SECURITY CONTEXT OBTAINING METHOD AND APPARATUS, AND COMMUNICATIONS SYSTEM

TECHNICAL FIELD

[0001] The present invention relates to the communications field, and more specifically, to a security context obtaining method and apparatus, and a communications system.

BACKGROUND

[0002] In a 5th generation (5th generation, 5G) communication scenario, because of movement of user equipment, a network device serving the user equipment changes. In a possible handover scenario, the user equipment is handed over from a 4th generation (4th generation, 4G) communications system to a 5G communications system. In this handover scenario, the user equipment is handed over from a 4G access network device to a 5G access network device, and from a 4G core network device to a 5G core network device. The handover between the core network devices includes handover between core network elements that provide a mobility management service for the user equipment, in other words, handover from a mobility management entity (mobility management entity, MME) in the 4G communications system to an access and mobility management function (access and mobility management function, AMF) in the 5G communications system.

[0003] In an existing scenario in which the user equipment is handed over from the 4G communications system to the 5G communications system, in addition to an AMF (a first AMF) selected by an MME, the 5G communications system further includes an AMF (a second AMF) that stores a security context of the user equipment. In this case, how the first AMF obtains the security context of the user equipment from the second AMF becomes an urgent problem to be resolved.

SUMMARY

[0004] This application provides a security context obtaining method and apparatus, and a communications system. A second registration request message sent by a first AMF to a second AMF is integrity protected based on a native security context between user equipment and the second AMF, so that the second AMF can validate integrity of the second registration request message based on the native security context between the user equipment and the second AMF, to improve a possibility that the second AMF successfully validates the second registration request message. If the validation is successful, the first AMF can successfully obtain a security context of the user equipment from the second AMF.

[0005] According to a first aspect, a security context obtaining method is provided. The method includes: A first access and mobility management function AMF receives a first registration request message sent by user equipment, where the first registration request message carries a second registration request message, the second registration request message is integrity protected using a first security context, the first security context is a native security context between the user equipment and a second AMF, and the first AMF is an AMF providing an access and mobility management service for the user equipment after the user equipment is handed over from a 4G communications system to a 5G communications system. The first AMF sends the second registration request message to the second AMF. The second AMF validates integrity of the second registration request message. If the second AMF successfully validates the integrity of the second registration request message, the second AMF sends a security context of the user equipment to the first AMF.

[0006] According to the security context obtaining method provided in this embodiment of this application, when the user equipment is handed over from the 4G communications system to the 5G communications system, the security context of the user equipment is stored by the user equipment and the second AMF before the handover. After the user equipment is handed over from the 4G communications system to the 5G communications system, the first AMF provides the access and mobility management service for the user equipment. The first AMF needs to obtain the security context of the user equipment from the second AMF. Specifically, after receiving a

handover command, the user equipment may perform integrity protection on a fourth registration request message based on the natively stored security context between the user equipment and the second AMF, generate the second registration request message, add the second registration request message to the first registration request message, and send the first registration request message to the first AMF. In this way, the first AMF may forward the second registration request message to the second AMF, and the second AMF may validate the integrity of the second registration request message. After successfully validating the integrity of the second registration request message, the second AMF may return the security context of the user equipment to the first AMF. This can improve a possibility that the first AMF successfully obtains the security context of the user equipment from the second AMF.

[0007] With reference to the first aspect, in some implementations of the first aspect, the security context of the user equipment includes: the first security context, or a second security context obtained based on the first security context.

[0008] According to the security context obtaining method provided in this embodiment of this application, the security context of the user equipment may be the native security context between the user equipment and the second AMF. Alternatively, when the second AMF performs key derivation and generates a new key, the security context of the user equipment may be the second security context generated through key derivation based on the first security context.

[0009] With reference to the first aspect, in some implementations of the first aspect, that the first AMF sends the second registration request message to the second AMF includes: The first AMF sends a user equipment context transfer service invoking request to the second AMF, where the user equipment context transfer service invoking request carries the second registration request message.

[0010] According to the security context obtaining method provided in this embodiment of this application, the second registration request message sent by the first AMF to the second AMF may be carried in the user equipment context transfer service invoking request sent by the first AMF to the second AMF.

[0011] With reference to the first aspect, in some implementations of the first aspect, that the second AMF sends the security context of the user equipment to the first AMF includes: The second AMF sends a first response message to the first AMF, where the first response message carries the security context of the user equipment.

[0012] According to the security context obtaining method provided in this embodiment of this application, when returning the security context of the user equipment to the first AMF, the second AMF may send the first response message carrying the security context of the user equipment to the first AMF.

[0013] With reference to the first aspect, in some implementations of the first aspect, the method further includes: When the first AMF receives a message indicating that the second AMF fails to validate the integrity of the second registration request message, the first AMF continues to use a mapped security context, or initiates initial authentication to the user equipment.

[0014] According to the security context obtaining method provided in this embodiment of this application, when the first AMF fails to obtain the security context of the user equipment from the second AMF, the first AMF may continue to use the mapped security context generated through negotiation with the user equipment; or the first AMF may initiate initial authentication to the user equipment to generate a security context between the first AMF and the user equipment.

[0015] With reference to the first aspect, in some implementations of the first aspect, the mapped security context is obtained based on a security context between a mobility management entity MME and the user equipment, and the MME is a network element in the 4G communications system.

[0016] In the security context obtaining method provided in this embodiment of this application, the mapped security context is a security context generated by the user equipment and the first AMF separately through derivation based on the security context between the user equipment and the MME.

[0017] With reference to the first aspect, in some implementations of the first aspect, that the second AMF validates the integrity of the second registration request message includes: The second AMF validates the integrity of the second registration request message based on the native security context between the second AMF and the user equipment.

[0018] According to a second aspect, a security context obtaining method is provided. The method includes: A second access and mobility management function AMF receives a second registration request message sent by a first AMF, where the second registration request message is integrity protected using a first security context, the first security context is a native security context between user equipment and the second AMF, and the first AMF is an AMF providing an access and mobility management service for the user equipment after the user equipment is handed

over from a 4G communications system to a 5G communications system. The second AMF validates integrity of the second registration request message. If the second AMF successfully validates the integrity of the second registration request message, the second AMF sends a security context of the user equipment to the first AMF.

[0019] According to the security context obtaining method provided in this embodiment of this application, when the user equipment is handed over from the 4G communications system to the 5G communications system, the security context of the user equipment is stored by the user equipment and the second AMF before the handover. After the user equipment is handed over from the 4G communications system to the 5G communications system, the first AMF provides the access and mobility management service for the user equipment. The first AMF needs to obtain the security context of the user equipment from the second AMF. Specifically, after receiving a handover command, the user equipment may perform integrity protection on a fourth registration request message based on the natively stored security context between the user equipment and the second AMF, and then generate the second registration request message. The UE adds the second registration request message to a first registration request message sent to the first AMF. In this way, the first AMF may forward the second registration request message to the second AMF, and the second AMF may validate the integrity of the second registration request message. After successfully validating the integrity of the second registration request message, the second AMF sends the security context of the user equipment to the first AMF. This can improve a possibility that the first AMF successfully obtains the security context of the user equipment from the second AMF.

[0020] With reference to the second aspect, in some implementations of the second aspect, the security context of the user equipment includes: the first security context, or a second security context generated through key derivation based on the first security context.

[0021] According to the security context obtaining method provided in this embodiment of this application, the security context of the user equipment may be the native security context between the user equipment and the second AMF. Alternatively, when the second AMF performs key derivation and generates a new key, the security context of the user equipment may be the second security context generated through key derivation based on the first security context.

[0022] With reference to the second aspect, in some implementations of the second aspect, that the second AMF receives the second registration request message sent by the first AMF includes:

The second AMF receives a user equipment context transfer service invoking request sent by the first AMF, where the user equipment context transfer service invoking request carries the second registration request message.

[0023] According to the security context obtaining method provided in this embodiment of this application, the second registration request message sent by the first AMF to the second AMF may be carried in the user equipment context transfer service invoking request sent by the first AMF to the second AMF.

[0024] With reference to the second aspect, in some implementations of the second aspect, that the second AMF sends the security context of the user equipment to the first AMF includes: The second AMF sends a first response message to the first AMF, where the first response message carries the security context of the user equipment.

[0025] According to the security context obtaining method provided in this embodiment of this application, when returning the security context of the user equipment to the first AMF, the second AMF may send the first response message carrying the security context of the user equipment to the first AMF.

[0026] With reference to the second aspect, in some implementations of the second aspect, that the second AMF validates the integrity of the second registration request message includes: The second AMF validates the integrity of the second registration request message based on the first security context.

[0027] According to a third aspect, a security context obtaining method is provided. The method includes: User equipment determines a second registration request message, and performs integrity protection on the second registration request message, where the second registration request message is integrity protected using a first security context, and the first security context is a native security context between the user equipment and a second access and mobility management function AMF. The user equipment sends a first registration request message to a first access and mobility management function AMF, where the first registration request message carries the second registration request message, and the first AMF is an AMF providing an access and mobility management service for the user equipment after the user equipment is handed over from a 4G communications system to a 5G communications system.

[0028] According to the security context obtaining method provided in this embodiment of this application, when the user equipment is handed over from the 4G communications system to

the 5G communications system, a security context of the user equipment is stored by the user equipment and the second AMF before the handover. After the user equipment is handed over from the 4G communications system to the 5G communications system, the first AMF provides the access and mobility management service for the user equipment. The first AMF needs to obtain the security context of the user equipment from the second AMF. Specifically, after receiving a handover command, the user equipment may perform integrity protection on a fourth registration request message based on the natively stored security context between the user equipment and the second AMF, and then generate the second registration request message. The UE adds the second registration request message to the first registration request message sent to the first AMF. In this way, the first AMF may forward the second registration request message to the second AMF, and the second AMF may validate integrity of the second registration request message. After successfully validating the integrity of the second registration request message, the second AMF may return the security context of the user equipment to the first AMF. This can improve a possibility that the first AMF successfully obtains the security context of the user equipment from the second AMF.

[0029] With reference to the third aspect, in some implementations of the third aspect, the method further includes: if a non-access stratum security mode command NAS SMC message sent by the first AMF is received, validating integrity of the NAS SMC; and if the validation is successful, sending a non-access stratum security mode complete message to the first AMF.

[0030] According to the security context obtaining method provided in this embodiment of this application, if the user equipment receives the NAS SMC message sent by the first AMF, and the user equipment successfully validates the NAS SMC message, the user equipment sends the non-access stratum security mode complete message to the first AMF.

[0031] According to a fourth aspect, a security context obtaining method is provided. The method includes: A first access and mobility management function AMF receives a first registration request message sent by user equipment, where the first registration request message carries a second registration request message, the second registration request message is integrity protected using a first security context, the first security context is a native security context between the user equipment and a second AMF, and the first AMF is an AMF providing an access and mobility management service for the user equipment after the user equipment is handed over from a 4G communications system to a 5G communications system. The first AMF sends the

second registration request message to the second AMF. If the second AMF successfully validates integrity of the second registration request message, the first AMF receives a security context of the user equipment that is sent by the second AMF.

[0032] According to the security context obtaining method provided in this embodiment of this application, when the user equipment is handed over from the 4G communications system to the 5G communications system, the security context of the user equipment is stored by the user equipment and the second AMF before the handover. After the user equipment is handed over from the 4G communications system to the 5G communications system, the first AMF provides the access and mobility management service for the user equipment. The first AMF needs to obtain the security context of the user equipment from the second AMF. Specifically, after receiving a handover command, the user equipment may perform integrity protection on a fourth registration request message based on the natively stored security context between the user equipment and the second AMF, and then generate the second registration request message. The UE adds the second registration request message to the first registration request message sent to the first AMF. In this way, the first AMF may forward the second registration request message to the second AMF, and the second AMF may validate the integrity of the second registration request message. After successfully validating the integrity of the second registration request message, the second AMF may return the security context of the user equipment to the first AMF. This can improve a possibility that the first AMF successfully obtains the security context of the user equipment from the second AMF.

