METHOD FOR PROTECTING TERMINAL PARAMETER UPDATE AND COMMUNICATION APPARATUS

TECHNICAL FIELD

[0001] This application relates to the field of terminal parameters security technologies, and in particular, to a method for protecting terminal parameters update and a communication apparatus.

~~**[0001]**~~**[0002]**

BACKGROUND

~~**[0002]**~~**[0003]** In a new radio (new radio, NR) network system, there are multiple network entities capable of performing different network functions. For example, the NR system includes a visited public land mobile network (visited public land mobile network, VPLMN) and a home public land mobile network (home public land mobile network, HPLMN). In a communication process, an HPLMN entity sends some configuration parameters to a terminal. In the sending process, the HPLMN entity needs to send the configuration parameters to the terminal via a VPLMN entity. For example, a unified data management (unified data management, UDM) entity in the HPLMN needs to send updated subscription data to the terminal via an access and mobility management function (access and mobility management function, AMF) entity in the VPLMN. For another example, a policy control function (policy control function, PCF) entity in the HPLMN needs to send policy information to the terminal sequentially via a PCF entity and an AMF entity in the VPLMN.

~~**[0003]**~~**[0004]** It can be learned that a parameter to be sent by an HPLMN entity to the terminal can be forwarded only via a VPLMN entity. However, the parameter may be intercepted or tampered with by the VPLMN entity in the forwarding process, causing security risks. In view of this, the UDM requests an authentication service function (authentication server function, AUSF) entity in the HPLMN to protect a configuration parameter or an updated subscription parameter, or the like transmitted between the HPLMN and the terminal. To be specific, the UDM requests

the AUSF entity to encrypt the parameter, and then sends the encrypted parameter to the terminal via the AMF entity.

~~[0004]~~[0005] The AUSF may protect the foregoing parameter using a key generated in an authentication process of the terminal, and the terminal verifies, using the key generated in the authentication process, the foregoing parameter sent by the AUSF. However, in a dual-registration scenario, that is, in a scenario in which the terminal registers with two serving networks, multiple keys exist in one AUSF. If the AUSF randomly selects a key to encrypt the parameter, the key selected by the AUSF is inconsistent with the key generated in the authentication process of the terminal. As a result, the terminal's verification of the parameter fails.

SUMMARY

~~[0005]~~[0006] This application provides a method for protecting terminal parameters update and a communication apparatus, to ensure security of a parameter sent by an HPLMN to a terminal in a transmission process.

~~[0006]~~[0007] According to a first aspect, an embodiment of this application provides a method for protecting terminal parameters update. The method may be performed by a first communication apparatus. The first communication apparatus may be a communication device or a communication apparatus supporting a communication device in implementing functions required by the method, for example, a chip system. The following provides descriptions by using an example in which the communication device is a UDM entity. The method includes:

~~[0007]~~[0008] The UDM sends a protection request message to a first AUSF. Then, the UDM receives a response message that is of the protection request message and that is sent by the first AUSF, and sends terminal parameters update information via an AMF corresponding to a first serving network. The protection request message requests to protect the terminal parameters update information, and the protection request message carries the terminal parameters update information and information about the first serving network.

~~[0008]~~[0009] In this embodiment of this application, the protection request message that is for protecting the terminal parameters update information and that is sent by the UDM to the first AUSF carries information (namely, the information about the first serving network) for identifying the first serving network. Therefore, the first AUSF may select, based on the information about the

first serving network, a first key (which may also be considered as an authentication service function key, and is briefly referred to as a key below) corresponding to the first serving network, to encryption protect the terminal parameters update information. In this way, even if a terminal registers with a home network (home network, HN) via multiple serving networks, that is, when an AUSF corresponds to multiple keys, a key used by the first AUSF can be specified using this solution. This ensures that the terminal successfully verifies the terminal parameters update information that is sent by the HPLMN via the AMF.

~~[0009]~~[0010] In a possible implementation, before the UDM sends the protection request message to the first AUSF, the UDM determines the information about the first serving network according to a local policy. In this solution, the UDM may specify, for the first AUSF, the first serving network for a subsequent terminal parameters update procedure, that is, the UDM specifies a key to be used by the first AUSF, to ensure that, when the terminal is in a dual-registration mode (when the terminal registers with at least two serving networks), a key selected by the first AUSF is consistent with a key generated in an authentication process of the terminal even if AMFs in the at least two serving networks select a same AUSF.

~~[0010]~~[0011] In another possible implementation, when determining that there are multiple serving networks, the UDM determines the first serving network for the terminal parameters update procedure. In this solution, the UDM determines the first serving network only when determining that there are multiple serving networks, to avoid determining, in a case in which the terminal registers with one serving network, the first serving network for a SoR procedure, that is, avoid performing an unnecessary step.

~~[0011]~~[0012] In a possible implementation, the method further includes: The UDM determines the first AUSF based on the information about the first serving network. In this solution, when the terminal registers with the HN sequentially via multiple different serving networks, and the different serving networks select different AUSFs, the UDM specifies the first AUSF to protect SoR information. Because one AUSF corresponds to one key, this can ensure that a key selected by the first AUSF is consistent with the key generated in the authentication process of the terminal.

~~[0012]~~[0013] In a possible implementation, before sending the protection request message to the first AUSF, the UDM may further determine that the first AUSF includes authentication results for the terminal in multiple serving networks, where the multiple serving networks include the first serving network; or the UDM may determine that the terminal is in multiple serving networks,

where the multiple serving networks include the first serving network; or the UDM may determine that the terminal is in a dual-registration mode, that is, the terminal registers with the HN via two serving networks. The solution may include: When determining that multiple keys exist (for example, one AUSF corresponds to multiple keys or there are multiple AUSFs (each AUSF corresponds to a key)), the UDM specifies a key based on the information about the first serving network, so that the key selected by the first AUSF is consistent with the key generated in the authentication process of the terminal. This can prevent the sent protection request message from carrying unnecessary information about the first serving network.

~~[0013]~~[0014] In a possible implementation, for example, the information about the first serving network includes a name of the first serving network. For another example, the information about the first serving network includes a public land mobile network (public land mobile network, PLMN) identifier ID of the first serving network or an ID of the first serving network. For another example, the information about the first serving network includes an authentication event identifier of the terminal. The foregoing lists only four implementations of the information about the first serving network. It should be understood that a specific implementation of the information about the first serving network is not limited in this embodiment of this application, provided that the information can identify the first serving network.

~~[0014]~~[0015] In a possible implementation, the terminal parameters update information includes steering of roaming (steering of roaming, SoR) information.

~~[0015]~~[0016] According to a second aspect, an embodiment of this application provides a method for protecting terminal parameters update. The method may be performed by a second communication apparatus. The second communication apparatus may be a communication device or a communication apparatus supporting a communication device in implementing functions required by the method, for example, a chip system. The following provides descriptions by using an example in which the communication device is an AUSF entity. The method includes:

~~[0016]~~[0017] A first AUSF receives a protection request message sent by a UDM, where the protection request message requests to protect terminal parameters update information, the protection request message carries the parameters update information and information about a first serving network, and the protection request message requests to protect the terminal parameters update information. Then, the first AUSF determines a first key based on the information about the first serving network, where the first key is for protecting the terminal parameters update

information, and security protects the terminal parameters update information based on the first key.

~~[0017]~~[0018] In a possible implementation, the information about the first serving network is information about one of multiple first serving networks that is stored by the UDM.

~~[0018]~~[0019] In a possible implementation, there are multiple AUSFs, and the first AUSF is an AUSF corresponding to the information about the first serving network.

~~[0019]~~[0020] In a possible implementation, the first AUSF includes authentication results for a terminal in multiple serving networks, where the multiple serving networks include the first serving network; the terminal is in multiple serving networks, where the multiple serving networks include the first serving network; or the terminal is in a dual-registration mode.

~~[0020]~~[0021] In a possible implementation, the information about the first serving network includes a name of the first serving network; or

the information about the first serving network includes a PLMN ID of the first serving network, or the information about the first serving network includes an authentication event identifier of the terminal.

~~[0021]~~[0022] In a possible implementation, the terminal parameters update information includes steering of roaming (steering of roaming, SoR) information.

~~[0022]~~[0023] For technical effects achieved by the second aspect or the possible implementations of the second aspect, refer to the descriptions of the technical effects of the first aspect or the possible implementations of the first aspect.

~~[0023]~~[0024] According to a third aspect, an embodiment of this application provides a method for protecting terminal parameters update. The method may be performed by a third communication apparatus. The third communication apparatus may be a communication device or a communication apparatus supporting a communication device in implementing functions required by the method, for example, a chip system. The following provides descriptions by using an example in which the communication device is a UDM entity. The method includes:

~~[0024]~~[0025] The UDM sends a first message to a first AUSF, where the first message indicates the first AUSF to delete a first key used when a terminal registers with a first serving network in which a first AMF is located, and the first AUSF is an AUSF for authentication when the terminal registers with the first serving network. Then, when determining that the terminal is in a single-registration mode, the UDM determines to send terminal parameters update information via a

second AMF.

~~[0025]~~[0026] In this embodiment of this application, the UDM may indicate the AUSF to delete the first key used when the terminal registers with the first serving network in which the first AMF is located. In this way, even if the terminal registers with a second serving network in which the second AMF is located, it can be still ensured that a key in the AUSF is unique, that is, the key is consistent with a key in an authentication process of the terminal.

~~[0026]~~[0027] In a possible implementation, when the UDM sends a second message to the first AMF or receives a third message sent by the first AMF, the UDM sends the first message to the first AUSF, where the second message is for deleting registration information of the terminal, and the third message is a response message of the second message. In this solution, when the terminal registers with the second serving network in which the second AMF is located, the UDM may send the first message to the first AUSF. This ensures that the terminal is in the single-registration mode, and ensures that the key in the first AUSF is unique.

~~[0027]~~[0028] In a possible implementation, the first message carries identification information of the first serving network or identification information of the terminal.

~~[0028]~~[0029] According to a fourth aspect, an embodiment of this application provides a method for protecting terminal parameters update. The method may be performed by a fourth communication apparatus. The fourth communication apparatus may be a communication device or a communication apparatus supporting a communication device in implementing functions required by the method, for example, a chip system. The following provides descriptions by using an example in which the communication device is an AUSF entity. The method includes:

~~[0029]~~[0030] A first AUSF receives a first message sent by a UDM, where the first message indicates the first AUSF to delete a first key used by a terminal when the terminal registers with a first serving network in which a first AMF is located, and the first AUSF is an AUSF for authentication when the terminal registers with the first serving network. Then, the first AUSF deletes the first key used when the terminal registers with the first serving network in which the first AMF is located.

~~[0030]~~[0031] In a possible implementation, the first message carries identification information of the first serving network or identification information of the terminal.

~~[0031]~~[0032] For technical effects achieved by the fourth aspect or the possible implementations of the fourth aspect, refer to the descriptions of the technical effects of the third

aspect or the possible implementations of the third aspect.

~~[0032]~~[0033] According to a fifth aspect, a communication apparatus is provided. For example, the communication apparatus is the foregoing UDM. The communication apparatus has functions of implementing behavior in the method embodiment in the first aspect. The functions may be implemented by hardware or may be implemented by hardware executing corresponding software. The hardware or software includes one or more modules corresponding to the functions. In a possible design, the communication apparatus includes, for example, a processing module and a transceiver module coupled to each other. The transceiver module is configured to: send a protection request message to a first AUSF, and receive a response message that is of the protection request message and that is sent by the first AUSF, where the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first serving network. The processing module is configured to control the transceiver module to send the parameters update information via an AMF corresponding to the first serving network.

~~[0033]~~[0034] In a possible implementation, the transceiver module is further configured to: before sending the protection request message to the first AUSF, determine the information about the first serving network according to a local policy.

