CLAIMS

What is claimed is:

1. A method for obtaining a security context, comprising:

receiving, by a first access and mobility management function AMF, a first registration request message sent by user equipment;

validating, by the first AMF, integrity of the first registration request message;

sending, by the first AMF, a second request message to a second AMF when the first AMF successfully validates integrity of the first registration request message, wherein the second request message carries indication information, and the indication information is used to indicate that the user equipment is validated; and

receiving, by the first AMF, a 5G security context of the user equipment sent by the second AMF based on the second request message;

wherein the second AMF and the first AMF are in a 5G communication system.

2. The method according to claim 1, wherein security protection is performed on the first registration request message by using a mapped security context.

3. The method according to claim 2, wherein the security protection comprises encryption protection and/or integrity protection.

4. The method according to claim 2 or 3, wherein the mapped security context is derived by the user equipment based on a 4G security context between a mobility management entity MME and the user equipment.

5. The method according to any one of claims 2-4, wherein

the mapped security context is derived by the user equipment based on a key K_{ASME}.

6. The method according to any one of claims 1-5, wherein the first registration request message is sent after the user equipment completes a handover procedure.

7. The method according to any one of claims 1-6, wherein the first registration request message is a Registration Request message.

8. The method according to any one of claims 1-7, wherein the first registration request message comprises a 5G globally unique temporary user equipment identity GUTI of the user equipment.

9. The method according to claim 8, wherein the 5G GUTI is configured by the second AMF for the user equipment, and is used to identify the user equipment and the second AMF.

10. The method according to any one of claims 1-9, wherein the second request message comprises a 5G globally unique temporary user equipment identity GUTI or a subscriber permanent identity SUPI of the user equipment.

11. The method according to claim any one of claims 1-10, wherein the second AMF does not need to validate the user equipment.

12. The method according to any one of claims 1-11, wherein that the indication information is used to indicate that the user equipment is validated specifically comprises that the indication information is used to indicate that integrity of the first registration request message received by the first AMF from the user equipment is successfully validated.

13. The method according to any one of claims 1-12, wherein the second AMF refers to an AMF that saves the 5G security context of the user equipment other than the first AMF in a 5G communication system in a process in which the user equipment is handed over from a 4G communication system to the 5G communication system.

14. The method according to any one of claims 1-13, wherein the first AMF refers to an AMF selected by a mobility management entity MME in a 4G communication system for the user equipment from a 5G communication system to provide a core network service for the user equipment in a process in which the user equipment is handed over from the 4G communication system to the 5G communication system.

15. The method according to any one of claims 1-14, wherein the receiving, by the first AMF, a 5G security context of the user equipment sent by the second AMF based on the second request message specifically comprises:

receiving, by the first AMF, a context of the user equipment sent by the second AMF based on the second request message, wherein the context of the user equipment comprises a 5G security context of the user equipment determined through negotiation between the second AMF and the user equipment, and the 5G security context of the user equipment comprises a key K_{AMF2} and a non-access stratum count NAS COUNT.

16. The method according to any one of claims 8-15, wherein a reason why the 5G security context and the 5G GUTI of the user equipment are stored between the user equipment and the second AMF comprises: before the user equipment is handed over from a 4G communication system to a 5G communication system, the user equipment is handed over from the 5G network communication system to the 4G communication system; or the user equipment supporting dual

connectivity accesses the 5G communication system through a non-3GPP connection, accesses the 4G communication system through a 3GPP connection, and is handed over from the 4G communication system to the 5G communication system in connected mode.

17. The method according to any one of claims 1-16, wherein the method further comprises:

when the first AMF fails to validate integrity of the first registration request message, continuing, by the first AMF, to use a mapped security context generated through negotiation between the first AMF and the user equipment, or initiating, by the first AMF, an initial authentication to the user equipment to generate a security context between the first AMF and the user equipment.

18. The method according to any one of claims 1-17, wherein the method further comprises: when the first AMF fails to validate integrity of the first registration request message, failing, by the first AMF, to receive a 5G security context of the user equipment sent by the second AMF.

