

AUTHENTICATION METHOD AND DEVICE, MEDIUM AND CHIP

FIELD

[0001] The present disclosure relates to the field of communication, and more particularly to an authentication method, an authentication apparatus, a medium and a chip.

BACKGROUND

[0002] In the wireless communication system, 3GPP (3rd Generation Partnership Project) defines the session security protection function between the User Equipment (UE) and the application function, and proposes an application-based key management method, i.e., authentication and key management for applications based on 3GPP credentials (AKMA).

[0003] In the related art, the user equipment can exchange messages with an application function (AF) entity based on AKMA, and determine the access authority of the user equipment to the application function AF entity, so as to establish a secure session with the application function AF entity, which will increase the load of the application function AF entity and reduce the efficiency of the AF entity.

SUMMARY

[0004] In order to overcome the above problems in the related art, the present disclosure provides an authentication method, an authentication apparatus, a medium and a chip.

[0005] According to a first aspect of embodiments of the present disclosure, an authentication method is provided, which is applied to a user equipment, and includes:

[0006] determining, from one or more first entities, a target entity with which communication is requested;

[0007] determining a first authority request parameter according to the target entity;

[0008] sending an application session establishment request message to a first proxy entity according to the first authority request parameter; where the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with the target entity according to the first authority request parameter; the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;

[0009] determining whether the user equipment has the first communication authority with the target entity in response to receiving an application session establishment response message sent by the first proxy entity; and

[0010] in case that the user equipment has the first communication authority with the target entity, performing authentication through the first proxy entity.

[0011] According to a second aspect of embodiments of the present disclosure, an authentication method is provided, which is applied to a first proxy entity, and includes:

[0012] receiving an application session establishment request message sent by a user equipment; where the application session establishment request message includes a first authority request parameter, the

application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with a target entity according to the first authority request parameter, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;

[0013] determining whether the user equipment has the first communication authority with the target entity according to the first authority request parameter; and

[0014] in case that the user equipment has the first communication authority with the target entity, sending an application session establishment response message to the user equipment, and performing authentication of the user equipment.

[0015] According to a third aspect of embodiments of the present disclosure, an authentication method is provided, which is applied to a third entity, and includes:

[0016] receiving a second authority request parameter sent by a first proxy entity; where the second authority request parameter is configured to instruct the third entity to determine whether a user equipment has a first communication authority with a target entity, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, the first proxy entity provides an authentication proxy function for the first entity, and the third entity includes an entity that provides AKMA authorization and application key derivation functions;

[0017] determining whether the user equipment has the first communication authority with the target entity according to the second authority request parameter;

[0018] acquiring first pending key information in case that the user equipment has the first communication authority with the target entity; and

[0019] sending the first pending key information to the first proxy entity.

[0020] According to a fourth aspect of embodiments of the present disclosure, an authentication method is provided, which is applied to a target entity in one or more first entities, and includes:

[0021] acquiring an authentication result of a first proxy entity to a user equipment, where the authentication result includes a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with the target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the first entity includes an entity providing an application function, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

[0022] communicating with the user equipment according to the authentication result.

[0023] According to a fifth aspect of embodiments of the present disclosure, an authentication method is provided, which is applied to a second entity, and includes:

[0024] acquiring an authentication result of a first proxy entity to a user equipment; where the authentication result includes a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with a target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an untrusted entity providing an application function outside a 3GPP operator domain, the first proxy entity includes a trusted entity providing an authentication function inside the 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

[0025] sending the authentication result to the target entity to make the target entity communicate with the user equipment according to the authentication result.

[0026] According to a sixth aspect of embodiments of the present disclosure, an authentication apparatus is provided, which is applied to a user equipment, and includes:

[0027] a target entity determining module configured to determine, from one or more first entities, a target entity with which communication is requested;

[0028] a parameter determining module configured to determine a first authority request parameter according to the target entity;

[0029] a first message sending module configured to send an application session establishment request message to a first proxy entity according to the first authority request parameter; where the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with the target entity according to the first authority request parameter; the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;

[0030] a first message receiving module configured to determine whether the user equipment has the first communication authority with the target entity in response to receiving an application session establishment response message sent by the first proxy entity; and

[0031] an authentication module configured to perform authentication through the first proxy entity in case that the user equipment has the first communication authority with the target entity.

[0032] According to a seventh aspect of embodiments of the present disclosure, an authentication apparatus is provided, which is applied to a first proxy entity, includes:

[0033] a first proxy receiving module configured to receive an application session establishment request message sent by a user equipment; where the application session establishment request message includes a first authority request parameter, the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with a target entity according to the first authority request parameter, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;

[0034] a first proxy determining module configured to determine whether the user equipment has the first communication authority with the target entity according to the first authority request parameter; and

[0035] a first proxy sending module configured to send an application session establishment response message to the user equipment, and perform authentication of the user equipment in case that the user equipment has the first communication authority with the target entity.

[0036] According to an eighth aspect of embodiments of the present disclosure, an authentication apparatus is provided, which is applied to a third entity, and includes:

[0037] a third receiving module configured to receive a second authority request parameter sent by a first proxy entity; where the second authority request parameter is configured to instruct the third entity to determine whether a user equipment has a first communication authority with a target entity, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, the first proxy entity provides an authentication proxy function for the first entity, and the third entity includes an entity that provides AKMA authorization and application key derivation functions;

[0038] a third determining module configured to determine whether the user equipment has the first communication authority with the target entity according to the second authority request parameter;

[0039] a third key module configured to acquire first pending key information in case that the user equipment has the first communication authority with the target entity; and

[0040] a third sending module configured to send the first pending key information to the first proxy entity.

[0041] According to a ninth aspect of embodiments of the present disclosure, an authentication apparatus is provided, which is applied to a target entity in one or more first entities, and includes: a first communication module configured to:

[0042] acquire an authentication result of a first proxy entity to a user equipment, where the authentication result includes a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with the target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the first entity includes an entity providing an application function, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

[0043] communicate with the user equipment according to the authentication result.

[0044] According to a tenth aspect of embodiments of the present disclosure, an authentication apparatus is provided, which is applied to a second entity, and includes:

[0045] a second receiving module configured to acquire an authentication result of a first proxy entity to a user equipment; where the authentication result includes a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with a target entity; the second authentication result is configured to indicate that the

user equipment has a second communication authority with the target entity; the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an untrusted entity providing an application function outside a 3GPP operator domain, the first proxy entity includes a trusted entity providing an authentication function inside the 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

[0046] a second sending module configured to send the authentication result to the target entity to make the target entity communicate with the user equipment according to the authentication result.

[0047] According to an eleventh aspect of embodiments of the present disclosure, an authentication apparatus is provided, which includes: a processor; and a memory for storing instructions executable by the processor. The processor is configured to perform the steps of the authentication method according to the first aspect of the present disclosure.

[0048] According to a twelfth aspect of embodiments of the present disclosure, an authentication apparatus is provided, which includes: a processor; and a memory for storing instructions executable by the processor. The processor is configured to perform the steps of the authentication method according to the second aspect of the present disclosure.

[0049] According to a thirteenth aspect of embodiments of the present disclosure, an authentication apparatus is provided, which includes: a processor; and a memory for storing instructions executable by the processor. The processor is configured to perform the steps of the authentication method according to the third aspect of the present disclosure.

[0050] According to a fourteenth aspect of embodiments of the present disclosure, an authentication apparatus is provided, which includes: a processor; and a memory for storing instructions executable by the processor. The processor is configured to perform the steps of the authentication method according to the fourth aspect of the present disclosure.

[0051] According to a fifteenth aspect of embodiments of the present disclosure, an authentication apparatus is provided, which includes: a processor; and a memory for storing instructions executable by the processor. The processor is configured to perform the steps of the authentication method according to the fifth aspect of the present disclosure.

[0052] According to a sixteenth aspect of embodiments of the present disclosure, a computer-readable storage medium is provided, which has stored therein computer program instructions that, when executed by a processor, cause the steps of the authentication method according to the first aspect of the present disclosure to be implemented.

[0053] According to a seventeenth aspect of embodiments of the present disclosure, a computer-readable storage medium is provided, which has stored therein computer program instructions that, when executed by a processor, cause the steps of the authentication method according to the second aspect of the present disclosure to be implemented.

[0054] According to an eighteenth aspect of embodiments of the present disclosure, a computer-readable storage medium is provided, which has stored therein computer program instructions that, when executed by a processor, cause the steps of the authentication method according to the third aspect of the present disclosure to be implemented.

[0055] According to a nineteenth aspect of embodiments of the present disclosure, a computer-readable

storage medium is provided, which has stored therein computer program instructions that, when executed by a processor, cause the steps of the authentication method according to the fourth aspect of the present disclosure to be implemented.

[0056] According to a twentieth aspect of embodiments of the present disclosure, a computer-readable storage medium is provided, which has stored therein computer program instructions that, when executed by a processor, cause the steps of the authentication method according to the fifth aspect of the present disclosure to be implemented.

[0057] According to a twenty-first aspect of embodiments of the present disclosure, a chip is provided, which includes a processor and an interface. The processor is configured to read instructions to perform the steps of the authentication method according to the first aspect of the present disclosure.

[0058] According to a twenty-second aspect of embodiments of the present disclosure, a chip is provided, which includes a processor and an interface. The processor is configured to read instructions to perform the steps of the authentication method according to the second aspect of the present disclosure.

[0059] According to a twenty-third aspect of embodiments of the present disclosure, a chip is provided, which includes a processor and an interface. The processor is configured to read instructions to perform the steps of the authentication method according to the third aspect of the present disclosure.

[0060] According to a twenty-fourth aspect of embodiments of the present disclosure, a chip is provided, which includes a processor and an interface. The processor is configured to read instructions to perform the steps of the authentication method according to the fourth aspect of the present disclosure.

[0061] According to a twenty-fifth aspect of embodiments of the present disclosure, a chip is provided, which includes a processor and an interface. The processor is configured to read instructions to perform the steps of the authentication method according to the fifth aspect of the present disclosure.

[0062] The technical solutions provided by embodiments of the present disclosure may include the following beneficial effects. the target entity with which communication is requested is determined from one or more first entities; the first authority request parameter is determined according to the target entity; the application session establishment request message is sent to the first proxy entity according to the first authority request parameter; it is determined whether the user equipment has the first communication authority with the target entity in response to receiving the application session establishment response message sent by the first proxy entity; and in case that the user equipment has the first communication authority with the target entity, the authentication is performed through the first proxy entity. The application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has the first communication authority with the target entity according to the first authority request parameter; the first entity may include the entity providing the application function, the first proxy entity may include the trusted entity providing the authentication function inside the 3GPP operator domain, and the first proxy entity provides the authentication proxy function for the first entity. In this way, the trusted first proxy entity inside the 3GPP operator domain may determine whether the user equipment has the first communication authority with the first entity, and perform the authentication of the user equipment in case that the user equipment has the first communication authority, so that part of functions of the first entity can be realized through the first proxy entity, thereby reducing the load of the first entity and improving the efficiency of the first entity. Moreover, the user equipment realizes the authorization and authentication with one or more first entities through the unified first

proxy entity, which also reduces the complexity of authentication of the user equipment and improves the efficiency of the user equipment.

[0063] It is to be understood that both the foregoing general description and the following detailed description are illustrative and explanatory only, and are not restrictive of the present disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0064] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate embodiments consistent with the present disclosure and together with the description, serve to explain the principles of the present disclosure.

[0065] Fig. 1 is a schematic diagram of a communication system to which embodiments of the present disclosure are applicable according to an illustrative embodiment.

[0066] Fig. 2 is a schematic diagram of another communication system to which embodiments of the present disclosure are applicable according to an illustrative embodiment.

[0067] Fig. 3 is a flowchart of an authentication method according to an illustrative embodiment.

[0068] Fig. 4 is a flowchart of an authentication method according to an illustrative embodiment.

[0069] Fig. 5 is a flowchart of an authentication method according to an illustrative embodiment.

[0070] Fig. 6 is a flowchart of an authentication method according to an illustrative embodiment.

[0071] Fig. 7 is a flowchart of an authentication method according to an illustrative embodiment.

[0072] Fig. 8 is a flowchart of an authentication method according to an illustrative embodiment.

[0073] Fig. 9 is a flowchart of an authentication method according to an illustrative embodiment.

[0074] Fig. 10 is a flowchart of an authentication method according to an illustrative embodiment.

[0075] Fig. 11 is a flowchart of an authentication method according to an illustrative embodiment.

[0076] Fig. 12 is a flowchart of an authentication method according to an illustrative embodiment.

[0077] Fig. 13 is a block diagram of an authentication apparatus according to an illustrative embodiment.

[0078] Fig. 14 is a block diagram of an authentication apparatus according to an illustrative embodiment.

[0079] Fig. 15 is a block diagram of an authentication apparatus according to an illustrative embodiment.

[0080] Fig. 16 is a block diagram of an authentication apparatus according to an illustrative embodiment.

[0081] Fig. 17 is a block diagram of an authentication apparatus according to an illustrative embodiment.

[0082] Fig. 18 is a block diagram of an authentication apparatus according to an illustrative embodiment.

[0083] Fig. 19 is a block diagram of an authentication apparatus according to an illustrative embodiment.

[0084] Fig. 20 is a block diagram of an authentication apparatus according to an illustrative embodiment.

DETAILED DESCRIPTION

[0085] Reference will now be made in detail to illustrative embodiments, examples of which are illustrated in the accompanying drawings. When the following description refers to the drawings, unless otherwise indicated, the same numbers in different drawings indicate the same or similar elements. The implementations described in the following illustrative embodiments do not represent all implementations consistent with the present disclosure. Rather, they are merely examples of devices and methods consistent with some aspects of the present disclosure as detailed in the appended claims.

[0086] It should be noted that all the actions of acquiring signals, information or data in the present disclosure are carried out under the premise of complying with the corresponding data protection laws and policies of the country where the present disclosure is and obtaining authorization from the owner of the corresponding device.

[0087] In the present disclosure, terms such as “first” and “second” are used to distinguish similar objects without necessarily being understood as a specific order or precedence. In addition, in the description with reference to the drawings, the same reference numerals in different drawings indicate the same elements unless otherwise specified.

[0088] In the description of the present disclosure, unless otherwise specified, “a plurality of” means two or more, and other quantifiers are similar to this. The expression “at least one of the following items” or other similar expressions refer to any combination of these items, including any combination of singular items or plural items. For example, at least one of a, b, or c can mean: a, b, c, a-b, a-c, b-c, or a-b-c, where a, b, and c can be singular or plural; “and/or” is an association relationship that describes the associated objects, which means that there can be three kinds of relationships, for example, A and/or B can mean that A exists alone, A and B exist at the same time, and B exists alone, where A and B can be singular or plural.

[0089] Although the operations are described in a specific order in the drawings in the embodiments of the present disclosure, it should not be construed as requiring that these operations be performed in the specific order or serial order shown, or that all the operations shown be performed, to acquire the desired results. In certain circumstances, multitasking and parallel processing may be beneficial.

[0090] In the related art, the user equipment can exchange messages with an application function (AF) entity based on AKMA, and determine the access authority of the user equipment to the application function AF entity, so as to establish a secure session with the application function AF entity. However, the message interaction caused by a plurality of user equipment will increase the load of the application function AF entity and reduce the efficiency of the application function AF entity. Moreover, when there exist a plurality of application function AF entities in the network, direct message interaction of the UE with the AF to determine the access authority will also reduce the efficiency for the UE.

[0091] In order to solve the above problems, the present disclosure provides an authentication method, an authentication apparatus, a medium and a chip.

[0092] First, the implementation environment of embodiments of the present disclosure will be introduced.

[0093] Embodiments of the present disclosure may be applied to a 4G (the 4th Generation) network system, such as a Long Term Evolution (LTE) system, or it may also be applied to a 5G (the 5th Generation) network system, such as an access network adopting a New Radio Access Technology (New RAT); a Cloud

Radio Access Network (CRAN) or other communication systems.

[0094] Fig. 1 is a schematic diagram of a communication system to which embodiments of the present disclosure are applicable according to an illustrative embodiment. It should be noted that embodiments of the present disclosure are not limited by the system shown in Fig. 1, and in addition, the entities in Fig. 1 may be hardware, software divided in terms of functions or a combination thereof. The entities shown in Fig. 1 may be entities in any communication network architecture, and the communication network may be a 4G network, a 5G network or a 6G network, etc.

