CLAIMS

1. An access control method, applied to a first communications device, the first communications device comprises a terminal, wherein the access control method comprises:

sending first information and/or first indication information to a second communications device, wherein the first information comprises at least one of the following:

index information of a second authentication server;

vendor-related information of the first communications device; and

address-related information of the second authentication server; and

the first indication information is used for requesting to obtain a credential related to a first network, or used to indicate that an access type is a restricted service;

wherein the access control method further comprises:

obtaining second information from the second communications device, wherein the second information comprises:

address-related information of a first server; wherein

the first server is a server capable of configuring the credential related to the first network.

2. The method according to claim 1, wherein the sending first information comprises:

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

the first condition comprises at least one of the following:

the first communications device has a second credential;

the first communications device has no credential related to the first network;

the first communications device requests to access the first network;

the first communications device requests to access a restricted service of the first network;

the first communications device requests to obtain a credential related to the first network;

at least one piece of the first information has been obtained;

request information for the first information has been obtained;

information that the first network supports the restricted service has been obtained;

information that the first network supports and/or requests authentication for the restricted service has been obtained;

information that the first network supports and/or requests authentication on the first communications device has been obtained; and

information that the first network supports configuring, for the first communications device, the credential related to the first network has been obtained;

wherein the request information for the first information comprises at least one of the following:

first request information, wherein the first request information is used to request vendor information of the first communications device;

second request information, wherein the second request information is used to request index information of the second authentication server; and

third request information, wherein the third request information is used to request address-related information of the second authentication server.

3. The method according to claim 2, wherein the credential related to the first network comprises at least one of the following: a credential directly related to the first network, a credential for accessing a normal service of the first network, a credential that can be directly authenticated by an authentication server of the first network, and a credential for accessing an unrestricted service of the first network;

and/or,

the second credential comprises at least one of the following:

a credential for accessing the first network in a case that the terminal has no credential related to the first network,

a credential for accessing the first network in a case that the terminal requests for configuration of the credential related to the first network,

a credential for accessing a restricted service of the first network,

a credential configured for the first communications device by a vendor of the first communications device, and

a credential that can be authenticated by the second authentication server.

4. The method according to claim 1, wherein before the step of sending first information, the method further comprises:

sending an access request and/or sending the first indication information to the second communications device; wherein

the first indication information is used for requesting to obtain the credential related to the first network, or used to indicate that the access type is a restricted service;

or,

wherein before the step of sending first information, the method further comprises:

receiving at least one of the following information that is sent by the second communications device:

request information for the first information;

information that the first network supports the restricted service;

information that the first network supports and/or requests authentication for the restricted service;

information that the first network supports and/or requests authentication on the first communications device; and

information that the first network supports configuring, for the first communications device, the credential related to the first network.

5. The method according to claim 1, wherein the second communications device comprises a communications device in the first network, and the second authentication server comprises an authentication server outside the first network.

6. The method according to claim 1, wherein the second information further comprises at least one of the following:

a first terminal routing policy;

default DNN information being left blank;

default slice information being left blank;

related information for establishing a first data channel;

second indication information;

third indication information; and

address-related information of the second authentication server; wherein

the first terminal routing policy is used for accessing the first server or a credential download application;

the first data channel is a data channel in the first network;

the second indication information is used to indicate at least one of the following:

the first data channel is used for interaction between the first communications device and the first server,

the first data channel is used by the first communications device to request the credential related to the first network; and

the first data channel is used for configuring, for the first communications device, the credential related to the first network; and

the third indication information is used to indicate at least one of the following: only a restricted service being allowed, only control plane being allowed while user plane being prohibited, only access to the first server being allowed, and only a credential download application being allowed.

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

obtaining at least one of first information, first indication information, a legitimate device list, and third information; and

performing a first operation based on at least one of the first information, the first indication information, the legitimate device list, and the third information; wherein

the first information send by a first communications device comprises at least one of the following: index information of a second authentication server, vendor-related information of the first communications device, and address-related information of the second authentication server;

the first indication send by the first communications device information is used for requesting to obtain a credential related to a first network, or used to indicate that an access type is a restricted service; and

the third information send by a third communications device comprises at least one of the following:

mapping information between the index information of the second authentication server and the address-related information of the second authentication server; and

the address-related information of the second authentication server;

wherein the first communications device comprises a terminal;

wherein the access control method further comprises: in a case that the first communications device is determined to be a legitimate device in the first network, sending, by the second communications device, second information to the first communications device,

wherein the second information comprises address-related information of a first server,

wherein the first server is a server capable of configuring the credential related to the first network.

8. The method according to claim 7, wherein the first operation comprises at least one of the following:

determining the second authentication server;

determining to request the second authentication server to perform authentication on the first communications device;

requesting the second authentication server to perform authentication on the first communications device;

requesting a first server to perform authentication on the first communications device;

sending the first information to the first server;

determining whether the first communications device is a legitimate device in the first network;

determining whether configuring, for the first communications device, the credential related to the first network is allowed; and

determining whether accepting a registration request of the first communications device by the first network is allowed; wherein

the first server is a server capable of configuring, for the first communications device, the credential related to the first network.

