

TERMINAL INFORMATION TRANSFER METHOD AND RELEVANT PRODUCTS

TECHNICAL FIELD

[0001] The present disclosure relates to the field of communication technologies, and more particularly, to a method for transmitting terminal information and a related product.

BACKGROUND

[0002] In new radio technologies, policy selection related information transmitted between a network device and a terminal is plaintext in the initial registration of the terminal on a network side, and such mechanism has the risk of exposing privacy information of the terminal.

SUMMARY

[0003] Embodiments of the present disclosure provide a method for transmitting terminal information and a related product, which improve the safety of the interaction of information between a network side and a terminal in the inquiring of a terminal policy.

[0004] In a first aspect, an embodiment of the present disclosure provides a method for transmitting terminal information which is applied in a network device which includes a first network element. The method includes:

[0005] receiving, by the first network element, first information from a terminal, wherein the first information is used to indicate a terminal policy stored in the terminal, and includes content that is not represented in the form of plaintext.

[0006] The first network element inquires the terminal policy based on the first information.

[0007] In a second aspect, an embodiment of the present disclosure provides a method for transmitting terminal information which is applied in a terminal. The method includes:

[0008] receiving, by the terminal, second information from a first network element, wherein the second information is used to indicate a terminal policy stored by the terminal, and includes content that is not represented in the form of plaintext.

[0009] The terminal inquires the terminal policy based on the second information.

[0010] In a third aspect, an embodiment of the present disclosure provides a network device, which has functions of implementing an action of a first network device in the design of the above methods. The functions may be implemented by hardware or by corresponding software implemented by hardware. The hardware or software includes one or more modules corresponding to the functions described above. In a possible design, the network device includes a processor which is configured to support the network device to perform corresponding functions in the methods described above. Further, the network device may further include a transceiver which supports communication between the network device and the terminal. Further, the network device may further include a memory which is coupled to the processor and stores program instructions and data necessary for the network device.

[0011] In a fourth aspect, an embodiment of the present disclosure provides a terminal, which has functions of implementing an action of a first terminal in the design of the above methods. The functions may be implemented by hardware or by corresponding software implemented by hardware. The hardware or software includes one or more modules corresponding to the functions described above. In a possible design, the terminal includes a processor which is configured to support the terminal to perform corresponding functions in the methods described above. Further, the terminal may further include a transceiver which supports communication between the terminal and the network device. Further, the terminal may further include a memory which is coupled to the processor and stores program instructions and data necessary for the terminal.

[0012] In a fifth aspect, an embodiment of the present disclosure provides a network device including a processor, a memory, a transceiver and one or more programs. The one or more programs are stored in the memory and executed by the processor, the programs including instructions for performing steps in any of the methods in the first aspect of the embodiment of the present disclosure.

[0013] In a sixth aspect, an embodiment of the present disclosure provides a terminal including a processor, a memory, a transceiver and one or more programs. The one or more programs are stored in the memory and executed by the processor, the programs including instructions for performing steps in any of the methods in the second aspect according to the

embodiments of the present disclosure.

[0014] In a seventh aspect, an embodiment of the present disclosure provides a computer readable storage medium storing computer programs for electronic data exchange, wherein the computer programs cause a computer to perform all or part of the steps described in any of the methods in the first aspect according to the embodiments of the present disclosure.

[0015] In an eighth aspect, an embodiment of the present disclosure provides a computer readable storage medium storing computer programs for electronic data exchange, wherein the computer programs cause a computer to perform all or part of the steps described in any of the methods in the second aspect according to the embodiments of the present disclosure.

[0016] In a ninth aspect, an embodiment of the present disclosure provides a computer program product which includes a non-transitory computer readable storage medium storing computer programs which are operable to cause a computer to perform all or part of the steps described in any of the methods in the first aspect according to the embodiments of the present disclosure. The computer program product can be a software installation package.

[0017] In a tenth aspect, an embodiment of the present disclosure provides a computer program product which includes a non-transitory computer readable storage medium storing computer programs which are operable to cause a computer to perform all or part of the steps described in any of the methods in the second aspect of the embodiment of the present disclosure. The computer program product can be a software installation package.

[0018] It can be seen that in the embodiments of the present disclosure, the first network element of the network device firstly receives the first information from the terminal, and secondly inquires the terminal policy based on the first information. Since the first information is non-plaintext content, the first information can be prevented from being illegally stolen and directly utilized during transmission of the first information between the first network element and the terminal, which is beneficial to improving the safety of the interaction of information between the network side and the terminal in the inquiring of the terminal policy.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] Hereinafter, the accompanying drawings to be used in the description of the embodiments or the prior art will be described briefly.

[0020] Fig. 1A is a diagram of a network architecture of a possible communication system according to an embodiment of the present disclosure.

[0021] Fig. 1B is a diagram of an example of a relationship between a terminal policy and a PSI parameter according to an embodiment of the present disclosure.

[0022] Fig. 2A is a schematic flowchart of a method for transmitting terminal information according to an embodiment of the present disclosure.

[0023] Fig. 2B shows an example format for identifying a PSI parameter of a UE policy according to an embodiment of the present disclosure.

[0024] Fig. 2C is another example format for identifying a PSI parameter of a UE policy according to an embodiment of the present disclosure.

[0025] Fig. 2D is another example format for identifying a PSI parameter of a UE policy according to an embodiment of the present disclosure.

[0026] Fig. 2E is an example format of first information according to an embodiment of the present disclosure.

[0027] Fig. 2F is another example format of first information according to an embodiment of the present disclosure.

[0028] Fig. 2G is an exemplary diagram illustrating the processing of encrypting and transmitting a registration and request message according to an embodiment of the present disclosure.

[0029] Fig. 3A is a schematic flowchart of a method for transmitting terminal information according to an embodiment of the present disclosure.

[0030] Fig. 3B is a schematic flowchart of a method for transmitting terminal information according to an embodiment of the present disclosure.

[0031] Fig. 3C is a schematic flowchart of a method for transmitting terminal information according to an embodiment of the present disclosure.

[0032] Fig. 4A is a schematic flowchart of a method for transmitting terminal

information according to an embodiment of the present disclosure.

[0033] Fig. 4A1 is a schematic diagram of a correspondence between a user identifier and a PSI parameter according to an embodiment of the present disclosure.

[0034] Fig. 4A2 is a schematic diagram of another correspondence between a user identifier and a PSI parameter according to an embodiment of the present disclosure.

[0035] Fig. 4B is a schematic flowchart of another method for transmitting terminal information according to an embodiment of the present disclosure.

[0036] Fig. 4C is a schematic flowchart of another method for transmitting terminal information according to an embodiment of the present disclosure.

[0037] Fig. 4D is a schematic flowchart of another method for transmitting terminal information according to an embodiment of the present disclosure.

[0038] Fig. 5 is a structure diagram of a network device according to an embodiment of the present disclosure.

[0039] Fig. 6 is a structure diagram of a terminal according to an embodiment of the present disclosure.

[0040] Fig. 7 is a structure diagram of a network device according to an embodiment of the present disclosure.

[0041] Fig. 8 is a structure diagram of a terminal according to an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0042] Technical solutions in embodiments of the present disclosure will be described below with reference to the accompanying drawings.

[0043] Fig. 1A exemplarily illustrates a wireless communication system involved in the present disclosure. A wireless communication system 100 is operated at a high frequency band. The wireless communication system 100 is not limited to a Long Term Evolution (LTE) system, and can also be a future evolution system, such as the 5th generation (5G) mobile communication system, a new radio (NR) system, or a Machine to Machine (M2M) communication system. The wireless communication system 100 includes one or more network devices 101, one or more terminals 103 and a core network device 105. The network

device 101 may be a base station, which is used to communicate with one or more terminals, or may be used to communicate with one or more base stations having part of terminal functions (e.g. a macro base station and a micro base station). The base station can be a Base Transceiver Station (BTS) in a Time Division Synchronous Code Division Multiple Access (TD-SCDMA) system, an Evolutional Node B (eNB) in a LTE system, or a base station in a 5G system and a new radio (NR) system. Furthermore, the base station can also be an Access Point (AP), a Trans (TRP) node, a Central Unit (CU) or other network entities, and can include all or a part of functions of the above network entities. The core network device 105 includes core network side devices, such as Access and Mobility Management Function (AMF) entities, User Plane Function (UPF) entities and Session Management Function (SMF) entities. The terminal 103 is distributed throughout the wireless communication system 100, either stationarily or movably. In some embodiments of the present disclosure, the terminal 103 may be a mobile device (e.g. a smart phone), a mobile station, a mobile unit, an M2M terminal, a wireless unit, a remote unit, a user agent, a mobile client, and so on.