[0095] As shown in Fig. 1, the communication system may include: a first entity 101, a third entity 103, a first proxy entity 110 and a user equipment 160, and the first entity 101 may include one or more entities, for example, the first entity 101 may include: a first entity 1011, a first entity 1012, ..., a first entity 101n, and the like. The first proxy entity 110 may be connected with the one or more first entities 101 (for example, through a wired network, a wireless network or a combination of both), and the first proxy entity may be connected with the third entity, and the user equipment may be connected with the first proxy entity and the third entity.

[0096] In some embodiments, the first entity 101 may include a trusted entity providing an application function inside a 3GPP operator domain, the first proxy entity 110 may include a trusted entity providing an authentication proxy function inside the 3GPP operator domain, and the third entity 103 may include an entity providing AKMA authorization and application key derivation functions, for example, the third entity 103 may be a functional entity that provides an AKMA anchor function and authenticates a communication authority between the user equipment and the first entity.

[0097] For example, the first entity may include: an application function (AF) entity or a service capability server SCS/application server AS; the first proxy entity may include an authentication proxy AP (AKMA authentication proxy) entity; and the third entity may include: an AKMA anchor function AAnF entity.

[0098] In some embodiments, the first entity may include a trusted entity providing an application function inside the 3GPP operator domain, the first proxy entity may include a trusted entity providing an authentication function inside the 3GPP operator domain, and the first proxy entity provide an authentication proxy function for the first entity, and the first entity may include one or more entities.

[0099] Fig. 2 is a schematic diagram of another communication system to which embodiments of the present disclosure are applicable according to an illustrative embodiment. As shown in Fig. 2, the communication system may include: a first entity 101, a second entity 122, a third entity 103, a first proxy entity 110 and a user equipment 160, and the first entity 101 may include one or more entities. The second entity 102 may be connected with the one or more first entities 101 (for example, through a wired network, a wireless network, or a combination of both), the first proxy entity may be connected with the second entity and the third entity, and the user equipment may be connected with the first proxy entity and the third entity.

[0100] In Fig. 2, the first entity 101 may include an untrusted entity providing an application function outside the 3GPP operator domain, for example, an application function (AF) entity or a service capability server SCS/application server AS; the first proxy entity 110 may include a trusted entity providing an authentication proxy function inside the 3GPP operator domain, for example, an authentication proxy AP (AKMA authentication proxy) entity; and the third entity 103 may include an entity that provides AKMA authorization and application key derivation functions, for example, an AKMA anchor function AAnF entity. The second

entity may include an entity providing a network exposure function, for example, a network exposure function (NEF) entity or a service capability exposure function (SCEF) entity.

[0101] Fig. 3 shows an authentication method according to an illustrative embodiment, which may be applied to the user equipment in the above communication system. As shown in Fig. 3, the method may include the following operations.

[0102] In S301, the user equipment determines, from one or more first entities, a target entity with which communication is requested.

[0103] For example, the first entity may include an entity providing an application function, such as an application function AF entity. The user equipment can determine, according to the user's functional requirements, an AF entity with which communication is requested.

[0104] In S302, the user equipment determines a first authority request parameter according to the target entity.

[0105] In some embodiments, a first target entity identifier of the target entity may be acquired first, and the first authority parameter may be determined according to the first target entity identifier.

[0106] For example, the first target entity identifier may include one or more of: a Fully Qualified Domain Name (FQDN), an Internet Protocol (IP) address and a Port Number of the target entity.

[0107] In some embodiments, the first authority request parameter may be acquired according to the first target entity identifier and a user equipment identifier representing the identity of the user equipment.

[0108] The user equipment identifier may include a key identifier A-KID corresponding to the user equipment, the key identifier A-KID may be derived according to hardware information of the user equipment and registration information sent by the communication system when the user equipment registers to access the communication system, and the key identifier A-KID may uniquely identify one user equipment in the communication system.

[0109] For example, the first target entity identifier and the key identifier A-KID corresponding to the user equipment may be used as the first authority request parameter.

[0110] In S303, the user equipment sends an application session establishment request message to a first proxy entity according to the first authority request parameter.

[0111] The application session establishment request message may be configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with the target entity according to the first authority request parameter.

[0112] In some embodiments, the first proxy entity is connected with one or more first entities. For example, a unified first proxy entity may be set in a trust domain or an edge node, and the first proxy entity can be connected with each first entity in the trust domain or the edge node. In case that the user equipment requests to communicate with the target entity in the trust domain or the edge node, an application session establishment request message may be sent to the first proxy entity.

[0113] In some embodiments, the first entity may include an entity providing an application function (such as a trusted entity providing an application function inside a 3GPP operator domain, or an untrusted entity providing an application function outside the 3GPP operator domain), the first proxy entity may include a trusted entity providing an authentication function inside the 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity, and one or more first entities may be provided.

[0114] In some embodiments, the user equipment may be pre-configured with a proxy domain name (e.g., FQDN) of the first proxy entity, and the user equipment is able to perform message interaction or data transmission with the first proxy entity through the FQDN.

[0115] In S304, the user equipment determines whether the user equipment has the first communication authority with the target entity in response to receiving an application session establishment response message sent by the first proxy entity.

[0116] In some embodiments, the user equipment may determine that the user equipment has the first communication authority with the target entity in case that the application session establishment response message is received.

[0117] On the contrary, if the user equipment does not receive the application session establishment response message within a preset time, it can be determined that the user equipment does not have the first communication authority with the target entity.

[0118] In some other embodiments, the user equipment may determine that the user equipment has the first communication authority with the target entity in case that the user equipment receives the application session establishment response message, and the application session establishment response message includes success indication information.

[0119] On the contrary, if the application session establishment response message received by the user equipment does not include the success indication information or includes failure indication information, it can be determined that the user equipment does not have the first communication authority with the target entity. The success indication information may be any indication information set in advance.

[0120] In some other embodiments, the user equipment may determine that the user equipment has the first communication authority with the target entity in case that the user equipment receives the application session establishment response message, and the application session establishment response message does not include the failure indication information.

[0121] On the contrary, if the application session establishment response message received by the user equipment includes the failure indication information, it can be determined that the user equipment does not have the first communication authority with the target entity. The failure indication information may be any error code set in advance.

[0122] In S305, in case that the user equipment has the first communication authority with the target entity, the user equipment performs authentication through the first proxy entity.

[0123] For example, the user equipment is able to derive an entity key K_{AF} corresponding to the target entity based on the FQDN of the target entity, and perform the authentication with the first proxy entity based on the entity key K_{AF} .

[0124] It should be noted that the way for the user equipment to perform the authentication can refer to the implementation in the related art, for example, the authentication may be performed based on the entity key information corresponding to the target entity, or the authentication may be performed based on user key information corresponding to the user equipment and the entity key information corresponding to the target entity, which is not limited in the present disclosure.

[0125] By adopting the above method, the target entity with which communication is requested is determined from one or more first entities; the first authority request parameter is determined according to the

target entity; the application session establishment request message is sent to the first proxy entity according to the first authority request parameter; it is determined whether the user equipment has the first communication authority with the target entity in response to receiving the application session establishment response message sent by the first proxy entity; and in case that the user equipment has the first communication authority with the target entity, the authentication is performed through the first proxy entity. The application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has the first communication authority with the target entity according to the first authority request parameter; the first entity may include the entity providing the application function, the first proxy entity may include the trusted entity providing the authentication function inside the 3GPP operator domain, and the first proxy entity provides the authentication proxy function for the first entity. In this way, the trusted first proxy entity inside the 3GPP operator domain may determine whether the user equipment has the first communication authority with the first entity, and perform the authentication of the user equipment in case that the user equipment has the first communication authority, so that part of functions of the first entity can be realized through the first proxy entity, thereby reducing the load of the first entity and improving the efficiency of the first entity. Moreover, the user equipment realizes the authorization and authentication with one or more first entities through the unified first proxy entity, which also reduces the complexity of authentication of the user equipment and improves the efficiency of the user equipment.

[0126] In some embodiments, the first communication authority may include one or more of the following authorities.

[0127] Authority 1: the user equipment has an access authority to the target entity.

[0128] Authority 2: the user equipment has an access authority to the first proxy entity.

[0129] Authority 3: the first proxy entity has a proxy authority to the target entity.

[0130] Authority 4: the target entity has an acquisition authority to an identity of the subscriber of the user equipment.

[0131] For example, it may be determined that the user equipment has the first communication authority with the target entity in case that it is determined that the user equipment has the access authority to the target entity; it may also be determined that the user equipment has the first communication authority with the target entity in case that it is determined that the user equipment has the access authority to the first proxy entity and the first proxy entity has the proxy authority to the target entity; or it may also be determined that the user equipment has the first communication authority with the target entity in case that it is determined that the user equipment has the access authority to the target entity, the user equipment has the access authority to the first proxy entity, and the first proxy entity has the proxy authority to the target entity.

[0132] In some embodiments, the user equipment having the first communication authority with the target entity may include that the user equipment has the access authority to the first proxy entity, and the first proxy entity has the proxy authority to the target entity. For example, in case that the FQDN of the first proxy entity is the same as that of the target entity, the first communication authority can be used.

[0133] In some other embodiments, the user equipment having the first communication authority with the target entity may include that the user equipment has the access authority to the target entity, the user equipment has the access authority to the first proxy entity, and the first proxy entity has the proxy authority to the target entity. For example, in case that the FQDN of the first proxy entity is different from that of the target

entity, the first communication authority can be used.

[0134] In some embodiments, the first proxy entity may include a trusted authentication proxy AP entity inside the 3GPP operator domain.

[0135] In some embodiments, the first entity may include a trusted entity providing an application function inside the 3GPP operator domain. For example, the first entity may include: a trusted application function AF entity inside the 3GPP operator domain or a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain.

[0136] In some other embodiments, the above first entity may include an untrusted entity providing an application function outside the 3GPP operator domain, the first proxy entity may communicate with the first entity through a second entity; the second entity may include an entity providing a network exposure function. For example, the first entity may include: an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain; and the second entity may include: a network exposure function NEF entity or a service capability exposure function SCEF entity.

[0137] In this way, the user equipment can communicate with the AF entity outside the operator domain through the AP.

[0138] In some embodiments, after the authentication through the first proxy entity is successful, the user equipment can communicate with the target entity.

[0139] For example, the user equipment can communicate with the target entity directly or through the first proxy entity, for example, a communication message between the user equipment and the target entity is forwarded through the first proxy entity.

[0140] In some other embodiments, after the authentication through the first proxy entity is successful, the user equipment can also determine whether a proxy domain name of the first proxy entity is the same as a first domain name of the target entity, and can communicate with the target entity in case that the proxy domain name is different from the first domain name.

[0141] On the contrary, in case that the proxy domain name is the same as the first domain name, whether the user equipment has a second communication authority with the target entity may be further determined through a secure session between the user equipment and the proxy entity; and in case that the user equipment has the second communication authority, the user equipment can communicate with the target entity.

[0142] It should be noted that the proxy domain name may be a fully qualified domain name FQDN corresponding to the first proxy entity, and the first domain name may be a fully qualified domain name FQDN corresponding to the target entity. In some scenarios, the first proxy entity and the target entity can use the same FQDN, but different IP addresses or port numbers. In this scenario, the first communication authority can indicate that the user equipment has the access authority to the FQDN, but not necessarily indicate that the user equipment has the access authority to the target entity corresponding to the IP address or port number. At this time, it may be further determined whether the user equipment has the second communication authority with the target entity through the secure session between the user equipment and the proxy entity.

[0143] Fig. 4 shows an authentication method according to an illustrative embodiment, which may be applied to the user equipment. As shown in Fig. 4, the method may include the following operations.

[0144] In S401, in case that the user equipment has the first communication authority with the target

entity, the user equipment performs authentication through the first proxy entity.

[0145] In S402, after the authentication through the first proxy entity is successful, the user equipment establishes a secure session with the first proxy entity.

[0146] For example, the secure session may be a transport layer security (TLS) session, through which confidentiality and data integrity can be achieved for the communication between the user equipment and the first proxy entity.

[0147] In S403, the user equipment acquires a proxy domain name of the first proxy entity and a first domain name of the target entity.

[0148] In some embodiments, the proxy domain name may be the fully qualified domain name FQDN corresponding to the first proxy entity, and the first domain name may be the fully qualified domain name FQDN corresponding to the target entity.

[0149] In S404, in case that the proxy domain name is the same as the first domain name, the user equipment determines whether the user equipment has the second communication authority with the target entity through the secure session.

[0150] In S405, in case that it is determined that the user equipment has the second communication authority with the target entity, the user equipment communicates with the target entity.

[0151] Similarly, the user equipment can communicate with the target entity directly or through the first proxy entity, for example, the communication message between the user equipment and the target entity is forwarded through the first proxy entity.

[0152] In this way, by authenticating the first communication authority and the second communication authority, it can also be determined that the user equipment has the access authority to the target entity in case that the FQDN of the first proxy entity is the same as that of the target entity, thereby further enhancing security.

[0153] In some embodiments, determining whether the user equipment has the second communication authority with the target entity through the secure session in step S404 may include the following operations.

[0154] Firstly, the user equipment sends a target entity service request message to the first proxy entity through the secure session.

[0155] For example, the target entity service request message may include a second target entity identifier, which is a protected entity identifier acquired by the user equipment according to the first target entity identifier. The target entity service request message is used to instruct the first proxy entity to determine whether the user equipment has the second communication authority with the target entity according to the second target entity identifier.

[0156] In some embodiments, the second target entity identifier is an identifier determined after protecting the first target entity identifier corresponding to the target entity according to the requirements of the secure session (such as the TLS session).

[0157] In some other embodiments, the first target entity identifier can also be directly used as the second target entity identifier, and the second target entity identifier can be transmitted through the secure session, so as to protect the first target entity identifier and prevent the entity identifier from being tampered with during transmission.

[0158] Then, in response to receiving a target entity service response message sent by the first proxy entity, the user equipment determines whether the user equipment has the second communication authority with

the target entity.

[0159] In some embodiments, the user equipment may determine that the user equipment has the second communication authority with the target entity in case that the user equipment receives the target entity service response message.

[0160] On the contrary, in case that the user equipment does not receive the target entity service response message within a preset time, it can be determined that the user equipment does not have the second communication authority with the target entity.

[0161] In some other embodiments, the user equipment may determine that the user equipment has the second communication authority with the target entity in case that the user equipment receives the target entity service response message, and the target entity service response message contains success indication information.

[0162] On the contrary, in case that the target entity service response message received by the user equipment does not contain the success indication information or contains failure indication information, it can be determined that the user equipment does not have the second communication authority with the target entity. The success indication information can be any indication information set in advance.

[0163] In some other embodiments, the user equipment may determine that the user equipment has the second communication authority with the target entity in case that the user equipment receives the target entity service response message, and the target entity service response message does not contain the failure indication information.

[0164] On the contrary, in case that the target entity service response message received by the user equipment contains the failure indication information, it can be determined that the user equipment does not have the second communication authority with the target entity. The failure indication information can be any error code set in advance.

[0165] In this way, the user equipment can determine whether the user equipment has the second communication authority with the target entity through the secure session.

[0166] In some embodiments, the second communication authority may include one or more of the following authorities.

[0167] Authority 6: the user equipment has an access authority to the target entity.

[0168] Authority 7: the first proxy entity has a proxy authority to the target entity.

[0169] Authority 8: the target entity has an acquisition authority to the identity of the subscriber of the user equipment.

[0170] In this way, it can be determined whether the user equipment has the second communication authority with the target entity through the secure session between the user equipment and the first proxy entity, thus further improving the reliability of authentication.

[0171] Fig. 5 shows an authentication method according to an illustrative embodiment, which may be applied to the first proxy entity in the communication system. As shown in Fig. 5, the method may include the following operations.

[0172] In S501, the first proxy entity receives an application session establishment request message sent by the user equipment.

[0173] The application session establishment request message includes a first authority request

parameter, and the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with a target entity according to the first authority request parameter, the target entity is an entity which is determined from one or more first entities by the user equipment and with which communication is requested, and the first entity may include an entity providing an application function, the first proxy entity may include a trusted entity providing an authentication function inside the 3GPP operator domain, the first proxy entity provides an authentication proxy function for the first entity, and one or more first entities may be provided.

[0174] In S502, the first proxy entity determines whether the user equipment has the first communication authority with the target entity according to the first authority request parameter.