19. The method according to any one of claims 10-18, wherein the receiving, by the first AMF, a 5G security context of the user equipment sent by the second AMF based on the second request message specifically comprises:

receiving, by the first AMF, the 5G security context of the user equipment determined by the second AMF based on the 5G GUTI in the second request message.

20. The method according to any one of claims 5-19, wherein that the mapped security context is derived by the user equipment based on a key K_{ASME} specifically comprises:

a key K_{AMF1} is derived by the user equipment based on the saved key K_{ASME}, a next hop parameter NH, and a preset formula, wherein the preset formula is:

K_{AMF1} = HMAC-SHA-256 (Key, FC||P0||L0), wherein FC = 0x76, P0 = NH value, L0 = length of NH value, and KEY = K_{ASME}.

21. The method according to any one of claims 4-20, wherein before the receiving, by a first access and mobility management function AMF, a first registration request message sent by user equipment, the method further comprises:

receiving, by the first AMF, a first forward relocation request from the MME, wherein the first forward relocation request comprises the 4G security context between the user equipment and the MME;

determining, by the first AMF, the mapped security context based on the 4G security context between the user equipment and the MME;

sending, by the first AMF, a forward relocation response message to the MME.

22. The method according to claim 21, wherein the method further comprises:

the first forward relocation request comprising a key K_{ASME} and a next hop parameter NH; and

deriving, by the first AMF, a key K_{AMF1} based on the K_{ASME} and the NH.

23. The method according to claim 22, wherein the deriving, by the first AMF, a key K_{AMF1} based on the K_{ASME} and the NH specifically comprises:

after the first AMF receives the K_{ASME} and the NH, deriving, by the first AMF, the K_{AMF1} based on a preset formula, wherein the preset formula is:

K_{AMF1} = HMAC-SHA-256 (Key, FC||P0||L0), wherein FC = 0x76, P0 = NH value, L0 = length of NH value, and KEY = K_{ASME}.

24. The method according to claim 23, wherein the method further comprises:

calculating, by the first AMF, an integrity protection key $K_{NASint1}$ and a confidentiality protection key $K_{NASenc1}$ based on the K_{AMF1} and a security algorithm negotiated with the user equipment.

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

generating, by the first AMF based on the key K_{AMF1} and a non-access stratum NAS integrity protection algorithm and a confidentiality protection algorithm that are negotiated between the user equipment and the first AMF, an integrity protection key $K_{NASint1}$ and a confidentiality protection key $K_{NASenc1}$ that are used to protect a NAS message,

wherein a formula for calculating the integrity protection key $K_{NASint1}$ comprises: $K_{NASint1}$ = HMAC-SHA-256 (KEY,S), wherein S = FC||$P0_1$||$L0_1$||$P1_1$||$L1_1$, FC = 0x69, $P0_1$ = algorithm type distinguisher, $L0_1$= length of algorithm type distinguisher, $P1_1$= algorithm identity, $L1_1$ = length of algorithm identity, and KEY = K_{AMF1},

wherein a formula for calculating the confidentiality protection key $K_{NASenc1}$ comprises: $K_{NASenc1}$ = HMAC-SHA-256 (KEY, S), wherein S = FC||P0||L0||P1||L1, FC = 0x69, P0 = algorithm type distinguisher, L0 = length of algorithm type distinguisher, P1 = algorithm identity, L1 = length of algorithm identity, and KEY = K_{AMF1}.

26. The method according to any one of claims 21-25, wherein the forward relocation response message is used to notify the MME that the first AMF is an AMF that provides an access and mobility management service for the user equipment in a 5G communication system when the

user equipment is handed over from a 4G communication system to the 5G communication system.

27. The method according to any one of claims 1-26, wherein the indication information is used to indicate that the user equipment is validated comprises:

the indication information is used to indicate that integrity of the first registration request message is successfully validated, wherein the second request message is configured to cause the second AMF to skip verifying the UE.