~~[0034]~~[0035] In a possible implementation, the processing module is specifically configured to: when determining that there are multiple serving networks, determine the first serving network for terminal parameters update.

~~[0035]~~[0036] In a possible implementation, the processing module is specifically configured to determine the first AUSF based on the information about the first serving network.

~~[0036]~~[0037] In a possible implementation, the processing module is specifically configured to: before the protection request message is sent to the first AUSF, determine that

the first AUSF includes authentication results for the terminal in multiple serving networks, where the multiple serving networks include the first serving network;

the terminal is in multiple serving networks, where the multiple serving networks include the first serving network; or

the terminal is in a dual-registration mode.

~~[0037]~~[0038] In a possible implementation, the information about the first serving network includes a name of the first serving network;

the information about the first serving network includes a PLMN identifier ID of the first serving network or an ID of the first serving network; or

the information about the first serving network includes an authentication event identifier of the terminal.

~~[0038]~~[0039] In a possible implementation, the parameters update information includes SoR information.

~~[0039]~~[0040] According to a sixth aspect, a communication apparatus is provided. For example, the communication apparatus is the AUSF described above. The communication apparatus has functions of implementing behavior in the method embodiment in the second aspect. The functions may be implemented by hardware or may be implemented by hardware executing corresponding software. The hardware or software includes one or more modules corresponding to the functions. In a possible design, the communication apparatus includes, for example, a processing module and a transceiver module coupled to each other. The transceiver module is configured to receive a protection request message sent by a UDM, where the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first serving network. The processing module is configured to: determine a first key based on the information about the first serving network, and security protect the parameters update information based on the first key, where the first key is for protecting the parameters update information.

~~[0040]~~[0041] In a possible implementation, the information about the first serving network is information about one of multiple first serving networks that is stored by the UDM.

~~[0041]~~[0042] In a possible implementation, there are multiple AUSFs, and the first AUSF is an AUSF corresponding to the information about the first serving network.

~~[0042]~~[0043] In a possible implementation, the first AUSF includes authentication results for a terminal in multiple serving networks, where the multiple serving networks include the first serving network;

the terminal is in multiple serving networks, where the multiple serving networks include the first serving network; or

the terminal is in a dual-registration mode.

~~[0043]~~[0044] In a possible implementation, the information about the first serving network includes a name of the first serving network;

the information about the first serving network includes a PLMN identifier of the first serving network; or

the information about the first serving network includes an authentication event identifier of the terminal.

~~[0044]~~[0045] In a possible implementation, the parameters update information includes steering of roaming SoR information.

~~[0045]~~[0046] According to a seventh aspect, a communication apparatus is provided. For example, the communication apparatus is the foregoing UDM. The communication apparatus has functions of implementing behavior in the method embodiment in the third aspect. The functions may be implemented by hardware or may be implemented by hardware executing corresponding software. The hardware or software includes one or more modules corresponding to the function. In a possible design, the communication apparatus includes, for example, a processing module and a transceiver module coupled to each other. The transceiver module is configured to send a first message to a first AUSF, where the first message indicates the first AUSF to delete a first key used when a terminal registers with a first serving network in which a first AMF is located, and the first AUSF is an AUSF for authentication when the terminal registers with a first serving network. The processing module is configured to: when determining that the terminal is in a single-registration mode, determine to send terminal parameters update information via a second AMF.

~~[0046]~~[0047] In a possible implementation, the transceiver module is specifically configured to: when sending a second message to the first AMF or receiving a third message sent by the first AMF, send the first message to the first AUSF, where the second message is for deleting registration information of the terminal, and the third message is a response message of the second message.

~~[0047]~~[0048] In a possible implementation, the first message carries identification information of the first serving network or identification information of the terminal.

~~[0048]~~[0049] According to an eighth aspect, a communication apparatus is provided. For example, the communication apparatus is the AUSF described above. The communication apparatus has functions of implementing behavior in the method embodiment in the fourth aspect. The functions may be implemented by hardware or may be implemented by hardware executing corresponding software. The hardware or software includes one or more modules corresponding to the functions. In a possible design, the communication apparatus includes, for example, a

processing module and a transceiver module coupled to each other. The transceiver module is configured to receive a first message sent by a UDM, where the first message indicates a first AUSF to delete a first key used when a terminal registers with a first serving network in which a first AMF is located, and the first AUSF is an AUSF for authentication when the terminal registers with the first serving network. The processing module is configured to delete the first key used when the terminal registers with the first serving network in which the first AMF is located.

~~[0049]~~[0050] In a possible implementation, the first message carries identification information of the first serving network or identification information of the terminal.

~~[0050]~~[0051] According to a ninth aspect, a communication apparatus is provided. The communication apparatus may be the UDM in the foregoing method embodiments or a chip deployed in the UDM. Alternatively, the communication apparatus may be the AUSF in the foregoing method embodiments or a chip deployed in the AUSF. The communication apparatus includes a communication interface and a processor. Optionally, the communication apparatus further includes a memory. The memory is configured to store a computer program or instructions. The processor is coupled to the memory and the communication interface. When the processor executes the computer program or the instructions, the communication apparatus is enabled to perform the method performed by the corresponding functional entity in the foregoing method embodiments. For example, when the processor executes the computer program or the instructions, the communication apparatus is enabled to perform the method performed by the UDM in the foregoing method embodiments. For another example, when the processor executes the computer program or the instructions, the communication apparatus is enabled to perform the method performed by the AUSF in the foregoing method embodiments.

~~[0051]~~[0052] The communication interface in the communication apparatus in the ninth aspect may be a transceiver in the communication apparatus. For example, the communication interface is implemented using an antenna, a feeder, a codec, and the like in the communication apparatus. Alternatively, if the communication apparatus is a chip deployed in the communication apparatus, the communication interface may be an input/output interface of the chip, for example, an input/output pin.

~~[0052]~~[0053] According to a tenth aspect, a communication system is provided. The communication system includes any communication apparatus in the fifth aspect and any communication apparatus in the sixth aspect, or includes any communication apparatus in the

seventh aspect and any communication apparatus in the eighth aspect.

~~[0053]~~[0054] According to an eleventh aspect, this application provides a chip system. The chip system includes a processor for implementing functions of the UDM or the AUSF in the methods in the foregoing aspects. In a possible design, the chip system further includes a memory for storing program instructions and/or data. The chip system may include a chip, or may include a chip and another discrete component.

~~[0054]~~[0055] According to a twelfth aspect, a computer program product is provided. The computer program product includes computer program code. When the computer program code is run, the methods performed by the UDM or the AUSF in the foregoing aspects are performed.

~~[0055]~~[0056] According to an thirteenth ~~eleventh~~ aspect, this application provides a computer-readable storage medium. The computer-readable storage medium stores a computer program. When the computer program is run, the methods performed by the UDM or the AUSF in the foregoing aspects are performed.

~~[0056]~~[0057] In embodiments of this application, the protection request message that is for protecting the terminal parameters update information and that is sent by the UDM to the first AUSF carries an identifier indicating the first serving network. Even if a terminal registers with the HN via multiple serving networks, that is, when one AUSF corresponds to multiple keys, a key used by the first AUSF can be specified. This ensures that the terminal successfully verifies the parameters update information in a terminal parameters update procedure performed by the UDM.

BRIEF DESCRIPTION OF DRAWINGS

~~[0057]~~[0058] FIG. 1 is a schematic diagram of a network architecture according to an embodiment of this application;

~~[0058]~~[0059] FIG. 2 is a schematic diagram of a roaming architecture in a network architecture according to an embodiment of this application;

~~[0059]~~[0060] FIG. 3 is a schematic diagram of another roaming architecture in a network architecture according to an embodiment of this application;

~~[0060]~~[0061] FIG. 4 is a schematic flowchart of a method for protecting terminal parameters update according to an embodiment of this application;

~~[0061]~~[0062] FIG. 5 another schematic flowchart of a method for protecting terminal

parameters update according to an embodiment of this application;

~~[0062]~~[0063] FIG. 6 is a schematic diagram of schematic flowchart of another method for protecting terminal parameters update according to an embodiment of this application;

~~[0063]~~[0064] FIG. 7 is a schematic diagram of a structure of a communication apparatus according to an embodiment of this application; and

~~[0064]~~[0065] FIG. 8 is another schematic diagram of a structure of a communication apparatus according to an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

~~[0065]~~[0066] The following describes the technical solutions in embodiments of the present invention with reference to the accompanying drawings in embodiments of the present invention. In the descriptions of this application, unless otherwise specified, "multiple" means two or more than two. In addition, it should be understood that, in the descriptions of embodiments of this application, terms such as "first" and "second" are merely intended for differentiated description, and should not be construed as an indication or an implication of relative importance, or an indication or an implication of a sequence.

~~[0066]~~[0067] FIG. 1 is a schematic diagram of a network architecture applicable to an embodiment of this application. The network architecture may be applied to an NR communication system or a next-generation communication system. The network architecture includes a core network, an access network, and a terminal.

~~[0067]~~[0068] The access network is mainly to control the terminal to wirelessly access a mobile communication network. The access network is a part of a mobile communication system, and implements a radio access technology. Conceptually, the access network resides in a device (such as a mobile phone, a computer, or any remote controller), and provides a connection to the core network.

~~[0068]~~[0069] The core network includes a VPLMN and an HPLMN. The VPLMN includes a mobility management network element (an AMF entity is used as an example in this specification), a session management network element (an SMF entity is used as an example in this specification), a policy control network element (a PCF entity is used as an example in this specification), and the like. The HPLMN includes an authentication service function network element (an AUSF

entity is used as an example in this specification), a data management network element (a UDM entity is used as an example in this specification), an AMF entity, a PCF entity, and the like.

~~[0069]~~[0070] The AMF may be responsible for authentication for a terminal, mobility management of the terminal, selection of an SMF entity, maintenance and management of status information of the terminal, and the like. In 5G communication, the mobility management network element may be an AMF network element. In future communication, for example, in 6th generation (the 6th generation, 6G) communication, the mobility management network element may still be the AMF network element or may have another name. This is not limited in this application.

~~[0070]~~[0071] The SMF includes session-related functionalities such as session management (for example, session establishment, modification, and release, including tunnel maintaining between a UPF and a RAN), selection and control of a UPF network element, determining a service and session continuity (Service and Session Continuity, SSC) mode, and roaming. In 5G communication, the session management network element may be an SMF network element. In future communication, for example, in 6G communication, the session management network element may still be the SMF network element or may have another name. This is not limited in this application.

~~[0071]~~[0072] The UPF includes user plane–related functionalities such as packet routing and transmission, packet inspection, traffic usage reporting, quality of service (Quality of Service, QoS) handling, lawful interception, uplink traffic verification, and downlink packet buffering. In 5G communication, the user plane network element may be a UPF network element. In future communication, for example, in 6G communication, the user plane network element may still be the UPF network element or have another name. This is not limited in this application.

~~[0072]~~[0073] The UDM is an operator-specific control plane network element, and is responsible for storing information such as a subscription permanent identifier (subscription permanent identifier, SUPI), a credential (credential), a security context (security context), and subscription data of a subscriber in an operator's network. The information stored in the UDM network element may be for authentication and authorization for the terminal device to access the operator's network. The subscriber in the operator's network may be specifically a user using a service provided by the operator's network, for example, a user using a China Telecom SIM card, or a user using a China Mobile SIM card. The subscription permanent identifier (Subscription

Permanent Identifier, SUPI) of the subscriber may be a number of the SIM card or the like. The credential and the security context of the subscriber may be stored small files such as an encryption key of the SIM card or encryption-related information of the SIM card, which are for authentication and/or authorization. The security context may be data (cookie), a token (token), or the like stored in a local terminal (for example, a mobile phone) of a subscriber. The subscription data of the subscriber may be a supporting service of the SIM card, for example, a data package or an available network of the SIM card. It should be noted that the permanent identifier, the credential, the security context, the authentication data (cookie), and the token are equivalent to authentication and authorization–related information. For ease of description, they are not limited or distinguished between each other in this application document of the present invention. Unless otherwise specified, security context is used as an example for description in embodiments of this application. However, authentication and/or authorization information described in another manner are also applicable to embodiments of this application. In 5G communication, the data management network element may be a UDM network element. In future communication, for example, in 6G communication, the data management network element may still be the UDM network element or may have another name. This is not limited in this application.

