CLAIMS

What is claimed is:

1. A communications system, comprising:

a target access network device configured to:

receive a radio resource control (RRC) resume request from a user equipment (UE), wherein the RRC resume request comprises an inactive–radio network temporary identifier (I-RNTI); and

send a context information obtaining request comprising the I-RNTI; and

a source access network device configured to:

receive the context information obtaining request from the target access network device;

obtain first indication information based on the I-RNTI, wherein the first indication information indicates a user plane security protection method used before the source access network device and the UE enter an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled; and

send a context information obtaining response to the target access network device, wherein the context information obtaining response comprises the first indication information,

wherein the target access network device is further configured to:

receive the context information obtaining response from the source access network device; and

activate, using the user plane security protection method, user plane security between the target access network device and the UE when the user plane security protection method can be supported.

2. The communications system according to claim 1, wherein the target access network device is further configured to send an RRC message to the UE when the user plane security protection method cannot be supported, and wherein the RRC message is configured to trigger the UE to re-establish an RRC connection to the target access network device.

3. The communications system according to claim 1, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are

used by the source access network device and a new access stratum key (KgNB*) generated by the source access network device, and wherein the target access network device is further configured such that when the target access network device supports the encryption algorithm and the integrity protection algorithm, the target access network device determines a first user plane security key between the target access network device and the UE based on the KgNB*.

4. The communications system according to claim 1, wherein the target access network device is further configured to:

receive first uplink user plane data from the UE; and

perform user plane security deprotection on the first uplink user plane data to obtain uplink user plane data.

5. The communications system according to claim 1, wherein the context information obtaining response further comprises at least one user plane security policy of the UE, and wherein the at least one user plane security policy comprises at least one of a user plane encryption protection policy or a user plane integrity protection policy.

6. The communications system according to claim 1, wherein the context information obtaining response further comprises a protocol data unit (PDU) session identifier (ID) corresponding to the first indication information.

7. The communications system according to claim 1, wherein the source access network device is further configured to:

send an RRC release message to the UE, wherein the RRC release message indicates to the UE to enter the inactive state;

store the first indication information;

delete an RRC encryption key, a user plane encryption key, and a user plane integrity protection key; and

store an RRC integrity protection key and the first indication information.

8. The communications system according to claim 1, wherein the target access network device

is further configured to determine whether the user plane security protection method can be supported.

9. A target access network device, comprising:

at least one processor; and

a memory coupled to the at least one processor and configured to store program instructions, which when executed by the at least one processor, cause the target access network device to:

receive a radio resource control (RRC) resume request from a user equipment (UE), wherein the RRC resume request comprises an inactive–radio network temporary identifier (I-RNTI);

send a context information obtaining request comprising the I-RNTI to a source access network device;

receive a context information obtaining response from the source access network device, wherein the context information obtaining response comprises first indication information, wherein the first indication information indicates a user plane security protection method used before the UE enters an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled; and

activate, using the user plane security protection method, user plane security between the target access network device and the UE when the user plane security protection method can be supported.

10. The target access network device according to claim 9, wherein the program instructions further cause the target access network device to send an RRC message to the UE when the user plane security protection method cannot be supported, and wherein the RRC message is configured to trigger the UE to re-establish an RRC connection to the target access network device.

11. The target access network device according to claim 9, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key (KgNB*) generated by the source access network device, and wherein the program instructions further cause the target access network device to determine a first user plane security key between the target

access network device and the UE based on the KgNB* when the target access network device supports the encryption algorithm and the integrity protection algorithm.

12. The target access network device according to claim 9, wherein the program instructions further cause the target access network device to:

receive first uplink user plane data from the UE;

perform user plane security deprotection on the first uplink user plane data to obtain uplink user plane data; and

send the uplink user plane data.

13. The target access network device according to claim 9, wherein the context information obtaining response further comprises at least one user plane security policy of the UE, and wherein the at least one user plane security policy comprises at least one of a user plane encryption protection policy or a user plane integrity protection policy.

14. The target access network device according to claim 9, wherein the context information obtaining response further comprises a protocol data unit (PDU) session identifier (ID) corresponding to the first indication information.

15. The target access network device according to claim 9, wherein the program instructions further cause the target access network device to determine whether the user plane security protection method can be supported.

16. An apparatus, comprising:

at least one processor; and

a memory coupled to the at least one processor and configured to store program instructions, which when executed by the at least one processor, cause the apparatus to:

store first indication information, wherein the first indication information indicates a user plane security protection method used before the apparatus enters an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled;

send a radio resource control (RRC) resume request to a target access network device; and

activate, using the user plane security protection method, user plane security between the apparatus and the target access network device when receiving an RRC resume message from the target access network device.

17. The apparatus according to claim 16, wherein the program instructions further cause the apparatus to:

determine a first user plane security key between the apparatus and the target access network device;

perform user plane security protection on uplink user plane data based on the user plane security protection method and the first user plane security key;

obtain first uplink user plane data based on performing the user plane security protection on the uplink user plane data; and

send the first uplink user plane data to the target access network device.

18. The apparatus according to claim 17, wherein the program instructions further cause the apparatus to determine the first user plane security key between the apparatus and the target access network device according to the user plane security protection method.

19. The apparatus according to claim 16, wherein the program instructions further cause the apparatus to receive an RRC release message from a source access network device, and wherein the RRC release message indicates to the apparatus to enter the inactive state.

