

认证和/或密钥管理方法、第一设备、终端及通信设备

相关申请的交叉引用

本申请基于申请号为 202111681982.1、申请日为 2021 年 12 月 31 日的中国专利申请和申请号为 202210701819.5、申请日为 2022 年 06 月 20 日的中国专利申请提出，并要求上述中国专利申请的优先权，上述中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本申请涉及通信技术领域，尤其是指一种认证和/或密钥管理方法、第一设备、终端及通信设备。

10 背景技术

目前有基于 5G（第五代移动通信技术）中的 3GPP 凭证为上层应用提供认证和密钥管理能力的架构和流程，包括 AKMA（Authentication and Key Management for Applications，应用层认证和密钥管理）的基本网络模型、AKMA 推衍和锚定流程及 AKMA 应用密钥（ K_{AF} ）的推衍过程，如图 1 至图 4 所示。

当 UE（User Equipment，用户设备，也可以称为终端或者用户）需要同时与多个 AF（Application Function，应用功能）使用 AKMA 生成应用层共享密钥时，存在以下问题：如果 AF 不支持 AKMA，则无法使用如图 4 所示的 AKMA 应用密钥推衍过程生成 UE 和 AF 之间的应用密钥；如果所有 AF 均属于同一个信任域，一个 UE 去与每个 AF 建立 AKMA 时，会导致 AUSF（Authentication Server Function，认证服务器功能）、AAnF（AKMA Anchor Function，AKMA 锚点功能）为每个 UE 和 AF 之间分别生成 K_{AKMA} （AKMA Anchor Key，AKMA 锚点密钥）和 K_{AF} （AKMA Application Key，AKMA 应用密钥），消耗 AUSF 和 AAnF 资源，产生网络宽带消耗，攻击者甚至可使用恶意 UE 故意发起 AKMA 过程，造成对 AUSF 和 AAnF 的资源消耗。

发明内容

为解决相关技术问题，本申请实施例提供一种认证和/或密钥管理方法、第一设备、终端及通信设备。

本申请实施例的技术方案是这样实现的：

本申请实施例提供一种认证和/或密钥管理方法，所述方法包括：

第一设备接收 UE 发起的会话建立请求消息，所述请求消息中携带密钥标识；

5 所述第一设备根据所述密钥标识获取与所述 UE 之间的第一密钥。

上述方案中，所述方法还包括：所述第一设备基于所述第一密钥，为第二设备生成所述 UE 与第二设备之间的第二密钥。

上述方案中，所述第一设备基于所述第一密钥，为第二设备生成所述 UE 与第二设备之间的第二密钥，包括：

10 所述第一设备基于所述第一密钥和所述第二设备的标识信息生成第二密钥。

上述方案中，所述方法还包括：

所述第一设备接收所述 UE 基于第三密钥保护的数据，并将所述数据发送给第二设备，所述第三密钥是所述 UE 生成的，与所述第一密钥相同；

15 和/或，所述第一设备接收第二设备发送的数据，基于所述第一密钥对所述数据进行保护，并将所述数据发送给所述 UE。

上述方案中，所述根据所述密钥标识获取与所述 UE 之间的第一密钥，包括：

20 所述第一设备根据所述密钥标识，获取本地该密钥标识对应的第一密钥；

或者，所述第一设备根据所述密钥标识，从 AAnF 获取该密钥标识对应的第一密钥。

上述方案中，所述方法还包括：所述第一设备为所述 UE 提供所述 UE 能够访问的第二设备列表。

25 上述方案中，所述方法还包括：所述第一设备与 UE 建立 TLS（传输层安全）安全通道。

上述方案中，所述第一设备与所述 UE 建立 TLS 安全通道，包括：

所述第一设备根据所述第一密钥或所述第一密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。

30 上述方案中，所述方法还包括：

所述第一设备向 UE 发送第一保护数据，所述第一保护数据包括所述第一设备基于所述第一密钥或所述第一密钥的衍生密钥保护的数据。

上述方案中，所述方法还包括：

35 所述第一设备接收 UE 发送的、基于所述第三密钥或第三密钥的衍生密钥保护的数据，其中所述第三密钥为 UE 生成的、与所述第一密钥相同的密钥。

上述方案中，所述第一设备用于代理一组 AF/AS（Application Server，应用服务器）或代理处于同一信任域的 AF/AS。

上述方案中，所述第一设备包括 AAP/AP（AAP 是 AKMA Application Proxy（AKMA 应用代理）或 AKMA Authentication proxy（AKMA 认证代理）的缩写，AP 是 Authentication proxy（认证代理）的缩写）。

本申请实施例还提供一种认证和/或密钥管理方法，所述方法包括：

5 UE 向所述第一设备发送会话建立请求消息，所述请求消息中携带密钥标识；

所述 UE 接收所述第一设备发送的第一保护数据，所述第一保护数据包括所述第一设备基于第一密钥或第一密钥的衍生密钥保护的数据，所述第一密钥是所述第一设备根据所述密钥标识获取得到的。

10 上述方案中，所述方法还包括：

所述 UE 生成与所述第一密钥相同的第三密钥，向所述第一设备发送基于所述第三密钥或第三密钥的衍生密钥保护的数据，以使所述第一设备将所述数据发送给第二设备；

和/或，所述 UE 生成与所述第二密钥相同的第四密钥，接收所述第二设备发送的第二保护数据，所述第二保护数据包括所述第二设备基于所述第二密钥保护的数据，所述第二密钥是所述第一设备基于所述第一密钥，为所述第二设备生成的；