[0044] It should be noted that the wireless communication system 100 is illustrated in Fig. 1A to more clearly describe the technical solutions of the present disclosure, and it does not impose any limitations on the present disclosure. It will be clear to those skilled in the art that the technical solutions of the present disclosure can be equivalently applicable to similar technical problems as the network architectures evolve and new service scenarios emerge.

[0045] Related technologies of the present disclosure will be described below.

[0046] At present, a terminal policy is referred to as a UE Policy, and includes an access network discovery and selection policy (ANDSP) and a UE Route Selection Policy (URSP). ANDSP is a policy used for selecting a Service Set Identifier (SSID) for Wireless LAN (WLAN) access, and URSP is a policy used for selecting a different packet protocol data unit session (PDU Session). At present, for the UE Policy, a policy section identifier (PSI) parameter has been set up to flexibly recognize the UE Policy. Examples of a WLANSPP policy and a URSP policy in a protocol will be given below.

[0047] 1. Examples of WLANSPP

[0048] Wireless Local Area Network Selection Policy (WLANSPP) rule 1:

[0049] Priority 1, Validity Conditions (PLMN 1), Group of Selection Criteria with

priority 1: PreferredSSIDList = Priority 1: myoperator1, Priority 2: myoperator2, MinimumBackhaulThreshold = 2Mbps in the downlink, Group of Selection Criteria with priority 2, PreferredSSIDList = Priority 1: myoperator3;

[0050] WLANSP rule 2:

[0051] Priority 2, Validity Conditions (PLMN 1), Group of Selection Criteria with priority 1: PreferredRoamingPartnerList = Priority 1: partner1.com, Priority 2: partner2.com, MaximumBSSLoad = 60.

[0052] 2. Examples of URSP

[0053] URSP rule 1:

[0054] Priority: 1, Traffic filter: App=DummyApp, Direct offload: Prohibited, Slice Info: S-NSSAI-a, Continuity Types: SSC Mode 3, DNNs: internet, Access Type: 3GPP access;

[0055] URSP rule 2:

[0056] Priority:2、 Traffic filter: App=App1, App2, Direct offload: Permitted, Slice Info: S-NSSAI-a, Access Type: Non-3GPP access.

[0057] At present, as shown in Tables 1 and 2, for URSP, relevant contents have been specified.

[0058] Table 1: UE Route Selection Policy Rule

Information name	Description	Category	PCF permitted to modify in a UE context	Scope
Rule Precedence	Determines the order the URSP rule is enforced in the UE.	Mandatory (NOTE 1)	Yes	UE context
Traffic descriptor	This part defines the traffic descriptors for the policy			
Application identifiers	Application identifier(s)	Optional	Yes	UE context
IP descriptors	IP 3 tuple(s) (destination IP address or IPv6 network prefix, destination port number, protocol ID of the protocol above IP)	Optional	Yes	UE context
Non-IP descriptors	Descriptor(s) for non-IP traffic	Optional	Yes	UE context

Information name	Description	Category	PCF permitted to modify in a UE context	Scope
Rule Precedence	Determines the order the URSP rule is enforced in the UE.	Mandatory (NOTE 1)	Yes	UE context
List of Route Selection Descriptors	A list of Route Selection Descriptors. The components of a Route Selection Descriptor are described in table 6.6.2-2.	Mandatory		
NOTE 1: Rules in a URSP shall have different precedence values.				

[0059] Table 2: Route Selection Descriptors

Information name	Description	Category	PCF permitted to modify in a UE context	Scope
Route Selection Descriptor Precedence	Determines the order in which the Route Selection Descriptors are to be applied.	Mandatory (NOTE 1)	Yes	UE context
Route selection components	This part defines the route selection components	Mandatory (NOTE 2)		
SSC Mode Selection	One single value of SSC mode.	Optional	Yes	UE context
Network Slice Selection	Either one single value or a list of values of S-NSSAI(s).	Optional	Yes	UE context
DNN Selection	Either one single value or a list of values of DNN(s).	Optional	Yes	UE context
Non-seamless Offload indication	Indicates if the traffic of the matching application is to be offloaded to non-3GPP access outside of a PDU Session.	Optional (NOTE 3)	Yes	UE context
Access Type preference	Indicates the preferred Access Type (3GPP or non-3GPP) when the UE establishes a PDU Session for the matching application.	Optional	Yes	UE context
NOTE 1: Every Route Selection Descriptors in the list shall have a different precedence value. NOTE 2: At least one of the route selection component shall be present. NOTE 3: If this indication is present in a Route Selection Descriptor, no other components shall be included in the Route Selection Descriptor.				

[0060] For example, as shown in Fig. 1B, USRP rule 1-N denotes the first part of the UE policy which corresponds to policy ID: PSI1, and USRP rule 1-M denotes the second part of the UE policy which corresponds to policy ID: PSI2, and ANDSP denotes the third part of the UE policy which corresponds to policy ID: PSI3. Therefore, one SUPI generally corresponds to one or more PSIs on a network side. For the use of PSI, a policy section

identifier PSI saved in the terminal is added to an initial registration request message to be transmitted to a packet control function (PCF) network element. In this way, the PCF network element may be aware of PSI that is currently stored in the terminal and adjust the UE Policy as required. Since PSI added in the initial registration request message is plaintext, it can be easily intercepted by the other party, which may result in the security issue: the terminal's privacy information is exposed and an attacker may use the information for illegal acts.

[0061] In view of the above issue, the following embodiments are provided in the present disclosure, and will be described in detail below with reference to the accompanying drawings.

[0062] Fig. 2A shows a method for transmitting terminal information according to an embodiment of the present disclosure. The method is applied in a network device in the above exemplary communication system, and the network device includes a first network element. The method includes the following steps:

[0063] In step 201, the first network element receives first information from a terminal.

[0064] The first network element can be a policy control function (PCF) network element. The first information may be transparently transmitted to the PCF network element by the terminal via an access network (RAN) device and an Access and Mobility Management Function (AMF) network element.

[0065] The first information is used to indicate a terminal policy stored in the terminal, and includes non-plaintext contents. The non-plaintext contents specifically indicate that contents that are included in the first information and are indicative of a device identifier (corresponding to a user ID) of the terminal are non-plaintext identification information. The non-plaintext identification information specifically can be encrypted information (which is encrypted in the form of SUCI or encrypted by other secret keys such as a first secret key and/or is under integrity protection using a second secret key) or identification information in other format that is in direct association with the terminal policy and that does not directly contain the user ID (e.g. SUPI).

[0066] In step 202, the first network element inquires the terminal policy based on the first information.

[0067] It can be seen that in the embodiment of the present disclosure, the first network element of the network device firstly receives the first information from the terminal, and secondly inquires the terminal policy based on the first information. Since the first information are non-plaintext contents, the first information can be prevented from being illegally stolen and directly utilized during the transmission of the first information between the first network element and the terminal, which is beneficial to improving the safety of the interaction of information between the network side and the terminal in the inquiring of the terminal policy.

[0068] In a possible example, the first information is used to indicate a terminal policy that is stored in the terminal; after the first network element receives the first information from the terminal, the method further includes:

[0069] inquiring, by the first network element, the terminal policy based on the first information.

[0070] In a possible example, the first information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID.

[0071] For example, it is assumed that the terminal should include 4 UE policies, which are respectively a first part of the UE policy, a second part of the UE policy, a third part of the UE policy and a fourth part of the UE policy. The first part of the UE policy is identified by PSI1, and the second part of the UE policy is identified by PSI2, and the third part of the UE policy is identified by PSI3, and the fourth part of the UE policy is identified by PSI4. As shown in Table 3, the first information can include a PSI list as shown in Table 3.

