ACCESS CONTROL METHOD, ACCESS CONTROL APPARATUS, AND COMMUNICATIONS DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to Chinese Patent Application No. 202010762196.3, filed in China on July 31, 2020, and Chinese Patent Application No. 202110369540.7, filed in China on April 6, 2021, which are incorporated herein by reference in their entireties.

TECHNICAL FIELD

[0002] Embodiments of this application relate to the field of communications technologies, and in particular, to an access control method, an access control apparatus, and a communications device.

BACKGROUND

[0003] At present, in a process of accessing another network (such manner may be referred to as onboarding) to download a credential for accessing a standalone non-public network (Standalone Non-public Network, SNPN), a terminal needs to pass authentication of a default credential server. However, at that time, an authentication server function (Authentication Server Function, AUSF) of the another network may be neither related to the terminal nor related to a subscription permanent identifier of the terminal. In this case, how to select an authentication service network element is a problem to be urgently resolved.

SUMMARY

[0004] Embodiments of this application provide an access control method, an access control apparatus, and a communications device, so as to resolve a problem of how to select an authentication service network element.

[0005] In order to resolve the foregoing technical problem, this application is implemented as follows:

[0006] According to a first aspect, an embodiment of this application provides an access control method, applied to a first communications device and including:

obtaining first information and/or second information, where the first information includes at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier, and the second information includes at least one of the following: the first-type network identifier, the first-type routing indication, a first-type group identifier, and identification information of a terminal; and

performing a first operation based on the first information and/or the second information.

[0007] The first operation includes at least one of the following:

selecting a first authentication service network element;

determining the first-type group identifier, the first-type routing indication, information about a service provider, and/or the first-type network identifier; and

requesting, based on the first-type group identifier, the first-type routing indication, the first-type network identifier, the information about the service provider, and/or the indication information of the first access mode, to discover an authentication service network element.

[0008] The indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for

using only a restricted service, where the credential for accessing the first network by the terminal is a default credential.

[0009] The first network and the second network are a same network or different networks.

[0010] The first authentication service network element includes at least one of the following: an authentication service network element that provides an authentication service for a terminal being in the first access mode, and an authentication service network element that provides an authentication service for a terminal having a default credential.

[0011] The first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type network identifier includes: a network identifier used in the first access mode;

the first-type routing indication includes: a routing indication used in the first access mode;

the identification information of the terminal includes at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[0012] According to a second aspect, an embodiment of this application provides an access control method, applied to a second communications device and including:

sending first information; where

the first information includes at least one of the following: indication information of a first access mode, a first-type routing indication, a first-type network identifier, and identification information of a terminal;

the first-type routing indication includes: a routing indication used in the first access mode;

the first-type network identifier includes: a network identifier used in the first access mode;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the identification information of the terminal includes at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[0013] According to a third aspect, an embodiment of this application provides an access control method, applied to a third communications device and including:

obtaining third information and/or fourth information, where the third information includes at least one of the following: a first-type group identifier, information about an authentication provider, a first-type routing indication, a

first-type network identifier, and indication information of a first access mode; and the fourth information is used to indicate home information of an authentication service network element, and the fourth information includes at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; and

performing a third operation based on the third information and/or the fourth information.

[0014] The third operation includes at least one of the following:

discovering an authentication service network element matching the third information, where fourth information of the authentication service network element matches the third information; and

sending the discovered authentication service network element.

[0015] An authentication service type supported by the authentication service network element includes supporting provision of an authentication service to a terminal having a default credential;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type routing indication includes: a routing indication used in the first access mode; and

the first-type network identifier includes: a network identifier used in the first access mode.

[0016] According to a fourth aspect, an embodiment of this application provides an access control method, applied to a fourth communications device and including:

sending fourth information; where

the fourth information is used to indicate home information of an authentication service network element, and the fourth information includes at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; where

a routing indication supported by the authentication service network element is the first-type routing indication;

a network identifier of a network to which the authentication service network element belongs is the first-type network identifier;

an identifier of a group to which the authentication service network element belongs is the first-type group identifier;

an access mode supported by the authentication service network element includes the first access mode;

an authentication service type supported by the authentication service network element includes supporting provision of an authentication service to a terminal having a default credential;

the first access mode includes at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service;

the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode; and

the first-type network identifier includes: a network identifier used in the first access mode.

[0017] According to a fifth aspect, an embodiment of this application provides an access control apparatus, applied to a first communications device and including:

a first obtaining module, configured to obtain first information and/or second information, where the first information includes at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier, and the second information includes at least one of the following: the first-type network identifier, the first-type routing indication, a first-type group identifier, and identification information of a terminal; and

a first execution module, configured to perform a first operation based on the first information and/or the second information.

[0018] The first operation includes at least one of the following:

selecting a first authentication service network element;

determining the first-type group identifier, the first-type routing indication, information about a service provider, and/or the first-type network identifier; and

requesting, based on the first-type group identifier, the first-type routing indication, the first-type network identifier, the information about the service

provider, and/or the indication information of the first access mode, to discover an authentication service network element; where

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first authentication service network element includes at least one of the following: an authentication service network element that provides an authentication service for a terminal being in the first access mode, and an authentication service network element that provides an authentication service for a terminal having a default credential;

the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type network identifier includes: a network identifier used in the first access mode;

the first-type routing indication includes: a routing indication used in the first access mode;

the identification information of the terminal includes at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[0019] According to a sixth aspect, an embodiment of this application provides an access control apparatus, applied to a second communications device and including:

a first sending module, configured to send first information; where

the first information includes at least one of the following: indication information of a first access mode, a first-type routing indication, a first-type network identifier, and identification information of a terminal;

the first-type routing indication includes: a routing indication used in the first access mode;

the first-type network identifier includes: a network identifier used in the first access mode;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the identification information of the terminal includes at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[0020] According to a seventh aspect, an embodiment of this application provides an access control apparatus, applied to a third communications device and including:

a second obtaining module, configured to obtain third information and/or fourth information, where the third information includes at least one of the following: a first-type group identifier, a first-type routing indication, a first-type network identifier, information about an authentication provider, and indication information of a first access mode; and the fourth information is used to indicate home information of an authentication service network element, and the fourth information includes at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; and

a second execution module, configured to perform a third operation based on the third information and/or the fourth information.

[0021] The third operation includes at least one of the following:

discovering an authentication service network element matching the third information, where fourth information of the authentication service network element matches the third information; and

sending the discovered authentication service network element; where

an authentication service type supported by the authentication service network element includes supporting provision of an authentication service to a terminal having a default credential;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type routing indication includes: a routing indication used in the first access mode; and

the first-type network identifier includes: a network identifier used in the first access mode.

[0022] According to an eighth aspect, an embodiment of this application provides an access control apparatus, applied to a fourth communications device and including:

a second sending module, configured to send fourth information; where

the fourth information is used to indicate home information of an authentication service network element, and the fourth information includes at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication

provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; where

a routing indication supported by the authentication service network element is the first-type routing indication;

a network identifier of a network to which the authentication service network element belongs is the first-type network identifier;

an identifier of a group to which the authentication service network element belongs is the first-type group identifier;

an access mode supported by the authentication service network element includes the first access mode;

an authentication service type supported by the authentication service network element includes supporting provision of an authentication service to a terminal having a default credential;

the first access mode includes at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service;

the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode; and

the first-type network identifier includes: a network identifier used in the first access mode.

[0023] According to a ninth aspect, an embodiment of this application provides an access control method, applied to a fifth communications device and including:

performing a fifth operation in a case that a fifth condition is satisfied.

[0024] The fifth operation includes at least one of the following:

skipping using fifth information to select a network element for a terminal; where

the fifth condition includes at least one of the following: the terminal is in the first access mode; and

the fifth information includes at least one of the following: a user identifier of the terminal, an MNC in the user identifier of the terminal, an MCC in the user identifier of the terminal, information in realm in the user identifier of the terminal, a first network identifier NID in the user identifier of the terminal, and a network identifier in the user identifier of the terminal.

[0025] According to a tenth aspect, an embodiment of this application provides an access control apparatus, applied to a second communications device and including:

a third execution module, configured to perform a fifth operation in a case that a fifth condition is satisfied.

[0026] The fifth operation includes at least one of the following:

skipping using fifth information to select a network element for a terminal; where

the fifth condition includes at least one of the following: the terminal is in the first access mode; and

the fifth information includes at least one of the following: a user identifier of the terminal, network identification information in the user identifier of the terminal, and information in realm in the user identifier of the terminal.

[0027] According to an eleventh aspect, an embodiment of this application provides a communications device, including a processor, a memory, and a computer program stored on the memory and capable of running on the processor. When the computer program is executed by the processor, the steps of the access control method according to the first aspect are implemented, or the steps of the access control method according to the second aspect are implemented, or the steps of the access control method according to the third aspect are implemented, or the steps of the access control method according to the fourth aspect are implemented, or the steps of the access control method according to the ninth aspect are implemented.

[0028] According to a twelfth aspect, an embodiment of this application provides a readable storage medium, where the readable storage medium stores a program or an instruction, and when the program or the instruction is executed by a processor, the steps of the access control method according to the first aspect are implemented, the steps of the access control method according to the second aspect are implemented, or the steps of the access control method according to the third aspect are implemented, or the steps of the access control method according to the fourth aspect are implemented, or the steps of the access control method according to the ninth aspect are implemented.

[0029] It is easy to understand that with the embodiments, selection of the authentication service network element can be supported in the foregoing scenario in which the terminal accesses the first network in the first access mode.