[0033] With reference to the fourth aspect, in some implementations of the fourth aspect, the security context of the user equipment includes: the first security context, or a second security context generated through key derivation based on the first security context.

[0034] According to the security context obtaining method provided in this embodiment of this application, the security context of the user equipment may be the native security context between the user equipment and the second AMF. Alternatively, when the second AMF performs key derivation and generates a new key, the security context of the user equipment may be the second security context generated through key derivation based on the first security context.

[0035] With reference to the fourth aspect, in some implementations of the fourth aspect, that the first AMF sends the second registration request message to the second AMF includes: The first AMF sends a user equipment context transfer service invoking request to the second AMF, where

the user equipment context transfer service invoking request carries the second registration request message.

[0036] According to the security context obtaining method provided in this embodiment of this application, the second registration request message sent by the first AMF to the second AMF may be carried in the user equipment context transfer service invoking request sent by the first AMF to the second AMF.

[0037] With reference to the fourth aspect, in some implementations of the fourth aspect, that the first AMF receives the security context of the user equipment that is sent by the second AMF includes: The first AMF receives a first response message sent by the second AMF, where the first response message carries the security context of the user equipment.

[0038] According to the security context obtaining method provided in this embodiment of this application, when returning the security context of the user equipment to the first AMF, the second AMF may send the first response message carrying the security context of the user equipment to the first AMF.

[0039] With reference to the fourth aspect, in some implementations of the fourth aspect, the method further includes: When the first AMF receives a message indicating that the second AMF fails to validate the integrity of the second registration request message, the first AMF continues to use a mapped security context, or initiates initial authentication to the user equipment.

[0040] According to the security context obtaining method provided in this embodiment of this application, when the first AMF fails to obtain the security context of the user equipment from the second AMF, the first AMF may continue to use the mapped security context generated through negotiation with the user equipment; or the first AMF may initiate initial authentication to the user equipment to generate a security context between the first AMF and the user equipment.

[0041] With reference to the fourth aspect, in some implementations of the fourth aspect, the mapped security context is obtained based on a security context between a mobility management entity MME and the user equipment, and the MME is a network element in the 4G communications system.

[0042] In the security context obtaining method provided in this embodiment of this application, the mapped security context is a security context generated by the user equipment and the first AMF separately through derivation based on the security context between the user equipment and the MME.

[0043] According to a fifth aspect, a security context obtaining method is provided. The method includes: A first access and mobility management function AMF sends a user equipment context transfer service invoking request to a second AMF, where the user equipment context transfer service invoking request is used to obtain a security context of user equipment, the user equipment context transfer service invoking request carries indication information, the indication information is used to indicate that the user equipment is validated, and the first AMF is an AMF providing an access and mobility management service for the user equipment after the user equipment is handed over from a 4G communications system to a 5G communications system. The first AMF receives a second response message sent by the second AMF, where the second response message carries the security context of the user equipment.

[0044] According to the security context obtaining method provided in this embodiment of this application, the user equipment context transfer service invoking request sent by the first AMF to the second AMF carries the indication information indicating that the UE is validated. This can avoid that the second AMF fails to verify the UE and does not send the security context of the UE to the first AMF, and improve a possibility that the first AMF successfully obtains the security context of the user equipment from the second AMF.

[0045] With reference to the fifth aspect, in some implementations of the fifth aspect, that the indication information is used to indicate that the user equipment is validated includes: The indication information is used to indicate that integrity of a registration request message is successfully validated, where the registration request message is received by the first AMF from the user equipment.

[0046] According to the security context obtaining method provided in this embodiment of this application, the indication information, sent by the first AMF to the second AMF, indicating that the UE is validated may be used by the first AMF to notify the second AMF that the integrity of the registration request message sent by the UE is successfully validated. This provides a flexible optional solution for indicating that the UE is validated.

[0047] With reference to the fifth aspect, in some implementations of the fifth aspect, before the first AMF sends the user equipment context transfer service invoking request to the second AMF, the method further includes: The first AMF successfully validates integrity protection for the registration request message, where the registration request message is received by the first AMF from the user equipment; and/or the first AMF determines that the registration request

message is a registration request message sent by the user equipment after the user equipment is handed over from the 4G communications system to the 5G communications system.

[0048] According to the security context obtaining method provided in this embodiment of this application, the first AMF determines, based on a result indicating that the registration request message is successfully validated and/or based on that the received registration request message is the registration request message sent by the user equipment after the user equipment is handed over from the 4G communications system to the 5G communications system, that the user equipment context transfer service invoking request may be sent to the second AMF.

[0049] With reference to the fifth aspect, in some implementations of the fifth aspect, the user equipment context transfer service invoking request carries an identity of the user equipment.

[0050] According to the security context obtaining method provided in this embodiment of this application, to enable the second AMF to learn that the first AMF needs to obtain a security context of user equipment, the first AMF adds an identity of the user equipment to the context transfer service invoking request.

[0051] With reference to the fifth aspect, in some implementations of the fifth aspect, the user equipment context transfer service invoking request carries an uplink non-access stratum count UL NAS COUNT of the user equipment.

[0052] According to the security context obtaining method provided in this embodiment of this application, to enable the second AMF to learn of the UL NAS COUNT, the first AMF may add the UL NAS COUNT to the context transfer service invoking request.

[0053] With reference to the fifth aspect, in some implementations of the fifth aspect, that the user equipment context transfer service invoking request carries the UL NAS COUNT includes: The user equipment context transfer service invoking request carries a plaintext registration request message, where the plaintext registration request message includes the UL NAS COUNT, and the registration request message is received by the first AMF from the user equipment.

[0054] According to the security context obtaining method provided in this embodiment of this application, that the user equipment context transfer service invoking request carries the UL NAS COUNT may be implemented by carrying the plaintext registration request message in the user equipment context transfer service invoking request, where the plaintext registration request message includes the UL NAS COUNT. This provides a flexible optional solution for the first AMF to send the UL NAS COUNT to the second AMF.

[0055] According to a sixth aspect, a security context obtaining method is provided. The method includes: A second access and mobility management function AMF receives a user equipment context transfer service invoking request sent by a first AMF, where the user equipment context transfer service invoking request is used to obtain a security context of user equipment, the user equipment context transfer service invoking request carries indication information, the indication information is used to indicate that the user equipment is validated, and the first AMF is an AMF providing an access and mobility management service for the user equipment after the user equipment is handed over from a 4G communications system to a 5G communications system. The second AMF sends a second response message to the first AMF, where the second response message carries the security context of the user equipment.

[0056] According to the security context obtaining method provided in this embodiment of this application, the user equipment context transfer service invoking request sent by the first AMF and received by the second AMF carries the indication information indicating that the UE is validated. Based on the indication information, the second AMF does not need to verify the UE. This can avoid that the second AMF fails to verify the UE and does not send the security context of the UE to the first AMF, and improve a possibility that the first AMF successfully obtains the security context of the user equipment from the second AMF.

[0057] With reference to the sixth aspect, in some implementations of the sixth aspect, that the indication information is used to indicate that the user equipment is validated includes: The indication information is used to indicate that integrity of a registration request message is successfully validated, where the registration request message is received by the first AMF from the user equipment.

[0058] According to the security context obtaining method provided in this embodiment of this application, the indication information, sent by the first AMF and received by the second AMF, indicating that the UE is validated may be used by the first AMF to notify the second AMF that the integrity of the registration request message sent by the UE is successfully validated. This provides a flexible optional solution for indicating that the UE is validated.

[0059] With reference to the sixth aspect, in some implementations of the sixth aspect, the user equipment context transfer service invoking request carries an identity of the user equipment.

[0060] According to the security context obtaining method provided in this embodiment of this application, based on the identity of the user equipment that is carried in the context transfer

service invoking request, the second AMF may determine that the first AMF needs to obtain the security context of the user equipment.

[0061] With reference to the sixth aspect, in some implementations of the sixth aspect, the user equipment context transfer service invoking request carries an uplink non-access stratum count UL NAS COUNT of the user equipment.

[0062] According to the security context obtaining method provided in this embodiment of this application, the second AMF may learn of the UL NAS COUNT based on the UL NAS COUNT carried in the context transfer service invoking request.

[0063] With reference to the sixth aspect, in some implementations of the sixth aspect, that the user equipment context transfer service invoking request carries the UL NAS COUNT includes: The user equipment context transfer service invoking request carries a plaintext registration request message, where the plaintext registration request message includes the UL NAS COUNT, and the registration request message is received by the first AMF from the user equipment.

[0064] According to the security context obtaining method provided in this embodiment of this application, that the user equipment context transfer service invoking request carries the UL NAS COUNT may be implemented by carrying the plaintext registration request message in the user equipment context transfer service invoking request, where the plaintext registration request message includes the UL NAS COUNT. This provides a flexible optional solution for the first AMF to send the UL NAS COUNT to the second AMF.

[0065] With reference to the sixth aspect, in some implementations of the sixth aspect, the method further includes: The second AMF performs key derivation based on the UL NAS COUNT.

[0066] According to the security context obtaining method provided in this embodiment of this application, the second AMF may perform key derivation based on the received UL NAS COUNT.

[0067] According to a seventh aspect, a communications system is provided. The communications system includes the first AMF and the second AMF that may be configured to perform operations performed by the first AMF and the second AMF in any one of the first aspect or the possible implementations of the first aspect. Specifically, the communications apparatus may include a corresponding component (means) configured to perform the steps or functions described in any one of the first aspect or the possible implementations of the first aspect, and the component may be the first AMF and the second AMF in the first aspect, or chips or functional

modules inside the first AMF and the second AMF in the first aspect. The steps or functions may be implemented by software, hardware, or a combination of hardware and software.

[0068] According to an eighth aspect, a security context obtaining apparatus is provided. The apparatus may be configured to perform an operation performed by the first AMF in any one of the fifth aspect, the fourth aspect, the possible implementations of the fifth aspect, or the possible implementations of the fourth aspect. Specifically, the security context obtaining apparatus may include a corresponding component (means) configured to perform the steps or functions described in any one of the fifth aspect, the fourth aspect, the possible implementations of the first aspect, or the possible implementations of the fourth aspect, and the component may be the first AMF in the fourth and fifth aspects, or a chip or a functional module inside the first AMF in the fourth and fifth aspects. The steps or functions may be implemented by software, hardware, or a combination of hardware and software.

[0069] According to a ninth aspect, a security context obtaining apparatus is provided. The apparatus may be configured to perform an operation performed by the second AMF in any one of the second aspect, the sixth aspect, the possible implementations of the second aspect, or the possible implementations of the sixth aspect. Specifically, the security context obtaining apparatus may include a corresponding component (means) configured to perform the steps or functions described in any one of the second aspect, the sixth aspect, the possible implementations of the second aspect, or the possible implementations of the sixth aspect, and the component may be the second AMF in the second and sixth aspects, or a chip or a functional module in the second AMF in the second and sixth aspects. The steps or functions may be implemented by software, hardware, or a combination of hardware and software.

[0070] According to a tenth aspect, a security context obtaining apparatus is provided. The apparatus may be configured to perform an operation performed by the user equipment in the third aspect. Specifically, the security context obtaining apparatus may include a corresponding component (means) configured to perform the steps or functions described in the third aspect, and the component may be the user equipment in the third aspect, or a chip or a functional module in the user equipment in the third aspect. The steps or functions may be implemented by software, hardware, or a combination of hardware and software.

[0071] According to an eleventh aspect, a communications device is provided, including a processor, a transceiver, and a memory. The memory is configured to store a computer program.