15 和/或，所述 UE 接收所述第一设备基于所述第一密钥保护并转发的数据。

20 上述方案中，所述方法还包括：所述 UE 从所述第一设备获取所述 UE 能够访问的第二设备列表。

上述方案中，所述方法还包括：所述 UE 与所述第一设备建立 TLS 安全通道。

上述方案中，所述 UE 与所述第一设备建立 TLS 安全通道，包括：

25 所述 UE 生成与所述第一密钥相同的第三密钥；

所述 UE 根据所述第三密钥或所述第三密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。

上述方案中，所述第一设备用于代理一组 AF/AS 或代理处于同一信任域的 AF/AS。

30 上述方案中，所述第一设备包括 AAP/AP。

本申请实施例还提供一种用于认证和/或密钥管理的第一设备，所述第一设备包括第一处理模块和第一获取模块；

所述第一处理模块，配置为接收 UE 发起的会话建立请求消息，所述请求消息中携带密钥标识；

35 所述第一获取模块，配置为根据所述密钥标识获取与所述 UE 之间的第一密钥。

上述方案中，所述第一设备还包括生成模块；

所述生成模块，配置为基于所述第一密钥，为第二设备生成所述 UE

与第二设备之间的第二密钥。

上述方案中，所述生成模块，还配置为基于所述第一密钥和所述第二设备的标识信息生成第二密钥。

上述方案中，所述第一处理模块，还配置为：

5 接收所述 UE 基于第三密钥保护的数据，并将所述数据发送给第二设备，所述第三密钥是所述 UE 生成的，与所述第一密钥相同；

和/或，接收第二设备发送的数据，基于所述第一密钥对所述数据进行保护，并将所述数据发送给所述 UE。

上述方案中，所述第一获取模块，还配置为：

10 根据所述密钥标识，获取本地该密钥标识对应的第一密钥；

或者，根据所述密钥标识，从 AAnF 获取该密钥标识对应的第一密钥。

上述方案中，所述第一处理模块，还配置为为所述 UE 提供所述 UE 能够访问的第二设备列表。

15 上述方案中，所述第一处理模块，还配置为与所述 UE 建立 TLS 安全通道。

上述方案中，所述第一处理模块，还配置为根据所述第一密钥或所述第一密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。

20 上述方案中，所述第一处理模块，还配置为向 UE 发送第一保护数据，所述第一保护数据包括所述第一设备基于所述第一密钥或所述第一密钥的衍生密钥保护的数据。

上述方案中，所述第一处理模块，还配置为接收所述 UE 发送的、基于所述第三密钥或第三密钥的衍生密钥保护的数据，其中所述第三密钥为 UE 生成的、与所述第一密钥相同的密钥。

25 上述方案中，所述第一设备用于代理一组 AF/AS 或代理处于同一信任域的 AF/AS。

上述方案中，所述第一设备包括 AAP/AP。

本申请实施例还提供一种用于认证和/或密钥管理的终端，所述终端包括第二处理模块和第一接收模块：

30 所述第二处理模块，配置为向所述第一设备发送会话建立请求消息，所述请求消息中携带密钥标识；

所述第一接收模块，配置为接收所述第一设备发送的第一保护数据，所述第一保护数据包括所述第一设备基于所述第一密钥或第一密钥的衍生密钥保护的数据，所述第一密钥是所述第一设备根据所述密钥标识获取到的。
35

上述方案中，所述终端还包括：

第三处理模块，配置为生成与所述第一密钥相同的第三密钥，向所述第一设备发送基于所述第三密钥或第三密钥的衍生密钥保护的数据，以使

所述第一设备将所述数据发送给第二设备;

第四处理模块,配置为生成与所述第二密钥相同的第四密钥;

第二接收模块,配置为:

接收所述第二设备发送的第二保护数据,所述第二保护数据包括所述
5 第二设备基于所述第二密钥保护的数据,所述第二密钥是所述第一设备基
于所述第一密钥,为所述第二设备生成的;

和/或,接收所述第一设备基于所述第一密钥保护并转发的数据。

上述方案中,所述终端还包括:第二获取模块,配置为从所述第一设
备获取所述 UE 能够访问的第二设备列表。

10 上述方案中,所述第二处理模块,还配置为与所述第一设备建立 TLS
安全通道。

上述方案中,所述第二处理模块,还配置为:

生成与所述第一密钥相同的第三密钥;

根据所述第三密钥或所述第三密钥的衍生密钥生成所述 TLS 安全通道
15 的预主密钥或外部预共享密钥。

上述方案中,所述第一设备用于代理一组 AF/AS 或代理处于同一信任
域的 AF/AS。

上述方案中,所述第一设备包括 AAP/AP。

本申请实施例还提供一种通信设备,包括存储器、处理器及存储在所
20 述存储器上并可在所述处理器上运行的程序,所述处理器执行所述程序时
实现如上所述的认证和/或密钥管理方法。

本申请实施例还提供一种计算机可读存储介质,其上存储有计算机程
序,该程序被处理器执行时实现如上所述的认证和/或密钥管理方法中的步
骤。

25 本申请的上述技术方案至少具有如下有益效果:

本申请实施例提供的认证和/或密钥管理方法、第一设备及通信设备,
在 AKMA 基本网络模型中引入 AAP/AP (也即第一设备,其中 AAP 指
AKMA 应用代理或 AKMA 认证代理,AP 指认证代理),该 AAP/AP 作为
一组或处于同一信任域的 AF/AS 的代理,或者也可以由一组或处于同一个
30 信任域的 AF/AS 中的某个 AF/AS 作为 AAP/AP,也就是说, AAP/AP 可以
替代一个或者多个 AF/AS 来申请 AKMA 应用密钥,AF/AS 是信任 AAP/AP
的,从而减少 AUSF、AAnF 为 UE 与 AF/AS 建立 AKMA 应用密钥时的资
源,减少获取 AKMA 密钥时延,满足低时延场景的业务需求;并且,还可
以解决相关技术中 AF 不支持 AKMA 基本网络模型,但仍需使用 AKMA
35 实现应用层认证和密钥提供的问题。

附图说明

- 图 1 表示相关技术中 AKMA 的基本网络模型示意图；
图 2a 表示相关技术中 AF 在核心网内的 AKMA 的参考点网络模型示意图；
5 图 2b 表示相关技术中 AF 在核心网外的 AKMA 的参考点网络模型示意图；
图 3 表示相关技术中 K_{AKMA} 推衍和锚定流程图；
图 4 表示相关技术中 AKMA 应用密钥推衍过程示意图；
图 5 表示本申请实施例提供的引入 AAP/AP 的 AKMA 网络模型示意图；
10 图 6a 表示本申请实施例提供的引入 AAP/AP 的 AF/AS 在核心网内的 AKMA 参考点网络模型示意图；
图 6b 表示本申请实施例提供的引入 AAP/AP 的 AF/AS 在核心网外的 AKMA 参考点网络模型示意图；
图 7 表示本申请实施例提供的认证和/或密钥管理方法流程图；
15 图 8 表示本申请实施例提供的认证和/或密钥管理方法的另一流程图；
图 9 表示本申请实施例提供的认证和/或密钥管理方法的示意图；
图 10 表示本申请实施例提供的另一认证和/或密钥管理方法流程图；
图 11 表示本申请实施例提供的第一设备结构示意图；
图 12 表示本申请实施例提供的终端结构示意图；
20 图 13 表示本申请实施例提供的边缘云系统下低时延场景 AAP/AP 部署的示意图。

具体实施方式

为使本申请要解决的技术问题、技术方案和优点更加清楚，下面将结合附图及具体实施例进行详细描述。

- 25 如图 5、图 6a、图 6b 所示，本申请实施例提供了引入 AAP/AP 的 AKMA 基本网络模型、引入 AAP/AP 的 AF/AS 在核心网内的 AKMA 参考点网络模型示意图、引入 AAP/AP 的 AF/AS 在核心网外的 AKMA 参考点网络模型示意图。AAP/AP 是在相关架构上新增的实体，其中，AAP 指 AKMA 应用代理（AKMA Application Proxy）或 AKMA 认证代理（Authentication proxy），AP 指认证代理（Authentication proxy），该 AAP/AP 作为一组或处于同一信任域的 AF/AS 的代理，或者也可以由一组或处于同一个信任域的 AF/AS 中的某个 AF/AS 作为 AAP/AP，该 AAP/AP 可以替代一个或者多个 AF/AS 来申请 AKMA 应用密钥，AF/AS 是信任 AAP/AP 的，各个 AF/AS 可以属于同一个信任域，如属于同一个垂直行业的一组应用。另外，可以理解，AF 是按照网络功能定义的名称，与 5G 系统其它网络功能（也可以理解为网元）类似；而 AS 是从业务层面的定义，按照业务功能划分。所以
35

AS 一般对网络层不可见，但是一般地，AF 的实现可以是 AS，也即 AF 与 AS 在某些情况下可以是等价的概念。

本申请实施例引入 AAP/AP 之后的 K_{AKMA} 推衍和锚定流程同原有的标准流程，如图 3 所示流程，UE 和 AAnF 均具有了 K_{AKMA} ，此时将进行 AKMA 应用密钥推演过程。

在 UE 和 AAP/AP 之间的通信开始之前，UE 和 AAP/AP 需要知道是否能够使用 AKMA，并且 UE 和 AAP/AP 需要知道 UE 通过 AAP/AP 能够与哪些 AF/AS 生成应用密钥。这隐含在 UE 和 AAP/AP 的具体应用中，或由 AAP/AP 向 UE 作出指示，如用户发起访问，AAP/AP 通过 Ua* 协议回复 AKMA 启动消息以及 UE 通过 AAP/AP 能够访问的 AF/AS 列表，该 AF/AS 列表中包含每个 AF/AS 的标识。其中，一个 AAP/AP 所维护的 AF/AS 的标识不重复。

如图 7 所示，本申请实施例提供一种认证和/或密钥管理方法，所述方法包括：

步骤 701：第一设备接收 UE 发起的会话建立请求消息，该请求消息中携带密钥标识；

其中，该第一设备可以包括 AAP/AP，具体可以包括运营商网络内部 AAP/AP、或运营商网络外部的 AAP/AP，当 AAP/AP 位于运营商网络外部时，AAP/AP 通过 NEF 与核心网网元通信。

该会话建立请求消息中携带的密钥标识可以为 AKMA 密钥标识 A-KID。

实际应用时，该 AAP/AP 在通过运营商网络的认证和授权后，可以通过 AKMA 密钥标识 A-KID 向 AAnF 请求 AKMA 应用密钥 K_{AF} ，AAP/AP 可作为一组或处于同一信任域的 AF/AS 的代理，或者可以由一组或处于同一信任域的 AF/AS 中的某一个 AF/AS 充当 AAP/AP 的角色，为这些 AF/AS 从 K_{AF} 推演出 AKMA 密钥。