BRIEF DESCRIPTION OF DRAWINGS

[0030] Other advantages and benefits will become apparent to those of ordinary skill in the art by reading detailed description of the exemplary embodiments below. The accompanying drawings are merely intended to illustrate the purposes of the preferred implementations, and should not be construed as a limitation on this application. Throughout the accompanying drawings, the same reference numerals represent the same components. In the accompanying drawings:

[0031] FIG. 1A is a schematic architectural diagram of a wireless communications system according to an embodiment of this application;

[0032] FIG. 1B is a schematic diagram of a relationship between network elements in a first access mode in this application;

[0033] FIG. 2 is a schematic flowchart of an access control method according to an embodiment of this application;

[0034] FIG. 3 is a schematic flowchart of an access control method according to another embodiment of this application;

[0035] FIG. 4 is a schematic flowchart of an access control method according to still another embodiment of this application;

[0036] FIG. 5 is a schematic flowchart of an access control method according to yet another embodiment of this application;

[0037] FIG. 6 is a flowchart of a service authentication indication process in an application scenario 1 according to an embodiment of this application;

[0038] FIG. 7 is a flowchart of a service selection process in an application scenario 2 according to an embodiment of this application;

[0039] FIG. 8 is a flowchart of a service selection process in an application scenario 3 according to an embodiment of this application;

[0040] FIG. 9 is a structural diagram of an access control apparatus according to an embodiment of this application;

[0041] FIG. 10 is a structural diagram of another access control apparatus according to an embodiment of this application;

[0042] FIG. 11 is a structural diagram of another access control apparatus according to an embodiment of this application;

[0043] FIG. 12 is a structural diagram of another access control apparatus according to an embodiment of this application; and

[0044] FIG. 13 is a structural diagram of a communications device according to an embodiment of this application.

DETAILED DESCRIPTION OF EMBODIMENTS

[0045] The following clearly and completely describes the technical solutions in the embodiments of this application with reference to the accompanying drawings in the embodiments of this application. Apparently, the described embodiments are only some rather than all of the embodiments of this application. All other embodiments obtained by a person of ordinary skill in the art based on the embodiments of this application without creative efforts shall fall within the protection scope of this application.

[0046] In the specification and claims of this application, the terms such as "first", "second", and the like are intended to distinguish between similar objects but do not necessarily indicate a specific order or sequence. It should be understood that the numbers used in this way are interchangeable in appropriate circumstances so that the embodiments of this application can be implemented in other orders than the order illustrated or described herein, and "first" and "second" are usually for distinguishing same-type objects but not limiting the number of objects, for example, a first object may be one or multiple. In addition, "and/or" in this specification and claims indicates at least one of connected objects, and the symbol "/" generally indicates that the associated objects are in an "or" relationship.

[0047] FIG. 1A is a block diagram of a wireless communications system to which the embodiments of this application are applicable. The wireless communications system includes a terminal 11 and a network-side device 12. The terminal 11 may include a relay supporting a terminal function and/or a terminal supporting a relay function. The terminal 11 may also be referred to as a terminal device or user equipment (User Equipment, UE), and the terminal 11 may be a terminal-side device, such as a mobile phone, a tablet computer (Tablet Personal Computer), a laptop computer (Laptop Computer) or a notebook computer, a personal digital assistant (Personal Digital Assistant, PDA), a palmtop computer, a netbook, an ultra-mobile personal computer (ultra-mobile personal computer, UMPC), a mobile Internet device (Mobile Internet Device, MID), a wearable device (Wearable Device) or vehicle user equipment (Vehicle User Equipment, VUE), or pedestrian user equipment (Pedestrian User Equipment, PUE). The wearable device includes: a wrist band, earphones, glasses, or the like. It should be noted that a specific type of the terminal 11 is not limited in the embodiments of this application. The network-side device 12 may be a base station or a core network. The base station may be referred to as an access point, a base transceiver station (Base Transceiver Station, BTS), a radio base station, a radio transceiver, a basic service set (Basic Service Set, BSS), an extended service set (Extended Service Set, ESS), a NodeB, an evolved NodeB (eNB), a home NodeB, a home evolved NodeB, a WLAN

access point, a Wi-Fi node, a transmission and reception Point (Transmitting Receiving Point, TRP), or another appropriate term in the art. Provided that a same technical effect is achieved, the base station is not limited to a specific technical term. It should be noted that in the embodiments of this application, the base station in an NR system is merely used as an example, and a specific type of the base station is not limited.

[0048] In some communication scenarios, there are scenarios in which a communications device having no credential of a network still needs to access the network. For example, when a standalone non-public network (Standalone Non-public Network, SNPN) is being deployed, the UE may still have no credential for accessing the SNPN or UE identifier, for example, an SNPN deployed in the factory and a terminal just purchased in the market, or an SNPN deployed at a concert site and terminals of the audience.

[0049] If such type of UE needs to obtain a credential for accessing an SNPN and a UE identifier, the UE may access a specific network (hereinafter referred to as a first network) and download the credential for accessing the SNPN. For example, the UE accesses the first network, establishes a data channel, connects to a configuration server through the data channel, and downloads an SNPN credential from the configuration server; or the UE accesses the first network, and a control network element of the first network downloads, for the UE, the SNPN credential from the configuration server.

[0050] A manner of accessing the first network to download a credential for accessing a second network may be referred to as onboarding. The first network and the second network may be a same network.

[0051] In a case that the UE does not have a credential of the first network, the first network needs to authenticate the UE before downloading the credential for the UE or establishing a data channel for downloading the credential. The UE may have a default credential; in this case, the first network may request a default credential server (DCS Default Credential Server) to authenticate the UE having the default

credential. The DCS may directly authenticate the UE or request another entity to authenticate the UE.

[0052] Such type of authentication is analogous to authentication for roaming to access other networks by UE, but is different from authentication for roaming of the UE.

[0053] In a case of roaming, an access and mobility management function (Access and Mobility Management Function, AMF) of a network accessed by the UE selects, for the UE, a home authentication server function (Home-Authentication Server Function, home AUSF) of the network to which the UE belongs to, and requests the home AUSF to authenticate the UE.

[0054] In an onboarding manner, as shown in FIG. 1B, an AMF of the first network may select, for the UE, an authentication proxy server (for example, an authentication server function (Authentication Server Function, AUSF) or an AAA (Authentication Authorization Accounting Server) serve proxy) of the first network accessed by the UE, and the authentication proxy server requests a default credential server (Default Credential Server, DCS) in another network to authenticate the UE. When the default credential that the UE has is a credential for a communications network (for example, a 3GPP network), the DCS may be a home AUSF of a home network of the UE. An NRF stores a relationship of network elements and may be called to query network elements.

[0055] UE having a public land mobile network (Public Land Mobile Network, PLMN) credential is able to: (1) roam to access other PLMN networks using the PLMN credential, (2) access an SNPN using the PLMN credential, and (3) onboard the first network for authentication on a default credential. In the manner (1), an AMF of a network accessed by the UE communicates with an AUSF of a home network of the UE. In the manner (3), the AMF of the network accessed by the UE communicates with an authentication proxy server (for example, an AUSF or an AAA server proxy) of the accessed network, and the authentication proxy server communicates with a home AUSF of the UE. In the manner (2), an authentication

structure in the manner (1) may be used or an authentication structure in the manner (3) may be used.

[0056] In order to support the authentication structure in the manner (3), the following problems still need to be resolved:

[0057] Problem 1: Currently during selection of an AUSF connected to the AMF, the AMF performs selection based on a home network identifier (Home Network Identifier) in a subscription permanent identifier (Subscription Permanent Identifier, SUPI) provided by the UE or an AUSF group identifier (Group ID) associated with the SUPI. However, in an onboarding architecture, the AMF in the first network needs to select, for the UE, the AUSF in the first network, and the AUSF then selects, for the UE, a home AUSF of the UE. The AUSF of the first network is neither related to the UE nor related to the SUPI of the UE. How to select different AUSFs for UEs of different access types becomes a problem that needs to be resolved.

[0058] In the embodiments of this application, optionally, obtaining may be understood as acquiring from configuration, receiving, obtaining through receiving upon a request, obtaining through self-learning, obtaining through deduction based on non-received information, or obtaining through processing received information, which may be determined according to actual needs. This is not limited in the embodiments of this application. For example, when specific capability indication information transmitted by a device is not received, it can be deduced that the device does not support the capability.

[0059] Optionally, transmitting may include broadcasting, broadcasting through a system message, or returning a response upon reception of a request.

[0060] In an embodiment of this application, a non-public network is an abbreviation of non public network. The non-public network may be referred to as one of the following: a non-public communications network. The non-public network may include at least one of the following deployment manners: a physical non-public network, a virtual non-public network, and a non-public network implemented on a public network. In an implementation, the non-public network is a

closed access group (Closed Access Group, CAG). A CAG may include a group of terminals.

[0061] In an embodiment of this application, a non-public network service is an abbreviation of non public network service. The non-public network service may also be referred to as one of the following: non-public-network network service, non-public communication service, non-public network communication service, non-public-network network service, or other names. It should be noted that the naming manner is not specifically limited in the embodiments of this application. In an implementation, the non-public network is a closed access group, and in this case, the non-public network service is a network service of the closed access group.

[0062] In an embodiment of this application, the non-public network may include or be referred to as a private network. The private network may be referred to as one of the following: a private communications network, a private network, a local area network (LAN), a private virtual network (Private Virtual Network, PVN), an isolated communications network, a dedicated communications network, or other names. It should be noted that the naming manner is not specifically limited in the embodiments of this application.

[0063] In an embodiment of this application, a public network is an abbreviation of public network. The public network may be referred to as one of the following: a public communications network or other names. It should be noted that the naming manner is not specifically limited in the embodiments of this application.

[0064] In an optional embodiment of this application, an authentication service includes initiating an authentication request for the terminal to an authentication server (such as a DCS or a home AUSF). An authentication service network element may be an authentication proxy that provides an authentication service for the terminal. Optionally, the authentication service network element may include but is not limited to one of the following: an AUSF and an AAA proxy.

[0065] In an optional embodiment of this application, indication information of a first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network,

an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential.

[0066] In an optional embodiment of this application, the credential for accessing the first network by the terminal being a default credential means that a credential corresponding to a terminal identifier and provided to the first network is a default credential when the terminal accesses the first network. In an implementation, the default credential is not a credential of the first network.

[0067] Optionally, the first network and the second network are a same network or different networks.