~~[0073]~~[0074] The PCF is an operator-specific control plane function providing policies of a PDU session for the SMF network element. The policies may include a charging-related policy, a QoS-related policy, an authorization-related policy, and the like. In 5G communication, the policy control network element may be a PCF network element. In future communication, for example, in 6G communication, the policy control network element may still be the PCF network element or may have another name. This is not limited in this application.

~~[0074]~~[0075] The AUSF has an authentication service function for terminating an authentication function requested by a network element that attempts to authenticate the terminal. In an authentication process, the AUSF receives an authentication vector sent by the UDM, processes the authentication vector, and sends a processed authentication vector to the network element that attempts to authenticate the terminal.

~~[0075]~~[0076] The terminal, also be referred to as user equipment (user equipment, UE), is a device having a wireless transceiver function. The terminal may be deployed on land, including an indoor device, an outdoor device, a handheld device, or a vehicle-mounted device; or may be deployed on the water (for example, on a ship); or may be deployed in the air (for example, on

aircraft, balloons, satellites). The terminal device may be a mobile phone (mobile phone), a tablet computer (pad), a computer having a wireless transceiver function, a virtual reality (virtual reality, VR) terminal, an augmented reality (augmented reality, AR) terminal, a wireless terminal in industrial control (industrial control), a wireless terminal in self driving (self driving), a wireless terminal in telemedicine (remote medical), a wireless terminal in a smart grid (smart grid), a wireless terminal in transportation safety (transportation safety), a wireless terminal in a smart city (smart city), a wireless terminal in a smart home (smart home), or the like.

~~[0076]~~[0077] The HPLMN entities may communicate with each other through interfaces, or may communicate with the VPLMN entities through interfaces. For example, in a roaming scenario, the HPLMN needs to send parameters to the terminal, for example, parameters of a home network such as a preferred PLMN or subscription data that needs to be updated. An HPLMN entity, for example, the UDM, needs to send these parameters to the terminal via a VPLMN entity, for example, the AMF. For another example, the PCF entity in the HPLMN needs to send policy information to the terminal sequentially via the PCF entity and the AMF entity in the VPLMN. Considering security levels of these parameters and the like, the HPLMN needs to prevent the VPLMN and the like from tampering with these parameters. Therefore, in the process in which the HPLMN sends these parameters to the terminal, these parameters are encryption protected using a key generated by the AUSF in the HPLMN. Because the terminal generates a key in a process of registering with a network, the terminal can verify received parameters using the corresponding key, provided that the key of the terminal is consistent with a key used by the AUSF for protecting the parameters transmitted between the HPLMN and the terminal.

~~[0077]~~[0078] However, in a dual registration scenario for the terminal, the key selected by the AUSF may be inconsistent with the key on the terminal side. As a result, verification at the terminal fails.

~~[0078]~~[0079] For example, FIG. 2 is a roaming architectural diagram of a network architecture to which an embodiment of this application is applicable. In FIG. 2, a terminal registers via two serving networks (serving networks, SNs). To be specific, the terminal registers with an AMF 1 using a key 1, and the terminal registers with an AMF 2 using a key 2. The AMF 1 and the AMF 2 select a same AUSF in an HN of the terminal. It should be understood that the AUSF corresponds to two keys (the key 1 and the key 2). Alternatively, the terminal first registers with the HN via an SN1, and then registers with the HN via an SN2, and the SN1 and the SN2 select a same AUSF in

the HN of the terminal. In this case, if a UDM needs to perform a SoR procedure or a UE parameters update (UE parameters update, UPU) procedure, the UDM sends a protection request message to the AUSF. If the AUSF randomly selects one of the keys to encryption protect SoR information or UPU information, the key selected by the AUSF may be inconsistent with a key on the terminal side. As a result, the terminal's verification on the received SoR information or UPU information fails. For example, the UDM selects the AMF 2 for the subsequent SoR procedure, but the key selected by the AUSF is the key 1, which is obviously inconsistent with the key 2 on the terminal side. As a result, verification on the received SoR information fails on the terminal side.

~~[0079]~~[0080] For another example, FIG. 3 is a roaming architectural diagram of a network architecture to which an embodiment of this application is applicable. In FIG. 3, a terminal registers via two ANs. To be specific, the terminal registers with an AMF 1 using a key 1, and the terminal registers with an AMF 2 using a key 2. The AMF 1 selects an AUSF 1 in an HN of the terminal, and the AMF 2 selects an AUSF 2 in the HN of the terminal. It should be understood that a key 1 exists in the AUSF 1, and a key 2 exists in the AUSF 2. Similar to FIG. 2, there are two keys on the AUSF side. In this case, if a UDM randomly selects an AUSF to encryption protect SoR information or UPU information, a key in the selected AUSF may be inconsistent with a key on the terminal side. As a result, the received SoR information or UPU information fails the verification of the terminal. For example, the AMF 1 performs the subsequent SoR procedure for the terminal side, but the UDM selects the AUSF 2 to protect the SoR information, that is, a key selected by the AUSF 2 is the key 2. Obviously, the key 2 is inconsistent with the key 1 on the terminal side. As a result, verification on the received SoR information fails on the terminal side.

~~[0080]~~[0081] In view of this, embodiments of this application provide a protection method for network roaming and a communication apparatus. In embodiments of this application, a UDM sends an identifier of an SN included in a protection request message to an AUSF. In other words, the UDM indicates the selected SN, so that an AUSF selects a key corresponding to the SN. Because a key of a terminal uniquely corresponds to the SN, and a key selected by the AUSF uniquely corresponds to the SN, it can be ensured that the key on the AUSF side is consistent with the key on the terminal side, and that the terminal successfully verifies SoR information in a SoR procedure performed by the UDM or UPU information in a UPU procedure performed by the UDM.

~~[0081]~~[0082] The following describes in detail the method provided in embodiments of this application with reference to the accompanying drawings.

~~[0082]~~[0083] FIG. 4 is a flowchart of a positioning method according to an embodiment of this application. The following provides description using an example in which the method is applied to the communication systems shown in FIG. 1 to FIG. 3. In addition, the method may be performed by two communication apparatuses. The two communication apparatuses are, for example, a first communication apparatus and a second communication apparatus. For ease of description, the following uses an example in which the method is performed by an AUSF and a UDM. In other words, an example in which the first communication apparatus is the UDM and the second communication apparatus is the AUSF is used. It should be noted that in embodiments of this application, the communication systems in FIG. 1 to FIG. 3 are only used as an example, which are not limited to this scenario. In addition, embodiments of this application are applicable to protection of parameters update information sent by an HPLMN to a terminal via an AMF. For example, embodiments of this application are applicable to a SoR procedure or a UPU procedure. The following uses an example in which the terminal parameters update information is SoR information.

~~[0083]~~[0084] Specifically, a specific procedure of the method for protecting terminal parameters update provided in an embodiment of this application is described as follows.

~~[0084]~~[0085] S401: A UDM sends a protection request message to a first AUSF, and the first AUSF receives the protection request message, where the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first SN.

~~[0085]~~[0086] This embodiment of this application resolves the following problem: When the terminal registers with an HN via multiple SNs, a key used by an AUSF for protecting a parameter sent between the HPLMN and the terminal is inconsistent with a key on the terminal side. Therefore, in this embodiment of this application, the protection request message sent to the first AUSF by the UDM carries identification information of an SN. It should be understood that the identification information indicates an SN serving the terminal, where the SN is referred to as the first SN in this specification. In other words, the UDM may select the first SN from multiple SNs in advance, and then select an AUSF corresponding to the first SN to encryption protect the terminal parameters update information. Because the key of the terminal uniquely corresponds to

the first SN, and the key selected by the AUSF also uniquely corresponds to the first SN, it can be ensured that the key on the AUSF side is consistent with the key on the terminal side, and that the terminal successfully verifies SoR information in a SoR procedure performed by the UDM or UPU information in a UPU procedure performed by the UDM.

~~[0086]~~[0087] It should be understood that, if the terminal parameters update information is SoR information, the protection request message requests to protect the SoR information. Therefore, in some embodiments, the protection request message is also referred to as a SoR protection request (SoR protection request) message. It should be noted that a name of the protection request message is not specifically limited in this embodiment of this application. For example, if the protection request message is for protecting terminal subscription data update, the protection request message may also be referred to as a UPU protection request message.

~~[0087]~~[0088] There are multiple specific implementations of identifying the first SN, and this is not limited in this embodiment of this application. For example, SN information for identifying the first SN may be a name of the first SN, a PLMN ID of the first SN, or an ID of the first SN. Alternatively, the information about the first SN may include an authentication event identifier of the terminal. It should be understood that the authentication event ID (authEvent ID) of the terminal is sent by the UDM to the AUSF in an authentication procedure to identify an authentication event of the UE in the first SN. Therefore, the authEvent ID may uniquely correspond to a key.

~~[0088]~~[0089] S402: The first AUSF determines a first key based on the information about the first SN in the protection request message, and security protect the terminal parameters update information based on the first key.

~~[0089]~~[0090] It should be understood that the first key may be considered as an authentication service function key (Kausf). If the information about the first serving network is the name of the first SN, the ID of the first SN, or the PLMN ID of the first SN, the first AUSF may select a corresponding Kausf based on a SUPI and the information about the first serving network, and encryption protect, using the Kausf, the SoR information carried in the protection request message. If the information about the first serving network is the authEvent ID, the first AUSF may select a corresponding Kausf based on the authEvent ID, and encryption protect, using the Kausf, the SoR information carried in the protection request message. The first AUSF may generate a protection result for protecting a parameter of the terminal, for example, a MAC value or other information.

~~[0090]~~[0091] S403: The first AUSF sends a response message of the protection request message to the UDM.

~~[0091]~~[0092] It should be understood that the first AUSF sends the response message to the UDM after generating the protection result, where the response message is a message in response to the protection request message.

~~[0092]~~[0093] In some embodiments, the response message may include information such as a SoR counter or a UPU counter, a SoR message authentication code MAC, or a UPU message authentication code MAC, to notify the first AUSF of the protection result of the terminal parameters update information.

~~[0093]~~[0094] S404: The UDM sends the terminal parameters update information via an AMF corresponding to the first serving network.

~~[0094]~~[0095] After receiving the response message sent by the first AUSF, the UDM may perform the terminal parameters update procedure, for example, the SoR procedure via the first SN. For example, the UDM initiates a request message for invoking a subscription data management notification (SDM_notification) service to the AMF in the first SN, where the request message carries roaming configuration information, for example, a priority list of a combination of a PLMN and access technologies, or a SoR message authentication code MAC.

~~[0095]~~[0096] In some embodiments, before sending the protection request message to the first AUSF, the UDM determines the first SN for the terminal parameters update procedure. The terminal may be in a single-registration mode or a dual-registration mode. When the terminal is in the single-registration mode, the UDM may not determine the first SN, that is, may not perform the step for determining the first SN.

~~[0096]~~[0097] For example, FIG. 5 is an example flowchart of a method for protecting terminal parameters update according to an embodiment of this application.