9. The method according to claim 8, wherein the step of determining the second authentication server comprises at least one of the following:

determining the second authentication server based on the index information of the second authentication server in the first information and the mapping information between the index information of the second authentication server and the address-related information of the second authentication server in the third information;

determining the second authentication server based on the vendor-related information of the first communications device in the first information and the mapping information between the index information of the second authentication server and the address-related information of the second authentication server in the third information;

determining the second authentication server based on the address-related information of the second authentication server in the first information and/or the address-related information of the second authentication server in the third information; and

determining the second authentication server based on the first indication information and/or the address-related information of the second authentication server in the third information;

and/or,

the step of determining to request the second authentication server to perform authentication on the first communications device comprises but is not limited to at least one of the following:

determining, based on the first indication information and/or the first information, to request the second authentication server to perform authentication on the first communications device; and

determining, based on the first indication information and/or the address-related information of the second authentication server in the third information, to request the second authentication server to perform authentication on the first communications device.

10. The method according to claim 8, wherein in a case that the first communications device satisfies a second condition, the first communications device is determined to be a legitimate device in the first network; wherein

the second condition comprises at least one of the following:

the first communications device is authenticated successfully by the second authentication server; and

the first communications device is a communications device in the legitimate device list;

wherein the legitimate device list comprises at least one of the following:

a legitimate communications device, not yet configured with a credential related to the first network, in the first network; and

a communications device for which configuring a credential related to the first network is allowed.

11. The method according to claim 7, wherein the second communications device comprises a communications device in the first network, the third communications device comprises a communications device outside the first network, and the second authentication server comprises an authentication server outside the first network.

12. The method according to claim 7, wherein before the step of obtaining first information, the method further comprises:

receiving an access request and/or first indication information from the first communications device; wherein the first indication information is used for requesting to obtain the credential related to the first network, or used to indicate that the access type is a restricted service; and

sending request information for the first information based on the access request and/or the first indication information;

wherein the request information for the first information comprises at least one of the following:

first request information, wherein the first request information is used to request vendor information of the first communications device;

second request information, wherein the second request information is used to request index information of the second authentication server; and

third request information, wherein the third request information is used to request address-related information of the second authentication server.

13. The method according to claim 7, wherein the second information further comprises at least one of the following:

related information for establishing a first data channel; and

second indication information; wherein

the first data channel is a data channel in the first network; and

the second indication information is used to indicate at least one of the following:

the first data channel is used for interaction between the first communications device and the first server;

the first data channel is used by the first communications device to request the credential related to the first network; and

the first data channel is used for configuring, for the first communications device, the credential related to the first network.

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

determining third information; and

sending the third information to a second communications device; wherein

the third information comprises:

the address-related information of the second authentication server.

15. The method according to claim 14, wherein the second communications device comprises a communications device in the first network, the third communications device comprises a communications device outside the first network, and the second authentication server comprises an authentication server outside the first network.

16. The method according to claim 14, wherein the sending information related to the second authentication server comprises:

in a case that a third condition is satisfied, sending the information related to the second authentication server; wherein

the third condition comprises at least one of the following:

mutual authentication between the third communications device and the second authentication server is successful; and

mutual authentication between the third communications device and a first network is successful.

17. An access control method, applied to a fourth communications device, the fourth communications device comprises a terminal, wherein the access control method comprises:

obtaining second information from a fifth communications device; and

performing a second operation based on the second information; wherein

the second information comprises:

address-related information of a first server; wherein

the first server is a server capable of configuring a credential related to a first network.

18. The method according to claim 17, wherein the second operation comprises at least one of the following:

establishing a first data channel, wherein the first data channel satisfies at least one of the following: the first data channel is used for interaction between the first communications device and the first server; the first data channel is used by the first communications device to request a credential related to the first network; and the first data channel is used for configuring, for the first communications device, the credential related to the first network;

requesting the first server to configure the credential related to the first network;

requesting the second authentication server to configure the credential related to the first network;

declining an access request or a data sending request for a target not being the first server and/or a credential download application at an application layer; and

allowing an access request or a data sending request only for a target being the first server and/or the credential download application.

19. The method according to claim 17, wherein the fifth communications device comprises a communications device in a first network.

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

sending second information to a fourth communications device, wherein the fourth communications device comprises a terminal, wherein the second information comprises:

address-related information of a first server; wherein

the first server is a server capable of configuring a credential related to a first network.

21. The method according to claim 20, wherein in a case that a fourth condition is satisfied, an operation related to determining of the second information is performed and/or the second information is sent; wherein

the fourth condition comprises:

a terminal accesses a restricted service of the first network or receives first indication information sent by the terminal;

it is determined that the terminal has passed initial authentication, or it is determined that the terminal has been authenticated successfully by the second authentication server;

it is determined that the first communications device is a non-counterfeit device;

it is determined that the terminal is a legitimate device in the first network or that the terminal is a communications device in a legitimate device list; and

it is determined that configuring, for the terminal, a credential related to the first network is allowed.

22. The method according to claim 20, wherein the fifth communications device comprises a communications device in a first network.

23. A communications device, comprising a processor, a memory, and a computer program stored in the memory and capable of running on the processor, wherein when the computer program is executed by the processor, the steps of the access control method according to any one of claims 1 to 6 are implemented, or the steps of the access control method according to any one of claims 7 to 13 are implemented, or the steps of the access control method according to any one of claims 14 to 16 are implemented, or the steps of the access control method according to according to any one of claims 17 to 19 are implemented, or the steps of the access control method according to according to any one of claims 20 to 22 are implemented.

24. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program, and when the computer program is executed by a processor, the steps of the access control method according to any one of claims 1 to 6 are implemented, or the steps of the access control method according to any one of claims 7 to 13 are implemented, or the steps of the access control method according to any one of claims 14 to 16 are implemented, or the steps of the access control method according to according to any one of claims 17 to 19 are implemented, or the steps of the access control method according to according to any one of claims 20 to 22 are implemented.