[0068] In an optional embodiment of this application, a network type of the first network may include but is not limited to one of the following: a public network (such as a PLMN), a standalone non-public network (such as an NPN), and a public network integrated non-public network (such as a PNI NPN).

[0069] In an optional embodiment of this application, having no credential for accessing the first network includes having no credential for accessing an unrestricted service of the first network.

[0070] (1) In an implementation, a terminal directly having a credential of a network B may be considered as the terminal having a credential for accessing the network B.

[0071] (2) In another implementation, an agreement (such as a roaming agreement) is present between a service provider A (including a network A) and the network B, and allows A's terminals to access the network B to use network services. In this case, it can be considered that A's terminals have a credential for accessing the network B, that is, a credential of A. Herein, accessing the network B by a terminal of the service provider A and a terminal in the network B may be considered to access an unrestricted service.

[0072] (3) In another implementation, in a manner in which a terminal of a service provider C (including a network C) accesses the network B to download a credential for accessing the network B, a credential of C that the terminal has can

help the network B to request an authentication server in C to authenticate the terminal. In this case, the credential of C that the terminal has is not a credential for accessing the network B, but a credential for authenticating the terminal by the network B, which is generally referred to as a default credential. Herein, accessing the network B by the terminal of the service provider C may be considered as accessing a restricted service.

[0073] In an optional embodiment of this application, an authentication provider is a provider that can authenticate a terminal having a default credential. In an implementation, the authentication provider does not include a home network of the terminal in a roaming scenario.

[0074] In an optional embodiment of this application, information about the authentication provider of the terminal includes at least one of the following: a network identifier of a network corresponding to the default credential of the terminal, a network identifier in a terminal identifier corresponding to the default credential of the terminal, a network identifier of a home network of the terminal, index information of an authentication provider of the default credential, and index information of a DCS. It is easy to understand that the credential of the terminal corresponds to the identifier of the terminal, and the information about the authentication provider of the terminal may be included in the identifier of the terminal.

[0075] In an optional embodiment of this application, a first identifier of the terminal includes one of the following: a terminal identifier corresponding to the default credential of the terminal, or a terminal identifier of the terminal in the DCS.

[0076] In an implementation, an identifier of the home network of the terminal is a network identifier in the terminal identifier corresponding to the default credential of the terminal. In another implementation, an identifier of the home network of the terminal is a network identifier of the authentication provider.

[0077] Optionally, the DCS is a device of the authentication provider of the terminal. When the DCS includes a home AUSF of the terminal, the first identifier of the terminal is a terminal identifier of the terminal in the home network. In this case,

the index information of the authentication provider of the default credential or the index information of the DCS is the identifier of the home network of the terminal.

[0078] In an optional embodiment of this application, the home network may be a network corresponding to the default credential of the terminal. In an implementation, the home AUSF is an AUSF in the home network. A home NRF is an NRF in the home network. Other home network elements are network elements in the home network.

[0079] In an optional embodiment of this application, a first-type network identifier includes a first-type home network identifier. The first-type home network identifier includes: a home network identifier used in the first access mode.

[0080] In another optional embodiment of this application, the first-type network identifier may be one of the following: a network identifier of the authentication provider, a network identifier corresponding to the default credential of the terminal, and a network identifier in the terminal identifier corresponding to the default credential of the terminal.

[0081] In an optional embodiment of this application, the communications device may include at least one of the following: a communications network element and a terminal.

[0082] In an embodiment of this application, the communications network element may include at least one of the following: a core-network network element and a radio-access-network network element.

[0083] In the embodiments of this application, a core-network network element (CN network element) may include but is not limited to at least one of the following: a core network device, a core network node, a core network function, a core-network network element, a mobility management entity (Mobility Management Entity, MME), an access mobility management function (Access Management Function, AMF), a network repository function (Network Repository Function, NRF), a session management function (Session Management Function, SMF), a user plane function (User Plane Function, UPF), a serving gateway (serving Gate Way, SGW), a PDN gateway (PDN Gate Way, PDN-GW), a policy control function (Policy Control

Function, PCF), a policy and charging rules function (Policy and Charging Rules Function, PCRF) unit, a GPRS serving support node (Serving GPRS Support Node, SGSN), a gateway GPRS support node (Gateway GPRS Support Node, GGSN), a unified data management (Unified Data Management, UDM), a unified data repository (Unified Data Repository, UDR), a home subscriber server (Home Subscriber Server, HSS), and an application function (Application Function, AF).

[0084] The following describes the access control method in the embodiments of this application.

[0085] Referring to FIG. 2, an embodiment of this application provides an access control method, applied to a first communications device. The first communications device includes an AMF. Optionally, the first communications device is a communications device in a first network. As shown in FIG. 2, the method includes the following steps.

[0086] Step 21: Obtain first information and/or second information.

[0087] The first information includes, but is not limited to, at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier. The second information includes, but is not limited to, at least one of the following: the first-type network identifier, the first-type routing indication, a first-type group identifier, and identification information of a terminal.

[0088] Optionally, the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode.

[0089] Optionally, the first-type network identifier includes: a network identifier used in the first access mode.

[0090] Optionally, the first-type routing indication includes: a routing indication used in the first access mode.

[0091] In an implementation, the first information may be received and obtained from the terminal. The first information may be included in an identifier (such as a SUCI or SUPI) of the terminal for transmission.

[0092] In another implementation, the second information may be obtained through local configuration on the first communications device.

[0093] The identification information of the terminal may include at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal.

[0094] (1) The first identifier of the terminal includes information about an authentication provider of the terminal. The authentication provider is a provider capable of authenticating a terminal having a default credential, or a provider capable of authenticating the terminal (for example, a home network of the terminal or a network corresponding to the default credential of the terminal). In an implementation, the authentication provider does not include a home network of the terminal in a roaming scenario.

[0095] The information about the authentication provider of the terminal includes at least one of the following: a network identifier of a network corresponding to the default credential of the terminal, a network identifier in a terminal identifier corresponding to the default credential of the terminal, a network identifier of a home network of the terminal, index information of an authentication provider of the default credential, and index information of a DCS. It is easy to understand that the credential of the terminal corresponds to the identifier of the terminal, and the information about the authentication provider of the terminal may be included in the identifier of the terminal.

[0096] The first identifier of the terminal includes one of the following: a terminal identifier corresponding to the default credential of the terminal, or a terminal identifier of the terminal in the DCS.

[0097] Optionally, the DCS is a device of the authentication provider of the terminal. When the DCS includes a home AUSF of the terminal, the first identifier of the terminal is a terminal identifier of the terminal in the home network. In this case, the index information of the authentication provider of the default credential or the index information of the DCS is an identifier of the home network of the terminal.

[0098] (2) The second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication.

[0099] (3) The third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[00100] It is easy to understand that the first-type network identifier and/or the first-type routing indication may be determined based on the second identifier of the terminal or the third identifier of the terminal.

[00101] (1) In an implementation, the first identifier of the terminal and the first-type network identifier may be sent.

[00102] (2) In another implementation, the first identifier of the terminal and the first-type routing indication may be sent.

[00103] (3) In another implementation, the first identifier of the terminal and the second identifier of the terminal may be sent.

[00104] (4) In another implementation, the third identifier of the terminal may be sent.

[00105] Step 22: Perform a first operation based on the first information and/or the second information.

[00106] The first operation may include at least one of the following:

selecting a first authentication service network element;

determining the first-type group identifier, the first-type routing indication, information about a service provider, and/or the first-type network identifier; and

requesting, based on the first-type group identifier, the first-type routing indication, the first-type network identifier, the information about the service provider, and/or the indication information of the first access mode, to discover an authentication service network element.

[00107] Optionally, the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing

the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential.

[00108] Optionally, the first network and the second network are a same network or different networks.

[00109] In an implementation, the indication information of the first access mode includes a first registration type. The first registration type may be used to indicate at least one of the following: a registration manner of performing registration to access the first network in order to download a credential for accessing the second network, and a registration manner of registering with the first network without a credential for accessing the first network.

[00110] Optionally, the credential for accessing the first network includes a credential for accessing an unrestricted service of the first network. Having no credential for accessing the first network includes having no credential for accessing an unrestricted service of the first network.

[00111] (1) In an implementation, a terminal directly having a credential of a network B may be considered as the terminal having a credential for accessing the network B.

[00112] (2) In another implementation, an agreement (such as a roaming agreement) is present between a service provider A (including a network A) and the network B, and allows A's terminals to access the network B to use network services. In this case, it can be considered that A's terminals have a credential for accessing the network B, that is, a credential of A. Herein, accessing the network B by a terminal of the service provider A and a terminal in the network B may be considered to access an unrestricted service.

[00113] (3) In another implementation, in a manner in which a terminal of a service provider C (including a network C) accesses the network B to download a credential for accessing the network B, a credential of C that the terminal has can help the network B to request an authentication server in C to authenticate the terminal. In this case, the credential of C that the terminal has is not a credential for

accessing the network B, but a credential for authenticating the terminal by the network B, which is generally referred to as a default credential. Herein, accessing the network B by the terminal of the service provider C may be considered as accessing a restricted service.

[00114] Optionally, the first authentication service network element includes at least one of the following: an authentication service network element that provides an authentication service for a terminal being in the first access mode, and an authentication service network element that provides an authentication service for a terminal having a default credential.

[00115] In an implementation, the authentication service includes initiating an authentication request for the terminal to an authentication server (such as a DCS or a home AUSF).

[00116] In this embodiment of this application, the requesting, based on the first-type group identifier, the first-type routing indication, the first-type network identifier, or the indication information of the first access mode, to discover an authentication service network element may include at least one of the following:

sending the first-type group identifier to a first target end, where the first-type group identifier is used by the first target end to discover an authentication service network element matching the first-type group identifier;

sending the indication information of the first access mode to the first target end, where the indication information of the first access mode is used by the first target end to discover an authentication service network element matching the indication information of the first access mode;

sending the first-type routing indication to the first target end, where the first-type routing indication is used by the first target end to discover an authentication service network element matching the first-type routing indication; and

sending the first-type network identifier to the first target end, where the first-type network identifier is used by the first target end to discover an authentication service network element matching the first-type network identifier.