The transceiver is configured to perform sending and receiving steps in the security context obtaining apparatus method in any possible implementation in the first to the fifth aspects. The processor is configured to invoke the computer program from the memory and run the computer program, to enable the communications device to perform the security context obtaining apparatus method in any possible implementation in the first to the sixth aspects.

[0072] Optionally, there are one or more processors and one or more memories.

[0073] Optionally, the memory may be integrated with the processor, or the memory and the processor may be separately disposed.

[0074] Optionally, the transceiver includes a transmitter (transmitter) and a receiver (receiver).

[0075] According to a twelfth aspect, a system is provided. The system includes the security context obtaining apparatuses provided in the eighth aspect and the ninth aspect.

[0076] According to a thirteenth aspect, a computer program product is provided. The computer program product includes a computer program (which may also be referred to as code or an instruction). When the computer program is run, a computer is enabled to perform the method in any possible implementation in the first to the sixth aspects.

[0077] According to a fourteenth aspect, a computer-readable medium is provided. The computer-readable medium stores a computer program (which may also be referred to as code or an instruction). When the computer program is run on a computer, the computer is enabled to perform the method in any possible implementation in the first to the sixth aspects.

[0078] According to a fifteenth aspect, a chip system is provided, including a memory and a processor. The memory is configured to store a computer program. The processor is configured to invoke the computer program from the memory and run the computer program, so that a communications device on which the chip system is installed performs the method in any possible implementation in the first to the sixth aspects.

BRIEF DESCRIPTION OF DRAWINGS

[0079] FIG. 1 is a network architecture applicable to embodiments of this application;

[0080] FIG. 2 is a schematic flowchart of handover between communications systems;

[0081] FIG. 3 is a schematic diagram of a security context obtaining method according to an embodiment of this application;

[0082] FIG. 4 is a schematic diagram of another security context obtaining method according to an embodiment of this application;

[0083] FIG. 5 is a schematic diagram of a security context obtaining apparatus 50 according to an embodiment of this application;

[0084] FIG. 6 is a schematic structural diagram of user equipment 60 according to an embodiment of this application;

[0085] FIG. 7 is a schematic diagram of a security context obtaining apparatus 70 according to an embodiment of this application;

[0086] FIG. 8 is a schematic structural diagram of a first AMF 80 according to an embodiment of this application;

[0087] FIG. 9 is a schematic diagram of a security context obtaining apparatus 90 according to an embodiment of this application; and

[0088] FIG. 10 is a schematic structural diagram of a second AMF 100 according to an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

[0089] The following describes technical solutions of this application with reference to accompanying drawings.

[0090] The technical solutions of the embodiments of this application may be applied to various communications systems, such as a global system for mobile communications (global system for mobile communications, GSM), a code division multiple access (code division multiple access, CDMA) system, a wideband code division multiple access (wideband code division multiple access, WCDMA) system, a general packet radio service (general packet radio service, GPRS) system, a long term evolution (long term evolution, LTE) system, an LTE frequency division duplex (frequency division duplex, FDD) system, an LTE time division duplex (time division duplex, TDD) system, a universal mobile telecommunications system (universal mobile telecommunication system, UMTS), a worldwide interoperability for microwave access (worldwide interoperability for microwave access, WiMAX) communications system, a future 5th generation (5th generation, 5G) system, or a new radio (new radio, NR) system.

[0091] FIG. 1 is a network architecture applicable to the embodiments of this application. As

shown in FIG. 1, the following separately describes components in the network architecture.

[0092] 1. User equipment (user equipment, UE) 110 may include various handheld devices, vehicle-mounted devices, wearable devices, and computing devices that have a wireless communication function, or other processing devices connected to a wireless modem, and various forms of terminals, mobile stations (mobile station, MS), terminals (terminal), soft clients, and the like. For example, the user equipment 110 may be a water meter, an electricity meter, or a sensor.

[0093] 2. A (radio) access network (radio access network, (R)AN) element 120 is configured to provide a network access function for authorized user equipments in a specific area, and can use transmission tunnels with different quality based on levels, service requirements, and the like of the user equipments.

[0094] The (R)AN element can manage radio resources and provide an access service for user equipment, to forward a control signal and user equipment data between the user equipment and a core network. The (R)AN element may also be understood as a base station in a conventional network.

[0095] 3. A user plane network element 130 is used for packet routing and forwarding, quality of service (quality of service, QoS) processing of user plane data, and the like.

[0096] In a 5G communications system, the user plane network element may be a user plane function (user plane function, UPF) network element. In a future communications system, the user plane network element may still be a UPF network element, or may have another name. This is not limited in this application.

[0097] 4. A data network element 140 is configured to provide a network for data transmission.

[0098] In the 5G communications system, the data network element may be a data network (data network, DN) element. In the future communications system, the data network element may still be a DN element, or may have another name. This is not limited in this application.

[0099] 5. An access and mobility management network element 150 is mainly configured to perform mobility management, access management, and the like. The access and mobility management network element 150 may be configured to implement functions, for example, lawful interception and access authorization/authentication, other than session management in functions of a mobility management entity (mobility management entity, MME).

[00100] In the 5G communications system, the access and mobility management network element may be an access and mobility management function (access and mobility management

function, AMF). In the future communications system, the access and mobility management device may still be an AMF, or may have another name. This is not limited in this application.

[00101] 6. A session management network element 160 is mainly configured to manage a session, assign and manage an internet protocol (internet protocol, IP) address of user equipment, select an endpoint that can manage a user plane function interface and a policy control and charging function interface, notify downlink data, and the like.

[00102] In the 5G communications system, the session management network element may be a session management function (session management function, SMF) network element. In the future communications system, the session management network element may still be an SMF network element, or may have another name. This is not limited in this application.

[00103] 7. A policy control network element 170 is configured to guide a unified policy framework of network behavior, and provide policy rule information for a control plane function network element (such as the AMF or the SMF network element), and the like.

[00104] In a 4G communications system, the policy control network element may be a policy and charging rules function (policy and charging rules function, PCRF) network element. In the 5G communications system, the policy control network element may be a policy control function (policy control function, PCF) network element. In the future communications system, the policy control network element may still be a PCF network element, or may have another name. This is not limited in this application.

[00105] 8. An authentication server 180 is configured to authenticate a service, generate a key to implement two-way authentication for user equipment, and support a unified authentication framework.

[00106] In the 5G communications system, the authentication server may be an authentication server function (authentication server function, AUSF) network element. In the future communications system, the authentication server function network element may still be an AUSF network element, or may have another name. This is not limited in this application.

[00107] 9. A data management network element 190 is configured to process a user equipment identity, perform access authentication, registration, and mobility management, and the like.

[00108] In the 5G communications system, the data management network element may be a unified data management (unified data management, UDM) network element. In the 4G communications system, the data management network element may be a home subscriber server

(home subscriber server, HSS) network element. In the future communications system, the unified data management may still be a UDM network element, or may have another name. This is not limited in this application.

[00109] 10. An application network element 1100 is configured to perform application-affected data routing, access a network exposure function network element, interact with a policy framework to perform policy control, and the like.

[00110] In the 5G communications system, the application network element may be an application function (application function, AF) network element. In the future communications system, the application network element may still be an AF network element, or may have another name. This is not limited in this application.

[00111] 11. A network storage network element is configured to maintain real-time information of all network function services in a network.

[00112] In the 5G communications system, the network storage network element may be a network repository function (network repository function, NRF) network element. In the future communications system, the network storage network element may still be an NRF network element, or may have another name. This is not limited in this application.

[00113] It may be understood that the foregoing network elements or functions may be network elements in a hardware device, software functions running on dedicated hardware, or virtualized functions instantiated on a platform (for example, a cloud platform). For ease of description, this application is described below by using an example in which the access and mobility management device is the AMF, the data management network element is the UDM network element, the session management network element is the SMF network element, and the user plane network element is the UPF network element.

[00114] For ease of description, in the embodiments of this application, a session establishment method is described by using an example in which an apparatus is an AMF entity or a UDM entity. For an implementation method in which the apparatus is a chip in an AMF entity or a chip in a UDM entity, refer to specific descriptions about the session establishment method in which the apparatus is the AMF entity or the UDM entity. Details are not repeated.

[00115] In the network architecture shown in FIG. 1, the user equipment is connected to the AMF through an N1 interface, the (R)AN is connected to the AMF through an N2 interface, and the (R)AN is connected to the UPF through an N3 interface. UPFs are connected to each other

through an N9 interface, and the UPF is interconnected to a DN through an N6 interface. The SMF controls the UPF through an N4 interface. The AMF is connected to the SMF through an N11 interface. The AMF obtains subscription data of the user equipment from a UDM unit through an N8 interface. The SMF obtains the subscription data of the user equipment from the UDM unit through an N10 interface.

[00116] It should be understood that the foregoing network architecture applied to the embodiments of this application is merely an example, and a network architecture applicable to the embodiments of this application is not limited thereto. Any network architecture that can implement functions of the foregoing network elements is applicable to the embodiments of this application.

[00117] For example, in some network architectures, network function network elements and entities such as the AMF, the SMF network element, the PCF network element, a BSF network element, and the UDM network element are all referred to as network function (network function, NF) network elements. Alternatively, in some other network architectures, a set of network elements such as the AMF, the SMF network element, the PCF network element, a BSF network element, and the UDM network element may be referred to as a control plane function network element.

[00118] The user equipment in the embodiments of this application may be an access terminal, a subscriber unit, a subscriber station, a mobile station, a mobile console, a relay station, a remote station, a remote terminal, a mobile device, a user terminal (user terminal), terminal equipment (terminal equipment), a terminal (terminal), a wireless communications device, a user agent, a user apparatus, or the like. The user equipment may alternatively be a cellular phone, a cordless phone, a session initiation protocol (session initiation protocol, SIP) phone, a wireless local loop (wireless local loop, WLL) station, a personal digital assistant (personal digital assistant, PDA), a handheld device having a wireless communication function, a computing device, another processing device connected to a wireless modem, a vehicle-mounted device, a wearable device, user equipment in a future 5G network, user equipment in a future evolved public land mobile network (public land mobile network, PLMN), or the like. This is not limited in the embodiments of this application.

[00119] A network device in the embodiments of this application may be any device that has a wireless transceiver function and that is configured to communicate with the user equipment. The device includes but is not limited to an evolved NodeB (evolved Node B, eNB), a radio network

controller (radio network controller, RNC), a NodeB (Node B, NB), a base station controller (base station controller, BSC), a base transceiver station (base transceiver station, BTS), a home base station (for example, a home evolved NodeB, or a home Node B, HNB), a baseband unit (baseBand unit, BBU), an access point (access point, AP) in a wireless fidelity (wireless fidelity, WIFI) system, a wireless relay node, a wireless backhaul node, a transmission point (transmission point, TP), a transmission and reception point (transmission and reception point, TRP), or the like. Alternatively, the device may be a gNB or a transmission point (TRP or TP) in a 5G system such as an NR system, may be one antenna panel or a group (including a plurality of antenna panels) of antenna panels of a base station in a 5G system, or may be a network node, such as a baseband unit (BBU) or a distributed unit (distributed unit, DU), that constitutes a gNB or a transmission point.

[00120] In some deployments, the gNB may include a centralized unit (centralized unit, CU) and the DU. The gNB may further include an active antenna unit (active antenna unit, AAU). The CU implements some functions of the gNB, and the DU implements some functions of the gNB. For example, the CU is responsible for processing a non-real-time protocol and service, and implements functions of a radio resource control (radio resource control, RRC) layer and a packet data convergence protocol (packet data convergence protocol, PDCP) layer. The DU is responsible for processing a physical layer protocol and a real-time service, and implements functions of a radio link control (radio link control, RLC) layer, a media access control (media access control, MAC) layer, and a physical (physical, PHY) layer. The AAU implements some physical layer processing functions, radio frequency processing, and a function related to an active antenna. Information at the RRC layer is eventually converted into information at the PHY layer, or is converted from information at the PHY layer. Therefore, in this architecture, higher layer signaling such as RRC layer signaling may also be considered as being sent by the DU or sent by the DU and the AAU. It may be understood that the network device may be a device including one or more of a CU node, a DU node, and an AAU node. In addition, the CU may be a network device in an access network (radio access network, RAN), or may be a network device in a core network (core network, CN). This is not limited in this application.

