

CLAIMS

What is claimed is:

1. A key obtaining method, comprising:

5 sending, by a communication apparatus~~remote terminal device~~, a first identifier and a relay service code to a relay terminal device, wherein ~~the first identifier is an identifier that is of the remote terminal device and that is corresponding to the relay service code, or~~ the first identifier is an anonymous identifier of ~~the~~a remote terminal device; and

generating, by the communication apparatus~~remote terminal device~~ based on a first shared key, the relay service code, and at least one first freshness parameter, a root key for communication
10 between the remote terminal device and the relay terminal device, wherein a remote authentication service function network element is an authentication service function network element that serves the remote terminal device, and the first shared key is a key shared between the remote terminal device and the remote authentication service function network element.

2. The method according to claim 1, wherein the first identifier is a subscription concealed
15 identifier SUCI of the remote terminal device.

~~3. The method according to claim 1, wherein the method further comprises:~~

~~obtaining, by the remote terminal device, the first identifier.~~

~~4. The method according to claim 3, wherein the obtaining, by the remote terminal device, the first identifier comprises:~~

20 ~~sending, by the remote terminal device, the relay service code; and~~

~~receiving, by the remote terminal device, the first identifier corresponding to the relay service code.~~

~~5. The method according to claim 3, wherein the method further comprises:~~

25 ~~generating, by the remote terminal device, a temporary identifier based on the first shared key and the relay service code; and~~

~~obtaining, by the remote terminal device, the first identifier based on the temporary identifier.~~

~~6. The method according to claim 5, wherein the generating, by the remote terminal device, a temporary identifier based on the first shared key and the relay service code comprises:~~

30 ~~generating, by the remote terminal device, the temporary identifier based on the first shared key, the relay service code, and a second freshness parameter.~~

7. ~~The method according to claim 3, wherein the obtaining, by the remote terminal device, the first identifier comprises:~~

~~generating, by the remote terminal device, the first identifier based on a second freshness parameter, a route indication, and a home network identifier.~~

5 8. ~~The method according to claim 6 or 7, wherein the method further comprises:~~

~~sending, by the remote terminal device, the relay service code; and~~

~~receiving, by the remote terminal device, the second freshness parameter corresponding to the relay service code.~~

10 9. ~~The method according to claim 6 or 7, wherein the second freshness parameter is a value of a counter locally maintained by the remote terminal device.~~

~~10. The method according to any one of claims 3 to 9, wherein the first identifier comprises the route indication and the home network identifier.~~

15 11. ~~The method according to any one of claims 1 to 10, wherein the method further comprises: sending, by the remote terminal device, first verification information to the relay terminal device, wherein the first verification information is generated based on a first temporary key and all or some information elements of a message carrying the first verification information, and the first temporary key is generated based on the first shared key.~~

20 12. ~~The method according to claim 11, wherein the first temporary key is generated based on the first shared key and at least one of the following: the relay service code, a third freshness parameter, a second identifier of the remote terminal device, and the first identifier, and the third freshness parameter is generated by the remote terminal device.~~

25 13. ~~The method according to any one of claims 1 to 12, wherein the method further comprises: sending, by the remote terminal device, second verification information to the relay terminal device, wherein the second verification information is generated based on the first freshness parameter, the relay service code, and the first shared key.~~

143. The method according to any one of claims 1 to 13 claim 1 or 2, wherein the at least one first freshness parameter comprises a first random number, and the method further comprises:

sending, by the communication apparatus ~~remote terminal device~~, the first random number to the relay terminal device.

30 154. The method according to any one of claims 1 to 143, wherein the at least one first freshness parameter comprises a second random number, and the method further comprises:

receiving, by the communication apparatus~~remote terminal device~~, the second random number from the relay terminal device.

~~16. The method according to any one of claims 1 to 13, wherein the at least one first freshness parameter is a value of a counter locally maintained by the remote terminal device.~~

5 ~~175.~~ The method according to any one of claims 1 to ~~164~~, wherein the first shared key is a key Kausf negotiated between the remote terminal device and the remote authentication service function network element when the remote terminal device accesses a network.

~~186.~~ The method according to any one of claims 1 to ~~175~~, wherein the generating, by the communication apparatus~~remote terminal device~~ based on a first shared key, the relay service code, and at least one first freshness parameter, a root key for communication between the remote terminal device and the relay terminal device comprises:

generating, by the communication apparatus~~remote terminal device~~, a second shared key based on the first shared key and the relay service code, and

generating, by the communication apparatus, the root key based on the second shared key and the at least one first freshness parameter, wherein the second shared key is a key shared between the remote terminal device and a proximity-based services key management function network element.

7. The method according to any one of claims 1 to 6, wherein the communication apparatus is the remote terminal device, or an apparatus including the remote terminal device, or a chip in the remote terminal device or a functional module in the remote terminal device.

