

CLAIMS

What is claimed is:

1. An authentication method, comprising:

receiving a first registration request message from a terminal device;

5 sending an authentication vector request message to a home subscriber server;

receiving an authentication vector request response from the home subscriber server, wherein the authentication vector request response comprises a first hash value of a security parameter and a second hash value of the security parameter, the first hash value is calculated based on a first security algorithm, and the second hash value is calculated based on a second security algorithm;

10 sending an authentication challenge request message to the terminal device, wherein the authentication challenge request message comprises information about the first security algorithm and information about the second security algorithm;

receiving a second registration request message from the terminal device, wherein the second registration request message comprises a first authentication response and information about a third security algorithm, the first authentication response is calculated based on the third security algorithm, and the third security algorithm is the first security algorithm or the second security algorithm;

selecting, from the first hash value and the second hash value, a hash value corresponding to the third security algorithm;

20 calculating a second authentication response based on the third security algorithm and the hash value corresponding to the third security algorithm; and

checking the first authentication response by using the second authentication response, to obtain an authentication result of the terminal device.

2. The method according to claim 1, wherein the first hash value and the second hash value are in the authentication vector request response in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm; and

wherein selecting the hash value corresponding to the third security algorithm comprises: selecting, based on the preset order of the first hash value and the second hash value, the hash value corresponding to the third security algorithm.

30

3. The method according to claim 1, wherein the information about the first security algorithm and the information about the second security algorithm are comprised in the authentication challenge request message in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm.

5 4. The method according to claim 1, wherein the first security algorithm is a secure hash algorithm (SHA)256 or a secure hash algorithm (SHA)512, and the second security algorithm is a message digest 5 algorithm.

5. An authentication method, comprising:

10 sending a first registration request message to a serving call session control function network element;

 receiving an authentication challenge request message from the serving call session control function network element, wherein the authentication challenge request message carries information about a first security algorithm and information about a second security algorithm;

15 determining, as a third security algorithm, the first security algorithm or the second security algorithm;

 calculating a hash value of a security parameter based on the third security algorithm;

 calculating an authentication response based on the third security algorithm and the hash value; and

20 sending a second registration request message to the serving call session control function network element, wherein the second registration request message carries the authentication response and information about the third security algorithm, and the authentication response is used to authenticate a terminal device.

25 6. The method according to claim 5, wherein the authentication challenge request message comprises the information about the first security algorithm and the information about the second security algorithm that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm.

30 7. The method according to claim 6, wherein when the priority of the first security algorithm is higher than the priority of the second security algorithm, the information about the first security algorithm is located before the information about the second security algorithm in the authentication challenge request message.

8. The method according to claim 7, wherein the determining, as the third security algorithm,

the first security algorithm or the second security algorithm comprises: determining, as the third security algorithm, a 1st security algorithm that is supported by the terminal device and that is in the authentication challenge request message.

9. The method according to claim 6, wherein the determining, as the third security algorithm, the first security algorithm or the second security algorithm comprises: determining, as the third security algorithm, a 1st security algorithm that is supported by the terminal device and that is in the authentication challenge request message.

10. The method according to claim 5, wherein the first security algorithm is a secure hash algorithm (SHA)256, and the second security algorithm is a message digest 5 algorithm.

11. The method according to claim 5, wherein the security parameter comprises a login username, a password, and realm information of the terminal device.

12. The method according to claim 5, wherein the method is performed by the terminal device or a chip applied to the terminal device.

13. A communication apparatus, comprising at least one processor and one or more memories coupled to the at least one processor and storing programming instructions for execution by the at least one processor to perform the method according to any one of claims 1 to 4.

14. A communication apparatus, comprising at least one processor and one or more memories coupled to the at least one processor and storing programming instructions for execution by the at least one processor to perform the method according to any one of claims 5 to 12.

15. A computer-readable storage medium, wherein the computer-readable storage medium stores computer instructions, and when the computer instructions are run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 12.

16. A computer program product, wherein when the computer program product runs on a computer, the computer is enabled to perform the method according to any one of claims 1 to 12.

17. A chip, comprising a processing circuit and a transceiver pin, wherein the processing circuit is configured to perform a processing operation in the method according to any one of claims 1 to 12, and the transceiver pin is configured to perform a communication operation in the method according to any one of claims 1 to 12.

