COMMUNICATION METHOD AND APPARATUS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to Chinese Patent Application No. 202110502638.5, filed with the China National Intellectual Property Administration on May 9, 2021 and entitled "COMMUNICATION METHOD AND APPARATUS", which is incorporated herein by reference in its entirety.

[0002]

TECHNICAL FIELD

[0003] Embodiments of this application relate to the wireless communication field, and in particular, to a communication method and apparatus.

BACKGROUND

[0004] FIG. 1 shows an enhanced service-based architecture. In the enhanced service-based architecture, network elements may communicate with each other in a direct manner (which is briefly referred to as direct communication), or may communicate with each other in an indirect manner (which may be briefly referred to as indirect communication, and may also be referred to as non-direct communication). In an indirect communication process, two network elements that communicate with each other may exchange messages through a service communication proxy (service communication proxy, SCP). During direct communication and indirect communication, two communication parties are respectively referred to as a service consumer (consumer) and a service producer (producer). A consumer is a service requester or a service caller, and a producer is a service producer. The service consumer is also referred to as a service consumer network element, and the service producer is also referred to as a service producer network element.

[0005] In an indirect communication scenario, an authentication scheme based on a client credentials assertion (client credentials assertion, CCA) is introduced. The consumer includes a CCA in a service request, so that a receiver can authenticate the consumer. In different indirect communication scenarios, the consumer (namely, a peer) needs to generate a correct CCA, so that the receiver (namely, an authenticator) can accurately authenticate the consumer and provide, when the authentication succeeds, a service requested by the consumer to the consumer. However,

an existing standard does not define how to generate the correct CCA in the different indirect communication scenarios, to avoid a problem that the service consumer network element may fail to request the service.

SUMMARY

[0006] Embodiments of this application provide a communication method and apparatus, to avoid a case in which a service consumer network element fails to request a service.

[0007] According to a first aspect, an embodiment of this application provides a communication method. The method includes:

[0008] A service consumer network element sends a first service request message to a service communication proxy, where the first service request message is used to request a first service from a service producer network element, the first service request message includes a first client credentials assertion, the first client credentials assertion is used to authenticate the service consumer network element, the first client credentials assertion includes a first network function type and a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service. The service consumer network element receives a response message for the first service request message from the service communication proxy.

[0009] According to the foregoing method, when the service consumer network element requests the first service from the service producer network element through the service communication proxy, the service consumer network element carries, in the first service request message sent to the service communication proxy, the client credentials assertion including the first network function type and the second network function type. This can ensure that when the service communication proxy requests the second service, the network element providing the second service successfully authenticates the service consumer network element, further ensures that the service consumer network element requests the first service, and resolves a problem, in an indirect communication scenario, that the service consumer network element fails to request the service because the authentication based on the client credentials assertion fails.

[0010] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service.

[0011] In a possible design, the service consumer network element determines that there is no available access token corresponding to the first service.

[0012] According to the foregoing design, the service consumer network element can generate the first client credentials assertion as required, and this prevents the first client credentials assertion from being abused.

[0013] In addition, after the service consumer network element determines that there is no available access token corresponding to the first service, the service consumer network element may carry, in the first service request message, a parameter for obtaining the access token corresponding to the first service.

[0014] In a possible design, that the service consumer network element determines that there is no available access token corresponding to the first service may include the following cases: The service consumer network element determines that the access token corresponding to the first service is not stored; or the service consumer network element determines that a stored access token corresponding to the first service expires.

[0015] In a possible design, the service consumer network element deletes the expired access token when the stored access token corresponding to the first service expires.

[0016] According to the foregoing design, storage space can be released in time, and storage load of a system can be reduced.

[0017] In a possible design, the second service is used to provide information about the service producer network element.

[0018] In a possible design, the service consumer network element determines that the first service request message triggers the service communication proxy to request the second service.

[0019] In a possible design, when the service consumer network element determines that the first service request message triggers the service communication proxy to request the second service, the service consumer network element determines, based on one or more of the following cases, that the first service request message triggers the service communication proxy to request the second service: context of a first terminal device is not stored and the first terminal device is associated with the first service; context of the first service is not stored; the service producer network element belongs to a first slice and context corresponding to the first slice is not stored; or the service consumer network element communicates with the service communication proxy for the first time.

[0020] In addition, after the service consumer network element determines that the first service request message can trigger the service communication proxy to request the second service, the service consumer network element may carry, in the first service request message, a parameter for discovering the service producer network element.

[0021] In a possible design, the service consumer network element determines to request the first service in an indirect communication mode, namely, a mode D.

[0022] For example, it may be agreed on in a standard protocol or configured based on preconfiguration information that, when the service consumer network element communicates with the service communication proxy in the mode D, the first service request message always carries the client credentials assertion including the first network function type and the second network function type; or when the service consumer network element communicates with the service communication proxy in the mode D and determines that the first service request message can trigger the service communication proxy to request the second service, the first service request message carries the client credentials assertion including the first network function type and the second network function type.

[0023] In a possible design, the service consumer network element sends a second service request message to the service communication proxy, where the second service request message is used to request the first service, the second service request message includes a second client credentials assertion, the second client credentials assertion includes the first network function type, and the second client credentials assertion is used to authenticate the service consumer network element. The service consumer network element receives a response message for the second service request message from the service communication proxy, where the response message for the second service request message includes indication information. When the service consumer network element sends the first service request message to the service communication proxy, the service consumer network element sends the first service request message to the service communication proxy based on the indication information.

[0024] According to the foregoing design, the service consumer network element may send the first service request message to the service communication proxy based on the indication information.

[0025] In a possible design, the indication information includes a third client credentials assertion, the third client credentials assertion includes the second network function type, and the third client credentials assertion is used to authenticate the network element providing the second service. When the service consumer network element sends the first service request message to the service communication proxy based on the indication information, the service consumer network element sends the first service request message to the service communication proxy when the authentication, based on the third client credentials assertion, on the network element providing the second service succeeds.

[0026] According to the foregoing design, the service consumer network element may authenticate, based on the third client credentials assertion, the network element providing the second service, and send, when the authentication succeeds, the first service request message based on the second network function type included in the third client credentials assertion.

[0027] In a possible design, the network element providing the second service is a network repository function network element.

[0028] In a possible design, the first client credentials assertion further includes one or more of the following: an identifier of the service consumer network element or validity time information, where the validity time information represents validity time of the first client credentials assertion.

[0029] According to a second aspect, this application provides a communication method. The method includes: A first network element receives a first service request message from a service communication proxy, where the first service request message is used to request a first service from the first network element, the first service request message includes a first client credentials assertion, the first client credentials assertion is used to authenticate a service consumer network element, and the first client credentials assertion includes a plurality of network function types. The first network element authenticates the service consumer network element based on the first client credentials assertion. That the first network element authenticates the service consumer network element based on the first client credentials assertion includes: The first network element determines whether a network function type of the first network element matches one or more of the plurality of network function types; and the first network element sends, based on an authentication result, a response message for the first service request message to the service communication proxy.

[0030] According to the foregoing method, when the first client credentials assertion includes the plurality of network function types, the first network element determines whether the network function type of the first network element matches one or more of the plurality of network function types, to obtain the authentication result. Therefore, according to the foregoing method, when the client credentials assertion includes the plurality of network function types, it can be determined whether the authentication on the service consumer network element succeeds, so that network elements with different network function types can authenticate the service consumer network element based on a same client credentials assertion.

[0031] In a possible design, when the authentication result is that the authentication succeeds, the first network element sends the response message for the first service request message to the service communication proxy, where the response message for the first service request message is used to provide the first service. Alternatively, when the authentication result is that the authentication fails, the first network element sends the response message for the first service request message to the service communication proxy, where the response message for the first service request message indicates that requesting of the first service fails.

[0032] In a possible design, the plurality of network function types include a first network

function type and a second network function type. The first network function type is the network function type of the first network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service.

[0033] According to the foregoing design, network elements with two different network function types can authenticate the service consumer network element based on a same client credentials assertion.

[0034] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service; or the second service is used to provide information about the first network element.

[0035] In a possible design, the network element providing the second service is a network repository function network element.

[0036] In a possible design, the first service is used to provide an access token corresponding to a second service, and the access token corresponding to the second service indicates that the service consumer network element has permission to obtain the second service; or the first service is used to provide information about a second service network element.

[0037] According to the foregoing design, network elements with two different network function types can authenticate the service consumer network element based on a same client credentials assertion.

[0038] In a possible design, the first network element is a network repository function network element.

[0039] In a possible design, the first network element receives a second service request message from the service communication proxy, where the second service request message is used to request the first service from the first network element, the second service request message includes a second client credentials assertion, and the second client credentials assertion includes a third network function type. When the third network function type does not match the network function type of the first network element, the first network element sends, a response message for the second service request message to the service communication proxy, where the response message for the second service request message includes indication information, and the indication information is used to trigger the first service request message.

[0040] According to the foregoing design, when a network function type in the client credentials assertion does not match the network function type of the first network element, the first network element may carry the indication information in the response message for the second service request message. The indication information may be used to trigger the first service request

message, to obtain a client credentials assertion including a network function type that matches the network function type of the first network element, so that the first network element successfully authenticates the service consumer network element.

[0041] In a possible design, the indication information includes a third client credentials assertion used to authenticate the first network element, and the third client credentials assertion includes the network function type of the first network element.

[0042] According to the foregoing design, the network function type of the first network element may be carried in the indication information, to trigger the first client credentials assertion in the first service request message to carry the network function type that matches the network function type of the first network element, so as to successfully authenticate the service consumer network element.

[0043] In a possible design, the first client credentials assertion further includes an identifier of the service consumer network element and validity time information of the first client credentials assertion, and the validity time information of the first client credentials assertion represents validity time of the first client credentials assertion. That the first network element authenticates the service consumer network element based on the first client credentials assertion further includes one or more of the following: The first network element verifies whether a signature of the first client credentials assertion succeeds, verifies, based on the validity time information included in the first client credentials assertion, whether the first client credentials assertion expires, or verifies whether the identifier of the service consumer network element in the first client credentials assertion is the same as an identifier of a network element in a certificate for signing the first client credentials assertion.

[0044] According to a third aspect, this application provides a communication method. The method includes: A service consumer network element sends a first service request message to a service communication proxy, where the first service request message is used to request a first service from a service producer network element. The first service request message includes a fourth client credentials assertion and a fifth client credentials assertion, the fourth client credentials assertion is used by the service producer network element to authenticate the service consumer network element, and the fifth client credentials assertion is used by a network element providing a second service, to authenticate the service consumer network element. The fourth client credentials assertion includes a first network function type, and the fifth client credentials assertion includes a second network function type. The first network function type is a network function type of the service producer network element, the second network function type is a network function type of the network element providing the second service, and the second service is associated with the first service. The service consumer network element receives a response

message for the first service request message from the service communication proxy.

[0045] In the foregoing embodiment, the service consumer network element sends the first service request message to the service communication proxy, where the first service request message includes the fourth client credentials assertion and the fifth client credentials assertion, the fourth client credentials assertion includes the first network function type, and the fifth client credentials assertion includes the second network function type, so that the network element providing the second service can successfully authenticate the service consumer network element. This ensures that the service consumer network element requests the first service, and resolves a problem, in an indirect communication scenario, that the service consumer network element fails to request the service because the authentication based on the client credentials assertion fails.

[0046] In a possible design, the fourth client credentials assertion further includes an identifier of the service consumer network element and validity time information of the fourth client credentials assertion, and the validity time information of the fourth client credentials assertion represents validity time of the fourth client credentials assertion. The fifth client credentials assertion further includes the identifier of the service consumer network element and validity time information of the fifth client credentials assertion, where the validity time information of the fifth client credentials assertion represents validity time of the fifth client credentials assertion.

[0047] In a possible design, the validity time of the fifth client credentials assertion is shorter than the validity time of the fourth client credentials assertion.

[0048] According to the foregoing design, a risk that the fifth client credentials assertion is maliciously used by the service communication proxy can be reduced, to ensure security of a communication process.

[0049] In a possible design, the validity time of the fourth client credentials assertion is associated with first duration, and the first duration is determined based on a transmission delay between the service consumer network element and the service communication proxy and a transmission delay between the service communication proxy and the network element providing the second service.

[0050] The foregoing configuration rules for the validity time of the fourth client credentials assertion and the validity time of the fifth client credentials assertion can ensure, as much as possible, that the fourth client credentials assertion and the fifth client credentials assertion are not maliciously used by the service communication proxy, to ensure security of a communication process.

[0051] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service.

[0052] In a possible design, the service consumer network element determines that there is no available access token corresponding to the first service.

[0053] In addition, after the service consumer network element determines that there is no available access token corresponding to the first service, the service consumer network element may carry, in the first service request message, a parameter for obtaining the access token corresponding to the first service.

[0054] According to the foregoing design, the service consumer network element can generate the first client credentials assertion as required, and this prevents the first client credentials assertion from being abused.

[0055] In a possible design, that the service consumer network element determines that there is no available access token corresponding to the first service may include the following cases: The service consumer network element determines that the access token corresponding to the first service is not stored; or the service consumer network element determines that a stored access token corresponding to the first service expires.

[0056] In a possible design, the service consumer network element deletes the expired access token when the stored access token corresponding to the first service expires.

[0057] According to the foregoing design, storage space can be released in time, and storage load of a system can be reduced.

[0058] In a possible design, the second service is used to provide information about the service producer network element.

[0059] In a possible design, the service consumer network element determines that the first service request message triggers the service communication proxy to request the second service.

[0060] In a possible design, when the service consumer network element determines that the first service request message triggers the service communication proxy to request the second service, the service consumer network element determines, based on one or more of the following cases, that the first service request message triggers the service communication proxy to request the second service: context of a first terminal device is not stored and the first terminal device is associated with the first service; context of the first service is not stored; the service producer network element belongs to a first slice and context corresponding to the first slice is not stored; or the service consumer network element communicates with the service communication proxy for the first time.

[0061] In addition, after the service consumer network element determines that the first service request message can trigger the service communication proxy to request the second service, the service consumer network element may carry, in the first service request message, a parameter for discovering the service producer network element.

[0062] In a possible design, the service consumer network element determines to request the first service in an indirect communication mode, namely, a mode D.

[0063] For example, it may be agreed on in a standard protocol or configured based on preconfiguration information that, when the service consumer network element communicates with the service communication proxy in the mode D, the first service request message always carries the client credentials assertion including the first network function type and the second network function type; or when the service consumer network element communicates with the service communication proxy in the mode D and determines that the first service request message can trigger the service communication proxy to request the second service, the first service request message carries the client credentials assertion including the first network function type and the second network function type.

[0064] In a possible design, the service consumer network element sends a second service request message to the service communication proxy, where the second service request message is used to request the first service, the second service request message includes a second client credentials assertion, the second client credentials assertion includes the first network function type, and the second client credentials assertion is used to authenticate the service consumer network element. The service consumer network element receives a response message for the second service request message from the service communication proxy, where the response message for the second service request message includes indication information. When the service consumer network element sends the first service request message to the service communication proxy, the service consumer network element sends the first service request message to the service communication proxy based on the indication information.

[0065] According to the foregoing design, the service consumer network element may send the first service request message to the service communication proxy based on the indication information.

[0066] In a possible design, the indication information includes a third client credentials assertion, the third client credentials assertion includes the second network function type, and the third client credentials assertion is used to authenticate the network element providing the second service. When the service consumer network element sends the first service request message to the service communication proxy based on the indication information, the service consumer network element sends the first service request message to the service communication proxy when the authentication, based on the third client credentials assertion, on the network element providing the second service succeeds.

[0067] According to the foregoing design, the service consumer network element may authenticate, based on the third client credentials assertion, the network element providing the

second service, and send, when the authentication succeeds, the first service request message based on the second network function type included in the third client credentials assertion.

[0068] In a possible design, the network element providing the second service is a network repository function network element.

[0069] According to a fourth aspect, this application provides a communication method. The method includes: A service communication proxy receives a first service request message from a service consumer network element, where the first service request message is used to request a first service from a service producer network element. The first service request message includes a fourth client credentials assertion and a fifth client credentials assertion. The fourth client credentials assertion is used by the service producer network element to authenticate the service consumer network element, and the fifth client credentials assertion is used by a first network element to authenticate the service consumer network element. The fourth client credentials assertion includes a first network function type, and the fifth client credentials assertion includes a second network function type. The first network function type is a network function type of the service producer network element, and the second network function type is a network function type of the first network element. The service communication proxy sends a second service request message to the first network element in response to the first service request message, where the second service request message is used to request a second service, and the second service request message includes the fifth client credentials assertion. The service communication proxy receives a response message for the second service request message from the first network element. The service communication proxy sends a third service request message to the service producer network element based on the response message for the second service request message, where the third service request message is used to request the first service from the service producer network element, and the third service request message includes the fourth client credentials assertion.

[0070] In the foregoing embodiment, the service consumer network element sends the first service request message to the service communication proxy, where the first service request message includes the fourth client credentials assertion and the fifth client credentials assertion, the fourth client credentials assertion includes the first network function type, the fifth client credentials assertion includes the second network function type, and the service communication proxy carries the fifth client credentials assertion when requesting the second service, so that a network element providing the second service can successfully authenticate the service consumer network element, and the service communication proxy carries the fourth client credentials assertion when requesting the first service, so that the service producer network element can successfully authenticate the service consumer network element. This ensures that the service

consumer network element requests the first service, and resolves a problem, in an indirect communication scenario, that the service consumer network element fails to request the service because the authentication based on the client credentials assertion fails.

[0071] In a possible design, the service communication proxy determines, based on the first service request message, that the second service needs to be requested from the first network element; and the service communication proxy determines, based on the network function type of the first network element, to carry the fifth client credentials assertion in the second service request message.

[0072] According to the foregoing design, the service communication proxy may parse the first service request message, select the fifth client credentials assertion from the fourth client credentials assertion and the fifth client credentials assertion based on the network function type of the first network element, and add the fifth client credentials assertion to the second service request message.

[0073] In a possible design, the service communication proxy determines, based on the network function type of the service producer network element, to carry the fourth client credentials assertion in the third service request message.

[0074] According to the foregoing design, the service communication proxy may parse the first service request message, select the fourth client credentials assertion from the fourth client credentials assertion and the fifth client credentials assertion based on the network function type of the service producer network element, and add the fourth client credentials assertion to the second service request message.

[0075] In a possible design, before the service communication proxy receives the first service request message from the service consumer network element, the service communication proxy receives a fourth service request message from the service consumer network element, where the fourth service request message is used to request the first service, the third service request message includes a sixth client credentials assertion, and the sixth client credentials assertion includes a third network function type. The service communication proxy sends a fifth service request message to the first network element, where the fifth service request message is used to request the second service, and the fifth service request message includes the sixth client credentials assertion. The service communication proxy receives a response message for the fifth service request message from the first network element, where the response message for the fifth service request message includes indication information. The service communication proxy sends a response message for the fourth service request message to the service consumer network element based on the indication information.

[0076] According to the foregoing design, the service communication proxy may send, based

on the indication information, the response message for the fourth service request message to the service consumer network element, to obtain a client credentials assertion that matches the network function type of the first network, so that the first network element successfully authenticates the service consumer network element.

[0077] In a possible design, the indication information includes a seventh client credentials assertion, the seventh client credentials assertion includes the network function type of the first network element, and the response message for the fourth service request message further includes the seventh client credentials assertion.

[0078] According to the foregoing design, the indication information may be used to trigger the service consumer network element to send the first service request message, and the first service request message includes the client credentials assertion that matches the network function type of the first network.

[0079] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service.

[0080] In a possible design, the service communication proxy determines that an available access token corresponding to the first service is not stored and the first service request message does not include the access token corresponding to the first service.

[0081] In a possible design, the second service is used to provide information about the service producer network element.

[0082] In a possible design, the service communication proxy determines that the information about the service producer network element is not stored and the first service request message does not include the information about the service producer network element.

[0083] In a possible design, the fourth client credentials assertion further includes an identifier of the service consumer network element and validity time information of the fourth client credentials assertion, and the validity time information of the fourth client credentials assertion represents validity time of the fourth client credentials assertion. The fifth client credentials assertion further includes the identifier of the service consumer network element and validity time information of the fifth client credentials assertion, where the validity time information of the fifth client credentials assertion represents validity time of the fifth client credentials assertion.

[0084] In a possible design, the validity time of the fifth client credentials assertion is shorter than the validity time of the fourth client credentials assertion.

[0085] According to the foregoing design, a risk that the fifth client credentials assertion is maliciously used by the service communication proxy can be reduced, to ensure security of a communication process.

[0086] In a possible design, the validity time of the fourth client credentials assertion is associated with first duration, and the first duration is determined based on a transmission delay between the service consumer network element and the service communication proxy and a transmission delay between the service communication proxy and the network element providing the second service.

[0087] The foregoing configuration rules for the validity time of the fourth client credentials assertion and the validity time of the fifth client credentials assertion can ensure, as much as possible, that the fourth client credentials assertion and the fifth client credentials assertion are not maliciously used by the service communication proxy, to ensure security of a communication process.

[0088] In a possible design, the network element providing the second service is a network repository function network element.

[0089] According to a fifth aspect, this application provides a communication method. The method includes: A first network element receives a first service request message from a service communication proxy, where the first service request message is used to request a first service from the first network element, the first service request message includes a plurality of client credentials assertions, and each client credentials assertion includes a network function type. The first network element authenticates the service consumer network element based on the plurality of client credentials assertions. When the first network element authenticates the service consumer network element based on the plurality of client credentials assertions, the first network element determines whether one or more client credentials assertions in the plurality of client credentials assertions successfully authenticate the service consumer network element. The first network element sends, based on an authentication result, a response message for the first service request message to the service communication proxy.

[0090] According to the foregoing method, when the first service request message includes a plurality of client credentials assertions, the first network element determines that one or more client credentials assertions successfully authenticate the service consumer network element, and obtains the authentication result. Therefore, in the foregoing method, it can be determined, when there are a plurality of client credentials assertions, whether authentication on the service consumer network element succeeds.

[0091] In a possible design, when the authentication result indicates that one or more client credentials assertions successfully authenticate the service consumer network element, the first network element sends the response message for the first service request message to the service communication proxy, where the response message for the first service request message is used to provide the first service. Alternatively, when the authentication result indicates that any one of the

plurality of client credentials assertions fails to authenticate the service consumer network element, the first network element sends the response message for the first service request message to the service communication proxy, where the response message for the first service request message indicates that requesting of the first service fails.

[0092] According to the foregoing design, when one or more client credentials assertions successfully authenticate the service consumer network element, it is determined that the authentication on the service consumer network element succeeds. Alternatively, when any one of the plurality of client credentials assertions fails to authenticate the service consumer network element, that is, all client credentials assertions fail to authenticate the service consumer network element, it is determined that the authentication on the service consumer network element fails.

[0093] In a possible design, the plurality of client credentials assertions include a fourth client credentials assertion and a fifth client credentials assertion. The fourth client credentials assertion includes a first network function type, and the fifth client credentials assertion includes a second network function type. The first network function type is a network function type of the first network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service.

[0094] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service; or the second service is used to provide information about the first network element.

[0095] In a possible design, the network element providing the second service is a network repository function network element.

[0096] In a possible design, the first service is used to provide an access token corresponding to a second service, and the access token corresponding to the second service indicates that the service consumer network element has permission to obtain the second service; or the first service is used to provide information about a second service network element.

[0097] In a possible design, the first network element is a network repository function network element.

[0098] In a possible design, the first network element receives a second service request message from the service communication proxy, where the second service request message is used to request the first service from the first network element, the second service request message includes a sixth client credentials assertion, and the sixth client credentials assertion includes a third network function type. When the third network function type does not match the network function type of the first network element, the first network element sends, a response message for the third service request message to the service communication proxy, where the response message

for the third service request message includes indication information, and the indication information is used to trigger the first service request message.

[0099] According to the foregoing design, when a network function type in the client credentials assertion does not match the network function type of the first network element, the first network element may carry the indication information in the response message for the third service request message. The indication information may be used to trigger the first service request message, to obtain a client credentials assertion including a network function type that matches the network function type of the first network element, so that the first network element successfully authenticates the service consumer network element.

[00100] In a possible design, the indication information includes a seventh client credentials assertion used to authenticate the first network element, and the seventh client credentials assertion includes the network function type of the first network element.

[00101] According to the foregoing design, the network function type of the first network element may be carried in the indication information, to trigger a first client credentials assertion in the first service request message to carry the client credentials assertion including the network function type that matches the network function type of the first network element, so as to successfully authenticate the service consumer network element.

[00102] According to a sixth aspect, this application provides a communication method. The method is used in a scenario in which a service consumer network element requests a first service from a service producer network element through a service communication proxy. The method includes: The service communication proxy sends a client credentials assertion request message to the service consumer network element, where the client credentials assertion request message is used to request a first client credentials assertion, the first client credentials assertion is used by a network element providing a second device, to authenticate the service consumer network element, and the second service is associated with the first service. The service communication proxy receives a response message for the client credentials assertion request message from the service consumer network element, where the response message for the client credentials assertion request message includes the first client credentials assertion, and the first client credentials assertion includes a first network function type and a second network function type, or the first client credentials assertion includes a second network function type. The first network function type is a network function type of the service producer network element, and the second network function type is a network function type of the network element providing the second service.

[00103] According to the foregoing design, the service communication proxy may request the client credentials assertion, to ensure that the service communication proxy requests the second service and the service consumer network element requests the first service.

[00104] In a possible design, before the service communication proxy sends the client credentials assertion request message to the service consumer network element, the service communication proxy receives a first service request message from the service consumer network element, where the first service request message is used to request the first service, the first service request message includes a second client credentials assertion, and the second client credentials assertion includes the first network function type. The service communication proxy sends a second service request message to a first network element, where the second service request message is used to request the second service, and the second service request message includes the second client credentials assertion. The service communication proxy receives a response message for the second service request message from the first network element, where the response message for the second service request message includes indication information. When the service communication proxy sends the client credentials assertion request message to the service consumer network element, the service communication proxy sends the client credentials assertion request message to the service consumer network element based on the indication information.

[00105] According to the foregoing design, when a network function type in the client credentials assertion does not match a network function type of the first network element, the first network element may carry the indication information in the response message for the second service request message. The indication information may be used to trigger the client credentials assertion request message, to obtain a client credentials assertion including a network function type that matches the network function type of the first network element, so that the first network element successfully authenticates the service consumer network element.

[00106] In a possible design, the indication information includes a third client credentials assertion, the third client credentials assertion includes the network function type of the first network element, and the client credentials assertion request message includes the third client credentials assertion.