[0072] Table 3

UE policy of terminal	PSI parameter
first part of UE policy	PSI1
second part of UE policy	PSI2
third part of UE policy	PSI3
fourth part of UE policy	PSI4

[0073] As shown in Fig. 2B, an example format for identifying a PSI parameter of the UE policy includes a user ID and a unique ID. The user ID may be SUPI or SUCI or MSISDN or Domain Name, and the unique ID1 may be a serial number of the UE policy, for

example, the unique ID corresponding to the first part of the UE policy is 1, and the unique ID corresponding to the third part of the UE policy is 3.

[0074] As shown in Fig. 2C, another example format for identifying the PSI parameter of the UE policy includes a public land mobile network (PLMN) and a unique ID. The PLMN+unique ID uniquely identifies the global uniqueness of the corresponding UE policy. There will be a great number of bits in the unique ID (in the order of hundreds of millions) and one SUPI can carry multiple PSI IDs, which has a great impact on the network side.

[0075] In a possible example, the first information includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

[0076] For example, it is assumed that the terminal should include 4 UE policies, which are respectively a first part of the UE policy, a second part of the UE policy, a third part of the UE policy and a fourth part of the UE policy. The first part of the UE policy is identified by unique ID1, the second part of the UE policy is identified by unique ID2, the third part of the UE policy is identified by unique ID3, and the fourth part of the UE policy is identified by unique ID4. As shown in Table 4, the first information can include a PSI list as shown in Table 4.

UE policy of terminal	PSI parameter
first part of UE policy	unique ID1
first part of UE policy	unique ID2
third part of UE policy	unique ID 3
fourth part of UE policy	unique ID 4

[0077] The unique ID is a unique code generated by the network side (e.g. the first network element). The unique code is in one-to-one correspondence to contents corresponding to the PSI. The network side may index the contents corresponding to the PSI based on the unique code.

[0078] For example, as shown in Fig. 2D, it is assumed that four PSI parameters of the terminal include PSI1, PSI2, PSI3 and PSI4. The network side randomly generates a unique code for each of the PSI parameters and these unique codes include unique ID1, unique ID2, unique ID3 and unique ID4. Correspondence between the four unique codes and the four PSI parameters may be that PSI1 corresponds to the unique ID1, PSI2 corresponds to

the unique ID2, PSI3 corresponds to the unique ID3, and PSI4 corresponds to the unique ID4.

[0079] In a possible example, the first information includes a PLMN ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

[0080] For example, it is assumed that the terminal should include four UE policies, which are respectively a first part of the UE policy, a second part of the UE policy, a third part of the UE policy and a fourth part of the UE policy. The first part of the UE policy is identified by the unique ID1, the second part of the UE policy is identified by the unique ID2, the third part of the UE policy is identified by the unique ID3, and the fourth part of the UE policy is identified by the unique ID4. As shown in Fig. 2E, the first information may include a PLMN ID and a PSI list.

[0081] In a possible example, the first information includes a PSI list, and each PSI parameter in the PSI list is represented by a PLMN ID and a unique ID.

[0082] For example, it is assumed that the terminal should include four UE policies, which are respectively a first part of the UE policy, a second part of the UE policy, a third part of the UE policy and a fourth part of the UE policy. The first part of the UE policy is identified by PLMN ID + unique ID1, the second part of the UE policy is identified by PLMN ID + unique ID2, the third part of the UE policy is identified by PLMN ID + unique ID3, and the fourth part of the UE policy is identified by PLMN ID + unique ID4. As shown in Fig. 2F, the first information may include a PSI list as shown in 2F.

[0083] In a possible example, PSI parameter(s) in the PSI list is(are) globally unique; or the PSI parameter(s) in the PSI list is(are) unique within the PLMN.

[0084] In a possible example, the user ID or the PSI parameter includes any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), Mobile Subscriber International ISDN/PSTN number (MSISDN) and a Domain Name.

[0085] The unique ID is used to indicate any one of a preset number of terminal policies under the constraint of the user ID. When the user ID is SUPI or SUCI, the preset number is less than a preset threshold, which may be 10.

[0086] In a possible example, when the user ID is not SUPI, the method further includes:

[0087] inquiring, by the first network element, a SUPI value corresponding to the user

ID from the second network element.

[0088] In a possible example, the second network element has a subscription identifier de-concealing function (SIDF).

[0089] In a possible example, inquiring, by the first network element, the terminal policy based on the first information includes:

[0090] inquiring, by the first network element, the terminal policy from a third network element using the SUPI and/or the unique ID.

[0091] In a possible example, inquiring, by the first network element, the terminal policy based on the first information includes:

[0092] directly inquiring, by the first network element, the terminal policy from the third network element using the PSI parameter(s) in the first information reported by the terminal.

[0093] In a possible example, the third network element is a core network data storage network element.

[0094] In a possible example, the first information is data transmitted to the first network element by the terminal, and a part or all of the data is encrypted by the first secret key and/or is under integrity protection using the second secret key.

[0095] In a possible example, the method further includes decrypting and/or checking integrity, by the first network element, based on the first information to obtain the first content.

[0096] In a possible example, the method further includes inquiring the terminal policy, by the first network element, based on the first content.

[0097] In a possible example, the first secret key or the second secret key is generated by a third secret key via a preset algorithm.

[0098] In a possible example, the third secret key is sent to the terminal by a fourth network element.

[0099] In a possible example, the fourth network element is an authentication server function (AUSF) network element on the network side.

[00100] The process of encrypting and transmitting the PSI list in the registration request message will be illustratively described below with reference to Fig. 2G.

[00101] A user equipment (UE) first sends an initial request message (e.g. a registration request message) to a base station.

[00102] After receiving the initial request message, the base station forwards it to a core network element.

[00103] After receiving the initial request message, the core network element completes a key negotiation process and an algorithm negotiation process in cooperation with the UE.

[00104] The UE uses a secret key and an algorithm to encrypt and/or carry out the integrity protection of the PSI list, and sends the encrypted and/or integrity-protected PSI list and related contents to the core network element through an uplink non-access stratum (NAS) message.

[00105] After receiving the NAS message, the core network element performs the decryption and/or integrity check of the PSI list and related contents, and at last sends the decrypted PSI list and related contents to a PCF network element through a specific interface (e.g. an N7 interface).

[00106] In a possible example, the first secret key is pre-configured at the first network element and the terminal.

[00107] Correspondingly with the embodiment shown in Fig. 2A, Fig. 3A shows another method for transmitting terminal information according to an embodiment of the present disclosure. The method is applied in a network device in the foregoing exemplary communication system, and the network device includes a first network element. The method includes the following steps:

[00108] In step 3A01, the first network element receives first information from a terminal.

[00109] The first information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID. The first information alternatively includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID. PSI parameter(s) in the PSI list is(are) globally unique; or PSI parameter(s) in the PSI list is(are) unique within a PLMN.

[00110] The user ID or the PSI parameter include any one of a Subscriber Permanent

Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or contents of the PSI parameter.

[00111] The user ID is not a SUPI.

[00112] In step 3A02, the first network element inquires a SUPI value corresponding to the user ID from a second network element.

[00113] The second network element has a subscription identifier de-concealing function (SIDF). For example, the second network element may be a Session Management Function (SMF) network element, and the present disclosure is not limited to this.

[00114] In step 3A03, the first network element inquires the terminal policy from a third network element using the SUPI and/or the unique ID.

[00115] The third network element is a core network data storage network element.

[00116] It can be seen that in the embodiment of the present disclosure, the first network element of the network device firstly receives the first information from the terminal, and secondly inquires the SUPI value corresponding to the user ID in the first information from the second network element, and at last uses the SUPI and/or the unique ID to inquire the terminal policy from the third network element. It is clear that since the first information transmitted between the first network element and the terminal does not directly include any SUPI for indicating an identifier of the terminal, the first information can be prevented from being stolen and directly utilized during transmission of the first information, which is beneficial to improving the safety of the interaction of information between a network side and the terminal in the inquiring of the terminal policy.

[00117] Correspondingly with the embodiments in Figs. 2A and 3A, Fig. 3B shows a method for transmitting terminal information according to an embodiment of the present disclosure. The method is applied in a network device in the foregoing exemplary communication system, and the network device includes a first network element. The method includes the following steps:

[00118] In step 3B01, the first network element receives first information from a

terminal.