[00117] Optionally, the first target end may include: a network element device responsible for querying a network element in the network, for example, a network repository function (Network Repository Function, NRF).

[00118] Optionally, the authentication service network element may include but is not limited to one of the following: an AUSF and an AAA proxy. In an implementation, the authentication service network element may be an authentication proxy that provides an authentication service for the terminal.

[00119] In an implementation, an AUSF group identifier specially used for the first access mode may be used to request the NRF to discover an AUSF.

[00120] Optionally, the obtaining first information includes: obtaining the first information from the terminal; and/or the obtaining second information includes: obtaining the second information according to a configuration on the first communications device.

[00121] Optionally, the obtaining first information and/or second information may include at least one of the following:

obtaining the indication information of the first access mode from the terminal; and

obtaining the first-type group identifier, the first-type routing indication, or the first-type network identifier according to a configuration on the first communications device.

[00122] Further, the performing a first operation based on the first information and/or the second information may include:

determining the first-type group identifier, the first-type routing indication, or the first-type network identifier based on the indication information of the first access mode; and

requesting, based on the first-type group identifier, the first-type routing indication, and/or the first-type network identifier, to discover the authentication service network element.

[00123] Optionally, the obtaining first information and/or second information may include at least one of the following:

obtaining the first-type network identifier and/or the first-type routing indication from the terminal; and

obtaining the first-type group identifier according to a configuration on the first communications device.

[00124] Further, the performing a first operation based on the first information and/or the second information may include:

determining the first-type group identifier based on the first-type network identifier and/or the first-type routing indication; and

requesting, based on the first-type group identifier, to discover the authentication service network element.

[00125] Optionally, the first operation further includes at least one of the following:

receiving an authentication service network element that is discovered as requested;

exporting the first-type network identifier and/or the first-type routing indication based on the second identifier of the terminal or the third identifier of the terminal;

skipping sending the second identifier of the terminal to the first authentication service network element or the discovered authentication service network element;

exporting the first identifier of the terminal based on the third identifier of the terminal; and

sending the first identifier of the terminal to the first authentication service network element or the discovered authentication service network element.

[00126] It is easy to understand that with the embodiments, selection of the authentication service network element can be supported in the foregoing scenario in which the terminal accesses the first network in the first access mode.

[00127] Referring to FIG. 3, an embodiment of this application provides an access control method, applied to a second communications device. The second

communications device includes UE. As shown in FIG. 3, the method includes the following step.

[00128] Step 31: Send first information.

[00129] The first information may include at least one of the following: indication information of a first access mode, a first-type routing indication, a first-type network identifier, and identification information of a terminal.

[00130] The first-type routing indication includes: a routing indication used in the first access mode.

[00131] The first-type network identifier includes: a network identifier used in the first access mode.

[00132] The indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential.

[00133] The first network and the second network are a same network or different networks.

[00134] Optionally, the first information is sent to the first network accessed by the terminal. A manner of accessing the first network by the terminal is the first access mode. The first information may be included in an identifier (such as a SUCI or SUPI) of the terminal for transmission.

[00135] Optionally, the sending first information may include: sending the first information in a case that a first condition is satisfied. The first condition includes at least one of the following:

a purpose of accessing the first network by the second communications device is to download a credential for accessing the second network;

the second communications device has no credential for accessing the first network; and

the second communications device accessing the first network is merely allowed to use a restricted service.

[00136] The first network and the second network are a same network or different networks.

[00137] In an implementation, the network identifier used in the first access mode is sent by using a subscription permanent identifier SUPI of the terminal.

[00138] It should be noted that the second communications device having no credential for accessing the first network includes: the second communications device having no credential of the first network, or the second communications device having no credential of a service provider for accessing the first network.

[00139] The credential for accessing the first network may include a credential for accessing an unrestricted service of the first network. Having no credential for accessing the first network includes having no credential for accessing an unrestricted service of the first network.

[00140] (1) In an implementation, a terminal directly having a credential of a network B may be considered as the terminal having a credential for accessing the network B.

[00141] (2) In another implementation, an agreement (such as a roaming agreement) is present between a service provider A (including a network A) and the network B, and allows A's terminals to access the network B to use network services. In this case, it can be considered that A's terminals have a credential for accessing the network B, that is, a credential of A. Herein, accessing the network B by a terminal of the service provider A and a terminal in the network B may be considered to access an unrestricted service.

[00142] (3) In another implementation, in a manner in which a terminal of a service provider C (including a network C) accesses the network B to download a credential for accessing the network B, a credential of C that the terminal has can help the network B to request an authentication server in C to authenticate the terminal. In this case, the credential of C that the terminal has is not a credential for accessing the network B, but a credential for authenticating the terminal by the

network B, which is generally referred to as a default credential. Herein, accessing the network B by the terminal of the service provider C may be considered as accessing a restricted service.

[00143] Optionally, the identification information of the terminal may include at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal.

[00144] (1) The first identifier of the terminal includes information about an authentication provider of the terminal. The authentication provider is a provider capable of authenticating a terminal having a default credential, or a provider (for example, a home network of the terminal) capable of authenticating the terminal.

[00145] The information about the authentication provider of the terminal includes at least one of the following: a network identifier of a network corresponding to the default credential of the terminal, a network identifier in a terminal identifier corresponding to the default credential of the terminal, a network identifier of a home network of the terminal, index information of an authentication provider of the default credential, and index information of a DCS. The information about the authentication provider of the terminal may be included in the identifier of the terminal.

[00146] It is easy to understand that the credential of the terminal corresponds to the identifier of the terminal, and the first identifier of the terminal includes one of the following: a terminal identifier corresponding to the default credential of the terminal, or a terminal identifier of the terminal in the DCS.

[00147] Optionally, the DCS is a device of the authentication provider of the terminal. When the DCS includes a home AUSF of the terminal, the first identifier of the terminal is a terminal identifier of the terminal in the home network. In this case, the index information of the authentication provider of the default credential or the index information of the DCS is an identifier of the home network of the terminal.

[00148] (2) The second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication.

[00149] (3) The third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[00150] It is easy to understand that the first-type network identifier and/or the first-type routing indication may be determined based on the second identifier of the terminal or the third identifier of the terminal.

[00151] (1) In an implementation, the first identifier of the terminal and the first-type network identifier may be sent.

[00152] (2) In another implementation, the first identifier of the terminal and the first-type routing indication may be sent.

[00153] (3) In another implementation, the first identifier of the terminal and the second identifier of the terminal may be sent.

[00154] (4) In another implementation, the third identifier of the terminal may be sent.

[00155] Optionally, before the step of sending first information, the method may further include at least one of the following:

generating the second identifier of the terminal, and setting a routing indication in an identifier of the terminal to the first-type routing indication and/or setting a home network identifier in the identifier of the terminal to the first-type network identifier; and

generating a third identifier of the terminal, and adding the first-type network identifier to the identifier of the terminal and/or adding the first-type routing indication to the identifier of the terminal.

[00156] In an implementation, the operation of generating the second identifier of the terminal and/or generating the third identifier of the terminal is performed in a case that the first condition is satisfied. The first condition is as described above, and details are not repeated herein.

[00157] It is easy to understand that with the embodiments, selection of the authentication service network element can be supported in the foregoing scenario in which the terminal accesses the first network in the first access mode.

[00158] Referring to FIG. 4, an embodiment of this application provides an access control method, applied to a third communications device. The third communications device includes an NRF. Optionally, the third communications device is a communications device in a first network. As shown in FIG. 4, the method includes the following steps.

[00159] Step 41: Obtain third information and/or fourth information.

[00160] Optionally, the third information may include at least one of the following: a first-type group identifier, a first-type routing indication, a first-type network identifier, information about an authentication provider, and indication information of a first access mode.

[00161] Optionally, the fourth information is used to indicate home information of an authentication service network element. The fourth information may include at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential.

[00162] Optionally, the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential.

[00163] Optionally, the first network and the second network are a same network or different networks.

[00164] Optionally, the first-type routing indication includes: a routing indication used in the first access mode.

[00165] In an implementation, the restricted service includes a service for downloading a certificate for accessing the network.

[00166] Optionally, the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode.

[00167] In an implementation, the third information may be obtained from an AMF.

[00168] In another implementation, the fourth information, that is, the home information of the authentication service network element, may be obtained from the authentication service network element (such as an AUSF or an AAA proxy).

[00169] Step 42: Perform a third operation based on the third information and/or the fourth information.

[00170] The third operation may include at least one of the following:

discovering an authentication service network element matching the third information, where fourth information of the authentication service network element matches the third information; and

sending the discovered authentication service network element.

[00171] An authentication service type supported by the authentication service network element includes supporting provision of an authentication service to a terminal having a default credential.

[00172] In an implementation, the discovered authentication service network element is sent to a second target end. The second target end includes an AMF. In an implementation, the third information is received from the second target end.

[00173] Optionally, the authentication service network element may include one of the following: an AUSF and an AAA proxy.

[00174] In an implementation, the authentication service network element matching the third information is a first authentication service network element. The first authentication service network element includes an authentication service network element for providing an authentication service to a terminal being in the first access mode.

[00175] In an implementation, the first-type group identifier includes one of the following: an AUSF group ID and an AAA proxy group ID.

[00176] In an implementation, the NRF may be requested to discover an AUSF.

[00177] Optionally, in the operation of discovering an authentication service network element matching the third information, in a case that the third information includes the indication information of the first access mode, an access mode supported by the discovered authentication service network element is the first access mode; or in a case that the third information includes the first-type routing indication, a routing indication supported by the discovered authentication service network element is the first-type routing indication; or in a case that the third information includes the first-type network identifier, a network identifier of a network to which the discovered authentication service network element belongs is the first-type network identifier; or in a case that the third information includes the first-type group identifier, an identifier of a group to which the discovered authentication service network element belongs is the first-type group identifier; or in a case that the third information includes the information about the authentication provider, information about an authentication provider supported by the discovered authentication service network element includes the information about the authentication provider in the third information.

