CLAIMS

1. A method for wireless communication by a user equipment (UE), comprising:

receiving a first message for establishing a secure connection with a network, wherein the first message comprises network policy information, and wherein the network policy information comprises security features of the network;

generating a first key by a key derivation function (KDF), wherein a second key and the network policy information are inputs into the KDF; and

verifying the network policy information based, at least in part, on the first key.

2. The method of claim 1, wherein verifying the network policy information comprises determining whether the first message is valid based in part on the first key.

3. The method of claim 2, wherein:

the first message is integrity protected with a protection key derived from a third key; and

determining whether the first message is valid comprises performing an integrity verification of the first message based on the first key.

4. The method of claim 2, further comprising:

establishing a secure connection with the network if the determination is that the first message is valid.

5. The method of claim 1, wherein the first message further includes an amount of time that the network policy information is valid.

6. The method of claim 1, wherein the first key is an access and mobility management function (AMF) key and the second key is an anchor key shared between the UE and a security anchor function (SEAF) in the network.

7. The method of claim 6, further comprising performing at least one of an authentication or registration procedure with the SEAF, prior to receiving the first message, wherein the anchor key is established based on at least one of the authentication or registration procedure.

8. The method of claim 1, wherein the network policy information comprises an indication of whether the UE will receive a session management token, from a session management function (SMF) in the network, when establishing a communication session with the network.

9. The method of claim 1, wherein the first message is received from an access and mobility management function (AMF) in the network.

10. The method of claim 9, wherein the network policy information comprises an indication of whether the AMF is collocated with a security anchor function (SEAF) in the network.

11. The method of claim 9, wherein the network policy information comprises a security level of the AMF.

12. The method of claim 1, wherein:

the first message is received from an access and mobility management function (AMF) in the network; and

establishing the secure connection comprises sending a second message to the AMF.

13. The method of claim 12, wherein:

the first message is a security mode command (SMC) message; and

the second message is a SMC complete message.

14. The method of claim 12, wherein the secure connection comprises a non-access stratum (NAS) secure connection.

15. The method of claim 1, further comprising sending UE policy information to the network, wherein the UE policy information comprises at least one of UE capability information or UE security information.

16. The method of claim 15, wherein generating the first key is based on the UE policy information sent to the network.

17. The method of claim 15, wherein the network policy information is based on the UE policy information.

18. A method for wireless communication by a security anchor function (SEAF), comprising:

generating a first key for a network node by inputting a second key and network policy information into a key derivation function (KDF), wherein the network policy information comprises security features of the network, and wherein the first key is usable for establishing a secure connection between a user equipment (UE) and the network node; and

sending the first key to the network node.

19. The method of claim 18, further comprising:

participating in at least one of an authentication procedure or registration procedure with the UE prior to generating the first key, wherein the participating comprises establishing an anchor key to be shared between the UE and the SEAF.

20. The method of claim 19, wherein the first key is an access and mobility management function (AMF) key and the second key is the anchor key.

21. The method of claim 20, further comprising:

sending the network policy information to the network node.

22. The method of claim 18, wherein the network policy information comprises an indication of whether the network node is collocated with the SEAF in the network.

23. The method of claim 18, wherein the network policy information comprises a security level of the network node.

24. The method of claim 18, wherein the network policy information comprises an indication of whether a session management function (SMF) in the network is to generate a session management token for a communication session between the UE and the network, and transmit the session management token to the UE.

25. The method of claim 18, further comprising:

receiving a message comprising policy information of the UE, wherein the UE policy information comprises at least one of UE capability information or UE security information.

26. The method of claim 25, wherein the first key is generated further based on the UE policy information.

27. The method of claim 25, wherein the message comprises a registration message or an attach request message.

28. The method of claim 25, wherein the network policy information is determined based on the UE policy information.

29. The method of claim 18, wherein the network node is an access and mobility management function (AMF) in the network.

30. A user equipment (UE), comprising:

a memory for storing instructions; and

a processor, wherein when the processor executes the instructions, the processor is configured to:

receive a first message for establishing a secure connection with a network, wherein the first message comprises network policy information, and wherein the network policy information comprises security features of the network;

generate a first key by a key derivation function (KDF), wherein a second key and the network policy information are inputs into the KDF; and

verify the network policy information based, at least in part, on the first key.

31. The UE of claim 30, wherein the processor is configured to verify the network policy information by determining whether the first message is valid based in part on the first key.

32. The UE of claim 31, wherein:

the first message is integrity protected with a protection key derived from a third key; and

wherein the processor is configured to determine whether the first message is valid by performing an integrity verification of the first message based on the first key.

33. The UE of claim 31, wherein the processor is configured to establish a secure connection with the network if the determination is that the first message is valid.

34. The UE of claim 30, wherein the first key is an access and mobility management function (AMF) key and the second key is an anchor key shared between the UE and a security anchor function (SEAF) in the network.

35. The UE of claim 34, wherein the processor is configured to perform at least one of an authentication or registration procedure with the SEAF, prior to receiving the first message, wherein the anchor key is established based on at least one of the authentication or registration procedure.

36. The UE of claim 30, wherein the network policy information comprises a security level of an access and mobility function (AMF).

37. The UE of claim 30, wherein:

the first message is received from an access and mobility management function (AMF) in the network; and

wherein the processor is configured to establish the secure connection by sending a second message to the AMF.

38. The UE of claim 37, wherein:

the first message is a security mode command (SMC) message; and

the second message is a SMC complete message.

39. A security anchor function (SEAF), comprising:

a memory for storing instructions; and

a processor, wherein when the processor executes the instructions, the processor is configured to:

generate a first key for a network node by inputting a second key and network policy information into a key derivation function (KDF), wherein the network policy information comprises security features of the network, and wherein the first key is usable for establishing a secure connection between a user equipment (UE) and the network node; and

send the first key to the network node.

40. The SEAF of claim 39, wherein the processor is configured to participate in at least one of an authentication procedure or registration procedure with the UE prior to generating the first key, wherein the participating comprises establishing an anchor key to be shared between the UE and the SEAF.

41. The SEAF of claim 40, wherein the first key is an access and mobility management function (AMF) key and the second key is the anchor key.

42. The SEAF of claim 39, wherein the processor is configured to send the network policy information to the network node.

43. The SEAF of claim 39, wherein the network policy information comprises an indication of whether the network node is collocated with the SEAF in the network.

44. The SEAF of claim 39, wherein the network policy information comprises a security level of the network node.

45. The SEAF of claim 39, wherein the processor is configured to receive a message comprising policy information of the UE, wherein the UE policy information comprises at least one of UE capability information or UE security information.

46. The SEAF of claim 45, wherein the message comprises a registration message or an attach request message.

47. The SEAF of claim 39, wherein the network node is an access and mobility management function (AMF).