[00119] The first information includes a list of policy section identifiers (PSIs), and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID. The first information alternatively includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID. PSI parameter(s) in the PSI list is(are) globally unique; or PSI parameter(s) in the PSI list is(are) unique within a PLMN.

[00120] The user ID or the PSI parameter include any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or content of the PSI parameter.

[00121] The user ID is not a SUPI.

[00122] In step 3B02, the first network element directly inquires the terminal policy from a third network element using the PSI parameter in the first information reported by the terminal.

[00123] The third network element is a core network data storage network element.

[00124] It can be seen that in the embodiment of the present disclosure, the first network element of the network device firstly receives the first information from the terminal, and secondly uses the PSI parameter in the first information reported by the terminal to directly inquire the terminal policy from the third network element. It can be seen that since the PSI parameter in the first information do not directly include any SUPI, the first information can be prevented from being stolen and directly utilized during transmission of the first information, which is beneficial to improving the safety of the interaction of information between a network side and the terminal in the inquiring of the terminal policy.

[00125] Correspondingly with the embodiments in Figs. 2A and 3A, Fig. 3C shows a method for transmitting terminal information according to an embodiment of the present disclosure. The method is applied in a network device in the foregoing exemplary communication system, and the network device includes a first network element. The method includes the following steps:

[00126] In step 3C01, the first network element receives first information from a terminal.

[00127] The first information is data transmitted to the first network element by the terminal, and a part or all of the data is encrypted by a first secret key.

[00128] In step 3C02, the first network element decrypts and/or checks integrity based on the first information to obtain first content.

[00129] The first content includes PSI relevant information, or specific content of a UE policy, and an example in which the first content includes the PSI relevant information will be described.

[00130] In step 3C03, the first network element inquires a terminal policy based on the first content.

[00131] The first secret key or a second secret key is generated by a third secret key via a preset algorithm. The third secret key is sent to the terminal by a fourth network element. The fourth network element is an authentication server function (AUSF) network element on a network side.

[00132] The first secret key is pre-configured at the first network element and the terminal. The first network element is alternatively a policy control function (PCF) network element.

[00133] It can be seen that in the embodiment of the present disclosure, the first network element of the network device firstly receives the first information from the terminal, and secondly decrypts it based on the first secret key to obtain relevant information, and at last inquires the terminal policy of the terminal based on the relevant information. It can be seen that since the first information is encrypted by the first secret key, the first information can be prevented from being stolen and directly utilized during transmission of the first information, which is beneficial to improving the safety of the interaction of information between the network side and the terminal in the inquiring of the terminal policy.

[00134] Correspondingly with the embodiments in Figs. 2A and 3A-3C, Fig. 4A shows a method for transmitting terminal information according to an embodiment of the present disclosure. The method is applied in a terminal in the foregoing exemplary communication system. The method includes the following steps:

[00135] In step 4A01, the terminal receives second information from a first network element.

[00136] The first network element is a network element in a network device.

[00137] The second information is used to indicate a terminal policy stored by the terminal, and includes non-plaintext contents. The non-plaintext contents specifically indicate that contents that are included in the second information and are indicative of a device identifier (corresponding to a user ID) of the terminal are non-plaintext identification information. The non-plaintext identification information specifically can be encrypted information (which is encrypted in the form of SUCI or encrypted by other secret keys such as a first secret key and/or is under integrity protection using a second secret key) or identification information in other format that is in direct association with the terminal policy and that does not directly contain the user ID (e.g. SUPI).

[00138] In step 4A02, the terminal inquires the terminal policy based on the second information.

[00139] It can be seen that in the embodiment of the present disclosure, the terminal firstly receives the first information from the first network element of the network device, and secondly inquires the terminal policy according to the second information. Since the second information are non-plaintext contents, the second information can be prevented from being illegally stolen and directly utilized during the transmission of the second information between the network terminal and the terminal, which is beneficial to improving the safety of the interaction of information between the network side and the terminal in the inquiring of the terminal policy.

[00140] In a possible example, the second information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID.

[00141] In a possible example, the second information includes a PSI list, and each PSI parameter in the PSI list is represented by a PLMN ID and a unique ID.

[00142] In a possible example, the second information includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

[00143] In this possible example, the terminal stores the terminal policy according to a

correspondence between the PLMN ID and a PSI.

[00144] In a roaming scenario, an hPCF of a home location sends to a vPCF a policy, in which a PLMN ID and its corresponding PSI list of the home location are included. In the meanwhile, the vPCF adds a policy of a visited place by itself and forms a PLMN ID and its corresponding PSI list of the visited place. The vPCF then puts the two groups of PLMN IDs and their corresponding PSI lists in one message and sends them to the terminal.

[00145] In a possible example, PSI parameter(s) in the PSI list is(are) globally unique; or PSI parameter(s) in the PSI list is(are) unique within a PLMN.

[00146] In a possible example, the user ID or the PSI parameter(s) includes any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or content of the PSI parameter.

[00147] In a possible example, when the user ID is not SUPI, the method further includes: inquiring, by the terminal, a SUPI value corresponding to the user ID from the second network element.

[00148] In a possible example, the second network element has an identifier de-concealing function.

[00149] In a possible example, inquiring, by the terminal, the terminal policy based on the second information includes:

[00150] inquiring, by the terminal, the terminal policy from a third network element using the SUPI and/or the unique ID.

[00151] In a possible example, inquiring, by the terminal, the terminal policy based on the second information includes: directly inquiring, by the terminal, the terminal policy from the third network element using the PSI parameter in the second information issued by the first network element.

[00152] In a possible example, the third network element is a core network data storage network element.

[00153] In a possible example, the second information is data transmitted to the

terminal by the first network element, and a part or all of the data is encrypted by a first secret key and/or is under integrity protection using the second secret key.

[00154] In a possible example, the method further includes decrypting and/or checking integrity, by the terminal, based on the second information to obtain second content.

[00155] In a possible example, the method further includes inquiring the terminal policy, by the terminal, based on the second content.

[00156] In a possible example, the first secret key or the second secret key is generated by a third secret key via a preset algorithm.

[00157] In a possible example, the third secret key is sent to the terminal by a fourth network element.

[00158] In a possible example, the fourth network element is an authentication server function (AUSF) network element on the network side.

[00159] In a possible example, the first secret key is pre-configured at the first network element and the terminal.

[00160] In a possible example, the first network element is a policy control function (PCF) network element.

[00161] In a possible example, receiving, by the terminal, the second information from the first network element includes receiving, by the terminal, second information sent by the first network element according to mapping relationship information, which includes a correspondence between the user identifiers and the PSI parameters.

[00162] In a possible example, each of the user identifiers corresponds to at least one of the PSI parameters in the mapping relationship information.

[00163] In a possible example, one PSI parameter merely corresponds to one user identifier in the mapping relationship information.

[00164] For example, as shown in Fig. 4A1, it is assumed that 3 user identifiers are included, which are respectively User-1, User-2 and User-3, and 10 PSI parameters are included, which are respectively PSI1, PSI2, PSI3, PSI4, PSI5, PSI6, PSI7, PSI8 and PSI9. PSI1 is used to indicate content 1 of the UE policy, PSI2 is used to indicate content 2 of the UE policy, PSI3 is used to indicate content 3 of the UE policy, PSI4 is used to indicate content 3 of the UE policy, PSI5 is used to indicate content 4 of the UE policy, PSI6 is used

to indicate content 5 of the UE policy, PSI7 is used to indicate content 10 of the UE policy, PSI8 is used to indicate content 9 of the UE policy, and PSI9 is used to indicate content 10 of the UE policy. A mapping relationship between the user identifiers and the PSI parameters may be that User-1 corresponds to PSI1, PSI2 and PSI3, and User-2 corresponds to PSI4, PSI5, PSI6 and PSI7, and User-3 corresponds to PSI8 and PSI9.

[00165] The correspondence between the user identifiers and the PSI parameters may be stored on the network side.

[00166] In a possible example, one PSI parameter at least corresponds to one user identifier in the mapping relationship information.