步骤 702：所述第一设备根据密钥标识获取与 UE 之间的第一密钥。

该步骤中，第一设备根据该密钥标识获取到第一设备与 UE 之间的第一密钥，该第一密钥可以为 AKMA 应用密钥 K_{AF} ，进而第一设备可以根据该第一密钥为一组或处于同一信任域中的其它 AF/AS 推演出 AKMA 密钥。

具体地，所述根据密钥标识获取与 UE 之间的第一密钥，包括：

所述第一设备根据所述密钥标识，获取本地该密钥标识对应的第一密钥；

或者，所述第一设备根据所述密钥标识，从 AAnF 获取该密钥标识对应的第一密钥。

本申请实施例中，所述第一设备可以作为一组或处于同一信任域的 AF/AS 的代理，作为处于同一信任域的 AF/AS 的代理时，该第一设备可以基于所述第一密钥，为第二设备生成 UE 与第二设备之间的第二密钥。具体

地, 所述第一设备可以基于所述第一密钥和所述第二设备的标识信息生成第二密钥, 其中, 该第二设备与第一设备处于同一信任域。

本申请实施例中, 该第一设备与第二设备或 UE 之间进行数据传输。具体地, 所述第一设备接收 UE 基于第三密钥保护的数据, 并将所述数据发送给第二设备, 所述第三密钥是所述 UE 生成的, 与所述第一密钥相同; 和/或, 所述第一设备接收第二设备发送的数据, 基于所述第一密钥对该数据进行保护, 并将所述数据 (即基于所述第一密钥保护后的数据) 发送给所述 UE。

实际应用中, 所述第一设备可以为所述 UE 提供所述 UE 能够访问的第二设备列表, 该列表中可以包含每个第二设备的标识, 且第二设备的标识不重复。

在一实施例中, 该方法还可以包括: 所述第一设备与所述 UE 建立 TLS 安全通道; 如此, 所述第一设备与所述 UE 可以通过 TLS 安全通道进行安全传输。

本领域技术人员可以理解的是, 建立安全通道的本质实质上是: 第一设备与 UE 分别推导出对称密钥, 利用该对称密钥进行数据的加密和/或完整性保护。

在本申请实施例中, 所述第一设备与 UE 建立 TLS 安全通道, 具体可以包括: 所述第一设备根据所述第一密钥或所述第一密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。也即本申请实施例可以利用基于 AKMA 技术生成的第一密钥或其衍生密钥作为 TLS 通道建立的预共享密钥 (Pre-shared key/secret, 或 Pre shared key/secret), 推导出 TLS 安全通道的预主密钥 (Premaster key/secret) 或外部预共享密钥 (external pre-shared key/secret, PSK), (预主密钥与外部预共享密钥的概念是等价的, 为简化描述, 后文仅以预主密钥这一名称来进行说明), 后续可以根据预主密钥或预主密钥的衍生密钥对数据进行加密和/或完整性保护。这样做的好处是: 不仅巧妙地利用 AKMA 机制生成的第一密钥或其衍生密钥解决 TLS 通道预共享密钥设置的问题, 同时也利用 TLS 安全通道机制有效保证了第一设备与 UE 之间通信的安全性。该方案无需额外的复杂操作, 也无需对设备进行较大改进, 方案简单易实现, 易于大规模部署与推广。

在一些实施方式中, 该方法还可以包括:

所述第一设备向 UE 发送第一保护数据, 所述第一保护数据包括所述第一设备基于所述第一密钥或所述第一密钥的衍生密钥保护的数据。

在一些实施方式中, 该方法还可以包括:

所述第一设备接收所述 UE 发送的、基于第三密钥或第三密钥的衍生密钥保护的数据, 所述第三密钥为 UE 生成的、与所述第一密钥相同的密钥。

若所述第一设备与 UE 是利用 TLS 安全通道来保护通信安全的, 那么这里的第一密钥或所述第一密钥的衍生密钥也即为 TLS 通道的预主密钥或

预主密钥的衍生密钥，进而利用预主密钥或预主密钥的衍生密钥来进行数据的安全保护。

同理，若所述第一设备与 UE 是利用 TLS 安全通道来保护通信安全的，那么这里的第三密钥或第三密钥的衍生密钥即为 TLS 通道的预主密钥或其衍生密钥，进而利用预主密钥或预主密钥的衍生密钥来进行数据的安全保护。

这里的衍生密钥，可以理解为基于第一密钥/第三密钥进行一次或多次衍生，所得到的密钥。第一密钥经过 n 次衍生后的衍生密钥可以作为 TLS 通道的预共享密钥，第一密钥经过 m 次衍生后的衍生密钥可以作为 TLS 通道的预主密钥，第三密钥的衍生密钥与第一密钥的衍生密钥类似。

下面结合实际网络部署描述本提案提供的技术方案：

如图 8、9 所示，本申请实施例提供一种认证和/或密钥管理方法，所述方法包括：

步骤 801：AAP/AP 接收 UE 发起的会话建立请求消息，该会话建立请求消息中携带 AKMA 密钥标识；

其中，A-KID 的全称为 AKMA Key Identifier，AKMA 密钥标识，简称 AKMA 密钥标识。

具体地，实际应用时，该步骤之前，可以从 K_{AUSF} 推导出 K_{AKMA} 和 A-KID。

当 UE 启动与 AAP/AP 的通信时，在 Application Session Establishment Request（即应用层会话建立请求）消息中包括 A-KID 参数，UE 可能在发送该消息之前或之后推导出 K_{AKMA} 和/或 K_{AF} 。