[00121] In the embodiments of this application, the user equipment or the network device includes a hardware layer, an operating system layer running above the hardware layer, and an application layer running above the operating system layer. The hardware layer includes hardware such as a central processing unit (central processing unit, CPU), a memory management unit

(memory management unit, MMU), and a memory (also referred to as a main memory). The operating system may be any one or more types of computer operating systems that implement service processing by using a process (process), for example, a Linux operating system, a Unix operating system, an Android operating system, an iOS operating system, or a Windows operating system. The application layer includes applications such as a browser, an address book, word processing software, and instant communications software. In addition, a specific structure of an entity for performing a method provided in the embodiments of this application is not particularly limited in the embodiments of this application, provided that a program recording code of the method provided in the embodiments of this application can be run to perform communication according to the method provided in the embodiments of this application. For example, the entity for performing the method provided in the embodiments of this application may be the user equipment or the network device, or may be a functional module capable of invoking and executing the program in the user equipment or the network device.

[00122] In addition, aspects or features of this application may be implemented as a method, an apparatus or a product that uses standard programming and/or engineering technologies. The term "product" used in this application covers a computer program that can be accessed from any computer-readable component, carrier or medium. For example, the computer-readable medium may include but is not limited to: a magnetic storage component (for example, a hard disk, a floppy disk or a magnetic tape), an optical disc (for example, a compact disc (compact disc, CD) or a digital versatile disc (digital versatile disc, DVD)), a smart card, and a flash memory component (for example, an erasable programmable read-only memory (erasable programmable read-only memory, EPROM), a card, a stick, or a key drive). In addition, various storage media described in this specification may indicate one or more devices and/or other machine-readable media that are configured to store information. The term "machine-readable storage media" may include but is not limited to a radio channel, and various other media that can store, contain, and/or carry an instruction and/or data.

[00123] The embodiments of this application mainly relate to the mobility management entity MME when the network architecture shown in FIG. 1 is a 4G network architecture, and the access and mobility management function AMF and the UE when the network architecture shown in FIG. 1 is a 5G network architecture. For the AMF, this application relates to a first AMF and a second AMF. Specifically, the first AMF in this application is an AMF that is selected, from the 5G

communications system in a process in which the user equipment is handed over from the 4G communications system to the 5G communications system, for the UE by an MME in the 4G communications system to provide a core network service for the UE. The second AMF in this application is an AMF, other than the first AMF in the 5G communications system in the process in which the user equipment is handed over from the 4G communications system to the 5G communications system, that stores a security context of the UE.

[00124] It should be understood that "first" and "second" in this application are merely used for differentiation, and should not be construed as any limitation on this application. For example, the first AMF and the second AMF are merely used to differentiate between different AMFs.

[00125] To facilitate understanding of a security context obtaining method provided in the embodiments of this application, the following briefly describes, with reference to FIG. 2, a process in which user equipment is handed over from a 4G communications system to a 5G communications system. FIG. 2 is a schematic flowchart of handover between communications systems. The schematic flowchart includes the UE, an MME, a first AMF, and a second AMF.

[00126] The handover between the communications systems includes the following steps.

[00127] S210: The MME sends a forward relocation request (forward relocation request) message to the first AMF.

[00128] Specifically, the MME in the 4G communications system learns that the user equipment is handed over from the 4G communications system to the 5G communications system, and needs to select, for the UE, the first AMF from the 5G communications system to continue to provide an access and mobility management service for the UE. When the UE accesses the 4G communications system, the UE and the MME obtain a same key K_{ASME}. When the UE is handed over from the 4G communications system to the 5G communications system, the MME selects the first AMF and sends the K_{ASME} and a next hop parameter (next hop parameter, NH) to the first AMF. In other words, the forward relocation request message carries parameters such as the K_{ASME} and the NH.

[00129] In this embodiment of this application, how the MME learns of handover between systems is not limited. For details, refer to specifications for a procedure of handover from the 4G communications system to the 5G communications system in an existing protocol. For example, a base station in the 4G communications system may send a handover request to the MME, so that the MME learns that the user equipment needs to be handed over from the 4G communications

system to the 5G communications system.

[00130] In addition, in this embodiment of this application, how the MME selects the first AMF is not limited. For details, refer to specifications in the existing protocol. For example, the MME stores at least one AMF configured by an operator. When the MME learns that the user equipment needs to be handed over from the 4G communications system to the 5G communications system, the MME selects the first AMF from the at least one AMF.

[00131] S220: The first AMF determines a mapped (mapped) security context.

[00132] Specifically, the first AMF derives the mapped security context based on the parameters, such as the K_{ASME} and the NH, carried in the received relocation request message. The mapped security context is included in a mapped context of the UE. It should be understood that the mapped context in this application is a security context of the UE that is derived by the first AMF and the UE separately based on a context generated through negotiation between the UE and the MME in the 4G communications system. For how to derive the security context of the UE based on the 4G context, refer to specifications in the existing protocol, and this process is not limited in this application. The mapped security context is obtained by the first AMF and the UE separately based on a security context between the MME and the user equipment. In addition, in this application, the context negotiated between the UE and the MME in the 4G communications system includes the security context between the UE and the MME, and may also be referred to as a 4G context of the UE for differentiation. Likewise, in this application, before the UE is handed over from the 4G communications system to the 5G communications system, the security context of the UE that is stored in the UE and the second AMF is a context negotiated between the UE and the second AMF in the 5G communications system, includes a security context between the UE and the second AMF, and may also be referred to as a 5G context of the UE for differentiation.

[00133] For ease of description, in the following, the security context obtained by the first AMF and the UE separately through derivation based on the security context between the MME and the user equipment is referred to as the mapped security context, and the security context between the second AMF and the UE is referred to as a native (native) security context.

[00134] It should be further understood that this embodiment of this application mainly relates to sending the security context of the UE by the second AMF to the first AMF. The security context of the UE is a part of a context of the UE, and may be transferred along with the context of the UE. Therefore, for ease of description, in this embodiment of this application, sending the security

context of the UE by the second AMF to the first AMF may be described as sending the context of the UE or sending the security context of the UE. This is merely used for ease of description, and does not constitute any limitation on the protection scope of the embodiments of this application.

[00135] That the first AMF derives the mapped security context of the UE based on the parameters, such as the K_{ASME} and the NH, carried in the received relocation request message includes that the first AMF derives a key K_{AMF1} based on the K_{ASME} and the NH.

[00136] For example, after receiving the K_{ASME} and the NH, the first AMF may calculate the key K_{AMF1} by using a preset derivation formula. The derivation formula is: K_{AMF1} = HMAC – SHA – 256 (Key, FC||P0||L0), where FC = 0x76, P0 = NH value, L0 = length of the NH value (i.e. 0x00 0x20), and KEY = K_{ASME}. The first AMF calculates an integrity protection key $K_{NASint1}$ and a confidentiality protection key $K_{NASenc1}$ based on the key K_{AMF1} and a security algorithm negotiated with the UE, where K_{AMF1}, $K_{NASint1}$, and $K_{NASenc1}$ are included in the security context of the UE. K_{AMF1}, $K_{NASint1}$, and $K_{NASenc1}$ are derived based on K_{ASME} and the NH, and K_{ASME} and the NH are the security context between the UE and the MME. Therefore, K_{AMF1}, $K_{NASint1}$, and $K_{NASenc1}$ are referred to as the mapped security context of the UE.

[00137] S230: The first AMF sends a forward relocation response (forward relocation response) message to the MME.

[00138] Specifically, after determining the mapped security context, the first AMF sends the forward relocation response message to the MME. The forward relocation response message is used to notify the MME that the first AMF may be used as an AMF providing the access and mobility management service for the UE in the 5G communications system when the UE is handed over from the 4G communications system to the 5G communications system.

[00139] S240: The MME sends a handover command (handover command) message to the UE.

[00140] After receiving the forward reallocation response message sent by the first AMF, the MME learns that the first AMF can provide the access and mobility management service for the UE. In this case, the MME sends the handover command message to the UE, so that the UE learns that the UE can be handed over from the 4G communications system to the 5G communications system.

[00141] S250: The UE determines the mapped security context.

[00142] After receiving the handover command message, the UE calculates, by using the preset

derivation formula, the key K_{AMF1} based on the key K_{ASME} and the NH that are stored in the UE. For a specific derivation process, refer to the foregoing S220, and details are not described herein again.

[00143] After S250, the UE and the first AMF obtain the same key K_{AMF1}, and the key K_{AMF1} may be subsequently used to derive another key.

[00144] For example, the UE and the first AMF obtain the same key K_{AMF1}. Then, based on K_{AMF1} and a non-access stratum (non-access stratum, NAS) integrity protection algorithm and a confidentiality protection algorithm that are negotiated between the UE and the first AMF, the UE and the first AMF generate the integrity protection key $K_{NASint1}$ and the confidentiality protection key $K_{NASenc1}$ that are used to protect a NAS message (for example, a registration request message). Specifically, $K_{NASint1}$ and $K_{NASenc1}$ are calculated as follows:

[00145] $K_{NASint1}$ = HMAC – SHA – 256 (KEY, S), where S = FC||$P0_1$||$L0_1$||$P1_1$||$L1_1$, FC = 0x69, $P0_1$ = algorithm type distinguisher (algorithm type distinguisher), $L0_1$ = length of the algorithm type distinguisher (length of algorithm type distinguisher) (i.e. 0x00 0x01), $P1_1$ = algorithm identity (algorithm identity), $L1_1$ = length of the algorithm identity (length of algorithm identity) (i.e. 0x00 0x01), and KEY = K_{AMF1}.

[00146] $K_{NASenc1}$ = HMAC – SHA – 256 (KEY, S), where S = FC||P0||L0||P1||L1, FC = 0x69, P0 = algorithm type distinguisher, L0 = length of algorithm type distinguisher (i.e. 0x00 0x01), P1 = algorithm identity, L1 = length of algorithm identity (i.e. 0x00 0x01), and KEY = K_{AMF1}.

[00147] The algorithm type distinguisher and the algorithm identity for calculating $K_{NASint1}$ are different from those for calculating $K_{NASenc1}$.

[00148] After the handover is completed, the UE initiates mobility registration, in other words, performs S260. The UE sends the registration request (registration request) message to the first AMF, and the UE performs security protection on the registration request message by using the mapped security context generated through derivation based on the foregoing generated K_{AMF1}. The security protection includes encryption protection and/or integrity protection.

[00149] It should be understood that a message sent by the UE to a core network device may be forwarded by an access network device. Because a function of an access device is not limited in this embodiment of this application, the access network device may forward a message between the UE and the first AMF. For brevity, in this application, forwarding the message between the UE and the first AMF is described as that the UE sends the registration request message to the first

AMF and the MME sends a message to the UE. The registration request message sent by the UE further includes a globally unique temporary user equipment identity (globally unique temporary user equipment identity, GUTI) in the mapped context, and the GUTI is used by the access network device to determine to forward the registration request message to the first AMF. Because the GUTI is included in the mapped context, the GUTI may be referred to as a mapped GUTI.

[00150] Optionally, when the UE sends the registration request message to the first AMF, the UE stores a security context of the UE that is between the UE and another AMF (the second AMF) and a 5G globally unique temporary user equipment identity (5th generation globally unique temporary user equipment identity, 5G-GUTI) of the user equipment. Therefore, the UE adds the 5G-GUTI to the registration request message.