[00167] For example, as shown in Fig. 4A2, it is assumed that 3 user identifiers are included, which are respectively User-1, User-2 and User-3, and n (n is a positive integer) PSI parameters are included, which are respectively PSI1, PSI2, PSI3... PSIn. PSI1 is used to indicate content 1 of the UE policy, PSI2 is used to indicate content 2 of the UE policy, PSI3 is used to indicate content 3 of the UE policy, and PSI4 is used to indicate content 3 of the UE policy, and so on, and PSIn is used to indicate content n of the UE policy. The correspondence between the user identifiers and the PSI parameters may be that User-1 corresponds to PSI1, PSI3 and PSI5, User-2 corresponds to PSI2 and PSI3, and User-3 corresponds to PSI4, PSI5 and PSIn.

[00168] The correspondence between the user identifiers and the PSI parameters may be stored on the network side.

[00169] Correspondingly with the embodiments in Figs. 2A, 3A-3C and 4A, Fig. 4B shows a method for transmitting terminal information according to an embodiment of the present disclosure. The method is applied in a terminal in the foregoing exemplary communication system, and includes the following steps:

[00170] In step 4B01, the terminal receives second information from a first network element.

[00171] The second information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID. The second information alternatively includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID. PSI parameter(s) in the PSI list is(are) globally

unique; or PSI parameter(s) in the PSI list is(are) unique within a PLMN.

[00172] The user ID or the PSI parameters include any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or contents of the PSI parameters.

[00173] The user ID is not a SUPI.

[00174] In step 4B02, the terminal inquires a SUPI value corresponding to the user ID from a second network element.

[00175] The second network element has a subscription identifier de-concealing function (SIDF). For example, the second network element may be a Session Management Function (SMF) network element, and the present disclosure is not limited to this.

[00176] In step 4B03, the terminal inquires a terminal policy from a third network element using the SUPI and/or the unique ID.

[00177] The third network element is a core network data storage network element.

[00178] It can be seen that in the embodiment of the present disclosure, the terminal firstly receives the second information from a network device, and secondly inquires the SUPI value corresponding to the user ID in the second information from the second network element, and at last uses the SUPI and/or the unique ID to inquiry the terminal policy from the third network element. It can be seen that since the second information transmitted between the terminal and the network device does not directly include the SUPI for indicating an identifier of the terminal, the second information can be prevented from being stolen and directly utilized during transmission of the second information, which is beneficial to improving the safety of the interaction of information between a network side and the terminal in the inquiring of the terminal policy.

[00179] Correspondingly with the embodiments in Figs. 2A, 3A-3C, 4A and 4B, Fig. 4C shows a method for transmitting terminal information according to an embodiment of the present disclosure. The method is applied in a terminal in the foregoing exemplary communication system, and includes the following steps:

[00180] In step 4C01, the terminal receives second information from a first network element.

[00181] The first network element is a network element in a network device.

[00182] The second information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID. The second information alternatively includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID. PSI parameter(s) in the PSI list is(are) globally unique; or PSI parameter(s) in the PSI list is(are) unique within a PLMN.

[00183] The user ID or the PSI parameters include any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or contents of the PSI parameters.

[00184] The user ID is not a SUPI.

[00185] In step 4C02, the terminal directly inquires a terminal policy from a third network element using the PSI parameter(s) in the second information issued by the network device.

[00186] The third network element is a core network data storage network element.

[00187] It can be seen that in the embodiment of the present disclosure, the terminal firstly receives the second information issued by the network device, and secondly uses the PSI parameter(s) in the second information to directly inquire the terminal policy from the third network element. It can be seen that since the PSI parameter(s) in the second information does(do) not directly include the SUPI, the second information can be prevented from being stolen and directly utilized during transmission of the second information, which is beneficial to improving the safety of the interaction of information between a network side and the terminal in the inquiring of the terminal policy.

[00188] Correspondingly with the embodiments in Figs. 2A, 3A-3C and 4A-4C, Fig. 4D shows a method for transmitting terminal information according to an embodiment of the present disclosure. The method is applied in a terminal in the foregoing exemplary

communication system, and includes:

[00189] In step 4D01, the terminal receives second information from a network device.

[00190] The second information is data transmitted to a first network element by the terminal, and a part or all of the data is encrypted by a first secret key.

[00191] The first secret key or a second secret key is generated by a third secret key via a preset algorithm. The third secret key is sent to the terminal by a fourth network element. The fourth network element is an authentication server function (AUSF) network element on a network side.

[00192] The first secret key is pre-configured at the first network element and the terminal. Alternatively, the first network element is a policy control function (PCF) network element.

[00193] In step 4D02, the terminal decrypts and/or checks integrity based on the second information to obtain second content.

[00194] The first content includes PSI relevant information, or specific content of a UE policy, and an example in which the first content includes the PSI relevant information will be described.

[00195] In step 4D03, the terminal inquires a terminal policy based on the second content.

[00196] It can be seen that in the embodiment of the present disclosure, the terminal firstly receives the second information from the network device, and secondly decrypts and/or checks the integrity based on the second information to obtain the second content, and finally inquires the terminal strategy based on the second content. Since decryption is performed and/or integrity is checked based on the second information to obtain the second content of plaintext, so as to inquire the terminal policy, the second information can be prevented from being stolen and directly utilized during transmission of the second information, which is beneficial to improving the safety of the interaction of information between the network side and the terminal in the inquiring of the terminal policy.

[00197] Correspondingly with the above-described embodiments, Fig. 5 is a schematic structural diagram of a network device according to an embodiment of the present disclosure. As shown in the figure, the network device includes a processor, a memory, a communication

interface and one or more programs. The the one or more programs are stored in the memory, and are configured to be executed by the processor. The the one or more programs include instructions for performing the following steps.

[00198] First information is received from a terminal; the first information is used to indicate a terminal policy stored in the terminal, and is content in the form of non-plaintext. The content in the form of non-plaintext specifically indicates that the content that is included in the first information and is indicative of a device identifier (corresponding to a user ID) of the terminal is non-plaintext identification information. The non-plaintext identification information specifically can be encrypted information (which is encrypted in the form of SUCI or encrypted by other secret keys such as a first secret key) or identification information that is in direct association with the terminal policy and that does not directly contain the user ID (e.g. SUPI).

[00199] The terminal policy is inquired based on the first information.

[00200] It can be seen that in the embodiment of the present disclosure, a first network element of the network device firstly receives the first information from the terminal, and secondly inquires the terminal policy based on the first information. Since the first information is the content in the form of non-plaintext, the first information can be prevented from being illegally stolen and directly utilized during transmission of the first information between the first network element and the terminal, which is beneficial to improving the safety of the interaction of information between a network side and the terminal in the inquiring of the terminal policy.

[00201] In a possible example, the first information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID.

[00202] In a possible example, the first information includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

[00203] In a possible example, PSI parameter(s) in the PSI list is(are) globally unique; or the PSI parameter(s) in the PSI list is(are) unique within the PLMN.

[00204] In a possible example, the user ID or the PSI parameters include any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile

Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or contents of the PSI parameters.

[00205] In a possible example, when the user ID is not SUPI, the programs further include instructions to perform an operation of inquiring a SUPI value corresponding to the user ID from the second network element.

[00206] In a possible example, the second network element has a subscription identifier de-concealing function (SIDF).

[00207] In a possible example, when the first network element inquires the terminal policy based on the first information, the instructions in the programs are specifically configured to perform an operation of using the SUPI and/or the unique ID to inquire the terminal policy from the third network element.

[00208] In a possible example, when the user ID is not SUPI, and the first network element inquires the terminal policy based on the first information, the instructions in the programs are specifically configured to perform an operation of using the PSI parameters in the first information reported by the terminal to directly inquire the terminal policy from the third network element.

[00209] In a possible example, the third network element is a core network data storage network element.

[00210] In a possible example, the first information is data transmitted to the first network element by the terminal, and a part or all of the data is encrypted by the first secret key; when the terminal policy is inquired based on the first information, the instructions in the programs are specifically configured to perform an operation of decrypting the first information based on the first secret key to obtain relevant information, and inquiring the terminal policy of the terminal based on the relevant information.

[00211] In a possible example, the first secret key is generated by a second secret key through a preset algorithm.

[00212] In a possible example, the second secret key is provided by a fourth network element, and sent to the terminal by an Access and Mobility Management Function (AMF)

network element, and the fourth network element is an authentication server function (AUSF) network element on the network side.

