(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 4 月 7 日 (07.04.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/067831 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *H04W 12/06* (2021.01)

(21) 国际申请号: PCT/CN2020/119764

(22) 国际申请日: 2020 年 9 月 30 日 (30.09.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 吴义壮(**WU, Yizhuang**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李赫(**LI, He**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 雷鳌(**LEI, Ao**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (**TDIP & PARTNERS**); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

WO 2022/067831 A1

(54) **Title:** METHOD AND APPARATUS FOR ESTABLISHING SECURE COMMUNICATION

(54) 发明名称: 一种建立安全通信方法及装置

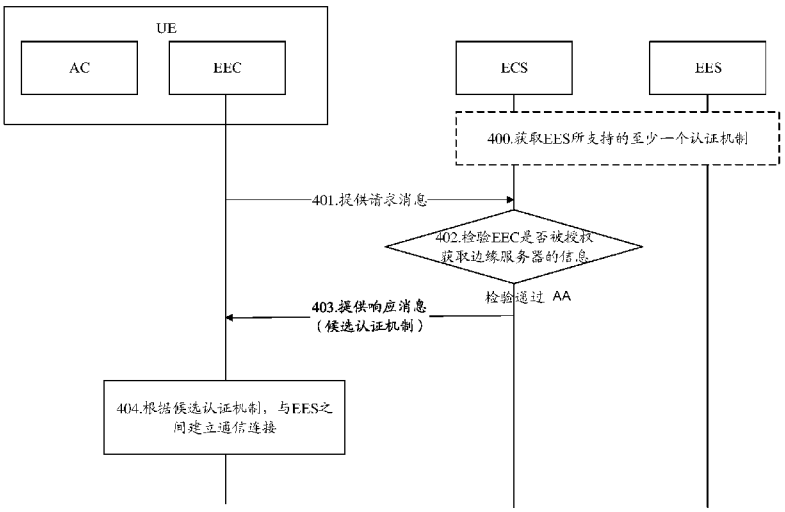

图 4

400 ACQUIRE AT LEAST ONE AUTHENTICATION MECHANISM SUPPORTED BY THE EES
401 PROVIDE A REQUEST MESSAGE
402 VERIFY WHETHER THE EEC IS AUTHORIZED TO ACQUIRE INFORMATION OF AN EDGE SERVER
403 PROVIDE A RESPONSE MESSAGE (CANDIDATE AUTHENTICATION MECHANISM)
404 ESTABLISH A COMMUNICATION CONNECTION WITH THE EES ACCORDING TO THE CANDIDATE AUTHENTICATION MECHANISM
AA VERIFICATION IS PASSED

(57) **Abstract:** A method and apparatus for establishing secure communication. The method comprises: a terminal device receiving a first message from a first network element, the first message comprising an identifier of a second network element and first indication information, and the first indication information being used for indicating a candidate authentication mechanism associated with the second network element; and the terminal device establishing a communication connection with the second network element on the basis of the candidate authentication mechanism. By using the method and apparatus in the embodiments of the present application,

[见续页]

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

a terminal device can acquire an authentication mechanism of a dynamically configured second network element, so as to meet the requirement of establishing a secure communication connection under an MEC architecture by means of authentication.

(57) 摘要：一种建立安全通信方法及装置，该方法包括：终端设备接收来自第一网元的第一消息，所述第一消息包括第二网元的标识以及第一指示信息，所述第一指示信息用于指示与所述第二网元关联的候选认证机制；所述终端设备基于所述候选认证机制，与所述第二网元之间建立通信连接。采用本申请实施例的方法及装置，终端设备可以获取动态配置的第二网元的认证机制，以满足MEC架构下通过认证以建立安全的通信连接的需求。

一种建立安全通信方法及装置

技术领域

本申请涉及通信技术领域，尤其涉及一种建立安全通信方法及装置。

背景技术

多接入边缘计算（multi-access edge computing，MEC），可利用无线接入网络就近为电信用户提供信息技术（information technology，IT）所需服务和云端技术功能，从而创造出一个具备高性能、低延迟与高带宽的电信级服务环境，加速网络中各项内容、服务及应用的快速下载，让用户享有不间断的高质量网络体验。

其中，在第三代合作伙伴计划（3rd generation partnership project，3GPP）的 SA6 的 MEC 研究中，如图 1 所示，定义了如下结构模型。

边缘数据网络（edge data network，EDN）上动态的部署有一个或者多个边缘使能服务器（edge enabler server，EES）和一个或者多个边缘应用服务器（edge application server，EAS）。用户设备（user equipment，UE）中包括应用客户端（application client，AC）和边缘使能客户端(edge enabler client，EEC)。独立于用户设备和 EDN 之外，MEC 架构中还包括一个或者多个边缘配置服务器 (edge configuration server，ECS)。

为了保护客户端与服务器间（如 AC 与 EAS 之间、EEC 与 ECS 之间或 EEC 和 EES 之间）的通信安全，通常在客户端与服务器间进行应用层数据传输前，客户端与服务器之间需要进行认证。

目前，常见的认证机制包括用于应用的认证和密钥管理（authentication and key management for applications，AKMA）机制、通用引导架构（generic bootstrapping architecture，GBA）机制以及基于证书的认证机制等。

在 MEC 架构下，由于 EES、EAS 和 ECS 都是动态部署的，所以 UE 无法获知这些动态部署的 EES、EAS 和 ECS 所支持的认证机制。进而 UE 无法准确的使用相应的认证机制发起与 EES、EAS 或者 ECS 之间的连接建立请求。

因此，当前亟需一种能够适用于 MEC 架构下，在客户端与服务器之间通过认证以建立安全的通信连接的方法。

发明内容

本申请提供一种建立安全通信方法及装置，用以解决 MEC 架构下，无法预先获知服务器支持的认证机制，以建立安全的通信连接的问题。

第一方面，提供一种建立安全通信方法，该方法包括：终端设备接收来自第一网元的第一消息，所述第一消息中包括第二网元的标识以及第一指示信息，所述第一指示信息用于指示第二网元关联的候选认证机制；终端设备基于候选认证机制，与第二网元之间建立通信连接。

通过上述方法，终端设备可以获取动态部署的第二网元的候选认证机制；且基于上述候选认证机制与第二网元之间建立通信连接。可选的，第二网元可以为 ECS，EES 或 EAS 等，可满足 MEC 架构的需求。

可选的，该方法还包括：终端设备向第一网元发送第二消息，第一消息为第二消息的响应消息。

通过上述方法，终端设备可先向第一网元发送第二消息，之后第一网元向终端设备发送第二消息的响应消息，即第一消息。也就是，终端设备在需要获取第二网元对应的候选认证机制时，可直接向第一网元请求，从而使得终端设备可以获取动态部署的第二网元的候选认证机制。

在一种设计中，所述候选认证机制为终端设备与第二网元之间建立通信连接时使用的至少一个第一认证机制；所述第二消息中包括所述终端设备所支持的至少一个第二认证机制。

通过上述方法，第二网元在接收到第二消息时，可直接获取该第二消息中终端设备所支持的至少一个认证机制；第二网元根据该终端设备所支持的至少一个认证机制和第二网元所支持的至少一个认证机制，确定候选认证机制，从而保证所述候选认证机制是终端设备和第二网元都支持的。同时，终端设备在接收到候选认证机制时，可直接利用该候选认证机制建立通信连接即可，终端设备无需再做进一步处理，减少了终端设备的处理复杂度，节省电量。

可选的，上述所述第二消息中包括所述终端设备接入所述第二网元所使用的网络类型。如此，上述第二网元确定候选认证机制时，还可以考虑终端设备接入所述第二网元所使用的网络类型，从而保证所选择的候选认证机制是网络也支持的。如此设计，主要是考虑，有些认证机制是需要网络支持的，比如，对于 AKMA 认证机制，需要 5G 网络的支持；而对于 GBA 认证机制，需要 4G 网络的支持。

可选的，上述第二消息中还包括至少一个第二认证机制中的优先级信息。第二网元在确定候选认证机制时，还可以考虑终端设备和第二网元所支持的认证机制的优先级，优先选择两者都支持的高优先级的认证机制建立通信连接。

可选的，所述终端设备基于所述候选认证机制，与所述第二网元之间建立通信连接，包括：所述终端设备从所述至少一个第一认证机制中确定目标认证机制；所述终端设备生成与所述目标认证机制对应的第一密钥以及第一密钥标识；所述终端设备向所述第二网元发送通信连接建立请求，所述通信连接建立请求中包括所述第一密钥标识。可选的，所述第一密钥标识可以用于标识所述终端设备。

一种可能的涉及中，所述目标认证机制对应的第一密钥以及第一密钥标识可能事先已经生成并保存在终端设备中，则这种情况下，终端设备之间获取所述目标认证机制对应的第一密钥标识符即可。即所述终端设备基于所述候选认证机制，与所述第二网元之间建立通信连接，包括：所述终端设备从所述至少一个第一认证机制中确定目标认证机制；所述终端设备获取与所述目标认证机制对应的第一密钥标识；所述终端设备向所述第二网元发送通信连接建立请求，所述通信连接建立请求中包括所述第一密钥标识。

通过上述方法，由于终端设备基于候选认证机制，可以获取动态部署的第二网元的认证机制，从而使得终端设备在上述通信连接建立请求中，可以直接携带候选认证机制对应的密钥标识，直接建立通信连接。相对于，终端设备不能获取动态部署的第二网元的认证机制，需要先向第二网元发送通信连接建立请求，然后第二网元指示第二网元支持的认证机制；终端设备再向第二网元发送通信连接建立请求，该请求中再携带第二网元所支持认证机制的密钥标识的过程，可减少信令开销，降低连接时延等。

在另一种设计中，所述候选认证机制为所述第二网元所支持的至少一个第三认证机制。

通过上述方法，第二网元直接将第二网元所支持的认证机制发送给终端设备，终端设备基于该第二网元所支持的认证机制与终端设备所支持的认证机制，再选择目标认证机制建立通信连接。这样，第二网元侧无需进一步判断，减少第二网元的工作量。进一步，在上述两者通信的过程中，无需再传输终端设备所支持的认证机制，减少了信令开销。

可选的，所述终端设备基于所述候选认证机制，与所述第二网元之间建立通信连接，包括：所述终端设备基于所述至少一个第三认证机制和辅助信息，确定目标认证机制，所述辅助信息中包括以下至少一项：所述终端设备所支持的至少一个第二认证机制，和所述终端设备接入所述第二网元所使用的网络类型；所述终端设备生成与所述目标认证机制对应的第一密钥以及第一密钥标识；所述终端设备向所述第二网元发送通信连接建立请求，所述通信连接建立请求包括所述第一密钥标识。

通过上述方法，终端设备在通信连接建立请求中可直接携带目标认证机制对应的密钥，发送一次通信连接建立请求，即可成功建立两者间的通信连接。相对比需要多次发送通信连接建立请求的方案，可减少信令开销，降低连接时延等。

可选的，终端设备还可以考虑优先级信息，比如所述至少一个第二认证机制的优先级信息和所述至少一个第三认证机制的优先级信息等，确定候选认证机制。如此，可保证优先选择优先级高的认证机制，建立通信连接。可选的，在此设计中，上述第一消息还可以包括：第二网元所支持的至少一个认证机制中的优先级信息等。

可选的，在上述两种设计中，上述目标认证机制是与网络类型对应的认证机制。比如，终端设备当前接入的网络为 5G 网络，则目标认证机制可以为 AKMA 机制。或者，终端设备当前接入的网络为 4G 网络，则目标认证机制可以为 GBA 机制等。

可选的，在上述两种设计中，还可以包括：所述终端设备根据所述第一密钥以及所述第二网元的标识，生成第二密钥；所述终端设备使用所述第二密钥对所述通信连接建立请求进行安全保护，以生成第一消息认证码 MAC；其中，所述通信连接建立请求还包括所述第一 MAC。

在上述方法中，第二网元在接收到通信连接建立请求后，可获取通信连接建立请求中的第一密钥标识，根据第一密钥标识获取第二密钥；根据第二密钥生成第二 MAC；若第一 MAC 和第二 MAC 相同，则验证通过，两者间可建立通信连接。后续，终端设备与第二网元间也可以采用第二密钥进行其它安全保护，不作限定，从而保证两者间建立安全的通信连接。

可选的，所述方法还包含：所述终端设备接收第二网元发送的通信连接建立响应。所述通信连接建立响应使用所述第二密钥进行安全保护。例如，所述通信连接建立响应中包括第三 MAC。所述第三 MAC 是所述第二网元基于所述第二密钥对所述连接建立响应中的部分或者全部信息计算得到的。相应地，所述终端设备还基于所述第二密钥对所述第三 MAC 进行校验，以确定通信连接建立响应没有被篡改，间接地也验证了所述第二网元为合法的网元。

可选的，所述第一网元为边缘配置服务器 ECS，所述第二网元为边缘使能服务器 EES，终端设备可以通过 ECS 获取 EES 对应的候选认证机制；或者，所述第一网元为 EES，所述第二网元为边缘应用服务器 EAS，终端设备可以通过 EES 获取 EAS 对应的候选认证机

制；或者，所述第一网元为接入和移动性管理功能 AMF 或者会话管理功能 SMF，所述第二网元为 ECS，终端设备可以通过 AMF 或 SMF 获取 ECS 对应的候选认证机制。在该设计中，上述第一消息可以为非接入层 NAS 消息。比如，所述第一消息为所述终端设备请求注册的响应消息，或者所述终端设备请求建立协议数据单元 PDU 会话的响应消息等，不作限定。

通过上述方法，可实现终端设备获取动态部署的 EES、EAS 或 ECS 的候选认证机制，满足 MEC 架构的需求。

可选的，所述候选认证机制包括以下至少一项：应用的认证和密码管理 AKMA 服务，通用引导架构 GBA 服务，证书机制或其它用于终端设备与第二网元间进行认证的机制等。

通过上述方法，在不同的认证机制下，终端设备均可以获取动态部署的第二网元对应的候选认证机制，实现灵活，适用范围广。

第二方面，提供一种建立安全通信方法，包括：第一网元确定候选认证机制；所述第一网元向终端设备发送第一消息，所述第一消息中包括第二网元的标识以及第一指示信息，所述第一指示信息用于指示第二网元关联的所述候选认证机制，所述候选认证机制用于所述终端设备与所述第二网元间建立通信连接。

通过上述方法，第一网元可以将第二网元对应的候选认证机制指示给终端设备。上述第二网元可以为动态部署的，比如 MEC 架构中的 ECS，EES 或 EAS 等，从而使得终端设备可以动态获取第二网元的候选认证机制，满足 MEC 架构的需求。

可选的，上述方法还包括：所述第一网元接收来自所述终端设备的第二消息，所述第一消息为所述第二消息的响应消息。

通过上述方法，终端设备可先向第一网元发送第二消息，之后第一网元向终端设备发送第二消息的响应消息，即第一消息。也就是，终端设备在需要获取第二网元对应的候选认证机制时，可直接向第一网元请求，从而使得终端设备可以获取动态部署的第二网元的候选认证机制。

在一种可能的实现方式中，所述候选认证机制为所述终端设备与所述第二网元之间建立通信连接时使用的至少一个第一认证机制，所述第一网元确定候选认证机制，包括：所述第一网元根据所述第二网元所支持的至少一个第三认证机制和辅助信息，确定候选认证机制，所述辅助信息包括以下至少一项：终端设备所支持的至少一个第二认证机制，和所述终端设备接入所述第二网元所使用的网络类型。

通过上述方法，第一网元可以将终端设备和第二网元间建立通信连接时所使用的认证机制直接指示给终端设备，终端设备无需再进一步做判断，降低终端设备侧的处理复杂度，节省电量。

可选的，第二网元在确定候选认证机制时，还可以考虑终端设备接入所述第二网元所使用的网络类型，从而使得选择的候选认证机制可以得到接入网的支持。相应的，上述第二消息中包括所述终端设备支持的至少一个第二认证机制。可选的，第二网元在确定候选认证机制时，还可以考虑优先级信息，比如，终端设备所支持的第二认证机制的优先级信息和第二网元所支持的第三认证机制的优先级信息等，从而使得所选择的候选认证机制是优先级较高的。此时，上述第二消息中还可以包括终端设备所支持的至少一个第二认证机制的优先级信息。

在另一种设计中，所述候选认证机制为所述第二网元所支持的至少一个第三认证机制。

通过上述方法，第一网元直接把第二网元支持的认证机制指示给终端设备，无需做额外处理，且终端设备也无需将自己支持的认证机制通知第一网元，降低第一网元侧的处理过程，节省信令开销。

可选的，在上述方法中，由终端设备根据第二网元支持的认证机制，确定两者间最终的目标认证机制。可选的，终端设备还可以考虑两者认证机制的优先级信息，因此，第一网元需要将自己所支持的认证机制的优先级信息通知终端设备。比如，上述第一消息中还包括所述终端设备所支持的至少一个第三认证机制的优先级信息。

