

CLAIMS

1. A key generation method, applied to a terminal device, comprising:

determining a first key KSEAF based on a long-term key K; and

generating a current session key based on the first key KSEAF and at least one of additional keys, and communicating with a network side-device based on the current session key;

wherein the at least one of additional keys comprises: an initial session key generated when the terminal device is connected to a network for the first time and/or a session key used in the previous session, and the first key KSEAF and the additional keys are symmetric keys.

2. The method of claim 1, wherein before determining the first key KSEAF based on the long-term key K, the method further comprises:

when the terminal device is connected to the network for the first time, completing mutual authentication with the network side-device and generating the initial session key.

3. The method of claim 2, wherein generating the current session key based on the first key KSEAF and the at least one of the additional keys comprises:

generating the current session key based on the first key KSEAF and the initial session key.

4. The method of claim 1, wherein generating the current session key based on the first key KSEAF and the at least one of the additional keys comprises:

generating the current session key based on the first key KSEAF and the session key used in the previous session.

5. The method of claim 1 or 2, wherein generating the current session key based on the first key KSEAF and the at least one of the additional keys comprises:

generating the current session key based on the first key KSEAF, the initial session key and the session key used in the previous session.

6. A key generation method, applied to a network device, comprising:

determining a first key KSEAF corresponding to a terminal device based on a long-term key K corresponding to the terminal device; and

generating a current session key corresponding to the terminal device based on the first key KSEAF and at least one of additional keys, and communicating with the terminal device based on the current session key;

wherein the at least one of additional keys comprises: an initial session key generated when the terminal device is connected to a network for the first time and/or a session key used in the previous session with the terminal device, and the first key KSEAF and the additional keys are symmetric keys.

7. The method of claim 6, wherein before determining the first key KSEAF corresponding to the terminal device based on the long-term key K corresponding to the terminal device, the method further comprises:

after the terminal device is connected to the network for the first time and has completed mutual authentication with the network device, generating the initial session key corresponding to the terminal device.

8. The method of claim 7, wherein generating the current session key corresponding to the terminal device based on the first key KSEAF and the at least one of the additional keys

comprises:

generating the current session key used by a network side to communicate with the terminal device based on the first key KSEAF corresponding to the terminal device and the initial session key generated when the terminal device is connected to the network for the first time.

9. The method of claim 6, wherein generating the current session key corresponding to the terminal device based on the first key KSEAF and the at least one of the additional keys comprises:

generating the current session key used by a network side to communicate with the terminal device based on the first key KSEAF and the session key used in the previous session with the terminal device.

10. The method of claim 7, wherein generating the current session key corresponding to the terminal device based on the first key KSEAF and the at least one of the additional keys comprises:

generating the current session key used by a network side to communicate with the terminal device based on the first key KSEAF, the initial session key generated when the terminal device is connected to the network for the first time, and the session key used in the previous session with the terminal device.

11. A terminal device, comprising:

a first key generation unit, configured to determine a first key KSEAF based on a long-term key K, and generate a current session key based on the first key KSEAF and at least one of additional keys; and

a first communication unit, configured to communicate with a network ~~side~~-device based on the current session key;

wherein the at least one of additional keys comprises: an initial session key generated when the terminal device is connected to a network for the first time and/or a session key used in the previous session, and the first key KSEAF and the additional keys are symmetric keys.

12. A terminal device, comprising:

a first processor, configured to determine a first key KSEAF based on a long-term key K, and generate a current session key based on the first key KSEAF and at least one of additional keys; and

a first communication interface, configured to communicate with a network side-device based on the current session key;

wherein the at least one of additional keys comprises: an initial session key generated when the terminal device is connected to a network for the first time and/or a session key used in the previous session, and the first key KSEAF and the additional keys are symmetric keys.

13. The terminal device of claim 12, wherein the first processor is configured to complete, when connecting to the network for the first time, mutual authentication with the network device, and generate the initial session key.

14. The terminal device of claim 13, wherein the first processor is configured to generate the current session key based on the first key KSEAF and the initial session key.

15. The terminal device of claim 12, wherein the first processor is configured to generate the current session key based on the first key KSEAF and the session key used in the previous session.