[00178] Alternatively, the discovered authentication service network element satisfies at least one of the following:

a routing indication supported by the discovered authentication service network element is the first-type routing indication;

a network identifier of a network to which the discovered authentication service network element belongs is the first-type network identifier;

an identifier of a group to which the discovered authentication service network element belongs is the first-type group identifier;

an access mode supported by the discovered authentication service network element is the first access mode; and

an authentication service type supported by the discovered authentication service network element is supporting provision of an authentication service to a terminal having a default credential.

[00179] It is easy to understand that with the embodiments, selection of the authentication service network element can be supported in the foregoing scenario in which the terminal accesses the first network in the first access mode.

[00180] Referring to FIG. 5, an embodiment of this application provides an access control method, applied to a fourth communications device. The fourth communications device includes an AUSF. Optionally, the fourth communications device is a communications device in a first network. As shown in FIG. 5, the method includes the following step.

[00181] Step 51: Send fourth information.

[00182] The fourth information is used to indicate home information of an authentication service network element. The fourth information may include at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential.

[00183] A routing indication supported by the authentication service network element is the first-type routing indication.

[00184] A network identifier of a network to which the authentication service network element belongs is the first-type network identifier.

[00185] An identifier of a group to which the authentication service network element belongs is the first-type group identifier.

[00186] An access mode supported by the authentication service network element includes the first access mode.

[00187] An authentication service type supported by the authentication service network element includes supporting provision of an authentication service (for example, acting as an authentication proxy) to a terminal having a default credential.

[00188] The first access mode includes at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential.

[00189] The first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode.

[00190] The first-type routing indication includes: a routing indication used in the first access mode.

[00191] The first-type network identifier includes: a network identifier used in the first access mode.

[00192] Optionally, the sending fourth information includes: sending the fourth information in a case that a second condition is satisfied; where the second condition includes that the authentication service network element is an authentication service network element for providing an authentication service to a terminal being in the first access mode.

[00193] It is easy to understand that with this embodiment, selection of the authentication service network element can be supported in the foregoing scenario in which the terminal accesses the first network in the first access mode.

[00194] An embodiment of this application provides an access control method, applied to a fifth communications device. The fifth communications device includes an AMF, an AUSF, and a UDM. Optionally, the fifth communications device is a communications device in a first network. The method includes:

performing a fifth operation in a case that a fifth condition is satisfied.

[00195] The fifth operation includes at least one of the following:

skipping using fifth information to select a network element for a terminal; where

the fifth condition includes at least one of the following: the terminal is in the first access mode; and

the fifth information includes at least one of the following: a user identifier of the terminal, network identification information in the user identifier of the terminal, and information in realm in the user identifier of the terminal.

[00196] In an implementation, for a terminal that accesses the network in a non-first access mode, selecting a network device for the terminal based on the information in the user identifier of the terminal is a default operation. Therefore, an additional operation needs to be performed for the terminal that accesses the network in the non-first access mode.

[00197] The network identification information in the user identifier of the terminal includes at least one of the following: an MNC in the user identifier of the terminal, an MCC in the user identifier of the terminal, and a network identifier NID in the user identifier of the terminal.

[00198] Optionally, before the step of performing a fifth operation in a case that a fifth condition is satisfied, the method further includes: obtaining first information, where the first information includes at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier, and the second information includes at least one of the following: the first-type network identifier, the first-type routing indication, a first-type group identifier, and identification information of the terminal; where

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first-type group identifier includes: a group identifier of an authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type network identifier includes: a network identifier used in the first access mode;

the first-type routing indication includes: a routing indication used in the first access mode;

the identification information of the terminal includes at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[00199] Optionally, after the step of obtaining first information, it is determined based on the first information that the fifth condition is satisfied.

[00200] Optionally, the network element includes at least one of the following: a core-network network element, an authentication service function AUSF, a unified data management UDM, and a unified data repository UDR.

[00201] In an implementation, the network element may be a network device.

[00202] The following describes the methods provided in the embodiments of this application with reference to specific application scenarios.

[00203] Application scenario 1

[00204] In the application scenario 1, as shown in FIG. 6, an indication process of service authentication may include the following step.

[00205] Step 61: An authentication service network element for providing an authentication service to a terminal being in a first access mode (an AUSF is used as

an instance for description below) initiates, to an NRF, a registration request, for example, Nnrf_NF Management_NF Register.

[00206] Optionally, the registration request includes fourth information, where the fourth information is used to indicate home information of the authentication service network element, and the fourth information may include at least one of the following: a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the discovered authentication service network element belongs, and an access mode supported by the authentication service network element.

[00207] In an implementation, in a case that the network identifier of the network to which the authentication service network element belongs is a first-type home network identifier, it may indicate that the authentication service network element is used to provide an authentication service for the terminal being in the first access mode.

[00208] In another implementation, in a case that the identifier of the group to which the authentication service network element belongs is a first-type group identifier, it may indicate that the authentication service network element is used to provide an authentication service for the terminal being in the first access mode.

[00209] Application scenario 2

[00210] In the application scenario 2, UE registers with a first network, and a type of the registration is a first access mode. The first network needs to request a DCS to authenticate the UE. An AMF, an NRF, and an AUSF are communications devices in the first network, a home NRF and a home AUSF are devices in a home network of the UE, and the home AUSF is an embodiment of the DCS. As shown in FIG. 7, the process of selecting an AUSF may include the following steps.

[00211] Step 71: The UE initiates a registration request to the AMF, where a registration type of the registration request is indication information of the first access mode (for example, a first registration type).

[00212] Step 72: Based on the indication information of the first access mode (for example, the first registration type) provided by the UE, the AMF performs an AUSF selection operation, including at least one of the following.

[00213] (1) Select an AUSF locally configured for the first access mode.

[00214] (2) Select an AUSF group identifier (AUSF Group ID) locally configured for the first access mode, and request the NRF based on the AUSF group identifier to discover an AUSF.

[00215] (3) Send the indication information of the first access mode to the NRF by using a network function discovery request, for example, Nnrf_NF Discovery_Request, so as to request to discover an AUSF that supports the first access mode.

[00216] It is easy to understand that before this, during registration with the NRF, the AUSF needs to provide an access mode supported by the AUSF, for example, the first access mode.

[00217] (4) Send a first-type network identifier (Home Network ID) to the NRF by using a network function discovery request, for example, Nnrf_NF Discovery_Request.

[00218] It is easy to understand that before this, during registration with the NRF, the AUSF supporting the first access mode needs to provide a network identifier of a network to which the authentication service network element belongs, where the network identifier is a network identifier for the first access mode, for example, a network identifier specially used for the first access mode.

[00219] (5) Send a first-type group identifier to the NRF by using a network function discovery request, for example, Nnrf_NF Discovery_Request.

[00220] It is easy to understand that before this, during registration with the NRF, the AUSF supporting the first access mode needs to provide an identifier of a group to which the authentication service network element belongs, where the identifier is a group identifier for the first access mode, for example, a group identifier of the authentication service network element specially used for the first access mode.

[00221] Step 73: The NRF performs a third operation based on third information and/or fourth information that is obtained.

[00222] The third information may include at least one of the following: a first-type group identifier, a first-type network identifier, and indication information of the first access mode. The fourth information is used to indicate home information of an authentication service network element. The fourth information may include at least one of the following: a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, and an access mode supported by the authentication service network element.

[00223] The third operation includes at least one of the following:

discovering an authentication service network element matching the third information (using an AUSF as an example for description below); and

sending the discovered authentication service network element to the AMF.

[00224] Step 74: The AMF sends, to the AUSF, a UE authentication request, for example, Nausf_UEAuthentication_Authenticate Request, where the request may include a first identifier of the terminal (a real first SUCI or first SUPI of the UE).

[00225] Step 75 to step 78: The AUSF discovers a home AUSF by using the NRF and a home NRF based on the first identifier of the terminal, a home network identifier in a first UE identifier, or an AUSF group identifier corresponding to the first UE identifier.

[00226] Specifically, in step 75, the AUSF sends to the NRF a network function discovery request, for example, Nnrf_NF Discovery_Request. The discovery request may include one of the following: the first identifier of the terminal, a home network identifier Home Network ID of the terminal, an AUSF group identifier related to the first identifier of the terminal, and the like.

[00227] In step 76, the NRF sends to the home NRF a network function discovery request, for example, Nnrf_NF Discovery_Request. The discovery request may include the first identifier of the terminal, the home network identifier in the first UE

identifier, the AUSF group identifier corresponding to the first UE identifier, or the like.

[00228] In step 77, the home NRF sends to the NRF a network function discovery response, for example, Nnrf_NF Discovery_Response.

[00229] In step 78, the NRF returns to the AUSF a network function discovery response, for example, Nnrf_NF Discovery_Response.

[00230] Step 79: The AUSF initiates, to the home AUSF, a UE authentication request, for example, Nausf_UE Authentication_Authenticate Request. The request includes a second SUCI or first SUPI that is generated, an SN-name, the indication information of the first access mode, and the like.

[00231] Then, the home AUSF may initiate an authentication procedure to the UE.

[00232] Application scenario 3

[00233] In the application scenario 3, UE registers with a first network and provides identification information of the terminal. The first network needs to request a DCS to authenticate the UE. An AMF, an NRF, and an AUSF are communications devices in the first network, a home NRF and a home AUSF are devices in a home network of the UE, and the home AUSF is an embodiment of the DCS. As shown in FIG. 8, the process of selecting an AUSF may include the following steps.

[00234] Step 81: The UE initiates a registration request to the AMF. Optionally, the registration request includes first information, for example, the identification information of the terminal.

[00235] The identification information of the terminal may include at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal.

[00236] The first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes a first-type network identifier and/or a first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[00237] The AMF may perform: exporting the first-type network identifier and/or the first-type routing indication based on the second identifier of the terminal or the third identifier of the terminal.