[00107] According to the foregoing design, the network function type of the first network element may be carried in the indication information, to trigger a first client credentials assertion in the first service request message to carry the client credentials assertion including the network function type that matches the network function type of the first network element, so as to successfully authenticate the service consumer network element.

[00108] In a possible design, the first client credentials assertion includes the second network function type. The service communication proxy sends a third service request message to the first network element, where the third service request message is used to request the second service, and the third service request message includes the first client credentials assertion. The service communication proxy receives a response message for the third service request message from the

first network element. The service communication proxy sends a fourth service request message to the service producer network element based on the response message for the third service request message, where the fourth service request message is used to request the first service, and the fourth service request message includes the second client credentials assertion.

[00109] According to the foregoing design, the service communication proxy parses a response message for the client credentials assertion, carries the first client credentials assertion in the third service request message based on the network function type of the first network element, and carries the second client credentials assertion in the fourth service request message based on the network function type of the service producer network element.

[00110] In a possible design, the first client credentials assertion includes the first network function type and the second network function type. The service communication proxy sends a third service request message to the first network element, where the third service request message is used to request the second service, and the third service request message includes the first client credentials assertion. The service communication proxy receives a response message for the third service request message from the first network element. The service communication proxy sends a fourth service request message to the service producer network element based on the response message for the third service request message, where the fourth service request message is used to request the first service, and the fourth service request message includes the first client credentials assertion, or the fourth service request message includes the second client credentials assertion.

[00111] According to the foregoing design, the service communication proxy parses a response message for the client credentials assertion, carries the first client credentials assertion in the third service request message based on the network function type of the first network element, and carries the first client credentials assertion or the second client credentials assertion in the fourth service request message based on the network function type of the service producer network element.

[00112] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service.

[00113] In a possible design, the service communication proxy determines that the access token corresponding to the first service is not stored and the first service request message does not include the first access token.

[00114] In a possible design, the second service is used to provide information about the service producer network element.

[00115] In a possible design, the service communication proxy determines that the information about the service producer network element is not stored and the first service request message does

not include the information about the service producer network element.

[00116] In a possible design, the network element providing the second service is a network repository function network element.

[00117] According to a seventh aspect, this application provides a communication apparatus. The apparatus includes a transceiver unit and a processing unit. The processing unit invokes the transceiver unit to: send a first service request message to a service communication proxy, where the first service request message is used to request a first service from a service producer network element, the first service request message includes a first client credentials assertion, the first client credentials assertion is used to authenticate the apparatus, the first client credentials assertion includes a first network function type and a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service; and receive a response message for the first service request message from the service communication proxy.

[00118] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service represents that the apparatus has permission to obtain the first service.

[00119] In a possible design, the processing unit is configured to determine that there is no available access token corresponding to the first service.

[00120] In a possible design, the processing unit is configured to: determine, when determining that there is no available access token corresponding to the first service, that the access token corresponding to the first service is not stored; or determine that a stored access token corresponding to the first service expires.

[00121] In a possible design, the processing unit is configured to delete the expired access token when the stored access token corresponding to the first service expires.

[00122] In a possible design, the second service is used to provide information about the service producer network element.

[00123] In a possible design, the processing unit is configured to determine that the first service request message triggers the service communication proxy to request the second service.

[00124] In a possible design, when determining that the first service request message triggers the service communication proxy to request the second service, the processing unit is configured to determine, based on one or more of the following cases, that the first service request message triggers the service communication proxy to request the second service: context of a first terminal device is not stored and the first terminal device is associated with the first service; context of the first service is not stored; the service producer network element belongs to a first slice and context

corresponding to the first slice is not stored; or the apparatus communicates with the service communication proxy for the first time.

[00125] In a possible design, the processing unit is configured to determine to request the first service in an indirect communication mode, namely, a mode D.

[00126] In a possible design, the transceiver unit is configured to: send a second service request message to the service communication proxy, where the second service request message is used to request the first service, the second service request message includes a second client credentials assertion, the second client credentials assertion includes the first network function type, and the second client credentials assertion is used to authenticate the apparatus; and receive a response message for the second service request message from the service communication proxy, where the response message for the second service request message includes indication information. When the first service request message is sent to the service communication proxy, the processing unit is configured to send the first service request message to the service communication proxy based on the indication information.

[00127] In a possible design, the indication information includes a third client credentials assertion, the third client credentials assertion includes the second network function type, and the third client credentials assertion is used to authenticate the network element providing the second service. The transceiver unit is configured to: when the first service request message is sent to the service communication proxy based on the indication information, send the first service request message to the service communication proxy when the authentication, based on the third client credentials assertion, on the network element providing the second service succeeds.

[00128] In a possible design, the network element providing the second service is a network repository function network element.

[00129] In a possible design, the first client credentials assertion further includes one or more of the following: an identifier of the apparatus or validity time information, where the validity time information represents validity time of the first client credentials assertion.

[00130] According to an eighth aspect, this application provides a communication apparatus. The apparatus includes a transceiver unit and a processing unit. The transceiver unit is configured to receive a first service request message from a service communication proxy, where the first service request message is used to request a first service from the apparatus, the first service request message includes a first client credentials assertion, the first client credentials assertion is used to authenticate a service consumer network element. The first client credentials assertion includes a plurality of network function types. The processing unit is configured to authenticate the service consumer network element based on the first client credentials assertion. When the service consumer network element is authenticated based on the first client credentials assertion, the

processing unit determines whether a network function type of the processing unit matches one or more of the plurality of network function types. The processing unit invokes the transceiver unit to send, based on an authentication result, a response message for the first service request message to the service communication proxy.

[00131] In a possible design, when the authentication result is that the authentication succeeds, the transceiver unit is configured to send the response message for the first service request message to the service communication proxy, where the response message for the first service request message is used to provide the first service. Alternatively, when the authentication result is that the authentication fails, the transceiver unit is configured to send the response message for the first service request message to the service communication proxy, where the response message for the first service request message indicates that requesting of the first service fails.

[00132] In a possible design, the plurality of network function types include a first network function type and a second network function type. The first network function type is a network function type of the apparatus, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service.

[00133] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service; or the second service is used to provide information about the apparatus.

[00134] In a possible design, the network element providing the second service is a network repository function network element.

[00135] In a possible design, the first service is used to provide an access token corresponding to the second service, and the access token corresponding to the second service indicates that the service consumer network element has permission to obtain the second service; or the first service is used to provide information about a second service network element.

[00136] In a possible design, the apparatus is a network repository function network element.

[00137] In a possible design, the transceiver unit is configured to receive a second service request message from the service communication proxy, where the second service request message is used to request the first service from the apparatus, the second service request message includes a second client credentials assertion, and the second client credentials assertion includes a third network function type.

[00138] When the third network function type does not match the network function type of the apparatus, the transceiver unit is configured to send a response message for the second service request message to the service communication proxy, where the response message for the second

service request message includes indication information, and the indication information is used to trigger the first service request message.

[00139] In a possible design, the indication information includes a third client credentials assertion used to authenticate the apparatus, and the third client credentials assertion includes the network function type of the apparatus.

[00140] In a possible design, the first client credentials assertion further includes an identifier of the service consumer network element and validity time information of the first client credentials assertion, and the validity time information of the first client credentials assertion represents validity time of the first client credentials assertion. That the processing unit is configured to authenticate the service consumer network element based on the first client credentials assertion further includes one or more of the following: verifying whether a signature of the first client credentials assertion succeeds, verifying, based on the validity time information included in the first client credentials assertion, whether the first client credentials assertion expires, or verifying whether the identifier of the service consumer network element in the first client credentials assertion is the same as an identifier of a network element in a certificate for signing the first client credentials assertion.

[00141] According to a ninth aspect, this application provides a communication apparatus. The apparatus includes a transceiver unit and a processing unit. The processing unit invokes the transceiver unit to: send a first service request message to a service communication proxy, where the first service request message is used to request a first service from a service producer network element, the first service request message includes a fourth client credentials assertion and a fifth client credentials assertion, the fourth client credentials assertion is used by the service producer network element to authenticate a service consumer network element, the fifth client credentials assertion is used by a network element providing a second service, to authenticate the service consumer network element, the fourth client credentials assertion includes a first network function type, the fifth client credentials assertion includes a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of the network element providing the second service, the second service is associated with the first service; and receive a response message for the first service request message from the service communication proxy.

[00142] In a possible design, the fourth client credentials assertion further includes an identifier of the service consumer network element and validity time information of the fourth client credentials assertion, and the validity time information of the fourth client credentials assertion represents validity time of the fourth client credentials assertion. The fifth client credentials assertion further includes the identifier of the service consumer network element and validity time

information of the fifth client credentials assertion, where the validity time information of the fifth client credentials assertion represents validity time of the fifth client credentials assertion.

[00143] In a possible design, the validity time of the fifth client credentials assertion is shorter than the validity time of the fourth client credentials assertion.

[00144] In a possible design, the validity time of the fourth client credentials assertion is associated with first duration, and the first duration is determined based on a transmission delay between the service consumer network element and the service communication proxy and a transmission delay between the service communication proxy and the network element providing the second service.

[00145] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service represents that the apparatus has permission to obtain the first service.

[00146] In a possible design, the processing unit is configured to determine that there is no available access token corresponding to the first service.

[00147] In a possible design, the processing unit is configured to: determine, when determining that there is no available access token corresponding to the first service, that the access token corresponding to the first service is not stored; or determine that a stored access token corresponding to the first service expires.

[00148] In a possible design, the processing unit is configured to delete the expired access token when the stored access token corresponding to the first service expires.

[00149] In a possible design, the second service is used to provide information about the service producer network element.

[00150] In a possible design, the processing unit is configured to determine that the first service request message triggers the service communication proxy to request the second service.

[00151] In a possible design, when determining that the first service request message triggers the service communication proxy to request the second service, the processing unit is configured to determine, based on one or more of the following cases, that the first service request message triggers the service communication proxy to request the second service: context of a first terminal device is not stored and the first terminal device is associated with the first service; context of the first service is not stored; the service producer network element belongs to a first slice and context corresponding to the first slice is not stored; or the apparatus communicates with the service communication proxy for the first time.

[00152] In a possible design, the processing unit is configured to determine to request the first service in an indirect communication mode, namely, a mode D.

[00153] In a possible design, the transceiver unit is configured to: send a second service request

message to the service communication proxy, where the second service request message is used to request the first service, the second service request message includes a second client credentials assertion, the second client credentials assertion includes the first network function type, and the second client credentials assertion is used to authenticate the apparatus; and receive a response message for the second service request message from the service communication proxy, where the response message for the second service request message includes indication information. When the first service request message is sent to the service communication proxy, the processing unit is configured to send the first service request message to the service communication proxy based on the indication information.

[00154] In a possible design, the indication information includes a third client credentials assertion, the third client credentials assertion includes the second network function type, and the third client credentials assertion is used to authenticate the network element providing the second service. The transceiver unit is configured to: when the first service request message is sent to the service communication proxy based on the indication information, send the first service request message to the service communication proxy when the authentication, based on the third client credentials assertion, on the network element providing the second service succeeds.

[00155] In a possible design, the network element providing the second service is a network repository function network element.

[00156] In a possible design, the first client credentials assertion further includes one or more of the following: an identifier of the apparatus or validity time information, where the validity time information represents validity time of the first client credentials assertion.

[00157] According to a tenth aspect, this application provides a communication apparatus. The apparatus includes a transceiver unit and a processing unit. The processing unit invokes the transceiver unit to: receive a first service request message from a service consumer network element, where the first service request message is used to request a first service from a service producer network element, the first service request message includes a fourth client credentials assertion and a fifth client credentials assertion, the fourth client credentials assertion is used by the service producer network element to authenticate the service consumer network element, the fifth client credentials assertion is used by a first network element to authenticate the service consumer network element, the fourth client credentials assertion includes a first network function type, the fifth client credentials assertion includes a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of the first network element; send a second service request message to the first network element in response to the first service request message, where the second service request message is used to request a second service, and the second

service request message includes the fifth client credentials assertion; receive a response message for the second service request message from the first network element; and send a third service request message to the service producer network element based on the response message for the second service request message, where the third service request message is used to request the first service from the service producer network element, and the third service request message includes the fourth client credentials assertion.

[00158] In a possible design, the processing unit is configured to: determine, based on the first service request message, that the second service needs to be requested from the first network element; and determine, based on the network function type of the first network element, to carry the fifth client credentials assertion in the second service request message.

[00159] In a possible design, the processing unit is configured to determine, based on the network function type of the service producer network element, to carry the fourth client credentials assertion in the third service request message.

[00160] In a possible design, before the first service request message from the service consumer network element is received, the transceiver unit is configured to: receive a fourth service request message from the service consumer network element, where the fourth service request message is used to request the first service, the third service request message includes a sixth client credentials assertion, and the sixth client credentials assertion includes a third network function type; send a fifth service request message to the first network element, where the fifth service request message is used to request the second service, and the fifth service request message includes the sixth client credentials assertion; receive a response message for the fifth service request message from the first network element, where the response message for the fifth service request message includes indication information; and send a response message for the fourth service request message to the service consumer network element based on the indication information.

[00161] In a possible design, the indication information includes a seventh client credentials assertion, the seventh client credentials assertion includes the network function type of the first network element, and the response message for the fourth service request message further includes the seventh client credentials assertion.

[00162] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service.

[00163] In a possible design, the processing unit is configured to determine that an available access token corresponding to the first service is not stored and the first service request message does not include the access token corresponding to the first service.

[00164] In a possible design, the second service is used to provide information about the service

producer network element.

[00165] In a possible design, the processing unit is configured to determine that the information about the service producer network element is not stored and the first service request message does not include the information about the service producer network element.

[00166] In a possible design, the fourth client credentials assertion further includes an identifier of the service consumer network element and validity time information of the fourth client credentials assertion, and the validity time information of the fourth client credentials assertion represents validity time of the fourth client credentials assertion. The fifth client credentials assertion further includes the identifier of the service consumer network element and validity time information of the fifth client credentials assertion, where the validity time information of the fifth client credentials assertion represents validity time of the fifth client credentials assertion.

[00167] In a possible design, the validity time of the fifth client credentials assertion is shorter than the validity time of the fourth client credentials assertion.

[00168] In a possible design, the validity time of the fourth client credentials assertion is associated with first duration, and the first duration is determined based on a transmission delay between the service consumer network element and the service communication proxy and a transmission delay between the service communication proxy and the network element providing the second service.

[00169] In a possible design, the network element providing the second service is a network repository function network element.

[00170] According to an eleventh aspect, this application provides a communication apparatus. The apparatus includes a transceiver unit and a processing unit. The processing unit invokes the transceiver unit to: receive a first service request message from a service communication proxy, where the first service request message is used to request a first service from a first network element, the first service request message includes a plurality of client credentials assertions, and each client credentials assertion includes a network function type. The first network element authenticates a service consumer network element based on the plurality of client credentials assertions. That the first network element authenticates the service consumer network element based on the plurality of client credentials assertions includes: The first network element determines whether one or more client credentials assertions in the plurality of client credentials assertions successfully authenticate the service consumer network element. The first network element sends, based on an authentication result, a response message for the first service request message to the service communication proxy.

[00171] In a possible design, when the authentication result indicates that one or more client credentials assertions successfully authenticate the service consumer network element, the first

network element sends the response message for the first service request message to the service communication proxy, where the response message for the first service request message is used to provide the first service. Alternatively, when the authentication result indicates that any one of the plurality of client credentials assertions fails to authenticate the service consumer network element, the first network element sends the response message for the first service request message to the service communication proxy, where the response message for the first service request message indicates that requesting of the first service fails.

[00172] In a possible design, the plurality of client credentials assertions include a fourth client credentials assertion and a fifth client credentials assertion. The fourth client credentials assertion includes a first network function type, and the fifth client credentials assertion includes a second network function type. The first network function type is a network function type of the first network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service.

[00173] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service; or the second service is used to provide information about the first network element.

[00174] In a possible design, the network element providing the second service is a network repository function network element.

[00175] In a possible design, the first service is used to provide an access token corresponding to the second service, and the access token corresponding to the second service indicates that the service consumer network element has permission to obtain the second service; or the first service is used to provide information about a second service network element.

[00176] In a possible design, the first network element is a network repository function network element.

[00177] In a possible design, the transceiver unit is configured to receive a second service request message from the service communication proxy, where the second service request message is used to request the first service from the first network element, the second service request message includes a sixth client credentials assertion, and the sixth client credentials assertion includes a third network function type.

[00178] When the third network function type does not match the network function type of the first network element, the transceiver unit is configured to send a response message for the second service request message to the service communication proxy, where the response message for the second service request message includes indication information, and the indication information is used to trigger the first service request message.

[00179] In a possible design, the indication information includes a seventh client credentials assertion used to authenticate the first network element, and the seventh client credentials assertion includes the network function type of the first network element.

[00180] According to a twelfth aspect, this application provides a communication apparatus. The apparatus includes a transceiver unit and a processing unit. A service consumer network element requests a first service from a service producer network element by using the apparatus. The processing unit invokes the transceiver unit to: send a client credentials assertion request message to the service consumer network element, where the client credentials assertion request message is used to request a first client credentials assertion, the first client credentials assertion is used by a network element providing a second device, to authenticate the service consumer network element, and the second service is associated with the first service; and receive a response message for the client credentials assertion request message from the service consumer network element, where the response message for the client credentials assertion request message includes the first client credentials assertion, and the first client credentials assertion includes a first network function type and a second network function type, or the first client credentials assertion includes a second network function type. The first network function type is a network function type of the service producer network element, and the second network function type is a network function type of the network element providing the second service.

[00181] In a possible design, before the client credentials assertion request message is sent to the service consumer network element, the transceiver unit is configured to: receive a first service request message from the service consumer network element, where the first service request message is used to request the first service, the first service request message includes a second client credentials assertion, and the second client credentials assertion includes the first network function type; send a second service request message to the network element providing the second service, where the second service request message is used to request the second service, and the second service request message includes the second client credentials assertion; receive a response message for the second service request message from the network element providing the second service, where the response message for the second service request message includes indication information; and send, when the client credentials assertion request message is sent to the service consumer network element, the client credentials assertion request message to the service consumer network element based on the indication information.

[00182] In a possible design, the indication information includes a third client credentials assertion, the third client credentials assertion includes a network function type of a first network element, and the client credentials assertion request message includes the third client credentials assertion.

[00183] In a possible design, the first client credentials assertion includes the second network function type. The service communication proxy sends a third service request message to the first network element, where the third service request message is used to request the second service, and the third service request message includes the first client credentials assertion. The service communication proxy receives a response message for the third service request message from the first network element. The service communication proxy sends a fourth service request message to the service producer network element based on the response message for the third service request message, where the fourth service request message is used to request the first service, and the fourth service request message includes the second client credentials assertion.

[00184] In a possible design, the first client credentials assertion includes the first network function type and the second network function type. The transceiver unit is configured to: send a third service request message to the first network element, where the third service request message is used to request the second service, and the third service request message includes the first client credentials assertion; receive a response message for the third service request message from the first network element; and send a fourth service request message to the service producer network element based on the response message for the third service request message, where the fourth service request message is used to request the first service, and the fourth service request message includes the first client credentials assertion, or the fourth service request message includes the second client credentials assertion.

[00185] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service.

[00186] In a possible design, before the client credentials assertion request message is sent to the service consumer network element, the processing unit is configured to determine that a first access token is not stored and the first service request message does not include the access token corresponding to the first service.

[00187] In a possible design, the second service is used to provide information about the service producer network element.

[00188] In a possible design, before the client credentials assertion request message is sent to the service consumer network element, the processing unit is configured to determine that the information about the service producer network element is not stored and the first service request message does not include the information about the service producer network element.

[00189] In a possible design, the network element providing the second service is a network repository function network element.

[00190] According to a thirteenth aspect, this application further provides a communication

apparatus. The apparatus may perform the foregoing method design. The apparatus may be a chip or a circuit that can perform a function corresponding to the foregoing method, or a device including the chip or the circuit.

[00191] In a possible implementation, the apparatus includes: a memory, configured to store computer-executable program code; and a processor, where the processor is coupled to the memory. The program code stored in the memory includes instructions. When the processor executes the instructions, the apparatus or a device on which the apparatus is installed is enabled to perform the method in any one of possible designs of the first aspect to the sixth aspect.

[00192] The apparatus may further include a communication interface. The communication interface may be a transceiver. Alternatively, if the apparatus is a chip or a circuit, the communication interface may be an input/output interface of the chip, for example, an input/output pin.

[00193] In a possible design, the apparatus includes corresponding functional units, which are respectively configured to implement the steps in the foregoing method. The function may be implemented by hardware, or may be implemented by hardware executing corresponding software. The hardware or the software includes one or more units corresponding to the foregoing function.

[00194] According to a fourteenth aspect, an embodiment of this application provides a computer-readable storage medium, where the computer-readable storage medium stores a computer program, and when the computer program is run on an apparatus, the method in any one of the possible designs of the first aspect to the sixth aspect is performed.

[00195] According to a fifteenth aspect, an embodiment of this application provides a computer program product, where the computer program product includes a computer program, and when the computer program is run on an apparatus, the method in any one of the possible designs of the first aspect to the sixth aspect is performed.

[00196] According to a sixteenth aspect, this application provides a communication chip, where the communication chip stores instructions, and when the instructions are run on a communication device, the communication chip is enabled to perform the method in any one of the possible designs of the first aspect to the sixth aspect.

BRIEF DESCRIPTION OF DRAWINGS

[00197] FIG. 1 is a schematic diagram of an architecture of a mobile communication system to which an embodiment of this application is applied;

[00198] FIG. 2 is a schematic diagram of an indirect communication mode, namely, a mode C according to an embodiment of this application;

[00199] FIG. 3 is a schematic diagram of an indirect communication mode, namely, a mode D according to an embodiment of this application;

[00200] FIG. 4 is a schematic diagram of direct interaction between an NF service consumer and an NRF in an indirect communication mode, namely, a mode C according to an embodiment of this application;

[00201] FIG. 5 is a schematic diagram of interaction between an NF service consumer and an NRF through an SCP in an indirect communication mode, namely, a mode C according to an embodiment of this application;

[00202] FIG. 6 is a schematic diagram 1 of interaction between an NF service consumer and an NRF through an SCP in an indirect communication mode, namely, a mode D according to an embodiment of this application;

[00203] FIG. 7 is a schematic diagram 2 of interaction between an NF service consumer and an NRF through an SCP in an indirect communication mode, namely, a mode D according to an embodiment of this application;

[00204] FIG. 8 is an overview flowchart 1 of a communication method according to an embodiment of this application;

[00205] FIG. 9 shows a specific process in which a service consumer network element sends a first service request message to a service communication proxy based on indication information according to an embodiment of this application;

[00206] FIG. 10 is an overview flowchart 2 of a communication method according to an embodiment of this application;

[00207] FIG. 11 is an overview flowchart 3 of a communication method according to an embodiment of this application;

[00208] FIG. 12 is an overview flowchart 4 of a communication method according to an embodiment of this application;

[00209] FIG. 13 is a flowchart 1 in which an NF service consumer obtains a first service when it is determined that the first service needs to be requested and there is no available access token corresponding to the first service according to an embodiment of this application;

[00210] FIG. 14 is a flowchart 2 in which an NF service consumer obtains a first service when it is determined that the first service needs to be requested and there is no available access token corresponding to the first service according to an embodiment of this application;

[00211] FIG. 15 is a flowchart 3 in which an NF service consumer obtains a first service when it is determined that the first service needs to be requested and there is no available access token corresponding to the first service according to an embodiment of this application;

[00212] FIG. 16 is a flowchart in which an NF service consumer obtains a first service when it

is determined that the first service needs to be requested and there is an available access token corresponding to the first service according to an embodiment of this application;

[00213] FIG. 17 is a flowchart 1 in which an NF service consumer obtains a first service when the first service needs to be requested and the first service is requested to trigger an SCP to request a parameter of an NF service producer according to an embodiment of this application;

[00214] FIG. 18 is a flowchart 2 in which an NF service consumer obtains a first service when the first service needs to be requested and the first service is requested to trigger an SCP to request a parameter of an NF service producer according to an embodiment of this application;

[00215] FIG. 19A and FIG. 19B are a flowchart in which an NF service consumer sends a service request message to an SCP based on indication information to obtain a first service according to an embodiment of this application;

[00216] FIG. 20A and FIG. 20B are a flowchart in which an NF service consumer obtains a first service when an SCP actively requests a client credentials assertion according to an embodiment of this application;

[00217] FIG. 21 is a schematic diagram 1 of a structure of a communication apparatus according to an embodiment of this application; and

[00218] FIG. 22 is a schematic diagram 2 of a structure of a communication apparatus according to an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

[00219] The following clearly and completely describes the technical solutions in embodiments of this application with reference to the accompanying drawings in embodiments of this application. It is clear that the described embodiments are merely some but not all of embodiments of this application. In this specification, claims, and accompanying drawings of this application, the terms "first", "second", corresponding term numbers, 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 terms used in such a way are interchangeable in proper circumstances, which is merely a distinguishing manner that is used when objects having a same attribute are described in embodiments of this application. In addition, the terms "include", "contain" and any other variants mean to cover the non-exclusive inclusion, so that a process, method, system, product, or device that includes a series of units is not necessarily limited to those units, but may include other units not expressly listed or inherent to such a process, method, system, product, or device.

[00220] In descriptions of this application, "/" means "or" unless otherwise specified. For example, A/B may represent A or B. In this application, "and/or" describes only an association

relationship for describing associated objects and represents that three relationships may exist. For example, A and/or B may represent the following three cases: Only A exists, both A and B exist, and only B exists. In addition, in the descriptions of this application, "at least one item" means one or more items, and "a plurality of items" means two or more items. "At least one item (piece) of the following" or a similar expression thereof means any combination of these items, including a singular item (piece) or any combination of plural items (pieces). For example, at least one item (piece) of a, b, or c may indicate a, b, c, a and b, a and c, b and c, or a, b, and c, where a, b, and c may be singular or plural.

[00221] The technical solutions in embodiments of this application may be applied to various communication systems, for example, a wideband code division multiple access (Wideband Code Division Multiple Access, WCDMA) system, a general packet radio service (general packet radio service, GPRS), a long term evolution (Long Term Evolution, LTE) system, an LTE frequency division duplex (frequency division duplex, FDD) system, an LTE time division duplex (time division duplex, TDD) system, a universal mobile telecommunication system (universal mobile telecommunication system, UMTS), a worldwide interoperability for microwave access (worldwide interoperability for microwave access, WiMAX) communication system, a 5th generation (5th generation, 5G) system, or a further 6th generation communication system.

[00222] For ease of understanding embodiments of this application, an application scenario used in this application is described by using an enhanced service-based architecture shown in FIG. 1 as an example. Specifically, the enhanced service-based architecture may specifically include but is not limited to the following devices.