[00213] In a possible example, the first secret key is pre-configured for the terminal by the network side.

[00214] In a possible example, the first network element is a policy control function (PCF) network element.

[00215] Correspondingly with the above-described embodiments, Fig. 6 is a schematic structural diagram of a terminal according to an embodiment of the present disclosure. As shown in the figure, the terminal includes a processor, a memory, a communication interface and one or more programs. The one or more programs are stored in the memory, are configured to be executed by the processor, and include instructions for performing the following steps:

[00216] Second information is received from a network device. The second information is also used to indicate a terminal policy stored in the terminal, and the second information is content in a form of non-plaintext. The content in the form of non-plaintext specifically indicate that content that is included in the second information and is indicative of a device identifier (corresponding to a user ID) of the terminal is non-plaintext identification information. The non-plaintext identification information specifically can be encrypted information (which is encrypted in the form of SUCI or encrypted by other secret keys such as a first secret key and/or is under integrity protection of a second secret key) or identification information that is in direct association with the terminal policy and that does not directly contain the user ID (e.g. SUPI).

[00217] The terminal policy is inquired based on the second information.

[00218] It can be seen that in the embodiment of the present disclosure, the terminal firstly receives the second information from the network device, and secondly inquires the terminal policy based on the second information. Since the second information is content in the form of non-plaintext, the second information can be prevented from being illegally stolen and directly utilized during transmission of the second information between a first network element and the terminal, which is beneficial to improving the safety of the interaction of information between a network side and the terminal in the inquiring of the

terminal policy.

[00219] In a possible example, the second information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID.

[00220] In a possible example, the second information includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

[00221] In a possible example, PSI parameter(s) in the PSI list is(are) globally unique; or PSI parameter(s) in the PSI list is(are) unique within a PLMN.

[00222] In a possible example, the user ID or the PSI parameters include any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or contents of the PSI parameters.

[00223] In a possible example, when the user ID is not SUPI, the programs further include instructions to perform an operation of inquiring a SUPI value corresponding to the user ID from a second network element.

[00224] In a possible example, the second network element has an identifier de-concealing function.

[00225] In a possible example, when the terminal policy is inquired based on the second information, the instructions in the programs are specifically configured to perform an operation of using the SUPI and/or the unique ID to inquire the terminal policy from the third network element.

[00226] In a possible example, when the terminal policy is inquired based on the second information, the instructions in the programs are specifically configured to perform an operation of inquiring the terminal policy from the third network element using the PSI parameters in the second information issued by the first network element.

[00227] In a possible example, the third network element is a core network data storage network element.

[00228] In a possible example, the second information is data transmitted to the

terminal by the first network element, and a part or all of the data is encrypted by a first secret key and/or is under integrity protection using the second secret key.

[00229] In a possible example, the programs further include instructions to perform an operation of decrypting and/or checking integrity based on the second information to obtain second content.

[00230] In a possible example, the programs further include instructions to perform an operation of inquiring the terminal policy based on the second content.

[00231] In a possible example, the first secret key or the second secret key is generated by a third secret key via a preset algorithm.

[00232] In a possible example, the third secret key is sent to the terminal by a fourth network element.

[00233] In a possible example, the fourth network element is an authentication server function (AUSF) network element on the network side.

[00234] In a possible example, the first secret key is pre-configured at the first network element and the terminal.

[00235] In a possible example, the first network element is a policy control function (PCF) network element.

[00236] The solutions of the embodiments of the present disclosure are described above mainly from the perspective of the interactions among the respective network elements. It can be understood that the terminal and the network device include corresponding hardware structures and/or software modules for performing respective functions in order to implement the above-described functions. Those skilled in the art will readily appreciate that, as can be seen from the the units and algorithm steps of the various examples described in the embodiments disclosed herein, the present disclosure can be carried out by hardware or the combination of hardware and computer software. Whether a function is implemented by hardware or by driving hardware using computer software depends on specific applications and design constraints of the technical solutions. For each of the particular applications, a person skilled in the art can use different methods to implement the described functions, but such implementations should not be considered as exceeding the scope of the application.

[00237] In the embodiments of the present disclosure, function units of the terminal

and the network device may be divided according to the examples of the foregoing methods. For example, the function units may be divided based on their functions, or two or more functions may be integrated into one processing unit. The above integrated units may be implemented by hardware or a software program module. It should be noted that the division of the units in the embodiments of the present disclosure is illustrative, and it is only a kind of logical function division. In practice, other division manners may be used.

[00238] When integrated units are used, Fig. 7 shows a block diagram of a possible construction of function units of the network device in the above embodiments. A network device 700 includes a processing unit 702 and a communication unit 703. The processing unit 702 is used to control and manage actions of the network device. For example, the processing unit 702 is used to support the network device to perform steps 201 and 202 in Fig. 2A, steps 3A01, 3A02 and 3A03 in Fig. 3A, steps 3B01 and 3B02 in Fig. 3B, steps 3C01 to 3C03 in Fig. 3C and/or other procedures of technologies described herein. The communication unit 703 is used to support communication between the network device and other devices, for example communication between the network device and the terminal shown in Fig. 3C. The network device may further include a storage unit 701 used to store program codes and data of the network device.

[00239] The processing unit 702 can be a processor or a controller, for example a Central Processing Unit (CPU), a general-purpose processor, a Digital Signal Processor (DSP), an Application-Specific Integrated Circuit (ASIC), a Field Programmable Gate Array (FPGA) or other programmable logic devices, transistor logic devices, hardware components or any combination thereof. They can implement or carry out the various exemplary logical blocks, modules and circuits described with reference to the contents disclosed by the present disclosure. The processor may also be a combination of components that implement computing functions, for example, a combination of one or more microprocessors, a combination of a DSP and a microprocessor and the like. The communication unit 703 may be a transceiver, a transceiver circuit or the like and the storage unit 701 may be a memory.

[00240] The processing unit 702 is configured to receive first information from the terminal via the communication unit 703. The first information is used to indicate a terminal policy stored by the terminal, and the first information is content that is in the form of

non-plaintext. The content in the form of non-plaintext specifically refers to that content that is included in the first information and is indicative of a device identifier (corresponding to a user ID) of the terminal is non-plaintext identification information. The non-plaintext identification information specifically can be encrypted information (which is encrypted in the form of SUCI or encrypted by other secret keys such as a first secret key) or identification information that is in direct association with the terminal policy and that does not contain the user ID (e.g. SUPI). The terminal policy is inquired based on the first information.

[00241] It can be seen that in this example a first network element of the network device firstly receives the first information from the terminal, and secondly inquires the terminal policy based on the first information. Since the first information is content in the form of non-plaintext, the first information can be prevented from being illegally stolen and directly utilized during transmission of the first information between the first network element and the terminal, which is beneficial to improving the safety of the interaction of information between the network side and the terminal in the inquiring of the terminal policy.

[00242] In a possible example, the first information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID.

[00243] In a possible example, the first information includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

[00244] In a possible example, PSI parameter(s) in the PSI list is(are) globally unique; or PSI parameter(s) in the PSI list is(are) unique within a PLMN.

[00245] In a possible example, the user ID or the PSI parameters include any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or contents of the PSI parameters.

[00246] In a possible example, when the user ID is not a SUPI, the processing unit 702 is further configured to inquire, by the communication unit 703, a SUPI value corresponding to the user ID from a second network element.

[00247] In a possible example, the second network element has a subscription identifier de-concealing function (SIDF).

[00248] In a possible example, when the terminal policy is inquired based on the second information, the processing unit 702 is specifically configured to inquire the terminal policy by the communication unit 703 from a third network element using the SUPI and/or the unique ID.

[00249] In a possible example, when the user ID is not a SUPI and the terminal policy is inquired based on the first information, the processing unit 702 is specifically configured to directly inquire the terminal policy from the third network element using the PSI parameters in the first information reported by the terminal.

[00250] In a possible example, the third network element is a core network data storage network element.

[00251] In a possible example, the first information is data transmitted to the first network element by the terminal, and a part or all of the data is encrypted by the first secret key; and when the terminal policy is inquired based on the first information, the processing unit 702 is specifically configured to decrypt the first information according to the first secret key to obtain relevant information, and inquire the terminal policy of the terminal based on the relevant information.