步骤 802：根据 AKMA 密钥标识获取与 UE 之间的 K_{AF} ；

实际应用中，该 AAP/AP 可以选择一个 AAnF 发送密钥请求消息，接收所述 AAnF 响应消息中携带的 AKMA 应用密钥 K_{AF} ；

其中，若 AAP/AP 中没有与 A-KID 相关联的激活上下文，AAP/AP 会选择一个 AAnF，并向 AAnF 发送 Naanf_AKMA_ApplicationKey_Get Request 消息（即密钥请求消息）请求 UE 的 K_{AF} 。AAP/AP 可以按照相关技术定义的流程选择一个 AAnF。

其中，密钥请求消息中该携带 A-KID 和 AF/AS 标识（比如 AF_ID）。AF_ID 可以包括 AF 的 FQDN（Fully Qualified Domain Name，全限定域名）和安全协议标识符，该安全协议标识符可以表示为 Ua^* 协议标识符，其中 Ua^* 协议标识符用于标识 AAP/AP 与 UE 之间使用的安全协议。

实际应用时，AAnF 可以根据配置的本地策略，或 NRF（网络存储库功能）提供的授权信息或策略，确认是否向 AAP/AP 提供服务。具体地，AAnF 确认是否向 AAP/AP 提供服务，可以包括：

所述 AAnF 根据 AF/AS 标识检查所述 AAnF 能否向 AAP/AP 提供服务；检查结果为所述 AAnF 能向 AAP/AP 提供服务时，根据所述 A-KID 查

找所述 AAnF 是否存在有效的 K_{AKMA} ;

所述 AAnF 中存在有效的 K_{AKMA} 时, 确定出用户能被授权使用的 AKMA;

所述 AAnF 中没有有效的 K_{AKMA} 时, 发出错误响应。

- 5 根据图 9 可知, 如果 AAnF 没有 K_{AF} 的话, 则 AAnF 由 K_{AKMA} 推衍得到 UE 的 AKMA 应用密钥 K_{AF} 。

具体推衍 K_{AF} 的过程可以根据相关技术中的定义执行, 本申请实施例不再赘述。

- 10 如图 9 所示, AAnF 可以向 AAP/AP 发送 Naanf_AKMA_ApplicationKey_Get Response 消息 (即密钥响应消息), 该密钥响应消息中携带 K_{AF} 和生命周期, 即 AAP/AP 接收 AAnF 发送的密钥响应消息中携带的 UE 的 AKMA 应用密钥 K_{AF} 和生命周期。

步骤 803: 向 UE 发送应用层会话建立响应消息。

- 15 将图 8 结合图 9 可以看出, AAP/AP 向 UE 发送 Application Session Establishment Response (即应用层会话建立响应) 消息, 如果图 9 中第 4 步的信息中表明了 AKMA 密钥请求失败, 则 AAP/AP 应拒绝应用会话建立请求, 并在本步骤中携带错误原因。之后, UE 可能会向 AAP/AP 发起新的应用会话建立请求, 携带最新的 A-KID。

- 20 实际应用时, 当 AAP/AP 位于运营商网络外部时, AAP/AP 可以通过 NEF (Network Exposure Function, 网络开放功能) 从 AAnF 获得 K_{AF} 和生命周期。

- 25 UE 和 AAP/AP 之间拥有 K_{AF} 之后, AAP/AP 可基于为 AAP/AP 所关联的 AF/AS 推演密钥, 如将 K_{AF} 和 AF/AS 的身份标识作为推演 UE 和 AF/AS 之间应用密钥的输入。UE 基于同样的算法生成 UE 和 AF/AS 之间的应用密钥。当 UE 向 AF/AS 发送应用请求时, AF/AS 可向 AAP/AP 请求应用密钥, 然后与 UE 之间基于该密钥进行后续认证或会话保护。

- 30 实际应用时, AAP/AP 也可不为 AF/AS 推演单独的密钥, 当 UE 与 AF/AS 通信时, 可以将 AF/AS 的标识携带在业务消息发送给 AAP/AP, 由 AAP/AP 转发给 AF/AS。由于 UE 和 AAP/AP 之间可基于进行认证和传输数据保护, 而 AAP/AP 和 AF/AS 之间互相信任, 可使用安全协议通信, 所以可实现 UE 到 AAP/AP、AAP/AP 到 AF/AS 之间的逐跳的应用层安全保护, 从而实现 UE 到每个 AF/AS 的数据传输安全。

- 35 本申请实施例提供的认证和/或密钥管理方法, 在 AKMA 基本网络模型中引入 AAP/AP, 该 AAP/AP 作为一组或处于同一信任域的 AF/AS 的代理, 或者也可以由一组或处于同一个信任域的 AF/AS 中的某个 AF/AS 作为 AAP/AP, 也就是说, AAP/AP 可以替代一个或者多个 AF/AS 来申请 AKMA 应用密钥, AF/AS 是信任 AAP/AP 的, 从而减少 AUSF、AAnF 为 UE 与 AF/AS 建立 AKMA 应用密钥时的资源, 减少获取 AKMA 密钥时延, 满足

低时延场景的业务需求。

如图 10 所示,本申请实施例还提供一种认证和/或密钥管理方法,所述方法包括:

5 步骤 1001: UE 向第一设备发送会话建立请求消息,该请求消息中携带密钥标识;

其中,该第一设备可以包括 AAP/AP,具体可以包括运营商网络内部 AAP/AP、或运营商网络外部的 AAP/AP,当 AAP/AP 位于运营商网络外部时, AAP/AP 可以通过 NEF 与核心网网元通信。