~~[0097]~~[0098] S501: Before sending a protection request message to a first AUSF, a UDM determines a first SN for a terminal parameters update procedure.

~~[0098]~~[0099] In this embodiment of this application, before sending the protection request message, the UDM may determine the first SN in which an AMF sending terminal parameters update information is located. Because the first SN is selected before the protection request message is sent, even if the terminal is in a dual-registration mode (that is, the terminal registers with at least two serving networks) and AMFs in the at least two serving networks select a same

AUSF, it can be ensured that a key selected by the first AUSF is consistent with a key generated in an authentication process of the terminal.

~~[0099]~~[00100] In some embodiments, the UDM may determine, according to a local policy, the first SN in which the AMF sending the terminal parameters update information is located. For example, the UDM determines, based on information such as a priority, the first SN in which the AMF sending the terminal parameters update information is located.

~~[00100]~~[00101] Further, when determining that there are multiple SNs, the UDM determines the first SN for the subsequent terminal parameters update procedure. This can avoid a case in which the UDM still determines the first SN for the subsequent terminal parameters update procedure in case of one SN. This has better compatibility with an existing mechanism of the terminal parameters update procedure.

~~[00101]~~[00102] S502: Before sending the protection request message to the first AUSF, the UDM determines whether there are multiple keys in the AUSF.

~~[00102]~~[00103] For example, before sending the protection request message to the first AUSF, the UDM may determine whether the first AUSF includes authentication results for the terminal in multiple SNs. If the first AUSF includes authentication results for the terminal in the multiple SNs, it may be considered that multiple keys exist in the first AUSF. In this case, the protection request message sent by the UDM to the first AUSF may carry an identifier of an SN. It should be understood that the multiple SNs include the first SN. Otherwise, if there are no authentication results for the terminal in the multiple SNs in the first AUSF, it may be considered that no multiple keys exist in the first AUSF, that is, one key exists in the first AUSF. In this case, the protection request message sent by the UDM to the first AUSF may not carry an identifier of an SN.

~~[00103]~~[00104] For another example, before sending the protection request message to the first AUSF, the UDM may determine whether the terminal is in multiple SNs. If the terminal is in multiple SNs, it may be considered that multiple keys exist in the first AUSF. In this case, the protection request message sent by the UDM to the first AUSF may carry an identifier of an SN. It should be understood that the multiple SNs include the first SN. Otherwise, if the terminal is not in multiple SNs, it may be considered that no multiple keys exist in the first AUSF, that is, tone key exists in the first AUSF. In this case, the protection request message sent by the UDM to the first AUSF may not carry an identifier of an SN.

~~[00104]~~[00105] It should be noted that, that the terminal is in multiple SNs means that the

terminal device accesses multiple SNs; or multiple SNs provide services for the terminal; or the terminal registers with multiple SNs; or the terminal is authenticated in multiple SNs; or registration modes of the terminal with multiple SNs exist in the UDM; or authentication states of the terminal in multiple SNs exist in the UDM.

~~[00105]~~[00106] For still another example, before sending the protection request message to the first AUSF, the UDM may determine whether the terminal is in a dual-registration mode, that is, determine whether the terminal registers with the HN via two SNs. If the terminal is in a dual-registration mode, it may be considered that multiple keys exist in the first AUSF. In this case, the protection request message sent by the UDM to the first AUSF may carry an identifier of an SN. Otherwise, if the terminal is not in a dual-registration mode, it may be considered that no multiple keys exist in the first AUSF, that is, one key exists in the first AUSF. In this case, the protection request message sent by the UDM to the first AUSF may not carry an identifier of an SN.

~~[00106]~~[00107] Before sending the protection request message to the first AUSF, the UDM determines whether there are multiple keys in the AUSF. The UDM sends an identifier of an SN only when determining that there are multiple keys in the AUSF. This can prevent the sent protection request message from carrying an unnecessary identifier. In addition, the UDM specifies a key based on the identifier of the first SN, so that the key selected by the first AUSF is consistent with the key generated in the authentication process of the terminal.

~~[00107]~~[00108] S503: Before sending the protection request message to the first AUSF, the UDM determines the first AUSF corresponding to the first SN.

~~[00108]~~[00109] In this embodiment of this application, the first AUSF may be an AUSF, for example, the AUSF shown in FIG. 2, selected by multiple SNs in the dual-registration scenario of the terminal. Alternatively, the first AUSF may be an AUSF in multiple AUSFs in the dual-registration scenario of the terminal, for example, an AUSF in the two AUSFs shown in FIG. 3. It should be understood that, in the scenario shown in FIG. 3, the first AUSF is selected by the UDM from multiple AUSFs. Therefore, before sending the protection request message to the first AUSF, the UDM may select the first AUSF from the multiple AUSFs. In this way, even if the terminal registers with the HN sequentially via multiple different serving networks, and the different serving networks select different AUSFs, because the UDM specifies the first AUSF to protect SoR information, and the first AUSF corresponds to a unique SN (or corresponds to a unique key), it can be ensured that the key selected by the first AUSF is consistent with the key generated in the

authentication process of the terminal.

~~[00109]~~[00110] It should be noted that, as S501, S502, and S503 are optional steps, they are shown using dashed lines in FIG. 5. In addition, a sequence of S501, S502, and S503 is not limited in this embodiment of this application.

~~[00110]~~[00111] In an alternative solution of the foregoing embodiment, FIG. 6 is a schematic flowchart of another method for protecting terminal parameters update according to an embodiment of this application. The process is described as follows:

~~[00111]~~[00112] S601: A UDM sends a first message to a first AUSF, and the first AUSF receives the first message, where the first message indicates the first AUSF to delete a first key generated when a terminal registers with a first SN in which a first AMF is located, and the first AUSF is an AUSF for authentication when the terminal registers with the first SN.

~~[00112]~~[00113] S602: The first AUSF deletes the first key generated by the terminal when the terminal registers with the first SN in which the first AMF is located.

~~[00113]~~[00114] S603: When determining that the terminal is in a single-registration mode, the UDM determines to send terminal parameters update information via a second AMF.

~~[00114]~~[00115] In a possible scenario, for example, if the terminal first registers with an HN via an SN1, and then registers with the HN via an SN2, there are two first keys in the AUSF. In this case, in this embodiment of this application, when the terminal registers with an SN in which another AMF (the second AMF is used as an example below) is located, the UDM may indicate a corresponding AUSF to delete the first key used when the terminal registers with the first SN in which the registered AMF (the first AMF is used as an example below) is located. In this way, even if the terminal registers with the SN2 in which the second AMF is located, it can be ensured that a key in the AUSF is unique, that is, the key is consistent with a key in an authentication process of the terminal.

~~[00115]~~[00116] It should be understood that the first message carries identification information of the first serving network or identification information of the terminal, so that the AUSF determines to delete the key corresponding to the first serving network.

~~[00116]~~[00117] It should be understood that, when sending a second message to the first AMF, for example, a message (Nudm_UECM_DeregistrationNotify message) for deleting registration information of the terminal, the UDM sends the first message to the first AUSF. Alternatively, when receiving a response message, namely, a third message (Nudm_SDM_Unsubscribe message),

that is of the second message and that is sent by the first AMF, the UDM sends the first message to the first AUSF.

~~[00117]~~[00118] In this embodiment of this application, a protection request message that is for protecting terminal parameters update information and that is sent by the UDM to the first AUSF carries an identifier indicating the first serving network. Even if the terminal registers with the HN via multiple serving networks, that is, when one AUSF corresponds to multiple keys, a key used by the first AUSF can be specified. This ensures that the terminal successfully verifies the parameters update information in a terminal parameters update procedure performed by the UDM.

~~[00118]~~[00119] As an alternative solution of the foregoing embodiment, to ensure that the terminal and the AUSF obtain a same K_{AUSF} when using authentication service function keys K_{AUSF}, the UE, the AUSF, and the UDM may perform the following action:

~~[00119]~~[00120] The UE deletes a stored old K_{AUSF} or deleting a stored old K_{AUSF} generated in a same serving network upon the terminal receives a security mode command SMC message, or upon the terminal receives a security mode command SMC message and successfully performs verification, or upon the terminal receives an AUTN and successfully performs verification, or upon the terminal sends an authentication response, or upon the terminal sends a security mode complete (security mode complete message), or upon the terminal receives an extensible authentication protocol success EAP success message, or upon the terminal generates a new K_{AUSF}. In an optional implementation, when the terminal generates a new K_{AUSF} and/or the foregoing condition is met, a timer may further be set. When the timer expires, the terminal deletes the stored old K_{AUSF} or deletes the old K_{AUSF} generated in the same serving network.

~~[00120]~~[00121] The AUSF deletes the stored old K_{AUSF} generated during authentication for the terminal or deletes the stored old K_{AUSF} generated by the terminal during authentication in the same serving network, upon successfully verifying an authentication response returned by the terminal, or upon sending an authentication result confirmation request for the terminal to the UDM, or upon generating a new K_{AUSF}, or upon receiving an authentication result confirmation response for the terminal returned by the UDM. In an optional implementation, when the AUSF generates a new K_{AUSF} during authentication for the terminal and/or when the foregoing condition is met, a timer may further be set. When the timer expires, the AUSF deletes the stored old K_{AUSF} generated during authentication for the terminal or deletes the old K_{AUSF} generated by the terminal during authentication in the same serving network.

~~[00121]~~[00122] When the UDM needs to perform SoR or UPU, the UDM selects an AUSF that successfully completes an authentication procedure with the terminal most recently. It should be understood that after completing authentication with the terminal, the AUSF returns an authentication result for the terminal to the UDM, where the authentication result records an authentication time and a name of a serving network. Therefore, the UDM may select, based on the recorded time, an AUSF that completes authentication most recently. In an optional implementation, because the authentication result further records the name of the serving network, the UDM may further select an AUSF, in the serving network in which SoR or UPU is performed, that successfully completes an authentication procedure with the terminal most recently. In an optional implementation, because different AUSFs may share a same K_{AUSF} of the terminal, the UDM may randomly select an AUSF.

~~[00122]~~[00123] In this way, even if the terminal sequentially registers with the HN via multiple different serving networks and different serving networks select a same AUSF or different AUSFs, because the UE and the AUSF side maintain a same K_{AUSF}, there is a unique key K_{AUSF} in the AUSF or there is a unique K_{AUSF} for a same serving network when the UDM specifies an AUSF to protect SoR or UPU information, and it can be ensured that a key selected by the AUSF is consistent with a key selected by the terminal.

~~[00123]~~[00124] Specifically, for example, in a primary authentication procedure between the terminal and a network, for EAP-AKA' authentication, the UDM returns a UE authentication obtaining response to the AUSF, where the response carries keys CK' and IK'. After receiving the UE authentication obtaining response returned by the UDM, the AUSF returns a UE authentication response to a security anchor function SEAF (which may be co-deployed with the AMF). After receiving the UE authentication response returned by the AUSF, the SEAF initiates an authentication request to the UE. The UE receives the authentication request sent by the SEAF, calculates an authentication response and keys CK' and IK', and returns the authentication response to the SEAF, where the authentication response is comprised in an EAP response. After receiving the authentication response of the UE, the SEAF initiates a UE authentication request to the AUSF, where the UE authentication request carries the EAP response. The AUSF authenticates the received EAP response. If the authentication succeeds, the AUSF generates a first K_{AUSF} based on CK' and IK' obtained from the UDM, and also deletes a stored old K_{AUSF} (if any). Then, the AUSF returns a UE authentication response to the SEAF, where the UE authentication response carries

an EAP success message. After receiving the UE authentication response from the AUSF, the SEAF returns the EAP success message to the UE. Upon receiving the EAP success message, the UE generates a second K_{AUSF} based on the calculated CK' and IK', and deletes a stored old K_{AUSF} (if any). The first K_{AUSF} is the same as the second K_{AUSF}. In this way, the old keys K_{AUSF} stored on the UE side and the AUSF side are deleted in the primary authentication procedure. This ensures that the unique first K_{AUSF} exists on the AUSF side and the unique second K_{AUSF} exists on the UE side. When the UDM needs to perform SoR or UPU, the UDM selects an AUSF that completes primary authentication with the UE most recently, and the selected AUSF stores only a K_{AUSF} consistent with that of the UE, to ensure that the key selected by the AUSF is consistent with the key selected by the terminal.