16. The terminal device of claim 12 or 13, wherein the first processor is configured to generate

the current session key based on the first key KSEAF, the initial session key, and the session key used in the previous session.

17. A network device, comprising:

a second key generation unit, configured to determine a first key KSEAF corresponding to a terminal device based on a long-term key K corresponding to the terminal device, and generate a current session key corresponding to the terminal device based on the first key KSEAF and at least one of additional keys;

a second communication unit, configured to communicate with the terminal device based on the current session key;

wherein the at least one of additional keys comprises: an initial session key generated when the terminal device is connected to a network for the first time and/or a session key used in the previous session with the terminal device, and the first key KSEAF and the additional keys are symmetric keys.

18. A network device, comprising:

a second processor, configured to determine a first key KSEAF corresponding to a terminal device based on a long-term key K corresponding to the terminal device, and generate a current session key corresponding to a terminal device based on the first key KSEAF and at least one of additional keys;

a second communication interface, configured to communicate with the terminal device based on the current session key;

wherein the at least one of additional keys comprises: an initial session key generated when the terminal device is connected to a network for the first time and/or a session key used in the previous session with the terminal device, and the first key KSEAF and the additional keys are symmetric keys.

19. The network device of claim 18, wherein the second processor is configured to generate the initial session key corresponding to the terminal device after the terminal device is connected to the network for the first time and has completed mutual authentication with the network device.

20. The network device of claim 19, wherein the second processor is configured to generate the current session key used by a network side to communicate with the terminal device based on the first key KSEAF corresponding to the terminal device and the initial session key generated when the terminal device is connected to the network for the first time.

21. The network device of claim 18, wherein the second processor is configured to generate the current session key used by a network side to communicate with the terminal device based on the first key KSEAF and the session key used in the previous session with the terminal device.

22. The network device of claim 19, wherein the second processor is configured to generate the current session key used by a network side to communicate with the terminal device based on the first key KSEAF, the initial session key generated when the terminal device is connected to the network for the first time, and the session key used in the previous session with the terminal device.

23. A computer storage medium, having stored a computer program thereon that, when executed by a processor, implements operations of the method of any one of claims 1 to 5.

24. A computer storage medium, having stored a computer program thereon that, when executed by a processor, implements operations of the method of any one of claims 6 to 10.

25. A key generation system, comprising: at least one terminal device and an authentication server function (AUSF) entity; wherein,

the terminal device is configured to determine a first key KSEAF based on a long-term key K, generate a current session key based on the first key KSEAF and at least one of additional keys, and communicate with a network ~~side-device~~ based on the current session key; and

the AUSF entity is configured to determine the first key KSEAF corresponding to the terminal device based on the long-term key K corresponding to the terminal device, generate the current session key corresponding to the terminal device based on the first key KSEAF and the at least one of the additional keys, and communicate with the terminal device based on the current session key; wherein the at least one of additional keys comprises: an initial session key generated when the terminal device is connected to a network for the first time and/or a session key used in the previous session with the terminal device, and the first key KSEAF and the additional keys are symmetric keys.

26. The system of claim 25, further comprising: a unified data management (UDM) entity, configured to complete authentication with the terminal device when the terminal device is connected to the network device for the first time;

the terminal device is configured to complete, when being connected to the network for the first time, authentication with the UDM entity, generate and save the initial session key.

27. The system of claim 26, wherein the terminal device is configured to generate the current session key based on the first key KSEAF and the initial session key;

the AUSF entity is configured to generate the current session key used by the network side to communicate with the terminal device based on the first key KSEAF corresponding to the terminal device and the initial session key generated when the terminal device is connected to the network for the first time.

28. The system of claim 25, wherein the terminal device is configured to generate the current

session key based on the first key KSEAF and the session key used in the previous session;

the AUSF entity is configured to generate the current session key used by the network side to communicate with the terminal device based on the first key KSEAF and the session key used in the previous session with the terminal device.

29. The system of claim 25 or 26, wherein the terminal device is configured to generate the current session key based on the first key KSEAF, the initial session key, and the session key used in the previous session;

the AUSF entity is configured to generate the current session key used by the network side to communicate with the terminal device based on the first key KSEAF, the initial session key generated when the terminal device is connected to the network for the first time, and the session key used in the previous session with the terminal device.