~~198.~~ A key obtaining method, comprising:

obtaining, by a communication apparatus~~remote authentication service function network element~~, a relay service code and ~~one of a first identifier or a second identifier of a remote terminal device, wherein the second identifier is a permanent identifier of the remote terminal device, and the first identifier is an identifier that is of the remote terminal device and that is corresponding to the relay service code;~~

obtaining, by the communication apparatus~~remote authentication service function network element~~, a first shared key corresponding to the first identifier or the second identifier, wherein the first shared key is a key shared between the remote terminal device and ~~the~~ a remote authentication service function network element;

generating, by the communication apparatus~~remote authentication service function network~~

~~element~~ based on the first shared key, the relay service code, and at least one first freshness parameter, a root key for communication between the remote terminal device and a relay terminal device; and

5 ~~sending, by the communication apparatus~~~~remote authentication service function network element~~, the root key.

9. The method according to claim 8, wherein the generating, by the communication apparatus based on the first shared key, the relay service code, and at least one first freshness parameter, a root key for communication between the remote terminal device and a relay terminal device comprises:

10 generating, by the communication apparatus, a second shared key based on the first shared key and the relay service code, and

generating, by the communication apparatus, the root key based on the second shared key and the at least one first freshness parameter, wherein the second shared key is a key shared between the remote terminal device and a proximity-based services key management function network
15 element.

10. The method according to claim 9, further comprising:

sending, by the communication apparatus, the second shared key to the proximity-based services key management function network element.

20 11. The method according to any one of claims 8 to 10, wherein the sending, by the communication apparatus, the root key comprises:

sending, by the communication apparatus, the root key to the relay terminal device.

~~20. The method according to claim 19, wherein the obtaining, by a remote authentication service function network element, one of a first identifier or a second identifier of a remote terminal~~
25 ~~device comprises:~~

~~receiving, by the remote authentication service function network element, one of the first identifier or the second identifier of the remote terminal device.~~

~~21. The method according to claim 19, wherein the obtaining, by a remote authentication service function network element, one of a first identifier or a second identifier of a remote terminal~~
30 ~~device comprises:~~

~~generating, by the remote authentication service function network element, a temporary~~

identifier based on the first shared key and the relay service code; and

generating, by the remote authentication service function network element, the first identifier based on the temporary identifier.

22. The method according to claim 21, wherein the generating, by the remote authentication service function network element, a temporary identifier based on the first shared key and the relay service code comprises:

generating, by the remote terminal device, the temporary identifier based on the first shared key, the relay service code, and a second freshness parameter.

23. The method according to claim 19, wherein the obtaining, by a remote authentication service function network element, one of a first identifier or a second identifier of a remote terminal device comprises:

generating, by the remote authentication service function network element, the first identifier based on a second freshness parameter, a route indication, and a home network identifier of the remote terminal device.

24. The method according to claim 22 or 23, wherein the second freshness parameter is a value of a counter locally maintained by the remote authentication service function network element.

25. The method according to claim 22 or 23, wherein the method further comprises:

receiving, by the remote authentication service function network element, the relay service code; and

sending, by the remote authentication service function network element, the second freshness parameter.

26. The method according to any one of claims 19 to 25, wherein the method further comprises:

receiving, by the remote authentication service function network element, the relay service code; and

sending, by the remote authentication service function network element, the first identifier.

27. The method according to any one of claims 19 to 26, wherein the first identifier comprises the route indication and the home network identifier.

28. The method according to any one of claims 19 to 27, wherein the method further comprises:

receiving, by the remote authentication service function network element, first verification information;

generating, by the remote authentication service function network element, a first temporary key based on the first shared key, and obtaining third verification information based on the first temporary key and all or some information elements of a message carrying the first verification information; and

comparing, by the remote authentication service function network element, the first verification information with the third verification information to verify the remote terminal device.

29. The method according to claim 28, wherein the generating, by the remote authentication service function network element, a first temporary key based on the first shared key comprises:

generating, by the remote authentication service function network element, the first temporary key based on the first shared key and at least one of the following: the relay service code, a third freshness parameter, the second identifier, and the first identifier of the remote terminal device, wherein the third freshness parameter is generated by the remote terminal device.

3012. The method according to any one of claims 19-8 to 2911, wherein the at least one first freshness parameter comprises a first random number, and the method further comprises:

receiving, by the communication apparatusremote authentication service function network element, the first random number.

3113. The method according to any one of claims 19-8 to 3012, wherein the at least one first freshness parameter comprises a second random number, and the method further comprises:

sending, by the communication apparatusremote authentication service function network element, the second random number.

32. The method according to any one of claims 19 to 30, wherein the at least one first freshness parameter is a value of a counter locally maintained by the remote authentication service function network element.

33. The method according to any one of claims 19 to 32, wherein the method further comprises:

sending, by the remote authentication service function network element, the first identifier to a unified data management network element.

3414. The method according to any one of claims 19-8 to 3313, wherein the first shared key is a key Kausf negotiated between the remote terminal device and the remote authentication service

function network element when the remote terminal device accesses a network.

15. The method according to any one of claims 8 to 14, wherein the communication apparatus is the remote authentication service function network element, or an apparatus including the remote authentication service function network element, or a chip in the remote authentication service function network element, or a functional module in the remote authentication service function network element

16. The method according to claim 10, further comprising:

receiving, by the proximity-based services key management function network element, the second shared key.