~~[00124]~~[00125] Specifically, for example, in a primary authentication procedure between the terminal and a network, for 5G AKA authentication, the UDM returns a UE authentication obtaining response to the AUSF, where the response carries a first K_{AUSF}. After receiving the UE authentication obtaining response returned by the UDM, the AUSF returns a UE authentication response to a security anchor function SEAF (which may be co-deployed with the AMF), where the UE authentication response carries an authentication token AUTN. After receiving the UE authentication response returned by the AUSF, the SEAF initiates an authentication request to the UE, where the authentication request carries the AUTN. Upon receiving the authentication request sent by the SEAF, and successfully checking the AUTN, the UE calculates an authentication response RES* and a second key K_{AUSF}, deletes a stored old K_{AUSF} (if any), and then returns an authentication response to the SEAF, where the authentication response carries the RES*. After receiving the authentication response of the UE, the SEAF initiates a UE authentication request to the AUSF, where the UE authentication request carries the RES*. After the AUSF authenticates the received RES*, the AUSF deletes a stored old K_{AUSF} (if any) if the authentication succeeds, or deletes the first K_{AUSF} if the authentication fails. The first K_{AUSF} is the same as the second K_{AUSF}. In this way, the old keys K_{AUSF} stored on the UE side and the AUSF side are deleted in the primary authentication procedure. This ensures that the unique first K_{AUSF} exists on the AUSF side and the unique second K_{AUSF} exists on the UE side. When the UDM needs to perform SoR or UPU, the UDM selects an AUSF that completes primary authentication with the UE most recently, and the selected AUSF stores only a K_{AUSF} consistent with that of the UE, to ensure that the key selected by the AUSF is consistent with the key selected by the terminal.

~~[00125]~~[00126] Specifically, for another example, in a primary authentication procedure and a security mode command SMC procedure between the terminal and the network, for EAP-AKA' authentication, the UDM returns a UE authentication obtaining response to the AUSF, where the UE authentication obtaining response carries keys CK' and IK'. After receiving the UE authentication obtaining response returned by the UDM, the AUSF returns a UE authentication response to a security anchor function SEAF (which may be co-deployed with the AMF). After receiving the UE authentication response returned by the AUSF, the SEAF initiates an authentication request to the UE. The UE receives the authentication request sent by the SEAF, calculates an authentication response and keys CK' and IK', and returns the authentication response to the SEAF, where the authentication response is comprised in an EAP response. After receiving the authentication response of the UE, the SEAF initiates a UE authentication request to the AUSF, where the UE authentication request carries the EAP response. The AUSF authenticates the received EAP response. If the authentication succeeds, the AUSF generates a first K_{AUSF} based on CK' and IK' obtained from the UDM, and deletes a stored old K_{AUSF} (if any). Then, the AUSF returns a UE authentication response to the SEAF, where the UE authentication response carries an EAP success message. After receiving the UE authentication response from the AUSF, the SEAF returns the EAP success message to the UE. Upon receiving the EAP success message, the UE generates a second K_{AUSF} based on the calculated CK' and IK'. The first K_{AUSF} is the same as the second K_{AUSF}. After the authentication, the AMF sends a security mode command SMC message to the terminal, and the terminal deletes a stored old K_{AUSF} (if any) upon the security mode command SMC message is successfully integrity checked. In this way, the old keys K_{AUSF} stored on the UE side and the AUSF side are deleted in the primary authentication procedure and the security mode command SMC procedure. This ensures that the unique first K_{AUSF} exists on the AUSF side and the unique second K_{AUSF} exists on the UE side. When the UDM needs to perform SoR or UPU, the UDM selects an AUSF that completes primary authentication with the UE most recently, and the selected AUSF stores only a K_{AUSF} consistent with that of the UE, to ensure that the key selected by the AUSF is consistent with the key selected by the terminal.

~~[00126]~~[00127] Specifically, for another example, in a primary authentication procedure and a security mode command SMC procedure between the terminal and the network, for 5G AKA authentication, the UDM returns a UE authentication obtaining response to the AUSF, where the UE authentication obtaining response carries a first K_{AUSF}. After receiving the UE authentication

obtaining response returned by the UDM, the AUSF returns a UE authentication response to a security anchor function SEAF (which may be co-deployed with the AMF), where the UE authentication response carries an authentication token AUTN. After receiving the UE authentication response returned by the AUSF, the SEAF initiates an authentication request to the UE, where the authentication request carries the AUTN. The UE receives the authentication request sent by the SEAF, and after successfully verifying the AUTN, the UE calculates an authentication response RES* and a second key K_{AUSF}, and then returns an authentication response to the SEAF, where the authentication response carries the RES*. After receiving the authentication response of the UE, the SEAF initiates a UE authentication request to the AUSF, where the UE authentication request carries the RES*. After the AUSF authenticates the received RES*, the AUSF deletes a stored old K_{AUSF} (if any) if the authentication succeeds, or deletes the first K_{AUSF} if the authentication fails. The first K_{AUSF} is the same as the second K_{AUSF}. After the authentication, the AMF sends a security mode command SMC message to the terminal, and the terminal deletes a stored old K_{AUSF} (if any) upon the security mode command SMC message is successfully integrity checked. In this way, the old keys K_{AUSF} stored on the UE side and the AUSF side are deleted in the primary authentication procedure and the security mode command SMC procedure. This ensures that the unique first K_{AUSF} exists on the AUSF side and the unique second K_{AUSF} exists on the UE side. When the UDM needs to perform SoR or UPU, the UDM selects an AUSF that completes primary authentication with the UE most recently, and the selected AUSF stores only a K_{AUSF} consistent with that of the UE, to ensure that the key selected by the AUSF is consistent with the key selected by the terminal. Specifically, for example, in a primary authentication procedure, a security mode command SMC procedure, and an authentication result confirmation procedure between the terminal and the network, for EAP-AKA' authentication, the UDM returns a UE authentication obtaining response to the AUSF, where the response carries keys CK' and IK'. After receiving the UE authentication obtaining response returned by the UDM, the AUSF returns a UE authentication response to a security anchor function SEAF (which may be co-deployed with the AMF). After receiving the UE authentication response returned by the AUSF, the SEAF initiates an authentication request to the UE. The UE receives the authentication request sent by the SEAF, calculates an authentication response and keys CK' and IK', and returns the authentication response to the SEAF, where the authentication response is comprised in an EAP response. After receiving the authentication response of the UE, the SEAF initiates a UE

authentication request to the AUSF, where the UE authentication request carries the EAP response. The AUSF authenticates the received EAP response. If the authentication succeeds, the AUSF generates a first K_{AUSF} based on CK' and IK' obtained from the UDM. Then, the AUSF returns a UE authentication response to the SEAF, where the UE authentication response carries an EAP success message. After receiving the UE authentication response from the AUSF, the SEAF returns the EAP success message to the UE. Upon receiving the EAP success message, the UE generates a second K_{AUSF} based on the calculated CK' and IK'. The first K_{AUSF} is the same as the second K_{AUSF}. After the authentication, the AMF sends a security mode command SMC message to the terminal, and the terminal deletes a stored old K_{AUSF} (if any) upon the security mode command SMC message is successfully integrity checked. In addition, after the AUSF completes authentication on the UE, the AUSF sends an authentication result confirmation request for the terminal to the UDM, and deletes a stored old K_{AUSF} (if any) upon receiving an authentication result confirmation response for the terminal returned by the UDM. In this way, the old keys K_{AUSF} stored on the UE side and the AUSF side are deleted in the primary authentication procedure, the security mode command SMC procedure, and the authentication result confirmation procedure. This ensures that the unique first K_{AUSF} exists on the AUSF side and the unique second K_{AUSF} exists on the UE side. When the UDM needs to perform SoR or UPU, the UDM selects an AUSF that completes primary authentication with the UE most recently, and the selected AUSF stores only a K_{AUSF} consistent with that of the UE, to ensure that the key selected by the AUSF is consistent with the key selected by the terminal.

~~[00127]~~[00128] Specifically, for another example, in a primary authentication procedure, a security mode command SMC procedure, and an authentication result confirmation procedure between the terminal and a network for 5G AKA authentication, the UDM returns a UE authentication obtaining response to the AUSF, where the UE authentication obtaining response carries the first K_{AUSF}. After receiving the UE authentication obtaining response returned by the UDM, the AUSF returns a UE authentication response to a security anchor function SEAF (which may be co-deployed with the AMF), where the UE authentication response carries an authentication token AUTN. After receiving the UE authentication response returned by the AUSF, the SEAF initiates an authentication request to the UE, where the authentication request carries the AUTN. After receiving the authentication request sent by the SEAF, and successfully verifying the AUTN, the UE calculates an authentication response RES* and a second key K_{AUSF}, and then

returns an authentication response to the SEAF, where the authentication response carries the RES*. After receiving the authentication response of the UE, the SEAF initiates a UE authentication request to the AUSF, where the UE authentication request carries the RES*. The first K_{AUSF} is the same as the second K_{AUSF}. After the authentication, the AMF sends a security mode command SMC message to the terminal, and the terminal deletes a stored old K_{AUSF} (if any) upon the security mode command SMC message is successfully integrity checked. In addition, after the AUSF authenticates the UE, the AUSF sends an authentication result confirmation request for the terminal to the UDM, and deletes a stored old K_{AUSF} (if any) upon receiving an authentication result confirmation response for the terminal returned by the UDM. In this way, the old keys K_{AUSF} stored on the UE side and the AUSF side are deleted in the primary authentication procedure, the security mode command SMC procedure, and the authentication result confirmation procedure. This ensures that the unique first K_{AUSF} exists on the AUSF side and the unique second K_{AUSF} exists on the UE side. When the UDM needs to perform SoR or UPU, the UDM selects an AUSF that completes primary authentication with the UE most recently, and the selected AUSF stores only a K_{AUSF} consistent with that of the UE, to ensure that the key selected by the AUSF is consistent with the key selected by the terminal.

~~[00128]~~[00129] In the foregoing embodiments provided in this application, the methods provided in embodiments of this application are described from the perspective of interaction between the UDM and the AUSF. To implement the functions in the methods provided in embodiments of this application, the UDM and the AUSF each may include a hardware structure and/or a software module, to implement the foregoing functions in a form of the hardware structure, the software module, or a combination of the hardware structure and the software module. Whether a specific function in the foregoing functions is performed by the hardware structure, the software module, or the combination of the hardware structure and the software module depends on a specific application and a design constraint of the technical solutions.

~~[00129]~~[00130] The following describes, with reference to the accompanying drawings, apparatuses for implementing the foregoing methods in embodiments of this application. Therefore, all the foregoing content may be used in the following embodiments. Repeated content is not described again.

~~[00130]~~[00131] FIG. 7 is a possible example block diagram of a communication apparatus in this application. The communication apparatus 700 may correspondingly implement functions or steps

implemented by the UDM or the AUSF in the foregoing method embodiments. The communication apparatus may include a transceiver module 701 and a processing module 702. Optionally, the apparatus may further include a storage module for storing instructions (code or a program) and/or data. The transceiver module 701 and the processing module 702 may be coupled to the storage module. For example, the processing module 702 may read the instructions (the code or the program) and/or the data from the storage module for implementing a corresponding method. The foregoing modules may be independently deployed, or may be partially or completely integrated.