[00238] The first-type network identifier includes: a specific value specially used for the first access mode, for example, 111.

[00239] The first-type routing indication includes: a specific value specially used for the first access mode.

[00240] (1) In an implementation, the registration request includes the first identifier of the terminal and the first-type network identifier.

[00241] (2) In another implementation, the registration request includes the first identifier of the terminal and the second identifier of the terminal.

[00242] (3) In another implementation, the registration request includes the third identifier of the terminal.

[00243] When the first identifier (SUPI or SUPI) of the terminal indicates subscription to a PLMN or an SNPN, index information of the DCS includes a real home network ID in the SUPI of the UE.

[00244] Step 82: The AMF sends to the NRF a network function discovery request, for example, Nnrf_NF Discovery_Request, that is, requests the NRF based on a home network identifier for the first access mode to query an AUSF, so as to obtain the AUSF.

[00245] Optionally, the request includes a home network ID and/or group ID of the AUSF.

[00246] Step 83: The NRF returns, to the AMF, a discovered authentication service network element, that is, the AUSF.

[00247] Step 84: The AMF sends, to the AUSF, a UE authentication request, for example, Nausf_UEAuthentication_Authenticate Request.

[00248] Optionally, the AMF may perform at least one of the following:

skipping sending the second identifier of the terminal to a first authentication service network element or the discovered authentication service network element;

exporting the first identifier of the terminal based on the third identifier of the terminal; and

sending the first identifier of the terminal to the first authentication service network element or the discovered authentication service network element.

[00249] Step 85 to step 89 are the same as steps 75 to 79 in the application scenario 2, which are not be repeated herein.

[00250] Referring to FIG. 9, an embodiment of this application provides an access control apparatus, applied to a first communications device. As shown in FIG. 9, the access control apparatus 90 includes:

a first obtaining module 91, configured to obtain first information and/or second information, where the first information includes at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier, and the second information includes at least one of the following: the first-type network identifier, the first-type routing indication, a first-type group identifier, and identification information of a terminal; and

a first execution module 92, configured to perform a first operation based on the first information and/or the second information.

[00251] The first operation includes at least one of the following:

selecting a first authentication service network element;

determining the first-type group identifier, the first-type routing indication, information about a service provider, and/or the first-type network identifier; and

requesting, based on the first-type group identifier, the first-type routing indication, the first-type network identifier, the information about the service provider, and/or the indication information of the first access mode, to discover an authentication service network element.

[00252] The indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first authentication service network element includes at least one of the following: an authentication service network element that provides an authentication service for a terminal being in the first access mode, and an authentication service network element that provides an authentication service for a terminal having a default credential;

the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type network identifier includes: a network identifier used in the first access mode;

the first-type routing indication includes: a routing indication used in the first access mode;

the identification information of the terminal includes at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[00253] Optionally, the first execution module 92 is further configured to perform at least one of the following:

sending the first-type group identifier to a first target end, where the first-type group identifier is used by the first target end to discover an authentication service network element matching the first-type group identifier;

sending the indication information of the first access mode to the first target end, where the indication information of the first access mode is used by the first target end to discover an authentication service network element matching the indication information of the first access mode;

sending the first-type routing indication to the first target end, where the first-type routing indication is used by the first target end to discover an authentication service network element matching the first-type routing indication; and

sending the first-type network identifier to the first target end, where the first-type network identifier is used by the first target end to discover an authentication service network element matching the first-type network identifier.

[00254] Optionally, the first obtaining module 91 is specifically configured to: obtain the first information from the terminal.

[00255] Optionally, the first obtaining module 91 is specifically configured to: obtain the second information according to a configuration on the first communications device.

[00256] Optionally, the first obtaining module 91 is specifically configured to perform at least one of the following:

obtaining the indication information of the first access mode from the terminal; and

obtaining the first-type group identifier, the first-type routing indication, or the first-type network identifier according to a configuration on the first communications device.

[00257] The performing a first operation based on the first information and/or the second information includes at least one of the following:

determining the first-type group identifier, the first-type routing indication, or the first-type network identifier based on the indication information of the first access mode; and

requesting, based on the first-type group identifier, the first-type routing indication, and/or the first-type network identifier, to discover the authentication service network element.

[00258] Optionally, the first obtaining module 91 is specifically configured to perform at least one of the following:

obtaining the first-type network identifier and/or the first-type routing indication from the terminal; and

obtaining the first-type group identifier according to a configuration on the first communications device.

[00259] The performing a first operation based on the first information and/or the second information includes at least one of the following:

determining the first-type group identifier based on the first-type network identifier and/or the first-type routing indication; and

requesting, based on the first-type group identifier, to discover the authentication service network element.

[00260] Optionally, the first operation further includes at least one of the following:

receiving an authentication service network element that is discovered as requested;

exporting the first-type network identifier and/or the first-type routing indication based on the second identifier of the terminal or the third identifier of the terminal;

skipping sending the second identifier of the terminal to the first authentication service network element or the discovered authentication service network element;

exporting the first identifier of the terminal based on the third identifier of the terminal; and

sending the first identifier of the terminal to the first authentication service network element or the discovered authentication service network element.

[00261] In this embodiment, the access control apparatus 90 is capable of implementing the processes implemented in the method embodiment shown in FIG. 2 of this application, with the same beneficial effects achieved. To avoid repetition, details are not described herein again.

[00262] Referring to FIG. 10, an embodiment of this application provides an access control apparatus, applied to a second communications device. As shown in FIG. 10, the access control apparatus 100 includes:

a first sending module 101, configured to send first information.

[00263] The first information includes at least one of the following: indication information of a first access mode, a first-type routing indication, a first-type network identifier, and identification information of a terminal;

the first-type routing indication includes: a routing indication used in the first access mode;

the first-type network identifier includes: a network identifier used in the first access mode;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the identification information of the terminal includes at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[00264] Optionally, the first sending module 101 is specifically configured to: send the first information in a case that a first condition is satisfied.

[00265] The first condition includes at least one of the following:

a purpose of accessing the first network by the second communications device is to download a credential for accessing the second network;

the second communications device has no credential for accessing the first network; and

the second communications device accessing the first network is merely allowed to use a restricted service.

[00266] Optionally, the access control apparatus 100 further includes:

a generating module, configured to generate the second identifier of the terminal, and set a routing indication in an identifier of the terminal to the first-type routing indication and/or set a home network identifier in the identifier of the terminal to the first-type network identifier; and/or

generate a third identifier of the terminal, and add the first-type network identifier to the identifier of the terminal and/or adding the first-type routing indication to the identifier of the terminal.

[00267] In this embodiment, the access control apparatus 100 is capable of implementing the processes implemented in the method embodiment shown in FIG. 3 of this application, with the same beneficial effects achieved. To avoid repetition, details are not described herein again.

[00268] Referring to FIG. 11, an embodiment of this application provides an access control apparatus, applied to a third communications device. As shown in FIG. 11, the access control apparatus 110 includes:

a second obtaining module 111, configured to obtain third information and/or fourth information, where the third information includes at least one of the following: a first-type group identifier, a first-type routing indication, a first-type network identifier, information about an authentication provider, and indication information of a first access mode; and the fourth information is used to indicate home information of an authentication service network element, and the fourth information includes at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; and

a second execution module 112, configured to perform a third operation based on the third information and/or the fourth information.

[00269] The third operation includes at least one of the following:

discovering an authentication service network element matching the third information, where fourth information of the authentication service network element matches the third information; and

sending the discovered authentication service network element.

[00270] An authentication service type supported by the authentication service network element includes supporting provision of an authentication service to a terminal having a default credential;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for

using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type routing indication includes: a routing indication used in the first access mode; and

the first-type network identifier includes: a network identifier used in the first access mode.

[00271] Optionally, in the operation of discovering an authentication service network element matching the third information,

in a case that the third information includes the indication information of the first access mode, an access mode supported by the discovered authentication service network element is the first access mode; or

in a case that the third information includes the first-type routing indication, a routing indication supported by the discovered authentication service network element is the first-type routing indication; or

in a case that the third information includes the first-type network identifier, a network identifier of a network to which the discovered authentication service network element belongs is the first-type network identifier; or

in a case that the third information includes the first-type group identifier, an identifier of a group to which the discovered authentication service network element belongs is the first-type group identifier; or

in a case that the third information includes the information about the authentication provider, information about an authentication provider supported by the discovered authentication service network element includes the information about the authentication provider in the third information; or

the discovered authentication service network element satisfies at least one of the following:

a routing indication supported by the discovered authentication service network element is the first-type routing indication;

a network identifier of a network to which the discovered authentication service network element belongs is the first-type network identifier;

an identifier of a group to which the discovered authentication service network element belongs is the first-type group identifier;

an access mode supported by the discovered authentication service network element is the first access mode; and

an authentication service type supported by the discovered authentication service network element is supporting provision of an authentication service to a terminal having a default credential.

[00272] In this embodiment, the access control apparatus 110 is capable of implementing the processes implemented in the method embodiment shown in FIG. 4 of this application, with the same beneficial effects achieved. To avoid repetition, details are not described herein again.

[00273] Referring to FIG. 12, an embodiment of this application provides an access control apparatus, applied to a fourth communications device. As shown in FIG. 12, the access control apparatus 120 includes:

a second sending module 121, configured to send fourth information.

[00274] The fourth information is used to indicate home information of an authentication service network element, and the fourth information includes at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication

provider being capable of authenticating a terminal having a default credential; where

a routing indication supported by the authentication service network element is the first-type routing indication;

a network identifier of a network to which the authentication service network element belongs is the first-type network identifier;

an identifier of a group to which the authentication service network element belongs is the first-type group identifier;

an access mode supported by the authentication service network element includes the first access mode;

an authentication service type supported by the authentication service network element includes supporting provision of an authentication service to a terminal having a default credential;

the first access mode includes at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first-type group identifier includes: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode; and

the first-type network identifier includes: a network identifier used in the first access mode.

