CLAIMS

What is claimed is:

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

generating, by first user equipment, a first temporary identifier based on a first key;

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

generating, by the first user equipment, a shared key based on a second key and the relay service code, wherein the shared key is used to protect the communication connection between the first user equipment and the second user equipment, and the second key and the first key each are a key generated in an authentication procedure or a key obtained through derivation based on an intermediate key generated in an authentication procedure.

2. The method according to claim 1, wherein the second key is the same as the first key, and the second key and the first key each are a key Kausf generated in the authentication procedure or a key obtained through derivation based on the Kausf.

3. The method according to claim 1 or 2, wherein the generating, by first user equipment, a first temporary identifier based on a first key comprises:

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

4. The method according to claim 3, wherein the generating, by the first user equipment, the first temporary identifier based on the first key, a network identifier of the first user equipment, and routing information comprises:

obtaining, by the first user equipment, a second temporary identifier based on the first key and the network identifier of the first user equipment 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.

5. The method according to claim 3 or 4, wherein the network identifier of the first user equipment 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.

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

sending, by the first user equipment, 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 user equipment supports to act as remote user equipment.

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

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

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

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

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

9. 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 first user equipment and a relay service code, the identifier of the first user equipment comprises the first temporary identifier or a network identifier of the first user equipment, and the network identifier of the first user equipment is used by a network side to identify information about the first user equipment;

generating, by the first network element, a shared key based on the identifier of the first user equipment, the relay service code, and a second key, wherein the shared key is used to protect a communication connection between the first user equipment and second user equipment, and the

second key and the first key each are a key generated in an authentication procedure of the first user equipment or a key obtained through derivation based on an intermediate key generated in an authentication procedure of the first user equipment; and

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

10. The method according to claim 9, wherein the generating, by the first network element, a shared key based on the identifier of the first user equipment, 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 user equipment, and generating, by the first network element, the shared key based on the second key and the relay service code.

11. The method according to claim 9 or 10, wherein the second key is the same as the first key, and the second key and the first key each are a key Kausf generated in the authentication procedure or a key obtained through derivation based on the Kausf.

12. The method according to any one of claims 9 to 11, 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 user equipment, and routing information, wherein the network identifier of the first user equipment is used by the network side to identify the information about the first user equipment, and the routing information is information used to determine a core network element related to the first user equipment.

13. The method according to claim 12, wherein the generating, by the first network element, the first temporary identifier based on the first key, the network identifier of the first user equipment, 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 user equipment 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.

14. The method according to any one of claims 9 to 13, wherein

the network identifier of the first user equipment 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.

15. The method according to any one of claims 9 to 14, 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 user equipment, 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 user equipment, the relay service code, the second key, and the first freshness parameter.

16. The method according to any one of claims 9 to 14, 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 user equipment, 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 user equipment, the relay service code, the second key, and the second freshness parameter.

17. The method according to any one of claims 9 to 16, wherein

the first network element is an authentication function network element.

18. The method according to any one of claims 9 to 17, 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.

19. 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 8.

20. 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 9 to 18.

21. 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 9 to 18; and

a second network element, configured to send a key obtaining message to the first network element, wherein the key obtaining message comprises an identifier of first user equipment and a relay service code, the identifier of the first user equipment comprises a first temporary identifier or a network identifier of the first user equipment, and the network identifier of the first user equipment is used by a network side to identify information about the first user equipment;

wherein the second network element is further configured to receive a shared key.

22. The system according to claim 21, 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.