~~[00131]~~[00132] It should be understood that the processing module 702 may be a processor or a controller, for example, may be a general-purpose central processing unit (central processing unit, CPU), a general-purpose processor, a digital signal processing (digital signal processor, DSP), an application-specific integrated circuit (application-specific integrated circuits, ASIC), a field programmable gate array (field programmable gate array, FPGA) or another programmable logic device, a transistor logic device, a hardware component, or any combination thereof. The processing module 702 can implement or execute various examples of logical blocks, modules, and circuits that are described with reference to the content disclosed in this application. Alternatively, the processor may be a combination of processors implementing a computing function, for example, a combination of one or more microprocessors, or a combination of a DSP and a microprocessor. The transceiver module 701 is an interface circuit of the apparatus, for receiving a signal from another apparatus. For example, when the apparatus is implemented as a chip, the transceiver module 701 is an interface circuit of the chip for receiving a signal from another chip or apparatus, or an interface circuit of the chip for sending a signal to another chip or apparatus.

~~[00132]~~[00133] The communication apparatus 700 may be the UDM or the AUSF in the foregoing embodiments, or may be a chip used in the UDM or the AUSF. For example, when the communication apparatus 700 is the UDM or the AUSF, the processing module 702 may be, for example, a processor, and the transceiver module 701 may be, for example, a transceiver. Optionally, the transceiver may include a radio frequency circuit, and the storage unit may be, for example, a memory. For example, when the communication apparatus 700 is the chip used in the UDM or the AUSF, the processing module 702 may be, for example, a processor, and the transceiver module 701 may be, for example, an input/output interface, pins, or a circuit. The

processing module 702 may execute computer-executable instructions stored in the storage unit. Optionally, the storage unit is a storage unit in the chip, such as a register or a cache. Alternatively, the storage unit may be a storage unit that is in the network device, the terminal, or the positioning management device and that is located outside the chip, for example, a read-only memory (read-only memory, ROM), another type of static storage device that can store static information and instructions, or a random access memory (random access memory, RAM).

~~[00133]~~[00134] In some possible implementations, the communication apparatus 700 can correspondingly implement behavior and functions of the UDM in the foregoing method embodiments. For example, the communication apparatus 700 may be a UDM, or may be a component (for example, a chip or a circuit) used in the UDM. The transceiver module 701 may be configured to support the UDM in communicating with another network entity, for example, support the UDM in communicating with the first AUSF and/or the AMF shown in FIG. 4 to FIG. 6. The processing module 702 is configured to control and manage actions of the UDM. For example, the processing module 702 is configured to support the network device in performing all operations of the UDM in FIG. 4 to FIG. 6 other than receiving and sending operations.

~~[00134]~~[00135] For example, the transceiver module 701 may be configured to perform all sending or receiving operations performed by the UDM in the embodiment shown in FIG. 4, for example, S401, S403, and S404 in the embodiment shown in FIG. 4, and/or support other processes of the technology described in this specification. The processing module 702 is configured to perform all operations other than the sending and receiving operations performed by the UDM in the embodiment shown in FIG. 4, and/or support other processes of the technology described in this specification.

~~[00135]~~[00136] For another example, the transceiver module 701 may be configured to perform all sending or receiving operations performed by the UDM in the embodiment shown in FIG. 5, for example, S401, S403, and S404 in the embodiment shown in FIG. 5, and/or support other processes of the technology described in this specification. The processing module 702 is configured to perform all operations other than the sending and receiving operations performed by the UDM in the embodiment shown in FIG. 5, for example, S501, S502, and S503 in the embodiment shown in FIG. 5, and/or support other processes of the technology described in this specification.

~~[00136]~~[00137] In some embodiments, the transceiver module 701 is configured to: send a

protection request message to a first AUSF, and receive a response message that is of the protection request message and that is sent by the first AUSF, where the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first serving network. The processing module 702 is configured to control the transceiver module 701 to send the parameters update information via an AMF corresponding to the first serving network.

~~[00137]~~[00138] In an optional implementation, the transceiver module 701 is further configured to: before sending the protection request message to the first AUSF, determine the information about the first serving network according to a local policy.

~~[00138]~~[00139] In an optional implementation, the processing module 702 is specifically configured to: when determining that there are multiple serving networks, determine the first serving network for terminal parameters update.

~~[00139]~~[00140] In an optional implementation, the processing module 702 is specifically configured to determine the first AUSF based on the information about the first serving network.

~~[00140]~~[00141] In an optional implementation, the processing module 702 is specifically configured to: before the protection request message is sent to the first AUSF, determine that the first AUSF includes authentication results for the terminal in multiple serving networks, where the multiple serving networks include the first serving network;

the terminal is in multiple serving networks, where the multiple serving networks include the first serving network; or

the terminal is in a dual-registration mode.

~~[00141]~~[00142] In an optional implementation, the information about the first serving network includes a name of the first serving network;

the information about the first serving network includes a PLMN ID of the first serving network or an ID of the first serving network; or

the information about the first serving network includes an authentication event identifier of the terminal.

~~[00142]~~[00143] In an optional implementation, the parameters update information includes SoR information.

~~[00143]~~[00144] It should be understood that the processing module 702 in this embodiment of this application may be implemented by a processor or a processor-related circuit component, and

the transceiver module 701 may be implemented by a transceiver or a transceiver-related circuit component.

~~[00144]~~[00145] For another example, the transceiver module 701 may be configured to perform all sending or receiving operations performed by the UDM in the embodiment shown in FIG. ~~5~~6, for example, S601 and S603 in the embodiment shown in FIG. 6, and/or support other processes of the technology described in this specification. The processing module 702 is configured to perform all operations other than the sending and receiving operations performed by the UDM in the embodiment shown in FIG. 6, for example, S602 in the embodiment shown in FIG. 6, and/or support other processes of the technology described in this specification.

~~[00145]~~[00146] In some embodiments, the transceiver module 701 is configured to send a first message to a first AUSF, where the first message indicates the first AUSF to delete a first key used when a terminal registers with a first serving network in which a first AMF is located, and the first AUSF is an AUSF for authentication when the terminal registers with the first serving network. The processing module 702 is configured to: when determining that the terminal is in a single-registration mode, determine to send terminal parameters update information via a second AMF.

~~[00146]~~[00147] In an optional implementation, the transceiver module 701 is specifically configured to: when sending a second message to the first AMF or receiving a third message sent by the first AMF, send the first message to the first AUSF, where the second message is for deleting registration information of the terminal, and the third message is a response message of the second message.

~~[00147]~~[00148] In an optional implementation, the first message carries identification information of the first serving network or identification information of the terminal.

~~[00148]~~[00149] In some possible implementations, the communication apparatus 700 can correspondingly implement behavior and functions of the first AUSF in the foregoing method embodiments. For example, the communication apparatus 700 may be an AUSF, or may be a component (for example, a chip or a circuit) used in the AUSF. The transceiver module 701 may be configured to support the AUSF in communicating with another network entity, for example, support the AUSF in communicating with the UDM shown in FIG. 4 to FIG. 6. The processing module 702 is configured to control and manage actions of the AUSF. For example, the processing module 702 is configured to support the AUSF in performing all operations other than sending and receiving operations in FIG. 4 to FIG. 6.

~~[00149]~~**[00150]** For example, the transceiver module 701 may be configured to perform all sending or receiving operations performed by the first AUSF in the embodiment shown in FIG. 4, for example, S401, S403, and S404 in the embodiment shown in FIG. 4, and/or support other processes of the technology described in this specification. The processing module 702 is configured to perform all operations other than the sending and receiving operations performed by the first AUSF in the embodiment shown in FIG. 4, for example, S402 in the embodiment shown in FIG. 4, and/or support other processes of the technology described in this specification.

~~[00150]~~**[00151]** For another example, the transceiver module 701 may be configured to perform all sending or receiving operations performed by the first AUSF in the embodiment shown in FIG. 5, for example, S401, S403, and S404 in the embodiment shown in FIG. 5, and/or support other processes of the technology described in this specification. The processing module 702 is configured to perform all operations other than the sending and receiving operations performed by the first AUSF in the embodiment shown in FIG. 5, for example, S402 in the embodiment shown in FIG. 5, and/or support other processes of the technology described in this specification.

~~[00151]~~**[00152]** The transceiver module 701 is configured to receive a protection request message sent by a UDM, where the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first serving network. The processing module 702 is configured to: determine a first key based on the information about the first serving network, and security protect the parameters update information based on the first key, where the first key is for protecting the parameters update information.

~~[00152]~~**[00153]** In a possible implementation, the information about the first serving network is information about one of multiple first serving networks that is stored by the UDM.

~~[00153]~~**[00154]** In an optional implementation, there are multiple AUSFs, and the first AUSF is an AUSF corresponding to the information about the first serving network.

~~[00154]~~**[00155]** In an optional implementation, the first AUSF includes authentication results for the terminal in multiple serving networks, where the multiple serving networks include the first serving network;

the terminal is in multiple serving networks, where the multiple serving networks include the first serving network; or

the terminal is in a dual-registration mode.

~~[00155]~~[00156] In an optional implementation, the information about the first serving network includes a name of the first serving network;

the information about the first serving network includes a PLMN identifier of the first serving network; or

the information about the first serving network includes an authentication event identifier of the terminal.

~~[00156]~~[00157] In an optional implementation, the parameters update information includes SoR information.

~~[00157]~~[00158] For another example, the transceiver module 701 may be configured to perform all sending or receiving operations performed by the first AUSF in the embodiment shown in FIG. 6, for example, S601 and S603 in the embodiment shown in FIG. 6, and/or support other processes of the technology described in this specification. The processing module 702 is configured to perform all operations other than the sending and receiving operations performed by the first AUSF in the embodiment shown in FIG. 6, for example, S602 in the embodiment shown in FIG. 6, and/or support other processes of the technology described in this specification.

~~[00158]~~[00159] The transceiver module 701 is configured to receive a first message sent by a UDM, where the first message indicates the first AUSF to delete a first key used when a terminal registers with a first serving network in which a first AMF is located, and the first AUSF is an AUSF for authentication when the terminal registers with the first serving network. The processing module 702 is configured to delete the first key used when the terminal registers with the first serving network in which the first AMF is located.

~~[00159]~~[00160] In a possible implementation, the first message carries identification information of the first serving network or identification information of the terminal.

~~[00160]~~[00161] FIG. 8 shows a communication apparatus 800 according to an embodiment of this application. The communication apparatus 800 may be a UDM capable of implementing functions of the UDM in the method provided in embodiments of this application. Alternatively, the communication apparatus 800 may be an AUSF capable of implementing functions of the first AUSF in the method provided in embodiments of this application. Alternatively, the communication apparatus 800 may be an apparatus supporting the UDM or the AUSF in implementing corresponding functions in the method provided in embodiments of this application. The communication apparatus 800 may be a chip system. In this embodiment of this application,

the chip system may include a chip, or may include a chip and another discrete component.

~~[00161]~~[00162] In hardware implementation, the transceiver module 701 may be a transceiver, and the transceiver is integrated into the communication apparatus 800 to form a communication interface 803.

~~[00162]~~[00163] The communication apparatus 800 includes at least one processor 802. The processor 802 may be a CPU, a microprocessor, an ASIC, or one or more integrated circuits for controlling program execution in the solutions of this application. The processor 802 is configured to implement or support the communication apparatus 800 in implementing functions of the UDM or the AUSF in the methods provided in embodiments of this application. For details, refer to detailed descriptions in the method examples. Details are not described herein again.