[00275] Optionally, the second sending module 121 is further configured to: send the fourth information in a case that a second condition is satisfied.

[00276] The second condition includes that the authentication service network element is an authentication service network element for providing an authentication service to a terminal being in the first access mode.

[00277] In this embodiment, the access control apparatus 120 is capable of implementing the processes implemented in the method embodiment shown in FIG. 5 of this application, with the same beneficial effects achieved. To avoid repetition, details are not described herein again.

[00278] This application further provides an access control apparatus, applied to a fifth communications device and including:

a third execution module, configured to perform a fifth operation in a case that a fifth condition is satisfied.

[00279] The fifth operation includes at least one of the following:

skipping using fifth information to select a network element for a terminal; where

the fifth condition includes at least one of the following: the terminal is in the first access mode; and

the fifth information includes at least one of the following: a user identifier of the terminal, network identification information in the user identifier of the terminal, and information in realm in the user identifier of the terminal.

[00280] In an implementation, for a terminal that accesses the network in a non-first access mode, selecting a network device for the terminal based on the information in the user identifier of the terminal is a default operation. Therefore, an additional operation needs to be performed for the terminal that accesses the network in the non-first access mode.

[00281] The network identification information in the user identifier of the terminal includes at least one of the following: an MNC in the user identifier of the terminal, an MCC in the user identifier of the terminal, and a network identifier NID in the user identifier of the terminal.

[00282] Optionally, the apparatus further includes:

a third obtaining module, configured to obtain first information, where the first information includes at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier, and the second information includes at least one of the following: the first-type

network identifier, the first-type routing indication, a first-type group identifier, and identification information of the terminal.

[00283] The indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, where the credential for accessing the first network by the terminal is a default credential;

the first-type group identifier includes: a group identifier of an authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type network identifier includes: a network identifier used in the first access mode;

the first-type routing indication includes: a routing indication used in the first access mode;

the identification information of the terminal includes at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal includes information about an authentication provider of the terminal;

the second identifier of the terminal includes the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal includes the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

[00284] Optionally, the apparatus further includes:

a determining module, configured to determine based on the first information that the fifth condition is satisfied.

[00285] Optionally, the network element includes at least one of the following: a core-network network element, an AUSF, a UDM, and a UDR.

[00286] In an implementation, the network element may be a network device.

[00287] Referring to FIG. 13, FIG. 13 is a schematic structural diagram of another communications device according to an embodiment of this application. As shown in FIG. 13, the communications device 130 includes a processor 131, a memory 132, and a computer program stored on the memory 132 and capable of running on the processor. The components of the communications device 130 are coupled together by using the bus interface 133. When the computer program is executed by the processor 131, the processes implemented in the method embodiment shown in FIG. 2 can be implemented, the processes implemented in the method embodiment shown in FIG. 3 can be implemented, the processes implemented in the method embodiment shown in FIG. 4 can be implemented, or the processes implemented in the method embodiment shown in FIG. 5 can be implemented, with the same technical effects achieved. To avoid repetition, details are not described herein again.

[00288] An embodiment of this application further provides a computer-readable storage medium, where a computer program is stored in the computer-readable storage medium, and when the computer program is executed by a processor, the processes implemented in the method embodiment shown in FIG. 2 are implemented, or the processes implemented in the method embodiment shown in FIG. 3 are implemented, or the processes implemented in the method embodiment shown in FIG. 4 are implemented, or the processes implemented in the method embodiment shown in FIG. 5 are implemented, with the same technical effects achieved. To avoid repetition, details are not described herein again. The computer-readable storage medium is, for example, a read-only memory (Read-Only Memory, ROM), a random access memory (Random Access Memory, RAM), a magnetic disk, or an optical disc.

[00289] It should be noted that the terms "include", "comprise", or any of their variants are intended to cover a non-exclusive inclusion, such that a process, a method, an article, or an apparatus that includes a list of elements not only includes those elements but also includes other elements that are not expressly listed, or further includes elements inherent to such process, method, article, or apparatus. In

absence of more constraints, an element preceded by "includes a..." does not preclude the existence of other identical elements in the process, method, article, or apparatus that includes the element.

[00290] According to the foregoing description of the implementations, a person skilled in the art may clearly understand that the methods in the foregoing embodiments may be implemented by using software in combination with a necessary common hardware platform, and certainly may alternatively be implemented by using hardware. However, in most cases, the former is a preferred implementation. Based on such an understanding, the technical solutions of this application essentially or the part contributing to the prior art may be implemented in a form of a software product. The software product is stored in a storage medium (such as a ROM/RAM, a magnetic disk, or an optical disc), and includes several instructions for instructing a terminal (which may be a mobile phone, a computer, a server, an air conditioner, a network device, or the like) to perform the methods described in the embodiments of this application.

[00291] The foregoing describes the embodiments of this application with reference to the accompanying drawings. However, this application is not limited to the foregoing specific embodiments. The foregoing specific embodiments are merely illustrative rather than restrictive. As instructed by this application, persons of ordinary skill in the art may develop many other manners without departing from principles of this application and the protection scope of the claims, and all such manners fall within the protection scope of this application.

CLAIMS

What is claimed is:

1. An access control method, applied to a first communications device and comprising:

obtaining first information and/or second information, wherein the first information comprises at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier, and the second information comprises at least one of the following: the first-type network identifier, the first-type routing indication, a first-type group identifier, and identification information of a terminal; and

performing a first operation based on the first information and/or the second information; wherein

the first operation comprises at least one of the following:

selecting a first authentication service network element;

determining the first-type group identifier, the first-type routing indication, information about a service provider, and/or the first-type network identifier; and

requesting, based on the first-type group identifier, the first-type routing indication, the first-type network identifier, the information about the service provider, and/or the indication information of the first access mode, to discover an authentication service network element; wherein

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, wherein the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first authentication service network element comprises at least one of the following: an authentication service network element that provides an authentication service for a terminal being in the first access mode, and an authentication service network element that provides an authentication service for a terminal having a default credential;

the first-type group identifier comprises: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type network identifier comprises: a network identifier used in the first access mode;

the first-type routing indication comprises: a routing indication used in the first access mode;

the identification information of the terminal comprises at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal comprises information about an authentication provider of the terminal;

the second identifier of the terminal comprises the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal comprises the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

2. The method according to claim 1, wherein the requesting, based on the first-type group identifier, the first-type routing indication, the first-type network identifier, the information about the service provider, and/or the indication information of the first access mode, to discover an authentication service network element comprises at least one of the following:

sending the first-type group identifier to a first target end, wherein the first-type group identifier is used by the first target end to discover an authentication service network element matching the first-type group identifier;

sending the indication information of the first access mode to the first target end, wherein the indication information of the first access mode is used by the first target end to discover an authentication service network element matching the indication information of the first access mode;

sending the first-type routing indication to the first target end, wherein the first-type routing indication is used by the first target end to discover an authentication service network element matching the first-type routing indication; and

sending the first-type network identifier to the first target end, wherein the first-type network identifier is used by the first target end to discover an authentication service network element matching the first-type network identifier.

3. The method according to claim 1, wherein the information about the authentication provider of the terminal comprises at least one of the following: a network identifier of a network corresponding to the default credential of the terminal, a network identifier in a terminal identifier corresponding to the default credential of the terminal, a network identifier of a home network of the terminal, index information of an authentication provider of the default credential, and index information of a DCS.

4. The method according to claim 1, wherein

the obtaining first information comprises: obtaining the first information from the terminal;

and/or,

the obtaining second information comprises: obtaining the second information according to a configuration on the first communications device;

or,

the obtaining first information and/or second information comprises at least one of the following:

obtaining the indication information of the first access mode from the terminal; and

obtaining the first-type group identifier, the first-type routing indication, or the first-type network identifier according to a configuration on the first communications device; wherein

the performing a first operation based on the first information and/or the second information comprises at least one of the following:

determining the first-type group identifier, the first-type routing indication, or the first-type network identifier based on the indication information of the first access mode; and

requesting, based on the first-type group identifier, the first-type routing indication, and/or the first-type network identifier, to discover the authentication service network element;

or,

the obtaining first information and/or second information comprises at least one of the following:

obtaining the first-type network identifier and/or the first-type routing indication from the terminal; and

obtaining the first-type group identifier according to a configuration on the first communications device; wherein

the performing a first operation based on the first information and/or the second information comprises at least one of the following:

determining the first-type group identifier based on the first-type network identifier and/or the first-type routing indication; and

requesting, based on the first-type group identifier, to discover the authentication service network element.

5. The method according to claim 1, wherein the first operation further comprises at least one of the following:

receiving an authentication service network element that is discovered as requested;

exporting the first-type network identifier and/or the first-type routing indication based on the second identifier of the terminal or the third identifier of the terminal;

skipping sending the second identifier of the terminal to the first authentication service network element or the discovered authentication service network element;

exporting the first identifier of the terminal based on the third identifier of the terminal; and

sending the first identifier of the terminal to the first authentication service network element or the discovered authentication service network element.

6. An access control method, applied to a second communications device and comprising:

sending first information; wherein

the first information comprises at least one of the following: indication information of a first access mode, a first-type routing indication, a first-type network identifier, and identification information of a terminal;

the first-type routing indication comprises: a routing indication used in the first access mode;

the first-type network identifier comprises: a network identifier used in the first access mode;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, wherein the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the identification information of the terminal comprises at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal comprises information about an authentication provider of the terminal;

the second identifier of the terminal comprises the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal comprises the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

7. The method according to claim 6, wherein the sending first information comprises:

sending the first information in a case that a first condition is satisfied; wherein

the first condition comprises at least one of the following:

a purpose of accessing the first network by the second communications device is to download a credential for accessing the second network;

the second communications device has no credential for accessing the first network; and

the second communications device accessing the first network is merely allowed to use a restricted service.

