证的信息；
获取到第一网络支持和/或要求对所述第一通信设备的认证的信息；
获取到所述第一网络支持向所述第一通信设备配置与所述第一网络相关的证书的信息。

可选的，所述对所述第一信息的请求信息包括以下至少一项：
对所述第一信息的请求信息包括以下至少一项：
第一请求信息，且所述第一请求信息用于请求所述第一通信设备的厂家信息，

第二请求信息，且所述第二请求信息用于请求所述第二认证服务器的索引信息，

第三请求信息，且所述第三请求信息用于请求所述第二认证服务器的地址相关信息。

可选的，所述发送第一信息的步骤之前，所述通信设备还包括：

第二发送模块，用于向所述第一目标端发送接入请求和/或发送第一指示信息，

其中，所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。

可选的，所述通信设备还包括：

接收模块，用于接收第一目标端发送的以下至少一项信息：

对所述第一信息的请求信息；

第一网络支持受限服务的信息；

第一网络支持和/或要求对受限服务进行认证的信息；

所述第一网络支持和/或要求对所述第一通信设备的认证的信息；

所述第一网络支持向所述第一通信设备配置与第一网络相关的证书的信息。

可选的，所述通信设备还包括：

获取模块，用于获取第二信息，其中，所述第二信息包括如下至少一项：

第一终端路由选择策略；

默认 DNN 信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

通信设备 1100 能够实现本发明方法实施例中第一通信设备实现的各个过程，以及达到相同的有益效果，为避免重复，这里不再赘述。

参见图 12，本发明实施例提供了另一种通信设备，该通信设备为第二通信设备，如图 12 所示，通信设备 1200 包括：

获取模块 1201，用于获取第一信息、第一指示信息、合法设备列表和第三信息中的至少一项；

执行模块 1202，用于根据所述第一信息、第一指示信息、合法设备列表和第三信息中的至少一项，执行第一操作；

其中，所述第一信息包括如下至少一项：第二认证服务器的索引信息，第一通信设备的厂家的相关信息，所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务；

所述第三信息包括以下至少一项：

所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

可选的，所述第一操作包括如下至少一项：

确定所述第二认证服务器；

确定向所述第二认证服务器请求对第一通信设备进行认证；

向所述第二认证服务器请求对第一通信设备进行认证；

向所述第二认证服务器请求对第一通信设备进行认证；

向第一服务器请求对所述第一通信设备进行认证；

向所述第一服务器发送所述第一信息；

确认所述第一通信设备是否为第一网络的合法设备；

确认是否允许为所述第一通信设备配置所述与第一网络相关的证书；

确认是否允许所述第一网络接受所述第一通信设备的注册请求；

其中，所述第一服务器为能够为所述第一通信设备配置与所述第一网络

相关的证书的服务器。

可选的，所述确定第二认证服务器的步骤包括但不限于如下至少一项：

根据第一信息中的所述第二认证服务器的索引信息，以及所述第三信息中的所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息，确定第二认证服务器；

根据第一信息中的所述第一通信设备的厂家的相关信息，以及所述第三信息中的所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息，确定第二认证服务器；