[00151] It should be understood that this embodiment of this application mainly relates to a process in which the first AMF successfully obtains the security context of the UE from the second AMF. Therefore, in this application, the following case is mainly considered: When the UE sends the registration request message to the first AMF, the UE stores the security context the UE that is negotiated between the UE and the second AMF as well as the 5G-GUTI.

[00152] It should be further understood that a reason why the security context and the 5G-GUTI of the UE are stored by the UE and the second AMF is not limited in this embodiment of this application, and may be specified in the existing protocol. For example, before the UE is handed over from the 4G communications system to the 5G communications system, the UE is handed over from the 5G network communications system to the 4G communications system. Alternatively, UE supporting dual connectivity accesses the 5G communications system through a non-3GPP connection, and accesses the 4G communications system through a 3GPP connection at the same time. In this way, the UE in connected mode is handed over from the 4G communications system to the 5G communications system.

[00153] It should be understood that when the security context of the UE that is between the second AMF and the UE exists on the second AMF, the first AMF needs to obtain the security context of the UE from the second AMF. Specifically, that the first AMF obtains the security context of the UE from the second AMF is determined based on the 5G-GUTI carried in the registration request message received from the UE. The 5G-GUTI is configured by the second AMF for the UE and may be used to identify the UE and the second AMF. As specified in a protocol, when a security context of UE exists in the 5G communications system, the security

context of the UE instead of a mapped security context determined through negotiation between the first AMF and the UE is preferentially used, because the mapped security context is obtained through mapping based on a security context of the UE that is between the UE and the MME in the 4G communications system. In other words, the procedure shown in FIG. 2 further includes S270 in which the first AMF initiates a user equipment context transfer service invoking request (Namf_Communication_UEContextTransfer).

[00154] Specifically, the first AMF receives the registration request message sent by the UE, and initiates the user equipment context transfer service invoking request to the second AMF based on the 5G-GUTI carried in the registration request message. The user equipment context transfer service invoking request carries the registration request message.

[00155] It should be understood that the registration request message is security protected based on the mapped security context between the UE and the first AMF, and the second AMF determines, based on a result of validating the registration request message, whether to return the security context of the UE to the first AMF. In other words, S290 is performed. The second AMF validates the registration request message.

[00156] In a possible implementation, the second AMF fails to validate the registration request message. In this case, the second AMF does not return the security context of the UE to the first AMF. Consequently, the first AMF fails to obtain the security context of the UE from the second AMF, and the first AMF cannot preferentially use the security context of the UE. This does not comply with the protocol.

[00157] In another possible implementation, the second AMF successfully validates integrity of the registration request message. In this case, the second AMF returns the security context of the UE to the first AMF, and performs S291 in which the second AMF sends the security context of the UE to the first AMF. Optionally, that the second AMF sends the security context of the UE to the first AMF may be described as that the second AMF sends the context of the UE to the first AMF. The context of the UE includes the security context of the UE that is determined through negotiation between the second AMF and the UE, and the security context of the UE includes a key K_{AMF2}, a non-access stratum count (non-access stratum count, NAS COUNT), and the like.

[00158] Optionally, before transferring the security context of the UE, the second AMF may perform key derivation on the key K_{AMF2} according to a local policy. If the second AMF has performed key derivation on K_{AMF2}, the second AMF sends, to the first AMF, a key K_{AMF2}'

obtained after derivation and derivation indication information that is used to indicate that the second AMF has performed key derivation on K_{AMF2}.

[00159] In a possible implementation, the key derivation in this application may be horizontal key derivation.

[00160] For example, a manner of performing horizontal key derivation on K_{AMF2} to generate K_{AMF2}' is as follows:

K_{AMF2}'=HMAC–SHA–256 (Key, S);

FC = 0x72;

P0 = 0x01;

L0 = length of P0 (i.e. 0x00 0x01);

P1 = uplink NAS COUNT;

L1 = length of P1 (i.e. 0x00 0x04);

KEY = K_{AMF2};

S=FC||P0||L0||P1||L1.

[00161] In another possible implementation, the key derivation in this application may be a key derivation manner agreed on between different network elements. For example, the first AMF and the second AMF agree on a preset key derivation manner. Provided that the security context of the UE that is sent by the second AMF to the first AMF includes the derivation indication information, the first AMF can determine that a key in the received security context of the UE is obtained by the second AMF by performing key derivation in the preset key derivation manner.

[00162] Similarly, after receiving the derivation indication information, the first AMF also sends the derivation indication information to the UE, to indicate the UE to perform key derivation on the key K_{AMF2} to obtain the key K_{AMF2}', so that the UE and a network side agree on the key. It should be understood that the UE receives a key identifier indicating the key K_{AMF2}, and therefore can determine to perform key derivation on the key K_{AMF2} instead of K_{AMF}. The key identifier is not improved in this application. Therefore, the key identifier is not described in detail herein.

[00163] It can be learned, from the process of handing over the user equipment from the 4G communications system to the 5G communications system in FIG. 2, that when the second AMF fails to verify the UE, the first AMF cannot obtain the security context of the UE from the second AMF. To avoid failing to obtain the security context of the UE, an embodiment of this application provides a security context obtaining method. When the first AMF obtains the security context of

the UE from the second AMF, the security context carries indication information. The indication information indicates that the UE has been successfully verified. Based on the indication information, the second AMF does not need to verify the UE, but directly returns the security context of the UE. This can avoid a possibility of failing to obtain the security context of the UE.

[00164] It should be understood that verifying the UE in this application means validating the integrity of the registration request message sent by the UE, for example, decrypting the registration request message and/or validating the integrity of the registration request message. Because a premise that the integrity of the registration request message is successfully validated is that the registration request message is successfully decrypted, in this embodiment of this application, that the UE is successfully verified is described as that the integrity of the registration request message is successfully validated.

[00165] With reference to FIG. 3, the following describes in detail a security context obtaining method provided in an embodiment of this application. FIG. 3 is a schematic diagram of a security context obtaining method according to an embodiment of this application. The schematic diagram includes UE, an MME, a first AMF, and a second AMF.

[00166] The security context obtaining method includes the following steps.

[00167] S310: The first AMF sends a second request message to the second AMF.

[00168] The second request message is used to request to obtain a security context of the UE. The second request message carries indication information, and the indication information is used to indicate that the UE is validated.

[00169] Optionally, the indication information may be referred to as a reason value (value).

[00170] Specifically, that the first AMF determines that the UE is validated is mainly determining whether a registration request message received from the UE satisfies a preset condition. It should be understood that, before the first AMF sends the second request message to the second AMF, a method procedure shown in FIG. 3 further includes S311 to S316.

[00171] S311: The MME sends a forward relocation request message to the first AMF. This step is similar to S210 in FIG. 2, and details are not described herein again.

[00172] S312: The first AMF determines a mapped security context. This step is similar to S220 in FIG. 2, and details are not described herein again.

[00173] S313: The first AMF sends a forward relocation response message to the MME. This step is similar to S230 in FIG. 2, and details are not described herein again.

[00174] S314: The MME sends a handover command message to the UE. This step is similar to S240 in FIG. 2, and details are not described herein again.

[00175] S315: The UE determines the mapped security context. This step is similar to S250 in FIG. 2, and details are not described herein again.

[00176] S316: The UE sends the registration request message to the first AMF. This step is similar to S260 in FIG. 2, and details are not described herein again.

[00177] Further, that the first AMF determines that the registration request message satisfies the preset condition includes:

the first AMF successfully validates integrity protection for the registration request message; or

the first AMF determines that the registration request message is a registration request message sent by the UE after the UE is handed over from a 4G communications system to a 5G communications system. For example, before receiving the registration request message sent by the UE, the first AMF receives the forward relocation request message sent by the MME. Therefore, the first AMF can learn that the currently received registration request message is the registration request message received from the UE in a handover procedure.

[00178] Specifically, that the first AMF successfully validates integrity protection for the registration request message may also be referred to as that the first AMF successfully verifies the UE. In other words, the method procedure shown in FIG. 3 further includes S317 in which the first AMF verifies the UE.

[00179] In a possible implementation, the second request message is a user equipment context transfer service invoking request (Namf_Communication_UEContextTransfer) initiated by the first AMF shown in FIG. 2. Different from the user equipment context transfer service invoking request shown in FIG. 2, the user equipment context transfer service invoking request in this embodiment of this application includes a newly added information element (information element, IE), namely, the indication information.

[00180] In another possible implementation, the second request message is another possible second request message that is sent by the first AMF to the second AMF and that is used to obtain the security context of the UE.

[00181] It should be understood that a specific form of the second request message is not limited in this application. The indication information may be added to existing signaling between the first

AMF and the second AMF, or may be added to signaling newly added between the first AMF and the second AMF.

[00182] In another possible implementation, in this embodiment of this application, it is limited only that the first AMF needs to send the indication information to the second AMF before sending the user equipment context transfer service invoking request to the second AMF. In other words, the first AMF may directly send the indication information to the second AMF, without adding the indication information to the second request message. This possible implementation is not shown in FIG. 3.

[00183] It should be further understood that how the indication information specifically indicates that the UE is validated is not limited in this application. In a possible implementation, the indication information may be a 5G-GUTI of the UE. In this case, the 5G-GUTI may be used to identify the UE and indicate that the UE is validated. In this implementation, a new indication function is added to an existing IE, and the second AMF may be notified, in a predefined manner, that the 5G-GUTI has the new function. In another possible implementation, the indication information may be at least one newly added bit, and a value of the bit is set to 1, to indicate that the UE is validated. The foregoing possible implementations are merely examples for description, and do not constitute any limitation on the protection scope of this application.

[00184] In a possible implementation, the indication information explicitly indicates that the UE is validated. Alternatively, in another possible implementation, the indication information implicitly indicates that the UE is validated. For example, the indication information indicates that integrity of the registration request message received by the first AMF from the UE is successfully validated.

[00185] Further, to enable the second AMF to determine that the first AMF needs to obtain the security context of the UE, the second request message further needs to carry an identity of the UE.

[00186] In a possible implementation, the identity of the UE may be the foregoing 5G-GUTI.

[00187] In another possible implementation, the identity of the UE may be a subscriber permanent identity (subscriber permanent identity, SUPI).

[00188] It should be understood that, if the first AMF determines, after receiving the 5G-GUTI of the UE from the UE, that the security context of the UE needs to be obtained from the second AMF, the first AMF may choose to continue to add the 5G-GUTI of the UE, the SUPI of the UE,

or both the 5G-GUTI and the SUPI of the UE to the second request message.

[00189] Optionally, to enable the second AMF to obtain an uplink non-access stratum count (uplink non-access stratum count, UL NAS COUNT) of the UE, in a possible implementation, the second request message carries a plaintext registration request message, where the plaintext registration request message includes the UL NAS COUNT; or in a possible implementation, the second request message carries the UL NAS COUNT.

[00190] Further, after receiving the second request message sent by the first AMF, the second AMF learns, based on the indication information, that the UE is validated. In this case, the second AMF does not need to verify the UE, in other words, performs S320 in which the second AMF determines that the UE does not need to be verified.

[00191] S330: The second AMF sends a second response message to the first AMF.

[00192] The second response message carries the security context of the UE.

[00193] In this embodiment of this application, the second AMF does not need to verify the UE. After receiving the second request message sent by the first AMF, the second AMF directly returns the security context of the UE to the first AMF. This avoids a case in which the first AMF fails to obtain the security context of the UE because the second AMF fails to verify the UE.

[00194] Optionally, when the second request message carries the plaintext registration request message, or the second request message carries the UL NAS COUNT, the second AMF can obtain the UL NAS COUNT. For example, because the plaintext registration request message is a registration request message on which no security protection is performed, the second AMF does not need to validate the plaintext registration request message, and may directly obtain the UL NAS COUNT from the plaintext registration request message.