针对上述两种设计，所述第一网元为边缘配置服务器 ECS，所述第二网元为边缘使能服务器 EES，终端设备可以通过 ECS 获取 EES 对应的候选认证机制；或者，所述第一网元为 EES，所述第二网元为边缘应用服务器 EAS，终端设备可以通过 EES 获取 EAS 对应的候选认证机制；或者，所述第一网元为接入和移动性管理功能 AMF 或者会话管理功能 SMF，所述第二网元为边缘配置服务器 ECS，终端设备可以通过 AMF 或 SMF 获取 ECS 对应的候选认证机制。在该设计中，上述第一消息可以为非接入层 NAS 消息。比如，所述第一消息为所述终端设备请求注册的响应消息，或者所述终端设备请求建立协议数据单元 PDU 会话的响应消息等，不作限定。

通过上述方法，可实现终端设备获取动态部署的 EES、EAS 或 ECS 的候选认证机制，满足 MEC 架构的需求。

可选的，所述候选认证机制包括以下至少一项：应用的认证和密码管理 AKMA 服务，通用引导架构 GBA 服务，证书机制或其它用于终端设备与第二网元间进行认证的机制等。

通过上述方法，在不同的认证机制下，终端设备均可以获取动态部署的第二网元对应的候选认证机制，实现灵活，适用范围广。

第三方面，本申请实施例还提供一种装置，该通信装置应用于终端设备，有益效果可参见第一方面的描述此处不再赘述。该装置具有实现上述第一方面的方法实施例中行为的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的单元。在一种可能的设计中，装置的结构中包括通信单元和处理单元，这些单元可以执行上述第一方面方法示例中的相应功能，具体参见方法实施例中的详细描述，此处不再赘述。

第四方面，本申请实施例还提供一种装置，该通信装置应用于第一网元，有益效果可参见第二方面的描述此处不作赘述。该装置具有实现上述第二方面的方法实例中行为的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。硬件或软件包括一个或多个与上述功能相对应的单元。在一个可能的设计中，装置的结构中包括通信单元和处理单元，这些单元可以执行上述第二方面方法示例中的相应功能，具体参见方法示例中的详细描述，此处不做赘述。

第五方面，本申请实施例还提供一种装置，通信装置应用于终端设备，有益效果可以参见第一方面的描述此处不再赘述。通信装置的结构中包括处理器和存储器，处理器被配置为支持终端设备执行上述第一方面方法中相应的功能。存储器与处理器耦合，其保存通信装置必要的程序指令和数据。通信装置的结构中还包括通信接口，用于与其他设备进行通信。

第六方面，本申请实施例还提供一种装置，通信装置应用于第一网元，有益效果可以参见第二方面的描述此处不再赘述。通信装置的结构中包括处理器和存储器，处理器被配

置为支持第一网元执行上述第二方面方法中相应的功能。存储器与处理器耦合，其保存通信装置必要的程序指令和数据。通信装置的结构中还包括通信接口，用于与其他设备进行通信。

第七方面，本申请还提供一种计算机可读存储介质，计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行上述第一方面的方法，或执行上述第二方面的方法。

第八方面，本申请还提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第一方面的方法，或执行上述第二方面的方法。

第九方面，本申请还提供一种计算机芯片，芯片与存储器相连，芯片用于读取并执行存储器中存储的软件程序，执行上述第一方面的方法，或执行上述第二方面的方法。

附图说明

图 1 为本申请实施例提供的 MEC 架构的一示意图；

图 2 为本申请实施例提供的 MEC 架构中通信过程的一示意图；

图 3 为本申请实施例提供的 3GPP 网络的一示意图；

图 4 为本申请实施例提供的通信方法的一流程图；

图 5 为本申请实施例提供的 ECS 获取 EES 所支持的至少一个认证机制的流程图；

图 6 为本申请实施例提供的通信方法的一流程图；

图 7 为本申请实施例提供的 EES 获取 EAS 所支持的至少一个认证机制信息的流程图；

图 8 为本申请实施例提供的通信方法的另一流程图；

图 9 为本申请实施例提供的通信方法的又一流程图；

图 10 为本申请实施例提供的 AKMA 认证的一流程图；

图 11 为本申请实施例提供的装置的一结构示意图；

图 12 为本申请实施例提供的装置的另一结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。其中，在本申请的描述中，除非另有说明，“/”表示前后关联的对象是一种“或”的关系，例如，A/B 可以表示 A 或 B；本申请中的“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，其中 A，B 可以是单数或者复数。并且，在本申请的描述中，除非另有说明，“多个”是指两个或多于两个。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a，b，或 c 中的至少一项（个），可以表示：a，b，c，a-b，a-c，b-c，或 a-b-c，其中 a，b，c 可以是单个，也可以是多个。另外，为了便于清楚描述本申请实施例的技术方案，在本申请的实施例中，采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并不限定一定不同。

此外，本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施

例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

本申请实施例提供一种多接入边缘计算（multi-access edge computing，MEC）的使能边缘应用架构，如图 1 所示，至少包含以下功能网元:

边缘应用服务器（edge application server，EAS），是部署在 EDN 中的应用服务器。其中，应用提供商可以根据需要在不同的 EDN 网络中动态实例化 EAS。

应用客户端（application client，AC），是 EAS 在终端设备侧的对等实体。AC 用于应用用户（user）从应用服务器获取应用业务。AC 是应用在终端设备中的客户端程序，AC 可以连接到云上的应用服务器获取应用业务，也可以连接到部署运行在一个或多个 EDN 中的 EAS 以获取应用业务。比如，AC 可以为安装在终端设备上的腾讯客户端，爱奇艺客户端，车联网（vehicle to everything，V2X）客户端，或关键任务（mission critical，MC）客户端等。

边缘使能服务器（edge enabler server，EES），可以为部署在 EDN 中的 EAS 提供使能能力。例如，EES 可以为 EAS 提供管理能力，可以支持边缘应用服务器 EAS 的注册，以获取 EAS 的标识和 EAS 支持的认证机制，可选的，还获取 EAS 支持的认证机制的优先级。EES 还可以为终端设备提供可用的 EAS 的标识和认证相关的信息等。其中，所述认证相关的信息用于终端设备和 EAS 之间的认证流程。进一步的，EES 还可支持将 EAS 的标识发送给 ECS。EES 部署在 EDN 中。一般情况下，EAS 注册到一个 EES 上，或者，通过管理系统将一个 EAS 的信息配置在一个 EES 上，该 EES 称为该 EAS 关联的 EES，EES 可以控制、管理、注册或配置该 EES 关联的 EAS 等。

边缘使能客户端（edge enabler client，EEC)，是 EES 在终端设备侧的对等实体。EEC 用于向 EES 注册 EEC 的信息及 AC 的信息、执行安全认证和鉴权、从 EES 获取 EAS 的标识、向 AC 提供边缘计算使能能力，如 EAS 发现服务，将 EAS 的标识返回给 AC 等。

边缘配置服务器 (edge configuration server，ECS)，负责 EDN 的配置管理，如向终端设备提供 EES 的信息。

其中，应用用户可以与应用的提供商签订服务协议，从而获得应用提供商的服务器提供的服务。应用用户可以通过登录终端设备上的 AC，通过 AC 与 EAS 连接进行通信，以使用应用提供商的服务器提供的服务。使能客户端（例如，EEC）可以为中间件层，一般位于操作系统中，或者位于 AC 与操作系统中间，也可以实现在 AC 内部。AC 可以通过应用编程接口（application program interface，API）的方式从使能客户端获取边缘使能服务。

在一种设计中，如图 2 所示，基于上述图 1 所示的 MEC 架构，AC 获取能够通信的 EAS 的流程如下:

1、边缘服务提供商根据需要动态部署 EDN 网络，在 EDN 网络中部署 EES，并根据应用提供商的需求动态实例化具体的 EAS。EAS 向 EES 发送注册流程，以便于向 EES 提供 EAS 信息。例如，EAS 身份标识，端口信息（如全量域名（fully qualified domain name，FQDN），IP 地址或统一资源标识符(uniform resource identifier，URI)等），和应用客户端的标识(application client identifier，AC ID)等。所述 EAS 信息使得 EES 能够根据 EEC 的请求提供可用的 EAS 给 EEC。

2、EDN 网络中的 EES 向 ECS 发起注册流程，以便于向 ECS 提供 EES 信息，所述 EES

信息使得 ECS 能够根据 EEC 的请求提供可用的 EES 给 EEC。进一步的，EES 还可以在注册流程中向 ECS 提供注册在 EES 上的 EAS 的信息。

3、基于上述注册流程，为了获取边缘应用服务，EEC 可首先向 ECS 请求提供边缘服务，以通过 ECS 获取可用的 EES 信息。ECS 可以根据 EEC 的请求向 EEC 发送可用的 EES 的信息。

4、EEC 根据从 ECS 获取的 EES 信息，确定通信的 EES，并与确定的 EES 建立连接，EEC 从连接的 EES 获取具体的提供边缘应用服务的 EAS 信息。

5、EEC 根据获取的 EAS 信息向 AC 发送 AC 对应的 EAS 信息。

6、AC 根据从 EEC 获取的 EAS 信息，与 EAS 建立连接以获取服务。

本申请实施例还提供一种网络架构，如图 3 所示，包括以下至少一项：终端设备，接入网，核心网，和数据网络（data network，DN）。不同接入网设备之间可通过 Xn 接口连接，接入网设备与核心网设备之间可通过 NG 接口连接。

终端设备可以简称为终端，是一种具有无线收发功能的设备，终端设备可以部署在陆地上，包括室内或室外、手持或车载；也可以部署在水面上（如轮船等）；还可以部署在空中（例如飞机、气球和卫星上等）。所述终端设备可以是手机、平板电脑、带无线收发功能的电脑、虚拟现实（virtual reality，VR）终端设备、增强现实（augmented reality，AR）终端设备、工业控制（industrial control）中的无线终端设备、无人驾驶中的无线终端设备、远程医疗中的无线终端设备、智能电网中的无线终端设备、运输安全中的无线终端设备、智慧城市中的无线终端设备、或智慧家庭中的无线终端设备等。终端设备还可以是蜂窝电话、无绳电话、会话启动协议（seesion initiation protocol，SIP）电话、无线本地环路（wirelees local loop，WLL）站、个人数字助理（personal digital assistant，PDA）、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备，未来第五代（the 5th generation，5G）网络中的终端设备或者未来演进的公用陆地移动通信网络（public land mobile network，PLMN）中的终端设备等。终端设备有时也可以称为用户设备（user equipment，UE）、接入终端设备、车载终端设备、工业控制终端设备、UE 单元、UE 站、移动站、移动台、远方站、远程终端设备、移动设备、无线通信设备、UE 代理或 UE 装置等。终端设备也可以是固定的或者移动的。本申请实施例对此并不限定。

接入网用于实现无线接入有关的功能，接入网可以为特定区域的终端设备提供入网功能，包括无线接入网（radio access network，RAN）设备和接入网（access network，AN）设备。RAN 设备主要是 3GPP 网络中定义的无线网络设备，AN 设备主要是非 3GPP 定义的接入网设备。RAN 设备可以为终端设备提供无线资源管理、服务质量管理、数据加密和压缩等功能。

核心网主要用于对终端设备进行管理，并提供与外网通信的功能。核心网设备可包括以下中的一个或多个网元:

接入和移动管理功能（accees and mobility management function，AMF）网元：主要负责移动网络中的移动性管理，如用户位置更新、用户注册网络、用户切换等。

会话管理功能（session management function，SMF）网元：主要用于会话管理、终端设备的 IP 地址分配和管理，选择用户平面功能，策略控制或收费功能接口的终结点以及下行数据通知等。

用户面功能（user plane function，UPF）网元：主要负责用户数据的转发和接收。在

下行传输中，UPF 网元可以从数据网络（data network，DN）接收用户数据，通过接入网设备传输给终端设备；在上行传输中，UPF 网元可以通过接入网设备从终端设备接收用户数据，向 DN 转发该用户数据。可选的，UPF 网元中为终端设备提供服务的传输资源和调度功能可以由 SMF 网元管理控制。

认证服务功能（authentication server function，AUSF）网元：主要用于对用户鉴权等。

网络开放功能（network exposure function，NEF）网元：主要用于支持能力和事件的开放，如用于安全地向外部开放由 3GPP 网络功能提供的业务和能力等。

网络存储功能（network function，NF，repository function，NRF）网元：用于保存网络功能实体以及其提供服务的描述信息，支持服务发现，和网元实体发现等。

策略控制功能（policy control function，PCF）网元：用于指导网络行为的统一策略框架，为控制平面功能网元（例如 AMF，SMF 网元等）提供策略规则信息，负责获取与策略决策相关的用户签约信息等。

统一数据管理（unified data management，UDM）网元：用于生成认证信任状，用户标识处理（如存储和管理用户永久身份等），接入授权控制和签约数据管理等。

网络切片特定认证和授权功能（network slice specific authentication and authorization function，NSSAAF）网元：用于支持切片认证和授权、重授权或授权撤销等相关的流程。

除此之外，上述核心网中还可能包括 NSSF，AF，和 SCP 等网元，不再一一介绍。需要说明的是，在不同的通信系统中，上述核心网中的网元可以有不同的名称。在上述图 1 所示的示意图中，是以第五代移动通信系统为例进行说明的，并不作为对本申请的限定。

DN 可以是为用户提供数据传输服务的网络。例如，DN 可以是 IP 多媒体业务（IP multi-media service）网络或互联网络等。DN 中可包括多个应用服务器。其中，终端设备可以建立从终端设备到 DN 的协议数据单元（protocol data unit，PDU）会话，来访问 DN。其中，一个数据网络可以有一个或多个本地数据网络（local data network，Local DN），这些本地数据网络为靠近用户附着点（point of attachment）的数据网络接入点（access point）。

在本申请实施例中，上述图 1 所示架构中的 EES 和 EAS 可以配置于上述一个或多个 EDN 中。与 EDN 对应的为远端 DN 或中心 DN，EDN 中部署的应用服务器称为 EAS，远端 DN 或中心 DN 中部署的服务器为远端服务器或中心服务器。每个 EAS 可以就近为用户提供应用服务，中心服务器或远端服务器可以为所有用户提供应用服务。

由于 EDN 网络可以根据需求动态部署，比如上海地区 A 举行大型活动，人流较大，可以在该地方部署一个 EDN 网络，以供附近人员接入。后续该大型活动结束后，还可以撤销地区 A 部署的 EDN 网络。可选的，针对每个 EDN 网络中的 EES 和 EAS 也是可以动态部署的，比如新上市一款游戏，且地区 B 大量聚集该游戏的青年，可以在地区 B 的 EDN 网络中实例化提供该游戏服务的 EAS。可见，在 MEC 架构中，EES，EAS 甚至 ECS 都是动态部署的，终端设备无法通过预配置的方式获知动态部署的 EES、EAS 和 ECS 所支持的认证机制。

在一种可能的竞争方案中，由于终端设备不知道服务器（如 EES、EAS 或 ECS）所支持的认证机制，终端设备直接向服务器发送通信连接建立请求，该通信连接建立请求中可以不携带任何认证信息。由于该通信连接建立请求中没有携带任何认证信息，服务器会指示终端设备采用自己支持的认证机制发送通信连接建立请求。例如，服务器会向终端设备发送通信建立连接响应，该信建立连接响应可指示终端设备采用服务器支持的认证机制发

起通信连接建立请求等。终端设备接收到该通信建立连接响应，根据该通信建立连接响应的指示，再次发起通信连接建立请求，不同的是该通信连接建立请求中此时携带有服务器所支持的认证机制对应的认证信息。服务器接收到该再次发起的通信连接建立请求时，建立两者的通信连接。

通过上述对比可以看出，该竞争方案虽然可以在客户端和服务器之间通过认证以建立安全的通信连接，但是会存在如下问题：1、对于终端设备来说发送了两次通信连接建立请求，并且需要处理两次通信连接建立响应，浪费了信令；2、在终端设备第一次发送了通信连接建立请求，并接收到对应的通信连接建立响应之后，终端设备需要根据对应的认证机制生成认证信息，并进一步的向服务器发送通信连接建立请求，从终端设备第一次发送通信连接建立请求到最终与服务器间建立安全的通信连接，时延较长，对用户的通信体验影响较大。特别是在 MEC 场景下，对通信时延敏感，这种影响在某些场景下可能是不可接受的。