28. The method according to claim 27, wherein the skipping verifying the UE comprises skipping verifying integrity of the second request message.

29. The method of any one of claims 1-28, wherein the first AMF validates integrity of the first registration request message in response to receiving the first registration request message.

30. The method of any one of claims 1-29, wherein after the first AMF receives the first registration request message and before the second AMF receives the second request message, the second AMF has not verified the UE.

31. A method for obtaining a security context, comprising:

receiving, by a second access and mobility management function AMF, a second request message sent by a first AMF, wherein the second request message carries indication information, and the indication information is used to indicate that user equipment is validated; and

after the second AMF receives the second request message, sending, by the second AMF, a 5G security context of the user equipment to the first AMF,

wherein the second request message is sent when the first AMF successfully validates integrity of a first registration request message, and the first registration message is sent by the user equipment to the first AMF;

wherein the second AMF and the first AMF are in a 5G communication system.

32. The method according to claim 31, wherein the second request message comprises a 5G globally unique temporary user equipment identity GUTI of the user equipment, wherein before the second AMF sends the 5G security context of the user equipment to the first AMF, the second AMF determines the 5G security context of the user equipment based on the 5G GUTI in the second request message.

33. The method according to claim 32, wherein a reason why the 5G security context and the 5G GUTI of the user equipment are stored between the user equipment and the second AMF comprises: before the user equipment is handed over from a 4G communication system to a 5G

communication system, the user equipment is handed over from the 5G network communication system to the 4G communication system; or the user equipment supporting dual connectivity accesses the 5G communication system through a non-3GPP connection, accesses the 4G communication system through a 3GPP connection, and is handed over from the 4G communication system to the 5G communication system in connected mode.

34. The method according to any one of claims 31-33, wherein the indication information is used to indicate that the UE is validated comprises:

the indication information is used to indicate that integrity of the first registration request message is successfully validated.

35. The method according to any one of claims 31-34, wherein the second request message is configured to cause the second AMF to skip verifying the UE.

36. The method according to claim 35, wherein the skipping verifying the UE comprises skipping verifying integrity of the second request message.

37. The method of any one of claims 1-36, wherein the integrity of the first registration request message is being validated by the first AMF in response to receiving the first registration request message.

38. The method of any one of claims 1-37, wherein after the first AMF receives the first registration request message and before the second AMF receives the second request message, the second AMF has not verified the UE.

39. A communication system, comprising a first access and mobility management function AMF and a second AMF, wherein

the first AMF is configured to:

receive a first registration request message sent by user equipment;

validate integrity of the first registration request message;

when the first AMF successfully validates integrity of the first registration request message, send a second request message to the second AMF, wherein the second request message carries indication information, and the indication information is used to indicate that the user equipment is validated; and

the second AMF is configured to:

receive the second request message; and

send a 5G security context of the user equipment to the first AMF based on the second request

message;

wherein the second AMF and the first AMF are in a 5G communication system.

40. The system according to claim 39, wherein before the first access and mobility management function AMF receives the first registration request message sent by the user equipment, the first AMF is further configured to:

receive a first forward relocation request from a mobility management entity MME, wherein the first forward relocation request comprises a 4G security context between the user equipment and the MME;

determine a mapped security context based on the 4G security context between the user equipment and the MME; and

send a forward relocation response message to the MME.

41. The system according to claim 40, wherein the first forward relocation request comprises a key K_{ASME} and a next hop parameter NH, and the first AMF is further configured to:

derive a key K_{AMF1} based on the K_{ASME} and the NH.

42. The system according to claim 41, wherein the first AMF is specifically configured to:

after the first AMF receives the K_{ASME} and the NH, derive the K_{AMF1} based on a preset formula, wherein the preset formula is:

K_{AMF1} = HMAC-SHA-256 (Key, FC||P0||L0), wherein FC = 0x76, P0 = NH value, L0 = length of NH value, and KEY = K_{ASME}.