[00195] Further, the second AMF can perform key derivation on a first key in the security context of the UE based on the UL NAS COUNT. In this case, a key in the security context of the UE that is returned by the second AMF to the first AMF is a second key obtained by performing key derivation on the first key.

[00196] Specifically, when the key in the security context of the UE that is sent by the second AMF to the first AMF is the second key, the second AMF further needs to send key derivation indication information to the first AMF, to indicate that the second key is a key obtained through key derivation.

[00197] It should be understood that a procedure after the first AMF obtains the security context

of the UE is similar to a procedure after the first AMF obtains the security context of the UE in an existing procedure of handing over the UE from the 4G communications system to the 5G communications system. For details, refer to the existing procedure. Details are not described herein again.

[00198] In the security context obtaining method shown in FIG. 3, the second request message sent by the first AMF to the second AMF carries the indication information, and the indication information is used to indicate that the UE is validated. Therefore, the second AMF can determine, based on the indication information, that the UE is validated, and does not need to verify the UE. After receiving the second request message carrying the indication information, the second AMF directly returns the security context of the UE to the first AMF. This avoids the case in which the first AMF fails to obtain the security context of the UE because the second AMF fails to verify the UE. This application further provides another security context obtaining method in which the second AMF verifies the UE. However, the method can improve a possibility that the second AMF successfully verifies the UE, thereby improving a possibility that the first AMF successfully obtains the security context of the user equipment from the second AMF.

[00199] The following describes the security context obtaining method in detail with reference to FIG. 4. FIG. 4 is a schematic diagram of another security context obtaining method according to an embodiment of this application. The schematic diagram includes UE, an MME, a first AMF, and a second AMF.

[00200] The security context obtaining method includes the following steps.

[00201] S410: The UE determines a first registration request message.

[00202] The first registration request message carries a second registration request message. The second registration request message is integrity protected using a first security context, and the first security context is a native (native) security context between the UE and the second AMF.

[00203] Specifically, that the UE determines the first registration request message is mainly determining the second registration request message. The second registration request message is a message obtained after the UE performs integrity protection on a fourth registration request message by using the native security context. The fourth registration request message includes a GUTI, key identifier (ngKSI) information, and an UL NAS COUNT that are in a context of the UE that is between the UE and the second AMF. For ease of differentiation, the GUTI may be referred to as a native GUTI, and a key identifier may be referred to as a native key identifier.

[00204] Optionally, the fourth registration request message may have the following several possible cases:

[00205] Case 1:

[00206] The fourth registration request message is a message generated by the UE based on the native GUTI, the native key identifier, and the UL NAS COUNT. In Case 1, the fourth registration request message may also be referred to as a fourth message or may have another possible name. A name of the message is not limited in this embodiment of this application.

[00207] It should be understood that the fourth registration request message generated by the UE based on the context of the UE that is between the UE and the second AMF may alternatively be in another form. For example, in addition to the native GUTI, the native key identifier, and the UL NAS COUNT, the fourth registration request message generated by the UE further includes another information element (information element, IE).

[00208] In Case 1, that the UE performs integrity protection on the fourth registration request message based on the first security context includes: The UE performs integrity protection on the fourth registration request message based on the first security context, and generates a first MAC. Therefore, carrying the second registration request message in the first registration request message may also be understood as carrying the first MAC and the fourth registration request message in the first registration request message.

[00209] Further, in Case 1, that the UE determines the first registration request message includes the following steps:

[00210] Step 1:

[00211] The UE constructs the fourth registration request message.

[00212] Step 2:

[00213] The UE performs integrity protection on the fourth registration request message based on the security context between the UE and the second AMF, and generates the first MAC.

[00214] Step 3:

[00215] The UE performs integrity protection on a third registration request message and the second registration request message (RR2) based on a mapped security context between the UE and the first AMF, and generates a fifth MAC. The third registration request message is the registration request message sent by the UE to the first AMF in the method procedure S260 shown in FIG. 2. Specifically, the third registration request message includes a GUTI and key identifier

information that are in the mapped context between the UE and the first AMF. For ease of differentiation, the GUTI may be referred to as a mapped GUTI, and a key identifier may be referred to as a mapped key identifier.

[00216] In this case, the first registration request message includes the fourth registration request message (RR4), the third registration request message (RR3), the fifth MAC (MAC5), and the first MAC (MAC1). MAC1 is a MAC value obtained by performing integrity protection on RR4 by using the native security context. MAC5 is a MAC value obtained by performing integrity protection on RR3 and RR2 by using the mapped security context (or MAC5 is a MAC value obtained by performing integrity protection on RR3, RR4, and MAC1 by using the mapped security context). It may also be understood that the first registration request message is a message on which integrity protection is performed sequentially based on the native security context and the mapped security context.

[00217] Case 2:

[00218] The fourth registration request message is a registration request message obtained after the UE performs integrity protection on a third registration request message based on a mapped security context.

[00219] In Case 2, that the UE performs integrity protection on the fourth registration request message based on the first security context includes: The UE performs integrity protection on the fourth registration request message based on the first security context, and generates a first MAC. Therefore, carrying the second registration request message in the first registration request message may also be understood as carrying the first MAC and the fourth registration request message in the first registration request message.

[00220] Further, in Case 2, that the UE determines the first registration request message includes the following steps:

[00221] Step 1:

[00222] The UE performs integrity protection on the third registration request message based on the mapped security context between the UE and the first AMF, and generates a third MAC.

[00223] Step 2:

[00224] The UE performs, based on the native security context between the UE and the second AMF, integrity protection on the third registration request message on which integrity protection is performed based on the mapped security context in the step 1, and generates the first MAC.

[00225] In this case, the first registration request message includes the third registration request message (RR3), the third MAC (MAC3), and the first MAC (MAC1). MAC3 is a MAC value obtained by performing integrity protection on RR3 by using the mapped security context. MAC1 is a MAC value obtained by performing integrity protection on RR3 and MAC3 by using the native security context. It may also be understood that the first registration request message is a message on which integrity protection is performed sequentially based on the mapped security context and the native security context.

[00226] Case 3:

[00227] The fourth registration request message is a third registration request message. The third registration request message is the registration request message sent by the UE to the first AMF in the method procedure S260 shown in FIG. 2.

[00228] In Case 3, that the UE performs integrity protection on the fourth registration request message based on the first security context includes: The UE performs integrity protection on the fourth registration request message based on the first security context, and generates a first MAC. Therefore, carrying the second registration request message in the first registration request message may also be understood as carrying the first MAC and the fourth registration request message in the first registration request message.

[00229] Further, in Case 3, that the UE determines the first registration request message includes the following steps:

[00230] Step 1:

[00231] The UE performs integrity protection on the third registration request message based on the native security context between the UE and the second AMF, and generates the first MAC.

[00232] Step 2:

[00233] The UE performs, based on a mapped security context between the UE and the first AMF, integrity protection on the third registration request message on which integrity protection is performed based on the native security context in the step 1, and generates a fourth MAC.

[00234] In this case, the first registration request message includes the third registration request message (RR3), the first MAC (MAC1), and the fourth MAC (MAC4). MAC1 is a MAC value obtained by performing integrity protection on RR3 by using the native security context. MAC4 is a MAC value obtained by performing integrity protection on RR3 and MAC1 by using the mapped security context. It may also be understood that the first registration request message is a

message on which integrity protection is performed sequentially based on the native security context and the mapped security context.

[00235] It should be understood that, in Case 1, the first AMF can determine, based on both the mapped GUITI and the native GUTI that are carried in the first registration request message sent by the UE, to send the second registration request message that is integrity protected by using the native security context to the second AMF.

[00236] It should be further understood that the foregoing Case 1 to Case 3 are merely examples to describe possible cases of the second registration request message and how the UE determines the first registration request message. Another undescribed possible form of the second registration request also falls within the protection scope of this application. For example, the fourth registration request message is another possible message constructed by the UE based on a native context.

[00237] S420: The UE sends the first registration request message to the first AMF.

[00238] Specifically, the UE sends the first registration request message determined in S410 to the first AMF.

[00239] It should be understood that the first registration request message sent by the UE to the first AMF may be forwarded by an access network device. A function of the access network device is not limited in this application. Therefore, that the first registration request message sent by the UE to the first AMF may be forwarded by the access network device is directly described as that the UE sends the first registration request message to the first AMF.

[00240] It should be further understood that, before the UE sends the first registration request message to the first AMF, the UE needs to determine the mapped security context. Therefore, before the UE sends the first registration request message to the first AMF, a method procedure shown in FIG. 4 further includes S411 to S414.

[00241] S411: The MME sends a forward relocation request message to the first AMF. This step is similar to S210 in FIG. 2, and details are not described herein again.

[00242] S412: The first AMF determines the mapped security context. This step is similar to S220 in FIG. 2, and details are not described herein again.

[00243] S413: The first AMF sends a forward relocation response message to the MME. This step is similar to S230 in FIG. 2, and details are not described herein again.

[00244] S414: The MME sends a handover command message to the UE. This step is similar

to S240 in FIG. 2, and details are not described herein again.

[00245] Specifically, after receiving the handover command message, the UE derives the mapped security context. Further, the UE performs security protection on the first registration request message by using the native security context and the mapped security context.

[00246] S430: The first AMF verifies the UE.

[00247] Specifically, that the first AMF determines that the UE is validated is mainly determining whether the first registration request message received from the UE satisfies a preset condition. That the first AMF determines that the first registration request message satisfies the preset condition includes:

the first AMF successfully validates integrity protection for the first registration request message based on the mapped security context; or

the first AMF determines that the first registration request message is a registration request message sent by the UE after the UE is handed over from a 4G communications system to a 5G communications system. For example, before receiving the first registration request message sent by the UE, the first AMF receives the forward relocation request message sent by the MME. Therefore, the first AMF can learn that the currently received first registration request message is the registration request message received from the UE in a handover procedure.

[00248] After verifying that the UE is validated, the first AMF sends the second registration request message to the second AMF, where the second registration request message is used by the second AMF to verify the UE. In other words, the method procedure shown in FIG. 4 further includes S440 in which the first AMF sends the second request message to the second AMF.

[00249] Optionally, the second registration request message is carried in a first request message, and is sent by the first AMF to the second AMF.

[00250] In a possible implementation, the first request message is a user equipment context transfer service invoking request (Namf_Communication_UEContextTransfer) initiated by the first AMF shown in FIG. 2. Different from the user equipment context transfer service invoking request shown in FIG. 2, the user equipment context transfer service invoking request in this embodiment of this application includes a newly added information element, namely, the first MAC.

[00251] In another possible implementation, the first request message is another possible first request message that is sent by the first AMF to the second AMF and that is used to obtain a

security context of the UE.

[00252] It should be understood that a specific form of the first request message is not limited in this application. The first MAC may be added to existing signaling between the first AMF and the second AMF, or may be added to signaling newly added between the first AMF and the second AMF.

[00253] Further, to enable the second AMF to determine that the first AMF needs to obtain the security context of the UE, the first request message further carries an identity of the UE. Specifically, the identity of the UE is included in the second registration request message sent by the first AMF to the second AMF.

[00254] In a possible implementation, the identity of the UE may be the mapped GUTI.

[00255] In a possible implementation, the identity of the UE may be the native GUTI.

[00256] In another possible implementation, the identity of the UE may be an SUPI.

[00257] It should be understood that, if the first AMF determines, after receiving the mapped GUTI of the UE from the UE, that the security context of the UE needs to be obtained from the second AMF, the first AMF may choose to continue to add the mapped GUTI of the UE, the SUPI of the UE, or both the mapped GUTI and the SUPI of the UE to the first request message.

[00258] It should be further understood that, when the first registration request message received by the first AMF is the first registration request message shown in Case 1 in S410, the first registration request message carries the second registration request message, and the second registration request message includes the native GUTI. In this case, the first AMF may choose to add the native GUTI of the UE to the first request message.