根据第一信息中的所述第二认证服务器的地址相关信息和/或所述第三信息中的所述第二认证服务器的地址相关信息，确定第二认证服务器；

根据第一指示信息和/或所述第三信息中的所述第二认证服务器的地址相关信息，确定第二认证服务器；

和/或，

所述确定向所述第二认证服务器请求对第一通信设备进行认证的步骤包括但不限于如下至少一项：

根据第一指示信息和/或第一信息，确定向所述第二认证服务器请求对第一通信设备进行认证；

根据第一指示信息和/或第三信息中的所述第二认证服务器的地址相关信息，确定向所述第二认证服务器请求对第一通信设备进行认证。

可选的，在所述第一通信设备满足第二条件时，确认所述第一通信设备为所述第一网络的合法设备；

其中，所述第二条件包括如下至少一项：

所述第一通信设备通过所述第二认证服务器的认证；

所述第一通信设备是合法设备列表中的通信设备。

可选的，所述合法设备列表包括如下至少一项：

还未配置与第一网络相关的证书的第一网络的合法通信设备；

允许配置与第一网络相关的证书的通信设备。

可选的，所述通信设备还包括：

接收模块，用于接收第一通信设备的接入请求和/或第一指示信息；其中，

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务；

第一发送模块，用于基于所述接入请求和/或第一指示信息，发送对第一信息的请求信息。

可选的，所述对第一信息的请求信息包括以下至少一项：

第一请求信息，且所述第一请求信息用于请求所述第一通信设备的厂家信息，

第二请求信息，且所述第二请求信息用于请求所述第二认证服务器的索引信息，

第三请求信息，且所述第三请求信息用于请求所述第二认证服务器的地址相关信息。

可选的，所述通信设备还包括：

第二发送模块，用于在确定所述第一通信设备为第一网络的合法设备的情况下，发送第二信息，其中，所述第二信息包括如下至少一项：

用于第一数据通道建立的相关信息；

第二指示信息；

第一服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一数据通道为第一网络中的数据通道；

第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互；

所述第一数据通道用于第一通信设备请求与第一网络相关的证书；

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书。

通信设备 1200 能够实现本发明方法实施例中第二通信设备实现的各个过程，以及达到相同的有益效果，为避免重复，这里不再赘述。

参见图 13，本发明实施例提供了另一种通信设备，该通信设备为第三通信设备，如图 13 所示，通信设备 1300 包括：

确定模块 1301，用于确定第三信息；

发送模块 1302，用于发送第三信息；

其中，所述第三信息包括如下至少一项：

第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

可选的，所述发送所述第二认证服务器的相关信息，包括：

满足第三条件的情况下，发送所述第二认证服务器的相关信息；

所述第三条件包括如下至少一项：

所述第三通信设备与所述第二认证服务器间相互认证通过；

所述第三通信设备与第一网络间相互认证通过。

通信设备 1300 能够实现本发明方法实施例中第三通信设备实现的各个过程，以及达到相同的有益效果，为避免重复，这里不再赘述。

参见图 14，本发明实施例提供了另一种通信设备，该通信设备为第四通信设备，如图 14 所示，通信设备 1400 包括：

获取模块 1401，用于获取第二信息；

执行模块 1402，用于根据所述第二信息，执行第二操作；

其中，所述第二信息包括如下至少一项：

第一终端路由选择策略；

默认 DNN 信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

可选的，所述第二操作包括以下至少一项：

建立第一数据通道，且所述第一数据通道满足至少以下之一：所述第一数据通道用于第一通信设备与第一服务器间的交互，所述第一数据通道用于第一通信设备请求与第一网络相关的证书，所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

向第一服务器请求配置与第一网络相关的证书；

向第二认证服务器请求配置与第一网络相关的证书；

拒绝应用层除了目标第一服务器和/或证书下载应用之外访问请求或数据发送请求；

仅允许目标为第一服务器和/或证书下载应用的访问请求或数据发送请求。

通信设备 1400 能够实现本发明方法实施例中第四通信设备实现的各个过程，以及达到相同的有益效果，为避免重复，这里不再赘述。

参见图 15，本发明实施例提供了另一种通信设备，该通信设备为第五通信设备，如图 15 所示，通信设备 1500 包括：

发送模块 1501，用于发送第二信息，其中，所述第二信息包括如下至少一项：

第一终端路由选择策略；

默认 DNN 信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

可选的，在满足第四条件的情况下，执行确定第二信息相关操作和/或发送第二信息；

其中，所述第四条件包括：

终端接入第一网络的受限服务或接收到终端发送的第一指示信息；

确认终端初始认证通过或确认所述终端通过所述第二认证服务器的认证；

确认所述第一通信设备是非仿冒设备；

确认所述终端为第一网络的合法设备或终端是合法设备列表中的通信设备；

确认终端允许被配置所述第一网络相关的证书。

通信设备 1500 能够实现本发明方法实施例中第三通信设备实现的各个过程，以及达到相同的有益效果，为避免重复，这里不再赘述。

参见图 16，图 16 是本发明实施例提供的通信设备的结构图之五。如图 16 所示，通信设备 1600 包括：存储器 1601、处理器 1602 及存储在存储器 1601 上并可在处理器 1602 上运行的计算机程序 16011。

其中，在通信设备 1600 表现为上述方法实施例中的第一通信设备时，计算机程序 16011 被处理器 1602 执行时实现如下步骤：

向第一目标端发送第一信息和/或第一指示信息，其中，所述第一信息包括如下至少一项：

第二认证服务器的索引信息，

所述第一通信设备的厂家的相关信息，

所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。

可选的，所述发送第一信息包括：

当满足第一条件时，发送第一信息；

其中，所述第一条件包括以下至少一项：

所述第一通信设备具有第二证书；

所述第一通信设备不具有与第一网络相关的证书；

所述第一通信设备请求接入第一网络；

所述第一通信设备请求接入第一网络的受限服务；

所述第一通信设备请求获取与第一网络相关的证书；

获取到所述第一信息中的至少一项；

获取到对所述第一信息的请求信息；

获取到第一网络支持受限服务的信息；

获取到第一网络支持和/或要求对受限服务进行认证的信息；

获取到第一网络支持和/或要求对所述第一通信设备的认证的信息；

获取到所述第一网络支持向所述第一通信设备配置与所述第一网络相关的证书的信息。

可选的，所述对所述第一信息的请求信息包括以下至少一项：

对所述第一信息的请求信息包括以下至少一项：

第一请求信息，且所述第一请求信息用于请求所述第一通信设备的厂家信息，

第二请求信息，且所述第二请求信息用于请求所述第二认证服务器的索引信息，

第三请求信息，且所述第三请求信息用于请求所述第二认证服务器的地址相关信息。

可选的，所述发送第一信息的步骤之前，计算机程序 16011 被处理器 1602 执行时还实现如下步骤：

向所述第一目标端发送接入请求和/或发送第一指示信息，

其中, 所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务。

可选的, 所述发送第一信息的步骤之前, 计算机程序 16011 被处理器 1602 执行时还实现如下步骤:

接收第一目标端发送的以下至少一项信息:

对所述第一信息的请求信息;

对所述第一信息的请求信息;

第一网络支持受限服务的信息;

第一网络支持和/或要求对受限服务进行认证的信息;

第一网络支持和/或要求对所述第一通信设备的认证的信息;

第一网络支持向所述第一通信设备配置与第一网络相关的证书的信息。

可选的, 计算机程序 16011 被处理器 1602 执行时还实现如下步骤:

获取第二信息, 其中, 所述第二信息包括如下至少一项:

第一终端路由选择策略;

默认 DNN 信息设置为空;

默认切片信息设置为空;

用于第一数据通道建立的相关信息;

第二指示信息;

第三指示信息;

第一服务器的地址相关信息;

第二认证服务器的地址相关信息;

其中, 所述第一服务器为能够配置与第一网络相关的证书的服务器;

所述第一终端路由选择策略用于访问第一服务器或证书下载应用;

所述第一数据通道为第一网络中的数据通道;

所述第二指示信息用于指示以下至少一项:

所述第一数据通道用于第一通信设备与第一服务器间的交互,

所述第一数据通道用于第一通信设备请求与第一网络相关的证书,

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书;

所述第三指示信息用于指示以下至少一项: 仅允许受限服务, 仅允许控

制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

其中，在通信设备 1600 表现为上述方法实施例中的第二通信设备时，计算机程序 16011 被处理器 1602 执行时实现如下步骤：

获取第一信息、第一指示信息、合法设备列表和第三信息中的至少一项；

根据所述第一信息、第一指示信息、合法设备列表和第三信息中的至少一项，执行第一操作；

其中，所述第一信息包括如下至少一项：第二认证服务器的索引信息，第一通信设备的厂家的相关信息，所述第二认证服务器的地址相关信息；

所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务；

所述第三信息包括以下至少一项：

所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

可选的，所述第一操作包括如下至少一项：

确定所述第二认证服务器；

确定向所述第二认证服务器请求对第一通信设备进行认证；

向所述第二认证服务器请求对第一通信设备进行认证；

向所述第二认证服务器请求对第一通信设备进行认证；

向第一服务器请求对所述第一通信设备进行认证；

向所述第一服务器发送所述第一信息；

确认所述第一通信设备是否为第一网络的合法设备；

确认是否允许为所述第一通信设备配置所述与第一网络相关的证书；

确认是否允许所述第一网络接受所述第一通信设备的注册请求；

其中，所述第一服务器为能够为所述第一通信设备配置与所述第一网络相关的证书的服务器。

可选的，所述确定第二认证服务器的步骤包括但不限于如下至少一项：

根据第一信息中的所述第二认证服务器的索引信息，以及所述第三信息中的所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息

的映射信息，确定第二认证服务器；

根据第一信息中的所述第一通信设备的厂家的相关信息，以及所述第三信息中的所述第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息，确定第二认证服务器；