[0175] In this way, the trusted first proxy entity inside the 3GPP operator domain may determine whether the user equipment has the first communication authority with the first entity, and perform the authentication of the user equipment in case that the user equipment has the first communication authority, so that part of functions of the first entity can be realized through the first proxy entity, thereby reducing the load of the first entity and improving the efficiency of the first entity. Moreover, the user equipment realizes the authorization and authentication with one or more first entities through the unified first proxy entity, which also reduces the complexity of authentication of the user equipment and improves the efficiency of the user equipment.

[0176] In some embodiments, the first proxy entity can determine whether the user equipment has the first communication authority with the target entity through message interaction with a third entity, which for example may include the following operations.

[0177] First, the first proxy entity determines a second authority request parameter according to the first authority request parameter.

[0178] In some embodiments, the first authority request parameter and a proxy entity identifier corresponding to the first proxy entity may be used as the second authority request parameter. For example, if the first authority request parameter includes a first target entity identifier of the target entity and a key identifier A-KID corresponding to the user equipment, the second authority request parameter may include the first target entity identifier, the key identifier A-KID, and the proxy entity identifier corresponding to the first proxy entity.

[0179] In some other embodiments, the first authority request parameter may be used as the second authority request parameter.

[0180] Secondly, the first proxy entity sends the second authority request parameter to the third entity.

[0181] For example, the third entity may include an entity providing AKMA authorization and application key derivation functions. The second authority request parameter may be configured to instruct the third entity to determine whether the user equipment has the first communication authority with the target entity.

[0182] Thirdly, the first proxy entity acquires first pending key information sent by the third entity.

[0183] The first pending key information is key information acquired by the third entity according to the second authority request parameter

[0184] In some embodiments, the first pending key information may include an application key K_{AF} corresponding to the target entity.

[0185] In some other embodiments, the first pending key information may include the application key K_{AF} and a key expiration time (K_{AF} expiration time) corresponding to the target entity.

[0186] In some embodiments, the first proxy entity may send the second authority request parameter to the third entity via a first key request message; the first key request message is configured to instruct the third entity to acquire the first pending key information and an identity of the subscriber of the user equipment; the first proxy entity may also receive a first key response message sent by the third entity; and acquire the first pending key information included in the first key response message.

[0187] Further, the first key response message may also include a second identity of the subscriber corresponding to the user equipment, and the first proxy entity may acquire the second identity of the subscriber according to the first key response message received. The second identity of the subscriber may include a subscription permanent identifier SUPI corresponding to the user equipment.

[0188] In some embodiments, the first proxy entity may send the second authority request parameter to the third entity via a second key request message; the second key request message is configured to indicate that the first proxy entity requests to acquire the first pending key information; the first proxy entity may also receive a second key response message sent by the third entity; and acquire the first pending key information included in the second key response message. Finally, the first proxy entity determines whether the user equipment has the first communication authority with the target entity according to the first pending key information.

[0189] For example, in case that the first pending key information includes the application key K_{AF} corresponding to the target entity, it can be determined that the user equipment has the first communication authority with the target entity. On the contrary, in case that the first pending key information does not include the application key K_{AF} corresponding to the target entity, or in case that the first pending key information does not include the valid application key K_{AF} , or in case that the first pending key information is not received within a preset time, it can be determined that the user equipment does not have the first communication authority with the target entity.

[0190] In this way, the first proxy entity can determine whether the user equipment has the first communication authority with the target entity through interaction with the third entity.

[0191] In some other embodiments, in case that the first proxy entity stores a communication authority policy of the user equipment, it can be directly determined whether the user equipment has the first communication authority with the target entity according to the first authority request parameter.

[0192] In S503, in case that the user equipment has the first communication authority with the target entity, the first proxy entity sends an application session establishment response message to the user equipment, and performs authentication of the user equipment.

[0193] In some embodiments, the first proxy entity may indicate that the user equipment has the first communication authority with the target entity by sending the application session establishment response message. On the contrary, by not sending the application session establishment response message, the first proxy entity may indicate that the user equipment does not have the first communication authority with the target entity.

[0194] In some other embodiments, the first proxy entity may include success indication information in the application session establishment response message, and it is indicated through the success indication information that the user equipment has the first communication authority with the target entity. On the contrary, by not including the success indication information in the application session establishment response message,

it is indicated that the user equipment does not have the first communication authority with the target entity. The success indication information may be any indication information set in advance.

[0195] In some other embodiments, in case that the user equipment does not have the first communication authority with the target entity, the first proxy entity may include failure indication information in the application session establishment response message to indicate that the user equipment does not have the first communication authority with the target entity. On the contrary, in case that the user equipment has the first communication authority with the target entity, the first proxy entity may indicate that the user equipment has the first communication authority with the target entity by not including the failure indication information in the application session establishment response message.

[0196] By adopting the above method, the authentication between the user equipment and the first entity can be realized through the first proxy entity, so that the problem of excessive load of the first entity caused by the authentication can be overcome.

[0197] In some embodiments, the first communication authority may include one or more of the following authorities.

[0198] Authority 1: the user equipment has an access authority to the target entity.

[0199] Authority 2: the user equipment has an access authority to the first proxy entity.

[0200] Authority 3: the first proxy entity has a proxy authority to the target entity.

[0201] Authority 4: the target entity has an acquisition authority to an identity of the subscriber of the user equipment.

[0202] In some embodiments, the above first proxy entity may include a trusted authentication proxy AP entity inside the 3GPP operator domain.

[0203] In some embodiments, the above first entity may include: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

[0204] In some embodiments, the above second entity may include: a network exposure function NEF entity or a service capability exposure function SCEF entity.

[0205] In some embodiments, the above third entity may include: an AKMA anchor function AAnF entity.

[0206] In some embodiments, in case that the authentication of the user equipment through the first proxy entity is successful, the first proxy entity may notify the target entity of a first authentication result of the authentication. The first authentication result is configured to indicate that the user equipment has a communication authority with the target entity.

[0207] For example, in case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain, the first proxy entity may send a first notification message to the target entity, and the first notification message may include the first authentication result. Further, in case that the first proxy entity acquires a second identity of the subscriber of the user equipment (for example, the second identity of the subscriber is acquired through the first key response message), the first notification message may also include the second identity of the subscriber.

[0208] For another example, in case that the target entity is an untrusted entity providing an application

function outside the 3GPP operator domain, the first proxy entity may send a second notification message to the second entity according to the first authentication result to instruct the second entity to send the first authentication result to the target entity. Similarly, in case that the first proxy entity acquires the second identity of the subscriber of the user equipment (for example, the second identity of the subscriber is acquired through the first key response message), the second notification message may also include the second identity of the subscriber.

[0209] Further, the authentication result notification message may also include the first identity of the subscriber corresponding to the user equipment. For example, in case that the first key response message includes the first identity of the subscriber corresponding to the user equipment, the first proxy entity may send the first identity of the subscriber to the target entity via the authentication result notification message.

[0210] It should be noted that the first identity of the subscriber may be any identifier for representing the user equipment, for example, it may be a generic public subscription identifier GPSI corresponding to the user equipment.

[0211] In this way, the first proxy entity can verify the communication authority between the user equipment and the first entity, and instruct the user equipment to communicate with the first entity in case that the user equipment has the communication authority with the first entity.

[0212] In some other embodiments, in case that the authentication of the user equipment through the first proxy entity is successful, the first proxy entity can acquire the proxy domain name of the first proxy entity and the first domain name of the target entity; in case that the proxy domain name is different from the first domain name, the first authentication result is notified to the target entity, so as to indicate that the target entity has the communication authority with the user equipment or the target entity communicates with the user equipment.

[0213] On the contrary, in case that the proxy domain name is the same as the first domain name, the first proxy entity temporarily does not notify the target entity of the first authentication result, but waits for whether the user equipment has a second communication authority with the target entity, and notifies the target entity of the second authentication result after determining that the user equipment has the second communication authority with the target entity.

[0214] For example, the first proxy entity may further determine whether the user equipment has the second communication authority with the target entity according to a target entity service request message sent by the user equipment.

[0215] It should also be noted that the proxy domain name may be a fully qualified domain name FQDN corresponding to the first proxy entity, and the first domain name may be a fully qualified domain name FQDN corresponding to the target entity. In some scenarios, the first proxy entity and the target entity can use the same FQDN, but different IP addresses or port numbers. In this scenario, the first communication authority can indicate that the user equipment has the access authority to the FQDN, but not necessarily indicate that the user equipment has the access authority to the target entity corresponding to the IP address or port number. At this time, it may be further determined whether the user equipment has the second communication authority with the target entity through a secure session between the user equipment and the proxy entity.

[0216] Fig. 6 shows an authentication method according to an illustrative embodiment, which may be applied to the first proxy entity. As shown in Fig. 6, the method may include the following operations.

[0217] In S601, after the authentication of the user equipment is successful, the first proxy entity establishes a secure session with the user equipment.

[0218] For example, the secure session may be a transport layer security (TLS) session, through which confidentiality and data integrity can be achieved for the communication between the first proxy entity and the user equipment.

[0219] In S602, the first proxy entity receives a target entity service request message sent by the user equipment through the secure session.

[0220] The target entity service request message includes a second target entity identifier, which is a protected entity identifier acquired by the user equipment according to the first target entity identifier of the target entity, and the target entity service request message is a message sent by the user equipment when determining that a proxy domain name of the first proxy entity is the same as a first domain name of the target entity.

[0221] In S603, the first proxy entity determines whether the user equipment has a second communication authority with the target entity according to the second target entity identifier.

[0222] In some embodiments, it may be determined that the user equipment has the second communication authority with the target entity in case that the second target entity identifier is the same as the first target entity identifier.

[0223] In some other embodiments, in case that the second target entity identifier is different from the first target entity identifier, the first proxy entity may determine whether the user equipment has the second communication authority with the target entity through message interaction with the third entity.

[0224] In S604, the first proxy entity sends a target entity service response message to the user equipment.

[0225] The target entity service response message is configured to indicate whether the user equipment has the second communication authority with the target entity.

[0226] In some embodiments, the first proxy entity may indicate that the user equipment has the second communication authority with the target entity by sending the target entity service response message. On the contrary, by not sending the target entity service response message, the first proxy entity indicates that the user equipment does not have the second communication authority with the target entity.

[0227] In some other embodiments, the first proxy entity may include success indication information in the target entity service response message, and indicate that the user equipment has the second communication authority with the target entity through the success indication information. On the contrary, by not including the success indication information in the target entity service response message, it indicates that the user equipment does not have the second communication authority with the target entity. The success indication information may be any indication information set in advance.

[0228] In some other embodiments, in case that the user equipment does not have the second communication authority with the target entity, the first proxy entity may include failure indication information in the target entity service response message to indicate that the user equipment does not have the second communication authority with the target entity. On the contrary, in case that the user equipment has the second communication authority with the target entity, the first proxy entity may indicate that the user equipment has the second communication authority with the target entity by not including the failure indication information in

the target entity service response message. The failure indication information may be any error code set in advance.

[0229] In this way, the first proxy entity can determine whether the user equipment has the second communication authority with the target entity through the secure session, and send the authorization result to the target device.

[0230] In some other embodiments, the first proxy entity may determine whether the user equipment has the second communication authority with the target entity through message interaction with the third entity.

[0231] Fig. 7 shows an authentication method according to an illustrative embodiment, which may be applied to the first proxy entity. As shown in Fig. 7, in case that the second target entity identifier is different from the first target entity identifier, the first proxy entity may determine whether the user equipment has the second communication authority with the target entity according to this method. The method may include the following operations.

[0232] In S701, the first proxy entity determines a third authority request parameter according to the second target entity identifier.

[0233] In S702, the first proxy entity sends the third authority request parameter to a third entity.

[0234] In S703, the first proxy entity acquires an authorization result parameter sent by the third entity.

[0235] In S704, the first proxy entity determines whether the user equipment has the second communication authority with the target entity according to the authorization result parameter.

[0236] With this method, when the second target entity identifier is different from the first target entity identifier, the first proxy entity may determine whether the user equipment has the second communication authority with the target entity through message interaction with the third entity.

[0237] The third authority request parameter may be configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity; the authorization result parameter may be configured to indicate whether the user equipment has the second communication authority with the target entity. For example, the third authority request parameter may include a key identifier A-KID, a second target entity identifier, and a proxy entity identifier corresponding to the first proxy entity; and the third authority request parameter may be configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity.

[0238] In some embodiments, the first proxy entity may send the third authority request parameter to the third entity via a third key request message; and the third key request message is configured to instruct the third entity to acquire an authorization result parameter and an identity of the subscriber of the user equipment. The first proxy entity may also receive a third key response message sent by the third entity; and acquire the authorization result parameter included in the third key response message.

[0239] Further, the third key response message also includes a second identity of the subscriber corresponding to the user equipment, and the first proxy entity may also acquire the second identity of the subscriber according to the third key response message received. The second identity of the subscriber may include a subscription permanent identifier SUPI corresponding to the user equipment.

[0240] In some embodiments, the third key request message may include an authorization indication parameter. The authorization indication parameter may be configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the third

key request message. Similarly, the third key response message may also include an authorization indication parameter to indicate that the third key response message is a response to the third key request message.

[0241] In some other embodiments, the first proxy entity may send the third authority request parameter to the third entity via a fourth key request message; and the fourth key request message is configured to indicate that the first proxy entity requests to acquire the authorization result parameter. The first proxy entity may also receive a fourth key response message sent by the third entity; and acquire the authorization result parameter included in the fourth key response message.

[0242] In some embodiments, the fourth key request message further includes an authorization indication parameter, and the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the fourth key request message. Similarly, the fourth key response message may also include an authorization indication parameter, which is configured to indicate that the fourth key response message is a response to the fourth key request message.

[0243] In some embodiments, the authorization result parameter may be configured to indicate authorization success or authorization failure. The first proxy entity determines whether the user equipment has the second communication authority with the target entity according to the authorization result parameter. For example, when the authorization result parameter is the authorization success, it may be determined that the user equipment has the second communication authority with the target entity. On the contrary, when the authorization result parameter is the authorization failure, or the above key response message (for example, the third key response message or the fourth key response message) does not include the authorization result parameter, it may be determined that the user equipment does not have the second communication authority with the target entity.

[0244] In some embodiments, the second communication authority may include one or more of the following authorities.

[0245] Authority 6: the user equipment has an access authority to the target entity.

[0246] Authority 7: the first proxy entity has a proxy authority to the target entity.

[0247] Authority 8: the target entity has an acquisition authority to the identity of the subscriber of the user equipment.

[0248] In this way, whether the user equipment has the second communication authority with the target entity can be determined through the secure session between the user equipment and the first proxy entity, which further improves the reliability of the authentication.

[0249] In some embodiments, when it is determined that the user equipment has the second communication authority with the target entity according to the authorization result parameter, the first proxy entity may notify the target entity of the second authentication result.

[0250] The second authentication result is configured to indicate that the user equipment has the communication authority with the target entity.

[0251] For example, in case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain, the first proxy entity may send a third notification message to the target entity, and the third notification message includes the second authentication result. Further, in case that the first proxy entity acquires the second identity of the subscriber of the user equipment (for example, the second identity of

the subscriber is acquired via the third key response message), the third notification message may also include the second identity of the subscriber.

[0252] For another example, in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain, the first proxy entity may send a fourth notification message to the second entity according to a first authentication result to instruct the second entity to send the first authentication result to the target entity. Further, in case that the first proxy entity acquires the second identity of the subscriber of the user equipment (for example, the second identity of the subscriber is acquired via the third key response message), the fourth notification message may also include the second identity of the subscriber.

[0253] In this way, the first proxy entity can verify the second communication authority between the user equipment and the first entity through the secure session, further improving the reliability of the authentication, and instruct the user equipment to communicate with the first entity in case that the user equipment has the second communication authority with the first entity.

[0254] Fig. 8 shows an authentication method according to an illustrative embodiment, which may be applied to a third entity. As shown in Fig. 8, the method may include the following operations.

[0255] In S801, the third entity receives a second authority request parameter sent by a first proxy entity.

[0256] The second authority request parameter is configured to instruct the third entity to determine whether a user equipment has a first communication authority with a target entity, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, the first proxy entity provides an authentication proxy function for the first entity, and the third entity includes an entity that provides AKMA authorization and application key derivation functions.

[0257] In S802, the third entity determines whether the user equipment has the first communication authority with the target entity according to the second authority request parameter.

