CLAIMS

What is claimed is:

1. A method for establishing secure communication, comprising:

receiving, by a first communication apparatus, a first message from a first network element, wherein the first message comprises an identifier of a second network element and first indication information, and the first indication information indicates a candidate authentication mechanism associated with the second network element; and

establishing, by the first communication apparatus, a communication connection with the second network element based on the candidate authentication mechanism

wherein the candidate authentication mechanism is an authentication mechanism supported by the second network element, or an authentication mechanism used for establishing a communication connection between the second network element and the first communication apparatus.

2. The method according to claim 1, further comprising:

sending, by the first communication apparatus, a second message to the first network element, wherein the first message is a response message of the second message.

3. The method according to claim 1 or 2, wherein the candidate authentication mechanism is at least one first authentication mechanism used when the first communication apparatus establishes the communication connection with the second network element.

4. The method according to claim 3, wherein the second message comprises a network type used by the first communication apparatus to access the second network element, wherein the at least one first authentication mechanism is an authentication mechanism that corresponds to the network type.

5. The method according to claim 3 or 4, wherein the second message comprises at least one second authentication mechanism supported by the first communication apparatus, wherein the at least one first authentication mechanism is comprised in the at least one second authentication mechanism.

6. The method according to claim 5, wherein the second message further comprises priority information of the at least one second authentication mechanism, and the at least one second authentication mechanism is used for selecting the at least one first authentication mechanism.

7. The method according to any one of claims 3 to 6, wherein the establishing, by the first communication apparatus, a communication connection with the second network element based on the candidate authentication mechanism comprises:

generating, by the first communication apparatus, a first key and a first key identifier that correspond to a target authentication mechanism, wherein the target authentication mechanism is one of the at least one first authentication mechanism; and

sending, by the first communication apparatus, a communication connection establishment request to the second network element, wherein the communication connection establishment request comprises the first key identifier.

8. The method according to claim 1 or 2, wherein the candidate authentication mechanism is at least one third authentication mechanism supported by the second network element.

9. The method according to claim 8, wherein the establishing, by the first communication apparatus, a communication connection with the second network element based on the candidate authentication mechanism comprises:

determining, by the first communication apparatus, a target authentication mechanism based on the at least one third authentication mechanism and assistance information, wherein the assistance information comprises at least one of the following: at least one second authentication mechanism supported by the first communication apparatus and a network type used by the first communication apparatus to access the second network element;

generating, by the first communication apparatus, a first key and a first key identifier that correspond to the target authentication mechanism; and

sending, by the first communication apparatus, a communication connection establishment request to the second network element, wherein the communication connection establishment request comprises the first key identifier.

10. The method according to claim 9, wherein the assistance information further comprises at least one of the following: priority information of the at least one second authentication mechanism and priority information of the at least one third authentication mechanism.

11. The method according to claim 10, wherein the first message further comprises the priority information of the at least one third authentication mechanism.

12. The method according to claim 7 or 9 further comprising:

generating, by the first communication apparatus, a second key based on the first key and the

identifier of the second network element.

13. The method according to claim 12 further comprising:

performing, by the first communication apparatus, security protection on the communication connection establishment request by using the second key, to generate a first message authentication code MAC, wherein the communication connection establishment request further comprises the first MAC.

14. The method according to any one of claims 1 to 13, wherein the first network element is an edge configuration server ECS, and the second network element is an edge enabler server EES; or the first network element is an EES, and the second network element is an edge application server EAS.

15. The method according to any one of claims 1 to 13, wherein the first network element is an access and mobility management function AMF or a session management function SMF, and the second network element is an edge configuration server ECS.

16. The method according to claim 15, wherein the first message is a non-access stratum NAS message.

17. The method according to claim 16, wherein the first message is a response message for the first communication apparatus to request registration or a response message for the first communication apparatus to request to establish a protocol data unit PDU session.

18. The method according to any one of claims 1 to 17, wherein the candidate authentication mechanism comprises at least one of the following: an authentication and key management for applications AKMA service, a generic bootstrapping architecture GBA service, and a certificate mechanism.

19. The method according to any one of claims 1 to 18, wherein the first communication apparatus is a terminal device, or a chip applied in the terminal device.

20. A method for establishing secure communication, comprising:

determining, by a first network element, a candidate authentication mechanism; and

sending, by the first network element, a first message to a terminal device, wherein the first message comprises an identifier of a second network element and first indication information, the first indication information indicates a candidate authentication mechanism associated with the second network element, and the candidate authentication mechanism is used by the terminal device to establish a communication connection with the second network element;

wherein the candidate authentication mechanism is an authentication mechanism supported by the second network element, or an authentication mechanism used for establishing a communication connection between the second network element and the first communication apparatus.

21. The method according to claim 20, further comprising:

receiving, by the first network element, a second message from the terminal device, wherein the first message is a response message of the second message.

22. The method according to claim 20 or 21, wherein the candidate authentication mechanism is at least one first authentication mechanism used when the terminal device establishes the communication connection with the second network element, and the determining, by a first network element, a candidate authentication mechanism comprises:

determining, by the first network element, the candidate authentication mechanism based on at least one third authentication mechanism supported by the second network element and assistance information, wherein the assistance information comprises at least one of the following: at least one second authentication mechanism supported by the terminal device and a network type used by the terminal device to access the second network element.

23. The method according to claim 22, wherein the second message comprises the network type used by the terminal device to access the second network element, wherein the at least one first authentication mechanism is an authentication mechanism that corresponds to the network type.

24. The method according to claim 22 or 23, wherein the second message comprises the at least one second authentication mechanism supported by the terminal device, wherein the at least one first authentication mechanism is comprised in the at least one second authentication mechanism.

25. The method according to any one of claims 22 to 24, wherein the assistance information further comprises at least one of the following: priority information of the at least one second authentication mechanism and priority information of the at least one third authentication mechanism, and the at least one second authentication mechanism is used for selecting the at least one first authentication mechanism.

26. The method according to claim 25, wherein the second message further comprises the priority information of the at least one second authentication mechanism.

27. The method according to claim 20 or 21, wherein the candidate authentication mechanism is at least one third authentication mechanism supported by the second network element.

28. The method according to claim 27, wherein the first message further comprises the priority information of the at least one third authentication mechanism.

29. The method according to any one of claims 20 to 28, wherein the first network element is an ECS, and the second network element is an EES; or the first network element is an EES, and the second network element is an EAS.

30. The method according to any one of claims 20 to 28, wherein the first network element is an AMF or an SMF, and the second network element is an ECS.

31. The method according to claim 30, wherein the first message is a NAS message.

32. The method according to claim 31, wherein the first message is a response message for the terminal device to request registration or a response message for the terminal device to request to establish a PDU session.

33. The method according to any one of claims 20 to 32, wherein the candidate authentication mechanism comprises at least one of the following: an AKMA service, a GBA service, and a certificate mechanism.

34. An apparatus, comprising a unit configured to implement the method according to any one of claims 1 to 19, or comprising a unit configured to implement the method according to any one of claims 20 to 33.

35. An apparatus, comprising a processor and a memory, wherein the memory stores instructions, and when the processor executes the instructions, the apparatus is enabled to perform the method according to any one of claims 1 to 19 or the method according to any one of claims 20 to 33.

36. A computer-readable storage medium, wherein the computer-readable storage medium stores instructions, and when the instructions are run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 19 or the method according to any one of claims 20 to 33.

37. A computer program product, comprising instructions, wherein when the instructions are executed, a communication apparatus is enabled to perform the method according to any one of claims 1 to 19, or to perform the method according to any one of claims 20 to 33.