根据第一信息中的所述第二认证服务器的地址相关信息和/或所述第三信息中的所述第二认证服务器的地址相关信息，确定第二认证服务器；

根据第一指示信息和/或所述第三信息中的所述第二认证服务器的地址相关信息，确定第二认证服务器；

和/或，

所述确定向所述第二认证服务器请求对第一通信设备进行认证的步骤包括但不限于如下至少一项：

根据第一指示信息和/或第一信息，确定向所述第二认证服务器请求对第一通信设备进行认证；

根据第一指示信息和/或第三信息中的所述第二认证服务器的地址相关信息，确定向所述第二认证服务器请求对第一通信设备进行认证。

可选的，在所述第一通信设备满足第二条件时，确认所述第一通信设备为所述第一网络的合法设备；

其中，所述第二条件包括如下至少一项：

所述第一通信设备通过所述第二认证服务器的认证；

所述第一通信设备是合法设备列表中的通信设备。

可选的，所述合法设备列表包括如下至少一项：

还未配置与第一网络相关的证书的第一网络的合法通信设备；

允许配置与第一网络相关的证书的通信设备。

可选的，所述获取第一信息之前，计算机程序 16011 被处理器 1602 执行时还实现如下步骤：

接收第一通信设备的接入请求和/或第一指示信息；其中，所述第一指示信息用于请求获取与第一网络相关的证书或指示接入的类型为受限服务；

基于所述接入请求和/或第一指示信息，发送对第一信息的请求信息。

可选的，所述对第一信息的请求信息包括以下至少一项：

第一请求信息，且所述第一请求信息用于请求所述第一通信设备的厂家信息，

第二请求信息，且所述第二请求信息用于请求所述第二认证服务器的索引信息，

第三请求信息，且所述第三请求信息用于请求所述第二认证服务器的地址相关信息。

可选的，计算机程序 16011 被处理器 1602 执行时还实现如下步骤：

在确定所述第一通信设备为第一网络的合法设备的情况下，发送第二信息，其中，所述第二信息包括如下至少一项：

用于第一数据通道建立的相关信息；

第二指示信息；

第一服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一数据通道为第一网络中的数据通道；

第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互；

所述第一数据通道用于第一通信设备请求与第一网络相关的证书；

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书。

其中，在通信设备 1600 表现为上述方法实施例中的第三通信设备时，计算机程序 16011 被处理器 1602 执行时实现如下步骤：

确定第三信息；

发送第三信息；

其中，所述第三信息包括如下至少一项：

第二认证服务器的索引信息与所述第二认证服务器的地址相关信息的映射信息；

所述第二认证服务器的地址相关信息。

可选的，所述发送所述第二认证服务器的相关信息，包括：

满足第三条件的情况下，发送所述第二认证服务器的相关信息；

所述第三条件包括如下至少一项：

所述第三通信设备与所述第二认证服务器间相互认证通过；

所述第三通信设备与第一网络间相互认证通过。

其中，在通信设备 1600 表现为上述方法实施例中的第四通信设备时，计算机程序 16011 被处理器 1602 执行时实现如下步骤：

获取第二信息；

根据所述第二信息，执行第二操作；

其中，所述第二信息包括如下至少一项：

第一终端路由选择策略；

默认 DNN 信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

可选的，所述第二操作包括以下至少一项：

建立第一数据通道，且所述第一数据通道满足至少以下之一：所述第一数据通道用于第一通信设备与第一服务器间的交互，所述第一数据通道用于第一通信设备请求与第一网络相关的证书，所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

向第一服务器请求配置与第一网络相关的证书；

向第二认证服务器请求配置与第一网络相关的证书；

拒绝应用层除了目标第一服务器和/或证书下载应用之外访问请求或数据发送请求；

仅允许目标为第一服务器和/或证书下载应用的访问请求或数据发送请求。

其中，在通信设备 1600 表现为上述方法实施例中的第五通信设备时，计算机程序 16011 被处理器 1602 执行时实现如下步骤：

发送第二信息，其中，所述第二信息包括如下至少一项：

第一终端路由选择策略；

默认 DNN 信息设置为空；

默认切片信息设置为空；

用于第一数据通道建立的相关信息；

第二指示信息；

第三指示信息；

第一服务器的地址相关信息；

第二认证服务器的地址相关信息；

其中，所述第一服务器为能够配置与第一网络相关的证书的服务器；

所述第一终端路由选择策略用于访问第一服务器或证书下载应用；

所述第一数据通道为第一网络中的数据通道；

所述第二指示信息用于指示以下至少一项：

所述第一数据通道用于第一通信设备与第一服务器间的交互，

所述第一数据通道用于第一通信设备请求与第一网络相关的证书，

所述第一数据通道用于向第一通信设备配置与第一网络相关的证书；

所述第三指示信息用于指示以下至少一项：仅允许受限服务，仅允许控制面，不允许用户面，仅允许访问第一服务器，仅允许证书下载应用。

可选的，在满足第四条件的情况下，执行确定第二信息相关操作和/或发送第二信息；

其中，所述第四条件包括：

终端接入第一网络的受限服务或接收到终端发送的第一指示信息；

确认终端初始认证通过或确认所述终端通过所述第二认证服务器的认证；

确认所述第一通信设备是非仿冒设备；

确认所述终端为第一网络的合法设备或终端是合法设备列表中的通信设备；

确认终端允许被配置所述第一网络相关的证书。

通信设备 1600 能够实现上述方法实施例中通信设备实现的各个过程，为避免重复，这里不再赘述。

本发明实施例还提供一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现上述任一接入控制方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。其中，所述的计算机可读存储介质，如只读存储器（Read-Only Memory, ROM）、随机存取存储器（Random Access Memory, RAM）、磁碟或者光盘等。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

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上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端（可以是手机，计算机，服务器，空调器，或者网络设备等等）执行本发明各个实施例所述的方法。

上面结合附图对本发明的实施例进行了描述，但是本发明并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本发明的启示下，在不脱离本发明宗旨和权利要求

所保护的范围内情况下，还可做出很多形式，均属于本发明的保护之内。