[00223] 1. Session management network element: is mainly configured to: manage a session, allocate and manage an internet protocol (internet protocol, IP) address of a terminal device, select an endpoint that can manage a user equipment plane function interface and a policy control or charging function interface, perform downlink data notification, and the like. In 5G communication, the session management network element may be a session management function (session management function, SMF) network element. In future communication such as 6G communication, the session management function network element may still be an SMF network element or have another name. This is not limited in this application. Nsmf is a service-based interface provided by an SMF. The SMF may communicate with another network function through the Nsmf.

[00224] 2. Access management network element: is mainly configured to perform mobility management, access management, and the like. The access management network element may be configured to implement a function, for example, lawful interception or access authorization (or authentication), in mobility management entity (mobility management entity, MME) functions

other than session management. In 5G communication, the access management network element may be an access and mobility management function (access and mobility management function, AMF) network element. In future communication such as 6G communication, the access management network element may still be an AMF network element or have another name. This is not limited in this application. Namf is a service-based interface provided by the AMF. The AMF may communicate with another network function through the Namf.

[00225] 3. Authentication service network element: is mainly configured to perform user authentication and the like. In 5G communication, the authentication service network element may be an authentication server function (authentication server function, AUSF) network element. In future communication such as 6G communication, the authentication service network element may still be an AUSF network element or have another name. This is not limited in this application. Nausf is a service-based interface provided by the AUSF. The AUSF may communicate with another network function through the Nausf.

[00226] 4. Network exposure network element: is configured to securely expose, to the outside, a service, a capability, and the like that are provided by a 3rd generation partnership project (3rd generation partnership project, 3GPP) network function. In 5G communication, the network exposure network element may be a network exposure function (network exposure function, NEF) network element. In future communication such as 6G communication, the network exposure function network element may still be an NEF network element or have another name. This is not limited in this application. Nnef is a service-based interface provided by the NEF. The NEF may communicate with another network function through the Nnef.

[00227] 5. Network repository network element: is configured to provide service registration, discovery, and authorization, and maintain available network function (network function, NF) instance information. These functions help achieve NF interconnections and on-demand network function and service configurations. The service registration means that an NF network element can provide a service only after being registered with the network repository network element. The service discovery means that when the NF network element needs another NF network element to provide a service for the NF network element, the NF network element needs to perform service discovery by using the network repository network element, to discover an expected NF network element that provides a service for the NF network element. For example, when an NF network element 1 needs an NF network element 2 to provide a service for the NF network element 1, the NF network element 1 needs to perform service discovery by using the network repository network element, to discover the NF network element 2. The service authorization means that when the NF network element needs another NF network element to provide a service, the NF network element needs to obtain authorization information by using the network repository network element, to

further obtain, based on the authorization information, the service provided by the another NF network element. For example, before the NF network element 1 requests a service from the NF

network element 2, the NF network element 1 first requests, from the network storage network element, authorization information for accessing the NF network element 2, and the NF network element 1 requests the service from the NF network element 2 based on the obtained authorization information. In 5G communication, the network repository network element may be a network repository function (network repository function, NRF) network element. In future communication such as 6G communication, the network repository function network element may still be an NRF network element or have another name. This is not limited in this application. Nnrf is a service-based interface provided by the NRF. The NRF may communicate with another network function through the Nnrf.

[00228] 6. Policy control network element: is configured to guide a unified policy framework for network behavior, provide policy rule information for a control plane function network element (for example, an AMF or an SMF), and the like. In 5G communication, the policy control network element may be a policy control function (policy control function, PCF) network element. In future communication such as 6G communication, the policy control function network element may still be an NEF network element or have another name. This is not limited in this application. Npcf is a service-based interface provided by the PCF. The PCF may communicate with another network function through the Npcf.

[00229] 7. Data management network element: is configured to perform user identifier processing, access authentication, registration, mobility management, or the like. In 5G communication, the data management network element may be a unified data management (unified data management, UDM) network element. In future communication such as 6G communication, the data management network element may still be a UDM network element or have another name. This is not limited in this application. Nudm is a service-based interface provided by the UDM. The UDM may communicate with another network function through the Nudm.

[00230] 8. Application network element: is configured to perform application-affected data routing, access a network exposure function, interact with a policy framework to perform policy control, or the like. In 5G communication, the application network element may be an application function (application function, AF) network element. In future communication such as 6G communication, the application network element may still be an AF network element or have another name. This is not limited in this application. Naf is a service-based interface provided by the AF. The AF may communicate with another network function through the Naf.

[00231] 9. User equipment (user equipment, UE): may include various handheld devices, vehicle-mounted devices, wearable devices, or computing devices having a wireless communication function, or another processing device connected to a wireless modem, and

terminals, mobile stations (mobile stations, MSs), terminals (terminals), user equipment (user equipment, UE), software terminals, and the like in various forms, for example, a water meter, an electricity meter, and a sensor.

[00232] 10. (Radio) access network (radio access network, (R)AN) network element: is configured to provide a network access function for authorized user equipment in a specific area, and can use transmission tunnels with different quality based on user equipment levels, service requirements, and the like.

[00233] The RAN network element can manage radio resources and provide an access service for a terminal device, to forward a control signal and user equipment data between the terminal and a core network. The RAN network element may also be understood as a base station in a conventional network.

[00234] 11. User plane (user plane function, UPF) network element: is configured to perform packet routing and forwarding, perform quality of service (quality of service, QoS) processing on user plane data, and the like. In 5G communication, the user plane network element may be a user plane function (user plane function, UPF) network element. In future communication such as 6G communication, the user plane network element may still be a UPF network element or have another name. This is not limited in this application.

[00235] 12. Data network (data network, DN) network element: is configured to provide a network for data transmission, for example, an internet network. The DN network element may be a data network authentication, authorization, and accounting (data network authentication, authorization, accounting) network element, an application server (application function), or the like.

[00236] 13. SCP: is configured to route and forward a service-oriented interface message. This may also be understood as that the SCP may provide routing and forwarding services for a sender of service-oriented interface signaling. For example, when an AMF requests an SMF to establish a session, the AMF sends a session establishment request message to the SCP, the SCP sends the session establishment request message to the SMF, and the SMF determines whether to respond to the session establishment request message. If the SMF sends a session establishment response message to the SCP, the SCP sends the session establishment response message to the AMF. If the SMF sends a session establishment reject message to the SCP, the SCP sends the session establishment reject message to the AMF. A message exchanged between the AMF and the SMF may pass through a one-hop SCP or multi-hop SCP.

[00237] It may be understood that the foregoing functions or network elements may be network elements in a hardware device, software functions running on dedicated hardware, or virtualized functions instantiated on a platform (for example, a cloud platform). An application scenario of

embodiments of this application is not limited thereto, and any network architecture that can implement the foregoing network functions is applicable to embodiments of this application.

[00238] It should be noted that in the following content, a consumer, a service consumer network element, and an NF service consumer are network elements of a same type, and a producer, a service producer network element, and an NF service producer are network elements of a same type. In the following embodiments of this application, it is assumed that a local operator policy indicates that a service request message sent by an NF service consumer to an SCP needs to carry a CCA. For example, the local operator policy may be configured as that the NF service consumer generates a CCA during indirect communication, to authenticate the NF service consumer based on the CCA.

[00239] Based on the foregoing enhanced service-based architecture, the following briefly describes several modes of an indirect communication procedure.

[00240] 1. Indirect communication without delegated discovery (indirect communication without delegated discovery) (which is briefly referred to as a mode C)

[00241] A consumer directly communicates with an NRF, to perform a service discovery procedure to select a corresponding service producer network element, and no SCP network element needs to participate in the service discovery procedure.

[00242] The following describes the mode C with reference to FIG. 2.

[00243] Step 201: The consumer sends a producer discovery message to the NRF.

[00244] Step 202: The NRF sends information about an available producer to the consumer.

[00245] In some embodiments, the consumer may select a target producer based on the obtained information about the available producer. The information about the available producer may include an NF set ID, a specific NF instance identifier, or the like. Specifically, the target producer may be any NF instance (namely, any producer in a producer set) corresponding to the NF set ID, a specific NF instance (namely, a specific producer) in an NF instance corresponding to a specific NF set ID, or a specific NF instance (namely, a specific producer).

[00246] In some embodiments, an SCP may be responsible for selecting a target producer. For details, refer to the following step 204.

[00247] Step 203: The consumer sends a service request message to the SCP, to request a specific service from the target producer through the SCP.

[00248] Step 204: The SCP interacts with the NRF to obtain a parameter for selecting the target producer.

[00249] For example, the parameter obtained by the SCP may include but is not limited to a location, a capacity, or the like of an NF instance.

[00250] It should be noted that step 204 is an optional step. For example, the service request

message includes information about the available producer. For example, the information about the available producer includes the NF set ID, in other words, the information about the available producer points to a group of NF instances. The SCP needs to select an NF instance from the group of NF instances as the target producer. Specifically, the SCP may select the target producer based on the parameter obtained from the NRF. For example, the SCP may determine the target producer from a group of NF instances based on the obtained location of the NF instance.

[00251] Step 205: The SCP sends a service request message to the target producer, to request the specific service from the target producer.

[00252] Step 206: The target producer sends, to the SCP, a service request response message for providing the specific service.

[00253] Step 207: The SCP sends, to the consumer, a service request response message for providing the specific service.

[00254] 2. Indirect communication with delegated discovery (indirect communication with delegated discovery) (which is briefly referred to as a mode D)

[00255] A consumer does not directly communicate with an NRF. An SCP network element serves as a proxy of the consumer to communicate with the NRF, to perform a service discovery procedure to select a corresponding service producer network element.

[00256] The following describes the mode D with reference to FIG. 3.

[00257] Step 301: The consumer sends a service request message to the SCP, to request a specific service from a target producer through the SCP.

[00258] The service request message includes a parameter used for target producer discovery and selection.

[00259] Step 302: The SCP interacts with the NRF to obtain information about an available producer.

[00260] The SCP may obtain the information about the available producer based on the parameter that is in the service request message in step 301 and that is used for target producer discovery and selection, and determine a target producer from the information about the available producer.

[00261] Step 303: The SCP sends a service request message to the target producer, to request the specific service from the target producer.

[00262] Step 304: The target producer sends, to the SCP, a service request response message for providing the specific service.

[00263] Step 305: The SCP sends, to the consumer, a service request response message for providing the specific service.

[00264] It should be noted that, in embodiments of this application, the service request message

received by the SCP from the consumer and the service request message sent by the SCP to the target producer may be the same or different. For example, the SCP may modify the service request message received from the consumer (for example, add, delete, or modify some information) to generate and send the service request message to the target producer. Similarly, the service request response message received by the SCP from the target producer and the service request response message sent by the SCP to the consumer may be the same or different. For example, the SCP may modify the service request response message received from the target producer to generate the service request response message sent to the consumer.

[00265] Further, in the indirect communication procedures shown in FIG. 2 and FIG. 3, when the consumer communicates with the producer through the SCP, the producer further needs to authenticate the consumer that initiates a service request. Similarly, when the consumer communicates with the NRF through the SCP, the NRF also needs to authenticate the consumer that initiates the service request.

[00266] For an authentication requirement in the foregoing indirect communication scenario, the following describes verification information in embodiments of this application.

[00267] 1. Client credentials assertion (client credentials assertion, CCA)

[00268] For example, the CCA may be a token (token) signed by a peer, and is used by an authenticator to authenticate/verify the peer, that is, determine an identity of the peer.

[00269] For example, the CCA is a token signed by an NF service consumer. The CCA is included in a message, so that a receiver (namely, the authenticator, for example, an NRF or an NF service producer) of the message authenticates the NF service consumer. For example, the CCA may be included in a message header or a message body of a hypertext transfer protocol (hypertext transfer protocol, HTTP) message.

[00270] The CCA may include three parts: a message header (head), a payload (payload), and a signature (signature).

[00271] The payload includes claims (claims). For example, the claims include an NF instance ID of the NF service consumer, a timestamp (timestamp), expiration time, and an NF type of an expected audience. The timestamp indicates release time of the CCA, and the expiration time indicates that the CCA is considered to expire after the time. The NF type of the expected audience is an NF type of a network element that authenticates the NF service consumer.

[00272] The message header and the payload are signed by the NF service consumer based on a private key of an NF service consumer certificate. The message header includes certificate information, namely, related information of the NF service consumer certificate. For example, the certificate information includes a certificate or a certificate chain that is located to a public key, or the certificate information includes a uniform resource locator (uniform resource locator, URL) of

a certificate or a certificate chain that is located to a public key.

[00273] When the authenticator (for example, the NRF or the NF service producer) receives a message containing the CCA, the authenticator authenticates the NF service consumer based on the CCA. The authentication process is as follows:

[00274] A signature of the CCA is verified. If the signature verification succeeds, whether the CCA expires is verified based on the timestamp and/or the expiration time of the CCA. If the CCA does not expire, the authenticator further verifies whether the NF type of the expected audience matches an NF type of the authenticator. If the NF type of the expected audience matches the NF type of the authenticator, the authenticator verifies whether an NF instance ID of the NF service consumer in the CCA matches an NF instance ID in a certificate for signing the CCA. If the NF instance ID of the NF service consumer matches the NF instance ID in the certificate, all verifications succeed, and the authenticator determines that the authentication on the NF service consumer succeeds. It should be noted that a sequence of the foregoing verification is not limited in this application.

[00275] That the authenticator verifies whether the NF type of the expected audience matches the NF type of the authenticator may include that, for example, the authenticator determines whether the NF type of the expected audience is the same as the NF type of the authenticator. For example, when the NF type of the expected audience is an AMF, the authenticator verifies whether the NF type of the authenticator is an AMF. Verifying whether the NF instance ID of the NF service consumer in the CCA matches the NF instance ID in the certificate for signing the CCA may include, for example, determining whether the NF instance ID of the NF service consumer in the CCA is the same as the NF instance ID in the certificate for signing the CCA.

[00276] It may be understood that the foregoing authentication process is merely an example, and the authenticator may further verify the CCA in another order. This is not limited in this application.

[00277] 2. Access token (access token)

[00278] The access token represents/indicates that the consumer has permission to obtain a service. A producer provides the corresponding service for the consumer only when the verification of the access token succeeds.

[00279] For example, the NRF receives an access token request message from the NF service consumer or the SCP, and the NRF performs authorization check, and determines that the authorization succeeds. In this case, the NRF generates an access token including claims.

[00280] There are two types of access tokens: an access token based on an NF type of an NF service producer (which is briefly referred to as a type A) and an access token based on an NF service producer instance or an NF service producer service instance (which is briefly referred to

as a type B).

[00281] An instance is defined based on a function. An instance may be an NF service consumer instance or an NF service producer instance. An instance is defined based on a service. An instance may also be referred to as a service instance. For example, a service instance may be a service instance providing a service A or a service instance providing a service B.

[00282] If the NF service consumer requests an access token of a type A, the requested access token indicates that the NF service consumer has permission to access any NF service producer corresponding to the NF type to obtain a service, or the requested access token indicates that the NF service consumer has permission to access a service of any NF service producer corresponding to the NF type. The access token request message includes an NF instance ID of the NF service consumer, an expected service name, an NF type of the NF service consumer, and an NF type of an expected NF service producer. Optionally, the access token request message may further include a single network slice selection assistance information (single network slice selection assistance information, S-NSSAI) list or a network slice instance identifier (network slice instance identifier, NSI ID) list of an expected NF service producer instance, an NF set ID of the expected NF service producer instance, an S-NSSAI list of an NF service consumer, and the like.

[00283] Correspondingly, the claims in the access token generated by the NRF include an NF instance ID of the NRF, the NF instance ID of the NF service consumer, the NF type of the NF service producer, the expected service name, and validity time of the access token. Optionally, the claims may further include an additional range (for example, a requested resource and a requested operation for the resource), the S-NSSAI list or NSI ID list of the expected NF service producer instance, and the NF set ID of the expected NF service producer instance.

[00284] If the NF service consumer requests an access token of a type B, the requested access token is used to authorize access to a specific NF service producer instance or NF service producer service instance to obtain a service. The access token request message includes an NF instance ID of the NF service consumer, the expected service name, and a requested NF service producer instance ID(s).

[00285] Correspondingly, the claims in the access token generated by the NRF include an NF instance ID of the NRF, the NF instance ID of the NF service consumer, the NF instance ID(s) of the NF service producer, the expected service name, and validity time of the access token. Optionally, the claims may further include an additional range (for example, a requested resource and a requested operation for the resource).

[00286] In addition, generally, validity time of the CCA is shorter than the validity time of the access token.

[00287] Further, after the NRF generates the access token, the NRF performs integrity

protection on the access token, for example, performs integrity protection on the claims based on a key shared with the NF service producer, for example, generates a message authentication code (message authentication code, MAC) or signs the claims based on a private key of an NRF certificate.

[00288] When the producer (for example, the NF service producer) receives a service request message including an access token, the producer performs integrity verification, for example, verifies a MAC of the access token based on a key shared with the NRF or verifies a signature of the access token based on a public key of the NRF certificate. If the integrity verification succeeds, the claims in the access token are further verified.

[00289] For claims in the access token of the type A, the producer specifically verifies the following content:

[00290] (1) The producer verifies whether an NF type of a requested NF service producer in the claims matches the NF type of the producer.

[00291] (2) If the claims include the S-NSSAI list or NSI ID list of the expected NF service producer instance, the producer verifies whether the producer can serve a corresponding slice.

[00292] (3) If the claims include the NF set ID of the expected NF service producer instance, the producer verifies whether the NF set ID in the claims matches an NF set ID of the producer.

[00293] (4) If the claims include the expected service name, the producer verifies whether a service operation requested by the service request message is matched.

[00294] (5) If the claims include additional scope information, the producer verifies whether the additional scope information matches the service operation requested by the service request message.

[00295] (6) The producer verifies the validity time in the access token based on current data/time to check whether the access token expires, or the producer verifies the validity time in the access token based on current data/time to check whether the access token falls within a validity period.

[00296] For claims in the access token of the type B, the producer specifically verifies the following content:

[00297] (1) The producer verifies whether an NF instance ID(s) of a requested NF service producer in the claims includes an ID of the producer.

[00298] (2) If the claims include the expected service name, the producer verifies whether a service operation requested by the service request message is matched.

[00299] (3) If the claims include additional scope information, the producer verifies whether the additional scope information matches the service operation requested by the service request message.

[00300] (4) The producer verifies the validity time in the access token based on current data/time to check whether the access token expires, or the producer verifies the validity time in the access token based on current data/time to check whether the access token falls within a validity period.

[00301] The following further describes an indirect communication scenario with reference to the foregoing CCA and access token verification processes.

[00302] Scenario 1: Indirect procedure without delegated discovery (mode C)

[00303] An NF service consumer directly interacts with an NRF, as shown in FIG. 4.

[00304] Step 401: The NF service consumer determines that there is no information about an available NF service producer, and the NF service consumer initiates an NF service producer discovery (discovery) procedure.

[00305] The discovery procedure is used to discover the available NF service producer.

[00306] For example, if an access token of a type B is requested in step 402 and step 403, the discovery procedure needs to be initiated before step 402, and an identifier of a specific NF service producer instance or an identifier of an NF service producer service instance needs to be determined.

[00307] For example, if an access token of a type A is requested in step 402 and step 403, an NF service producer discovery procedure may be initiated before step 402 and step 403 (that is, step 401), or an NF service producer discovery procedure may be initiated after step 402 and step 403 (that is, step 404).

[00308] It may be understood that the NF service consumer needs to initiate only one NF service producer discovery procedure.

[00309] Step 402: The NF service consumer sends an access token request message (for example, Nnrf_AccessToken_Get_Request) to the NRF. It can be learned from the foregoing content that there are two types of access tokens. For different types of access tokens, specific content included in access token request messages is different. For details, refer to the foregoing related description of the access token.

[00310] Step 403: The NRF sends an access token response message (for example, Nnrf_AccessToken_Get_Response) to the NF service consumer, where the access token response message includes an access token generated by the NRF.

[00311] Specifically, the NRF receives the access token request message from the NF service consumer, and the NRF performs authorization check, to be specific, verifies whether the NF service consumer is authorized to obtain a requested service. If the authorization succeeds, the NRF generates the access token and performs integrity protection on the access token.

[00312] Step 404: The NF service consumer determines that there is no information about an

available producer (that is, step 401 is not performed), and the NF service consumer initiates a producer discovery procedure.

[00313] Step 404 is an optional step, and only one of step 401 and step 404 may be performed.

[00314] Step 405: The NF service consumer sends a service request message (for example, a Service Request) to an SCP, where the service request message includes an access token and a CCA.

[00315] The CCA is used by the NF service producer to authenticate the NF service consumer. Specifically, claims in the CCA include an NF instance ID of the NF service consumer, a timestamp, expiration time, and an NF type of an expected audience. According to a definition of the CCA, if a receiver of the service request message is an NF service producer, the NF type of the expected audience is an NF type of the NF service producer. For the CCA, refer to the foregoing related content. Details are not described herein again.

[00316] For example, when an AMF requests, through the SCP, an SMF to establish a session, the AMF sends a session establishment request message to the SCP, where the session establishment request message includes an access token and a CCA. In this case, the CCA includes an NF instance ID of the AMF, a timestamp, and expiration time, and the NF type of the expected audience is the SMF.

[00317] Step 406: The SCP sends a service request message to the NF service producer.

[00318] For example, the SCP performs application programming interface (Application Programming interface, API) modification, and sends the received service request message to the NF service producer.

[00319] If the service request message includes the identifier of the specific NF service producer instance or the identifier of the NF service producer service instance, the SCP sends the service request message to the specific NF service producer instance or the NF service producer service instance. If the service request message includes an NF set ID, the SCP may select an NF instance from the specific NF service producer instance and the NF service producer service instance and send the service request message to the NF instance.

[00320] Step 407: The NF service producer receives the service request message from the SCP. The NF service producer verifies the CCA and the access token.

[00321] The NF service producer performs integrity verification on the access token. If the integrity verification succeeds, the NF service producer further verifies claims in the access token. For details, refer to related content of verification on the claims in the access token. The NF service producer further needs to verify the NF service consumer based on the CCA. For a specific process of verifying the CCA, refer to the foregoing related description of CCA verification.

[00322] Step 408: If the NF service producer determines that the verification on the access token

and the CCA succeeds, the NF service producer sends a service response message (for example, a Service Response) to the SCP.

[00323] Step 409: The SCP sends a service response message to the NF service consumer.

[00324] For example, the SCP receives the service response message from the NF service producer, performs API modification, and sends a service response message to the NF service consumer.

[00325] Scenario 2: Indirect procedure without delegated discovery (mode C): An NF service consumer interacts with an NRF through an SCP, as shown in FIG. 5.

[00326] Step 501: An NF service consumer determines that there is no information about an available NF service producer, and the NF service consumer initiates an NF service producer discovery procedure.

[00327] The discovery procedure is used to discover the available NF service producer.

[00328] For example, if an access token of a type B is requested in step 502 and step 503, the discovery procedure needs to be initiated before step 502, and an identifier of a specific NF service producer instance or an identifier of an NF service producer service instance needs to be determined.

[00329] For example, if an access token of a type A is requested in step 502 and step 503, an NF service producer discovery procedure may be initiated before step 502 and step 503 (that is, step 501), or an NF service producer discovery procedure may be initiated after step 502 and step 503 (that is, step 504).

[00330] It may be understood that the NF service producer needs to initiate only one discovery procedure.

[00331] Step 502: The NF service consumer sends an access token request message to the SCP.

[00332] A specific parameter included in the access token request message may be determined based on a type of a requested access token. For details, refer to related descriptions of the access token. In addition, the access token request message may further include a CCA*, and the CCA* is used by the NRF to authenticate the NF service consumer. Specifically, claims in the CCA* include an NF instance ID of the NF service consumer, a timestamp, expiration time, and an NF type of an expected audience. According to a definition of the CCA, if a receiver of the access token request message is an NF service producer, the NF type of the expected audience is an NFR.

[00333] Step 503: The SCP sends, to the NRF, the access token request message received in step 502.

[00334] Step 504: The NRF determines that verification on the CCA* succeeds, and generates an access token.

[00335] Specifically, the NRF authenticates the NF service consumer based on the CCA*. If

the authentication succeeds, the NRF further performs authorization check. If the authorization succeeds, the NRF generates the access token and performs integrity protection on the access token.

[00336] Step 505: The NRF sends an access token response message to the SCP, where the access token response message includes the access token generated by the NRF.

[00337] Step 506: The SCP sends the access token response message to the NF service consumer, where the access token response message includes the access token generated by the NRF.

[00338] For specific content of step 507 to step 511, refer to step 505 to step 509 in the embodiment shown in FIG. 5.

[00339] Scenario 3: Communication authorization in a delegated discovery procedure (mode D): An NF service consumer interacts with an NRF through an SCP, as shown in FIG. 6.

[00340] Step 601: The NF service consumer sends a service request message to the SCP. The service request message includes a CCA and an access token. The CCA and the access token do not expire. Claims in the CCA include an NF instance ID of the NF service consumer, a timestamp, expiration time, and an NF type of an expected audience. According to a definition of the CCA, if a receiver of the service request message is an NF service producer, the NF type of the expected audience is an NF type of the NF service producer.

[00341] Step 602: The SCP sends the service request message to the NF service producer, where the service request message includes the CCA and the access token.

[00342] For specific content of step 603 to step 605, refer to step 509 to step 511 in the embodiment shown in FIG. 5.

[00343] Scenario 4: Communication authorization in a delegated discovery procedure (mode D): An NF service consumer interacts with an NRF through an SCP, as shown in FIG. 7.

[00344] Step 701: The NF service consumer sends a service request message to the SCP, where the service request message includes a CCA. Claims in the CCA include an NF instance ID of the NF service consumer, a timestamp, expiration time, and an NF type of an expected audience. If a receiver of the service request message is an NF service producer, the NF type of the expected audience is an NF type of the NF service producer.

[00345] Step 702: The SCP sends an access token request message to the NRF.

[00346] For example, the SCP may determine, based on the service request message, whether to initiate an access token request procedure to the NRF. For example, if the SCP determines that the received service request message does not include an access token and there is no access token corresponding to the service request message locally, the SCP sends the access token request message to the NRF.

[00347] The access token request message includes the CCA in step 701.

[00348] Step 703: The NRF determines that CCA verification fails.

[00349] The NF type of the expected audience in the CCA is the NF type of the NF service producer. Because the NF type in the CCA is inconsistent with an NF type of the NRF, the NRF determines that the CCA verification fails.

[00350] Step 704: The NRF sends an access token response message to the SCP, where the access token response message does not include an access token.