[00252] In a possible example, the first secret key is generated by a second secret key through a preset algorithm.

[00253] In a possible example, the second secret key is provided by a fourth network element, and sent to the terminal by an Access and Mobility Management Function (AMF) network element and the fourth network element is an authentication server function (AUSF) network element on the network side.

[00254] In a possible example, the first secret key is pre-configured for the terminal by the network side.

[00255] In a possible example, the first network element is a policy control function (PCF) network element.

[00256] When the processing unit 702 is a processor, the communication unit 703 is a communication interface, and the storage unit 701 is a memory, the network device in the

embodiments of the present disclosure may be the network device shown in Fig. 5.

[00257] When integrated units are used, Fig. 8 shows a block diagram of a possible construction of function units of the terminal in the above embodiments. A terminal 800 includes a processing unit 802 and a communication unit 803. The processing unit 802 is used to control and manage actions of the terminal. For example, the processing unit 802 is used to support the terminal to perform steps 4A01 and 4A02 in Fig. 4A, steps 4B01-4B03 in Fig. 4B, steps 4C01 and 4C02 in Fig. 4C, steps 4D01 to 4D03 in Fig. 4D and/or other procedures of technologies described herein. The communication unit 803 is used to support communication between the terminal and other devices, for example communication between the terminal and the network device shown in Fig. 5. The terminal may further include a storage unit 801 used to store program codes and data of the terminal.

[00258] The processing unit 802 can be a processor or a controller, for example a Central Processing Unit (CPU), a general-purpose processor, a Digital Signal Processor (DSP), an Application-Specific Integrated Circuit (ASIC), a Field Programmable Gate Array (FPGA) or other programmable logic devices, transistor logic devices, hardware components or any combination thereof. They can implement or carry out the various exemplary logical blocks, modules and circuits described by referring to the contents disclosed in the present disclosure. The processor may also be a combination of components that implement computing functions, for example, a combination of one or more microprocessors, a combination of a DSP and a microprocessor and the like. The communication unit 803 may be a transceiver, a transceiver circuit or the like and the storage unit 801 may be a memory.

[00259] The processing unit 802 is configured to receive second information from the network device via the communication unit 803. The second information is used to indicate a terminal policy stored by the terminal, and is content in the form of non-plaintext. The content in the form of non-plaintext specifically refer to that the content that is included in the second information and is indicative of a device identifier (corresponding to a user ID) of the terminal is non-plaintext identification information. The non-plaintext identification information specifically can be encrypted information (which is encrypted in the form of SUCI or encrypted by other secret keys such as a first secret key and/or is under integrity protection of a second secret key) or identifier information that is in direct association with

the terminal policy and that does not contain the user ID (e.g. SUPI). The terminal policy is inquired by the communication unit 803 based on the second information.

[00260] It can be seen that in this example the terminal firstly receives the second information from the network device, and secondly inquires the terminal policy based on the second information. Since the second information is content that is not in the form of plaintext, the second information can be prevented from being illegally stolen and directly utilized during transmission of the second information between the first network element and the terminal, which is beneficial to improving the safety of the interaction of information between the network side and the terminal in the inquiring of the terminal policy.

[00261] In a possible example, the second information includes a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID.

[00262] In a possible example, the second information includes a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

[00263] In a possible example, PSI parameter(s) in the PSI list is(are) globally unique; or PSI parameter(s) in the PSI list is(are) unique within a PLMN.

[00264] In a possible example, the user ID or the PSI parameters include any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element. The serial number and/or the character string is in one-to-one correspondence to the user ID or contents of the PSI parameters.

[00265] In a possible example, when the user ID is not a SUPI, the processing unit 802 is further configured to inquire, by the communication unit 803, a SUPI value corresponding to the user ID from a second network element.

[00266] In a possible example, the second network element has an identifier de-concealing function.

[00267] In a possible example, when the terminal policy is inquired based on the second information, the processing unit 802 is specifically configured to inquire the terminal policy by the communication unit 803 from a third network element using the SUPI and/or

the unique ID.

[00268] In a possible example, when the terminal policy is inquired based on the second information, the processing unit 802 is specifically configured to directly inquire, by the communication unit 803, the terminal policy from the third network element using the PSI parameters in the second information issued by the first network element.

[00269] In a possible example, the third network element is a core network data storage network element.

[00270] In a possible example, the second information is data transmitted to the terminal by the first network element, and a part or all of the data is encrypted by a first secret key and/or is under integrity protection using the second secret key.

[00271] In a possible example, the processing unit 802 is further configured to decrypt and/or check integrity based on the second information to obtain second content.

[00272] In a possible example, the processing unit 802 is further configured to inquire the terminal policy based on the second content.

[00273] In a possible example, the first secret key or the second secret key is generated by a third secret key via a preset algorithm.

[00274] In a possible example, the third secret key is sent to the terminal by a fourth network element.

[00275] In a possible example, the fourth network element is an authentication server function (AUSF) network element on the network side.

[00276] In a possible example, the first secret key is pre-configured at the first network element and the terminal.

[00277] In a possible example, the first network element is a policy control function (PCF) network element.

[00278] When the processing unit 802 is a processor, the communication unit 803 is a communication interface, and the storage unit 801 is a memory, the terminal in the embodiments of the present disclosure may be the terminal shown in Fig. 6.

[00279] An embodiment of the present disclosure further provides a computer readable storage medium storing computer programs for electronic data exchange, which cause a computer to perform all or part of the steps described from the perspective of the terminal in

the above method embodiments.

[00280] An embodiment of the present disclosure further provides a computer readable storage medium storing computer programs for electronic data exchange, which cause a computer to perform all or part of the steps described from the perspective of the network device in the above method embodiments.

[00281] An embodiment of the present disclosure further provides a computer program product which includes a non-transitory computer readable storage medium storing computer programs which are operable to cause a computer to perform all or part of the steps described from the perspective of the terminal in the above method embodiments. The computer program product can be a software installation package.

[00282] An embodiment of the present disclosure further provides a computer program product which includes a non-transitory computer readable storage medium storing computer programs which are operable to cause a computer to perform all or part of the steps described from the perspective of the network device in the above method embodiments. The computer program product can be a software installation package.

[00283] The steps of the methods or algorithms described in the embodiments of the present disclosure are implemented in the form of hardware, or in the form of software instructions executed by a processor. The software instructions may be composed of corresponding software modules. The software modules may be stored in a Random Access Memory (RAM), a flash memory, a Read Only Memory (ROM), an Erasable Programmable ROM (EPROM), an Electrically EPROM (EEPROM), a register, a hard disk, a mobile hard disk, a compact disk read-only memory (CD-ROM) or any other types of storage mediums well-known in the art. An exemplary storage medium is coupled to the processor, and thus the processor is able to read information from the medium and and write information into the medium. Of course, the storage medium can also be a part of the processor. The processor and the storage medium are located in an ASIC. Furthermore, the ASIC is located in an access network device, a target network device, or a core network device. Of course, the processor and the storage medium may be provided as separate components in the access network device, the target network device, or the core network device.

[00284] Those skilled in the art should appreciate that the functions described in the

embodiments of the present disclosure may be implemented in whole or in part by software, hardware, firmware or any combination thereof in one or more of the above examples. When implemented in software, the functions may be implemented in whole or in part in the form of a computer program product which includes one or more computer instructions. When the computer program instructions are loaded and executed on a computer, the procedures or functions described in accordance with the embodiments of the present disclosure are generated in whole or in part. The computer is a general-purpose computer, a special-purpose computer, a computer network or other programmable devices. The computer instructions are stored in a computer readable storage medium, or transmitted from one computer readable storage medium to another. For example, the computer instructions are transmitted from one website, computer, server or data center to another website, computer, server or data center wiredly (e.g. a coaxial cable, a optical fiber, a Digital Subscriber Line (DSL)) or wirelessly (e.g. infrared, Wi-Fi, microwave etc.). The computer readable storage medium is any medium to which a computer can access or a data storage device such as a server that includes one or more media, a data center. The media is a magnetic medium (e.g. a floppy disk, a hard disk, a magnetic tape), an optical medium (e.g. a Digital Video Disc (DVD)), or a semiconductor medium (e.g. a Solid State Disk (SSD)).