[00259] Further, the second registration request message further includes the UL NAS COUNT of the UE, so that the second AMF can obtain the UL NAS COUNT of the UE.

[00260] Further, after receiving the first request message sent by the first AMF, the second AMF determines, based on an integrity validation result of the second registration request message, whether the UE is validated. To be specific, the second AMF performs S450, in other words, validates integrity of the second registration request message.

[00261] The second AMF validates the integrity of the second registration request message based on the security context between the second AMF and the user equipment. For example, the second AMF generates a second MAC based on a natively stored security context, and compares the first MAC with the second MAC. When the first MAC is equal to the second MAC, the second

AMF successfully verifies the UE, and determines that the UE is validated. In this case, the second AMF sends the security context of the UE to the first AMF.

[00262] It should be understood that the first MAC is a MAC generated by the UE based on the security context of the UE that is negotiated between the UE and the second AMF, and the second MAC is a MAC generated by the second AMF based on the security context of the UE that is negotiated between the UE and the second AMF. Therefore, there is a high probability that the first MAC is equal to the second MAC. In this case, the second AMF can successfully verify the UE, and returns the security context of the UE to the first AMF, unless the second AMF fails to verify the UE due to a low-probability event such as a transmission error. Compared with the method procedure shown in FIG. 2, the security context obtaining method shown in FIG. 4 improves a possibility that the first AMF successfully obtains the security context of the user equipment from the second AMF.

[00263] After successfully validating the integrity of the second registration request message, the second AMF performs S460, in other words, sends the security context of the user UE to the first AMF.

[00264] Optionally, the security context of the UE is carried in a first response message.

[00265] Further, if the security context of the UE is included in the context of the UE, the second AMF may send the context of the UE to the first AMF.

[00266] Optionally, the second AMF can perform key derivation on a first key in the security context of the UE based on the UL NAS COUNT. In this case, a key in the security context of the UE that is returned by the second AMF to the first AMF is a second key obtained by performing key derivation on the first key. In this embodiment of this application, the security context of the UE that includes the second key generated through key derivation may be referred to as a second security context. In other words, the security context of the UE that is sent by the second AMF to the first AMF may not undergo key derivation, may be the security context of the UE that is between the second AMF and the UE and that is natively stored in the second AMF, or may be the second security context when the second AMF performs, according to a local policy, key derivation on a key in the natively stored security context of the UE that is between the second AMF and the UE, to generate a derived key.

[00267] Specifically, when the key in the security context of the UE that is sent by the second AMF to the first AMF is the second key, the second AMF further needs to send key derivation

indication information to the first AMF, to indicate that the second key is a key obtained through key derivation.

[00268] It should be understood that a procedure after the first AMF obtains the security context of the UE is similar to a procedure after the first AMF obtains the security context of the UE in an existing procedure of handing over the UE from the 4G communications system to the 5G communications system. For details, refer to the existing procedure. Details are not described herein again.

[00269] For example, the UE and the first AMF subsequently negotiate to use the native security context. Specifically, the first AMF sends a non-access stratum security mode command (non-access stratum secure mode command, NAS SMC) message to the UE, and the UE validates integrity of the NAS SMC message. After the UE successfully validates the NAS SMC message, the UE sends a non-access stratum security mode complete (non-access layer security mode complete) message to the first AMF.

[00270] In a possible implementation, when the second AMF fails to validate the integrity of the second registration request message, the second AMF sends failure indication information to the first AMF, to notify the first AMF that the second AMF fails to validate the integrity of the second registration request message.

[00271] Further, after the first AMF receives the failure indication information indicating that the second AMF fails to validate the integrity of the second registration request message, the first AMF determines, according to a local policy, that the first AMF may continue to use the mapped security context, or the first AMF determines to initiate initial authentication to the UE according to a local policy, and generates a new security context between the first AMF and the UE.

[00272] It should be understood that sequence numbers of the foregoing processes do not mean execution sequences in the foregoing method embodiments. The execution sequences of the processes should be determined based on functions and internal logic of the processes, and should not be construed as any limitation on the implementation processes of the embodiments of this application.

[00273] The security context obtaining methods in the embodiments of this application are described above in detail with reference to FIG. 3 and FIG. 4. The following describes in detail security context obtaining apparatuses in the embodiments of this application with reference to FIG. 5 to FIG. 10.

[00274] FIG. 5 is a schematic diagram of a security context obtaining apparatus 50 according to this application. As shown in FIG. 5, the apparatus 50 includes a sending unit 510, a processing unit 520, and a receiving unit 530.

[00275] The sending unit 510 is configured to send a first registration request message to a first AMF.

[00276] The processing unit 520 is configured to determine the first registration request message.

[00277] The receiving unit 530 is configured to receive a handover command message sent by an MME.

[00278] The apparatus 50 completely corresponds to the user equipment in the method embodiments. The apparatus 50 may be the user equipment in the method embodiments, or a chip or a functional module inside the user equipment in the method embodiments. The corresponding units of the apparatus 50 are configured to perform corresponding steps performed by the user equipment in the method embodiments shown in FIG. 3 and FIG. 4.

[00279] The sending unit 510 of the apparatus 50 performs a sending step performed by the user equipment in the method embodiments. For example, the sending unit 510 performs the step S316 of sending the registration request message to the first AMF in FIG. 3 and the step S420 of sending the first registration request message to the first AMF in FIG. 4.

[00280] The processing unit 520 performs a step implemented or processed inside the user equipment in the method embodiments. For example, the processing unit 520 performs the step S315 of determining the mapped security context in FIG. 3 and the step S410 of determining the first registration request message in FIG. 4.

[00281] The receiving unit 530 performs a receiving step performed by the user equipment in the method embodiments. For example, the receiving unit 530 performs the step S314 of receiving the handover command message sent by the MME in FIG. 3 and the step S414 of receiving the handover command message sent by the MME in FIG. 4.

[00282] The sending unit 510 and the receiving unit 530 shown in the apparatus 50 may constitute a transceiver unit that has both receiving and sending functions. The processing unit 520 may be a processor. The sending unit 510 may be a transmitter, and the receiving unit 530 may be a receiver. The receiver and the transmitter may be integrated to constitute a transceiver.

[00283] FIG. 6 is a schematic structural diagram of user equipment 60 applicable to an

embodiment of this application. The user equipment 60 may be applied to the system shown in FIG. 1. For ease of description, FIG. 6 shows only main components of the user equipment. As shown in FIG. 6, the user equipment 60 includes a processor (corresponding to the processing unit 520 in FIG. 5), a memory, a control circuit, an antenna, and an input/output apparatus (corresponding to the sending unit 510 and the receiving unit 530 in FIG. 5). The processor is configured to control the antenna and the input/output apparatus to send and receive a signal. The memory is configured to store a computer program. The processor is configured to invoke the computer program from the memory and run the computer program, to perform a corresponding procedure and/or operation performed by the user equipment in the security context obtaining methods provided in this application. Details are not described herein again.

[00284] A person skilled in the art may understand that, for ease of description, FIG. 6 shows only one memory and only one processor. Actual user equipment may have a plurality of processors and a plurality of memories. The memory may also be referred to as a storage medium, a storage device, or the like. This is not limited in this embodiment of this application.

[00285] FIG. 7 is a schematic diagram of a security context obtaining apparatus 70 according to this application. As shown in FIG. 7, the apparatus 70 includes a receiving unit 710, a processing unit 720, and a sending unit 730.

[00286] The receiving unit 710 is configured to receive a first registration request message sent by user equipment, where the first registration request message carries a second registration request message, the second registration request message is integrity protected using a first security context, the first security context is a native security context between the user equipment and a second AMF, and a first AMF is an AMF providing an access and mobility management service for the user equipment after the user equipment is handed over from a 4G communications system to a 5G communications system.

[00287] The processing unit 720 is configured to determine a mapped security context.

[00288] The sending unit 730 is configured to send the second registration request message to the second AMF.

[00289] The apparatus 70 completely corresponds to the first AMF in the method embodiments. The apparatus 70 may be the first AMF in the method embodiments, or a chip or a functional module inside the first AMF in the method embodiments. The corresponding units of the apparatus 70 are configured to perform corresponding steps performed by the first AMF in the method

embodiments shown in FIG. 3 and FIG. 4.

[00290] The receiving unit 710 of the apparatus 70 performs a receiving step performed by the first AMF in the method embodiments. For example, the receiving unit 710 performs the step S311 of receiving the forward relocation request message sent by the MME in FIG. 3, the step S411 of receiving the forward relocation request message sent by the MME in FIG. 4, the step S316 of receiving the registration request message sent by the UE in FIG. 3, the step S420 of receiving the first registration request message sent by the UE in FIG. 3, the step S330 of receiving the second response message sent by the second AMF in FIG. 3, and the step S460 of receiving the security context of the UE that is sent by the second AMF in FIG. 4.

[00291] The processing unit 720 performs a step implemented or processed inside the first AMF in the method embodiments. For example, the processing unit 720 performs the step S312 of determining the mapped security context in FIG. 3, the step S412 of determining the mapped security context in FIG. 4, the step S317 of verifying the UE in FIG. 3, and the step S430 of verifying the UE in FIG. 4.

[00292] The sending unit 730 performs a sending step performed by the first AMF in the method embodiments. For example, the sending unit 730 performs the step S313 of sending the forward relocation response message to the MME in FIG. 3, the step S413 of sending the forward relocation response message to the MME in FIG. 4, the step S310 of sending the second request message to the second AMF in FIG. 3, and the step S440 of sending the second registration request message to the second AMF in FIG. 4.

[00293] The receiving unit 710 and the sending unit 730 may constitute a transceiver unit that has both receiving and sending functions. The processing unit 720 may be a processor. The sending unit 730 may be a transmitter. The receiving unit 710 may be a receiver. The receiver and the transmitter may be integrated to constitute a transceiver.

[00294] As shown in FIG. 8, an embodiment of this application further provides a first AMF 80. The first AMF 80 includes a processor 810, a memory 820, and a transceiver 830. The memory 820 stores an instruction or a program, and the processor 830 is configured to execute the instruction or the program stored in the memory 820. When the instruction or the program stored in the memory 820 is executed, the transceiver 830 is configured to perform operations performed by the receiving unit 710 and the sending unit 730 in the apparatus 70 shown in FIG. 7.

[00295] FIG. 9 is a schematic diagram of a security context obtaining apparatus 90 according

to this application. As shown in FIG. 9, the apparatus 90 includes a receiving unit 910, a processing unit 920, and a sending unit 930.

[00296] The receiving unit 910 is configured to receive a second registration request message sent by a first AMF, where the second registration request message is integrity protected using a first security context, and the first security context is a native security context between a user equipment and a second AMF.

[00297] The processing unit 920 is configured to validate integrity of the second registration request message.

[00298] The sending unit 930 is configured to: when the processing unit 920 successfully validates the integrity of the second registration request message, send a security context of the user equipment to the first AMF.

[00299] The apparatus 90 completely corresponds to the second AMF in the method embodiments. The apparatus 90 may be the second AMF in the method embodiments, or a chip or a functional module inside the second AMF in the method embodiments. The corresponding units of the apparatus 90 are configured to perform corresponding steps performed by the second AMF in the method embodiments shown in FIG. 3 and FIG. 4.

[00300] The receiving unit 910 of the apparatus 90 performs a receiving step performed by the second AMF in the method embodiments. For example, the receiving unit 910 performs the step S310 of receiving the second request message sent by the first AMF in FIG. 3 and the step S440 of receiving the second registration request message sent by the first AMF in FIG. 4.

[00301] The processing unit 920 performs a step implemented or processed inside the second AMF in the method embodiments. For example, the processing unit 920 performs the step S320 of determining that the UE does not need to be verified in FIG. 3 and the step S450 of validating the integrity of the second registration request message in FIG. 4.