[00351] Therefore, the SCP fails to obtain the access token. As a result, the NF service consumer fails to request a service from the NF service producer.

[00352] In the indirect communication scenario based on the mode D, embodiments of this application provide the following embodiments, to resolve a problem that when an NF service consumer directly sends a service request message to an SCP to trigger the SCP to request another service, because a receiver (a producer of the another service) of a service request fails to authenticate the NF service consumer, the SCP fails to request the another service, and consequently the NF service consumer fails to request a service.

[00353] The following first describes technical concepts in embodiments of this application.

[00354] 1. Embodiments of this application relate to at least two network function types. A first network function type is different from a second network function type. A network function type is a general name of network functions that provide a group of function behavior or a group of services in a network. For example, a network function type in a 5G network may include an AMF type, an SMF type, or the like. A function network element of the AMF type may provide a service related to access and mobility management, and a function network element of the SMF type may provide a service related to PDU session management.

[00355] 2. Embodiments of this application further relate to at least two services. A first service is different from a second service, and the first service is associated with the second service.

[00356] For example, the first service may be a request for session establishment, and the second service may be a request for an access token corresponding to the first service. Alternatively, the first service may be a request for session establishment, and the second service may be a request for information about a network element providing the first service.

[00357] For example, in an indirect communication scenario based on a mode D, when an AMF requests an SMF to establish a session, the AMF sends a session establishment request message to an SCP. Before the SCP sends the session establishment request to the SMF, if the SCP needs to first obtain an access token (which is denoted as an access token 1 below) corresponding to the session establishment request from an NRF, after the SCP obtains the access token 1 from the NRF, the SCP sends the session establishment request message to the SMF. In this case, the session establishment request message includes the access token 1. The first service herein is the request for session establishment, the second service is the request for the access token corresponding to

the first service, and the SCP requests the access token corresponding to the first service from the NRF before the SCP sends the session establishment request message to the SMF, that is, the SCP requests the second service before requesting the first service. In addition, in some scenarios, the SCP may request the second service after requesting the first service. This is not limited in embodiments of this application. Unless otherwise specified, the following merely uses an example in which the SCP requests the second service before requesting the first service for description.

[00358] An association between the first service and the second service may be that, for example, requesting the first service may trigger requesting the second service.

[00359] In an example, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service represents/indicates that a service consumer network element has permission to obtain the first service. Because the service consumer network element requests the first service, and the access token, corresponding to the first service, provided by the second service represents/indicates that the service consumer network element has the permission to obtain the first service, the first service is associated with the second service. For example, that an NF service consumer requests the first service may trigger the SCP to request the access token corresponding to the first service. The access token corresponding to the first service represents/indicates that the NF service consumer has permission to obtain the first service or permission to access the first service.

[00360] In another example, the second service is used to provide information about a service producer network element. Because the service consumer network element requests the first service, and the service producer network element indicated by the information about the service producer network element provided by the second service may provide the first service, the first service is associated with the second service. For example, that an NF service consumer requests the first service may trigger the SCP to request information about an NF service producer. The NF service producer provides the first service for the NF service consumer.

[00361] In addition, requesting the first service may further trigger requesting a plurality of second services. For example, that the NF service consumer requests the first service may trigger the SCP to request the information about the NF service producer, and trigger the SCP to request the access token corresponding to the first service. The NF service producer provides the first service for the NF service consumer, and the access token corresponding to the first service represents/indicates that the service consumer network element has the permission to obtain the first service. Specifically, the SCP may request the access token corresponding to the first service from an NRF 1, and request the information about the NF service producer from the NRF 1. In this case, the NRF 1 provides two second services. Alternatively, the SCP may request the access

token corresponding to the first service from an NRF 1, and request the information about the NF service producer from an NRF 2. In this case, the NRF 1 is different from the NRF 2, and the second service provided by the NRF 1 is different from the second service provided by the NRF 2.

[00362] It may be understood that the first service and the second service are merely examples, and are not intended to limit embodiments of this application.

[00363] The following merely uses an example in which a network element providing the second service is a network repository function network element for description. The network element providing the second service may alternatively be network element of another type. This is not limited in embodiments of this application.

[00364] An embodiment of this application provides a communication method. A service consumer network element sends a service request message to a service communication proxy, where the service request message includes a first client credentials assertion, and the first client credentials assertion may include at least two different network function types, so that different network elements can successfully authenticate the service consumer network element based on the first client credentials assertion. The following uses the embodiment shown in FIG. 8 as an example for description.

[00365] Step 801: The service consumer network element sends a first service request message to the service communication proxy, where the first service request message is used to request a first service from a service producer network element, and the first service request message includes the first client credentials assertion.

[00366] The first client credentials assertion is used to authenticate the service consumer network element. The first client credentials assertion includes a first network function type and a second network function type. The first network function type is a network function type of a network element providing the first service, namely, a network function type of the service producer network element. The second network function type is a network function type of a network element providing a second service. The second service is associated with the first service. The network function type of the network element providing the second service may be a network function type of a network repository function network element.

[00367] Compared with an existing CCA, the first client credentials assertion includes two network function types. Therefore, the existing CCA is used only by a receiver of a service request to authenticate the service consumer network element, that is, authenticate an identity of the service consumer network element. In this embodiment of this application, the first client credentials assertion may be used by network elements of two network function types to authenticate the service consumer network element, to be specific, the receiver of the service

request and a receiver of a request message triggered by the service request authenticate the identity of the service consumer network element. In addition, the first client credentials assertion further includes one or more of an identifier of the service consumer network element and validity time information of the first client credentials assertion. The validity time information of the first client credentials assertion indicates validity time of the first client credentials assertion. For example, the validity time information of the first client credentials assertion may include a timestamp and expiration time of the first client credentials assertion. The content has a same meaning as a corresponding concept in the existing CCA, and details are not described herein again. For example, if the timestamp indicates a moment A, and the expiration time indicates a moment B, the first client credentials assertion is valid within a time period determined between the moment A and the moment B. Alternatively, the validity time information of the first client credentials assertion may include a timestamp and validity duration of the first client credentials assertion. The timestamp herein has a same meaning as a corresponding concept in the existing CCA, and the validity duration may be a time period after the timestamp. For example, if the timestamp indicates a moment A, and the validity duration indicates a time period C (for example, 5 minutes), the first client credentials assertion is valid within the time period C after the moment A.

[00368] The validity time information of the first client credentials assertion is associated with first duration, and the first duration is determined based on a transmission delay between the service consumer network element and the service communication proxy, a transmission delay between the service communication proxy and the network element providing the second service, and a transmission delay between the service communication proxy and the service producer network element (namely, the network element providing the first service).

[00369] For example, the transmission delay between the service consumer network element and the service communication proxy is denoted as T_1, the transmission delay between the service communication proxy and the network element providing the second service is denoted as T_2, and the transmission delay between the service communication proxy and the service producer network element is denoted as T_3. The foregoing transmission delay may be an average value of transmission delays between two network elements or may be slightly greater than an average value of transmission delays. If the service communication proxy requests the second service earlier than the first service, the first duration=$T_1+2T_2+T_3$. In this case, the validity duration of the first client credentials assertion may be a sum of the first duration and preset duration. Alternatively, the expiration time of the first client credentials assertion may be determined based on the timestamp, the first duration, and the preset duration. The preset duration herein may be preset or determined through dynamic adjustment. It should be noted that, if the preset duration is set to

excessively large duration, validity time of the CCA may be excessively long, and the CCA may be repeatedly used.

[00370] The foregoing configuration rule for the validity time information of the first client credentials assertion can ensure, as much as possible, that the first client credentials assertion is not maliciously used by the service communication proxy, to ensure security of a communication process.

[00371] It may be understood that, before the service consumer network element sends the first service request message to the service communication proxy, the service consumer network element further needs to determine whether an available first client credentials assertion is locally stored, and if the available client credentials assertion is stored (for example, an unexpired client credentials assertion is stored), the unexpired client credentials assertion is used as the first client credentials assertion. If the available client credentials assertion is not stored (for example, the client credentials assertion expires or no client credentials assertion is stored), the service consumer network element generates the first client credentials assertion. In addition, when there is an expired client credentials assertion, the service consumer network element may delete the expired client credentials assertion. Therefore, the service consumer network element may delete the expired client credentials assertion, to release storage space, and reduce storage load of a system.

[00372] The following describes several possible scenarios in which the service consumer network element is triggered to send the first service request message to the service communication proxy.

[00373] Scenario 1: When the first service needs to be requested and there is no available access token corresponding to the first service, the service consumer network element sends the first service request message to the service communication proxy.

[00374] For example, when the service consumer network element determines that the first service needs to be requested and there is no available access token corresponding to the first service, the service consumer network element sends the first service request message to the service communication proxy.

[00375] In some embodiments, that the service consumer network element determines that there is no available access token corresponding to the first service includes: The service consumer network element determines that an access token corresponding to the first service is not stored; or the service consumer network element determines that a stored access token corresponding to the first service expires. Further, when the stored access token corresponding to the first service expires, the service consumer network element may delete the expired access token corresponding to the first service.

[00376] For example, an access token may be stored in public storage space of an NF service consumer (for example, the access token is stored in a node-level context). The NF service consumer may receive a service request message of UE, and determine, based on the service request message, that the first service needs to be requested. The NF service consumer obtains related information of the UE (for example, context information of the UE) based on an identifier of the UE. Further, the NF service consumer checks whether the public storage space includes an access token corresponding to the first service. If the access token corresponding to the first service is included and the access token does not expire, the access token is used. If the access token corresponding to the first service is not included, it is determined that there is no available access token. Alternatively, if the access token corresponding to the first service is included but the access token expires, it is determined that there is no available access token. Further, optionally, the NF service consumer deletes the access token. The related information of the UE may be stored in the public storage space of the NF service consumer, or the related information of the UE is obtained by the NF service consumer from another network element based on the identifier of the UE.

[00377] It may be understood that, if the service consumer network element determines that there is the available access token corresponding to the first service, the first service request message sent by the service consumer network element to the service communication proxy may not include the second network function type, and include only the first network function type.

[00378] Scenario 2: When the first service needs to be requested and requesting of the first service triggers the service communication proxy to request information about the service producer network element, the service consumer network element sends the first service request message to the service communication proxy.

[00379] For example, when the service consumer network element determines that the first service needs to be requested and requesting of the first service triggers the service communication proxy to request the information about the service producer network element, the service consumer network element sends the first service request message to the service communication proxy.

[00380] When one or more of the following cases occur, the service consumer network element may determine that requesting of the first service triggers the service communication proxy to request the information about the service producer network element. For example, the service consumer network element receives a first message associated with a first terminal device, and the service consumer network element determines, based on the first message, that the first service needs to be requested. Further, the service consumer network element determines, based on one or more of the following cases, requesting of the first service triggers the service communication proxy to request the information of the service producer network element.

[00381] Case 1: Context of the first terminal device is not stored.

[00382] For example, an NF service consumer may receive a service request message of UE, and determine, based on the service request message, that the first service needs to be requested. The NF service consumer obtains context information of the UE based on an identifier of the UE. If the context information of the UE is not obtained, that is, the UE is new UE, and has not triggered the NF service consumer to request a service from an NF service producer, the NF service consumer determines that requesting of the first service triggers the SCP to request information about the NF service producer. The context information of the UE may be stored in the NF service consumer, or the context information of the UE is obtained by the NF service consumer from another network element based on the identifier of the UE.

[00383] Case 2: Context of the first service is not stored.

[00384] For example, an NF service consumer may receive a service request message of UE, and determine, based on the service request message, that the first service needs to be requested. The NF service consumer obtains context information of the UE based on an identifier of the UE. If it is determined, based on the context information of the UE, that the context of the first service is not included, that is, the UE has not triggered the NF service consumer to request the first service from an NF service producer, the NF service consumer determines that requesting of the first service triggers the SCP to request information about the NF service producer. The context information of the UE may be stored in the NF service consumer, or the context information of the UE is obtained by the NF service consumer from another network element based on the identifier of the UE.

[00385] Case 3: A first slice belongs to the service producer network element and context of the first slice is not stored.

[00386] For example, an NF service consumer may receive a service request message of the UE, and determine, based on the service request message, that the first service needs to be requested and the first service needs to be requested from the service producer network element in the first slice. The NF service consumer obtains context information of the UE based on an identifier of the UE. If it is determined, based on the context information of the UE, that the context of the first slice is not included, that is, the UE has not triggered the NF service consumer to request the first service from an NF service producer in the first slice, the NF service consumer determines that requesting of the first service triggers the SCP to request information about the NF service producer. The context information of the UE may be stored in the NF service consumer, or the context information of the UE is obtained by the NF service consumer from another network element based on the identifier of the UE.

[00387] Case 4: The service consumer network element communicates with the service communication proxy for the first time.

[00388] It may be understood that the service consumer network element may request a service from the service producer network element through a plurality of service communication proxies. If the service consumer network element determines to send the first service request message to a new service communication proxy, that is, the service consumer network element communicates with the service communication proxy for the first time, the service consumer network element determines that the first service request message triggers the service communication proxy to request the second service.

[00389] In addition, the NF service consumer receives a service request response message, where the message includes a binding indication, and the binding indication is used in a subsequent related service message. In this scenario, when the NF service consumer requests the first service, the first service request message carries binding information, and the binding information may be used by the SCP to route the first service request message to a specific NF service producer. In this case, the SCP does not need to initiate an NF service producer discovery procedure.

[00390] Scenario 3: When the first service needs to be requested and the service consumer network element communicates with the service communication proxy in an indirect communication mode, namely, a mode D, the service consumer network element sends the first service request message to the service communication proxy.

[00391] For example, it may be agreed on in a standard protocol or configured based on preconfiguration information that, when the service consumer network element communicates with the service communication proxy in the mode D, the first service request message always carries the client credentials assertion including the first network function type and the second network function type.

[00392] Scenario 4: Before the service consumer network element sends the first service request message to the service communication proxy, the service consumer network element obtains indication information, and the service consumer network element sends the first service request message to the service communication proxy based on the indication information.

[00393] As shown in FIG. 9, the following describes a specific process in which the service consumer network element sends the first service request message to the service communication proxy based on the indication information in the scenario 4 in step 801 in FIG. 8.

[00394] Step 901: Before the service consumer network element sends the first service request message to the service communication proxy, the service consumer network element sends a second service request message to the service communication proxy, where the second service request message is used to request the first service, the second service request message includes a second client credentials assertion, the second client credentials assertion includes the first network function type, and the second client credentials assertion is used by the service producer network

element to authenticate the service consumer network element.

[00395] It should be noted that, in this case, the second client credentials assertion does not include the second network function type.

[00396] Step 902: The service communication proxy sends a third service request message to the network repository function network element, where the third service request message is used to request the second service, and the third service request message includes a second client credentials assertion. The network repository function network element is configured to provide the second service.

[00397] That the service communication proxy determines that requesting of the first service triggers requesting of the second service may include but is not limited to the following scenarios:

[00398] Scenario A: When an available access token corresponding to the first service is not stored and the second service request message does not include an access token corresponding to the first service, the service communication proxy sends the third service request message to the network repository function network element, where the third service request message is used to request the access token corresponding to the first service. The service communication proxy determines that the available access token corresponding to the first service is not stored and the second service request message does not include the access token corresponding to the first service, and the service communication proxy sends the third service request message to the network repository function network element.

[00399] For example, the service communication proxy may determine, based on the received second service request message, that the access token corresponding to the first service is required. For example, the service communication proxy may determine, based on a type of the service request message or an access scope of a service request, that the access token corresponding to the first service is required. Further, the service communication proxy queries whether the access token corresponding to the first service is stored. If the access token corresponding to the first service is not stored or a stored access token corresponding to the first service expires, and the second service request message does not include the access token, a parameter required for requesting the access token corresponding to the first service, namely, a parameter in the claim, for example, an expected service name or an NF instance ID of a consumer, may be determined based on the type of the service request message. In addition, when the stored access token corresponding to the first service expires, the service communication proxy may delete the expired access token.

[00400] Scenario B: When information about an available service producer network element is not stored and the second service request message does not include information about the service producer network element, the service communication proxy sends the third service request

message to the network repository function network element, where the third service request message is used to request the information about the service producer network element. The service communication proxy determines that the information about the available service producer network element is not stored and the second service request message does not include the information about the service producer network element; and sends the third service request message to the network repository function network element. For example, the service communication proxy may be determined based on a type of the second service request message and/or indication information in the second service request message.

[00401] After the service communication proxy receives the second service request message, the service communication proxy parses the second service request message, to determine who is a receiver of the message and whether the receiver of the message (namely, the service producer network element) needs to be discovered. That the service communication proxy determines whether the service producer network element needs to be discovered is logically similar to that the service consumer network element in direct communication determines whether a service producer needs to be discovered. For example, if a request message received by the SCP is a session establishment request, the SCP determines that the message needs to be forwarded to an SMF, and the SCP determines, based on a parameter in the message, whether SMF instance information meeting a condition exists locally.

[00402] Step 903: The network repository function network element determines, based on the second client credentials assertion, that the authentication on the service consumer network element fails.

[00403] For example, that the network repository function network element determines, based on the second client credentials assertion, that the authentication on the service consumer network element fails includes: The network repository function network element determines that the first network function type does not match the network function type of the network repository function network element.

[00404] Alternatively, that the network repository function network element determines, based on the second client credentials assertion, that the authentication on the service consumer network element fails includes: The network repository function network element verifies that a signature of the second client credentials assertion succeeds, verifies, based on a timestamp included in the second client credentials assertion and/or expiration time of the second client credentials assertion, that the second client credentials assertion does not expire, verifies that an identifier of the service consumer network element in the second client credentials assertion is the same as an identifier of a network element in a certificate for signing the second client credentials assertion, and verifies that the first network function type does not match the network function type of the network

repository function network element.

[00405] Step 904: When the first network function type does not match the network function type of the network repository function network element, the network repository function network element sends a response message for the third service request message to the service communication proxy. The response message for the third service request message includes a cause value and/or first indication information.

[00406] The cause value and/or the first indication information indicates/indicate that the second client credentials assertion does not include the second network function type, indicates/indicate that the first network function type included in the second client credentials assertion does not match the network function type of the network repository function network element, or indicates/indicate that the second client credentials assertion does not include a correct network function type.

[00407] Optionally, the first indication information may be a third client credentials assertion. The third client credentials assertion includes an identifier of the network repository function network element, a timestamp of the third client credentials assertion, expiration time of the third client credentials assertion, and a network function type of the service consumer network element. Optionally, the third client credentials assertion may further include the network function type of the network repository function network element, to indicate the service consumer network element to generate a client credentials assertion including the network function type of the network repository function network element.

[00408] It can be learned from step 903 that the network repository function network element fails to authenticate the service consumer network element, the response message for the third service request message may further indicate that a second service request fails.

[00409] Step 905: The service communication proxy sends, based on the response message for the third service request message, a response message for the second service request message to the service consumer network element, where the response message for the second service request message includes second indication information.

[00410] The second indication information is used to trigger the service consumer network element to send the first service request message (namely, a service request message that carries both the network function type of the service producer network element and the network function type of the network repository function network element) in step 801 of the embodiment in FIG. 8.

[00411] In a possible implementation, the second indication information indicates that the second client credentials assertion does not include the network function type of the network repository function network element (namely, the second network function type), indicates that the

first network function type included in the second client credentials assertion does not match the network function type of the network repository function network element, or indicates that the second client credentials assertion does not include the correct network function type.

[00412] In specific implementation, the second indication information may be the same as the first indication information, or may be information obtained by processing the first indication information by the service communication proxy. This is not limited in embodiments of this application.

[00413] In some embodiments, the service communication proxy may further generate the second indication information based on the response message for the third service request message. The second indication information may be used to trigger the service consumer network element to re-initiate a service request message for requesting the first service and carry, when the first service is requested again, a client credentials assertion including the network function type of the network repository function network element and the network function type of the service producer network element (that is, perform step 801).

[00414] Step 906: The service consumer network element sends the first service request message to the service communication proxy based on the second indication information.

[00415] In some embodiments, when the second indication information includes the third client credentials assertion and the third client credentials assertion includes the network function type of the network repository function network element, the service consumer network element may authenticate the network repository function network element based on the third client credentials assertion. When the authentication on the network repository function network element succeeds, the service consumer network element sends the first service request message to the service communication proxy, and the service consumer network element determines that the second network function type is the network function type of the network repository function network element (the network repository function network element is configured to provide the second service, and the network function type of the network repository function network element is the network function type of the network element providing the second service).

[00416] Step 802: The service communication proxy receives the first service request message from the service consumer network element, and the service communication proxy sends a fourth service request message to the network repository function network element, where the fourth service request message is used to request the second service, and the fourth service request message includes the first client credentials assertion.

[00417] For the service communication proxy determining that requesting of the first service triggers requesting of the second service, refer to the foregoing step 902. Details are not repeated.

[00418] Step 803: The network repository function network element receives the fourth service

request message from the service communication proxy, and the network repository function network element authenticates the service consumer network element based on the first client credentials assertion.

[00419] If the network repository function network element determines that a network function type the same as the network function type of the network repository function network element exists in the first network function type and the second network function type, the network repository function network element determines that the authentication on the service consumer network element succeeds. The second network function type is the same as the network function type of the network repository function network element.

[00420] Specifically, if the network repository function network element verifies that a signature of the first client credentials assertion succeeds, verifies, based on the timestamp and/or the expiration time of the first client credentials assertion included in the first client credentials assertion, that the first client credentials assertion does not expire, verifies that the identifier of the service consumer network element in the first client credentials assertion is the same as an identifier of a network element in a certificate for signing the first client credentials assertion, and verifies that the second network function type in the first network function type and the second network function type matches the network function type of the network repository function network element, the network repository function network element determines that the authentication on the service consumer network element succeeds.

[00421] Step 804: When the authentication on the service consumer network element succeeds, the network repository function network element sends a response message for the fourth service request message to the service communication proxy.

[00422] For example, if the fourth service request message is used to request the access token corresponding to the first service, after the authentication on the service consumer network element succeeds, the network repository function network element performs authorization check. If it is determined that the authorization succeeds, the network repository function network element generates the access token corresponding to the first service. The network repository function network element sends the response message for the fourth service request message to the service communication proxy. The response message for the fourth service request message includes the access token corresponding to the first service.

[00423] For example, if the fourth service request message is used to request the information about the service producer network element, after the authentication on the service consumer network element succeeds, the network repository function network element sends the response message for the fourth service request message to the service communication proxy. The response message for the fourth service request message includes the information about the service producer

network element.

[00424] Step 805: The service communication proxy receives the response message for the fourth service request message from the network repository function network element, and the service communication proxy sends, based on the response message for the fourth service request message, a fifth service request message to the service producer network element, where the fifth service request message is used to request the first service, and the fifth service request message includes the first client credentials assertion.

[00425] It may be understood that the fifth service request message further includes the access token corresponding to the first service.

[00426] For example, when the response message for the fourth service request message includes the access token corresponding to the first service, the service communication proxy sends the fifth service request message to the service producer network element, where the fifth service request message is used to request the first service, and the fifth service request message includes the first client credentials assertion and the access token corresponding to the first service.

[00427] For example, when the response message for the fourth service request message includes the information about the service producer network element, the service communication proxy sends the fifth service request message to the service producer network element indicated by the information about the service producer network element, where the fifth service request message is used to request the first service, and the fifth service request message includes the first client credentials assertion and the access token corresponding to the first service. In this case, the access token corresponding to the first service may be stored by the service communication proxy or carried in the first request message.

[00428] In another implementation, the service communication proxy requests, from the network repository function network element based on the first client credentials assertion, the access token corresponding to the first service and the information about the service producer network element. That is, step 802 to step 804 are performed twice, so that the service communication proxy may initiate a service request message for the second service twice, to respectively request the access token corresponding to the first service and the information about the service producer network element. In this case, the access token corresponding to the first service in step 805 may be obtained by the service communication proxy from the network repository function network element in step 802 to step 804.

[00429] Step 806: The service producer network element receives the fifth service request message from the service communication proxy, and the service producer network element authenticates the service consumer network element based on the first client credentials assertion.

[00430] It may be understood that the service producer network element further needs to verify

the access token corresponding to the first service. For details, refer to the foregoing verification process of the access token. Details are not described herein again.

[00431] That the service producer network element authenticates the service consumer network element based on the first client credentials assertion includes: The service producer network element determines whether the network function type of the service producer network element matches one or more of the first network function type and the second network function type.

[00432] Specifically, that the service producer network element authenticates the service consumer network element based on the first client credentials assertion further includes: The service producer network element verifies whether the signature of the first client credentials assertion succeeds, verifies, based on the timestamp and/or the expiration time of the first client credentials assertion included in the first client credentials assertion, whether the first client credentials assertion does not expire, and verifies whether the identifier of the service consumer network element in the first client credentials assertion is the same as the identifier of the network element in the certificate for signing the first client credentials assertion.

[00433] The network repository function network element and the service producer network element authenticate, based on the first client credentials assertion, the service consumer network element based on a same authentication idea. For corresponding content, refer to each other. Details are not described again.

[00434] Step 807: When the authentication on the service consumer network element succeeds, the service producer network element sends a response message for the fifth service request message to the service communication proxy.

[00435] For example, when the authentication on the service consumer network element succeeds and the verification on the access token corresponding to the first service succeeds, the response message for the fifth service request message indicates to provide the first service or indicates that a fifth service request succeeds. Alternatively, when the authentication on the service consumer network element fails and/or verification on the access token corresponding to the first service fails, the response message for the fifth service request message indicates that requesting of the first service fails.

[00436] Step 808: The service communication proxy sends a response message for the first service request message to the service consumer network element.

[00437] When the response message for the fifth service request message indicates to provide the first service or indicates that the fifth service request succeeds, the response message for the first service request message indicates to provide the first service or indicates that a first service request succeeds. Alternatively, when the response message for the fifth service request message indicates that a first service request fails, the response message for the first service request message

indicates that the first service request fails. For example, the service communication proxy may modify information in a message header of the response message for the fifth service request message, but content of the response message for the fifth service request message basically remains unchanged. The service communication proxy is mainly used for message routing.

[00438] In the foregoing embodiment, when the service consumer network element requests the first service from the service producer network element through the service communication proxy, the service consumer network element carries, in the first service request message sent to the service communication proxy, a client credentials assertion including the first network function type and the second network function type. This can ensure that when the service communication proxy requests the second service, the network element providing the second service successfully authenticates the service consumer network element, further ensures that the service consumer network element requests the first service, and resolves a problem, in an indirect communication scenario, that the service consumer network element fails to request the service because the authentication based on the client credentials assertion fails.