[0258] In some embodiments, the second authority request parameter may include a proxy entity identifier corresponding to the first proxy entity. After receiving the second authority request parameter, the third entity may determine whether the third entity has an authority to serve the first proxy entity according to a first preset policy. The first preset policy may include a preconfigured parameter.

[0259] In case that it is determined that the third entity has the authority to serve the first proxy entity, it is determined according to the second authority request parameter whether the user equipment has a first communication authority with the target entity.

[0260] On the contrary, in case that it is determined that the third entity does not have the authority to serve the first proxy entity, the flow may be terminated without checking whether the user equipment has the first communication authority with the target entity. At this time, the third entity can send a failure indication to the first proxy entity, so that the first proxy entity can perform a failure processing accordingly; or the third entity also directly stops processing and does not send any message.

[0261] In some embodiments, the second authority request parameter includes a key identifier A-KID corresponding to the user equipment, a first target entity identifier of the target entity and a proxy entity identifier corresponding to the first proxy entity. In this step, the way to determine whether the user equipment has the

first communication authority with the target entity includes one or more of the following.

[0262] Way 1: it is determined, according to the key identifier A-KID and the first target entity identifier, whether the user equipment has an access authority to the target entity.

[0263] Way 2: it is determined, according to the key identifier A-KID and the proxy entity identifier, whether the user equipment has an access authority to the first proxy entity.

[0264] Way 3: it is determined, according to the proxy entity identifier and the first target entity identifier, whether the first proxy entity has a proxy authority to the target entity.

[0265] Way 4: it is determined, according to the key identifier A-KID and the first target entity identifier, whether the target entity has an acquisition authority to the identity of the subscriber of the user equipment.

[0266] Way 5: it is determined, according to the key identifier A-KID, whether the user equipment is authorized to use the AKMA.

[0267] In some embodiments, the third entity may determine that the user equipment has the first communication authority with the target entity, in case that it is determined that the user equipment has the access authority to both the first proxy entity and the target entity, and the first proxy entity has the proxy authority to the target entity.

[0268] In some other embodiments, the third entity may determine that the user equipment has the first communication authority with the target entity, in case that it is determined that the user equipment has the access authority to the target entity and the first proxy entity has the proxy authority to the target entity.

[0269] In S803, the third entity acquires first pending key information in case that the user equipment has the first communication authority with the target entity.

[0270] For example, the first pending key information may be acquired according to entity key information corresponding to the target entity.

[0271] In some embodiments, the entity key information corresponding to the target entity may include an application key K_{AF} corresponding to the target entity.

[0272] In some other embodiments, the entity key information corresponding to the target entity may include the application key K_{AF} and a key expiration time (K_{AF} expiration time) corresponding to the target entity.

[0273] In S804, the third entity sends the first pending key information to the first proxy entity.

[0274] In this way, the first proxy entity determines whether the user equipment has the first communication authority with the target entity according to the first pending key information.

[0275] In some embodiments, the third entity may receive the second authority request parameter sent by the first proxy entity via a first key request message; and the first key request message is configured to instruct the third entity to acquire the first pending key information and the identity of the subscriber of the user equipment. The third entity may also send the first pending key information to the first proxy entity via a first key response message.

[0276] Further, the third entity may send the first pending key information and a second identity of the subscriber corresponding to the user equipment to the first proxy entity via the first key response message in case that it is determined that the target entity has the authority to acquire the identity of the subscriber.

[0277] For example, the third entity sends the first pending key information and the second identity of

the subscriber corresponding to the user equipment to the first proxy entity via a third key response message in case that it is determined that the target entity has the authority to acquire the identity of the subscriber. For example, the second identity of the subscriber corresponding to the user equipment is acquired, and the second identity of the subscriber and an authorization result parameter are sent to the first proxy entity via the third key response message.

[0278] In some embodiments, the second identity of the subscriber may be an identifier representing the user equipment in the 3GPP operator domain; for example, the second identity of the subscriber may be a subscription permanent identifier SUPI corresponding to the user equipment.

[0279] In some other embodiments, the third entity may receive the second authority request parameter sent by the first proxy entity via a second key request message; and the second key request message is configured to instruct the third entity to acquire the first pending key information. The third entity may also send the first pending key information to the first proxy entity via a second key response message.

[0280] In this way, the third entity can determine whether the user equipment has the first communication authority with the target entity, and notify the first proxy entity via the first pending key information.

[0281] In some embodiments, the above first proxy entity may include a trusted authentication proxy AP entity inside the 3GPP operator domain.

[0282] In some embodiments, the above first entity may include: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

[0283] In some embodiments, the above third entity may include: an AKMA anchor function AAnF entity.

[0284] Fig. 9 shows an authentication method according to an illustrative embodiment, which may be applied to a third entity. As shown in Fig. 9, after sending the third key response message to the second entity, the method may further include:

[0285] In S901, the third entity receives a third authority request parameter sent by a first proxy entity.

[0286] In S902, the third entity determines whether the user equipment has a second communication authority with the target entity according to the third authority request parameter.

[0287] In S903, the third entity sends an authorization result parameter to the first proxy entity.

[0288] The authorization result parameter may be configured to notify the first proxy entity whether the user equipment has the second communication authority with the target entity.

[0289] In some embodiments, the third authority request parameter may include a proxy entity identifier corresponding to the first proxy entity. After receiving a fourth key request message, the third entity may determine whether the third entity has the authority to serve the first proxy entity according to a first preset policy. The first preset policy may include a preconfigured parameter.

[0290] In case that it is determined that the third entity has the authority to serve the first proxy entity, it is determined according to the fourth key request message whether the user equipment has the second communication authority with the target entity.

[0291] On the contrary, in case that it is determined that the third entity does not have the authority to

serve the first proxy entity, the process may be terminated, without checking whether the user equipment has the first communication authority with the target entity. At this time, the third entity may send a failure indication to the second entity, so that the second entity performs a failure processing accordingly; or the third entity also directly stops processing and does not send any message.

[0292] In some embodiments, the third authority request parameter may include a key identifier A-KID, a second target entity identifier and a proxy entity identifier corresponding to the first proxy entity. The second target entity identifier is a protected entity identifier acquired by the user equipment according to a first proxy entity identifier of the target entity. The way for determining whether the target entity has the second communication authority with the target entity in step S902 may include one or more of the followings.

[0293] Way 6: it is determined, according to the key identifier A-KID and the second target entity identifier, whether the user equipment has an access authority to the target entity.

[0294] Way 7: it is determined, according to the proxy entity identifier and the second target entity identifier, whether the first proxy entity has a proxy authority to the target entity

[0295] Way 8: it is determined, according to the key identifier A-KID and the first target entity identifier, whether the target entity has an acquisition authority to an identity of the subscriber of the user equipment.

[0296] In some embodiments, the third entity may determine that the user equipment has the second communication authority with the target entity in case that it is determined that the user equipment has the access authority to the target entity and the first proxy entity has the proxy authority to the target entity.

[0297] In some embodiments, the third entity may receive the third authority request parameter sent by the first proxy entity via a third key request message; and the third key request message is configured to instruct the third entity to acquire an authorization result parameter and an identity of the subscriber of the user equipment. The third entity also can send the authorization result parameter to the first proxy entity via a third key response message.

[0298] Further, the third key request message may include an authorization indication parameter, and the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the third key request message. Similarly, the third key response message may also include an authorization indication parameter.

[0299] Further, in case that it is determined that the target entity has the acquisition authority to the identity of the subscriber, the third entity may send the authorization result parameter and a second identity of the subscriber corresponding to the user equipment to the first proxy entity via the third key response message.

[0300] For example, in case that it is determined that the target entity has the acquisition authority to the identity of the subscriber, the third entity may send the authorization result parameter and the second identity of the subscriber corresponding to the user equipment to the first proxy entity via the third key response message. For example, the second identity of the subscriber corresponding to the user equipment is acquired, and the second identity of the subscriber and the authorization result parameter are sent to the first proxy entity via the third key response message.

[0301] For example, the second identity of the subscriber may include a subscription permanent identifier SUPI corresponding to the user equipment.

[0302] In some other embodiments, the third entity may receive the third authority request parameter

sent by the first proxy entity via a fourth key request message; and the fourth key request message is configured to instruct the third entity to acquire the authorization result parameter. The third entity may also send the authorization result parameter to the first proxy entity via a fourth key response message.

[0303] Further, the fourth key request message may further include an authorization indication parameter, and the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the third key request message. Similarly, the fourth key response message may also include an authorization indication parameter to indicate that the fourth key response message is a response to the fourth key request message.

[0304] In some embodiments, the authorization result parameter may be configured to indicate authorization success or authorization failure. For example, the third entity may determine a value of the authorization result parameter based on whether the user equipment has the second communication authority with the target entity. For example, in case that it is determined that the user equipment has the second communication authority with the target entity, the third entity may set the authorization result parameter as authorization success (for example, with the value of 1); in case that it is determined that the user equipment does not have the second communication authority with the target entity, the third entity may set the value of the authorization result parameter as authorization failure (for example, with the value of 0).

[0305] In some other embodiments, the third entity may indicate that the user equipment does not have the second communication authority with the target entity by not including the authorization result information in the above key response message (such as the third key response message or the fourth key response message). For example, in case that the third entity determines that the user equipment does not have the second communication authority with the target entity, the authorization result information may not be included in the above key response message. On the contrary, in case that it is determined that the user equipment has the second communication authority with the target entity, the authorization result information may be included in the above key response message.

[0306] Fig. 10 shows an authentication method according to an illustrative embodiment, which may be applied to the first entity. As shown in Fig. 10, the method may also include the following operations.

[0307] In S1001, the first entity acquires an authentication result of a first proxy entity to a user equipment.

[0308] In S1002, the first entity communicates with the user equipment according to the authentication result.

[0309] The authentication result includes a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with the target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity.

[0310] It should be noted that the first entity may wait for the user equipment to initiate communication; or the first entity may actively initiate communication with the user equipment, which is not limited in the

present disclosure.

[0311] In some embodiments, an authentication result notification message includes a first identity of the subscriber of the user equipment. The first identity of the subscriber may be an identifier representing the user equipment outside the 3GPP operator domain. For example, the first identity of the subscriber is a generic public subscription identifier GPSI corresponding to the user equipment.

[0312] In case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain, the target entity may receive a first notification message sent by the first proxy entity, and the first notification message includes the first authentication result; or the target entity may receive a third notification message, and the third notification message includes the second authentication result.

[0313] Further, the first notification message or the third notification message further includes a second identity of the subscriber corresponding to the user equipment. The second identity of the subscriber may include a subscription permanent identifier SUPI correspond to the user equipment.

[0314] In case that the target entity is an untrusted entity providing the application function outside the 3GPP operator domain, the target entity may receive a fifth notification message sent by a second entity, the fifth notification message includes the first authentication result, and the fifth notification message is a message sent by the second entity in response to receiving a second notification message; or the target entity may receive a sixth notification message sent by the second entity, the sixth notification message includes the second authentication result, and the fifth notification message is a message sent by the second entity in response to receiving a fourth notification message.

[0315] Further, the fifth notification message or the sixth notification message further includes a first identity of the subscriber of the user equipment. The first identity of the subscriber may be a generic public subscription identifier GPSI corresponding to the user equipment.

[0316] In some embodiments, the first proxy entity may include a trusted authentication proxy AP entity inside the 3GPP operator domain.

[0317] In some embodiments, the first entity may include: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

[0318] In some embodiments, the second entity may include: a network exposure function NEF entity or a service capability exposure function SCEF entity.

[0319] In this way, the first entity can determine whether the user equipment has the first communication authority with the first entity according to the authentication result notification message of the first proxy entity, thereby reducing the load of the first entity and improving the efficiency of the first entity.

[0320] Fig. 11 shows an authentication method according to an illustrative embodiment, which may be applied to the second entity. As shown in Fig. 11, the method may include the following operations:

[0321] In S1101, the second entity acquires an authentication result of a first proxy entity to a user equipment.

[0322] The authentication result includes a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with a target entity; the second authentication result is configured to indicate that the user equipment

has a second communication authority with the target entity; the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an untrusted entity providing an application function outside a 3GPP operator domain, the first proxy entity includes a trusted entity providing an authentication function inside the 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity.

[0323] In S1102, the second entity sends the authentication result to the target entity.

[0324] As a result, the target entity can communicate with the user equipment according to the authentication result.

[0325] By adopting the above method, communication between the first proxy entity inside the 3GPP operator domain and the first entity outside the 3GPP operator domain can be realized through the second entity.

[0326] In some embodiments, the above second entity may include: a network exposure function NEF entity or a service capability exposure function SCEF entity; the above first proxy entity may include a trusted authentication proxy AP entity inside the 3GPP operator domain; the above first entity may include: an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

[0327] In some embodiments, the second entity may receive a second notification message sent by the first proxy entity; acquire the first authentication result according to the second notification message; and send a fifth notification message to the first entity according to the first authentication result. The second notification message is a message sent by the first proxy entity to the second entity according to the first authentication result in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain.

[0328] Further, in case that the second notification message includes a second identity of the subscriber corresponding to the user equipment, the second entity may acquire a first identity of the subscriber corresponding to the user equipment according to the second identity of the subscriber; and send the fifth notification message to the first entity according to the first authentication result and the first identity of the subscriber.

[0329] In some other embodiments, the second entity may receive a fourth notification message sent by the first proxy entity; acquire the second authentication result according to the second notification message; and send a sixth notification message to the first entity according to the second authentication result. The fourth notification message is a message sent by the first proxy entity to the second entity according to the second authentication result in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain.

[0330] Further, in case that the fourth notification message includes a second identity of the subscriber corresponding to the user equipment, the second entity may acquire a first identity of the subscriber corresponding to the user equipment according to the second identity of the subscriber; and send the sixth notification message to the first entity according to the second authentication result and the first identity of the subscriber.

[0331] In some embodiments, the second identity of the subscriber may be an identifier representing the user equipment inside the 3GPP operator domain; and the first identity of the subscriber may be an identifier representing the user equipment outside the 3GPP operator domain. For example, the second identity of the

subscriber may be a subscription permanent identifier SUPI corresponding to the user equipment; and the first identity of the subscriber may be a generic public subscription identifier GPSI corresponding to the user equipment.

[0332] The second entity may determine the first identity of the subscriber corresponding to the second identity of the subscriber according to a preset identifier correspondence relationship; and the preset identifier correspondence relationship includes a correspondence relationship between the second identity of the subscriber and the first identity of the subscriber.

[0333] Fig. 12 shows an authentication method according to an illustrative embodiment, as shown in Fig. 12, the method may include the following operations.

[0334] In S1201, the user equipment sends an application session establishment request message to the first proxy entity.

[0335] For example, the application session establishment request message may include a first authority request parameter, and the first authority request parameter may include a key identifier A-KID of the user equipment, and a first target entity identifier, Target AF ID, of the target entity. The target entity may be an entity which is determined by the user equipment from one or more first entities and with which communication is requested.

[0336] In some embodiments, the user equipment may acquire the key identifier A-KID through a preset function entity in the communication system, and the preset function entity may include an authentication service function AUSF entity.

[0337] In S1202, the first proxy entity sends a second authority request parameter to the third entity in response to receiving the application session establishment request message.

[0338] In some embodiments, the first proxy entity may receive the application session establishment request message sent by the user equipment, and determine the second authority request parameter according to the first authority request parameter in the application session establishment request message.

[0339] For example, in case that the first authority request parameter includes the key identifier A-KID of the user equipment, and the first target entity identifier, Target AF ID, of the target entity, it may be determined that the second authority request parameter includes the key identifier A-KID, the first target entity identifier (Target AF ID), and a proxy entity identifier of the first proxy entity.

[0340] In some embodiments, the first proxy entity may send the second authority request parameter to the third entity via a first key request message; and the first key request message is configured to instruct the third entity to acquire first pending key information and an identity of the subscriber of the user equipment. For example, the first key request message may be Naanf_AKMA_ApplicationKey_Get Request message.

[0341] In some other embodiments, the first proxy entity may send the second authority request parameter to the third entity via a second key request message; and the second key request message is configured to indicate that the first proxy entity requests to acquire the first pending key information. For example, the second key request message may be Naanf_AKMA_ApplicationKey_AnonUser_Get Request message.

[0342] In step S1203, the third entity acquires the first pending key information in case that it is determined that the user equipment has the first communication authority with the target entity according to the second authority request parameter.