基于上述，本申请实施例提供一种建立安全通信方法，利用该方法终端设备可以获知动态部署的 EES、EAS 或 ECS 所支持的至少一个认证机制，适用于 MEC 架构下，使得客户端与服务器之间执行认证建立安全的通信连接，该方法包括：终端设备接收来自第一网元的第一消息，第一消息中包括第二网元的标识以及第一指示信息，第一指示信息用于指示与第二网元关联的候选认证机制；可选的，上述第二网元的标识与第一指示信息可以通过同一个消息传输给终端设备，比如上述第一消息，还可以通过不同的消息传输给终端设备，不作限定。上述第二网元的标识可以为第二网元的统一资源标识符（uniform resource identifier，URI），全量域名（fully qualified domain name，FQDN），或互联网协议（internet protocol，IP）地址等。终端设备根据候选认证机制，与第二网元之间建立通信连接。其中，上述第二网元可以为 EES、EAS 或 ECS 等，上述候选认证机制可以为第二网元所支持的认证机制，或者为第二网元与终端设备间建立通信连接所使用的认证机制等，不作限定。示例的，上述终端设备基于候选认证机制，与第二网元之间建立通信连接的过程可以为：终端设备基于候选认证机制，向第二网元发送通信连接建立请求，该通信连接建立请求中携带有上述候选认证机制对应的认证信息（例如下文中的 Kakma 的密钥标识）。第二网元接收到该通信连接建立请求后，根据认证信息对终端设备进行验证，验证通过后，可获取终端设备与第二网元间安全通信使用的密钥，从而使得终端设备与第二网元间建立安全的通信连接。在一种可能的实现方式中，上述认证信息可以为密钥标识，第二网元在接收到通信连接建立请求时，可向 3GPP 网元发送密钥标识。可选的，在发送密钥标识前，3GPP 网元与第二网元之间执行相互认证，认证通过后。3GPP 网元根据密钥标识获取第二网元的密钥，并向第二网元发送所述密钥。第二网元通过与 3GPP 网元的交互，第二网元获取与 UE 之间共享的同一个密钥。进一步的，第二网元与 UE 之间可以基于共享的密钥执行进一步的认证并建立通信连接。

可选的，本申请实施例中的方法，还可以包括：终端设备向第一网元发送第二消息，所述第一消息为第二消息的响应消息。需要说明的是，本申请实施例中的第一网元可以是能够提供其它网元的标识以及其它网元对应的候选认证机制的网元。第二网元也不限定为 ECS，ESS 或 EAS 等，比如第二网元可以是能够使得第一网元能够获取其标识和对应候选认证机制的网元。本申请实施所涉及的认证机制可以包括以下至少一项：应用的认证和密钥管理（authentication and key management for applications，AKMA）服务，通用引导架构

（generic bootstrapping architecture GBA）服务，证书机制，EES 的信任状（credentials）或者其它用于终端设备与第二网元之间认证的机制。需要说明的是，若终端设备与第二网元之间使用证书认证，则以下实施例中的第二网元（例如，ECS，EES 或 EAS 等）所支持的至少一个认证机制可替换为“用于认证第二网元证书的信息”，如证书颁发机构（certificate authority，CA）公钥等，终端设备所支持的至少一个认证机制可替换为“用于认证 UE 证书的信息”等。

实施例一

在实施例一中，以终端设备为 UE，UE 包括 AC 和 EEC，第一网元为 ECS，第二网元为 EES，第二消息为提供请求（provisioning request）消息，第一消息为提供响应（provisioning response）消息为例，进行说明。

如图 4 所示，提供一种通信方法的流程，包括:

可选的，步骤 400: ECS 获取 EES 所支持的至少一个认证机制。可选的，ECS 还可以获取 EES 所支持的至少一个认证机制中一个或者多个认证机制的优先级信息。

其中，ECS 可以通过预配置的方式，获取 EES 所支持的至少一个认证机制和其对应的优先级信息。或者，ECS 可以通过与 EES 交互的方式，获取 EES 所支持的至少一个认证机制和其对应的优先级信息等，例如当 EES 实例化成功之后，可以通过主动注册的方式，将自己所支持的至少一个认证机制和其对应的优先级信息发送给 ECS 等。本申请实施例对于 ECS 获取 EES 的信息的具体方式，不作限定。

步骤 401: EEC 向 ECS 发送提供请求消息，该提供请求消息中包括 UE 标识和应用客户端配置文本信息。

具体的，EEC 可以根据预配置的 ECS 地址或发现的 ECS 地址或来自 AC 的 ECS 地址，向 ECS 发送提供请求消息等。

其中，UE 标识用于在公共陆地移动网络（public land mobile network，PLMN）网络中唯一的标识 UE，例如可以为通用公共用户标识（generic public subscription identifier，GPSI），本申请实施例并不限定 UE 标识的具体实现形式。应用客户端配置文本信息中包含用于确定 UE 中应用程序客户端 AC 所需服务和服务特征的信息等。例如，应用客户端配置文本中可以包括 AC ID，应用客户端类型，业务连续性是否必须支持等。其中，AC ID 用于标识终端设备上的特定应用，应用客户端类型可以是 V2X 类型等。

步骤 402: ECS 接收提供请求消息。可选的，ECS 检验 EEC 是否被授权获取边缘服务器的信息。

示例的，ECS 中存储有其授权的合法 EEC 的信息，只有其授权的合法 EEC 才能获取边缘服务器的信息。在本申请实施例中，ECS 可具体判断在其存储的合法 EEC 列表中，是否包含上述发送提供请求消息的 EEC，若包含，则对该 EEC 的授权检查通过，否则对该 EEC 的授权检查不通过。具体如何判断 EEC 是否授权获取边缘服务器的信息，本实施例不限制。

步骤 403: ECS 向 EEC 发送提供响应消息。

其中，若上述 EEC 的授权检查通过，则上述提供响应消息中可以包括 EES 的标识和第一指示信息，第一指示信息用于指示与 EES 关联的候选认证机制。或者，若上述 EEC 的授权检查不通过，则上述提供响应消息中可携带第二指示信息，该第二指示信息用于指

示 EEC 的授权检查失败等。

在一种可能的实现方案中，在 EEC 授权检查通过后，ECS 可根据上述提供请求消息中携带的应用客户端配置文本信息，确定其对应的 EDN 配置信息；ECS 向 EEC 发送的提供响应消息中可携带有上述 EDN 配置信息。其中，EDN 配置信息中包括 EES 信息，和 EDN 连接信息等。其中，EES 信息中包括 EES 标识，EES 标识可以为 EES 的 FQDN，URL 或 IP 地址等，不作限定。EDN 连接信息用于 UE 与 EDN 间建立 PDU 会话，EDN 连接信息中可包括数据网络名（data network name，DNN），接入点名（access point name，APN）等。可选的，上述 EDN 配置信息中还可以包含单网络切片选择辅助信息(single network slice selection assistance information，S-NSSAI)和 EDN 服务区等。在本申请实施例中，所述 EDN 配置信息中还可以包括用于指示 EES 关联的候选认证机制的第一指示信息等。

需要说明的是，为了便于描述，在某个消息/信息中携带有认证机制的指示信息，还可描述为在某个消息/信息中携带有认证机制，两者不作区分，可相互替换。如无额外说明，在下述描述中，统一表示为在某个消息/信息中携带有认证机制。

步骤 404：EEC 根据候选认证机制，与 EES 间建立通信连接。

为了便于区分不同的认证机制，在以下描述中，采用三种表示方式：ECS 所确定的 UE 与 EES 间通信所使用的认证机制称为第一认证机制；UE 所支持的认证机制可以称为第二认证机制；EES 所支持的认证机制可称为第三认证机制。可以理解的是，由于 UE 中包括 AC 或 EEC，所以在本申请实施例的以下描述，UE 所支持的认制机制，有时也可以描述为 EEC 或 AC 支持的认证机制。EEC 或 AC 与第二网元间建立通信连接，也可以描述为 UE 与第二网元间建立通信连接。当然，第二网元包括但不限于 ECS，EES，或 EAS 等。

在一种设计中，上述候选认证机制为 EES 所支持的至少一个第三认证机制。上述提供响应消息中携带有 EES 所支持的至少一个第三认证机制。可选的，该提供响应消息中还可以携带 EES 所支持的至少一个第三认证机制的优先级信息。EEC 根据 EES 所支持的至少一个第三认证机制和辅助信息，确定目标认证机制，所述辅助信息中包括以下至少一项：UE 所支持的至少一个第二认证机制，和 UE 接入 EES 所使用的网络类型等。可选的，上述辅助信息中还可以包括：UE 所支持的至少一个第二认证机制的优先级信息，和 EES 所支持的至少一个第三认证机制的优先级信息。

具体的，当所述辅助信息中包括 UE 所支持的至少一个第二认证机制时，EEC 可以将 UE 和 EES 都支持的认证机制，确定为目标认证机制。比如，EES 所支持的至少一个认证机制包括 A，B 和 C，UE 所支持的至少一个认证机制包括 C、D 和 E，则目标认证机制包括 C。

当所述辅助信息中包括 UE 接入 EES 所使用的网络类型时，所述目标认证机制可以为网络类型对应的认证机制。比如， EES 支持的认证机制包含 AKMA 和 GBA，且 AKMA 机制为基于 5G 网络的认证机制，GBA 机制为基于 4G 网络的认证机制，此时如果 UE 当前接入网络为 5G 网络，则 UE 确定所述目标认证机制为 AKMA；或者，如果 UE 的当前接入网络为 4G 网络，则 UE 确定所述目标认证机制为 GBA。

可选的，EEC 还可以考虑不同认证机制的优先级信息，优先选择优先级高的认证机制。例如，当所述辅助信息中包括所述 EES 所支持的至少一个第三认证机制的优先级信息时，则 UE 可以优先选择优先级高的认证机制作为目标认证机制。

之后，EEC 生成与目标认证机制对应的第一密钥和第一密钥标识。在一种可能的实现

方式中，EEC 还可向终端设备的底层请求目标认证机制对应的信息，终端设备底层的底层根据目标认证机制对应的信息，生成第一密钥和第一密钥的标识，终端设备底层向 EEC 发送第一密钥标识等；EEC 向 EES 发送通信连接建立请求，该通信连接建立请求中包括第一密钥标识。可选的，终端设备底层还可以根据第一密钥和 EES 的标识，生成第二密钥，并向 EEC 发送第二密钥；EEC 使用第二密钥对通信连接建立请求进行安全保护，比如根据第二密钥和通信连接建立请求中的全部信息或部分信息生成第一消息认证码（message authentication code，MAC）；其中，所述通信连接建立请求中包括第一 MAC。EES 在接收到通信连接建立请求时，可获取通信连接建立请求中的第一密钥标识；EES 根据第一密钥标识，获取第二密钥，比如，EES 可将第一密钥标识，发送给用于支持目标认证机制的 3GPP 网元，该 3GPP 网元可根据密钥标识与密钥的对应关系，获取第一密钥标识所对应的第一密钥，且根据第一密钥和 EES 的标识，生成第二密钥，将第二密钥返回给 EES；EES 根据第二密钥，生成第二 MAC；比较生成的第二 MAC 与上述通信连接建立请求中携带的第一 MAC 是否相同；若相同，可认为验证通过，否则，认为验证不通过。其中，EES 对 UE 的验证通过，可表示以含义：EES 可以认为从 UE 接收到的信息没有被攻击者篡改，且 UE 为被 3GPP 网元验证过的合法 UE 等。进一步的，UE 与 EES 之间可以根据第二密钥进一步协商后续通信所使用的安全上下文，所述安全上下文包含加密密钥和/或完整性保护密钥等，对应的加密算法，和完整性保护算法等。在一种示例中，EES 可以通过 NEF 向用于支持目标认证机制的 3GPP 网元发送第一密钥标识等。进一步的，在 EES 获取第二密钥的过程中，3GPP 网元与 EES 之间可以执行双向认证，只有合法的通过认证的 EES 才可以获取第一密钥标识对应的第二密钥。

在另一种设计中，所述候选认证机制为 EEC 与 EES 之间建立通信连接时使用的至少一个第一认证机制。该方法的实现过程可如下：上述提供请求消息中可携带有 UE 所支持的至少一个第二认证机制。可选的，该提供请求消息中还可以携带以下至少一项：UE 所支持的至少一个第三认证机制的优先级信息，和 UE 接入 EES 使用的网络类型等。ECS 根据 ECS 所支持的至少一个第三认证机制和辅助信息，确定候选认证机制，该辅助信息中至少包括 UE 所支持的至少一个第三认证机制，和 UE 接入 EES 使用的网络类型。可选的，该辅助信息中还可以包括以下至少一项：UE 所支持的至少一个第二认证机制的优先级信息，和 EES 所支持的至少一个第三认证机制的优先级信息等。上述提供响应消息中可以携带有上述候选认证机制。EEC 接收来自 ECS 的提供响应消息，获取该提供响应消息中的候选认证机制；可以理解的是，若上述候选认证机制中只包括一个第三认证机制，则 EEC 可直接根据该第三认证机制，与 EES 之间建立通信连接，该第三认证机制可以认为即为目标认证机制；或者，当上述候选认证机制中包括多个认证机制，EEC 可以在上述多个认证机制中，选择一个认证机制，建立通信连接，所选择的认证机制即为目标认证机制。EEC 与 EES 之间建立通信连接的过程，可参见上述描述，不再赘述。

可选的，在上述几种设计中，都是以 EEC 根据候选认证机制，确定目标认证机为例进行描述的，并不作限对本申请的限定。UE 中的其它模块也可以执行根据候选认证机制，确定目标认证机制的过程。

需要说明的是，在本申请的描述中，主要涉及 UE 所支持的至少一个认证机制的优先级信息，和 EES 所支持的至少一个认证机制的优先级信息。所述优先级信息可以采用显示指示的方式，例如，EES 所支持的多个认证机制分别为认证机制 A，认证机制 B 和认证机

制 C。则 EES 所支持的多个认证机制的优先级信息可分别为认证机制 A 的优先级信息 0，认证机制 B 的优先级信息 1，认证机制 C 的优先级信息 2。其中，优先级信息的取值越小，代表其对应的优先级越高。或者，所述优先级信息也可以采用隐示指示的方式，所述优先级信息还可称为优先级规则。仍沿用上述举例，可将上述三个认证机制按优先级规则进行排序。后续 UE 可根据上述优先级排序规则，确定 EES 所支持的多个认证机制的优先级。比如，UE 与 EES 间可预先协商，优先级越高的，排列位置越靠前。假设 EES 所支持的 3 个认证机制的排列顺序为：认证机制 C，认证机制 A，认证机制 B。UE 在接收到上述 3 个认证机制后，可根据上述 3 个认证机制的接收顺序，确定 3 个认证机制的优先级分别为：认证机制 C，认证机制 A，和认证机制 B 等。再例如，EES 所支持的 3 个认证机制可以包括推荐的认证机制，比如优先级信息可以是：认证机制 C（推荐），认证机制 A，和认证机制 B，则表明认证机制 C 的优先级最高，认证机制 A 和认证机制 B 的优先级次之，且两者的优先级相同。

需要说明的是，上述各种优先级信息举例只是为了便于说明，实际应用中上述优先级信息的举例可以互相组合，以形成各种灵活的优先级规则。本申请对此不做限定。例如，可以只显示指定高（或低）优先级的认证机制，其他认证机制的优先级按照排序确定优先级高低。本申请中优先级信息能够体现 EES 或者 UE 支持的至少一个认证机制中不同认证机制的优先级差异。

根据上述方法，EEC 通过与 ECS 交互，可以获取 EES 对应的候选认证机制，EEC 与 EES 间可基于候选认证机制建立通信连接，减少信令开销，降低建立通信时延，提高通信体验。

如图 5 所示，提供一种通信方法的流程，该流程可用于 ECS 与 EES 交互，以获取 EES 所支持的至少一个认证机制，包括：

步骤 501：EES 向 ECS 发送边缘使能服务注册或更新请求（edge enabler server registration/update request）消息，该注册或更新请求消息中包括 EES 标识（如 URI，FQDN，IP 地址等），EAS 配置等。

在本申请实施例中，上述注册或更新请求消息中还包括 EES 所支持的至少一个认证机制，或者，EES 提供商标识。可选的，上述注册或更新请求消息中还可以包括 EES 所支持的至少一个认证机制的优先级信息。其中，上述 EES 所支持的至少一个认证机制可以为用户按需设置的，或者预配置的默认值等，不作限定。下述实施例中的，EAS 或 EC 所支持的至少一个认证机制，同样可以为用户按需设置，或预配置的默认值等，后续不再说明。

步骤 502：接收到 EES 的注册或更新请求消息后，ECS 验证 EES 是否被授权。若被授权，则存储上述注册或更新请求消息中的信息。

在一种设计中，若上述注册或更新请求消息中包括 EES 所支持的至少一个认证机制，则 ECS 直接存储 EES 所支持的至少一个认证机制。可选的，ECS 还可以存储所述至少一个认证机制的优先级信息。在另一种设计中，若上述注册或更新请求消息中包括 EES 提供商标识，则 ECS 可根据上述 EES 提供商标识，确定 EES 所支持的至少一个认证机制。例如，ECS 存储该 EES 提供商所对应的至少一个认证机制，可选的还可以存储该 EES 提供商所对应的至少一个认证机制的优先级信息等。后续，ECS 可根据存储的 EES 提供商与认证机制的对应关系，确定所述 EES 所支持的至少一个认证机制，可选的，还可以确定至少一个认证机制的优先级信息。

步骤 503: ECS 向 EES 发送边缘使能服务注册或更新响应消息，该响应消息中包括注册/更新成功或失败的指示信息。可选的，该响应消息中还可以包括失效时间，用于指示注册或更新失效的时间。可选的，针对注册请求，响应消息中还可以包含注册 ID。

通过上述方案，ECS 通过与 EEC 交互，可获取 EES 所支持的至少一个认证机制和其对应的优先级信息等。

实施例二

在该实施例二中，以终端设备为 UE，UE 包括 AC 和 EEC，第一边缘服务器为 EES，第二边缘服务器为 EAS，第二消息为边缘使能客户端注册请求（edge enabler client registration request）消息，第一消息为边缘使能客户端注册响应（edge enabler client registration response）消息为例，进行说明。