~~[00163]~~[00164] The communication apparatus 800 may further include at least one memory 801 for storing program instructions and/or data. The memory 801 is coupled to the processor 802. Coupling in embodiments of this application is an indirect coupling or a communication connection between apparatuses, units, or modules, may be in an electrical, a mechanical, or another form, and is used for information exchange between apparatuses, units, or the modules. The processor 802 may coordinate with the memory 801. The processor 802 may execute the program instructions and/or the data stored in the memory 801, so that the communication apparatus 800 implements a corresponding method. At least one of the at least one memory may be included in the processor 802.

~~[00164]~~[00165] The communication apparatus 800 may further include the communication interface 803, configured to communicate with another device or a communication network such as a radio access network (radio access network, RAN), a wireless local area network (wireless local area network, WLAN), or a wired access network using any transceiver-type apparatus. The communication interface 803 is configured to communicate with another device via a transmission medium, so that an apparatus used in the communication apparatus 800 can communicate with the another device. For example, when the communication apparatus 800 is a UDM, the another device is an AUSF; or when the communication apparatus 800 is an AUSF, the another device is a UDM. The processor 802 may send and receive data through the communication interface 803. The communication interface 803 may be specifically a transceiver.

~~[00165]~~[00166] A connection medium between the communication interface 803, the processor 802, and the memory 801 is not specifically limited in this embodiment of this application. In this

embodiment of this application, the memory 801, the processor 802, and the communication interface 803 are connected through a bus 804 in FIG. 8. The bus is represented as a bold line in FIG. 8. A manner of connection between other components is merely an example for description, and imposes no limitation. The bus may be classified as an address bus, a data bus, a control bus, and the like. For ease of indication, the bus is indicated using only one bold line in FIG. 8. However, it does not indicate that there is only one bus or only one type of bus.

~~[00166]~~[00167] In this embodiment of this application, the processor 802 may be a general-purpose processor, a digital signal processor, an application-specific integrated circuit, a field programmable gate array or another programmable logic device, a discrete gate or transistor logic device, or a discrete hardware component. The processor 802 can implement or execute the methods, steps, and logical block diagrams disclosed in embodiments of this application. The general-purpose processor may be a microprocessor or any conventional processor. The steps of the methods disclosed with reference to embodiments of this application may be directly performed by a hardware processor, or may be performed by a combination of hardware in a processor and a software module.

~~[00167]~~[00168] The memory 801 may be a ROM, another type of static storage device that can store static information and instructions, a RAM, or another type of dynamic storage device that can store information and instructions, or may be an electrically erasable programmable read-only memory (electrically erasable programmable read-only memory, EEPROM), a compact disc read-only memory (compact disc read-only memory, CD-ROM) or another compact disc storage, an optical disc storage (including a compact disc, a laser disc, an optical disc, a digital versatile disc, a Blu-ray disc, and the like), a magnetic disk storage medium or another magnetic storage device, or any other medium that can be configured to carry or store expected program code in an instruction form or a data structure form and that can be accessed by a computer. However, the memory 801 is not limited thereto. The memory may exist independently and is connected to the processor through the communication bus 804. Alternatively, the memory may be integrated with the processor.

~~[00168]~~[00169] The memory 801 is configured to store computer-executable instructions for performing the solutions of this application, and the processor 802 controls the execution. The processor 802 is configured to execute the computer-executable instructions stored in the memory 801, to implement the method for protecting terminal parameters update provided in the foregoing

embodiment of this application.

~~[00169]~~[00170] Optionally, the computer-executable instructions in this embodiment of this application may also be referred to as application program code. This is not specifically limited in this embodiment of this application.

~~[00170]~~[00171] An embodiment of this application further provides a communication apparatus, which may be a circuit. The communication apparatus may be configured to perform actions performed by the UDM or the first AUSF in the foregoing method embodiments.

~~[00171]~~[00172] An embodiment of this application further provides a communication system. Specifically, the communication system includes a UDM and an ~~ASUF~~AUSF. For example, the communication system includes a UDM and an AUSF for implementing related functions in FIG. 4, FIG. 5, and FIG. 6. Optionally, the communication system may further include more UDMs and/or AUSFs.

~~[00172]~~[00173] The UDM is configured to implement UDM-related functions in FIG. 4, FIG. 5, and FIG. 6. The AUSF is configured to implement AUSF-related functions in FIG. 5, FIG. 6, FIG. 7, or FIG. 8. For details, refer to related description in the method embodiments. Details are not described herein again.

~~[00173]~~[00174] An embodiment of this application further provides a computer-readable storage medium, including instructions. When the instructions are run on a computer, the computer is enabled to perform the methods performed by the UDM or the AUSF in FIG. 4, FIG. 5, and FIG. 6.

~~[00174]~~[00175] An embodiment of this application further provides a computer program product, including instructions. When the instructions are run on a computer, the computer is enabled to perform the methods performed by the UDM or the AUSF in FIG. 4, FIG. 5, and FIG. 6.

~~[00175]~~[00176] An embodiment of this application provides a chip system. The chip system includes a processor, and may further include a memory for implementing functions of the UDM and the AUSF in the foregoing method. The chip system may include a chip, or may include a chip and another discrete component.

~~[00176]~~[00177] All or some of the methods in embodiments of this application may be implemented using software, hardware, firmware, or any combination thereof. When software is used for implementation, embodiments may be implemented completely or partially in a form of a computer program product. The computer program product includes one or more computer

instructions. When the computer program instructions are loaded and executed on a computer, the procedures or the functions according to embodiments of the present invention are all or partially generated. The computer may be a general-purpose computer, a dedicated computer, a computer network, a network device, user equipment, or another programmable apparatus. The computer instructions may be stored in a computer-readable storage medium or may be transmitted from a computer-readable storage medium to another computer-readable storage medium. For example, the computer instructions may be transmitted from a website, computer, server, or data center to another website, computer, server, or data center in a wired (for example, a coaxial cable, an optical fiber, or a digital subscriber line (digital subscriber line, DSL for short)) or wireless (for example, infrared, radio, or microwave) manner. The computer-readable storage medium may be any usable medium accessible by a computer, or a data storage device, for example, a server or a data center, integrating one or more usable media. The usable medium may be a magnetic medium (for example, a floppy disk, a hard disk, or a magnetic tape), an optical medium (for example, a digital video disc (digital video disc, DVD for short)), a semiconductor medium (for example, an SSD), or the like.

~~[00177]~~[00178] It is clearly that a person skilled in the art can make various modifications and variations to this application without departing from the scope of this application. This application is intended to cover these modifications and variations of this application provided that they fall within the scope of protection defined by the following claims and their equivalent technologies.

CLAIMS

What is claimed is:

~~1. A method for protecting terminal parameters update, comprising:~~

~~sending, by a unified data management UDM, a protection request message to a first authentication service function AUSF, wherein the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first serving network;~~

~~receiving, by the UDM, a response message that is of the protection request message and that is sent by the first AUSF; and~~

~~sending, by the UDM, the parameters update information via an access and mobility management function AMF corresponding to the first serving network.~~

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

~~before the UDM sends the protection request message to the first AUSF, determining, by the UDM, the information about the first serving network according to a local policy.~~

~~3. The method according to claim 2, wherein when determining that there are multiple serving networks, the UDM determines the first serving network for terminal parameters update.~~

~~4. The method according to claim 2 or 3, wherein the method further comprises:~~

~~determining, by the UDM, the first AUSF based on the information about the first serving network.~~

~~5. The method according to any one of claims 1 to 4, wherein the method further comprises:~~

~~before the UDM sends the protection request message to the first AUSF, determining, by the UDM, that~~

~~the first AUSF comprises authentication results for a terminal in multiple serving networks, wherein the multiple serving networks comprise the first serving network;~~

~~the terminal is in multiple serving networks, wherein the multiple serving networks comprise the first serving network; or~~

~~the terminal is in a dual-registration mode.~~

~~6. The method according to any one of claims 1 to 5, wherein the information about the first serving network comprises a name of the first serving network;~~

~~the information about the first serving network comprises a public land mobile network~~

PLMN identifier ID of the first serving network or an ID of the first serving network; or

the information about the first serving network comprises an authentication event identifier of the terminal.

7. The method according to any one of claims 1 to 6, wherein the parameters update information comprises steering of roaming SoR information.

8. A method for protecting terminal parameters update, comprising:

receiving, by a first authentication service function AUSF, a protection request message sent by a unified data management UDM, wherein the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first serving network;

determining, by the first AUSF, a first key based on the information about the first serving network, wherein the first key is for protecting the parameters update information; and

security protecting, by the first AUSF, the parameters update information based on the first key.

9. The method according to claim 8, wherein the information about the first serving network is information about one of multiple first serving networks that is stored by the UDM.

10. The method according to claim 8 or 9, wherein there are multiple AUSFs, and the first AUSF is an AUSF corresponding to the information about the first serving network.

11. The method according to claim 8 or 9, wherein the first AUSF comprises authentication results for a terminal in multiple serving networks, and the multiple serving networks comprise the first serving network;

the terminal is in multiple serving networks, wherein the multiple serving networks comprise the first serving network; or

the terminal is in a dual-registration mode.

12. The method according to any one of claims 8 to 11, wherein the information about the first serving network comprises a name of the first serving network;

the information about the first serving network comprises a public land mobile network PLMN identifier of the first serving network; or

the information about the first serving network comprises an authentication event identifier of the terminal.

13. The method according to any one of claims 8 to 12, wherein the parameters update

information comprises steering of roaming SoR information.

14. A communication apparatus, comprising a processing module and a transceiver module, wherein

the transceiver module is configured to send a protection request message to a first authentication service function AUSF, wherein the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first serving network;

the transceiver module is configured to receive a response message that is of the protection request message and that is sent by the first AUSF; and

the processing module is configured to control the transceiver module to send the parameters update information via an access and mobility management function AMF corresponding to the first serving network.

15. The communication apparatus according to claim 14, wherein the transceiver module is further configured to:

determine the information about the first serving network according to a local policy before sending the protection request message to the first AUSF.

16. The communication apparatus according to claim 15, wherein the processing module is specifically configured to: when determining that there are multiple serving networks, determine the first serving network for terminal parameters update.

17. The communication apparatus according to claim 15 or 16, wherein the processing module is specifically configured to:

determine the first AUSF based on the information about the first serving network.

18. The communication apparatus according to any one of claims 14 to 17, wherein the processing module is specifically configured to: before the protection request message is sent to the first AUSF, determine that

the first AUSF comprises authentication results for a terminal in multiple serving networks, wherein the multiple serving networks comprise the first serving network;

the terminal is in multiple serving networks, wherein the multiple serving networks comprise the first serving network; or

the terminal is in a dual-registration mode.

19. The communication apparatus according to any one of claims 14 to 18, wherein the

information about the first serving network comprises a name of the first serving network;

the information about the first serving network comprises a public land mobile network PLMN identifier ID of the first serving network or an ID of the first serving network; or

the information about the first serving network comprises an authentication event identifier of the terminal.

20. The communication apparatus according to any one of claims 14 to 19, wherein the parameters update information comprises steering of roaming SoR information.

21. A communication apparatus, comprising a processing module and a transceiver module, wherein

the transceiver module is configured to receive a protection request message sent by a unified data management UDM, wherein the protection request message requests to protect terminal parameters update information, and the protection request message carries the parameters update information and information about a first serving network;

the processing module is configured to determine a first key based on the information about the first serving network, wherein the first key is for protecting the parameters update information; and

the processing module is configured to security protect the parameters update information based on the first key.

22. The communication apparatus according to claim 21, wherein the information about the first serving network is information about one of multiple first serving networks that is stored by the UDM.

23. The communication apparatus according to claim 21 or 22, wherein there are multiple AUSFs, and the first AUSF is an AUSF corresponding to the information about the first serving network.