[0343] The third entity may authenticate the communication authority between the user equipment and

the target entity based on a preset authority policy to determine whether the user equipment has the first communication authority with the target entity. The examples are as follows.

[0344] In some embodiments, the way for the third entity to determine whether the user equipment has the first communication authority with the target entity may include one or more of the followings.

[0345] Way 1: it is determined, according to the key identifier A-KID and the first target entity identifier, whether the user equipment has the access authority to the target entity.

[0346] Way 2: it is determined, according to the key identifier A-KID and the proxy entity identifier, whether the user equipment has the access authority to the first proxy entity.

[0347] Way 3: it is determined, according to the proxy entity identifier and the first target entity identifier, whether the first proxy entity has the proxy authority to the target entity.

[0348] Way 4: it is determined, according to the key identifier A-KID and the first target entity identifier, whether the target entity has the acquisition authority to the identity of the subscriber of the user equipment.

[0349] Way 5: it is determined, according to the key identifier A-KID, whether the user equipment is authorized to use the AKMA.

[0350] In some other embodiments, the third entity may determine that the user equipment has the first communication authority with the target entity, in case that it is determined that the user equipment has the access authority to the target entity, and the first proxy entity has the proxy authority to the target entity. For example, the third entity may determine whether the user equipment has the first communication authority with the target entity through the following steps.

[0351] In S11, according to the proxy entity identifier and the first target entity identifier, it is determined whether the first proxy entity has the proxy authority to the target entity.

[0352] If it is determined that the first proxy entity does not have the proxy authority to the target entity, it is directly determined that the user equipment does not have the first communication authority with the target entity, and step S12 is not performed. On the contrary, if it is determined that the first proxy entity has the proxy authority to the target entity, step S12 continues to be performed.

[0353] In S12, according to the key identifier A-KID and the first target entity identifier, it is determined whether the user equipment has the access authority to the target entity.

[0354] If it is determined that the user equipment does not have the access authority to the target entity, it is directly determined that the user equipment does not have the first communication authority with the target entity, and step S13 is not performed. On the contrary, if it is determined that the user equipment has the access authority to the target entity, step S13 continues to be performed.

[0355] In S13, according to the key identifier A-KID, it is determined whether the user equipment is authorized to use the AKMA.

[0356] In case that it is determined that the user equipment is authorized to use the AKMA, it may be determined that the user equipment has the first communication authority with the target entity. On the contrary, in case that it is determined that the user equipment is not authorized to use the AKMA, it may be determined that the user equipment does not have the first communication authority with the target entity.

[0357] It should be noted that the first pending key information may include entity key information corresponding to the target entity.

[0358] In some embodiments, the entity key information corresponding to the target entity may include the application key K_{AF} corresponding to the target entity.

[0359] In some other embodiments, the entity key information corresponding to the target entity may include the application key K_{AF} and the key expiration time (K_{AF} expiration time) corresponding to the target entity.

[0360] In S1204, the third entity sends the first pending key information to the first proxy entity.

[0361] In some embodiments, the third entity may send the first pending key information to the first proxy entity via a first key response message. For example, the first key response message may be Naanf_AKMA_ApplicationKey_Get Responsemessage.

[0362] In some other embodiments, the third entity may send the first pending key information to the first proxy entity via a second key response message. For example, the second key response message may be Naanf_AKMA_ApplicationKey_AnonUser_Get Responsemessage

[0363] In some embodiments, the first key response message may also include a second identity of the subscriber of the user equipment, and the second identity of the subscriber may be an identifier representing the user equipment inside the 3GPP operator domain. For example, the second identity of the subscriber may be a subscription permanent identifier SUPI corresponding to the user equipment.

[0364] In S1205, the first proxy entity sends an application session establishment response message to the user equipment.

[0365] In case that the first proxy entity acquires the application key K_{AF} in the first key response message, it may be determined that the user equipment has the first communication authority with the target entity. At this time, the first proxy entity may send the application session establishment response message to the user equipment.

[0366] In S1206, the user equipment performs authentication through the first proxy entity.

[0367] The user equipment may perform the authentication through the first proxy entity in case that it is determined that the user equipment has the first communication authority with the target entity. For example, the user equipment can derive the entity key K_{AF} corresponding to the target entity based on the FQDN of the target entity, and perform the authentication with the first proxy entity based on the entity key K_{AF} .

[0368] In S1207a, the first proxy entity notifies the target entity of the first authentication result.

[0369] The first authentication result may be configured to indicate that the user equipment has the communication authority with the target entity.

[0370] In some embodiments, in case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain, the first proxy entity may send a first notification message to the target entity, and the first notification message may include the first authentication result. Further, in case that the first proxy entity acquires the second identity of the subscriber of the user equipment (for example, the second identity of the subscriber is acquired via the first key response message), the first notification message may also include the second identity of the subscriber.

[0371] In some other embodiments, in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain, the first proxy entity may send a second notification message to the second entity according to the first authentication result to instruct the second entity to send the first authentication result to the target entity. Similarly, in case that the first proxy entity acquires the second

identity of the subscriber of the user equipment (for example, the second identity of the subscriber is acquired via the first key response message), the second notification message may also include the second identity of the subscriber.

[0372] In some embodiments, in case that the authentication of the user equipment through the first proxy entity is successful, the first proxy entity may notify the target entity of the first authentication result (step S1207a is performed, while step S1207b and subsequent steps do not continue to be performed).

[0373] In some other embodiments, in case that the authentication of the user equipment through the first proxy entity is successful, the first proxy entity may acquire the proxy domain name of the first proxy entity and the first domain name of the target entity. In case that the proxy domain name is different from the first domain name, the first authentication result is notified to the target entity (step S1207a step is performed, while step S1209b and subsequent steps do not continue to be performed), so as to indicate that the target entity has the communication authority or communicates with the user equipment.

[0374] In some other embodiments, in case that the proxy domain name is the same as the first domain name, the first proxy entity may temporarily not send the authentication result notification message to the target entity, but waits for whether the user equipment has the second communication authority with the target entity, and notifies the target entity of the first authentication result after determining that the user equipment has the second communication authority with the target entity. That is, step S1207a is not performed, while step S1207b and subsequent steps continue to be performed.

[0375] In S1207b, the user equipment establishes a secure session with the first proxy entity.

[0376] The secure session may include a TLS session.

[0377] In S1208, the user equipment sends a target entity service request message to the first proxy entity.

[0378] The target entity service request message includes a second target entity identifier, which is a protected entity identifier acquired by the user equipment according to the first target entity identifier of the target entity.

[0379] In some embodiments, the target entity service request message may include the key identifier A-KID and the second target entity identifier.

[0380] In some embodiments, in case that the second target entity identifier is the same as the first target entity identifier, it may be determined that the user equipment has the second communication authority with the target entity, then the authentication result notification message may be sent to the target entity, and a target entity service response message may be sent to the user equipment. That is, steps S1209a and S1213 are performed, without need to perform steps S1209b to S1212.

[0381] In some other embodiments, in case that the second target entity identifier is different from the first target entity identifier, the first proxy entity may determine whether the user equipment has the second communication authority with the target entity through key request message interaction with the second entity. That is, step S1209a is not performed, and step S1209b and subsequent steps continue to be performed.

[0382] In S1209a, the first proxy entity notifies the target entity of the first authentication result.

[0383] In S1209b, the first proxy entity sends the third authority request parameter to the third entity.

[0384] In some embodiments, the third authority request parameter may include the key identifier A-KID, the second target entity identifier, and the proxy entity identifier corresponding to the first proxy entity;

and the third authority request parameter may be configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity.

[0385] In some embodiments, the first proxy entity may send the third authority request parameter to the third entity via a third key request message; and the third key request message is configured to instruct the third entity to acquire an authorization result parameter and the identity of the subscriber of the user equipment. For example, the third key request message may be a Naanf_AKMA_ApplicationKey_Get Request message.

[0386] In some other embodiments, the first proxy entity may send the third authority request parameters to the third entity via a fourth key request message; and the fourth key request message is configured to indicate that the first proxy entity requests to acquire the authorization result parameter. For example, the fourth key request message may be Naanf_AKMA_ApplicationKey_AnonUser_Get Request message.

[0387] In S1210, the third entity determines whether the user equipment has the second communication authority with the target entity according to the third authority request parameter.

[0388] For example, the way for the third entity to determine whether the user equipment has the second communication authority with the target entity may include one or more of the followings.

[0389] Way 6: it is determined, according to the key identifier A-KID and the second target entity identifier, whether the user equipment has the access authority to the target entity.

[0390] Way 7: it is determined, according to the proxy entity identifier and the second target entity identifier, whether the first proxy entity has the proxy authority to the target entity.

[0391] Way 8: it is determined, according to the key identifier A-KID and the first target entity identifier, whether the target entity has the acquisition authority to the identity of the subscriber of the user equipment.

[0392] In some embodiments, the third entity may determine that the user equipment has the second communication authority with the target entity, in case that it is determined that the user equipment has the access authority to the target entity and the first proxy entity has the proxy authority to the target entity.

[0393] In S1211, the third entity sends the authorization result parameter to the first proxy entity.

[0394] The authorization result parameter may be configured to notify the first proxy entity whether the user equipment has the second communication authority with the target entity.

[0395] In some embodiments, the third entity may send the authorization result parameter to the first proxy entity via a third key response message. For example, the third key response message may be Naanf_AKMA_ApplicationKey_Get Response message.

[0396] In some other embodiments, the third entity may send the authorization result parameter to the first proxy entity via a fourth key response message. For example, the fourth key response message may be Naanf_AKMA_ApplicationKey_AnonUser_Get Response message.

[0397] In some embodiments, in case that the third entity determines that the target entity has the authority to acquire the identity of the subscriber, the third key response message may also include the second identity of the subscriber of the user equipment. Similarly, the fourth key response message may also include the second identity of the subscriber of the user equipment. The second identity of the subscriber may be a subscription permanent identifier SUPI corresponding to the user equipment.

[0398] In S1212, the first proxy entity notifies the target entity of the second authentication result.

[0399] The second authentication result may be configured to indicate that the target entity has

communication authority with the user equipment.

[0400] For example, in case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain, the first proxy entity may send a third notification message to the target entity, and the third notification message includes the second authentication result. Further, in case that the first proxy entity acquires the second identity of the subscriber of the user equipment (for example, the second identity of the subscriber is acquired via the third key response message), the third notification message may also include the second identity of the subscriber.

[0401] For another example, in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain, the first proxy entity may send a fourth notification message to the second entity according to the first authentication result to instruct the second entity to send the first authentication result to the target entity. Further, in case that the first proxy entity acquires the second identity of the subscriber of the user equipment (for example, the second identity of the subscriber is acquired via the third key response message), the fourth notification message may also include the second identity of the subscriber.

[0402] In some embodiments, the second identity of the subscriber may be a subscription permanent identifier SUPI corresponding to the user equipment.

[0403] In step S1213, the first proxy entity sends a target entity service response message to the user equipment.

[0404] The target entity service response message is configured to indicate whether the user equipment has the second communication authority with the target entity.

[0405] In some embodiments, the first proxy entity may include a trusted authentication proxy AP entity inside the 3GPP operator domain.

[0406] In some embodiments, the first entity may include: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

[0407] In some embodiments, the second entity may include: a network exposure function NEF entity or a service capability exposure function SCEF entity.

[0408] In some embodiments, the third entity may include: an AKMA anchor function AAnF entity.

[0409] In this way, for the first entity, whether the user equipment has the communication authority with the first entity is determined by the trusted first proxy entity inside the 3GPP operator domain, and the authentication of the user equipment is performed in case that the user equipment has the first communication authority, so that part of functions of the first entity can be realized through the first proxy entity, thereby reducing the load of the first entity and improving the efficiency of the first entity. Moreover, the user equipment realizes the authorization and authentication with one or more first entities through the unified first proxy entity, which also reduces the complexity of authentication of the user equipment and improves the efficiency of the user equipment.

[0410] Fig. 13 is a block diagram of an authentication apparatus 1300 according to an illustrative embodiment, which may be applied to the user equipment. As shown in Fig. 13, the apparatus 1300 may include:

[0411] a target entity determining module 1301 configured to determine, from one or more first entities,

a target entity with which communication is requested;

[0412] a parameter determining module 1302 configured to determine a first authority request parameter according to the target entity;

[0413] a first message sending module 1303 configured to send an application session establishment request message to a first proxy entity according to the first authority request parameter; where the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with the target entity according to the first authority request parameter; the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;

[0414] a first message receiving module 1304 configured to determine whether the user equipment has the first communication authority with the target entity in response to receiving an application session establishment response message sent by the first proxy entity; and

[0415] an authentication module configured to perform authentication through the first proxy entity in case that the user equipment has the first communication authority with the target entity.

[0416] Optionally, the parameter determining module 1302 is configured to take a first target entity identifier of the target entity and a key identifier A-KID corresponding to the user equipment as the first authority request parameter.

[0417] Optionally, the first communication authority includes one or more of:

[0418] the user equipment having an access authority to the target entity;

[0419] the user equipment having an access authority to the first proxy entity;

[0420] the first proxy entity having a proxy authority to the target entity; or

[0421] the target entity having an acquisition authority to an identity of the subscriber of the user equipment.

[0422] Fig. 14 is a block diagram of an authentication apparatus 1300 according to an illustrative embodiment, which may be applied to the user equipment, as shown in Fig. 14, the apparatus 1300 may further include: a user communication module 1305 configured, after the authentication through the first proxy entity is successful, to: establish a secure session with the first proxy entity; acquire a proxy domain name of the first proxy entity and a first domain name of the target entity; determine whether the user equipment has a second communication authority with the target entity through the secure session in case that the proxy domain name is the same as the first domain name; and communicate with the target entity in case that it is determined that the user equipment has the second communication authority with the target entity.

[0423] Optionally, the user communication module 1305 is configured to: send a target entity service request message to the first proxy entity through the secure session; and determine whether the user equipment has the second communication authority with the target entity in response to receiving a target entity service response message sent by the first proxy entity. The target entity service request message includes a second target entity identifier, the second target entity identifier is a protected entity identifier acquired by the user equipment according to the first target entity identifier, and the target entity service request message is configured to instruct the first proxy entity to determine whether the user equipment has the second communication authority with the target entity according to the second target entity identifier.

[0424] Optionally, the second communication authority includes one or more of: the user equipment having an access authority to the target entity; the first proxy entity having a proxy authority to the target entity; or the target entity having an acquisition authority to an identity of the subscriber of the user equipment.

[0425] Optionally, first message receiving module 1304 is configured to: determine that the user equipment has the first communication authority with the target entity in case that the application session establishment response message is received; or determine that the user equipment has the first communication authority with the target entity, in case that the application session establishment response message is received and the session establishment response message includes success indication information.

[0426] Optionally, the first proxy entity includes a trusted authentication proxy AP entity inside the 3GPP operator domain.

[0427] Optionally, the first entity includes a trusted entity providing an application function inside the 3GPP operator domain.

[0428] Optionally, the first entity includes: a trusted application function AF entity inside the 3GPP operator domain, or a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain.

[0429] Optionally, the first entity includes an untrusted entity providing an application function outside the 3GPP operator domain, the first proxy entity communicates with the first entity through a second entity; and the second entity includes an entity providing a network exposure function.

[0430] Optionally, the first entity includes: an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS outside the 3GPP operator domain.

[0431] Optionally, the second entity includes: a network exposure function NEF entity or a service capability exposure function SCEF entity.

[0432] Fig. 15 is a block diagram of an authentication apparatus 1500 according to an illustrative embodiment, which may be applied to a first proxy entity. As shown in Fig. 15, the apparatus 1500 may include:

[0433] a first proxy receiving module 1501 configured to receive an application session establishment request message sent by a user equipment; where the application session establishment request message includes a first authority request parameter, the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with a target entity according to the first authority request parameter, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;

[0434] a first proxy determining module 1502 configured to determine whether the user equipment has the first communication authority with the target entity according to the first authority request parameter; and

[0435] a first proxy sending module 1503 configured to send an application session establishment response message to the user equipment, and perform authentication of the user equipment, in case that the user equipment has the first communication authority with the target entity

[0436] Optionally, the first authority request parameter includes a first target entity identifier of the

target entity and a key identifier A-KID corresponding to the user equipment.

[0437] Optionally, the first communication authority includes one or more of:

[0438] the user equipment having an access authority to the target entity;

[0439] the user equipment having an access authority to the first proxy entity;

[0440] the first proxy entity having a proxy authority to the target entity; or

[0441] the target entity having an acquisition authority to an identity of the subscriber of the user equipment.