10 步骤 1002: 所述 UE 接收第一设备发送的第一保护数据;
具体地,该第一保护数据包括所述第一设备基于第一密钥或第一密钥的衍生密钥保护的数据,所述第一密钥是所述第一设备根据密钥标识获取得到的,该第一密钥可以为 AKMA 应用密钥 K_{AF} 。

对于第一设备,其作为一组或处于同一信任域的 AF/AS 的代理,获取到第一密钥后,可为这些 AF/AS 从 K_{AF} 推导出 AKMA 密钥。该第一密钥是
15 所述第一设备根据所述密钥标识获取得到的,具体地,所述第一设备可以根据所述密钥标识从本地获取该密钥标识对应的第一密钥;或者,所述第一设备可以根据所述密钥标识从 AAnF 获取该密钥标识对应的第一密钥。

而对于所述 UE,所述 UE 可以生成与所述第一密钥相同的第三密钥,及生成与第二密钥相同的第四密钥,也就是说 UE 端的 AKMA 应用密钥是
20 UE 自己生成的,分别生成与第一设备、第二设备通信的第三密钥、第四密钥,且第三密钥、第四密钥分别与第一密钥、第二密钥相同,AF/AS 的 AKMA 应用密钥是 AAP/AP 生成的,如上所述,基于第一密钥和第二设备的标识信息生成第二密钥。

本申请实施例中,该第一设备与第二设备或 UE 之间进行数据传输,具体地,所述 UE 可以向所述第一设备发送基于所述第三密钥或第三密钥的衍生
25 密钥保护的数据,以使所述第一设备将所述数据发送给第二设备;

和/或,所述 UE 可以接收所述第二设备发送的第二保护数据,所述第二保护数据包括所述第二设备基于所述第二密钥保护的数据,所述第二密钥是所述第一设备基于所述第一密钥,为所述第二设备生成的;

30 和/或,所述 UE 可以接收所述第一设备基于所述第一密钥保护并转发的数据。

在一些实施方式中,该方法还可以包括:所述 UE 与所述第一设备建立 TLS 安全通道。

35 在一些实施方式中,所述 UE 与所述第一设备建立 TLS 安全通道,具体可以包括:

所述 UE 生成与所述第一密钥相同的第三密钥;

所述 UE 根据所述第三密钥或所述第三密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。UE 这一部分的内容在前文的第一

设备的内容中已经进行过阐述，在此不再赘述。

实际应用中，所述第一设备可以为 UE 提供 UE 能够访问的第二设备列表，即所述 UE 可以从所述第一设备获取 UE 能够访问的第二设备列表，该列表中可以包含每个第二设备的标识，且第二设备的标识不重复。

5 本申请实施例提供的认证和/或密钥管理方法，在 AKMA 基本网络模型中引入 AAP/AP，AAP/AP 可以替代一个或者多个 AF/AS 来申请 AKMA 应用密钥，AF/AS 是信任 AAP/AP 的，UE 通过与该 AAP/AP 的交互，获取到与 AAP/AP 之间的第一密钥，从而减少 AUSF、AAnF 为 UE 与 AF/AS 建立 AKMA 应用密钥时的资源，减少获取 AKMA 密钥时延，满足低时延场景的业务需求。

10 如图 11 所示，本申请实施例还提供一种用于认证和/或密钥管理的第一设备，所述第一设备包括第一处理模块 1101 和第一获取模块 1102；

所述第一处理模块 1101，配置为接收 UE 发起的会话建立请求消息，所述请求消息中携带密钥标识；

15 所述第一获取模块 1102，配置为根据所述密钥标识获取与所述 UE 之间的第一密钥。

在一实施例中，所述第一设备还可以包括生成模块；

所述生成模块，配置为基于所述第一密钥，为第二设备生成所述 UE 与第二设备之间的第二密钥。

20 在一实施例中，所述生成模块，还配置为基于所述第一密钥和所述第二设备的标识信息生成第二密钥。

在一实施例中，所述第一处理模块 1101，还配置为：

接收所述 UE 基于第三密钥保护的数据，并将所述数据发送给第二设备，所述第三密钥是所述 UE 生成的，与所述第一密钥相同；

25 和/或，接收第二设备发送的数据，基于所述第一密钥对所述数据进行保护，并将所述数据发送给所述 UE。

在一实施例中，所述第一获取模块 1102，还配置为：

根据所述密钥标识，获取本地该密钥标识对应的第一密钥；

或者，根据所述密钥标识，从 AAnF 获取该密钥标识对应的第一密钥。

30 在一实施例中，所述第一处理模块 1101，还配置为为所述 UE 提供所述 UE 能够访问的第二设备列表。

在一实施例中，所述第一处理模块 1101，还配置为与 UE 建立 TLS 安全通道。

35 在一实施例中，所述第一处理模块 1101，还配置为根据所述第一密钥或所述第一密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。

在一实施例中，所述第一处理模块 1101，还配置为向 UE 发送第一保护数据，所述第一保护数据包括所述第一设备基于所述第一密钥或所述第

一密钥的衍生密钥保护的数据。

在一实施例中，所述第一处理模块 1101，还配置为接收所述 UE 发送的、基于所述第三密钥或第三密钥的衍生密钥保护的数据，其中所述第三密钥为 UE 生成的、与所述第一密钥相同的密钥。

5 本申请实施例提供的第一设备，该第一设备可以替代一个或者多个 AF/AS 来申请 AKMA 应用密钥，这些 AF/AS 信任第一设备，可以属于同一个信任域，能够减少 AUSF、AAnF 为 UE 与 AF/AS 建立 AKMA 应用密钥时的资源，在一定程度上减少获取 AKMA 密钥时延，满足低时延场景的业务需求。

