

## CLAIMS

1. A key obtaining method, comprising:

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

5 and

generating, by the communication apparatus 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, 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 identifier SUCI of the remote terminal device.

3. The method according to 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, the first random number to the relay terminal device.

4. The method according to any one of claims 1 to 3, wherein the at least one first freshness parameter comprises a second random number, and the method further comprises:

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

5. The method according to any one of claims 1 to 4, wherein the first shared key is a key K<sub>ausf</sub> negotiated between the remote terminal device and the remote authentication service function network element when the remote terminal device accesses a network.

25 6. The method according to any one of claims 1 to 5, wherein the generating, by the communication apparatus 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, a second shared key based on the first shared key and the relay service code, and

30

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.

5           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.

8. A key obtaining method, comprising:

obtaining, by a communication apparatus, a relay service code and or a second identifier of a  
10 remote terminal device, wherein the second identifier is a permanent identifier of the remote terminal device;

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

15           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; and

sending, by the communication apparatus, the root key.

9. The method according to claim 8, wherein the generating, by the communication apparatus  
20 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:

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

25           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.

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

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

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.

5        12. The method according to any one of claims 8 to 11, wherein the at least one first freshness parameter comprises a first random number, and the method further comprises:

receiving, by the communication apparatus, the first random number.

13. The method according to any one of claims 8 to 12, wherein the at least one first freshness parameter comprises a second random number, and the method further comprises:

10        sending, by the communication apparatus, the second random number.

14. The method according to any one of claims 8 to 13, wherein the first shared key is a key K<sub>ausf</sub> negotiated between the remote terminal device and the remote authentication service function network element when the remote terminal device accesses a network.

15        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:

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

25        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.

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.

19. A system, comprising:

30        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. The system according to claim 19, further comprising:

5 a remote terminal device configured to perform the method according to any one of claims 1 to 7.

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

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

10