[0442] Optionally, the first proxy determining module 1502 is configured to: determine a second authority request parameter according to the first authority request parameter; send the second authority request parameter to a third entity, where the third entity includes an entity that provides AKMA authorization and application key derivation functions, and the second authority request parameter is configured to instruct the third entity to determine whether the user equipment has the first communication authority with the target entity; acquire first pending key information sent by the third entity, where the first pending key information is key information acquired by the third entity according to the second authority request parameter; and determine whether the user equipment has the first communication authority with the target entity according to the first pending key information.

[0443] Optionally, the first proxy determining module 1502 is configured to: take the first authority request parameter and a proxy entity identifier corresponding to the first proxy entity as the second authority request parameter.

[0444] Optionally, the first proxy determining module 1502 is configured to: send the second authority request parameter to the third entity via a first key request message, where the first key request message is configured to instruct the third entity to acquire the first pending key information and an identity of the subscriber of the user equipment; receive a first key response message sent by the third entity; and acquire the first pending key information included in the first key response message.

[0445] Optionally, the first key response message further includes a second identity of the subscriber corresponding to the user equipment, and the first proxy determining module 1502 is configured to acquire the second identity of the subscriber according to the first key response message received.

[0446] Optionally, the second identity of the subscriber includes a subscription permanent identifier SUPI corresponding to the user equipment.

[0447] Optionally, the first proxy determining module 1502 is configured to: send the second authority request parameter to the third entity via a second key request message, where the second key request message is configured to indicate that the first proxy entity requests to acquire the first pending key information; receive a second key response message sent by the third entity; and acquire the first pending key information included in the second key response message.

[0448] Optionally, the first proxy determining module 1502 is configured to: determine that the user equipment has the first communication authority with the target entity in case that the first pending key information includes entity key information corresponding to the target entity.

[0449] Optionally, in case that the authentication of the user equipment is successful, the first proxy sending module 1503 is configured to: notify the target entity of a first authentication result of the authentication.

[0450] Optionally, the first proxy sending module 1503 is configured to: acquire a proxy domain name

of the first proxy entity and a first domain name of the target entity; and notify the target entity of the first authentication result in case that the proxy domain name is different from the first domain name.

[0451] Optionally, in case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain, the first proxy sending module 1503 is configured to: send a first notification message to the target entity. The first notification message includes the first authentication result.

[0452] Optionally, in case that the first proxy entity acquires a second identity of the subscriber of the user equipment, the first notification message further includes the second identity of the subscriber.

[0453] Optionally, in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain, the first proxy sending module 1503 is configured to: send a second notification message to a second entity according to the first authentication result to instruct the second entity to send the first authentication result to the target entity.

[0454] Optionally, in case that the first proxy entity acquires a second identity of the subscriber of the user equipment, the second notification message further includes the second identity of the subscriber.

[0455] Optionally, after the authentication of the user equipment is successful, the apparatus further includes:

[0456] Fig. 16 is a block diagram of an authentication apparatus 1500 according to an illustrative embodiment, as shown in Fig. 16, the apparatus may further include: a first proxy communication module 1504 configured to: establish a secure session with the user equipment; receive, through the secure session, a target entity service request message sent by the user equipment, where the target entity service request message includes a second target entity identifier, the second target entity identifier is a protected entity identifier acquired by the user equipment according to a first target entity identifier of the target entity, and the target entity service request message is a message sent by the user equipment in case that it is determined that a proxy domain name of the first proxy entity is the same as a first domain name of the target entity; determine whether the user equipment has a second communication authority with the target entity according to the second target entity identifier; and send a target entity service response message to the user equipment, where the target entity service response message is configured to indicate whether the user equipment has the second communication authority with the target entity.

[0457] Optionally, the second communication authority includes one or more of:

[0458] the user equipment having an access authority to the target entity;

[0459] the first proxy entity having a proxy authority to the target entity; or

[0460] the target entity having an acquisition authority to an identity of the subscriber of the user equipment.

[0461] Optionally, the first proxy communication module 1504 is configured to: determine that the user equipment has the second communication authority with the target entity in case that the second target entity identifier is the same as the first target entity identifier.

[0462] Optionally, the first proxy communication module 1504 is configured to: determine a third authority request parameter according to the second target entity identifier in case that the second target entity identifier is different from the first target entity identifier; send the third authority request parameter to a third entity, where the third authority request parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity; acquire an authorization

result parameter sent by the third entity, where the authorization result parameter is configured to indicate whether the user equipment has the second communication authority with the target entity; and determine whether the user equipment has the second communication authority with the target entity according to the authorization result parameter.

[0463] Optionally, the first proxy communication module 1504 is configured to: take the second target entity identifier, a key identifier A-KID corresponding to the user equipment, and a proxy entity identifier corresponding to the first proxy entity as the third authority request parameter.

[0464] Optionally, the first proxy communication module 1504 is configured to: send the third authority request parameter to the third entity via a third key request message, where the third key request message is configured to instruct the third entity to acquire the authorization result parameter and an identity of the subscriber of the user equipment; receive a third key response message sent by the third entity; and acquire the authorization result parameter included in the third key response message.

[0465] Optionally, the third key response message further includes a second identity of the subscriber corresponding to the user equipment, and the first proxy communication module 1504 is configured to: acquire the second identity of the subscriber according to the third key response message received.

[0466] Optionally, the third key request message further includes an authorization indication parameter, and the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the third key request message.

[0467] Optionally, the first proxy communication module 1504 is configured to: send the third authority request parameter to the third entity via a fourth key request message, where the fourth key request message is configured to indicate that the first proxy entity requests to acquire the authorization result parameter; receive a fourth key response message sent by the third entity; and acquire the authorization result parameter included in the fourth key response message.

[0468] Optionally, the fourth key request message further includes an authorization indication parameter, the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the fourth key request message.

[0469] Optionally, the first proxy communication module 1504 is configured to: notify the target entity of a second authentication result in case that it is determined according to an authorization result parameter that the user equipment has the second communication authority with the target entity. The second authentication result is configured to indicate that the target entity has a communication authority with the target entity.

[0470] Optionally, the first proxy communication module 1504 is configured to: send a third notification message to the target entity, in case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain. The third notification message includes the second authentication result.

[0471] Optionally, in case that the first proxy entity acquires a second identity of the subscriber of the user equipment, the third notification message further includes the second identity of the subscriber.

[0472] Optionally, the first proxy communication module 1504 is configured to: send a fourth notification message to a second entity according to a first authentication result to instruct the second entity to

send the first authentication result to the target entity, in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain.

[0473] Optionally, in case that the first proxy entity acquires a second identity of the subscriber of the user equipment, the fourth notification message further includes the second identity of the subscriber.

[0474] Optionally, the first pending key information includes an application key K_{AF} and a key expiration time.

[0475] Optionally, the second entity includes a network exposure function NEF entity or a service capability exposure function SCEF entity.

[0476] Optionally, the first proxy entity includes a trusted authentication proxy AP entity inside the 3GPP operator domain.

[0477] Optionally, the first entity includes: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

[0478] Fig. 17 is a block diagram of an authentication apparatus 1700 according to an illustrative embodiment, which may be applied to a second entity. As shown in Fig. 17, the apparatus 1700 may include:

[0479] a second receiving module 1701, configured to acquire an authentication result of a first proxy entity to a user equipment, where the authentication result includes a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with a target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an untrusted entity providing an application function outside a 3GPP operator domain, the first proxy entity includes a trusted entity providing an authentication function inside the 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

[0480] a second sending module 1702, configured to send the authentication result to the target entity to make the target entity communicate with the user equipment according to the authentication result.

[0481] Optionally, the second receiving module 1701 is configured to: receive a second notification message sent by the first proxy entity, where the second notification message is a message sent by the first proxy entity to the second entity according to the first authentication result in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain; and acquire the first authentication result according to the second notification message. The second sending module 1702 is configured to: send a fifth notification message to the target entity according to the first authentication result.

[0482] Optionally, in case that the second notification message includes a second identity of the subscriber corresponding to the user equipment, the second sending module 1702 is configured to: acquire a first identity of the subscriber corresponding to the user equipment according to the second identity of the subscriber; and send the fifth notification message to the target entity according to the first authentication result and the first identity of the subscriber.

[0483] Optionally, the first identity of the subscriber is a generic public subscription identifier GPSI corresponding to the user equipment; and the second identity of the subscriber includes a subscription permanent

identifier SUPI corresponding to the user equipment.

[0484] Optionally, the second receiving module 1701 is configured to: receive a fourth notification message sent by the first proxy entity, where the fourth notification message is a message sent by the first proxy entity to the second entity according to the second authentication result in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain; and acquire the second authentication result according to the second notification message. The second sending module 1702 is configured to: send a sixth notification message to the target entity according to the second authentication result.

[0485] Optionally, in case that the fourth notification message includes a second identity of the subscriber corresponding to the user equipment, the second sending module 1702 is configured to: acquire a first identity of the subscriber corresponding to the user equipment according to the second identity of the subscriber; and send the sixth notification message to the target entity according to the second authentication result and the first identity of the subscriber.

[0486] Optionally, the second entity includes: a network exposure function NEF entity or a service capability exposure function SCEF entity.

[0487] Fig. 18 is a block diagram of an authentication apparatus 1800 according to an illustrative embodiment, which may be applied to a third entity. As shown in Fig. 18, the apparatus 1800 may include:

[0488] a third receiving module 1801 configured to receive a second authority request parameter sent by a first proxy entity, where the second authority request parameter is configured to instruct the third entity to determine whether a user equipment has a first communication authority with a target entity, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity includes an entity providing an application function, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, the first proxy entity provides an authentication proxy function for the first entity, and the third entity includes an entity that provides AKMA authorization and application key derivation functions;

[0489] a third determining module 1802 configured to determine whether the user equipment has the first communication authority with the target entity according to the second authority request parameter;

[0490] a third key module 1803 configured to acquire first pending key information in case that the user equipment has the first communication authority with the target entity; and

[0491] a third sending module 1804 configured to send the first pending key information to the first proxy entity.

[0492] Optionally, the second authority request parameter includes a key identifier A-KID corresponding to the user equipment, a first target entity identifier of the target entity and a proxy entity identifier corresponding to the first proxy entity; and the third determining module 1802 is configured to determine whether the user equipment has the first communication authority with the target entity by one or more of: determining whether the user equipment has an access authority to the target entity according to the key identifier A-KID and the first target entity identifier; determining whether the user equipment has an access authority to the first proxy entity according to the key identifier A-KID and the proxy entity identifier; or determining whether the first proxy entity has a proxy authority to the target entity according to the proxy entity identity and the first target entity identity.

[0493] Optionally, the third key module 1803 is configured to acquire the first pending key information

according to entity key information corresponding to the target entity.

[0494] Optionally, the third receiving module 1801 is configured to: receive the second authority request parameter sent by the first proxy entity via a first key request message; and the first key request message is configured to instruct the third entity to acquire the first pending key information and an identity of the subscriber of the user equipment. The third sending module 1804 is configured to send the first pending key information to the first proxy entity via a first key response message.

[0495] Optionally, the third sending module 1804 is configured to send the first pending key information and a second identity of the subscriber corresponding to the user equipment to the first proxy entity via the first key response message in case that it is determined that the target entity has an acquisition authority to the identity of the subscriber.

[0496] Optionally, the second identity of the subscriber is a subscription permanent identifier SUPI corresponding to the user equipment.

[0497] Optionally, the third receiving module 1801 is configured to: receive the second authority request parameter sent by the first proxy entity via a second key request message; and the second key request message is configured to instruct the third entity to acquire the first pending key information. The third sending module 1804 is configured to: send the first pending key information to the first proxy entity via a second key response message.

[0498] Optionally, the third determining module 1802 is configured, after sending the first pending key information to the first proxy entity, to: receive a third authority request parameter sent by the first proxy entity; determine whether the user equipment has a second communication authority with the target entity according to the third authority request parameter; and send an authorization result parameter to the first proxy entity. The authorization result parameter is configured to notify the first proxy entity whether the user equipment has the second communication authority with the target entity.

[0499] Optionally, the third authority request parameter includes a key identifier A-KID, a second target entity identifier, and a proxy entity identifier corresponding to the first proxy entity, and the second target entity identifier is a protected entity identifier acquired by the user equipment according to a first target entity identifier of the target entity. The third determining module 1802 is configured to determine whether the user equipment has the second communication authority with the target entity by one or more of: determining whether the user equipment has an access authority to the target entity according to the key identifier A-KID and the second target entity identifier; or determining whether the first proxy entity has a proxy authority to the target entity according to the proxy entity identifier and the second target entity identifier.

[0500] Optionally, the third determining module 1802 is configured to: receive the third authority request parameter sent by the first proxy entity via a third key request message, where the third key request message is configured to instruct the third entity to acquire an authorization result parameter and an identity of the subscriber of the user equipment; and send the authorization result parameter to the first proxy entity via a third key response message.

[0501] Optionally, the third key request message further includes an authorization indication parameter, and the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the third key request message.

[0502] Optionally, the third determining module 1802 is configured to: send the authorization result parameter and a second identity of the subscriber corresponding to the user equipment to the first proxy entity via the third key response message in case that it is determined that the target entity has an acquisition authority to the identity of the subscriber.

[0503] Optionally, the second identity of the subscriber is a subscription permanent identifier SUPI corresponding to the user equipment.

[0504] Optionally, the third determining module 1802 is configured to: receive the third authority request parameter sent by the first proxy entity via a fourth key request message, where the fourth key request message is configured to instruct the third entity to acquire the authorization result parameter; and send the authorization result parameter to the first proxy entity via a fourth key response message.

[0505] Optionally, the third determining module 1802 is configured to: determine whether the third entity has an authority to serve the first proxy entity according to a first preset policy; and determine whether the user equipment has the second communication authority with the target entity according to the third authority request parameter in case that the third entity has the authority to serve the first proxy entity.

[0506] Optionally, the third determining module 1802 is configured to: determine whether the third entity has an authority to serve the first proxy entity according to a first preset policy; and determine whether the user equipment has the first communication authority with the target entity according to the second authority request parameter in case that the third entity has the authority to serve the first proxy entity.

[0507] Optionally, the first proxy entity includes a trusted authentication proxy AP entity inside the 3GPP operator domain; and the third entity includes: an AKMA anchor function AAnF entity.

[0508] Optionally, the first entity includes: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

[0509] Fig. 19 is a block diagram of an authentication apparatus 1900 according to an illustrative embodiment, which may be applied to a first entity. As shown in Fig. 19, the apparatus 1900 may further include: a first communication module 1901 configured to: acquire an authentication result of a first proxy entity to a user equipment; and communicate with the user equipment according to the authentication result. The authentication result includes a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with the target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the first entity includes an entity providing an application function, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first proxy entity includes a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity

[0510] Optionally, the first communication module 1901 is configured to: receive a first notification message sent by the first proxy entity, where the first notification message includes the first authentication result; or receive a third notification message sent by the first proxy entity, where the third notification message includes the second authentication result, in case that the target entity is a trusted entity providing the application

function inside the 3GPP operator domain.

[0511] Optionally, the first notification message or the third notification message further includes a second identity of the subscriber corresponding to the user equipment.

[0512] Optionally, the second identity of the subscriber includes a subscription permanent identifier SUPI corresponding to the user equipment.

[0513] Optionally, the first communication module 1901 is configured to: receive a fifth notification message sent by a second entity, where the fifth notification message includes the first authentication result, and the fifth notification message is a message sent by the second entity in response to receiving a second notification message; or receive a sixth notification message sent by the second entity, where the sixth notification message includes the second authentication result, and the fifth notification message is a message sent by the second entity in response to receiving a fourth notification message, in case that the target entity is an untrusted entity providing the application function outside the 3GPP operator domain.

[0514] Optionally, the fifth notification message or the sixth notification message further includes a first identity of the subscriber of the user equipment.

[0515] Optionally, the first identity of the subscriber is a generic public subscription identifier GPSI corresponding to the user equipment.

[0516] Optionally, the first proxy entity includes a trusted authentication proxy AP entity inside the 3GPP operator domain.

[0517] Optionally, the first entity includes: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

[0518] With regard to the apparatuses in the above embodiments, the specific way in which each module performs operations has been described in detail in the embodiments of the methods, and will not be described in detail here.