10 需要说明的是，本申请实施例提供的第一设备是能够执行上述认证和/或密钥管理方法的装置，则上述认证和/或密钥管理方法的所有实施例均适用于该第一设备，且均能达到相同或相似的有益效果。

如图 12 所示，本申请实施例还提供一种用于认证和/或密钥管理的终端，所述终端包括第二处理模块 1201 和第一接收模块 1202：

15 第二处理模块 1201，配置为向所述第一设备发送会话建立请求消息，所述请求消息中携带密钥标识；

第一接收模块 1202，配置为接收所述第一设备发送的第一保护数据，所述第一保护数据包括所述第一设备基于所述第一密钥保护的数据，所述第一密钥是所述第一设备根据所述密钥标识获取到的。

20 在一实施例中，所述终端还可以包括：

第三处理模块，配置为生成与所述第一密钥相同的第三密钥，向所述第一设备发送基于所述第三密钥或第三密钥的衍生密钥保护的数据，以使所述

所述第一设备将所述数据发送给第二设备；

25 第四处理模块，配置为生成与所述第二密钥相同的第四密钥；

第二接收模块，配置为：
接收所述第二设备发送的第二保护数据，所述第二保护数据包括所述第二设备基于所述第二密钥保护的数据，所述第二密钥是所述第一设备基于所述第一密钥，为所述第二设备生成的；

和/或，接收所述第一设备基于所述第一密钥保护并转发的数据。

30 在一实施例中，所述终端还可以包括：第二获取模块，配置为从所述第一设备获取所述 UE 能够访问的第二设备列表。

在一实施例中，所述第二处理模块 1201，还配置为与所述第一设备建立 TLS 安全通道。

在一实施例中，所述第二处理模块 1201，还配置为：

35 生成与所述第一密钥相同的第三密钥；

根据所述第三密钥或所述第三密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。

本申请实施例提供的终端，在 AKMA 基本网络模型中引入 AAP/AP，

AAP/AP 可以替代一个或者多个 AF/AS 来申请 AKMA 应用密钥, AF/AS 是信任 AAP/AP 的, UE 通过与该 AAP/AP 的交互, 获取到与 AAP/AP 之间的第一密钥, 从而减少 AUSF、AAnF 为 UE 与 AF/AS 建立 AKMA 应用密钥时的资源, 减少获取 AKMA 密钥时延, 满足低时延场景的业务需求。

5 需要说明的是, 本申请实施例提供的终端是能够执行上述认证和/或密钥管理方法的装置, 则上述认证和/或密钥管理方法的所有实施例均适用于该终端, 且均能达到相同或相似的有益效果。

考虑到将相关 AKMA 网络模型应用在边缘计算场景时, 一个厂商可能有多个 APP (Application, 应用程序), 这些 APP 作为 AF/AS, 如果要使用 AKMA 应用密钥作为 UE 和 APP 之间的共享密钥, 用于后续推衍保护应用层的密钥, 那么每个 APP 均需要向核心网中的 AAnF 请求 AKMA 应用密钥。对于时延敏感的业务来说, 应用层共享密钥的生成时长可能无法满足低时延要求。

如图 13 所示, 本申请实施例提供了一种边缘云系统下低时延场景 AAP/AP 部署架构, 在边缘云上部署了多个对时延要求敏感的 APP (比如 APP1、APP2 等 (这些 APP 作为 AF/AS)), 此时通过 AAP/AP 提前与核心云的 NEF、AAnF 交互获取密钥后, 所有 APP 均可使用这个安全通道, 不用每个 APP 单独去找核心云获取密钥, 以建立 UE 和 APP 之间的应用层安全通道, 可满足低时延的要求。

20 本申请实施例还提供一种通信设备, 包括存储器、处理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, 所述处理器执行所述程序时实现如上所述的认证和/或密钥管理方法实施例中的各个过程, 且能达到相同的技术效果, 为避免重复, 这里不再赘述。

本申请实施例还提供一种计算机可读存储介质, 其上存储有计算机程序, 该程序被处理器执行时实现如上所述的认证和/或密钥管理方法实施例中的各个过程, 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, 简称 ROM)、随机存取存储器 (Random Access Memory, 简称 RAM)、磁碟或者光盘等。

30 本领域内的技术人员应明白, 本申请的实施例可提供为方法、系统或计算机程序产品。因此, 本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且, 本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可读存储介质 (包括但不限于磁盘存储器和光学存储器等) 上实施的计算机程序产品的形式。

35 本申请是参照根据本申请实施例的方法、设备 (系统) 和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、

嵌入式处理机或其它可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其它可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或一个方框或多个方框中指定的功能的装置。

- 5 这些计算机程序指令也可存储在能引导计算机或其它可编程数据处理设备以特定方式工作的计算机可读存储介质中，使得存储在该计算机可读存储介质中的指令产生包括指令装置的纸制品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

- 10 这些计算机程序指令也可装载到计算机或其它可编程数据处理设备上，使得计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

- 15 以上所述是本申请的一些实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请所述原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本申请的保护范围。