[00439] An embodiment of this application provides a communication method. A service consumer network element sends a service request message to a service communication proxy, where the service request message includes a fourth client credentials assertion and a fifth client credentials assertion, and the fourth client credentials assertion and the fifth client credentials assertion respectively include different network function types. The service communication proxy sends corresponding client credentials assertions to different network elements, so that the different network elements can authenticate the service consumer network element based on the different client credentials assertions. The following uses the embodiment shown in FIG. 10 as an example for description.

[00440] This embodiment of this application provides the communication method. As shown in FIG. 10, the method includes the following steps.

[00441] Step 1001: The service consumer network element sends a first service request message to the service communication proxy, where the first service request message is used to request a first service, and the first service request message includes the fourth client credentials assertion and the fifth client credentials assertion.

[00442] The fourth client credentials assertion is used by a service producer network element to authenticate the service consumer network element, and the fifth client credentials assertion is used by a network element providing a second service, to authenticate the service consumer network element. The fourth client credentials assertion includes a first network function type, and the fifth client credentials assertion includes a second network function type. The first network function type is a network function type of the service producer network element, the second

network function type is a network function type of the network element providing the second service, and the second service is associated with the first service.

[00443] The fourth client credentials assertion further includes one or more of an identifier of the service consumer network element and validity time information of the fourth client credentials assertion. The validity time information of the fourth client credentials assertion indicates expiration time of the fourth client credentials assertion. For example, the validity time information of the fourth client credentials assertion includes a timestamp and the expiration time of the fourth client credentials assertion. Alternatively, the validity time information of the fourth client credentials assertion may include a timestamp of the fourth client credentials assertion and validity duration of the fourth client credentials assertion. The fifth client credentials assertion further includes one or more of the identifier of the service consumer network element and validity time information of the fifth client credentials assertion. The validity time information of the fifth client credentials assertion indicates validity time of the fifth client credentials assertion. For example, the validity time information of the fifth client credentials assertion includes a timestamp of the fifth client credentials assertion and expiration time of the fifth client credentials assertion. Alternatively, the validity time information of the fifth client credentials assertion may include a timestamp of the fifth client credentials assertion and validity duration of the fifth client credentials assertion.

[00444] When the service communication proxy requests the second service earlier than the first service, the validity time of the fifth client credentials assertion is shorter than the validity time of the fourth client credentials assertion. For example, when the service communication proxy requests the second service earlier than the first service, the validity time of the fifth client credentials assertion is associated with first duration. The first duration is determined based on a transmission delay between the service consumer network element and the service communication proxy and a transmission delay between the service communication proxy and the network element providing the second service. For example, the transmission delay between the service consumer network element and the service communication proxy is denoted as T_1, and the transmission delay between the service communication proxy and the network element providing the second service is denoted as T_2. The foregoing transmission delay may be an average value of transmission delays or may be slightly greater than an average value of transmission delays. First duration=T_1+T_2. For example, the expiration time of the first client credentials assertion may be determined based on a timestamp, the first duration, and preset duration. The preset duration herein may be determined based on an empirical value.

[00445] When the service communication proxy requests the second service later than the first service, the validity time of the fifth client credentials assertion is longer than the validity time of

the fourth client credentials assertion.

[00446] The foregoing configuration rules for the validity time of the fourth client credentials assertion and the validity time of the fifth client credentials assertion can ensure, as much as possible, that the fourth client credentials assertion and the fifth client credentials assertion are not maliciously used by the service communication proxy, to ensure security of a communication process.

[00447] It may be understood that before the service consumer network element sends the first service request message to the service communication proxy, the service consumer network element further needs to determine whether an available client credentials assertion is locally stored, and if the available client credentials assertion is stored (for example, an unexpired client credentials assertion is stored), the available client credentials assertion is used as the fourth client credentials assertion. If the available client credentials assertion is not stored (for example, a stored client credentials assertion expires or no client credentials assertion is stored), the service consumer network element generates the fourth client credentials assertion. In addition, when there is an expired client credentials assertion, the service consumer network element may delete the expired client credentials assertion. Therefore, the service consumer network element may delete the expired client credentials assertion, to release storage space, and reduce storage load of a system. Similarly, this is applicable to the fifth client credentials assertion. Details are not described herein again.

[00448] The network function type of the network element providing the second service may be a network function type of a network repository function network element.

[00449] For several scenarios in which the service consumer network element is triggered to send the first service request message to the service communication proxy, refer to related content in the embodiment shown in FIG. 8. Details are not described again.

[00450] Step 1002: The service communication proxy receives the first service request message from the service consumer network element, and the service communication proxy sends a second service request message to the network repository function network element, where the second service request message is used to request the second service, and the second service request message includes the fifth client credentials assertion.

[00451] For the service communication proxy determining that requesting of the first service triggers requesting of the second service, refer to the foregoing step 902. Details are not repeated.

[00452] After the service communication proxy determines that requesting of the first service triggers requesting of the second service, the service communication proxy sends the second service request message to the network repository function network element based on the network function type of the network repository function network element, where the second service

request message includes the fifth client credentials assertion.

[00453] For example, the service communication proxy determines that an access token corresponding to the first service needs to be requested from the network repository function network element, selects the fifth client credentials assertion from the fourth client credentials assertion and the fifth client credentials assertion based on the network function type of the network repository function network element, and adds the fifth client credentials assertion to the second service request message. Alternatively, the service communication proxy determines that information about the service producer network element needs to be requested from the network repository function network element, selects the fifth client credentials assertion from the fourth client credentials assertion and the fifth client credentials assertion based on the network function type of the network repository function network element, and adds the fifth client credentials assertion to the second service request message.

[00454] Step 1003: The network repository function network element receives the second service request message from the service communication proxy, and the network repository function network element authenticates the service consumer network element based on the fifth client credentials assertion.

[00455] The network repository function network element determines that the authentication on the service consumer network element succeeds. Specifically, if the network repository function network element verifies that a signature of the fifth client credentials assertion succeeds, verifies, based on the timestamp and/or the expiration time of the fifth client credentials assertion included in the fifth client credentials assertion, that the fifth client credentials assertion does not expire, verifies that the identifier of the service consumer network element in the fifth client credentials assertion is the same as an identifier of a network element in a certificate for signing the fifth client credentials assertion, and verifies that the second network function type matches the network function type of the network repository function network element, the network repository function network element determines that the authentication on the service consumer network element succeeds.

[00456] Step 1004: The network repository function network element sends a response message for the second service request message to the service communication proxy.

[00457] For example, if the second service request message is used to request the access token corresponding to the first service, after the authentication on the service consumer network element succeeds, the network repository function network element performs authorization check. If it is determined that the authorization succeeds, the network repository function network element generates the access token corresponding to the first service. The network repository function network element sends the response message for the second service request message to the service

communication proxy. The response message for the second service request message includes the access token corresponding to the first service.

[00458] For example, if the second service request message is used to request the information about the service producer network element, after the authentication on the service consumer network element succeeds, the network repository function network element sends the response message for the second service request message to the service communication proxy. The response message for the second service request message includes the information about the service producer network element.

[00459] Optionally, when the authentication on the service consumer network element fails, the network repository function network element sends the response message for the second service request message to the service communication proxy, to indicate that requesting of the second service fails.

[00460] Step 1005: The service communication proxy receives the response message for the second service request message from the network repository function network element, and the service communication proxy sends, based on the response message for the second service request message, a third service request message to the service producer network element, where the third service request message is used to request the first service, and the third service request message includes the fourth client credentials assertion.

[00461] It may be understood that the third service request message further includes the access token corresponding to the first service.

[00462] For example, the service communication proxy determines that the service consumer network element requests the first service, selects the fourth client credentials assertion from the fourth client credentials assertion and the fifth client credentials assertion based on the network function type of the service producer network element, and adds the fourth client credentials assertion to the third service request message.

[00463] For example, when the response message for the second service request message includes the access token corresponding to the first service, the service communication proxy sends the third service request message to the service producer network element, where the third service request message is used to request the first service, and the third service request message includes the fourth client credentials assertion and the access token corresponding to the first service. Alternatively, when the response message for the second service request message includes the information about the service producer network element, the service communication proxy sends the third service request message to the service producer network element indicated by the information about the service producer network element, where the third service request message is used to request the first service, and the third service request message includes the fourth client

credentials assertion and the access token corresponding to the first service. In this case, the access token corresponding to the first service may be stored by the service communication proxy or carried in the first service request message.

[00464] Step 1006: The service producer network element receives the third service request message from the service communication proxy, and the service producer network element authenticates the service consumer network element based on the fourth client credentials assertion.

[00465] It may be understood that the service producer network element further needs to verify the access token corresponding to the first service. For details, refer to the foregoing verification process of the access token. Details are not described herein again.

[00466] The service producer network element determines that the authentication on the service consumer network element succeeds. Specifically, if the service producer network element verifies that a signature of the fourth client credentials assertion succeeds, verifies, based on the timestamp and/or the expiration time of the fourth client credentials assertion included in the fourth client credentials assertion, that the fourth client credentials assertion does not expire, verifies that the identifier of the service consumer network element in the fourth client credentials assertion is the same as an identifier of a network element in a certificate for signing the fourth client credentials assertion, and verifies that the first network function type matches the network function type of the service producer network element, the service producer network element determines that the authentication on the service consumer network element succeeds.

[00467] Step 1007: The service producer network element sends a response message for the third service request message to the service communication proxy.

[00468] When the authentication on the service consumer network element succeeds and the verification on the access token corresponding to the first service succeeds, the response message for the third service request message indicates to provide the first service or indicates that a third service request succeeds. Alternatively, when the authentication on the service consumer network element fails and/or verification on the access token corresponding to the first service fails, the response message for the third service request message indicates that a first service request fails.

[00469] Step 1008: The service communication proxy sends a response message for the first service request message to the service consumer network element.

[00470] When the response message for the third service request message indicates to provide the first service or indicates that the third service request succeeds, the response message for the first service request message indicates to provide the first service or indicates that a first service request succeeds. Alternatively, when the response message for the third service request message indicates that the first service request fails, the response message for the first service request message indicates that the first service request fails. For example, the service communication

proxy may modify information in a message header of the response message for the third service request message, but content of the response message for the third service request message basically remains unchanged. The service communication proxy is mainly used for message routing.

[00471] In the foregoing embodiment, the service consumer network element sends the first service request message to the service communication proxy, where the first service request message includes the fourth client credentials assertion and the fifth client credentials assertion, the fourth client credentials assertion includes the first network function type, and the fifth client credentials assertion includes the second network function type. This can ensure that when the service communication proxy requests the second service, the network element providing the second service successfully authenticates the service consumer network element, and further ensure that the service consumer network element requests the first service.

[00472] An embodiment of this application provides a communication method. A service consumer network element sends a service request message to a service communication proxy, where the service request message includes a fourth client credentials assertion and a fifth client credentials assertion, and the fourth client credentials assertion and the fifth client credentials assertion respectively include different network function types. When receiving the fourth client credentials assertion and the fifth client credentials assertion, a network repository function network element (or a service producer network element) determines, based on the fourth client credentials assertion, that authentication on the service consumer network element succeeds, or determines, based on the fifth client credentials assertion, that authentication on the service consumer network element succeeds. It can be determined that the authentication on the service consumer network element succeeds. The following uses the embodiment shown in FIG. 11 as an example for description.

[00473] This embodiment of this application provides the communication method. As shown in FIG. 11, the method includes the following steps.

[00474] Step 1101: The service consumer network element sends a first service request message to the service communication proxy, where the first service request message is used to request a first service, and the first service request message includes the fourth client credentials assertion and the fifth client credentials assertion.

[00475] For details, refer to step 1001 in FIG. 10. Details are not described again.

[00476] Step 1102: The service communication proxy receives the first service request message from the service consumer network element, and the service communication proxy sends a second service request message to the network repository function network element, where the second service request message is used to request a second service, and the second service request message

includes the fourth client credentials assertion and the fifth client credentials assertion.

[00477] For the service communication proxy determining that requesting of the first service triggers requesting of the second service, refer to the foregoing step 902. Details are not repeated.

[00478] Step 1103: The network repository function network element receives the second service request message from the service communication proxy, and the network repository function network element authenticates the service consumer network element based on the fourth client credentials assertion and the fifth client credentials assertion.

[00479] If the network repository function network element successfully authenticates the service consumer network element based on one or more of the fourth client credentials assertion and the fifth client credentials assertion, the network repository function network element determines that the authentication on the service consumer network element succeeds.

[00480] The network repository function network element determines, based on the fifth client credentials assertion, that the authentication on the service consumer network element succeeds. Specifically, if the network repository function network element verifies that a signature of the fifth client credentials assertion succeeds, verifies, based on a timestamp and/or expiration time of the fifth client credentials assertion included in the fifth client credentials assertion, that the fifth client credentials assertion does not expire, verifies that an identifier of the service consumer network element in the fifth client credentials assertion is the same as an identifier of a network element in a certificate for signing the fifth client credentials assertion, and verifies that a second network function type matches a network function type of the network repository function network element, the network repository function network element determines that the authentication on the service consumer network element succeeds.

[00481] The network repository function network element determines, based on the fourth client credentials assertion, that the authentication on the service consumer network element fails. Specifically, if the network repository function network element verifies that a signature of the fourth client credentials assertion succeeds, verifies, based on a timestamp and/or expiration time of the fourth client credentials assertion included in the fourth client credentials assertion, that the fourth client credentials assertion does not expire, verifies that an identifier of a service consumer network element in the fourth client credentials assertion is the same as an identifier of a network element in a certificate for signing the fourth client credentials assertion, and verifies that a first network function type does not match the network function type of the network repository function network element, the network repository function network element determines that the authentication on the service consumer network element fails.

[00482] It can be learned from the foregoing that if the network repository function network element successfully authenticates the service consumer network element based on the fifth client

credentials assertion, and fails to authenticate the service consumer network element based on the fourth client credentials assertion, the network repository function network element determines that the authentication on the service consumer network element succeeds.

[00483] Step 1104: When the authentication on the service consumer network element succeeds, the network repository function network element sends a response message for the second service request message to the service communication proxy.

[00484] For example, if the second service request message is used to request an access token corresponding to the first service, after the authentication on the service consumer network element succeeds, the network repository function network element performs authorization check. If it is determined that the authorization succeeds, the network repository function network element generates the access token corresponding to the first service. The network repository function network element sends the response message for the second service request message to the service communication proxy. The response message for the second service request message includes the access token corresponding to the first service.

[00485] For example, if the second service request message is used to request information about the service producer network element, after the authentication on the service consumer network element succeeds, the network repository function network element sends the response message for the second service request message to the service communication proxy. The response message for the second service request message includes the information about the service producer network element.

[00486] Step 1105: The service communication proxy receives the response message for the second service request message from the network repository function network element, and the service communication proxy sends, based on the response message for the second service request message, a third service request message to the service producer network element, where the third service request message is used to request the first service, and the third service request message includes the fourth client credentials assertion and the fifth client credentials assertion.

[00487] It may be understood that the third service request message further includes the access token corresponding to the first service.

[00488] For example, when the response message for the second service request message includes the access token corresponding to the first service, the service communication proxy sends the third service request message to the service producer network element, where the third service request message is used to request the first service, and the third service request message includes the fourth client credentials assertion and the access token corresponding to the first service.

[00489] For example, when the response message for the second service request message

includes the information about the service producer network element, the service communication proxy sends the third service request message to the service producer network element indicated by the information about the service producer network element, where the third service request message is used to request the first service, and the third service request message includes the fourth client credentials assertion and the access token corresponding to the first service. In this case, the access token corresponding to the first service may be stored by the service communication proxy or carried in the first service request message.

[00490] Step 1106: The service producer network element receives the third service request message from the service communication proxy, and the service producer network element verifies the fourth client credentials assertion and the fifth client credentials assertion.

[00491] It may be understood that the service producer network element further needs to verify the access token corresponding to the first service. For details, refer to the foregoing verification process of the access token. Details are not described herein again.

[00492] If the service producer network element successfully authenticates the service consumer network element based on one or more of the fourth client credentials assertion and the fifth client credentials assertion, the service producer network element determines that the authentication on the service consumer network element succeeds.

[00493] The service producer network element determines, based on the fourth client credentials assertion, that the authentication on the service consumer network element succeeds. Specifically, if the service producer network element verifies that the signature of the fourth client credentials assertion succeeds, verifies, based on the timestamp and/or the expiration time of the fourth client credentials assertion included in the fourth client credentials assertion, that the fourth client credentials assertion does not expire, verifies that the identifier of the service consumer network element in the fourth client credentials assertion is the same as the identifier of the network element in the certificate for signing the fourth client credentials assertion, and verifies that the first network function type matches the network function type of the service producer network element, the service producer network element determines that the authentication on the service consumer network element succeeds.

[00494] The service producer network element determines, based on the fifth client credentials assertion, that the authentication on the service consumer network element fails. Specifically, if the service producer network element verifies that the signature of the fifth client credentials assertion succeeds, verifies, based on the timestamp and/or the expiration time of the fifth client credentials assertion included in the fifth client credentials assertion, that the fifth client credentials assertion does not expire, verifies that the identifier of the service consumer network element in the fifth client credentials assertion is the same as the identifier of the network element in the

certificate for signing the fifth client credentials assertion, and verifies that the second network function type does not match the network function type of the service producer network element, the service producer network element determines that the authentication on the service consumer network element fails.

[00495] It can be learned from the foregoing that if the service producer network element successfully authenticates the service consumer network element based on the fourth client credentials assertion, and fails to authenticate the service consumer network element based on the fifth client credentials assertion, the service producer network element determines that the authentication on the service consumer network element succeeds.

[00496] Step 1107: The service producer network element sends a response message for the third service request message to the service communication proxy.

[00497] Step 1108: The service communication proxy sends a response message for the first service request message to the service consumer network element.

[00498] Step 1107 and step 1108 are respectively the same as step 1007 and step 1008 in the embodiment in FIG. 10. Details are not described again.

[00499] Compared with the embodiment in FIG. 10, in the embodiment in FIG. 11, the service communication proxy does not need to carry different CCAs in the service request message based on different objects of requesting services. This simplifies processing logic of the service communication proxy. In addition, after receiving a service request of the service consumer network element, the service communication proxy carries two CCAs regardless of requesting the second service from the network repository function network element or requesting the first service from the service producer network element. Therefore, it can be always ensured that the network repository function network element and the service producer network element successfully authenticate the service consumer network element, and a problem that the service consumer network element fails to request the service is avoided.

[00500] An embodiment of this application provides a communication method. When a service communication proxy fails to request a second service, the service communication proxy may actively request a client credentials assertion from a service consumer network element, to ensure that the service communication proxy can obtain the second service, and further ensure that the service consumer network element obtains a first service.

[00501] This embodiment of this application provides the communication method. As shown in FIG. 12, the method includes the following steps.

[00502] Step 1201: The service consumer network element sends a service request message 1 to the service communication proxy, where the service request message 1 is used to request the first service, the service request message 1 includes a client credentials assertion A, the client

credentials assertion A includes a first network function type, and the client credentials assertion A is used by a service producer network element to authenticate the service consumer network element. The first network function type is a network function type of the service producer network element.

[00503] It should be noted that, in this case, the client credentials assertion A does not include a second network function type. The second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service.

[00504] Step 1202: The service communication proxy sends a service request message 2 to a network repository function network element, where the service request message 2 is used to request the second service, and the service request message 2 includes the client credentials assertion A. The network repository function network element is configured to provide the second service.

[00505] Step 1203: The network repository function network element determines, based on the client credentials assertion A, that the authentication on the service consumer network element fails.

[00506] Step 1204: The network repository function network element sends a response message for the service request message 2 to the service communication proxy.

[00507] Step 1201 to step 1204 are respectively the same as step 901 to step 904 in the embodiment in FIG. 9. Details are not described again.

[00508] Step 1205: The service communication proxy sends a client credentials assertion request message to the service consumer network element based on the response message for the service request message 2.

[00509] The client credentials assertion request message may indicate that a first service request fails. The client credentials assertion request message may further include indication information.

[00510] In some embodiments, the indication information may include a client credentials assertion B and/or a cause value. When the indication information includes the client credentials assertion B, the service communication proxy may be prevented from maliciously triggering the service consumer network element to request a client credentials assertion.

[00511] In some embodiments, the service communication proxy may further generate the indication information based on the response message for the service request message 2. The indication information may alternatively include no client credentials assertion B or cause value. The indication information may indicate the service consumer network element to request a client credentials assertion and carry, when requesting the client credentials assertion, a client credentials assertion including a network function type of the network repository function network element.

[00512] Step 1206: The service consumer network element sends, based on the indication information, a response message for the client credentials assertion request message to the service communication proxy.

[00513] In some embodiments, when the indication information includes the client credentials assertion B and the client credentials assertion B includes the network function type of the network repository function network element, the service consumer network element may verify the client credentials assertion B. When the verification on the client credentials assertion B succeeds, the service consumer network element sends the response message for the client credentials assertion request message to the service communication proxy. The response message for the client credentials assertion request message includes a client credentials assertion C. The client credentials assertion C includes the first network function type and the second network function type, or the client credentials assertion C includes the second network function type. The first network function type is the network function type of the service producer network element, and the second network function type is the network function type of the network element providing the second service.

[00514] Step 1207: The service communication proxy receives the response message for the client credentials assertion request message from the service consumer network element, and sends a service request message 3 to the network repository function network element, where the service request message 3 is used to request the second service, and the service request message 3 includes the client credentials assertion C.

[00515] For example, when an available access token corresponding to the first service is not stored and the first service request message does not include an access token corresponding to the first service, the service communication proxy sends the service request message 3 to the network repository function network element, where the service request message 3 is used to request the access token corresponding to the first service.

[00516] Alternatively, when information about the service producer network element is not stored and the first service request message does not include the information about the service producer network element, the service communication proxy sends the service request message 3 to the network repository function network element, where the service request message 3 is used to request the information about the service producer network element.

[00517] Step 1208: The network repository function network element receives the service request message 3 from the service communication proxy, and the network repository function network element authenticates the service consumer network element based on the client credentials assertion C.

[00518] If the client credentials assertion C includes the first network function type and the

second network function type, and the network repository function network element determines that a network function type matching the network function type of the network repository function network element exists in the first network function type and the second network function type, the network repository function network element determines that verification on the client credentials assertion C succeeds. The second network function type matches the network function type of the network repository function network element. Specifically, if the network repository function network element verifies that a signature of the client credentials assertion C succeeds, verifies, based on a timestamp and/or expiration time of the client credentials assertion C included in the client credentials assertion C, that the client credentials assertion C does not expire, verifies that an identifier of the service consumer network element in the client credentials assertion C is the same as an identifier of a network element in a certificate for signing the client credentials assertion C, and verifies that the second network function type in the first network function type and the second network function type matches the network function type of the network repository function network element, the network repository function network element determines that the authentication on the service consumer network element succeeds.

[00519] If the client credentials assertion C includes the second network function type, and the network repository function network element verifies that a signature of the client credentials assertion C succeeds, verifies, based on a timestamp and/or expiration time of the client credentials assertion C included in the client credentials assertion C, that the client credentials assertion C does not expire, verifies that an identifier of the service consumer network element in the client credentials assertion C is the same as an identifier of a network element in a certificate for signing the client credentials assertion C, and verifies that the second network function type matches the network function type of the network repository function network element, the network repository function network element determines that the authentication on the service consumer network element succeeds.

[00520] Step 1209: When the authentication on the service consumer network element succeeds, the network repository function network element sends a response message for the service request message 3 to the service communication proxy.

[00521] For example, if the service request message 3 is used to request the access token corresponding to the first service, after the authentication on the service consumer network element succeeds, the network repository function network element performs authorization check. If it is determined that the authorization succeeds, the network repository function network element generates the access token corresponding to the first service. The network repository function network element sends the response message for the service request message 3 to the service communication proxy. The response message for the service request message 3 includes the access

token corresponding to the first service.

[00522] For example, if the service request message 3 is used to request the information about the service producer network element, after the authentication on the service consumer network element succeeds, the network repository function network element sends the response message for the service request message 3 to the service communication proxy. The response message for the service request message 3 includes the information about the service producer network element.

[00523] Step 1210: The service communication proxy receives the response message for the service request message 3 from the network repository function network element, and the service communication proxy sends a service request message 4 to the service producer network element based on the response message for the service request message 3, where the service request message 4 is used to request the first service, and the service request message 4 includes the client credentials assertion A or the client credentials assertion C.

[00524] It may be understood that the service request message 4 further includes the access token corresponding to the first service.

[00525] For example, when the response message for the service request message 3 includes the access token corresponding to the first service, the service communication proxy sends the service request message 4 to the service producer network element, where the service request message 4 is used to request the first service, and the service request message 4 includes a first client credentials assertion and the access token corresponding to the first service.

[00526] For example, when the response message for the service request message 3 includes the information about the service producer network element, the service communication proxy sends the service request message 4 to the service producer network element indicated by the information about the service producer network element, where the service request message 4 is used to request the first service, and the service request message 4 includes a first client credentials assertion and the access token corresponding to the first service. In this case, the access token corresponding to the first service may be stored by the service communication proxy or carried in the service request message 1.

[00527] Step 1211: The service producer network element receives the service request message 4 from the service communication proxy, and the service producer network element authenticates an NF service consumer based on the client credentials assertion A or the client credentials assertion C.

[00528] It may be understood that the service producer network element further needs to verify the access token corresponding to the first service. For details, refer to the foregoing verification process of the access token. Details are not described herein again.

[00529] If the service request message 4 includes the client credentials assertion C, and the

service producer network element determines that a network function type matching the network function type of the service producer network element exists in the first network function type and the second network function type, the service producer network element determines, based on the client credentials assertion C, that the authentication on the service consumer network element succeeds. The first network function type matches the network function type of the service producer network element. Specifically, if the service producer network element verifies that the signature of the client credentials assertion C succeeds, verifies, based on the timestamp and/or the expiration time of the client credentials assertion C included in the client credentials assertion C, that the client credentials assertion C does not expire, verifies that the identifier of the service consumer network element in the client credentials assertion C is the same as the identifier of the network element in the certificate for signing the client credentials assertion C, and verifies that the first network function type in the first network function type and the second network function type matches the network function type of the service producer network element, the service producer network element determines that the authentication on the service consumer network element succeeds.

[00530] If the service request message 4 includes the client credentials assertion A, the service producer network element verifies that a signature of the client credentials assertion A succeeds, verifies, based on a timestamp and/or expiration time of the client credentials assertion A included in the client credentials assertion A, that the client credentials assertion A does not expire, verifies that an identifier of the service consumer network element in the client credentials assertion A is the same as an identifier of a network element in a certificate for signing the client credentials assertion A, and verifies that the first network function type matches the network function type of the service producer network element, the service producer network element determines that the authentication on the service consumer network element succeeds.