20. The apparatus according to claim 16, wherein the program instructions further cause the apparatus to receive an RRC connection reconfiguration message from a source access network device, and wherein the RRC connection reconfiguration message comprises the first indication information.

21. A method comprising:

receiving, by a target access network device, a radio resource control (RRC) resume request from a user equipment (UE), wherein the RRC resume request comprises an inactive–radio

network temporary identifier (I-RNTI);

sending, by the target access network device, a context information obtaining request comprising the I-RNTI to a source access network device;

receiving, by the target access network device, a context information obtaining response from the source access network device, wherein the context information obtaining response comprises first indication information, wherein the first indication information indicates a user plane security protection method used before the UE enters an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled; and

activating, by the target access network device using the user plane security protection method, user plane security between the target access network device and the UE when the user plane security protection method can be supported.

22. The method according to claim 21, further comprising sending, by the target access network device, an RRC message to the UE when the user plane security protection method cannot be supported, and wherein the RRC message is configured to trigger the UE to re-establish an RRC connection to the target access network device.

23. The method according to claim 21, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key (KgNB*) generated by the source access network device, and wherein the method further comprises determining, by the target access network device, a first user plane security key between the target access network device and the UE based on the KgNB* when the target access network device supports the encryption algorithm and the integrity protection algorithm.

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

receiving, by the target access network device, first uplink user plane data from the UE;

performing, by the target access network device, user plane security deprotection on the first uplink user plane data to obtain uplink user plane data; and

sending, by the target access network device, the uplink user plane data.

25. The method according to claim 21, wherein the context information obtaining response further comprises at least one user plane security policy of the UE, and wherein the at least one user plane security policy comprises at least one of a user plane encryption protection policy or a user plane integrity protection policy.

26. The method according to claim 21, wherein the context information obtaining response further comprises a protocol data unit (PDU) session identifier (ID) corresponding to the first indication information.

27. The method according to claim 21, further comprising determining, by the target access network device, whether the user plane security protection method can be supported.

28. A method comprising:

storing, by an apparatus, first indication information, wherein the first indication information indicates a user plane security protection method used before the apparatus enters an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled;

sending, by the apparatus, a radio resource control (RRC) resume request to a target access network device; and

activating, by the apparatus using the user plane security protection method, user plane security between the apparatus and the target access network device when receiving an RRC resume message from the target access network device.

29. The method according to claim 28, further comprising:

determining, by the apparatus, a first user plane security key between the apparatus and the target access network device;

performing, by the apparatus, user plane security protection on uplink user plane data based on the user plane security protection method and the first user plane security key;

obtaining, by the apparatus, first uplink user plane data based on performing the user plane security protection on the uplink user plane data; and

sending, by the apparatus, the first uplink user plane data to the target access network device.

30. The method according to claim 29, wherein determining the first user plane security key comprises determining, by the apparatus, the first user plane security key between the apparatus and the target access network device according to the user plane security protection method.

31. The method according to claim 28, further comprising receiving, by the apparatus, an RRC connection reconfiguration message from a source access network device, wherein the RRC connection reconfiguration message comprises the first indication information.

32. A communications method, comprising:

receiving, by a target access network device, a radio resource control (RRC) resume request from a user equipment (UE), wherein the RRC resume request comprises an inactive–radio network temporary identifier (I-RNTI);

sending, by the target access network device, a context information obtaining request comprising the I-RNTI;

receiving, by the source access network device, the context information obtaining request from the target access network device;

obtaining, by the source access network device, first indication information based on the I-RNTI, wherein the first indication information indicates a user plane security protection method used before the source access network device and the UE enter an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled;

sending, by the source access network device, a context information obtaining response to the target access network device, wherein the context information obtaining response comprises the first indication information;

receiving, by the target access network device, the context information obtaining response from the source access network device; and

activating, by the target access network device using the user plane security protection method, user plane security between the target access network device and the UE when the user plane security protection method can be supported.

33. The communications method according to claim 32, further comprising sending, by the target access network device, an RRC message to the UE when the user plane security protection method cannot be supported, wherein the RRC message is configured to trigger the UE to re-establish an RRC connection to the target access network device.

34. The communications method according to claim 32, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key (KgNB*) generated by the source access network device, and wherein the communications method further comprises determining, by the target access network device, a first user plane security key between the target access network device and the UE based on the KgNB* when the target access network device supports the encryption algorithm and the integrity protection algorithm.

35. The communications method according to claim 32, wherein the context information obtaining response further comprises at least one user plane security policy of the UE, and wherein the at least one user plane security policy comprises at least one of a user plane encryption protection policy or a user plane integrity protection policy.

36. The communications method according to claim 32, wherein the context information obtaining response further comprises a protocol data unit (PDU) session identifier (ID) corresponding to the first indication information.

37. The communications method according to claim 32, further comprising:

sending, by the source access network device, an RRC release message to the UE, wherein the RRC release message indicates to the UE to enter the inactive state;

storing, by the source access network device, the first indication information;

deleting, by the source access network device, an RRC encryption key, a user plane encryption key, and a user plane integrity protection key; and

storing, by the source access network device, an RRC integrity protection key and the first indication information.

38. The communications method according to claim 32, further comprising determining, by the target access network device, whether the user plane security protection method can be supported.