如图 6 所示，提供一种通信方法的流程，包括:

可选的，步骤 600: EES 获取 EAS 所支持的至少一个认证机制。可选的，EES 还可以获取 EAS 所支持的至少一个认证机制的优先级信息。

示例的，EES 可以通过预配置的方式，获取 EAS 所支持的至少一个认证机制与其所对应的优先级信息，或者 EES 还可以通过与 EAS 交互的方式，获取 EAS 所支持的至少一个认证机制与其所对应的优先级信息。例如，当 EAS 实例化成功之后，可以通过主动注册的方式，将自己所支持的至少一个认证机制和其对应的优先级信息发送级 EES。本申请实施例对于 EES 获取 EAS 信息的方式不作限定。

步骤 601: EEC 向 EES 发送边缘使能客户端注册请求消息，该请求消息中包含 EEC ID 和应用客户端配置文件。

具体的，EEC 可根据从 ECS 获取的 EES 信息，向 EES 发送边缘使能客户端注册请求消息等。

其中，应用客户端配置文件中可包括 AC ID，EAS ID（用于标识请求发现的 EAS），和边缘服务器提供商等。其中，EEC ID 用于唯一标识一个 EEC。EAS ID 用于标识一个特定的应用。可选的，上述边缘使能客户端注册请求消息中还可以包括以下至少一项: UE ID，上下文 ID（context ID），分配上下文 ID 的 EES ID（又称为源 EES ID），和 EAS ID（用于标识已发现的 EAS）等。其中，上下文 ID 用于标识上一次 EEC 注册的上下文等。

步骤 602: EES 接收边缘客户端注册请求消息。可选的，EES 可执行授权检查，即 EES 检查 EEC 是否被授权请求发现的 EAS。

示例的，若 EEC 的授权检查通过，则在下述步骤 804 中的边缘使能客户端注册响应消息中可以携带授权发现的 EAS ID 和指示授权发现的 EAS 关联的候选认证机制的第一指示信息。否则，在下述步骤 804 中的边缘使能客户端注册响应消息中可以携带请求失败的第二指示信息等。

可选的，步骤 603: EEC 授权检查通过后，如果上述步骤 801 中的边缘使能客户端注册请求消息中包含上下文 ID 和源 EES ID，则 EES 从源 EES 中获取注册上下文。若请求消息中不包括上下文 ID 和源 EES ID，则跳过该步骤。EES 按照正常流程，获取注册上下文。

上述步骤 603 主要是针对移动场景所设计的。比如用户在上海移动到北京，则原来由上海的 EDN 网络为用户提供服务，后续需要由北京的 EDN 网络为用户提供服务。北京的 EDN 网络，可以去上海的 EDN 网络中获取相关的信息。

步骤 604：EES 向 EEC 发送边缘使能客户端注册响应消息。

在一种可能的实现方案中，若 EEC 授权检查通过，则所述边缘使能客户端注册响应消息中可包括 EAS 信息列表。比如，EEC 授权检查通过后，EES 可根据注册上下文，确定客户端配置文件指示的 EAS 信息列表。EAS 信息列表中包含 EAS ID 等，EASID 用于 AC 向 EAS 发送请求。可选的，EAS 信息列表中还可以包含 EAS 提供商标识，EAS 可用的存储等。在本申请实施例中，所述 EAS 信息列表中还可以包括 EAS 对应的候选认证机制。

为了便于区分不同的认证机制，在以下描述中，采用三种表示方式：EES 所确定的 UE 与 EAS 间通信所使用的认证机制称为第一认证机制；UE 所支持的认证机制可以称为第二认证机制；EAS 所支持的认证机制可称为第三认证机制。

在一种设计中，所述候选认证机制为 EAS 所支持的至少一个第三认证机制。所述边缘使能客户端注册响应消息中包括 EAS 所支持的至少一个第三认证机制。可选的，该边缘使能客户端注册响应消息中还可以包括 EAS 所支持的至少一个第三认证机制的优先级信息。EEC 接收边缘使能客户端注册响应消息，获取该边缘使能客户端注册响应消息中的 EAS 所支持的至少一个第三认证机制。可选的，还可以获取 EAS 所支持的至少一个第三认证机制的优先级信息。EEC 根据 EAS 所支持的至少一个认证机制和辅助信息，确定目标认证机制，所述辅助信息中至少包括以下至少一项：UE 所支持的至少一个第二认证机制，和 UE 接入 EAS 所使用的网络类型。可选的，辅助信息中还可以包括以下至少一项：UE 所支持的至少一个认证机制的优先级信息，和 EAS 所支持的至少一个认证机制的优先级信息。可选的，EEC 可从非接入层（non-access stratum，NAS）层或其它层获取 UE 所支持的至少一个认证机制中的优先级信息，或 UE 接入 EAS 使用的网络类型等。之后，EEC 向 AC 发送 EAS 信息提供消息，该 EAS 信息提供消息中包括候选认证机制，AC 根据目标认证机制，与 EAS 间建立通信连接，上述目标认证机制包括在上述至少一个第三认证机制中的一个认证机制中。关于 AC 与 EAS 间建立通信连接的过程，与 EEC 与 EES 间建立通信连接的过程相似，可相互参见。

在另一种设计中，所述候选认证机制为 EAS 所支持的至少一个第三认证机制。所述边缘使能客户端注册响应消息中包括 EAS 所支持的至少一个第三认证机制。可选的，该边缘使能客户端注册响应消息中还可以包括 EAS 所支持的至少一个第三认证机制的优先级信息。EEC 接收边缘使能客户端注册响应消息，获取该边缘使能客户端注册响应消息中的 EAS 所支持的至少一个第三认证机制。可选的，还可以获取 EAS 所支持的至少一个认证机制的优先级信息。EEC 向 AC 发送 EAS 所支持的至少一个第三认证机制。可选的，EEC 还可以向 AC 发送 EAS 所支持的至少一个认证机制的优先级信息。AC 根据 EAS 所支持的至少一个第三认证机制和辅助信息，确定目标认证机制，所述辅助信息中包括以下至少一项：UE 所支持的至少一个第二认证机制，和 UE 接入 EAS 所使用的网络类型。可选的，辅助信息中还可以包括以下至少一项：UE 所支持的至少一个第二认证机制的优先级信息，和 EAS 所支持的至少一个第三认证机制的优先级信息。示例的，AC 可以从 NAS 层或其它层获取 UE 所支持的至少一个第二认证机制的优先级信息，和/或 UE 接入 EAS 使用的网络类型等。之后，AC 根据目标认证机制，与 EAS 间建立通信连接。关于 AC 与 EAS 间建立通信连接的过程，与 EEC 与 EES 间建立通信连接的过程相似，可相互参见。

在另一种设计中，所述候选认证机制为 AC 与 EAS 之间建立通信连接时所使用的至少一个第一认证机制。所述边缘使能客户端注册请求消息中包括 UE 的能力信息，UE 的能力

信息包括 UE 所支持的至少一个第二认证机制。可选的，UE 的能力信息中还可以包括：UE 接入 EAS 所使用的网络类型，和 UE 所支持的至少一个认证机制的优先级信息。EES 根据 EAS 所支持的至少一个第三认证机制和辅助信息，确定候选认证机制，辅助信息中包括以下至少一项：UE 所支持的至少一个第二认证机制，和 EAS 所支持的至少一个第三认证机制。可选的，辅助信息中还可以包括以下至少一项：UE 所支持的至少一个第二认证机制的优先级信息，和 EAS 所支持的至少一个第三认证机制的优先级信息。EES 向 EEC 发送边缘客户端注册响应消息，该边缘客户端注册响应消息中包括上述候选认证机制。如果上述候选认证机制中包括一个认证机制，则该认证机制作为目标认证机制。或者，如果上述候选认证机制中包括多个认证机制，则可以在上述多个认证机制中选择一个认证机制，作为目标认证机制等。之后，EEC 可向 AC 发送 EAS 信息提供消息，该 EAS 信息提供消息中包括目标认证机制；AC 根据目标认证机制，与 EAS 之间建立通信连接。或者，EEC 可将候选认证机制直接发送给 AC；AC 根据候选认证机制，确定目标认证机制等，不作限定。

需要说明的是，在上述几种设计中，分别是以 EEC 或 AC 根据候选认证机制，确定目标认证机制为例进行说明的，并不作为本申请实施例的限定。比如，在本申请实施例中，还可以为 UE 中的其它模块执行上述根据候选认证机制，确定目标机制的过程。不同的是，上述其它模块需要把目标认证机制最终通知 AC。

步骤 605：EEC 向 AC 发送 EAS 信息提供消息，该 EAS 信息提供消息中包含 AC 对应的 EAS 的目标认证机制，或者，包括 AC 对应的 EAS 的候选认证机制。

步骤 606：AC 在向 EAS 发起请求时，根据从 EEC 接收的 EAS 对应的候选认证机制或目标认证机制，与 EAS 间建立通信连接。

通过上述可以看出，UE 通过与 EES 交互，可获取 EAS 对应的候选认证机制，EEC 与 EAS 之间无需再进行认证的协商流程，减少了信令开销，降低建立通信时延，提高通信体验。

如图 7 所示，提供一种通信方法的流程，该流程可以用于 EES 与 EAS 交互获取 EAS 所支持的至少一个认证机制，该流程包括：

可选的，步骤 701：EAS 确定需要注册到 EES。

步骤 702：EAS 向 EES 发送边缘应用服务注册或更新请求（edge application server registration/update request）消息。该注册或更新请求消息中包含以下至少一项：EAS 标识和 EAS 配置。可选的，该注册或更新请求消息中还可以包含 EAS 服务区，和 EAS 类型等。

在一种设计中，上述注册或更新请求消息中包含 EAS 所支持的至少一个认证机制。在另一种设计中，上述注册或更新请求消息中包括 EAS 提供商 ID。可选的，该注册或更新请求消息中还可以包括 EAS 所支持的至少一个认证机制的优先级信息。

步骤 703：接收到 EAS 的注册或更新请求消息后，EES 对 EAS 进行授权检查，验证 EAS 是否被授权。如果被授权，则存储上述注册或更新请求消息中的信息。

在一种设计中，若上述注册请求或更新请求消息中包括 EAS 所支持的至少一个认证机制，则 EES 直接存储 EAS 所支持的至少一个认证机制。在另一种设计中，若上述注册或更新请求消息中包括 EAS 提供商 ID，则 EES 可根据提供商与认证机制的对应关系，确定上述 EAS 提供商 ID 所对应的至少一个认证机制，该提供商 ID 所对应的至少一个认证机

制可以认为是 EAS 所支持的至少一个认证机制。

步骤 704：EES 向 EAS 发送边缘应用服务注册或更新响应消息，该响应消息中包含注册/更新成功或失败的指示。可选的，该响应消息中还可以包含失效时间，该失效时间用于指示注册或更新失效的时间。针对注册请求，该响应消息中还可以包含注册 ID。可选的，EES 还可以存储 EAS 所支持的至少一个认证机制的优先级信息。

通过上述方案，EES 通过与 EAS 交互，可以获取 EAS 所支持的至少一个认证机制和其对应的优先级信息。

实施例三

在该实施例三中，以终端设备为 UE，第一网元为 AMF，第二消息为终端设备的注册请求消息，第一消息为终端设备的注册请求的响应消息为例，介绍本申请实施中的方案。

如图 8 所示，提供一种通信方法的流程，至少包括以下步骤：

可选的，步骤 800：对于签约使用边缘服务的 UE，UDM 的接入和移动性管理用户签约信息中包含 UE 能够使用的 ECS 信息，ECS 信息中包含以下至少一项：ECS 标识和 ECS 所支持的至少一个认证机制。可选的，所述 ECS 信息中还可以包含 ECS 所支持的至少一个认证机制的优先级信息。

步骤 801：UE 通过接入网节点向 AMF 发送注册请求消息，该注册请求消息中包含 UE 标识。可选的，该注册请求消息中还可以包含以下至少一项：UE 所支持的至少一个认证机制，UE 是否支持边缘使能客户端的指示信息，和 UE 所支持的至少一个认证机制的优先级信息。

例如，在一种可能的实现方式中，上述注册请求消息中包含 UE 标识和 UE 能力，该 UE 的标识可以为用户隐藏标识（subscription concealed identifier，SUCI）或全球唯一临时标识（globally unique temporary identity，5G-GUTI）或映射的 5G-GUTI 等。UE 能力中包含以下至少一项：UE 支持的至少一个认证机制，UE 是否支持边缘使能客户端的指示信息，和 UE 所支持的至少一个认证机制的优先级信息。

步骤 802：接收到 UE 的注册请求消息之后，当 AMF 需要获取签约信息时，AMF 可向 UDM 发送签约数据管理获取请求（Nudm_subscriber data management get, Nudm_SDM_Get）请求消息，该请求消息中包含 UE 的标识。可选的，该请求消息中还以包含 UE 的能力信息。该 UE 的标识为根据步骤 801 中的 UE 标识确定的，可以为用户永久标识（subscription permanent identifier, SUPI）。

步骤 803：UDM 根据 Nudm_SDM_Get 请求消息中包含的 UE 的标识，获取 UE 的签约信息，并向 AMF 发送 Nudm_SDM_Get 响应消息，该响应消息中包含 ECS 信息，所述 ECS 信息中包含以下至少一项：ECS 标识和 ECS 关联的候选认证信息。关于 UDM 如何获取 ECS 对应的候选认证信息将在下述实施例中详细介绍。

步骤 804：AMF 接收到 UDM 发送的 Nudm_SDM_Get 响应消息，获取响应消息中的 ECS 信息，且向 UE 发送 ECS 信息。在一种设计中，AMF 可以通过注册响应消息向 UE 发送 ECS 信息，可参见步骤 804a 所示；或者，AMF 可以通过独立的配置流程 UE 配置更新（UE configuration update，UCU）流程向 UE 发送 ECS 信息，可参见步骤 804b 所示。

步骤 805：UE 的 NAS 层向对应的 EEC 发送接收到的 ECS 信息。NAS 层可以直接向 EEC 发送接收到的 ECS 信息，或者间接的通过上层向 EEC 发送 ECS 信息。

步骤 806: EEC 根据 ECS 信息中所包括的候选认证机制，与 ECS 之间建立通信连接。

为了便于区分不同的认证机制，在以下描述中，采用四种表示方式：AMF 所确定的 UE 与 ECS 间通信所使用的认证机制称为第一认证机制；UE 所支持的认证机制可以称为第二认证机制；ECS 所支持的认证机制可称为第三认证机制；将 UDM 确定的 UE 与 ECS 间通信所使用的认证机制作为第四认证机制。

在一种设计中，所述候选认证机制为所述 ECS 所支持的至少一个第三认证机制。Nudm_SDM_Get 响应消息中包括 ECS 所支持的至少一个第三认证机制。可选的，Nudm_SDM_Get 响应消息还可以包括 ECS 所支持的至少一个第三认证机制的优先级信息。AMF 在接收到 Nudm_SDM_Get 响应消息时，获取 ECS 所支持的至少一个第三认证机制。可选的，AMF 还可以获取 ECS 所支持的至少一个第三认证机制的优先级信息。AMF 向 UE 发送注册响应消息，或 UCU 流程，该注册响应消息或 UCU 流程中携带有 ECS 所支持的至少一个第三认证机制。可选的，该响应消息或 UCU 流程中还可包括 ECS 所支持的至少一个第三认证机制中的优先级信息。UE 根据 ECS 所支持的至少一个第三认证机制与辅助信息，确定目标认证机制，所述辅助信息中至少包括：UE 所支持的至少一个第二认证机制，和 UE 接入 ECS 使用的网络类型。可选的，辅助信息中还可以包括以下至少一项：UE 所支持的至少一个认证机制的优先级信息，和 ECS 所支持的至少一个认证机制的优先级信息。后续，UE 根据目标认证机制与 ECS 之间，建立通信连接。其中，UE 与 ECS 之间建立通信连接的过程，与 EEC 与 EES 之间建立通信过程的过程相似，可相互参见。

可选的，上述 UE 与 ECS 之间建立通信连接，还可以描述为 EEC 与 ECS 之间建立通信连接。可具体由 UE 中的 NAS 层执行上述“根据 ECS 所支持的至少一个认证机制和辅助信息，确定目标认证机制”的过程，之后 NAS 层将上述目标认证机制发送给 EEC，EEC 根据该目标认证机制与 ECS 之间建立通信连接。