[00531] Step 1212: The service producer network element sends a response message for the service request message 4 to the service communication proxy.

[00532] When the authentication on the service consumer network element succeeds and the verification on the access token corresponding to the first service succeeds, the response message for the service request message 4 indicates to provide the first service or indicates that a service request 4 succeeds. Alternatively, when the authentication on the service consumer network element fails and/or the verification on the access token corresponding to the first service fails, the response message for the service request message 4 indicates that the first service request fails.

[00533] Step 1213: The service communication proxy sends a response message for the service request message 1 to the service consumer network element.

[00534] When the response message for the service request message 4 indicates to provide the

first service or indicates that the service request 4 succeeds, the response message for the service request message 1 indicates to provide the first service or indicates that a service request 1 succeeds. Alternatively, when the response message for the service request message 4 indicates that the first service request fails, the response message for the service request message 1 indicates that the first service request fails.

[00535] In the foregoing embodiment, the service communication proxy sends the client credentials assertion request message to the service consumer network element, to ensure that when the service communication proxy requests the second service, the network element providing the second service successfully authenticates the service consumer network element, and further ensure that the service consumer network element requests the first service.

[00536] The embodiments shown in FIG. 8 to FIG. 12 are described below by using examples with reference to Embodiments 1 to 8.

[00537] Embodiment 1: With reference to the embodiment shown in FIG. 8, when it is determined that the first service needs to be requested and there is no available access token corresponding to the first service, the NF service consumer may obtain the first service according to, but not limited to, the following embodiment, as shown in FIG. 13.

[00538] Step 1301: The NF service consumer determines to request the first service and determines that there is no available access token corresponding to the first service, and the NF service consumer obtains a CCA, where the access token corresponding to the first service represents/indicates that the NF service consumer has permission to obtain the first service or permission to access the first service.

[00539] It may be understood that the NF service consumer may further determine, before step 1301, that a current indirect communication mode is the mode D.

[00540] After the NF service consumer determines to request the first service, the NF service consumer checks whether the access token corresponding to the first service is locally stored. That the NF service consumer determines that there is no available access token corresponding to the first service means that the NF service consumer determines that the access token corresponding to the first service is not stored or a stored access token corresponding to the first service expires. Further, when the NF service consumer determines that the stored access token corresponding to the first service expires, the NF service consumer deletes the expired access token corresponding to the first service.

[00541] For example, the NF service consumer may receive a service request message of UE, and determine, based on the service request message, that the first service needs to be requested. The NF service consumer obtains related information of the UE (for example, context information of the UE) based on an identifier of the UE. Further, the NF service consumer checks whether the

public storage space includes the access token corresponding to the first service. If the access token corresponding to the first service is included and the access token does not expire, the access token is used. If the access token corresponding to the first service is not included, it is determined that there is no available access token. Alternatively, if the access token corresponding to the first service is included but the access token expires, it is determined that there is no available access token. Further, optionally, the NF service consumer deletes the access token. The related information of the UE may be stored in the public storage space of the NF service consumer, or the related information of the UE is obtained by the NF service consumer from another network element based on the identifier of the UE.

[00542] In addition, the NF service consumer further needs to determine whether an available CCA is locally stored. If the available CCA is stored (for example, the CCA does not expire), the CCA is used. If the available CCA is not stored (for example, the CCA expires or the CCA is not stored), the NF service consumer generates the CCA. In addition, if the CCA expires, the NF service consumer deletes the expired CCA.

[00543] The CCA includes the first NF type and the second NF type. The first NF type is an NF type of an expected NF service producer providing the first service, and the second NF type is an NF type of an expected NRF providing an access token.

[00544] In addition, the CCA further includes an NF instance identifier of the NF service consumer, a timestamp, and expiration time.

[00545] Step 1302: The NF service consumer sends the first service request message to the SCP, where the first service request message includes the CCA in step 1301 and a parameter for obtaining an access token. The first service request message is used to request the first service.

[00546] The parameter for obtaining the access token and a parameter for discovering the NF service producer may be the same, or may be totally or partially different. The parameter for obtaining the access token and the parameter for discovering the NF service producer may be indicated by a same information element or different information elements. For example, if both the parameter for obtaining the access token and the parameter for discovering the NF service producer are the same, the same information element may be used for indication. If the parameter for obtaining the access token and the parameter for discovering the NF service producer are totally different, the first service request message further includes the parameter for discovering the NF service producer. If the parameter for obtaining the access token and the parameter for discovering the NF service producer are partially different, the first service request message further includes a remaining parameter for discovering the NF service producer.

[00547] For example, the parameter for obtaining the access token may include an expected service name, an NF type of the NF service consumer, an NF type of an expected NF service

producer, an S-NSSAI list or an NSI ID list of an expected NF service producer instance, an NF set ID of the expected NF service producer instance, an S-NSSAI list of the NF service consumer, and the like. The parameter for discovering the NF service producer may include the NF type of the expected NF service producer and the S-NSSAI list or NSI ID list of the expected NF service producer instance. In this case, the parameter for obtaining the access token may be partially same as the parameter for discovering the NF service producer.

[00548] Step 1303: The SCP sends an access token request message to the NRF, where the access token request message includes the CCA and the parameter for obtaining the access token.

[00549] Before the SCP sends the access token request message to the NRF, the SCP determines that the first service request message does not include the access token corresponding to the first service and the access token corresponding to the first service is not locally stored, or the SCP determines that the first service request message does not include the access token corresponding to the first service and the stored access token corresponding to the first service expires. If it is determined that the stored access token corresponding to the first service expires, the SCP deletes the expired access token corresponding to the first service.

[00550] In addition, it may be understood that if the access token corresponding to the first service is an access token of a type B, the SCP further needs to initiate the NF service producer discovery procedure before step 1303. Otherwise, the SCP may initiate the NF service producer discovery procedure after obtaining the access token corresponding to the first service. Alternatively, when information about the NF service producer is locally stored, the SCP may not initiate the NF service producer discovery procedure.

[00551] The access token request message may be an NNrf_AccessToken_Get_Request or another message. This is not limited in embodiments of this application.

[00552] Step 1304: The NRF receives the access token request message, and the NRF authenticates the NF service consumer based on the CCA.

[00553] The NRF successfully authenticates the NF service consumer based on the CCA, and performs authorization check. If it is determined that the authorization succeeds, the access token corresponding to the first service is generated.

[00554] The NRF verifies a signature of the CCA, verifies, based on the timestamp and/or the expiration time of the CCA, whether the CCA expires, and verifies whether the NF instance ID of the NF service consumer in the CCA matches an NF instance ID in a certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether an NF type the same as an NF type of the NRF exists in the first NF type and the second NF type that are included in the CCA. When the NRF determines that the second NF type matches the NF type of the NRF, the NRF determines that the authentication on

the NF service consumer succeeds.

[00555] Step 1305: The NRF sends an access token response message to the SCP, where the access token response message includes the access token corresponding to the first service.

[00556] Step 1306: The SCP sends a second service request message to the NF service producer. The second service request message includes the CCA and the access token corresponding to the first service.

[00557] Step 1307: The NF service producer receives the second service request message from the SCP. The NF service producer authenticates the NF service consumer based on the CCA.

[00558] The NF service producer performs integrity verification on the access token corresponding to the first service. If the integrity verification succeeds, the NF service producer further verifies claims in the access token corresponding to the first service. For details, refer to related content of verification on the claims in the access token.

[00559] The NF service producer further needs to authenticate the NF service consumer based on the CCA. The NF service producer verifies the signature of the CCA, verifies, based on the timestamp and/or the expiration time of the CCA, whether the CCA expires, and verifies whether the NF instance ID of the NF service consumer in the CCA matches the NF instance ID in the certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether an NF type matching the NF type of the NF service producer exists in the first NF type and the second NF type that are included in the CCA. When the NF service producer determines that the first NF type matches the NF type of the NF service producer, the NF service producer determines that the authentication on the NF service consumer succeeds.

[00560] Alternatively, the foregoing sequence of verifying the access token and the CCA may be that the CCA is first verified, and then the access token is verified after the verification succeeds. This is not limited herein.

[00561] In addition, the NF service producer further checks whether the NF instance ID of the NF service consumer in the CCA is the same as an NF instance ID of the NF service consumer included in the access token. If the NF instance ID of the NF service consumer in the CCA is the same as the NF instance ID of the NF service consumer included in the access token, the requested service is provided for the NF service consumer.

[00562] Step 1308: If the NF service producer determines that the verification on the first access token succeeds and the authentication on the NF service consumer succeeds, the NF service producer sends a response message for the second service request message to the SCP. The response message for the second service request message indicates to provide the first service or indicates that a second service request succeeds.

[00563] It may be understood that if the verification on the first access token fails and/or the authentication on the NF service consumer fails, the response message for the second service request message indicates that a first service request fails.

[00564] Step 1309: The SCP receives the response message for the second service request message from the NF service producer, and sends the response message for the first service request message to the NF service consumer.

[00565] The response message for the second service request message may include the access token corresponding to the first service. The NF service consumer stores the access token corresponding to the first service, to subsequently request the first service.

[00566] In addition, if the NF service consumer determines that there is the available access token corresponding to the first service, the NF service consumer may determine whether the available CCA is stored. If the available CCA is stored, the CCA is used. If the available CCA is not stored, a CCA is generated. It may be understood that, in this case, the CCA may not include the second NF type. However, if the NF service consumer determines, before step 1301, that the current indirect communication mode is the mode D, the first service request message needs to carry the first NF type and the second NF type.

[00567] In the foregoing embodiment, the CCA includes the first NF type and the second NF type. This can ensure that the NRF and the NF service producer successfully authenticate the NF service consumer based on the CCA, and further ensure that the NF service consumer obtains the first service.

[00568] Embodiment 2: With reference to the embodiment shown in FIG. 10, when it is determined that the first service needs to be requested and there is no available access token corresponding to the first service, the NF service consumer may obtain the first service according to, but not limited to, the following embodiment, as shown in FIG. 14.

[00569] Step 1401: The NF service consumer determines to request the first service and determines that there is no available access token corresponding to the first service, and the NF service consumer obtains a CCA 1 and a CCA 2, where the access token corresponding to the first service represents/indicates that the NF service consumer has permission to obtain the first service or permission to access the first service.

[00570] It may be understood that the NF service consumer may further determine, before step 1401, that a current indirect communication mode is a mode D. The NF service consumer determines to request the first service and determines that there is no available access token corresponding to the first service. For details, refer to related descriptions in step 1301 in FIG. 13. Details are not repeated.

[00571] In addition, the NF service consumer needs to determine whether available CCA 1 and

CCA 2 are locally stored. If the available CCA 1 is stored (for example, the CCA 1 does not expire), the CCA 1 is used. If the available CCA 1 is not stored (for example, the CCA 1 expires), the NF service consumer generates a CCA 1. If the available CCA 2 is stored (for example, the CCA 2 does not expire or the CCA 2 is not stored), the CCA 2 is used. If the available CCA 2 is not stored (for example, the CCA 2 expires or the CCA 2 is not stored), the NF service consumer generates a CCA 2. If the CCA 1 or the CCA 2 expires, the NF service consumer deletes the expired CCA.

[00572] The CCA 1 includes the first NF type, and the CCA 2 includes the second NF type. The first NF type is an NF type of an expected NF service producer providing the first service, and the second NF type is an NF type of an expected NRF providing an access token.

[00573] In addition, the CCA 1 further includes an NF instance identifier of the NF service consumer, a timestamp, and expiration time of the CCA 1. The CCA 2 further includes the NF instance identifier of the NF service consumer, a timestamp, and expiration time of the CCA 2.

[00574] Step 1402: The NF service consumer sends the first service request message to the SCP, where the first service request message includes the CCA 1 and the CCA 2 in step 1401 and a parameter for obtaining an access token. The first service request message is used to request the first service.

[00575] For the parameter for obtaining the access token and a parameter for discovering the NF service producer, refer to step 1402 in Embodiment 1. Details are not repeated.

[00576] Step 1403: The SCP sends an access token request message to the NRF. The access token request message includes the CCA 2 and the parameter for obtaining the access token.

[00577] Before the SCP sends the access token request message to the NRF, the SCP determines that the first service request message does not include the access token corresponding to the first service and the access token corresponding to the first service is not locally stored, or the SCP determines that the first service request message does not include the access token corresponding to the first service and a stored access token corresponding to the first service expires. If it is determined that the stored access token corresponding to the first service expires, the SCP deletes the expired access token corresponding to the first service.

[00578] The SCP needs to send the access token request message to the NRF. Therefore, the SCP adds the CCA 2 to the access token request message.

[00579] In addition, it may be understood that if the access token corresponding to the first service is an access token of a type B, the SCP further needs to initiate an NF service producer discovery procedure before step 1403. Otherwise, the SCP may initiate an NF service producer discovery procedure after obtaining the access token corresponding to the first service. Alternatively, when information about the NF service producer is locally stored, the SCP may not initiate an NF service producer discovery procedure.

[00580] For example, the access token request message may be an NNrf_AccessToken_Get_Request or another message. This is not limited in embodiments of this application.

[00581] Step 1404: The NRF receives the access token request message, and the NRF authenticates the NF service consumer based on the CCA 2.

[00582] The NRF successfully authenticates the NF service consumer based on the CCA 2, and performs authorization check. If it is determined that the authorization succeeds, the access token corresponding to the first service is generated.

[00583] The NRF verifies a signature of the CCA 2, verifies, based on the timestamp and/or the expiration time of the CCA 2, whether the CCA 2 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 2 matches an NF instance ID in a certificate for signing the CCA 2. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether the second NF type included in the CCA 2 is the same as an NF type of the NRF. Because the second NF type matches the NF type of the NRF, the NRF determines that the verification on the CCA 2 succeeds.

[00584] Step 1405: The NRF sends an access token response message to the SCP, where the access token response message includes the access token corresponding to the first service.

[00585] Step 1406: The SCP sends the second service request message to the NF service producer. The second service request message includes the CCA 1 and the access token corresponding to the first service.

[00586] Because the SCP needs to send the second service request message to the NF service producer, the SCP selects the CCA 1 and adds the CCA 1 to the second service request message.

[00587] Step 1407: The NF service producer receives the second service request message from the SCP, and the NF service producer verifies the CCA 1 and the access token corresponding to the first service.

[00588] The NF service producer performs integrity verification on the access token corresponding to the first service. If the integrity verification succeeds, the NF service producer further verifies claims in the access token corresponding to the first service. For details, refer to related content of verification on the claims in the access token.

[00589] The NF service producer further needs to authenticate the NF service consumer based on the CCA 1. The NF service producer verifies a signature of the CCA 1, verifies, based on the timestamp and/or the expiration time of the CCA 1, whether the CCA 1 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 1 matches an NF instance ID in a certificate for signing the CCA 1. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether the first NF type

included in the CCA 1 matches the NF type of the NF service producer. Because the first NF type matches the NF type of the NF service producer, it is determined that the authentication on the NF service consumer succeeds.

[00590] Alternatively, the foregoing sequence of verifying the access token and the CCA 1 may be that the CCA 1 is first verified, and then the access token is verified after the verification succeeds. This is not limited herein.

[00591] After both the verification on the access token and the verification on the CCA 1 succeed, the NF service producer further checks whether the NF instance ID of the NF service consumer in the CCA 1 is the same as an NF instance ID of the NF service consumer included in the access token. If the NF instance ID of the NF service consumer in the CCA 1 is the same as the NF instance ID of the NF service consumer included in the access token, the requested service is provided for the NF service consumer.

[00592] Step 1408: If the NF service producer determines that the verification on the first access token succeeds and the authentication on the NF service consumer succeeds, the NF service producer sends the response message for the second service request message to the SCP. The response message for the second service request message indicates to provide the first service or indicates that a second service request succeeds.

[00593] It may be understood that if the verification on the first access token fails and/or the authentication on the NF service consumer fails, the response message for the second service request message indicates that a first service request fails.

[00594] Step 1409: The SCP receives the response message for the second service request message from the NF service producer, and sends the response message for the first service request message to the NF service consumer.

[00595] The response message for the first service request message may include the access token corresponding to the first service. The NF service consumer stores the access token corresponding to the first service, to subsequently request the first service.

[00596] In addition, if the NF service consumer determines that there is the available access token corresponding to the first service, the NF service consumer may determine whether the available CCA 1 is stored. If the available CCA 1 is stored, the CCA 1 is used. If the available CCA 1 is not stored, a CCA 1 is generated. It may be understood that, in this case, the NF service consumer does not need to determine whether the available CCA 2 is stored. Even if the available CCA 2 is not stored, the NF service consumer does not need to generate the CCA 2, and does not need to obtain, through the SCP, the access token corresponding to the first service. The first service request message may not include the CCA 2. However, if the NF service consumer determines, before step 1401, that the current indirect communication mode is the mode D, the

first service request message needs to carry the CCA 1 and the CCA 2.

[00597] In the foregoing embodiment, the CCA 1 includes the first NF type, and the CCA 2 includes the second NF type. This can ensure that the NRF successfully authenticates the NF service consumer based on the CCA 2 and the NF service producer successfully authenticates the NF service consumer based on the CCA 1, and further ensure that the NF service consumer obtains the first service.

[00598] Embodiment 3: With reference to the embodiment shown in FIG. 11, when it is determined that the first service needs to be requested and there is no available access token corresponding to the first service, the NF service consumer may obtain the first service according to, but not limited to, the following embodiment, as shown in FIG. 15.

[00599] For step 1501 and step 1502, refer to step 1401 and step 1402 in FIG. 14. Details are not repeated.

[00600] Step 1503: The SCP sends an access token request message to the NRF. The access token request message includes a CCA 2, a CCA 1, and a parameter for obtaining an access token.

[00601] Before the SCP sends the access token request message to the NRF, the SCP determines that the first service request message does not include an access token corresponding to the first service and the access token corresponding to the first service is not locally stored, or the SCP determines that the first service request message does not include the access token corresponding to the first service and a stored access token corresponding to the first service expires. If it is determined that the stored access token corresponding to the first service expires, the SCP deletes the expired access token corresponding to the first service.

[00602] In addition, it may be understood that if the access token corresponding to the first service is an access token of a type B, the SCP further needs to initiate an NF service producer discovery procedure before step 1503. Otherwise, the SCP may initiate an NF service producer discovery procedure after obtaining the access token corresponding to the first service. Alternatively, when information about an NF service producer is locally stored, the SCP may not initiate an NF service producer discovery procedure.

[00603] For example, the access token request message may be an NNrf_AccessToken_Get_Request or another message. This is not limited in embodiments of this application.

[00604] Step 1504: The NRF receives the access token request message, and the NRF authenticates the NF service consumer based on the CCA 1 and the CCA 2.

[00605] The NRF successfully authenticates the NF service consumer based on the CCA 1 or successfully authenticates the NF service consumer based on the CCA 2, and performs authorization check. If it is determined that the authorization succeeds, the access token

corresponding to the first service is generated.

[00606] The NRF authenticates the NF service consumer based on the CCA 1 and the CCA 2. In this case, the NRF does not need to determine, based on the CCA 1, that the authentication on the NF service consumer succeeds, or determine, based on the CCA 2, that the authentication on the NF service consumer succeeds. When determining, based on the CCA 1, that the authentication on the NF service consumer succeeds, or determining, based on the CCA 2, that the authentication on the NF service consumer succeeds, the NRF determines that the authentication on the NF service consumer succeeds.

[00607] The NRF verifies a signature of the CCA 1, verifies, based on a timestamp and/or expiration time of the CCA 1, whether the CCA 1 expires, and verifies whether an NF instance ID of the NF service consumer in the CCA 1 matches an NF instance ID in a certificate for signing the CCA 1. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether a first NF type included in the CCA 1 matches the NF type of the NRF. Because the first NF type does not match the NF type of the NRF, the NRF determines that the authentication on the NF service consumer fails.

[00608] The NRF verifies a signature of the CCA 2, verifies, based on a timestamp and/or expiration time of the CCA 2, whether the CCA 2 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 2 matches an NF instance ID in a certificate for signing the CCA 2. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether a second NF type included in the CCA 2 matches the NF type of the NRF. Because the second NF type matches the NF type of the NRF, the NRF determines that the authentication on the NF service consumer succeeds.

[00609] Step 1505: The NRF sends an access token response message to the SCP, where the access token response message includes the access token corresponding to the first service.

[00610] Step 1506: The SCP sends the second service request message to the NF service producer. The second service request message includes the CCA 1, the CCA 2, and the access token corresponding to the first service.

[00611] Step 1507: The NF service producer receives the second service request message from the SCP. The NF service producer verifies the CCA 1, CCA 2, and the access token.

[00612] The NF service producer performs integrity verification on the access token corresponding to the first service. If the integrity verification succeeds, the NF service producer further verifies claims in the access token corresponding to the first service. For details, refer to related content of verification on the claims in the access token.

[00613] The NF service producer authenticates the NF service consumer based on the CCA 1 and the CCA 2. In this case, the NF service producer does not need to determine, based on the

CCA 1, that the authentication on the NF service consumer succeeds, or determine, based on the CCA 2, that the authentication on the NF service consumer succeeds. When the NF service producer determines, based on the CCA 1, that the authentication on the NF service consumer succeeds, or determines, based on the CCA 2, that the authentication on the NF service consumer succeeds, the NF service producer determines that the authentication on the NF service consumer succeeds.

[00614] The NF service producer verifies the signature of the CCA 1, verifies, based on the timestamp and/or the expiration time of the CCA 1, whether the CCA 1 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 1 matches the NF instance ID in the certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether the first NF type included in the CCA 1 matches the NF type of the NF service producer. Because the first NF type matches the NF type of the NF service producer, the NF service producer determines that the authentication on the NF service consumer succeeds.

[00615] The NF service producer verifies the signature of the CCA 2, verifies, based on the timestamp and/or the expiration time of the CCA 2, whether the CCA 2 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 2 matches the NF instance ID in the certificate for signing the CCA 2. In addition to successful verification of the foregoing verification content, the NF service producer further needs to verify whether the second NF type included in the CCA 2 matches the NF type of the NF service producer. Because the second NF type is an NF type of an expected NF service producer providing the access token corresponding to the first service, and the second NF type does not match the NF type of the NF service producer, the NF service producer determines that the authentication on the NF service consumer fails.

[00616] Step 1508: If the NF service producer determines that the verification on the first access token succeeds and the authentication on the NF service consumer succeeds, the NF service producer sends the response message for the second service request message to the SCP. The response message for the second service request message indicates to provide the first service or indicates that a second service request succeeds.

[00617] It may be understood that if the verification on the first access token fails and/or the authentication on the NF service consumer fails, the response message for the second service request message indicates that a first service request fails.

[00618] Step 1509: The SCP receives the response message for the second service request message from the NF service producer, and sends the response message for the first service request message to the NF service consumer.

[00619] The response message for the second service request message may include the access

token corresponding to the first service. The NF service consumer stores the access token corresponding to the first service, to subsequently request the first service.

[00620] In the foregoing embodiment, the CCA 1 includes the first NF type, and the CCA 2 includes the second NF type. This can ensure that the NRF successfully authenticates the NF service consumer based on the CCA 1 and the NF service producer successfully authenticates the NF service consumer based on the CCA 2, and further ensure that the NF service consumer obtains the first service.

[00621] Embodiment 4: When it is determined that the first service needs to be requested and there is an available access token corresponding to the first service, the NF service consumer may obtain the first service according to, but not limited to, the following embodiment, as shown in FIG. 16.

[00622] Step 1601: The NF service consumer determines to request the first service and determines that there is the available access token corresponding to the first service, and the NF service consumer obtains a CCA, where the access token corresponding to the first service represents/indicates that the NF service consumer has permission to obtain the first service or permission to access the first service.

[00623] If the NF service consumer determines that there is the available access token corresponding to the first service, the NF service consumer may further determine whether the available CCA is stored. If the available CCA is stored, the CCA is used. If the available CCA is not stored, a CCA is generated. It may be understood that, in this case, the CCA generated by the NF service consumer may not include a second NF type.

[00624] The CCA includes an NF instance identifier of the NF service consumer, a timestamp, expiration time, and a first NF type, and the first NF type is an NF type of an expected NF service producer providing the first service.

[00625] Step 1602: The NF service consumer sends a first service request message to the SCP, where the first service request message includes the CCA in step 1601 and the access token corresponding to the first service.

[00626] Step 1603: The SCP sends a second service request message to the NF service producer. The second service request message includes the CCA and the access token corresponding to the first service.

[00627] Before the SCP sends the second service request message to the NF service producer, the SCP determines that the first service request message includes the access token corresponding to the first service or a locally stored access token corresponding to the first service.

[00628] Step 1604: The NF service producer receives the second service request message from the SCP. The NF service producer authenticates the NF service consumer based on the CCA.

[00629] The NF service producer performs integrity verification on the access token corresponding to the first service. If the integrity verification succeeds, the NF service consumer further verifies claims in the access token corresponding to the first service. For details, refer to related content of verification on the claims in the access token. The NF service producer further needs to authenticate the NF service consumer based on the CCA. For details, refer to an existing CCA verification process.

[00630] The NF service producer verifies a signature of the CCA, verifies, based on the timestamp and/or the expiration time of the CCA, whether the CCA expires, and verifies whether the NF instance ID of the NF service consumer in the CCA matches an NF instance ID in a certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether the first NF type included in the CCA matches the NF type of the NF service producer. Because the first NF type matches the NF type of the NF service producer, the NF service producer determines that the authentication on the NF service consumer succeeds.

[00631] Step 1605: If the NF service producer determines that the verification on the first access token succeeds and the authentication on the NF service consumer succeeds, the NF service producer sends a response message for the second service request message to the SCP.

[00632] The response message for the second service request message indicates to provide the first service or indicates that a second service request succeeds.

[00633] It may be understood that if the verification on the first access token fails and/or the authentication on the NF service consumer fails, the response message for the second service request message indicates that a first service request fails.

[00634] Step 1606: The SCP receives the response message for the second service request message from the NF service producer, and sends the response message for the first service request message to the NF service consumer.

[00635] In the foregoing embodiment, by determining that the available CCA is stored, the NF service consumer may carry the first NF type to obtain the first service.

[00636] Embodiment 5: With reference to the embodiment shown in FIG. 8, when the first service needs to be requested and requesting of the first service triggers the SCP to request a parameter of the NF service producer (triggers the SCP to initiate the NF service producer discovery procedure), the NF service consumer may obtain the first service according to, but not limited to, the following embodiment, as shown in FIG. 17.