权利要求书

- 1、一种认证和/或密钥管理方法，所述方法包括：
第一设备接收用户设备 UE 发起的会话建立请求消息，所述请求消息中携带密钥标识；
5 所述第一设备根据所述密钥标识获取与所述 UE 之间的第一密钥。
2、根据权利要求 1 所述的方法，其中，所述方法还包括：所述第一设备基于所述第一密钥，为第二设备生成所述 UE 与第二设备之间的第二密钥。
3、根据权利要求 2 所述的方法，其中，所述第一设备基于所述第一
10 密钥，为第二设备生成所述 UE 与第二设备之间的第二密钥，包括：
 所述第一设备基于所述第一密钥和所述第二设备的标识信息生成第二密钥。
4、根据权利要求 1 所述的方法，其中，所述方法还包括：
 所述第一设备接收所述 UE 基于第三密钥保护的数据，并将所述数据
15 发送给第二设备，所述第三密钥是所述 UE 生成的，与所述第一密钥相同；
 和/或，所述第一设备接收第二设备发送的数据，基于所述第一密钥对所述数据进行保护，并将所述数据发送给所述 UE。
5、根据权利要求 1 所述的方法，其中，所述根据所述密钥标识获取与所述 UE 之间的第一密钥，包括：
20 所述第一设备根据所述密钥标识，获取本地该密钥标识对应的第一密钥；
 或者，所述第一设备根据所述密钥标识，从应用层认证和密钥管理锚点功能 AAnF 获取该密钥标识对应的第一密钥。
6、根据权利要求 1 所述的方法，其中，所述方法还包括：所述第一
25 设备为所述 UE 提供所述 UE 能够访问的第二设备列表。
7、根据权利要求 1 所述的方法，其中，所述方法还包括：所述第一设备与所述 UE 建立传输层安全 TLS 安全通道。
8、根据权利要求 7 所述的方法，其中，所述第一设备与所述 UE 建立 TLS 安全通道，包括：
30 所述第一设备根据所述第一密钥或所述第一密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。
9、根据权利要求 1、7、8 任一所述的方法，其中，所述方法还包括：
 所述第一设备向 UE 发送第一保护数据，所述第一保护数据包括所述
 第一设备基于所述第一密钥或所述第一密钥的衍生密钥保护的数据。
35 10、根据权利要求 1、7、8 任一所述的方法，其中，所述方法还包括：

所述第一设备接收所述 UE 发送的、基于第三密钥或第三密钥的衍生密钥保护的数据，所述第三密钥为 UE 生成的、与所述第一密钥相同的密钥。

11、根据权利要求 1 所述的方法，其中，所述第一设备用于代理一组应用功能 AF/应用服务器 AS 或代理处于同一信任域的 AF/AS。

12、根据权利要求 1 所述的方法，其中，所述第一设备包括应用层认证和密钥管理 AKMA 应用代理，或认证代理，或 AKMA 认证代理。

13、一种认证和/或密钥管理方法，所述方法包括：

UE 向第一设备发送会话建立请求消息，所述请求消息中携带密钥标识；

所述 UE 接收所述第一设备发送的第一保护数据，所述第一保护数据包括所述第一设备基于第一密钥或第一密钥的衍生密钥保护的数据，所述第一密钥是所述第一设备根据所述密钥标识获取到的。

14、根据权利要求 13 所述的方法，其中，所述方法还包括：

所述 UE 生成与所述第一密钥相同的第三密钥，向所述第一设备发送基于所述第三密钥或第三密钥的衍生密钥保护的数据，以使所述第一设备将所述数据发送给第二设备；

和/或，所述 UE 生成与第二密钥相同的第四密钥，接收所述第二设备发送的第二保护数据，所述第二保护数据包括所述第二设备基于所述第二密钥保护的数据，所述第二密钥是所述第一设备基于所述第一密钥，为所述第二设备生成的；

和/或，所述 UE 接收所述第一设备基于所述第一密钥保护并转发的数据。

15、根据权利要求 13 所述的方法，其中，所述方法还包括：所述 UE 从所述第一设备获取所述 UE 能够访问的第二设备列表。

16、根据权利要求 13 所述的方法，其中，所述方法还包括：所述 UE 与所述第一设备建立 TLS 安全通道。

17、根据权利要求 13 所述的方法，其中，所述 UE 与所述第一设备建立 TLS 安全通道，包括：

所述 UE 生成与所述第一密钥相同的第三密钥；

所述 UE 根据所述第三密钥或所述第三密钥的衍生密钥生成所述 TLS 安全通道的预主密钥或外部预共享密钥。

18、根据权利要求 13 所述的方法，其中，所述第一设备用于代理一组 AF/AS 或代理处于同一信任域的 AF/AS。

19、根据权利要求 13 所述的方法，其中，所述第一设备包括 AKMA 应用代理，或认证代理，或 AKMA 认证代理。

20、一种用于认证和/或密钥管理的第一设备，所述第一设备包括第一处理模块和第一获取模块；

所述第一处理模块,配置为接收 UE 发起的会话建立请求消息,所述请求消息中携带密钥标识;

所述第一获取模块,配置为根据所述密钥标识获取与所述 UE 之间的第一密钥。

- 5 21、一种用于认证和/或密钥管理的终端,所述终端包括第二处理模块和第一接收模块:

所述第二处理模块,配置为向第一设备发送会话建立请求消息,所述请求消息中携带密钥标识;

- 10 所述第一接收模块,配置为接收所述第一设备发送的第一保护数据,所述第一保护数据包括所述第一设备基于第一密钥保护的数据,所述第一密钥是所述第一设备根据所述密钥标识获取得到的。

- 22、一种通信设备,包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的程序;所述处理器执行所述程序时实现如权利要求 1 至 12 任一项所述的认证和/或密钥管理方法,或实现如权利要求 13 至 19 任一项所述的认证和/或密钥管理方法。

- 15 23、一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现如权利要求 1 至 12 任一项所述的认证和/或密钥管理方法中的步骤,或实现如权利要求 13 至 19 任一项所述的认证和/或密钥管理方法中的步骤。

20