在另一种设计中，所述候选认证机制为所述 EEC 与 ECS 通信时所使用的至少一个第一认证机制。上述注册请求消息中可携带 UE 的能力信息，UE 的能力信息中包括 UE 支持的至少一个第二认证机制，UE 接入 ECS 使用的网络类型，UE 支持的至少一个第二认证机制的优先级信息。AMF 接收注册请求消息，获取 UE 的能力。当 AMF 需要获取签约信息，向 UDM 发送 Nudm_SDM_Get 请求消息。AMF 接收来自 UDM 的 Nudm_SDM_Get 响应消息，该 Nudm_SDM_Get 响应消息中包括 ECS 所支持的至少一个第三认证机制。可选的，该响应消息中还可以包括 ECS 所支持的至少一个第三认证机制的优先级信息。AMF 根据 ECS 所支持的至少一个第三认证机制和辅助信息，确定候选认证机制。可选的，辅助信息中至少包括以下至少一项：UE 支持的至少一个第二认证机制，和 UE 接入 ECS 所使用的网络类型。可选的，上述辅助信息中还可以包括：UE 支持使用的至少一个第二认证机制的优先级信息，和 ECS 支持使用的至少一个认证机制的优先级信息。AMF 向 UE 发送注册响应消息，或 UCU 流程，该注册响应消息或 UCU 流程中包括候选认证机制。UE 获取该注册响应消息或 UCU 流程中的候选认证机制，根据该候选认证机制，确定目标认证机制。例如，所述候选认证机制中可能包括多个第一认证机制，UE 可以选择其中一个认证机制，作为目标认证机制。后续，UE 的 NAS 层可以向 EEC 发送目标认证机制，EEC 根据该目标认证机制，与 ECS 之间建立通信连接。或者，UE 在接收到上述候选认证机制时，可直接将该候选认证机制发送给 EEC，EEC 根据该候选认证机制，确定目标认证机制。

在又一种设计中，所述候选认证机制为所述 EEC 与 ECS 通信时所使用的至少一个第

四认证机制。上述注册请求消息中可携带 UE 的能力信息，UE 的能力信息中包括 UE 支持的至少一个第二认证机制，UE 接入 ECS 使用的网络类型，UE 支持的至少一个第二认证机制的优先级信息。AMF 接收注册请求消息，获取 UE 的能力。当 AMF 需要获取签约信息时，向 UDM 发送 Nudm_SDM_Get 请求消息，该 UDM 发送 Nudm_SDM_Get 请求消息中携带有 UE 的能力信息。UDM 根据 ECS 所支持的至少一个认证机制和辅助信息，确定候选认证机制，所述辅助信息中至少包括 UE 所支持的至少一个第二认证机制，和 UE 接入 ECS 所使用的网络类型。可选的，所述辅助信息中还可以包括以下至少一项：UE 所支持的至少一个认证机制中的优先级信息，和 ECS 所支持的至少一个认证机制的优先级信息等。UDM 向 AMF 发送 Nudm_SDM_Get 响应消息，该响应消息中包括候选认证机制。后续 AMF 通过注册响应消息，或 UCU 流程将候选认证机制发送给 UE，过程与上述方案相似，不再赘述。

在本申请实施例中，UE 与 AMF 交互可获取 ECS 所对应的候选认证机制，UE 与 ECS 间，无需再进行认证的协商流程，减少了信令开销，降低建立通信时延，提高通信体验。

实施例四

在该实施例四中，以终端设备为 UE，第一网元为 SMF，第二消息为 PDU 会话请求消息，第一消息为 PDU 会话响应消息为例，介绍本申请实施例中的方案。

如图 9 所示，提供一种通信方法的流程，至少包括以下步骤：

可选的，步骤 900：对于支持使用边缘服务的 UE，UDM 的会话管理用户签约信息中包含 UE 能够使用的 ECS 信息，ECS 信息中包含以下至少一项：ECS 标识和 ECS 所支持的至少一个认证机制等。可选的，该 ECS 信息中还可以包含：ECS 所支持的至少一个认证机制的优先级信息。

步骤 901：UE 确定建立 PDU 会话时，UE 通过无线接入网节点和 AMF 节点向 SMF 发送 PDU 会话请求消息，该消息中包含 PDU 会话 ID。可选的，该消息中还可以包含以下至少一项：UE 是否支持边缘使能客户端的指示信息，UE 所支持的至少一个认证机制，和 UE 所支持的至少一个认证机制的优先级信息。

例如，在一种可能的实现方案中，上述 PDU 会话请求消息中可以包含 UE 的能力。UE 的能力中包括以下至少一项：UE 所支持的至少一个认证机制，UE 是否支持边缘使能客户端的指示信息，和 UE 所支持的至少一个认证机制的优先级信息。或者，上述 UE 的能力可以单独发送，即 UE 通过无线接入网节点和 AMF 节点，向 SMF 发送 PDU 会话请求消息和 UE 的能力。

步骤 902：SMF 接收到 UE 发送的 PDU 会话请求消息之后，当需要获取 UE 的签约信息时，SMF 向 UDM 发送 Nudm_SDM_Get 请求消息，该请求消息中包含 UE 的标识。所述 UE 的标识可以为 SUPI。

步骤 903：UDM 根据上述请求消息中包含的 UE 的标识，获取 UE 的签约信息，并向 AMF 发送 Nudm_SDM_Get 响应消息，该响应消息中包含 ECS 信息。该 ECS 信息中包含以下至少一项：ECS 标识和 ECS 对应的候选认证机制。

步骤 904：SMF 接收 UDM 发送的 Nudm_SDM_Get 响应消息，向 UE 发送 PDU 会话响应消息，该 PDU 会话响应消息中包含 ECS 信息。一种可能的方案中，上述 ECS 信息中可包含在 PDU 会话响应消息的协议配置选项（protocol configuration option, PCO）中。

步骤 905：UE 的 NAS 层向对应的 EEC 发送接收到的 ECS 信息。可选的，NAS 层可以直接向 EEC 发送接收到的 ECS 信息，或者间接的通过上层向 EEC 发送 ECS 信息等。

步骤 906：EEC 根据接收到的 ECS 信息中包含的候选认证机制，与 ECS 之间建立通信连接。

为了便于区分不同的认证机制，在以下描述中，采用四种表示方式：SMF 所确定的 UE 与 ECS 间通信所使用的认证机制称为第一认证机制；UE 所支持的认证机制可以称为第二认证机制；ECS 所支持的认证机制可称为第三认证机制；将 UDM 确定的 UE 与 ECS 间通信所使用的认证机制作为第四认证机制。

在一种设计中，所述候选认证机制为 ECS 所支持的至少一个第三认证机制。上述 Nudm_SDM_Get 响应消息中的 ECS 信息中包括 ECS 所支持的至少一个第三认证机制。可选的，该消息中还包括 ECS 所支持的至少一个第三认证机制的优先级信息。SMF 接收到上述 Nudm_SDM_Get 响应消息，获取其中包含的 ECS 所支持的至少一个第三认证机制。可选的，SMF 还可以获取上述响应消息中包含的 ECS 所支持的至少一个第三认证机制中的优先级信息。SMF 向 UE 发送 PDU 会话响应消息，该 PDU 会话响应消息中包括 ECS 所支持的至少一个第三认证机制。可选的，该 PDU 会话响应消息中还可以包括 ECS 所支持的至少一个第三认证机制的优先级信息。UE 根据该 ECS 所支持的至少一个第三认证机制和辅助信息，确定目标认证机制，辅助信息中至少包括 UE 所支持的至少一个第二认证机制，和 UE 接入 ECS 所使用的网络类型。可选的，该辅助信息中还可以包括：UE 所支持的至少一个认证机制的优先级信息，ECS 所支持的至少一个认证机制中的优先级信息等。后续，UE 的 NAS 层向 EEC 发送目标认证机制，EEC 根据目标认证机制，与 ECS 之间建立通信连接。EEC 与 ECS 建立通信连接的过程，与 EES 与 EES 间建立通信连接的过程相似，可相互参见。在一种可能的方案中，可具体由 UE 中的 NAS 层执行上述“根据 ECS 所支持的至少一个第三认证机制和辅助信息，确定目标认证机制”的过程，之后 NAS 层将上述目标认证机制发送给 EEC，EEC 根据该目标认证机制与 ECS 之间建立通信连接。

在另一种设计中，所述候选认证机制为 UE 与 ECS 通信时所使用的至少一个第四认证机制。上述 PDU 会话请求中携带有 UE 的能力信息，UE 的能力信息中包括以下至少一项：UE 所支持的至少一个第二认证机制，UE 接入 ECS 使用的网络类型，和 UE 所支持的至少一个第二认证机制的优先级信息。当 SMF 需要获取 UE 的签约信息时，SMF 向 UDM 发送 Nudm_SDM_Get 请求消息，该请求消息中包括 UE 标识。在一种可能的方案中，上述 Nudm_SDM_Get 请求消息中包含 UE 的能力，UDM 根据 ECS 所支持的至少一个第三认证机制和辅助信息，确定候选认证机制。所述辅助信息中可以包括以下至少一项：UE 所支持的至少一个第二认证机制和 UE 所接入 ECS 所使用的网络类型。可选的，该辅助信息中还可以包括以下至少一项：UE 所支持的至少一个认证机制的优先级信息，和 ECS 所支持的至少一个认证机制的优先级信息。UDM 向 SMF 发送 Nudm_SDM_Get 响应消息，该响应消息中包括候选认证机制。SMF 向 UE 发送 PDU 会话响应消息，该 PDU 会话响应消息中包括候选认证机制；UE 获取该 PDU 会话响应消息中的候选认证机制，UE 的 NAS 层向 EEC 发送候选认证机制；EEC 根据候选认证机制，与 ECS 间建立通信连接等。

在另一种设计中，所述候选认证机制为 UE 与 ECS 通信时所使用的至少一个第四认证机制。上述 PDU 会话请求中携带有 UE 的能力信息。当 SMF 需要获取 UE 的签约信息时，SMF 向 UDM 发送 Nudm_SDM_Get 请求消息，该请求消息中包括 UE 标识。上述

Nudm_SDM_Get 响应消息包括 ECS 所支持的至少一个第三认证机制。SMF 根据 ECS 所支持的至少一个第三认证机制和辅助信息，确定候选认证机制。SMF 向 UE 发送 PDU 会话响应消息，该 PDU 会话响应消息中包括候选认证机制。UE 的 NAS 层向 EEC 发送候选认证机制。EEC 根据候选认证机制，与 ECS 之间建立通信连接。

在本申请实施例中，UE 与 SMF 交互可获取 ECS 所对应的候选认证机制，UE 与 ECS 间，无需再进行认证的协商流程，减少了信令开销，降低建立通信时延，提高通信体验。

实施例五

在该实施例中，以终端设备为 UE 为例，介绍终端设备与第一网元间采用 AKMA 认证机制，建立通信连接的过程，如图 10 所示，该流程至少包括:

步骤 1000a: UE 注册到运营商网络，并执行主认证流程，在主认证流程过程中，UE 和 AUSF 间分别生成鉴权密钥 K_{AUSF}。如果 UE 能够使用 AKMA 认证机制（例如 AUSF 可以根据从 UDM 接收到 AKMA 指示确定 UE 能够使用 AKMA 认证机制），则 AUSF 在主身份验证过程成功后，根据 TS33.535 中的定义生成 AKMA 密钥（K_{AKMA})和所述 AKMA 密钥对应的标识 A-KID。

步骤 1000b.在生成所述 AKMA 密钥后，AUSF 向 AAnF 发送 AKMA 认证密钥注册请求，该请求中包括 UE 的永久身份标识 SUPI、A-KID 和 K_{AKMA}。

步骤 1001: UE 接入网络后的任一时刻，当 UE 需要获取边缘服务时，UE 向第一网元发送第一消息。

步骤 1002: 第一网元根据 UE 发送的第一消息向 UE 发送第二消息，该第二消息中包括第二网元的标识和 AKMA 能力。AKMA 能力指示第二网元支持使用 AMKA 认证机制。

步骤 1003: 当 UE 确定与第二网元通信时，若 UE 支持 AKMA，且第二网元也支持 AKMA（可选的，可根据上述步骤 2 中的指示确定第二网元是否支持 AKMA），则 UE 根据 TS33.535 中的定义推演 AKMA 密钥和 A-KID，进一步的根据 AKMA 密钥推演第二网元对应的 K_{AF}。所述的推演参考 TS33.535 中的 K_{AF} 的推演方法。需要说明的是，上述 K_{AF} 的下标 AF 表示第二网元，若上述第二网元为 EES，则上述 K_{AF} 代表 K_{EES} 等。同理，若第二网元为 ECS，或 EAS 等，则需要将上述 K_{AF} 中的下标由 “AF” 更换为 “ECA 或 EAS” 等。对于支持 AKMA 的 UE，AKMA 密钥和 A-KID 的推演可以在主认证流程之后，到确定与第二网元使用 AKMA 之前的任意时间执行。另一种可能的实现方式为: 在确定与第二网元通信前，UE 已经推演了 AKMA 密钥和 A-KID。此时 UE 根据第二网元支持 AKMA 认证机制，获取本地存储的 A-KID，并在步骤 1004 中包含 A-KID。进一步的，根据本地存储的 AKMA 密钥生成第二网元对应的 K_{AF}.

步骤 1004: UE 使用 K_{AF} 和通信连接建立请求消息的所有信息或部分信息生成 MAC-I，并在通信连接建立请求消息中携带的 MAC-I，向第二网元发送包括 A-KID 和 MAC-I 的通信连接建立请求。

步骤 1005: 第二网元接收到通信连接建立请求后，第二网元发现 AKMA 锚点功能（AKMA Anchor Function，AAnF）或者 NEF。

步骤 1006: 第二网元获取与 UE 对应的 K_{AF} 密钥。在一种可能的实现方式中，可参见步骤 1006a，第二网元向 AAnF 发送 AKMA 认证密钥获取请求，AAnF 向第二网元发送 AKMA 认证密钥获取响应，该响应中包括 K_{AF} 密钥等。

步骤 1007：如果 UE 被授权执行操作，则第二网元使用 K_{AF} 验证 MAC-I；第二网元向 UE 发送通信连接建立请求的响应消息。

可选的，上述方法还包括：第二网元接收到通信连接建立请求，获取其中的 A-KID 和 MAC-I，第二网元向 AAnF 发送 A-KID，如果能够获取到 K_{AF}，则说明第二网元确定 UE 是合法的，即第二网元完成对 UE 的认证。

可选的，上述方法还包括：第二网元给 UE 返回的通信连接建立请求的响应消息中还可以包括第二 MAC；第二 MAC 是使用 K_{AF} 或者使用基于 K_{AF} 生成的密钥生成的；UE 接收通信连接建立请求的响应消息，获取其中的第二 MAC，对第二 MAC 验证，验证成功之后，UE 确认第二网元是合法的，即 UE 完成对第二网元的认证。进一步可选的，第二 MAC 使用 K_{AF} 或者使用基于 K_{AF} 生成的密钥和响应消息中的部分或全部信息生成的。

可以理解的是，在上述实施例一中，上述第一网元可以为 ECS，第二网元为 EES，或者，在上述实施例二中，上述第一网元可以为 EES，上述第二网元可以为 EAS，或者，在上述实施例三中，上述第一网元为 AMF，第二网元为 ECS，或者，在上述实施例四中，第一网元可以为 SMF，第二网元可以为 ECS。

通过上述可以看出，第一网元与第二网元间可进行双认证，使得两者间建立安全的通信连接。

基于与上述方法实施例同一发明构思，本申请实施例还提供一种装置，用于执行上述方法实施例中终端设备执行的方法。相关特征可参见上述方法实施例，此处不再赘述。如图 11 所示，该装置可以包括通信单元 1101 和处理单元 1102：

通信单元 1101，用于接收来自第一网元的第一消息，所述第一消息包括第二网元的标识以及第一指示信息，所述第一指示信息用于指示第二网元关联的候选认证机制；处理单元 1102，用于基于所述候选认证机制，与所述第二网元之间建立通信连接。

可选的，通信单元 1101，还用于向所述第一网元发送第二消息，所述第一消息为所述第二消息的响应消息。

在一种可能的设计中，所述候选认证机制为所述终端设备与所述第二网元之间建立通信连接时使用的至少一个第一认证机制。

可选的，所述第二消息中包括所述终端设备接入所述第二网元所使用的网络类型；其中，所述至少一个第一认证机制是与所述网络类型对应的认证机制。

可选的，所述第二消息中包括所述终端设备所支持的至少一个第二认证机制；其中，所述至少一个第一认证机制包括在所述至少一个第二认证机制中。

可选的，所述第二消息中还包括至少一个第二认证机制中的优先级信息；所述至少一个第二认证机制用于所述至少一个第一认证机制的选择。

可选的，所述基于所述候选认证机制，与所述第二网元之间建立通信连接，包括：

生成与所述目标认证机制对应的第一密钥以及第一密钥标识；其中，所述目标认证机制为所述至少一个认证机制中的一个；向所述第二网元发送通信连接建立请求，所述通信连接建立请求中包括所述第一密钥标识。

在另一种设计中，所述候选认证机制为所述第二网元所支持的至少一个第三认证机制。

可选的，所述基于所述候选认证机制，与所述第二网元之间建立通信连接，包括：基于所述至少一个第三认证机制和辅助信息，确定目标认证机制，所述辅助信息中包括以下至少一项：所述终端设备所支持的至少一个第二认证机制，和所述终端设备接入所述第二

网元所使用的网络类型；生成与所述目标认证机制对应的第一密钥以及第一密钥标识；向所述第二网元发送通信连接建立请求，所述通信连接建立请求包括所述第一密钥标识。

可选的，所述辅助信息还包括以下至少一项：所述至少一个第二认证机制中的优先级信息，和所述至少一个第三认证机制中的优先级信息。

可选的，所述第一消息中还包括所述至少一个第三认证机制中的优先级信息。

可选的，处理单元 1102 还用于：根据所述第一密钥以及所述第二网元的标识，生成第二密钥。

可选的，处理单元 1102，还用于：使用所述第二密钥对所述通信连接建立请求进行安全保护，以生成第一消息认证码 MAC；其中，所述通信连接建立请求还包括所述第一 MAC。