24. The communication apparatus according to claim 21 or 22, wherein the first AUSF comprises authentication results for a terminal in multiple serving networks, and the multiple serving networks comprise the first serving network;

the terminal is in multiple serving networks, wherein the multiple serving networks comprise the first serving network; or

the terminal is in a dual-registration mode.

25. The communication apparatus according to any one of claims 21 to 24, wherein the

~~information about the first serving network comprises a name of the first serving network;~~

~~the information about the first serving network comprises a public land mobile network PLMN identifier of the first serving network; or~~

~~the information about the first serving network comprises an authentication event identifier of the terminal.~~

~~26. The communication apparatus according to any one of claims 21 to 25, wherein the parameters update information comprises steering of roaming SoR information.~~

1. A communication method, comprising:

receiving, by a communication apparatus, a security mode command, SMC, message or an extensible authentication protocol success, EAP, success message; and

deleting, by the communication apparatus, a stored old authentication service function key, KAUSF, upon receiving the SMC message or receiving the EAP success message.

2. The method according to claim 1, when the method is implemented in 5G authentication and key agreement, AKA, authentication, the method further comprises:

receiving, by the communication apparatus, an authentication request from a security anchor function, wherein the authentication request comprises an authentication token, AUTN;

calculating, by the communication apparatus, an authentication response and a second KAUSF after successfully verifying the AUTN;

sending, by the communication apparatus, the authentication response to the security anchor function.

3. The method according to claim 1, when the method is implemented in EAP-AKA' authentication, the method is implemented in further comprises:

receiving, by the communication apparatus, an authentication request from a security anchor function;

calculating, by the communication apparatus, an authentication response and keys CK' and IK';

sending, by the communication apparatus, the authentication response comprised in an EAP response to the security anchor function; and

generating, by the communication apparatus, a second KAUSF based on the keys CK' and IK' after receiving the EAP success message.

4. A communication apparatus, wherein the communication apparatus comprises a processor

and a memory, the memory is configured to store program instructions, and the processor is configured to execute the program instructions stored in the memory to perform:

receiving a security mode command, SMC, message or an extensible authentication protocol success, EAP, success message;

deleting a stored old authentication service function key, K_{AUSF}, upon receiving the SMC message or receiving the EAP success message.

5. The apparatus according to claim 4, wherein the processor is configured to execute the program instructions stored in the memory to further perform:

receiving an authentication request from a security anchor function, wherein the authentication request comprises an authentication token, AUTN;

calculating an authentication response and a second K_{AUSF} after successfully verifying the AUTN;

sending the authentication response to the security anchor function.

6. The apparatus according to claim 4, wherein the processor is configured to execute the program instructions stored in the memory to further perform:

receiving an authentication request from a security anchor function;

calculating an authentication response and keys CK' and IK';

sending the authentication response comprised in an EAP response to the security anchor function; and

generating a second K_{AUSF} based on the keys CK' and IK' after receiving the EAP success message.

7. A communication method, comprising:

authenticating, by an authentication service function network element, an authentication response returned by a communication apparatus, and

deleting, by the authentication service function network element, an old authentication service function key, K_{AUSF}, corresponding to the communication apparatus if the authentication succeeds.

8. The method according to claim 7, when the method is implemented in 5G AKA authentication, the method further comprises:

receiving, by the authentication service function network element, an authentication obtaining response of the communication apparatus from a unified data management, wherein the

authentication obtaining response comprises a first KAUSF;

sending, by the authentication service function network element, an authentication response to a security anchor function, wherein the authentication response sent to the security anchor function comprises an authentication token, AUTN; and

receiving, by the authentication service function network element, an authentication request of the communication apparatus from the security anchor function, wherein the authentication request comprises the authentication response returned by the communication apparatus.

9. The method according to claim 7, when the method is implemented in EAP-AKA' authentication, the method further comprises:

receiving, by the authentication service function network element, an authentication obtaining response of the communication apparatus from a unified data management, wherein the authentication obtaining response comprises keys CK'and IK';

sending, by the authentication service function network element, an authentication response to a security anchor function;

receiving, by the authentication service function network element, an authentication request of the communication apparatus from the security anchor function, wherein the authentication request comprises the authentication response returned by the communication apparatus comprised in an extensible authentication protocol, EAP, response; and

generating, by the authentication service function network element, a first KAUSF based on the keys CK' and IK' if the authentication of the authentication response returned by the terminal succeeds;

sending, by the authentication service function network element, an authentication response to the security anchor function, wherein the terminal authentication response comprises an EAP success message.

10. A communication apparatus, wherein the communication apparatus comprises at least a processor and a memory, the memory is configured to store program instructions, and the processor is configured to execute the program instructions stored in the memory to perform:

authenticating an authentication response returned by a second communication apparatus, and

deleting an old authentication service function key, KAUSF, corresponding to the second communication apparatus if the authentication succeeds.

11. The apparatus according to claim 10, wherein the processor is configured to execute the

program instructions stored in the memory to further perform:

receiving an authentication obtaining response of the second communication apparatus from a unified data management, wherein the authentication obtaining response comprises a first K_{AUSF};

sending an authentication response to a security anchor function, wherein the authentication response sent to the security anchor function comprises an authentication token, AUTN; and

receiving an authentication request of the second communication apparatus from the security anchor function, wherein the authentication request comprises the authentication response returned by the second communication apparatus.

12. The apparatus according to claim 10, wherein the processor is configured to execute the program instructions stored in the memory to further perform:

receiving an authentication obtaining response of the second communication apparatus from a unified data management, wherein the authentication obtaining response comprises keys CK'and IK';

sending an authentication response to a security anchor function;

receiving an authentication request of the second communication apparatus from the security anchor function, wherein the authentication request comprises the authentication response returned by the second communication apparatus comprised in an extensible authentication protocol, EAP, response; and

generating a first K_{AUSF} based on the keys CK' and IK' if the authentication of the authentication response returned by the terminal succeeds;

sending an authentication response to the security anchor function, wherein the terminal authentication response comprises an EAP success message.

13. A communication method, comprising:

receiving, by an authentication service function network element, an authentication obtaining response of a terminal from a unified data management, wherein the authentication obtaining response comprises a first authentication service function key, K_{AUSF};

sending, by the authentication service function network element, a terminal authentication response to a security anchor function, wherein the terminal authentication response comprises an authentication token, AUTN; and

receiving, by the security anchor function, the terminal authentication response;

sending, by the security anchor function, an authentication request to the terminal;

receiving, by the security anchor function, an authentication response returned by the terminal;

sending, by the security anchor function, an authentication request of the terminal to the authentication service function network element, wherein the authentication request comprises the authentication response returned by the terminal;

receiving, by the authentication service function network element, the authentication request;

authenticating, by the authentication service function network element, the authentication response returned by the terminal; and

deleting, by the authentication service function network element, an old K_{AUSF} corresponding to the terminal if the authentication succeeds.

14. A communication method, comprising:

receiving, by a authentication service function network element, an authentication obtaining response of a terminal from a unified data management, wherein the authentication obtaining response comprises keys CK'and IK';

sending, by the authentication service function network element, a terminal authentication response to a security anchor function;

receiving, by the security anchor function, the terminal authentication response;

sending, by the security anchor function, an authentication request to the terminal;

receiving, by the security anchor function, an authentication response comprised in an extensible authentication protocol, EAP, response from the terminal;

sending, by the security anchor function, an authentication request of the terminal to the authentication service function network element, wherein the authentication request comprises the EAP response;

receiving, by the authentication service function network element, the authentication request of the terminal; and

authenticating, by the authentication service function network element, the authentication response returned by the terminal, and

generating, by the authentication service function network element, a first authentication service function key, $K_{AUSF,}$ based on the keys CK' and IK', and deleting, by the authentication service function network element, an old K_{AUSF} corresponding to the terminal if the authentication succeeds;

sending, by the authentication service function network element, a terminal authentication

response to the security anchor function, wherein the terminal authentication response comprises an EAP success message;

receiving, by the security anchor function, the EAP success message, and sending the EAP message to the terminal.

15. A communication system, comprising an authentication service function network element and a security anchor function,

wherein the authentication service function network element is configured to:

receive an authentication obtaining response of a terminal from a unified data management, wherein the authentication obtaining response comprises a first authentication service function key, KAUSF;

send a terminal authentication response to a security anchor function, wherein the terminal authentication response comprises an authentication token, AUTN; and

wherein the security anchor function is configured to:

receive the terminal authentication response;

send an authentication request to the terminal;

receive an authentication response returned by the terminal;

send an authentication request of the terminal to the authentication service function network element, wherein the authentication request comprises the authentication response returned by the terminal;

wherein the authentication service function network element is further configured to:

receive the authentication request;

authenticate the authentication response returned by the terminal; and

delete an old KAUSF corresponding to the terminal if the authentication succeeds.

16. A communication system, comprising an authentication service function network element and a security anchor function,

wherein the authentication service function network element is configured to:

receive an authentication obtaining response of a terminal from a unified data management, wherein the authentication obtaining

response comprises keys CK'and IK';

send a terminal authentication response to a security anchor function;

wherein the security anchor function is configured to:

receive the terminal authentication response;

send an authentication request to the terminal;

receive an authentication response from the terminal comprised in an extensible authentication protocol, EAP, response;

send an authentication request of the terminal to the authentication service function network element, wherein the authentication request comprises the EAP response;

wherein the authentication service function network element is further configured to:

receive the authentication request of the terminal; and

authenticate the authentication response returned by the terminal, and

generate a first authentication service function key, KAUSF, based on the keys CK' and IK', and deleting, by the authentication service function network element, an old KAUSF corresponding to the terminal if the authentication succeeds; and

send a terminal authentication response to the security anchor function, wherein the terminal authentication response comprises an EAP success message;

wherein the security anchor function is further configured to:

receive the EAP success message, and send the EAP message to the terminal.

~~27~~17. A communication apparatus, wherein the communication apparatus comprises a processor and a memory, the memory is configured to store ~~a computer~~ program instructions, and the processor is configured to execute the ~~computer~~ program instructions stored in the memory, so that the apparatus performs the method according to any one of claims 1 to ~~7~~ 3~~or claims 8 to 13~~.

18. A communication apparatus, wherein the communication apparatus comprises a processor and a memory, the memory is configured to store program instructions, and the processor is configured to execute the program instructions stored in the memory, so that the apparatus performs the method according to any one of claims 7 to 9.

~~28. A communication system, comprising the communication apparatus according to any one of claims 14 to 20 and the communication apparatus according to any one of claims 21 to 26.~~

~~29~~19. A computer-readable storage medium, wherein the computer-readable storage medium stores ~~a computer~~ program instructions, and when the ~~computer~~ program instructions is executed by a computer, the computer is enabled to perform the method according to any one of claims 1 to ~~7~~ 3~~or claims 8 to 13~~.

20. A computer-readable storage medium, wherein the computer-readable storage medium

stores program instructions, and when the program instructions is executed by a computer, the computer is enabled to perform the method according to any one of claims 7 to 9.

~~30~~21. A computer program product, wherein the computer program product stores ~~a computer~~ program instructions, and when the ~~computer~~ program instructions is executed by a computer, the computer is enabled to perform the method according to any one of claims 1 to ~~7~~ 3~~or claims 8 to 13~~.

22. A computer program product, wherein the computer program product stores program instructions, and when the program instructions is executed by a computer, the computer is enabled to perform the method according to any one of claims 7 to 9.

23. A chip, comprising a processor, wherein when the processor executes program instructions, the chip is enabled to perform the method according to any one of claims 1 to 3.

24. A chip, comprising a processor, wherein when the processor executes program instructions, the chip is enabled to perform the method according to any one of claims 7 to 9.