[00637] Step 1701: The NF service consumer determines to trigger the SCP to initiate the NF service producer discovery procedure, and the NF service consumer obtains a CCA.

[00638] It may be understood that the NF service consumer may further determine, before step

1701, that a current indirect communication mode is the mode D.

[00639] For example, the NF service consumer may determine, based on one or more of the following cases, to trigger the SCP to initiate the NF service producer discovery procedure:

[00640] Case 1: Context of the UE is not stored. For example, the NF service consumer determines, based on a service request message of the UE, that the first service needs to be requested.

[00641] Case 2: Context of the first service is not stored.

[00642] Case 3: A first slice belongs to the service producer network element and context of the first slice is not stored. For example, the NF service consumer determines, based on the service request message of the UE, that the first service needs to be requested from the service producer network element in the first slice.

[00643] Case 4: The service consumer network element communicates with the service communication proxy for the first time.

[00644] Before the NF service consumer generates the CCA, the NF service consumer needs to determine whether an available CCA is locally stored. If the available CCA is stored (for example, the CCA does not expire), the CCA is used. If the available CCA is not stored (for example, the CCA expires or the CCA is not stored), the NF service consumer generates the CCA. If the CCA expires, the NF service consumer deletes the expired CCA.

[00645] The CCA includes the first NF type and the second NF type. The first NF type is an NF type of an expected NF service producer providing the first service, and the second NF type is an NF type of an expected NRF providing the information about the NF service producer.

[00646] In addition, the CCA further includes an NF instance identifier of the NF service consumer, a timestamp, and expiration time.

[00647] Step 1702: The NF service consumer sends the first service request message to the SCP, where the first service request message includes the CCA in step 1701 and a parameter for discovering the NF service producer, and the first service request message is used to request the first service.

[00648] For example, the parameter for discovering the NF service producer may include the NF type of the expected NF service producer, an S-NSSAI list or NSI ID list of an expected NF service producer instance, or the like.

[00649] Step 1703: The SCP sends a discovery request message to the NRF, where the discovery request message includes the CCA and the parameter for discovering the NF service producer.

[00650] Before the SCP sends the discovery request message to the NRF, the SCP determines that the first service request message does not include the information about the NF service producer and the information about the NF service producer is not locally stored.

[00651] Herein, it is assumed that the first service request message further includes the access token corresponding to the first service or the SCP locally stores the access token corresponding to the first service.

[00652] Step 1704: The NRF receives the discovery request message, and the NRF authenticates the NF service consumer based on the CCA.

[00653] The NRF verifies a signature of the CCA, verifies, based on the timestamp and/or the expiration time of the CCA, whether the CCA expires, and verifies whether the NF instance ID of the NF service consumer in the CCA matches an NF instance ID in a certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether an NF type matching the NF type of the NRF exists in the first NF type and the second NF type that are included in the CCA. When the NRF determines that the second NF type matches the NF type of the NRF, the NRF determines that the authentication on the NF service consumer succeeds.

[00654] Step 1705: The NRF sends a discovery response message to the SCP, where the discovery response message includes the parameter of the NF service producer.

[00655] When the authentication on the NF service consumer succeeds, the NRF sends the discovery response message to the SCP, where the discovery response message includes the parameter of the NF service producer.

[00656] Step 1706: The SCP sends a second service request message to the NF service producer. The second service request message includes the CCA and the access token corresponding to the first service.

[00657] The SCP sends the second service request message to the NF service producer indicated by the parameter of the NF service producer in the discovery response message.

[00658] Step 1707: The NF service producer receives the second service request message from the SCP. The NF service producer authenticates the NF service consumer based on the CCA.

[00659] The NF service producer performs integrity verification on the access token corresponding to the first service. If the integrity verification succeeds, the NF service producer further verifies claims in the access token corresponding to the first service. For details, refer to related content of verification on the claims in the access token. The NF service producer further needs to authenticate the NF service consumer based on the CCA.

[00660] The NF service producer verifies the signature of the CCA, verifies, based on the timestamp and/or the expiration time of the CCA, whether the CCA expires, and verifies whether the NF instance ID of the NF service consumer in the CCA matches the NF instance ID in the certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether an NF type matching

the NF type of the NF service producer exists in the first NF type and the second NF type that are included in the CCA. When the NF service producer determines that the first NF type matches the NF type of the NF service producer, the NF service producer determines that the authentication on the NF service consumer succeeds.

[00661] Step 1708: If the NF service producer determines that the verification on the first access token succeeds and the authentication on the NF service consumer succeeds, the NF service producer sends a response message for the second service request message to the SCP. The response message for the second service request message indicates to provide the first service or indicates that a second service request succeeds.

[00662] It may be understood that if the verification on the first access token fails and/or the authentication on the NF service consumer fails, the response message for the second service request message indicates that a first service request fails.

[00663] Step 1709: The SCP receives the response message for the second service request message from the NF service producer, and sends the response message for the first service request message to the NF service consumer.

[00664] In the foregoing embodiment, the CCA includes the first NF type and the second NF type. This can ensure that the NRF and the NF service producer successfully authenticate the NF service consumer based on the CCA, and further ensure that the NF service consumer obtains the first service.

[00665] Embodiment 6: With reference to the embodiment shown in FIG. 10, when the first service needs to be requested and requesting of the first service triggers the SCP to request a parameter of an NF service producer (triggers the SCP to initiate an NF service producer discovery procedure), an NF service consumer may obtain the first service according to, but not limited to, the following embodiment, as shown in FIG. 18.

[00666] Step 1801: The NF service consumer determines to trigger the SCP to execute the NF service producer discovery procedure, and the NF service consumer obtains a CCA 1 and a CCA 2.

[00667] It may be understood that the NF service consumer may further determine, before step 1801, that a current indirect communication mode is a mode D.

[00668] For example, for the NF service consumer determining to trigger the SCP to execute the NF service producer discovery procedure, refer to related descriptions in step 1701 in Embodiment 5.

[00669] In addition, before the NF service consumer generates the CCA 1 and the CCA 2, the NF service consumer needs to determine whether an available CCA 1 and an available CCA 2 are locally stored. If the available CCA 1 is stored (for example, the CCA 1 does not reach expiration

time), the CCA 1 is used. If the available CCA 1 is not stored (for example, the CCA 1 expires or the CCA 1 is not stored), the NF service consumer generates the CCA 1. If the available CCA 2 is stored (for example, the CCA 2 does not expire), the CCA 2 is used. If the available CCA 2 is stored (for example, the CCA 2 expires or the CCA 2 is not stored), the NF service consumer generates the CCA 2. If the CCA 1 or the CCA 2 expires, the NF service consumer deletes the expired CCA.

[00670] The CCA 1 includes the first NF type, and the CCA 2 includes the second NF type. The first NF type is an NF type of an expected NF service producer providing the first service, and the second NF type is an NF type of an expected NRF providing information about the NF service producer.

[00671] In addition, the CCA 1 further includes an NF instance identifier of the NF service consumer, the timestamp, and the expiration time of the CCA 1. The CCA 2 further includes the NF instance identifier of the NF service consumer, a timestamp, and expiration time of the CCA 2.

[00672] Step 1802: The NF service consumer sends the first service request message to the SCP, where the first service request message includes the CCA 1 and the CCA 2 in step 1801 and a parameter for discovering the NF service producer. The first service request message is used to request the first service.

[00673] Step 1803: The SCP sends a discovery request message to the NRF, where the discovery request message includes the CCA 2 and the parameter for discovering the NF service producer.

[00674] Before the SCP sends the discovery request message to the NRF, the SCP determines that the first service request message does not include the information about the NF service producer and the information about the NF service producer is not locally stored.

[00675] Herein, it is assumed that the first service request message further includes the access token corresponding to the first service or the SCP locally stores the access token corresponding to the first service.

[00676] The SCP needs to send the discovery request message to the NRF. Therefore, the SCP selects the CCA 2 and adds the CCA 2 to the discovery request message.

[00677] Step 1804: The NRF receives the discovery request message, and the NRF authenticates the NF service consumer based on the CCA 2.

[00678] The NRF verifies a signature of the CCA 2, verifies, based on the timestamp and/or the expiration time of the CCA 2, whether the CCA 2 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 2 matches an NF instance ID in a certificate for signing the CCA 2. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether the second NF type included in the CCA 2 matches the NF type of

the NRF. Because the second NF type matches the NF type of the NRF, the NRF determines that the authentication on the NF service consumer succeeds.

[00679] Step 1805: The NRF sends a discovery response message to the SCP, where the discovery response message includes the information about the NF service producer.

[00680] When the authentication on the NF service consumer succeeds, the NRF sends the discovery response message to the SCP, where the discovery response message includes the parameter of the NF service producer.

[00681] Step 1806: The SCP sends the second service request message to the NF service producer. The second service request message includes the CCA 1 and the access token corresponding to the first service.

[00682] The SCP sends the second service request message to the NF service producer indicated by the parameter of the NF service producer in the discovery response message.

[00683] Because the SCP needs to send the second service request message to the NF service producer, the SCP selects the CCA 1 and adds the CCA 1 to the second service request message.

[00684] Step 1807: The NF service producer receives the second service request message from the SCP. The NF service producer authenticates the NF service consumer based on the CCA 1.

[00685] The NF service producer performs integrity verification on the access token corresponding to the first service. If the integrity verification succeeds, the NF service producer further verifies claims in the access token corresponding to the first service. For details, refer to related content of verification on the claims in the access token. The NF service producer further needs to authenticate the NF service consumer based on the CCA 1.

[00686] The NF service producer verifies a signature of the CCA 1, verifies, based on the timestamp and/or the expiration time of the CCA 1, whether the CCA 1 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 1 matches an NF instance ID in a certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether the first NF type included in the CCA 1 matches the NF type of the NF service producer. Because the first NF type matches the NF type of the NF service producer, the NF service producer determines that the authentication on the NF service consumer succeeds.

[00687] Step 1808: If the NF service producer determines that the verification on the first access token succeeds and the authentication on the NF service consumer succeeds, the NF service producer sends the response message for the second service request message to the SCP. The response message for the second service request message indicates to provide the first service or indicates that a second service request succeeds.

[00688] It may be understood that if the verification on the first access token fails and/or the

authentication on the NF service consumer fails, the response message for the second service request message indicates that a first service request fails.

[00689] Step 1809: The SCP receives the response message for the second service request message from the NF service producer, and sends the response message for the first service request message to the NF service consumer.

[00690] In addition, if the NF service consumer determines that the SCP does not need to be triggered to perform the NF service producer discovery procedure, the NF service consumer may determine whether the available CCA 1 is stored. If the available CCA 1 is stored, the CCA 1 is used. If the available CCA 1 is not stored, the CCA 1 is generated. It may be understood that, in this case, the NF service consumer does not need to determine whether the available CCA 2 is stored. Even if the available CCA 2 is not stored, the NF service consumer does not need to generate the CCA 2. The first service request message may not include the CCA 2. However, if the NF service consumer determines, before step 1801, that the current indirect communication mode is the mode D, the first service request message needs to carry the CCA 1 and the CCA 2.

[00691] In the foregoing embodiment, the CCA 1 includes the first NF type, and the CCA 2 includes the second NF type. This can ensure that the NRF successfully authenticates the NF service consumer based on the CCA 1 and the NF service producer successfully authenticates the NF service consumer based on the CCA 2, and further ensure that the NF service consumer obtains the first service.

[00692] Embodiment 7: With reference to the embodiments shown in FIG. 8 and FIG. 10, the NF service consumer obtains the indication information, the NF service consumer sends the service request message to the SCP based on the indication information, and the NF service consumer may obtain the first service according to, but not limited to, the following embodiment, as shown in FIG. 19A and FIG. 19B.

[00693] Step 1901: The NF service consumer obtains a CCA 1.

[00694] It may be understood that the NF service consumer may further determine, before step 1901, that a current indirect communication mode is a mode D.

[00695] The NF service consumer determines to request the first service, and the NF service consumer obtains the CCA 1. Before the NF service consumer generates the CCA 1, the NF service consumer needs to determine whether an available CCA 1 is locally stored. If the available CCA 1 is stored (for example, the CCA 1 does not expire), the CCA 1 is used. If the available CCA 1 is not stored (for example, the CCA 1 expires or the CCA 1 is not stored), the NF service consumer generates the CCA 1. In addition, if the CCA 1 expires, the NF service consumer deletes the expired CCA 1.

[00696] The CCA 1 includes an NF instance identifier of the NF service consumer, a timestamp,

expiration time of the CCA 1, and the first NF type, and the first NF type is an NF type of an expected NF service producer providing the first service.

[00697] Step 1902: The NF service consumer sends the first service request message to the SCP, where the first service request message includes the CCA 1 in step 1901. The first service request message is used to request the first service.

[00698] Step 1903: The SCP sends the second service request message to the NRF, where the second service request message includes the CCA 1, and the second service request message is used to request the second service.

[00699] Step 1904: The NRF receives the second service request message, and the NRF fails to authenticate the NF service consumer based on the CCA 1.

[00700] The NRF verifies a signature of the CCA 1, verifies, based on the timestamp and/or the expiration time of the CCA 1, whether the CCA 1 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 1 matches an NF instance ID in a certificate for signing the CCA 1. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether the first NF type included in the CCA 1 matches an NF type of the NRF. Because the first NF type does not match the NF type of the NRF, the NRF determines that the authentication on the NF service consumer fails.

[00701] Step 1905: The NRF sends the response message for the second service request message to the SCP. The response message for the second service request message includes the CCA 2. The CCA 2 includes an NF instance identifier of the NRF, a timestamp, expiration time, an NF type of the NF service consumer, and the NF type of the NRF.

[00702] Step 1906: The SCP sends the response message for the first service request message to the NF service consumer. The response message for the first service request message includes the CCA 2.

[00703] Step 1907: The NF service consumer sends the third service request message to the SCP, where the third service request message includes a CCA 3 and a CCA 4, or the third service request message includes a CCA 5.

[00704] The CCA 3 includes an NF instance identifier of the NF service consumer, a timestamp, expiration time of the CCA 3, and the first NF type.

[00705] The CCA 4 includes an NF instance identifier of the NF service consumer, a timestamp, expiration time of the CCA 4, and the second NF type.

[00706] The CCA 5 includes an NF instance identifier of the NF service consumer, a timestamp, expiration time of the CCA 5, the first NF type, and the second NF type.

[00707] The first NF type is the NF type of the expected NF service producer providing the first service, and the second NF type is an NF type of an expected NF service producer providing the

second service.

[00708] For example, if the NF service consumer authenticates the NRF based on the CCA 2, and determines that the authentication on the NRF succeeds, the NF service consumer generates the CCA 3 and the CCA 4, or the CCA 5 based on the NF type of the NRF in the CCA 2.

[00709] Step 1908: The SCP sends the fourth service request message to the NRF, where the fourth service request message includes the CCA 4 or the CCA 5, and the fourth service request message is used to request the second service.

[00710] Step 1909: The NRF receives the fourth service request message, and the NRF authenticates the NF service consumer based on the CCA in the fourth service request message.

[00711] For example, if the fourth service request message includes the CCA 4, the NRF successfully authenticates the NF service consumer based on the CCA 4. The NRF verifies a signature of the CCA 4, verifies, based on a timestamp and/or expiration time of the CCA 4, whether the CCA 4 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 4 matches an NF instance ID in a certificate for signing the CCA 4. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether the second NF type included in the CCA 4 matches the NF type of the NRF. Because the second NF type matches the NF type of the NRF, the NRF determines that the authentication on the NF service consumer succeeds.

[00712] For example, if the fourth service request message includes the CCA 5, the NRF successfully authenticates the NF service consumer based on the CCA 5. The NRF verifies a signature of the CCA 5, verifies, based on a timestamp and/or expiration time of the CCA 5, whether the CCA 5 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 5 matches an NF instance ID in a certificate for signing the CCA 5. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether an NF type matching the NF type of the NRF exists in the first NF type and the second NF type that are included in the CCA 5. Because the second NF type matches the NF type of the NRF, the NRF determines that the authentication on the NF service consumer succeeds.

[00713] Step 1910: The NRF sends the response message for the fourth service request message to the SCP.

[00714] Step 1911: The SCP sends the fifth service request message to the NF service producer. The fifth service request message includes the CCA 3 and an access token corresponding to the first service, or the fifth service request message includes the CCA 5 and an access token corresponding to the first service.

[00715] Step 1912: The NF service producer receives the fifth service request message from the SCP. The NF service producer authenticates the NF service consumer based on the CCA in the

fifth service request message.

[00716] The NF service producer performs integrity verification on the access token corresponding to the first service. If the integrity verification succeeds, the NF service producer further verifies claims in the access token corresponding to the first service. For details, refer to related content of verification on the claims in the access token.

[00717] If the fifth service request message includes the CCA 3, the NF service producer further needs to authenticate the NF service consumer based on the CCA 3. The NF service producer verifies a signature of the CCA 3, verifies, based on the timestamp and/or the expiration time of the CCA 3, whether the CCA 3 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 3 matches an NF instance ID in a certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether the first NF type included in the CCA 3 matches the NF type of the NF service producer. Because the first NF type matches the NF type of the NF service producer, it is determined that the authentication on the NF service consumer succeeds.

[00718] If the fifth service request message includes the CCA 5, the NF service producer further needs to authenticate the NF service consumer based on the CCA 5. The NF service producer verifies the signature of the CCA 5, verifies, based on the timestamp and/or the expiration time of the CCA 5, whether the CCA 5 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 5 matches an NF instance ID in a certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether the first NF type and the second NF type that are included in the CCA 5 include an NF type matching the NF type of the NF service producer. Because the first NF type matches the NF type of the NF service producer, it is determined that the authentication based on the CCA 5 succeeds.

[00719] Step 1913: If the NF service producer determines that the verification on the first access token succeeds and the authentication on the NF service consumer succeeds, the NF service producer sends the response message for the fifth service request message to the SCP. The response message for the fifth service request message indicates to provide the first service or indicates that a fifth service request succeeds.

[00720] It may be understood that if the verification on the first access token fails and/or the authentication on the NF service consumer fails, the response message for the fifth service request message indicates that a first service request fails.

[00721] Step 1914: The SCP receives the response message for the fifth service request message from the NF service producer, and sends the response message for the third service request message to the NF service consumer.

[00722] In the foregoing embodiment, the SCP sends the indication information to the NF service consumer, and the NF service consumer sends, based on the indication information, the service request message carrying the CCA 3 (the first NF type) and the CCA 4 (the second NF type), or the CCA 5 (the first NF type and the second NF type), to ensure that the NF service consumer obtains the first service.

[00723] Embodiment 8: With reference to the embodiment shown in FIG. 12, the SCP actively requests a client credentials assertion, and sends the client credentials assertion request message. The NF service consumer responds to the client credentials assertion request message. The NF service consumer may obtain the first service according to, but is not limited to, the following embodiment, as shown in FIG. 20A and FIG. 20B.

[00724] For step 2001 to step 2005, refer to related descriptions of step 1901 to step 1905 in Embodiment 7.

[00725] Step 2006: The SCP sends the CCA request message to the NF service consumer. The CCA request message includes a CCA 2.

[00726] Step 2007: The NF service consumer sends the response message for the CCA request message to the SCP, where the response message for the CCA request message includes a CCA 3, or the response message for the CCA request message includes a CCA 4.

[00727] The CCA 3 includes an NF instance identifier of the NF service consumer, a timestamp, expiration time of the CCA 3, and the second NF type.

[00728] The CCA 4 includes an NF instance identifier of the NF service consumer, a timestamp, expiration time of the CCA 4, the first NF type, and the second NF type.

[00729] The first NF type is an NF type of an expected NF service producer providing the first service, and the second NF type is an NF type of an expected NF service producer providing the second service.

[00730] For example, if the NF service consumer authenticates the NRF based on the CCA 2, and determines that the authentication on the NRF succeeds, the NF service consumer generates the CCA 3 or the CCA 4 based on an NF type of the NRF in the CCA 2.

[00731] Step 2008: The SCP sends a third service request message to the NRF, where the third service request message includes the CCA 3 or the CCA 4, and the third service request message is used to request the second service.

[00732] Step 2009: The NRF receives the third service request message, and the NRF authenticates the NF service consumer based on the CCA in the third service request message.

[00733] For example, if the third service request message includes the CCA 3, the NRF successfully authenticates the NF service consumer based on the CCA 3. The NRF verifies a signature of the CCA 3, verifies, based on the timestamp and/or the expiration time of the CCA 3,

whether the CCA 3 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 3 matches an NF instance ID in a certificate for signing the CCA 3. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether the second NF type included in the CCA 3 matches the NF type of the NRF. Because the second NF type matches the NF type of the NRF, the NRF determines that the authentication on the NF service consumer succeeds.

[00734] For example, if the third service request message includes the CCA 4, the NRF successfully authenticates the NF service consumer based on the CCA 4. The NRF verifies a signature of the CCA 4, verifies, based on the timestamp and/or the expiration time of the CCA 4, whether the CCA 4 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 4 matches an NF instance ID in a certificate for signing the CCA 4. In addition to successful verification of all the foregoing verification content, the NRF further needs to verify whether an NF type matching the NF type of the NRF exists in the first NF type and the second NF type that are included in the CCA 4. Because the second NF type matches the NF type of the NRF, the NRF determines that the authentication on the NF service consumer succeeds.

[00735] Step 2010: The NRF sends a response message for the third service request message to the SCP.

[00736] Step 2011: The SCP sends a fourth service request message to the NF service producer. The fourth service request message includes the CCA 3 and the access token corresponding to the first service, or the fourth service request message includes the CCA 4 and the access token corresponding to the first service.

[00737] Step 2012: The NF service producer receives the fourth service request message from the SCP. The NF service producer authenticates the NF service consumer based on the CCA in the fourth service request message.

[00738] The NF service producer performs integrity verification on the access token corresponding to the first service. If the integrity verification succeeds, the NF service producer further verifies claims in the access token corresponding to the first service. For details, refer to related content of verification on the claims in the access token.

[00739] If the fourth service request message includes the CCA 3, the NF service producer further needs to authenticate the NF service consumer based on the CCA 3. The NF service producer verifies the signature of the CCA 3, verifies, based on the timestamp and/or the expiration time of the CCA 3, whether the CCA 3 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 3 matches an NF instance ID in a certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether the first NF type included in the CCA 3 matches the NF type of the

NF service producer. Because the first NF type matches the NF type of the NF service producer, it is determined that the authentication on the NF service consumer succeeds.

[00740] If the fourth service request message includes the CCA 4, the NF service producer further needs to authenticate the NF service consumer based on the CCA 4. The NF service producer verifies the signature of the CCA 4, verifies, based on the timestamp and/or the expiration time of the CCA 4, whether the CCA 4 expires, and verifies whether the NF instance ID of the NF service consumer in the CCA 4 matches an NF instance ID in a certificate for signing the CCA. In addition to successful verification of all the foregoing verification content, the NF service producer further needs to verify whether the first NF type and the second NF type that are included in the CCA 4 include an NF type matching the NF type of the NF service producer. Because the first NF type matches the NF type of the NF service producer, it is determined that the authentication based on the CCA 4 succeeds.

[00741] Step 2013: If the NF service producer determines that the verification on the first access token succeeds and the authentication on the NF service consumer succeeds, the NF service producer sends a response message for the fourth service request message to the SCP. The response message for the fourth service request message indicates to provide the first service or indicates that a fourth service request succeeds.

[00742] It may be understood that if the verification on the first access token fails and/or the authentication on the NF service consumer fails, the response message for the fourth service request message indicates that a first service request fails.

[00743] Step 2014: The SCP receives the response message for the fourth service request message from the NF service producer, and sends the response message for the first service request message to the NF service consumer.

[00744] In the foregoing embodiment, the SCP sends the client credentials assertion request message to the NF service consumer, where the client credentials assertion request message includes the indication information, and the NF service consumer responds to the client credentials assertion request message based on the indication information. The response message for the client credentials assertion request message carries the CCA 3 (the second NF type) or the CCA 4 (the first NF type and the second NF type), to ensure that the NF service consumer obtains the first service.

[00745] FIG. 21 is a block diagram of a possible example of an apparatus according to an embodiment of this application. The apparatus 2100 includes a transceiver module 2110 and a processing module 2120. The transceiver module 2110 may include a receiving unit and a sending unit. The processing module 2120 is configured to control and manage an action of the apparatus 2100. The transceiver module 2110 is configured to support the apparatus 2100 in communicating

with another network entity. Optionally, the apparatus 2100 may further include a storage unit, and the storage unit is configured to store program code and data of the apparatus 2100.

[00746] Optionally, each module in the apparatus 2100 may be implemented by using software.

[00747] Optionally, the processing module 2120 may be a processor or a controller, for example, may be a general-purpose central processing unit (central processing unit, CPU), a general-purpose processor, a digital signal processor (digital signal processor, DSP), an application-specific integrated circuit (application-specific integrated circuit, ASIC), a field programmable gate array (field programmable gate array, FPGA) or another programmable logic device, a transistor logic device, a hardware component, or any combination thereof. The processor or controller may implement or execute various example logical blocks, modules, and circuits described with reference to content disclosed in embodiments of this application. The processor may be a combination of processors implementing a computing function, for example, a combination of one or more microprocessors, or a combination of the DSP and a microprocessor. The transceiver module 2110 may be a communication interface, a transceiver, a transceiver circuit, or the like. The communication interface is a general name. In specific implementation, the communication interface may include a plurality of interfaces, and the storage unit may be a memory.

[00748] When the apparatus 2100 is a service consumer network element or a chip in the service consumer network element, the processing module 2120 in the apparatus 2100 may support the apparatus 2100 in performing the actions of the service consumer network element in the foregoing method examples, for example, may support the apparatus 2100 in performing step 1401 in FIG. 14, step 1501 in FIG. 15, step 1601 in FIG. 16, step 1701 in FIG. 17, step 1801 in FIG. 18, step 1901 in FIG. 19A, and step 2001 in FIG. 20A.

[00749] The transceiver module 2110 may support communication between the apparatus 2100 and a service communication proxy (for example, an SCP). For example, the transceiver module 2110 may support the apparatus 2100 in performing step 801 and step 808 in FIG. 8, step 901, step 905, and step 906 in FIG. 9, step 1001 and step 1008 in FIG. 10, step 1101 and step 1108 in FIG. 11, step 1201, step 1205, step 1206, and step 1213 in FIG. 12, step 1302 and step 1309 in FIG. 13, step 1402 and step 1409 in FIG. 14, step 1502 and step 1509 in FIG. 15, step 1602 and step 1606 in FIG. 16, step 1702 and step 1709 in FIG. 17, step 1802 and step 1809 in FIG. 18, step 1902, step 1906, step 1907, step 1914 in FIG. 19A and FIG. 19B, and step 2002, step 2006, step 2007, and step 2014 in FIG. 20A and FIG. 20B.