在一种设计中，所述第一网元为边缘配置服务器 ECS，所述第二网元为边缘使能服务器 EES，或者，所述第一网元为 EES，所述第二网元为边缘应用服务器 EAS。

在另一种设计中，所述第一网元为接入和移动性管理功能 AMF 或者会话管理功能 SMF，所述第二网元为边缘配置服务器 ECS。

可选的，所述第一消息为非接入层 NAS 消息。

可选的，所述第一消息为所述终端设备请求注册的响应消息，或者所述终端设备请求建立协议数据单元 PDU 会话的响应消息。

可选的，所述候选认证机制包括以下至少一项：应用的认证和密码管理 AKMA 服务，通用引导架构 GBA 服务，和证书机制。

基于与上述方法实施例同一发明构思，本申请实施例还提供一种装置，用于执行上述方法实施例中第一网元执行的方法。相关特征可参见上述方法实施例，此处不再赘述。仍可参照图 11 所示，该装置包括通信单元 1101 和处理单元 1102：

处理单元 1102，用于确定候选认证机制；通信单元 1101，用于向终端设备发送第一消息，所述第一消息中包括第二网元的标识以及第一指示信息，所述第一指示信息用于指示第二网元关联的所述候选认证机制，所述候选认证机制用于所述终端设备与所述第二网元间建立通信连接。

可选的，通信单元 1101，还用于接收来自所述终设备的第二消息，所述第一消息为所述第二消息的响应消息。

可选的，所述候选认证机制为所述终端设备与所述第二网元之间建立通信连接时使用的至少一个第一认证机制，所述确定候选认证机制，包括：

根据所述第二网元所支持的至少一个第三认证机制和辅助信息，确定候选认证机制，所述辅助信息包括以下到少一项：终端设备所支持的至少一个第二认证机制，和所述终端设备接入所述第二网元所使用的网络类型。

可选的，所述第二消息中包括所述终端设备接入所述第二网元所使用的网络类型。

可选的，所述第二消息中包括所述终端设备支持的至少一个第二认证机制。

可选的，所述辅助信息还包括以下至少一项：所述至少一个第二认证机制中的优先级信息，和所述至少一个第三认证机制中的优先级信息。

可选的，所述第二消息中还包括至少一个第二认证机制中的优先级信息。

可选的，所述候选认证机制为所述第二网元所支持的至少一个第三认证机制。

可选的，所述第一消息中还包括所述至少一个第三认证机制中的优先级信息。

在一种设计中，所述第一网元为 ECS，所述第二网元为 EES，或者，所述第一网元为

EES，所述第二网元为 EAS。

在另一种设计中，所述第一网元为 AMF 或 SMF，所述第二网元为 ECS。

可选的，所述第一消息为 NAS 消息。

可选的，所述第一消息为所述终端设备请求注册的响应消息，或者所述终端设备请求建立 PDU 会话的响应消息。

可选的，所述候选认证机制包括以下至少一项：AKMA 服务，GBA 服务，和证书机制。

本申请实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，另外，在本申请各个实施例中的各功能单元可以集成在一个处理器中，也可以是单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

该集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或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中，包括若干指令用以使得一台终端设备（可以是个人计算机，手机，或者网络设备等）或处理器（processor）执行本申请各个实施例该方法的全部或部分步骤。而前述的存储介质包括: U 盘、移动硬盘、只读存储器（read-only memory，ROM）、随机存取存储器（random access memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

在本申请实施例中，所述基站和所述终端设备均可以采用集成的方式划分各个功能模块的形式来呈现。这里的“模块”可以指特定 ASIC，电路，执行一个或多个软件或固件程序的处理器和存储器，集成逻辑电路，和/或其他可以提供上述功能的器件。

在一个简单的实施例中，本领域的技术人员可以想到所述终端设备和第一网元可以采用图 12 所示的形式。

如图 12 所示的通信装置 1200，包括至少一个处理器 1201、存储器 1202，可选的，还可以包括通信接口 1203。

存储器 1202 可以是易失性存储器，例如随机存取存储器；存储器也可以是非易失性存储器，例如只读存储器，快闪存储器，硬盘（hard disk drive，HDD）或固态硬盘（solid-state drive，SSD）、或者存储器 1202 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器 1202 可以是上述存储器的组合。

本申请实施例中不限定上述处理器 1201 以及存储器 1202 之间的具体连接介质。本申请实施例在图中以存储器 1202 和处理器 1201 之间通过总线 1204 连接，总线 1204 在图中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。该总线 1204 可以分为地址总线、数据总线、控制总线等。为便于表示，图 12 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

处理器 1201 可以具有数据收发功能，能够与其他设备进行通信，在如图 12 装置中，也可以设置独立的数据收发模块，例如通信接口 1203，用于收发数据；处理器 1201 在与其他设备进行通信时，可以通过通信接口 1203 进行数据传输。

当终端设备采用图 12 所示的形式时，图 12 中的处理器 1201 可以通过调用存储器 1202

中存储的计算机执行指令，使得终端设备可以执行上述任一方法实施例中所述终端设备的功能。或者，当第一网元采用图 12 所示的形式时，图 12 中的处理器 1201 可以通过调用存储器 1202 中存储的计算机执行指令，使得第一网元可以执行上述任一方法实施例中所述第一网元的功能。

具体的，图 11 中的通信单元 1101 和处理单元 1102 的功能/实现可以通过图 12 中的处理器 1201 调用存储器 1202 中存储的计算机程序指令来实现。或者，图 11 中的处理单元 1102 的功能/实现过程可以通过图 12 中的处理器 1201 调用存储器 1202 中存储的计算机执行指令来实现，图 11 中的通信单元 1101 的功能/实现可以通过图 12 中的通信接口 1203 来实现。

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用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请的方法、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、嵌入式处理机或其他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他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／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，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。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在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。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1、一种建立安全通信方法，其特征在于，包括:

终端设备接收来自第一网元的第一消息，所述第一消息包括第二网元的标识以及第一指示信息，所述第一指示信息用于指示与所述第二网元关联的候选认证机制;

所述终端设备基于所述候选认证机制，与所述第二网元之间建立通信连接。

2、如权利要求 1 所述的方法，其特征在于，还包括:

所述终端设备向所述第一网元发送第二消息，所述第一消息为所述第二消息的响应消息。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述候选认证机制为所述终端设备与所述第二网元之间建立通信连接时使用的至少一个第一认证机制。

4、如权利要求 3 所述的方法，其特征在于，所述第二消息中包括所述终端设备接入所述第二网元所使用的网络类型；其中，所述至少一个第一认证机制是与所述网络类型对应的认证机制。

5、如权利要求 3 或 4 所述的方法，其特征在于，所述第二消息中包括所述终端设备所支持的至少一个第二认证机制；其中，所述至少一个第一认证机制包括在所述至少一个第二认证机制中。

6、如权利要求 5 所述的方法，其特征在于，所述第二消息中还包括至少一个第二认证机制的优先级信息；所述至少一个第二认证机制用于所述至少一个第一认证机制的选择。

7、如权利要求 3 至 6 中任一项所述的方法，其特征在于，所述终端设备基于所述候选认证机制，与所述第二网元之间建立通信连接，包括:

所述终端设备生成与目标认证机制对应的第一密钥以及第一密钥标识；其中，所述目标认证机制为所述至少一个第一认证机制中的一个;

所述终端设备向所述第二网元发送通信连接建立请求，所述通信连接建立请求中包括所述第一密钥标识。

8、如权利要求 1 或 2 所述的方法，其特征在于，所述候选认证机制为所述第二网元所支持的至少一个第三认证机制。

9、如权利要求 8 所述的方法，其特征在于，所述终端设备基于所述候选认证机制，与所述第二网元之间建立通信连接，包括:

所述终端设备基于所述至少一个第三认证机制和辅助信息，确定目标认证机制，所述辅助信息中包括以下至少一项：所述终端设备所支持的至少一个第二认证机制，和所述终端设备接入所述第二网元所使用的网络类型;

所述终端设备生成与所述目标认证机制对应的第一密钥以及第一密钥标识;

所述终端设备向所述第二网元发送通信连接建立请求，所述通信连接建立请求包括所述第一密钥标识。

10、如权利要求 9 所述的方法，其特征在于，所述辅助信息还包括以下至少一项：所述至少一个第二认证机制的优先级信息，和所述至少一个第三认证机制的优先级信息。

11、如权利要求 10 所述的方法，其特征在于，所述第一消息中还包括所述至少一个第三认证机制的优先级信息。

12、如权利要求 7 或 9 所述的方法，其特征在于，所述方法还包括:

所述终端设备根据所述第一密钥以及所述第二网元的标识，生成第二密钥。

13、如权利要求 12 所述的方法，其特征在于，所述方法还包括:

所述终端设备使用所述第二密钥对所述通信连接建立请求进行安全保护，以生成第一消息认证码 MAC；其中，所述通信连接建立请求还包括所述第一 MAC。

14、如权利要求 1 至 13 中任一项所述的方法，其特征在于，所述第一网元为边缘配置服务器 ECS，所述第二网元为边缘使能服务器 EES，或者，所述第一网元为 EES，所述第二网元为边缘应用服务器 EAS。

15、如权利要求 1 至 13 中任一项所述的方法，其特征在于，所述第一网元为接入和移动性管理功能 AMF 或者会话管理功能 SMF，所述第二网元为边缘配置服务器 ECS。

16、如权利要求 15 所述的方法，其特征在于，所述第一消息为非接入层 NAS 消息。

17、如权利要求 16 所述的方法，其特征在于，所述第一消息为所述终端设备请求注册的响应消息，或者所述终端设备请求建立协议数据单元 PDU 会话的响应消息。

18、如权利要求 1 至 17 中任一项所述的方法，其特征在于，所述候选认证机制包括以下至少一项：应用的认证和密码管理 AKMA 服务，通用引导架构 GBA 服务，和证书机制。

19、一种建立安全通信方法，其特征在于，包括:

第一网元确定候选认证机制;

所述第一网元向终端设备发送第一消息，所述第一消息中包括第二网元的标识以及第一指示信息，所述第一指示信息用于指示与所述第二网元关联的候选认证机制，所述候选认证机制用于所述终端设备与所述第二网元间建立通信连接。

20、如权利要求 19 所述的方法，其特征在于，还包括:

所述第一网元接收来自所述终设备的第二消息，所述第一消息为所述第二消息的响应消息。

21、如权利要求 19 或 20 所述的方法，其特征在于，所述候选认证机制为所述终端设备与所述第二网元之间建立通信连接时使用的至少一个第一认证机制，所述第一网元确定候选认证机制，包括:

所述第一网元根据所述第二网元所支持的至少一个第三认证机制和辅助信息，确定候选认证机制，所述辅助信息包括以下至少一项：终端设备所支持的至少一个第二认证机制，和所述终端设备接入所述第二网元所使用的网络类型。

22、如权利要求 21 所述的方法，其特征在于，所述第二消息中包括所述终端设备接入所述第二网元所使用的网络类型；其中，所述至少一个第一认证机制是与所述网络类型对应的认证机制。

23、如权利要求 21 或 22 所述的方法，其特征在于，所述第二消息中包括所述终端设备所支持的至少一个第二认证机制;；其中，所述至少一个第一认证机制包括在所述至少一个第二认证机制中。

24、如权利要求 21 至 23 中任一项所述的方法，其特征在于，所述辅助信息还包括以下至少一项：所述至少一个第二认证机制的优先级信息，和所述至少一个第三认证机制的优先级信息；所述至少一个第二认证机制用于所述至少一个第一认证机制的选择。

25、如权利要求 24 所述的方法，其特征在于，所述第二消息中还包括至少一个第二认证机制的优先级信息。

26、如权利要求 19 或 20 所述的方法，其特征在于，所述候选认证机制为所述第二网元所支持的至少一个第三认证机制。

27、如权利要求 26 所述的方法，其特征在于，所述第一消息中还包括所述至少一个第三认证机制的优先级信息。

28、如权利要求 19 至 27 中任一项所述的方法，其特征在于，所述第一网元为 ECS，所述第二网元为 EES，或者，所述第一网元为 EES，所述第二网元为 EAS。

29、如权利要求 19 至 27 中任一项所述的方法，其特征在于，所述第一网元为 AMF 或 SMF，所述第二网元为 ECS。

30、如权利要求 29 所述的方法，其特征在于，所述第一消息为 NAS 消息。

31、如权利要求 30 所述的方法，其特征在于，所述第一消息为所述终端设备请求注册的响应消息，或者所述终端设备请求建立 PDU 会话的响应消息。

32、如权利要求 19 至 31 中任一项所述的方法，其特征在于，所述候选认证机制包括以下至少一项：AKMA 服务，GBA 服务，和证书机制。

33、一种装置，其特征在于，包括用于实现权利要求 1 至 18 中任一项所述的方法的单元，或者包括用于实现权利要求 19 至 32 中任一项所述的方法的单元。

34、一种装置，其特征在于，包括处理器和存储器，所述存储器中存储有指令，所述处理器执行所述指令时，使得所述通信装置执行权利要求 1 至 18 中任一项所述的方法，或者使得通信装置执行权利要求 19 至 32 中任一项所述的方法。

35、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中存储有指令，当其在计算机上运行时，使得计算机执行权利要求 1 至 18 中任一项所述的方法，或者使得计算机执行权利要求 19 至 32 中任一项所述的方法。

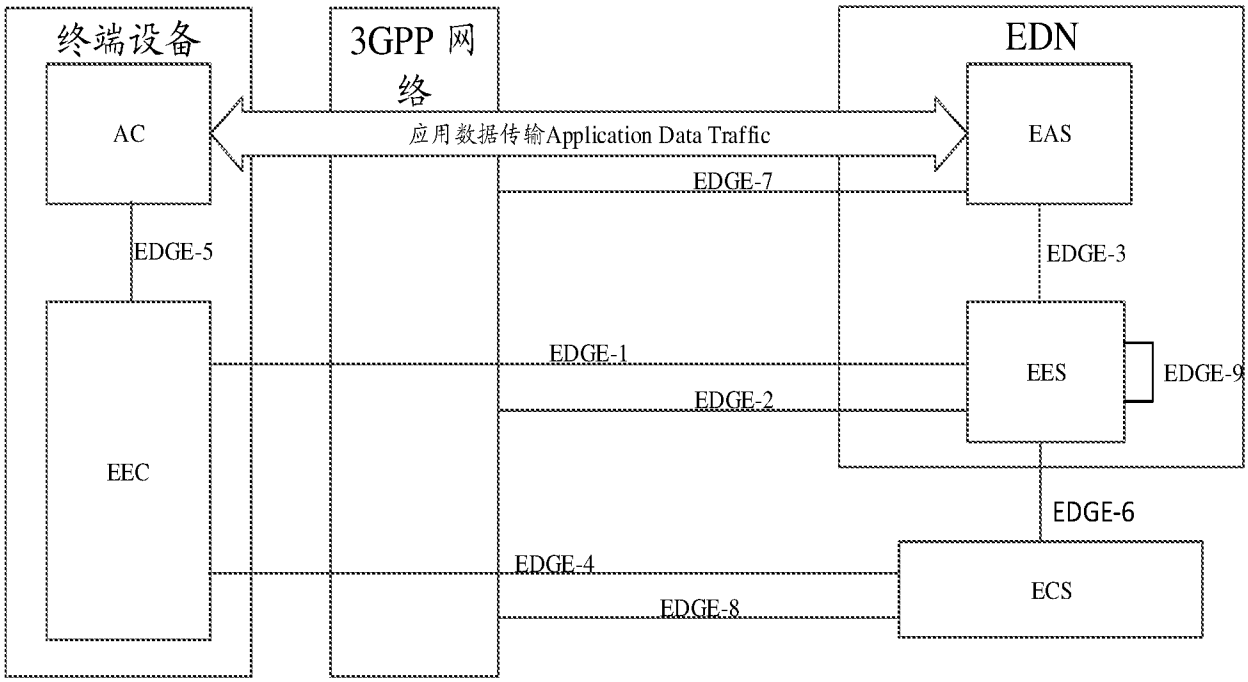
终端设备
3GPP 网络
EDN
AC
应用数据传输Application Data Traffic
EAS
EDGE-7
EDGE-5
EDGE-3
EDGE-1
EES
EDGE-9
EDGE-2
EEC
EDGE-6
EDGE-4
ECS
EDGE-8