[00285] The objectives, the technical solutions and advantageous effects of the embodiments of the present disclosure are described in detail in the above-mentioned specific embodiments. It should be understood that the foregoing descriptions are only exemplary embodiments of the present disclosure and are not intended to limit the scope of the embodiments of the present disclosure. Any changes, equivalent substitutions and modifications made based on the technical solutions of the embodiments of the present disclosure should fall within the scope of the embodiments of the present disclosure.

WHAT IS CLAIMED IS:

1. A method for transmitting terminal information, wherein the method is applied in a network device which comprises a first network element, and the method comprises:

receiving, by the first network element, first information from a terminal.

2. The method of claim 1, wherein the first information is used to indicate a terminal policy stored in the terminal; after the first network element receives the first information from the terminal, the method further comprises:

inquiring, by the first network element, the terminal policy based on the first information.

3. The method of claim 2, wherein the first information comprises a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID.

4. The method of claim 2, wherein the first information comprises a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

5. The method of claim 2, wherein the first information comprises one or more sets of public land mobile network (PLMN) IDs and corresponding PSI lists.

6. The method of claim 5, wherein each PSI parameter in the PSI lists is represented by a unique ID.

7. The method of claim 2, wherein the first information comprises a PSI list, and each PSI parameter in the PSI list comprises a PLMN ID.

8. The method of claim 7, wherein each PSI parameter further comprises a unique ID.

9. The method of any one of claims 3-8, wherein a PSI parameter in the PSI list is globally unique; or a PSI parameter in the PSI list is unique within a PLMN.

10. The method of any one of claims 3-9, wherein the user ID or the PSI parameter comprise any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network element, wherein the serial number and/or the character string is in one-to-one correspondence to the user ID or content of the PSI parameter.

11. The method of any one of claims 3-10, wherein when the user ID is not a SUPI, the

method further comprises:

inquiring, by the first network element, a SUPI value corresponding to the user ID from a second network element.

12. The method of claim 11, wherein the second network element has an identifier de-concealing function.

13. The method of claim 11 or 12, wherein the inquiring, by the first network element, the terminal policy based on the first information comprises:

inquiring, by the first network element, the terminal policy from a third network element using the SUPI and/or the unique ID.

14. The method of any one of claims 3-10, wherein the inquiring, by the first network element, the terminal policy based on the first information comprises:

directly inquiring, by the first network element, the terminal policy from a third network element using the PSI parameter in the first information reported by the terminal.

15. The method of claim 14, wherein the third network element is a core network data storage network element.

16. The method of claim 1, wherein the first information is data transmitted to the first network element from the terminal, and a part or all of the data is encrypted by a first secret key and/or is under integrity protection using a second secret key.

17. The method of claim 16, wherein the method further comprises:

decrypting and/or checking integrity, by the first network element, based on the first information to obtain first content.

18. The method of claim 17, wherein the method further comprises:

Inquiring, by the first network element, the terminal policy based on the first content.

19. The method of any one of claims 16-18, wherein the first secret key or the second secret key is generated by a third secret key via a preset algorithm.

20. The method of claim 19, wherein the third secret key is sent to the terminal by a fourth network element.

21. The method of claim 20, wherein the fourth network element is an authentication server function (AUSF) network element on a network side.

22. The method of any one of claims 16-18, wherein the first secret key is

pre-configured at the first network element and the terminal.

23. The method of any one of claims 1-22, wherein the first network element is a policy control function (PCF) network element.

24. A method for transmitting terminal information, wherein the method is applied in a terminal, and comprises:

receiving, by the terminal, second information from a first network element.

25. The method of claim 24, wherein the second information is used to indicate and/or configure a terminal policy stored by the terminal; after the terminal receives the second information from the first network element, the method further comprises:

inquiring, by the terminal, the terminal policy based on the second information.

26. The method of claim 25, wherein the second information comprises a policy section identifier (PSI) list, and each PSI parameter in the PSI list is represented by a user identifier (ID) and a unique ID.

27. The method of claim 25, wherein the second information comprises one or more sets of PLMN IDs and a list of their corresponding PSIs.

28. The method of claim 27, wherein each PSI parameter in the PSI lists is represented by a unique ID.

29. The method of claim 28, wherein the terminal stores the terminal policy according to correspondences between the PLMN IDs and the PSIs.

30. The method of claim 25, wherein the second information comprises a PSI list, and each PSI parameter in the PSI list comprise a PLMN ID.

31. The method of claim 25, wherein each PSI parameter further comprises a unique ID.

32. The method of claim 25, wherein the second information comprises a user ID and a PSI list, and each PSI parameter in the PSI list is represented by a unique ID.

33. The method of any of claims 26-32, wherein a PSI parameter in the PSI list is globally unique; or the PSI parameter in the PSI list is unique within a PLMN.

34. The method of any one of claims 26-33, wherein the user ID or the PSI parameter comprises any one of a Subscriber Permanent Identifier (SUPI), a Subscriber Concealed Identifier (SUCI), a Mobile Subscriber International ISDN/PSTN number (MSISDN), a Domain Name, and a serial number and/or a character string generated by the first network

element, wherein the serial number and/or the character string is in one-to-one correspondence to the user ID or content of the PSI parameter.

35. The method of any one of claims 26-34, wherein when the user ID is not a SUPI, the method further comprises:

inquiring, by the terminal, a SUPI value corresponding to the user ID from a second network element.

36. The method of claim 35, wherein the second network element has an identifier de-concealing function.

37. The method of claim 35 or 36, wherein the inquiring, by the terminal, the terminal policy based on the second information comprises:

inquiring, by the terminal, the terminal policy from a third network element using the SUPI and/or the unique ID.

38. The method of any one of claims 27-34, wherein the inquiring, by the terminal, the terminal policy based on the second information comprises:

directly inquiring, by the terminal, the terminal policy from the third network element using the PSI parameter in the second information issued by the first network element.

39. The method of claim 38, wherein the third network element is a core network data storage network element.

40. The method of claim 25, wherein the second information is data transmitted to the terminal from the first network element, and a part or all of the data is encrypted by a first secret key and/or is under integrity protection using a second secret key.

41. The method of claim 40, wherein the method further comprises:

decrypting and/or checking integrity, by the terminal, based on the second information to obtain second content.

42. The method of claim 41, wherein the method further comprises:

inquiring, by the terminal, the terminal policy based on the second content.

43. The method of any one of claims 39-42, wherein the first secret key or the second secret key is generated by a third secret key via a preset algorithm.

44. The method of claim 43, wherein the third secret key is sent to the terminal by a fourth network element.

45. The method of claim 43, wherein the fourth network element is an authentication server function (AUSF) network element on a network side.

46. The method of any one of claims 40-42, wherein the first secret key is pre-configured at the first network element and the terminal.

47. The method of any one of claims 25-46, wherein the first network element is a policy control function (PCF) network element.

48. The method of any one of claims 25-47, wherein the receiving, by the terminal, second information from a first network element comprises:

receiving, by the terminal, the second information sent by the first network element according to mapping relationship information, wherein the mapping relationship information comprises correspondences between user identifiers and PSI parameters.

49. The method of claim 48, wherein each of the user identifiers corresponds to at least one of the PSI parameters in the mapping relationship information.

50. The method of claim 49, wherein one of the PSI parameters only corresponds to one of the user identifiers in the mapping relationship information.

51. The method of claim 49, wherein one of the PSI parameters at least corresponds to one of the user identifiers in the mapping relationship information.

52. A network device, comprising a processing unit and a communication unit, wherein the processing unit is configured to receive first information from a terminal via the communication unit.

53. A terminal, comprising a processing unit and a communication unit, wherein the processing unit is configured to receive second information from a first network element via the communication unit.

54. A network device, comprising a processor, a memory, a transceiver and one or more programs, wherein the one or more programs are stored in the memory and executed by the processor, the programs comprising instructions for performing steps in the method of any of claims 1 to 23.

55. A terminal, comprising a processor, a memory, a transceiver and one or more programs, wherein the one or more programs are stored in the memory and executed by the processor, the programs comprising instructions for performing steps in the method of any of

claims 24 to 51.

56. A computer readable storage medium storing computer programs for electronic data exchange, wherein the computer programs cause a computer to perform the method of any one of claims 1 to 51.