[00302] The sending unit 930 performs a sending step performed by the second AMF in the method embodiments. For example, the sending unit 930 performs the step S330 of sending the second response message to the first AMF in FIG. 3 and the step S460 of sending the security context of the UE to the first AMF in FIG. 4.

[00303] The receiving unit 910 and the sending unit 930 may constitute a transceiver unit that has both receiving and sending functions. The processing unit 920 may be a processor. The sending unit 930 may be a transmitter, and the receiving unit 910 may be a receiver. The receiver and the

transmitter may be integrated to constitute a transceiver.

[00304] As shown in FIG. 10, an embodiment of this application further provides a second AMF 100. The second AMF 100 includes a processor 1010, a memory 1020, and a transceiver 1030. The memory 1020 stores an instruction or a program, and the processor 1030 is configured to execute the instruction or the program stored in the memory 1020. When the instruction or the program stored in the memory 1020 is executed, the transceiver 1030 is configured to perform operations performed by the receiving unit 910 and the sending unit 930 in the apparatus 90 shown in FIG. 9.

[00305] An embodiment of this application further provides a computer-readable storage medium. The computer-readable storage medium stores an instruction. When the instruction is run on a computer, the computer is enabled to perform steps performed by the first AMF in the methods shown in FIG. 3 and FIG. 4.

[00306] An embodiment of this application further provides a computer-readable storage medium. The computer-readable storage medium stores an instruction. When the instruction is run on a computer, the computer is enabled to perform steps performed by the second AMF in the methods shown in FIG. 3 and FIG. 4.

[00307] An embodiment of this application further provides a computer program product that includes an instruction. When the computer program product runs on a computer, the computer is enabled to perform steps performed by the first AMF in the methods shown in FIG. 3 and FIG. 4.

[00308] An embodiment of this application further provides a computer program product that includes an instruction. When the computer program product runs on a computer, the computer is enabled to perform steps performed by the second AMF in the methods shown in FIG. 3 and FIG. 4.

[00309] An embodiment of this application further provides a chip, including a processor. The processor is configured to read a computer program stored in a memory and run the computer program, to perform a corresponding operation and/or procedure performed by the second AMF in the security context obtaining methods provided in this application. Optionally, the chip further includes the memory. The memory is connected to the processor through a circuit or a cable. The processor is configured to read the computer program from the memory and execute the computer program. Optionally, the chip further includes a communications interface. The processor is connected to the communications interface. The communications interface is configured to receive

data and/or information that needs to be processed. The processor obtains the data and/or information from the communications interface, and processes the data and/or information. The communications interface may be an input/output interface.

[00310] This application further provides a chip, including a processor. The processor is configured to invoke a computer program stored in a memory and run the computer program, to perform a corresponding operation and/or procedure performed by the first AMF in the security context obtaining methods provided in this application. Optionally, the chip further includes the memory. The memory is connected to the processor through a circuit or a cable. The processor is configured to read the computer program from the memory and execute the computer program. Optionally, the chip further includes a communications interface. The processor is connected to the communications interface. The communications interface is configured to receive data and/or information that needs to be processed. The processor obtains the data and/or information from the communications interface, and processes the data and/or information. The communications interface may be an input/output interface.

[00311] A person of ordinary skill in the art may be aware that, in combination with the examples described in the embodiments disclosed in this specification, units and algorithm steps may be implemented by electronic hardware or a combination of computer software and electronic hardware. Whether the functions are performed by hardware or software depends on particular applications and design constraints of the technical solutions. A person skilled in the art may use different methods to implement the described functions for each particular application, but it should not be considered that the implementation goes beyond the scope of this application.

[00312] It may be clearly understood by a person skilled in the art that, for the purpose of convenient and brief description, for detailed working processes of the foregoing system, apparatus, and unit, refer to corresponding processes in the foregoing method embodiments, and details are not described herein again.

[00313] In the several embodiments provided in this application, it should be understood that the disclosed system, apparatus, and method may be implemented in other manners. For example, the described apparatus embodiment is merely an example. For example, division into the units is merely logical function division and may be other division in actual implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings

or direct couplings or communication connections may be implemented by using some interfaces. The indirect couplings or communication connections between the apparatuses or units may be implemented in electrical, mechanical, or other forms.

[00314] The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be distributed on a plurality of network units. Some or all of the units may be selected based on actual requirements to achieve the objectives of the solutions of the embodiments.

[00315] In addition, functional units in the embodiments of this application may be integrated into one processing unit, or each of the units may exist alone physically, or two or more units are integrated into one unit.

[00316] When the functions are implemented in a form of a software functional unit and sold or used as an independent product, the functions may be stored in a computer-readable storage medium. Based on such an understanding, the technical solutions of this application essentially, or the part contributing to the prior art, or some of the technical solutions may be implemented in a form of a software product. The software product is stored in a storage medium, and includes several instructions for instructing a computer device (which may be a personal computer, a server, a network device, or the like) to perform all or some of the steps of the methods described in the embodiments of this application. The foregoing storage medium includes: any medium that can store program code, such as a USB flash drive, a removable hard disk, a read-only memory (Read-Only Memory, ROM), a random access memory ((R)ANdom Access Memory, RAM), a magnetic disk, or an optical disc.

[00317] In addition, the term "and/or" in this application describes only an association relationship for describing associated objects and represents that three relationships may exist. For example, A and/or B may represent the following three cases: Only A exists, both A and B exist, and only B exists. In addition, the character "/" in this specification generally indicates an "or" relationship between the associated objects. The term "at least one" in this application may represent "one" and "two or more". For example, at least one of A, B, and C may represent: Only A exists, only B exists, only C exists, both A and B exist, and both A and C exist, C and B exist, and A, B, and C exist.

[00318] The foregoing descriptions are merely specific implementations of this application, but are not intended to limit the protection scope of this application. Any variation or replacement

readily figured out by a person skilled in the art within the technical scope disclosed in this application shall fall within the protection scope of this application. Therefore, the protection scope of this application shall be subject to the protection scope of the claims.

CLAIMS

What is claimed is:

1. A security context obtaining method, wherein the method comprises:

receiving, by a first access and mobility management function, AMF, a first registration request message sent by user equipment, UE;

validating, by the first AMF, integrity protection for the first registration request message;

if the first AMF successfully validates integrity protection for the first registration request message, sending, by the first AMF, a second request message to a second AMF;

receiving, by the second AMF, the second request message; and

if the second request message carries indication information and the indication information is used to indicate that the UE is validated, sending, by the second AMF, a security context of the UE to the first AMF.

2. The method according to claim 1, wherein the method further comprises:

sending, by a mobility management network element, MME, a forward relocation request message to the first AMF, wherein the forward relocation request message comprises a security context between the UE and the MME;

determining, by the first AMF, a mapped security context based on the security context between the user equipment and the MME; and

the validating, by the first AMF, integrity protection for the first registration request message comprises:

validating, by the first AMF, integrity protection for the first registration request message by using the mapped security context.

3. The method according to claim 1, wherein the first registration request message further comprises an identity 5G-GUTI of the user equipment.

4. The method according to claim 3, wherein the indication information is the 5G-GUTI.

5. The method according to claim 1, wherein the indication information is a reason value.

6. A security context obtaining system, wherein the system comprises a first access and mobility management function, AMF, and a second AMF;

the first AMF is configured to: receive a first registration request message sent by user equipment UE; validate integrity protection for the first registration request message; and if

successfully validating integrity protection for the first registration request message, send a second request message to the second AMF; and

the second AMF is configured to: receive the second request message; and if the second request message carries indication information and the indication information is used to indicate that the UE is validated, send a security context of the UE to the first AMF.

7. The system according to claim 6, wherein the system further comprises a mobility management network element MME;

the MME is configured to send a forward relocation request message to the first AMF, wherein the forward relocation request message comprises a security context between the UE and the MME; and

the first AMF is further configured to determine a mapped security context based on the security context between the user equipment and the MME; wherein

the validating integrity protection for the first registration request message comprises:

validating integrity protection for the first registration request message by using the mapped security context.

8. The system according to claim 6, wherein the first registration request message further comprises an identity 5G-GUTI of the user equipment.

9. A security context obtaining method, wherein the method comprises:

receiving, by a first access and mobility management function, AMF, a first registration request message sent by user equipment UE;

validating, by the first AMF, integrity protection for the first registration request message; and

if the first AMF successfully validates integrity protection for the first registration request message, sending, by the first AMF, a second request message to a second AMF, wherein the second request message carries indication information and the indication information is used to indicate that the UE is validated.

10. The method according to claim 9, wherein the method further comprises:

receiving, by the first AMF, a forward relocation request message sent by a mobility management network element MME, wherein the forward relocation request message comprises a security context between the user equipment and the MME;

determining, by the first AMF, a mapped security context based on the security context

between the UE and the MME; and

the validating, by the first AMF, integrity protection for the first registration request message comprises:

validating, by the first AMF, integrity protection for the first registration request message by using the mapped security context.

11. The method according to claim 9, wherein the first registration request message further comprises an identity 5G-GUTI of the user equipment.

12. The method according to claim 9, wherein the first registration request message is sent after the UE completed handover procedure.

13. The method according to claim 9, wherein the method further comprises:

the second AMF skipping authentication on the UE.

14. The method according to claim 9, wherein the second registration request message further comprises an identity 5G-GUTI of the UE.

15. The method according to claim 9, wherein the UE is connected state.

16. The method according to claim 9, wherein the first registration request message is integrity protected by the mapped security context.

17. The method according to claim 9, wherein the 5G GUTI is configured by the second AMF for the UE.

18. The method according to claim 9, wherein the method further comprises:

if the first AMF unsuccessfully validates integrity protection for the first registration request message, the first AMF continues to use the mapped security context generated through negotiation with the UE, or the first AMF initiates initial authentication to the UE to generate a security context between the first AMF and the UE.

19. The method according to claim 9, wherein the method further comprises:

if the first AMF unsuccessfully validates integrity protection for the first registration request message, the first AMF can not receive a security context of the UE from the second AMF.

20. A security context obtaining method, wherein the method comprises:

receiving, by a second access and mobility management function AMF, a request message sent by a first AMF; and

if the request message carries indication information and the indication information is used to indicate that user equipment UE is validated, sending, by the second AMF, a security context of

the UE to the first AMF.

21. The method according to claim 20, wherein before the sending, by the second AMF, a security context of the UE to the first AMF, the method further comprises:

skipping, by the second AMF, authentication on the UE.

22. A communications apparatus, wherein the apparatus comprises a processor, a memory, and a transceiver; the memory stores an instruction, and the processor is coupled to the transceiver; and when the instruction stored in the memory is executed, the processor performs the following operations:

receiving a first registration request message sent by user equipment, UE;

validating integrity protection for the first registration request message; and

if successfully validating integrity protection for the first registration request message, sending a second request message to a second AMF, wherein the second request message carries indication information and the indication information is used to indicate that the UE is validated.

23. The communications apparatus according to claim 22, wherein the processor further performs the following operations:

receiving a forward relocation request message sent by a mobility management network element MME, wherein the forward relocation request message comprises a security context between the user equipment and the MME;

determining a mapped security context based on the security context between the UE and the MME; and

the validating integrity protection for the first registration request message comprises: validating integrity protection for the first registration request message by using the mapped security context.

24. A communications apparatus, wherein the apparatus comprises a processor, a memory, and a transceiver; the memory stores an instruction, and the processor is coupled to the transceiver; and when the instruction stored in the memory is executed, the processor performs the following operations:

receiving a request message sent by a first AMF; and

if the request message carries indication information and the indication information is used to indicate that user equipment UE is validated, sending a security context of the UE to the first AMF.

25. The communications apparatus according to claim 24, wherein the processor further performs the following operation:

skipping authentication on the UE.