图 1

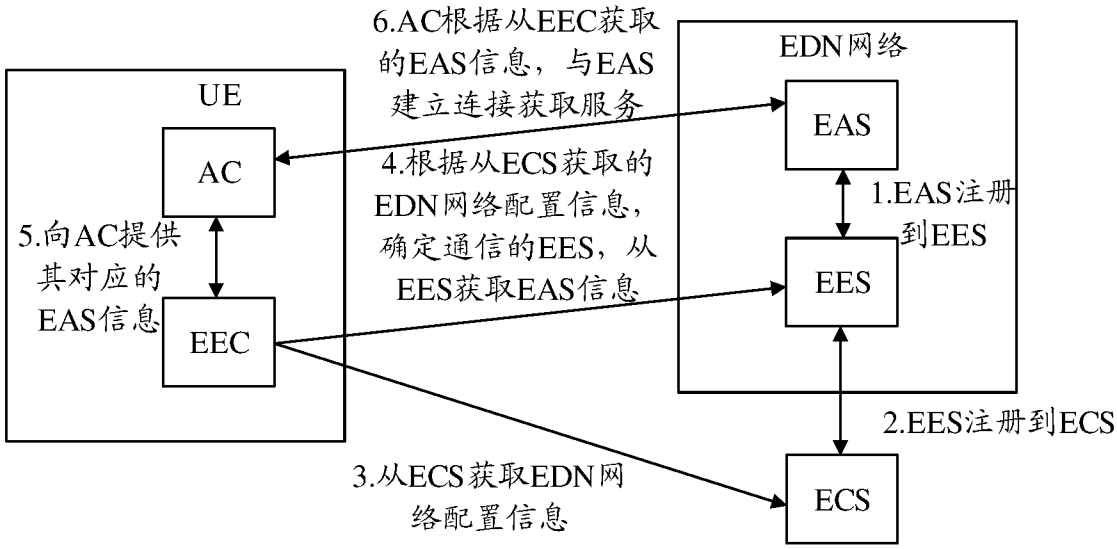
6.AC根据从EEC获取的EAS信息，与EAS建立连接获取服务
EDN网络
UE
EAS
AC
4.根据从ECS获取的EDN网络配置信息，确定通信的EES，从EES获取EAS信息
1.EAS注册到EES
5.向AC提供其对应的EAS信息
EES
EEC
2.EES注册到ECS
3.从ECS获取EDN网络配置信息
ECS

图 2

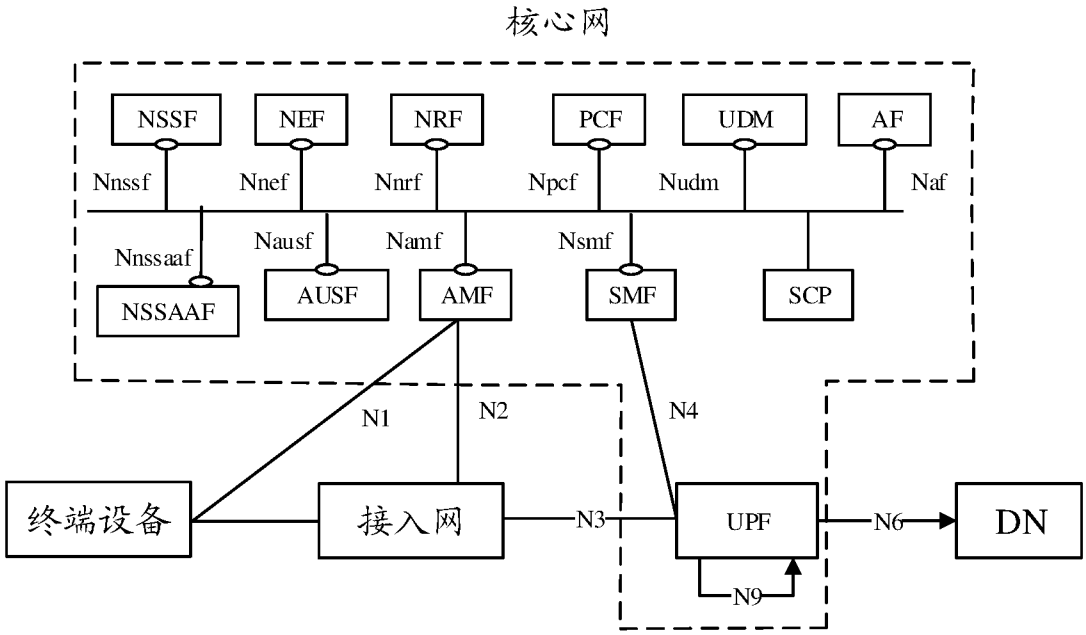
核心网
NSSF
NEF
NRF
PCF
UDM
AF
Nnssf
Nnef
Nnrf
Npcf
Nudm
Naf
Nnssaaf
Nausf
Namf
Nsmf
NSSAAF
AUSF
AMF
SMF
SCP
N1
N2
N4
终端设备
接入网
N3
UPF
N6
DN
N9

图 3

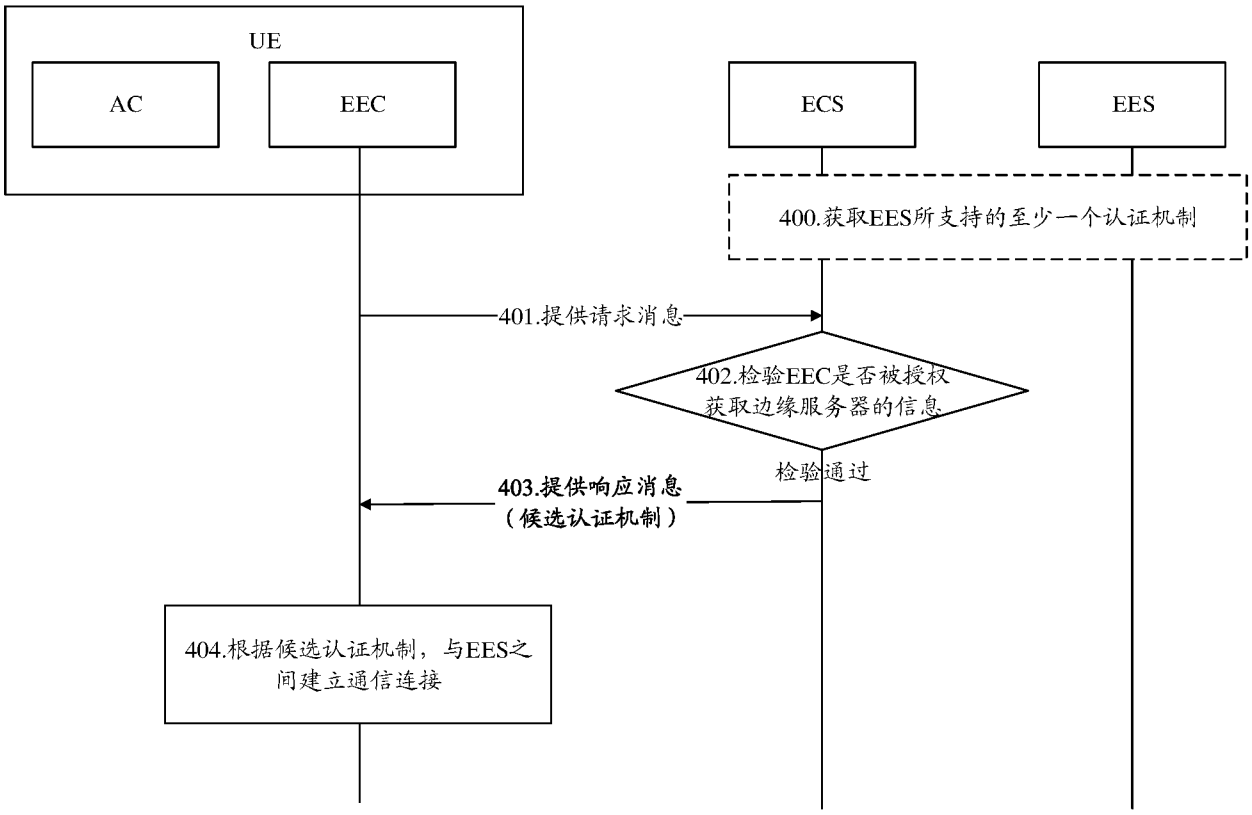
UE
AC
EEC
ECS
EES
400.获取EES所支持的至少一个认证机制
401.提供请求消息
402.检验EEC是否被授权
获取边缘服务器的信息
检验通过
403.提供响应消息
（候选认证机制）
404.根据候选认证机制，与EES之
间建立通信连接

图 4

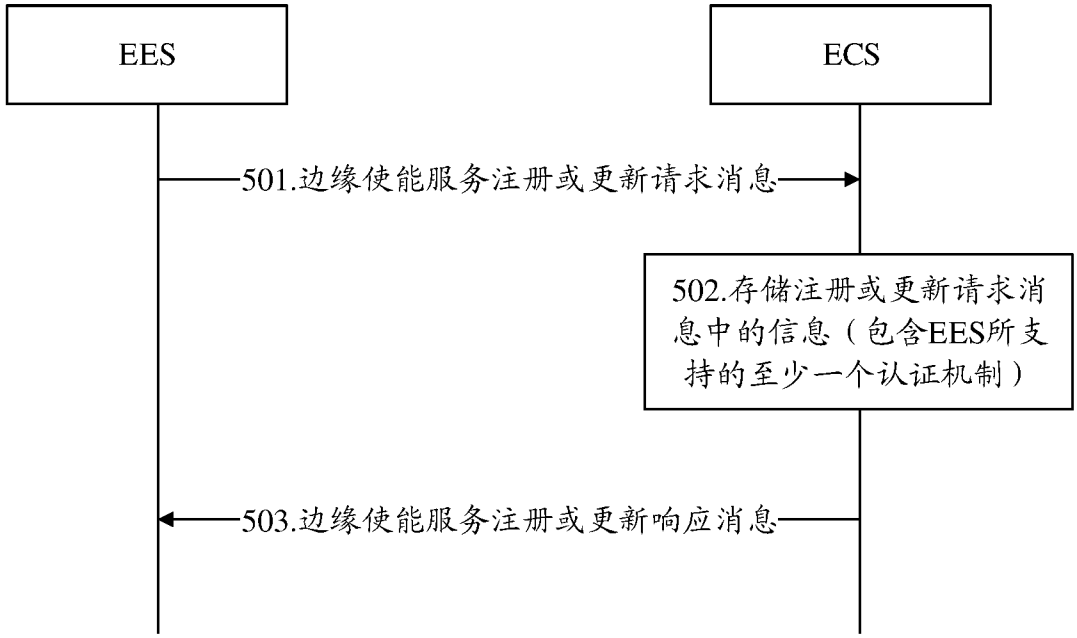
EES
ECS
501.边缘使能服务注册或更新请求消息
502.存储注册或更新请求消息中的信息（包含EES所支持的至少一个认证机制）
503.边缘使能服务注册或更新响应消息

图 5

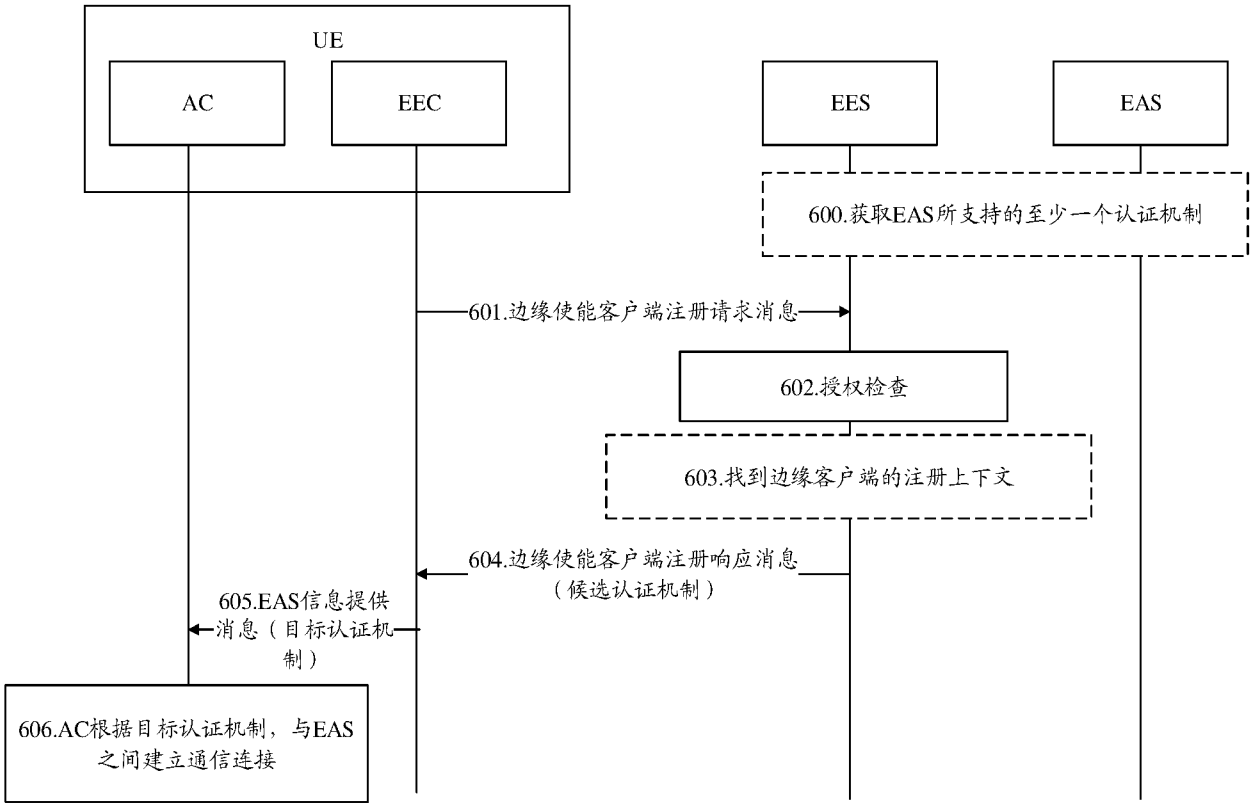
UE
AC
EEC
EES
EAS
600.获取EAS所支持的至少一个认证机制
601.边缘使能客户端注册请求消息
602.授权检查
603.找到边缘客户端的注册上下文
604.边缘使能客户端注册响应消息（候选认证机制）
605.EAS信息提供消息（目标认证机制）
606.AC根据目标认证机制，与EAS之间建立通信连接

图 6

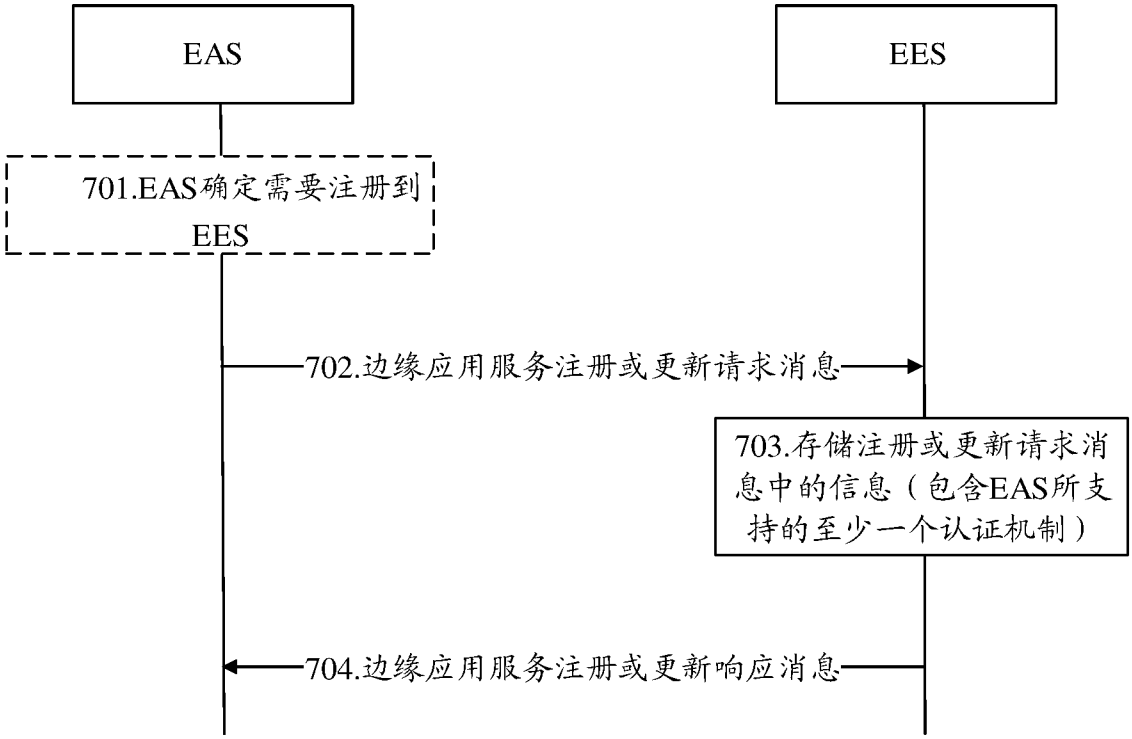
EAS
EES
701.EAS确定需要注册到EES
702.边缘应用服务注册或更新请求消息
703.存储注册或更新请求消息中的信息（包含EAS所支持的至少一个认证机制）
704.边缘应用服务注册或更新响应消息