[00750] For example, details may be as follows:

[00751] In an implementation, the apparatus 2100 further includes:

the transceiver module 2110 sends a first service request message to the service communication proxy, and the service consumer network element receives a response message for

the first service request message from the service communication proxy, where the first service request message is used to request a first service from a service producer network element, the first service request message includes a first client credentials assertion, the first client credentials assertion is used to authenticate the service consumer network element, the first client credentials assertion includes a first network function type and a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service.

[00752] In a possible implementation, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service.

[00753] In a possible implementation, the processing module 2120 is configured to determine, by using the service consumer network element, that there is no available access token corresponding to the first service.

[00754] In a possible implementation, the processing module 2120 is configured to: determine that the access token corresponding to the first service is not stored; or determine that a stored access token corresponding to the first service expires.

[00755] In a possible implementation, the second service is used to provide information about the service producer network element.

[00756] In a possible implementation, the processing module 2120 is configured to determine that the first service request message triggers the service communication proxy to request the second service.

[00757] In a possible implementation, the processing module 2120 is configured to: determine, based on one or more of the following cases, that the first service request message triggers the service communication proxy to request the second service: context of a first terminal device is not stored and the first terminal device is associated with the first service; context of the first service is not stored; the service producer network element belongs to a first slice and context corresponding to the first slice is not stored; or the service consumer network element communicates with the service communication proxy for the first time.

[00758] In a possible implementation, the processing module 2120 is configured to determine to request the first service in an indirect communication mode, namely, a mode D.

[00759] In a possible implementation, the transceiver module 2110 is configured to: send a second service request message to the service communication proxy, where the second service request message is used to request the first service, the second service request message includes a second client credentials assertion, the second client credentials assertion includes the first network

function type, and the second client credentials assertion is used to authenticate the service consumer network element; and receive a response message for the second service request message from the service communication proxy, where the response message for the second service request message includes indication information. The processing module 2120 is configured to send, by using the transceiver module 2110, the first service request message to the service communication proxy based on the indication information.

[00760] It should be understood that the apparatus 2100 in this embodiment of this application may correspond to the service consumer network element in the foregoing method embodiment, for example, the method in FIG. 8. In addition, operations and/or functions of modules in the apparatus 2100 are respectively used to implement corresponding steps of the method of the service consumer network element in the foregoing method embodiment. Therefore, beneficial effect in the foregoing method embodiment can also be achieved. For brevity, details are not described herein again.

[00761] When the apparatus 2100 is a first network element or a chip in the first network element, the processing module 2120 in the apparatus 2100 may support the apparatus 2100 in performing the actions of the network repository function network element or the service producer network element in the foregoing method examples.

[00762] For example, when the first network element is a network repository function network element, the first network element may support the apparatus 2100 in performing step 803 in FIG. 8, step 903 in FIG. 9, step 1003 in FIG. 10, step 1103 in FIG. 11, step 1203 and step 1208 in FIG. 12, step 1304 in FIG. 13, step 1404 in FIG. 14, step 1504 in FIG. 15, step 1704 in FIG. 17, step 1804 in FIG. 18, step 1904 and step 1909 in FIG. 19A, and step 2004 and step 2009 in FIG. 20A. The transceiver module 2110 may support communication between the apparatus 2100 and a service communication proxy (for example, an SCP). For example, the transceiver module 2110 may support the apparatus 2100 in performing step 802, step 804, and step 808 in FIG. 8, step 902 and step 904 in FIG. 9, step 1002 and step 1004 in FIG. 10, step 1102 and step 1104 in FIG. 11, step 1202, step 1204, step 1207, and step 1209 in FIG. 12, step 1303 and step 1305 in FIG. 13, step 1403 and step 1405 in FIG. 14, step 1503 and step 1505 in FIG. 15, step 1703 and step 1705 in FIG. 17, step 1803 and step 1805 in FIG. 18, step 1903, step 1905, step 1908, and step 1910 in FIG. 19A and FIG. 19B, and step 2003, step 2005, step 2008, and step 2010 in FIG. 20A and FIG. 20B.

[00763] For example, when the first network element is a service producer network element, the first network element may support the apparatus 2100 in performing step 803 in FIG. 8, step 1006 in FIG. 10, step 1106 in FIG. 11, step 1211 in FIG. 12, step 1307 in FIG. 13, step 1407 in FIG. 14, step 1507 in FIG. 15, step 1604 in FIG. 16, step 1707 in FIG. 17, step 1807 in FIG. 18,

step 1912 in FIG. 19B, and step 2012 in FIG. 20B. The transceiver module 2110 may support communication between the apparatus 2100 and a service communication proxy (for example, an SCP). For example, the transceiver module 2110 may support the apparatus 2100 in performing step 805, step 807, and step 808 in FIG. 8, step 1005 and step 1007 in FIG. 10, step 1105 and step 1107 in FIG. 11, step 1210 and step 1212 in FIG. 12, step 1306 and step 1308 in FIG. 13, step 1406 and step 1408 in FIG. 14, step 1506 and step 1508 in FIG. 15, step 1603 and step 1605 in FIG. 16, step 1706 and step 1708 in FIG. 17, step 1806 and step 1808 in FIG. 18, step 1911 and step 1913 in FIG. 19B, and step 2011 and step 2013 in FIG. 20B.

[00764] For example, details may be as follows:

[00765] In an implementation, the apparatus 2100 further includes:

the transceiver module 2110 is configured to receive a first service request message from the service communication proxy, where the first service request message is used to request a first service from the first network element, the first service request message includes a first client credentials assertion, the first client credentials assertion is used to authenticate a service consumer network element, and the first client credentials assertion includes a plurality of network function types.

[00766] The processing module 2120 is configured to: authenticate the service consumer network element based on the first client credentials assertion; when the service consumer network element is authenticated based on the first client credentials assertion, determine whether a network function type of the processing module matches one or more of the plurality of network function types; and send, by using the transceiver module 2110, a response message for the first service request message to the service communication proxy based on an authentication result.

[00767] In a possible design, the plurality of network function types include a first network function type and a second network function type. The first network function type is the network function type of the first network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service.

[00768] In a possible design, the second service is used to provide an access token corresponding to the first service, and the access token corresponding to the first service indicates that the service consumer network element has permission to obtain the first service; or the second service is used to provide information about the first network element.

[00769] In a possible design, the first service is used to provide an access token corresponding to the second service, and the access token corresponding to the second service indicates that the service consumer network element has permission to obtain the second service; or the first service is used to provide information about a second service network element.

[00770] In a possible design, the transceiver module 2110 is configured to: receive a second service request message from the service communication proxy, where the second service request message is used to request the first service from the first network element, the second service request message includes a second client credentials assertion, and the second client credentials assertion includes a third network function type; and when the third network function type does not match the network function type of the first network element, send a response message for the second service request message to the service communication proxy, where the response message for the second service request message includes indication information, and the indication information is used to trigger the first service request message.

[00771] It should be understood that the apparatus 2100 in this embodiment of this application may correspond to the method of the first network element (for example, the network repository function network element or the service producer network element) in the foregoing method embodiment, for example, the method in FIG. 8. In addition, operations and/or functions of modules in the apparatus 2100 are respectively used to implement corresponding steps of the method of the network repository function network element in the foregoing method embodiment, or the method in FIG. 8. In addition, operations and/or functions of the modules in the apparatus 2100 are respectively used to implement corresponding steps of the method of the service producer network element in the foregoing method embodiment. Therefore, beneficial effect in the foregoing method embodiment can also be achieved. For brevity, details are not described herein again.

[00772] When the processing module 2120 in this embodiment of this application is a processor, and the transceiver module 2110 is a transceiver, the apparatus 2100 in this embodiment of this application may be an apparatus 2200 shown in FIG. 22.

[00773] FIG. 22 is a schematic diagram of a structure of the communication apparatus 2200 according to an embodiment of this application. As shown in FIG. 22, the apparatus 2200 includes a processor 2201.

[00774] When the apparatus 2200 is a service consumer network element or a chip in the service consumer network element, in a possible implementation, when the processor 2201 is configured to invoke an interface to perform the following action: sending a first service request message to a service communication proxy. The service consumer network element receives a response message for the first service request message from the service communication proxy. The first service request message is used to request a first service from a service producer network element. The first service request message includes a first client credentials assertion. The first client credentials assertion is used to authenticate the service consumer network element. The first client credentials assertion includes a first network function type and a second network function type.

The first network function type is a network function type of the service producer network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service.

[00775] It should be understood that the apparatus 2200 may be further configured to perform another step and/or operation on the service consumer network element in the foregoing embodiments. For brevity, details are not described herein again.

[00776] When the apparatus 2200 is a first network element or a chip in the first network element, in a possible implementation, the processor 2201 is configured to invoke an interface to perform the following actions: receiving a first service request message from a service communication proxy, where the first service request message is used to request a first service from the first network element, the first service request message includes a first client credentials assertion, the first client credentials assertion is used to authenticate a service consumer network element, and the first client credentials assertion includes a plurality of network function types; authenticating the service consumer network element based on the first client credentials assertion; when the service consumer network element is authenticated based on the first client credentials assertion, determining whether a network function type of the processor matches one or more of the plurality of network function types; and sending, based on an authentication result, a response message for the first service request message to the service communication proxy.

[00777] It should be understood that the apparatus 2200 may be further configured to perform another step and/or operation on the first network element in the foregoing embodiments. For brevity, details are not described herein again.

[00778] It should be understood that the processor 2201 may invoke the interface to perform the foregoing receiving and sending actions. The invoked interface may be a logical interface or a physical interface. This is not limited. Optionally, the physical interface may be implemented by using a transceiver. Optionally, the apparatus 2200 further includes a transceiver 2203.

[00779] Optionally, the apparatus 2200 further includes a memory 2202. The memory 2202 may store program code in the foregoing method embodiments, so that the processor 2201 invokes the program code.

[00780] Specifically, if the apparatus 2200 includes the processor 2201, the memory 2202, and the transceiver 2203, the processor 2201, the memory 2202, and the transceiver 2203 communicate with each other through an internal connection path, to transfer a control signal and/or a data signal. In a possible design, the processor 2201, the memory 2202, and the transceiver 2203 may be implemented by using a chip. The processor 2201, the memory 2202, and the transceiver 2203 may be implemented in a same chip, or may be respectively implemented in different chips, or any two of the functions are combined and implemented in one chip. The memory 2202 may store the

program code, and the processor 2201 invokes the program code stored in the memory 2202, to implement a corresponding function of the apparatus 2200.

[00781] The methods disclosed in embodiments of this application may be applied to a processor or may be implemented by a processor. The processor may be an integrated circuit chip with a signal processing capability. In an implementation process, the steps in the foregoing method embodiments may be completed by using a hardware integrated logical circuit in the processor, or by using instructions in a form of software. The foregoing processor may be a general-purpose processor, a digital signal processor (digital signal processor, DSP), an application-specific integrated circuit (application-specific integrated circuit, ASIC), a field-programmable gate array (field-programmable gate array, FPGA) or another programmable logic device, a discrete gate or transistor logic device, a discrete hardware component, or may be a system on chip (system on chip, SoC), may be a central processing unit (central processing unit, CPU), may be a network processor (network processor, NP), may be a digital signal processor (digital signal processor, DSP), may be a micro controller unit (micro controller unit, MCU), or may be a programmable logic device (programmable logic device, PLD) or another integrated chip. The processor may implement or perform the methods, the steps, and logical block diagrams that are disclosed in embodiments of this application. The general-purpose processor may be a microprocessor, or the processor may be any conventional processor or the like. The steps of the methods disclosed with reference to embodiments of this application may be directly performed and completed by a hardware decoding processor, or may be performed and completed by a combination of hardware and software modules in the decoding processor. The software module may be located in a mature storage medium in the art, such as a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically erasable programmable memory, or a register. The storage medium is located in the memory, and the processor reads information in the memory and completes the steps in the foregoing methods in combination with hardware of the processor.

[00782] It may be understood that the memory in embodiments of this application may be a volatile memory or a nonvolatile memory, or may include both a volatile memory and a nonvolatile memory. The nonvolatile memory may be a read-only memory (read-only memory, ROM), a programmable read-only memory (programmable ROM, PROM), an erasable programmable read-only memory (erasable PROM, EPROM), an electrically erasable programmable read-only memory (electrically EPROM, EEPROM), or a flash memory. The volatile memory may be a random access memory (random access memory, RAM), and is used as an external cache. By way of example but not limitative description, many forms of RAMs may be used, for example, a static random access memory (static RAM, SRAM), a dynamic random access memory (dynamic RAM,

DRAM), a synchronous dynamic random access memory (synchronous DRAM, SDRAM), a double data rate synchronous dynamic random access memory (double data rate SDRAM, DDR SDRAM), an enhanced synchronous dynamic random access memory (enhanced SDRAM, ESDRAM), a synchronous link dynamic random access memory (synchlink DRAM, SLDRAM), and a direct rambus random access memory (direct rambus RAM, DR RAM). It should be noted that the memory in the system and the method described in this specification includes but is not limited to these memories and any memory of another proper type.

[00783] It should be understood that in embodiments of this application, numbers "first", "second", and the like are merely used to distinguish between different objects, for example, to distinguish between different parameter information or messages, and do not constitute a limitation on the scope of embodiments of this application. Embodiments of this application are not limited thereto.

[00784] It should be further understood that sequence numbers of the foregoing processes do not mean execution sequences in embodiments of this application. The execution sequences of the processes should be determined based on functions and internal logic of the processes. Numbers or sequence numbers in the foregoing processes are merely for differentiation for ease of description, and should not constitute any limitation on an implementation process of embodiments of this application.

[00785] It should also be understood that the term "and/or" in this specification describes only an association relationship between associated objects and represents that three relationships may exist. For example, A and/or B may represent the following three cases: Only A exists, both A and B exist, and only B exists. In addition, the character "/" in this specification generally indicates an "or" relationship between the associated objects.

[00786] Unless otherwise specified, an expression used in this application similar to an expression that "an item includes one or more of the following: A, B, and C" usually means that the item may be any one of the following: A; B; C; A and B; A and C; B and C; A, B, and C; A and A; A, A, and A; A, A, and B; A, A, and C; A, B, and B; A, C, and C; B and B; B, B and B; B, B and C; C and C; C, C, and C; and another combination of A, B and C. In the foregoing descriptions, three elements A, B, and C are used as an example to describe an optional case of the item. When an expression is "the item includes at least one of the following: A, B, …, and X", in other words, more elements are included in the expression, a case to which the item is applicable may also be obtained according to the foregoing rule.

[00787] A person of ordinary skill in the art may be aware that, with reference to the examples described in embodiments disclosed in this specification, units and algorithm steps can be implemented by electronic hardware or a combination of computer software and electronic

hardware. Whether the functions are performed by hardware or software depends on particular applications and design constraint conditions of the technical solutions. A person skilled in the art may use different methods to implement the described functions for each particular application, but it should not be considered that the implementation goes beyond the scope of this application.

[00788] It may be clearly understood by a person skilled in the art that, for the purpose of convenient and brief description, for a detailed working process of the foregoing system, apparatus, and unit, refer to a corresponding process in the foregoing method embodiments. Details are not described herein again.

[00789] In the several embodiments provided in this application, it should be understood that the disclosed system, apparatus, and method may be implemented in another manner. For example, the described apparatus embodiments are merely examples. For example, division into the units is merely logical function division. There may be another division manner during actual implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings or direct couplings or communication connections may be implemented through some interfaces. The indirect couplings or communication connections between the apparatuses or units may be implemented in an electronic form, a mechanical form, or another form.

[00790] The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, may be located in one position, or may be distributed on a plurality of network units. Some or all of the units may be selected according to actual requirements to achieve the objectives of the solutions of the embodiments.

[00791] In addition, functional units in embodiments of this application may be integrated into one processing unit, each of the units may exist alone physically, or two or more units are integrated into one unit.

[00792] When the functions are implemented in the form of a software functional unit and sold or used as an independent product, the functions may be stored in a computer-readable storage medium. Based on such an understanding, the technical solutions of this application essentially, or the part contributing to the conventional technology, or some of the technical solutions may be implemented in a form of a software product. The computer software product is stored in a storage medium, and includes several instructions for instructing a computer device (which may be a personal computer, a server, a network device, or the like) to perform all or some of the steps of the methods described in embodiments of this application. The foregoing storage medium includes: any medium that can store program code, such as a USB flash drive, a removable hard disk, a read-only memory ROM, a random access memory RAM, a magnetic disk, or an optical disc.

[00793] The foregoing descriptions are merely specific implementations of this application, but are not intended to limit the protection scope of this application. Any variation or replacement readily figured out by a person skilled in the art within the technical scope disclosed in this application shall fall within the protection scope of this application. Therefore, the protection scope of this application shall be subject to the protection scope of the claims.

CLAIMS

What is claimed is:

1. A communication method, wherein the method comprises:

sending, by a service consumer network element, a first service request message to a service communication proxy, wherein the first service request message is used to request a first service from a service producer network element, the first service request message comprises a first client credentials assertion, the first client credentials assertion is used to authenticate the service consumer network element, the first client credentials assertion comprises a first network function type and a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of a network element providing a second service, wherein the second service is used to provide information about the service producer network element; and

receiving, by the service consumer network element, a response message for the first service request message from the service communication proxy.

2. The method according to claim 1, further comprising:

determining, by the service consumer network element, that the first service request message triggers the service communication proxy to request the second service.

3. The method according to claim 2, wherein the determining, by the service consumer network element, that the first service request message triggers the service communication proxy to request the second service comprises:

determining, by the service consumer network element based on one or more of the following:

context of a first terminal device is not stored and the first terminal device is associated with the first service;

context of the first service is not stored;

the service producer network element belongs to a first slice and context corresponding to the first slice is not stored; or

the service consumer network element communicates with the service communication proxy for the first time.

4. The method according to any one of claims 1 to 3, further comprising:

determining, by the service consumer network element, to request the first service in an indirect communication mode, namely, a mode D.

5. The method according to any one of claims 1 to 4, further comprising:

sending, by the service consumer network element, a second service request message to the service communication proxy, wherein the second service request message is used to request the

first service, the second service request message comprises a second client credentials assertion, the second client credentials assertion comprises the first network function type, and the second client credentials assertion is used to authenticate the service consumer network element; and

receiving, by the service consumer network element, a response message for the second service request message from the service communication proxy, wherein the response message for the second service request message comprises indication information; and

the sending, by a service consumer network element, a first service request message to a service communication proxy comprises:

sending, by the service consumer network element, the first service request message to the service communication proxy based on the indication information.

6. The method according to claim 5, wherein the indication information comprises a third client credentials assertion, the third client credentials assertion comprises the second network function type, and the third client credentials assertion is used to authenticate the network element providing the second service; and

the sending, by the service consumer network element, the first service request message to the service communication proxy based on the indication information comprises:

sending, by the service consumer network element, the first service request message to the service communication proxy when the authentication, based on the third client credentials assertion, on the network element providing the second service succeeds.

7. The method according to any one of claims 1 to 6, wherein the network element providing the second service is a network repository function network element.

8. The method according to any one of claims 1 to 7, wherein the first client credentials assertion further comprises one or more of the following:

an identifier of the service consumer network element or validity time information, wherein the validity time information represents validity time of the first client credentials assertion.

9. A communication apparatus, comprising:

a memory storing instructions and

a processor configured to execute the instructions to cause the apparatus to:

send a first service request message to a service communication proxy, wherein the first service request message is used to request a first service from a service producer network element, the first service request message comprises a first client credentials assertion, the first client credentials assertion is used to authenticate the apparatus, the first client credentials assertion comprises a first network function type and a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of a network element providing a second service,

wherein the second service is used to provide information about the service producer network element; and

receive a response message for the first service request message from the service communication proxy.

10. The communication apparatus according to claim 9, wherein the instructions, when executed by the processor, further cause the apparatus to determine that the first service request message triggers the service communication proxy to request the second service.

11. The communication apparatus according to claim 9 or 10, wherein the instructions, when executed by the processor, further cause the apparatus to determine to request the first service in an indirect communication mode, namely, a mode D.

12. The communication apparatus according to any one of claims 9 to 11, wherein the network element providing the second service is a network repository function network element.

13. The communication apparatus according to any one of claims 9 to 12, wherein the first client credentials assertion further comprises one or more of the following:

an identifier of the apparatus or validity time information, wherein the validity time information represents validity time of the first client credentials assertion.

14. A computer-readable storage medium, wherein the storage medium stores a computer program or instructions, and when the computer program or the instructions are executed by a communication apparatus, the method according to any one of claims 1 to 8 is implemented.

15. A communication system, comprising a service consumer network element and a service communication proxy, wherein

the service consumer network element is configured to send a first service request message to the service communication proxy, wherein the first service request message is used to request a first service from a service producer network element, the first service request message comprises a first client credentials assertion, the first client credentials assertion is used to authenticate the service consumer network element, the first client credentials assertion comprises a first network function type and a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service;

the service communication proxy is configured to: receive the first service request message, and send a response message for the first service request message to the service consumer network element; and

the service consumer network element is further configured to receive the response message for the first service request message from the service communication proxy.

16. The system according to claim 15, wherein the service consumer network element is further configured to determine that the first service request message triggers the service communication proxy to request the second service.

17. The system according to claim 15 or 16, wherein the service consumer network element is further configured to determine to request the first service in an indirect communication mode, namely, a mode D.

18. The system according to any one of claims 15 to 17, wherein the system further comprises the network element providing the second service;

the service communication proxy is further configured to: after receiving the first service request message from the service consumer network element, send a second service request message to the network element providing the second service, wherein the second service request message is used to request the second service, and the second service request message comprises the first client credentials assertion; and

the network element providing the second service is configured to: receive the second service request message from the service communication proxy, and authenticate the service consumer network element based on the first client credentials assertion, wherein authenticating the service consumer network element based on the first client credentials assertion comprises: determining whether the network function type of the network element providing the second service matches one or more of the first network function type and the second network function type, and when the authentication on the service consumer network element succeeds, sending a response message for the second service request message to the service communication proxy, wherein the response message for the second service request message indicates to provide the second service.

19. The system according to claim 18, wherein the first client credentials assertion further comprises one or more of the following: an identifier of the service consumer network element or validity time information, wherein the validity time information represents validity time of the first client credentials assertion; and

that the network element providing the second service is configured to authenticate the service consumer network element based on the first client credentials assertion further comprises one or more of the following:

verifying whether a signature of the first client credentials assertion succeeds, verifying, based on the validity time information comprised in the first client credentials assertion, whether the first client credentials assertion expires, or verifying whether the identifier of the service consumer network element in the first client credentials assertion is the same as an identifier of a network element in a certificate for signing the first client credentials assertion.

20. The system according to any one of claims 15 to 19, wherein the network element

providing the second service is a network repository function network element.

21. The system according to any one of claims 15 to 20, wherein the second service is used to provide information about the service producer network element.

22. The system according to any one of claims 18 to 21, wherein the system further comprises the service producer network element;

the service communication proxy is further configured to: when the authentication on the service consumer network element succeeds, receive the response message for the second service request message from the network element providing the second service; and send a third service request message to the service producer network element based on the response message for the second service request message, wherein the third service request message is used to request the first service, and the third service request message comprises the first client credentials assertion; and

the service producer network element is configured to: receive the third service request message from the service communication proxy, and authenticate the service consumer network element based on the first client credentials assertion, wherein authenticating the service consumer network element based on the first client credentials assertion comprises: determining whether the network function type of the service producer network element matches one or more of the first network function type and the second network function type, and when the authentication on the service consumer network element succeeds, sending a response message for the third service request message to the service communication proxy, wherein the response message for the third service request message indicates to provide the first service.

23. The system according to claim 22, wherein the first client credentials assertion further comprises one or more of the following: the identifier of the service consumer network element or the validity time information, wherein the validity time information represents the validity time of the first client credentials assertion; and

that the service producer network element is configured to authenticate the service consumer network element based on the first client credentials assertion further comprises one or more of the following:

verifying whether the signature of the first client credentials assertion succeeds, verifying, based on the validity time information comprised in the first client credentials assertion, whether the first client credentials assertion expires, or verifying whether the identifier of the service consumer network element in the first client credentials assertion is the same as the identifier of the network element in the certificate for signing the first client credentials assertion.

24. A communication method, wherein the method comprises:

sending, by a service consumer network element, a first service request message to a service

communication proxy, wherein the first service request message is used to request a first service from a service producer network element, the first service request message comprises a first client credentials assertion, the first client credentials assertion is used to authenticate the service consumer network element, the first client credentials assertion comprises a first network function type and a second network function type, the first network function type is a network function type of the service producer network element, the second network function type is a network function type of a network element providing a second service, and the second service is associated with the first service;

receiving, by the service communication proxy, the first service request message from the service consumer network element; and

sending, by the service communication proxy, a response message for the first service request message to the service consumer network element.

25. The method according to claim 24, wherein the second service is used to provide information about the service producer network element.

26. The method according to claim 24 or 25, further comprising:

determining, by the service consumer network element, that the first service request message triggers the service communication proxy to request the second service.

27. The method according to any one of claims 24 to 26, further comprising:

determining, by the service consumer network element, to request the first service in an indirect communication mode, namely, a mode D.

28. The method according to any one of claims 24 to 27, further comprising:

sending, by the service consumer network element, a second service request message to the service communication proxy, wherein the second service request message is used to request the first service, the second service request message comprises a second client credentials assertion, the second client credentials assertion comprises the first network function type, and the second client credentials assertion is used to authenticate the service consumer network element;

receiving, by the service communication proxy, the second service request message from the service consumer network element; and

sending, by the service communication proxy, a response message for the second service request message to the service consumer network element, wherein the response message for the second service request message comprises indication information; and

the sending, by a service consumer network element, a first service request message to a service communication proxy comprises:

sending, by the service consumer network element, the first service request message to the service communication proxy based on the indication information.

29. The method according to claim 28, wherein the indication information comprises a third client credentials assertion, the third client credentials assertion comprises the second network function type, and the third client credentials assertion is used to authenticate the network element providing the second service; and

the sending, by the service consumer network element, the first service request message to the service communication proxy based on the indication information comprises:

sending, by the service consumer network element, the first service request message to the service communication proxy when the authentication, based on the third client credentials assertion, on the network element providing the second service succeeds.

30. The method according to any one of claims 24 to 29, wherein the network element providing the second service is a network repository function network element.

31. The method according to any one of claims 24 to 30, wherein the first client credentials assertion further comprises one or more of the following: an identifier of the service consumer network element or validity time information, wherein the validity time information represents validity time of the first client credentials assertion.