CLAIMS

1. A method for generating a key for inter-device communication, comprising:

generating, by a first communication apparatus, a first temporary identifier based on a first key;

sending, by the first communication apparatus, a first request to a second communication apparatus, wherein the first request is used to establish a communication connection between the first communication apparatus and the second communication apparatus, and the first request comprises the first temporary identifier and a relay service code; and

generating, by the first communication apparatus, a shared key based on the first key and the relay service code, wherein the shared key is used to protect the communication connection between the first communication apparatus and the second communication apparatus, and the first key is a key generated by a first network element in an authentication procedure,

wherein the generating, by first communication apparatus, a first temporary identifier based on a first key comprises:

generating, by the first communication apparatus, the first temporary identifier based on the first key, a network identifier of the first communication apparatus, and routing information, wherein the network identifier of the first communication apparatus is used by a network side to identify information about the first communication apparatus, and the routing information is information used to determine a core network element related to the communication apparatus.

2. The method according to claim 1, wherein the first key is a key Kausf.

3. The method according to claim 1 or 2, wherein the generating, by the first communication apparatus, the first temporary identifier based on the first key, a network identifier of the first communication apparatus, and routing information comprises:

obtaining, by the first communication apparatus, a second temporary identifier based on the first key and the network identifier of the first communication apparatus that are used as input parameters of a first preset algorithm; and

splicing the second temporary identifier and the routing information to obtain the first temporary identifier.

4. The method according to any one of claims 1 to 3, wherein the network identifier of the first communication apparatus is a subscription permanent identifier SUPI, an international mobile

subscriber identity IMSI, or a generic public subscription identifier GPSI; and the routing information is a routing indicator.

5. The method according to any one of claims 1 to 4, wherein the method further comprises:

sending, by the first communication apparatus, a non-access stratum NAS message to a mobility management network element, wherein the NAS message comprises capability information, and the capability information indicates that the first communication apparatus supports to act as a remote communication apparatus.

6. The method according to any one of claims 1 to 5, wherein the first request further comprises a first freshness parameter; and

the generating, by the first communication apparatus, a shared key based on a second key and the relay service code comprises: generating, by the first communication apparatus, the shared key based on the second key, the relay service code, and the first freshness parameter.

7. The method according to any one of claims 1 to 6, wherein the method further comprises:

receiving, by the first communication apparatus, a security mode command from the second communication apparatus, wherein the security mode command comprises a second freshness parameter; and

the generating, by the first communication apparatus, a shared key based on a second key and the relay service code comprises: generating, by the first communication apparatus, the shared key based on the second key, the relay service code, and the second freshness parameter.

8. A method for generating a key for inter-device communication, comprising:

generating, by a first network element, a first temporary identifier based on a first key;

receiving, by the first network element, a key obtaining message from a second network element, wherein the key obtaining message comprises an identifier of a first communication apparatus and a relay service code, the identifier of the first communication apparatus comprises the first temporary identifier;

generating, by the first network element, a shared key based on the identifier of the first communication apparatus, the relay service code, and the first key, wherein the shared key is used to protect a communication connection between the first communication apparatus and a second communication apparatus, and the first key is a key generated by the first network element in an authentication procedure of the first communication apparatus; and

sending, by the first network element, the shared key to the second network element,

wherein the generating, by a first network element, a first temporary identifier based on a first key comprises:

generating, by the first network element, the first temporary identifier based on the first key, the network identifier of the first communication apparatus, and routing information, wherein the network identifier of the first communication apparatus is used by a network side to identify information about the first communication apparatus, and the routing information is information used to determine a core network element related to the first communication apparatus.

9. The method according to claim 8, wherein the generating, by the first network element, a shared key based on the identifier of the first communication apparatus, the relay service code, and a second key comprises:

obtaining, by the first network element, the second key based on the identifier of the first communication apparatus, and generating, by the first network element, the shared key based on the second key and the relay service code.

10. The method according to claim 8 or 9, wherein the first key is a key Kausf.

11. The method according to any one of claims 8 to 10, wherein the generating, by the first network element, the first temporary identifier based on the first key, the network identifier of the first communication apparatus, and routing information comprises:

obtaining, by the first network element, a second temporary identifier based on the first key and the network identifier of the first communication apparatus that are used as input parameters of a first preset algorithm; and

splicing the second temporary identifier and the routing information to obtain the first temporary identifier.

12. The method according to any one of claims 8 to 11, wherein

the network identifier of the first communication apparatus is a subscription permanent identifier SUPI, an international mobile subscriber identity IMSI, or a generic public subscription identifier GPSI; and the routing information is a routing indicator.

13. The method according to any one of claims 8 to 12, wherein the key obtaining message further comprises a first freshness parameter; and

the generating, by the first network element, a shared key based on the identifier of the first communication apparatus, the relay service code, and a second key comprises: generating, by the first network element, the shared key based on the identifier of the first communication apparatus,

the relay service code, the second key, and the first freshness parameter.

14. The method according to any one of claims 8 to 12, wherein the method further comprises:

generating, by the first network element, a second freshness parameter; and

the generating, by the first network element, a shared key based on the identifier of the first communication apparatus, the relay service code, and a second key comprises: generating, by the first network element, the shared key based on the identifier of the first communication apparatus, the relay service code, the second key, and the second freshness parameter.

15. The method according to any one of claims 8 to 14, wherein

the first network element is an authentication function network element.

16. The method according to any one of claims 8 to 15, wherein

the second network element is a mobility management network element, an authentication function network element, or a proximity-based services security function network element.

17. A communication apparatus for generating a key for inter-device communication, comprising:

a memory, configured to store computer instructions; and

a processor, configured to execute the computer instructions stored in the memory, so that the communication apparatus performs the method according to any one of claims 1 to 7.

18. A communication apparatus for generating a key for inter-device communication, comprising:

a memory, configured to store computer instructions; and

a processor, configured to execute the computer instructions stored in the memory, so that the apparatus performs the method according to any one of claims 8 to 16.

19. A system for generating a key for inter-device communication, comprising:

a first network element, configured to perform the method according to any one of claims 8 to 16; and

a second network element, configured to send a key obtaining message to the first network element, and receive a shared key from the first network element.

20. The system according to claim 19, wherein the second network element is a mobility management network element, an authentication function network element, or a proximity-based services security function network element.

21. The system according to claim 19, further comprising: the first communication apparatus

configured to perform the method according to any one of claims 1 to 7.

22. A computer-readable storage medium having instructions stored thereon which, when executed by an apparatus, cause the apparatus to perform the method of any one of 1 to 7 or 8 to 16.

23. A computer program product having instructions which, when executed by an apparatus, cause the apparatus to perform the method of any one of claims 1 to 7 or 8 to 16.

24. A method for generating a key for inter-device communication, comprising:

performing, by a first network element, the method according to any one of claims 8 to 16; and

sending, by a second network element, a key obtaining message to the first network element, and receive a shared key from the first network element.

25. The method according to claim 24, further comprising: performing, by a first communication apparatus, the method according to any one of claims 1 to 7.