图 7

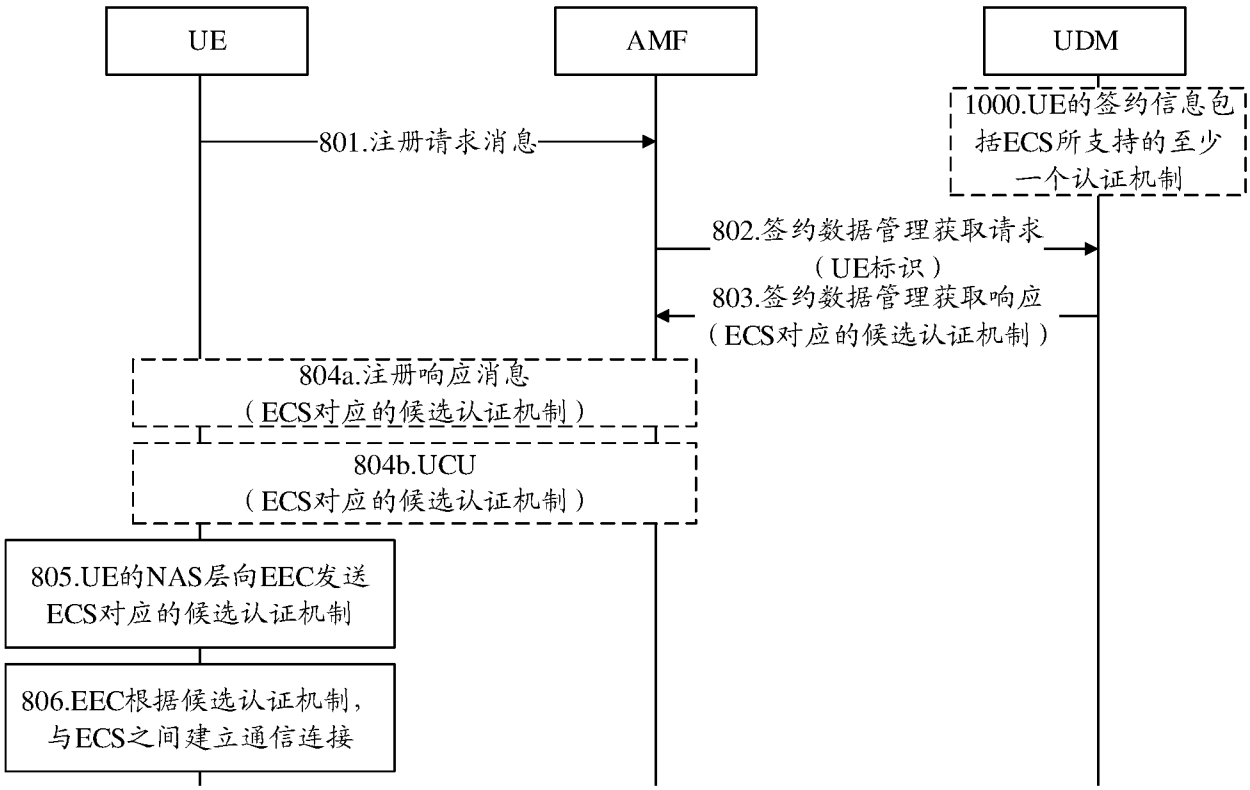
UE
AMF
UDM
1000.UE的签约信息包括ECS所支持的至少一个认证机制
801.注册请求消息
802.签约数据管理获取请求（UE标识）
803.签约数据管理获取响应（ECS对应的候选认证机制）
804a.注册响应消息（ECS对应的候选认证机制）
804b.UCU（ECS对应的候选认证机制）
805.UE的NAS层向EEC发送ECS对应的候选认证机制
806.EEC根据候选认证机制，与ECS之间建立通信连接

图 8

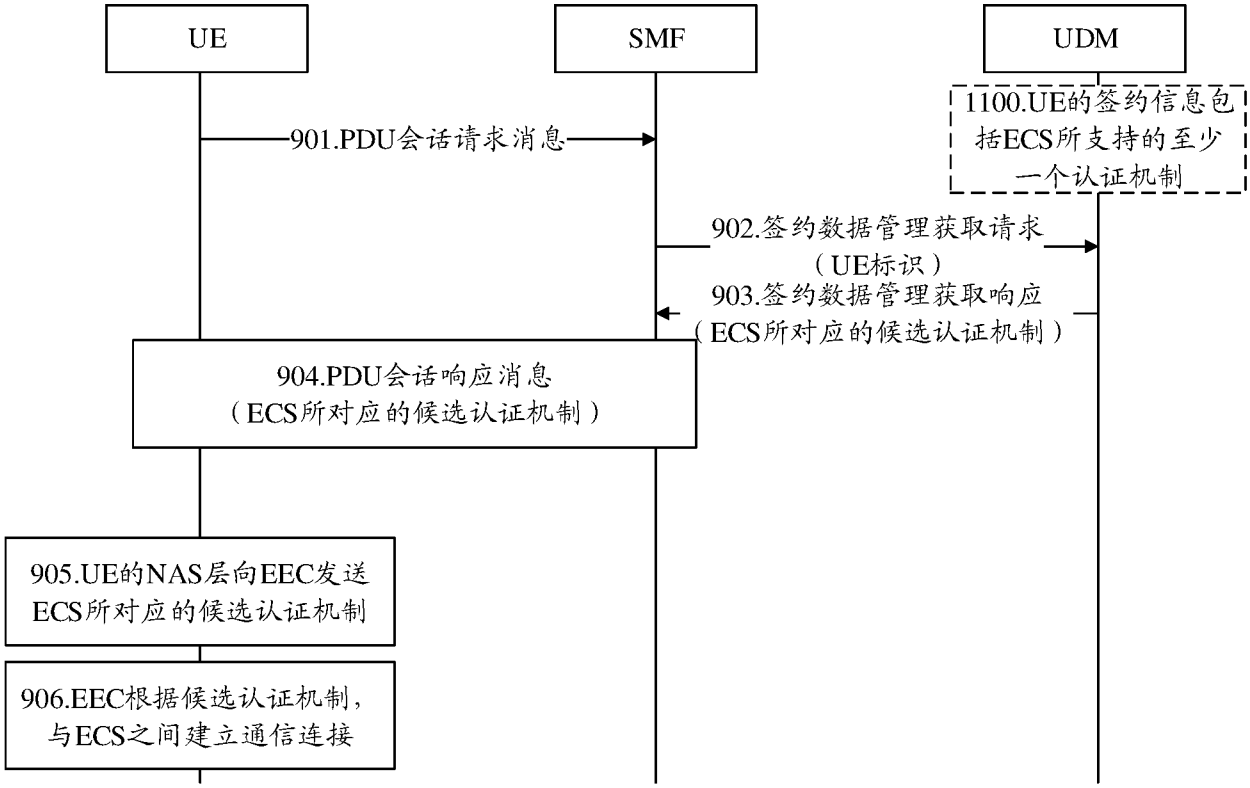
UE
SMF
UDM
1100.UE的签约信息包括ECS所支持的至少一个认证机制
901.PDU会话请求消息
902.签约数据管理获取请求（UE标识）
903.签约数据管理获取响应（ECS所对应的候选认证机制）
904.PDU会话响应消息（ECS所对应的候选认证机制）
905.UE的NAS层向EEC发送ECS所对应的候选认证机制
906.EEC根据候选认证机制，与ECS之间建立通信连接

图 9

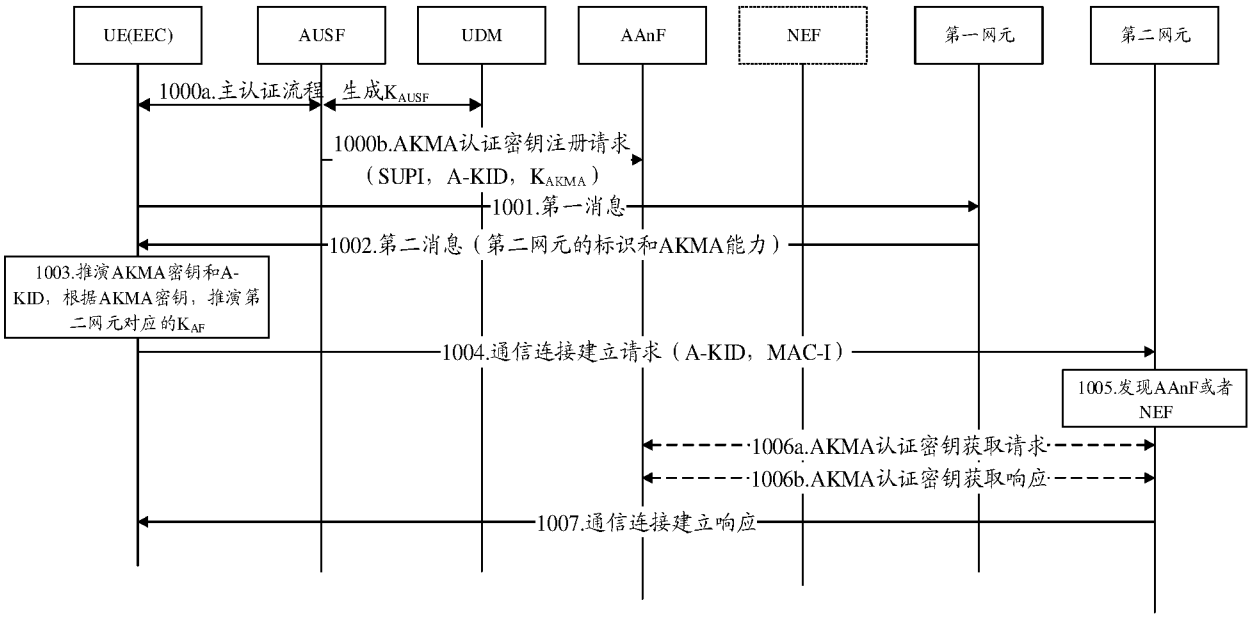
UE(EEC)
AUSF
UDM
AAnF
NEF
第一网元
第二网元
1000a.主认证流程
生成K_{AUSF}
1000b.AKMA认证密钥注册请求（SUPI，A-KID，K_{AKMA}）
1001.第一消息
1002.第二消息（第二网元的标识和AKMA能力）
1003.推演AKMA密钥和A-KID，根据AKMA密钥，推演第二网元对应的K_{AF}
1004.通信连接建立请求（A-KID，MAC-I）
1005.发现AAnF或者NEF
1006a.AKMA认证密钥获取请求
1006b.AKMA认证密钥获取响应
1007.通信连接建立响应

图 10

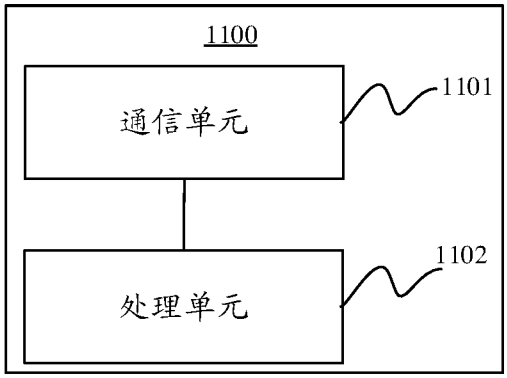
1100
通信单元
1101
处理单元
1102

图 11

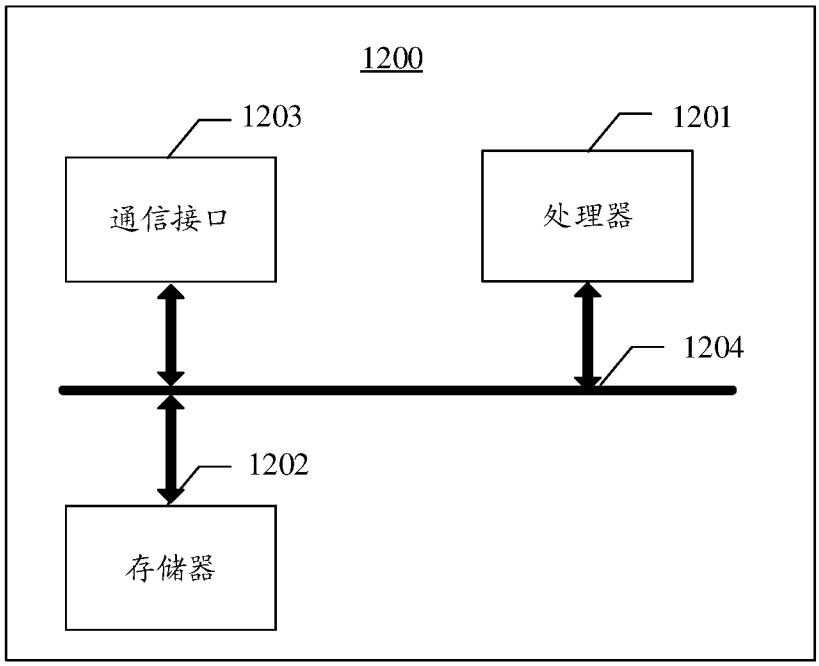
1200
1203
通信接口
1201
处理器
1204
1202
存储器

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/119764

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; H04W 12/06(2021.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, 3GPP: 认证, 鉴权, 机制, 方式, 模式, 方法, 候选, 支持, 备选, 可用, 能力, 指示, 告知, 通知, 边缘, MEC, EEC, AC, EES, EAS, ECS, AMF, SMF, AKMA, GBA, certificate, credential, capability, edge enabler, authenticat+, authoriz+, method, mechnism, mode, registration request, response, provisioning

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101753533 A (HUAWEI DEVICE CO., LTD.) 23 June 2010 (2010-06-23) description, paragraphs [0032]-[0117] and figure 2	1-35
X	CN 107820242 A (RESEARCH INSTITUTE OF CHINA MOBILE COMMUNICATIONS CORPORATION et al.) 20 March 2018 (2018-03-20) description, paragraphs [0025]-[0036]	1-35
A	CN 109964453 A (SHANGHAI NOKIA BELL CO., LTD.) 02 July 2019 (2019-07-02) entire document	1-35
A	3GPP TSG SA. "Study on Security Aspects of Enhancement of Support for Edge Computing in 5GC(Release 17)" *3GPP TR 33.839 V0.1.0,* 29 August 2020 (2020-08-29), pages 12 and 17-21	1-35
A	SAMSUNG. "EEC authentication and authorization" *S6-200731, 3GPP TSG-SA WG6 Meeting #37e,* 08 May 2020 (2020-05-08), entire document	1-35
A	WO 2019222604 A1 (CONVIDA WIRELESS, LLC.) 21 November 2019 (2019-11-21) entire document	1-35

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 June 2021	**28 June 2021**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/119764

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	101753533	A	23 June 2010	WO	2010063190	A1	10 June 2010
				US	2010146262	A1	10 June 2010
				EP	2200358	A2	23 June 2010
CN	107820242	A	20 March 2018	None			
CN	109964453	A	02 July 2019	EP	3513531	A1	24 July 2019
				WO	2018049646	A1	22 March 2018
				US	2019261179	A1	22 August 2019
WO	2019222604	A1	21 November 2019	CN	112119652	A	22 December 2020
				EP	3794857	A1	24 March 2021

国际检索报告

国际申请号
PCT/CN2020/119764

A. 主题的分类

H04L 9/32(2006.01)i; H04W 12/06(2021.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,WPI,EPODOC,CNKI,3GPP: 认证，鉴权，机制，方式，模式，方法，候选，支持，备选，可用，能力，指示，告知，通知，边缘，MEC, EEC, AC, EES, EAS, ECS, AMF, SMF, AKMA, GBA, certificate, credential, capability, edge enabler, authenticat+, authoriz+, method, mechnism, mode, registration request, response, provisioning

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 101753533 A (华为终端有限公司) 2010年 6月 23日 (2010-06-23) 说明书第[0032]-[0117]段及附图2	1-35
X	CN 107820242 A (中国移动通信有限公司研究院等) 2018年 3月 20日 (2018-03-20) 说明书第[0025]-[0036]段	1-35
A	CN 109964453 A (上海诺基亚贝尔股份有限公司) 2019年 7月 2日 (2019-07-02) 全文	1-35
A	3GPP TSG SA. "Study on Security Aspects of Enhancement of Support for Edge Computing in 5GC(Release 17)" 3GPP TR 33.839 V0.1.0, 2020年 8月 29日 (2020-08-29), 第12, 17-21页	1-35
A	SAMSUNG. "EEC authentication and authorization" S6-200731, 3GPP TSG-SA WG6 Meeting #37e, 2020年 5月 8日 (2020-05-08), 全文	1-35
A	WO 2019222604 A1 (CONVIDA WIRELESS, LLC) 2019年 11月 21日 (2019-11-21) 全文	1-35

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 6月 15日	2021年 6月 28日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 罗啸 电话号码 86-(10)-53961774

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/119764

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101753533	A	2010年 6月 23日	WO	2010063190	A1	2010年 6月 10日
				US	2010146262	A1	2010年 6月 10日
				EP	2200358	A2	2010年 6月 23日
CN	107820242	A	2018年 3月 20日		无		
CN	109964453	A	2019年 7月 2日	EP	3513531	A1	2019年 7月 24日
				WO	2018049646	A1	2018年 3月 22日
				US	2019261179	A1	2019年 8月 22日
WO	2019222604	A1	2019年 11月 21日	CN	112119652	A	2020年 12月 22日
				EP	3794857	A1	2021年 3月 24日