18. An authentication method, comprising:
receiving, by a serving call session control function network element, a first registration request message from a terminal device;

sending, by the serving call session control function network element, an authentication vector request message to a home subscriber server;

receiving, by the home subscriber server, the authentication vector request message;

calculating, by the home subscriber server, a first hash value of a security parameter based on
5 a first security algorithm;

calculating, by the home subscriber server, a second hash value of the security parameter based on a second security algorithm;

sending, by the home subscriber server, an authentication vector request response to the serving call session control function network element, wherein the authentication vector request
10 response comprises the first hash value and the second hash value;

receiving, by the serving call session control function network element, the authentication vector request response;

sending, by the serving call session control function network element, an authentication challenge request message to the terminal device, wherein the authentication challenge request
15 message comprises information about the first security algorithm and information about the second security algorithm;

receiving, by the serving call session control function network element, a second registration request message from the terminal device, wherein the second registration request message comprises a first authentication response and information about a third security algorithm, the first
20 authentication response is calculated based on the third security algorithm, and the third security algorithm is the first security algorithm or the second security algorithm;

selecting, by the serving call session control function network element, from the first hash value and the second hash value, a hash value corresponding to the third security algorithm;

calculating, by the serving call session control function network element, a second
25 authentication response based on the third security algorithm and the hash value corresponding to the third security algorithm; and

checking, by the serving call session control function network element, the first authentication response by using the second authentication response, to obtain an authentication result of the terminal device.

30 19. The method according to claim 18, wherein the information about the first security algorithm and the information about the second security algorithm are comprised in the

authentication challenge request message in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm.

20. The method according to claim 18, wherein the first security algorithm is a secure hash algorithm (SHA)256 or a secure hash algorithm (SHA)512, and the second security algorithm is a message digest 5 algorithm.

21. The method according to claim 18, further comprising:

sending, by the terminal device, the first registration request message to the serving call session control function network element;

receiving, by the terminal device, the authentication challenge request message from the serving call session control function network element;

determining, by the terminal device, the third security algorithm;

calculating, by the terminal device, a hash value of the security parameter based on the third security algorithm;

calculating, by the terminal device, the first authentication response based on the third security algorithm and the hash value; and

sending, by the terminal device, the second registration request message to the serving call session control function network element.

22. The method according to claim 21, wherein the determining, by the terminal device, the third security algorithm comprises: determining, by the terminal device, as the third security algorithm, a 1st security algorithm that is supported by the terminal device and that is in the authentication challenge request message.

23. A system, comprising a serving call session control function network element and a home subscriber server, wherein:

the serving call session control function network element is configured to:

receive a first registration request message from a terminal device; and

send an authentication vector request message to the home subscriber server;

the home subscriber server is configured to:

receive the authentication vector request message;

calculate a first hash value of a security parameter based on a first security algorithm;

calculate a second hash value of the security parameter based on a second security algorithm;

and

send an authentication vector request response to the serving call session control function network element, wherein the authentication vector request response comprises the first hash value and the second hash value;

the serving call session control function network element is further configured to:

5 receive the authentication vector request response;

send an authentication challenge request message to the terminal device, wherein the authentication challenge request message comprises information about the first security algorithm and information about the second security algorithm;

10 receive a second registration request message from the terminal device, wherein the second registration request message comprises a first authentication response and information about a third security algorithm, the first authentication response is calculated based on the third security algorithm, and the third security algorithm is the first security algorithm or the second security algorithm;

15 select, from the first hash value and the second hash value, a hash value corresponding to the third security algorithm;

calculate a second authentication response based on the third security algorithm and the hash value corresponding to the third security algorithm; and

check the first authentication response by using the second authentication response, to obtain an authentication result of the terminal device.

20 24. The system according to claim 23, wherein the information about the first security algorithm and the information about the second security algorithm are comprised in the authentication challenge request message in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm.

25 25. The system according to claim 23, wherein the first security algorithm is a secure hash algorithm (SHA)256 or a secure hash algorithm (SHA)512, and the second security algorithm is a message digest 5 algorithm.

26. The system according to claim 23, further comprising the terminal device, wherein the terminal device is configured to:

30 send the first registration request message to the serving call session control function network element;

receive the authentication challenge request message from the serving call session control

function network element;

determine the third security algorithm;

calculate a hash value of the security parameter based on the third security algorithm;

calculate the first authentication response based on the third security algorithm and the hash

5 value; and

send the second registration request message to the serving call session control function network element.