[0519] Fig. 20 is a block diagram of an authentication apparatus according to an illustrative embodiment. For example, the authentication apparatus 2000 may be a terminal device, such as a mobile phone, a computer, a digital broadcasting terminal, a messaging device, a game console, a tablet device, a medical device, a fitness device, a personal digital assistant, etc. The authentication apparatus 2000 may also be a server, such as a local server or a cloud server. The authentication apparatus 2000 may also be the user equipment shown in Fig. 1, and the authentication apparatus 2000 may also be any network entity in the communication system shown in Fig. 1, such as the first entity, the first proxy entity, the second entity or the third entity.

[0520] Referring to Fig. 20, the apparatus 2000 may include one or more of the following components: a processing component 2002, a memory 2004, and a communication component 2006.

[0521] The processing component 2002 generally controls the overall operation of the apparatus 2000, such as operations associated with display, telephone call, data communication, camera operation and recording operation. The processing component 2002 may include one or more processors 2020 to execute instructions so as to complete all or part of the steps of the authentication methods described above. In addition, the processing component 2002 may include one or more modules to facilitate the interaction between the processing component 2002 and other components. For example, the processing component 2002 may include a multimedia

module to facilitate the interaction between the multimedia component and the processing component 2002.

[0522] The memory 2004 is configured to store various types of data to support operations in the apparatus 2000. Examples of these data include instructions for any application or method operating on the apparatus 2000, contact data, phone book data, messages, pictures, videos, and the like. The memory 2004 may be realized by any type of volatile or nonvolatile memory device or their combination, such as a static random access memory (SRAM), an electrically erasable programmable read-only memory (EEPROM), an erasable programmable read-only memory (EPROM), a programmable read-only memory (PROM), a read-only memory (ROM), a magnetic memory, a flash memory, a magnetic disk or an optical disk.

[0523] The communication component 2006 is configured to facilitate wired or wireless communication between the apparatus 2000 and other devices. The apparatus 2000 can access a wireless network based on communication standards, such as WiFi, 2G or 3G, or a combination thereof. In an illustrative embodiment, the communication component 2006 receives a broadcast signal or broadcast related information from an external broadcast management system via a broadcast channel. In an illustrative embodiment, the communication component 2006 further includes a near field communication (NFC) module to facilitate short-range communication. For example, the NFC module can be implemented based on the radio frequency identification (RFID) technology, the infrared data association (IrDA) technology, the ultra-wideband (UWB) technology, the Bluetooth (BT) technology and other technologies.

[0524] In an illustrative embodiment, the apparatus 2000 may be implemented by one or more application-specific integrated circuits (ASIC), digital signal processors (DSP), digital signal processing devices (DSPD), programmable logic devices (PLD), field programmable gate arrays (FPGA), controllers, microcontrollers, microprocessors or other electronic components, for performing the above authentication methods.

[0525] Besides as an independent electronic device, the apparatus 2000 may also be a part of an independent electronic device. For example, in an embodiment, the electronic device may be an Integrated Circuit (IC) or a chip, where the integrated circuit may be one IC or a collection of a plurality of ICs. The chip may include, but is not limited to, the following types: a Graphics Processing Unit (GPU), Central Processing Unit (CPU), a Field Programmable Gate Array (FPGA), a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a System on Chip (SOC), etc. The integrated circuit or chip may be used to execute executable instructions (or codes) to realize the authentication methods. The executable instructions may be stored in the integrated circuit or chip, and may also be acquired from other devices or apparatuses. For example, the integrated circuit or chip includes a processor, a memory, and an interface for communicating with other devices. The executable instruction may be stored in the processor, and when the executable instructions are executed by the processor, the above authentication methods are realized. Alternatively, the integrated circuit or chip can receive the executable instructions through the interface and transmit them to the processor for execution, so as to realize the above authentication methods.

[0526] In an illustrative embodiment, there is also provided a non-transitory computer-readable storage medium including instructions, such as the memory 2004 including instructions, and the instructions may be executed by the processor 2020 of the apparatus 2000 to complete the above authentication methods. For example, the non-transitory computer-readable storage medium can be a ROM, a random access memory (RAM), a CD-ROM, a magnetic tape, a floppy disk, an optical data storage device, etc.

[0527] In another illustrative embodiment, there is also provided a computer program product including a computer program executable by a programmable device, and the computer program has code portions for executing the above authentication methods when executed by the programmable device.

[0528] Other embodiments of the present disclosure will easily occur to those skilled in the art after considering the specification and practicing the present disclosure. The present disclosure is intended to cover any variations, uses or adaptations of the present disclosure, which follow the general principles of the present disclosure and include common sense or common technical means in the related art that are not disclosed in the present disclosure. The specification and embodiments are to be regarded as illustrative only, with the true scope and spirit of the present disclosure being indicated by the following claims.

[0529] It should be understood that the present disclosure is not limited to the precise structure described above and shown in the drawings, and various modifications and changes can be made without departing from the scope of the present disclosure. The scope of the present disclosure is limited only by the appended claims.

WHAT IS CLAIMED IS:

1. An authentication method, applied to a user equipment, comprising:
 - determining, from one or more first entities, a target entity with which communication is requested;
 - determining a first authority request parameter according to the target entity;
 - sending an application session establishment request message to a first proxy entity according to the first authority request parameter; wherein the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with the target entity according to the first authority request parameter; the first entity comprises an entity providing an application function, the first proxy entity comprises a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;
 - determining whether the user equipment has the first communication authority with the target entity in response to receiving an application session establishment response message sent by the first proxy entity; and
 - in case that the user equipment has the first communication authority with the target entity, performing authentication through the first proxy entity.
2. The method according to claim 1, wherein determining the first authority request parameter according to the target entity comprises:
 - taking a first target entity identifier of the target entity and a key identifier A-KID corresponding to the user equipment as the first authority request parameter.
3. The method according to claim 1, wherein the first communication authority comprises one or more of:
 - the user equipment having an access authority to the target entity;
 - the user equipment having an access authority to the first proxy entity;
 - the first proxy entity having a proxy authority to the target entity; or
 - the target entity having an acquisition authority to an identity of the subscriber of the user equipment.
4. The method according to claim 1, wherein after the authentication through the first proxy entity is successful, the method further comprises:
 - establishing a secure session with the first proxy entity;
 - acquiring a proxy domain name of the first proxy entity and a first domain name of the target entity;
 - determining whether the user equipment has a second communication authority with the target entity through the secure session in case that the proxy domain name is the same as the first domain name; and
 - communicating with the target entity in case that it is determined that the user equipment has the second communication authority with the target entity.
5. The method according to claim 4, wherein determining whether the user equipment has the second communication authority with the target entity through the secure session comprises:
 - sending a target entity service request message to the first proxy entity through the secure session; wherein the target entity service request message comprises a second target entity identifier, the second target entity

identifier is a protected entity identifier acquired by the user equipment according to the first target entity identifier, and the target entity service request message is configured to instruct the first proxy entity to determine whether the user equipment has the second communication authority with the target entity according to the second target entity identifier; and

determining whether the user equipment has the second communication authority with the target entity in response to receiving a target entity service response message sent by the first proxy entity.

6. The method according to claim 4, wherein the second communication authority comprises one or more of:

the user equipment having an access authority to the target entity;

the first proxy entity having a proxy authority to the target entity; or

the target entity having an acquisition authority to an identity of the subscriber of the user equipment.

7. The method according to claim 1, wherein determining whether the user equipment has the first communication authority with the target entity in response to receiving the application session establishment response message sent by the first proxy entity comprises:

determining that the user equipment has the first communication authority with the target entity in case that the application session establishment response message is received; or

determining that the user equipment has the first communication authority with the target entity, in case that the application session establishment response message is received and the session establishment response message comprises success indication information.

8. The method according to any one of claims 1 to 7, wherein the first proxy entity comprises a trusted authentication proxy AP entity inside the 3GPP operator domain.

9. The method according to claim 8, wherein the first entity comprises a trusted entity providing an application function inside the 3GPP operator domain.

10. The method according to claim 9, wherein the first entity comprises: a trusted application function AF entity inside the 3GPP operator domain, or a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain.

11. The method according to claim 8, wherein the first entity comprises an untrusted entity providing an application function outside the 3GPP operator domain, the first proxy entity communicates with the first entity through a second entity; and the second entity comprises an entity providing a network exposure function.

12. The method according to claim 11, wherein the first entity comprises: an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS outside the 3GPP operator domain.

13. The method according to claim 11, wherein the second entity comprises: a network exposure function NEF entity or a service capability exposure function SCEF entity.

14. An authentication method, applied to a first proxy entity, comprising:
receiving an application session establishment request message sent by a user equipment; wherein the application session establishment request message comprises a first authority request parameter, the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with a target entity according to the first authority request parameter, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity comprises an entity providing an application function, the first proxy entity comprises a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;
determining whether the user equipment has the first communication authority with the target entity according to the first authority request parameter; and
in case that the user equipment has the first communication authority with the target entity, sending an application session establishment response message to the user equipment, and performing authentication of the user equipment.

15. The method according to claim 14, wherein the first authority request parameter comprises a first target entity identifier of the target entity and a key identifier A-KID corresponding to the user equipment.

16. The method according to claim 14, wherein the first communication authority comprises one or more of:
the user equipment having an access authority to the target entity;
the user equipment having an access authority to the first proxy entity;
the first proxy entity having a proxy authority to the target entity; or
the target entity having an acquisition authority to an identity of the subscriber of the user equipment.

17. The method according to claim 14, wherein determining whether the user equipment has the first communication authority with the target entity according to the first authority request parameter comprises:
determining a second authority request parameter according to the first authority request parameter;
sending the second authority request parameter to a third entity; wherein the third entity comprises an entity that provides AKMA authorization and application key derivation functions; and the second authority request parameter is configured to instruct the third entity to determine whether the user equipment has the first communication authority with the target entity;
acquiring first pending key information sent by the third entity, wherein the first pending key information is key information acquired by the third entity according to the second authority request parameter; and
determining whether the user equipment has the first communication authority with the target entity according to the first pending key information.

18. The method according to claim 17, wherein determining the second authority request parameter according to the first authority request parameter comprises:

taking the first authority request parameter and a proxy entity identifier corresponding to the first proxy entity as the second authority request parameter.

19. The method according to claim 17, wherein sending the second authority request parameter to the third entity comprises:

sending the second authority request parameter to the third entity via a first key request message; wherein the first key request message is configured to instruct the third entity to acquire the first pending key information and an identity of the subscriber of the user equipment;

wherein acquiring the first pending key information sent by the third entity comprises:

receiving a first key response message sent by the third entity; and

acquiring the first pending key information comprised in the first key response message.

20. The method according to claim 19, wherein the first key response message further comprises a second identity of the subscriber corresponding to the user equipment, and the method further comprises:

acquiring the second identity of the subscriber according to the first key response message received.

21. The method according to claim 20, wherein the second identity of the subscriber comprises a subscription permanent identifier SUPI corresponding to the user equipment.

22. The method according to claim 17, wherein sending the second authority request parameter to the third entity comprises:

sending the second authority request parameter to the third entity via a second key request message; wherein the second key request message is configured to indicate that the first proxy entity requests to acquire the first pending key information;

wherein acquiring the first pending key information sent by the third entity comprises:

receiving a second key response message sent by the third entity; and

acquiring the first pending key information comprised in the second key response message.

23. The method according to claim 17, wherein determining whether the user equipment has the first communication authority with the target entity according to the first pending key information comprises:

determining that the user equipment has the first communication authority with the target entity in case that the first pending key information comprises entity key information corresponding to the target entity.

24. The method according to claim 17, wherein in case that the authentication of the user equipment is successful, the method further comprises:

notifying the target entity of a first authentication result of the authentication.

25. The method according to claim 24, wherein notifying the target entity of the first authentication result

comprises:

acquiring a proxy domain name of the first proxy entity and a first domain name of the target entity; and
notifying the target entity of the first authentication result in case that the proxy domain name is different from the first domain name.

25. The method according to claim 24, wherein in case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain, notifying the target entity of the first authentication result comprises:

sending a first notification message to the target entity, wherein the first notification message comprises the first authentication result.

26. The method according to claim 25, wherein in case that the first proxy entity acquires a second identity of the subscriber of the user equipment, the first notification message further comprises the second identity of the subscriber.

27. The method according to claim 24, wherein in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain, notifying the target entity of the first authentication result comprises:

sending a second notification message to a second entity according to the first authentication result to instruct the second entity to send the first authentication result to the target entity.

28. The method according to claim 27, wherein in case that the first proxy entity acquires a second identity of the subscriber of the user equipment, the second notification message further comprises the second identity of the subscriber.

29. The method according to claim 14, wherein after the authentication of the user equipment is successful, the method further comprises:

establishing a secure session with the user equipment;

receiving, through the secure session, a target entity service request message sent by the user equipment; wherein the target entity service request message comprises a second target entity identifier, the second target entity identifier is a protected entity identifier acquired by the user equipment according to a first target entity identifier of the target entity, and the target entity service request message is a message sent by the user equipment in case that it is determined that a proxy domain name of the first proxy entity is the same as a first domain name of the target entity;

determining whether the user equipment has a second communication authority with the target entity according to the second target entity identifier; and

sending a target entity service response message to the user equipment; wherein the target entity service response message is configured to indicate whether the user equipment has the second communication authority with the target entity.

30. The method according to claim 29, wherein the second communication authority comprises one or more of:

- the user equipment having an access authority to the target entity;
- the first proxy entity having a proxy authority to the target entity; or
- the target entity having an acquisition authority to an identity of the subscriber of the user equipment.

31. The method according to claim 29, wherein determining whether the user equipment has the second communication authority with the target entity according to the second target entity identifier comprises:

determining that the user equipment has the second communication authority with the target entity in case that the second target entity identifier is the same as the first target entity identifier.

32. The method according to claim 29, wherein determining whether the user equipment has the second communication authority with the target entity according to the second target entity identifier comprises:

determining a third authority request parameter according to the second target entity identifier in case that the second target entity identifier is different from the first target entity identifier;

sending the third authority request parameter to a third entity; wherein the third authority request parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity;

acquiring an authorization result parameter sent by the third entity; wherein the authorization result parameter is configured to indicate whether the user equipment has the second communication authority with the target entity; and

determining whether the user equipment has the second communication authority with the target entity according to the authorization result parameter.

33. The method according to claim 32, wherein determining the third authority request parameter according to the second target entity identifier comprises:

taking the second target entity identifier, a key identifier A-KID corresponding to the user equipment, and a proxy entity identifier corresponding to the first proxy entity as the third authority request parameter.

34. The method according to claim 32, wherein sending the third authority request parameter to the third entity comprises:

sending the third authority request parameter to the third entity via a third key request message; wherein the third key request message is configured to instruct the third entity to acquire the authorization result parameter and an identity of the subscriber of the user equipment;

- wherein acquiring the authorization result parameter sent by the third entity comprises:
- receiving a third key response message sent by the third entity; and
- acquiring the authorization result parameter comprised in the third key response message.

35. The method according to claim 34, wherein the third key response message further comprises a second identity of the subscriber corresponding to the user equipment, and the method further comprises:

acquiring the second identity of the subscriber according to the third key response message received.

36. The method according to claim 34, wherein the third key request message further comprises an authorization indication parameter, and the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the third key request message.

37. The method according to claim 33, wherein sending the third authority request parameter to the third entity comprises:

sending the third authority request parameter to the third entity via a fourth key request message; wherein the fourth key request message is configured to indicate that the first proxy entity requests to acquire the authorization result parameter;

wherein acquiring the authorization result parameter sent by the third entity comprises:

receiving a fourth key response message sent by the third entity; and

acquiring the authorization result parameter comprised in the fourth key response message.

38. The method according to claim 37, wherein the fourth key request message further comprises an authorization indication parameter, the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the fourth key request message.

39. The method according to claim 31, wherein in case that it is determined according to an authorization result parameter that the user equipment has the second communication authority with the target entity, the method further comprises:

notifying the target entity of a second authentication result; wherein the second authentication result is configured to indicate that the target entity has a communication authority with the target entity.

40. The method according to claim 39, wherein in case that the target entity is a trusted entity providing an application function inside the 3GPP operator domain, notifying the target entity of the second authentication result comprises:

sending a third notification message to the target entity, wherein the third notification message comprises the second authentication result.

41. The method according to claim 40, wherein in case that the first proxy entity acquires a second identity of the subscriber of the user equipment, the third notification message further comprises the second identity of the subscriber.