35. A key obtaining method, comprising:

receiving, by a proximity-based services key management function network element, a first identifier of a remote terminal device and a relay service code, wherein the first identifier is an identifier that is of the remote terminal device and that is corresponding to the relay service code, or the first identifier is an anonymous identifier of the remote terminal device;

obtaining, by the proximity-based services key management function network element based on the first identifier, a root key for communication between the remote terminal device and a relay terminal device, wherein the root key is generated based on a first shared key, the relay service code, and at least one first freshness parameter, and the first shared key is a key shared between the remote terminal device and a remote authentication service function network element; and

sending, by the proximity-based services key management function network element, the root key.

36. The method according to claim 35, wherein the obtaining, by the proximity-based services key management function network element based on the first identifier, a root key for communication between the remote terminal device and a relay terminal device comprises:

sending, by the proximity-based services key management function network element, the first identifier to a unified data management function network element;

receiving, by the proximity-based services key management function network element, identification information of the remote authentication service function network element from the unified data management function network element;

sending, by the proximity-based services key management function network element, the first identifier to the corresponding remote authentication service function network element based on

the identification information; and

receiving, by the proximity-based services key management function network element, the root key from the remote authentication service function network element.

37. The method according to claim 35, wherein the obtaining, by the proximity-based services key management function network element based on the first identifier, a root key for communication between the remote terminal device and a relay terminal device comprises:

sending, by the proximity-based services key management function network element, the first identifier to a unified data management function network element;

receiving, by the proximity-based services key management function network element, identification information of the remote authentication service function network element and a permanent identifier of the remote terminal device from the unified data management function network element;

sending, by the proximity-based services key management function network element, the permanent identifier of the remote terminal device to the corresponding remote authentication service function network element based on the identification information; and

receiving, by the proximity-based services key management function network element, the root key from the remote authentication service function network element.

38. The method according to claim 35, wherein the obtaining, by the proximity-based services key management function network element based on the first identifier, a root key for communication between the remote terminal device and a relay terminal device comprises:

receiving, by the proximity-based services key management function network element, at least one second shared key from the remote authentication service function network element, wherein the second shared key is a key shared between the remote terminal device and the proximity-based services key management function network element, and the second shared key is generated based on the first shared key and the relay service code; and

generating, by the proximity-based services key management function network element based on the second shared key corresponding to the first identifier and the at least one first freshness parameter, the root key for communication between the remote terminal device and the relay terminal device.

39. The method according to claim 38, wherein the method further comprises:

receiving, by the proximity-based services key management function network element,

second verification information;

generating, by the proximity-based services key management function network element, fourth verification information based on the first freshness parameter and the second shared key; and

5 comparing, by the proximity-based services key management function network element, the second verification information with the fourth verification information to verify the remote terminal device.

40. The method according to any one of claims 35 to 39, wherein the at least one first freshness parameter comprises a first random number, and the method further comprises:

10 receiving, by the proximity-based services key management function network element, the first random number.

41. The method according to any one of claims 35 to 40, wherein the at least one first freshness parameter comprises a second random number, and the method further comprises:

15 sending, by the proximity-based services key management function network element, the second random number.

42. The method according to any one of claims 35 to 39, wherein the at least one first freshness parameter is a value of a counter locally maintained by the proximity-based services key management function network element.

43. The method according to any one of claims 35 to 42, wherein the first shared key is a key
20 Kauf negotiated between the remote terminal device and the remote authentication service function network element when the remote terminal device accesses a network.

44. A communication apparatus, comprising a processor, wherein the process is connected to a memory, the memory is configured to store a computer program, and the processor is configured to execute the computer program stored in the memory, to enable the communication apparatus to
25 perform the method according to any one of claims 1 to 18.

45. A communication apparatus, comprising a processor, wherein the process is connected to a memory, the memory is configured to store a computer program, and the processor is configured to execute the computer program stored in the memory, to enable the communication apparatus to perform the method according to any one of claims 19 to 34.

30 46. A communication apparatus, comprising a processor, wherein the process is connected to a memory, the memory is configured to store a computer program, and the processor is configured

~~to execute the computer program stored in the memory, to enable the communication apparatus to perform the method according to any one of claims 35 to 43.~~

5 17. A computer-readable storage medium, storing a computer program, wherein when the computer program is run on a computer or a processor, the computer or the processor is enabled to perform the method according to any one of claims 1 to 7, or the method according to any one of claims 8 to 15.

10 18. A computer program product comprising instructions, wherein when the instructions are run on a computer or a processor, the computer or the processor is enabled to perform the method according to any one of claims 1 to 7, or the method according to any one of claims 8 to 15.

15 19. A system, comprising:
 a remote authentication service function network element configured to perform the method according to any one of claims 8 to 15; and
 a proximity-based services key management function network element configured to receive a second shared key.

20 20. The system according to claim 19, further comprising:
 a remote terminal device configured to perform the method according to any one of claims 1 to 7.

25 21. A communication apparatus, comprising means for performing the method according to any one of claims 1 to 7.

30 22. A communication apparatus, comprising means for performing the method according to any one of claims 8 to 15.