43. The system according to claim 42, wherein the first AMF is further configured to:

calculate an integrity protection key $K_{NASint1}$ and a confidentiality protection key $K_{NASenc1}$ based on the K_{AMF1} and a security algorithm negotiated with the user equipment,

wherein a formula for calculating the integrity protection key $K_{NASint1}$ comprises: $K_{NASint1}$ = HMAC-SHA-256 (KEY,S), wherein S = FC||$P0_1$||$L0_1$||$P1_1$||$L1_1$, FC = 0x69, $P0_1$ = algorithm type distinguisher, $L0_1$= length of algorithm type distinguisher, $P1_1$= algorithm identity, $L1_1$ = length of algorithm identity, and KEY = K_{AMF1},

wherein a formula for calculating the confidentiality protection key $K_{NASenc1}$ comprises: $K_{NASenc1}$ = HMAC-SHA-256 (KEY, S), wherein S = FC||P0||L0||P1||L1, FC = 0x69, P0 = algorithm type distinguisher, L0 = length of algorithm type distinguisher, P1 = algorithm identity, L1 = length of algorithm identity, and KEY = K_{AMF1}.

44. The system according to any one of claims 40-43, wherein the forward relocation response

message is used to notify the MME that the first AMF is an AMF that provides an access and mobility management service for the user equipment in a 5G communication system when the user equipment is handed over from a 4G communication system to the 5G communication system.

45. The system according to any one of claims 39-44, wherein the first registration request message is a Registration Request message.

46. The system according to any one of claims 40-45, wherein before the first access and mobility management function AMF receives the first registration request message sent by the user equipment, the MME is further configured to:

sending, by the MME, a handover command message to the user equipment; and

determining, by the user equipment, the mapped security context.

47. The system according to any one of claims 39-46, wherein the first registration request message comprises a 5G globally unique temporary user equipment identity GUTI of the user equipment.

48. The system according to claim 47, wherein the 5G GUTI is configured by the second AMF for the user equipment, and is used to identify the user equipment and the second AMF.

49. The system according to claim 47 or 48, wherein a reason why the 5G security context and the 5G GUTI of the user equipment are stored between the user equipment and the second AMF comprises: before the user equipment is handed over from a 4G communication system to a 5G communication system, the user equipment is handed over from the 5G network communication system to the 4G communication system; or the user equipment supporting dual connectivity accesses the 5G communication system through a non-3GPP connection, accesses the 4G communication system through a 3GPP connection, and is handed over from the 4G communication system to the 5G communication system in connected mode.

50. The system according to any one of claims 39-49, wherein the second request message comprises a 5G globally unique temporary user equipment identity GUTI or a subscriber permanent identity SUPI of the user equipment, wherein the second AMF is further configured to:

determine the 5G security context of the user equipment based on the 5G GUTI in the second request message when the second AMF receives the second request message.

51. The system according to any one of claims 39-50, wherein the second request message is configured to cause the second AMF to skip verifying the UE, wherein the skipping verifying the UE comprises skipping verifying integrity of the second request message.

52. The system according to any one of claims 39-51, wherein the first AMF validates integrity of the first registration request message in response to receiving the first registration request message, wherein after the first AMF receives the first registration request message and before the second AMF receives the second request message, the second AMF has not verified the UE.

53. An apparatus for obtaining a security context, wherein the apparatus is applied to a network system, the network system comprises a first AMF and a second AMF, and the apparatus comprises a processor, an interface circuit, a memory, and a system bus; and

the memory is configured to store computer executable instructions, and the processor executes the computer executable instructions stored in the memory to enable the apparatus to perform the method according to any one of claims 1 to 38.

54. A network device for obtaining a security context, comprising a processor and a memory, wherein the memory is configured to store a computer program, and the processor executes computer executable instructions stored in the memory to enable the network device to perform the method according to any one of claims 1 to 30.

55. A network device for obtaining a security context, comprising a processor and a memory, wherein the memory is configured to store a computer program, and the processor executes computer executable instructions stored in the memory to enable the network device to perform the method according to any one of claims 31 to 38.