42. The method according to claim 39, wherein in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain, notifying the target entity of the second authentication result comprises:

sending a fourth notification message to a second entity according to a first authentication result to instruct the second entity to send the first authentication result to the target entity.

43. The method according to claim 43, wherein in case that the first proxy entity acquires a second identity of the subscriber of the user equipment, the fourth notification message further comprises the second identity of the subscriber.

44. The method according to claim 17, wherein the first pending key information comprises an application key K_{AF} and a key expiration time.

45. The method according to claim 17, wherein a second entity comprises a network exposure function NEF entity or a service capability exposure function SCEF entity.

46. The method according to any one of claims 14 to 45, wherein the first proxy entity comprises a trusted authentication proxy AP entity inside the 3GPP operator domain.

47. The method according to any one of claims 14 to 45, wherein the first entity comprises: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

48. An authentication method, applied to a third entity, comprising:

receiving a second authority request parameter sent by a first proxy entity; wherein the second authority request parameter is configured to instruct the third entity to determine whether a user equipment has a first communication authority with a target entity, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity comprises an entity providing an application function, the first proxy entity comprises a trusted entity providing an authentication function inside a 3GPP operator domain, the first proxy entity provides an authentication proxy function for the first entity, and the third entity comprises an entity that provides AKMA authorization and application key derivation functions;

determining whether the user equipment has the first communication authority with the target entity according to the second authority request parameter;

acquiring first pending key information in case that the user equipment has the first communication authority with the target entity; and

sending the first pending key information to the first proxy entity.

49. The method according to claim 48, wherein the second authority request parameter comprises a key identifier A-KID corresponding to the user equipment, a first target entity identifier of the target entity and a proxy entity identifier corresponding to the first proxy entity; wherein determining whether the user equipment

has the first communication authority with the target entity according to the second authority request parameter comprises one or more of:

- determining whether the user equipment has an access authority to the target entity according to the key identifier A-KID and the first target entity identifier;

- determining whether the user equipment has an access authority to the first proxy entity according to the key identifier A-KID and the proxy entity identifier;

- determining whether the first proxy entity has a proxy authority to the target entity according to the proxy entity identity and the first target entity identity; or

- determining whether the target entity has an acquisition authority to an identity of the subscriber of the user equipment according to the key identifier A-KID and the first target entity identifier.

50. The method according to claim 48, wherein acquiring the first pending key information comprises:
acquiring the first pending key information according to entity key information corresponding to the target entity.

51. The method according to claim 48, wherein receiving the second authority request parameter sent by the first proxy entity comprises:

- receiving the second authority request parameter sent by the first proxy entity via a first key request message; wherein the first key request message is configured to instruct the third entity to acquire the first pending key information and an identity of the subscriber of the user equipment; and

- wherein sending the first pending key information to the first proxy entity comprises:

- sending the first pending key information to the first proxy entity via a first key response message.

52. The method according to claim 51, wherein sending the first pending key information to the first proxy entity via the first key response message comprises:

- sending the first pending key information and a second identity of the subscriber corresponding to the user equipment to the first proxy entity via the first key response message in case that it is determined that the target entity has an acquisition authority to the identity of the subscriber.

53. The method according to claim 52, wherein the second identity of the subscriber is a subscription permanent identifier SUPI corresponding to the user equipment.

54. The method according to claim 48, wherein receiving the second authority request parameter sent by the first proxy entity comprises:

- receiving the second authority request parameter sent by the first proxy entity via a second key request message; wherein the second key request message is configured to instruct the third entity to acquire the first pending key information; and

- wherein sending the first pending key information to the first proxy entity comprises:

- sending the first pending key information to the first proxy entity via a second key response message.

55. The method according to claim 48, wherein after sending the first pending key information to the first proxy entity, the method further comprises:

receiving a third authority request parameter sent by the first proxy entity;

determining whether the user equipment has a second communication authority with the target entity according to the third authority request parameter; and

sending an authorization result parameter to the first proxy entity; wherein the authorization result parameter is configured to notify the first proxy entity whether the user equipment has the second communication authority with the target entity.

56. The method according to claim 55, wherein the third authority request parameter comprises a key identifier A-KID, a second target entity identifier, and a proxy entity identifier corresponding to the first proxy entity, wherein the second target entity identifier is a protected entity identifier acquired by the user equipment according to a first target entity identifier of the target entity, and

wherein determining whether the user equipment has the second communication authority with the target entity according to the third authority request parameter comprises one or more of:

determining whether the user equipment has an access authority to the target entity according to the key identifier A-KID and the second target entity identifier;

determining whether the first proxy entity has a proxy authority to the target entity according to the proxy entity identifier and the second target entity identifier; or

determining whether the target entity has an acquisition authority to an identity of the subscriber of the user equipment according to the key identifier A-KID and the second target entity identifier.

57. The method according to claim 53, wherein receiving the third authority request parameter sent by the first proxy entity comprises:

receiving the third authority request parameter sent by the first proxy entity via a third key request message; wherein the third key request message is configured to instruct the third entity to acquire an authorization result parameter and an identity of the subscriber of the user equipment;

wherein sending the authorization result parameter to the first proxy entity comprises:

sending the authorization result parameter to the first proxy entity via a third key response message.

58. The method according to claim 57, wherein the third key request message further comprises an authorization indication parameter, and the authorization indication parameter is configured to instruct the third entity to determine whether the user equipment has the second communication authority with the target entity according to the third key request message.

59. The method according to claim 57, wherein sending the authorization result parameter to the first proxy entity via the third key response message comprises:

sending the authorization result parameter and a second identity of the subscriber corresponding to the user equipment to the first proxy entity via the third key response message in case that it is determined that the target entity has an acquisition authority to the identity of the subscriber.

60. The method according to claim 59, wherein the second identity of the subscriber is a subscription permanent identifier SUPI corresponding to the user equipment.

61. The method according to claim 53, wherein receiving the third authority request parameter sent by the first proxy entity comprises:

receiving the third authority request parameter sent by the first proxy entity via a fourth key request message; wherein the fourth key request message is configured to instruct the third entity to acquire the authorization result parameter;

wherein sending the authorization result parameter to the first proxy entity comprises:

sending the authorization result parameter to the first proxy entity via a fourth key response message.

62. The method according to claim 55, wherein before determining whether the user equipment has the second communication authority with the target entity according to the third authority request parameter, the method further comprises:

determining whether the third entity has an authority to serve the first proxy entity according to a first preset policy; and

wherein determining whether the user equipment has the second communication authority with the target entity according to the third authority request parameter comprises:

determining whether the user equipment has the second communication authority with the target entity according to the third authority request parameter in case that the third entity has the authority to serve the first proxy entity.

63. The method according to claim 48, wherein before determining whether the user equipment has the first communication authority with the target entity according to the second authority request parameter, the method further comprises:

determining whether the third entity has an authority to serve the first proxy entity according to a first preset policy; and

wherein determining whether the user equipment has the first communication authority with the target entity according to the second authority request parameter comprises:

determining whether the user equipment has the first communication authority with the target entity according to the second authority request parameter in case that the third entity has the authority to serve the first proxy entity.

64. The method according to any one of claims 48 to 63, wherein the first proxy entity comprises a trusted authentication proxy AP entity inside the 3GPP operator domain; and the third entity comprises: an AKMA anchor function AAnF entity.

65. The method according to any one of claims 48 to 63, wherein the first entity comprises: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server

SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

66. An authentication method, applied to a target entity in one or more first entities, comprising:

acquiring an authentication result of a first proxy entity to a user equipment, wherein the authentication result comprises a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with the target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the first entity comprises an entity providing an application function, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first proxy entity comprises a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

communicating with the user equipment according to the authentication result.

67. The method according to claim 66, wherein in case that the target entity is a trusted entity providing the application function inside the 3GPP operator domain, acquiring the authentication result of the first proxy entity to the user equipment comprises:

receiving a first notification message sent by the first proxy entity, wherein the first notification message comprises the first authentication result; or

receiving a third notification message sent by the first proxy entity, wherein the third notification message comprises the second authentication result.

68. The method according to claim 67, wherein the first notification message or the third notification message further comprises a second identity of the subscriber corresponding to the user equipment.

69. The method according to claim 68, wherein the second identity of the subscriber comprises a subscription permanent identifier SUPI corresponding to the user equipment.

70. The method according to claim 66, wherein in case that the target entity is an untrusted entity providing the application function outside the 3GPP operator domain, acquiring the authentication result of the first proxy entity to the user equipment comprises:

receiving a fifth notification message sent by a second entity; wherein the fifth notification message comprises the first authentication result, and the fifth notification message is a message sent by the second entity in response to receiving a second notification message; or

receiving a sixth notification message sent by the second entity; wherein the sixth notification message comprises the second authentication result, and the fifth notification message is a message sent by the second entity in response to receiving a fourth notification message.

71. The method according to claim 70, wherein the fifth notification message or the sixth notification message further comprises a first identity of the subscriber of the user equipment.

72. The method according to claim 71, wherein the first identity of the subscriber is a generic public subscription identifier GPSI corresponding to the user equipment.

73. The method according to any one of claims 66 to 72, wherein the first proxy entity comprises a trusted authentication proxy AP entity inside the 3GPP operator domain.

74. The method according to any one of claims 66 to 72, wherein the first entity comprises: a trusted application function AF entity inside the 3GPP operator domain, a trusted service capability server SCS/application server AS entity inside the 3GPP operator domain, an untrusted application function AF entity outside the 3GPP operator domain, or an untrusted service capability server SCS/application server AS entity outside the 3GPP operator domain.

75. An authentication method, applied to a second entity, comprising:

acquiring an authentication result of a first proxy entity to a user equipment; wherein the authentication result comprises a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with a target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity comprises an untrusted entity providing an application function outside a 3GPP operator domain, the first proxy entity comprises a trusted entity providing an authentication function inside the 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

sending the authentication result to the target entity to make the target entity communicate with the user equipment according to the authentication result.

76. The method according to claim 75, wherein acquiring the authentication result of the first proxy entity to the user equipment comprises:

receiving a second notification message sent by the first proxy entity; wherein the second notification message is a message sent by the first proxy entity to the second entity according to the first authentication result in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain; and

acquiring the first authentication result according to the second notification message;

wherein sending the authentication result to the target entity comprises:

sending a fifth notification message to the target entity according to the first authentication result.

77. The method according to claim 76, wherein in case that the second notification message comprises a second identity of the subscriber corresponding to the user equipment, sending the fifth notification message to

the target entity according to the first authentication result comprises:

- acquiring a first identity of the subscriber corresponding to the user equipment according to the second identity of the subscriber; and

- sending the fifth notification message to the target entity according to the first authentication result and the first identity of the subscriber.

78. The method according to claim 77, wherein the first identity of the subscriber is a generic public subscription identifier GPSI corresponding to the user equipment; and the second identity of the subscriber comprises a subscription permanent identifier SUPI corresponding to the user equipment.

79. The method according to claim 75, wherein acquiring the authentication result of the first proxy entity to the user equipment comprises:

- receiving a fourth notification message sent by the first proxy entity; wherein the fourth notification message is a message sent by the first proxy entity to the second entity according to the second authentication result in case that the target entity is an untrusted entity providing an application function outside the 3GPP operator domain; and

- acquiring the second authentication result according to the second notification message;

- wherein sending the authentication result to the target entity comprises:

- sending a sixth notification message to the target entity according to the second authentication result.

80. The method according to claim 79, wherein in case that the fourth notification message comprises a second identity of the subscriber corresponding to the user equipment, sending the sixth notification message to the target entity according to the second authentication result comprises:

- acquiring a first identity of the subscriber corresponding to the user equipment according to the second identity of the subscriber; and

- sending the sixth notification message to the target entity according to the second authentication result and the first identity of the subscriber.

81. The method according to any one of claims 66 to 80, wherein the second entity comprises: a network exposure function NEF entity or a service capability exposure function SCEF entity.

82. An authentication apparatus, applied to a user equipment, comprising:

- a target entity determining module configured to determine, from one or more first entities, a target entity with which communication is requested;

- a parameter determining module configured to determine a first authority request parameter according to the target entity;

- a first message sending module configured to send an application session establishment request message to a first proxy entity according to the first authority request parameter; wherein the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with the target entity according to the first authority request

parameter; the first entity comprises an entity providing an application function, the first proxy entity comprises a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;

- a first message receiving module configured to determine whether the user equipment has the first communication authority with the target entity in response to receiving an application session establishment response message sent by the first proxy entity; and

- an authentication module configured to perform authentication through the first proxy entity in case that the user equipment has the first communication authority with the target entity.

83. An authentication apparatus, applied to a first proxy entity, comprising:

- a first proxy receiving module configured to receive an application session establishment request message sent by a user equipment; wherein the application session establishment request message comprises a first authority request parameter, the application session establishment request message is configured to instruct the first proxy entity to determine whether the user equipment has a first communication authority with a target entity according to the first authority request parameter, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity comprises an entity providing an application function, the first proxy entity comprises a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity;

- a first proxy determining module configured to determine whether the user equipment has the first communication authority with the target entity according to the first authority request parameter; and

- a first proxy sending module configured to send an application session establishment response message to the user equipment, and perform authentication of the user equipment in case that the user equipment has the first communication authority with the target entity.

84. An authentication apparatus, applied to a third entity, comprising:

- a third receiving module configured to receive a second authority request parameter sent by a first proxy entity; wherein the second authority request parameter is configured to instruct the third entity to determine whether a user equipment has a first communication authority with a target entity, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity comprises an entity providing an application function, the first proxy entity comprises a trusted entity providing an authentication function inside a 3GPP operator domain, the first proxy entity provides an authentication proxy function for the first entity, and the third entity comprises an entity that provides AKMA authorization and application key derivation functions;

- a third determining module configured to determine whether the user equipment has the first communication authority with the target entity according to the second authority request parameter;

- a third key module configured to acquire first pending key information in case that the user equipment has the first communication authority with the target entity; and

- a third sending module configured to send the first pending key information to the first proxy entity.

85. An authentication apparatus, applied to a target entity in one or more first entities, comprising: a first communication module configured to:

acquire an authentication result of a first proxy entity to a user equipment, wherein the authentication result comprises a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with the target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the first entity comprises an entity providing an application function, the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first proxy entity comprises a trusted entity providing an authentication function inside a 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

communicate with the user equipment according to the authentication result.

86. An authentication apparatus, applied to a second entity, comprising:

a second receiving module configured to acquire an authentication result of a first proxy entity to a user equipment; wherein the authentication result comprises a first authentication result or a second authentication result, the first authentication result is configured to indicate that the user equipment has a first communication authority with a target entity; the second authentication result is configured to indicate that the user equipment has a second communication authority with the target entity; the target entity is an entity which is determined by the user equipment from one or more first entities and with which communication is requested, the first entity comprises an untrusted entity providing an application function outside a 3GPP operator domain, the first proxy entity comprises a trusted entity providing an authentication function inside the 3GPP operator domain, and the first proxy entity provides an authentication proxy function for the first entity; and

a second sending module configured to send the authentication result to the target entity to make the target entity communicate with the user equipment according to the authentication result.

87. An authentication apparatus, comprising:

a processor; and

a memory for storing instructions executable by the processor;

wherein the processor is configured to perform the steps of the method according to any one of claims 1 to 13, or the processor is configured to perform the steps of the method according to any one of claims 14 to 47, or the processor is configured to perform the steps of the method according to any one of claims 48 to 65, or the processor is configured to perform the steps of the method according to any one of claims 66 to 74, or the processor is configured to perform the steps of the method according to any one of claims 75 to 81.

88. A computer-readable storage medium, having stored therein computer program instructions that, when executed by a processor, cause the steps of the method according to any one of claims 1 to 13, or the steps of the method according to any one of claims 14 to 47, or the steps of the method according to any one of claims 48 to 65, or the steps of the method according to any one of claims 66 to 74, or the steps of the method according to any one of claims 75 to 81 to be implemented.

89. A chip, comprising a processor and an interface, wherein the processor is configured to read instructions to perform the steps of the method according to any one of claims 1 to 13, or the processor is configured to read instructions to perform the steps of the method according to any one of claims 14 to 47, or the processor is configured to read instructions to perform the steps of the method according to any one of claims 48 to 65, or the processor is configured to read instructions to perform the steps of the method according to any one of claims 66 to 74, or the processor is configured to read instructions to perform the steps of the method according to any one of claims 75 to 81.