8. The method according to claim 6, wherein before the step of sending first information, the method further comprises at least one of the following:

generating the second identifier of the terminal, and setting a routing indication in an identifier of the terminal to the first-type routing indication and/or setting a home network identifier in the identifier of the terminal to the first-type network identifier; and

generating a third identifier of the terminal, and adding the first-type network identifier to the identifier of the terminal and/or adding the first-type routing indication to the identifier of the terminal.

9. An access control method, applied to a third communications device and comprising:

obtaining third information and/or fourth information, wherein the third information comprises at least one of the following: a first-type group identifier, a

first-type routing indication, a first-type network identifier, information about an authentication provider, and indication information of a first access mode; and the fourth information is used to indicate home information of an authentication service network element, and the fourth information comprises at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; and

performing a third operation based on the third information and/or the fourth information; wherein

the third operation comprises at least one of the following:

discovering an authentication service network element matching the third information, wherein fourth information of the authentication service network element matches the third information; and

sending the discovered authentication service network element; wherein

an authentication service type supported by the authentication service network element comprises supporting provision of an authentication service to a terminal having a default credential;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, wherein the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first-type group identifier comprises: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type routing indication comprises: a routing indication used in the first access mode; and

the first-type network identifier comprises: a network identifier used in the first access mode.

10. The method according to claim 9, wherein in the operation of discovering an authentication service network element matching the third information,

in a case that the third information comprises the indication information of the first access mode, an access mode supported by the discovered authentication service network element is the first access mode; or

in a case that the third information comprises the first-type routing indication, a routing indication supported by the discovered authentication service network element is the first-type routing indication; or

in a case that the third information comprises the first-type network identifier, a network identifier of a network to which the discovered authentication service network element belongs is the first-type network identifier; or

in a case that the third information comprises the first-type group identifier, an identifier of a group to which the discovered authentication service network element belongs is the first-type group identifier; or

in a case that the third information comprises the information about the authentication provider, information about an authentication provider supported by the discovered authentication service network element comprises the information about the authentication provider in the third information; or

the discovered authentication service network element satisfies at least one of the following:

a routing indication supported by the discovered authentication service network element is the first-type routing indication;

a network identifier of a network to which the discovered authentication service network element belongs is the first-type network identifier;

an identifier of a group to which the discovered authentication service network element belongs is the first-type group identifier;

an access mode supported by the discovered authentication service network element is the first access mode; and

an authentication service type supported by the discovered authentication service network element is supporting provision of an authentication service to a terminal having a default credential.

11. An access control method, applied to a fourth communications device and comprising:

sending fourth information; wherein

the fourth information is used to indicate home information of an authentication service network element, and the fourth information comprises at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; wherein

a routing indication supported by the authentication service network element is the first-type routing indication;

a network identifier of a network to which the authentication service network element belongs is the first-type network identifier;

an identifier of a group to which the authentication service network element belongs is the first-type group identifier;

an access mode supported by the authentication service network element comprises the first access mode;

an authentication service type supported by the authentication service network element comprises supporting provision of an authentication service to a terminal having a default credential;

the first access mode comprises at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, wherein the credential for accessing the first network by the terminal is a default credential;

the first-type group identifier comprises: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode; and

the first-type network identifier comprises: a network identifier used in the first access mode.

12. The method according to claim 11, wherein the sending fourth information comprises:

sending the fourth information in a case that a second condition is satisfied; wherein

the second condition comprises that the authentication service network element is an authentication service network element for providing an authentication service to a terminal being in the first access mode.

13. An access control method, applied to a fifth communications device and comprising:

performing a fifth operation in a case that a fifth condition is satisfied; wherein

the fifth operation comprises at least one of the following:

skipping using fifth information to select a network element for a terminal;

wherein

the fifth condition comprises at least one of the following: the terminal is in the first access mode; and

the fifth information comprises at least one of the following: a user identifier of the terminal, network identification information in the user identifier of the terminal, and information in realm in the user identifier of the terminal.

14. The method according to claim 13, wherein before the step of performing a fifth operation in a case that a fifth condition is satisfied, the method further comprises: obtaining first information, wherein the first information comprises at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier, and second information comprises at least one of the following: the first-type network identifier, the first-type routing indication, a first-type group identifier, and identification information of the terminal; wherein

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, wherein the credential for accessing the first network by the terminal is a default credential;

the first-type group identifier comprises: a group identifier of an authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type network identifier comprises: a network identifier used in the first access mode;

the first-type routing indication comprises: a routing indication used in the first access mode;

the identification information of the terminal comprises at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal comprises information about an authentication provider of the terminal;

the second identifier of the terminal comprises the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal comprises the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication; after the step of obtaining first information,

it is determined based on the first information that the fifth condition is satisfied; the network element comprises at least one of the following: a core-network network element, an authentication service function AUSF, a unified data management UDM, and a unified data repository UDR.

15. An access control apparatus, applied to a first communications device and comprising:

a first obtaining module, configured to obtain first information and/or second information, wherein the first information comprises at least one of the following: indication information of a first access mode, a first-type routing indication, and a first-type network identifier, and the second information comprises at least one of the following: the first-type network identifier, the first-type routing indication, a first-type group identifier, and identification information of a terminal; and

a first execution module, configured to perform a first operation based on the first information and/or the second information; wherein

the first operation comprises at least one of the following:

selecting a first authentication service network element;

determining the first-type group identifier, the first-type routing indication, information about a service provider, and/or the first-type network identifier; and

requesting, based on the first-type group identifier, the first-type routing indication, the first-type network identifier, the information about the service provider, and/or the indication information of the first access mode, to discover an authentication service network element; wherein

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first

network without a credential for accessing the first network, and an access mode for using only a restricted service, wherein the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first authentication service network element comprises at least one of the following: an authentication service network element that provides an authentication service for a terminal being in the first access mode, and an authentication service network element that provides an authentication service for a terminal having a default credential;

the first-type group identifier comprises: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type network identifier comprises: a network identifier used in the first access mode;

the first-type routing indication comprises: a routing indication used in the first access mode;

the identification information of the terminal comprises at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal comprises information about an authentication provider of the terminal;

the second identifier of the terminal comprises the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal comprises the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

16. An access control apparatus, applied to a second communications device and comprising:

a first sending module, configured to send first information; wherein

the first information comprises at least one of the following: indication information of a first access mode, a first-type routing indication, a first-type network identifier, and identification information of a terminal;

the first-type routing indication comprises: a routing indication used in the first access mode;

the first-type network identifier comprises: a network identifier used in the first access mode;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, wherein the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the identification information of the terminal comprises at least one of the following: a first identifier of the terminal, a second identifier of the terminal, and a third identifier of the terminal;

the first identifier of the terminal comprises information about an authentication provider of the terminal;

the second identifier of the terminal comprises the first-type network identifier and/or the first-type routing indication; and

the third identifier of the terminal comprises the information about the authentication provider of the terminal, the first-type network identifier, and/or the first-type routing indication.

17. An access control apparatus, applied to a third communications device and comprising:

a second obtaining module, configured to obtain third information and/or fourth information, wherein the third information comprises at least one of the following: a first-type group identifier, a first-type routing indication, a first-type network

identifier, information about an authentication provider, and indication information of a first access mode; and the fourth information is used to indicate home information of an authentication service network element, and the fourth information comprises at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; and

a second execution module, configured to perform a third operation based on the third information and/or the fourth information; wherein

the third operation comprises at least one of the following:

discovering an authentication service network element matching the third information, wherein fourth information of the authentication service network element matches the third information; and

sending the discovered authentication service network element; wherein

an authentication service type supported by the authentication service network element comprises supporting provision of an authentication service to a terminal having a default credential;

the indication information of the first access mode is used to indicate at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service, wherein the credential for accessing the first network by the terminal is a default credential;

the first network and the second network are a same network or different networks;

the first-type group identifier comprises: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode;

the first-type routing indication comprises: a routing indication used in the first access mode; and

the first-type network identifier comprises: a network identifier used in the first access mode.

18. An access control apparatus, applied to a fourth communications device and comprising:

a second sending module, configured to send fourth information; wherein

the fourth information is used to indicate home information of an authentication service network element, and the fourth information comprises at least one of the following: a routing indication supported by the authentication service network element, a network identifier of a network to which the authentication service network element belongs, an identifier of a group to which the authentication service network element belongs, an access mode supported by the authentication service network element, an authentication service type supported by the authentication service network element, and information about an authentication provider supported by the authentication service network element, the authentication provider being capable of authenticating a terminal having a default credential; wherein

a routing indication supported by the authentication service network element is the first-type routing indication;

a network identifier of a network to which the authentication service network element belongs is the first-type network identifier;

an identifier of a group to which the authentication service network element belongs is the first-type group identifier;

an access mode supported by the authentication service network element comprises the first access mode;

an authentication service type supported by the authentication service network element comprises supporting provision of an authentication service to a terminal having a default credential;

the first access mode comprises at least one of the following: an access mode for accessing a first network to download a credential for accessing a second network, an access mode for accessing the first network without a credential for accessing the first network, and an access mode for using only a restricted service;

the first-type group identifier comprises: a group identifier of the authentication service network element that provides an authentication service for a terminal being in the first access mode; and

the first-type network identifier comprises: a network identifier used in the first access mode.

19. An access control apparatus, applied to a fifth communications device and comprising:

a third execution module, configured to perform a fifth operation in a case that a fifth condition is satisfied; wherein

the fifth operation comprises at least one of the following:

skipping using fifth information to select a network element for a terminal;

wherein

the fifth condition comprises at least one of the following: the terminal is in the first access mode; and

the fifth information comprises at least one of the following: a user identifier of the terminal, network identification information in the user identifier of the terminal, and information in realm in the user identifier of the terminal.

20. A readable storage medium, wherein the readable storage medium stores a program or an instruction, and when the program or the instruction is executed by a processor, the steps of the access control method according to any one of claims 1 to 5 are implemented, or the steps of the access control method according to any one of claims 6 to 8 are implemented, or the steps of the access control method according to claim 9 or 10 is implemented, or the steps of the access control method according to

claim 11 or 12 is implemented, or the steps of the access control method according to claim 13 or 14 is implemented.